

HT841/HT881 Firmware Release Notes

IMPORTANT UPGRADING NOTE

Table of Content

IMPORTANT UPGRADING NOTE	1
FIRMWARE VERSION 1.0.11.8.....	5
PRODUCT NAME.....	5
DATE	5
FIRMWARE FILE INFORMATION	5
ENHANCEMENT	5
BUG FIX	6
NEW FEATURES OVERVIEW	7
<i>Enable Bypass Locked State.....</i>	7
<i>Maximum Transmission Unit (MTU)</i>	7
<i>OpenVPN® TLS Key</i>	8
<i>Enable TR069 Through Management Interface</i>	9
<i>SCEP Support.....</i>	9
<i>Enable Manual VLAN Configuration.....</i>	12
<i>Enable T.38 TEP.....</i>	12
<i>Use Random SIP Registration Failure Retry Wait Time.....</i>	13
<i>Random SIP Registration Failure Retry Wait Time: Minimum and Maximum.....</i>	13
FIRMWARE VERSION 1.0.9.9	15
PRODUCT NAME.....	15
DATE	15
FIRMWARE FILE INFORMATION	15
ENHANCEMENT	15
BUG FIX	16
NEW FEATURES OVERVIEW	16
<i>Subscribe Retry Wait Time upon 403 Forbidden.....</i>	16
<i>Secondary NTP server</i>	17
<i>Local Time</i>	17
<i>Syslog header format.....</i>	18
<i>OpenVPN® Additional Options.....</i>	18
<i>Static DNS Cache.....</i>	19
<i>HELD Use LLDP Information.....</i>	26
<i>Enable LLDP.....</i>	27
<i>LLDP TX Interval.....</i>	27
<i>Enable CDP</i>	28
<i>Off-hook Auto Dial</i>	28

<i>Support GRUU</i>	28
<i>Support outbound</i>	29
<i>Random RTP Port Range</i>	29
<i>Force DTMF to be sent via SIP INFO simultaneously</i>	30
<i>Re-INVITE Upon CNG Count</i>	30
<i>OpenVPN® Server Secondary</i>	31
<i>T.38 Max Bit Rate</i>	31

FIRMWARE VERSION 1.0.7.333

PRODUCT NAME.....	33
DATE	33
FIRMWARE FILE INFORMATION	33
ENHANCEMENT	33
BUG FIX	33

FIRMWARE VERSION 1.0.5.1034

PRODUCT NAME.....	34
DATE	34
FIRMWARE FILE INFORMATION	34
ENHANCEMENT	34

FIRMWARE VERSION 1.0.5.935

PRODUCT NAME.....	35
DATE	35
FIRMWARE FILE INFORMATION	35
ENHANCEMENT	35
BUG FIX	35
NEW FEATURES OVERVIEW	36
<i>Enable Early Media for VoIP-to-PSTN Calls</i>	36
<i>Request URI Routing ID</i>	36
<i>Auto Send DTMF Upon Call Start</i>	37
<i>RTP/RTCP Keep Alive on Hold</i>	37

FIRMWARE VERSION 1.0.3.439

PRODUCT NAME.....	39
DATE	39
FIRMWARE FILE INFORMATION	39
ENHANCEMENT	39
BUG FIX	39
NEW FEATURES OVERVIEW	39
<i>Polarity On Answer Delay</i>	39

<i>AVS DTMF Detector Parameters</i>	40
<i>Radius Auth Protocol</i>	40

FIRMWARE VERSION 1.0.1.242

PRODUCT NAME	42
DATE	42
FIRMWARE FILE INFORMATION	42
ENHANCEMENT	42

FIRMWARE VERSION 1.0.11.8

PRODUCT NAME

HT841, HT881

Software Version: Program 1.0.11.8; Core 1.0.11.4; Base 1.0.11.8; Boot 1.0.11.4; CPE 1.0.5.43

DATE

08/14/2026

FIRMWARE FILE INFORMATION

- Firmware file name: ht8x1fw.bin
MD5: 3489a87fc42fec9d6ca4afbde18554a2

ENHANCEMENT

- Changed the default value of Web Access Mode (P1650) to "0 – HTTPS".
- Changed the default value of "Enable/Disable Weak Cipher Suites" (P8536) to "8 - Disable All Of The Above Weak TLS Ciphers Suites".
- Changed the default value of "Use Random SIP Port" (P20501–20503) to "1 - Yes".
- Changed the default value of "Use Random RTP Port" (P20505/20507) to "1 - Yes".
- Changed the default value of "Minimum TLS Version" (P22293) to "12 - TLS 1.2".
- Changed the default value of "Profile Active" (P271/401/501) to "0 – No".
- Changed the default value of "Enable Port" (P4595–4603) for FXS Port and FXO Ports 1–8 to "0 - No".
- Added support for "Radius bypass locked state". [Enable Bypass Locked State]
- Added support for "Maximum Transmission Unit (MTU)". [Maximum Transmission Unit (MTU)]
- Added support to periodically save time to a time file.
- Added support for remote access to WebUI via GDMS.
- Added support for OpenVPN TLS Key and Key Type. [OpenVPN® TLS Key]
- Added support to hang up FXO calls directly from the WebUI.
- Updated WebUI wording from "OPUS" to "Opus".
- Adjusted DHCP Option 160 to have higher priority than Option 66 to match other Grandstream devices.
- Added support for "Enable TR-069 Through Management Interface". [Enable TR069 Through Management Interface]
- Added support for AES-GCM encryption.
- Added the ability to calculate and append checksum values to outbound UDP RTP packets.
- Added and improved features for customizing default vendor configuration files ([X GRANDSTREAM Vendor Configuration File]).
- Added support for the SCEP protocol. [SCEP Support]
- Added support for RFC 8760

- Added the ability to configure VLAN settings via TR-069. [Enable Manual VLAN Configuration]
- Added support for displaying GSDVC info on the System Info page.
- Added support for DHCP Options 43–250.
- Added support for enabling T.38 Talker Echo Protection (TEP). [Enable T.38 TEP]
- Added support for the SIP PUBLISH method.
- Added the ability to configure minimum and maximum values for the registration retry wait time. [Use Random SIP Registration Failure Retry Wait Time]
- Added the ability to configure minimum and maximum values for the registration retry timer. [Random SIP Registration Failure Retry Wait Time: Minimum and Maximum]
- Added security improvements.
- Added non-WebUI P-values:
 - P28931–28933 — Minimum On-hook Voltage Threshold (Range: 10–26, Default: 18).

