User Manual
PA2

Software Version：2.6.0

Release Date：2019/09/20

Directory

1 Picture

2 Table

3 Safety Instruction

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

- Please use the external power supply that is included in the package. Other power supply may cause damage to the phone and affect the behavior or induce noise.
- Before using the external power supply in the package, please check the home power voltage. Inaccurate power voltage may cause fire and damage.
- Please do not damage the power cord. If power cord or plug is impaired, do not use it because it may cause fire or electric shock.
- Do not drop, knock or shake the phone. Rough handling can break internal circuit boards.
- This phone is design for indoor use. Do not install the device in places where there is direct sunlight. Also do not put the device on carpets or cushions. It may cause fire or breakdown.
- Avoid exposure the phone to high temperature or below 0℃ or high humidity.
- Avoid wetting the unit with any liquid.
- Do not attempt to open it. Non-expert handling of the device could damage it. Consult your authorized dealer for help, or else it may cause fire, electric shock and breakdown.
- Do not use harsh chemicals, cleaning solvents, or strong detergents to clean it. Wipe it with a soft cloth that has been slightly dampened in a mild soap and water solution.
- When lightning, do not touch power plug, it may cause an electric shock.
- Do not install this phone in an ill-ventilated place. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

4 Overview

PA2 is a SIP audio and video intercom developed specifically for the needs of industry users. Media streaming adopts the standard IP/RTP/RTSP protocol. It inherits the advantages of good stability of azimuthphone and carrier-grade sound quality, and is perfectly compatible with all current mainstream sip-based IPPBX/ soft switch /IMS platforms, such as Asterisk, Broadsoft, Metaswitch, 3CX, Elastix, etc. It sets a variety of functional interfaces in one: intercom, broadcast, video, security, recording, broadcast, adapt to a variety of use environment, convenient and rapid deployment of equipment, is the ideal choice.

5 Installation Guide

5.1 Use POE or external Power Adapter

PA2, called as ‘the device’ hereafter, supports two power supply modes, power supply from external power adapter or over Ethernet (POE) complied switch.

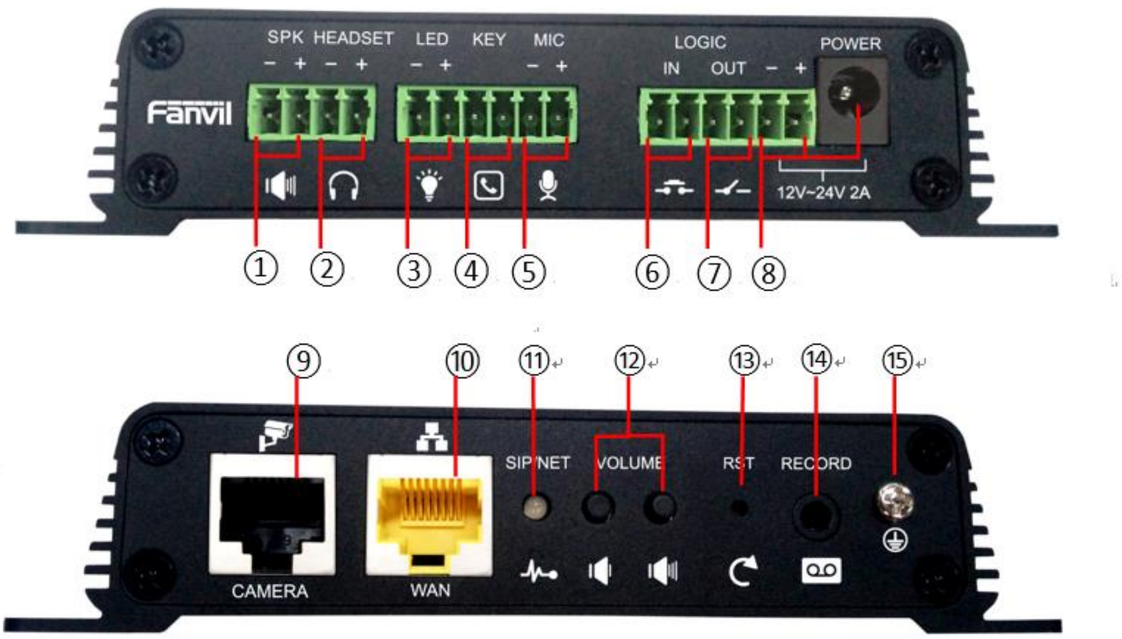
POE power supply saves the space and cost of providing the device additional power outlet. With a POE switch, the device can be powered through a single Ethernet cable which is also used for data transmission. By attaching UPS system to POE switch, the device can keep working at power outage just like traditional PSTN telephone which is powered by the telephone line.

For users who do not have POE equipment, the traditional power adaptor should be used. If the device is connected to both PoE switch and external power adapter, PA2 will get power supply from PoE switch in priority, and change to external power adapter once the PoE power supply fails.
Please use the power adapter supplied by Fanvil and the POE switch met the specifications to ensure the device work properly.

5.2 Install

Before you start using the device, please install the following:

5.2.1 button instruction



Picture 1 - button instruction

The image above shows the key layout of the device. Each button provides its own specific function. The user can refer to the instructions for the keys in the illustration in this section to operate the device.

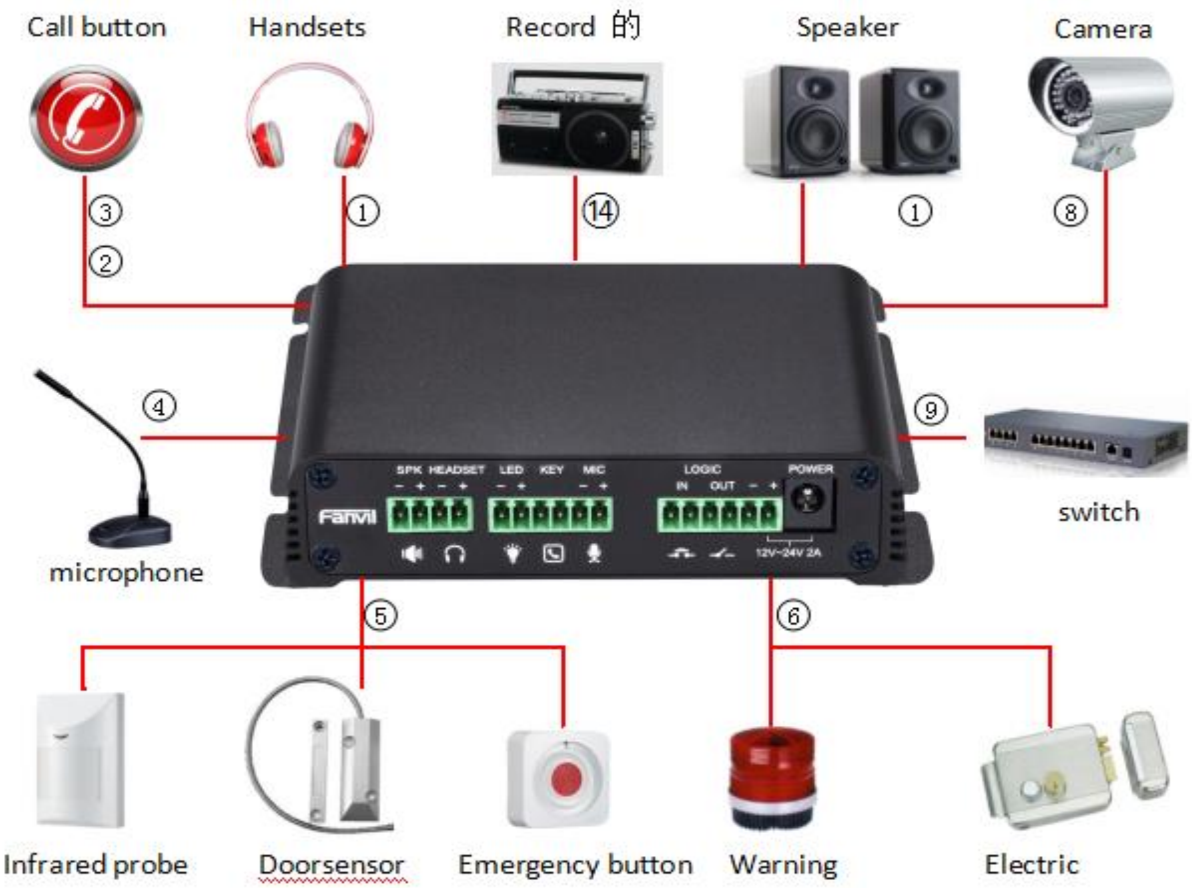
Table 1 - button instruction

Label	Explanation
① Speaker interface	according to the device input voltage adaptive output maximum power; 4Ω speaker, POE / 10W, 12V / 10W, 18V / 20W, 24V / 30W. The greater the horn impedance, the smaller the output power. Suggested wire diameter: 18AWG or larger diameter.
② Headset interface	Speaker audio line signal output impedance 32 Ohm, single ended output voltage 1.2V, used for external headphones or active speakers
③ LED interface	Output 5V voltage 5 mA current, can be an external LED, indicating the network status, call status, registration status.
④ Function key interface	connection switch, you can log on page set the call number or IP address.
⑤ Microphone interface	Recommend the use of 2.2K Ohm impedance electret condenser microphone, sensitivity: -38dB, bias voltage 2.2V. Microphone signal cable it is recommended to use a shielded cable and do not connect the shield cable to the grounding screw, improve

	anti-interference.
⑥ Switch input interface	Connect an infrared probe or emergency switch or Doorsensor and other switch components.
⑦ Switch output interface	corresponding to the short-circuit input interface, login device security page settings, you can control the alarm light, electric locks and other equipment; with the adjacent ⑧ power port connection for external equipment power supply.
⑧ Power input interface	12V ~ 24V 2A input, according to the input voltage to determine the maximum output power amplifier.
⑨ Camera interface	standard RJ45 interface, connect the original camera, the proposed use of five or five sub-network cable
⑩ Ethernet interface	WAN port, standard RJ45 interface, 10 / 100M adaptive, support POE input, it is recommended to use five or super five network cable.
⑪Registration/Network LED	indicates network status, call status, registration status. Fast flashing: network anomaly or SIP account exception. Slow flashing: during a call. Always bright: successful registration.
⑫Volume control key	When device is idle, the button is used to adjust the volume of ringtone, when the device is in call, the button is used to adjust call volume and when device is having broadcast, the button is used to adjust broadcast volume.
⑬Restore factory key	press and hold for 3 seconds to flash the device to restart and restore the factory settings.
⑭Recording output interface	the local microphone voice and call voice mixed output, suitable for computer and other equipment recording.
⑮Grounding screw	When PA2’ s external part is connected to metal shell or panel, please connect the external part to this interface, in order to prevent static electricity or other interferences which may affect the device’ s normal working.

5.2.2 Confirm the connection

Confirm whether the equipment of the power cord, network cable and the boot-up is normal. (Check the network state of light)



Picture 2 - connected graphs

5.3 Appendix Table

5.3.1 Common command mode

Table 2 - Common command mode

Action	Description
Standby to IP	Wait for captain to press volume down button 3s to report IP
Switching network mode	In standby mode, long press the volume button for 10 seconds, and there will be a beep sound and the indicator light will flash for 5 seconds. Within 5 seconds, press the volume up button for three times continuously to switch the network mode. Network status is static or PPPoE mode will be switched to DHCP mode; When the network is DHCP mode, it will be switched to static IP 192.168.1.128, and IP will be reported after successful switch

5.3.2 Function key LED state

Table 3 - Function key LED state

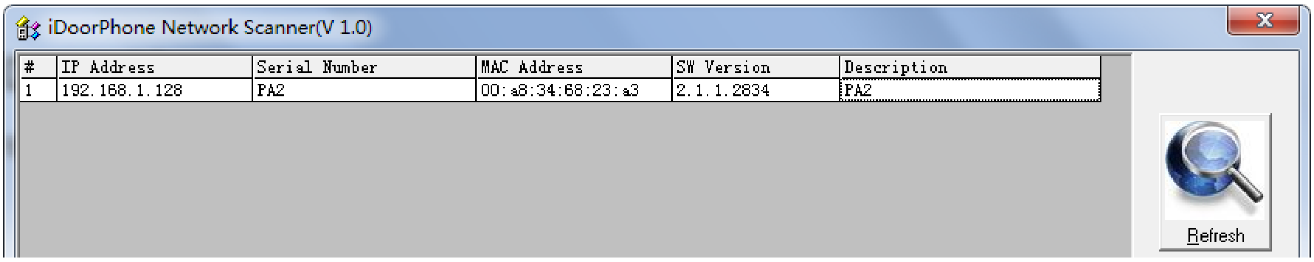
Type	LED	State
Line/network	Quick flashing	Registration failed/ network abnormal
	Normally on	Successfully registered
	Slow flashing	In call

6 Basic Introduction

6.1 Quick Setting

Before proceeding with this step, make sure your Internet broadband connection is working properly and complete the network hardware connection. The default factory mode of is fixed IP address mode, which is 192.168.1.128 by default.

