i61&i62&i63&i64
User Manual

Software Version:0.0.14

Release Date：2021/10/25

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

i61&i62&i63&i64 is a SIP Audio and Video Door Phone specially developed for the needs of users in the security industry. It has the advantages of high reliability and high-quality audio/video. It integrates intelligent security and audio and video access control into one. Can provide users with quality access control security and communication intercom services.

5 Install Guide

5.1 Use POE or external Power Adapter

i61&i62&i63&i64 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 a POE switch and power adapter at the same time, the power adapter will be used in priority and will switch to POE power supply once it fails.

Please use the power adapter and the POE switch met the specifications to ensure the device work properly.

5.2 Appendix

5.2.1 Common command modes

Table 1- Common command mode

Action behavior	Description
Standby report IP	In standby mode, long press the speed dial button for 3 seconds, there will be a toot sound will 5 seconds, please press the speed dial button once within 5 seconds, the toot sound will stop automatically reporting IP. Note: I63 press the first speed dial button. I64 press the button in the upper right corner  .
Switch network mode	In the standby mode, long-press the speed dial button for 3 seconds and the beep will last for 5 seconds. Within 5 seconds, press the speed dial button three times quickly to switch to the network mode. If there is no IP at present, switch to the default static IP (192.168.1.128). Then switch to DHCP mode when it is the default static IP (192.168.1.128) When DHCP gets to IP, then do not switch and report the IP directly.

	Report the IP after the successful switch.
Voice loop mode	After you press the speeddial button twice, the device enters the voice loopback mode. After you press the MIC speaker, you can check the voice related problems. After you press the speeddial button again, you can exit the voice loopback mode

5.2.2 LED status

i61 and i62 indicators have the same position and behavior

Table 2 - i61&i62 LED status

Type	Indicator status	Indicator status
LED light	Steady green	Standby (No registration, normal network)
	Steady cyan	Registration success
	Cyan light flash	talking/Calling/going
	Red slow flash	Registration failed
	Red slow flash	Network anomaly
	Orange light flash	Upgrade and restore factory
Card reader indicator light	Steady	Standby
	Flashing 1s	A credit card

i63 has five key indicators, the same color in each state

Table 3 - i63 LED status

Type	Indicator status	Status indicators
LED light	Steady green	Standby (No registration, normal network)
	Steady cyan	Registration success
	Cyan light flash	talking/Calling/going
	Red slow flash	Registration failed
	Red slow flash	Network anomaly
	Orange light flash	Upgrade and restore factory
Card reader indicator light	Steady	Standby
	Flashing 1s	A credit card

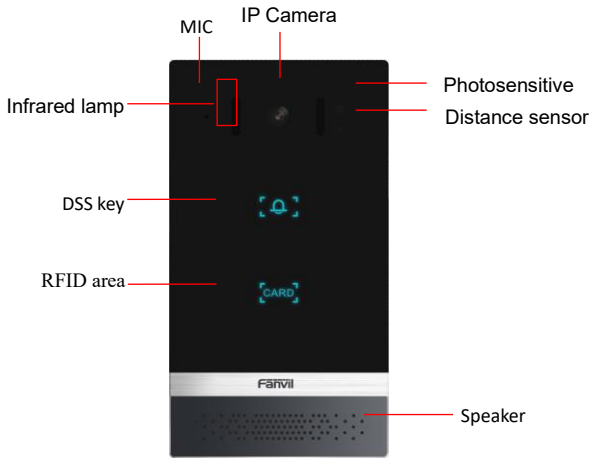
i64 has a status indicator. The color of keyboard backlight does not change according to device status.

Table 4 - i64 LED status

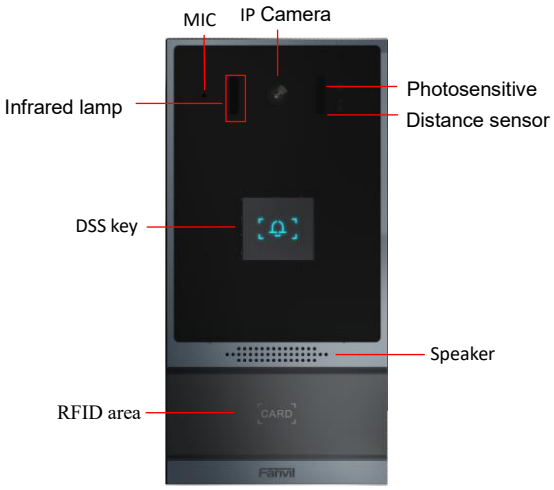
Type	Indicator status	Indicator status
LED light	Steady green	Standby (No registration, normal network)
	Steady cyan	Registration success
	Cyan light flash	talking/Calling/going
	Red slow flash	Registration failed
	Red slow flash	Network anomaly
	Orange light flash	Upgrade and restore factory
Card reader indicator light	Steady	Standby
	Flashing 1s	A credit card

6 User Guide

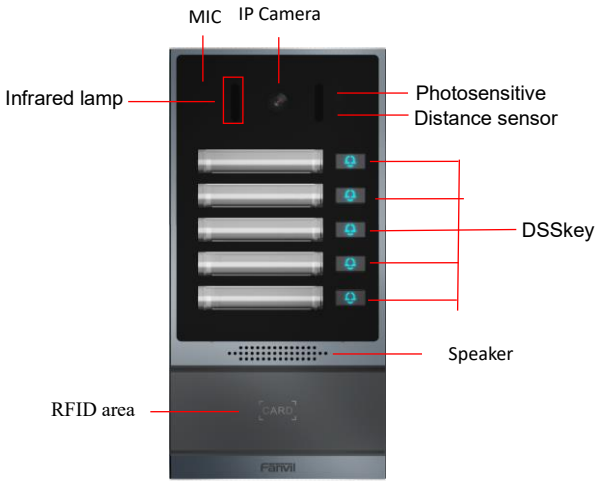
6. 1 Interface description



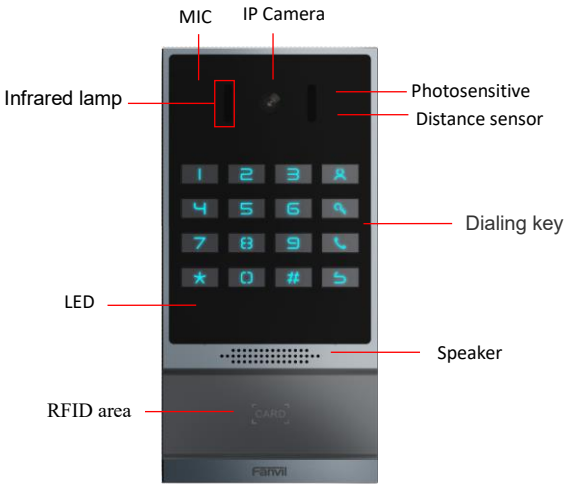
Picture 1 - i61 Panel



Picture 2 - i62 Panel



Picture 3 - i63 Panel



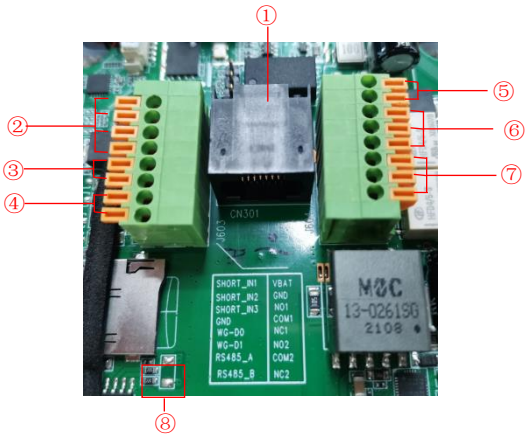
Picture 4 - i64 Panel

Table 5 - Panel introduction

Number	Name	Description
1	IP Camera Infrared lamp	Video signal acquisition and transmission
2	MIC	Audio acquisition
3	DSS key	For speed dial, multicast, intercom, IP broadcast and other functions
4	RFID area	Identification card
5	Speaker	Play sound
5	Photosensitive	Difficulty of sensing light
7	Distance sensor	The distance between the sensing device and the object

6.2 Interface description

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



Picture 5 - Interface

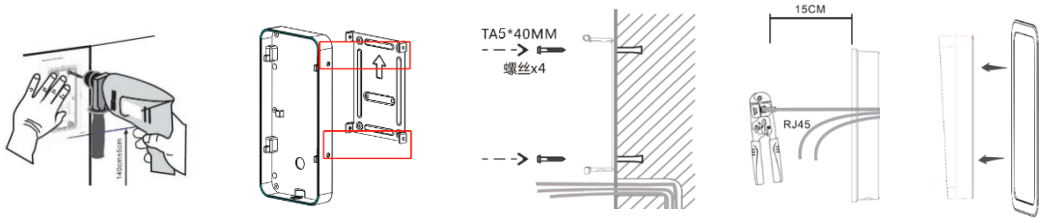
Table 6 - Interface

SN	Description
①	Ethernet interface: standard RJ45 interface, 10/100M adaptive, it is recommended to use five or five types of network cable
②	Two groups of short-circuit input detection interfaces: for connecting switches, infrared probes, door magnets, vibration sensors and other input devices
③	Wiggins interface
④	RS485 interface
⑤	Power interface: 12V/1A input，UP-positive electrode，DOWN-negative electrode
⑥、⑦	Two groups of short-circuit output control interface: used to control electric locks, alarms, etc.
⑧	Line out interface，accessibility aids for the deaf

6.3 Installation instructions

6.3.1 Installation

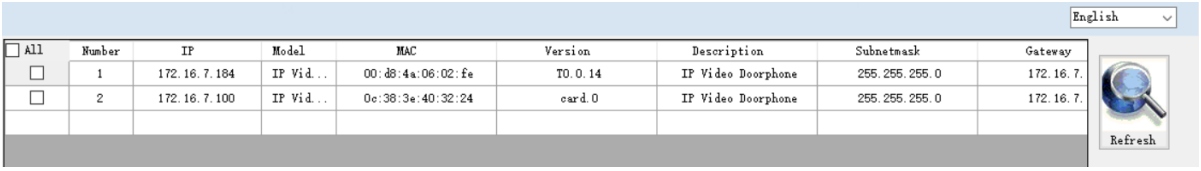
1. Draw the installation holes on the wall according to the installation dimension drawing provided by the equipment, use an electric drill to make the vacant place, after drilling the hole, remove the installation dimension drawing, and use a hammer to drive the plastic plug into the drilled hole;
2. Use a screwdriver to loosen the 4 screws on the back, separate the back shell from the wall bracket, and lock the screws on the back of the device at the same time;
3. Align the screw holes of the wall bracket with the holes made on the wall, and fix it to the wall with the supplied screws;
4. Pass all the wires through the silicone plug in the middle of the bottom shell. All wires need to reserve a length of 15-20cm.
5. Hang the device and the wall bracket tightly from top to bottom, and tighten the screws at the bottom



Picture 6 - Installation

6.3.2 Device IP address

Method 1:
Open the iDoorPhone Network Scanner. Press the Refresh button to search the device and find the IP address.



Method 2:
Connect the speaker, touch and hold the speed-dial button for 3 seconds (30 seconds after power on), wait for the speaker to beep. Press the speed-dial button within 5 seconds, and the system will automatically announce the IP address by voice.

Method 3：

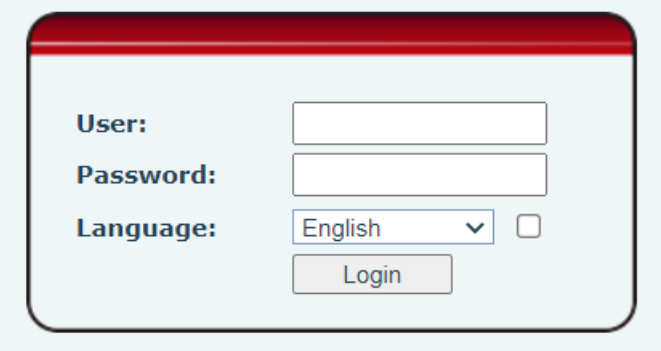
Touch and hold the speed-dial button for 3 seconds, wait for the speaker to beep, press the speed-dial button three times within 5 seconds, and the system will automatically announce the IP address by voice after successfully switching to the network mode.

Table 7 - Configuration instructions

Default configuration			
DHCP mode	**Default enable**	**Static IP**	**192.168.1.128**
Voice read IP address	**Touch and hold the speed-dial button for 3 seconds, press the speed dial button one times within 5 seconds**	**Server port**	**80**

6.4 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 7 - 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

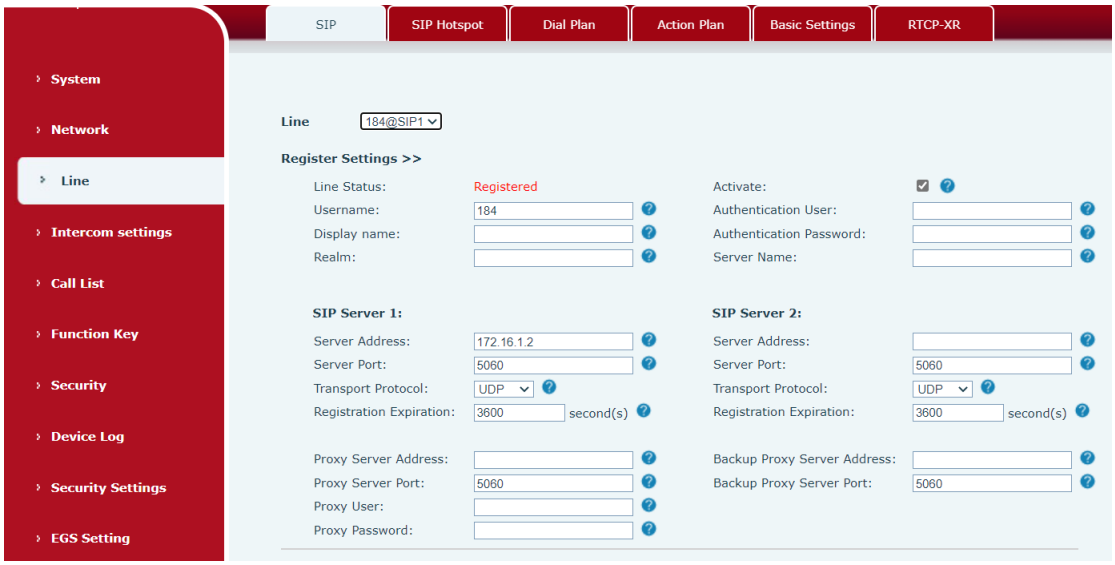
6.5 SIP Configurations

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 8 - SIP Line Configuration

6. 6 Door opening operation

Unlock the door in the following five ways:

1) Open the door by swiping the RFID card, which supports IC card and ID card.
2) The access control helps to call owner, and the owner enters the remote opening password to open the door.
3) The other device helps to call the door phone, enters the corresponding remote authentication code, and opens the door after timeout or the password check length is reached (the authentication code shall be configured in the access list).
4) The door can be opened through the indoor door button when the door phone is in any state.
5) Timed door opening: automatically opens the door in a predetermined time period by setting a timed task.

7 Basic Function

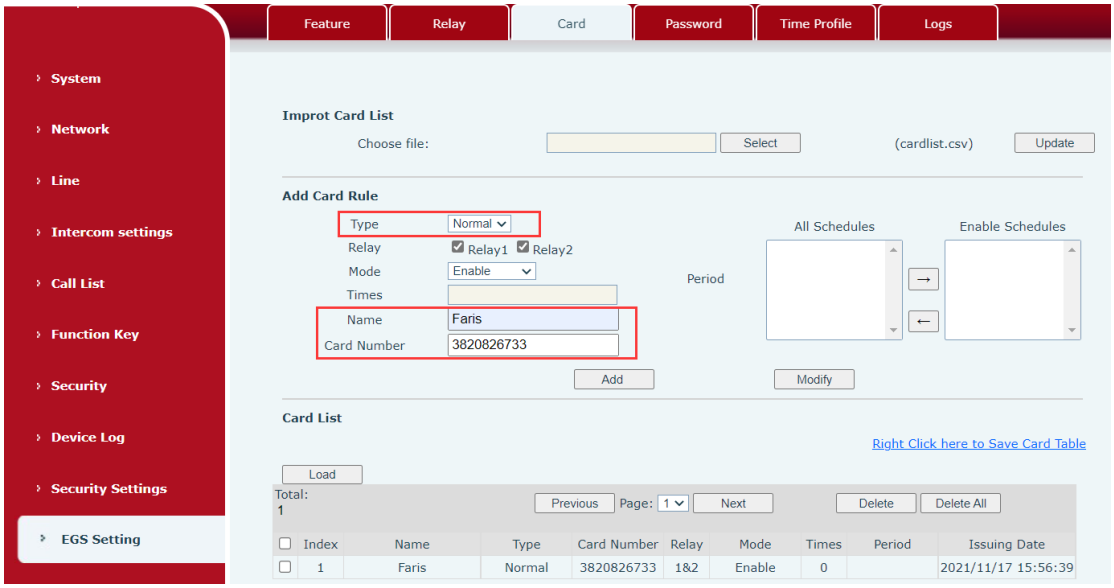
7.1 Swipe to open the door

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

- Entere your name and card number (just enter the first 10 digits of the card number), and clicking "Add" to add the card to the list.

- Access the card reading area of the device through the configured ID card 

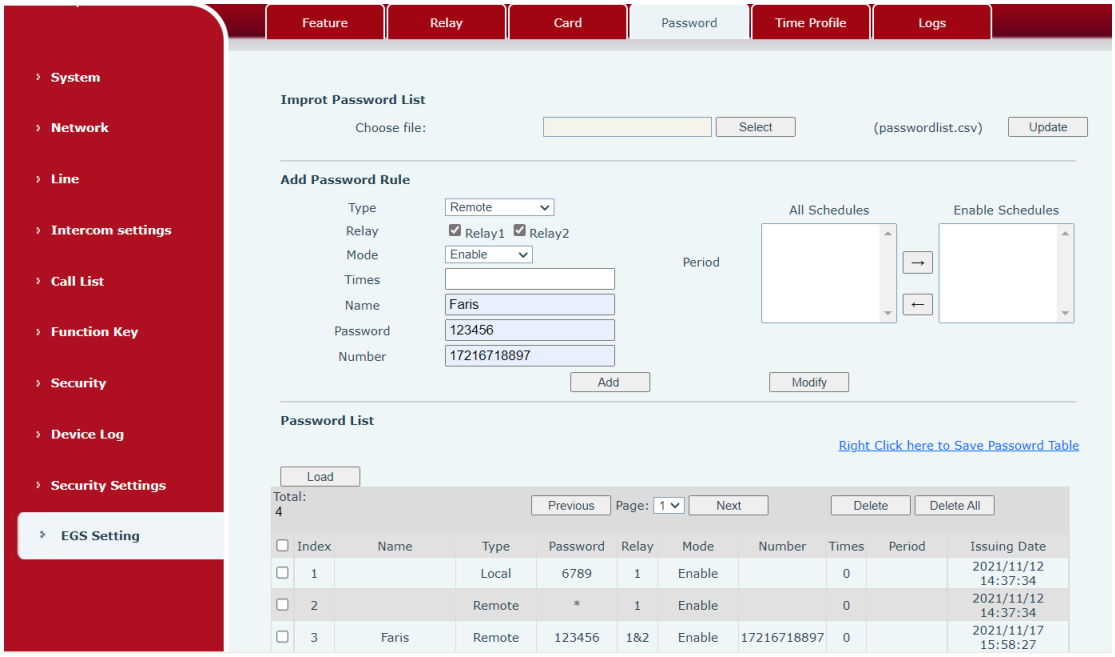
to open the door.



Picture 9 - Card

7.2 Remote Door Opening

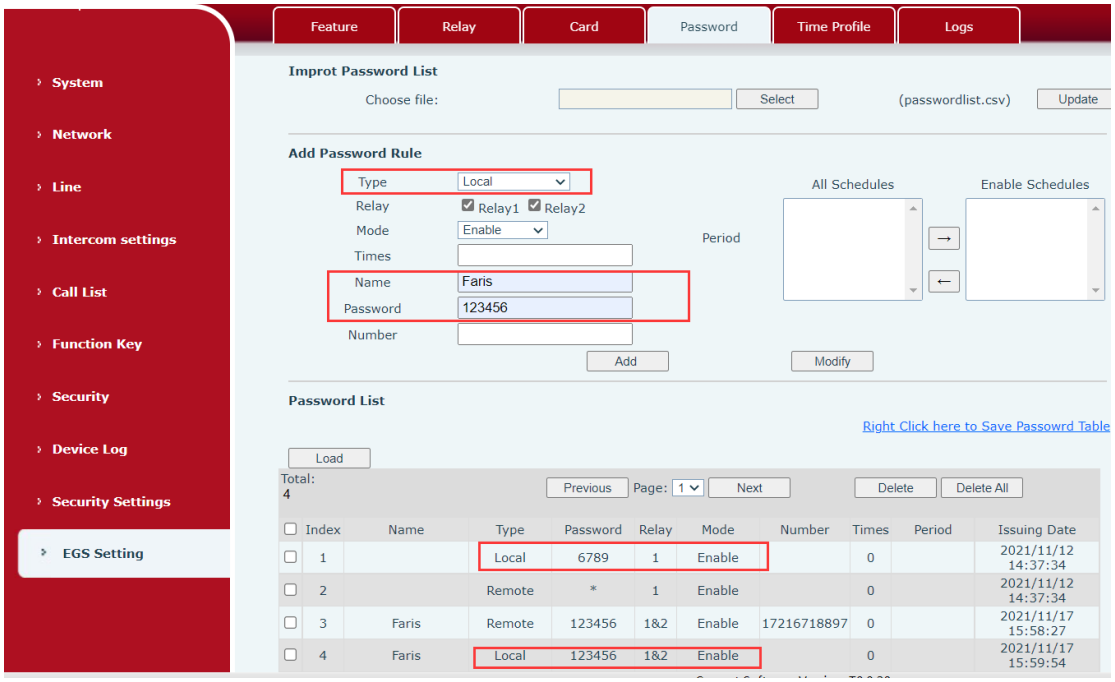
- Set access control on the web page→ EGS Setting→Password→ Add password rule → Select "Remote "
- Enter your name, password and number, add to the password list.
- The owner answers the access control call and presses " * "(default password) or "123456" (new password) to open the door for visitors.



