
# User Manual

## i33V&i33VF

**Software Version**：2.4.0

**Release Date**：2019/03/04

# 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 cause noise issue.
- Before using the external power supply in the package, please check the home power voltage. Inappropriate 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 low temperature 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 may get 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

i33V &i33VF is an access control product with LCD specially developed for the needs of industry users on the basis of VoIP telephone technology for more than ten years. The standard IP/RTP protocol is used for voice transmission, and the RTSP is used for video transmission. With the advantages of good stability and carrier-grade sound quality of local-phone, it is perfectly compatible with all current sip-based mainstream IP PBX/ softswitch /IMS platforms, such as Asterisk, Broadsoft, 3CX, Elastix and so on, providing convenient experice for users to quickly deploy equipment. Integrated with remote door.

# 5 Install Guide

## 5.1 Use POE or external Power Adapter

i33V&i33VF, 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 is useful. 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 which meets the specifications to ensure the device work properly.

# 6 Appendix Table

## 6.1 Common command mode

*Table 1 - Common command mode*

| Action | Description |
|---|---|
| IP Broadcast under standby mode | In standby mode, long presse '#' |
| Switch network mode | In standby mode, long press 'C' for 10 seconds, there will be a toot sound. Within 5 seconds, press 'C' 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 |

## 6.2 Icon

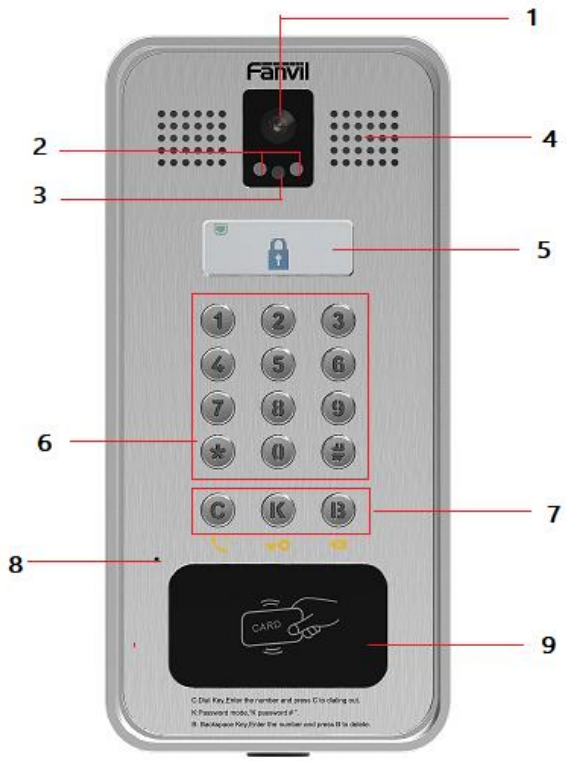
*Table 2 - Icon Status*

| Icon | Description | Icon | Description |
|---|---|---|---|
|  | Connect to the network |  | Network not connected，flashing |
|  | Successfully registered |  | Registration failed, flashing |
|  | Ringing |  | Dialing |
|  | Call failed (no response) |  | Hang up by the other party |
|  | Lock off |  | Lock on |
|  | Dial interface lock |  | Dial interface lock is open |
|  | Open the door |  | Handsfree |
|  | Fault prompt 1<br>(with error number) |  | Fault prompt 2<br>(？: flashing) |

| Icon | Description | Icon | Description |
|---|---|---|---|
|  | Connected to the TR069 |  | Not connected to the TR069，flashing |
|  | Password error |  | Invalid card |

# 7 Basic Introduction

## 7.1 Panel Overview




***Picture 1 - Panel***

***Table 3 - Panel introduction***

| Number | Name | Description |
|---|---|---|
| 1 | IP Camera | Video signal acquisition and transmission |
| 2、3 | IR LED/ Photoresistor | Watch video clearly even in weak light environment |
| 4 | Speaker | Play sound |
| 5 | LCD | Display status and prompts |
| 6 | Numeric keypad | Password and dialing |
| 7 | Function key | C: Dial Key, Enter the number and press C to dialing out. |

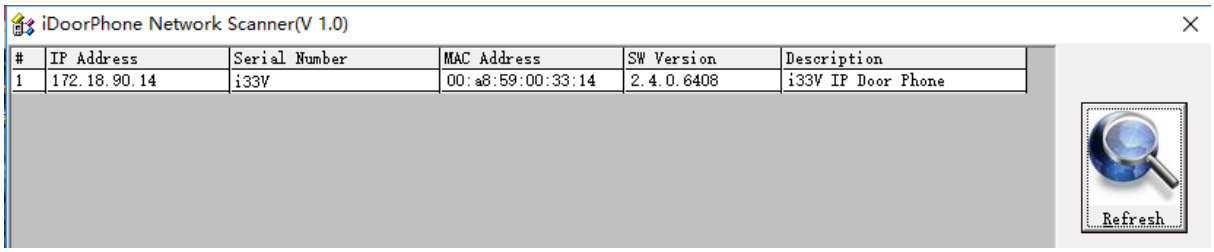
| | | |
|---|---|---|
| | | K: Password mode, “K password # ”<br>B: Backspace Key, Enter the number and press B to delete |
| 8 | MIC | Sound collecting |
| 9 | RFID area | Open the door with card |

## 7.2 Quick Setting

Before proceeding with this step, make sure your Internet broadband connection is working properly and connecting to the network hardware. The default factory mode of i33V&i33VF is DHCP. IP address can be viewed by.

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

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



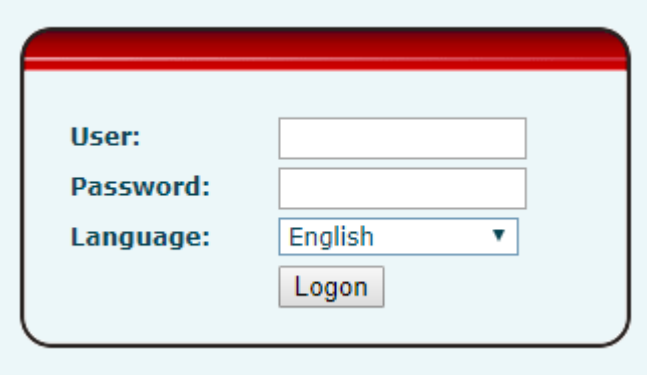

***Picture 2 - Quickly setting***

- Long press DSS key for 10 seconds(after power-on for 30 seconds), and when the speaker beeps rapidly, press DSS key again quickly, the beeps stop ,the intercom will report the IP address by itself.
- In addition, device provides the device surface DSS key operation to switch IP address acquisition mode:

  Long press the DSS key for 10 seconds. When the speaker beeps, press the DSS key three times, the beep stops. Wait for 10 seconds, then the system will broadcast the current IP address automatically.
- Login to the device's WEB page for configuration setting 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;

## 7.3 WEB configuration

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




*Picture 3 - WEB Login*

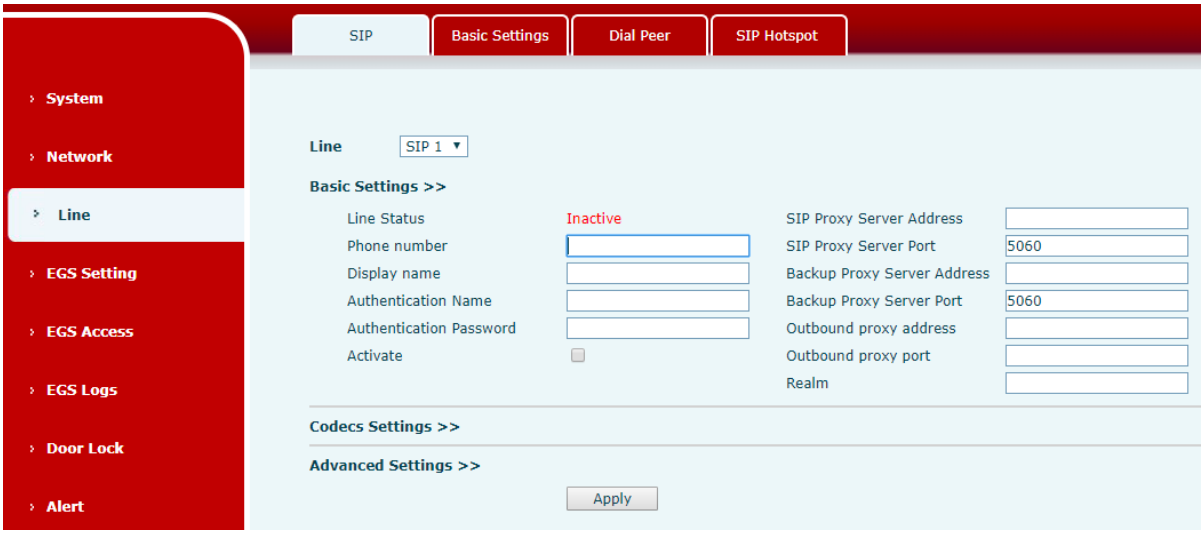
The username and password should be entered into the web page correctly. **The default username and password are "admin"**. For the specific details of the operation of the web page, please refer to 10 Web Configurations

## 7.4 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 the account information of service provider for registration and authentication. When the configuration is working on the device, it will help to register automatically with the server's address and user's authentication which is 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 4 - SIP Line Configuration*

## 7.5 Door opening operation

Unlock the door in the following eight ways:

1) Open the door with the local password, and press “K key + local door open password +#” to open the door.
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, 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) The door can be opened through the indoor door button when the door phone is in any state.
6) Enter the position speed dial and 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) In the case of door phone software exception, you can open the door through the super administrator card and super administrator password (the password of super administrator can only visit the devices with keyboard).
8) Open the door with active URL control command

   The URL of openning door 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..

# 8 Basic Function

## 8.1 Making Calls

In standby mode, you can make a call by:

- Enter the number and press the “C”
- Press “C” to enter the number, then press “C”
- IP direct dialing in standby:
- Set to the length of the IP address as the length of the received number
- Set the programmable button "*" key dial mode to DTMF input
- In standby mode, enter xxx*xxx*xxx*xxx and press “C” to call out.

