



FH-S01 User Manual

Software Version: 1.0.0

Release Date: 2022.8.24





Directory

Directory	••••••••••	1
1 Picture		2
2 Table	错误!	未定义书签。
3 Safety Instruction	•••••	1
4 Overview	••••••	3
5 Install Guide	•••••	4
5.1 Use POE or external Power Adapter		4
5.2 Appendix		
5.2.1 LED Status		
6 User Guide	•••••	6
6.1 Interface description		6
6. 2 Installation instructions		
6.2.1 Peripheral connection		6
6.2.2 Installation Method		7
6.2.3 Device IP address		8
6.3 WEB configuration		
6.4 SIP Configurations		8
6. 5 Volume setting		9
7 Basic Function		11
7.1 Answering Calls		11
7.2 Auto Answer		11
7.3 Call Waiting		12
8 Advance Function	,	14
8.1 Intercom		14
8.2 MCAST		
8.3 Hotspot		
9 Web Configurations	••••••	18
9.1 Web Page Authentication		
9.2 System >> Information		
9.3 System >> Account		19
9.4 System >> Configurations		19
9. 5 System >> Upgrade		20
9.6 System >> Auto Provision		
9.7 System >> FDMS		
		1



9.8 System >> Tools	
9.9 Network >> Basic	
9.10 Network >> service port	27
9.11 Network >> VPN	
9.12 Network >> Advanced	
9.13 Lines >> SIP	
9.14 Lines >> SIP Hotspot	
9.15 Line >> Action Plan	
9.16 Line >> Basic Settings	
9.17 Intercom settings >> Features	41
9.18 Intercom settings >> Media Settings	
9.19 Intercom Setting >> MCAST	45
9.20 Intercom Setting >> Action URL	
9.21 Intercom Setting >> Time/Date	
9. 22 Intercom settings>>Time plan	
9.23 Intercom settings >> Tone	
9.24 Call List >> Call List	
9. 25 Call List >> Web Dial	49
9.26 Security >> Web filter	49
9. 27 Security >> Trust Certificates	50
9. 28 Security >> Device Certificates	
9.29 Security >> Firewall	51
9.30 Device Log	
9.31 Security settings	
10 Trouble Shooting	57
10.1 Get device system information	
10.2 Reboot device	57
10.3 Device factory reset	
10.4 Network Packets Capture	57
10.5 Get device log	
10.6 Common Trouble Cases	



1 Picture

Picture 1	- Interface display	6
Picture 2	- DC power supply peripheral connection mode	7
Picture 3	- POE power supply peripheral connection mode	7
Picture 4	- WEB Login	8
Picture 5	- SIP Line Configuration	9
Picture 6	- Volume Set	10
Picture 7	- WEB line enable auto answer	. 11
Picture 8	- Enable auto answer for IP calls	.12
Picture 9	- Call Waiting	13
Picture 10	- Call Waiting tone	13
Picture 11	- WEB Intercom Settings	14
Picture 12	- MCAST Setting	.15
Picture 13	- SIP hotspot	17
Picture 14	- WEB Account	19
Picture 15	- System Setting	19
Picture 16	- Upgrade Settings	.20
Picture 17	- Online upgrade settings	21
Picture 18	- Auto provision Settings	.22
Picture 19	- FDMS	.25
Picture 20	- Tools	.25
Picture 21	- Network Basic Setting	26
Picture 22	- Service port setting interface	27
Picture 23	- Network VPN	.28
Picture 24	- Network Setting	30
Picture 25	- SIP Settings(1)	32
Picture 26	- SIP Settings(2)	32
Picture 27	- SIP Settings(3)	33
Picture 28	- SIP Settings(4)	33
Picture 29	- SIP Settings(5)	34
picture 30	- Action plan	39
picture 31	- Network Basic	.40
picture 32	- Line Basic Setting	40
picture 33	- Features	41
picture 34	- Media Settings	.43
picture 35	- Action URL	.45
picture 36	- Time/Date	.46



picture 37	- Time plan	47
picture 38	- Tone	. 48
picture 39	- Web Dial	49
picture 40	- WEB filter	. 49
picture 41	-Trust Certificates	. 50
picture 42	- Device Certificates	.51
picture 43	- Firewall	51
picture 44	- Firewall rules list	52
picture 45	- Delete firewall rules	. 53
picture 46	- Security settings (1)	. 53
picture 47	- Security settings (2)	. 54
picture 48	- Security settings (3)	. 54



2 Table

Table 1	- LED Status
Table 2	- Interface description
Table 3	- Intercom description
Table 4	- MCAST parameter 15
Table 5	- SIP Hotspot16
Table 6	- Firmware upgrade21
Table 7	- Auto provision Settings
Table 8	- FDMS Information
Table 9	- Basic Setting Parameters
Table 10	- Server Port
Table 11	- Network Basic Setting Paramater
Table 12	- SIP Settings
Table 13	- Action Plan
Table 14	- Line Basic Setting40
Table 15	- Features41
Table 16	- Media Settings
Table 17	- Time & Date settings
Table 18	- Time plan
Table 19	- Web Firewall
Table 20	- Security Settings
Table 21	- Trouble Cases



3 Safety Instruction

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

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



4 Overview

FH-S01 is a SIP ceiling speaker featuring paging, multicasting, broadcasting and talkback functionalities. It supports up to 10 multicast zones with prioritization.

It delivers high-intelligibility performance with G.722&Opus codecs. Adopted standard SIP 2.0(RFC3261) and related RFC protocols, it has strong compatibility and scalability.

FH-S01 has a built-in microphone, which supports monitoring and intercom applications. At the same time, Audio power up to 15W with built-in class D amplifier; Support customize the WAV file for emergency notification and alarm; It has the function of linkage security alarm equipment, and Support remote configuration via web page and auto-provisioning; It has 100M Ethernet and can adapt to 10/100 Mbps Ethernet, Integrated PoE(IEEE 802.3af, class 0),Ideal for school, office, station, retail, factory, etcetc.



5 Install Guide

5.1 Use POE or external Power Adapter

FH-S01, supports two power supply modes, power supply from external power adapter or over Ethernet (POE) complied switch.

POE power supply saves the space and cost of providing the device additional power outlet. With a POE switch, the device can be powered through a single Ethernet cable which is also used for data transmission. By attaching UPS system to POE switch, the device can keep working at power outage just like traditional PSTN telephone which is powered by the telephone line.

For users who do not have POE equipment, the traditional power adaptor should be used. If the device is connected to both POE switch and external power adapter, FH-S01 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 supplied by Fanvil and the POE switch met the specifications to ensure the device work properly.

5.2 Appendix

5.2.1 LED Status

Туре	Status	description	
		When the call is ringing, the LED light	
	Rina	will flash slowly. It supports four states:	
		ON、OFF、Fastblink and Slowblink .	
Status Light		Default Slowblink, settable	
	In Usina	The display status of the LED light in the	
		call or dialing status. It supports four	
		states: ON、OFF、Fastblink and	
		Slowblink . Default OFF, settable	
	Network Abnormal	When the network is in an abnormal	

Table 1 - LED Status

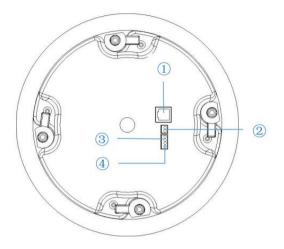


Туре	Status	description
		state, the indicator flashes once every
		second. It supports four states: ON_{n}
		$OFF_{\mathbf{v}}$ Fastblink and Slowblink . Default
		Fastblink, settable
		SIP registered successfully in normal
		standby state.The device supports four
	SIP Register Success	states: ON、OFF、Fastblink and
		Slowblink ,Default OFF, settable
		When the SIP registration fails, the LED
	SIP Register Fail	light flashes once every second. It
		supports four states: ON、OFF、Fastblink
		and Slowblink. Default Fastblink,
		settable



6 User Guide

6.1 Interface description



Picture 1 - Interface display

 Table 2 - Interface description

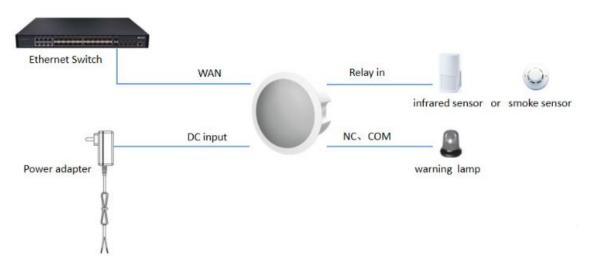
Number	Name	Description	
	Ethernet	standard RJ45 interface, 10/100M adaptive,	
1	interface	support PoE powered, it is recommended to	
	Internate	use CAT5 or CAT5E network cable.	
2	Power interface	18V/2A input	DC OC+ DC-
3	1 set of short-circuit input interface	input devices for connecting switches, infrared sensor, door sensor, vibration sensors etc.	Relay input
4	1 set of short-circuit output interface	corresponding to the short-circuit input interface, login device web page settings, can be connected to electric alarms etc	Logic COM NC

6.2 Installation instructions

6.2.1 Peripheral connection

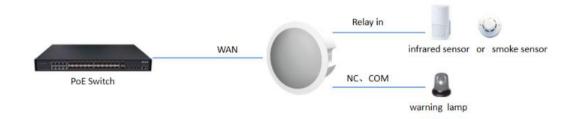
DC power supply connection mode:





Picture 2 - DC power supply peripheral connection mode

POE power supply connection mode:



Picture 3 - POE power supply peripheral connection mode

6.2.2 Installation Method

The device supports ceiling type installation

- Ceiling Installation
- **Step 1**: Make a circular hole on the pre installation position of the ceiling that can accommodate the cylinder at the back end of the ceiling speaker.
- Step 2: Turn out the four buckles of the ceiling speaker and press down to eject the net cover.

Step 3: Turn back the buckle, insert the Ceiling Speaker into the ceiling from the round hole drilled before, turn out the buckle, press the back of the ceiling, and tighten the screws corresponding to the buckle.

Step 4: Reinstall the speaker net cover and complete the installation.

Step 5: If other input/output devices need to be connected externally, connect to the host through the connecting tail line.



Step 6: Power on test, plug in the Internet cable and power supply, and the indicatorlightof the equipment is on, indicating that the power supply is connectednormally.

6.2.3 Device IP address

Open the web page and enter http://download.fanvil.com/tool/iDoorPhoneNetworkScanner.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.

IDoorPhoneNetworkScanner V1.0.2

	IP	Model	MAC	Version	Description
Γ	172.16.7.134	FH-S01	00:d8:4a:03:d1:4c	1.0.0	IP Paging Gatewa

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/ and you can see the login interface of the web page management.

