i30 IP Video Door Phone

User Manual V3.0

Document VER	**Firmware VER**	**Explanation**	**Time**
V1.0	2.1.1.2545	Initial issue	20161117
V2.0	2.1.1.2909	Add FDMS, video linkage function. Changed default in passive mode to the electric-lock.	20170726
V3.0	2.1.1.2909	Change company address and add IP scan tool download address in QIG	20171027

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 would 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

I. **Product introduction** 6
1. **Appearance of the product** 6
2. **Description** 7

II. **Start Using** 8
1. **Confirm the connection** 8
1) **Power, Electric Lock, Indoor switch port** 8
2) **Driving mode of electric-lock(Default in passive mode)** 8
3) **Wiring instructions** 9
2. **Quick Setting** 10

III. **Basic operation** 11
1. **Answer a call** 11
2. **Call** 11
3. **End call** 11
4. **Open the door** 11

IV. **Page settings** 12
1. **Browser configuration** 12
2. **Password Configuration** 12
3. **Configuration via WEB** 13
(1) **System** 13
a) **Information** 13
b) **Account** 14
c) **Configurations** 15
d) **Upgrade** 15
e) **Auto Provision** 16
f) **FDMS** 18
g) **Tools** 19
(2) **Network** 20
a) **Basic** 20
b) **VPN** 22
(3) **Line** 23
a) **SIP** 23
b) **Basic Settings** 28
c) **Dial Peer** 30

(4) **EGS Setting** 31

a) **Features**........ 31

a) **Audio**........ 34

b) **Video**........ 35

c) **MCAST** 38

d) **Action URL**........ 41

e) **Time/Date** 41

(5) **EGS Access**........ 43

(6) **EGS Logs** 45

(7) **Function Key** 46

V. **Appendix** 49

1. **Technical parameters**........ 49
2. **Basic functions** 50
3. **Schematic diagram** 50

VI. **Other instructions**........ 51

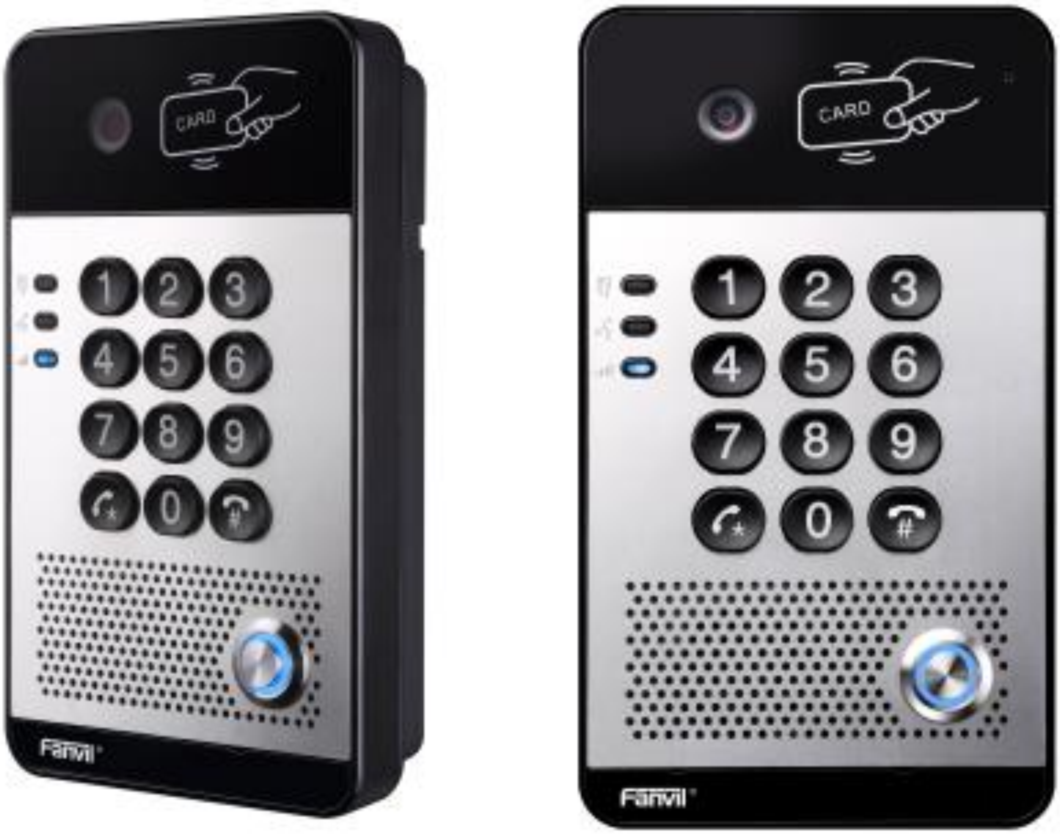
1. **Open door modes**........ 51
2. **Management of card** 51

I. Product introduction

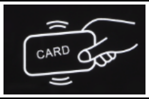
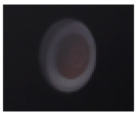
i30 is a full digital network door phone. It uses mature VoIP solution (Broadcom chip), with stable and reliable performance; it supports hands-free with full-duplex, which voice is loud and clear; I30 have generous appearance, also solid durable, easy for installation, comfortable keypad and low power consumption.

I30 video door phone supports entrance guard control, voice intercom, ID card and keypad remote opening the door.

1. Appearance of the product



2. Description

Buttons and icons	Description	Function
	Numeric keyboard	Input password to open the door or dial for call
	Programmable keys	It can be set with a variety of functions in order to meet the needs of different occasions
	Induction zone	RFID induction area
	Camera	Video signal acquisition and transmission
	Lock status	Door unlocking: On Door locking: Off
	Call/Ring status	Standby: Off Talking: On Ringing: Blink every 1 second
	Network/SIP Registration	Network error: Blink every 1 second Network running: Off Registration failed: Blink every 3 second Registration succeeded: On

II. Start Using

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

1. Confirm the connection

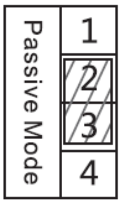
- Confirm whether the equipment of the power cord, network cable, electric lock control line connection and the boot-up is normal. (Check the network state of light)

1) Power, Electric Lock, Indoor switch port

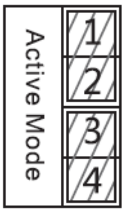
Voice access the power supply ways: 12v/DC or POE.