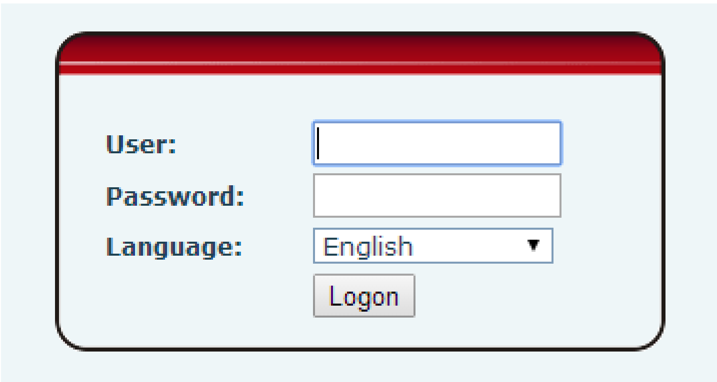
- Long press the volume down button on the device for 3 seconds (30 seconds after power on), and the voice will automatically play the IP address of the device or use the "IP scan tool" software to find the IP address of the device.（Download http://download.fanvil.com/tool/iDoorPhoneNetworkScanner.exe）
- Long press the volume up button for 10 seconds (30 seconds after power on), wait for the speaker to emit rapid beep sound, then quickly press the volume up button for three times, the beep stops. After waiting for 10 seconds, the system will automatically broadcast the IP address after successfully switching to dynamic IP acquisition. Switch again to a fixed IP address.
- Login to the device's WEB page for configuration according to the IP address
- Configure the account, user name, server address and other parameters required for registration provided by the service provider on the WEB configuration page;



Picture 3 - Quickly setting

6.2 WEB configuration

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



Picture 4 - WEB Login

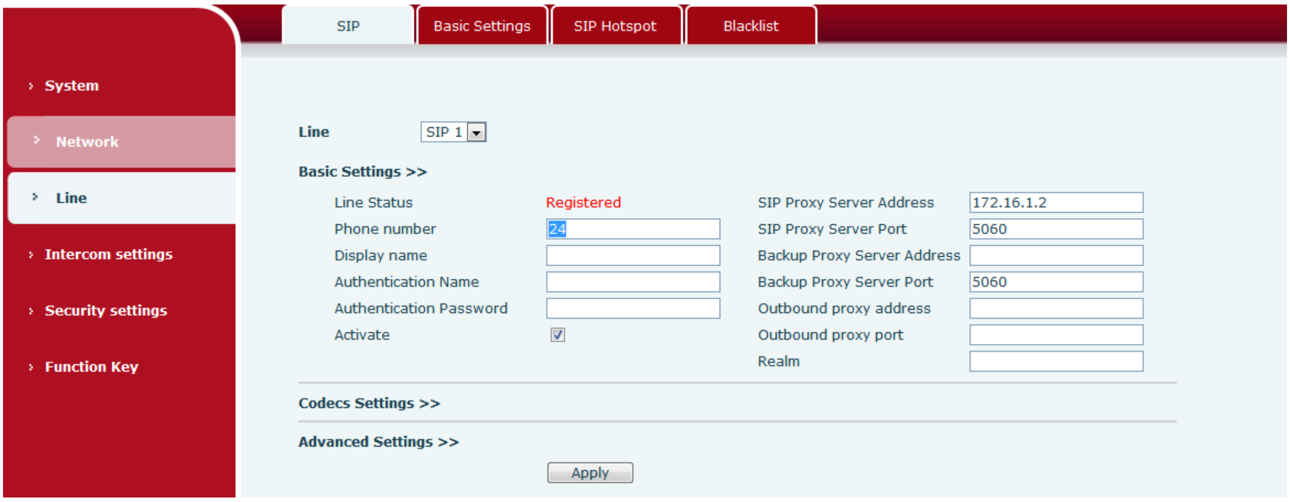
The username and password should be correct to log in to the web page. **The default username and password are "admin"**. For the specific details of the operation of the web page, please refer to [9 Web Configurations]

6.3 SIP Configurations

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

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

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

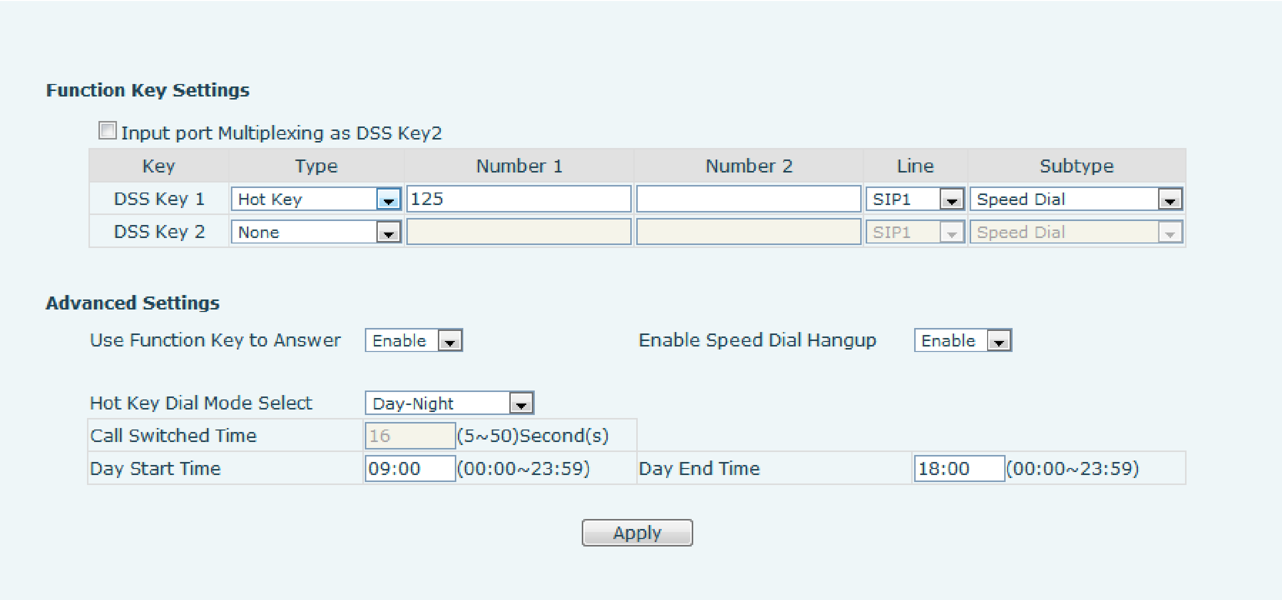


Picture 5 - SIP Line Configuration

7 Basic Function

7.1 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:



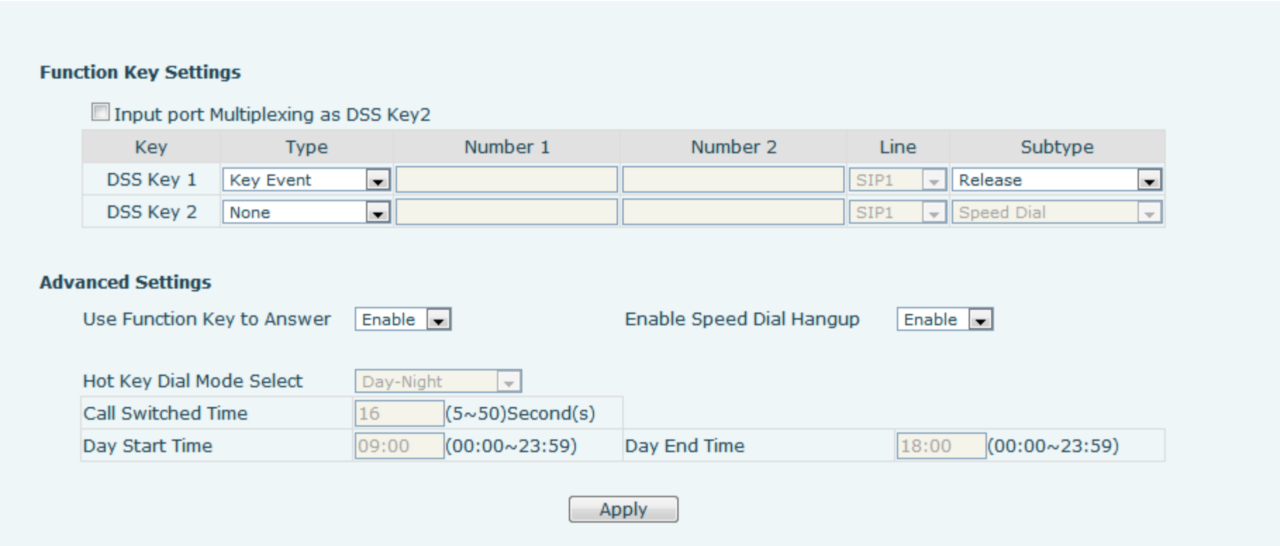
Picture 6 - Function Setting

See detailed configuration instructions 9.26 Function Key

7.2 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.

7.3 End of the Call



Picture 7 - - Function Setting

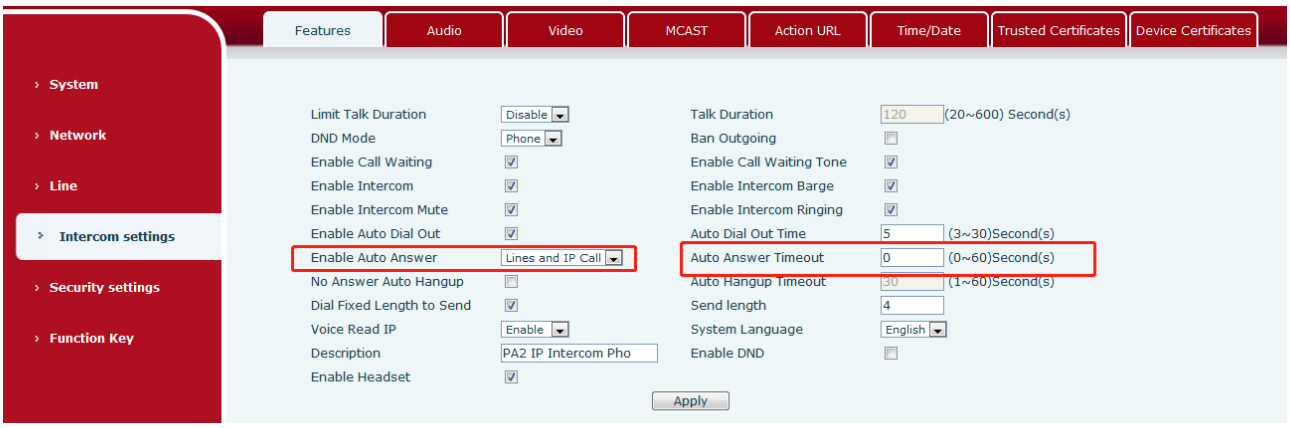
You can hang up the call through the Release key (you can set the function key as the Release key) or turn on the speed dial button to hang up the call. See detailed configuration instructions 9.26 Function Key.

7.4 Auto-Answering

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

Web interface:

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



Picture 8 - Enable Auto Answer

- Auto Answer mode:
  - Disable：Turn off the automatic answer function, the device has a call, ring, will not time out to answer automatically.
  - Line1：Line 1 has an automatic call timeout.

■ Line2：Line 2 has an automatic call timeout.

■ Line1 and Line2：Line 1 and line 2 have an automatic call timeout.

■ Lines and IP Call：Line and IP direct dial call timeout automatically answer.

- Auto Answer Timeout（0~60）

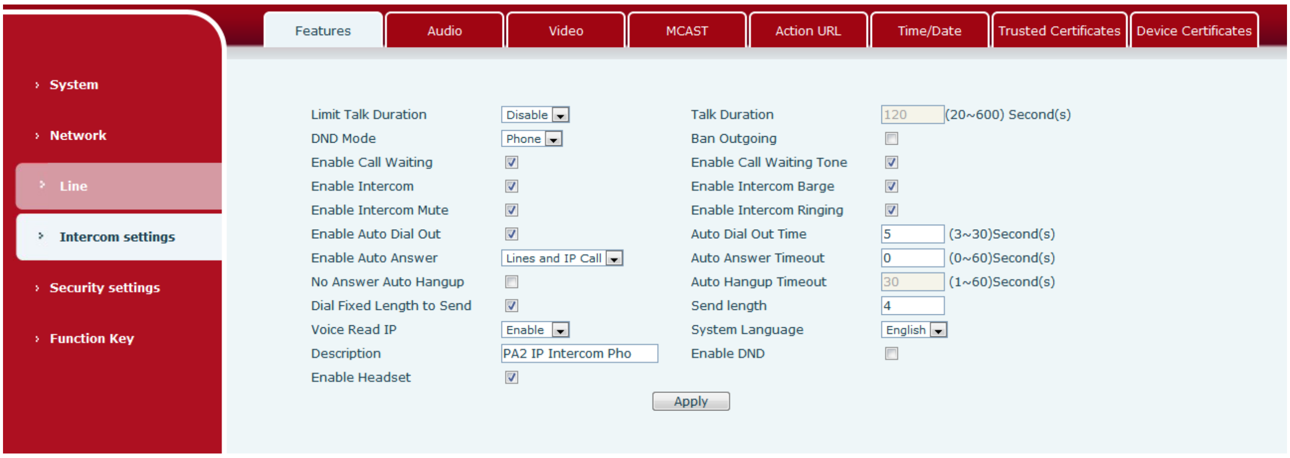
The range can be set to 0~60s, and the call will be answered automatically when the timeout is set.

7.5 DND

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

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

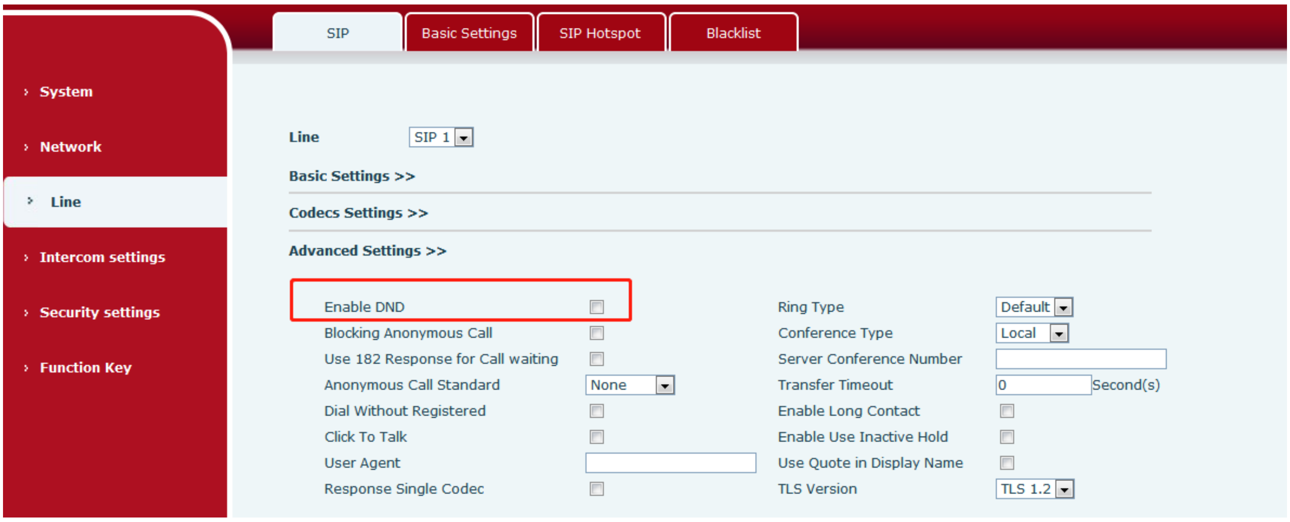
- Web interface: enter [**Intercom Settings**] >> [**Features**], set the DND Mode to phone and Enable DND.



Picture 9 - Set DND Option

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

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



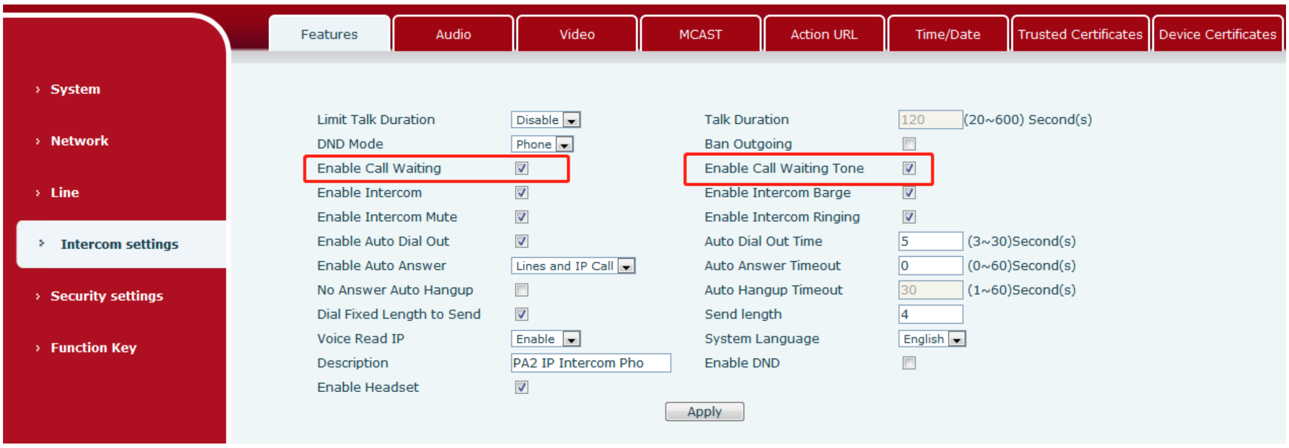
Picture 10 - Enable DND

7.6 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.

