User Manual

W712

Software Version: 2.12.0

Release Date：2023/2/3

Directory

1 Picture

2 Table

3 Safety Instruction

3.1 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 device and affect the behavior or induce noise.
- Before using the external power supply in the package, please check the home power voltage. Inaccurate power voltage may cause fire and damage.
- Please do not damage the power cord. If power cord or plug is impaired, do not use it because it may cause fire or electric shock.
- Do not drop, knock or shake the device. Rough handling can break internal circuit boards.
- This device 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.
- Avoid exposure the device to high temperature or below 0℃ or high humidity.
- Avoid wetting the unit with any liquid.
- Do not attempt to open it. Non-expert handling of the device could damage it. Consult your authorized dealer for help, or else it may cause fire, electric shock and breakdown.
- Do not use harsh chemicals, cleaning solvents, or strong detergents to clean it. Wipe it with a soft cloth that has been slightly dampened in a mild soap and water solution.
- When lightning, do not touch power plug, it may cause an electric shock.
- Do not install this device 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.

3.2 Precautions

The equipment supports one digital channel or analog channel, but cannot be mixed. When the gateway is set as a digital channel, please use the digital radios to call. When the gateway is set as an analog channel, please use the analog radios to call. If one party is set as a digital channel, and the other party is set as an analog channel (no sub-tone code status), forced mixed use at the same frequency, the phone end and the radios end may have use problems.

3.3 FCC

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference.

(2) this device must accept any interference received, including interference that may cause undesired operation.

4 Overview

W712 is a RoIP intercom gateway developed specifically for the needs of industrial users. It supports the interconnection between traditional analog/digital intercom and SIP industry products. Audio intercom is realized by connecting analog/digital intercom and SIP products. It has strong penetration and can adapt to various environments such as communities, buildings, warehouses, and parks, facilitating rapid deployment of devices. And the equipment size is small, suitable for all kinds of integration of DIY applications.

In order to help some users who are interested to read every detail of the product, this user manual is provided as a user's reference guide. Stil, the document might not be up to date with the newly release software, so please kindly download updated user manual from Fanvil website , or contact with Fanvil support if you have any question using W712.

5 Desktop Installation

5.1 Use POE or external Power Adapter

W712 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 teledevice which is powered by the teledevice line.

For users who do not have POE equipment, the traditional power adaptor should be used. If the device is connected to both POE switch and external power adapter, W712 will get power supply from POE switch in priority, and change to external power adapter once the POE power supply fails.

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

5.2 Replacement battery

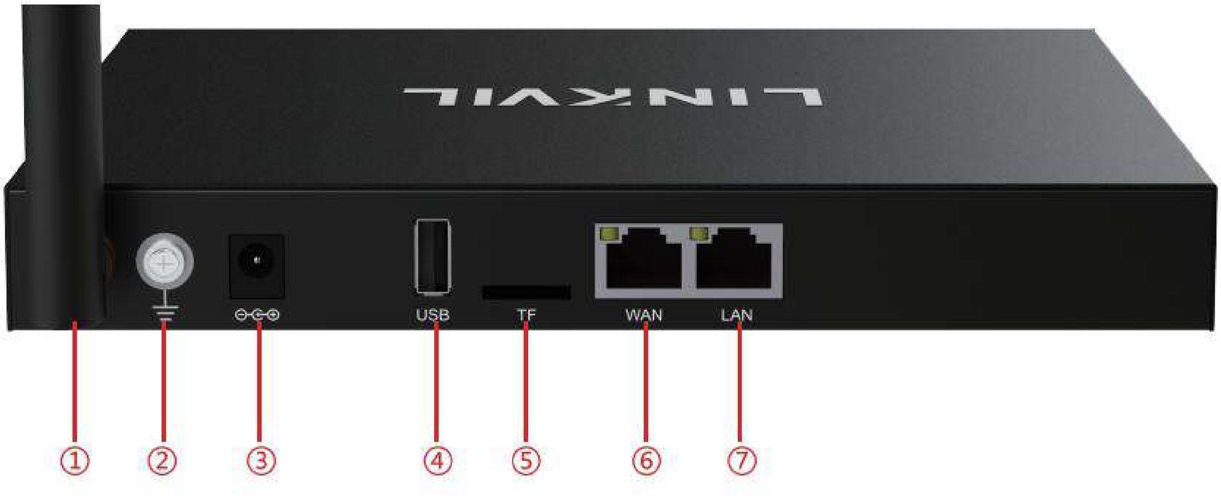
5.2.1 LED status

Table 1 - Button and LED status

Type	**LED**	**status**
POWER LED	Normally on	Turn on power
SIP	Normally on	Register successfully
	Fast flashing	In the call
Bicolor	Red normally on	Emitting status
	Green normally on	Receiving status
Bicolor/SIP	Fast flash at the same time	Power starting

6 Introduction to the User

6.1 Interface description



Picture 1 - Interface display

Table 2 - Interface Description

Number	Name	Description
①	External antenna interface	Transmit and receive signals
②	Grounding screw interface	Grounding protection device to prevent leakage
③	Power interface	12V/1.5A input, pay attention to internal positive and external negative
④	USB interface	External USB flash disk can be connected, up to 128G
⑤	TFcard interface	External USB flash disk can be connected, up to 128G
⑥/⑦	Ethernet WAN/LAN interface	Standard RJ45 interface, 10/100M adaptive, recommended to use Category 5 or super Category 5 network cable

6.2 Installation instructions

6.2.1 Installation

1. Voltage check

Check whether the voltage of DC power or external power supply is within the working voltage range of this product (12V/2A)

2. Product inspection

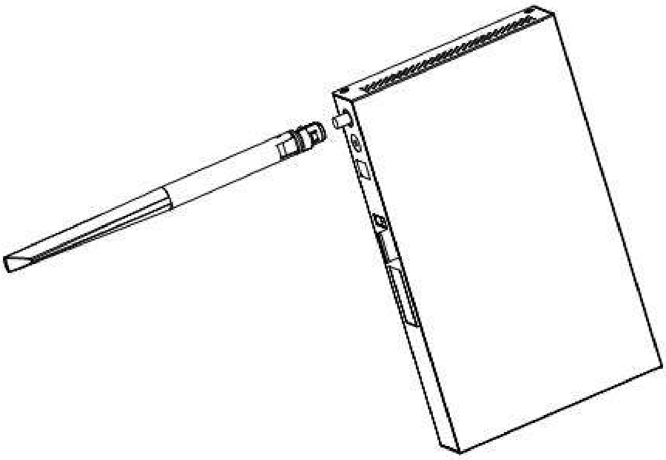
After the power is turned on, check whether the product runs normally by observing the status of all indicators on the front panel. Please refer to "Basic Functional Operation".

3. Accessories installation

When this device is not enabled, first of all, it is necessary to install the supporting narrow belt antennas, power adapter, and connected to WAN network cable.

4. Install antenna

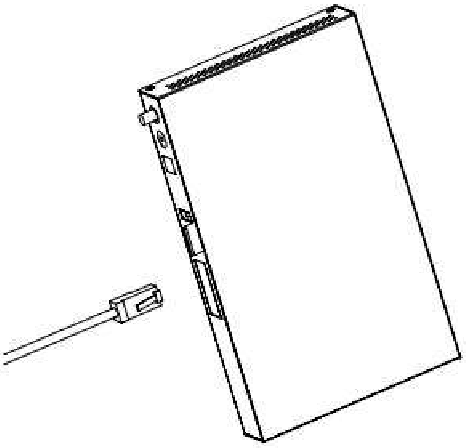
Insert a threaded end with a thread into a narrowband connector and then tighten.



Picture 2 -Install antenna

5. Install network cable

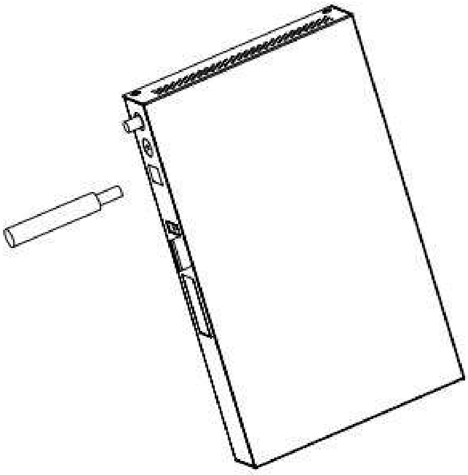
Insert the network cable into the WAN mesh (Ethernet) and support POE power supply (802.3AT).



Picture 3 - Install network cable

6. Install power adapter

Insert the connection head of the power adapter wire into the 12V power connector of the device.

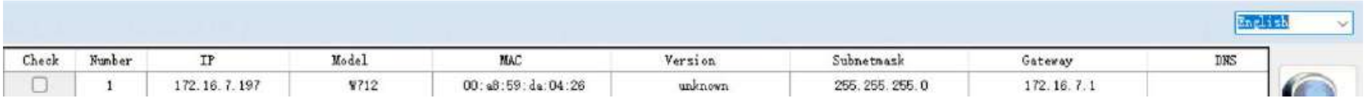


Picture 4 - Install power adapter

6.2.2 Device IP address

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

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

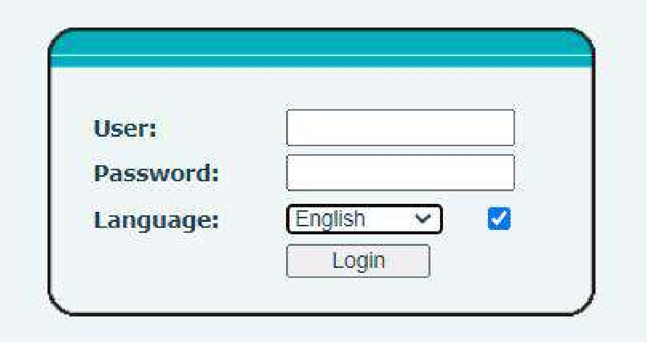


Check	Number	IP	Model	MAC	Version	Subnetmask	Gateway	DNS
□	1	172.16.7.197	W712	00:a8:59:da:04:26	unknown	255.255.255.0	172.16.7.1	

Picture 5 - IP address

6.3 Web Management

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.


User:

Password:

Language: English ☑

Picture 6 - WEB Login

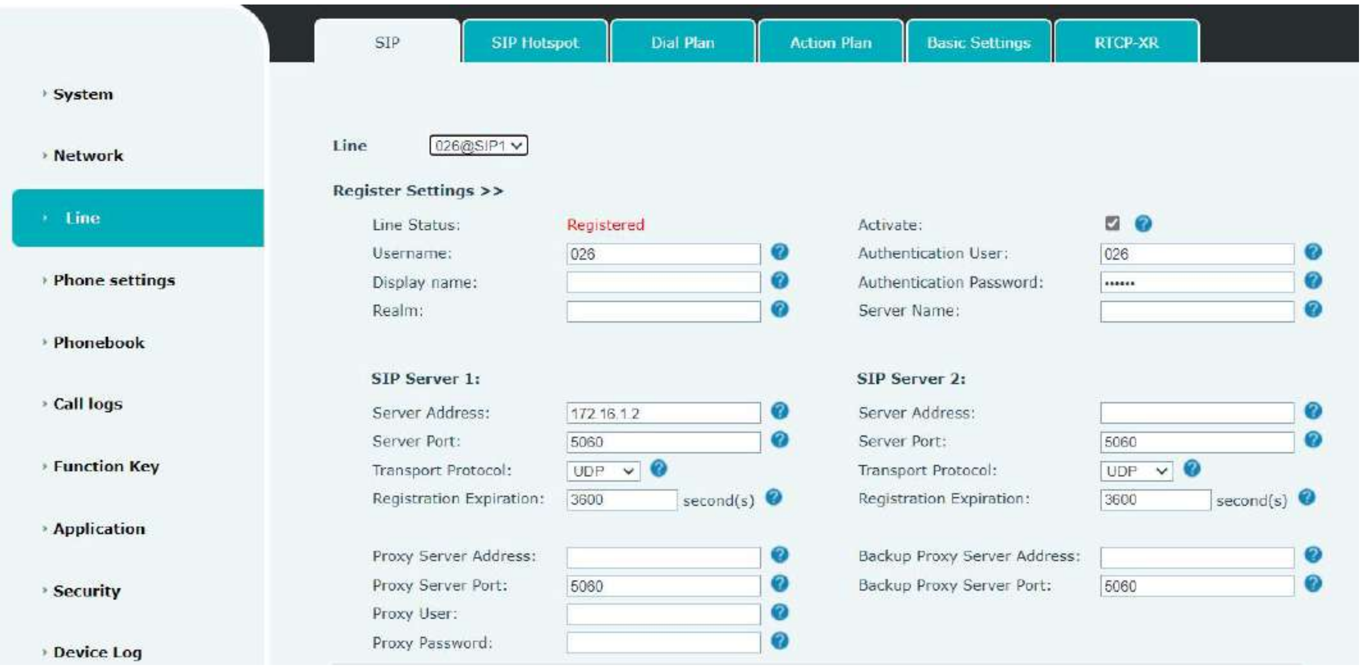
The username and password should be correct to log in to the web page. **The default username and password are "admin"**. For the specific details of the operation of the web page, please refer to 9 Web Configurations

.

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 device, it stores the service provider and the account information used for registration and authentication. When the device is applied with the configuration, it will register the device to the service provider with the server's address and user's authentication as stored in the configurations.

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



Line: 026@SIP1

Register Settings >>

Line Status:	Registered	Activate:	☑
Username:	026	Authentication User:	026
Display name:		Authentication Password:	••••••
Realm:		Server Name:	

SIP Server 1:		SIP Server 2:	
Server Address:	172.16.1.2	Server Address:	
Server Port:	5060	Server Port:	5060
Transport Protocol:	UDP	Transport Protocol:	UDP
Registration Expiration:	3600 second(s)	Registration Expiration:	3600 second(s)
Proxy Server Address:		Backup Proxy Server Address:	
Proxy Server Port:	5060	Backup Proxy Server Port:	5060
Proxy User:			
Proxy Password:			

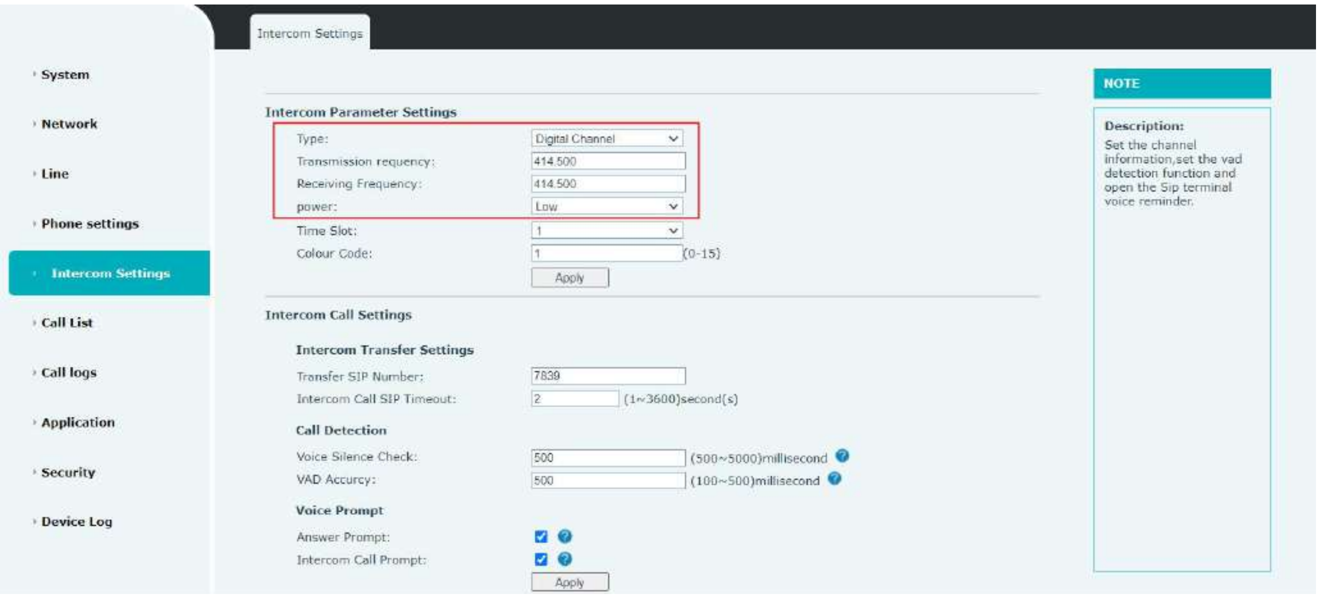
Picture 7 - Web SIP registration

6.5 Channel configuration

Setting requires configuration channel information to provide intercom services. If you want to talk to the intercom, set the transmitting and receiving frequency to the same as the intercom. Click Edit to edit the unique parameters of the digital channel/analog channel.

Digital channel settings are set up in intercom after the color code, and only when the transmission and receiving color code can be transmitted. The analog channel configuration can also talk normally after the Asian code is configured; the intercom that does not match the Asian sound cannot speak. The frequency can be set for any value within the scope of the state regulations.

The power level determines the scope of launch. On the uninteresting urban road, the maximum range of 4W is 3 kilometers and the maximum range of 0.5W is 1.2 kilometers. Customers can choose power according to the distance.



