



User Manual

i10&i10V&i10D

Software Version: 1.0.0

Release Date: 2019/07/24



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 Overview..... | 5 |
| 6.2 Quick Setting..... | 5 |
| 6.3 WEB configuration..... | 6 |
| 6.4 SIP Configurations..... | 7 |
| 7 Basic Function | 8 |
| 7.1 Making Calls..... | 8 |
| 7.2 Answering Calls..... | 8 |
| 7.3 End of the Call..... | 8 |
| 7.4 Auto-Answering..... | 8 |
| 7.5 Call Waiting..... | 10 |
| 8 Advance Function | 11 |
| 8.1 Intercom..... | 11 |
| 8.2 MCAST..... | 11 |
| 8.3 Hotspot..... | 13 |
| 9 Web Configurations | 15 |
| 9.1 Web Page Authentication..... | 15 |
| 9.2 System >> Information..... | 15 |
| 9.3 System >> Account..... | 16 |
| 9.4 System >> Configurations..... | 16 |
| 9.5 System >> Upgrade..... | 17 |
| 9.6 System >> Auto Provision..... | 19 |
| 9.7 System >> FDMS..... | 22 |
| 9.8 System >> Tools..... | 22 |

| | | |
|-----------|---------------------------------------|-----------|
| 9.9 | Network >> Basic..... | 23 |
| 9.10 | Network >> Service Port..... | 25 |
| 9.11 | Network >> VPN..... | 26 |
| 9.12 | Line >> SIP..... | 27 |
| 9.13 | Line >> SIP Hotspot..... | 32 |
| 9.14 | Line >> Basic Settings..... | 32 |
| 9.15 | Intercom Setting >> Features..... | 34 |
| 9.16 | Intercom Setting >> Audio..... | 36 |
| 9.17 | Intercom Setting >> MCAST..... | 37 |
| 9.18 | Intercom Setting >> Action..... | 38 |
| 9.19 | Intercom Setting >> Time/Date..... | 38 |
| 9.20 | Intercom settings >> Tone..... | 39 |
| 9.21 | Call List >> Call List..... | 40 |
| 9.22 | Web Dial..... | 41 |
| 9.23 | Function Key..... | 41 |
| 9.24 | Security >> Web Filter..... | 45 |
| 9.25 | Security >> Trusted Certificates..... | 45 |
| 9.26 | Security >> Device Certificates..... | 46 |
| 9.27 | Security >> Firewall..... | 47 |
| 9.28 | Device Log..... | 48 |
| 9.29 | Security Settings..... | 48 |
| 10 | Trouble Shooting..... | 52 |
| 10.1 | Get device system information..... | 52 |
| 10.2 | Reboot device..... | 52 |
| 10.3 | Device factory reset..... | 52 |
| 10.4 | Network Packets Capture..... | 52 |
| 10.5 | Get Log Information..... | 53 |
| 10.6 | Common Trouble Cases..... | 53 |

1 Picture

| | |
|---|----|
| Figure 1 - Panel..... | 5 |
| Figure 2 - Quickly setting..... | 6 |
| Figure 3 - WEB Login..... | 6 |
| Figure 4 - SIP Line Configuration..... | 7 |
| Figure 5 - Function Setting..... | 8 |
| Figure 6 - Enable Auto Answer..... | 9 |
| Figure 7 - Enable Auto Answer..... | 9 |
| Figure 8 - Call Waiting..... | 10 |
| Figure 9 - Intercom..... | 11 |
| Figure 10 - MCAST..... | 12 |
| Figure 11 - SIP Hotspot..... | 14 |
| Figure 12 - WEB Account..... | 16 |
| Figure 13 - System Setting..... | 16 |
| Figure 14 - Upgrade..... | 17 |
| Figure 15 - Online Upgrade..... | 18 |
| Figure 16 - Auto Provision..... | 19 |
| Figure 17 - FDMS..... | 22 |
| Figure 18 - Tools..... | 23 |
| Figure 19 - Network Basic Settings..... | 23 |
| Figure 20 - Service Port..... | 25 |
| Figure 21 - VPN..... | 26 |
| Figure 22 - SIP..... | 28 |
| Figure 23 - Network Basic..... | 33 |
| Figure 24 - Line Basic Setting..... | 33 |
| Figure 25 - Intercom Setting..... | 34 |
| Figure 26 - Media Setting..... | 36 |
| Figure 27 - MCAST..... | 37 |
| Figure 28 - time/date..... | 38 |
| Figure 29 - Tone..... | 40 |
| Figure 30 - Call List..... | 40 |
| Figure 31 - Web Dial..... | 41 |
| Figure 32 - Function Key..... | 42 |
| Figure 33 - Function Key Settings..... | 43 |
| Figure 34 - Memory Key Settings..... | 44 |
| Figure 35 - Multicast Settings..... | 44 |
| Figure 36 - Multicast Settings..... | 45 |

| | |
|---------------------------------------|----|
| Figure 37 - Trusted Certificates..... | 46 |
| Figure 38 - Device Certificates..... | 46 |
| Figure 39 - Firewall..... | 47 |
| Figure 40 - Security Settings..... | 49 |

2 Table

| | |
|---------------------------------------|----|
| Table 1 - Common command mode..... | 4 |
| Table 2 - Function key LED state..... | 4 |
| Table 3 - Panel introduction..... | 5 |
| Table 4 - Intercom..... | 11 |
| Table 5 - MCAST..... | 12 |
| Table 6 - SIP Hotspot..... | 13 |
| Table 7 - Online Upgrade..... | 18 |
| Table 8 - Auto Provision..... | 20 |
| Table 9 - FDMS..... | 22 |
| Table 10 - Network Basic Setting..... | 24 |
| Table 11 - Service port..... | 25 |
| Table 12 - Line Basic Setting..... | 33 |
| Table 13 - Intercom Setting..... | 34 |
| Table 14 - Media Setting..... | 36 |
| Table 15 - action URL..... | 38 |
| Table 16 - time/date..... | 38 |
| Table 17 - Function Key..... | 42 |
| Table 18 - Function Key Settings..... | 43 |
| Table 19 - Memory Key Settings..... | 44 |
| Table 20 - Multicast Settings..... | 44 |
| Table 21 - Firewall..... | 47 |
| Table 22 - Security Settings..... | 49 |
| Table 23 - Common Trouble Cases..... | 53 |

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 the power cord or plug is impaired, do not use it because it may cause fire or electric shock.
- Do not drop, knock or shake the phone. Rough handling can break internal circuit boards.
- This phone is designed for indoor 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.
- Before using the product, please confirm that the temperature and humidity of the environment meet the working requirements of the product.
- Avoid wetting the unit with any liquid.
- Do not attempt to open it. Non-expert handling of the device could damage it. Consult your authorized dealer for help, or else it may cause fire, electric shock and breakdown.
- Do not use harsh chemicals, cleaning solvents, or strong detergents to clean it. Wipe it with a soft cloth that has been slightly dampened in a mild soap and water solution.
- When lightning, do not touch the 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

The i10/i10V/i10D SIP mini intercom is designed for indoor scenes with IP54 waterproof and dustproof. Supports wall mounting installation. It combines security, audio/video intercom and broadcasting functionalities and offers a qualified communication solution for users.

5 Install Guide

5.1 Use POE or external Power Adapter

i10/i10V/i10D, called as 'the device' hereafter, supports two power supply modes, power supply from an external power adapter or over Ethernet (POE) complied switch.

POE power supply saves the space and cost of providing the device an 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 works 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 press the speed dial button for 3 seconds, there will be a toot sound will 5 seconds, please press the speed dial button once within 5 seconds, the toot sound will stop automatically reporting IP |
| Switch network mode | <p>In the standby mode, long-press the speed dial button for 3 seconds and the beep will last for 5 seconds. Within 5 seconds, press the speed dial button three times quickly to switch to the network mode.</p> <p>If there is no IP at present, switch to the default static IP (192.168.1.128).</p> <p>Then switch to DHCP mode when it is the default static IP (192.168.1.128)</p> <p>When DHCP gets to IP, then do not switch and report the IP directly.</p> <p>Report the IP after the successful switch.</p> |

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

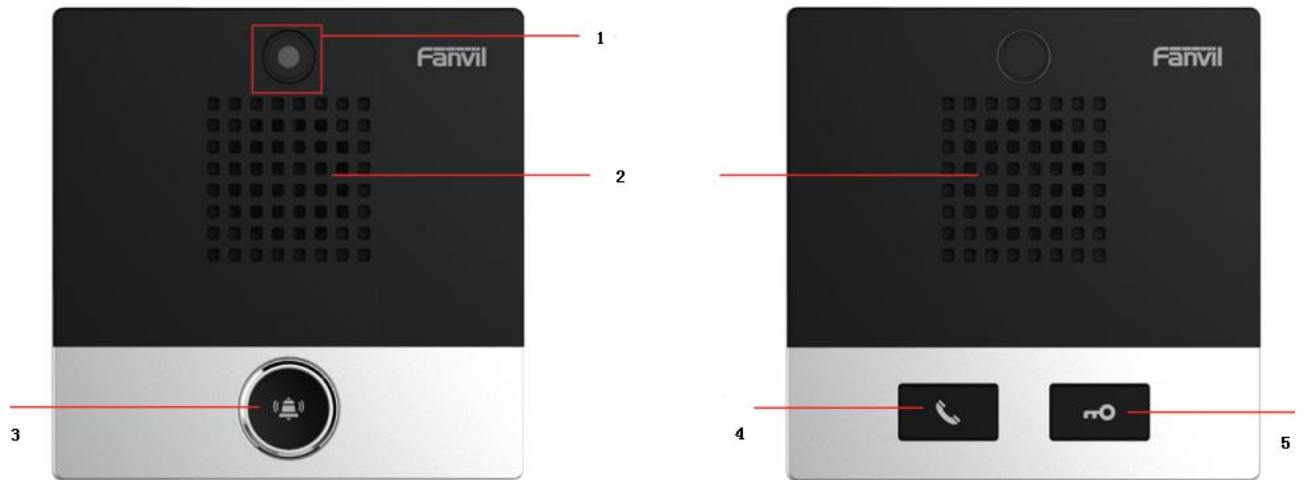


Figure 1 - Panel

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 | Speed dial/Answer button | For speed dial/answer button, multicast, intercom, IP broadcast and other functions |
| 5 | Unlock | Unlock door |

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 is DHCP. IP address can be viewed by.

- In standby mode, long press the speed dial button for 3 seconds, there will be a toot sound will 5 seconds, please press the speed dial button once within 5 seconds (please do not operate within 30 seconds when power on), the toot sound will stop automatically reporting IP.
- 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>)

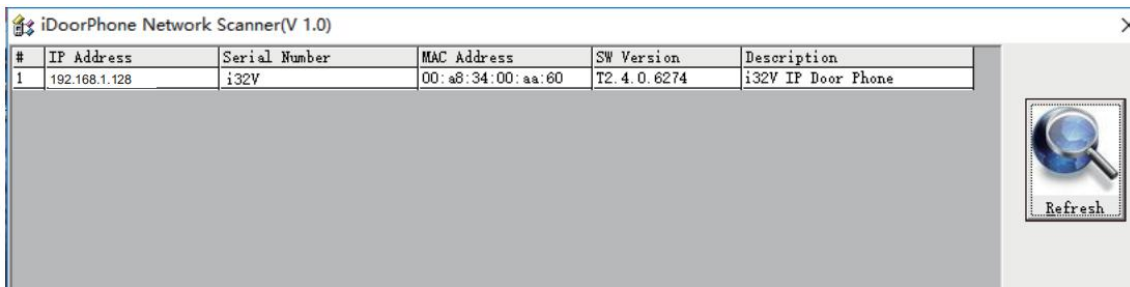


Figure 2 - Quickly setting

- In the standby mode, long-press the speed dial button for 3 seconds and the beep will last for 5 seconds. Within 5 seconds, press the speed dial button three times quickly to switch to the network mode.
- 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;

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 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:

Figure 4 - SIP Line Configuration

7 Basic Function

7.1 Making Calls

After setting the function key to memory key and the subtype as speed dial and setting the number, press the function key to immediately call out the set number, as shown below:

| Key | Type | Name | Value | Value2 | Subtype | Line |
|-----------|------------|------|-------|--------|------------|------------|
| DSS Key 1 | Memory Key | | 21976 | | Speed Dial | 21972@SIP1 |
| DSS Key 2 | None | | | | None | AUTO |
| DSS Key 3 | None | | | | None | AUTO |

Figure 5 - Function Setting

See detailed configuration instructions [9.23 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 the 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

When there is a call, you can press the speed dial button to hang up the call, the default setting is to end the call. See detailed configuration instructions [9.23 Function Key](#).

7.4 Auto-Answering

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

- **Enable auto answering on the line:**

Web interface: enter [Line] >> [SIP], Enable auto answer, set mode and auto answer time and click submit.

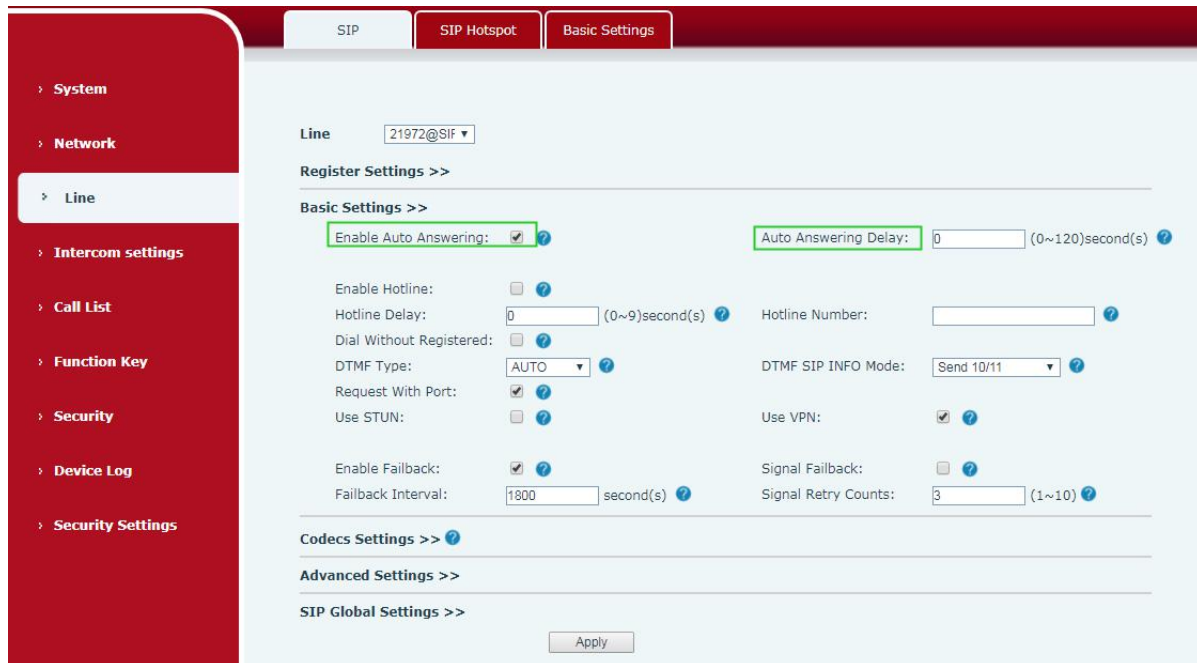


Figure 6 - Enable Auto Answer

- **Enable auto answering P2P:**

Web interface: enter [line] >> [Basic Settings] >> [SIP P2P Settings], enable automatic answering, setting mode and automatic answering time, and click submit.