Picture 10 - Remote Door Opening

7.3 Password to Open Door

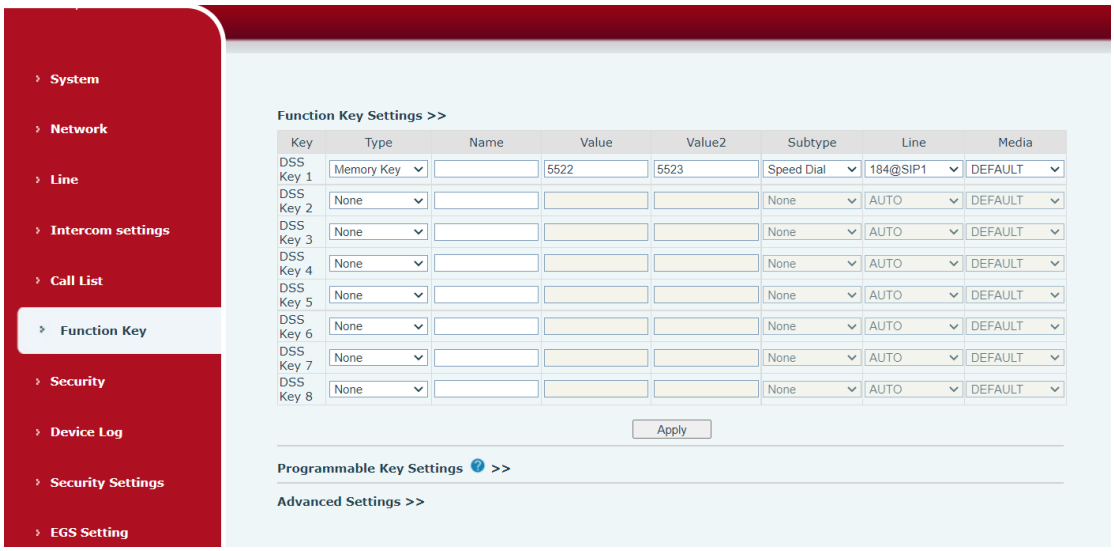
- Configure access on Web→EGS Setting →Password → Add password rule → Select "Local " (only the i64 supports local password access)
- Enter your your name and password password to the password list.
- Owners and visitors can open the door by entering "6789" (default password) or "123456" (new password) by using the keypad.



Picture 11 - Remote Door Opening

7.4 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 12 - Function Setting

See detailed configuration instructions 9.26 Function Key

After setting the speed dial according to the above settings, i64 can directly dial the set number by pressing the management center button  .

You can also press the dial button first  , then enter the number you want to call, and automatically call after timeout.

7.5 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.

7.6 End of the Call

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

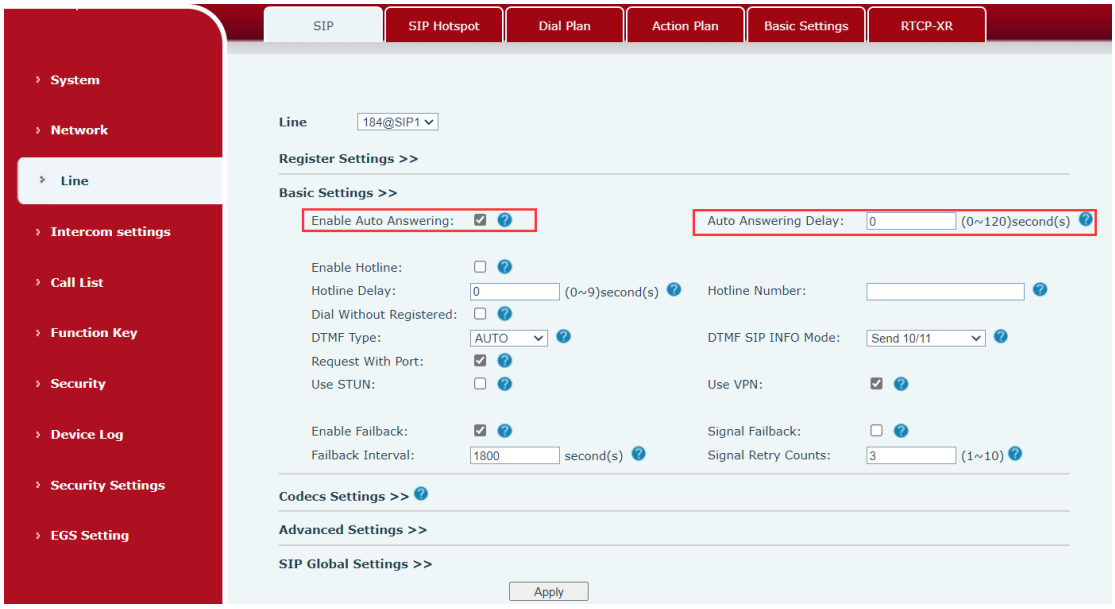
i64 can also use the back button  to hang up the call.

7.7 Auto Answer

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

Web interface:

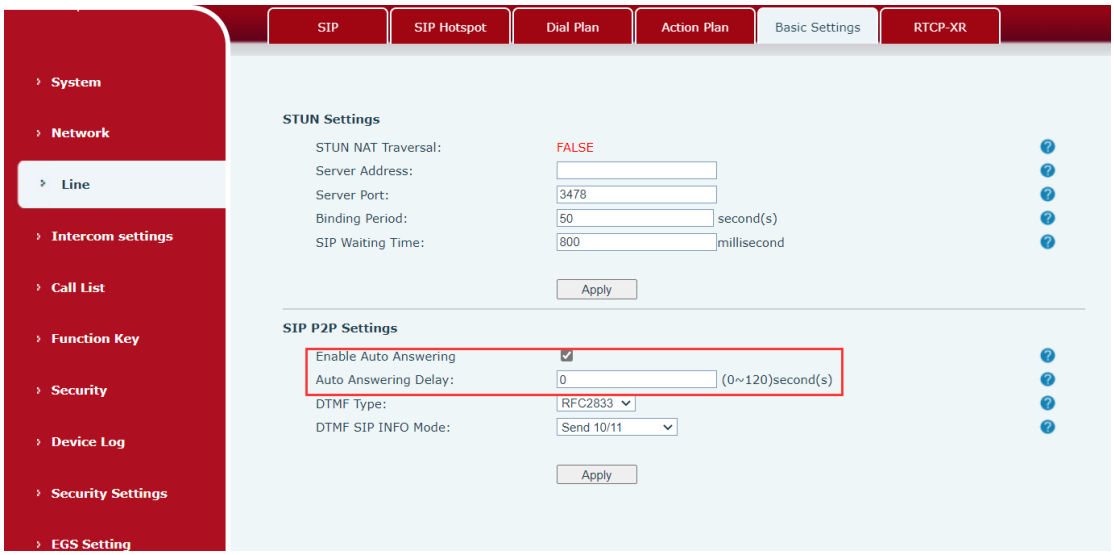
Enter [**Line**] >> [**SIP**], Enable auto answer and set auto answer time and click submit.



Picture 13 - WEB line enable auto answer

SIP P2P auto answering：

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



Picture 14 - Enable auto answer for IP calls

- Auto Answer Timeout（0~120）

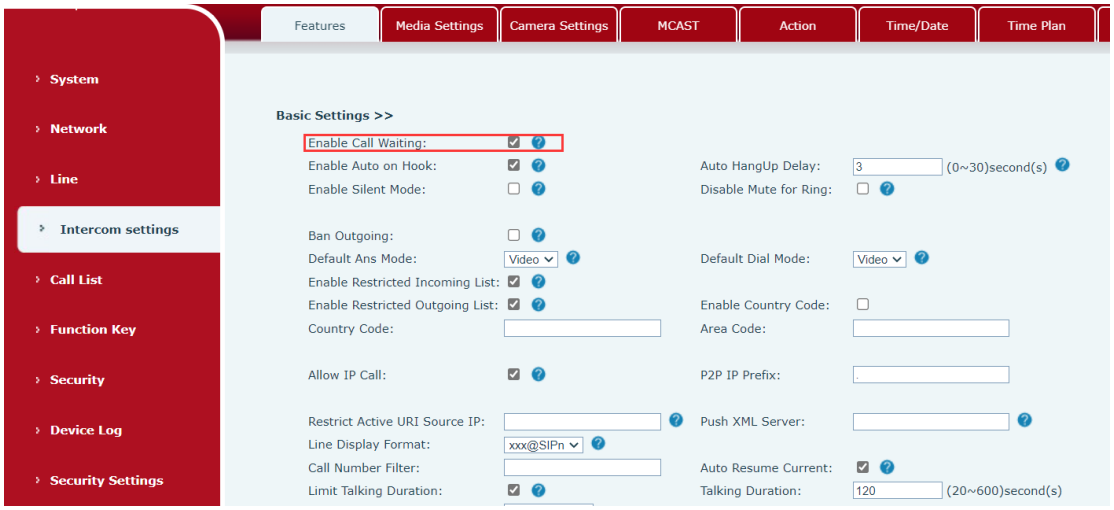
The range can be set to 0~120s, and the call will be answered automatically when the timeout is set.

7.8 Call Waiting

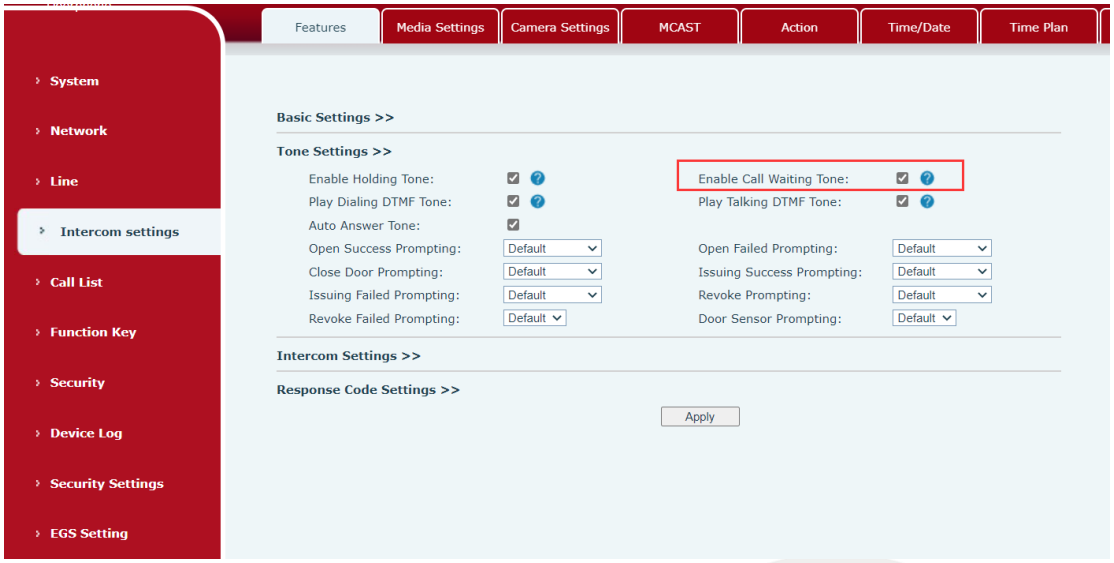
- Enable call waiting: new calls can be accepted during a call.
- Disable call waiting: new calls will be automatically rejected and a busy signal will be prompted.
- Enable call waiting tone: when you receive a new call on the line, the device will beep.

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 15 - Call Waiting

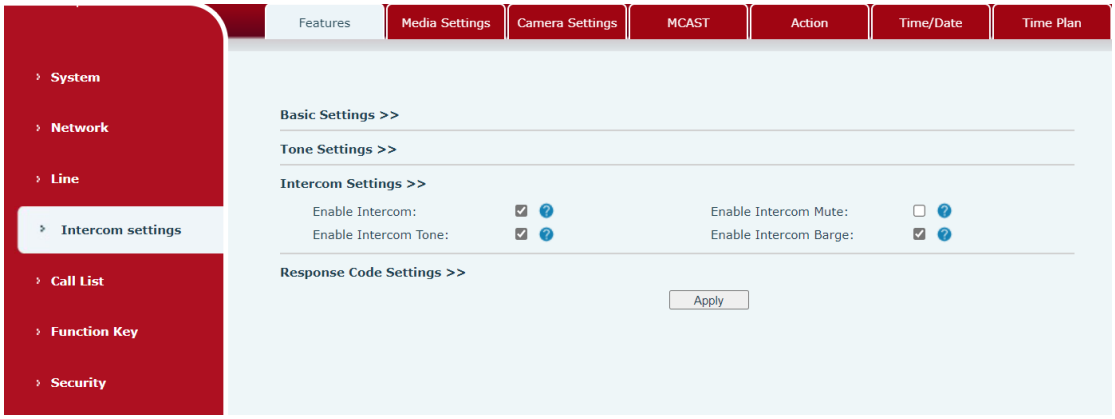


Picture 16 - Call Waiting tone

8 Advance Function

8.1 Intercom

The equipment can answer intercom calls automatically.



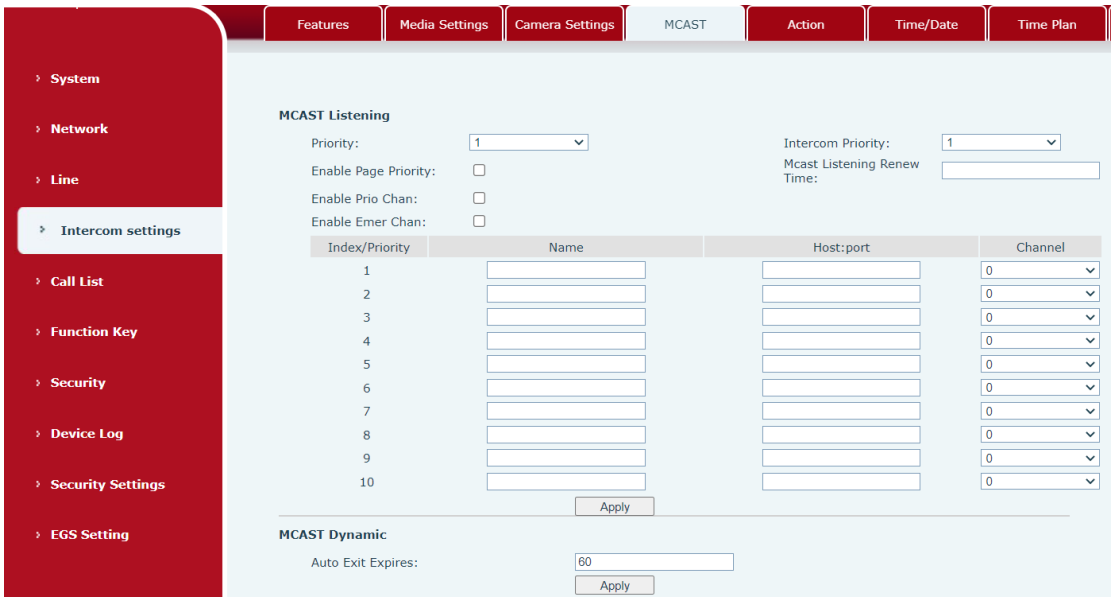
Picture 17 - WEB Intercom

Table 8 - 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, device will answer the intercom call automatically while it is in a normal call, and it will reject new intercom call if there is already one 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 18 - MCAST

Table 9 - 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.

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.

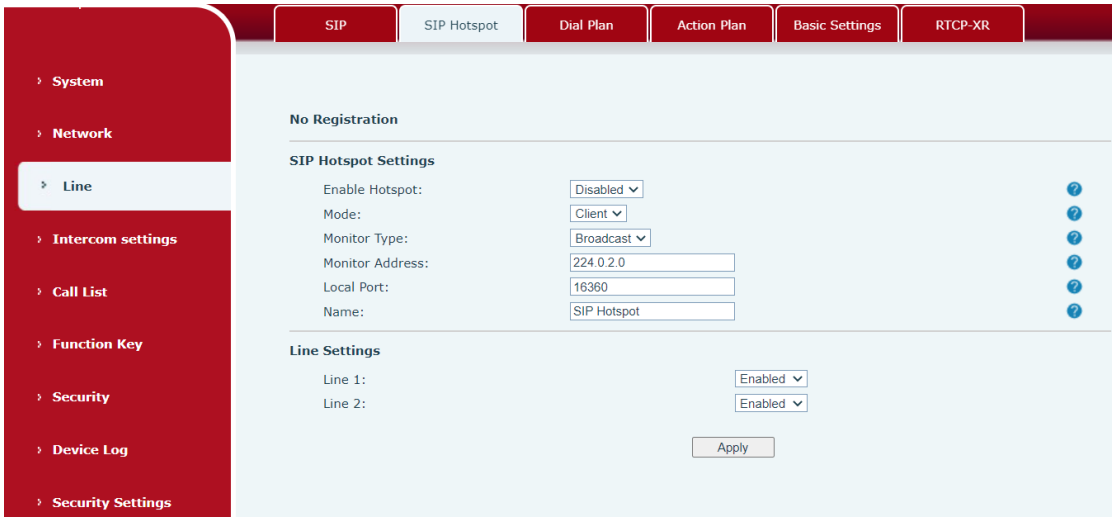
Table 10 - SIP Hotspot

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 19 - 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 lockedIf 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
- Software
- Uptime
- Last uptime
- MEMInfo
- System time

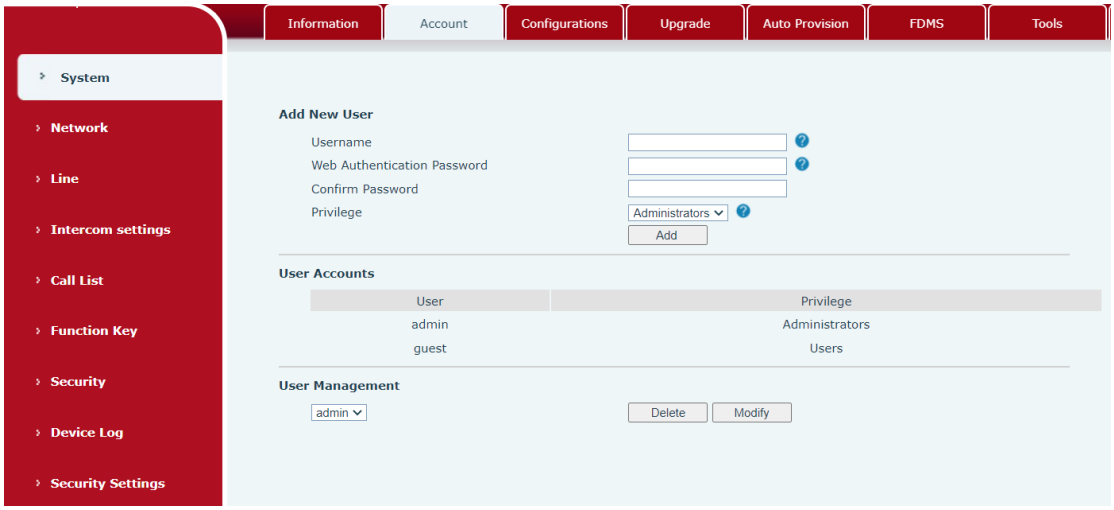
And summarization of network status,

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

Besides, summarization of SIP account status,

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

9.3 System >> Account



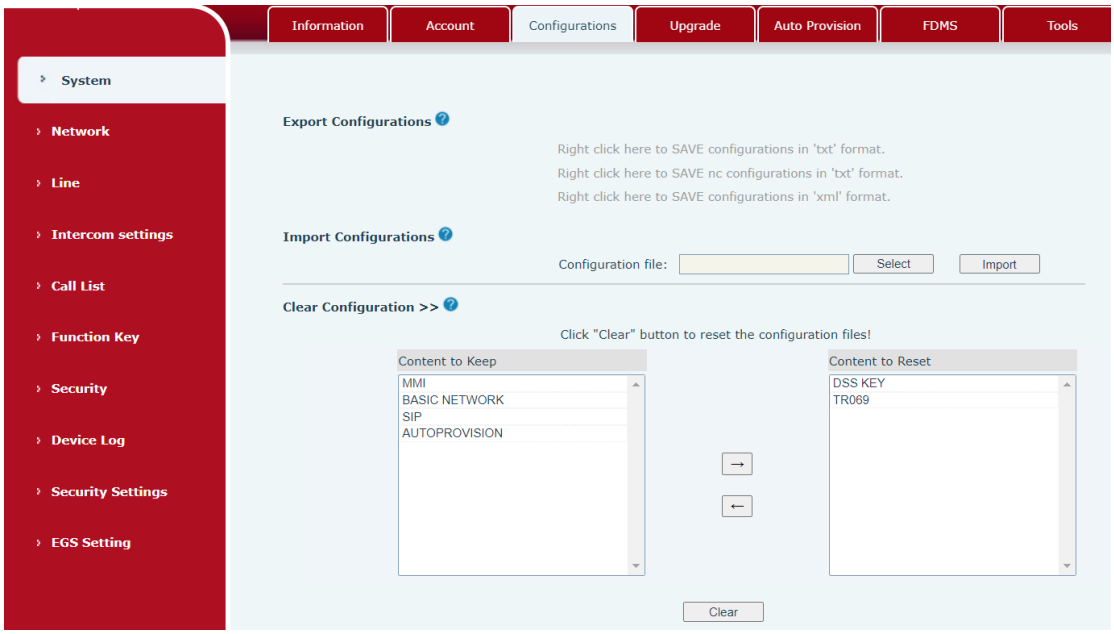
Picture 20 - WEB Account

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 21 - 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

