



# A212 User Manual

Software Version: 2.12.45.10.1

**Release Date: 2024/6/30** 





# Directory

Directory	1
1 Picture	
2 Table	5
3 Safety Instruction	6
4 Overview	7
5 Install Guide	
5.1 Use POE or External Power Adapter	
5.2 Appendix	
5.2.1 Common Command Modes	
5.2.2 LED Status	
6 User Guide	
6.1 Interface Description	
6.2 Installation Instructions	
6.2.1 Installation	
6.2.2 Device IP Address	
6.3 WEB Configuration	
6.4 SIP Configurations	
6.5 Volume Setting	
7 Basic Function	
7.1 Making Calls	
7.2 Answering Calls	
7.3 End of the Call	
7.4 Auto Answer	
7.5 Call Waiting	
8 Advance Function	
8.1 Intercom	
8.2 MCAST	
8.3 Hotspot	
9 Web Configurations	
9.1 Web Page Authentication	
9.2 System >> Information	
9.3 System >> Account	
9.4 System >> Configurations	
9.5 System >> Upgrade	



	9.6 System >> Auto Provision	
	9.7 System >> Tools	29
	9.8 System>>Reboot	
	9.9 Network >> Basic	
	9.10 Network >> Service Port	
	9.11 Network>>VPN	
	9.12 Network >> Advanced	
	9.13 Line>> SIP	
	9.14 Line >> SIP Hotspot	42
	9.15 Line >> Basic Settings	42
	9.16 Line>>Action Plan	44
	9.17 Settings >> Features	
	9.18 Settings >> Noise Reducation	47
	9.19 Settings >> Media Settings	48
	9.20 Settings>>Camera Settings	49
	9.21 Settings >> MCAST	51
	9.22 Settings >> Action	51
	9.23 Settings >> Time/Date	51
	9.24 Settings>>Time plan	53
	9.25 Settings >> Tone	54
	9.26 Call list >> Call List	55
	9.27 Call list >> Web Dial	55
	9.28 Function Key	56
	9.29 Security >> Web Filter	60
	9.30 Security >> Trust Certificates	61
	9.31 Security >> Device Certificates	
	9.32 Security >> Firewall	
	9.33 Device Log	64
	9.34 Security Settings	65
10 T	rouble Shooting	68
	10.1 Get Device System Information	68
	10.2 Reboot Device	
	10.3 Device Factory Reset	
	10.4 Network Packets Capture	
	10.5 Get Device Log	
	10.6 Common Trouble Cases	



# 1 Picture

picture 1 - Interface	10
Picture 2 - WEB Login	. 13
Picture 3 - SIP Line Configuration	. 14
Picture 4 - Volume Set	. 14
Picture 5 - Function Setting	. 15
Picture 6 - WEB line enable auto answer	. 16
Picture 7 - Enable auto answer for IP calls	16
Picture 8 - Call Waiting	17
Picture 9 - Call Waiting tone	17
Picture 10 - WEB Intercom	. 18
Picture 11 - MCAST	. 19
Picture 12 - SIP hotspot	. 21
Picture 13 - WEB Account	23
Picture 14 - System Setting	23
Picture 15 - Upgrade	24
Picture 16 - Web page firmware upgrade	. 25
Picture 17 - Auto provision settings	. 27
Picture 18 - Tools	. 30
Picture 19 - Network Basic Setting	. 31
Picture 20 - Service port setting interface	. 32
Picture 21 - Network VPN	33
Picture 22 - Network Setting	. 35
Picture 23 - SIP	. 38
Picture 24 - Basic Settings	43
Picture 25 - Line Basic Setting	. 43
Picture 26 - Action Plan	44
Picture 27 - Feature	45
Picture 28 - Media Settings	48
Picture 29 - Camera Settings	. 50
Picture 30 - Action URL	51
Picture 31 - Time/Date	52
Picture 32 - Time Plan	. 53
Picture 33 - Tone	55
Picture 34 - Webpage Dial	. 56
Picture 35 - Function Key	56
Picture 36 - Memory Key	. 59



Picture 37 - Multicast	60
Picture 38 - Advanced Setting	60
Picture 39 - WEB filter	61
Picture 40 - Trust Certificates	
Picture 41 - Device Certificates	62
Picture 42 - Firewall	63
Picture 43 - Firewall rules list	64
Picture 44 - Delete firewall rules	64
Picture 45 - Security Settings	65



# 2 Table

Table 1 - Common command mode	8
Table 2   - LED Status	9
Table 3   - Interface	10
Table 4   - Configuration instructions	12
Table 5 - Intercom	18
Table 6 - MCAST	19
Table 7   - SIP Hotspot	20
Table 8 - Firmware upgrade	25
Table 9 - Auto Provision	27
Table 10   - Network Basic Setting	
Table 11 - Server Port	
Table 12 - Network Setting	35
Table 13 - SIP	
Table 14 - Line Basic Setting	43
Table 15   - Action Plan	44
Table 16 - Common device function Settings on the web page	45
Table 17 - Media Settings	
Table 18 - Camera Settings	
Table 19 - Action URL	51
Table 20 - Time/Date	52
Table 21 - Time Plan	53
Table 22 - Function Key	56
Table 23 - Memory Key	
Table 24 - Web Multicast	60
Table 25 - Web Firewall	63
Table 26 - Security Settings	65

# 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 product-specified power adapter. If you need to use a power adapter provided by another manufacturer due to special circumstances, please confirm that the voltage and current of the provided adapter meet the specifications of this product, and it is recommended to use a product that has passed safety certification, otherwise it may cause fire or electric shock accidents. When using this product, do not damage the power cord, do not twist, stretch and strap it, and do not press it under heavy objects or sandwich between items, otherwise it may cause fire or electric shock accident fire or electric shock caused by broken power cord.
- 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.
- 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

A212 is a wall-mounted broadcasting and intercom speaker that boasts powerful features, combining intelligent security, audio/video intercom, and broadcasting functions. It offers high cost-effectiveness.

The A212 system features strong compatibility and high expandability, supporting standard SIP 2.0 (RFC3261) and related RFC protocols. Suitable for indoor and outdoor scenarios, it provides users with high-quality communication and intercom services.

Moreover, the speaker can be used with a broadcasting system to meet the audio playback needs of public areas, supporting 10 multicast zone priorities and utilizing G.722 and Opus encoding for high-quality voice communication. It also supports external passive speakers for enhanced sound expansion.

With wall-mount installation, the A212 saves space and is easy to deploy in various environments. Whether used in corporate offices, educational institutions, or public spaces for information broadcasts, this speaker delivers clear and stable audio output, making it an ideal choice for efficient communication and broadcasting.



# 5 Install Guide

#### 5.1 Use POE or External Power Adapter

A212, 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, A212 will get power supply from power adaptor in priority, and change to external power adapter once the power adaptor supply fails.

Note:

- The current POE power supply default is AT mode. If the current POE power supply is in AF mode, adjust the speaker power to 7W in [Device Settings] >> [Media Settings] >> [Speaker Power] to avoid the risk of over power.
- When using an external passive speaker, it must be powered by a 24V power supply, otherwise it may not function properly.

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 Common Command Modes

Action behavior	Description		
Standby report IP	In standby mode, long press the Reset button for 3 seconds, there		
	will be a toot sound will 5 seconds, please press the Reset butt		

#### Table 1- Common command mode



	once within 5 seconds, the toot sound will stop automatically		
	reporting IP		
	In the standby mode, long-press the Reset button for 3 seconds		
	and the beep will last for 5 seconds. Within 5 seconds, press Reset		
	button three times quickly to switch to the network mode.		
	If there is no IP at present, switch to the default static IP		
Switch network	(192.168.1.128).		
mode	Then switch to DHCP mode when it is the default static IP		
(192.168.1.128) When DHCP gets to IP, then do not switch and repo			
	Report the IP after the successful switch.		

#### 5.2.2 LED Status

# TypeIndicator statusIndicator statusLED LightBlue light solidNetwork anomalyBlue slow flashNetwork abnormal/no network cable plugged<br/>inGreen light solidCallingGreen slow flashRegistration failed

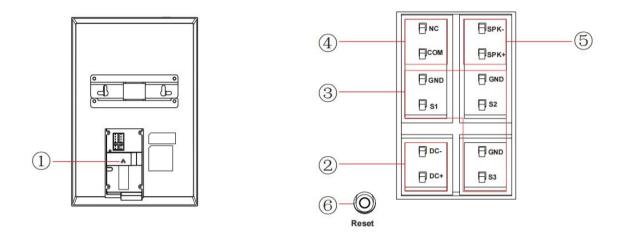
#### Table 2 - LED Status



# 6 User Guide

# 6.1 Interface Description

On the back of the device, there is a row of terminal blocks for connecting the power supply, indoor switches, etc., the connection is as follows:



picture 1- Interface

 Table 3 - Interface

SN	Description				
	Ethernet interface: standard RJ45 interface, 10/100M adaptive,				
1	support POE powered, it is recommended to use CAT5 or CAT5E				
	network cable.				
2	Power interface: DC 24V/2A input.				
3	3 set of short-circuit input interface: input devices for connecting				
	switches, infrared sensor, door sensor, vibration sensors etc.				
	1 set of short-circuit output interface: corresponding to the				
4	short-circuit input interface, login device web page settings,				
	can be connected to electric locks, etc.				
	1 set of SPK interface: supports connecting $8\Omega 15W$ passive speakers.				
5	(Standard DC24V/2A power supply support, do not use POE power s				
	upply!)				
(6)	Reset button, supports the following functions:				
	Report the IP address: Long press reset button for3 seconds, and				



when the speaker beeps rapidly, press reset button again quickly, th				
stop, the speaker will report the IP address by itself. e beeps				
Switch IP address acquisition mode: Long press reset button for 3				
seconds, and when the speaker beeps rapidly, press reset button				
three times, after the success of the system automatically broadcast				
the current IP address.				
Factory reset: Long press reset button for 10 seconds, the device will				
be restored to factory settings.				

#### 6.2 Installation Instructions

#### 6.2.1 Installation

Wall-mounted installation:

Drill holes on the wall to be installed, the hole spacing is 80mm. And then drive the rubber plug into the wall, and use the two screws provided with the equipment to drive the hole into the wall.

