

# **SIP Intercom System**

# **Door Phone**

# **DSP9323**



# User Manual

Thank you for using our DSPPA public address system. Please read this User Manual carefully to make better use of this equipment.

# Guangzhou DSPPA Audio Co., Ltd.

http://www.DSPPA.com

http://www.dsppatech.com

# **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.

# Content

I.	PR	ODUCT INTRODUCTION	5
1.	A	APPEARANCE OF THE PRODUCT	5
2.	D	DESCRIPTION	5
II.	STA	ART USING	5
1.	C	CONFIRM THE CONNECTION	6
	1)	Power, Electric Lock, Indoor switch port	6
	2)	Driving mode of electric-lock(Default in active mode)	6
	3)	Wiring instructions	6
2.	Ç	UICK SETTING	7
III.	B	SASIC OPERATION	8
1.	A	ANSWER A CALL	8
2.	C	CALL	8
3.	E	ND CALL	8
4.	C	PPEN THE DOOR OPERATION	8
IV.	Р	PAGE SETTINGS	9
1.	B	ROWSER CONFIGURATION	9
2.	P	ASSWORD CONFIGURATION	9
3.	C	CONFIGURATION VIA WEB	10
	(1)	System	10
	a	) Information	10
	b	) Account	11
	c	) Configurations	12
	d	) Upgrade	12
	e	) Auto Provision	13
	f)	) Tools	14
	(2)	Network	16
	a	) Basic	16
	b	) Advanced	16
	c	·	
	(3)	Line	20
	a	, ,	
	b	,	
	(4)	EGS Setting	
	a	, ,	
	b	,	
	c	·	
	d	) Action URL	33

	<u>SPP</u>	<b>A</b> * *	SIP Intercom System
	e)	Time/Date	
(	5)	EGS Cards	
	a)	EGS Cards	
	b)	EGS ACCESS	
(	6)	EGS Logs	
(	7)	Function Key	
	a)		
<b>V.</b> A	APPI	ENDIX	41
1.	TE	CCHNICAL PARAMETERS	41
2.	BA	ASIC FUNCTIONS	
3.	SCI	THEMATIC DIAGRAM	
VI.	OT	THER INSTRUCTIONS	43
1.	OP	PEN DOOR MODES	
2.	MA	ANAGEMENT OF CARD	

# I. Product introduction

DSP9323 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.

DSP9323 door phone supports entrance guard control, voice intercom, ID card and keypad remote to open the door.

# 1. Appearance of the product



## 2. Description

Buttons and icons	Description	Function
123 456 789 *0#	Numeric keyboard	Input password to open the door or to call.
	programmable keys	Can be set to a variety of functions, in order to meet the needs of different occasions
CARD DATA	induction zone	RFID induction area
	Lock Status	Door unlocking: On
	LOCK Status	Door locking: Off
		Standby: Off
SE 🔵	Call/Ring status	Calls: On
		Ringing: Blink with 1s
		Network error: Blink with 1s
	Network/SIP	Network running: Off
	Registration	Registration failed: Blink with 3s
		Registration succeeded: On

# **II. 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

Door phone the power supply ways: 12v/DC or POE.

1	2	3	4	5	6	7	
+12V	VSS	NC	COM	NO	S_IN	S_OUT	
12V 1A/DC		Elec	tric-lock sv	vitch	Indoor	switch	

### 2) Driving mode of electric-lock(Default in active mode)



Pa	1
assive	(2/)
e Mo	<b>/</b> 3/
ode	4

Active	// /2/
Mode	[ <u>3</u> ] [4]

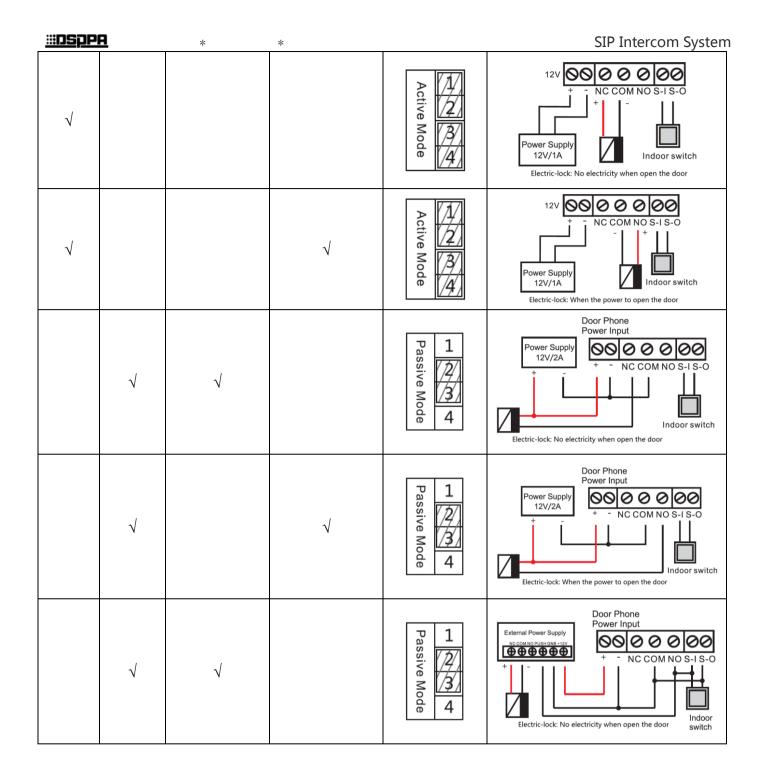
**(Note)** device is in active mode, in easily engree //700mA's with output maximum, to which a standard electric-lock or another compatible electrical appliance can be connected.

- 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

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

Drivin	ng Mode	Electric lock			
Active	Passive	No electricity when open	When the power to open	Jumper port	Connections



### 2. Quick Setting

The product provides a complete function and parameter setting. Users may need to have the network and SIP protocol knowledge to understand the meaning represented by all parameters. In order to let equipment users enjoy the high quality of voice service and low cost advantage brought by the device immediately, here we list some basic but compulsory setting options in this section to let users know how to operate without understanding such complex SIP protocols.

In prior to this step, please make sure your broadband Internet online can be normal operated, and complete the connection of the network hardware. The product factory default network mode is DHCP. Thus, only connect equipment 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

#### <u> III DSPPA</u>

×

"iDoorPhoneNetworkScanner.exe" software to find the IP address of the device.

- > Note: when power on, 30s waiting is needed for device running.
- > Log on 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).

🏦 iDoorPhone Network Scanner(V 1.0)

# IP Address	Serial Number	MAC Address	SW Version	Description	
172.18.2.80	0 DSP9323	00:a8:23:6a:6c:0e	2.0.0.2485	DSP9323 IP Door Phone	
					<u>B</u> efresh

# **III.** Basic operation

### 1. Answer a call

When a call comes in, the device will answer automatically. If you cancel auto answer feature and set auto answer time, you will hear the bell ring at the set time and the device will auto answer after a timeout.

# 2. Call

Configure shortcut key as hot key and setup a number, then press shortcut key can call the configured number.

### 3. End call

Enable Release key hang up to end call.

# 4. Open the door operation

Through the following seven ways to open the door:

- 1) Input password on the keyboard to open the door.
- 2) Access to call the owner and the owner enter the remote password to open the door.
- 3) Owner/other equipment call the access control and enter the access code to open the door. (access code should be included in the list of access configuration, and enable for remote calls to open the door)
- 4) Swipe the RFID cards to open the door.
- 5) By means of indoor switch to open the door.

6) Private access code to open the door.

Enable for local authentication, and set private access code. Input the access code directly under standby mode to open the door. In this way, the door log will record corresponding card number and user name.

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 input error by low-frequency short chirp.

Password input successfully followed by high-frequency sirens sound, while input error is followed by high-frequency short chirp.

When door has been opened, the device will play sirens sound to prompt.

# **IV.** 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.

#### <u> III DSPPA</u>

\*

- Default user with root level:
  - User name: admin
  - Password: admin

#### 10 /

3. Configuration via WEB

# (1) System

# a) Information

	Information	Account	Configurations	Upgrade	Auto Provision	Tools
System	System Informatio	n				
System	Model:		DSP9323			
› Network	Hardware:		2.1			
Network	Software:		2.0.0.2485			
> Line	Uptime:		04:24:57			
< Lille	Last uptime:		00:21:03			
EGS Setting	MEMInfo:		ROM: 0.8/8(M)	RAM: 1.8/	16(M)	
	Network					
› EGS Cards	Network mode	2:	DHCP			
	MAC:		00:a8:23:6a:6c:0e			
EGS Logs	IP:		172.18.2.80			
	Subnet mask:		255.255.0.0			
Function Key	Default gatew	ay:	172.18.1.1			
	SIP Accounts					
	Line 1	N/A	Inactiv	/e		
	Line 2	N/A	Inactiv	/e		

Information							
Field Name	Explanation						
System	Display equipment model, hardware version, software version, uptime, Last uptime and						
Information	MEMinfo.						
Network	Shows the configuration information for WAN port, including connection mode of 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

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	Tools	
System	Change Web And	h					
> Network	Old Passwo New Passwo		word [				
› Line	Confirm Pas	sword:		Apply			
› EGS Setting	Add New User						
› EGS Cards	Username Web Auther	tication Password	[ I				
› EGS Logs	Confirm Pas Privilege	sword		Administrators 🗸			
> Function Key				Add			
	User Accounts						
	Use	er	Privile	ege			
	adm	iin	Administ	rators		Delete	

Account	Account					
Field Name	Explanation					
Change Web Authentication Password						
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	Account	Configurations	Upgrade	Auto Provision	Tools	
System	Export Configura	ations					
> Network	Export comgan		-	_	ations in 'txt' format. ations in 'xml' format.		
> Line	Import Configur	ations					
› EGS Setting			Configuration file:		Select	Import	
› EGS Cards	Reset to factory	defaults	Click the [Res	et] button to reset	the phone to factory o	defaults.	
> EGS Logs			ALL USER'S DA	ATA WILL BE LOST /	AFTER RESET!		
> Function Key							

Configurations					
Field Name	Explanation				
Export	Save the equipment configuration to a txt or xml file. Please note to Right click on				
Configurations	the choice and then choose "Save Link As."				
Import					
Configurations	Browse to the config file, and press Update to load it to the equipment.				
Reset to factory	This will restore 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	Tools
System						
> Network	Software upgrad		nt Software Version:	2.0.0.2485		
› Line		System	n Image File		Select	Upgrade

Upgrade			
Field Name	Explanation		
Software upgrade			
Browse to the firmware, and press Update to load it to the equipment.			