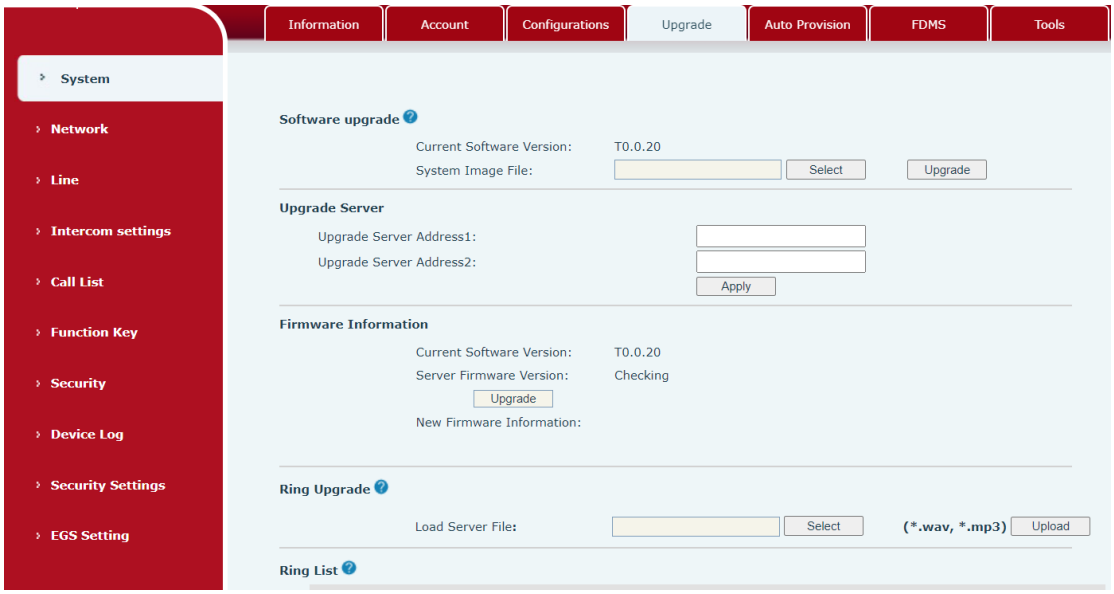
■ **Clear Tables**

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 22 - Upgrade

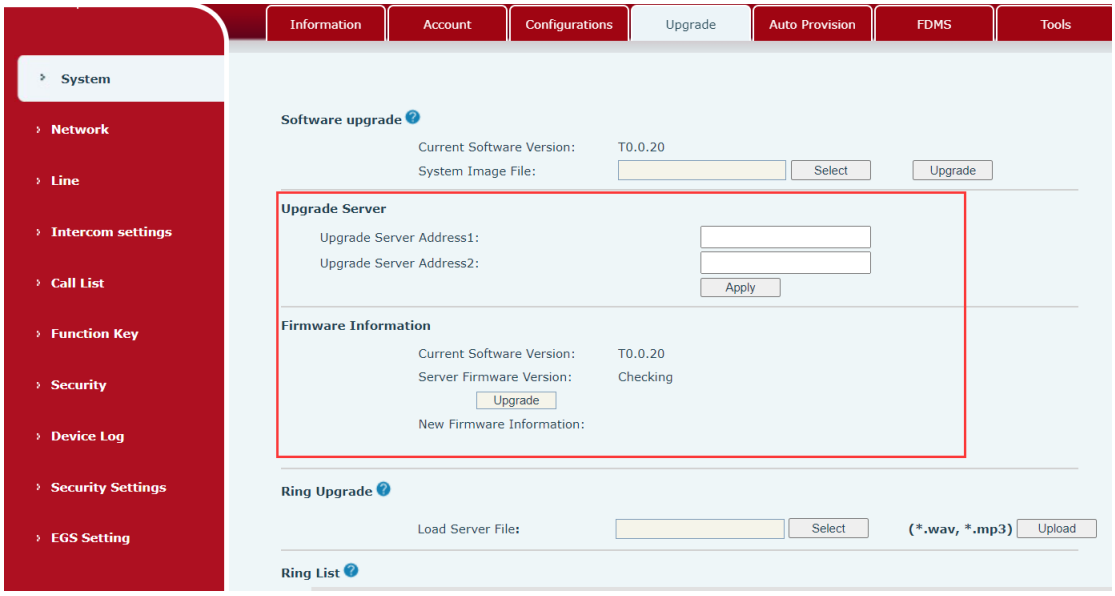
Upgrade the software version of the device, and upgrade to the new version through the webpage. After the upgrade, the device will automatically restart and update to the new version.

Click select, select the version and then click upgrade.

Upgrade the ringtone,support wav and MP3 format.

Firmware Upgrade：

- Web page： Login phone web page, go to [**System**] >> [**Upgrade**].

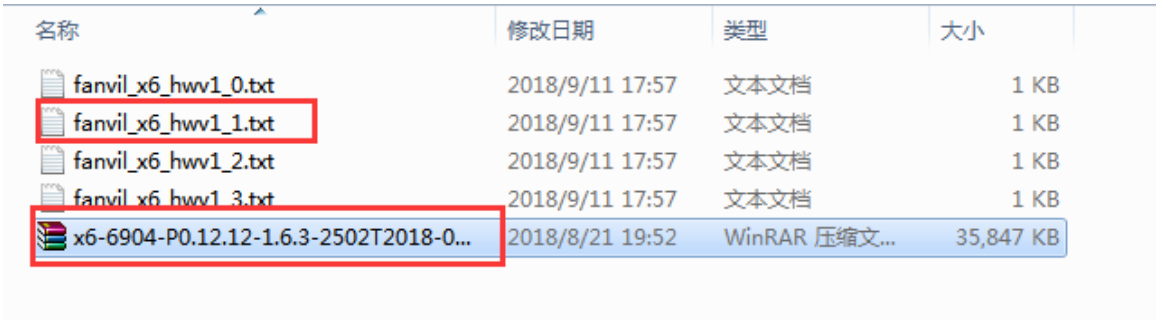


Picture 23 - Web page firmware upgrade

Table 11 - 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.

- 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 server, as shown in the figure:

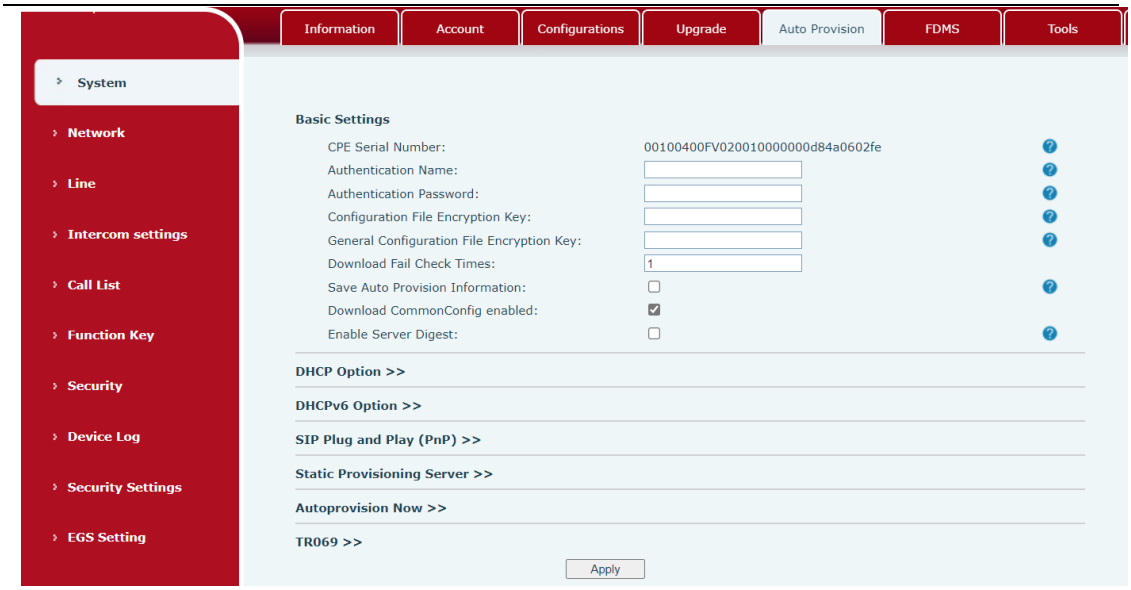


- TXT file format must be UTF-8
- vendor_model_hw10.TXT The file format is as follows：
  Version=1.6.3 #Firmware
  Firmware=xxx/xxx.z #URL，Relative paths are supported and absolute paths are possible, distinguished by the presence of protocol headers.
  BuildTime=2018.09.11 20:00
  Info=TXT|XML

  Xxxxx
  Xxxxx
  Xxxxx
  Xxxxx
- After the interval of update cycle arrives, if the server has available files and versions, the phone will prompt as shown below. Click [view] to check the version information and upgrade.

9.6 System >> Auto Provision

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



Picture 24 - Auto provision settings

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

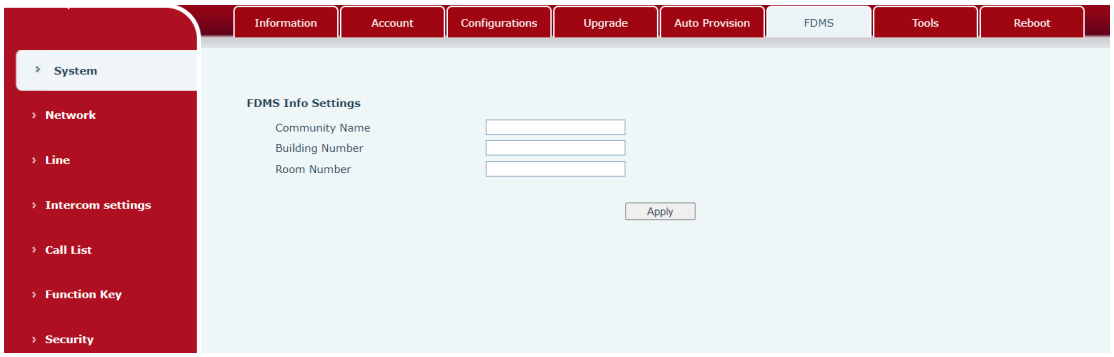
Table 12 - Auto Provision

Auto Provision	
Parameters	**Description**
Basic settings	
CPE Serial Number	Display the device SN
Authentication Name	The user name of provision server
Authentication Password	The password of provision server
Configuration File Encryption Key	If the device configuration file is encrypted , user should add the encryption key here
General Configuration File Encryption Key	If the common configuration file is encrypted, user should add the encryption key here
Save Auto Provision Information	Save the HTTP/HTTPS/FTP user name and password. If the provision URL is kept, the information will be kept.
Download Common Config enabled	Whether phone will download the common configuration file.
Enable Get	When the feature is enable, if the configuration of server is

Digest From Server	changed, phone will download and update.
DHCP Option	
Option Value	Configure DHCP option, DHCP option supports DHCP custom option | DHCP option 66 | DHCP option 43, 3 methods to get the provision URL. The default is Option 66.
Custom Option Value	Custom Option value is allowed from 128 to 254. The option value must be same as server define.
Enable DHCP Option 120	Use Option120 to get the SIP server address from DHCP server.
DHCPv6 Option	
Option Value	Configure DHCPv6 option, DHCPv6 option supports custom option | option 66 | option 43, 3 methods to get the provision URL. The default is Disable.
Custom Option Value	Custom option number. Must be from 128 to 254.
Enable DHCP 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 enabled, 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	Provisioning server address. Support both IP address and domain address.
Configuration File Name	The configuration file name. If it is empty, phone will request the common file and device file which is named as its MAC address. The file name could be a common name, $mac.cfg, $input.cfg. The file format supports CFG/TXT/XML.
Protocol Type	Transferring protocol type ， supports FTP、TFTP、HTTP and HTTPS
Update Interval	Configuration file update interval time. As default it is 1, means phone will check the update every 1 hour.
Update Mode	Provision Mode. 1. Disabled. 2. Update after reboot. 3. Update after interval.

Static Provisioning Server	
TR069	
Enable TR069	Enable TR069 after selection
ACS Server Type	There are 2 options Serve type, common and CTC.
ACS Server URL	ACS server address
ACS User	ACS server username (up to is 59 character)
ACS Password	ACS server password (up to is 59 character)
Enable TR069 Warning Tone	If TR069 is enabled, there will be a prompt tone when connecting.
TLS Version	TLS Version
STUN server address	Enter the STUN address
Enable the STUN	Enable the STUN

9. 7 System >> FDMS



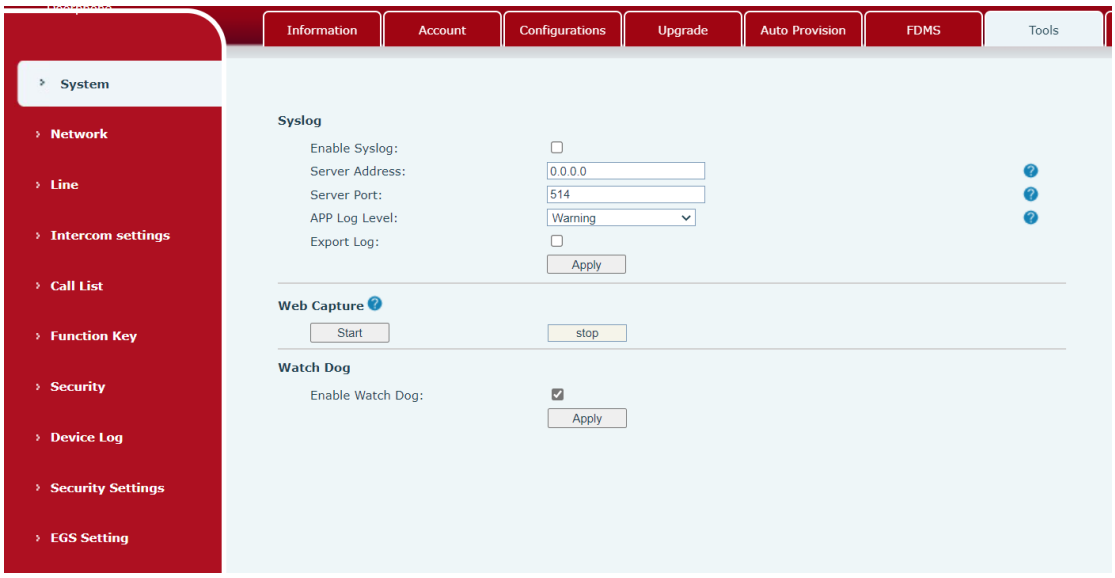
Picture 25 - FDMS

Table 13 - 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.

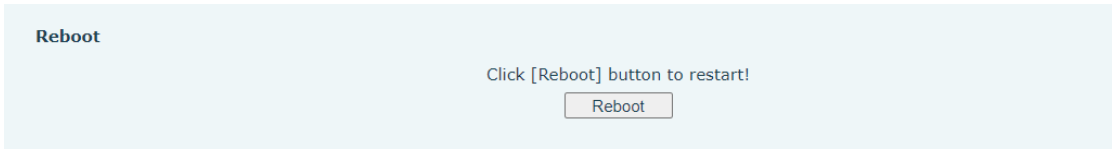


Picture 26 - Tools

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 technical support.

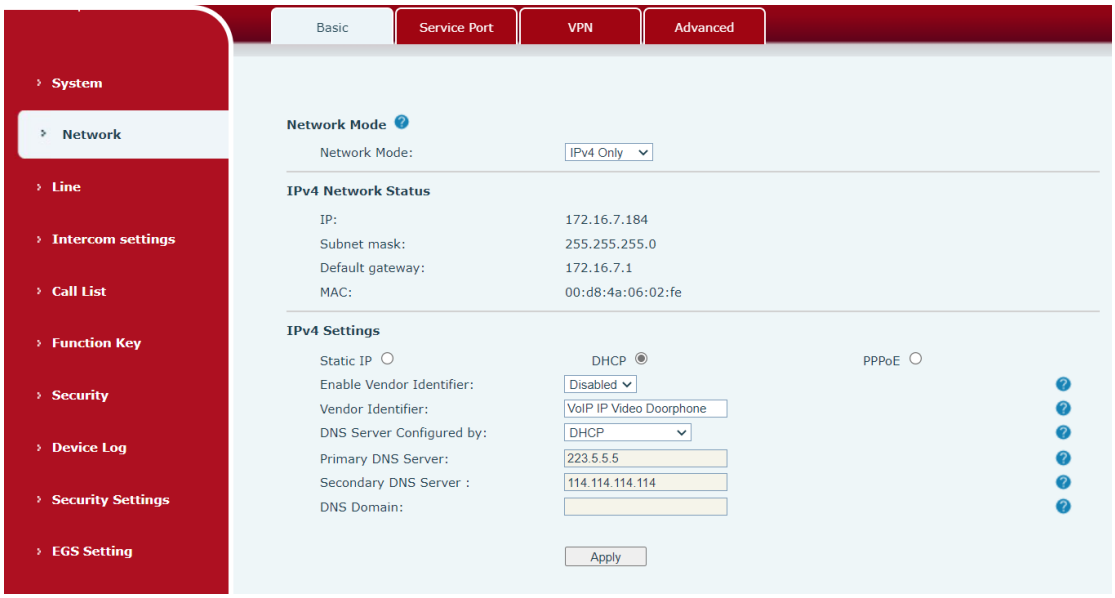
9.9 System >> Reboot

This page can restart the device.



9.10 Network >> Basic

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



Picture 27 - Network Basic Setting

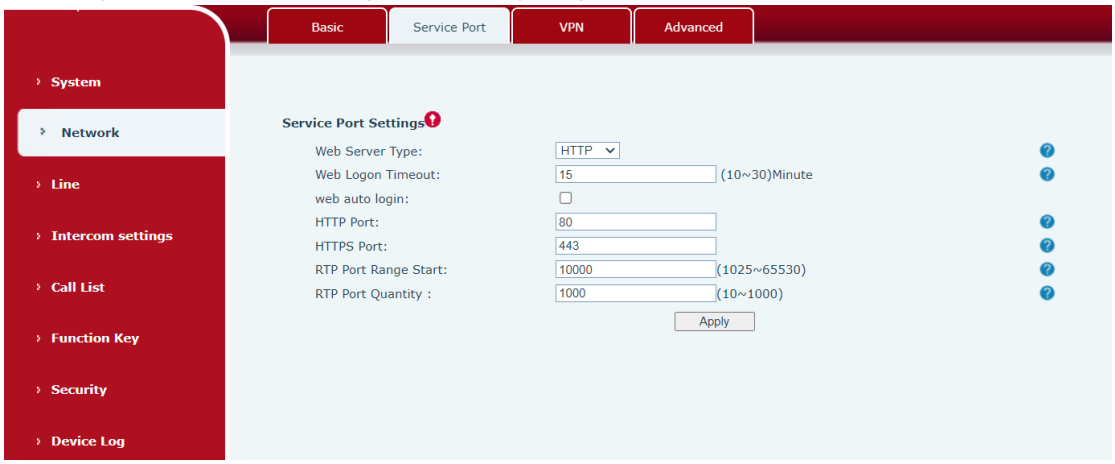
Table 14 - Network Basic Setting

Field Name	Explanation
IPv4 Network Status	
IP	The current IP address of the equipment
Subnet mask	The current Subnet Mask
Default gateway	The current Gateway IP address
MAC	The MAC address of the equipment
IPv4 Settings	
Settings	
Select the appropriate network mode. The equipment supports three network modes:	
Static IP	Network parameters must be entered manually and will not be changed. All parameters are provided by the ISP.
DHCP	Network parameters are provided automatically by a DHCP server.
If Static IP is chosen, the screen below will appear. Enter values provided by the ISP.	
DNS Server Configured by	Select the Configured mode of the DNS Server.
Primary DNS Server	Enter the server address of the Primary DNS.
Secondary DNS Server	Enter the server address of the Secondary DNS.
DNS Domain	Enter the domain of the DNS.
attention： 1）After setting the parameters, click【Apply】to take effect.	

