



User Manual PA2

Software Version: 2.6.0

Release Date: 2019/09/20



Directory

Directory	1
1 Picture	3
2 Table	5
3 Safety Instruction	1
4 Overview	2
5 Install Guide	错误!未定义书签。
5.1 Use POE or external Power Adapter	3
5.2 Install	4
5.2.1 button instruction	4
5.2.2 Confirm the connection	5
5.3 Appendix Table	6
5.3.1 Common command mode	6
5.3.2 Function key LED state	6
6 Basic Introduction	8
6.1 Quick Setting	8
6.2 WEB configuration	8
6.3 SIP Configurations	9
7 Basic Function	10
7.1 Making Calls	10
7.2 Answering Calls	10
7.3 End of the Call	11
7.4 Auto-Answering	11
7.5 DND	
7.6 Call Waiting	13
8 Advance Function	14
8.1 Intercom	14
8.2 MCAST	14
8.3 Hotspot	16
9 Web Configurations	
9.1 Web Page Authentication	18
9.2 System >> Information	
9.3 System >> Account	
9.4 System >> Configurations	
9.5 System >> Upgrade	20

	9.6 System >> Auto Provision	20
	9.7 System >> FDMS	23
	9.8 System >> Tools	23
	9.9 Network >> Basic	24
	9.10 Network >> Advanced	26
	9.11 Network >> VPN	27
	9.12 Network >> Web Filter	28
	9.13 Line >> SIP	29
	9.14 Line >> Basic Settings	32
	9.15 Line >> SIP Hotspot	33
	9.16 Intercom settings >> Blacklist	34
	9.17 Intercom settings >> Features	34
	9.18 Intercom Setting >> Audio	36
	9.19 Intercom Setting >> Video	38
	9.20 Intercom Setting >> MCAST	39
	9.21 Intercom Setting >> action URL	41
	9.22 Intercom Setting >> Time/Date	41
	9.23 Intercom Setting >> Trusted Certificates	43
	9.24 Intercom Setting >> Device Certificates	43
	9.25 Security Settings	44
	9.26 Function Key >> Function Key Settings	46
10 Tr	rouble Shooting	50
	10.1 Get device system information	50
	10.2 Reboot device	50
	10.3 Device factory reset	50
	10.4 Network Packets Capture	50
	10.5 Common Trouble Cases	50

1 Picture

Picture 1 - button instruction	4
Picture 2 - connected graphs	6
Picture 3 - Quickly setting	8
Picture 4 - WEB Login	9
Picture 5 - SIP Line Configuration	9
Picture 6 - Function Setting	10
Picture 7 Function Setting	11
Picture 8 - Enable Auto Answer	11
Picture 9 - Set DND Option	12
Picture 10 - Enable DND	12
Picture 11 - Call Waiting	13
Picture 12 - WEB Intercom	14
Figure 1 - Picture 13 - MCAST	15
Picture 14 - SIP Hotspot	17
Picture 15 - WEB Account	19
Picture 16 - System Setting	19
Picture 17 - Upgrade	20
Picture 18 - Auto provision	20
Picture 19 - FDMS	23
Picture 20 - Tools	24
Picture 21 - Network Basic Setting	24
Picture 22 - Network Setting	26
Picture 23 - VPN	27
Picture 24 - WEB Filter Table	28
Picture 25 - SIP	29
Picture 26 - Network Basic	32
Picture 27 - Line Basic Setting	33
Picture 28 - SIP Hotspot	34
Picture 29 - Blacklist	34
Picture 30 - Feature	35
Picture 31 - Audio	36
Picture 32 - Video Setting	38
Picture 33 - MCAST	40
Picture 34 - Action URL	41
Picture 35 - Time/Date	42
Picture 36 - Trusted Certificates	43

Picture 37	- Trusted Certificates	43
Picture 38	- Alert/Security Settings	44
Picture 39	- Function Key Settings	46
Picture 40	- Hot Key Settings	47
Picture 41	- Multicast Settings	47
Picture 42	- Advanced Settings	48

2 Table

Table 1	- button instruction	4
Table 2	- Common command mode	6
Table 3	- Function key LED state	6
Table 4	- Intercom	14
Table 5	- MCAST	15
Table 6	- SIP Hotspot	16
Table 7	- Auto provision	21
Table 8	- FDMS	23
Table 9	- Network Basic Setting	24
Table 10	- Network Setting	26
Table 11	- SIP	29
Table 12	- Line Basic Setting	33
Table 13	- Common device function Settings on the web page	35
Table 14	- Video Setting	38
Table 15	- MCAST parameters	40
Table 16	- Action URL	41
Table 17	- Time/Date	42
Table 18	- Alert/Security Settings	44
Table 19	- Function Key Settings	46
Table 20	- Hot Key Settings	47
Table 21	- Multicast Settings	47
Table 22	- Advanced Settings	48



3 Safety Instruction

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

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

4 Overview

PA2 is a SIP audio and video intercom developed specifically for the needs of industry users. Media streaming adopts the standard IP/RTP/RTSP protocol. It inherits the advantages of good stability of azimuthphone and carrier-grade sound quality, and is perfectly compatible with all current mainstream sip-based IPPBX/ soft switch /IMS platforms, such as Asterisk, Broadsoft, Metaswitch, 3CX, Elastix, etc. It sets a variety of functional interfaces in one: intercom, broadcast, video, security, recording, broadcast, adapt to a variety of use environment, convenient and rapid deployment of equipment, is the ideal choice.

5 Installation Guide

5.1 Use POE or external Power Adapter

PA2, called as 'the device' hereafter, supports two power supply modes, power supply from external power adapter or over Ethernet (POE) complied switch.

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

For users who do not have POE equipment, the traditional power adaptor should be used. If the device is connected to both PoE switch and external power adapter, PA2 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 Install

Before you start using the device, please install the following:

5.2.1 button instruction



Picture 1 - button instruction

The image above shows the key layout of the device. Each button provides its own specific function. The user can refer to the instructions for the keys in the illustration in this section to operate the device.

Table 1 - button in	struction
---------------------	-----------

Label	Explanation	
	according to the device input voltage adaptive output maximum power; 4 Ω	
1 Snaakar interface	speaker, POE / 10W, 12V / 10W, 18V / 20W, 24V / 30W. The greater the horn	
(1) Speaker Interface	impedance, the smaller the output power. Suggested wire diameter: 18AWG or larger	
	diameter.	
O Handard interface	Speaker audio line signal output impedance 32 Ohm, single ended output voltage 1.2V,	
(2) Headset Interface	used for external headphones or active speakers	
	Output 5V voltage 5 mA current, can be an external LED, indicating the network status,	
(3) LED Interface	call status, registration status.	
④ Function key interface	connection switch, you can log on page set the call number or IP address.	
	Recommend the use of 2.2K Ohm impedance electret condenser microphone,	
(5) Microphone interface	sensitivity: -38dB, bias voltage 2.2V. Microphone signal cable it is recommended to use	
	a shielded cable and do not connect the shield cable to the grounding screw, improve	

	anti-interference.		
6 Switch input interface	Connect an infrared probe or emergency switch or Doorsensor and other switch components.		
⑦ Switch output interface	corresponding to the short-circuit input interface, login device security page settings, you can control the alarm light, electric locks and other equipment; with the adjacent ⑧ power port connection for external equipment power supply.		
8 Power input interface	12V ~ 24V 2A input, according to the input voltage to determine the maximum output power amplifier.		
(9) Camera interface	standard RJ45 interface, connect the original camera, the proposed use of five or five sub-network cable		
WAN port, standard RJ45 interface, 10 / 100M adaptive, support POE inpresentation of the standard to use five or super five network cable.			
(1)Registration/Network LED	indicates network status, call status, registration status. Fast flashing: network anomaly or SIP account exception. Slow flashing: during a call. Always bright: successful registration.		
12 Volume control key	When device is idle, the button is used to adjust the volume of ringtone, when the device is in call, the button is used to adjust call volume and when device is having broadcast, the button is used to adjust broadcast volume.		
③Restore factory key	press and hold for 3 seconds to flash the device to restart and restore the factory settings.		
(14) Recording output	the local microphone voice and call voice mixed output, suitable for computer and		
interface	other equipment recording.		
(15)Grounding screw	When PA2's external part is connected to metal shell or panel, please connect the external part to this interface, in order to prevent static electricity or other interferences which may affect the device's normal working.		

