User Manual

i16V&i32V

Software Version：2.4.0

Release Date：2019/03/04

Directory

Directory 1

1 Picture 3

2 Table 5

3 Safety Instruction 1

4 Overview 2

5 Install Guide 3

5.1 Use POE or external Power Adapter 3

5.2 Appendix Table 4

5.2.1 Common command mode 4

5.2.2 Function key LED state 4

6 Basic Introduction 5

6.1 Panel shows 5

6.2 Quick Setting 5

6.3 WEB configuration 6

6.4 SIP Configurations 7

6.5 Door opening operation (only for i32V Door Phone) 7

7 Basic Function 9

7.1 Making Calls 9

7.2 Answering Calls 9

7.3 End of the Call 9

7.4 Auto-Answering 10

7.5 DND 11

7.6 Call Waiting 12

8 Advanced Function 14

8.1 Intercom 14

8.2 MCAST 14

8.3 Hotspot 16

9 Web Configurations 18

9.1 Web Page Authentication 18

9.2 System >> Information 18

9.3 System >> Account 19

9.4 System >> Configurations 19

9.5 System >> Upgrade 20

9.6 System >> Auto Provision 20

9.7 System >> FDMS 23
9.8 System >> Tools 23
9.9 Network >> Basic 24
9.10 Network >> VPN 27
9.11 Network >> Web Filter 28
9.12 Line >> SIP 29
9.13 Line >> Basic Settings 33
9.14 Line >> SIP Hotspot 34
9.15 EGS Setting >> Features 35
9.16 EGS Setting & Intercom Setting >> Audio 38
9.17 EGS Setting & Intercom Setting >> Video 40
9.18 EGS Setting & Intercom Setting >> MCAST 43
9.19 EGS Setting & Intercom Setting >> action URL 43
9.20 EGS Setting & Intercom Setting >> Time/Date 43
9.21 EGS Settings >> Trusted Certificates 44
9.22 EGS Settings >> Device Certificates 45
9.23 EGS Access 46
9.24 EGS Logs 48
9.25 Door Lock 49
9.26 Alert &Security Settings 51
9.27 Function Key 53

10 Trouble Shooting 57

10.1 Get device system information 57
10.2 Reboot device 57
10.3 Device factory reset 57
10.4 Network Packets Capture 57
10.5 Common Trouble Cases 57

1 Picture

Figure 1 - Panel 5
Figure 2 - Quickly setting 6
Figure 3 - WEB Login 6
Figure 4 - Line Registered 7
Figure 5 - Function Setting 9
Figure 6 - Set Release 10
Figure 7 - Enable Auto Answer 10
Figure 8 - Set DND Option 11
Figure 9 - Enable DND 12
Figure 10 - Call Waiting 13
Figure 11 - WEB Intercom 14
Figure 12 - MCAST 15
Figure 13 - SIP Hotspot 17
Figure 14 - WEB Account 19
Figure 15 - System Setting 19
Figure 16 - Upgrade 20
Figure 17 - Auto Provision 20
Figure 18 - FDMS 23
Figure 19 - Tools 24
Figure 20 - Network Basic Setting 25
Figure 21 - VPN 27
Figure 22 - WEB Filter 28
Figure 23 - WEB Filter Table 29
Figure 24 - SIP Line Configuration 30
Figure 25 - Network Basic 33
Figure 26 - Line Basic Setting 34
Figure 27 - EGS Setting 35
Figure 28 - Audio Setting 38
Figure 29 - Video Setting 40
Figure 30 - Trusted Certificates 45
Figure 31 - Device Certificates 45
Figure 32 - EGS Access 46
Figure 33 – EGS Logs 48
Figure 34 - Door Lock 49
Figure 35 - Alert/Security Settings 51
Figure 36 - Function Key Settings 53

Figure 37 – Hot Key Settings 54
Figure 38 – Multicast Settings 54
Figure 39 – Advanced Settings 55

2 Table

Table 1 – Common command mode....4
Table 2 - Function key LED state....4
Table 3 - Panel introduction....5
Table 4 - Intercom....14
Table 5 - MCAST....15
Table 6 - SIP Hotspot....16
Table 7 - Auto Provision....21
Table 8 - FDMS....23
Table 9 - Network Basic Setting....25
Table 10 - SIP Line Configuration....30
Table 11 - Line Basic Setting....34
Table 12 - EGS Setting....35
Table 13 - Audio Setting....38
Table 14 - Video Setting....43
Table 15 - MCAST parameters....43
Table 16 - action URL....43
Table 17 - Time/Date....43
Table 19 - EGS Logs Parameter....49
Table 20 - Door Lock Parameter....50
Table 21 - Alert/Security Settings....51
Table 22 - Function Key Settings....53
Table 23 – Hot Key Settings....54
Table 24 – Multicast Settings....55
Table 25 – Advanced Settings....55
Table 26 – Common Trouble Cases....58

3 Safety Instruction

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

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

4 Overview

i16V is a SIP visual intercom and i32V is a SIP video door phone developed for industry users on the basis of over ten years of VoIP phone technology. The voice transmission is based on the standard IP/RTP protocol, and the video transmission on RTSP protocol. They inherit Fanvil IP phones' advantages like good stability and tele-grade sound quality, and perfectly compatible with all current SIP-based main IP PBX/ soft switch /IMS platforms, such as Asterisk, Broadsoft, 3CX, Elastix, etc., for quickly deploying and provision.

i32V integrates multiple door open methods like remote door opening, password door opening, RFID card opening and indoor opening, with high cost performance and is the ideal choice for customers.

5 Install Guide

5.1 Use POE or external Power Adapter

i16V&i32V, 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 supplied by Fanvil and the POE switch met the specifications to ensure the device work properly.

5.2 Appendix Table

5.2.1 Common command mode

Table 1 - Common command mode

Action	Description
IP Broadcast under standby mode	In standby mode, long presse the speed dial button for 10 seconds, there will be a toot sound and the indicator light will flash 5 seconds, please press the speed dial button once within 5 seconds, the toot sound will stop automatically reporting IP
Switch network mode	In standby mode, long press the speed dial button for 10 seconds, there will be a toot sound and the indicator light will flash 5 seconds. Within 5 seconds, press the speed dial button three times quickly to switch the network mode. Network state in static or PPPoE mode will be switched to DHCP mode; If the network is in DHCP mode, it will switch to static IP 192.168.1.128. IP will be reported after successful switch

5.2.2 Function key LED state

Table 2 - Function key LED state

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

6 Basic Introduction

6.1 Panel Overview

i32V i16V

Figure 1 - Panel

Table 3 - Panel introduction

Number	Name	Description
1	IP Camera	Video signal acquisition and transmission
2	Speaker	Play sound
3	Speed dial button	For speed dial, multicast, intercom, IP broadcast and other functions
4	MIC	Collect voice
5	Card reader area	RFID card reader area,supports IC card and ID card

6.2 Quick Setting

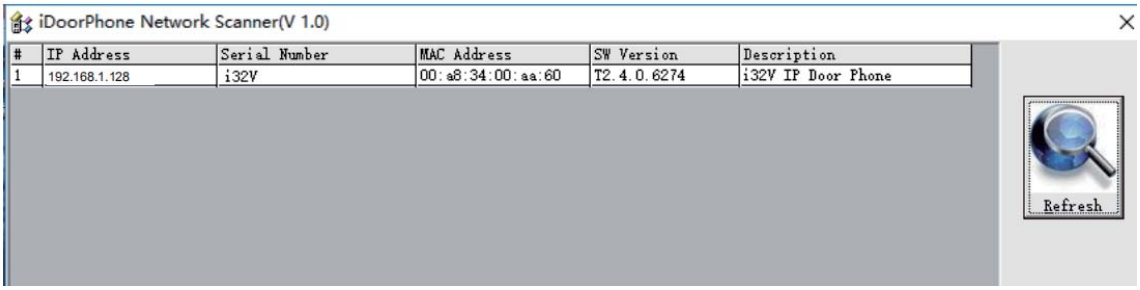
Before proceeding with this step, make sure your Internet broadband connection is working properly and complete the network hardware connection. The default factory mode of i32V is DHCP and i16V is static IP address mode. IP address can be viewed by.

- In standby mode, long presses the speed dial button for 10 seconds, there will be a beeping sound and indicator light flashes for 5 seconds, press the speed dial button once within 5

seconds (please do not operate within 30 seconds when power on), the voice will automatically play the IP address of the device or use the "IP scanning tool. exe" software to find the IP address of the device.

（Download http://download.fanvil.com/tool/iDoorPhoneNetworkScanner.exe）

- In standby mode, long presses the speed dial button for 10 seconds, there will be a beeping sound and indicator light flashes for 5 seconds, press the speed dial button once within 5 seconds (30 seconds after the power on), the voice will automatically play the IP address of the machine or use the "IP scanning tool. exe" software to find the IP address of the device.
- Login to the device's WEB page for configuration according to the IP address:
- Configure the account, user name, server address and other parameters required for registration provided by the service provider on the WEB configuration page;



The above picture shows the device information founded by the IP scanning tool, and the IP address is dynamic.

Figure 2 - Quickly setting

6.3 WEB configuration

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

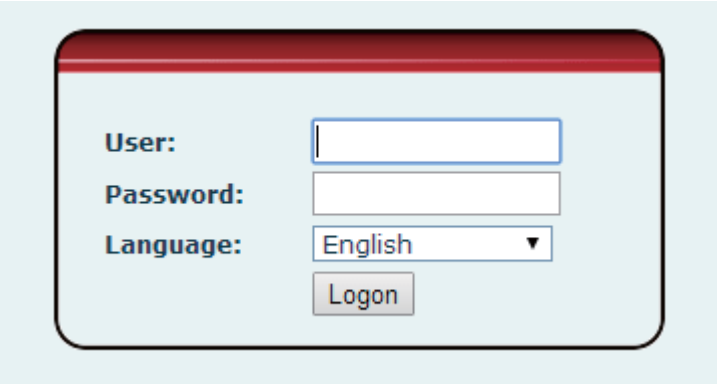


Figure 3 - WEB Login

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

6.4 SIP Configurations

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

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

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

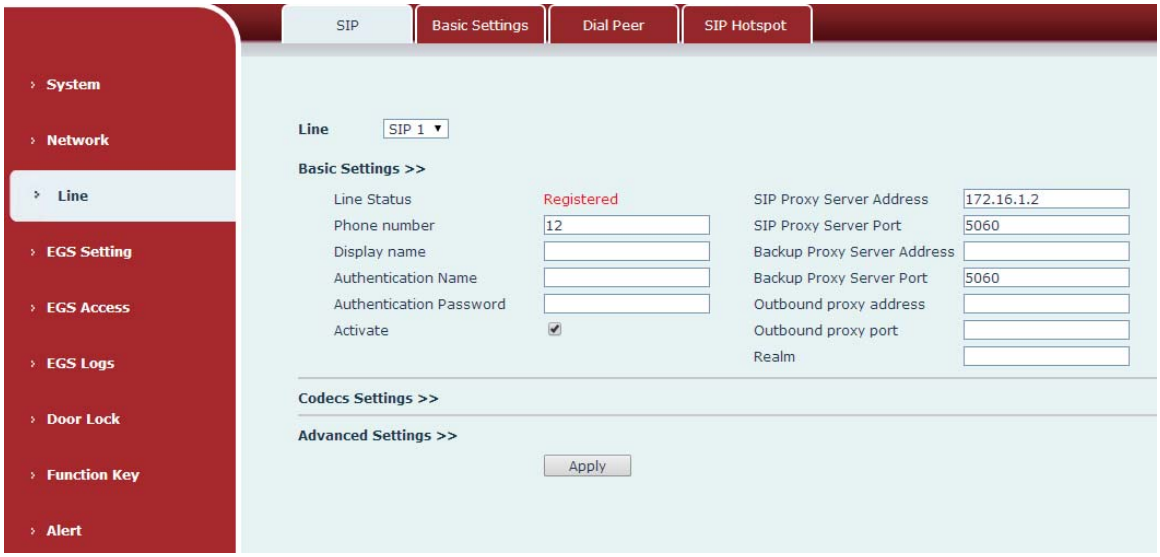


*Figure 4 - **SIP Line Configuration***

6.5 Door opening operation (only for i32V Door Phone)

Unlock the door in the following eight ways:

1) The door phone calls the appointed number, and the receiver enters the remote door opening password to open the door.

3) The other device calls 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, and the remote telephone opening shall be enabled).
4) Open the door by swiping the RFID card, which supports IC card and ID card.
5) Indoor door opening, the door can be opened through the indoor door button when the door phone is in any state.
6) Enter the position speed dial + authentication code to open the door, and directly enter this authentication code to open the door in standby mode. Please refer to the access list Settings for details.
7) super administrator card and super administrator password to open the door, in the case of door phone software exception, can open the door through the super administrator card and super administrator password (super administrator password is only limited to the device with a keyboard).
8) Active URL control command opens the door
The open URL is http://user:pwd@host/cgi-bin/ConfigManApp.com?Key = F_LOCK & code = openCode
A. user and PWD are user names and passwords for logging into the web
B. openCode is the remote door opening password, and the default is *
Example: http://admin:admin@172.18.3.25/cgi-bin/ConfigManApp.com?Key = *
Access code input correct play long sound prompt access and remote users, input error through the low frequency short sound prompt.
Password input is prompted by high frequency long sound successful, input error is prompted by high frequency short sound.
When the door lock is opened, it will be prompted by playing the long sound..

7 Basic Function

7.1 Making Calls

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

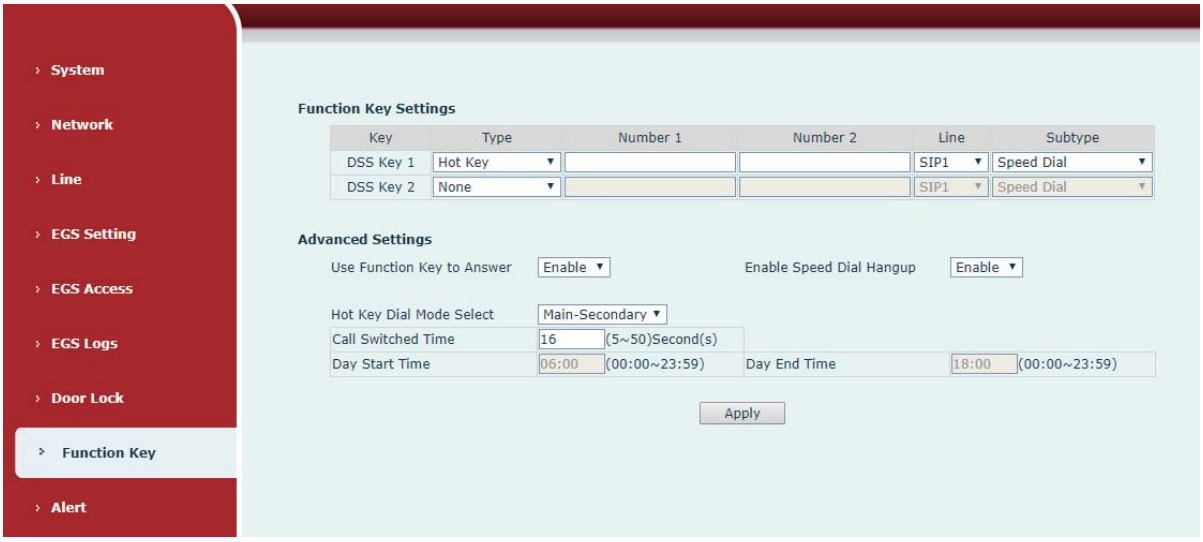


Figure 5 - Function Setting

See detailed configuration instructions 9.27 Function Key

7.2 Answering Calls

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

7.3 End of the Call

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 9.27 Function Key.