2）If you change the IP address, the webpage will no longer 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

9.11 Network >> service port

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

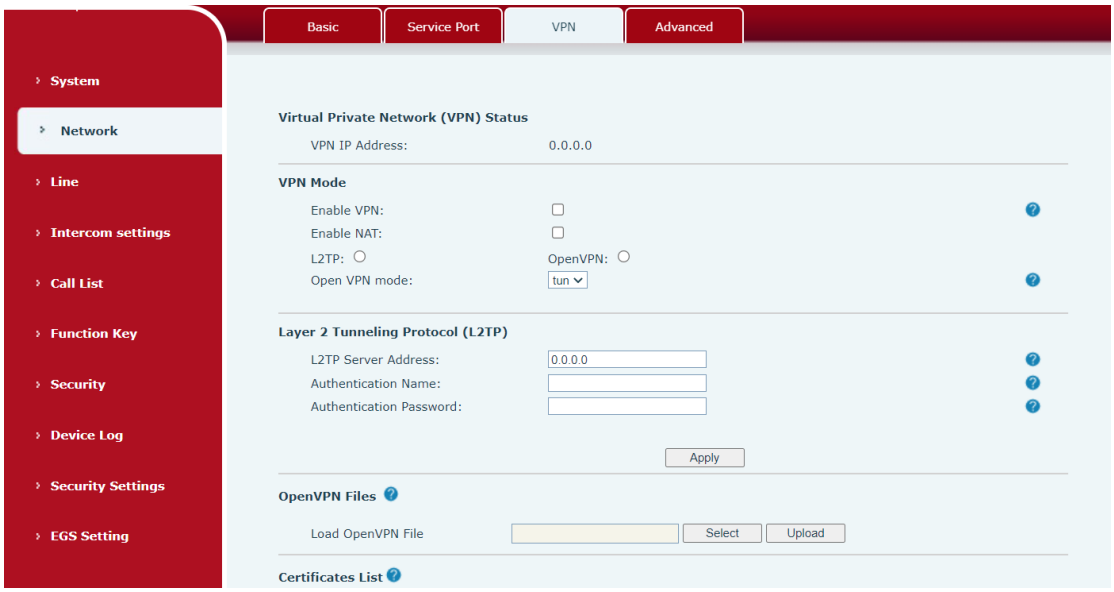


Picture 28 - Service port setting interface

Table 15 - 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

9.12 Network >> VPN



Picture 29 - Network VPN Settings

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

- **OpenVPN**

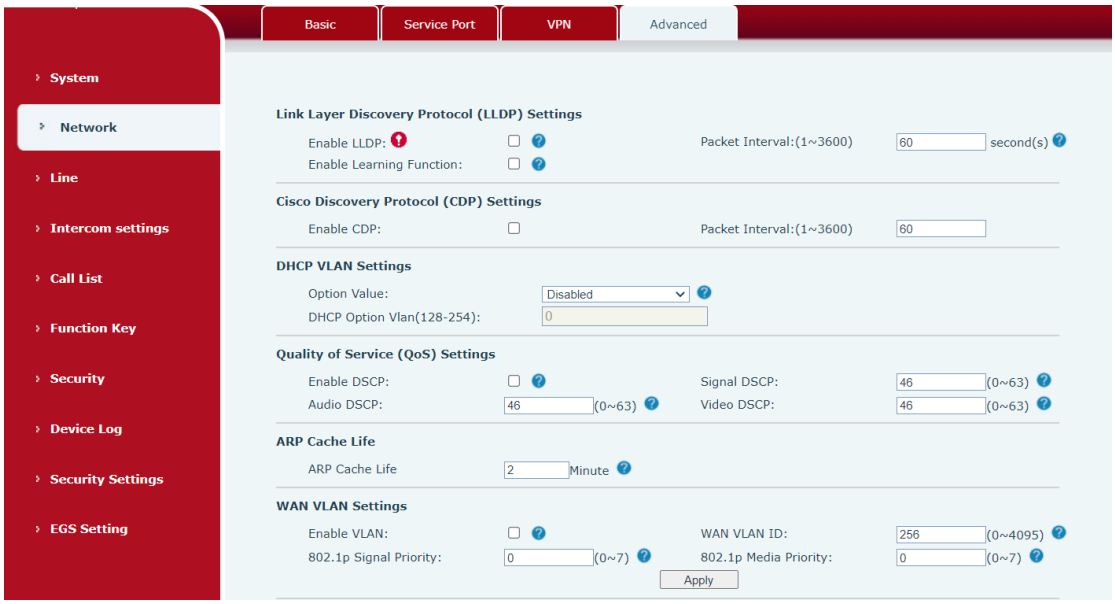
To establish an OpenVPN connection, user should get the following authentication and configuration files from the OpenVPN hosting provider and name them as the following,

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.

9.13 Network >> Advanced



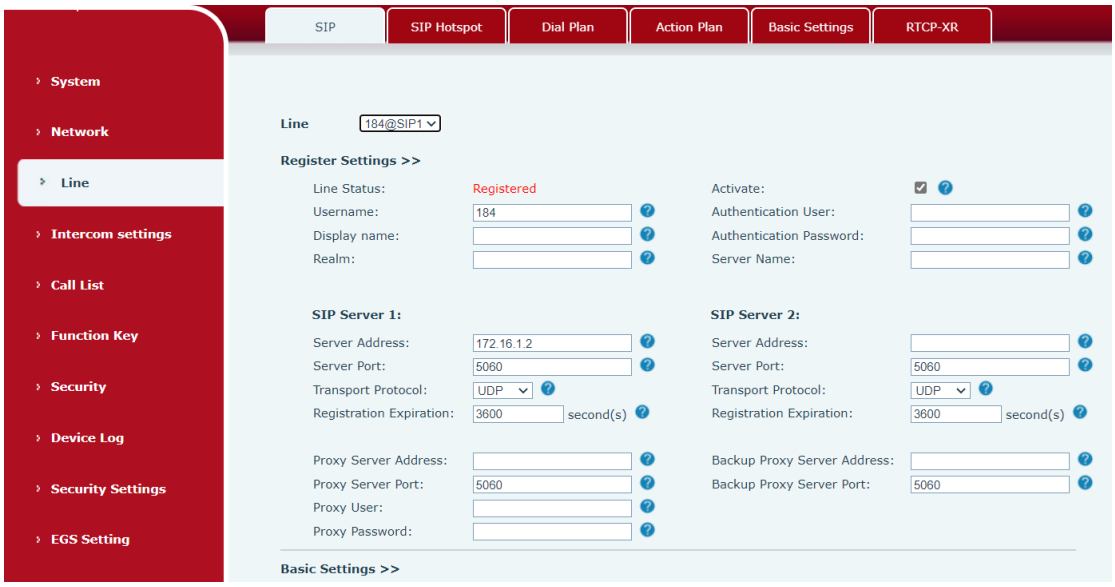
Picture 30 - Network Setting

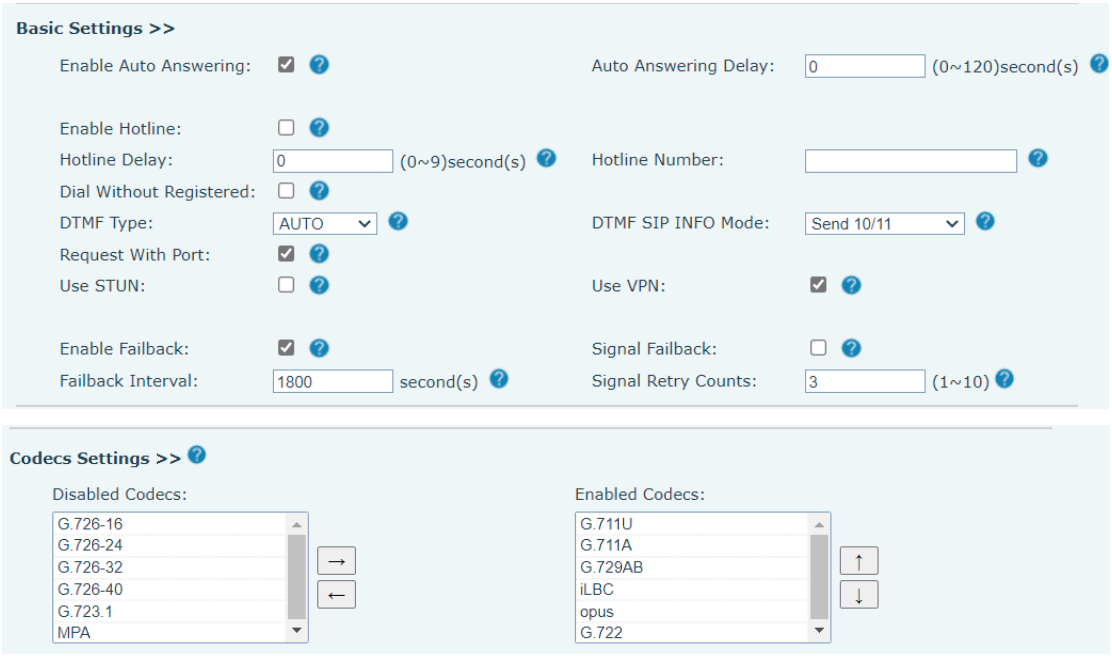
Network advanced Settings are typically configured by IT administrators to improve the quality of device service.

Table 16 - 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. 14 Line >> SIP





Picture 31 - SIP

Table 17 - SIP

Parameters	Description
Register Settings	
Line Status	Display the current line status at page loading. To get the up to date line status, user has to refresh the page manually.
Activate	Whether the service of the line should be activated
Username	Enter the username of the service account.
Authentication User	Enter the authentication user of the service account
Display Name	Enter the display name to be sent in a call request.
Authentication Password	Enter the authentication password of the service account
Realm	Enter the SIP domain if requested by the service provider
Server Name	Input server name.
SIP Server 1	
Server Address	Enter the IP or FQDN address of the SIP server
Server Port	Enter the SIP server port, default is 5060
Transport Protocol	Set up the SIP transport line using TCP or UDP or TLS.
Registration Expiration	Set SIP expiration date.
SIP Server 2	
Server Address	Enter the IP or FQDN address of the SIP server
Server Port	Enter the SIP server port, default is 5060
Transport Protocol	Set up the SIP transport line using TCP or UDP or TLS.

Registration Expiration	Set SIP expiration date.
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server.
Proxy Server Port	Enter the SIP proxy server port, default is 5060.
Proxy User	Enter the SIP proxy user.
Proxy Password	Enter the SIP proxy password.
Backup Proxy Server Address	Enter the IP or FQDN address of the backup proxy server.
Backup Proxy Server Port	Enter the backup proxy server port, default is 5060.
Basic Settings	
Enable Auto Answering	Enable auto-answering, the incoming calls will be answered automatically after the delay time
Auto Answering Delay	Set the delay for incoming call before the system automatically answered it
Enable Hotline	Enable hotline configuration, the device will dial to the specific number immediately at audio channel opened by off-hook handset or turn on hands-free speaker or headphone
Hotline Delay	Set the delay for hotline before the system automatically dialed it
Hotline Number	Set the hotline dialing number
Dial Without Registered	Set call out by proxy without registration
Enable Missed Call Log	If enabled, the phone will save missed calls into the call history record.
DTMF Type	Set the DTMF type to be used for the line
Use VPN	Set the line to use VPN restrict route
Use STUN	Set the line to use STUN for NAT traversal
Enable Failback	Whether to switch to the primary server when it is available.
Failback Interval	A Register message is used to periodically detect the time interval for the availability of the main Proxy.
Signal Failback	Multiple proxy cases, whether to allow the invite/register request to also execute failback.
Signal Retry Counts	The number of attempts that the SIP Request considers proxy unavailable under multiple proxy scenarios.
Codecs Settings	Set the priority and availability of the codecs by adding or remove them from the list.
Advanced Settings	
Use Feature Code	When this setting is enabled, the features in this section will not be handled by the device itself but by the server instead. In order to control the enabling of the features, the device will send feature code to the server by dialing the number specified in

	each feature code field.
Enable Blocking Anonymous Call	Set the feature code to dial to the server
Disable Blocking Anonymous Call	Set the feature code to dial to the server
Call Waiting On Code	Set the feature code to dial to the server
Call Waiting Off Code	Set the feature code to dial to the server
Send Anonymous on Code	Set the feature code to dial to the server
Send Anonymous Off Code	Set the feature code to dial to the server
Enable Session Timer	Set the line to enable call ending by session timer refreshment. The call session will be ended if there is not new session timer event update received after the timeout period
Session Timeout	Set the session timer timeout period
BLF Server	The registered server will receive the subscription package from ordinary application of BLF phone. Please enter the BLF server, if the sever does not support subscription package, the registered server and subscription server will be separated.
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole opened
Keep Alive Interval	Set the keep alive packet transmitting interval
Keep Authentication	Keep the authentication parameters from previous authentication
Blocking Anonymous Call	Reject any incoming call without presenting caller ID
User Agent	Set the user agent, the default is Model with Software Version.
Specific Server Type	Set the line to collaborate with specific server type
SIP Version	Set the SIP version
Anonymous Call Standard	Set the standard to be used for anonymous
Local Port	Set the local port
Ring Type	Set the ring tone type for the line
Enable user=phone	Sets user=phone in SIP messages.
Use Tel Call	Set use tel call
Auto TCP	Using TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes

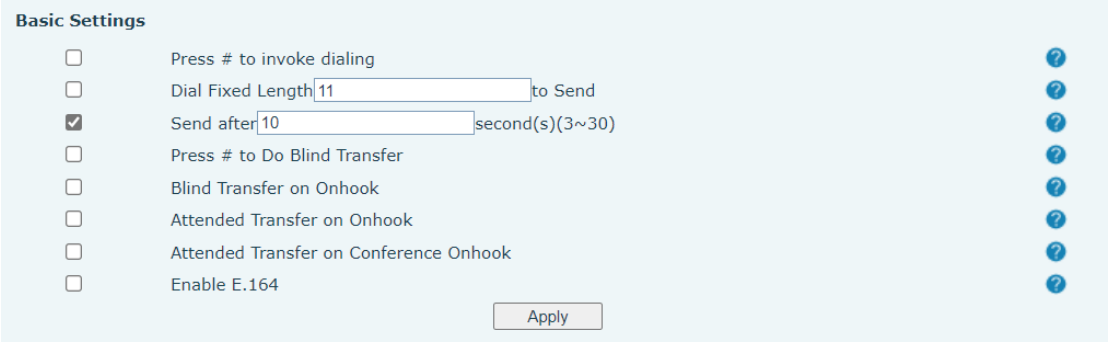
Enable Rport	Set the line to add rport in SIP headers
Enable PRACK	Set the line to support PRACK SIP message
DNS Mode	Select DNS mode, A, SRV, NAPTR
Enable Long Contact	Allow more parameters in contact field per RFC 3840
Enable Strict Proxy	Enables the use of strict routing. When the phone receives packets from the server，it will use the source IP address, not the address in via field.
Convert URI	Convert not digit and alphabet characters to %hh hex code
Use Quote in Display Name	Whether to add quote in display name, i.e. “VoIP” vs VoIP
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)
Sync Clock Time	Time Sync with server
Enable Inactive Hold	With the post-call hold capture package enabled, you can see that in the INVITE package, SDP is inactive.
Caller ID Header	Set the Caller ID Header
Use 182 Response for Call waiting	Set the device to use 182 response code at call waiting response
Enable Feature Sync	Feature Sync with server
Enable SCA	Enable/Disable SCA (Shared Call Appearance)
CallPark Number	Set the CallPark number.
Server Expire	Set the timeout to use the server.
TLS Version	Choose TLS Version.
uaCSTA Number	Set uaCSTA Number.
Enable Click to Talk	With the use of special server, click to call out directly after enabling.
Enable Chgport	Whether port updates are enabled.
Intercom Number	Set Intercom Number.
Unregister On Boot	Whether to enable logout function.
Enable MAC Header	Whether to open the registration of SIP package with user agent with MAC or not.
Enable Register MAC Header	Whether to open the registration is user agent with MAC or not.
PTime(ms)	Set whether to bring ptime field, default no.
SIP Global Settings	
Strict Branch	Set up to strictly match the Branch field.
Enable Group	Set open group.
Enable RFC4475	Set to enable RFC4475.
Enable Strict UA Match	Enable strict UA matching.
Registration Failure Retry Time	Set the registration failure retry time.

Local SIP Port	Modify the phone SIP port.
Enable uaCSTA	Set to enable the uaCSTA function.

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.

9.16 Line >> Dial Plan

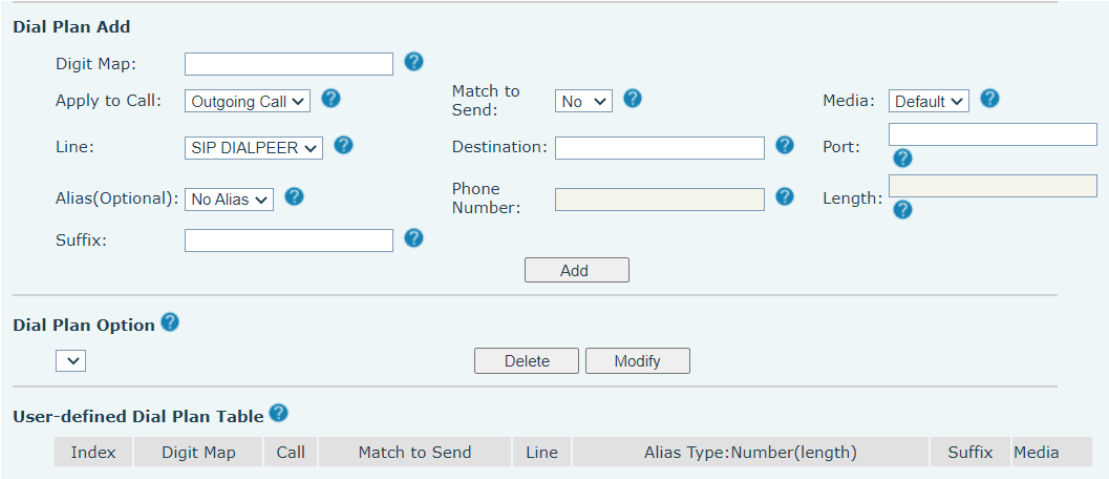


Picture 32 - Dial Plan

Table 18 - Phone 7 dialing methods

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

Dial Plan Add:



Picture 33 - Custom setting of dial - up rules

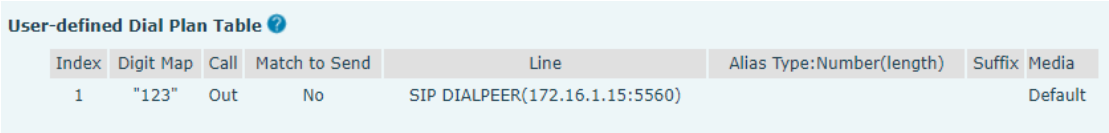
Table 19 - Dial - up rule configuration table

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

Suffix	Characters to be added at the end of the phone number. It is an optional item.
Length	Set the number of characters to be deleted. For example, if this is set to 3, the phone will delete the first 3 digits of the phone number. It is an optional item.

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

Example 1: All Substitution -- Assume that it is desired to place a direct IP call to IP address 172.168.2.208. Using this feature, 123 can be substituted for 172.168.2.208.



User-defined Dial Plan Table

Index	Digit Map	Call	Match to Send	Line	Alias Type:Number(length)	Suffix	Media
1	"123"	Out	No	SIP DIALPEER(172.16.1.15:5560)			Default

Picture 34 - Dial rules table (1)

Example 2: Partial Substitution -- To dial a long-distance call to Beijing requires dialing area code 010 before the local phone number. Using this feature 1 can be substituted for 010. For example, to call 62213123 would only require dialing 162213123 instead of 01062213123.

User-defined Dial Plan Table

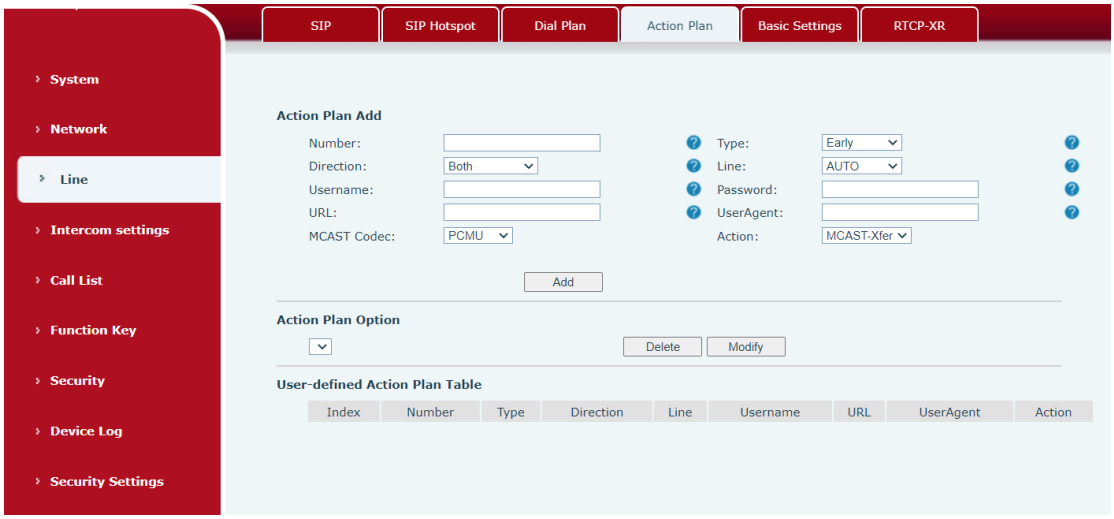
Index	Digit Map	Call	Match to Send	Line	Alias Type:Number(length)	Suffix	Media
1	"1T"	Out	No	Fanvil@SIP1	rep:010(1)		Default

Picture 35 - Dial rules table (2)

Example 3: Addition -- Two examples are shown. In the first case, it is assumed that 0 must be dialed before any 11-digit number beginning with 13. In the second case, it is assumed that 0 must be dialed before any 11-digit number beginning with 135, 136, 137, 138, or 139. Two different special characters are used.

x -- Matches any single digit that is dialed.
[] -- Specifies a range of numbers to be matched. It may be a range, a list of ranges separated by commas, or a list of digits.