## 8.2 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 it will not answer the phone automatically over time.

When canceling the automatic answering, there are incoming calls that can be answered as follows:

- Press the "*" button to answer (the default "*" button to answer, if you want to use the "#" button to answer, you can use the programmable button to set)
- Press “C” to answer

## 8.3 End of the Call

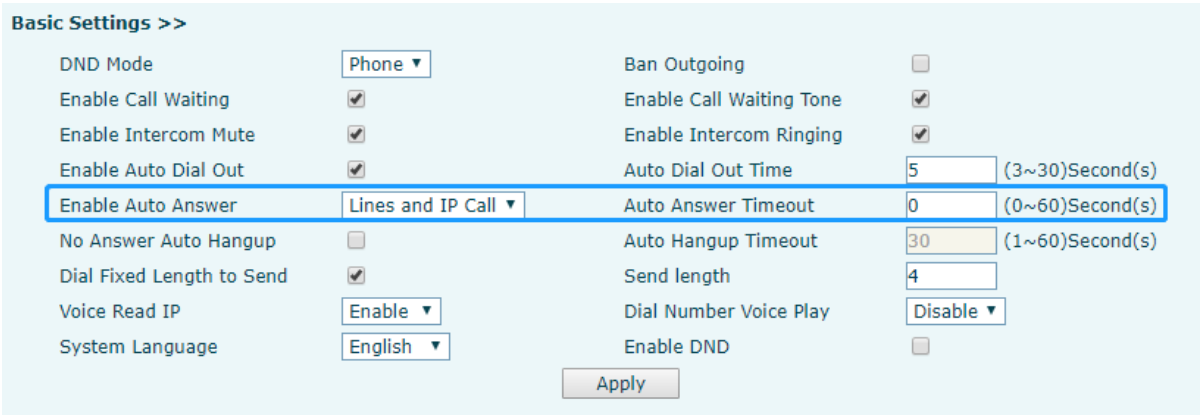
You can hang up the call during the call by:

- Press “C” to hang up
- Press “#” to hang up (the default “#” key hangs up. If you want to hang up with “*” key, you can set it by programmable button)

## 8.4 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.



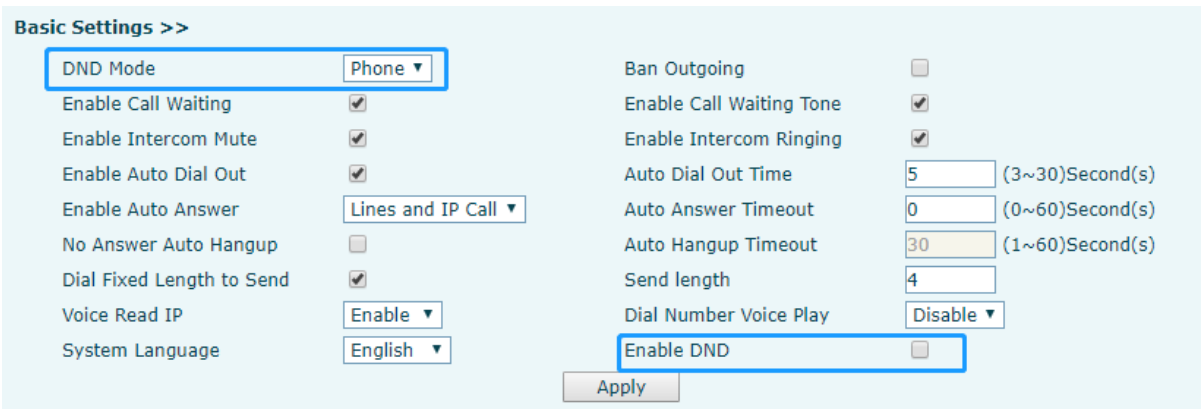

*Picture 5 - Enable Auto Answer*

- **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.

## 8.5 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:

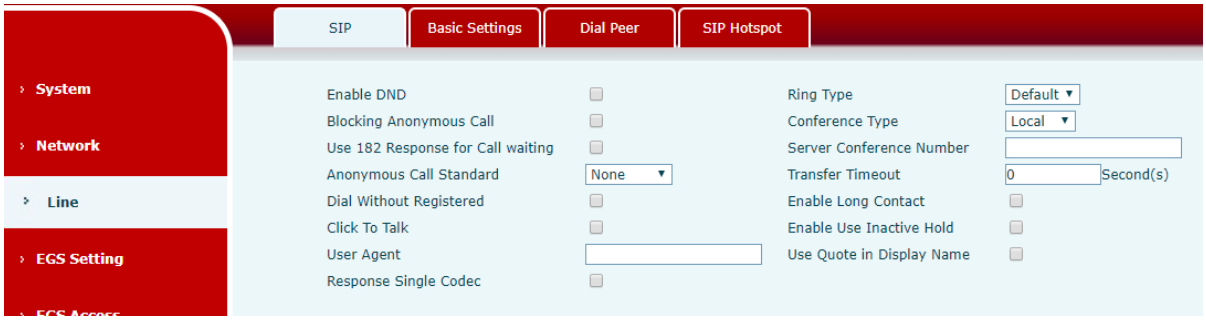
- Web interface: enter [**EGS Setting**] >> [**Features**], set the DND Mode to phone and Enable DND




*Picture 6 - 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.



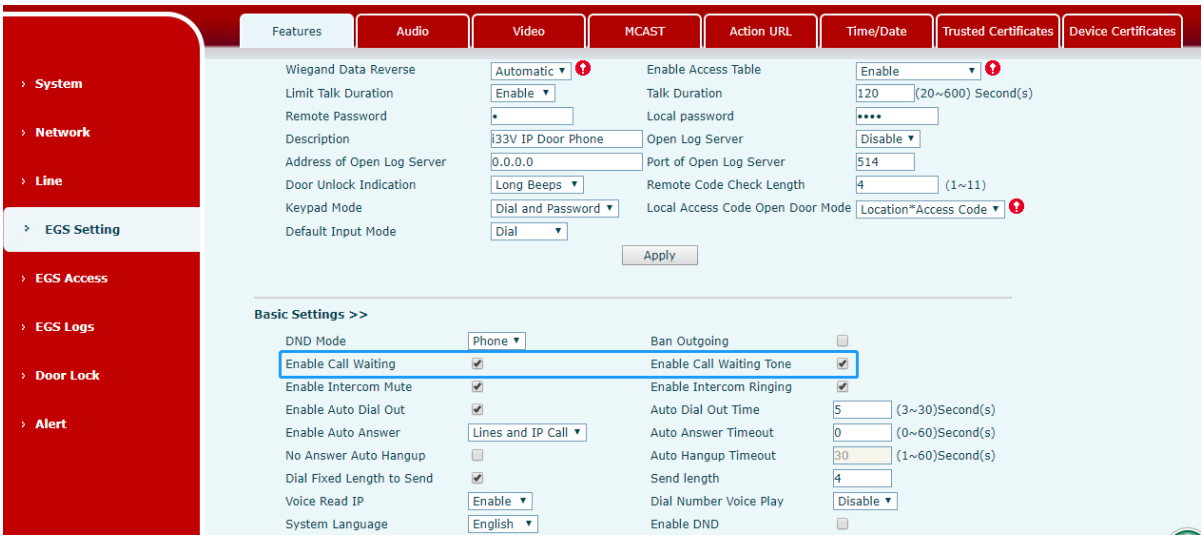

*Picture 7 - Enable DND*

## 8.6 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.

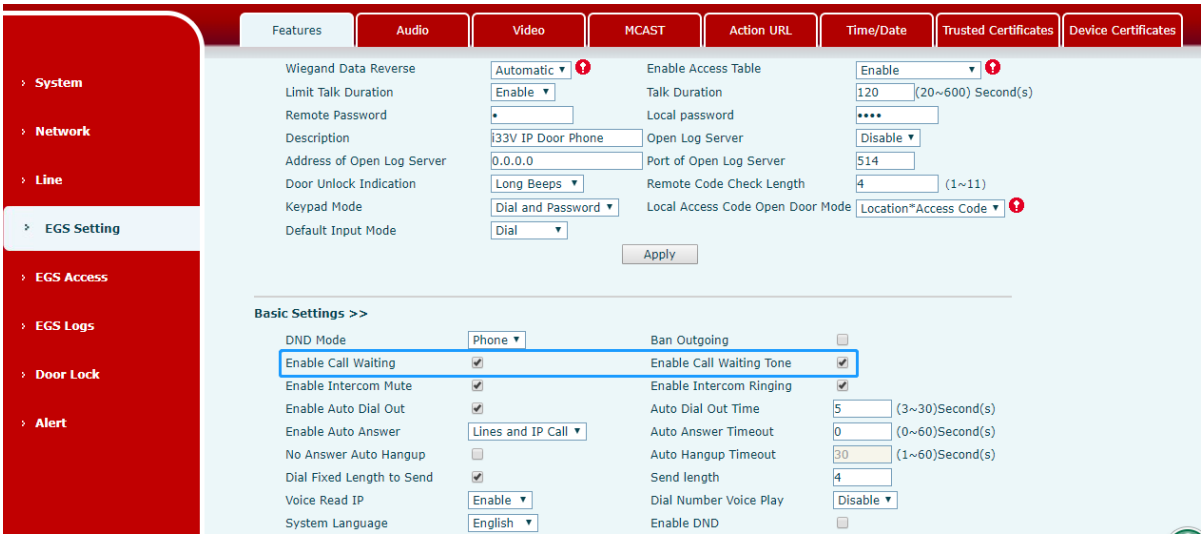



*Picture 8 - Call Waiting*

# 9 Advance Function

## 9.1 Intercom

The equipment can answer intercom calls automatically.



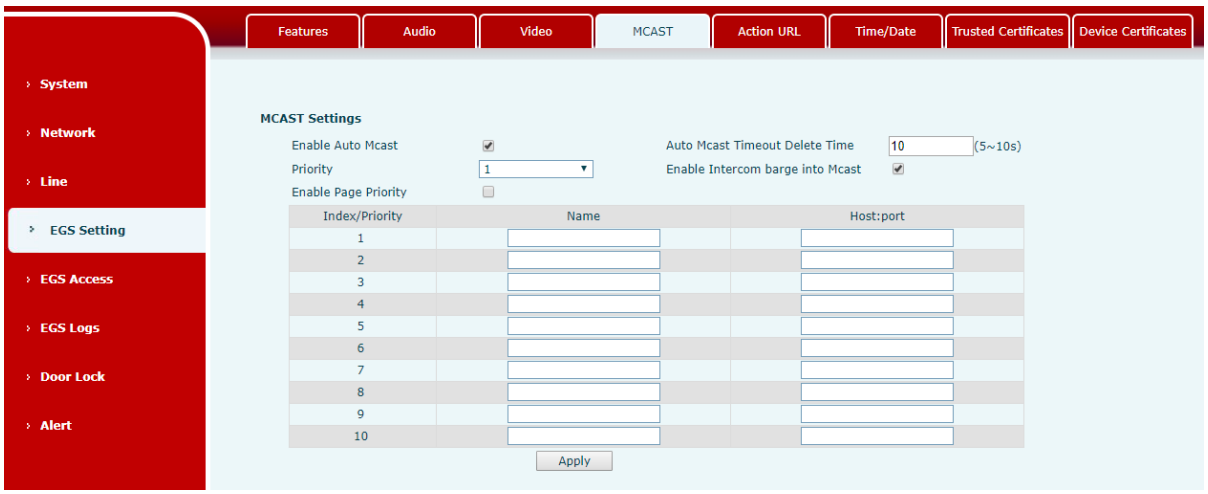

***Picture 9 - WEB Intercom***

***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. |

## 9.2 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 10 - Multicast Settings*

*Table 5 - MCAST Parameters on Web*

| Parameters | Description |
|---|---|
| Enable Auto Mcast | The multicast configuration information is sent through Sip Notify signaling. After receiving the information, the device will be configured to the system for multicast monitoring or cancel multicast monitoring in the system. |
| Delete Time of Auto Mcast Timeout | When a multicast call does not end normally, but for some reason the device can no longer receive the multicast RTP packet, with this configuration, the monitoring is cancelled after the specified time. |
| Priority | Defines the priority in the current call, with 1 being the highest priority to 10 the lowest. |
| Enable Intercom barge into Mcast | When enabled, intercom insertion is allowed for multicast calls. |
| Enable Page Priority | The voice call in progress shall take precedence over all incoming paging calls. |
| 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.