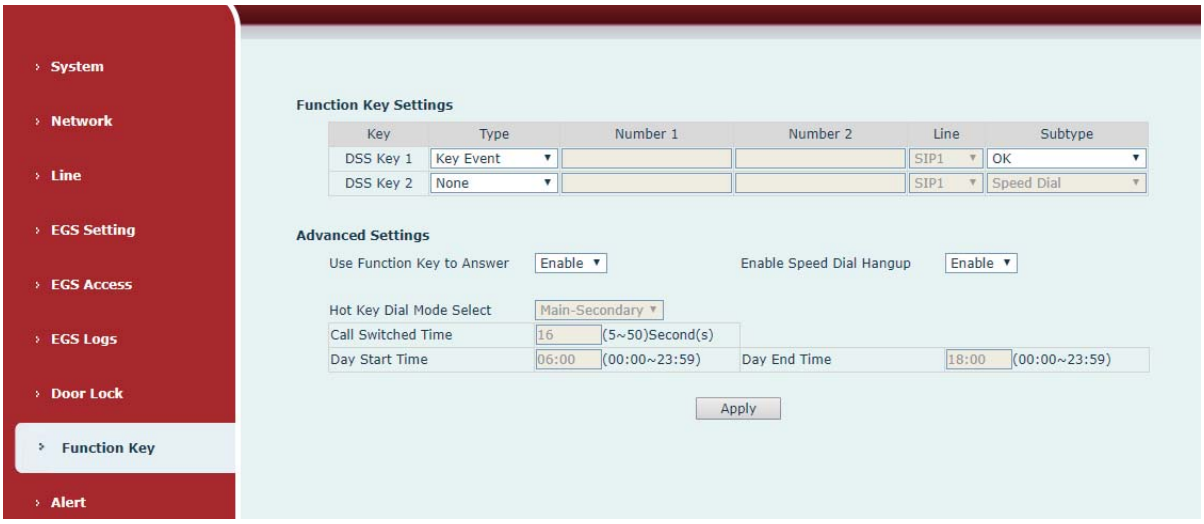


Figure 6 - Set Release

7.4 Auto-Answering

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

Web interface: enter [**EGS Setting**] >> [**Features**], Enable auto answer, set mode and auto answer time and click submit.

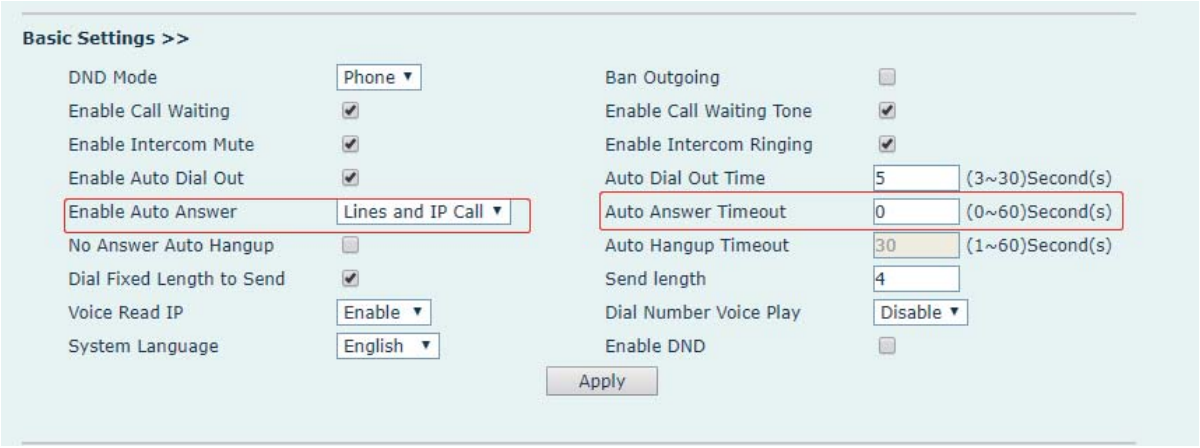


Figure 7 - Enable Auto Answer

- Auto Answer mode:
  - Disable：Turn off the automatic answer function, the device has a call, ring, will not time out to answer automatically.
  - Line1：Line 1 has an automatic call timeout.
  - Line2：Line 2 has an automatic call timeout.

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

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

- Auto Answer Timeout（0~60）

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

7.5 DND

Users can turn on the do-not-disturb (DND) feature on the device's web page to reject incoming calls (including call waiting).Do not disturb can be set by the SIP line respectively on/off.
Turn on/off all lines of the device without interruption by the following methods:

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

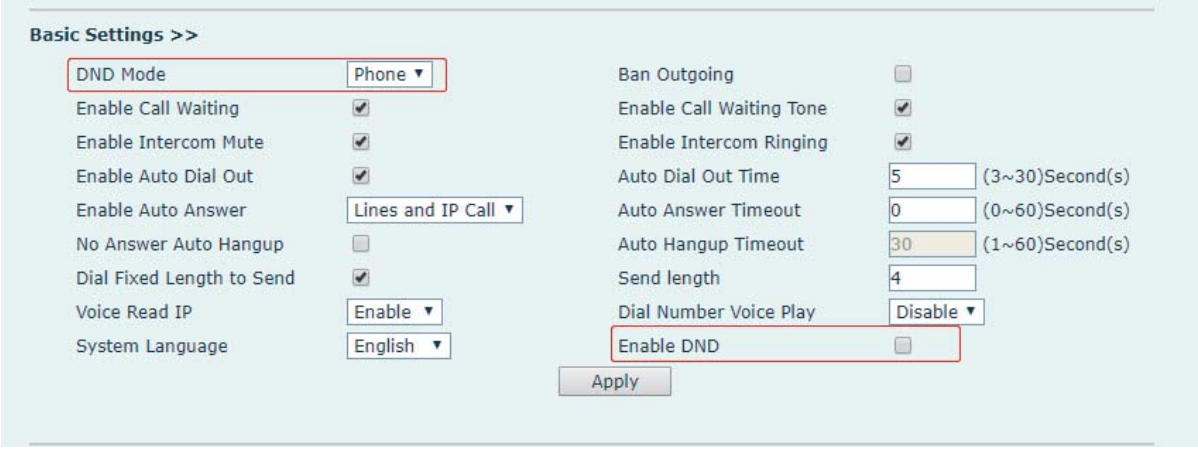


Figure 8 - Set DND Option

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

- Web interface: enter [**EGS Setting**] >> [**Features**], set the do not disturb type to Line, enter [**Line**] >> [**SIP**], choose a Line and enter [**Line**] >> [**Advanced settings**], Enable DND.

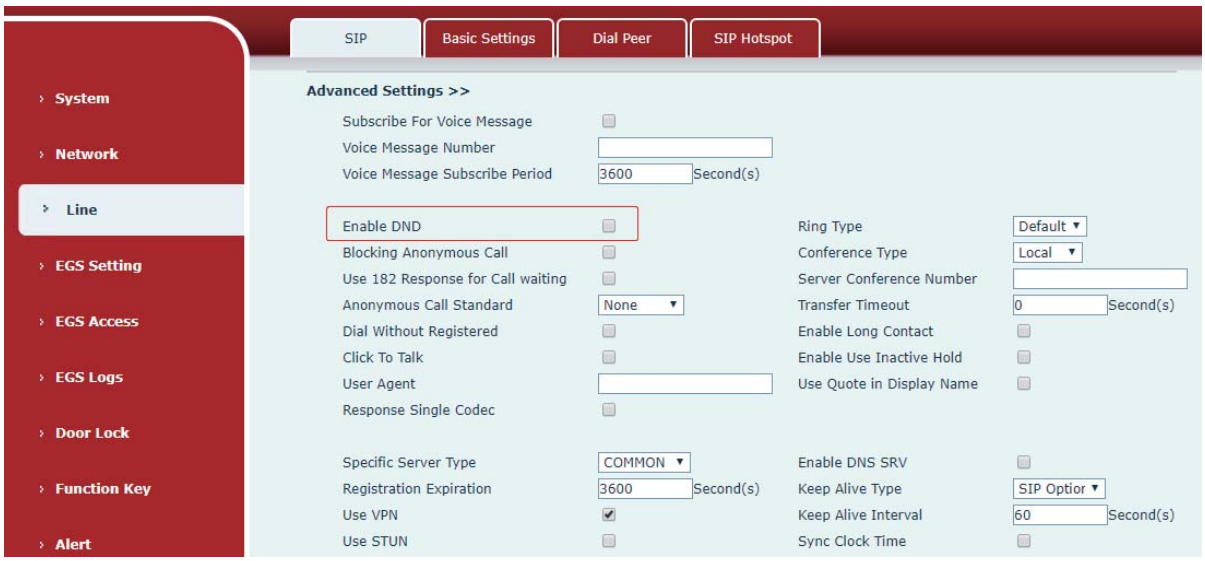


Figure 9 - Enable DND

7.6 Call Waiting

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

Users can enable/disable call waiting in the device interface and the web interface.

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

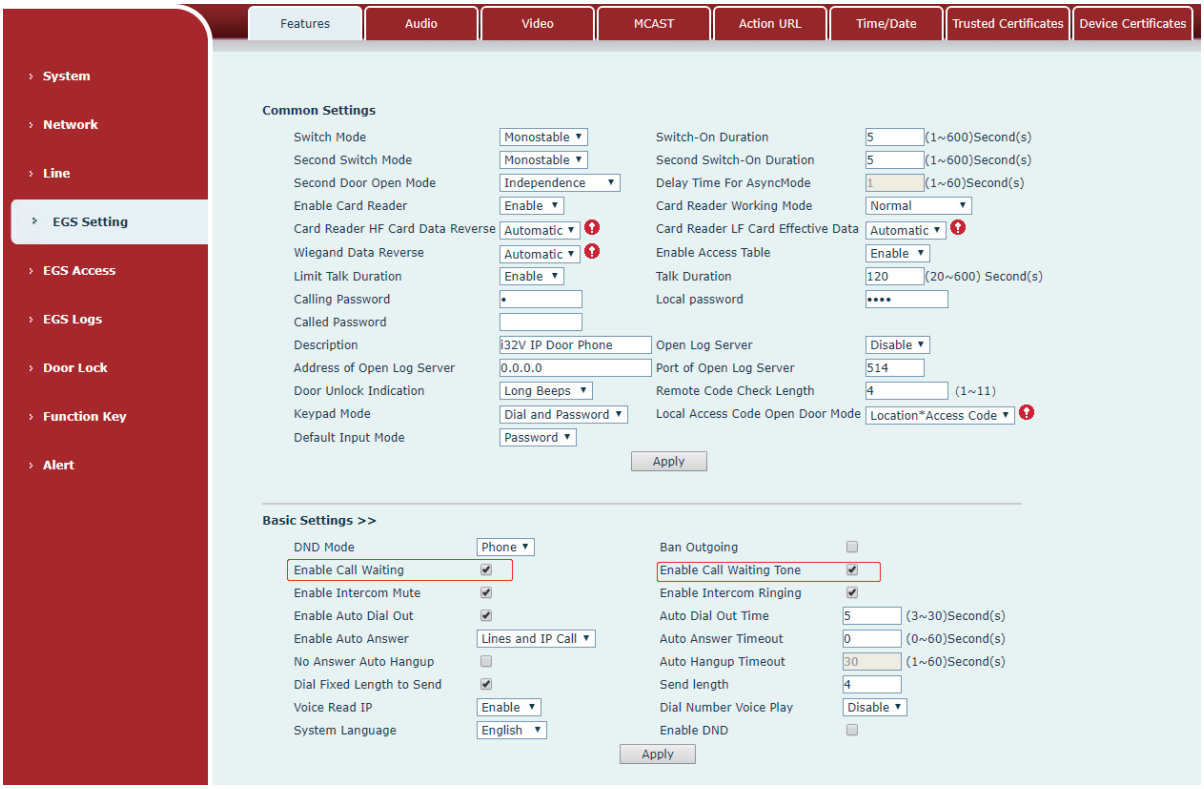


Figure 10 – Call Waiting

8 Advance Function

8.1 Intercom

The equipment can answer intercom calls automatically.

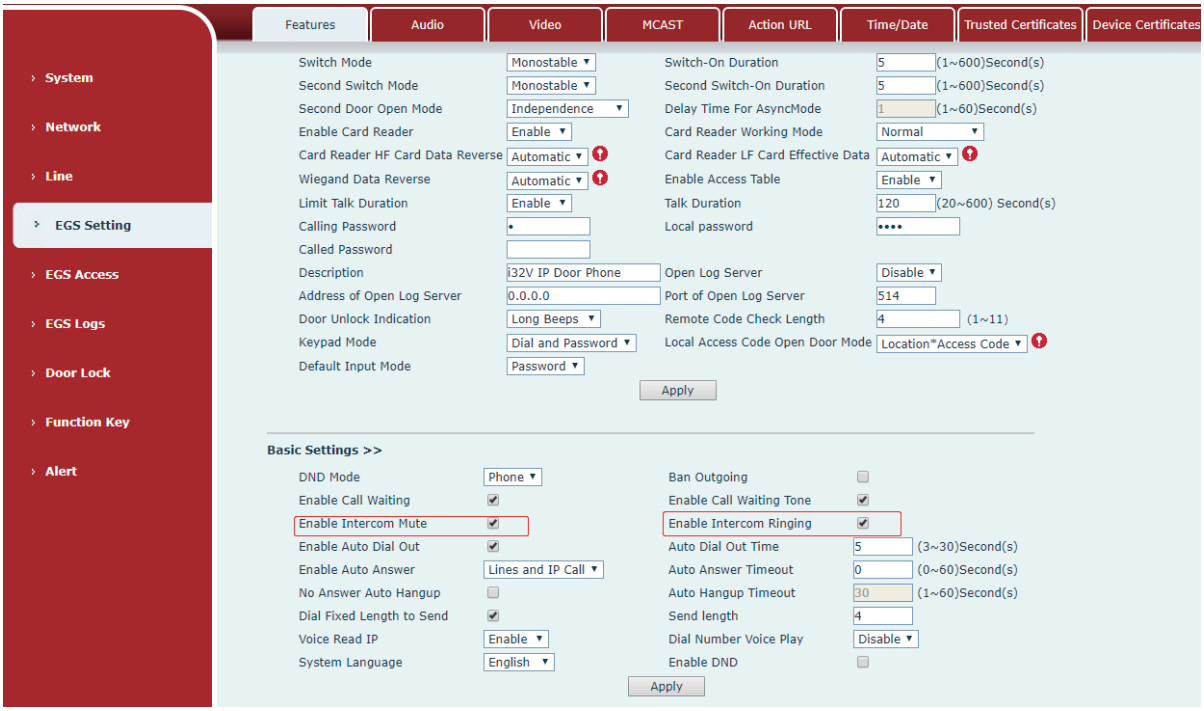


Figure 11 - WEB Intercom

Table 4 - Intercom

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

8.2 MCAST

This feature allows user to make some kind of broadcast call to people who are in multicast group. User can configure a multicast DSS Key on the phone, which allows user to send a Real Time Transport Protocol (RTP) stream to the pre-configured multicast address without involving SIP signaling. You can also configure the phone to receive an RTP stream from pre-configured multicast listening address without involving SIP signaling. You can specify up to 10 multicast listening addresses.