9. 17 Line >> Action Plan



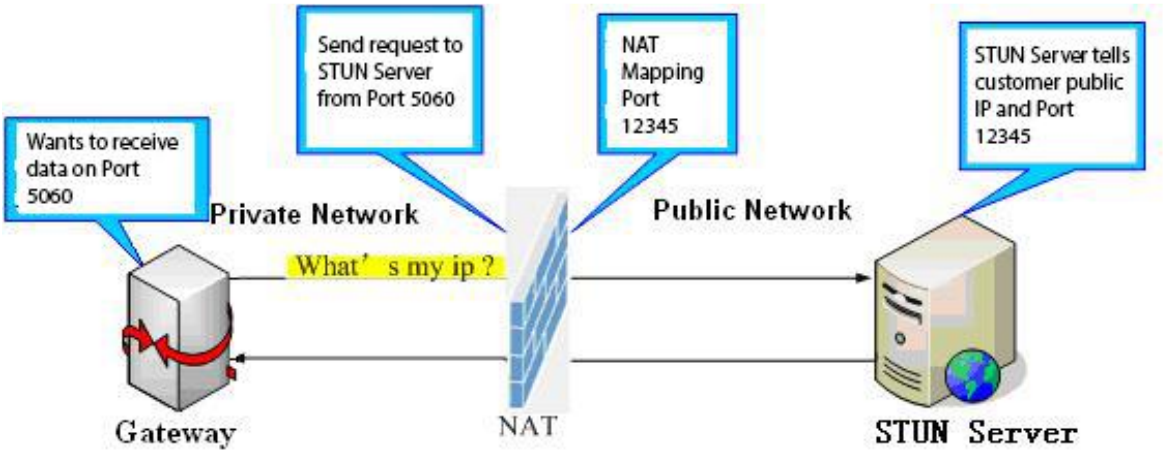
Picture 36 - Action Plan

Table 20 - Action Plan

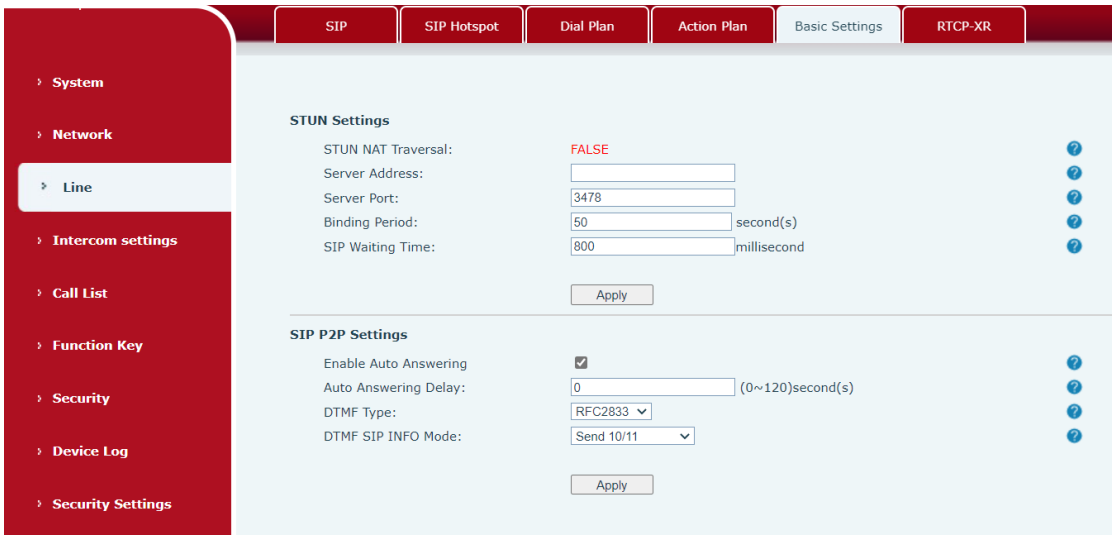
Parameter	Description
Number	Auxiliary phone number (support video)
Type	Support video display on call.
Direction	For call mode, incoming/outgoing call displays video
Line	Set up outgoing lines.
Username	Bind the user name of the IP camera.
Password	Bind IP camera password.
URL	Video streaming information.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

9. 18 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 37 - Basic Settings



Picture 38 - Line Basic Setting

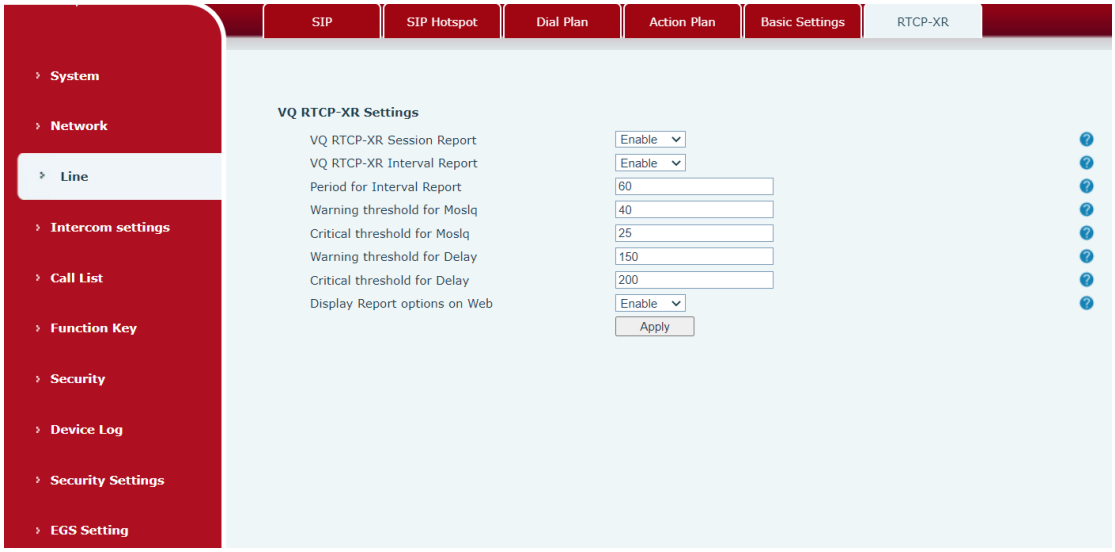
Table 21 - Line Basic Setting

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	Set SIP INFO mode to send '*' and '#' or '10' and '11'

Mode	

9. 19 Line >> PTCR-XR

The RTCP-XR mode is based on THE RTP Control Extended Report (RFC3611). It sends RTCP-XR packets to evaluate network packet loss, delay, and voice quality.

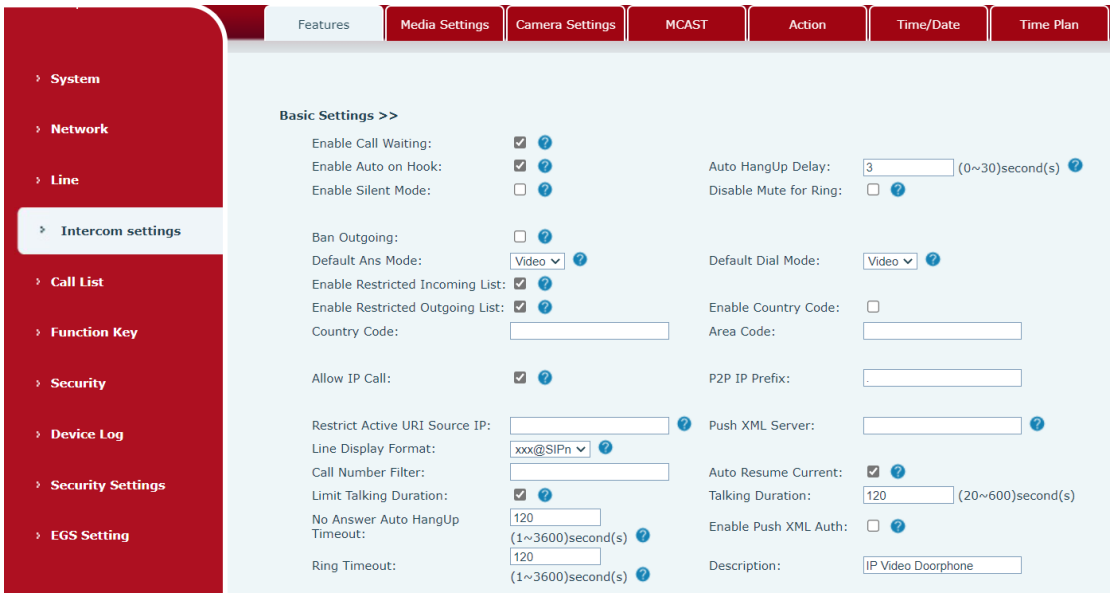


Picture 39 - RTCP-XR

Table 22 - set RTCP-XR

Parameters	Description
VQ RTCP-XR Settings	
VQ RTCP-XR Session Report	Whether to enable sending VQ reports in session mode
VQ RTCP-XR Interval Report	Whether to enable sending VQ reports in Interval mode
Period for Interval Report (5~99)	The interval at which VQ reports are periodically sent
Warning threshold for Moslq(15~40)	When the Moslq value x10 is lower than the threshold, a warning message is generated
Critical threshold for Moslq(15~40)	When the CALCULATED Moslq value x10 is lower than the threshold, a critical report is generated
Warning Threshold for Delay (10~2000)	When the One-way delay is greater than the threshold, the IP phone generates a warning report
Critical Threshold for Delay (10~2000)	When the One-way delay is greater than the threshold, the IP phone generates a critical report
Display Report Options on web	Whether to display the VQ report data for the last call through a web page

9. 20 Intercom settings >> Features



`

Picture 40 - Features

Table 23 - Feature Parameters

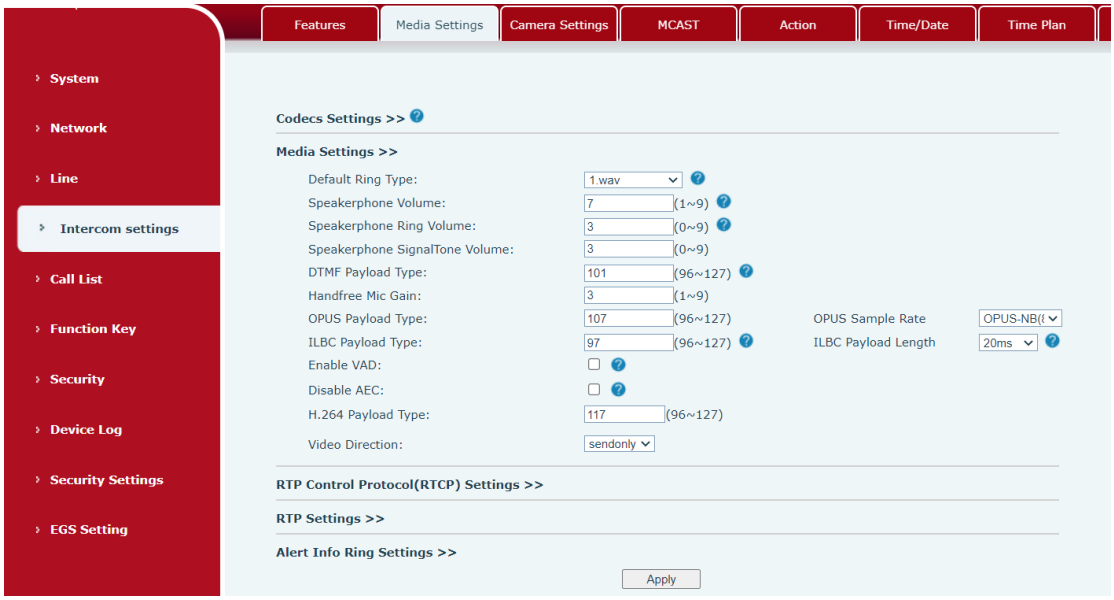
Parameters	Description
Basic Settings	
Enable Call Waiting	Enable this setting to allow user to take second incoming call during an established call. Default enabled.
Enable Auto Handdown	The phone will hang up and return to the idle automatically at hands-free mode
Auto Handdown Time	Specify Auto handdown 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 Reply Mode	Select the default mode after an incoming call, including Video and Audio
Default Dial Mode	Select the default mode after an dialling, including Video and Audio
Enable Restricted Incoming List	Whether enable Restricted Incoming List
Enable Restricted	Wether enable Restricted Outgoing List

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.
Line Display Format	Line display format including SIPn/SIPn：xxx/xxx@SIPn
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
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
Ringing timeout	If the call is not answered, automatic hang-up after timeout
Show description information	Show description information on the IP scan tool software. Default is "IP Video Doorphone"
Tone Settings	
Enable Holding Tone	When 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 digit 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 beep	When switched on, a beep will be heard when the auto-answer is activated.
Tone of open door successfully	Closed: No prompt tone is played after the door is opened successfully Default: Use the default prompt tone

	Voice: built-in voice prompt by default, default is "open the door successfully" Support custom door opening success prompt tone, which can be customized in system - upgrade - ringtone or after the door is opened and the ringtone file upgrades successfully
Tone of open door unsuccessfully	Closed: There is no prompt tone after the door fails to open Default: Use the default prompt tone Voice: built-in voice prompt by default, default is "failed to open the door" Supports custom door opening failure prompt tone, in the system - upgrade - ringtone, or after failing to open the door and the ringtone file upgrades unsuccessfully
Door closing beep	Close: no beep after closing the door Default: Use the default beep Voice: default built-in voice prompt, default is "Close" Support custom door closing tone, in the system - upgrade - ringtones, after upgrading the ringtone file under the door closing available settings to use the custom
Successful card addition beep	Close: No beep after successful card addition Default: Use the default beep Voice: default built-in voice prompt, default is "Card added successfully" Support customizable beep for successful card addition, in the system - upgrade - ringtones, after upgrading the ringtones file available under successful card addition settings to use a custom
Add card failure beep	Close: No beep after failed card addition Default: Use the default beep Voice: default built-in voice prompt, default is "card refill failed"Support customizable sound for card failure, in the system - upgrade - ringtones, after upgrading the ringtones file under the card failure can be set to use a custom
Successful beep for card deletion	Close: No beep after successful card deletion Default: Use the default beep Voice: default built-in voice prompt, default is "card deletion successful" Support for customising the successful card deletion tone, in System - Upgrade - Ringtone, after upgrading the ringtone file under the successful card deletion you can set to use a

	customised
Card deletion failure beep	Close: No beep after failed card deletion Default: Use the default beep Voice: default built-in voice prompt, default is "card deletion failed" Support for customising the card deletion failure tone, in System - Upgrade - Ringtone, after upgrading the ringtone file under the card deletion failure can be set to use a customised
Magnetic door detection beep	Closed: No beep after door magnetic detection anomaly Default: Use the default beep Voice: default built-in voice prompt, default is "Please close the door" Customised door detection tones are available under System - Upgrade - Ringtones, after upgrading the ringtone file the door detection can be set to use a customised
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

9.21 Intercom settings >> Media



Picture 41 - Media Settings

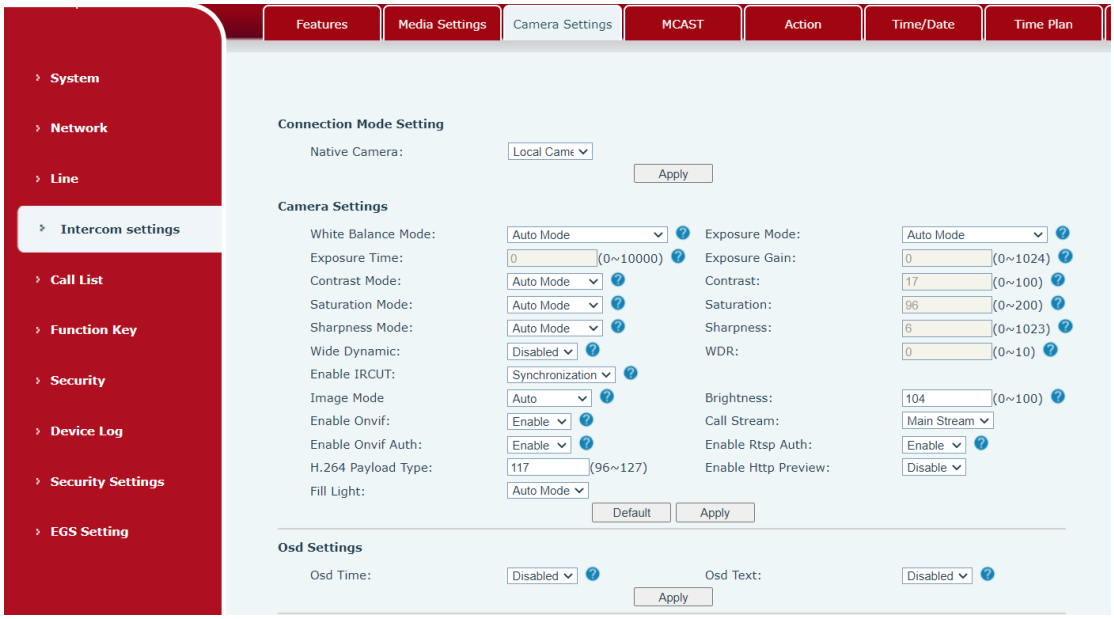
Table 24 - Media Setting

Parameters	Description
Codecs Settings	Select the enabled and disabled voice codecs codec:G. 711A/U, G. 722, G. 729, ILBC, opus
Media Setting	
Default Ring Type	Set the default ring type. If the caller ID of an incoming call was not configured with specific ring type, the default ring will be used.
Speakerphone Volume	Set the speakerphone volume, the value must be 1~9
Speakerphone Ring Volume	Set the ring volume in the speakerphone, the value must be 1~9
Speakerphone Ring Volume	Set the ring volume in the speakerphone, the value must be 1~9
DTMF Payload Type	Enter the DTMF payload type, the value must be 96~127.
Opus playload type	Enter the opus payload type, the value must be 96~127.
OPUS Sample Rate	Set the opus sample rate，including OPUS-NB（8KHz), OPUS-WB（16KHz）
ILBC Payload Type	Set the ILBC Payload Type
ILBC Payload Length	Set the ILBC Payload Length
Enable VAD	Enable Voice Activity Detection. When enabled, the device will suppress the audio transmission with artificial comfort noise signal to save the bandwidth.
H.264Payload Type	Set the H264 Payload Type，the value must be 96~127.

RTP Control Protocol(RTCP) Settings	
CNAME user	Set CNAME user
CNAME host	Set CNAME host
RTP Settings	
RTP keep alive	Hold the call and send the packet after 30s
Alert Info Ring Settings	
Value	Set the value to specify the ring type.
Ring Type	Type1-Type9

9. 22 Intercom settings>>Camera Settings

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



Picture 42 - Camera Settings

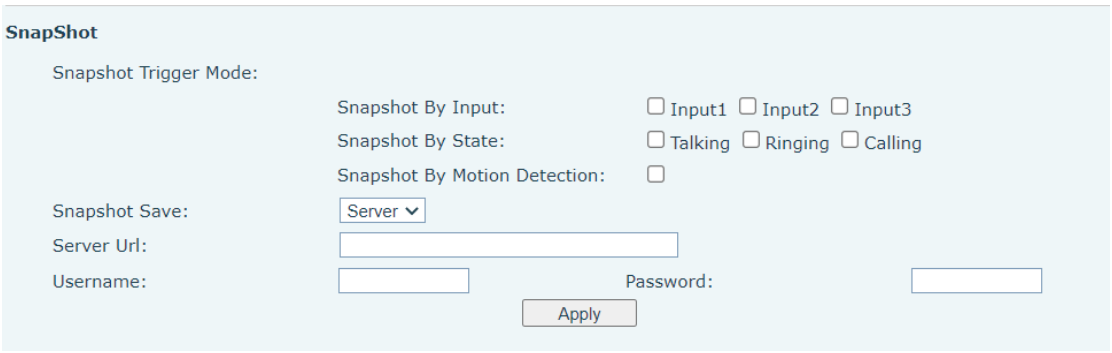
Table 25 - Camera Settings

Parameters	Description
Connection Mode Setting	
Native Camera	Local: Automatically use the local camera to transmit images External: After setting the external camera, it will automatically use the external camera to transmit images
camera settings	
White Balance Mode	Auto mode：The camera automatically makes the most appropriate adjustments according to the color temperature of the shooting scene, and automatically compensates for the color of the light source.。 Lock mode：Fixed white balance parameters will not be automatically adjusted according to the actual color temperature.

