

SIP Audio Door Phone i23S

USER MANUAL

V1.0





Document	Firmware	Explanation	Time
VER	VER		
V1.0	2.1.1.3445	Initial issue	20180208





Safety Notices

- 1. Please use the specified power adapter. If you need to use the power adapter provided by other manufacturers under special circumstances, please make sure that the voltage and current provided is in accordance with the requirements of this product, meanwhile, please use the safety certificated products, otherwise may cause fire or get an electric shock.
- 2. When using this product, please do not damage the power cord either by forcefully twist it, stretch pull, banding or put it under heavy pressure or between items, otherwise it may cause damage to the power cord, lead to fire or get an electric shock.
- 3. Before using, please confirm that the temperature and environment is humidity suitable for the product to work. (Move the product from air conditioning room to natural temperature, which may cause this product surface or internal components produce condense water vapor, please open power use it after waiting for this product is natural drying).
- 4. Please do not let non-technical staff to remove or repair. Improper repair may cause electric shock, fire, malfunction, etc. It will lead to injury accident or cause damage to your product.
- 5. Do not use fingers, pins, wire, other metal objects or foreign body into the vents and gaps. It may cause current through the metal or foreign body, which may even cause electric shock or injury accident. If any foreign body or objection falls into the product please stop using.
- 6. Please do not discard the packing bags or store in places where children could reach, if children trap his head with it, may cause nose and mouth blocked, and even lead to suffocation.
- 7. Please use this product with normal usage and operating, in bad posture for a long time to use this product may affect your health.
- 8. Please read the above safety notices before installing or using this phone. They are crucial for the safe and reliable operation of the device.





Directory

Α	Pr	oduct introduction	6
	1.	Appearance of the product	6
	2.	Description	6
В	St	art Using	7
	1.	Confirm the connection	7
	1	1)Power, Electric Lock, Indoor switch port	7
	2	2)Driving mode of electric-lock(Default in Passive mode)	7
	3	3)Wiring instructions	
	2.	Quick Setting	9
С	Ba	asic operation	9
	1.	Answer a call	9
	2.	Call	9
	3.	End call	10
	4.	Open the door operation	10
Е	Pa	nge settings	11
	1.	Browser configuration	
	2.	Password Configuration	
	3.	Configuration via WEB	12
	((1)System	12
		a)Information	12
		b)Account	
		c)Configurations	13
		d)Upgrade	
		e)Auto Provision	
		f)FDMS	
		g)Tools	
	((2)Network	
		a)Basic	
		b)Advanced	
		c)VPN	
	((3)Line	
		a)SIP	
		b)Basic Settings	
	1	c)Dial Peer	
	(a)Features	
		b)Audio	
		o ji tudio	



		c)Video	
		d)MCAST	
		e)Action URL	40
		f)Time/Date	
	(5)EGS Access	
	(6)EGS Logs	45
	(7)Door Lock	45
	(8)Function Key	
	(9)Alert	47
Е	Ар	opendix	48
	1.	Technical parameters	
	2.	Basic functions	
	3.	Schematic diagram	
F	Ot	her instructions	50
	1.	Open door modes	
	2.	Management of card	50





A.Product introduction

i23S SIP door phone is a full digital network door phone, with its core part adopts mature VoIP solution (Broadcom chip), stable and reliable performance, hands-free adopting digital full-duplex mode, voice loud and clear, generous appearance, solid durable, easy for installation, comfortable keypad and low power consumption.

i23S SIP door phone supports entrance guard control, voice intercom, RFID/IC card and keypad remote to open the door.

1. Appearance of the product





2. Description

Buttons and icons	Description	Function
	Numeric keyboard	Input password to open the door or to call.
	Programmable key	Can be set to a variety of functions, in order to meet the needs of different occasions
CARD ODD	Card reader area	Use RFID/IC Cards to open the door
Π	Lock Status	Door unlocking: On
		Door locking: Off
		Standby: Off
	Call status	Call Holding: Blink with 1s
		Calls: On
Δ	Ping status	Standby: Off
44 	Ring status	Ringing: On

 -

	Network error: Blink with 1s
 Network/SIP	Network running: Off
 Registration	Registration failed: Blink with 3s
	Registration succeeded: On

B.Start Using

Before you start to use the equipment, please make the following installation.

1. Confirm the connection

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

1) Power, Electric Lock, Indoor switch port

There are 2 power supply options: 12V/DC or POE (Powered By Ethernet). PIN 1 (+12V) and PIN 2 (VSS) connected to the power supply. PIN3/4/5 used to connect the electric lock, only 2 of them (NC and COM, or NO and COM) will be connected usually, depending on the type of electric lock. PIN6/7 used to connect indoor switch which control the open/lock of electric lock.

			CN7				
1	2	3	4	5	6	7	
+12V	VSS	NC	СОМ	NO	S_IN	S_OUT	
12V 1	A/DC	Elec	tric-lock s	witch	Indoor	switch	



2) Driving mode of electric-lock(Default in Passive mode)



Pa	1
assive	(2/)
	/3/
Mode	4

Jumper in passive mode



Jumper in active mode

Driving mode of electric-lock decides whether the electric-lock use an independent power supply. The independent power supply will be required in passive mode, while electric-lock will be powered by i31S in active mode.

[Note] When the device is in active mode, it can drive 12V/650mA switch output maximum, to which a standard electric-lock or another compatible electrical appliance can be connected.

- When using the active mode, it is 12V DC in output.
- When using the passive mode, output is short control (normally open mode or normally close mode).



3) Wiring instructions

I23S use a relay to control the state of electric-lock, before that, the electric-lock must be powered correctly. There are 3 contacts of the relay:

- NO: Normally Open Contact.
- COM: Common Contact.
- NC: Normally Close Contact.

Drivin	g Mode	Electr	ric lock		
Activ e	Passiv e	No electricity when open	When the power to open	Jumper port	Connections
\checkmark		\checkmark		Active Mode	12V OO O O OO + - NC COM NO S-I S-O +
\checkmark				Active Mode	12V OO O O O OO + - NC COM NO S-I S-O
				Passive Mode	Door Phone Power Input Power Supply 12V/2A + - NC COM NO S-I S-O Indoor switch Electric-lock: No electricity when open the door
	\checkmark			Passive Mode	Door Phone Power Input Power Supply 12V/2A + - NC COM NO S-I S-O + - NC COM NO S-I S-O Indoor switch Electric-lock: When the power to open the door
	\checkmark	\checkmark		Passive Mode	Door Phone Power Input COUND PUSH (SWB - 12) DOOR Phone Power Input DOOR Phone Power Input DOOR OP JOINT Power Input Power In



2. Quick Setting

The product provides a completed function and parameter settings. To understand all meaning of parameters well, it is better for users to have knowledge of network and SIP protocol. In order to make users enjoy the high-quality voice service and low-cost advantage immediately, here we list some basic but compulsory setting options in this section. Users can use it without understanding such complex SIP protocols.

In prior to this step, please make sure your broadband Internet online can be normally operated and complete the connection of the network hardware. The product factory network mode is DHCP. Thus, only the equipment is connected with DHCP network environment that network can be automatically connected.

- Press and hold "#" key for 3 seconds and the door phone will report the IP address by voice. Or use the "iDoorPhoneNetworkScanner.exe" software to find the IP address of the device. (Download address <u>http://download.fanvil.com/tool/iDoorPhoneNetworkScanner.exe</u>)
- > Note: Waiting for 30s to run the device when it is power on.
- > Log in to the WEB device configuration.
- In a Line page configuration service account, user name, parameters that are required for server address register.
- > You can set DSS key in the Function key page.
- > You can set Door Phone parameters in the Webpage (EGS Setting-> Features).

IP Address	Serial Number	MAC Address	SW Version	Description	
172. 18. 2. 185	i23S	Oc:38:3e:1e:61:dd	2.1.1.3445	i23S IP Door Phone	1

C.Basic operation

1. Answer a call

By default, the incoming call will be answered automatically without any ringing. User MAY want to hear ring before answer the incoming call. This could be configured under EGS setting -> Features -> Basic Settings -> Auto Answer timeout. This parameter is the ringing time. Auto answered could be disabled under EGS setting -> Features -> Basic settings -> Enable auto Answer.

2. Call

There are 2 options to place a call:

1) Press * to enter dialing mode, then type in the number and press * to send the call



immediately.

Here the feature of "pressing * to send the call" could be disabled by the option "press * to send" under EGS setting -> Features -> Basic Settings

Another 2 important options are "dial Fixed Length to Send" and "send Length". When user is typing in the number under dialing mode on keypad, device will check the length of number after every new digit was typed. Once the length matches the parameter "send Length", the number will be called immediately. If this feature is disabled, user will need to wait "auto dial out time" seconds before the call is sending out.

2) By pressing the DSS key, the preconfigured number will be called. The option is under Function Key -> Function Key settings. The type is hot key, subtype is Speed dial. There are 2 numbers available here, the number 1 will be called first, if number 1 is not answered, the call will be transferred to number2.

3. End call

The key "#" is used to end the active call. There are another 2 important features:

- 1) Release the processing call
- 2) Reject the incoming call when it's ringing

4. Open the door operation

There are seven options to open the door:

1)In idle state, Input "local password" on the keyboard to open the door, it could be configured under EGS Setting -> Feature -> Local Password.

2) Open with remote password. Make a call to the owner, the owner enters the remote password to open the door. "remote password" could be configured under EGS setting -> Feature -> Remote Password.

3) Open with Access code. The owner makes a call to the access control, the access control will answer the call automatically. Then owner enter the "access code" on his keypad to open the door. The owner's number and access code are configured under EGS Access -> Access Table & Add Access rule.

4) Swipe the RFID/IC cards to open the door. Before user can use the card, it must be added under EGS Access -> Access Table.

