FH-S01
User Manual

Software Version: 1.0.0

Release Date：2022.8.24

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 designed for indoor environment. 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.
- Before using the product, please confirm that the temperature and humidity of the environment meet the working requirements of the product.
- 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

FH-S01 is a SIP ceiling speaker featuring paging, multicasting, broadcasting and talkback functionalities. It supports up to 10 multicast zones with prioritization.

It delivers high-intelligibility performance with G.722&Opus codecs. Adopted standard SIP 2.0(RFC3261) and related RFC protocols, it has strong compatibility and scalability.

FH-S01 has a built-in microphone, which supports monitoring and intercom applications. At the same time, Audio power up to 15W with built-in class D amplifier; Support customize the WAV file for emergency notification and alarm; It has the function of linkage security alarm equipment, and Support remote configuration via web page and auto-provisioning; It has 100M Ethernet and can adapt to 10/100 Mbps Ethernet, Integrated PoE(IEEE 802.3af, class 0),Ideal for school, office, station, retail, factory, etcetc.

.

5 Install Guide

5.1 Use POE or external Power Adapter

FH-S01, 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, FH-S01 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 Appendix

5.2.1 LED Status

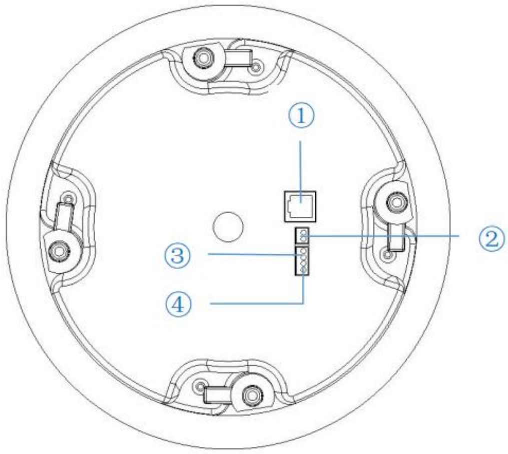
Table 1 - LED Status

Type	Status	description
Status Light	Ring	When the call is ringing, the LED light will flash slowly. It supports four states: ON、OFF、Fastblink and Slowblink . Default Slowblink, settable
	In Using	The display status of the LED light in the call or dialing status. It supports four states: ON、OFF、Fastblink and Slowblink . Default OFF, settable
	Network Abnormal	When the network is in an abnormal

Type	Status	description
		state, the indicator flashes once every second. It supports four states: ON、OFF、 Fastblink and Slowblink . Default Fastblink, settable
	SIP Register Success	SIP registered successfully in normal standby state.The device supports four states: ON、 OFF、 Fastblink and Slowblink ,Default OFF, settable
	SIP Register Fail	When the SIP registration fails, the LED light flashes once every second. It supports four states: ON、OFF、Fastblink and Slowblink. Default Fastblink, settable

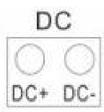
6 User Guide

6. 1 Interface description



Picture 1 - Interface display

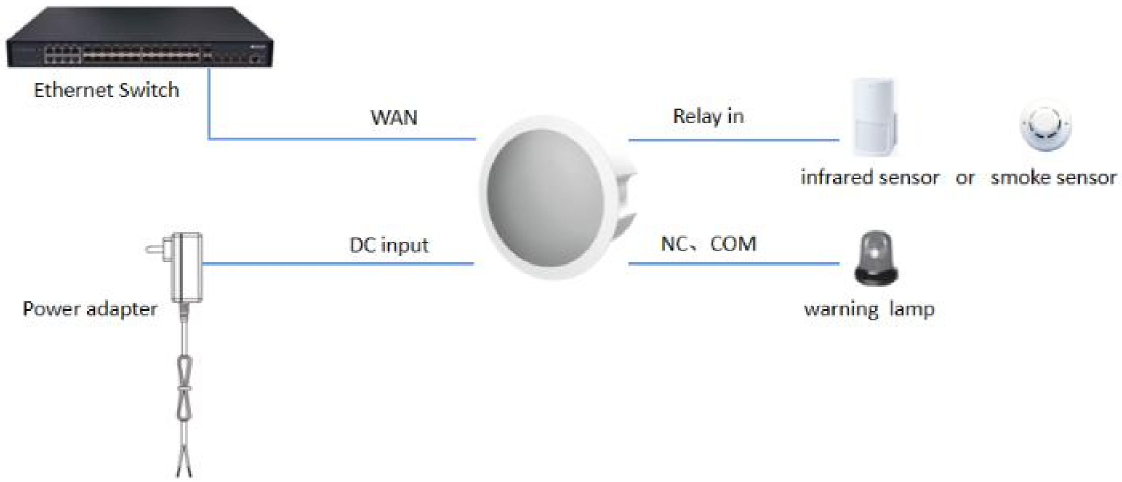
Table 2 - Interface description

Number	Name	Description	
①	Ethernet interface	standard RJ45 interface, 10/100M adaptive, support PoE powered, it is recommended to use CAT5 or CAT5E network cable.	
②	Power interface	18V/2A input	
③	1 set of short-circuit input interface	input devices for connecting switches, infrared sensor, door sensor, vibration sensors etc.	
④	1 set of short-circuit output interface	corresponding to the short-circuit input interface, login device web page settings, can be connected to electric alarms etc	

6. 2 Installation instructions

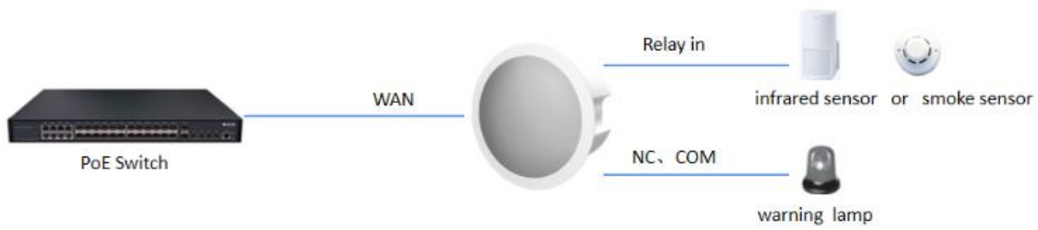
6.2.1 Peripheral connection

DC power supply connection mode:



Picture 2 - DC power supply peripheral connection mode

POE power supply connection mode:



Picture 3 - POE power supply peripheral connection mode

6.2.2 Installation Method

The device supports ceiling type installation

- Ceiling Installation

Step 1: Make a circular hole on the pre installation position of the ceiling that can accommodate the cylinder at the back end of the ceiling speaker.

Step 2: Turn out the four buckles of the ceiling speaker and press down to eject the net cover.

Step 3: Turn back the buckle, insert the Ceiling Speaker into the ceiling from the round hole drilled before, turn out the buckle, press the back of the ceiling, and tighten the screws corresponding to the buckle.

Step 4: Reinstall the speaker net cover and complete the installation.

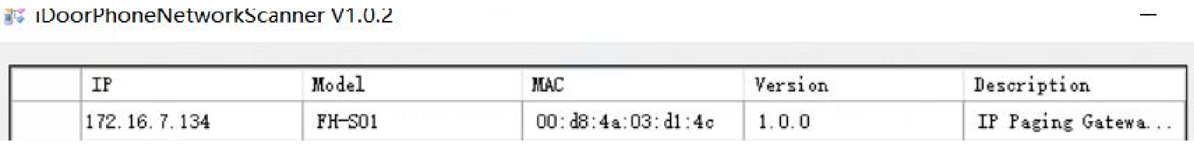
Step 5: If other input/output devices need to be connected externally, connect to the host through the connecting tail line.

Step 6: Power on test, plug in the Internet cable and power supply, and the indicator light of the equipment is on, indicating that the power supply is connected normally.

6.2.3 Device IP address

Open the web page and enter http://download.fanvil.com/tool/iDoorPhoneNetworkScanner.exe to download and install the IP scanning tool.

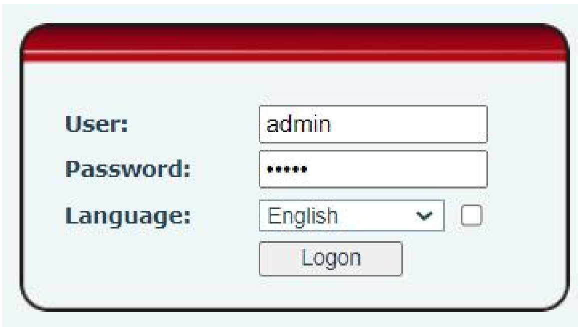
Open the IP scanning tool, click the refresh button, search for the device and find the corresponding IP address.


iDoorPhoneNetworkScanner V1.0.2

	IP	Model	MAC	Version	Description
	172.16.7.134	FH-S01	00:d8:4a:03:d1:4c	1.0.0	IP Paging Gatewa...

6.3 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

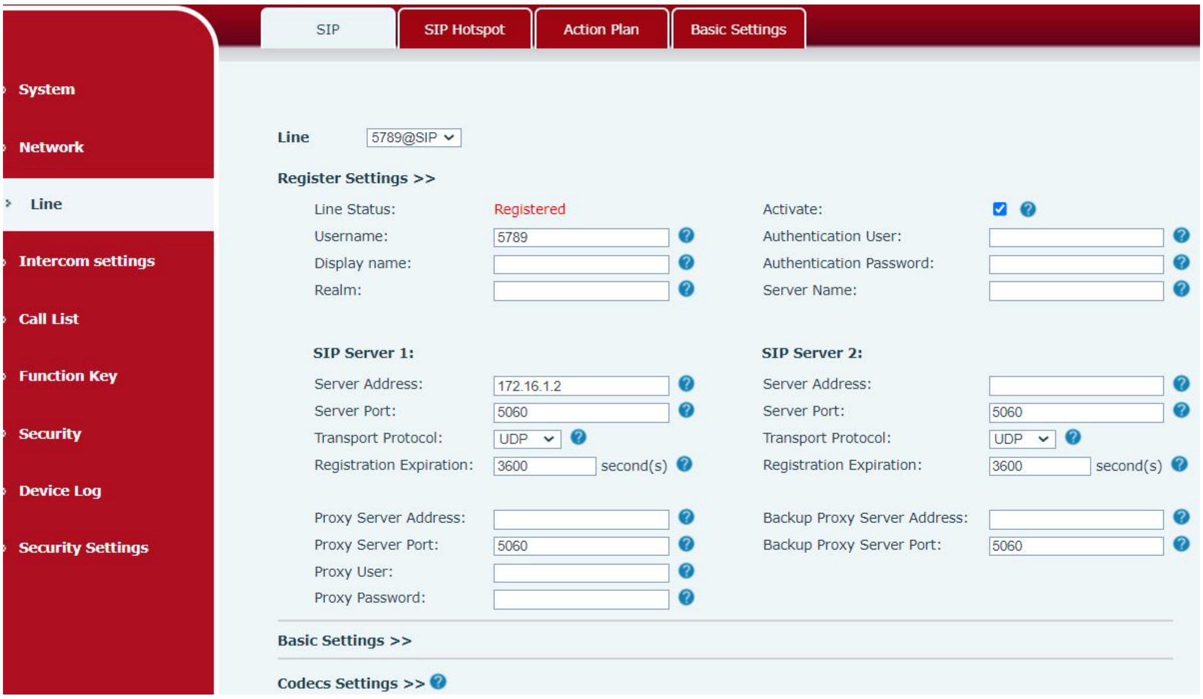
The username and password should be correct to log in to the web page. **The default username and password are "admin"**. For the specific details of the operation of the web page, please refer to 9 Web Configurations

6.4 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:



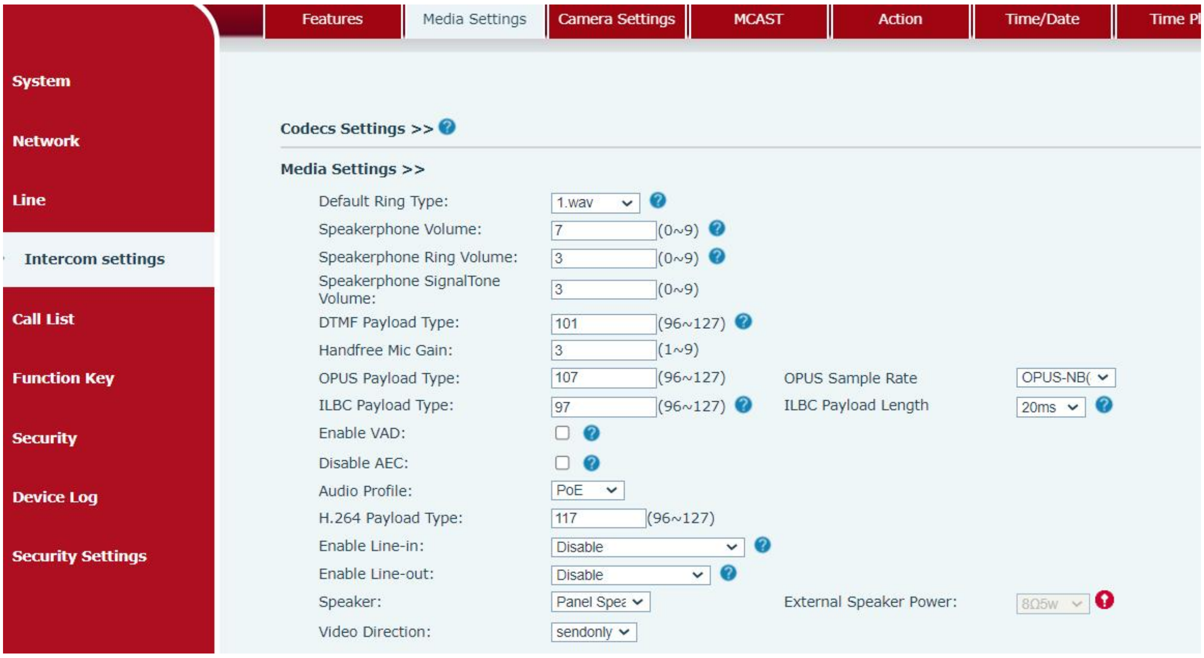
Picture 5 - SIP Line Configuration

6. 5 Volume setting

[Intercom Settings] >> **[Media Settings]** >> **[Media Settings]**, as shown below, click **[Submit].**

Hands-free volume setting: Set the speaker output volume.

Hands-free microphone gain: microphone volume level.



Picture 6 - Volume Set

7 Basic Function

7. 1 Answering Calls

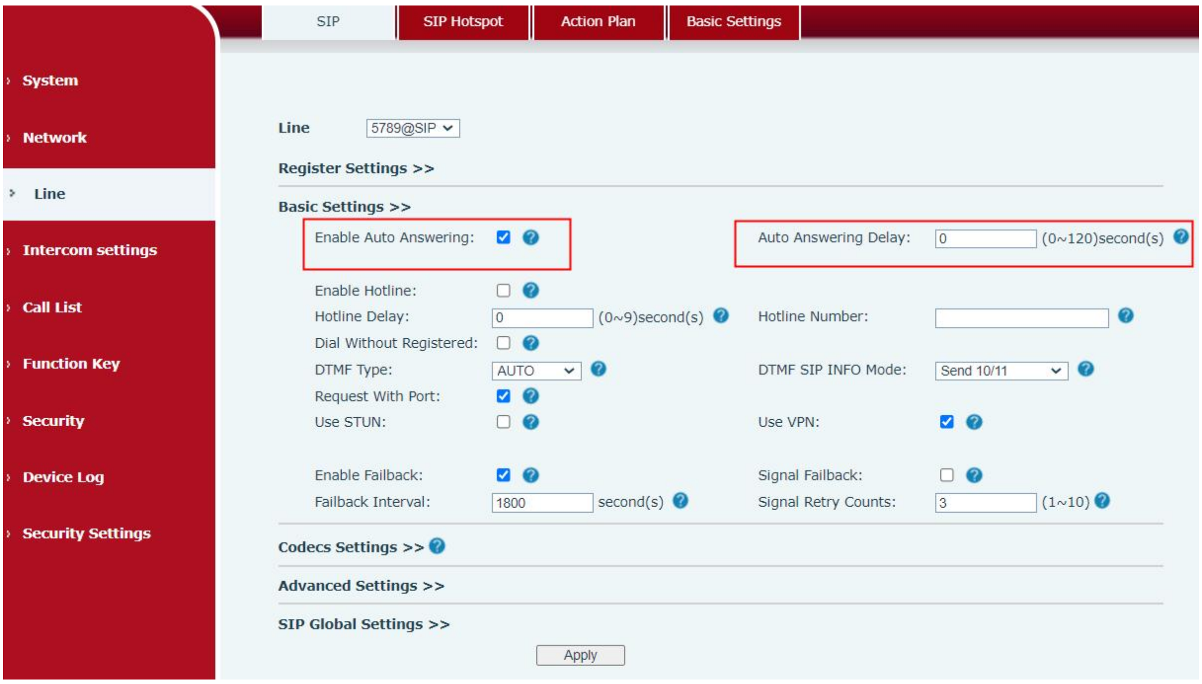
After setting up the automatic answer and setting up the automatic answer time, it will hear the ringing bell within the set time and automatically answer the call after timeout. Cancel automatic answering. When a call comes in, you will hear the ringing bell and will not answer the phone over time.

