PLANET
Networking & Communication

User’s Manual

720p SIP Vandalproof Door Phone with PoE

► **HDP-1160PT**

www.PLANET.com.tw

Copyright

Federal Communication Commission (FCC) Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

To assure continued compliance, use only shielded interface cables when connecting to computer or peripheral devices. Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1)

This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User's Manual of 720p SIP Vandalproof Door Phone with PoE

Model: HDP-1160PT

Rev: 1.00 (November, 2019)

Part No. EM-HDP-1160PT_v1.0

Table of Contents

Chapter 1. Product Introduction

1.1 Package Contents

The package should contain the following:

- 1 x HDP-1160PT
- 1 x Quick Installation Guide
- 1 x Mounting Label
- 1 x Screw Kit
- 1 x Connector
- 1 x Wrench
- 1 x Screw Driver

Note	If any of the above items are missing, please contact your seller immediately.

1.2 Overview

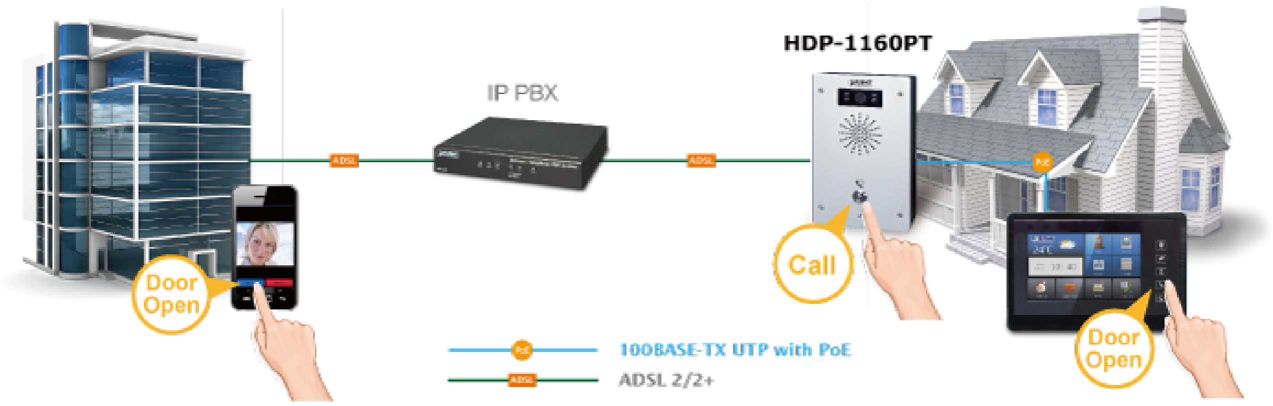
Security is Ensured with PLANET Video Door Phone

PLANET HDP-1160PT Vandalproof Video Door Phone is designed for homes and other purposes that need a visitor's identification for the sake of security. With its high-quality audio and video, the identification and voice of the visitor can be clearly seen and heard once the visitor press the call button of the door phone. The HDP-1160PT works like an intercom. As its name implies, it is vandalproof and has a video feature.

It supports the standard IETF SIP protocol and ONVIF protocol for easy operation and interfaces with the VoIP and IP surveillance world in an instant it connects you with. It delivers excellent picture quality in 720p HD resolutions with 112-degree wide angle. The door phone has infrared night vision that can capture any unusual activity in low light. It also supports HD voice and G.722 codec that relax bandwidth limitation and provide clear communications. It provides the flexibility and control required for high-quality visitor management, property protection, intercom, and message service.

Easy Communication via Intercom

The two-way intercom function provided by the HDP-1160PT allows you to see the visitors and also communicate with them. The HDP-1160PT includes 2 short-in detect port and 2 short-out control port for connecting with external devices such as door lock or door sensors. When the visitors press the call button at your door, you can press the unlock button on your mobile phone or PLANET VTS-700P 7-inch SIP Indoor Touch Screen PoE Video Intercom to open the door for your visitors.

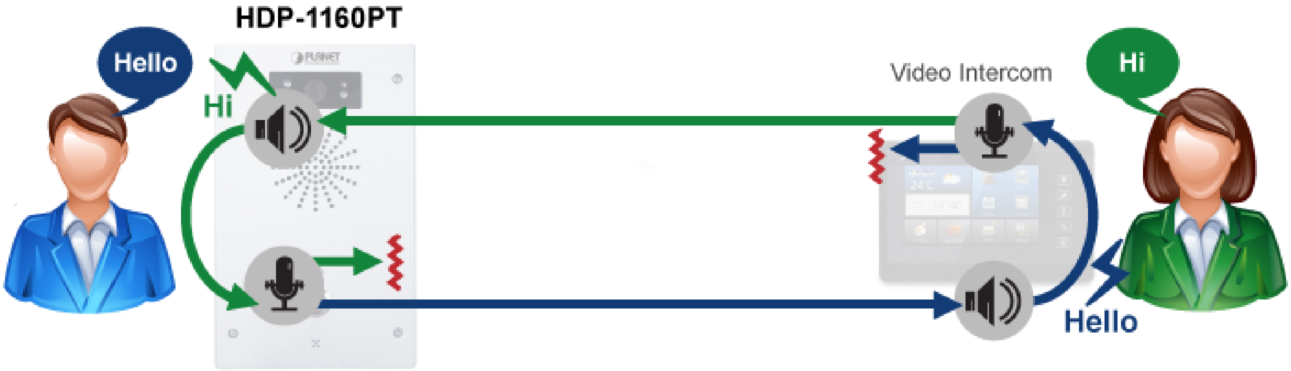


A Door Guard for Extreme Conditions

The HDP-1160PT is an extremely durable IP intercom that can withstand even the most demanding conditions. Its Industrial design with -40 to 70 degrees C operating temperature and resilience to dust, water (IP65) and vandalism (IK10) provides maximum security.

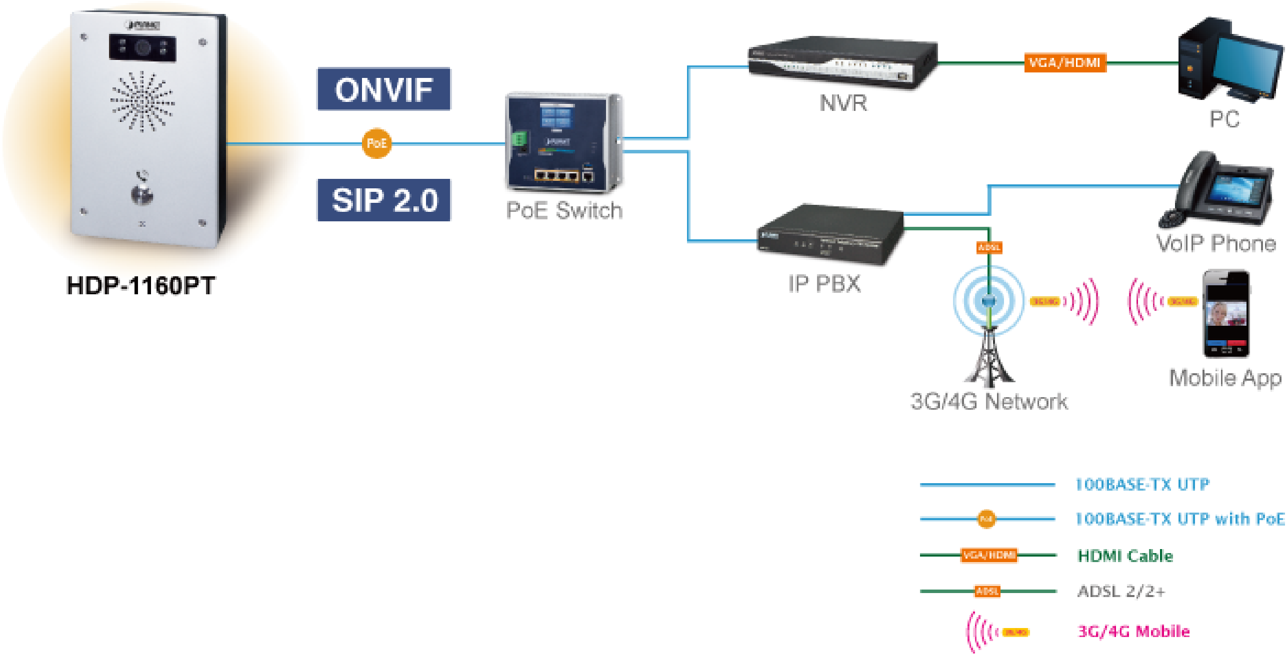
AEC (Acoustic Echo Cancellation)

Acoustic Echo Cancellation (AEC) technology is adopted in PLANET's HDP1160PT Door Phone and VTS-700P 7-inch SIP Indoor Touch Screen PoE Video Intercom to enable users to minimize the voice/sound signal distortion shown in the diagram below, thus guaranteeing the best-in-class sound quality.



Standard Protocol Compliance

The HDP-1160PT supports IETF Session Initiation Protocol 2.0 (RFC 3261) and ONVIF protocol for easy integration with general voice over IP system and video management system. The IP PBX/NVR device is able to broadly interoperate with equipment provided by VoIP/IP surveillance infrastructure providers, thus enabling them to provide their customers with better multimedia exchange services.


ONVIF
PoE
SIP 2.0
HDP-1160PT
PoE Switch
NVR
VGA/HDMI
PC
VoIP Phone
IP PBX
ADSL
3G/4G Network
Mobile App
100BASE-TX UTP
100BASE-TX UTP with PoE
HDMI Cable
ADSL 2/2+
3G/4G Mobile

1.3 Specifications

Product	HDP-1160PT
Video	
Image Device	2 megapixels with 1/2.7” color CMOS
Video Compression	H.264
Resolution	Main stream: 1280 × 720@25fps Sub stream: 704 × 576(D1)@25fps
Viewing Angle	112° (H), 84° (V)
Minimum Illumination	0.1lux with infrared illumination
IR Illuminations	IR LED x 2, effective up to 5 meters *The IR distance is based on the environment.
Audio	
Audio Streaming	Two-way audio
Microphone	Built-in microphone and speaker input
Narrowband Codec	G.711a/u, G.723.1, G.726-32K, G.729AB Wideband Codec: G.722
DTMF	In-band, Out of Band DTMF (RFC2833) and SIP INFO
Audio Output	Full-duplex Acoustic Echo Canceller (AEC) – a tail length of 96ms in hands-free mode
Audio Features	Voice Activity Detection (VAD) Comfort Noise Generation (CNG) Background Noise Estimation (BNE) Packet Loss Concealment (PLC) Dynamic Adaptive Litter Buffer up to 300ms
Protocol and Security	
Protocols	IETF SIP (RFC 3261 and companion RFCs), SIP2.0 over UDP/TCP/TLS, RTP/RTCP/SRTP, STUN, DHCP, LLDP, PPPoE, 802.1x, L2TP, OpenVPN, SNTP, FTP/TFTP, HTTP/HTTPS and TR-069
Security	Network access authority authentication: 802.1x Web Filter, Transport Layer Security (TLS) Secure Real-time Transport Protocol (SRTP) NAT traversal: STUN mode

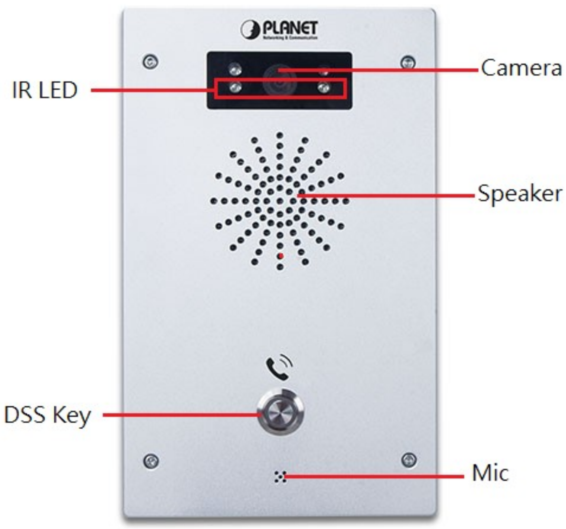
	HTTP/HTTPS web server, HTTPS certificate manager
Network and Provisioning	
Network Interface	1 x 10/100BASE-Tx RJ45 Ethernet interface, auto-MDIX
IP Configuration	Static/DHCP/PPPoE
VPN	L2TP / OpenVPN
Deployment/Maintenance	Auto-provisioning via FTP/TFTP/HTTP/HTTPS/DHCP OPT66/SIP PnP/TR-069 Web Management Portal Web-based Packet Dump Configuration Import and Export Firmware Upgrade Syslog
General	
Keypad	1 DSS button (speed dial button)
Power Requirements	Power over Ethernet (IEEE 802.3af/at), class 2 and DC12V/
Net Weight	1015g
Dimensions (W x D x H)	195 x 120 x 34 mm
Emission	CE, FCC
Connectors	1 10/100Mbps Ethernet, RJ45 1 audio output interface 1 recording output interface 2 short-circuit input interfaces 2 relays: Max. DC30V,1A; AC125V,0.5A 2 indoor magnetic switches 1 Tamperproof protection/alarm Active switching output: 12V/500mA DC (only 1 relay support)
Installation	Wall-mount type
External Power Supply	12V±15%/1A DC
Environments	
Storage Temperature	-40~70°C
Operating Humidity	10~90%

Chapter 2. Hardware Interface

2.1 Physical Descriptions

Product Dimensions (W x D x H)	195 x 120 x 34 mm
Net Weight	1015g

Front Panel



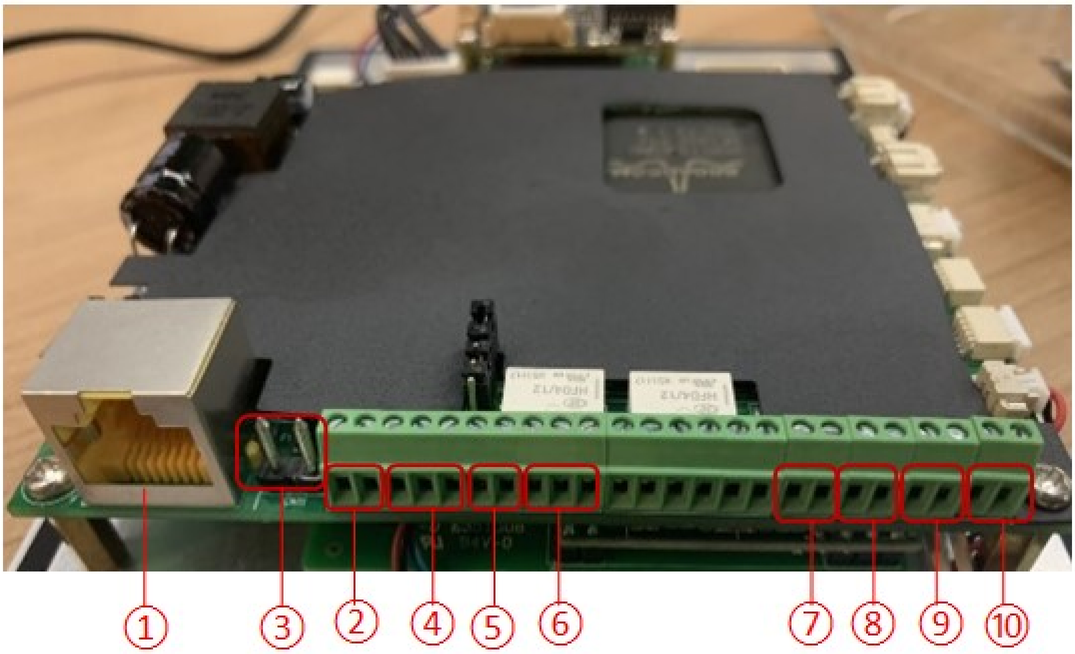
Number	Interface	Description
1	**Wall-mount Housing**	IP65 and IK10 outdoor housing for rigorous environment
2	**CMOS Sensor**	Video signal acquisition and transmission
3	**IR LED**	Emits infrared light to provide light source in dark places
3	**Speaker**	The door phone has a built-in speaker for convenient communication and alert use
4	**DSS Key (Speed dial button)**	For speed dial, multicast, intercom, IP broadcast and other functions
5	**Mic**	The door phone has a built-in microphone hidden in the pinhole located on the front panel

Function Key LED State

Type	LED	State
DSS Key (Speed dial button)	**Normally on**	Successfully registered
	Quick flashing	Registration failed/network abnormal
	Slow flashing	In call

Interface Description

Open the rear case of the device, there is a row of terminal blocks for connecting the power supply, electric lock control, etc. The connection is as follows:



Number	Description	Wiring port description (example above)
1	Ethernet interface: Standard RJ45 interface, 10/100M adaptive; it is recommended to use Cat 5e cable	-
2	Power interface: 12V,1A input	Left: positive (+) Right: grounded (-)
3, 5	Two groups of short-circuit input detection interfaces: For connecting switches, infrared probes, door magnets, vibration sensors and other input devices	Left: IN Right: OUT
4, 6	Two groups of short-circuit output control interface: Used to control electric locks, alarms, etc.	Left (NC): Normally Close Contact Center (COM): Common Contact

		Right (NO): Normally Open Contact
7, 8	Two groups of gate magnetic detection	Left: grounded Right: door magnetic input
9	Recording output interface: Mix the device and the sound of the far-end call. One is the recording signal line, and the other is the ground line. (Please be sure to ground the line, otherwise there will be noise)	Left: grounded Right: recording output
10	External active speaker interface: External active speakers for audio power amplification. One is the audio signal line, and the other is the ground line. (Please be sure to ground the line, otherwise there will be noise)	Left: grounded Right: external active speaker

Note	The HDP-1160PT requires either IEEE 802.3af/at PoE or DC power from the power connector.

Power Connector

The picture shows the two-pin connector that comes with system power source of 12V DC, 1A (maximum for the two-pin connector).

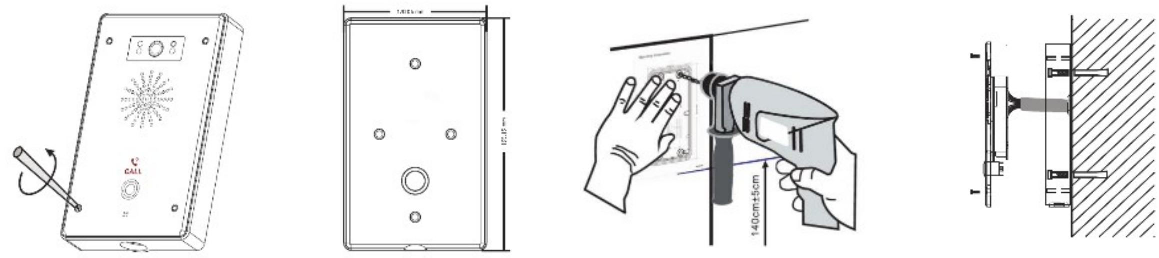
1	2
+12V DC	GND

Power Connector

2.2 Hardware Installation

Wall mounting steps:

A. Use the given screw tool to remove the cover.
B. Place the back cover on the wall and mark the four holes on the wall with a pencil.
C. Drill the marked four holes, place the back cover on the wall, and slightly hammer the plastic anchors through the four holes.
D. Get the power cord and network cable connected, and secure it tightly with the screws.



