HT801/HT802 Firmware Release Notes

IMPORTANT UPGRADING NOTE

- Once HT801/HT802 is upgraded to 1.0.3.2 or above, downgrading to 1.0.2.x firmware version or lower is not supported.
- Once HT801/HT802 is upgraded to 1.0.2.7, downgrading to 1.0.1.x firmware version or lower is not supported.
# Table of Content

**IMPORTANT UPGRADING NOTE** ................................................................. 1

**FIRMWARE VERSION 1.0.9.3** ................................................................. 5

- PRODUCT NAME ......................................................................................... 5
- DATE ........................................................................................................... 5
- FIRMWARE FILE INFORMATION ................................................................. 5
- ENHANCEMENT ......................................................................................... 5
- BUG FIX ..................................................................................................... 5
- NEW FEATURES OVERVIEW ................................................................. 5
  - CUSTOM CERTIFICATE ............................................................................. 5
  - CONFERENCE PARTY HANGUP TONE ..................................................... 6
  - USE P-ACCESS-NETWORK-INFO HEADER ........................................ 6
  - USE P-EMERGENCY-INFO HEADER ..................................................... 7

**FIRMWARE VERSION 1.0.8.7** ................................................................. 8

- PRODUCT NAME ......................................................................................... 8
- DATE ........................................................................................................... 8
- IMPORTANT UPGRADING NOTE ............................................................. 8
- ENHANCEMENT ......................................................................................... 8
- BUG FIX ..................................................................................................... 8
- NEW FEATURES OVERVIEW ................................................................. 8
  - VALIDATE SERVER CERTIFICATES ....................................................... 9
  - DDNS ........................................................................................................ 9
  - BLACKLIST FOR INCOMING CALLS ..................................................... 10
  - TELNET .................................................................................................... 10
  - PLAY BUSY/REORDER TONE BEFORE LOOP CURRENT DISCONNECT .... 11

**FIRMWARE VERSION 1.0.5.11** ................................................................. 12

- PRODUCT NAME ......................................................................................... 12
- DATE ........................................................................................................... 12
- IMPORTANT UPGRADING NOTE ............................................................. 12
- ENHANCEMENT ......................................................................................... 12
- BUG FIX ..................................................................................................... 13
- NEW FEATURES OVERVIEW ................................................................. 14
  - BLACKLIST FOR WAN SIDE PORT ..................................................... 14
  - RANDOMIZED AUTOMATIC UPGRADE .............................................. 14
AUTOMATIC UPGRADE END HOUR .............................................................. 15
AUTOMATIC REBOOT ................................................................................. 15
RADIUS .......................................................................................................... 16
SNMPv3 ........................................................................................................... 17
EXPORT BACKUP CONFIGURATION .............................................................. 19
RESTORE FROM BACKUP CONFIGURATION .............................................. 19
NEW VIEWER PASSWORD ........................................................................... 20
WEB SESSION TIMEOUT ............................................................................... 20
WEB ACCESS ATTEMPT LIMIT .................................................................... 20
WEB LOCKOUT DURATION ........................................................................... 21
DHCP OPTION 17 ENTERPRISE NUMBER ................................................... 21
CALLER ID FETCH ORDER ......................................................................... 22
ENABLE HIGH RING POWER ........................................................................ 22
ENABLE PULSE DIALING ............................................................................... 23
INTERNET PROTOCOL .................................................................................. 23
IPv6 ADDRESS .............................................................................................. 24

FIRMWARE VERSION 1.0.3.7 ........................................................................ 25

PRODUCT NAME ............................................................................................ 25
DATE .................................................................................................................. 25
IMPORTANT UPGRADING NOTE ................................................................. 25
ENHANCEMENT ............................................................................................. 25
BUG FIX .......................................................................................................... 25
NEW FEATURES OVERVIEW ....................................................................... 26
USE ACTUAL EPHMERAL PORT IN CONTACT WITH TCP/TLS .................. 26
SIP URI SCHEME WHEN USING TLS ........................................................... 26
BACKUP OUTBOUND PROXY ....................................................................... 27
PREFER PRIMARY OUTBOUND PROXY ......................................................... 27
ENABLE RTCP ................................................................................................. 28
HOLD TARGET BEFORE REFER .................................................................... 28
ENABLE SESSION TIMER ........................................................................... 29
CONFERENCE URI .......................................................................................... 29
WHITE LIST FOR WAN SIDE ....................................................................... 30
BLACK LIST FOR WAN SIDE ....................................................................... 30
WEB ACCESS MODE ....................................................................................... 31
HTTPS WEB PORT .......................................................................................... 31
SSH PORT ....................................................................................................... 31
SNMP .............................................................................................................. 32

FIRMWARE VERSION 1.0.3.2 ........................................................................ 33

PRODUCT NAME ............................................................................................ 33
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE</td>
<td>33</td>
</tr>
<tr>
<td>IMPORTANT UPGRADING NOTE</td>
<td>33</td>
</tr>
<tr>
<td>ENHANCEMENT</td>
<td>33</td>
</tr>
<tr>
<td>BUG FIX</td>
<td>33</td>
</tr>
<tr>
<td>NEW FEATURES OVERVIEW</td>
<td>34</td>
</tr>
<tr>
<td>DNS SRV USE REGISTERED IP</td>
<td>34</td>
</tr>
<tr>
<td>FIRMWARE VERSION 1.0.2.7</td>
<td>35</td>
</tr>
<tr>
<td>PRODUCT NAME</td>
<td>35</td>
</tr>
<tr>
<td>DATE</td>
<td>35</td>
</tr>
<tr>
<td>IMPORTANT UPGRADING NOTE</td>
<td>35</td>
</tr>
<tr>
<td>ENHANCEMENT</td>
<td>35</td>
</tr>
<tr>
<td>BUG FIX</td>
<td>35</td>
</tr>
<tr>
<td>FIRMWARE VERSION 1.0.2.5</td>
<td>36</td>
</tr>
<tr>
<td>PRODUCT NAME</td>
<td>36</td>
</tr>
<tr>
<td>DATE</td>
<td>36</td>
</tr>
<tr>
<td>IMPORTANT UPGRADING NOTE</td>
<td>36</td>
</tr>
<tr>
<td>KNOWN ISSUE</td>
<td>36</td>
</tr>
<tr>
<td>ENHANCEMENT</td>
<td>36</td>
</tr>
<tr>
<td>BUG FIX</td>
<td>36</td>
</tr>
<tr>
<td>NEW FEATURES OVERVIEW</td>
<td>36</td>
</tr>
<tr>
<td>OPUS PAYLOAD TYPE DEFAULT VALUE</td>
<td>36</td>
</tr>
<tr>
<td>FIRMWARE VERSION 1.0.2.3</td>
<td>38</td>
</tr>
<tr>
<td>PRODUCT NAME</td>
<td>38</td>
</tr>
<tr>
<td>DATE</td>
<td>38</td>
</tr>
<tr>
<td>IMPORTANT UPGRADING NOTE</td>
<td>38</td>
</tr>
<tr>
<td>ENHANCEMENT</td>
<td>38</td>
</tr>
<tr>
<td>BUG FIX</td>
<td>38</td>
</tr>
<tr>
<td>NEW FEATURES OVERVIEW</td>
<td>39</td>
</tr>
<tr>
<td>PASSWORD CHANGE CONFIRMATION</td>
<td>39</td>
</tr>
</tbody>
</table>
FIRMWARE VERSION 1.0.9.3

