HT813 Firmware Release Notes

Table of Content

FIRMWARE VERSION 1.0.1.2 25

FIRMWARE VERSION 1.0.17.2

PRODUCT NAME

HT813

DATE

05/09/2023

FIRMWARE FILE INFORMATION

- HT813 firmware file name: ht813fw.bin
  MD5: 9b6cd1aa0494db9276ad0dd2c74f0a96

ENHANCEMENT

- Added support "SIP URI Scheme When Using TLS" option on the FXO page.
- Added the "Incoming Call Duration Limit" in PSTN. [Incoming Call Duration Limit]
- Added ability to have a second VLAN under switch mode. [LAN Port VLAN Feature Under Bridge Mode]
- Added support for "https://" in Config Server Path field.
- Added "Device.DeviceInfo.SupportedDataModel" in TR data model.
- Added some missing parameters to the TR069 data model.
- Improved Web UI login response time.

BUG FIX

- Fixed a bug that caused the device to not make outgoing calls with the specific firmware.
- Fixed the device using a random sip port requires a reboot to take effect.
- Fixed unit sends BYE with wrong CSeq.
- Fixed inaccurate encoding and decoding of DTMF durations.
- Fixed invalid HTTP headers provided by Web GUI.
- Fixed vulnerabilities detected by Nexpose rapid 7 scab tools.
- Fixed device registration with a random port after a reboot.
- Fixed device cannot log in to the web if the password length exceeds 18 characters.
- Fixed NAPTR/SRV mode does not send NAPTR DNS register requests.
- Fixed device Preferred Vocoder can't choose ILBC in choice 8.
- Fixed Inbound long duration call fails under certain configurations.
- Fixed an issue that caused the device not to work with Alarm System.
- Fixed the off-hook delay problem that occurs when the FAX runs for a long timer running.
- Fixed the off-hook not detected during ringing.
- Fixed the Prompt Tone Access Code type error.
- Fixed the FW upgrade by TR069 doesn't use Target File Name.
- Fixed the TR-069 Device report 9002 error when requesting Call Waiting Enable.

- Fixed a bug that caused encountered dialing confusion after running for hours.
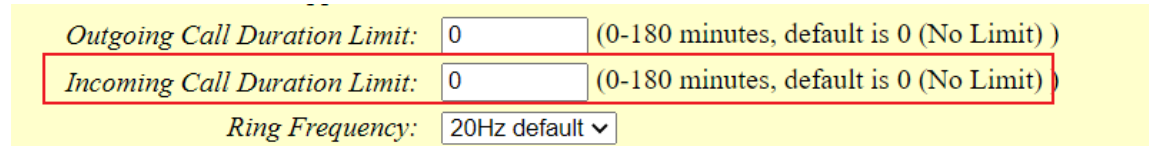- Fixed the issue that the IPV6 address has no abbreviation.

NEW FEATURES OVERVIEW

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

Incoming Call Duration Limit

- **Web Configuration**

Users can find the configuration section in Web -> FXS or FXO.

Outgoing Call Duration Limit:	0	(0-180 minutes, default is 0 (No Limit))
Incoming Call Duration Limit:	0	(0-180 minutes, default is 0 (No Limit))
Ring Frequency:	20Hz default	

- **Functionality**
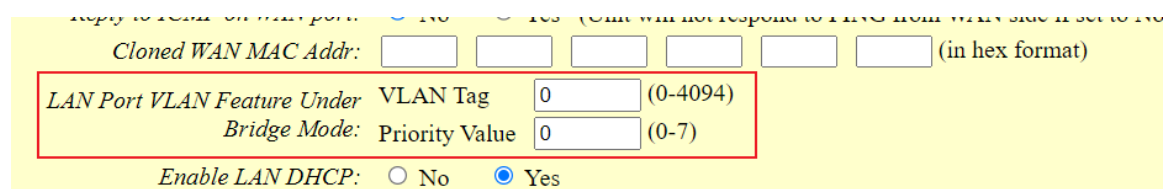
This feature allows users to configure the call duration limit for the incoming calls, default is 0 (No limit).