5) By pressing the indoor switch to open the door. The indoor switch must be connected correctly according to the section 1.

6) Private access code to open the door.

The private access code could be configured under EGS Access -> Access Table & Add Access Rule. To open door with private access code, user enter "location code" + "*" + "Access Code". For example, the location code is 1, and Access code is 123, User enter "1*123#" to open the door.

NOTE: ended with "#" to send the code immediately.

7) Active URL control command to open the door.



URL is

"http://user:pwd@host/cgi-bin/ConfigManApp.com?key=F_LOCK&code=openCode"

a. User and pwd is Web the user name and password.

b. "openCode" is the remote-control code to open the door.

Example: "http://admin:admin@172.18.3.25/cgi-bin/ConfigManApp.com?key=*"

If access code is input correctly, the device will play sirens sound to prompt access control and the remote user, while user input the incorrect code, the device will play low-frequency short chirp.

If password is input successfully, then high-frequency sirens sound will follow by. If password is input incorrectly, high-frequency short chirp will follow by.

When door is open , the device will play sirens sound to prompt.

D.Page settings

1. Browser 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.

Enter the user name and password and click the [logon] button to enter the settings screen.

User:		
Password:		
Language:	English	~
	Logon	

2. Password Configuration

There are two levels of access: root level and general level. A user with root level access can browse and set all configuration parameters, while a user with general level can set all configuration parameters except server parameters for SIP.

- Default user with general level: The default is not set, are free to add.
- Default user with root level:
 - User name: admin
 - Password: admin



3. Configuration via WEB

(1) System

a) Information

	Information	Account Co	nfigurations	Upgrade	Auto Provision	FDMS	Tools
> System							
Network	System Information						
NELWOIK	Model:		i235				
	Hardware:		2.1				
Line	Software:		2.1.1.3445				
	Uptime:		00:24:29				
EGS Setting	Last uptime:		00:15:05				
	MEMInfo:		ROM: 0.8/8(M)	RAM: 2.2/	16(M)		
EGS Access	System Time:		2018-04-10 18	03			
EGS Logs	Network						
	Network mode:		DHCP				
Door Lock	MAC:		Oc:38:3e:1e:61	:dd			
	IP:		172.18.2.185				
Function Key	Subnet mask:		255.255.0.0				
Tunction key	Default gateway:		172.18.1.1				
Alert	SIP Accounts						
	Line 1	5528	Registe	red			
	Line 2	N/A	Inactiv	e			

Information					
Field Name	Explanation				
System	Display equipment model, hardware version, software version, uptime, Last				
Information	uptime and MEMinfo.				
Network	Shows the configuration information for WAN port, including connection mode of				
Network	WAN port (Static, DHCP, PPPoE), MAC address, IP address of WAN port.				
SIP Accounts	Shows the phone numbers and registration status for the 2 SIP LINES.				

b) Account

www.fanvil.com



Through this page, user can add or remove users depends on their needs and can modify existing user permission.

	Information Account	Configurations Upgrade	Auto Provision	FDMS	Tools	
> System						
> Network	Change Web Authentication Pas	sword				
› Line	New Password: Confirm Password:					
EGS Setting	Add New User	Apply				
EGS Access	Username Web Authentication Password					
EGS Logs	Confirm Password Privilege	Administrators V				
Door Lock		Add				
Function Key	User Accounts	Privilege				
Alert	admin	Administrators		Delete		

Account				
Field Name	Explanation			
Change Web Authentication Password				
You Can modif	You Can modify the login password to the account			
Add New User				
You can add new user				
User Accounts				
Show the existing user information				

c) Configurations



	Information Acco	unt Configurations Upgrade	Auto Provision	FDMS	Tools
System					
etwork	Export Configurations				
		Right click here to SAVE configur Right click here to SAVE configur			
	Import Configurations	Agric click here to over configu	duona in xim torindu		
5 Setting		Configuration file:	Select	Import	
GS Access	Reset to factory defaults	Click the [Reset] button to reset ALL USER'S DATA WILL BE LOST		ults.	
Logs		Reset	AFTER RESET!		
			AFTER RESET!		
S Logs or Lock nction Key			AFTER RESET		

Configurations	
Field Name	Explanation
Export	Save the equipment configuration to a txt or xml file. Please note to Right
Configurations	click on the choice and then choose "Save Link As."
Import	Prowee to the config file, and proce Lindote to load it to the equipment
Configurations	Browse to the config file, and press Update to load it to the equipment.
Reset to factory	This will restars factory default and remove all configuration information
defaults	This will restore factory default and remove all configuration information.

d) Upgrade

	Information	Account Configurations	Upgrade	Auto Provision	FDMS	Tools	
> System							
> Network	Software upgrade	Current Software Version:	2.1.1.3445	<u>.</u>			
› Line		System Image File		Select	Upgrade		
Upgrade							
Field Name	Explanation						
Software upgr	ade						
Browse to the f	irmware, and pre	ss Update to load i	t to the eq	uipment.			

e) Auto Provision



	Information	Account	Configurations	Upgrade	Auto Provision	FDMS	Tools	
> System								
> Network		nfiguration Version						
• Line	General Co CPE Serial	nfiguration Version Number	00100400FV0	2001000000c383e1e	:61dd			
> EGS Setting	Authenticat Authenticat	ion Name ion Password						
> EGS Access	Configurati	on File Encryption K nfiguration File Encr	State of the second sec					
	Key	Provision Informatio						
› EGS Logs	DHCP Option >							
> Door Lock	SIP Plug and P							
> Function Key	Static Provision	ning Server >>						
	TR069 >>							
> Alert			Apply					
DHCP Option >>								
Option Value		Option 66	~					
Custom Option	n Value	66	(128	8~254)				
CTD plug and play	(0-0) >>							
SIP Plug and Play Enable SIP Pn								
Server Addres		224.0.1.75						
Server Port		5060						
Transportation	n Protocol	UDP 🗸						
Update Interv	al	1	Ho	ur				
Static Provisionin	a Server >>							
Server Addres		0.0.0.0						
Configuration								
Protocol Type		FTP V						
Update Interv	al	1	Но	ur				
Update Mode		Disabled	~					
TR069 >>		_						
Enable TR069 Enable TR069	Warning Tono							
ACS Server Ty		Common 🔽	ก					
ACS Server UP		0.0.0.0						
ACS User		admin						
ACS Password								
TLS Version:		TLS 1.0 🗸						
INFORM Sendi	ng Period	3600	Seco	ond(s)				
STUN Server A	Addr	0.0.0						
STUN Enable								
		Apply						

Auto Provision		
Field Name	Explanation	



Common Settings	
Current Configuration Version	Show the current config file's version. If the version of configuration downloaded is higher than this, the configuration will be upgraded. If the endpoints confirm the configuration by the Digest method, the configuration will not be upgraded unless it differs from the current configuration
General Configuration Version	Show the common config file's version. If the configuration downloaded and this configuration is the same, the auto provision will stop. If the endpoints confirm the configuration by the Digest method, the configuration will not be upgraded unless it differs from the current configuration.
CPE Serial Number	Serial number of the equipment
Authentication Name	Username for configuration server. Used for FTP/HTTP/HTTPS. If this is blank the phone will use anonymous
Authentication Password	Password for configuration server. Used for FTP/HTTP/HTTPS.
Configuration File Encryption Key	Encryption key for the configuration file
General Configuration File Encryption Key	Encryption key for common configuration file
Save Auto Provision Information	Save the auto provision username and password in the phone until the server url changes
DHCP Option	
Option Value	The equipment supports configuration from Option 43, Option 66, or a Custom DHCP option. It may also be disabled.
Custom Option Value	Custom option number. Must be from 128 to 254.
SIP Plug and Play	(PnP)
Enable SIP PnP	If this is enabled, the equipment will send SIP SUBSCRIBE messages to a multicast address when it boots up. Any SIP server understanding that message will reply with a SIP NOTIFY message containing the Auto Provisioning Server URL where the phones can request their configuration.
Server Address	PnP Server Address
Server Port	PnP Server Port
Transportation Protocol	PnP Transfer protocol – UDP or TCP



Update Interval	Interval time for querying PnP server. Default is 1 hour.					
Static Provisioning	Server					
Server Address	Set FTP/TFTP/HTTP server IP address for auto update. The address can					
Server Address	be an IP address or Domain name with subdirectory.					
Configuration File	Specify configuration file name. The equipment will use its MAC ID as the					
Name	config file name if this is blank.					
Protocol Type	Specify the Protocol type FTP, TFTP or HTTP.					
Update Interval	Specify the update interval time. Default is 1 hour.					
	1. Disable – no update					
Update Mode	2. Update after reboot – update only after reboot.					
	3. Update at time interval – update at periodic update interval					
TR069						
Enable TR069	Enable/Disable TR069 configuration					
Enable TR069	Enable/Disable TR069 warning tone					
Warning Tone						
ACS Server Type	Select Common or CTC ACS Server Type.					
ACS Server URL	ACS Server URL.					
ACS User	User name for ACS.					
ACS Password	ACS Password.					
TLS Version	Select the TLS transport layer security protocol version, in accordance with					
	the service version					
INFORM Sending	Time between transmissions of "Inform" Unit is seconds.					
Period						
STUN Server Addr	Set STUN Server IP address					
STUN Enable	Enable/Disable STUN					

f) FDMS



	Information	Account Cor	nfigurations	Upgrade	Auto Provision	FDMS	Tools	
System								
etwork	FDMS Settings Enable FDMS							
ne	FDMS Interval		3600					
GS Setting	Doorphone Info Se		[
GS Access	Community Nar Building Numbe Room Number							
SS Logs			Apply					
oor Lock								
Inction Key								
lert								

FDMS Settings					
Enable FDMS	nable/Disable FDMS configuration				
FDMS Interval	The time to send sip Subscribe information to the FDMS server is on a				
FDIVIS Interval	regular basis. Unit is seconds				
Doorphone Info Se	ttings				
Community Name	The name of the community where the device is installed				
Building Number The name of the building where the equipment is installed					
Room Number	The name of the room where the equipment is installed				

g) Tools

	Information Account	Configurations Upgrade Auto Provision FDMS Tools
system	Syslog	
	Enable Syslog	
twork	Server Address	0.0.0.0
	Server Port	514
	APP Log Level	None
ie	SIP Log Level	None
		Apply
S Setting		
	Network Packets Capture	
S Access		Start
S Logs	Auto Reboot Setting	
lo Lugs	Reboot Mode	Disable V
or Lock	Fixed Time	2 (0~23)
	Uptime	72 (h)
nction Key		
пстюп кеу	Sip Reg Fail Reboot	
	Waiting Time	180 (s)
art	Network Fail Reboot	
	Waiting Time	300 (s)
	Handing Hille	
		Amply
		Apply



Reboot Phone

Click [Reboot] button to restart the phone!