## 9.3 SIP Hotspot

SIP hotspot is a simple but practical function. With simple configurations, the SIP hotspot function can implement group ringing. SIP accounts can be expanded.

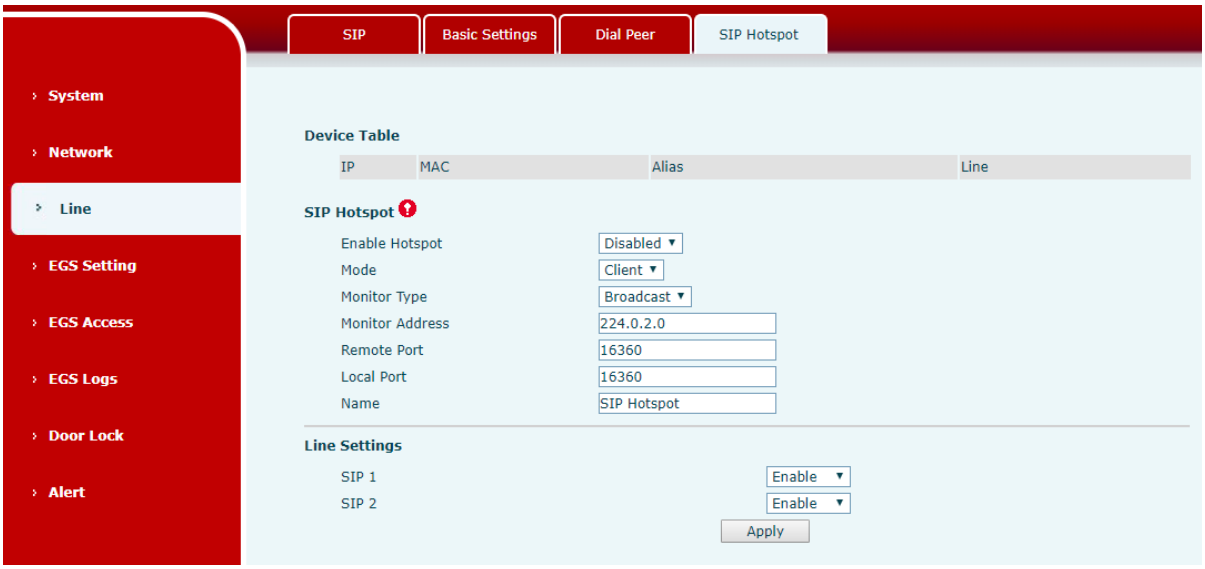
Set a Phone set as a SIP hotspot and other phone sets (B and C) as SIP hotspot clients. When somebody calls the phone set A, then the phone sets A, B, and C will all ring. When any phone set answers the call, other phone sets will stop ringing. The call can be answered by only one phone set. When B or C initiates a call, the SIP number registered by phone set A is the calling number.

***Table 6 - SIP hotspot Parameters***

| Parameters | Description |
|---|---|
| Device Table | If your phone is set to “SIP hotspot server”, Device Table will display as Client Device Table which connected to your phone.<br>If your phone is set to “SIP hotspot client”, Device Table will display as Server Device Table which you can connect to. |
| **SIP hotspot** | |
| Enable hotspot | Set it to be Enable to enable the feature. |
| Mode | Choose hotspot, phone will be a “SIP hotspot server”; Choose Client, phone will be a “SIP hotspot Client” |
| Monitor Type | Either the Multicast or Broadcast is ok. If you want to limit the broadcast packets, you’d better use broadcast. But, if client choose broadcast, the SIP hotspot phone must be broadcast. |
| Monitor Address | The address of broadcast, hotspot server and hotspot client must be same. |
| Remote Port | Type the Remote port number. |

Configure SIP hotspot client:

As a SIP hotspot client, no SIP account needs to be set. The Phone set will automatically obtain and configure a SIP account. On the SIP Hotspot tab page,change the mode into “Client”. The setting method of other options is the same as that of the hotspot.




***Picture 11 - SIP hotspot client configuration***

As the hotspot server, the default extension number is 0. When the phone is used as the client, the extension number is increased from 1, you can view the extension number through the [**SIP Hotspot**] page.

Call extension number:

- The hotspot server and the client can dial each other through the extension number.
- For example, extension 1 dials extension 0.

# 10 Web Configurations

## 10.1Web 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

## 10.2System >> 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

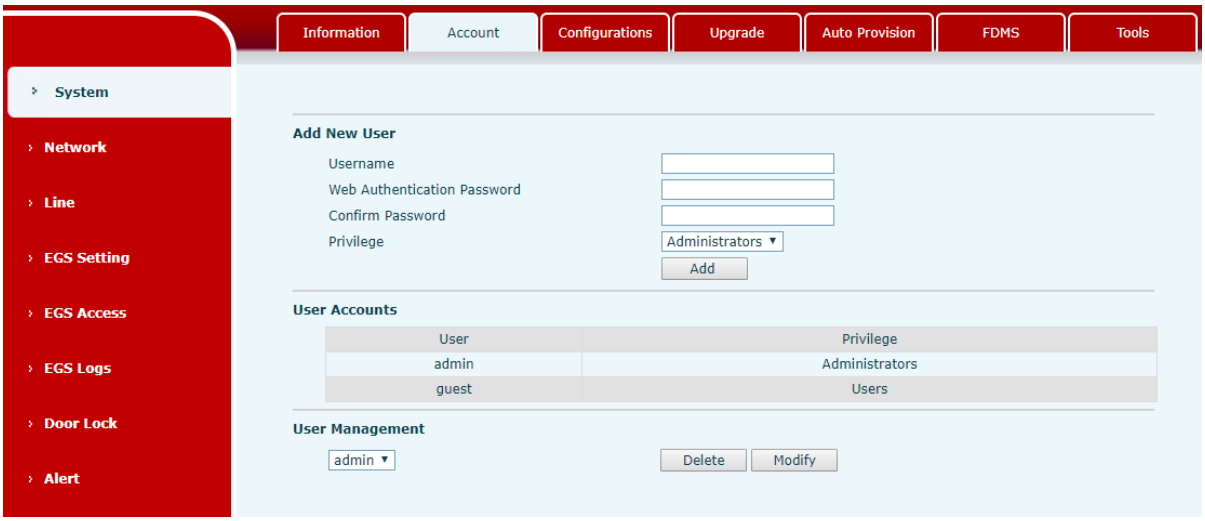
And summarization of network status,

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

Besides, summarization of SIP account status,

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

## 10.3System >> Account

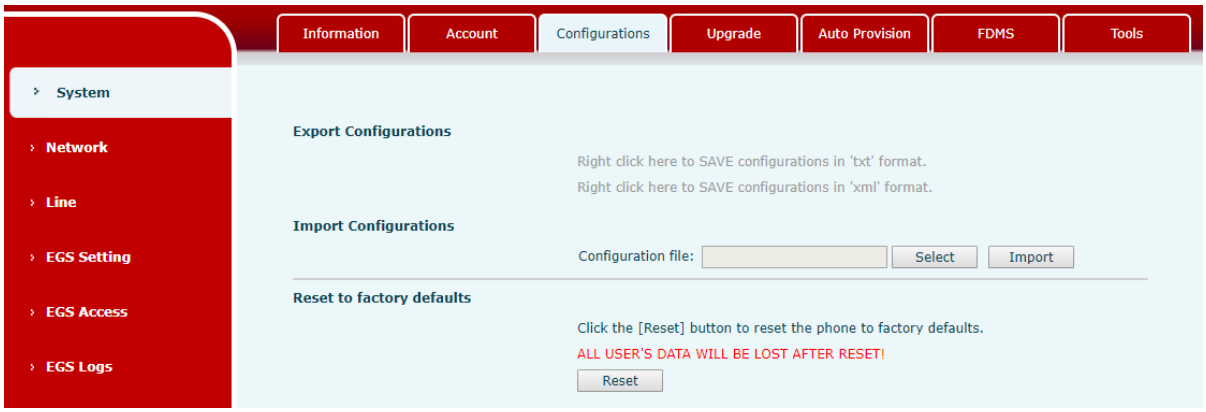



*Picture 12 - WEB Account Settings*

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.

## 10.4System >> Configurations

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




*Picture 13 - System 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)

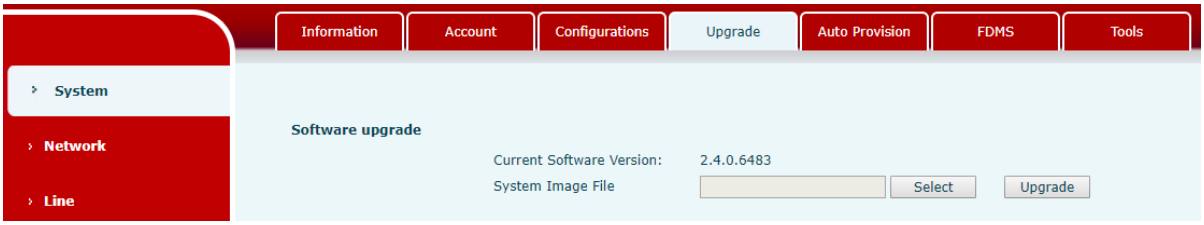
- **Import Configurations**

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.