Pvalue	Description	Value range	Default
28760	Incoming Call Duration Limit (FXS)	Number: 0 – 180 (0 is No Limit)	0
28761	Incoming Call Duration Limit (FXO)	Number: 0 – 180 (0 is No Limit)	0

LAN Port VLAN Feature Under Bridge Mode

- **Web Configuration**

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

Cloned WAN MAC Addr:							(in hex format)
LAN Port VLAN Feature Under Bridge Mode:	VLAN Tag	0	(0-4094)
	Priority Value	0	(0-7)
Enable LAN DHCP:	○ No ● Yes		

- **Functionality**

This feature allows users to configure   a different VLAN tag and priority value for the second network port when HT is configured in bridge mode.

Pvalue	Description	Value range	Default
229	LAN Port VLAN Feature Under Bridge Mode: VLAN Tag	Number: 0 – 4094	0
230	LAN Port VLAN Feature Under Bridge Mode: Priority Value	Number: 0 – 7	0

FIRMWARE VERSION 1.0.15.7

PRODUCT NAME

HT813

DATE

01/03/2023

FIRMWARE FILE INFORMATION

- HT813 firmware file name: ht813fw.bin
  MD5: 18101a5a0330f670eba09ac0e1460f22

ENHANCEMENT

- Added support for Always send HTTP Basic Authentication Information. [Always send HTTP Basic Authentication Information]
- Added Sectigo CA to our Trusted List
- Added support for Ring frequency 25Hz on FXS port
- Updated the "Let's encrypt" root CA certificate
- Added the ability to set up system cadence with multiple cadences through TR-069.
- Added support to fill the Device.ProvisionCode using DHCP option 43 sub-option 2.
- Added support to "Distinctive Ring Tone", "incoming caller ID", and "Ring Tone" on the HTs TR-069 template.
- Added support for more SRTP methods.
- Updated Syslog and make it more user-friendly.
- Redesigned the display of the software version on the status page and make it looks better.
- Updated the copyright translated into Russian on the Russian language page.
- Added support for variable on Provisioning link. [Enable using tags in the URL]
- Added feature Configuration File Types Allowed. [Configuration File Types Allowed].
- Added Charter CA to the approved certificate list.
- Added support of DHCP Option 150. [Additional Override DHCP Option]
- Add SSL Key Log File. [With Secret Key Information]
- Added support for Inband DTMF Duration. [Inband DTMF Duration]
- Added support for DSP DTMF Detector Duration Threshold. [DSP DTMF Detector Duration Threshold]
- Added support for Download and Process ALL Available Config Files. [Download and Process ALL Available Config Files]
- Added support for new override config file option in "cfgMAC_override.xml".
- Added support for When to Restart Session After Re-INVITE received. [When to Restart Session After Re-INVITE received]

- Added support following up not on WebUI P-values:

    P8603 - Root CA Version (0 - Current Root; 1 - New Root, default is 1)

    P8604 - Provision and upgrade to new Gen-2 certificate. (1- upgrade; 0 - no upgrade, default is 0).

    P8605 - Contents (text string) of Gen-2 certificate to upgrade. (String. Maxlength 8192, no default)

    P8606 - Contents (text string) of Gen-2 EC private key to upgrade. (String. Maxlength 8192, no default)