Syslog provide a client/server mechanism for the log messages which is recorded by the system. The Syslog server receives the messages from clients and classifies them based on priority and type. Then these messages will be written into a log by rules which the administrator has configured.

There are 8 levels of debug information.

Level 0: emergency; System is unusable. This is the highest debug info level.

Level 1: alert; Action must be taken immediately.

Level 2: critical; System is probably working incorrectly.

Level 3: error; System may not work correctly.

Level 4: warning; System may work correctly but needs attention.

Level 5: notice; It is the normal but significant condition.

Level 6: Informational; It is the normal daily messages.

Level 7: debug; Debug messages normally used by system designer. This level can only be displayed via telnet.

Tools				
Field Name	Explanation			
Syslog				
Enable	Enable or disable system log			
Syslog	Enable or disable system log.			
Server	System log sonver IP address			
Address	System log server IP address.			
Server Port	System log server port.			
APP Log	Set the level of ADD leg			
Level	Set the level of APP log.			
SIP Log Level	Set the level of SIP log.			
Network Pack	ets Capture			
Capture a pack	set stream from the equipment. This is normally used to troubleshoot problems.			
Auto Reboot S	Setting			
Configure the restart mode and restart time of the device and restart it to restore the device to its				
best state.				
Reboot Phone				



Some configuration modifications require a reboot to become effective. Clicking the Reboot button will lead to reboot immediately.

Note: Be sure to save the configuration before rebooting.

(2) Network

a) Basic

System Network Line	Network Status IP: Subnet mask: Default gateway: MAC: MAC Timestamp: Settings	172.18.2.185 255.255.0.0 172.18.1.1 0c:38:3e:1e:61:dd 20170301		
	Subnet mask: Default gateway: MAC: MAC Timestamp:	255.255.0.0 172.18.1.1 Oc:38:3e:1e:61:dd		
	Default gateway: MAC: MAC Timestamp:	172.18.1.1 Oc:38:3e:1e:61:dd		
line	MAC: MAC Timestamp:	Oc:38:3e:1e:61:dd		
ine	MAC Timestamp:			
		20170301		
	Settings			
EGS Setting				
	Static IP 🔘	DHCP	PPPoE O	
EGS Access	DNS Server Configured by	DHCP		
	Primary DNS Server			
EGS Logs	Secondary DNS Server			
		Apply		
Door Lock		Арріу		
	Service Port Settings			
unction Key	Web Server Type	HTTP V		
	HTTP Port	80		
Alert	HTTPS Port	443		
		Apply		
	HTTPS Certification File: https	.pem 4501 Bytes Up	load Delete	

Field Name	Explanation		
Network Status			
IP	The current IP address of the equipment		
Subnet mask	The current Subnet Mask		
Default	The current Catoway IP address		
gateway	The current Gateway IP address		
MAC	The MAC address of the equipment		



MAC	Get the MAC address of time.					
Timestamp						
Settings	Settings					
Select the appro	priate 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 cho	osen, the screen below will appear. Enter values provided by the ISP.					
DNS Server	Coloct the Configured mode of the DNC Comer					
Configured by	Select the Configured mode of the DNS Server.					
Primary DNS						
Server	Enter the server address of the Primary DNS.					
Secondary	Estantia como delas of the Secondary DNS					
DNS Server	Enter the server address of the Secondary DNS.					

Click the APPLY button after entering the new settings. The equipment will save the new settings and apply them. If a new IP address was entered for the equipment, it must be used to login to the phone after clicking the APPLY button.

Service Port Se	ttings			
Web Server	Specify Web Server Type – HTTP or HTTPS			
Туре				
	Port for web browser access. Default value is 80. Change this from the default			
HTTP Port	to enhance security. Setting this port to 0 will disable HTTP access.			
	Example: The IP address is 192.168.1.70 and the port value is 8090. The			
	accessing address is http://192.168.1.70:8090.			
	Port for HTTPS access. An https authentication certification must be			
HTTPS Port	downloaded into the equipment before using https.			
	Default value is 443. Change this from the default to enhance security.			
Note:				

Note:

1) Any changes made on this page require a reboot to become active.

2) It is suggested that the make the values bigger than 1024 if users change the port to HTTPS. Values less than 1024 are reserved.

3) If the HTTP port is set to 0, HTTP service will be disabled.

b) Advanced



	Basic Advanced	VPN			
> System	Link Layer Discovery Protocol				
> Network	Enable LLDP 9 Enable Learning Function		Packet Interval(1~3600)	60 Second(s)	
> Line	ARP Cache Life ARP Cache Life	10 Minute			
› EGS Setting	VLAN Settings Enable VLAN		VLAN ID	256 (0~4095)	
> EGS Access	802.1p Signal Priority	0 (0~7)	802.1p Media Priority	0 (0~7)	
> EGS Logs	Quality of Service (QoS) Settin Enable DSCP QoS		Signal QoS Priority	46(0~63)	
> Door Lock	Media QoS Priority 802.1X Settings	46 (0~63)			
Function Key	Enable 802.1X Username	admin			
> Alert	Password	••••			
			Apply		

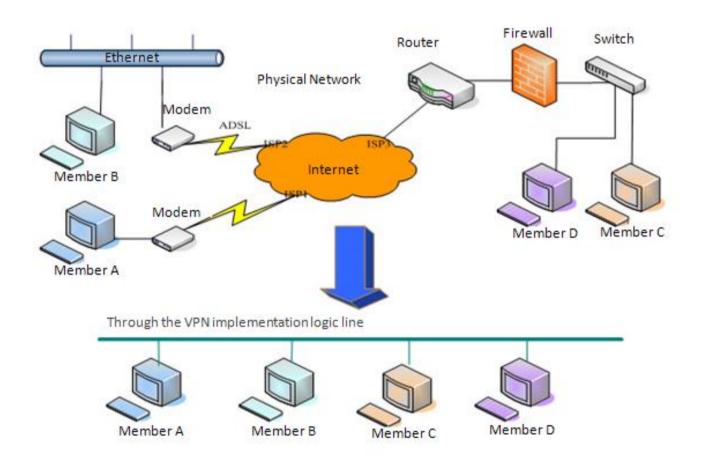
Field Name	Explanation			
Link Layer Discovery Protocol (LLDP)Settings				
Enable LLDP	Enable the device to send LLDP packets.			
Packet				
Interval(1~3600	The time interval of device sending packet. The default value is 60s.			
)				
	Open the device to learn LLDP function, after opening, the device will			
Enable Learning	automatically learn the switch QoS,vlan id,802.1p and other configuration			
Function	values. If not, the device will automatically be updated to the value in the			
switch, synchronizing with the switch's				
ARP Cache Life				
ARP Cache Life	The default ARP aging time is 10 minutes. You can configure the ARP aging			
	time to a reasonable value.			
VLAN Settings				
Enable VLAN	Enable VLAN for WAN			
VLAN ID	Manually set the VLAN ID value, which range is 0-4095			
802.1p Signal	Set the SID 902 1D value, the range is 0.7			
Priority	Set the SIP 802.1P value, the range is 0-7			
802.1p Media	Set the media 202 1D value, the range is 0.7			
Priority	Set the media 802.1P value, the range is 0-7			
Quality of Servic	e (QoS) Settings			



Enable	DSCP			
QoS		enable DSCP		
Signal	QoS	Set the SIP DSCP value		
Priority		Set the SIP DSCP value		
Media	QoS	Set the media RTP DSCP value		
Priority				
802.1X S	ettings			
Enable 8	02.1X	enable 802.1X		
Username Set the 802.1X user name		Set the 802.1X user name		
Password S		Set the 802.1X password		

c) VPN

The device supports remote connection via VPN. It supports both Layer 2 Tunneling Protocol (L2TP) and OpenVPN protocol. This allows users securely connect from public network to local network remotely.





	Basic Advance	d VPN	
→ System	Virtual Private Network (VP	N) Status	
		VPN IP Address:	0.0.0.0
> Network	VPN Mode		
> Line		Enable VPN 🗌 L2TP 〇	OpenVPN 💿
> EGS Setting	Layer 2 Tunneling Protocol ((L2TP)	
> EGS Access		L2TP Server Address Authentication Name	
› EGS Logs		Authentication Password	
> Door Lock	OpenVPN Files		Apply
> Function Key	OpenVPN Configuration file:	client.ovpn N/A	Upload Delete
> Alert	CA Root Certification: Client Certification:	ca.crt N/A client.crt N/A	Upload Delete
	Client Key:	client.key N/A	Upload Delete

Field Name	Explanation				
VPN IP Address	Show the current VPN IP address.				
VPN Mode	VPN Mode				
Enable VPN	Enable/Disable VPN.				
L2TP	Select Layer 2 Tunneling Protocol				
	Select OpenVPN Protocol. (Only one protocol may be activated. After the				
OpenVPN	selection is made, the configuration should be saved and the phone be				
	rebooted.)				
Layer 2 Tunneling Protocol (L2TP)					
L2TP Server	Set VPN L2TP Server IP address.				
Address					
Authentication	Set User Name access to VPN L2TP Server.				
Name	Set User Marile access to VFIN LZTF Server.				
Authentication	Set Password access to VPN L2TP Server.				
Password					
Open VPN Files					
Upload or delete Open VPN Certification Files					

(3) Line a) SIP

Configure a SIP server on this page.