BUG FIX

- Fixed an issue where the device became non-configurable and unable to upgrade after updating firmware to 1.0.5.10.
- Fixed a certificate expiration warning issue.
- Fixed an issue where the device detected that a call was answered while it was still ringing.
- Fixed an incorrect time zone setting for Argentina.
- Fixed an issue where the device failed to obtain an IP address via PPPoE.
- Fixed an issue where the device failed to validate the server certificate timestamp for 802.1x authentication.
- Fixed an issue where the device could not send faxes.
- Fixed a device crash issue.
- Fixed an issue where the device failed to validate certificates with the outbound proxy.
- Fixed Zoom ZPLS compatibility issues.
- Fixed an issue where SRTP renegotiation failure during call forwarding caused disconnections.
- Fixed an issue where the device was unable to change passwords via ACS.
- Fixed an issue with malformed DHCP packets.
- Fixed an issue on the System Info page ("Device Details") displaying incorrect default gateway information.
- Fixed a faxing issue with the SR140 faxing platform.
- Fixed an issue causing the device not to send DNS queries.
- Fixed an issue causing the device not to use DNS replies.
- Fixed an issue where the FXO port got stuck in the Idle status.
- Fixed a call failure issue occurring after firmware upgrades.
- Fixed a device upgrade failure issue.
- Fixed an incorrect circuit ID value sent in TR-069 connection requests when CID was pushed using DHCP Option 82.
- Fixed a DNS delete-after-malloc memory issue.
- Fixed a firmware update path issue.

- Fixed an issue where the Session ID was not incremented after an SDP update.
- Fixed an issue where the TR-069 Connection Request URL did not follow the expected device format.
- Fixed an issue where FXO detected Caller ID from Bizvoice lines as special characters.
- Fixed an FXO call termination issue with unanswered calls.
- Fixed missing GDMS ports showing the status of registered extensions.
- Fixed an issue where the CA Bundle Manifest failed to display uploaded certificate details.
- Fixed an issue where the device sent DNS AAAA queries when only IPv4 was enabled.
- Fixed an issue where the SIP trunk failed to register after an upgrade.
- Fixed a potential memory leak issue.
- Fixed a memory leak related to subjectAltNames during TLS connection validation.
- Fixed an issue where FXS ports became unresponsive (no dial tone / no IVR response), requiring a reboot to recover.
- Fixed internal bugs.

NEW FEATURES OVERVIEW

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

Enable Bypass Locked State

- **Web Configuration**

Users can find the configuration section in WebUI-> System Settings -> RADIUS Settings

Action upon Radius Auth Server Error  ☐ Reject Access ☒ Authenticate Locally

Enable Bypass Locked State  ☐

RADIUS Auth Protocol 

PAP 

- **Functionality**

This feature allows users to configure the Bypass Locked State. When the user enables it, RADIUS accounts can bypass the WebUI locked state caused by local accounts.

- **New P Values**

Pvalue	Description	Value Range	Default
28930	Enable Bypass Locked State	Number: 0 - No 1 - Yes	0 - No

Maximum Transmission Unit (MTU)

- **Web Configuration**

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

Use ARP to detect network connectivity  ☒

Maximum Transmission Unit (MTU) 

1500

- **Functionality**

This feature allows users to configure the Maximum Transmission Unit (MTU). Users can configure the MTU in bytes. The default value is 1500 bytes, and the range is 576-1500 bytes.

- **New P Values**

Pvalue	Description	Value Range	Default
244	Maximum Transmission Unit (MTU)	Number: 576 –1500	1500

OpenVPN® TLS Key

- **Web Configuration**

Users can find the configuration section in WebUI-> Network Settings -> OpenVPN® Settings.

OpenVPN® Client Key Password 

OpenVPN® TLS Key 

OpenVPN® TLS Key Type 

none

OpenVPN® Additional Options 

- **Functionality**

This feature allows users to configure the OpenVPN® TLS Key and OpenVPN® TLS Key type.

- **New P Values**

Pvalue	Description	Value Range	Default
22371	OpenVPN® TLS Key	String: Max Length: 8192	(Null)
22457	OpenVPN® TLS Key Type	Number: 0 – none, 1 – TLS-Auth, 2 – TLS-Crypt.	0 - none

Enable TR069 Through Management Interface

- Web Configuration**

Users can find the configuration section in WebUI-> System Settings-> Management Settings->Management Interface.

Enable SNMP Through Management Interface  ☐ 

Enable TR069 Through Management Interface  ☐ 

Enable Syslog Through Management Interface  ☐ 

Enable Radius Through Management Interface  ☐ 

- Functionality**

This feature allows users to configure Enable TR069 Through Management Interface. Users allow dedicated activation of the TR-069 protocol access through a dedicated management interface for remote device management and configuration. Disabled by default.

- New P Values**

Pvalue	Description	Value Range	Default
8607	Enable TR069 Through Management Interface	Number: 0 - No 1 - Yes	0 - No

SCEP Support

- Web Configuration**

Users can find the configuration section in WebUI-> System Settings -> Security Settings-> SCEP.