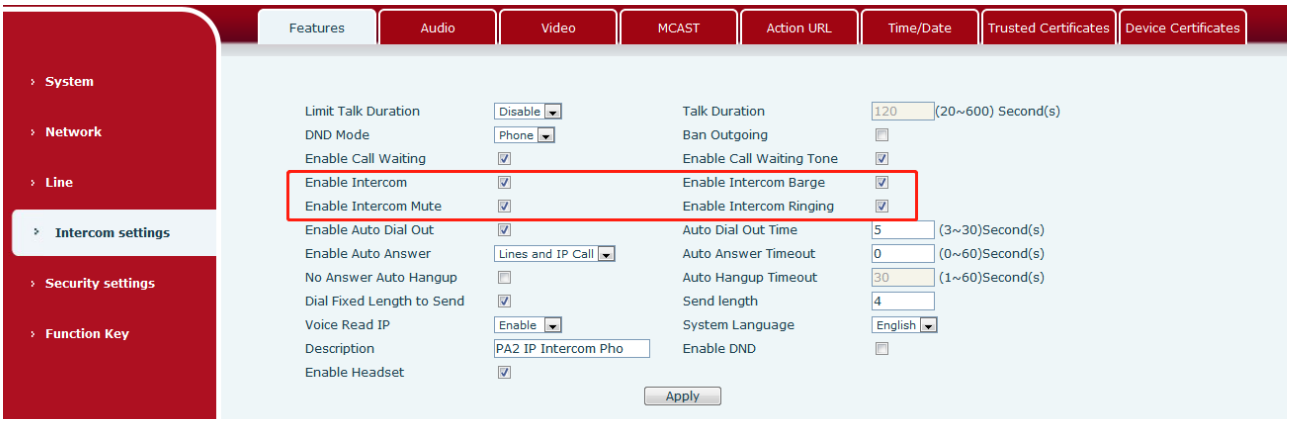


Picture 11 - Call Waiting

8 Advance Function

8.1 Intercom

The equipment can answer intercom calls automatically.



Picture 12 - WEB Intercom

Table 4 - Intercom

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, PA2 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 intercome call
Enable Intercom Mute	Enable mute during intercom mode
Enable Intercom Ringing	If the incoming call is intercom call, the device plays the intercom tone.

8.2 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.

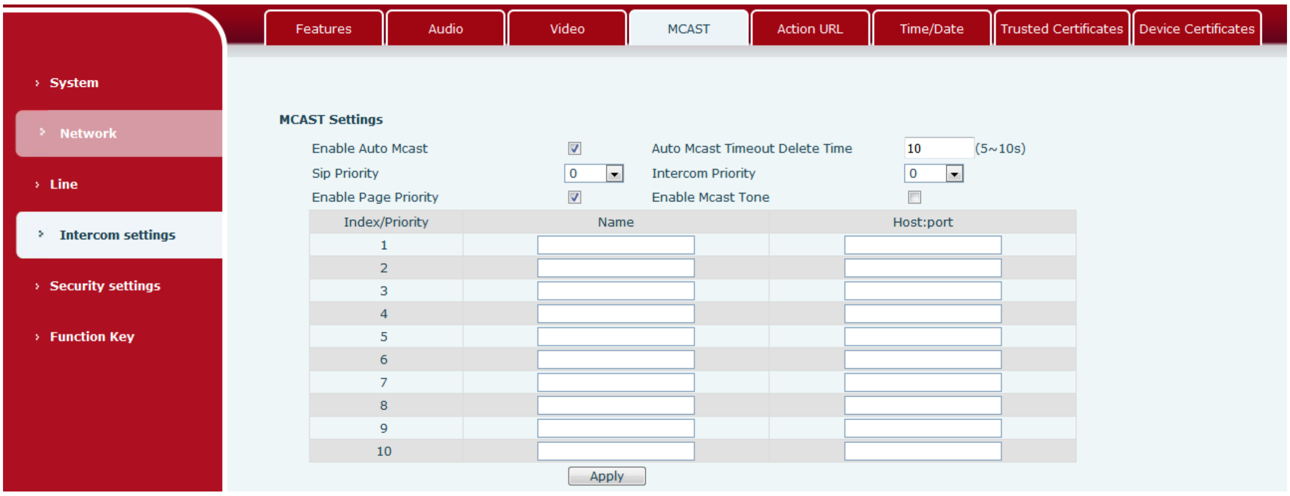


Figure 1 - Picture 13 - MCAST

Table 5 - MCAST

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.
- Receive end will receive multicast call and play multicast automatically.

8.3 Hotspot

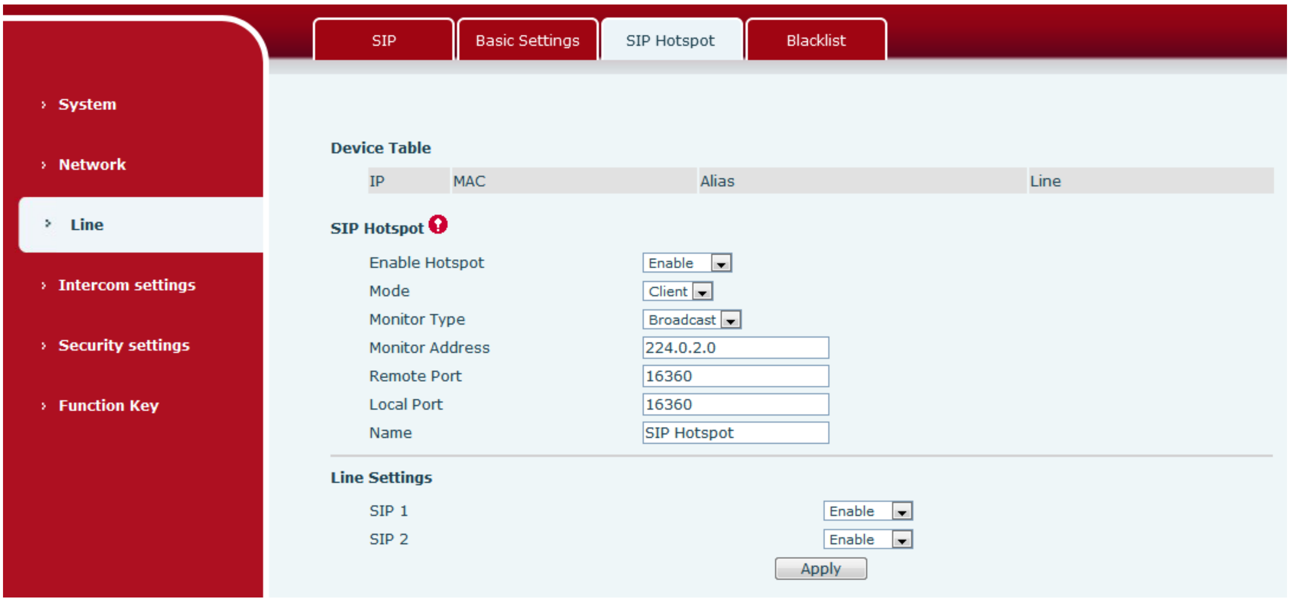
SIP hotspot is a simple utility. Its configuration is simple, which can realize the function of group vibration and expand thequantity of sip account. Take one device A as the SIP hotspot and the other devices (B, C) as the SIP hotspot client. When someone calls device A, devices A, B, and C will ring, 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.

Table 6 - SIP Hotspot

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 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.



Picture 14 - SIP Hotspot

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

9 Web Configurations

9.1 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 is also locked

9.2 System >> Information

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

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

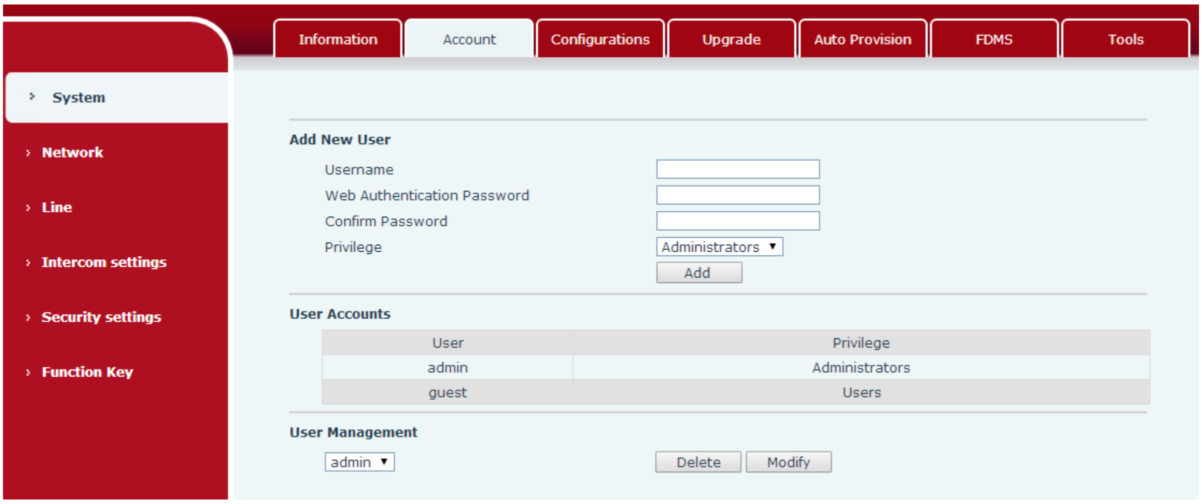
And summarization of network status,

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

Besides, summarization of SIP account status,

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

9.3 System >> Account

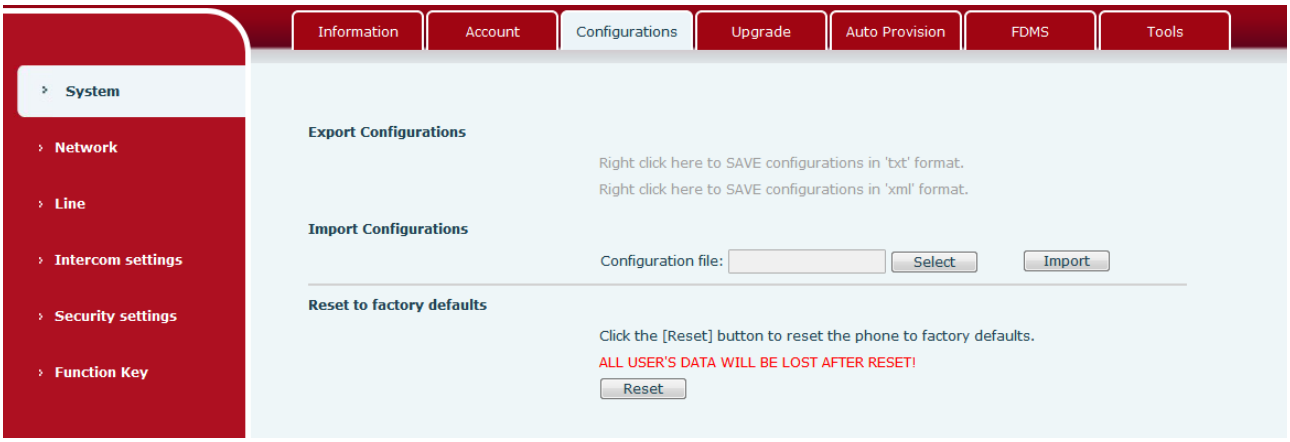


Picture 15 - WEB Account

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

9.4 System >> Configurations

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



Picture 16 - System Setting

- **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)

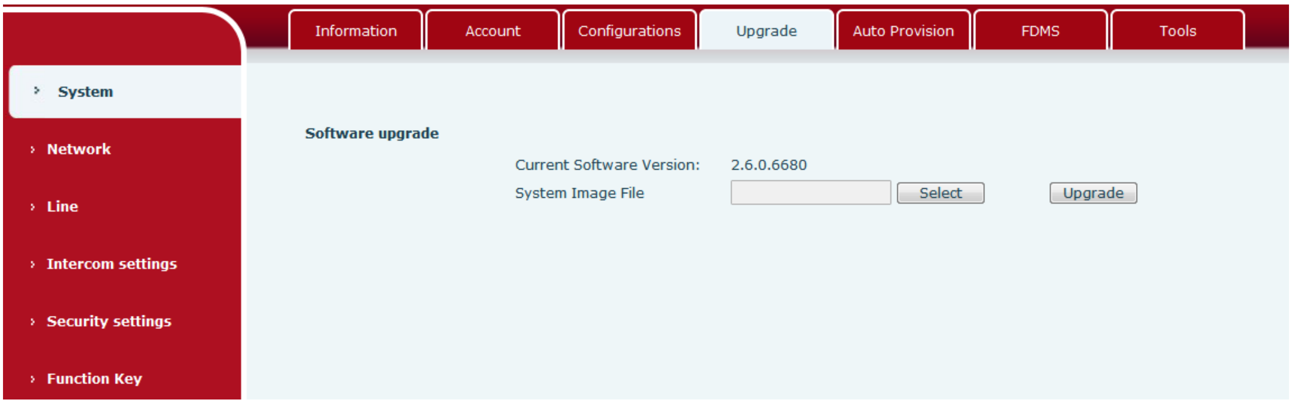
- **Import Configurations**

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

■ **Reset Phone**

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

9.5 System >> Upgrade



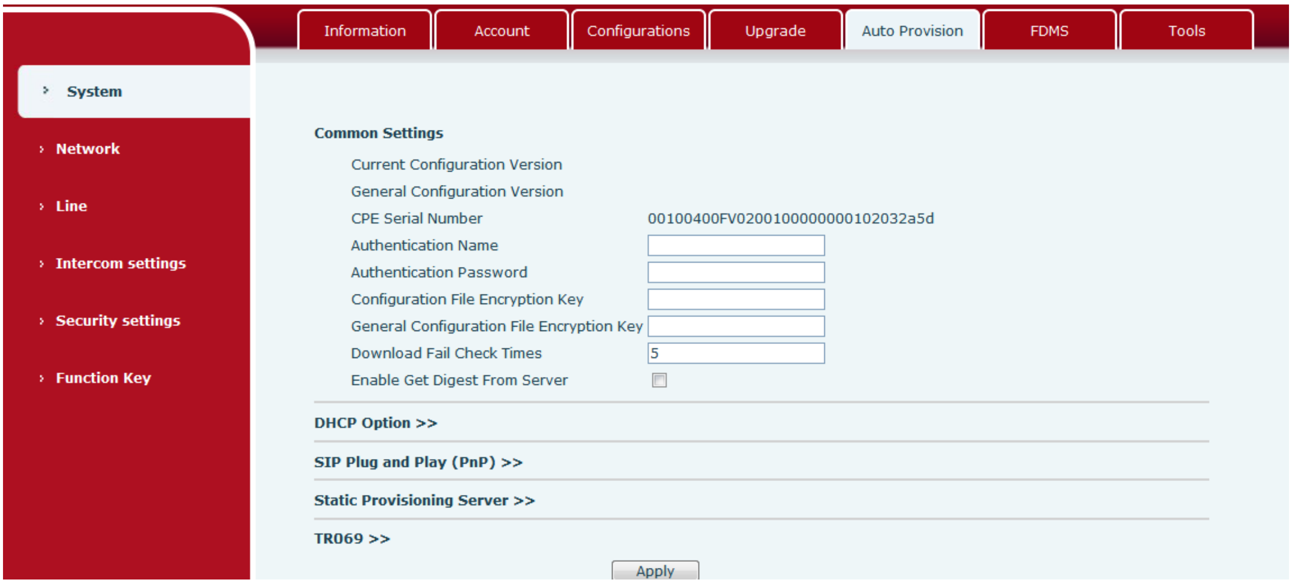
Picture 17 - Upgrade

Upgrade the software version of the device, and upgrade to the new version through the webpage. After the upgrade, the device will automatically restart and update to the new version.

