User's Manual

720p SIP Multi-unit Video Door Phone with RFID and PoE

► HDP-5240PT

www.PLANET.com.tw

Copyright

Federal Communication Commission 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, for example, 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.

Federal Communication Commission (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; they should be collected separately.

Revision

User’s Manual of PLANET 720p SIP Multi-unit Video Door Phone with RFID and PoE
Model: HDP-5240PT
Rev: 1.00 (March, 2017)
Part No. EM-HDP-5240PT_v1.1

Table of Contents

Chapter 1. Product introduction

1.1 Package Contents

Please read the following safety notices before installing or using this unit. They are crucial for the safe and reliable operation of the device.

The package should contain the following items:

- SIP Door Phone Unit x 1
- Quick Installation Guide x 1
- Screw Kit x 1
- Wrench x 1
- RFID Card x 3

Note	If any of the above items are missing, please contact your dealer immediately. Using the power supply that is not the one included in the camera packet will cause damage and void the warranty for this product.

1.2 Overview

Security is Ensured with PLANET Video Door Phone

PLANET HDP-5240PT is a SIP Door Phone with PoE feature. It supports H.264 video compression format and delivers excellent picture quality in 720p HD video resolutions at 10~30 frames per second (fps). It also supports HD (High Definition) voice and G.722 codec that relax bandwidth limitation and provide clear communications. It provides the flexibility and control required for high-quality property complex visitor management, property protection, intercom, and message service.

High-quality Audio and Video

With the integrated HD camera and advanced audio system with the echo cancellation function, the intercom provides sharp images and excellent audibility in all conditions. With the HTS-1000P touch screen control pad, you can view video from the intercom camera at any time. This allows you to have a constant overview of what is happening outside the door.

Keyless Control and Convenience

PLANET HDP-5240PT advancements in residential door lock security have been enhanced with secure authentication technology which supports many ways of opening door without a key. The door not only can be open via an RFID card but also a password if it is an electronic door lock. Thus, you can enter your home without having to use a key.

SIP 2.0 Standard Compliance

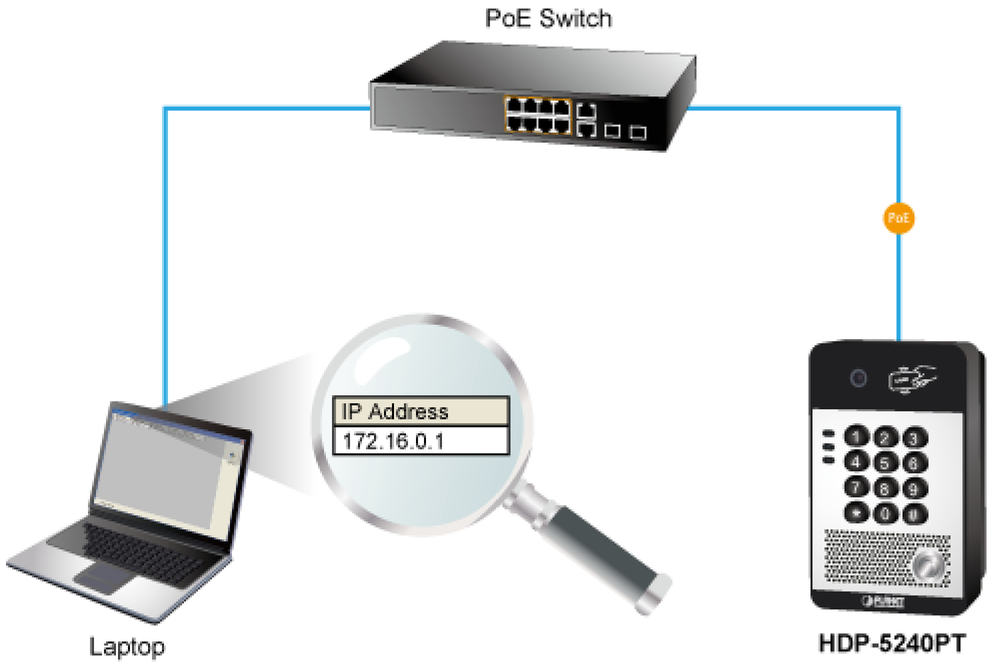
The HDP-5240PT supports Session Initiation Protocol 2.0 (RFC 3261) for easy integration with general voice over IP system. The IP phone is able to broadly interoperate with equipment provided by VoIP infrastructure providers, thus enabling them to provide their customers with better multimedia exchange services.

AEC (Acoustic Echo Cancellation)

Acoustic Echo Cancellation (AEC) technology is adopted in PLANET's HDP-5240PT Door Phone and HTS-1000P Touch Screen Control Pad to enable users to minimize the voice/sound signal distortion shown in the diagram below, thus guaranteeing the best-in-class sound quality.

Finding the Door Phone via Planet Search Tool

PLANET Search Tool is a simple, freely-available application for locating intercoms from the IP family in the network. After searching the network, the application shows the device name, firmware version and IP address of all intercoms found on a chart. This simplifies the administration and installation of intercom systems. Simply run the easy-to-use software to get immediate results.


PoE Switch
PoE
IP Address
172.16.0.1
Laptop
HDP-5240PT

1.3 Features

Benefits

- See/Talk visitors with High Definition Video and Voice
- Unlock the door with an RFID, Remote DTMF or Local Password
- Control Communication and Security over Internet

Hardware

- HD camera with infrared light and night vision
- IP65 for rigorous environment
- Supports several ways of opening door (DTMF, password, RFID card, switch)
- -20 to 60 degrees C operating temperature

Video and Audio

- Maximum resolution 1280 x 720 @ 30 fps
- Acoustic Echo Cancellation (AEC) is featured on speaker path
- Adjustable brightness, contrast and volume settings
- HD voice using wideband G.722 coding produces clearer sound
- Barge-in and calls can be switched automatically

Network and Configuration

- Standard IETF SIP protocol (RFC2361)
- Compatible with the Asterisk IP PBX systems or various platforms
- Compliant with IEEE 802.3af/at PoE interface for flexible deployment
- VPN, VLAN, QoS, 802.1x, HTTPS, TR069 and auto-provisioning

Easy Installation and Management

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

1.4 Specifications

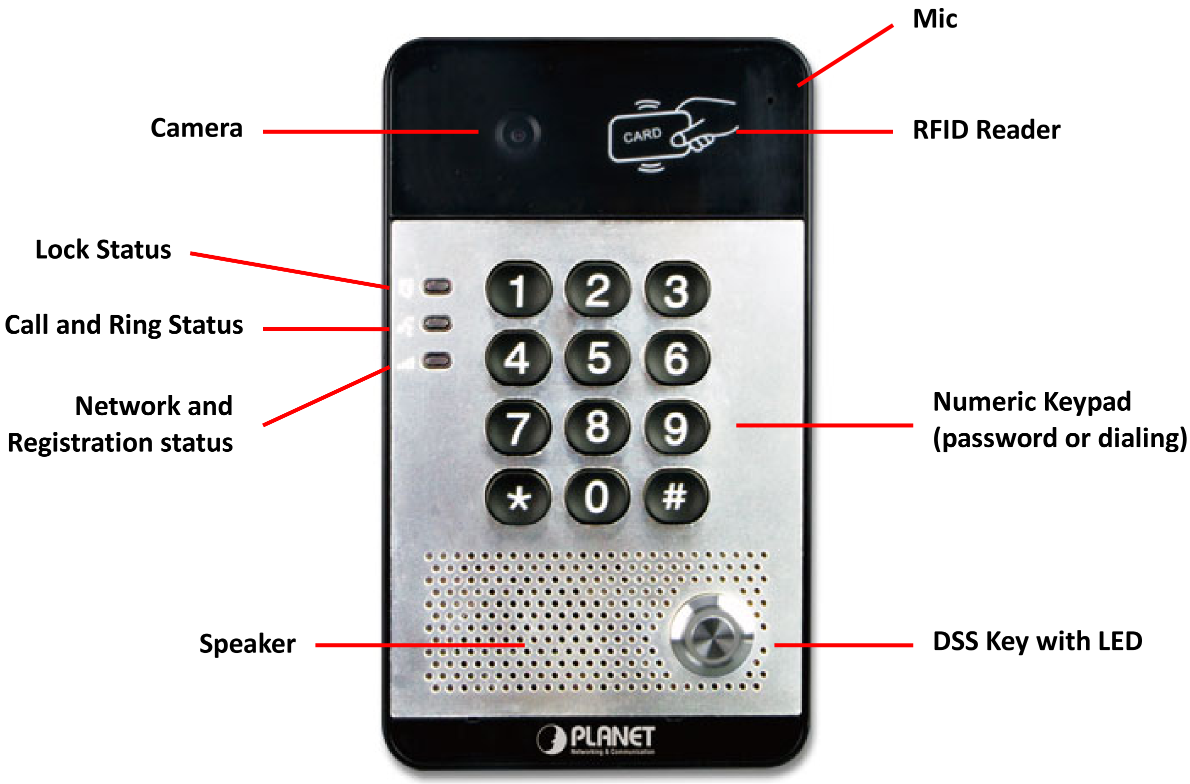
Product	HDP-5240PT
Video	
Image Device	1/4" color CMOS, Pixels: 1 million
Video Codec	H.264
Resolution	Main stream 1280 x 720 Sub-stream 640 x 360, 352 x 288, 32 x 240
Viewing Angle	110° (H), 95° (V)
Minimum Illumination	1 lux
Audio	
Audio Streaming	Two-way audio
Narrowband Codec	G.711a/u, G.723.1, G.726-32K, G.729AB
Broadband Speech Codec	G.722
Microphone	Built-in microphone (-38dB) and speaker (4Ω / 3W) input
Audio Output	Acoustic Echo Cancellation
DTMF	In-band, Out-of-Band (RFC2833), SIP info
Access Control Function	
Lines	Two SIP lines, supporting SIP 2.0 (RFC3261) and related RFC
Open the Door Operation	DTMF, password, RFID card, switch
Door Phone Features	Full-duplex handsfree (HF) Default Auto Answer 200,000 door open records 2000 remote access list Up to 2000 RFID cards access Electric lock internal or external power supply options Support customized DSS keys Network Time Synchronization Action URL / Active URI remote control

Network and Protocols	
Network Standard	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3af Power over Ethernet IEEE 802.3at Power over Ethernet Plus
QoS	802.1p/q, DSCP
VPN	L2TP / openVPN
Protocol	Primary and secondary DNS VLAN SNTP client SRTP HTTP / HTTPS web pages MD5 authentication Web Filter DHCP / Static / PPPoE STUN Auto Provision TR069
Physical Specifications	
Keypad	1 DSS button (speed dial button) 4 indicator lights (including hot-key backlight) Numeric keypad
Switch	1 indoor switch 1 relay: MAX DC30V / 1A, AC125V / 0.5A Active switching output: 12V / 650mA DC
RFID Reader	ID (EM4100) standard type
Power Supply	12V ± 15% / 1A DC or 802.3af/at PoE
Power Requirements	802.3af PoE, (Class 3 - 6.49 to 12.95W)
Standby Power	2.76W, 12V / 230mA
Shell Material	Metal surface, ABS bottom shell
Protection Class	IP65
Installation	Wall-mounted installation

Net Weight	0.33kg
Dimensions (W x D x H)	160 x 93 x 35 mm
Emission	CE, FCC
Environment	
Operating Temperature	-20~60°C
Storage Temperature	-40~70°C
Relative Humidity	10~90%

Chapter 2. Hardware Interface and Installation

2.1 Physical Descriptions



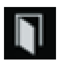
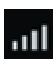
2.2 Description

Interface	Description
Camera	The door phone has a built-in IP camera supporting a high-resolution video of up to 1280 x 720 pixels.
Mic	The door phone has a built-in microphone hidden in the pinhole located on the front panel.
Speaker	The door phone has a built-in speaker for convenient communication and alert use.
RFID Reader	Use RFID cards to unlock the door by touching RFID reader of device.

Button Definition

Button	Description
Programmable Keys	It can be set with a variety of functions in order to meet the needs of different occasions
Numeric Keyboard	Input password to open the door or calls.

LED Definition

LED	Status	Description
 Lock	Steady Blue	Door unlocking
	Off	Door locking
 Call & Ring	Blinks per second	Call Hold or Ringing
	Off	On Hook
	Blinks every 3 seconds	Device in the issuing state
	Steady Blue	Online talking
 Network & SIP Registration	Blinks per second	Network error
	Off	Network is normal, SIP is not registered
	Blinks every 3 seconds	SIP Registration failed
	Steady Blue	SIP Registration succeeded

Chapter 3. Start Using

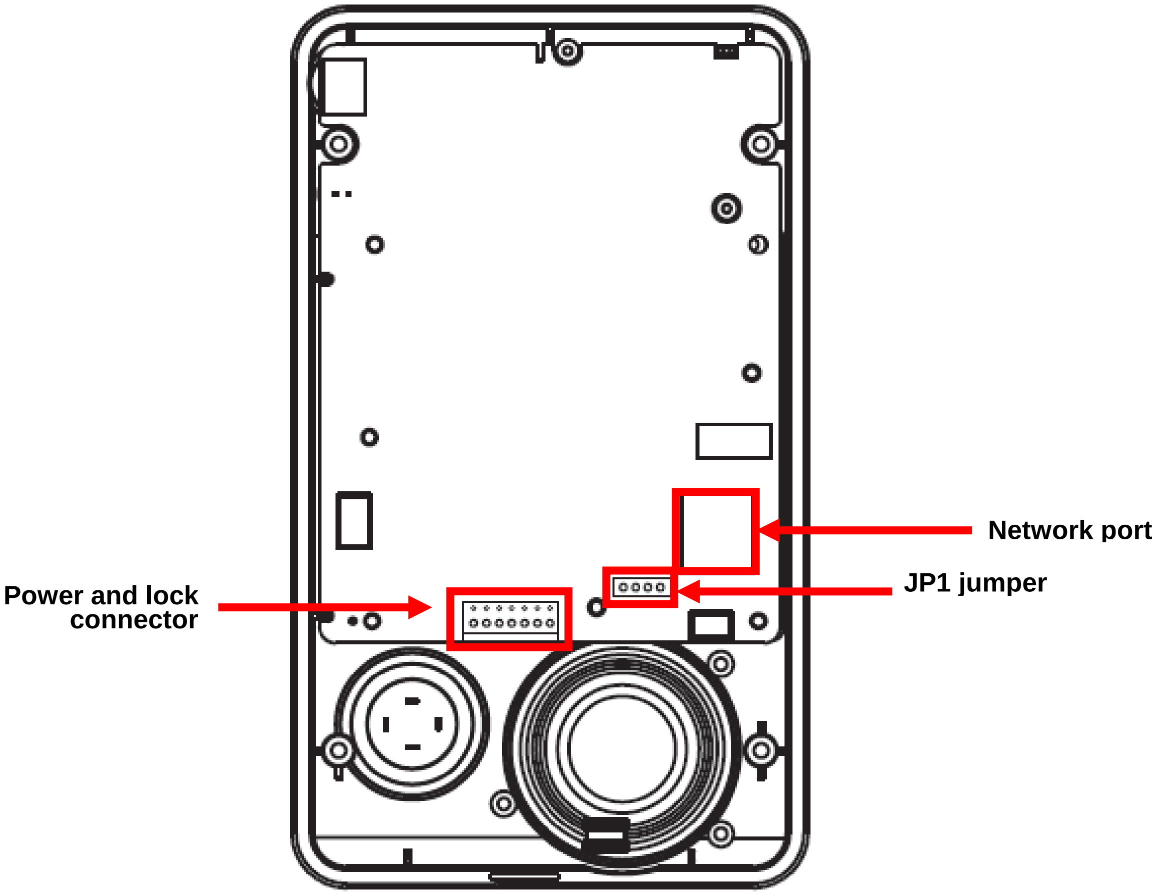
Before you start to use the equipment, please make the following installation.

3.1 Confirm the Connection

Confirm whether the equipment of the power cord, network cable and electric lock control line are accurately connected and the boot-up is normal. (Check the network state of light.)

3.1.1 I/O Control Description

After removing the front panel of HDP-5240PT, there are two terminal block connectors for power connection and digital I/O connections as shown in the picture below.



3.1.2 Power, Electric Lock, Indoor Switch Port

Voice access via 12V DC or PoE.

- **Power Connector**

The HDP-5240PT requires either IEEE 802.3af/at PoE or DC power from the power connector.

It shows the two-pin connector comes with a power source of 12V DC, 1A (max.).

- **Network Connector**

- **Power and Electric-lock Connector**

CN7						
1	**2**	**3**	**4**	**5**	**6**	**7**
+12V	VSS	NC	COM	NO	S_IN	S_OUT
12V DC, 1A		Electric-lock switch			Indoor switch	

3.1.3 Driving Mode of Electric Lock (Default in active mode)

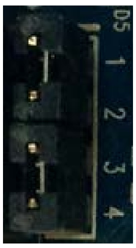
- **JP1 Jumper**

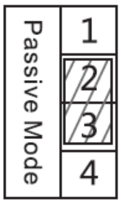
There are two modes for power supply of electric lock as shown in the picture below.

(The default is “Active Mode”.)

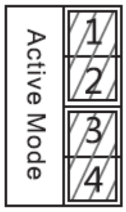
Passive Mode: When the electric lock starting current is more than 12V/650mA, the electric lock interface for short circuit output control in the external drive mode is used.

Active Mode: When the electric lock starting current is less than 12V/650mA, the electric lock interface with 12V DC output in the internal drive mode is used.





Jumper in passive mode

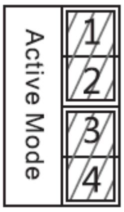
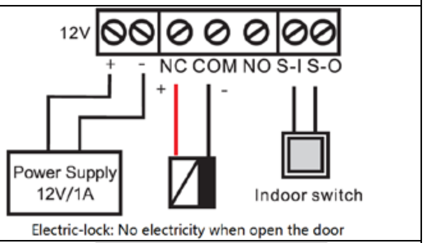
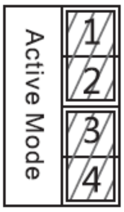
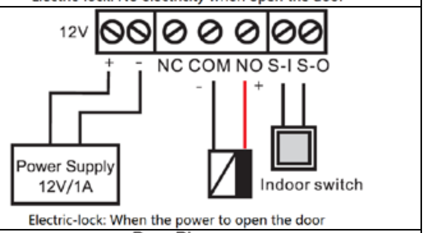
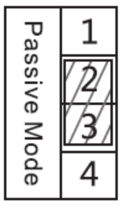
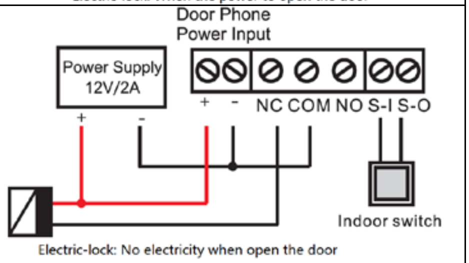
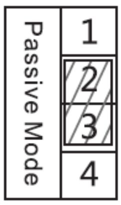
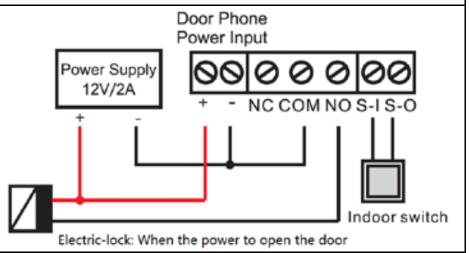
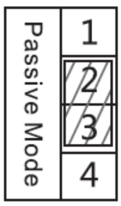
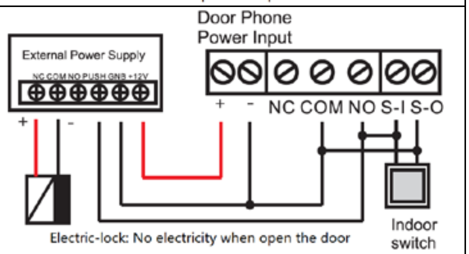


Jumper in active mode

Note	
Note	When the device is in the active mode, the maximum switch output is 12V, 650mA; if the electric lock needs power supply over 12V 650mA, it will ask the device in the passive mode to get an additional power to drive the lock to switch on/off. ● When using the active mode, it is 12V DC output. ● When using the passive mode, output is short control (normally open mode or normally close mode).

3.1.4 Wiring Instructions

- NO: Normally Open Contact.
- COM: Common Contact.
- NC: Normally Close Contact.

Driving Mode		Electric Lock		Jumper port	Connections
Active	Passive	No electricity when open	Power signaling to open		
√					
√			√		
	√	√			
	√		√		
	√	√			

3.2 Installation

The HDP-5240PT is constructed of four parts as shown below. Prior to the installation, the installer is required to remove the front panel of the HDP-5240PT for wall mounting. Please follow the steps below for the installation.

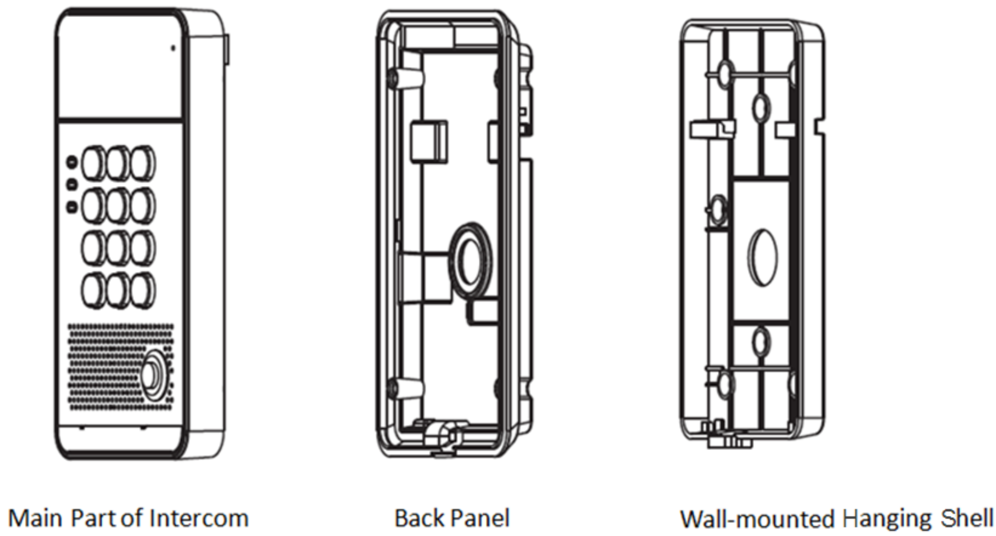


Figure 1 Three Major Parts of HDP-5240PT

Step 1: Installation Preparation

A. Check the following contents:

- Hex wrench x 1
- RJ45 plugs x 2 (1 spare)
- KA4 x 25mm screws x 4
- 25mm screw anchors x 4

B. Tools that may be required:

- Hex wrench
- Phillips screwdriver (Ph2 or Ph3), hammer, RJ45 crimper
- Electric impact drill with a 6mm drill bit.