B. Open the cable cover of the speaker, connect the network cable, if you need to connect other input and output devices, you can access the corresponding interface of the speaker, lead out the cable from the bottom, cover the cable cover.

C. Align the hole of the wall hanging bracket at the back of the speaker with two screws, and clamp it to fix it without shaking.

D. Power on the device, If it works normally, the installation is complete.

#### 6.2.2 Device IP Address

#### Method one:

1. Go to the official website of Fanvil [Support] >> [Download Center] >>[Tools]>> [IPScanner] module, click and download the DeviceManager,

2. Open the IP scan tool, the tool supports LAN scan and cross network segment scan.

3. For LAN scanning:

.Click the desktop icon, run the DeviceManager tool

4. Cross-segment scan: Fill in the cross-segment setting in the upper right corner of the page in the format of: IP address/mask. That is: IP address/N.



Devic	e Manager	Device				
Total: 28	Search	Q Version Status	Refresh		0.0.0/24	Rescan
Index	MAC	IP Address	Model 🗸	Version	Version Status	description
1	• 0c:38:3e:2f:7a:eb	172.16.7.123	i57A	1.0.0.29		2000 X
2	• 0c:38:3e:16:94:c4	172.16.7.129	V62	T2.12.16.3.2		
3	• 0c:38:3e:26:be:66	172.16.7.149	X5U-V2	2.12.16.15		12221
4	• 0c:11:05:18:81:b9	172.16.7.120	C319	119.30.1.242		1575
5	• 0c:38:3e:2f:c2:36	172.16.7.100	X303	2.12.4.1		
6	• 0c:38:3e:2f:c2:02	172.16.7.192	X301	2.12.4.1		1221
7	34:3a:6e:8c:87:16	172.16.7.126	i64	2.12.19		(375)
8	• 00:a8:59:ff:b2:43	172.16.7.93	GW11G	2.4.5		
9	00:a8:59:ff:b2:43	172.16.7.93	GW11G	2.4.5		1221
10	• 00:a8:59:ef:4c:71	172.16.7.108	IP Phone	2.4.3		1000
11	• 0c:38:3e:3d:b0:20	172.16.7.103	X6U	2.4.11		
12	• 00:a8:59:ff:b2:62	172.16.7.111	GW12G	2.4.5		
13	• 0c:38:3e:2f:7a:ed	172.16.7.118	i57A	1.0.0.71		
14	• 0c:38:3e:30:10:e5	172.16.7.107	X7	2.4.5		1000
15	• 00:a8:59:db:15:5e	172.16.7.102	X6U	2.4.12		
16		170 16 7 1 10	14/74011	TO 10 / bardware//arei		

#### Method two:

After the device boots up (about 30s), in standby mode, press and hold the Call button (the key with the serial number 6 in the <u>6.1 panel Overview</u>) for 3s, release the key immediately after the speaker beeps, and then press the Reset button quickly within 5s (the same key as the above long press), and the device starts to broadcast IP.

#### Method three:

After the device boots up (about 30s), in standby mode, press and hold the Call button (the key with serial number 6 in <u>6.1 panel Overview</u>) for 3 seconds, release the key immediately after the speaker beeps, and then press the Call button three times quickly within 5s (the same key as the above long press) to complete the operation. After successfully switching to dynamic IP, the system automatically announces the IP address by voice.

Default configuration					
DHCP mode		Default enable	Static IP	192.168.1.128	
Voice read IP		Long press the Reset button for 3	Server port	80	
address		seconds, press the Reset button one			
		times within 5 seconds			



#### 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:	
Password:	
Password.	
Language:	English 🔻 📃

Picture 2 - 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:



	SIP SIP Hots	pot Basic Settings	Accie	on Plan			
System							NOTE
Network	Line (1010@SIP >)						Description:
	Register Settings >>						It shows phone registration account basic
Line	Line Status:	Registered		Activate:			settings and sip account function advanced
	Username:	1010	0	Authentication User:		0	settings.
Settings	Display name:	1010	0	Authentication Password:		0	
	Realm:		0	Server Name:		0	
Call List							
	SIP Server 1:			SIP Server 2:			
Function Key	Server Address:	172.16.1.7	0	Server Address:		0	
	Server Port:	5060	0	Server Port:	5060	0	
Security	Transport Protocol:	UDP 🗸 🕜		Transport Protocol:	UDP 🗸 🕜		
	Registration Expiration:	3600 second(s)	0	Registration Expiration:	3600 second(s)	0	
Device Log							
	Proxy Server Address:		0	Backup Proxy Server Address:		0	
Security Settings	Proxy Server Port:	5060	0	Backup Proxy Server Port:	5060	0	
	Proxy User:		0				
	Proxy Password:		0				
	Basic Settings >>						
	Codecs Settings >> 🕜						
	Advanced Settings >>						
	SIP Global Settings >>						
	oottings + -	Apply					

Picture 3 - SIP Line Configuration

# 6.5 Volume Setting

Set the volume (if the speaker or microphone is not connected, you can skip it)

[Settings] >> [Media Settings] >> [Media Settings], as shown below, click [Apply].

Speakerphone Volume: Set the speaker output volume.

Handfree Mic Gain: Microphone volume level.

Media Settings >>					
Default Ring Type:	1.wav 🗸	0			
Speakerphone Volume:	7	(1~9) 🕜	Speakerphone Ring Volume:	5	(0~9) 🤇
Speakerphone SignalTone Volume:	5	(1~9)			
DTMF Payload Type:	101	(96~127) 🕜			
Handfree Mic Gain:	3	(1~9)			
OPUS Payload Type:	107	(96~127)	OPUS Sample Rate	OPUS-NB({ ✓	
ILBC Payload Type:	97	(96~127) 🕜	ILBC Payload Length	20ms 🗸 🕜	
Enable VAD:					
Audio Delay:	0	(0~1000ms)			
RTP Control Protocol(RTCP) Settings	>>				
RTP Settings >>					
Alert Info Ring Settings >>					

Picture 4- Volume Set



# 7 Basic Function

#### 7.1 Making Calls

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

	Function	Key												
> System														NOTE
Network	Function Key	Key Setting Type		Name	Value			Subtyp	e	Line		Media		Description: Soft function key, which
Line	DSS Key	None	~			+	-	None	~	AUTO	~	DEFAULT	~	can be defined by soft function key on different
Line	DSS Key 2	Key Event	~			+	-	Handfree	~	AUTO	~	DEFAULT	~	call interface.
Device Settings	0.00.11	None	~			+	-	None	~	AUTO	~	DEFAULT	~	
Call List		nable Key !			[	Apply	)							
Function Key				• • >>										
Security	Advanced	Settings >	•>											
Device Log														

#### **Picture 5- Function Setting**

See detailed configuration instructions 9.29 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

When there is a call, you can press the Call button or hang up the key to hang up the call, the Call button is set to end the call by default. See detailed configuration instructions <u>9.29 Function</u> Key.

#### 7.4 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], Enable auto answer and set auto answer time and click submit.



					NOTE
vork	Line SIP1 🗸				Description:
	Register Settings >>				It shows phone registration account basic
Line	Basic Settings >>				settings and sip account function advanced
Settings	Enable Auto Answering:	20	Auto Answering Delay:	0 (0~120)second(s) 🥝	settings.
	Enable Hotline:				
Call List	Hotline Delay:	0 (0~9)second(s) @	Hotline Number:	0	
	Dial Without Registered:		The first fi		
unction Key	DTMF Type:	AUTO V	DTMF SIP INFO Mode:	Send 10/11 V	
	Request With Port:				
Security	Use STUN:		Use VPN:		
Device Log	Enable Failback:	2 🕜	Signal Failback:		
	Failback Interval:	1800 second(s) 🕜	Signal Retry Counts:	3 (1~10)	
Security Settings	Codecs Settings >> 💡				
	Advanced Settings >>				
	SIP Global Settings >>				
		Apply			

Picture 6 - WEB line enable auto answer

SIP P2P auto answering:

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

	SIP SIP Hotspot	Basic Settings Action Plan	
> System			NOTE
> Network	STUN Settings STUN NAT Traversal:	FALSE	Description:     Phone line basic settings,     including STUN, certificate
> Line	Server Address: Server Port:	3478	files.
› Settings	Binding Period: SIP Waiting Time:	50 second(s) 800 millisecond	0 0
Call List		Apply	
› Function Key	SIP P2P Settings Enable Auto Answering		0
› Security	Auto Answering Delay: DTMF Type:	0 (0~120)second(s) RFC2833 V	0 0
> Device Log	DTMF SIP INFO Mode: Block RTP When Alerting:	Send 10/11 V	0
Security Settings		Apply	

Picture 7- Enable auto answer for IP calls

• Auto Answer Timeout (0~120)

The range can be set to  $0\sim120$ s, and the call will be answered automatically when the timeout is set.



# 7.5 Call Waiting

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

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

• Web interface: enter [Settings] >> [Features], enable/disable call waiting, enable/disable call waiting tone.

	Features Media Settings	Camera Settings	MCAST	Action	Time/Date	Time Plan	Tone	ι
tem							NOTE	
twork	Basic Settings >> Enable Call Waiting:						Description: Function setting	
ine	Enable Auto On Hook:	2 🕜		Auto HangUp Delay:	3	(0~30)second(s)	set the phone f including the ba	eatures, isic
	Auto HangUp Tone:						settings, tone s DND settings, i	ntercom
Device Settings	Enable Silent Mode:			Disable Mute For Ring:			settings, redial the correspond settings, passw	ng code
all List	Ban Outgoing:						settings, passw settings, power settings.	
	Default Ans Mode:	Video 🗸 🕜		Default Dial Mode:	Video 🗸 🕜			
unction Key	Enable CallLog:	Enable	v 🕜					
	Enable Restricted Incoming List	t: 🗹 🕜						
ecurity	Enable Restricted Outgoing List	: 🗹 🕜		Enable Country Code:	: 🗆			
	Country Code:			Area Code:				
evice Log	Allow IP Call:			P2P IP Prefix:				
curity Settings	Caller Name Priority:	LocalContact-NetConta	act-SIP DisplayName 🗸					
	Search path:	LDAP	v 🕜	LDAP Search:	✓ Ø			
tform Access								
	Restrict Active URI Source IP:	172.16.65.69	0	Push XML Server:		0		
	Line Display Format:							

#### Picture 8 - Call Waiting

	Featur	Media Settings	Local IP Camera	MCAST	Action	Time/Date	Time Plan	Tone	Led	
> System								NOTE		
> Network	Basic Se	ettings >>						Description:		
	Tone Se	ttings >>						Function setting set the phone f	gs, you can	
> Line	Ena	ble Holding Tone:			e Call Waiting Tone:	2 🕜		including the ba	asic	
		Dialing DTMF Tone:	2 🕜	Play T	alking DTMF Tone:			settings, tone s DND settings, i	ntercom	
Settings		Boot Tone:						settings, redial the correspond	ing code	
	Ring	g Back Tone:	Default	✓ Busy	Tone:	Default 🗸		settings, passw settings, power	ord dial	
› Call List	Intercor	n Settings >>						settings.		
> Function Key	Respons	se Code Settings >>		Apply	)					
> Security										
> Device Log										
> Security Settings										

Picture 9 - Call Waiting tone



# 8 Advance Function

#### 8.1 Intercom

The equipment can answer intercom calls automatically.