### e) Auto Provision

	Information	Account	Configurations	Upgrade	Auto Provision	Tools	
System	Common Setting	15					
> Network		nfiguration Version					
› Line	General Cor CPE Serial N Authenticat		00100400FV0	2001000000a823	36a6c0e		
> EGS Setting	Authentication Password						
> EGS Cards	Encryption I	nfiguration File Key Provision Informatio	n []				
› EGS Logs	DHCP Option >>						
Function Key	SIP Plug and Play (PnP) >>						
	Static Provision	ing Server >>					
	TR069 >>						
			Apply				

# Auto Provision

Field Name	Explanation
<b>Common Settings</b>	
Current	Show the current config file's version. If the version of configuration downloaded
Configuration	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
Version	it differs from the current configuration
General	Show the common config file's version. If the configuration downloaded and this
Configuration	configuration is the same, the auto provision will stop. If the endpoints confirm the
Version	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	Username for configuration server. Used for FTP/HTTP/HTTPS. If this is blank
Name	the phone will use anonymous
Authentication	Password for configuration server. Used for FTP/HTTP/HTTPS.
Password	
Configuration File	Encryption key for the configuration file
Encryption Key	
General	
Configuration File	Encryption key for common configuration file
Encryption Key	
Save Auto Provision	Save the auto provision username and password in the phone until the server url
Information	changes
<b>DHCP</b> Option	

URL where the phones can request their configuration.Server AddressPnP Server AddressServer PortPnP Server PortTransportation ProtocolPnP Transfer protocol – UDP or TCPUpdate IntervalInterval time for querying PnP server. Default is 1 hour.Static Provisioning ServerServer IP address for auto update. The address can be an IF address or Domain name with subdirectory.	<u> III DSPPA</u>	* * SIP Intercom System							
DHCP option. It may also be disabled.Custom Option ValueCustom option number. Must be from 128 to 254.SIP Plug and Play (PnP)Enable SIP PnPIf 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 AddressPnP Server AddressServer PortPnP Server AddressServer PortPnP Transfer protocol – UDP or TCP ProtocolUpdate IntervalInterval time for querying PnP server. Default is 1 hour.Static Provisioning ServerServer AddressServer AddressServer AddressServer OrtUpdate IntervalInterval time for querying PnP server. Default is 1 hour.Static Provisioning ServerServer AddressServer AddressServer AddressServer Ortiguration file name if this is blank.Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalSpecify the update interval time. Default is 1 hour.1. Disable – no update1. Disable – no update2. Update at time interval – update at periodic update intervalTR069Enable TR069Enable TR069Enable TR069Enable TR069Enable TR069Enable Tot CACS Server URLACS Server URLACS Server URLACS Server URLACS Server URLACS Server URL <td>Option Value</td> <td>The equipment supports configuration from Option 43, Option 66, or a Custom</td>	Option Value	The equipment supports configuration from Option 43, Option 66, or a Custom							
Value       Custom option number. Must be from 128 to 254.         SIP Plug and Play (P=P)         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       PnP Transfer protocol – UDP or TCP         Protocol       Interval time for querying PnP server. Default is 1 hour.         Static Provisioning Server       Set FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.         Configuration File       Specify configuration file name. The equipment will use its MAC ID as the conf 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       2. Update after reboot – update only after reboot.         3. Update at time interval – update at periodic update interval         TR069       Enable/Disable TR069 configuration         ACS Server URL       ACS Server URL.         ACS User       User name for ACS.	Option value	DHCP option. It may also be disabled.							
Value       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       PnP Transfer protocol – UDP or TCP         Protocol       PnP Transfer protocol – UDP or TCP         Server Address       Set FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.         Configuration File       Specify configuration file name. The equipment will use its MAC ID as the conf         Name       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.         Name       1. Disable – no update         2. Update after reboot – update only after reboot.       3. Update at time interval – update at periodic update interval         TBR069       Enable/Disable TR069 configuration         ACS Server URL       ACS Server URL         ACS User       User name for ACS.	Custom Option	Custom option number. Must be from 128 to 254							
Enable SIP PnPIf 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 AddressPnP Server AddressServer PortPnP Server PortTransportation ProtocolPnP Transfer protocol – UDP or TCPUpdate IntervalInterval time for querying PnP server. Default is 1 hour.Static Provisioning ServerSet FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.Configuration File NameSpecify configuration file name. The equipment will use its MAC ID as the conf file name if this is blank.Protocol TypeSpecify the Update interval time. Default is 1 hour.Update IntervalI. Disable – no update0. Update a filer reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server URLACS Server URL.ACS UserUser name for ACS.	Value	Custom option number. Must de nom 126 to 234.							
Enable SIP PnPmulticast 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 AddressPnP Server AddressServer PortPnP Server PortTransportation ProtocolPnP Transfer protocol – UDP or TCPStatic Provisioning ServerSet FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.Server AddressSet FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.Configuration File NameSpecify configuration file name. The equipment will use its MAC ID as the conf file name if this is blank.Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalI. Disable – no update 2. Update after reboot. 3. Update at time interval – update only after reboot. 3. Update at time interval – update at periodic update interval <b>TR069</b> Enable/Disable TR069 configurationACS Server URL ACS Server URLACS Server URL.ACS UserUser name for ACS.	SIP Plug and Play (F	PnP)							
Enable SIP PnPwill reply with a SIP NOTIFY message containing the Auto Provisioning Server URL where the phones can request their configuration.Server AddressPnP Server AddressServer PortPnP Server PortTransportation ProtocolPnP Transfer protocol – UDP or TCPUpdate IntervalInterval time for querying PnP server. Default is 1 hour.Static Provisioning ServerServer AddressSet FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.Configuration File NameSpecify configuration file name. The equipment will use its MAC ID as the conf file name if this is blank.Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalSpecify the oupdate interval time. Default is 1 hour.Lupdate IntervalSpecify the update interval time. Default is 1 hour.Update IntervalUpdate after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server URL ACS Server URLACS Server URL.ACS UserUser name for ACS.		If this is enabled, the equipment will send SIP SUBSCRIBE messages to a							
will reply with a SIP NOTIFY message containing the Auto Provisioning Server URL where the phones can request their configuration.Server AddressPnP Server AddressServer PortPnP Server PortTransportation ProtocolPnP Transfer protocol – UDP or TCPUpdate IntervalInterval time for querying PnP server. Default is 1 hour.Static Provisioning ServerServer AddressSet FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.Configuration File NameSpecify configuration file name. The equipment will use its MAC ID as the config NameProtocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalI. Disable – no update 2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server URL ACS Server URLACS Server URL.ACS UserUser name for ACS.	Enchla CID DuD	multicast address when it boots up. Any SIP server understanding that message							
Server AddressPnP Server AddressServer PortPnP Server PortTransportation ProtocolPnP Transfer protocol – UDP or TCPUpdate IntervalInterval time for querying PnP server. Default is 1 hour.Static Provisioning ServerServer AddressSet FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.Configuration FileSpecify configuration file name. The equipment will use its MAC ID as the conf file name if this is blank.Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalSpecify the update interval time. Default is 1 hour.1. Disable – no update 2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server URLACS Server URLACS UserUser name for ACS.	Enable SIP PhP	will reply with a SIP NOTIFY message containing the Auto Provisioning Server							
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       Set FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.         Server Address       Set FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.         Configuration File       Specify configuration file name. The equipment will use its MAC ID as the conf 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       1. Disable – no update         2. Update after reboot – update only after reboot.       3. Update at time interval – update at periodic update interval         TR069       Enable/Disable TR069 configuration         ACS Server Type       Select Common or CTC ACS Server Type.         ACS Server URL       ACS Server URL.         ACS User       User name for ACS.		URL where the phones can request their configuration.							
Transportation ProtocolPnP Transfer protocol – UDP or TCPUpdate IntervalInterval time for querying PnP server. Default is 1 hour.Static Provisioning S=verServer AddressSet FTP/TFTP/HTTP server IP address for auto update. The address can be an IP address or Domain name with subdirectory.Configuration FileSpecify configuration file name. The equipment will use its MAC ID as the configuration file name if this is blank.Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalSpecify the update interval time. Default is 1 hour.Update Mode2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server URLACS Server URL.ACS UserUser name for ACS.	Server Address	PnP Server Address							
ProtocolPnP Transfer protocol – UDP or TCPProtocolInterval time for querying PnP server. Default is 1 hour.Static Provisioning ServerServer AddressSet FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.Configuration FileSpecify configuration file name. The equipment will use its MAC ID as the conf file name if this is blank.Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalSpecify the update interval time. Default is 1 hour.1. Disable – no update1. Disable – no updateUpdate Mode2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server URLACS Server URL.ACS UserUser name for ACS.	Server Port	PnP Server Port							
ProtocolIntervalUpdate IntervalInterval time for querying PnP server. Default is 1 hour.Static Provisioning ServerServer AddressSet FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.Configuration FileSpecify configuration file name. The equipment will use its MAC ID as the conf file name if this is blank.Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalSpecify the update interval time. Default is 1 hour.1. Disable – no update2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server URLACS Server URL.ACS UserUser name for ACS.	Transportation								
Static Provisioning ServerServer AddressSet FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.Configuration FileSpecify configuration file name. The equipment will use its MAC ID as the conf file name if this is blank.Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalSpecify the update interval time. Default is 1 hour.1. Disable – no update2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server TypeSelect Common or CTC ACS Server Type.ACS UserUser name for ACS.	Protocol	PhP Transfer protocol – UDP or TCP							
Server AddressSet FTP/TFTP/HTTP server IP address for auto update. The address can be an IF address or Domain name with subdirectory.Configuration FileSpecify configuration file name. The equipment will use its MAC ID as the conf file name if this is blank.Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalSpecify the update interval time. Default is 1 hour.1. Disable – no update2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server TypeSelect Common or CTC ACS Server Type.ACS UserUser name for ACS.	Update Interval	Interval time for querying PnP server. Default is 1 hour.							
Server Addressaddress or Domain name with subdirectory.Configuration FileSpecify configuration file name. The equipment will use its MAC ID as the confNamefile name if this is blank.Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalSpecify the update interval time. Default is 1 hour.1. Disable – no update1. Disable – no updateUpdate Mode2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server TypeSelect Common or CTC ACS Server Type.ACS UserUser name for ACS.	Static Provisioning S	Server							
address or Domain name with subdirectory.Configuration FileSpecify configuration file name. The equipment will use its MAC ID as the confNamefile name if this is blank.Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalSpecify the update interval time. Default is 1 hour.Update Mode1. Disable – no update2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server TypeSelect Common or CTC ACS Server Type.ACS UserUser name for ACS.	Comercia Addresse	Set FTP/TFTP/HTTP server IP address for auto update. The address can be an IP							
Namefile name if this is blank.Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalSpecify the update interval time. Default is 1 hour.Lpdate Interval1. Disable – no update2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server TypeSelect Common or CTC ACS Server Type.ACS Server URLACS Server URL.ACS UserUser name for ACS.	Server Address	address or Domain name with subdirectory.							
Protocol TypeSpecify the Protocol type FTP, TFTP or HTTP.Update IntervalSpecify the update interval time. Default is 1 hour.1. Disable – no update1. Disable – no update2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server TypeSelect Common or CTC ACS Server Type.ACS UserUser name for ACS.	Configuration File	Specify configuration file name. The equipment will use its MAC ID as the config							
Update IntervalSpecify the update interval time. Default is 1 hour.I. Disable – no updateUpdate Mode2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable TR069Enable/Disable TR069 configurationACS Server TypeSelect Common or CTC ACS Server Type.ACS Server URLACS UserUser name for ACS.	Name	file name if this is blank.							
Image: Constraint of the constra	Protocol Type	Specify the Protocol type FTP, TFTP or HTTP.							
Update Mode2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update intervalTR069Enable/Disable TR069 configurationACS Server TypeSelect Common or CTC ACS Server Type.ACS Server URLACS Server URL.ACS UserUser name for ACS.	Update Interval	Specify the update interval time. Default is 1 hour.							
3. Update at time interval – update at periodic update intervalTR069Enable TR069Enable/Disable TR069 configurationACS Server TypeSelect Common or CTC ACS Server Type.ACS Server URLACS Server URL.ACS UserUser name for ACS.		1. Disable – no update							
TR069Enable TR069Enable/Disable TR069 configurationACS Server TypeSelect Common or CTC ACS Server Type.ACS Server URLACS Server URL.ACS UserUser name for ACS.	Update Mode	2. Update after reboot – update only after reboot.							
Enable TR069Enable/Disable TR069 configurationACS Server TypeSelect Common or CTC ACS Server Type.ACS Server URLACS Server URL.ACS UserUser name for ACS.		3. Update at time interval – update at periodic update interval							
ACS Server TypeSelect Common or CTC ACS Server Type.ACS Server URLACS Server URL.ACS UserUser name for ACS.	TR069								
ACS Server URL     ACS Server URL.       ACS User     User name for ACS.	Enable TR069	Enable/Disable TR069 configuration							
ACS User 1 User name for ACS.	ACS Server Type	Select Common or CTC ACS Server Type.							
	ACS Server URL	ACS Server URL.							
ACS Password ACS Password.	ACS User	User name for ACS.							
	ACS Password	ACS Password.							
TR069 Auto Login Enable/Disable TR069 Auto Login.	TR069 Auto Login	Enable/Disable TR069 Auto Login.							
INFORM Sending									
Period Time between transmissions of "Inform" Unit is seconds.	-	I ime between transmissions of "Inform" Unit is seconds.							