		91		
	SIP Bas	sic Settings Dial Peer		
⊁ System				
> Network		SIP 1 🔽		
> Line	Basic Settings >>	2		
Eline	Line Status Phone number	Registered 5528		172.18.1.88
› EGS Setting	Display name	5528	Backup Proxy Server Address	
	Authentication Nar	1000 C		5060
EGS Access	Authentication Pas Activate	sword	Outbound proxy address Outbound proxy port	
› EGS Logs	Addivate	¥.	Realm	
	Codecs Settings >>			
› Door Lock	Advanced Settings >>			
	Advanced Settings >>	Apply		
Function Key				
Alert				
Codecs Settings >>				
Disabled Codecs		En	abled Codecs	
	→		722 711U	
		G	711A 729AB	
1		_ <u></u>		
Advanced Settings >	·>			
Subscribe For Voi	ice Message			
Voice Message Nu	umber			
Voice Message Su		3600 Second	l(s)	
Enable DND			Ring Type	Default 🖌
Blocking Anonym	ous Call		Conference Type	Local 💙
Use 182 Respons	e for Call waiting		Server Conference Number	
Anonymous Call S	Standard	None 🗸	Transfer Timeout	0 Second(s)
Dial Without Regi			Enable Long Contact	
Click To Talk			Enable Use Inactive Hold	
User Agent			Use Quote in Display Name	
Response Single	Codec			
200 CONTROL 201 815				
Use Feature Code	2			
Enable DND			DND Disabled	
Enable Blocking A	Anonymous Call		Disable Blocking Anonymous	Call



Specific Server Type	COMMON 🗸	Enable DNS SRV	
Registration Expiration	60 Second(s)	Keep Alive Type	UDP 🔽
Use VPN	\checkmark	Keep Alive Interval	30 Second(s)
Use STUN		Sync Clock Time	
Convert URI	\checkmark	Enable Session Timer	
DTMF Type	AUTO 🔽	Session Timeout	0 Second(s)
DTMF SIP INFO Mode	Send */# 🖌	Enable Rport	
Transportation Protocol	UDP 🗸	Enable PRACK	
Local Port	5060	Auto Change Port	
SIP Version	RFC3261 🗸	Keep Authentication	
Caller ID Header	PAI-RPID-	Auto TCP	
Enable Strict Proxy		Enable Feature Sync	
Enable user=phone	\checkmark	Enable GRUU	
Enable SCA		BLF Server	
Enable BLF List		BLF List Number	
SIP Encryption		RTP Encryption	
SIP Encryption Key		RTP Encryption Key	

SIP			
Field Name	Explanation		
Basic Settings (Choose the SIP line to configured)			
	Display the current line status at page loading. To get the up to date line		
	status, user has to refresh the page manually. There is some status here:		
	1) Inactive, indicates that this line is not activated yet, user can activate		
	the line by selecting the option "activate".		
	2) Timeout, indicates the SIP registration status timeout. It means that		
	there's no response from SIP server. User may need to check the network		
	or SIP server IP address and port.		
Line Status	3) Registered, indicates the SIP account is registered to SIP server		
	successfully, is able to send or receive calls.		
	4) 403 forbidden, indicates the SIP error code 403, means SIP server		
	rejected the SIP registration because the username and password is		
	incorrect. User will need to check the username and password, they must		
	be matched with the username and password which were provided by SIP		
	server.		
	Other SIP error code, check SIP protocol standard, or contact support.		
Username	Enter the username of the service account		
Display name	Enter the display name to be sent in a call request.		
Authentication Name	Enter the authentication name of the service account, which is assigned		
	by IPPBX administrator, or provided by ISP provider.		
Authentication	Enter the authentication password of the service account, which is		
Password	assigned by IPPBX administrator, or provided by ISP provider.		

www.fanvil.com



Activate	Whether the service of the line should be activated		
SIP Proxy Server			
Address	Enter the IP or FQDN address of the SIP proxy server		
SIP Proxy Server Port	Enter the SIP proxy server port, default is 5060		
Outbound proxy	Enter the IP or FQDN address of outbound proxy server which are		
address	provided by the service provider		
Outbound proxy port	Enter the outbound proxy port, default is 5060		
Realm	Enter the SIP domain if requested by the service provider		
Codecs Settings			
Set the priority and avai	ilability of the codecs by adding or removing them from the list.		
Advanced Settings			
	Enable the device to subscribe a voice message of waiting notification, if it		
Subscribe For Voice	is enabled, the device will receive notification from the server when there		
Message	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 DND	Enable Do-not-disturb, any incoming call to this line will be rejected automatically		
Blocking Anonymous Call	Reject any incoming call without presenting caller ID		
Use 182 Response for Call waiting	Set the device to use 182 response code at call waiting response		
Anonymous Call Standard	Set the standard to be used for anonymous		
Dial Without Registered	Set call out by proxy without registration		
Click To Talk	Set Click To Talk		
User Agent	Set the user agent, the default is Model with Software Version.		
Response Single	If setting is enabled, the device will use single codec in responding to an		
Codec	incoming call request		
Ring Type	Set the ring tone type for the line		
	Set the type of call conference, Local=set up call conference by the device		
Conference Type	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		
Transfer Timeout	Set the timeout of call transfer process.		



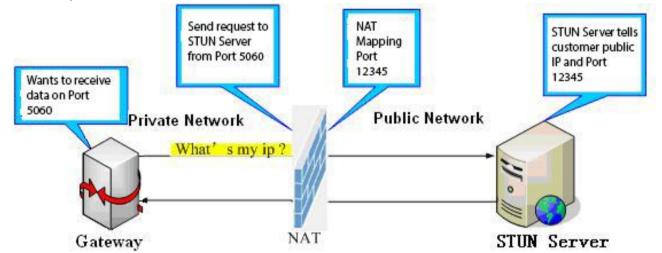
Enable Long Contact	Allow more parameters in contact field per RFC 3840.		
Enable Use Inactive	When Inactive Hold is enabled, the caller's SIP packet will with Inactive		
Hold	fields on the condition of holding a call.		
Use Quote in Display			
Name	Whether to add quote in display name.		
	When this setting is enabled, the features in this section will not be		
Use Feature Code	handled by the device itself but by the server instead. In order to control		
Use realure Code	the enabling of the features, the device will send feature code to the		
	server by dialing the number specified in each feature code field.		
Specific Server Type	Set the line to collaborate with specific server type.		
Registration Expiration	Set the SIP expiration interval.		
Use VPN	Set the line to use VPN restrict route.		
Use STUN	Set the line to use STUN for NAT traversal.		
Convert URI	Convert not digit and alphabet characters to %hh hex code.		
DTMF Type	Set the DTMF type to be used for the line.		
DTMF SIP INFO			
Mode	Set the SIP INFO mode to send '*' and '#' or '10' and '11'.		
Transportation	Set the line to use TCD or LIDD for CID transmission		
Protocol	Set the line to use TCP or UDP for SIP transmission.		
Local Port	Set the Local Port.		
SIP Version	Set the SIP version.		
Caller ID Header	Set the Caller ID Header.		
Enable Strict Drovy	Enables the use of strict routing. When the phone receives packets from		
Enable Strict Proxy	the server, it will use the source IP address, not the address in via field.		
Enable user=phone	Sets user=phone in SIP messages.		
Enable SCA	Enable/Disable SCA (Shared Call Appearance)		
Enable DNS SRV	Set the line to use DNS SRV which will resolve the FQDN in proxy server		
	into a service list.		
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to keep NAT		
Reep Alive Type	pinhole opened.		
Keep Alive Interval	Set the keep alive packet transmitting interval.		
Sync Clock Time	Synchronize with server time.		
	Set the line to enable call ending by session timer refreshment. The call		
Enable Session Timer	session will be ended if there is not new session timer event update		
	received after the timeout period.		
Session Timeout	Set the session timer timeout period.		
Enable rPort	Set the line to add rPort in SIP headers.		
Enable PRACK	Set the line to support PRACK SIP message.		

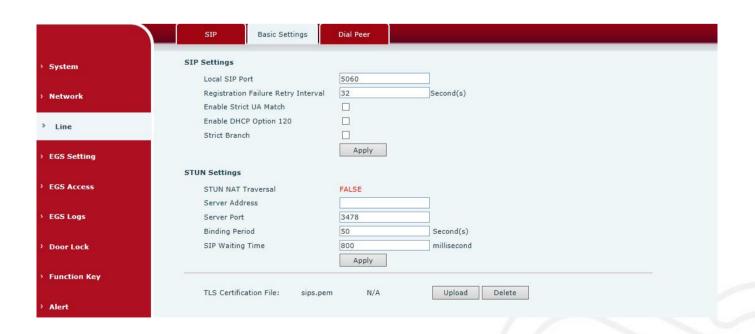


Auto Change Port	Enable/Disable Auto Change Port.	
Keep Authentication	Keep the authentication parameters from previous authentication.	
	Using TCP protocol to guarantee usability of transport for SIP messages	
Auto TCP	above 1500 bytes.	
Enable Feature Sync	Feature Sycn with server.	
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)	
RTP Encryption	Enable RTP encryption such that RTP transmission will be encrypted.	
RTP Encryption Key	Set the pass phrase for RTP encryption.	

b) 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.