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



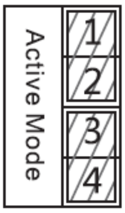
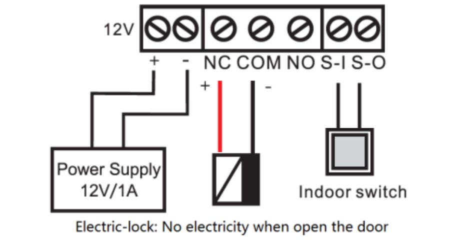
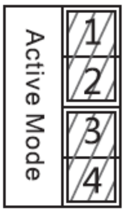
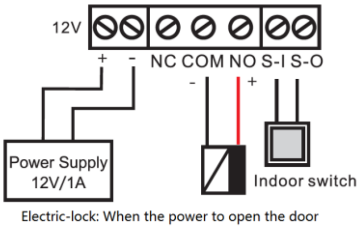
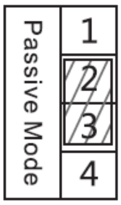
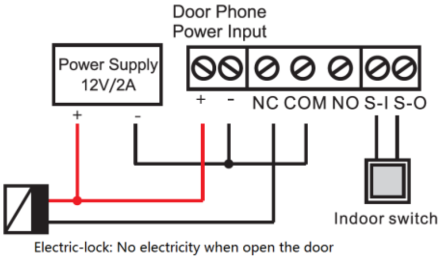
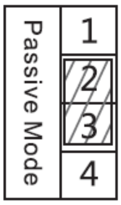
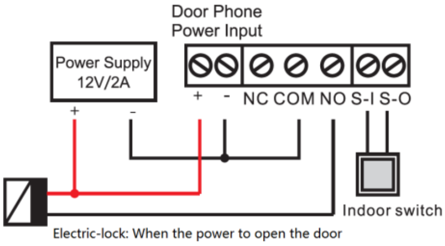
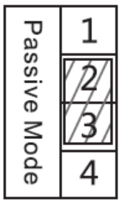
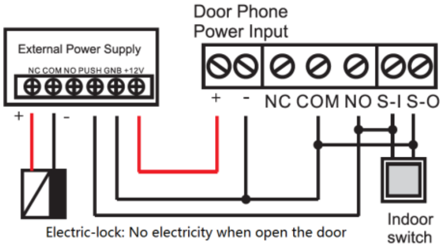
Jumper in active mode

【Note】When the device is in active mode, it can drive 12V/650mA switch output maximum（maximally）; if the electric-lock needs power supply over 12V/650mA, it will ask the device in passive mode to get additional power to drive the lock switch on/off.

- When using the active mode, it is 12V DC 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.

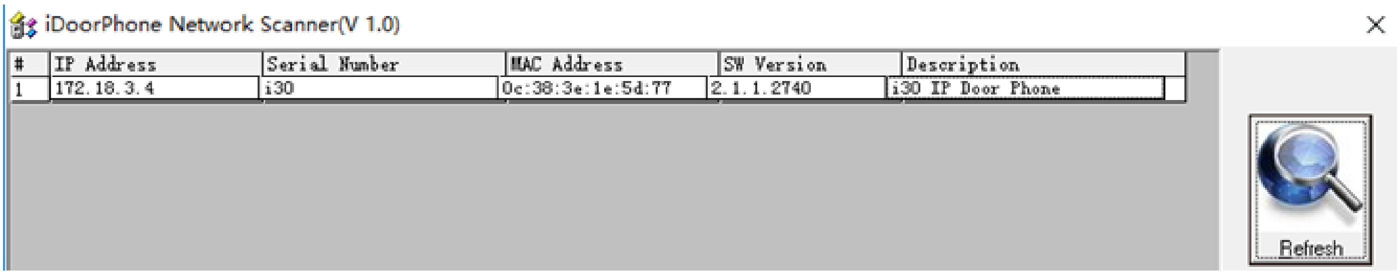
Driving Mode		Electric lock		Jumper port	Connections
Active	Passive	No electricity when open	When the power to open		
√					 12V + - NC COM NO S-I S-O + - Power Supply 12V/1A Indoor switch Electric-lock: No electricity when open the door
√			√		 12V + - NC COM NO S-I S-O - + Power Supply 12V/1A Indoor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

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 all parameters represent. 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 necessary setting options in this section to let users know how to operate I30 without understanding such complex SIP protocols.

In prior to this step, please make sure your broadband Internet can be normally operated, and you must complete the connection of the network hardware. The product factory default network mode is DHCP. Thus, only connecting equipment with DHCP network environment would let system have network access automatically.

- Press and hold "#" key for 3 seconds; the door phone would report the IP address by voice. Or you can also use the "iDoorPhoneNetworkScanner.exe" software to find the IP address of the device. (Download address http://download.fanvil.com/tool/iDoorPhoneNetworkScanner.exe)
- **Note:** when the I30 is powered on, 30s waiting is needed for device running.
- Log on to the WEB device configuration.
- In a line configuration page, service account, user name, server address and other parameters are required for server address registration.
- You can set DSS key in the function key page.
- You can set Door Phone parameters in the webpage (EGS Settings -> Features).



#	IP Address	Serial Number	MAC Address	SW Version	Description
1	172.18.3.4	i30	0c:38:3e:1e:5d:77	2.1.1.2740	i30 IP Door Phone

III. Basic operation

1. Answer a call

When a call comes in, the device would answer automatically. If you cancel auto answer feature and set auto answer time, you would hear the ring at the set time and the device would auto answer after configured timer.

2. Call

Configure shortcut key as hot key and then set up a number; after that you might press the shortcut key for making call to the configured extension(s).

3. End call

Enable Release（You can enable release）key for hanging up feature to end call.

4. Open the door

You might open doors through the following seven ways:

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 enabled 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 would 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 the user name and password of logging in web page.
   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 has been input correctly, the device would play sirens sound to prompt I30 and the remote user, while input error by low-frequency short chirp.

Password input successfully followed by high-frequency sirens sound, while input falsely, there would be high-frequency short chirp.