# f) Tools

<u> III DSPPA</u>	*	*				SIP Inter	com System
	Information	Account	Configurations	Upgrade	Auto Provision	Tools	
System							
› Network	<b>Syslog</b> Enable Sysl	og					
> Line	Server Addı Server Port		0.0.0.0				
› EGS Setting	APP Log Lev SIP Log Lev		None	~			
› EGS Cards			Apply				
› EGS Logs	Network Packet	s Capture	Start				
Function Key	Reboot Phone						
			Click [Reboot] Reboot	button to restart f	the phone!		

Syslog is a protocol used to record log messages using a client/server mechanism. 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 Syslog	Enable or disable system log.			
Server Address	System log server IP address.			
Server Port	System log server port.			
APP Log Level	Set the level of APP log.			
SIP Log Level	Set the level of SIP log.			
Network Packets Capture				
Capture a packet stream from the equipment. This is normally used to troubleshoot problems.				
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

	Basic Advanced	VPN		
› System				
Network	Network Status			
Network	IP:	172.18.2.80		
> Line	Subnet mask:	255.255.0.0		
? Line	Default gateway:	172.18.1.1		
. 500 C-W	MAC:	00:a8:23:6a:6c:0e		
› EGS Setting	MAC Timestamp	20160722		
› EGS Cards	Settings			
	Static IP 🔘	DHCP 🖲	PPPoe O	
> EGS Logs	DNS Server Configured by	DHCP		
	Primary DNS Server	172.18.1.1		
Function Key	Secondary DNS Server	0.0.0.0		
		Apply		

Field Name	Explanation						
Network Status	Network Status						
IP	The current IP address of the equipment						
Subnet mask	The current Subnet Mask						
Default gateway	The current Gateway IP address						
MAC	The MAC address of the equipment						
MAC	Get the MAC address of time.						
Timestamp	Get the MAC address of thile.						
Settings							
Select the appropri	iate network mode. The equipment supports three network modes:						
Static IP	Network parameters must be entered manually and will not change. All parameters are						
Static IP	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 chosen	sen, the screen below will appear. Enter values provided by the ISP.						
DNS Server	Select the Configured mode of the DNS Server.						
Configured by	Select the Configured mode of the DNS Server.						
Primary DNS	Enter the server address of the Primary DNS.						
Server	Enter the server address of the Frindary D145.						
Secondary DNS	Enter the server address of the Secondary DNS.						
Server Enter the server address of the Secondary DNS.							
After entering the	new settings, click the APPLY button. 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.							

### b) Advanced

#### <u> #OSppa</u>

The equipment supports 802.1Q/P protocol and DiffServ configuration. VLAN function can support the different VLAN ID mode of processing in the WAN port and LAN port.

Chart 1 shows a network switch with no VLAN. Any broadcast frames will be transmitted to all other ports. For example, frames broadcast from Port 1 will be sent to Ports 2, 3, and 4.

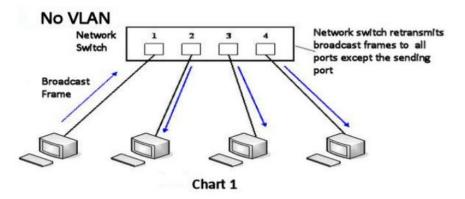
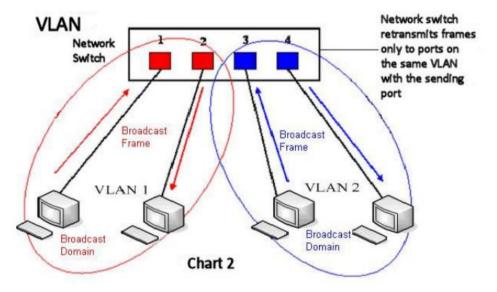


Chart 2 shows an example with two VLANs indicated by red and blue. In this example, frames broadcast from Port 1 will only go to Port 2 since Ports 3 and 4 are in a different VLAN. VLANs can be used to divide a network by restricting the transmission of broadcast frames.



Note: In practice, VLANs are distinguished by the use of VLAN IDs.