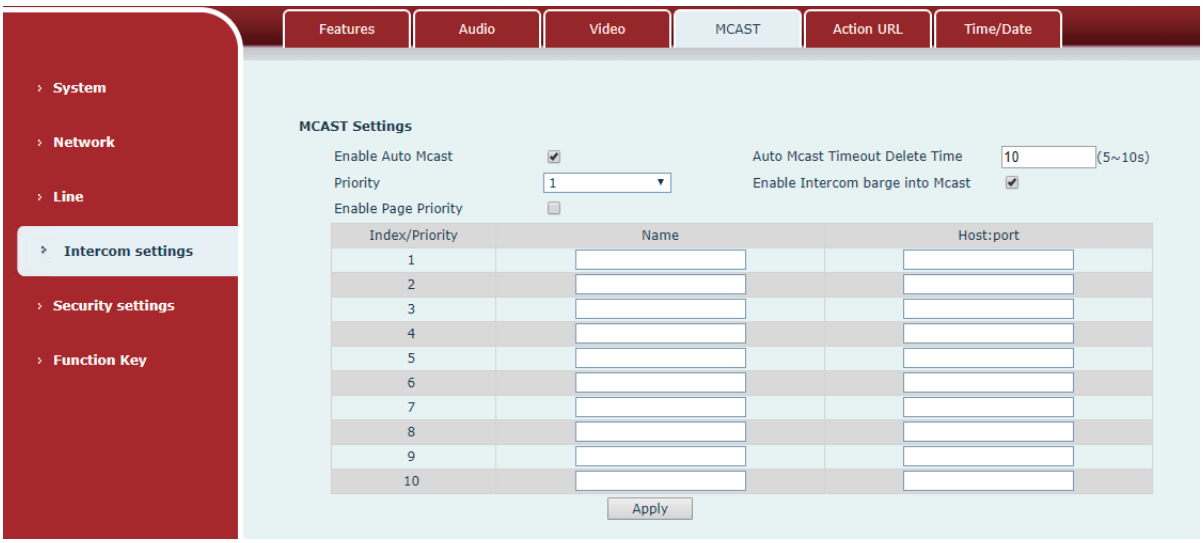


Figure 12 - MCAST

Table 5 - MCAST

Parameters	Description
Enable Auto Mcast	Send the multicast configuration information by Sip Notify signaling, and the device will configure the information to the system for multicast listening or cancel the multicast listening in the system after receiving the information
Auto Mcast Timeout Delete Time	When a multicast call does not end normally, but for some reason the device can no longer receive a multicast RTP packet, this configuration cancels the listening after a specified time
Priority	The priority defined in the current call, 1 is the highest priority and 10 is the lowest.
Enable Intercom barge into Mcast	When enabled, intercom insertion is allowed on multicast calls
Enable Page Priority	Regardless of which of the two multicast groups is called in first, the device will receive the higher priority multicast first.
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 [**Phone Settings**] >> [**MCAST**].

- Press the DSSKY of Multicast Key which you set.
- Receive end will receive multicast call and play multicast automatically.

8.3 Hotspot

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

Table 6 - SIP Hotspot

Parameters	Description
Enable Hotspot	Set the enable hotspot option in the SIP hotspot configuration TAB to enabled
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.

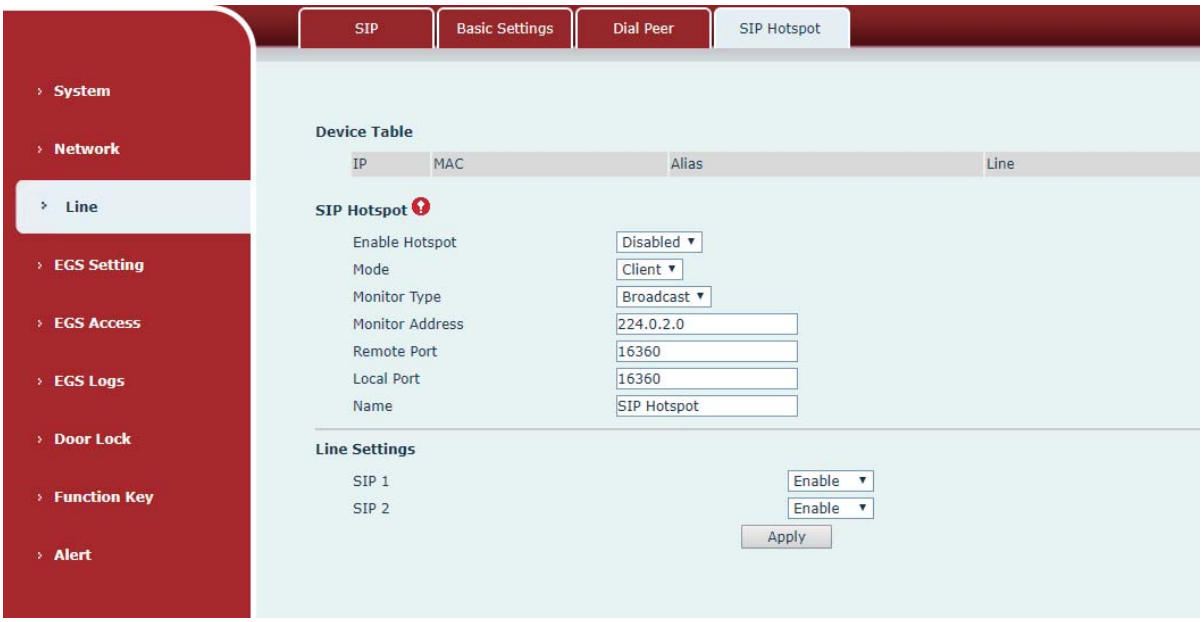


Figure 13 - SIP Hotspot

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

Calling internal extension:

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

9 Web Configurations

9.1 Web Page Authentication

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

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

9.2 System >> Information

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

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

And summarization of network status,

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

Besides, summarization of SIP account status,

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

9.3 System >> Account

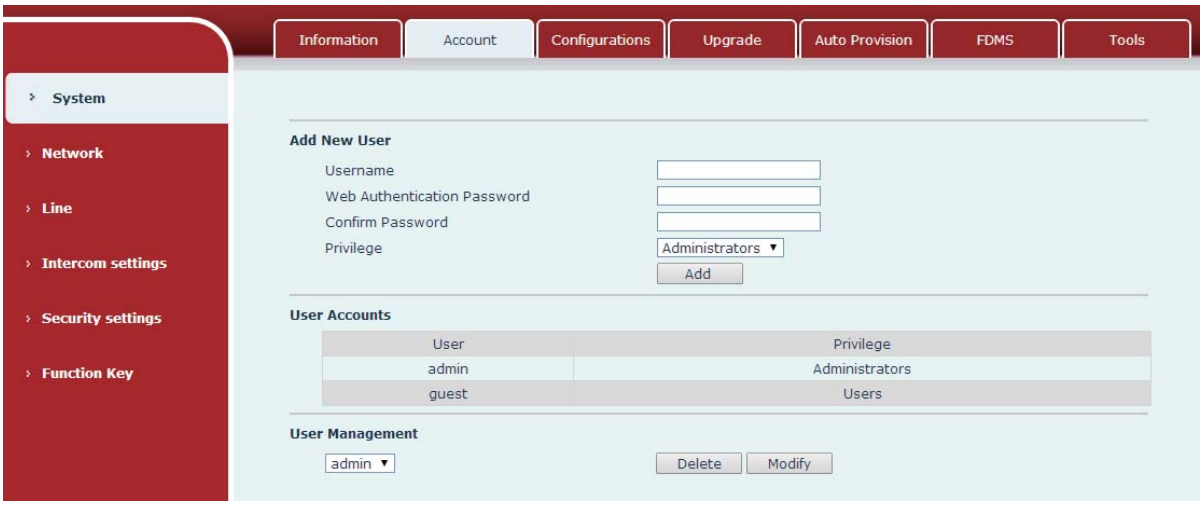


Figure 14 - WEB Account

On this page the user can change the password for the login page.

Users with administrator rights can also add or delete users, manage users, and set permissions and passwords for new users

9.4 System >> Configurations

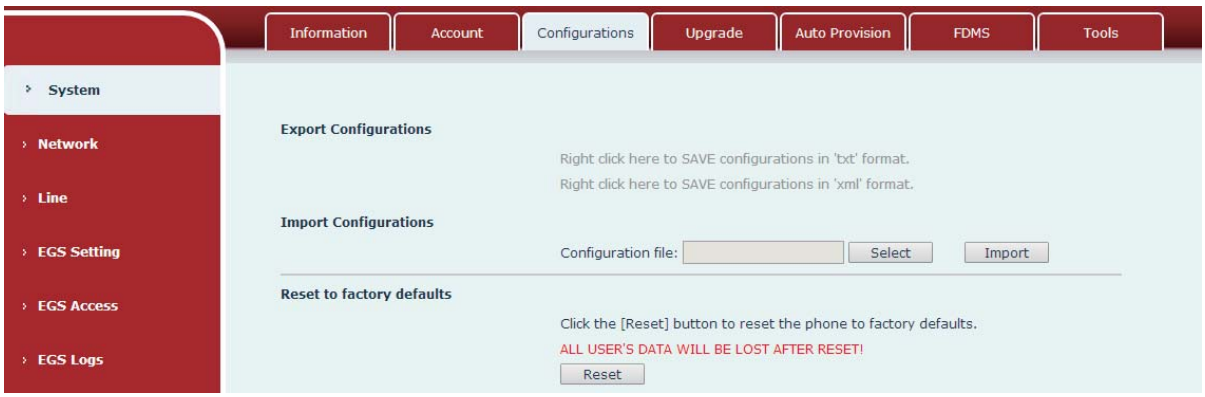


Figure 15 - System Setting

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

- **Export Configurations**

Right click to select target save as, that is, to download the device's configuration file, suffix ".txt". (note: profile export requires administrator privileges)

- **Import Configurations**

Import the configuration file of Settings. The device will restart automatically after successful

import, and the configuration will take effect after restart

■ **Reset Phone**

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

9.5 System >> Upgrade

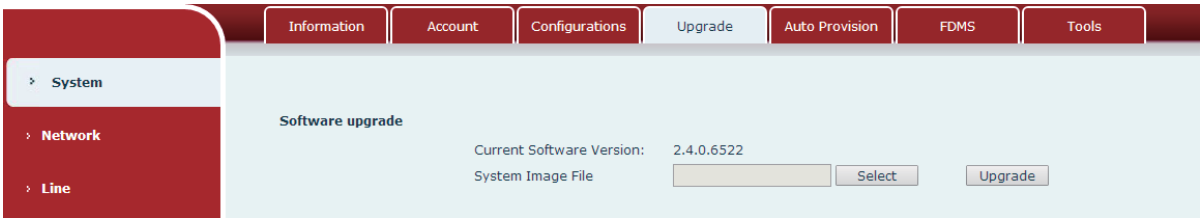


Figure 16 - Upgrade

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

9.6 System >> Auto Provision

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

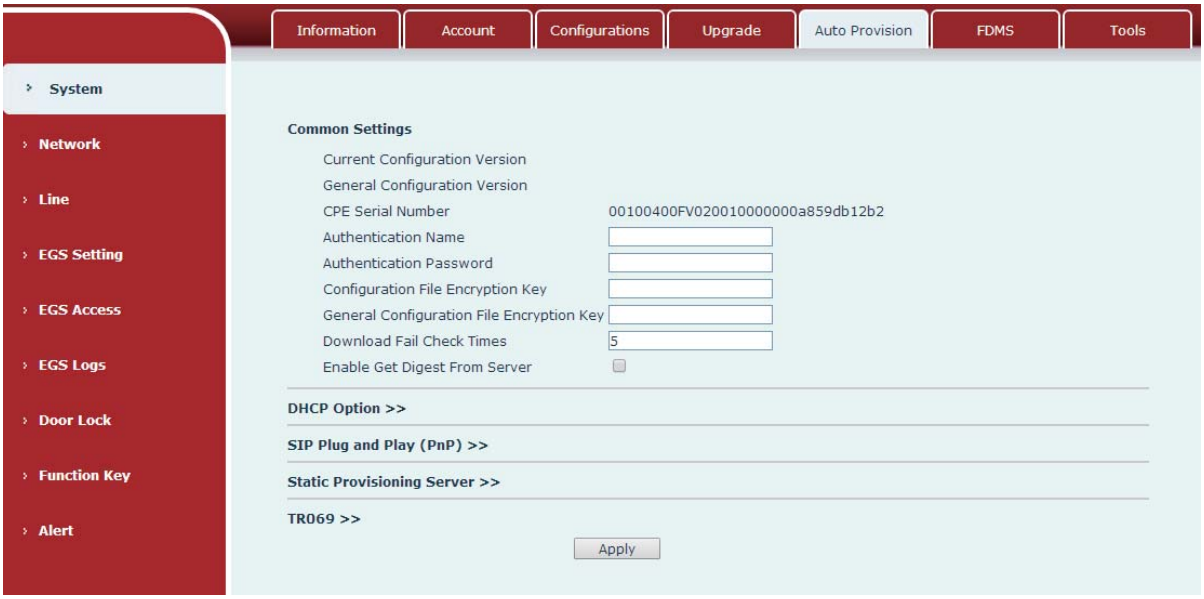


Figure 17 - Auto Provision

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

PNP>DHCP>TR069> Static Provisioning

Transferring protocol: FTP、 TFTP、 HTTP、 HTTPS

Details refer to **Fanvil Auto Provision**

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

Table 7 - Auto Provision

Parameters	Description
Basic settings	
Current Configuration Version	Show the current config file's version. If the version of configuration downloaded is higher than this, the configuration will be upgraded. If the endpoints confirm the configuration by the Digest method, the configuration will not be upgraded unless it differs from the current configuration
General Configuration Version	Show the common config file's version. If the configuration downloaded and this configuration is the same, the auto provision will stop. If the endpoints confirm the configuration by the Digest method, the configuration will not be upgraded unless it differs from the current configuration.
CPE Serial Number	Serial number of the equipment
Authentication Name	Username for configuration server. Used for FTP/HTTP/HTTPS. If this is blank the phone will use anonymous
Authentication Password	Password for configuration server. Used for FTP/HTTP/HTTPS.
Configuration File Encryption Key	Encryption key for the configuration file
General Configuration File Encryption Key	Encryption key for common configuration file
Save Auto Provision Information	Save the auto provision username and password in the phone until the server url changes
Download Fail Check Times	The default value is 5. If the download configuration fails, it will be downloaded 5 times.
Enable Server Digest	When the feature is enable, if the configuration of server is changed, phone will download and update.
DHCP Option	

Option Value	The equipment supports configuration from Option 43, Option 66, or a Custom DHCP option. It may also be disabled.
Custom Option Value	Custom option number. Must be from 128 to 254.
Enable DHCP Option 120	Set the SIP server address through DHCP option 120.
SIP Plug and Play (PnP)	
Enable SIP PnP	Whether enable PnP or not. If PnP is enable, phone will send a SIP SUBSCRIBE message with broadcast method. Any server can support the feature will respond and send a Notify with URL to phone. Phone could get the configuration file with the URL.
Server Address	Broadcast address. As default, it is 224.0.0.0.
Server Port	PnP port
Transport Protocol	PnP protocol, TCP or UDP.
Update Interval	PnP message interval.
Static Provisioning Server	
Server Address	Set FTP/TFTP/HTTP server IP address for auto update. The address can be an IP address or Domain name with subdirectory.
Configuration File Name	The configuration file name. If it is empty, phone will request the common file and device file which is named as its MAC address. The file name could be a common name, $mac.cfg, $input.cfg. The file format supports CFG/TXT/XML.
Protocol Type	Transferring protocol type ，supports FTP、TFTP、HTTP and HTTPS
Update Interval	Configuration file update interval time. As default it is 1, means phone will check the update every 1 hour.
Update Mode	Provision Mode. 1. Disabled. 2. Update after reboot. 3. Update after interval.
TR069	
Enable TR069	Enable TR069 after selection
Enable TR069 Warning Tone	If TR069 is enabled, there will be a prompt tone when connecting.
ACS Server Type	There are 2 options Serve type, common and CTC.
ACS Server URL	ACS server address
ACS User	ACS server username (up to is 59 character)
ACS Password	ACS server password (up to is 59 character)