User:	admin	
Password:	•••••	
Language:	English	•
	Logon	

Picture 4 - 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 <u>9 Web Configurations</u>

6.4 SIP Configurations

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



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

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

System				
Network	Line 5789@SIP 🗸			
	Register Settings >>			
Line	Line Status:	Registered	Activate:	Ø
	Username:	5789	Authentication User:	
intercom settings	Display name:	0	Authentication Password:	
	Realm:	0	Server Name:	
Call List				
	SIP Server 1:		SIP Server 2:	
unction Key	Server Address:	172.16.1.2	Server Address:	
	Server Port:	5060	Server Port:	5060
ecurity	Transport Protocol:		Transport Protocol:	
	Registration Expiration:	3600 second(s)	Registration Expiration:	3600 second(s)
evice Log				becond(b)
	Proxy Server Address:	0	Backup Proxy Server Address:	
ecurity Settings	Proxy Server Port:	5060	Backup Proxy Server Port:	5060
	Proxy User:	0		
	Proxy Password:	0		
		L		

Picture 5 - SIP Line Configuration

6.5 Volume setting

[Intercom Settings] >> [Media Settings] >> [Media Settings], as shown below, click [Submit].

Hands-free volume setting: Set the speaker output volume.

Hands-free microphone gain: microphone volume level.



	Features Media Settings	Camera Settings MCA	ST Action	Time/Date T
stem				
twork	Codecs Settings >> 🕜			
	Media Settings >>			
ne	Default Ring Type:	1.wav 🗸 🕜		
	Speakerphone Volume:	7 (0~9) 🕜		
ntercom settings	Speakerphone Ring Volume:	3 (0~9) 🕜		
CENTRAL CONTRAL	Speakerphone SignalTone Volume:	3 (0~9)		
ll List	DTMF Payload Type:	101 (96~127) 🥝		
	Handfree Mic Gain:	3 (1~9)		
nction Key	OPUS Payload Type:	107 (96~127)	OPUS Sample Rate	OPUS-NB(🛩
	ILBC Payload Type:	97 (96~127) 🕜	ILBC Payload Length	20ms 🗸 🕜
curity	Enable VAD:			
	Disable AEC:			
vice Log	Audio Profile:	PoE 🗸		
	H.264 Payload Type:	117 (96~127)		
curity Settings	Enable Line-in:	Disable 🗸 🤇		
	Enable Line-out:	Disable 🗸 🥝		
	Speaker:	Panel Spea 🗸	External Speaker Power:	8Ω5w 🗸 😯
	Video Direction:	sendonly ~		

Picture 6 - Volume Set



7 **Basic Function**

7.1 Answering Calls

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

7.2 Auto Answer

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

• Web interface:

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

	SIP SIP Hots	pot	Action Plan Basic Se	ettings		
System						
vetwork	Line 5789@SIP V					
Line	Register Settings >> Basic Settings >>					
tercom settings	Enable Auto Answering:	Ø] [Auto Answering Delay:	0	(0~120)second(s) ဈ
all List	Enable Hotline: Hotline Delay:	0	(0~9)second(s) 🥝	Hotline Number:		0
nction Key	Dial Without Registered: DTMF Type: Request With Port:		∽ Ø	DTMF SIP INFO Mode:	Send 10/11	✓
urity	Use STUN:			Use VPN:	•	
ce Log	Enable Failback: Failback Interval:	✓ ✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓✓<	second(s) 💡	Signal Failback: Signal Retry Counts:	3	(1~10) 🕑
urity Settings	Codecs Settings >> 🕜					
	Advanced Settings >>					
	Advanced Settings >> SIP Global Settings >>		Apply			

Picture 7 - WEB line enable auto answer

• SIP P2P auto answering:

Enter [Line]>>[Basic settings]>> [SIP P2P Settings], Enable auto answer and set auto answer time and click submit.



	SIP SIP Hotspot	Action Plan Basic	Settings	
em				
vork	STUN Settings			
VOLK	STUN NAT Traversal:	FALSE		0
	Server Address:			0
Line	Server Port:	3478		0
	Binding Period:	50	second(s)	0
rcom settings	SIP Waiting Time:	800	millisecond	Ø
List		Apply		
ction Key	SIP P2P Settings			
V 40 (710020)	Enable Auto Answering			0
rity	Auto Answering Delay:	0	(0~120)second(s)	Ø
	DTMF Type:	RFC2833 ¥		0
	DTMF SIP INFO Mode:	Send 10/11 🗸		C
vice Log surity Settings		Apply		

Picture 8 - Enable auto answer for IP calls

• Auto Answer Timeout (0~120)

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

7.3 Call Waiting

- Enable call waiting: new calls can be accepted during a call.
- Disable call waiting: new calls will be automatically rejected and a busy signal will be prompted
- Enable call waiting tone: when you receive a new call on the line, the device will beep. Users can enable/disable call waiting in the device interface and the web interface.
- Web interface: enter [Intercom Settings] >> [Features], enable/disable call waiting, enable/disable call waiting tone.



	Features Media Settings	Camera Settings	MCAST Action	Time/Date Time Plan	Tone Led
› System					NOTE
› Network	Basic Settings >> Enable Call Waiting:				Description: Function settings, you can
> Line	Enable Auto on Hook: Enable Silent Mode:		Auto HangUp Delay: Disable Mute for Ring:	3 (0~30)second(s) 2	set the phone features, including the basic settings, tone settings, intercom settings, the
Intercom settings	Ban Outgoing: Default Ans Mode:	Video V 🔇	Default Dial Mode:	Video 🗸 🕜	corresponding code settings.
› Call List	Enable Restricted Incoming List Enable Restricted Outgoing List		Enable Country Code:		
> Function Key	Country Code:		Area Code:		
> Security	Allow IP Call:	2 0	P2P IP Prefix:		
› Device Log	Restrict Active URI Source IP: Line Display Format:	xxx@SIPn 🗸 🕐	Push XML Server:		
> Security Settings	Call Number Filter: Limit Talking Duration:		Auto Resume Current: Talking Duration:	2 0 120 (20~600)second(s)	
	No Answer Auto HangUp Timeout:	120 (1~3600)second(s) ?	Enable Push XML Auth:		
	Ring Timeout: Enable Tamper Alarm:	(1~3600)second(s) 🔮 Enable Tamper Alarm 🗸 🔮	Description:	IP Paging Gateway	
	Tone Settings >>				

Picture 9 - Call Waiting

	Features	Media Settings	Ca	mera Settings	MCAST		Action	Time	/Date	Time Plan
System										
Network	Basic Settings >	>								
	Tone Settings >:	>								
Line	Enable Holdi	ng Tone:		0		Enable Cal	I Waiting Tone:	2	0	
	Play Dialing I	DTMF Tone:		0	1	Play Talkin	g DTMF Tone:	~	0	
Intercom settings	Auto Answer	Tone:								
	Intercom Setting	gs >>								
Call List	Response Code 9	Settings >>								
Function Key					Арр	ply				
Security										
Device Log										

Picture 10 - Call Waiting tone



8 Advance Function

8.1 Intercom

The device can answer intercom calls automatically.

	Features	Media Settings	Camera Settings	MCAST	Action	Time/Date	Time Plan	Tone	Led
› System								NOTE	_
› Network	Basic Settings	>>						Description:	
› Line	Tone Settings							Function setting set the phone fe including the bas	atures,
	Intercom Setti Enable Inte	-	2 0	Enable	e Intercom Mute:			settings, tone se intercom setting	ttings, s, the
> Intercom settings		ercom Tone:	20	Enable	e Intercom Barge:	20		corresponding co settings.	bue
› Call List	Response Code	e Settings >>		Apply					
Function Key									
› Security									
› Device Log									
› Security Settings									

Picture 11 - WEB Intercom Settings

Table 3 - Intercom description

Parameters	Description
	When the intercom system is enabled, the device will accept the SIP
Enable Intercom	header call-info of the Call request
	Command automatic call
	If the option is enabled, PA3 will answer the intercom call
Enable Intercom Barge	automatically while it is in a normal call, and it will reject new intercom
	call if there is already one intercome call
Enable Intercom Mute	Enable mute during intercom mode
Enable Intercom Binging	If the incoming call is intercom call, the device plays the intercom
Enable Intercom Ringing	tone.

8.2 MCAST

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



listening addresses.

	Features Media Setti	ngs Camera Settings	MCAST	Action	Time/Date	Time Plan	Tone	Led
System							NOTE	
Network	MCAST Listening Priority: Enable Page Priority:		~				Description: Set the multicas and multicast pr	t address,
Line	Enable Page Friding. Enable Prio Chan: Enable Emer Chan:							ioney.
Intercom settings	Index/Priority	Name		Host:port		Channel		
Call List	1 2 3					0 × 0 ×		
Function Key	4 5							
Security	6 7					0 ~		
Device Log	8 9							
Security Settings	10	Apply				0 ~		
	MCAST Dynamic							
	Auto Exit Expires:	60 Apply						
	Index	Priority M	ICAST Ip		Port			

Picture 12 - MCAST Setting

Parameters	Description
Priority	Defines the priority in the current call, with 1 being the highest
	priority and 10 the lowest.
Enable Page Priority	Compared with multicast and SIP priority, high priority is pluggable
	and low priority is rejected.
Enable Prio Priority	When enabled, the same port and channel can be connected.
	Channel 24 is a priority channel, higher than 1-23; A channel of 0
	indicates that the channel is not used.
Enable Emer Chan	When enabled, channel 25 has the highest priority
Name	Name of the server listening to multicast
Host:port	Server address listening to multicast: port
Channel	0-25 (24 priority channels, 25 emergency channels)

Multicast:

- Go to web page of [Function Key] >> [Function Key], select the type to multicast, set the multicast address, and select the codec.
- Click Apply.
- Set up the name, host and port of the receiving multicast on the web page of [Intercom Settings] >> [MCAST].
- Press the DSSKey of Multicast Key which you set.
- Receive end will receive multicast call and play multicast automatically.



MCAST Dynamic:

Description: send multicast configuration information through SIP notify signaling. After receiving the message, the device configures it to the system for multicast monitoring or cancels multicast monitoring in the system.

8.3 Hotspot

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

Parameters	Description
Enable Hotspot	Enable or disable hotspot.
Mode	This device can only be used as a client.
Monitor Type	The monitoring type can be broadcast or multicast. If you want to
	restrict broadcast packets in the network, you can choose multicast.
	The type of monitoring on the server side and the client side must be
	the same, for example, when the device on the client side is selected
	for multicast, the device on the SIP hotspot server side must also be
	set for multicast.
Monitor Address	The multicast address used by the client and server when the
	monitoring type is multicast. If broadcasting is used, this address does
	not need to be configured, and the system will communicate by
	default using the broadcast address of the device's wan port IP.
Remote Port	Fill in a custom hotspot communication port. The server and client
	ports need to be consistent.
Name	Fill in the name of the SIP hotspot. This configuration is used to
	identify different hotspots on the network to avoid connection conflicts.
Line Settings	Sets whether to enable the SIP hotspot function on the corresponding
	SIP line.

Table 5 - SIP Hotspot

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.