7.2 Auto Answer

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

- **Web interface:**

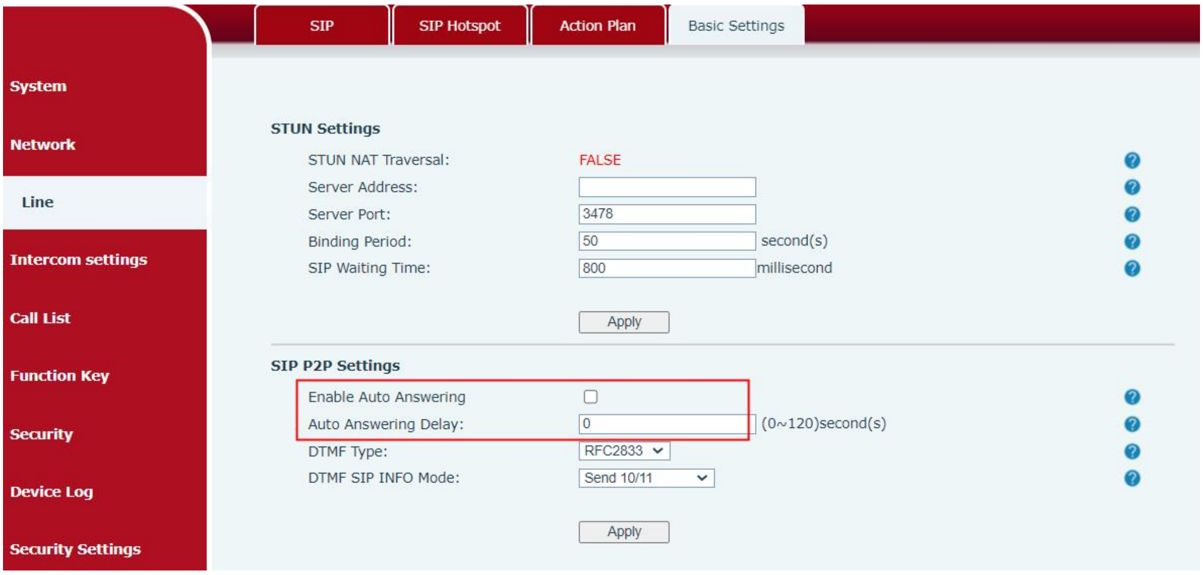
Enter [**Line**] >> [**SIP**]>>【**Basic Settings**】, Enable auto answer and set auto answer time and click submit.



Picture 7 - WEB line enable auto answer

- SIP P2P auto answering:

Enter [**Line**]>>[**Basic settings**]>>【SIP P2P Settings】,Enable auto answer and set auto answer time and click submit.



Picture 8 - Enable auto answer for IP calls

- Auto Answer Timeout（0~120）

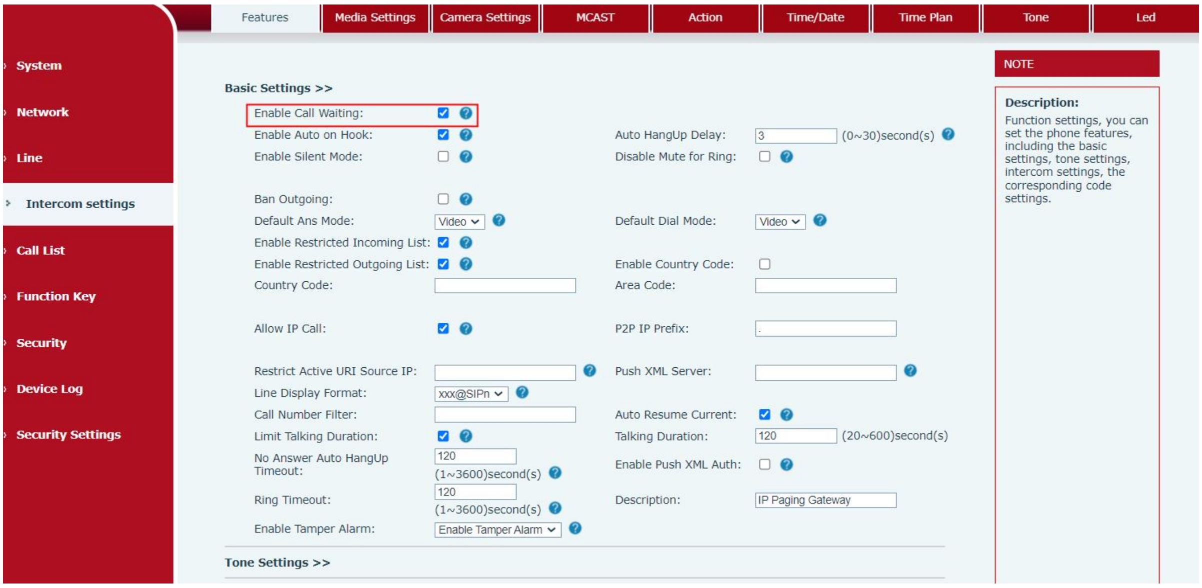
The range can be set to 0~120s, and the call will be answered automatically when the timeout is set.

7. 3 Call Waiting

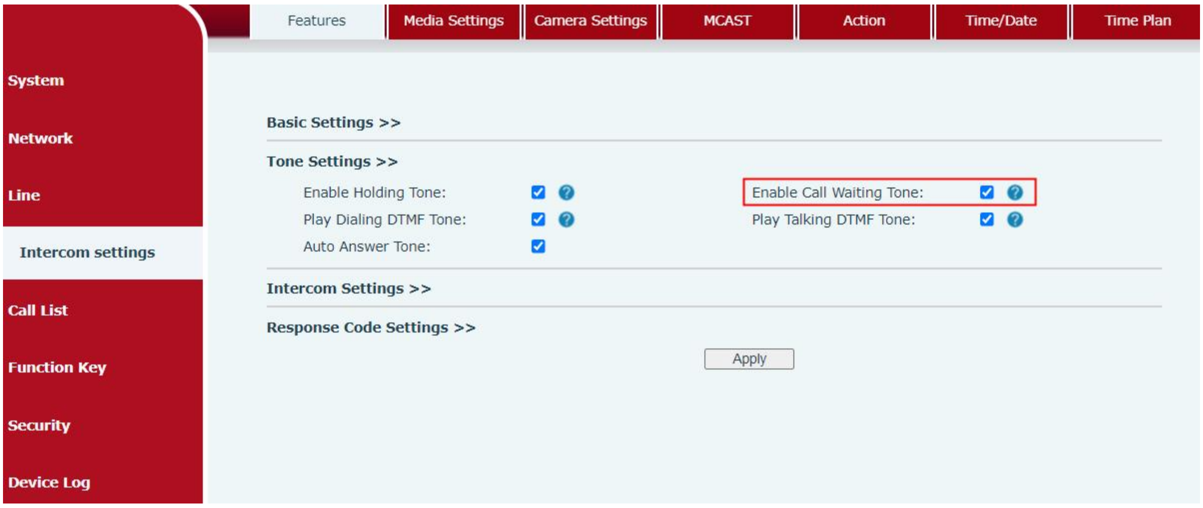
- Enable call waiting: new calls can be accepted during a call.
- Disable call waiting: new calls will be automatically rejected and a busy signal will be prompted
- Enable call waiting tone: when you receive a new call on the line, the device will beep.

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 9 - Call Waiting

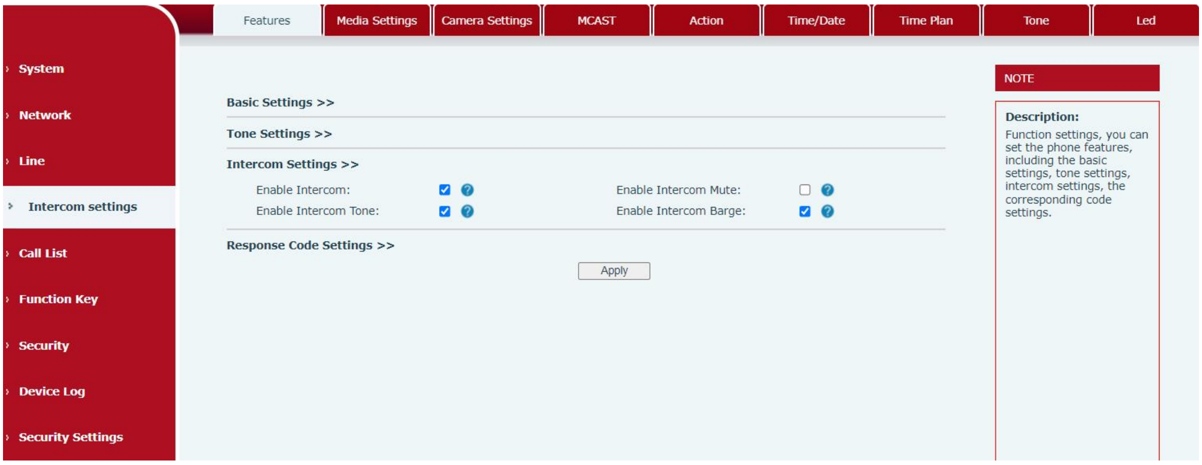


Picture 10 - Call Waiting tone

8 Advance Function

8. 1 Intercom

The device can answer intercom calls automatically.



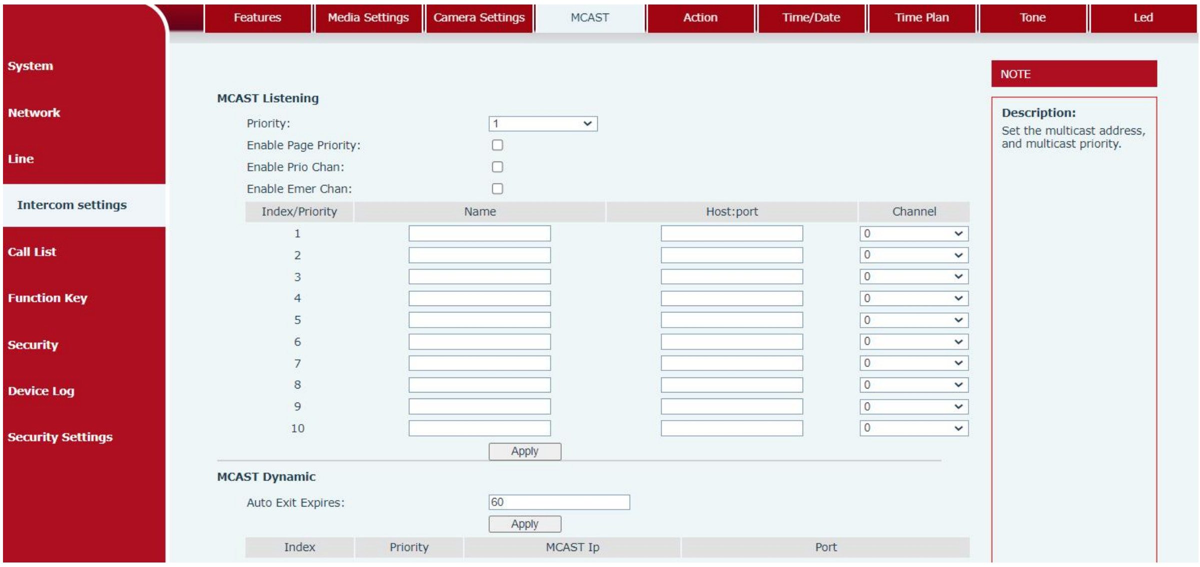
Picture 11 - WEB Intercom Settings

Table 3 - Intercom description

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, PA3 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.



Picture 12 - MCAST Setting

Table 4 - MCAST parameter

Parameters	**Description**
Priority	Defines the priority in the current call, with 1 being the highest priority and 10 the lowest.
Enable Page Priority	Compared with multicast and SIP priority, high priority is pluggable and low priority is rejected.
Enable Prio Priority	When enabled, the same port and channel can be connected. Channel 24 is a priority channel, higher than 1-23; A channel of 0 indicates that the channel is not used.
Enable Emer Chan	When enabled, channel 25 has the highest priority
Name	Name of the server listening to multicast
Host:port	Server address listening to multicast: port
Channel	0-25 (24 priority channels, 25 emergency channels)

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.

MCAST Dynamic：

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

8.3 Hotspot

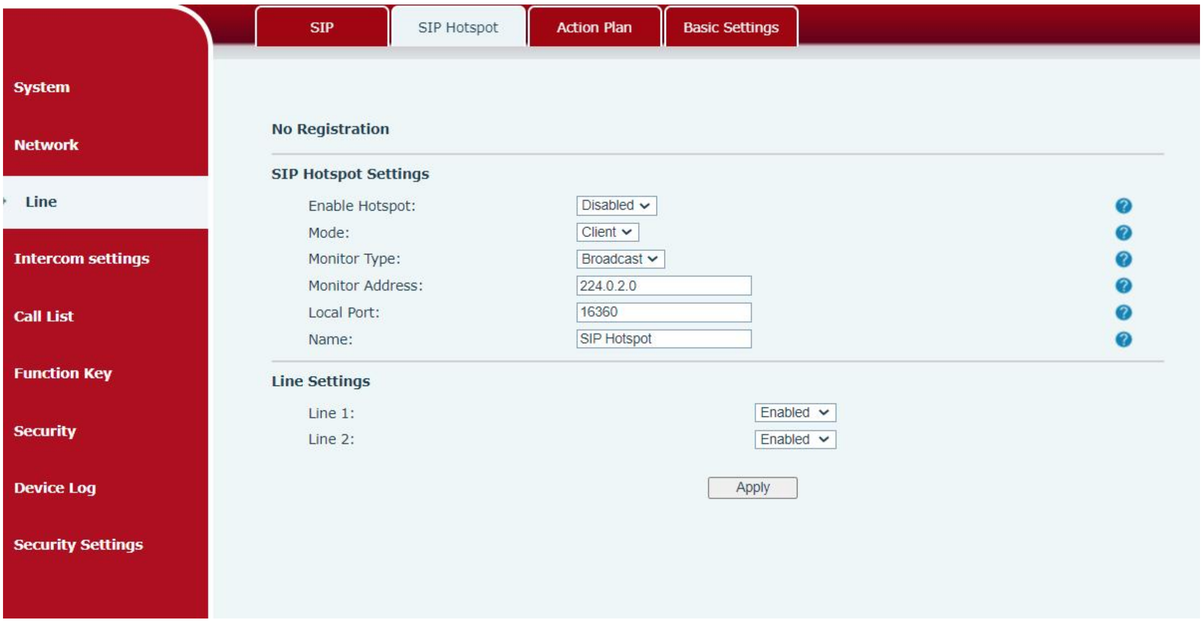
SIP hotspot is a simple utility. Its configuration is simple, which can realize the function of group vibration and expand thequantity of sip account. Take one device A as the SIP hotspot and the other devices (B, C) as the SIP hotspot client. When someone calls device A, devices A, B, and C will ring, 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 5 - 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 13 - 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

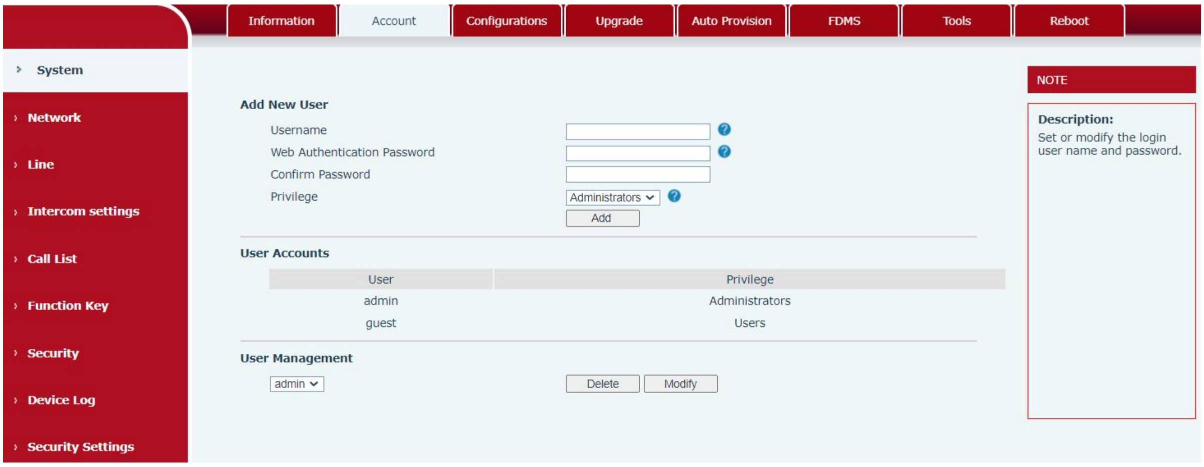
And summarization of network status,

- 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

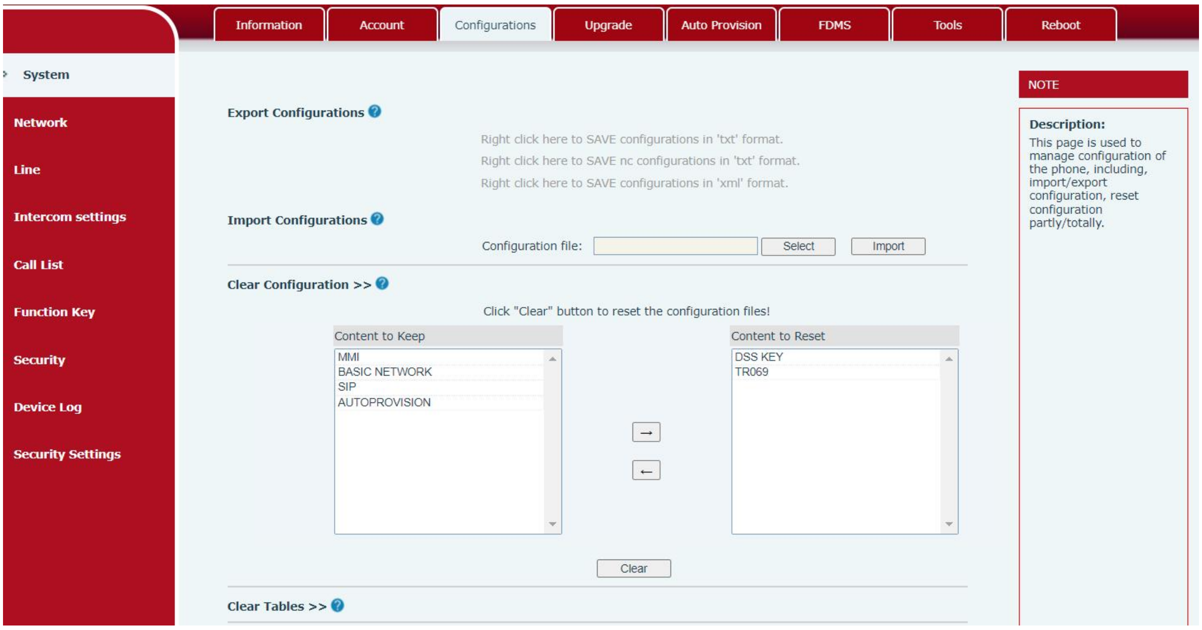


Picture 14 - WEB Account

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 15 - 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

- **Clear Configurations**

  Select the module in the configuration file to clear.