PRODUCT NAME
HT801, HT802

DATE
05/15/2018

FIRMWARE FILE INFORMATION
- HT801 firmware file name: ht801fw.bin
  MD5: bc86e8e094db5c157808f37fd04bf421
- HT802 firmware file name: ht802fw.bin
  MD5: fc7886794222920e831f7492a5aff46b

ENHANCEMENT
- Added feature “Custom Certificate”. [CUSTOM CERTIFICATE]
- Added feature “Conference Party Hangup Tone”. [CONFERENCE PARTY HANGUP TONE]
- Added feature “Use P-Access-Network-Info Header”. [USE P-ACCESS-NETWORK-INFO HEADER]
- Added feature “Use P-Emergency-Info Header”. [USE P-EMERGENCY-INFO HEADER]
- Add support for call waiting tone to be repeated while the caller is still calling.
- Add support for HTTPS based on TLS v1.2

BUG FIX
- Fixed device would not auto-reboot after factory reset via TR-069.
- Fixed when using pulse dialing mode, device plays dial tone after first digit.
- Fixed device stops communicating with TR-069 server when receiving GetOptions RPC Method.
- Change “Validate Server Certificates” default value to No.

NEW FEATURES OVERVIEW
This section lists major new features and describes how to use it from the user’s point of view.

CUSTOM CERTIFICATE
- Web Configuration
User can find the configuration in Web UI -> Advanced Settings.
**Functionality**
This feature allows users to update to the device their own certificate signed by custom CA certificate to manage client authentication.

**New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P8472</td>
<td>Custom Certificate (Private Key + Certificate)</td>
<td>10 - Rows</td>
<td>Null</td>
</tr>
<tr>
<td></td>
<td></td>
<td>64 - Columns</td>
<td></td>
</tr>
</tbody>
</table>

**CONFERENCE PARTY HANGUP TONE**

**Web Configuration**
User can find the configuration in Web UI -> Advanced Settings.

Syntax: \( f1=\text{val1}, f2=\text{val2}, c=\text{on1/off1}[-\text{on2/off2}[-\text{on3/off3}]] \)

(Frequencies are in (300, 3400) Hz and cadence on and off are in (0, 64000) ms)

**Functionality**
With this feature, device will play custom tone when a party leave the established 3-way conference. User needs to set "Special Feature" to MTS to use this function.

**New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P28133</td>
<td>Conference Party Hangup Tone</td>
<td>(300, 3400) Hz – Frequency (0, 64000) ms – cadence on and off</td>
<td>( f1=425@-15,c=600/600; )</td>
</tr>
</tbody>
</table>

**USE P-ACCESS-NETWORK-INFO HEADER**

**Web Configuration**
User can find the configuration in Web UI -> Profile Settings.
- **Functionality**
  With this feature enabled, device will populate the WAN access node with IEEE-802.11a, IEEE-802.11b in P-Access-Network-Info SIP header.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P26058</td>
<td>Use P-Access-Network-Info Header (FXS 1)</td>
<td>0 - No 1 - Yes</td>
<td>1 - Yes</td>
</tr>
<tr>
<td>P26158</td>
<td>Use P-Access-Network-Info Header (FXS 2)</td>
<td>0 - No 1 - Yes</td>
<td>1 - Yes</td>
</tr>
</tbody>
</table>

**USE P-EMERGENCY-INFO HEADER**

- **Web Configuration**
  User can find the configuration in Web UI -> Profile Settings.

- **Functionality**
  This feature support of IEEE-48-addr and IEEE-EUI-64 in SIP header for emergency calls.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P26059</td>
<td>Use P-Emergency-Info Header (FXS 1)</td>
<td>0 - No 1 - Yes</td>
<td>1 - Yes</td>
</tr>
<tr>
<td>P26159</td>
<td>Use P-Emergency-Info Header (FXS 2)</td>
<td>0 - No 1 - Yes</td>
<td>1 - Yes</td>
</tr>
</tbody>
</table>
FIRMWARE VERSION 1.0.8.7

PRODUCT NAME
HT801, HT802

DATE
04/16/2018

IMPORTANT UPGRADING NOTE
- Once HT801/HT802 is upgraded to 1.0.8.7, downgrading to 1.0.2.x firmware version or lower is not supported.

ENHANCEMENT
- Added “MTS” to Special Feature.
- Added support for Russian in WebUI and IVR.
- Added support for upgrade device via FTP/FTPS server.
- Added support to have the call waiting tone through SIP INFO.
- Added feature “Validate Server Certificates”. [VALIDATE SERVER CERTIFICATES]
- Added support for DDNS. [DDNS]
- Added feature Blacklist for Incoming Calls. [BLACKLIST FOR INCOMING CALLS]
- Added support for Telnet. [TELNET]
- Added feature “Play busy/reorder tone before Loop Current Disconnect.” [PLAY BUSY/REORDER TONE BEFORE LOOP CURRENT DISCONNECT]

BUG FIX
- Fixed device queried wrong FQDN.
- Fixed device played random DTMF during conversation.
- Fixed device missing parameter to configure the off-hook auto dial feature.
- Fixed device does not receive Connection Request from ACS.
- Fixed unselected syslog levels messages are sent from device.
- Fixed device failed to resolve Backup Outbound Proxy domain name.
- Fixed when device DNS mode set to NAPTR/SRV, device failed to send domain name resolution to preferred DNS server.
- Fixed device would send domain resolution to DHCPv6’s DNS server when Internet protocol set to Prefer IPv4.

NEW FEATURES OVERVIEW
This section lists major new features and describes how to use it from the user’s point of view.
VALIDATE SERVER CERTIFICATES

- **Web Configuration**
  User can find the configuration in Web UI -> Advanced Settings.