Security Settings

[Web/SSH Access](#)
[User Info Management](#)
[Client Certificate](#)
[Trusted CA Certificates](#)
[SCEP](#)

Basic Settings

Enable SCEP ⓘ

☐

SCEP Server URL ⓘ

CA FingerPrint Infomation ⓘ

Challenge Password ⓘ

Local configuration

Local Public and Private Key Length ⓘ

The Name of Certificate Applicant ⓘ

The Country of Certificate Applicant Located ⓘ

The State of Certificate Applicant Located ⓘ

The Locality of Certificate Applicant Located ⓘ

The Organization of Certificate Applicant Located ⓘ

The organization unit of Certificate Applicant ⓘ

HTTP Authentication

CID ⓘ

Password ⓘ

Certificates and Updates

CA Certificates ⓘ

View

Client Certificate Alternative Name ⓘ

Update Interval before Certificate Expiration ⓘ

Update now

Scope of Use ⓘ

☒ Custom Certificate
 ☐ 802.1X
 ☐ OpenVPN
 ☐ TR069

• Functionality

This feature allows users to configure the SCEP-related settings. It allows users to enable the Simple Certificate Enrollment Protocol and specify the SCEP Server URL, CA Fingerprint, and Challenge Password. Additionally, users can configure local certificate settings, such as key length and applicant details (e.g., Name, Country, State), and set the HTTP authentication credentials and certificate update intervals.

- **New P Values**

Pvalue	Description	Value Range	Default
8647	Enable SCEP	Number: 0 – No, 1 – Yes.	0 – No
8648	SCEP Server URL	String: (Initial with "http://") Maxlength 256 characters	(Null)
8652	CA FingerPrint Information	String: Password Maxlength 256 characters	(Null)
8653	Challenge Password	String: Password Maxlength 256 characters	(Null)
8654	Local Public and Private Key Length	Number: 0 – 1024 bit 1 – 2048 bit 2 – 3072 bit 3 – 4096 bit	2 - 3072 bit
8655	The Name of Certificate Applicant	String: Maxlength 64 characters	
8656	The Country of Certificate Applicant Located	String: (Check config template for details)	US - United States of America (US)
8657	The State of Certificate Applicant Located	String: Maxlength 128 characters	
8658	The Locality of Certificate Applicant Located	String: Maxlength 128 characters	
8659	The Organization of Certificate Applicant Located	String: Maxlength 64 characters	
8660	The organization unit of Certificate Applicant	String: Maxlength 64 characters	
8649	CID	String: Maxlength 256 characters	
8650	Password	String: Password Maxlength 256 characters	
8661	Client Certificate Alternative Name	String: Maxlength 1024 characters	\$MAC.local
8662	Update Interval before Certificate Expiration	Number: 1- 30	20
8663	Scope of Use	String: checkbox CustomCertificate-Custom	CustomCertificate

		Certificate 802.1X- 802.1X OpenVPN- OpenVPN TR069 - TR069	
--	--	--	--

Enable Manual VLAN Configuration

- Web Configuration**

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

Enable CDP  ☒

Enable Manual VLAN Configuration  ☒

- Functionality**

This feature allows users to configure the “Enable Manual VLAN Configuration” option. It allows users to allow the phone to keep the VLAN configuration without applying it.

- New P Values**

Pvalue	Description	Value Range	Default
22174	Enable Manual VLAN Configuration	Number: 0 – No, 1 – Yes.	1 –Yes

Enable T.38 TEP

- Web Configuration**

Users can find the configuration section in WebUI-> Port Settings -> FXS or FXO Profile-> Codec Settings.

T.38 Max Bit Rate  9600bps 

Enable T.38 TEP  ☐

Re-INVITE After Fax Tone Detected  ☒

- Functionality**

This feature allows users to configure the Enable T.38 TEP. When enabled, talker echo protection (TEP) will be activated for T.38 fax calls. TEP helps reduce echo interference but may impact transmission reliability on some connections. Enable only if echo is affecting fax quality.

- **New P Values**

Pvalue	Description	Value Range	Default
22667 22668 22669	Enable T.38 TEP	Number: 0 – No 1 – Yes	0 – No

Use Random SIP Registration Failure Retry Wait Time

Web Configuration

Users can find the configuration section in Web->FXS or FXO Profile -> SIP Settings -> SIP Basic Settings.

SIP Registration Failure Retry Wait Time ⓘ

Use Random SIP Registration Failure Retry Wait Time ⓘ ☐

Random SIP Registration Failure Retry Wait Time Range ⓘ -

- **Functionality**

This feature allows users to configure the Use Random SIP Registration Failure Retry Wait Time. When enabled, the waiting time to resend a registration request in case of SIP registration failure will become a random number in the setting “Random SIP Registration Failure Retry Wait Time Range”.

- **New P Values**

Pvalue	Description	Value Range	Default
60096 60196 60296	Use Random SIP Registration Failure Retry Wait Time	Number: 0 – No 1 – Yes	0 – No

Random SIP Registration Failure Retry Wait Time: Minimum and Maximum

- **Web Configuration**

Users can find the configuration section in WebUI -> Profile -> SIP Settings -> SIP Basic Settings.

Use Random SIP Registration Failure Retry Wait Time ⓘ ☐

Random SIP Registration Failure Retry Wait Time Range ⓘ -

SIP Registration Failure Retry Wait Time upon 403 Forbidden ⓘ

- **Functionality**

This feature allows users to set the range of random wait time before retrying registration after failure. The unit is seconds. Valid values range from 60 to 600 seconds.

