SIP Audio Door Phone i23S

USER MANUAL

V1.0

www.fanvil.com

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

Safety Notices

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

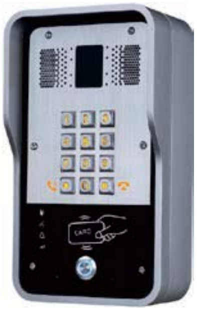
Directory

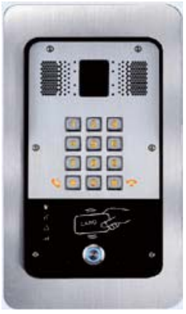
A.Product introduction

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

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

1. Appearance of the product





2. Description

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

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

B.Start Using

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

1. Confirm the connection

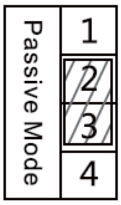
Confirm whether the equipment of the power cord, network cable, electric lock control line connection and the boot-up is normal. (Check the network state of light)

1) Power, Electric Lock, Indoor switch port

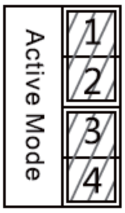
There are 2 power supply options: 12V/DC or POE (Powered By Ethernet). PIN 1 (+12V) and PIN 2 (VSS) connected to the power supply. PIN3/4/5 used to connect the electric lock, only 2 of them (NC and COM, or NO and COM) will be connected usually, depending on the type of electric lock. PIN6/7 used to connect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

CN7							
1	**2**	**3**	**4**	**5**	**6**	**7**	
+12V	VSS	NC	COM	NO	S_IN	S_OUT	
12V 1A/DC		Electric-lock switch			Indoor switch		

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



Jumper in passive mode



Jumper in active mode

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

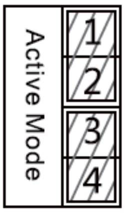
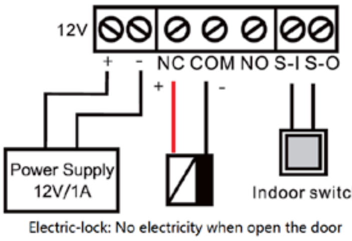
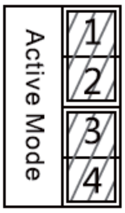
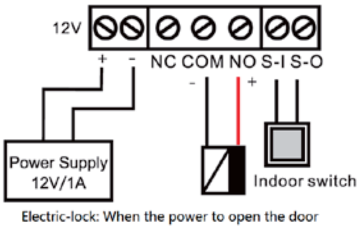
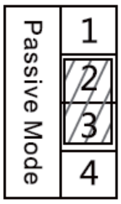
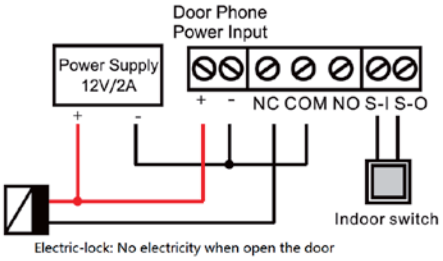
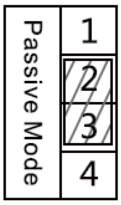
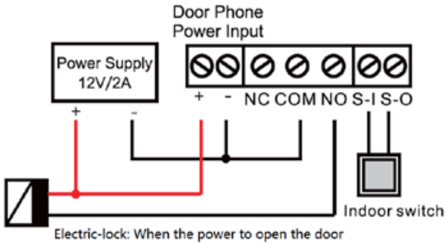
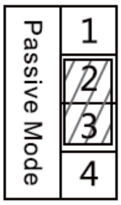
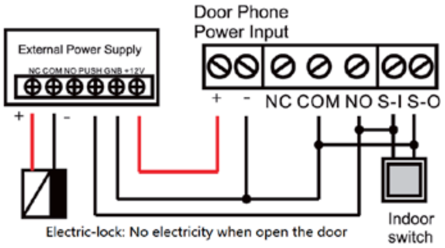
【**Note**】When the device is in active mode, it can drive 12V/650mA switch output maximum, to which a standard electric-lock or another compatible electrical appliance can be connected.

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

3）Wiring instructions

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

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

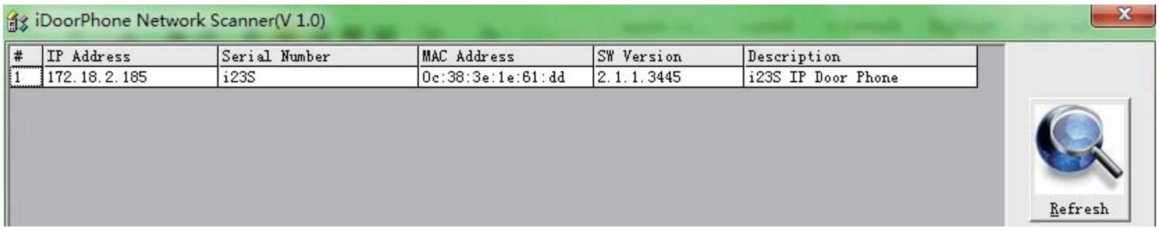
Driving Mode		Electric lock		Jumper port	Connections
Activ e	Passiv e	No electricity when open	When the power to open		
√		√			 12V + - NC COM NO S-I S-O + - Power Supply 12V/1A Indoor switch Electric-lock: No electricity when open the door
√			√		 12V + - NC COM NO S-I S-O - + Power Supply 12V/1A Indoor switch Electric-lock: When the power to open the door
	√	√			 Door Phone Power Input Power Supply 12V/2A + - + - NC COM NO S-I S-O Indoor switch Electric-lock: No electricity when open the door
	√		√		 Door Phone Power Input Power Supply 12V/2A + - + - NC COM NO S-I S-O Indoor switch Electric-lock: When the power to open the door
	√	√			 Door Phone Power Input External Power Supply NC COM NO PUSH GND +12V + - + - NC COM NO S-I S-O Indoor switch Electric-lock: No electricity when open the door

2. Quick Setting

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

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

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



iDoorPhone Network Scanner(V 1.0)

#	IP Address	Serial Number	MAC Address	SW Version	Description
1	172.18.2.185	i23S	0c:38:3e:1e:61:dd	2.1.1.3445	i23S IP Door Phone

C.Basic operation

1. Answer a call

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

2. Call

There are 2 options to place a call:

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

immediately.

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

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

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

3. End call

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

1) Release the processing call

2) Reject the incoming call when it’s ringing

4. Open the door operation

There are seven options to open the door:

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

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

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

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

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

6) Private access code to open the door.

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

NOTE: ended with “#” to send the code immediately.

7) Active URL control command to open the door.

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

a. User and pwd is Web the user name and password.
b. “openCode” is the remote-control code to open the door.

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

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

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

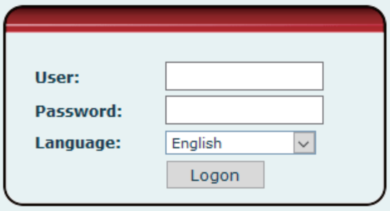
When door is open , the device will play sirens sound to prompt.

D.Page settings

1. Browser configuration

When the device and your computer are successfully connected to the network, enter the IP address of the device on the browser as http://xxx.xxx.xxx.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.



2. Password Configuration

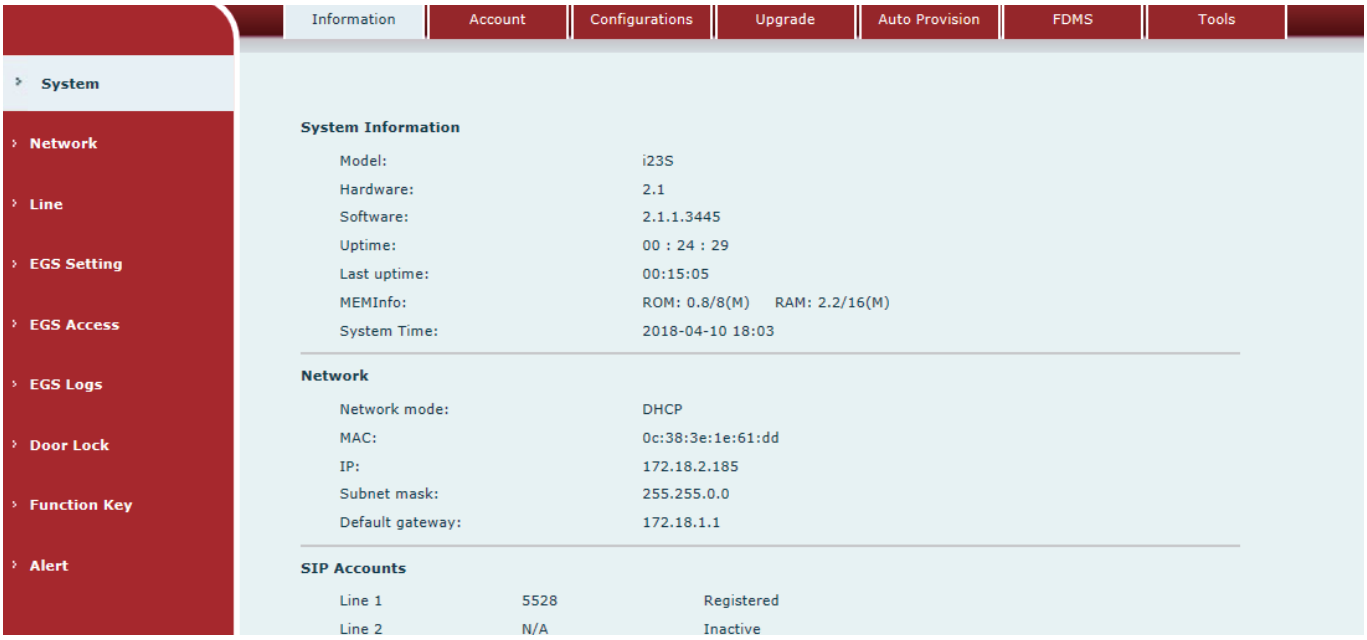
There are two levels of access: root level and general level. A user with root level access can browse and set all configuration parameters, while a user with general level can set all configuration parameters except server parameters for SIP.

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

3. Configuration via WEB

(1) System

a) Information



System Information

```
Model:              i23S
Hardware:           2.1
Software:           2.1.1.3445
Uptime:             00 : 24 : 29
Last uptime:        00:15:05
MEMInfo:            ROM: 0.8/8(M)     RAM: 2.2/16(M)
System Time:        2018-04-10 18:03
```

Network

```
Network mode:       DHCP
MAC:                0c:38:3e:1e:61:dd
IP:                 172.18.2.185
Subnet mask:        255.255.0.0
Default gateway:    172.18.1.1
```

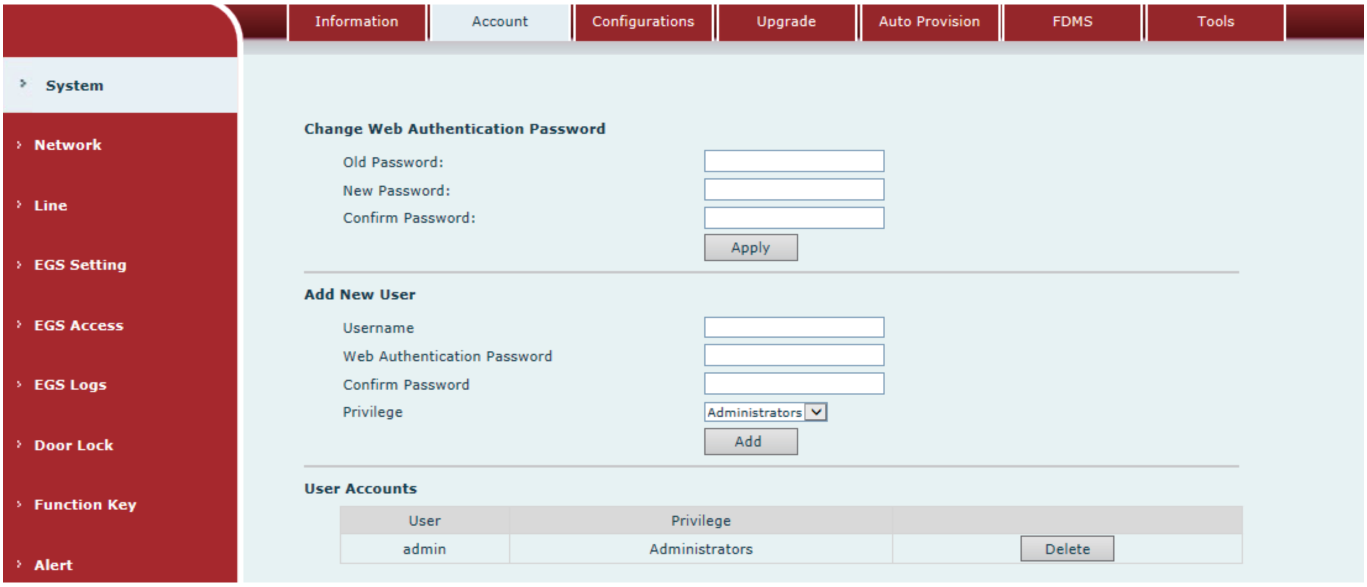
SIP Accounts

```
Line 1      5528      Registered
Line 2      N/A       Inactive
```

Information	
Field Name	**Explanation**
System Information	Display equipment model, hardware version, software version, uptime, Last uptime and 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.



Change Web Authentication Password

Old Password:

New Password:

Confirm Password:

Add New User

Username

Web Authentication Password

Confirm Password

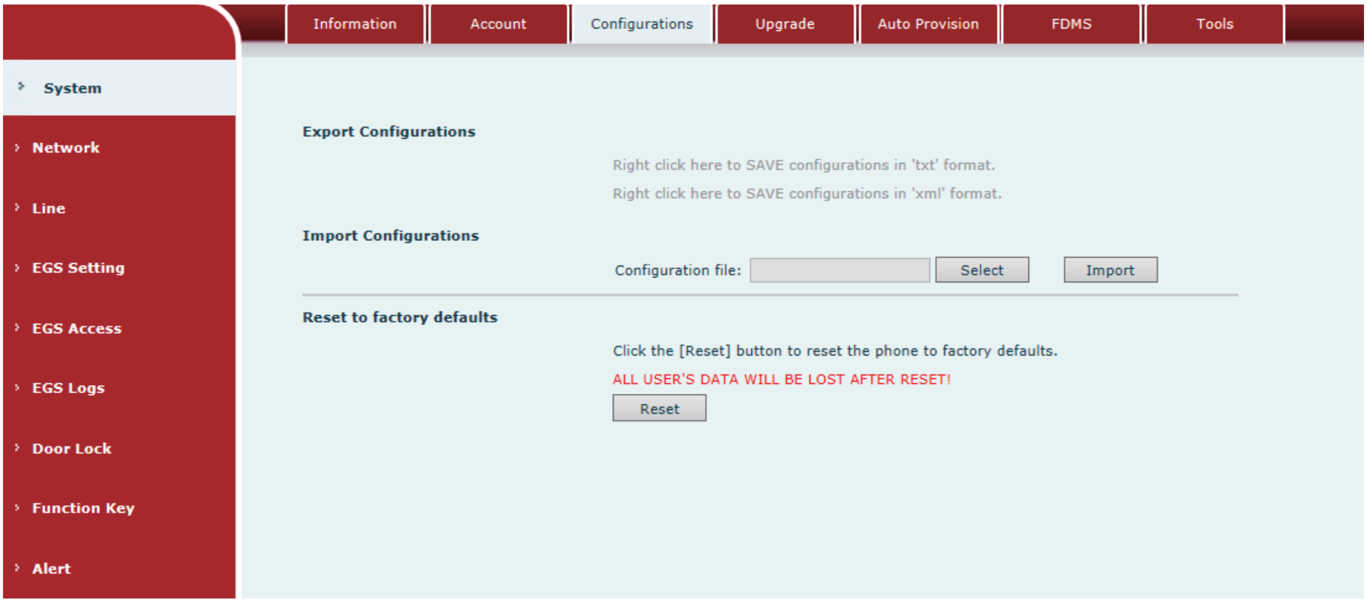
Privilege: Administrators

User Accounts

User	Privilege	
admin	Administrators	Delete

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



Export Configurations

Right click here to SAVE configurations in 'txt' format.

Right click here to SAVE configurations in 'xml' format.

Import Configurations

Configuration file: Select Import

Reset to factory defaults

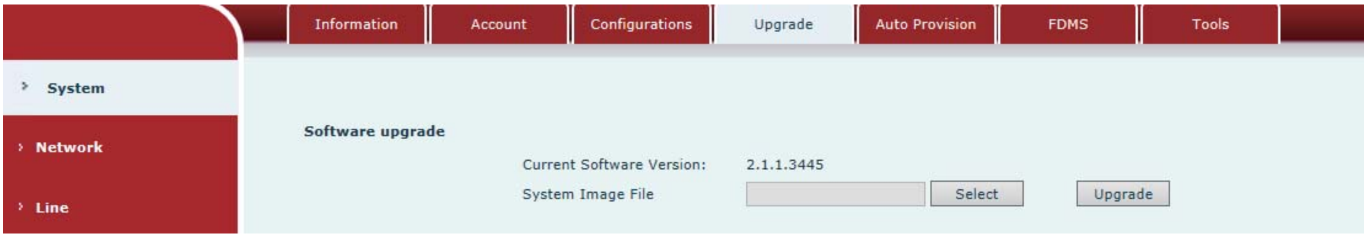
Click the [Reset] button to reset the phone to factory defaults.

ALL USER'S DATA WILL BE LOST AFTER RESET!