BUG FIX

- Fixed a bug that caused an ATA crash after provision.
- Fixed an issue that caused the Fax pass-through mode to fail with firmware 1.0.33.4.
- Fixed P-value P2486/P2386 duplication.
- Fixed the packet loss rate in the call quality of the HT device incorrectly displayed.
- Fixed the device does not start RTP session when receiving 183 message.
- Fixed issue caused SIP Phone cannot be registered after the certificate verification is enabled.
- Fixed the device does not apply "No key Entry Timeout" with less than 4 seconds through TR-069.
- Fixed device does not apply Frequency power setting through TR-069.
- Fixed device does not apply Candence setting through TR-069.
- Fixed the GPV error when getting to 2048 characters.
- Fixed device debugging functionality that bypass restrictions and achieves root access.
- Fixed device reported 9002 error when requesting specific parameters through TR-069.
- Fixed device Some options cannot be found on the Parameter tree via TR-069.
- Fixed SLIC setting on TR-069 not matching selection on device web UI.
- Fixed an RTP-Event (DTMF) issue.
- Fixed an issue made Sin 227 - BT coded CID displayed as anonymous.
- Fixed device the line bottom noise is too large and there is no FSK signal.
- Fixed device crashed when PSTN does an incoming call with FXO, and the FXS port establishes an OB call or 3WC.
- Fixed device using the TR-069 protocol push Secondary Outbound Proxy configuration parameter is not correct.
- Fixed device does not accept changing admin password through TR-069.
- Fixed the device does not accept setting frequency to 0 through TR-069.
- Fixed an issue causing the call to get ended by the server after 30 mins on hold.
- Fixed an issue that caused call transfer failures.
- Fixed an issue that caused faxes may not to be sent and received normally with some specific brands of fax machines.
- Fixed the device still uses a random port for SIP registration when it's set to No.
- Fixed device Second Register has no auth header by default.
- Foxed device "P-Access-Network-Info" Header not in Register.
- Fixed an issue that caused the device not to terminate PSTN call properly.
- Fixed an issue that caused the device to have no audio on both sides and the IVR to become invalid after the fax is sent.

- Fixed a bug that caused the device not to start sending RTP.
- Fixed device the sip server address and port settings that do not conform to the rules can be saved.
- Fixed Jitter Buffer Type not getting used.
- Fixed device reports the call status as P2P after the local three-party conference ends.
- Fixed device SIPs TLS registration failed after filling in the Custom Certificate with the GEN 1 certificate.
- Fixed device the memory is out of memory when the specific version firmware is changed.
- Fixed device the call is abnormal after the participant transfers the call.
- Fixed device after the FTP upgrade fails, the status light is abnormal.
- Fixed a bug that caused audio loss when call waiting caller ID is enabled.
- Fixed the log server domain name resolution order is incorrect.
- Fixed the device will not send require when path contains % character.
- Fixed a bug that caused the ATA to crash after calling itself.
- Fixed the wrong ACS port causes high CPU usage on the device.
- Fixed the "Distinctive Ring Tone for Caller ID" Error 9002 when filling in a numeric number.
- Fixed an issue that made the device unable to enter ATE mode.
- Fixed device when the AC Termination Model is set to Auto Detected, the FXO interface will automatically off hook.
- Fixed a bug that caused no audio for the second call received.
- Fixed device the Syslog is enabled on the HT device in the local deployment, and the content of the Syslog package is empty.
- Fixed device the Authenticate server certificate domain/chain option needs to be restarted to take effect.
- Fixed the device stops sending periodic information after a time.
- Fixed device in secondary dialing, auxiliary sending of different DTMF at the same time will lead to device program confusion.
- Fixed an issue that made click FXS port redirects to the wrong page on WebUI.
- Fixed device the DTMF Negotiation fails upon transfer.
- Fixed Call quality data not reported after the device factory reset.
- Fixed a bug that made DDNS Username and DDNS Password could not save as null.
- Fixed CPE doesn't recover XMPP session when XMMP server goes down.
- Fixed a bug that made Notifications not be sent to the ACS.
- Fixed device CPE crash after executing deleteObject.
- Fixed device deleting node via ACS server will cause CPE crash.
- Fixed device could not config "OpenVPN Transport" via TR-069.
- Fixed device did not use ACS URL passed in DHCP option.
- Fixed the device did not send HTTP to ACS if only IPV6 in WIFI.
- Fixed device OUI reported by CPE mismatch with real OUI in MAC address.
- Fixed an issue that caused HT device cannot connect to local deployment environment.
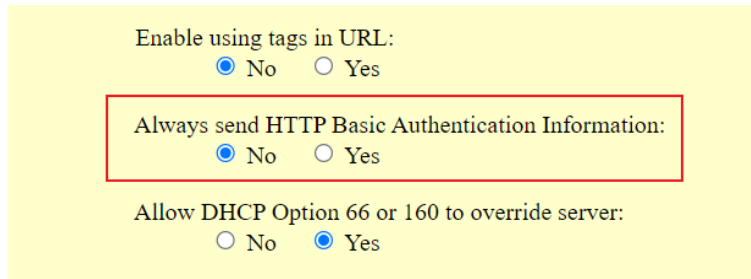
NEW FEATURES OVERVIEW