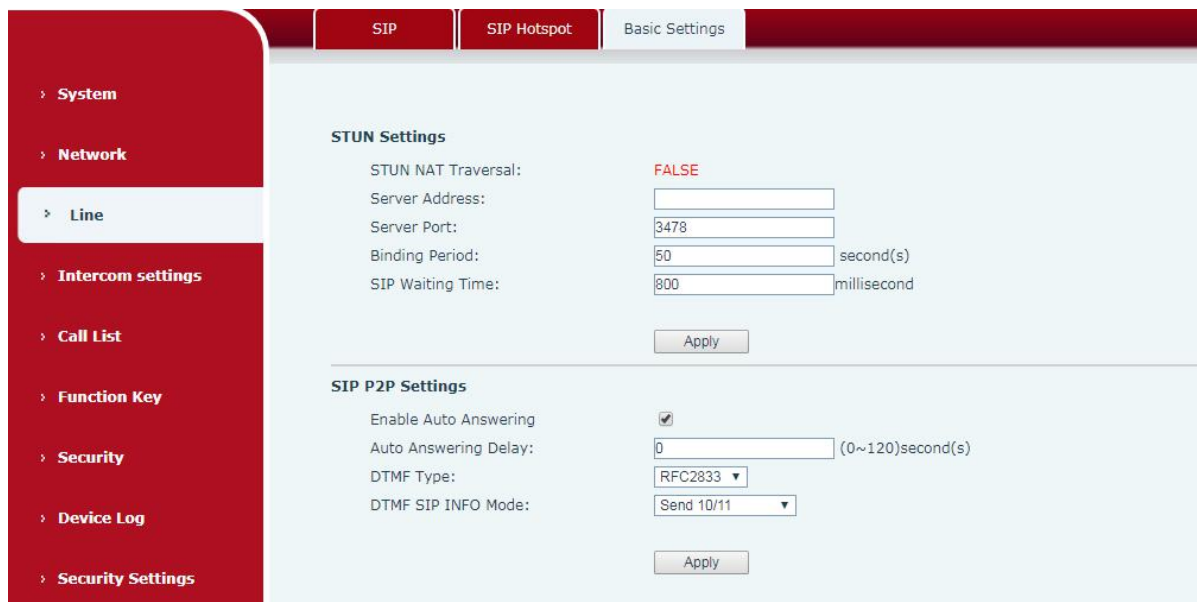


Figure 7 - Enable Auto Answer

- **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 Call Waiting

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

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

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

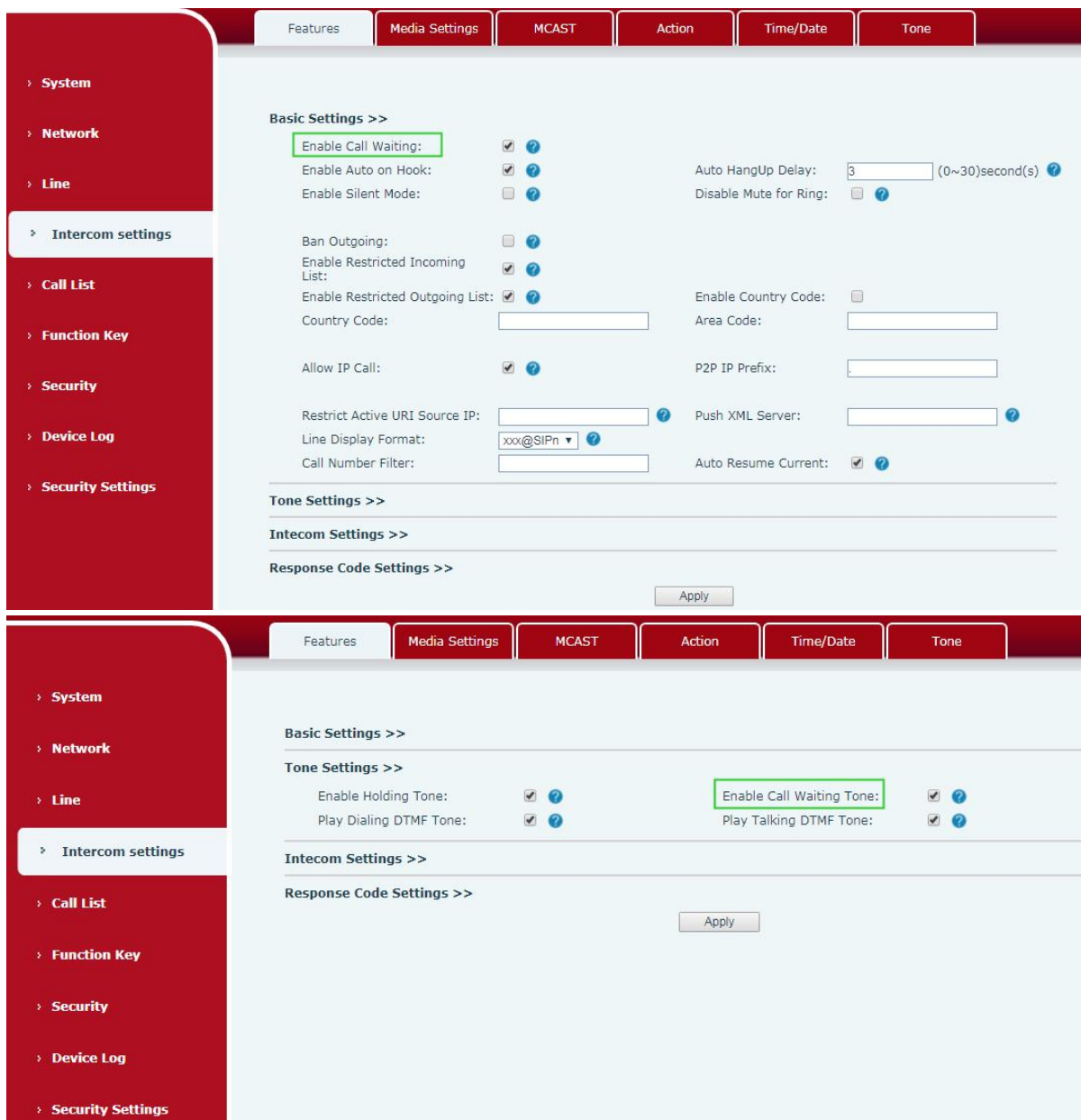


Figure 8 - Call Waiting

8 Advance Function

8.1 Intercom

The equipment can answer intercom calls automatically.

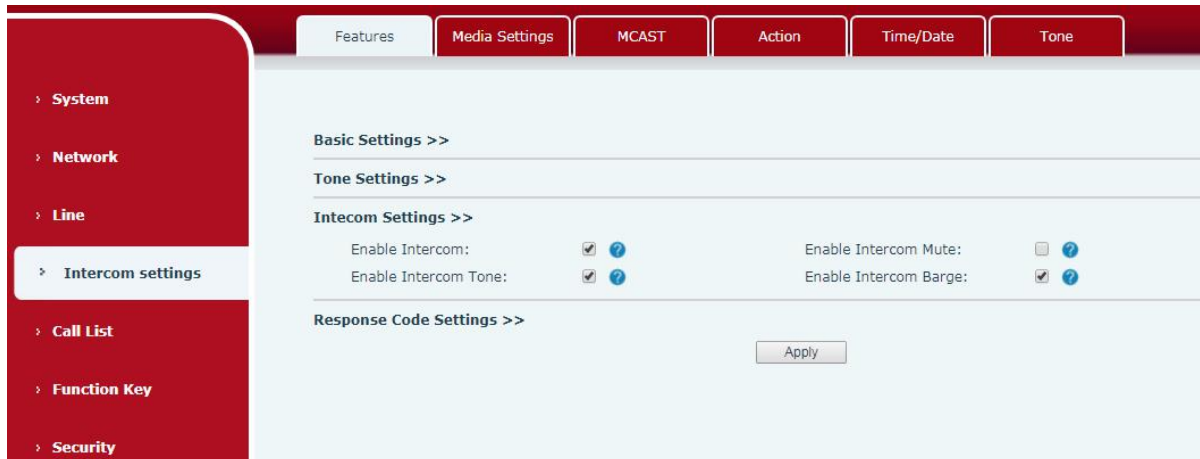


Figure 9 - Intercom

Table 4 - Intercom

| Parameters | Description |
|-----------------------|--|
| Enable Intercom | When intercom is enabled, the device will accept the incoming call request with a SIP header of Alert-Info instruction to automatically answer the call after a specific delay. |
| Enable Intercom Mute | Enable mute during intercom mode |
| Enable Intercom Tone | If the incoming call is intercom call, the device plays the intercom tone. |
| Enable Intercom Barge | If enable intercom barge, the device answers the intercom call automatically while it is in a call. If the current call is intercom call, the device will reject the second intercom call. |

8.2 MCAST

This feature allows the user to make some kind of broadcast call to people who are in the multicast group. The user can configure a multicast DSS Key on the device, which allows the 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 device to receive an RTP stream from the pre-configured multicast listening address without involving SIP signaling. You

can specify up to 10 multicast listening addresses.

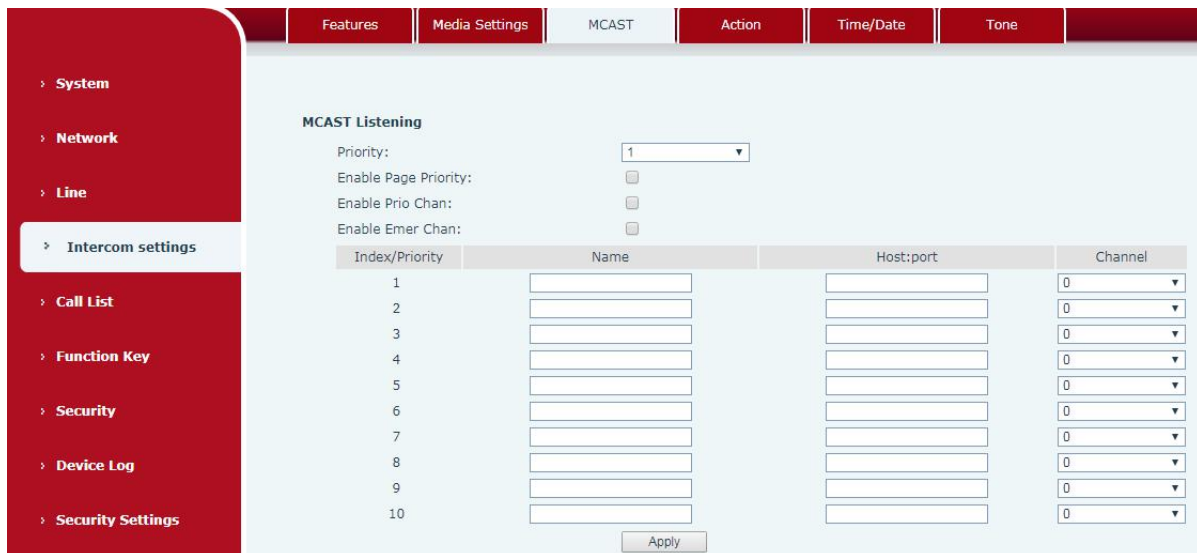


Figure 10 - MCAST

Table 5 - MCAST

| Parameters | Description |
|----------------------|--|
| Priority | Define the current call's priority, 1 means the highest priority and 10 means the lowest. |
| Enable Page Priority | If enable page priority, the device will receive the multicast from address with higher priority, regardless of which of the two multicast groups sending the multicast first. |
| Enable Prio Chan | If enable this option, the only multicast with the same port and channel can be connected. Channel 24 has the higher priority, its priority is higher than 1-23; Set channel value to be 0, it means no channel is used. |
| Enable Emer Chan | When enabled, channel 25 has the highest priority |
| Name | Set the multicast server name. |
| Host:port | Set the multicast server's multicast IP address and port. |
| Channel | 0-25 (24 priority channel, 25 emergency channel). |

Multicast:

Send multicast:

- Go to web page of [Function Key] >> [Function Key Settings], select the type to be multicast, set the multicast address, and select the codec.
- Click Apply.
- Press the DssKey of Multicast Key which you set.

Receive multicast:

- Set up the name, host and port of the receiving multicast on the web page of

[Intercom Settings] >> [MCAST].

- When the remote server sends the multicast, the device will receive multicast call and play multicast automatically.

8.3 Hotspot

SIP hotspot is a simple utility. Its configuration is simple, which can realize the function of group vibration and expand 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 answers, 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.

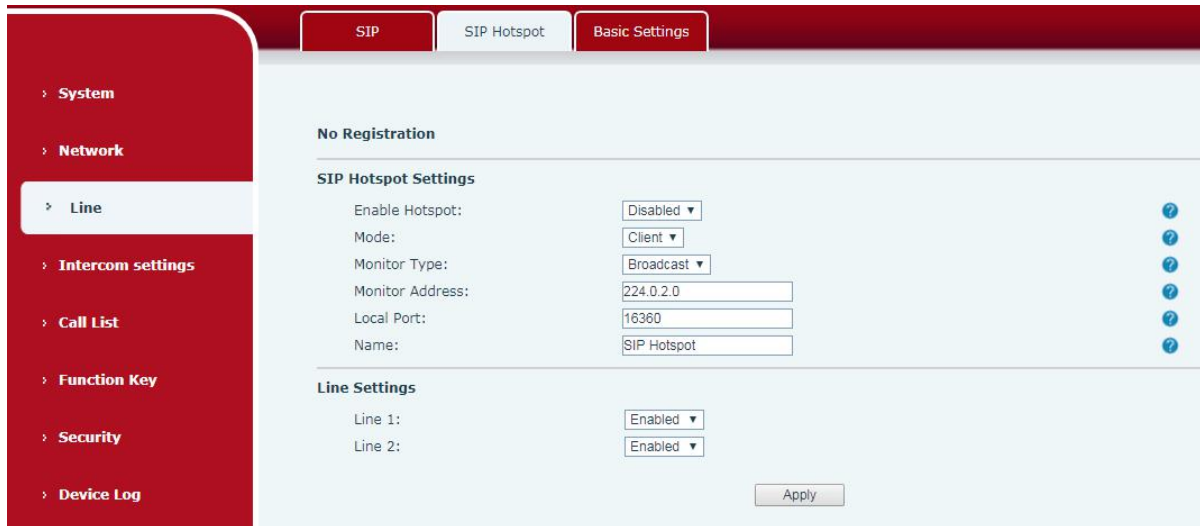


Figure 11 - SIP Hotspot

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 login the device's webpage to manage and operate the device. User must provide the correct username and password to login. If the password is incorrect for three times, the webpage will be locked for 5 minutes and then the user can try to login again.