Reset

Configurations	
Field Name	**Explanation**
Export Configurations	Save the equipment configuration to a txt or xml file. Please note to Right click on 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 defaults	This will restore factory default and remove all configuration information.

d) Upgrade



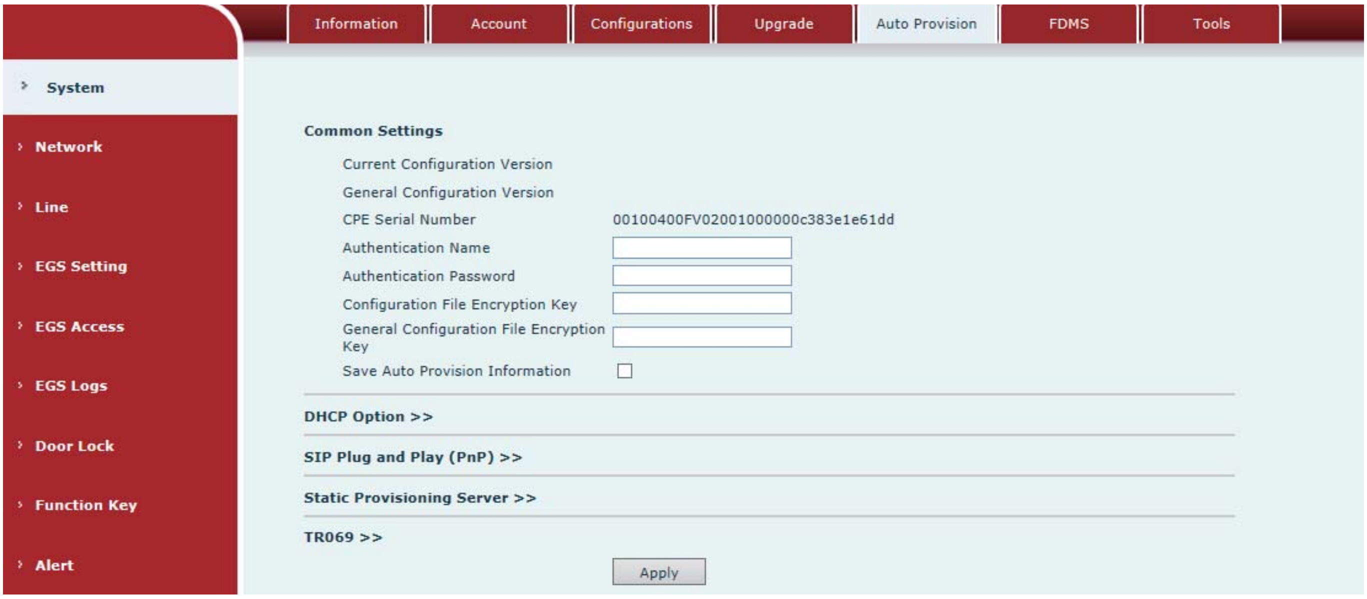
Software upgrade

Current Software Version: 2.1.1.3445

System 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



Common Settings

Current Configuration Version	
General Configuration Version	
CPE Serial Number	00100400FV02001000000c383e1e61dd
Authentication Name	
Authentication Password	
Configuration File Encryption Key	
General Configuration File Encryption Key	
Save Auto Provision Information	□

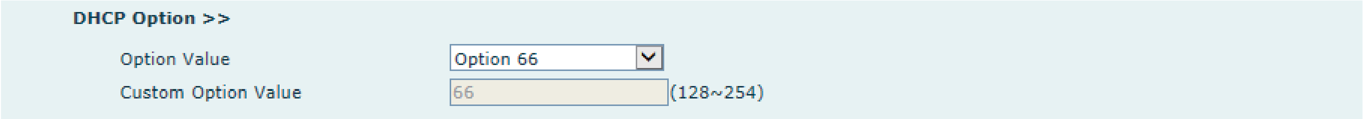
DHCP Option >>

SIP Plug and Play (PnP) >>

Static Provisioning Server >>

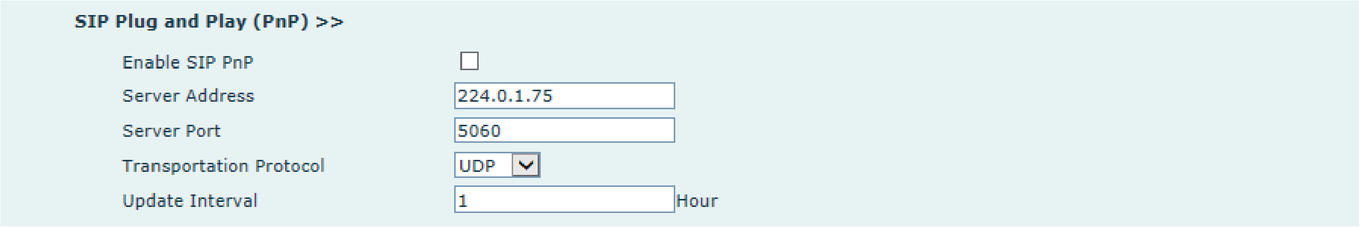
TR069 >>

Apply



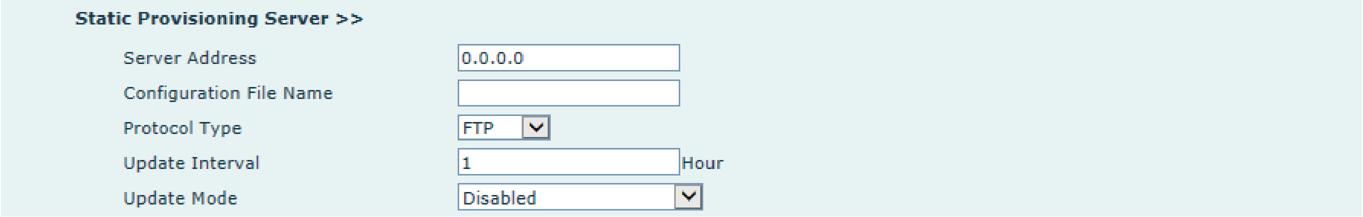
DHCP Option >>

Option Value	Option 66
Custom Option Value	66 (128~254)



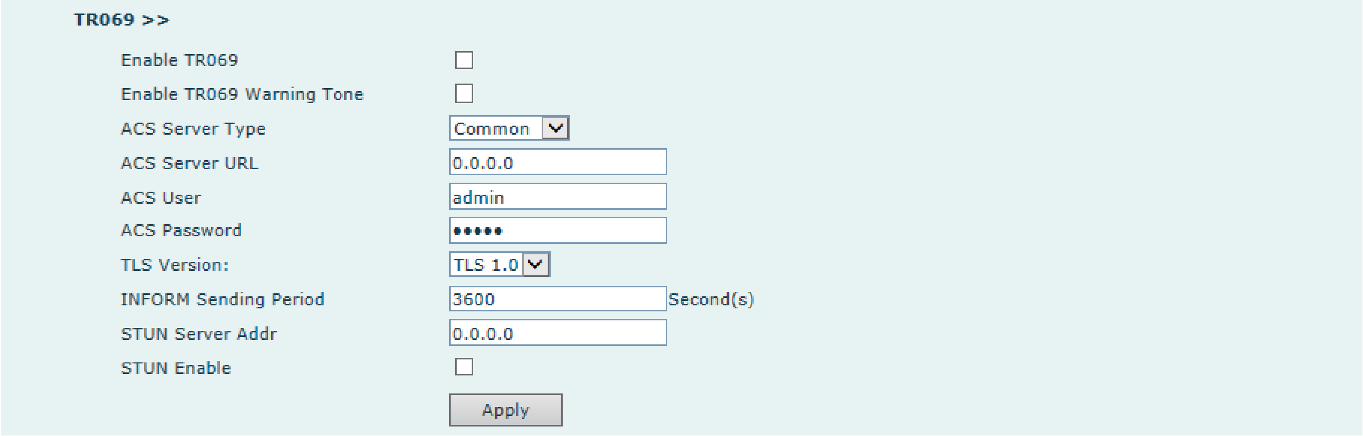
SIP Plug and Play (PnP) >>

Enable SIP PnP	□
Server Address	224.0.1.75
Server Port	5060
Transportation Protocol	UDP
Update Interval	1 Hour



Static Provisioning Server >>

Server Address	0.0.0.0
Configuration File Name	
Protocol Type	FTP
Update Interval	1 Hour
Update Mode	Disabled



TR069 >>

Enable TR069	□
Enable TR069 Warning Tone	□
ACS Server Type	Common
ACS Server URL	0.0.0.0
ACS User	admin
ACS Password	•••••
TLS Version:	TLS 1.0
INFORM Sending Period	3600 Second(s)
STUN Server Addr	0.0.0.0
STUN Enable	□

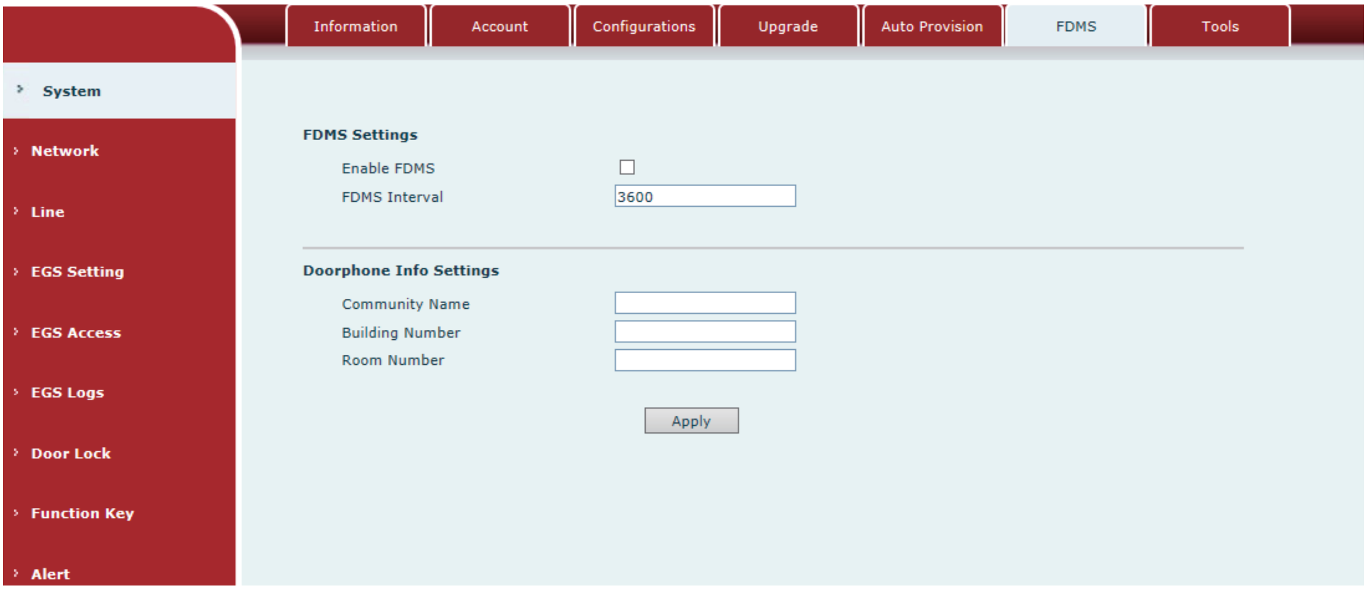
Apply

Auto Provision	
Field Name	**Explanation**
Common Settings	

Current Configuration Version	Show the current config file’s version. If the version of configuration downloaded is higher than this, the configuration will be upgraded. If the endpoints confirm the configuration by the Digest method, the configuration will not be upgraded unless it differs from the current configuration
General Configuration Version	Show the common config file’s version. If the configuration downloaded and this configuration is the same, the auto provision will stop. If the endpoints confirm the configuration by the Digest method, the configuration will not be upgraded unless it differs from the current configuration.
CPE Serial Number	Serial number of the equipment
Authentication Name	Username for configuration server. Used for FTP/HTTP/HTTPS. If this is blank the phone will use anonymous
Authentication Password	Password for configuration server. Used for FTP/HTTP/HTTPS.
Configuration File Encryption Key	Encryption key for the configuration file
General Configuration File Encryption Key	Encryption key for common configuration file
Save Auto Provision Information	Save the auto provision username and password in the phone until the server url changes
DHCP Option	
Option Value	The equipment supports configuration from Option 43, Option 66, or a Custom DHCP option. It may also be disabled.
Custom Option Value	Custom option number. Must be from 128 to 254.
SIP Plug and Play (PnP)	
Enable SIP PnP	If this is enabled, the equipment will send SIP SUBSCRIBE messages to a multicast address when it boots up. Any SIP server understanding that message will reply with a SIP NOTIFY message containing the Auto Provisioning Server URL where the phones can request their configuration.
Server Address	PnP Server Address
Server Port	PnP Server Port
Transportation Protocol	PnP Transfer protocol – UDP or TCP
Update Interval	Interval time for querying PnP server. Default is 1 hour.

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

f) FDMS



FDMS Settings

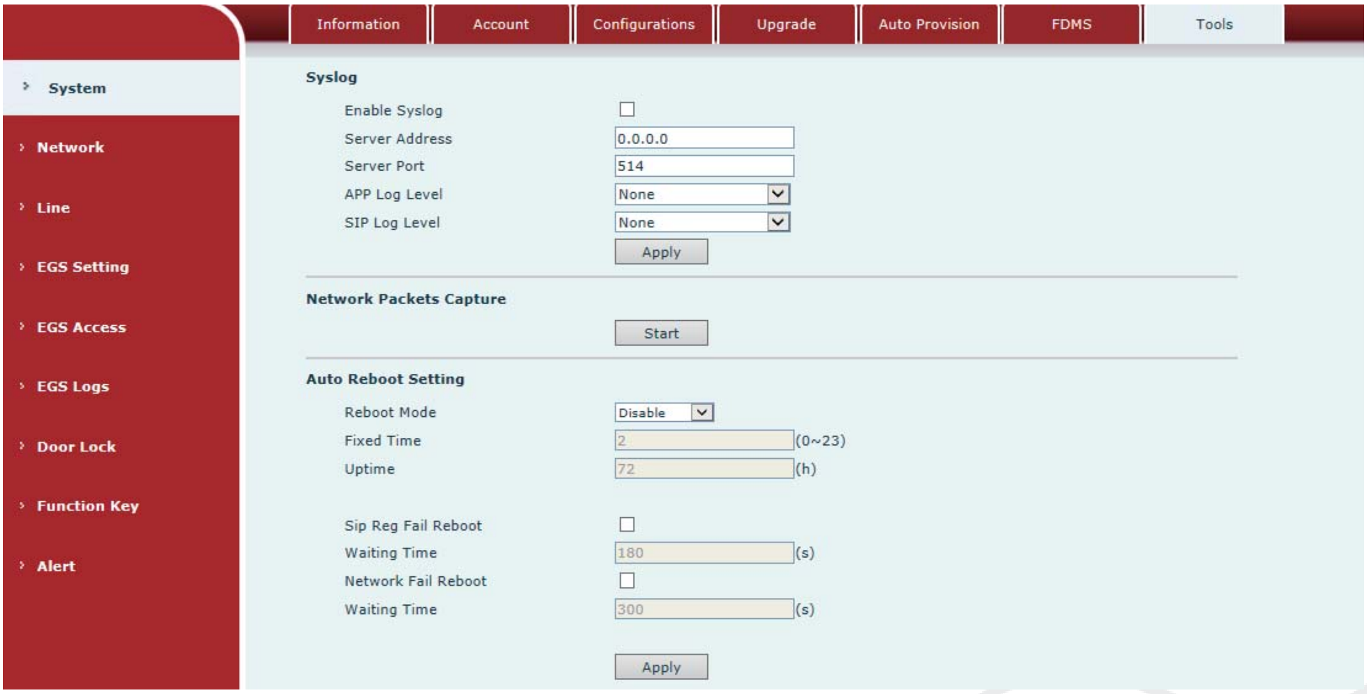
Enable FDMS	□
FDMS Interval	3600

Doorphone Info Settings

Community Name	
Building Number	
Room Number	

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

g) Tools



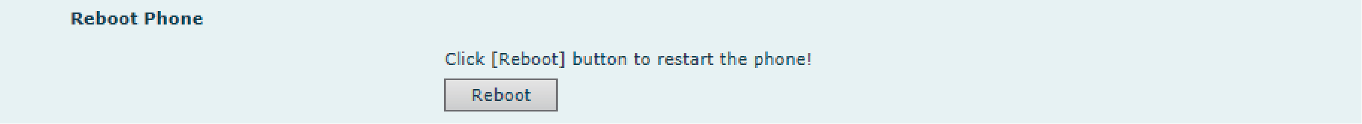
Syslog

Enable Syslog	□
Server Address	0.0.0.0
Server Port	514
APP Log Level	None
SIP Log Level	None

Network Packets Capture

Auto Reboot Setting

Reboot Mode	Disable
Fixed Time	2 (0~23)
Uptime	72 (h)
Sip Reg Fail Reboot	□
Waiting Time	180 (s)
Network Fail Reboot	□
Waiting Time	300 (s)



Reboot Phone

Click [Reboot] button to restart the phone!

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

There are 8 levels of debug information.

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

Level 1: alert; Action must be taken immediately.

Level 2: critical; System is probably working incorrectly.

Level 3: error; System may not work correctly.

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

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

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

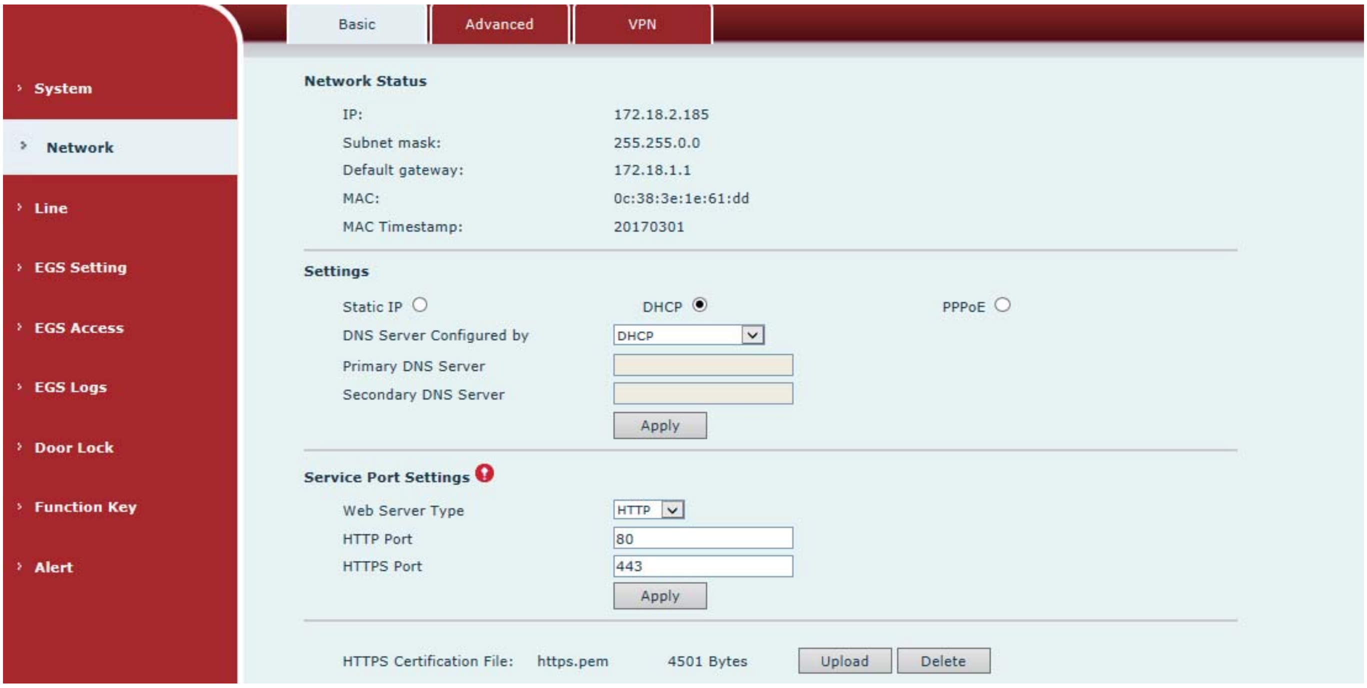
Level 7: debug; Debug messages normally used by system designer. This level can only be displayed via telnet.