- **Functionality**
  This feature allows users to validate server certificates with our trusted list of TLS connections. Default is enabled. The device needs to reboot after changing the setting.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P8463</td>
<td>Validate Server Certificates</td>
<td>0 - No</td>
<td>0 - No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - Yes</td>
<td></td>
</tr>
</tbody>
</table>

DDNS

- **Web Configuration**
  User can find the configuration in Web UI -> Advanced Settings.

- **Functionality**
  Allow users to use DDNS.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P28121</td>
<td>Enable DDNS</td>
<td>0 - No</td>
<td>0 - No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - Yes</td>
<td></td>
</tr>
<tr>
<td>P28122</td>
<td>DDNS Server</td>
<td>0 - dyndns.org</td>
<td>0 – dyndns.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - freedns.afraid.org</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - zoneedit.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - no-ip.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - oray.net</td>
<td></td>
</tr>
<tr>
<td>P28123</td>
<td>DDNS Username</td>
<td>64 – Max String Length</td>
<td>Null</td>
</tr>
</tbody>
</table>
BLACKLIST FOR INCOMING CALLS

- **Web Configuration**
  User can find the configuration section at Web -> Advanced Settings.

  ![Blacklist For Incoming Calls](image)

- **Functionality**
  Allow users to block incoming calls from specific list of numbers. Maximum allow 10 SIP numbers and each number should be separated by a comma (',') in webUI. Other allowed characters are 0-9, 26 letters (A-Z and a-z), comma (""), asterisk ('*'), pound sign ('#') and plus sign ('+').

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P28127</td>
<td>Blacklist For Incoming Calls</td>
<td>10 – Maximum allowed SIP numbers</td>
<td>Null</td>
</tr>
</tbody>
</table>

TELNET

- **Web Configuration**
  User can find the configuration section at Web -> Basic Settings.

  ![Enable Telnet and Disable Telnet](image)

- **Functionality**
  This feature allows users to access device CLI by using Telnet. The default Telnet port is 23, this should be different from SSH port.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P28120</td>
<td>Disable Telnet</td>
<td>0 - No 1 - Yes</td>
<td>1 - Yes</td>
</tr>
<tr>
<td>P28128</td>
<td>Telnet Port</td>
<td>5 – Max String Length</td>
<td>23</td>
</tr>
</tbody>
</table>
PLAY BUSY/REORDER TONE BEFORE LOOP CURRENT DISCONNECT

- **Web Configuration**
  User can find the configuration section at Web -> Profile Settings.

  ![](Play%20busy/reorder%20tone%20before%20Loop%20Current.png)

- **Functionality**
  Allow user to configure if it will play busy/reorder tone before loop current disconnect upon call fail. Default is No.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P21925</td>
<td>Play busy/reorder tone before Loop Current Disconnect. (FXS 1)</td>
<td>0 - No</td>
<td>0 – No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td></td>
</tr>
<tr>
<td>P21926</td>
<td>Play busy/reorder tone before Loop Current Disconnect (FXS 2)</td>
<td>0 - No</td>
<td>0 – No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td></td>
</tr>
</tbody>
</table>
FIRMWARE VERSION 1.0.5.11

PRODUCT NAME
HT801 and HT802

DATE
12/13/2017

IMPORTANT UPGRADING NOTE
- Once HT801/HT802 is upgraded to 1.0.5.11, downgrading to 1.0.2.x firmware version or lower is not supported.

ENHANCEMENT
- Added support for DHCP option 33.
- Added support for DHCP option 121.
- Added feature "Black List for WAN Side Port". [BLACKLIST FOR WAN SIDE PORT]
- Added feature “Randomized Automatic Upgrade”. [RANDOMIZED AUTOMATIC UPGRADE]
- Added feature “Automatic Upgrade End Hour”. [AUTOMATIC UPGRADE END HOUR]
- Added feature “Automatic Reboot”. [AUTOMATIC REBOOT]
- Added support for RADIUS. [RADIUS]
- Added support for SNMPv3. [SNMPv3]
- Added feature “Export Backup Configuration”. [EXPORT BACKUP CONFIGURATION]
- Added feature "Restore From Backup Configuration". [RESTORE FROM BACKUP CONFIGURATION]
- Added feature “New Viewer Password”. [NEW VIEWER PASSWORD]
- Added feature “Web Session Timeout”. [WEB SESSION TIMEOUT]
- Added feature “Web Access Attempt Limit”. [WEB ACCESS ATTEMPT LIMIT]
- Added feature “Web Lockout Duration”. [WEB LOCKOUT DURATION]
- Added support for DHCP option 124, 125 for TR069.
- Added support for DHCPv6 option 16 for TR069.
- Added support for DHCP option 17 in IPv6 implementation.
- Added feature “DHCP Option 17 Enterprise Number”. [DHCP OPTION 17 ENTERPRISE NUMBER]
- Added feature “Caller ID Fetch Order” to specify the priority for caller ID display. [CALLER ID FETCH ORDER]
- Added option “Enable High Ring Power”. [ENABLE HIGH RING POWER]
- Added option “Enable Pulse Dialing”. [ENABLE PULSE DIALING]
- Added option to disable/enable HTTP Web Access.
- Added dial plan rule timer T.
• Added feature “Internet Protocol” to choose from “IPv4 Only”, “IPv6 Only”, “Both, prefer IPv4”, “Both, prefer IPv6”. [INTERNET PROTOCOL]
• Added feature “IPv6 Address” to configure IPv6 Address. [IPv6 ADDRESS]