Intercom Parameter Settings

Type: Digital Channel

Transmission requency: 414.500

Receiving Frequency: 414.500

power: Low

Time Slot: 1

Colour Code: 1 (0-15)

Intercom Call Settings

Intercom Transfer Settings

Transfer SIP Number: 7839

Intercom Call SIP Timeout: 2 (1~3600)second(s)

Call Detection

Voice Silence Check: 500 (500~5000)millisecond

VAD Accurcy: 500 (100~500)millisecond

Voice Prompt

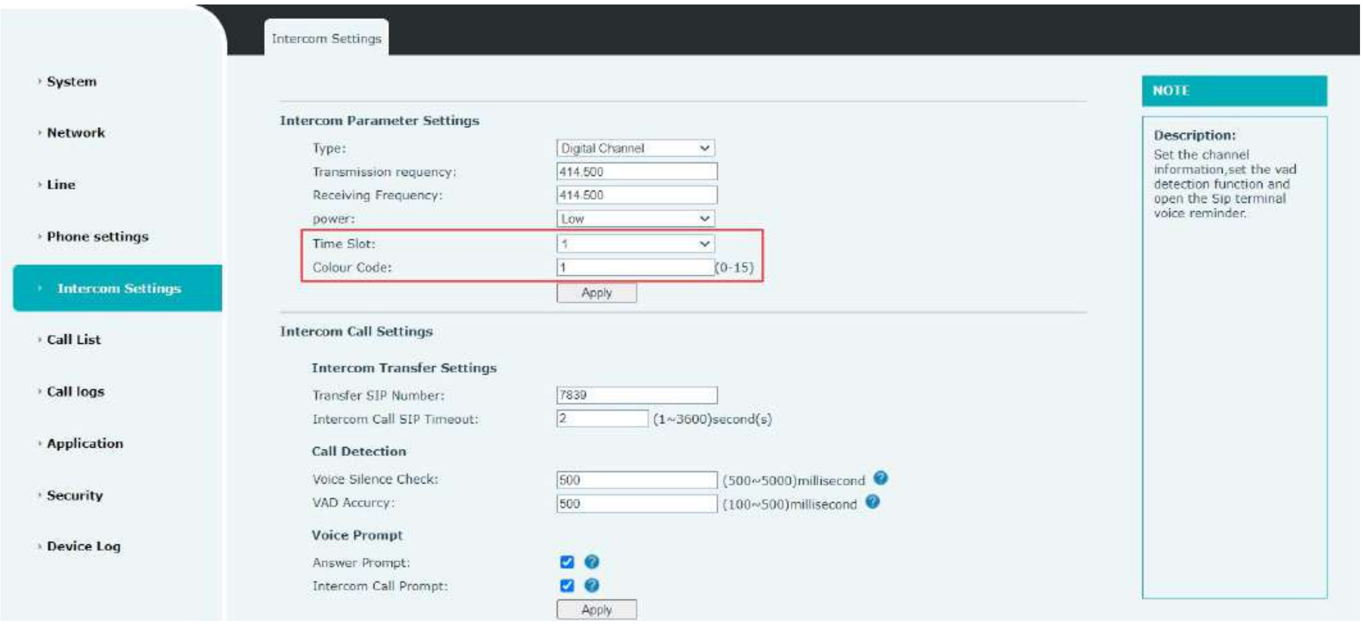
Answer Prompt: ☑

Intercom Call Prompt: ☑

NOTE

Description:
Set the channel information,set the vad detection function and open the Sip terminal voice reminder.

Picture 8 - Channel configuration



Intercom Parameter Settings

Type: Digital Channel

Transmission requency: 414.500

Receiving Frequency: 414.500

power: Low

Time Slot: 1

Colour Code: 1 (0-15)

Intercom Call Settings

Intercom Transfer Settings

Transfer SIP Number: 7839

Intercom Call SIP Timeout: 2 (1~3600)second(s)

Call Detection

Voice Silence Check: 500 (500~5000)millisecond

VAD Accurcy: 500 (100~500)millisecond

Voice Prompt

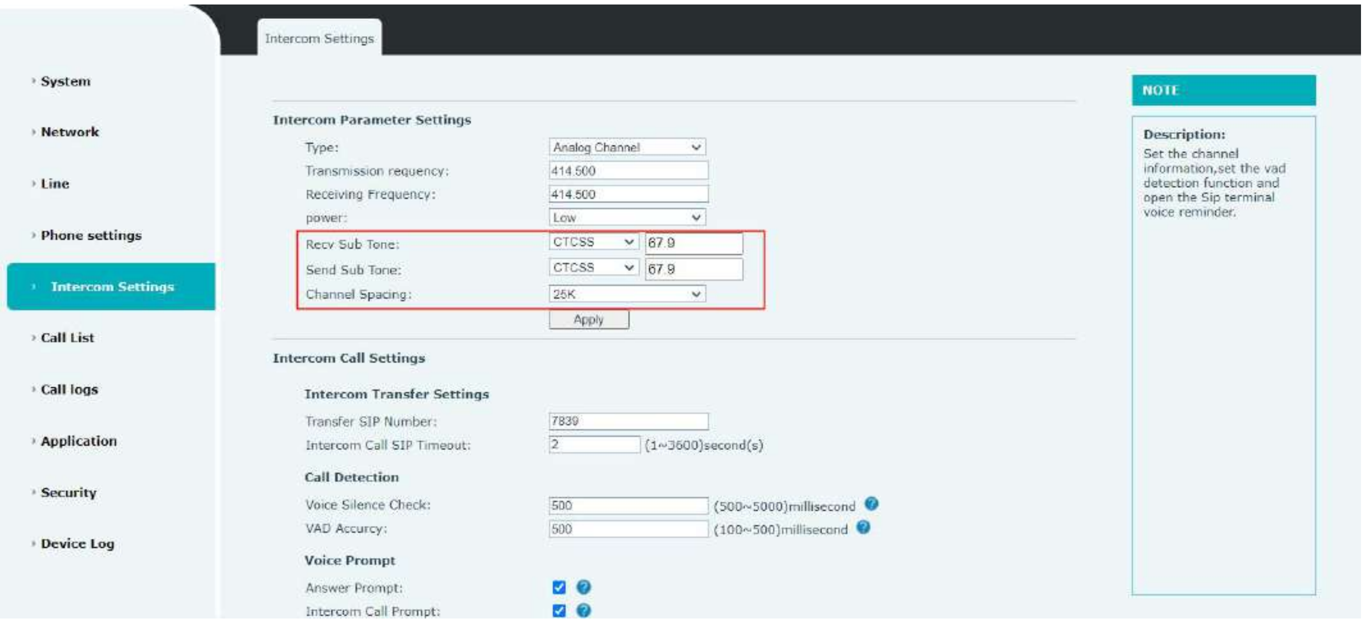
Answer Prompt: ☑

Intercom Call Prompt: ☑

NOTE

Description:
Set the channel information,set the vad detection function and open the Sip terminal voice reminder.

Picture 9 - Digital channel parameters



Intercom Parameter Settings

Type: Analog Channel
Transmission requency: 414.500
Receiving Frequency: 414.500
power: Low
Recv Sub Tone: CTCSS 67.9
Send Sub Tone: CTCSS 67.9
Channel Spacing: 25K

Intercom Call Settings

Intercom Transfer Settings

Transfer SIP Number: 7839
Intercom Call SIP Timeout: 2 (1~3600)second(s)

Call Detection

Voice Silence Check: 500 (500~5000)millisecond
VAD Accurcy: 500 (100~500)millisecond

Voice Prompt

Answer Prompt: ☑
Intercom Call Prompt: ☑

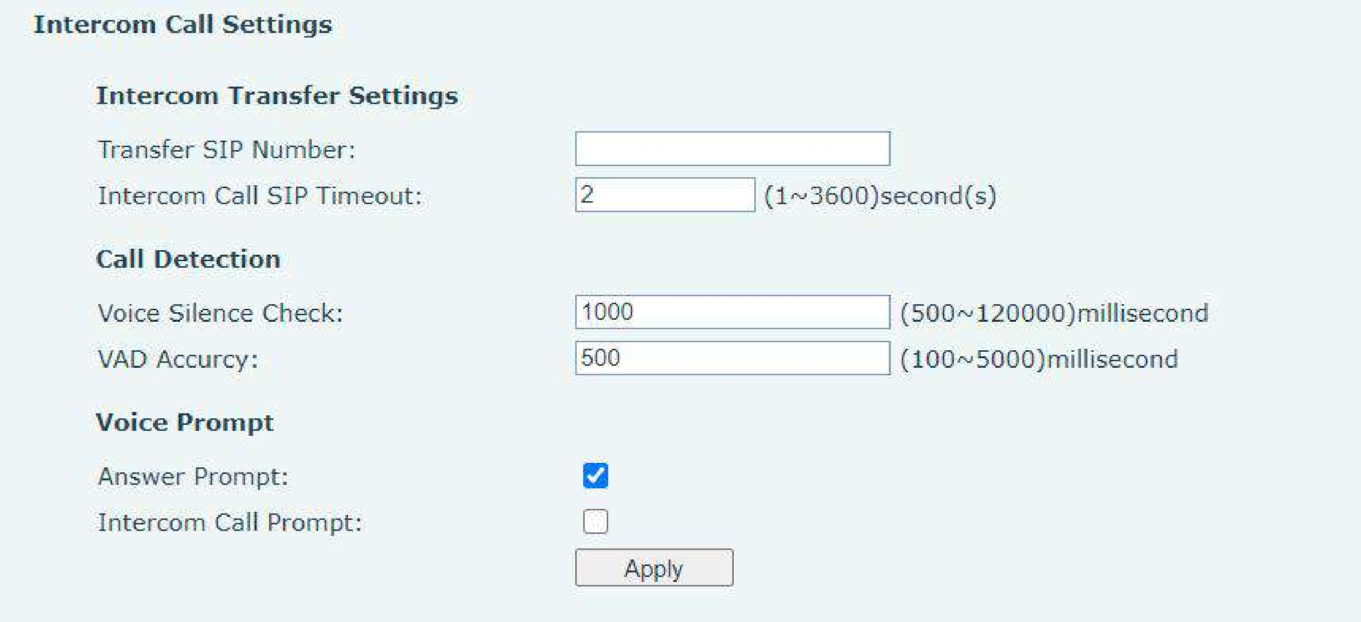
NOTE

Description:
Set the channel information,set the vad detection function and open the Sip terminal voice reminder.

Picture 10 - Analog channel parameters

6.6 Call configuration

If you want to use the intercom to call the phone directly for calling, you need to configure the number of intercom. Configure SIP number or multicast.



Intercom Call Settings

Intercom Transfer Settings

Transfer SIP Number:
Intercom Call SIP Timeout: 2 (1~3600)second(s)

Call Detection

Voice Silence Check: 1000 (500~120000)millisecond
VAD Accurcy: 500 (100~5000)millisecond

Voice Prompt

Answer Prompt: ☑
Intercom Call Prompt: □

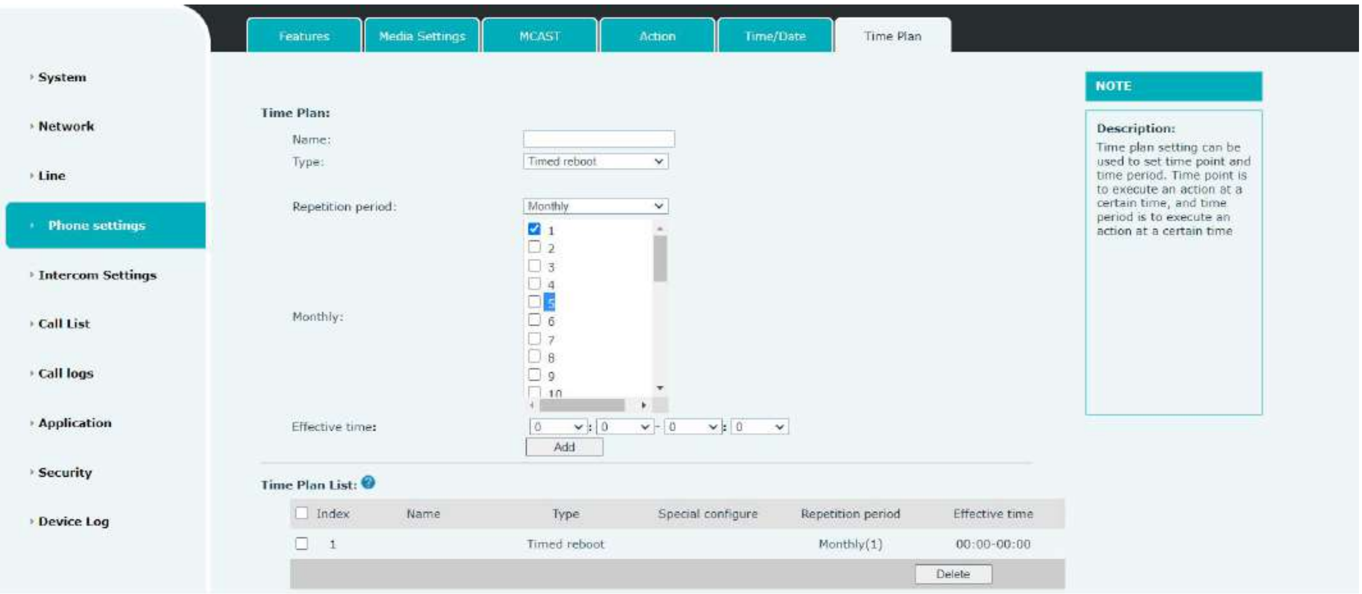
Picture 11 - Channel configuration

6.7 Maintenance instruction

To ensure stable operation of the device, it is recommended to perform a scheduled restart of the device as follows:

1. Enter 【Phone Settings】 - 【Time Plan】

2. Select the type as scheduled restart, the recurrence period as monthly, and select a certain day and effective time to add.



Time Plan:

Name:

Type: Timed reboot

Repetition period: Monthly

Monthly: ☑ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10

Effective time: 0 : 0 - 0 : 0

Time Plan List:

□ Index	Name	Type	Special configure	Repetition period	Effective time
□ 1		Timed reboot		Monthly(1)	00:00-00:00

Description:
Time plan setting can be used to set time point and time period. Time point is to execute an action at a certain time, and time period is to execute an action at a certain time

Picture 12 - Time Plan

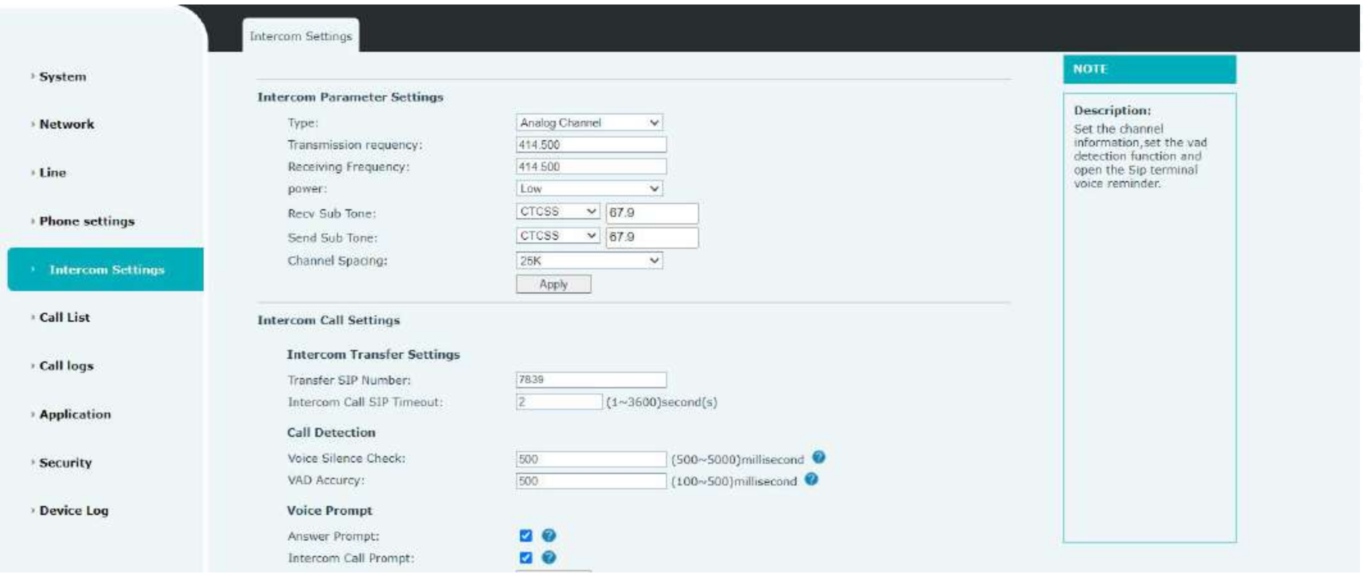
7 Basic Function

7.1 Forward the call side call to the intercom side

When there is a phone call, the device is automatically answered by default and does not need to configure the user. When the user is configured on the webpage, the channel related parameters are consistent with the intercom. When the user speaks on the phone, the gateway automatically forwards the voice on the side of the phone to the intercom side side to the side of the intercom side side.

When there is a multicast, when the user speaks, the gateway will automatically forward the voice on the side of the phone to the side of the intercom.

Note: When the user uses a multicast to the gateway on the side of the phone, the transmission needs to be manually ended immediately after the speech, otherwise it will affect the gateway to transmit the intercom to the phone



Intercom Parameter Settings

Type: Analog Channel
Transmission requency: 414.500
Receiving Frequency: 414.500
power: Low
Recv Sub Tone: CTCSS 67.9
Send Sub Tone: CTCSS 67.9
Channel Spacing: 25K

Intercom Call Settings

Intercom Transfer Settings

Transfer SIP Number: 7839
Intercom Call SIP Timeout: 2 (1~3600)second(s)

Call Detection

Voice Silence Check: 500 (500~5000)millisecond
VAD Accurcy: 500 (100~500)millisecond

Voice Prompt

Answer Prompt: ☑
Intercom Call Prompt: ☑

NOTE

Description:
Set the channel information,set the vad detection function and open the Sip terminal voice reminder.