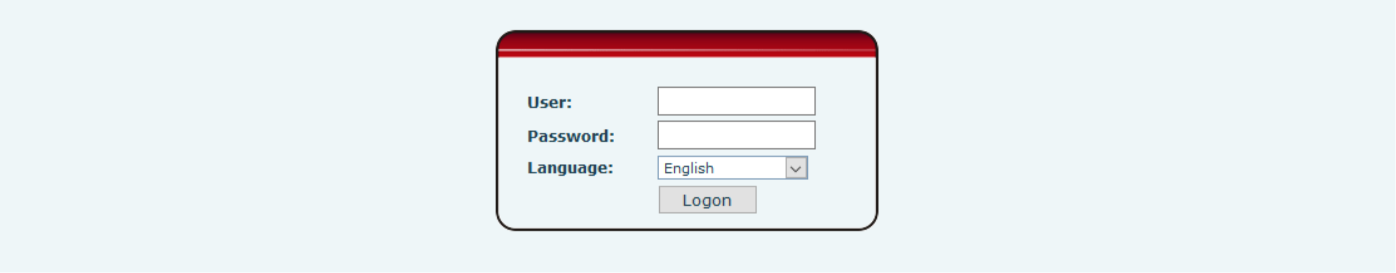
When door has been opened, the device would play sirens sound to prompt guests.

IV.Page settings

1. Browser configuration

When the device and your computer are successfully connected to the network, you might enter the IP address of the device in 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

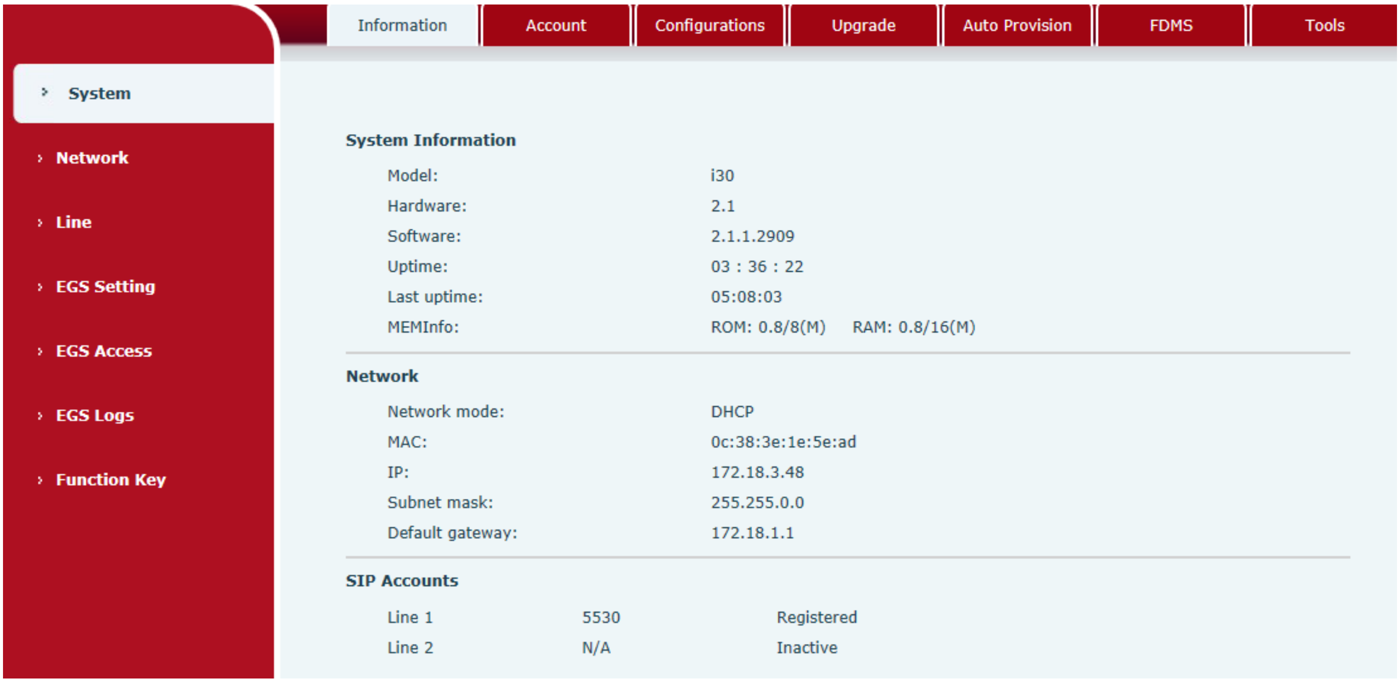
There are two levels of access: root level and general level. A user with root level can browse and set all configuration parameters, while a user with general level can set all configuration parameters except server parameters for SIP.

- General level: It is not be set by default, you can add the feature when you need
- User uses root level by default:
  - User name: admin
  - Password: admin

3. Configuration via WEB

(1) System

a) Information



System Information

Model: i30
Hardware: 2.1
Software: 2.1.1.2909
Uptime: 03 : 36 : 22
Last uptime: 05:08:03
MEMInfo: ROM: 0.8/8(M) RAM: 0.8/16(M)

Network

Network mode: DHCP
MAC: 0c:38:3e:1e:5e:ad
IP: 172.18.3.48
Subnet mask: 255.255.0.0
Default gateway: 172.18.1.1