  SIP: account configuration.

  AUTOPROVISION: automatically upgrades the configuration

  TR069:TR069 related configuration

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

  DSS Key: DSS Key configuration

  Basic Network

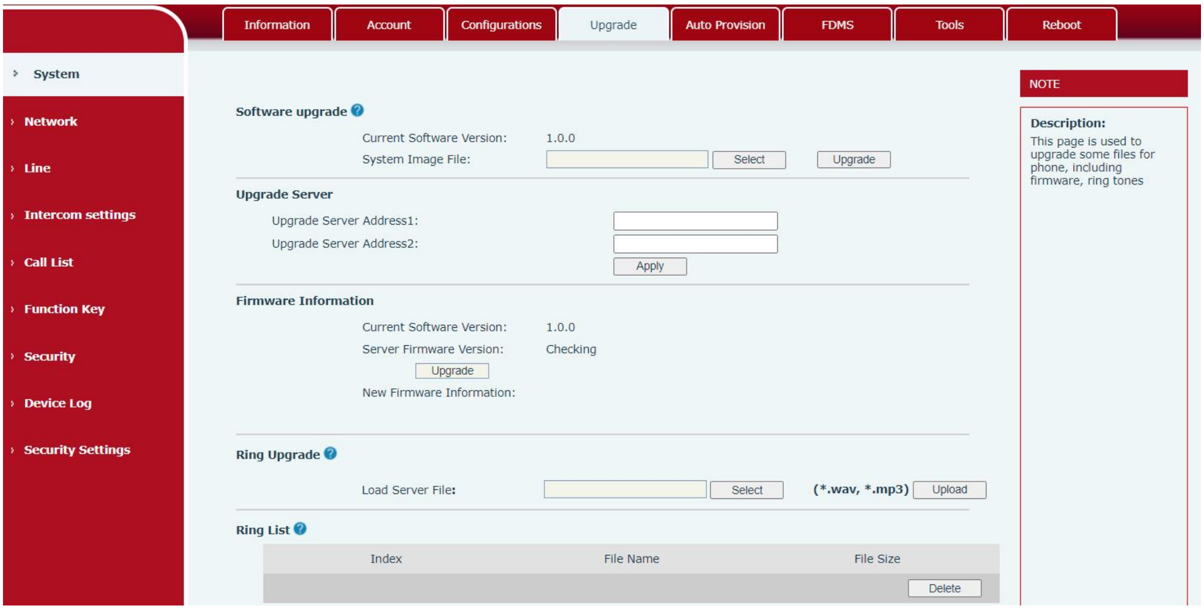
- **Clear Tables**

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

- **Reset Phone**

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

9. 5 System >> Upgrade



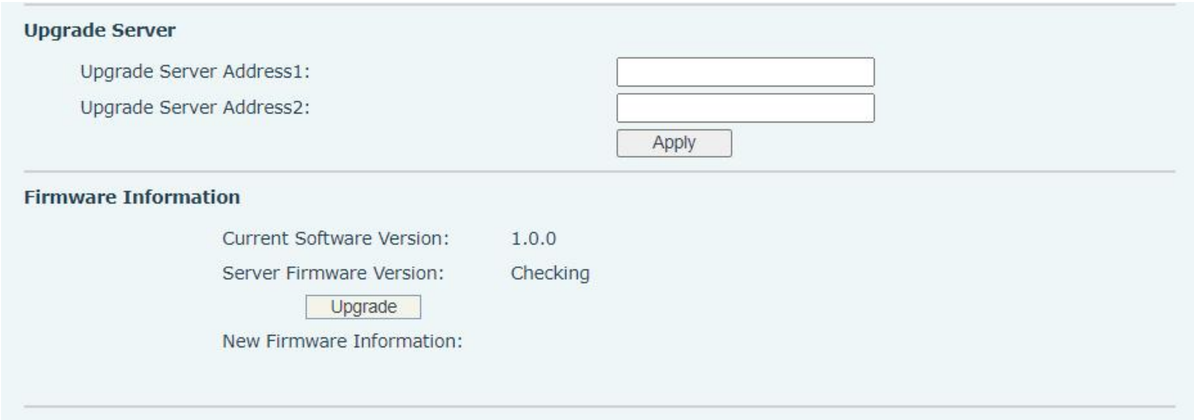
Picture 16 - Upgrade Settings

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.

Upgrade the ringtone,support wav and MP3 format.

Firmware Upgrade:

Firmware online upgrade means that the device sends an HTTP request to the server, and the server returns the corresponding description file or 404 or timeout. After receiving it, the device parses the version description file and prompts the user whether to upgrade the new version



Picture 17 - Online upgrade settings

Table 6 - Firmware upgrade

Parameter	Description
Upgrade server	
Enable Auto Upgrade	Enable automatic upgrade, If there is a new version txt and new software firmware on the server, phone will show a prompt upgrade message after Update Interval.
Upgrade Server Address1	Set available upgrade server address.
Upgrade Server Address2	Set available upgrade server address.
Update Interval	Set Update Interval.
Firmware Information	
Current Software Version	It will show Current Software Version.
Server Firmware Version	It will show Server Firmware Version.
[Upgrade] button	If there is a new version txt and new software firmware on the server, the page will display version information and upgrade button will become available; Click [Upgrade] button to upgrade the new firmware.
New version description information	When there is a corresponding TXT file and version on the server side, the TXT and version information will be displayed under the new version description information.

- 设备向服务器请求的文件为 TXT 文件，文件名称为 vendor_model_hw1_0.txt。hw 后面是硬件版本号。文件名中有空格全部改为下划线。
- The file requested from the server is a TXT file called vendor_model_hw10.txt.hw followed by the hardware version number, it will be written as hw10 if no difference on hardware. All

Spaces in the filename are replaced by underline.

- The URL requested by the phone is HTTP:// server address/vendor_Model_hw10.txt：The new version and the requested file should be placed in the download directory of the HTTP serve。
- TXT file format must be UTF-8
- vendor_model_hw10.TXT The file format is as follows：

Version=1.6.3 #Firmware version

Firmware=xxx/xxx.z #URL,Relative paths are supported and absolute paths are possible, distinguished by the presence of protocol headers.

BuildTime=2018.09.11 20:00

Info=TXT|XML

Xxxxx

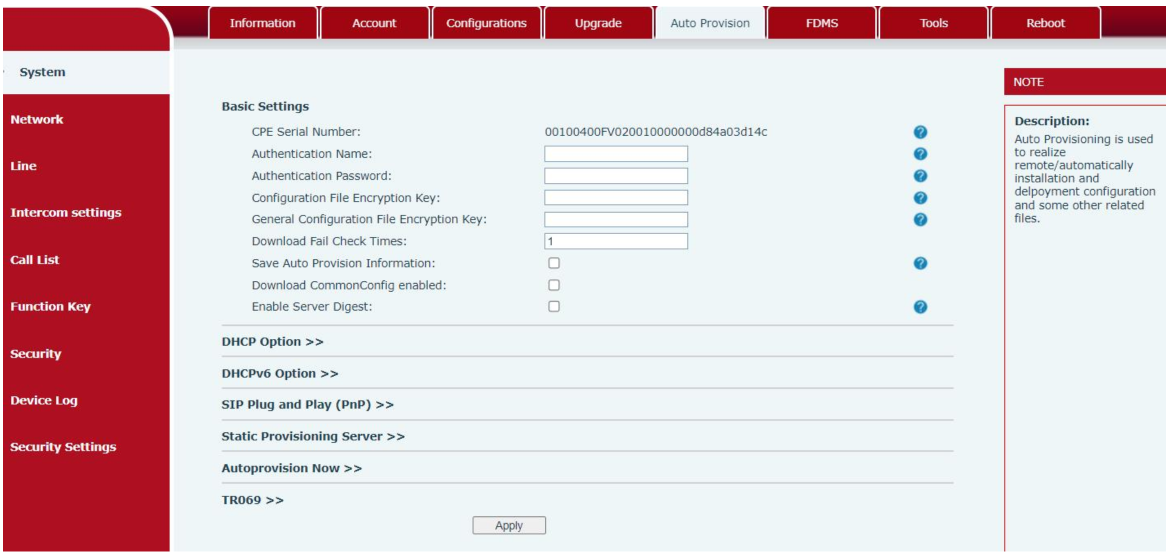
Xxxxx

Xxxxx

Xxxxx

9. 6 System >> Auto Provision

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



Picture 18 - Auto provision Settings

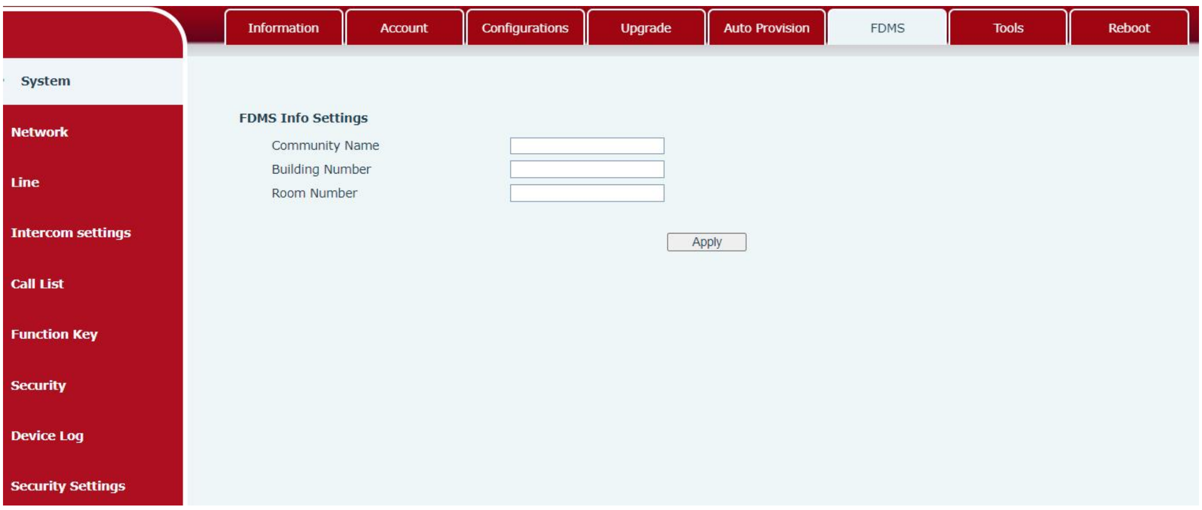
The azimuth terminal supports SIP plug and play, DHCP selection parameters, static deployment server and TR069 to obtain automatic deployment application . parameters.Transferring protocol: FTP、 TFTP、 HTTP、 HTTPS

Table 7 - Auto provision Settings

Auto provision	
Parameters	**Description**
Basic settings	
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 Server Digest	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)
TLS Version	TLS Version,Valid Value:TLS1.0/1.1/1.2.
INFORM Sending Period	TR069 message cycle.Valid Value:1~9999 seconds.
STUN Server address	Enter the STUN address
Enable the STUN	Enable the STUN

9.7 System >> FDMS



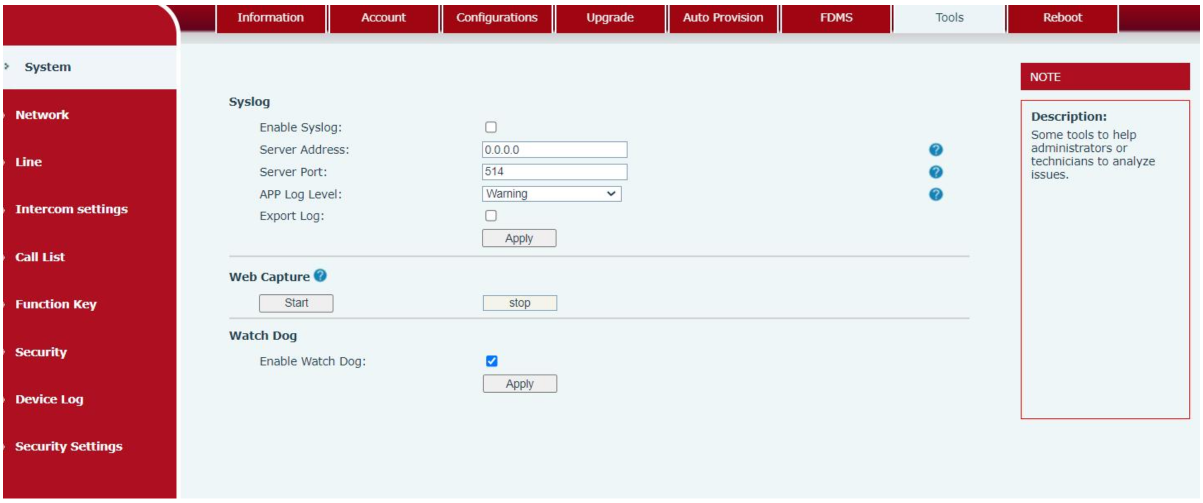
Picture 19 - FDMS

Table 8 - FDMS Information

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.



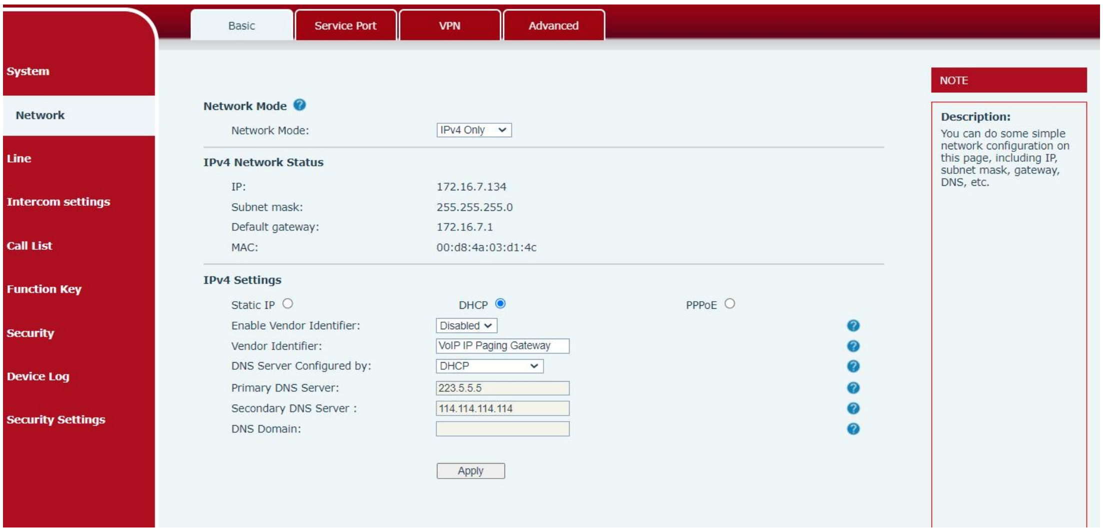
Picture 20 - Tools

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.

Refer to 10 troubleshooting for details.

9.9 Network >> Basic

Users can configure network connection types and parameters through this page.