Picture 13 - Web Setting Gateway Channel

7.2 Forward the intercom side to the call side

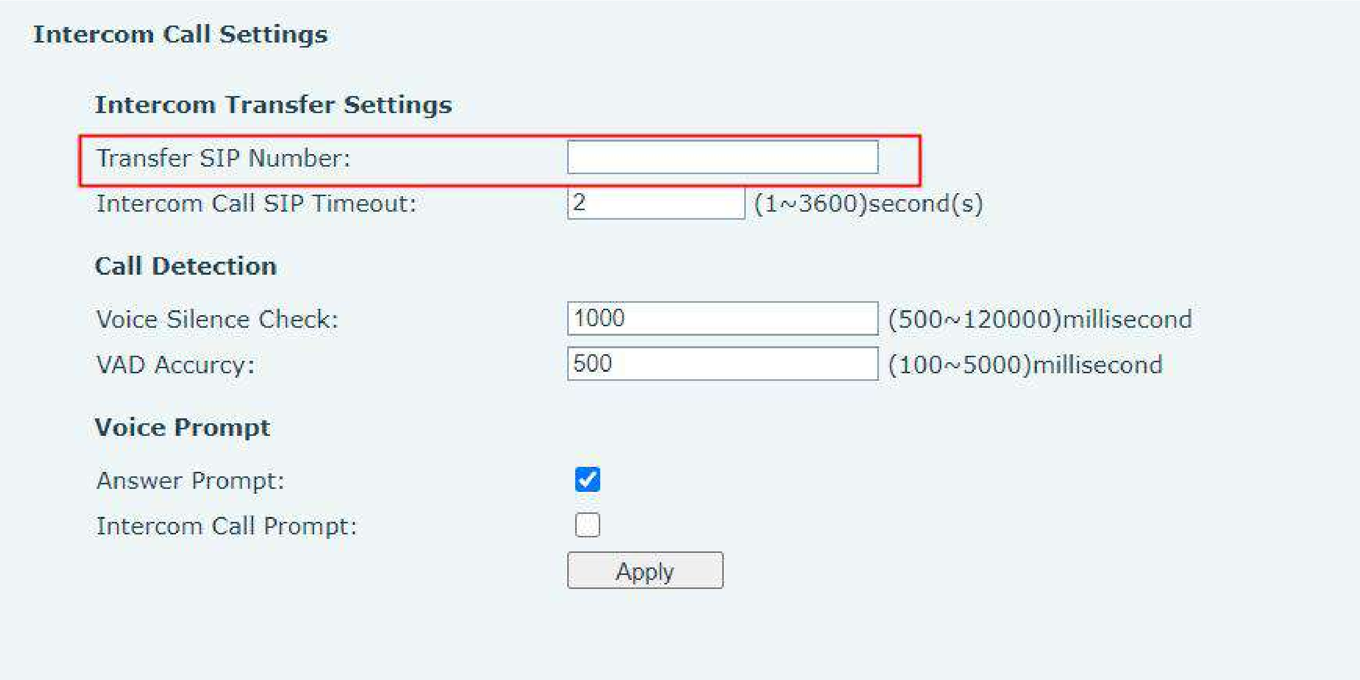
There are two cases of the gateway to the side of the interpretation to the side of the phone.

When the phone actively initiates the call:

Users do not need to set up the intercom's call number on the intercom. Before the call is not over, the user presses the PTT speech on the side of the intercom directly to initiate the call before the call is over. machine

When the intercom is initiated to initiate a call:

Users need to set up the intercom's call number on the [intercom settings] >> [call and VAD detection function]. After setting, the user presses the PTT to speak on the intercom side to be forwarded to the corresponding number to set the corresponding number.



Intercom Call Settings

Intercom Transfer Settings

Transfer SIP Number:	
Intercom Call SIP Timeout:	2 (1~3600)second(s)

Call Detection

Voice Silence Check:	1000 (500~120000)millisecond
VAD Accurcy:	500 (100~5000)millisecond

Voice Prompt

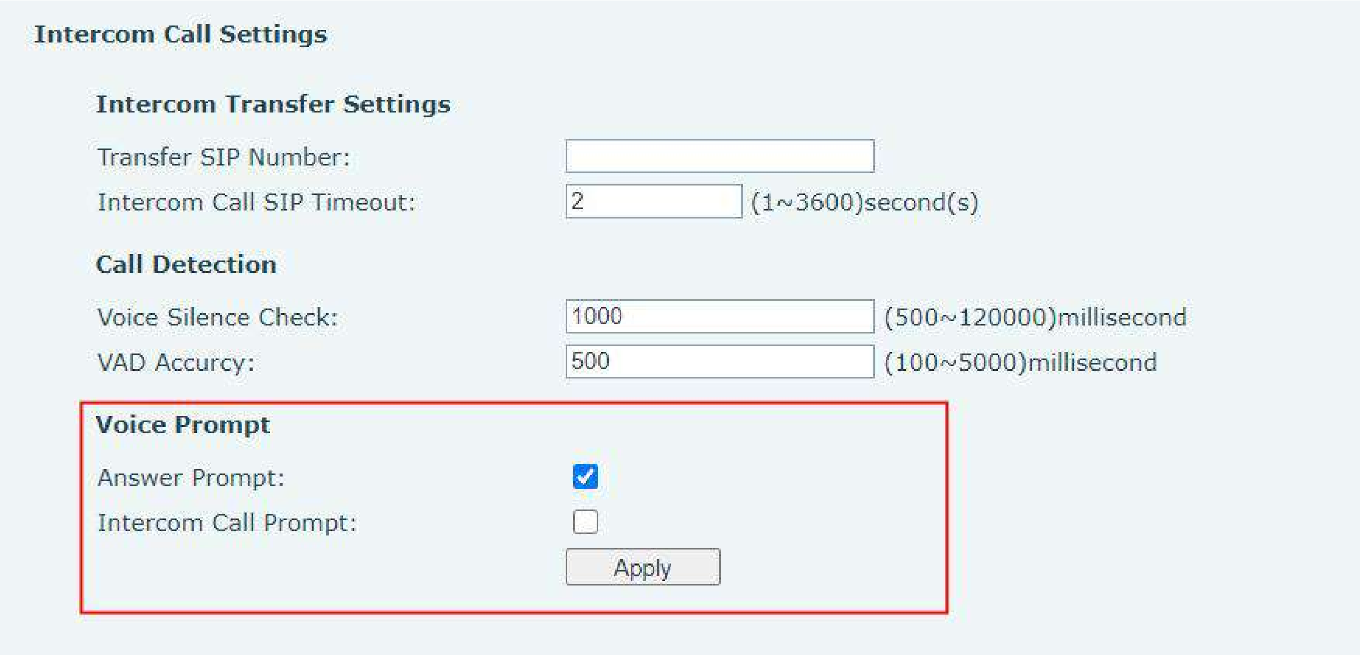
Answer Prompt:	☑
Intercom Call Prompt:	□

Picture 14 - Web setting transfer number

7.3 Tone

When the user uses the phone side to initiate a call actively, a beep can be heard when connecting the gateway to indicate that it is connected, and the user can start talking

When the user continues to establish a call on the phone side, when the radios connects or releases PTT, it will send a beep to the phone end to indicate that the radios end has started or ended the call



Intercom Call Settings

Intercom Transfer Settings

Transfer SIP Number:

Intercom Call SIP Timeout: 2 (1~3600)second(s)

Call Detection

Voice Silence Check: 1000 (500~120000)millisecond

VAD Accurcy: 500 (100~5000)millisecond

Voice Prompt

Answer Prompt: ☑

Intercom Call Prompt: □

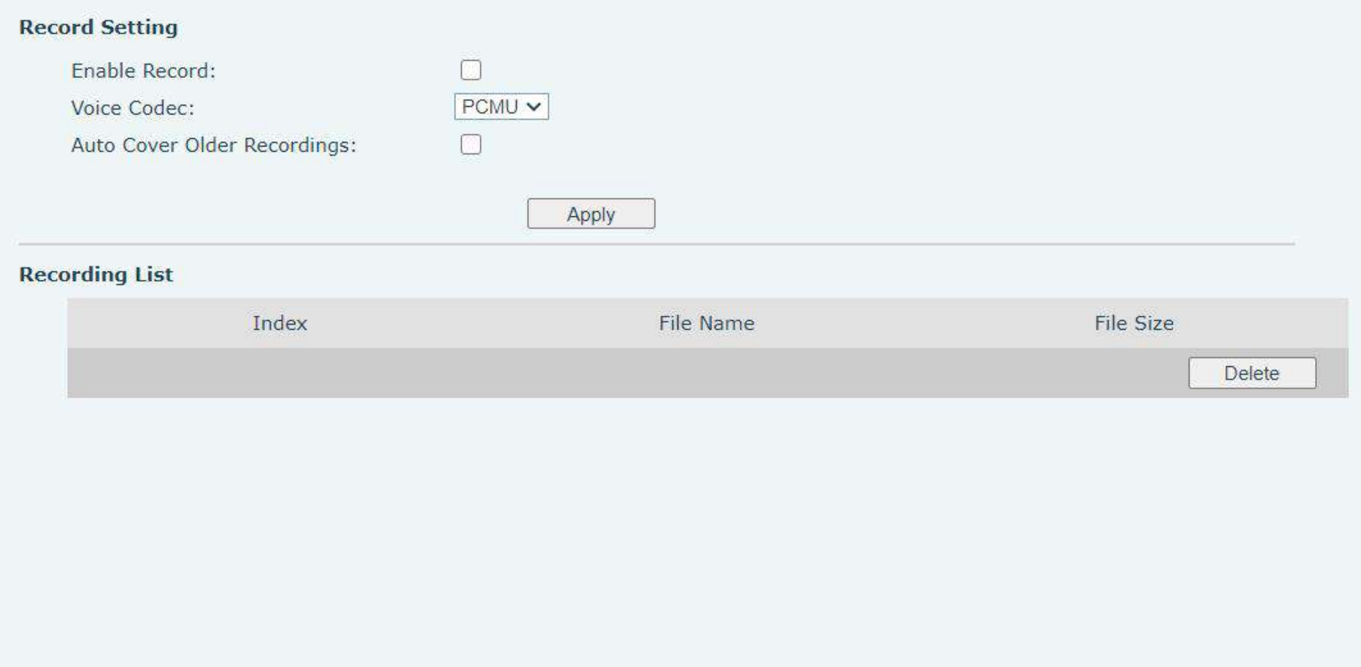
Picture 15 - Setting voice prompt

8 Advance Function

8.1 Record

After inserting a U disk or TF card, the device supports recording operations during call. At the same time, the web page displays the available capacity and the total capacity of the U disk or TF card.

You must first start the recording on the phone web [Application] >> [Recording Management] to set up voice coding. All calls reposted by the gateway will be recorded. The specific web is as follows:



Record Setting

Enable Record: □

Voice Codec: PCMU

Auto Cover Older Recordings: □

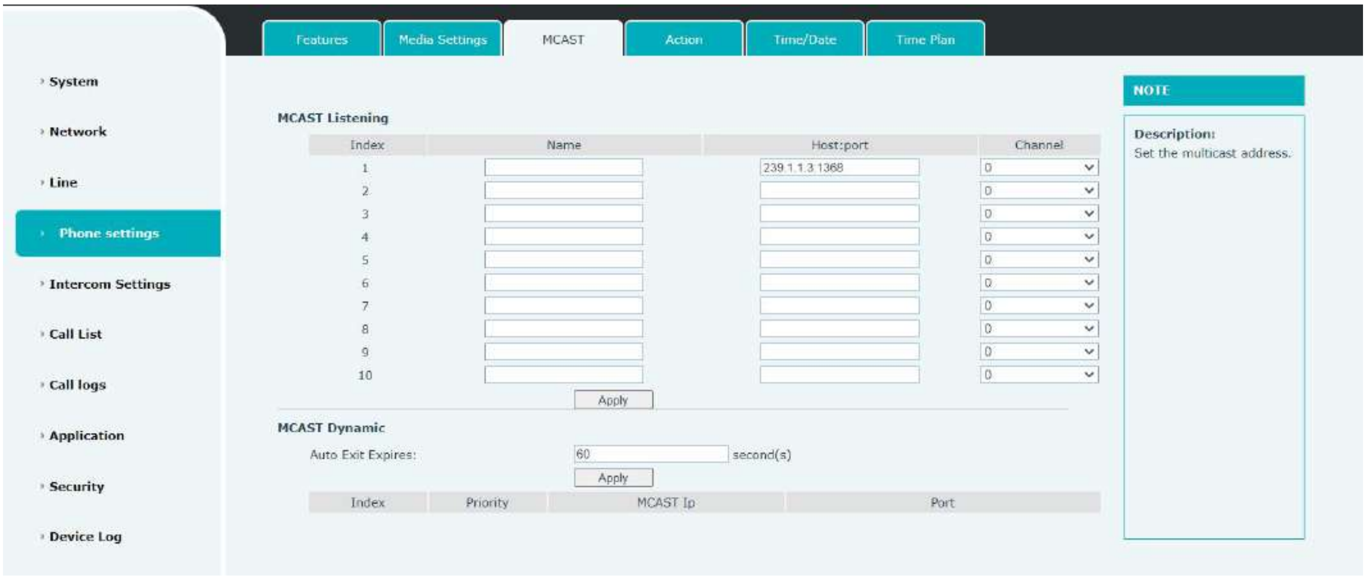
Recording List

Index	File Name	File Size

Picture 16 - recording settings Page

8.2 MCAST

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



MCAST Listening

Index	Name	Host:port	Channel
1		239.1.1.3:1368	0
2			0
3			0
4			0
5			0
6			0
7			0
8			0
9			0
10			0

MCAST Dynamic

Auto Exit Expires: 60 second(s)

Index	Priority	MCAST Ip	Port

NOTE

Description:
Set the multicast address.

Picture 17 - Multicast Settings Page

Table 3 - MCAST Parameters on Web

Parameters	Description
Name	Listened multicast server name
Host:port	Listened multicast server’s multicast IP address and port.

Multicast:

- Go to web page of [**Intercom Settings**] >> [**Transfer Number**] Set the programming address
- Click Apply.
- Set up the name, host and port of the receiving multicast on the web page of [**Phone Settings**] >> [**MCAST**].
- Press the PTT key of the intercom
- Receive end will receive multicast call and play multicast automatically.The receiver will receive a multicast and automatically play the multicast

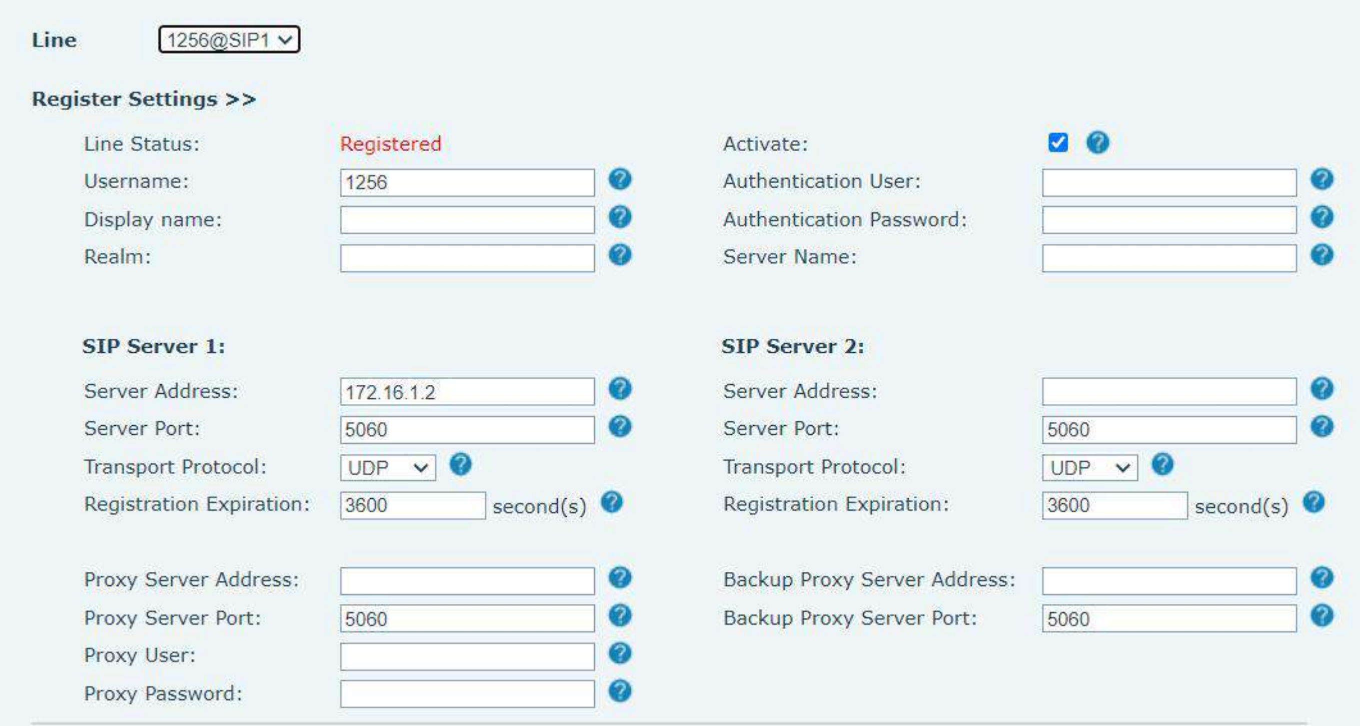
8.3 SIP Hotspot

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

The users can set functions as a SIP hotspot and other devices set (B and C) function as SIP hotspot clients. When somebody calls device set A, device sets A, B, and C all ring at the same time. When any device set answers the call, other device sets stop ringing. The call can be answered by only one device set.

When B or C initiates a call, the SIP number registered by device set A is the calling number.

To set a SIP hotspot, register at least one SIP account.