	SIP SIP Hotspo	t Action Plan Basic Settings	
System			
Network	No Registration		
	SIP Hotspot Settings		
Line	Enable Hotspot:	Disabled V	0
1	Mode:	Client 🗸	0
Intercom settings	Monitor Type:	Broadcast 🗸	0
unseessante statungites s	Monitor Address:	224.0.2.0	0
all List	Local Port:	16360	0
	Name:	SIP Hotspot	0
unction Key	Line Settings		
	Line 1:	Enabled V	
ecurity	Line 2:	Enabled V	
Device Log		Apply	
ecurity Settings			

Picture 13 - SIP hotspot

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

Calling internal extension:

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



9 Web Configurations

9.1 Web Page Authentication

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

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

9.2 System >> Information

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

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

And summarization of network status,

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

Besides, summarization of SIP account status,

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



9.3 System >> Account

	Information	Account	igurations Upgrade	Auto Provision	FDMS	Tools	Reboot	
System							NOTE	
Network	Add New User Username			0			Description: Set or modify t	the login
Line	Confirm Passv	cation Password word		Ø			user name and	l passwor
Intercom settings	Privilege		Administrators Add					
Call List	User Accounts	User		Privilege				
Function Key		admin guest		Administrators Users				
Security	User Managemen	ıt						
Device Log	admin 🗸		Delete	lodify				
Security Settings								

Picture 14 - WEB Account

On this page the user can change the password for the login page. Users with administrator rights can also add or delete users, manage users, and set permissions and passwords for new users

9.4 System >> Configurations

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

	Information	Account	Configurations	Upgrade	Auto Provision	FDMS	Tools	Reboot	
> System								NOTE	
Network	Export Configu	rations 🕜	Diele statistickers b	CAN T F	antiana in that formant			Description:	
Line			Right click here to	o SAVE nc confi	ations in 'txt' format. gurations in 'txt' forma ations in 'xml' format.			This page is us manage config the phone, inc import/export	juration of luding,
Intercom settings	Import Configu	rations 🕜						configuration, configuration partly/totally.	reset
Call List	Clear Configura	tion >> 🕜	Configuration file			Select	port		
Function Key			Click "Clear" but	ton to reset the	configuration files!				
Security		Content to Keep			Content to DSS KEY	Reset			
Security		BASIC NETWORK			TR069				
Device Log		AUTOPROVISION		_					
Security Settings				→ ←					
			w				*		
				Clear]				
	Clear Tables >:	• 🕜							

Picture 15 - System Setting

Export Configurations

Right click to select target save as, that is, to download the device's configuration file, suffix



".txt". (note: profile export requires administrator privileges)

Import Configurations

Import the configuration file of Settings. The device will restart automatically after successful import, and the configuration will take effect after restart

Clear Configurations

Select the module in the configuration file to clear.
 SIP: account configuration.
 AUTOPROVISION: automatically upgrades the configuration
 TR069:TR069 related configuration
 MMI: MMI module, including authentication user information, web access protocol, etc.
 DSS Key: DSS Key configuration
 Basic Network
 Clear Tables

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

Reset Phone

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

9.5 System >> Upgrade

	Information Account Configurations Upgrade Auto Provision FDMS Tools	Reboot
> System		NOTE
> Network	Software upgrade @ Current Software Version: 1.0.0	Description:
› Line	System Image File: Select Upgrade	This page is used to upgrade some files for phone, including firmware, ring tones
› Intercom settings	Upgrade Server Upgrade Server Address1:	
› Call List	Upgrade Server Address2: Apply	
› Function Key	Firmware Information Current Software Version: 1.0.0	
> Security	Server Finnware Version: Checking	
> Device Log	New Firmware Information:	
› Security Settings	Ring Upgrade 🔮	
	Load Server File: [*.wav, *.mp3] Upload	
	Ring List 🖗	
	Index File Name File Size	
	Delete	

Picture 16 - Upgrade Settings

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

Upgrade the ringtone, support wav and MP3 format.



Firmware Upgrade:

Firmware online upgrade means that the device sends an HTTP request to the server, and the server returns the corresponding description file or 404 or timeout. After receiving it, the device parses the version description file and prompts the user whether to upgrade the new version

Upgrade Serve	r		
Upgrade Server Address1:			
Upgrade Server Address2:			
			Apply
Firmware Info	rmation		
	Current Software Version:	1.0.0	
	Server Firmware Version:	Checking	
	Upgrade		
	New Firmware Information:		

Picture 17 - Online upgrade settings

Table 6 - Firmw	are upgrade
-----------------	-------------

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

● 设备向服务器请求的文件为 TXT 文件,文件名称为 vendor_model_hw1_0.txt。hw 后面是硬件 版本号。文件名中有空格全部改为下划线。

• The file requested from the server is a TXT file called vendor_model_hw10.txt.hw followed by the hardware version number, it will be written as hw10 if no difference on hardware. All



Spaces in the filename are replaced by underline.

- The URL requested by the phone is HTTP:// server address/vendor_Model_hw10.txt: The new version and the requested file should be placed in the download directory of the HTTP serve.
- TXT file format must be UTF-8
- vendor_model_hw10.TXT The file format is as follows: Version=1.6.3 #Firmware version Firmware=xxx/xxx.z #URL,Relative paths are supported and absolute paths are possible, distinguished by the presence of protocol headers. BuildTime=2018.09.11 20:00 Info=TXT|XML
 Xxxxx

Xxxxx Xxxxx

Ххххх

9.6 System >> Auto Provision

	Information	Account	Configurations	Upgrade	Auto Provision	FDMS	Tools	Reboot	
System								NOTE	
Network	Basic Settings CPE Serial N	lumber:		00100400FV02001	10000000d84a03d14c		0	Description: Auto Provision	
Line		on Password:					0	to realize remote/autom installation an delpoyment co	natically
Intercom settings	General Con	n File Encryption k ifiguration File Enc ail Check Times:		1			0	and some oth files.	
Call List	Save Auto P	rovision Informatio ommonConfig enal					0		
Function Key	Enable Serve	er Digest:					0		
Security	DHCP Option >> DHCPv6 Option								
Device Log	SIP Plug and Pla	ay (PnP) >>							
Security Settings	Static Provision	-							
	Autoprovision N	low >>							
	TR069 >>		Apply						

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

Picture 18 - Auto provision Settings

The azimuth terminal supports SIP plug and play, DHCP selection parameters, static deployment server and TR069 to obtain automatic deployment application . parameters.Transferring protocol: FTP、 TFTP、 HTTP、 HTTPS

Table 7 - Auto provision Settings



Auto provision	Auto provision						
Parameters	Description						
Basic settings							
CPE Serial Number	Serial number of the equipment						
Authentication Name	Username for configuration server. Used for FTP/HTTP/HTTPS.						
Authentication Name	If this is blank the phone will use anonymous						
Authentication	Password for configuration server. Used for FTP/HTTP/HTTPS						
Password							
Configuration File	Encryption key for the configuration file						
Encryption Key							
General							
Configuration File	Encryption key for common configuration file						
Encryption Key							
Download Fail Check	The default value is 5. If the download configuration fails, it will be						
Times	downloaded 5 times.						
Enable Server Digest	When the feature is enable, if the configuration of server is						
	changed, phone will download and update.						
DHCP Option							
Option Value	The equipment supports configuration from Option 43, Option 66,						
	or a Custom DHCP option. It may also be disabled.						
Custom Option Value	Custom option number. Must be from 128 to 254.						
Enable DHCP Option	Set the SIP server address through DHCP option 120.						
120							
SIP Plug and Play (Pr	וP)						
	Whether enable PnP or not. If PnP is enable, phone will send a						
Enable SIP PnP	SIP SUBSCRIBE message with broadcast method. Any server						
	can support the feature will respond and send a Notify with URL to						
	phone. Phone could get the configuration file with the URL.						
Server Address	Broadcast address. As default, it is 224.0.0.0.						
Server Port	PnP port						
Transport Protocol	PnP protocol, TCP or UDP.						
Update Interval	PnP message interval.						
Static Provisioning S	erver						
Server Address	Set FTP/TFTP/HTTP server IP address for auto update. The						
	address can be an IP address or Domain name with subdirectory.						
Configuration File	The configuration file name. If it is empty, phone will request the						
Name	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.					
Drotocol Turno	Transferring protocol type, supports FTP、TFTP、HTTP and					
Protocol Type	HTTPS					
	Configuration file update interval time. As default it is 1, means					
Update Interval	phone will check the update every 1 hour.					
	Provision Mode.					
	1. Disabled.					
Update Mode	2. Update after reboot.					
	3. Update after interval.					
TR069						
Enable TR069	Enable TR069 after selection					
Enable TR069	If TDOCO is analyzed, there will be a present tang when comparing					
Warning Tone	If TR069 is enabled, there will be a prompt tone when connecting.					
ACS Server Type	There are 2 options Serve type, common and CTC.					
ACS Server URL	ACS server address					
ACS User	ACS server username (up to is 59 character)					
ACS Password	ACS server password (up to is 59 character)					
TLS Version	TLS Version,Valid Value:TLS1.0/1.1/1.2.					
INFORM Sending	TR069 message cycle.Valid Value:1~9999 seconds.					
Period						
STUN Server						
address	Enter the STUN address					
Enable the STUN	Enable the STUN					

9.7 System >> FDMS

	Information	Account	Configurations	Upgrade	Auto Provision	FDMS	Tools	Reboot
System								
Network	FDMS Info Settin Community I							
Line	Building Nun Room Numbe							
Intercom settings				Ар	ply			
Call List								
Function Key								
Security								
Device Log								
Security Settings								



Picture 19 - FDMS

Table 8 - FDMS Information

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

9.8 System >> Tools

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

	Information	Account	Configurations	Upgrade	Auto Provision	FDMS	Tools	Reboot
> System								NOTE
Network	Syslog Enable Syslog:							Description: Some tools to help
Line	Server Address: Server Port:		0.0.0.0				0	administrators or technicians to analyze issues.
Intercom settings	APP Log Level: Export Log:		Warning Apply	~			0	
Call List	Web Capture 🕜							
Function Key	Start Watch Dog		stop					
 Security Device Log 	Enable Watch Do	g:	Apply					
 Security Settings 								

Picture 20 - Tools

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

Refer to <u>10 troubleshooting</u> for details.

9.9 Network >> Basic

Users can configure network connection types and parameters through this page.