TR069 Auto Login	Enable/Disable TR069 Auto Login.
STUN server address	Enter the STUN address
Enable the STUN	Enable the STUN

9.7 System >> FDMS

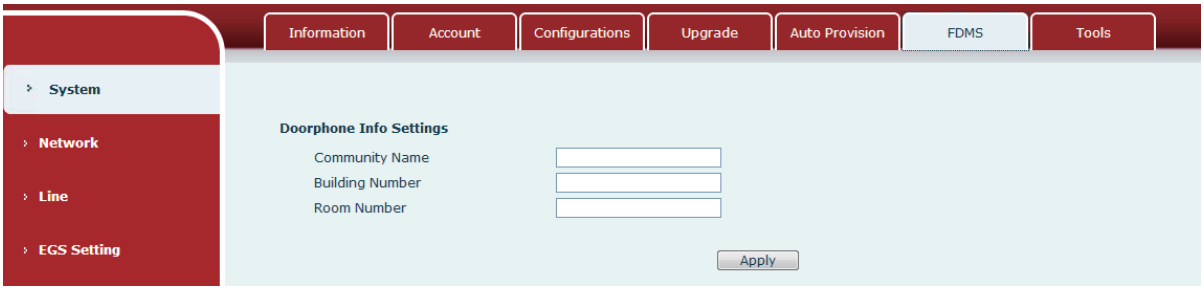


Figure 18 - FDMS

Table 8 - FDMS

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

9.8 System >> Tools

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

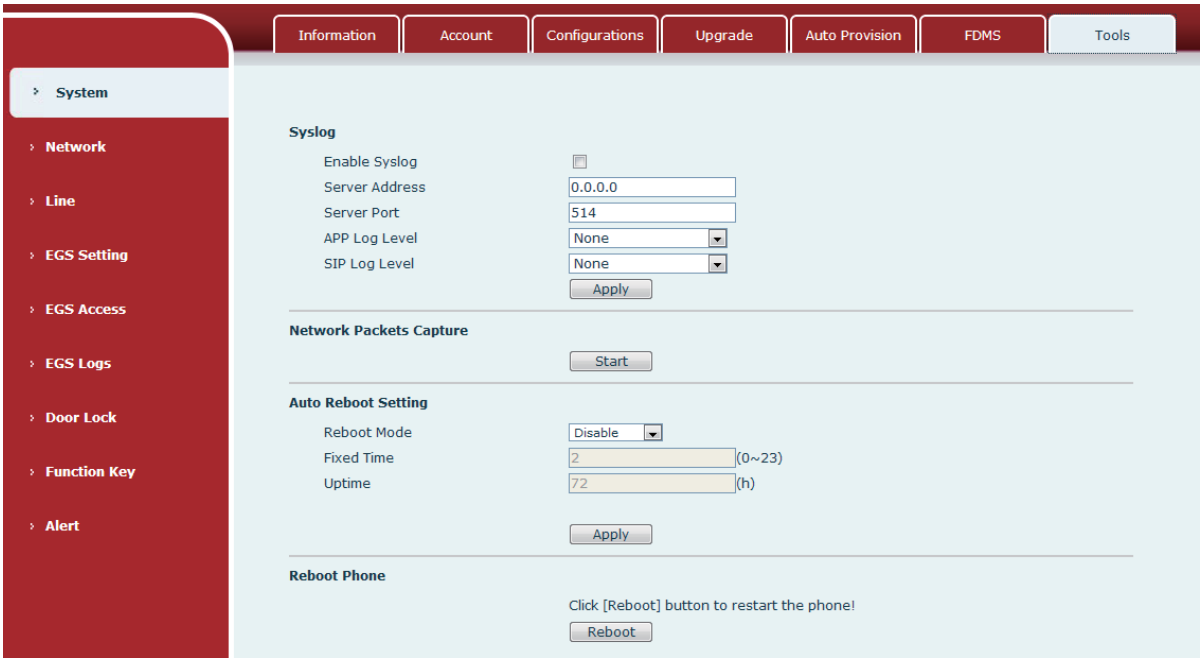


Figure 19 - Tools

Syslog： When enabled, set the syslog software address, and log information of the device will be recorded in the syslog software during operation. If there is any problem, log information can be analyzed by Fanvil technical support.

Auto Reboot Setting:

Reboot Mode:

Disable：It will not restart at set time after disabled

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

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

For other details, please refer to 10 trouble shooting

9.9 Network >> Basic

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

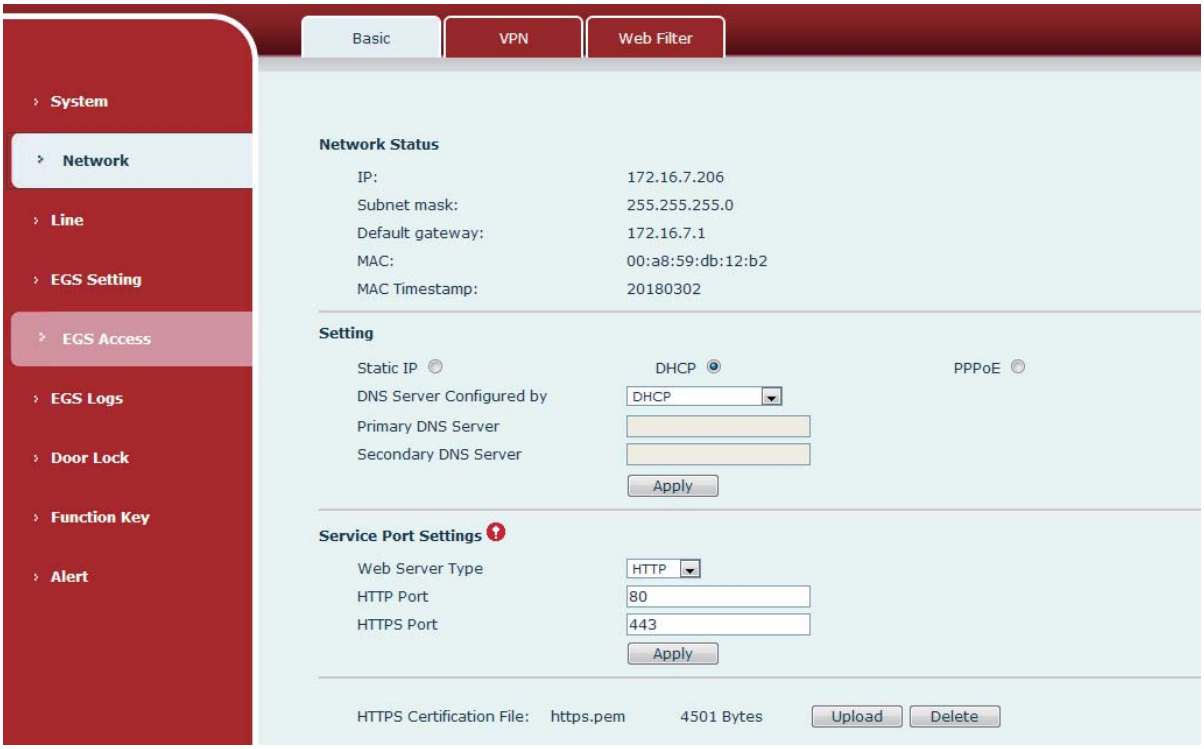


Figure 20 - Network Basic Setting

Table 9 - Network Basic Setting

Field Name	Explanation
Network Status	
IP	The current IP address of the equipment
Subnet mask	The current Subnet Mask
Default gateway	The current Gateway IP address
MAC	The MAC address of the equipment
MAC Time stamp	Get the MAC address of time.
Settings	
Select the appropriate network mode. The equipment supports three network modes:	
Static IP	Network parameters must be entered manually and will not change. All parameters are provided by the ISP.
DHCP	Network parameters are provided automatically by a DHCP server.
PPPoE	Account and Password must be input manually. These are provided by your ISP.
If Static IP is chosen, the screen below will appear. Enter values provided by the ISP.	

DNS Server Configured by	Select the Configured mode of the DNS Server.
Primary DNS Server	Enter the server address of the Primary DNS.
Secondary DNS Server	Enter the server address of the Secondary DNS.
attention： 1) After setting the parameters, click【submit】to take effect. 2) If you change the IP operation, the web page will no longer respond, at this time should be entered in the address bar new IP to connect to the device. 3) f the system USES DHCP to obtain IP at start up, and the network address of the DHCP Server is the same as the network address of the system LAN, then after the system obtains the DHCP IP, it will add 1 to the last bit of the network address of LAN and modify the IP address segment of the DHCP Server of LAN. If the DHCP access is reconnected to the WAN after the system is started, and the network address assigned by the DHCP server is the same as that of the LAN, then the WAN will not be able to obtain IP access to the network	
Service Port Settings	
Web Server Type	Specify Web Server Type – HTTP or HTTPS
HTTP Port	Port for web browser access. Default value is 80. To enhance security, change this from the default. Setting this port to 0 will disable HTTP access. Example: The IP address is 192.168.1.70 and the port value is 8090, the accessing address is http://192.168.1.70:8090.
HTTPS Port	Port for HTTPS access. Before using https, an https authentication certification must be downloaded into the equipment. Default value is 443. To enhance security, change this from the default.

9.10 Network >> VPN

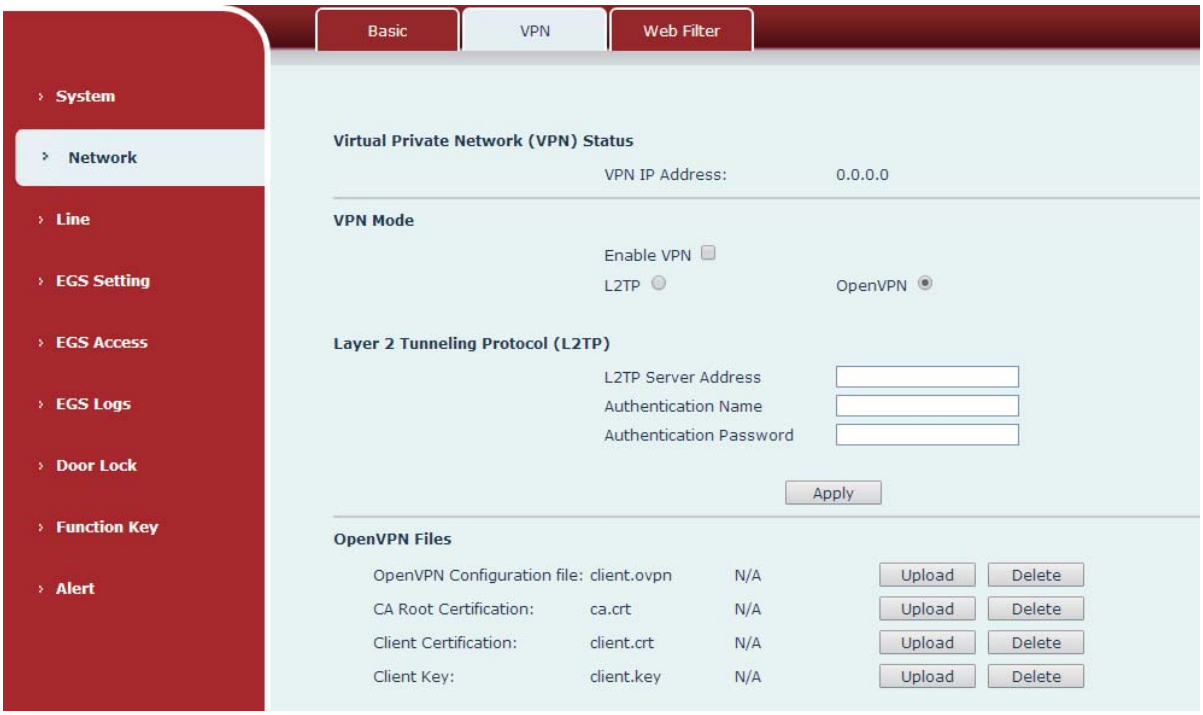


Figure 21 - VPN

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

For some users, especially enterprise users, a VPN connection might be required to be established before activate a line registration. The device supports two VPN modes, Layer 2 Transportation Protocol (L2TP) and OpenVPN.

The VPN connection must be configured and started (or stopped) from the device web portal.

- **L2TP**

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

To establish a L2TP connection, users should log in to the device web portal, open webpage [**Network**] >> [**VPN**]. In VPN Mode, check the "Enable VPN" option and select "L2TP", then fill in the L2TP server address, Authentication Username, and Authentication Password in the L2TP section. Press "Apply" then the device will try to connect to the L2TP server.

When the VPN connection established, the VPN IP Address should be displayed in the VPN

status. There may be some delay of the connection establishment. User may need to refresh the page to update the status.