Network   Basic Settings >>   Tone Settings >>   Ine   Ine   Inercom Settings >>   Intercom Settings >>   Enable Intercom Tone:   Call List   Response Code Settings >>   Porticion Key   Security   Device Log		Features Media Settings	Local IP Camera	MCAST	Action	Time/Date	Time Plan	Tone	Led
> Network   Tone Settings >>   Ine   Ine <td< td=""><td>› System</td><td></td><td></td><td></td><td></td><td></td><td></td><td>NOTE</td><td></td></td<>	› System							NOTE	
Ine Intercom Settings >>   Settings Enable Intercom:   Call List Response Code Settings >>   Ponction Key   Ponction Key   Ponction Key	> Network								
> Settings Enable Intercom Tone: ☑ ◎ Enable Intercom Barge: ☑ ◎   > Call List > Function Key > Security > Device Log O Private Log	› Line	Intercom Settings >>						set the phone f including the ba settings, tone s	eatures, asic ettings,
Call List     Response Code Settings >>     settings, power light settings.       > Function Key     Apply       > Security       > Device Log	> Settings							settings, redial the correspond	settings, ng code
<ul> <li>Security</li> <li>Device Log</li> </ul>	› Call List	Response Code Settings >>		Apply				settings, power	ord dial light
Device Log	> Function Key								
	> Security								
> Security Settings	> Device Log								
	Security Settings								

Picture 10 - WEB Intercom

Table	5- In	itercom
-------	-------	---------

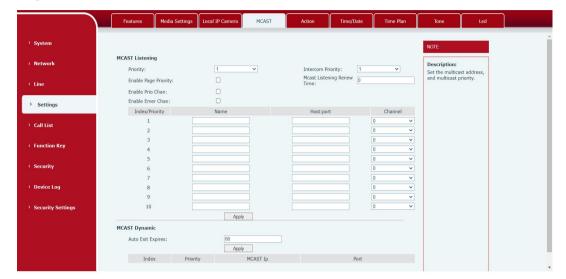
Parameters	Description
	When the intercom system is enabled, the device will accept
Enable Intercom	the SIP header call-info of the Call request
	Command automatic call
Enable Intercom Barge	If the option is enabled, device will answer the intercom call automatically while it is in a normal call, and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

#### 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.



#### Picture 11 - MCAST

Table 6- MCAST

Parameters	Description
Priority	Defines the priority in the current call, with 1 being the highest priority
	and 10 being the lowest.
Intercom Priority	The priority of the intercom call, 1 is the highest priority, 10 is the
	lowest, and the high priority can be inserted into the low priority
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 Prio Chan	Once enabled, the same port and channel can only be connected.
	Channel 24 is the priority channel, higher than 1-23; A channel of 0
	indicates that no channel is used
Enable Emer Chan	When enabled, channel 25 has the highest priority
Multicast Listening Renew	Set the wait time to renew to the multicast
Time	

#### 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 [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 the quantity of sip accounts. 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
Local Port	It shows the Hotspot listening port.Enter the custom hotspot
	communication port. The ports of the server and client 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 7 - 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 Hotspot Basic Settings Action Plan	
› System		NOTE
> Network	No Registration	
PNELWORK	SIP Hotspot Settings	Description: Hotspot feature settings.
> Line		Hot client as the
· Line	Enable Hotspot: Disabled V Mode: Client V	end to connect to the hot
> Settings	Mode: Client V Monitor Type: Broadcast V	server side has an
7 Settings	Monitor Type: Broadcast  Monitor Address: 224.0.2.0	<ul> <li>incoming call, the client</li> <li>will ring at the same time,</li> </ul>
a marine	Local Port: 16360	and can replace server to answer. The server and
Call List	Name: SIP Hotspot	the client can use the hot
		cornet to call each other.
> Function Key	Line Settings	
	Line 1: Enabled ¥	]
> Security	Line 2: Enabled V	]
> Device Log	Apply	
Security Settings		

#### Picture 12 - 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
- MEM info
- 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 A	ccount Configuration	is Upgrade	Auto Provision	FDMS	Tools	Reboot	
> System							NOTE	
> Network	Add New User Username			0			Description:	legin
> Line	Web Authentication Confirm Password	Password		<b>@</b>			Set or modify the user name and pa	ssword.
> Settings	Privilege		Administrators V					
› Call List	User Accounts							
> Function Key	ad	ser min		Privilege Administrators				
> Security	gu User Management	est		Users				
> Device Log	admin 🗸		Delete	odify				
Security Settings							L	

Picture 13- 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	1 - C
> Network	Export Configur	ations 🕜	Right click he	ere to SAVE configu	irations in 'txt' format.			Description: This page is used to	1
> Line			Right click he	ere to SAVE nc conf	figurations in 'txt' forma irations in 'xml' format.			manage configuration of the phone, including, import/export configuration, reset	
› Settings	Import Configu	rations 🕝	C - E N	<i>E</i> .	6	lect Imp	- 1	configuration partly/totally.	
› Call List	Clear Configura	tion >> 🕐	Configuration		Se	lect Imp	DIT		
> Function Key			Click "Clear"	button to reset the	e configuration files!				
		Content to Keep			Content to	Reset			
> Security		MMI BASIC NETWORK SIP		•	DSS KEY TR069		-		
> Device Log		AUTOPROVISION			1				
Security Settings				-	]				
			-				*		
				Clear					
		4							

Picture 14 - 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

#### 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: T2.12.8	Description: This page is used to
> Line	System Image File: Select Upgrade	upgrade some files for phone, including firmware, ring tones, wall
> Settings	Upgrade Server Upgrade Server Address1:	paper, etc.
Y Call List	Upgrade Server Address2: Apply	
Function Key	Firmware Information	
• Security	Current Software Version: T2.12.8 Server Firmware Version: Upgrade	
> Device Log	New Firmware Information:	
Security Settings	Ring Upgrade 🎯	
	Load Server File: Select (*.wav,*.mp3,etc.tar.g2) Upload	
	Ring List 📀	
	Index File Name File Size	

Picture 15- 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. Upgrade the ringtone, support wav and MP3 format.

#### Firmware Upgrade:

• Web page:	Login phone	web page, go t	o [System]	] >> [Upgra	de].		
	Information	Account Configuratio	ons Upgrade	Auto Provision	FDMS	Tools	Reboot Phone
> System							NOTE
> Network	Software upgrade	Ourrent Software Version:	T0.0.17				Description: This page is use
› Line		System Image File:		Select	Upgrade		phone, includin firmware, ring
› Intercom settings	Upgrade Server Upgrade Serv						
› Call List	Upgrade Serv	er Address2:	Ap	oply			
> Function Key	Firmware Informa	tion Current Software Version:	T0.0.17				
› Security		Server Firmware Version:	Checking				
› Device Log		New Firmware Information:					
> Security Settings	Ring Upgrade 🕜						
		Load Server File:		Select	(*.wav, *.mp3)	Upload	
	Ring List 🕜						
		Index	File Nam	e	File Size	Delete	

Picture 16 - Web page firmware upgrade

#### Table 8- Firmware upgrade

Parameter	Description
Upgrade server	
	Enable automatic upgrade, If there is a new version txt
Enable Auto Upgrade	and new 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 server, the page will display version information
[Upgrade] button	and upgrade button will become available; Click
	[Upgrade] button to upgrade the new firmware.
New version description	When there is a corresponding TXT file and version on



information	the server side, the TXT and version information will be	
	displayed under the new version description information.	

- The file requested from the server is a TXT file called vendor\_model\_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 server, as shown in the figure:

名称	修改日期	类型	大小
fanvil_x6_hwv1_0.txt	2018/9/11 17:57	文本文档	1 KB
fanvil_x6_hwv1_1.txt	2018/9/11 17:57	文本文档	1 KB
fanvil_x6_hwv1_2.txt	2018/9/11 17:57	文本文档	1 KB
fanvil x6 hwv1 3.txt	2018/9/11 17:57	文本文档	1 KB
ac-6904-P0.12.12-1.6.3-2502T2018-0	2018/8/21 19:52	WinRAR 压缩文	35,847 KB

- TXT file format must be UTF-8
- vendor\_model\_hw10.TXT The file format is as follows:

Version=1.6.3 #Firmware

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

Ххххх

Ххххх

• After the interval of update cycle arrives, if the server has available files and versions, the phone will prompt as shown below. Click [view] to check the version information and upgrade.