Picture 21 - Network Basic Setting

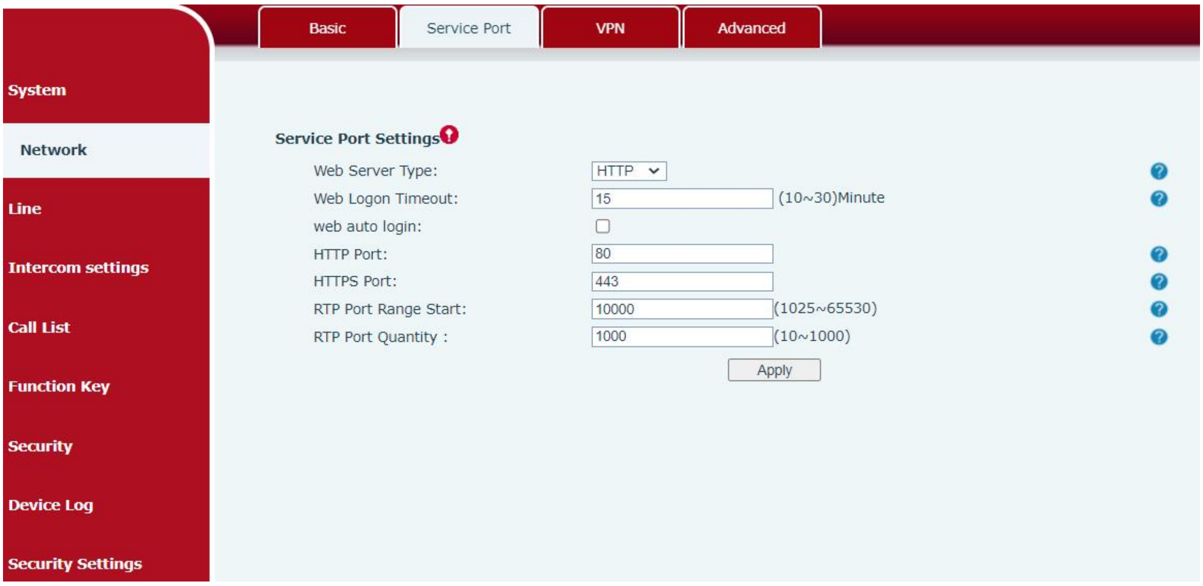
Table 9 - Basic Setting Parameters

Parameters	**Description**
Network Mode	IPv4、IPv6 and IPv4&IPv6
IPv4 Network Status	
IP	The current IP address of the device
Subnet mask	The current Subnet Mask
Default gateway	The current Gateway IP address
MAC	The MAC address of the device
IPv4 Settings	
For the network connection mode of the device, please select the appropriate network mode according to the actual network environment. The device provides three network modes:	
Static IP	If your ISP service provider provides a fixed IP address, you can select this item. After selection, you must fill in the static table: static IP address / subnet mask / gateway / DNS and other relevant information. If you do not know this information, please ask your ISP service provider or network administrator for assistance.
DHCP	Network parameters are provided automatically by a DHCP server.
PPPoE	When selecting this mode, you must enter the ADSL online account and password.
Enable Vendor Identifier	Enable DHCP OPTION 60 to take vendor information.
Vendor Identifier	DHCP OPTION 60,vendor class identifier.Valid Value:

	Alphanumeric. Up to 20 characters.
When using static mode, you need to set relevant static configuration.	
DNS Server Configured by	Use DNS server assigned by DHCP server.
Primary DNS Server	Preferred DNS server.
Secondary DNS Server	alternate DNS server.
DNS Domain	DNS Domain
NOTE: 1) After setting the parameters, you need to click submit to take effect. 2) If you change the IP, the web page will no longer respond. At this time, you should enter a new IP in the address bar to connect to the device.	

9. 10 Network >> service port

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



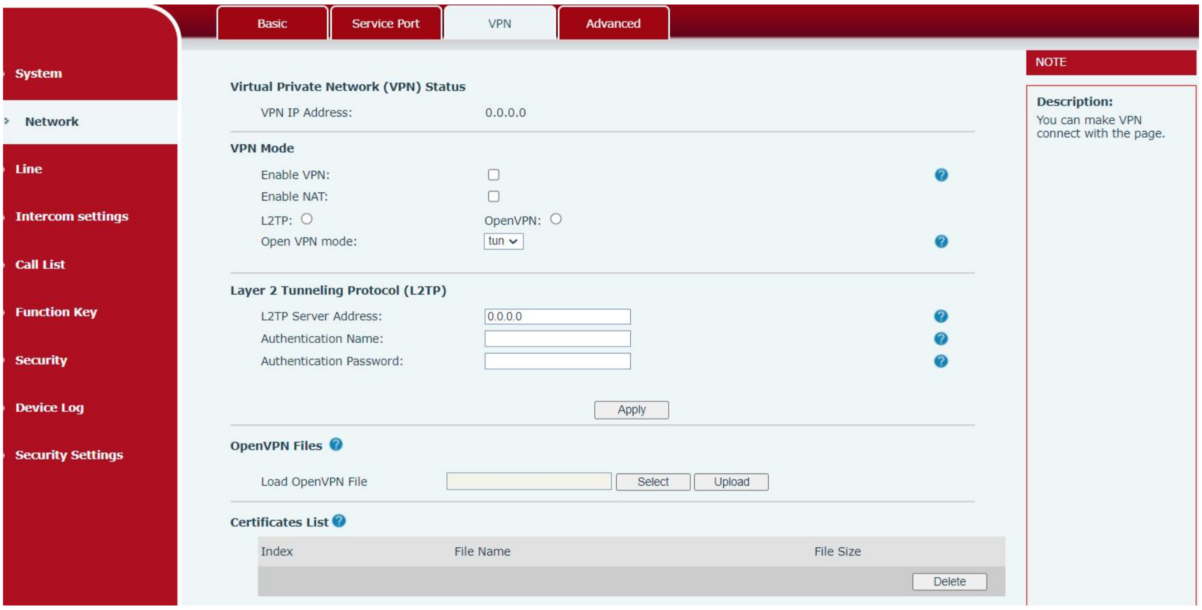
Picture 22 - Service port setting interface

Table 10 - Server Port

parameter	description
Web server type	Restart after setting takes effect. Optional web login as HTTP/HTTPS
Web login timeout	The default is 15 minutes, the timeout will automatically log out of

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

9. 11 Network >> VPN



Picture 23 - Network 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 page [**Network**] -> [**VPN**]. In VPN Mode, check the “Enable VPN” option and select “L2TP”, then fill in the L2TP server address, Authentication Username, and Authentication Password in the L2TP section. Press “Apply” then the device will try to connect to the L2TP server.

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

Once the VPN is configured, the device will try to connect to the VPN automatically when the device boots up every time until user disable it. Sometimes, if the VPN connection does not established immediately, user may try to reboot the device and check if VPN connection established after reboot.

- **OpenVPN**

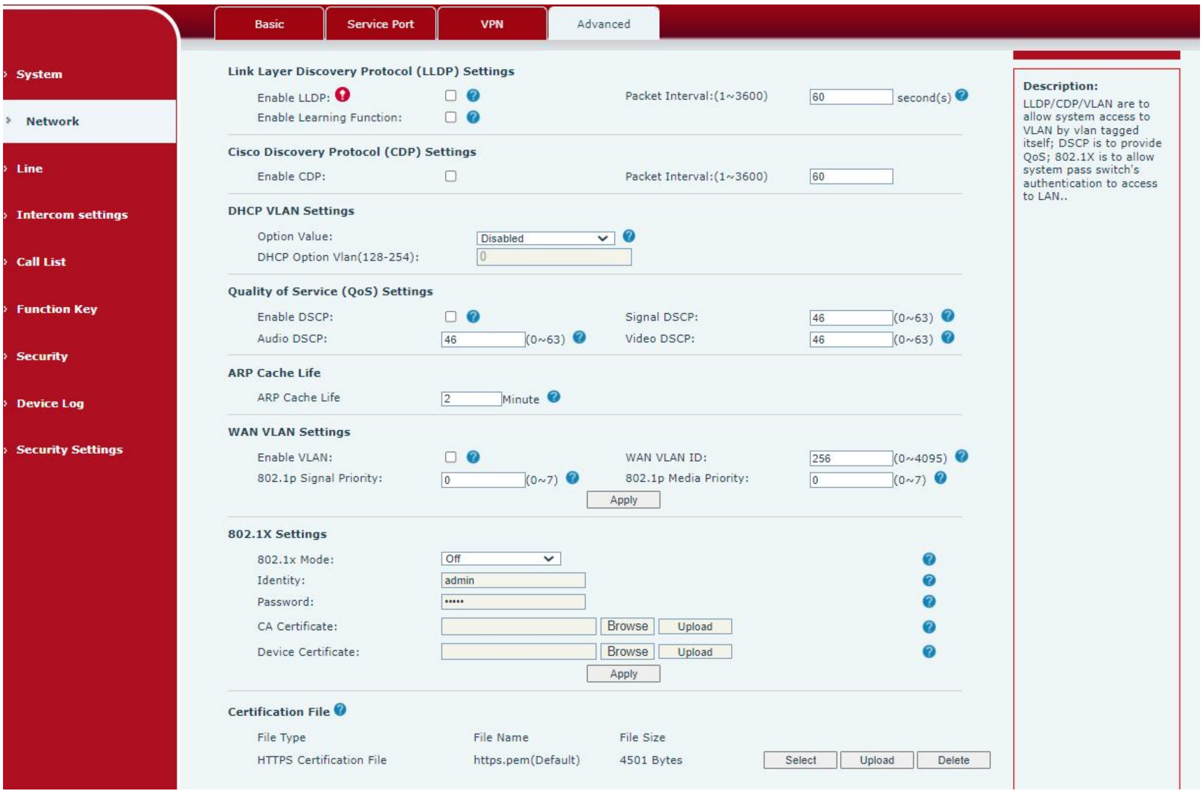
To establish an OpenVPN connection, user should get the following authentication and configuration files from the OpenVPN hosting provider and name them as the following,

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

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

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

9. 12 Network >> Advanced



Picture 24 - Network Setting

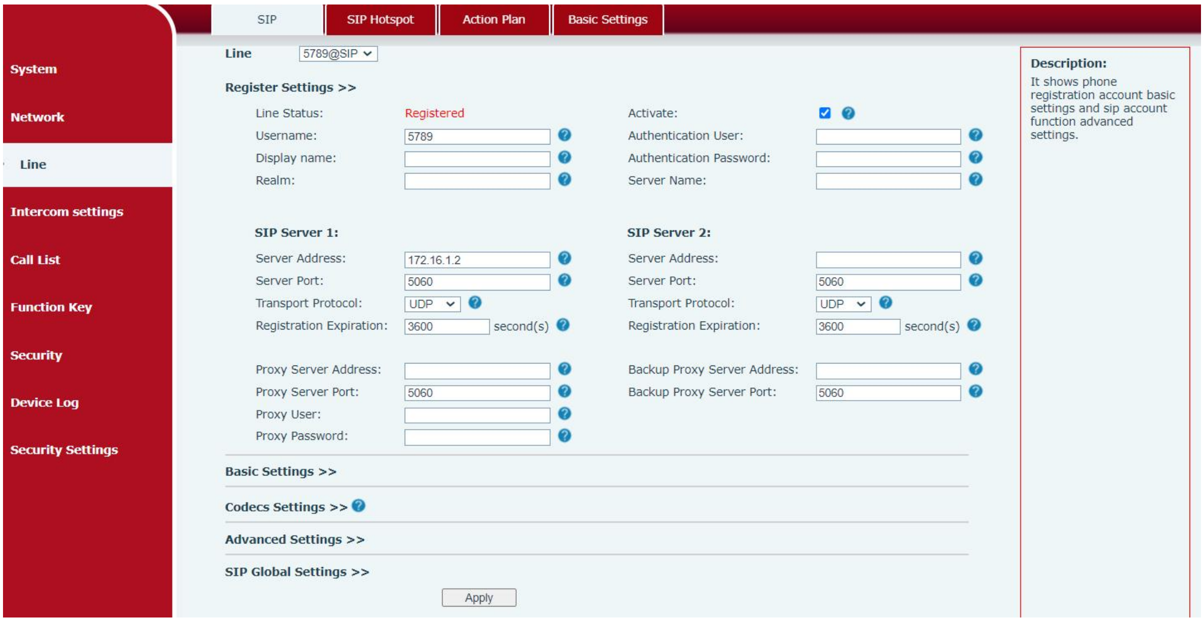
Network advanced Settings are typically configured by IT administrators to improve the quality of device service.

Table 11 - Network Basic Setting Paramater

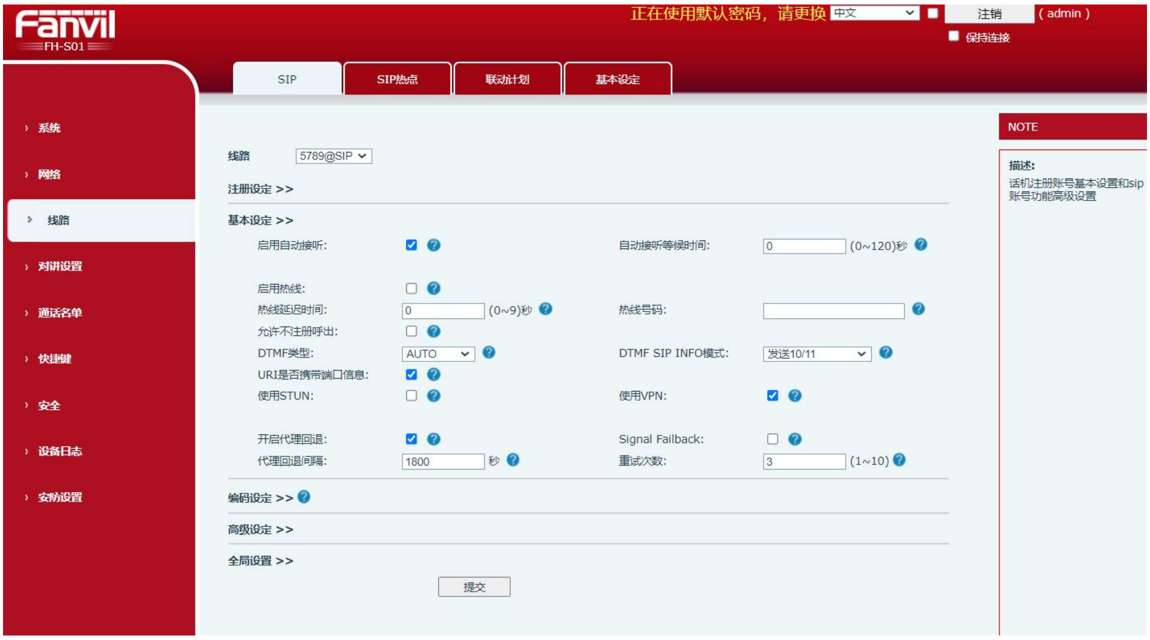
parameter	description
LLDP Settings	
Enable LLDP	Enables LLDP (Linker Layer Discovery Protocol) function.
Packet Interval	LLDP message sent periodic interval.Valid Value:1 to 3600 seconds.
Enable Learning Function	Enable VLAN settings learned via LLDP-MED
Cisco Discovery Protocol (CDP) Settings	
Enable CDP	Enable CDP
Packet Interval	Valid Value:1 to 3600 seconds.Default 60s
Quality of Service (QoS) Settings	
Enable DSCP	Enable DSCP to get best offset QoS for voice quality.
Signal DSCP	DSCP value for SIP messages.Valid Value:0~63.

Audio DSCP	DSCP value for voice RTP data.Valid Value:0~63.
Video DSCP	DSCP value for video RTP data.Valid Value:0~63.
ARP Cache Life	
ARP Cache Life	Set ARP cache life. Do not modify this value if there is no problem with the system.Valid Value:0~99
DHCP VLAN Settings	
Option Value	The DHCP option for Vlan Discovery
WAN VLAN Settings	
Enable VLAN	Enable VLAN to let system access to VLAN network with vlan tagged.
WAN VLAN ID	VLAN ID for system WAN port.Valid Value:0~4095.
802.1p Signal Priority	802.1P priority for SIP messages.Valid Value:0-lowest priority；7-highest priority
802.1p Media Priority	Valid Value:Integer from 0 to 7.
802.1X Settings	
802.1x Mode	It configures the 802.1x authentication method.Valid Value:static.network.802_1x.mode (0-Disabled;1-EAP-MD5;2-EAP-TLS;3-PEAP-MSCHAPv2).:
Identity	认证用户名
Password	认证密码
CA Certificate	上传 CA 证书
Device Certificate	上传设备证书
Certification File	
File Type	System's HTTPS server CA file type.
File Name	System's HTTPS server CA file name.
File Size	System's HTTPS server CA file size.