The details as following:

- If one IP logins more than the specified number of times with different username/passwords, web login will be locked.
- If a same user login more than a specified number of times from different IP addresses, web login will be locked too.

9.2 System >> Information

Users can get the following information in **System>>Information** page:

Basic system information:

- Model
- Hardware Version
- Software Version
- Uptime
- Last uptime
- MEMInfo

And summarization of network status:

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

Besides, the summarization of SIP account status:

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

9.3 System >> Account

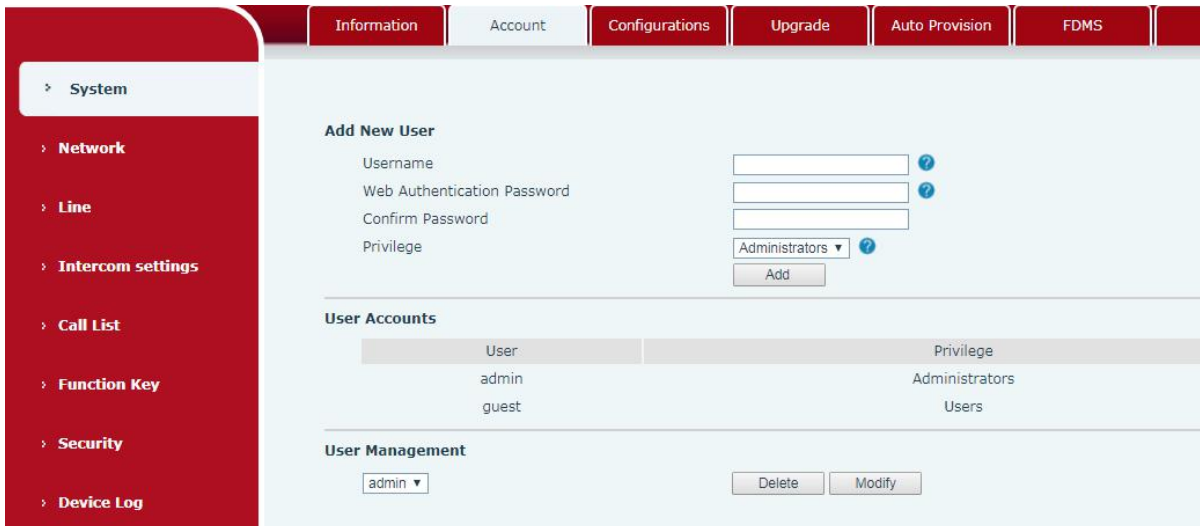


Figure 12 - WEB Account

On this page, user can change the webpage login password. Administration user can also add or delete users, manage users, set permissions and passwords for new users.

9.4 System >> Configurations

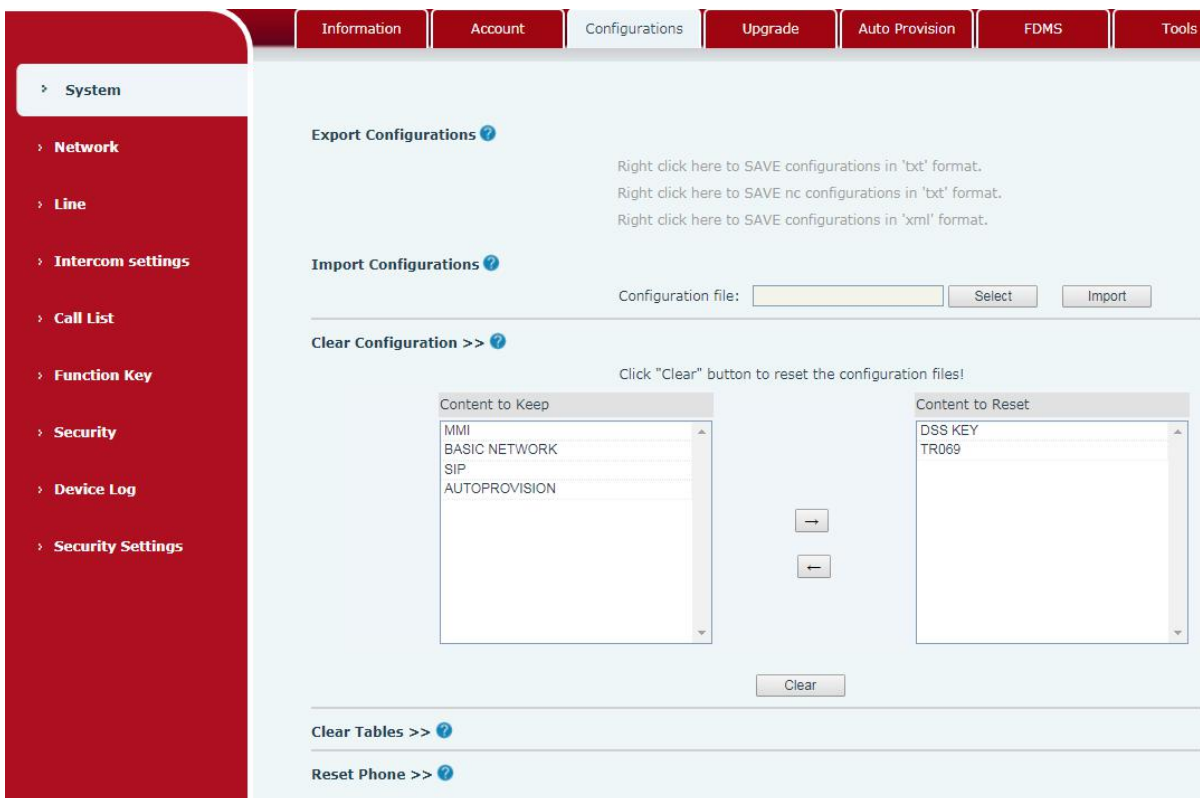


Figure 13 - System Setting

In this page, administration user can view, export, or import the configuration file, or restore the device to factory settings.

■ **Export Configurations**

Right click to download the device's configuration file to your PC, the file format is “.txt”. (Notice: only administrator user can export the configuration file.)

■ **Import Configurations**

Import the configuration file of settings. The device will restart automatically after successful importation, and the configuration will take effect after a restart

■ **Clear Configurations**

Select the module in the configuration file to clear.

SIP: SIP account configuration

AUTOPROVISION: Provision related configuration

TR069:TR069 related configuration

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

DSS Key: DSS key configuration

■ **Clear Tables**

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

■ **Reset Phone**

The device data will be cleared, including configurations and database tables.

9.5 System >> Upgrade

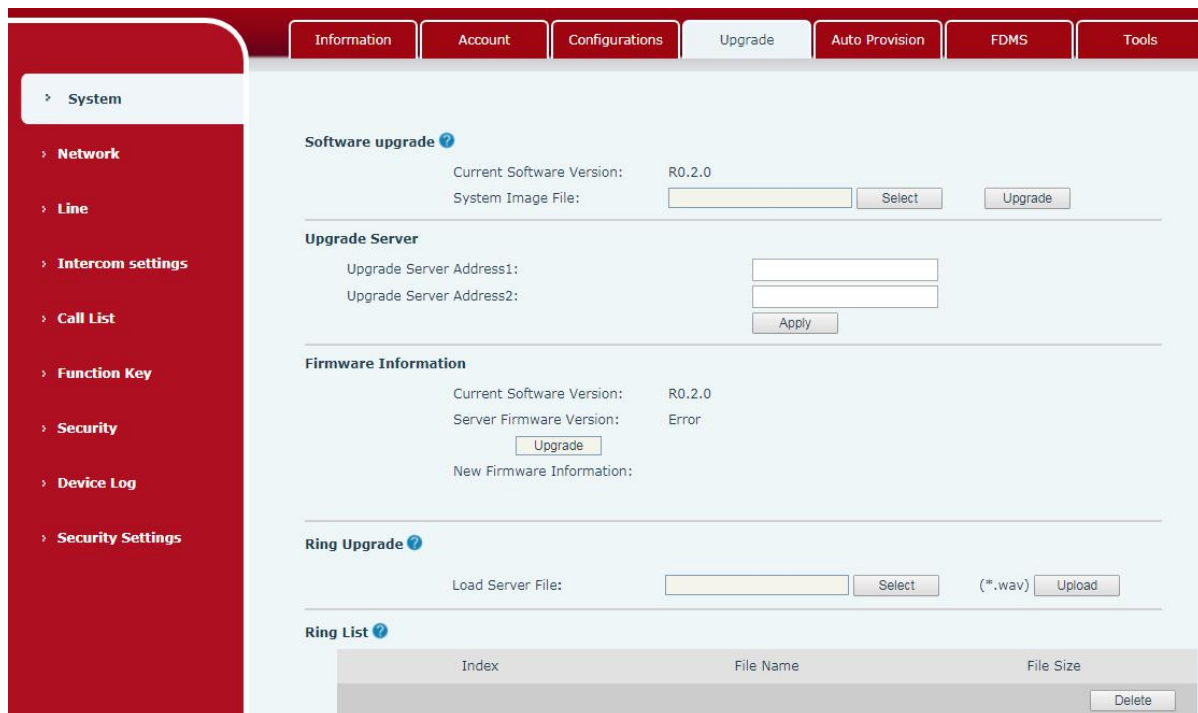


Figure 14 - Upgrade

In this page, user can upgrade the software for the device. After the upgrade, the device will automatically restart and update to the new version.

Click select to select the software file from local PC and then click upgrade to start upgrading.

Online upgrade:

Online Firmware update is when a device sends an HTTP request to a server, the server replies with a corresponding description file or 404 or timeout. After device gets the reply, it analyzes the version description file and prompts the user whether to upgrade the new version or not.

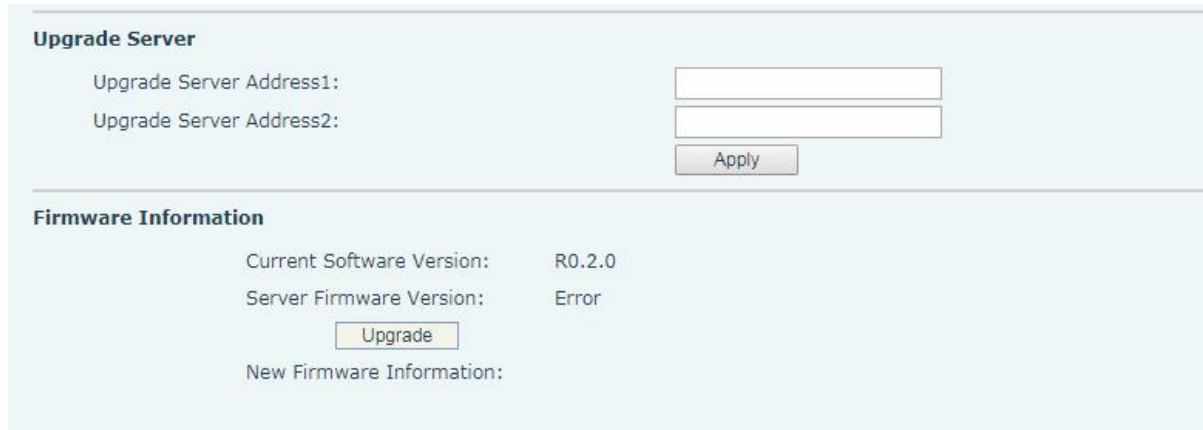


Figure 15 - Online Upgrade

Table 7 - Online Upgrade

| Parameters | Description |
|-----------------------------|--|
| Upgrade Server | |
| Upgrade Server Address1 | Fill in the available primary upgrade server (HTTP server) address. |
| Upgrade Server Address2 | Fill in the available backup upgrade server (HTTP server) address, when the primary server is not available, device will send the request to backup server. |
| Firmware Information | |
| Current Software Version | Displays the current device software version information. |
| Server Firmware Version | Displays the server software version information. |
| [Upgrade] button | When there is a corresponding TXT file and firmware file on the server side, the "upgrade" button changes from gray to available state. Click "upgrade" to choose whether to upgrade or not. |
| New Firmware Information | When the server side has the corresponding TXT file and firmware file, the new firmware information will display the version information in TXT. |

- The device requests TXT file to the server, the TXT file named with

vendor_model_hw1_0.txt. Hw is followed by the hardware version information. All spaces in file names are changed to underlined.

- The URL requested by the device is HTTP:// server address /, and both the new version and the requested file are placed in the download directory of the HTTP server.
- The TXT file format must be UTF-8.
- Vendor_model_hw1_0.txt file format is as following:

Version=1.6.3 # software Version

Firmware=xxx/xxx.z #xxx.z or http:// server IP: port/directory /xxx.z

BuildTime = 2018.09.11 20:00

Info = TXT | XML

Xxxxx

Xxxxx

Xxxxx

Xxxxx

9.6 System >> Auto Provision

Webpage: Login device's webpage and go to [System] >> [Auto provision].