<u> III DSPPA</u>	*	*			SIP Intercom System
	Basic	Advanced	VPN		
› System	Enable I			Packet Interval(1~3600)	60 Second(s)
Network	Enable I VLAN Setting	Learning Function			
> Line	Enable 802.1p	, VLAN Signal Priority	0 (0~7)	VLAN ID 802.1p Media Priority	256 (0~4095) 0 (0~7)
› EGS Setting		ervice (QoS) Settin		,	
› EGS Cards		DSCP QoS oS Priority	✓ 46 (0~63)	Signal QoS Priority	46 (0~63)
› EGS Logs	802.1X Setti	-	_		
Function Key	Enable 8 Usernar Passwo	ne	admin	]	
			[	Apply	
	HTTPS Certi	fication File: https.p	pem N/A	Upload Delete	

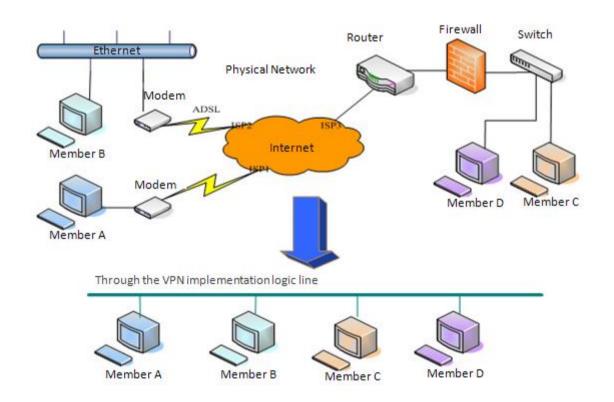
Advanced				
Field Name	Explanation			
Link Layer Discovery Pr	rotocol (LLDP) Settings			
Enable LLDP	Enable or Disable Link Layer Discovery Protocol (LLDP)			
	Enables the telephone to synchronize its VLAN data with the Network			
Enable Learning	Switch. The telephone will automatically synchronize DSCP, 802.1p, and			
Function	VLAN ID values even if these values differ from those provided by the			
	LLDP server.			
Packet Interval(1~3600)	The time interval for sending LLDP Packets			
VLAN Settings				
Enable VLAN	Enable or Disable WAN Port VLAN			
VLAN ID	Specify the value of the VLAN ID. Range is 0-4095			
802.1p Signal Priority	Specify the value of the signal 802.1p priority. Range is 0-7			
802.1p Media Priority	Specify the value of the voice 802.1p priority. Range is 0-7			
Quality of Service (QoS)	Quality of Service (QoS) Settings			
Enable DSCP QoS	Enable or Disable Differentiated Services Code Point (DSCP)			
Media QoS Priority	Specify the value of the Media DSCP in decimal			
Signal QoS Priority	Specify the value of the Signal DSCP in decimal			

802.1X Settings

<u>#DSppa</u> *	*	SIP Intercom System
802.1X Settings		
Enable 802.1X		
Username	admin	
Password	••••	
		Apply
Enable 802.1X	Enable or Disable 812.1X	
Username	802.1X user account	
Password	802.1X password	
HTTPS Certification File	e	
Upload or delete HTTPS (	Certification File	

### c) VPN

The device supports remote connection via VPN. It supports both Layer 2 Tunneling Protocol (L2TP) and OpenVPN protocol. This allows users at remote locations on the public network to make secure connections to local networks.



Basic       Advanced       VPN         > System       Virtual Private Network (VPN) Status <ul> <li>VPN IP Address:</li> <li>0.0.0</li> </ul> Network       VPN Mode       Enable VPN       L2TP       OpenVPN O         > EGS Setting       Layer 2 Tunneling Protocol (L2TP)         L2TP Server Address               Authentication Name             Authentication Password	<u> III DSPPA</u>	*	*			SIP Intercom System
> System VPN IP Address: 0.0.0   Network VPN Mode   > Line		Basic	Advanced	VPN		
Network       VPN Mode         Line       Layer 2 Tunneling Protocol (L2TP)         EGS Setting       Layer 2 Tunneling Protocol (L2TP)         EGS Cards       Authentication Name         EGS Logs       Authentication Password         Function Key       OpenVPN Files         OpenVPN Configuration file: client.ovpn       N/A         Upload       Delete         Client Certification:       ca.crt       N/A         Upload       Delete		Virtual Privat	e Network (VPN) Status			
Line Layer 2 Tunneling Protocol (L2TP)   EGS Setting Layer 2 Tunneling Protocol (L2TP)   EGS Cards L2TP Server Address   Authentication Name   Authentication Password     Function Key     OpenVPN Configuration file: client.ovpn     N/A   Upload   Delete   Client Certification:   client.crt	› System		VPN IP	Address:	0.0.0.0	
Line LZTP O OpenVPN O   LGS Setting Layer 2 Tunneling Protocol (L2TP)   LGS Cards LZTP Server Address   Authentication Name   Authentication Password   Function Key   OpenVPN Files   OpenVPN Configuration file: client.ovpn   N/A   Upload   Delete   Client Certification:   client.ort	Network	VPN Mode				
<ul> <li>EGS Setting</li> <li>EGS Cards</li> <li>EGS Logs</li> <li>Function Key</li> <li>OpenVPN Files</li> <li>OpenVPN Configuration file: client.ovpn N/A Upload Delete</li> <li>CA Root Certification: ca.crt N/A Upload Delete</li> <li>Client Certification: client.ort N/A Upload Delete</li> </ul>			Enable	VPN		
<ul> <li>EGS Cards</li> <li>EGS Logs</li> <li>Function Key</li> <li>CopenVPN Files</li> <li>OpenVPN Configuration file: client.ovpn N/A Upload Delete</li> <li>CA Root Certification: ca.crt N/A Upload Delete</li> <li>Client Certification: client.ort N/A Upload Delete</li> </ul>	› Line		L2TP C	)	OpenVPN O	
> EGS Cards   > EGS Logs   > Function Key     OpenVPN Files   OpenVPN Configuration file: client.ovpn   N/A   Upload   Delete   CA Root Certification:   ca.crt   N/A   Upload   Delete   Client Certification:   client.crt   N/A   Upload   Delete	› EGS Setting	Layer 2 Tunn	eling Protocol (L2TP)			
<ul> <li>&gt; EGS Logs</li> <li>&gt; Function Key</li> <li>Authentication Password</li> <li>Apply</li> <li>OpenVPN Files</li> <li>OpenVPN Configuration file: client.ovpn N/A Upload Delete</li> <li>CA Root Certification: ca.crt N/A Upload Delete</li> <li>Client Certification: client.ort N/A Upload Delete</li> </ul>			L2TP Se	rver Address		
<ul> <li>&gt; EGS Logs</li> <li>&gt; Function Key</li> <li>Apply</li> <li>OpenVPN Files</li> <li>OpenVPN Configuration file: client.ovpn N/A Upload Delete</li> <li>CA Root Certification: ca.crt N/A Upload Delete</li> <li>Client Certification: client.crt N/A Upload Delete</li> </ul>	> EGS Cards					
Function Key       OpenVPN Files         OpenVPN Configuration file: client.ovpn       N/A       Upload       Delete         CA Root Certification:       ca.crt       N/A       Upload       Delete         Client Certification:       client.crt       N/A       Upload       Delete	> EGS Logs		Authent	ication Password		
Function Key       OpenVPN Files         OpenVPN Configuration file: client.ovpn       N/A       Upload       Delete         CA Root Certification:       ca.crt       N/A       Upload       Delete         Client Certification:       client.crt       N/A       Upload       Delete					Apply	
OpenVPN Configuration file: client.ovpnN/AUploadDeleteCA Root Certification:ca.crtN/AUploadDeleteClient Certification:client.crtN/AUploadDelete	Function Key					
CA Root Certification:     ca.crt     N/A     Upload     Delete       Client Certification:     client.crt     N/A     Upload     Delete		OpenVPN File	25			
Client Certification: client.crt N/A Upload Delete		OpenVPN	V Configuration file: client.ovp	n N/A	Upload Dele	ete
		CA Root	Certification: ca.crt	N/A	Upload Dele	ete
Client Key: client.key N/A Upload Delete		Client Ce	ertification: client.crt	N/A	Upload Dele	ete
		Client Ke	ey: client.key	N/A	Upload Dele	ete

Field Name	Explanation
VPN IP Address	Shows the current VPN IP address.
VPN Mode	
Enable VPN	Enable/Disable VPN.
L2TP	Select Layer 2 Tunneling Protocol
OpenVDN	Select OpenVPN Protocol. (Only one protocol may be activated. After the selection
OpenVPN	is made, the configuration should be saved and the phone be rebooted.)
Layer 2 Tunneling	g Protocol (L2TP)
L2TP Server	Set VPN L2TP Server IP address.
Address	Set VFIN L21F Server IF address.
Authentication	Set User Name access to VPN L2TP Server.
Name	Set User Manie access to VFIN L21F Server.
Authentication	Set Password access to VPN L2TP Server.
Password	Set Password access to VPN L21P Server.
<b>Open VPN Files</b>	
Upload or delete O	pen VPN Certification Files

# (3) Line

# a) SIP

Configure a SIP server on this page.