. A B C D

Wall Mounting Steps of HDP-1160PT

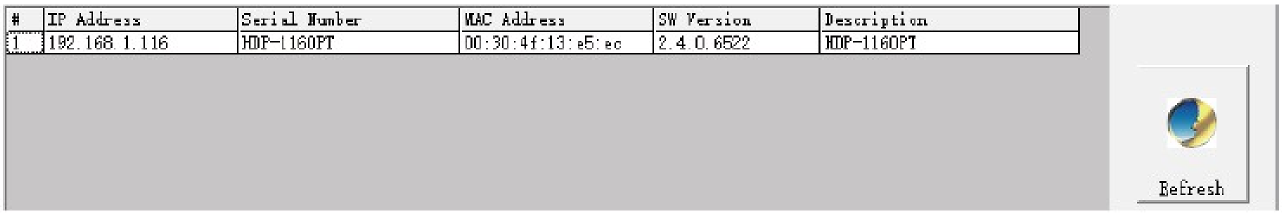
Caution	**While drilling or fixing the HDP-1160PT, hold it tight or else it may drop that may accidentally hurt the installer.**

2.3 Initial Utility Installation

There are two methods as shown below to search the HDP-1160P.

Method 1:

Open the Planet Door Phone Finder Utility. Press the **Refresh** button to search the HDP-1160PT and find the IP address.



Method 2:

Press and hold the DSS key for 10 seconds.When the speaker beeps rapidly, press the DSS key again quickly. When the beep stops, the intercom will report the IP address by voice.

Default Setting	
Default IP Address	**172.16.0.1**
Default Web Port	80
Default Login User Name	**admin**
Default Login Password	**123**
Report IP address	Hold the DSS key for 10 seconds to report IP address by voice
Searching Tools	Planet Door Phone Finder

Chapter 3. Web-based Management

Please take a few minutes to read through this guide to familiarize with the steps required to set up your door phone. This chapter provides setup details of the door phone Web-based Interface.

3.1 Introduction

When the device and your computer successfully connect to the network, enter the IP address of the device. You will see the Webpage management interface login screen. Enter the user name and password and click the button to enter the settings screen.

Door phone can be configured with your Web browser. Before configuring, please make sure your PC is in the same IP segment as the door phone.

3.2 Web Configuration

The login username and password are **admin** and **123**, respectively.

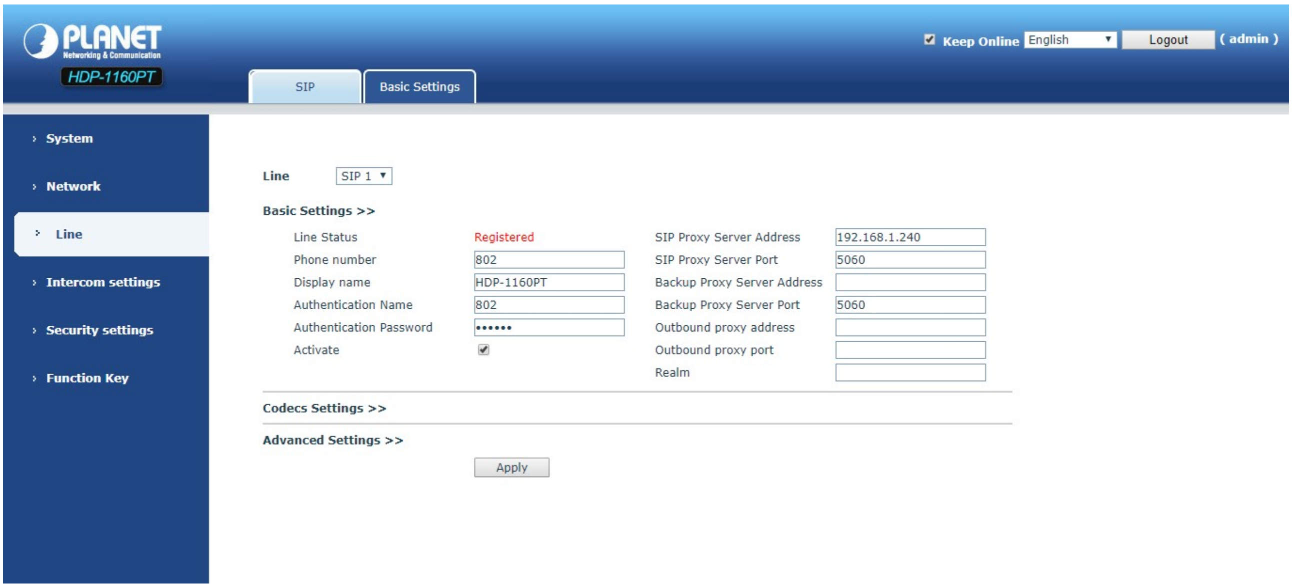
Enter "admin" for user name and "123" for password to access interface.

3.3 SIP Configuration

At least one SIP line should be configured properly to enable the telephony service. The line configuration is like a virtualized SIM card. Just like a SIM card on a mobile phone, it stores the service provider and the account information used for registration and authentication. When the device is applied with the configuration, it will register the device to the service provider with the server's address and user's authentication as stored in the configurations.

The SIP line configuration should be set via the Web configuration page by entering the correct information such as phone number, authentication name/password, SIP server address, server port, etc. which are provided by the SIP server administrator.

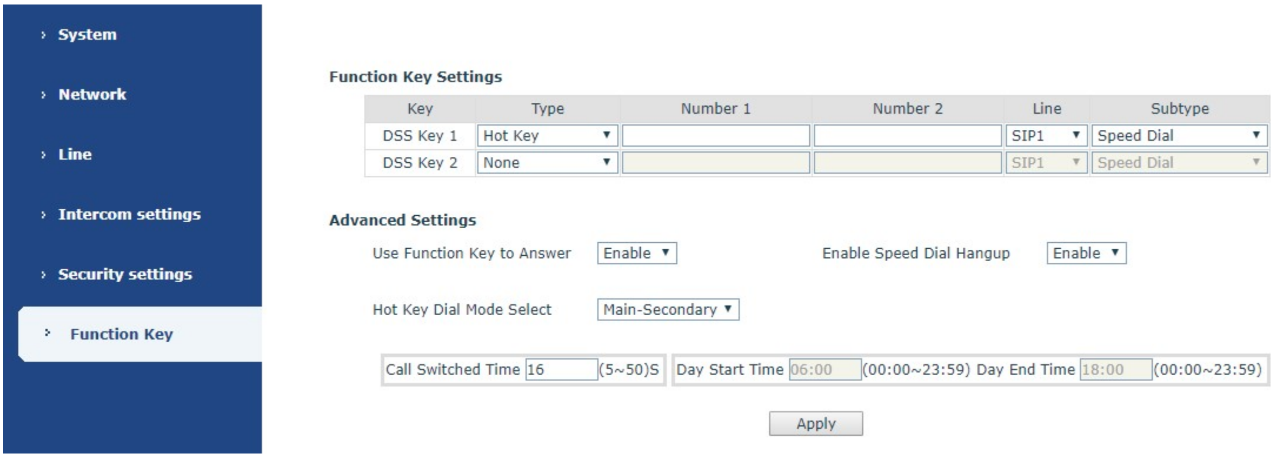
- Web interface: After logging into the phone page, enter **[Line**] >> [**SIP**] and select **SIP1/SIP2** for configuration, click apply to complete registration after configuration, as shown below:



Chapter 4. Basic Function

4.1 Making Calls

After setting the function key to “Hot Key” and the “Number”, press the function key to immediately call out the set number, as shown below:



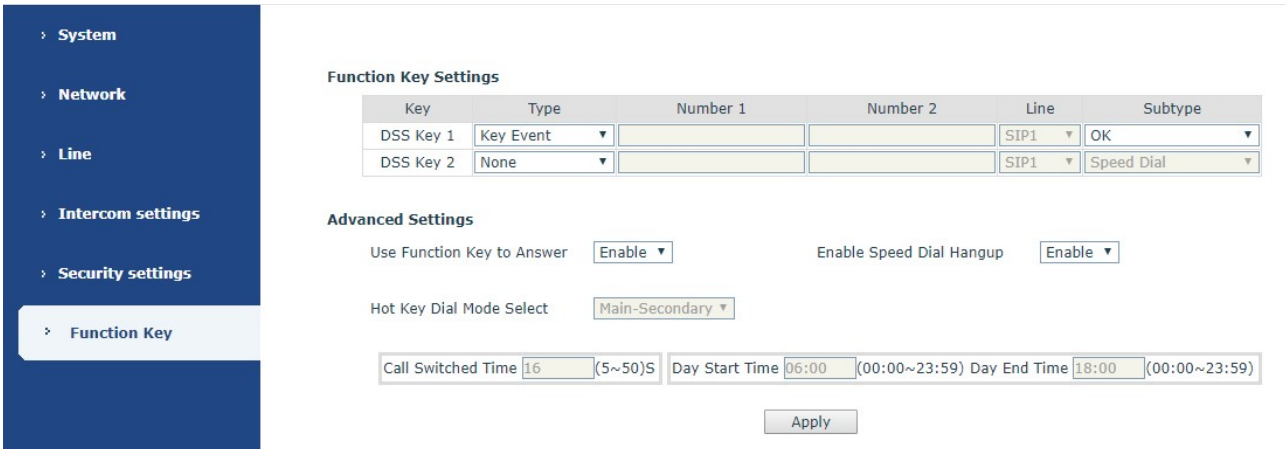
For more details on configuration, refer to **5.6 Function Key**.

4.2 Answering Calls

After setting up the automatic answer and the automatic answer time, you will hear the ringing bell within the set time and the call will be automatically answered after the timeout. When canceling automatic answering, the call will not be automatically answered after the timeout .

4.3 End of the Call

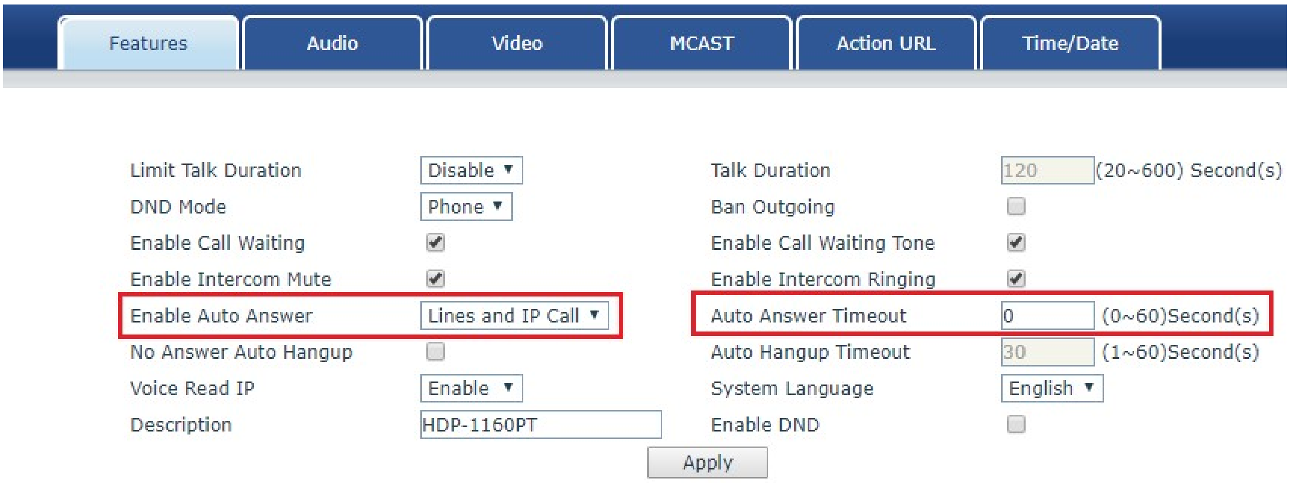
You can hang up the call through the Release key (you can set the function key as the Release key) or turn on the speed dial button to hang up the call. For more details on configuration, refer to **5.6 Function Key**.



4.4 Auto-Answering

The user can turn off the auto-answer function (enabled by default) on the device webpage, and the ring tone will be heard after the shutdown, and the auto-answer will not time out.

Web interface: enter **[Intercom Settings]** >> **[Features]**, Enable auto answer, set mode and auto answer time and click submit.



Auto-Answering	
Field Name	**Description**
Auto Answer Mode	
Disable	Turn off the automatic answer function; the call will not time out to answer automatically.
Line 1	Line 1 has an automatic call timeout.
Line 2	Line 2 has an automatic call timeout.
Line 1 & Line 2	Line 1 and line 2 have an automatic call timeout.
Lines and IP Call	Call will be automatically answered after the timeout.

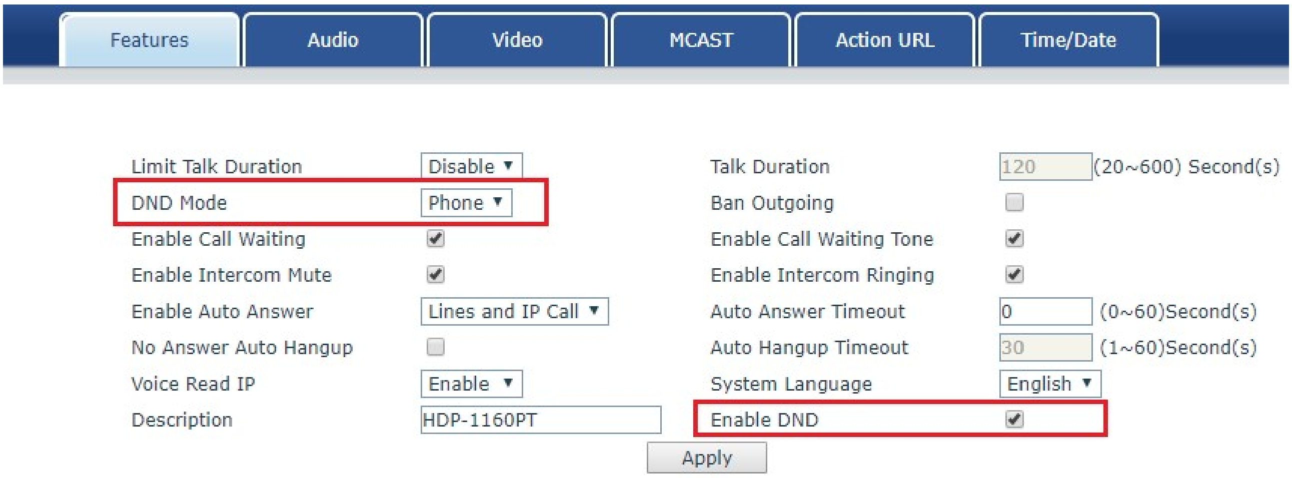
Auto-Answering	
Field Name	**Description**
Auto Answer Timeout (0~60)	
The range can be set to 0~ 60s and the call will be answered automatically when the timeout is set.	

4.5 DND

Users can turn on the do-not-disturb (DND) feature on the device's web page to reject incoming calls (including call waiting).Do not disturb can be set by the SIP line respectively on/off.

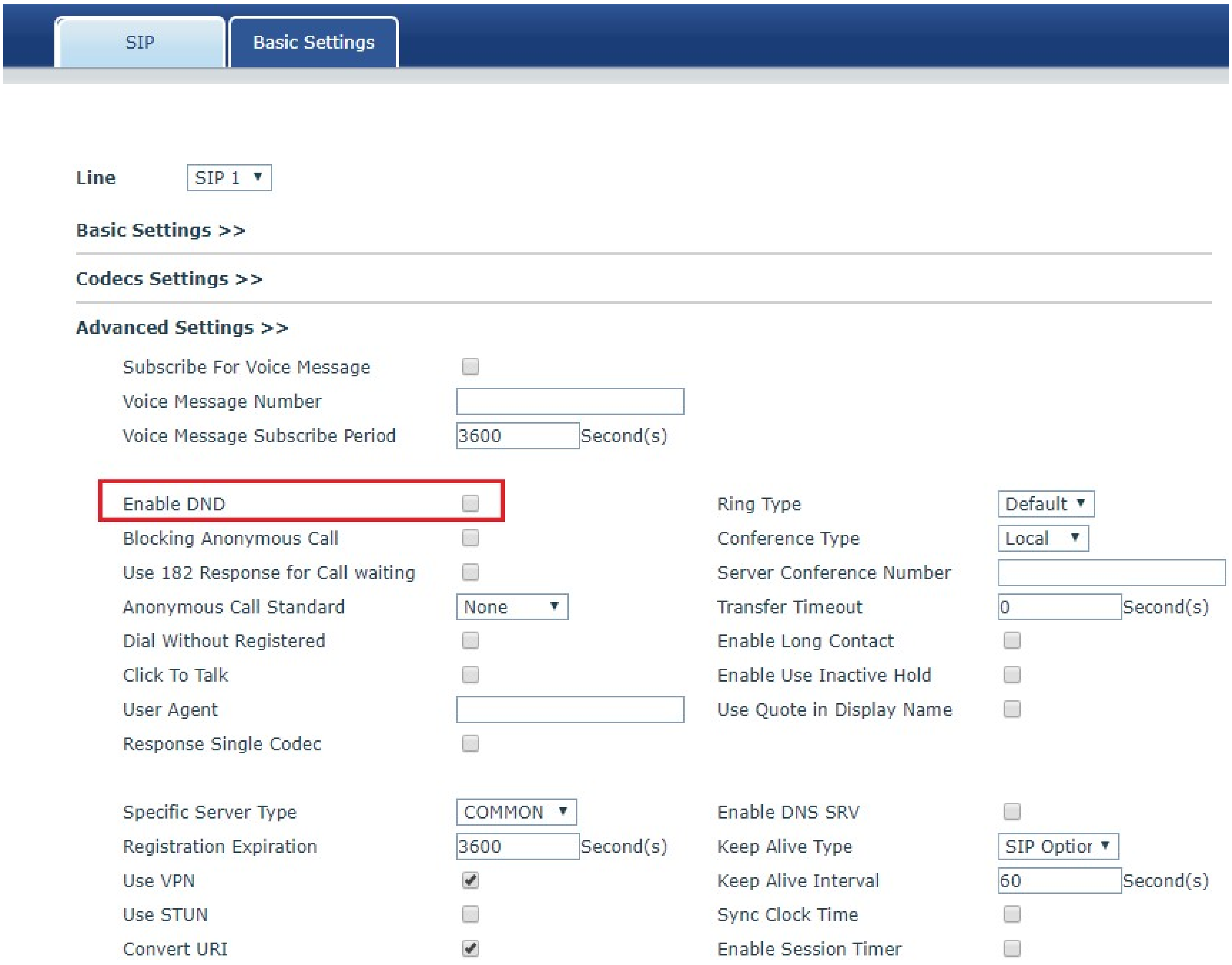
Turn on/off all lines of the device without interruption by the following methods:

- Web interface: enter [**Intercom Settings**] >> [**Features**], set the DND Mode to Phone and Enable DND.