## 10.5System >> Upgrade

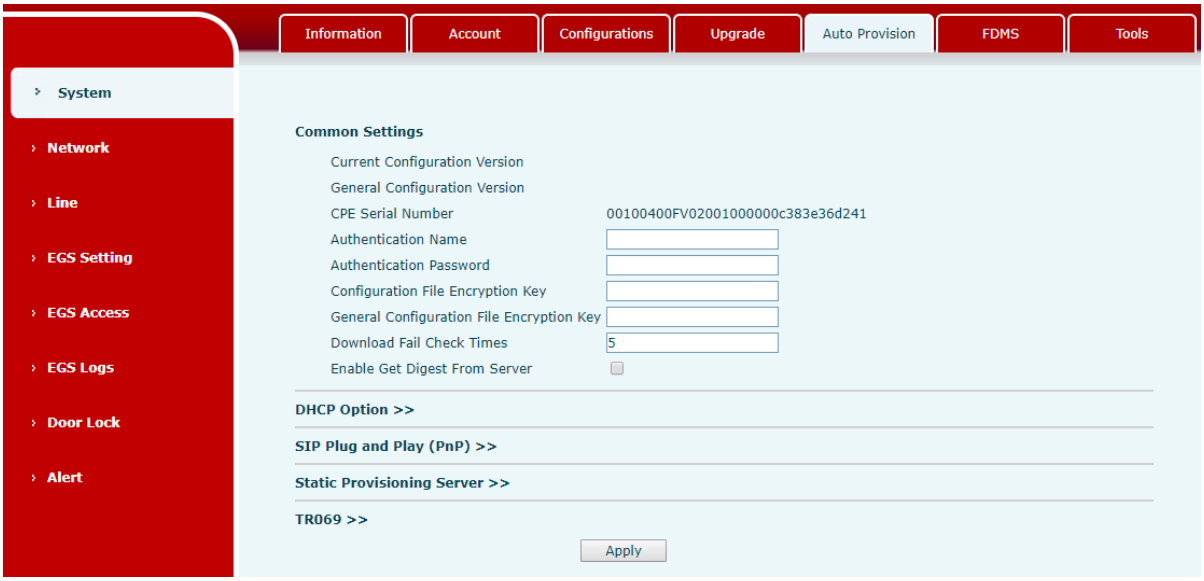



*Picture 14 - Upgrade Settings*

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

## 10.6System >> Auto Provision

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




*Picture 15 - Auto Provision Settings*

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/20180920/5ba3816f8d5f0.pdf

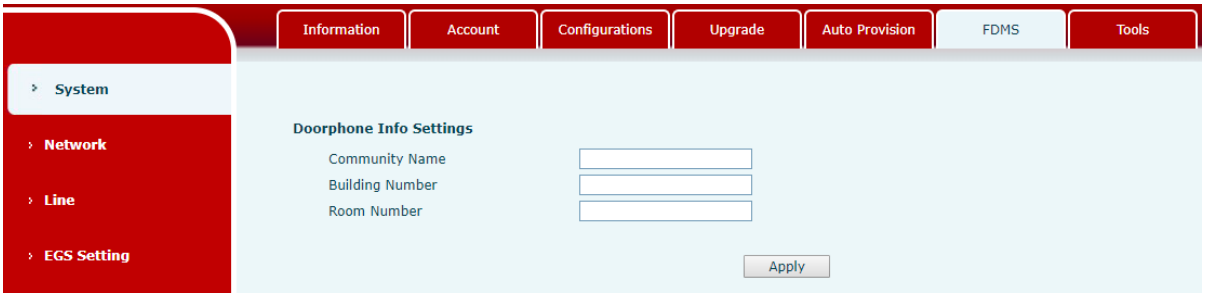
***Table 7 - Auto Provision Parameters***

| **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 be default for 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 | The default value is 5. If the download configuration fails, it will be |

| | |
|---|---|
| Check Times | 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 supporting for this special message 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.<br>1. Disabled.<br>2. Update after reboot.<br>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 |

## 10.7System >> FDMS



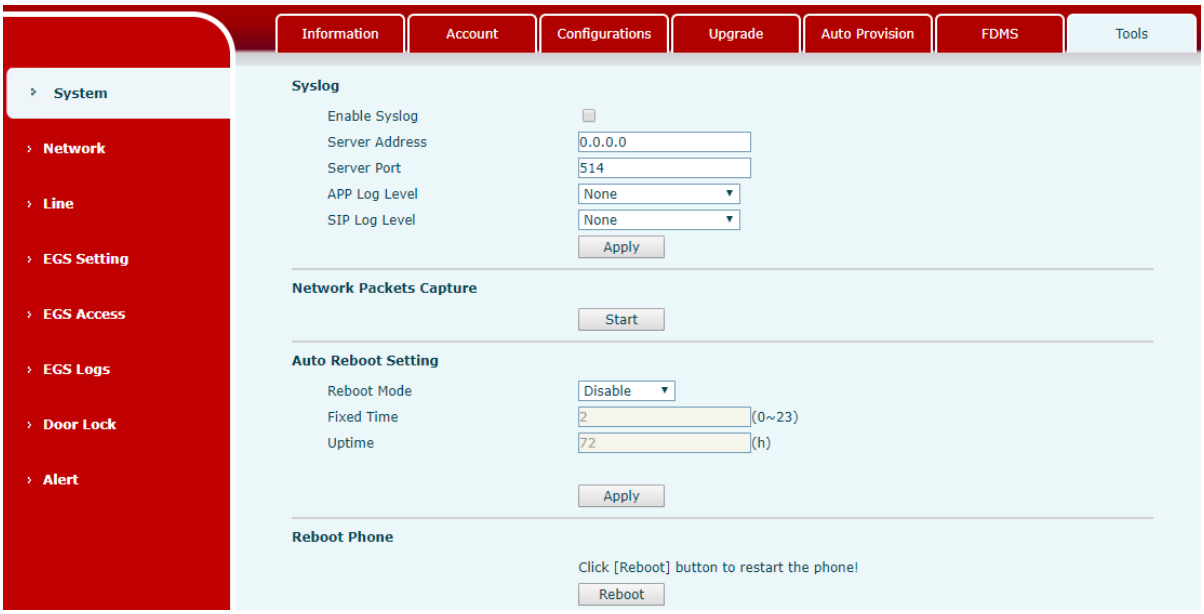

*Picture 16 - FDMS Configuration*

*Table 8 - FDMS Parameters*

| **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 |

## 10.8System >> Tools

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




*Picture 17 - System 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

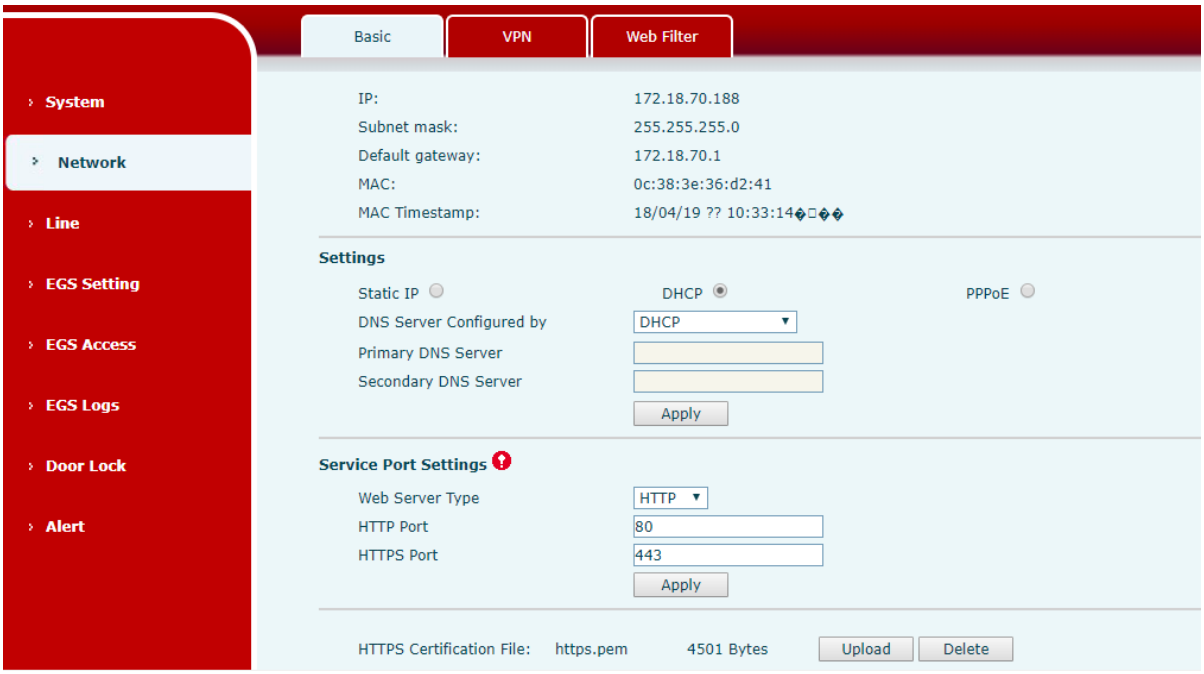
Fixed Time：In the range of 0~24 (h), restart will be conducted at the setting point every day after the setting is completed

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

For other details, please refer to 10 trouble shooting

## 10.9Network >> Basic

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



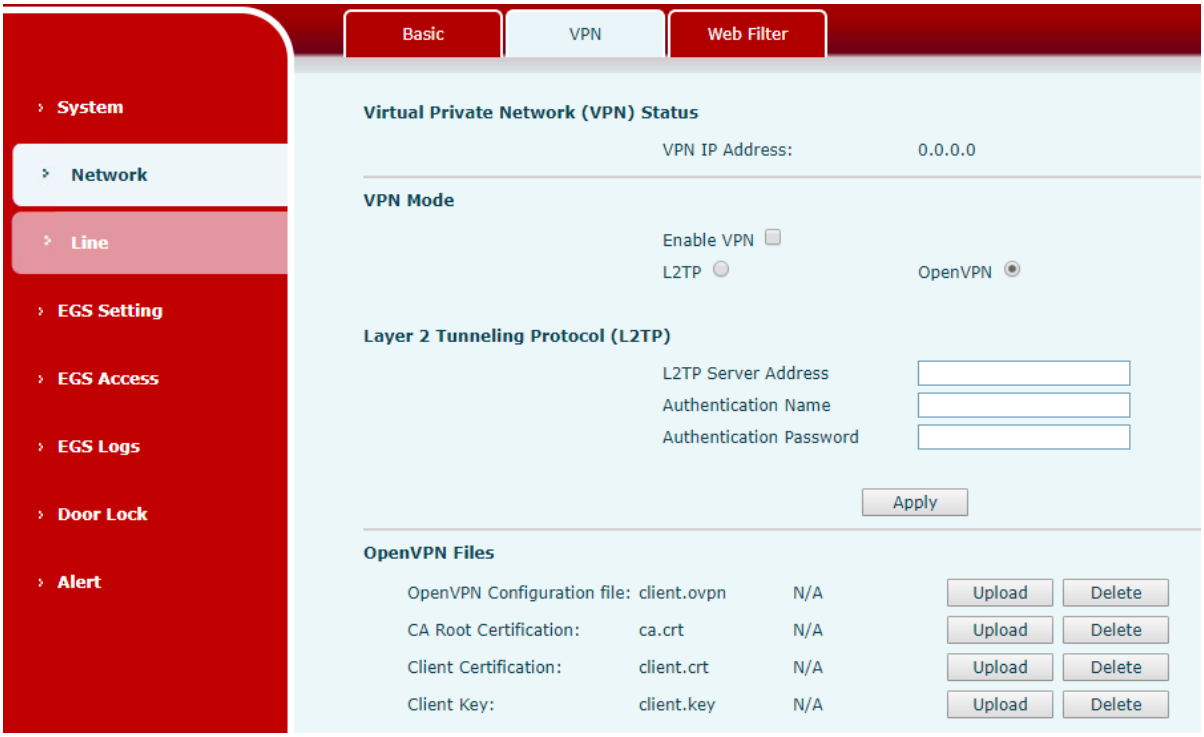

*Picture 18 - Basic Network Settings*

*Table 9 - Basic setting parameters*

| 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 be changed. 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 | Select the Configured mode of the DNS Server. |

| | |
|---|---|
| by | |
| Primary DNS Server | Enter the server address of the Primary DNS. |
| Secondary DNS Server | Enter the server address of the Secondary DNS. |
| **attention：**<br><br>1）After setting the parameters, click【submit】to take effect.<br><br>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.<br><br>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.<br>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.<br>Default value is 443. To enhance security, change this from the default. |