Network Network Mode ● Note Network Network Mode ● PP4 Only ▼ Pescription: ine IP4 Network Status IP: 172.16.7.134 Pescription: You can do some simple, including P intercom settings IP: 172.16.7.134 Default gateway: 172.16.7.1 call List MAC: 00:d8:4a:03:d1:4c DNS, etc. INS, etc. Function Key IP4 Settings DHCP ● PPope O Perof O security DNS Server :: DHCP ● PPope O ● Privary DNS Server :: 114.114.114.114 ● ●		Basic Service Port	VPN Advanced		
Network Description: ine IP-4 Network Status IP-1 172.16.7.134 intercom settings Subnet mask: Subnet mask: 255.255.05 Default gateway: 172.16.7.1 AAC: 00:d8:4a:03:d1:4c Static IP O DHCP ● Static IP O DHCP ● PPope O Imapped in the status Static IP O DHCP ● Provide Configured by: DHCP ● Provide Configured by: DHCP ● Provide Configured by: DHCP ● Privation Identifier: Disabled Status Security ONS Server: Privator Status Q Privator Status Q Privator Status DHCP ● Privator Identifier: Disabled Status DNS server: DHCP ● Privator Identifier: DHCP ● Secondary DNS Server:	System				NOTE
ine IPv4 Network Status intervork status intervork configuration intercom settings IP: 172.16.7.134 Subnet mask: 255.255.255.0 Default gateway: 172.16.7.1 and List MAC: 00:d8:4a:03:d1:4c unction Key IPv4 Settings Static IP ○ DHCP ● Enable Vendor Identifier: Disabled ▼ Vendor Identifier: Volf P aging Gateway 0NS Server: 0235.55 Primary DNS Server: 0235.55 Security Secondary DNS Server: Primary DNS Server: 114.114.114.114	Network				
IP: 172.16.7.134 DNS, etc. Subnet mask: 255.255.255.0 255.255.255.0 Default gateway: 172.16.7.1 MAC: 00/d8140:03:d1:4c IPv4 Settings Static IP O Static IP O DHCP ● PPope O ecurity Enable Vendor Identifier: Vendor Identifier: IDisabled ~ ONS server: C255.55 Secondary DNS Server: Tit.114.114.114	ine				 network configuration this page, including II
All List MAC: 00:d8:4a:03:d1:4c Inction Key IPv4 Settings Static IP O DHCP ® PPPoE O Enable Vendor Identifier: Disabled ~ 0 Vendor Identifier: VoliP IP paging Gateway 0 Pv1Ce Log Primary DNS Server: 223.55.5 0 Secondary DNS Server : 114.114.114.114 0	itercom settings				DNS, etc.
Linction Key C DHCP • PPPoE Static IP O DHCP • PPPoE example Enable Vendor Identifier: Disabled • Vendor Identifier: VolP IP Paging Gateway 0 exice Log Primary DNS Server: 223.55.5 exice Secondary DNS Server : 114.114.114.114	all List				
Enable Vendor Identifier: Disabled v Image: Constraint of the state of the stat	Inction Key	IPv4 Settings			—
DNS Server Configured by: DHCP Ø Primary DNS Server: 223.5.5.5 Ø Secondary DNS Server: 114.114.114 Ø	ecurity	Enable Vendor Identifier:	Disabled ~		
Primary DNS Server: 223.5.5.5 Ø Secondary DNS Server : 114.114.114.114 Ø	vice Log	DNS Server Configured by:	DHCP	0 0	
				0 0 0	
			Apply		

Picture 21 - Network Basic Setting

Table	9 -	Basic	Setting	Parameters
-------	-----	-------	---------	-------------------

Parameters	Description		
Network Mode	IPv4、IPv6 and IPv4&IPv6		
IPv4 Network Stat	tus		
IP	The current IP address of the device		
Subnet mask	The current Subnet Mask		
Default gateway	The current Gateway IP address		
MAC	The MAC address of the device		
IPv4 Settings			
For the network co	nnection mode of the device, please select the appropriate network		
mode according to	the actual network environment. The device provides three network		
modes:			
	If your ISP service provider provides a fixed IP address, you can		
	select this item. After selection, you must fill in the static table:		
Static IP	static IP address / subnet mask / gateway / DNS and other		
	relevant information. If you do not know this information, please		
	ask your ISP service provider or network administrator for		
	assistance.		
DHCP	Network parameters are provided automatically by a DHCP		
DIICI	server.		
PPPoE	When selecting this mode, you must enter the ADSL online		
	account and password.		
Enable Vendor	Enable DHCP OPTION 60 to take vendor information.		
Identifier			
Vendor Identifier	DHCP OPTION 60, vendor class identifier. Valid Value:		



Alphanumeric. Up to 20 characters.					
When using static	When using static mode, you need to set relevant static configuration.				
DNS Server	Lice DNS conver assigned by DHCP conver				
Configured by	Use DNS server assigned by DHCP server.				
Primary DNS	Preferred DNS server.				
Server					
Secondary DNS	alternate DNS server.				
Server					
DNS Domain DNS Domain					
NOTE:					
1) After setting the parameters, you need to click submit to take effect.					
2) If you change the IP, the web page will no longer respond. At this time, you should					
enter a new IP in the address bar to connect to the device.					

9.10 Network >> service port

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

	Basic Service Port	VPN Advanced	
System			
Network	Service Port Settings		
	Web Server Type:	HTTP 🗸	0
Line	Web Logon Timeout:	15 (10~30)Minute	0
	web auto login:		
	HTTP Port:	80	0
Intercom settings	HTTPS Port:	443	0
	RTP Port Range Start:	10000 (1025~65530)	0
Call List	RTP Port Quantity :	1000 (10~1000)	0
Function Key		Apply	
Security			
Device Log			
Security Settings			

Picture 22 - Service port setting interface

Table 10 - Server Port

parameter	description	
Web server type	Restart after setting takes effect. Optional web login as	
	HTTP/HTTPS	
Web login timeout	The default is 15 minutes, the timeout will automatically log out of	



	the login page, and you need to log in again	
Web page automatic	No need to enter the user name and password after the timeout,	
login	it will automatically log in to the web page.	
HTTP port	The default is 80, if you want system security, you can set other	
	port	
	Such as: 8080, web page login: HTTP://ip:8080	
HTTPS port	The default is 443, same as HTTP port usage	
RTP port start range	The value range is 1025-65535. The value of rtp port starts from	
	the initial value set. Each time a call is made, the value of the	
	voice and video ports is increased by 2	
RTP port quantity	Number of calls	

9.11 **Network >> VPN**

	Basic Service Port	VPN Advanced		
System	Virtual Private Network (VPN) Stat	tus		NOTE
> Network	VPN IP Address:	0.0.0.0		Description: You can make VPN connect with the page.
	VPN Mode			
Line	Enable VPN:		0	
	Enable NAT:			
Intercom settings	L2TP: O	OpenVPN: O		
	Open VPN mode:	tun 🗸	0	
Call List				
	Layer 2 Tunneling Protocol (L2TP)			
Function Key	L2TP Server Address:	0.0.0.0	0	
	Authentication Name:	0.0.0	0	
Security	Authentication Password:		0	
occarry	Addicideadon rassword.			
Device Log		Apply		
Security Settings	OpenVPN Files 📀			
	Load OpenVPN File	Select	Upload	
	Certificates List 🕐			
	Index	File Name	File Size	
			Delete	
			Delete	

Picture 23 - Network 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 page [**Network**] -> [**VPN**]. In VPN Mode, check the "Enable VPN" option and select "L2TP", then fill in the L2TP server address, Authentication Username, and Authentication Password in the L2TP section. Press "Apply" then the device will try to connect to the L2TP server.

When the VPN connection established, the VPN IP Address should be displayed in the VPN status. There may be some delay of the connection establishment. User may need to refresh the page to update the status.

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

OpenVPN

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

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

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

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



9.12 Network >> Advanced

	Basic Service Port	VPN	Advanced		
m	Link Layer Discovery Protocol (LLD	P) Settings			
	Enable LLDP: 🚺		Packet Interval:(1~3600)	60 second(s) 3	Description: LLDP/CDP/VLAN are to
vork	Enable Learning Function:	0			allow system access to VLAN by vian tagged
	Cisco Discovery Protocol (CDP) Set	tings			itself; DSCP is to provid QoS; 802.1X is to allow
	Enable CDP:	٦	Packet Interval:(1~3600)	60	system pass switch's authentication to access
om settings	DHCP VLAN Settings				to LAN
	Option Value:	Disabled	~ ⊘		
ist	DHCP Option Vlan(128-254):	0			
	Quality of Service (QoS) Settings				
ion Key	Enable DSCP:	3 📀	Signal DSCP:	46 (0~63)	
ity	Audio DSCP:	46 (0~63)	Video DSCP:	46 (0~63)	
	ARP Cache Life				
e Log	ARP Cache Life	2 Minute 🥝			
	WAN VLAN Settings				
ity Settings	Enable VLAN:	0	WAN VLAN ID:	256 (0~4095) 🕜	
	802.1p Signal Priority:	0~7)	802.1p Media Priority: Apply	0 (0~7)	
	802.1X Settings				
	802.1x Mode:	Off 🗸		0	
	Identity:	admin		0	
	Password:			0	
	CA Certificate:		Browse Upload	0	
	Device Certificate:		Browse Upload	0	
	Certification File 🕖				
	File Type	File Name	File Size		
	HTTPS Certification File	https.pem(Defau	lt) 4501 Bytes	Select Upload Delete	

Picture 24 - Network Setting

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

parameter	description	
LLDP Settings		
Enable LLDP	Enables LLDP (Linker Layer Discovery Protocol) function.	
Packet Interval	LLDP message sent periodic interval.Valid Value:1 to 3600	
	seconds.	
Enable Learning Function	Enable VLAN settings learned via LLDP-MED	
Cisco Discovery Protocol (CD	P) Settings	
Enable CDP	Enable CDP	
Packet Interval	Valid Value:1 to 3600 seconds.Default 60s	
Quality of Service (QoS) Settings		
Enable DSCP	Enable DSCP to get best offset QoS for voice quality.	
Signal DSCP	DSCP value for SIP messages.Valid Value:0~63.	

 Table 11 - Network Basic Setting Paramater



Audio DSCP	DSCP value for voice RTP data.Valid Value:0~63.		
Video DSCP	DSCP value for video RTP data.Valid Value:0~63.		
ARP Cache Life			
ARP Cache Life	Set ARP cache life. Do not modify this value if there is no		
	problem with the system.Valid Value:0~99		
DHCP VLAN Settings			
Option Value	The DHCP option for Vlan Discovery		
WAN VLAN Settings	· ·		
Enable VLAN	Enable VLAN to let system access to VLAN network with vlan		
	tagged.		
WAN VLAN ID	VLAN ID for system WAN port.Valid Value:0~4095.		
802.1p Signal Priority	802.1P priority for SIP messages.Valid Value:0-lowest priority;		
	7-highest priority		
802.1p Media Priority	Valid Value:Integer from 0 to 7.		
802.1X Settings	· ·		
802.1x Mode	It configures the 802.1x authentication method.Valid		
	Value:static.network.802_1x.mode		
	(0-Disabled;1-EAP-MD5;2-EAP-TLS;3-PEAP-MSCHAPv2).:		
Identity	认证用户名		
Password	认证密码		
CA Certificate	上传 CA 证书		
Device Certificate	上传设备证书		
Certification File			
File Type	System's HTTPS server CA file type.		
File Name	System's HTTPS server CA file name.		
File Size	System's HTTPS server CA file size.		
	1		