#### 9.6 System >> Auto Provision

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



	Information Account Configuratio	ns Upgrade Auto Provision FDM	IS Tools	Reboot Phone
System				NOTE
Network	Basic Settings			Description
	CPE Serial Number:	00100400FV02001000000c3b4c8c1597	0	Auto Provis
ine	Authentication Name:		0	to realize remote/aut
ine :	Authentication Password:		0	installation
	Configuration File Encryption Key:		0	delpoymen and some of
tercom settings	General Configuration File Encryption Key:		0	files.
	Download Fail Check Times:	1		
all List	Save Auto Provision Information:		0	
	Download CommonConfig enabled:			
unction Key	Enable Server Digest:		0	
ecurity	DHCP Option >>			
	DHCPv6 Option >>			
evice Log	SIP Plug and Play (PnP) >>			
ecurity Settings	Static Provisioning Server >>			
	Autoprovision Now >>			
	TR069 >>			
	App	ly ly		

Picture 17- Auto provision settings

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

#### PNP>DHCP>TR069> Static Provisioning

Transferring protocol: FTP 、 TFTP 、 HTTP 、 HTTPS

Table 9-A	uto Provision
-----------	---------------

Auto provision	Auto provision			
Parameters	Description			
Basic settings				
	Shows the current config file's version. If the version of the			
	downloaded configuration file is same with this one, the			
Current Configuration	configuration file will not be applied. If the device confirm the			
Version	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.			
	Shows the common config file's version. If the version of the			
	downloaded configuration file is same with this one, the			
General	configuration file will not be applied. If the device confirm the			
Configuration Version	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 for common configuration file		
Encryption Key	Encryption key for common configuration file		
Download Fail Chec	k The default value is 5. If the download configuration fails, it will be		
Times	downloaded 5 times.		
Enable Get Digest From Server	When the feature is enable, if the configuration of server is		
	changed, phone will download and update.		
Download			
CommonConfig	Set whether to enable downloading generic profiles		
enabled			
Enable Server Digest computer digest by server before downloading			
Provision Config Priority	Provision Config Priority		
DHCP Option			
	The equipment supports configuration from Option 43, Option 66,		
Option Value	or a Custom DHCP Option. It may also be disabled.		
Custom Option Value			
Enable DHCP Option 120			
DHCPv6 Option			
Option Value	DHCP Option type for Auto Provisioning.		
•	When Option Value is selected as Custom Option, you can		
Custom Option Value	e customize the value of the Option, which ranges from 128~254		
SIP Plug and Play (			
	Whether enable PnP or not. If PnP is enable, phone will send a SIP		
	SUBSCRIBE message with broadcast method. Any server can		
Enable SIP PnP	pport 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 nort		
	PnP port		
Transport Protocol	PnP port PnP protocol, TCP or UDP.		



Static Provisionin	g Server			
	Set FTP/TFTP/HTTP server IP address for auto update. The address			
Server 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 $\$ TFTP $\$ HTTP and HTTPS			
Lindata Interval	Configuration file update interval time. As default it is 1, means			
Update Interval	phone will check the update every 1 hour.			
	Provision Mode.			
Update Mode	1. Disabled.			
	2. Update after reboot.			
	3. Update after interval.			
Auto provision No	W			
TR069				
Enable TR069	Enable TR069 after selection			
Enable TR069	If TP060 is enabled, there will be a prompt tope when connecting			
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)			
STUN	Enter the STUN address			
server address	Enter the STON address			
Enable the STUN	Enable the STUN			
TLS Version	TLS Version			
INFORM Sending	TR069 message cycle.			
Period	Valid Value:1~9999 seconds.			

# 9.7 System >> Tools

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



	Information Account	Configurations Upgrade	Auto Provision	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.
> Device Settings	APP Log Level: Export Log:				0	
> Call List	LAN Network Capture	Apply				
> Function Key	Start	stop				
> Security	Watch Dog Enable Watch Dog:					
> Device Log	Diagnostics 😵	Apply				
> Security Settings	Command Option: IP Address:	PING V	Start	stop		
> Platform Access	Diagnostics Result:				-	x

Picture 18 - 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.

# 9.8 System>>Reboot

	Information	Account	Configurations	Upgrade	Auto Provision	FDMS	Tools	Reboot
> System								NOTE
> Network	Reboot		Click [R	leboot] button to re	start the device!			Description:
> Line				Reboot	]			Reboot phone directly.
> Settings								
> Call List								
› Function Key								
› Security								
> Device Log								
Security Settings								
			Fanvil Tech	Version: T2. nology Co., Ltd. (C)2	12.9 023 All Rights Reserved			

#### 9.9 Network >> Basic

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



	Basic Service Port	VPN Advanced			
> System					NOTE
> Network	Network Mode 🎯 Network Mode:	IPv4 Only V			Description: You can do some simple
> Line	IPv4 Network Status				network configuration on this page, including IP, subnet mask, gateway,
> Device Settings	ETH IP: Subnet Mask:	172.16.7.232 255.255.255.0			DNS, etc.
› Call List	Default Gateway: MAC:	172.16.7.1 0c:38:3e:61:38:5a			
> Function Key	IPv4 Settings Static IP 〇	DHCP ()	PPPoe O		
› Security	DHCP Hostname: Enable Vendor Identifier:	A212 Disabled V		0	
> Device Log	Vendor Identifier: DNS Server Configured By:	Fanvil A212 DHCP V		0	
Security Settings	Primary DNS Server: Secondary DNS Server : DNS Domain:	223.5.5.5 114.114.114.114		0	
> Platform Access	Divs Domain:			v	
		Apply			

# Picture 19 - Network Basic Setting

#### Table 10 - Network Basic Setting

Field Name	Explanation	
Net Type	IPv4, IPv6, IPv4 and IPv6 three modes	
IPv4 Network	Status	
IP	The current IP address of the equipment	
Subnet	The current Subnet Mask	
mask		
Default	The current Gateway IP address	
gateway	The current Galeway in address	
MAC	The MAC address of the equipment	
MAC Time	Display the time when the device gets the MAC address	
stamp	Display the time when the device gets the MAC address	
Settings		
Select the app	propriate network mode. The equipment supports three network modes:	
Static IP	Network parameters must be entered manually and will not change. All parameters are provided by the ISP.	
DHCP	Network parameters are provided automatically by a DHCP server.	
PPPoE	Account and Password must be input manually. These are provided by your ISP.	
If Static IP is c	hosen, the screen below will appear. Enter values provided by the ISP.	
DHCP	Set the name that is displayed when DHCP scanning	
Hostname	Set the name that is displayed when Drice scanning	
DNS Server	Select the Configured mode of the DNS Server.	



Configurad				
Configured				
by				
Primary DNS	Enter the server address of the Primary DNS.			
Server	Litter the server address of the Filmary DNS.			
Secondary	Enter the conver address of the Secondary DNS			
DNS Server	Enter the server address of the Secondary DNS.			
attention :				
1) After settin	g the parameters, click【Apply】to take effect.			
2) If you chang	ge the IP address, the webpage will no longer responds, please enter the			
new IP address in web browser to access the device.				
3 ) If the system 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	system obtains the DHCP IP, it will add 1 to the last bit of the network			
address of LA	N and modify the IP address segment of the DHCP Server of LAN. If the			
DHCP access is reconnected to the WAN after the system is started, and the network				
address assigned by the DHCP server is the same as that of the LAN, then the WAN				
will not be able	e to obtain IP access to the network			

# 9.10 Network >> Service Port

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

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

Picture 20- Service port setting interface

Table 11- 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

		VPN Advanced	
System			
Network	Virtual Private Network (VPN) VPN IP Address:	Status 0.0.0.0	
Line	VPN Mode		
	Enable VPN:		0
Intercom settings	Enable NAT:		
	L2TP: O	OpenVPN:	
Call List	Open VPN mode:	tun 💌	0
unction Key	Layer 2 Tunneling Protocol (L	2TP)	
	L2TP Server Address:	0.0.0.0	0
Security	Authentication Name:		0
	Authentication Password:		0
Device Log			
		Apply	
Security Settings	OpenVPN Files 🔞		
	Load OpenVPN File	Select U	pload
	Certificates List 🕜		
	Index	File Name	File Size
			Delete

Picture 21- 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.ovpnCA Root Certification:ca.crtClient Certification:client.crtClient 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.

	Basic Wi-Fi Settings	Service Port V	PN Advanced		
ł.					NOTE
	Link Layer Discovery Protocol (I	LDP) Settings			
ork	Enable LLDP: 9		Packet Interval:(1~3600)	60 second(s) 🕜	Description: LLDP/CDP/VLAN are to
	Enable Learning Function:				allow system access to VLAN by vian tagged
	Cisco Discovery Protocol (CDP)	Settings			itself; DSCP is to provide QoS; 802.1X is to allow
5	Enable CDP:	Y	Packet Interval:(1~3600)	60	system pass switch's authentication to access
1	DHCP VLAN Settings				to LAN
	Option Value:	Custom Option 🗸 🔮	Option Value Data Type:	Auto 🛩	
n Key	DHCP Option Vlan(128-254):	132	]		
	Quality of Service (QoS) Setting	s			
<b>v</b>	Enable DSCP:		Signal DSCP:	46 (0~63) 🕜	
	Audio DSCP:	46 (0~63) 🕜			
1	ARP Cache Life				
ettings	ARP Cache Life	2 Minute 🕜			
	WAN VLAN Settings				
	Enable VLAN:		WAN VLAN ID:	256 (0~4095) 🕜	
	802.1p Signal Priority:	0 (0~7) 🕜	802.1p Media Priority:	0 (0~7)	
			Apply		
	802.1X Settings				
	802.1x Mode:	Off 🗸		0	
	Identity:	admin		0	
	Password:			0	

#### 9.12 Network >> Advanced

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	
Enable DSCP	Enable DSCP to get best offset QoS for voice quality.
Signal DSCP	DSCP value for SIP messages.
Audio DSCP	DSCP value for voice RTP data.
ARP Cache Life	Set ARP cache life.
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	
CA Certificate	CA certificate.	
Device Certificate	device certificate.	
Certification File	System's HTTPS server CA file.	

