PLANET
Networking & Communication

User's Manual

1080p SIP Vandalproof Door Phone with RFID and PoE

► **HDP-1261PT**

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 1080p SIP Vandalproof Door Phone with RFID and PoE
Model: HDP-1261PT
Rev: 1.00 (February, 2024)
Part No. EM-HDP-1261PT_v1.0

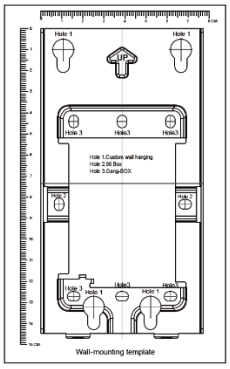
Table of Contents

Chapter 1. Product Introduction

1.1 Package Contents

Thank you for purchasing PLANET SIP Vandalproof Door Phone, HDP-1261PT.

Open the box of the SIP Vandalproof Door Phone and carefully unpack it. The box should contain the following items:

SIP Vandalproof Door Phone x 1	Quick Installation Guide QR Code Sheet x 1	Wall-mounted Kit x 1
		
Mounting Template x 1	**RFID Card x 2**	**Screw Kit x 1**
		
Screw Driver x 1	**Pin Cable x 1**	
		

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-1261PT Vandalproof Video Door Phone is designed for offices, 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 presses the call button of the door phone. The HDP-1261PT works like an intercom. As its name implies, it is vandalproof and has a video feature.

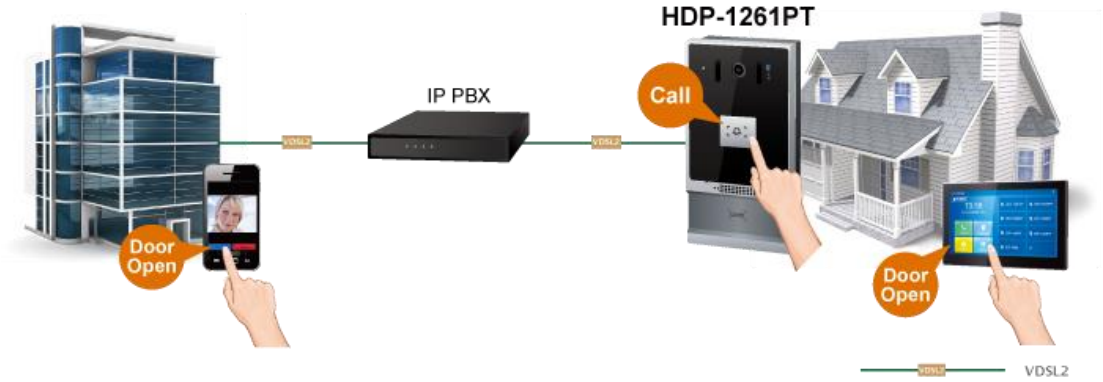
It supports the standard IETF **SIP** protocol and **ONVIF** protocol for easy operation and interfaces with the VoIP and IP surveillance world in an instant it connects you with. It delivers excellent picture quality in **1080p** HD resolutions with a viewing angle of **120° (H)**, **60° (V)**. The 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.

With DSS key button and the **RFID** system, it offers the users keyless control and convenience for opening the door without a key. The door can be opened remotely and also with a local IC/ID card if it is an electronic door lock.

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-1261PT allows you to see the visitors and also communicate with them. The HDP-1261PT includes 3 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 SIP Indoor Touch Screen PoE Video Intercom to open the door for your visitors.

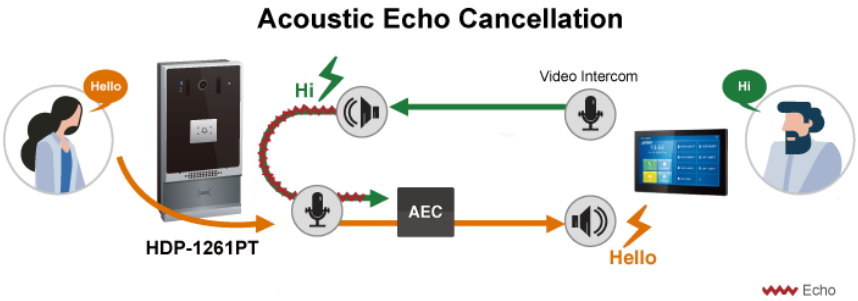


A Door Guard for Extreme Conditions

The HDP-1261PT is an extremely durable IP intercom that can withstand even the most demanding conditions. Its Industrial design supports **-40** to **70** degrees C operating temperature, and resilience to dust, water **(IP66)** and vandalism **(IK07)** to ensure maximum security.

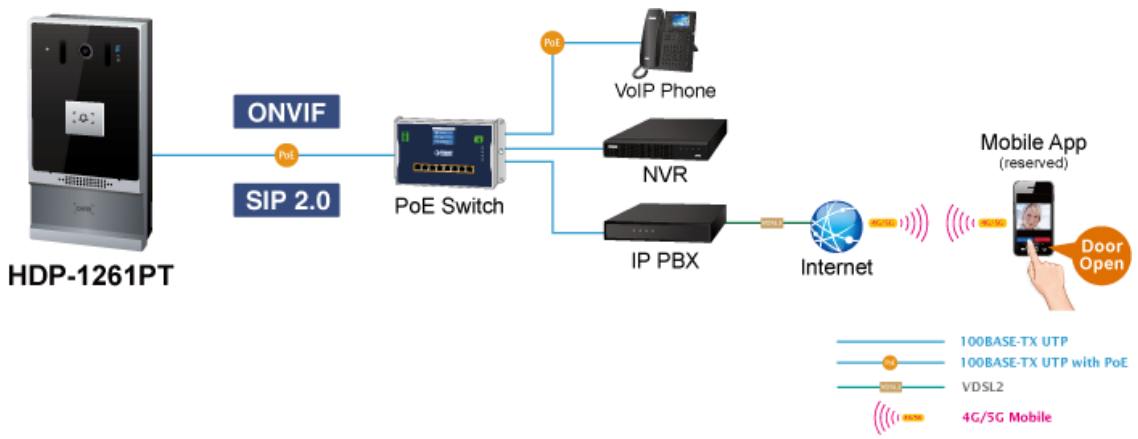
Acoustic Echo Cancellation

Acoustic Echo Cancellation (AEC) technology is adopted in PLANET's HDP-1261PT Door Phone and 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-1261PT 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.



1.3 Features

Benefits

- Unlock the door with an **RFID**, and Remote **DTMF**
- Viewing angle of 120° (H), 60° (V) HD camera with infrared light and night vision
- HD voice using wideband G.722 coding produces clearer sound
- Secure communication with TLS & Secure RTP (SRTP)
- Access Control with the electric lock (Built-in 3 short-in/2 short-out)
- IP66- and IK07-rated for rigorous environment
- Compatible with the Asterisk IP PBX system that can run on SIP/ONVIF and other platforms
- Support for seamless integration with P2P applications

Intercom Functions

- 2 SIP identities/accounts for Intercom
- Intelligent DSS Key for one-touch speed dial, hotline
- Full-duplex handsfree and auto answer
- Action URL/Active URI and dynamic multicast function

Hardware

- HD voice speech quality with built-in 2.5W speaker and Acoustic Echo Canceller (AEC)
- High intensity IR LEDs for picture lighting during dark hours with internal light sensor
- 3 built-in short-in detection ports and 2 short-out control ports
- Industrial design made to withstand -40 to 70 degrees C operating temperature
- Wall-mount design for outdoor unit

Video and Audio

- Maximum resolution 1920 x 1080 @ 30 fps
- Acoustic Echo Cancellation (AEC) is featured on speaker path
- Volume adjustment can be performed either through the button or the web page.
- HD voice using wideband G.722 coding produces clearer sound

Network and Configuration

- Standard IETF SIP protocol for VoIP services
- Compatible with the ONVIF for video surveillance
- Compliant with IEEE 802.3af/at PoE interface for flexible deployment
- HTTPS, TR069 and auto-provisioning
- PLANET DDNS and Easy DDNS
- PLANET Smart Discovery Utility for deployment management

➢ Easy Installation and Management

- Hands-free intercommunication
- Conveniently unlock the door for visitors without having to go to it
- Have peace of mind from being able to see, hear and speak to your visitors before opening the door

1.4 Specifications

Product	HDP-1261PT
Access Control	
Door Access	Dual SIP line, Dual SIP servers DTMF tones, RFID /IC card: ID (EM4100,125KHz) & IC (MIFARE ONE,13.56MHz) ✓ Supports up to 10,000 RFID cards. ✓ Records door open events with a capacity of 200,000 entries
Door Phone features	Full-duplex Default auto answer Action URL/Active URI remote control Speed Dial
Video	
Image Device	2MP color CMOS camera
Max. Image Transfer Rate	1080p -30fps (1080p expected to be launched by firmware upgrade in 2024/Q1)
Video Codec	H.264
Resolution	Main stream 1080P@30fps Sub stream VGA@30fps
Viewing Angle	120° (H), 60° (V) , 141° (D)
Minimum illumination	0.1Lux, support for infrared illumination
IR Illuminations	IR LED x 4, effective up to 5 meters *The IR distance is based on the environment.
Audio	
Audio Streaming	HD voice Two-way audio stream
Microphone	Built-in microphone and speaker
Narrowband Codec	G.711A/U, G.729A/B,iLBC,G.723.1,G.726-32K Wideband Codec: G.722, Opus
DTMF	In-band, Out-of-Band (RFC2833/ SIP INFO)
Audio Output	Acoustic Echo Cancellation (AEC) audio output
Protocol and Security	
Protocols	SIP v1 (RFC2543), v2 (RFC3261) over UDP/TCP/TLS RTP/RTCP/SRTP ONVIF STUN DHCP IPv6 PPPoE L2TP

	OpenVPN SNTP FTP/TFTP TR-069
Security	Web Filter, Transport Layer Security (TLS) Secure Real-time Transport Protocol (SRTP) NAT traversal: STUN mode HTTP/HTTPS web server, HTTPS certificate manager Firewall
Network and Provisioning	
Network Interface	1 x 10/100BASE-TX RJ45 Ethernet interface, auto-MDIX
IP Configuration	Static/DHCP/PPPoE
Deployment/Maintenance	Auto provisioning: FTP/TFTP/HTTP/HTTPS/DHCP OPT66/SIP PNP/TR-069 VLAN Web Management Web-based packet dump Configuration backup/restore Firmware Upgrade via Web Syslog PLANET DDNS and Easy DDNS PLANET Smart Discovery Utility
Physical Interface	
Keypad	1 DSS button (speed dial button)
Power Requirements	Power over Ethernet (IEEE 802.3af/at), class 3 and DC12V
Net Weight	493g
Dimensions (W x D x H)	88 x 36.15 x 177.4 mm
Emission	CE, FCC
Connectors	1 100M/10M RJ45 Ethernet Short-in detection port x 3 ✓ Port: Terminal socket Short-out control port x 2 (built-in relay) ✓ Relay: Max. DC30V / 2A, AC125V / 0.5A ✓ Port: Terminal socket Tamper switch x 1 TF card slot x 1: connect TF card, up to 128GB RF Card Reader:125KHz & 13.56MHz RS485 (Reserved for future use) Wiegand Port: In/Out configurable, Wiegand in by default

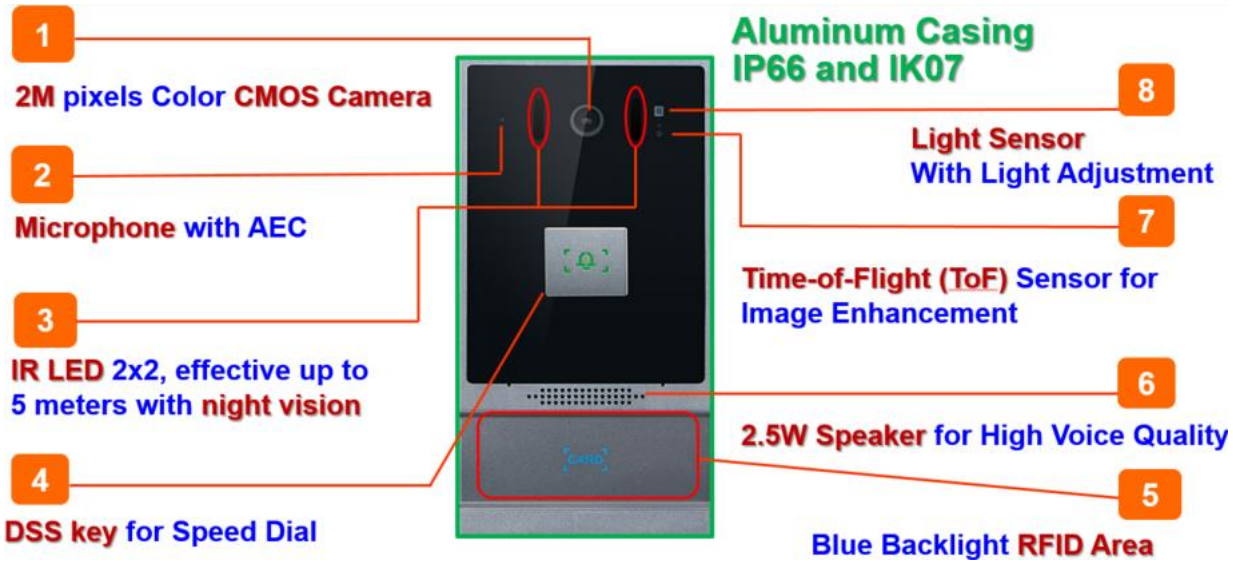
	Line-out port x 1: for induction loop antenna loop DC port x 1: DC power input ✓ DC power input: DC12V/1A ✓ Port: Terminal socket
Installation	Wall-mount type
External Power Supply	DC 12V, 1A
Environments	
Operating Temperature	-40~70˚C
Storage Temperature	-40~70˚C
Operating Humidity	10~95% (non-condensing)

Chapter 2. Hardware Interface

2.1 Physical Descriptions

Product Dimensions (W x D x H)	88 x 36.15 x 177.4 mm
Net Weight	493g

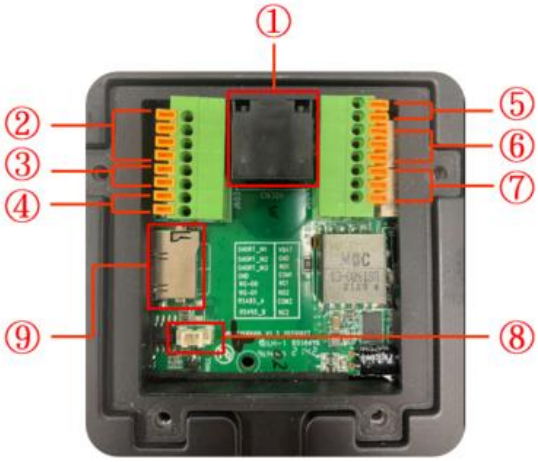
Front Panel



Number	Interface	Description
1	**Camera**	The door phone has a built-in IP camera supporting a high-resolution video of up to 1920 x 1080 pixels.
2	**Mic**	The door phone has a built-in microphone hidden in the pinhole located on the front panel.
3	**IR LED**	The door phone provides 4 IR LEDs for clear image in low light condition.
4	**DSS Key**	For speed dial, multicast, intercom, IP broadcast and other functions. (Function can be set by user.)
5	**RFID Sensor**	Use the corresponding RFID door card to open the door by swiping the card. With one beep sound, the door is opened.
6	**Speaker**	The door phone has a built-in speaker for convenient communication and alert use.
7	**Distance Sensor**	The distance between the sensing device and the object.
8	**Photosensitive**	Sensor for image enhancement.

I/O Control Description

Open the rear case of the device and find a row of terminal blocks for connecting the power supply, electric lock control, etc. The connections are shown in the table below:



Serial Number	Description
1	Ethernet interface: standard RJ45 interface, 10/100M adaptive (It is recommended to use CAT5 or CAT5E network cable.).
2	3 short-circuit input detection interfaces for connecting switches, infrared probes, door magnets, vibration sensors and other input devices.
3	Wiegand interface
4	RS485 interface (Reserved for future use)
5	Power interface: 12V/1A input up positive, down grounded
6、7	2 short-circuit output control interfaces for controlling electric locks, alarms, etc.
8	Line out interface
9	SD card slot

Note

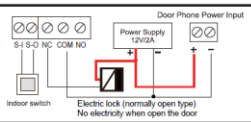
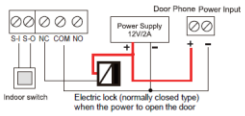
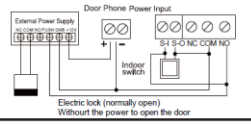
The HDP-1261PT requires either IEEE 802.3af/at PoE or DC power from the power connector.

Wiring Instructions:

NO: Normally Open Contact；

COM: Common Contact；

NC: Normally Closed Contact.

Driving Mode	Electric-lock Mode		Connections
Passive	No electricity when open	Electrify when open	
√	√		
√		√	
√	√		

Reset to Factory Default

When the HDP-1261PT is powered on and the DSS button indicator is rapidly flashing, press the DSS button once to enter POST mode. Then press the speed-dial button three times to reset the system to default and automatically announce the IP address by voice after successfully switching to the network mode.

2.2 Hardware Installation

Wall mounting steps:

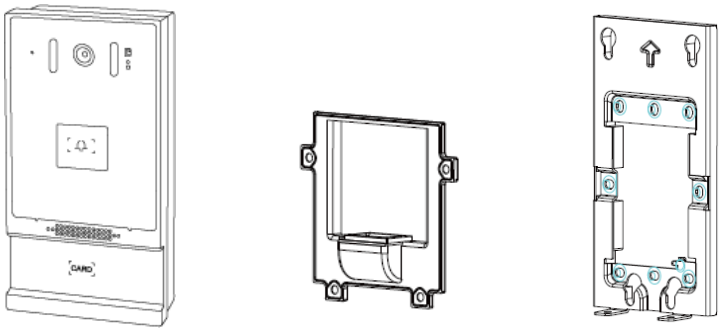


Figure 2-2-1 Three Major Parts of HDP-1261PT

(Main Body, Back Shell and Wall Bracket)

Step 1: Installation preparation

A. Check the following contents:

- φ5.2*φ3*6mm screws x 3
- TA4*30mm screws x 5
- φ6*30mm screw anchors x 5
- PM4*16mm screw x 3
- TM6*20mm screw x 5
- Screw Driver x 1
- Pin Cable x 1

B. Tools that may be required:

- Phillips screwdriver, hammer, RJ45 crimper
- Electric impact drill with an 8mm drill bit

Step 2: Drilling

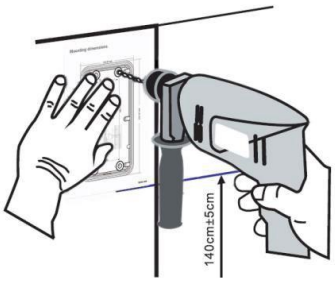


Figure 2-2-2 Wall Mounting

A. Place the mounting template with dimensions on the surface of a wall in a desired flat position.

B. Use an electric drill to drill the 4 holes marked on the mounting template. It is recommended to drill about 50mm deep. Remove the template when finishing drilling.

C. Push or hammer wall anchors into the drilled holes.

Step 3: Removing hanging bracket and back panel

A. Detach the wall bracket downward from the device and loosen the four screws on the rear cover with a screwdriver, as shown in Figures 2-2-3-1 and 2-2-3-2.

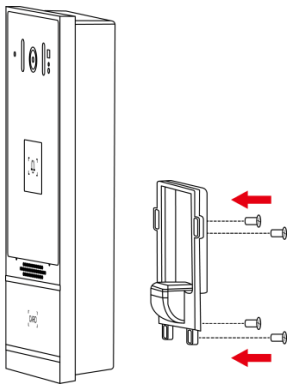


Figure 2-2-3-1

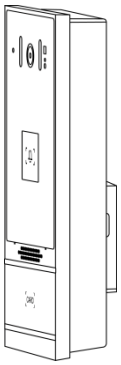


Figure 2-2-3-2

Step 4: Install the wall bracket, wiring and casing

A. Align the screw holes of the wall bracket with the holes in the wall and fix them to the wall with the screws, as shown in Figure 2-2-4.

B. Pass all the wires through the silicone plug in the middle of the bottom case.

The length of all the lines should be 15 to 20 cm, as shown in Figure 2-2-5.

Note	The outlet hole of the bottom case faces down.

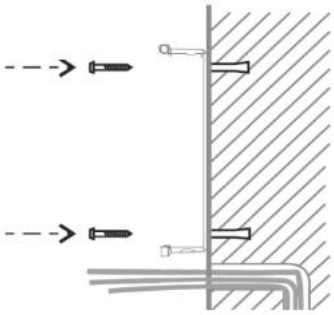


Figure 2-2-4

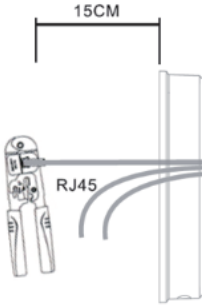


Figure 2-2-5

C. Connect the cables of RJ45, power, and electric-lock to the motherboard socket as mentioned in connector description.

D. Connect the terminal of the wired cable to the motherboard socket.

E. Test whether there is electricity by doing the following: Press the DSS key button for 3 seconds to get the IP address of intercom by voice. Input access password or press the indoor switch to check electric-lock installation.

Note	Do not proceed mounting until you have finished the electrical inspection .

F. Attach the device to the wall bracket in a top-down manner, locking the screws at the Bottom, as shown in Figure 2-2-6.

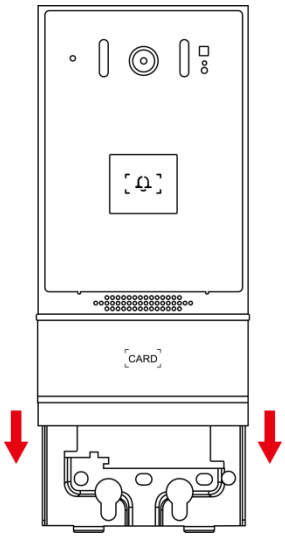


Figure 2-2-6

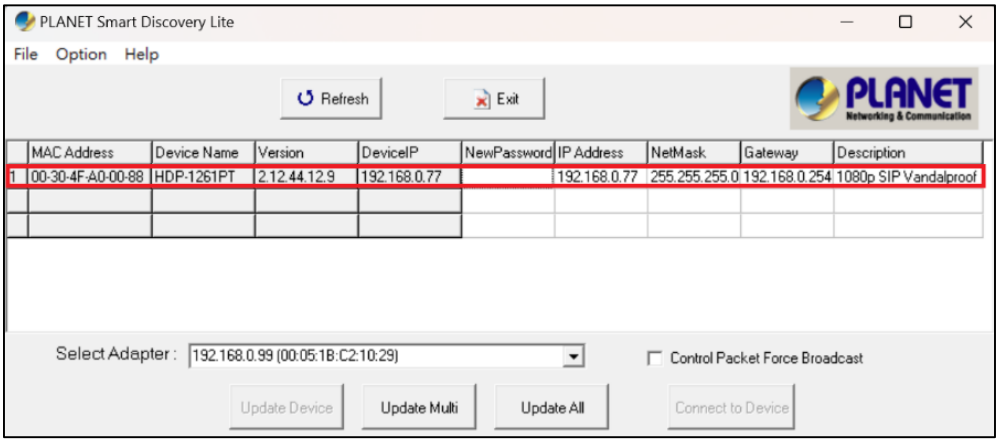
Note	While drilling or fixing the HDP-1261PT, hold it tight or else it may drop and accidentally hurt the installer.

2.3 Searching Door Phone

There are two methods as shown below to search the HDP-1261PT.

Method 1:

Open the **Planet SmartDiscoveryLite Utility**. Press the Refresh button to search the HDP-1261PT and find the IP address.



Method 2:

Long-press **DSS key** for **3 seconds** after powering on for 30 seconds, and when the speaker beeps rapidly, press the **speed-dial button** within **5 seconds**, and the system will automatically announce the IP address by voice.

In addition, the device offers DSS key operation on the device surface to switch the IP address acquisition mode.