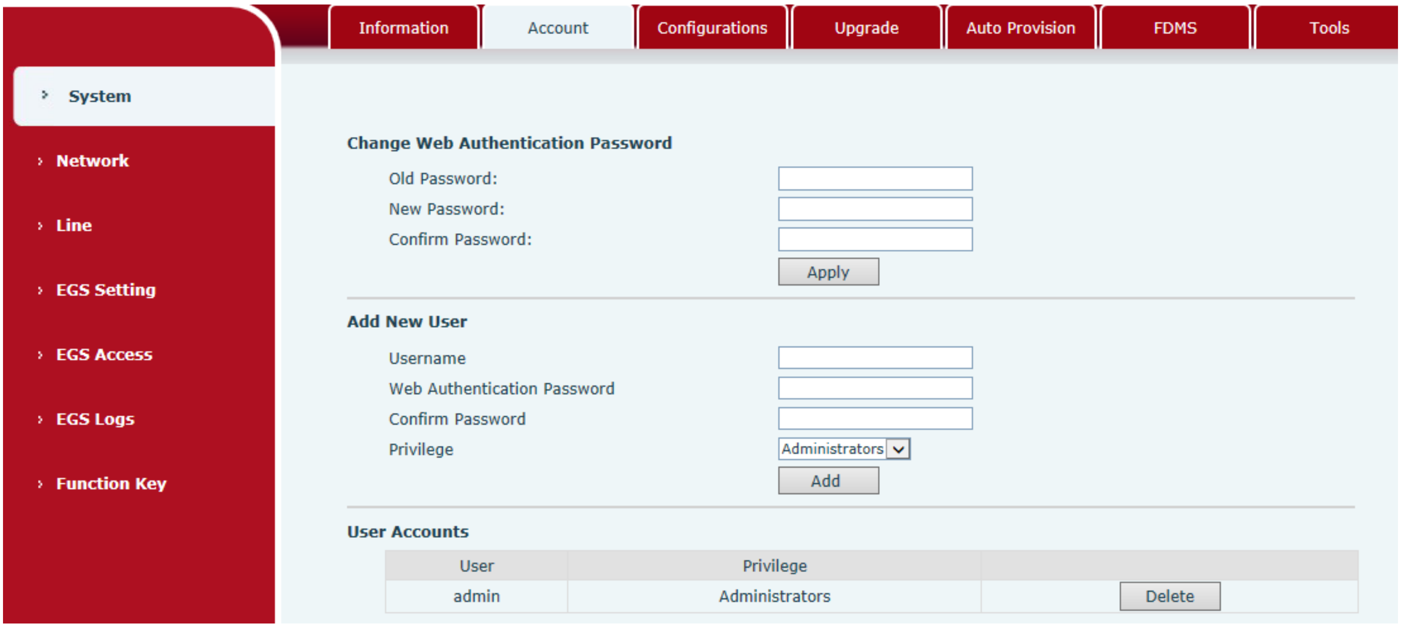
SIP Accounts

Line 1 5530 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 of 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 of the 2 SIP LINES.

b) Account

Through this page, admininstrator can add or remove user accounts depend on their needs, or modify existed user accounts permission.



Change Web Authentication Password

Old Password:

New Password:

Confirm Password:

Apply

Add New User

Username

Web Authentication Password

Confirm Password

Privilege: Administrators

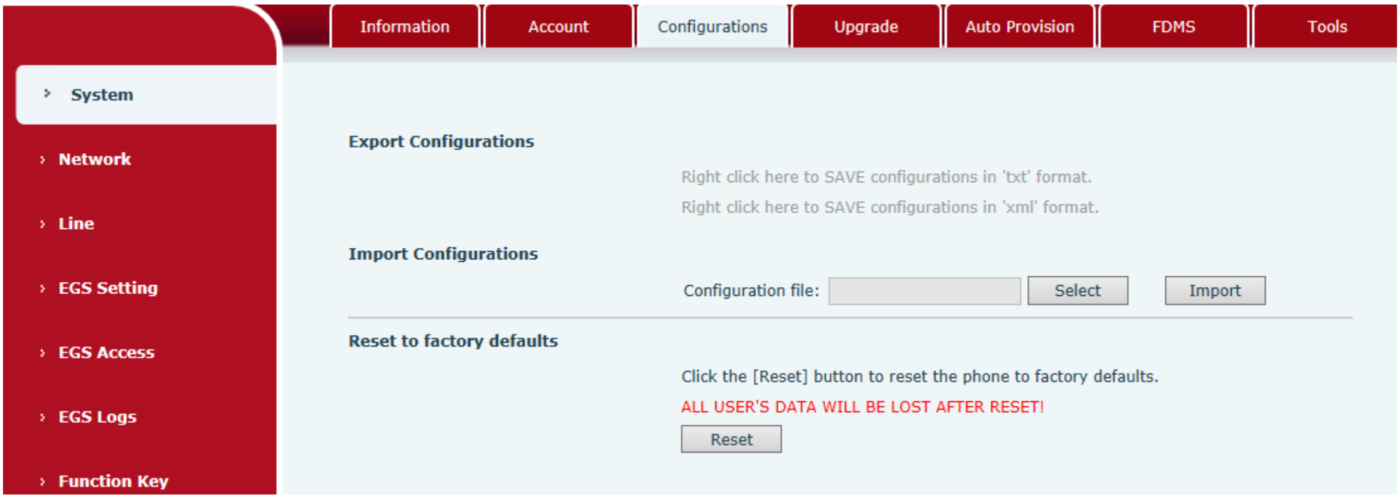
Add

User Accounts

User	Privilege	
admin	Administrators	Delete

Account	
Field Name	**Explanation**
Change Web Authentication Password	
You can modify the login password of the account	
Add New User	
You can add new user	
User Accounts	
Show the existed user accounts' 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:

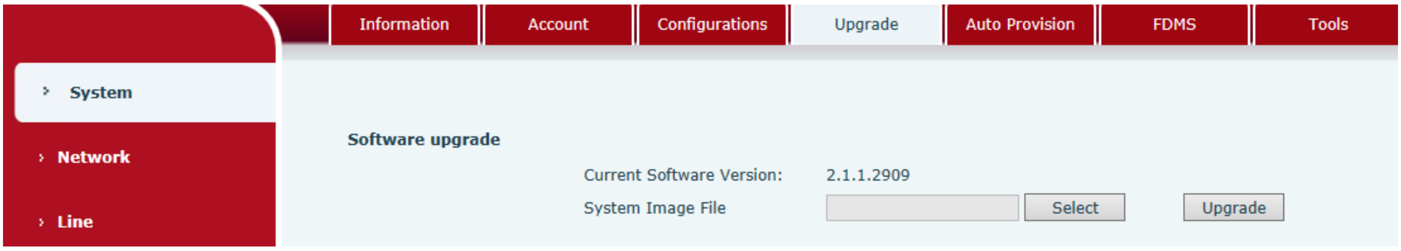
Reset to factory defaults

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

ALL USER'S DATA WILL BE LOST AFTER RESET!