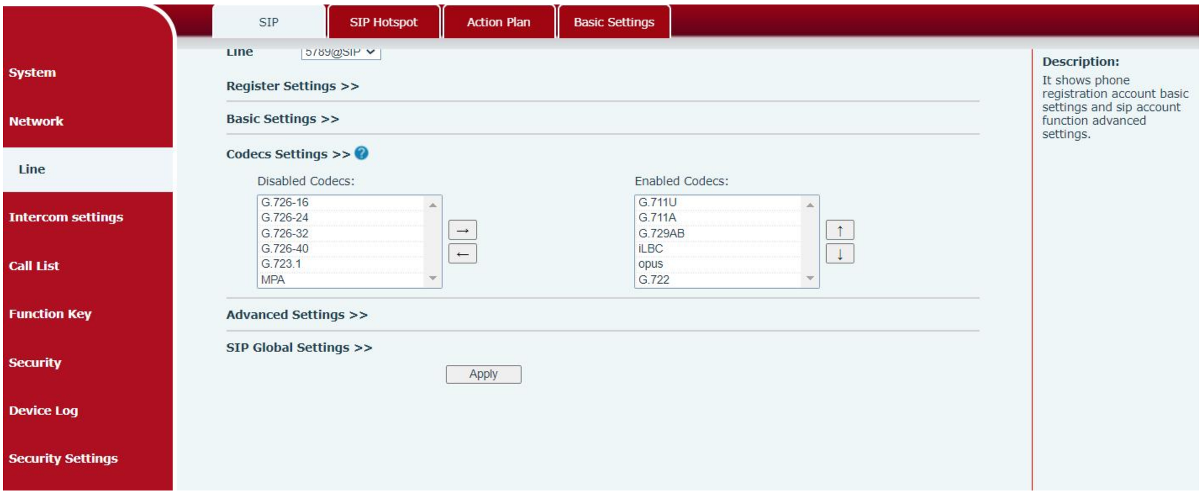
9.13 Lines >> SIP



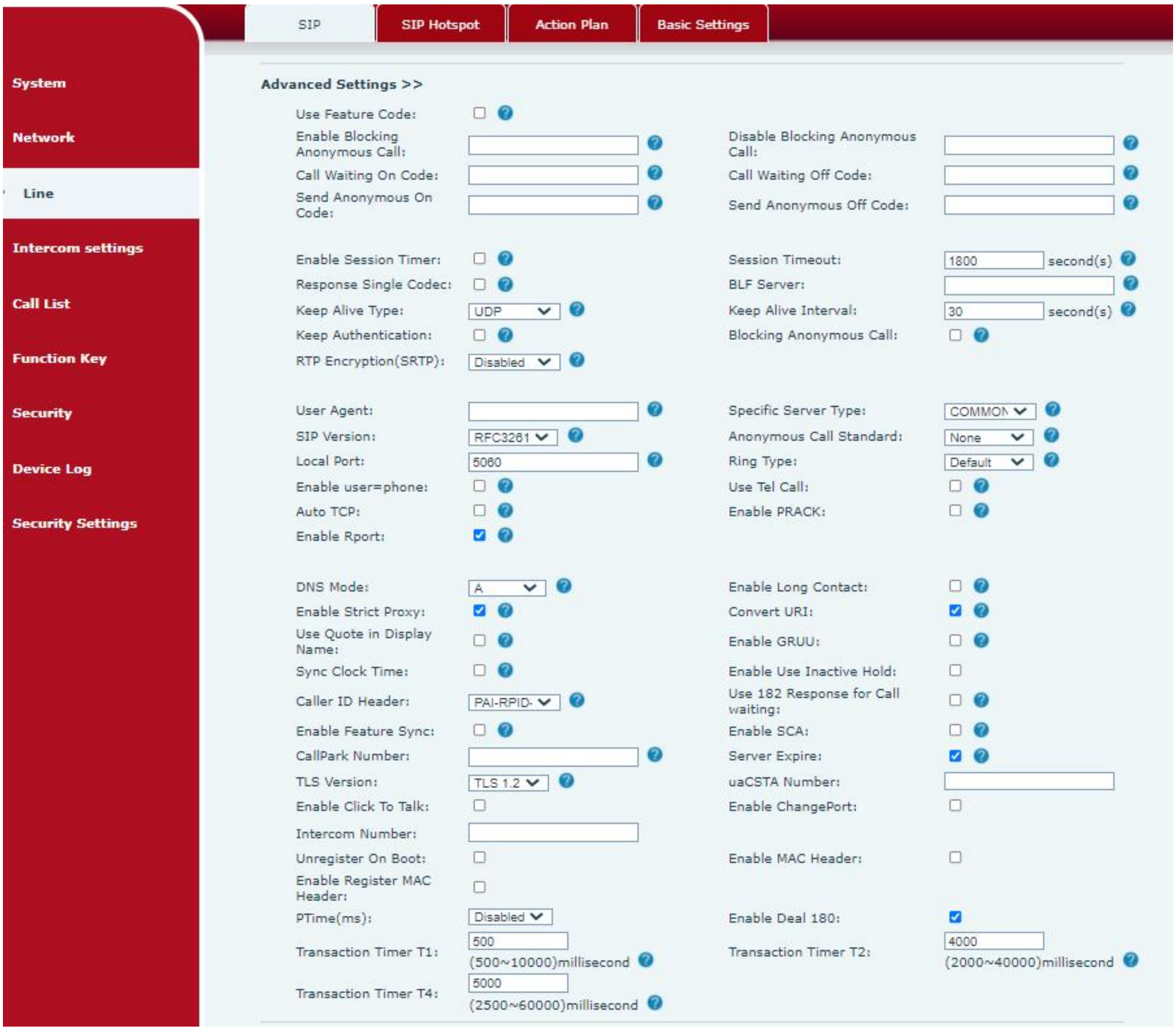
Picture 25 - SIP Settings(1)



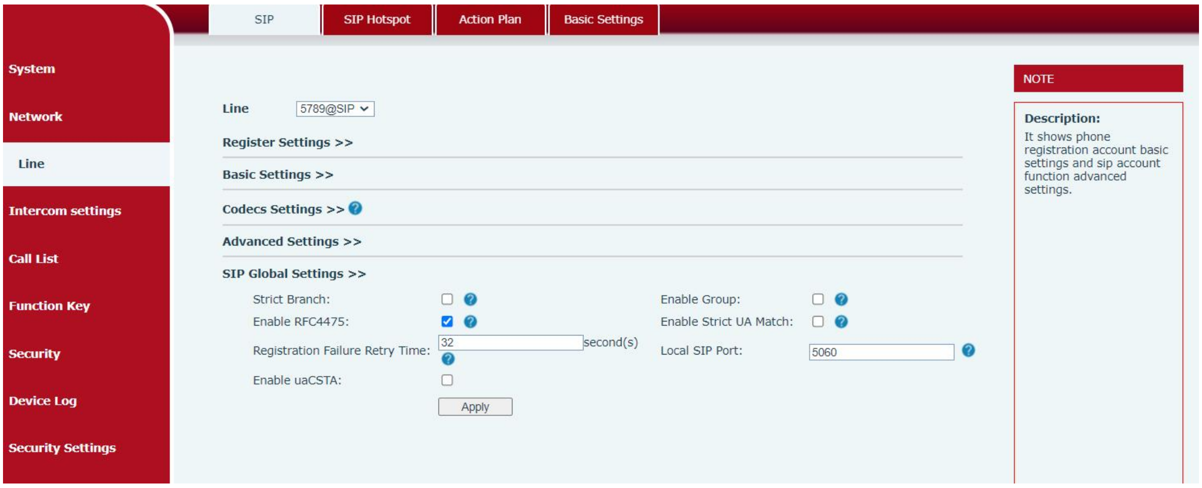
Picture 26 - SIP Settings(2)



Picture 27 - SIP Settings(3)



Picture 28 - SIP Settings(4)



Picture 29 - SIP Settings(5)

Table 12 - SIP Settings

Parameters	Description
Register Settings	
Line Status	Display the current line status at page loading. To get the up to date line status, user has to refresh the page manually.
Activate	It enables or disables the account X.
Username	It configures the display name for account X.
Authentication User	It configures the register user name for account X.Valid Value:String within 80 characters.
Display name	It configures the display name for account X.
Authentication Password	It configures the password for register authentication for account X.Valid Value:String within 80 characters.
Realm	It configures the address of Domain Name.
Server Name	It configures the server name for account X.
SIP Server 1	
Server Address	It configures the SIP server.Valid Value:IP address and Domain Name.
Server Port	It configures the port of the SIP server.
Transport Protocol	Select transfer protocol.
Registration Expiration	It configures the interval (in seconds) between IP phones retrying account X before the registration timeout.Valid Value:Integer from 30 to 2147483647.
SIP Server 2	
Server Address	It configures the SIP server.Valid Value:IP address and Domain Name.
Server Port	It configures the port of the SIP server.

Transport Protocol	Select transfer protocol.
Registration Expiration	It configures the interval (in seconds) between IP phones retrying account X before the registration timeout.Valid Value:Integer from 30 to 2147483647.
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server
Proxy Server Port	Enter the SIP proxy server port, default is 5060
Proxy User	Enter the SIP proxy user
Proxy Password	Enter the SIP proxy password
Backup Proxy Server Address	Enter the IP or FQDN address of the backup proxy server
Backup Proxy Server Port	Enter the backup proxy server port, default is 5060
Basic Settings	
Enable Auto Answering	Enable auto-answering, the incoming calls will be answered automatically after the delay time
Auto Answering Delay	Set the delay for incoming call before the system automatically answered it
Enable Hotline	Enable hotline configuration, the device will dial to the specific number immediately at audio channel opened by off-hook handset or turn on hands-free speaker or headphone
Hotline Delay	Set the delay for hotline before the system automatically dialed it
Hotline Number	Set the hotline dialing number
Dial Without Registered	Set call out by proxy without registration
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'
Request With Port	Enable the Rport.
Use VPN	Set the line to use VPN restrict route
Use STUN	Set the line to use STUN for NAT traversal
Enable Failback	When the main server is available， whether switch to the master server
Failback Interval	Using Register message to periodically detect whether the time interval of main Proxy is available.
Signal Failback	In the case of multiple proxy, whether invite/register request is allowed to execute failback
Signal Retry Counts	Multiple proxy cases SIP Request considers the number of attempts proxy is not available.
Codecs Settings	It enables or disables the specified codec for account X.
Advanced Settings	

Use Feature Code	When this setting is enabled, the features in this section will not be handled by the device itself but by the server instead. In order to control the enabling of the features, the device will send feature code to the server by dialing the number specified in each feature code field.
Enable Blocking Anonymous Call	Set the feature code to dial to the server
Disable Blocking Anonymous Call	Set the feature code to dial to the server
Call Waiting On Code	Set the feature code to dial to the server
Call Waiting Off Code	Set the feature code to dial to the server
Send Anonymous On Code	Set the feature code to dial to the server
Send Anonymous Off Code	Set the feature code to dial to the server
Enable Session Timer	Set the line to enable call ending by session timer refreshment. The call session will be ended if there is not new session timer event update received after the timeout period
Session Timeout	Set the session timer timeout period
Response Single Codec	If setting enabled, the device will use single codec in response to an incoming call request
BLF Server	The registered server will receive the subscription package from ordinary application of BLF phone. Please enter the BLF server, if the sever does not support subscription package, the registered server and subscription server will be separated.
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole opened
Keep Alive Interval	Set the keep alive packet transmitting interval
Keep Authentication	Keep the authentication parameters from previous authentication
Blocking Anonymous Call	Reject any incoming call without presenting caller ID
RTP Encryption	Enable RTP encryption such that RTP transmission will be encrypted
User Agent	Set the user agent, the default is Model with Software Version.
Specific Server Type	Set the line to collaborate with specific server type
SIP Version	Set the SIP version
Anonymous Call Standard	Set the standard to be used for anonymous
Local Port	Set the local port
Ring Type	Set the ring tone type for the line

Enable user=phone	Sets user=phone in SIP messages.
Use Tel Call	Set use tel call
Auto TCP	Using TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes
Enable Rport	Set the line to add rport in SIP headers
Enable PRACK	Set the line to support PRACK SIP message
DNS Mode	Select DNS mode, A, SRV, NAPTR
Enable Long Contact	Allow more parameters in contact field per RFC 3840
Enable Strict Proxy	Enables the use of strict routing. When the phone receives packets from the server，it will use the source IP address, not the address in via field.
Convert URI	Convert not digit and alphabet characters to %hh hex code
Use Quote in Display Name	Whether to add quote in display name, i.e. “Fanvil” vs Fanvil
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)
Sync Clock Time	Time Sycn with server
Enable Use Inactive Hold	启用后通话hold抓包可以看到(INVITE包中)SDP中是inactive
Caller ID Header	Set the Caller ID Header
Use 182 Response for Call waiting	Set the device to use 182 response code at call waiting response
Enable Feature Sync	Feature Sycn with server
Enable SCA	Enable/Disable SCA (Shared Call Appearance)
CallPark Number	Set the callPark number
Server Expire	Use the timeout of the server.
TLS Version	Choose TLS Version
uaCSTA Number	Set uaCSTA number
Enable Click To Talk	Use with special server, click to call directly after enabling
Enable ChangePort	Enable port update
Intercom Number	Set intercom number
Unregister On Boot	Whether to enable the logout function
Enable MAC Header	Whether to enable the SIP package and user agent with or without MAC during registration
Enable Register MAC Header	Whether to open registration: Yes, user agent (with or without MAC)
PTime(ms)	Set whether to bring the ptime field. The default is not
Enable Deal 180	On: after receiving 183 + SDP, play IVR, and then play local tone when receiving 180. Close: after receiving 183 + SDP, play IVR, and then do not

	play local tone when receiving 180.
Transaction Timer T1	It configures the SIP Transaction Timer T1(in millionseconds),Valid Value:500~10000
Transaction Timer T2	It configures the SIP Transaction Timer T2(in millionseconds),Valid Value:2000~40000
Transaction Timer T4	It configures the SIP Transaction Timer T2(in millionseconds),Valid Value:2500~60000
SIP Global Settings	
Strict Branch	Strictly match the Branch field.
Enable Group	Enable SIP group server function as server backup.
Enable RFC4475	After enabling, strictly observe RFC4475.
Enable Strict UA Match	Open a strict UA match and only accept requests from the server.
Registration Failure Retry Time	The registration failure retries time, if the SIP account fails to register, the chance to register half of the retransmission time is registered until the registration is successful.
Local SIP Port	The SIP port used by the device.
Enable uaCSTA	Set whether to enable uacsta function

9.14 Lines >> SIP Hotspot

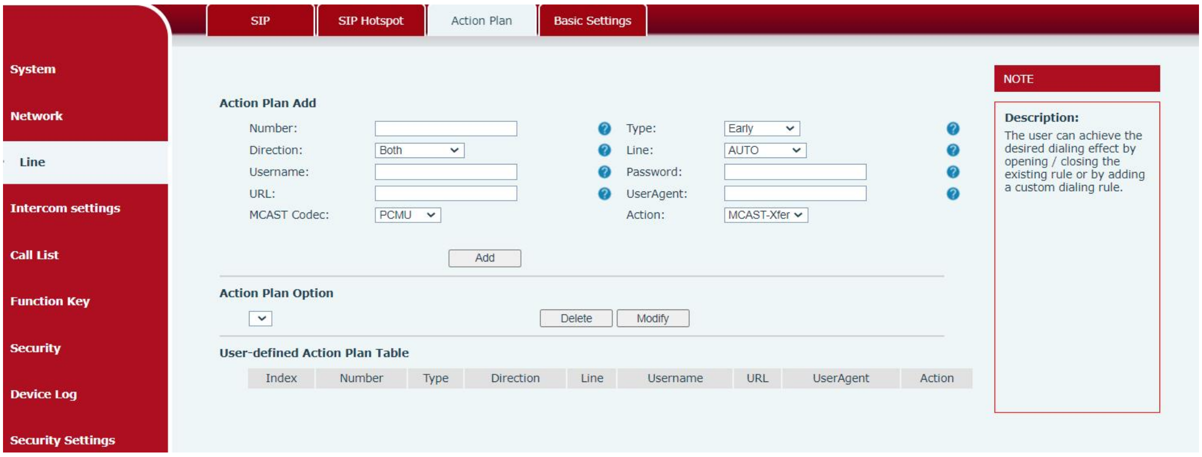
SIP hotspot is a simple and practical function. It is simple to configure, can realize the function of group vibration, and can expand the number of SIP accounts.

See 8.3 Hotspot for details

9.15 Line >> Action Plan

When calling to a phone, the bounded IP camera synchronously transmits video to the opposite phone (video support).

Log in to the device web, visit [**Line**] >[**Action plan**], and configure action plan rules.