Touch and hold the **speed-dial button** for **3 seconds**, wait for the speaker to beep, press the **speed-dial button three times** within **5 seconds**, and the system will automatically announce the IP address by voice after successfully switching to the network mode.

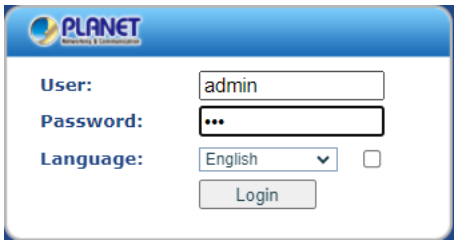
Default Setting	
Default IP Address	**172.16.0.1**
Default Web Port	80
Default Login User Name	**admin**
Default Login Password	**123**

2.4 Starting Web Management and Door Phone Setting

Step 1: Log in the web setting page of door phone

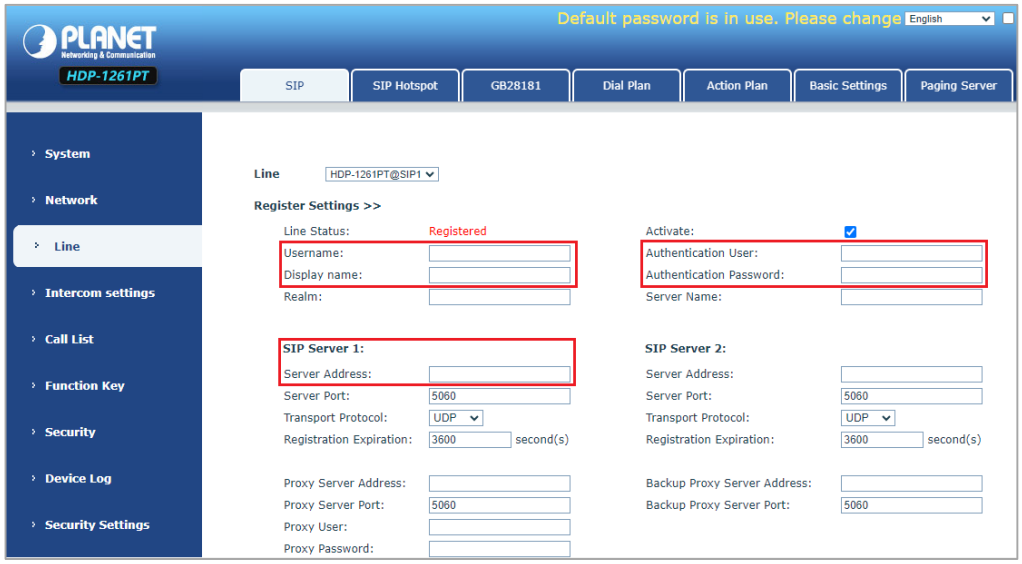
Enter the IP address of the door phone (e.g., https://172.16.0.1) in the address bar using the **https** method of your PC's web browser.

The default user name and password are **admin** and **123**, respectively



Step 2：Add the SIP account.

Set SIP server address, port, user name, password and SIP user with assigned SIP account parameters. Select “Activate”, and then click Apply to save this setting.



Step 3: Setting DSS key

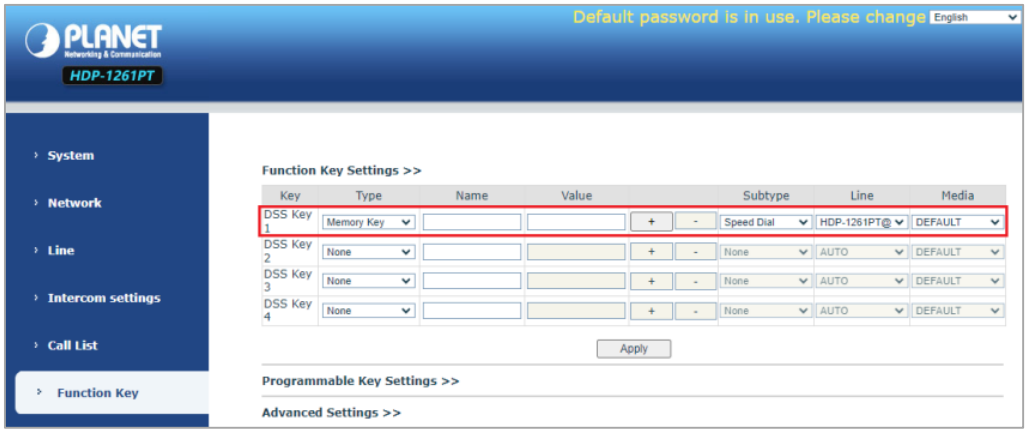
Set the DSS key as shown below for a quick start. Click “Apply” to save this setting.

Type: Memory Key.

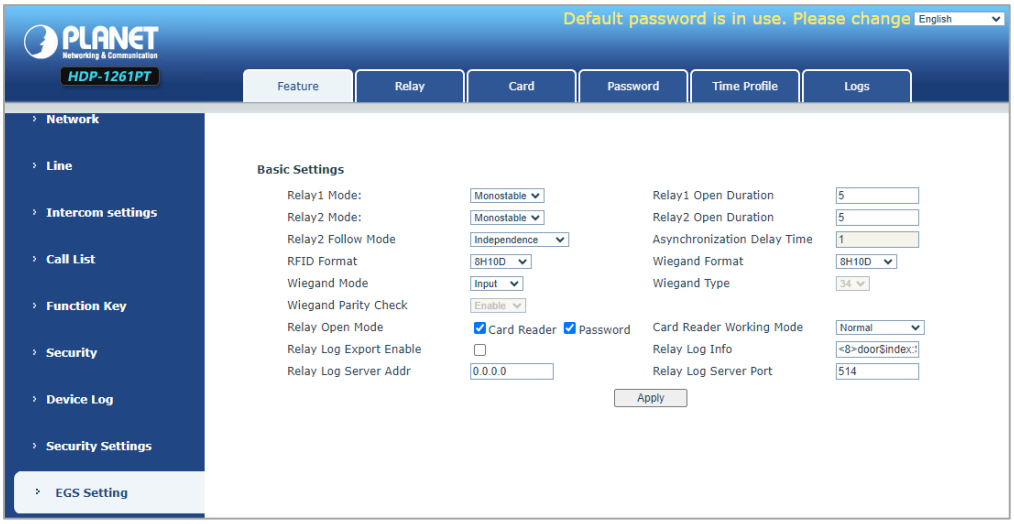
Value: The DSS Key will dial to this value.

+: If value is unavailable, it will be forwarded to another value.

Line: Working line.
Subtype: Speed dial.



Step 4: Door Phone Setting



2.5 Door Unlocking Setting

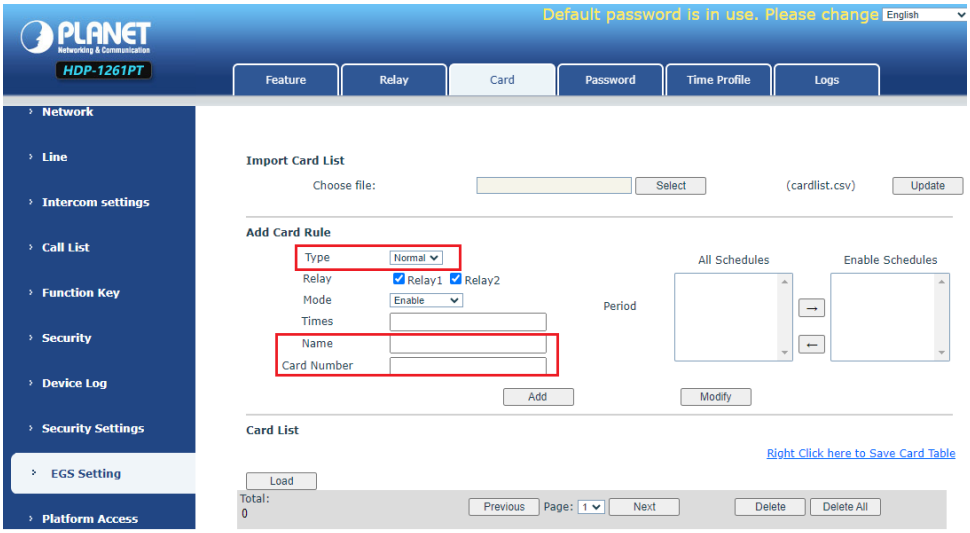
RFID Card

Step 1: Access control settings on web page→EGS Setting→Add Card Rule →Select "Type" ("Normal" card provides door opening function, "Add" card and "Del" card provide add and delete card function, Default "Normal" card)

Step 2: Enter your name and card number (just enter the first 10 digits of the card number), and click "Add" to add the card to the list.

Step3: Access the card reading area of the device through the configured ID card 

to open the door.

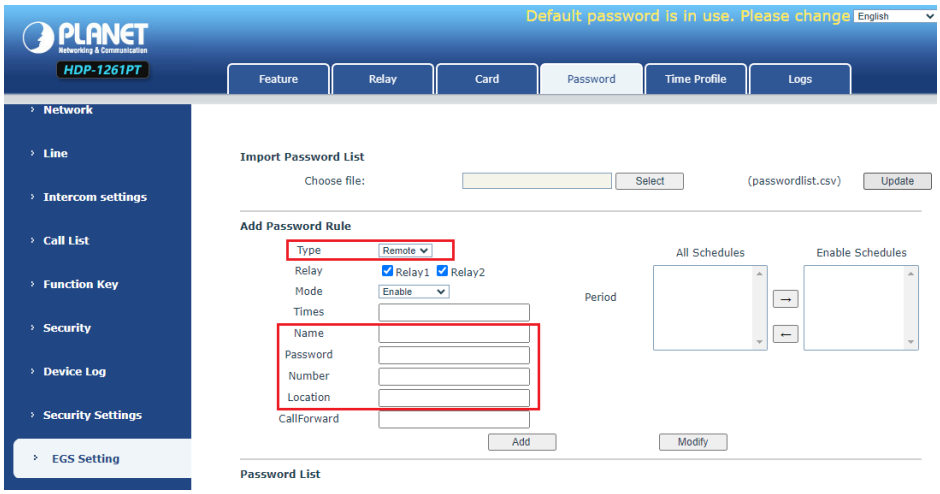


Remote Password

Step 1: Set access control on the web page→ EGS Setting→Password→ Add password rule → Select "Remote "

Step 2: Enter the Name, Password and Number. Press Add to Password Table.

Step 3: The owner answers the access control call and presses " * " (default password) or "123456" (new password) to open the door for visitors.



Chapter 3. Basic Function

3.1 Swipe to Open the Door

Access control settings on **web page → EGS Setting → Card → Add Card Rule → Select " Type"** (Normal card provides open door function, Add card and Del card provide add and delete card function.Default is Normal card).

- Enter your name and card number (just enter the first 10 digits of the card number), and click "Add" to add the card to the list.
- Access the card reading area of the device through the configured ID card 

to open the door.

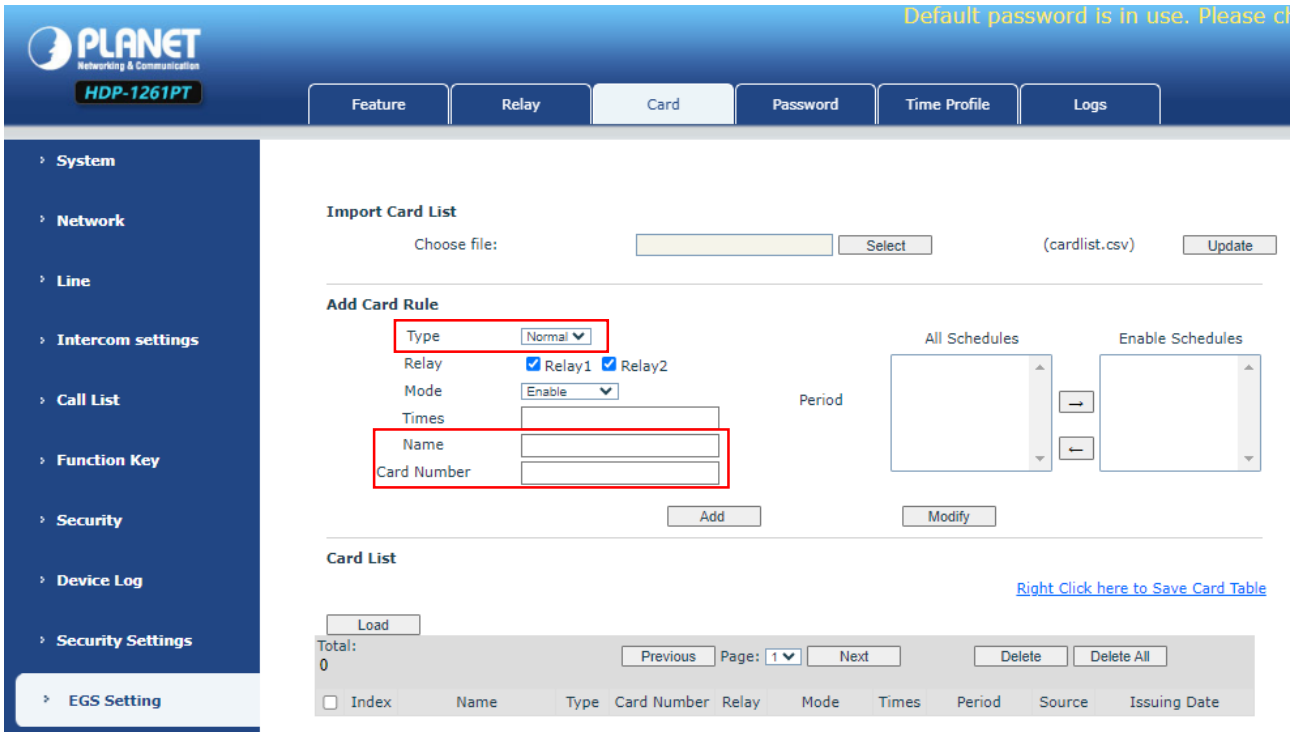


Figure 3-1-1 Card Setting Page Screenshot

3.2 Remote Door Opening

- Set access control on the **web page → EGS Setting → Password → Add password rule → Select "Remote "**
- Enter your name, password and number, add to the password list.
- The owner answers the access control call and presses " * "(default password) or "123456" (new password) to open the door for visitors.

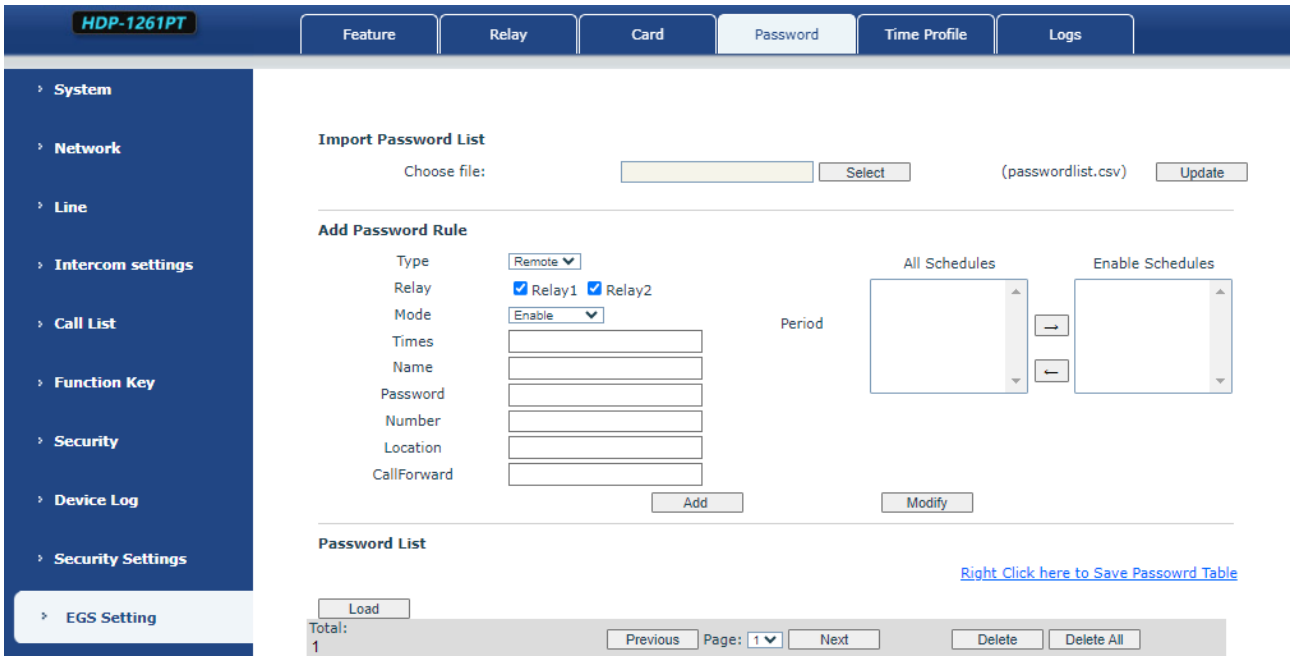


Figure 3-2-1 Remote Door Opening Setting Page Screenshot

3.3 Making Calls

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

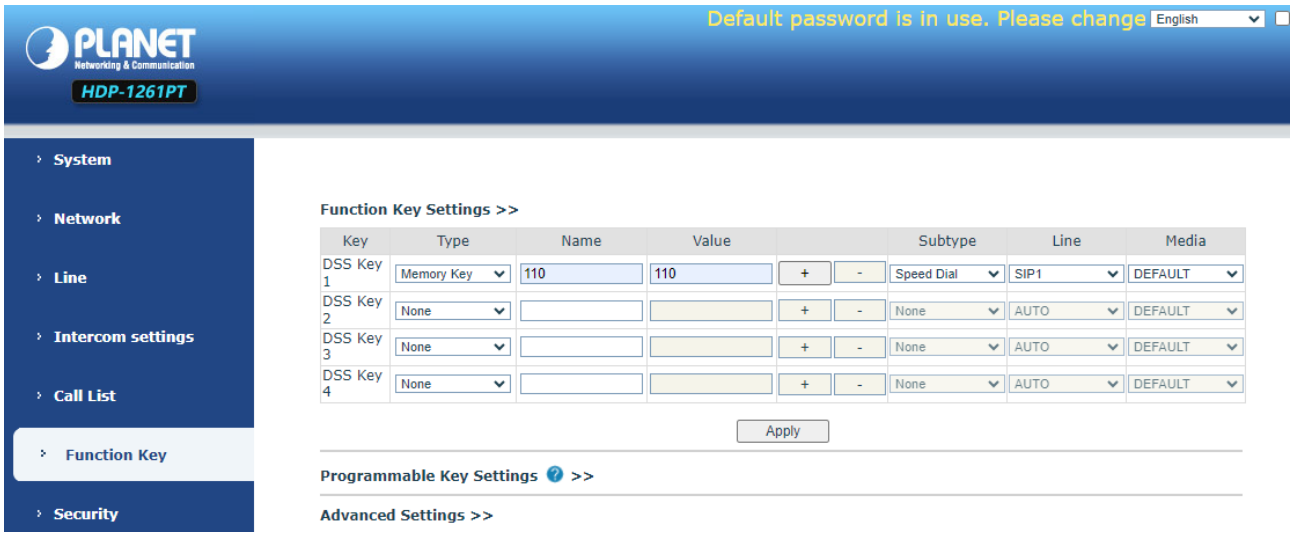


Figure 3-3-1 Function Setting Page Screenshot

After setting the speed dial according to the above settings, you can directly dial the set number by pressing the button  .

3.4 Answering Calls

After setting up the automatic answer and setting up the automatic answer time, it will hear the ringing bell within the set time and automatically answer the call after timeout. Cancel automatic answering. When a call comes in, you will hear the ringing bell and will not answer the phone over time.

3.5 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.

3.6 Auto Answer

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 [**Line**] >> [**SIP**], Enable auto answer and set auto answer time and click submit.

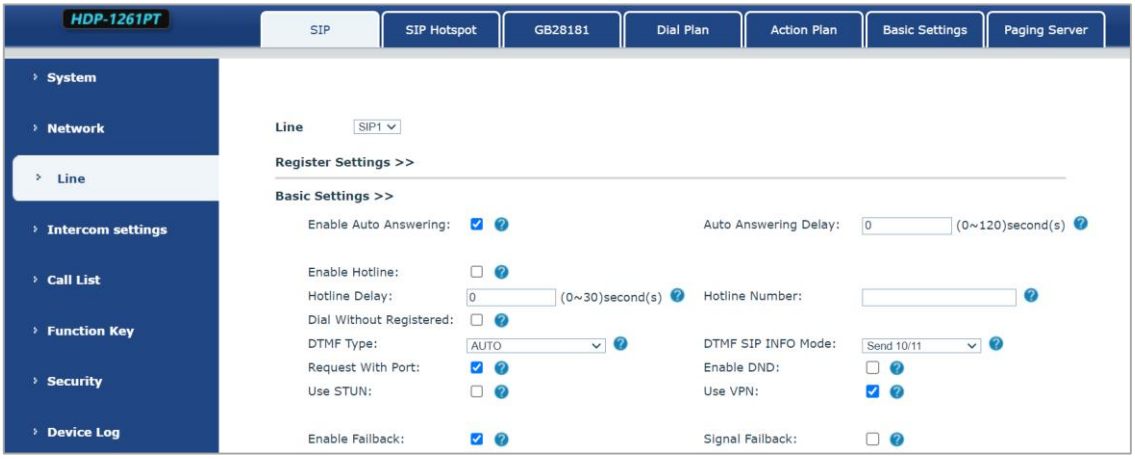


Figure 3-6-1 Line Enable Auto Answer Setting Page Screenshot

SIP P2P auto answering：

Enter [**Line**] >> [**Basic settings**], enable auto answer and set auto answer time and click submit.

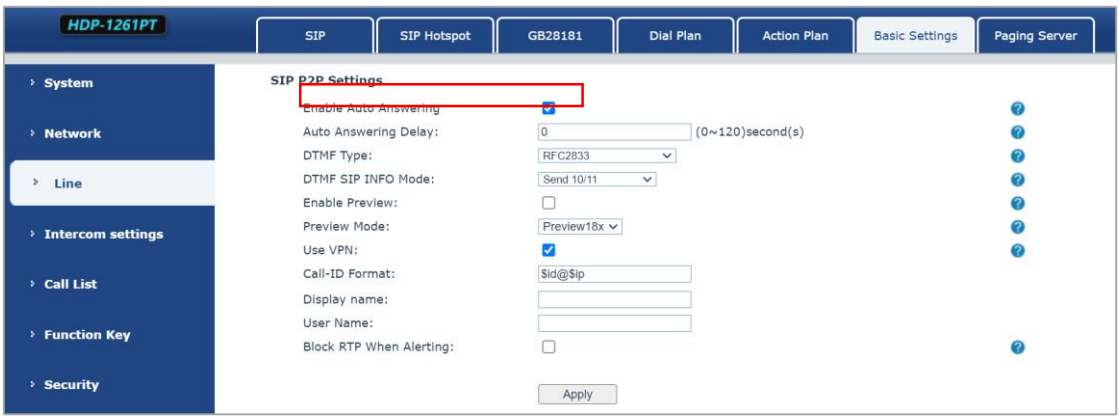


Figure 3-6-2 Enable IP Call Auto Answer Setting Page Screenshot

- Auto Answer Timeout（0~120）

The range can be set to 0~120s, and the call will be answered automatically when the timeout is set.

3.7 Call Waiting

- 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.