Step 2: Drilling

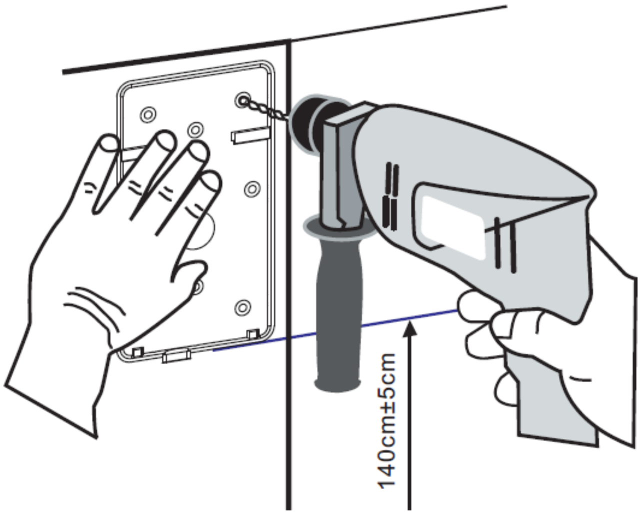


Figure 2 Wall Mounting

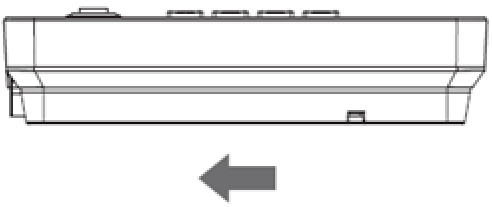
A. Place the mounting template with dimensions on the surface of a wall in a desired flat position.

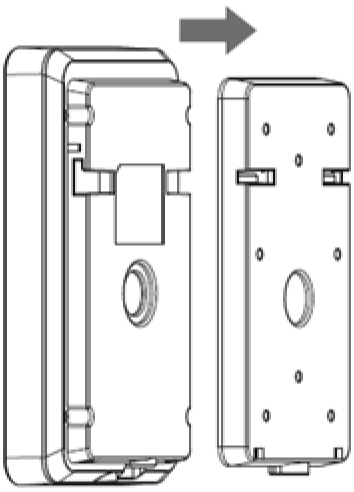
B. Use an electric drill to drill the 4 holes marked on the mounting template. It is recommended to drill about 30mm deep. Remove the template when finishing drilling.

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

Step 3: Removing Hanging Panel

A. Remove the hanging shell in Figure 3 and Figure 4.





en click

<Delete>.

B. With Phillips screwdriver, unpack the Back Panel and the main part of intercom as shown in Figure 5.

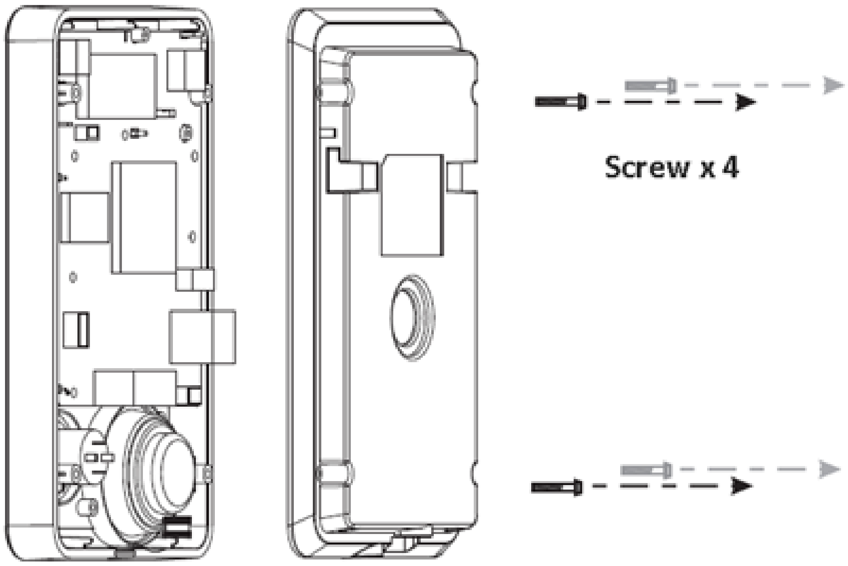


Figure 5

Step 4: Hanging Shell Fixing and Cabling

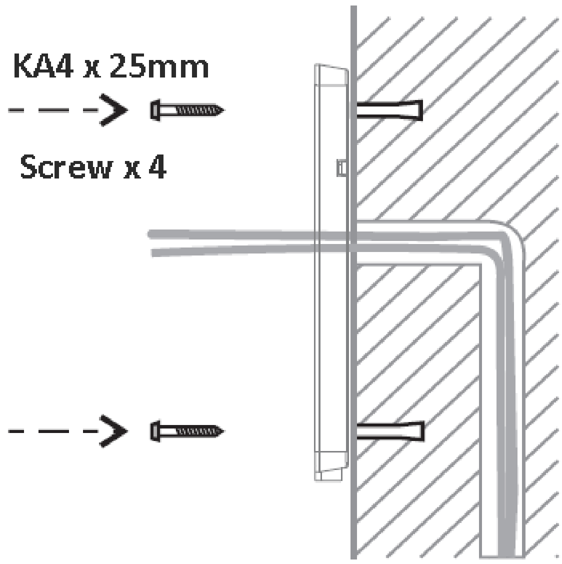


Figure 6

A. Select the hole for cable supply; cable length of 15cm to 20cm is recommended.

B. With 4 KA4 x 25mm screws, tighten the wall-mounted hanging shell as shown in Figure 6.

Step 5: Connection Line

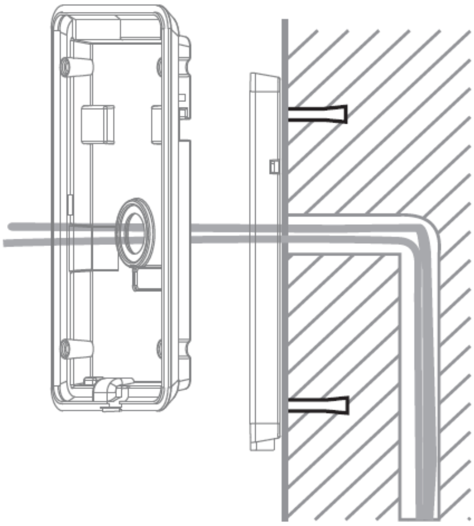


Figure 7

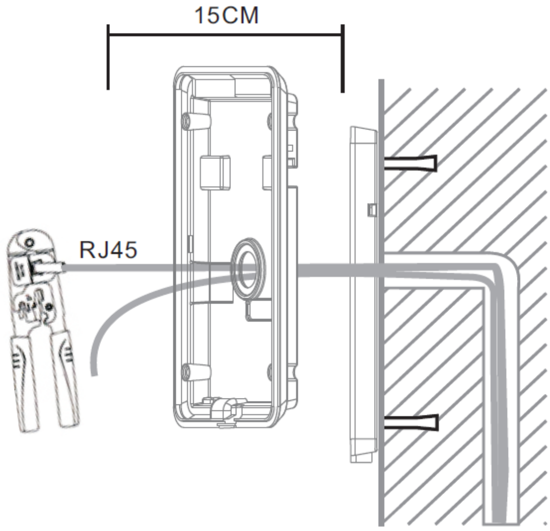


Figure 8

A. Select the hole for cable supply.

B. Connect the cables of RJ45, power, and electric lock to the motherboard socket as mentioned in connectors description (refer to Section 2).

C. Test whether there is electricity by doing the following:

(A) Press the # button for 3 seconds to get the IP address of intercom by voice.

(B) Input access password or press the indoor switch to check electric-lock installation.

Caution	Do not proceed mounting until you have finished checking the electricity!

Step 6: Mounting

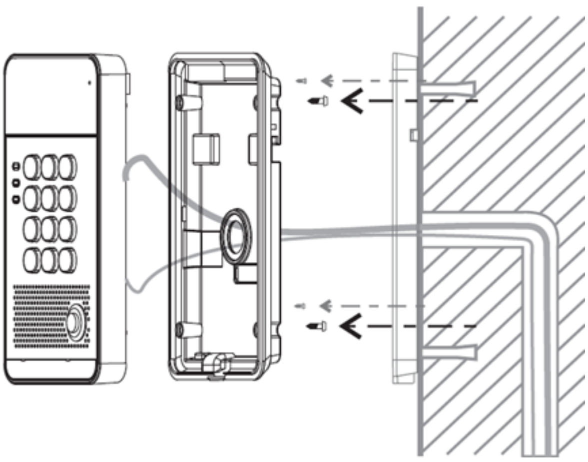


Figure 9

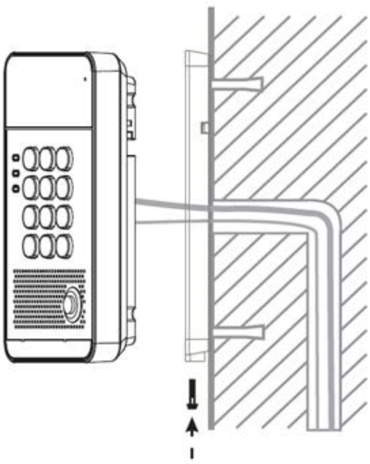


Figure 10

A. Use the 4 screws to tighten the main part of intercom on the back panel as shown in Figure 9.
B. Push the device into the wall-mounted hanging shell and tighten it with 1 screw as shown in Figure 10.
C. Make sure the screws have been tightened properly for better waterproof effect.

3.3 Quick Setting

The product provides a complete function and parameter setting. Users may need to have the network and SIP protocol knowledge to understand the meaning all parameters represent. In order to let equipment users enjoy the high quality of voice service and low cost advantage brought by the device immediately, here we list some basic but necessary setting options in this section to let users know how to operate the HDP-5240PT without understanding such complex SIP protocols.

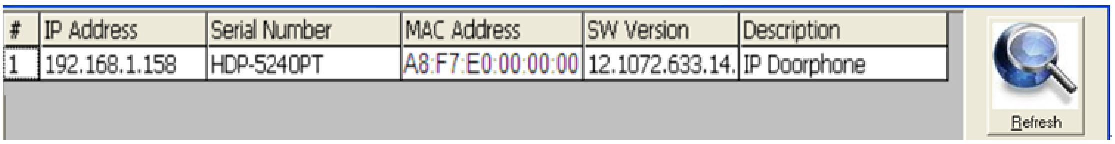
Prior to this step, please make sure your broadband Internet can be normally operated, and you must complete the connection of the network hardware.

Press and hold **"#"** key for **3** seconds; the door phone would report the IP address by voice.

Or you can also use the **"Planet Door Phone Finder Utility"** software to find the IP address of the device.

Note	When the HDP-5240PT is powered on, wait for 30 seconds before running the device.

A. Log on to the Web device configuration.
B. On the line configuration page, service account, user name, server address and other parameters are required for server address registration.
C. You can set DSS key on the function key page.
D. You can set Door Phone parameters on the web page (**Phone Settings -> Features**).



#	IP Address	Serial Number	MAC Address	SW Version	Description
1	192.168.1.158	HDP-5240PT	A8:F7:E0:00:00:00	12.1072.633.14.	IP Doorphone

Chapter 4. Basic Operation

4.1 Answer a Call

When a call comes in, the device would answer automatically. If you cancel auto answer feature and set auto answer time, you would hear the ring at the set time and the device would auto answer after configuring the timer.

4.2 Call

Configure the shortcut key as hot key and then set up a number; after that you might press the shortcut key for making a call to the configured extension(s).

4.3 End Call

Enable the Release (You can enable release) key for hanging up feature to end call.

4.4 Open the Door

You might open door through the following seven ways:

A. Input password on the keyboard to open the door.
B. Have access to calling the owner and the owner enters the remote password to open the door.
C. Owner/other equipment accesses control and enter the access code to open the door. (access code should be included in the list of access configuration, and enabled for remote calls to open the door)
D. Swipe the RFID cards to open the door.
E. Use the indoor switch to open the door.
F. Use private access code to open the door.
   Enable for local authentication, and set private access code. Input the access code directly in standby mode to open the door. In this way, the door log would record corresponding card number and user name.
G. Active URL control command to open the door.
   URL is “http://user:pwd@host/cgi-bin/ConfigManApp.com?key=F_LOCK&code=openCode”
   (A) User and pwd are the user name and password of logging on to web page.
   (B) “openCode” is the remote control code to open the door.
   For example, “http://admin:admin@172.18.3.25/cgi-bin/ConfigManApp.com?key=*”

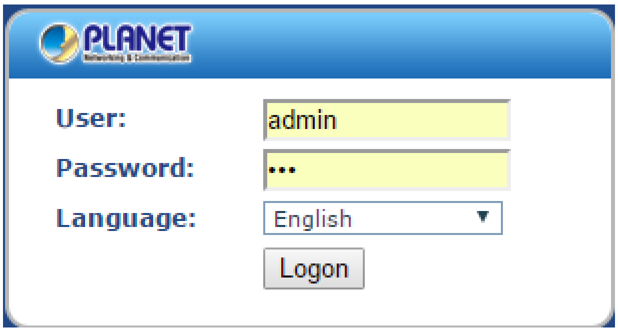
If access code has been input correctly, the device would play siren sound to prompt the HDP-5240PT and the remote user, while input error by low-frequency short chirp. Password input successfully followed by high-frequency siren sound, while input falsely, there would be high-frequency short chirp. When the door has been opened, the device would play siren sound to prompt guests.

Chapter 5. Page Settings

5.1 Browser Configuration

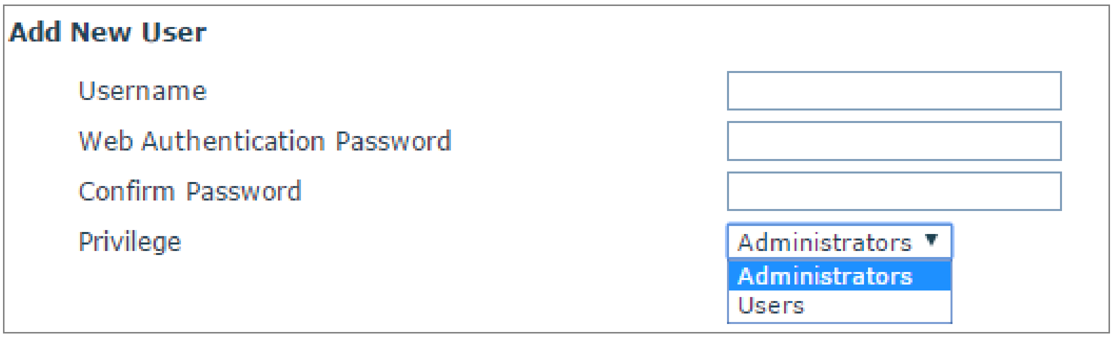
When the device and your computer are successfully connected to the network, you might enter the IP address of the device in the browser as http://172.16.0.1/ and you can see the login interface of the web page management.

Enter the user name and password and click the Logon button to enter the settings screen.



5.2 Password Configuration

There are two levels of access: **Administrator** level and **User** level. A user with root level can browse and set all configuration parameters, while a user with general level can set all configuration parameters except server parameters for SIP.



A. User level: It is not set by default; you can add the feature when needed.

B. User uses Administrator level by default:

(A) User name: **admin**

(B) Password: **123**

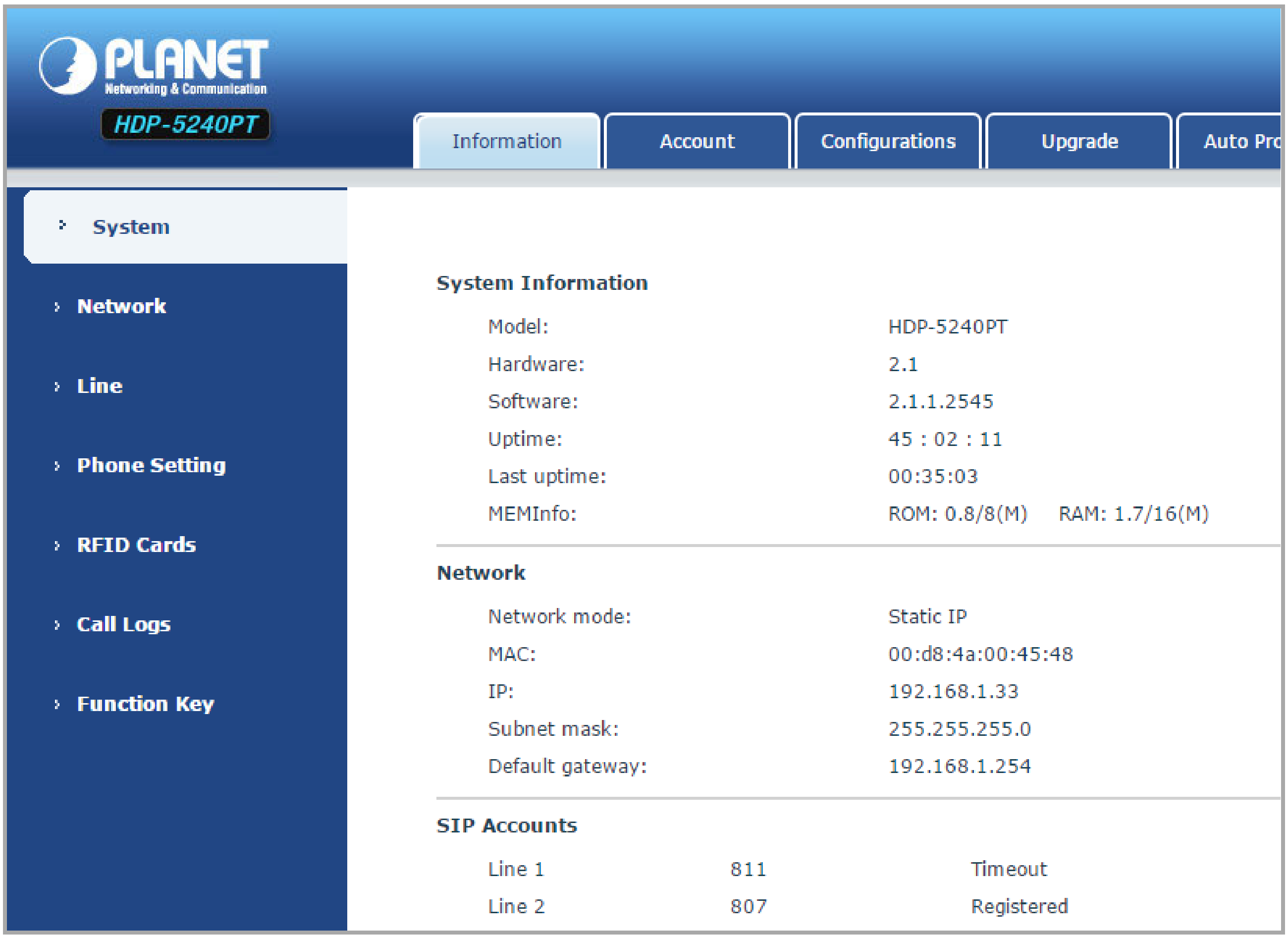
Default Setting	
Default DHCP Client	Off
Default IP Address	172.16.0.1

Default Setting	
Default Web Port	80
Default Login User Name	admin
Default Login Password	123
Report IP Address	Hold # key for 3 seconds to report IP address by voice
Searching Tools	Planet Door Phone Finder

5.3 Configuration via Web

5.3.1 System

A. Information

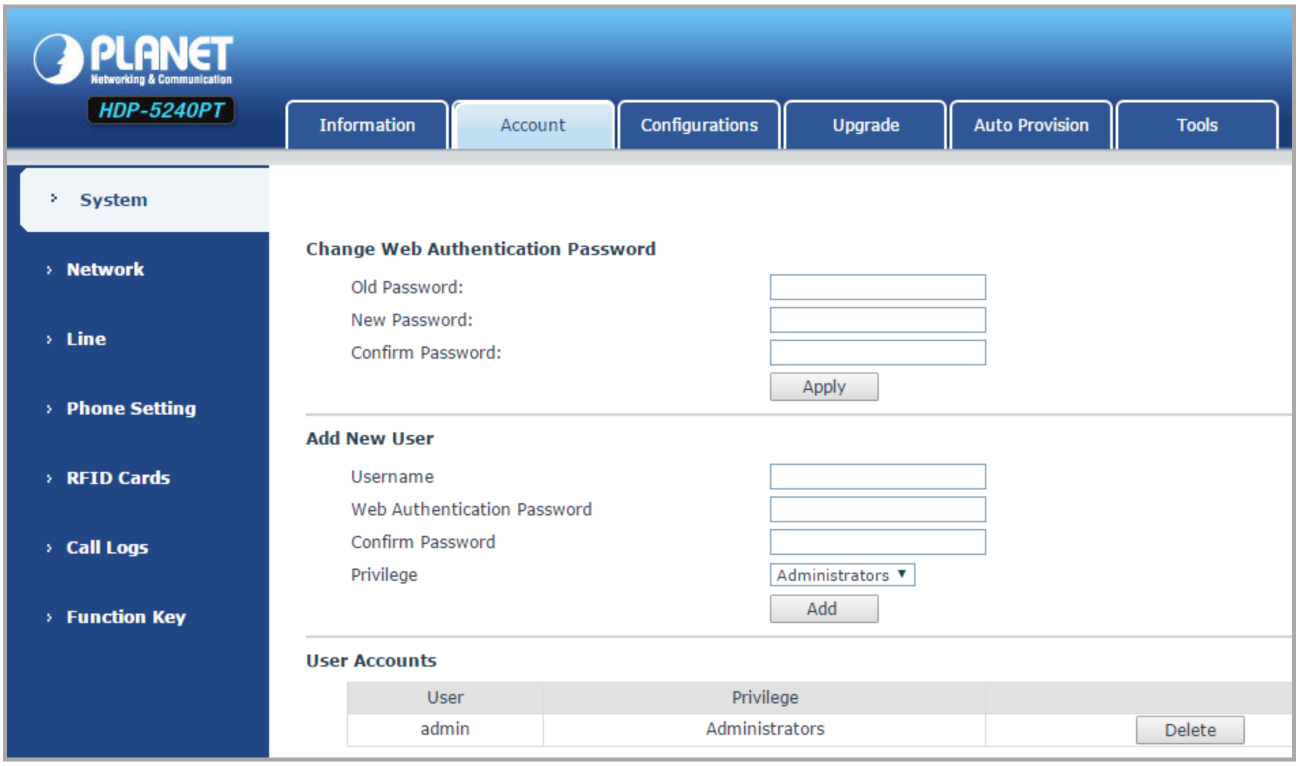


Information	
Field Name	**Explanation**
System Information	Display equipment model, hardware version, software version, uptime, last uptime and meminfo.