Basic Settings			
Field Name	Explanation		
SIP Settings			
Local SIP Port	Set the local SIP port used to send/receive SIP messages.		
Registration Failure Retry Interval	Set the retry interval of SIP REGISTRATION when registration failed.		
Enable Strict UA Match	Enable or disable Strict UA Match		
Enable DHCP Option 120	DHCP Server would respond an OPTION message to the request from DHCP client. To work with the terminal device, Access device and DHCP policy server would be able to implement the zero configuration and auto provisioning. OPTION 120 is one of the OPTIONS in which the device could obtain the SIP server address from the ACK response sent back by the DHCP server. Then the SIP Agent of terminal device starts register with the SIP server address.		
Strict Branch The value determined whether it's exactly matched the Branch			
STUN Settings	-		
Server Address	STUN Server IP address		
Server Port	STUN Server Port – Default is 3478.		
Binding Period	STUN blinding period – STUN packets are sent at this interval to keep the NAT mapping active.		
SIP Waiting Time Waiting time for SIP. This will vary depending on the network.			
TLS Certification File			
Upload or delete the TLS certification file used for encrypted SIP transmission.			
Note: the SIP STUN	is used to achieve the SIP penetration of NAT, and the realization of a		
service, when the ec	uipment configuration of the STUN server IP and port (usually the default is		
3478), and select the Use Stun SIP server, the use of NAT equipment to achieve penetration.			

C) Dial Peer

Configure the Dial Peer to make the device call more flexible.



	SIP Dial Peer
em	
rork	Import Dial Peer Table Select File Browse (dialPeer.csv) Update
e	Dial Peer Table
Setting	Total: 0 Prev Page: V Next Octave Data Peer Table
Access	Index Number Destination(Optional) Port (Optional) Call Mode Alias(Optional) Suffix Deleted Length (Optional) (Optional) Add Dial Peer
Logs	Number Destination(Optional)
Lock	Port(Optional) Alias(Optional) Call Mode SIP Suffix(Optional) Deleted Length(Optional)
	Add Modify

Import Dial peer Table		
Field Name	Explanation	
Select File	Select an existing dialing rule file. The file type must be a .CSV	
Add Dial Peer		
	To add an outgoing call number. The outgoing call number can be divided	
	into two types: one is the exact match, and after the exact match, if the	
	number is exactly the same as the user dialing the called number, the	
	device will use the IP address of this number mapping or (This is the area	
Number	code prefix function of the PSTN). If the number matches the N-bit (prefix	
Number	number length) of the called number, the device uses the IP address or	
	configuration mapped to this number. Make a call. Configuration prefix	
	matching needs to be followed by a prefix number to match the exact	
	match number; the longest support is 30 bits; also supports the use of \mathbf{x}	
	format and range of numbers.	
	Configure the destination address. If it's configured as a point-to-point call,	
Destination	write the peer IP address directly. Can also be set to domain name, by the	
Destination	device DNS server to resolve the specific IP address. If it is not configured,	
	the IP address is 0.0.0.0. This is an optional configuration item	
Port	Configure the signaling port of the other party. This is an optional	
	configuration item. The default is 5060	
Alias	Configure aliases. This is an optional item: the replacement number will be	
ΠΙαδ	used when the prefix is prefixed, and no alias when it is configured	



Note: aliases are divided into four types and must be combined with the replacement length: 1) add: xxx, add xxx before the number. This can help users save dialing length;

2) all: xxx, all replaced by xxx; can achieve speed dial, such as user configuration dial-up 1, then by configuring all: number to change the actual call out the number;

3) del, delete the number before the n bit, n by the replacement length set;

4) rep: xxx, the number n before the number is replaced by xxx, n is set by the replacement length. For example, if the user wants to dial the PSTN (010-62281493) through the floor service provided by the VoIP operator, and the actual call should be 010-62281493, then we can configure the called number 9T, then rep: 010, and then delete the length Set to 1. Then all users call the 9 at the beginning of the phone will be replaced with 010 + number sent. To facilitate the user to call the habit of thinking mode;

Call Mode	Configuration selection of different signaling protocols, SIP;	
Suffix	Configure the suffix, this is optional configuration items: that is, after the	
Sullix	dial-up number to add this suffix, no configuration shows no suffix;	
Deleted Length	Configure the replacement / delete length, the number entered by the user	
	is replaced / deleted by this length; this is an optional configuration item;	

(4) EGS Setting

a) Features

	Features Audio	Video	MCAST Action URL	Time/Date
n				
	Common Settings			
ork	Switch Mode	Monostable 🗸	Switch-On Duration	5 (1~600)Second(s
	Enable Card Reader	Enable 🗸	Card Reader Working Mode	Normal
	Card Reader HF Card Data Reverse	Disable 🗸 😡		
Setting	Limit Talk Duration	Enable 🔽	Talk Duration	120 (20~600) Second (s)
	Remote Password	•	Local password	
ccess	APP Door Open	Disable 🗸	APP Password	•
	Enable Indoor Open	Enable 🔽	Enable Access Table	Enable 💙
ogs	Description	i23S IP Door Phone	Enable Open Log Server	Disable 🗸
	Address of Open Log Server	0.0.0.0	Port of Open Log Server	514
Lock	Door Unlock Indication	Long Beeps 🔽	Remote Code Check Length	4 (1~11)
			Apply	
ion Key				
	Basic Settings >>			
	Block Out Settings >>			



Enable DND		Ban Outgoing		
Enable Intercom Mute	\checkmark	Enable Intercom Ringing	~	
Enable Auto Dial Out	✓	Auto Dial Out Time	5	(3~30)Second(s)
Enable Auto Answer	Lines and IP Call 🗸	Auto Answer Timeout	0	(0~60)Second(s)
No Answer Auto Hangup		Auto Hangup Timeout	30	(1~60)Second(s)
Dial Fixed Length to Send	\checkmark	Send length	4	
Dial Number Voice Play	Disable 🗸	Voice Play Language	English	~
Enable Delay Start		Delay Start Time	1	(1~180)Second(s
Voice Read IP	Enable 🔽	Press "*" to Send	~	
		Apply		
Block Out Settings >>				
		Block Out List		
	Add	v		Delete

Features			
Field Name	Explanation		
Common Settings			
	Monostable: there is only one fixed action status for door unlocking. See		
	"Switch-On Duration" too.		
Switch Mode	Bistable: there are two actions and statuses, door unlocking and door		
Switch Mode	locking. Each action might be triggered and changed to the other status.		
	After changed, the status would be kept.		
	default Value is Monostable		
Switch-On Duration	Door unlocking time for Monostable mode only. If the time is up, the door		
Switch-Off Duration	would be locked automatically. Default Value is 5 seconds.		
Enable Card Reader	Enable or disable card reader for RFID/IC cards.		
	Set RFID/IC card stats:		
	Normal: This is the work mode, in which user can use the authorized		
	card can to open the door.		
Card Reader Working	Card Issuing: This is the issuing mode; the swiped card will be added in		
Mode	access list automatically. User could edit other parameters under EGS		
	access.		
	Card Revoking: This is the revoking mode; the swiped card will be		
	deleted from Access List.		
Card Reader HF	Set the format of HF card to make the data sequence reverse to meet		
Card Data Reverse	with specific card.		
Limit Talk Duration	If enabled, calls would be forced ended after talking time is up.		
Talk Duration	The call will be ended automatically when time up. Initial Value is 120		
	seconds		



Remote Password	Remote door unlocking password. Initial Value is "*".				
Local password	Local door unlocking password via keypad, the default password length is 4. Initial Value is "6789".				
APP Door Open	Enable or disable the APP Door Open.				
APP password	APP door unlocking password. Initial Value is "*".				
Enable Indoor Open	Enable or disable to use indoor switch to unlock the door.				
Enable Access Table	 Enable Access Table: enter <access code=""> for opening door during calls.</access> Disable Access Table: enter <remote password=""> for opening door during calls.</remote> Default Enable. 				
Description	Device description displayed on IP scanning tool software. Initial Value is "i23S IP Door Phone".				
Enable Open Log Server	Enable or disable to connect with log server.				
Address of Open Log Server	Log server address (IP or domain name)				
Port of Open Log Server	Log server port (0-65535), Initial Value is 514.				
Door Unlock	Indication tone for door unlocked. There are 3 types of tone: silent/short				
Indication	beeps/long beeps.				
Remote Code Check Length	The remote access code length would be restricted with it. If the input access code length is matched with it, system would check it immediately. Initial Value is 4.				
Basic Settings					
Enable DND	DND might be disabled phone for all SIP lines, or line for SIP individually. But the outgoing calls will not be affected.				
Ban Outgoing	If enabled, no outgoing calls can be made.				
Enable Intercom Mute	If enabled, mutes incoming calls during an intercom call.				
Enable Intercom Ringing	If enabled, plays intercom ring tone to alert to an intercom call.				
Enable Auto Dial Out	Enable Auto Dial Out.				
Auto Dial Out Time	Set Auto Dial Out Time.				
Enable Auto Answer	Enable Auto Answer function.				
Auto Answer Timeout	Set Auto Answer Timeout.				
No Answer Auto Hangup	Enable automatically hang up when no answer.				
Auto Hangup Timeout	Configuration in a set time, automatically hang up when no answer.				