<u> III DSPPA</u>	* *	*			SIP In	tercom System
	SIP	Basic Settings				
› System						
, system						
> Network	Line Basic Settings >>	SIP 1 🗸				
Line	Line Status	Registere	ed	SIP Proxy Server Addre	ss 172.18.1.8	8
	Username	8207		SIP Proxy Server Port	5060	
› EGS Setting	Display name Authentication	8207 Name 8207		Outbound proxy add. Outbound proxy port		
› EGS Cards	Authentication			Realm		
	Activate					
> EGS Logs	Codecs Settings >>	<b>&gt;</b>				
Function Key	Advanced Settings	>>				
· · · · · · · · · · · · · · · · · · ·		Apply				
Codecs Settings >>						
Disabled Codecs			Enabled Codece	S		
	$\land \rightarrow$		G.722 G.711U	$\uparrow$ $\uparrow$		
	. ←		G.711A G.729AB	_ ↓		
			0.725AD			
Advanced Settings >>						
Call Forward Unconditio	nal 🗌		Enable Auto	Answering		
Call Forward Number fo Unconditional	r		Auto Answe	ring Delay	5	Second(s)
Call Forward on Busy			Subscribe Fo	or Voice Message		
Call Forward Number fo	r Busy		Voice Messa	ge Number		
Call Forward on No Ans	wer		Voice Messa Period	ge Subscribe	3600	Second(s)
Call Forward Number fo Answer	r No					
Call Forward Delay for N Answer		Second(s)	Enable Hotli	ne		
Hotline Delay	0		s) Hotline Num	ber		
Enable DND			Ring Type		Default 🗸	
Blocking Anonymous Ca			Conference	Туре	Local 🗸	
Use 182 Response for C waiting			Server Conf	erence Number		
Anonymous Call Standa	rd None	~	Transfer Tim	eout	0	Second(s)
Dial Without Registered			Enable Long	) Contact		
Click To Talk			Enable Use	Inactive Hold		
User Agent			Enable Miss	ed Call Log		
Use Quote in Display Na	ame 🗌		Response Si	ingle Codec		

<u> #DS</u>	<u>67PA</u>	*	*		SIP Intercom System
	Use Feature Code				
E	Enable DND			DND Disabled	
-	Enable Call Forward Unconditional			Disable Call Forward Unconditional	
E	Enable Call Forward on	Busy		Disable Call Forward on Busy	
	Enable Call Forward on Answer	No		Disable Call Forward on No Answer	
	Enable Blocking Anonym Call	ious		Disable Blocking Anonymous Call	
5	Specific Server Type		COMMON ~	Enable DNS SRV	
F	Registration Expiration		60 Second(s)	Keep Alive Type	UDP 🗸
	Use VPN		$\checkmark$	Keep Alive Interval	30 Second(s)
, i	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	
1	Transportation Protocol		UDP 🗸	Enable PRACK	
9	SIP Version		RFC3261 🗸	Keep Authentication	
(	Caller ID Header		FROM	Auto TCP	
I	Enable Strict Proxy			Enable Feature Sync	
I	Enable user=phone			Enable GRUU	
1	Enable SCA			BLF Server	
I	Enable BLF List			BLF List Number	
	SIP Encryption			RTP Encryption	
	SIP Encryption Key			RTP Encryption Key	
:	эте спотурион кеу		Apply	KIP EIGYPUOIT KEY	

SIP	SIP			
Field Name	Explanation			
Basic Settings (Choose t	the SIP line to configured)			
Line Status	Display the current line status at page loading. To get the up to date line status,			
Line Status	user has to refresh the page manually.			
Username	Enter the username of the service account.			
Display name	Enter the display name to be sent in a call request.			
Authentication Name	Enter the authentication name of the service account			
Authentication	Enter the authentication password of the service account			
Password	Enter the authentication password of the service account			
Activate	Whether the service of the line should be activated			
SIP Proxy Server	Enter the IP or FQDN address of the SIP proxy server			
Address	Enter the IP of 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 provided by the service			
address	provider			
Outbound proxy port	Enter the outbound proxy port, default is 5060			

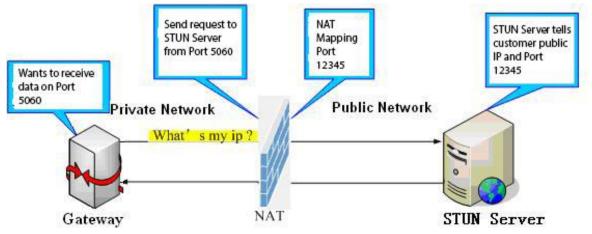
<u>IIIDSPPA</u> .	* * SIP Intercom System		
Realm	Enter the SIP domain if requested by the service provider		
<b>Codecs Settings</b>			
Set the priority and availa	ability of the codecs by adding or remove them from the list.		
Advanced Settings			
Call Forward	Enable unconditional call forward, all incoming calls will be forwarded to the		
Unconditional	number specified in the next field		
Call Forward Number			
for Unconditional	Set the number of unconditional call forward		
Call Farmer al car Deces	Enable call forward on busy, when the phone is busy, any incoming call will be		
Call Forward on Busy	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	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		
Answer	specified in the next field		
Call Forward Number	Set the number of call forward on no answer		
for No Answer			
Call Forward Delay for	Set the delay time of not answered call before being forwarded		
No Answer	Set the delay time of not answered can before being forwarded		
Hotline Delay	Set the delay for hotline before the system automatically dialed it		
Enable Auto Answering	Enable auto-answering, the incoming calls will be answered automatically after		
Eliable Auto Aliswering	the delay time		
Auto Answering Delay	Set the delay for incoming call before the system automatically answered it		
Subscribe For Voice	Enable the device to subscribe a voice message waiting notification, if enabled,		
Message	the device will receive notification from the server if there is voice message		
Wiessage	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 configuration, the device will dial to the specific number		
Enable Hotline			
Hotline Number			
Enable DND			
Blocking Anonymous			
Call	Reject any incoming call without presenting caller ID		
-	Set the device to use 182 response code at call waiting response		
Anonymous Call			
Standard	Set the standard to be used for anonymous		
Subscribe Period Enable Hotline Hotline Number Enable DND Blocking Anonymous Call Use 182 Response for Call waiting Anonymous Call	Set the interval of voice message notification subscription Enable hotline configuration, the device will dial to the specific nur immediately at audio channel opened by off-hook handset or turn on hands- speaker or headphone Set the hotline dialing number Enable Do-not-disturb, any incoming call to this line will be rejected automatically Reject any incoming call without presenting caller ID Set the device to use 182 response code at call waiting response Set the standard to be used for anonymous		

<u>IIIDSPPA</u> ,	* * SIP Intercom System
Dial Without	Set call out by proxy without registration
Registered	Set can but by proxy without registration
Click To Talk	Set Click To Talk
User Agent	Set the user agent, the default is Model with Software Version.
Use Quote in Display Name	Whether to add quote in display name
Ring Type	Set the ring tone type for the line
0 11	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
51	dialing to a conference room on the server
Server Conference Number	Set the conference room number when conference type is set to be Server
Transfer Timeout	Set the timeout of call transfer process
Enable Long Contact	Allow more parameters in contact field per RFC 3840
Enable Missed Call Log	If enabled, the phone will save missed calls into the call history record.
	If setting enabled, the device will use single codec in response to an incoming
Response Single Codec	call request
	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
Use Feature Code	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 Protocol	Set the line to use TCP or UDP for SIP transmission
SIP Version	Set the SIP version
Caller ID Header	Set the Caller ID Header
Enchla Strict Drover	Enables the use of strict routing. When the phone receives packets from the
Enable Strict Proxy	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 BLF List	Enable/Disable BLF List
Eachia DNG CDV	Set the line to use DNS SRV which will resolve the FQDN in proxy server into
Enable DNS SRV	a service list
Voor Aline True	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole
Keep Alive Type	opened
	Set the keep alive packet transmitting interval

<u> III DSPPA</u>	* * SIP Intercom System
	Set the line to enable call ending by session timer refreshment. The call session
Enable Session Timer	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
Keep Authentication	Keep the authentication parameters from previous authentication
Auto TCP	Using TCP protocol to guarantee usability of transport for SIP messages above
Auto ICP	1500 bytes
Enable Feature Sync	Feature Sycn with server
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)
	The registered server will receive the subscription package from ordinary
BLF Server	application of BLF phone.
DLI SCIVCI	Please enter the BLF server, if the sever does not support subscription package,
	the registered server and subscription server will be separated.
BLF List Number	BLF List allows one BLF key to monitor the status of a group. Multiple BLF
BLF List Nulliber	lists are supported.
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

### 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.



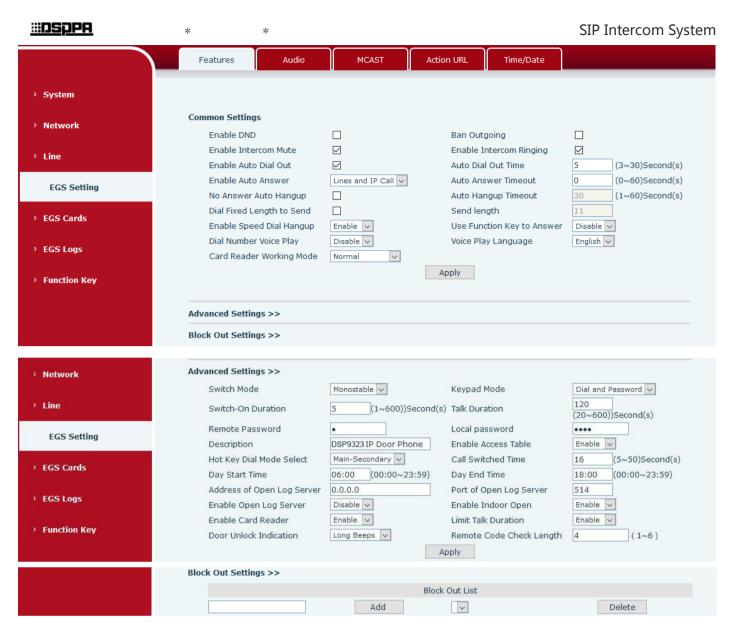
<u> III DSPPA</u>	* *		SIP Intercom System
	SIP Basic Settings		
› System	SIP Settings		
> Network	Local SIP Port Registration Failure Retry Interv	5060       val     32       Second(s)	
Line	STUN Settings		
› EGS Setting	Server Address Server Port Binding Period	3478 50 Second(s)	
› EGS Cards	SIP Waiting Time	800 millisecond	
› EGS Logs	SIP Line Using STUN	Apply	
› Function Key	Use STUN	SIP 1	
	TLS Certification File: sips.pem	N/A Upload Delete	

Basic Settings					
Field Name	Explanation				
SIP Settings					
Local SIP Port	Set the local SIP port used to send/receive SIP messages.				
<b>Registration Failure</b>	Set the retry interval of SIP REGISTRATION when registration failed.				
Retry Interval	Set the fetry interval of SIF REOISTRATION when registration failed.				
STUN Settings					
Server Address	STUN Server IP address				
Server Port	STUN Server Port – Default is 3478.				
Dinding Daried	STUN blinding period – STUN packets are sent at this interval to keep the NAT				
Binding Period	mapping active.				
SIP Waiting Time	Waiting time for SIP. This will vary depending on the network.				
SIP Line Using STUN	N(SIP1 or SIP2)				
Use STUN	Enable/Disable STUN on the selected line.				
TLS Certification Fil	e				
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, is the realization of a service, when the					

equipment 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.