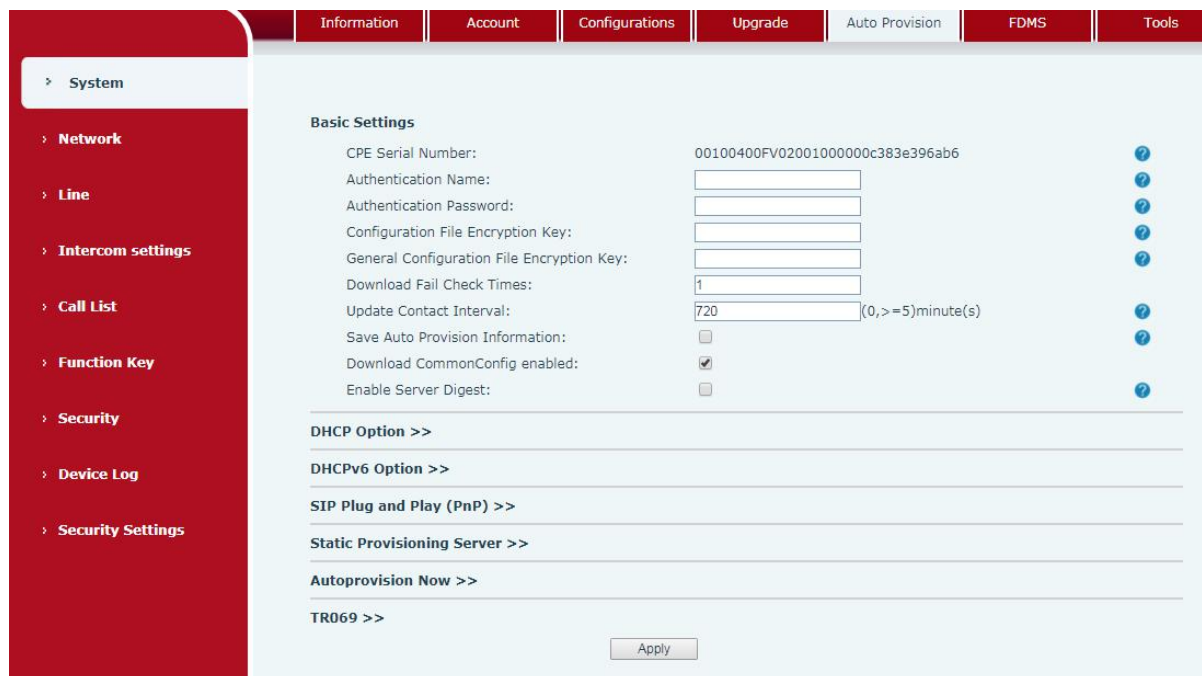


Figure 16 - Auto Provision

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

PNP>DHCP>TR069> Static Provisioning

Transferring protocol: FTP/ TFTP/HTTP/HTTPS

More details, please refer to **Fanvil Auto Provision**.

<http://www.fanvil.com/Support/download/cid/14.html>

Table 8 - Auto Provision

| Parameters | Description |
|---|---|
| Basic settings | |
| Current Configuration Version | Show the current config file's version. If the device confirm the downloaded .CFG configuration file is same with the one it uses, the device won't perform auto provision. Or if the device is matching the configuration file's context via Digest method, when the configuration file of server is modified or configuration file of device is different with server's, the device will perform provision. |
| General Configuration Version | Show the common config file's version. If the device confirm the downloaded .CFG configuration file is same with the one it uses, the device won't perform auto provision. Or if the device is matching the configuration file's context via Digest method, when the configuration file of server is modified or configuration file of device is different with server's, the device will perform provision. |
| CPE Serial Number | Serial number of the equipment |
| Authentication Name | Configure FTP server's username, TFTP server does not require this option. When use FTP server, device uses anonymous as authentication name if user leave this option blank. |
| Authentication Password | Corresponding password for FTP server. |
| Configuration File Encryption Key | Encryption key for the encrypted configuration file. |
| General Configuration File Encryption Key | Encryption key for encrypted common configuration file. |
| Save Auto Provision Information | Configure whether to save the auto provision information or not. |
| Download Fail Check Times | The default value is 5. When device fails to download configuration file, it will retry until it counts to fail check times. |
| Enable Server Digest | When the feature is enabled, if the configuration file of server is changed, or device's configuration is different from server's, the |

| | |
|-----------------------------------|---|
| | device will download and update. |
| DHCP Option | |
| Option Value | The equipment supports configuration from Option 43, Option 66, or a Custom DHCP option. User can select any of the three method to perform auto provision, by default, the option is disabled. |
| Custom Option Value | The custom option value should be same with the one of server, it can be any number 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, i10 series device will send a SIP SUBSCRIBE message with broadcast method. Any server which can support the feature will respond and send a Notify with URL to phone. The device could get the configuration file with the URL. |
| Server Address | Input SIP PnP server address. |
| Server Port | Input SIP PnP server port. |
| Transport Protocol | Select SIP PnP protocol, TCP or UDP. |
| Update Interval | Configure SIP 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, for example ftp.domain.com . And the device supports to access server subdirectory, 192.168.1.1/ftp/config or ftp.domain.com/ftp/config , it means server address is 192.168.1.1 or ftp.domain.com , file path is /ftp/config/. |
| Configuration File Name | Input the configuration file name. If it is empty, i10 series device will request the file which is named as its MAC address. |
| Protocol Type | Select transportation protocol type, i10 series support FTP/TFTP/HTTP and HTTPS |
| Update Interval | Set configuration file update interval time. As default it is 1, which means i10 series will check the update every 1 hour. |
| Update Mode | Select Provision Mode: <ol style="list-style-type: none"> 1. Disabled. 2. Update after reboot. 3. Update at a time interval. |
| TR069 | |
| Enable TR069 | Select it to enable TR069. |
| Enable TR069 Warning Tone | If TR069 is enabled, there will be a prompt tone when connecting to TR069 server successfully. |

| | |
|---------------------|---|
| ACS Server Type | There are 4 kinds of ACS server: China Unicom, China Telecom, common and esight. |
| ACS Server URL | Input ACS server address. |
| ACS User | Input ACS server username. |
| ACS Password | Input ACS server password. |
| TR069 Auto Login | Enable/Disable TR069 Auto Login. If TR069 auto login is enabled, every time user reboot the device, it will use the previous correct username or password to connect ACS server instead of asking TR069 username or password. |
| STUN server address | Enter the STUN address |
| Enable the STUN | Select it to enable STUN. |

9.7 System >> FDMS

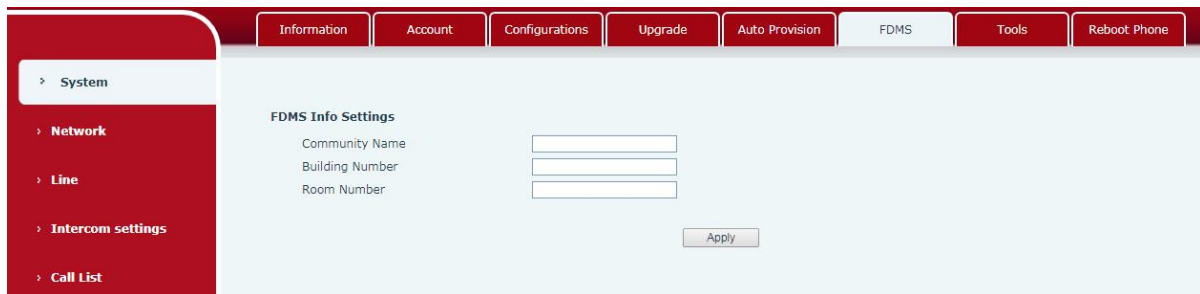


Figure 17 - FDMS

Table 9 - FDMS

| FDMS information Settings | |
|---------------------------|---|
| Community Name | Name of equipment installation community. |
| Building Number | Name of equipment installation building. |
| Room Number | Name of equipment installation room. |

9.8 System >> Tools

This page provides users the tools to check the problems.

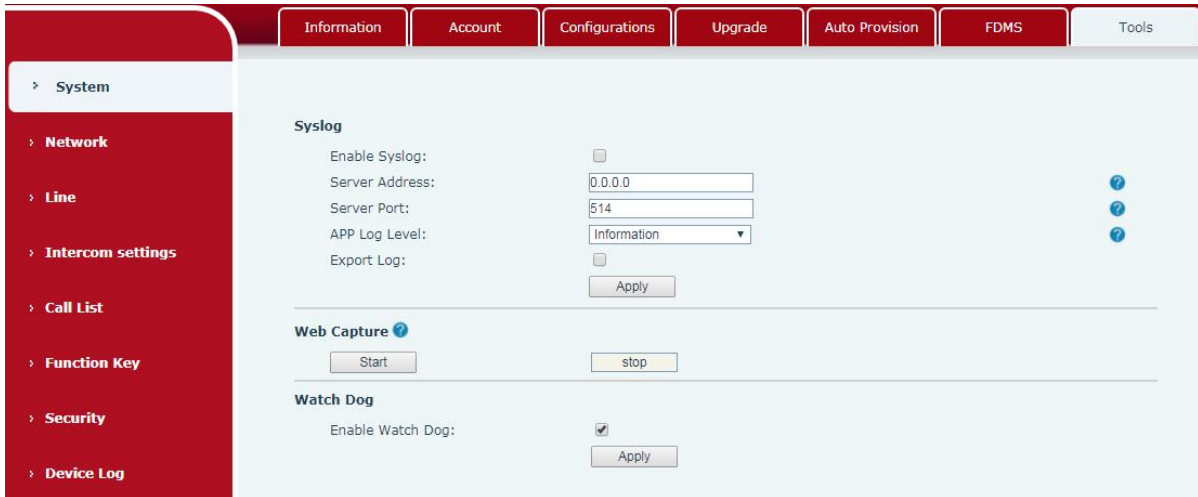


Figure 18 - Tools

Syslog: When the user open syslog and set syslog server address, the log information of the device will be recorded in the syslog server during operation. If there is any problem, send the logs to Fanvil support team to analyze.

For other details, please refer to [10 Trouble Shooting](#).

9.9 Network >> Basic

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

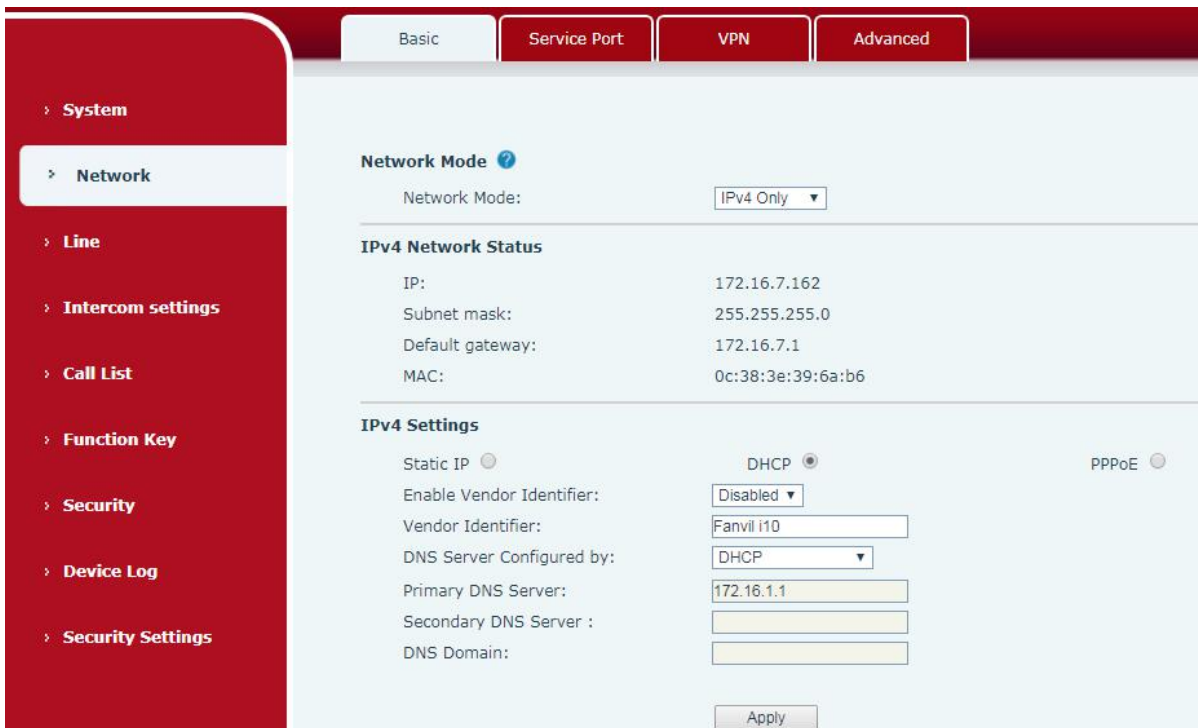


Figure 19 - Network Basic Settings

Table 10 - Network Basic Setting

| Parameters | Description |
|--|---|
| Network Mode | IPv4 only、IPv6 only、IPv4&IPv6 |
| Network Status | |
| IP | The current IP address of the equipment. |
| Subnet mask | The current Subnet Mask of the device. |
| Default gateway | The current Gateway IP address. |
| MAC | The MAC address of the equipment. |
| Settings | |
| Select the appropriate network mode. The equipment supports three kinds of network mode: | |
| Static IP | Network parameters must be entered manually and will not change. All parameters are provided by the ISP. Please contact ISP or network administrator for help if you do not know these information. |
| DHCP | Network parameters are provided automatically by a DHCP server. |
| PPPoE | Account and Password must be input manually. These are provided by your ISP. |
| Enable Vendor Identifier | When enabled, you will see the vendor identifier information in the DHCP option60 field |
| Vendor Identifier | Support for customization. When vendor identity is enabled, you will see the vendor identifier information in the DHCP option60 field |
| 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. |
| <p>Notice:</p> <p>1) After set the parameters, click 【Apply】 to make settings take effect.</p> <p>2) If you change the IP address, the current webpage will no longer respond, user should enter new IP address in URL to re-connect and re-login to the device's webpage.</p> | |

9.10 Network >> Service Port

This page provides settings for Web page login protocol, protocol port settings and RTP port.

Figure 20 - Service Port

Table 11 - Service port

| Parameter | Description |
|----------------------|---|
| Web Server Type | Reboot the device to make settings take effective. i10 series supports two kinds of web login: HTTP and HTTPS. |
| Web Logon Timeout | Default value is 15 minutes, when login time expires, web login will exit automatically, user need to login again. |
| Web auto login | If enable web auto login, after web login exits, refresh the webpage to login, user does not need to input username and password. |
| HTTP Port | The default value is 80. If you want more secure system management, you can set other value. Such as :8080, webpage login URL is: HTTP://ip:8080 |
| HTTPS Port | The default is 443, using method is similar to HTTP port. |
| RTP Port Range Start | The value range is 1025 to 65535. The value of RTP port starts from the initial value, each call, the value of voice and video port will added 2. |
| RTP Port Quantity | Number of calls. |

9.11 Network >> VPN

| File Type | File Name | File Size | |
|-----------------------------|-------------|-----------|----------------------|
| OpenVPN Configuration file: | client.ovpn | N/A | Select Upload Delete |
| CA Root Certification: | ca.crt | N/A | Select Upload Delete |
| Client Certification: | client.crt | N/A | Select Upload Delete |
| Client Key: | client.key | N/A | Select Upload Delete |

Figure 21 - VPN

Virtual Private Network (VPN) is a technology to allow the 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 activating 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 webpage.