9.13 Lines >> SIP

	SIP SIP Hots	spot Action Plan	Basic Settings		
System	Line 5789@SIP >				Description: It shows phone registration account basic
Network	Line Status: Username:	Registered	Activate: Authentication User:	20	settings and sip account basic function advanced settings.
Line	Display name: Realm:		 Authentication Password: Server Name: 	Ø	
Intercom settings	SIP Server 1:		SIP Server 2:		
Call List	Server Address: Server Port:	172.16.1.2 5060	Server Address:Server Port:	5060	
Function Key	Transport Protocol: Registration Expiration:	UDP V 🛛	Transport Protocol: Registration Expiration:	UDP 🗸 🍘 3600 second(s) 🥝	
Security	Proxy Server Address:		Backup Proxy Server Address:		
Device Log	Proxy Server Port: Proxy User: Proxy Password:	5060	Backup Proxy Server Port:	5060	
Security Settings	Basic Settings >>		U		
	Codecs Settings >> 🕜				
	Advanced Settings >> SIP Global Settings >>				
	-	Apply			

Picture 25 - SIP Settings(1)

				正在使用默认密	码,请更换	中文 💙 🗖	注销 目 保持运	
	SIP	SIP热点	联动计划	基本设定				
› 系统							1	NOTE
) 网络	线路 5789@SIP マ 注册设定 >>							描述: 话机注册账号基本设置和sip 账号功能高级设置
> 线路	基本设定 >>							
> 对讲设置	启用自动接听:	20		自动接听等候时间:	0	(0~120)秒 🕜		
and the second	启用热线:							
› 通话名单	热线延迟时间: 允许不注册呼出:	0	(0~9)秒 🕜	热线号码:		0		
> 快捷键	DTMF类型:		v 🕜	DTMF SIP INFO模式:	发送10/11	✓ Ø		
	URI是否携带端口信息:	Ø						
⁾ 安全	使用STUN:			使用VPN:				
WART	开启代理回退:	20		Signal Failback:				
> 设备日志	代理回退间隔:	1800	秒 🕜	重试次数:	3	(1~10) 🕜		
> 安防设置	编码设定 >> 🕜							
	高级设定 >>							
	全局设置 >>		提交					

Picture 26 - SIP Settings(2)



	SIP SIP Hotspot	Action Plan	Basic Settings	
System	Line 5789@SIP > Register Settings >>			Description: It shows phone registration account basic
Network	Basic Settings >>			settings and sip account function advanced settings.
Line	Codecs Settings >> 🕜 Disabled Codecs:		Enabled Codecs:	beengu
Intercom settings	G.726-16 G.726-24 G.726-32	→	G.711U G.711A G.729AB	
Call List	G.726-40 G.723.1 MPA	-	ILBC opus G.722	
Function Key	Advanced Settings >>			
Security	SIP Global Settings >>	Apply		
Device Log				
Security Settings				

Picture 27 - SIP Settings(3)

	SIP SIP Hots	pot Action Plan	n 🛛 Basic Set	tings	
System	Advanced Settings >>				
	Use Feature Code:				
Network	Enable Blocking			Disable Blocking Anonymous	
	Anonymous Call:			Call:	•
	Call Waiting On Code:		0	Call Waiting Off Code:	0
Line	Send Anonymous On Code:		0	Send Anonymous Off Code:	
Intercom settings	Enable Session Timer:			Session Timeout:	1800 second(s)
	Response Single Codec:	0 0		BLF Server:	
Call List	Keep Alive Type:			Keep Alive Interval:	30 second(s)
	Keep Authentication:			Blocking Anonymous Call:	
Function Key	RTP Encryption(SRTP):	Disabled V			
	User Agent:		0	Specific Server Type:	
Security	SIP Version:	RFC3261 V		Anonymous Call Standard:	None V
	Local Port:	5060	0	Ring Type:	
Device Log	Enable user=phone:			Use Tel Call:	
	Auto TCP:			Enable PRACK:	
Security Settings	Enable Roort:			Enable PRACK:	
	Enable reports				
	DNS Mode:	A 🗸 🎯		Enable Long Contact:	0 0
	Enable Strict Proxy:	20		Convert URI:	
	Use Quote in Display Name:	00		Enable GRUU:	0 0
	Sync Clock Time:			Enable Use Inactive Hold:	
	Caller ID Header:			Use 182 Response for Call waiting:	
	Enable Feature Sync:			Enable SCA:	
	CallPark Number:		0	Server Expire:	
	TLS Version:	TLS 1.2 🗸 🥝		uaCSTA Number:	
	Enable Click To Talk:			Enable ChangePort:	
	Intercom Number:				
	Unregister On Boot:			Enable MAC Header:	
	Enable Register MAC Header:	D			
	PTime(ms):	Disabled 🗸		Enable Deal 180:	
	Transaction Timer T1:	500	-	Transaction Timer T2:	4000
		(500~10000)millised	cond 🕜		(2000~40000)millisecond 🥝
	Transaction Timer T4:	(2500~60000)millise	econd 🕜		

Picture 28 - SIP Settings(4)



	SIP SIP H	otspot Action Plan	Basic Settings				
System							NOTE
Network	Line 5789@SIP ✓						Description:
Line	Register Settings >> Basic Settings >>						It shows phone registration account basic settings and sip account function advanced settings.
Intercom settings	Codecs Settings >> 🕜						settings.
Call List	Advanced Settings >> SIP Global Settings >>						
Function Key	Strict Branch:			Enable Group:			
Security	Enable RFC4475: Registration Failure Re Enable uaCSTA:	try Time:	second(s)	Enable Strict UA Match: Local SIP Port:	5060	0	
Device Log	Ellable daCSTA,	Apply					
Security Settings							

Picture 29 - SIP Settings(5)

	Tuble 12 - 511 Settings
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	It enables or disables the account X.
Username	It configures the display name for account X.
Authentication User	It configures the register user name for account X.Valid
	Value:String within 80 characters.
Display name	It configures the display name for account X.
Authentication Password	It configures the password for register authentication for
	account X.Valid Value:String within 80 characters.
Realm	It configures the address of Domain Name.
Server Name	It configures the server name for account X.
SIP Server 1	
Server Address	It configures the SIP server.Valid Value:IP address and
	Domain Name.
Server Port	It configures the port of the SIP server.
Transport Protocol	Select transfer protocol.
Registration Expiration	It configures the interval (in seconds) between IP phones
	retrying account X before the registration timeout.Valid
	Value:Integer from 30 to 2147483647.
SIP Server 2	
Server Address	It configures the SIP server.Valid Value:IP address and
	Domain Name.
Server Port	It configures the port of the SIP server.

Table 12 - SIP Settings



Advanced Settings	
Codecs Settings	It enables or disables the specified codec for account X.
Oignaí Neiry Counts	attempts proxy is not available.
Signal Retry Counts	Multiple proxy cases SIP Request considers the number of
Signal Failback	In the case of multiple proxy, whether invite/register request is allowed to execute failback
Signal Failhack	time interval of main Proxy is available.
Failback Interval	Using Register message to periodically detect whether the
	master server
Enable Failback	When the main server is available, whether switch to the
Use STUN	Set the line to use STUN for NAT traversal
Use VPN	Set the line to use VPN restrict route
Request With Port	Enable the Rport.
DTMF SIP INFO Mode	Set the SIP INFO mode to send '*' and '#' or '10' and '11'
DTMF Type	Set the DTMF type to be used for the line
Dial Without Registered	Set call out by proxy without registration
Hotline Number	Set the hotline dialing number
	dialed it
Hotline Delay	Set the delay for hotline before the system automatically
	headphone
	off-hook handset or turn on hands-free speaker or
	specific number immediately at audio channel opened by
Enable Hotline	Enable hotline configuration, the device will dial to the
	automatically answered it
Auto Answering Delay	Set the delay for incoming call before the system
	automatically after the delay time
Enable Auto Answering	Enable auto-answering, the incoming calls will be answered
Basic Settings	
Backup Proxy Server Port	Enter the backup proxy server port, default is 5060
Backup Proxy Server Address	Enter the IP or FQDN address of the backup proxy server
Proxy Password	Enter the SIP proxy password
Proxy User	Enter the SIP proxy user
Proxy Server Port	Enter the SIP proxy server port, default is 5060
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server
	Value:Integer from 30 to 2147483647.
	retrying account X before the registration timeout.Valid
Registration Expiration	It configures the interval (in seconds) between IP phones
Transport Protocol	Select transfer protocol.



	1
Use Feature Code	When this setting is enabled, the features in this section will
	not be handled by the device itself but by the server instead.
	In order to control the enabling of the features, the device will
	send feature code to the server by dialing the number
	specified in each feature code field.
Enable Blocking Anonymous Call	Set the feature code to dial to the server
Disable Blocking Anonymous Call	Set the feature code to dial to the server
Call Waiting On Code	Set the feature code to dial to the server
Call Waiting Off Code	Set the feature code to dial to the server
Send Anonymous On Code	Set the feature code to dial to the server
Send Anonymous Off Code	Set the feature code to dial to the server
Enable Session Timer	Set the line to enable call ending by session timer
	refreshment. The call session will be ended if there is not
	new session timer event update received after the timeout
	period
Session Timeout	Set the session timer timeout period
Response Single Codec	If setting enabled, the device will use single codec in
	response to an incoming call request
BLF Server	The registered server will receive the subscription package
	from ordinary application of BLF phone.
	Please enter the BLF server, if the sever does not support
	subscription package, the registered server and subscription
	server will be separated.
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to
	keep NAT pinhole opened
Keep Alive Interval	Set the keep alive packet transmitting interval
Keep Authentication	Keep the authentication parameters from previous
	authentication
Blocking Anonymous Call	Reject any incoming call without presenting caller ID
RTP Encryption	Enable RTP encryption such that RTP transmission will be
	encrypted
User Agent	
	Set the user agent, the default is Model with Software
	Set the user agent, the default is Model with Software Version.
Specific Server Type	
Specific Server Type SIP Version	Version.
	Version. Set the line to collaborate with specific server type
SIP Version	Version. Set the line to collaborate with specific server type Set the SIP version