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

- **OpenVPN**

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

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

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

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

9.11 Network >> Web Filter

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

Figure 22 - WEB Filter

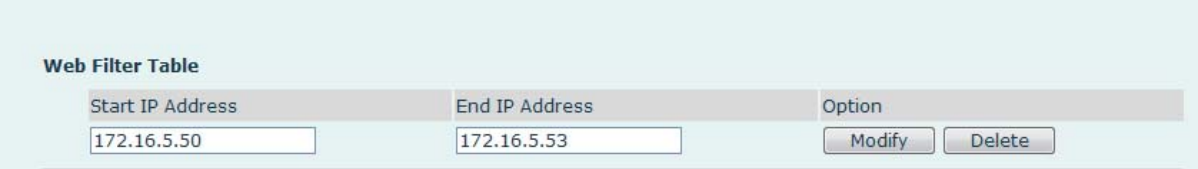


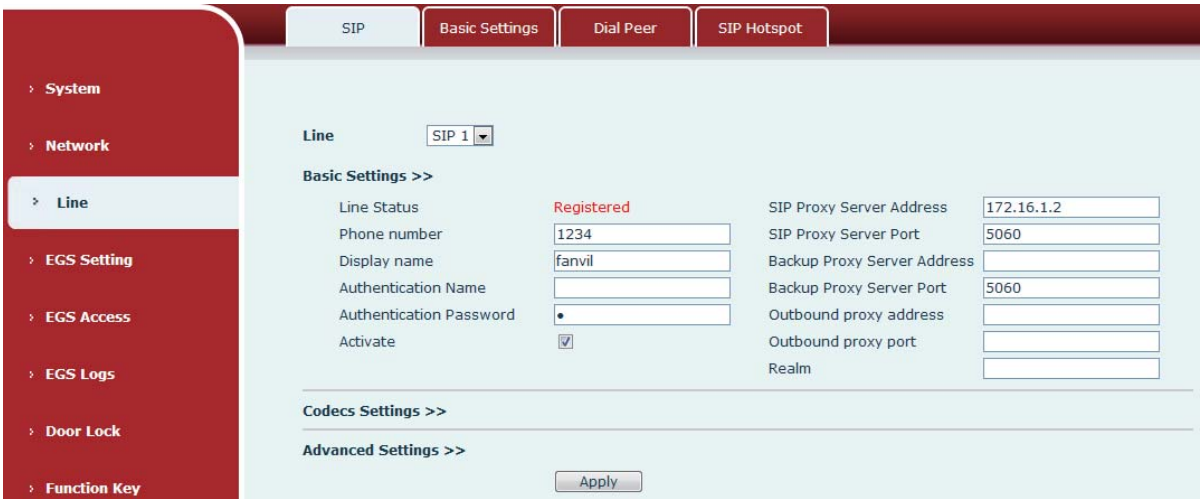
Figure 23 - WEB Filter Table

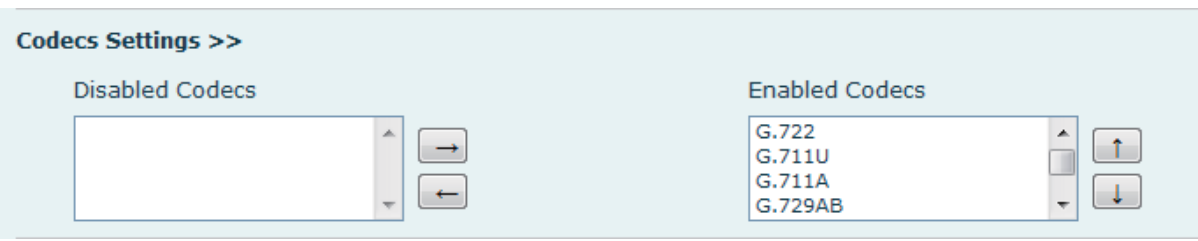
Add and remove IP segments that are accessible; Configure the starting IP address within the start IP, end the IP address within the end IP, and click [**Add**] to submit to take effect. A large network segment can be set, or it can be divided into several network segments to add. When deleting, select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

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

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

9.12 Line >> SIP





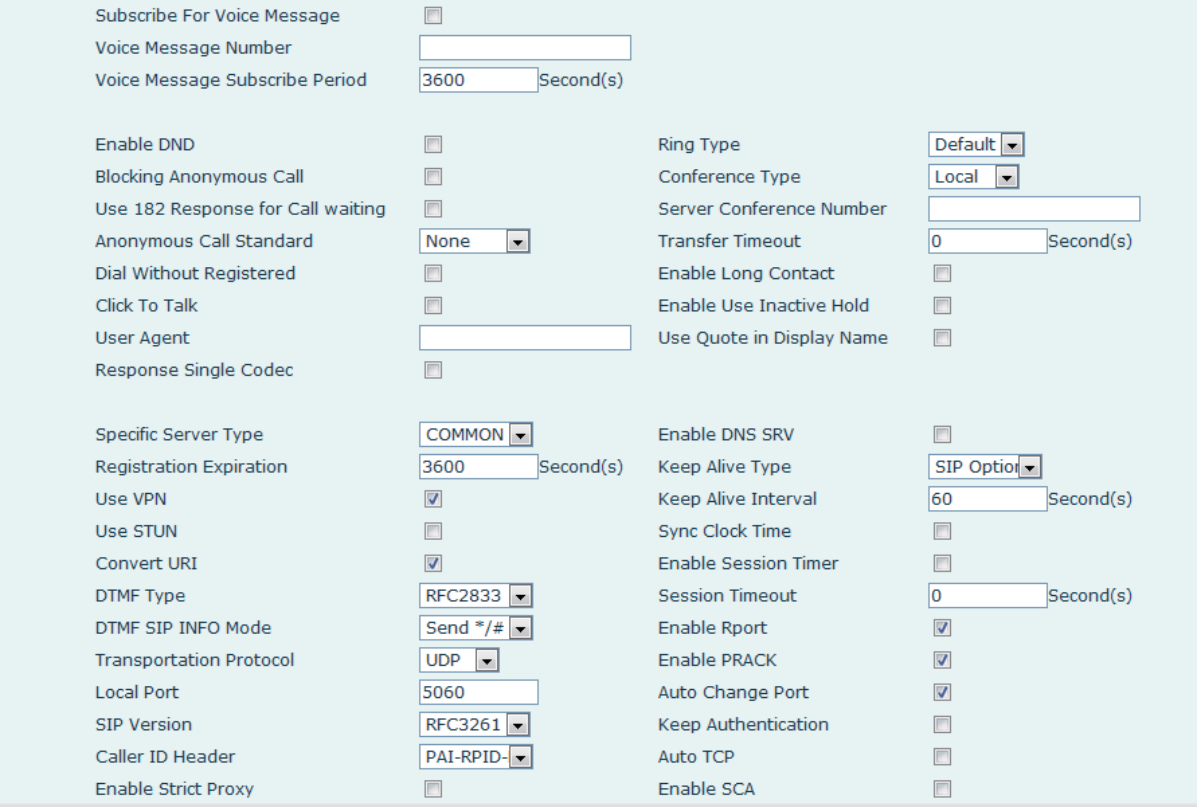


Figure 24 - SIP

Configure the service configuration for the wire on this page.

Table 10 - SIP

SIP	
Field Name	**Explanation**
Basic Settings (Choose the SIP line to configured)	
Line Status	Display the current line status at page loading. To get the up to date line status, user has to refresh the page manually.
Username	Enter the username of the service account.
Display name	Enter the display name to be sent in a call request.
Authentication Name	Enter the authentication name of the service account
Authentication Password	Enter the authentication password of the service account
Activate	Whether the service of the line should be activated
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server
SIP Proxy Server Port	Enter the SIP proxy server port, default is 5060

Outbound proxy address	Enter the IP or FQDN address of outbound proxy server provided by the service provider
Outbound proxy port	Enter the outbound proxy port, default is 5060
Realm	Enter the SIP domain if requested by the service provider
Codecs Settings	
Set the priority and availability of the codecs by adding or remove them from the list.	
Advanced Settings	
Subscribe For Voice Message	Enable the device to subscribe a voice message waiting notification, if enabled, the device will receive notification from the server if there is voice message waiting on the server
Voice Message Number	Set the number for retrieving voice message
Voice Message Subscribe Period	Set the interval of voice message notification subscription
Enable DND	Enable Do-not-disturb, any incoming call to this line will be rejected automatically
Blocking Anonymous Call	Reject any incoming call without presenting caller ID
Use 182 Response for Call waiting	Set the device to use 182 response code at call waiting response
Anonymous Call Standard	Set the standard to be used for anonymous
Dial Without Registered	Set call out by proxy without registration
Click To Talk	Set Click To Talk
User Agent	Set the user agent, the default is Model with Software Version.
Response Single Codec	If setting enabled, the device will use single codec in response to an incoming call request
Ring Type	Set the ring tone type for the line
Conference Type	Set the type of call conference, Local=set up call conference by the device itself, maximum supports two remote parties, Server=set up call conference by dialing to a conference room on the server
Server Conference Number	Set the conference room number when conference type is set to be Server
Transfer Timeout	Set the timeout of call transfer process
Enable Long Contact	Allow more parameters in contact field per RFC 3840
Enable the Inactive	Active capture package SDP is inactive, while the hold is sendrecv.

Hold	Active capture package has no response of 400, etc. Hold the hair inactive After closing the grab packet, you can see that the DSP is sendonly and the hold is sendrecv
Use Quote in Display Name	Whether to add quote in display name
Specific Server Type	Set the line to collaborate with specific server type
Registration Expiration	Set the SIP expiration interval
Use VPN	Set the line to use VPN restrict route
Use STUN	Set the line to use STUN for NAT traversal
Convert URI	Convert not digit and alphabet characters to %hh hex code
DTMF Type	Set the DTMF sending mode, there are four types: In-band RFC2833 SIP_INFO AUTO Different service providers may offer different models
DTMF SIP INFO Mode	When the device's DTMF type is set to SIP_INFO The DTMF_SIP_INFO type is configured to send */#, and when the device presses the */# key, the actual value sent is */#; Configured to send 10/11, when the device presses the */# key, the actual value sent is 10/11.
Transportation Protocol	Set the line to use TCP or UDP for SIP transmission
Local Port	Set the Local Port
SIP Version	Set the SIP version
Caller ID Header	Set the Caller ID Header
Enable Strict Proxy	Enables the use of strict routing. When the phone receives packets from the server, it will use the source IP address, not the address in via field.
Enable user=phone	Sets user=phone in SIP messages.
Enable SCA	Enable/Disable SCA (Shared Call Appearance)
Enable DNS SRV	Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole opened
Keep Alive Interval	Set the keep alive packet transmitting interval

Enable Session Timer	Set the line to enable call ending by session timer refreshment. The call session will be ended if there is not new session timer event update received after the timeout period
Session Timeout	Set the session timer timeout period
Enable Rport	Set the line to add rport in SIP headers
Enable PRACK	Set the line to support PRACK SIP message
Enable DNS SRV	Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list
Auto Change Port	Enable/Disable Auto Change Port
Keep Authentication	Keep the authentication parameters from previous authentication
Auto TCP	Using TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)
RTP Encryption	Set the pass phrase for RTP encryption
With Mac field	When enabled, all SIP messages strip Mac fields
Register with the Mac field	When enabled, register the message ribbon Mac field

9.13 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.

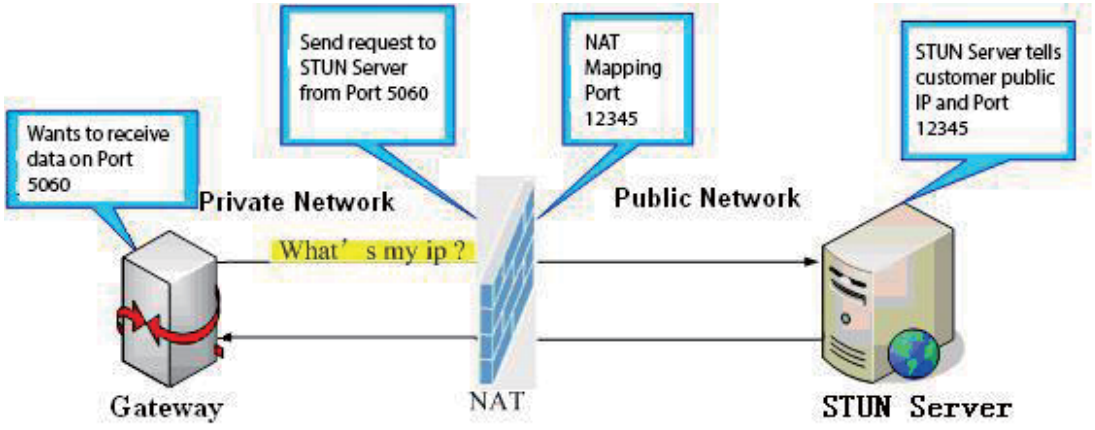


Figure 25 - Network Basic

Setting up SIP Global Configuration:

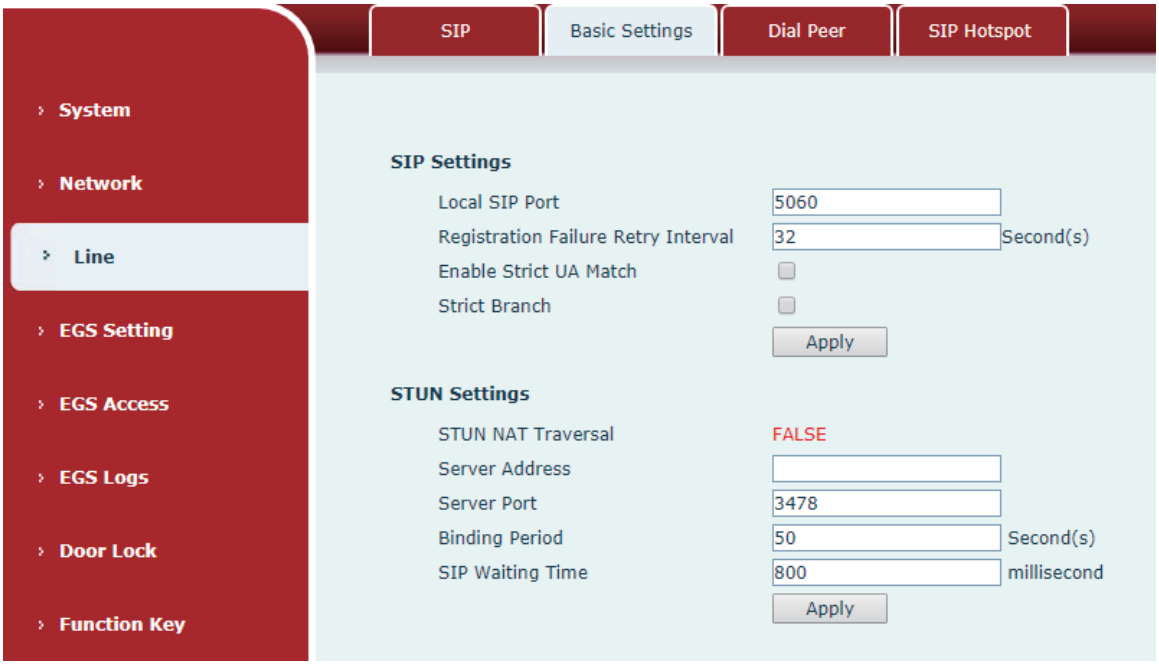


Figure 26 - Line Basic Setting

Table 11 - Line Basic Setting

Field Name	Explanation
SIP Settings	
Local SIP Port	Set the local SIP port used to send/receive SIP messages.
Registration Failure Retry Interval	Set the retry interval of SIP REGISTRATION when registration failed.
Enable Strict UA Match	Enable or disable Strict UA Match
Field Name	**Explanation**
STUN Settings	
Server Address	STUN Server IP address
Server Port	STUN Server Port – Default is 3478.
Binding Period	STUN blinding period – STUN packets are sent at this interval to keep the NAT mapping active.
SIP Waiting Time	Waiting time for SIP. This will vary depending on the network.

9.14 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.