Configurations	
Field Name	**Explanation**
Export Configurations	Save the equipment configuration to a txt or xml file. Please right click on the choice and then choose "Save Link As."
Import Configurations	Find the config file, and press **Update** to load it to the equipment.
Reset to factory defaults	I30 would restore to factory default configuration and remove all configuration information.

d) Upgrade



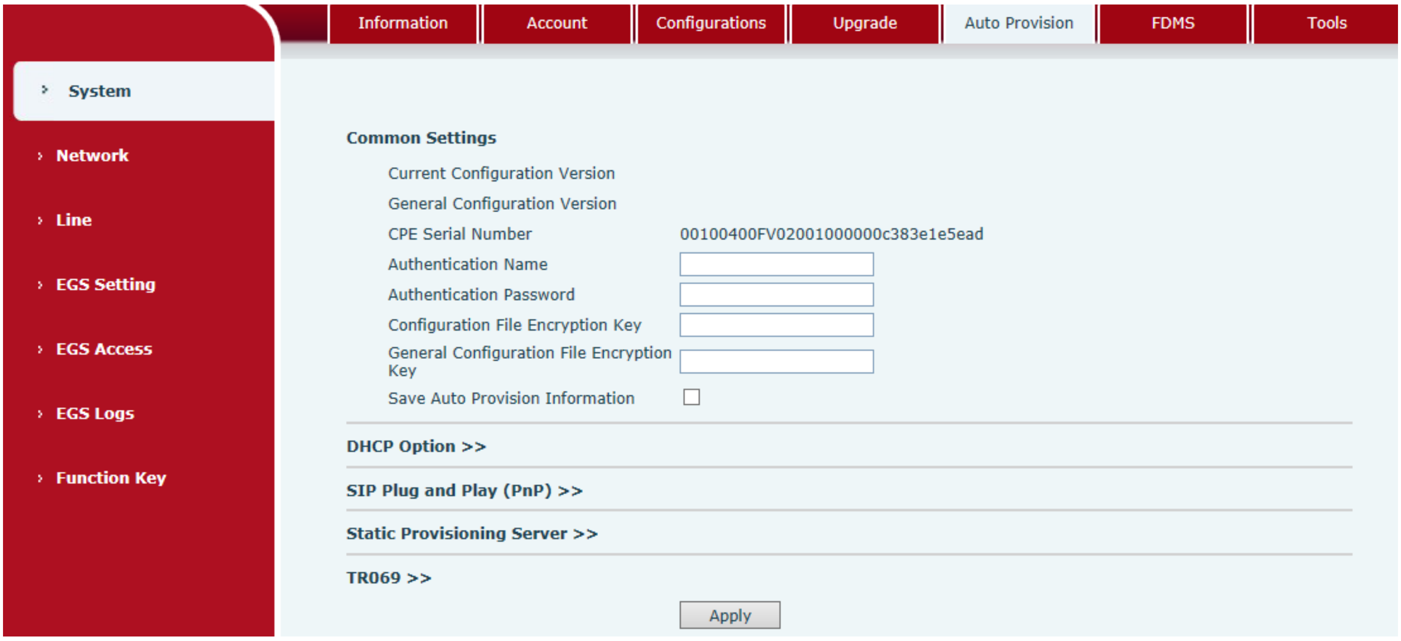
Software upgrade

Current Software Version: 2.1.1.2909

System Image File

Upgrade	
Field Name	**Explanation**
Software upgrade	
Find 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 00100400FV02001000000c383e1e5ead

Authentication Name

Authentication Password

Configuration File Encryption Key

General Configuration File Encryption Key

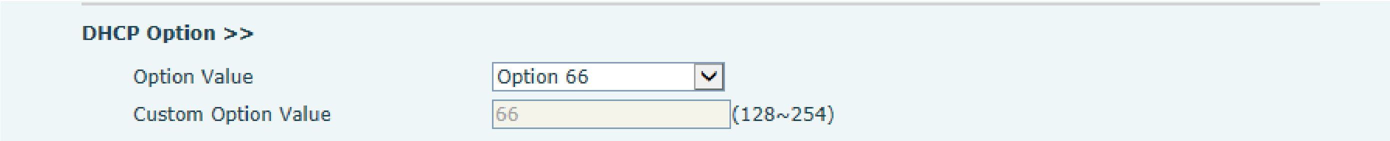
Save Auto Provision Information □

DHCP Option >>

SIP Plug and Play (PnP) >>

Static Provisioning Server >>

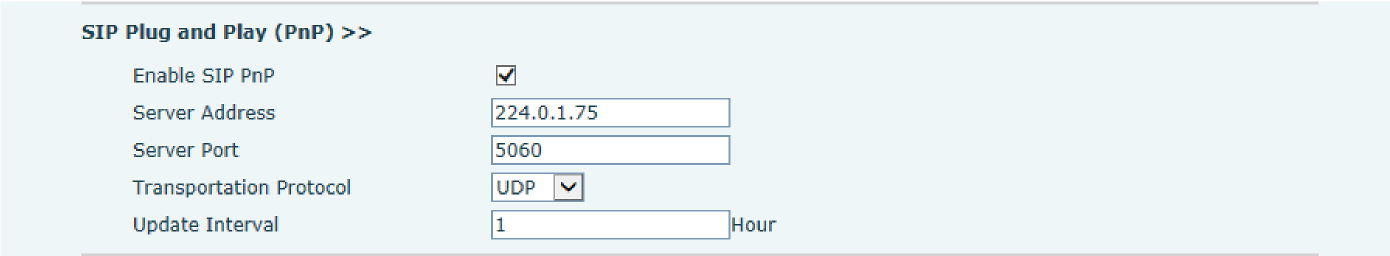
TR069 >>



DHCP Option >>

Option Value: Option 66

Custom Option Value: 66 (128~254)