Dial Fixed Length to	Enable or disable dial fixed length to send.			
Send	Enable of disable dial liked length to send.			
Send length	The number will be sent to the server after the specified numbers of			
	digits are dialed.			
Dial Number Voice	Configuration Open / Class Dial Number Vision Play			
Play	Configuration Open / Close Dial Number Voice Play.			
Voice Play Language	Set language of the voice prompt.			
Enable Delay Start	Enable or disable the start delay.			
Delay Start Time	Set start delay time.			
Voice Read IP	Enable or disable voice broadcast IP address.			
Press "*" to Send	Enable or disable the Press "*" to Send, Initial Value is enable.			
Block Out Settings				
Add or delete blocked numbers – enter the prefix of numbers which should not be dialed by the				
phone. For example, if 001 is entered, the phone would not dial any number beginning with 001.				
X and x are wildcards which match single digit. For example, if 4xxx or 4XXX is entered, the				
phone would not dial any 4 digits numbers beginning with 4. It would dial numbers beginning with				
4 which are longer or shorter than 4 digits.				

b) Audio

This page configures audio parameters such as voice codec, speak volume, mic volume and ringer volume.

	Features Audio	Video	MCAST	Action URL	Time/Date	
> System	Audio Settings					
> Network	First Codec Third Codec Fifth Codec	G.722 V G.711U V None V	Second Co Fourth Co Sixth Cod	dec	G.711A G.729AB None	
› Line	DTMF Payload Type Pass Tone	101 (96~127) Default 🗸	Default Ring Type Fail Tone		Type 1 Default United Sta 6.3kb/s 5 (1~9) 4 (0~9)	
> EGS Setting	G.729AB Payload Length G.722 Timestamps	20ms V 160/20ms V 5 (1~9) 5 (1~9)	Tone Standard G.723.1 Bit Rate			
+ EGS Access	Speakerphone Volume Broadcast Output Volume		MIC Input Volume Signal Tone Volume			
> EGS Logs	Enable VAD					
> Door Lock		Apply				
Sound Update Sound Update Sound Update Sound Update Select (*.wav) Upgrade						
> Alert	Sound Delete					?
	Sound Delete 🔽 Delete	a				

Audio Setting		
Field Name	Explanation	
First Codec	The first codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB	
Second Codec	The second codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB,	
	None	

www.fanvil.com



Third Codec	The third codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, None			
Fourth Codec	The forth codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, None			
DTMF Payload Type	The RTP Payload type that indicates DTMF. Default is 101			
Default Ring Type	Ring Sound – There are 9 standard types and 3 User types.			
Pass Tone	When the door opened successfully, the device will play the correct tone s by the user.			
Fail Tone	When the door fails to open, the terminal will play an error tone set by the user.			
G.729AB Payload Length	G.729AB Payload Length – Adjusts from 10 – 60 ms.			
Tone Standard	Configure tone standard area.			
G.722 Timestamps	Choices are 160/20ms or 320/20ms.			
G.723.1 Bit Rate	Choices are 5.3kb/s or 6.3kb/s.			
Speakerphone Volume	Set the speaker calls the volume level.			
MIC Input Volume	Set the MIC calls the volume level.			
Broadcast Output Volume	Set the broadcast the output volume level.			
Signal Tone Volume	Set the audio signal the output volume level.			
Enable VAD	Enable or disable Voice Activity Detection (VAD). If VAD is enabled, G729 Payload length cannot be set greater than 20 ms.			

c) Video

This page allows you to set the video capture and video encode.



Max S Num N/A Use 0 Inc Position <		Features Aud	io Video	MCAST	Action URL	Time/Date	
Network Max M Num N/A Use 0 Max S Num N/A Use 0 Ine Ip Camera Settings>> Position ipCameraName (40 Characters) Ver	> System						
Network Max S Num N/A Use 0 Ine Ip Camera Settings>> Position ipCameraName (40 Characters) Position User (40 Characters) Password							
Max S Num N/A Use 0 Ine Ip Camera Settings>> Position Position User Password Password Ip Camera Brand IP Port Stage Port Stage Max S Num Position Ip Camera Settings>> Position Position Position Ip Camera Brand XM IP Port Stage Max S Num Port Stage Main Stream Url Sub Stream Url Apply Punction Key Advanced Settings >>) Network	Max M Num	N/A	Use		0	
Position ipCameraName Iser User Password	2 HELWOIK	Max S Num	N/A	Use		0	
> EGS Setting User Password	› Line	Ip Camera Settings>>					
Password		Position	ipCameraNan	ne	(40 Characters)		
> EGS Access Ip Camera Brand IP IP > EGS Logs Port Sub Stream Url Sub Stream Url Apply Alert	> EGS Setting	User					
IP Port Port Main Stream Url Sub Stream Url Sub Stream Url		Password					
IP Port Sub Stream Url Sub Stream Url Sub Stream Url	FGS Access	Ip Camera Brand	XM	ľ			
Main Stream Url Sub Stream Url Sub Stream Url Apply Advanced Settings >> RTSP Information		IP					
Kus Lugs Main Stream Url Main Stream Url Apply Sub Stream Url Apply Function Key Advanced Settings >> RTSP Information		Port	554				
 > Door Lock > Function Key > Advanced Settings >> RTSP Information 	> EGS Logs						
 Door Lock Apply Function Key Advanced Settings >> Alert RTSP Information 							
Alert	> Door Lock	Sub Stream on	Apply				
> Alert	• Function Key	Advanced Settings >>					
	N ATOM	RTSP Information					
Main Stream Url : F	Alen	Main Stream Url :					Previ
Sub Stream Url :		Sub Stream Url :					Previe

Video					
Field Name		Explanation			
Camera Status : Display the relevant information of the camera, including maximum acces					
maximum stream,	max	imum sub stream, and the status.			
IP Camera Settin	gs				
Position		Set IP Camera Name.			
User name		External camera login required account.			
Password		External camera login password required.			
IP Camera Brand		Select the camera manufacturers.			
IP address		IP address of the camera, please use the camera matching scan tool to			
IF address		obtain the IP address.			
Port		Camera port number.			
Advanced Setting	gs				
Video Direction	Sele	ect the transport type of the video stream.			
H.264 Payload	Sot	the payload type of H 264			
Туре	Set the payload type of H.264.				
RTSP information		Click [Apply], the connection automatically shows the camera does no			
		show the reverse.			
Preview		Copy and paste the main stream or sub-stream URL into the VLC player,			
Preview		or click [Preview] to display the current camera video.			

d) MCAST



MCAST Settings		
Priority	1	
Enable Page Priority		
Index/Priority	Name	Host:port
1		
2		
3		
4		
5		
10		
	Priority Enable Page Priority Index/Priority 1 2 3 4	Priority 1 Enable Page Priority Index/Priority Name 1 2 3 4 5 6 7 8 9

It is easy and convenient to use multicast function to send notice to each member of the multicast by 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.

MCAST Settings

Equipment can be set up to monitor up to 10 different multicast addresses, which is used to receive the multicast RTP stream sent by the multicast address.

Here are the ways to change equipment receiving multicast RTP stream processing mode in the Web interface: set the ordinary priority and enable page priority.

• Priority:

In the drop-down box to choose priority of ordinary calls the priority, if the priority of the incoming flows of multicast RTP, lower precedence than the current common calls, device will automatically ignore the group RTP stream. If the priority of the incoming flow of multicast RTP is higher than the current common calls priority, device will automatically receive the group RTP stream, and keep the current common calls in state. You can also choose to disable in the receiving threshold drop-down box, the device will automatically ignore all local network multicast RTP stream.

- The options are as follows:
 - \diamond 1-10: To definite the priority of the common calls, 1 is the top level while 10 is the lowest
 - ♦ Disable: ignore all incoming multicast RTP stream
 - \diamond Enable the page priority:

Page priority determines the device how to deal with the new receiving multicast RTP stream when it is in multicast session currently. When Page priority switch is enabled, the device will automatically ignore the low priority multicast RTP stream but receive top-level priority multicast RTP stream, and keep the current multicast session in state; If it is not enabled, the device will automatically ignore all receiving multicast RTP stream.

Web Settings:

www.fanvil.com



ST Settings		
Priority	1	
Enable Page Priority		
Index/Priority	Name	Host:port
1	SS	239.1.1.1:1366
2	ee	239.1.1.1:1367

The multicast SS priority is higher than that of EE, which is the highest priority.

Note: when pressing the multicast key for multicast session, both multicast sender and receiver will beep.

riority	3	
nable Page Priority		
Index/Priority	Name	Host:port
1	group 1	224.0.0.2:2366
2	group 2	224.0.0.2:1366
3	group 3	224.0.0.6:3366
4		
5		
6		
7		
8		
9		
10		

Blue part (name)

"Group 1","Group 2" and "Group 3" are your setting monitoring multicast name. The group name will be displayed on the screen when you answer the multicast. If you have not set, the screen will display the IP: port directly.

Purple part (host: port)

It is a set of addresses and ports to listen, separated by a colon.

Pink part (index / priority)

Multicast is a sign of listening, but also the monitoring multicast priority. The smaller number refers to higher priority.

Red part (priority)

It is the general call, non-multicast call priority. The smaller number refers to high priority. The followings will explain how to use this option:

www.fanvil.com



- The purpose of setting monitoring multicast "Group 1" or "Group 2" or "Group 3" launched a multicast call.
- ♦ All equipment has one or more common non-multicast communication.
- When you set the Priority for the disable, multicast any level will not answer, multicast call is rejected.
- when you set the Priority to a value, only higher than the priority of multicast can come in, if you set the Priority is 3, group 2 and group 3 for priority level equal to 3 and less than 3 were rejected, 1 priority is 2 higher than ordinary call priority device can answer the multicast message at the same time, keep the hold the other call.