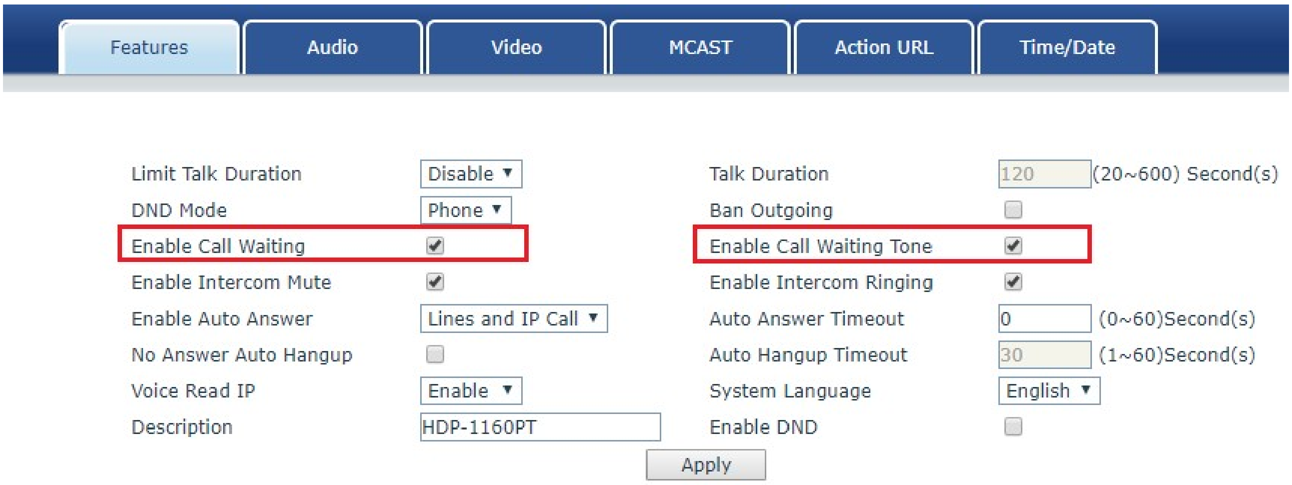
Turn on/off the interruption for the specific line of the device as follows:

- Web interface: enter [**Line**] >> [**SIP**], choose a Line and enter [**Line**] >> [**Advanced settings**], Enable DND.



4.6 Call Waiting

- Web interface: enter [**Intercom Settings**] >> [**Features**], enable/disable call waiting, enable/disable call waiting tone.



Call Waiting	
Field Name	**Description**
Enable Call Waiting	New calls can be accepted during a call.
Disable Call Waiting	New calls will be automatically rejected and a busy signal will be prompted.
Enable Call Waiting Tone	When you receive a new call on the line, the device will beep. Users can enable/disable call waiting in the device interface and the web interface.

Chapter 5. Advanced Function

5.1 System

5.1.1 Information

User can get the system information of the device in this page including,

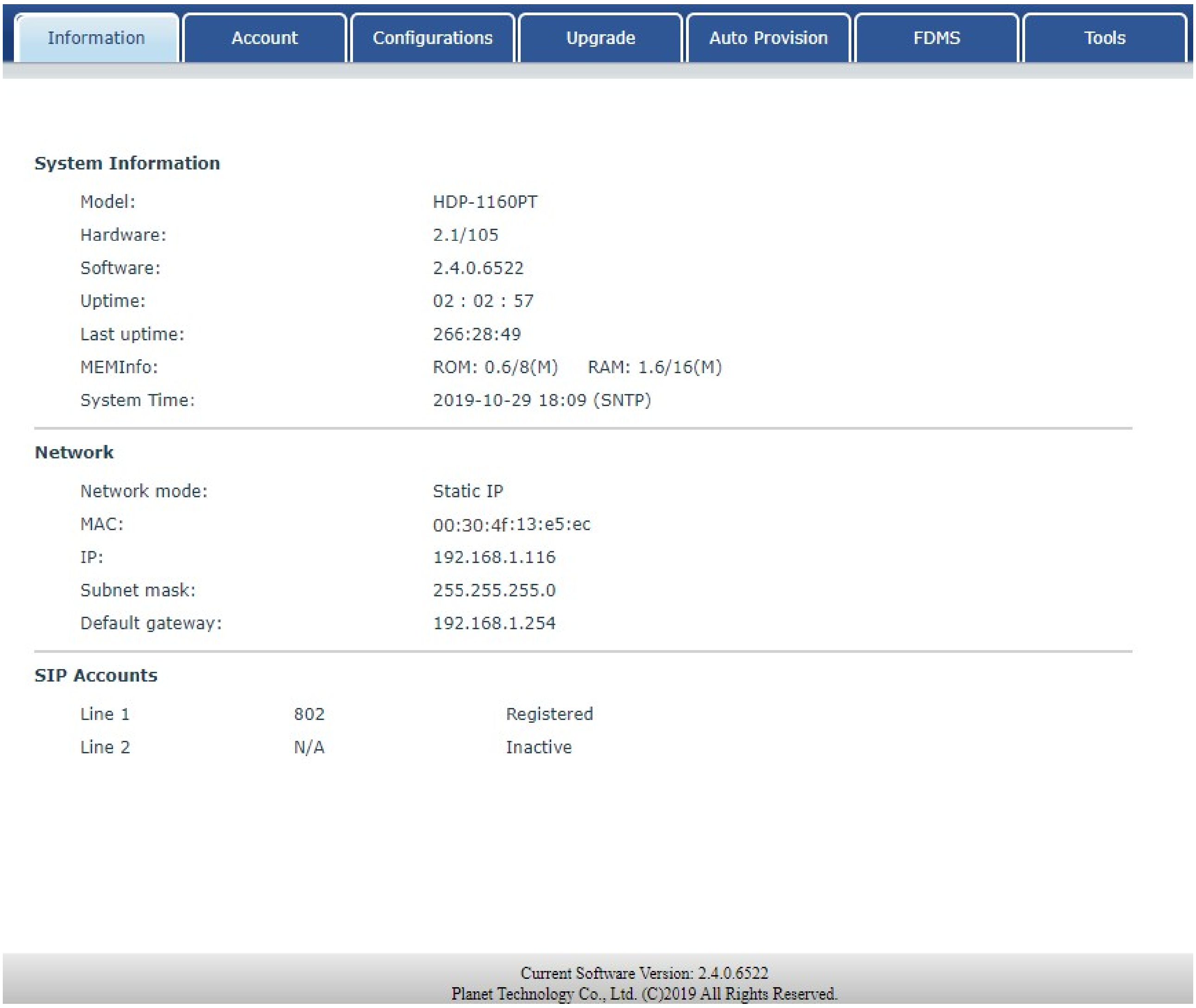
- Model
- Hardware Version
- Software Version
- Uptime
- Last uptime
- MEMinfo
- System Time

And summarization of network status,

- Network Mode
- MAC Address
- IP
- Subnet Mask
- Default Gateway

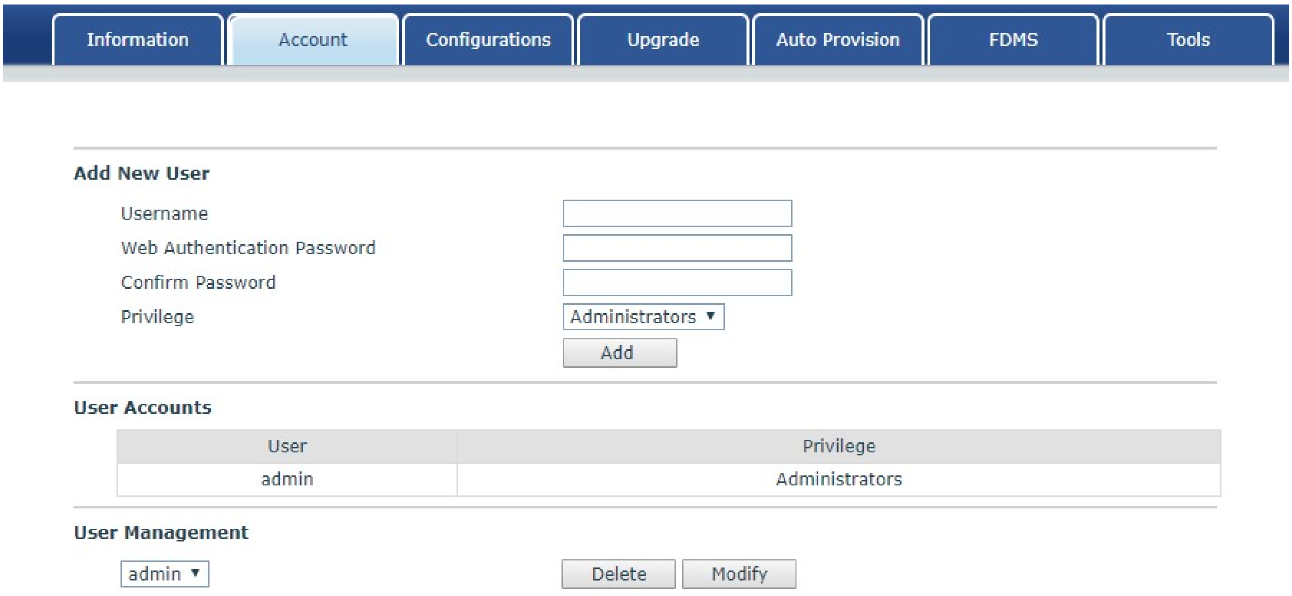
Besides, summarization of SIP account status,

- SIP User
- SIP account status (Registered / Unapplied / Trying / Timeout)



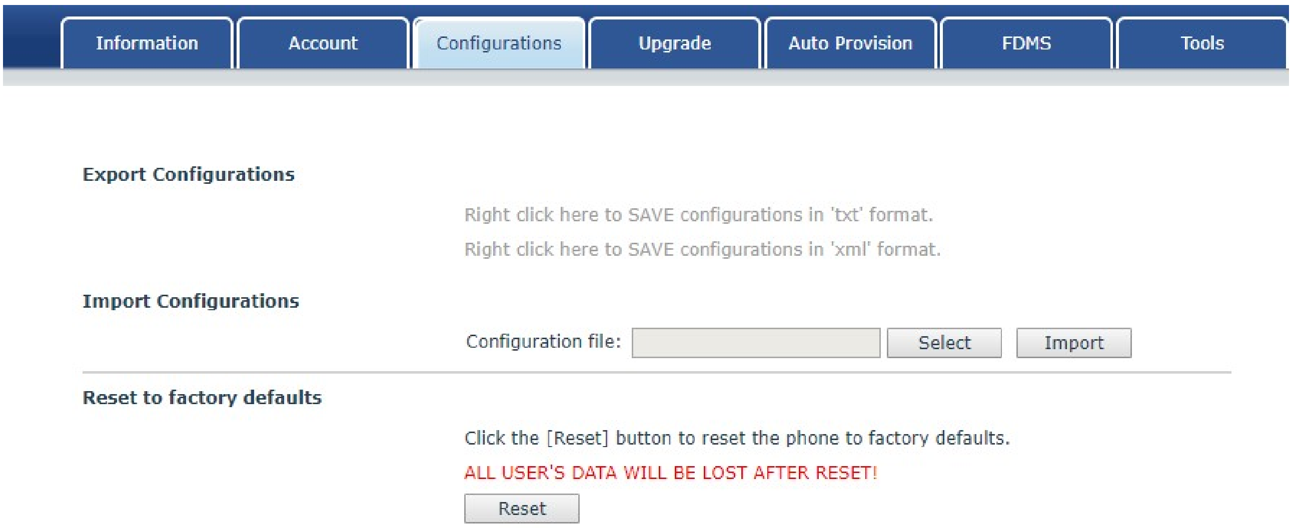
5.1.2 Account

On this page the user can change the password for the login page. Users with administrator rights can also add or delete users, manage users, and set permissions and passwords for new users.



5.1.3 Configurations

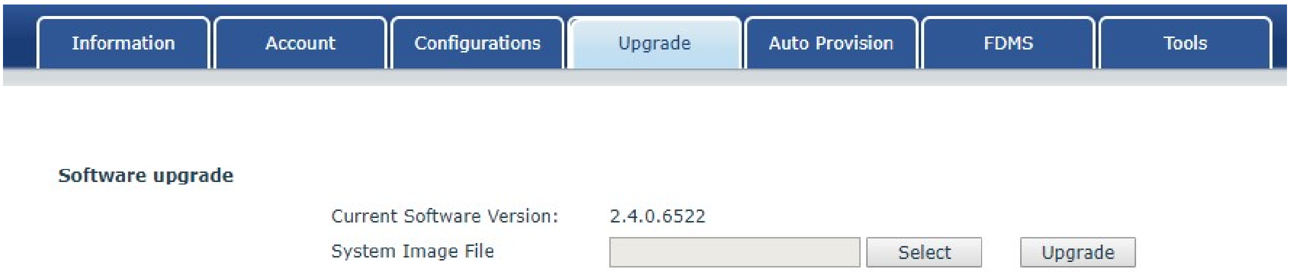
On this page, users with administrator privileges can view, export, or import the phone configuration, or restore the phone to factory settings.



Configurations	
Field Name	**Description**
Export Configurations	Right click to select target save as, that is, to download the device's configuration file, suffix ".txt". (note: profile export requires administrator privileges)
Import Configurations	The device will restart automatically after successful import, and the configuration will take effect after restart.
Reset Phone	The phone data will be cleared, including configuration and database tables.

5.1.4 Upgrade

Upgrade the software version of the device, and upgrade to the new version through the webpage. After the upgrade, the device will automatically restart and update to the new version. Click “Select”, select the version and then click “Upgrade”.

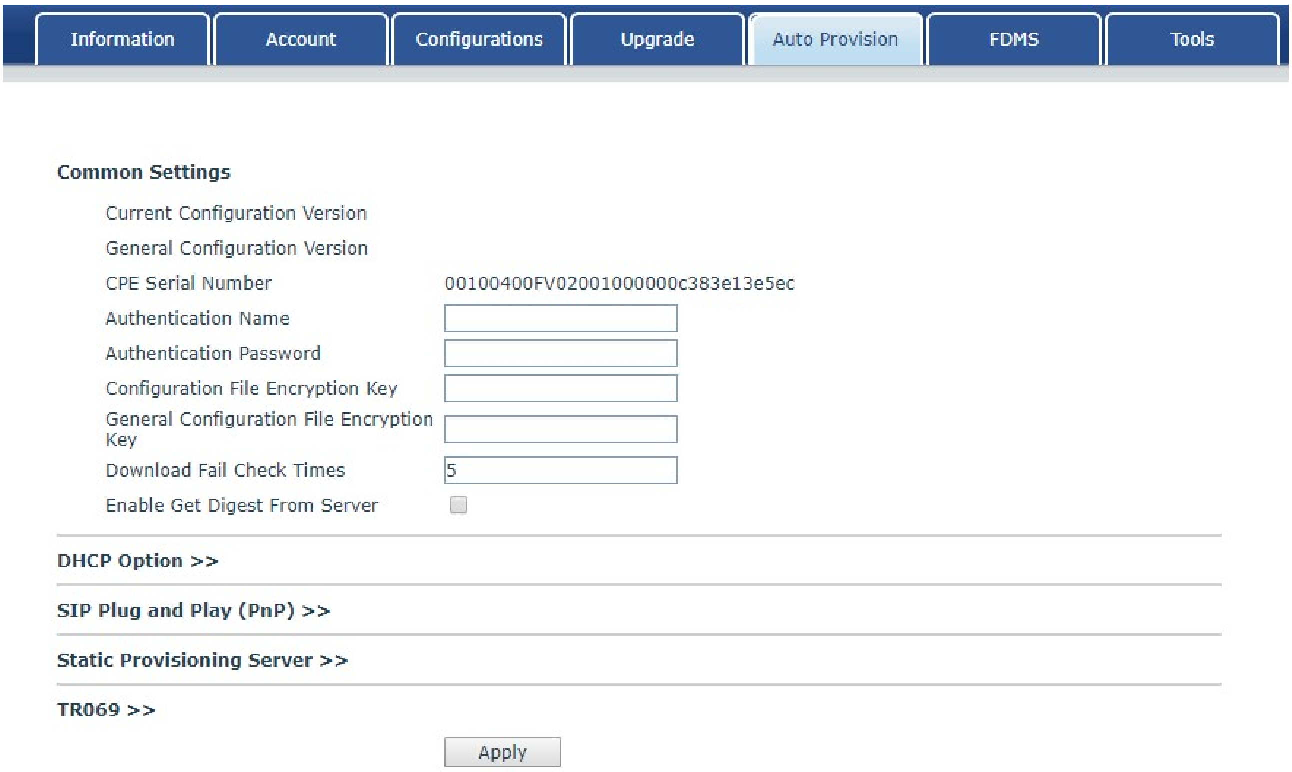


5.1.5 Auto Provision

The HDP-1160PT supports SIP PnP, DHCP options, static provision, and TR069. If all of the 4 methods are enabled, the priority from high to low is shown below:

PNP>DHCP>TR069> Static Provisioning

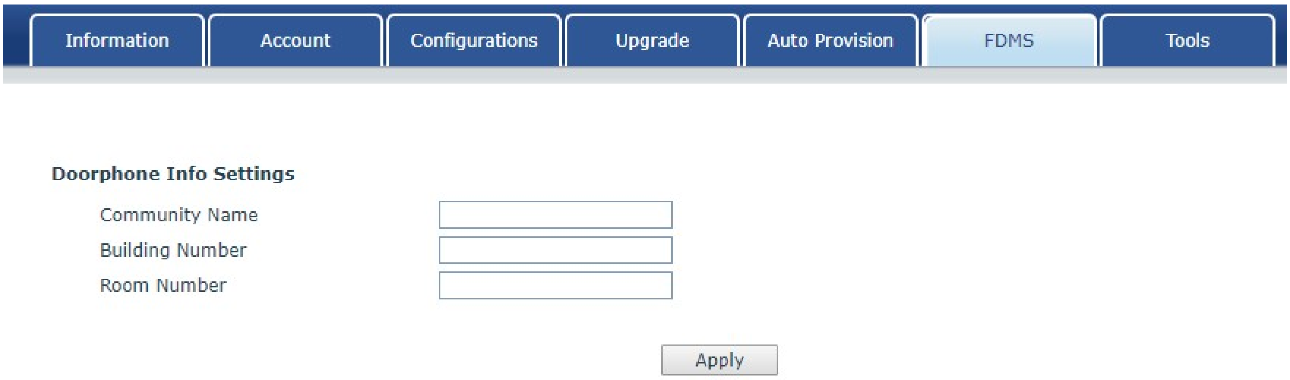
Transferring protocols: FTP, TFTP, HTTP and HTTPS



Auto Provision	
Field Name	**Description**
Common Settings	
Current Configuration Version	It will show the current config file's version. If the version of configuration downloaded is higher than this, the configuration will be upgraded. If the endpoints confirm the configuration by the Digest method, the configuration will not be upgraded unless it differs from the current configuration.
General Configuration Version	It will show the common config file's version. If the configuration downloaded and this configuration are the same, the auto provision will stop. If the endpoints confirm the configuration by the Digest method, the configuration will not be upgraded unless it differs from the current configuration.
CPE Serial Number	Serial number of the equipment.
Authentication Name	Username for configuration server. Used for FTP/HTTP/HTTPS. If this is blank the phone will use anonymous.
Authentication Password	Password for configuration server. Used for FTP/HTTP/HTTPS.
Configuration File Encryption Key	Encryption key for the configuration file.
General Configuration File Encryption Key	Encryption key for common configuration file.
Download Fail Check Times	The default value is 5. If the download configuration fails, it will be downloaded 5 times.
Enable Get Digest From Server	When the feature is enabled and the configuration of server is changed, phone will download and update.
DHCP Option Settings	
Option Value	The equipment supports configuration from Option 43, Option 66, or a Custom DHCP option. It may also be disabled.
Custom Option Value	Custom option number. Must be from 128 to 254.
Enable DHCP Option 120	Set the SIP server address through DHCP option 120.
SIP Plug and Play (PnP) Settings	
Enable PnP	If PnP is enabled, phone will send a SIP SUBSCRIBE message with broadcast method. Any server that supports the feature will respond and send a Notification with URL to phone. Phone gets the configuration file with the URL.

