

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 1.0.11.6	6
PRODUCT NAME	6
DATE	6
FIRMWARE FILE INFORMATION	6
ENHANCEMENT	6
BUG FIX	6
NEW FEATURES OVERVIEW	6
<i>MANAGEMENT INTERFACE</i>	<i>7</i>
<i>IDLE CALL SETUP ACTION</i>	<i>8</i>
<i>SSH IDLE TIMEOUT</i>	<i>9</i>
<i>TELNET IDLE TIMEOUT</i>	<i>10</i>
<i>USE ARP TO DETECT NETWORK CONNECTIVITY</i>	<i>10</i>
<i>CALL RECORD</i>	<i>10</i>
FIRMWARE VERSION 1.0.10.6	12
PRODUCT NAME	12
DATE	12
FIRMWARE FILE INFORMATION	12
ENHANCEMENT	12
BUG FIX	12
NEW FEATURES OVERVIEW	13
<i>INBAND DTMF DURATION</i>	<i>13</i>
<i>RFC2543 HOLD</i>	<i>13</i>
<i>VISUAL MWI TYPE</i>	<i>14</i>
<i>RING FREQUENCY</i>	<i>14</i>
<i>ALLOW SIP FACTORY RESET</i>	<i>14</i>
FIRMWARE VERSION 1.0.9.3	16
PRODUCT NAME	16
DATE	16
FIRMWARE FILE INFORMATION	16
ENHANCEMENT	16
BUG FIX	16
NEW FEATURES OVERVIEW	16

<i>CUSTOM CERTIFICATE.....</i>	<i>16</i>
<i>CONFERENCE PARTY HANGUP TONE</i>	<i>17</i>
<i>USE P-ACCESS-NETWORK-INFO HEADER.....</i>	<i>17</i>
<i>USE P-EMERGENCY-INFO HEADER</i>	<i>18</i>

FIRMWARE VERSION 1.0.8.719

PRODUCT NAME	19
DATE	19
IMPORTANT UPGRADING NOTE	19
ENHANCEMENT.....	19
BUG FIX	19
NEW FEATURES OVERVIEW.....	19
<i>VALIDATE SERVER CERTIFICATES</i>	<i>20</i>
<i>DDNS.....</i>	<i>20</i>
<i>BLACKLIST FOR INCOMING CALLS</i>	<i>21</i>
<i>TELNET.....</i>	<i>21</i>
<i>PLAY BUSY/REORDER TONE BEFORE LOOP CURRENT DISCONNECT</i>	<i>22</i>

FIRMWARE VERSION 1.0.5.1123

PRODUCT NAME	23
DATE	23
IMPORTANT UPGRADING NOTE	23
ENHANCEMENT.....	23
BUG FIX	24
NEW FEATURES OVERVIEW.....	25
<i>BLACKLIST FOR WAN SIDE PORT.....</i>	<i>25</i>
<i>RANDOMIZED AUTOMATIC UPGRADE</i>	<i>25</i>
<i>AUTOMATIC UPGRADE END HOUR</i>	<i>26</i>
<i>AUTOMATIC REBOOT</i>	<i>26</i>
<i>RADIUS</i>	<i>27</i>
<i>SNMPv3</i>	<i>28</i>
<i>EXPORT BACKUP CONFIGURATION</i>	<i>30</i>
<i>RESTORE FROM BACKUP CONFIGURATION.....</i>	<i>30</i>
<i>NEW VIEWER PASSWORD.....</i>	<i>30</i>
<i>WEB SESSION TIMEOUT</i>	<i>31</i>
<i>WEB ACCESS ATTEMPT LIMIT</i>	<i>31</i>
<i>WEB LOCKOUT DURATION</i>	<i>32</i>
<i>DHCP OPTION 17 ENTERPRISE NUMBER.....</i>	<i>32</i>
<i>CALLER ID FETCH ORDER.....</i>	<i>33</i>
<i>ENABLE HIGH RING POWER.....</i>	<i>33</i>
<i>ENABLE PULSE DIALING</i>	<i>34</i>

INTERNET PROTOCOL	34
IPv6 ADDRESS	35

FIRMWARE VERSION 1.0.3.736

PRODUCT NAME	36
DATE	36
IMPORTANT UPGRADING NOTE	36
ENHANCEMENT	36
BUG FIX	36
NEW FEATURES OVERVIEW	37
<i>USE ACTUAL EPHEMERAL PORT IN CONTACT WITH TCP/TLS</i>	37
<i>SIP URI SCHEME WHEN USING TLS</i>	37
<i>BACKUP OUTBOUND PROXY</i>	38
<i>PREFER PRIMARY OUTBOUND PROXY</i>	38
<i>ENABLE RTCP</i>	39
<i>HOLD TARGET BEFORE REFER</i>	39
<i>ENABLE SESSION TIMER</i>	40
<i>CONFERENCE URI</i>	40
<i>WHITE LIST FOR WAN SIDE</i>	41
<i>BLACK LIST FOR WAN SIDE</i>	41
<i>WEB ACCESS MODE</i>	42
<i>HTTPS WEB PORT</i>	42
<i>SSH PORT</i>	42
<i>SNMP</i>	43

FIRMWARE VERSION 1.0.3.244

PRODUCT NAME	44
DATE	44
IMPORTANT UPGRADING NOTE	44
ENHANCEMENT	44
BUG FIX	44
NEW FEATURES OVERVIEW	45
<i>DNS SRV USE REGISTERED IP</i>	45

FIRMWARE VERSION 1.0.2.746

PRODUCT NAME	46
DATE	46
IMPORTANT UPGRADING NOTE	46
ENHANCEMENT	46
BUG FIX	46

FIRMWARE VERSION 1.0.2.547

PRODUCT NAME	47
DATE	47
IMPORTANT UPGRADING NOTE.....	47
KNOWN ISSUE.....	47
ENHANCEMENT.....	47
BUG FIX	47
NEW FEATURES OVERVIEW.....	47
<i>OPUS PAYLOAD TYPE DEFAULT VALUE</i>	47

FIRMWARE VERSION 1.0.2.3.....49

PRODUCT NAME	49
DATE	49
IMPORTANT UPGRADING NOTE.....	49
ENHANCEMENT.....	49
BUG FIX	49
NEW FEATURES OVERVIEW.....	50
<i>PASSWORD CHANGE CONFIRMATION</i>	50