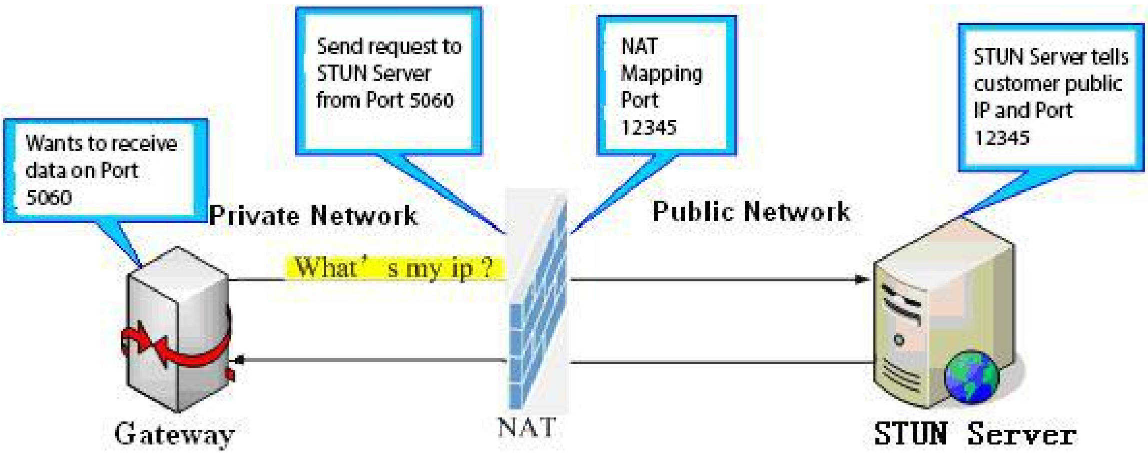
picture 30 - Action plan

Table 13 - Action Plan

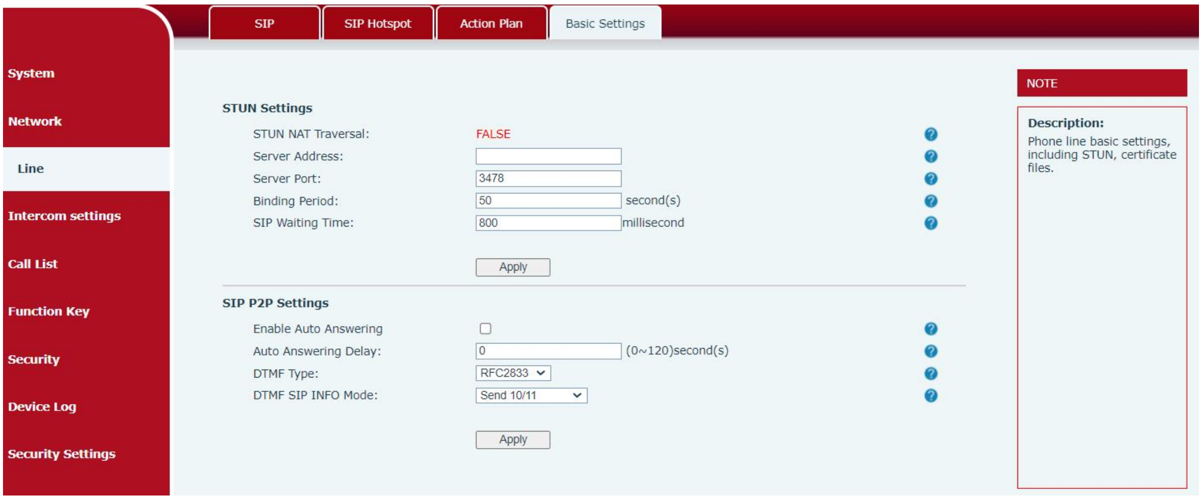
Parameter	Description
Number	Auxiliary phone number (support video)
Type	Support video display on call.
Direction	For call mode, incoming/outgoing call displays video
Line	Set up outgoing lines.
Username	Bind the user name of the IP camera.
Password	Bind IP camera password.
URL	Video streaming information.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

9. 16 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 31 - Network Basic



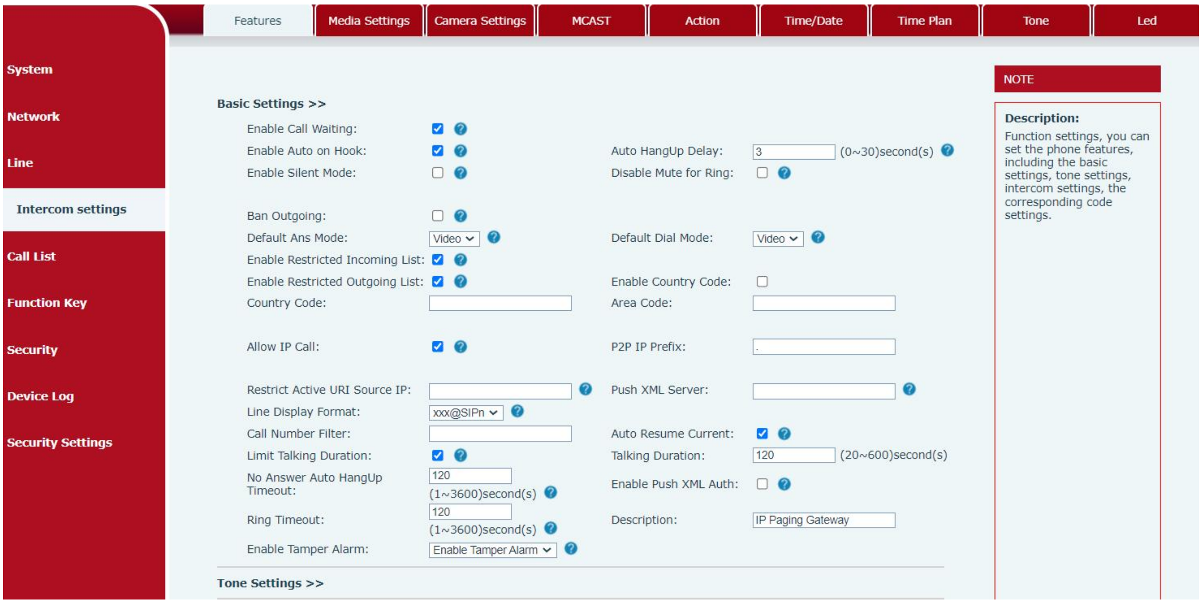
picture 32 - Line Basic Setting

Table 14 - Line Basic Setting

Parameters	Description
STUN Settings	
Server Address	Set the STUN server address
Server Port	Set the STUN server port, default is 3478
Binding Period	Set the STUN binding period which can be used to keep the NAT pinhole opened.
SIP Waiting Time	Set the timeout of STUN binding before sending SIP messages
SIP P2P Settings	
Enable Auto Answering	Automatically answer incoming IP calls after the timeout period is enabled
Auto Answering Delay	Automatic answer timeout setting

DTMF Type	Set the DTMF type of the line.
DTMF SIP INFO Mode	Set SIP INFO mode to send ‘*’ and ‘#’ or ‘10’ and ‘11’

9. 17 Intercom settings >> Features



picture 33 - Features

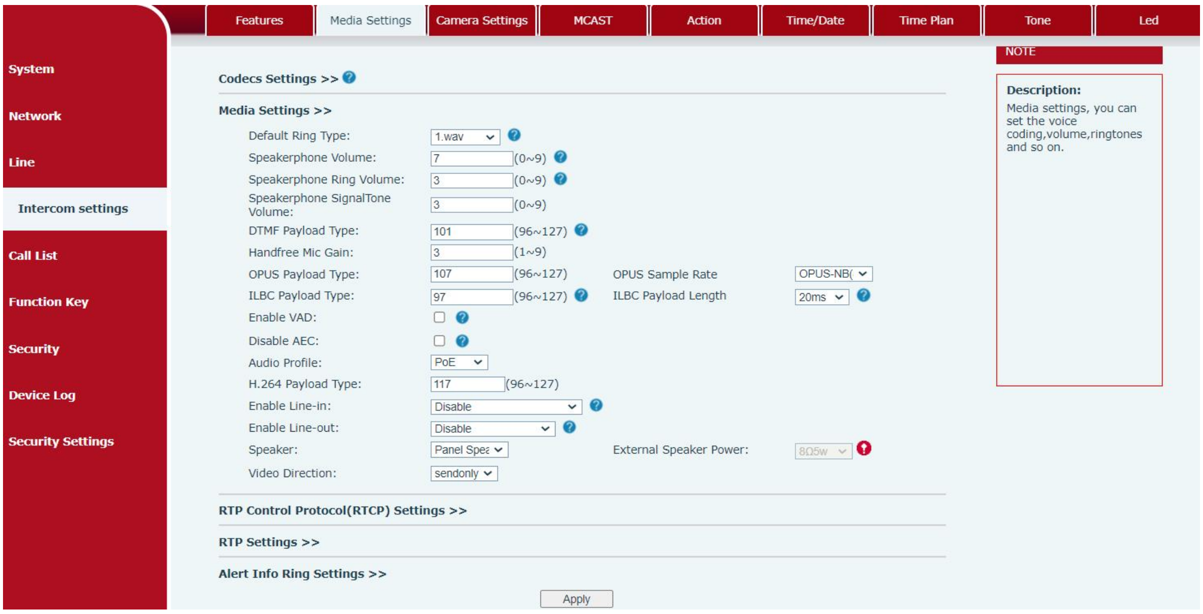
Table 15 - Features

Parameters	Description
Basic Settings	
Enable Call Waiting	Enable this setting to allow user to take second incoming call during an established call. Default enabled.
Enable Auto On Hook	The device will hang up and return to the idle automatically at hands-free mode
Auto HangUp Delay	Specify Auto handup time, the phone will hang up and return to the idle automatically after Auto Hand down time at hands-free mode, and play dial tone Auto handdown time at handset mode
Enable Silent Mode	When enabled, the phone is muted, there is no ringing when calls, you can use the volume keys and mute key to unmute.
Disable Mute for Ring	When it is enabled,you can not mute the phone.
Ban Outgoing	If you select Ban Outgoing to enable it, and you cannot dial out any number.
Default Ans Mode	Default Ans Mode:video or audio.

Default Dial Mode	Default Dial Mode:video or audio.
Enable Restricted Incoming List	Whether enable Restricted Incoming List
Enable Restricted Outgoing List	Wether enable Restricted Outgoing List
Enable country Code	Wether enable country Code
Country Code	Country Code
Area Code	Area Code
Allow IP Call	If enabled, user can dial out with IP address
P2P IP Prefix	You can set IP call prefix,for example,i set it as “172.16.2.”,then i input #160 in dialpad and press dial key ,it will call 172.16.2.160 automatically
Restrict Active URI Source IP	Set the device to accept Active URI command from specific IP address.
Push XML Server	Configure the Push XML Server, when phone receives request, it will determine whether to display corresponding content on the phone which sent by the specified server or not.
Call Number Filter	Configure a special character & ,if the number is 78 & 9. The call will be filtered out&
Auto Resume Current	If the current path changes, the hold will be automatically resume
Auto Resume Current	If the current path changes, the hold will be automatically resume
Limit Talking Duration	Automatically hang up the call after enabling the time set for the call
Talking Duration	Call duration ,20-600s
No Answer Auto HangUp Timeout	If the call is not answered, the call will be automatically hung up after the timeout
Enable Push XML Auth	To enable push xml auth, user password is required
Ring Timeout	It configures ringing time of incoming call
Description	
Enable Tamper Alarm	Enable or prohibit anti disassembly detection and handle detection
Tone Settings	
Enable Holding Tone	When turned on, a tone plays when the call is held
Enable Call Waiting Tone	When turned on, a tone plays when call waiting
Play Dialing DTMF Tone	Play DTMF tone on the device when user pressed a phone digits at dialing, default enabled.
Play Talking DTMF Tone	Play DTMF tone on the device when user pressed a phone digits during taking, default enabled.
Auto Answer Tone	Start auto answer prompt tone
Intercom Settings	

Enable Intercom	When intercom is enabled, the device will accept the incoming call request with a SIP header of Alert-Info instruction to automatically answer the call after specific delay.
Enable Intercom Mute	Enable mute mode during the intercom call
Enable Intercom Tone	If the incoming call is intercom call, the phone plays the intercom tone
Enable Intercom Barge	Enable Intercom Barge by selecting it, the phone auto answers the intercom call during a call. If the current call is intercom call, the phone will reject the second intercom call
Response Code Settings	
Busy Response Code	Set the SIP response code on line busy
Reject Response Code	Set the SIP response code on call rejection

9. 18 Intercom settings >> Media Settings



picture 34 - Media Settings

Table 16 - Media Settings

Parameters	Description
Codecs Settings	Select the enabled and disabled voice codecs codec:G.711A/U,G.722,G.729AB,G.726-16,G.729-24,G.729-32,G.726-40,MPA,opus
Audio Settings	
Default Ring Type	Set the default ring type. If the caller ID of an incoming call was not configured with specific ring type, the default ring will be used.

Speakerphone Volume	Set the speakerphone volume, the value must be 0~9	
Speakerphone Ring Volume	Set the ring volume in the speakerphone, the value must be 0~9	
Speakerphone SignalTone Volume		
DTMF Payload Type	Enter the DTMF payload type, the value must be 96~127.	
Handfree Mic Gain		
Opus playload type	Enter the opus payload type, the value must be 96~127.	
OPUS Sample Rate	Set the opus sample rate，including OPUS-NB（8KHz), OPUS-WB（16KHz）	
ILBC Payload Type	Set the ILBC Payload Type	
ILBC Payload Length	Set the ILBC Payload Length	
Enable VAD	Enable Voice Activity Detection. When enabled, the device will suppress the audio transmission with artificial comfort noise signal to save the bandwidth.	Enable Voice device will supp comfort noise si
Disable AEC	Enable or disable the AEC (echo cancellation) function.	
Audio Profile	Select power supply or Poe form	
H.264 Payload Type	Range: 96 ~ 127	
Enable Line-in	enable or disable the line-in function	
Enable Line-out	enable or disable the line-out function	
Speaker	Support panel speaker and external speaker	
External Speaker Power	External speaker power , support 10W, 20W, 30W, when using the corresponding speaker, you must select the corresponding power supply.	
Video Direction		
RTP Control Protocol(RTCP) Settings		
CNAME user	Set the CNAME user	
CNAME host	Set the CNAME host	
RTP		
RTP keep alive	Keep talking, send a packet 30 seconds after enable it	
Alert Info Ring Settings （alert-info）		
Value of notification message 1 to 10	Set the value of the specified ring type	
ring type	The ring type	
line	Select the line of the incoming ring tone	

9.19 Intercom Setting >> MCAST

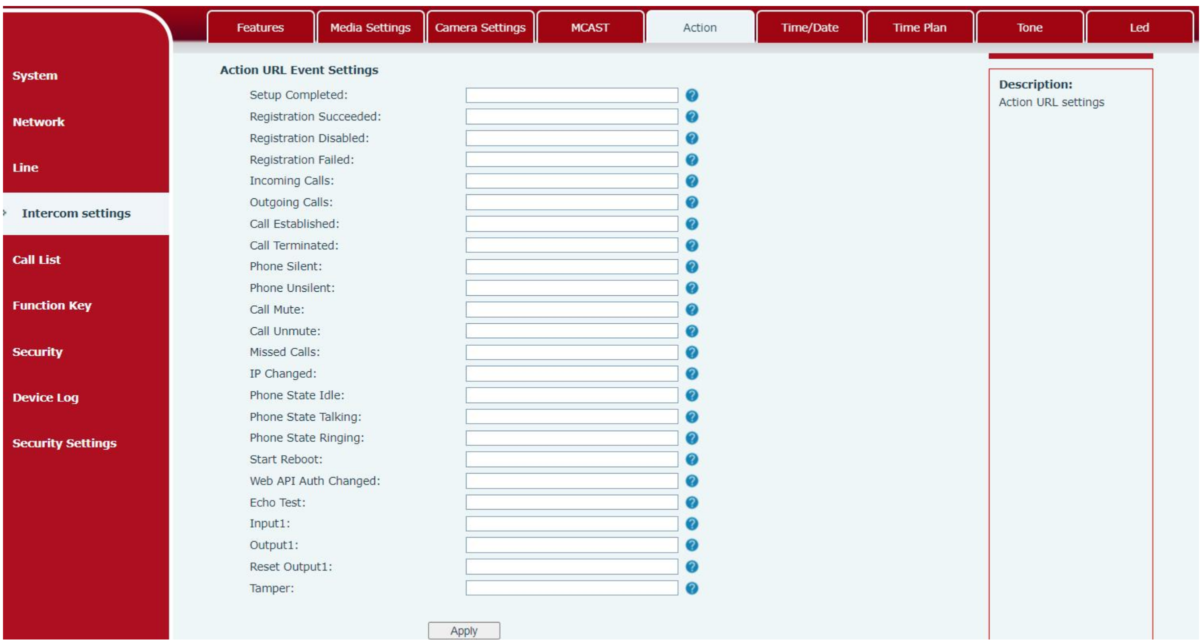
It is easy and convenient to use multicast function to send notice to each member of the multicast via setting the multicast key on the device and sending multicast RTP stream to pre-configured multicast address. By configuring monitoring multicast address on the device, monitor and play the RTP stream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