BUG FIX
• Fixed device does not register when enable Allow Incoming SIP Messages from SIP Proxy Only.
• Fixed web vulnerability about CSRF and XSS.
• Fixed device cannot connect to ACS server when using PPPoE IPv4.
• Fixed device would crash after being transferred during in IP call.
• Fixed device does not auto-reboot after factory reset via TR069.
• Fixed set Web Access Mode to HTTPS via TR069, it would take effect as HTTP.
• Fixed device LED light would always be flashing and unable to reboot when switched the web page during uploading the firmware.
• Fixed device does not request a DNS IP from the PPPoE server.
• Fixed sometimes device could not access the web page when Internet Protocol change from preferred IPv6 to IPv6 Only.
• Fixed when IPv4 set to PPPoE, device could not login via SSH after set the Internet Protocol to IPv6 Only.
• Fixed the static IPv6 address does not take effect when device using PPPoE IPv4 address.
• Fixed device failed in adding the Trusted CA.
• Fixed device does not request config file from updated config server path.
• Fixed device would send domain name resolution to DHCPv6’s DNS server when Internet protocol set to prefer IPv4.
• Fixed device always displays the IPv6 DNS server in SSH.
• Fixed device always uses the stateful IPv6 address even the DHCPv6 server is used.
• Fixed after device reboot, port will be detected as “Off Hook” status.
• Fixed device only supports 3 RENs.
• Fixed when login the device via SSH, needs to enter password twice.
• Fixed the 3rd and 4th preferred DNS server do not take effect.
• Fixed ACS cannot connect to DUT after DUT connects ACS using internal IP.
• Fixed the URL with underscore "_" is not supported.
• Fixed device drop call after receiveT.38 re-invite.
• Fixed device does not open a new TCP window when registration over TLS fails.
• Fixed device would not send register message when enabling PPPoE.
• Fixed device would not auto-reboot after factory reset via TR-069.
• Fixed device would not download configuration or firmware when the Internet protocol is set to IPv6 Only.
• Fixed DHCP option 120 does not take effect when using IPv6.
• Fixed device prompts wrong IP address in IVR when using static IP address.
• Fixed when logging in device via SSH, IPv6 DNS server does not display.
• Fixed when using static IPv4 address, device could not make calls when Internet protocol is set to IPv6 Only.
• Fixed device could not check IPv6 address via IVR.
• Fixed device does not perform IPv6 DNS query for ACS URL.
• Fixed device does not implement HTTPS TR-069 connection when Internet Protocol is set to IPv6 Only.

NEW FEATURES OVERVIEW
This section lists major new features and describes how to use it from the user’s point of view.

BLACKLIST FOR WAN SIDE PORT
• Web Configuration
User can find the configuration in Web UI -> Advanced Settings.

![Black List for WAN Side Port](image)

**Stun server is:** [(URI or IP:port)]

• Functionality
This feature allows users to manually block specific ports or ports range. Users can disable the port with following type of port range (take port1, port2 and port 3 as an example):

1) P1,P2-P3
   This type allows users to disable the port P1, P2 to P3
2) -P1,P2-P3
   This type allows users to disable the port from 0 to P1 and disable port from P2 to P3
3) P1-
   This type allows users to disable the port from P1 to P65535

The following ASCII characters are valid:
1) ‘0’ – ‘9’: Port number
2) ‘,’ : Separator for different port or port range
3) ‘-‘: Used to indicate the port range

• New P Values

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P28115</td>
<td>Black List for WAN Side Port</td>
<td>0 – 65535</td>
<td>None</td>
</tr>
</tbody>
</table>

RANDOMIZED AUTOMATIC UPGRADE
• Web Configuration
User can find the configuration in Web UI -> Advanced Settings.
**Functionality**
Allow user to enable Randomized Automatic Upgrade. When this feature enabled, user could customize device random firmware/configuration download start/end time to avoid that all device is upgraded at the same time when it makes a change on firmware/configuration files.

**New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P8458</td>
<td>Randomized Automatic Upgrade</td>
<td>0 – No</td>
<td>1 - Yes</td>
</tr>
</tbody>
</table>

**AUTOMATIC UPGRADE END HOUR**

**Functionality**
When “Automatic Upgrade” is set to “Yes, daily at”, users can choose a start time and end time of one day when the phone will request the firmware/config file.

**New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P8459</td>
<td>Automatic Upgrade End Hour</td>
<td>0 – 23</td>
<td>22</td>
</tr>
</tbody>
</table>

**AUTOMATIC REBOOT**

**Functionality**
This feature allows users to configure a specific day on a month to auto restart the device.
• **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P21929</td>
<td>Automatic Reboot</td>
<td>0 – No, 1 – Yes, reboot every day at hour, 2 – Yes, reboot every week at day, 3 – Yes, reboot every month at day</td>
<td>0 - No</td>
</tr>
<tr>
<td>P21930</td>
<td>Automatic reboot hour of day</td>
<td>0 – 23</td>
<td>1</td>
</tr>
<tr>
<td>P21931</td>
<td>Automatic reboot day of week</td>
<td>0 – 6</td>
<td>1</td>
</tr>
<tr>
<td>P28118</td>
<td>Automatic reboot at day of the month</td>
<td>0 – 30</td>
<td>1</td>
</tr>
</tbody>
</table>

**RADIUS**

• **Web Configuration**

User can find the configuration section at Web -> Advanced Settings.

![Enable RADIUS Web Access Control: No Yes](image)

- **Action upon Radius Auth Server Error:**
  - Reject Access
  - Authenticate Locally

- **RADIUS Auth Server Address:**
- **RADIUS Auth Server Port:**
- **RADIUS Shared Secret:**
- **RADIUS VSA Vendor ID:** 42397
- **RADIUS VSA Access Level Attribute:**

• **Functionality**

Allow user to “Enable RADIUS Web Access Control” and configure three level access through RADIUS authorization. Grandstream Vendor ID is 42397.

• **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P28107</td>
<td>Enable RADIUS Web Access Control</td>
<td>0 – No, 1 – Yes</td>
<td>0 – No</td>
</tr>
<tr>
<td>P28114</td>
<td>Action upon Radius Auth Server Error</td>
<td>0 – Reject Access, 1 – Authenticate Locally</td>
<td>1 – Authenticate Locally</td>
</tr>
<tr>
<td>P28108</td>
<td>RADIUS Auth Server Address</td>
<td>64 - Max Character Number</td>
<td>None</td>
</tr>
</tbody>
</table>
P28109  RADIUS Auth Server Port  64 - Max Character Number  None
P28110  RADIUS Shared Secret  64 - Max Character Number  None
P28111  RADIUS VSA Vendor ID  64 - Max Character Number  42397
P28112  RADIUS VSA Access Level Attribute  64 - Max Character Number  None

SNMPv3

- **Web Configuration**
  User can find the configuration section at Web -> Advanced Settings.

- **Functionality**
  This function allows users to configure SNMPv3 feature.