Enable user=phone	Sets user=phone in SIP messages.
Use Tel Call	Set use tel call
Auto TCP	Using TCP protocol to guarantee usability of transport for SIP
	messages above 1500 bytes
Enable Rport	Set the line to add rport in SIP headers
Enable PRACK	Set the line to support PRACK SIP message
DNS Mode	Select DNS mode, A, SRV, NAPTR
Enable Long Contact	Allow more parameters in contact field per RFC 3840
Enable Strict Proxy	Enables the use of strict routing. When the phone receives
	packets from the server,it will use the source IP address, not
	the address in via field.
Convert URI	Convert not digit and alphabet characters to %hh hex code
Use Quote in Display Name	Whether to add quote in display name, i.e. "Fanvil" vs Fanvil
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)
Sync Clock Time	Time Sycn with server
Enable Use Inactive Hold	启用后通话 hold 抓包可以看到(INVITE 包中)SDP 中是 inactive
Caller ID Header	Set the Caller ID Header
Use 182 Response for Call	Set the device to use 182 response code at call waiting
waiting	response
Enable Feature Sync	Feature Sycn with server
Enable SCA	Enable/Disable SCA (Shared Call Appearance)
CallPark Number	Set the callPark number
Server Expire	Use the timeout of the server.
TLS Version	Choose TLS Version
uaCSTA Number	Set uaCSTA number
Enable Click To Talk	Use with special server, click to call directly after enabling
Enable ChangePort	Enable port update
Intercom Number	Set intercom number
Unregister On Boot	Whether to enable the logout function
Enable MAC Header	Whether to enable the SIP package and user agent with or
	without MAC during registration
Enable Register MAC Header	Whether to open registration: Yes, user agent (with or without
	MAC)
PTime(ms)	Set whether to bring the ptime field. The default is not
Enable Deal 180	On: after receiving 183 + SDP, play IVR, and then play local
	tone when receiving 180.
	Close: after receiving 183 + SDP, play IVR, and then do not



	pla	play local tone when receiving 180.					
Transaction Timer T1	lt	configures	the	SIP	Transaction	Timer	T1(in
	mil	lionseconds),	Valid V	alue:50	0~10000		
Transaction Timer T2	lt	configures	the	SIP	Transaction	Timer	T2(in
	mil	lionseconds),	Valid V	alue:20	00~40000		
Transaction Timer T4	lt	configures	the	SIP	Transaction	Timer	T2(in
	mil	lionseconds),	Valid V	alue:25	500~60000		
SIP Global Settings							
Strict Branch	Str	Strictly match the Branch field.					
Enable Group	Enable SIP group server function as server backup.						
Enable RFC4475	After enabling, strictly observe RFC4475.						
Enable Strict UA Match	Open a strict UA match and only accept requests from the						
	sei	ver.					
Registration Failure Retry Time	The registration failure retries time, if the SIP account fails to						
	register, the chance to register half of the retransmission time						
	is registered until the registration is successful.						
Local SIP Port	The SIP port used by the device.						
Enable uaCSTA	Se	Set whether to enable uacsta function					

9.14 Lines >> SIP Hotspot

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

See 8.3 Hotspot for details

9.15 Line >> Action Plan

When calling to a phone, the bounded IP camera synchronously transmits video to the opposite phone (video support).

Log in to the device web, visit [Line] >[Action plan], and configure action plan rules.



	SIP SIP Hotspot Action Plan Basic Settings	
System		NOTE
Network	Action Plan Add Number: Ø Type: Early V Ø	Description: The user can achieve the
Line	Direction: Both Image: Comparison AUTO Image: Comparison	desired dialing effect by opening / closing the existing rule or by adding a custom dialing rule.
Intercom settings	URL: OUSErAgent: OSERAGENT: OSERA	a custom draing rule.
Call List	Add	
Function Key	Action Plan Option	
Security	User-defined Action Plan Table	
Device Log	Index Number Type Direction Line Username URL UserAgent Action	
Security Settings		

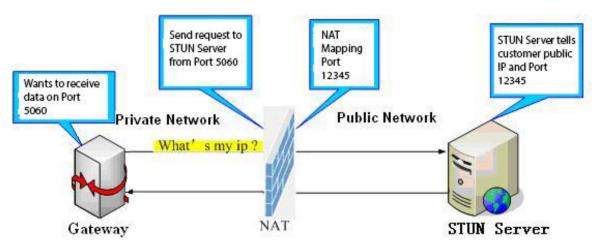
picture 30 - Action plan

Parameter	Description
Number	Auxiliary phone number (support video)
Туре	Support video display on call.
Direction	For call mode, incoming/outgoing call displays video
Line	Set up outgoing lines.
Username	Bind the user name of the IP camera.
Password	Bind IP camera password.
URL	Video streaming information.
User Agent	Set user agent information
MCAST Codec	Set multicast coding
Action	Action when the configured number is triggered

9.16 Line >> Basic Settings

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





picture 31 - Network Basic

	SIP SIP Hotspot	Action Plan Basic Settings		
System				NOTE
Network	STUN Settings STUN NAT Traversal:	FALSE	0	Description: Phone line basic settings,
Line	Server Address: Server Port:	3478	0	including STUN, certificate files.
Intercom settings	Binding Period: SIP Waiting Time:	50 second(s) 800 millisecond	() ()	
Call List		Apply		
Function Key	SIP P2P Settings Enable Auto Answering		0	
Security	Auto Answering Delay: DTMF Type:	0 (0~120)second(s)	0 0	
Device Log	DTMF SIP INFO Mode:	Send 10/11 V	Ø	
Security Settings		Apply		

picture 32 - Line Basic Setting

Table 14 - Line Basic Setting

Parameters	Description
STUN Settings	
Server Address	Set the STUN server address
Server Port	Set the STUN server port, default is 3478
Binding Period	Set the STUN binding period which can be used to keep the NAT
	pinhole opened.
SIP Waiting Time	Set the timeout of STUN binding before sending SIP messages
SIP P2P Settings	
Enable Auto	Automatically answer incoming IP calls after the timeout period is
Answering	enabled
Auto Answering	Automatic answer timeout setting
Delay	



DTMF Type	Set the DTMF type of the line.
DTMF SIP INFO	Set SIP INFO mode to send '*' and '#' or '10' and '11'
Mode	

9.17 Intercom settings >> Features

	Features Media Settings	Camera Settings	MCAS	T Action	Time/Date	Time Plan	Tone	Led
System							NOTE	
Network	Basic Settings >>						Description:	
	Enable Call Waiting:	2 0					Function setting	
Line	Enable Auto on Hook:			Auto HangUp Delay:		0)second(s) 🕜	set the phone f	eatures,
	Enable Silent Mode:			Disable Mute for Ring:			settings, tone s	ettings,
Intercom settings		-					corresponding of	
	Ban Outgoing:						settings.	
Call List	Default Ans Mode:	Video 🗸 🕜		Default Dial Mode:	Video 🗸 🧭			
	Enable Restricted Incoming List							
0.000000000	Enable Restricted Outgoing List:			Enable Country Code:	0			
Function Key	Country Code:			Area Code:				
Security	Allow IP Call:	20		P2P IP Prefix:				
Device Log	Restrict Active URI Source IP:		0	Push XML Server:		0		
Device Log	Line Display Format:	xxx@SIPn 🗸 🕘	-					
Security Settings	Call Number Filter:			Auto Resume Current:	2 0			
occurry occurry	Limit Talking Duration:	2 🕜		Talking Duration:	p Delay: 3 (0~30)second(s) e for Ring: a a Mode: Video ▼ a e for Ring: a a Mode: Video ▼ Amode: a a a attry Code: a a a a a a a a e Current: a a a a a YML Auth: a NOTE Description: Function settings, the corresponding code settings. Note: Note: Provide: Provide:			
	No Answer Auto HangUp Timeout:	120 (1~3600)second(s) ?		Enable Push XML Auth:				
	Ring Timeout:	120 (1~3600)second(s) ?		Description:	IP Paging Gateway			
	Enable Tamper Alarm:	Enable Tamper Alarm 🗸	0					
	Tone Settings >>							

picture 33 - Features

Table 15 - Features

Parameters	Description
Basic Settings	
Enable Call Waiting	Enable this setting to allow user to take second incoming call during an
	established call. Default enabled.
Enable Auto On Hook	The device will hang up and return to the idle automatically at
	hands-free mode
	Specify Auto handup time, the phone will hang up and return to the idle
Auto HangUp Delay	automatically after Auto Hand down time at hands-free mode, and play
	dial tone Auto handdown time at handset mode
Enable Silent Mode	When enabled, the phone is muted, there is no ringing when calls, you
Enable Slient Mode	can use the volume keys and mute key to unmute.
Disable Mute for Ring	When it is enabled, you can not mute the phone.
Per Outroing	If you select Ban Outgoing to enable it, and you cannot dial out any
Ban Outgoing	number.
Default Ans Mode	Default Ans Mode:video or audio.



Default Dial Mode	Default Dial Mode:video or audio.
Enable Restricted	
Incoming List	Whether enable Restricted Incoming List
Enable Restricted	
Outgoing List	Wether enable Restricted Outgoing List
Enable country Code	Wether enable country Code
Country Code	Country Code
Area Code	Area Code
Allow IP Call	If enabled, user can dial out with IP address
P2P IP Prefix	You can set IP call prefix, for example, i set it as "172.16.2.", then i input
	#160 in dialpad and press dial key ,it will call 172.16.2.160 automatically
Restrict Active URI	Set the device to accept Active URI command from specific IP address.
Source IP	
Push XML Server	Configure the Push XML Server, when phone receives request, it will
	determine whether to display corresponding content on the phone which
	sent by the specified server or not.
Call Number Filter	Configure a special character & ,if the number is 78 & 9. The call will be
	filtered out&
Auto Resume Current	If the current path changes, the hold will be automatically resume
Auto Resume Current	If the current path changes, the hold will be automatically resume
Limit Talking Duration	Automatically hang up the call after enabling the time set for the call
Talking Duration	Call duration ,20-600s
No Answer Auto HangUp	If the call is not answered, the call will be automatically hung up after the
Timeout	timeout
Enable Push XML Auth	To enable push xml auth, user password is required
Ring Timeout	It configures ringing time of incoming call
Description	
Enable Tamper Alarm	Enable or prohibit anti disassembly detection and handle detection
Tone Settings	
Enable Holding Tone	When turned on, a tone plays when the call is held
Enable Call Waiting Tone	When turned on, a tone plays when call waiting
Play Dialing DTMF Tone	Play DTMF tone on the device when user pressed a phone digits at
	dialing, default enabled.
Play Talking DTMF Tone	Play DTMF tone on the device when user pressed a phone digits during
	taking, default enabled.
Auto Answer Tone	Start auto answer prompt tone
Intercom Settings	



Enable Intercom	When intercom is enabled, the device will accept the incoming call
	request with a SIP header of Alert-Info instruction to automatically
	answer the call after specific delay.
Enable Intercom Mute	Enable mute mode during the intercom call
Enable Intercom Tone	If the incoming call is intercom call, the phone plays the intercom tone
Enable Intercom Barge	Enable Intercom Barge by selecting it, the phone auto answers the
	intercom call during a call. If the current call is intercom call, the phone
	will reject the second intercom call
Response Code Settings	6
Busy Response Code	Set the SIP response code on line busy
Reject Response Code	Set the SIP response code on call rejection

9. 18 Intercom settings >> Media Settings

	Features	Media Settings	Camera Settings	MCAST	Action	Time/Date	Time Plan	Tone	Led
System	Codecs Setting	s >> 🕜						NOTE Description:	
Network	Media Settings							Media settings, set the voice	
Line	Default Ring Speakerpho Speakerpho		1.wav V 2 7 (0~9 3 (0~9					coding,volume, and so on.	ringtones
Intercom settings		ne SignalTone	3 (0~9						
Call List	Handfree M OPUS Paylo	ic Gain:	3 (1~9 107 (96~)	Sample Rate	OPUS-NB(¥			
Function Key	ILBC Payloa Enable VAD		97 (96~	127) 🕜 ILBC	Payload Length	20ms 🗸 🔇			
Security	Disable AEC Audio Profile		PoE V						
Device Log	H.264 Paylo Enable Line	-in:	117 (96~1) Disable	~ Ø					
Security Settings	Enable Line Speaker: Video Direct		Disable Panel Spea sendonly	✓ 🕜 Exter	nal Speaker Power:	8Ω5w 🗸 🗘			
		otocol(RTCP) Setti	·						
	RTP Settings >								
	Alert Info Ring	Settings >>	1	Apply					

picture 34 - Media Settings

Table 16 - Media Settings

Parameters	Description
Codecs Settings	Select the enabled and disabled voice codecs
	codec:G.711A/U,G.722,G.729AB,G.726-16,G.729-24,G.729-32,G.
	726-40,MPA,opus
Audio Settings	
Default Ring Type	Set the default ring type. If the caller ID of an incoming call was not
	configured with specific ring type, the default ring will be used.