Line: 1256@SIP1

Register Settings >>

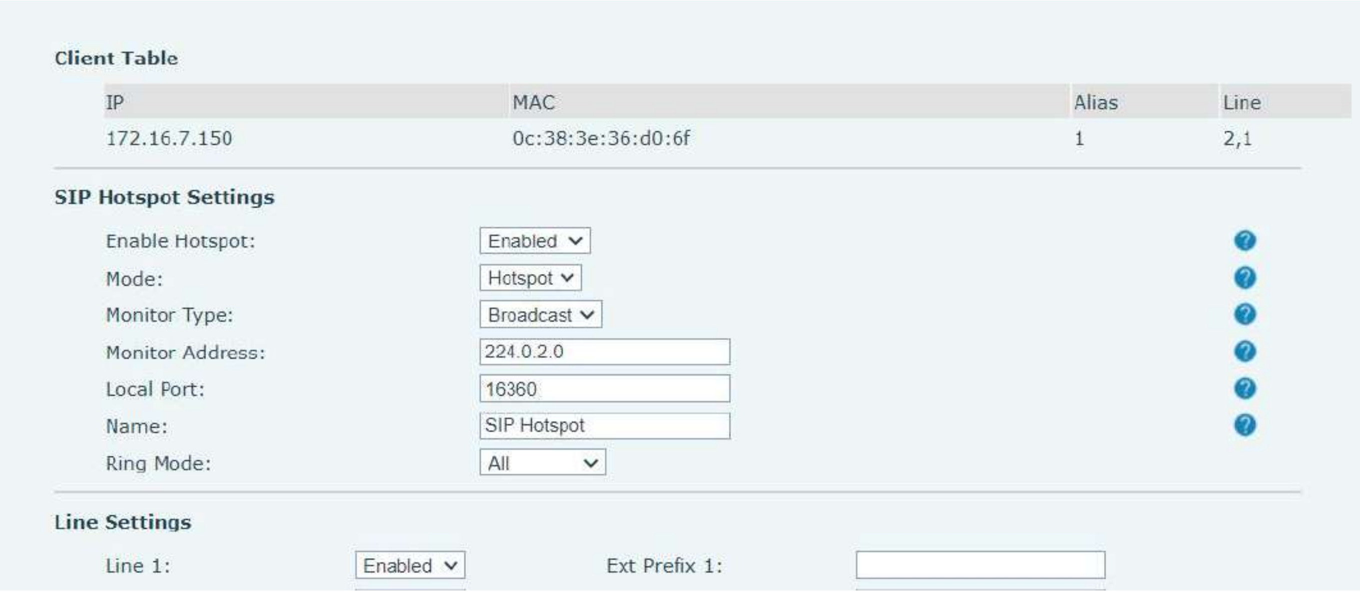
Line Status:	Registered	Activate:	☑
Username:	1256	Authentication User:	
Display name:		Authentication Password:	
Realm:		Server Name:	
SIP Server 1:		**SIP Server 2:**	
Server Address:	172.16.1.2	Server Address:	
Server Port:	5060	Server Port:	5060
Transport Protocol:	UDP	Transport Protocol:	UDP
Registration Expiration:	3600 second(s)	Registration Expiration:	3600 second(s)
Proxy Server Address:		Backup Proxy Server Address:	
Proxy Server Port:	5060	Backup Proxy Server Port:	5060
Proxy User:			
Proxy Password:			

Picture 18 - Register SIP account

Table 4 - SIP hotspot Parameters

Parameters	Description
Device Table	If your device is set to “SIP hotspot server”, Device Table will display as Client Device Table which connected to your device. If your device 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, device will be a “SIP hotspot server”; Choose Client, device 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 device 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 server:



Client Table

IP	MAC	Alias	Line
172.16.7.150	0c:38:3e:36:d0:6f	1	2,1

SIP Hotspot Settings

Enable Hotspot: Enabled

Mode: Hotspot

Monitor Type: Broadcast

Monitor Address: 224.0.2.0

Local Port: 16360

Name: SIP Hotspot

Ring Mode: All

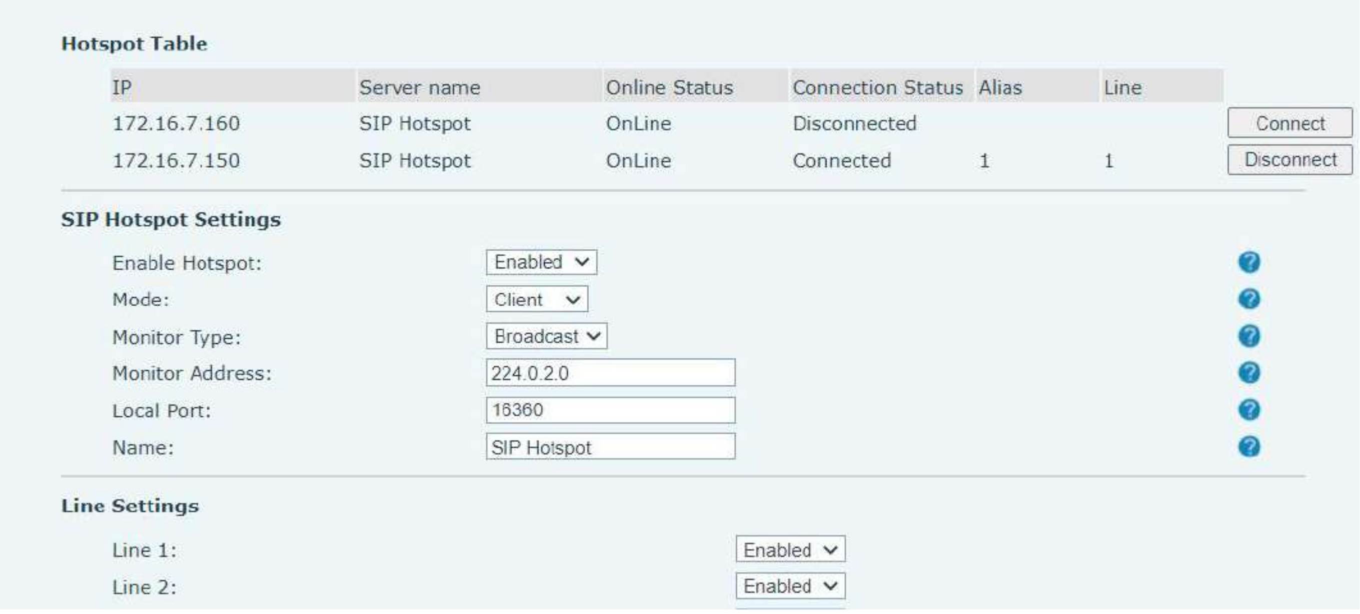
Line Settings

Line 1: Enabled Ext Prefix 1:

Picture 19 - SIP hotspot server configuration

Configure SIP hotspot client:

To set as a SIP hotspot client, no SIP account needs to be set. The device set will automatically obtain and configure a SIP account. On the SIP Hotspot tab page, set Mode to Client. The values of other options are the same as those of the hotspot.



Hotspot Table

IP	Server name	Online Status	Connection Status	Alias	Line	
172.16.7.160	SIP Hotspot	OnLine	Disconnected			Connect
172.16.7.150	SIP Hotspot	OnLine	Connected	1	1	Disconnect

SIP Hotspot Settings

Enable Hotspot: Enabled

Mode: Client

Monitor Type: Broadcast

Monitor Address: 224.0.2.0

Local Port: 16360

Name: SIP Hotspot

Line Settings

Line 1: Enabled

Line 2: Enabled

Picture 20 - SIP hotspot client configuration

As the hotspot server, the default extension number is 0. When the device 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.

9 Web Configurations

9.1 Web Page Authentication

The user can log into the web page of the device to manage the user's device information and operate the device. Users must provide the correct user name and password to log in.

9.2 System >> Information

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

- Model
- Hardware Version
- Software Version
- Uptime
- Memory information
- System time

And summarization of network status,

- Network Mode
- Ethernet MAC
- Wi-Fi MAC
- Ethernet IP
- Wi-Fi IP
- Subnet Mask
- Default Gateway

Besides, summarization of SIP account status,

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

9.3 System >> Account

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

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

9.4 System >> Configurations

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

- **Clear Configurations**

Select the module in the configuration file to clear.

SIP: account configuration.

AUTOPROVISION: automatically upgrades the configuration

TR069:TR069 related configuration

- **Clear Data Tables**

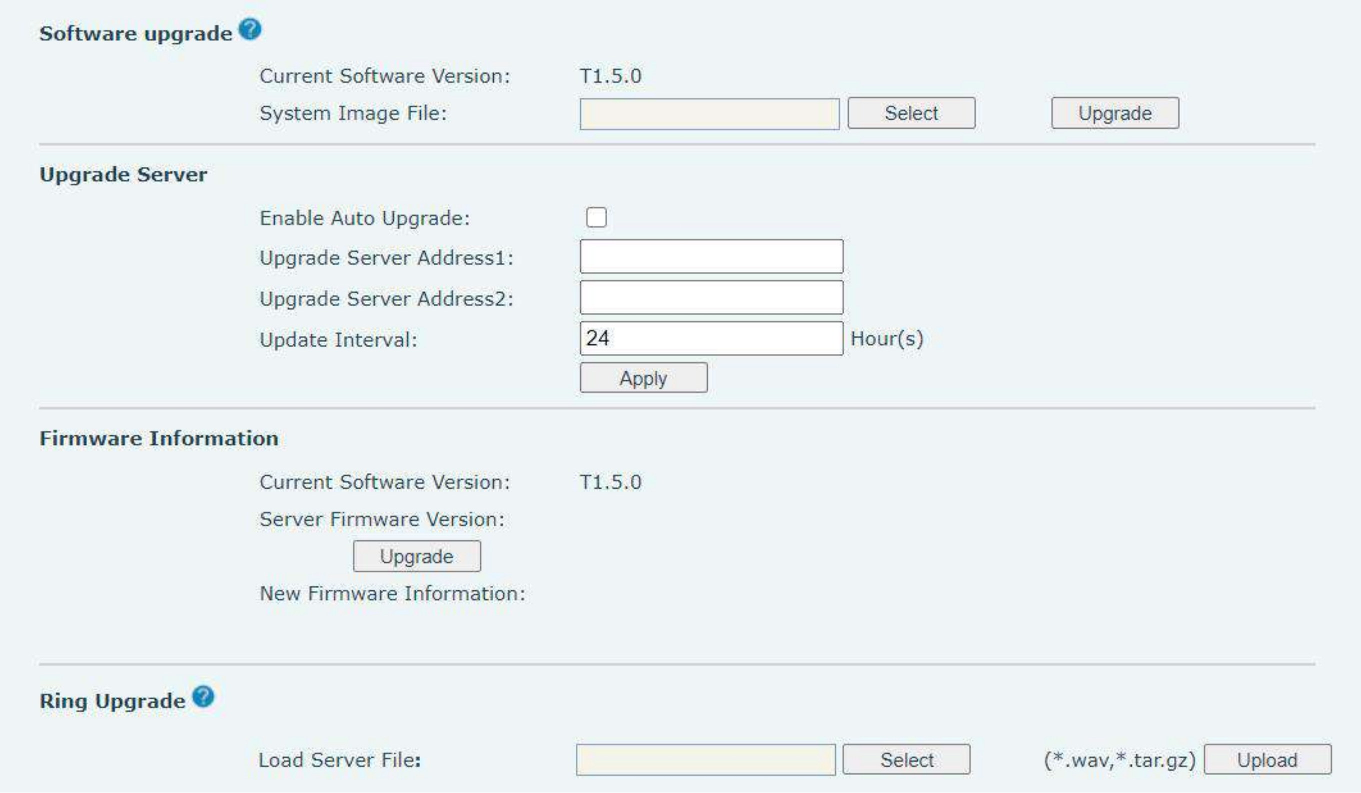
Select the local data table to be cleared, all selected by default.

- **Reset device**

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

9.5 System >> Upgrade

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



Software upgrade

Current Software Version: T1.5.0

System Image File:

Upgrade Server

Enable Auto Upgrade: □

Upgrade Server Address1:

Upgrade Server Address2:

Update Interval: 24 Hour(s)

Firmware Information

Current Software Version: T1.5.0

Server Firmware Version:

New Firmware Information:

Ring Upgrade

Load Server File: (*.wav,*.tar.gz)

Picture 21 - Web page firmware upgrade

Table 5 - Firmware upgrade

Parameter	Description
Upgrade server	
Enable Auto Upgrade	Enable automatic upgrade, If there is a new version txt and new software firmware on the server, device will show a prompt upgrade

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

- The file requested from the server is a TXT file called vendor_model_hw1_0.txt.Hw followed by the hardware version number, it will be written as hw1_0 if no difference on hardware. All Spaces in the filename are replaced by underline.
- For example, the txt file name requested by X7C device is linkvil _w712_hwv1_0.txt
- The URL requested by the device is HTTP:// server address/vendor_Model_hw10 .txt： The new version and the requested file should be placed in the download directory of the HTTP server, as shown in the figure:

- TXT file format must be UTF-8
- vendor_model_hw10.TXT The file format is as follows：

  Version=2.12.1 #Firmware

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

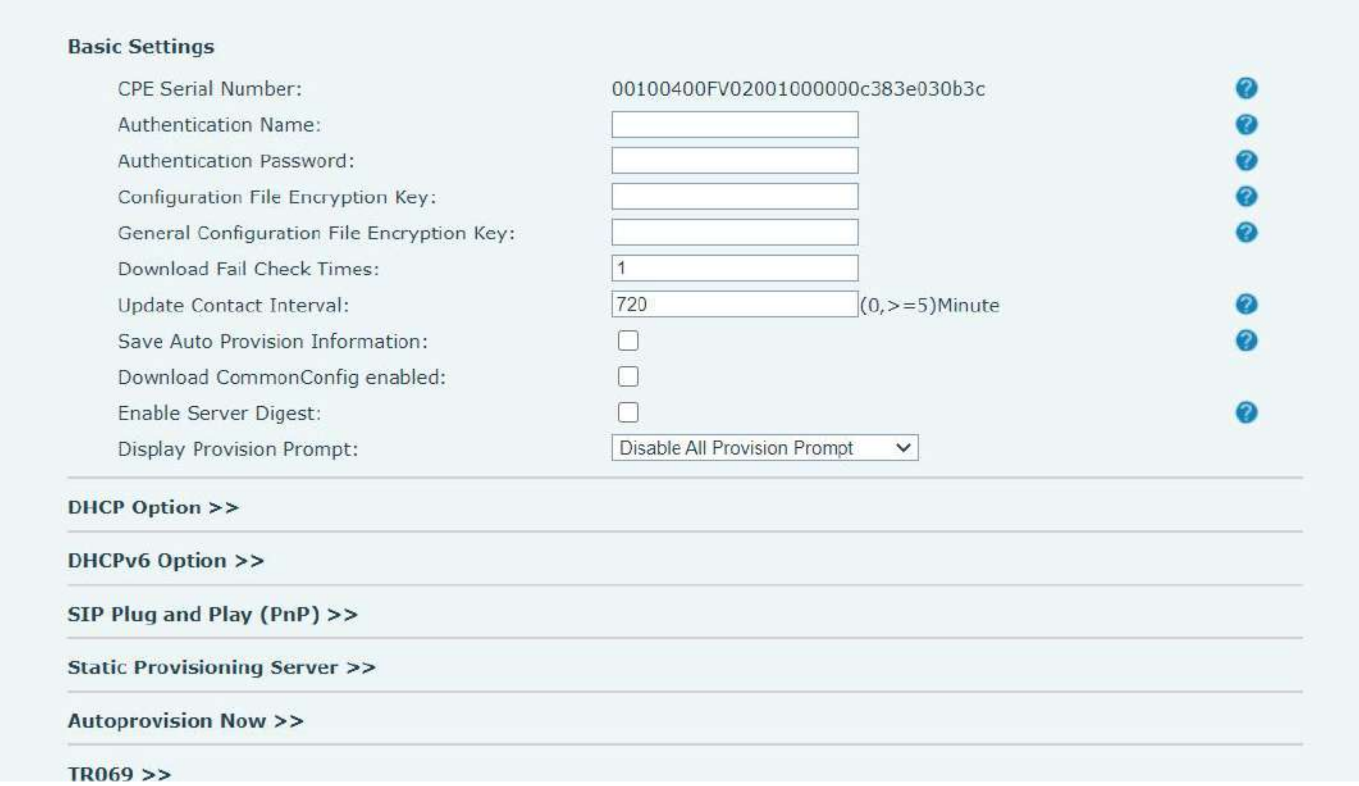
  BuildTime=2022.05.06 20:00

  Info=TXT

  Xxxxx
  Xxxxx
  Xxxxx
  Xxxxx

9.6 System >> Auto Provision

The Auto Provision settings help IT manager or service provider to easily deploy and manage the devices in mass volume. For the detail of Auto Provision, please refer to this link Auto Provision Description。device Webpage: Login and go to [**System**] >> [**Auto provision**].



Basic Settings

CPE Serial Number:	00100400FV02001000000c383e030b3c
Authentication Name:	
Authentication Password:	
Configuration File Encryption Key:	
General Configuration File Encryption Key:	
Download Fail Check Times:	1
Update Contact Interval:	720 (0,>=5)Minute
Save Auto Provision Information:	□
Download CommonConfig enabled:	□
Enable Server Digest:	□
Display Provision Prompt:	Disable All Provision Prompt

Picture 22 - Page auto provision Settings

Fanvil devices support SIP PnP, DHCP options, Static provision, TR069. If all of the 4 methods are enabled, the device will be upgraded according to the method obtained first.

Transferring protocol: FTP, TFTP, HTTP, HTTPS

This article only briefly introduces automatic deployment. For details, please refer to the document **Fanvil Auto Provision**.