9.15 EGS Setting >> Features

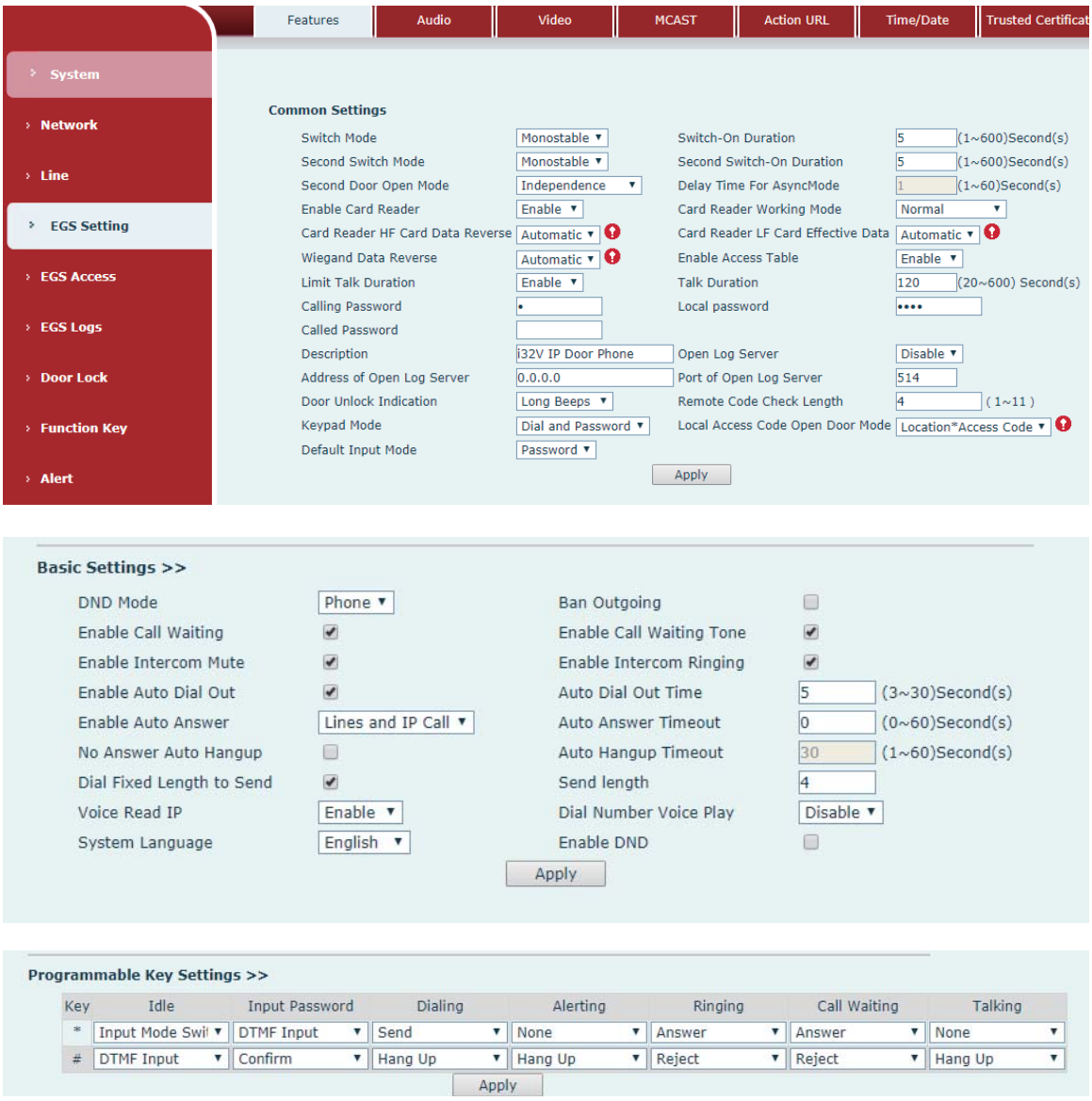


Figure 27 - EGS Setting

Table 12 - EGS Setting

EGS Features Setting (Only for Door phone)	
Field Name	**Explanation**
Basic Settings	
Switch Mode	Monostable: there is only one fixed action status for door unlocking. Bistable: there are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After changed, the status would be kept.

	Initial Value is Monostable
Switch-On Duration	Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial Value is 5 seconds.
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.
Card Reader HF Card Data Reverse	Set the HF card data reverse order, the default value is automatic. You can set it up when the card display is not consistent with the card number.
Card Reader LF Card Effective Data	The LF Card Effective Data, the default value is automatic.
Wiegand Data Reverse	Set Wiegand Data Reverse, the default value is automatic.
Enable Access Table	Disable remote password implementations for all calls to open doors; Enable remote password to open the door after calling only by access guard
Limit Talk Duration	If enabled, calls would be forced ended after talking time is up.
Talk Duration	The call will be ended automatically when time up. Initial Value is 120 seconds
Calling Password	Remote door unlocking password. Initial Value is “*”.
Description	Device description displayed on IP scanning tool software. Initial Value is “i32V IP Door Phone”.
Enable Open Log Server	Enable or disable to connect with log server
Address of Open Log Server	Log server address(IP or domain name)
Port of Open Log Server	Log server port (0-65535) , Initial Value is 514.
Door Unlock Indication	Indication tone for door unlocked. There are 3 type of tone: silent/short beeps/long beeps.
Remote Code Check Length	The remote access code length would be restricted with it. If the input access code length is matched with it, system would check it immediately. Initial Value is 4.
Basic Settings（Door Phone &Intercom Phone）	

DND (Do Not Disturb)	DND might be disabled phone for all SIP lines, or line for SIP individually. But the outgoing calls will not be affected
Ban Outgoing	If enabled, no outgoing calls can be made.
Enable Call Waiting	The default value is enabled. Allow users to answer the second call while maintaining the call.
Enable Call Waiting Tone	The default value is enabled. When enabled, the call waiting tone can be heard while waiting for a call. If this function is turned off, when waiting for a call, the beep will not be heard.
Enable Intercom Mute	If enabled, mutes incoming calls during an intercom call.
Enable Intercom Tone	If enabled, plays intercom ring tone to alert to an intercom call.
Enable Auto Dial Out	Enable Auto Dial Out when timeout.
Auto Dial Out Time	Configure waiting time for timeout dialing.
Enable Auto Answer	Enable Auto Answer function
Auto Answer Timeout	Set Auto Answer Timeout
No Answer Handdown	Enable automatically hang up when no answer
No Answer Auto Hangup	Configuration automatically hangs up when no answer occurs within the set time.
Auto Hangup Timeout	Set the time of no answer auto hangs up.
Dial Fixed Length to Send	Configure to enable/disable fixed-length automatic dial-out numbers.
Send length	Configure the receiving number length; default is 4. After the user dials the 4-digit number, the device will automatically call out the 4-digit number.
Dial Number Voice Play	Configure to enable/disable dial-up voice prompts, which are disabled by default.
System Language	Language for configuring voice prompts.
Enable DND	If this item is selected, the device will reject any incoming calls and the caller will remind the device not to use, but the local exhalation will not be affected.
Voice Read IP	Configure IP broadcasting (press the # key for 3 seconds in standby state); the default value is enabled.
Block Out Settings(Only for Door phone)	
Add or delete blocked numbers – enter the prefix of numbers which should not be dialed by the phone. For example, if 001 is entered, the phone would not dial any number beginning with	

001.
X and x are wildcards which match single digit. For example, if 4xxx or 4XXX is entered, the phone would not dial any 4 digits numbers beginning with 4. It would dial numbers beginning with 4 which are longer or shorter than 4 digits.

9.16 EGS Setting & Intercom Setting >> Audio

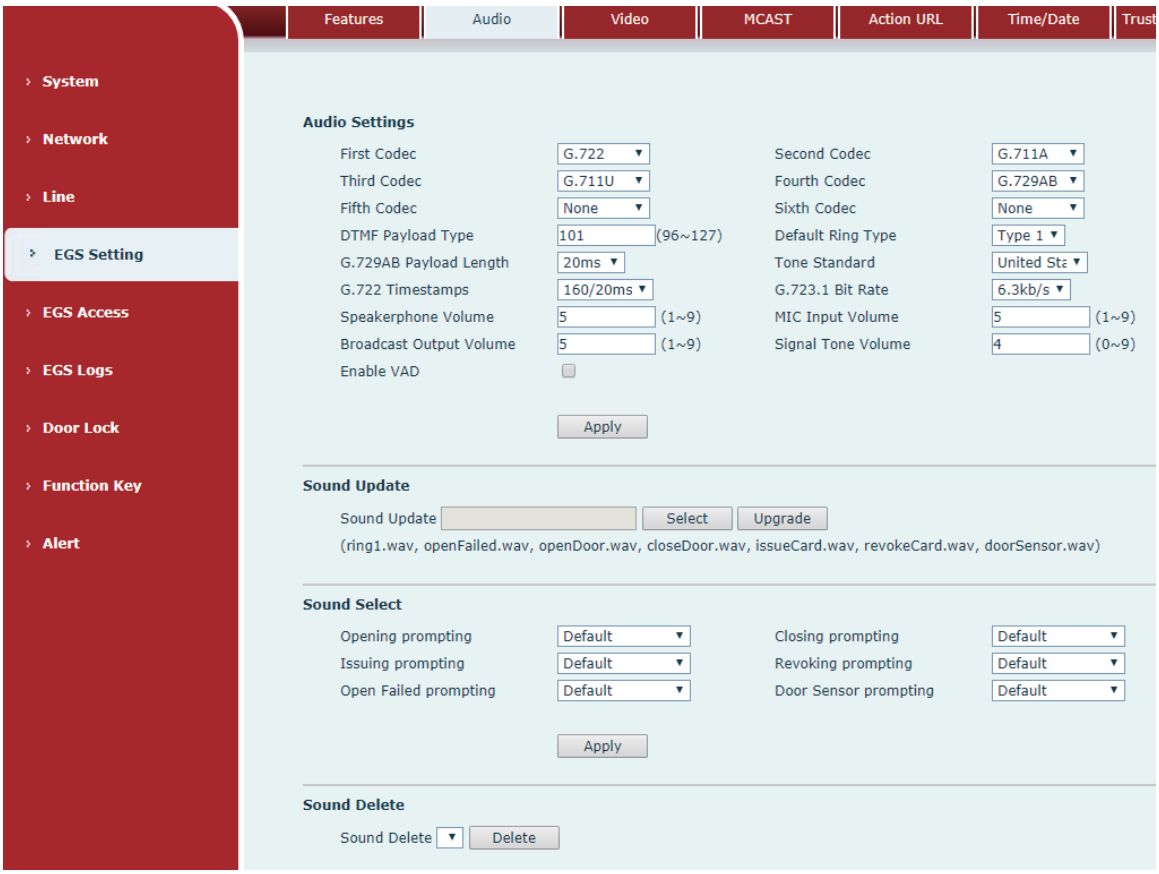


Figure 28 - Audio Setting

Table 13 - Audio Setting

Field Name	Explanation
Audio Settings	
Codec Setting	Select enabled or disabled audio codec: G.711A/U,G.722,G.723,G.729, G.726-16,G726-24,G726-32,G.726-40, ILBC,AMR,AMR-WB, opus
DTMF Payload Type	Setting DTMF payload type, the value range must be 96~127.
Default Ring Type	Configure the default ring tone. If no special ringtone is set for the caller number, the default ringtone will be used.

G.729AB Payload Length	You can select the G.729AB Payload Length ,the options are 10ms、20ms、30ms、40ms、50ms、60ms.
G.722 Timestamps	You can choose G.722 Timestamps for 160/20ms or 320/20ms.
G.723.1 Bit Rate	You can choose G.723.1 Bit Rate of 5.3 kb/s or 6.3 kb/s.
Speakerphone Volume	Set the hands-free volume to 1-9
MIC Input Volume	Set the microphone volume to 1~9
Broadcast Output Volume	Set the broadcast output volume to 1~9
Signal Tone Volume	Set the signal sound volume to 0~9
Enable VAD	Whether voice activity detection is enabled.
Sound Update	
Sound Update	Can be upgraded suffix ". Wav "format of the door, door, and other custom prompt sound
Sound Select	
Opening prompting	Can be set to default and voice prompt
Closing prompting	Can be set to default and voice prompt
Issuing prompting	Can be set to default and voice prompt
Revoking prompting	Can be set to default and voice prompt
Open Failed prompting	Can be set to default and voice prompt
Sound Delete	
Sound Delete	Upgraded ringtones are displayed in the delete list, which can be optionally deleted

9.17 EGS Setting & Intercom Setting >> Video

Figure 29 - Video Setting

Camera connection Settings	
Field Name	**Explanation**
Camera status and number of visits	Camera status: When the device is restarted, the camera status shows whether it is currently available. The maximum number of accesses, the maximum number of main code streams, the maximum number of subcode streams and the number of uses.
Video Capture（Local）	
IRCUT Mode	Auto: IRCUT switches according to the actual ambient light level of the camera Synchronization: The switching of the IRCUT is determined by the actual brightness of the IR lamp.
Day/Night Mode	Automatic: automatically switches according to the DNC Threshold and the brightness of the actual environment where the camera is located Day Mode: The camera's video screen is always colored, if there is IR-cut will be synchronized to switch. Night Mode: the camera's video screen is always black and white, if there is IR-cut will be synchronized switch.
White Balance	Automatic: Automatically adjusts according to the actual environment in which the camera is located. Outdoor: installed in the outdoor preferred. Indoor: installed in the room preferred.
Horizon Flip	The video is flipped horizontally
Anti Flicker	Enable the option. In a fluorescent environment can eliminate the video horizontal scroll
Vertical Flip	The video is flipped horizontally
IR Swap	IR-cut filter switch
DNC Threshold	In the Day / Night mode Auto option, the color switching black and white threshold is set Set the video color to black and white threshold in the day and night mode selection auto mode
Backlight Compensation	In front of a very strong background light can see people or objects clearly
AutoFill Sensitivity	In the environment changes in light and shade, the higher the sensitivity the faster the video changes
wide dynamic	The wide dynamic is related to the optimization of the backlight scene. When people are in the backlight condition, it may be because the background is

	too bright and the person is a piece of black, which is helpful for optimization after opening
Wide dynamic upper limit	range
Fill Light	Provide auxiliary light when shooting in the absence of light conditions
Time Title	Video can see the time information
Video Title	Enable/disable camera titles
Video Title Content	When enabled, video can see the set title information
Video Encode（Local）	
Field Name	**Explanation**
Encode Format	Only H.264 encoding format is supported
Resolution	Main stream: support 720P Sub-stream: D1 (704 * 576)
Frame Rate	The larger the value is, the more coherent the video would be got; not recommend adjusted.
Bitrate Control	CBR: If the code rate (bandwidth) is insufficient, it is preferred. VBR: Image quality is preferred, not recommended.
Quality	Video quality adjustment, the better the quality needs to transfer faster
Bit rate	It is proportional to video file size, not recommend adjusted.
I Frame Interval	The greater the value is, the worse the video quality would be, otherwise the better video quality would be; not recommend adjusted.
Activate	When you selected it, the stream is enabled, otherwise disabled
Encoder static setting	Baseline: catch the packet for filtering H264, see H264 nal unit payload for Baseline profile Main profile/High profile: see the H264 nal unit payload as Main profile/High profile
"Default" reverts to factory video configuration, and "submit" saves Settings	
Advanced Settings	
Video Direction	Sendonly: establish video call, and the SDP packet in the invite packet is Sendonly; Sendrecv: to create a call, the SDP package in the invite package is Sendrecv
RTSP Over TCP	The RTSP goes over the TCP protocol
H.264 Payload Type	Set the h. 264 Payload type. The range is between 96 and 127. The default is 117
Default Call Stream	Optional main stream and substream

Enable Onvif	Enable the ONVIF feature, and when enabled, discover the device via the video recorder that supports ONVIF
RTSP Information	
Main Stream Url	Access the main address of RTSP
Sub Stream Url	Access the child address of RTSP

Table 14 - Video Setting

9.18 EGS Setting & 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.

Table 15 - MCAST parameters

Parameters	Description
Normal Call Priority	Define the priority of the active call, 1 is the highest priority, 10 is the lowest.
Enable Page Priority	Two multicasts, regardless of who first calls in, the device will receive the multicast with higher priority.
Name	Listened multicast server name
Host: port	Listened multicast server's multicast IP address and port.