- **New P Values**

Pvalue	Description	Value Range	Default
60097 60197 60297	Random SIP Registration Failure Retry Wait Time Range: Minimum	Number: 60-600 (seconds)	60
60098 60198 60298	Random SIP Registration Failure Retry Wait Time Range: Maximum	Number: 60-600 (seconds)	600

FIRMWARE VERSION 1.0.9.9

PRODUCT NAME

HT841, HT881

DATE

01/28/2025

FIRMWARE FILE INFORMATION

- Firmware file name: ht8x1fw.bin
MD5: a94e33ee5e04f447aec067114e1f722

ENHANCEMENT

- Added IVR support to check Device Individual Certificate information.
- Added support for Subscribe Retry Wait Time upon 403 Forbidden. [Subscribe Retry Wait Time upon 403 Forbidden]
- Added support for Secondary NTP server. [Secondary NTP server]
- Added the option to validate SIP User ID in Request-Line.
- Added the TR-069 Command for Triggering False Ring Signal.
- Changed the "anonymous" to "private" and "unknown" to "unavailable" in the X-ATA-CallerID header.
- Added ability to set local date and time. [Local Time]
- Added support for the Syslog header format. [Syslog header format]
- Added support for WebUI hides "Conference URI" when "Special Feature" is set to "BroadSoft"
- Added support to upload config template in txt format.
- Added the ability to pull the SIP User ID per port via SNMP.
- Added the ability to set OpenVPN options. [OpenVPN® Additional Options]
- Added support to configure the static DNS SRV records. [Static DNS Cache]
- Added support CIDR when configuring static IP from WebUI.
- Updated the "Enable High Ring Power" (P4234) to "Ring Power".
(P4234 Ring Power. 0 - 45Vrms default, 3 - 50Vrms, 4 - 55Vrms. Default is 0.)
- Added support for HELD Use LLDP Information. [HELD Use LLDP Information]
- Added support for Enable LLDP. [Enable LLDP]
- Added support for LLDP TX Interval. [LLDP TX Interval]
- Added support for Enable CDP. [Enable CDP]
- Added ability to set off-hook Auto-Dial number via feature code. [Off-hook Auto Dial]
- Added support for Firmware Upgrade via Resync SIP Notify.
- Added support for RFC5627 GRUU. [Support GRUU]
- Added support for RFC5626 outbound. [Support outbound]
- Added support RTP port range. [Random RTP Port Range]
- Added support sending multiple DTMF modes simultaneously. [Force DTMF to be sent via SIP]

INFO simultaneously]

- Added support to initiate a Re-Invite for fax transmission when the fax machine is the sender. [Re-INVITE Upon CNG Count]
- Added support for the SIP PUBLISH method (RFC 6035).
- Added support OpenVPN® failover option. [OpenVPN® Server Secondary]
- Added support for T.38 Max Bit Rate. [T.38 Max Bit Rate]
- Updated the “VAD(P50/750/550)” to “Silence Suppression”
- Updated the default value of NTP Server(P30) “us.pool.ntp.org” to “pool.ntp.org”
- Changed the “Black List” to “Block List”, and “White List” to “Allow List”
- Updated the “3CX Auto Provision (P1414)” to “Auto Provision”.
- Enhanced the security of HT devices.
- Optimized parameter’s location on the WebUI for better usability.

BUG FIX

- Fixed the unit can't establish SRTP Session after re-invite.
- Fixed the DTMF transmission failure issue.
- Fixed the device FXO profile's lack of "stats" data model.
- Fixed the device MIB files do not show the exact model's name.
- Fixed device unable to import MIB file to PRTG.
- Fixed device has an issue sending RTP/AVP in the 200 OK over SRTP outbound calls.
- Fixed the User level WebUI access could show all tabs other than the Status tab.
- Fixed device could hear the voicemail reminder with the Offhook Auto-Dial enabled.
- Fixed device fails to apply configuration using XML template.
- Fixed device OpenVPN settings do not remain after turning off the HT.
- Fixed device keeps sending EAPOL Start when a Linux PC is connected to the LAN port on bridge mode.
- Fixed the Swedish Pulse dialing.
- Fixed HT device to reboot and generate a Core Dump when receiving a call.
- Fixed the SIGSEGV in relnit_Socket during SIP operation.

NEW FEATURES OVERVIEW

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

Subscribe Retry Wait Time upon 403 Forbidden

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

SUBSCRIBE for MWI ?	No, do not send SUBSCRIBE for Message Wait ?
Subscribe Retry Wait Time upon 403 Forbidden ?	0
Local SIP Port ?	5060

Functionality

This feature allows users to configure the Subscribe Retry Wait Time upon 403 Forbidden. This specifies the wait time to retry subscribe after receiving 403 Forbidden. The valid range is 0 to 10080 in minutes, default is 0. If the value is not 0, the device will retry 10 times first, then wait for the specified time before trying again. If the value is 0, the device will follow the "Retry-After" header if present. Otherwise, the device will wait 20 minutes before sending subscribe again.

Pvalue	Description	Value Range	Default
60068	Subscribe Retry Wait Time upon 403 Forbidden	Number: 0 - 10080	0

Secondary NTP server

User can find the configuration section in Web -> System Settings -> Time and Language.

NTP Server ⓘ

Secondary NTP Server ⓘ

Allow DHCP Option 42 to Override NTP Server ⓘ
☒ ⓘ

- Functionality**

This feature allows users to configure the Secondary NTP Server. Configure the URL or IP address of the NTP server. The device may obtain the date and time from the server.

Pvalue	Description	Value Range	Default
8333	Secondary NTP Server	String: Server address	(Null)

Local Time

User can find the configuration section in Web -> System Settings -> Time and Language.

Self-Defined Time Zone ⓘ
 ⓘ

Allow DHCP Option 2 to Override Time Zone Setting ⓘ
☒ ⓘ

Local Time

Sync PC

- Functionality**

This feature allows users to set device time from the host PC time via the browser. After clicking the bottom "Sync PC", the device will display the notice of the synchronized local time.

Local Time

Sync PC

The synchronized local time is: 2025-1-27 21:42:38

Pvalue	Description	Value Range	Default
	Local Time	Button	(Null)

Syslog header format

User can find the configuration section in Web-> Maintenance -> System Diagnosis->Syslog.

Syslog Protocol  UDP

Syslog Header Format  Default

Send SIP Log  ☒

- Functionality**

This feature allows users to configure the Syslog Header Format. When "RFC3164 Compliant" is enabled, the syslog header will contain the PRI and timestamp information to be compatible with RFC3164.