- **New P Values**
<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P21904</td>
<td>SNMP Version</td>
<td>1 – Version 1</td>
<td>3 – Version 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 – Version 2c</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 – Version 3</td>
<td></td>
</tr>
<tr>
<td>P21903</td>
<td>SNMP Port</td>
<td>162 or 1025-65535</td>
<td>162</td>
</tr>
<tr>
<td>P21902</td>
<td>SNMPv1/v2c Community</td>
<td>64 - Max Character Number</td>
<td>None</td>
</tr>
<tr>
<td>P21905</td>
<td>SNMPv3 User Name</td>
<td>64 - Max Character Number</td>
<td>None</td>
</tr>
<tr>
<td>P21910</td>
<td>SNMPv3 Security Level</td>
<td>0 – noAuthUser</td>
<td>0 - None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – authUser</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - privUser</td>
<td></td>
</tr>
<tr>
<td>P21906</td>
<td>SNMPv3 Authentication Protocol</td>
<td>0 – None</td>
<td>0 - None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – MD5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 – SHA</td>
<td></td>
</tr>
<tr>
<td>P21907</td>
<td>SNMP Privacy Protocol</td>
<td>0 – None</td>
<td>0 – None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – DES</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 – AES</td>
<td>AES128</td>
</tr>
<tr>
<td>P21908</td>
<td>SNMPv3 Authentication Key</td>
<td>5 – Rows</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>64 – Columns</td>
<td></td>
</tr>
<tr>
<td>P21909</td>
<td>SNMPv3 Privacy Key</td>
<td>5 – Rows</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>64 – Columns</td>
<td></td>
</tr>
<tr>
<td>P21911</td>
<td>SNMPv3 Trap User Name</td>
<td>64 - Max Character Number</td>
<td>None</td>
</tr>
<tr>
<td>P21916</td>
<td>SNMPv3 Trap Security Level</td>
<td>0 – noAuthUser</td>
<td>0 - noAuthUser</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – authUser</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - privUser</td>
<td></td>
</tr>
<tr>
<td>P21912</td>
<td>SNMPv3 Trap Authentication Protocol</td>
<td>0 – None</td>
<td>0 - None</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>1 – MD5</td>
<td>2 - SHA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P21913 SNMP Trap Privacy Protocol</td>
<td>0 – None</td>
<td>0 – None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 – DES</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 – AES</td>
<td>AES-128</td>
<td></td>
</tr>
<tr>
<td>P21914 SNMPv3 Trap Authentication Key</td>
<td>5 – Rows</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>64 – Columns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P21915 SNMPv3 Trap Privacy Key</td>
<td>5 – Rows</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>64 – Columns</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**EXPORT BACKUP CONFIGURATION**

- **Web Configuration**
  User can find the configuration in Web UI -> Advanced Settings.

- **Functionality**
  Export backup package which contains device configuration along with personal data.

**RESTORE FROM BACKUP CONFIGURATION**

- **Web Configuration**
  User can find the configuration in Web UI -> Advanced Settings.

- **Functionality**
  This feature allows users to upload backup package and restore.
NEW VIEWER PASSWORD

- Web Configuration
User can find the configuration section at Web -> Basic Settings.

![New Viewer Password](purposely not displayed for security protection)

- Functionality
Allow users to configure Viewer Password. The default viewer password is viewer.

- New P Values

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P28113</td>
<td>New Viewer Password</td>
<td>30 – Max Character Number</td>
<td>viewer (purposely not displayed for security protection)</td>
</tr>
</tbody>
</table>

WEB SESSION TIMEOUT

- Web Configuration
User can find the configuration section at Web -> Basic Settings.

![Web/SSH Access:](Web Session Timeout: 10 (1-60, default 10 minutes.)  
Web Access Attempt Limit: 5 (1-10, default 5.)  
Web Lockout Duration: 15 (0-60, default 15 minutes.)

- Functionality
This feature allows users to set the idle time to logout the user from the Web.

- New P Values

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P28116</td>
<td>Web Session Timeout</td>
<td>1 - 60 minutes</td>
<td>10 minutes</td>
</tr>
</tbody>
</table>

WEB ACCESS ATTEMPT LIMIT

- Web Configuration
User can find the configuration section at Web -> Basic Settings.

![Web/SSH Access:](Web Session Timeout: 60 (1-60, default 10 minutes.)  
Web Access Attempt Limit: 5 (1-10, default 5.)  
Web Lockout Duration: 15 (0-60, default 15 minutes.)
• **Functionality**
  This feature allows users to customize the number of failed attempt that the device will allow to block the web access.

• **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P28117</td>
<td>Web Access Attempt Limit</td>
<td>1 - 10</td>
<td>5</td>
</tr>
</tbody>
</table>

**WEB LOCKOUT DURATION**

• **Web Configuration**
  User can find the configuration section at Web -> Basic Settings.

  ![Web/SSH Access](image)

• **Functionality**
  This feature allows users to customize the duration that the web UI access will be blocked due to failed login attempt.

• **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1683</td>
<td>Web Lockout Duration</td>
<td>0 – 60 minutes</td>
<td>15 minutes</td>
</tr>
</tbody>
</table>

**DHCP OPTION 17 ENTERPRISE NUMBER**

• **Web Configuration**
  User can find the configuration in Web UI -> Advanced Settings.

  ![DHCP Option 17 Enterprise Number](image)

• **Functionality**
  Set DHCP Option 17 Enterprise Number. The default value is “3561”

• **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P8457</td>
<td>DHCP Option 17 Enterprise Number</td>
<td>5 – Max Character Number</td>
<td>3561</td>
</tr>
</tbody>
</table>
CALLER ID FETCH ORDER

- **Web Configuration**
  User can find the configuration section at Web -> FXS Port

![Caller ID Fetch Order: Auto Disabled From Header]

**Functionality**
Allow users to configure Caller ID display from SIP INVITE based on option “Auto”, “Disabled” or “From Header”. In "Auto" mode, device will look for the caller ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and From Header in the coming SIP INVITE. In “Disabled” mode, all incoming calls caller ID will be disabled. In “From Header” mode, device will search caller ID from ‘FROM’ header of incoming calls.

**New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2324</td>
<td>Caller ID Fetch Order. (FXS 1)</td>
<td>0 – Auto, 1 - Disabled, 2 – From Header</td>
<td>0 – Auto</td>
</tr>
<tr>
<td>P2424</td>
<td>Caller ID Fetch Order. (FXS 2)</td>
<td>0 - Auto, 1 - Disabled, 2 - From Header</td>
<td>0 – Auto</td>
</tr>
</tbody>
</table>

ENABLE HIGH RING POWER

- **Web Configuration**
  User can find the configuration section at Web -> FXS Port.

![Ring Frequency: 20 (15-60 Hz, default is 20 Hz )]

**Functionality**
Allow users to enable High Ring Power option under FXS port.

**New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P4234</td>
<td>Enable High Ring Power. (FXS 1)</td>
<td>0 - No</td>
<td>0 – No</td>
</tr>
</tbody>
</table>
### Enable Pulse Dialing

- **Web Configuration**
  User can find the configuration section at Web -> FXS Port.