Information	
Field Name	**Explanation**
Network	Shows the configuration information of WAN port, including connection mode of WAN port (Static, DHCP, PPPoE), MAC address, IP address of WAN port.
SIP Accounts	Shows the phone numbers and registration status of the 2 SIP lines.

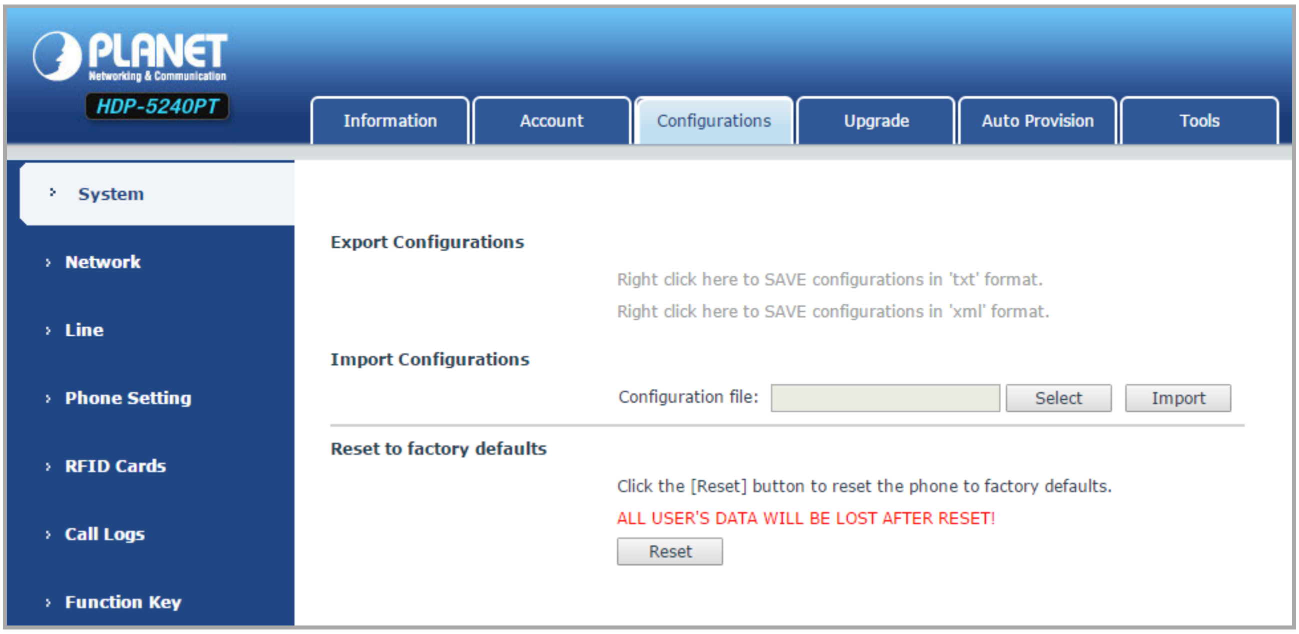
B. Account

Through this page, administrator can add or remove user accounts depending on their needs, or modify the existing user accounts by permission.



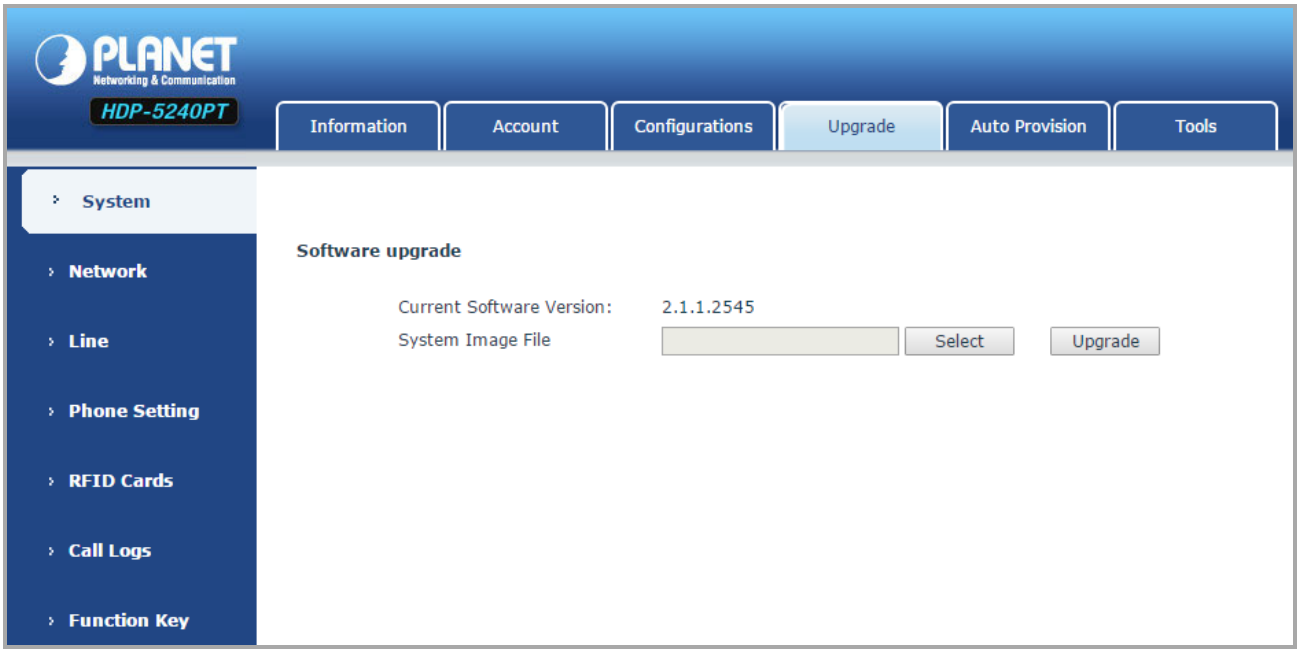
Account	
Field Name	**Explanation**
Change Web Authentication Password	You can modify the login password of the account
Add New User	You can add new user
User Accounts	Show the existing user accounts' information

C. Configurations



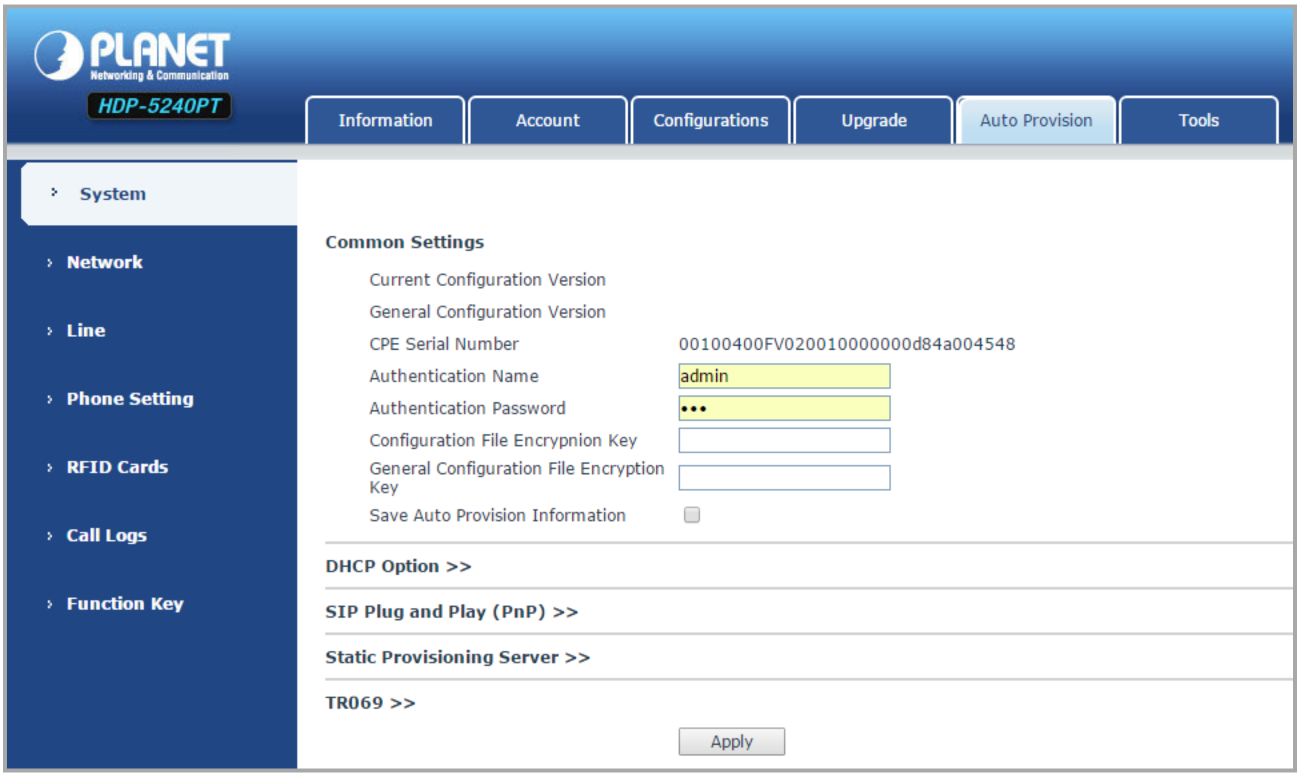
Configurations	
Field Name	**Explanation**
Export Configurations	Save the equipment configuration to a txt or xml file. Please right-click on the choice and then choose “Save Link As.”
Import Configurations	Find the config file, and press Update to load it to the equipment.
Reset to factory defaults	The HDP-5240PT would restore to factory default configuration and remove all configuration information.

D. Upgrade



Upgrade	
Field Name	**Explanation**
Software upgrade	
Find the firmware, and press Update to load it to the equipment.	

E. Auto Provision

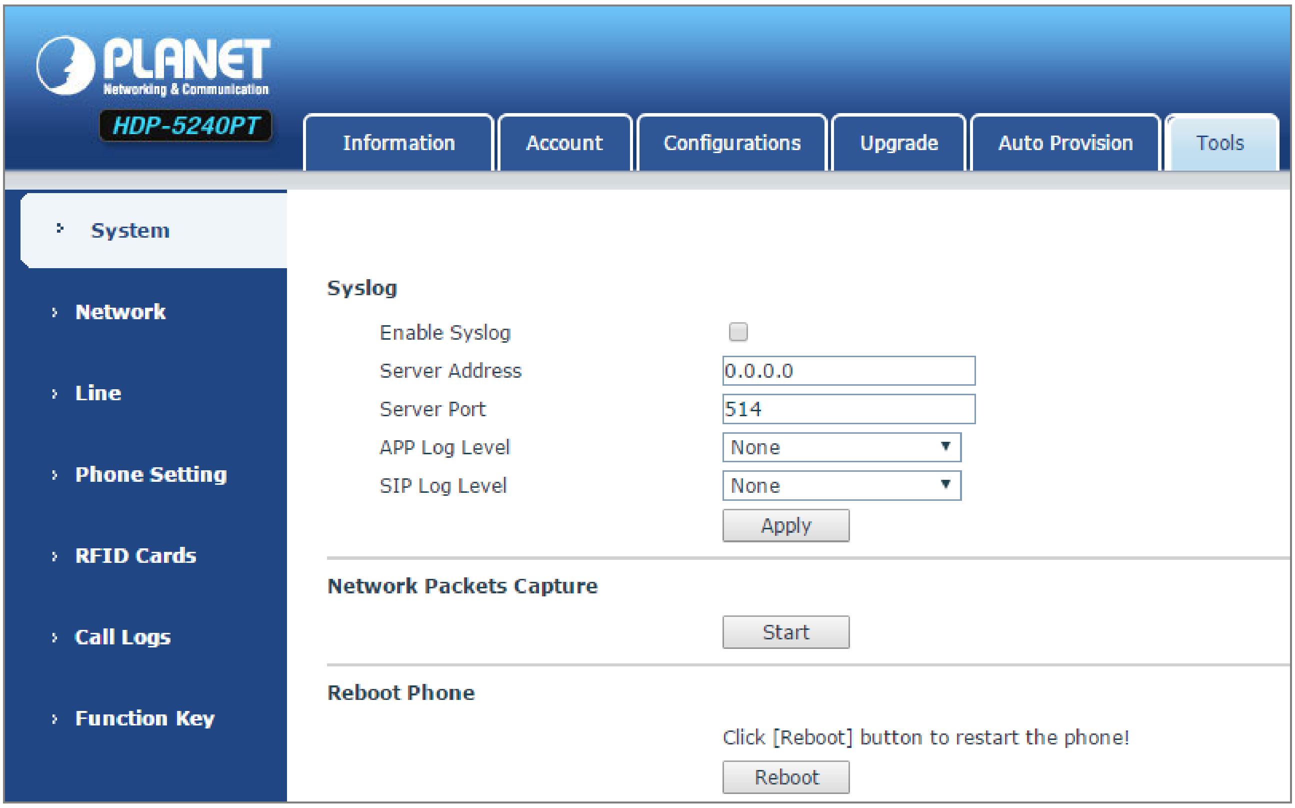


Auto Provision	
Field Name	**Explanation**
Common Settings	
Current Configuration Version	Show the current config file's version. If the config file to be downloaded is higher than the current version, the configuration would be upgraded. If the endpoints confirm the configuration by the Digest method, the configuration would not be upgraded unless it differs from the current configuration
General Configuration Version	Show the common config file's version. If the configuration to be downloaded and this configuration is the same, the auto provision would stop. If the endpoints confirm the configuration by the Digest method, the configuration would not be upgraded unless it differs from the current configuration.
CPE Serial Number	Serial number of the equipment
Authentication Name	Username for configuration server. It is used for FTP/HTTP/HTTPS. If this is blank, the phone would use anonymous access
Authentication Password	Password for configuration server. It is used for FTP/HTTP/HTTPS.
Configuration File Encryption Key	Encryption key for the configuration file

Auto Provision	
Field Name	**Explanation**
General Configuration File Encryption Key	Encryption key for common configuration file
Save Auto Provision Information	Save the auto provision username and password in the phone until the server URL is changed
DHCP Option	
Option Value	The equipment supports configuration from Option 43, Option 66, or a Custom DHCP option. It may also be disabled.
Custom Option Value	Custom option number. It must be from 128 to 254.
SIP Plug and Play (PnP)	
Enable SIP PnP	If it is enabled, the equipment would send SIP SUBSCRIBE messages to the server address when it boots up. Any SIP server compatible with that message would reply with a SIP NOTIFY message containing the Auto Provisioning Server URL where the phones can request their configuration.
Server Address	PnP Server Address
Server Port	PnP Server Port
Transportation Protocol	PnP Transfer protocol – UDP or TCP
Update Interval	Interval time for querying PnP server. Default is 1 hour.
Static Provisioning Server	
Server Address	Set FTP/TFTP/HTTP server IP address for auto update. The address can be an IP address or domain name with subdirectory.
Configuration File Name	Specify configuration file name. The equipment would use its MAC ID as the config file name if this is blank.
Protocol Type	Specify the Protocol type FTP, TFTP or HTTP.
Update Interval	Specify the update interval time. Default is 1 hour.
Update Mode	1. Disable – not to update 2. Update after reboot – update only after reboot. 3. Update at time period – update at periodic update period
TR069	
Enable TR069	Enable/Disable TR069 configuration
ACS Server Type	Select Common or CTC ACS Server Type.
ACS Server URL	ACS Server URL.
ACS User	User name of ACS.
ACS Password	ACS Password.
TR069 Auto Login	Enable/Disable TR069 Auto Login.

Auto Provision	
Field Name	**Explanation**
INFORM Sending Period	Time between transmissions of “Inform”; the unit is second.

F. Tools



Syslog is a protocol used to record log messages using a client/server mechanism. The Syslog server receives the messages from clients, and classifies them based on priority and type. Then these messages would be written into a log by rules which the administrator has configured.

There are 8 levels of debug information.

Level 0 (emergency): System is unusable. This is the highest debug info level.

Level 1(alert): Action must be taken immediately.

Level 2 (critical): System is probably working incorrectly.

Level 3 (error): System may not work correctly.

Level 4 (warning): System may work correctly but needs attention.

Level 5 (notice): It is normal but significant condition.

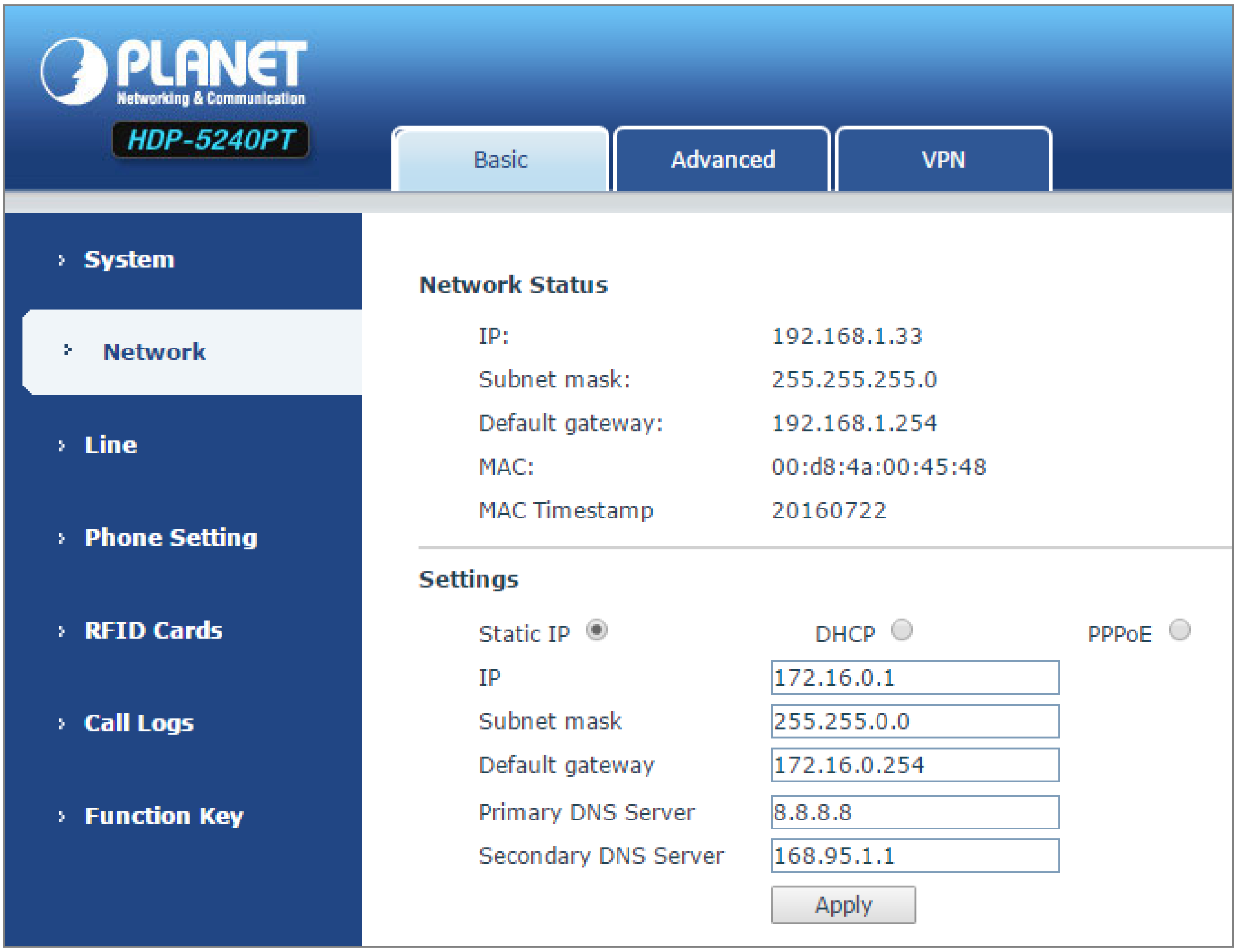
Level 6 (informational): It is normal daily message.

Level 7 (debug): Debug messages normally are used by system designer. This level can only be displayed via telnet.