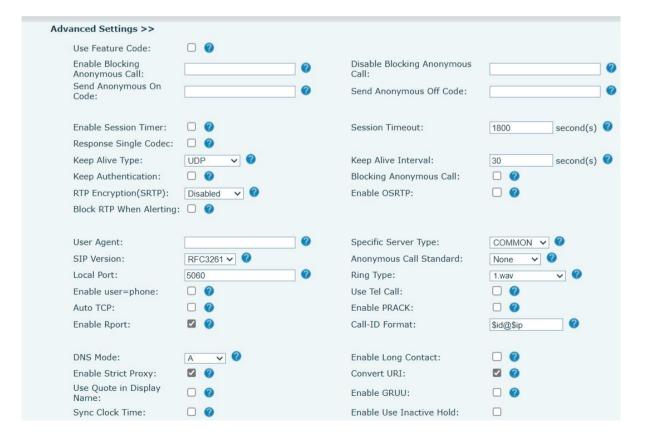
# 9.13 Line>> SIP

	SIP SIP Hots	spot Basic Settings			
› System					
› Network	Line 1356@SIP· •				
> Line	Register Settings >> Line Status:				
Line	Username:	Registered	Activate: Authentication User:	2 0	
Intercom settings		1356	Authentication Oser: Authentication Password:		0
Intercom setungs	Display name: Realm:		Server Name:		0
	Realm:		Server Name:		0
Call List					
	SIP Server 1:		SIP Server 2:		
Function Key	Server Address:	172.16.1.2	Server Address:		0
	Server Port:	5060	Server Port:	5060	0
Security	Transport Protocol:	UDP V	Transport Protocol:	UDP V	-
	Registration Expiration:	3600 second(s) 🕐	Registration Expiration:	3600 second(s)	0
Device Log		·			
	Proxy Server Address:	0	Backup Proxy Server Address:		0
Security Settings	Proxy Server Port:	5060	Backup Proxy Server Port:	5060	0
	Proxy User:	0		-	
	Proxy Password:	0			
	Basic Settings >>				
	Codecs Settings >> 💡				
	Advanced Settings >>				
	SIP Global Settings >>	Apply			



Basic Settings >>			
Enable Auto Answering:		Auto Answering Delay:	0 (0~120)second(s) 🤇
Enable Hotline:			
Hotline Delay:	0 (0~9)second(s) 😗	Hotline Number:	0
Dial Without Registered:			
DTMF Type:	AUTO 🔻 🥝	DTMF SIP INFO Mode:	Send 10/11 🔹 🕜
Request With Port:			
Use STUN:		Use VPN:	?
Enable Failback:		Signal Failback:	
Failback Interval:	1800 second(s) 🕜	Signal Retry Counts:	3 (1~10) 🕜







		Caller ID Header:	PAI-RPID-FIV
Use 182 Response for Call waiting:			
Enable Feature Sync:		Enable SCA:	
Enable Click To Talk:		Enable ChangePort:	
VQ Name:		VQ Server:	· · · · · · · · · · · · · · · · · · ·
VQ Server Port:	5060	VQ Http/Https server:	
Server Expire:	2		
TLS Version:	TLS 1.2 🗸 🕜		
Unregister On Boot:		Enable MAC Header:	
Enable Register MAC Header:			
PTime(ms):	Disabled V millisecond	Enable Deal 180:	
Transaction Timer T1:	500 (500~10000)millisecond <b>2</b>	Transaction Timer T2:	4000 (2000~40000)millisecond
Transaction Timer T4:	5000 (2500~60000)millisecond 2	Enable TCP Transaction Timer:	
CallPark Number:	<b>Ø</b>		
Intercom Number:			

### Picture 23-SIP

Table 13 - SIP

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.
Server Address	Enter the IP or FQDN address of the SIP server
Server Port	Enter the SIP server port, default is 5060
Authentication User	Enter the authentication user of the service account
Authentication Password	Enter the authentication password of the service account
Username	Enter the username of the service account.
Display Name	Enter the display name to be sent in a call request.
Activate	Whether the service of the line should be activated
Realm	Enter the SIP domain if requested by the service provider
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server
Proxy Server Port	Enter the SIP proxy server port, default is 5060
Proxy User	Enter the SIP proxy user
Proxy Password	Enter the SIP proxy password
Backup Proxy Server	Enter the IP or FQDN address of the backup proxy server
Address	
Backup Proxy Server Port	Enter the backup proxy server port, default is 5060
Basic Settings	



Enable Auto Answering	Enable auto-answering, the incoming calls will be answered automatically after the delay time	
Auto Answering Delay	Set the delay for incoming call before the system automatically answered it	
Call Forward Unconditional	Enable unconditional call forward, all incoming calls will be forwarded to the number specified in the next field	
Call Forward Number for Unconditional	Set the number of unconditional call forward	
Call Forward on Busy	Enable call forward on busy, when the phone is busy, any incoming call will be forwarded to the number specified in the next field	
Call Forward Number for Busy	Set the number of call forward on busy	
Call Forward on No Answer	Enable call forward on no answer, when an incoming call is not answered within the configured delay time, the call will be forwarded to the number specified in the next field	
Call Forward Number for No Answer	Set the number of call forward on no answer	
Call Forward Delay for No Answer	Set the delay time of not answered call before being forwarded	
Transfer Timeout	Set the timeout of call transfer process	
Conference Type	Set the type of call conference, Local=set up call conference by the	
	device itself, maximum supports two remote parties, Server=set up call	
	conference by dialing to a conference room on the server	
Server Conference	Set the conference room number when conference type is set to be	
Number	Server	
Subscribe For Voice Message	Enable the device to subscribe a voice message waiting notification, if enabled, the device will receive notification from the server if there is	
	voice message waiting on the server	
Voice Message Number	Set the number for retrieving voice message	
Voice Message Subscribe Period	Set the interval of voice message notification subscription	
Enable Hotline	Enable hotline configuration, the device will dial to the specific number	
	immediately at audio channel opened by off-hook handset or turn on	
	hands-free speaker or headphone	
Hotline Delay	Set the delay for hotline before the system automatically dialed it	
Hotline Number	Set the hotline dialing number	
Dial Without Registered	Set call out by proxy without registration	



Enable Missed Call Log	If enabled, the phone will save missed calls into the call history record.
DTMF Type	Set the DTMF type to be used for the line
DTMF SIP INFO Mode	Set the SIP INFO mode to send '*' and '#' or '10' and '11'
Enable DND	Enable Do-not-disturb, any incoming call to this line will be rejected
	automatically
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
Codec Settings	Set the priority and availability of the codecs by adding or remove them
	from the list.
Advanced Settings	·
Use Feature Code	When this setting is enabled, the features in this section will not be
	handled by the device itself but by the server instead. In order to
	control the enabling of the features, the device will send feature code
	to the server by dialing the number specified in each feature code field.
Enable DND	Set the feature code to dial to the server
Disable DND	Set the feature code to dial to the server
Enable Call Forward	Set the feature code to dial to the server
Unconditional	
Disable Call Forward	Set the feature code to dial to the server
Unconditional	
Enable Call Forward on	Set the feature code to dial to the server
Busy	
Disable Call Forward on	Set the feature code to dial to the server
Busy	
Enable Call Forward on	Set the feature code to dial to the server
No Answer	
Disable Call Forward on	Set the feature code to dial to the server
No Answer	
Enable Blocking	Set the feature code to dial to the server
Anonymous Call	
Disable Blocking	Set the feature code to dial to the server
Anonymous Call	
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	Set the feature code to dial to the server
Code	
Send Anonymous Off	Set the feature code to dial to the server



Code		
SIP Encryption	Enable SIP encryption such that SIP transmission will be encrypted	
SIP Encryption Key	Set the pass phrase for SIP encryption	
RTP Encryption	Enable RTP encryption such that RTP transmission will be encrypted	
RTP Encryption Key	Set the pass phrase for RTP encryption	
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 BLF List	Enable/Disable BLF List	
BLF List Number	BLF List allows one BLF key to monitor the status of a group. Multiple	
	BLF lists are supported.	
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	
User Agent	Set the user agent, the default is Model with Software Version.	
Specific Server Type	Set the line to collaborate with specific server type	
SIP Version	Set the SIP version	
Anonymous Call Standard	Set the standard to be used for anonymous	
Local Port	Set the local port	
Ring Type	Set the ring tone type for the line	
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	
Transport Protocol	Set the line to use TCP or UDP for SIP transmission	
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	Whether to add quote in display name, i.e. "Fanvil" vs Fanvil	



Name	
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)
Sync Clock Time	Time Sycn with server
Caller ID Header	Set the Caller ID Header
Use 182 Response for	Set the device to use 182 response code at call waiting response
Call waiting	
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.
Enable Feature Sync	Feature Sycn with server
Enable SCA	Enable/Disable SCA (Shared Call Appearance)
CallPark Number	Set the callPark number
Server Expire	
TLS Version	Choose TLS Version
PTime(ms)	Set whether to bring ptime field, default no.
Transaction Timer T1	Configure the duration of SIP transaction timer T1
Transaction Timer T2	Configure the duration of SIP transaction timer T2
Transaction Timer T4	Configure the duration of SIP transaction timer T4

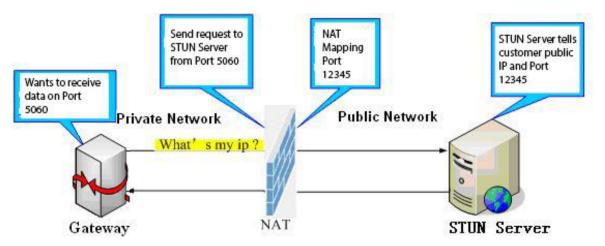
### 9.14 Line >> SIP Hotspot

SIP hotspot is a simple and practical function. It is simple to configure, can realize the function of group vibration, and can expand the number of SIP accounts. See <u>8.3 Hotspot</u> for details.