FIRMWARE VERSION 1.0.11.6

PRODUCT NAME

HT801, HT802

DATE

04/15/2019

FIRMWARE FILE INFORMATION

- HT801 firmware file name: ht801fw.bin
MD5: 36997c4788ecedab44ee69ce5e3024dc
- HT802 firmware file name: ht802fw.bin
MD5: 96d9bdc667dec220644399f8b3b7e8f9

ENHANCEMENT

- Added “CPU Load” on Web UI status page.
- Added support for SIP keep-alive to use SIP NOTIFY.
- Added feature “Network Cable Status” on Web UI status page.
- Added support for Management Interface. [MANAGEMENT INTERFACE]
- Added feature “Idle Call Setup Action”. [IDLE CALL SETUP ACTION]
- Added feature “SSH Idle Timeout”. [SSH IDLE TIMEOUT]
- Added feature “Telnet Idle Timeout”. [TELNET IDLE TIMEOUT]
- Added feature “Use ARP to detect network connectivity”. [USE ARP TO DETECT NETWORK CONNECTIVITY]
- Added feature “Call Record”. [CALL RECORD]

BUG FIX

- Fixed PPPoE password is not hidden on Web interface.
- Fixed device will enter a DHCP loop if the DHCP Option 3 contained the IP address of a device that became offline.
- Fixed the security vulnerability that DHCP Options allows user to set any device Pvalue.
- Fixed device used an expired certificate for SIP mutual TLS authentication.
- Fixed device freeze after few hours.
- Fixed device network LED flashes abnormally when unplug network cable from WAN port and plug in later.
- Fixed device will not send PRACK in Allow header when send 180 Ringing.
- Fixed when enable SIP NOTIFY Authentication, device will reboot without sending a 200OK.

NEW FEATURES OVERVIEW

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

MANAGEMENT INTERFACE

- Web Configuration**

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

Enable Management Interface: ☒ No ☐ Yes

Management Access: Management Interface Only ▼

Management Interface IPv4 Address: 802.1Q/VLAN Tag 0 (0-4094)
 802.1p priority value 0 (0-7)

☒ dynamically assigned via DHCP
☐ statically configured as:

IP Address: 192.168.100.100

Subnet Mask: 255.255.255.0

Default Router: 192.168.100.1

DNS Server 1: 0.0.0.0

DNS Server 2: 0.0.0.0

- Functionality**

- Allow administrator to setup a Virtual Network Interface on top of the physical interface for device management.

- New P Values**

Pvalue	Description	Value range	Default
P28161	Enable Management Interface	0 – No 1 – Yes	0 – No
P28162	Management Access	0 – Management Interface Only 1 – Both Service and Management Interfaces	0 – Management Interface Only
P22105	Voice VLAN Type	0 – dynamically assigned via DHCP 1 – statically configured as	0 - dynamically assigned via DHCP
P22106	IP Address	IP Format	192.168.100.100
P22107	Subnet Mask	IP Format	255.255.255.0
P22108	Default Router	IP Format	192.168.100.1
P22109	DNS Server 1	IP Format	0.0.0.0
P22110	DNS Server 2	IP Format	0.0.0.0
P22111	Management Interface IPv4 Address: 802.1Q/VLAN Tag	0 – Minimum 4094 – Maximum	0

P22112	Management Interface IPv4 Address: 802.1p priority value	0 – Minimum 7 – Maximum	0
--------	---	----------------------------	---

IDLE CALL SETUP ACTION

- Functionality**

This feature allows users to customize dial tone when user does not enter any digit. If the user picks up the handset without entering any digit, device will behave in the following manner:

- For the first 20 seconds, device will play the configured dial tone.
- If the user does not enter any digit during the first 20 seconds, device will play the configured busy tone for 60 seconds, then go to silence after the busy tone.

This feature is configurable through config file or via SSH. No option in Web UI. Need to reboot device after configuration.

- New P Values**

Pvalue	Description	Value range	Default
P28000	Idle Call Setup Action 1 (FXS 1)	0 – Continue 1 – Busy Tone 2 – Howler Tone 3 – CPC (disconnect) 4 – Reorder Tone 5 – Silence 6 – Stop Sequence	0 – Continue
P28001	Idle Call Setup Action 1 (FXS 2)	0 – Continue 1 – Busy Tone 2 – Howler Tone 3 – CPC (disconnect) 4 – Reorder Tone 5 – Silence 6 – Stop Sequence	0 – Continue
P28004	Duration of Idle Call Setup Action 1 (FXS 1)	Min – 1 second Max – 3600 seconds	60
P28005	Duration of Idle Call Setup Action 1 (FXS 2)	Min – 1 second Max – 3600 seconds	60
P28016	Idle Call Setup Action 2 (FXS 1)	0 – Continue 1 – Busy Tone 2 – Howler Tone 3 – CPC (disconnect) 4 – Reorder Tone 5 – Silence 6 – Stop Sequence	2 – Howler Tone
P28017	Idle Call Setup Action 2 (FXS 2)	0 – Continue	2 – Howler Tone

		1 – Busy Tone 2 – Howler Tone 3 – CPC (disconnect) 4 – Reorder Tone 5 – Silence 6 – Stop Sequence	
P28020	Duration of Idle Call Setup Action 2 (FXS 1)	Min – 1 second Max – 3600 seconds	30
P28021	Duration of Idle Call Setup Action 2 (FXS 2)	Min – 1 second Max – 3600 seconds	30
P28032	Idle Call Setup Action 3 (FXS 1)	0 – Continue 1 – Busy Tone 2 – Howler Tone 3 – CPC (disconnect) 4 – Reorder Tone 5 – Silence 6 – Stop Sequence	6 – Stop Sequence
P28033	Idle Call Setup Action 3 (FXS 2)	0 – Continue 1 – Busy Tone 2 – Howler Tone 3 – CPC (disconnect) 4 – Reorder Tone 5 – Silence 6 – Stop Sequence	6 – Stop Sequence
P28036	Duration of Idle Call Setup Action 3 (FXS 1)	Min – 1 second Max – 3600 seconds	1
P28037	Duration of Idle Call Setup Action 3 (FXS 2)	Min – 1 second Max – 3600 seconds	1

SSH IDLE TIMEOUT

- Web Configuration**

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

SSH Port:	<input type="text" value="22"/>	(default is 22. Cannot be the same as Telnet Port.)
SSH Idle Timeout:	<input type="text" value="0"/>	(0-86400 seconds. default 0 means never timeout.)

- Functionality**

This feature allows users to configure SSH session timeout. When there is no activity on the session, the session will close automatically.