Tools	
Field Name	**Explanation**
Syslog	
Enable Syslog	Enable or disable system log.
Server Address	System log server IP address.
Server Port	System log server port.
App Log Level	Set the level of App log.
SIP Log Level	Set the level of SIP log.
Network Packets Capture	
Capture a packet stream from the equipment. This is normally used to troubleshoot problems.	
Reboot Phone	
Some configuration modifications require a reboot to become effective. Clicking the Reboot button would lead to reboot immediately. Note: Be sure to save the configuration before rebooting.	

5.3.2 Network

A. Basic



Field Name	Explanation
Network Status	
IP	The current IP address of the equipment
Subnet Mask	The current Subnet Mask
Default Gateway	The current Gateway IP address
MAC	The MAC address of the equipment
MAC Timestamp	Get the MAC address' time.
Settings	
Select the appropriate network mode. The equipment supports three network modes:	
Static IP	Network parameters must be entered manually and would not change. All parameters are provided by the ISP.
DHCP	Network parameters are provided automatically by a DHCP server.
PPPoE	Account and Password must be input manually. These are provided by your ISP.

Field Name	Explanation
If static IP is chosen, the screen below would 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.
After entering the new settings, click the **Apply** button. The equipment would save the new settings and apply them. If a new IP address was entered for the equipment, it must be used to login to the phone after clicking the **Apply** button.	

B. Advanced

The equipment supports 802.1Q/P protocol and DiffServ configuration. VLAN function can support the different VLAN ID mode of processing the WAN port and LAN port.

(A) Chart 1 shows a network switch with no VLAN. Any broadcast frames would be transmitted to all other ports. For example, frames broadcast from port 1 would be sent to Ports 2, 3, and 4.

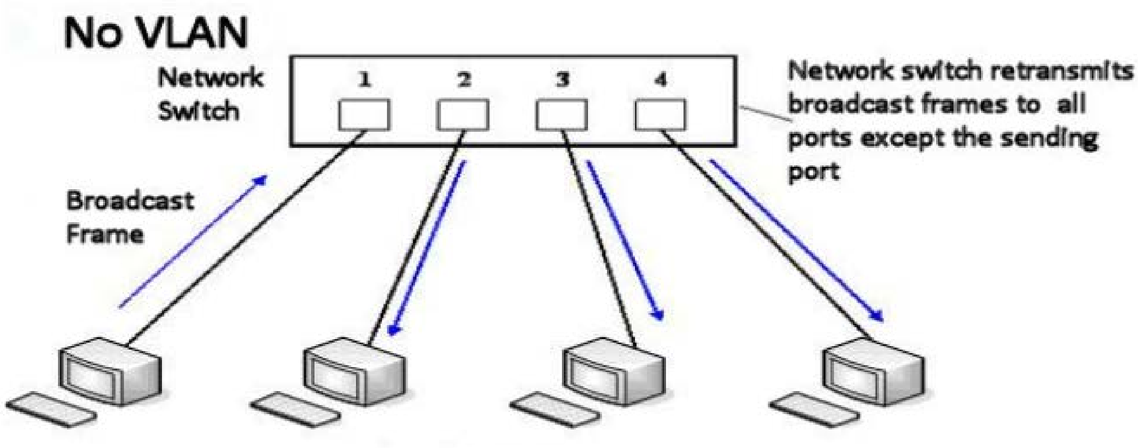
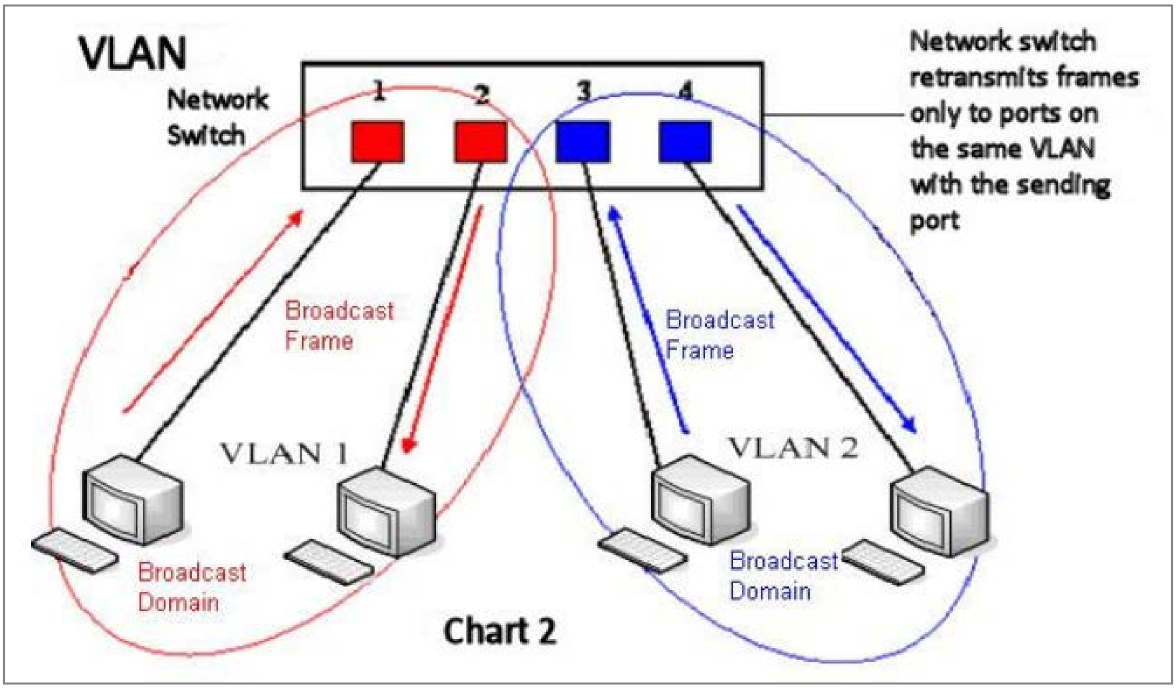
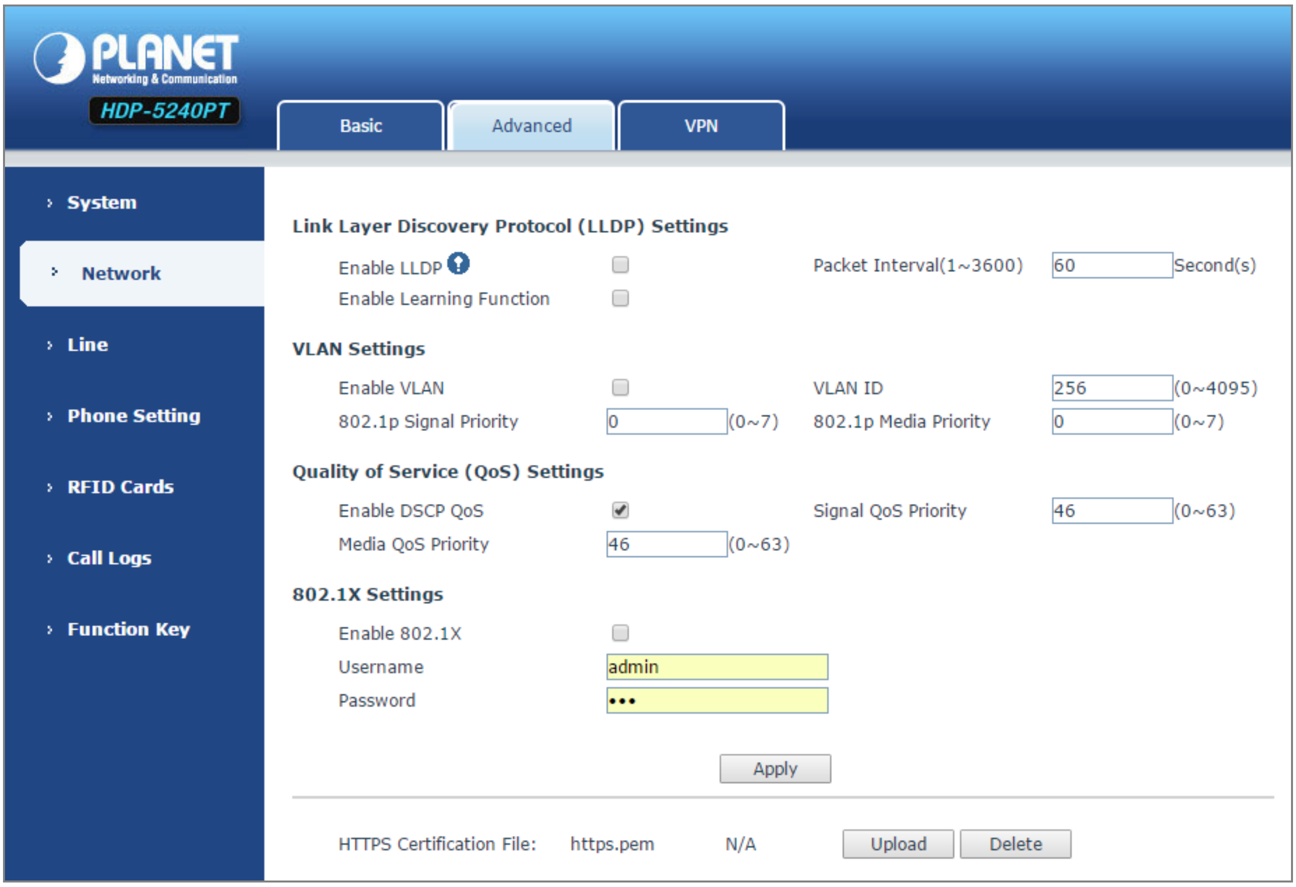


Chart 1

(B) Chart 2 shows an example with two VLANs indicated in red and blue. In this example, frames broadcast from Port 1 would only go to Port 2 since Ports 3 and 4 are in a different VLAN. VLANs can be used to divide a network by restricting the transmission of broadcast frames.

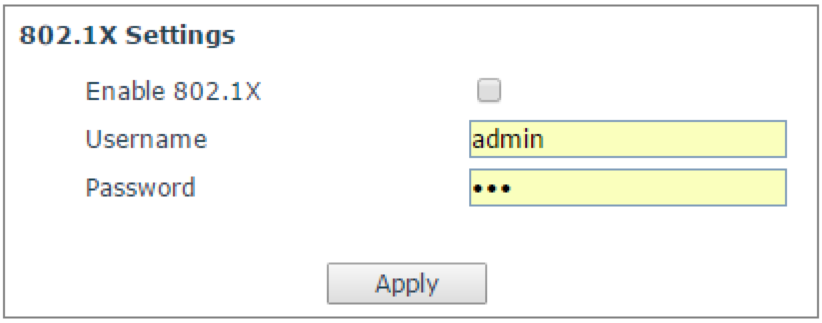


Note	In practice, VLANs are distinguished by the use of VLAN IDs.



Advanced	
Field Name	**Explanation**
Link Layer Discovery Protocol (LLDP) Settings	
Enable LLDP	Enable or Disable Link Layer Discovery Protocol (LLDP).
Enable Learning Function	Enables the telephone to synchronize its VLAN data with the Network Switch. The telephone would automatically synchronize DSCP, 802.1p, and VLAN ID values even if these values differ from those provided by the LLDP server.
Packet Interval (1~3600)	The time interval of sending LLDP Packets
VLAN Settings	
Enable VLAN	Enable or Disable WAN port VLAN.
VLAN ID	Specify the value of the VLAN ID. Range is 0-4095.
802.1p Signal Priority	Specify the value of the signal 802.1p priority. Range is 0-7.
802.1p Media Priority	Specify the value of the voice 802.1p priority. Range is 0-7.
Quality of Service (QoS) Settings	
Enable DSCP QoS	Enable or Disable Differentiated Services Code Point (DSCP).
Media QoS Priority	Specify the value of the Media DSCP in decimal.
Signal QoS Priority	Specify the value of the Signal DSCP in decimal.

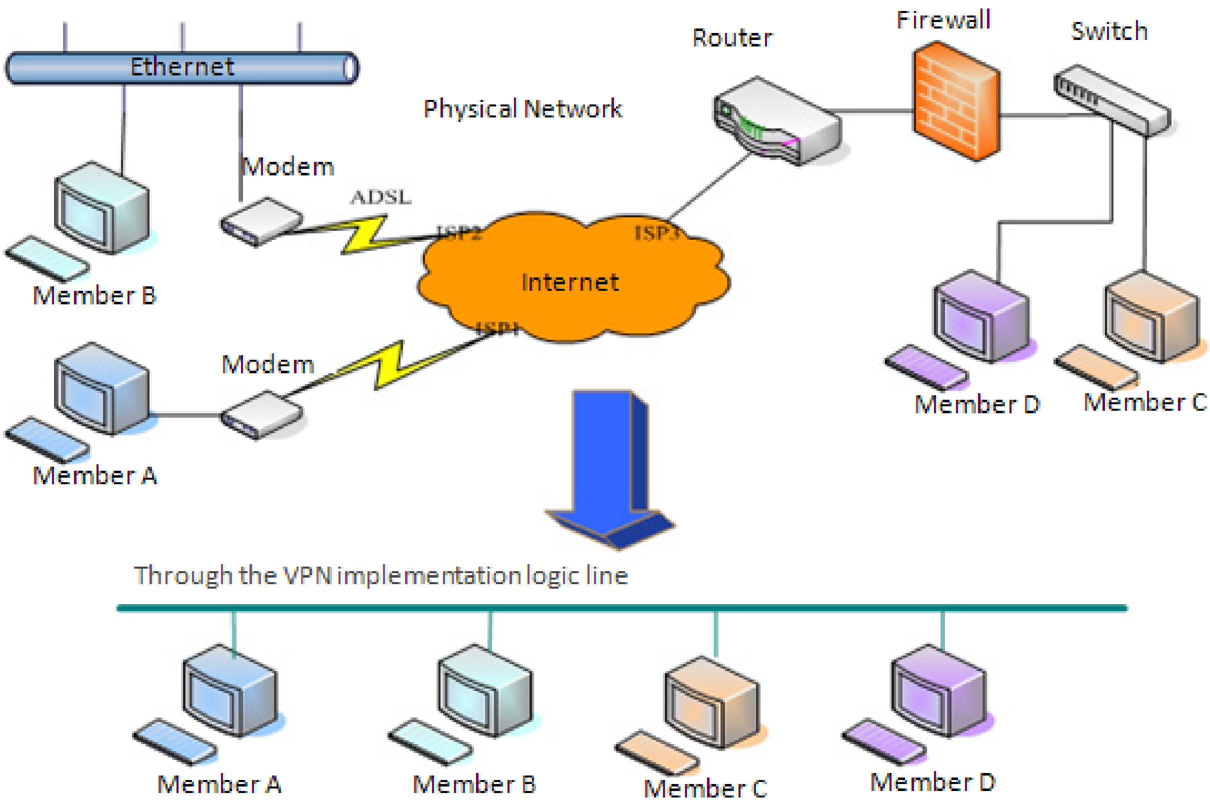
802.1X Settings

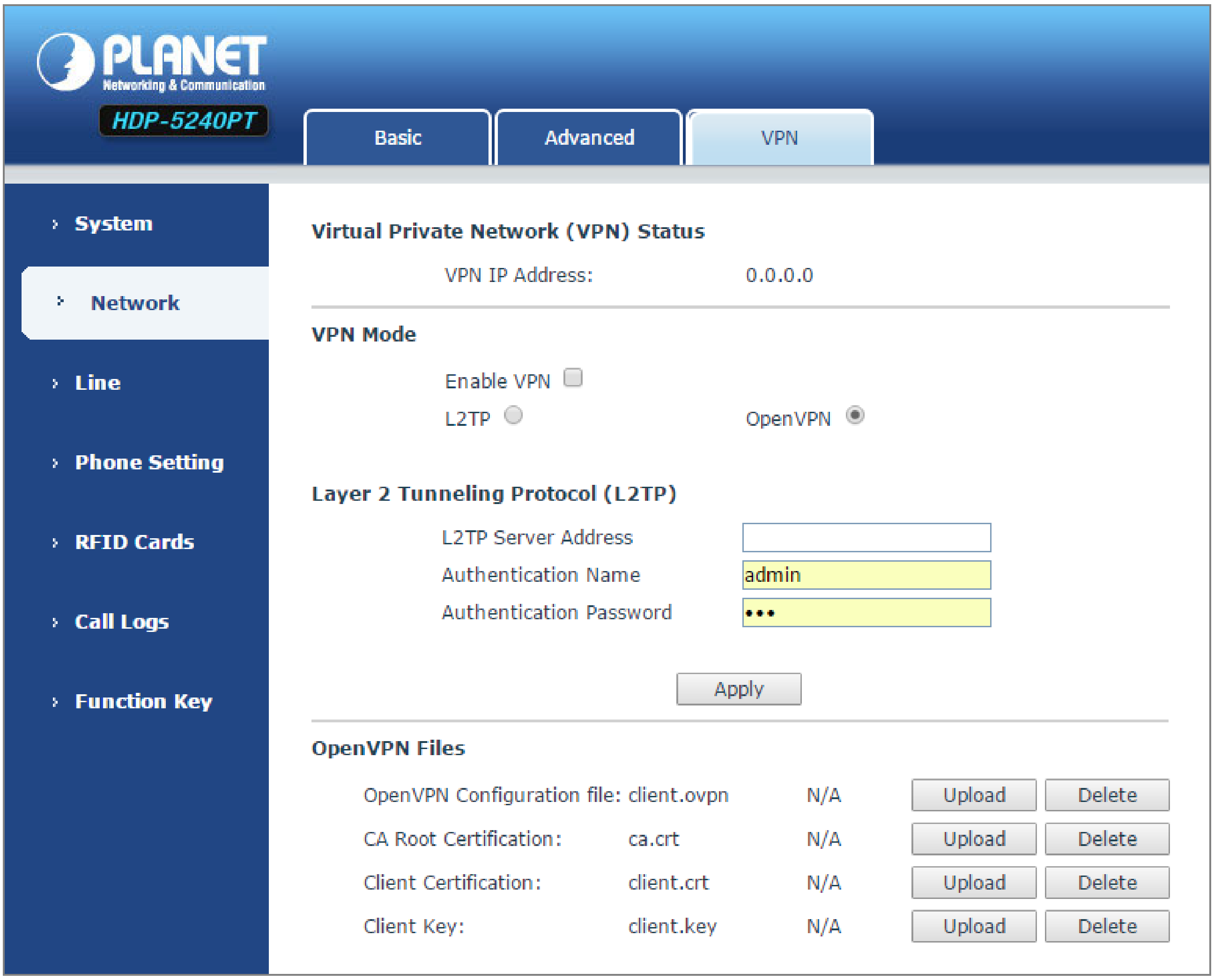


Enable 802.1X	Enable or Disable 812.1X.
Username	802.1X user account
Password	802.1X password
HTTPS Certification File	
Upload or delete HTTPS Certification File.	

C. VPN

The device supports remote connection via VPN. It supports both Layer 2 Tunneling Protocol (L2TP) and OpenVPN protocol. This allows users at remote locations on the public network to make secure connections to local networks.



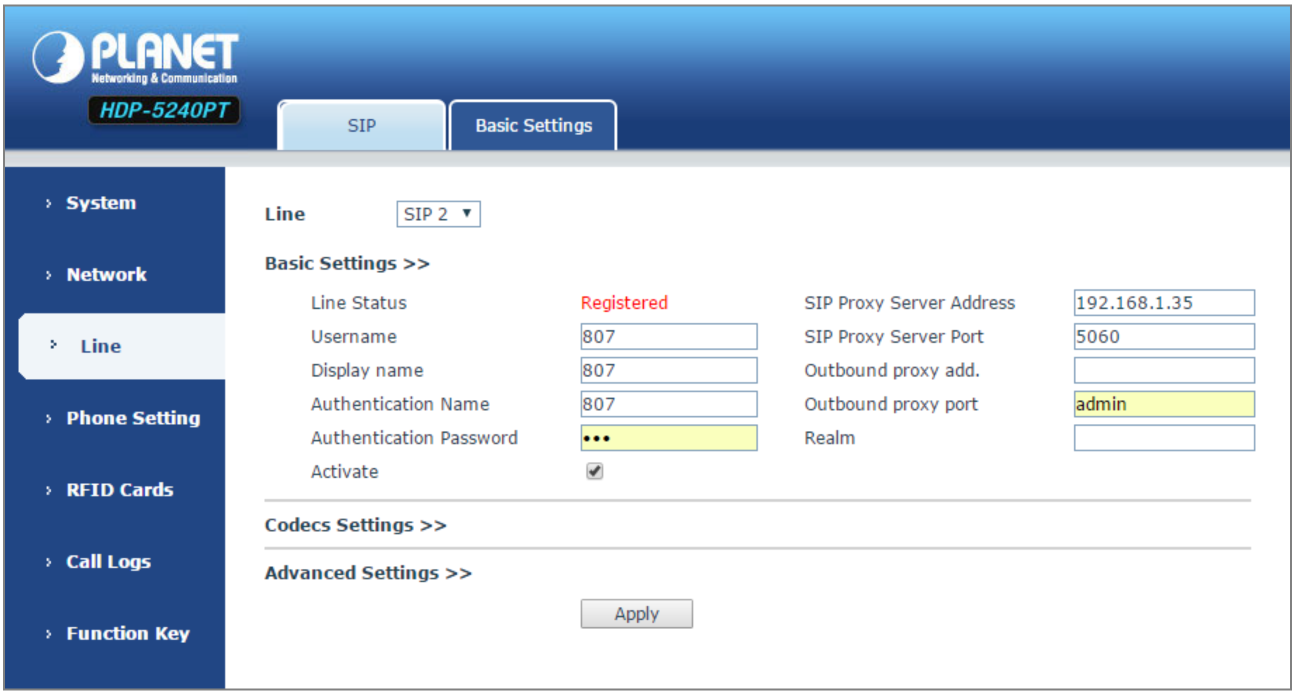


Field Name	Explanation
VPN IP Address	Shows the current VPN IP address.
VPN Mode	
Enable VPN	Enable/Disable VPN.
L2TP	Select Layer 2 Tunneling Protocol.
OpenVPN	Select OpenVPN Protocol. (Only one protocol may be activated. After the selection is made, the configuration should be saved and the phone be rebooted.)
Layer 2 Tunneling Protocol (L2TP)	
L2TP Server Address	Set VPN L2TP Server IP address.
Authentication Name	Set User Name access to VPN L2TP Server.
Authentication Password	Set Password access to VPN L2TP Server.
Open VPN Files	
Upload or delete Open VPN Certification Files.	