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

Always send HTTP Basic Authentication Information

- **Web Configuration**

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

- **Functionality**
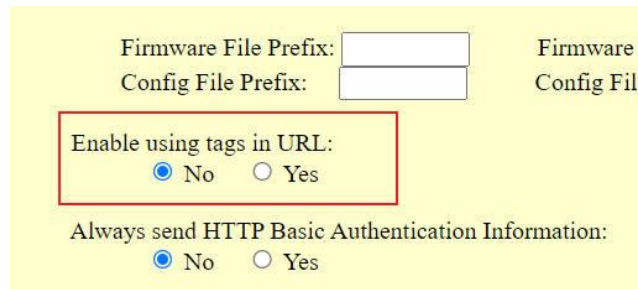
This feature allows users to configure user name and password within HTTP request before server sends authentication challenge.

Pvalue	Description	Value range	Default
20713	Always send HTTP Basic Authentication Information	0 – No 1 - Yes	0 – No

Enable using tags in the URL

- **Web Configuration**

Users can find the configuration section in Web -> Advanced Settings.

- **Functionality**

This feature allows users to configure variables on the configuration server path to differentiate the directories on the server.

Pvalue	Description	Value range	Default
8609	Enable using tags in the URL	0 - No 1 - Yes	0 - No

Configuration File Types Allowed

- **Web Configuration**

User can find the configuration section in Web -> Advanced Settings.
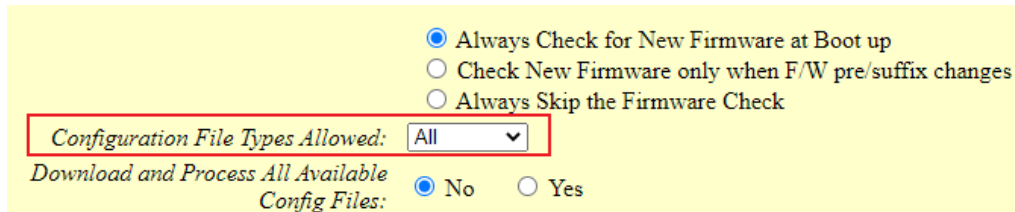
- **Functionality**

This feature allows users to configure provision configuration file type in xml file only or all file types.

Pvalue	Description	Value range	Default
8601	Configuration File Types Allowed	47 - All 46 - XML only	47 - All

Additional Override DHCP Option

- **Web Configuration**

Users can find the configuration section in Web -> Advanced Settings.
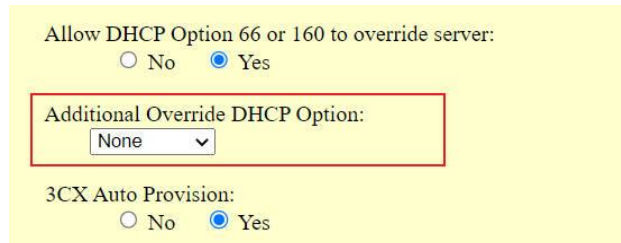
- **Functionality**

This feature allows users to enable the Additional Override DHCP Option in Option 150.

Pvalue	Description	Value range	Default
8337	Additional Override DHCP Option	0 – None 1 – Option 150	0 – None

With Secret Key Information

- **Web Configuration**

Users can find the configuration section in Web -> Advanced Settings-> Information Capture-> Capture.

- **Functionality**

This feature allows users to make packet capture including the secret key to decrypt the captured TLS packets.

Pvalue	Description	Value range	Default
22419	With Secret Key Information	0 - No 1 - Yes	0 - No

Inband DTMF Duration

- **Web Configuration**

Users can find the configuration section in Web -> FXS Port or FXO Port.

- **Functionality**

This feature allows users to config the Inband DTMF Duration.

Pvalue	Description	Value range	Default
28134 28135	Inband DTMF Duration - duration	Min: 40 Max: 2000	100
28138 28139	Inband DTMF Duration - inter-duration	Min: 40 Max: 2000	50

DSP DTMF Detector Duration Threshold

- **Web Configuration**

Users can find the configuration section in Web -> FXS Port or FXO Port.