Tools	
Field Name	**Explanation**
Syslog	
Enable 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.	
Auto Reboot Setting	
Configure the restart mode and restart time of the device and restart it to restore the device to its best state.	
Reboot Phone	

Some configuration modifications require a reboot to become effective. Clicking the Reboot button will lead to reboot immediately.
Note: Be sure to save the configuration before rebooting.

(2) Network

a) Basic



Network Status

IP: 172.18.2.185
Subnet mask: 255.255.0.0
Default gateway: 172.18.1.1
MAC: 0c:38:3e:1e:61:dd
MAC Timestamp: 20170301

Settings

Static IP ○ DHCP ● PPPoE ○
DNS Server Configured by: DHCP
Primary DNS Server:
Secondary DNS Server:

Service Port Settings

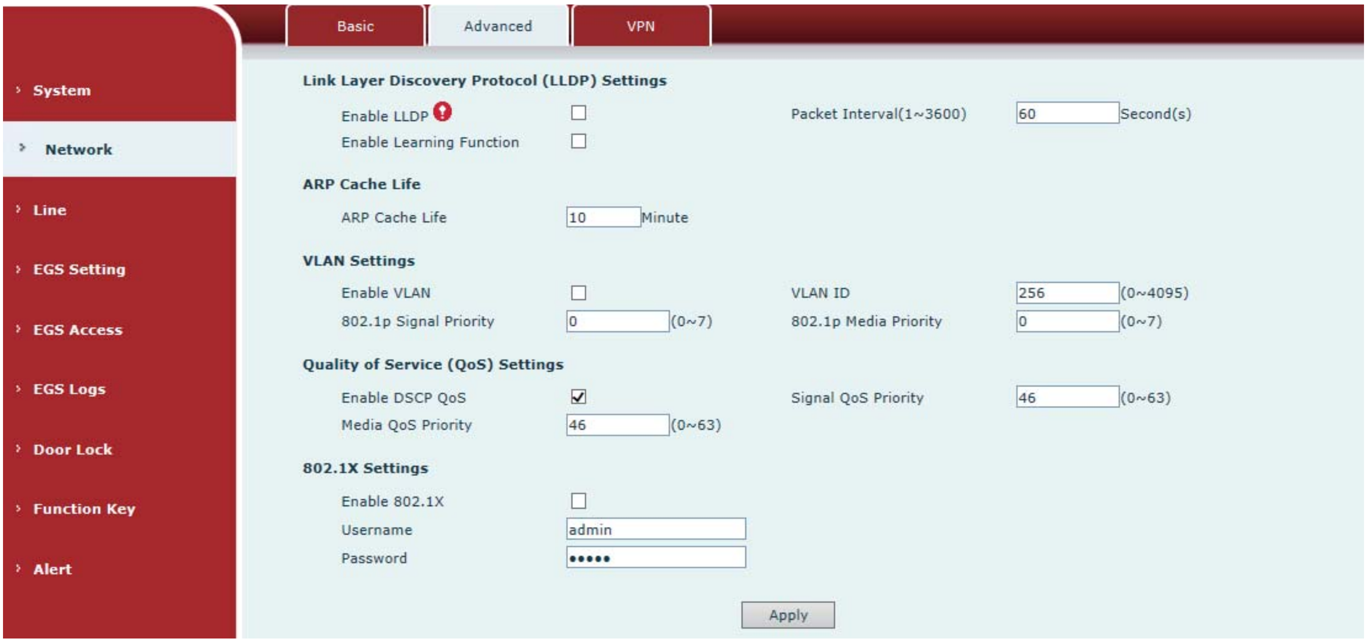
Web Server Type: HTTP
HTTP Port: 80
HTTPS Port: 443

HTTPS Certification File: https.pem 4501 Bytes

Field Name	Explanation
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 Timestamp	Get the MAC address of time.
Settings	
Select the appropriate network mode. The equipment supports three network modes:	
Static IP	Network parameters must be entered manually and will not change. All parameters are provided by the ISP.
DHCP	Network parameters are provided automatically by a DHCP server.
PPPoE	Account and Password must be input manually. These are provided by your ISP.
If Static IP is chosen, the screen below will appear. Enter values provided by the ISP.	
DNS Server Configured by	Select the Configured mode of the DNS Server.
Primary DNS Server	Enter the server address of the Primary DNS.
Secondary DNS Server	Enter the server address of the Secondary DNS.
Click the APPLY button after entering the new settings. The equipment will save the new settings and apply them. If a new IP address was entered for the equipment, it must be used to login to the phone after clicking the APPLY button.	
Service Port Settings	
Web Server Type	Specify Web Server Type – HTTP or HTTPS
HTTP Port	Port for web browser access. Default value is 80. Change this from the default to enhance security. Setting this port to 0 will disable HTTP access. Example: The IP address is 192.168.1.70 and the port value is 8090. The accessing address is http://192.168.1.70:8090.
HTTPS Port	Port for HTTPS access. An https authentication certification must be downloaded into the equipment before using https. Default value is 443. Change this from the default to enhance security.
Note: 1) Any changes made on this page require a reboot to become active. 2) It is suggested that the make the values bigger than 1024 if users change the port to HTTPS. Values less than 1024 are reserved. 3) If the HTTP port is set to 0, HTTP service will be disabled.	

b) Advanced



Link Layer Discovery Protocol (LLDP) Settings

Enable LLDP □ Packet Interval(1~3600) 60 Second(s)

Enable Learning Function □

ARP Cache Life

ARP Cache Life 10 Minute

VLAN Settings

Enable VLAN □ VLAN ID 256 (0~4095)

802.1p Signal Priority 0 (0~7) 802.1p Media Priority 0 (0~7)

Quality of Service (QoS) Settings

Enable DSCP QoS ☑ Signal QoS Priority 46 (0~63)

Media QoS Priority 46 (0~63)

802.1X Settings

Enable 802.1X □

Username admin

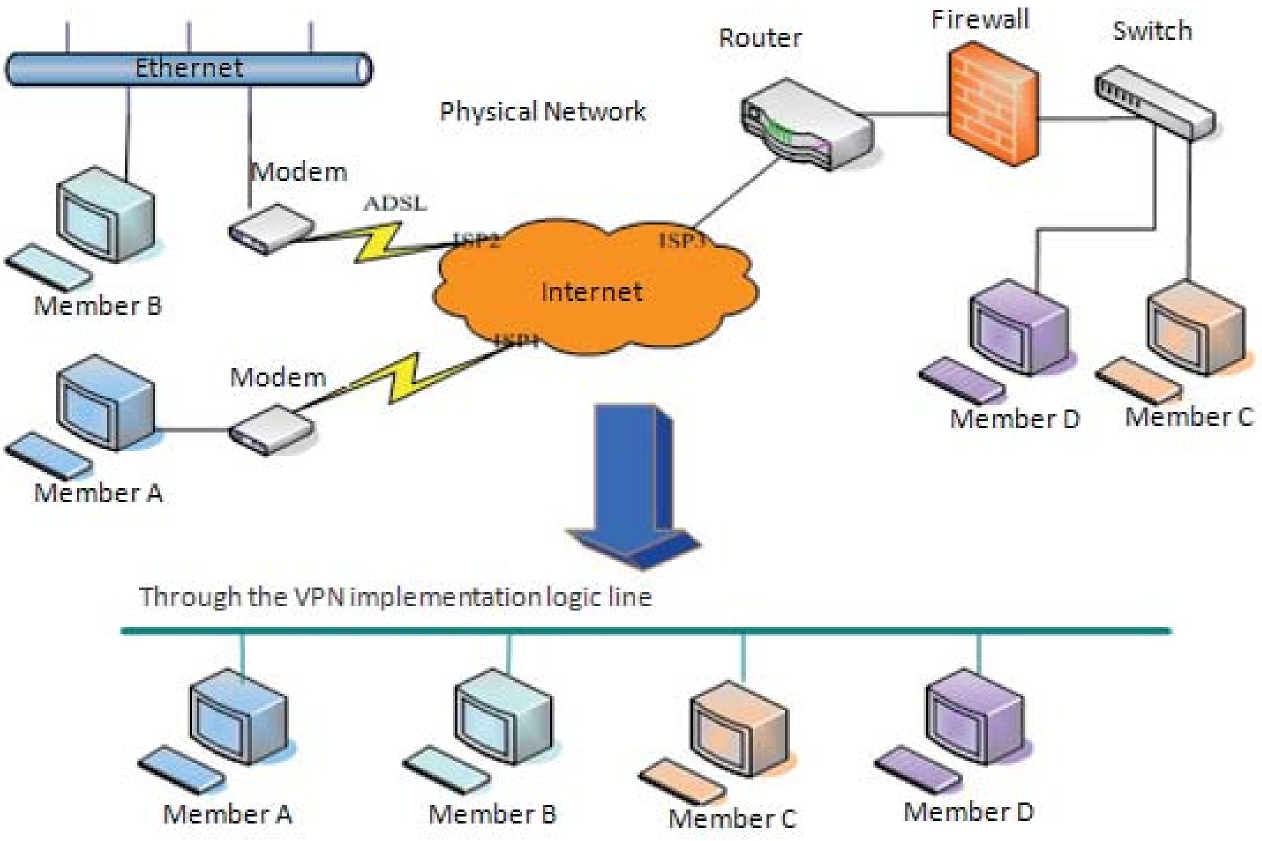
Password •••••

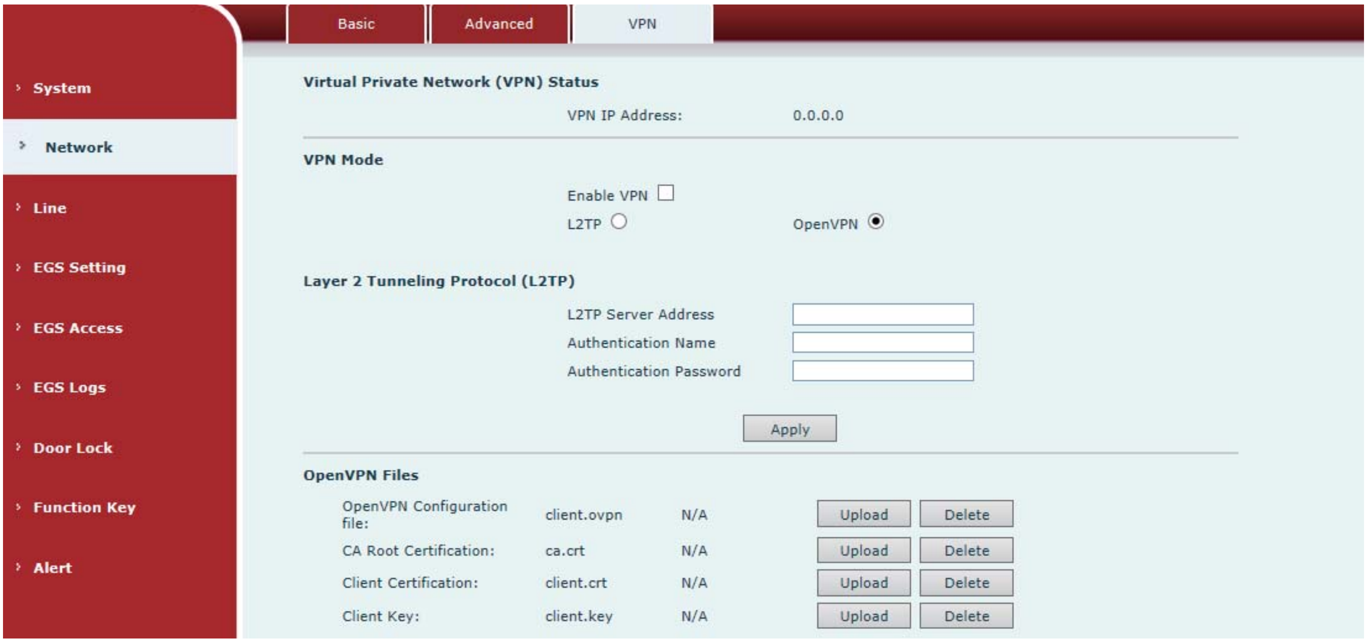
Field Name	Explanation
Link Layer Discovery Protocol (LLDP)Settings	
Enable LLDP	Enable the device to send LLDP packets.
Packet Interval(1~3600)	The time interval of device sending packet. The default value is 60s.
Enable Learning Function	Open the device to learn LLDP function, after opening, the device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

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

c) VPN

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





Virtual Private Network (VPN) Status

VPN IP Address: 0.0.0.0

VPN Mode

Enable VPN □

L2TP ○ OpenVPN ●

Layer 2 Tunneling Protocol (L2TP)

L2TP Server Address

Authentication Name

Authentication Password

OpenVPN Files

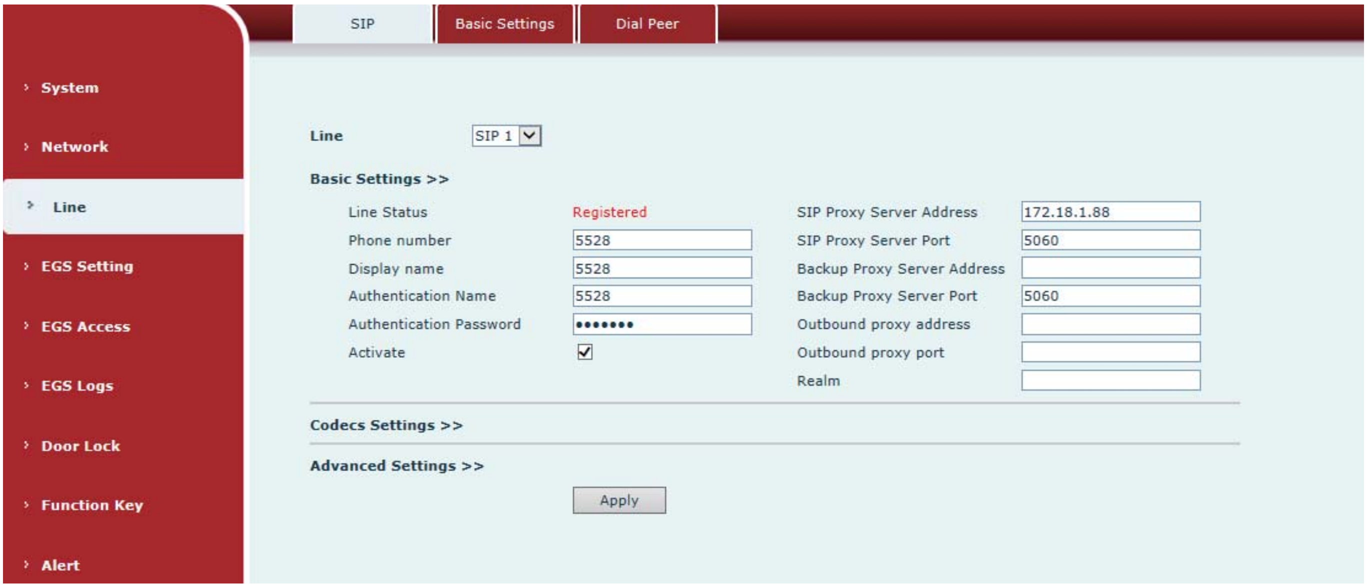
OpenVPN Configuration file:	client.ovpn	N/A	Upload Delete
CA Root Certification:	ca.crt	N/A	Upload Delete
Client Certification:	client.crt	N/A	Upload Delete
Client Key:	client.key	N/A	Upload Delete

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

(3) Line

a) SIP

Configure a SIP server on this page.