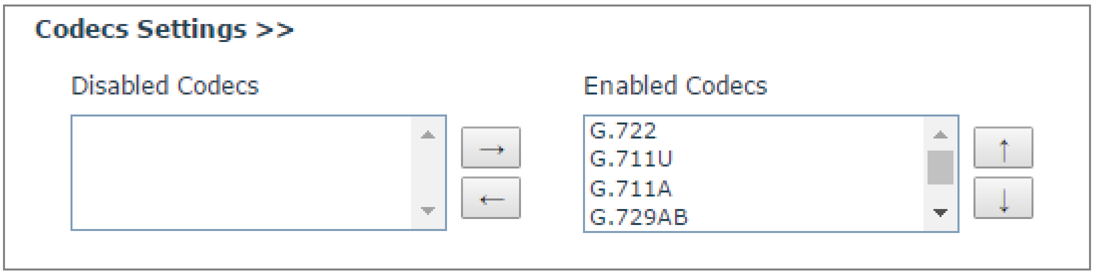
5.3.3 Line

A. SIP

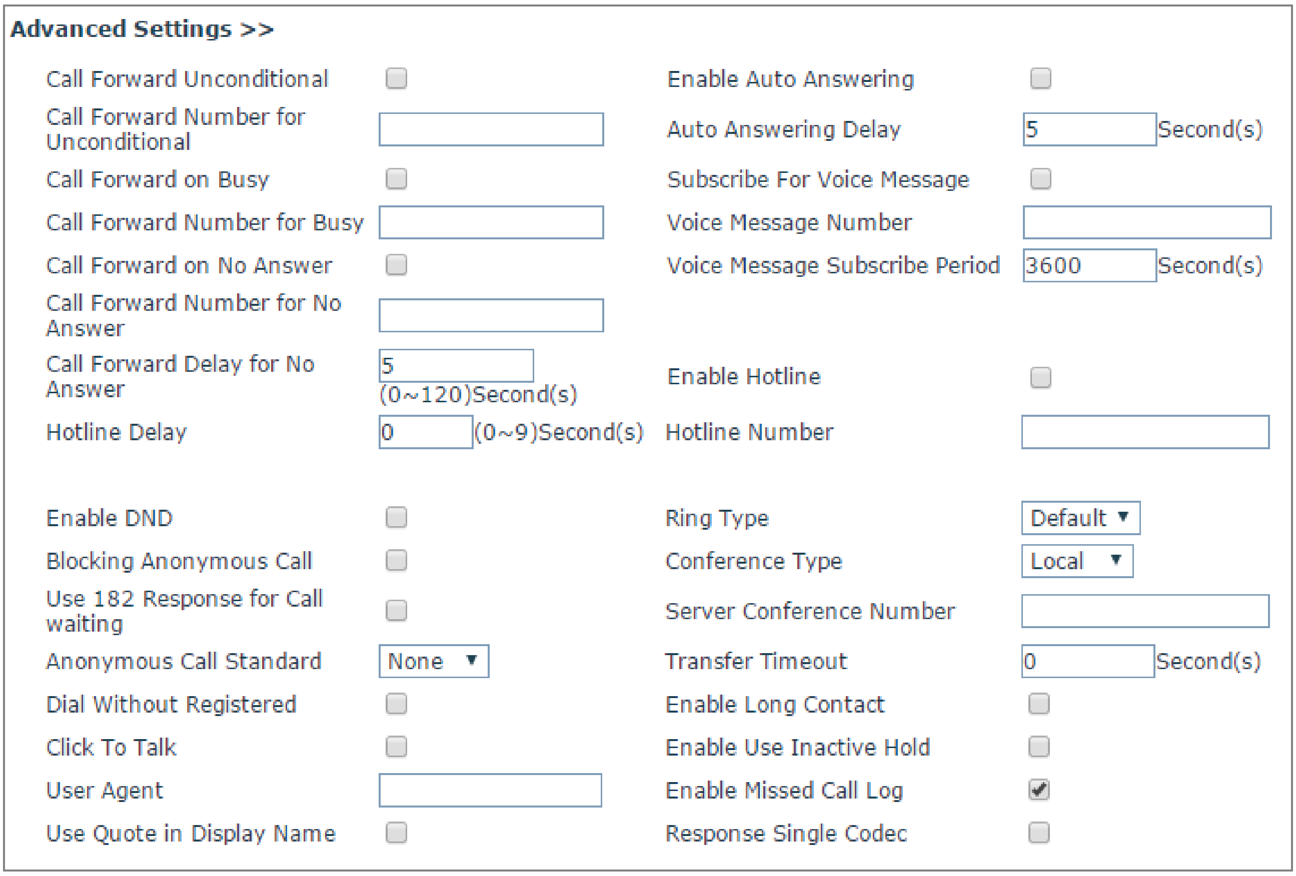
You can configure a SIP server on this page.

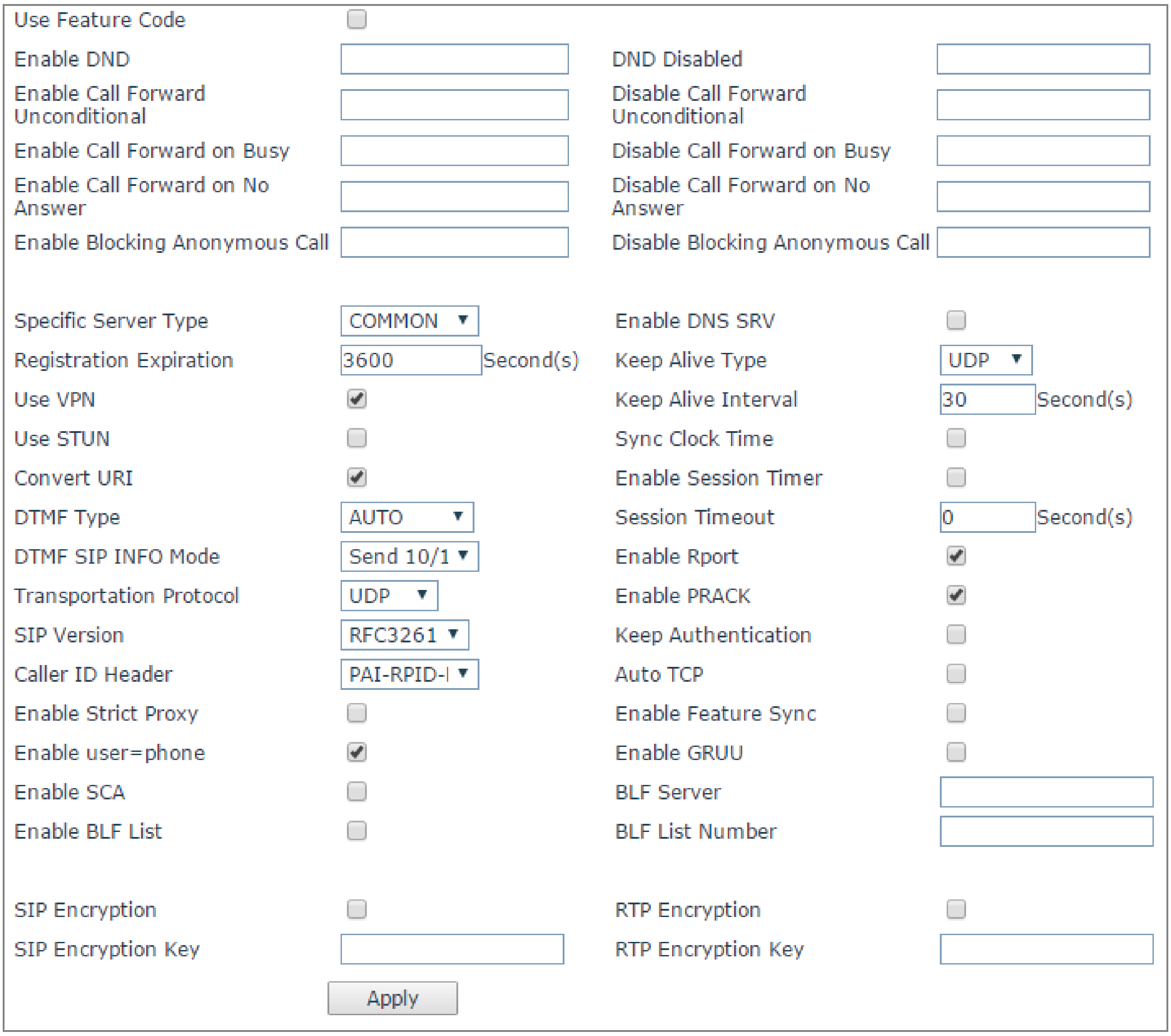


SIP	
Field Name	**Explanation**
Basic Settings (Choose the SIP line to configure)	
Line Status	Display the current line status after page loading. To get the up-to-date line status, user has to refresh the page manually.
User Name	Enter the username of the service account.
Display Name	Enter the display name to be sent in a call request.
Authentication Name	Enter the authentication name of the service account.
Authentication Password	Enter the authentication password of the service account.
Activate	Whether the service of the line should be activated.
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server.
SIP Proxy Server Port	Enter the SIP proxy server port, default is 5060.
Outbound proxy address	Enter the IP or FQDN address of outbound proxy server provided by the service provider.
Outbound proxy port	Enter the outbound proxy port, default is 5060.
Realm	Enter the SIP domain if it is needed by the service provider.



SIP	
Field Name	**Explanation**
Codecs Settings	
Set the priority and availability of the codecs by adding or removing them from the list.	





SIP	
Field Name	**Explanation**
Advanced Settings	
Call Forward Unconditional	Enable unconditional call forwarding; all incoming calls would be forwarded to the number specified in the next field.
Call Forward Number for Unconditional	Set the number of unconditional call forwarding.
Call Forward on Busy	Enable call forward on busy; when the phone is busy, any incoming call would be forwarded to the number specified in the next field.
Call Forward Number for Busy	Set the number of call forwarding when the HDP-5240PT is busy.
Call Forward on No Answer	Enable call forward on no answer; when an incoming call is not answered within the configured delay time, the call would be forwarded to the number

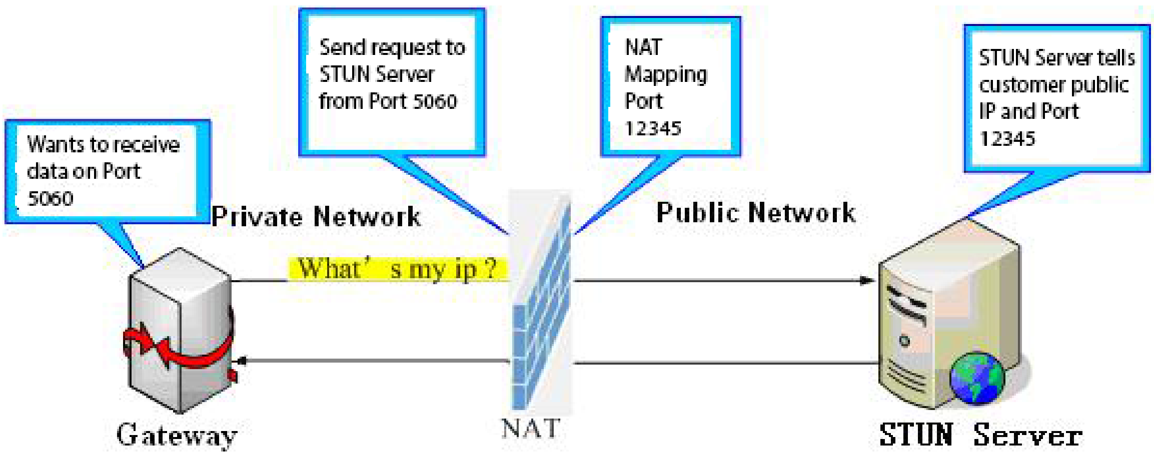
SIP	
Field Name	**Explanation**
	specified in the next field.
Call Forward Number for No Answer	Set the number of call forward on no answer.
Call Forward Delay for No Answer	Set the delay time of not answered call before being forwarded.
Hotline Delay	Set the delay for hotline before the system automatically dial it.
Enable Auto Answering	The incoming calls would be answered automatically after the delay time.
Auto Answering Delay	Set the delay for incoming call before the system automatically answers it.
Subscribe For Voice Message	Enable the device to subscribe a voice message waiting notification. If you enable it , the device would receive notification from the server if there is voice message waiting on the server.
Voice Message Number	Set the number for retrieving voice message.
Voice Message Subscribe Period	Set the period of voice message notification subscription.
Enable Hotline	The device would dial to the specific number immediately at audio channel opened by off-hook or turning on hands-free speaker or headphone.
Hotline Number	Set the hotline dialing number.
Enable DND	Any incoming call on this line would be rejected automatically.
Blocking Anonymous Call	Reject any incoming call without presenting caller ID.
Use 182 Response for Call waiting	Set the device to use 182 response code at call waiting response.
Anonymous Call Standard	Set the standard to be used for anonymous call.
Dial Without Registered	Set call out by proxy without registration.
Click To Talk	Set Click To Talk.
User Agent	Set the user agent -- the default is Model with Software Version.
Use Quote in Display Name	Whether to add quote in display name.
Ring Type	Set the ring tone type for the line.
Conference Type	Set the type of call conference -- For Local, set up call conference by the device itself; HDP-5240PT supports two remote parties. For Server, set up call conference by dialing to a conference room on the server.
Server Conference Number	Set the conference room number when conference type is set to be Server.
Transfer Timeout	Set the timeout of call transfer process.
Enable Long Contact	Allow more parameters in contact field per RFC 3840.
Enable Missed Call Log	If it is enabled, the phone would save missed calls into the call history

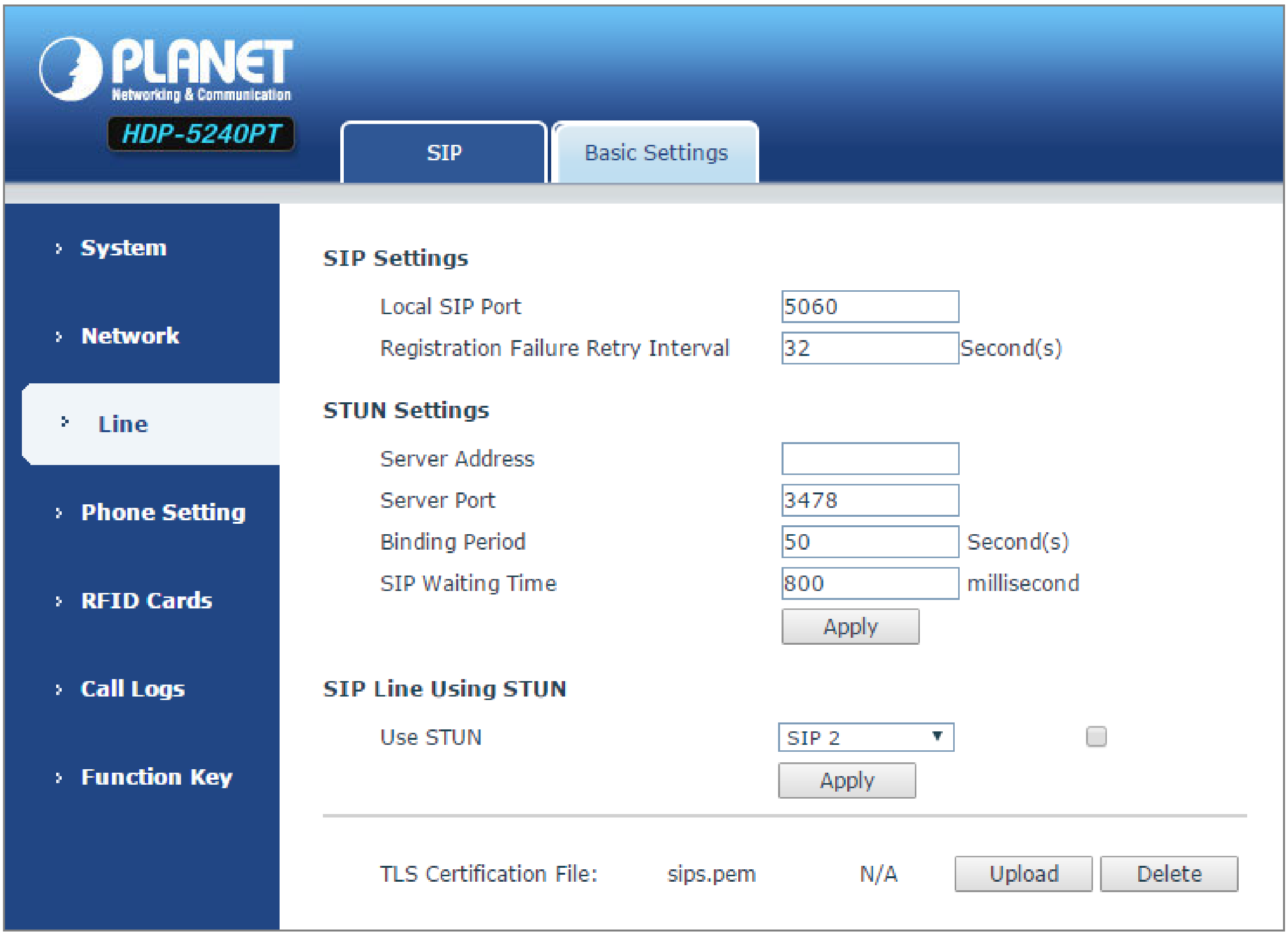
SIP	
Field Name	**Explanation**
	record.
Response Single Codec	If it is enabled, the device would use single codec in response to an incoming call request.
Use Feature Code	When this setting is enabled, the features in this section would not be handled by the device itself but by the server instead. In order to control the authorization of the features, the device would send feature code to the server by dialing the number specified in each feature code field.
Specific Server Type	Set the line to collaborate with specific server type.
Registration Expiration	Set the SIP expiration period.
Use VPN	Set the line to use VPN restrict route.
Use STUN	Set the line to use STUN for NAT traversal.
Convert URI	Convert not digit and alphabet characters to %hh hex code.
DTMF Type	Set the DTMF type to be used for the line.
DTMF SIP INFO Mode	Set the SIP INFO mode to send '*' and '#' or '10' and '11'.
Transportation Protocol	Set the line to use TCP or UDP for SIP transmission.
SIP Version	Set the SIP version.
Caller ID Header	Set the Caller ID Header.
Enable Strict Proxy	Enables the use of strict routing. When the phone receives packets from the server, it would use the source IP address, not the address in via field.
Enable user=phone	Sets user=phone in SIP messages.
Enable SCA	Enable/Disable SCA (Shared Call Appearance)
Enable BLF List	Enable/Disable BLF List
Enable DNS SRV	Set the line to use DNS SRV which would resolve the FQDN in proxy server into a service list.
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole opened.
Keep Alive Interval	Set the keep alive packet transmitting interval.
Enable Session Timer	Set the line to enable call ending by session timer refreshment. The call session would be ended if there is not new session timer event updating received after the timeout period.
Session Timeout	Set the session timer timeout period.
Enable Rport	Set the line to add Rport in SIP headers.
Enable PRACK	Set the line to support PRACK SIP message.
Keep Authentication	Keep the authentication parameters of previous authentication.
Auto TCP	Using TCP protocol to guarantee usability of transport when SIP messages

SIP	
Field Name	**Explanation**
	have more than 1500 bytes.
Enable Feature Sync	Feature Sync with server.
Enable GRUU	Support Globally Routable User-Agent URI (GRUU).
BLF Server	The registered server would 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 would be separated.
BLF List Number	BLF List allows one BLF key to monitor the status of a group. Multiple BLF lists are supported.
SIP Encryption	Enable SIP encryption such that SIP transmission would be encrypted.
SIP Encryption Key	Set the pass phrase for SIP encryption.
RTP Encryption	Enable RTP encryption such that RTP transmission would be encrypted.
RTP Encryption Key	Set the pass phrase for RTP encryption.