- New P Values**

Pvalue	Description	Value range	Default
--------	-------------	-------------	---------

P28163	SSH Idle Timeout	0 seconds – Minimum 86400 seconds – Maximum	0
--------	------------------	--	---

TELNET IDLE TIMEOUT

- Web Configuration**

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

Telnet Port: (default is 23. Cannot be the same as SSH Port.)

Telnet Idle Timeout: (0-86400 seconds. default 0 means never timeout.)

- Functionality**

This feature allows users to configure Telnet session timeout. When there is no activity on the session, the session will close automatically.

- New P Values**

Pvalue	Description	Value range	Default
P28164	Telnet Idle Timeout	0 seconds – Minimum 86400 seconds – Maximum	0

USE ARP TO DETECT NETWORK CONNECTIVITY

- Web Configuration**

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

Use DNS to detect network connectivity: ☒ No ☐ Yes

Use ARP to detect network connectivity: ☐ No ☒ Yes

- Functionality**

This feature allows use to control device network detection mechanism.

- New P Values**

Pvalue	Description	Value range	Default
P8512	Use ARP to detect network connectivity	0 – No 1 – Yes	1 – Yes

CALL RECORD

- Web Configuration**

User can find the configuration in Web UI -> Status.

Call Record:

Provision: Not running. Last status : Firmware server is not configured.

Core Dump: Clean

- Functionality**

Allow user to download call history from the web GUI in CSV format. The file size limitation is 100KB. No

more record will be stored if it reaches 100KB.

FIRMWARE VERSION 1.0.10.6

PRODUCT NAME

HT801, HT802

DATE

12/11/2018

FIRMWARE FILE INFORMATION

- HT801 firmware file name: ht801fw.bin
MD5: 70dbb7f70c8d0971e0a5f5c0b7490e17
- HT802 firmware file name: ht802fw.bin
MD5: 2c25e6d9cacfc6f97b0321ae4a6e3331

ENHANCEMENT

- Added feature "Inband DTMF Duration". [INBAND DTMF DURATION]
- Added feature "RFC2543 Hold". [RFC2543 HOLD]
- Added feature "Visual MWI Type". [VISUAL MWI TYPE]
- Added feature "Ring Frequency". [RING FREQUENCY]
- Added feature "Allow SIP Factory Reset". [ALLOW SIP FACTORY RESET]
- Added support for G722 Codec.
- Added support for allow user to choose preference codec from PCMU and PCMA for FAX pass-through codec.
- Added Charter OEM ID 75.
- Increased device off-hook current to 30mA.

BUG FIX

- Fixed it took long time when device upgrade via TFTP domain name.
- Fixed NAT is not working in PPPoE mode.
- Fixed in 3-way conference call, the remote party could not hear the conference hang-up tone.
- Fixed when enable 'Remove OBP from Route Heade' function, OBP route header was shown when device registered in the Backup Outbound Proxy.
- Fixed device status page did not display core dump file when device crashed.
- Fixed Custom certificate provisioning failed using Pvalue P8472.
- Fixed device failed to register to the second IP of SRV records.
- Fixed device using LAN MAC address to connect ACS server instead of WAN MAC address.
- Fixed factory reset initiated by ACS did not reset the TR-069 config parameters.
- Fixed call failed when Enable 100rel feature set to Yes.
- Fixed device did not respond to ACS with STUN.
- Set the MAC address on syslog message to be lowercase.

- Fixed device failed in getting IP address when the gateway IP is changed.
- Fixed when set device hunting group to circular mode, device will drop the call once the last hunting group member is reached.

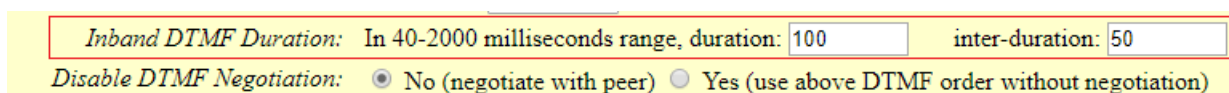
NEW FEATURES OVERVIEW

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

INBAND DTMF DURATION

- **Web Configuration**

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



Inband DTMF Duration: In 40-2000 milliseconds range, duration: inter-duration:

Disable DTMF Negotiation: ☒ No (negotiate with peer) ☐ Yes (use above DTMF order without negotiation)

- **Functionality**

This feature allows users to adjust the DTMF duration.

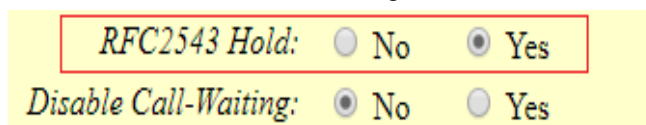
- **New P Values**

Pvalue	Description	Value range	Default
P28134	Inband DTMF Duration: duration (FXS 1)	40 milliseconds – Minimum 2000 milliseconds – Maximum	100
P28135	Inband DTMF Duration: duration (FXS 2)	40 milliseconds – Minimum 2000 milliseconds – Maximum	100
P28138	Inband DTMF Duration: inter-duration (FXS 1)	40 milliseconds – Minimum 2000 milliseconds – Maximum	50
P28139	Inband DTMF Duration: inter-duration (FXS 2)	40 milliseconds – Minimum 2000 milliseconds – Maximum	50

RFC2543 HOLD

- **Web Configuration**

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



RFC2543 Hold: ☐ No ☒ Yes

Disable Call-Waiting: ☒ No ☐ Yes

- **Functionality**

This feature allows users to toggle between RFC2543 hold and RFC3261 hold. RFC2543 hold (0.0.0.0) allows user to disable the hold music sent to the other side. RFC 3261 (a line) will play the hold music to the other side.

- **New P Values**

Pvalue	Description	Value range	Default
P26062	RFC2543 Hold (FXS 1)	0 – No	1 - Yes

		1 – Yes	
P26162	RFC2543 Hold (FXS 2)	0 – No 1 – Yes	1 - Yes

VISUAL MWI TYPE

- Web Configuration**

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

Disable Visual MWI: ☒ No ☐ Yes
Visual MWI Type: ☒ FSK ☐ NEON

- Functionality**

This feature allows use to configure Visual WMI Type.