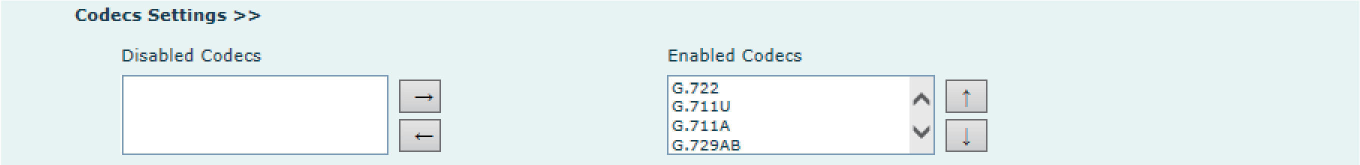
Line: SIP 1

Basic Settings >>

Line Status	Registered	SIP Proxy Server Address	172.18.1.88
Phone number	5528	SIP Proxy Server Port	5060
Display name	5528	Backup Proxy Server Address	
Authentication Name	5528	Backup Proxy Server Port	5060
Authentication Password	•••••••	Outbound proxy address	
Activate	☑	Outbound proxy port	
		Realm	

Codecs Settings >>

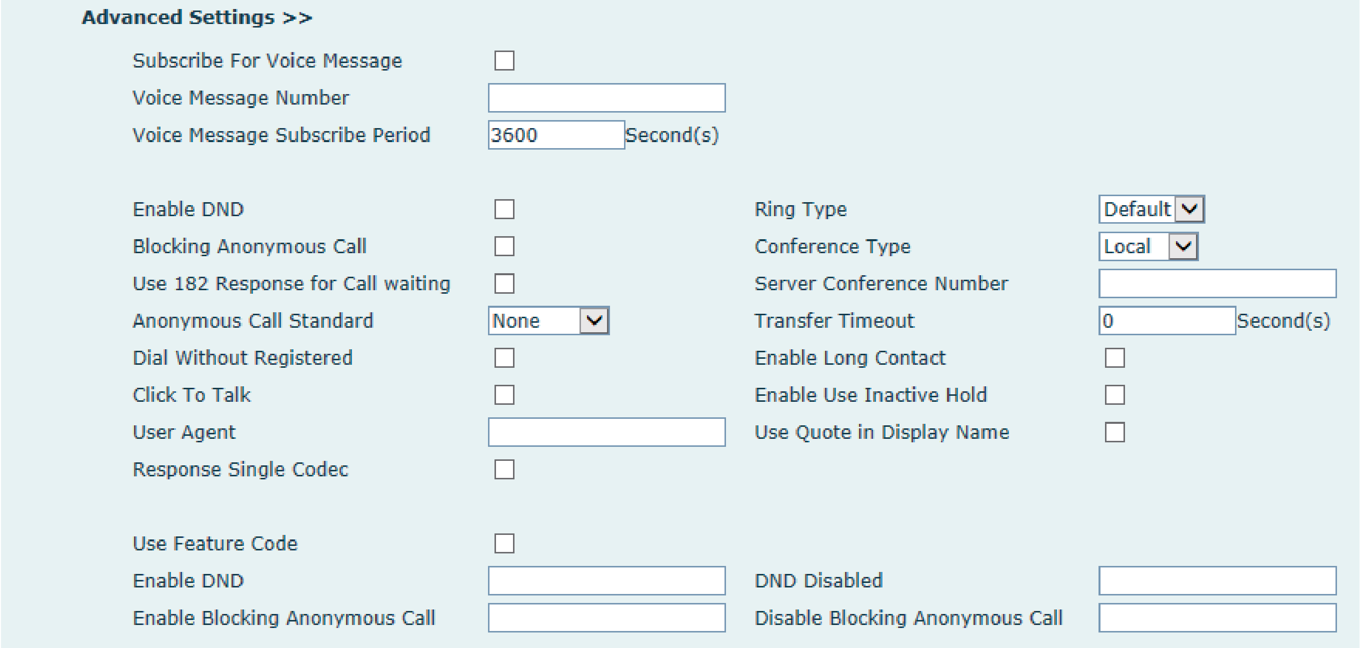
Advanced Settings >>



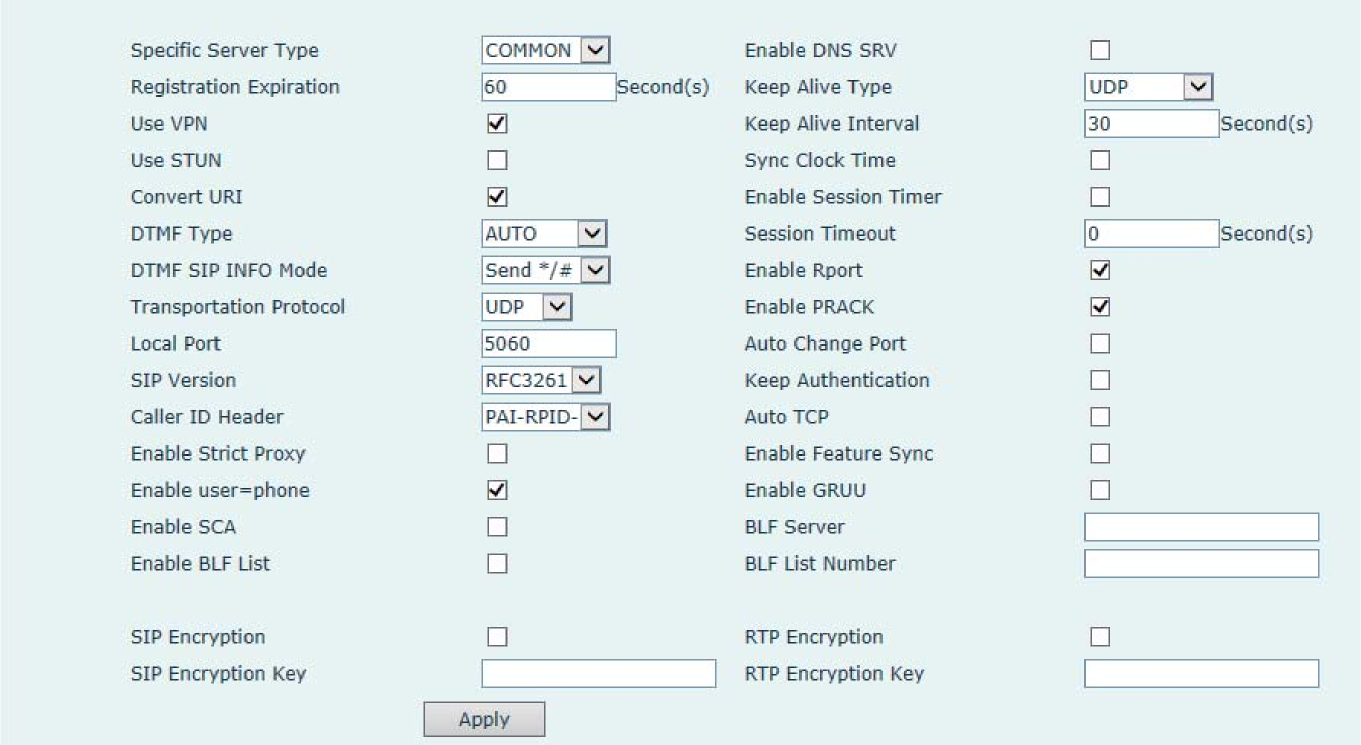
Codecs Settings >>

Disabled Codecs

Enabled Codecs: G.722, G.711U, G.711A, G.729AB


Advanced Settings >>

Subscribe For Voice Message	□		
Voice Message Number			
Voice Message Subscribe Period	3600 Second(s)		
Enable DND	□	Ring Type	Default
Blocking Anonymous Call	□	Conference Type	Local
Use 182 Response for Call waiting	□	Server Conference Number	
Anonymous Call Standard	None	Transfer Timeout	0 Second(s)
Dial Without Registered	□	Enable Long Contact	□
Click To Talk	□	Enable Use Inactive Hold	□
User Agent		Use Quote in Display Name	□
Response Single Codec	□		
Use Feature Code	□		
Enable DND		DND Disabled	
Enable Blocking Anonymous Call		Disable Blocking Anonymous Call	



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

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

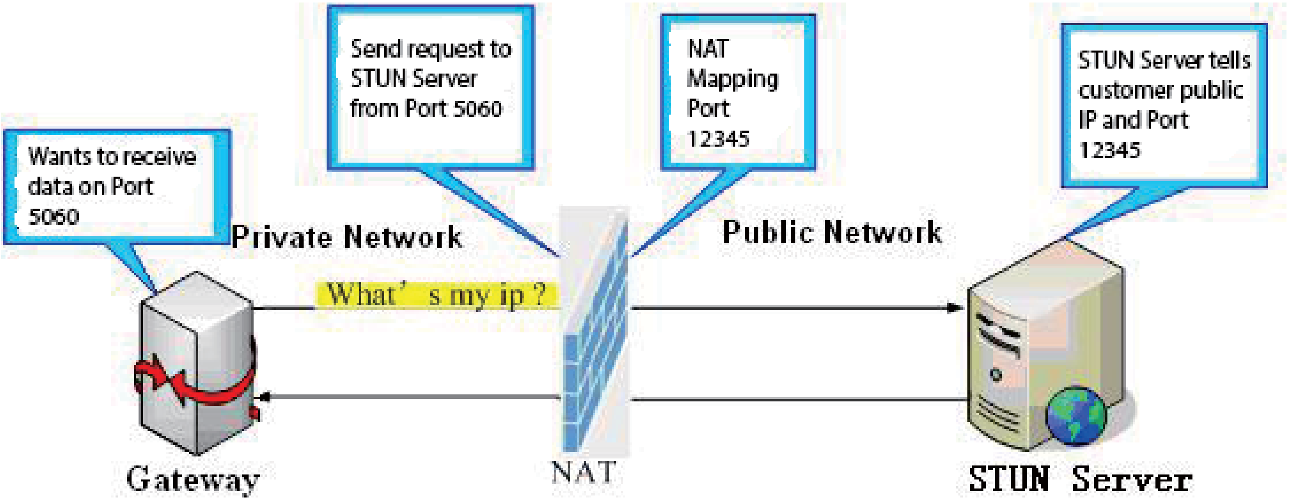
Activate	Whether the service of the line should be activated
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server
SIP Proxy Server Port	Enter the SIP proxy server port, default is 5060
Outbound proxy address	Enter the IP or FQDN address of outbound proxy server which are provided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

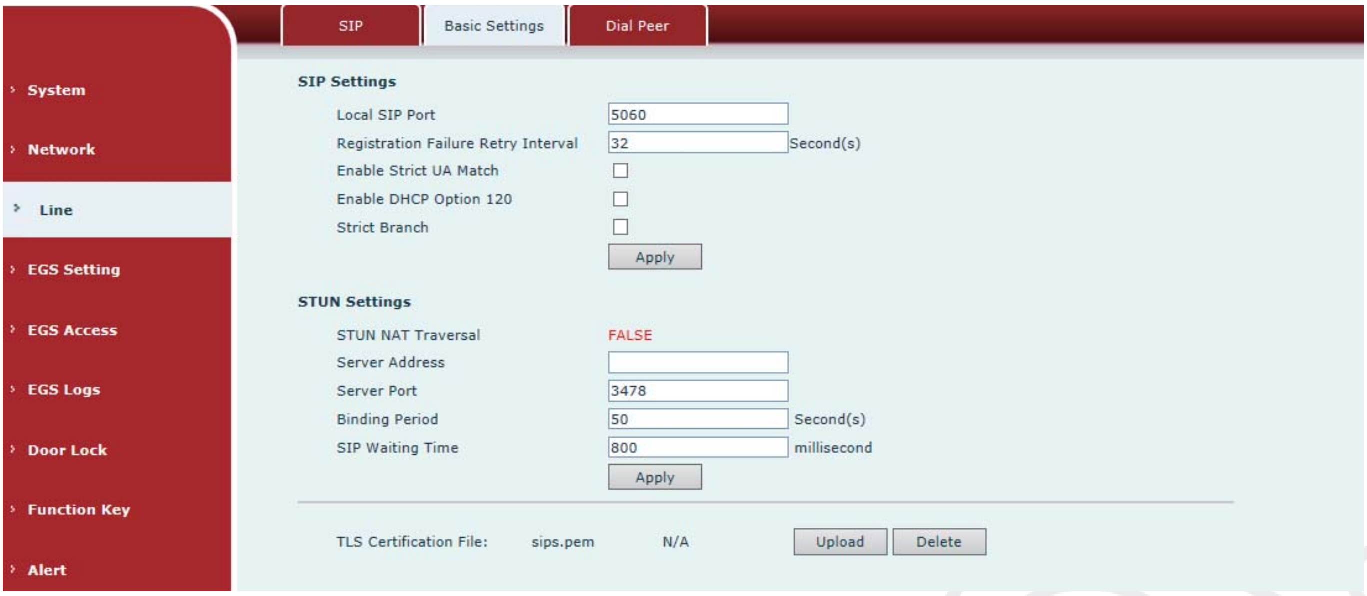
Enable Long Contact	Allow more parameters in contact field per RFC 3840.
Enable Use Inactive Hold	When Inactive Hold is enabled, the caller's SIP packet will with Inactive fields on the condition of holding a call.
Use Quote in Display Name	Whether to add quote in display name.
Use Feature Code	When this setting is enabled, the features in this section will not be handled by the device itself but by the server instead. In order to control the enabling of the features, the device will send feature code to the server by dialing the number specified in each feature code field.
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.
Local Port	Set the Local Port.
SIP Version	Set the SIP version.
Caller ID Header	Set the Caller ID Header.
Enable Strict Proxy	Enables the use of strict routing. When the phone receives packets from the server, it will use the source IP address, not the address in via field.
Enable user=phone	Sets user=phone in SIP messages.
Enable SCA	Enable/Disable SCA (Shared Call Appearance)
Enable DNS SRV	Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list.
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole opened.
Keep Alive Interval	Set the keep alive packet transmitting interval.
Sync Clock Time	Synchronize with server time.
Enable Session Timer	Set the line to enable call ending by session timer refreshment. The call session will be ended if there is not new session timer event update received after the timeout period.
Session Timeout	Set the session timer timeout period.
Enable rPort	Set the line to add rPort in SIP headers.
Enable PRACK	Set the line to support PRACK SIP message.

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

b) Basic Settings

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


Send request to STUN Server from Port 5060
NAT Mapping Port 12345
STUN Server tells customer public IP and Port 12345
Wants to receive data on Port 5060
Private Network
Public Network
What' s my ip ?
Gateway
NAT
STUN Server



SIP Settings

Local SIP Port	5060	
Registration Failure Retry Interval	32	Second(s)
Enable Strict UA Match	□	
Enable DHCP Option 120	□	
Strict Branch	□	

STUN Settings

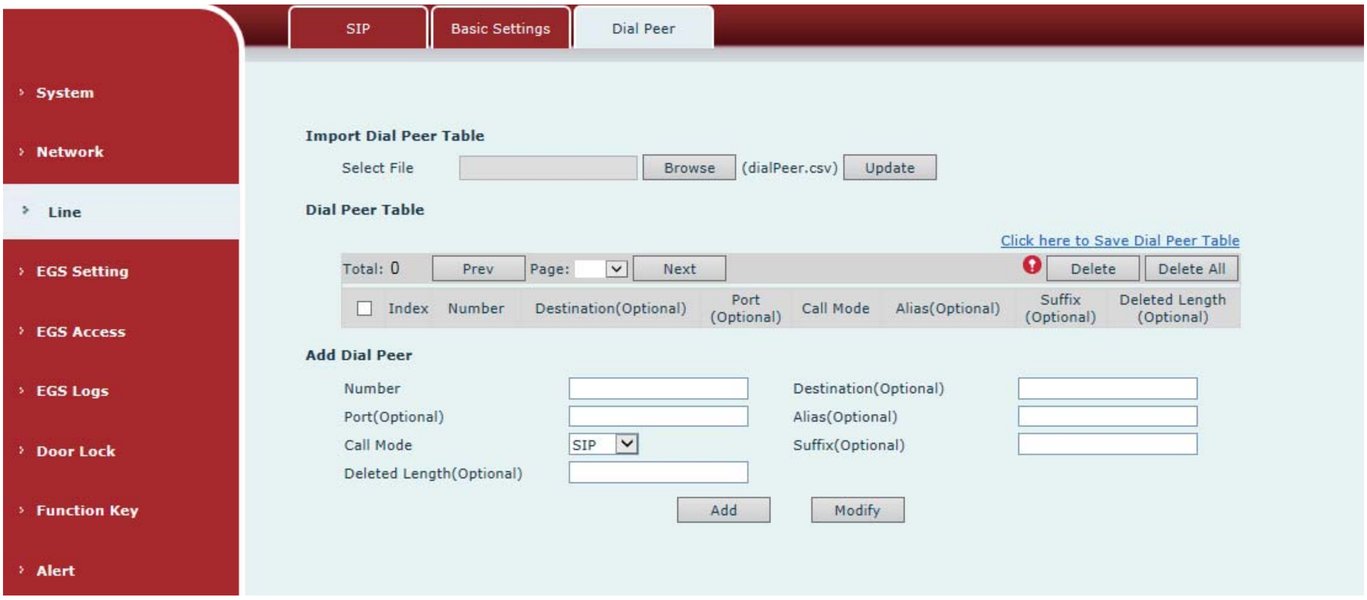
STUN NAT Traversal	FALSE	
Server Address		
Server Port	3478	
Binding Period	50	Second(s)
SIP Waiting Time	800	millisecond