Table 6 - Auto Provision

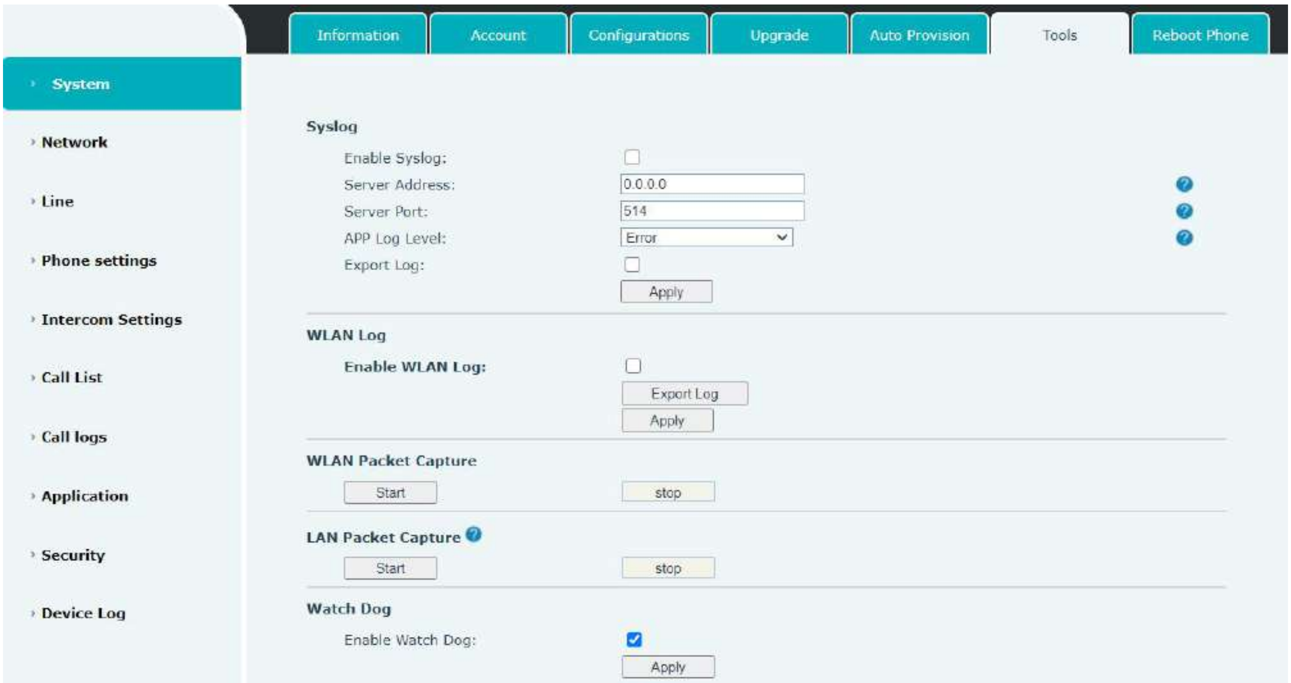
Parameters	**Description**
Basic settings	
CPE Serial Number	Display the device SN
Authentication Name	The user name of provision server
Authentication Password	The password of provision server
Configuration File Encryption Key	If the device configuration file is encrypted , user should add the encryption key here

General Configuration File Encryption Key	If the common configuration file is encrypted, user should add the encryption key here
Download Fail Check Times	If there download is failed, device will retry with the configured times.
Update Contact Interval	device will update the devicebook with the configured interval time. If it is 0, the feature is disabled.
Save Auto Provision Information	Save the HTTP/HTTPS/FTP user name and password. If the provision URL is kept, the information will be kept.
Download Common Config enabled	Whether device will download the common configuration file.
Enable Server Digest	When the feature is enable, if the configuration of server is changed, device will download and update.
DHCP Option	
Option Value	Confiugre DHCP option, DHCP option supports DHCP custom option | DHCP option 66 | DHCP option 43, 3 methods to get the provision URL. The default is Option 66.
Custom Option Value	Custom Option value is allowed from 128 to 254. The option value must be same as server define.
Enable DHCP Option 120	Use Option120 to get the SIP server address from DHCP server.
SIP Plug and Play (PnP)	
Enable SIP PnP	Whether enable PnP or not. If PnP is enable, device will send a SIP SUBSCRIBE message with broadcast method. Any server can support the feature will respond and send a Notify with URL to device. device could get the configuration file with the URL.
Server Address	Broadcast address. As default, it is 224.0.0.0
Server Port	PnP port
Transport Protocol	PnP protocol, TCP or UDP.
Update Interval	PnP message interval.
Static Provisioning Server	
Server Address	Provisioning server address. Support both IP address and domain address.
Configuration File Name	The configuration file name. If it is empty, device 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 device will check the update every 1 hour.

Update Mode	Provision Mode. 1. Disabled. 2. Update after reboot. 3. Update after interval.
TR069	
Enable TR069	Enable TR069 after selection
ACS Server Type	There are 2 options Serve type, common and CTC.
ACS Server URL	ACS server address
ACS User	ACS server username (up to is 59 character)
ACS Password	ACS server password (up to is 59 character)
Enable TR069 Warning Tone	If TR069 is enabled, there will be a prompt tone when connecting.
TLS Version	TLS version (TLS 1.0, TLS 1.1, TLS 1.2)
INFORM Sending Period	INFORM signal interval time. It ranges from 1s to 999s
STUN Server Address	Configure STUN server address
STUN Enable	To enable STUN server for TR069

9.7 System >> Tools

Tools provided in this page help users to identify issues at trouble shooting. Please refer to 10 Trouble Shooting for more detail.



Syslog

Enable Syslog: □

Server Address: 0.0.0.0

Server Port: 514

APP Log Level: Error

Export Log: □

Apply

WLAN Log

Enable WLAN Log: □

Export Log

Apply

WLAN Packet Capture

Start stop

LAN Packet Capture

Start stop

Watch Dog

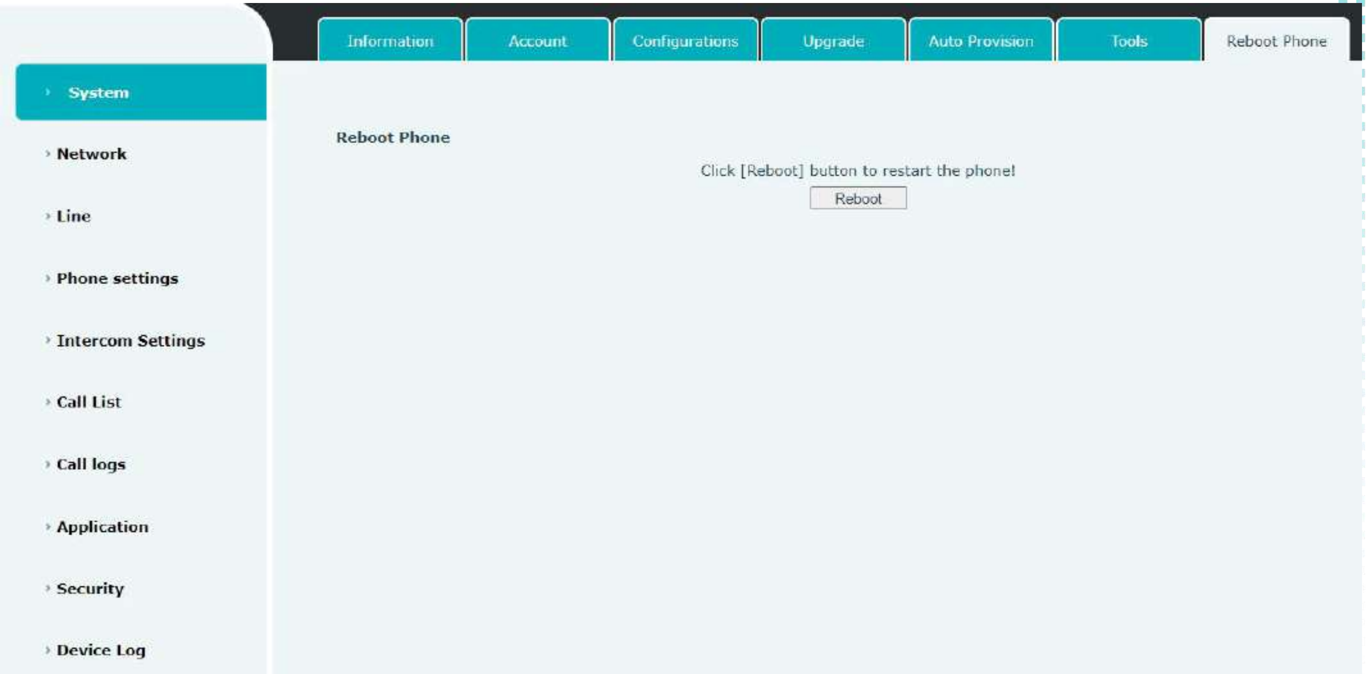
Enable Watch Dog: ☑

Apply

Picture 23 - Tools

9.8 System >> Reboot device

This page can restart the device.



Reboot Phone

Click [Reboot] button to restart the phone!

Picture 24 - Reboot Phone

9.9 Network >> Basic

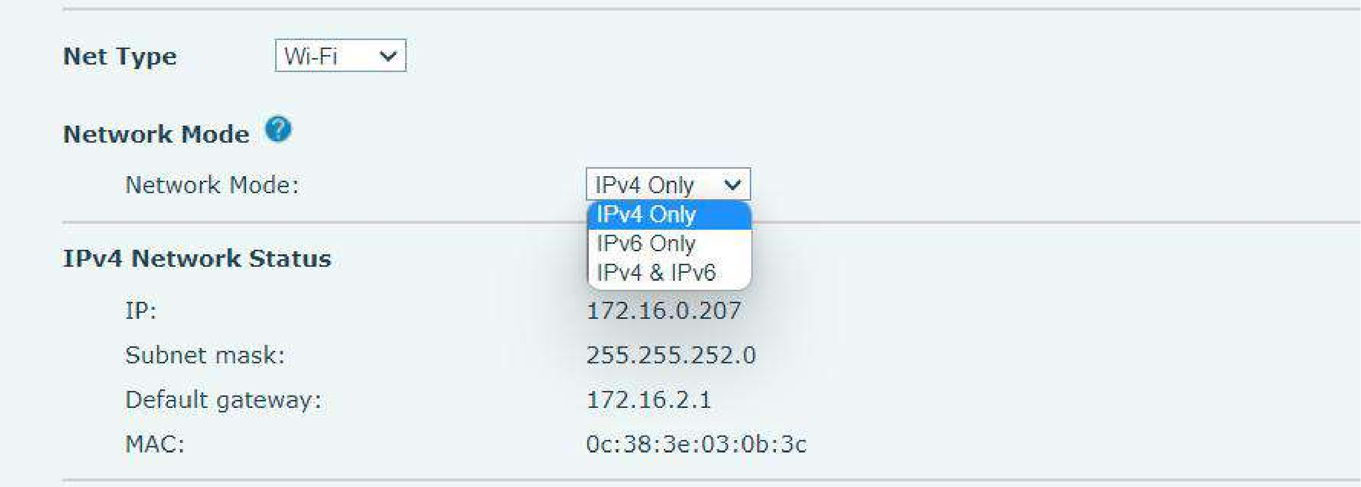
This page allows users to configure network connection types and parameters.

9.9.1 Network Settings

- **IP Mode**

There are 3 network protocol mode options, IPv4, IPv6 and IPv4 & IPv6.

Users can set it on the webpage [**Network**] >> [**Basic**].Select Wi-Fi for the network type, and you can set the network mode.



Net Type: Wi-Fi

Network Mode

Network Mode: IPv4 Only

IPv4 Network Status

IP: 172.16.0.207

Subnet mask: 255.255.252.0

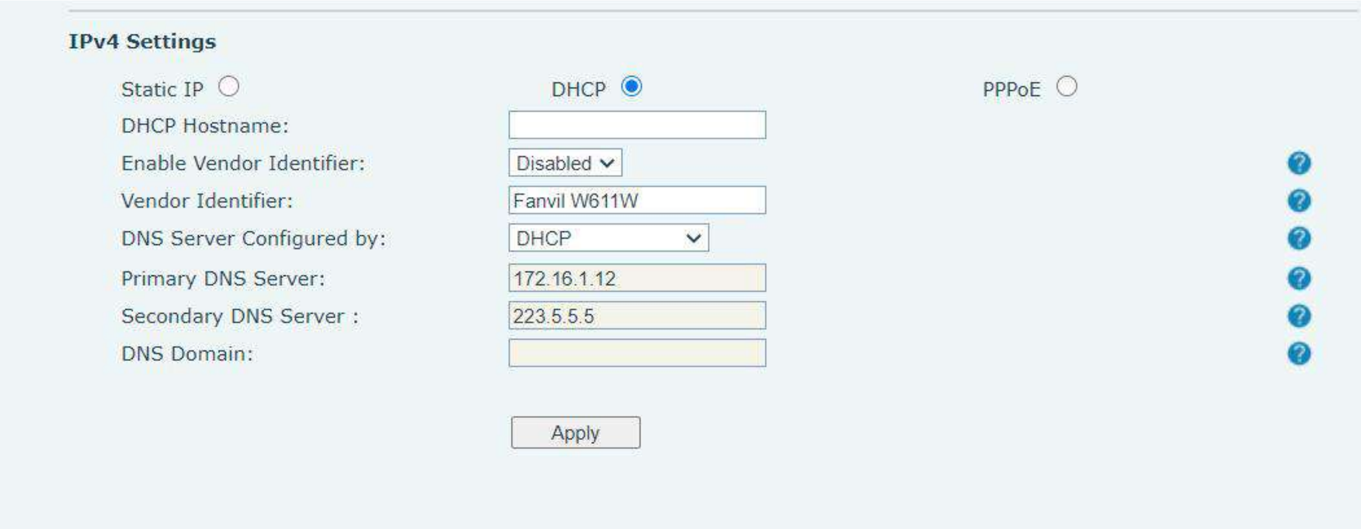
Default gateway: 172.16.2.1

MAC: 0c:38:3e:03:0b:3c

Picture 25 - Network mode Settings

- **IPv4**

In IPv4 mode, there are 3 connection mode options: DHCP, PPPoE and Static IP.



IPv4 Settings

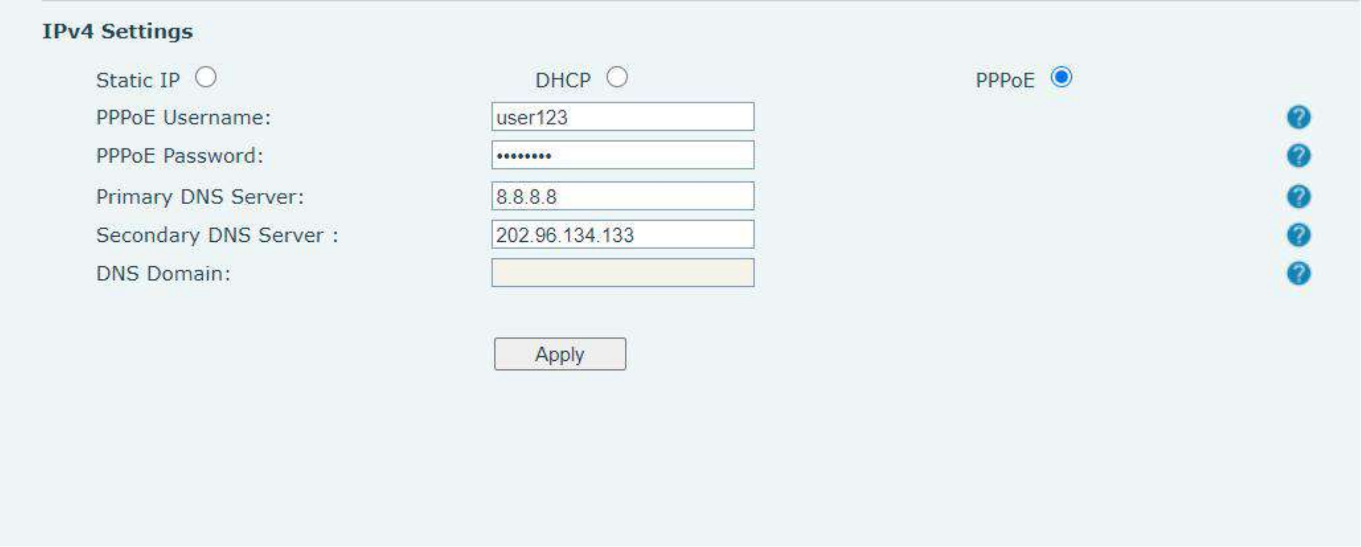
Static IP ○ DHCP ● PPPoE ○

DHCP Hostname:	
Enable Vendor Identifier:	Disabled
Vendor Identifier:	Fanvil W611W
DNS Server Configured by:	DHCP
Primary DNS Server:	172.16.1.12
Secondary DNS Server :	223.5.5.5
DNS Domain:	

Picture 26 - DHCP network mode

When using DHCP mode, device will get the IP address from DHCP server (router).

- Use DHCP DNS: It is enabled as default. “Enable” means device will get DNS address from DHCP server and “disable” means not.
- Use DHCP time: It is disabled as default. “Enable” to manage the time of get DNS address from DHCP server and “disable” means not.



IPv4 Settings

Static IP ○ DHCP ○ PPPoE ●

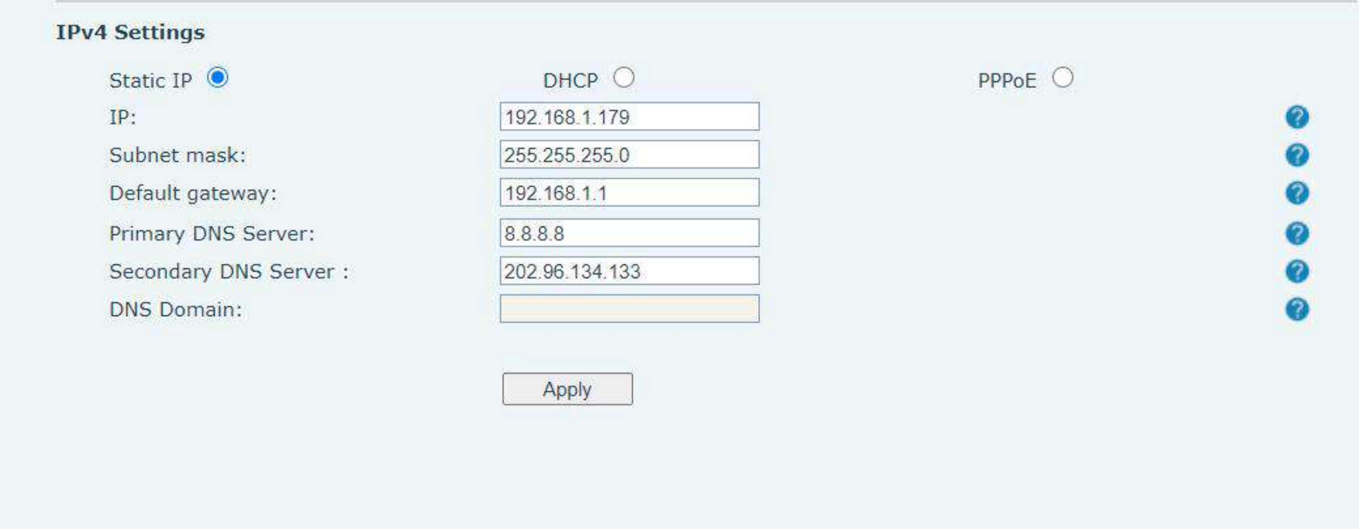
PPPoE Username:	user123
PPPoE Password:	••••••••
Primary DNS Server:	8.8.8.8
Secondary DNS Server :	202.96.134.133
DNS Domain:	

Picture 27 - PPPoE network mode

When using PPPoE, device will get the IP address from PPPoE server.