- **Functionality**

This feature allows users to config the DSP DTMF Detector Duration Threshold.

Pvalue	Description	Value range	Default
28201 28202	DSP DTMF Detector Duration Threshold - duration	Min: 20 Max: 200	30
28205 28206	DSP DTMF Detector Duration Threshold - inter-duration	Min: 20 Max: 200	30

Download and Process ALL Available Config Files

- **Web Configuration**

Users can find the configuration section in Web -> Advanced Settings.

- **Functionality**

This feature allows users to inverse downloading all config files. The default cfg provision behavior of HT813 is request cfgMAC.xml at first, then request the first available config in order of "DHCP option 67 bootfile", cfgMAC.xml, cfgProductModel.xml, cfg.xml.

Pvalue	Description	Value range	Default
8467	Download and Process ALL Available Config Files	0 - No 1 - Yes	0 - No

When to Restart Session After Re-INVITE received

- **Web Configuration**

Users can find the configuration section in Web -> FXS Port or FXO Port.

	Force INVITE:	◉ No	○ Yes (Always refresh with INVITE instead of UPDATE)
When To Restart Session After Re-INVITE received:		◉ Immediately	○ After replying 200OK
	Enable 100rel:	◉ No	○ Yes

- **Functionality**

This feature allows users to support to delay posting Media Change Event with this new feature.

Pvalue	Description	Value range	Default
28744 28745 28746 28747	When To Restart Session After Re-INVITE received	0 - Immediately 1 - After replying 200OK	0 - Immediately

FIRMWARE VERSION 1.0.13.3

PRODUCT NAME

HT813

DATE

04/22/2021

FIRMWARE FILE INFORMATION

- HT813 firmware file name: ht813fw.bin
  MD5: 1028e7482f820138c0b28b03f142b763

ENHANCEMENT

- Added support for handling of NOTIFY with Event=check-sync;reboot=false.
- Increased dial plan maximum supported character length.
- Increased P2386/P2486, P280, P8220 supported maximum character length to 8192.

BUG FIX

- Fixed the caller ID is not updated on analog phones after. completing an attended transfer.
- Fixed if the server replies 200 OK with the SDP containing port 0, device will freeze.
- Removed.TR069 parameter "Device.X_GRANDSTREAM_Diagnostics.Capture.DiagnosticsState" as HT813 does not support packets capture.
- Fixed FXO port does not detect caller ID from BSNL analog lines.

FIRMWARE VERSION 1.0.11.2

PRODUCT NAME

HT813

DATE

03/03/2021

FIRMWARE FILE INFORMATION

- HT813 firmware file name: ht813fw.bin
  MD5: 9bbc1f1622661ca001eba6bb2940393f

BUG FIX

- Fixed extreme low audio transmitted randomly.
- Fixed when RTP attack happens, calls have no audio.
- Fixed devices freeze randomly and is HTTP/SSH inaccessible with no dial tone in the attached analog phone.
- Fixed the caller ID is not displayed when receiving incoming calls.
- Fixed if device missed the chance to resolve STUN server host name during booting, STUN fails and will cause calls failure.
- Fixed device could not upgrade via TFTP.
- Fixed device fails to connect to GDMS local deployed environment after restarting.
- Fixed device will obviate the T flag on dial plan.
- Fixed losing connectivity on LAN connected devices on ATA's using PPPoE.
- Fixed when upgrade via HTTPS, if server returns more data than requested in partial content, the provision will fail.
- Added support for more than 2 layers certificate chain loading.
- Fixed with option 43, device could not upgrade via FTPS.
- Fixed when Internet Protocol set to Both, prefer IPv6, device does not send registration after changing the sip transport from TCP to UDP.
- Removed gssu commend from SSH and Telnet.
- Fixed outbound VoIP to FXO slow call setup and loss of audio at start of the call.