- New P Values**

Pvalue	Description	Value range	Default
P4371	Visual MWI Type (FXS 1)	1 – FSK 2 - NEON	1 - FSK
P4372	Visual MWI Type (FXS 2)	1 – FSK 2 - NEON	1 - FSK

RING FREQUENCY

- Web Configuration**

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

Ring Frequency: 20Hz default ▾
Enable High Ring Power: ☒ No ☐ Yes

- Functionality**

This feature allows user to customize ring frequency.

- New P Values**

Pvalue	Description	Value range	Default
P4429	Ring Frequency (FXS 1)	20 – 20Hz default 25 – 25Hz	20 – 20Hz default
P4430	Ring Frequency (FXS 2)	20 – 20Hz default 25 – 25Hz	20 – 20Hz default

ALLOW SIP FACTORY RESET

- Web Configuration**

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

Caller ID Fetch Order: ☒ Auto ☐ Disabled ☐ From Header
Allow SIP Factory Reset: ☒ No ☐ Yes

- **Functionality**

This feature allows user to reset the devices directly through SIP Notify.

- **New P Values**

Pvalue	Description	Value range	Default
P26015	Allow SIP Factory Reset (FXS 1)	0 – No 1 – Yes	0 - No
P26115	Allow SIP Factory Reset (FXS 2)	0 – No 1 – Yes	0 - No

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.

SIP TLS Private Key Password:

Custom Certificate:
(Private Key + Certificate)

- **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**

Pvalue	Description	Value range	Default
P8472	Custom Certificate (Private Key + Certificate)	10 - Rows 64 - Columns	Null

CONFERENCE PARTY HANGUP TONE

- **Web Configuration**

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

Conference Party Hangup Tone:

Syntax: `f1=val[,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]]];`
 (Frequencies are in (300, 3400) Hz and cadence on and off are in (0, 64000) ms)

- **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**

Pvalue	Description	Value range	Default
P28133	Conference Party Hangup Tone	(300, 3400) HZ – Frequency (0, 6400) ms – cadence on and off	f1=425@-15,c=600/600;

USE P-ACCESS-NETWORK-INFO HEADER

- **Web Configuration**

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

Use P-Preferred-Identity Header: ☒ Default ☐ No ☐ Yes
Use P-Access-Network-Info Header: ☐ No ☒ Yes
Use P-Emergency-Info Header: ☐ No ☒ Yes

- **Functionality**

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.

- **New P Values**

Pvalue	Description	Value range	Default
P26058	Use P-Access-Network-Info Header (FXS 1)	0 - No 1 - Yes	1 - Yes
P26158	Use P-Access-Network-Info Header (FXS 2)	0 - No 1 - Yes	1 - Yes

USE P-EMERGENCY-INFO HEADER

- **Web Configuration**

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

Use P-Preferred-Identity Header: ☒ Default ☐ No ☐ Yes
Use P-Access-Network-Info Header: ☐ No ☒ Yes
Use P-Emergency-Info Header: ☐ No ☒ Yes

- **Functionality**

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

- **New P Values**

Pvalue	Description	Value range	Default
P26059	Use P-Emergency-Info Header (FXS 1)	0 - No 1 - Yes	1 - Yes
P26159	Use P-Emergency-Info Header (FXS 2)	0 - No 1 - Yes	1 - Yes

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.

Authenticate Conf File: ☒ No ☐ Yes (cfg file would be authenticated before acceptance if set to Yes)

Validate Server Certificates: ☒ No ☐ Yes (validate server certificates with our trusted list of TLS connections)

- 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**

Pvalue	Description	Value range	Default
P8463	Validate Server Certificates	0 - No 1 - Yes	0 - No

DDNS

- Web Configuration**

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

Enable DDNS: ☒ No ☐ Yes

DDNS Server:

DDNS Username:

DDNS Password:

DDNS Hostname:

DDNS Hash:

- Functionality**

Allow users to use DDNS.

- New P Values**

Pvalue	Description	Value range	Default
P28121	Enable DDNS	0 - No 1 - Yes	0 - No
P28122	DDNS Server	0 - dyndns.org 1 - freedns.afraid.org 2 - zoneedit.com 3 - no-ip.com 4 - oray.net	0 – dyndns.org
P28123	DDNS Username	64 – Max String Length	Null

P28124	DDNS Password	64 – Max String Length	Null
P28125	DDNS Hostname	64 – Max String Length	Null
P28126	DDNS Hash	64 – Max String Length	Null

BLACKLIST FOR INCOMING CALLS

- Web Configuration**

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

Blacklist For Incoming Calls:

- 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**

Pvalue	Description	Value range	Default
P28127	Blacklist For Incoming Calls	10 – Maximum allowed SIP numbers	Null

TELNET

- Web Configuration**

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

Disable SSH: ☒ No ☐ Yes

SSH Port: (default is 22. Cannot be the same as Telnet Port.)

Disable Telnet: ☐ No ☒ Yes

Telnet Port: (default is 23. Cannot be the same as SSH Port.)

- Functionality**

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

- New P Values**

Pvalue	Description	Value range	Default
P28120	Disable Telnet	0 - No 1 - Yes	1 - Yes
P28128	Telnet Port	5 – Max String Length	23

PLAY BUSY/REORDER TONE BEFORE LOOP CURRENT DISCONNECT

- Web Configuration**

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

Play busy/reorder tone before Loop Current ☒ No ☐ Yes (play busy/reorder tone before loop current disconnect upon call Disconnect: fail)

- 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**

Pvalue	Description	Value range	Default
P21925	Play busy/reorder tone before Loop Current Disconnect. (FXS 1)	0 - No 1 – Yes	0 – No
P21926	Play busy/reorder tone before Loop Current Disconnect (FXS 2)	0 - No 1 – Yes	0 – No

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 receive T.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:

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**

Pvalue	Description	Value range	Default
P28115	Black List for WAN Side Port	0 – 65535	None

RANDOMIZED AUTOMATIC UPGRADE

- **Web Configuration**

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

Randomized Automatic Upgrade: ☒ No ☐ Yes

- **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**

Pvalue	Description	Value range	Default
P8458	Randomized Automatic Upgrade	0 – No 1 - Yes	0 - No

AUTOMATIC UPGRADE END HOUR

- **Web Configuration**

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

Automatic Upgrade:

☒ No
☐ Yes, every 10080 minutes(30-5256000).
☐ Yes, daily at start hour 1 (0-23), at end hour 22 (0-23).
☐ Yes, weekly on day 1 (0-6).