### 9.15 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 24- Basic Settings

	SIP SIP Hotspot	Basic Settings		
› System				NOTE
> Network	STUN Settings STUN NAT Traversal:	FALSE	0	Description: Phone line basic settings,
› Line	Server Address: Server Port:	3478	0 0	including STUN, certificate files.
> Intercom settings	Binding Period: SIP Waiting Time:	50 second(s) 800 millisecond	0	
› 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 •	0	
> Security Settings		Apply		

Picture 25 - 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	

### 9.16 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 Basic Settings Action Plan Paging Server
> System	
> Network	Action Plan Add Action: MCAST-Xter V
> Line	Number: Direction: Both V V Line: AUTO V V
› Settings	MCAST Codec: PCMU V V URL:
→ Call List	Action Plan Option
> Function Key	Delete Modify
> Security	User-defined Action Plan Table Index Action Number Type Direction Line URL Index Username URL UserAgent
> Device Log	
› Security Settings	

Picture 26 - Action Plan

 Table 15 - Action Plan

Parameters	Description
	Convert multicast: When the rule is triggered, the phone converts
Action	incoming calls or multicast to multicast and sends them to the set
	multicast address port.
Number	The calling number corresponding to each Action Plan; The same
	number expression as the dial plan is supported
	123;1xx;1.;1[3,5,7,8]xxxxxxxx;5753[5-6]xxxx
	X means any bit match;
	Indicates any bit matching;
	[] represents a matching rule corresponding to a certain bit;



Line	The selected rule corresponds to the matching SIP line			
	The behavior of the corresponding configuration rule is handled			
Direction	Both: trigger both incoming and outgoing calls at the same time;			
Direction	Outgoing call: Triggered when outbound calling:			
	Incoming call: triggered when inbound call;			
MCAST				
Codec	Set MCAST Codec			
MCAST URL	The URL corresponding to the action plan			

# 9.17 Settings >> Features

	Features Media Settings	Camera Settings	MCAS	5T Action	Time/I	Date Ti	me Plan	Tone
System								NOTE
	Basic Settings >>							
Network	Enable Call Waiting:	<b>e</b> 🕜						Description: Function settings, you car
and the second se	Enable Auto on Hook:			Auto HangUp Delay:	3	(0~30)second	d(s) 🕜	set the phone features,
Line	Enable Silent Mode:	<b>e</b> 🕜		Disable Mute for Ring:				including the basic settings, tone settings,
								intercom settings, the corresponding code
Intercom settings	Ban Outgoing:							settings.
	Default Ans Mode:	Video 🔻 🕜		Default Dial Mode:	Video 🔻 🤇			
Call List	Enable Restricted Incoming List:	<b>I</b>						
1200024032400	Enable Restricted Outgoing List	· 🕑 🕜		Enable Country Code:				
Function Key	Country Code:			Area Code:				
Security	Allow IP Call:	<b>e</b>		P2P IP Prefix:				
Device Log	Restrict Active URI Source IP:		0	Push XML Server:		6		
	Line Display Format:	xxx@SIPn 🔻 🚷						
Security Settings	Call Number Filter:			Auto Resume Current:	<b>e</b>			
1000 C	Limit Talking Duration:			Talking Duration:	120	(20~600)sec	ond(s)	
	No Answer Auto HangUp Timeout:	130 (1~300)second(s)		Enable Push XML Auth:	• •			
	Tone Settings >>							
	Intercom Settings >>							
	Response Code Settings >>		-	Apply				

## Picture 27 - Feature

Table 16- Common device function Settings on the web page	Table 16- Common	device function	Settings on the	web page
---	------------------	-----------------	-----------------	----------

Parameters	Description				
Basic Settings					
Enable Call Waiting	Enable this setting to allow user to take second incoming call during an				
established call. Default enabled.					
Enchle Auto en Lleek	The device will hang up and return to the idle automatically at				
Enable Auto on Hook	hands-free mode.				
	Specify Auto On hook time, the device will hang up and return to the idle				
Auto Hang Up Delay	automatically after Auto Hand down time at hands-free mode, and play				
	dial tone Auto On hook time at handset mode.				



Auto HangUp Tone	Enable auto hang up tone to play tone after peer hangs up			
Enable Silent Mode	When enabled, the phone is muted, there is no ringing when calls, you			
	can use the volume keys and mute key to unmute.			
Disable Mute for Ring	When it is enabled, you can not mute the phone.			
Rop Outgoing	If you select Ban Outgoing to enable it, and you cannot dial out any			
Ban Outgoing	number.			
Enable Restricted	Whether enable Restricted Incoming List			
Incoming List				
Enable Restricted	Whether enable Restricted Outgoing List			
Outgoing List				
Enable country Code	Whether 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 dial pad and press dial key ,it will call 172.16.2.160			
	automatically			
Disable AEC	Enable or disable AEC functionality			
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.			
Line Display Format	Line display format including SIPn/SIPn : xxx/xxx@SIPn			
Block XML When Call	Blocked Push XML When Call			
SIP Notify	when enabled, when the phone receives relevant notify content, the			
	corresponding information will be displayed.			
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			
Limit Talking Duration	Automatically hang up the call after enabling the time set for the call			
Talking Duration	Call duration ,20-600s			
Call Timeout	The remote phone does not answer within the time, the local			
	automatically hangs up			
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			
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.
Enable Http Api Auth	Enable HttpApi authentication push xml
Http API UserName	Set the Http API username
Http Api PassWord	Set the HTTP API password
Description	Sets the description information displayed
Tone Settings	
Enable Holding Tone	whether enable call holding tone.
Enable Call Waiting Tone	whether enable call waiting tone.
Play Dialing DTMF Tone	Play DTMF tone on the device when user pressed a phone digit at
	dialing, default enabled
Play Talking DTMF Tone	Play DTMF tone on the device when user pressed a phone digitsduring
	taking, default enabled
Ring Back Tone	When the user is on a call, use a custom-set ring back tone
Busy Tone	When the user hangs up at the end of the call, use the custom-set wake
	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	<b>3</b>
Busy Response Code	Set the SIP response code on line busy
Reject Response Code	Set the SIP response code on call rejection

# 9.18 Settings >> Noise Reducation

Different levels of noise reduction technology can be configured, supporting intelligent noise reduction. When activated, it can effectively reduce noise, making calls clearer.



	Features Media Settings	Camera Settings MCAST	Action	Time/Date	Time P
> System					
› Network	Codecs Settings >> 🕜				
	Noise Reduction >>				
> Line	Noise Reduction Mode:	Default	~		
Device Settings	Media Settings >>				
	RTP Control Protocol(RTCP) Setting	s >>			
> Call List	RTP Settings >>				
> Function Key	Alert Info Ring Settings >>	Apply			
> Security					
> Device Log					
> Security Settings					

# 9.19 Settings >> Media Settings

Codecs Settings >> 🔞					Description:
Noise Reduction >>					Media settings, you can set the voice
Media Settings >>					coding,volume,ringtone and so on.
Default Ring Type:	1.wav	✓ Ø			
Speakerphone Volume:	1	(1~9) 🕜	Speakerphone Ring Volume:	1 (0~9) 🕜	
Speakerphone SignalTone Volume:	1	(1~9)			
MCAST Handfree Volume:	1	(1~9)			
DTMF Payload Type:	101	(96~127) 🥝			
Handfree Mic Gain:	3	(1~9)			
OPUS Payload Type:	107	(96~127)	OPUS Sample Rate	OPUS-NB(€ ✓	
ILBC Payload Type:	97	(96~127) 🕜	ILBC Payload Length	20ms 🗸 🕜	
Enable VAD:					
Disable AEC:					
Enable Line-in:	Disable	~			
Rtp Detection Timeout:	0	(0~3600s)			
Speaker Power		AI	F 🗸 🚺		
Audio Delay:		0	(0~1000ms)		

Picture 28- Media Settings

Table	17-	Media	Settings
-------	-----	-------	----------

Parameters	Description
Codecs Settings	Select the enabled and disabled voice codecs
	codec:G.711A/U,G.722,G.723,G.729AB,G.726-32,
	ILBC, Opus
Noise Reduction	Select the noise reduction level, configure it as intelligent
	noise reduction, it can effectively isolate noise.
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 1~9
Speakerphone Ring Volume	Set the ring volume in the speakerphone, the value must
	be 0~9
Speakerphone SignalTone	Set the SignalTone Volume in the speakerphone, the
Volume	value must be 1~9
DTMF Payload Type	Enter the DTMF payload type, the value must be 96~127.
Handfree Mic Gain	Set Handfree Mic Gain, the value must be 1~9
Opus playload type	Enter the opus payload type, the value must be 96~127.
	Set the opus sample rate $\cdot$ including OPUS-NB ( 8KHz),
OPUS Sample Rate	OPUS-WB(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 suppress the audio transmission with artificial
	comfort noise signal to save the bandwidth.
Audio Delay	When multicast is enabled, set the delay time for audio
	playback to facilitate audio playback by multiple devices.
Speaker Power	
RTP Control Protocol(RTC	P) 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	Set the value of the specified ring type
message 1 to 10	
ring type	The ring type

## 9.20 Settings>>Camera Settings

Customers can use it to configure camera-related parameters and adjust video encoding related settings.



connection mode setting			
Camera Status:			
Connect Mode:	External 🗸		
	Ap	pply	
P Camera Add			
Name:		0	
Username:		0	
Password:		0	
Ip Camera Brand:	TOPSEE 🗸		
IP:			
Port:	554		
UserAgent:			
URL1:			
URL2:			
		Add	
P Camera Option			
~	Dele	Modify	
P Camera List			

## Picture 29- Camera Settings

## Table 18- Camera Settings

Parameters	Description				
Connection mode setting					
Camera Status					
Connect Mode	Set the connection mode of the camera, only external cameras are				
Connect Mode	supported				
IP Camera Add					
Name	Set the camera name				
Username	The username that is authenticated when accessing the URL				
Password	The password that is authenticated when accessing the URL				
Ip Camera Brand	Set the camera brand				
IP	Set the IP address of the camera				
Port	Set the port for the camera				
User Agent	The user agent parameter that is carried when accessing the URL				
IP Camera List					
Video Direction	Set the video direction to Send Only, Receive Only, or Send and Receive				
H.264 Payload	Set the H 264 lead turne				
Туре	Set the H.264 load type				



#### 9.21 Settings >> 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>

### 9.22 Settings >> Action

Table 19- Action URL

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

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

	Features Media Settings Local IP Camera MCAST Action Time/Date	Time Plan Tone Led
› System		NOTE
	Action URL Event Settings	
> Network	Setup Completed:	Description: Action URL settings
	Registration Succeeded:	Action ORE settings
> Line	Registration Disabled:	
	Registration Failed:	
Settings	Incoming Calls:	
	Outgoing Calls:	
> Call List	Call Established:	
	Call Terminated:	
> Function Key	Phone Silent:	
	Phone Unsilent:	
> Security	Call Mute:	
	Call Unmute:	
> Device Log	IP Changed:	
	Device State Idle:	
> Security Settings	Device State Talking:	
/ Security Settings	Device State Ringing:	
	Start Reboot:	
	Web API Auth Changed:	
	Echo Test:	
	Input1:	
	Output1:	
	Reset Output1:	
	Dsskey:	