5.2.2 Confirm the connection

Confirm whether the equipment of the power cord, network cable and the boot-up is normal. (Check the network state of light)



Picture 2 - connected graphs

5.3 Appendix Table

5.3.1 Common command mode

Table 2 - (Common	command	mode
-------------	--------	---------	------

Action	Description
Standby to IP	Wait for captain to press volume down button 3s to report IP
	In standby mode, long press the volume button for 10 seconds, and
	there will be a beep sound and the indicator light will flash for 5
Switching notwork	seconds. Within 5 seconds, press the volume up button for three times
Switching network	continuously to switch the network mode. Network status is static or
mode	PPPoE mode will be switched to DHCP mode; When the network is
	DHCP mode, it will be switched to static IP 192.168.1.128, and IP will be
	reported after successful switch

5.3.2 Function key LED state

Туре	LED	State
Line/network Quick flashing R		Registration failed/ network abnormal
	Normally on	Successfully registered
	Slow flashing	In call

6 Basic Introduction

6.1 Quick Setting

Before proceeding with this step, make sure your Internet broadband connection is working properly and complete the network hardware connection. The default factory mode of is fixed IP address mode, which is 192.168.1.128 by default.

- Long press the volume down button on the device for 3 seconds (30 seconds after power on), and the voice will automatically play the IP address of the device or use the "IP scan tool" software to find the IP address of the device. (Download http://download.fanvil.com/tool/iDoorPhoneNetworkScanner.exe)
- Long press the volume up button for 10 seconds (30 seconds after power on), wait for the speaker to emit rapid beep sound, then quickly press the volume up button for three times, the beep stops. After waiting for 10 seconds, the system will automatically broadcast the IP address after successfully switching to dynamic IP acquisition. Switch again to a fixed IP address.
- Login to the device's WEB page for configuration according to the IP address
- Configure the account, user name, server address and other parameters required for registration provided by the service provider on the WEB configuration page;

iDoorPhone Network Scanner(V 1.0)				×		
#	IP Address	Serial Number	MAC Address	SW Version	Description	
1	192.168.1.128	PA2	00:a8:34:68:23:a3	2.1.1.2834	PA2	
						<u>R</u> efresh

Picture 3 - Quickly setting

6.2 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:	
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</u> <u>Web Configurations</u>

6.3 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:

	SIP Basic Settin	ngs SIP Hotspot	Blacklist	
> System				
> Network	Line SIP 1 -			
	Basic Settings >>			
> Line	Line Status	Registered	SIP Proxy Server Address	172.16.1.2
	Phone number	24	SIP Proxy Server Port	5060
Intercom settings	Display name		Backup Proxy Server Address	
	Authentication Name		Backup Proxy Server Port	5060
 Security settings 	Authentication Password		Outbound proxy address	
	Activate		Outbound proxy port	
> Function Key			Realm	
	Codecs Settings >>			
	Advanced Settings >>			
		Apply		

Picture 5 - SIP Line Configuration

7 Basic Function

7.1 Making Calls

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

	interpretating as	DSS K	(ey2				
Key	Туре		Number 1	Number 2	Line		Subtype
DSS Key 1	Hot Key	-	125		SIP1	•	Speed Dial
DSS Key 2	None				SIP1	-	Speed Dial
n ced Settings Jse Function K	ey to Answer	Enat	ole 💌	Enable Speed Dial Hangu	JD E	nabl	e 💌
nced Settings Jse Function K Hot Key Dial Me	ey to Answer ode Select	Enat	ole 💌	Enable Speed Dial Hangu	ıp E	nabl	e 💌
nced Settings Jse Function K Hot Key Dial M Call Switched 1	iey to Answer ode Select îme	Enal Day	-Night v (5~50)Second(s)	Enable Speed Dial Hangi	ıb E	nabl	e

Picture 6 - Function Setting

See detailed configuration instructions 9.26 Function Key

7.2 Answering Calls

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

7.3 End of the Call

Input port l	Multiplexing as	DSS Key	2					
Кеу	Туре		Number 1	Number 2	Line		Subtype	
DSS Key 1	Key Event	-			SIP1	-	Release	-
DSS Key 2	None	_			SIP1	-	Speed Dial	-
iced Settings Jse Function K	ey to Answer	Enable	•	Enable Speed Dial Hang	up E	nable	×	
nced Settings Jse Function K Hot Key Dial Mo	ey to Answer ode Select	Enable Day-Nig	ght 💌	Enable Speed Dial Hang	up E	nable	×	
nced Settings Jse Function K Hot Key Dial Mo Call Switched T	ey to Answer ode Select ime	Enable Day-Nig 16	ght v (5~50)Second(s)	Enable Speed Dial Hang	up E	nable	×	

Picture 7 - - Function Setting

You can hang up the call through the Release key (you can set the function key as the Release key) or turn on the speed dial button to hang up the call. See detailed configuration instructions <u>9.26 Function</u> Key.

7.4 Auto-Answering

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

Web interface:

enter [Intercom Settings] >> [Features], Enable auto answer, set mode and auto answer time and click submit.

	Features Audio	Video	MCAST Action URL	Time/Date Trusted Certificates Device Certificates
› System				
> Network	Limit Talk Duration DND Mode	Disable 💌 Phone 💌	Talk Duration Ban Outgoing	120 (20~600) Second(s)
› Line	Enable Call Waiting Enable Intercom		Enable Call Waiting Tone Enable Intercom Barge	
> Intercom settings	Enable Auto Dial Out	Lines and IP Call	Auto Dial Out Time	5 (3~30)Second(s)
Security settings	No Answer Auto Hangup Dial Fixed Length to Send		Auto Hangup Timeout Send length	30 (1~60)Second(s)
› Function Key	Voice Read IP Description	Enable 💌 PA2 IP Intercom Pho	System Language Enable DND	English 💌
	Enable Headset		Apply	

Picture 8 - Enable Auto Answer

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

- Line2 : Line 2 has an automatic call timeout.
- Line1 and Line2 : Line 1 and line 2 have an automatic call timeout.
- Lines and IP Call : Line and IP direct dial call timeout automatically answer.
- Auto Answer Timeout (0~60)

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

7.5 DND

Users can turn on the do-not-disturb (DND) feature on the device's web page to reject incoming calls (including call waiting). Do not disturb can be set by the SIP line respectively on/off.

Turn on/off all lines of the device without interruption by the following methods:

Web interface: enter [Intercom Settings] >> [Features], set the DND Mode to phone and Enable DND.

	Features Audio	Video	MCAST Action URL	Time/Date Trusted Certificates Device Certificates
> System				
	Limit Talk Duration	Disable 💌	Talk Duration	120 (20~600) Second(s)
> Network	DND Mode	Phone 💌	Ban Outgoing	
	Enable Call Waiting		Enable Call Waiting Tone	
> Line	Enable Intercom		Enable Intercom Barge	
	Enable Intercom Mute		Enable Intercom Ringing	
> Intercom settings	Enable Auto Dial Out		Auto Dial Out Time	5 (3~30)Second(s)
	Enable Auto Answer	Lines and IP Call 💌	Auto Answer Timeout	0 (0~60)Second(s)
Security settings	No Answer Auto Hangup		Auto Hangup Timeout	30 (1~60)Second(s)
	Dial Fixed Length to Send		Send length	4
> Function Key	Voice Read IP	Enable 💌	System Language	English 💌
	Description	PA2 IP Intercom Pho	Enable DND	
	Enable Headset			
			Apply	

Picture 9 - Set DND Option

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

 Web interface: enter [Line] >> [SIP], choose a Line and enter [Line] >> [Advanced settings], Enable DND.

	SIP Basic Settings SI	IP Hotspot Blacklis	;t	
> System				
Network	Line SIP 1			
Line	Basic Settings >>			
> Intercom settings	Advanced Settings >>			
> Intercom settings	Advanced Settings >>		Ping Type	Default
Intercom settings Security settings	Advanced Settings >> Enable DND Blocking Anonymous Call		Ring Type Conference Type	Default
Intercom settings Security settings	Advanced Settings >> Enable DND Blocking Anonymous Call Use 182 Response for Call waiting		Ring Type Conference Type Server Conference Number	Default 💌
Intercom settings Security settings Function Key	Advanced Settings >> Enable DND Blocking Anonymous Call Use 182 Response for Call waiting Anonymous Call Standard	IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Ring Type Conference Type Server Conference Number Transfer Timeout	Default Local
Intercom settings Security settings Function Key	Advanced Settings >> Enable DND Blocking Anonymous Call Use 182 Response for Call waiting Anonymous Call Standard Dial Without Registered	IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Ring Type Conference Type Server Conference Number Transfer Timeout Enable Long Contact	Default Local Second(s)
Intercom settings Security settings Function Key	Advanced Settings >> Enable DND Blocking Anonymous Call Use 182 Response for Call waiting Anonymous Call Standard Dial Without Registered Click To Talk	[] [] None •	Ring Type Conference Type Server Conference Number Transfer Timeout Enable Long Contact Enable Use Inactive Hold	Default Local Second(s)
Intercom settings Security settings Function Key	Advanced Settings >> Enable DND Blocking Anonymous Call Use 182 Response for Call waiting Anonymous Call Standard Dial Without Registered Click To Talk User Agent		Ring Type Conference Type Server Conference Number Transfer Timeout Enable Long Contact Enable Use Inactive Hold Use Quote in Display Name	Default v Local v 0 Second(s