9.19 EGS Setting & Intercom Setting >> action URL

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

Table 16 - action URL

Note! The operation URL is used by the IPPBX system to submit device events. Please refer to the details Fanvil Action URL。

http://www.fanvil.com/Uploads/Temp/download/20190122/5c46debfbde37.pdf

9.20 EGS Setting & Intercom Setting >> Time/Date

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

Table 17 - Time/Date

Field Name	Explanation
Network Time Server Settings	
Time Synchronized via SNTP	Enable time-sync through SNTP protocol
Time Synchronized via DHCP	Enable time-sync through DHCP protocol
Primary Time Server	Set primary time server address
Secondary Time Server	Set secondary time server address, when primary server is not reachable, the device will try to connect to secondary time server to get time synchronization.
Time zone	Select the time zone
Resync Period	Time of re-synchronization with time server
Daylight Saving Time Settings	
Location	Select the user's time zone specific area
DST Set Type	Select automatic DST according to the preset rules of DST, or the manually input rules
Offset	The DST offset time
Month Start	The DST start month
Week Start	The DST start week
Weekday Start	The DST start weekday
Hour Start	The DST start hour
Month End	The DST end month
Week End	The DST end week
Weekday End	The DST end weekday
Hour End	The DST end hour
Manual Time Settings	
Manual Time Settings	The time set by hand, need to disable SNTP service first

9.21 EGS Settings >> Trusted Certificates

The certificate management page uploads and deletes uploaded certificates.

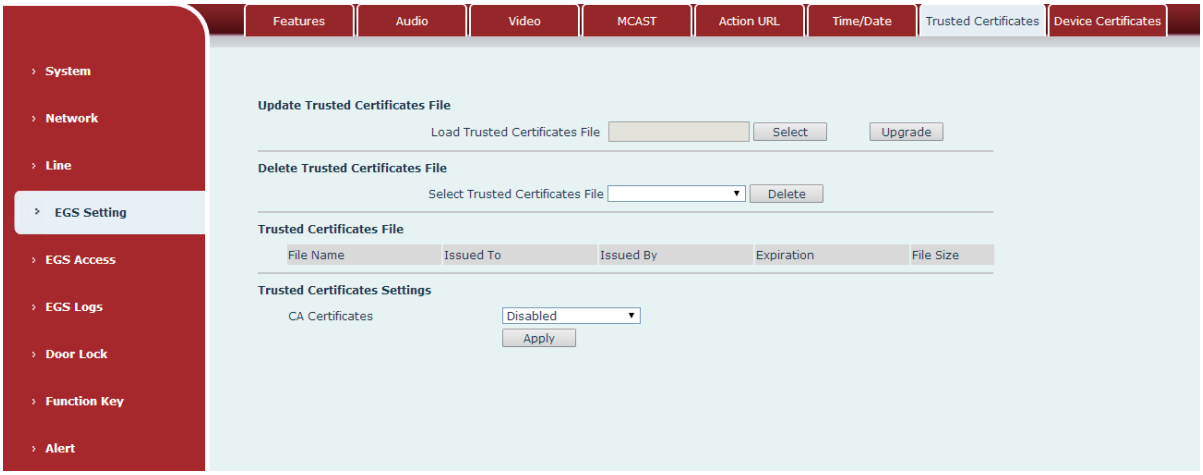


Figure 30 - Trusted Certificates

9.22 EGS Settings >> Device Certificates

Select the device certificate as the default and custom certificate.

You can upload and delete uploaded certificates.

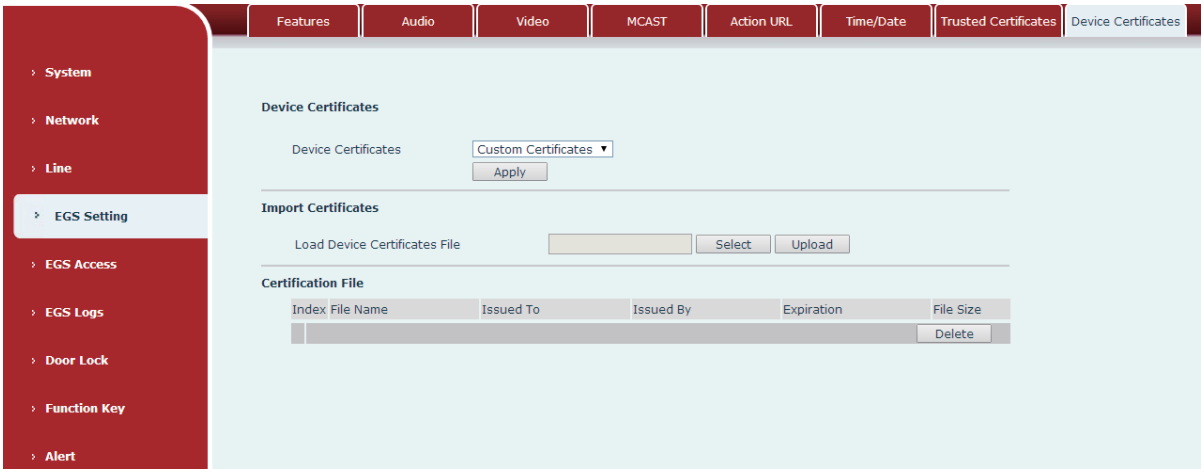


Figure 31 - Device Certificates

9.23 EGS Access

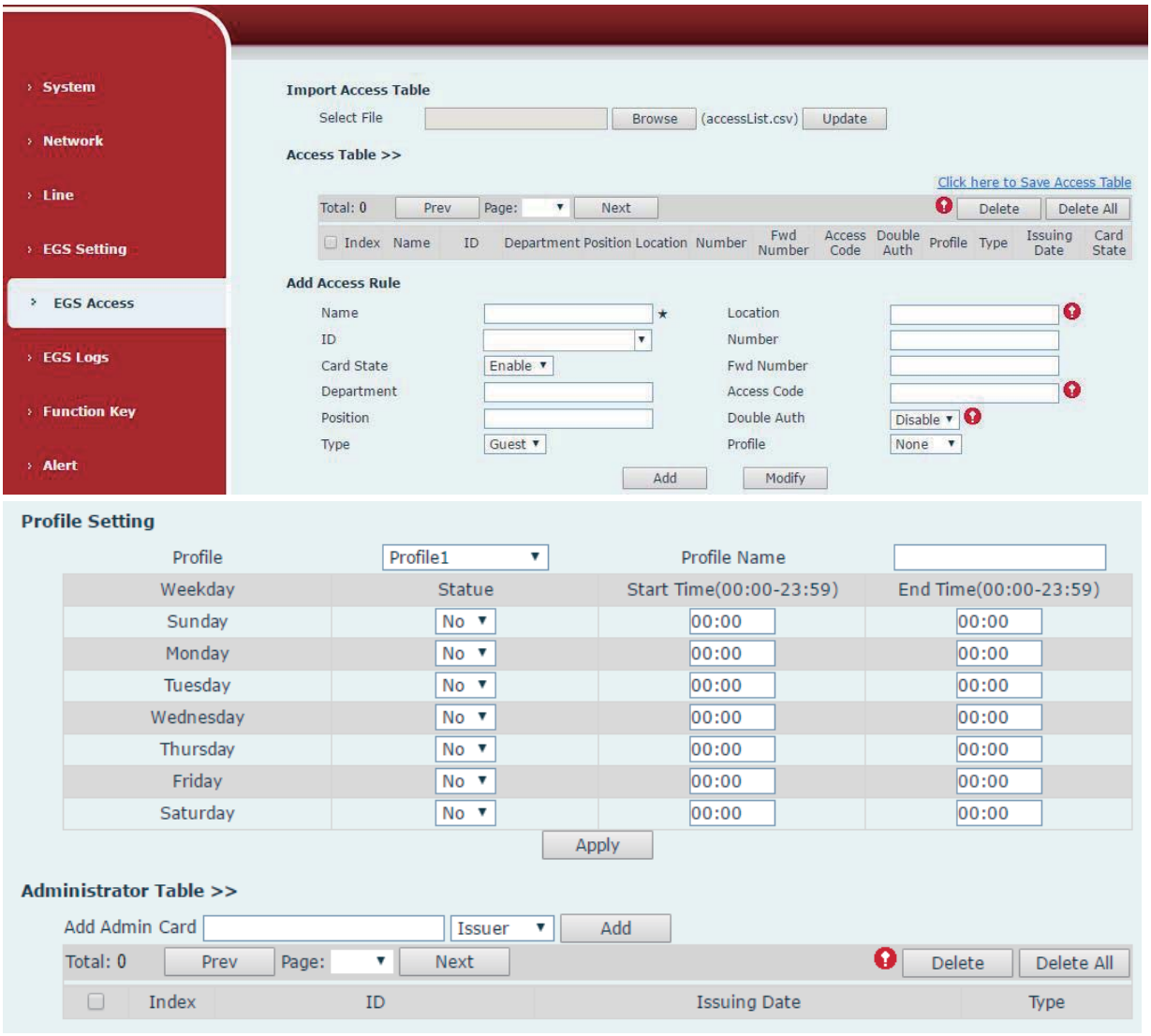


Figure 32 - EGS Access

Table 18 - EGS Access Parameter

EGS Access	
Field Name	**Explanation**
Import Access Table	
Click the <Browse> to choose to import remote access list file (access List.csv) and then clicking <Update> can batch import remote access rule.	
Access Table	
According to entrance guard access rules have been added, you can choose single or multiple rules on this list to delete operation. Click " Click here to Save Access Table " to export the saved access list.	
Add Access Rule	

According to door phone access rules have been added, you can choose single or multiple rules on this list to delete operation.	
Name(necessary)	User name
Location	When the speed dial is input, it will be mapped to the corresponding number. The outgoing order is: the owner number (priority), the forwarding number will be called if the owner number is busy or no answer.
ID	RFID card number. You can manually fill in the first 10 digits of the card number or select the existing card number. e.g. 0004111806
Number	User phone number
Card State	Enable or disable holder's RFID card
Fwd Number	Call forwarding number when above phone number is unavailable.
Department	Card holder's department
Access Code	1. When the door phone answers the call from the corresponding <Number> user, then the <Number> user can input the access code via keypad to unlock the door remotely. 2. The user's private password should be input via keypad for local door unlocking. The private password format is Location * Access Code.
Position	Card holder's position
Double Auth	When the feature is enabled, private password inputting and RFID reading must be matched simultaneously for door unlocking.
Type	Host: the door phone would answer all call automatically. Guest: the door phone would ring for incoming call, if the auto answer is disabled.
Period	The current user's access rule authentication is valid for the period of use, and [None] is not limited for 24 hours.
Add	After the relevant rules are disposed in the "Add Access Rules" sub-item, click "Add" to complete the addition.
Modify	In the "Access Table", select the "Index" to be modified. After the relevant rules are disposed in the "Add Access Rule" sub-item, click "Modify" to complete the modification.
Profile Setting	
Profile	There are 4 sections for time profile configuration
Profile Name	The name of profile to help administrator to remember the time definition
Status	If it is yes, the time profile would be taken effect. Other time sections not included in the profiles would not allow users to open door
Start Time	The start time of section
End Time	The end time of section

Administrator Table	
Add Admin Card	You should input the top 10 digits of RFID card numbers. for example, 0004111806, then select the type of admin card and click <add>.
Type：Open/ Add/ Delete. Open：Super administrator card, the device can open the door through the super management card when the device cannot open due to software processing error or configuration read failure. When door phone is in normal working state, swipe card (issuing card) would make door phone into the issuing state, and then you can swipe a new card to add into the database; when you swipe the issuing card again after cards added done, door phone would return to normal state. Delete card operation is the same with issuing card. The device can support up to 10 admin cards, 1000 copies of ordinary cards. Note: in the issuing state, deleted card by swiping is invalid.	
Admin card database: Shows the card ID, Issuing Date and Card Type	
Delete	Click <Delete> would delete the admin card list of the selected ID cards.
Delete All	Click <Delete All>, to delete all admin card lists.

9.24 EGS Logs

According to open event log, the device can record up to 200,000 pcs open events. New records will cover the oldest records once the records reaches the limit. Click here to Save Logs Right click on the links to select save target as the door log can export CSV format.

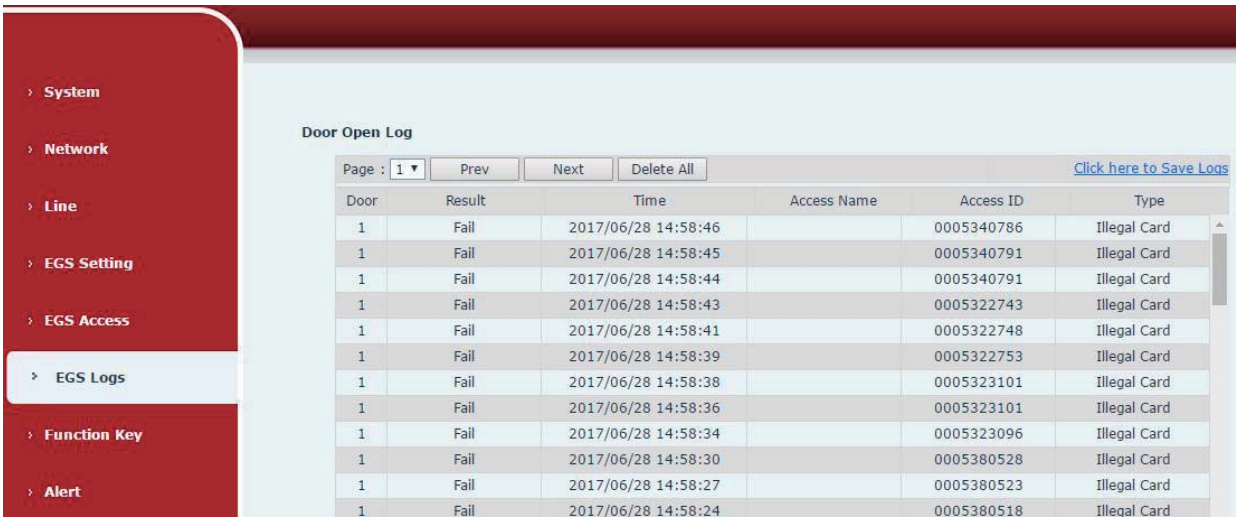


Figure 33 – EGS Logs

Table 18 - EGS Logs Parameter

Field Name	Explanation
Door Open Log	
Result	Show the results door open history (Succeeded or Failed)
Time	The door open time.
Access Name	If the door was opened by swipe card or remote unlocking door, the device would display remote access name.
Type	Open type: 1. Local, 2. Remote, 3. Card Note: there are three kinds of card feedback results. Temporary Card (only added the card number, without adding other rules) Valid Card (added access rules) Illegal Card (the card not added in the door phone database)