Auto Provision	
Field Name	**Description**
Server Address	Broadcast address. As default, it is 224.0.0.0.
Server port	PnP port.
Transporation Protocol	PnP protocol, TCP or UDP.
Update Interval	PnP message interval.
Static Provisioning Server	
Server Address	Set FTP/TFTP/HTTP server IP address for auto update. The address can be an IP address or Domain name with subdirectory.
Configuration File Name	If it is empty, phone will request the common file and device file is named as its MAC address. The file name could be a common name, $mac.cfg, $input.cfg. The file format supports CFG/TXT/XML.
Protocol Type	FTP, TFTP, HTTP and HTTPS
Update Interval	Configuration file updates interval time. As default it is 1, meaning phone will check the update every 1 hour.
Update Mode	Provision Mode 1. Disabled. 2. Update after reboot 3. Update after interval
TR069 Settings	
Enable TR069	Enable TR069 after selection
Enable TR069 Warning Tone	If TR069 is enabled, there will be a prompt tone when connecting.
ACS Server Type	There are 2 options -- common and CTC
ACS Server URL	ACS server address
ACS User	ACS server username (up to 59 characters)
ACS Password	ACS server password (up to 59 characters)
TLS Version	TLS 1.0/TLS 1.1/TLS 1.2 selections
Inform Sending Period	The default value is 3600 seconds.
STUN Server Address	Enter the STUN address
STUN Enable	Enable the STUN

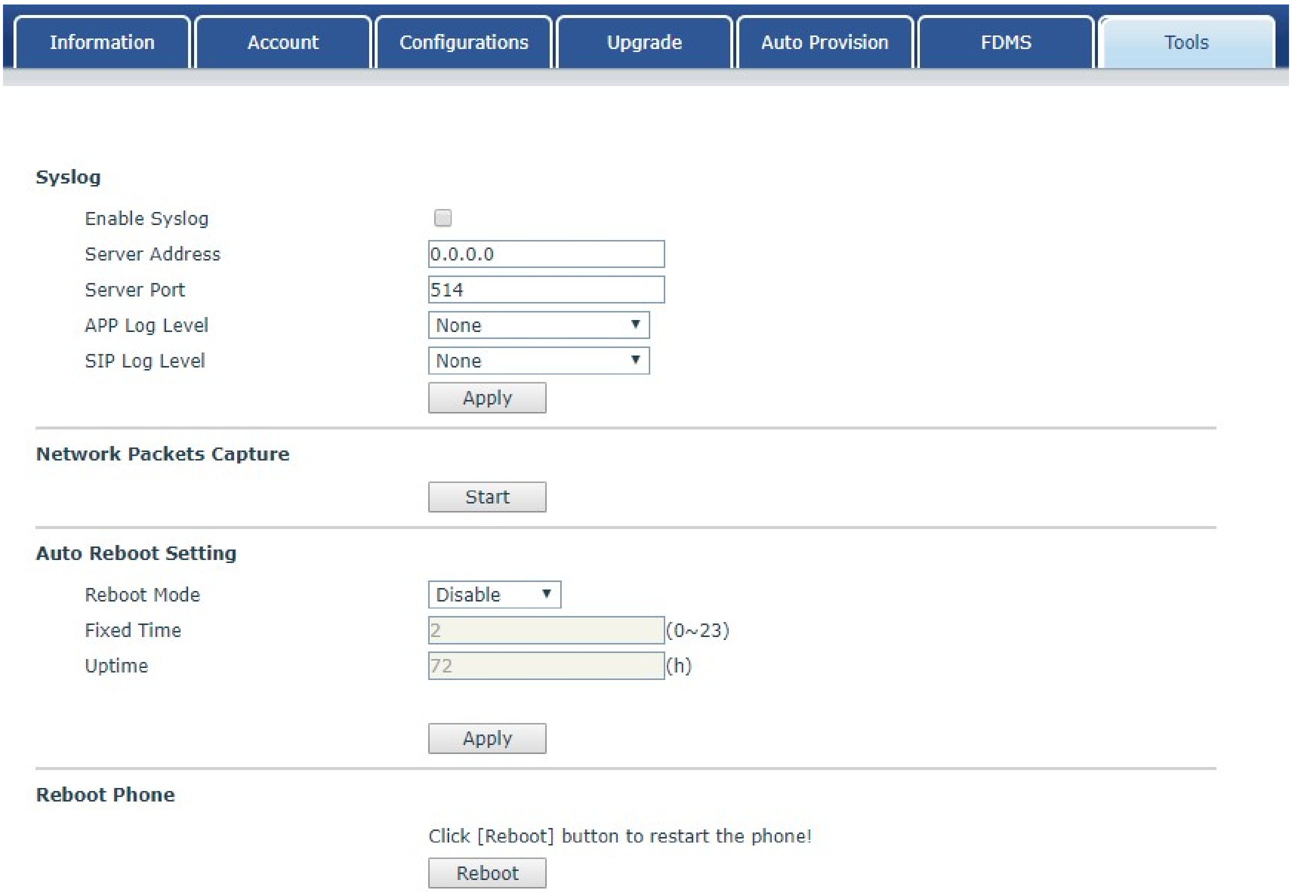
5.1.6 FDMS



FDMS	
Field Name	**Description**
Community Name	Name of equipment installation community.
Building Number	Name of equipment installation building.
Room Number	Equipment installation room name.

5.1.7 Tools

This page gives the user the tools to solve the problem.

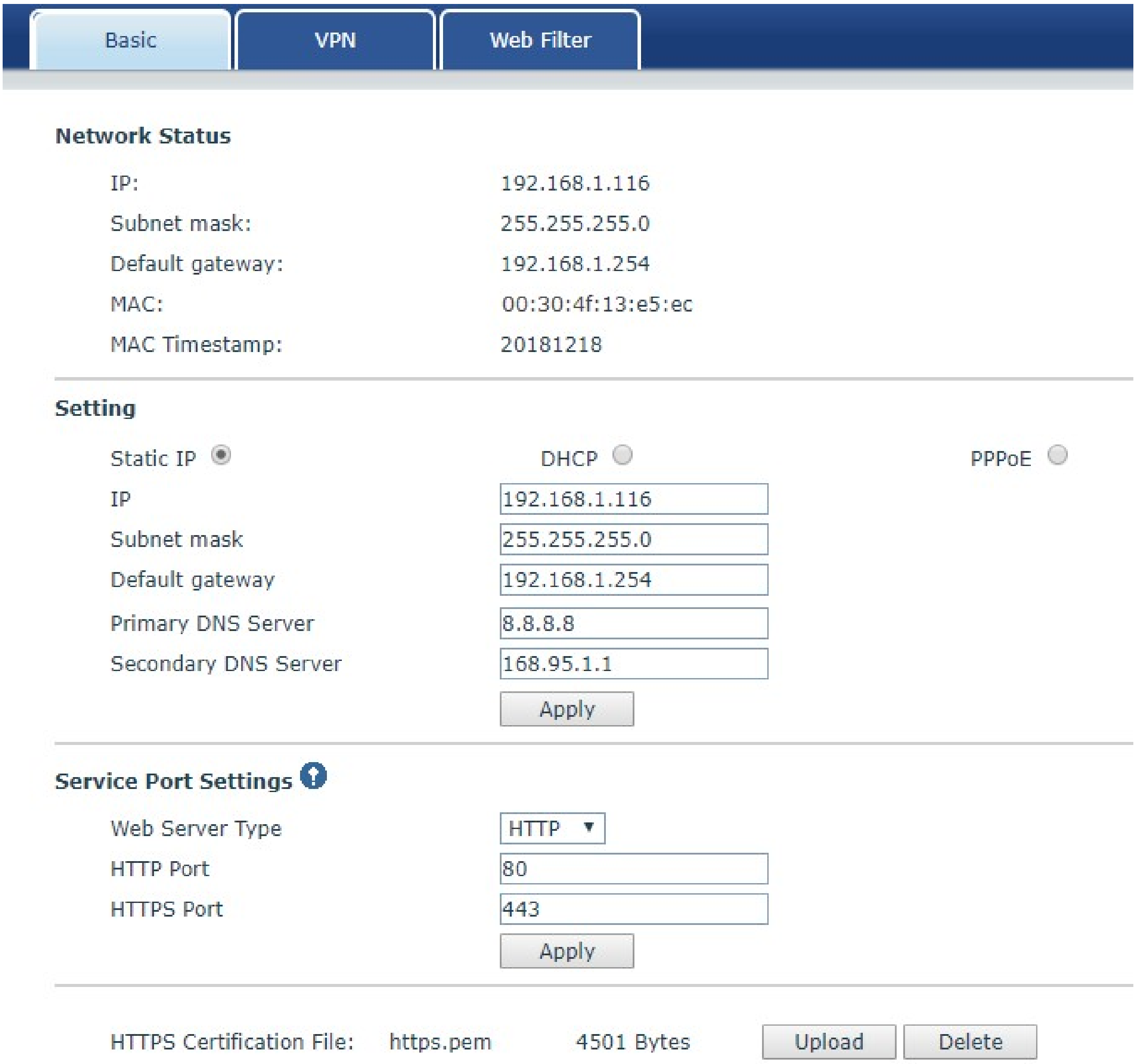


Tools	
Field Name	**Description**
Syslog	When enabled, set the syslog software address, and log information of the device will be recorded in the syslog software during operation. If there is any problem, log information can be analyzed by PLANET technical support.
Network Packets Capture	It generates a network packet file via start/stop automatically and the file can be analyzed by PLANET technical support.
Auto Reboot Setting	**Reboot Mode**: It will not restart at set time after disabled. **Fixed Time**: In the range of 0~24 (h), restart will be conducted at the setting point every day after the setting is completed. **Uptime**: Set the maximum length to 3 bits and restart at run time.
Reboot Phone	Restart the HDP-1160PT manually.

5.2 Network

5.2.1 Basic

This page allows users to configure network connection types and parameters.



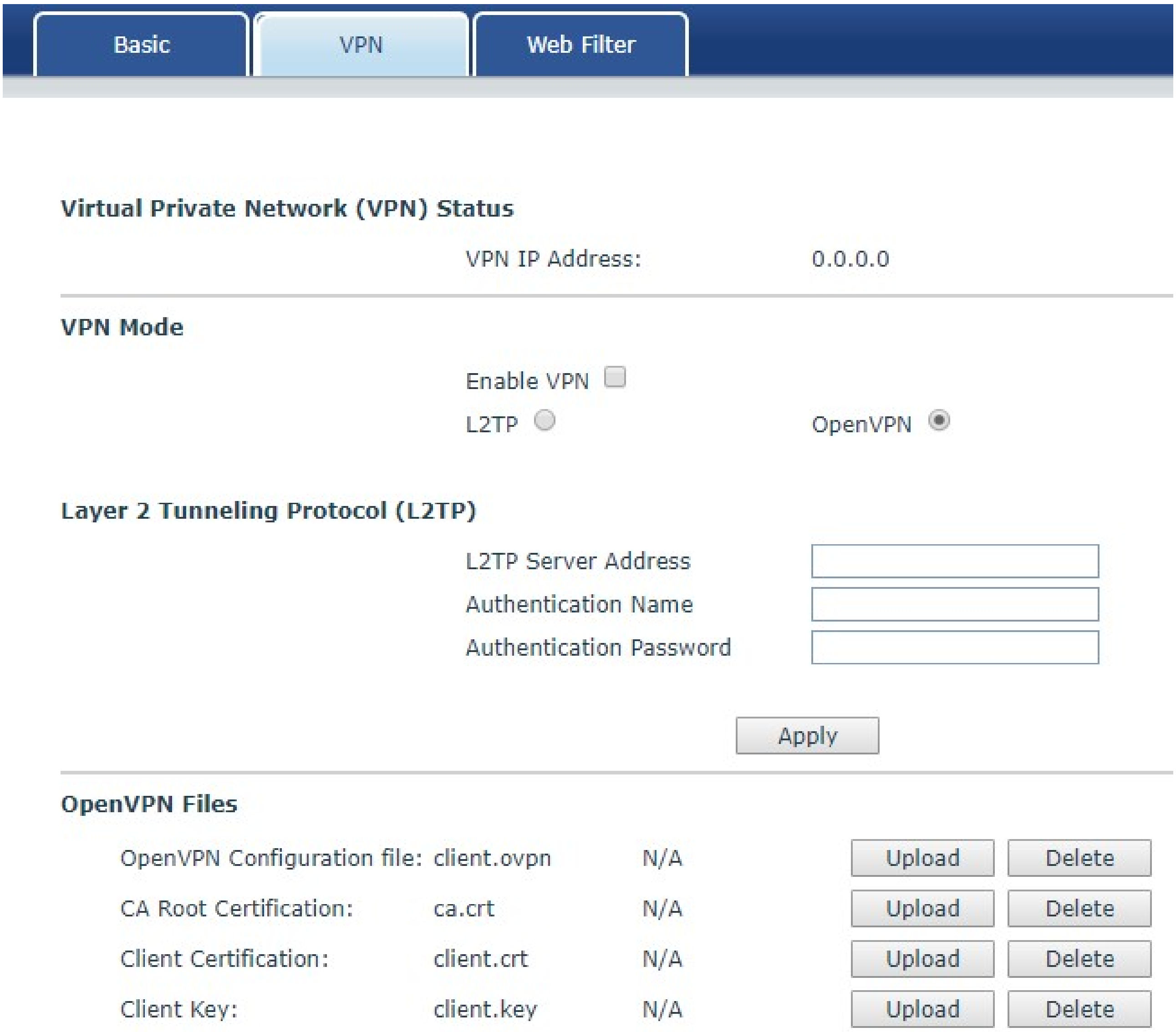
Basic	
Field Name	**Description**
Network Status	
IP	The current IP address of the equipment.
Subnet Mask	The current Subnet Mask.
Default Gateway	The current Gateway IP address.
MAC	The MAC address of the equipment.
MAC Time Stamp	Get the MAC address of time.

Basic	
Field Name	**Description**
Settings	
Select the appropriate network mode. The equipment supports three network modes:	
Static IP	Network parameters must be entered manually and will not change. All parameters are provided by the ISP.
DHCP	Network parameters are provided automatically by a DHCP server.
PPPoE	Account and Password must be input manually. These are provided by your ISP.
If DHCP is chosen, the screen below will appear. Enter values provided by the ISP.	
DNS Server Configured by	Select the Configured mode of the DNS Server.
Primary DNS Server	Enter the server address of the Primary DNS.
Secondary DNS Server	Enter the server address of the Secondary DNS.
Attention： 1）After setting the parameters, click【submit】to take effect. 2）If you change the IP operation, the web page will no longer respond, at this time should be entered in the address bar the new IP to connect to the device. 3）If the system uses DHCP to obtain IP at startup, and the network address of the DHCP Server is the same as the network address of the system LAN, then after the system obtains the DHCP IP, it will add 1 to the last bit of the network address of LAN and modify the IP address segment of the DHCP Server of LAN. If the DHCP access is reconnected to the WAN after the system is started, and the network address assigned by the DHCP server is the same as that of the LAN, then the WAN will not be able to obtain IP access to the network.	
Service Port Settings	
Web Server Type	Specify Web Server Type – HTTP or HTTPS
HTTP Port	Port for web browser access -- Default value is 80. To enhance security, change this from the default. Setting this port to 0 will disable HTTP.
HTTPS Port	Port for HTTPS access -- Before using https, an https authentication certification must be downloaded into the equipment. Default value is 443. To enhance security, change this from the default.

5.2.2 VPN

Virtual Private Network (VPN) is a technology to allow device to create a tunneling connection to a server and becomes part of the server's network. The network transmission of the device may be routed through the VPN server.

For some users, especially enterprise users, a VPN connection might be required to be established before activating a line registration. The device supports two VPN modes, Layer 2 Transportation Protocol (L2TP) and OpenVPN. The VPN connection must be configured and started (or stopped) from the device web portal.



■ **L2TP**

To establish a L2TP connection, users should log in to the device web portal, open webpage [**Network**] >> [**VPN**]. In VPN Mode, check the "Enable VPN" option and select "L2TP", then fill in the L2TP server address, Authentication Username, and Authentication Password in the L2TP section. Press "Apply" then the device will try to connect to the L2TP server.

When the VPN connection is established, the VPN IP Address should be displayed in the VPN status. There may be some delay of the connection establishment. User may need to refresh the page to update the status. Once the VPN is configured, the device will try to connect with the VPN automatically when the device boots up every time until user disables it. Sometimes, if the VPN connection does not establish immediately, user may try to reboot the device and check if VPN connection is established after rebooting.

Note	The device only supports non-encrypted basic authentication and non-encrypted data tunneling. For users who need data encryption, please use OpenVPN instead.