■ L2TP

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

To establish a L2TP connection, the user should log in to the device webpage, go to page [Network] >> [VPN]. In VPN Mode, check the “Enable VPN” option and select “L2TP”, then fill in the L2TP server address, Authentication Username, and Authentication Password in the corresponding option. Press “Apply” to save changes and 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 option. 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 server automatically every time it boots up, unless user disable VPN. Sometimes, if the VPN connection does not establish immediately, user may try to reboot the device and check again.

■ OpenVPN

To establish an OpenVPN connection, user should get the following authentication and configuration files from the OpenVPN service 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

Select OpenVPN files and then click upload to upload these files to the device in the webpage [Network] >> [VPN]. 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 system boots up unless the user disable it manually.

9.12 Line >> SIP

Basic Settings >>

| | |
|--|--|
| Enable Auto Answering: <input checked="" type="checkbox"/> | Auto Answering Delay: 0 (0~120)second(s) |
| Enable Hotline: <input type="checkbox"/> | Hotline Number: |
| Hotline Delay: 0 (0~9)second(s) | DTMF SIP INFO Mode: Send 10/11 |
| Dial Without Registered: <input type="checkbox"/> | Use VPN: <input checked="" type="checkbox"/> |
| DTMF Type: AUTO | Signal Failback: <input type="checkbox"/> |
| Request With Port: <input checked="" type="checkbox"/> | Signal Retry Counts: 3 (1~10) |
| Use STUN: <input type="checkbox"/> | |
| Enable Failback: <input checked="" type="checkbox"/> | |
| Failback Interval: 1800 second(s) | |

| | |
|--|---|
| Use Feature Code: <input type="checkbox"/> | Disable Blocking Anonymous Call: |
| Enable Blocking Anonymous Call: | Call Waiting Off Code: |
| Call Waiting On Code: | Send Anonymous Off Code: |
| Send Anonymous On Code: | |
| SIP Encryption: <input type="checkbox"/> | RTP Encryption(SRTP): Disabled |
| Enable Session Timer: <input type="checkbox"/> | Session Timeout: 0 second(s) |
| Response Single Codec: <input type="checkbox"/> | BLF Server: |
| Keep Alive Type: UDP | Keep Alive Interval: 30 second(s) |
| Keep Authentication: <input type="checkbox"/> | Blocking Anonymous Call: <input type="checkbox"/> |
| User Agent: | Specific Server Type: COMMON |
| SIP Version: RFC3261 | Anonymous Call Standard: None |
| Local Port: 5060 | Ring Type: Default |
| Enable user=phone: <input type="checkbox"/> | Use Tel Call: <input type="checkbox"/> |
| Auto TCP: <input type="checkbox"/> | Enable PRACK: <input type="checkbox"/> |
| Enable Rport: <input checked="" type="checkbox"/> | |
| DNS Mode: A | Enable Long Contact: <input type="checkbox"/> |
| Enable Strict Proxy: <input checked="" type="checkbox"/> | Convert URI: <input checked="" type="checkbox"/> |
| Use Quote in Display Name: <input type="checkbox"/> | Enable GRUU: <input type="checkbox"/> |
| Sync Clock Time: <input type="checkbox"/> | Enable Use Inactive Hold: <input type="checkbox"/> |
| Caller ID Header: PAI-RPID-F | Use 182 Response for Call waiting: <input type="checkbox"/> |
| Enable Feature Sync: <input type="checkbox"/> | Enable SCA: <input type="checkbox"/> |
| CallPark Number: | Server Expire: <input checked="" type="checkbox"/> |
| TLS Version: TLS 1.0 | uaCSTA Number: |
| Enable Click To Talk: <input type="checkbox"/> | Enable ChangePort: <input type="checkbox"/> |
| Intercom Number: | Enable MAC Header: <input type="checkbox"/> |
| Unregister On Boot: <input type="checkbox"/> | Enable Deal 180: <input checked="" type="checkbox"/> |
| Enable Register MAC Header: <input type="checkbox"/> | |
| PTime(ms): Disabled | |

| | |
|---|--|
| Strict Branch: <input type="checkbox"/> | Enable Group: <input type="checkbox"/> |
| Enable RFC4475: <input checked="" type="checkbox"/> | Enable Strict UA Match: <input type="checkbox"/> |
| Registration Failure Retry Time: 32 second(s) | Local SIP Port: 5060 |
| Enable uaCSTA: <input type="checkbox"/> | |

Figure 22 - SIP

Table 111 - SIP

| Parameters | Description |
|-----------------------------|--|
| Register Settings | |
| Line Status | Display the current line status. To get the latest line status, user has to refresh the page manually. |
| Activate | Whether to activate the line or not. |
| Username | Enter the username of the service account. |
| Authentication User | Enter the authentication user name of the service account. |
| Display Name | Enter the display name which will be sent in a call request. |
| Authentication Password | Enter the authentication password of the service account. |
| Realm | Enter the SIP domain provided by the service provider. |
| Server Name | Input server name. |
| SIP Server 1 | |
| Server Address | Enter the IP or FQDN address of the SIP server |
| Server Port | Enter the SIP server port, default is 5060 |
| Transport Protocol | Set up the SIP transportation protocol: TCP or UDP or TLS. |
| Registration Expiration | Set SIP registration expiration time. |
| SIP Server 2 | |
| Server Address | Enter the IP or FQDN address of the SIP server |
| Server Port | Enter the SIP server port, default is 5060 |
| Transport Protocol | Set up the SIP transportation protocol: TCP or UDP or TLS. |
| Registration Expiration | Set SIP registration expiration time. |
| SIP Proxy Server Address | Enter the IP or FQDN address of the SIP proxy server. |
| Proxy Server Port | Enter the SIP proxy server port, default is 5060. |
| Proxy User | Enter the SIP proxy username. |
| Proxy Password | Enter the SIP proxy password. |
| Backup Proxy Server Address | Enter the IP or FQDN address of the backup proxy server. |
| Backup Proxy Server Port | Enter the backup proxy server port, default is 5060. |
| Basic Settings | |
| Enable Auto Answering | Enable auto-answering, the incoming calls will be answered automatically after the delay time. |
| Auto Answering Delay | Set the delay time for incoming call before the system automatically answers it. |
| Enable Hotline | Enable hotline configuration, the device will dial the specific number immediately once audio channel is opened. |
| Hotline Delay | Set the delay time for hotline before the call sends out. |
| Hotline Number | Set the hotline dialing number |

| | |
|---------------------------------|--|
| Dial Without Registered | Enable call out without registration. |
| DTMF Type | Set the DTMF type for the line |
| DTMF SIP INFO Mode | Set the SIP INFO mode to send '*' and '#' or '10' and '11' |
| Use VPN | Set the line to use VPN restrict route |
| Use STUN | Set the line to use STUN for NAT traversal |
| Enable Failback | Whether to switch to the primary server when it is available. |
| Failback Interval | The time interval of detecting the availability of the main Proxy using Register message. |
| Signal Failback | When there are multiple proxy, whether to allow the invite/register request to execute failback or not. |
| Signal Retry Counts | When there are multiple proxy, the attempt times that the SIP Request considers proxy is unavailable. |
| Codecs Settings | Set the priority and availability of the codecs by adding or removing them from the list. |
| Advanced Settings | |
| Use Feature Code | When this setting is enabled, the features in this section will not be handled by the device itself but by the server instead. In order to control the device, the device will send feature code to the server by dialing the number specified in each feature code field. |
| Enable Blocking Anonymous Call | Set the feature code to dial to the server. |
| Disable Blocking Anonymous Call | Set the feature code to dial to the server. |
| Call Waiting On Code | Set the feature code to dial to the server. |
| Call Waiting Off Code | Set the feature code to dial to the server. |
| Send Anonymous On Code | Set the feature code to dial to the server. |
| Send Anonymous Off Code | Set the feature code to dial to the server |
| SIP Encryption | Enable SIP encryption, and SIP transmission will be encrypted. |
| RTP Encryption | Enable RTP encryption, and RTP transmission will be encrypted. |
| Enable Session Timer | Set the line to enable call ending by session timer refreshment. The call session will be ended if there is no new session timer event update received after the timeout period. |
| Session Timeout | Set the session timer timeout period. |
| Response Single Codec | If enable this option, the device will use single codec to respond to incoming call request. |
| BLF Server | Input BLF server address. Ordinary BLF application is that device sends subscription message to SIP server. If your SIP server does not support subscription, please input BLF server address to |

| | |
|-----------------------------------|---|
| | separate SIP registration server and BLF server. |
| Keep Alive Type | Set the line to use dummy UDP or SIP OPTION packet to keep NAT opened. |
| Keep Alive Interval | Set the keep alive packet transmitting interval. |
| Keep Authentication | Keep the previous authentication parameters. |
| Blocking Anonymous Call | Reject any incoming call without presenting caller ID. |
| User Agent | Set the user agent, the default value is device model with software version. |
| Specific Server Type | Set the line to collaborate with specific server type. |
| SIP Version | Set the SIP version. |
| Anonymous Call Standard | Set the standard for anonymous call. |
| Local Port | Set the local port. |
| Ring Type | Set the ring tone type for the line. |
| Enable user=phone | In SIP invite message, there is user=phone field. |
| Use Tel Call | Enable or disable use tel call. |
| Auto TCP | Using TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes. |
| Enable Rport | Set the line to add Rport in SIP headers. |
| Enable PRACK | Set the line to support PRACK SIP message. |
| DNS Mode | Select DNS mode, options are A, SRV and NAPTR. |
| Enable Long Contact | Enable this will allow more parameters in contact field per RFC 3840. This option should work together with SEM server. |
| Enable Strict Proxy | This is used for matching special server. When the i10 series receives packets from the server, it will reply with the source IP address, not the address in via field. |
| Convert URI | Whether to enable convert URI or not. |
| Use Quote in Display Name | Whether to add quote in display name, i.e. "Fanvil" vs Fanvil. |
| Enable GRUU | Enable Globally Routable User-Agent URI (GRUU) or not. |
| Sync Clock Time | Time Sync with server. |
| Enable Inactive Hold | With inactive hold enabled, you can see SDP is inactive in the SDP packet. |
| Caller ID Header | Set the Caller ID Header. |
| Use 182 Response for Call waiting | Set the device to use 182 response code at call waiting. |
| Enable Feature Sync | Enable or disable Feature Sync with server. |
| Enable SCA | Enable/Disable SCA (Shared Call Appearance) |
| CallPark Number | Set the CallPark number. |

| | |
|---------------------------------|---|
| Server Expire | Set the timeout of using the server. |
| TLS Version | Choose TLS Version. |
| uaCSTA Number | Set uaCSTA Number. |
| Enable Click To Talk | This is used to match special server, click to call out directly after enable this option. |
| Enable Change port | Whether to enable change port or not. |
| Intercom Number | Set intercom number. |
| Unregister On Boot | Whether to enable logout function. |
| Enable MAC Header | Whether to enable MAC header. When enable, there is MAC information in SIP packet and user agent when register |
| BLF Dialog Strict Match | Whether to enable accurate matching of BLF sessions. |
| PTime(ms) | Set whether to bring ptime field, by default it is no. |
| Enable Deal 180 | Enable: after receives 183+ SDP, device will play ivr; and after receives 180, device will play local tone. Disable: after receives 183+ SDP, device will play ivr. After receives 180, device does not play local tone. |
| SIP Global Settings | |
| Strict Branch | Enable or disable this to strictly match the Branch field. |
| Enable Group | Enable or disable SIP group server function as server backup. |
| Enable RFC4475 | Enable or disable RFC4475. |
| Enable Strict UA Match | Enable strict UA matching. |
| Registration Failure Retry Time | Set the registration failure retry time. |
| Local SIP Port | Modify the device SIP port. |
| Enable uaCSTA | Set to enable the uaCSTA function. |

9.13 Line >> SIP Hotspot

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

Please check [8.3 Hotspot](#) for more details.

9.14 Line >> Basic Settings

STUN -Simple Traversal of UDP through NAT -A STUN server allows the device in a private network to know its public IP and port as well as the type of NAT being used. The equipment can use this information to register itself to a SIP server so that it can receive calls from public

network while it is in a private network.

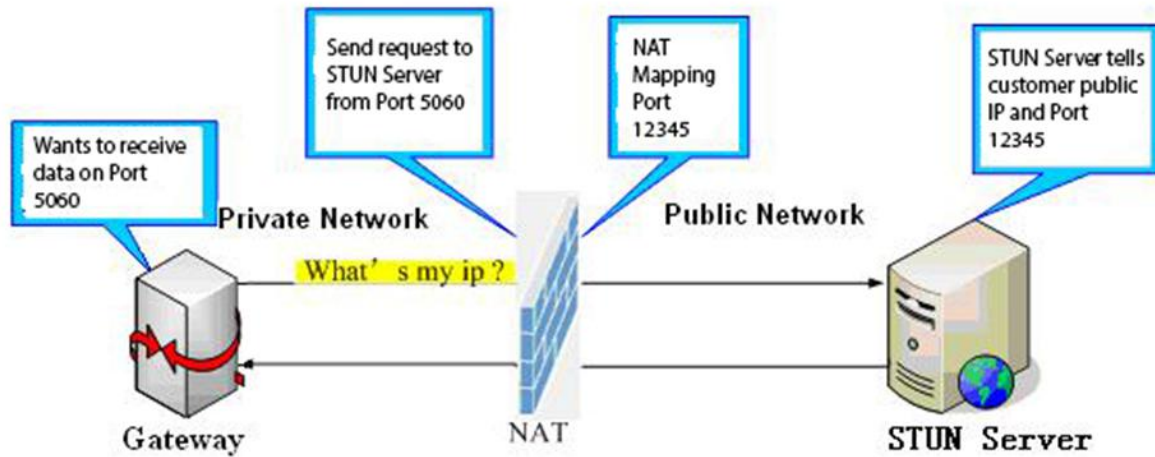


Figure 23 - Network Basic

SIP
SIP Hotspot
Basic Settings

STUN Settings

STUN NAT Traversal: FALSE

Server Address:

Server Port:

Binding Period: second(s)

SIP Waiting Time: millisecond

SIP P2P Settings

Enable Auto Answering:

Auto Answering Delay: (0~120)second(s)

DTMF Type:

DTMF SIP INFO Mode:

Figure 24 - Line Basic Setting

Table 12 - Line Basic Setting

| Parameters | Description |
|----------------------|-------------|
| STUN Settings | |

| | |
|-------------------------|---|
| Server Address | Input the STUN server address. |
| Server Port | Input the STUN server port, default is 3478. |
| Binding Period | Set the STUN binding period which can be used to keep the NAT open. |
| SIP Waiting Time | Set the timeout of STUN binding before sending SIP messages. |
| SIP P2P Settings | |
| Enable Auto Answering | Enable timeout to automatically answer IP calls |
| Auto Answering Delay | Automatic answer timeout setting |
| DTMF Type | Set the DTMF type of the line. |
| DTMF SIP INFO Mode | Set up SIP INFO mode to send '*' and '#' or '10' and '11' |