Picture 30- Action URL

## 9.23 Settings >> Time/Date

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



	Features Media Settings	Camera Settings MCAST		/Date Time Plan	Tone
System					NOTE
	Network Time Server Settings				
Network	Time Synchronized via SNTP			0	Description: Time and date settings,
100	Time Synchronized via DHCP			0	you can set the time through the network time
Line	Time Synchronized via DHCPv6			0	server, or manually set the time, select the time
	Primary Time Server	0.pool.ntp.org		0	the time, select the time zone and date format.
> Intercom settings	Secondary Time Server	time.nist.gov		0	
	Time zone	(UTC+8) Beijing,Singapore,Perth,Irkuts	•	0	
> Call List	Resync Period	60 second(s)		0	
Function Key	Time/Date Format				
runcuon key	12-hour clock				
Security	Time/Date Format	DD MMM WW TO OCT SA	π		
CT0000000					
Device Log					
	Daylight Saving Time Settings				
Security Settings	Location	None 🔻			
	DST Set Type	Disabled V			
		Apply			
	Manual Time Settings				
	2020-10-10 18	▼ 16 ▼	Apply		

Picture 31 - Time/Date

Table 20- Time/Date

Time/Date				
Field Name	Explanat	ion		
Network Time Ser	ver Setti	ngs		
Time Synchronized vi	a SNTP	Enable time-sync through SNTP protocol		
Time Synchronized vi	a DHCP	Enable time-sync through DHCP protocol		
Primary Time Server		Set primary time server address		
		Set secondary time server address, when primary server is not		
Secondary Time Serv	er	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 Setti	ngs		
Location		Select the user's time zone specific area		
DST Set Type		Select automatic DST according to the preset rules of DST, or the		
DST Set Type		manually input rules		
Offset		The DST offset time		
Month Start		The DST start month		
Week Start		The DST start week		
Weekday Start		The DST start weekday		
Hour Start		The DST start hour		
Month End		The DST end month		



Week End	The DST end week			
Weekday End	The DST end weekday			
Hour End	The DST end hour			
Manual Time Settings				
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)				

# 9.24 Settings>>Time plan

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

	Features	Media Settings	Local IP Camera	MCAST	Action	Time/Date	Time Plan	Tone	Led	
› System								NOTE		Î
> Network	Time Plan Sett							Description: Time plan setti	ng can be	_
> Line	Enable Tim	e Plan List: 🛛 🛛		Apply	Time Plan Pause:			used to set tim time period. Tir to execute an a	e point and ne point is action at a	_
> Settings	Time Plan: Name:							certain time, an period is to exe action at a cert	cute an	_
Call List	Type:		Timed reboot	~						_
> Function Key	Repetition	period:	No repetition	~						- 1
> Security > Device Log	Monthly:		2 3 4 5 6 7							
› Security Settings	Effective tir	ne:	□ 8 □ 9 ↓ 10 ↓ 10		. 0 •					
	Time Plan List:		Add	J						
	Index	Name	Туре	Special co	nfigure Repe	tition period	Effective time			
	Time Plan Paus	se:								-
			Fanvil Techn	Version: T2.1 ology Co., Ltd. (C)20	2.9 23 All Rights Reserve	d.			1	

Picture 32- Time Plan

Table 21- Time Plan

Parameters	Description			
Time Plan Settings				
Enable Time Plan List	Turn on the time management list, and then perform the set action at the			
	set time period			
Enable Time Plan	Turn on the pause list, and the device will not perform the set action until			
Pause	the time of setting pause			
Time Plan				



Name	Enter a custom name
Туре	Timed reboot, Timed upgrade, Timed echo test, Timed play audio ,Timed
	config
Audio Path	Support on-premises
	Local: Select the locally uploaded audio file
Play mode	When the type is selected as Play Audio, it supports setting to loop
	playback or play it once
Play Type	Local: The device plays audio
	Multicast: The device sends audio over multicast
	Local & Multicast: While the device plays locally, it also sends audio
	through multicast
Multicast address	Sets the multicast address when playing audio
Code	The encoding used when multicast audio
Repetition period	No repetition: Execute once within the set time range
	Daily: Perform this operation in the same time range every day
	Weekly: Do this within the time range of the day of the week
	Monthly: Perform this operation within the time range of the day of each
	month
Effective time	Set the execution period
Time Plan List	
Time Plan Pause	
Name	Pause list name
Start time	Set start time
Stop time	Set stop time
Time Plan Pause List	

# 9.25 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
/stem						NOTE
	Tone Settings					
twork	Select Your Tone:	United States			<b>v</b> 🔞	Tone: cadence[,cadence]
	Dial Tone:	350+440/0			0	[,cadence]Where
le	Ring Back Tone:	440+480/2000,0/4000			0	cadence = Freq1[+Frec [+Freq3]
	Busy Tone:	480+620/500,0/500			0	[+Freq4]/Duration.Freq The frequency of the
ntercom settings	Congestion Tone:				0	tone:200~4000HZ, If i set to 0Hz, it means the
	Call waiting Tone:	440/300,0/10000,440/300,0/1000	0,0/0		0	tone won't be played.A
List	Holding Tone:				0	tone is comprised of at most four different
	Error Tone:				0	frequencies.Freq1+Freq The juxtaposition of two
nction Key	Stutter Tone:				0	frequencies Freq1 and
	Information Tone:				0	Freq2 without modulation.Freq1*Freq
curity	Dial Recall Tone:	350+440/100.0/100,350+440/100	,0/100,350+440/100,0/100,35	0+440/0	0	Freq1 is modulated by Freq2.Duration The time
1968). 197	Message Tone:				0	duration of the tone:0~30000ms.If it is
vice Log	Howler Tone:				0	set to 0ms, it means th
	Number Unobtainable Tone:	400/500,0/6000			0	tone will keep on playin until stopped by system
curity Settings	Warning Tone:	1400/500,0/0			0	it is set to 0/0, it means the tone is stopped. The
curity Settings	Auto Answer Tone:				0	composition of Tone: Yo
		Apply				can configure at most eight different cadences
						for one tone, and separate tones by
						commas.

Picture 33- Tone

### 9.26 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.

#### 9.27 Call list >> Web Dial

Use web page to call, answer and hang up.

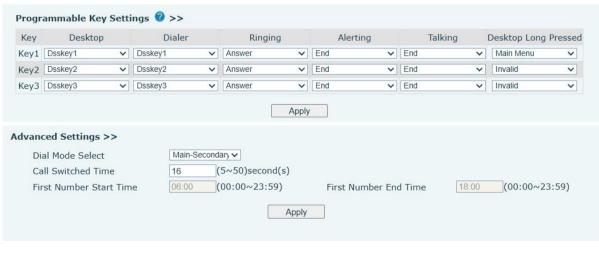


	Call List Web Dial
> System	
> Network	Web Dial Settings
› Line	Dial Answer Hang-up
› Intercom settings	
> Call List	
› Function Key	
> Security	
> Device Log	
> Security Settings	

Picture 34- Webpage Dial

# 9.28 Function Key

Key	Туре	Name	Value			Subtype	Line	Media
DSS Key 1	None 🗸			+		None 🗸	AUTO 🗸	DEFAULT 🗸
DSS Key 2	Key Event 🗸			+	-	Handfree 🗸	AUTO 🗸	DEFAULT 🗸
DSS Key 3	None 🗸			+	-	None 🗸	AUTO 🗸	DEFAULT 🗸



Picture 35- Function Key





Function key set	tings					
memory	Speed Dial: The user can directly dial the set number. This feature is					
	convenient for customers to dial frequent numbers.					
	Intercom: This feature allows the operator or secretary to quickly connect					
	to the phone, widely used in office environments					
Key event	The user can select a function key as a shortcut to trigger an event for					
	example: None /Handfree					
DTMF	Press during a call to send the set DTMF					
Mcast Paging	Configure the multicast address and voice encoding. User can initiate					
	multicast by pressing this key					
Action URL	The user can use a specific URL to make basic calls to the device, open					
	the door, etc.					
Mcast Listening	In standby, press the function key, if the RTP of the multicast is detected,					
	the device will monitor the multicast					
PTT	Speed dial: Make a call when pressed, and end the call when lifted.					
	Intercom: Start the intercom when pressed, and end the intercom when					
	lifted.					
	Multicast: Initiate multicast when pressed, and end multicast when lifted					
Programmable K	ey Settings					
Desktop	None: Nothing happens when you press the Call button					
	Dsskey1: When it is set to dsskey1, follow the settings of dsskey1 to make					
	call, answer, etc.					
	Dsskey2: When it is set to dsskey2, perform operations such as calling					
	and answering according to the setting of dsskey2					
	Dsskey3: When it is set to dsskey3, perform operations such as calling					
	and answering according to the setting of dsskey3					
Dialer	None: Nothing happens when you press the Call button					
	Dsskey1: When it is set to dsskey1, follow the settings of dsskey1 to make					
	call, answer, etc.					
	Dsskey2: When it is set to dsskey2, perform operations such as calling					
	and answering according to the setting of dsskey2					
	Dsskey3: When it is set to dsskey3, perform operations such as calling					
	and answering according to the setting of dsskey3					
Ringing	Answer: Set to answer, when there is an incoming call, if auto answer is					
	disabled, press the Call button to answer the call					
	End: set to end, when there is an incoming call, press the Call button to					
	hang up the call					
Talking	End: set to end, when there is a call, press the Call button to hang up the					



	call
	Volume up: set as volume up button, when there is a call, press the Call
	button to increase the volume
	Volume down: set as volume up button, when there is a call, press the Call
	button to decrease the volume
	Dsskey1: When it is set to dsskey1, follow the settings of dsskey1 to make
	call, answer, etc.
	Dsskey2: When it is set to dsskey2, perform operations such as calling
	and answering according to the setting of dsskey2
	Dsskey3: When it is set to dsskey3, perform operations such as calling
	and answering according to the setting of dsskey3
Desktop Long	None: Long press the Call button does not respond
Pressed	Main menu: Long press the Call button to enter the command line mode,
	see 5.2.1 Common Command Mode for details
Advanced Settings	5
	Number 1 call number 2 mode selection.
	<main secondary="">: If the first number is not answered within the set time,</main>
Hot Key Dial Mode	the second number will be automatically switched.
Select	<day night=""> : The system time is automatically detected during the call. If</day>
	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
	The start time of the day when the <day night=""> mode is defined. Default</day>
Day Start Time	"06:00"
Day End Time	The end time of the day when the <day night=""> mode is defined. Default</day>
Day End Time	"18:00

## > Memory

Enter the phone number in the input box. When you press the function key, the device will call out the set phone number. This button can also be used to set the IP address, press the function key to make an IP direct call.