TLS Certification File: sips.pem N/A

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

C) **Dial Peer**

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

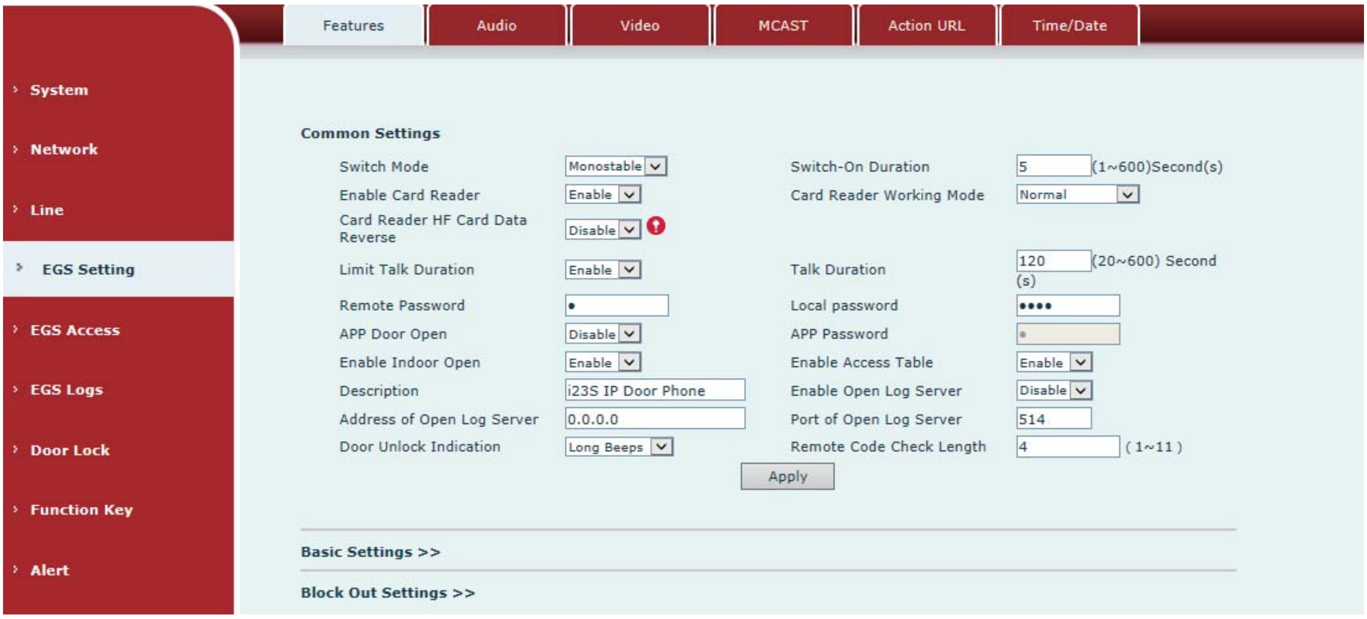


Import Dial peer Table	
Field Name	**Explanation**
Select File	Select an existing dialing rule file. The file type must be a .CSV
Add Dial Peer	
Number	To add an outgoing call number. The outgoing call number can be divided into two types: one is the exact match, and after the exact match, if the number is exactly the same as the user dialing the called number, the device will use the IP address of this number mapping or (This is the area code prefix function of the PSTN). If the number matches the N-bit (prefix number length) of the called number, the device uses the IP address or configuration mapped to this number. Make a call. Configuration prefix matching needs to be followed by a prefix number to match the exact match number; the longest support is 30 bits; also supports the use of x format and range of numbers.
Destination	Configure the destination address. If it’s configured as a point-to-point call, write the peer IP address directly. Can also be set to domain name, by the device DNS server to resolve the specific IP address. If it is not configured, the IP address is 0.0.0.0. This is an optional configuration item
Port	Configure the signaling port of the other party. This is an optional configuration item. The default is 5060
Alias	Configure aliases. This is an optional item: the replacement number will be used when the prefix is prefixed, and no alias when it is configured
Note: aliases are divided into four types and must be combined with the replacement length: 1) add: xxx, add xxx before the number. This can help users save dialing length; 2) all: xxx, all replaced by xxx; can achieve speed dial, such as user configuration dial-up 1, then by configuring all: number to change the actual call out the number; 3) del, delete the number before the n bit, n by the replacement length set;	

4) rep: xxx, the number n before the number is replaced by xxx, n is set by the replacement length. For example, if the user wants to dial the PSTN (010-62281493) through the floor service provided by the VoIP operator, and the actual call should be 010-62281493, then we can configure the called number 9T, then rep: 010, and then delete the length Set to 1. Then all users call the 9 at the beginning of the phone will be replaced with 010 + number sent. To facilitate the user to call the habit of thinking mode;	
Call Mode	Configuration selection of different signaling protocols, SIP;
Suffix	Configure the suffix, this is optional configuration items: that is, after the dial-up number to add this suffix, no configuration shows no suffix;
Deleted Length	Configure the replacement / delete length, the number entered by the user is replaced / deleted by this length; this is an optional configuration item;

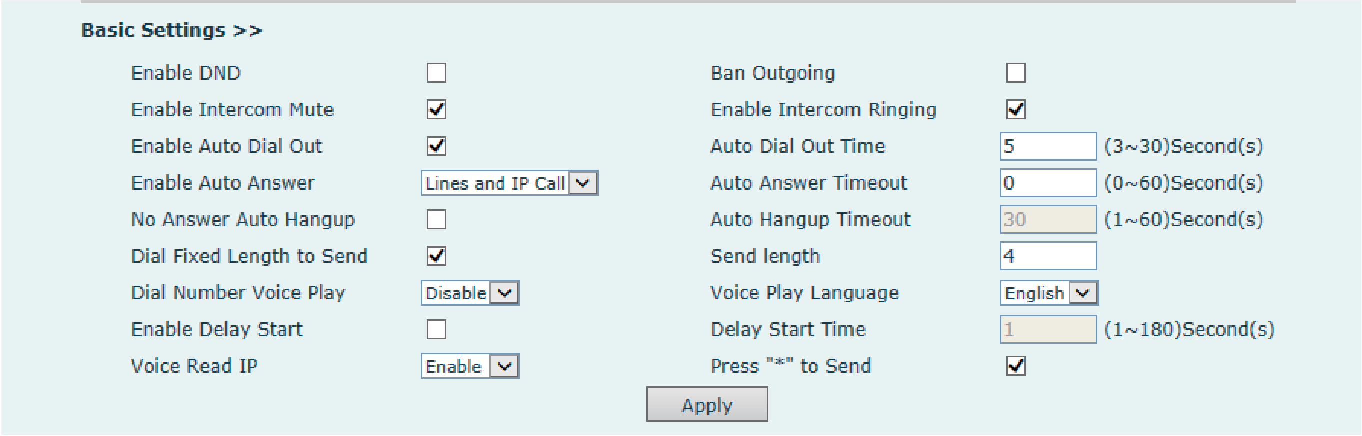
(4) EGS Setting

a) Features



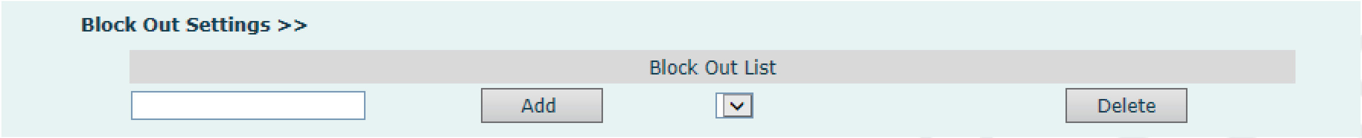
Common Settings

Switch Mode	Monostable	Switch-On Duration	5 (1~600)Second(s)
Enable Card Reader	Enable	Card Reader Working Mode	Normal
Card Reader HF Card Data Reverse	Disable		
Limit Talk Duration	Enable	Talk Duration	120 (20~600) Second (s)
Remote Password	•	Local password	••••
APP Door Open	Disable	APP Password	•
Enable Indoor Open	Enable	Enable Access Table	Enable
Description	i23S IP Door Phone	Enable Open Log Server	Disable
Address of Open Log Server	0.0.0.0	Port of Open Log Server	514
Door Unlock Indication	Long Beeps	Remote Code Check Length	4 (1~11)



Basic Settings >>

Enable DND	□	Ban Outgoing	□
Enable Intercom Mute	☑	Enable Intercom Ringing	☑
Enable Auto Dial Out	☑	Auto Dial Out Time	5 (3~30)Second(s)
Enable Auto Answer	Lines and IP Call	Auto Answer Timeout	0 (0~60)Second(s)
No Answer Auto Hangup	□	Auto Hangup Timeout	30 (1~60)Second(s)
Dial Fixed Length to Send	☑	Send length	4
Dial Number Voice Play	Disable	Voice Play Language	English
Enable Delay Start	□	Delay Start Time	1 (1~180)Second(s)
Voice Read IP	Enable	Press "*" to Send	☑



Block Out Settings >>

Block Out List

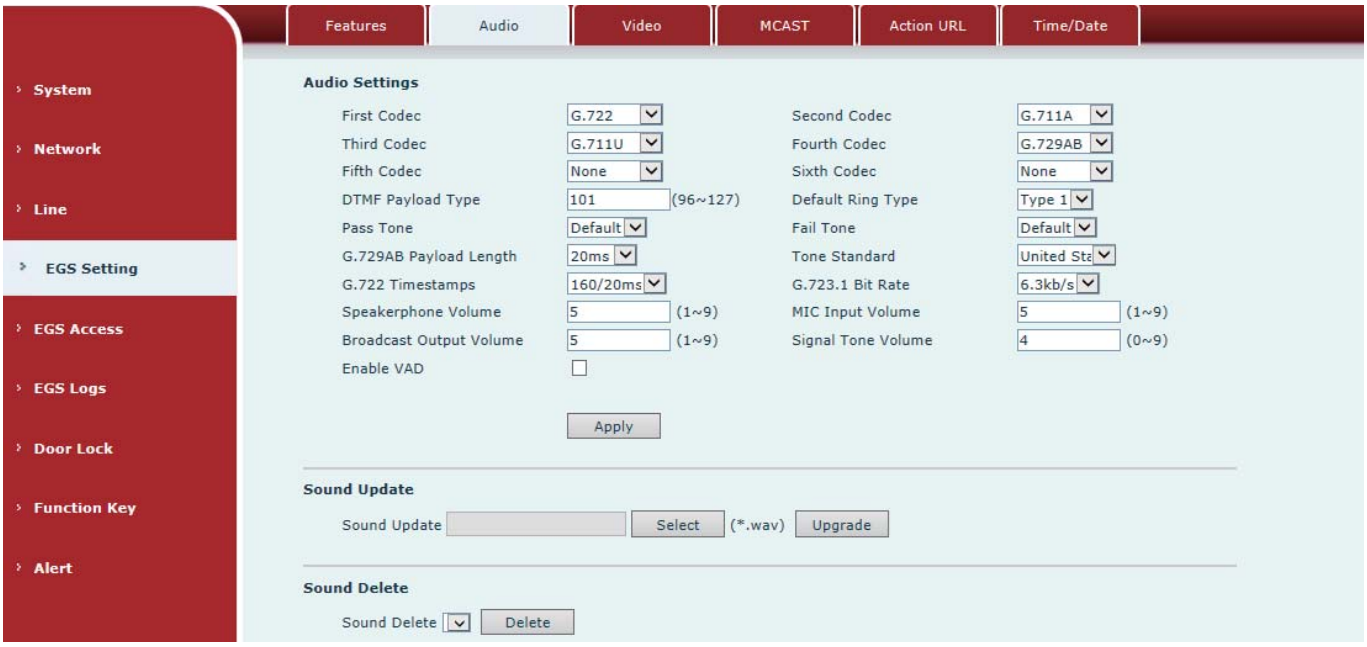
Features	
Field Name	**Explanation**
Common Settings	
Switch Mode	Monostable: there is only one fixed action status for door unlocking. See “Switch-On Duration” too. Bistable: there are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After changed, the status would be kept. default Value is Monostable
Switch-On Duration	Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Default Value is 5 seconds.
Enable Card Reader	Enable or disable card reader for RFID/IC cards.
Card Reader Working Mode	Set RFID/IC card stats: Normal: This is the work mode, in which user can use the authorized card can to open the door. Card Issuing: This is the issuing mode; the swiped card will be added in access list automatically. User could edit other parameters under EGS access. Card Revoking: This is the revoking mode; the swiped card will be deleted from Access List.
Card Reader HF Card Data Reverse	Set the format of HF card to make the data sequence reverse to meet with specific card.
Limit Talk Duration	If enabled, calls would be forced ended after talking time is up.
Talk Duration	The call will be ended automatically when time up. Initial Value is 120 seconds
Remote Password	Remote door unlocking password. Initial Value is “*”.
Local password	Local door unlocking password via keypad, the default password length is 4. Initial Value is “6789”.
APP Door Open	Enable or disable the APP Door Open.
APP password	APP door unlocking password. Initial Value is “*”.
Enable Indoor Open	Enable or disable to use indoor switch to unlock the door.
Enable Access Table	Enable Access Table: enter <Access Code> for opening door during calls. Disable Access Table: enter <Remote Password> for opening door during calls. Default Enable.
Description	Device description displayed on IP scanning tool software. Initial Value is “i23S IP Door Phone”.

Enable Open Log Server	Enable or disable to connect with log server.
Address of Open Log Server	Log server address (IP or domain name)
Port of Open Log Server	Log server port (0-65535), Initial Value is 514.
Door Unlock Indication	Indication tone for door unlocked. There are 3 types of tone: silent/short beeps/long beeps.
Remote Code Check Length	The remote access code length would be restricted with it. If the input access code length is matched with it, system would check it immediately. Initial Value is 4.
Basic Settings	
Enable DND	DND might be disabled phone for all SIP lines, or line for SIP individually. But the outgoing calls will not be affected.
Ban Outgoing	If enabled, no outgoing calls can be made.
Enable Intercom Mute	If enabled, mutes incoming calls during an intercom call.
Enable Intercom Ringing	If enabled, plays intercom ring tone to alert to an intercom call.
Enable Auto Dial Out	Enable Auto Dial Out.
Auto Dial Out Time	Set Auto Dial Out Time.
Enable Auto Answer	Enable Auto Answer function.
Auto Answer Timeout	Set Auto Answer Timeout.
No Answer Auto Hangup	Enable automatically hang up when no answer.
Auto Hangup Timeout	Configuration in a set time, automatically hang up when no answer.
Dial Fixed Length to Send	Enable or disable dial fixed length to send.
Send length	The number will be sent to the server after the specified numbers of digits are dialed.
Dial Number Voice Play	Configuration Open / Close Dial Number Voice Play.
Voice Play Language	Set language of the voice prompt.
Enable Delay Start	Enable or disable the start delay.
Delay Start Time	Set start delay time.
Voice Read IP	Enable or disable voice broadcast IP address.
Press "*" to Send	Enable or disable the Press "*" to Send, Initial Value is enable.
Block Out Settings	

Add or delete blocked numbers – enter the prefix of numbers which should not be dialed by the phone. For example, if 001 is entered, the phone would not dial any number beginning with 001. X and x are wildcards which match single digit. For example, if 4xxx or 4XXX is entered, the phone would not dial any 4 digits numbers beginning with 4. It would dial numbers beginning with 4 which are longer or shorter than 4 digits.

b) Audio

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



Audio Settings

First Codec	G.722	Second Codec	G.711A
Third Codec	G.711U	Fourth Codec	G.729AB
Fifth Codec	None	Sixth Codec	None
DTMF Payload Type	101 (96~127)	Default Ring Type	Type 1
Pass Tone	Default	Fail Tone	Default
G.729AB Payload Length	20ms	Tone Standard	United Sta
G.722 Timestamps	160/20ms	G.723.1 Bit Rate	6.3kb/s
Speakerphone Volume	5 (1~9)	MIC Input Volume	5 (1~9)
Broadcast Output Volume	5 (1~9)	Signal Tone Volume	4 (0~9)
Enable VAD	□		

Sound Update

Sound Update (*.wav)

Sound Delete

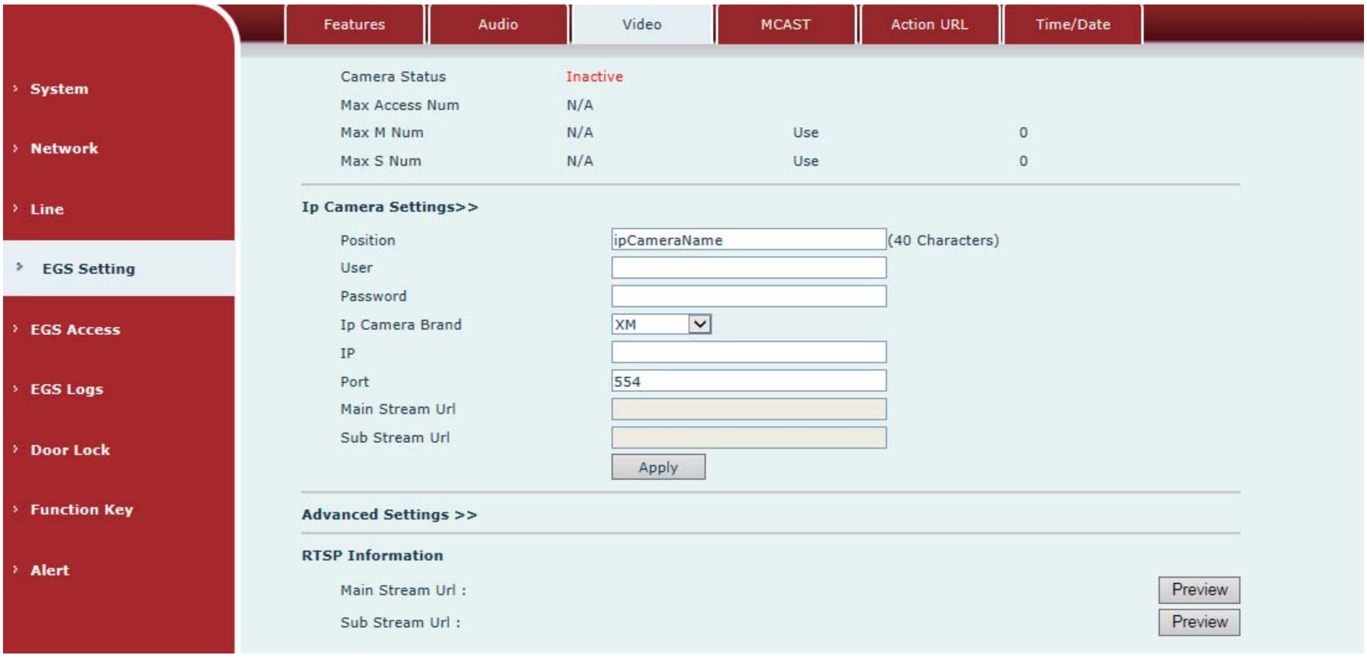
Sound Delete

Audio Setting	
Field Name	**Explanation**
First Codec	The first codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB
Second Codec	The second codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, None
Third Codec	The third codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, None
Fourth Codec	The forth codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, None
DTMF Payload Type	The RTP Payload type that indicates DTMF. Default is 101
Default Ring Type	Ring Sound – There are 9 standard types and 3 User types.
Pass Tone	When the door opened successfully, the device will play the correct tone set by the user.
Fail Tone	When the door fails to open, the terminal will play an error tone set by the user.