Click select, select the version and then click upgrade

9.6 System >> Auto Provision

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



Picture 18 - Auto provision

Fanvil devices support SIP PnP, DHCP options, Static provision, TR069. If all of the 4 methods are enabled, the priority from high to low as below:

PNP>DHCP>TR069> Static Provisioning

Transferring protocol: FTP 、 TFTP 、 HTTP 、 HTTPS

Details refer to **Fanvil Auto Provision**

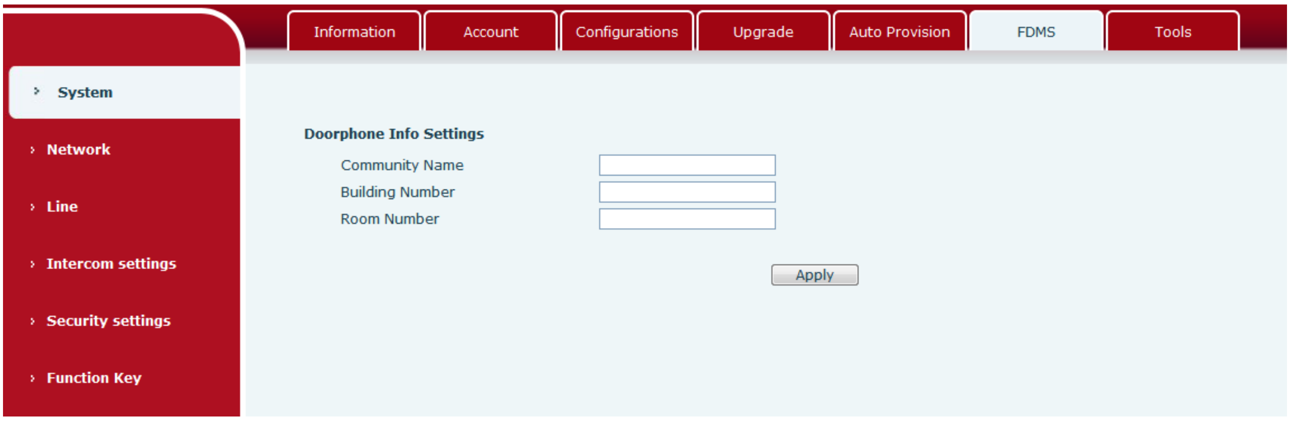
http://www.fanvil.com/Uploads/Temp/download/20180920/5ba38170d79fb.pdf

Table 7 - Auto provision

Auto provision	
Parameters	**Description**
Basic settings	
Current Configuration Version	Shows the current config file' s version. If the version of the downloaded configuration file is same with this one, the configuration file will not be applied. If the device confirm the configuration by the Digest method, once the configuration of server is modified or the device' s configurations are different from server' s, the device will download and apply the configurations.
General Configuration Version	Shows the common config file' s version. If the version of the downloaded configuration file is same with this one, the configuration file will not be applied. If the device confirm the configuration by the Digest method, once the configuration of server is modified or the device' s configurations are different from server' s, the device will download and apply the configurations.
CPE Serial Number	Serial number of the equipment
Authentication Name	Username for configuration server. Used for FTP/HTTP/HTTPS. If this is blank the phone will use anonymous
Authentication Password	Password for configuration server. Used for FTP/HTTP/HTTPS.
Configuration File Encryption Key	Encryption key for the configuration file
General Configuration File Encryption Key	Encryption key for common configuration file
Download Fail Check Times	The default value is 5. If the download configuration fails, it will be downloaded 5 times.
Enable Get Digest From Server	When the feature is enable, if the configuration of server is changed, phone will download and update.
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. Must be from 128 to 254.

Enable DHCP Option 120	Set the SIP server address through DHCP option 120.
SIP Plug and Play (PnP)	
Enable SIP PnP	Whether enable PnP or not. If PnP is enable, phone will send a SIP SUBSCRIBE message with broadcast method. Any server can support the feature 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	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	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.
TR069	
Enable TR069	Enable TR069 after selection
Enable TR069 Warning Tone	If TR069 is enabled, there will be a prompt tone when connecting.
ACS Server Type	There are 2 options 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)
STUN server address	Enter the STUN address
Enable the STUN	Enable the STUN
TLS Version	TLS Version

9.7 System >> FDMS



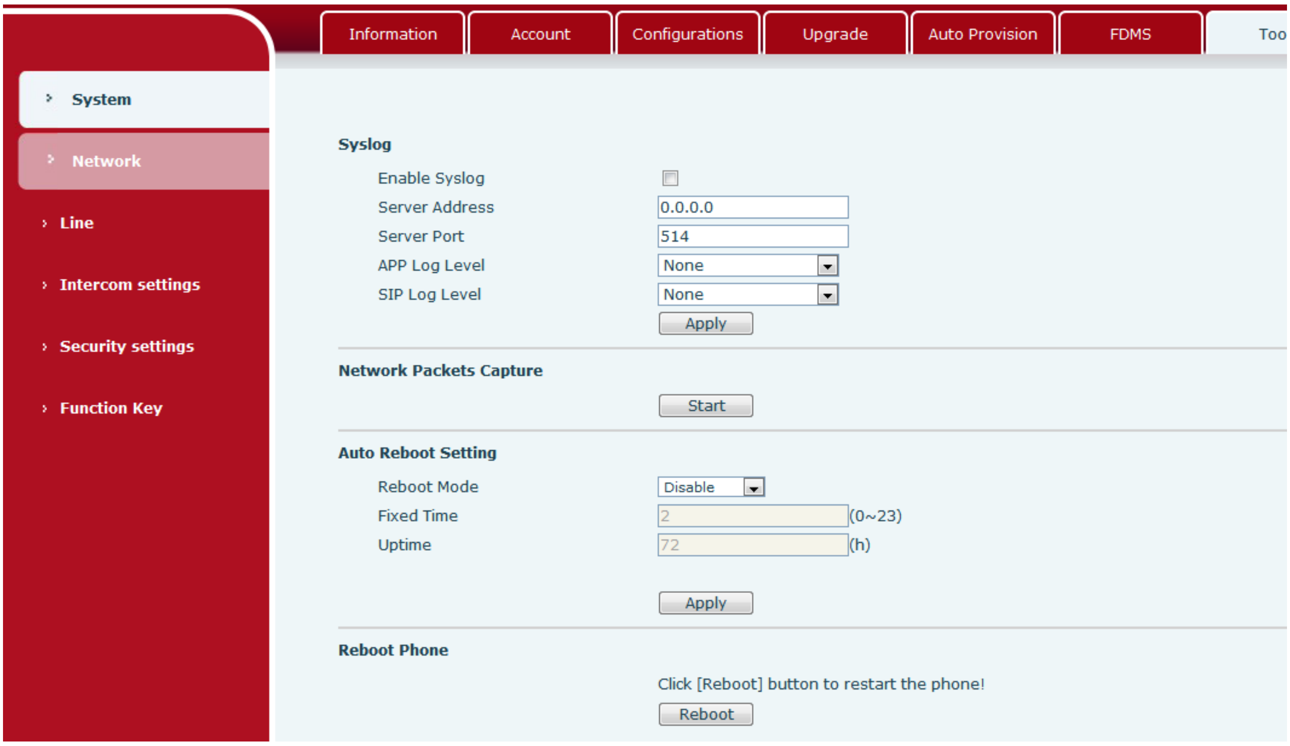
Picture 19 - FDMS

Table 8 - FDMS

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

9.8 System >> Tools

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



Picture 20 - Tools

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 Fanvil technical support.

Auto Reboot Setting:

Reboot Mode:

Disable：It will not restart at set time after disabled

Fixed Time：In the range of 0~24 (h), restart will be conducted at the setting point every day after the setting is completed

Uptime：**Set the maximum** length to 3 bits and restart at run time

For other details, please refer to 10 trouble shooting

9.9 Network >> Basic

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

Picture 21 - Network Basic Setting

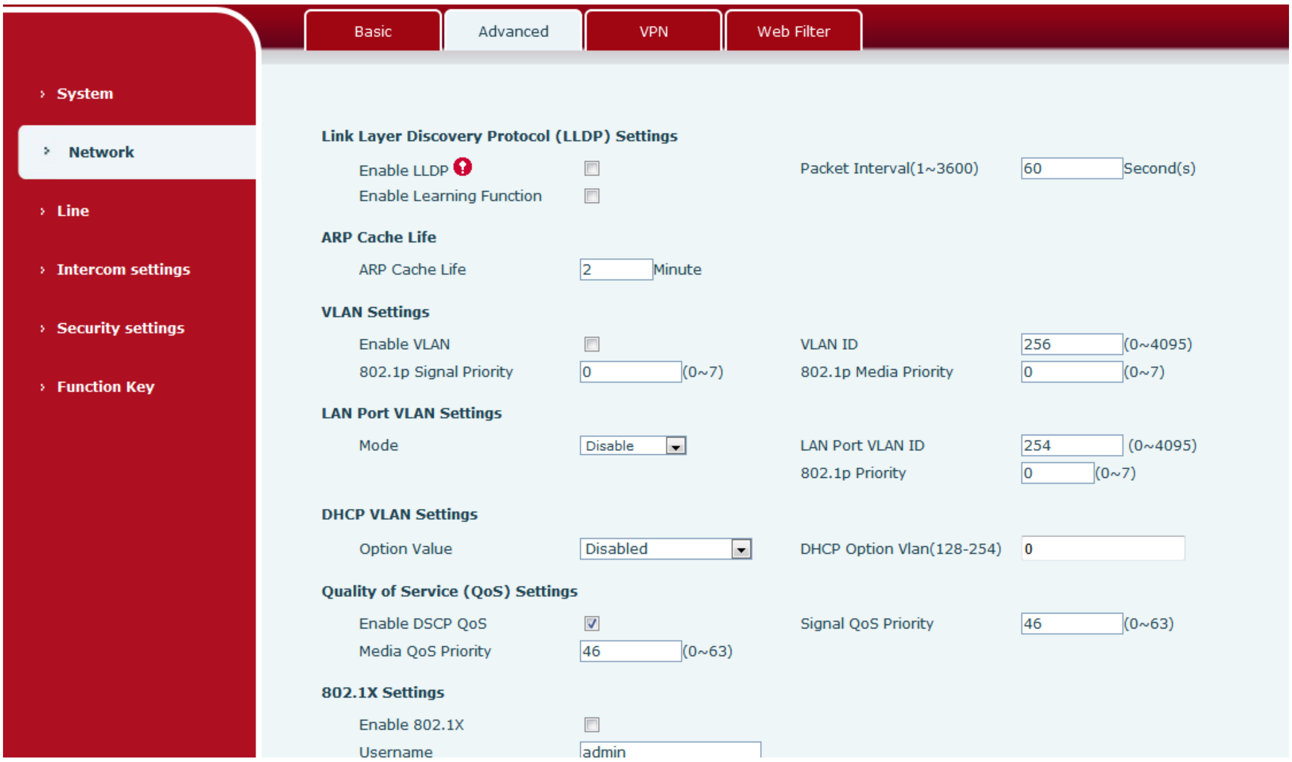
Table 9 - Network Basic Setting

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 Time stamp	Display the time when the device gets the MAC address
Settings	
Select the appropriate network mode. The equipment supports three network modes:	
Static IP	Network parameters must be entered manually and will not change. All parameters are provided by the ISP.
DHCP	Network parameters are provided automatically by a DHCP server.
PPPoE	Account and Password must be input manually. These are provided by your ISP.
If 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.
attention： 1）After setting the parameters, click【Apply】to take effect. 2）If you change the IP address, the webpage will no longer responds, 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	
Service Port Settings	
Web Server Type	Specify Web Server Type – HTTP or HTTPS
HTTP Port	Port for web browser access. Default value is 80. To enhance security, change this from the default. Setting this port to 0 will disable HTTP access. Example: The IP address is 192.168.1.70 and the port value is 8090,

	the accessing address is http://192.168.1.70:8090.
HTTPS Port	Default value is 443. To enhance security, change this from the default.

9.10 Network >> Advanced



Picture 22 - Network Setting

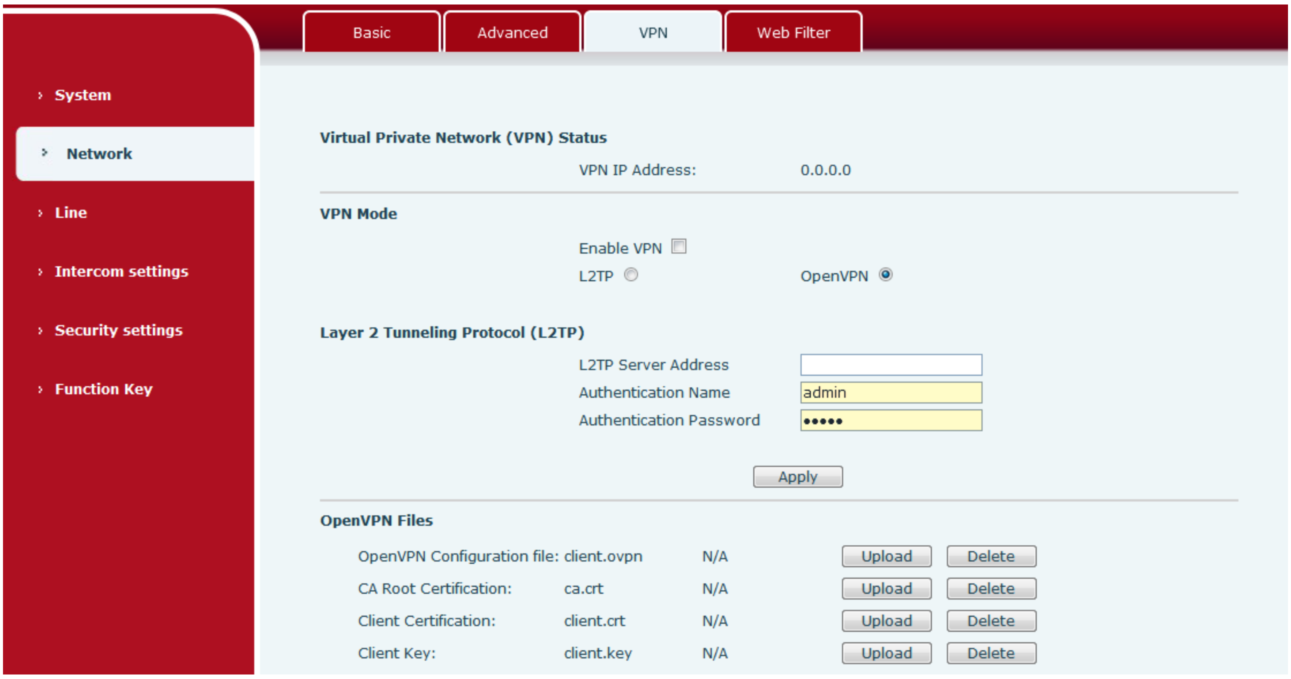
Network advanced Settings are typically configured by IT administrators to improve the quality of device service.