Pvalue	Description	Value Range	Default
8723	Syslog Header Format	Number: 0 – Default 1 – RFC3164 Compliant	0 – Default

OpenVPN® Additional Options

User can find the configuration section in Web-> Network Settings -> OpenVPN® Settings

OpenVPN® Client Key Password 

OpenVPN® Additional Options 

- Functionality**

This feature allows users to configure the OpenVPN® Additional Options, which are appended to the OpenVPN® config file. Note: Additional options are separated by semicolons.

For example: "connect-retry 5; tls-client; keepalive 10 60." Please use it with caution. Make sure that the options are supported by OpenVPN® and do not unnecessarily override other configurations.

Pvalue	Description	Value Range	Default
8460	OpenVPN® Additional Options	String: Maxlength 2048 characters	(Null)

Static DNS Cache

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

NAPTR

[NAPTR](#) [SRV](#) [A](#)

Order	NAPTR DNS Cache Name	NAPTR DNS Cache Time Interval (s)	NAPTR DNS Cache Order	NAPTR DNS Cache Preference	NAPTR DNS Cache Replacement	NAPTR DNS Cache Service	Operation
1		300	0	0		SIP+D2U	
2		300	0	0		SIP+D2U	
3		300	0	0		SIP+D2U	
4		300	0	0		SIP+D2U	
5		300	0	0		SIP+D2U	
6		300	0	0		SIP+D2U	
7		300	0	0		SIP+D2U	
8		300	0	0		SIP+D2U	
9		300	0	0		SIP+D2U	
10		300	0	0		SIP+D2U	
11		300	0	0		SIP+D2U	
12		300	0	0		SIP+D2U	
13		300	0	0		SIP+D2U	
14		300	0	0		SIP+D2U	
15		300	0	0		SIP+D2U	
16		300	0	0		SIP+D2U	

Add

×

NAPTR DNS Cache Name ?

NAPTR DNS Cache Time Interval (s) ?

NAPTR DNS Cache Order ?

NAPTR DNS Cache Preference ?

NAPTR DNS Cache Replacement ?

NAPTR DNS Cache Service ?

Cancel

Save

SRV:

NAPTR SRV A

Order	SRV DNS Cache Name	SRV DNS Cache Time Interval (s)	SRV DNS Cache Priority	SRV DNS Cache Weight	SRV DNS Cache Target	SRV DNS Cache Port	Operation
1		300	0	0		0	
2		300	0	0		0	
3		300	0	0		0	
4		300	0	0		0	
5		300	0	0		0	
6		300	0	0		0	
7		300	0	0		0	
8		300	0	0		0	
9		300	0	0		0	
10		300	0	0		0	
11		300	0	0		0	

Add

×

SRV DNS Cache Name ?



SRV DNS Cache Time Interval (s) ?

300



SRV DNS Cache Priority ?

0



SRV DNS Cache Weight ?

0



SRV DNS Cache Target ?



SRV DNS Cache Port ?

0



Cancel

Save

A:

Order	A DNS Cache Name	A DNS Cache Time Interval(s)	A DNS Cache IP Address	Operation
1		300		
2		300		
3		300		
4		300		
5		300		
6		300		
7		300		
8		300		
9		300		
10		300		

Add

×

A DNS Cache Name ?

!

A DNS Cache Time Interval(s) ?

!

A DNS Cache IP Address ?

!

Cancel

Save

• Functionality

This feature could let the user configure the DNS Cache Name, DNS Cache Time Interval(s), DNS Cache Order, DNS Cache Preference, DNS Cache Replacement, DNS Cache Service, DNS Cache Priority, DNS Cache Weight, DNS Cache Target, DNS Cache Port, and DNS Cache IP Address for different DNS modes in NAPTR, SRV, and A Record.

NAPTR Settings

Pvalue	Description	Value range	Default
93000 93020 93040 93060 93080 93100 93120 93140 93160 93180	NAPTR DNS Cache Name	String: Max length 512 characters	(Null)

93200			
93220			
93240			
93260			
93280			
93300			
93320			
93340			
93001	NAPTR DNS Cache Time Interval(s)	Number:	300
93021			
93041		300 to 65535	
93061			
93081			
93101			
93121			
93141			
93161			
93181			
93201			
93221			
93241			
93261			
93281			
93301			
93321			
93341			
93002	NAPTR DNS Cache Order	Number:	0
93022			
93042		0 to 65535	
93062			
93082			
93102			
93122			
93142			
93162			
93182			
93202			
93222			
93242			
93262			
93282			
93302			
93322			
93342			
93003	NAPTR DNS Cache Preference	Number:	0
93023			
93043		0 to 65535	
93063			
93083			
93103			
93123			
93143			
93163			
93183			
93203			
93223			
93243			

93263			
93283			
93303			
93323			
93343			
93007	NAPTR DNS Cache Replacement	String:	(Null)
93027			
93047			
93067			
93087			
93107			
93127			
93147			
93167			
93187			
93207			
93227			
93247			
93267			
93287			
93307			
93327			
93347			
93005	Service	String:	SIP+D2U
93025			
93045			
93065		Max length 512	
93085		characters	
93105			
93125			
93145			
93165			
93185			
93205			
93225			
93245			
93265			
93285			
93305			
93325			
93345			

SRV Settings

Pvalue	Description	Value range	Default
93008	SRV DNS Cache Order Name	String:	(Null)
93028			
93048			
93068		Max length 512	
93088		characters	
93108			
93128			
93148			
93168			
93188			
93208			

93228 93248 93268 93288 93308 93328 93348			
93009 93029 93049 93069 93089 93109 93129 93149 93169 93189 93209 93229 93249 93269 93289 93309 93329 93349	SRV DNS Cache Time Interval(s)	Number: 300 to 65535	300
93010 93030 93050 93070 93090 93110 93130 93150 93170 93190 93210 93230 93250 93270 93290 93310 93330 93350	SRV DNS Cache Priority	Number: 0 to 65535	0
93011 93031 93051 93071 93091 93111 93131 93151 93171 93191 93211 93231 93251 93271	SRV DNS Cache Weight	Number: 0 to 65535	0