The detail for 8.2 MCAST

9.20 Intercom Setting >> Action URL

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

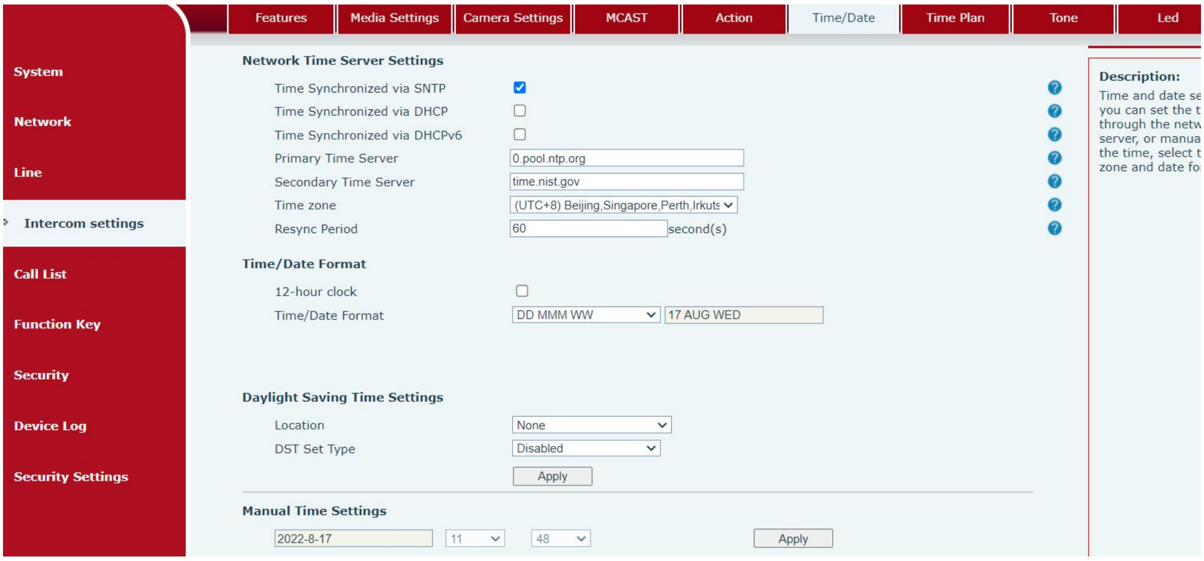
Action URL setting: configure the URL to report actions to the server. For example, fill in the URL: http://InternalServer /FileName.xml? (InternalServer is the IP address of the server, and FileName is the XML file name of the action reported by the storage device)



picture 35 - Action URL

9.21Intercom Setting >> Time/Date

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



picture 36 - Time/Date

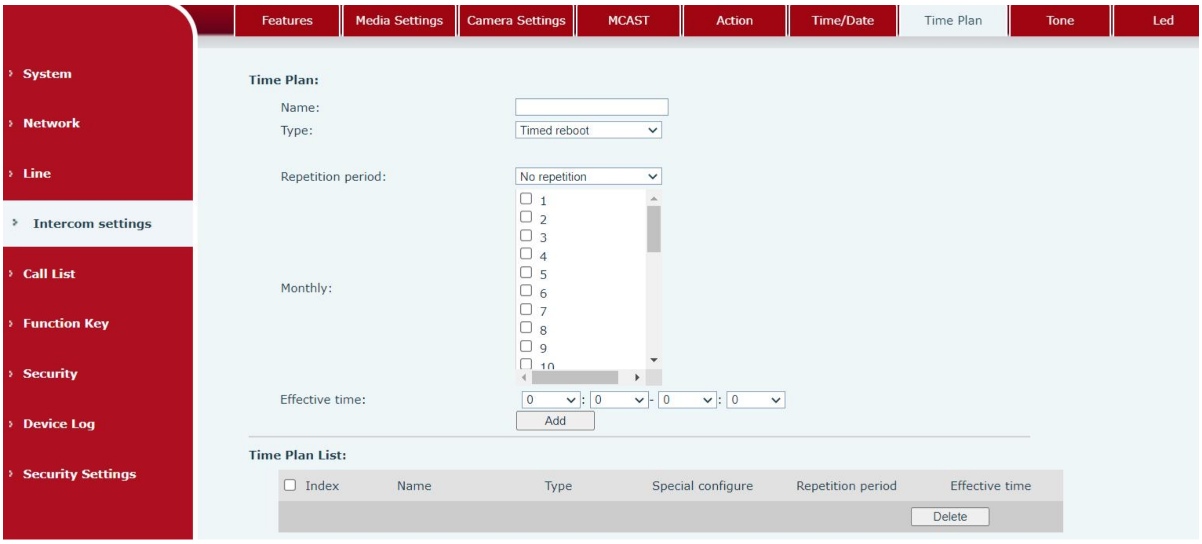
Table 17 - Time & Date settings

Parameters	Description
Network Time Server Settings	
Time Synchronized via SNTP	Enable time-sync through SNTP protocol
Time Synchronized via DHCP	Enable time-sync through DHCP protocol
Time Synchronized via DHCPv6	Enable time-sync through DHCPv6 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
12-Hour Clock	Set the time display in 12-hour mode
Date Format	Select the time/date display format
Daylight Saving Time Settings	
Local	Choose your local, device will set daylight saving time automatically based on the local
DST Set Type	Choose DST Set Type, if Manual, you need to set the start time and end time.
Fixed Type	Daylight saving time rules are based on specific dates or

	relative rule dates for conversion. Display in read-only mode in automatic mode.
Offset	The offset minutes when DST started
Month Start	The DST start month
Week Start	The DST start week
Weekday Start	The DST start weekday
Hour Start	The DST start hour
Minute Start	The DST start minute
Month End	The DST end month
Week End	The DST end week
Weekday End	The DST end weekday
Manual Time Settings	You can set your time manually

9. 22 Intercom settings>>Time plan

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



picture 37 - Time plan

Table 18 - Time plan

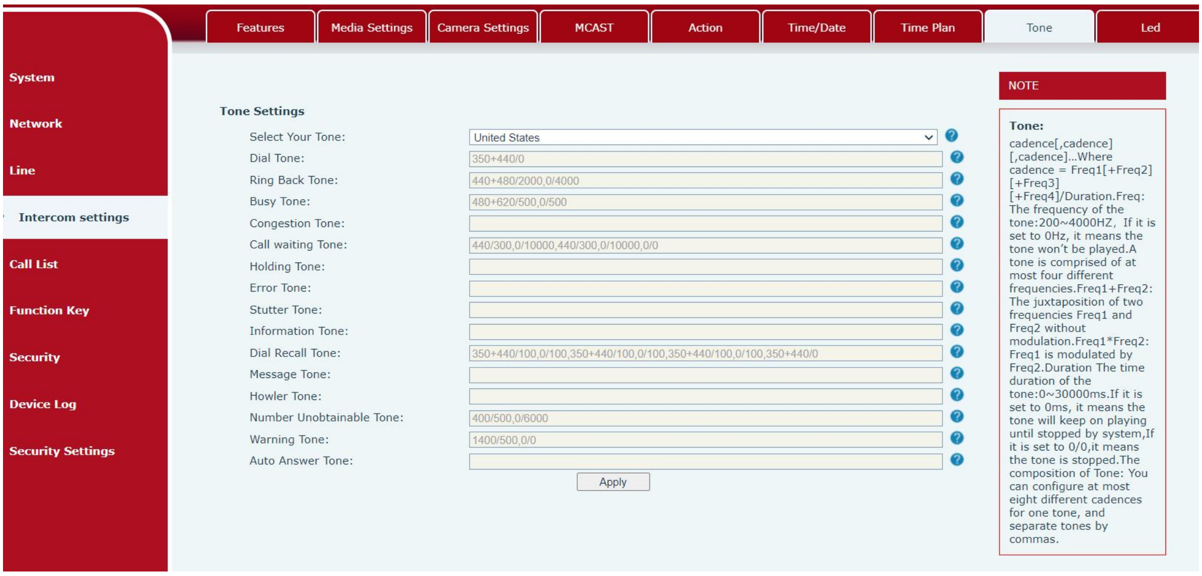
Parameters	Description
type	Timing restart, timing upgrade, timing sound detection, timing playback audio
Repeat cycle	Do not repeat: execute once within the set time range Daily: Perform this operation in the same time frame every day Weekly: Do this in the time frame of the day of the week

	Monthly: the time frame of the month to perform this operation
Effective time	Set the time period for execution

9. 23 Intercom settings >> Tone

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

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



picture 38 - Tone

9. 24 Call List >> Call List

■ Restricted Incoming Calls

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

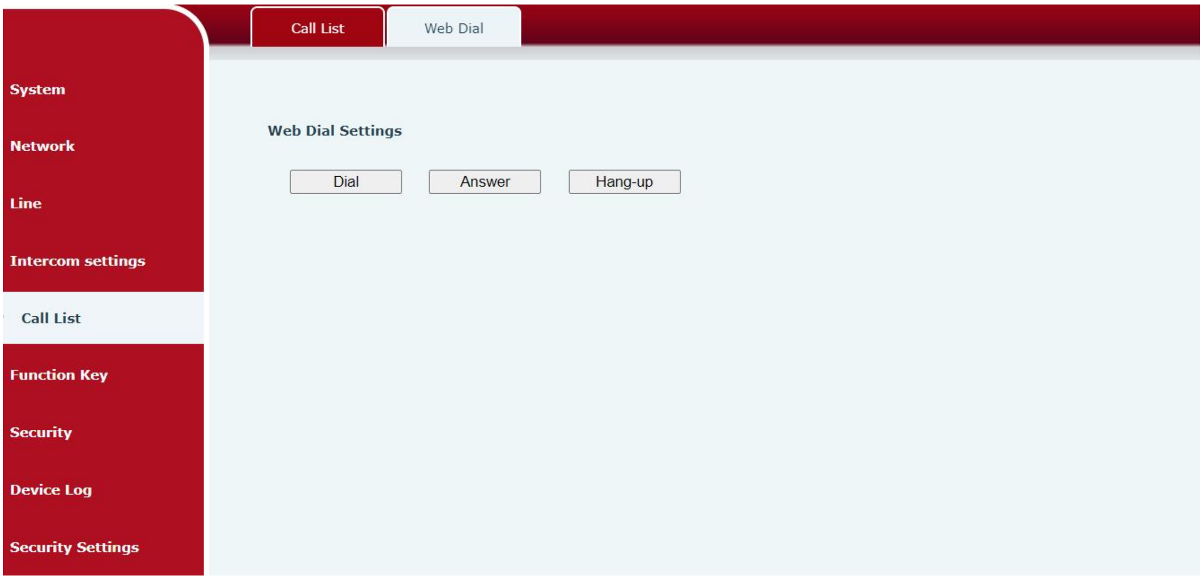
User can add specific number to be blocked, or a prefix where any numbers matched the prefix will all be blocked.

■ Restrict Outgoing Call

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

9. 25 Call List >> Web Dial

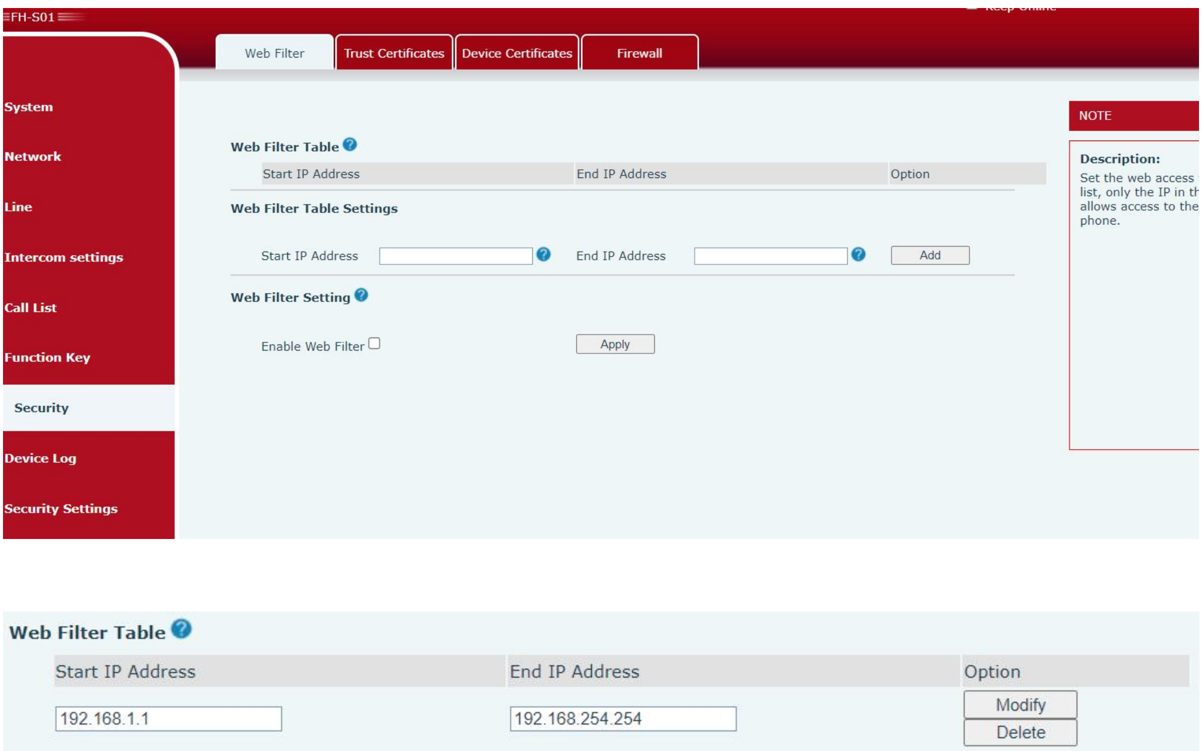
Use web page to call, answer and hang up.



picture 39 - Web Dial

9. 26 Security >> Web filter

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



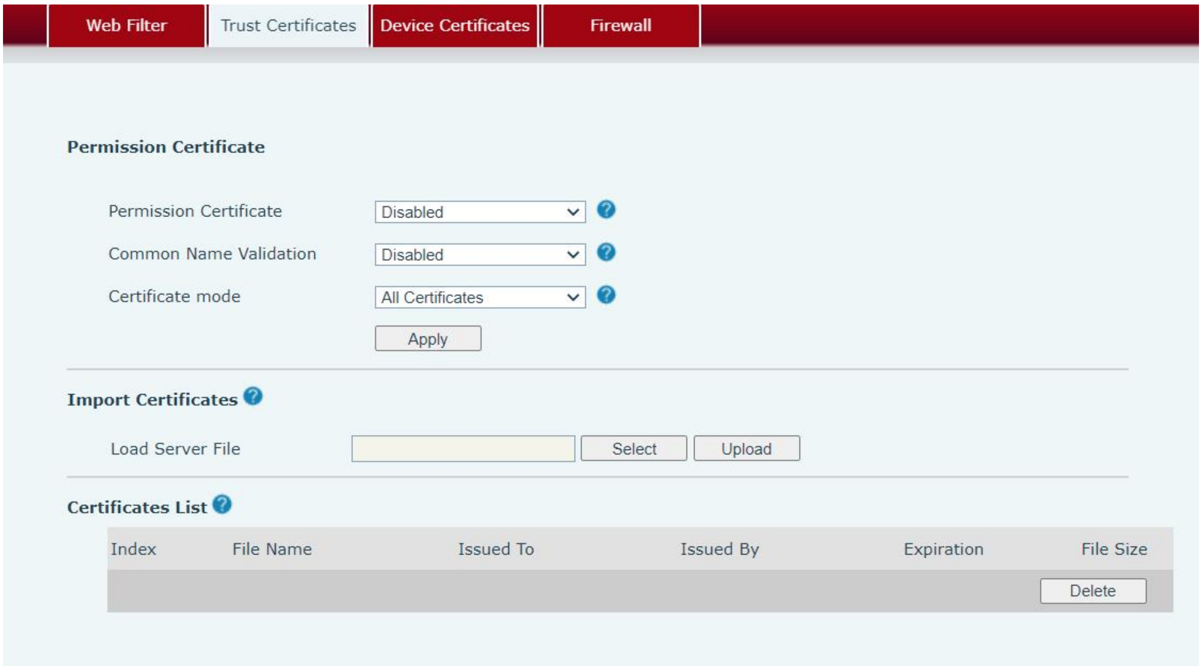
picture 40 - WEB filter

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

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

9. 27 Security >> Trust Certificates

You can upload and delete uploaded trust certificates.