- Username: PPPoE user name.

- Password: PPPoE password.



IPv4 Settings

Static IP ● DHCP ○ PPPoE ○

IP: 192.168.1.179

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1

Primary DNS Server: 8.8.8.8

Secondary DNS Server : 202.96.134.133

DNS Domain:

Apply

Picture 28 - Static IP network mode

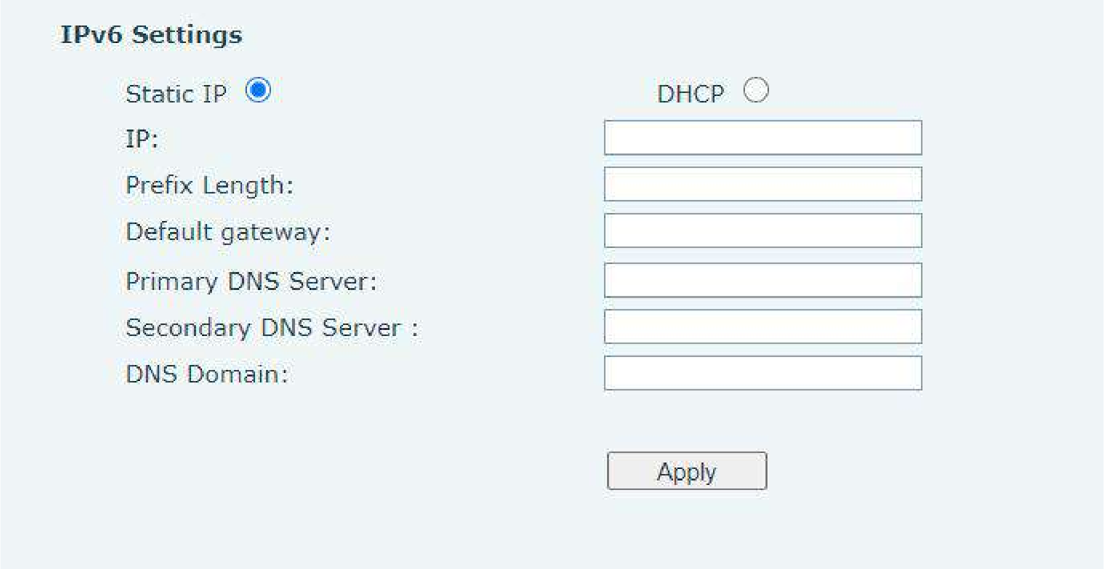
When using Static IP mode, user must configure the IP address manually.

- IP Address: device IP address.
- Mask: sub mask of your LAN.
- Gateway: The gateway IP address. device could access the other network via it.
- Primary DNS: Primary DNS address. The default is 8.8.8.8, Google DNS server address.
- Secondary DNS: When primary DNS is not available, Secondary DNS will work.

- **IPv6**

In IPv6, there are 2 connection mode options, DHCP and Static IP.

- DHCP configuration refers to IPv4 introduction in last page.
- Static IP configuration is almost same as IPv4’s, except the IPv6 Prefix.
- IPv6 Prefix: IPv6 prefix, it is similar with mask of IPv4.



IPv6 Settings

Static IP ● DHCP ○

IP:

Prefix Length:

Default gateway:

Primary DNS Server:

Secondary DNS Server :

DNS Domain:

Apply

Picture 29 - IPv6 Static IP network mode

9.9.2 VPN

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

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

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

- **L2TP**

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

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

When the VPN connection established, the VPN IP Address should be displayed in the VPN status. There may be the 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**

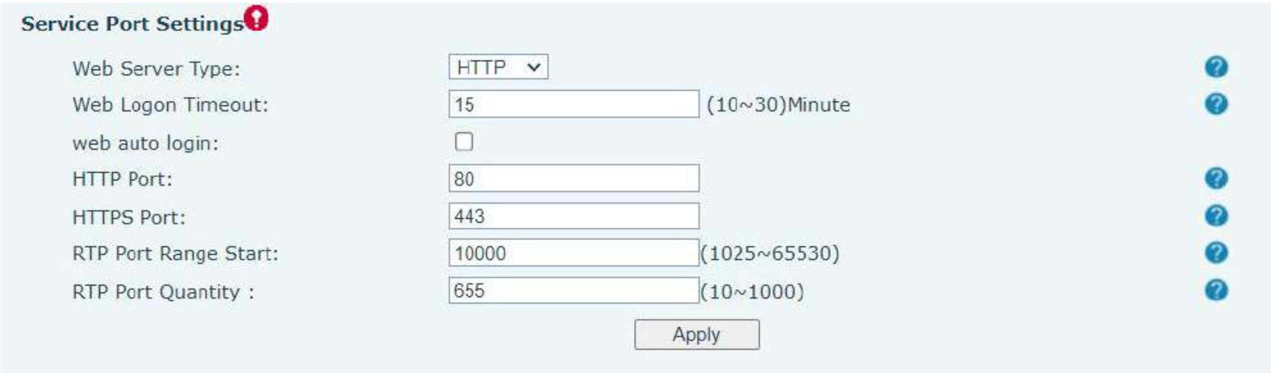
To establish an OpenVPN connection, user should get the following authentication and configuration files from the OpenVPN hosting provider and name them as the following,

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

User then upload these files to the device in the web page [**Network**] >> [**VPN**], select OpenVPN Files. Then user should check "Enable VPN" and select "OpenVPN" in VPN Mode and click "Apply" to enable OpenVPN connection. Same as L2TP connection, the connection will be established every time when system rebooted until user disable it manually.

9.10 Network >> Service Port

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



Service Port Settings

Web Server Type:	HTTP	
Web Logon Timeout:	15	(10~30)Minute
web auto login:	□	
HTTP Port:	80	
HTTPS Port:	443	
RTP Port Range Start:	10000	(1025~65530)
RTP Port Quantity :	655	(10~1000)

Picture 32 - Service Port Settings

Table 7 - Service port

Parameter	Description
Web Server Type	Reboot to take effect after settings. Optionally, the web page login is HTTP/HTTPS.
Web Logon Timeout	Default as 15 minutes, the timeout will automatically exit the login page, need to login again.
Web auto login	After the timeout does not need to enter a user name password, will automatically login to the web page.
HTTP Port	The default is 80. If you want system security, you can set ports other than 80. Such as :8080, webpage login: HTTP://ip:8080
HTTPS Port	The default is 443, the same as the HTTP port.
RTP Port Range Start	The value range is 1025 to 65535. The value of RTP port starts from the initial value set. For each call, the value of voice and video port is added 2.
RTP Port Quantity	Number of calls.

9.11 Network >> VPN

Users can configure a VPN connection on this page. See 9.9.2 VPN for more details.

9.12 Line >> SIP

Configure the Line service configuration on this page.

Table 8 - Line configuration on the web page

Parameters	Description
Register Settings	
Line Status	Display the current line status at page loading. To get the up to date line status, user has to refresh the page manually.
Activate	Whether the service of the line is activated
Username	Enter the username of the service account.
Authentication User	Enter the authentication user of the service account
Display Name	Enter the display name to be sent in a call request.
Authentication Password	Enter the authentication password of the service account
Realm	Enter the SIP domain if requested by the service provider
Server Name	Input server name.
SIP Server 1	
Server Address	Enter the IP or FQDN address of the SIP server
Server Port	Enter the SIP server port, default is 5060
Transport Protocol	Set up the SIP transport line using TCP or UDP or TLS.
Registration Expiration	Set SIP expiration date.
SIP Server 2	
Server Address	Enter the IP or FQDN address of the SIP server
Server Port	Enter the SIP server port, default is 5060
Transport Protocol	Set up the SIP transport line using TCP or UDP or TLS.
Registration Expiration	Set SIP expiration date.
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server.
Proxy Server Port	Enter the SIP proxy server port, default is 5060.
Proxy User	Enter the SIP proxy user.
Proxy Password	Enter the SIP proxy password.
Backup Proxy Server Address	Enter the IP or FQDN address of the backup proxy server.
Backup Proxy Server Port	Enter the backup proxy server port, default is 5060.
Basic Settings	
Dial Without Registered	Set call out by proxy without registration
DTMF Type	Set the DTMF type to be used for the line
DTMF SIP INFO Mode	Set the SIP INFO mode to send '*' and '#' or '10' and '11'
Request With Port	Whether the URI carries port number.
Use VPN	Set the line to use VPN restrict route
Use STUN	Set the line to use STUN for NAT traversal

Enable Failback	Whether to switch to the primary server when it is available.
Failback Interval	A Register message is used to periodically detect the time interval for the availability of the main Proxy.
Signal Failback	Multiple proxy cases, whether to allow the invite/register request to also execute failback.
Signal Retry Counts	The number of attempts that the SIP Request considers proxy unavailable under multiple proxy scenarios.
Codecs Settings	Set the priority and availability of the codecs by adding or remove them from the list.
System	
Enable Session Timer	Set the line to enable call ending by session timer refreshment. The call session will be ended if there is not new session timer event update received after the timeout period
Session Timeout	Set the session timer timeout period
Response Single Codec	If setting enabled, the device will use single codec in response to an incoming call request
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole opened
Keep Alive Interval	Set the keep alive packet transmitting interval
Keep Authentication	Keep the authentication parameters from previous authentication
User Agent	Set the user agent, the default is Model with Software Version.
Specific Server Type	Set the line to collaborate with specific server type
SIP Version	Set the SIP version
Local Port	Set the local port
Enable user=device	Sets user=device in SIP messages.
Use Tel Call	Set use tel call
Auto TCP	Using TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes
Enable Rport	Set the line to add rport in SIP headers
Enable PRACK	Set the line to support PRACK SIP message
DNS Mode	Select DNS mode, A, SRV, NAPTR
Enable Long Contact	Allow more parameters in contact field per RFC 3840
Enable Strict Proxy	Enables the use of strict routing. When the device receives packets from the server, it will use the source IP address, not the address in via field.
Use Quote in Display Name	Whether to add quote in display name, i.e. “Fanvil” vs Fanvil
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)

Caller ID Header	Set the Caller ID Header
Enable Feature Sync	Feature Sync with server
Enable SCA	Enable/Disable SCA (Shared Call Appearance)
Server Expire	Set the timeout to use the server.
TLS Version	Choose TLS Version.
Enable Click To Talk	With the use of special server, click to call out directly after enabling.
Flash mode	Chose Flash mode, normal or SIP info.
Flash Info Content-Type	Set the SIP info content type.
Flash Info Content-Body	Set the SIP info content body.
Enable MAC Header	When opening the registration, are IP package and user agent with MAC.
SIP Global Settings	
Strict Branch	Set up to strictly match the Branch field.
Enable Group	Set open group.
Enable RFC4475	Set to enable RFC4475.
Enable Strict UA Match	Enable strict UA matching.
Registration Failure Retry Time	Set the registration failure retry time.
Local SIP Port	Modify the device SIP port.

9.13 Line >> SIP Hotspot

Please refer to 9.6 SIP Hotspot

9.14 Line >> Basic Settings

Set up the register global configuration.

Table 9 - Set the line global configuration on the web page

Parameters	Description
STUN Settings	
Server Address	Set the STUN server address
Server Port	Set the STUN server port, default is 3478
Binding Period	Set the STUN binding period which can be used to keep the NAT pinhole opened.
SIP Waiting Time	Set the timeout of STUN binding before sending SIP messages
The TLS authentication	
TLS Certification File	Upload or delete the TLS certification file used for encrypted SIP

	transmission.

9.15 Line >> RTCP-XR

RTCP-XR mode is based on RFC3611 (RTP Control Extended Report), which can measure and evaluate network packet loss, delay and voice quality by sending RTCP-XR packets.

Table 10 - VQ RTCP-XR Settings

Parameters	Description
VQ RTCP-XR Settings	
VQ RTCP-XR Session Report	VQ report on whether session mode is enabled or not.
VQ RTCP-XR Interval Report	Whether to turn on Interval mode for VQ report sending.
Period for Interval Report(5~99)	The time interval at which VQ reports are sent periodically.
Warning threshold for Moslq(15~40)	When the device calculated the Moslq value x10 below the set threshold, a warning was issued.
Critical threshold for Moslq(15~40)	When the device calculates the Moslq value x10 below the set threshold, the critical report is issued.
Warning Threshold for Delay(10~2000)	When the one-way delay of the device is greater than the set threshold, warning is issued.
Critical Threshold for Delay(10~2000)	When the device computes that the one-way delay is greater than the set threshold, the critical report is issued.
Display Report Options on device	Whether to display the VQ report data of the last call on the device
Display Report Options on web	Whether to display the VQ report data for the last call through the web page.

9.16 device settings >> Features

Configuration device features.

Table 11 - General function Settings

Parameters	Description
Basic Settings	
Enable Auto Onhook	The device will hang up and return to the idle automatically at hands-free mode
Auto HangUp Delay	Specify Auto Onhook time, the device will hang up and return to the idle

	automatically after Auto Hand down time at hands-free mode, and play dial tone Auto Onhook time at handset mode
Enable Default Line	If enabled, user can assign default SIP line for dialing out rather than SIP1.
Enable Auto Switch Line	Enable device to select an available SIP line as default automatically
Default Ext Line	Select the default line to use for outgoing calls
Ban Outgoing	If you select Ban Outgoing to enable it, and you cannot dial out any number.
Enable CallLog	Select whether to save the call log.
Enable Restricted Incoming List	Whether to enable restricted call list.
Enable Restricted Outgoing List	Whether to enable the restricted allocation list.
Enable Country Code	Whether the country code is enabled.
Country Code	Fill in the country code.
Area Code	Fill in the area code.
Enable Number Privacy	Whether to enable number privacy.
Match Direction	Matching direction, there are two kinds of rules from right to left and from left to right.
Start Position	Open number privacy after the start of the hidden location.
Hide Digits	Turn on number privacy to hide the number of digits.
Allow IP Call	If enabled, user can dial out with IP address
P2P IP Prefix	Prefix a point-to-point IP call.
Restrict Active URI Source IP	Set the device to accept Active URI command from specific IP address.
Line Display Format	Custom line format: SIPn/SIPn: xxx/xxx@SIPn
SIP notify	When enabled, the device displays the information when it receives the relevant notify content.

9.17 device settings >> Media Settings

Change voice Settings.

Table 12 - Voice settings

Parameters	**Description**
Codecs Settings	Select enable or disable voice encoding: G.711A/U, G.722, G.729, G726, ILBC, opus，G.723.1
Audio Settings	

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 96~127.
Opus playload type	Set Opus load type, range 96~127.
ILBC Payload Type	Set the ILBC Payload Type, the value must be 96~127.
RTP Control Protocol(RTCP) Settings	
CNAME user	Set CNAME user
CNAME host	Set CNAME host
RTP Settings	
RTP keep alive	Hold the call and send the packet after 30s

9.18 device settings >> 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 device, 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 device to receive an RTP stream from pre-configured multicast listening address without involving SIP signaling. You can specify up to 10 multicast listening addresses.

Table 13 - Multicast parameters

Parameters	Description
Name	Listened multicast server name
Host: port	Listened multicast server's multicast IP address and port.

9.19 device settings >> Action

Action URL

Action urls are used for IPPBX systems to submit device events.

9.20 device settings >> Time/Date

The user can configure the time Settings of the device on this page.

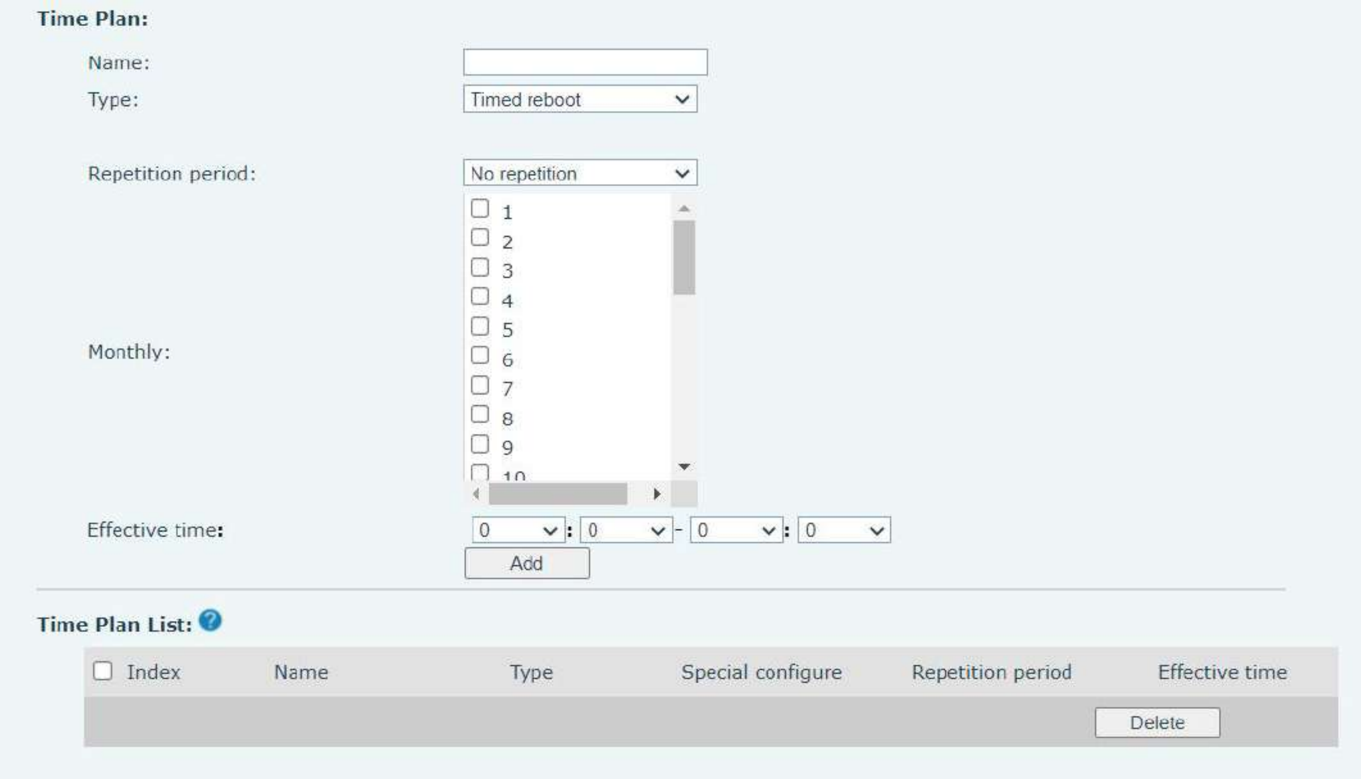
Table 14 - Time&Date settings

Parameters	Description
Network Time Server Settings	
Time Synchronized via SNTP	Enable time-sync through SNTP protocol
Time Synchronized via DHCP	Enable time-sync through DHCP protocol

Primary Time Server	Set primary time server address
Secondary Time Server	Set secondary time server address, when primary server is not reachable, the device will try to connect to secondary time server to get time synchronization.
Time Zone	Select the time zone
Resync Period	Time of re-synchronization with time server
12-Hour Clock	Set the time display in 12-hour mode
Date Format	Select the time/date display format
Daylight Saving Time Settings	
Local	Choose your local, device will set daylight saving time automatically based on the local
DST Set Type	Choose DST Set Type, if Manual, you need to set the start time and end time.
Fixed Type	Daylight saving time rules are based on specific dates or relative rule dates for conversion. Display in read-only mode in automatic mode.
Offset	The offset minutes when DST started
Month Start	The DST start month
Week Start	The DST start week
Weekday Start	The DST start weekday
Hour Start	The DST start hour
Minute Start	The DST start minute
Month End	The DST end month
Week End	The DST end week
Weekday End	The DST end weekday
Hour End	The DST end hour
Minute End	The DST end minute
Manual Time Settings	You can set your time manually

9.21 device settings >> Time Plan

Time Plan (time management) settings can set a time point or a time period. The time point is to perform an action at a certain time, and the time period is to perform an action for a certain period of time.