Table 10 - Network Setting

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

9.11 Network >> VPN



Picture 23 - VPN

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

For some users, especially enterprise users, a VPN connection might be required to be established before 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**

NOTICE! 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 webpage [**Network**] >> [**VPN**]. In VPN Mode, check the "Enable VPN" option and select "L2TP", then fill in the L2TP server address, Authentication Username, and Authentication Password in the L2TP section. Press "Apply" then the device will try to connect to the L2TP server.

When the VPN connection established, the VPN IP Address should be displayed in the VPN status. There may be some delay of the connection establishment. User may need to refresh the page to update the status.

Once the VPN is configured, the device will try to connect with the VPN automatically when the device boots up every time until user disable it. Sometimes, if the VPN connection does not establish 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,

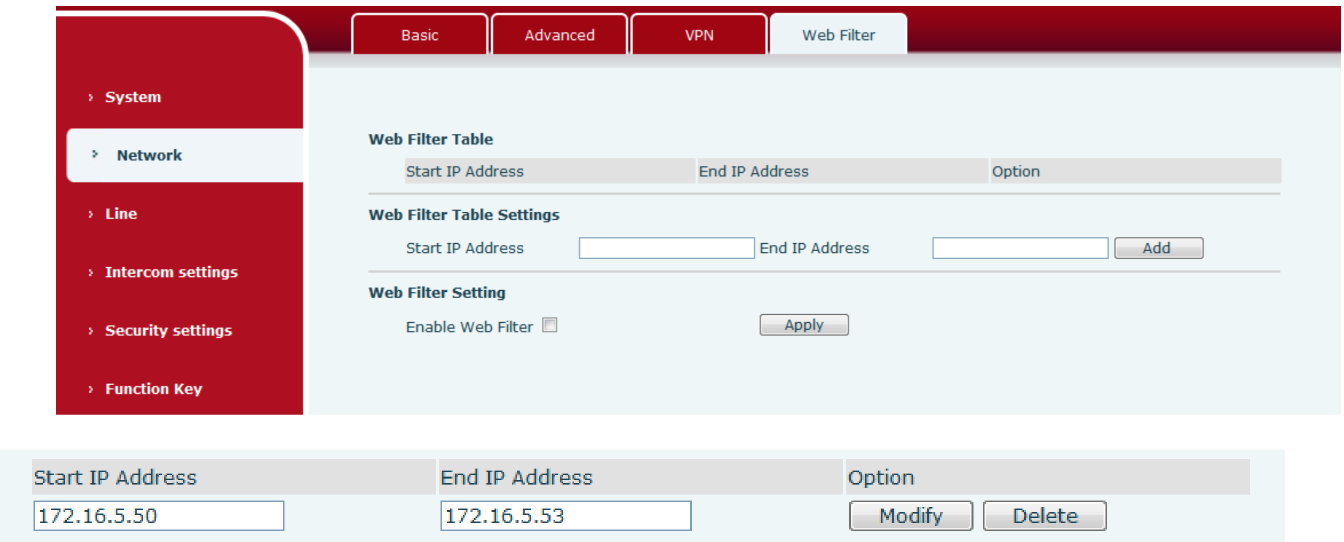
OpenVPN Configuration file:	client.ovpn
CA Root Certification:	ca.crt
Client Certification:	client.crt
Client Key:	client.key

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

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

9.12 Network >> Web Filter

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



Picture 24 - WEB Filter Table

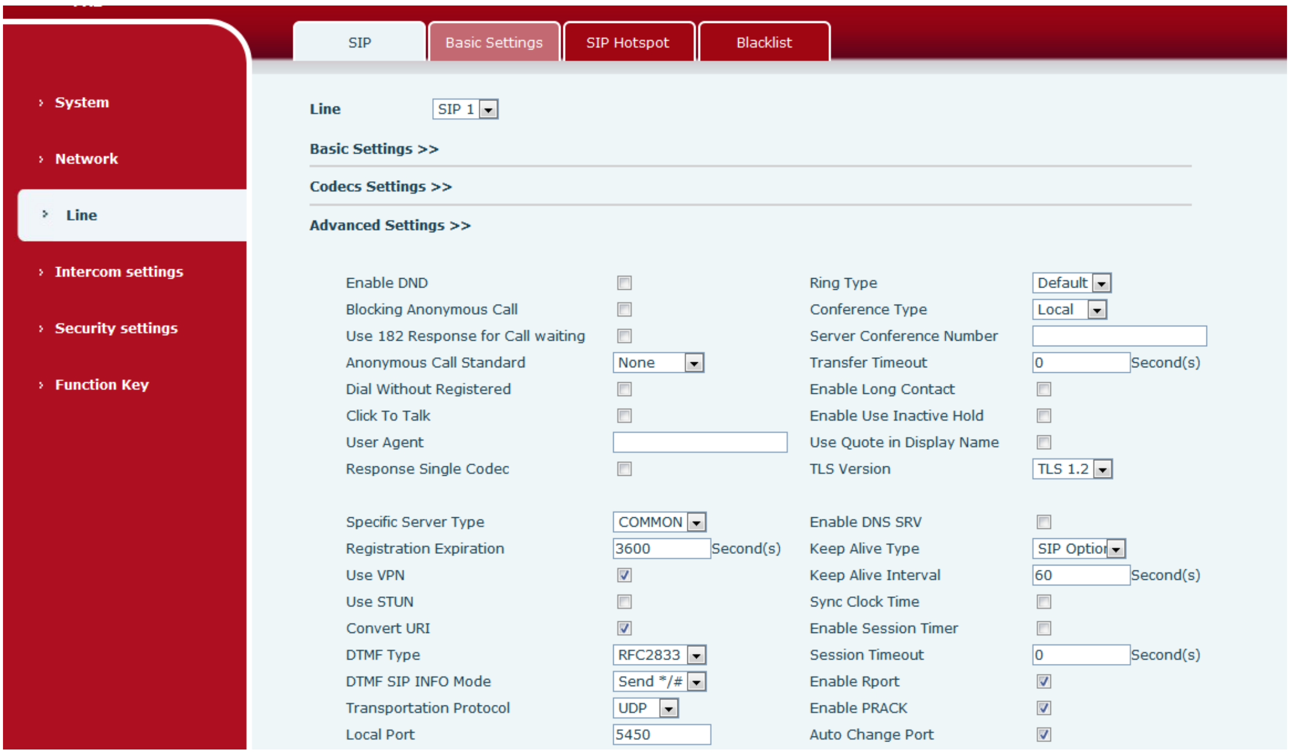
Add and remove IP segments that are accessible; Configure the starting IP address within the start IP, end the IP address within the end IP, and click [**Add**] to submit to take effect. A large network segment can be set, or it can be divided into several network segments to add. When deleting, select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

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

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

9.13 Line >> SIP

Configure the service configuration for the wire on this page.



Picture 25 - SIP

Table 11 - SIP

SIP	
Field Name	**Explanation**
Basic Settings (Choose the SIP line to configured)	
Line Status	Display the current line status at page loading. To get the up to date line status, user has to refresh the page manually.

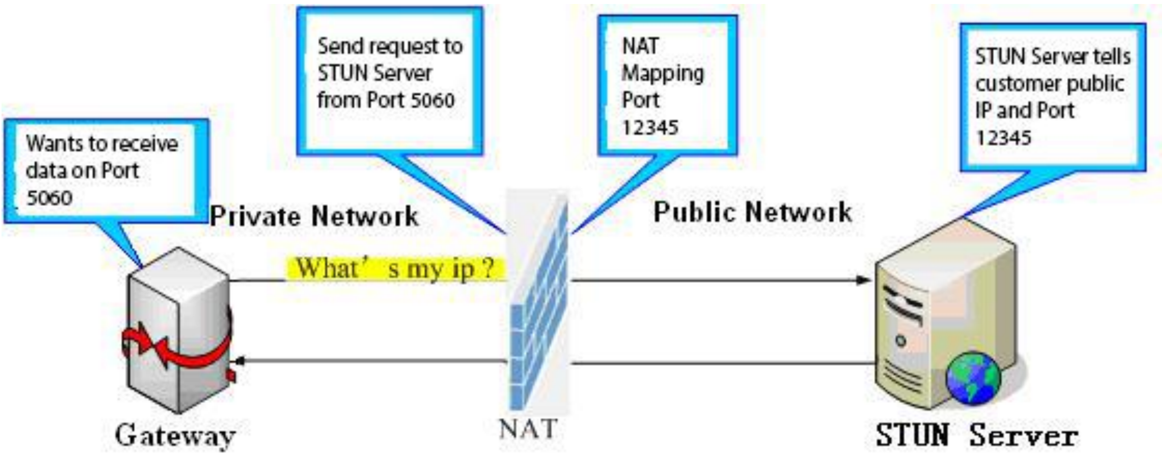
Username	Enter the username of the service account.
Display name	Enter the display name to be sent in a call request.
Authentication Name	Enter the authentication name of the service account
Authentication Password	Enter the authentication password of the service account
Activate	Whether the service of the line should be activated
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server
SIP Proxy Server Port	Enter the SIP proxy server port, default is 5060
Outbound proxy address	Enter the IP or FQDN address of outbound proxy server provided by the service provider
Outbound proxy port	Enter the outbound proxy port, default is 5060
Realm	Enter the SIP domain if requested by the service provider
Codecs Settings	
Set the priority and availability of the codecs by adding or remove them from the list.	
Advanced Settings	
Enable DND	Enable Do-not-disturb, any incoming call to this line will be rejected automatically
Blocking Anonymous Call	Reject any incoming call without presenting caller ID
Use 182 Response for Call waiting	Set the device to use 182 response code at call waiting response
Anonymous Call Standard	Set the standard to be used for anonymous
Dial Without 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.
Response Single Codec	If setting enabled, the device will use single codec in response to an incoming call request
Ring Type	Set the ring tone type for the line
Conference Type	Set the type of call conference, Local=set up call conference by the device itself, maximum supports two remote parties, Server=set up call conference by dialing to a conference room on the server
Server Conference Number	Set the conference room number when conference type is set to be Server
Enable Long Contact	Allow more parameters in contact field per RFC 3840
Enable use inactive hold	Active capture package SDP is inactive, while the hold is sendrecv. Active capture package has no response of 400, etc. Hold the hair inactive

	After closing the grab packet, you can see that the DSP is sendonly and the hold is sendrecv
TLS version	TLS version
Specific Server Type	Set the line to collaborate with specific server type
Registration Expiration	Set the SIP expiration interval
Use VPN	Set the line to use VPN restrict route
Use STUN	Set the line to use STUN for NAT traversal
Convert URI	Convert not digit and alphabet characters to %hh hex code
DTMF Type	Set the DTMF sending mode, there are four types: In-band RFC2833 SIP_INFO AUTO Different service providers may offer different models
DTMF SIP INFO Mode	When the device's DTMF type is set to SIP_INFO The DTMF_SIP_INFO type is configured to send */#, and when the device presses the */# key, the actual value sent is */#; Configured to send 10/11, when the device presses the */# key, the actual value sent is 10/11.
Transportation Protocol	Set the line to use TCP or UDP for SIP transmission
Local Port	Set the Local Port
SIP Version	Set the SIP version
Caller ID Header	Set the Caller ID Header
Enable Strict Proxy	Enables the use of strict routing. When the phone receives packets from the server, it will use the source IP address, not the address in via field.
Enable user=phone	Sets user=phone in SIP messages.
Enable SCA	Enable/Disable SCA (Shared Call Appearance)
Enable DNS SRV	Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole opened
Keep Alive Interval	Set the keep alive packet transmitting interval
Enable Session Timer	Set the line to enable call ending by session timer refreshment. The call session will be ended if there is not new session timer event update received after the timeout period

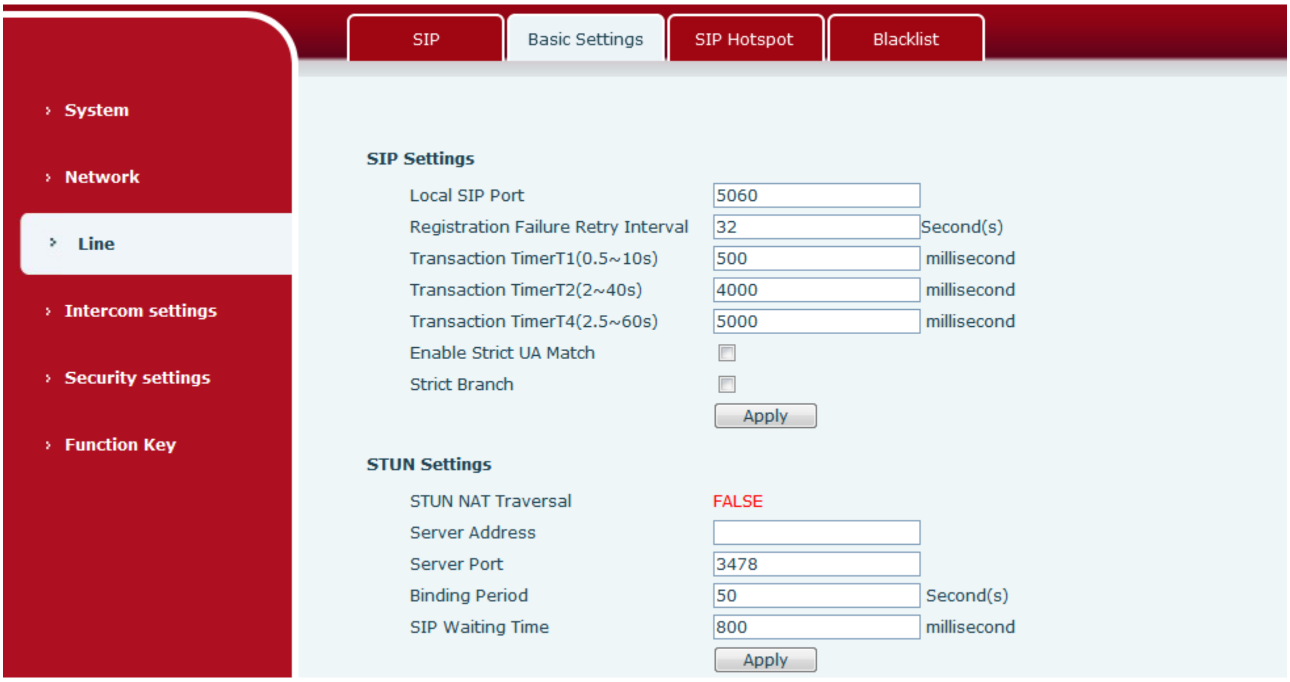
Session Timeout	Set the session timer timeout period
Enable Rport	Set the line to add rport in SIP headers
Enable PRACK	Set the line to support PRACK SIP message
Enable DNS SRV	Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list
Auto Change Port	Enable/Disable Auto Change Port
Keep Authentication	Keep the authentication parameters from previous authentication
Auto TCP	Using TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)
RTP Encryption	Set the pass phrase for RTP encryption
Enable MAC Header	When enabled, all SIP messages strip Mac fields
Enable Register MAC Header	When enabled, register the message ribbon Mac field