93291			
93311			
93331			
93351			
93013	SRV DNS Cache Target	String:	(Null)
93033			
93053			
93073			
93093			
93113			
93133			
93153			
93173			
93193			
93213			
93233			
93253			
93273			
93293			
93313			
93333			
93353			
93012	SRV DNS Cache Port	Number: 0 to 65535	0
93032			
93052			
93072			
93092			
93112			
93132			
93152			
93172			
93192			
93212			
93232			
93252			
93272			
93292			
93312			
93332			
93352			

A Settings

Pvalue	Description	Value range	Default
93014	A DNS Cache Name	String: max length 512 Characters	(Null)
93034			
93054			
93074			
93094			
93114			
93134			
93154			
93174			
93194			
93214			
93234			

93254 93274 93294 93314 93334 93354			
93015 93035 93055 93075 93095 93115 93135 93155 93175 93195 93215 93235 93255 93275 93295 93315 93335 93355	A DNS Cache Time Interval(s)	Number: 300 to 65535	300
93016 93036 93056 93076 93096 93116 93136 93156 93176 93196 93216 93236 93256 93276 93296 93316 93336 93356	A DNS Cache IP Address	String:	(Null)

HELD Use LLDP Information

User can find the configuration section in Web -> System Settings -> E911/HELD.

HELD Location Types ⓘ

HELD Use LLDP Information ⓘ ☐

HELD NAI ⓘ ☐

- **Functionality**

This feature allows users to configure HELD Use LLDP Information. If "Yes", the information from the LLDP-support switch is used to generate ChassisID and PortID; otherwise, the MAC address of the gateway and phone is used as default.

Pvalue	Description	Value Range	Default
8575	HELD Use LLDP Information	Number: 0 – No 1 – Yes	0 – No

Enable LLDP

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

Enable LLDP ? ☒

LLDP TX Interval ?

Enable CDP ? ☒

- **Functionality**

This feature allows users to enable or disable LLDP. It controls the LLDP (Link Layer Discovery Protocol) service.

Pvalue	Description	Value Range	Default
1684	Enable LLDP	Number: 0 – No 1 – Yes	1 – Yes

LLDP TX Interval

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

Enable LLDP ? ☒

LLDP TX Interval ?

Enable CDP ? ☒

- **Functionality**

This feature allows users to configure LLDP TX Interval (in seconds). The valid range is 1 to 3600.

Pvalue	Description	Value Range	Default
22122	LLDP TX Interval	Number: 1 - 3600	60

Enable CDP

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

LLDP TX Interval ⓘ

Enable CDP ⓘ ☒

Layer 2 QoS 802.1Q/VLAN Tag ⓘ ⓘ

- Functionality**

This feature allows users to configure the enable or disable CDP. If enabled, the device will use the Cisco Discovery Protocol feature.

Pvalue	Description	Value Range	Default
22119	Enable CDP	Number: 0 – No 1 – Yes	1 – Yes

Off-hook Auto Dial

User can find the configuration section in Web-> FXS -> Call Features Settings-> Off-hook Auto Dial

| Off-hook Auto Dial

Set Offhook Auto-Dial Feature ⓘ ☒

Enable set Offhook Auto-Dial ⓘ

- Functionality**

This feature allows users to configure the enable or disable the Off-hook Auto Dial and set up the number of Enable set Offhook Auto-Dial.

Pvalue	Description	Value Range	Default
24089	Set Offhook Auto-Dial Feature	Number: 0 – No 1 – Yes	1 – Yes
24040	Enable set Offhook Auto-Dial	String: Number Max length 2 characters	77

Support GRUU

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

Support outbound ? ☐

Support GRUU ? ☐

SIP URI Scheme When Using TLS ? ☐ sip ☒ sips

- **Functionality**

This feature allows users to configure the Support GRUU for RFC 5627.

Pvalue	Description	Value Range	Default
60080	Support GRUU	Number: 0 – No 1 – Yes	0 – No

Support outbound

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

Support SIP Instance ID ? ☒

Support outbound ? ☐

Support GRUU ? ☐

- **Functionality**

This feature allows users to configure the Support outbound for RFC 5626.

Pvalue	Description	Value Range	Default
60081	Support outbound	Number: 0 – No 1 – Yes	0 – No

Random RTP Port Range

User can find the configuration section in Web-> FXS -> Codec Settings-> RTP Setting.

Use Random RTP Port ? ☐

Random RTP Port Range ?

 -

Symmetric RTP ? ☐

- **Functionality**

This feature allows users to set the Random RTP Port Range, range is 1024-65535.

Pvalue	Description	Value Range	Default
60084	Random RTP Port Range: Min	Number: 1024 - 65535	(Null)
60085	Random RTP Port Range: Max	Number: 1024 - 65535	(Null)

Force DTMF to be sent via SIP INFO simultaneously

User can find the configuration section in Web-> FXS -> Codec Settings-> DTMF Settings.

Preferred DTMF ⓘ choice 1 RFC2833
 choice 2 SIP INFO
 choice 3 In-audio

Force DTMF to be sent via SIP INFO simultaneously ⓘ ☐

Inband DTMF Duration ⓘ Duration: 100 ms, Inter Duration: 50 ms

- **Functionality**

This feature allows users to configure the Force DTMF to be sent via SIP INFO simultaneously.

Pvalue	Description	Value Range	Default
28794	Force DTMF to be sent via SIP INFO simultaneously	Number: 0 – No 1 – Yes	0 – No

Re-INVITE Upon CNG Count

User can find the configuration section in WebUI-> FXS/FXO -> Codec Settings-> Vocoder Settings

Re-INVITE After Fax Tone Detected ⓘ ☒

Re-INVITE Upon CNG Count ⓘ 0

Jitter Buffer Type ⓘ ☐ Fixed ☒ Adaptive

- **Functionality**

This feature allows users to initiate a Re-Invite for fax transmission when the fax machine is the sender.