  ![Enable Pulse Dialing: No Yes](image)

  ![Enable Hook Flash: No Yes](image)

- **Functionality**
  Allow users to enable Pulse Dialing option under FXS Port.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P20521</td>
<td>Enable Pulse Dialing. (FXS 1)</td>
<td>0 - No</td>
<td>0 – No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td></td>
</tr>
<tr>
<td>P20522</td>
<td>Enable Pulse Dialing. (FXS 2)</td>
<td>0 - No</td>
<td>0 – No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td></td>
</tr>
</tbody>
</table>

### Internet Protocol

- **Web Configuration**
  User can find the configuration in Web UI -> Basic Settings.

  ![Internet Protocol: IPv4 Only IPv6 Only Both, prefer IPv4 Both, prefer IPv6](image)

  ![IPv4 Address: dynamically assigned via DHCP DHCP hostname: optional](image)

- **Functionality**
  Selects Internet protocol. The default setting is “IPv4 Only”.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1415</td>
<td>Internet Protocol</td>
<td>0 – Both, prefer IPv4 1 – Both, prefer IPv6</td>
<td>2 – IPv4 Only</td>
</tr>
</tbody>
</table>
IPv6 ADDRESS

- **Web Configuration**
  User can find the configuration section at Web -> Basic Settings.

  ![IPv6 Address Configuration](image)

- **Functionality**
  Allow users to configure the appropriate network settings to obtain IPv6 address.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1419</td>
<td>IPv6 Address dynamically assigned via DHCP or statically configured</td>
<td>0 – dynamically assigned via DHCP 1 – statically configured as</td>
<td>0 – dynamically assigned via DHCP</td>
</tr>
<tr>
<td>P1420</td>
<td>Static IPv6 Address for Full Static mode</td>
<td>40 – Max Character Number</td>
<td>Null</td>
</tr>
<tr>
<td>P1421</td>
<td>IPv6 Prefix Length for Full Static mode</td>
<td>3 – Max Character Number</td>
<td>Null</td>
</tr>
<tr>
<td>P1422</td>
<td>IPv6 Prefix (64 bits) for Prefix Static mode</td>
<td>40 – Max Character Number</td>
<td>Null</td>
</tr>
<tr>
<td>P1423</td>
<td>Preferred DNS Server</td>
<td>40 – Max Character Number</td>
<td>Null</td>
</tr>
<tr>
<td>P1424</td>
<td>DNS Server 1</td>
<td>40 – Max Character Number</td>
<td>Null</td>
</tr>
<tr>
<td>P1425</td>
<td>DNS Server 2</td>
<td>40 – Max Character Number</td>
<td>Null</td>
</tr>
</tbody>
</table>
FIRMWARE VERSION 1.0.3.7

PRODUCT NAME
HT802 and HT801

DATE
07/05/2017

IMPORTANT UPGRADING NOTE
• Once HT802/HT801 is upgraded to 1.0.3.7, downgrading to 1.0.2.x firmware version or lower is not supported.

ENHANCEMENT
• Added option “Use Actual Ephemeral Port in Contact with TCP/TLS” to force device to use actual ephemeral port. [USE ACTUAL EPHEMERAL PORT IN CONTACT WITH TCP/TLS]
• Added option “SIP URI Scheme When Using TLS” to choose between ‘SIP’ and ‘SIPS’. [SIP URI SCHEME WHEN USING TLS]
• Added Option “Backup Outbound Proxy” to use backup Outbound Proxy if Outbound Proxy registration expires. [BACKUP OUTBOUND PROXY]
• Added option “Prefer Primary Outbound Proxy” to enable registration through primary outbound proxy if registration expires. [PREFER PRIMARY OUTBOUND PROXY]
• Added option “Enable RTCP” to enable RTCP function through Web UI. [ENABLE RTCP]
• Added option “Hold Target Before Refer” to enable device to hold before being referred. [HOLD TARGET BEFORE REFER]
• Added Option “Enable Session Timer” to disable session timer. [ENABLE SESSION TIMER]
• Added feature “Conference URI” to support Conference URI. [CONFERENCE URI]
• Added feature “White List for WAN Side” for remote management. [WHITE LIST FOR WAN SIDE]
• Added feature “Black List for WAN Side” for remote management. [BLACK LIST FOR WAN SIDE]
• Added option “Web Access Mode” to choose between “HTTPS” and “HTTP” to access device Web UI. [WEB ACCESS MODE]
• Added feature “HTTPS Web Port” to set HTTPS web port instead of using default HTTPS port. [HTTPS WEB PORT]
• Added feature “SSH Port” to self-configure SSH port. [SSH PORT]
• Added SNMP related features. [SNMP]

BUG FIX
• Fixed device could not offhook and it keeps sending registration packet after call is canceled.
- Fixed device would not send SIP Register message to failover SIP server when registration to primary SIP server fails.
- Fixed device does not contact ACS after being provisioned from GAPS.
- Fixed device is missing parameter on TR-069.
- Fixed device does not send keep-alive signal on initial provision.
- Fixed device session re-transmission mechanism does not work.
- Fixed device crashes randomly without generating core dump.

NEW FEATURES OVERVIEW
This section lists major new features and describes how to use it from the user's point of view.

USE ACTUAL EPHEMERAL PORT IN CONTACT WITH TCP/TLS
- **Web Configuration**
User can find the configuration in Web UI -> Profile Settings page.

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2331</td>
<td>Use Actual Ephemeral Port in Contact with TCP/TLS. (FXS 1)</td>
<td>0 – No</td>
<td>0 – No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td></td>
</tr>
<tr>
<td>P2431</td>
<td>Use Actual Ephemeral Port in Contact with TCP/TLS. (FXS 2)</td>
<td>0 – No</td>
<td>0 – No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td></td>
</tr>
</tbody>
</table>

SIP URI SCHEME WHEN USING TLS
- **Web Configuration**
User can find the configuration under Web UI -> Profile Settings page.
- **Functionality**
  Specifies if "sip" or "sips" will be used when TLS/TCP is selected for SIP Transport. The default setting is "sips".

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2329</td>
<td>SIP URI Scheme When Using TLS. (FXS 1)</td>
<td>0 – No</td>
<td>1 – Yes</td>
</tr>
<tr>
<td>P2429</td>
<td>SIP URI Scheme When Using TLS (FXS 2)</td>
<td>0 – No</td>
<td>1 – Yes</td>
</tr>
</tbody>
</table>

**BACKUP OUTBOUND PROXY**

- **Web Configuration**
  User can find the configuration under web UI -> Profile Settings page.