9.14 Line >> 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.



Picture 26 - Network Basic



Picture 27 - Line Basic Setting

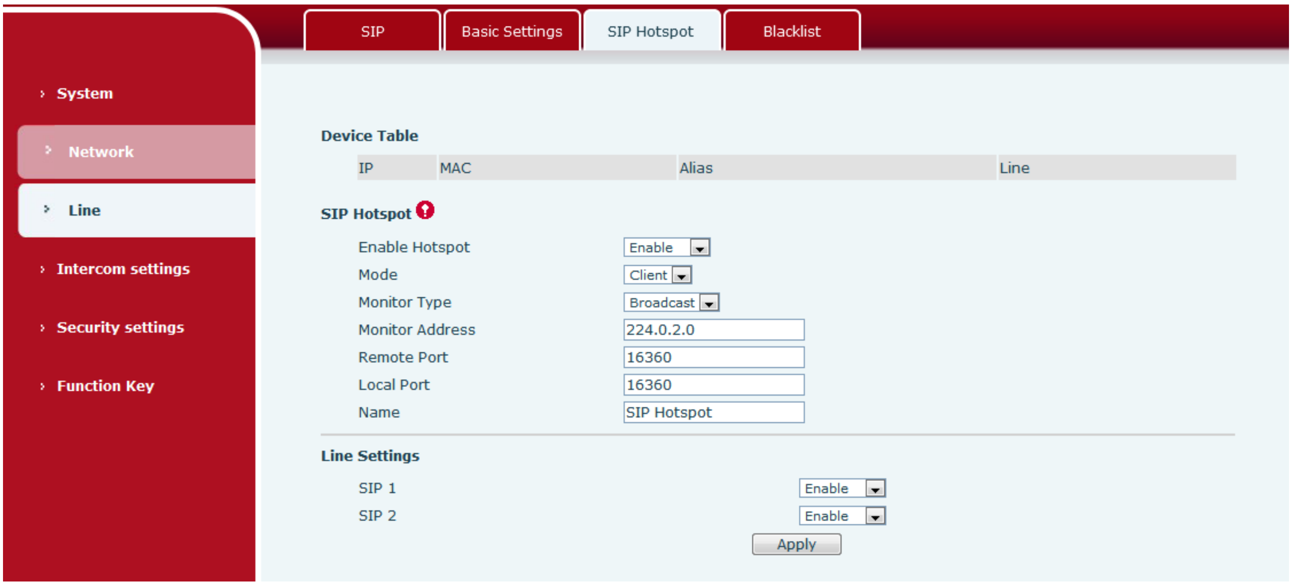
Table 12 - Line Basic Setting

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.
Enable Strict UA Match	Enable or disable Strict UA Match
Field Name	**Explanation**
STUN Settings	
Server Address	STUN Server IP address
Server Port	STUN Server Port – Default is 3478.
Binding Period	STUN blinding period – STUN packets are sent at this interval to keep the NAT mapping active.
SIP Waiting Time	Waiting time for SIP. This will vary depending on the network.

9.15 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.

See 8.3 Hotspot for details.



Picture 28 - SIP Hotspot

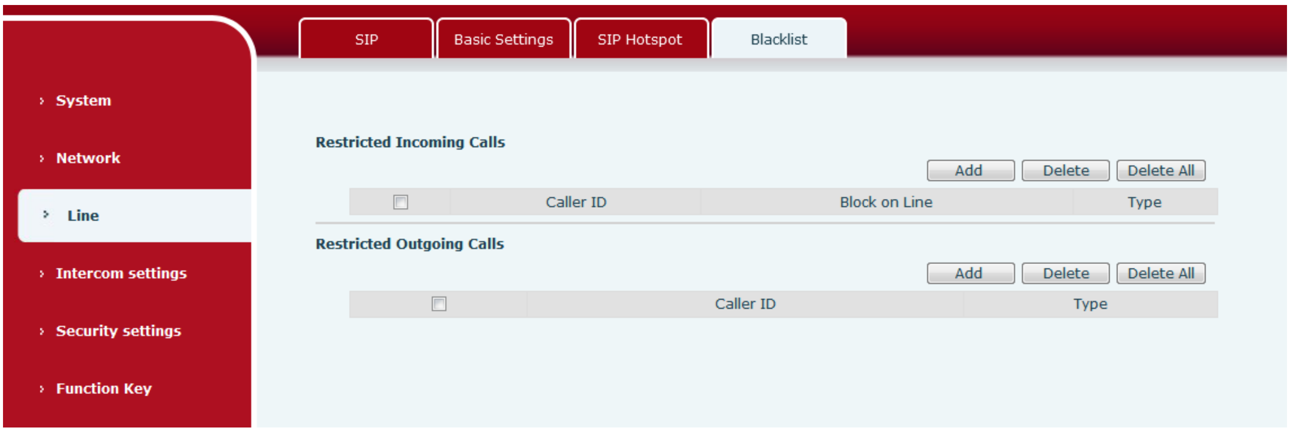
9.16 Intercom settings >> Blacklist

Web page to add call limit function, you can set the number or prefix to limit calls. The rules are as follows:

Add x, type number, x cannot call. Add x, type prefix, then the number beginning with x cannot call.

X could be a number or an IP. To add a whitelist rule, the number /IP should be preceded by a "-", followed by a ". ",

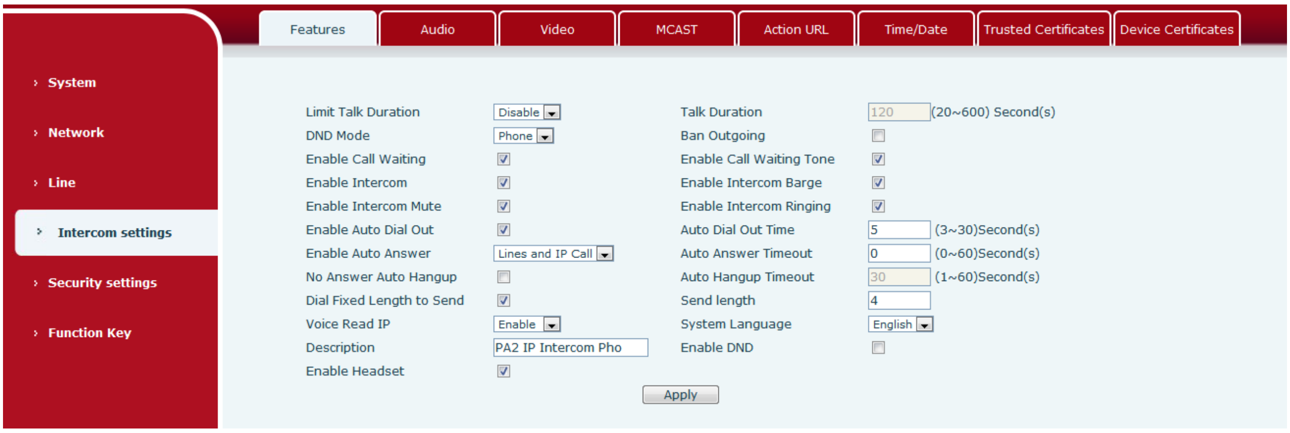
After addition, only the number in the whitelist is allowed to call, and the number outside the whitelist is refused.



Picture 29 - Blacklist

9.17 Intercom settings >> Features

Configure intercom Settings.



Picture 30 - Feature

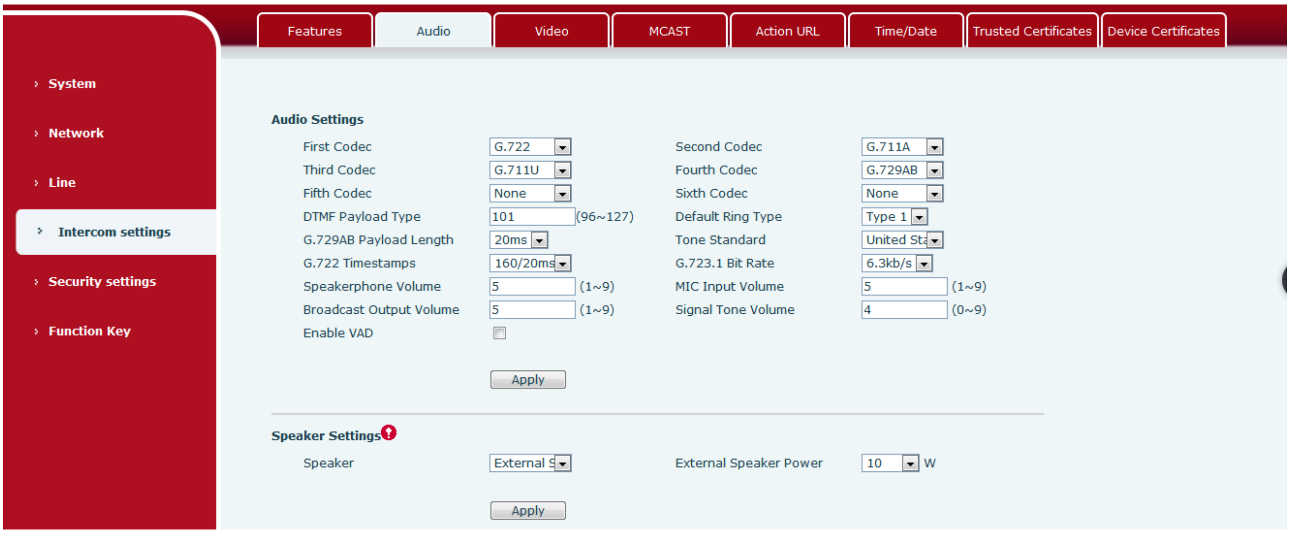
Table 13 - Common device function Settings on the web page

Features Setting	
Field Name	**Explanation**
Basic Settings	
Limit Talk Duration	If user enables the option, PA2 will hang up the call automatically while talk duration is achieved
Talk Duration	Time out to hang up
DND (Do Not Disturb)	DND might be disabled phone for all SIP lines, or line for SIP individually. But the outgoing calls will not be affected
Ban Outgoing	If enabled, no outgoing calls can be made.
Enable Call Waiting	The default value is enabled. Allow users to answer the second call while maintaining the call.
Enable Call Waiting Tone	The default value is enabled. When enabled, the call waiting tone can be heard while waiting for a call. If this function is turned off, when waiting for a call, the beep will not be heard.
Enable Intercom	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	Automatically answer calls in intercom mode during a call if the current call is intercom mode Type, refused to answer the new intercom mode
Enable Intercom Mute	If enabled, mutes incoming calls during an intercom call.
Enable Intercom Tone	If enabled, plays intercom ring tone to alert to an intercom call.
Enable Auto Dial Out	Enable Auto Dial Out when timeout.
Auto Dial Out Time	Configure waiting time for timeout dialing.
Enable Auto	Enable Auto Answer function

Answer	
Auto Answer Timeout	Set Auto Answer Timeout
Auto Hangup Timeout	Set the time of no answer auto hangs up.
Dial Fixed Length to Send	Configure to enable/disable fixed-length automatic dial-out numbers.
Voice Read IP	Turn on or off device voice broadcast IP address
System Language	Language for configuring voice prompts.
Description	Description information displayed on IP scan tool software or FDMS. The default is "PA2"
Enable Headset	Active speaker and SPK output when enabled, SPK only when off

9.18 Intercom Setting >> Audio

Change voice Settings



Picture 31 - Audio

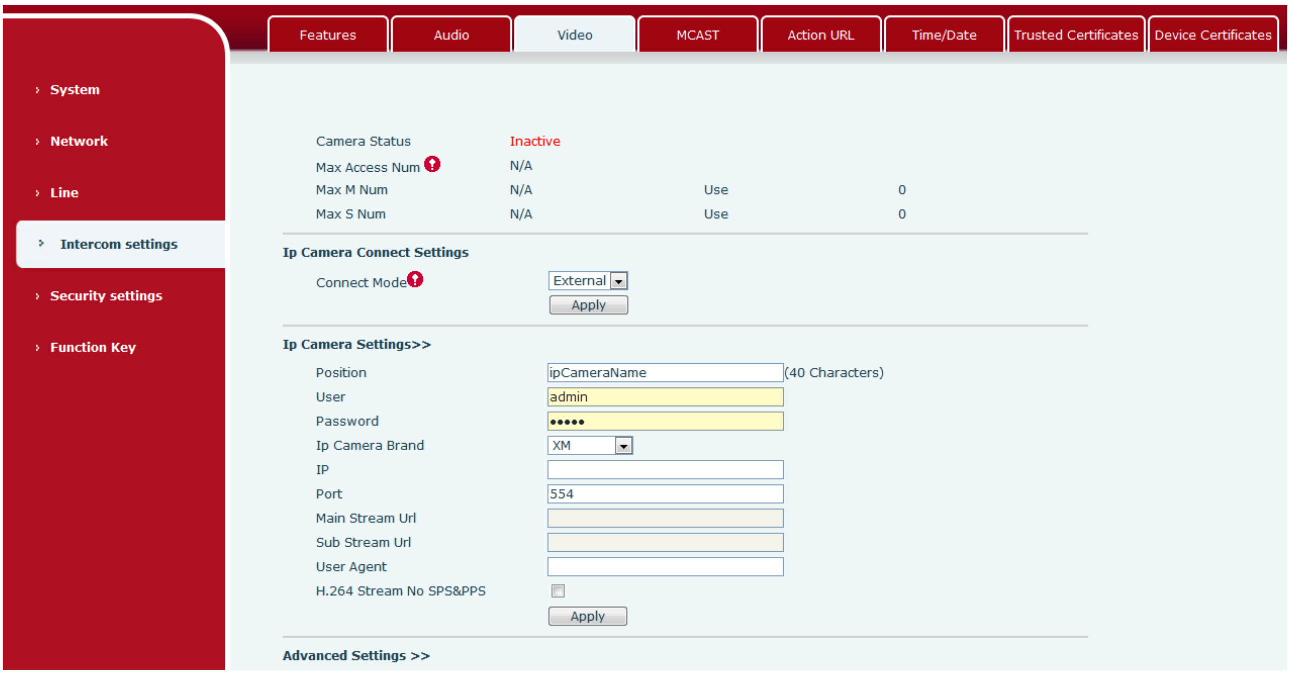
Table 1 - Voice Settings on web pages

Voice Settings	
Field Name	**Explanation**
First Codec	The first codec choice: G.711A/u, G.722， G.723, G.729， G.726-32
Second Codec	The second codec choice: G.711A/u, G.722， G.723, G.729， G.726-32
Third Codec	The third codec choice: G.711A/u, G.722， G.723, G.729， G.726-32
Fourth Codec	The forth codec choice: G.711A/u, G.722， G.723, G.729， G.726-32