Picture 10 - Enable DND

7.6 Call Waiting

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

	Features Audio	Video	MCAST Action URL	Time/Date Trusted Certificates Device Certificates
> System				
› Network	Limit Talk Duration DND Mode	Disable Phone	Talk Duration Ban Outgoing	120 (20~600) Second(s)
> Line	Enable Call Waiting Enable Intercom Enable Intercom Mute		Enable Call Waiting Tone Enable Intercom Barge Enable Intercom Ringing	V
> Intercom settings	Enable Auto Dial Out Enable Auto Answer	Lines and IP Call	Auto Dial Out Time Auto Answer Timeout	5 (3~30)Second(s) 0 (0~60)Second(s)
Security settings	No Answer Auto Hangup Dial Fixed Length to Send		Auto Hangup Timeout Send length	30 (1~60)Second(s)
› Function Key	Voice Read IP Description	Enable PA2 IP Intercom Pho	System Language Enable DND	English
	Enable Headset	V	Apply	

Picture 11 - Call Waiting

8 Advance Function

8.1 Intercom

The equipment can answer intercom calls automatically.

	Features Audio	Video	MCAST	Action URL	Time/Date	Trusted Certificates	Device Certificates
> System							
> Network	Limit Talk Duration DND Mode	Disable Phone	Talk Durati Ban Outgo	on ing	120 (20~60	0) Second(s)	
› Line	Enable Call Waiting Enable Intercom Enable Intercom Mute		Enable Car Enable Int Enable Int	ercom Barge ercom Ringing			
> Intercom settings	Enable Auto Dial Out Enable Auto Answer	Lines and IP Call	Auto Dial C Auto Answ	out Time er Timeout	5 (3~30) 0 (0~60)	Second(s) Second(s)	
 Security settings 	No Answer Auto Hangup Dial Fixed Length to Send		Auto Hang Send lengt	up Timeout :h	30 (1~60) 4	Second(s)	
› Function Key	Voice Read IP Description	Enable PA2 IP Intercom Pho	System La Enable DN	nguage D	English 💌		
	Enable Headset		Apply				

Picture 12 - WEB Intercom

Table 4 - In	itercom
--------------	---------

Parameters	Description
	When the intercom system is enabled, the device will accept
Enable Intercom	the SIP header call-info of the Call request
	Command automatic call
Enable Intercom Barge	If the option is enabled, PA2 will answer the intercom call 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 Ringing	If the incoming call is intercom call, the device plays the intercom tone.

8.2 MCAST

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

	Features Audio	Video MCAST	Action URL Time/Date	Trusted Certificates Device Certificat
> System				
	MCAST Settings			
? Network	Enable Auto Mcast	Auto Mcast Timeout	Delete Time 10 (5	~10s)
L Lino	Sip Priority	0 Intercom Priority	0 💌	
, cine	Enable Page Priority	Enable Mcast Tone		
> Intercom settings	Index/Priority	Name	Host:port	
· Intercom settings	1			
Socurity cottings	2			
7 Security settings	3			
. Eurotion Kou	4			
> Function Key	5			
	7			
	8			
	9			
	10			
		Apply		

Figure 1 - Picture 13 - MCAST

Table 5 - MCAST

Parameters	Description
Enable Auto Mcast	Send the multicast configuration information by Sip Notify signaling,
	and the device will configure the information to the system for
	multicast listening or cancel the multicast listening in the system after
	receiving the information
Auto Mcast Timeout Delete	When a multicast call does not end normally, but for some reason the
Time	device can no longer receive a multicast RTP packet, this
	configuration cancels the listening after a specified time
SIP Priority	Defines the priority in the current call, with 1 being the highest priority
	and 10 the lowest.
Intercom Priority	Compared with multicast and SIP priority, high priority is pluggable
	and low priority is rejected
Enable Page Priority	Regardless of which of the two multicast groups is called in first, the
	device will receive the higher priority multicast first.
Enable Mcast Tone	When enabled, play the prompt sound when receiving multicast
Name	Listened multicast server name
Host:port	Listened multicast server's multicast IP address and port.

Multicast:

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

8.3 Hotspot

SIP hotspot is a simple utility. Its configuration is simple, 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	The multicast address used by the client and server when the monitoring
Address	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 6 - 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	Basic Settings	SIP Hotspot	Blacklist		
› System						
> Network	Device Table					
	IP	MAC	Alias		Line	
> Line	SIP Hotspot 9					
> Intercom settings	Enable Hot	tspot	Enable 💌			
	Mode Monitor Ty	pe	Broadcast 💌			
Security settings	Monitor Ad	dress	224.0.2.0			
> Function Key	Remote Po Local Port	rt	16360			
	Name		SIP Hotspot			
	Line Settings					
	SIP 1			Enable	v	
	SIP 2			Enable	×	
				Apply		

Picture 14 - 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 Configu	rations Upgrade Auto Provision FDM:	5 Tool
Add New User Username		
Web Authentication Password Confirm Password		
Privilege	Administrators Add	
User Accounts		
User	Privilege	
admin	Administrators	
guest	Users	

Picture 15 - 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
> System					
> Network	Export Configurations	Right click here to SAVE configura	ations in 'txt' format.		
> Line	Import Configurations	Right click here to SAVE configura	ations in 'xml' format.		
Intercom settings		Configuration file:	Select	Import	
 Security settings 	Reset to factory defaults	Click the (Reset) butten to react	the phone to factory	dofaulta	
› Function Key		ALL USER'S DATA WILL BE LOST / Reset	AFTER RESET!	uerauits.	

Picture 16 - 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

Reset Phone

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

9.5 System >> Upgrade

	Information	Account Configurations	Upgrade	Auto Provision	FDMS To	pols
> System						
> Network	Software upgrade	Current Software Version:	2.6.0.6680			
› Line		System Image File		Select	Upgrade	
> Intercom settings						
> Security settings						
› Function Key						

Picture 17 - Upgrade

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

9.6 System >> Auto Provision

	Information Account Configurations Upgrade Auto Provision FDMS Tools
> System	
	Common Settings
› Network	Current Configuration Version
	General Configuration Version
› Line	CPE Serial Number 00100400FV020010000000102032a5d
	Authentication Name
› Intercom settings	Authentication Password
	Configuration File Encryption Key
Security settings	General Configuration File Encryption Key
	Download Fail Check Times 5
> Function Key	Enable Get Digest From Server
	DHCP Option >>
	SIP Plug and Play (PnP) >>
	Static Provisioning Server >>
	TR069 >>
	Apply

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

Picture 18 - Auto provision

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

PNP>DHCP>TR069> Static Provisioning

Transferring protocol: FTP 、 TFTP 、 HTTP 、 HTTPS

Details refer to Fanvil Auto Provision

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

Auto provision	
Parameters	Description
Basic settings	
Current Configuration Version	Shows the current config file's version. If the version of the downloaded configuration file is same with this one, the configuration file will not be applied. If the device confirm the configuration by the Digest method, once the configuration of server is modified or the device's configurations are different
	from server's, the device will download and apply the configurations.
General Configuration Version	Shows the common config file's version. If the version of the downloaded configuration file is same with this one, the configuration file will not be applied. If the device confirm the configuration by the Digest method, once the configuration of server is modified or the device's configurations are different from server's, the device will download and apply the configurations.
CPE Serial Number	Serial number of the equipment
Authentication Name	Username for configuration server. Used for FTP/HTTP/HTTPS. If this is blank the phone will use anonymous
Authentication Password	Password for configuration server. Used for FTP/HTTP/HTTPS.
Configuration File Encryption Key	Encryption key for the configuration file
General Configuration File Encryption Key	Encryption key for common configuration file
Download Fail Check	The default value is 5. If the download configuration fails, it will be
Times	downloaded 5 times.
Enable Get Digest	When the feature is enable, if the configuration of server is
From Server	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.