G.729AB Payload Length	G.729AB Payload Length – Adjusts from 10 – 60 ms.
Tone Standard	Configure tone standard area.
G.722 Timestamps	Choices are 160/20ms or 320/20ms.
G.723.1 Bit Rate	Choices are 5.3kb/s or 6.3kb/s.
Speakerphone Volume	Set the speaker calls the volume level.
MIC Input Volume	Set the MIC calls the volume level.
Broadcast Output Volume	Set the broadcast the output volume level.
Signal Tone Volume	Set the audio signal the output volume level.
Enable VAD	Enable or disable Voice Activity Detection (VAD). If VAD is enabled, G729 Payload length cannot be set greater than 20 ms.

c) Video

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



Camera Status Inactive
Max Access Num N/A
Max M Num N/A Use 0
Max S Num N/A Use 0

Ip Camera Settings>>

Position ipCameraName (40 Characters)
User
Password
Ip Camera Brand XM
IP
Port 554
Main Stream Url
Sub Stream Url

Advanced Settings >>

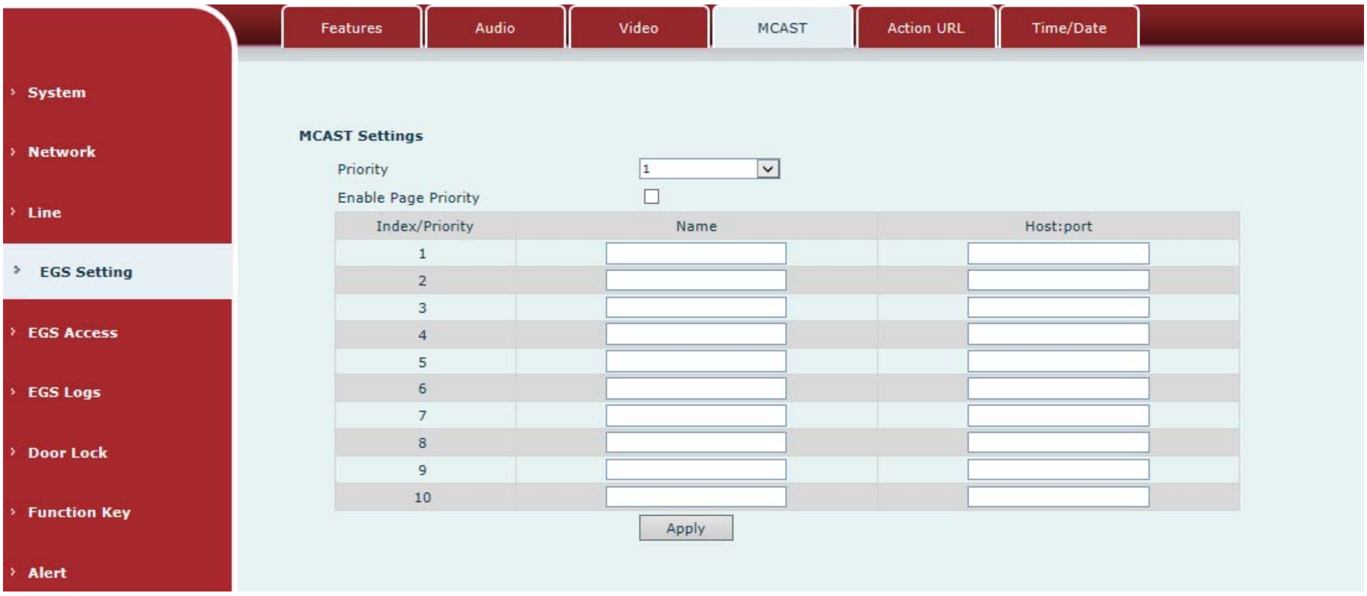
RTSP Information

Main Stream Url :
Sub Stream Url :

Video	
Field Name	**Explanation**
Camera Status：Display the relevant information of the camera, including maximum access, maximum stream, maximum sub stream, and the status.	
IP Camera Settings	
Position	Set IP Camera Name.
User name	External camera login required account.
Password	External camera login password required.

IP Camera Brand	Select the camera manufacturers.
IP address	IP address of the camera, please use the camera matching scan tool to obtain the IP address.
Port	Camera port number.
Advanced Settings	
Video Direction	Select the transport type of the video stream.
H.264 Payload Type	Set the payload type of H.264.
RTSP information	Click [Apply], the connection automatically shows the camera does not show the reverse.
Preview	Copy and paste the main stream or sub-stream URL into the VLC player, or click [Preview] to display the current camera video.

d) MCAST



MCAST Settings

Priority: 1

Enable Page Priority ☐

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

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

MCAST Settings

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

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

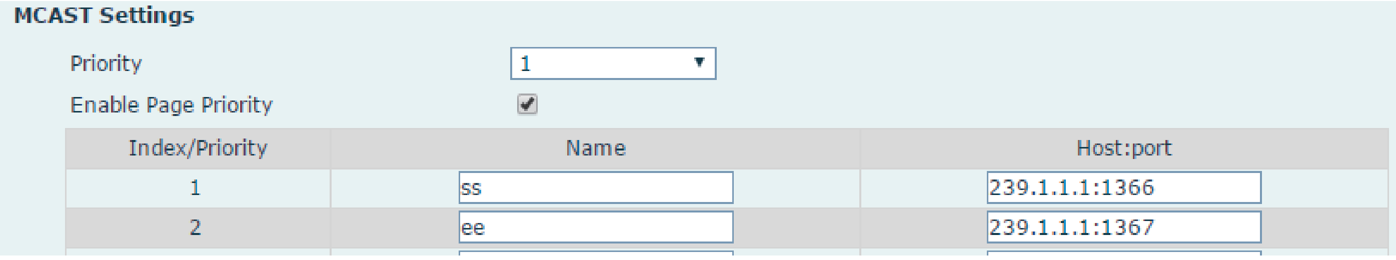
- Priority:

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

- The options are as follows:
  - ✧ 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
  - ✧ Enable the page priority:

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

- Web Settings:



MCAST Settings

Priority: 1 ▼

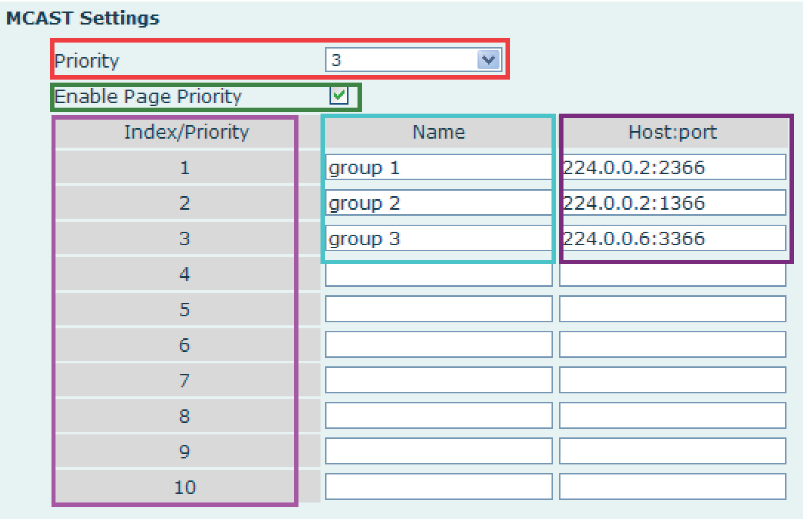
Enable Page Priority: ☑

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



MCAST 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.

✧ All equipment has one or more common non-multicast communication.

✧ When you set the Priority for the disable, multicast any level will not answer, multicast call is rejected.

✧ when you set the Priority to a value, only higher than the priority of multicast can come in, if you set the Priority is 3, group 2 and group 3 for priority level equal to 3 and less than 3 were rejected, 1 priority is 2 higher than ordinary call priority device can answer the multicast message at the same time, keep the hold the other call.

- **Green part (Enable Page priority)**

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

✧ The purpose of setting monitoring multicast "group 1" or "3" set up listening "group of 1" or "3" multicast address multicast call.

✧ All equipment has been a path or multi-path multicast phone, such as listening to "multicast information group 2".

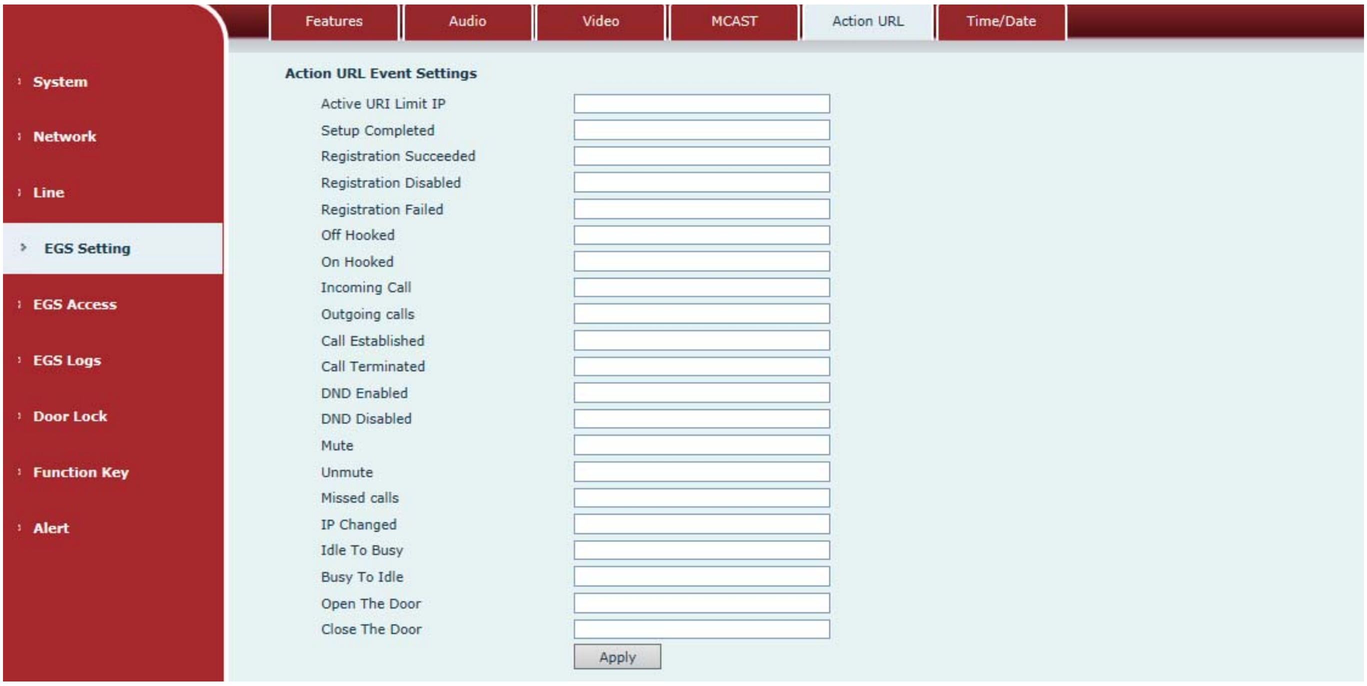
✧ If multicast is a new "group of 1", because "the priority group 1" is 2, higher than the current call "priority group 2" 3, so multicast call will can come in.

- ✧ If multicast is a new "group of 3", because "the priority group 3" is 4, lower than the current call "priority group 2" 3, "1" will listen to the equipment and maintain the "group of 2".

Multicast service

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

e) Action URL

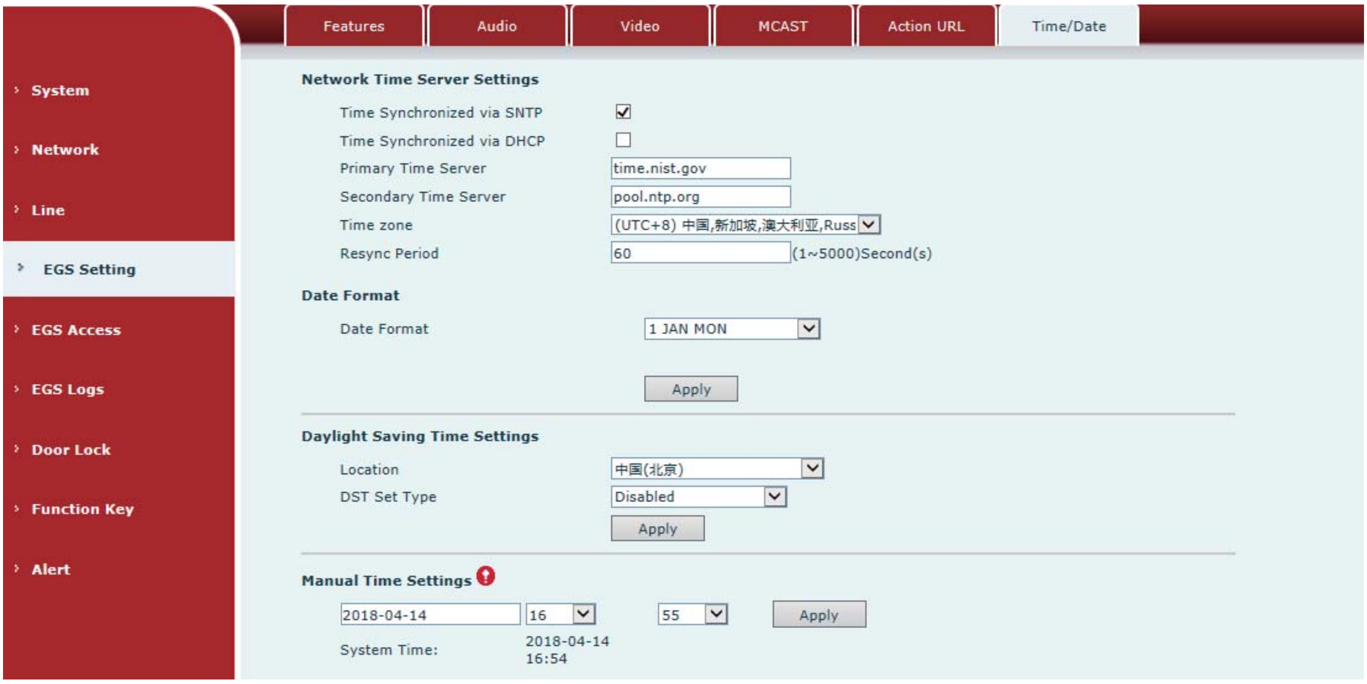


Action URL Event Settings

Active URI Limit IP
Setup Completed
Registration Succeeded
Registration Disabled
Registration Failed
Off Hooked
On Hooked
Incoming Call
Outgoing calls
Call Established
Call Terminated
DND Enabled
DND Disabled
Mute
Unmute
Missed calls
IP Changed
Idle To Busy
Busy To Idle
Open The Door
Close The Door

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

f) Time/Date



Network Time Server Settings

Time Synchronized via SNTP	☑
Time Synchronized via DHCP	□
Primary Time Server	time.nist.gov
Secondary Time Server	pool.ntp.org
Time zone	(UTC+8) 中国,新加坡,澳大利亚,Russ
Resync Period	60 (1~5000)Second(s)

Date Format

Date Format	1 JAN MON

Daylight Saving Time Settings

Location	中国(北京)
DST Set Type	Disabled

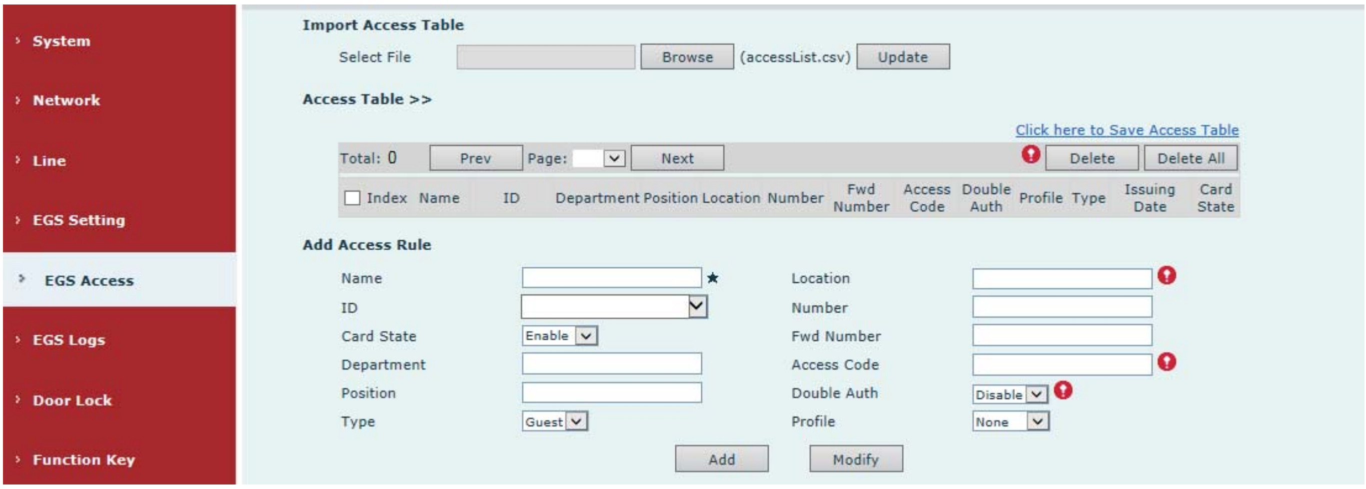
Manual Time Settings

2018-04-14 16 55

System Time: 2018-04-14 16:54

Time/Date	
Field Name	**Explanation**
Network Time Server Settings	
Time Synchronized via SNTP	Enable time-sync through SNTP protocol
Time Synchronized via DHCP	Enable time-sync through DHCP protocol
Primary Time Server	Set primary time server address
Secondary Time Server	Set secondary time server address, when primary server is not reachable, the device will try to connect to secondary time server to get time synchronization.
Time zone	Select the time zone
Resync Period	Time of re-synchronization with time server
Date Format	
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 manually input rules
Manual Time Settings	
The time set by hand, need to disable SNTP service first.	
Daylight Saving Time Settings	