B. Basic Settings

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



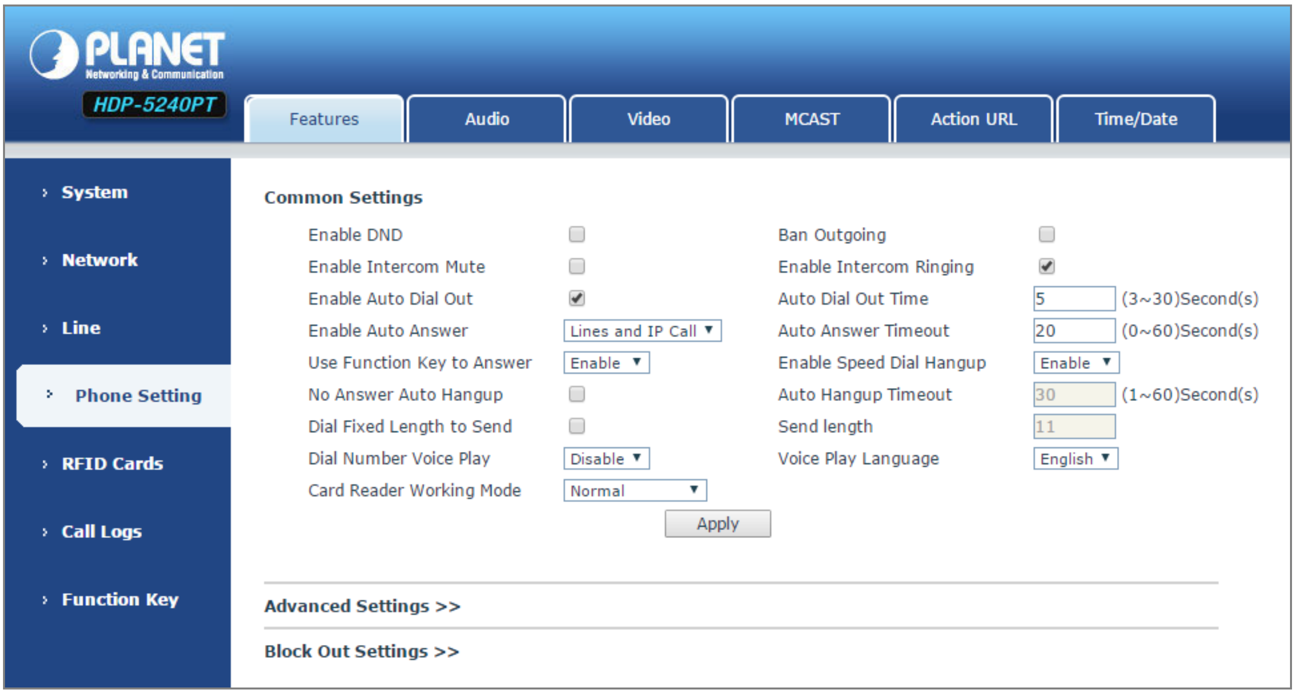


Basic Settings	
Field Name	**Explanation**
SIP Settings	
Local SIP Port	Set the local SIP port used to send/receive SIP messages.
Registration Failure Retry Interval	Set the retry interval of SIP registration when registration failed.
STUN Settings	
Server Address	STUN Server IP address
Server Port	STUN Server Port – Default is 3478.
Binding Period	STUN blinding period – STUN packets are sent once every this period to keep the NAT mapping active.
SIP Waiting Time	Waiting time for SIP. This would vary depending on the network.
SIP Line Using STUN (SIP1 or SIP2)	
Use STUN	Enable/Disable STUN on the selected line.
TLS Certification File	
Upload or delete the TLS certification file used for encrypting SIP transmission.	

Note	The SIP STUN is used to achieve the penetration of SIP NAT; it is a realization of service. When the equipment configures the STUN server IP and port (usually the default is 3478), and selects "Use Stun SIP server", you can make common SIP equipment achieve penetration.

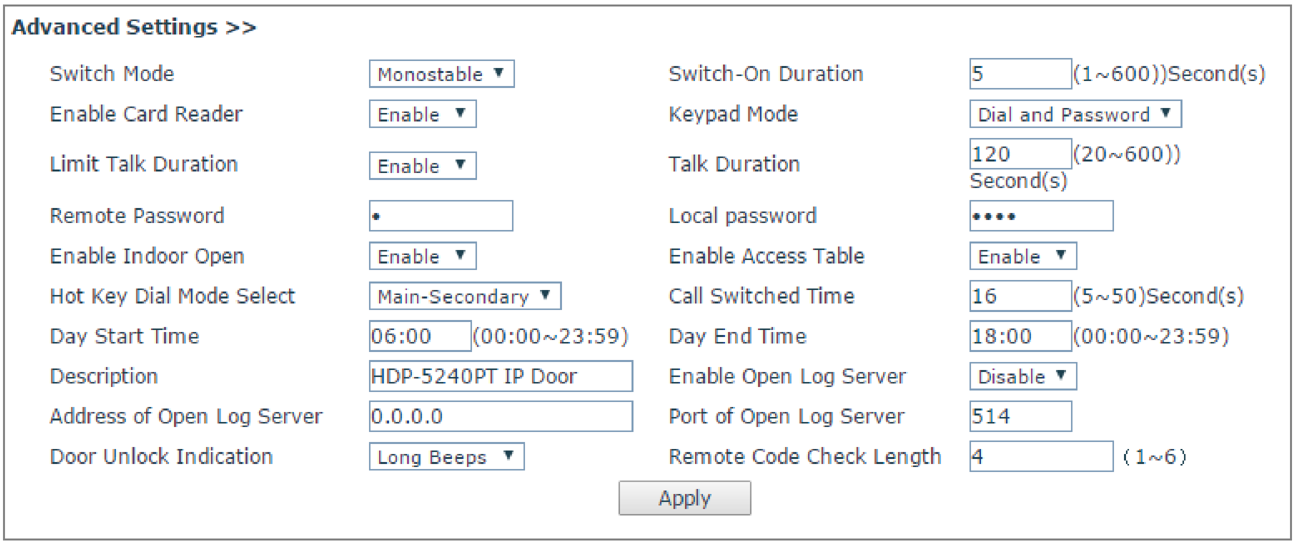
5.3.4 RFID Setting

A. Features



Features	
Field Name	**Explanation**
Common Settings	
Enable DND	DND feature can refuse all incoming calls for all SIP lines, or for individual SIP line. But the outgoing calls would not be affected.
Ban Outgoing	If it is enabled, no outgoing calls can be made.
Enable Intercom Mute	If it is enabled, device would mute incoming calls during an intercom call.
Enable Intercom Ringing	If it is enabled, device would play intercom ring tone to alert that there is a new incoming call during an intercom call.
Enable Auto Dial Out	Enable Auto Dial Out.
Auto Dial Out Time	Set Auto Dial Out Time.
Enable Auto Answer	Enable Auto Answer function.
Auto Answer Timeout	Set Auto Answer Timeout.
No Answer Auto Hangup	Enable automatically hang up feature when there is no answer.
Auto Hangup Timeout	Configuration in a set time -- The device would automatically hang up when there is no answer.

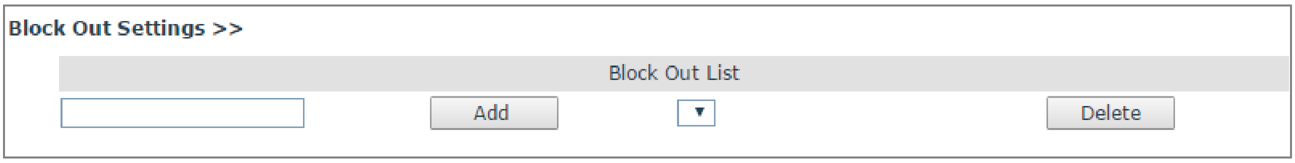
Features	
Field Name	**Explanation**
Dial Fixed Length to Send	Enable or disable dial fixed length.
Send Length	The number would be sent to the server after the specified digits are dialed.
Enable Speed Dial Hangup	Enable Speed Dial Hand Up function.
Use Function Key to Answer	Configure whether to enable the function keys; the feature is disabled by default.
Dial Number Voice Play	Configuration Open / Close Dial Number Voice Play
Voice Play Language	Set language of the voice prompt.
Card Reader Working Mode	Set ID card status: Normal: This mode helps you to open the door by swiping the card reader. Card Issuing: This mode comes with an ID added to the card reader. Card Revoking: This mode has an ID deleted from the card reader.



Features	
Field Name	**Explanation**
Advanced Settings	
Switch 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 changing, the status would be kept. Initial mode is Monostable
Keypad Mode	Password+dialing: password inputting mode is default. Dialing mode is shown below if you want.

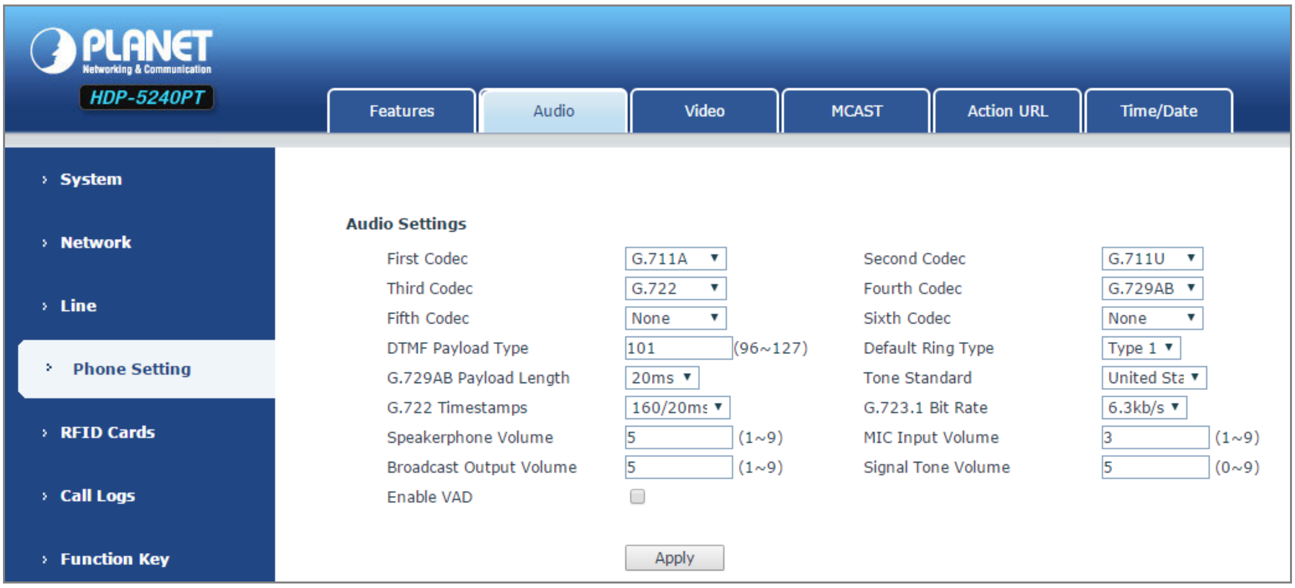
Features	
Field Name	**Explanation**
	Only password: password input only, dialing would be forbidden. Only dialing: dial input only, you can press * key to enter the dial, the # key for hanging up. Initial mode is password and dialing.
Switch-On Duration	Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial time is 5 seconds.
Talk Duration	The call would be ended automatically when time is up. Initial time is 120 seconds.
Remote Password	Remote unlocking door password. Initial password is “*”.
Local Password	Local unlocking door password via keypad; the default password length is 4. Initial password is “6789”.
Description	Device description displayed on IP scanning tool software. Initial description is “HDP-5240PT IP Door Phone”.
Enable Access Table	Enable Access Table: enter <Access Code> for opening door during calls. Disable Access Table: enter <Remote Password> for opening door during calls. The device enables the feature by default.
Hot Key Dial Mode Select	<Primary/Secondary>mode allows system to call primary extension first; if there is no answer, system would cancel the call and then call secondary extension automatically. <Day/Night>mode allows system to check whether the calling time belongs to day time or night time, and then system decides to call the number 1 or number 2 automatically. Users just press speed dial key once.
Call Switched Time	The period between hot key dialing to the first and second number. Initial time is 16 seconds.
Day Start Time	The start time of the day when you select<Day/Night>mode.
Day End Time	The end time of the day when you select <Day/Night>mode.
Address of Open Log Server	Log server address (IP or domain name)
Port of Open Log Server	Log server port (0-65535); initial port is 514.
Enable Open Log Server	Enable or disable connection with log server
Enable Indoor Open	Enable or disable using indoor switch to unlock the door.
Enable Card Reader	Enable or disable card reader for RFID cards.
Limit Talk Duration	If enabled, calls would be forced to end after talking time is up.

Features	
Field Name	**Explanation**
Door Unlock Indication	Indication tone for door unlocked. There are 3 types of tone: silent, short beeps and long beeps.
Remote Code Check Length	The remote access code length would be restricted with it. If the input access code length is matched with it, system would check it immediately. Initial length is 4.
Block Out Settings	
Add or delete blocked numbers – enter the prefix of numbers which should not be dialed by the phone. For example, if 001 is entered, the phone would not dial any number beginning with 001. X and x are wildcards which match single digit. For example, if 4xxx or 4XXX is entered, the phone would not dial any 4 digits beginning with 4. It would dial numbers beginning with 4 which are longer or shorter than 4 digits.	



B. Audio

This page configures audio parameters such as voice codec, speakerphone volume, mic volume and ringer volume.

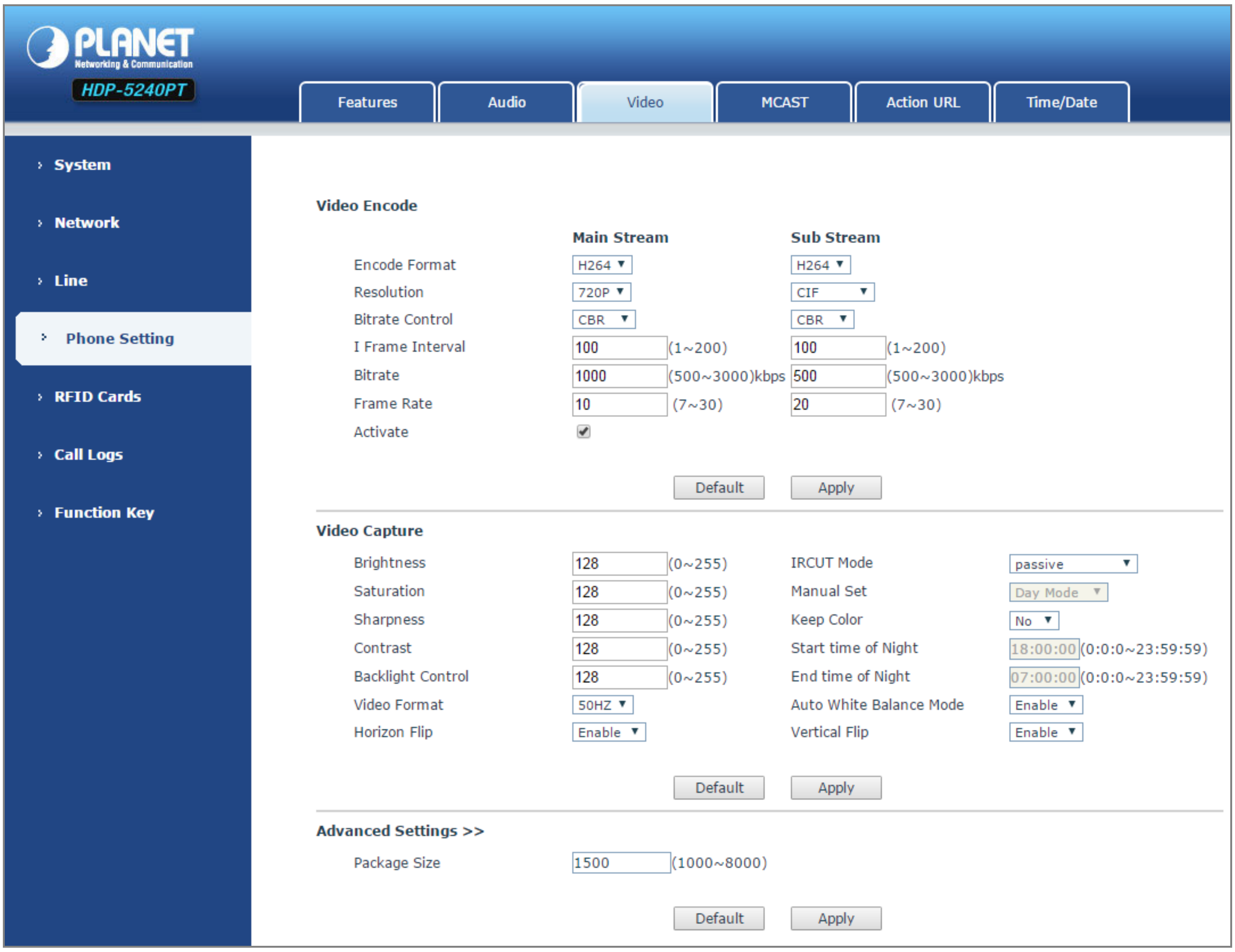


Audio Setting	
Field Name	**Explanation**
First Codec	The first codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB
Second Codec	The second codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, None

Audio Setting	
Field Name	**Explanation**
Third Codec	The third codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, None
Fourth Codec	The fourth codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, None
DTMF Payload Type	The RTP Payload type that indicates DTMF. Default is 101
Default Ring Type	Ring sound – there are 9 standard types and 3 user types.
G.729AB Payload Length	G.729AB Payload length – adjust from 10 – 60 msec.
Tone Standard	Configure tone standard area.
G.722 Timestamps	Choices are 160/20ms or 320/20ms.
G.723.1 Bit Rate	Choices are 5.3kb/s or 6.3kb/s.
Speakerphone Volume	Set the speaker call volume level.
MIC Input Volume	Set the MIC call volume level.
Broadcast Output Volume	Set the broadcast output volume level.
Signal Tone Volume	Set the audio signal output volume level.
Enable VAD	Enable or disable Voice Activity Detection (VAD). If VAD is enabled, G729 Payload length cannot be set greater than 20 msec.

C. Video

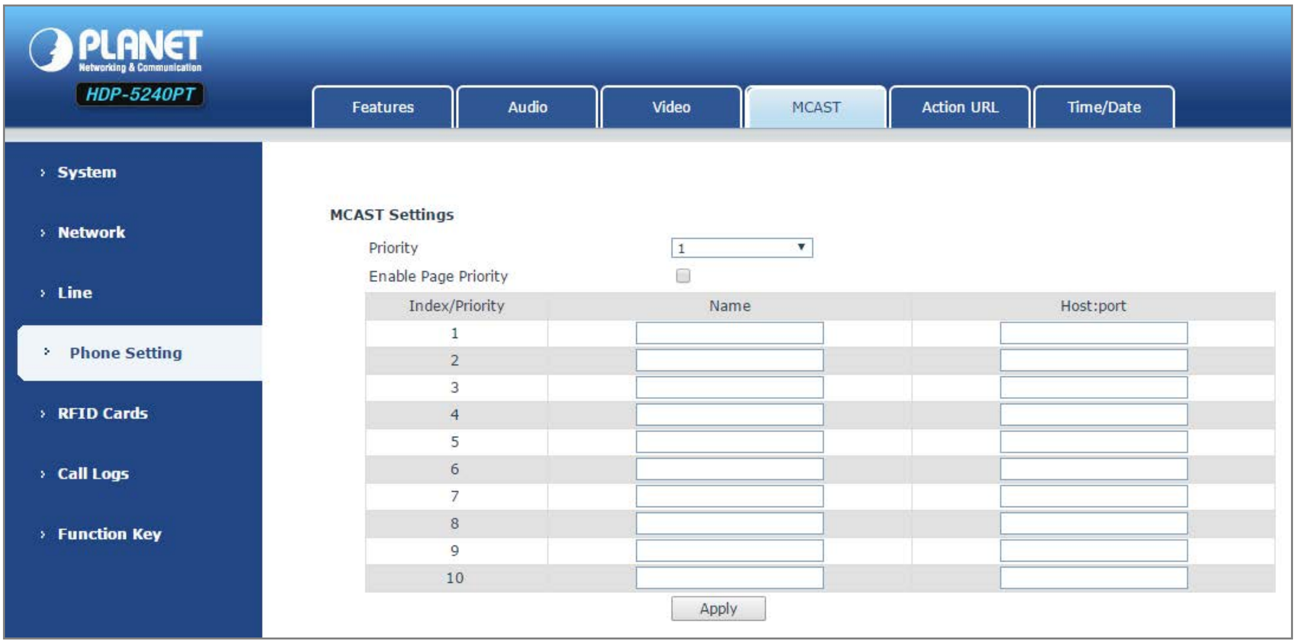
This page allows you to set the video encoding and video capture, and other information.



Video Encode	
Field Name	**Explanation**
Encode	Only H.264 encoding format is supported
Resolution	Main stream: support 720p Sub-stream: you can select 360P, CIF (352 x 288), QVGA (240 x 320)
Bitrate Control	CBR: If the code rate (bandwidth) is insufficient, it is preferred. VBR: Image quality is preferred, not recommended. CVBR: greater than the minimum bit rate (bandwidth), smaller than the maximum bit rate (bandwidth), the setting is complex; the type is not recommended.
I Frame Interval	The greater the value is, the worse the video quality would be; if not, the better video quality. Not recommended to adjust.
Bitrate	It is proportional to video file size; not recommended to adjust.
Frame Rate	The larger the value is, the more coherent the video would be; not recommended to adjust.

Video Encode	
Field Name	**Explanation**
Activate	When you select it, the main stream is enabled; otherwise, disabled
Video Capture	
Brightness	Adjust the video brightness level
Saturation	Adjust the video color purity; the higher the value is, the more vivid colors might be displayed
Sharpness	Adjust video clarity
Contrast	Adjust the video brightness ratio
Backlight Control	Video background brightness
Video Format	Based on the power frequency used, common frequency is 50Hz
Horizon Flip	The video is flipped horizontally
IR-cut Mode	IR-cut operating mode selection: **Day & Night Mode**: The camera automatically switches to black and white in "Night Start Time" and "Night End Time" (In black and white mode, you can see things in a dark environment.). **Manual mode:** The user needs to manually select the camera day / night mode; night mode is black and white.
Manual Set	You need to manually select the camera day / night mode; night mode is black and white.
Keep Color	Select whether or not the camera is to be remained in color.
Start time of Night	In IR-cut day and night mode, the camera switches to black and white start time.
End time of Night	In IR-cut day and night mode, the camera switches to black and white end time.
Auto White Balance Mode	The camera automatically adjusts the video image based on ambient light.
Vertical Flip	The video is flipped horizontally.

D. 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, the device monitors and plays the RTP stream which is sent by the multicast address.