Table 7 - Auto provision

Enable DHCP Optic	n Set the SIP server address through DHCP option 120.				
120					
SIP Plug and Play	(PnP)				
	Whether enable PnP or not. If PnP is enable, phone will send a SIP				
Enable SIP PnP	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	g Server				
Server Address	Set FTP/TFTP/HTTP server IP address for auto update. The				
Server Address	address can be an IP address or Domain name with subdirectory.				
	The configuration file name. If it is empty, phone will request the				
Configuration File	common file and device file which is named as its MAC address.				
Name	The file name could be a common name, \$mac.cfg, \$input.cfg. The				
	file format supports CFG/TXT/XML.				
Protocol Type	Transferring protocol type, supports $FTP \smallsetminus TFTP \backsim HTTP$ and $HTTPS$				
l Indate Interval	Configuration file update interval time. As default it is 1, means				
Opuale interval	phone will check the update every 1 hour.				
	Provision Mode.				
Undata Mada	1. Disabled.				
Opuale Mode	2. Update after reboot.				
	3. Update after interval.				
TR069					
Enable TR069	Enable TR069 after selection				
Enable TR069	If TROGO is anabled, there will be a prompt tope when connecting				
Warning Tone	in rivolog 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)				
STUN	Enter the STUN address				
server address					
Enable the STUN	Enable the STUN				
TLS Version	TLS Version				

9.7 System >> FDMS

	Information	Account	Configurations	Upgrade	Auto Provision	FDMS	Tools	
> System								
> Network	Doorphone Info Community	Settings Name						
› Line	Building Nur Room Numb	nber er						
› Intercom settings				Apply				
> Security settings								
> Function Key								

Picture 19 - FDMS

Table 8 - FDMS

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

9.8 System >> Tools

	Information Account	Configurations	Upgrade	Auto Provision	FDMS	То
System						
Notwork	Syslog					
Network	Enable Syslog					
	Server Address	0.0.0				
	Server Port	514				
	APP Log Level	None	•			
settings	SIP Log Level	None	•			
		Apply				
ttings	Network Packets Capture					
		Start				
	Auto Reboot Setting					
	Reboot Mode	Disable				
	Fixed Time	2	(0~23)	1		
	Uptime	72	(h)			
		Apply				
	Reboot Phone					
		Click [Reboot] bu	itton to restart	the phone!		
		Reboot				

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

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.

Auto Reboot Setting:

Reboot Mode:

Disable : It will not restart at set time after disabled

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

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

For other details, please refer to 10 trouble shooting

9.9 Network >> Basic

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

	Basic	Advanced	VPN	Web Filter	
› System					
> Network	Network Status				
	IP:		172.16.12.104	1	
	Subnet mas	sk:	255.255.255.0)	
> Line	Default gate	eway:	172.16.12.1		
	MAC:		00:01:02:03:2	2a:5d	
> Intercom settings	MAC Timest	amp:	20160714		
 Security settings 	Setting				
	Static IP 🔘		DHCP 🖲		PPPoE 🔘
> Function Key	DNS Server	Configured by	DHCP	-	
	Primary DNS	5 Server			
	Secondary I	DNS Server			
			Apply		
	Service Port Set	ttings 😧			
	Web Server	Туре	HTTP 💌		
	HTTP Port		80		
	HTTPS Port		443		
			Apply		
	HTTPS Certi	fication File: ht	ttps.pem 4501 E	lytes Uplo	Delete

Picture 21 - Network Basic Setting

Table 9 - Network Basic Setting

Field Name	Explanation
Network Sta	tus
IP	The current IP address of the equipment

Subnet	The current Subnet Mask				
mask					
Default	The current Gateway IP address				
gateway					
MAC	The MAC address of the equipment				
MAC Time	Display the time when the dovice gots the MAC address				
stamp	Display the time when the device gets the Mr. to address				
Settings					
Select the app	ropriate network mode. The equipment supports three network modes:				
	Network parameters must be entered manually and will not change. All				
Static IP	parameters are provided by the ISP.				
DHCP	Network parameters are provided automatically by a DHCP server.				
PPPoF	Account and Password must be input manually. These are provided by				
TTTOE	your ISP.				
If Static IP is cl	nosen, the screen below will appear. Enter values provided by the ISP.				
DNS Server					
Configured	Select the Configured mode of the DNS Server.				
by					
Primary DNS	Enter the server address of the Primany DNS				
Server					
Secondary	Enter the server address of the Secondary DNS				
DNS Server					
attention :					
1) After setting	g the parameters, click 【Apply】 to take effect.				
2) If you change the IP address, the webpage will no longer responds, please enter the					
new IP address	s in web browser to access the device.				
3) If the system	m USES DHCP to obtain IP when device boots up, and the network				
address of the	DHCP Server is the same as the network address of the system LAN,				
then after the s	system obtains the DHCP IP, it will add 1 to the last bit of the network				
address of LAN	and modify the IP address segment of the DHCP Server of LAN. If the				
DHCP access	is reconnected to the WAN after the system is started, and the network				
address assigr	ned by the DHCP server is the same as that of the LAN, then the WAN				
will not be able to obtain IP access to the network					
Service Port Settings					
Web Server	Specify Web Server Type HTTP or HTTPS				
Туре					
	Port for web browser access. Default value is 80. To enhance security,				
HTTP Port	change this from the default. Setting this port to 0 will disable HTTP access.				

Example: The IP address is 192.168.1.70 and the port value is 8090,

	the accessing address is http://192.168.1.70:8090.
UTTDS Dort	Default value is 443. To enhance security, change this from the
HIF3 POIL	default.

9.10 Network >> Advanced

	Basic Advanced	VPN	Web Filter	
› System				
> Network	Link Layer Discovery Protocol (LLDP) Settings		
- Hethork	Enable LLDP 😧		Packet Interval(1~3600)	60 Second(s)
> Line	Enable Learning Function			
	ARP Cache Life			
> Intercom settings	ARP Cache Life	2 Minute		
Socurity sottings	VLAN Settings			
7 Security settings	Enable VLAN		VLAN ID	256 (0~4095)
› Function Key	802.1p Signal Priority	0 (0~7)	802.1p Media Priority	0 (0~7)
	LAN Port VLAN Settings			
	Mode	Disable	LAN Port VLAN ID	254 (0~4095)
			802.1p Priority	0 (0~7)
	DHCP VLAN Settings			
	Option Value	Disabled 💌	DHCP Option Vlan(128-254)	0
	Quality of Service (QoS) Settin	gs		
	Enable DSCP QoS		Signal QoS Priority	46 (0~63)
	Media QoS Priority	46 (0~63)		
	802.1X Settings			
	Enable 802.1X			
	Username	admin]	

Picture 22 - Network Setting

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

Field Name	Explanation
LLDP Settings	
Enable LLDP	Enable or disable LLDP
Packet Interval	LLDP Send detection cycle
Enable Learning Function	Learn the discovered device information on the device
QoS Settings	
Pattern	Voice quality assurance (off by default)
DHCP VLAN Settings	
parameters values	128-254, Obtain the VLAN value through DHCP
WAN port virtual Wan	
WAN port virtual Wan	WAN port Settings
LAN port virtual LAN	

LAN port virtual LAN	LAN port Settings
802.1X	
Enable 802.1X	Enable or disable 802.1X
Username	Confirm Username
Password	Confirm Password

9.11 Network >> VPN

	Basic Advanced	VPN	Web Filter
> System			
> Network	Virtual Private Network (VPN)	Status VPN IP Address:	0.0.0.0
> Line	VPN Mode		
› Intercom settings		Enable VPN 🔲 L2TP 💿	OpenVPN 🖲
> Security settings	Layer 2 Tunneling Protocol (L2	TP)	
› Function Key		L2TP Server Address Authentication Name Authentication Passwo	admin ord
			Apply
	OpenVPN Files		
	OpenVPN Configuration file:	client.ovpn N/A	Upload Delete
	CA Root Certification:	ca.crt N/A	Upload Delete
	Client Certification:	client.crt N/A	Upload Delete
	Client Key:	client.key N/A	Upload Delete

Picture 23 - VPN

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

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

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

■ L2TP

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

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

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

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

OpenVPN

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

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

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

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

9.12 Network >> Web Filter

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

	Basic	Advanced	VPN	Web Filter		
> System						
> Network	Web Filter Table	3				
. Helwork	Start IP Add	lress	End IP Ad	dress	Option	
> Line	Web Filter Table	Settings				
 Intercom settings 	Start IP Add	lress	E	nd IP Address		.dd
	Web Filter Setti	ng 	_			
Security settings	Enable Web	o Filter 🔲		Apply		
> Function Key						
Start IP Address	End I	IP Address		Option	1	
172.16.5.50	172.	16.5.53		Mo	dify Delete	

Picture 24 - WEB Filter Table

Add and remove IP segments that are accessible; Configure the starting IP address within the start IP,

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

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

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

9.13 Line >> SIP

Configure the service configuration for the wire on this page.