### (4) EGS Setting

a) Features



Features					
Field Name	Explanation				
<b>Common Settings</b>					
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	If analysis, intersom ring tong to short to an intersom call				
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				

<u> III DSPPA</u>	* * SIP Intercom System					
Dial Fixed Length to	Enable or disable dial fixed length to send.					
Send	Enable of disable dial fixed length to send.					
Send length	The number will be sent to the server after the specified numbers of digits are					
Send length	dialed.					
Enable Speed Dial	Enable Speed Diel Hand Up function					
Hangup	Enable Speed Dial Hand Up function					
Use Function Key to	Configure whether to enable the function have is disabled by default					
Answer	Configure whether to enable the function keys, is disabled by default.					
Dial Number Voice	Carfierentian Onen (Class Dial Namber Vaire Dian					
Play	Configuration Open / Close Dial Number Voice Play					
Voice Play Language	Set language of the voice prompt					
	Set ID card stats:					
Cand Daadan Warking	Normal: This is the work mode, after the slot card can to open the door.					
Card Reader Working	Card Issuing: This is the issuing mode, after the slot card can to add ID cards.					
Mode	Card Revoking: This is the revoking mode, after the slot card can to delete ID					
	cards.					

Field Name	Explanation			
Advanced Settings				
	Monostable: there is only one fixed action status for door unlocking.			
	Bistable: there are two actions and statuses, door unlocking and door locking.			
Switch Mode	Each action might be triggered and changed to the other status. After changed,			
	the status would be kept.			
	Initial Value is Monostable			
	Password+dialing: password input is default. Dialing mode is as below if you			
	want.			
Keypad Mode	Only password: password input only, dialing would be forbidden.			
	Only dialing: dial input only, * Key to enter the dial, the # key to hang up.			
	Initial Value is Password and dialing.			
Switch-On Duration	Door unlocking time for Monostable mode only. If the time is up, the door			
Switch-On Duration	would be locked automatically. Initial Value is 5 seconds.			
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 pageword	Local door unlocking password via keypad, the default password length is 4.			
Local password	Initial Value is "6789".			
Description	Device description displayed on IP scanning tool software. Initial Value is			
Description	"DSP9323 IP Door Phone".			
	Enable Access Table: enter <access code=""> for opening door during calls.</access>			
Enable Access Table	Disable Access Table: enter <remote password=""> for opening door during calls.</remote>			
	Default Enable.			

<u>#DSPPA</u> ,	* * SIP Intercom System					
	<primary secondary="">mode allow system to call primary extension first, if</primary>					
	there were no answer, it would cancel the call and then call secondary					
Hot Key Dial Mode	extension automatically.					
Select	<day night="">mode allow system to check the calling time is belong to Day or</day>					
	Night time, and then decide to call the number 1 or number 2 automatically.					
	Users just press speed dial key once.					
Call Switched Time	The period between hot key dialing to the first and second number. Initial Value					
Call Switched Time	is 16 seconds.					
Day Start Time	The start time of the Day When you select <day night="">mode.</day>					
Day End Time	The end time of the day When you select <day night="">mode.</day>					
Address of Open Log	Log server address(IP or domain name)					
Server	og server address(IP or domain name)					
Port of Open Log	Log server port (0-65535), Initial Value is 514.					
Server	Log server port (0-05555), mittar value is 514.					
Enable Open Log	Enable or disable to connect with log server					
Server	Enable of disable to connect with log server					
Enable Indoor Open	Enable or disable to use indoor switch to unlock the door.					
Enable Card Reader	Enable or disable card reader for RFID cards.					
Limit Talk Duration	If enabled, calls would be forced ended after talking time is up.					
Door Unlock Indication	Indication tone for door unlocked. There are 3 type of tone: silent/short					
Door Uniock Indication	beeps/long beeps.					
Remote Code Check	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					
Length	Value is 4.					
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 will not dial any numbers beginning with 001.

X and x are wildcards which match single digits. For example, if 4xxx or 4XXX is entered, the phone will not dial any 4 digit numbers beginning with 4. It will 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.

<u> IIIDSPPA</u>	* *			SIP Intercom System
	Features Audio	MCAST Act	ion URL Time/Date	
› System				
› Network	Audio Settings First Codec	G.722	Second Codec	G.711A 🗸
› Line	Third Codec Fifth Codec	G.711U V None V	Fourth Codec Sixth Codec	G.729AB \
EGS Setting	DTMF Payload Type G.729AB Payload Length	101 (96~127) 20ms 🗸	Default Ring Type Tone Standard	Type 1 V United Stav
› EGS Cards	G.722 Timestamps Speakerphone Volume	160/20ms v 5 (1~9)	G.723.1 Bit Rate MIC Input Volume	6.3kb/s 🗸 5 (1~9)
› EGS Logs	Broadcast Output Volume Enable VAD	5 (1~9)	Signal Tone Volume	4 (0~9)
› Function Key		Apply		

Audio Setting							
Field Name I	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						
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.						
G.729AB Payload Length G.729AB Payload Length – Adjusts from 10 – 60 mSec.							
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	e Set the MIC calls the volume level.						
Broadcast Output	Set the broadcast the output volume level						
Volume     Set the broadcast the output volume level.							
Signal Tone	Set the audio signal the output volume level.						
Volume							
Enable VAD	Enable or disable Voice Activity Detection (VAD). If VAD is enabled, G729						
	Payload length cannot be set greater than 20 mSec.						

# c) MCAST

<u> III DSPPA</u>	* *		SIP Int	ercom System
	Features Audio	MCAST Action URL	Time/Date	
> System				
> Network	MCAST Settings Priority	1		
> Line	Enable Page Priority Index/Priority	Name	Host:port	
EGS Setting	1 2			
› EGS Cards	3 4			
› EGS Logs	5			
› Function Key	7 8			
	9 10			
		Apply		

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.

#### **MCAST Settings**

Equipment can be set up to monitor up to 10 different multicast addresses, 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.

#### <u> IIISPPA</u>

\*

\*

#### • Web Settings:

MCA	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.

#### Listener configuration

ST Settings		
Priority	3 🗸	
Enable 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:

- ☆ The purpose of setting monitoring multicast "Group 1" or "Group 2" or "Group 3" launched a multicast call.
- $\diamond$  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.

#### SIP Intercom System

#### 

♦ 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.
- **Lmonitor:** IP port and priority configuration monitoring device, when the call is initiated and incoming multicast, directly into the Talking interface equipment.

### d) Action URL

	Features	Audio	MCAST	Action URL	Time/Date
	Action URL Event S	ettings			
> System	Active URI Limit	t IP			
	Setup Complet	ed			
> Network	Registration Su	ucceeded			
	Registration Di	sabled			
> Line	Registration Fa	iled			
	Off Hooked				
EGS Setting	On Hooked				
	Incoming Call				
EGS Cards	Outgoing calls				
	Call Established				
> EGS Logs	Call Terminated	ł			
	DND Enabled				
Function Key	DND Disabled				
	Mute				
	Unmute				
	Missed calls				
	IP Changed				
	Idle To Busy				

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

\*

# e) Time/Date

	Features	Audio	MCAST	Action URL	Time/Date	
> System	Network Time S	-	_			
		onized via SNTP				
> Network		onized via DHCP				
	Primary Tim		time.nist.gov			
› Line	Secondary 1 Time zone	nme Server	pool.ntp.org	a,Singapore,Austra		
	Resync Peri	od	60		0)Second(s)	
EGS Setting	Resync Pen	ou	00	(1~500	0)Second(s)	
	Date Format					
EGS Cards	12-hour clo	ck				
	Date Forma	t	1 JAN MON	$\sim$		
EGS Logs						
			Apply			
Function Key						
> Network						
	Daylight Saving T	ime Settings				
> Line	Location		China(Beijing)	$\sim$		
	DST Set Type		Automatic	$\sim$		
EGS Setting	Fixed Type		Disabled	$\sim$		
	Offset		0	Minute		
EGS Cards			Start		End	
	Month		January	$\sim$	January	~
EGS Logs	Week		1	$\sim$	1	~
	Weekday		Sunday	~	Sunday	~
Function Key	Hour		0	$\sim$	0	~
			Apply			
	Manual Time Setti	ings				
	2016-08-17	-	× 41 ×	Apply		
	2010-03-17		41 4	עיקקא		

Time/Date				
Field Name	Explanation			
Network Time Server	Settings			
Time Synchronized	Enable time sure through SNTP protocol			
via SNTP	ble time-sync through SNTP protocol			
Time Synchronized	Enable time-sync through DHCP protocol			
via DHCP	Enable time-sync through DHCF protocol			
Primary Time Server	Set primary time server address			
Secondary Time	Set secondary time server address, when primary server is not reachable, the device will try			
Server	to connect to secondary time server to get time synchronization.			
Time zone	Select the time zone			

<u> III DSPPA</u>	* *	SIP Intercom System
Resync Period	Time of re-synchronization with time server	
Date Format		
12-hour clock	Set the time display in 12-hour mode	
Date Format	Select the time/date display format	
Daylight Saving Time	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 n	nanually 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		
The time set by hand, n	eed to disable SNTP service first.	