- **OpenVPN**

To establish an OpenVPN connection, user should get the following authentication and configuration files from the OpenVPN hosting provider and name them as follows:

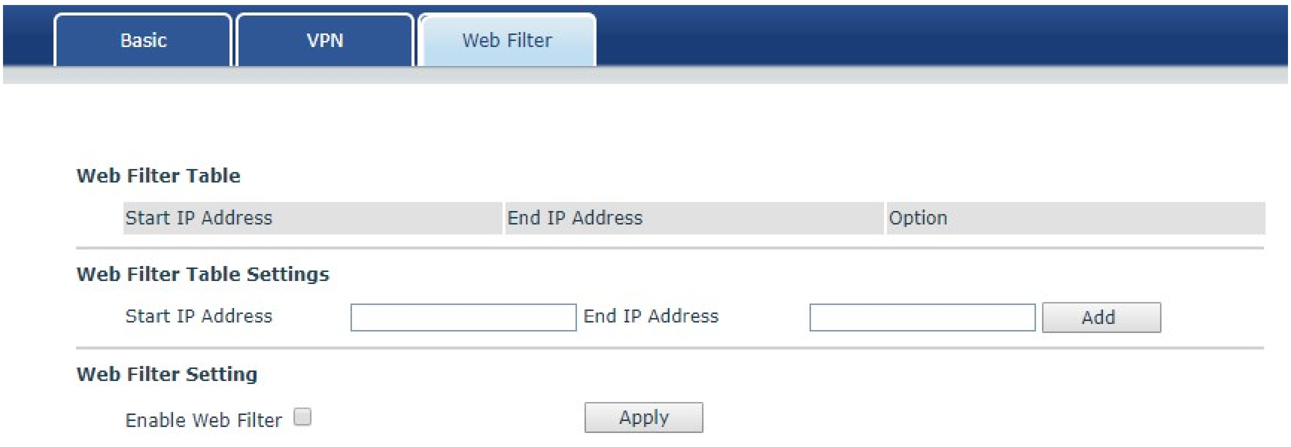
OpenVPN Configuration file:	client.ovpn
CA Root Certification:	ca.crt
Client Certification:	client.crt
Client Key:	client.key

User can upload these files to the device in the web page [Network] >> [VPN], select OpenVPN Files. Then user should check “Enable VPN” and select “OpenVPN” in VPN Mode and click “Apply” to enable OpenVPN connection.

Like L2TP connection, the connection will be established every time when system is rebooted until user disables it manually.

5.2.3 Web Filter

A user can set up a configuration management device that allows only machines with a certain network segment IP to access the configuration management device.



Web Filter Table

Start IP Address	End IP Address	Option
172.16.1.50	172.16.1.60	Modify Delete

Add and remove IP segments that are accessible; configure the starting IP address within the start IP, end the IP address within the end IP, and click [**Add**] to submit to take effect. A large network segment can be set, or it can be divided into several network segments to add. When deleting, select the initial IP of the network segment to be deleted from the drop-down menu, and then click [**Delete**] to take effect.

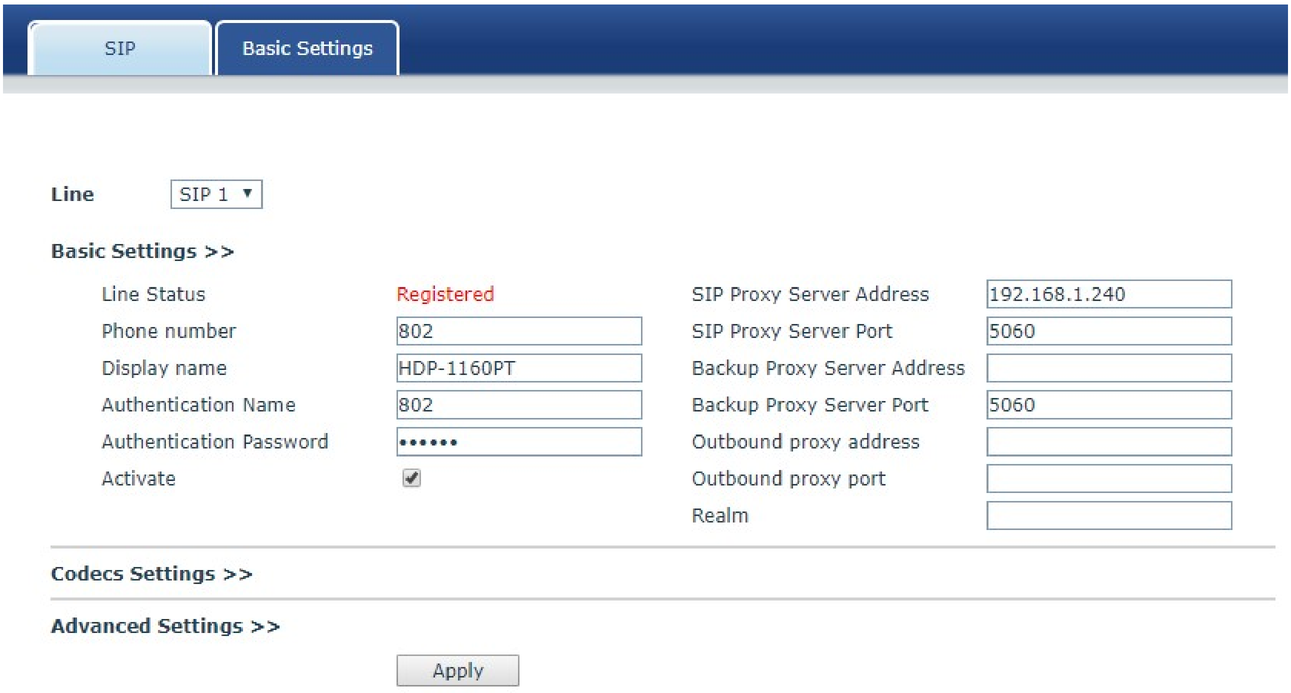
Enable web page filtering: Configure enable/disable web page access filtering. Click the "apply" button to take effect.

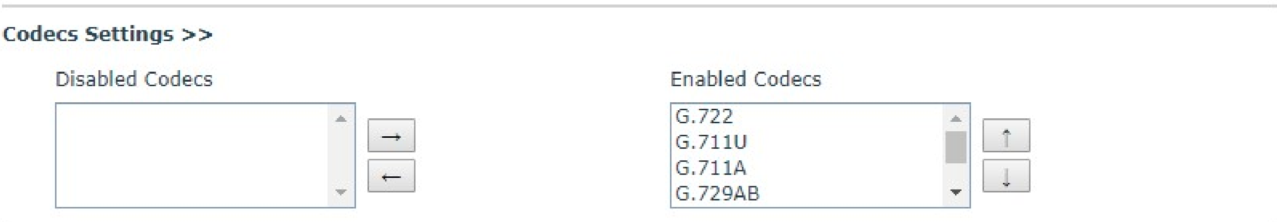
Note	If the device you are accessing is in the same network segment as the phone, please do not configure the filter segment of the web page to be outside your own network segment, otherwise you will not be able to log in the web page.

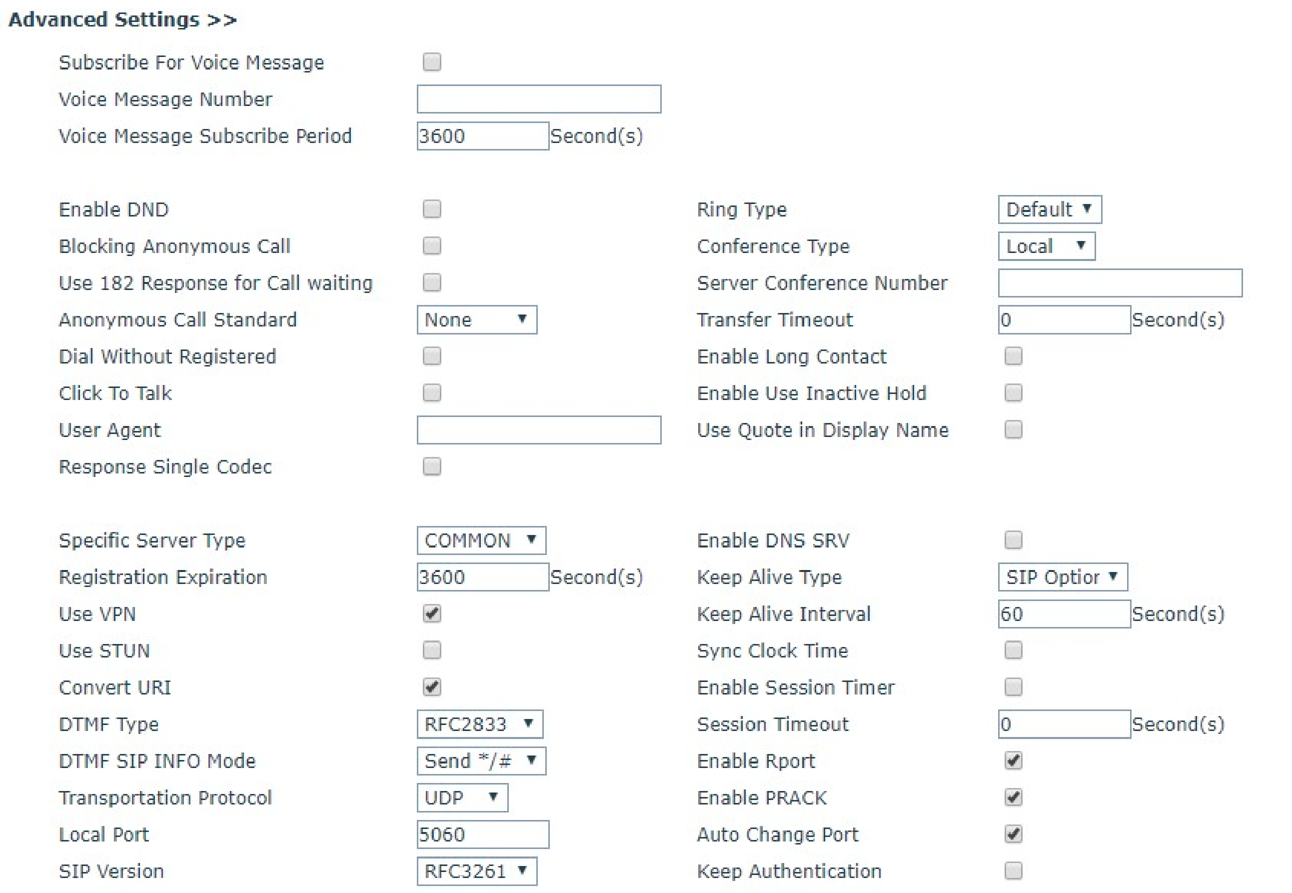
5.3 Line

5.3.1 SIP

Configure the service configuration for the wire on this page.







SIP	
Field Name	**Description**
Basic Settings (Choose the SIP line to be configured)	
Line Status	Display the current line status at page loading. To get the up to date line status, user has to refresh the page manually.
Username	Enter the username of the service account.
Display Name	Enter the display name to be sent in a call request.
Authentication Name	Enter the authentication name of the service account.
Authentication Password	Enter the authentication password of the service account.
Activate	Whether the service of the line should be activated.
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server.
SIP Proxy Server Port	Enter the SIP proxy server port; default is 5060.
Outbound Proxy Address	Enter the IP or FQDN address of outbound proxy server provided by the service provider.
Outbound Proxy Port	Enter the outbound proxy port; default is 5060.
Realm	Enter the SIP domain if requested by the service provider.
Codecs Settings	
Set the priority and availability of the codecs by adding or removing them from the list.	

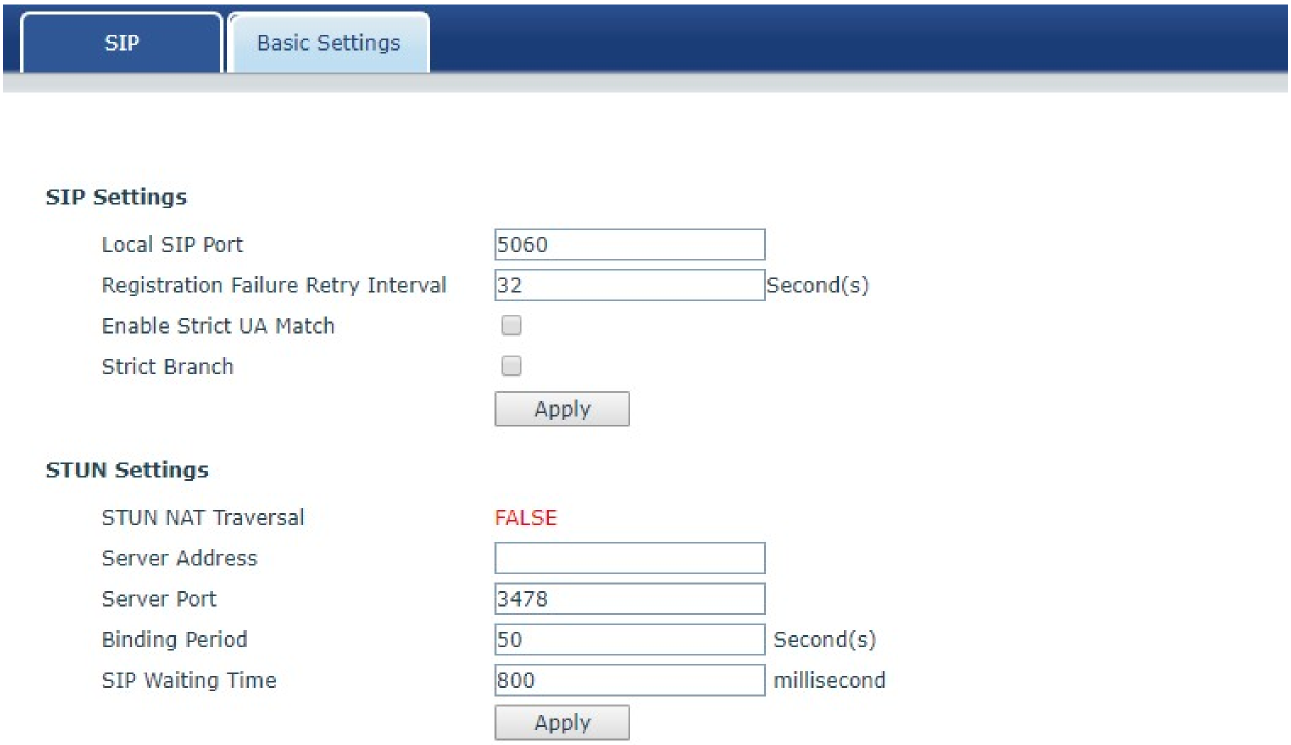
SIP	
Field Name	**Description**
Advanced Settings	
Subscribe For Voice Message	Enable the device to subscribe a voice message waiting notification; if enabled, the device will receive notification from the server if there is voice message waiting on the server.
Voice Message Number	Set the number for retrieving voice message.
Voice Message Subscribe Period	Set the interval of voice message notification subscription.
Enable DND	Any incoming call to this line will be rejected automatically.
Blocking Anonymous Call	Reject any incoming call without presenting caller ID.
Use 182 Response for Call waiting	Set the device to use 182 response code at call waiting response.
Anonymous Call Standard	Set the standard to be used for anonymous.
Dial without Registration	Set call out by proxy without registration.
Click To Talk	Set Click To Talk.
User Agent	The user agent is set by default
Response Single Codec	If setting enabled, the device will use single codec in response to an incoming call request.
Ring Type	Set the ring tone type for the line.
Conference Type	Set the type of call conference, Local=set up call conference by the device itself, maximum supports two remote parties, Server=set up call conference by dialing to a conference room on the server.
Server Conference Number	Set the conference room number when conference type is set to be Server.
Transfer Timeout	Set the timeout of call transfer process.
Enable Long Contact	Allow more parameters in contact field per RFC 3840.
Enable the Inactive Hold	Active capture package SDP is inactive, while the hold is sendrecv. Active capture package has no response of 400, etc. Hold the hair inactive After closing the grab packet, you can see that the DSP is sendonly and the hold is sendrecv.
Use Quote in Display Name	Whether to add quote in display name.
Specific Server Type	Set the line to collaborate with specific server type.
Registration Expiration	Set the SIP expiration interval.
Use VPN	Set the line to use VPN restrict route.
Use STUN	Set the line to use STUN for NAT traversal.
Convert URI	Convert not digit and alphabet characters to %hh hex code.
DTMF Type	Set the DTMF sending mode; there are four types:

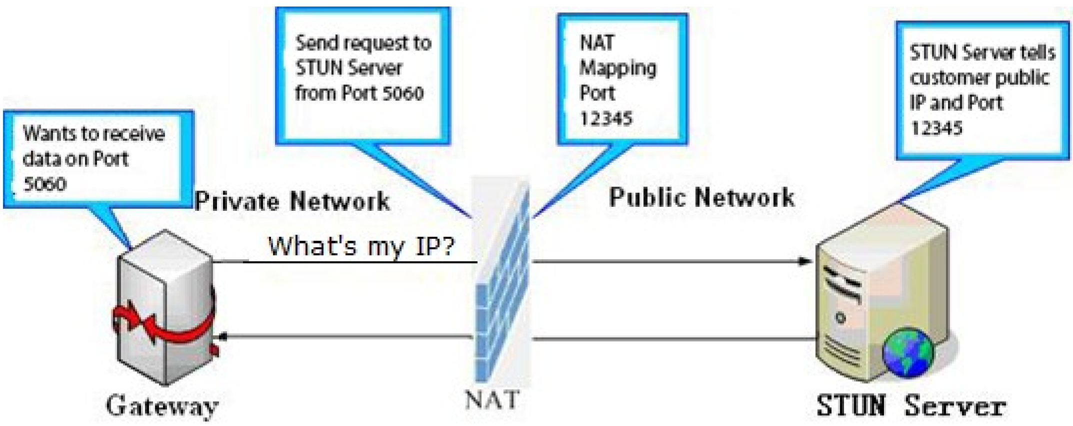
SIP	
Field Name	**Description**
	In-band RFC2833 SIP_INFO AUTO Different service providers may offer different models
DTMF SIP INFO Mode	When the device's DTMF type is set to SIP_INFO The DTMF_SIP_INFO type is configured to send */#, and when the device presses the */# key, the actual value sent is */#; Configured to send 10/11, when the device presses the */# key, the actual value sent is 10/11.
Transportation Protocol	Set the line to use TCP or UDP for SIP transmission.
Local Port	Set the Local Port.
SIP Version	Set the SIP version.
Caller ID Header	Set the Caller ID Header.
Enable Strict Proxy	Enables the use of strict routing. When the phone receives packets from the server, it will use the source IP address, not the address in via field.
Enable user=phone	Sets user=phone in SIP messages.
Enable SCA	Enable/Disable SCA (Shared Call Appearance).
Enable DNS SRV	Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list.
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole opened.
Keep Alive Interval	Set the keep alive packet transmitting interval.
Enable Session Timer	Set the line to enable call ending by session timer refreshment. The call session will be ended if there is not new session timer event update received after the timeout period.
Session Timeout	Set the session timer timeout period.
Enable Rport	Set the line to add rport in SIP headers.
Enable PRACK	Set the line to support PRACK SIP message.
Enable DNS SRV	Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list.
Auto Change Port	Enable/Disable Auto Change Port.
Keep Authentication	Keep the authentication parameters from previous authentication.
Auto TCP	Using TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes.
Enable GRUU	Support Globally Routable User-Agent URI (GRUU).