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

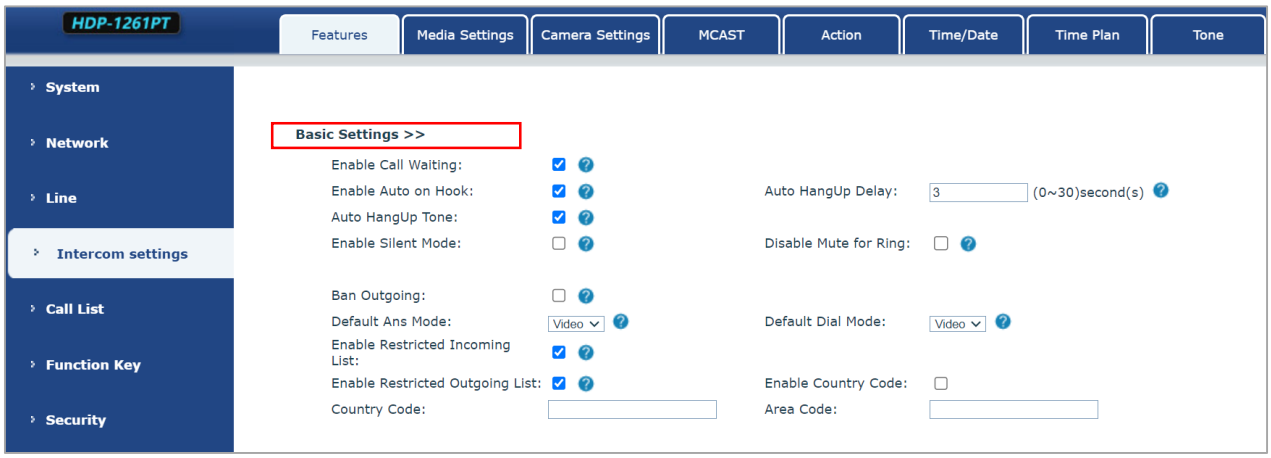


Figure 3-7-1 Call Waiting Setting Page Screenshot

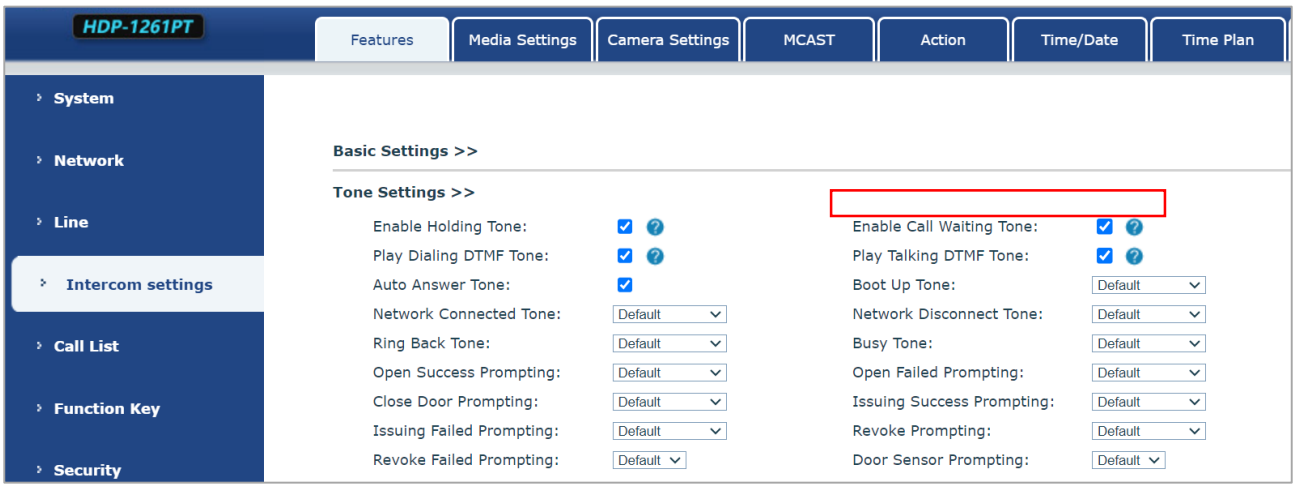


Figure 3-7-2 Call Waiting Tone Setting Page Screenshot

Chapter 4. Advanced Function

4.1 Intercom

The equipment can answer intercom calls automatically.

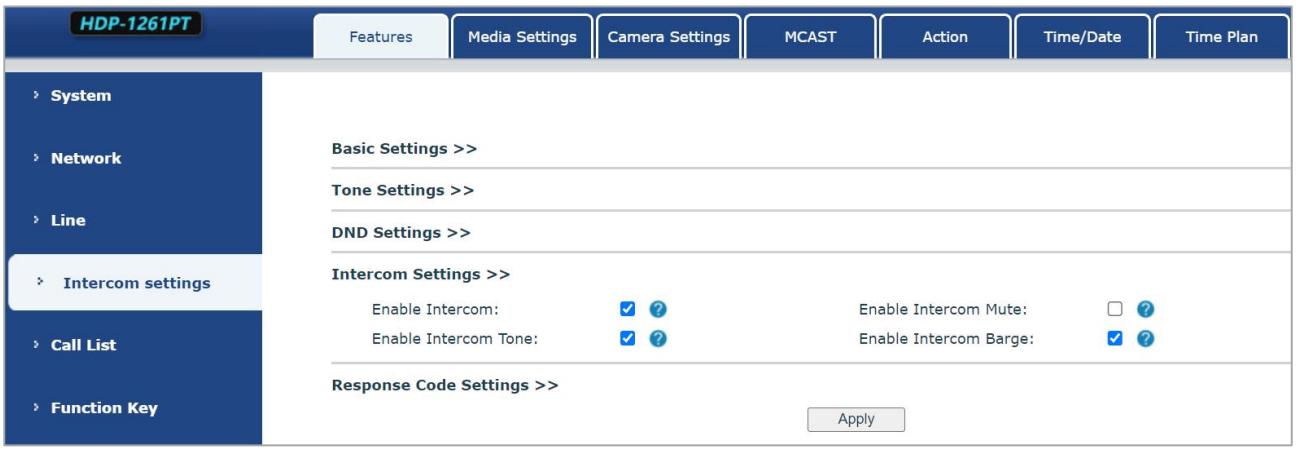


Figure 4-1-1 Intercom Setting Page Screenshot

Parameters	Description
Enable Intercom	When the intercom system is enabled, the device will accept the SIP header call-info of the Call request Command automatic call
Enable Intercom Barge	If the option is enabled, device will answer the intercom call automatically while it is in a normal call, and it will reject new intercom call if there is already one intercom call
Enable Intercom Mute	Enable mute in the intercom mode
Enable Intercom Ringing	If the incoming call is intercom call, the device will play the intercom tone.

4.2 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.

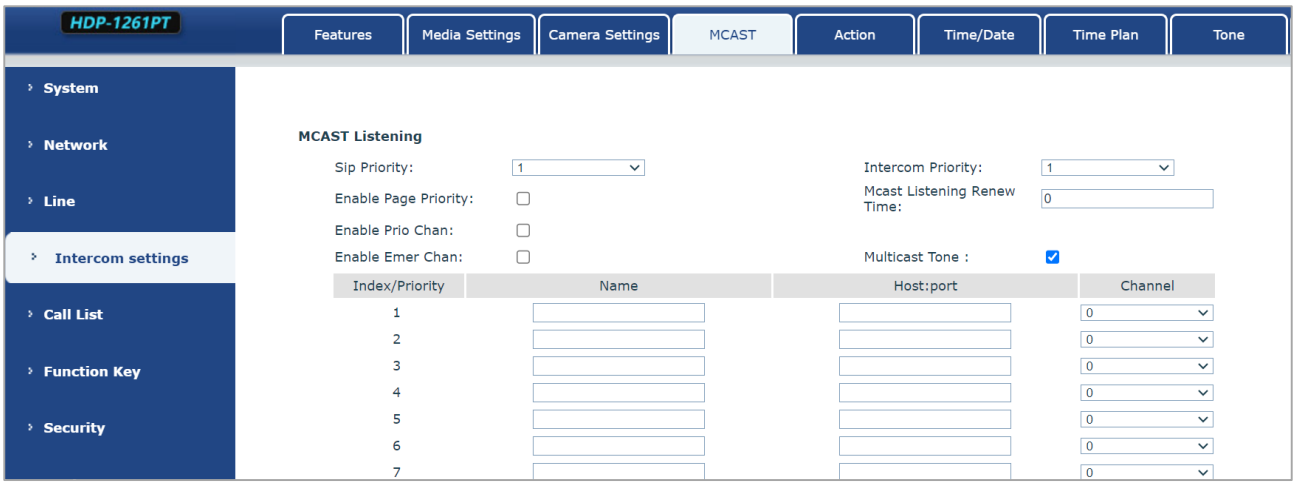


Figure 4-2-1 MCAST Setting Page Screenshot

Parameters	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
SIP Priority	Defines the priority in the current call, with 1 being the highest priority and 10 the lowest.
Intercom Priority	Compared with multicast and SIP priority; high priority is pluggable and low priority is rejected
Enable Page Priority	Regardless of which of the two multicast groups is called in first, the device will receive the higher priority multicast first.
Enable Mcast Tone	When enabled, play the prompt sound when receiving multicast
Name	Listened multicast server name
Host: port	Listened multicast server's multicast IP address and port.

Multicast：

- Go to web page of [**Function Key**] >> [**Function Key**], 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 DSSKey of Multicast Key which you set.
- The receiving end will receive multicast call and play multicast automatically.

MCAST Dynamic：

- Description: send multicast configuration information through SIP notify signaling. After receiving the message, the device configures it to the system for multicast monitoring or cancels multicast monitoring in the system.

4.3 Hotspot

SIP hotspot is a simple utility. Its configuration is simple, which can realize the function of group vibration and expand thequantity of SIP account. Take one device A as the SIP hotspot and the other devices (B, C) as the SIP hotspot clients. When someone calls device A, devices A, B, and C will ring, and if any of them answer, the other devices will stop ringing and not be able to answer at the same time. When A B or C device is called out, it is called out with A SIP number registered with device A.

Parameters	Description
Enable Hotspot	Enable or disable hotspot
Mode	This device can only be used as a client
Monitor Type	The monitoring type can be broadcast or multicast. If you want to restrict broadcast packets in the network, you can choose multicast. The type of monitoring on the server side and the client side must be the same, for example, when the device on the client side is selected for multicast, the device on the SIP hotspot server side must also be set for multicast
Monitor Address	The multicast address is used by the client and server when the monitoring type is multicast. If broadcasting is used, this address does not need to be configured, and the system will communicate by default using the broadcast address of the device's WAN port IP
Remote Port	Fill in a custom hotspot communication port. The server and client ports need to be consistent
Name	Fill in the name of the SIP hotspot. This configuration is used to identify different hotspots on the network to avoid connection conflicts
Line Settings	Sets whether to enable the SIP hotspot function on the corresponding SIP line

Client Settings:

As a SIP hotspot client, there is no need to set up a SIP account, which is automatically acquired and configured when the device is enabled. Just change the mode to "client" and the other options are set in the same way as the hotspot.

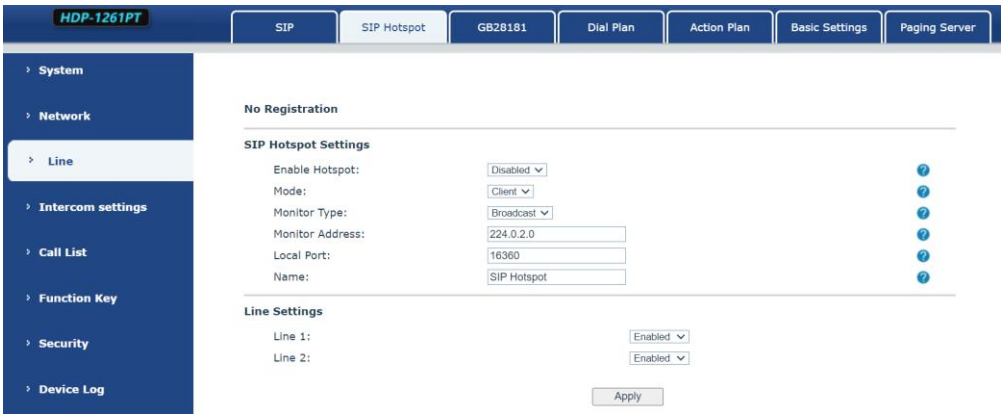


Figure 4-4-1 SIP Hotspot Setting Page Screenshot

The device is the hotspot server, and the default extension is 0. The device acts as a client, and the extension number is increased from 1 (the extension number can be viewed through the [SIP hotspot] page of the webpage).

Calling internal extension:

- The hotspot server and client can dial each other through the extension number before Extension 1 dials extension 0.

Chapter 5. Web Configurations

5.1 Web Page Authentication

Users can log into the device's web page to manage user device information and operate the device. Users must provide the correct user name and password to log in. If the password is entered incorrectly three times, it will be locked and can be entered again after 5 minutes.

The details are as follows:

- If an IP is logged in more than the specified number of times with a different user name, it will be locked. If a user name logs in more than a specified number of times on a different IP, it will also be locked.

5.2 System >> Information

User can get the system information of the device in this page shown below:

- Model
- Hardware
- Software
- Uptime
- Last uptime
- MEM Info
- System time

And summarization of network status,

- Network Mode
- MAC
- IP
- Subnet mask
- Default getaway

Besides, summarization of SIP account status,

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

5.3 System >> Account

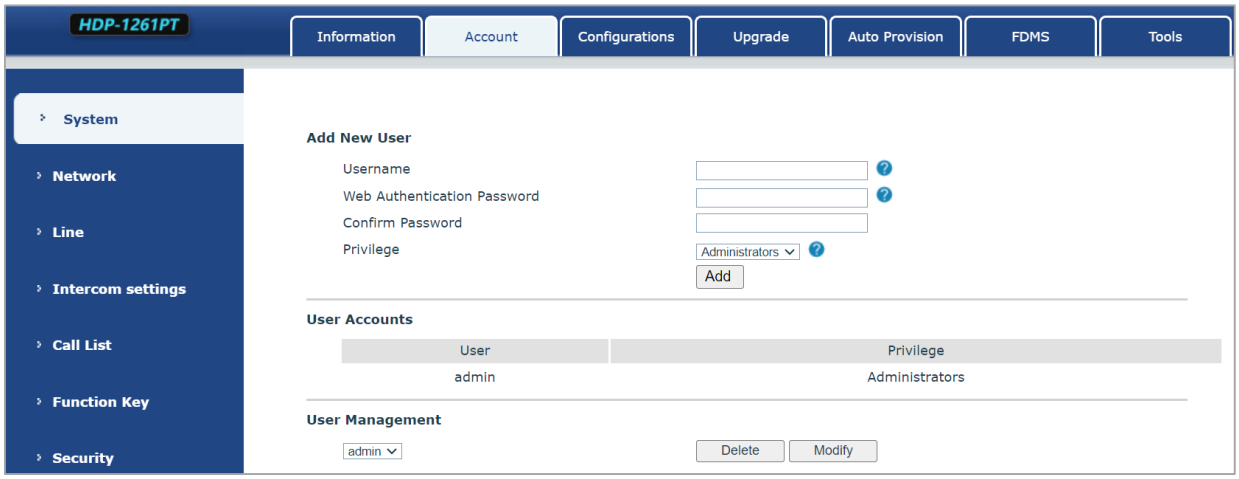


Figure 5-3-1 Account Setting Page Screenshot

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.

5.4 System >> Configurations

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

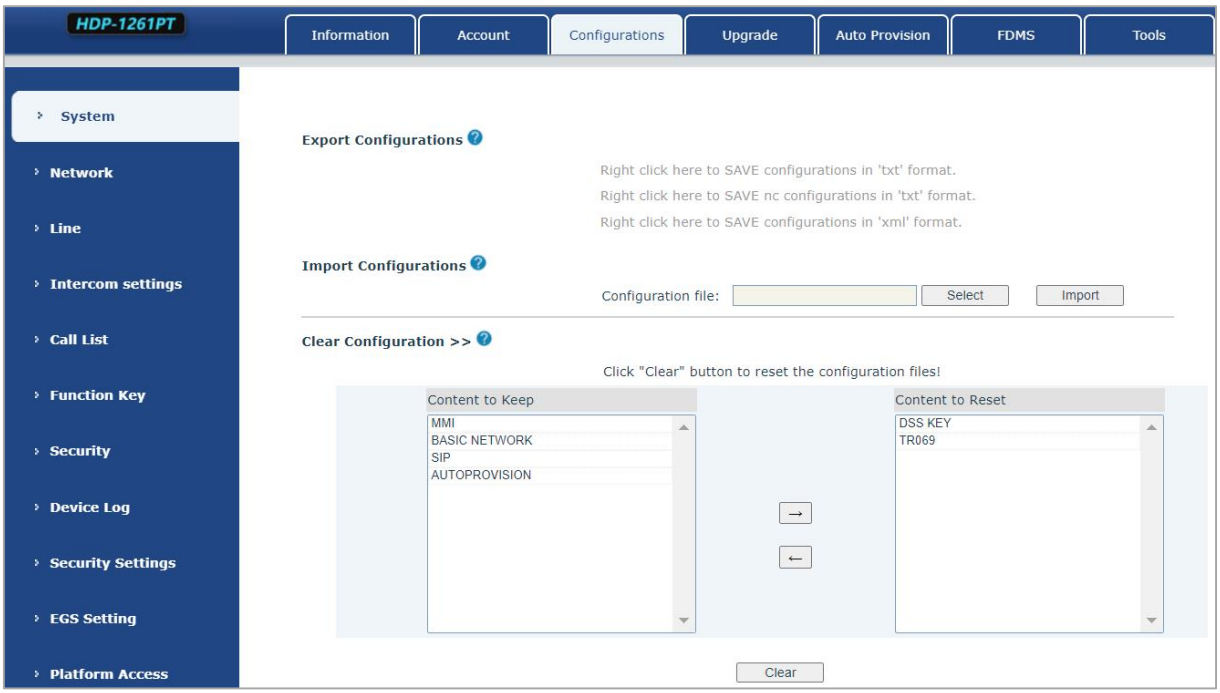


Figure 5-4-1 System Setting Page Screenshot

- **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**

  Import the configuration file of Settings. The device will restart automatically after a successful import, and the configuration will take effect after restart

- **Clear Configurations**

  Select the module in the configuration file to clear.

  SIP: account configuration.

  Auto-provisioning: automatically upgrades the configuration

  TR069:TR069 related configuration

  MMI: MMI module, including authentication user information, web access protocol, etc.

  DSS Key: DSS Key configuration

- **Clear Tables**

  Select the local data table to be cleared; all selected by default.

- **Reset Phone**

  The phone data will be cleared, including configuration and database tables.

5.5 System >> Upgrade

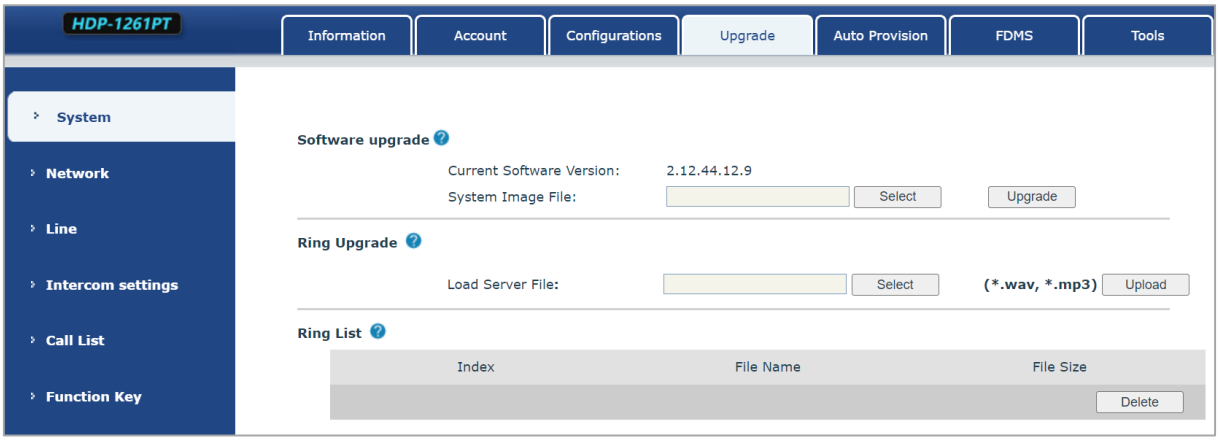


Figure 5-5-1 Upgrade Setting Page Screenshot

Upgrade the software version of the device to a 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. Upgrade the ringtone, support way and MP3 format.

5.6 System >> Auto Provisioning

Webpage: Login and go to [**System**] >> [**Auto provision**].

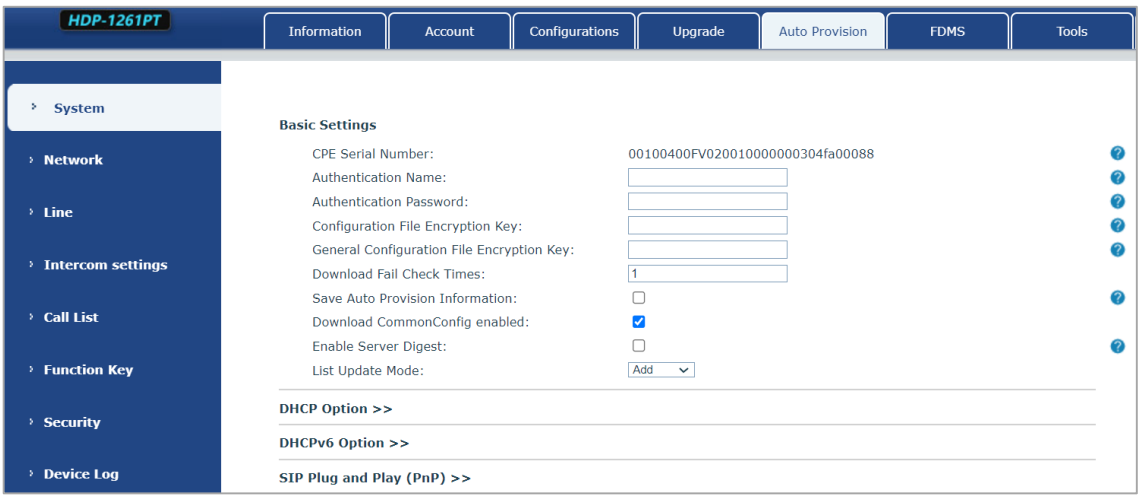


Figure 5-6-1 Auto Provision Setting Page Screenshot

Devices support 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 Provisioning	
Parameters	**Description**
Basic settings	
CPE Serial Number	Display the device SN
Authentication Name	The user name of provision server
Authentication Password	The password of provision server
Configuration File Encryption Key	If the device configuration file is encrypted , user should add the encryption key here
General Configuration File Encryption Key	If the common configuration file is encrypted, user should add the encryption key here
Save Auto Provisioning Information	Save the HTTP/HTTPS/FTP user name and password. If the provision URL is kept, the information will be kept.
Download Common Config enabled	Whether phone will download the common configuration file.
Enable Get Digest From Server	When the feature is enable, if the configuration of server is changed, phone will download and update.
DHCP Option	
Option Value	Configure DHCP option, DHCP option supports DHCP custom option | DHCP option 66 | DHCP option 43, 3 methods to get the provision URL. The default is Option 66.
Custom Option Value	Custom Option value is allowed from 128 to 254. The option value must be same as server define.
Enable DHCP Option 120	Use Option120 to get the SIP server address from DHCP server.
DHCPv6 Option	
Option Value	Configure DHCPv6 option, DHCPv6 option supports custom option | option 66 | option 43, 3 methods to get the provision URL. The default is Disable.
Custom Option Value	Custom option number. Must be from 128 to 254.
Enable DHCP	Set the SIP server address through DHCP option 120.