# (5) EGS Cards

### a) EGS Cards

	EGS CARDS EGS ACCESS
› System	
› Network	Import Door Card Table     Browse     (doorCard.csv)     Update
> Line	Door Card Table >>
› EGS Setting	Add Door Card     Add     Click here to Save Door Card Table       Index     Name     ID     Issuing Date     Card State
EGS Cards	Total: 0 Prev Page: v Next Oelete All
	Administrator Table >>
› EGS Logs	Add Admin Card Issuer V Add
	Index ID Issuing Date Type
Function Key	Total: 0 Prev Page: V Next Oelete All

EGS Cards						
Field Name	xplanation					
Import Door Card	Table					
Click the <browse></browse>	> to choose to import door card list file (doorCard.csv), click <update> can be batch</update>					
import.						
Door Card Table						
Add Door Card	The input RFID card numbers the top 10, for example, 0004111806, click <add>.</add>					
Click here to	<u>Click here to Save Door Card Table</u> Right-click it and select save target to your					

<u> IIIDSPPA</u>	* * SIP Intercom System
Save Door Card	computer.
Table	
Name	The name of has been issuer cards.
ID	The card number of has been issuer cards.
	(Note: The card is not registered in the remote access list is unable to open the door.)
Issuing Date	The issuing date of has been issuer cards.
Card State	To have been issuer cards the state.
Delete	Click <delete>, will delete the door card list within the selected ID cards.</delete>
Delete All	Click <delete all="">, to delete all door card lists.</delete>
Administrator Tal	ble
Add Admin Card	The input RFID card numbers the top 10, for example, 0004111806, select admin
Add Admin Cald	card the type, click <add>.</add>
Type: Issuer and Re	evoking.
Entrance guard in r	ormal state, brush card(issuing card) entrance guard into the issuing state, and then
brush to add a card	the card is added to the database, add swipe again after card(issuing card) entrance
guard returned to n	ormal. Delete card operation and issuing card the same.
Can release at most	10 cards, 500 copies of ordinary cards.
Note: in the issuing	state to delete brush card is invalid, and vice versa.
The show admin ca	rd the ID, Date and Type.
Delete	Click <delete>, will delete the admin card list within the selected ID cards.</delete>
All Delete	Click <delete all="">, to delete all admin card lists.</delete>

# b) EGS ACCESS

<u> III DSPPA</u>	* * SIP Intercom Syste
	EGS CARDS EGS ACCESS
› System	Import Access Table       Select File     Browse     (accessList.csv)     Update
› Network	Access Table
› Line	□ Index Name ID Department Position Location Number Fwd Number Code Access by Access by Profile Type Code Auth Call Psw
› EGS Setting	Total: 0     Prev     Page:     V     Next     Delete     Delete All
EGS Cards	Add Access Rule     Name   ★   Double Auth   Disable <   \$
› EGS Logs	ID  Type    Department  Profile
Function Key	Position     Location       Access Code     Image: State of the s
	Access Code Action Remote Call and Local A Fwd Number
› EGS Setting	Profile Setting
	Profile     Profile1     Profile Name       Weekday     Statue     Start Time(00:00-23:59)     End Time(00:00-23:59)
EGS Cards	Sunday         No         O0:00         O0:00
	Monday No 🗸 00:00 00:00
› EGS Logs	Tuesday No 🗸 00:00 00:00
L Function Kour	Wednesday No V 00:00 00:00
Function Key	Thursday         № ∨         00:00         00:00           Friday         №          00:00         00:00
	Friday         No <
	Apply

Field Name	Explanation				
Import Access '	<b>Table</b>				
Click the <brow< td=""><td>vse&gt; to choose to import remote access list file (access List.csv) and then click <update></update></td></brow<>	vse> to choose to import remote access list file (access List.csv) and then click <update></update>				
can be batch imp	port remote access rule.				
Access Table					
According to en	trance guard access rules have been added, can choose single or multiple rules on this list				
to delete operati	on.				
Add Access Ru	le				
Name	User name				
ID	RFID card number				
Department Card holder's department					
Position	Card holder's position				
	1/ When the door phone has been answering the call from below <phone num=""> user,</phone>				
Access Code	then the <phone num=""> user can input the access code by keypad to unlock the door</phone>				
Access Code	remotely.				
	2/ The user's private password for local door unlocking by door phone's keypad.				
Access Code	Select Access Code Action mode				
Action	Select Access Code Action mode				
Double Auth	When enabled, private password inputting and RFID reading must be matched				
Double Auth	simultaneously for door unlocking.				
Туре	Host: the door phone would answer all call automatically.				

<u> III DSPPA</u>	* * SIP Intercom System
	Guest: the door phone would be ringing for incoming call, if the auto answer had been
	disabled.
Drofilo	Valid for user access rules (including RFID, access code, etc) within corresponding time
Profile	section. If NONE is selected, it would be taken effect all day.
Location	Virtual extension number, used to make position call instead of real number.
Location	It might be taken with unit number, or room number.
Number	User Phone Number
Fwd Number	Call forwarding number when above Phone Num is unavailable.
<b>Profile Setting</b>	
Profile	There are 4 sections for time profile configuration
Profile Name	The name of profile to help administrator to remember the time definition
Charles a	If it were yes, the time profile would be taken effect. Other time section not included in
Statue	the profiles would not allow users to open door
Start Time	The start time of section
End Time	The end time of section

# (6) EGS Logs

According to open event log, can record up to 1.5 w open event, after more than cover the old records. <u>Click here to Save Logs</u> Right click on the links to select save target as the door log can export CSV format.

	\						
› System							
> Network	Door O	pen Log					
	P	age : 1 🗸	Prev Next De	elete All		Clic	k here to Save Loo
> Line		Result	Time	Duration	Access Name	Access ID	Туре
		Failed	2016/08/17 11:38:46	0 Second(s)		0006800281	Illegal Card
EGS Setting		Success	2016/08/17 11:38:40	5 Second(s)	Hugo	0006800815	Valid Card
		Success	2016/08/17 11:38:32	5 Second(s)		0012345678	Temporary Card
> EGS Cards		Success	2016/08/17 11:36:30	5 Second(s)			Local
		Success	2016/08/17 11:36:11	5 Second(s)		8105	Remote

> Function Key

Field Name	Explanation			
Door Open Log				
Result	Show the results of the open the door (Success or Failed)			
Time	en the door of time.			
Duration	Duration of open the door.			
Access Name	If is the open the door for slot card or remote, will display remote access the name.			
	1. If open the door way to brush card shows card number			
Access ID	2. If the door way to open the door for the remote display the phone number of the			
Access ID	door.			
	3. If open the door way to open the door for local, no display information.			
Туре	Open type: 1. local, 2. Remote, 3. Brush card (Temporary Card, Valid Card and Illegal			

<u> </u>	* *	SIP Intercom System
	Card).	
	Note: there are three kinds of credit card feedback results.	
	1. Temporary Card (Only add the card number, without addin	g other rules )
	2. Valid Card (Has been added access rules)	
	3. Illegal Card (Did not add information)	

# (7) Function Key a) Function Key Settings

em								
ork	Function Key Setti	ngs						
	Key	Туре	Number 1	Number 2	Line	2	Subtype	
	DSS Key 1	Key Event 🗸			SIP1	$\sim$	ок	$\sim$
	DSS Key 2	None 🗸			SIP1	$\sim$	Speed Dial	$\sim$
	DSS Key 3	None 🗸			SIP1	$\sim$	Speed Dial	$\sim$
EGS Setting	DSS Key 4	None 🗸			SIP1	$\sim$	Speed Dial	~
5			A	pply				
(ey								

# ➢ Key Event

Set the key type to the Key Event.

Кеу	Туре	Number 1	Number 2	Line	Subtype
DSS Key 1	Key Event 🗸			SIP1 \	ОК 🗸
DSS Key 2	None Hot Key			SIP1 \	None Dial
DSS Key 3	Line			SIP1 \	Release
DSS Key 4	Key Event Multicast			SIP1	OK Handfree

Туре	Subtype	Usage
	None	Not responding
	Dial	Dial function
Key Event	Release	Delete password input, Cancel dial input and End calls
	OK	Identify key
	Handfree	The hand-free key(with hook dial, hang up)

# > Hot Key

#### <u> III DSPPA</u>

Enter the phone number in the input box, when you press the shortcut key, equipment will dial set telephone number. This button can also be used to set the IP address, press the shortcut key IP direct dial call.

Key	Туре	Number 1	Number 2	Line		Subtype	
DSS Key 1	Hot Key 🗸			SIP1	$\sim$	Speed Dial	$\sim$
DSS Key 2	None Hot Key			SIP1	$\sim$	Speed Dial Intercom	
DSS Key 3	Line			SIP1	$\sim$	Speed Dial	$\sim$
DSS Key 4	Key Event Multicast			SIP1	$\sim$	Speed Dial	$\sim$

Туре	Number	Line	Subtype	Usage
c	Fill the called party's SIP	The SIP account	Speed Dial	In Speed dial mode, with Enable Speed Dial Hangup Enable can define whether this call is allowed to be hang up by re-press the speed dial
	account or address	correspondi ng lines	Intercom	In Intercom mode, if the caller's IP phone support intercom feature, can realize auto answer

### > Multicast

Multicast function is launched will voice messages sent to set the multicast address, all equipment to monitor the group multicast address can receive sponsors speech information, etc. Using multicast functionality can be simple and convenient to send notice to each member in the multicast.