• Green part (Enable Page priority)

Set whether to open more priority is the priority of multicast, multicast is pink part number. Explain how to use:

- The purpose of setting monitoring multicast "group 1" or "3" set up listening "group of 1" or "3" multicast address multicast call.
- ♦ All equipment has been a path or multi-path multicast phone, such as listening to "multicast information group 2".
- If multicast is a new "group of 1", because "the priority group 1" is 2, higher than the current call
 "priority group 2" 3, so multicast call will can come in.
- If multicast is a new "group of 3", because "the priority group 3" is 4, lower than the current call
 "priority group 2" 3, "1" will listen to the equipment and maintain the "group of 2".

Multicast service

- **Send:** when configured ok, our key press shell on the corresponding equipment, equipment directly into the Talking interface, the premise is to ensure no current multicast call and 3-way of the case, the multicast can be established.
- **Monitor:** IP port and priority configuration monitoring device, when the call is initiated and incoming multicast, directly into the Talking interface equipment.

e) Action URL



	Features Audio	Video	MCAST Action URL	
System	Action URL Event Settings			
	Active URI Limit IP			
Network	Setup Completed			
	Registration Succeeded			
Line	Registration Disabled			
Line	Registration Failed			
	Off Hooked			
EGS Setting	On Hooked			
	Incoming Call			
EGS Access	Outgoing calls			
	Call Established			
EGS Logs	Call Terminated			
	DND Enabled			
Door Lock	DND Disabled			
	Mute			
Function Key	Unmute			
	Missed calls			
Alert	IP Changed			
	Idle To Busy			
	Busy To Idle			
	Open The Door			
	Close The Door			
		Apply		

Action URL Event Settings

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

f) Time/Date



	Features Audio	Video	MCAST	Action URL	Time/Date
tem	Network Time Server Settings				
	Time Synchronized via SNTP	\checkmark			
work	Time Synchronized via DHCP				
	Primary Time Server	time.nist.gov			
e	Secondary Time Server	pool.ntp.org			
	Time zone	(UTC+8) 中国,新加	坡,澳大利亚,Russ	~	
	Resync Period	60	(1~5000)	Second(s)	
SS Setting	Date Format				
Access	Date Format	1 JAN MON	~		
i Logs		Apply			
or Lock	Daylight Saving Time Settings				
	Location	中国(北京)	~		
ction Key	DST Set Type	Disabled	~		
		Apply			
rt	Manual Time Settings 9				
	2018-04-14 16	✓ 55 ✓	Apply]	
		terre and the second se		-	

Time/Date	Time/Date			
Field Name	Explanation			
Network Time Server Settings				
Time Synchronized via SNTP	Enable time-sync through SNTP protocol			
Time Synchronized via DHCP	Enable time-sync through DHCP protocol			
Primary Time Server	Set primary time server address			
Secondary Time	Set secondary time server address, when primary server is not reachable, the device			
Server	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			
Date Format				
Date Format	Select the time/date display format			
Daylight Saving Tim	e Settings			
Location	Select the user's time zone specific area			
DST Set Type	Select automatic DST according to the preset rules of DST, or the manually input			
DSTSetType	rules			
Manual Time Setting	JS			
The time set by hand,	, need to disable SNTP service first.			
Daylight Saving Time Settings				

(5) EGS Access

www.fanvil.com



> System	Import Access Table	2					
	Select File		Browse (acces	sList.csv) Update			
> Network	Access Table >>						
	Total: 0	Prev Page: 🗸	Next		Click here to S	ave Access Table Delete All	
> Line				mbor Fwd Access	Daubla	Issuing Card	
> EGS Setting	Index Name	ID Departmer	nt Position Location Nu	umber Fwd Access Number Code	Auth Profile Type	Date State	
	Add Access Rule		11 M				
EGS Access	Name	-	*	Location		0	
> EGS Logs	ID Card State	Enable 🗸	Ľ	Number Fwd Number	7 <u>2</u> 		
2 Eus Logs	Department			Access Code		0	
> Door Lock	Position			Double Auth	Disable 🔽 🚺		
	Туре	Guest 💙		Profile	None 🗸		
Function Key			Add	Modify			
Profile Setting							
Profile		Profile1	T	Profile Name			
					2.50) 55	d Time/00.0	0.22.50)
Weekday		Statue	SL	art Time(00:00-2	(3:59) En	d Time(00:0	10-23:59)
Sunday		No 🔻		00:00		00:00	
Monday		No 🔻		00:00		00:00	
Tuesday		No 🔻		00:00		00:00	
Wednesda	у	No 🔻		00:00		00:00	
Thursday		No 🔻		00:00		00:00	
Friday		No 🔻		00:00		00:00	
Saturday		No 🔻		00:00		00:00	
			Apply				
Administrator Table >>	28	1					
Add Admin Card		Issuer	▼ Add		_		
Total: 0 Prev	Page:	Next			0	Delete	Delete All
🗌 Index	I)		Issuing Dat	te		Туре
EGS Access							
Field Name Ex	planation						
Import Access Tal	-						
		• •					

Click the <Browse> to choose to import remote access list file (access List.csv) and then clicking <Update> can batch import remote access rule.

Access Table

According to entrance guard access rules have been added, you can choose single or multiple rules on this list to delete operation.

Add Access Rule			
Name(necessar y)	User name		
Location	Virtual extension number, used to make position call instead of real number.		
	It might be taken with unit number, or room number.		
	RFID/IC card number. You can manually fill in the first 10 digits of the card		
ID	number or select the existing card number		



Number	User phone number
Card State	Enable or disable holder's RFID card
Fwd Number	Call forwarding number when above phone number is unavailable.
Department	Card holder's department
Access Code	 1/ When the door phone answers the call from the corresponding <phone< li=""> Num> user, then the <phone num=""> user can input the access code via keypad to unlock the door remotely.</phone> 2/ The user's private password should be input via keypad for local door unlocking. The private password format is Location * Access Code. </phone<>
Position	Card holder's position
Double Auth	When the feature is enabled, private password inputting and RFID reading must be matched simultaneously for door unlocking.
Туре	Host: the door phone would answer all call automatically. Guest: the door phone would ring for incoming call, if the auto answer is disabled.
Profile	It is valid for user access rules (including RFID/IC, access code, etc.) within corresponding time section. If NONE is selected, the feature would be taken effect all day.
Profile Setting	
Profile	There are 4 sections for time profile configuration
Profile Name	The name of profile to help administrator to remember the time definition
Status	If it is yes, the time profile would be taken effect. Other time sections not included in the profiles would not allow users to open door
Start Time	The start time of section
End Time	The end time of section
Administrator Ta	able
Add Admin Card	You should input the top 10 digits of RFID card numbers. for example, 0004111806, selected the type of admin card, click <add>.</add>
Type: Issuer and	revocation
entrance guard in	uard is in normal state, swipe card (issuing card) would make to the issuing state, and then you can swipe a new card, which the card would database; when you swipe the issuing card again after cards added
done, entrance g	uard would return to normal state. Delete card operation is the same with
	upport up to 10 admin cards, 5000 copies of ordinary cards.
	ng state, swiping deleted card is invalid.
· · · · · · · · · · · · · · · · · · ·	uing Date and Type of admin card
Delete	Clicking <delete> would delete the selected admin card in the list.</delete>
Delete All	Click <delete all="">, to delete all admin card lists.</delete>



(6) EGS Logs

EGS Logs is used to record the log to open the door, no matter it's success or failure. It supports up to 200 thousand record, the latest record will be displayed on the top. Once the total record reaches the limit value 200 thousand, the new record will replace the oldest record. To export the record, user can right click "Click here to Save Logs" and select "Save link as" to save the log to a CSV format file.

→ System							
> Network	Door Open Log						
	Page : Prev Next Delete All Click here to Save Logs						
› Line	Door Result Time Access Name Access ID Type						
> EGS Setting							
› EGS Access							
> EGS Logs							
> Door Lock							
> Function Key							
› Alert							
Field Name	Explanation						
Door Open Log	9						
Result	Show the results of the open the door (Succeeded or Failed)						
Time	The time of opening door.						
Access Name	If the door was opened by swipe card or remote unlocking door, the device						
Access Name	would display remote access name.						
	1. If the opening door method is swiping card, it wound display the card number						
	2. If the opening door way is remote access, it wound display the remote						
Access ID	extension's number.						
	3. If the opening door way is local access, there is no display information.						
	Open type: 1. Local, 2. Remote, 3. Brush card (Temporary Card, Valid Card and						
	Illegal Card).						
	Note: there are three kinds of brushing card feedback results.						
Туре	1. Temporary Card (only added) the card number, without adding other rules)						
	 Valid Card (added access rules) 						
	3. Illegal Card (Did not add information)						

(7) Door Lock



System	Current Lock Status	
	Door Lock 1:	Door Close
Network	Door Lock Control	
Line	Door Lock	
	Action	Door Open 🗸
EGS Setting	Open Mode	Once V
EGS Access		Apply
	Auto Open Setting	
EGS Logs	Sip Register Fail	
	Line	Sip 1 🗸
Door Lock	Door Lock	1 🗸
	Waiting Time	180 (s)
Function Key		
	Network Connect Fail	
Alert	Door Lock	1 🗸
	Waiting Time	180 (s)
		Apply

Field Name	Explanation				
Current Lock S	tatus				
Door Lock	Display the current lock status.				
Door Lock Con	trol				
Door Lock	Door lock code				
Action	Action to open/close the door				
	The action of door open mode:				
	#1 The door will open after choose the "once" and it will return to normal status				
Open Mode	after timeout.				
	#2 The door will open after choose the "always" and it will keep the open status				
	until someone close the door via Web/TR-069.				
Auto Open Set	ting				
Set the door ope	en when "SIP registration failed" and "Network connection failed".				
Sip Register	Enable "SIP registration failed" to open the door automatically.				
Fail					
Line	Select the line information when "SIP registration failed" is enabled.				
Door Lock	Select "SIP registration failed" to automatically open the door lock.				
Waiting Time	Set the duration of door open.				
Network	Enable "Notwork connection foiled" to open the deer outematically				
Connect Fail	Enable "Network connection failed" to open the door automatically.				
Door Lock	Select "SIP registration failed" to open the door automatically.				
Waiting Time	Set the duration of door open.				