	SIP Basic Settings SI	IP Hotspot Blacklist		
› System	Line SIP 1			
> Network	Basic Settings >>			
	Codecs Settings >>			
> Line	Advanced Settings >>			
	······································			
> Intercom settings	Enable DND	[]	Ring Type	Default 💌
	Blocking Anonymous Call		Conference Type	Local 💌
Security settings	Use 182 Response for Call waiting		Server Conference Number	
	Anonymous Call Standard	None	Transfer Timeout	0 Second(s)
Function Key	Dial Without Registered		Enable Long Contact	
	Click To Talk		Enable Use Inactive Hold	
	User Agent		Use Quote in Display Name	
	Response Single Codec		TLS Version	TLS 1.2 💌
	Specific Server Type	COMMON -	Enable DNS SRV	
	Registration Expiration	3600 Second(s)	Keep Alive Type	SIP Option
	Use VPN		Keep Alive Interval	60 Second(s)
	Use STUN		Sync Clock Time	
	Convert URI		Enable Session Timer	
	DTMF Type	RFC2833 -	Session Timeout	0 Second(s)
	DTMF SIP INFO Mode	Send */# 💌	Enable Rport	
	Transportation Protocol	UDP 💌	Enable PRACK	
	Local Port	5450	Auto Change Port	

Picture 25 - SIP



SIP				
Field Name	Explanation			
Basic Settings (Choose the SIP line to configured)				
Line Status	Display the current line status at page loading. To get the up to date line			
	status, user has to refresh the page manually.			

Username		Enter the username of the service account.			
Display name		Enter the display name to be sent in a call request.			
Authentication Name		Enter the authentication name of the service account			
Authentication		Enter the authentication password of the carving account			
Password					
Activate		Whether the service of the line should be activated			
SIP Proxy Serve	r	Enter the IP or FODN address of the SIP provy server			
Address		בוונפו נוופ וד טו רעטוע מעטופאט טו נוופ טור אוטאט צפועפו			
SIP Proxy Serve	r Port	Enter the SIP proxy server port, default is 5060			
Outbound proxy		Enter the IP or FQDN address of outbound proxy server provided by the			
address		service provider			
Outbound proxy	port	Enter the outbound proxy port, default is 5060			
Realm		Enter the SIP domain if requested by the service provider			
Codecs Setting	s				
Set the priority	and ava	ilability of the codecs by adding or remove them from the list.			
Advanced Sett	ings				
		Enable Do-not-disturb, any incoming call to this line will be rejected			
Enable DND		automatically			
Blocking Anonyr	nous				
Call		Reject any incoming call without presenting caller ID			
Use 182 Response for		Set the device to use 182 response code at call waiting response			
Call waiting					
Anonymous	Sot th	e standard to be used for anonymous			
Call Standard	occur				
Dial Without	Set call out by proxy without registration				
Registered	00100				
Click To Talk	Set C	ick To Talk			
User Agent	Set th	e user agent, the default is Model with Software Version.			
Response	lf setti	ng enabled, the device will use single codec in response to an incoming call			
Single Codec	reque	st			
Ring Type	Set th	e ring tone type for the line			
Conforance	Set th	e type of call conference, Local=set up call conference by the device itself,			
Tupo	maxin	maximum supports two remote parties, Server=set up call conference by dialing to			
туре	a conf	a conference room on the server			
Server					
Conference Set the		e conference room number when conference type is set to be Server			
Number					
Enable Long	۸ II	more peremeters in contact field are DEC 2040			
Contact	AIIOW	more parameters in contact neid per RFC 3840			
Enable use	Active	e capture package SDP is inactive, while the hold is sendrecv. Active capture			
inactive hold	packa	ge has no response of 400, etc. Hold the hair inactive			

	After closing the grab packet, you can see that the DSP is sendonly and the hold is			
	sendrecv			
TLS version	TLS version			
Specific Server	Set the line to collaborate with specific server type			
Registration Expiration	Set the SIP expiration interval			
Use VPN	Set the line to use VPN restrict route			
Use STUN	Set the line to use STUN for NAT traversal			
Convert URI	Convert not digit and alphabet characters to %hh hex code			
DTMF Type	Set the DTMF sending mode, there are four types: In-band RFC2833			
	AUTO			
	When the device's DTME type is set to SIP_INEQ			
	The DTMF_SIP_INFO type is configured to send */# and when the device presses			
DTMF SIP	the */# key, the actual value sent is */#:			
INFO Mode	Configured to send 10/11, when the device presses the */# key, the actual value			
	sent is 10/11.			
Transportation Protocol	Set the line to use TCP or UDP for SIP transmission			
Local Port	Set the Local Port			
SIP Version	Set the SIP version			
Caller ID Header	Set the Caller ID Header			
Enable Strict	Enables the use of strict routing. When the phone receives packets from the server,			
Proxy	it will use the source IP address, not the address in via field.			
Enable user=phone	Sets user=phone in SIP messages.			
Enable SCA	Enable/Disable SCA (Shared Call Appearance)			
Enable DNS	Set the line to use DNS SRV which will resolve the FQDN in proxy server into a			
SRV	service list			
Keep Alive	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole			
Туре	opened			
Keep Alive Interval	Set the keep alive packet transmitting interval			
Enable Session Timer	Set the line to enable call ending by session timer refreshment. The call session will be ended if there is not new session timer event update received after the timeout period			

Session			
Timeout	Set the session timer timeout period		
Enable Rport	Set the line to add rport in SIP headers		
Enable PRACK	Set the line to support PRACK SIP message		
Enable DNS	Set the line to use DNS SRV which will resolve the FQDN in proxy server into a		
SRV	service list		
Auto Change	Enchle/Dischle Auto Change Dort		
Port	Enable/Disable Auto Change Port		
Кеер			
Authentication	Keep the authentication parameters from previous authentication		
	Using TCP protocol to guarantee usability of transport for SIP messages above		
AULOTCP	1500 bytes		
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)		
RTP	Cat the name physics for DTD an an other		
Encryption	Set the pass phrase for RTP encryption		
Enable MAC	When each all CID measures strip Mas fields		
Header	When enabled, all SIP messages strip Mac fields		
Enable			
Register MAC	When enabled, register the message ribbon Mac field		
Header			

9.14 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 26 - Network Basic

	SIP Basic Settings	SIP Hotspot Blacklist	
› System			
> Network	SIP Settings Local SIP Port	5060	
> Line	Registration Failure Retry Interval Transaction TimerT1(0.5~10s)	32 Second(s) 500 millisecond	
› Intercom settings	Transaction TimerT2(2~40s) Transaction TimerT4(2.5~60s)	4000 millisecond 5000 millisecond	
 Security settings 	Enable Strict UA Match Strict Branch		
 Function Key 	STUN Settings	Арріу	
	STUN NAT Traversal	FALSE	
	Server Address Server Port	3478	
	Binding Period	50 Second(s)	
	SIP Waiting Time	800 millisecond	

Picture 27 - Line Basic Setting

Table 12 - Line Basic Setting

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

9.15 Line >> SIP Hotspot

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

See $\underline{8.3 \text{ Hotspot}}$ for details.

	SIP Basic Settings	SIP Hotspot Blacklist	
› System			
Network	Device Table		
> Line	IP MAC	Alias	Line
	Enable Hotspot	Enable	
> Intercom settings	Mode Monitor Type	Client 💌 Broadcast 💌	
Security settings	Monitor Address Remote Port	224.0.2.0 16360	
Function Key	Local Port Name	16360 SIP Hotspot	
	Line Settings		
	SIP 1 SIP 2	Enable	•
		Apply	

Picture 28 - SIP Hotspot

9.16 Intercom settings >> Blacklist

Web page to add call limit function, you can set the number or prefix to limit calls. The rules are as follows:

Add x, type number, x cannot call. Add x, type prefix, then the number beginning with x cannot call.

X could be a number or an IP. To add a whitelist rule, the number /IP should be preceded by a "-", followed by a ". ",

After addition, only the number in the whitelist is allowed to call, and the number outside the whitelist is refused.

	SIP Basic Se	ttings SIP Hotspot	Blacklist		
> System					
> Network	Restricted Incoming Calls			Add Delete	Delete All
> Line		Caller ID	Block on Lir	ne	Туре
› Intercom settings	Restricted Outgoing Calls			Add Delete	Delete All
Security settings			Caller ID	Туре	
› Function Key					



9.17 Intercom settings >> Features

Configure intercom Settings.