## 10.10 Network >> VPN




***Picture 19 - 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 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,

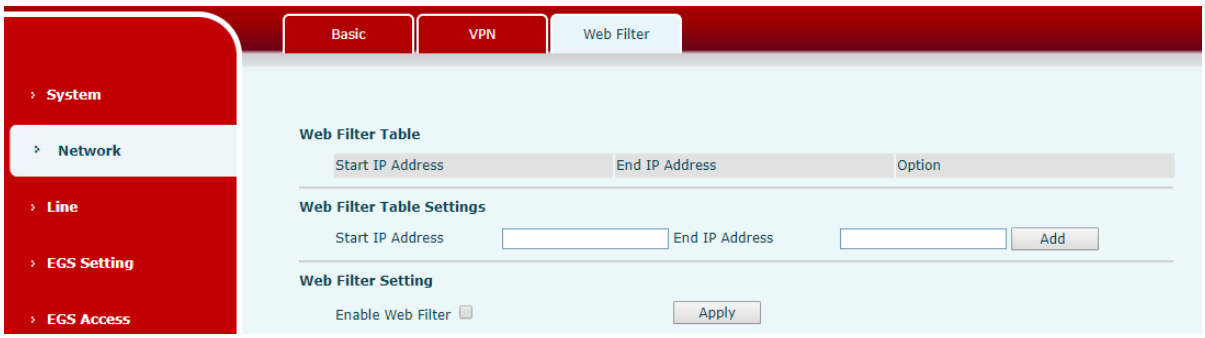
| | |
|---|---|
| OpenVPN Configuration file: | client.ovpn |
| CA Root Certification: | ca.crt |
| Client Certification: | client.crt |
| Client Key: | client.key |

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.

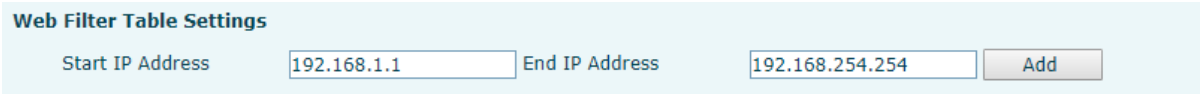
Same as L2TP connection, the connection will be established every time when system rebooted until user disable it manually.

## 10.11 Network >> Web Filter

Users can set up machines that allow access to configuration management devices only for a given network segment IP.




*Picture 20 - Web Filter settings*



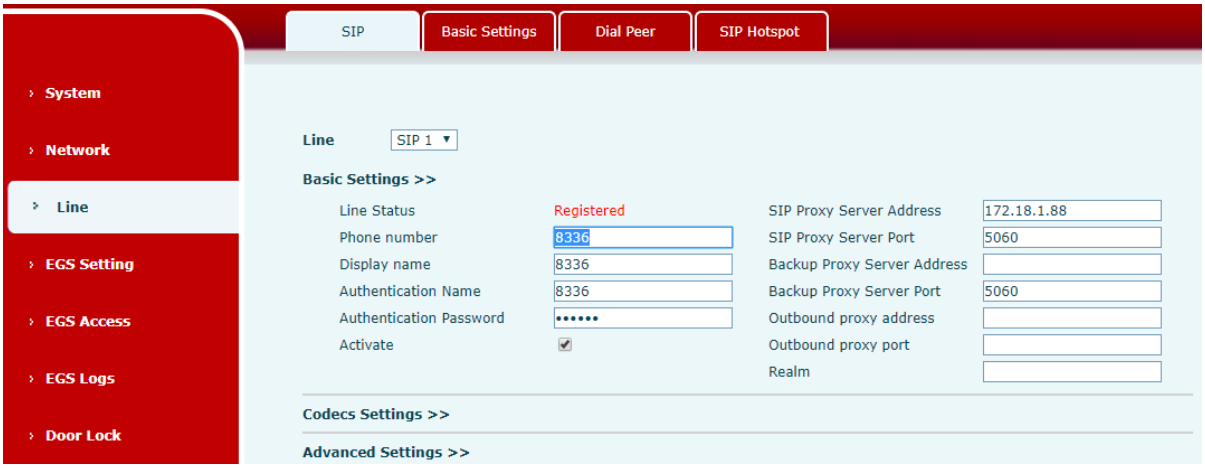

*Picture 21 - Web Filter Table*

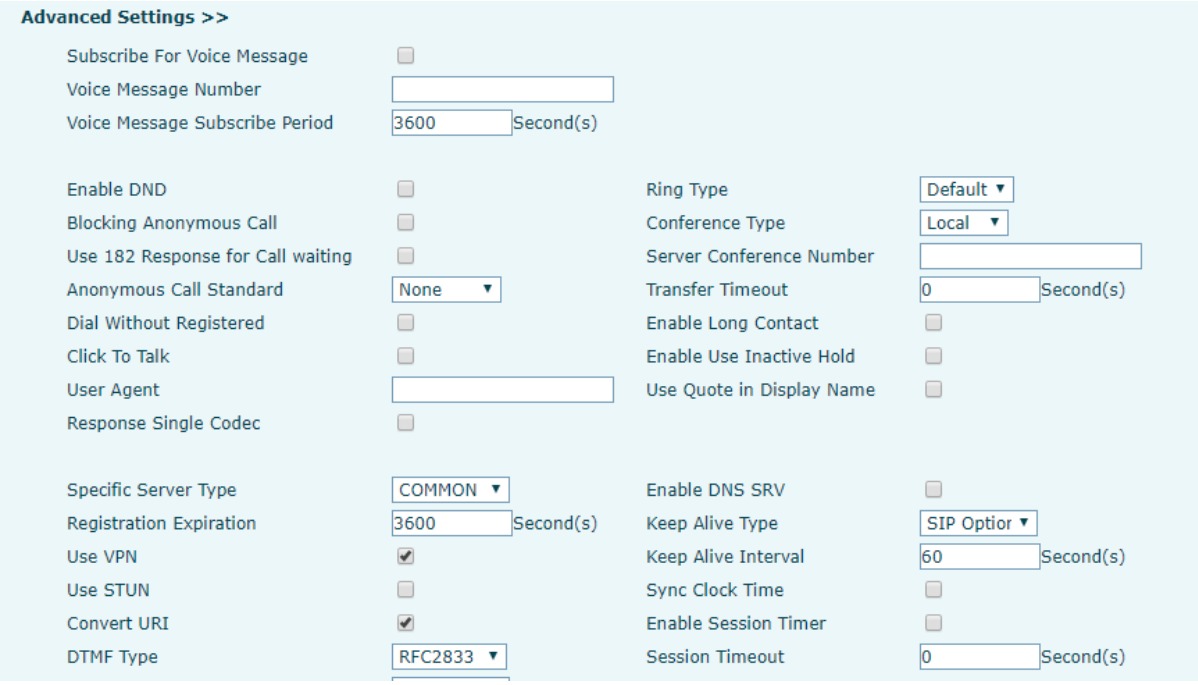
Add and remove accessible IP segments; Configure the starting IP address within the start IP, end the IP address within the end IP, and click [**Add**] to submit to take effect. A large network segment can be set, or it can be divided into several network segments to add. When deleting, select the initial 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.

## 10.12 Line >> SIP






***Picture 22 - SIP Line Configuration***

Configure the service configuration for the wire on this page.

***Table 10 - Line configuration on the web page***

| **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 |

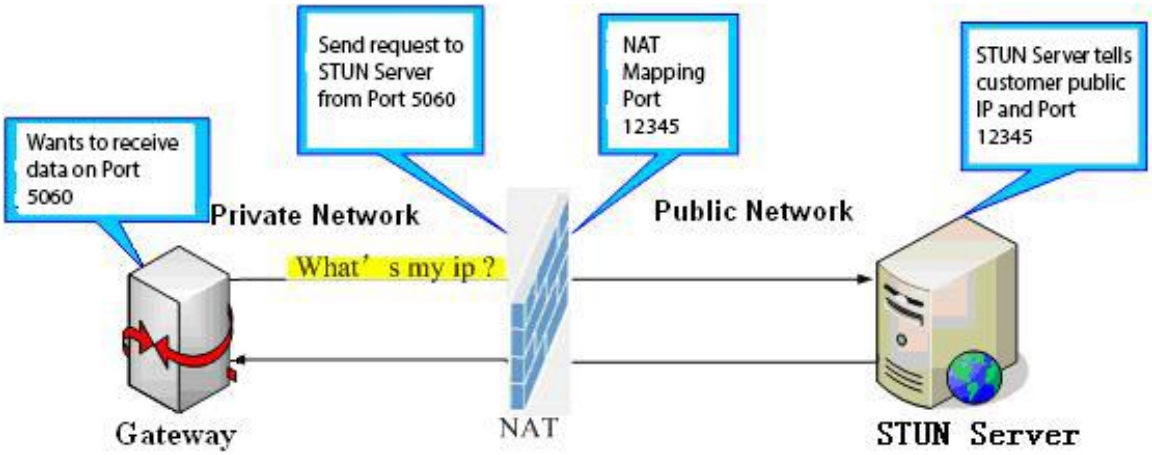
| | |
|---|---|
| Outbound proxy port | Enter the outbound proxy port, default is 5060 |
| Realm | Enter the SIP domain if requested by the service provider |
| **Codecs Settings** | |
| Set the priority and availability of the codecs by adding or remove them from the list. | |
| **Advanced Settings** | |
| 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 Hold | Active capture package SDP is inactive, while the hold is sendrecv. Active capture package has no response of 400, etc. Hold the hair inactive |

| | |
|---|---|
| | After closing the grab packet, you can see that the DSP is sendonly and the hold is sendrecv |
| 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:<br>In-band<br>RFC2833<br>SIP_INFO<br>AUTO<br>Different service providers may offer different models |
| DTMF SIP INFO Mode | When the device's DTMF type is set to SIP_INFO<br>The DTMF_SIP_INFO type is configured to send */#, and when the device presses the */# key, the actual value sent is */#;<br>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 |