Key	Туре	Name	Value			Subtype		Line		Media	
DSS Key Left	None 🗸			+	-	None	~	SIP1	×	DEFAULT	v
DSS Key Middle	Memory Key 🗸			+	-	Speed Dial	~	SIP1	~	DEFAULT	~
DSS Key Right	None 🗸			+	-	None	~	AUTO	×	DEFAULT	Y
Short circuit input	None 🗸			+	-	None	~	AUTO	~	DEFAULT	~
				Apply							
Programi	mable Key Setting	s 🕜 >>									

Picture 36 - Memory Key

Table 23- Memory Key

Туре	number	line	Subtype	usage
	Fill in the		Speed	Using the speed dial mode, press the button
	SIP	The line	Dial	to quickly dial the set number.
	account or	correspon		
memory IP addre	IP	ding to the		Using the intercom mode, when the SIP
	address of	SIP	Intercom	phone at the opposite end supports the
	the called	account		intercom function, the call can be
	party			automatically answered.

# > 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:

Key	Туре	Name	Value			Subtyp	е	Line	Media	
DSS Key Left	None 🗸			+	(	None	~	SIP1 V	DEFAULT	~
DSS Key Middle	MCAST Paging			+	1.7	G.711U	~	SIP1 V	Remote Only	~
DSS Key Right	None 🗸			+	-	None	~	AUTO 🗸	DEFAULT	~
Short circuit input	None			+	-	None	~	AUTO 🗸	DEFAULT	~
				Apply						
Programi	nable Key Settings	?>>								



#### Picture 37- Multicast

#### Table 24- Web Multicast

Туре	Number	Subtype
		G.711A
	Set the host IP address and port number, they must	G.711U
N 4. 14: 4	be separated by a colon (The IP address range is	G.729AB
Multicast	224.0.0.0 to 239.255.255.255, and the port number	iLBC
	is preferably set between 1024 and 65535)	opus
		G.722

#### > PTT

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

Key	Туре	Name	Value			Subtype		Line	Media	
DSS Key Left	None 🗸			+	-	None	~	SIP1 🗸	DEFAULT	~
DSS Key Middle	PTT V			+	-	Speed Dial	~	SIP1 🗸	DEFAULT	~
DSS Key Right	None 🗸			+	-	None	~	AUTO 🗸	DEFAULT	~
Short circuit input	None			+	-	None	~	AUTO 🗸	DEFAULT	~
				Apply						
	mable Key Settings	0								

#### Picture 38 - Advanced Setting

## 9.29 Security >> Web Filter

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



	Web Filter Trust Certi	ficates Device Certificates Firewall	
System			
Network	Web Filter Table 🔮		
- 11 Mar	Start IP Address	End IP Address	Option
Line	Web Filter Table Settings		
Intercom settings	Start IP Address	End IP Address	Add
Call List	Web Filter Setting 🔗		
Function Key	Enable Web Filter 🗐	Apply	
> Security			
Device Log			
Security Settings			
Web Filter Table 🕖			
Start IP Address		End IP Address	Option
172.16.80.6		172.16.80.69	Modify
			Delete

Picture 39- 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.

#### 9.30 Security >> Trust Certificates

You can upload and delete uploaded trust certificates.



	0
Network     Permission Certificate     Disabled     T     Common Name Validation     Disabled     T	0
Line     Common Name Validation     Disabled	0
Intercom settings     Certificate mode     All Certificates	0
Apply	
> Call List Import Certificates 😵	
Function Key Load Server File	Select Upload
> Security Certificates List 🖓	
Device Log	Issued By Expiration File Size Delete
> Security Settings	

Picture 40 - Trust Certificates

# 9.31 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 Certificates	Device Certificates	Firewall		
> System						
> Network	Device Certifica	tes 🕜				
> Line	Device Certi	ficates	Default Certificates Apply	▼ (exister	ice)	
> Intercom settings	Import Certifica	ites 🕜				
› Call List	Load Server	File		Select	Upload	
> Function Key	Certification File	e 🕖				
	File	e Name	Issued To	Issued	I By Expiration	File Size
> Security						Delete
> Device Log						
Security Settings						

Picture 41- Device Certificates



### 9.32 Security >> Firewall

	Web Filter         Trust Certificates         Firewall
› System	
› Network	Firewall Type 🔮 Enable Input Rules: 💿 Enable Output Rules: 💿
› Line	Apply
› Intercom settings	Firewall Input Rule Table 🥑 Index Deny/Permit Protocol Src Address Src Mask Src Port Range Dst Address Dst Mask Dst Port Range
› Call List	
› Function Key	Firewall Output Rule Table 🔮 Index Deny/Permit Protocol Src Address Src Mask Src Port Range Dst Address Dst Mask Dst Port Range
> Security	Firewall Settings
> Device Log	Input/Output Input  Src Address Deny/Permit Deny  Src Mask Add
Security Settings	Protocol UDP  Src Port Range Dst Port Range
	Rule Delete Option ?       Input/Output     Input ▼       Index To Be Deleted     Delete

#### Picture 42 - 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:

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。
Port range	Port range
Src Address	The source address can be the host address, network address, or

#### Table 25- Web Firewall



	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.
Src Port Range	It is the source address mask. When it is configured as
	255.255.255.255, it means it is a specific host. When it is set as a
	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
	255.255.255.255, it means it is a specific host. When it is set as a
Dst Port Range	subnet mask of 255.255.255.0 type, it means that a network
	segment is filtered;

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

	irewall Input Rule Table 🕜				
Src Port Range D	Ost Address	Dst Mask	Dst Port Range		
	Src Port Range [	Src Port Range Dst Address	Src Port Range Dst Address Dst Mask		

#### Picture 43- 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.

Input 🔻	Index To Be Deleted	Delete
	Input 💌	

Picture 44- Delete firewall rules

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

### 9.33 Device 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.



## 9.34 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.

Basic Settings Ringtone Duration: Input & Tamper Server Ad Message:		] 🕖	er;Mac=\$mac;IP=\$ip;port=\$trigg
message.	Alarm_inio.Description-3	Apply	er,wac-smac,iP-sip,port-singge
Input Settings >>			
Output Settings >>			
Triggered By DTMF RingTo	one:	None 🗸	
Triggered By URI Rington	e:	None 🗸	
Triggered By SMS Ringtor	ie:	None 🗸	
Triggered By Dsskey Ring	tone:	None 🗸	
Output1:			
Standard Status:	NC:closed V	Output Duration:	5 (0~600)s
Output Trigger Mode:	Trigger By DTMF	DTMF Trigger Code:	1234
		DTMF Reset Code:	4321
		Reset By:	By Duration 🗸
	Trigger By Active URI	Trigger Message:	OUT1_SOS
		Reset Message:	OUT1_CLR
	Trigger By SMS	Trigger Message:	ALERT=OUT1_SOS
		Reset Message:	ALERT=OUT1_CLR
	Trigger By Input:	Input1	

Picture 45 - Security Settings

#### Table 26- Security Settings

Security Settings		
Parameters	Description	
Basic Settings		
Ringtone Duration	Set the ringtone duration, default value is 5 seconds.	
	Set remote server address. The device will send message to the	
Input & Tamper	server when the alarm is triggered. The message format is :	
Server Address	Alarm_Info: Description=A212;SIP User=;Mac=0c:38:3e:3a:06:65;IP=;	
	port=Input .	
Input settings		
Input Detect	Enable or disable Input Detect	
	When choosing the low level trigger (closed trigger), detect the input	
Triana and have	port (low level) closed trigger.	
Triggered by	When choosing the high level trigger (disconnect trigger), detect the	
	input port (high level) disconnected trigger.	



Input Duration	Set input duration		
	Send SMS: Set the alert message send to server if selected.		
Triggered Action	Dss Key: The device will perform corresponding Dss Key		
	configurations if any key is selected, by default the value is none.		
	Triggered Ringtone: Select triggered ring tone.		
Output Settings			
Output Response	Enable or disable Output Response		
Triggered by DTMF Ring tone	Select the DTMF trigger ring tone.		
Triggered by URI Ringtone	Select the URI trigger ring tone.		
Triggered By SMS Ringtone	Select the SMS trigger ring tone.		
Triggered By Dsskey Ringtone	Select the Dsskey trigger ring tone.		
	When choosing the low level trigger (NO: normally open), when meet		
Standard Status	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 change duration time, the default is 5 seconds.		
	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 DTMF reset code, default value is 4321.		
	Reset the output port mode by duration or state.		
Reset By	By duration: Reset the output port status when output duration occurs.		
,,	By state: Reset the output port status when device's call state		
	changes.		
	Enable or disable trigger by URI.		
Trigger by URI	User can send commands from remote device or server to A212 series		
	device, if the command is correct, then device will trigger		
	corresponding output port.		
Trigger Message	Input trigger message for trigger by URI mode.		
Rest Message	Input reset message for trigger by URI mode.		
	Enable or disable trigger by SMS.		
Trigger by SMS	User can send ALERT command to A212 series device, if the		
	command is correct, then device will trigger corresponding output port.		



Trigger SMS	Input trigger message for trigger by SMS mode.	
Reset SMS	Input reset message for trigger by SMS mode.	
	Select the input port, when the input port meets the trigger condition,	
Trigger by Input	the output port will be triggered (The Port level time change, By <	
	Output Duration > control)	
	Select call state to trigger the output port, options are:	
	Talking: When the device's talking status changes, trigger the output	
	port.	
Trigger By Call 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.	
	Enable or disable trigger by DssKey. If any of the DssKey is selected,	
Trigger By DssKey	when the DssKey application performs, the output port will be	
	triggered.	



# **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**

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

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

#### **10.3 Device Factory Reset**

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

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

#### **10.4 Network Packets Capture**

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
	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" (Solid orange), 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 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.

#### Table 25 - Trouble Cases