	Incandescent lamp mode：To compensate for the hue of incandescent lamps, it is suitable for use under beige light sources (bulbs, tungsten lamps, candles) and other light sources of this type.。 Warm light mode：Compensate the hue of warm light, suitable for light sources with a color temperature of about 2700K。 Naturl light mode：It can be used for white balance in outdoor shooting and has a wide range of applications.。 Fluorescent lamp light：Compensate the hue of fluorescent lamps, suitable for use under fluorescent light sources (fluorescent lamps, energy-saving lamps) and other types of light sources。
Exposure Mode	**Auto mode** ：The camera automatically sets the parameters, no need for the operator to adjust. **Manual exposure time** ：Set the exposure time by yourself, the range is 0~10000 **Manual exposure gain**：Set the exposure gain by yourself, the range is 0~1024 All manual ：Manually set the exposure time and gain.
Exposure Time	It refers to the time to press the shutter. Increasing the exposure time can increase the signal-to-noise ratio and make the image clear. The longer the time, the more the sum of photons to the CCD\CMOS surface, the brighter the captured image will be, but if it is overexposed, the photo will be too bright and lose the image details; if it is underexposed, the photo will be too dark.
Exposure Gain	It refers to the amplification gain of the analog signal after double sampling, but the noise signal is also amplified in the process of amplifying the image signal. The gain is generally only used when the signal is weak, but you do not want to increase the exposure time.
Contrast Mode	Auto mode：The camera automatically sets the contrast according to the environment, no need for the operator to adjust Manual mode：Manually set the camera's contrast parameters.
Contrast	Contrast refers to the contrast between light and dark in the picture. Increase the contrast, the brighter areas will be brighter and the darker areas will be darker, and the contrast between light and dark will increase.
Saturation Mode	Auto mode：The camera automatically sets the saturation according to the environment, without the need for the operator to adjust **Manual mode**：Manually set the camera's saturation parameters.
Saturation	Saturation refers to the color. Adjusting the saturation will change the color. The greater the adjustment, the more distorted the image color. Adjusting the saturation is only suitable for pictures with insufficient colors. When the saturation is adjusted to the lowest, the

	image will lose its color and become a black and white image.
Sharpness Mode	Auto mode：The camera automatically sets the sharpness according to the environment, no need for the operator to adjust **Manual mode**：Manually set the sharpness parameters of the camera
Sharpness	Sharpness is sometimes called "sharpness", which is an indicator that reflects the sharpness of the image plane and the sharpness of the edges of the image. If you increase the sharpness, the contrast of the details on the image plane is also higher and it looks clearer.
Wide dynamic	Enable or disable wide dynamic. Turning on wide dynamic allows the camera to see the image in a very strong contrast
Wide dynamic range	Set image brightness by yourself, range 0~10
Turn on IRCUT	Whether to open IRCUT
Image mode	Daytime (color): The camera transmits color images when there is sufficient light during the day Night (black and white): The camera transmits black and white images when there is insufficient light at night Automatic: The camera transmits color images when the light is sufficient during the day according to the light sensitivity, and transmits black and white images when the light is insufficient at night
brightness	Set the image brightness by yourself, the range is 0~100
Enable Onvif	Enable or disable the onvif protocol, after enabling it, the device can be discovered through a recorder that supports ONVIF
Call Stream	Main stream or sub stream used in video call
Enable Onvif Auth	Is authentication required when using onvif protocol (with username and password)
Enable Rtsp Auth	When using rtsp protocol, whether authentication is required (with username and password)
H.264 Payload Type	Set the load type of h.264, the range is 96~127
Osd Settings	
Osd Time	Turn on/off the date display of the camera image interface.
Osd Text	Enable/disable the text display of the camera image interface.
Video Codecs	
H264 Video Stream	Support H.264 encoding format

Bitrate Control	VBR：Video call will adapt to the bit rate of the opposite end, so that the video effect is better. CBR：The video call will not change according to the bit rate set by itself.
Resolution	Support 1080P，720P，4CIF,VGA,CIF,QVGA
Frame Rate (fps)	The larger the value is, the more fluent the video is, and the higher the requirement for network bandwidth is; adjustment is not recommended
BitRate	It refers to the data flow used by video files in unit time, also known as code rate or code flow rate. Generally speaking, sampling rate is the most important part of picture quality control in video coding. Generally, the unit we use is KB / s or MB / s
I Frame Interval	The larger the value, the worse the video quality, otherwise the better the video quality; adjustment is not recommended.
RTSP Information	
Main Stream Url	Display the main stream URL address
Sub Stream Url	Display the sub stream URL address
Snapshot	
Input trigger	Select the input port that triggers the capture
Call trigger	Select the call status that triggers the capture
Movement detection trigger	Whether to enable monitoring capture
Saving Method of Capture	Set how to save the captured image, including: server, Storage Card, Server and Storage Card
server address	Enter the server address
Username	Enter a username
Password	Enter a password



Picture 43 - SnapShot

Capture trigger mode: input trigger, call status trigger, Movement detection trigger

Input trigger: Select the input port to trigger the snapshot

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

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

Save the screenshot to the server or SD card.

Server address (Upload through FTP, TFTP, HTTP, or HTTPS) :*ftp://IP:port@用户名:密码/*

9.23 Intercom Setting >> MCAST

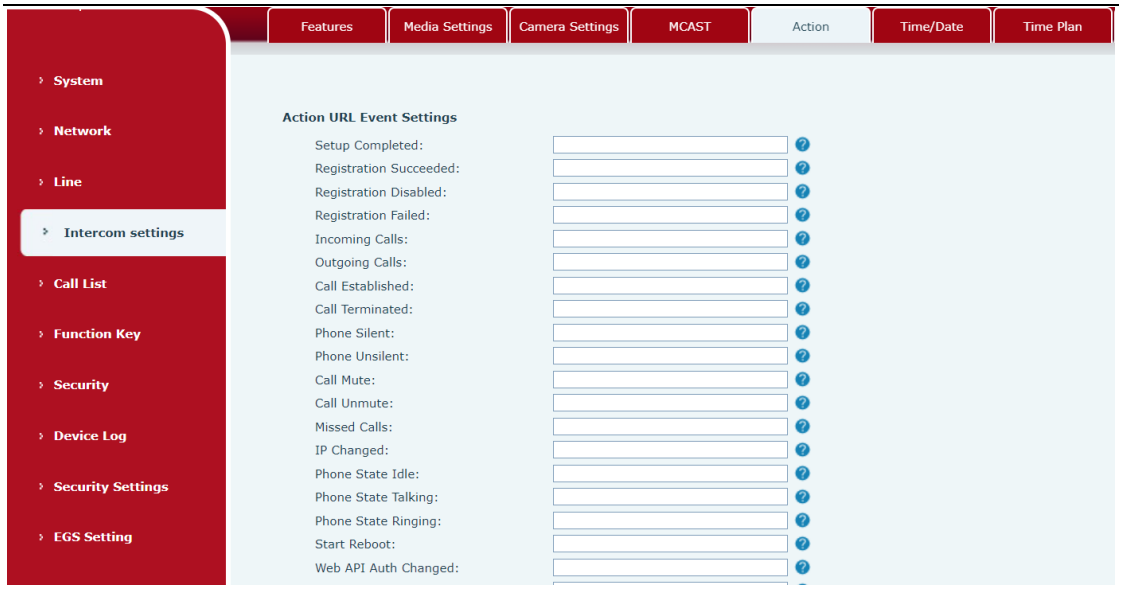
It is easy and convenient to use multicast function to send notice to each member of the multicast via setting the multicast key on the device and sending multicast RTP stream to pre-configured multicast address. By configuring monitoring multicast address on the device, monitor and play the RTP stream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

The detail for 8.2 MCAST

9.24 Intercom Setting >> Action URL

Table 26 - action URL

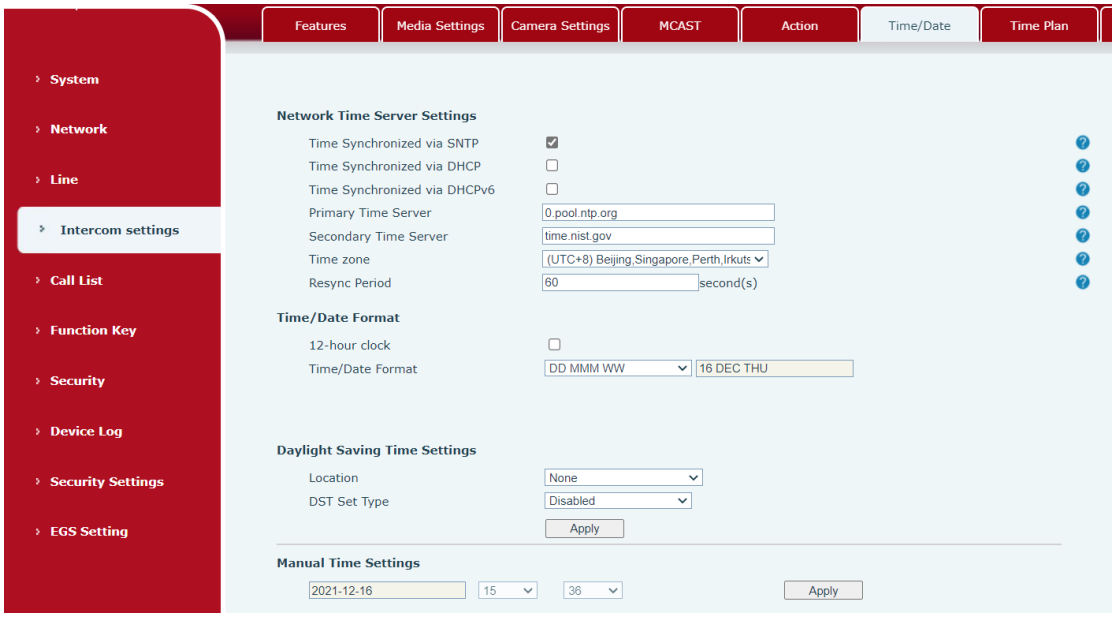
Action URL Event Settings
URL for various actions performed by the phone. These actions are recorded and sent as xml files to the server. Sample format is http://InternalServer /FileName.xml



Picture 44 - Action URL

9. 25 Intercom Setting >> Time/Date

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



Picture 45 - Time/Date

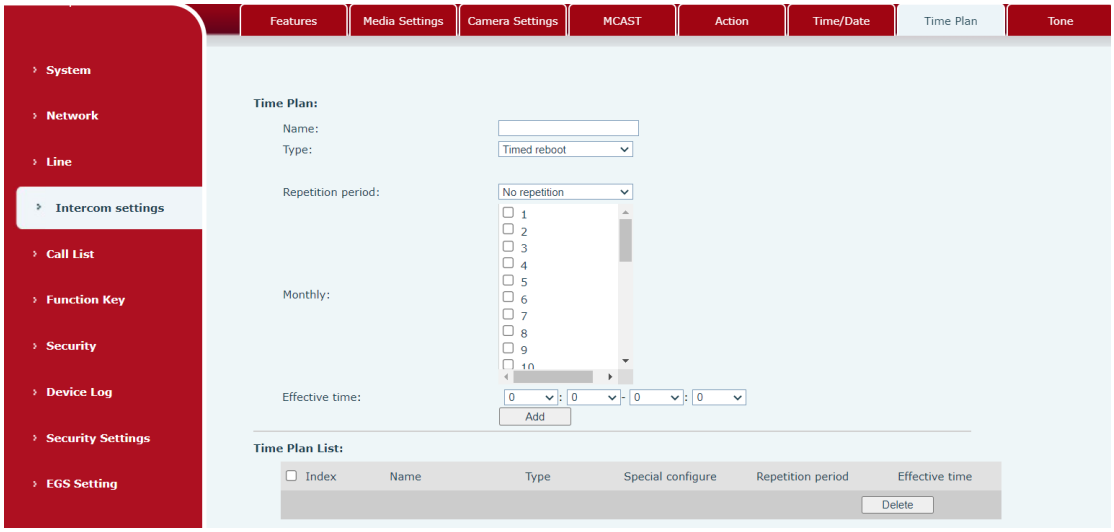
Table 27 - Time/Date

Time/Date	
Field Name	**Explanation**
Network Time Server Settings	
Time Synchronized via	Enable time-sync through SNTP protocol

SNTP	
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)	

9.26 Intercom settings>>Time plan

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



Picture 46 - Time Plan

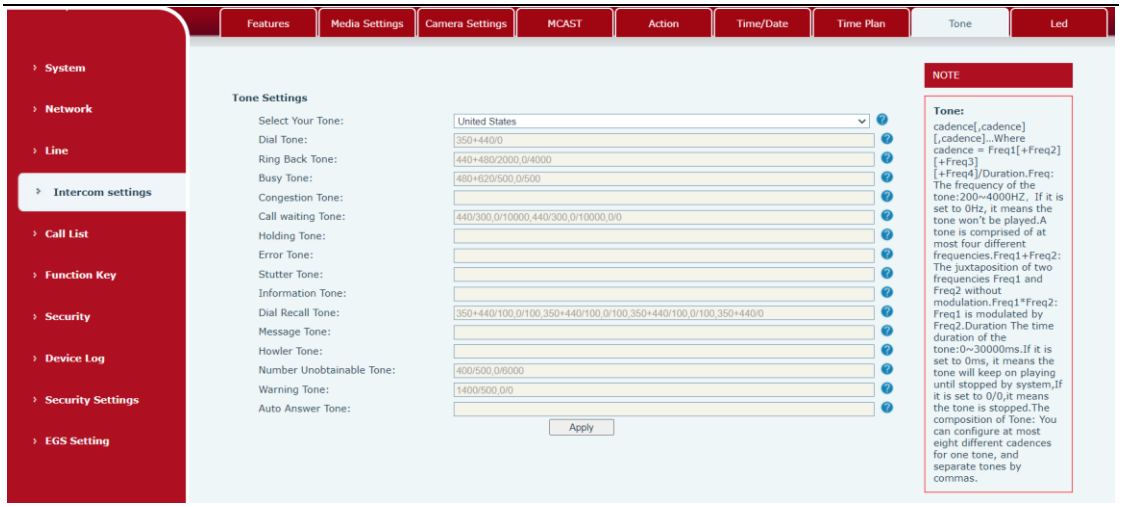
Table 28 - Time Plan

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

9.27 Intercom settings >> Tone

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

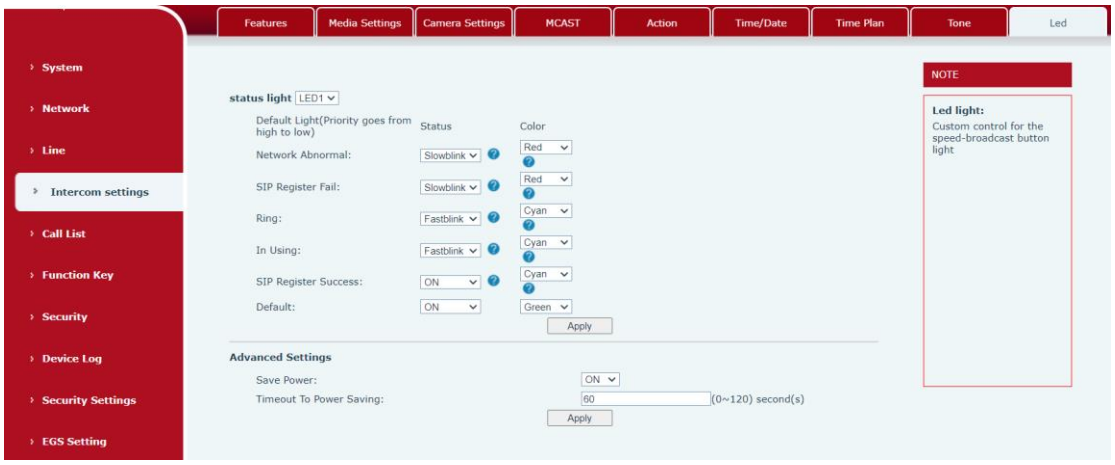
You can select the country area or customize the area. The selected area can directly appear the default information, and the customized one can modify the key tone, callback tone and other information.



Picture 47 - Tone

9. 28 Intercom settings >> Led

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



Picture 48 - Led

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

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

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

9. 29 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.

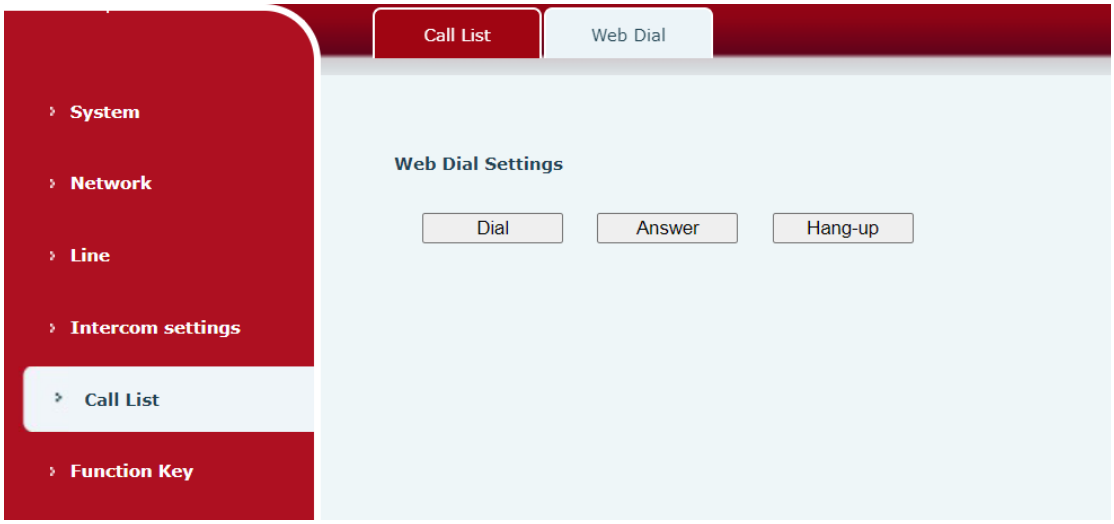
User can add specific number to be blocked, or a prefix where any numbers matched the prefix will all be blocked.

■ Restrict Outgoing Call

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

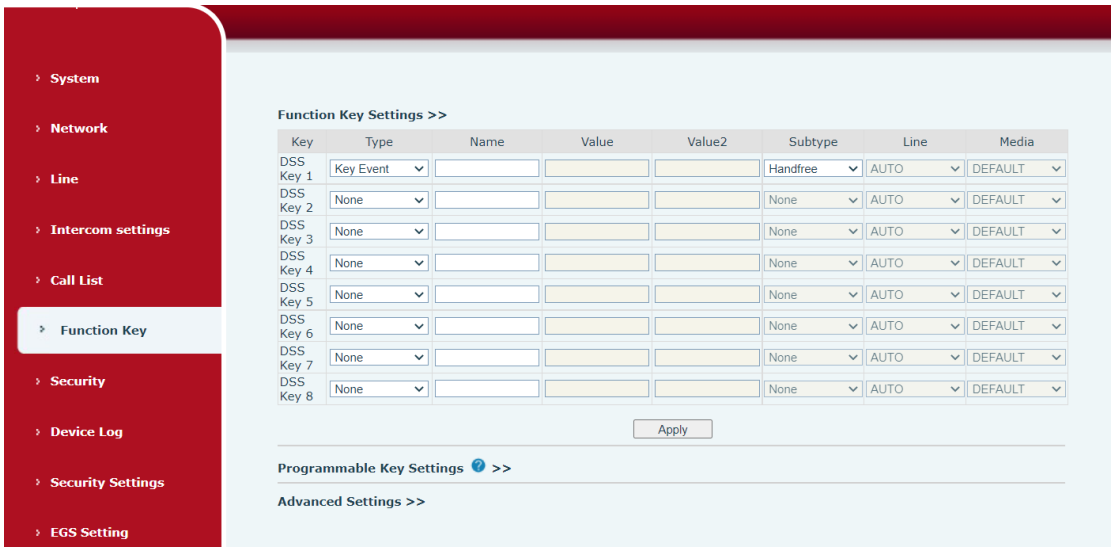
9. 30 Call list >> Web Dial

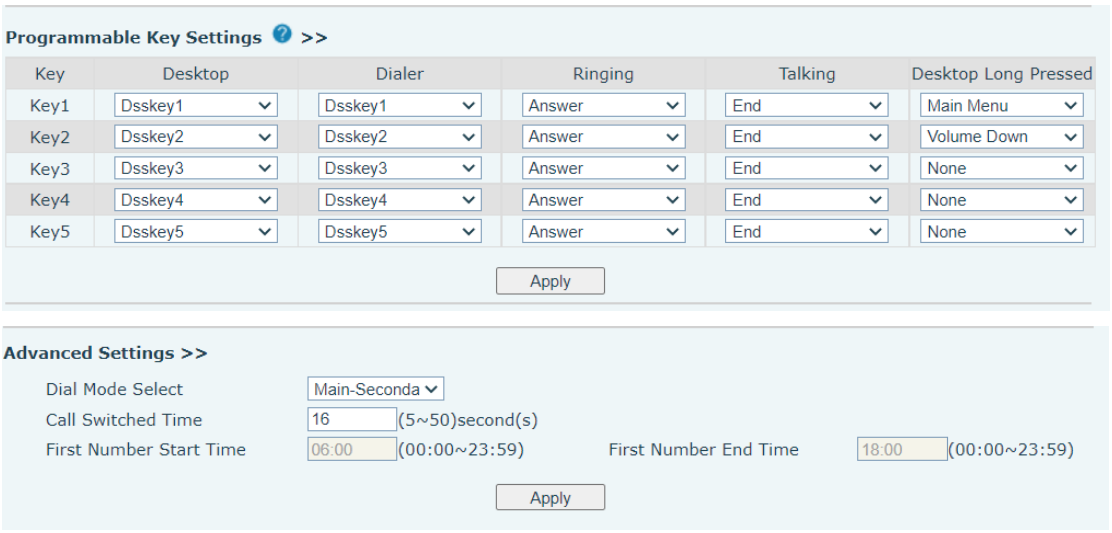
Use web page to call, answer and hang up.