FIRMWARE VERSION 1.0.9.1

PRODUCT NAME
HT813

DATE
09/01/2020

FIRMWARE FILE INFORMATION
- HT813 firmware file name: ht813fw.bin
  MD5: 99aacc1f80bc23142d19e62ac370bfc9

ENHANCEMENT
- Added feature "DHCP domain name". [DHCP DOMAIN NAMELOAD CA CERTIFICATES]

BUG FIX
- Fixed device will crash when NAT Traversal is set to STUN.
- Fixed that device does not support IPv6 address without square brackets.
- Fixed after a reboot, there may no audio when making a call, and there is no IVR
- Fixed device will not try to reach GAPS when WAN subnet coincides with default LAN subnet.
- Fixed device will crash when FXO port is doing an PSTN to VoIP incoming call, and FXS port establishes an outbound call or performing a 3-Way conference call.

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

DHCP DOMAIN NAME

- **Web Configuration**

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

DHCP domain name:		(optional)

- **Functionality**

This feature allows user to configure DHCP domain name. This option specifies the domain name that client should use when resolving hostnames via the Domain Name System.

- **New P Values**

Pvalue	Description	Default
P147	DHCP domain name	NULL

FIRMWARE VERSION 1.0.7.1

PRODUCT NAME

HT813

DATE

08/03/2020

FIRMWARE FILE INFORMATION

- HT813 firmware file name: ht813fw.bin
  MD5: 096aeb84f2e964e816d7e00e3bb2cf41

ENHANCEMENT

- Added feature "Load CA Certificates". [LOAD CA CERTIFICATES]
- Increased "SIP TLS Certificate" and "SIP TLS Private Key" supported maximum length from 2048 to 4096.
- Added New Zealand Standard for Pulse Dialing Standard.

BUG FIX

- Fixed a security vulnerability that device will crash if an attacker sends a TCP message that does not contain a '\r'.
- Fixed a security vulnerability that device will crash due to a null pointer dereference when an authentication header is present in the HTTP Get request, but the header is not a well-formed digest message.
- Fixed a security vulnerability that the TR-069 interface hardcodes the nonce and opaque values that the HTTP digest authentication values could be reused.
- Fixed the security vulnerability related to provisioning XML password bypass and command injection.
- Removed gssu commend from SSH.
- Fixed when Internet Protocol is set to IPv6 Only, HT813 will not switch to IPv4 to get registered if IPv6 is not available.
- Fixed HT813 will send SIP requests to default port 5060 when a different port was configured.
- Fixed when set up an admin password longer than 15 characters, the web access will keep showing "Sorry. Your Login Password is not recognized. Please try again."
- Fixed device does not take port from SRV results when SIP transport type is TLS.
- Fixed incoming calls will reach the destination number after a number of rings different than configured on the HT813
- Fixed incoming call does not work with TLSv1.2
- Fixed distinctive ring tone does not take effect when it is set to more than 9000ms.
- Fixed device could not make a call when use *19 to disable SRTP per call.

NEW FEATURES OVERVIEW

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

LOAD CA CERTIFICATES

- **Web Configuration**

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

| Load CA Certificates: | Built-in trusted certificates ▾ |

- **Functionality**

This feature allows user to specify which CA certificate to trust when performing server authentication.

- **New P Values**

Pvalue	Description	Value range	Default
P8502	Load CA Certificates	0 – Built-in trusted certificates 1 – Custom trusted certificates 2 – All trusted certificates	0 – Built-in trusted certificates

FIRMWARE VERSION 1.0.5.2

PRODUCT NAME
HT813

DATE
04/15/2020

FIRMWARE FILE INFORMATION

- HT813 firmware file name: ht813fw.bin
  MD5: b2882d93cf659701b132bfa2c1dd9d21

ENHANCEMENT

- Updated Brazil / Sao Paulo time zone to UTC-3 without Daylight Time Saving.
- Added support for unlimited ring without timeout. When configure "Ring Timeout" to 0, will have no ring timeout
- Added feature "Connection Request Port". [CONNECTION REQUEST PORT]
- Added feature "SIP User-Agent". [SIP USER-AGENT]