- **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**

Pvalue	Description	Value range	Default
P8459	Automatic Upgrade End Hour	0 – 23	22

AUTOMATIC REBOOT

- **Web Configuration**

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

Automatic Reboot:

☒ No
☐ Yes, reboot every day at hour 1 (0-23)
☐ Yes, reboot every week at day 1 (0-6)
☐ Yes, reboot every month at day 1 (0-30)

Download Device Configuration: [Download](#)

- **Functionality**

This feature allows users to configure a specific day on a month to auto restart the device.

- **New P Values**

Pvalue	Description	Value range	Default
--------	-------------	-------------	---------

P21929	Automatic Reboot	0 – No 1 – Yes, reboot every day at hour 2 – Yes, reboot every week at day 3 – Yes, reboot every month at day	0 - No
P21930	Automatic reboot hour of day	0 - 23	1
P21931	Automatic reboot day of week	0 - 6	1
P28118	Automatic reboot at day of the month	0 - 30	1

RADIUS

- Web Configuration**

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

Enable RADIUS Web Access Control: ☒ No ☐ Yes
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:
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**

Pvalue	Description	Value range	Default
P28107	Enable RADIUS Web Access Control	0 - No 1 - Yes	0 – No
P28114	Action upon Radius Auth Server Error	0 – Reject Access 1 – Authenticate Locally	1 – Authenticate Locally
P28108	RADIUS Auth Server Address	64 - Max Character Number	None
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.

Enable SNMP: ☒ No ☐ Yes

SNMP Version:

SNMP Port: (161 or 1025-65535. Default 161)

SNMP Trap IP Address:

SNMP Trap Port: (162 or 1025-65535. Default 162)

SNMP Trap Version:

SNMP Trap Interval: (1-1440. Default 5 minutes)

SNMPv1/v2c Community:

SNMPv1/v2c Trap Community:

SNMPv3 User Name:

SNMPv3 Security Level:

SNMPv3 Authentication Protocol:

SNMPv3 Privacy Protocol:

SNMPv3 Authentication Key:

SNMPv3 Privacy Key:

SNMPv3 Trap User Name:

SNMPv3 Trap Security Level:

SNMPv3 Trap Authentication Protocol:

SNMPv3 Trap Privacy Protocol:

SNMPv3 Trap Authentication Key:

SNMPv3 Trap Privacy Key:

- Functionality**

This function allows users to configure SNMPv3 feature.

- New P Values**

Pvalue	Description	Value range	Default
P21904	SNMP Version	1 – Version 1 2 – Version 2c	3 – Version 3

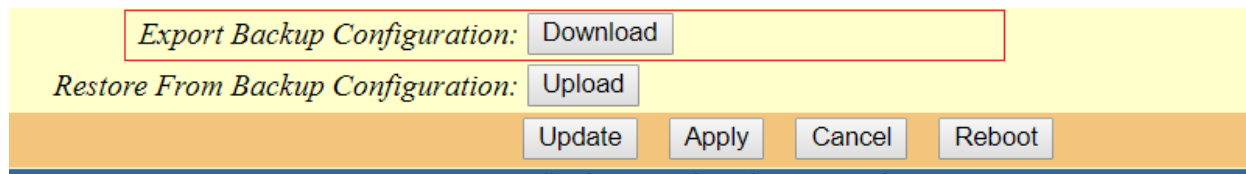
		3 – Version 3	
P21903	SNMP Port	162 or 1025-65535	162
P21902	SNMPv1/v2c Community	64 - Max Character Number	None
P21905	SNMPv3 User Name	64 - Max Character Number	None
P21910	SNMPv3 Security Level	0 – noAuthUser 1 – authUser 2 - privUser	0 - noAuthUser
P21906	SNMPv3 Authentication Protocol	0 – None 1 – MD5 2 - SHA	0 - None
P21907	SNMP Privacy Protocol	0 – None 1 – DES 2 – AES AES128	0 – None
P21908	SNMPv3 Authentication Key	5 – Rows 64 – Columns	None
P21909	SNMPv3 Privacy Key	5 – Rows 64 – Columns	None
P21911	SNMPv3 Trap User Name	64 - Max Character Number	None
P21916	SNMPv3 Trap Security Level	0 – noAuthUser 1 – authUser 2 - privUser	0 - noAuthUser
P21912	SNMPv3 Trap Authentication Protocol	0 – None 1 – MD5	0 - None

		2 - SHA	
P21913	SNMP Trap Privacy Protocol	0 – None 1 – DES 2 – AES AES-128	0 – None
P21914	SNMPv3 Trap Authentication Key	5 – Rows 64 – Columns	None
P21915	SNMPv3 Trap Privacy Key	5 – Rows 64 – Columns	None

EXPORT BACKUP CONFIGURATION

- Web Configuration**

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



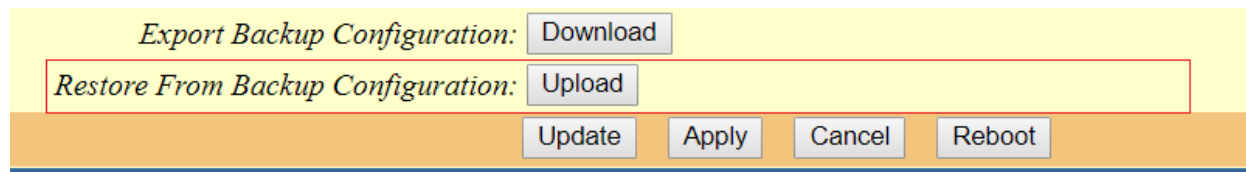
- Functionality**

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)
Confirm Viewer Password:

- **Functionality**

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

- **New P Values**

Pvalue	Description	Value range	Default
P28113	New Viewer Password	30 – Max Character Number	viewer (purposely not displayed for security protection)

WEB SESSION TIMEOUT

- **Web Configuration**

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

Web/SSH Access:

Web Session Timeout: (1-60, default 10 minutes.)
Web Access Attempt Limit: (1-10, default 5.)
Web Lockout Duration: (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**

Pvalue	Description	Value range	Default
P28116	Web Session Timeout	1 - 60 minutes	10 minutes

WEB ACCESS ATTEMPT LIMIT

- **Web Configuration**

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

Web/SSH Access:

Web Session Timeout: (1-60, default 10 minutes.)
Web Access Attempt Limit: (1-10, default 5.)
Web Lockout Duration: (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**

Pvalue	Description	Value range	Default
P28117	Web Access Attempt Limit	1 - 10	5

WEB LOCKOUT DURATION

- **Web Configuration**

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

Web/SSH Access:

Web Session Timeout: (1-60, default 10 minutes.)