9.15 Intercom Setting >> Features

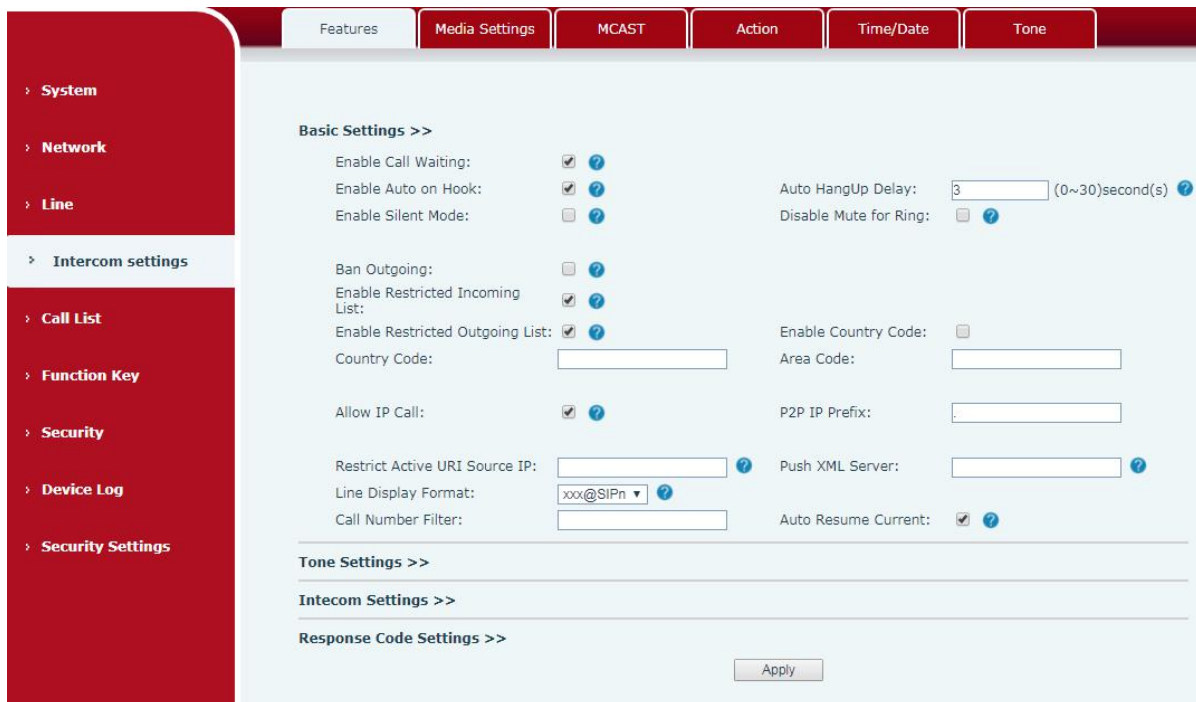


Figure 25 - Intercom Setting

Table 13 - Intercom Setting

| Parameters | Description |
|-----------------------|--|
| Basic Settings | |
| Enable Call Waiting | Enable this setting to allow user to take second incoming call during an established call. By default it is enabled. |
| Enable Auto Onhook | Enable auto onhook or not. If enable, the device will hang up the call and return to the idle status automatically. |

| | |
|---------------------------------|---|
| Auto Onhook Time | Specify Auto Onhook time, the device will hang up and return to the idle automatically after Auto onhook time. |
| Enable Silent Mode | When enabled, the device is muted, there is no ringing when calls, you can use the volume keys and mute key to unmute. |
| Disable Mute for Ring | Disable the mute mode, if this option is clicked, mute button on device does not take effect. |
| Ban Outgoing | Enable or disable ban outgoing, if enable, the device can not dial out any number. |
| Enable Restricted Incoming List | Whether to enable restricted incoming call list. |
| Enable Restricted Outgoing List | Whether to enable the restricted outgoing list. |
| Enable Country Code | Whether to enable the country code. |
| Country Code | Fill in the country code. |
| Area Code | Fill in the area code. |
| Allow IP Call | If enabled, user can dial out with IP address. |
| P2P IP Prefix | Set prefix for point-to-point IP calls. |
| Restrict Active URI Source IP | Set the device to accept Active URI command from specific IP address. Notice: this function is usually used to manage device. |
| Push XML Server | Configure the Push XML Server, when phone receives request, it will determine whether to display corresponding content on the phone which sent by the specified server. |
| Line Display Format | Custom line format: SIPn or SIPn:xxx or xxx@SIPn |
| Call Number Filter | Configure a special ampersand, the called number is 78-9, the ampersand will be filtered when device sends the call out. |
| Auto Resume Current | Automatically break HOLD if current call changes. |
| Tone Settings | |
| Enable Holding Tone | Whether to enable call holding tone. |
| Enable Call Waiting Tone | Whether to enable call waiting tone. |
| Play Dialing DTMF Tone | Play DTMF tone on the device when user presses a digits when dial the call, by default it is enabled. |
| Play Talking DTMF Tone | Play DTMF tone on the device when user presses a phone digits during taking, by default it is enabled. |
| Intercom Settings | |
| Enable Intercom | When intercom is enabled, the device will accept the incoming call which requests with a SIP header of Alert-Info automatically. |
| Enable Intercom Mute | Enable mute mode during the intercom call. |
| Enable Intercom Tone | If the incoming call is intercom call, the device plays the intercom |

| | |
|-------------------------------|--|
| | tone. |
| Enable Intercom Barge | While enable intercom barge, the device will auto answer the intercom call during a call. If the current call is intercom call, the device will reject the second intercom call. |
| Response Code Settings | |
| Busy Response Code | Set the SIP response code when line is busy. |
| Reject Response Code | Set the SIP response code when device reject one call. |

9.16 Intercom Setting >> Audio

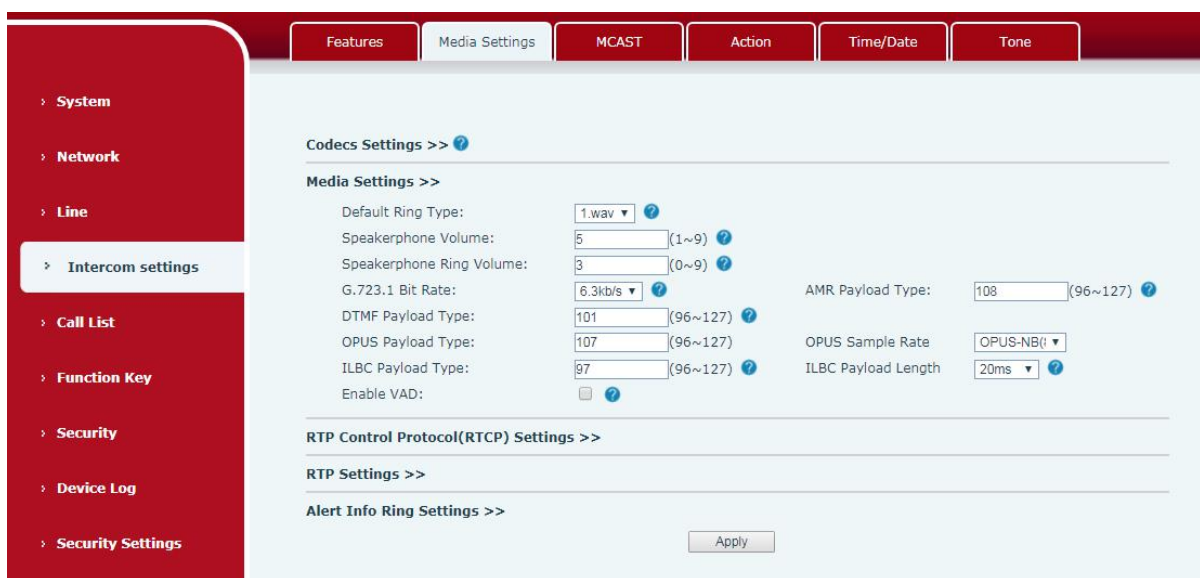


Figure 26 - Media Setting

Table 14 - Media Setting

| Parameter | Description |
|--------------------------|--|
| Codecs Settings | Select enable or disable voice codecs: G.711A/U, G.722, G.729AB, iLBC, opus. |
| Media Settings | |
| Default Ring Type | Configure default ringtones. If no special ringtone is set, the default ringtone will be used. |
| Speakerphone Volume | Set the speaker volume, value can be 1~9. |
| Speakerphone Ring Volume | Set the speaker ring volume, value can be 1~9. |
| G.723.1 Bit Rate | 5.3kb/s or 6.3kb/s is available. |
| DTMF Payload Type | Enter the DTMF payload type, the value must be 96~127. |
| AMR Payload Type | Set AMR load type, range is 96~127. |
| Opus payload type | Set Opus load type, range is 96~127. |

| | |
|--|---|
| OPUS Sample Rate | Set Opus sampling rate, including opus-nb (8KHz) and opus-wb (16KHz). |
| ILBC Payload Type | Set the ILBC Payload Type, the value must be 96~127. |
| ILBC Payload Length | Set the ILBC Payload Length. |
| Enable VAD | Whether to enable voice activity detection. |
| RTP Control Protocol(RTCP) Settings | |
| CNAME user | Set CNAME user |
| CNAME host | Set CNAME host |
| RTP Settings | |
| RTP keep alive | Hold the call and send the packet every 30s. |
| Alert Info Ring Settings | |
| Value | Set the value to specify the ring type. |
| Ring Type | Select ring type. |

9.17 Intercom Setting >> MCAST

It is easy and convenient to use multicast function to send notice to each member of the multicast group 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, the device will receive multicast from the configured monitoring multicast address.

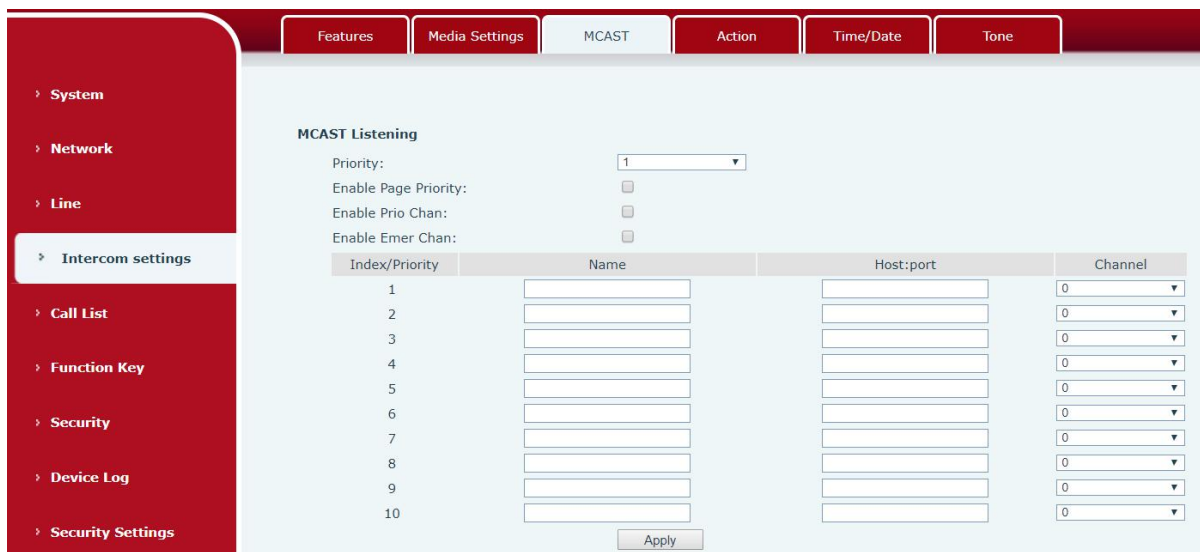


Figure 27 - MCAST

9.18 Intercom Setting >> Action

Action URL Event Settings

Set URL for the device to report its action to server. These actions are recorded and sent as xml files to the server. Sample format is `http://InternalServer /FileName.xml`.

(Internal Server: The IP address of server; File Name: the device's xml file used to report action.)

Table 15 - action URL

Notice: 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/20190122/5c46debfbd37.pdf>

9.19 Intercom Setting >> Time/Date

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

Figure 28 - time/date

Table 16 - time/date

| Parameter | Description |
|-------------------------------------|---|
| Network Time Server Settings | |
| Time Synchronized via SNTP | Enable time-sync through SNTP protocol. |
| Time Synchronized via DHCP | Enable time-sync through DHCP protocol. |
| Time Synchronized via | Enable time-sync through DHCPv6 protocol. |

| | |
|--------------------------------------|---|
| DHCPv6 | |
| 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 interval of re-synchronization with time server |
| Time/Date Format | |
| 12-hour clock | Enable or disable 12-hour clock. |
| Time/Date Format | Set time/date format. |
| Daylight Saving Time Settings | |
| Location | Select the user's time zone specific area |
| DST Set Type | Select DST type, and set the DST rules. |
| Fixed Type | Select DST fixed type. |
| 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 time manually, please disable SNTP service first. |

9.20 Intercom settings >> Tone

User can set device's tone in this page.

You can select the corresponding country and use the settings directly, or select custom and set the tone manually.

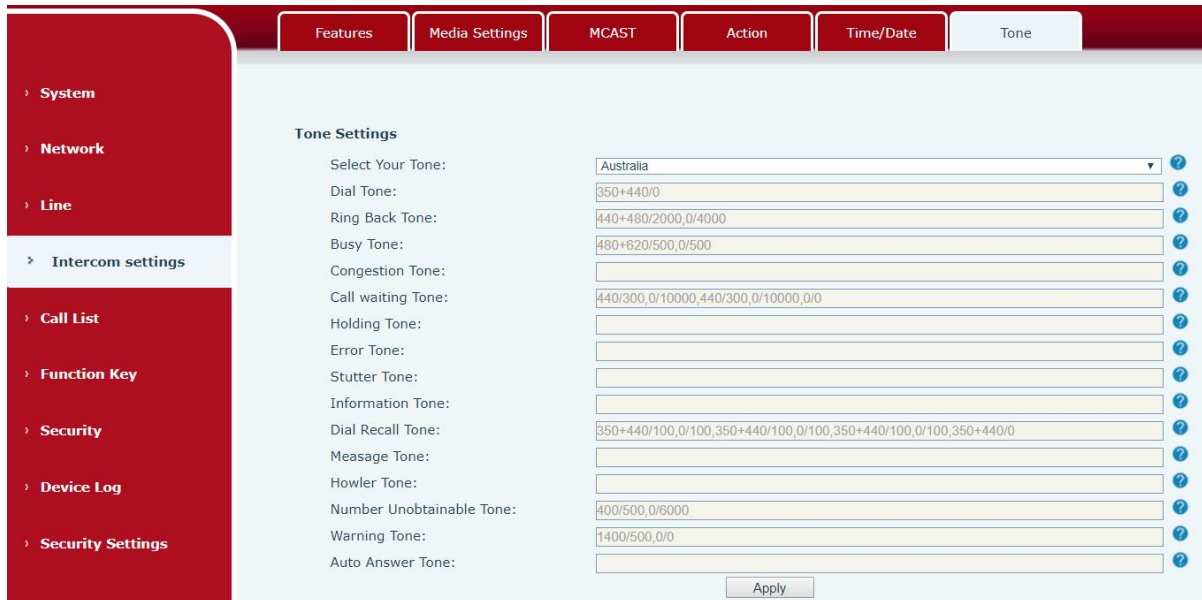


Figure 29 - Tone

9.21 Call List >> Call List

User can set restricted incoming calls list and restricted outgoing calls list in this page.