Five Codec	The Five codec choice: G.711A/u, G.722， G.723, G.729， G.726-32
Six Codec	The Six codec choice: G.711A/u, G.722， G.723, G.729， G.726-32
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.
G.723.1 Bit Rate	Configure signal tone standard area.
G.722 Timestamps	Select a timestamp for the g. 722 encoding, optional 160/20ms,320/20ms；
G.723.1 Bit Rate	Select the rate of G723, optional5.3kb/s,6.3kb/s；
Speakerphone Volume	Configure speakerphone volume level
MIC Input Volume	Configure the call volume level for the microphone
Broadcast Output Volume	Configure the output volume level for broadcast
Signal Tone Volume	Configure the output volume level of the signal sound
Enable VAD	Mute detection; If VAD is enabled, the payload length of g.729 should not be greater than 20ms
Player Settings	
Player	The player has two modes of choice, panel speaker or external speaker. "Panel horn" means that both the speaker and the microphone are installed in the same shell and are mainly used for intercom. At this time, the sound effect of two-way intercom is required to be better. Therefore, the output power of the speaker needs to be optimized to ensure the sound effect of intercom. "External speaker" refers to the external speaker, microphone and speaker are separately deployed, at this time the broadcast sound requirements are larger
External speaker power	External speaker power can only be selected in the "external speaker" mode, 10W/20W/30W respectively. At this time, the impedance of the speaker used is 4 ohms. Note that the corresponding power supply is POE(or 12VDC)/18VDC/24VDC 2A power supply

AEC Settings	
AEC Settings	Provide adjustment parameter Settings for different power connection states
Sound Update/Delete	
Sound Update	Optional.wav suffix ring tone upgrade
Sound Delete	The upgraded ringtone is shown in the delete list and can be optionally deleted
Alert Info Ring Settings	
The value of notification information 1 to 10	Sets the value to specify the ringtone type
Ring Type	Type1-Type9

9.19 Intercom Setting >> Video



Picture 32 - Video Setting

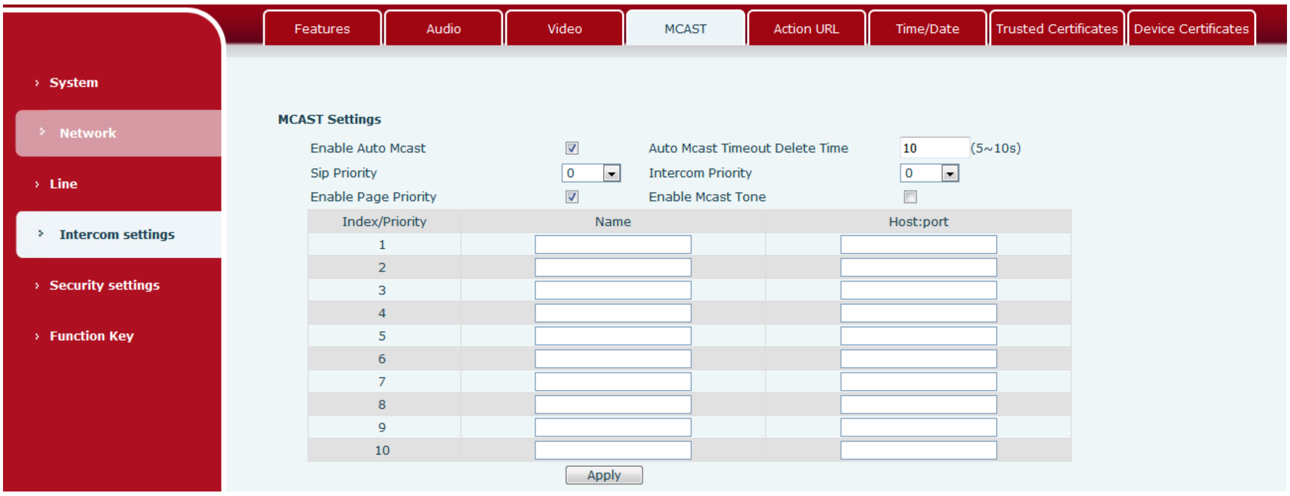
Table 14 - Video Setting

Connection Mode	Select external, click submit, and restart the device	
Camera Settings (external mode)		
Field Name	**Explanation**	

Name	Camera name
User name	External camera login name
Password	External camera login password
Camera type	Select camera manufacturer
IP address	Camera IP address, please use the camera matching scan tool to get the IP address
port	Camera port number
Main Stream Url	After user submit the camera information and apply the changes, if the device connects external camera successfully, the page will display the main stream URL directly, or the information is blank.
Sub Stream Url	After user submit the camera information and apply the changes, if the device connects external camera successfully, the page will display the sub stream URL directly, or the information is blank. If the IP camera user used is not in the list, and user select CUSTOMER as IP camera brand, he also need input the main stream URL manually.
No SPS&PPS h. 264 streams	Compatible with cameras without SPS&PPS can display video normally
Advanced Settings	
Video Direction	Sendonly: establish video call, and the SDP packet in the invite packet is Sendonly; Sendrecv: to create a call, the SDP package in the invite package is Sendrecv
RTSP Over TCP	The RTSP goes over the TCP protocol
H.264 Payload Type	Set the h. 264 Payload type. The range is between 96 and 127. The default is 117
Default Call Stream	Optional main stream and substream
RTSP Information	
Main Stream Url	Display the main stream URL address
Sub Stream Url	Display the sub stream URL address

9.20 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 sent by the multicast address.



Picture 33 - MCAST

Table 15 - MCAST parameters

Field Name	Explanation
Enable Auto Mcast	SIP Notify information is used to issue mcast configurations, after device receives the information, it can finish the configurations to listen the mcast or cancel mcast listening.
Auto Mcast Timeout Delete Time	When a multicast call does not end normally, but for some reason the device can no longer receive the multicast RTP packets, enable this option will make the device cancel listening after a specified period
SIP priority	Defines the priority in the current call, with 1 being the highest priority and 10 the lowest.
Broadcast priority	Compared with multicast and SIP priority, higher priority is pluggable and low priority is rejected
Enable Page Priority	Two multicasts, regardless of who first calls in, the device will accept the multicast with higher priority.
Multicast prompt tone	When enabled, play the prompt sound first when receiving multicast
Name	Listened multicast server name
Host: port	Listened multicast server’s multicast IP address and port.

9.21 Intercom Setting >> action URL

Picture 34 - Action URL

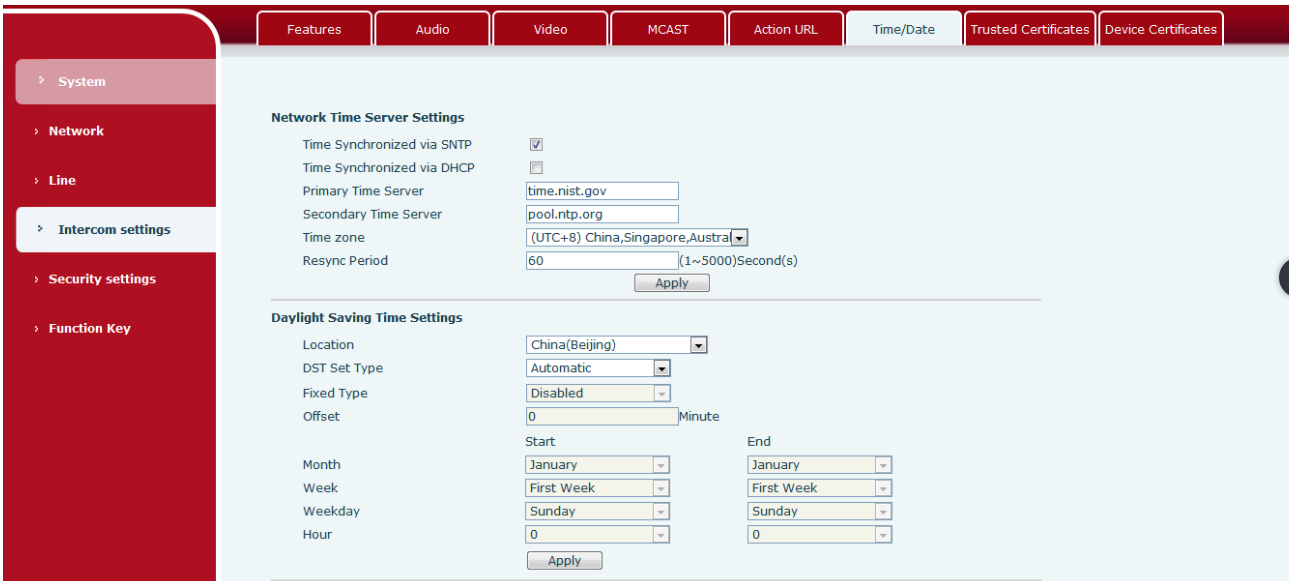
Table 16 - Action URL

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

Note! The operation URL is used by the IPPBX system to submit device events. Please refer to the details Fanvil Action URL。
http://www.fanvil.com/Uploads/Temp/download/20190122/5c46debfbde37.pdf

9.22 Intercom Setting >> Time/Date

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



Picture 35 - Time/Date

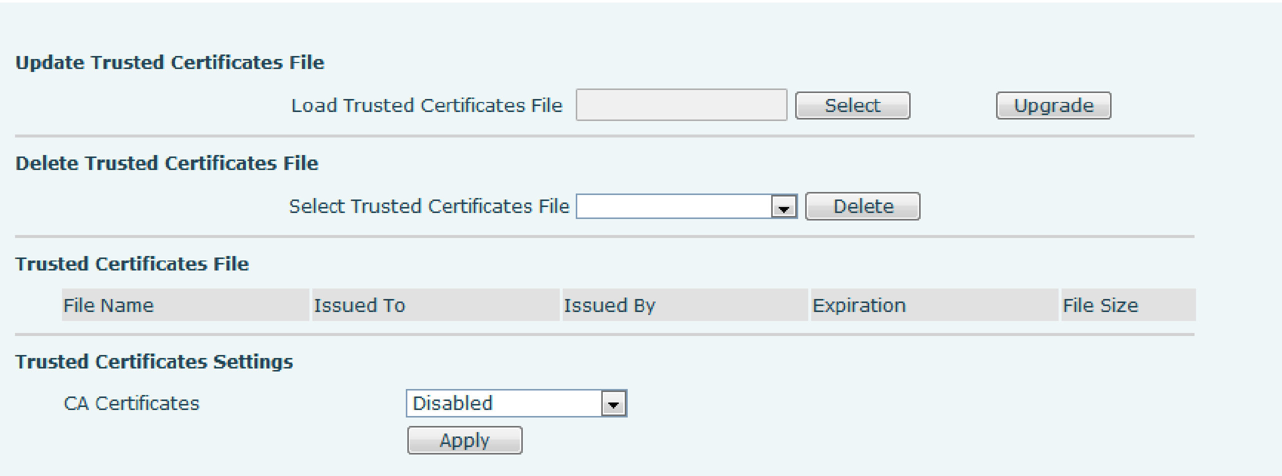
Table 17 - Time/Date

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 will try to connect to secondary time server to get time synchronization.
Time zone	Select the time zone
Resync Period	Time of re-synchronization with time server
Daylight Saving Time Settings	
Location	Select the user's time zone specific area
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)

9.23 Intercom Setting >> Trusted Certificates

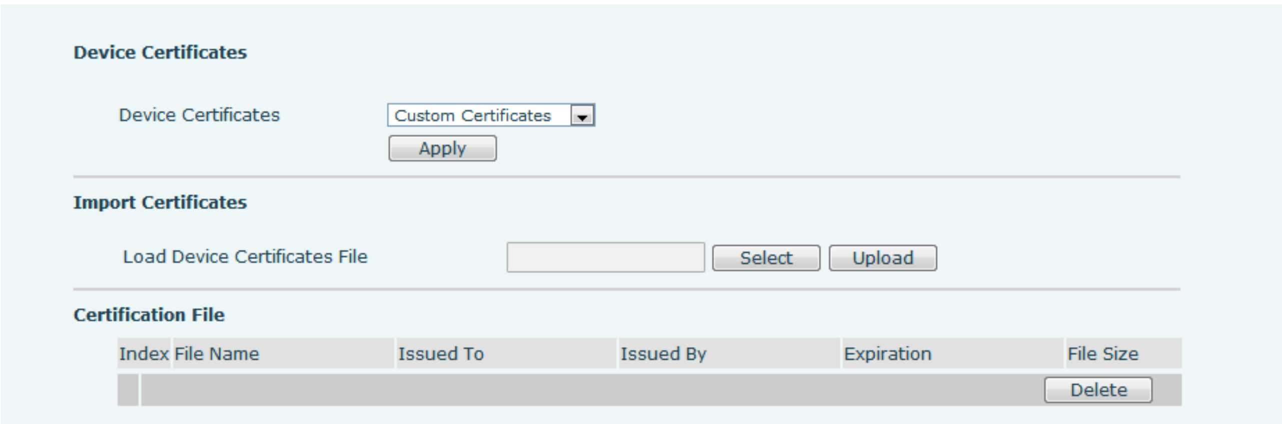
User can upload and delete the uploaded certificates in certificate management page.



Picture 36 - Trusted Certificates

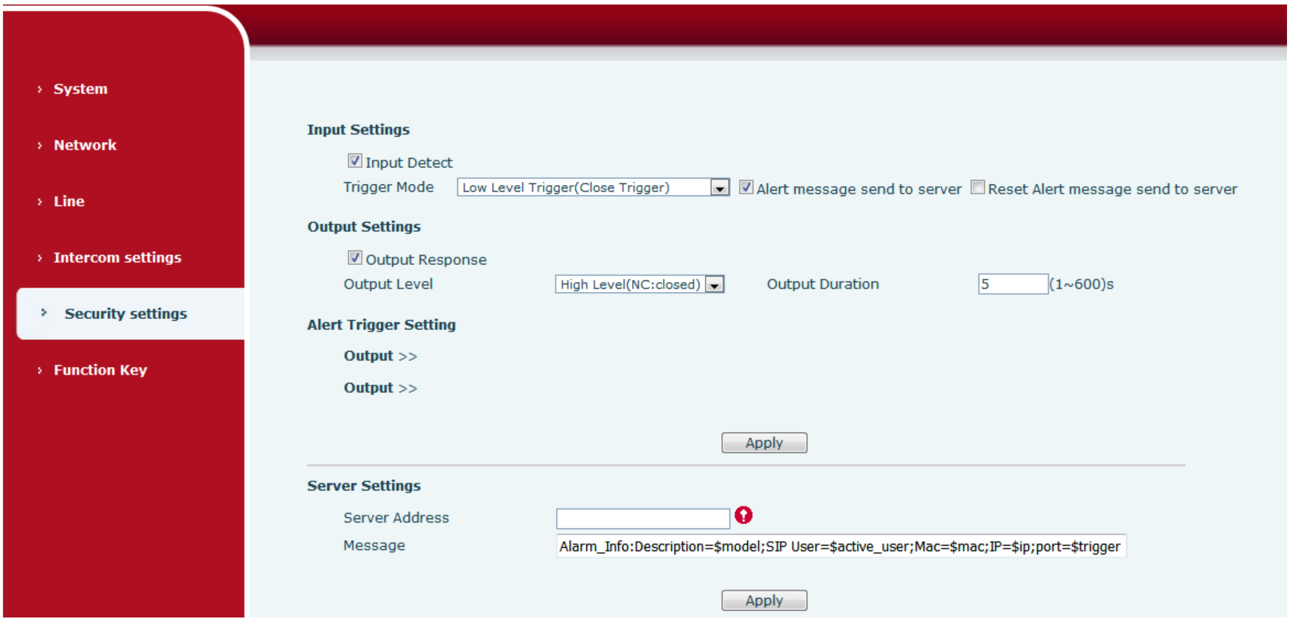
9.24 Intercom Setting >> Device Certificates

User can upload and delete the uploaded certificates for device in device certificates page.