SIP Plug and Play (PnP) >>

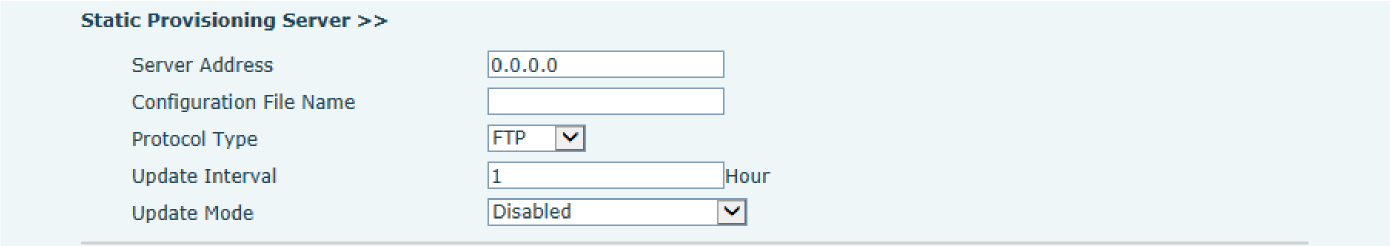
Enable SIP PnP ☑

Server Address: 224.0.1.75

Server Port: 5060

Transportation Protocol: UDP

Update Interval: 1 Hour



Static Provisioning Server >>

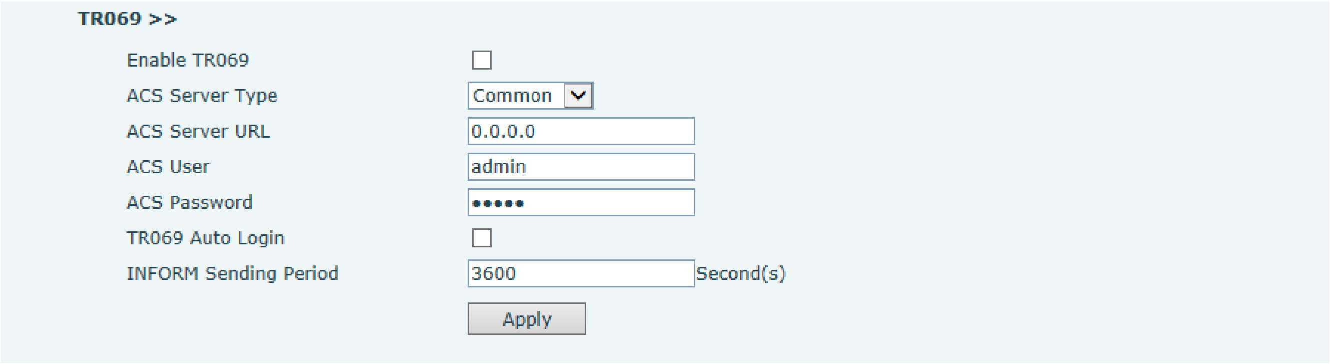
Server Address: 0.0.0.0

Configuration File Name:

Protocol Type: FTP

Update Interval: 1 Hour

Update Mode: Disabled



TR069 >>

Enable TR069 □

ACS Server Type: Common

ACS Server URL: 0.0.0.0

ACS User: admin

ACS Password: •••••

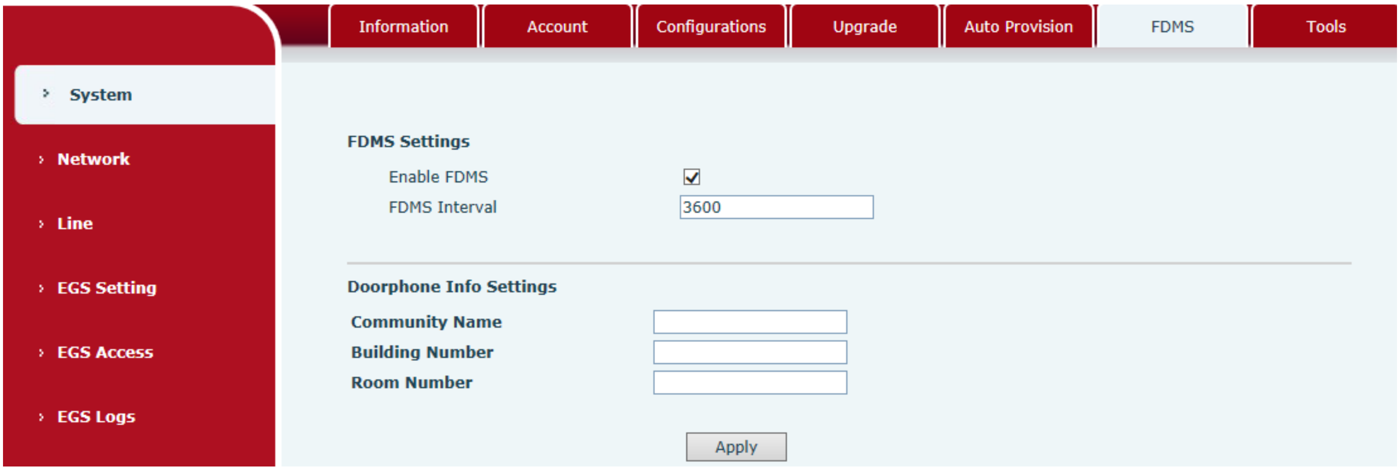
TR069 Auto Login □

INFORM Sending Period: 3600 Second(s)

Auto Provision	
Field Name	**Explanation**
Common Settings	
Current Configuration Version	Show the current config file's version. If the config file to be downloaded is higher than current version, the configuration would be upgraded. If the endpoints confirm the configuration by the Digest method, the configuration would not be upgraded unless it differs from the current configuration
General Configuration Version	Show the common config file's version. If the configuration to be downloaded and this configuration is the same, the auto provision would stop. If the endpoints confirm the configuration by the Digest method, the configuration would not be upgraded unless it differs from the current configuration.
CPE Serial Number	Serial number of the equipment
Authentication Name	Username for configuration server. It is used for FTP/HTTP/HTTPS. If this is blank, the phone would use anonymous access
Authentication Password	Password for configuration server. It is 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 changed
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. It must be from 128 to 254.
SIP Plug and Play (PnP)	
Enable SIP PnP	If it is enabled, the equipment would send SIP SUBSCRIBE messages to the server address when it boots up. Any SIP server compatible with that message would 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 would 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 – not to update 2. Update after reboot – update only after reboot. 3. Update at time period – update at periodic update period
TR069	
Enable 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 of ACS.
ACS Password	ACS Password.
TR069 Auto Login	Enable/Disable TR069 Auto Login.
INFORM Sending Period	Time between transmissions of “Inform”; the unit is second.