SIP	
Field Name	**Description**
RTP Encryption	Set the pass phrase for RTP encryption.
With Mac field	When enabled, all SIP messages strip Mac fields.
Register with the Mac field	When enabled, register the message ribbon Mac field.

5.3.2 Basic Settings

A STUN server allows a phone in a private network to know its public IP and port as well as the type of NAT being used. The equipment can then use this information to register itself to a SIP server so that it can make and receive calls while in a private network.





Basic Settings	
Field Name	**Description**
SIP Settings	
Local SIP Port	Set the local SIP port used to send/receive SIP messages.
Registration Failure Retry Interval	Set the retry interval of SIP REGISTRATION when registration failed.
Enable Strict UA Match	Enable or disable Strict UA Match.
STUN Settings	
Server Address	STUN Server IP address.
Server Port	STUN Server Port – Default is 3478.
Binding Period	STUN blinding period – STUN packets are sent at this interval to keep the NAT mapping active.
SIP Waiting Time	Waiting time for SIP. This will vary depending on the network.

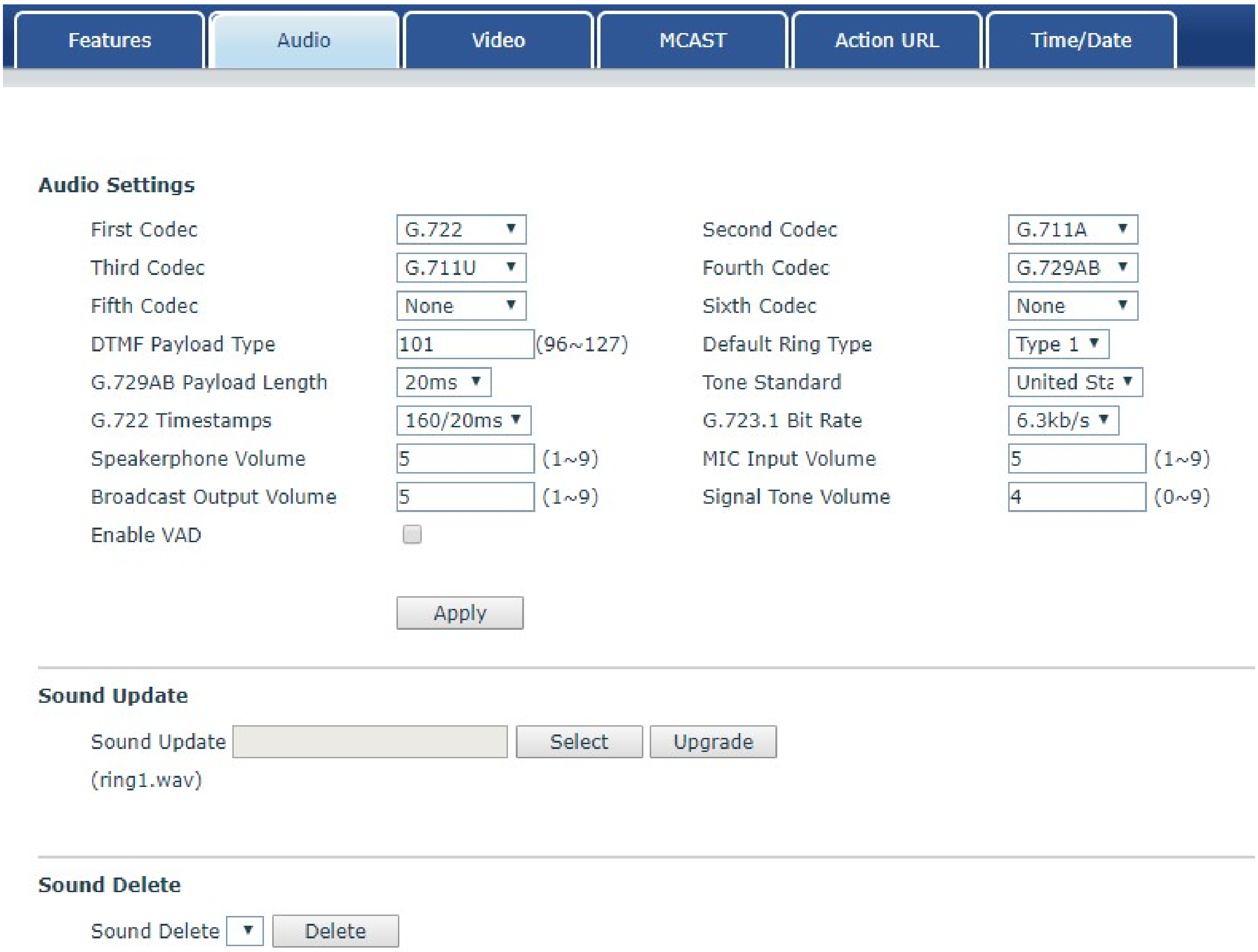
5.4 Intercom Settings

5.4.1 Features

Features	
Field Name	**Description**
Limit Talk Duration	If enabled, calls would be forced to end after talking time is up.
Talk Duration	The call will be ended automatically when time is up. Initial Value is 120 seconds.
DND (Do Not Disturb)	DND might be disabled phone for all SIP lines, or line for SIP individually. But the outgoing calls will not be affected.
Ban Outgoing	If enabled, no outgoing calls can be made.
Enable Call Waiting	The default value is enabled. Allow users to answer the second call while maintaining the call.
Enable Call Waiting Tone	The default value is enabled. When enabled, the call waiting tone can be heard while waiting for a call. If this function is turned off, when waiting for a call, the beep will not be heard.
Enable Intercom Mute	If enabled, mute incoming calls during an intercom call.
Enable Intercom Ringing	If enabled, play intercom ring tone to alert to an intercom call.
Enable Auto Answer	Enable Auto Answer function.
Auto Answer Timeout	Set Auto Answer Timeout.
No Answer Auto Hangup	Configuration automatically hangs up when no answer occurs within the set time.
Auto Hangup Timeout	Set the time of no answer auto hangs up.
Voice Read IP	Configure IP broadcasting (press the # key for 3 seconds in standby state); the default value is enabled.

Features	
Field Name	**Description**
System Language	Language for configuring voice prompts.
Enable DND	If this item is selected, the device will reject any incoming calls and the caller will remind the device not to use, but the local exhalation will not be affected.

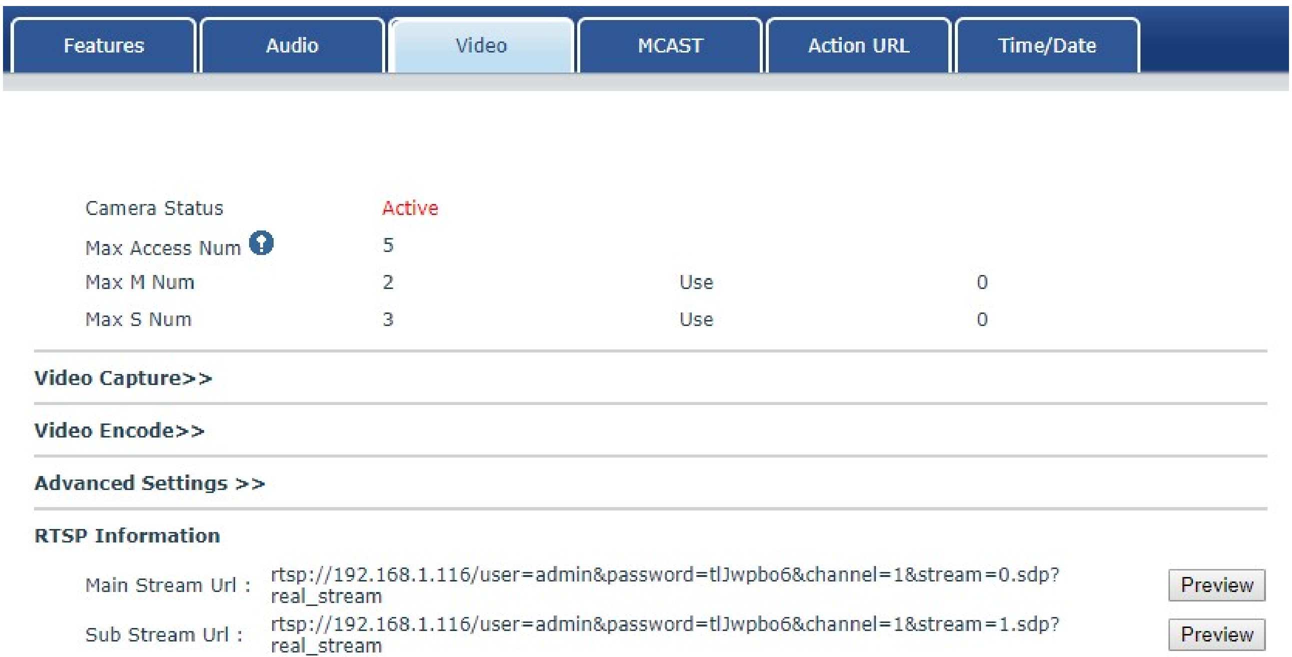
5.4.2 Audio

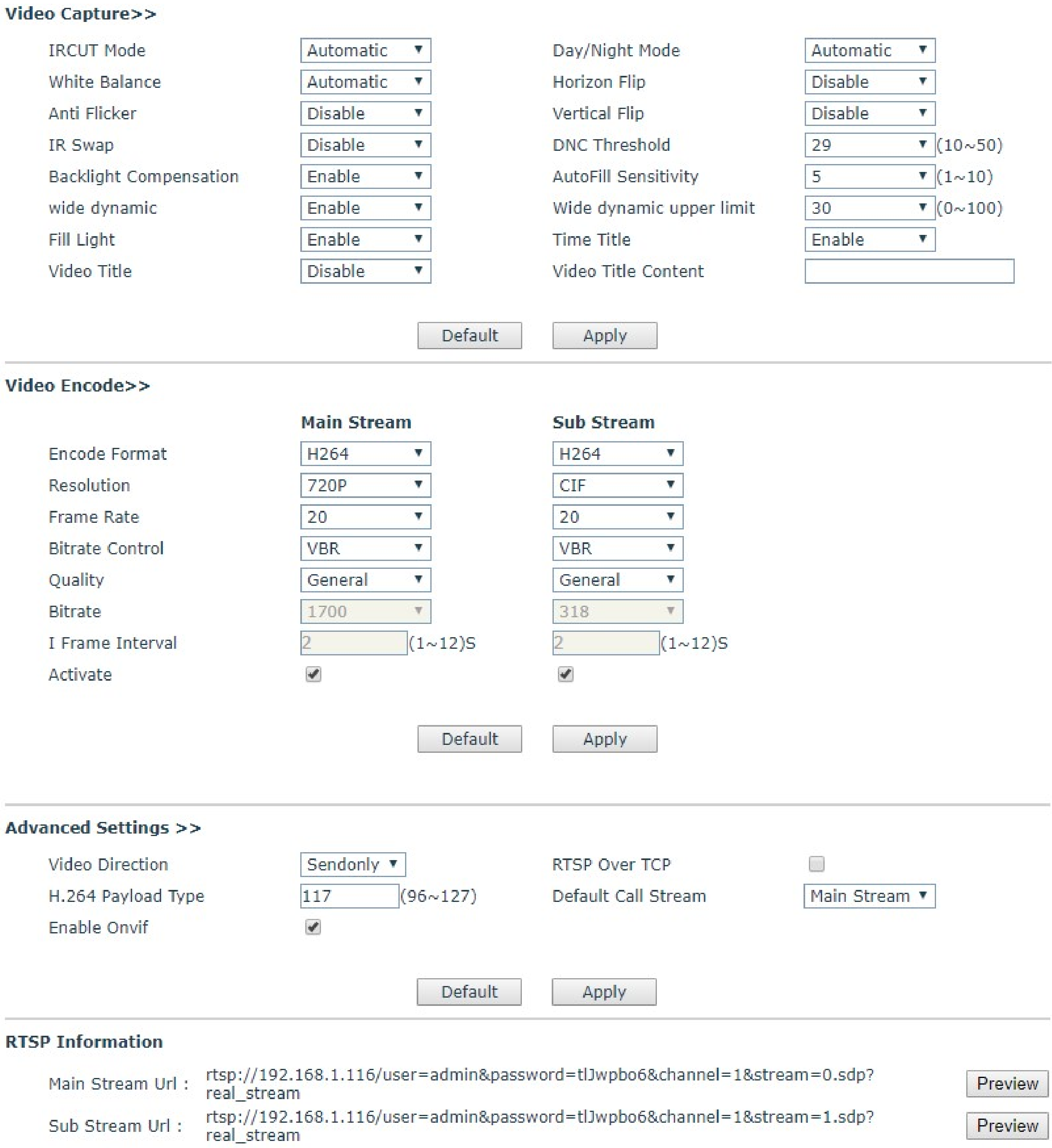


Audio	
Field Name	**Description**
Audio Settings	
Codec Setting	Select enabled or disabled audio codec: G.711A/U,G.722,G.723,G.729, G.726-16,G726-24,G726-32,G.726-40, ILBC,AMR,AMR-WB, opus

Audio	
Field Name	**Description**
DTMF Payload Type	Setting DTMF payload type, the value range must be 96~127.
Default Ring Type	Configure the default ring tone. If no special ringtone is set for the caller number, the default ringtone will be used.
G.729AB Payload Length	You can select the G.729AB Payload Length ,the options are 10ms、20ms、30ms、40ms、50ms、60ms.
G.722 Timestamps	You can choose G.722 Timestamps for 160/20ms or 320/20ms.
G.723.1 Bit Rate	You can choose G.723.1 Bit Rate of 5.3 kb/s or 6.3 kb/s.
Speakerphone Volume	Set the hands-free volume to 1-9.
MIC Input Volume	Set the microphone volume to 1~9.
Broadcast Output Volume	Set the broadcast output volume to 1~9.
Signal Tone Volume	Set the signal sound volume to 0~9.
Enable VAD	Whether voice activity detection is enabled.
Sound Update	
Sound Udate	Can be upgraded suffix ". Wav "format of the door, door, and other custom prompt sound.
Sound Delete	
Sound Delete	Upgraded ringtones are displayed in the delete list, which can be optionally deleted.

5.4.3 Video





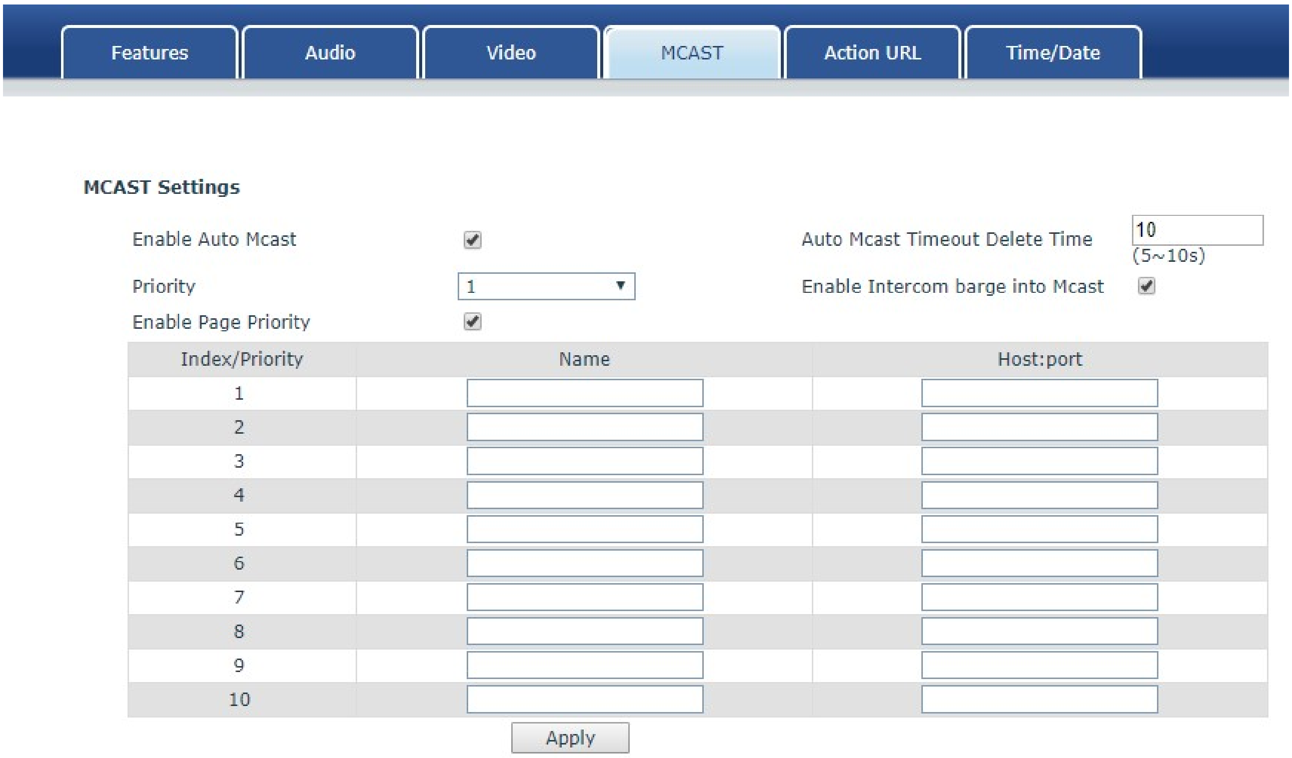
Video	
Field Name	**Description**
Camera status and number of visits	Camera status: When the device is restarted, the camera status shows whether it is currently available. The maximum number of accesses, the maximum number of main code streams, the maximum number of subcode streams and the number of uses.

Video	
Field Name	**Description**
Video Capture (Local)	
IRCUT Mode	**Auto**: IRCUT switches according to the actual ambient light level of the camera. **Synchronization**: The switching of the IRCUT is determined by the actual brightness of the IR lamp.
Day/Night Mode	**Automatic**: automatically switches according to the DNC Threshold and the brightness of the actual environment where the camera is located **Day Mode**: The camera's video screen is always colored, if there is IR-cut will be synchronized to switch. **Night Mode**: the camera's video screen is always black and white, if there is IR-cut will be synchronized switch.
White Balance	**Automatic**: Automatically adjusts according to the actual environment in which the camera is located. **Outdoor**: installed in the outdoor preferred. Indoor: installed in the room preferred.
Horizon Flip	The video is flipped horizontally.
Anti Flicker	Enable the option. In a fluorescent environment can eliminate the video horizontal scroll.
Vertical Flip	The video is flipped horizontally.
IR Swap	IR-cut filter switch.
DNC Threshold	In the Day / Night mode Auto option, the color switching black and white threshold is set Set the video color to black and white threshold in the day and night mode selection auto mode.
Backlight Compensation	In front of a very strong background light can see people or objects clearly.
AutoFill Sensitivity	In the environment changes in light and shade, the higher the sensitivity the faster the video changes.
wide dynamic	The wide dynamic is related to the optimization of the backlight scene. When people are in the backlight condition, it may be because the background is too bright and the person is a piece of black, which is helpful for optimization after opening.
Wide dynamic upper limit	Range 0~100 and the default is 30.
Fill Light	Provide auxiliary light when shooting in the absence of light conditions.
Time Title	Video can see the time information.
Video Title	Enable/disable camera titles.