Picture 49 - Webpage Dial

9. 31 Function key





Picture 50 - Function Key Settings

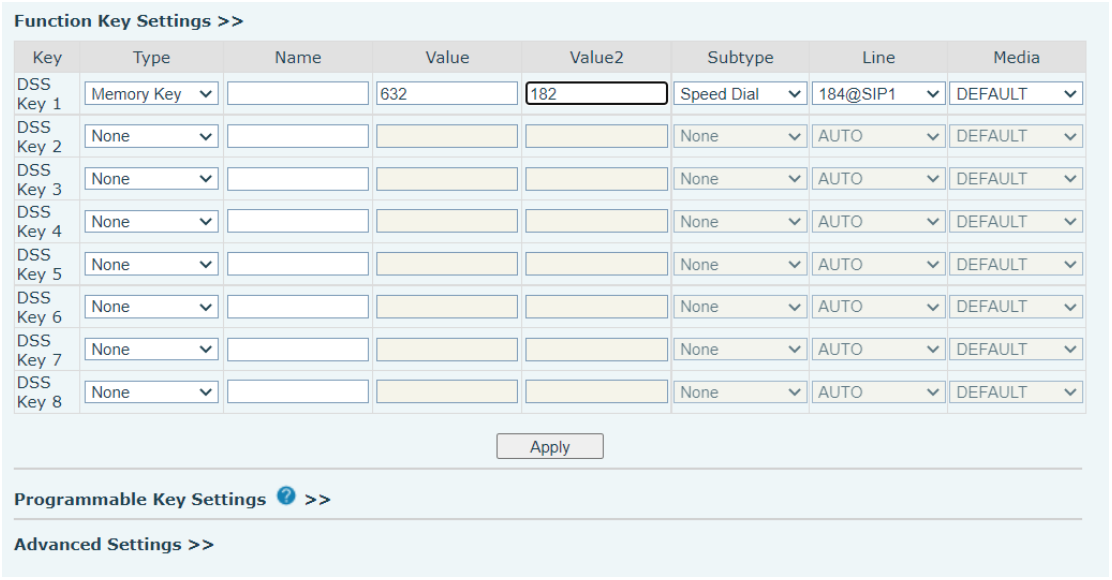
Table 29 - Function Key Settings

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

Programmable Key Settings	
Desktop	None：Nothing happens when you press the speed dial Dsskey1：When it is set to dsskey1, follow the settings of dsskey1 to make call, answer, etc. Dsskey2：When it is set to dsskey2, perform operations such as calling and answering according to the setting of dsskey2
Dialer	None：Nothing happens when you press the speed dial Dsskey1：When it is set to dsskey1, follow the settings of dsskey1 to make call, answer, etc. Dsskey2：When it is set to dsskey2, perform operations such as calling and answering according to the setting of dsskey2
Ringing	Answer：Set to answer, when there is an incoming call, if auto answer is disabled, press the speed dial key to answer the call End: set to end, when there is an incoming call, press the speed dial button to hang up the call
Talking	End: set to end, when there is a call, press the speed dial key to hang up the call Volume up: set as volume up button, when there is a call, press the speed dial button to increase the volume Volume down: set as volume up button, when there is a call, press the speed dial button to decrease the volume Dsskey1：When it is set to dsskey1, follow the settings of dsskey1 to make call, answer, etc. Dsskey2：When it is set to dsskey2, perform operations such as calling and answering according to the setting of dsskey2
Desktop Long Pressed	None: Long press the speed dial key does not respond Main menu: Long press the speed dial key to enter the command line mode, see 5.2.1 Common Command Mode for details
Advanced Settings	
Hot Key Dial Mode Select	Number 1 call number 2 mode selection. <Main/Secondary>: If the first number is not answered within the set time, the second number will be automatically switched. <Day/Night>：The system time is automatically detected during the call. If it is daytime, the first number is called, otherwise the second number is called.
Call Switched Time	Set number 1 to call number 2 time, default 16 seconds
Day Start Time	The start time of the day when the <Day/Night> mode is defined. Default "06:00"
Day End Time	The end time of the day when the <Day/Night> mode is defined. Default "18:00

➢ **Memory**

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



Picture 51 - Memory Key

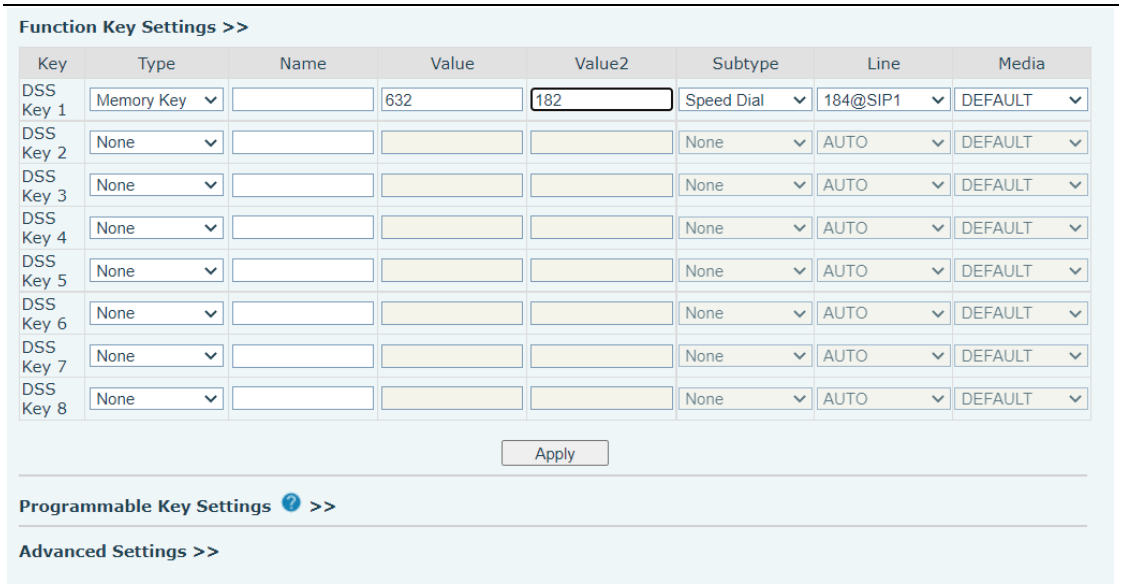
Table 30 - Memory Key

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

➢ Multicast

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

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



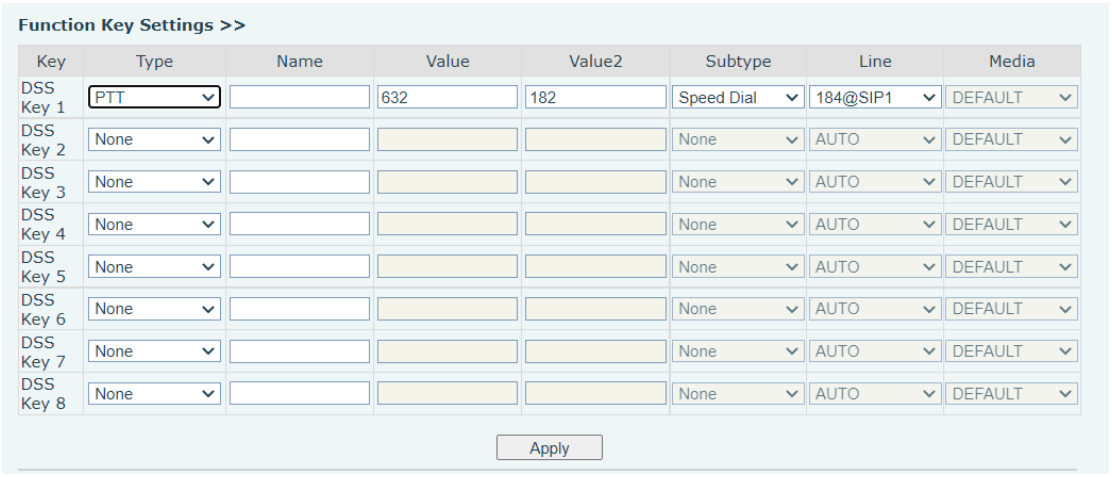
Picture 52 - Multicast

Table 31 - Web Multicast

Type	Number	Subtype
Multicast	Set the host IP address and port number, they must be separated by a colon (The IP address range is 224.0.0.0 to 239.255.255.255, and the port number is preferably set between 1024 and 65535)	G.711A
		G.711U
		G.729AB
		iLBC
		opus
		G.722

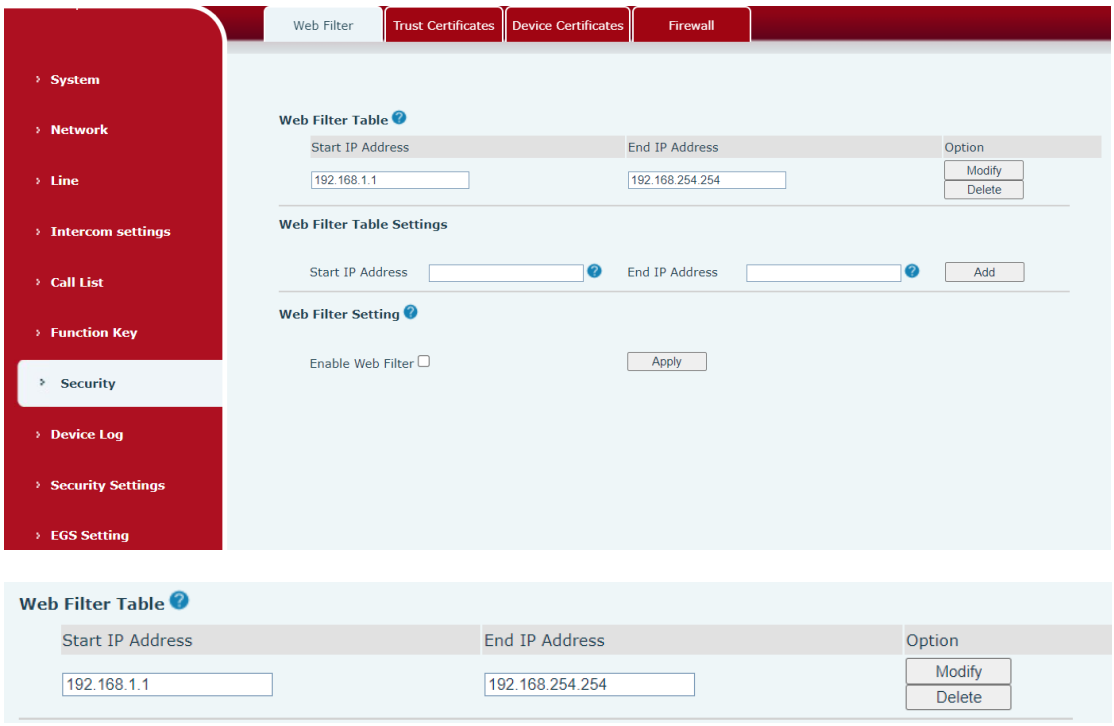
➢ **PTT**

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



9. 32 Security >> Web filter

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



Picture 53 - WEB filter

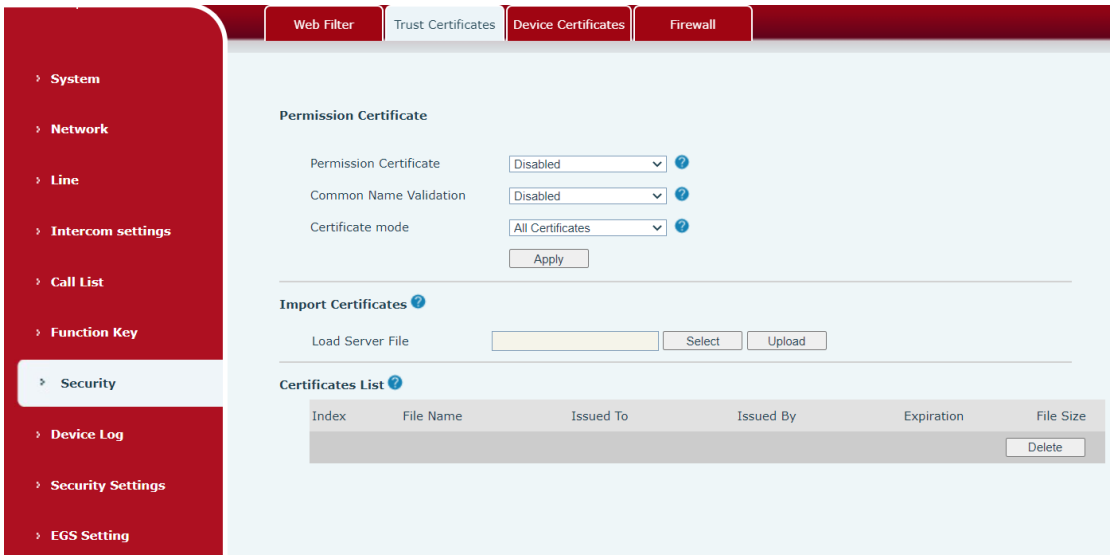
Add and delete the allowed IP network segments; configure the start IP address in the start IP, configure the end IP address in the end IP, and then click [Add] to add successfully. You can set a large network segment or add it into several network segments. When deleting, select the starting IP of the 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. 33 Security >> Trust Certificates

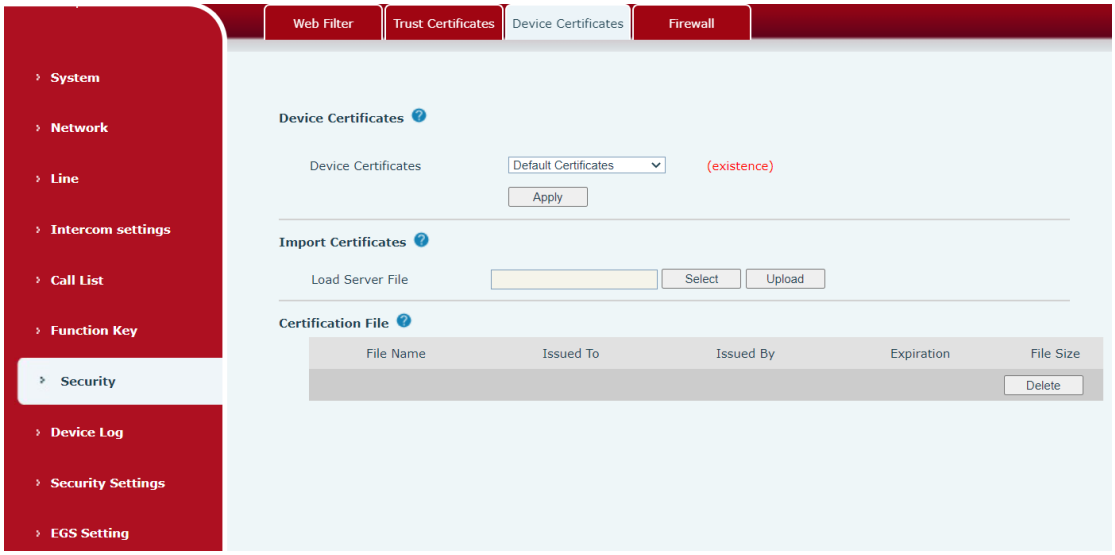
You can upload and delete uploaded trust certificates.



Picture 54 - Trust Certificates

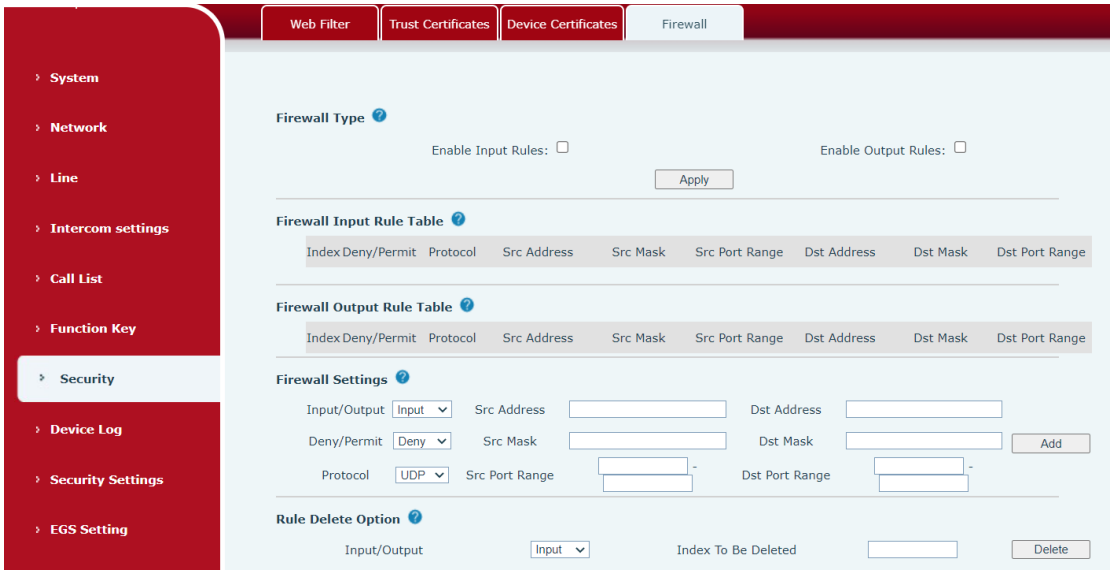
9. 34 Security >> Device Certificates

Select the default certificate or the custom certificate as the device certificate.
You can upload and delete uploaded certificates.



Picture 55 - Device Certificates

9. 35 Security >> Firewall



Picture 56 - 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.

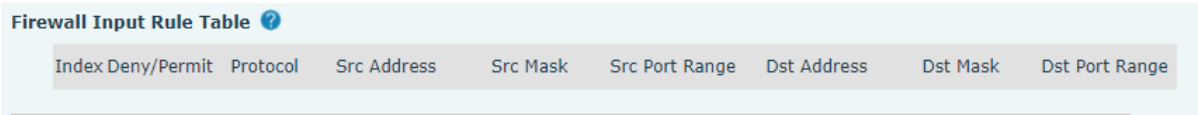
Taking into account the complexity of firewall settings, the following will illustrate with an example:

Table 32 - 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

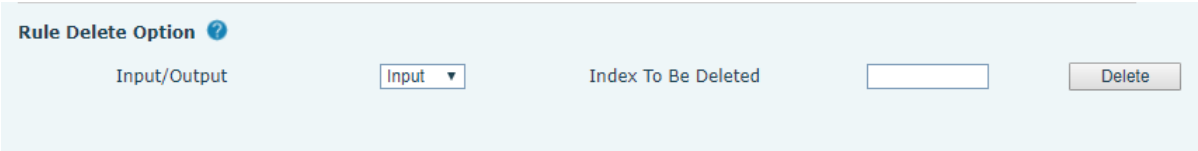
	255.255.255.255, it means it is a specific host. When it is set as a subnet mask of type 255.255.255.0, it means that the filter is a network segment;
Dst Port Range	It is the destination address mask. When it is configured as 255.255.255.255, it means it is a specific host. When it is set as a subnet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

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



Picture 57 - 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 58 - Delete firewall rules

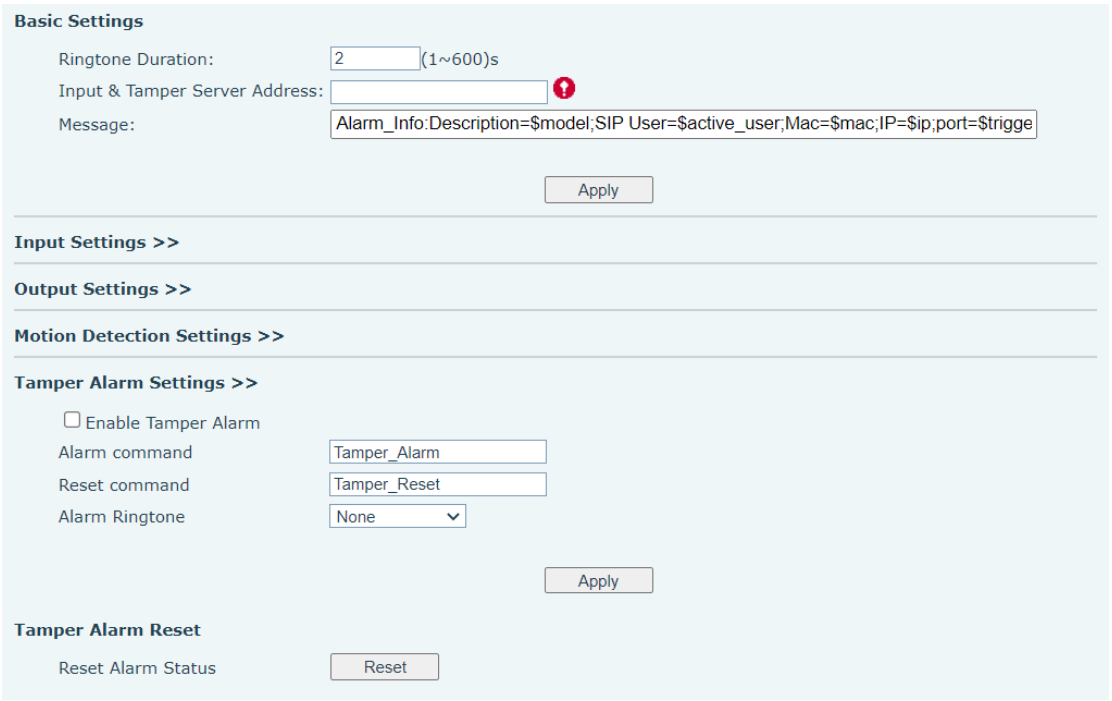
Select the list you want to delete and click [Delete] to delete the selected list.