	Features Audio	Video M	ICAST Action URL	Time/Date Trusted Certificates Device Certificates
› System				
> Network	Limit Talk Duration DND Mode	Disable 💌	Talk Duration Ban Outgoing	120 (20~600) Second(s)
> Line	Enable Call Waiting Enable Intercom		Enable Call Waiting Tone Enable Intercom Barge Enable Intercom Ringing	V V 7
> Intercom settings	Enable Auto Dial Out Enable Auto Answer	Lines and IP Call	Auto Dial Out Time Auto Answer Timeout	5 (3~30)Second(s) 0 (0~60)Second(s)
> Security settings	No Answer Auto Hangup Dial Fixed Length to Send		Auto Hangup Timeout Send length	30 (1~60)Second(s) 4
› Function Key	Voice Read IP Description	Enable 💌 PA2 IP Intercom Pho	System Language Enable DND	English 💌
	Enable Headset		Apply	

Picture 30 - Feature

Features Setting					
Field Name	Explanation				
Basic Settings					
Limit Talk	If user enables the option, PA2 will hang up the call automatically while talk				
Duration	duration is achieved				
Talk Duration	Time out to hang up				
DND (Do Not	DND might be disabled phone for all SIP lines, or line for SIP individually.				
Disturb)	But the outgoing calls will not be affected				
Ban Outgoing	If enabled, no outgoing calls can be made.				
Enable Call	The default value is enabled. Allow users to answer the second call while				
Waiting	maintaining the call.				
Enable Call	The default value is enabled. When enabled, the call waiting tone can be				
	heard while waiting for a call. If this function is turned off, when waiting for a				
waiting tone	call, the beep will not be heard.				
	When the intercom system is enabled, the device will accept the SIP header				
Enable Intercom	call-info of the Call request				
	Command automatic call				
Enable Intercom	Automatically answer calls in intercom mode during a call if the current call				
Barge	is intercom mode				
	Type, refused to answer the new intercom mode				
Enable Intercom	If anabled, mutae incoming calls during an intercom call				
Mute	in enabled, mutes incoming cans during an intercom can.				
Enable Intercom	If anabled, plays intercom ring tong to plat to an intercom call				
Tone	in enabled, plays intercomming tone to alert to an intercom call.				
Enable Auto Dial	Enable Auto Dial Out when timeout				
Out	Enable Auto Dial Out when timeout.				
Auto Dial Out	Configure weiting time for timeout dipling				
Time					
Enable Auto	Enable Auto Answer function				

Table 13 - Common device function Settings on the web page

Answer	
Auto Answer	Set Auto Apswer Timoout
Timeout	Set Auto Answer Timeout
Auto Hangup	Sat the time of no answer auto hangs up
Timeout	Set the time of no answer auto hangs up.
Dial Fixed Length	Configure to anable/disable fixed length automatic dial out numbers
to Send	
Voice Read IP	Turn on or off device voice broadcast IP address
System	Language for configuring voice promote
Language	Language for configuring voice prompts.
Description	Description information displayed on IP scan tool software or FDMS. The
Description	default is "PA2"
Enable Headset	Active speaker and SPK output when enabled, SPK only when off

9.18 Intercom Setting >> Audio

Change voice Settings

	Features Audio	Video	MCAST Action URL	Time/Date Trus	sted Certificates Device Certificates	
> System						
> Network	Audio Settings First Codec	G.722 💌	Second Codec	G.711A 💌		
> Line	Third Codec Fifth Codec	G.711U V None V	Fourth Codec Sixth Codec	G.729AB 💌 None 💌		
> Intercom settings	DTMF Payload Type G.729AB Payload Length	101 (96~127) 20ms 💌	Default Ring Type Tone Standard	Type 1 💌 United Sta		
 Security settings 	G.722 Timestamps Speakerphone Volume Broadcast Output Volume	160/20ms 5 (1~9) 5 (1-0)	G.723.1 Bit Rate MIC Input Volume	6.3kb/s 5 (1~9)		(
› Function Key	Enable VAD	[5] (1~9)	Signal fone volume	4 (0~9)		
		Apply				
	Speaker Settings					
	Speaker	External S	External Speaker Power	10 • W		
		Apply				

Picture 31 - Audio

Table 1 - Voice Settings on web pages

Voice Setting	Voice Settings				
Field Name	Explanation				
First Codec	The first codec choice: G.711A/u, G.722,G.723, G.729,G.726-32				
Second	The exceeded the inc. C 7414/0 C 722 C 722 C 720 C 72C 22				
Codec	The second codec choice: G./11A/u, G./22,G./23, G./29,G./26-32				
Third Codec	The third codec choice: G.711A/u, G.722,G.723, G.729,G.726-32				
Fourth	The forth reduce chainer $C_{2110}(u, C_{222}, C_{222}, C_{220}, $				
Codec	The forth codec choice: G.711A/u, G.722, G.723, G.729, G.726-32				

Five Codec	The Five codec choice: G.711A/u, G.722,G.723, G.729,G.726-32
Six Codec	The Six codec choice: G.711A/u, G.722,G.723, G.729,G.726-32
DTMF	
Payload	The RTP Payload type that indicates DTMF. Default is 101
Туре	
Default Ring	Bing sound there are 0 standard types and 2 user types
Туре	Ring sound – there are 9 standard types and 3 user types.
G.729AB	
Payload	G.729AB Payload length – adjust from 10 – 60 msec.
Length	
G.723.1 Bit	Configure signal tone standard area
Rate	
G.722	Select a timestamp for the g. 722 encoding, optional
Timestamps	160/20ms,320/20ms;
G.723.1 Bit	
Rate	Select the rate of G723, optional5.3kb/s,6.3kb/s;
Speakerpho	
ne Volume	Configure speakerphone volume level
MIC Input	
Volume	Configure the call volume level for the microphone
Broadcast	
Output	Configure the output volume level for broadcast
Volume	
Signal Tone Volume	Configure the output volume level of the signal sound
	Mute detection; If VAD is enabled, the payload length of g.729 should not
Enable VAD	be greater than 20ms
Player Setting	gs
Player	The player has two modes of choice, panel speaker or external speaker. "Panel horn" means that both the speaker and the microphone are installed in the same shell and are mainly used for intercom. At this time, the sound effect of two-way intercom is required to be better. Therefore, the output power of the speaker needs to be optimized to ensure the sound effect of intercom. "External speaker" refers to the external speaker, microphone and speaker are separately deployed, at this time
External speaker power	the broadcast sound requirements are larger External speaker power can only be selected in the "external speaker" mode, 10W/20W/30W respectively. At this time, the impedance of the speaker used is 4 ohms. Note that the corresponding power supply is POE(or 12VDC)/18VDC/24VDC 2A power supply

AEC Settings	
AEC Satting	Provide adjustment parameter Settings for different power connection
ALC Settings	states
Sound Updat	e/Delete
Sound Undate	Optional.wav suffix ring tone upgrade
Sound Optiate	
Sound Delete	The upgraded ringtone is shown in the delete list and can be optionally
Sound Delete	deleted
Alert Info Ring	Settings
The value of	Sets the value to specify the ringtone type
notification	
information	
1 to 10	
Ring Type	Type1-Type9

9.19 Intercom Setting >> Video

	Features Audio	Video	MCAST	Action URL	Time/Date	Trusted Certificates	Dev
System							
Network	Camera Status	Inactive					
	Max Access Num 😧	N/A					
Line	Max M Num	N/A	Use		0		
	Max S Num	N/A	Use		0		
Intercom settings	Ip Camera Connect Settings						
Security settings	Connect Mode	External Apply	-				
Function Key	Ip Camera Settings>>						
Function Key	Ip Camera Settings>> Position	ipCamera	Name	(40 Characters))		
Function Key	Ip Camera Settings>> Position User	ipCamera admin	Name	(40 Characters))		
Function Key	Ip Camera Settings>> Position User Password	ipCamera admin	Name	(40 Characters))		
Function Key	Ip Camera Settings>> Position User Password Ip Camera Brand	ipCamera admin •••••	Name	(40 Characters))		
Function Key	Ip Camera Settings>> Position User Password Ip Camera Brand IP	ipCamera admin ••••• XM	Name	(40 Characters))		
Function Key	Ip Camera Settings>> Position User Password Ip Camera Brand IP Port	ipCamera admin ••••• XM 554	Name	(40 Characters))		
Function Key	Ip Camera Settings>> Position User Password Ip Camera Brand IP Port Main Stream Url	ipCamera admin ••••• XM 554	Name	(40 Characters))		
Function Key	Ip Camera Settings>> Position User Password Ip Camera Brand IP Port Main Stream Url Sub Stream Url	ipCamera admin ••••• XM 554	Name	(40 Characters))		
Function Key	Ip Camera Settings>> Position User Password Ip Camera Brand IP Port Main Stream Url Sub Stream Url User Agent	ipCamera admin XM 554	Name	(40 Characters))		
Function Key	Ip Camera Settings>> Position User Password Ip Camera Brand IP Port Main Stream Url Sub Stream Url User Agent H.264 Stream No SPS&PPS	ipCamera admin XM 554	Name	(40 Characters))		