9.25 Door Lock

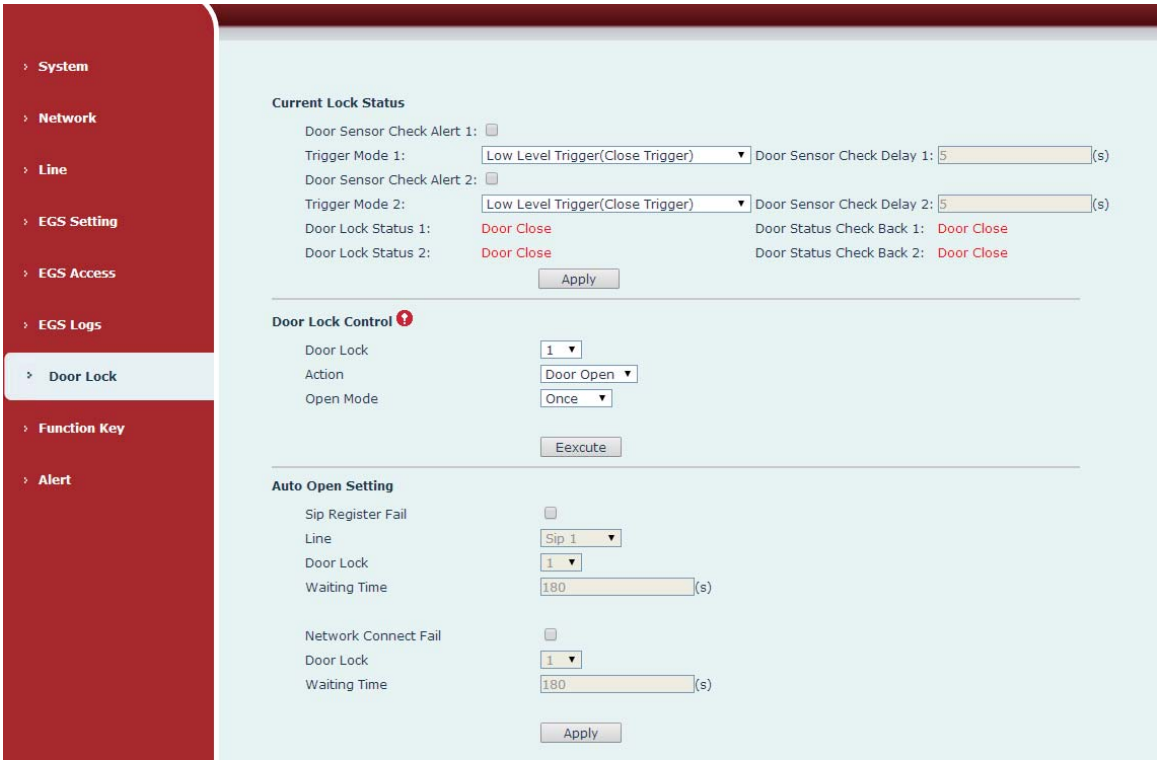


Figure 34 - Door Lock

Table 19 - Door Lock Parameter

Field Name	Explanation
Current lock Status	
Door Sensor Check Alert	Enable/disable the door phone alarm. When the timeout period is enabled, the alarm will be triggered when the door status and the door lock status are inconsistent.
Trigger mode	When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger.
	When choosing the high level trigger (disconnected trigger), detect the input port (high level) disconnected trigger.
Door Sensor Check Delay	Door magnetic detection delay time setting
Lock Status	Door Close/Open
Door Status Check Back	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.
Auto Open Setting	
SIP Register Fail	When the SIP line registration fails, the door lock could be set to open automatically after the timeout period.
Line	The Line could select line 1 / line 2 / all
Door Lock	The door lock could select lock 1 / lock 2 / all lock
Waiting Time	The door will be opened automatically when timeout. (unit: second)
Network Connect Fail	When the network connection fails, the door lock could be set to be opened automatically after the timeout period.
Door Lock	The door lock could select lock 1 / lock 2 / all lock
Waiting Time	Timeout time automatically opens the door, unit s

9.26 Alert &Security Settings

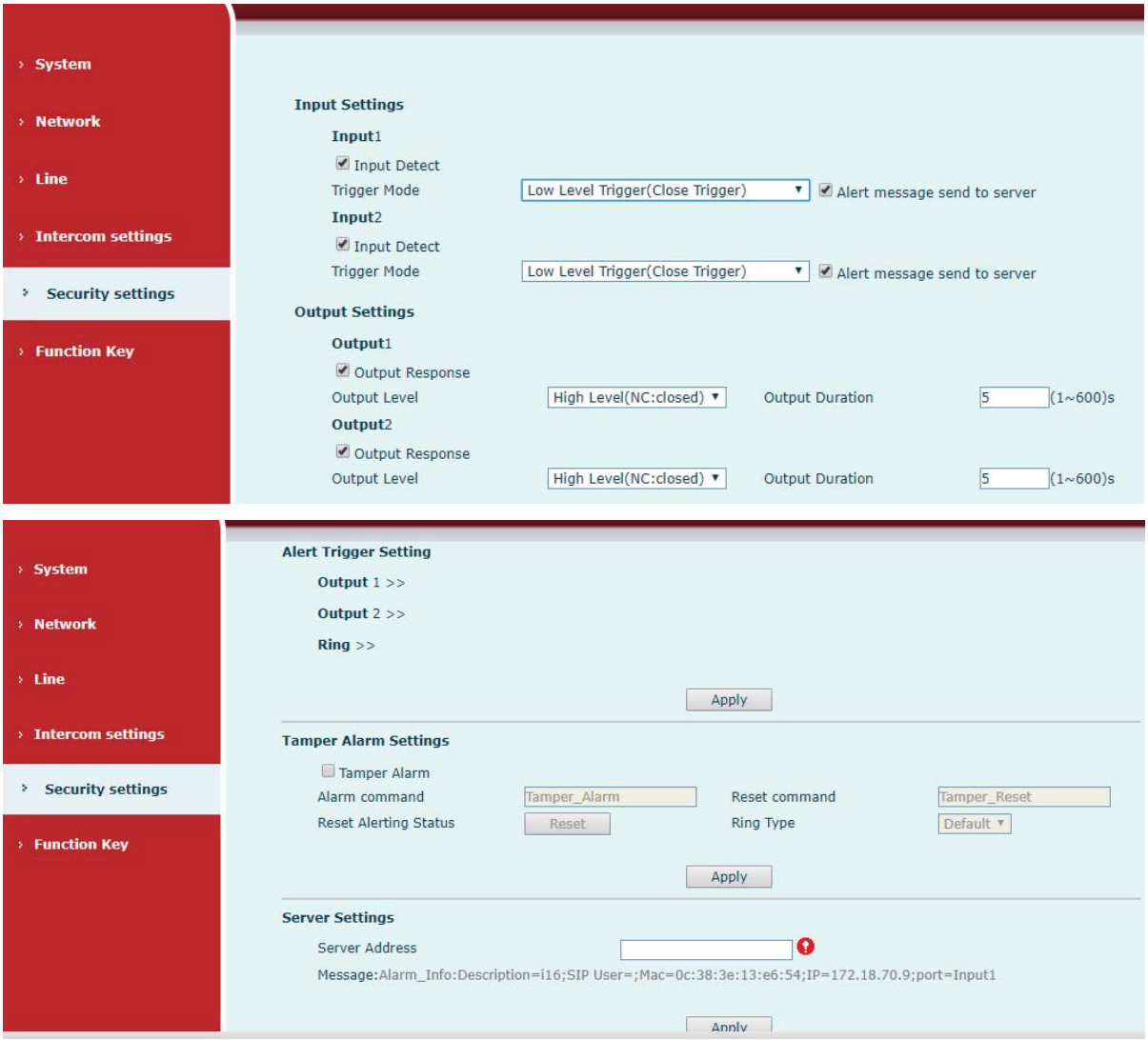


Figure 35 - Alert/Security Settings

Table 20 - Alert/Security Settings

Security Settings	
Field Name	**Explanation**
Input settings	
Input Detect	Enable or disable Input Detect
Trigger Mode	When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger.
	When choosing the high level trigger (disconnected trigger), detect the input port (high level) disconnected trigger.
Alert message	Set the Alert message send to server

sends to server		
Output Settings		
Output Response	Enable or disable Output Response	
Output Level	When choosing the low level trigger (NO: normally open), when meet the trigger condition, trigger the NO port disconnected.	
	When choosing the high level trigger (NO: normally close), when meet the trigger condition, trigger the NO port close.	
Output Duration	Changes in port, the duration of. The default is 5 seconds.	
Alert Trigger Setting		
Alarm Ring Duration	Set the Alarm Ring Duration. The default is 5 seconds.	
Input trigger	When the input port meets the trigger condition, the output port will be triggered (The Port level time change, By < Output Duration > control)	
DTMF output Duration	By duration	Port switch amount change time, press <output duration> control
	By Calling State	By call state control, after the end of the call, port to return the default state
Remote DTMF trigger	Receive the DTMF password sent by the remote device. If it is correct, trigger the corresponding output port. You can choose to enable or disable ringtones	
DTMF trigger code	During the call, the receiving terminal device sends a DTMF password, and if it is correct, the corresponding output port is triggered. The default is 1234.	
Remote SMS trigger	Enable or disable remote SMS triggering. You can choose to enable or disable ringtones	
Trigger Message Format	Send instructions on remote devices or servers, ALERT= [set instructions], if correct, trigger the corresponding port output.	
Call status trigger	The port outputs a continuous time trigger type, including the trigger condition. For example, the call triggers the output port, and the output port will be in the call state and continue to respond) 1 Talking 2 Talking and Ringing 3 Ringing 4 Calling 5 Calling and Talking 6 Calling and Ringing	

	7 Calling, Ringing and Talking
Tamper Alarm Settings	
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
Reset Alerting Status	Reset to resume and stop ringtone playback
Ring Type	Ringtone can be set to none / preset
Server Settings	
Server Address	Send message to the server when the alarm is triggered. message format：Alarm Info: Description=i32V;SIP User=;Mac=00:a8:34:68:23:d1;IP=172.18.90.235;port=Input1

9.27 Function Key

➢ Key Event

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

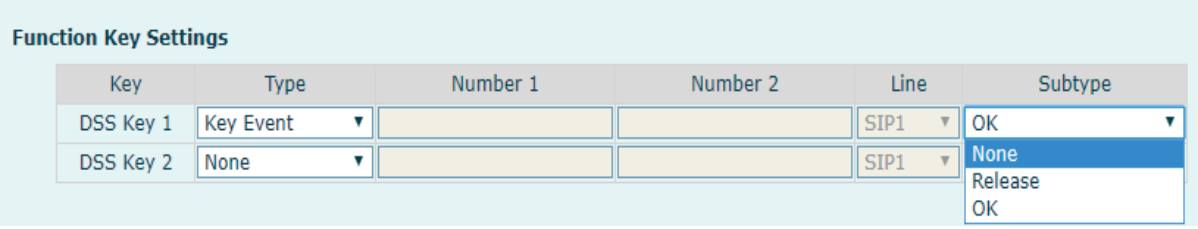


Figure 36 - Function Key Settings

Table 21 - Function Key Settings

Type	Subtype	Usage
Key Event	None	No responding
	Release	Delete password input, cancel dialing input and end call
	OK	Identification key

➢ Hot Key

When the speed dial key set as Hot Key, the device would dial preset telephone number. This button can also be used to set the IP address: you can press the speed dial button to directly

make an IP call.

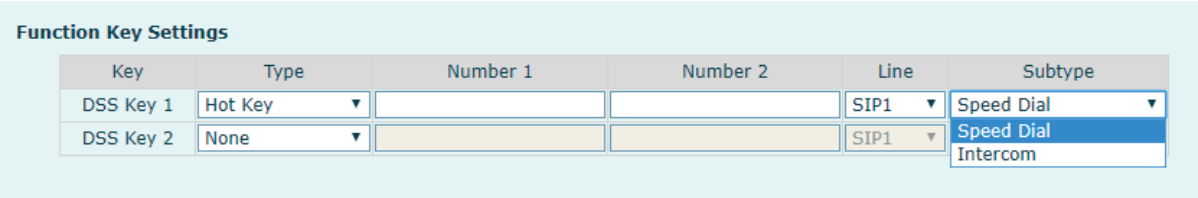


Figure 37 – ***Hot Key Settings***

Table 22 – ***Hot Key Settings***

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

➢ Multicast

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

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

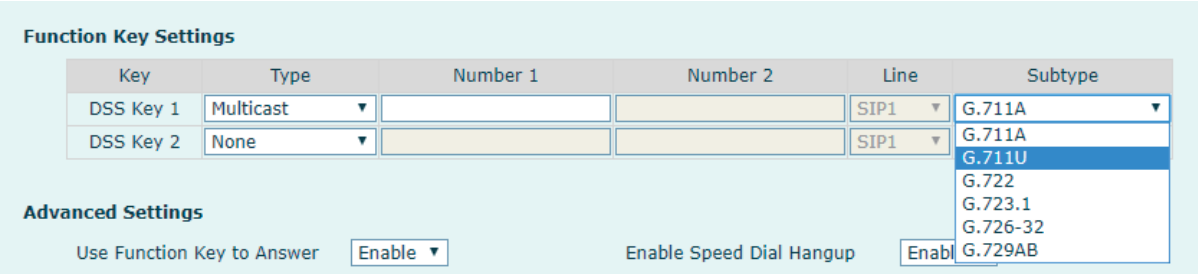


Figure 38 – ***Multicast Settings***

Table 23 - Multicast Settings

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

➢ Advanced Settings

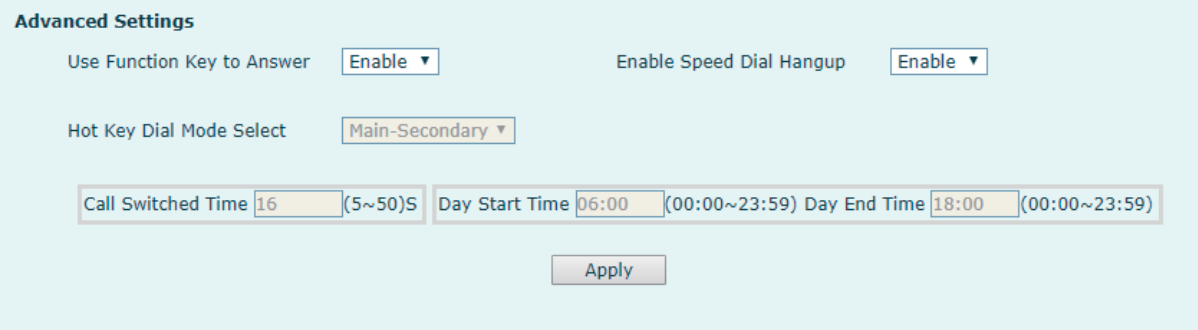


Figure 39 - Advanced Settings

Table 24 - Advanced Settings

Advanced Settings	
Field Name	**Explanation**
Input port is multiplexed as function key 2	Enable or disable the input port to be multiplexed as speed dial button 2
Use Function Key to Answer	Enable or disable shortcuts to answer calls
Enable Speed Dial Hang up	Enable or disable shortcuts to hang up calls
Hot Key Dial Mode Select	Number 1 call number 2 mode selection. <Main/Secondary>: If the first number is not answered within the set time, the second number will be automatically switched. <Day/Night> : The system time is automatically detected during the call. If it is daytime, the first number is called, otherwise the second number

	is called.
Call Switched Time	Set number 1 to call number 2 time, default 16 seconds
Day Start Time	The start time of the day when the <Day/Night> mode is defined. Default "06:00"
Day End Time	The end time of the day when the <Day/Night> mode is defined. Default "18:00

10 Trouble Shooting

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

10.1 Get device system information

Users can obtain information through the [**System**] >> [**Information**] option on the device webpage. The following information will be provided:
Device information (model, software and hardware version) and Internet Information etc.

10.2 Reboot device

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

10.3 Device factory reset

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

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

10.4 Network Packets Capture

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

10.5 Common Trouble Cases

Table 25 - Common Trouble Cases

Trouble Case	Solution
Device could not boot up	1. If the device enters "POST mode" (the SIP/NET and function button indicators are always on), the device system is damaged. Please contact your location technical support to help you restore your equipment system. 2. If the device enters "POST mode" (the SIP/NET and function button indicators are always on), the device system is damaged. Please contact your location technical support to help you restore your equipment system.
Device could not register to a service provider	1. Please check if the device is connected to the network. The network cable must be connected to the [Network] interface instead of the [Computer] interface. 2. Please check if the device has an IP address. Check the system information. If the IP address is Negotiating..., the device has not obtained an IP address. Please check if the network configuration is correct. 3. If the network connection is good, please check your line configuration again. If all configurations are correct, contact your service provider for support, or follow the instructions in "10.4 Network Data Capture" to obtain a registered network packet and send it to the Fanvil Support Email to help analyze the issue.