Through the DSS Key configuration multicast calling WEB is as follows:

Key	Туре	Number 1	Number 2	Line		Subtype	
DSS Key 1	Multicast 🗸			SIP1	$\sim$	G.711A	$\sim$
DSS Key 2	None Hot Key			SIP1	$\sim$	G.711A G.711U	
DSS Key 3	Line			SIP1	$\sim$	G.722	
DSS Key 4	Key Event Multicast			SIP1	$\sim$	G.723.1 G.726-32	
						G.729AB	

Туре	Number	Subtype	Usage
Multicast		G.711A	Normowhand anoach acding (4Khz)
	Set the host IP address and	G.711U	Narrowband speech coding (4Khz)
	port number, the middle	G.722	Wideband speech coding (7Khz)
	separated by a colon	G.723.1	
	1 5	G.726-32	Narrowband speech coding (4Khz)
		G.729AB	

#### $\diamond$ operation mechanism

Device through the DSS Key configuration of multicast address and port and started coding; set by WEB to monitor the multicast address and port; device sends a multicast, listens to the address of the device can receive the multicast content.

#### $\diamond$ calling configuration

The call is already exists, and three party or initiated multicast communication, so it will not be able to launch a new multicast call.

# V. Appendix

# 1. Technical parameters

Communi	cation protocol	SIP 2.0(RFC-3261)				
Main chip	set	Broadcom				
Varia	DSS Key	1(Stainless steel)				
Keys	Numeric keyboard	Support				
	MIC	1				
	Speaker	$3W/4\Omega$				
Audio	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	12V/700mA DC				
Ports	WAN	10/100BASE-TX s Auto-MDIX, RJ-45				
DEID/IC -	and noodon(nolon)	EM4100 (125Khz)Standard configuration				
KFID/IC C	card reader(relay)	MIFARE One(13.56Mhz)Custom-made				
Power sup	ply mode	12V / 1A DC or PoE				
РоЕ		PoE 802.3af (Class 3 - 6.49~12.95W)				
Cables		CAT5 or better				
Shell Mate	erial	Metal panel, ABS face-piece and back shell				
Working t	emperature	-10 °C to 60 °C				

<u>IIIOSPPA</u> * *	SIP Intercom System
Working humidity	10% - 90%
Storage temperature	-40 °C to 70 °C
Installation way	Wall mounted
External size	160 x 93 x 35mm
Package size	178 x 104 x 55mm
Gross weight	420g

## 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
- Integrated RFID Card reader
- 1 indoor switch interface
- 1 electric lock relay
- External power supply
- Door phone: call, password, RFID card, indoor switch
- Protection level: IP54, CE/FCC

# 3. Schematic diagram



\*

# VI. Other instructions

### 1. Open door modes

#### Local control

#### 1) Local Password

- ☆ Set <Local Password> (the password is "6789" by default) via DOOR PHONE\DOOR PHONE as above.
- $\diamond$  Input password via keypad and press the "#" key, then the door will be unlocked.

#### 2) Private access code

- ♦ Set <Add Access Rule\Access Code> and enable local authentication.
- $\diamond$  Input access code via keypad and press the "#" key, then the door will be unlocked.

#### • Remote control

#### 1) Visitors call the owner

- Visitors can call the owner via position speed dial or phone number. (After setting the speed dial key, visitors can press it to call direct.)
- $\diamond$  The owner answers the call and presses the "\*" key to unlock the door for visitors.

#### 2) Owner calls visitors

- ♦ Owner calls visitors via SIP phone.
- $\diamond$  SIP door phone answers the call automatically.
- $\diamond$  Owner inputs corresponding <Access codes> via SIP phone keypad to unlock the door.

#### • Swiping cards

♦ Use pre-assigned RFID cards to unlock the door, by touching RFID area of the device.

#### Indoor switch

 $\diamond$  Press indoor switch, which is installed and connected with the 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 Open Log Server	0.0.0	Port of Open Log Server	514
Enable Open Log Server	Disable 🗸	Enable Indoor Open	Enable 🗸
Enable Card Reader	Enable 🗸	Limit Talk Duration	Disable Enable
Door Unlock Indication	Long Beeps 🗸	Remote Code Check Length	4 (1~6)
	Ar	oply	

### 2. Management of card

#### 1) Administrator Table

<Issuer> and <Revocation>

Adm	inistrat	or Table	>>		
	Add Adı Card	min [	Issuer	~ Add	
		Index	ID	Issuing Date	Туре
		1	0003476384	2016/08/17 11:26:12	Issuer
		2	0003408919	2016/08/17 11:26:23	Revocation
	Total: 2	2	Prev Page: 1 🗸 Next	9 Delete	Delete All

#### • Add Administrator cards

Input a card's ID, selected <Issuer> or <Revocation> in the types and Clicked <Add>, you can add administrator card.

Admi	Administrator Table >>							
	Add Admin Card		0003476384		Issuer	$\sim$	Add	
	Index			ID	Issuer Revocation			Issuing Date

#### • Delete Administrator cards

Select the admin card of need to delete, click <Delete>.

Ministrate Add Adr Card		>> Issuer	✓ Add	
	Index	ID	Issuing Date	Туре
	1	0003476384	2016/08/17 11:26:12	Issuer
	2	0003408919	2016/08/17 11:26:23	Revocation
Total: 2	2	Prev Page: 1 🗸 Next	9 Delete	Delete All

### 2) Add user cards

- Method 1: used to add cards for starters typically
- ☆ In web page < EGS Setting →Features →Card Reader Working Mode > option, select <Card Issuing>.

Dial Number Voice Play	Disable 🗸	Voice Play Language	English 🗸
Card Reader Working Mode	Card Issuing V Normal Card Issuing Card Revoking	Apply	

♦ Click <Apply>, Card Reader would be entered the issuing status.

#### 

- ♦ Use new card to touch card reader induction area, and then you might hear the confirmed indication tone from the device. Repeat step can to add more cards.
- $\diamond$  In web page < EGS Setting  $\rightarrow$  Features  $\rightarrow$  Card Reader Working Mode > option, select <Normal>.

Dial Number Voice Play	Disable 🗸	Voice Play Language	English 🗸
Card Reader Working Mode	Normal  Normal Card Issuing Card Revoking	Apply	

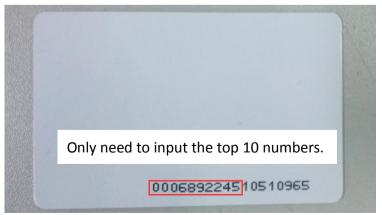
- $\diamond$  Click <Apply>, Card Reader would be back to the Normal status.
- $\diamond$  The issuing records can be found from the door card table list.

Add Door Card Add			Add	Click here to Save Door Card Table		
	Index	Name	ID	Issuing Date	Card State	
	1		0004770424	2016/08/17 11:12:01	Enable 🗸	
	2		0003477117	2016/08/17 11:12:14	Enable 🗸	
	3		0003408920	2016/08/17 11:12:30	Enable 🗸	

- Methods 2: used to add cards for professionals
- ♦ Use <Issuer admin card> to touch card reader induction area, and it would be entered issuing card status.
- ♦ Use new card to touch card reader induction area, and you might hear the confirmed indication tone from the device. Repeat step 2 to add more cards.
- ♦ Use <Issuer admin card> to touch card reader induction area again, it would be back to normal working status.
- Method 3: use to add few cards
- $\diamond$  Input cards number in door card settings page, and then click <Add>.



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



### 3) Delete user cards

• Method 1: used to batch delete cards for starters.

#### <u> III DSPPA</u>

#### \*

☆ In web page < EGS Setting →Features →Card Reader Working Mode > option, select <Card Revoking>.

Dial Number Voice Play	Disable 🗸	Voice Play Language	English 🗸
Card Reader Working Mode	Card Revoking 🗸		
	Normal Card Issuing	Apply	
	Card Revoking		

- ♦ Click <Apply>, Card Reader would be entered the revoking status.
- ♦ Use card to touch card reader induction area, and you might hear the card reader confirmed indication tone. Repeat step can to delete more cards.
- $\diamond$  In web page <EGS Setting  $\rightarrow$ Features  $\rightarrow$ Card Reader Working Mode >option, select <Normal>.

Dial Number Voice Play	Disable 🗸	Voice Play Language	English 🗸
Card Reader Working Mode	Normal V Normal Card Issuing Card Revoking	Apply	

- ♦ Click <Apply>, Card Reader would be back to the Normal status.
- Method 2: used to batch add cards for intermediates.
- ♦ Use < Revocation admin card> to touch card reader induction area, and it would be entered revoking card status.
- ♦ Use the cards you want to delete from system, to touch card reader induction area, and you might hear the card reader confirmed indication tone. Repeat step 2 to delete cards.
- ♦ Use <Revocation admin card> to touch card reader induction area, and it would be back to card read only status.
- Method 3: use to bulk delete or partially delete card records
- $\Rightarrow$  In web page<EGS Cards  $\rightarrow$  Door Card Table>select the card ID and then click <Delete>.

Note: If you click <Delete All>, system will delete all the ID card records.

#### Door Card Table >>

Add Do	Add Door Card Click here to Save Door Card Tab				<u>a Door Card Table</u>
	Index	Name	ID	Issuing Date	Card State
$\checkmark$	1		0004770424	2016/08/17 11:12:01	Enable 🗸
	2		0003477117	2016/08/17 11:12:14	Enable 🗸
	3		0003408920	2016/08/17 11:12:30	Enable 🗸
Total: 3 Prev Page: 1 🗸 Next 😡 Delete Delete All					

Guangzhou DSPPA Audio Co., Ltd