BUG FIX

- Fixed when device FXO port "Enable Polarity Reversal" set to Yes, FXO port does not have dial tone when doing PSTN to VoIP calls.
- Fixed the SSH connection will disconnected when enable or disable Telnet.
- Fixed FXO "NAT Traversal" could not be set via TR-069.
- Fixed device TR-069 NAT Traversal AvailableAddressingType does not have UPnP.
- Fixed device TR-069 Device.LAN.AddressingType lack of PPPoE.
- Fixed could DeleteObject or AddObject on ACS server.
- Increase the maximum ptime from 30 to 60 when using codec G729
- Fixed device SNMP host name is HT8XX instead of HT813.
- Fixed DHCP IP Lease Time could be set to negative.
- Fixed device will crash if factory reset via TR-069.
- Fixed PSTN pass through could not detect DTMFs after dial PSTN Access Code.
- Fixed device may OOM when doing upgrade.
- Fixed device LAN DHCP Base IP is not changing automatically when the WAN port receives 192.168.2.1 IP address from the network.
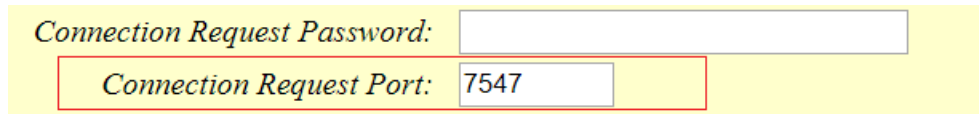
NEW FEATURES OVERVIEW
This section lists major new features and describes how to use it from the user's point of view.

CONNECTION REQUEST PORT

- **Web Configuration**

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

Connection Request Password:
Connection Request Port: 7547

- **Functionality**

This feature allows user to configure the TR-069 connection request port.

- **New P Values**

Pvalue	Description	Value range	Default
P4518	Connection Request Port	0 – 65535	7547

SIP USER-AGENT

- **Web Configuration**

User can find the configuration in Web UI -> FXS/FXO Port.

SIP User-Agent:
SIP User-Agent Postfix:

- **Functionality**

This feature allows users to configure SIP User-Agent. If not configured, device will use the default User-Agent header.

- **New P Values**

Pvalue	Description	Value range	Default
P29071	SIP User-Agent (FXS)	1024 – Max String Length	Null
P29171	SIP User-Agent (FXO)	1024 – Max String Length	Null

FIRMWARE VERSION 1.0.3.12

PRODUCT NAME

HT813

DATE

11/08/2019

FIRMWARE FILE INFORMATION

- HT813 firmware file name: ht813fw.bin
  MD5: 01a43fbb111953cb53969d0ee02ae7df

ENHANCEMENT

- Added support for T.38 Fax mode under FXO Port.
- Set the MAC address on syslog to lower case.
- Updated mini_httpd version to 1.30.
- Added ability to support provisioning server path containing the server authentication credentials for the DHCP option 66. Format should be "username:password@Provisioning_Server_IP".
- Added support for DHCP Option 67.
- Updated Dropbear version to 2019.78.
- Updated Pvalue for Automatic Upgrade from P194 to P22296.
- Updated "São Paulo" time zone to UTC-3.
- Added support for GDMS platform.
- Added feature "Allow SIP Factory Reset". [ALLOW SIP FACTORY RESET]
- Added feature "Pulse Dialing Standard". [PULSE DIALING STANDARD]
- Added support for RFC2833 Count. [RFC2833 COUNT]
- Added feature "Disable Weak TLS Cipher Suites". [DISABLE WEAK TLS CIPHER SUITES]
- Added feature "TLS Version". [TLS VERSION]
- Added feature "Allow SIP Factory Reset". [SYSLOG PROTOCOL]

BUG FIX

- Fixed incoming PSTN call only ring once on FXS port.
- Fixed HT813 will include the outbound proxy as Route in the ACK message which leads to calls disconnection.
- Fixed when there is no rport in OPTIONS, device will send 200 OK to the originating source port instead of the port in the Via header.
- Fixed device did not send PRACK option when "Enable 100rel" set to Yes.
- Fixed device will consistently resolve DNS before every STUN refresh interval.
- Fixed when enable SIP NOTIFY Authentication, device will reboot without sending a 200OK.
- Fixed when downloaded a config file, device could not escape "<, >, ", ', &" symbols properly.