Option 120	
SIP Plug and Play (PnP)	
Enable SIP PnP	Whether enable PnP or not. If PnP is enabled, phone will send a SIP SUBSCRIBE message with broadcast method. Any server can support the feature that will respond and send a Notify with URL to phone. Phone could get the configuration file with the URL.
Server Address	Broadcast address. As default, it is 224.0.0.0.
Server Port	PnP port
Transport Protocol	PnP protocol, TCP or UDP.
Update Interval	PnP message interval.
Static Provisioning Server	
Server Address	Provisioning server address. Support both IP address and domain address.
Configuration File Name	The configuration file name. If it is empty, phone will request the common file and device file which 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	Transferring protocol type ，supports FTP、TFTP、HTTP and HTTPS
Update Interval	Configuration file update interval time. As default it is 1, means phone will check the update every 1 hour.
Update Mode	Provision Mode. 1. Disabled. 2. Update after reboot. 3. Update after interval.
Static Provisioning Server	
TR069	
Enable TR069	Enable TR069 after selection
ACS Server Type	There are 2 options Serve type, common and CTC.
ACS Server URL	ACS server address
ACS User	ACS server username (up to is 59 character)
ACS Password	ACS server password (up to is 59 character)
Enable TR069 Warning Tone	If TR069 is enabled, there will be a prompt tone when connecting.
TLS Version	TLS Version
STUN server address	Enter the STUN address
Enable the STUN	Enable the STUN

5.7 System >> FDMS

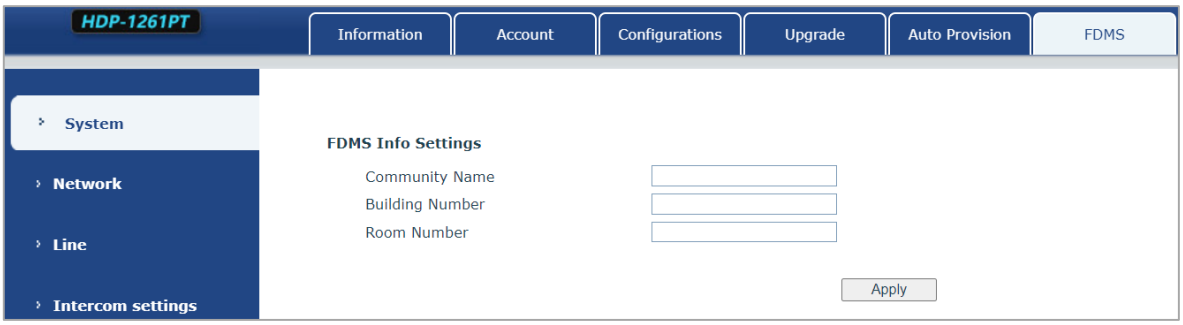


Figure 5-7-1 FDMS Setting Page Screenshot

FDMS information Settings	
Community Designations	Name of equipment installation community
Building a movie theater	Name of equipment installation building
room number	Equipment installation room name

5.8 System >> Tools

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

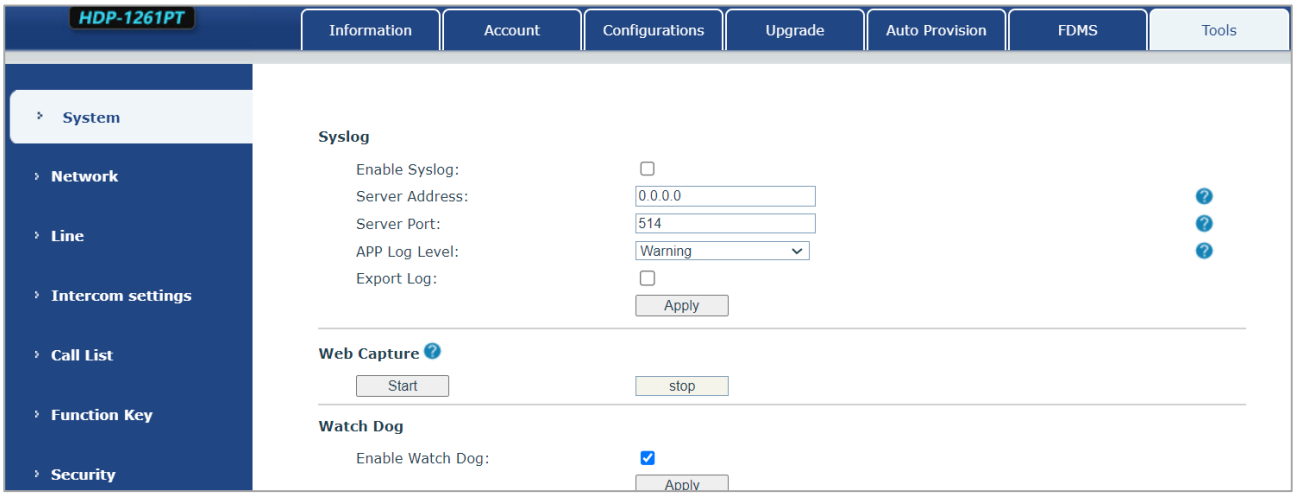
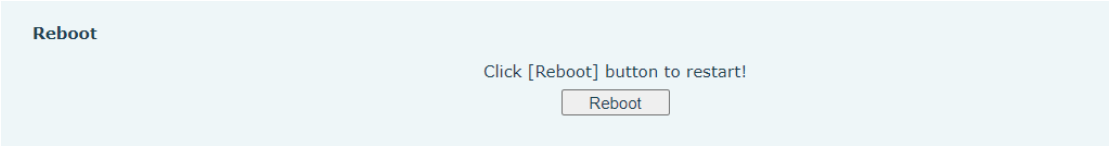


Figure 5-8-1 Tools Setting Page Screenshot

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 technical support.

5.9 System >> Reboot

This page can restart the device.



5.10 Network >> Basic

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

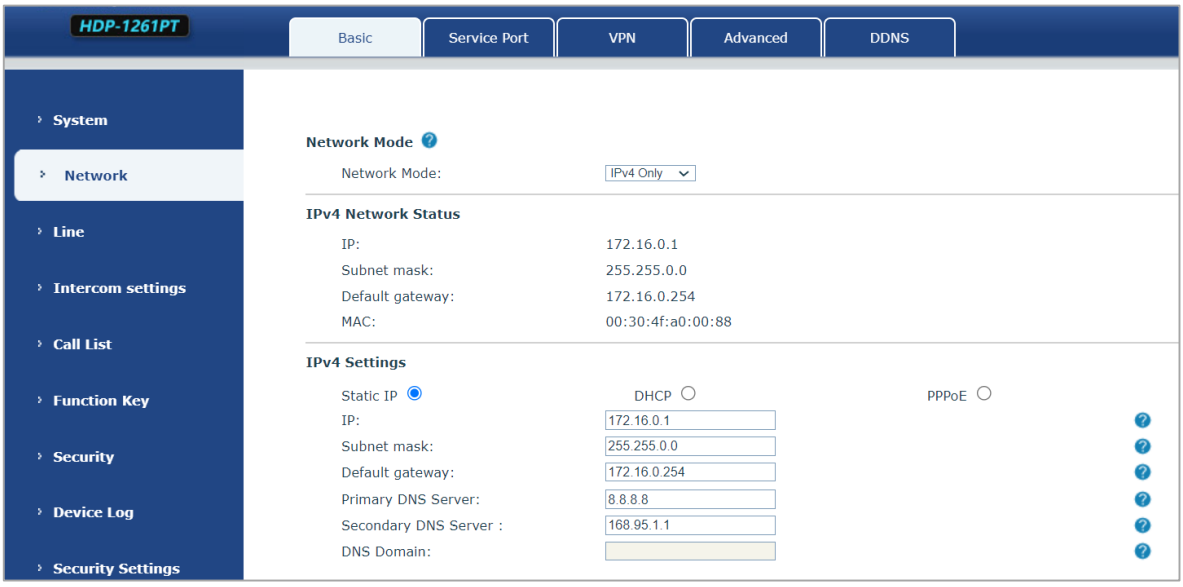


Figure 5-10-1 Network Setting Page Screenshot

Field Name	Explanation
IPv4 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
IPv4 Settings	
Settings	
Select the appropriate network mode. The equipment supports three network modes:	
Static IP	Network parameters must be entered manually and will not be changed. All parameters are provided by the ISP.
DHCP	Network parameters are provided automatically by a DHCP server.
If Static IP 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.
DNS Domain	Enter the domain of the DNS.
Attention: 1）After setting the parameters, click【Apply】to take effect. 2）If you change the IP address, the webpage will no longer respond, please enter the new IP address in web browser to access the device. 3）If the system USES DHCP to obtain IP when device boots up, 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	

5.11 Network >> Service Port

This page provides the settings of webpage login protocol, protocol port and RTP port.

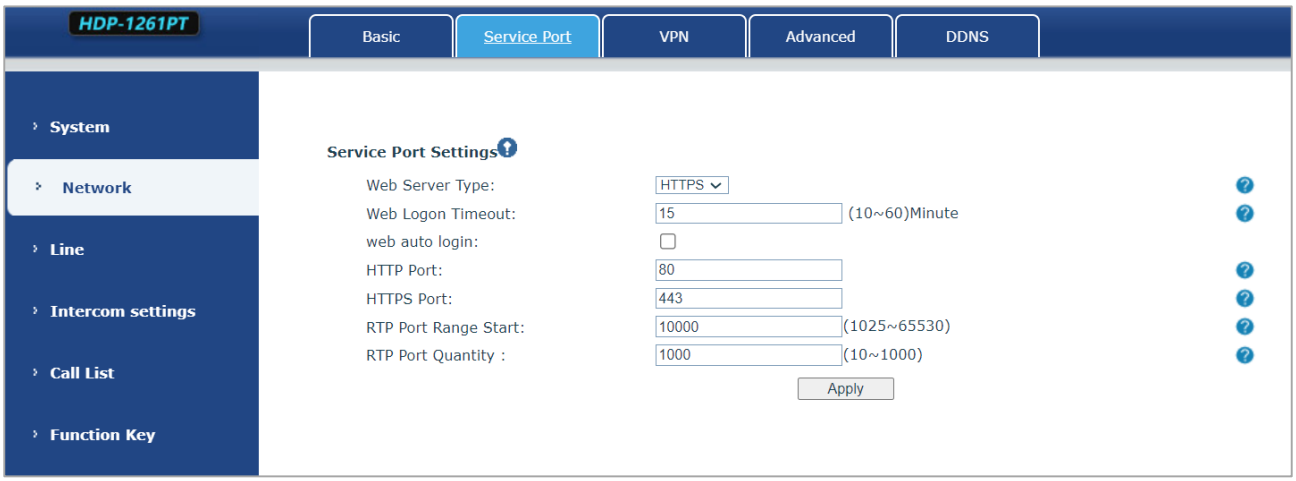


Figure 5-11-1 Service Port Setting Page Screenshot

parameter	description
Web server type	Restart after setting takes effect. Optional web login as HTTP/HTTPS
Web login timeout	The default is 15 minutes, the timeout will automatically log out of the login page, and you need to log in again
Web page automatic login	No need to enter the user name and password after the timeout, it will automatically log in to the web page.
HTTP port	The default is 80, if you want system security, you can set other port Such as: 8080, web page login: HTTP://ip:8080
HTTPS port	The default is 443, same as HTTP port usage
RTP port start range	The value range is 1025-65535. The value of rtp port starts from the initial value set. Each time a call is made, the value of the voice and video ports is increased by 2
RTP port quantity	Number of calls

5.12 Network >> VPN

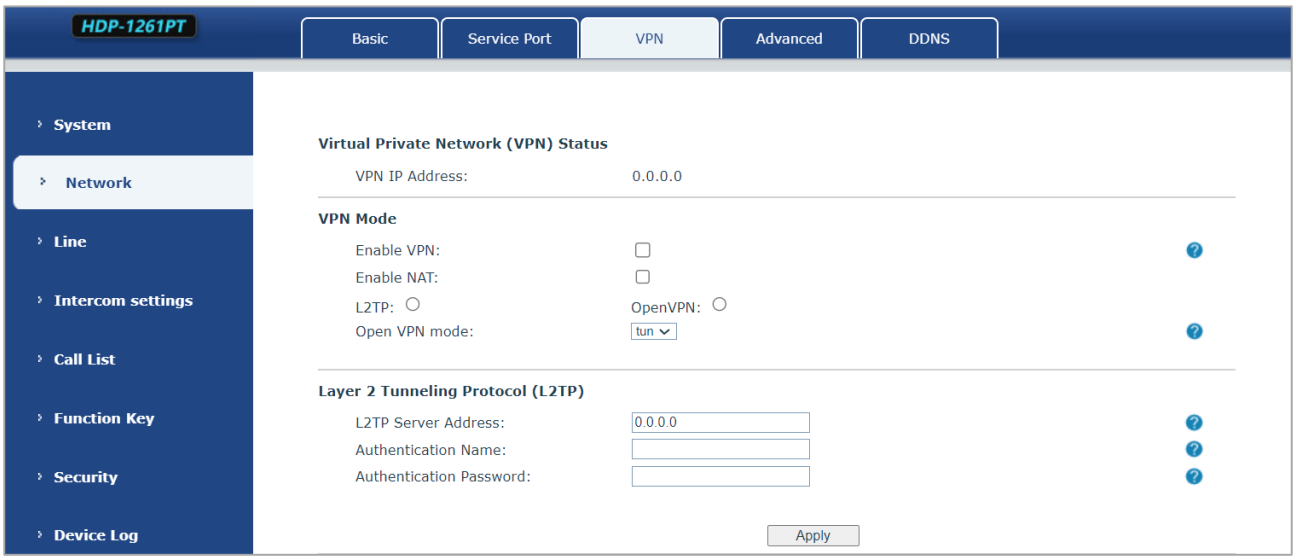


Figure 5-12-1 Service Port Setting Page Screenshot

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 activate 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

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

To establish a L2TP connection, users should log in to the device web portal, open page [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 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 to the VPN automatically when the device boots up every time until user disable it. Sometimes, if the VPN connection does not established immediately, user may try to reboot the device and check if VPN connection established after reboot.

■ OpenVPN

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

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

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

Same as L2TP connection, the connection will be established every time when system rebooted until user disable it manually.

5.13 Network >> Advanced

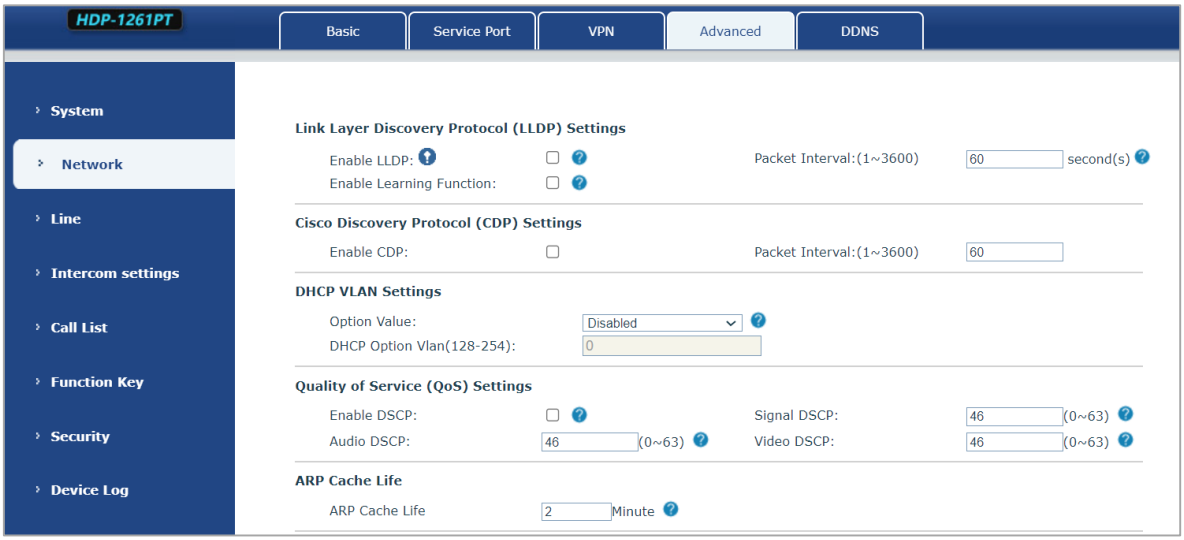


Figure 5-13-1 Network Advanced Setting Page Screenshot

Network advanced Settings are typically configured by IT administrators to improve the quality of device service.

Field Name	Explanation
LLDP Settings	
Enable LLDP	Enable or disable LLDP
Packet Interval	LLDP Send detection cycle
Enable Learning Function	Learn the discovered device information on the device
QoS Settings	
Pattern	Voice quality assurance (off by default)
DHCP VLAN Settings	
parameters values	128-254，Obtain the VLAN value through DHCP
WAN port virtual Wan	
WAN port virtual Wan	WAN port Settings
LAN port virtual LAN	
LAN port virtual LAN	LAN port Settings
802.1X	
Enable 802.1X	Enable or disable 802.1X
Username	Confirm Username
Password	Confirm Password

5.14 Network >> DDNS

This page provides the settings of DDNS. The default is Disable. You can choose PLANET DDNS or Easy DDNS.

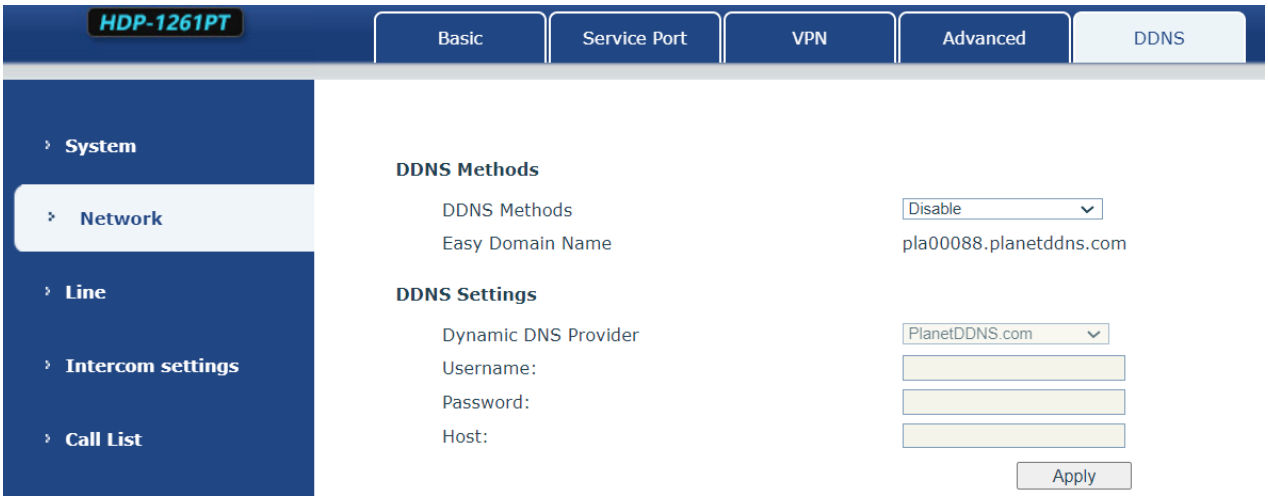


Figure 5-14-1 DDNS Setting Page Screenshot

5.15 Line >> SIP

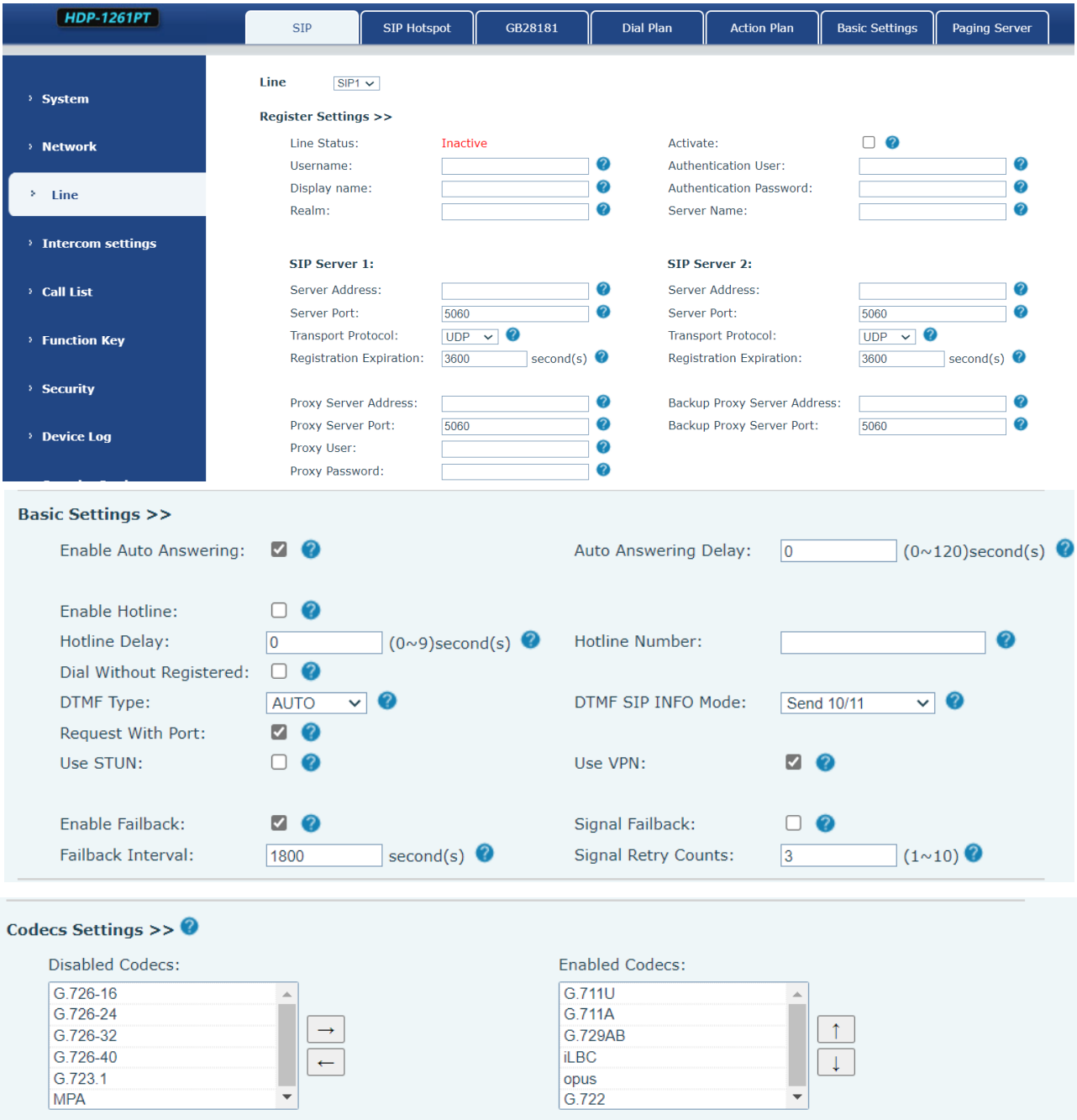


Figure 5-15-1 SIP Setting Page Screenshot

Parameters	Description
Register Settings	
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.
Activate	Whether the service of the line should be activated
Username	Enter the username of the service account.
Authentication User	Enter the authentication user of the service account

Display Name	Enter the display name to be sent in a call request.
Authentication Password	Enter the authentication password of the service account
Realm	Enter the SIP domain if requested by the service provider
Server Name	Input server name.
SIP Server 1	
Server Address	Enter the IP or FQDN address of the SIP server
Server Port	Enter the SIP server port, default is 5060
Transport Protocol	Set up the SIP transport line using TCP or UDP or TLS.
Registration Expiration	Set SIP expiration date.
SIP Server 2	
Server Address	Enter the IP or FQDN address of the SIP server
Server Port	Enter the SIP server port, default is 5060
Transport Protocol	Set up the SIP transport line using TCP or UDP or TLS.
Registration Expiration	Set SIP expiration date.
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server.
Proxy Server Port	Enter the SIP proxy server port, default is 5060.
Proxy User	Enter the SIP proxy user.
Proxy Password	Enter the SIP proxy password.
Backup Proxy Server Address	Enter the IP or FQDN address of the backup proxy server.
Backup Proxy Server Port	Enter the backup proxy server port, default is 5060.
Basic Settings	
Enable Auto Answering	Enable auto-answering, the incoming calls will be answered automatically after the delay time
Auto Answering Delay	Set the delay for incoming call before the system automatically answered it
Enable Hotline	Enable hotline configuration, the device will dial to the specific number immediately at audio channel opened by off-hook handset or turn on hands-free speaker or headphone
Hotline Delay	Set the delay for hotline before the system automatically dialed it
Hotline Number	Set the hotline dialing number
Dial Without Registered	Set call out by proxy without registration

Enable Missed Call Log	If enabled, the phone will save missed calls into the call history record.
DTMF Type	Set the DTMF type to be used for the line
Use VPN	Set the line to use VPN restrict route
Use STUN	Set the line to use STUN for NAT traversal
Enable Failback	Whether to switch to the primary server when it is available.
Failback Interval	A Register message is used to periodically detect the time interval for the availability of the main Proxy.
Signal Failback	Multiple proxy cases, whether to allow the invite/register request to also execute failback.
Signal Retry Counts	The number of attempts that the SIP Request considers proxy unavailable under multiple proxy scenarios.
Codecs Settings	Set the priority and availability of the codecs by adding or remove them from the list.
Advanced Settings	
Use Feature Code	When this setting is enabled, the features in this section will not be handled by the device itself but by the server instead. In order to control the enabling of the features, the device will send feature code to the server by dialing the number specified in each feature code field.
Enable Blocking Anonymous Call	Set the feature code to dial to the server
Disable Blocking Anonymous Call	Set the feature code to dial to the server
Call Waiting On Code	Set the feature code to dial to the server
Call Waiting Off Code	Set the feature code to dial to the server
Send Anonymous on Code	Set the feature code to dial to the server
Send Anonymous Off Code	Set the feature code to dial to the server
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

BLF Server	The registered server will receive the subscription package from ordinary application of BLF phone. Please enter the BLF server, if the sever does not support subscription package, the registered server and subscription server will be separated.
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
Keep Authentication	Keep the authentication parameters from previous authentication
Blocking Anonymous Call	Reject any incoming call without presenting caller ID
User Agent	Set the user agent, the default is Model with Software Version.
Specific Server Type	Set the line to collaborate with specific server type
SIP Version	Set the SIP version
Anonymous Call Standard	Set the standard to be used for anonymous
Local Port	Set the local port
Ring Type	Set the ring tone type for the line
Enable user=phone	Sets user=phone in SIP messages.
Use Tel Call	Set use tel call
Auto TCP	Using TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes
Enable Rport	Set the line to add rport in SIP headers
Enable PRACK	Set the line to support PRACK SIP message
DNS Mode	Select DNS mode, A, SRV, NAPTR
Enable Long Contact	Allow more parameters in contact field per RFC 3840
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.
Convert URI	Convert not digit and alphabet characters to %hh hex code
Use Quote in Display Name	Whether to add quote in display name, i.e. “VoIP” vs VoIP
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)
Sync Clock Time	Time Sync with server
Enable Inactive Hold	With the post-call hold capture package enabled, you can see that in the INVITE package, SDP is inactive.
Caller ID Header	Set the Caller ID Header
Use 182 Response	Set the device to use 182 response code at call waiting response

for Call waiting	
Enable Feature Sync	Feature Sync with server
Enable SCA	Enable/Disable SCA (Shared Call Appearance)
CallPark Number	Set the CallPark number.
Server Expire	Set the timeout to use the server.
TLS Version	Choose TLS Version.
uaCSTA Number	Set uaCSTA Number.
Enable Click to Talk	With the use of special server, click to call out directly after enabling.
Enable Chgport	Whether port updates are enabled.
Intercom Number	Set Intercom Number.
Unregister On Boot	Whether to enable logout function.
Enable MAC Header	Whether to open the registration of SIP package with user agent with MAC or not.
Enable Register MAC Header	Whether to open the registration is user agent with MAC or not.
PTime(ms)	Set whether to bring ptime field, default no.
SIP Global Settings	
Strict Branch	Set up to strictly match the Branch field.
Enable Group	Set open group.
Enable RFC4475	Set to enable RFC4475.
Enable Strict UA Match	Enable strict UA matching.
Registration Failure Retry Time	Set the registration failure retry time.
Local SIP Port	Modify the phone SIP port.
Enable uaCSTA	Set to enable the uaCSTA function.