If it is set to 0, this feature is disabled. Equal to or greater than 1: ATA will initialize the re-invite request when the CNG count is reached. The valid range is [0, 6].

Pvalue	Description	Value Range	Default
28923	Re-INVITE Upon CNG Count	Number: 0 - 6	0
28924			
28925			

OpenVPN® Server Secondary

Users can find the configuration section in Web -> Maintenance-> VPN.

OpenVPN® Server Secondary Address 

OpenVPN® Secondary Port 

Randomly Select Server  ☐

- Functionality**

This feature allows users to configure the OpenVPN® Server Secondary Address for the failover. The user could set the OpenVPN® Server Secondary Address and Port and decide if to enable the Randomly Select Server. If it is enabled, a server will be randomly selected in the configuration to start OpenVPN® requests. If closed, requests will be made in the order of server configuration.

Pvalue	Description	Value Range	Default
22597	OpenVPN® Server Secondary Address	String: maximum length: 253 characters	(Null)
22598	OpenVPN® Secondary Port	Number: 1 - 65535	1194
22599	Randomly Select Server	Number: 0 – No 1 – Yes	0 - No

T.38 Max Bit Rate

User can find the configuration section in WebUI-> FXS/FXO -> Codec Settings-> Vocoder Settings

Fax Mode  ☒ T.38 ☐ Pass-Through

T.38 Max Bit Rate 

Re-INVITE After Fax Tone Detected  ☒

- Functionality**

This feature allows user to select the maximum T.38-bit rate. Lowering the maximum fax bit rate may help improve the fax success rate. Only effective when the fax machine is fax receipt.

Pvalue	Description	Value Range	Default
28913 28914 28915	T.38 Max Bit Rate	Number: 1 - 4800bps, 2 - 9600bps, 3 - 14400bps	2 - 9600bps,

FIRMWARE VERSION 1.0.7.3

PRODUCT NAME

HT841, HT881

DATE

07/01/2024

FIRMWARE FILE INFORMATION

- Firmware file name: ht8x1fw.bin
MD5: 0f838418ec2fff575a830b7aabd65992

ENHANCEMENT

- Added IVR support to check Device Individual Certificate information.
- Added support to sort downloaded XML config file p-values in ascending order.
- Added support for p-value not on WebUI:
P82307 Syslog Setting and Internal Logs Protection. (0- No, 1- Yes. The default is 0.
If set to '1 - Yes', Syslog settings and internal logs will be saved across a factory reset)

BUG FIX

- Fixed the Inbound SRTP call fails with "488 Not Acceptable Here" due to the index value of 88 used by Netsapiens.
- Fixed the issue which caused Registration spamming.
- Fixed unit can't establish SRTP Session after re-invite.
- Fixed a bug that caused the device not to request the config file until a reboot.
- Fixed device UAC will re-attempt requests with the same Credentials after 403 Forbidden.
- Fixed a bug that caused CID not to be detected using Bellcore Scheme.
- Fixed an issue of WebUI wording change request for DNS SRV failover.
- Fixed the bug of Prompt Tone Access Code was removed from the DTMF buffer.

FIRMWARE VERSION 1.0.5.10

PRODUCT NAME

HT841, HT881

DATE

04/28/2024

FIRMWARE FILE INFORMATION

- Firmware file name: ht8x1fw.bin
MD5: 6ea8117d84f686c96785d246a5f90e62

ENHANCEMENT

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

FIRMWARE VERSION 1.0.5.9

PRODUCT NAME

HT841, HT881

DATE

04/23/2024

FIRMWARE FILE INFORMATION

- Firmware file name: ht8x1fw.bin
MD5: 099b15ce88c7a34406c08eeaa4a0c72c

ENHANCEMENT

- Added support for New WebUI.
- Added support for "Enable Early Media for VoIP-to-PSTN Calls".[Enable Early Media for VoIP-to-PSTN Calls]
- Added support tone configuration by port. (Check the changelog for the details)
- Added support for "Request URI Routing ID" on FXO port. [Request URI Routing ID]
- Added support "SIP Destination Port" on the "Port Status" page. (WebUI->Status->Port Status)
- Added the status check whether local sip ports are the same between different profiles.
- Update the FXO's Hook Flash Timing from "300 – 1500" to "100 – 1500".
- Added support for "Auto Send DTMF Upon Call Start".[Auto Send DTMF Upon Call Start]
- Update the "DSP DTMF Detector SNR" value range from "0 – 2" to "0 – 12".
- Added RTP/RTCP Keep Alive on Hold. [RTP/RTCP Keep Alive on Hold]
- Added support for p-value not on WebUI:
Initial Line Polarity (P28834/28835/28836) (0 - Forward, 1 – Reverse. Default is 1)

BUG FIX

- Fixed the DDNS does not work issue.
- Fixed unit stops responding after a couple of hours.
- Fixed an issue that causes the caller not to hear the echo when leaving a message on the answering machine.
- Fixed a bug that caused the device to freeze after a few hours.
- Fixed an issue with the registration.
- Fixed a bug that caused the call to fail when the DDI line was connected to the FXS port of the device on the Macau DDI environment.
- Fixed the remote party perceiving echo.
- Fixed the Inaccurate encoding and decoding of DTMF durations with SIP Info.
- Fixed the Peer trunk with the FXO profile fails issue.
- Fixed the SRTP decrypt RTP fail causing one-way audio after a 20+ minute call.

- Fixed no audio on 200ok/ack with UAS on outbound calls.
- Fixed device cannot connect to OpenVPN server issue.

NEW FEATURES OVERVIEW

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

Enable Early Media for VoIP-to-PSTN Calls

Users can find the configuration section in Web -> FXO Profile 1 or 2-> FXO Termination.

PIN for PSTN-to-VoIP Calls 

Enable Early Media for VoIP-to-PSTN Calls  ☐ No ☒ Yes

• Functionality

This feature allows users to set the in-band ringtone option to hear ringtones and other alert tones in reverse polarity signals and supports responding with 183 progress on the FXO port.