- Fixed device sent SIP requests to outbound proxy 5060 when configured as a different port.
- Fixed Custom certificate provisioning failed using Pvalue P8472.
- Fixed device will keep sending BOOTSTRAP messages to ACS server.
- Fixed TR-069 manufacture field is empty on the INFORM header.
- Fixed dial plan prefix displayed null when set to ".
- Fixed device will crash when Caller ID Scheme set to NTT Japan.
- Fixed encryption xml file could not write to device successfully.
- Fixed when DNS SRV is used, device will send sip Register to wrong SIP destination port.

NEW FEATURES OVERVIEW

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

ALLOW SIP FACTORY RESET

- **Web Configuration**

User can find the configuration in Web UI -> FXS/FXO Port.

- **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)	0 – No 1 – Yes	0 - No
P26115	Allow SIP Factory Reset (FXO)	0 – No 1 – Yes	0 - No

PULSE DIALING STANDARD

- **Web Configuration**

User can find the configuration in Web UI -> FXS Port.

- **Functionality**

This feature allows users to use Swedish pulse dialing standard.

- **New P Values**

Pvalue	Description	Value range	Default
P28165	Pulse Dialing Standard (FXS Port)	0 – General Standard 1 – Swedish Standard	0 – General Standard

RFC2833 COUNT

- **Web Configuration**

User can find the configuration in Web UI -> FXS Port.

| RFC2833 Events Count: | 8 | (between 2 and 10, default is 8) |
| RFC2833 End Events Count: | 3 | (between 2 and 10, default is 3) |

- **Functionality**

This feature allows users to customize the count of RFC2833 events and end events.

- **New P Values**

Pvalue	Description	Value range	Default
P28173	RFC2833 Events Count (FXS Port)	2 – minimum 10 – Maximum	8
P28177	RFC2833 End Events Count (FXS Port)	2 – minimum 10 – Maximum	3

DISABLE WEAK TLS CIPHER SUITES

- **Web Configuration**

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

| Disable Weak TLS Cipher Suites: | Enable Weak TLS Ciphers Suites ▼ |

- **Functionality**

This feature allows users to disable weak ciphers.

- **New P Values**

Pvalue	Description	Value range	Default
P8536	Disable Weak TLS Cipher Suites	0 – Enable Weak TLS Ciphers Suites 1 – Disable Symmetric Encryption RC4/DES/3DES 2 - Disable Symmetric Encryption SEED 3 - Disable All Of The Above Weak Symmetric Encryption 4 - Disable Symmetric Authentication MD5 5 - Disable All Of The Above Weak Symmetric Authentication 6 - Disable Protocol Version SSLv2/SSLv3	0 – Enable Weak TLS Ciphers Suites

		7 - Disable All Of The Above Weak Protocol Version 8 - Disable All Of The Above Weak TLS Ciphers Suites	

TLS VERSION

- **Web Configuration**

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

Minimum TLS Version:	Unlimited ▾
Maximum TLS Version:	Unlimited ▾

- **Functionality**

These features allow customer to chose desired TLS Version.

- **New P Values**

Pvalue	Description	Value range	Default
P22293	Minimum TLS Version	99 - Unlimited 10 – TLS 1.0 11 – TLS 1.1 12 – TLS 1.2	99 - Unlimited
P22294	Maximum TLS Version	99 - Unlimited 10 – TLS 1.0 11 – TLS 1.1 12 – TLS 1.2	99 - Unlimited

SYSLOG PROTOCOL

- **Web Configuration**

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

Syslog Protocol:	UDP ▾
Syslog Server:	

- **Functionality**

    Allow users to customize the Syslog Protocol.

- **New P Values**

Pvalue	Description	Value range	Default
P8402	Syslog Protocol	0 – UDP 1 – SSL/TLS	0 – UDP

FIRMWARE VERSION 1.0.1.2

PRODUCT NAME

HT813

DATE

10/05/2018

FIRMWARE FILE INFORMATION

- Firmware file name: ht813fw.bin

  MD5: abf81fb6f13276bcc6084124efd5c0ba

BUG FIX

- Fixed device will not unconditional Forward Calls to VoIP when FXO port is unregister.
- Fixed Fax does not have Re-Invite message and Fax transmitted as Pass Through in T38 mode.
- Fixed device INVITE SDP message carried wrong Vocoder information.