Picture 32 - Video Setting

Table 14 - Video Setting

Connection Mode	Select external, click submit, and restart the device		
Camera Settings (external mode)			
Field Name	Explanation		

Name	Camera name
User name	External camera login name
Password	External camera login password
Camera type	Select camera manufacturer
IP address	Camera IP address, please use the camera matching scan tool to get the IP address
port	Camera port number
Main Stream Url	After user submit the camera information and apply the changes, if the device connects external camera successfully, the page will display the main stream URL directly, or the information is blank.
Sub Stream Url	After user submit the camera information and apply the changes, if the device connects external camera successfully, the page will display the sub stream URL directly, or the information is blank. If the IP camera user used is not in the list, and user select CUSTOMER as IP camera brand, he also need input the main stream URL manually.
No SPS&PPS h. 264 streams	Compatible with cameras without SPS&PPS can display video normally
Advanced Setting	gs
Video Direction	Sendonly: establish video call, and the SDP packet in the invite packet is Sendonly; Sendrecv: to create a call, the SDP package in the invite package is Sendrecv
RTSP Over TCP	The RTSP goes over the TCP protocol
H.264 Payload	Set the h. 264 Payload type. The range is between 96 and 127. The default is
Default Call Stream	Optional main stream and substream
RTSP Information	on
Main Stream Url	Display the main stream URL address
Sub Stream Url	Display the sub stream URL address

9.20 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.

	Features Audio	Video	MCAST Action URL	Time/Date Trusted C	Certificates Device Certificat
› System					
A Maturali	MCAST Settings				
* NELWORK	Enable Auto Mcast	🔽 At	to Mcast Timeout Delete Time	10 (5~10s)	
s Lino	Sip Priority	0 💌 In	tercom Priority	0 💌	
	Enable Page Priority	🔽 Er	able Mcast Tone		
> Intercom cattings	Index/Priority	Name		Host:port	
· Intercom settings	1				
 Socurity sottings 	2				
7 Security settings	3				
- Eurotian Koy	4				
7 Function Rey	5				
	7				
	8				
	9				
	10				

Picture 33 - MCAST

Table 15 - MCAST parameters

Field Name	Explanation
	SIP Notify information is used to issue mcast configurations, after
Enable Auto Mcast	device receives the information, it can finish the configurations to listen
	the mcast or cancel mcast listening.
	When a multicast call does not end normally, but for some reason
Auto Mcast Timeout Delete	the device can no longer receive the multicast RTP packets,
Time	enable this option will make the device cancel listening after a
	specified period
SIP priority	Defines the priority in the current call, with 1 being the highest
	priority and 10 the lowest.
Broadcast priority	Compared with multicast and SIP priority, higher priority is
	pluggable and low priority is rejected
Enable Page Priority	Two multicasts, regardless of who first calls in, the device will
	accept the multicast with higher priority.
Multicast prompt tone	When enabled, play the prompt sound first when receiving
	multicast
Name	Listened multicast server name
Host: port	Listened multicast server's multicast IP address and port.

9.21 Intercom Setting >> action URL

\square	Features Audio	Video	MCAST	Action URL	Time/Date	Trusted Certificates Device Certificates
> System	Action URL Event Settings					
> Network	Active URI Limit IP Setup Completed					
› Line	Registration Succeeded Registration Disabled					
> Intercom settings	Registration Failed Incoming Call					
> Security settings	Outgoing calls Call Established					
› Function Key	Call Terminated DND Enabled					
	DND Disabled Mute					
	Unmute Missed calls					
	IP Changed Idle To Busy					
	Busy To Idle Input1					
	Reset Input1 Output1					

Picture 34 - Action URL

Table 16 - Action URL

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

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

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

9.22 Intercom Setting >> Time/Date

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

	Features Audio	Video MCAST	Action URL	Time/Date	Trusted Certificates	Device Certificates	
> System							
> Network	Network Time Server Settings Time Synchronized via SNTP						
› Line	Time Synchronized via DHCP Primary Time Server	time.nist.gov					
> Intercom settings	Secondary Time Server Time zone	pool.ntp.org (UTC+8) China,Singapore,	Austra				
Security settings	Resync Period	Apply	~5000)Second(s)				
> Function Key	Daylight Saving Time Settings	Chipa(Reijing)					
	DST Set Type	Automatic 💌					
	Fixed Type	Disabled 💌					
	Offset	0M	inute				
		Start	End				
	Month	January 🚽	January	-			
	Week	First Week 👻	First Week	T			
	Weekday	Sunday -	Sunday	~			
	Hour	0	0	v			
		Apply					

Picture 35 - Time/Date

Table 17 - Time/Date

Time/Date				
Field Name	Explanation			
Network Time Server Settings				
Time Synchronized	via SNTP	Enable time-sync through SNTP protocol		
Time Synchronized	via DHCP	Enable time-sync through DHCP protocol		
Primary Time Serve	r	Set primary time server address		
		Set secondary time server address, when primary server is not		
Secondary Time Ser	rver	reachable, the device will try to connect to secondary time server to		
		get time synchronization.		
Time zone		Select the time zone		
Resync Period		Time of re-synchronization with time server		
Daylight Saving T	ime Setting	s		
Location		Select the user's time zone specific area		
		Select automatic DST according to the preset rules of DST, or the		
DSTSetType		manually input rules		
Offset		The DST offset time		
Month Start		The DST start month		
Week Start		The DST start week		
Weekday Start		The DST start weekday		
Hour Start		The DST start hour		
Month End		The DST end month		
Week End		The DST end week		
Weekday End		The DST end weekday		
Hour End		The DST end hour		
Manual Time Sett	ings	·		

To set the time manually, you need to disable the SNTP service first, and you need to fill in and submit each item of year, month, day, hour and minute in the figure above to make the manual settings successful.

System time: Display system time and its source

(SIP automatic get >SNTP automatic get >manual manual setting)

9.23 Intercom Setting >> Trusted Certificates

User can upload and delete the uploaded certificates in certificate management page.

Ipdate Trusted Certif	icates File			
	Load Trusted Certific	ates File	Select	Upgrade
elete Trusted Certifi	cates File			
	Select Trusted Certific	ates File	Delete	
rusted Certificates F	ile			
File Name	Issued To	Issued By	Expiration	File Size
rusted Certificates S	ettings			
CA Certificates	Disabled			

Picture 36 - Trusted Certificates

9.24 Intercom Setting >> Device Certificates

User can upload and delete the uploaded certificates for device in device certificates page.

Device Certificates	Custom Certificates Apply	s 💌		
Import Certificates				
			act Upland	
Load Device Certificates File		Sele	Opioad	
Load Device Certificates File Certification File		Sele		
Certification File	Issued To	Issued By	Expiration	File Size

Picture 37 - Trusted Certificates

9.25 Security Settings

> System	
> Network	Input Settings Input Detect
> Line	Trigger Mode Low Level Trigger(Close Trigger) 💌 🗹 Alert message send to server 🗌 Reset Alert message send to server
› Intercom settings	Output Response Output Level High Level(NC:closed) Output Duration 5 (1~600)s
> Security settings	Alert Trigger Setting
> Function Key	Output >> Output >>
	Apply
	Server Settings
	Server Address
	Message Alarm_Info:Description=\$model;SIP User=\$active_user;Mac=\$mac;IP=\$ip;port=\$trigger
	Apply

Picture 38 - Alert/Security Settings

Table	18	- Alert/S	Security	Settings
-------	----	-----------	----------	----------