(A) MCAST Settings

Equipment can be set up to monitor up to 10 different multicast addresses and used to receive the multicast RTP stream sent by the multicast address. Here are the ways to change equipment receiving multicast RTP stream processing mode in the web interface: set the ordinary priority and enable page priority.

a. Priority:

From the drop-down box, choose priority of ordinary calls. If the priority of the incoming streams of multicast RTP has lower precedence than the current common calls, device would automatically ignore the group RTP streams. If the priority of the incoming stream of multicast RTP is higher than the current common calls priority, device would automatically receive the group RTP streams, and keep the current common calls in maintained status. You can also choose to disable the function from the receiving threshold drop-down box. The device would automatically ignore all local network multicast RTP streams.

b. The options are as follows:

(a) 1-10: To definite the priority of the common calls, 1 is the top level while 10 is the lowest

(b) Disable: Ignore all incoming multicast RTP streams

(c) Enable the page priority:

Page priority determines the device how to deal with the new receiving multicast RTP streams when it is in multicast session currently. When page priority switch is enabled, the device would automatically ignore the low priority multicast RTP streams but receive top-level priority multicast RTP streams, and keep the current multicast session in the current status. If it is not enabled, the device would automatically ignore all receiving multicast RTP streams.

c. Web Settings:

MCAST Settings

Priority: 1

Enable Page Priority: ☑

Index/Priority	Name	Host:port
1	Group A	239.1.1.1:1366
2	Group B	239.1.1.1:1367

The multicast SS priority is higher than that of Group B; Group A has the highest priority.

Note	When you press the multicast key for multicast session, both multicast sender and receiver would beep.

(B) Listener configuration

MCAST Settings

Priority: 3

Enable Page Priority: ☑

Index/Priority	Name	Host:port
1	group 1	224.0.0.2:2366
2	group 2	224.0.0.2:1366
3	group 3	224.0.0.6:3366
4		
5		
6		
7		
8		
9		
10		

a. Blue part (name)

"Group 1", "Group 2" and "Group 3" are your setting monitoring multicast names.The group name would be displayed on the screen when you answer the multicast. If you have not set, the screen would display the IP: port directly.

b. Purple part (host: port)

It is a set of addresses and ports to listen, separated by a colon.

c. Pink part (index / priority)

Multicast is a sign of listening, but also the monitoring multicast priority. The smaller number refers to higher priority.

d. Red part (priority)

It is the general call, non-multicast call priority. The smaller number refers to higher priority. The following would explain how to use this option:

(a) The purpose of setting monitoring multicast "Group 1" or "Group 2" or "Group 3" is to launch a multicast call.

(b) All equipment has one or more common non multicast communication.

(c) When you set the priority as disabled, any level of multicast would not be answered , multicast call is rejected.

(d) When you set the priority as some value, only the multicast higher than the priority can come in. If you set the priority as 3, group 2 and group 3 would be rejected, for its priority level is equal to 3 and less than 3; multicast 1 priority is set up with 2, higher than ordinary call priority, device can answer the multicast message, at the same time, holding the other call.

e. Green part (Enable Page priority)

Set whether to open multicast comparison function, multicast priority is pink part number. The following explains how to use:

(a) The purpose of setting monitoring multicast "group 1" or “group 3”is listening "group of 1" or “group 3”multicast call of multicast address.

(b) The device has a path or multi-path multicast calls, such as listening to "multicast information group 2".

(c) If multicast is a new "group 1", and because the priority of group 1" is 2, higher than the current call priority 3 of “group 2”, so multicast call would come in.

(d) If multicast is a new "group 3", and because the priority of group 3" is 4, lower than the current call priority 3 of “group 2”, the device would listen to the “group 1” and maintain the "group 2".

(C) Multicast service

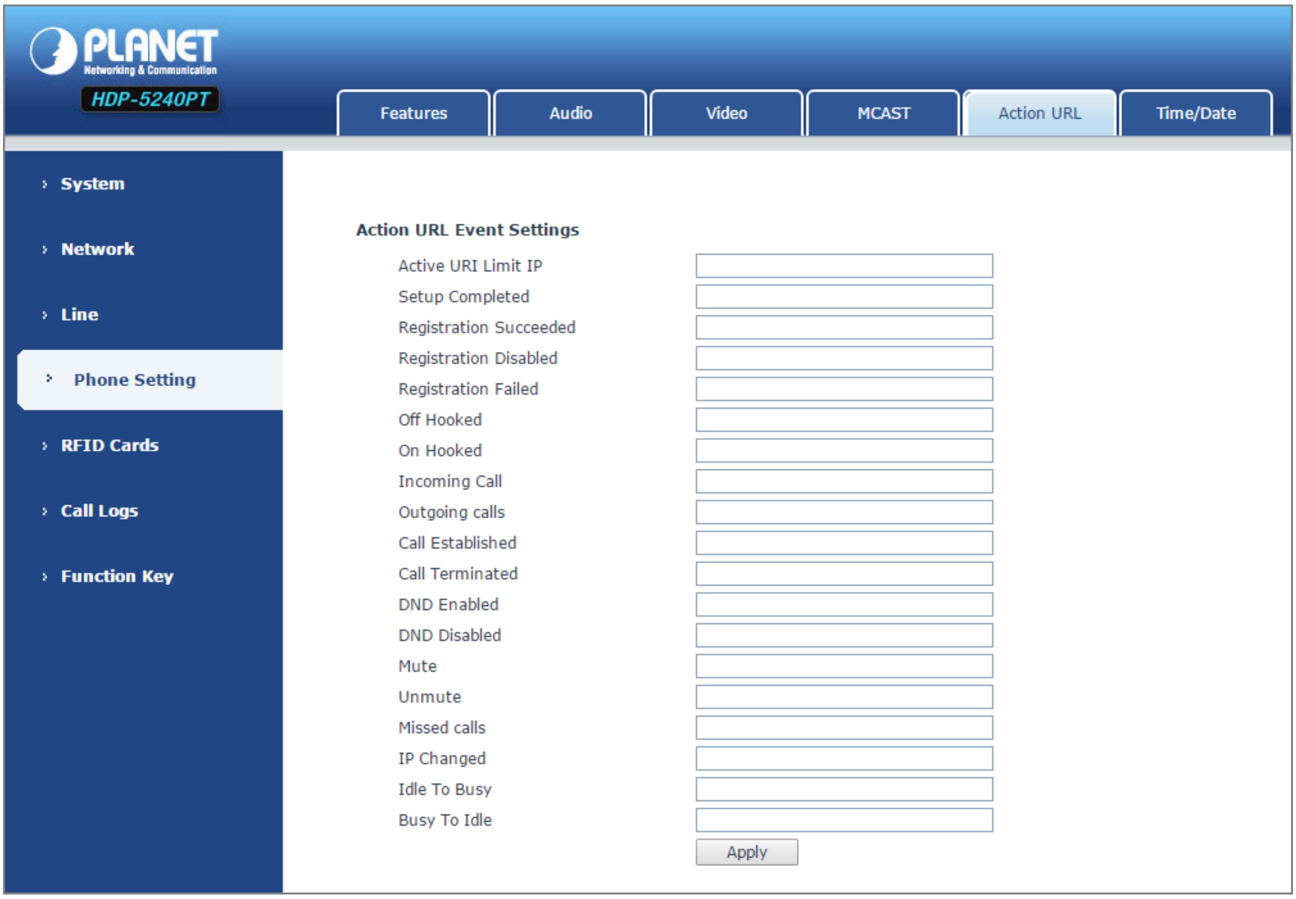
a. Send:

When you configure the item, pressing the corresponding key on the equipment shell, equipment would directly enter the Talking interface; the premise is to ensure no current multicast call and three-way conference, so the multicast can be established.

b. Monitor:

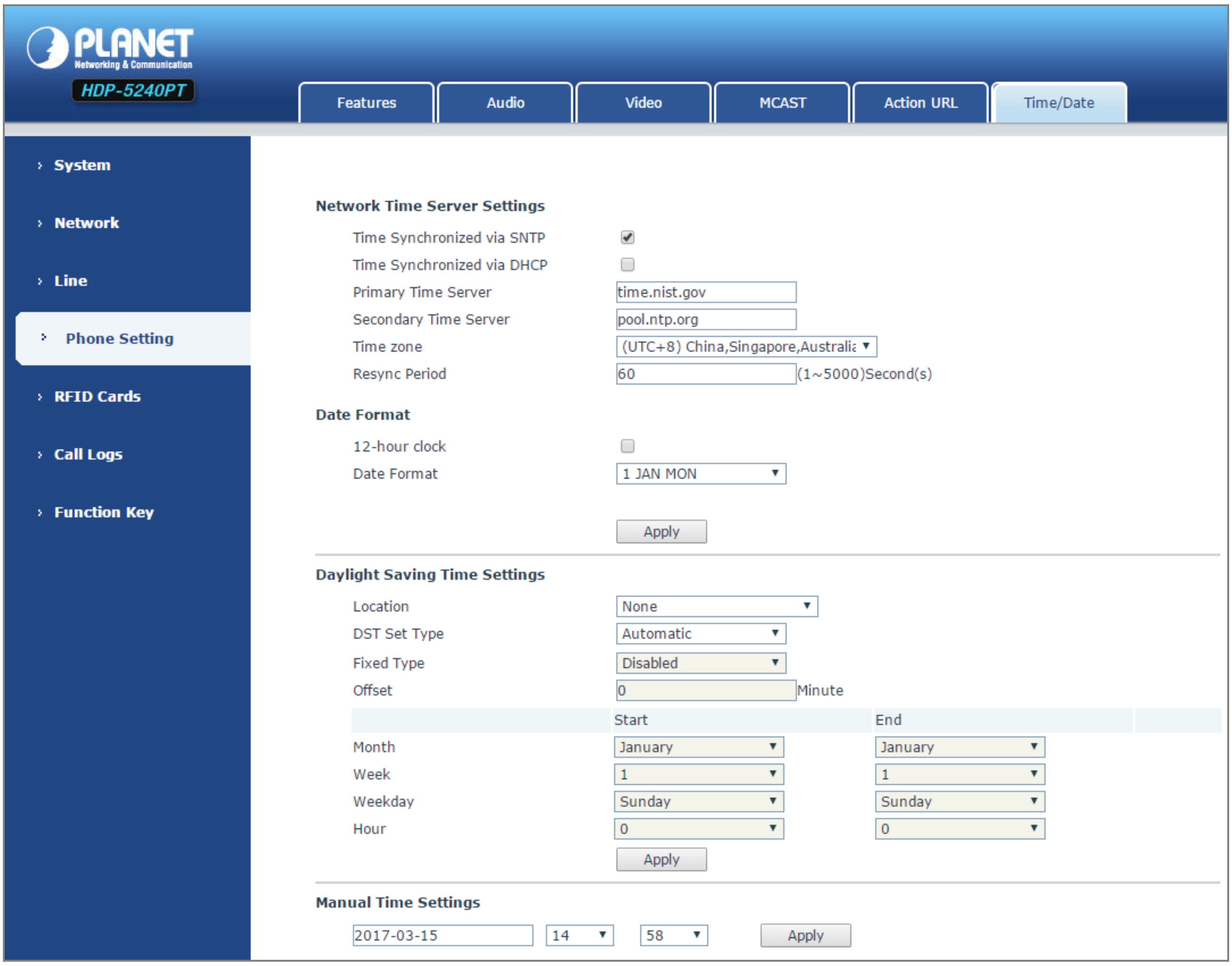
IP port and priority are configured to monitor the device; when the call is initiated by multicast and the call is successful, the device would directly enter the Talking interface.

E. Action URL



Action URL	
Field Name	**Explanation**
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.	

F. Time/Date

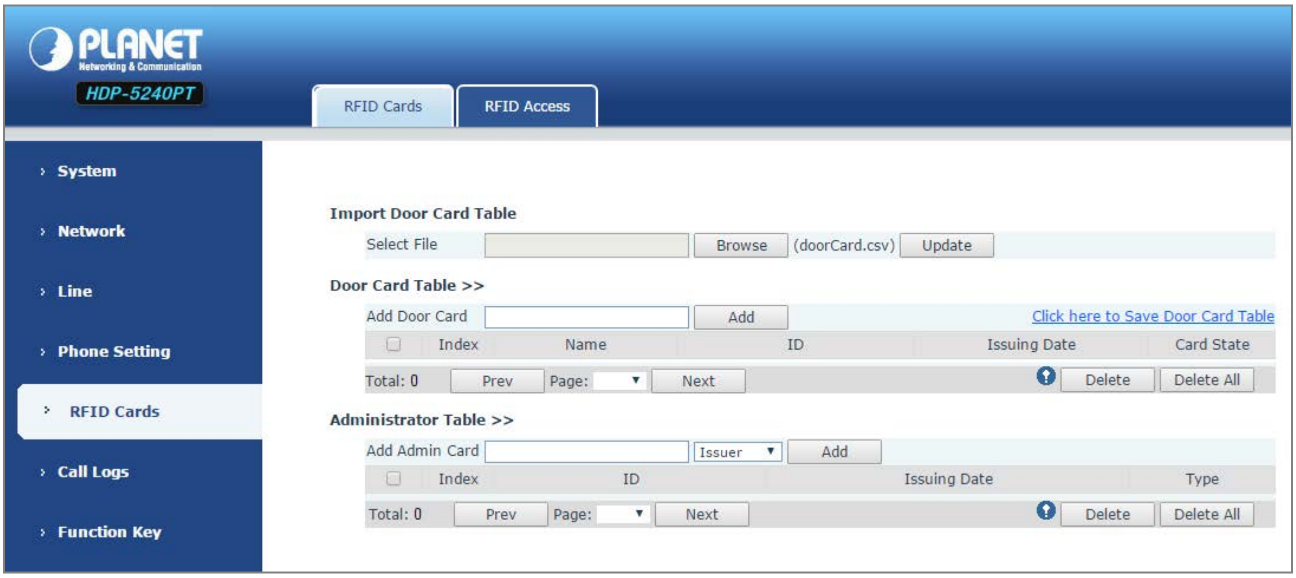


Time/Date	
Field Name	**Explanation**
Network Time Server Settings	
Time Synchronized via SNTP	Enable time-sync through SNTP protocol.
Time Synchronized via DHCP	Enable time-sync through DHCP protocol.
Primary Time Server	Set primary time server address
Secondary Time Server	Set secondary time server address. When primary server is not reachable, the device would 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

Time/Date	
Field Name	**Explanation**
Date Format	
12-hour Clock	Set the time display in 12-hour mode.
Date Format	Select the time/date display format.
Daylight Saving Time Settings	
Location	Select the user's time zone according to specific area.
DST Set Type	Select automatic DST according to the preset rules of DST, or you can 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	
The time might be set manually. It needs user to disable SNTP service first.	

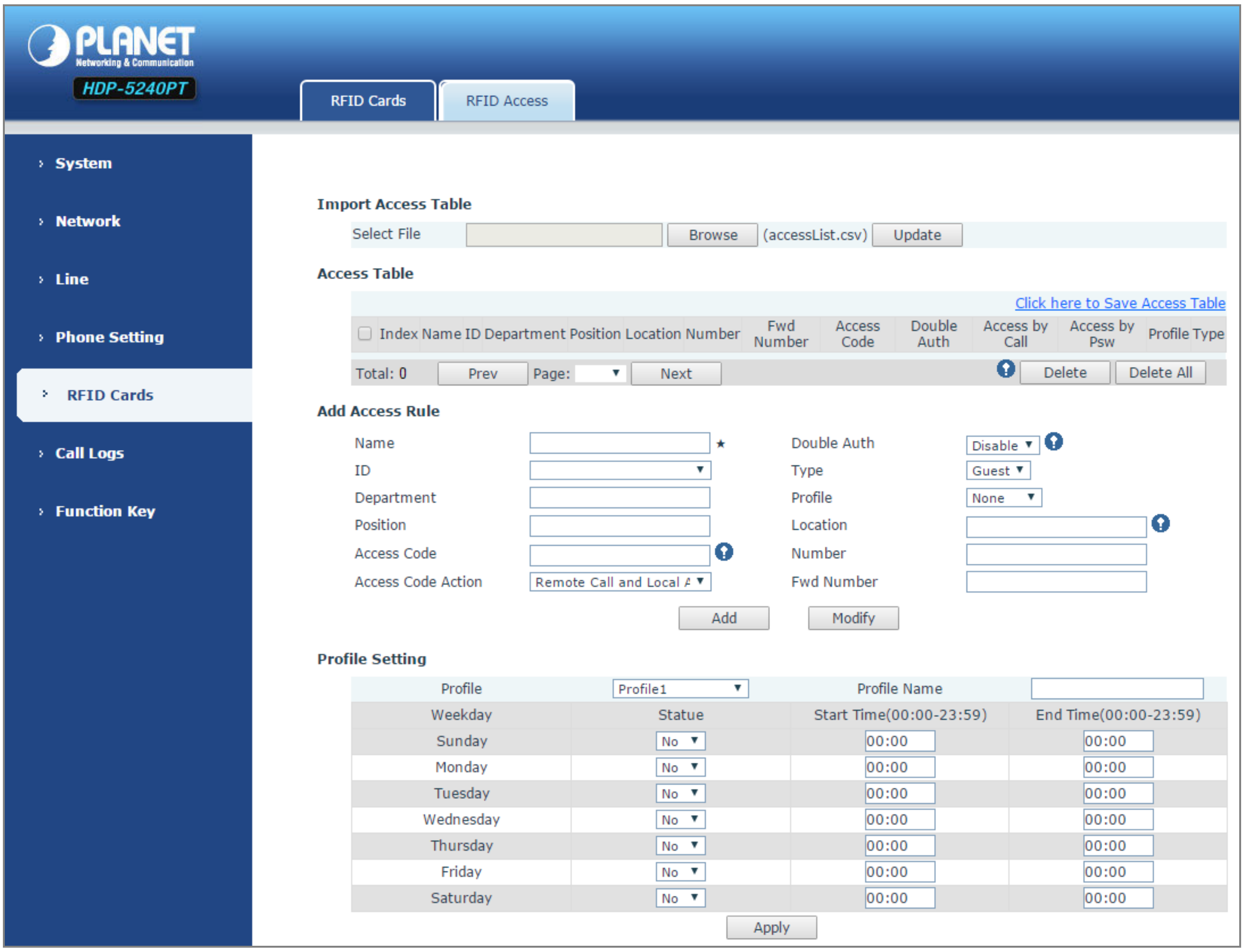
5.3.5 RFID Cards

A. RFID Cards



RFID Cards	
Field Name	**Explanation**
Import Door Card Table	
Click <Browse> to choose importing door card list file (doorCard.csv); click <Update> to batch import.	
Door Card Table	
Add Door Card	You should input the top 10 digits of RFID card numbers, for example, 0004111806, by clicking <add>.
Click Here to Save Door Card Table	Click here to Save Door Card Table Right-click it and select saving target to your computer.
Name	The name of users who own issued cards.
ID	The card number of issued cards. Note: The card not registered to the remote access list is unable to open the door.
Issuing Date	The issuing date of issued cards.
Card State	The state of issued cards.
Delete	Click <Delete> to delete the door card list of the selected ID cards.
Delete All	Click <Delete All> to delete all door card lists.
Administrator Table	
Add Admin Card	You should input the top 10 digits of RFID card numbers, for example, 0004111806, to select the type of admin card by clicking <add>.
Type: issuing and revoking When entrance guard is in normal state, swiping card (issuing card) would make entrance guard into the issuing state. When swiping a new card that can be added to the database and when you swipe the issuing card again after cards are added, entrance guard would return to normal state. Deleting card operation is the same as the issuing card. The device can support up to 10 admin cards and 500 copies of ordinary cards. Note: In the issuing state, swiping deleted card is invalid.	
Shows the ID, Date and Type of admin card	
Delete	Clicking <Delete> would delete the admin card list of the selected ID cards.
All Delete	Clicking <Delete All> to delete all admin card lists.

B. RFID Access

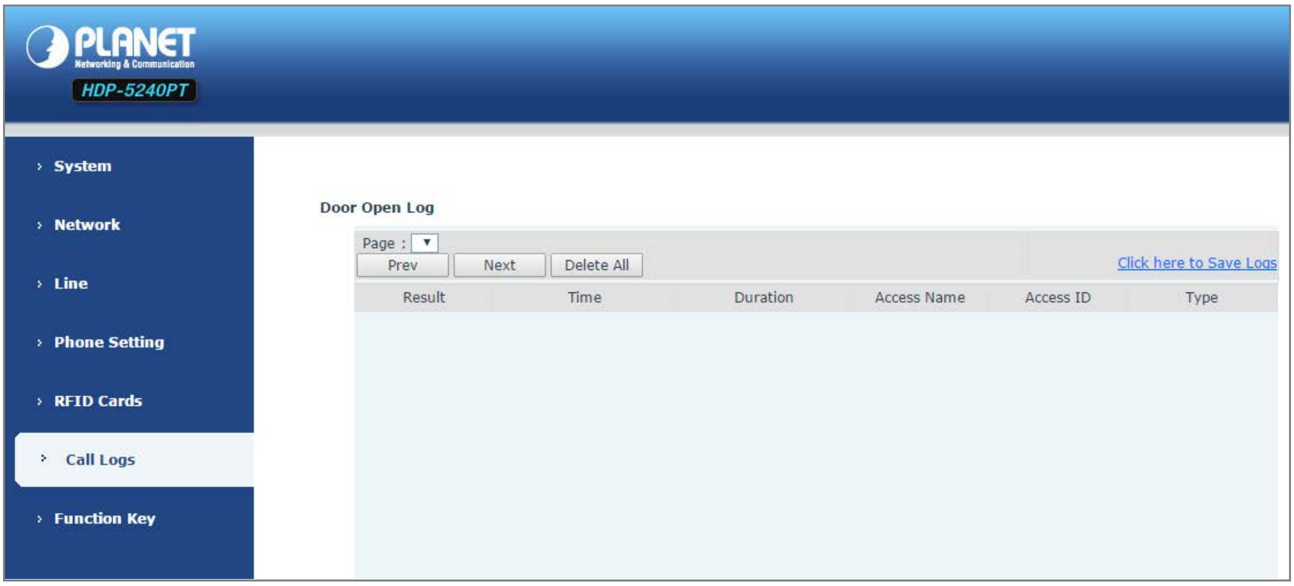


Field Name	Explanation
Import Access Table	
Click the <Browse> to choose to import remote access list file (access List.csv) and then clicking <Update> can batch import remote access rule.	
Access Table	
According to entrance guard access rules that have been added, you can choose single or multiple rules on this list to delete operation.	
Add Access Rule	
Name	User name
ID	RFID card number
Department	Card holder's department
Position	Card holder's position
Access Code	1. When the door phone answers the call from the corresponding <Phone Num> user, the <Phone Num> user can input the access code via keypad to unlock the door remotely.