(5) EGS Access



Import Access Table

Select File [ ] Browse (accessList.csv) Update

Access Table >>

Click here to Save Access Table

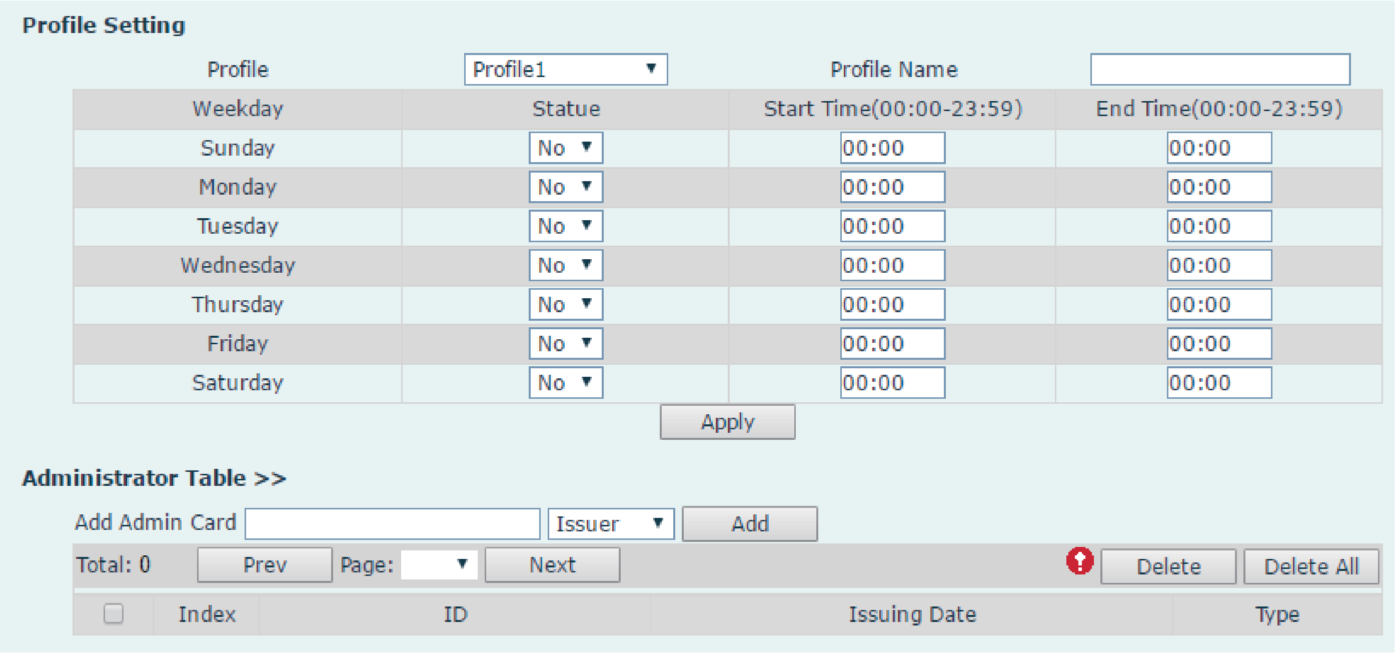
Total: 0 Prev Page: Next Delete Delete All

□	Index	Name	ID	Department	Position	Location	Number	Fwd Number	Access Code	Double Auth	Profile	Type	Issuing Date	Card State

Add Access Rule

Name	★	Location	
ID		Number	
Card State	Enable	Fwd Number	
Department		Access Code	
Position		Double Auth	Disable
Type	Guest	Profile	None

Add Modify



Profile Setting

Profile: Profile1 Profile Name: [ ]

Weekday	Statue	Start Time(00:00-23:59)	End Time(00:00-23:59)
Sunday	No	00:00	00:00
Monday	No	00:00	00:00
Tuesday	No	00:00	00:00
Wednesday	No	00:00	00:00
Thursday	No	00:00	00:00
Friday	No	00:00	00:00
Saturday	No	00:00	00:00

Apply

Administrator Table >>

Add Admin Card [ ] Issuer Add

Total: 0 Prev Page: Next Delete Delete All

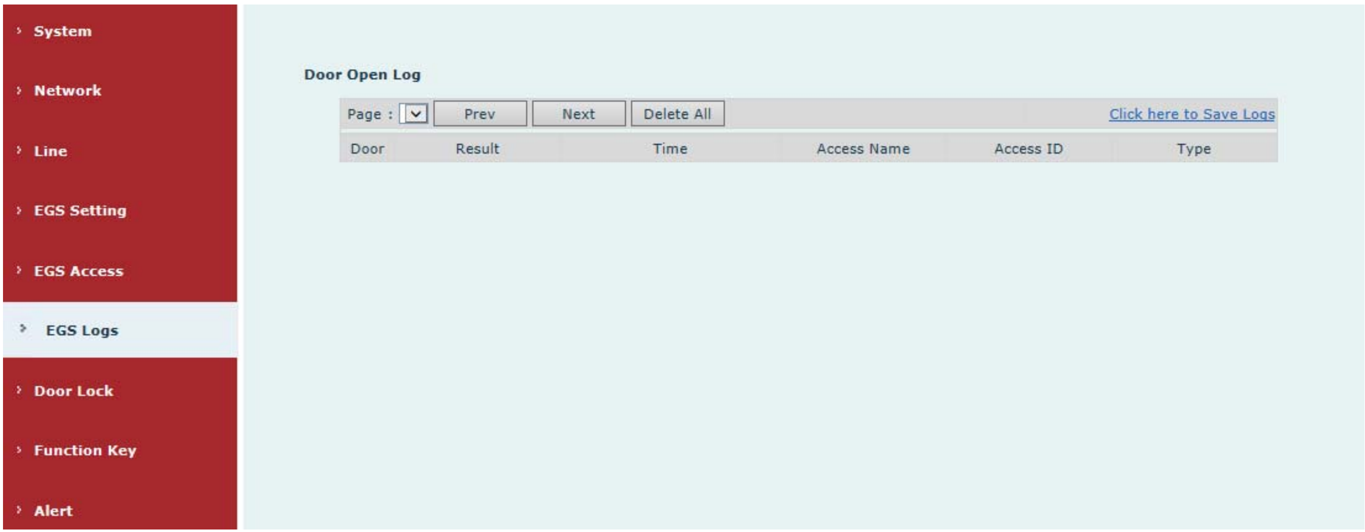
□	Index	ID	Issuing Date	Type

EGS Access	
Field Name	**Explanation**
Import Access Table	
Click the <Browse> to choose to import remote access list file (access List.csv) and then clicking <Update> can batch import remote access rule.	
Access Table	
According to entrance guard access rules have been added, you can choose single or multiple rules on this list to delete operation.	
Add Access Rule	
Name(necessary)	User name
Location	Virtual extension number, used to make position call instead of real number. It might be taken with unit number, or room number.
ID	RFID/IC card number. You can manually fill in the first 10 digits of the card number or select the existing card number

Number	User phone number
Card State	Enable or disable holder's RFID card
Fwd Number	Call forwarding number when above phone number is unavailable.
Department	Card holder's department
Access Code	1/ When the door phone answers the call from the corresponding <Phone Num> user, then the <Phone Num> user can input the access code via keypad to unlock the door remotely. 2/ The user’s private password should be input via keypad for local door unlocking. The private password format is **Location** * **Access Code.**
Position	Card holder's position
Double Auth	When the feature is enabled, private password inputting and RFID reading must be matched simultaneously for door unlocking.
Type	Host: the door phone would answer all call automatically. Guest: the door phone would ring for incoming call, if the auto answer is disabled.
Profile	It is valid for user access rules (including RFID/IC, access code, etc.) within corresponding time section. If NONE is selected, the feature would be taken effect all day.
Profile Setting	
Profile	There are 4 sections for time profile configuration
Profile Name	The name of profile to help administrator to remember the time definition
Status	If it is yes, the time profile would be taken effect. Other time sections not included in the profiles would not allow users to open door
Start Time	The start time of section
End Time	The end time of section
Administrator Table	
Add Admin Card	You should input the top 10 digits of RFID card numbers. for example, 0004111806, selected the type of admin card, click <add>.
Type: Issuer and revocation When entrance guard is in normal state, swipe card (issuing card) would make entrance guard into the issuing state, and then you can swipe a new card, which the card would be added into the database; when you swipe the issuing card again after cards added done, entrance guard would return to normal state. Delete card operation is the same with issuing card. The device can support up to 10 admin cards, 1000 copies of ordinary cards. Note: in the issuing state, swiping deleted card is invalid.	
Shows the ID, Issuing Date and Type of admin card	
Delete	Clicking <Delete> would delete the selected admin card in the list.
Delete All	Click <Delete All>, to delete all admin card lists.

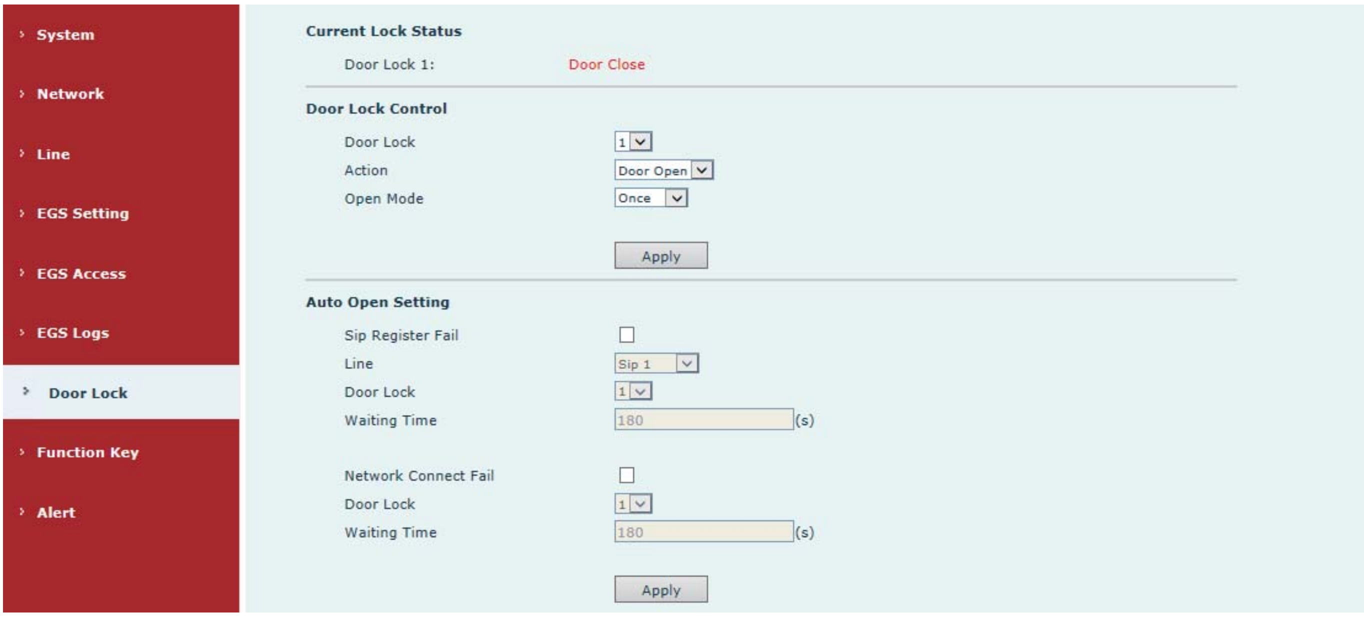
(6) EGS Logs

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



Field Name	Explanation
Door Open Log	
Result	Show the results of the open the door (Succeeded or Failed)
Time	The time of opening door.
Access Name	If the door was opened by swipe card or remote unlocking door, the device would display remote access name.
Access ID	1. If the opening door method is swiping card, it wound display the card number 2. If the opening door way is remote access, it wound display the remote extension's number. 3. If the opening door way is local access, there is no display information.
Type	Open type: 1. Local, 2. Remote, 3. Brush card (Temporary Card, Valid Card and Illegal Card). Note: there are three kinds of brushing card feedback results. 1. Temporary Card (only added) the card number, without adding other rules) 2. Valid Card (added access rules) 3. Illegal Card (Did not add information)

(7) Door Lock



Current Lock Status

Door Lock 1: Door Close

Door Lock Control

Door Lock: 1

Action: Door Open

Open Mode: Once

Auto Open Setting

Sip Register Fail: □

Line: Sip 1

Door Lock: 1

Waiting Time: 180 (s)

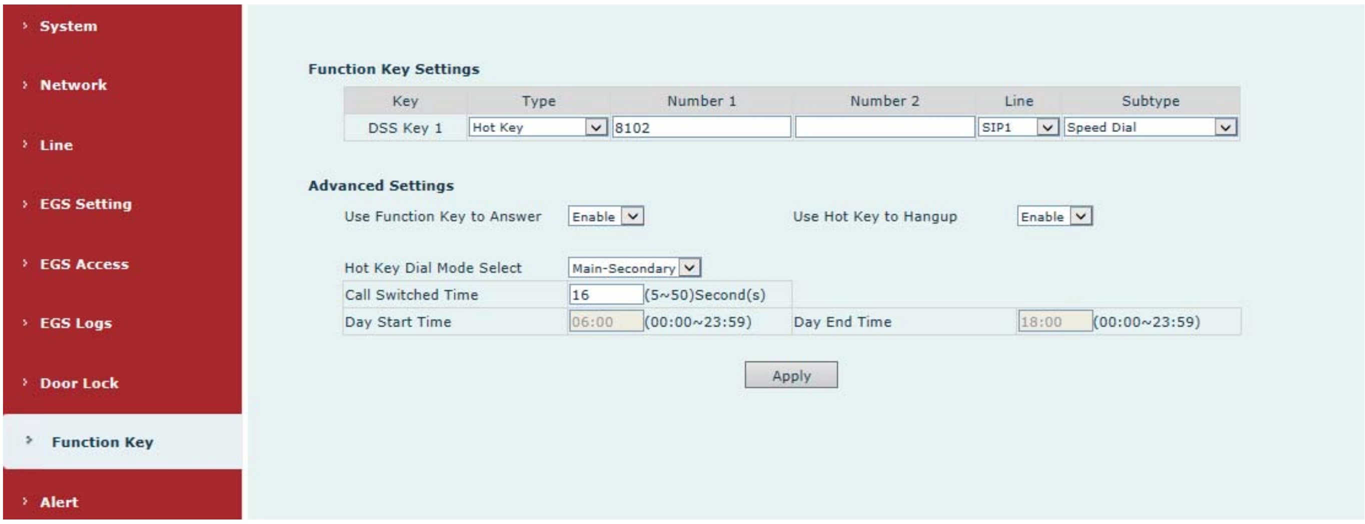
Network Connect Fail: □

Door Lock: 1

Waiting Time: 180 (s)

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

(8) Function Key



Function Key Settings

Key	Type	Number 1	Number 2	Line	Subtype
DSS Key 1	Hot Key	8102		SIP1	Speed Dial

Advanced Settings

Use Function Key to Answer: Enable

Use Hot Key to Hangup: Enable

Hot Key Dial Mode Select: Main-Secondary

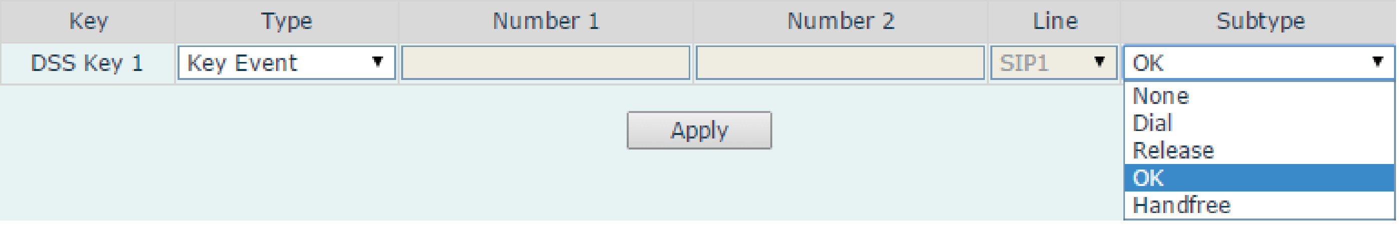
Call Switched Time: 16 (5~50)Second(s)

Day Start Time: 06:00 (00:00~23:59)

Day End Time: 18:00 (00:00~23:59)

➢ Key Event

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

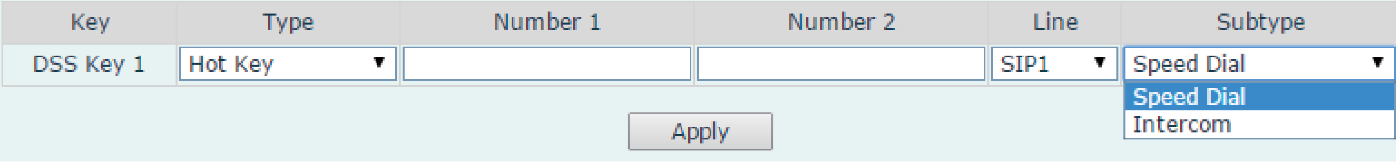


Key	Type	Number 1	Number 2	Line	Subtype
DSS Key 1	Key Event			SIP1	OK

Type	Subtype	Usage
Key Event	None	No responding
	Dial	Dialing function
	Release	Delete password input, cancel dialing input and end call
	OK	identification key

➢ Hot Key

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



Key	Type	Number 1	Number 2	Line	Subtype
DSS Key 1	Hot Key			SIP1	Speed Dial

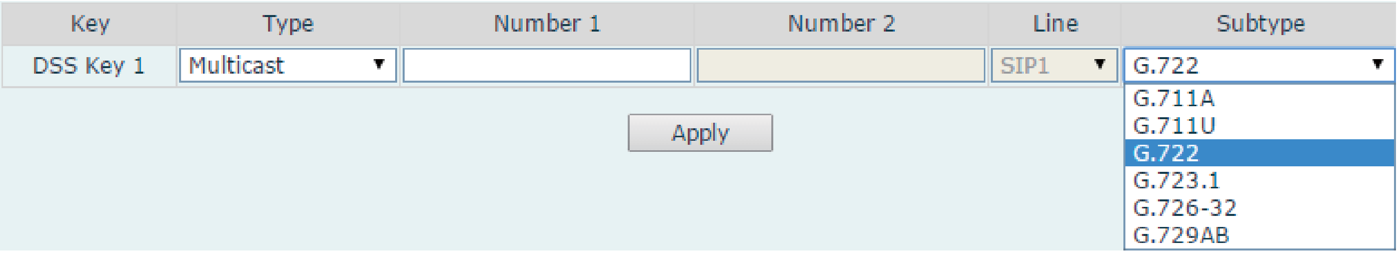
Type	Number	Line	Subtype	Usage
Hot Key	Fill the called party's SIP	The SIP account correspond	Speed Dial	Using Speed Dial mode together with Enable Speed Dial Hangup Enable, can define whether this call is allowed to be hung up