Speakerphone Volume	Set the speakerphone volume, the value must be 0~9	
· ·	g Set the ring volume in the speakerphone, the value must be $0\sim9$	
Volume		
Speakerphone SignalTon	e	
Volume		
DTMF Payload Type	Enter the DTMF payload type, the value must be 96~127.	
Handfree Mic Gain		
Opus playload type	Enter the opus payload type, the value must be 96~127.	
	Set the opus sample rate, including OPUS-NB (8KHz), OPUS-WB	
OPUS Sample Rate	(16KHz)	
ILBC Payload Type	Set the ILBC Payload Type	
ILBC Payload Length	Set the ILBC Payload Length	
Enable VAD	Enable Voice Activity Detection. When enabled, the device will	Enable Voice
	suppress the audio transmission with artificial comfort noise signal	device will supp
	to save the bandwidth.	comfort noise si
Disable AEC	Enable or disable the AEC (echo cancellation) function.	
Audio Profile	Select power supply or Poe form	
H.264 Payload Type	Range: 96 ~ 127	
Enable Line-in	enable or disable the line-in function	
Enable Line-out	enable or disable the line-out function	
Speaker	Support panel speaker and external speaker	
External Speaker Power	External speaker power , support 10W, 20W, 30W, when using the	
	corresponding speaker, you must select the corresponding power	
	supply.	
Video Direction		
RTP Control Protocol(RT	CP) Settings	
CNAME user	Set the CNAME user	
CNAME host	Set the CNAME host	
RTP		
RTP keep alive	Keep talking, send a packet 30 seconds after enable it	
Alert Info Ring Settings	(alert-info)	
Value of notification	n Set the value of the specified ring type	
message 1 to 10	The value of the specified fing type	
ring type	The ring type	



9.19 Intercom Setting >> MCAST

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

The detail for <u>8.2 MCAST</u>

9. 20 Intercom Setting >> Action URL

Note! The operation URL is used for the IPPBX system to submit device events.

Action URL setting: configure the URL to report actions to the server. For example, fill in the URL: http://InternalServer /FileName.xml? (InternalServer is the IP address of the server, and FileName is the XML file name of the action reported by the storage device)

	Features Media Setting	s Camera Settings	MCAST	Action	Time/Date	Time Plan	Tone	Led
System	Action URL Event Settings							
	Setup Completed:			0			Description: Action URL settin	05
letwork	Registration Succeeded:			0			ACTION OKE SECTIO	ys
	Registration Disabled:			0				
ine	Registration Failed:			0				
ine	Incoming Calls:			0				
	Outgoing Calls:			0				
Intercom settings	Call Established:			0				
	Call Terminated:			0				
Call List	Phone Silent:			0				
	Phone Unsilent:			0				
unction Key	Call Mute:			0				
	Call Unmute:			0				
ecurity	Missed Calls:			0				
	IP Changed:			0				
evice Log	Phone State Idle:			0				
	Phone State Talking:			0				
ecurity Settings	Phone State Ringing:			0				
	Start Reboot:			0				
	Web API Auth Changed:			0				
	Echo Test:			0				
	Input1:			0				
	Output1:			0				
	Reset Output1:			0				
	Tamper:			0				

picture 35 - Action URL



9.21Intercom Setting >> Time/Date

	Features Media Settings	Camera Settings MCA	AST Action	Time/Date	Time Plan	Tone	Led
System	Network Time Server Settings						Description:
	Time Synchronized via SNTP					0	Time and date se
Network	Time Synchronized via DHCP					0	you can set the t through the netw
Network	Time Synchronized via DHCPv6	5 🗌				0	server, or manua
	Primary Time Server	0.pool.ntp.org				0	the time, select t zone and date fo
Line	Secondary Time Server	time.nist.gov				0	zone and date to
	Time zone	(UTC+8) Beijing, Sing	apore,Perth,Irkuts V			0	
> Intercom settings	Resync Period	60	second(s)			0	
Call List	Time/Date Format						
Call List	12-hour clock						
Function Key	Time/Date Format	DD MMM WW	✓ 17 AUG WED				
Security							
	Daylight Saving Time Settings						
Device Log	Location	None	~				
	DST Set Type	Disabled	~				
Security Settings		Apply					
	Manual Time Settings						
		40 41		Analy			
	2022-8-17 11	1 ~ 48 ~		Apply			

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

picture 36 - Time/Date

Table 17 - 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
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 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
Manual Time Settings	You can set your time manually

9. 22 Intercom settings>>Time plan

	Features	Media Settings	Camera Settings	MCAST	Action	Time/Date	Time Plan	Tone	Led
› System	Time Plan:								
> Network	Name: Type:		Timed rebo	ot 🗸					
› Line	Repetition	period:	No repetitio	n 🗸					
Intercom settings									
› Call List	Monthly:		□ 4 □ 5 □ 6						
> Function Key			□ 7 □ 8 □ 9						
› Security	Effective	ime:		• • •	v: 0 v	1			
> Device Log	Time Plan Lis		Add						
> Security Settings			Туре	Spec	ial configure	Repetition period	Effective t	ime	
							Delete		

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

picture 37 - Time plan

Table 18 - Time plan

Parameters	Description
type	Timing restart, timing upgrade, timing sound detection, timing playback
	audio
Repeat cycle	Do not repeat: execute once within the set time range
	Daily: Perform this operation in the same time frame every day
	Weekly: Do this in the time frame of the day of the week



	Monthly: the time frame of the month to perform this operation
Effective time	Set the time period for execution

9. 23 Intercom settings >> Tone

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

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

	Features	Media Settings	Camera Settings	MCAST	Action	Time/Date	Time Plan	Tone	Led
System								NOTE	
Network	Tone Settings Select Your	Tone:	United States				~ Ø	Tone: cadence[,caden	cel
Line	Dial Tone: Ring Back T	one:	350+440/0 440+480/2000				0	[,cadence]Wh cadence = Freq [+Freq3] [+Freq4]/Durati	ere 1[+Freq2]
Intercom settings	Busy Tone: Congestion		480+620/500,0				0	The frequency of tone:200~4000 set to 0Hz, it mo	of the HZ, If it is eans the
Call List	Call waiting Holding Ton Error Tone:		440/300,0/100	00,440/300,0/10000,0				tone won't be p tone is comprise most four differ frequencies.Freq	ed of at ent
Function Key	Stutter Tone Information						0	The juxtapositio frequencies Free Freq2 without	n of two q1 and
Security	Dial Recall 1 Message To		350+440/100,0	/100,350+440/100,0/	100,350+440/100,0/100	0,350+440/0	0	modulation.Freq Freq1 is modula Freq2.Duration duration of the	ited by
Device Log	Howler Tone Number Un	e: obtainable Tone:	400/500,0/600				0	tone:0~30000m set to 0ms, it m tone will keep o	eans the n playing
Security Settings	Warning Tor Auto Answe		1400/500,0/0				0	until stopped by it is set to 0/0,it the tone is stop composition of 1	t means ped.The
				Apply				can configure at eight different c for one tone, an separate tones l commas.	t most adences id

picture 38 - Tone

9.24 Call List >> Call List

Restricted Incoming Calls

It same as blacklist.By adding a number into the blacklist, user will no longer receive phone call from that number and it will be rejected automatically by the device until user delete it from the blacklist.

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

Restrict Outgoing Call

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



9. 25 Call List >> Web Dial

	Call List Web Dial
System	
Network	Web Dial Settings
Line	Dial Answer Hang-up
Intercom settings	
Call List	
Function Key	
Security	
Device Log	
Security Settings	

Use web page to call, answer and hang up.

picture 39 - Web Dial

9.26 Security >> Web filter

≡FH-S01		cep online
	Web Filter Trust Certificates Device Certificates Firewall	
System		NOTE
Network	Web Filter Table 🕗	Description:
Line	Start IP Address End IP Address Option Web Filter Table Settings	Set the web access list, only the IP in th allows access to the phone.
Intercom settings	Start IP Address O End IP Address Add	
Call List	Web Filter Setting 🛛	
Function Key	Enable Web Filter	
Security		
Device Log		
Security Settings		

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

Filter Table 🕜		
Start IP Address	End IP Address	Option
192 168 1 1	102 100 254 254	Modify
192.108.1.1	192.168.254.254	Delete

picture 40 - WEB filter



Add and delete the allowed IP network segments; configure the start IP address in the start IP, configure the end IP address in the end IP, and then click [Add] to add successfully. You can set a large network segment or add it into several network segments. When deleting, select the starting IP of the network segment to be deleted in the list, and then click [Delete] to take effect. Enable web filtering: configure to enable/disable web access filtering; click the [Submit] button to take effect

Note: If the device you access to the device is on the same network segment as the device, do not configure the web filtering network segment to be outside your own network segment, otherwise you will not be able to log in to the web page.

9. 27 Security >> Trust Certificates

Permission Co	ertificate			
Permissio	n Certificate	Disabled	✓ Ø	
Common	Name Validation	Disabled	✓ Ø	
Certificate	e mode	All Certificates	✓ ⑦	
		Apply		
Import Certif	icates 🕜			
			Select Upload	
Load Serv	ver File			
Load Serv				

You can upload and delete uploaded trust certificates.

picture 41 - Trust Certificates

9. 28 Security >> Device Certificates

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



	Web Filter Trust Certificat	es Device Certificates	Firewall		
System					
Network	Device Certificates 🕜				
Line	Device Certificates	Default Certificates	✓ (existence)		
Intercom settings	Import Certificates 🥝				
Call List	Load Server File		Select Upload		
Function Key	Certification File 🥝				
Security	File Name	Issued To	Issued By	Expiration	File Size Delete
Device Log					
Security Settings					

picture 42 - Device Certificates

9. 29 Security >> Firewall

	Web Filter Trust Certificates Firewall	
System	Firewall Type 🜒	NOTE
Network	Enable Input Rules:	Description: Set firewall function.
Line	Apply	
Intercom settings	Index Deny/Permit Protocol Src Address Src Mask Src Port Range Dst Address Dst Mask Dst Port Range	
Call List	Firewall Output Rule Table 🥥	
Function Key	Index Deny/Permit Protocol Src Address Src Mask Src Port Range Dst Address Dst Mask Dst Port Range	
Security	Firewall Settings Imput/Output Input/Output Input ~ Src Address Dst Address	
Device Log	Deny/Permit Deny V Src Mask Dst Mask Add	
Security Settings	Rule Delete Option	
	Input/Output Index To Be Deleted Delete	

picture 43 - Firewall

Through this page, you can set whether to enable the input and output firewalls, and at the same time, you can set the input and output rules of the firewall. Use these settings to prevent malicious network access, or restrict internal users from accessing some resources of the external network, and improve safety.