9. 36 Device 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. 37 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 59 - Security Settings

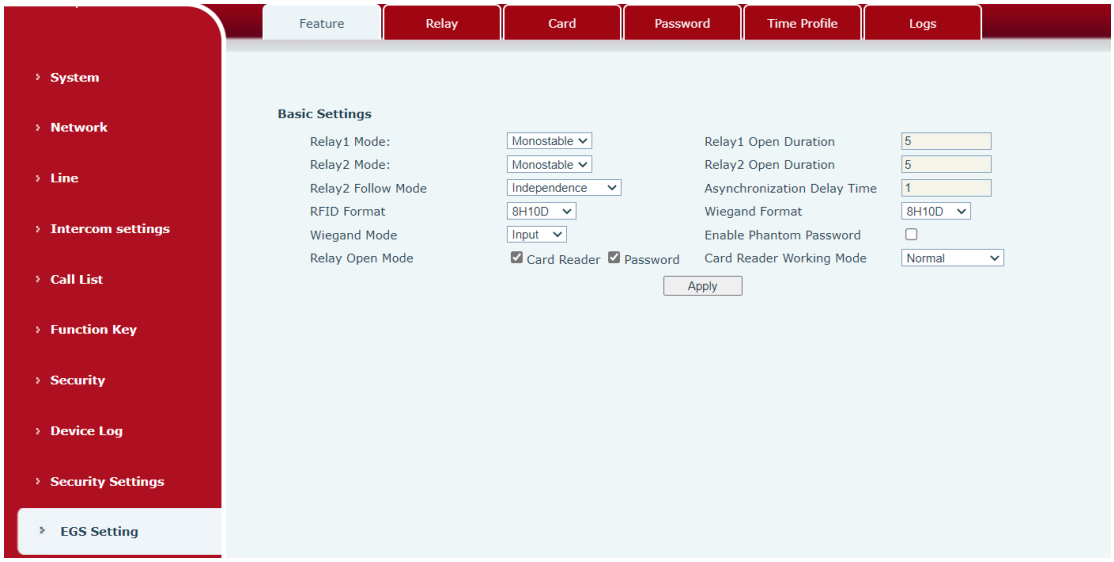
Table 33 - Security Settings

Security Settings	
Parameters	**Description**
Basic Settings	
Ringtone Duration	Set the ringtone duration, default value is 2 seconds.
Input & Tamper Server Address	Set remote server address. The device will send message to the server when the alarm is triggered. The message format is：Alarm_Info:Description=i16SV;SIP User=;Mac=0c:38:3e:3a:06:65;IP=; port=Input .
Information	Fill in the information attached to the upload server
Input settings	
Input	Enable or disable Input
Triggered by	When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger.
	When choosing the high level trigger (disconnect trigger), detect the input port (high level) disconnected trigger.
Input Duration	Set the Input change duration time, the default is 5 seconds.
Triggered Action	**Send SMS:** Set the alert message send to server if selected. **Event:** The device will perform corresponding Dss Key configurations if any key is selected, by default the value is none. **Triggered Ringtone:** Select triggered ring tone.
Triggered Ringtone	Ringtone selection
Output Settings	

Enable Logs	Enable or disable LOG
Triggered by DTMF Ring tone	Select the DTMF trigger ring tone.
Triggered by URI Ringtone	Select the URI trigger ring tone.
Triggered By SMS Ringtone	Select the SMS trigger ring tone.
Triggered By Dsskey Ringtone	Select the Dsskey trigger ring tone.
Output Response	Enable or disable Output Response
Standard Status	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 NC port close.
Output Duration	Set the output change duration time, the default is 5 seconds.
Input trigger	When the input port meets the trigger condition, the output port will trigger (the port level time changes, controlled by <output duration>).
Trigger by DTMF	Enable or disable trigger by DTMF. The device will check the received DTMF sent by remote device, if it matches the DTMF trigger code, the device will trigger corresponding output port.
DTMF Trigger Code	Input the DTMF trigger code, default value is 1234.
DTMF Reset Code	Input the DTMF reset code, default value is 4321.
Reset By	Reset the output port mode by duration or state. By duration: Reset the output port status when output duration occurs. By state: Reset the output port status when device's call state changes.
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 Message	Input trigger message for trigger by URI mode.
Rest Message	Input reset message for trigger by URI mode.
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 SMS	Input trigger message for trigger by SMS mode.
Reset SMS	Input reset message for trigger by SMS mode.

Trigger by Input	Select the input port, when the input port meets the trigger condition, the output port will be triggered (The Port level time change, By < Output Duration > control)
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.
Triggered Hangup	Trigger the output port after hanging up
Hangup Delay	Hang up trigger delay, default 5 seconds
Motion detection settings	
Motion Detection Alarm	Enable or disable motion detection
Trigger Duration	Set the trigger delay time, the default is 3 seconds, the range: 0~3600 seconds
Trigger ringtone	Support ringtone selection
Trigger behavior: Send SMS	Enable or disable the input port to send messages to the server
Function key	When set to dsskey1 or dsskey2, trigger dsskey to make a call, the default is none
Tamper Alarm Settings	
Enable Tamper Alarm	Whether to enable tamper detection, if the terminal is violently dismantled, the tamper is triggered and always play the set alarm ringtone
Alarm command	When detected someone tampering the equipment, the alarm signal will be sent to the corresponding server
Reset command	When the equipment receives the command of reset from server, the equipment will stop alarm
Alarm Ringtone	Alarm ringtone setting
Detachable alarm reset	
Reset alarm state	Reset the play of stop ringtone

9. 38 EGS Setting >> Features



Picture 60 - ESG Feature Settings

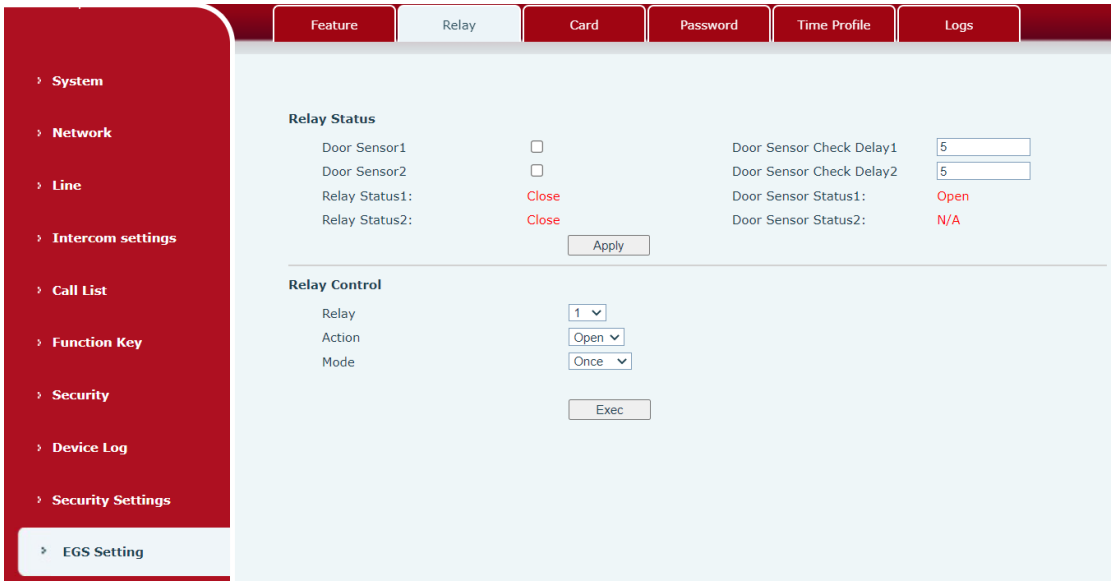
You can set basic access control Settings on this screen

Table 34 - ESG Feature Parameters

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

Relay2Follow mode	Independent: Open the door independently with Relay1 Synchronous: open the door at the same time as Relay1 Asynchronous: Relay1 opens after a period of time Relay2 opens
Asynchronous delay	The user can set the asynchronous door opening delay time of Relay1 and Relay2, the default is 1 second
RFID card format	Supported access control card format
Wiegand format	Supported Wiegand access card format
Wiegand mode	Optional input port or output port
Enable Virtual password	After enabling, the correct password will be included in the consecutively entered numbers to open the door
Enable Card Reader	Enable or disable card reader for RFID cards.
Card Reader Working Mode	Set ID card stats: Normal: This is the work mode, after the slot card can to open the door. Card Issuing: This is the issuing mode, after the slot card can to add ID cards. Card Revoking: This is the revoking mode, after the slot card can to delete ID cards.

9. 39 EGS Setting >> Relay



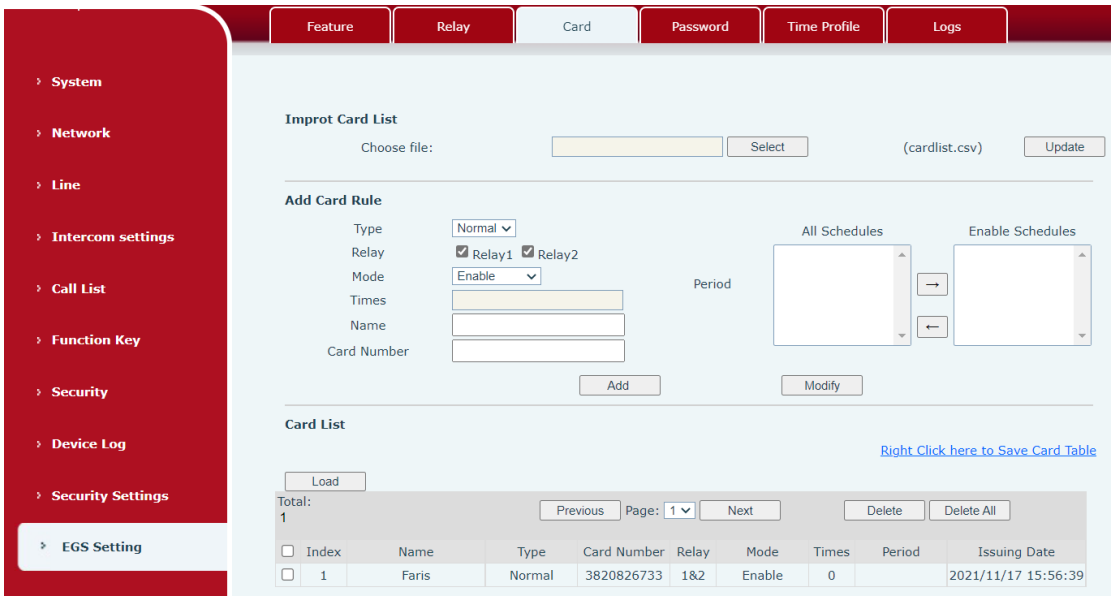
Picture 61 - Relay

Table 35 - Relay

Field Name	Explanation
Relay Status	

Door Sensor1	Enable or disable door sensor 1
Door Sensor Check Delay 1	Door Sensor1 detection delay time setting,5 seconds by default
Door Sensor2	Enable or disable door status sensor 2
Door Sensor Check Delay 2	Door Sensor2 detection delay time setting,5 seconds by default
Lock Status 1	Door Close/Open
Door Sensor Status1	Door Close/Open
Lock Status 2	Door Close/Open
Door Sensor Status2	Door Close/Open
Door Lock Control	
Door Lock	Execute a door lock to open or close the door
Action	Door Open/Close
Open mode	Once: perform door opening action, and will be closed automatically when timeout. Continue: perform the door opening action, the door will not be closed automatically and need to closed manually when timeout.

9. 40 EGS Setting >> Card



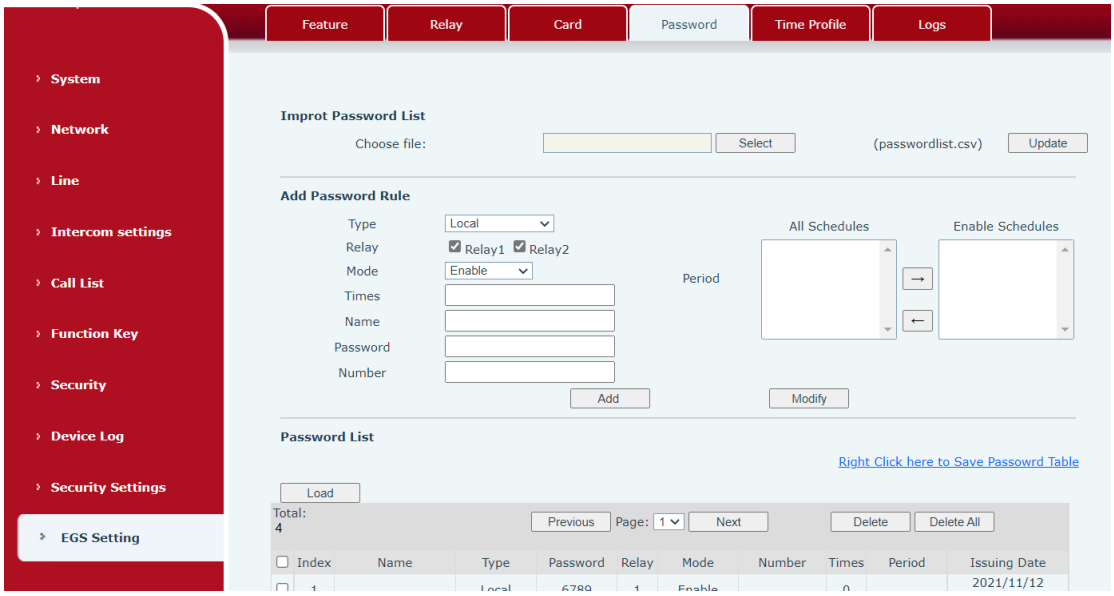
Picture 62 - Card

Table 36 - Card rule

Field Name	Explanation

Import Card List	
Click the <Select> to choose to import remote card list file (cardlist.csv) and then clicking <Update> can batch import remote card rule.	
Add Card Rule	
Type	Standard, namely to open the door card Add, swipe the added card administrator card in the standby mode, the device will enter the card add mode, and then swipe the card, the card that has not been added to the card list will be added Delete, swipe the added card delete administrator card in standby, the device will enter the card delete mode, and then swipe the card, the added card will be deleted
Relay	Swipe to open the door lock
Mode	Closed, swiping is unsuccessful after disabling Enable, swipe the card to take effect after enabling Time zone, swiping the card in the set time zone takes effect
Times	The number of times the card can be swiped in a time period
Name	User name
Card Number	RFID card number. You can manually fill in the first 10 digits of the card number or select the existing card number
Period	The time to add the card, automatically generated
Card List	
Operation	Delete, delete all Export, support to export to csv. file

9. 41 EGS Setting >> Password

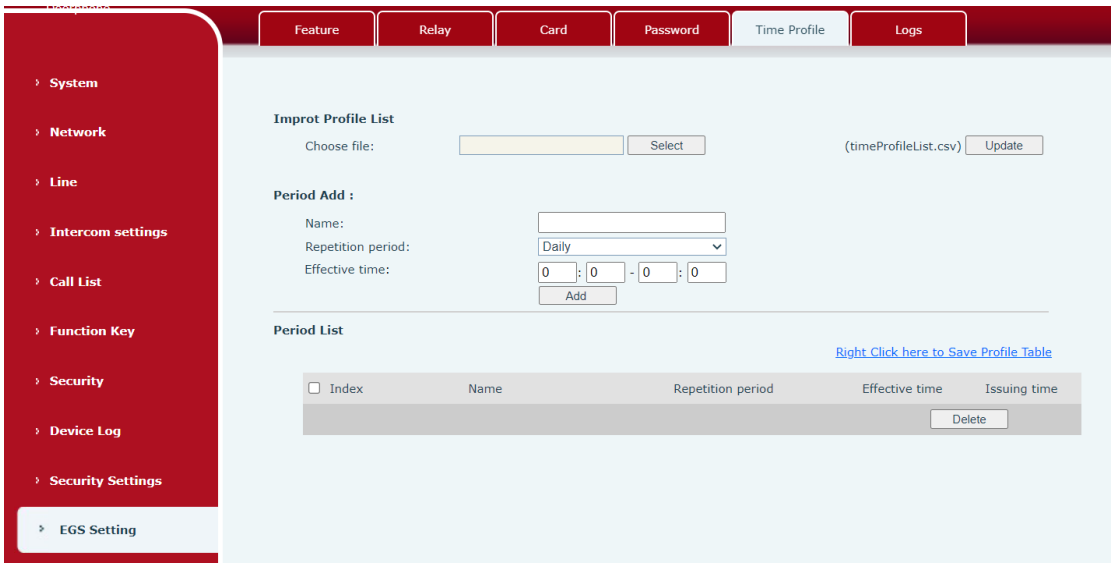


Picture 63 - Password Rule

Table 37 - Time to add the card, automatically generatedd Rule

Field Name	Explanation
Import Password List	
Click the <Select> to choose to import remote password list file (passwordlist.csv) and then clicking <Update> can batch import remote password rule.	
Add Password Rule	
Type	Local, that is, the local door opening password, enter the password dial interface in standby and enter the set opening password to open the door immediately Remote, remote opening password, when the indoor unit calls the door or when the door calls the indoor unit to open the door, enter the DTMF password to open the door Remote and local, one password supports two door opening methods at the same time
Relay	A door lock with a code
Mode	Closed, unsuccessful password opening after disabling Enable, after enabling the password to open the door to take effect Time zone, the password to open the door takes effect during the set time zone
Times	The number of times the door can be opened with a password in a time period
Name	User name
Password	Password to open the door
Number	When the indoor unit calls the access control or the access control calls the indoor unit to open the door, enter the DTMF password to open the door
Period	Time to add the card, automatically generated
Password List	
Operation	Delete, delete all Export, support to export to csv. file

9. 42 EGS Setting >> Time Profile

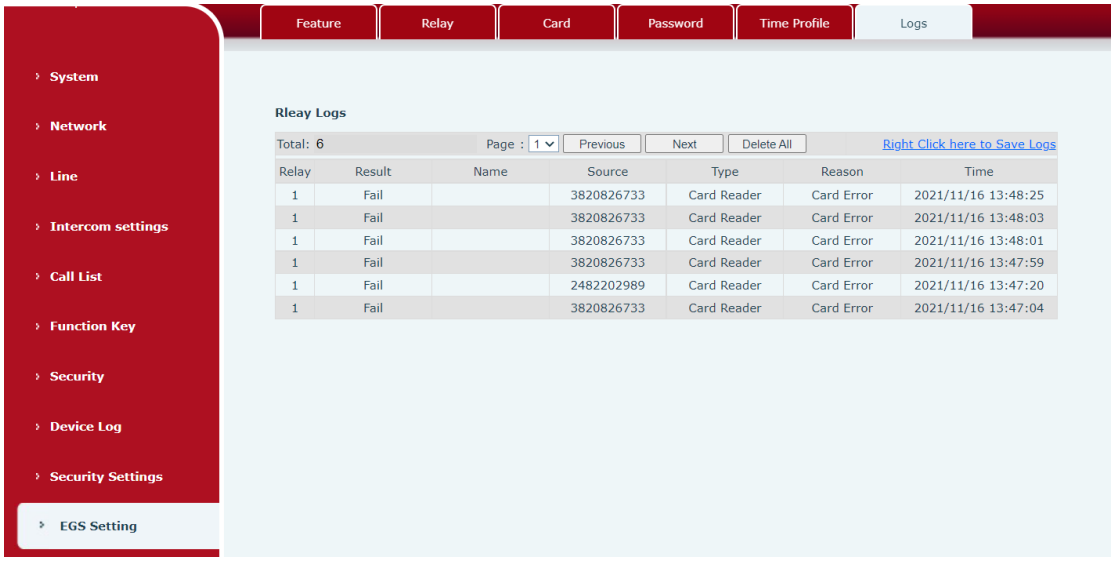


Picture 64 - Time Profile

Table 38 - Time Profile

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

9. 43 EGS Setting >> Logs



Picture 65 - Logs

Table 39 - Logs

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

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 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

User can restart the device through the webpage, click [**System**] >> [**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 configurations, database and configuration files on the device and the device will be restored to factory default state.

To restore the factory settings, please go to [**System**] >> [**Configuration**] >> [**Reset Phone**] page, and click [**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 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 40 - Trouble Cases

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