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

➢ Multicast

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

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



Key	Type	Number 1	Number 2	Line	Subtype
DSS Key 1	Multicast			SIP1	G.722

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

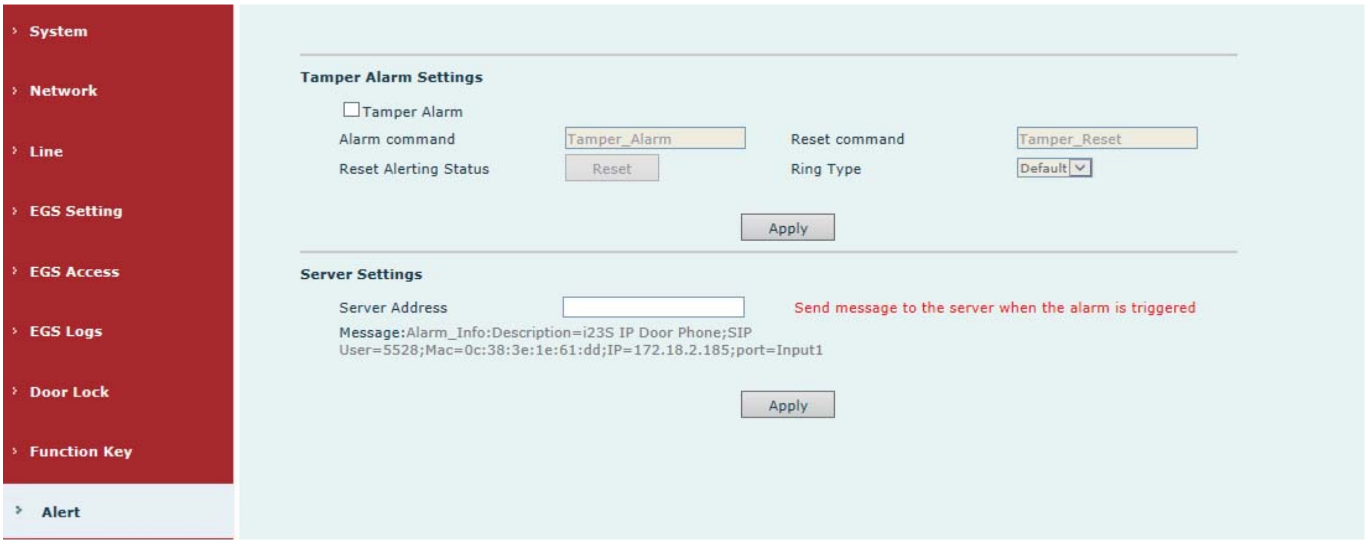
✧ operation mechanism

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

✧ calling configuration

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

(9) Alert



Tamper Alarm Settings

□ Tamper Alarm

Alarm command: Tamper_Alarm

Reset command: Tamper_Reset

Reset Alerting Status

Ring Type: Default

Server Settings

Server Address

Send message to the server when the alarm is triggered

Message:Alarm_Info:Description=i23S IP Door Phone;SIP User=5528;Mac=0c:38:3e:1e:61:dd;IP=172.18.2.185;port=Input1

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

E. Appendix

1. Technical parameters

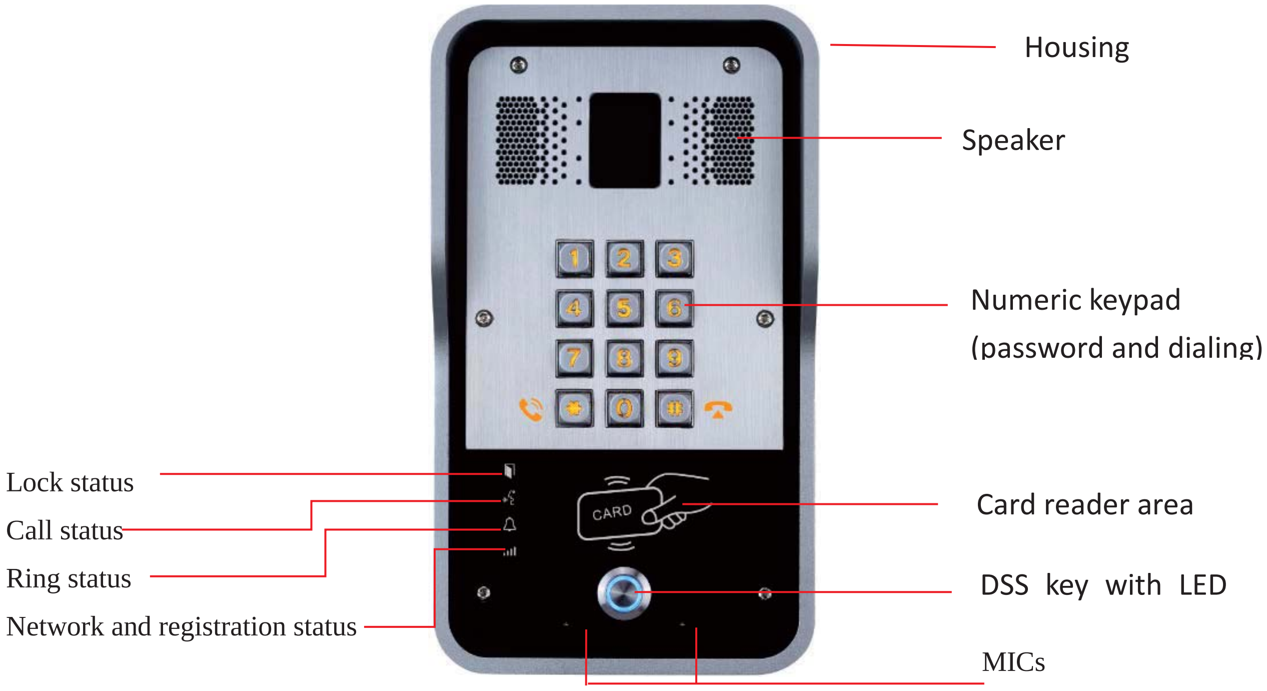
Communication protocol		SIP 2.0(RFC-3261)
Main chipset		Broadcom
Keys	**DSS Key**	1 (Stainless steel)
	Numeric keyboard	Support
Audio	**MIC**	1
	Speaker	3W/4Ω
	Volume control	Adjustable
	Full duplex speakerphone	Support (AEC)

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

2. Basic functions

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

3. Schematic diagram

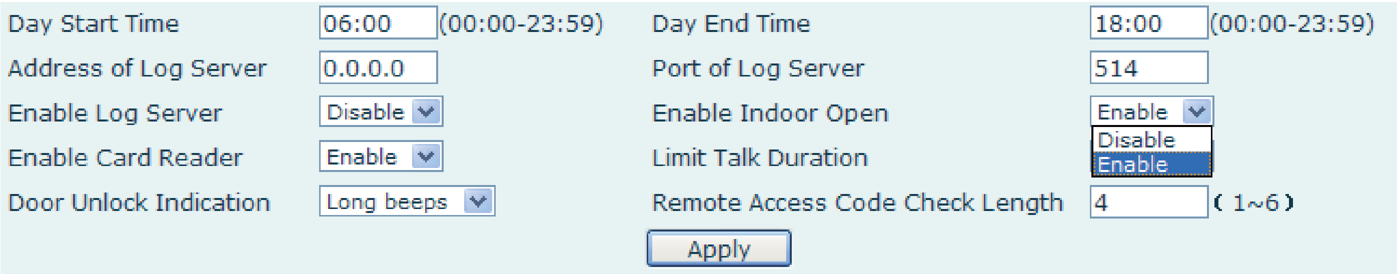


F. Other instructions

1. Open door modes

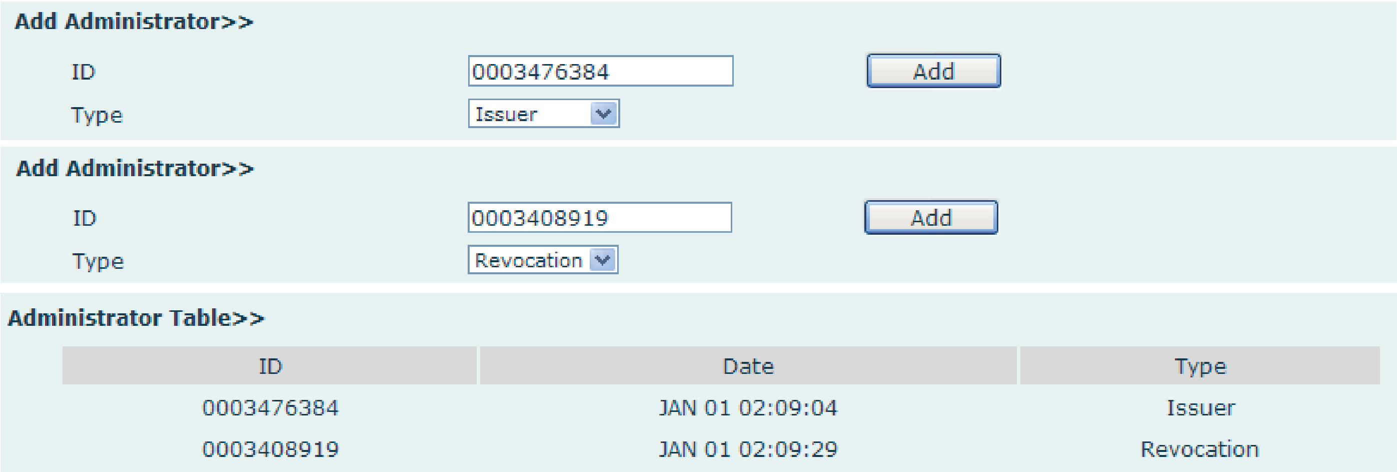
- **Local**

✧ Press indoor switch, which is installed and connected with device, to unlock the door.



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

2. Management of card



Add Administrator>>

ID	0003476384	Add
Type	Issuer	

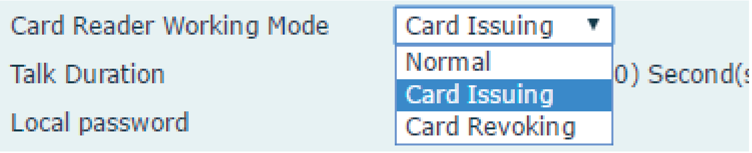
Add Administrator>>

ID	0003408919	Add
Type	Revocation	

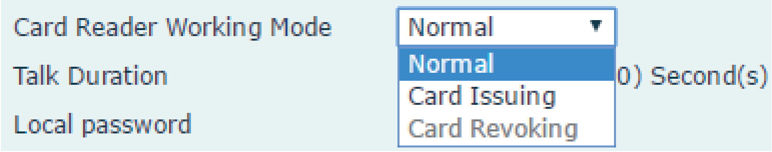
Administrator Table>>

ID	Date	Type
0003476384	JAN 01 02:09:04	Issuer
0003408919	JAN 01 02:09:29	Revocation

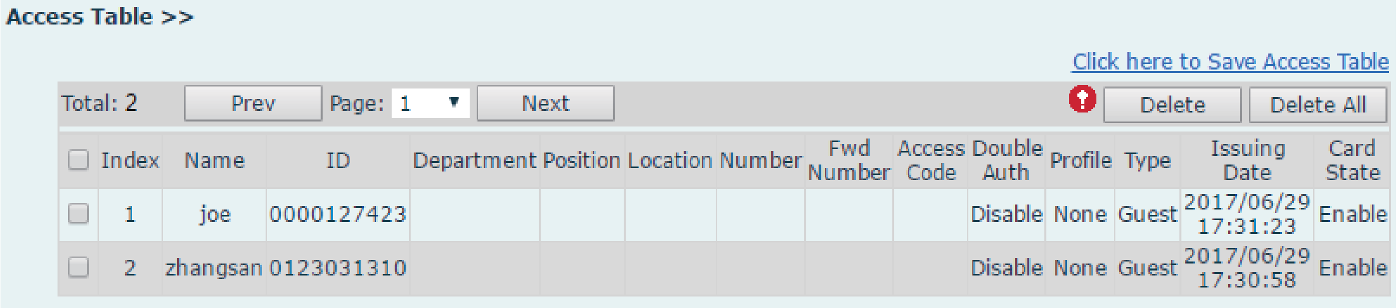
Method 1: used to add cards for starters typically



Card Reader Working Mode	Card Issuing ▼
Talk Duration	0) Second(s
Local password	



Card Reader Working Mode	Normal ▼
Talk Duration	0) Second(s)
Local password	



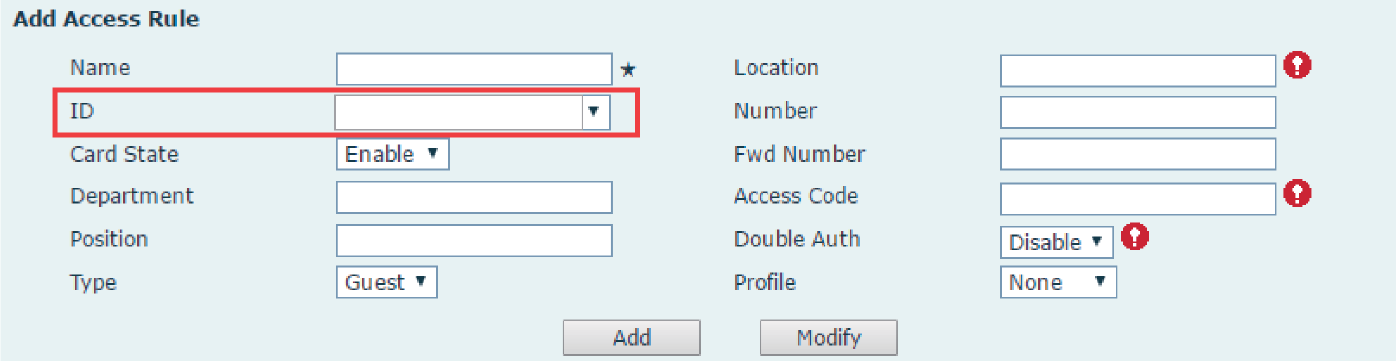
Access Table >>

Click here to Save Access Table

□	Index	Name	ID	Department	Position	Location	Number	Fwd Number	Access Code	Double Auth	Profile	Type	Issuing Date	Card State
□	1	joe	0000127423							Disable	None	Guest	2017/06/29 17:31:23	Enable
□	2	zhangsan	0123031310							Disable	None	Guest	2017/06/29 17:30:58	Enable

Method 2: used to add cards for professionals

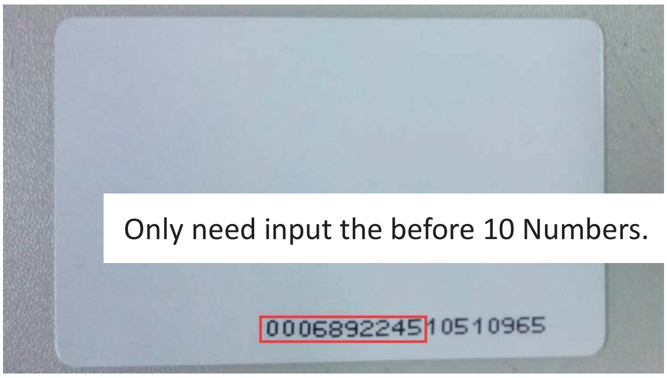
Methods 3: use to add few cards



Add Access Rule

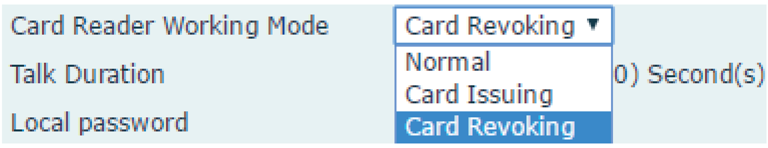
Name	★	Location	
ID	▼	Number	
Card State	Enable ▼	Fwd Number	
Department		Access Code	
Position		Double Auth	Disable ▼
Type	Guest ▼	Profile	None ▼

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

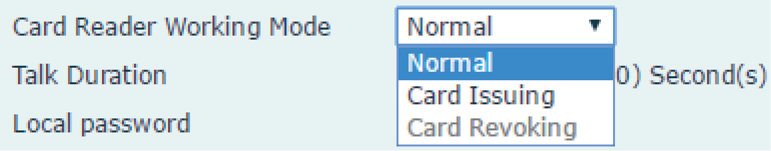


Only need input the before 10 Numbers.

Method 1: used to batch delete cards for starters.



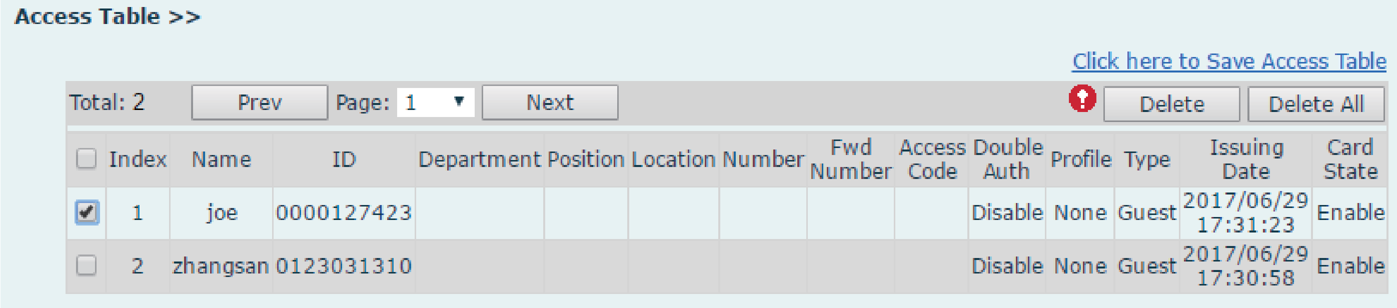
Card Reader Working Mode	Card Revoking ▼
Talk Duration	0) Second(s)
Local password	



Card Reader Working Mode	Normal ▼
Talk Duration	0) Second(s)
Local password	

Method 2: used to batch add cards for intermediates.

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



Access Table >>

Click here to Save Access Table

☐	Index	Name	ID	Department	Position	Location	Number	Fwd Number	Access Code	Double Auth	Profile	Type	Issuing Date	Card State
☑	1	joe	0000127423							Disable	None	Guest	2017/06/29 17:31:23	Enable
☐	2	zhangsan	0123031310							Disable	None	Guest	2017/06/29 17:30:58	Enable