5.16 Line >> SIP Hotspot

SIP hotspot is a simple and practical function. It is simple to configure, can realize the function of group vibration, and can expand the number of SIP accounts.

5.17 Line >> Dial Plan

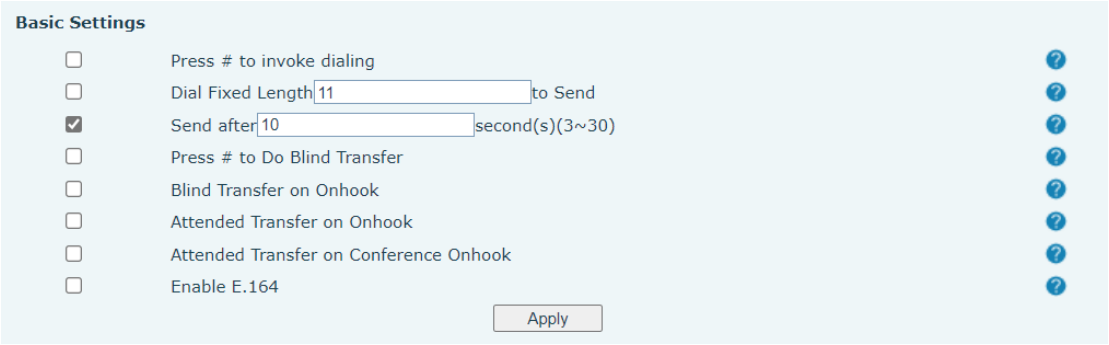


Figure 5-17-1 Dial Plan Setting Page Screenshot

Parameters	Description
Press # to invoke dialing	The user dials the other party's number and then adds the # number to dial out;
Dial Fixed Length	The number entered by the user is automatically dialed out when it reaches a fixed length
Timeout dial	The system dials automatically after timeout

Dial Plan Add:

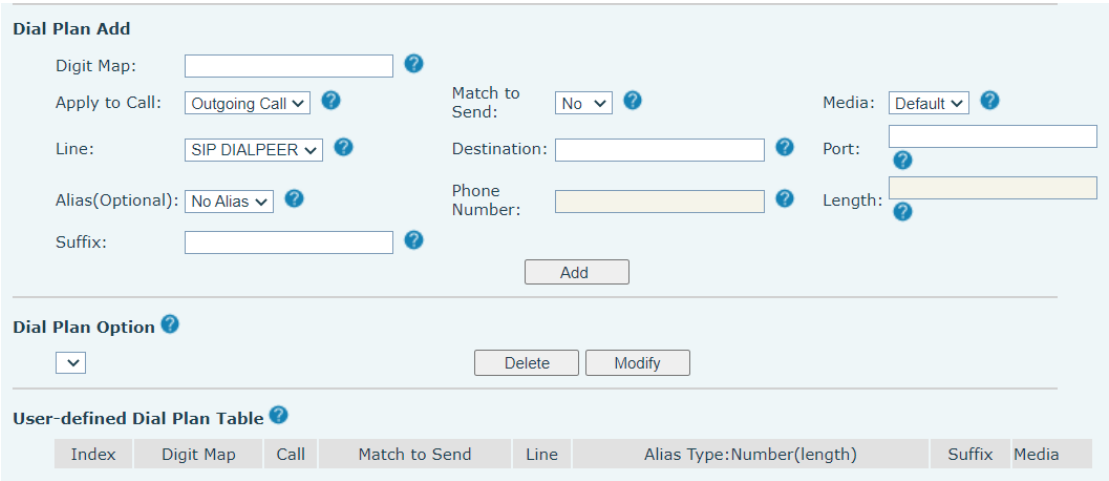


Figure 5-17-2 Dial Plan Add Setting Page Screenshot

Parameters	Description
Dial rule	There are two types of matching: Full Matching or Prefix Matching. In Full matching, the entire phone number is entered and then mapped per the Dial Peer rules. In prefix matching, only part of the number is entered followed by T. The mapping with then take place whenever these digits are dialed. Prefix mode supports a maximum of 30 digits.
Note: Two different special characters are used. ■ x -- Matches any single digit that is dialed. ■ [ ] -- Specifies a range of numbers to be matched. It may be a range, a list of ranges separated by commas, or a list of digits.	
Destination	Set Destination address. This is for IP direct.
Port	Set the Signal port, and the default is 5060 for SIP.
Alias	Set the Alias. This is the text to be added, replaced or deleted. It is an optional item.
Note: There are four types of aliases. ■ all: xxx – xxx will replace the phone number. ■ add: xxx – xxx will be dialed before any phone number. ■ del –The characters will be deleted from the phone number. ■ rep: xxx – xxx will be substituted for the specified characters.	
Suffix	Characters to be added at the end of the phone number. It is an optional item.
Length	Set the number of characters to be deleted. For example, if this is set to 3, the phone will delete the first 3 digits of the phone number. It is an optional item.

This feature allows the user to create rules to make dialing easier. There are several different options for dialing rules. The examples below will show how this can be used.

5.18 Line >> Action Plan

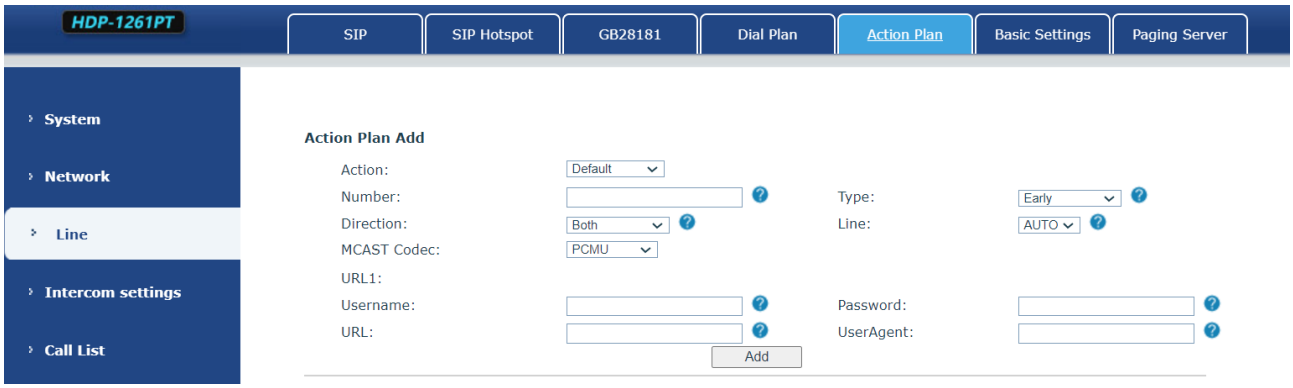
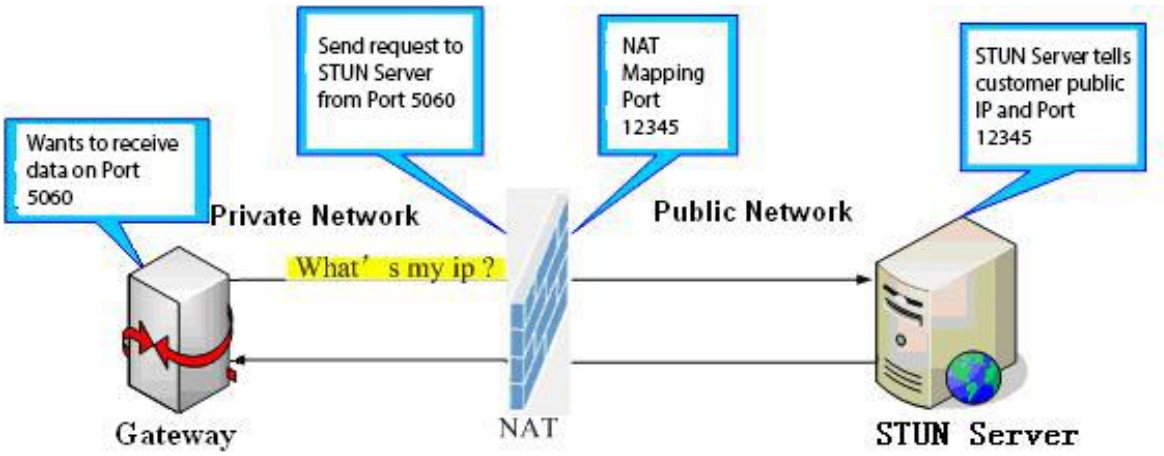


Figure 5-18-1 Action Plan Setting Page Screenshot

Parameter	Description
Number	Auxiliary phone number (support video)
Type	Support video display on call.
Direction	For call mode, incoming/outgoing call displays video
Line	Set up outgoing lines.
Username	Bind the user name of the IP camera.
Password	Bind IP camera password.
URL	Video streaming information.
User Agent	Set user agent information
MCAST Codec	Set mcast codec
Action	Select action

5.19 Line >> Basic Settings

A STUN (Simple Traversal of UDP through NAT) 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.



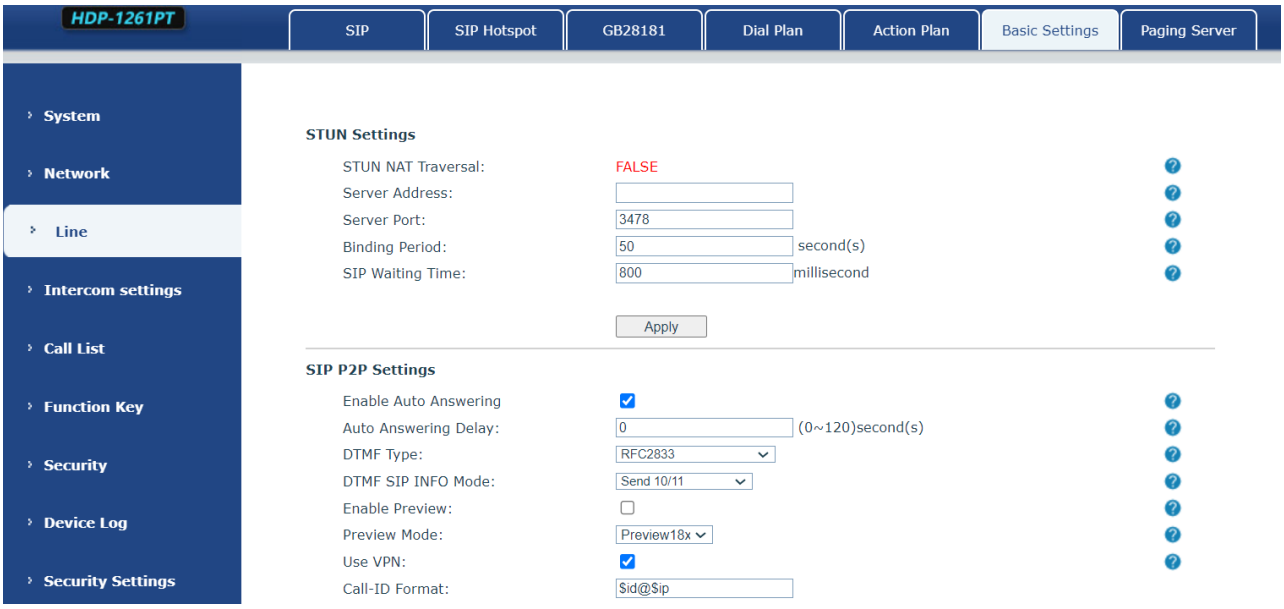


Figure 5-19-1 STUN Setting Page Screenshot

Parameters	Description
STUN Settings	
Server Address	Set the STUN server address
Server Port	Set the STUN server port, default is 3478
Binding Period	Set the STUN binding period which can be used to keep the NAT pinhole opened.
SIP Waiting Time	Set the timeout of STUN binding before sending SIP messages
SIP P2P Settings	
Enable Auto Answering	Automatically answer incoming IP calls after the timeout period is enabled
Auto Answering Delay	Automatic answer timeout setting
DTMF Type	Set the DTMF type of the line.
DTMF SIP INFO Mode	Set SIP INFO mode to send '*' and '#' or '10' and '11'

5.20 Intercom Setting >> Features

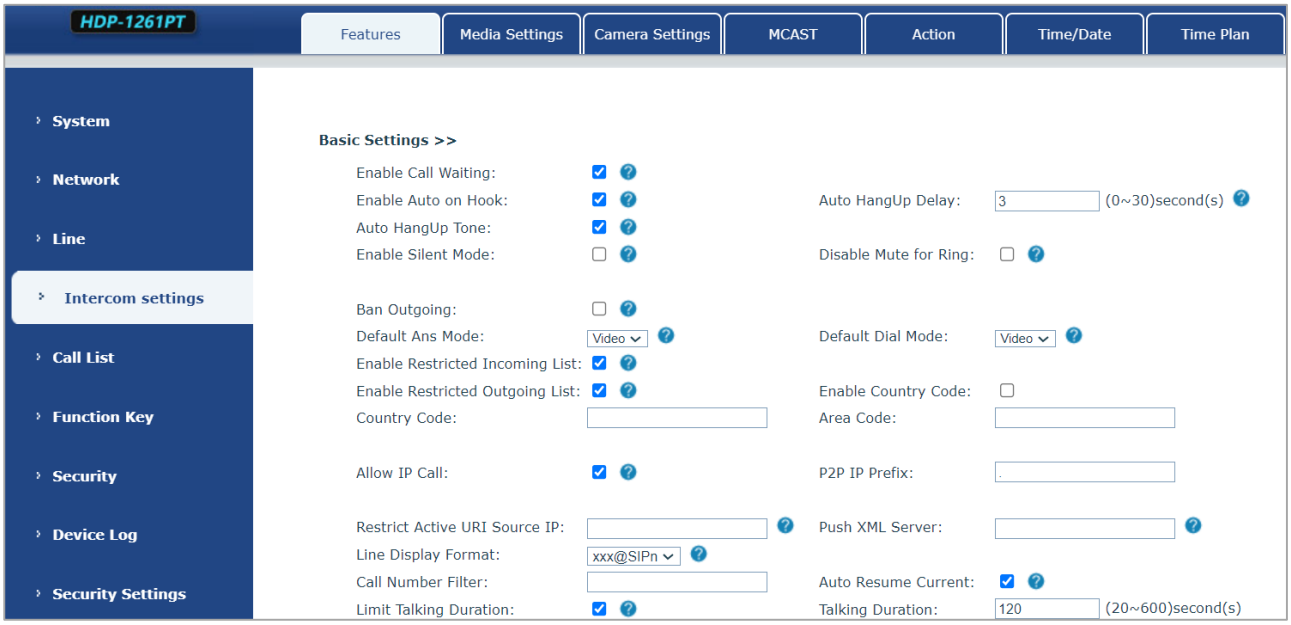


Figure 5-20-1 Intercom Features Setting Page Screenshot

Parameters	Description
Basic Settings	
Enable Call Waiting	Enable this setting to allow user to take second incoming call during an established call. “enabled” by default.
Enable Auto Handdown	The phone will hang up and return to idle automatically in the hands-free mode
Auto Handdown Time	The phone will automatically disconnect and return to idle mode after the Auto Hand Down time elapses in hands-free mode. In handset mode, it will play the dial tone after the Auto Hand Down time is completed.
Enable Silent Mode	When enabled, the phone is in a muted state, preventing ringing during calls. To unmute, you can utilize the volume keys and the mute key.
Disable Mute for Ring	When it is enabled,you cannot mute the phone.
Ban Outgoing	If you select Ban Outgoing, you cannot dial out any number.
Default Reply Mode	Select the default mode after an incoming call, including Video and Audio
Default Dial Mode	Specify the default mode for both video and audio after dialing.
Enable Restricted Incoming List	Specify whether to enable the Restricted Incoming List.
Enable Restricted Outgoing List	Specify whether to enable the Restricted Outgoing List.
Enable Country Code	Specify whether to enable Country Code.
Country Code	Country Code
Area Code	Area Code
Allow IP Call	If enabled, user can dial out with IP address.
P2P IP Prefix	You can configure an IP call prefix; for instance, setting it as "172.16.2." means that inputting #160 in the dialpad and pressing the dial key will automatically initiate a call to 172.16.2.160.
Restrict Active URI Source IP	Set the device to accept Active URI command from specific IP address.
Push XML Server	When the phone receives a request, it will assess whether to display the corresponding content sent by the specified server on the phone or not.
Line Display Format	Line display format includes SIPn/SIPn: xxx/xxx@SIPn
Call Number Filter	Configure a special character "&" such that if the number includes

	"78&9," the call will be filtered out.
Auto Resume Current	If the current path changes, the hold will be automatically resume.
Limit Talking Duration	Automatically terminate the call once the designated time limit has been enabled.
Talking Duration	Specify a call duration within the range of 20 to 600 seconds.
No Answer Auto HangUp Timeout	If the call is not answered, the call will be automatically hung up after the timeout.
Enable Push XML Auth	To enable push xml auth, user password is required.
Ringing timeout	If the call is not answered, it will automatically hang up after timeout.
Show Description Information	Show description information on the IP scan tool software. Default is "IP Video Doorphone".
Tone Settings	
Enable Holding Tone	When activated, a tone will be played when the call is placed on hold.
Enable Call Waiting Tone	When enabled, a tone will be played for call waiting notifications.
Play Dialing DTMF Tone	By default, play a DTMF tone on the device when the user presses a phone digit during dialing.
Play Talking DTMF Tone	By default, play DTMF tones on the device when the user presses phone digits during a call.
Auto-answer beep	When switched on, a beep will be heard when the auto-answer is activated.
Tone of opening door successfully	Closed: No prompt tone is played after the door is opened successfully. Default: Use the default prompt tone. Voice: Include a built-in voice prompt with the default message set to "open the door successfully." The system supports customization of the door opening success prompt tone, which can be modified in the system settings under "Upgrade" and "Ringtone." This customization can also be done after the door is opened and the ringtone file upgrade is successful.
Tone of opening door unsuccessfully	Closed: There is no prompt tone after the door fails to open Default: Use the default prompt tone Voice: Include a default built-in voice prompt that states "failed to open the door" in case of unsuccessful attempts. The system supports customization of the door opening failure prompt tone. This customization can be done in the system settings under "Upgrade"

	and "Ringtone," or after a failed attempt to open the door, if the ringtone file upgrade is unsuccessful.
Door closing beep	Close: No beep is expected after closing the door. Default: Use the default beep. Voice: The default built-in voice prompt is set to "Close." The system supports the customization of the door closing tone. Users can set a custom door closing tone in the system settings under "Upgrade" and "Ringtones." After upgrading the ringtone file, it can be applied to the door closing settings for a personalized experience.
Successful card addition beep	Close: No beep after successful card addition Default: Use the default beep Voice: The default built-in voice prompt is set to "Card added successfully." The system supports the customization of the beep for successful card addition. Users can set a custom beep in the system settings under "Upgrade" and "Ringtones." After upgrading the ringtones file, the custom beep can be applied to the settings for successful card addition.
Add card failure beep	Close: No beep after failed card addition Default: Use the default beep Voice: The default built-in voice prompt is set to "Card refill failed." The system supports customization of the sound for card failure. Users can set a custom sound in the system settings under "Upgrade" and "Ringtones." After upgrading the ringtones file, the custom sound can be applied to the settings for card failure.
Successful beep for card deletion	Close: No beep after successful card deletion Default: Use the default beep Voice: The default built-in voice prompt is set to "Card deletion successful." The system supports customization of the successful card deletion tone. Users can set a custom tone in the system settings under "Upgrade" and "Ringtone." After upgrading the ringtone file, the custom tone can be applied to the settings for successful card deletion.
Card deletion failure beep	Close: No beep after failed card deletion Default: Use the default beep Voice: The default built-in voice prompt is set to "Card deletion failed." The system supports customization of the card deletion failure tone.

	Users can set a custom tone in the system settings under "Upgrade" and "Ringtone." After upgrading the ringtone file, the custom tone can be applied to the settings for card deletion failure.
Magnetic door detection beep	Closed: No beep will occur after detecting an anomaly in the door magnetic detection. Default: Use the default beep Voice: The default built-in voice prompt is set to "Please close the door." Customized door detection tones can be configured in the system settings under "Upgrade" and "Ringtones." After upgrading the ringtone file, the custom tones can be applied to the settings for door detection.
Intercom Settings	
Enable Intercom	When intercom is enabled, the device will accept the incoming call request with a SIP header of Alert-Info instruction to automatically answer the call after specific delay.
Enable Intercom Mute	Enable mute mode during the intercom call.
Enable Intercom Tone	If the incoming call is intercom call, the phone will play the intercom tone.
Enable Intercom Barge	Enable Intercom Barge by selecting it; the phone will auto answers the intercom call during a call. If the current call is intercom call, the phone will reject the second intercom call.
Response Code Settings	
Busy Response Code	Specify the SIP response code for a busy line.
Reject Response Code	Configure the SIP response code for call rejection.