f) FDMS



FDMS Settings

Enable FDMS ☑

FDMS Interval 3600

Doorphone Info Settings

Community Name

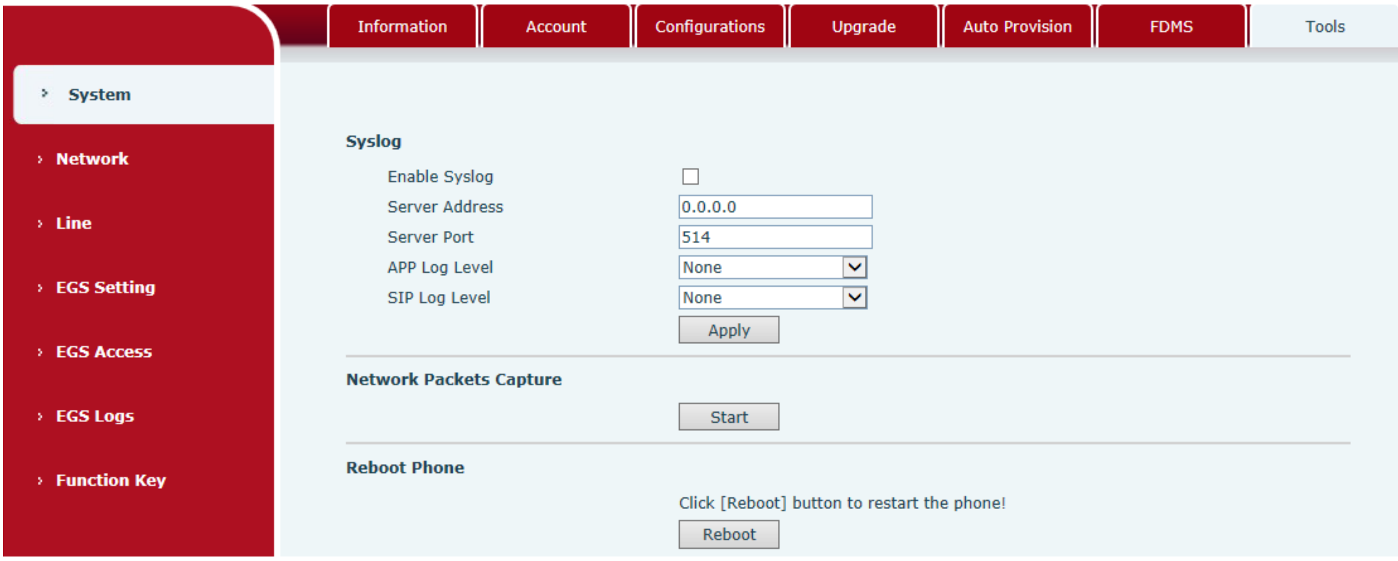
Building Number

Room Number

FDMS Settings	
Enable FDMS	Enable/Disable FDMS configuration
FDMS Interval	The time to send sip Subscribe information to the FDMS server on a regular basis. Unit 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

Apply

Network Packets Capture

Start

Reboot Phone

Click [Reboot] button to restart the phone!

Reboot

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 would 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 normal but significant condition.

Level 6: Informational; It is normal daily messages.

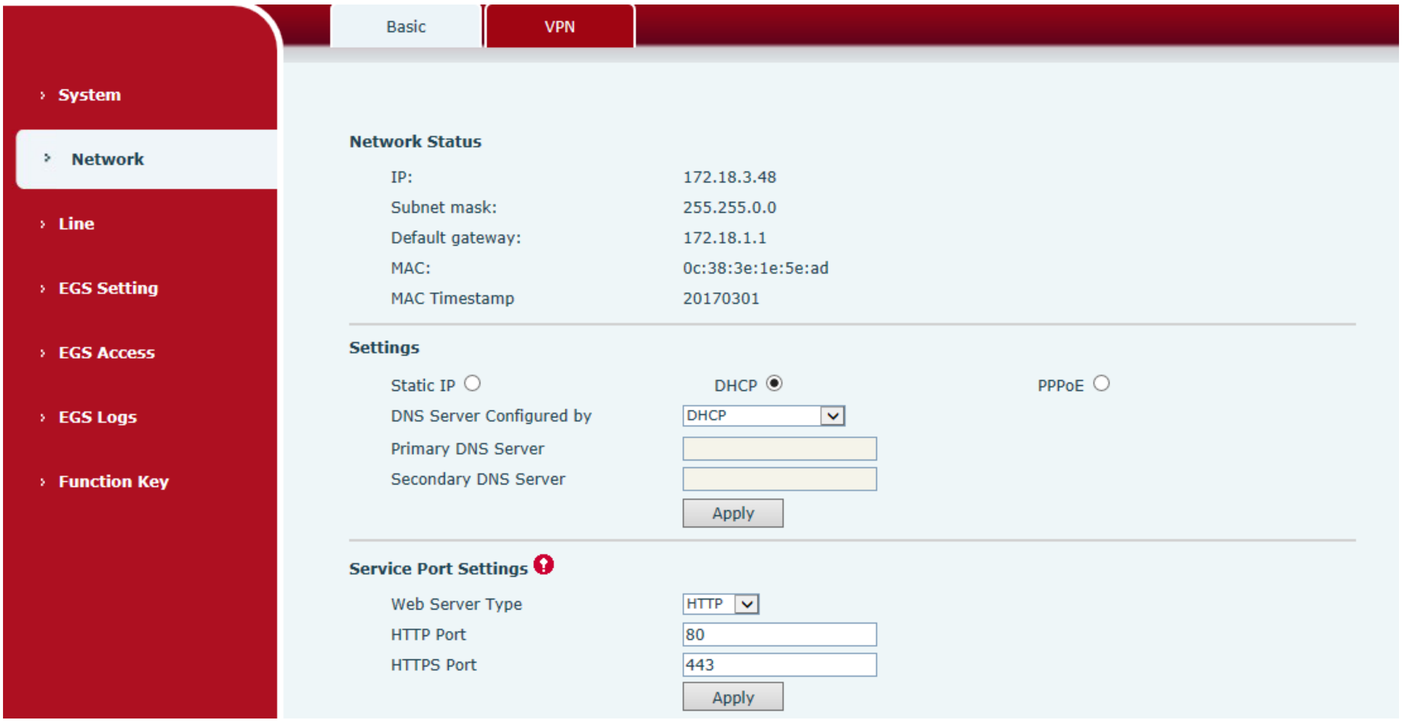
Level 7: debug; Debug messages normally used by system designer. This level can only be displayed via telnet.

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 would lead to reboot immediately. Note: Be sure to save the configuration before rebooting.	