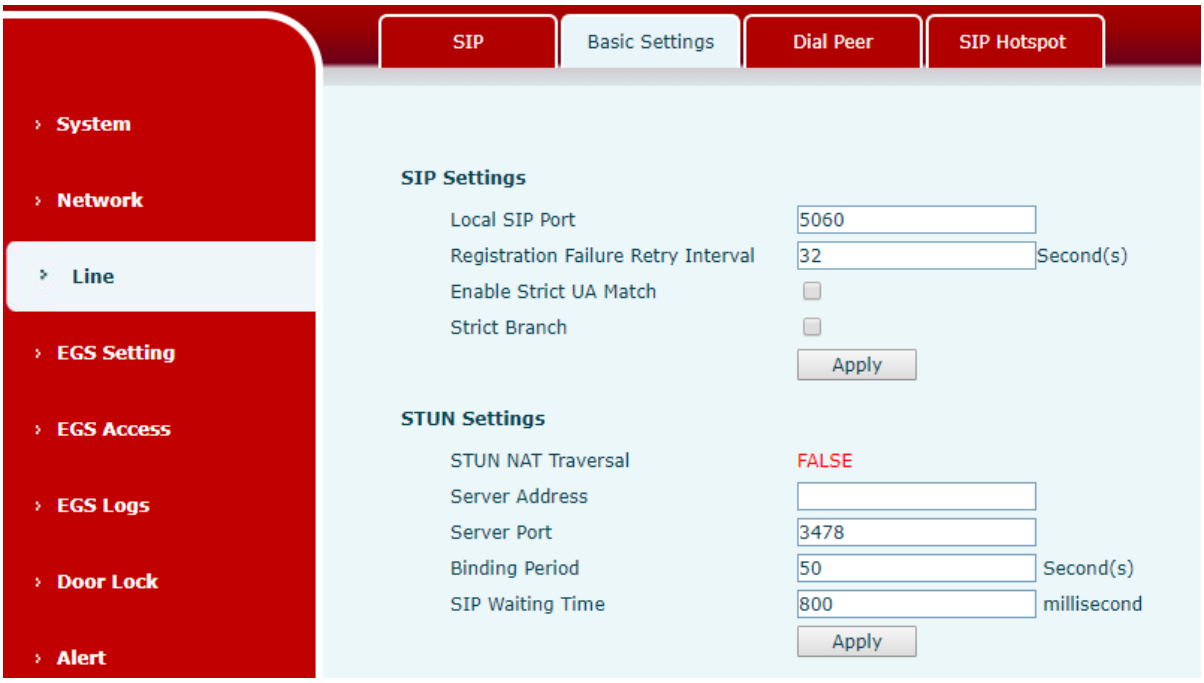
## 10.13 Line >> Basic Settings

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.




*Picture 23 - Network Basic*

Setting up SIP Global Configuration:




*Picture 24 - Basic Line Settings*

*Table 11 - Basic Line Settings*

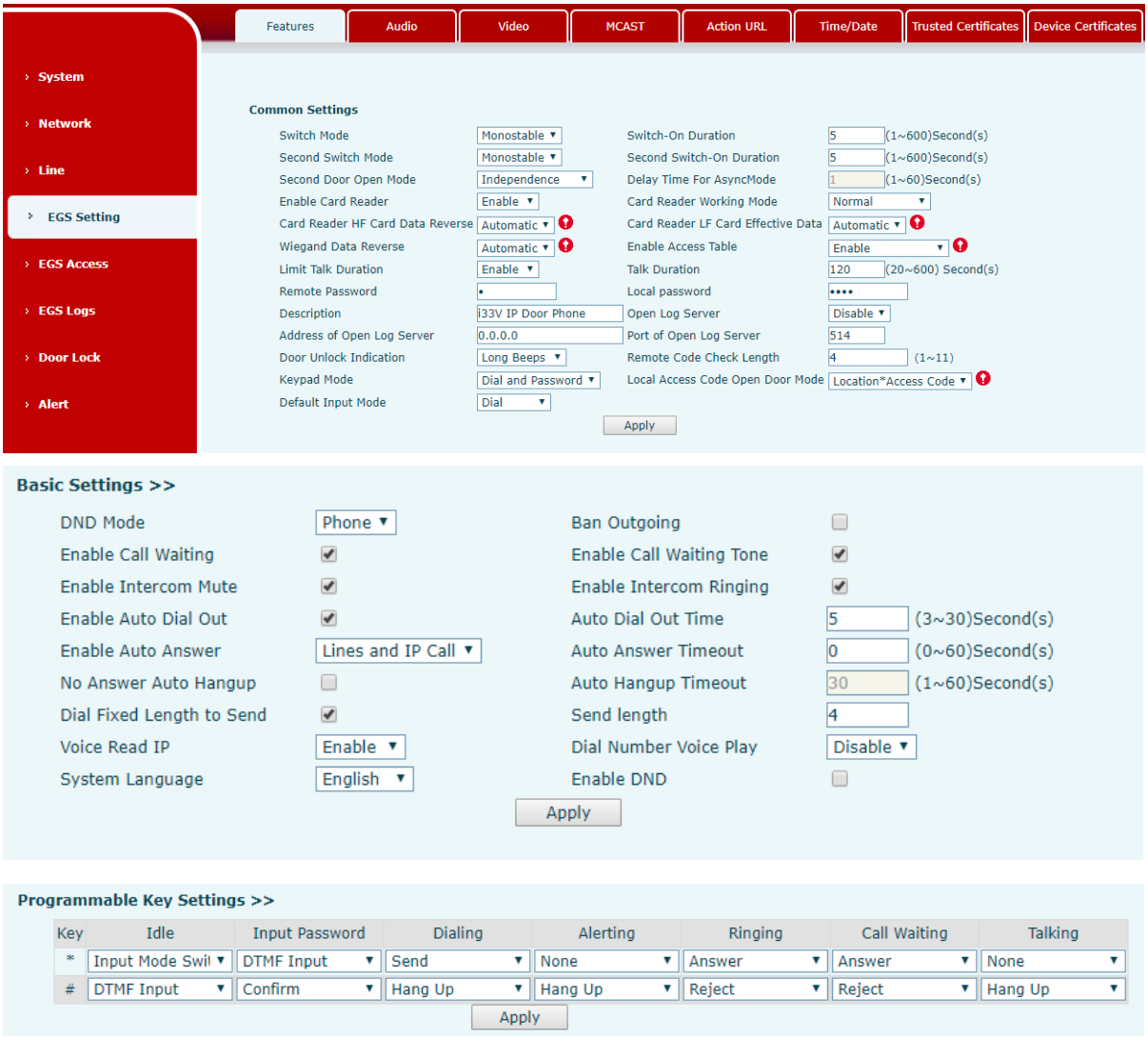
| Field Name | Explanation |
|---|---|
| **SIP Settings** | |
| Local SIP Port | Set the local SIP port used to send/receive SIP messages. |
| Registration Failure Retry Interval | Set the retry interval of SIP REGISTRATION when registration failed. |
| Enable Strict UA Match | Enable or disable Strict 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. |

## 10.14 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.

## 10.15 EGS Setting >> Features




***Picture 25 - ESG Feature Settings***

***Table 12 - ESG Feature Parameters***

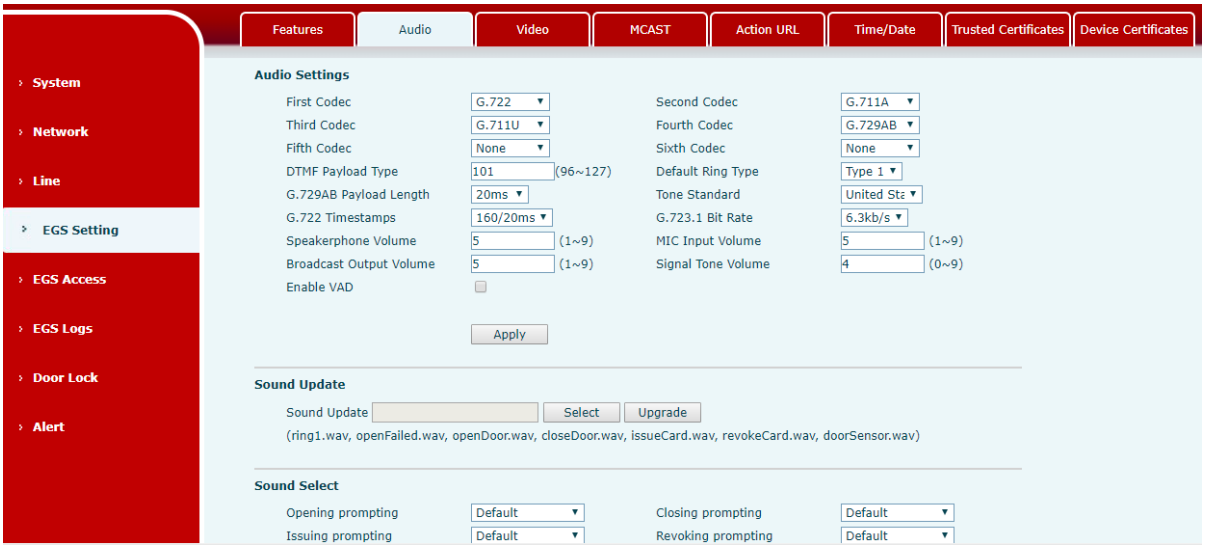
| **EGS Features Setting (Only for Door phone)** | |
|---|---|
| **Field Name** | **Explanation** |
| **Basic Settings** | |
| Switch Mode | Monostable: there is only one fixed action status for door unlocking.<br>Bistable: there are two actions and statuses, door unlocking and door locking. Each action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

| | |
|---|---|
| | status. After changed, the status would be kept.<br>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:<br>Normal: This is the work mode, after the slot card can to open the door.<br>Card Issuing: This is the issuing mode, after the slot card can to add ID cards.<br>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;<br>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 “i33V 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. |
| Switch Mode | Monostable: there is only one fixed action status for door unlocking.<br>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.<br>Initial Value is Monostable |
| 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. |
| The key pattern | Close keyboard input;<br>Only the Password；<br>Only the Dial；<br>Dial and Password； |
| Local authentication code door opening method | Disable: after disable, cannot use the authentication code to open the door.<br>Location*Access Code：Use the location speed dial + Authentication code in the setting access rules to open the door.<br>Access Code Only：Just use the identification code to open the door |
| Default Input Mode | Password: if set to password, enter password by default.<br>Dial: if set to dial, the default number is entered. |
| **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, mute the incoming calls during an intercom call. |
| Enable Intercom Tone | If enabled, play the intercom ring tone to alert the coming of 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 | Automatic hangs up when no answer occurs within the set time. |
| Auto Hangup | Set the time of no answer auto hangs up. |

| | |
|---|---|
| Timeout | |
| 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. |
| **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.<br>X and x are wildcards which match a 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. | |
| **Programmable Key Settings(Only for Door phone, "*""#"key of customer setting)** | |
| Idle | Set the function of "*" and "#"key when idle. |
| Input Password | Set the function of "*" and "#"key when Input password. |
| Dialing | Set the function of "*" and "#"key when dialing. |
| Alerting | Set the function of "*" and "#"key when alerting. |
| Ringing | Set the function of "*" and "#"key when ringing. |
| Call Waiting | Set the function of "*" and "#"key when call waiting. |
| Talking | Set the function of "*" and "#"key when talking. |