Field Name	Explanation
	2. The user's private password should be input via keypad for local door unlocking.
Access Code Action	Select Access Code Action mode
Double Auth	When the feature is enabled, private password inputting and RFID reading must be matched simultaneously for door unlocking.
Type	Host: The door phone would answer all calls automatically. Guest: The door phone would ring for incoming call, if the auto answer is disabled.
Profile	It is valid for user access rules (including RFID, access code, etc) within corresponding time section. If NONE is selected, the feature would be taken effect all day.
Location	Virtual extension number is used to make position call, instead of real number. It might be taken with unit number, or room number.
Number	User phone number
Fwd Number	Call forwarding number when the above phone number is unavailable.
Profile Setting	
Profile	There are 4 sections for time profile configuration.
Profile Name	The name of profile to help administrator to remember the time definition.
Status	If it is yes, the time profile would be taken effect. Other time sections not included in the profiles would not allow users to open door.
Start Time	The start time of section
End Time	The end time of section

5.3.6 Call Logs

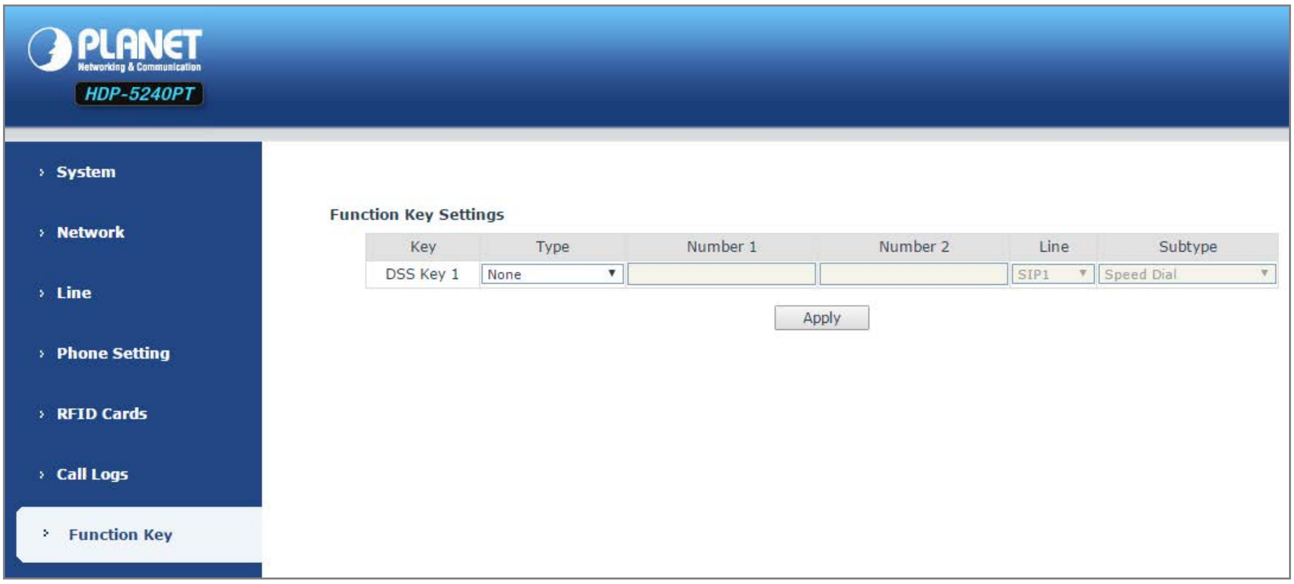
According to open event log, the device can record up to 150 thousands of open events; it would cover the old records after the records exceed 150 thousands. Click here to Save Logs Right-click on the links to select saving target as the door log can export CSV format.



Field Name	Explanation
Door Open Log	
Result	Show the result of the door opening (Succeeded or Failed)
Time	The time of opening door.
Duration	Duration of opening the door.
Access Name	If the door was opened by swiping card or remotely unlocking door, the device would display remote access name.
Access ID	1. If the opening door method is swiping card, it wound display the card number 2. If the opening door way is done via remote access, it wound display the remote extension number. 3. If the opening door way is done via local access, there is no display information.
Type	Open type: 1. Local, 2. Remote, 3. Brush card (Temporary Card, Valid Card and Illegal Card). Note: There are three kinds of brushing card feedback results. Temporary Card (only added) the card number, without adding other rules) Valid Card (added access rules) Illegal Card (Did not add information)

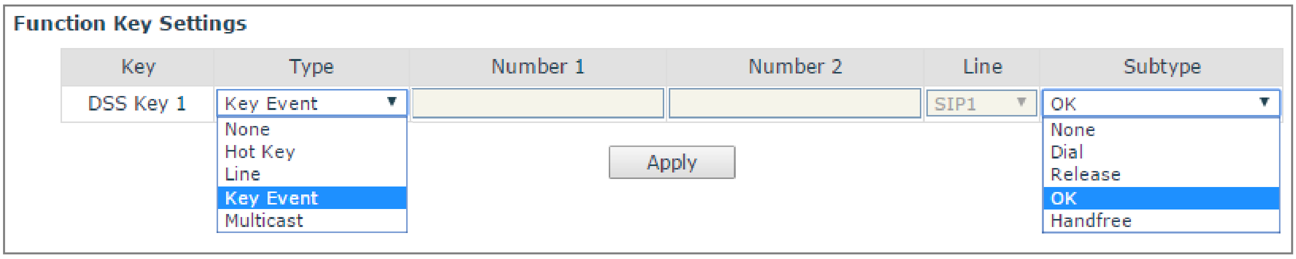
5.3.7 Function Key

A. Function Key Settings



(A) Key Event

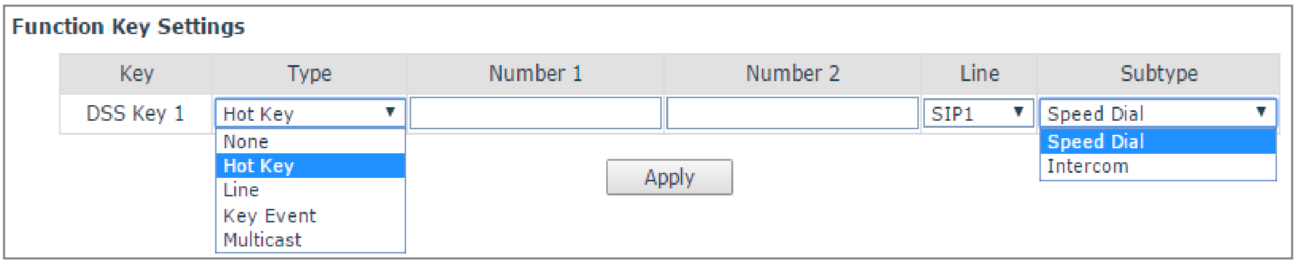
You might set up the key type with the Key Event.



Type	Subtype	Usage
Key Event	None	Not responding
	Dial	Dialing function
	Release	Delete password input, cancel dialing input and end call
	OK	identification key
	Handsfree	The hands-free key(with hooking dial, hanging up functions)

(B) Hot Key

You might enter the phone number in the input box. When you press the shortcut key, equipment would dial preset telephone number. This button can also be used to set the IP address: you can press the shortcut key to directly make an IP call.

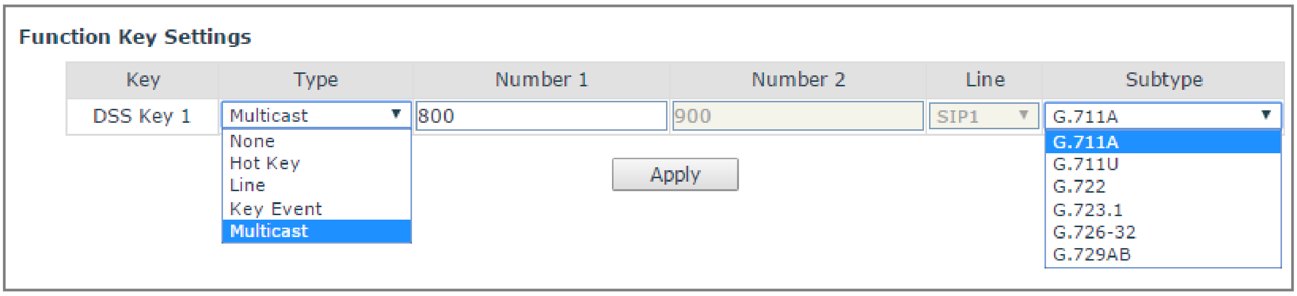


Type	Number	Line	Subtype	Usage
Hot Key	Fill out the called party's SIP account or IP address	The SIP account corresponding lines	Speed Dial	Using Speed Dial mode together with Enable Speed Dial Hangup Enable, can define whether this call is allowed to be hung up by re-pressing the speed dial key.
		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

(C) Multicast

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

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



Type	Number	Subtype	Usage
Multicast	Set the host IP address and port number; they must be separated by a colon	G.711A	Narrowband speech coding (4Khz)
		G.711U	
		G.722	Wideband speech coding (7Khz)
		G.723.1	Narrowband speech coding (4Khz)
		G.726-32	
		G.729AB	

a. Operation mechanism

You can define the DSS Key configuration with multicast address, port and used codec. The device can configure via Web to monitor the multicast address and port. When the device makes a multicast, all devices monitoring the address can receive the multicast data.

b. Calling configuration

If the device is on calls, or it is a three-way conferencing, or initiated multicast communication, the device would not be able to launch a new multicast call.

Chapter 6. Other instructions

6.1 Open door modes

A. Local control

(A) Local Password

a. Set **<Local Password>** (the password is "**6789**" by default) via **Phone Setting\Feature\Advanced Settings**.

b. Input password via keypad and press the "#" key, then the door would be unlocked.

(B) Private access code

a. Set <Add Access Rule\Access Code> and enable local authentication.

b. Input access code via keypad and press the "#" key, then the door would be unlocked.

B. Remote control

(A) Visitors call the owner

a. Visitors can call the owner via position speed dial or phone number. (After setting the speed dial key, visitors can press it to call directly)

b. The owner answers the call and presses the "*" key to unlock the door for visitors.

(B) Owner calls visitors

a. Owner calls visitors via SIP phone.

b. SIP door phone answers the call automatically.

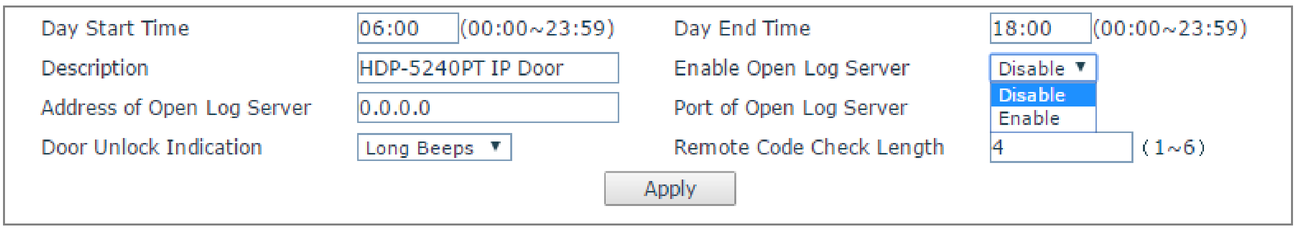
c. Owner inputs the corresponding access codes via SIP phone keypad to unlock the door.

C. Swiping cards

Use pre-assigned RFID cards to unlock the door by touching RFID area of the device.

D. Indoor switch

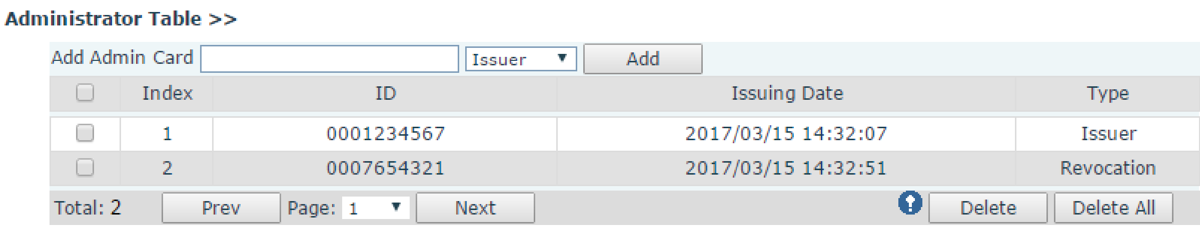
Press indoor switch, which is installed and connected with the device, to unlock the door.



6.2 Management of Card

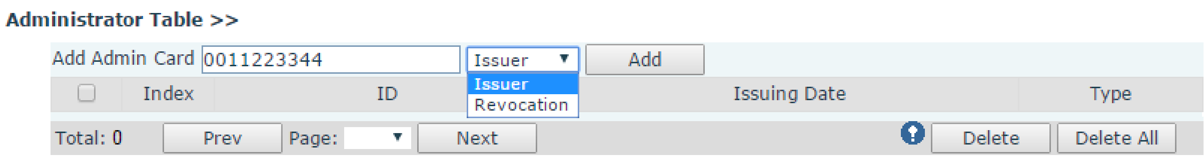
6.2.1 Administrator Table

A. <Issuer> and <Revocation>



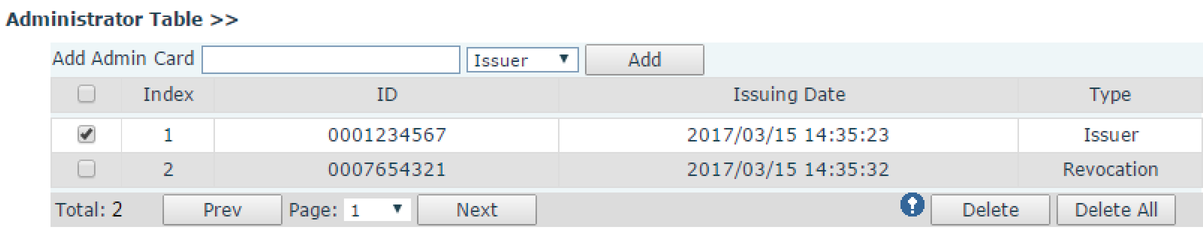
(A) Add Administrator cards

Input a card's ID, selected **<Issuer>** or **<Revocation>** in the field and then click **<Add>**; you would add administrator card.



(B) Delete Administrator cards

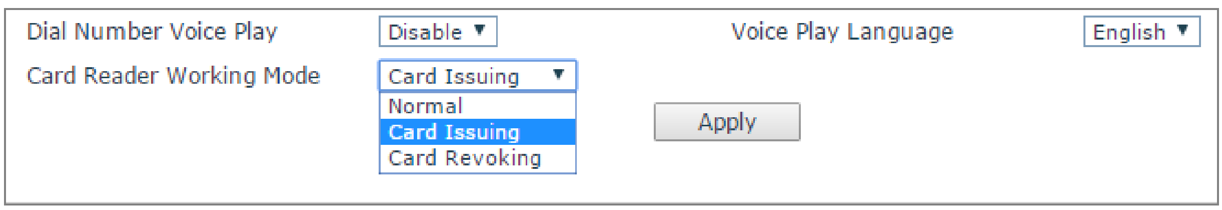
To delete the selected admin card, click **<Delete>**.



6.2.2 Add user cards

A. Method 1: It is used to add cards for starters typically

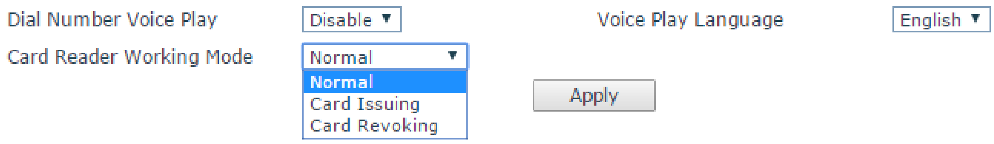
(A) On the web page **< Phone Setting →Features →Card Reader Working Mode >** option, select **<Card Issuing>**.



(B) Click **<Apply>** and Card Reader would enter the issuing status.

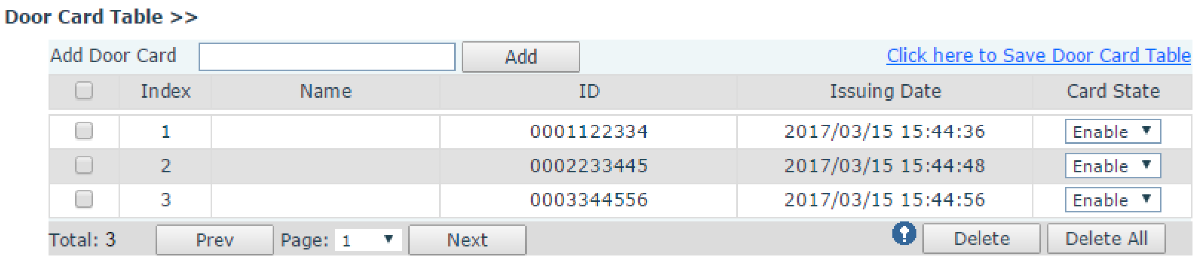
(C) Use new card to touch card reader induction area, and then you might hear the confirmed indication tone from the device. Repeat step to add more cards.

(D) On the web page **< Phone Setting →Features →Card Reader Working Mode >** option, select **<Normal>**.



(E) Click **<Apply>** and Card Reader would return to the Normal status.

(F) The issuing records can be found from the door card table list.



B. Methods 2: It is used to add cards for professionals

(A) Use issuer admin card to touch card reader induction area, and it would enter issuing card status.

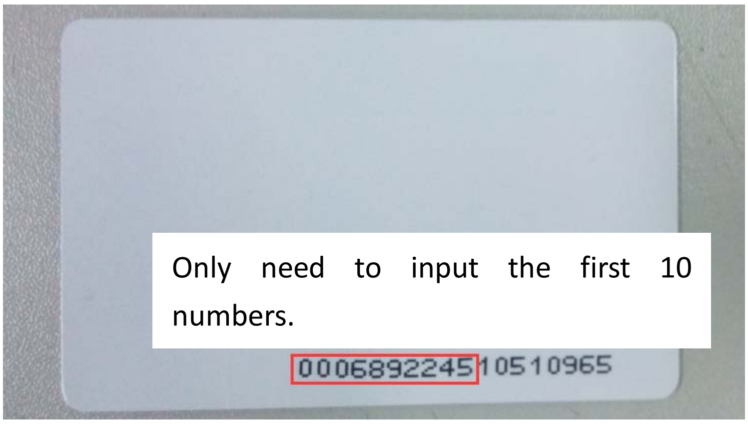
(B) Use new card to touch card reader induction area, and you might hear the confirmed indication tone from the device. Repeat step 2 to add more cards.

(C) Use issuer admin card to touch card reader induction area again and it would go back to normal working status.

C. Method 3: It is use to add few cards

(A) Input card number on the door card settings page, and then click **<Add>**.

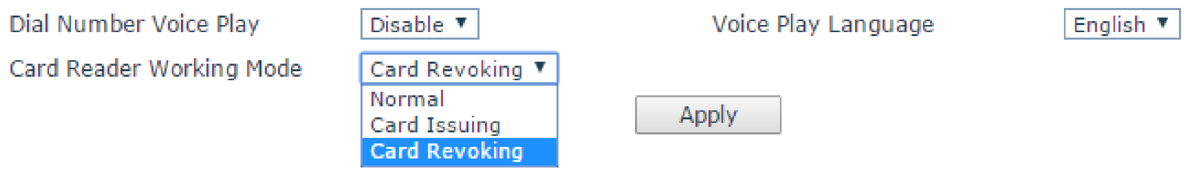
Note	You can also use the USB card reader connected with PC to get card ID automatically.



6.2.3 Delete user cards

A. Method 1: It is used to batch delete cards for starters.

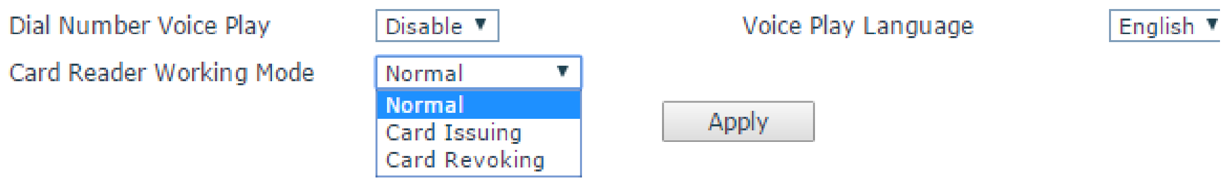
(A) On the web **page < Phone Setting →Features →Card Reader Working Mode >** option, select **<Card Revoking>**.



(B) Click **<Apply>** and card reader would enter the revoking status.

(C) Use card to touch card reader induction area, and you might hear the card reader confirmed indication tone. Repeat step to delete more cards.

(D) On the web page **<Phone Setting →Features →Card Reader Working Mode >**option, select **<Normal>**.



(E) Click **<Apply>** and card reader would go back to the Normal status.

B. Method 2: It is used to batch add cards for intermediates.

(A) Use revocation admin card to touch card reader induction area, and it would enter revoking card status.

(B) Use the cards you want to delete from system to touch card reader induction area, and you might hear the card reader confirmed indication tone. Repeat step 2 to delete cards.

(C) Use revocation admin card to touch card reader induction area, and it would go back to card read only status.

C. Method 3: bulk delete or partially delete card records

(A) On the web page <**RFID Cards →Door Card Table >** select the card ID and then click **<Delete>**.

> Note
>
> If you click **<Delete All>,** system would delete all the ID card records.