Web Access Attempt Limit: (1-10, default 5.)

Web Lockout Duration: (0-60, default 15 minutes.)

- **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**

Pvalue	Description	Value range	Default
P1683	Web Lockout Duration	0 – 60 minutes	15 minutes

DHCP OPTION 17 ENTERPRISE NUMBER

- **Web Configuration**

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

DHCP Option 17 Enterprise Number:

Syslog Server:

Syslog Level:

Send SIP Log: ☐ No ☒ Yes

- **Functionality**

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

- **New P Values**

Pvalue	Description	Value range	Default
P8457	DHCP Option 17 Enterprise Number	5 – Max Character Number	3561

CALLER ID FETCH ORDER

- Web Configuration**

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

Caller ID Fetch Order: ☒ Auto ☐ Disabled ☐ From Header

SIP T1 Timeout:

SIP T2 Interval:

- 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**

Pvalue	Description	Value range	Default
P2324	Caller ID Fetch Order. (FXS 1)	0 – Auto 1 – Disabled 2 – From Header	0 – Auto
P2424	Caller ID Fetch Order. (FXS 2)	0 - Auto 1 - Disabled 2- From Header	0 – Auto

ENABLE HIGH RING POWER

- Web Configuration**

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

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

Enable High Ring Power: ☒ No ☐ Yes

- Functionality**

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

- New P Values**

Pvalue	Description	Value range	Default
P4234	Enable High Ring Power. (FXS 1)	0 - No	0 – No

		1 – Yes	
P4235	Enable High Ring Power. (FXS 2)	0 - No 1 – Yes	0 – No

ENABLE PULSE DIALING

- Web Configuration**

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

Enable Pulse Dialing: ☒ No ☐ Yes
Enable Hook Flash: ☐ No ☒ Yes

- Functionality**

Allow users to enable Pulse Dialing option under FXS Port.

- New P Values**

Pvalue	Description	Value range	Default
P20521	Enable Pulse Dialing. (FXS 1)	0 - No 1 – Yes	0 – No
P20522	Enable Pulse Dialing. (FXS 2)	0 - No 1 – Yes	0 – No

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
IPv4 Address: ☒ dynamically assigned via DHCP
 DHCP hostname: (optional)

- Functionality**

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

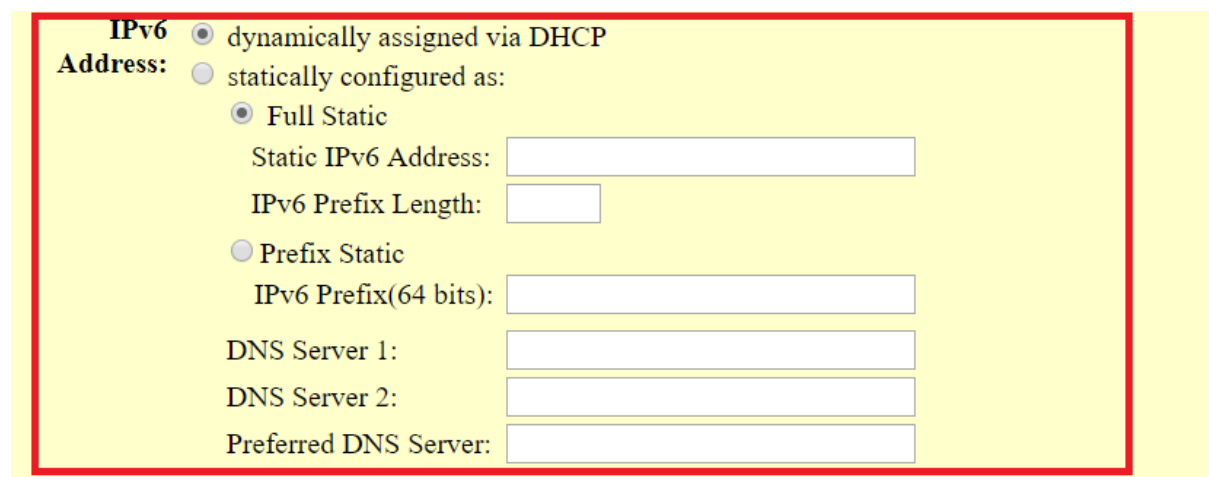
- New P Values**

Pvalue	Description	Value range	Default
P1415	Internet Protocol	0 – Both, prefer IPv4 1 – Both, prefer IPv6 2 – IPv4 Only 3 – IPv6 Only	2 – IPv4 Only

IPv6 ADDRESS

- Web Configuration**

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



- Functionality**

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

- New P Values**

Pvalue	Description	Value range	Default
P1419	IPv6 Address dynamically assigned via DHCP or statically configured	0 – dynamically assigned via DHCP 1 – statically configured as	0 – dynamically assigned via DHCP
P1426	Full Static or Prefix Static	0 – Full Static 1 – Prefix Static	0 – Full Static
P1420	Static IPv6 Address for Full Static mode	40 – Max Character Number	Null
P1421	IPv6 Prefix Length for Full Static mode	3 – Max Character Number	Null
P1422	IPv6 Prefix (64 bits) for Prefix Static mode	40 – Max Character Number	Null
P1424	DNS Server 1	40 – Max Character Number	Null
P1425	DNS Server 2	40 – Max Character Number	Null
P1423	Preferred DNS Server	40 – Max Character Number	Null

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.

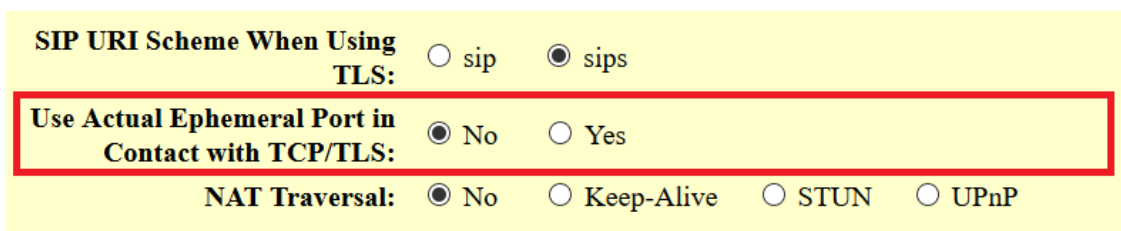
NEW FEATURES OVERVIEW

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.