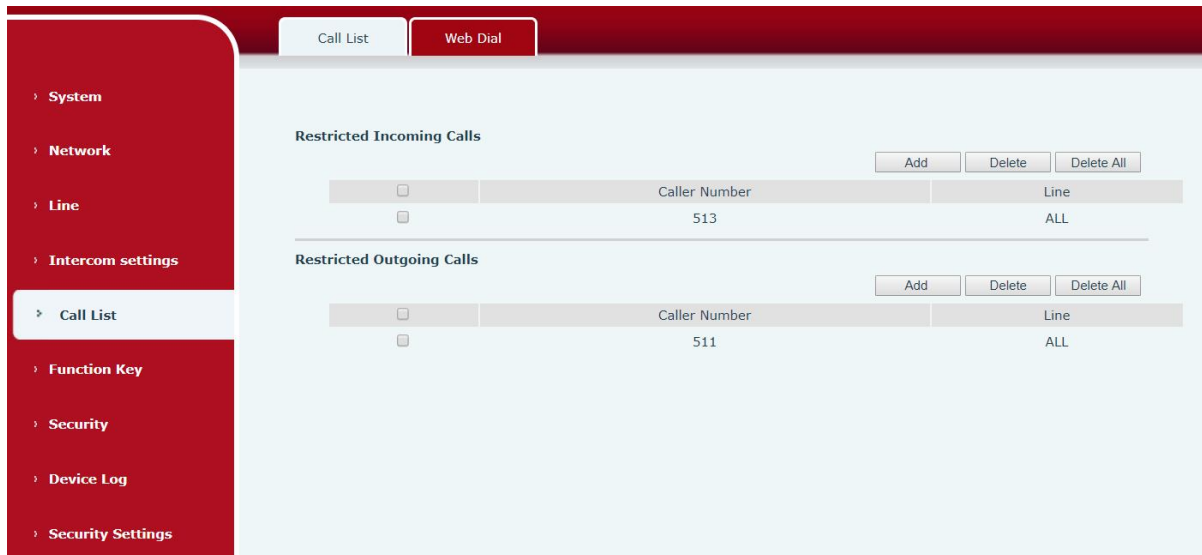


Figure 30 - Call List

■ Restricted Incoming Calls:

The function is same with blacklist. Add the numbers in restricted incoming calls list, the device will reject all the calls from these blacklist numbers, unless user deletes the numbers from the list.

User can add both numbers and prefix in the restricted incoming calls list, the i10 series device will reject all the calls from the blacklist numbers or calls from numbers with blacklist prefix.

■ Restricted Outgoing Calls:

Add numbers to restricted outgoing calls list, the i10 series device will end the calling when user dial these numbers, unless user removes the numbers from the list.

9.22 Web Dial

In this page, user can make calls, answer the calls or hang up the calls.

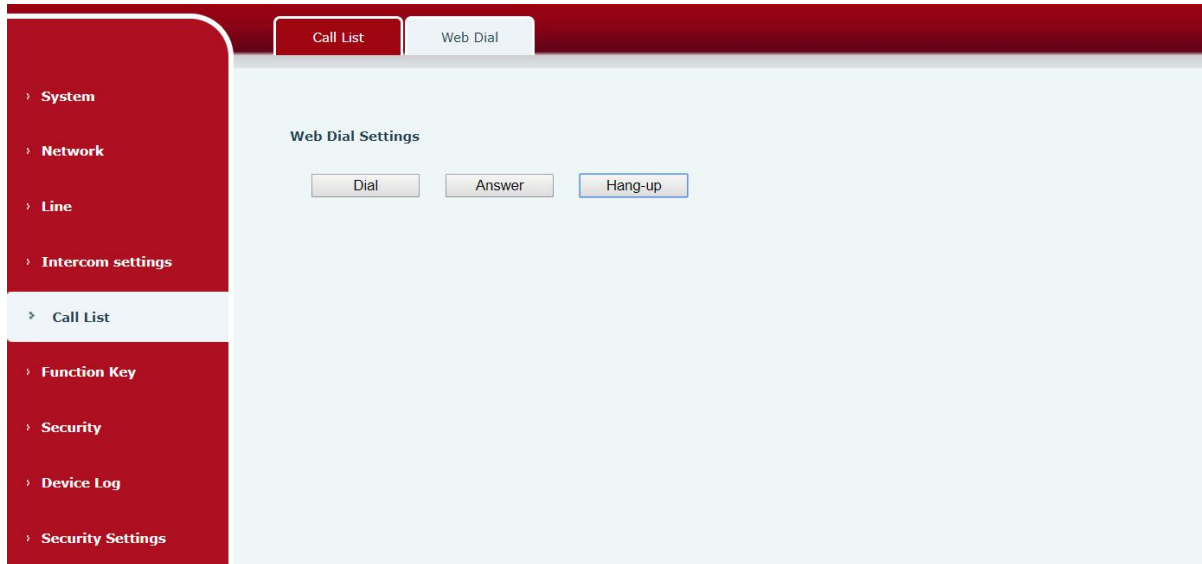
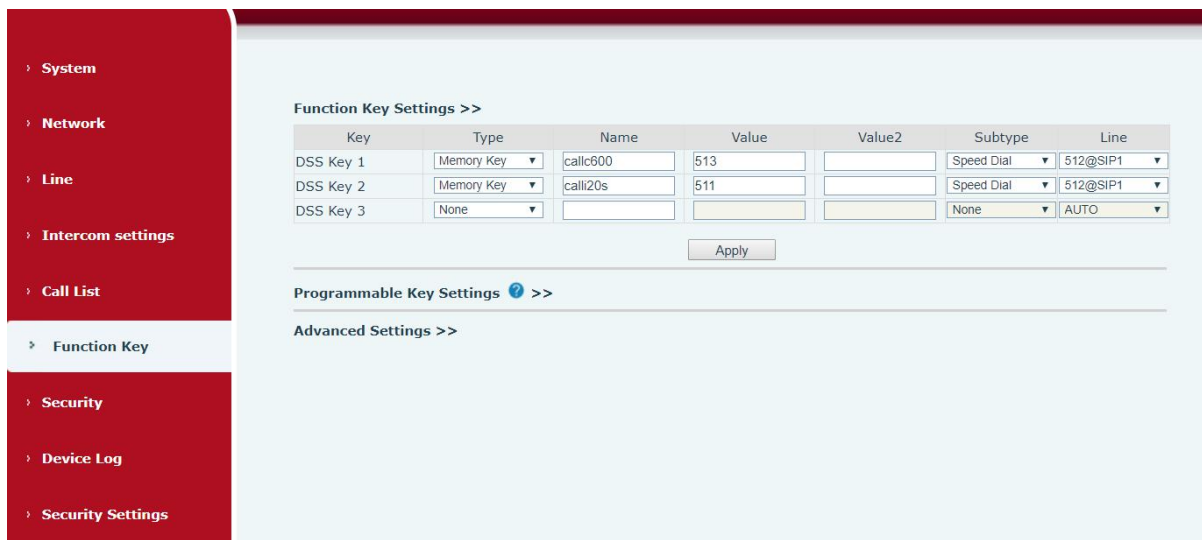


Figure 31 - Web Dial

9.23 Function Key



Advanced Settings >>

Dial Mode Select

Call Switched Time (5~50)second(s)

First Number Start Time (00:00~23:59) First Number End Time (00:00~23:59)

Apply

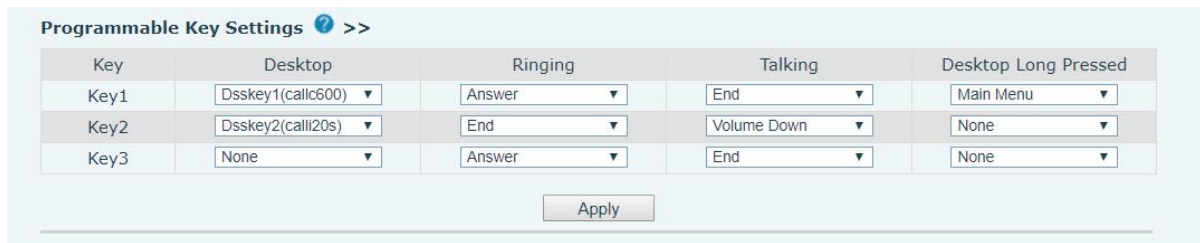


Figure 32 - Function Key

Table 17 - Function Key

| Parameters | Description |
|----------------------------------|--|
| Function Key Settings | |
| Memory Key | Speed dial: User can set one number or IP address in Value option. It is convenient to use this function to make calls to specified numbers/IP address used continually. Intercom: The intercom function make the operator or secretary to answer calls directly, which is popular in office. |
| Key Event | Use key event function to activate one application directly. Example: None/Handfree. |
| DTMF | Send the DTMF directly with the corresponding settings. |
| MCAST Paging | Set paging IP address and voice codec, user can initiate paging directly by pressing the button. |
| Action URL | User can use specified URL to make calls or open the doors. |
| MCAST Listening | When device is idle, use the MCAST listening key to monitor the MCAST from the paging IP address user set. |
| Programmable Key Settings | |
| Desktop | None: None. Dsskey1: Call out or pick up calls according to dsskey1's settings. Dsskey2: Call out or pick up calls according to dsskey2's settings. Dsskey3: Call out or pick up calls according to dsskey3's settings. |
| Ringing | Answer: When there is one incoming call and auto answer is disabled, use this key to pick up the call. End: When there is one incoming call, use this key to end the call. |
| Talking | End: Press the key to end the call when device is in one call. Volume Up: Press the key to increase volume when the device is in one call. Volume Down: Press the key to decrease volume when the device is in one call. Dsskey1: Call out or pick up calls according to dsskey1's settings. Dsskey2: Call out or pick up calls according to dsskey2's settings. |

| | |
|-------------------------|--|
| | Dsskey3: Call out or pick up calls according to dsskey3's settings. |
| Desktop Long pressed | None: None. Main Menu: Long press the key to make device go to command mode, details please check chapter 5.2.1 Common command mode . |
| Advanced Settings | |
| Dial Mode Select | Set the dial mode between calling 1 st number and calling 2 nd number. Main-Secondary: If the 1 st number does not pick up the call in specified time, then the device will call 2 nd number. Time Period: Device check the system time and send the call to 1 st number in 1 st number's time period, or the device will send call to the 2 nd number. |
| Call Switched Time | Set the switched time between 1 st number and 2 nd number when device calls out, by default the value is 16 seconds. |
| First Number Start Time | Set 1 st called number's start time, by default it is 06:00am. |
| First Number End Time | Set 1 st called number's end time, by default it is 18:00pm. |

➤ **Key Event**

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

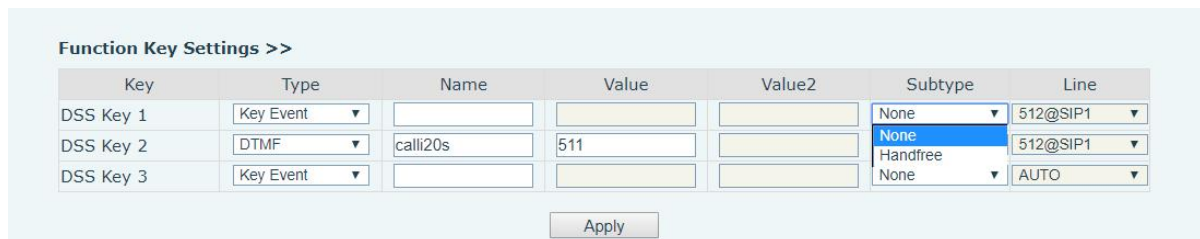


Figure 33 - Function Key Settings

Table 18 - Function Key Settings

| Type | Subtype | Usage |
|-----------|----------|---------------|
| Key Event | None | No responding |
| | Handfree | Handfree |

➤ **Memory Key**

When the speed dial key set as Memory 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.

Function Key Settings >>

| Key | Type | Name | Value | Value2 | Subtype | Line |
|-----------|------------|----------|-------|---------------|------------|----------|
| DSS Key 1 | Memory Key | callc600 | 513 | 172.18.60.142 | Speed Dial | 512@SIP1 |
| DSS Key 2 | Memory Key | calli20s | 511 | | NONE | 512@SIP1 |
| DSS Key 3 | Key Event | | | | Intercom | AUTO |

Apply

Figure 34 - Memory Key Settings

Table 19 - Memory Key Settings

| Type | Number | Line | Subtype | Usage |
|---------|---|-------------------------------------|------------|--|
| Hot Key | Fill the called party's SIP account or IP address | The SIP account corresponding lines | Speed Dial | Set speed dial, press the key to call out the number. |
| | | | 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:

Function Key Settings >>

| Key | Type | Name | Value | Value2 | Subtype | Line |
|-----------|--------------|----------|----------------|---------------|------------|----------|
| DSS Key 1 | Memory Key | callc600 | 513 | 172.18.60.142 | Speed Dial | 512@SIP1 |
| DSS Key 2 | MCAST Paging | calli20s | 224.0.0.5:3356 | | G.711U | 512@SIP1 |
| DSS Key 3 | Key Event | | | | G.711U | AUTO |

Apply

Figure 35 - Multicast Settings

Table 20 - Multicast Settings

| Type | Number | Subtype |
|-----------|--|---|
| Multicast | Set the host IP address and port number, they must be separated by a colon (The IP address range is 224.0.0.0 to 239.255.255.255, and the port number is preferably set between 1024 and 65535). | G.711U G.711A G729AB iLBC opus G.722 |

9.24 Security >> Web Filter

In this page, user can set the IP address segment which is allowed to access the device.