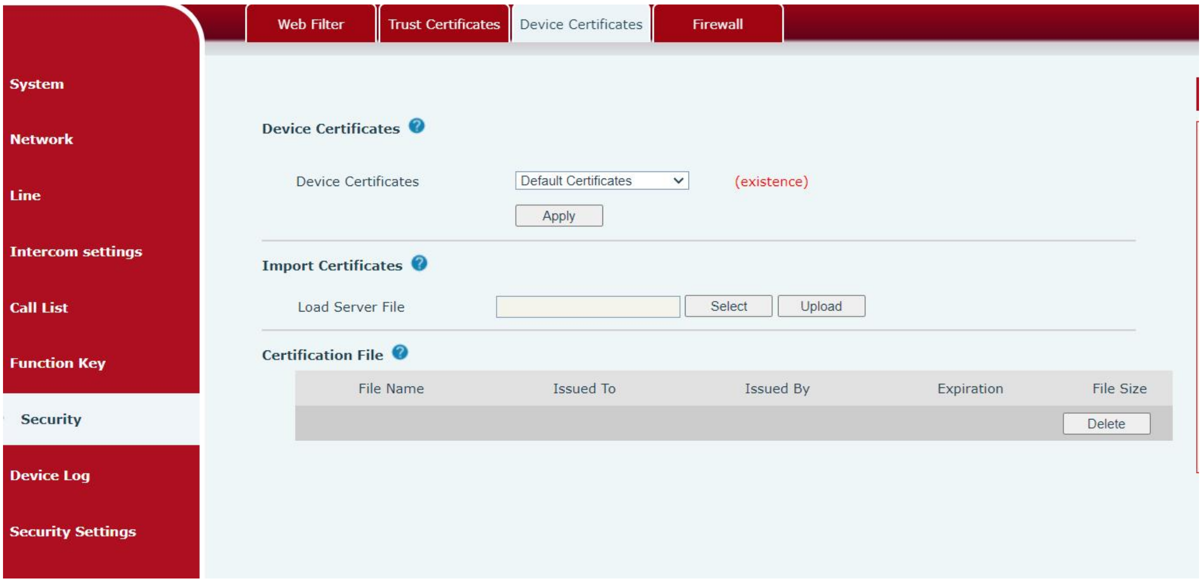


picture 41 -Trust Certificates

9. 28 Security >> Device Certificates

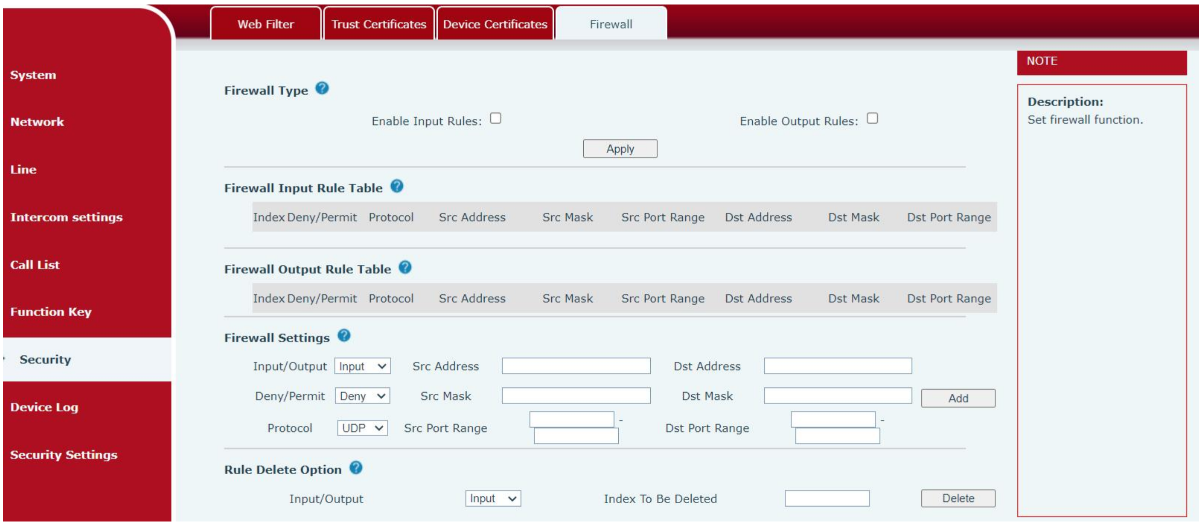
Select the default certificate or the custom certificate as the device certificate.

You can upload and delete uploaded certificates.



picture 42 - Device Certificates

9. 29 Security >> Firewall



picture 43 - Firewall

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

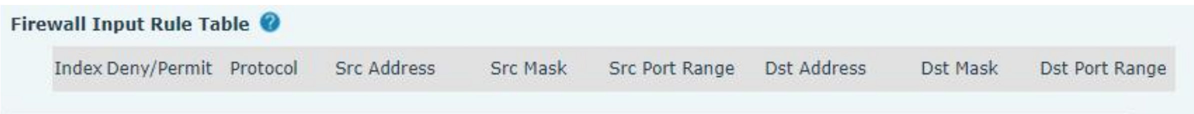
The firewall rule setting is a simple firewall module. This function supports two kinds of rules: input rules and output rules. Each rule will be assigned a serial number, and a maximum of 10 each rule can be set.

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

Table 19 - Web Firewall

parameter	Description
Enable Input Rules	whether enable Input Rules
Enable Output Rules	Whether enable Output Rules
input/output	Select the current rule as an input or output rule
Deny/permit	Choose the current rule is deny or allowed;
protocol	There are four types of protocols：TCP，UDP，ICMP，IP。
Port range	Port range
Src Address	The source address can be the host address, network address, or all addresses 0.0.0.0; it can also be a network address similar to *.*.*.0, such as 192.168.1.0.
Dst Mask	The destination address can be a specific IP address or all addresses 0.0.0.0; it can also be a network address similar to *.*.*.0, such as 192.168.1.0.
Src Port Range	It is the source address mask. When it is configured as 255.255.255.255, it means it is a specific host. When it is set as a subnet mask of type 255.255.255.0, it means that the filter is a network segment;
Dst Port Range	It is the destination address mask. When it is configured as 255.255.255.255, it means it is a specific host. When it is set as a subnet mask of 255.255.255.0 type, it means that a network segment is filtered;
源端口范围	
目的端口范围	

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



picture 44 - Firewall rules list

Then select and click the button [Submit].

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

picture 45 - Delete firewall rules

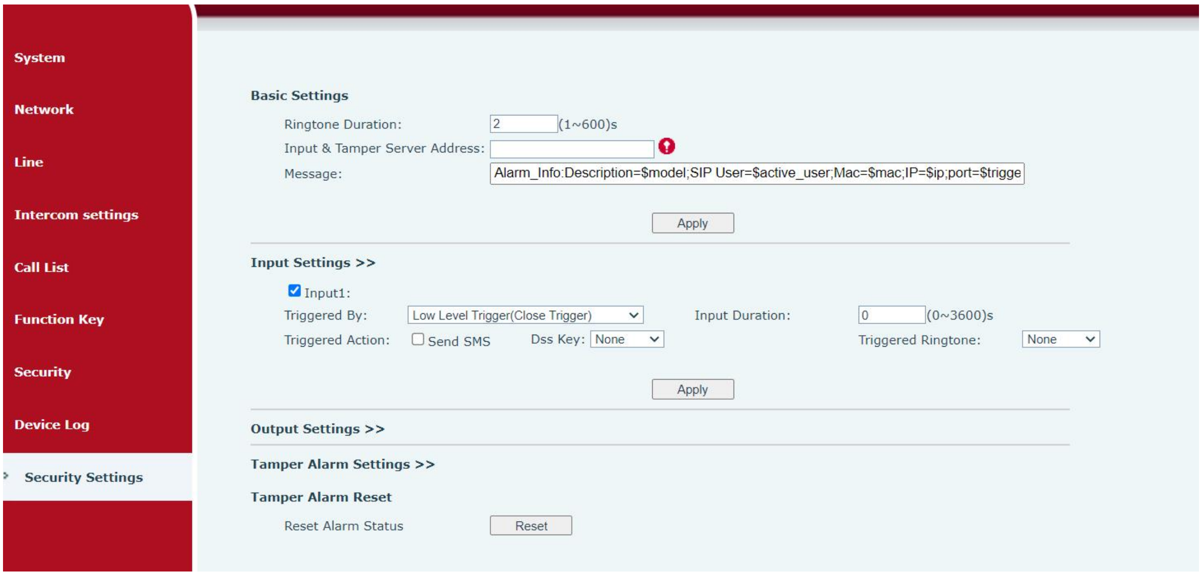
Select the list you want to delete and click [Delete] to delete the selected list.

9.30Device Log

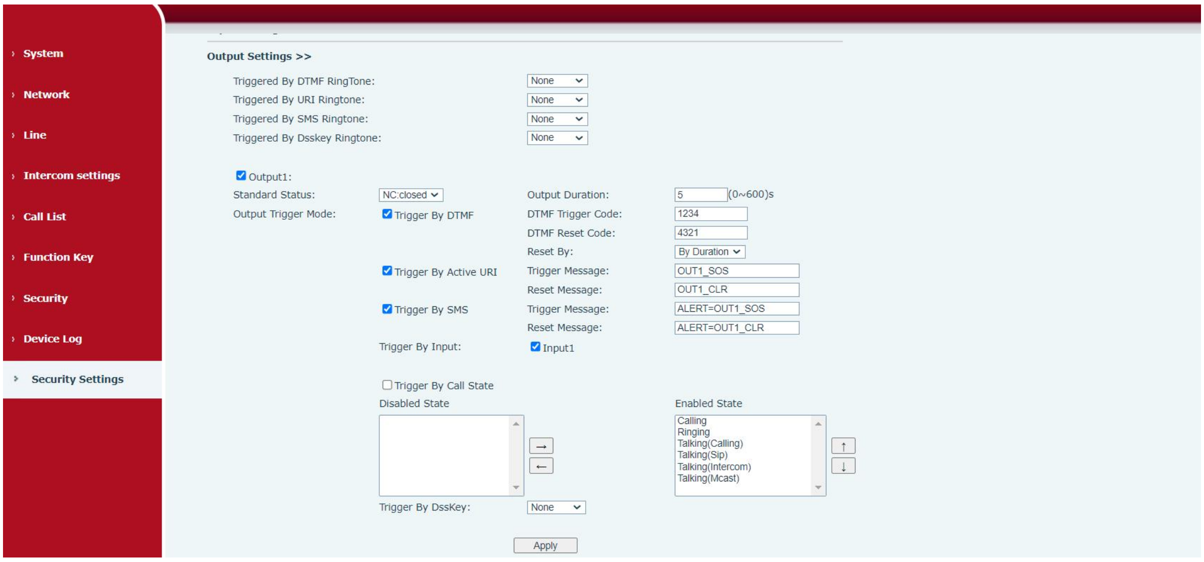
You can crawl the device log, when you encounter unusual problems, please send the device log to the technical staff for positioning problem.For more detail 10.5 get device log。

9. 31 Security settings

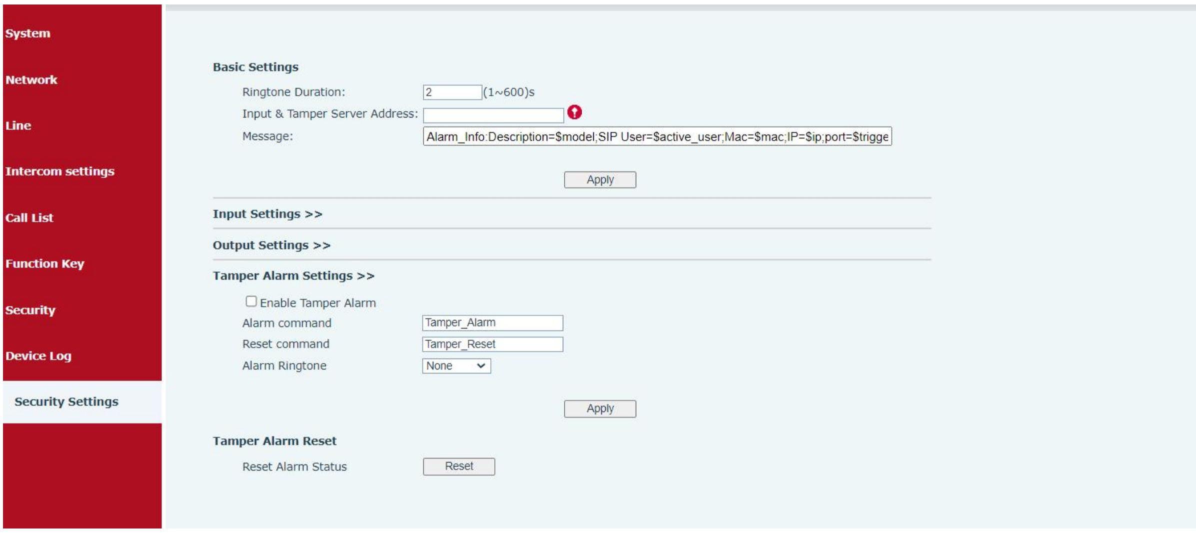
Enable Tamper: after enable, when the device is removed by force, the alarm information will be sent to the server and the alarm ring will be played.



picture 46 - Security settings（1）



picture 47 - Security settings（2）



picture 48 - Security settings（3）

Table 20 - Security Settings

Security Settings	
Parameters	**Description**
Basic Settings	
Ringtone Duration	Set the ringtone duration, default value is 5 seconds.
Input & Tamper Server Address	Set remote server address. The device will send message to the server when the alarm is triggered. The message format is ：Alarm_Info:Description=i16SV;SIP User=;Mac=0c:38:3e:3a:06:65;IP=;port=Input . The message content can also be customized.
Message	When the input port is triggered, a short message will be sent to the

<table>
<tr><td></td><td colspan="2">server. The message format is as follows：
Alarm_Info:Description=$model;SIP
User=$active_user;Mac=$mac;IP=$ip;port=$trigger</td></tr>
<tr><td colspan="3">Input settings</td></tr>
<tr><td>Input Detect</td><td colspan="2">Enable or disable Input Detect</td></tr>
<tr><td rowspan="2">Triggered by</td><td colspan="2">When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger.</td></tr>
<tr><td colspan="2">When choosing the high level trigger (disconnect trigger), detect the input port (high level) disconnected trigger.</td></tr>
<tr><td>Input Duration</td><td colspan="2">事件行为在持续检测时间内不断，触发相应的设置</td></tr>
<tr><td>Triggered Action</td><td colspan="2">启用或禁用输入端口发送消息到服务器</td></tr>
<tr><td>Dss Key</td><td colspan="2">设置为 dsskey 时，触发 dsskey 进行呼叫，默认为 none</td></tr>
<tr><td>Triggered Ringtone</td><td colspan="2">Select triggered ring tone.</td></tr>
<tr><td colspan="3">Output Settings</td></tr>
<tr><td>Output Detect</td><td colspan="2">Enable or disable Output Detect</td></tr>
<tr><td>Triggered by DTMF Ring tone</td><td colspan="2">Select the DTMF trigger ring tone.</td></tr>
<tr><td>Triggered by URI Ringtone</td><td colspan="2">Select the URI trigger ring tone.</td></tr>
<tr><td>Triggered By SMS Ringtone</td><td colspan="2">Select the SMS trigger ring tone.</td></tr>
<tr><td>Triggered By Dsskey Ringtone</td><td colspan="2">Select the Dsskey trigger ring tone.</td></tr>
<tr><td rowspan="2">Standard Status</td><td colspan="2">When choosing the low level trigger (NO: normally open), when meet the trigger condition, trigger the NO port disconnected.</td></tr>
<tr><td colspan="2">When choosing the high level trigger (NC: normally close), when meet the trigger condition, trigger the NC port close.</td></tr>
<tr><td>Output Duration</td><td colspan="2">Set the output change duration time, the default is 5 seconds.</td></tr>
<tr><td>Output Trigger Mode</td><td colspan="2">When the input port meets the trigger condition, the output port will trigger (the port level time changes, controlled by < output duration >).</td></tr>
<tr><td>Trigger by DTMF</td><td colspan="2">Enable or disable trigger by DTMF. The device will check the received DTMF sent by remote device, if it matches the DTMF trigger code, the device will trigger corresponding output port.</td></tr>
<tr><td>DTMF Trigger Code</td><td colspan="2">Input the DTMF trigger code, default value is 1234.</td></tr>
<tr><td>DTMF Reset Code</td><td colspan="2">Input the DTMF reset code, default value is 4321.</td></tr>
<tr><td>Reset By</td><td>By duration</td><td>Reset the output port status when output duration occurs.</td></tr>
</table>

	By state	Reset the output port status when device's call state changes.
Trigger by URI	Enable or disable trigger by URI. User can send commands from remote device or server to i16SV series device, if the command is correct, then device will trigger corresponding output port.	
Trigger by SMS	Enable or disable trigger by SMS. User can send ALERT command to i16SV series device, if the command is correct, then device will trigger corresponding output port.	
Trigger By Call state	Select call state to trigger the output port, options are: Talking: When the device's talking status changes, trigger the output port. Ringing: When the device's ringing status changes, trigger the output port. Calling: When the device's calling status changes, trigger the output port.	
Trigger By DssKey	Enable or disable trigger by dsskey. If any of the dsskey is selected, when the dsskey application performs, the output port will be triggered.	
Tamper Alarm Settings		
Enable Tamper Alarm	If the terminal is forcibly removed, the tamper will be triggered and the set alarm ring will be played all the time	
Alarm command	When the alarm is triggered, the server sends the command immediately	
Reset command	If the alarm bell needs to be stopped, the remote end can send a short message to the terminal. The content of the short message is the value set in the reset command. At this time, the terminal will stop playing the alarm bell	
Alarm Ringtone	The ringtone of alarm	
Tamper Alarm Reset		
Reset Alarm Status	One key reset alarm status	

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 Get device log

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

10.6 Common Trouble Cases

Table 21 - Trouble Cases

Trouble Case	Solution
Device could not boot up	1. The device is powered by external power supply via power adapter or PoE switch. Please use standard power adapter provided by Fanvil or PoE switch met with the specification requirements and check if device is well connected to power source. 2. If the device enters "POST mode" (the SIP/NET and function button indicators are always on), the device system is damaged. Please contact your location technical support to help you restore your equipment system.
Device could not register to a service provider	1. Please check if the device is connected to the network. 2. If network connection is fine, please check again your line configurations. If all configurations are correct, please kindly contact your service provider to get support, or follow the instructions in "10.4 Network Packet Capture" to get the network packet capture of registration process and send it to Fanvil support to analyze the issue.