Time Plan:

Name:

Type: Timed reboot

Repetition period: No repetition

Monthly: □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10

Effective time: 0 : 0 - 0 : 0

Add

Time Plan List:

□ Index	Name	Type	Special configure	Repetition period	Effective time

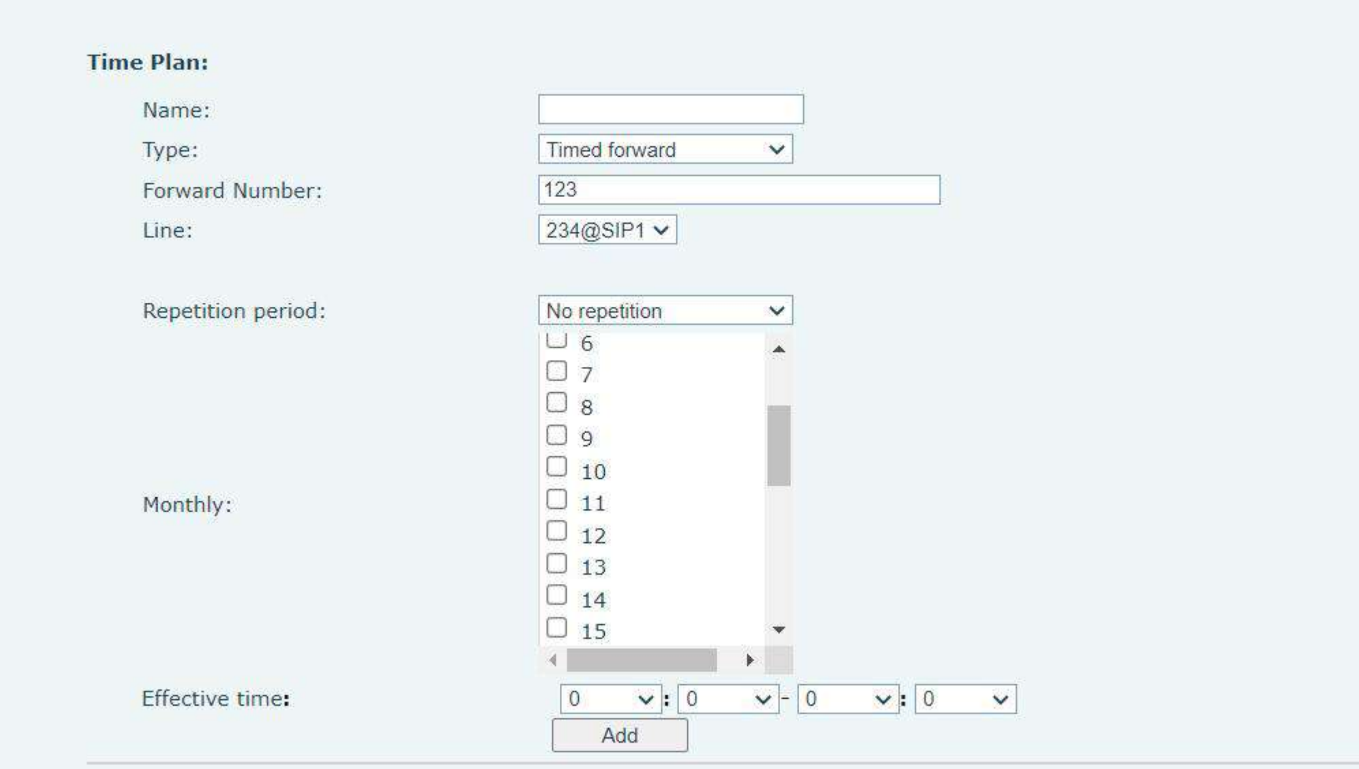
Delete

Picture 33 - Time Plan (1)

Table 15 - Time Plan

configure	Value	Description
Time plan Type	1：Timed reboot 2：Timed upgrade 3：Timed forward 4：Timed config	Type，Action performed at a time point/time period
Repetition periodRepetition period	0：No repetition 1：Daily 2：Weekly 3：Monthly	repeat type
in weeks	0-6 ：Sunday-Saturday, supports multiple separated by ";" 1-31：1-31 day	When the repetition type is daily/non-repeating, the value is empty
in days	xx:xx-xx:xx	start time - end time period

When the Time Plan type is selected as timed forwarding, the webpage will prompt to enter the forwarding number and forwarding line, as shown in the figure.



Time Plan:

Name:

Type: Timed forward

Forward Number: 123

Line: 234@SIP1

Repetition period: No repetition

Monthly: □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15

Effective time: 0 : 0 - 0 : 0

Picture 34 - Time Plan (2)

Forwarding Number: Configure the forwarding number to forward to the number within the set time period.

Line: Forward the specified line, when the line is set to a certain line, it will only take effect for this line.

1. Timed forwarding rules:

1) When there is forwarding under the line, the forwarding number under the line is used; when there is no forwarding number under the SIP line, when there is an incoming call within the time period set by the scheduled forwarding, the device will be forwarded to the specified scheduled forwarding number; when outside the time period, no forwarding is performed. That is, the priority Line>Time Plan.

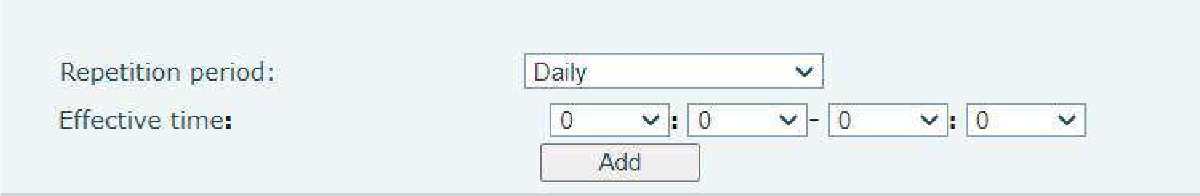
2) All scheduled forwarding types are unconditional forwarding.

9.21.1 Repeat Period Select Daily

Select daily as the repetition period, and enter any time in the date format from 00:00 to 23:59 in the effective time input box.

The first and third input boxes only allow input of any integer from 00 to 23, and 0 is automatically added before inputting an integer less than 10.

The second and fourth input boxes only allow input of any integer from 00 to 59, and 0 is automatically added before inputting an integer less than 10.



Repetition period: Daily

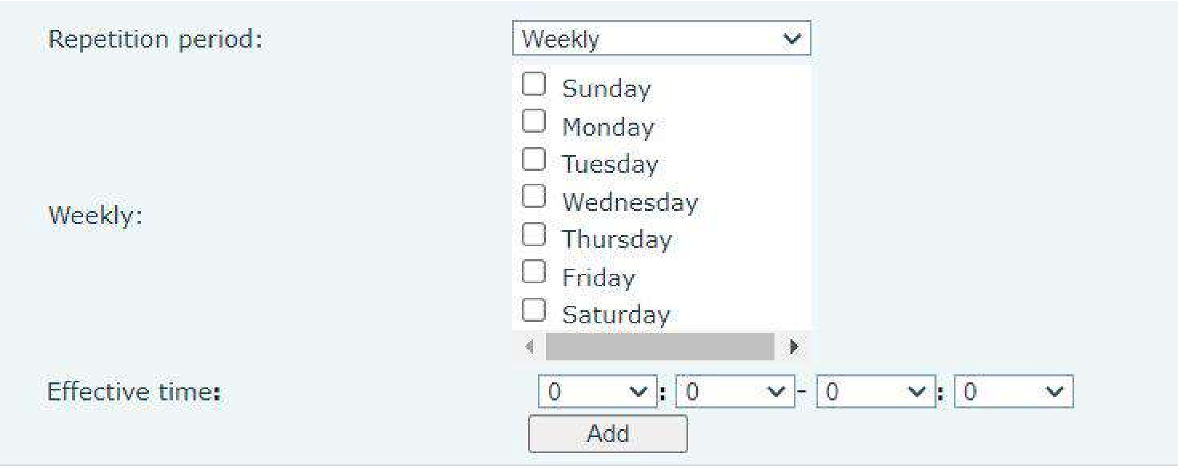
Effective time: 0 : 0 - 0 : 0

Picture 35 - Time Plan (3)

9.21.2 Repeat Period Select Weekly

Day of the week selection box, check it to take effect.

The final effective time is the combination of the day of the week and the set time.



Repetition period: Weekly

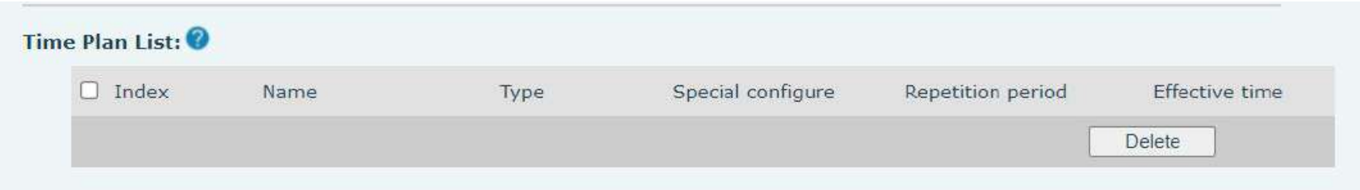
Weekly:
☐ Sunday
☐ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday

Effective time: 0 : 0 - 0 : 0

Picture 36 - Time Plan (4)

9.21.3 Time Plan List

All configurations submitted after the configuration is submitted are displayed in a list, and the order is sorted by week (day, Monday, Tuesday...), and if the week is the same, it is sorted by time (time from small to large). The function sequence is restarted first and then upgraded.



Time Plan List:

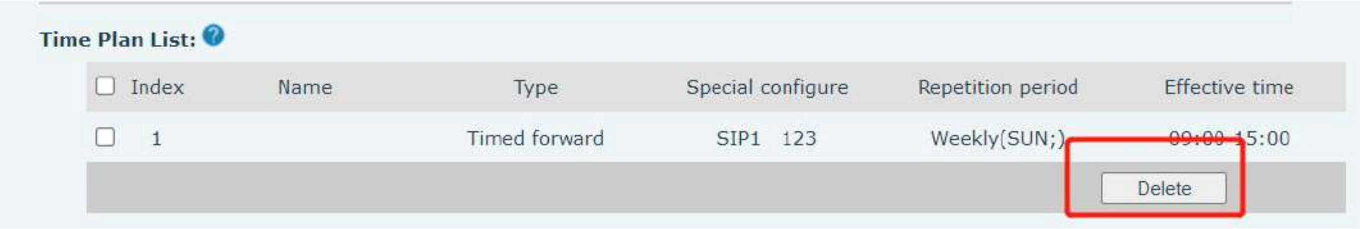
☐ Index	Name	Type	Special configure	Repetition period	Effective time

Picture 37 - Time Plan (5)

9.21.4 Delete

Check the box before the serial number, click to select all configuration items in the list.

Click Delete to delete the checked configuration in the configuration list, and it will become invalid after deletion.



Time Plan List:

□ Index	Name	Type	Special configure	Repetition period	Effective time
□ 1		Timed forward	SIP1 123	Weekly(SUN;)	09:00-15:00

Picture 38 - Time Plan (6)

9.22 Intercom Settings>> Channel Settings

Users can configure an analog channel or digital channel for the gateway through this page.

- **Digital channel**

When the channel type is set to a digital channel, the device can communicate with the digital intercom.

- Transmission frequency: You can fill in the port emitting frequency. When the receiving frequency of the intercom is consistent with the transmission frequency of the gateway, you can receive the gateway sending
- Receive frequency: You can fill in the receiving frequency of the gateway. When the transmission frequency of the intercom is consistent with the receiving frequency of the gateway, it can be sent to the gateway
- Power: Choose high/low, high power communication distance, low -power communication distance, short power use power consumption than low power than low power
- Time slot: The gateway slot can be set. DMR divides the 12.5K Hertz channel into two alternate time slots. Users can choose any temporary clearance for voice calls and data transmission.
- Colour code: Settings can be set. Users who need to communicate with each other must be set to the same color code, and the terminals do not respond to channel activities that do not match the preset color code.

- **Analog channel**

When the channel type is set to analog channel, the device can communicate with the analog intercom.

- Transmission frequency: You can fill in the port emitting frequency. When the receiving frequency of the intercom is consistent with the transmission frequency of the gateway, you can receive the gateway sending
- Receive frequency: You can fill in the receiving frequency of the gateway. When the transmission frequency of the intercom is consistent with the receiving frequency of the gateway, it can be sent to the gateway
- Power: Choose high/low, high power communication distance, low -power communication distance,

short power use power consumption than low power than low power

- Recv/Send Sub Tone: You can set the receiving and sending Asian sounds as CTCSS/CDCSS.
- Channel Spacingl: Broadband (25kHz) or narrowband (12.5kHz) can be selected

9.23 Intercom Settings>> Call and VAD detection function

Users can set some parameters on this page, including VAD -related parameters.

Table 16 - Call and VAD detection function

Parameter	Description
Call and VAD detection function	
Transfer Number	Set the intercom machine number to call the machine number, you can set the SIP number and the broadcast address
Call Timeout	Set the call timeout and unsolved gateway hanging time
Voice Silence Check	Set the silent detection time. If the unmanned voice of the SIP end exceeds the configuration parameter, it will think that the line is mute and releases the SIP terminal
VAD Accurcy	Set the time parameter to analyze whether there is no sound within the duration of the configuration parameter on the SIP side, and the sound is forwarded to the intercom.
Voice Prompt	
Answer Prompt	Whether to enable an answer prompt
Release Prompt	Whether to enable the release prompt

9.24 Call List

- Restricted Incoming Calls:

It is similar like a Blocked List. Add the number to the Blocked List, and the user will no longer receive calls from the stored number until the user removes it from the list.

Users can add specific Numbers to the Blocked List or add specific prefixes to the Blocked List to block calls with all Numbers with this prefix.

- Restricted Outgoing Calls:

Adds a number that restricts outgoing calls and cannot be called until the number is removed from the table.

9.25 Call Log

Users can browse the complete call records on this page. Call records can be named according to the main call number, the call number is called, and the time or length of time can be sorted. You can also screen the call records through the call record type (the SIP side actively call or intercom).

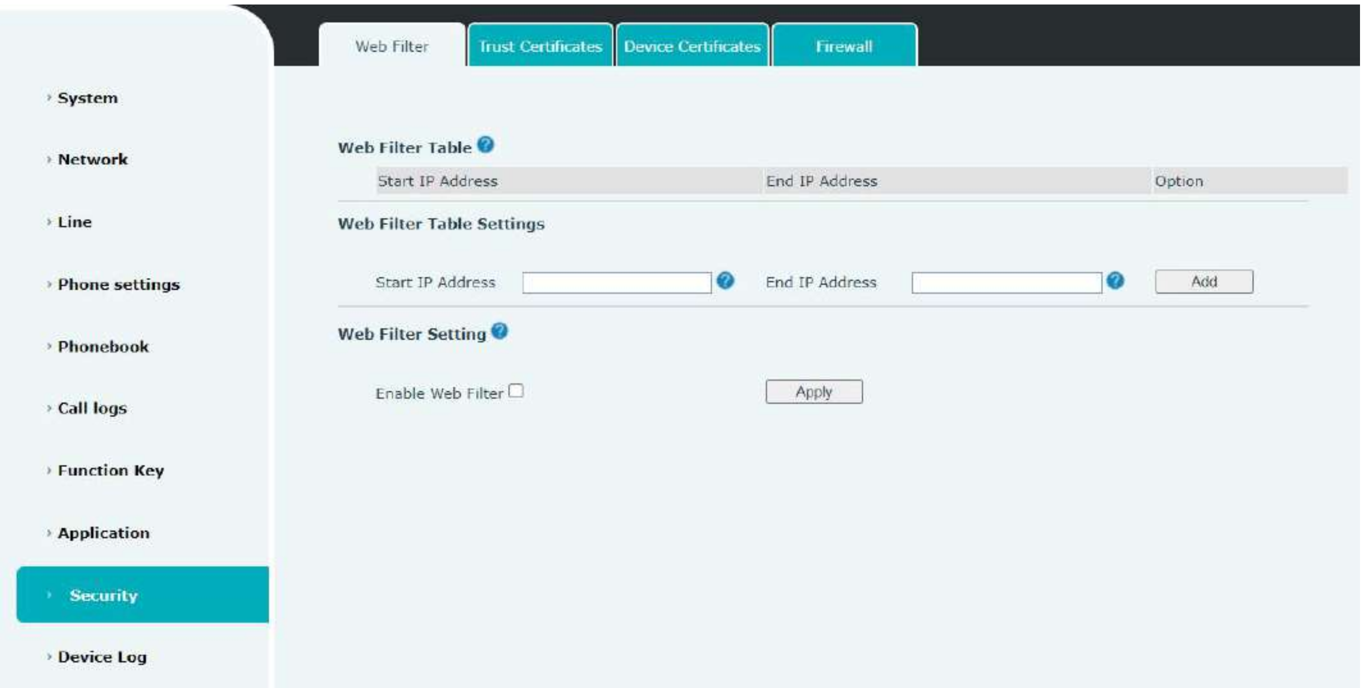
Users can also add the SIP number in the call record to the blocked List.