(8) Function Key



System									
Network	Function Key Settin								
	Key	Туре		Number 1	Number 2	Line	10 M	Subtype	
Line	DSS Key 1	Hot Key	✓ 8:	102		SIP1	✓ Spe	eed Dial	~
	Advanced Settings								
EGS Setting	Use Function Ke	v to Answer	Enable	~	Use Hot Key to Hangup	Er	able 🗸]	
EGS Access	Hot Key Dial Mo	le Select	Main-Se	condary 🗸					
	Call Switched Ti	ne	16	(5~50)Second(s)					
EGS Logs	Day Start Time		06:00	(00:00~23:59)	Day End Time	18	8:00	(00:00~23:59)	
Door Lock Function Key					Apply				
Alert									

> Key Event

You might set up the key type with the Key Event.

Key	Туре	Number 1	Number 2	Line	Subtype
DSS Key 1	Key Event 🔻			SIP1 V	ОК
		A	pply		None Dial Release OK Handfree
Туре	Subtype	Usage	1		
	None	No res	ponding		
	Dial	Dialing	function		
Key Event	Release	Delete	password input, c	ancel dialing	g input and end
		call			
	OK	identifi	cation key		

> Hot Key

You might enter the phone number in the input box. When you press the shortcut key, equipment would dial preset telephone number. This button can also be used to set the IP address: you can press the shortcut key to directly make an IP call.

Key	Туре	Number 1	Number 2	Line	Subtype	
DSS Key 1	Hot Key 🔻			SIP1	Speed Dial	•
	,		51V		Speed Dial	
		Δι	pply		Intercom	

Туре	Number	Line	Subtype	Usage
	Fill the	The SIP		Using Speed Dial mode together with
Hot Key	called	account	Speed Dial	Enable Speed Dial Hangup Enable v, can define
	party's SIP	correspond		whether this call is allowed to be hung up



	account or	ing lines		by re-pressing the speed dial key.
	IP address			
				In Intercom mode, if the caller's IP phone
			Intercom	supports Intercom feature, the device can
				automatically answer the Intercom calls

> Multicast

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

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

Key	Туре	Number 1	Number 2	Line	Subtype
DSS Key 1	Multicast 🔹			SIP1 •	G.722
) () (-	A	oply		G.711A G.711U G.722
					G.723.1 G.726-32 G.729AB

Туре	Number	Subtype	Usage
		G.711A	Nerrowhand anosch adding (4Khz)
	Set the host IP address	G.711U	Narrowband speech coding (4Khz)
Multicast	and port number; they must be separated by a colon	G.722	Wideband speech coding (7Khz)
wullicast		G.723.1	
		G.726-32	Narrowband speech coding (4Khz)
		G.729AB	

\diamond operation mechanism

You can define the DSS Key configuration with multicast address, port and used codec. The device can configure via WEB to monitor the multicast address and port. When the device makes a multicast, all devices monitoring the address can receive the multicast data.

♦ calling configuration

If the device is in calls, or it is three-way conference, or initiated multicast communication, the device would not be able to launch a new multicast call.



System		
Network	Tamper Alarm Settings	
ine	Alarm command Tamper_Alarm Reset command Tamper_Reset Reset Alerting Status Reset Ring Type Default 🗸	
GS Setting	Apply	
GS Access	Server Settings	
GS Logs	Server Address Send message to the server when the alarm is triggere Message:Alarm_Info:Description=i23S IP Door Phone;SIP User=5528;Mac=0c:38:3e:1e:61:dd;IP=172.18.2.185;port=Input1	ed
oor Lock	Apply	
unction Key		
Alert		

Field Name	Explanation				
Tamper Alarm	Settings				
Tamper Alarm	When the selection is enabled, the tamper detection enabled				
Alarm	When detected someone tampering the equipment, will be sent alarm to the				
command	corresponding server				
Reset	When the equipment receives the command of reset from server, the				
command	equipment will stop alarm				
Reset Alerting	Directly stop the clarm from equipment in the Webpege				
Status	Directly stop the alarm from equipment in the Webpage				
Ring Type	Set the Ring Type				
Server settings					
Server	Set the Alert measure and condite appointing conver				
Address	Set the Alert message and send to specific server				

E.Appendix

1. Technical parameters

Commun	ommunication protocolSIP 2.0(RFC-3261)	
Main chip	oset	Broadcom
Kovo	DSS Key	1 (Stainless steel)
Keys	Numeric keyboard	Support
	MIC	1
Audio	Speaker	3₩/4Ω
	Volume control	Adjustable



	Full duplex speakerphone	Support (AEC)				
Speech	Protocols	RTP				
flow	Decoding	G.729、G.723、G.711、G.722、G.726				
Ports Active Switched Output WAN		12V/650mA DC				
		10/100BASE-TX s Auto-MDIX, RJ-45				
RFID/IC card reader		EM4100 (125Khz)				
		MIFARE One(13.56Mhz)				
Power supp	oly mode	12V / 1A DC or PoE				
PoE		PoE				
Cables		CAT5 or better				
Shell Mater	ial	Cast aluminium panel, Cast aluminium back shell				
Working ter	mperature	-40°C to 70°C				
Working hu	ımidity	10% - 95%				
Storage temperature		-40°C to 70°C				
Installation	way	Wall mounted or In-wall				
Dimension		Wall mounted: 223*130*74mm				
Dimension		In-wall: 270*150*61mm				
Package size	ze	310x175x115mm				
Equipment	weight	1500g				
Gross weig	ht	1800g				

2. Basic functions

- 2 SIP lines
- PoE Enabled
- Full-duplex speakerphone (HF)
- Numeric keypad (Dial pad or Password input)
- Intelligent DSS Keys (Speed Dial/intercom etc.)
- Wall mounted / In-wall
- Integrated RFID/IC Card reader
- 1 indoor switch interface
- 1 electric lock relay
- Anti-tamper switch
- External power supply
- Door phone: call, password, RFID/IC card, indoor switch
- Protection level: IP65, IK10, CE/FCC



3. Schematic diagram



F. Other instructions

1. Open door modes

- Local
 - ♦ Press indoor switch, which is installed and connected with device, to unlock the

door.

Day Start Time	06:00 (00:00-23:59)	Day End Time	18:00 (00:00-23:59)
Address of Log Server	0.0.0.0	Port of Log Server	514
Enable Log Server	Disable 💌	Enable Indoor Open	Enable 💌
Enable Card Reader	Enable 💌	Limit Talk Duration	Disable Enable
Door Unlock Indication	Long beeps 💌	Remote Access Code Check Length	4 (1~6)
		Apply	



2. Management of card

Add Administrator>>			
ID	0003476384	Add	
Туре	Issuer		
Add Administrator>>			
ID	0003408919	Add	
Туре	Revocation 💙		
Administrator Table>>			
ID	Date		Туре
0003476384	JAN 01 02:09:04		Issuer

JAN 01 02:09:29

Method 1: used to add cards for starters typically

0003408919

Card Reader Working Mode	Card Issuing	
Talk Duration	Normal	0) Second(s
	Card Issuing	o) second(:
Local password	Card Revoking	
		- 5
		1
Card Reader Working Mode	Normal 🔻]
Card Reader Working Mode Talk Duration	Normal	0) Second(s)
		0) Second(s)

Access Table >>

Click here to Save Access Table

Revocation

Tot	al: 2	Pre	v Page: 1	•	Next					0	Dele	ete Dele	te All
	Index	Name	ID	Depart	ment Position	Location Number	Fwd Number	Access Code	Double Auth	Profile	Туре	Issuing Date	Card State
	1	joe	0000127423						Disable	None	Guest	2017/06/29 17:31:23	Enable
	2	zhangsan	0123031310						Disable	None	Guest	2017/06/29 17:30:58	Enable

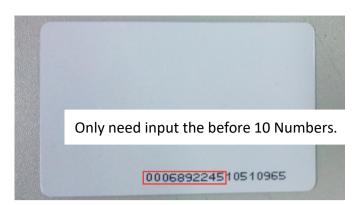
Method 2: used to add cards for professionals

Methods 3: use to add few cards

Name		*	Location		0
ID.		T	Number		
Card State	Enable 🔻		Fwd Number		
Department			Access Code		0
Position			Double Auth	Disable 🔻 🚺	
Гуре	Guest 🔻		Profile	None 🔻	

Note: you can also use the USB card reader connected with PC to get cards ID automatically.





Method 1: used to batch delete cards for starters.

Card Reader Working Mode	Card Revoking 🔻	
Talk Duration	Normal Card Issuing	0) Second(s)
Local password	Card Revoking	
Card Reader Working Mode	Normal	1
Talk Duration	Normal	0) Second(s)
Local password	Card Issuing Card Revoking	0,00000000

Method 2: used to batch add cards for intermediates.

Method 3: use to batch delete cards or delete few cards.

											_		to Save Acce	
Tota	al: 2	Pre	Page: 1		Vext						0	Dele	ete Dele	te All
	Index	Name	ID	Departmen	t Position	Location	Number	Fwd Number	Access Code	Double Auth	Profile	Туре	Issuing Date	Card State
	1	joe	0000127423							Disable	None	Guest	2017/06/29 17:31:23	Enable
	2	zhangsan	0123031310							Disable	None	Guest	2017/06/29 17:30:58	Enabl