Video	
Field Name	**Description**
Video Title Content	When enabled, video can see the set title information.
Video Encode (Local)	
Encode Format	Only H.264 encoding format is supported.
Resolution	Main stream: support 720P Sub-stream: D1 (704 * 576)
Frame Rate	The larger the value is, the more coherent the video would be got; not recommend adjusted.
Bitrate Control	CBR: If the code rate (bandwidth) is insufficient, it is preferred. VBR: Image quality is preferred, not recommended.
Quality	Video quality adjustment, the better the quality needs to transfer faster
Bit rate	It is proportional to video file size, not recommend adjusted.
Frame Interval	The greater the value is, the worse the video quality would be, otherwise the better video quality would be; not recommend adjusted.
Activate	When you selected it, the stream is enabled, otherwise disabled.
Encoder static setting	Baseline: catch the packet for filtering H264, see H264 nal unit payload for Baseline profile. Main profile/High profile: see the H264 nal unit payload as Main profile/High profile.
"Default" reverts to factory video configuration, and "submit" saves settings.	
Advanced Settings	
Video Direction	Sendonly: establish video call, and the SDP packet in the invite packet is Sendonly; Sendrecv: to create a call, the SDP package in the invite package is Sendrecv.
RTSP Over TCP	The RTSP goes over the TCP protocol.
H.264 Payload Type	Set the h. 264 Payload type. The range is between 96 and 127. The default is 117.
Default Call Stream	Optional main stream and substream.
Enable ONVIF	Enable the ONVIF feature, and when enabled, discover the device via the video recorder that supports ONVIF.
RTSP Information	
Main Stream URL	Access the main address of RTSP.
Sub Stream URL	Access the child address of RTSP.

5.4.4 MCAST

This feature allows user to make some kind of broadcast call to people who are in multicast group. User can configure a multicast DSS Key on the phone, which allows user to send a Real-time Transport Protocol (RTP) stream to the pre-configured multicast address without involving SIP signaling. You can also configure the phone to receive an RTP stream from pre-configured multicast listening address without involving SIP signaling. You can specify up to 10 multicast listening addresses.



MCAST	
Field Name	**Description**
Enable Auto Mcast	Send the multicast configuration information by Sip Notify signaling, and the device will configure the information to the system for multicast listening or cancel the multicast listening in the system after receiving the information.
Auto Mcast Timeout Delete Time	When a multicast call does not end normally, but for some reason the device can no longer receive a multicast RTP packet, this configuration cancels the listening after a specified time.
Priority	The priority defined in the current call, 1 is the highest priority and 10 is the lowest.
Enable Intercom barge into Mcast	When enabled, intercom insertion is allowed on multicast calls.
Enable Page	Regardless of which of the two multicast groups is called in first, the device will receive

MCAST	
Field Name	**Description**
Priority	the higher priority multicast first.
Name	Listened multicast server name.
Host:port	Listened multicast server’s multicast IP address and port.

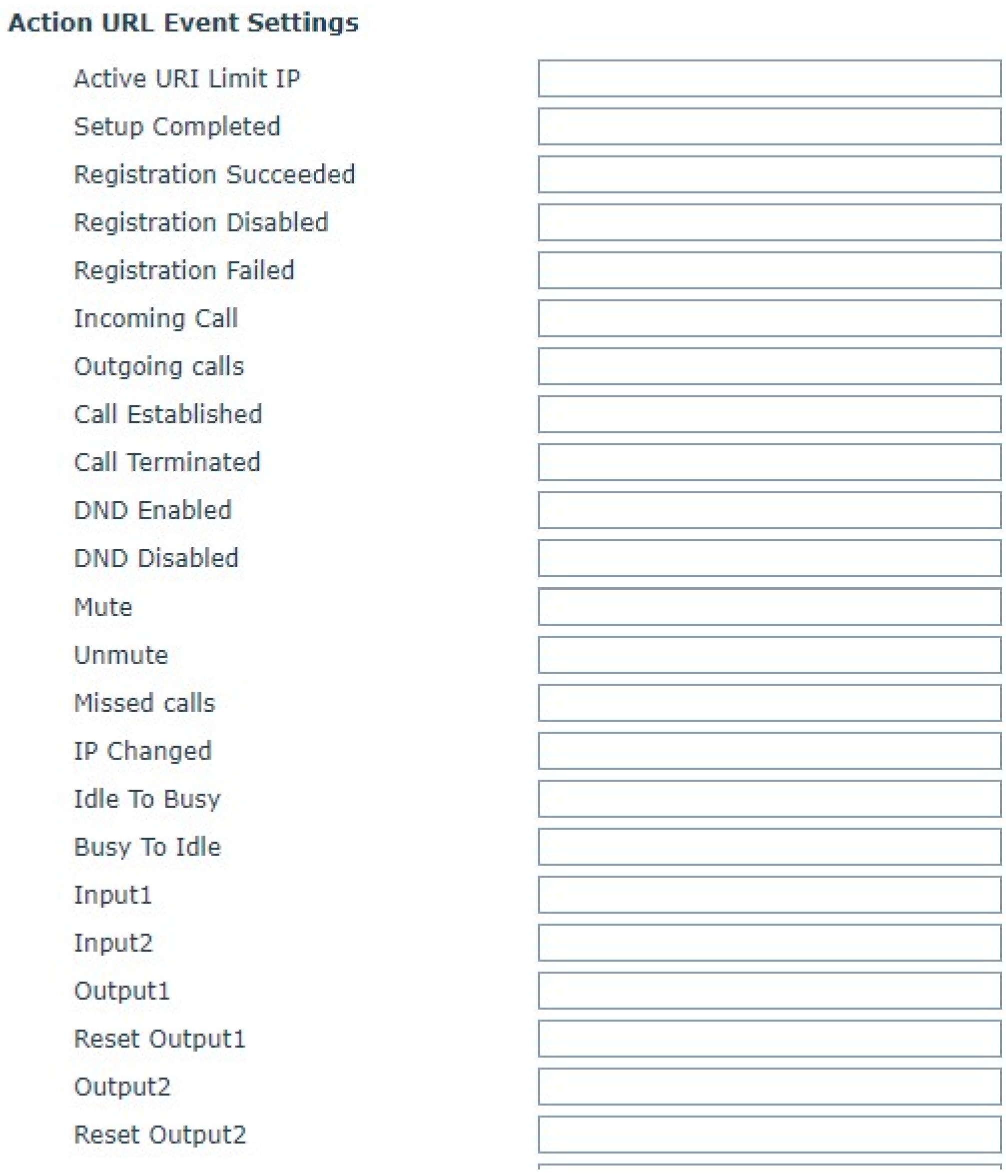
Multicast Configuration Steps:

- Go to web page of [**Function Key**] >> [**Function Key Settings**], select the type to multicast, set the multicast address, and select the codec.
- Click Apply.
- Set up the name, host and port of the receiving multicast on the web page of [**Intercom Settings**] >> [**MCAST**].
- Press the DSSKY of Multicast Key which you set.
- Receive end will receive multicast call and play multicast automatically.

5.4.5 Action URL

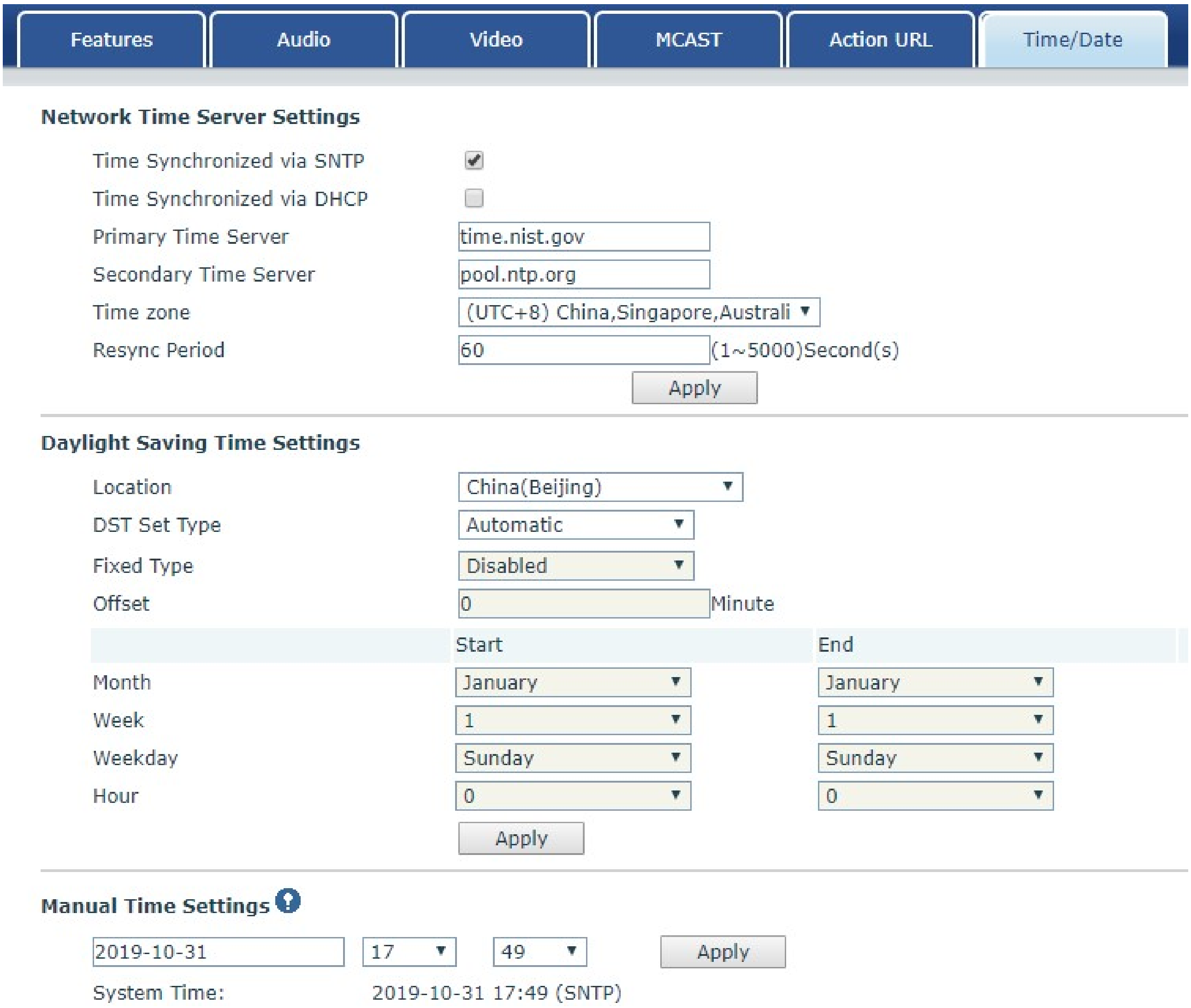
URL for various actions performed by the phone. These actions are recorded and sent as xml files to the server. Sample format is http://InternalServer /FileName.xml.

Note	The operation URL is used by the IPPBX system to submit device events.



5.4.6 Time/Date

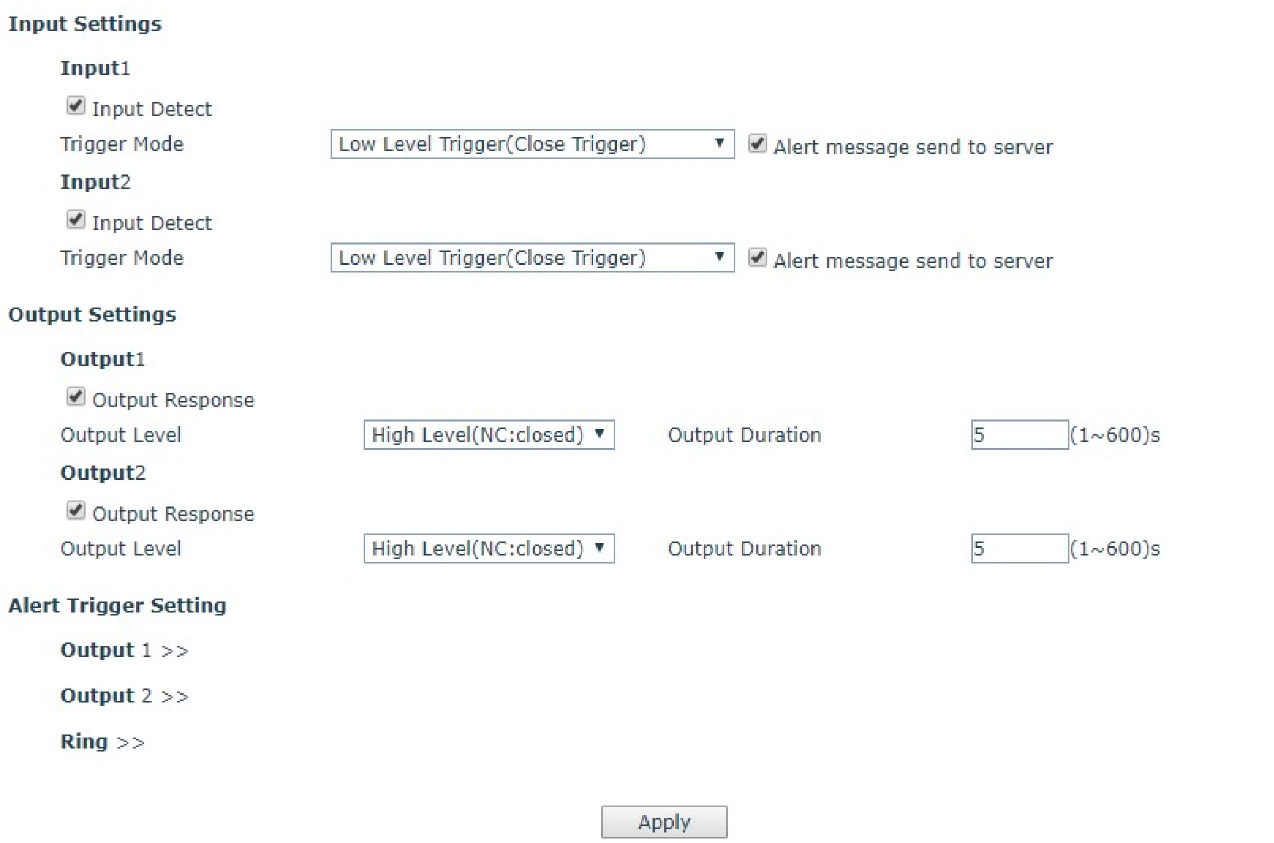
Users can configure the device's time settings on this page.

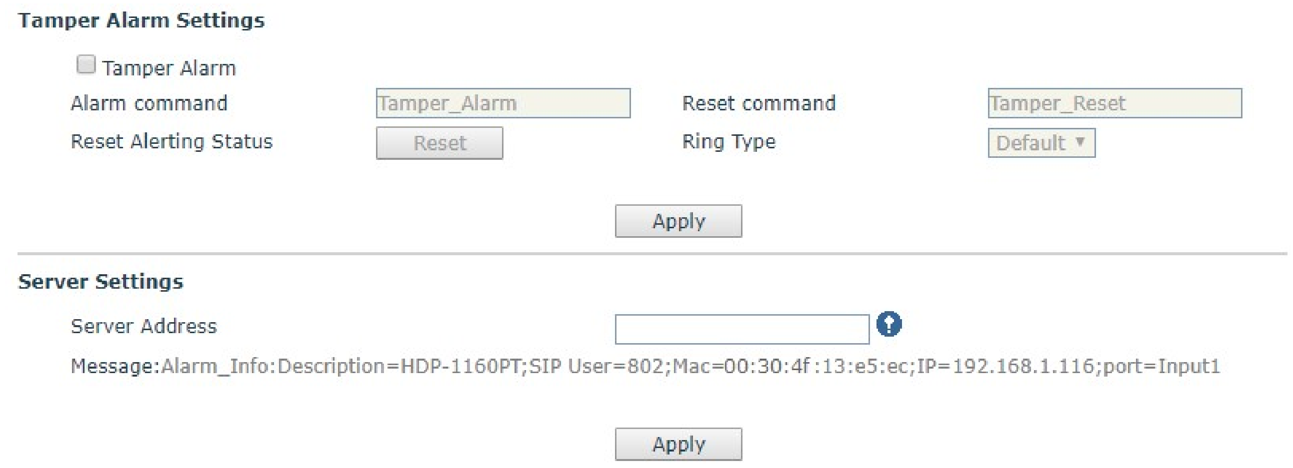


Time/Date	
Field Name	**Description**
Network Time Server Settings	
Time Synchronized via SNTP	Enable time-sync through SNTP protocol.
Time Synchronized via DHCP	Enable time-sync through DHCP protocol.
Primary Time Server	Set primary time server address.
Secondary Time Server	Set secondary time server address, when primary server is not reachable, the device will try to connect to secondary time server to get time synchronization.
Time Zone	Select the time zone.
Resync Period	Time of re-synchronization with time server.
Daylight Saving Time Settings	
Location	Select the user's time zone specific area.

Time/Date	
Field Name	**Description**
DST Set Type	Select automatic DST according to the preset rules of DST, or the manually input rules.
Offset	The DST offset time.
Month Start	The DST start month.
Week Start	The DST start week.
Weekday Start	The DST start weekday.
Hour Start	The DST start hour.
Month End	The DST end month.
Week End	The DST end week.
Weekday End	The DST end weekday.
Hour End	The DST end hour.
Manual Time Settings	
Manual Time Settings	The time set by hand, need to disable SNTP service first.