- **Functionality**
  If the user has configured backup outbound proxy, when the "Outbound Proxy" registration fails, device will use the backup outbound proxy. By default, this field is left empty.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2333</td>
<td>Backup Outbound Proxy. (FXS 1)</td>
<td>96 - Max String Length</td>
<td>Null</td>
</tr>
<tr>
<td>P2433</td>
<td>Backup Outbound Proxy. (FXS 2)</td>
<td>96 – Max String Length</td>
<td>Null</td>
</tr>
</tbody>
</table>

**PREFER PRIMARY OUTBOUND PROXY**

- **Web Configuration**
  User can find the configuration under web UI -> Profile Settings page.
• **Functionality**
  If the user configures this option to “Yes”, when registration expires, device will re-register via primary outbound proxy. By default, this option is disabled.

• **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P28096</td>
<td>Prefer Primary Outbound Proxy. (FXS 1)</td>
<td>0 – No</td>
<td>0 – No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td></td>
</tr>
<tr>
<td>P28097</td>
<td>Prefer Primary Outbound Proxy. (FXS 2)</td>
<td>0 – No</td>
<td>0 – No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td></td>
</tr>
</tbody>
</table>

**ENABLE RTCP**

• **Web Configuration**
  User can find the configuration under web UI -> Profile Settings page.

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2392</td>
<td>Enable RTCP. (FXS 1)</td>
<td>0 – No</td>
<td>1 – Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td></td>
</tr>
<tr>
<td>P2492</td>
<td>Enable RTCP. (FXS 2)</td>
<td>0 – No</td>
<td>1 – Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td></td>
</tr>
</tbody>
</table>

**HOLD TARGET BEFORE REFER**

• **Web Configuration**
  User can find the configuration under web UI -> Profile Settings page.

• **Functionality**
This function allows user to hold or not hold the phone call before referring. The default setting is “Yes”.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P26003</td>
<td>Hold Target Before Refer. (FXS 1)</td>
<td>0 – No</td>
<td>1 – Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td>1 – Yes</td>
</tr>
<tr>
<td>P26103</td>
<td>Hold Target Before Refer. (FXS 2)</td>
<td>0 – No</td>
<td>1 – Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td>1 – Yes</td>
</tr>
</tbody>
</table>

**ENABLE SESSION TIMER**

- **Web Configuration**

User can find the configuration under Web -> Profile Settings page.

![Enable Session Timer](image)

- **Functionality**

If set this option to “No”, session timer will be disabled. By default, this option is enabled.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2395</td>
<td>Enable Session Timer. (FXS 1)</td>
<td>0 – No</td>
<td>1 – Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td>1 – Yes</td>
</tr>
<tr>
<td>P2495</td>
<td>Enable Session Timer. (FXS 2)</td>
<td>0 – No</td>
<td>1 – Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td>1 – Yes</td>
</tr>
</tbody>
</table>

**CONFERENCE URI**

- **Web Configuration**

User can find the configuration under web UI -> Profile Settings page.

![Conference URI](image)

- **Functionality**

This option allows to manually configure conference URL. The default is null.

- **New P Values**
<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2318</td>
<td>Conference URI. (FXS 1)</td>
<td>1024 - Max String Length</td>
<td>Null</td>
</tr>
<tr>
<td>P2418</td>
<td>Conference URI. (FXS 2)</td>
<td>1024 – Max String Length</td>
<td>Null</td>
</tr>
</tbody>
</table>

**WHITE LIST FOR WAN SIDE**

- **Web Configuration**
  User can find the configuration under web UI -> Basic Settings page.

  ![Image of white list config]

- **Functionality**
  This function allows users to list White List for WAN Side used for remote management.

  **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P20701</td>
<td>White List for WAN Side</td>
<td>3 –Rows</td>
<td>Null</td>
</tr>
<tr>
<td></td>
<td></td>
<td>51 – Columns</td>
<td></td>
</tr>
</tbody>
</table>

**BLACK LIST FOR WAN SIDE**

- **Web Configuration**
  User can find the configuration under Web UI -> Basic Settings page.

  ![Image of black list config]

- **Functionality**
  This function allows users list Black List for WAN Side to ban WAN side web access.

  **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P20702</td>
<td>Black List for WAN Side</td>
<td>3 –Rows</td>
<td>Null</td>
</tr>
<tr>
<td></td>
<td></td>
<td>51 – Columns</td>
<td></td>
</tr>
</tbody>
</table>
WEB ACCESS MODE

- **Web Configuration**
  User can find the configuration under web UI -> Basic Settings page.

![Web/SSH Access](image)

- **Functionality**
  This function enables user to choose Web Access Mode between “HTTPS” and “HTTP”. If “HTTPS” is selected, web UI will be accessed using HTTPS. By default, “HTTP” is selected.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1650</td>
<td>Web Access Mode</td>
<td>0 - HTTPS</td>
<td>1 - HTTP</td>
</tr>
</tbody>
</table>

HTTPS WEB PORT

- **Web Configuration**
  User can find the configuration under web UI -> Basic Settings page.

![HTTP/HTTPS Port](image)

- **Functionality**
  This feature enables user to self-configure HTTPS Web Port. By default, the port number is 443.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P27010</td>
<td>HTTPS Web Port</td>
<td>5 - Max String Length</td>
<td>443</td>
</tr>
</tbody>
</table>

SSH PORT

- **Web Configuration**
  User can find the configuration under web UI -> Basic Settings page.

![SSH Configuration](image)

- **Functionality**
  This feature enables user to self-configure SSH Port number. By default, the port number is 22.
- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P27006</td>
<td>SSH Port</td>
<td>5 - Max String Length</td>
<td>22</td>
</tr>
</tbody>
</table>

**SNMP**

- **Web Configuration**

Users can find the configuration under web UI -> Advanced Setting page.

![Image of SNMP configuration]

- **Functionality**

This feature allows users to configure SNMP functions, including “Enable SNMP”, “SNMP Trap Community”, “SNMP Trap IP Address”, “SNMP Trap Port”, “SNMP Trap Version”, and “SNMP Trap Interval”.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P21896</td>
<td>Enable SNMP</td>
<td>0 – No</td>
<td>0 – No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Yes</td>
<td></td>
</tr>
<tr>
<td>P21897</td>
<td>SNMP Trap IP Address</td>
<td>64 - Max String Length</td>
<td>Null</td>
</tr>
<tr>
<td>P21898</td>
<td>SNMP Trap Port</td>
<td>5 - Max String Length</td>
<td>162</td>
</tr>
<tr>
<td>P21901</td>
<td>SNMP Trap Interval</td>
<td>4 - Max String Length</td>
<td>5</td>
</tr>
<tr>
<td>P21900</td>
<td>SNMP Trap Community</td>
<td>64 - Max Length</td>
<td>Null</td>
</tr>
<tr>
<td>P21899</td>
<td>SNMP Trap Version</td>
<td>1 – Version 1</td>
<td>2 – Version2c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 – Version 2c</td>
<td></td>
</tr>
</tbody>
</table>
FIRMWARE VERSION 1.0.3.2

PRODUCT NAME
HT802

DATE
1/27/2017

IMPORTANT UPGRADING NOTE
- Once HT802 is upgraded to 1.0.3.2, downgrading to 1.0.2.x firmware version or lower is not supported.