The firewall rule setting is a simple firewall module. This function supports two kinds of rules: input rules and output rules. Each rule will be assigned a serial number, and a maximum of 10 each rule can be set.

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



Table 19 - Web Firewall

parameter	Description
Enable Input Rules	whether enable Input Rules
Enable Output Rules	Whether enable Output Rules
input/output	Select the current rule as an input or output rule
Deny/permit	Choose the current rule is deny or allowed;
protocol	There are four types of protocols: TCP, UDP, ICMP, IP $_{\circ}$
Port range	Port range
	The source address can be the host address, network address, or
Src Address	all addresses 0.0.0.0; it can also be a network address similar to
	..*.0, such as 192.168.1.0.
	The destination address can be a specific IP address or all
Dst Mask	addresses 0.0.0.0; it can also be a network address similar to
	..*.0, such as 192.168.1.0.
	It is the source address mask. When it is configured as
Src Port Range	255.255.255.255, it means it is a specific host. When it is set as a
Sic Fort Nange	subnet mask of type 255.255.255.0, it means that the filter is a
	network segment;
	It is the destination address mask. When it is configured as
Dst Port Range	255.255.255.255, it means it is a specific host. When it is set as a
	subnet mask of 255.255.255.0 type, it means that a network
	segment is filtered;
源端口范围	
目的端口范围	

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

all Input Rule Tab	ble 🕜						
ndex Deny/Permit	Protocol	Src Address	Src Mask	Src Port Range	Dst Address	Dst Mask	Dst Port Range

picture 44 - Firewall rules list

Then select and click the button [Submit].

In this way, when the device runs: ping 192.168.1.118, it will not be able to send data packets to 192.168.1.118 because of the prohibition of the output rule. But ping other IPs in the 192.168.1.0 network segment can still receive the response packets from the destination host normally.



le Delete Option 🥝			
Input/Output	Input 🔻	Index To Be Deleted	Delete

picture 45 - Delete firewall rules

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

9.30Device Log

You can crawl the device log, when you encounter unusual problems, please send the device log to the technical staff for positioning problem. For more detail 10.5 get device log.

9.31 Security settings

Enable Tamper: after enable, when the device is removed by force, the alarm information will be sent to the server and the alarm ring will be played.

stwork Basic Settings ne Basic Settings Input & Tamper Server Address: Message: Alarm_Info:Description=\$model;SIP User=\$active_user,Mac=\$mac;IP=\$ip;port=\$trigge Message: Alarm_Info:Description=\$model;SIP User=\$active_user,Mac=\$mac;IP=\$ip;port=\$trigge Input Settings >> Input Settings >> Input Settings >> security exvice Log Output Settings >> Tamper Alarm Settings >> Tamper Alarm Settings >> Tamper Alarm Reset		
twork Basic Settings Ringtone Duration: 2 (1~600)s Input & Tamper Server Address: • Message: Alarm_Info.Description=\$model,SIP User=\$active_user,Mac=\$mac,IP=\$ip,port=\$trigge} It ist Input Settings >> It ist Input Settings >> I list Input Settings >> I riggered By: Low Level Trigger(Close Trigger) ~ Input Settings Dist Mone ~ I input Settings >> Input Settings >> Curity Output Settings >> Vice Log Output Settings >> Eecurity Settings Tamper Alarm Settings >>		
twork Ringtone Duration: Ringtone Duration: Input & Tamper Server Address: Message: Message: Alarm_Info:Description=\$model;SIP User=\$active_user,Mac=\$mac;IP=\$ip;port=\$trigge It ist Input Settings >> Input Settings >> curity vice Log Output Settings >> iecurity Settings	tem	
Message: Alarm_Info:Description=\$model;SIP User=\$active_user;Mac=\$mac;IP=\$ip;port=\$trigge List Apply II List Input Settings >> action Key Input1: Triggered By: Low Level Trigger(Close Trigger) V Triggered By: Low Level Trigger(Close Trigger) V Triggered By: Send SMS Dss Key: None V Apply	work	Ringtone Duration: 2 (1~600)s
Input Settings >> Input Settings >> Input Settings >> Input Settings >> Input Settings >> Input Settings >> Input Settings >>		
Input: Input:: Input::	ercom settings	Apply
Inction Key Triggered By: Low Level Trigger(Close Trigger) Input Duration: 0 (0~3600)s Triggered Action: Send SMS Dss Key: None Triggered Ringtone: None scurity Apply evice Log Output Settings >> Security Settings	List I	
evice Log Output Settings >> Security Settings Tamper Alarm Settings >>	iction Key	Triggered By: Low Level Trigger(Close Trigger) Input Duration: 0 (0~3600)s
Tamper Alarm Settings >>	urity	Apply
Security Settings	rice Log O	utput Settings >>
		amper Alarm Settings >>
		amper Alarm Reset
Reset Alarm Status Reset		

picture 46 - Security settings (1)



> System Output Settings >>	
ouprocessing	
Triggered By DTMF RingTone: None v	
Inggerea by okt kingtone.	
Tinggered By SMS Ringtone: None Line Triggered By Dsskey Ringtone:	
Line Triggered By Dsskey Ringtone: None	
> Intercom settings Voltput1:	
Standard Status: NC:closed > Output Duration: 5 (0~600)s	
→ Call List Output Trigger Mode: Z Trigger By DTMF DTMF Trigger Code: 1234	
DTMF Reset Code: 4321	
Function Key Reset By: By Duration	
☑ Trigger By Active URI Trigger Message: OUT1_SOS	
Security Reset Message: OUT1_CLR	
Z Trigger By SMS Trigger Message: ALERT=OUT1_SOS	
Device Log Reset Message: ALERT=OUT1_CLR	
Trigger By Input:	
Security Settings Drigger By Call State	
Disabled State Enabled State	
Calling A	
Ringing Tatking(calling)	
Talking(Sip)	
Talking(Mcast)	
Trigger By Dsskey: None	
Apply	

picture 47 - Security settings (2)

System	
Network	Basic Settings Ringtone Duration: 2 (1~600)s
Line	Input & Tamper Server Address: Message: Alam_Info Description=\$model;SIP User=\$active_user;Mac=\$mac;IP=\$ip;port=\$trigge
Intercom settings	Apply
Call List	Input Settings >>
Function Key	Output Settings >> Tamper Alarm Settings >>
Security	Enable Tamper Alarm Alarm command Tamper_Alarm
Device Log	Reset command Tamper_Reset Alarm Ringtone None
Security Settings	Apply
	Tamper Alarm Reset Reset Alarm Status Reset

picture 48 - Security settings (3)

Table 20 - 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=i16SV;SIP User=;Mac=0c:38:3e:3a:06:65;IP=; port=Input . The message content can also be customized.		
Message	When the input port is triggered, a short message will be sent to the		



	1			
	server. The m	essage format is as follows:		
	Alarm_Info:Description=\$model;SIP			
	User=\$active	_user;Mac=\$mac;IP=\$ip;port=\$trigger		
Input settings				
Input Detect	Enable or disa	able Input Detect		
	When choosi	ng the low level trigger (closed trigger), detect the input		
Triggered by	port (low leve	I) closed trigger.		
inggered by	When choosi	ng the high level trigger (disconnect trigger), detect the		
	input port (high level) disconnected trigger.			
Input Duration	事件行为在持续检测时间内不断,触发相应的设置			
Triggered Action	启用或禁用输	启用或禁用输入端口发送消息到服务器		
Dss Key	设置为 dsskey 时,触发 dsskey 进行呼叫,默认为 none			
Triggered Ringtone	Select triggered ring tone.			
Output Settings				
Output Detect	Enable or disable Output Detect			
Triggered by				
DTMF Ring tone	Select the DTMF trigger ring tone.			
Triggered by URI				
Ringtone	Select the URI trigger ring tone.			
Triggered By SMS	Select the SMS trigger ring tone			
Ringtone	Select the SMS trigger ring tone.			
Triggered By	Select the Deckov trigger ring tend			
Dsskey Ringtone	Select the Dsskey trigger ring tone.			
	When choosir	ng the low level trigger (NO: normally open), when meet		
Chandend Chatus	the trigger condition, trigger the NO port disconnected.			
Standard Status	When choosing the high level trigger (NC: normally close), when meet			
	the trigger condition, trigger the NC port close.			
Output Duration	Set the output	t change duration time, the default is 5 seconds.		
Output Trigger	When the inp	ut port meets the trigger condition, the output port will		
Mode	trigger (the po	ort level time changes, controlled by < output duration >).		
	Enable or disable trigger by DTMF. The device will check the received			
Trigger by DTMF	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 DTM	/F reset code, default value is 4321.		
Decet Di	D	Reset the output port status when output duration		
Reset By	By duration	occurs.		
-	1	1		



					
	By state	Reset the output port status when device's call state changes.			
	Enable or disa	able trigger by URI.			
Trigger by UDI	User can sei	nd commands from remote device or server to i16SV			
Trigger by URI	series device, if the command is correct, then device will trigger				
	corresponding output port.				
	Enable or disa	able trigger by SMS.			
Trigger by SMS	User can se	end ALERT command to i16SV series device, if the			
	command is c	correct, then device will trigger corresponding output port.			
	Select call sta	te to trigger the output port, options are:			
	Talking: Whe	n the device's talking status changes, trigger the output			
Trigger By Call	port.				
state	Ringing: When the device's ringing status changes, trigger the output				
	port.				
	Calling: When the device's calling status changes, trigger the output				
	port.				
Trigger By DssKey	Enable or dis	able trigger by dsskey. If any of the dsskey is selected,			
when the dsskey application performs, the output port will be trigg		key application performs, the output port will be triggered.			
Tamper Alarm Sett	ings				
Enable Tamper	If the terminal is forcibly removed, the tamper will be triggered and the				
Alarm	set alarm ring	will be played all the time			
Alarm command	When the ala	rm is triggered, the server sends the command			
	immediately				
	If the alarm be	ell needs to be stopped, the remote end can send a short			
Reset command	message to the terminal. The content of the short message is the value				
	set in the reset command. At this time, the terminal will stop playing the				
	alarm bell				
Alarm Ringtone	The ringtone	of alarm			
Tamper Alarm Res	et				
Reset Alarm Status	One key rese	t alarm status			
้อเลเนร					



10 Trouble Shooting

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

10.1 Get device system information

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

Device information (model, software and hardware version) and Internet Information etc.

10.2 Reboot device

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

10.3 Device factory reset

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

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

10.4 Network Packets Capture

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



10.5 Get device log

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

10.6 Common Trouble Cases

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 by Fanvil
	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	1. Please check if the device is connected to the network.
service provider	2. If network connection is fine, please check again your line
	configurations. If all configurations are correct, please kindly contact
	your service provider to get support, or follow the instructions in " 10.4
	Network Packet Capture" to get the network packet capture of
	registration process and send it to Fanvil support to analyze the issue.

Table 21 - Trouble Cases