9.26 Application >> Manage Recording

See 8.1 Record for details of recording.

9.27 Security >> Web Filter

The user can set up a configuration management device that allows only machines with a certain network segment IP access.



Web Filter Table

Start IP Address	End IP Address	Option

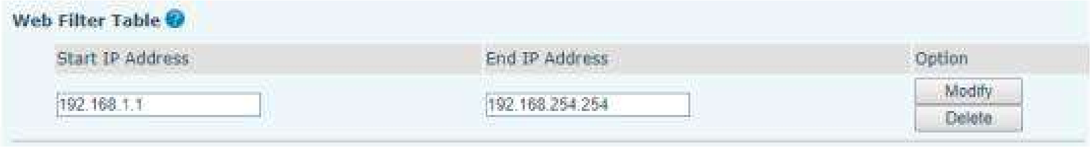
Web Filter Table Settings

Start IP Address ____ End IP Address ____ Add

Web Filter Setting

Enable Web Filter □ Apply

Picture 39 - Web Filter settings



Web Filter Table

Start IP Address	End IP Address	Option
192.168.1.1	192.168.254.254	Modify Delete

Picture 40 - Web Filter Table

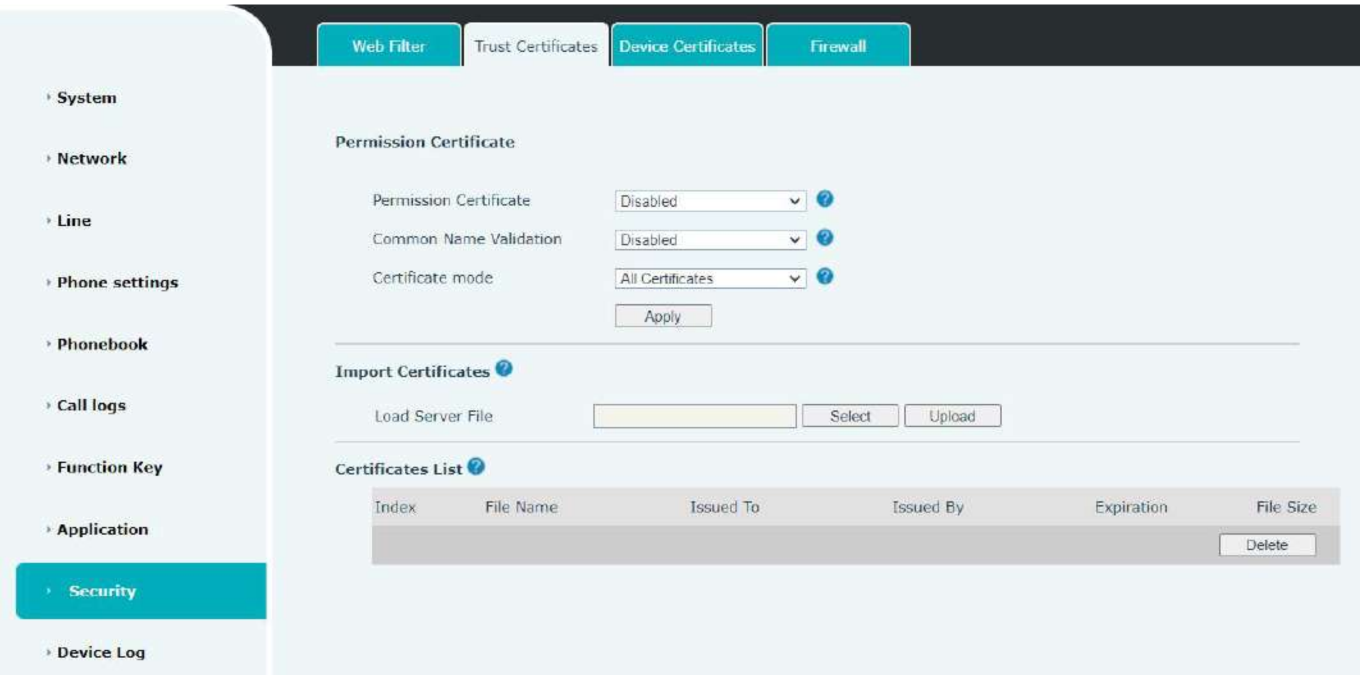
Adding and removing IP segments are accessible. Configure the starting IP address within the start IP, end the IP address within the end IP, and click [**Add**] to submit to take effect. A large network segment can be set, or it can be divided into several network segments to add. If the user wants to delete, 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 device, please do not configure the filter segment of the web page to be outside your own network segment, otherwise you will not be able to log in the web page.

9.28 Security >> Trust Certificates

Set whether to open license certificate and general name validation, select certificate module. You can upload and delete uploaded certificates.



Permission Certificate

Permission Certificate	Disabled
Common Name Validation	Disabled
Certificate mode	All Certificates

Import Certificates

Load Server File

Certificates List

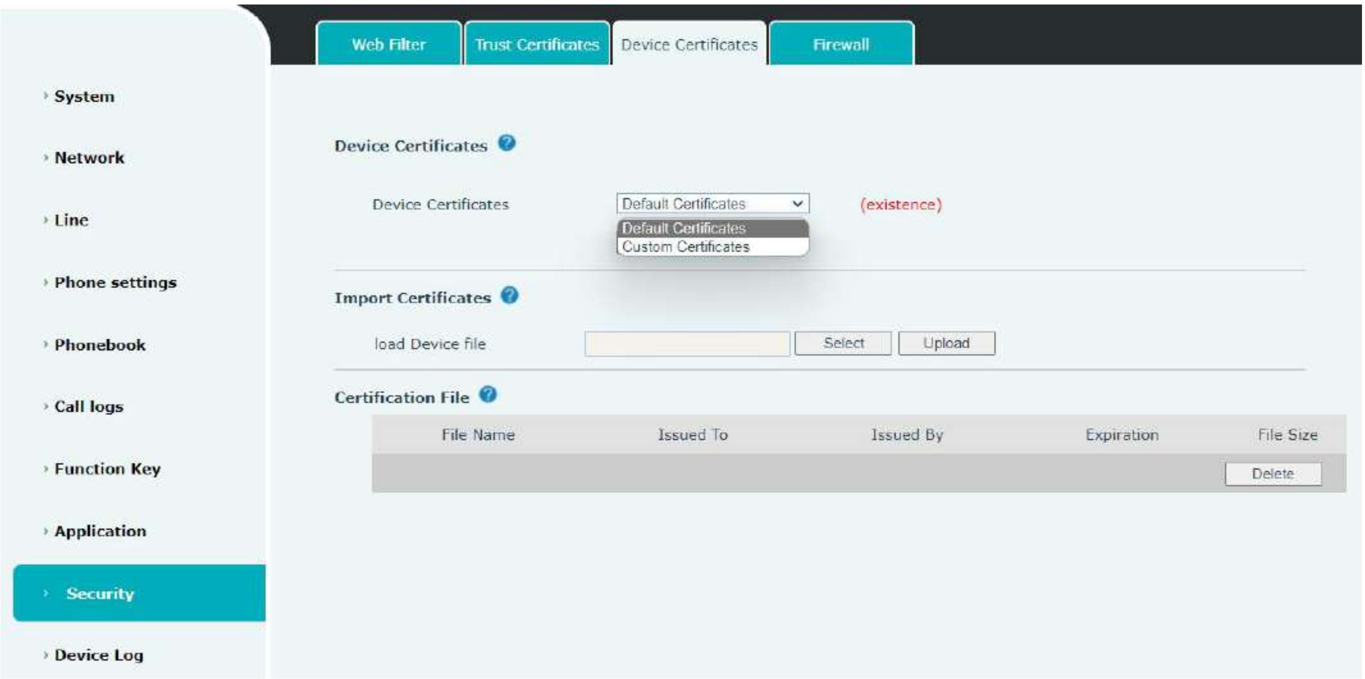
Index	File Name	Issued To	Issued By	Expiration	File Size

Picture 41 - Certificate of settings

9.29 Security >> Device Certificates

Select the device certificate as the default and custom certificate.

You can upload and delete uploaded certificates.



Device Certificates

Device Certificates: Default Certificates (existence)

Default Certificates
Custom Certificates

Import Certificates

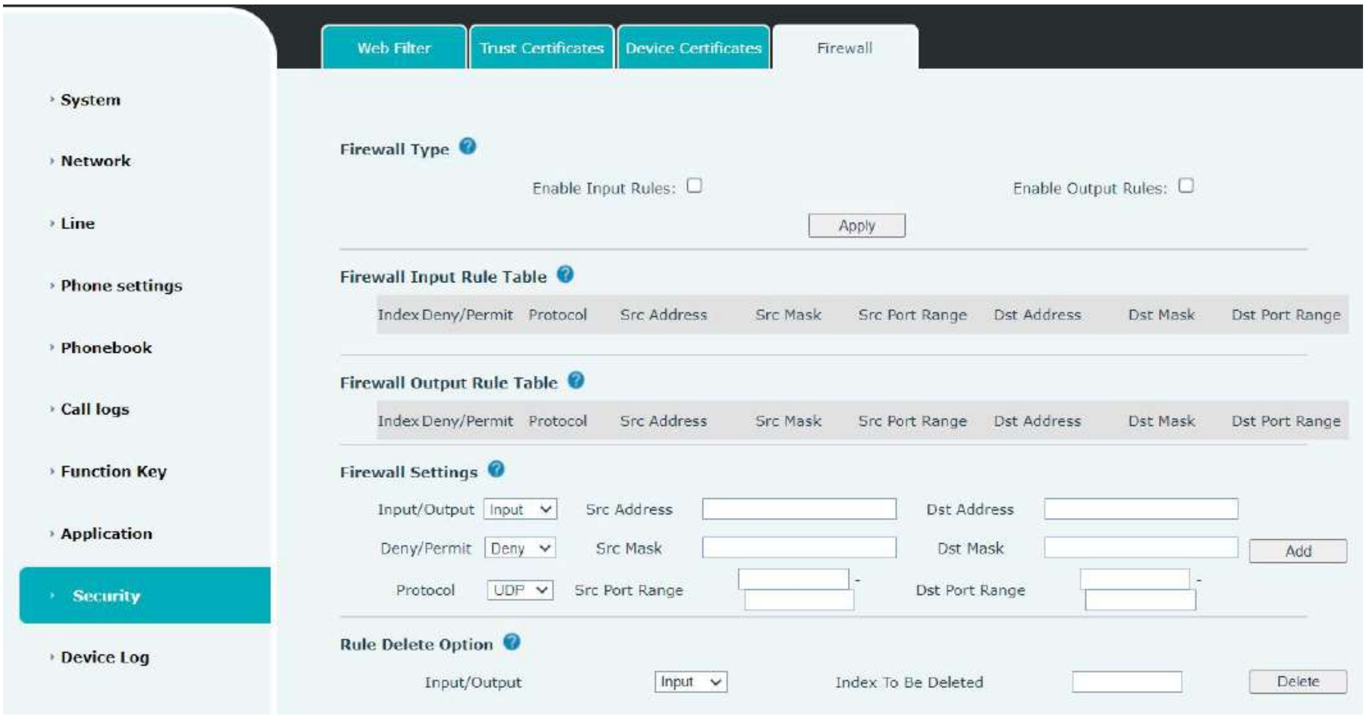
load Device file

Certification File

File Name	Issued To	Issued By	Expiration	File Size

Picture 42 - Device certificate setting

9.30 Security >> Firewall



Firewall Type

Enable Input Rules: □ Enable Output Rules: □

Firewall Input Rule Table

Index	Deny/Permit	Protocol	Src Address	Src Mask	Src Port Range	Dst Address	Dst Mask	Dst Port Range

Firewall Output Rule Table

Index	Deny/Permit	Protocol	Src Address	Src Mask	Src Port Range	Dst Address	Dst Mask	Dst Port Range

Firewall Settings

Input/Output: Input Src Address Dst Address

Deny/Permit: Deny Src Mask Dst Mask

Protocol: UDP Src Port Range - Dst Port Range -

Rule Delete Option

Input/Output: Input Index To Be Deleted

Picture 43 - Network firewall Settings

The user can set whether to enable the input through this page, output firewall and set the firewall input and output rules. Using these Settings can prevent some malicious network access, or restrict internal users access to some resources of the external network, which can improve security.

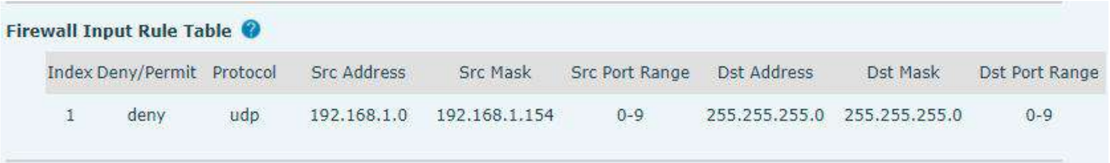
Firewall rule set is a simple firewall module. This feature supports two types of rules: input rules and output rules. Each rule is assigned an ordinal number, allowing up to 10 for each rule.

Considering the complexity of firewall Settings, the following is an example to illustrate:

Table 17 - Network Firewall

Parameter	**Description**
Enable Input Rules	Indicates that the input rule application is enabled.
Enable Output Rules	Indicates that the output rule application is enabled.
Input/Output	To select whether the currently added rule is an input or output rule.
Deny/Permit	To select whether the current rule configuration is disabled or allowed;
Protocol	There are four types of filtering protocols: TCP | UDP | ICMP | IP.
Src Port Range	Filter port range
Src Address	Source address can be host address, network address, or all addresses 0.0.0.0; It can also be a network address similar to *.*.*.0, such as: 192.168.1.0.
Dst Address	The destination address can be either the specific IP address or the full address 0.0.0.0; It can also be a network address similar to *.*.*.0, such as: 192.168.1.0.
Src Mask	Is the source address mask. When configured as 255.255.255.255, it means that the host is specific. When set as 255.255.255.0, it means that a network segment is filtered.
Dst Mask	Is the destination address mask. When configured as 255.255.255.255, it means the specific host. When set as 255.255.255.0, it means that a network segment is filtered.

After setting, click [**Add**] and a new item will be added in the firewall input rule, as shown in the figure below:



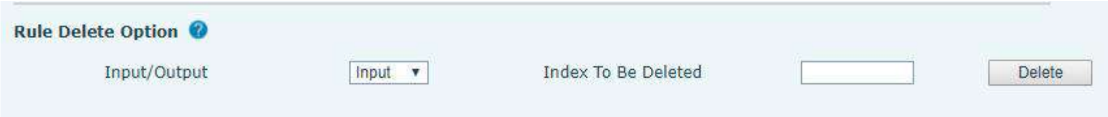
Firewall Input Rule Table

Index	Deny/Permit	Protocol	Src Address	Src Mask	Src Port Range	Dst Address	Dst Mask	Dst Port Range
1	deny	udp	192.168.1.0	192.168.1.154	0-9	255.255.255.0	255.255.255.0	0-9

Picture 44 - Firewall Input rule table

Then select and click the button [**Apply**].

In this way, when the device is running: ping 192.168.1.118, the packet cannot be sent to 192.168.1.118 because the output rule is forbidden. However, the other IP of the ping 192.168.1.0 network segment can still receive the response packet from the destination host normally.



Rule Delete Option

Input/Output: Input

Index To Be Deleted:

Picture 45 - Delete firewall rules

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

9.31 Device Log >> Device Log

You can grab the device log, and when you encounter an abnormal problem, you can send the log to the technician to locate the problem. See 10.5 Get log information.

10 Trouble Shooting

When the device is not in normal use, the user can try the following methods to restore normal operation of the device or collect relevant information and send a problem report to Fanvil technical support mailbox.

10.1 Get Device System Information

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

10.2 Reboot Device

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

10.3 Reset Device to Factory Default

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

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

10.4 Network Packets Capture

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

10.5 Get Log Information

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

10.6 U disk/TF card upgrade

When the W712 fails to use the webpage to upgrade, you can try to upgrade through the U disk/TF card upgrade. What you need to upgrade is the suffix name of the suffix .z, copy this file to the root directory. Note that the format needs to be FAT/ FAT32/ EXT3/ 4/ Squashfs

Enter the upgrade mode step:

1) Insert U disk/TF card containing upgrade files

2) Press the RESET key in the green LED light flash in the equipment on the equipment to observe the LED light to become a slow flash state

3) Successful entering the upgrade mode, the equipment green LED light will become flash. At this time, the device will automatically select the upgrade file in the U disk. After finding it, the equipment will be upgraded. After completion, the device will automatically restart.

4) If the U disk and TF card are stored and inserted both, check the U disk first, then check the TF card

10.7 Common Trouble Cases

Table 18 - Trouble Cases

Trouble Case	**Solution**
Device could not boot up	1. The device is powered by external power supply via power adapter or POE switch. Please use standard power adapter provided or POE switch met with the specification requirements and check if device is well connected to power source. 2. If the device enters "POST mode" (the SIP/NET and function button indicators are always on), the device system is damaged. Please contact your location technical support to help you restore your equipment system.
Device could not register to a service provider	1. Please check if the device is connected to the network. 2. 2. If the network connection is good, please check your line

	configuration again. If all configurations are correct, contact your service provider for support, or follow the instructions in "12.4 Network Data Capture" to obtain a registered network packet and send it to the Support Email to help analyze the issue.