## 10.16 EGS Setting & Intercom Setting >> Audio



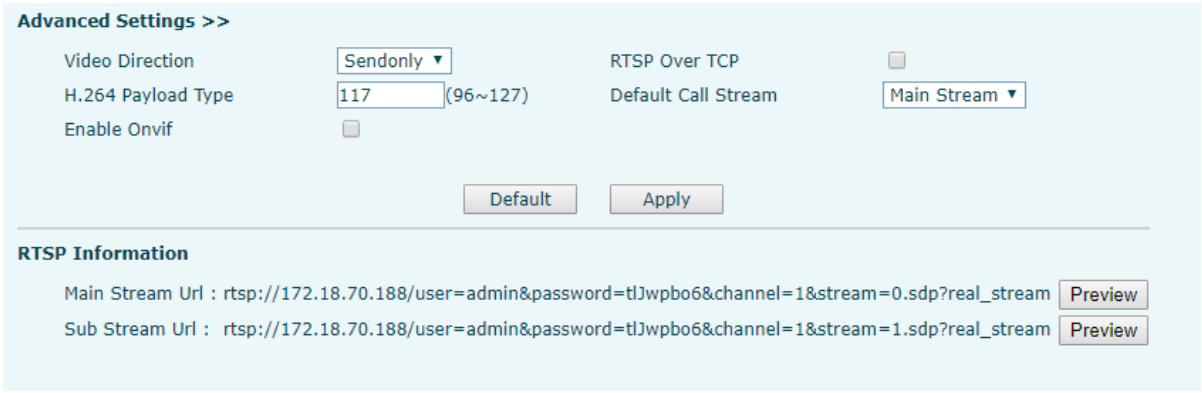

*Picture 26 - EGS Audio Settings*

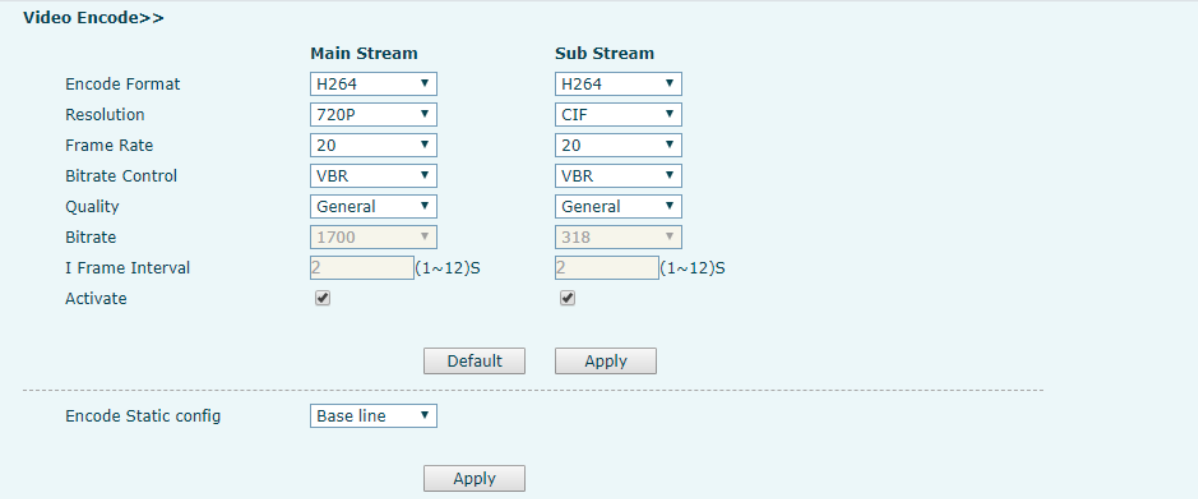
*Table 13 - EGS Audio Parameters*

| Field Name | Explanation |
|---|---|
| **Audio Settings** | |
| Codec Setting | Select enabled or disabled audio codec:<br>G.711A/U,G.722,G.723,G.729,<br>G.726-16,G726-24,G726-32,G.726-40,<br>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<br>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 openning, door |

| | |
|---|---|
| | closing, and other custom prompt sound |
| **Field Name** | **Explanation** |
| **Audio Settings** | |
| **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 |

## 10.17 EGS Setting & Intercom Setting >> Video




*Picture 27 - EGS Video Settings*

*Table 14 - EGS Video Parameters*

| **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.<br>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<br>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<br>Day Mode: The camera's video screen is always colored, if there is IR-cut will be synchronized to switch.<br>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.<br>Outdoor: installed in the outdoor preferred.<br>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<br>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<br>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.<br>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;<br>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 |

## 10.18 EGS Setting & Intercom Setting >> MCAST

It is easy and convenient to use a 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 the 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 - Web multicast 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. |

## 10.19 EGS Setting & Intercom Setting >> Action URL

*Table 16 - Action URL Settings*

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

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

http://www.fanvil.com.cn/Uploads/Temp/download/20190122/5c46dd1ad4635.pdf

## 10.20 EGS Setting & Intercom Setting >> Time/Date

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

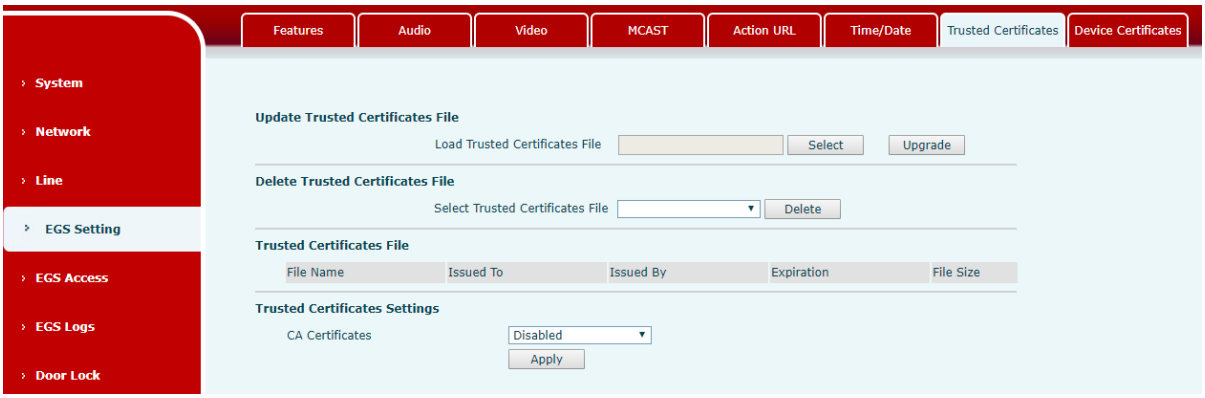
*Table 17 - Date&Time Parameters*

| 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 | Set the time by hand, which needs to disable SNTP service first |

## 10.21 EGS Settings >> Trusted Certificates

Upload and delete uploaded certificates on the certificate management page .

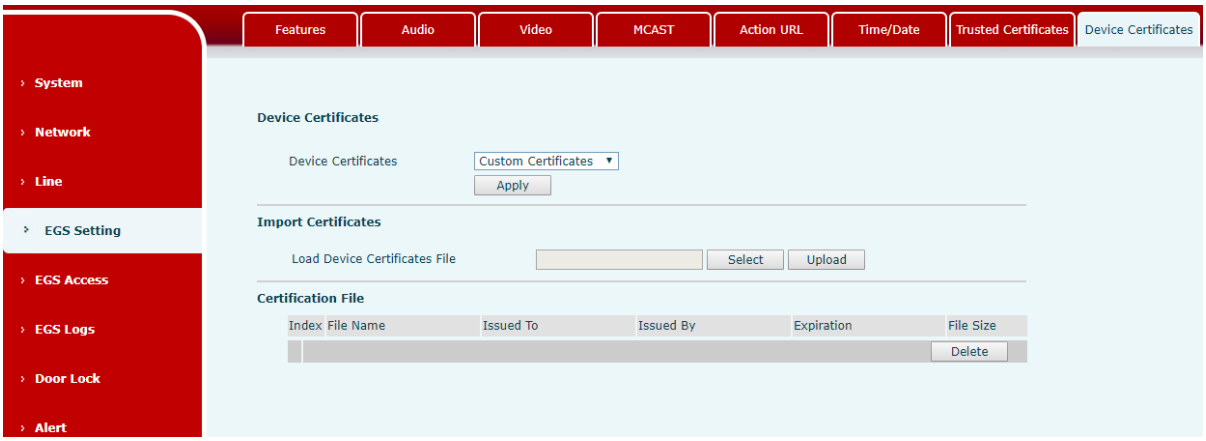



*Picture 28 - Certificate Management*

## 10.22 EGS Settings >> Device Certificates

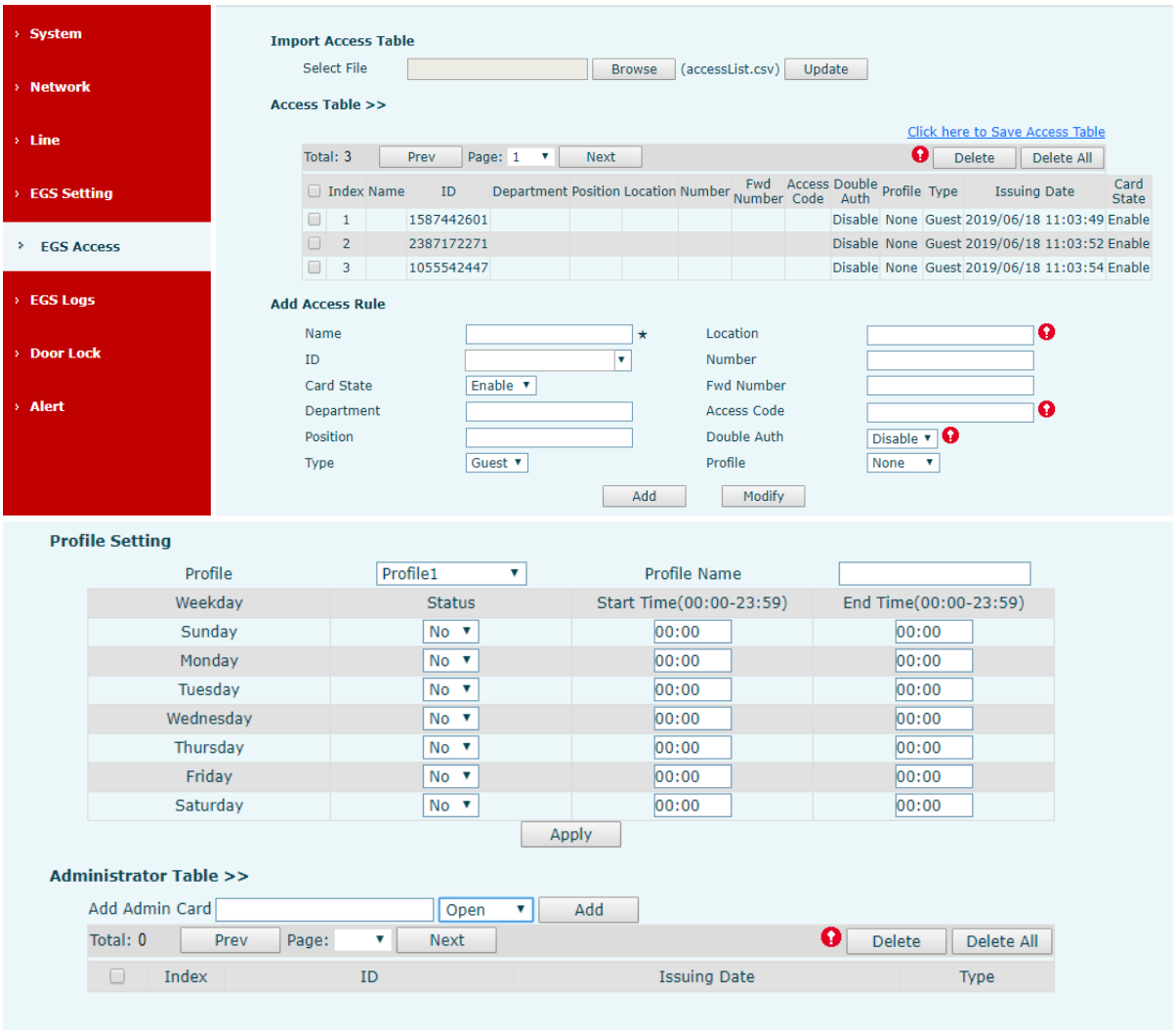
Select the device certificate as the default and custom certificate.