Figure 36 - Multicast Settings

Add or delete the allowed IP address segment. Please input start IP address in Start IP address option, and input end IP address in End IP address option and click Apply to save the settings.

Click Delete to remove the corresponding IP address segment.

Enable Web Filter: Enable or disable web filter, select it and click apply to save the settings.

Notice: Please remove your PC's IP address from the filter IP address list, or your PC is not able to access the device's webpage.

9.25 Security >> Trusted Certificates

User can upload or delete the trusted certificates in this page.

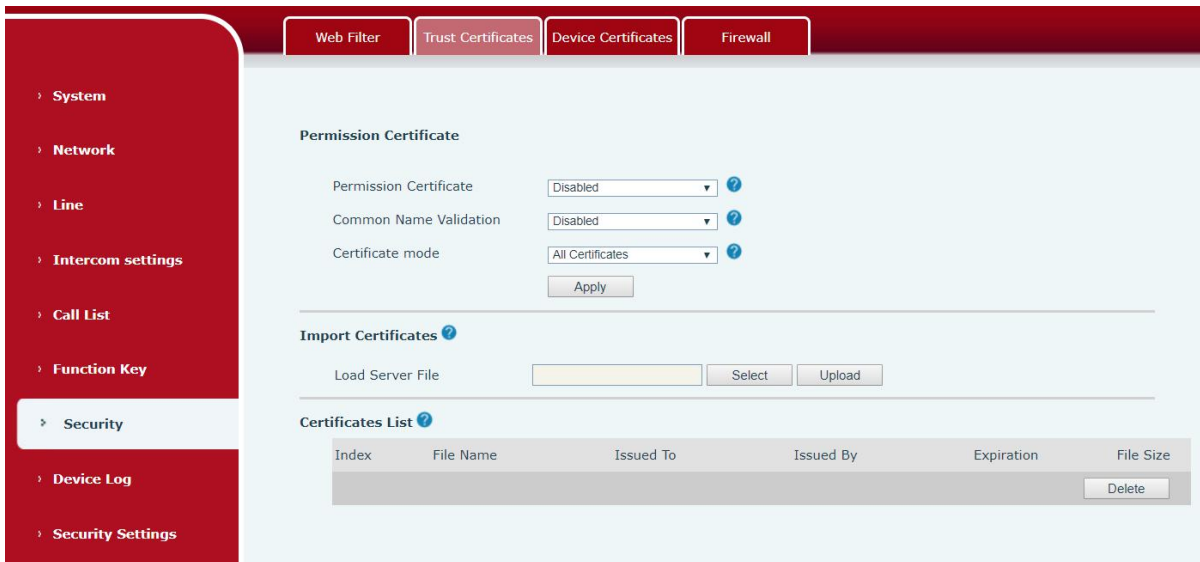


Figure 37 - Trusted Certificates

9.26 Security >> Device Certificates

Select the device certificate to use default certificates or custom certificate.

You can upload and delete uploaded certificates.

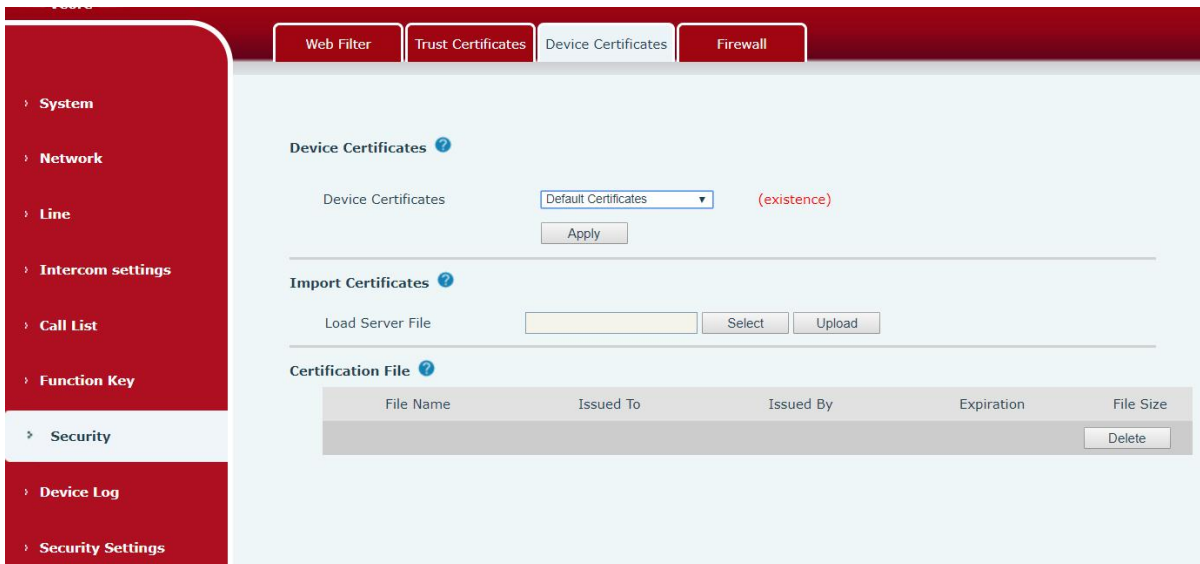


Figure 38 - Device Certificates

9.27 Security >> Firewall

Figure 39 - Firewall

In this page, user can select whether to enable input or output firewall, and set the detailed rules. These settings are used to prevent illegal network access, limit the internal user to access Internet sources, enhance the security.

Table 21 - Firewall

| Parameters | Description |
|----------------------|---|
| Firewall Type | |
| Enable Input Rules | Enable or disable input rules. |
| Enable Output Rules | Enable or disable output rules. |
| Input/Output | Set the rule to be input rule or output rule. |
| Deny/Permit | Set the rule to be denying rule or permitting rule. |
| Protocol | Select the firewall protocol, options are UDP, TCP and ICMP. |
| Src Address | Input source address. The source IP can be one host address or network address, you can input 0.0.0.0 to represent all the IP addresses, or input one *.*.*.0 network IP, like 192.168.1.0. |
| Src Mask | Input source mask. If user configure source mask to be 255.255.255.255, the source IP should be one detailed IP address; if user configure source mask to be 255.255.255.0, the source IP contains a segment of IP addresses. |
| Src Port Range | Input source port range. |
| Dst Address | Input destination address. The destination IP can be one specified IP |

| | |
|----------------|---|
| | address, or 0.0.0.0 which represents all the IP addresses, or network IP address *.*.*.0, like 192.168.1.0. |
| Dst Mask | Input destination mask. If user configure destination mask to be 255.255.255.255, the destination IP should be one detailed IP address; if user configure source mask to be 255.255.255.0, the destination IP contains a segment of IP addresses. |
| Dst Port Range | Input destination port range. |

Input the parameters and click Add, the new rules will be added to the firewall list, for example:

| Index | Deny/Permit | Protocol | Src Address | Src Mask | Src Port Range | Dst Address | Dst Mask | Dst Port Range |
|-------|-------------|----------|--------------|---------------|----------------|---------------|---------------|----------------|
| 1 | deny | icmp | 192.168.1.14 | 255.255.255.0 | 1-1023 | 192.168.1.118 | 255.255.255.0 | 2-1024 |

Select Input/Output rule, and enter the index of the rule in Index to Be deleted option, click delete then the corresponding rule will be removed.

| | | | | |
|--------------|-------|---------------------|---|--------|
| Input/Output | Input | Index To Be Deleted | 1 | Delete |
|--------------|-------|---------------------|---|--------|

9.28 Device Log

In this page, user can get the device's logs. When device works abnormally, user can get the logs and send to Fanvil support team. Details please check chapter [10.5 Get Log Information](#).

9.29 Security Settings

The screenshot shows the 'Security Settings' page. On the left is a red sidebar with a navigation menu containing: System, Network, Line, Intercom settings, Call List, Function Key, Security, Device Log, and Security Settings (highlighted). The main content area is titled 'Basic Settings' and includes:

- Ringtone Duration: 5 (1~600)s
- Input & Tamper Server Address: [Empty field]
- Message: Alarm_Info:Description=;SIP User=512;Mac=0c:38:3e:3a:06:65;IP=172.18.60.192;port=Input
- An 'Apply' button.

 Below this is the 'Input Settings >>' section:

- Input1: [Checked]
- Triggered By: Low Level Trigger(Close Trigger)
- Triggered Action: Send SMS, Dss Key: [None]
- Triggered Ringtone: 2.wav
- An 'Apply' button.

 At the bottom are 'Output Settings >>' and 'Tamper Alarm Settings >>' sections.

Output Settings >>

Triggered By DTMF RingTone:

Triggered By URI Ringtone:

Triggered By SMS Ringtone:

Triggered By Dsskey Ringtone:

Output1:

Standard Status:

Output Duration: (1~600)s

Output Trigger Mode: Trigger By DTMF

DTMF Trigger Code:

DTMF Reset Code:

Reset By:

Trigger By Active URI

Trigger Message:

Reset Message:

Trigger By SMS

Trigger Message:

Reset Message:

Trigger By Input: Input1

Trigger By Call State: Talking Ringing Calling

Trigger By DssKey:

Tamper Alarm Settings >>

Enable Tamper Alarm

Alarm command:

Reset command:

Alarm Ringtone:

Figure 40 - Security Settings

Table 22 - Security Settings

| Security Settings | |
|-------------------------------|---|
| Parameters | Description |
| Basic Settings | |
| Ringtone Duration | Set the ringtone duration, default value is 5 seconds. |
| Input & Tamper Server Address | Set remote server address. The device will send message to the server when the alarm is triggered. The message format is : Alarm_Info:Description=i10;SIP User=;Mac=0c:38:3e:3a:06:65;IP=; port=Input . |
| Input settings | |
| Input Detect | Enable or disable Input Detect |
| Triggered by | When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger. |
| | When choosing the high level trigger (disconnect trigger), detect the input port (high level) disconnected trigger. |
| Triggered Action | <p>Send SMS: Set the alert message send to server if selected.</p> <p>Dss Key: The device will perform corresponding Dss Key configurations if any key is selected, by default the value is none.</p> <p>Triggered Ringtone: Select triggered ring tone.</p> |

| Output Settings | |
|------------------------------|--|
| Output Response | Enable or disable Output Response |
| Triggered by DTMF Ring tone | Select the DTMF trigger ring tone. |
| Triggered by URI Ringtone | Select the URI trigger ring tone. |
| Triggered By SMS Ringtone | Select the SMS trigger ring tone. |
| Triggered By Dsskey Ringtone | Select the Dsskey trigger ring tone. |
| Standard Status | When choosing the low level trigger (NO: normally open), when meet the trigger condition, trigger the NO port disconnected. |
| | When choosing the high level trigger (NC: normally close), when meet the trigger condition, trigger the NC port close. |
| Output Duration | Set the output change duration time, the default is 5 seconds. |
| Trigger by DTMF | Enable or disable trigger by DTMF. The device will check the received DTMF sent by remote device, if it matches the DTMF trigger code, the device will trigger corresponding output port. |
| DTMF Trigger Code | Input the DTMF trigger code, default value is 1234. |
| DTMF Reset Code | Input the DTMF reset code, default value is 4321. |
| Reset By | Reset the output port mode by duration or state. By duration: Reset the output port status when output duration occurs. By state: Reset the output port status when device's call state changes. |
| Trigger by URI | Enable or disable trigger by URI. User can send commands from remote device or server to i10 series device, if the command is correct, then device will trigger corresponding output port. |
| Trigger Message | Input trigger message for trigger by URI mode. |
| Rest Message | Input reset message for trigger by URI mode. |
| Trigger by SMS | Enable or disable trigger by SMS. User can send ALERT command to i10 series device, if the command is correct, then device will trigger corresponding output port. |
| Trigger SMS | Input trigger message for trigger by SMS mode. |
| Reset SMS | Input reset message for trigger by SMS mode. |
| Trigger by Input | Select the input port, when the input port meets the trigger condition, the output port will be triggered (The Port level time change, By < Output Duration > control) |

| | |
|------------------------------|--|
| <p>Trigger By Call state</p> | <p>Select call state to trigger the output port, options are:</p> <p>Talking: When the device's talking status changes, trigger the output port.</p> <p>Ringing: When the device's ringing status changes, trigger the output port.</p> <p>Calling: When the device's calling status changes, trigger the output port.</p> |
| <p>Trigger By DssKey</p> | <p>Enable or disable trigger by dsskey. If any of the dsskey is selected, when the dsskey application performs, the output port will be triggered.</p> |

10 Trouble Shooting

When the device doesn't work properly, user 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

User can obtain information through the **[System]** >> **[Information]** option on device's webpage. The following information will be provided:

Device information (model, software and hardware version), network Information and SIP Accounts Information etc.

10.2 Reboot device

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

When the device has problems and user can't access the web page, you can disassemble the surface shell and press the "RESET" button. The device will restart and the configuration will not change.

10.3 Device factory reset

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

To restore the factory settings, please go to **[System]** >> **[Configuration]** >> **[Reset Phone]** page, and click **[Reset]** button, the device will return to the factory default state.

10.4 Network Packets Capture

Sometimes, when the device has problems, the data packet is very helpful. In order to obtain the data packet of the device, please log in the device's webpage, and go to **[System]** >> **[Tools]** page, and click the **[Start]** option in the "Web Capture". A message will inform user that capturing starts and at this time, user can perform related operations, such as starting/deactivating the line or making a call, please click the **[Stop]** button on the webpage after complete. Network packets are saved in a file, users can analyze the packet or send it to Fanvil Technical Support team.

10.5 Get Log Information

Log information is helpful when encountering an abnormal problem. In order to get the log, the user can login device's webpage, and go to page **[Device Log]**, click the **[Start]** option, and perform device until the problem appears, click **[Save]** to save the logs to local PC, user can analyze the logs or send the log file to the technician to check the problem.

10.6 Common Trouble Cases

Table 23 - Common Trouble Cases

| Trouble Case | Solution |
|---|--|
| Device could not boot up | <ol style="list-style-type: none"> 1. Please check device's power connection and confirm the power adapter or PoE switch is in Fanvil list. 2. If the device go to "POST mode" (the LED flashes slowly), it means the device system is damaged. Please contact Fanvil technical support to help you restore. |
| Device could not register to a service provider | <ol style="list-style-type: none"> 1. Please check network cable connection and confirm the device is connected to Internet well. 2. If the network connection is good, please check your SIP line configuration again. If all configurations are correct, please contact your service provider for support, or obtain a registration network packet according to the instructions in "10.4 Network Data Capture", and send the packet to Fanvil support team to help analyze the issue. |