5.21 Intercom Setting >> Media

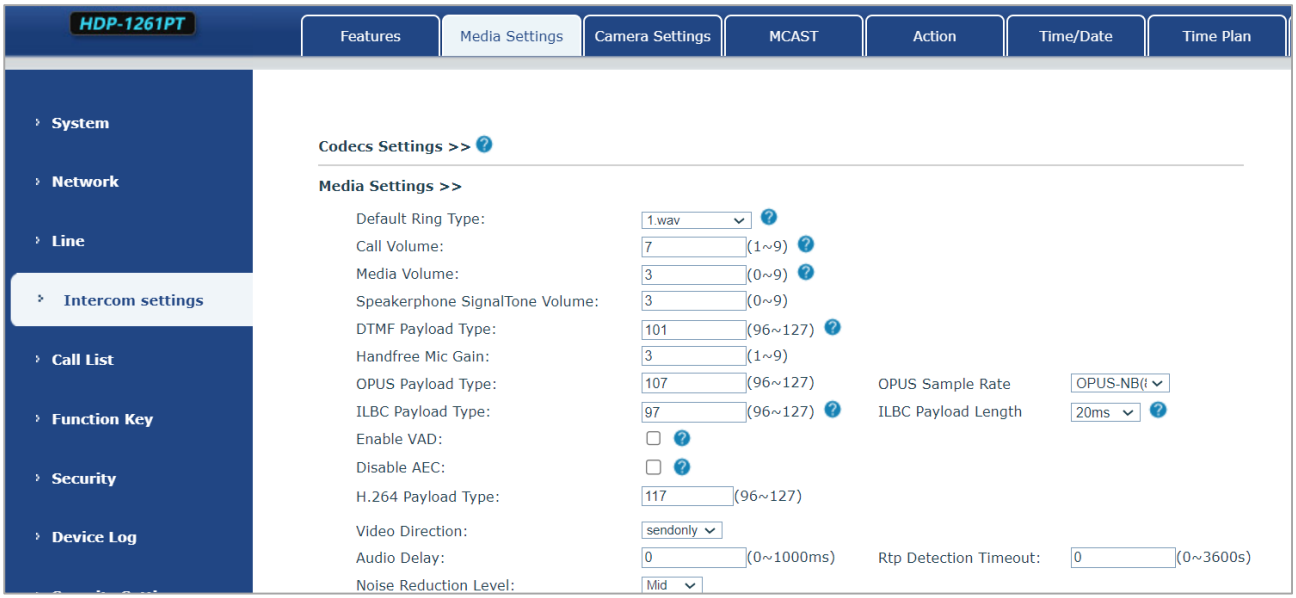


Figure 5-21-1 Media Setting Page Screenshot

Parameters	Description
Codecs Settings	Select the enabled and disabled voice codecs codec:G.711A/U,G.722,G.729,ILBC,opus,G.726,G.723.1
Media Setting	
Default Ring Type	Set the default ring type. If the caller ID of an incoming call was not configured with specific ring type, the default ring will be used.
Speakerphone Volume	Set the speakerphone volume, the value must be 1~9.
Speakerphone Ring Volume	Set the ring volume in the speakerphone, the value must be 1~9.
Speakerphone Ring Volume	Set the ring volume in the speakerphone, the value must be 1~9.
DTMF Payload Type	Enter the DTMF payload type, the value must be 96~127.
Opus Playload Type	Enter the opus payload type, the value must be 96~127.
OPUS Sample Rate	Set the opus sample rate including OPUS-NB（8KHz), OPUS-WB（16KHz）
ILBC Payload Type	Set the ILBC Payload Type
ILBC Payload Length	Set the ILBC Payload Length
Enable VAD	Enable Voice Activity Detection. When enabled, the device will suppress the audio transmission with artificial comfort

	noise signal to save the bandwidth.
H.264Payload Type	Set the H264 Payload Type, the value must be 96~127.
RTP Control Protocol(RTCP) Settings	
CNAME user	Set CNAME user
CNAME host	Set CNAME host
RTP Settings	
RTP keep alive	Hold the call and send the packet after 30s
Alert Info Ring Settings	
Value	Set the value to specify the ring type.
Ring Type	Type1-Type9

5.22 Intercom Setting >> Camera Settings

Customers can configure camera related parameters and adjust video coding related settings.

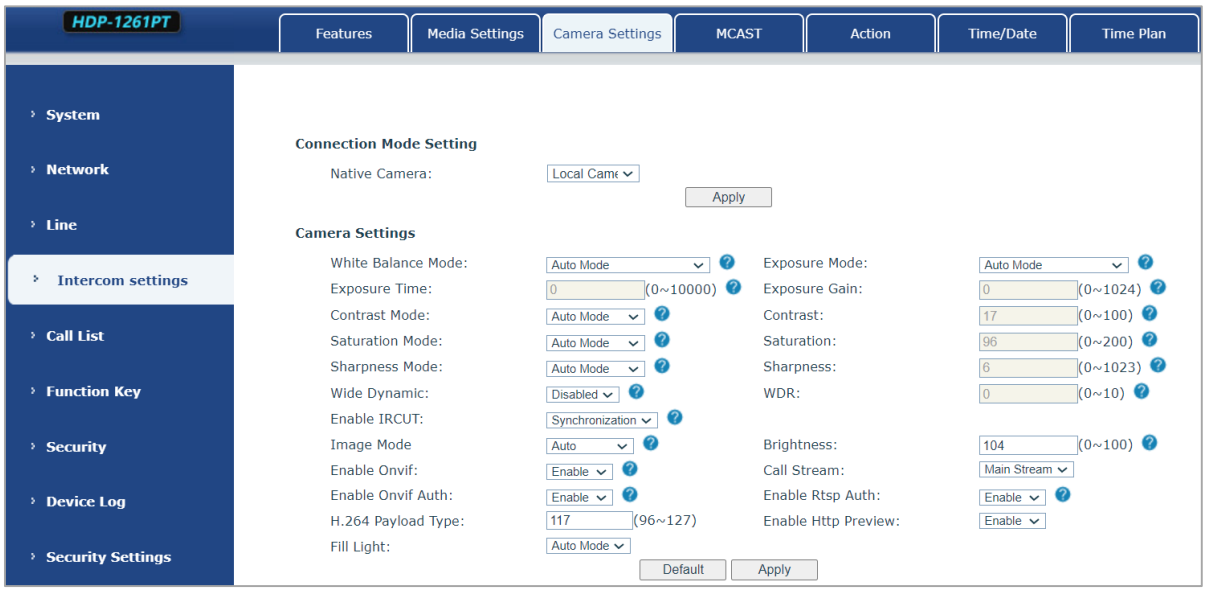


Figure 5-22-1 Media Setting Page Screenshot

Parameters	Description
Connection Mode Setting	
Native Camera	Local: Automatically use the local camera to transmit images. External: After setting the external camera, it will automatically use the external camera to transmit images.
camera settings	
White Balance Mode	Auto mode: The camera automatically makes the most appropriate adjustments according to the color temperature of the shooting scene, and automatically compensates for the color of the light source. Lock mode: Fixed white balance parameters will not be automatically adjusted according to the actual color temperature. Incandescent lamp mode: To compensate for the hue of incandescent lamps, it is suitable for use under beige light sources (bulbs, tungsten lamps, candles) and other light sources of this type. Warm light mode: To compensate the hue of warm light, it is suitable for light sources with a color temperature of about 2700K. Natural light mode: It can be used for white balance in outdoor shooting and has a wide range of applications. Fluorescent lamp light: To compensate the hue of fluorescent lamps, it is suitable for use under fluorescent light sources (fluorescent lamps, energy-saving lamps) and other types of light sources.

Exposure Mode	**Auto mode**: The camera automatically sets the parameters; no need for the operator to adjust. **Manual exposure time**: Set the exposure time by yourself; the range is 0~10000. **Manual exposure gain**: Set the exposure gain by yourself; the range is 0~1024. All manual: Manually set the exposure time and gain.
Exposure Time	This refers to the duration of pressing the shutter button. Increasing the exposure time has the potential to enhance the signal-to-noise ratio, resulting in clearer images. A longer exposure time allows for a greater accumulation of photons on the CCD/CMOS surface, resulting in a brighter captured image. However, overexposure can lead to excessively bright photos, causing a loss of image details. Conversely, underexposure may result in dark photos with insufficient details.
Exposure Gain	It refers to the amplification gain of the analog signal after double sampling, but the noise signal is also amplified in the process of amplifying the image signal. The gain is generally only used when the signal is weak, but you do not want to increase the exposure time.
Contrast Mode	Auto mode: The camera automatically sets the contrast according to the environment; no need for the operator to adjust Manual mode: Manually set the camera's contrast parameters.
Contrast	It refers to the contrast between light and dark in the picture. By increasing the contrast, the brighter areas will be brighter and the darker areas will be darker, and the contrast between light and dark will increase.
Saturation Mode	Auto mode: The camera automatically sets the saturation according to the environment, without the need for the operator to adjust. Manual mode: Manually set the camera's saturation parameters.
Saturation	Saturation refers to the color. Adjusting the saturation will change the color. The greater the adjustment, the more distorted the image color. Adjusting the saturation is only suitable for pictures with insufficient colors. When the saturation is adjusted to the lowest, the image will lose its color and become a black and white image.
Sharpness Mode	Auto mode: The camera automatically sets the sharpness according to the environment; no need for the operator to adjust. Manual mode**:** Manually set the sharpness parameters of the camera.
Sharpness	Sharpness is sometimes called "sharpness", which is an indicator that reflects the sharpness of the image plane and the sharpness of the edges of the image. If you increase the sharpness, the contrast of the

	details on the image plane is also higher and it looks clearer.
Wide dynamic	Enable or disable wide dynamic. Turning on wide dynamic allows the camera to see the image in a very strong contrast.
Wide dynamic range	Set image brightness by yourself; the range is 0~10.
Turn on IRCUT	Whether to open IRCUT
Image mode	Daytime (color): The camera transmits color images when there is sufficient light during the day. Night (black and white): The camera transmits black and white images when there is insufficient light at night. Automatic: The camera transmits color images when the light is sufficient during the day according to the light sensitivity, and transmits black and white images when the light is insufficient at night.
Brightness	Set the image brightness by yourself; the range is 0~100.
Enable ONVIF	Enable or disable the ONVIF protocol after enabling it. the device can be discovered through a recorder that supports ONVIF.
Call Stream	Main stream or sub stream is used in video call.
Enable ONVIF Auth	Authentication is required when using ONVIF protocol (with username and password).
Enable Rtsp Auth	When using rtsp protocol, authentication is required (with username and password).
H.264 Payload Type	Set the load type of H.264; the range is 96~127.
Osd Settings	
Osd Time	Turn on/off the date display of the camera image interface.
Osd Text	Enable/disable the text display of the camera image interface.
Video Codecs	
H264 Video Stream	Supports H.264 encoding format.
Bitrate Control	VBR: Video call will adapt to the bit rate of the opposite end, so that the video effect is better. CBR：The video call will not change according to the bit rate set by itself.
Resolution	Supports 1080P, 720P, 4CIF, VGA, CIF, QVGA.
Frame Rate (fps)	The larger the value is, the more fluent the video will be, and the higher the requirement for network bandwidth will be; adjustment is not recommended.

BitRate	It refers to the data flow used by video files in unit time, also known as code rate or code flow rate. Generally speaking, sampling rate is the most important part of picture quality control in video coding. Generally, the unit we use is KB / s or MB / s.
Frame Interval	The larger the value, the worse the video quality; otherwise, adjustment is not recommended.
RTSP Information	
Main Stream Url	Display the main stream URL address.
Sub Stream Url	Display the sub stream URL address.
Snapshot	
Input trigger	Select the input port that triggers the capture
Call trigger	Select the call status that triggers the capture
Movement detection trigger	Whether to enable monitoring capture
Saving Method of Capture	Set how to save the captured image, including Server and Storage Card
Server address	Enter the server address
Username	Enter a username
Password	Enter a password

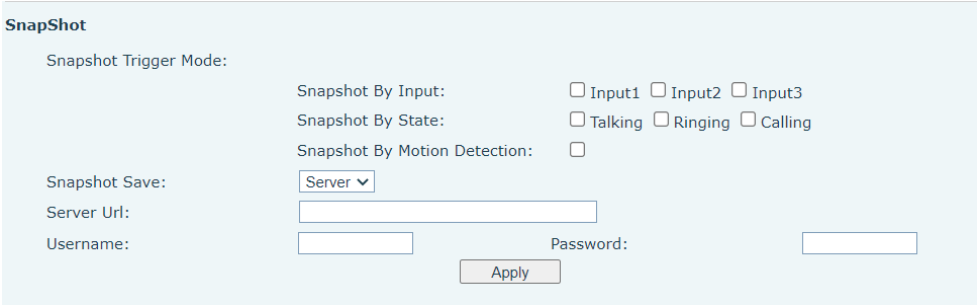


Figure 5-22-2 Snapshot Setting Page Screenshot

Capture trigger mode: Input trigger, call status trigger, movement detection trigger

Input trigger: Select the input port to trigger the snapshot.

Call status trigger: The snapshot is triggered when an incoming call occurs.

Movement detection trigger: A capture is triggered when the camera detects abnormal action.

Snapshot Save: Save the screenshot to the server or SD card. Supports 128G

Server url: Server address (Upload through FTP, TFTP, HTTP, or HTTPS)

5.23 Intercom Setting >> MCAST

It is easy and convenient to use multicast function to send notice to each member of the multicast via setting the multicast key on the device and sending multicast RTP stream to pre-configured multicast address. By configuring monitoring multicast address on the device, monitor and play the RTP stream which is sent by the multicast address.

5.24 Intercom Setting >> Action URL

Action URL Event Settings
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

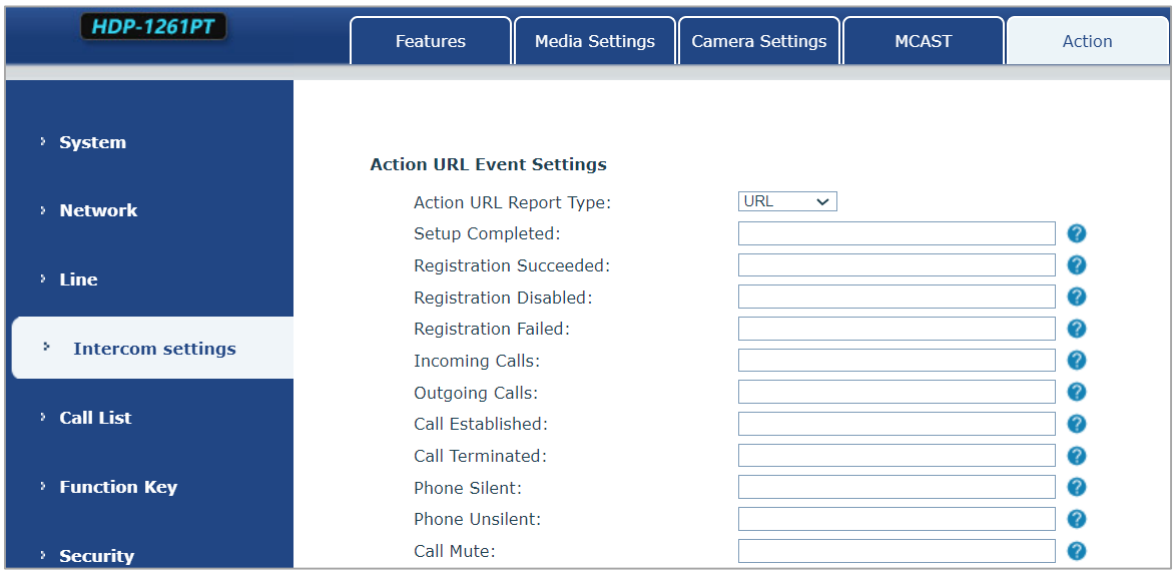


Figure 5-24-1 Action URL Setting Page Screenshot

5.25 Intercom Setting >> Time/Date

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

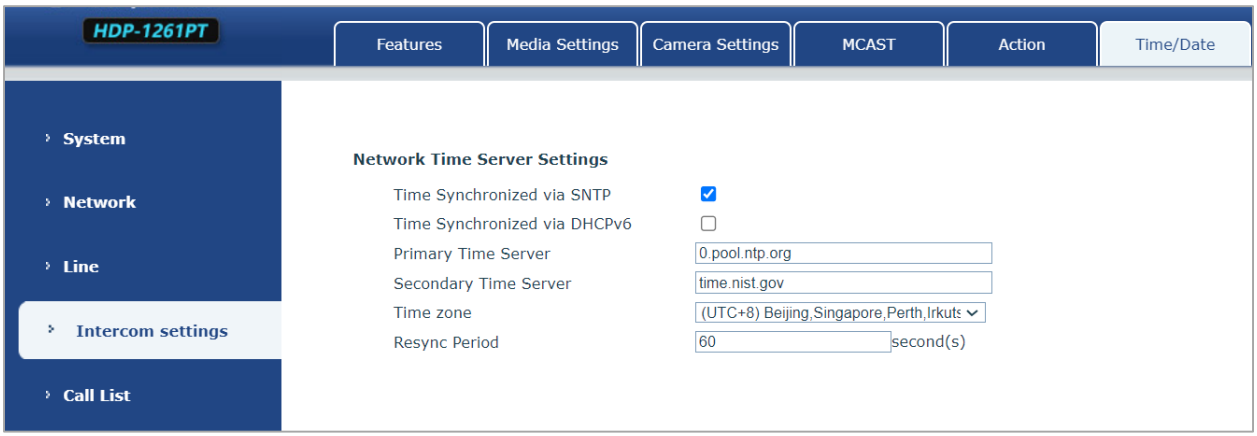


Figure 5-25-1 Time/Date Setting Page Screenshot

Time/Date	
Field Name	**Explanation**
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
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
To set the time manually, you need to disable the SNTP service first, and you need to fill in and submit each item of year, month, day, hour and minute in the figure above to make the manual settings successful.
System time: Display system time and its source (SIP automatic get >SNTP automatic get >manual manual setting)

5.26 Intercom Setting >> Time plan

The user can set the time point and time period for the device to perform a certain action.

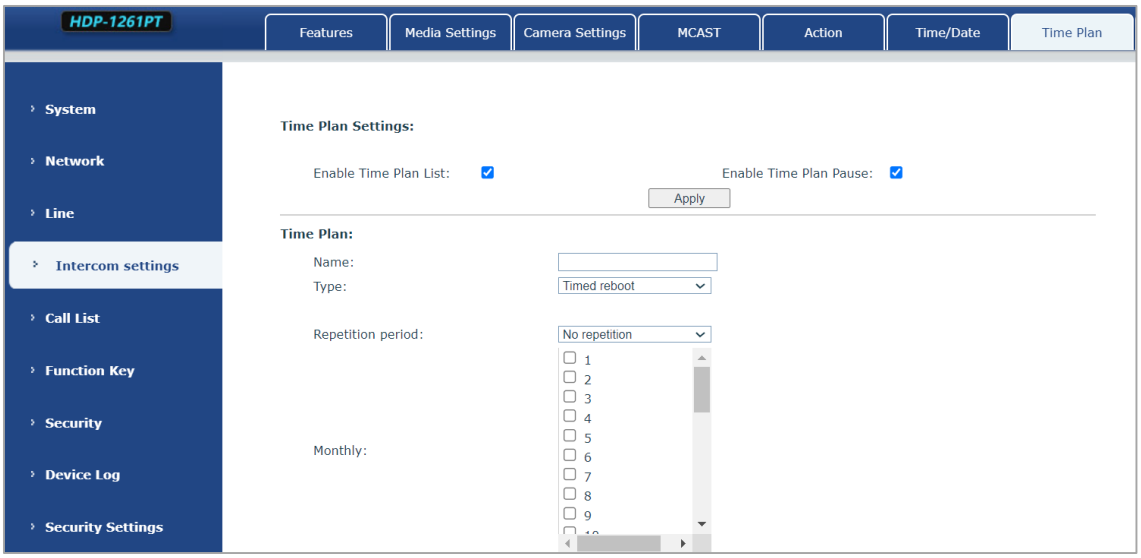


Figure 5-26-1 Time Plan Setting Page Screenshot

Parameters	Description
Name	Enter a defined action name
Type	Timing restart, timing upgrade, timing sound detection, timing playback audio
Audio path	Supports local Local: Select the audio file uploaded locally
Audio settings	Select the audio file you want to play; it supports trial listening, and you can play it immediately after clicking the trial listening
Repeat cycle	Do not repeat: execute once within the set time range Daily: Perform this operation in the same time frame every day Weekly: Do this in the time frame of the day of the week Monthly: The time frame of the month to perform this operation
Effective time	Set the time period for execution

5.27 Intercom Setting >> Tone

The user can configure the prompt tone of the device on this page.

You can select the country area or customize the area. The selected area can directly appear the default information, and the customized one can modify the key tone, callback tone and other information.

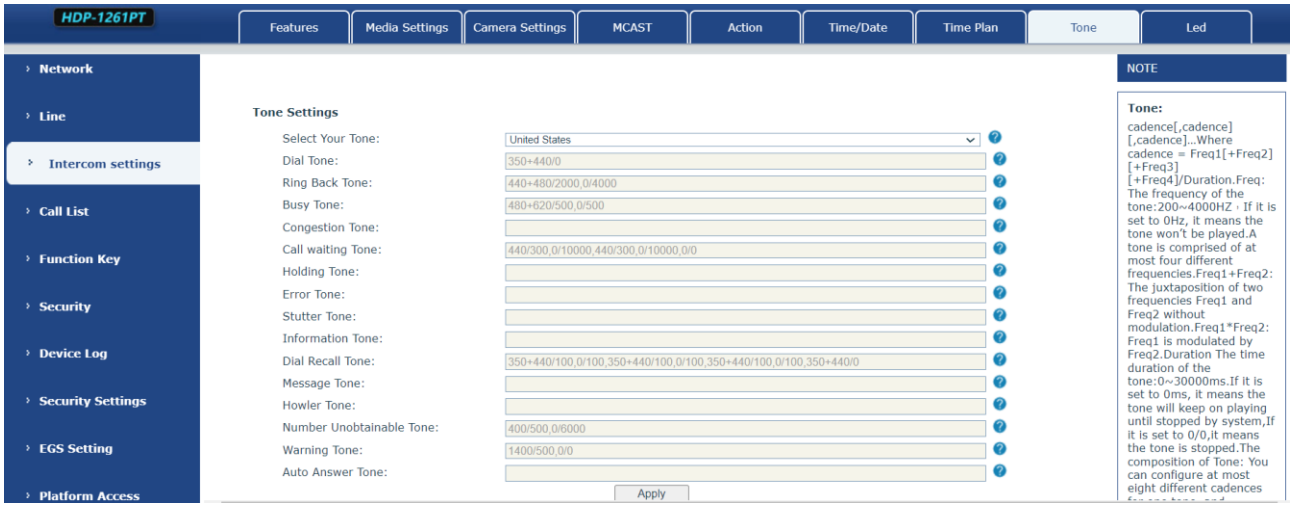


Figure 5-27-1 Tone Setting Page Screenshot

5.28 Intercom Setting >> Led

The user can configure the status and color of the indicator light on this page.

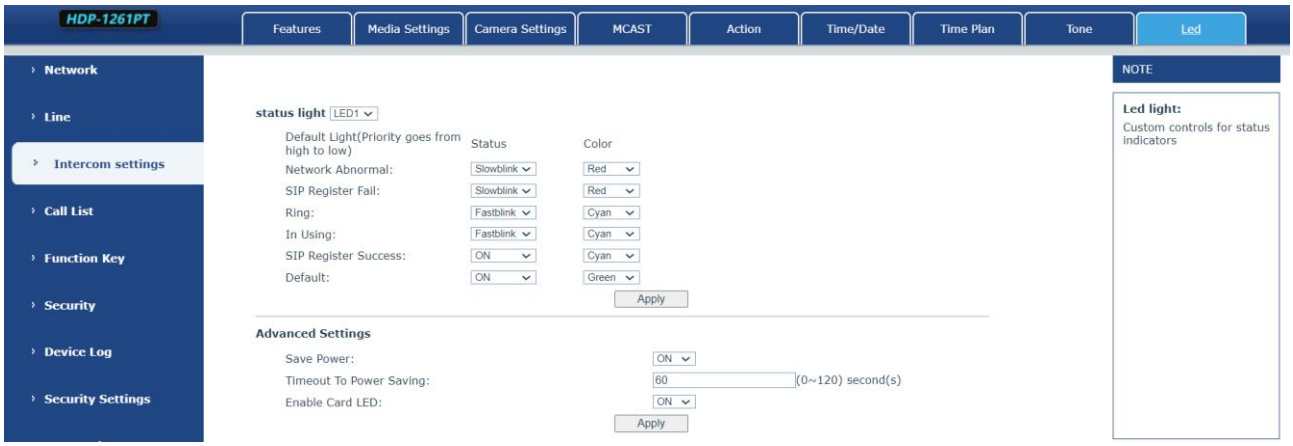


Figure 5-28-1 LED Setting Page Screenshot

Status indicator: The user can customize how the LED displays when the device is in different status.