Security Sett	ings					
Field Name	Explanation					
Input settin	gs					
Field Name	Explanation					
Input Detect	Enable or disable Input Detect					
	When choosing the low level trigger (closed trigger), detect the input port (low level)					
Trigger	closed trigger.					
Mode	When choosing the high level trigger (disconnected trigger), detect the input port					
	(high level) disconnected trigger.					
Alert						
message						
send to	Set the Alert message send to server					
server						
Reset Alert						
message						
send to	Enable or disable sending reset messages to the server					
server						
Output Sett	ings					
Output						
Response	Enable or disable Output Response					
Output Level	When choosing the low level trigger (NO: normally open), when meet the trigger					

	condition, tri	gger the NO port disconnected.				
	When choos	ing the high level trigger (NC: normally close), when meet the trigger				
	condition, tri	gger the NO port close.				
Output	The duration	of the changes in the output port, default value is 5 seconds				
Duration	The duration	or the changes in the output port, donant value is 5 seconds.				
Alert Trigge	er Setting					
Input trigger	When the in	put port meets the trigger condition, the output port will be triggered				
	(The trigger d	uration is controlled by option Output Duration.)				
DTMF	By duration	Port switch amount change time, press <output duration=""> control</output>				
output	By Calling	By call state control, after the end of the call, port to return the default				
Duration	State	state				
Remote	Receive the	DTMF password sent by the remote device. If it is correct, trigger the				
DTMF	corresponding output port. You can choose to enable or disable ringtones					
trigger	corresponding output port. You can choose to enable or disable ringtones					
DTMF	During the c	all, the receiving terminal device sends a DTMF password, and if it is				
trigger code	correct, the	corresponding output port is triggered. The default is 1234.				
reset code	After receivi	ng the corresponding instruction, the test device will reset the state and				
	stop playing	the corresponding ringtone				
Active Uri	When device	receives the active URI trigger message sent by the remote device and if it is				
triggers	correct, the co	orresponding output port will be triggered.				
	You can choo	se to enable or disable ringtones.				
Trigger	When the test	device receives the right trigger message, the output port will be triggered				
message		actice receives the fight digger message, the output port will be diggered.				
Reset	When the test	device receives the right reset message, the device will reset its status and				
message	stop playing t	he corresponding ringtone.				
Remote	Enable or di	sable remote SMS triggering. You can choose to enable or disable				
SMS trigger	ringtones					
Trigger	Send instruc	tions on remote devices or servers. ALERT= [set instructions]. if				
Message	correct, trigo	er the corresponding port output.				
Alert	,					
	Continued trig	ggering the output port by device's call status. For example, When the call				
	triggers the ou	atput port, the output will be triggered while the call status does not change.				
	1 Talking					
	2 Talking and	d Ringing				
Call State	3 Ringing					
Trigger	4 Calling					
	5 Calling and	d Talking				
	6 Calling and	d Talking (dialing)				
	7 Calling and	d Ringing				
	8 Calling and	d Ringing(called)				
9 Calling, Ringing and Talking						

Server Setting	S
	Send message to the server when the alarm is triggered. Message format : Alarm
Server	Info: Description=PA2;SIP
Address	User=;Mac=00:a8:34:68:23:d1;IP=172.18.90.235;port=Input1

9.26 Function Key >> Function Key Settings

Key Event

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

🔲 Input port Multiplexi	ng as DSS Key2	2				
Кеу 1	ype	Number 1	Number 2	Line	•	Subtype
DSS Key 1 Key Eve	nt 💌			SIP1	-	Release 💌
DSS Key 2 None				SIP1	-	None
						Redial
						Call Back
ivanced Settings						Release
Use Function Key to Ans	wer Enable		Enable Speed Dial Hangu	p E	nable	ОК
						Handfree
Hot Key Dial Mode Selec	t Day-Nig	ht 🚽				VOL UP
Call Switched Time	16	(5~50)Second(s)				VOL DOWN
Day Start Time	09:00	(00:00~23:59)	Day End Time	1	B:00	(00:00~23:59)

Picture 39 - Function Key Settings

Table 19 - Function Key Settings

Туре	Subtype	Usage
	None	No responding
Key	Release	Delete password input, cancel dialing input and
Event		end call
	ОК	Confirm key
	Call Back	The user can redial the last number dialed
	Redial	Call the nearest missed number
	Handfree	Use as a hands-free button
	VOL UP	Turn up volume
	VOL DOWN	Turn down volume

> Hot Key

When the speed dial key is set as Hot Key, the device will dial pre-set telephone number. The number option can also be configured with IP address. User can press the speed dial button to make direct IP call.

	ruluplexing as	DSS Key2					
Key	Туре		Number 1	Number 2	L	ine	Subtype
DSS Key 1	Key Event	-			SIP1	-	Release
DSS Key 2	Hot Key	-			SIP1	-	Speed Dial
							Speed Dial
and Cottings							Intercom
auced Settings			-				Intercom
a uced Settings Use Function Ke	ey to Answer	Enable 💌]	Enable Speed Dial Ha	ngup	Enabl	Intercom
uced Settings Use Function Ke	ey to Answer	Enable 💌]	Enable Speed Dial Ha	ngup	Enabl	Intercom
Use Function Ke	ey to Answer ode Select	Enable 💌 Day-Night		Enable Speed Dial Ha	ngup	Enabl	Intercom le 💌
Use Function Ke Hot Key Dial Mo Call Switched Ti	ey to Answer ode Select îme	Enable Day-Night	▼ (5~50)Second(s)	Enable Speed Dial Ha	ngup	Enabl	Intercom le 💌

Picture 40 - Hot Key Settings

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

> Multicast

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

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

> System					
> Network	Function Key Settings	DSS Key2			
	Кеу Туре	Number 1	Number 2	Line	Subtype
> Line	DSS Key 1 Key Event	•		SIP1 🔻	Release
	DSS Key 2 Multicast	224.0.0.5:1063		SIP1 🔻	G.711A 💌
Intercom settings					G.711A
	Advanced Settings				G.711U
> Security settings	Use Function Key to Answer	Enable 💌	Enable Speed Dial Hang	up Enab	G.722 G.723.1
					G.726-32
Function Key	Hot Key Dial Mode Select	Day-Night 👻			G.729AB
	Call Switched Time	16 (5~50)Second(s)			
	Day Start Time	09:00 (00:00~23:59)	Day End Time	18:0	0 (00:00~23:59)
		A	pply		

Picture 41 - Multicast Settings

Table 21 - Multicast Settings

Туре	Number	Subtype	Usage		
Set the host IP address and		G.711A	Nerrowband apaceh anding (4Khz)		
	port number, they must be	G.711U	Narrowband speech coding (4Khz)		
Multico	separated by a colon (The IP	G.722	Wideband speech coding (7Khz)		
et	address range is 224.0.0.0 to	G.723.1			
239.25	239.255.255.255, and the	G.726-32	Narrowband speech coding (4Khz)		
	port number is preferably set	C 720 A P	Narrowband speech county (4Khz)		
between 1024 and 65535)		G.129AD			

> PTT

Keep pressing the shortcut key set to make a call, release it and hang up

	Multiplexing as	DSS Key2					
Кеу	Туре		Number 1	Number 2	Line		Subtype
DSS Key 1	Key Event	-			SIP1	-	Release 💌
DSS Key 2	PTT	-			SIP1	ſ	Speed Dial 💌
							Speed Dial
anced Setting	-					Т	Intercom
unceu Setting.	,		_				Multicast
Use Function I	Key to Answer	Enable	-	Enable Speed Dial Hangu	ip Er	abl	
Hot Key Dial M	lode Select	Day-Nigh	t 💌				
	Time	16	(5~50)Second(s)				
Call Switched							

> Advanced Settings

Use Function Key to Answer	Enable 💌	Enable Speed Dial Hangup	Enable 💌
Hot Key Dial Mode Select	Day-Night 👻		
Call Switched Time	16 (5~50)Second(s)		
Day Start Time	09:00 (00:00~23:59)	Day End Time	18:00 (00:00~23:59)

Picture 42 - Advanced Settings

Table 22 - Advanced	l Settings
---------------------	------------

Advanced Settings		
Field Name	Explanation	
Input port is		
multiplexed as	Enable or disable the input port to be multiplexed as speed dial button 2	
function key 2		

Use Function Key to	Enchle er dischle charteute te encurer celle
Answer	Enable of disable shortcuts to answer calls
Enable Speed Dial	Enchle er dischle shorteute te hang up colle
Hang up	Enable of disable shortcuts to hang up calls
	Number 1 call number 2 mode selection.
	<main secondary="">: If the first number is not answered within the set</main>
Hot Key Dial Mode	time, the second number will be automatically switched.
Select	<day night="">: The system time is automatically detected during the call.</day>
	If it is daytime, the first number is called, otherwise the second number
	is called.
Call Switched Time	Set number 1 to call number 2 time, default 16 seconds
Dov Stort Time	The start time of the day when the <day night=""> mode is defined.</day>
Day Start Time	Default "06:00"
Day End Time	The end time of the day when the <day night=""> mode is defined. Default</day>
Day Enu Time	"18:00

10 Trouble Shooting

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

10.1 Get device system information

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

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

10.2 Reboot device

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

10.3 Device factory reset

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

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

10.4 Network Packets Capture

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

10.5 Common Trouble Cases

Trouble Case	Solution
Device could not boot up	1. If the device enters "POST mode" (the SIP/NET and function button
	indicators are always on), the device system is damaged. Please

Table 2 - Common Trouble Cases

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