You can upload and delete uploaded certificates.




*Picture 29 - Device Certificates*

## 10.23 EGS Access




*Picture 30 - EGS Management*

*Table 18 - EGS Manage Parameters*

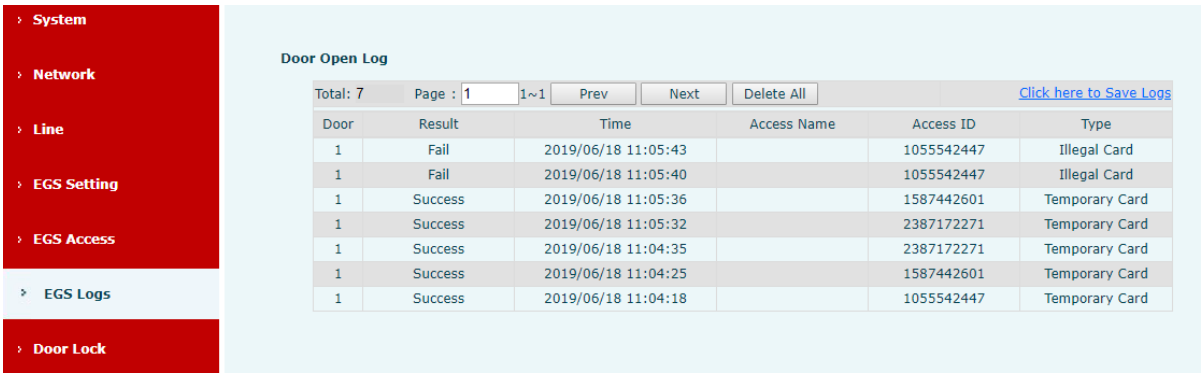
| **EGS Access** | |
|---|---|
| **Field Name** | **Explanation** |
| **Import Access Table** | |
| Click the <Browse> to choose to import remote access list file (access List.csv) and then clicking <Update> can batch import remote access rule. | |
| **Access Table** | |
| According to entrance guard 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.<br>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.<br>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.<br><br>Open：Super administrator card, the device can open the door through the super management card when the device cannot open due to the software processing error or configuration read failure.<br>When door phone is in the 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 as issuing a card.<br>The device can support up to 10 admin cards, 1000 copies of ordinary cards.<br>Note: in the issuing state, deleted card by swiping is invalid. | |
| Admin card database: Show 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. |

## 10.24 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.



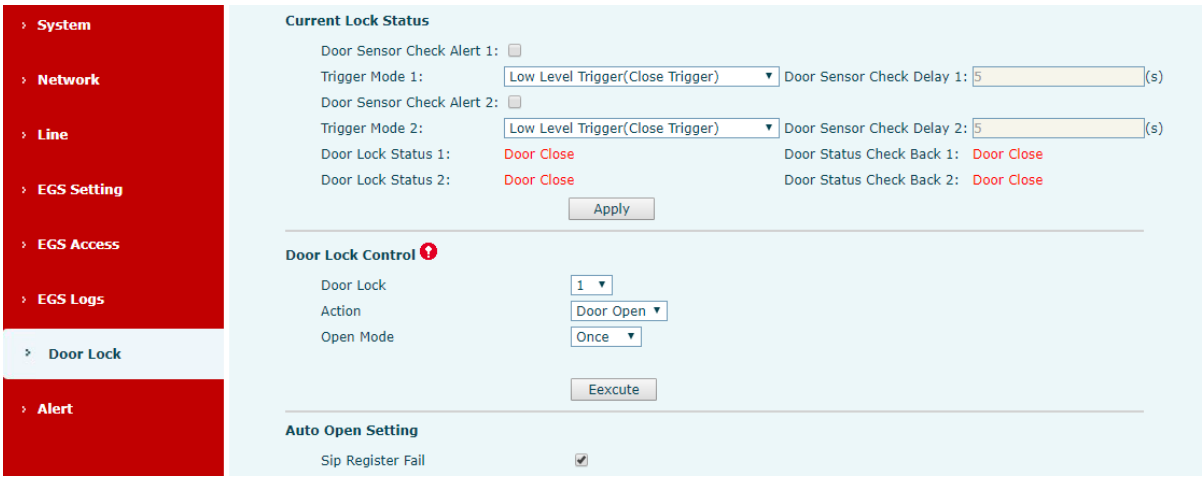

*Picture 31 - EGS Logs*

*Table 19 - EGS Logs Parameters*

| Field | Explanation |
|---|---|

| Name | |
|---|---|
| **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<br>Note: there are three kinds of card feedback results.<br>Temporary Card (only added the card number, without adding other rules )<br>Valid Card (added access rules)<br>Illegal Card (the card not added in the door phone database) |

## 10.25 Door Lock



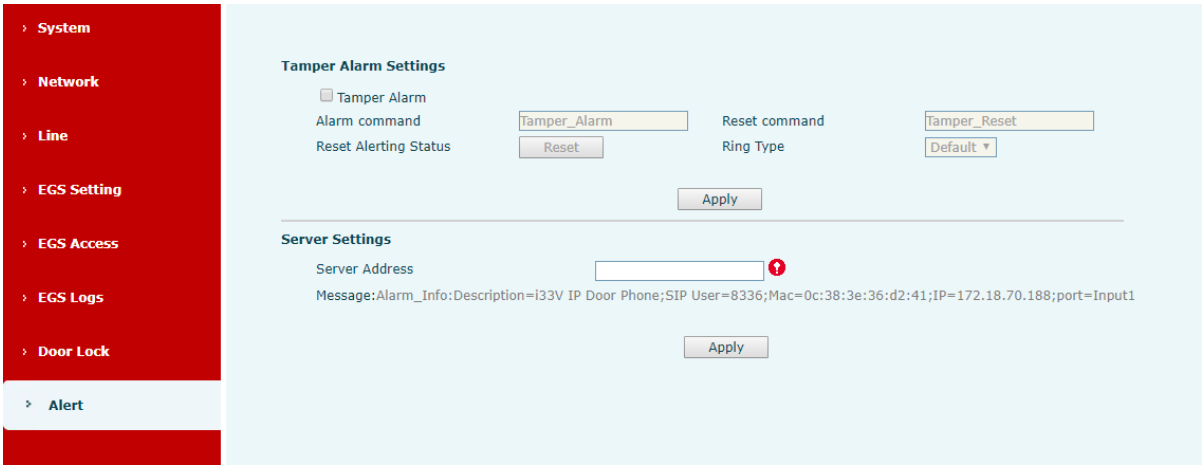

*Picture 32 - Door Lock*

*Table 20 - Door Lock Parameters*

| 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 | Door magnetic detection delay time setting |

| | |
|---|---|
| Check Delay | |
| 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.<br>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 |

## 10.26 Alert




*Picture 33 - Alert Settings*

*Table 21 - Alert Settings Parameters*

| 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.<br>message format：Alarm Info: Description=i33V;SIP User=;Mac=00:a8:34:68:23:d1;IP=172.18.90.235;port=Input1 |

# 11 Trouble Shooting

When the phone can't be used normally, the user can try the following methods to restore normal operation of the phone or collect relevant information and send a problem report to Fanvil technical support mailbox.

## 11.1Get Device System Information

Users can get information by pressing the [**Menu**] >> [**Status**] option in the phone.The following information will be provided:
The network information
Equipment information (model, software and hardware version), etc.

## 11.2Reboot Device

Users can reboot the device from soft-menu, [**Menu**] >> [**Basic**] >> [**Reboot System**], and confirm the action by [**OK**]. Or, simply remove the power supply and restore it again.

## 11.3Reset Device to Factory Default

Reset Device to Factory Default will erase all user's configuration, preference, database and profiles on the device and restore the device back to the state as factory default.

To perform a factory default reset, user should press [**Menu**] >> [**Advanced**] , and then input the password to enter the interface. Then choose [**Factory Reset**] and press [**Enter**], and confirm the action by [**OK**]. The device will be rebooted into a clean factory default state.

## 11.4Network Packets Capture

Sometimes it is helpful to dump the network packets of the device for issue identification. To get the packets to dump of the device, user needs to log in the device web portal, open page [**System**] >> [**Tools**] and click [**Start**] in "Network Packets Capture" section. A pop-up message will be prompt to ask user to save the capture file. User then should perform relevant operations such as activate/deactivate line or making phone calls and click [**Stop**] button on the web page

when operation finished. The network packets of the device during the period have been dumped to the saved file.Users can analyze packets or send them to the Fanvil support mailbox.

## 11.5Common Trouble Cases

***Table 22 - Trouble Cases***

| Trouble cases | Solution |
|---|---|
| Device could not boot up | 1. The device is powered by external power supply via power adapter or PoE switch. Please use standard power adapter provided by Fanvil or PoE switch met with the specification requirements and check if the device is well connected to power source.<br>2. If you saw “POST MODE” on the device screen,（SIP/NET and Function key indicator light is always on） the device system image has been damaged. Please contact local technicist to help you restore the phone system. |
| Device could not register to a service provider | 1. Please check if device is well connected to the network. The network Ethernet cable should be connected to the [Network] port NOT the [PC] port.<br>2. Please check if the device has an IP address. Check the system information, if the IP displays “Negotiating…”, the device does not have an IP address. Please check if the network configurations is correct.<br>3. If network connection is fine, please check again your line configurations. If all configurations are correct, please kindly contact your service provider to get support, or follow the instructions to get the network packet capture of registration process and send it to Fanvil support email box to analyze the issue. |

**Warning**

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER’S AUTHORITY TO OPERATE THE EQUIPMENT.