Energy-saving mode: The device automatically turns off the LED when the device is not in use. The user can turn on or off the energy-saving mode.

Energy-saving mode timeout: The user can set the timeout of the energy-saving mode after inactivity. The default timeout is 60 seconds.

5.29 Call list >> Call List

■ Restricted Incoming Calls

It's same as blacklist.By adding a number to the blacklist, user will no longer receive phone call from that number and it will be rejected automatically by the device until user deletes it from the blacklist.

User can add a specific number to be blocked, or a prefix where any numbers matched the prefix will all be blocked.

■ Restrict Outgoing Call

You can set the rule to restrict some numbers from dialing out, until you remove the number from the list.

5.30 Call list >> Web Dial

Use web page to call, answer and hang up.

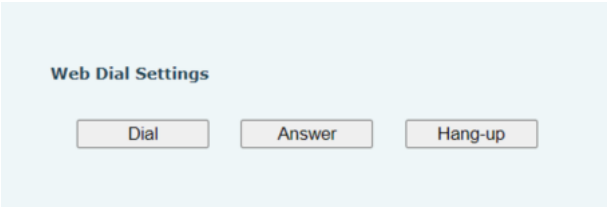


Figure 5-30-1 Webpage Dial Page Screenshot

5.31 Function Key

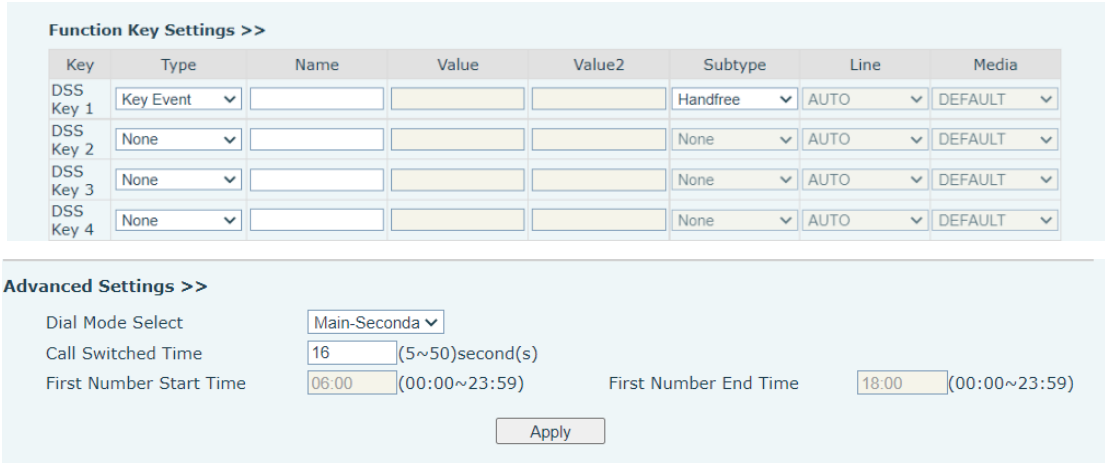


Figure 5-31-1 Function Key Setting Page Screenshot

Parameters	Description
Function key settings	
Memory	**Speed Dial**:The user can directly dial the set number. This feature is convenient for customers to dial frequent numbers. **Intercom:** This feature allows the operator or secretary to quickly connect to the phone, widely used in office environments.
Key event	The user can select a function key as the shortcut to trigger an event. Handsfree: One click to open the handsfree function. Audio play: Play music stored locally. OK: Confirm key. Volume Up: Increase the volume. Volume Down: Decrease the volume. Redial: Redial out the last number dialed. Release: Hang up the call. Call Back: Dial back the last call. Volume Circle
DTMF	Press during a call to send the set DTMF.
Mcast Paging	Configure the multicast address and voice encoding. User can initiate multicast by pressing this key.
Action URL	The user can use a specific URL to make basic calls to the device, open the door, etc.
Mcast Listening	In standby, press the function key. If the RTP of the multicast is detected, the device will monitor the multicast

PTT	**Speed dial**: Make a call when pressed, and end the call when lifted. Intercom: Start the intercom when pressed, and end the intercom when lifted. Multicast: Initiate multicast when pressed, and end multicast when lifted.
Programmable Key Settings	
Desktop	None: Nothing happens when you press the speed dial. Dsskey1: When it is set to dsskey1, follow the settings of dsskey1 to make call, answer, etc. Dsskey2: When it is set to dsskey2, perform operations such as calling and answering according to the setting of dsskey2.
Dialer	None: Nothing happens when you press the speed dial. Dsskey1: When it is set to dsskey1, follow the settings of dsskey1 to make call, answer, etc. Dsskey2: When it is set to dsskey2, perform operations such as calling and answering according to the setting of dsskey2.
Ringing	Answer: When there is an incoming call, if auto answer is disabled, press the speed dial key to answer the call. End: When there is an incoming call, press the speed dial button to hang up the call.
Talking	End: When there is a call, press the speed dial key to hang up the call. Volume up: When there is a call, press the speed dial button to increase the volume. Volume down: When there is a call, press the speed dial button to decrease the volume. Dsskey1：When it is set to dsskey1, follow the settings of dsskey1 to make call, answer, etc. Dsskey2：When it is set to dsskey2, perform operations such as calling and answering according to the setting of dsskey2.
Desktop Long Pressed	None: Long-pressing the speed dial key does not respond. Main menu: Long-press the speed dial key to enter the command line mode, see 5.2.1 Common Command Mode for details.
Advanced Settings	
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"

➢ **Memory**

Enter the phone number in the input box. When you press the function key, the device will call out the set phone number. This button can also be used to set the IP address, press the function key to make an IP direct call.

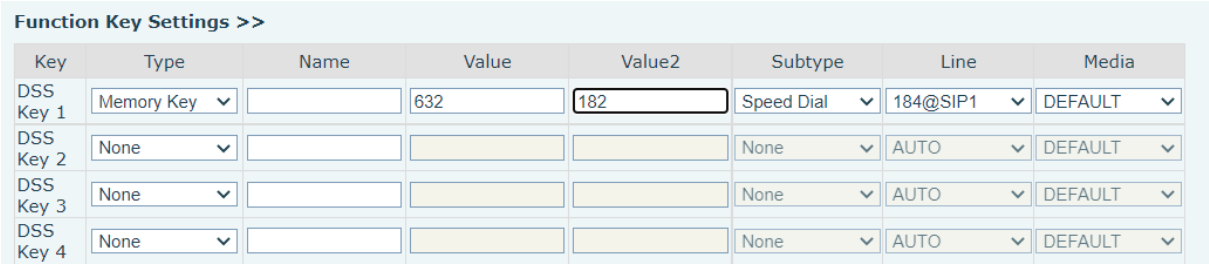


Figure 5-31-2 Memory Key Setting Page Screenshot

Type	number	line	Subtype	usage
Memory	Fill in the SIP account or IP address of the called party	The line corresponding to the SIP account	Speed Dial	Using the speed dial mode, press the button to quickly dial the set number.
			Intercom	Using the intercom mode, when the SIP phone at the opposite end supports the intercom function, the call can be automatically answered.

➢ **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:

Type	Number	Subtype
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
		G.711U
		G.729AB
		iLBC
		opus
		G.722

➢ **PTT**

Keep pressing the shortcut key set to make a call, release it and hang up.

5.32 Security >> Web Filter

Users can set up to allow only a certain network segment IP to access the device.

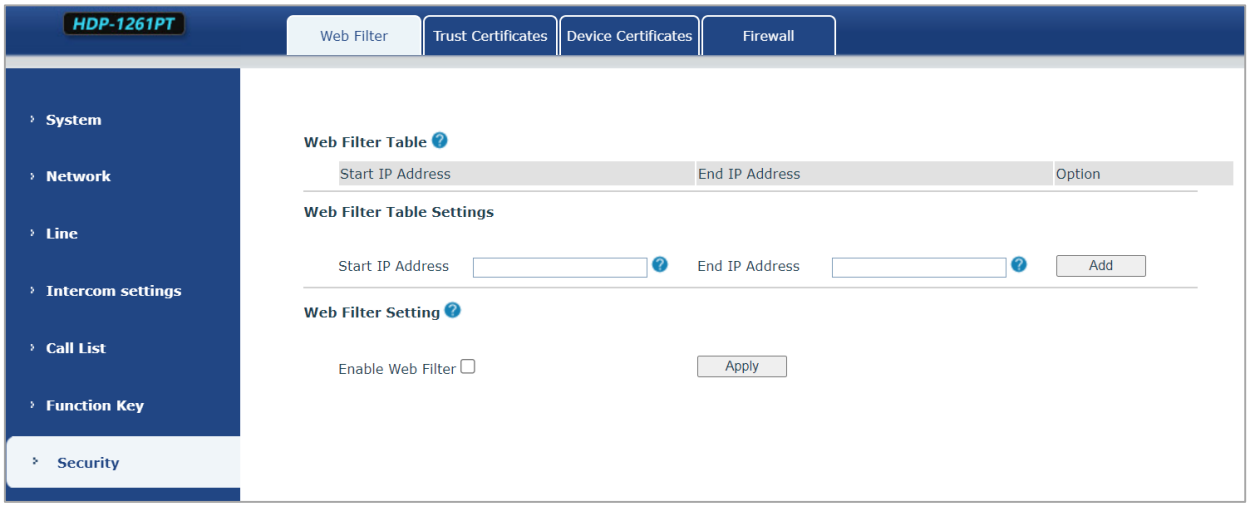


Figure 5-32-1 Web Filter Setting Page Screenshot

Add and delete the allowed IP network segments; configure the start IP address in the start IP, configure the end IP address in the end IP, and then click [Add] to add successfully. You can set a large network segment or add it into several network segments. When deleting, select the starting IP of the network segment to be deleted in the list, and then click [Delete] to take effect.

Enable web filtering: Configure to enable/disable web access filtering; click the [Submit] button to take effect.

Note	If the device you access to the device is on the same network segment as the device, do not configure the web filtering network segment to be outside your own network segment, otherwise you will not be able to log in to the web page.

5.33 Security >> Trust Certificates

You can upload and delete uploaded trust certificates.

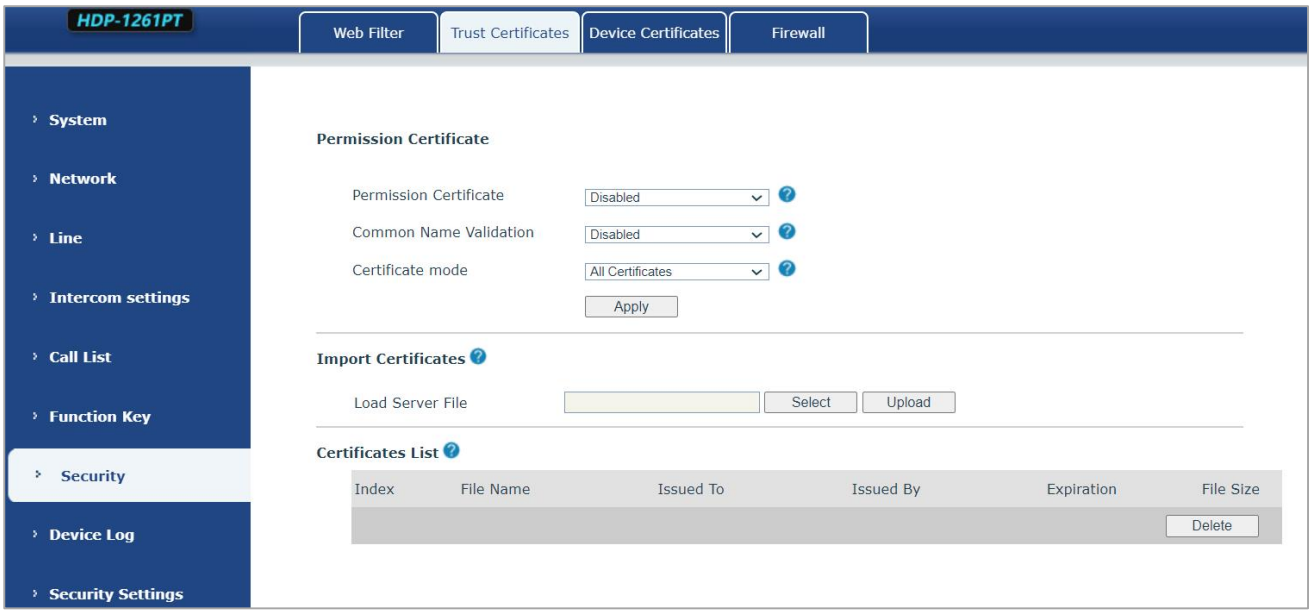


Figure 5-33-1 Trust Certificates Setting Page Screenshot

5.34 Security >> Device Certificates

Select the default certificate or the custom certificate as the device certificate.

You can upload and delete uploaded certificates.

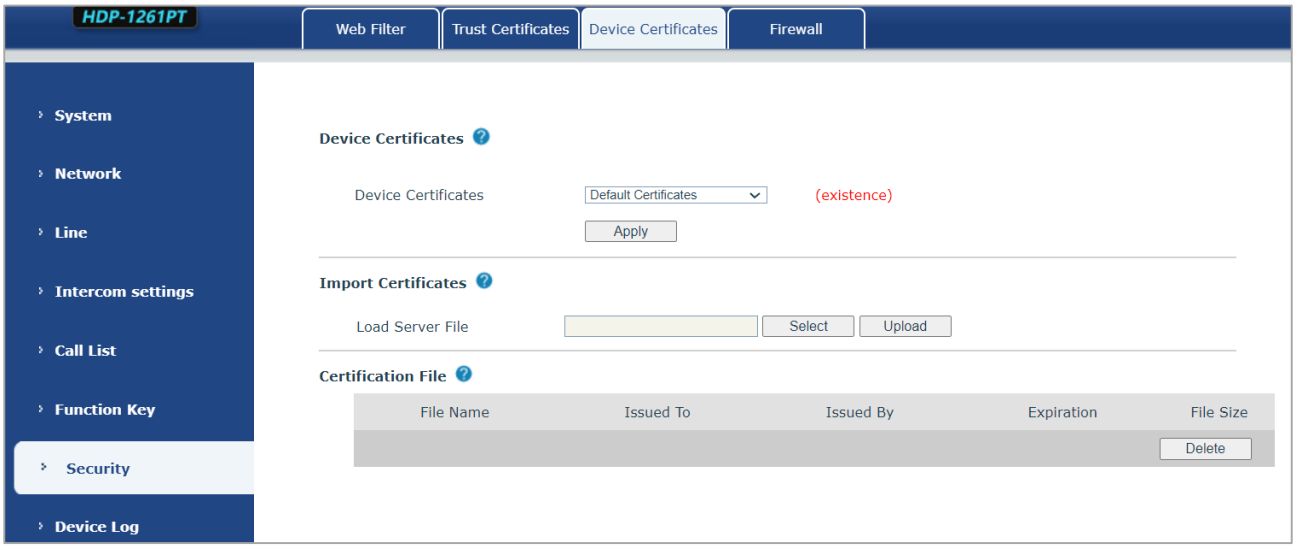


Figure 5-34-1 Device Certificates Setting Page Screenshot

5.35 Security >> Firewall

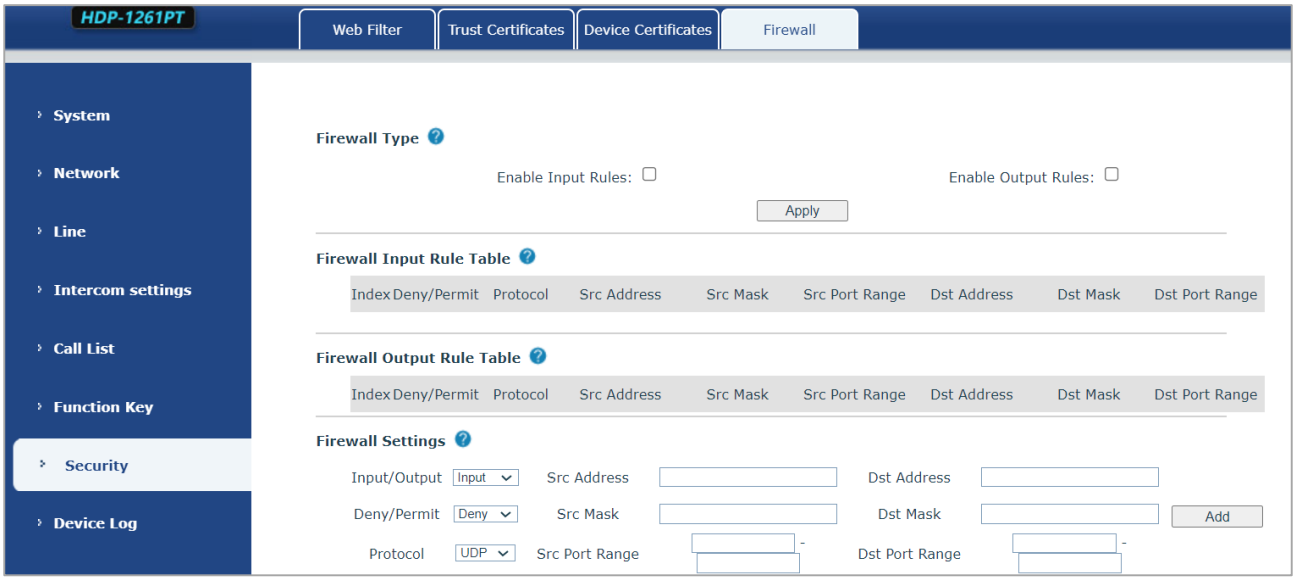


Figure 5-35-1 Firewall Setting Page Screenshot

Through this page, you can set whether to enable the input and output firewalls, and at the same time, you can set the input and output rules of the firewall. Use these settings to prevent malicious network access, or restrict internal users from accessing some resources of the external network, and improve safety.

The firewall rule setting is a simple firewall module. This function supports two kinds of rules: input rules and output rules. Each rule will be assigned a serial number, and a maximum of 10 each rule can be set.

Taking into account the complexity of firewall settings, the following will illustrate with an example:

Parameter	Description
Enable Input Rules	Whether to enable Input Rules
Enable Output Rules	Whether to enable Output Rules
Input/Output	Select the current rule as an input or output rule
Deny/permit	Choosing the current rule is denied or allowed
Protocol	There are four types of protocols: TCP, UDP, ICMP and IP
Port range	Port range
Src Address	The source address can be the host address, network address, or all addresses 0.0.0.0; it can also be a network address similar to *.*.*.0, such as 192.168.1.0.
Dst Mask	The destination address can be a specific IP address or all addresses 0.0.0.0; it can also be a network address similar to *.*.*.0, such as 192.168.1.0.
Src Port Range	It is the source address mask. When it is configured as 255.255.255.255, it means it is a specific host. When it is set as a

	subnet mask of type 255.255.255.0, it means that the filter is a network segment;
Dst Port Range	It is the destination address mask. When it is configured as 255.255.255.255, it means it is a specific host. When it is set as a subnet mask of 255.255.255.0 type, it means that a network segment is filtered;

After setting, click [Add], a new item will be added to the firewall output rules, as shown in the figure below:

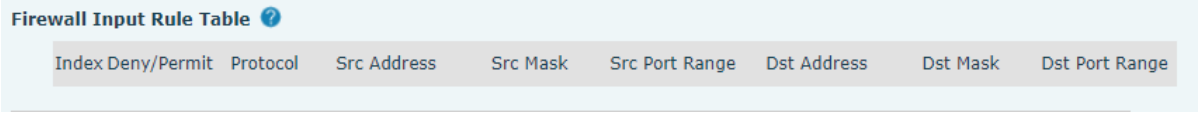
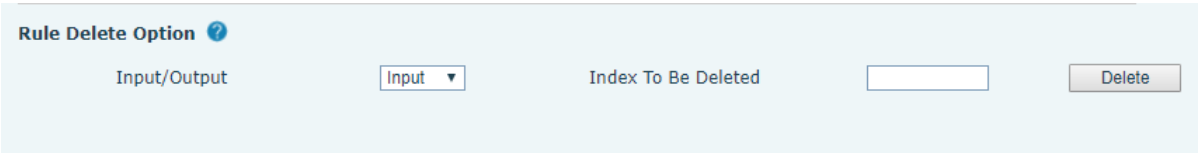


Figure 5-35-2 Firewall Rules List Page Screenshot

Then select and click the button [Submit].

In this way, when the device runs: ping 192.168.1.118, it will not be able to send data packets to 192.168.1.118 because of the prohibition of the output rule. But ping other IPs in the 192.168.1.0 network segment can still receive the response packets from the destination host normally.



Select the list you want to delete and click [Delete] to delete the selected list.

5.36 Device Log

You can access the device log to troubleshoot unusual issues. If you encounter problems, please send the device log to the technical staff for problem diagnosis and resolution.

5.37 Security Settings

Tamper protection is enabled. Upon activation, if the device is forcibly removed, an alarm message will be sent to the server, and an alarm ring will be played.