SIP URI Scheme When Using TLS: ☐ sip ☒ sips

Use Actual Ephemeral Port in Contact with TCP/TLS: ☒ No ☐ Yes

NAT Traversal: ☒ No ☐ Keep-Alive ☐ STUN ☐ UPnP

- **Functionality**

This option is used to control the port information in the Via header and Contact header. If set to “No”, these port numbers will use the permanent listening port on the phone. Otherwise, they will use the ephemeral port for the connection. The default setting is “No”.

- **New P Values**

Pvalue	Description	Value range	Default
P2331	Use Actual Ephemeral Port in Contact with TCP/TLS. (FXS 1)	0 – No 1 – Yes	0 – No
P2431	Use Actual Ephemeral Port in Contact with TCP/TLS. (FXS 2)	0 – No 1 – Yes	0 – No

SIP URI SCHEME WHEN USING TLS

- **Web Configuration**

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

SIP URI Scheme When Using TLS: <input type="radio"/> sip <input checked="" type="radio"/> sips
Use Actual Ephemeral Port in Contact with TCP/TLS: <input checked="" type="radio"/> No <input type="radio"/> Yes
NAT Traversal: <input checked="" type="radio"/> No <input type="radio"/> Keep-Alive <input type="radio"/> STUN <input type="radio"/> UPnP

- **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**

Pvalue	Description	Value range	Default
P2329	SIP URI Scheme When Using TLS. (FXS 1)	0 – No 1 – Yes	1 – Yes
P2429	SIP URI Scheme When Using TLS (FXS 2)	0 – No 1 – Yes	1 – Yes

BACKUP OUTBOUND PROXY

- **Web Configuration**

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

Outbound Proxy: <input style="width: 150px;" type="text"/> (e.g., proxy.myprovider.com, or IP address, if any)
Backup Outbound Proxy: <input style="width: 150px;" type="text"/> (e.g., proxy.myprovider.com, or IP address, if any)

- **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**

Pvalue	Description	Value range	Default
P2333	Backup Outbound Proxy. (FXS 1)	96 - Max String Length	Null
P2433	Backup Outbound Proxy. (FXS 2)	96 – Max String Length	Null

PREFER PRIMARY OUTBOUND PROXY

- **Web Configuration**

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

Prefer Primary Outbound Proxy: ☒ No ☐ Yes (yes - will reregister via Primary Outbound Proxy if registration expires)

SIP Transport: ☒ UDP ☐ TCP ☐ TLS (default is UDP)

- **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**

Pvalue	Description	Value range	Default
P28096	Prefer Primary Outbound Proxy. (FXS 1)	0 – No 1 – Yes	0 – No
P28097	Prefer Primary Outbound Proxy. (FXS 2)	0 – No 1 – Yes	0 – No

ENABLE RTCP

- **Web Configuration**

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

Use Random RTP Port: ☒ No ☐ Yes

Enable RTCP: ☐ No ☒ Yes

- **Functionality**

This option allow user to enable RTCP. The default setting is “Yes”.

- **New P Values**

Pvalue	Description	Value range	Default
P2392	Enable RTCP. (FXS 1)	0 – No 1 – Yes	1 – Yes
P2492	Enable RTCP. (FXS 2)	0 – No 1 – Yes	1 – Yes

HOLD TARGET BEFORE REFER

- **Web Configuration**

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

Enable RTCP: ☐ No ☒ Yes

Hold Target Before Refer: ☐ No ☒ Yes

Refer-To Use Target Contact: ☒ No ☐ Yes

- **Functionality**

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

- **New P Values**

Pvalue	Description	Value range	Default
P26003	Hold Target Before Refer. (FXS 1)	0 – No 1 – Yes	1 – Yes
P26103	Hold Target Before Refer. (FXS 2)	0 – No 1 – Yes	1 – Yes

ENABLE SESSION TIMER

- **Web Configuration**

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

Special Feature: Standard

Enable Session Timer: ☐ No ☒ Yes

- **Functionality**

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

- **New P Values**

Pvalue	Description	Value range	Default
P2395	Enable Session Timer. (FXS 1)	0 – No 1 – Yes	1 – Yes
P2495	Enable Session Timer. (FXS 2)	0 – No 1 – Yes	1 – Yes

CONFERENCE URI

- **Web Configuration**

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

Add Auth Header On Initial REGISTER: ☒ No ☐ Yes

Conference URI:

- **Functionality**

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

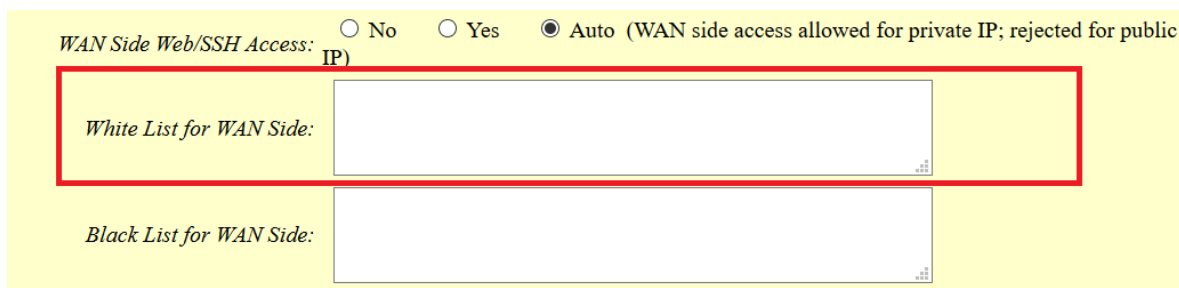
- **New P Values**

Pvalue	Description	Value range	Default
P2318	Conference URI. (FXS 1)	1024 - Max String Length	Null
P2418	Conference URI. (FXS 2)	1024 – Max String Length	Null

WHITE LIST FOR WAN SIDE

- Web Configuration**

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



WAN Side Web/SSH Access: ☐ No ☐ Yes ☒ Auto (WAN side access allowed for private IP; rejected for public IP)

White List for WAN Side:

Black List for WAN Side:

- Functionality**

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

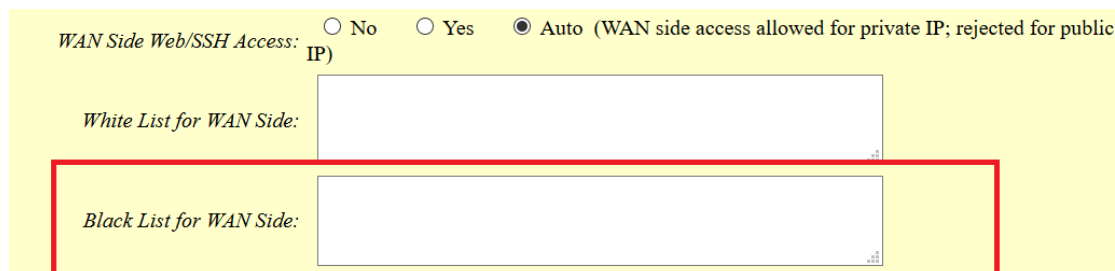
- New P Values**

Pvalue	Description	Value range	Default
P20701	White List for WAN Side	3 –Rows 51 – Columns	Null

BLACK LIST FOR WAN SIDE

- Web Configuration**

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



WAN Side Web/SSH Access: ☐ No ☐ Yes ☒ Auto (WAN side access allowed for private IP; rejected for public IP)

White List for WAN Side:

Black List for WAN Side:

- Functionality**

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

- New P Values**

Pvalue	Description	Value range	Default
P20702	Black List for WAN Side	3 –Rows 51 – Columns	Null

WEB ACCESS MODE

- Web Configuration**

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

Web/SSH Access:

Web Access Mode: ☐ HTTPS ☒ HTTP
HTTP Web Port: (default is 80)

- 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**

Pvalue	Description	Value range	Default
P1650	Web Access Mode	0 – HTTPS 1 – HTTP	1 – HTTP

HTTPS WEB PORT

- Web Configuration**

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

HTTP Web Port: (default is 80)
HTTPS Web Port: (default is 443)

- Functionality**

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

- New P Values**

Pvalue	Description	Value range	Default
P27010	HTTPS Web Port	5 - Max String Length	443

SSH PORT

- Web Configuration**

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

Disable SSH: ☒ No ☐ Yes
SSH Port:

- Functionality**

This feature enables user to self-configure SSH Port number. By default, the port number is 22.

- **New P Values**

Pvalue	Description	Value range	Default
P27006	SSH Port	5 - Max String Length	22

SNMP

- **Web Configuration**

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

Enable SNMP: ☒ No ☐ Yes

SNMP Trap Community:

SNMP Trap IP Address:

SNMP Trap Port: (162 or 1025-65535. Default 162)

SNMP Trap Version: ▾

SNMP Trap Interval: (1-1440. Default 5 minutes)

- **Functionality**

This feature allows user to configure SNMP function, included “Enable SNMP”, “SNMP Trap Community”, “SNMP Trap IP Address”, “SNMP Trap Port”, “SNMP Trap Version”, and “SNMP Trap Interval”.

- **New P Values**

Pvalue	Description	Value range	Default
P21896	Enable SNMP	0 – No 1 – Yes	0 – No
P21897	SNMP Trap IP Address	64 – Max String Length	Null
P21898	SNMP Trap Port	5 – Max String Length	162
P21901	SNMP Trap Interval	4 – Max String Length	5
P21900	SNMP Trap Community	64 – Max Length	Null
P21899	SNMP Trap Version	1 – Version 1 2 – Version 2c	2 – Version2c

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 from 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.

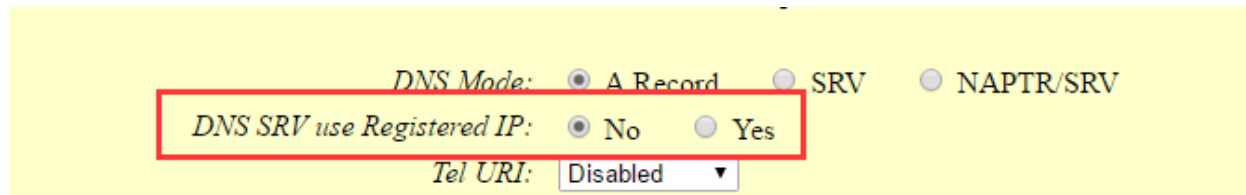
NEW FEATURES OVERVIEW

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



DNS Mode: ☒ A Record ☐ SRV ☐ NAPTR/SRV

DNS SRV use Registered IP: ☒ No ☐ Yes

Tel URI: Disabled ▼

- 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**

Pvalue	Description	Value range	Default
P28092	DNS SRV use Registered IP. (FXS 1)	0 – No 1 – Yes	0 – No
P28093	DNS SRV use Registered IP. (FXS 2)	0 – No 1 – Yes	0 – No

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 UPGRADING 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.

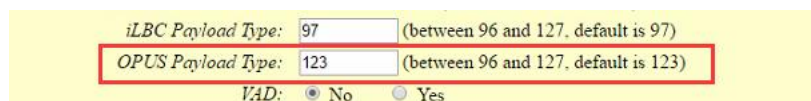
NEW FEATURES OVERVIEW

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



The screenshot shows a configuration form with the following fields:

- iLBC Payload Type:* 97 (between 96 and 127, default is 97)
- OPUS Payload Type:* 123 (between 96 and 127, default is 123) - This field is highlighted with a red box.
- VAD:* ☒ No ☐ Yes

- **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.

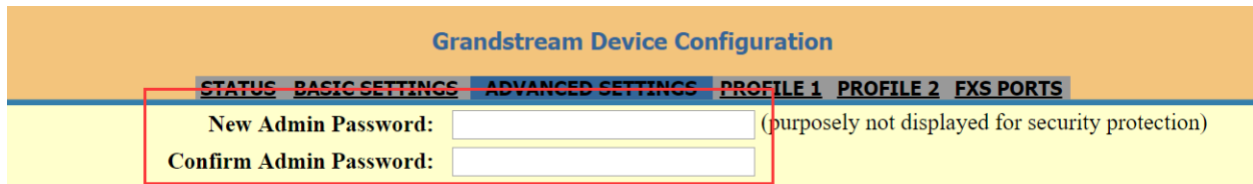
NEW FEATURES OVERVIEW

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



The screenshot shows the 'Grandstream Device Configuration' web interface. At the top, there is a navigation bar with tabs: STATUS, BASIC SETTINGS, ADVANCED SETTINGS, PROFILE 1, PROFILE 2, and FXS PORTS. The 'ADVANCED SETTINGS' tab is currently selected. Below the navigation bar, there are two input fields: 'New Admin Password:' and 'Confirm Admin Password:'. A red rectangular box highlights these two fields. To the right of the 'New Admin Password:' field, there is a note in parentheses: '(purposely not displayed for security protection)'.

- **Functionality**

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