Picture 37 - Trusted Certificates

9.25 Security Settings



Picture 38 - Alert/Security Settings

Table 18 - Alert/Security Settings

Security Settings	
Field Name	**Explanation**
Input settings	
Field Name	**Explanation**
Input Detect	Enable or disable Input Detect
Trigger Mode	When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger.
	When choosing the high level trigger (disconnected trigger), detect the input port (high level) disconnected trigger.
Alert message send to server	Set the Alert message send to server
Reset Alert message send to server	Enable or disable sending reset messages to the server
Output Settings	
Output Response	Enable or disable Output Response
Output Level	When choosing the low level trigger (NO: normally open), when meet the trigger

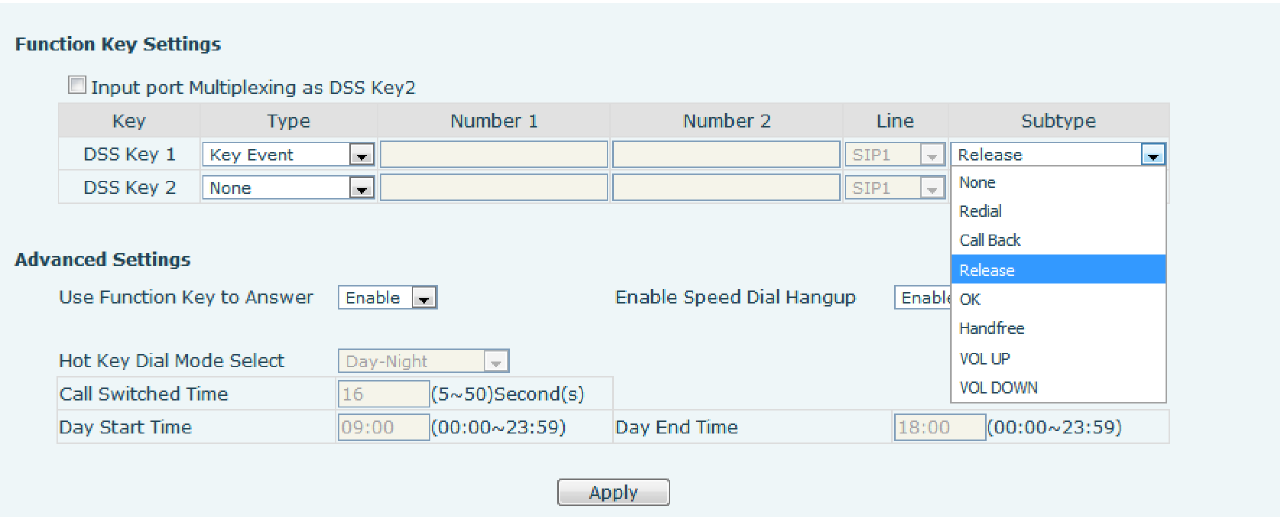
	condition, trigger the NO port disconnected.	
	When choosing the high level trigger (NC: normally close), when meet the trigger condition, trigger the NO port close.	
Output Duration	The duration of the changes in the output port, default value is 5 seconds.	
Alert Trigger Setting		
Input trigger	When the input port meets the trigger condition, the output port will be triggered (The trigger duration is controlled by option Output Duration.)	
DTMF output Duration	By duration	Port switch amount change time, press <output duration> control
	By Calling State	By call state control, after the end of the call, port to return the default state
Remote DTMF trigger	Receive the DTMF password sent by the remote device. If it is correct, trigger the corresponding output port. You can choose to enable or disable ringtones	
DTMF trigger code	During the call, the receiving terminal device sends a DTMF password, and if it is correct, the corresponding output port is triggered. The default is 1234.	
reset code	After receiving the corresponding instruction, the test device will reset the state and stop playing the corresponding ringtone	
Active Uri triggers	When device receives the active URI trigger message sent by the remote device and if it is correct, the corresponding output port will be triggered. You can choose to enable or disable ringtones.	
Trigger message	When the test device receives the right trigger message, the output port will be triggered.	
Reset message	When the test device receives the right reset message, the device will reset its status and stop playing the corresponding ringtone.	
Remote SMS trigger	Enable or disable remote SMS triggering. You can choose to enable or disable ringtones	
Trigger Message Alert	Send instructions on remote devices or servers, ALERT= [set instructions], if correct, trigger the corresponding port output.	
Call State Trigger	Continued triggering the output port by device’s call status. For example, When the call triggers the output port, the output will be triggered while the call status does not change. 1 Talking 2 Talking and Ringing 3 Ringing 4 Calling 5 Calling and Talking 6 Calling and Talking（dialing） 7 Calling and Ringing 8 Calling and Ringing(called ） 9 Calling, Ringing and Talking	

Server Settings	
Server Address	Send message to the server when the alarm is triggered. Message format：Alarm Info: Description=PA2;SIP User=;Mac=00:a8:34:68:23:d1;IP=172.18.90.235;port=Input1

9.26 Function Key >> Function Key Settings

➢ Key Event

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



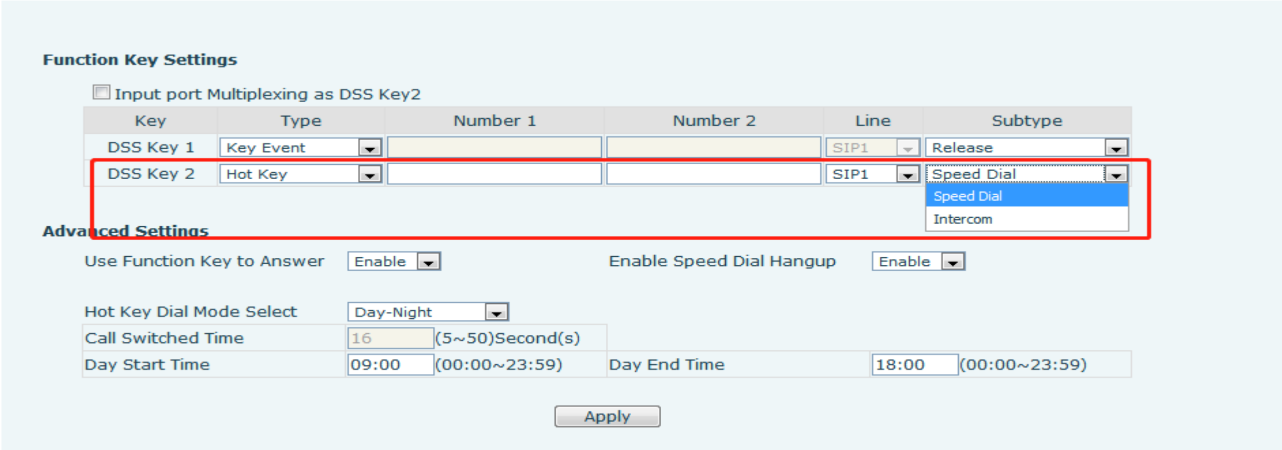
Picture 39 - Function Key Settings

Table 19 - Function Key Settings

Type	**Subtype**	**Usage**
Key Event	None	No responding
	Release	Delete password input, cancel dialing input and end call
	OK	Confirm key
	Call Back	The user can redial the last number dialed
	Redial	Call the nearest missed number
	Handfree	Use as a hands-free button
	VOL UP	Turn up volume
	VOL DOWN	Turn down volume

➢ Hot Key

When the speed dial key is set as Hot Key, the device will dial pre-set telephone number. The number option can also be configured with IP address. User can press the speed dial button to make direct IP call.



Picture 40 - Hot Key Settings

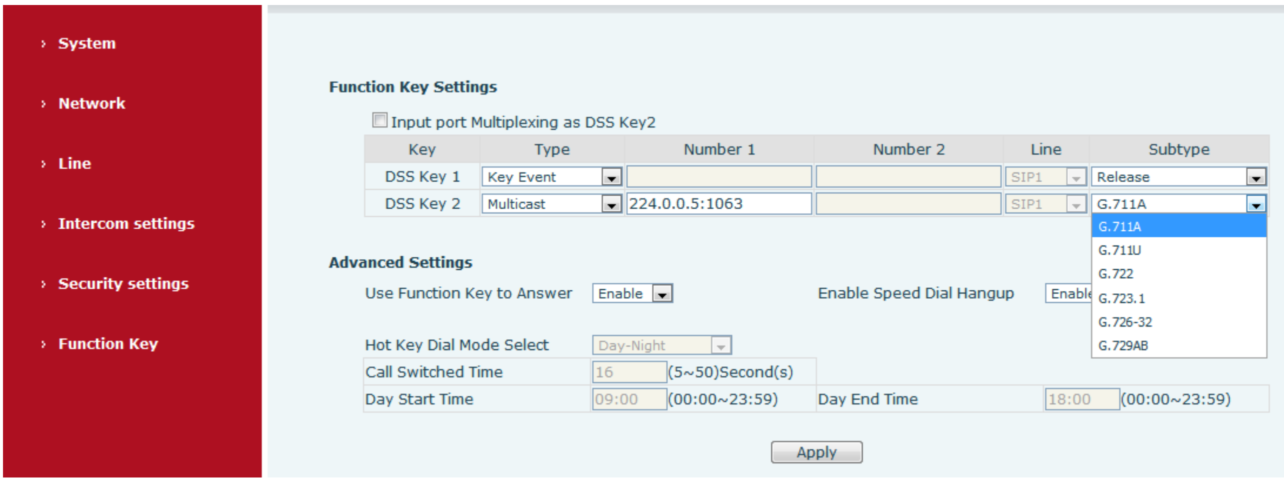
Table 20 - Hot Key Settings

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

➢ Multicast

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

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



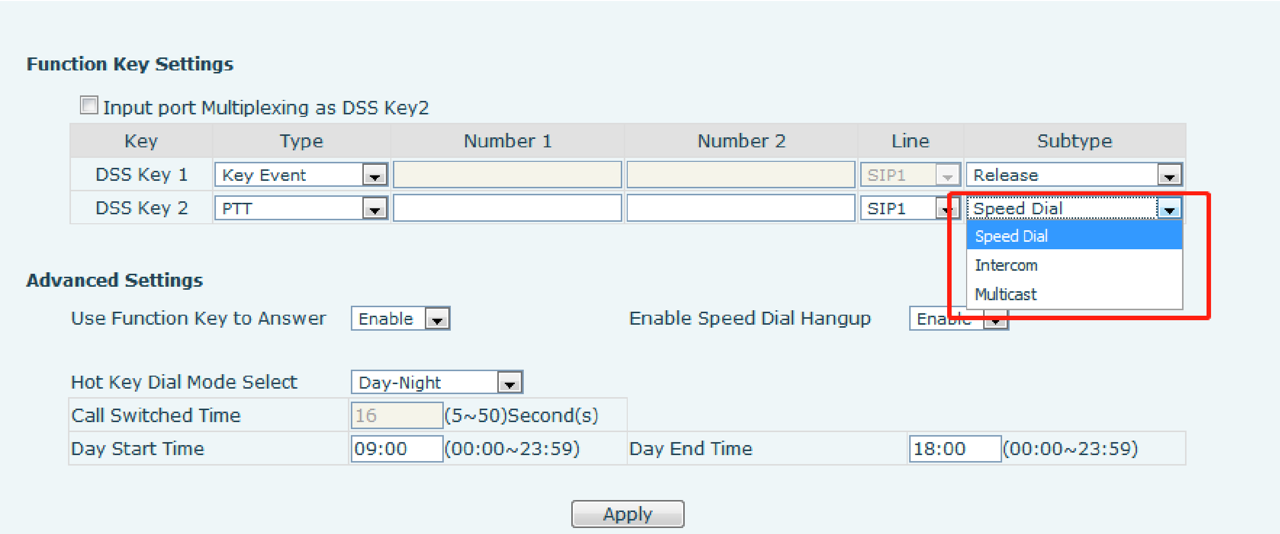
Picture 41 - Multicast Settings

Table 21 - Multicast Settings

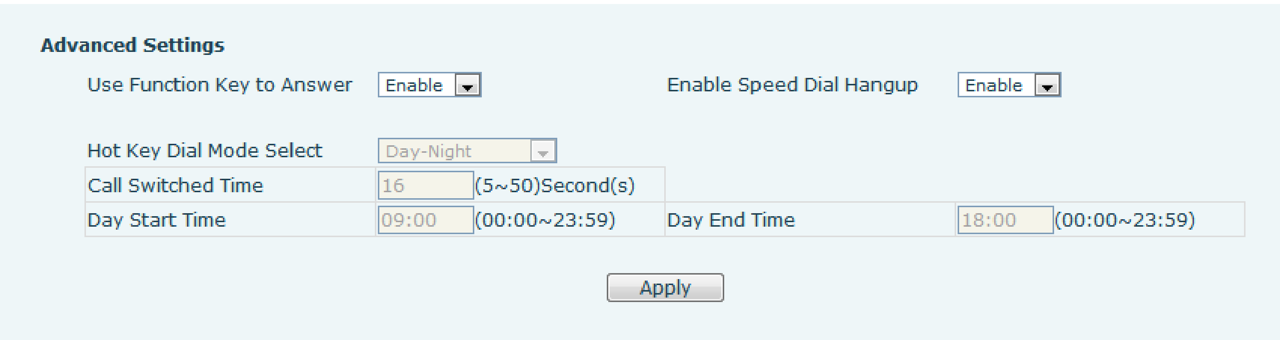
Type	Number	Subtype	Usage
Multicast	Set the host IP address and port number, they must be separated by a colon (The IP address range is 224.0.0.0 to 239.255.255.255, and the port number is preferably set between 1024 and 65535)	G.711A	Narrowband speech coding (4Khz)
		G.711U	
		G.722	Wideband speech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

➢ PTT

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



➢ Advanced Settings



Picture 42 - Advanced Settings

Table 22 - Advanced Settings

Advanced Settings	
Field Name	**Explanation**
Input port is multiplexed as function key 2	Enable or disable the input port to be multiplexed as speed dial button 2

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

10 Trouble Shooting

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 Fanvil technical support mailbox.

10.1 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.

10.2 Reboot device

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

10.3 Device factory reset

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

To restore the factory settings, you need to log in to the webpage [**System**] >> [**Configuration**], and click [**Reset**] button, the device will return to the factory default state.

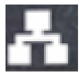
10.4 Network Packets Capture

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

10.5 Common Trouble Cases

Table 2 - Common Trouble Cases

Trouble Case	**Solution**
Device could not boot up	1. If the device enters "POST mode" (the SIP/NET and function button indicators are always on), the device system is damaged. Please

	contact your location technical support to help you restore your equipment system. 2. If the device enters "POST mode" (the SIP/NET and function button indicators are always on), the device system is damaged. Please contact your 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. The network cable must b**e co**nnected to the  [Network] interface instead of the [Camera] interface. 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 follow the instructions in "10.4 Network Data Capture" to obtain a registered network packet and send it to the Fanvil Support Email to help analyze the issue.