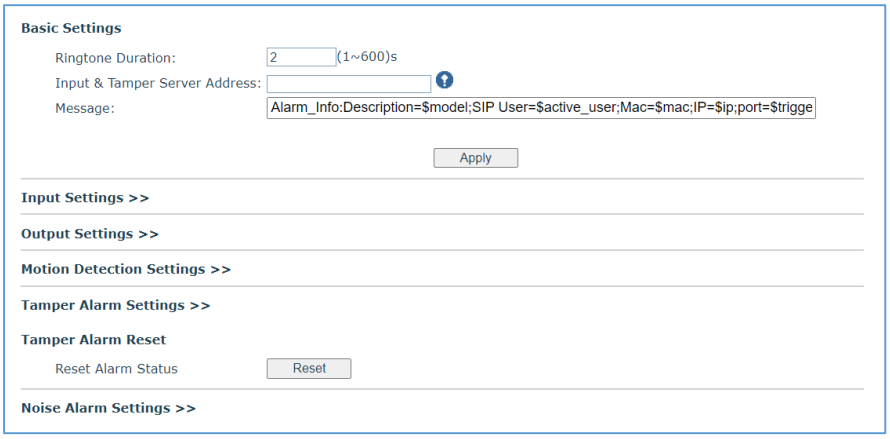


Figure 5-37-1 Security Setting Page Screenshot

Security Settings	
Parameters	**Description**
Basic Settings	
Ringtone Duration	Set the ringtone duration, default value is 2 seconds.
Input & Tamper Server Address	Set remote server address. The device will send message to the server when the alarm is triggered. The message format is: Alarm_Info:Description=HDP-1261PT;SIP User=;Mac=00:30:4f:xx:xx:xx;IP=; port=Input .
Information	Fill in the information attached to the upload server
Input settings	
Input	Enable or disable Input
Triggered by	When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger.
	When choosing the high level trigger (disconnect trigger), detect the input port (high level) disconnected trigger.
Input Duration	Set the Input change duration time, the default is 5 seconds.
Triggered Action	**Send SMS:** Set the alert message to be sent to server if selected. **Event:** The device will perform corresponding Dss Key configurations if any key is selected; by default the value is none. **Triggered Ringtone:** Select triggered ring tone.
Triggered Ringtone	Ringtone selection
Output Settings	
Enable Logs	Enable or disable LOG

Triggered by DTMF Ring tone	Select the DTMF trigger ringtone.
Triggered by URI Ringtone	Select the URI trigger ringtone.
Triggered By SMS Ringtone	Select the SMS trigger ringtone.
Triggered By Dsskey Ringtone	Select the Dsskey trigger ringtone.
Output Response	Enable or disable Output Response
Standard Status	When selecting the low-level trigger (NO: normally open), meeting the trigger condition will result in the disconnection of the NO port.
	When opting for the high-level trigger (NC: normally closed), meeting the trigger condition will cause the closure of the NC port.
Output Duration	Set the output change duration time, the default is 5 seconds.
Input trigger	When the input port meets the trigger condition, the output port will trigger (the port level time changes, controlled by <output duration>).
Triggered by DTMF	Enable or disable trigger by DTMF. The device will check the received DTMF sent by remote device. If it matches the DTMF trigger code, the device will trigger corresponding output port.
DTMF Trigger Code	Input the DTMF trigger code, default value is 1234.
DTMF Reset Code	Input the DTMF reset code, default value is 4321.
Reset By	Reset the output port mode by duration or state. By duration: Reset the output port status when output duration occurs. By state: Reset the output port status when device's call state changes.
Triggered by URI	Enable or disable trigger by URI. User can send commands from remote device or server to i16SV series device. If the command is correct, then device will trigger corresponding output port.
Trigger Message	Input trigger message for trigger in URI mode.
Rest Message	Input reset message for trigger in URI mode.
Triggered by SMS	Enable or disable trigger by SMS. User can send ALERT command to i16SV series device. If the command is correct, then device will trigger corresponding output port.
Trigger SMS	Input trigger message for trigger in SMS mode.
Reset SMS	Input reset message for trigger in SMS mode.
Triggered by Input	Select the input port. When the input port meets the trigger condition, the output port will be triggered (The Port level time change, By < Output

	Duration > control).
Triggered by Call state	Select call state to trigger the output port. Options are: Talking: When the device's talking status changes, trigger the output port. Ringing: When the device's ringing status changes, trigger the output port. Calling: When the device's calling status changes, trigger the output port.
Triggered by DssKey	Enable or disable trigger by dsskey. If any of the dsskey is selected and when the dsskey application performs, the output port will be triggered.
Triggered Hangup	Trigger the output port after hanging up.
Hangup Delay	Hang up trigger delay, default 5 seconds
Motion detection settings	
Motion Detection Alarm	Enable or disable motion detection
Trigger Duration	Set the trigger delay time, the default is 3 seconds, the range: 0~3600 seconds
Trigger ringtone	Support ringtone selection
Trigger behavior: Send SMS	Enable or disable the input port to send messages to the server
Function key	When setting to dsskey1 or dsskey2, and triggering dsskey to make a call, the default is none
Tamper Alarm Settings	
Enable Tamper Alarm	Whether to enable tamper detection. If the terminal is violently dismantled, the tamper will be triggered and will always play the set alarm ringtone.
Alarm command	When someone is detected for 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.
Alarm Ringtone	Alarm ringtone setting
Detachable alarm reset	
Reset alarm state	Reset the play of stop ringtone

5.38 EGS Setting >> Features

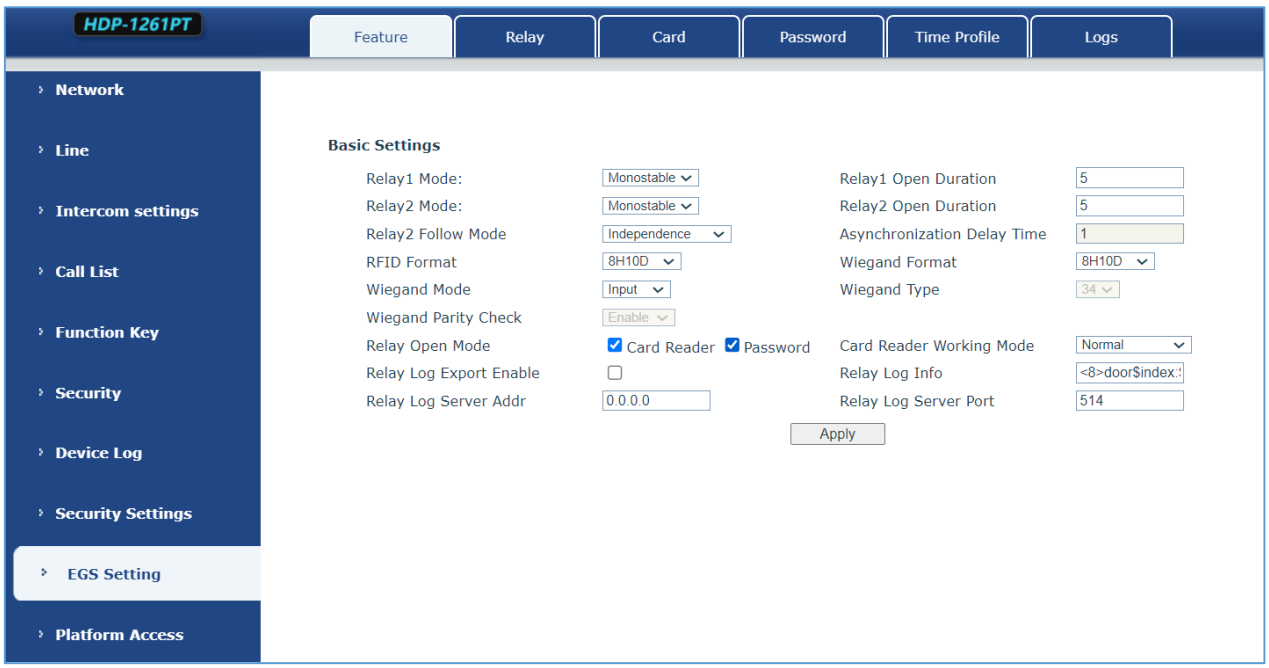


Figure 5-38-1 ESG Feature Setting Page Screenshot

You can set basic access control settings on this screen

Field Name	Explanation
Basic Settings	
Relay1 Mode	Monostable: There is only one fixed action status for door unlocking. Bistable: There are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After the change, the status would be kept. Initial Value is Monostable.
Relay1 Duration	Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial Value is 5 seconds.
Relay2 Mode	Monostable: There is only one fixed action status for door unlocking. Bistable: There are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After the change, the status would be kept. Initial Value is Monostable.
Relay2 Duration	Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial Value is 5 seconds.

Relay2 Mode	Monostable: There is only one fixed action status for door unlocking. Bistable: There are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After the change, the status would be kept. Initial Value is Monostable.
Relay2 Duration	Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial Value is 5 seconds.
Relay2Follow mode	Independent: Open the door independently with Relay 1. Synchronous: Open the door at the same time as Relay1. Asynchronous: Relay1 opens after a period of time Relay2 opens.
Asynchronous delay	The user can set the asynchronous door opening delay time of Relay1 and Relay2, the default is 1 second.
RFID card format	Supported access control card format
Wiegand format	Supported Wiegand access card format
Wiegand mode	Optional input port or output port, default in
Wiegand Type	Supports 26 and 34
Enable Card Reader	Enable or disable card reader for RFID cards.
Card Reader Working Mode	Set ID card stats: Normal: This is the work mode where the slot card can open the door. Card Issuing: This is the issuing mode where the slot card can add ID cards. Card Revoking: This is the revoking mode where the slot card can delete ID cards.

5.39 EGS Setting >> Relay

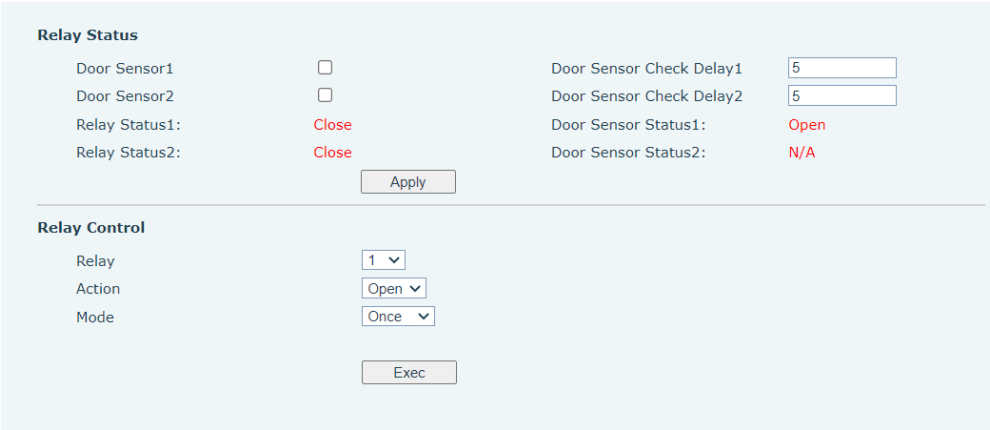


Figure 5-39-1 Relay Setting Page Screenshot

Field Name	Explanation
Relay Status	
Door Sensor1	Enable or disable door sensor 1.
Door Sensor Check Delay 1	Door Sensor1 detection delay time setting, 5 seconds by default.
Door Sensor2	Enable or disable door status sensor 2.
Door Sensor Check Delay 2	Door Sensor2 detection delay time setting, 5 seconds by default.
Lock Status 1	Door Close/Open
Door Sensor Status1	Door Close/Open
Lock Status 2	Door Close/Open
Door Sensor Status2	Door Close/Open
Door Lock Control	
Door Lock	Execute a door lock to open or close the door
Action	Door Open/Close
Open mode	The door will close automatically when time is out. The door will not close automatically and need to close manually when time is out.

5.40 EGS Setting >> Card

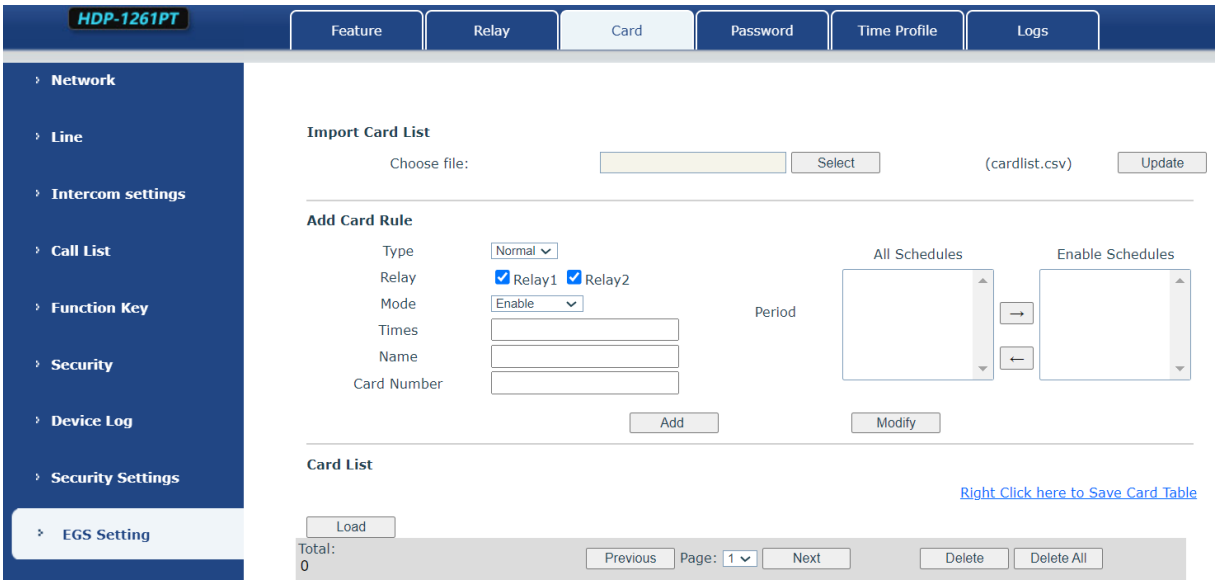


Figure 5-40-1 Card Setting Page Screenshot

Field Name	Explanation
Import Card List	
Click the <Select> button to choose and import the remote card list file (cardlist.csv). Subsequently, click <Update> to facilitate the batch import of remote card rules.	
Add Card Rule	
Type	In standard mode, the door is opened by presenting the designated card. For card administration: To add a card, swipe the administrator card in standby mode. The device will enter the card add mode, allowing you to swipe cards to add those not present in the card list. To delete a card, swipe the administrator card in standby mode. The device will enter the card delete mode, enabling you to swipe cards for removal. Any cards previously added will be deleted.
Relay	Swipe to open the door lock
Mode	In the "Closed" mode, swiping is unsuccessful after disabling. In the "Enable" mode, swiping the card becomes effective after enabling. For the "Time zone" mode, swiping the card within the set time zone takes effect
Times	The number of times the card can be swiped in a time period
Name	User name
Card Number	You can manually fill in the first 10 digits of the RFID card number or select the existing card number
Period	The time to add the card, automatically generated
Card List	
Operation	Delete -- delete all Export -- support to export to csv. file

5.41 EGS Setting >> Password

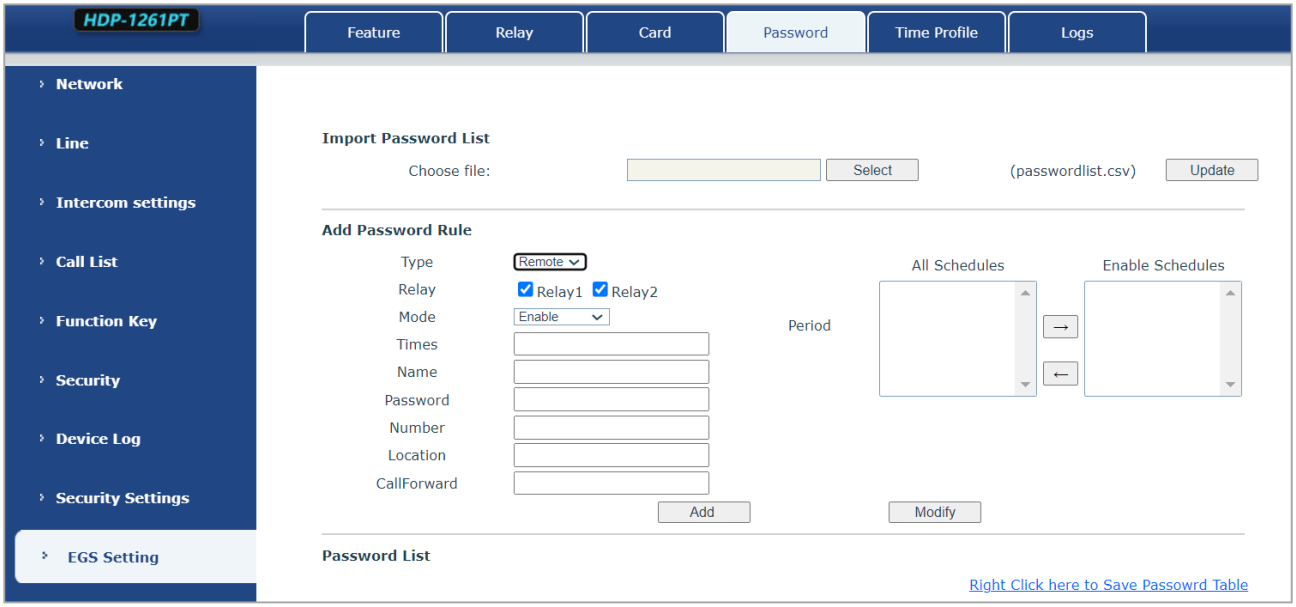


Figure 5-41-1 Password Rule Setting Page Screenshot

Field Name	Explanation
Import Password List	
Click the <Select> button to choose and import the remote password list file (passwordlist.csv). Then, click <Update> to perform a batch import of remote password rules.	
Add Password Rule	
Type	In the "Local" mode, the local door opening password can be used. Enter the password on the dial interface in standby, and inputting the set opening password will open the door immediately. For the "Remote" mode, the remote opening password is utilized. When the indoor unit calls the door or when the door calls the indoor unit, enter the DTMF password to open the door. In the "Remote and local" mode, one password supports both local and remote door opening methods simultaneously.
Relay	A door lock with a code
Mode	In the "Closed" mode, attempting to open the door with a password is unsuccessful after disabling. In the "Enable" mode, the password for opening the door becomes effective after enabling. For the "Time zone" mode, the password for opening the door takes effect only during the set time zone.
Times	The number of times the door can be opened with a password in a time

	period.
Name	User name
Password	Password to open the door
Number	When the indoor unit calls the access control or the access control calls the indoor unit to open the door, the door can be opened by entering the DTMF password.
Period	Time to add the card, automatically generated
Password List	
Operation	Delete -- delete all Export -- support to export to csv. file

5.42 EGS Setting >> Time Profile

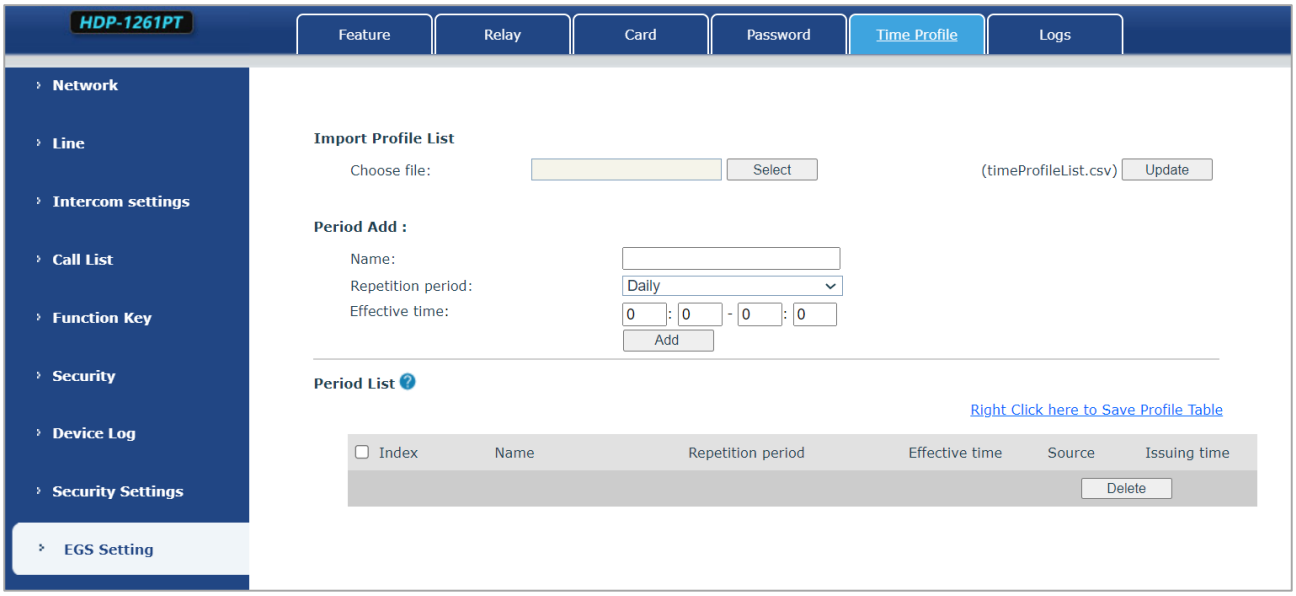


Figure 5-42-1 Time Profile Setting Page Screenshot

Field Name	Explanation
Import time list	
Click the <Select> button to choose and import the remote Profile list file (timeProfileList.csv). Then, click <Update> to perform a batch import of remote time periods.	
Period Add	
Name	Set the name of the time period
Repetition period	No repetition: Opening the door in the set time period is valid, and it is invalid at other times. Daily: It is valid to open the door in the time period set daily, and it is invalid at other times. Weekly: It is valid to open the door in the time period set every week, and it is invalid at other times. Monthly: It is valid to open the door in the time period set every month, and it is invalid at other times.
Effective time	Set the effective time.

5.43 EGS Setting >> Logs

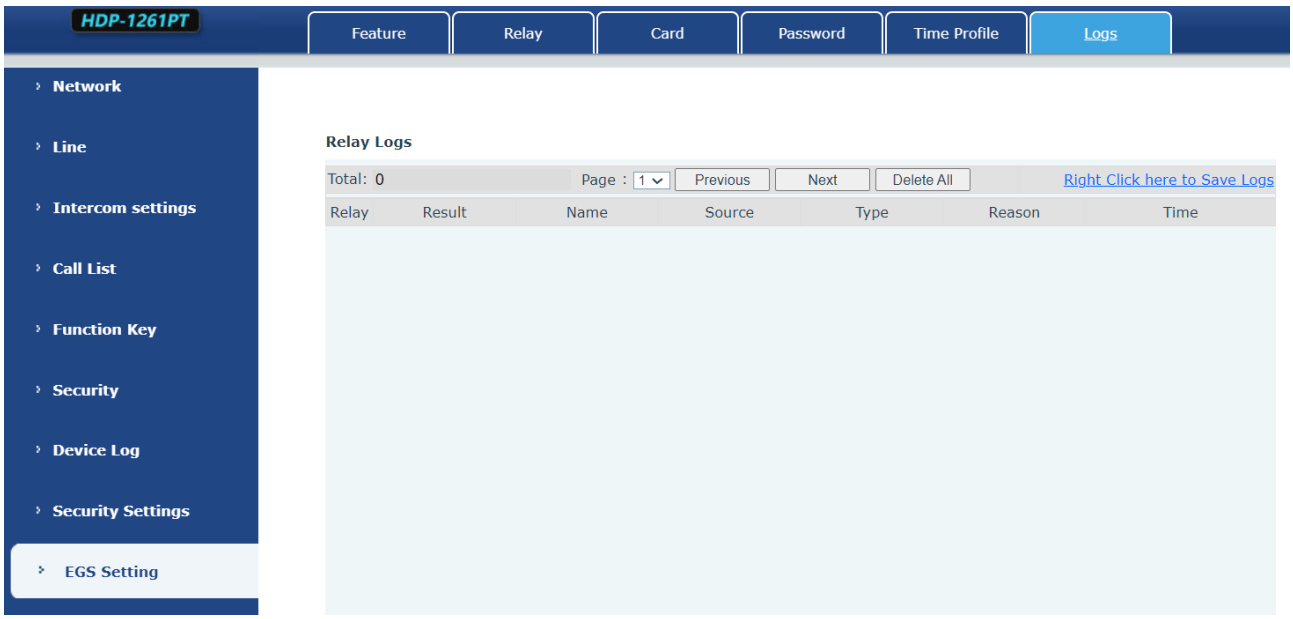


Figure 5-43-1 Logs Page Screenshot

Field Name	Explanation
Relay	Relay
Result	Display the result of a single door opening (success or failure)
Name	The name of the person who opened the door.
Source	Card number or password to open the door
Type	Door opening type, including password, credit card
Reason	Reasons for failed door opening
Time	Opening time

Chapter 6. Troubleshooting

When the device is not working properly, users can try the following methods to restore the device to normal operation or collect relevant information to send a problem report to the technical support mailbox.

6.1 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) and Internet Information, etc.

6.2 Reboot Device

User can restart the device through the webpage by clicking [**System**] >> [**Reboot**] and then click the [**Reboot**] button, or directly unplug the power to restart the device.

6.3 Device Factory Reset

Restoring the factory settings will delete all configurations, database and configuration files on the device and the device will be restored to factory default state.

To restore the factory settings, please go to [**System**] >> [**Configuration**] >> [**Reset Phone**] page, and click the [**Reset**] button, to return to the factory default state.

6.4 Network Packets Capture

In order to obtain the data packet of the device, the user needs to log in to the webpage of the device by opening 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. Users can analyze the packet or send it to the Technical Support mailbox.

6.5 Get Device Log

Log information is helpful when encountering abnormal problems. In order to obtain the log information of the device, the user can log on to the device web page by opening the web page [device log], and clicking the "start" button to follow the steps of the problem. Click the "end" button, and "save" to the local for analysis or send the log to the technician to locate the problem.

6.6 Common Trouble Cases

Trouble Case	Solution
Device could not boot up	1. The device is powered by external power supply via power adapter or PoE switch. Please use standard power adapter provided or PoE switch met with the specification requirements and check if device is well connected to power source. 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 location technical support to help you restore your equipment system.
Device could not register to a service provider	1. Please check if the device is connected to the network. 2. If the network connection is good, please check your line configuration again. If all configurations are correct, contact your service provider for support, or obtain a registered network packet and send it to the Support Email to help analyze the issue.