ENHANCEMENT
- Added option “DNS SRV use Registered IP” to force DNS SRV to use registered IP instead of use the first SRV.
- Changed default NTP server from us.pool.ntp.org to pool.ntp.org.

BUG FIX
- Fixed If NOTIFY arrives within 32 seconds of last NOTIFY that the device will generate a 500 Error.
- Fixed after device booted up, NTP synchronize will reach MWI SUBSCRIBE expiration and renew SUBSCRIBE immediately.
- Fixed device cannot be provision “SIP Authentication ID” via TR-069
- Fixed problem that sip response status code sometimes displayed in hex number in syslog
- Fixed device cannot get IP if SIP/RTP Layer 2 QoS priority is not set to 0.
- Fixed when device received HTTP 302 redirect to a HTTPS server, device cannot switch to the new IP address.
- Fixed device does not download the firmware and configuration file form option66 server via http and https
- Fixed that in DHCP option 66/160, IP address does not support HTTP and HTTPS prefix but only support default TFTP prefix.
- Fixed device does not carry Proxy-Require field when the proxy is a domain.
- Fixed in PPPoE IP mode, disconnect/connect the uplink network cable will cause the network LED keep blinking.
NEW FEATURES OVERVIEW

This section lists major new features and describes how to use it from the user’s point of view.

DNS SRV USE REGISTERED IP

- **Web Configuration**
  
  User can find the re-enter confirm box at Web -> Profile Settings

- **Functionality**

  If set this option to “Yes”, when registered on second SRV and making an outbound call, it will try the second SRV (registered IP) first. By default, this option is disabled and the DNS SRV will use first SRV instead of the registered IP.

- **New P Values**

<table>
<thead>
<tr>
<th>Pvalue</th>
<th>Description</th>
<th>Value range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>P28092</td>
<td>DNS SRV use Registered IP. (FXS 1)</td>
<td>0 – No, 1 – Yes</td>
<td>0 – No</td>
</tr>
<tr>
<td>P28093</td>
<td>DNS SRV use Registered IP. (FXS 2)</td>
<td>0 – No, 1 – Yes</td>
<td>0 – No</td>
</tr>
</tbody>
</table>
FIRMWARE VERSION 1.0.2.7

PRODUCT NAME
HT802

DATE
11/10/2016

IMPORTANT UPGRADING NOTE
• Once HT802 is upgraded to 1.0.2.7 or above, downgrading to 1.0.1.x firmware version or lower is not supported.

ENHANCEMENT
• None.

BUG FIX
• Fixed HT802 cannot factory reset through webpage.
• Fixed HT802 failed to send 10-page fax.
• Fixed HT802 WAN port LED will light about 10s during boot up without connecting any network cables.
FIRMWARE VERSION 1.0.2.5

PRODUCT NAME
HT802

DATE
11/07/2016

IMPORTANT UPGRAADING NOTE
• For HT802, once upgraded to 1.0.2.5 or above, downgrading to 1.0.1.x firmware version or lower is not supported.

KNOWN ISSUE
• Factory reset via web UI is not allowed on HT802 firmware 1.0.2.5.

ENHANCEMENT
• Changed OPUS Payload Type default value to 123 to match other GS products.

BUG FIX
• Fixed The value of DTMF payload can be set to empty.
• Fixed HT802 would crash after failed attended transfer as transferee.
• Fixed HT802 does not play ring back tone in Broadsoft mode if Call-Waiting Caller ID is disabled.
• Fixed No CID with callback from call on hold.
• Fixed Call audio would become very poor if change RTP mode to SRTP after call transferred.
• Fixed Device did not prompt "Device not registered" when use Spanish IVR.
• Fixed DUT cannot open configure file that download through TR-069.

NEW FEATURES OVERVIEW
This section lists major new features and describes how to use it from the user’s point of view.

OPUS PAYLOAD TYPE DEFAULT VALUE
• Web Configuration
User can find the re-enter confirm box at Web -> FXS Port Settings

![Web Configuration Screenshot]
- Functionality
  Change OPUS Payload Type default value to 123.
FIRMWARE VERSION 1.0.2.3

PRODUCT NAME
HT802

DATE
10/05/2016

IMPORTANT UPGRADING NOTE
• For HT802, once upgraded to 1.0.2.3 or above, downgrading to 1.0.1.x firmware version or lower is not supported.

ENHANCEMENT
• Added a re-enter box to confirm change user and admin password on web GUI to avoid typo or mistakes. [PASSWORD CHANGE CONFIRMATION]

BUG FIX
• Fixed the problem that Configure File Prefix (P234) is set to '/' and cannot download configure file correctly.
• Fixed HT802 cannot off-hook normally when register server is domain and sip transport is TLS
• Fixed call waiting tone only play once.
• Fixed HT802 used an incorrect User-Agent when sending configure file request to UCM.
• Fixed HT802 will play ring back tone after playing call waiting tone.
• Fixed If the value of On Hook Timing set to less than 80ms, the FXS port cannot detect on hook event.
• Fixed After changed sip port, only account 1 will take effect and all other accounts will use random port instead.
• Fixed When setting the language to "Spanish IVR", some options on web page will display Spanish.
NEW FEATURES OVERVIEW
This section lists major new features and describes how to use it from the user’s point of view.

PASSWORD CHANGE CONFIRMATION

- **Web Configuration**
  User can find the re-enter confirm box at Web -> Advanced Settings

<table>
<thead>
<tr>
<th>Status</th>
<th>Basic Settings</th>
<th>Advanced Settings</th>
<th>Profile 1</th>
<th>Profile 2</th>
<th>FXS Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>New Admin Password:</td>
<td>Confirm Admin Password:</td>
<td>(purposely not displayed for security protection)</td>
<td></td>
</tr>
</tbody>
</table>

- **Functionality**
  When change admin password, re-enter the changed password to confirm the new password is correctly entered.