Pvalue	Description	Value Range	Default
28830 28831	Enable Early Media for VoIP-to-PSTN Calls	Number: 0 – No 1 – Yes	0 – No

Request URI Routing ID

Users can find the configuration section in Web -> Port Settings-> FXO PORTS.

Hunting Group	Request URI Routing ID	Enable Port
Disabled 		☐ No ☒ Yes
Disabled 		☐ No ☒ Yes
Disabled 		☐ No ☒ Yes
Disabled 		☐ No ☒ Yes
Disabled 		☐ No ☒ Yes
Disabled 		☐ No ☒ Yes
Disabled 		☐ No ☒ Yes
Disabled 		☐ No ☒ Yes

- **Functionality**

This feature allows users to set up a specific FXO port on the outbound call when using FXO Hunting Group.

Pvalue	Description	Value Range	Default
4670 4671 4672 4673 4674 4675 4676 4677	Request URI Routing ID	Number: Max Length 64	(Null)

Auto Send DTMF Upon Call Start

Users can find the configuration section in Web -> FXO Profile 1 or 2-> Call Settings.

Auto Send DTMF Upon Call Start ?

Early Dial ? ☒ No ☐ Yes

- **Functionality**

This feature allows users to set DTMF digits to send to the TDM side after the call from the VoIP side gets started.

Pvalue	Description	Value Range	Default
28845 28846	Auto Send DTMF Upon Call Start	Number: Max Length 16	(Null)

RTP/RTCP Keep Alive on Hold

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

Use Random RTP Port ? ☒ No ☐ Yes

RTP/RTCP Keep Alive On Hold ? ☒ No ☐ Yes

Hold Target Before Refer ? ☐ No ☒ Yes

This feature allows users to set the RTP/RTCP keep Alive on Hold feature. If the RTCP is enabled, the device stops sending RTCP packets once the call is put on hold.

Pvalue	Description	Value Range	Default
28839 28840 28841	RTP/RTCP Keep Alive On Hold	Number: 0 – No 1 – Yes	0

FIRMWARE VERSION 1.0.3.4

PRODUCT NAME

HT841, HT881

DATE

10/23/2023

FIRMWARE FILE INFORMATION

- Firmware file name: ht8x1fw.bin
MD5: c07b9582ff0e837e3491edab1fe8f62f

ENHANCEMENT

- Added support "Polarity On Answer Delay". [Polarity On Answer Delay]
- Updated config file download request starts from cfgMAC.xml.
- Added new value "4 - Auto" in NAT Traversal(P52/730/630).
- Added support "AVS DTMF Detector Parameter" [AVS DTMF Detector Parameters]
- Added support "Radius auth protocol". [Radius Auth Protocol]
- Removed "Ring Timeout" (P816/516) from FXO page.

BUG FIX

- Fixed DNS SRV Failover fails when "Check Domain Certificates" is enabled.
- Fixed device config file download request does not start from cfgMAC.xml.
- Fixed NAT Traversal does not have the "Auto" option.
- Fixed Call Waiting CID cannot be displayed.
- Fixed an issue caused device echo during calls.

NEW FEATURES OVERVIEW

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

Polarity On Answer Delay

Users can find the configuration section in Web -> FXO Profile -> FXO Termination

Enable Polarity Reversal: ☒ No ☐ Yes (Default No. Check with your PSTN carrier before setting to Yes)

Polarity On Answer Delay: (200-30000 milliseconds. Default 1000 milliseconds)

- Functionality**

This feature allows users to configure the Polarity On Answer Delay.

Pvalue	Description	Value Range	Default
28825 28826	Polarity On Answer Delay	Number: 200 - 30000	1000

AVS DTMF Detector Parameters

User can find the configuration section in Web -> FXO Profile/FXO Profile.

DSP DTMF Detector Min Level: (-45-0 dBm, default is -25)

DSP DTMF Detector Snr: (0-2, default is 1)

DSP DTMF Detector Deviation: (0-25, default is 25)

DSP DTMF Detector Twist: (0-12 dB, default is 5)

Disable DTMF Negotiation: ☒ No (negotiate with peer) ☐ Yes (use above)

• Functionality

This feature allows users to configure the AVS DTMF detector related parameters. DSP DTMF Detector Min Level sets the minimum level required for DTMF tone to be considered valid, DSP DTMF Detector SNR sets the Maximum signal-to-noise ratio required for DTMF tone to be considered valid, DSP DTMF Detector Deviation sets the deviation, above and below the central frequency, DSP DTMF Detector Twist sets the maximum value by which one frequency energy level can surpass another frequency energy level.

Pvalue	Description	Value Range	Default
28804 28805 28806	DSP DTMF Detector Min Level	Number: -45 – 0	-25
28808 28809 28810	DSP DTMF Detector SNR	Number: 0 – 2	1
28812 28813 28814	DSP DTMF Detector Deviation	Number: 0 – 25	25
28816 28817 28818	DSP DTMF Detector Twist	Number: 0 – 12	5

Radius Auth Protocol

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

Error: ☐ Reject Access ☒ Authenticate Locally

RADIUS Auth Protocol: PAP

RADIUS Auth Server Address:

RADIUS Auth Server Port:

RADIUS Shared Secret:

- **Functionality**

This feature allows users to configure RADIUS authentication protocol.

Pvalue	Description	Value Range	Default
28803	RADIUS Auth Protocol	Number: 0 – PAP 1 – CHAP 2 – MsCHAPv1 3 – MsCHAPv2	0 – PAP

FIRMWARE VERSION 1.0.1.2

PRODUCT NAME

HT841, HT881

DATE

09/04/2023

FIRMWARE FILE INFORMATION

- firmware file name: ht8x1fw.bin

MD5: a22de4261464c204dd4b6029c8fbb92d

ENHANCEMENT

- This is the initial release version of HT8X1 firmware.