5.5 Security Settings

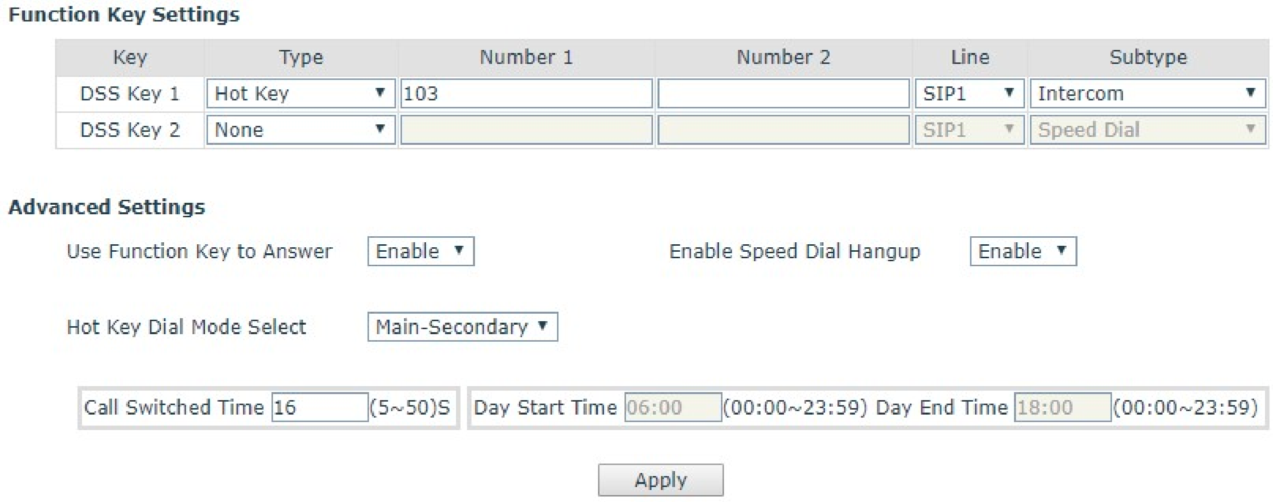




<table>
<tr><th colspan="3">Security Settings</th></tr>
<tr><th>Field Name</th><th colspan="2">Description</th></tr>
<tr><th colspan="3">Input Settings</th></tr>
<tr><td>Input Detect</td><td colspan="2">Enable or disable Input Detect.</td></tr>
<tr><td rowspan="2">Trigger Mode</td><td colspan="2">When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger.</td></tr>
<tr><td colspan="2">When choosing the high level trigger (disconnected trigger), detect the input port (high level) disconnected trigger.</td></tr>
<tr><td>Alert message sends to server</td><td colspan="2">Set the Alert message send to server</td></tr>
<tr><th colspan="3">Output Settings</th></tr>
<tr><td>Output Response</td><td colspan="2">Enable or disable Output Response.</td></tr>
<tr><td rowspan="2">Output Level</td><td colspan="2">When choosing the low level trigger (NO: normally open), when meet the trigger condition, trigger the NO port disconnected.</td></tr>
<tr><td colspan="2">When choosing the high level trigger (NO: normally close), when meet the trigger condition, trigger the NO port close.</td></tr>
<tr><td>Output Duration</td><td colspan="2">Changes in port, the duration of. The default is 5 seconds.</td></tr>
<tr><th colspan="3">Alert Trigger Settings</th></tr>
<tr><td>Alarm Ring Duration</td><td colspan="2">Set the Alarm Ring Duration. The default is 5 seconds.</td></tr>
<tr><td>Input trigger</td><td colspan="2">When the input port meets the trigger condition, the output port will be triggered (The Port level time change, By < Output Duration > control).</td></tr>
<tr><td rowspan="2"></td><td>By duration</td><td>Port switch amount change time, press <output duration> control.</td></tr>
<tr><td>By Calling State</td><td>By call state control, after the end of the call, port to return the default state.</td></tr>
<tr><td>Remote DTMF trigger</td><td colspan="2">Receive the DTMF password sent by the remote device. If it is correct, trigger the corresponding output port. You can choose to enable or disable</td></tr>
</table>

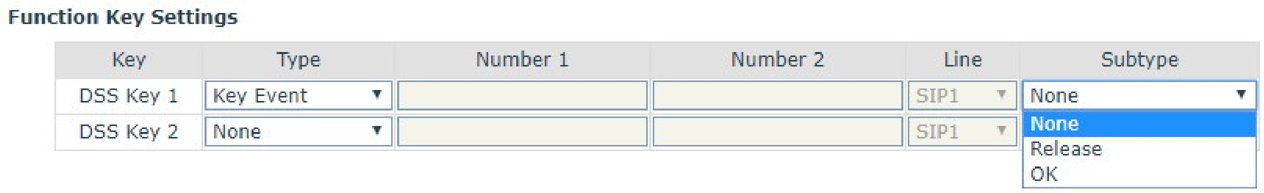
Security Settings	
Field Name	**Description**
	ringtones
DTMF trigger code	During the call, the receiving terminal device sends a DTMF password, and if it is correct, the corresponding output port is triggered. The default is 1234.
Remote SMS trigger	Enable or disable remote SMS triggering. You can choose to enable or disable ringtones
Trigger Message Format	Send instructions on remote devices or servers, ALERT= [set instructions], if correct, trigger the corresponding port output.
Call status trigger	The port outputs a continuous time trigger type, including the trigger condition. For example, the call triggers the output port, and the output port will be in the call state and continue to respond) 1 Talking 2 Talking and Ringing 3 Ringing 4 Calling 5 Calling and Talking 6 Calling and Ringing 7 Calling, Ringing and Talking
Tamper Alarm Settings	
Alarm command	When detected someone tampering the equipment, the alarm signal will be sent to the corresponding server
Reset command	When the equipment receives the command of reset from server, the equipment will stop alarm
Reset Alerting Status	Reset to resume and stop ringtone playback
Ring Type	Ringtone can be set to none / preset
Server Settings	
Server Address	Send message to the server when the alarm is triggered. message format：Alarm Info: Description=HDP-1160PT;SIP User=;Mac=00:30:4f:68:23:d1;IP=172.18.90.235;port=Input1

5.6 Function Keys



Key Event

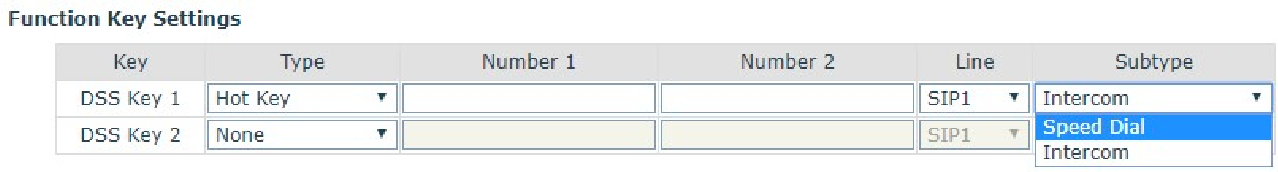
The speed dial key type could be set as Key Event.



Function Key		
Type	**Subtype**	**Usage**
Key Event	None	No responding
	Release	Delete password input, cancel dialing input and end call
	OK	Identification key

Hot Key

When the speed dial key is set as Hot Key, the device would dial preset telephone number. This button can also be used to set the IP address. You can press the speed dial button to directly make an IP call.

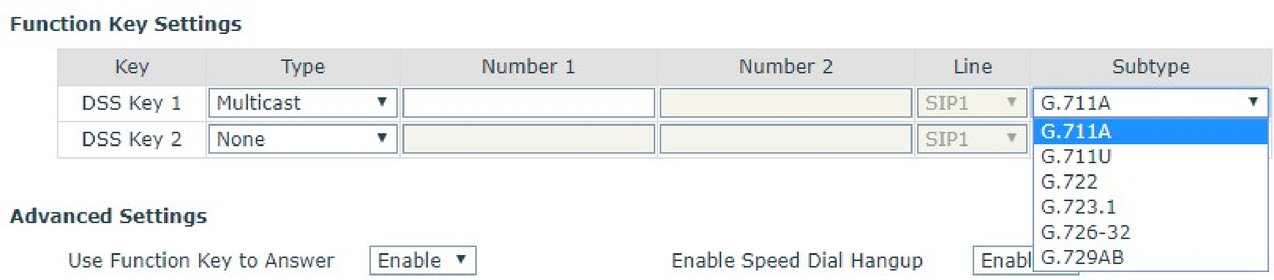


Function Key				
Type	**Number**	**Line**	**Subtype**	**Usage**
Hot Key	Fill the called party's SIP account or IP address	The SIP account corresponding lines	Speed Dial	Using Speed Dial mode together with Enable Speed Dial Hangup [Enable], can define whether this call is allowed to be hung up by re-pressing the speed dial key.
			Intercom	In Intercom mode, if the caller's IP phone supports Intercom feature, the device can automatically answer the Intercom calls.

Multicast

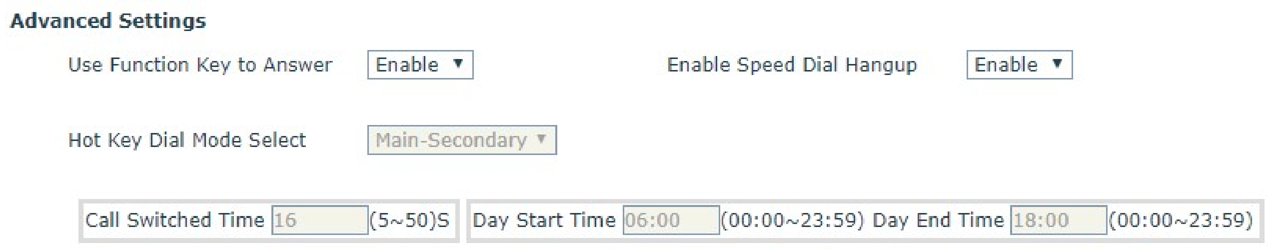
Multicast function is to deliver voice streams to configured multicast address; all equipment monitored the multicast address can receive and play the broadcasting. Using multicast functionality would make deliver voice one to multiple which are in the multicast group simply and conveniently.

The DSS Key multicast web configuration for calling party is as follows:



Function Key			
Type	**Number**	**Subtype**	**Usage**
Multicast	Set the host IP address and port number, they must be separated by a colon (The IP address range is 224.0.0.0 to 239.255.255.255, and the port number is preferably set between 1024 and 65535)	G.711A	Narrowband speech coding (4Khz)
		G.711U	
		G.722	Wideband speech coding (7Khz)
		G.723.1	Narrowband speech coding (4Khz)
		G.726-32	
		G.729AB	

Advanced Settings



Advanced Settings	
Field Name	**Explanation**
Input port is multiplexed as function key 2	Enable or disable the input port to be multiplexed as speed dial button 2
Use Function Key to Answer	Enable or disable shortcuts to answer calls
Enable Speed Dial Hang up	Enable or disable shortcuts to hang up calls
Hot Key Dial Mode Select	Number 1 call number 2 mode selection. <Main/Secondary>: If the first number is not answered within the set time, the second number will be automatically switched. <Day/Night>：The system time is automatically detected during the call. If it is daytime, the first number is called, otherwise the second number is called.
Call Switched Time	Set number 1 to call number 2 time, default 16 seconds
Day Start Time	The start time of the day when the <Day/Night> mode is defined. Default "06:00"
Day End Time	The end time of the day when the <Day/Night> mode is defined. Default "18:00

Appendix A: Troubleshootings

If the following fixes cannot troubleshoot your problems, contact the supplier where the purchase is made or PLANET technical support team.

Get device system information

Users can obtain information through the [System] >> [Information] option on the device webpage. The following information will be provided:
Device information (model, software and hardware version), Internet Information, etc.

Reboot device

The user can restart the device through the webpage -- click [**System**] >> [**Tools**] >> [**Reboot Phone**] and click the [**Reboot**] button, or directly unplug the power to restart the device.

Device factory reset

Restoring the factory settings will delete all configuration, database and configuration files on the device and the device will be restored to the factory default state.
To restore the factory settings, you need to log in to the webpage [**System**] >> [**Configuration**], and click the [**Reset**] button.

Netowork Packets Capture

In order to obtain the data packet of the device, the user needs to log in to the webpage of the device, open the webpage [**System**] >> [**Tools**], and click the [**Start**] option in the "Network Packets Capture". A message will pop up asking the user to save the captured file. At this time, the user can perform related operations, such as starting/deactivating the line or making a call, and clicking the [**Stop**] button on the webpage after completion. Network packets during the device are saved in a file.

Common Problematic Cases

Problematic Case	Solution
Device could not boot up	1. If the device enters "POST mode" (the SIP/NET and function button indicators are always on), the device system is damaged. Please contact your local technical support to help you restore your equipment system. 2. If the device enters "POST mode" (the SIP/NET and function button indicators are always on), the device system is damaged. Please contact your local technical support to help you restore your equipment system.
Device could not register according to a service provider	1. Please check if the device is connected to the network. The network cable must be connected to the [Network] interface instead of the [Computer] interface.

Problematic Case	Solution
	2. Please check if the device has an IP address. Check the system information. If the IP address is Negotiating..., the device has not obtained an IP address. Please check if the network configuration is correct. 3. If the network connection is good, please check your line configuration again. If all configurations are correct, contact your service provider for support, or follow the instructions in "5.1.7 Network Data Capture" to obtain a registered network packet.

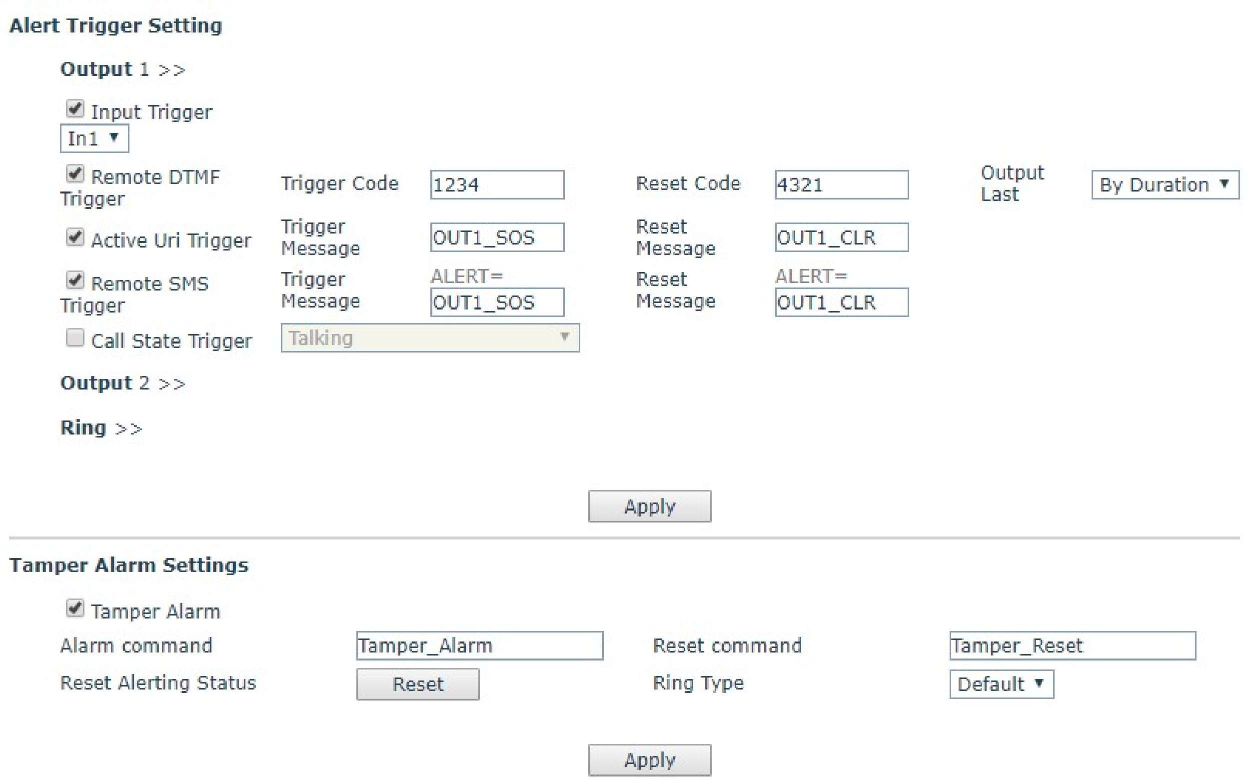
Appendix B: How to use ICF-1800 to open door via DTMF code

Step 1. Install HDP-1160PT x 1 ICF-1800 x 1 and IPX-330 x 1 and anode lock x 1 at the client.

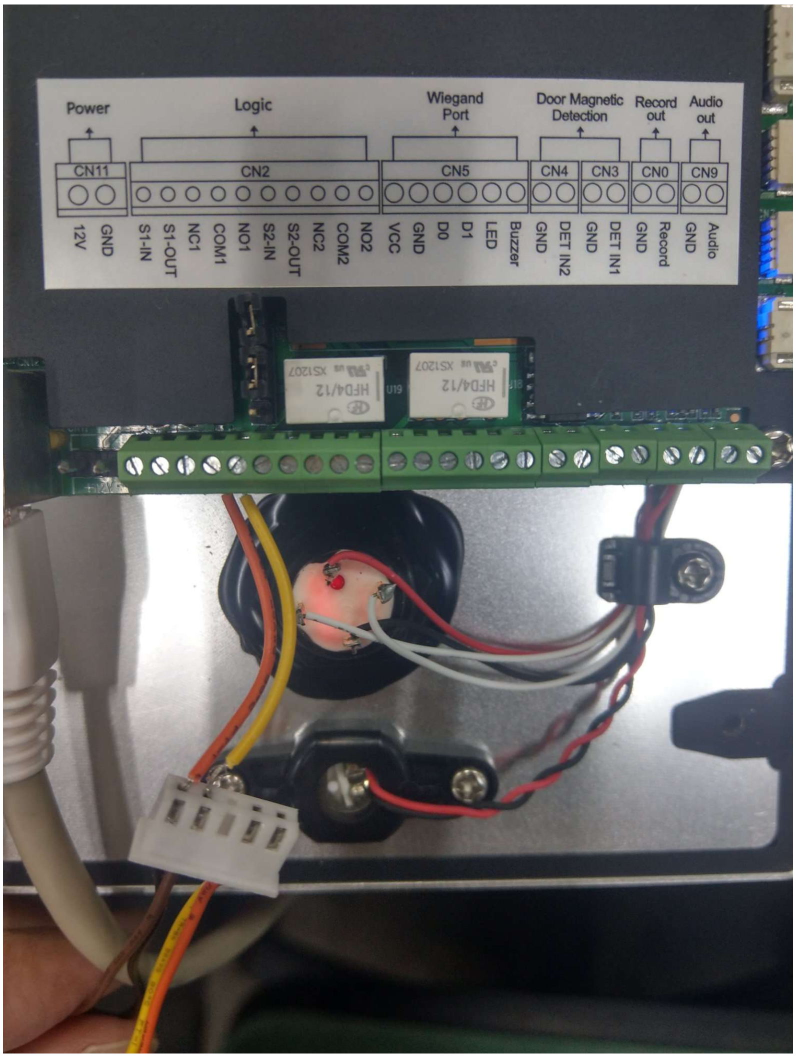
Step 2. Register account at HDP-1160PT and ICF-1800 to IPBPBX.

Step 3. Set up DSS key of HDP-1160PT and make sure the equipment can dial to ICF-1800 after pressing call button.

Step 4. Set up Alert Trigger Setting of HDP-1160PT and disable Call State Trigger.



Step 5. Connect HDP-1160PT with anode lock as shown below.



Step 6. Open anode lock through remote DTMF of ICF-1800 (The default is 1234).