(2) Network

a) Basic



Network Status

```
IP:                     172.18.3.48
Subnet mask:            255.255.0.0
Default gateway:        172.18.1.1
MAC:                    0c:38:3e:1e:5e:ad
MAC Timestamp           20170301
```

Settings

Static IP ○ DHCP ● PPPoE ○

```
DNS Server Configured by    DHCP
Primary DNS Server
Secondary DNS Server
```

Service Port Settings

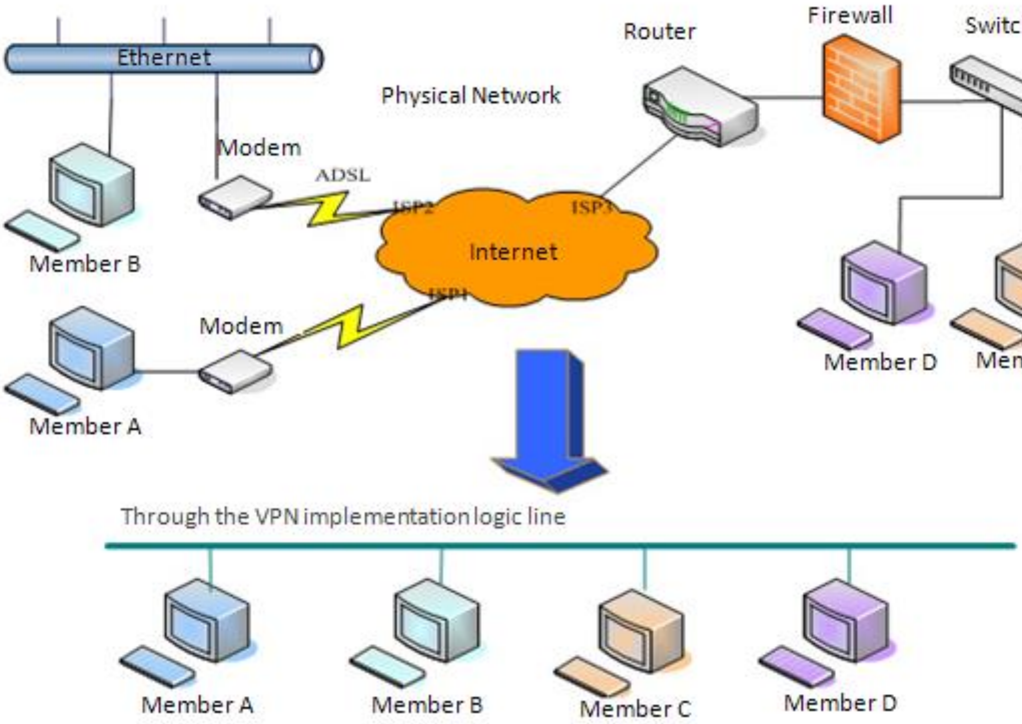
```
Web Server Type     HTTP
HTTP Port           80
HTTPS Port          443
```

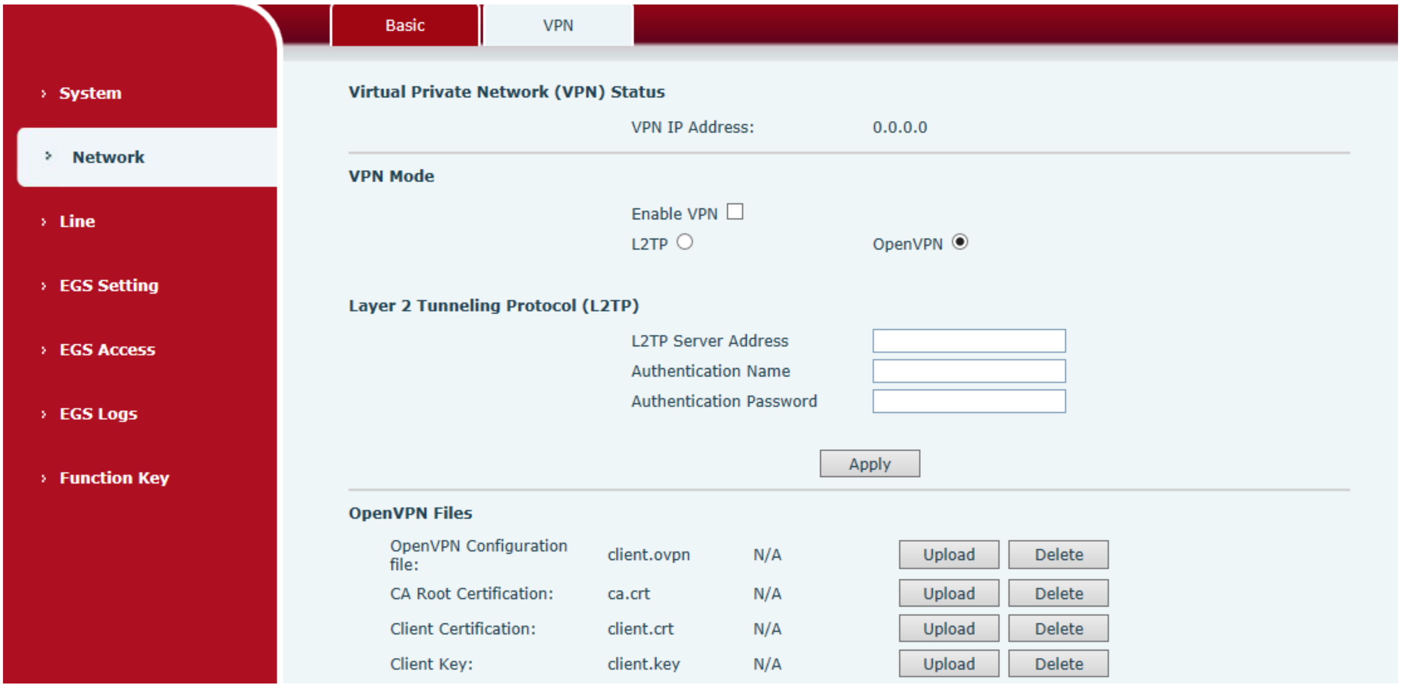
Field Name	Explanation
Network Status	
IP	The current IP address of the equipment
Subnet mask	The current Subnet Mask
Default gateway	The current Gateway IP address
MAC	The MAC address of the equipment
MAC Timestamp	Get the MAC address of time.
Settings	
Select the appropriate network mode. The equipment 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.
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.	
Service Port Settings	
Web Server Type	Specify Web Server Type – HTTP or HTTPS
HTTP Port	Port for web browser access. Default value is 80. To enhance security, change this from the default. Setting this port to 0 will disable HTTP access. Example: The IP address is 192.168.1.70 and the port value is 8090, the accessing address is http://192.168.1.70:8090.
HTTPS Port	Port for HTTPS access. Before using https, an https authentication certification must be downloaded into the equipment. Default value is 443. To enhance security, change this from the default.
Note: 1) Any changes made on this page require a reboot to become active. 2) It is suggested that changes to HTTP Port be values greater than 1024.Values less than 1024 are reserved. 3) If the HTTP port is set to 0, HTTP service will be disabled.	

b) 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.





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	

Apply

OpenVPN Files

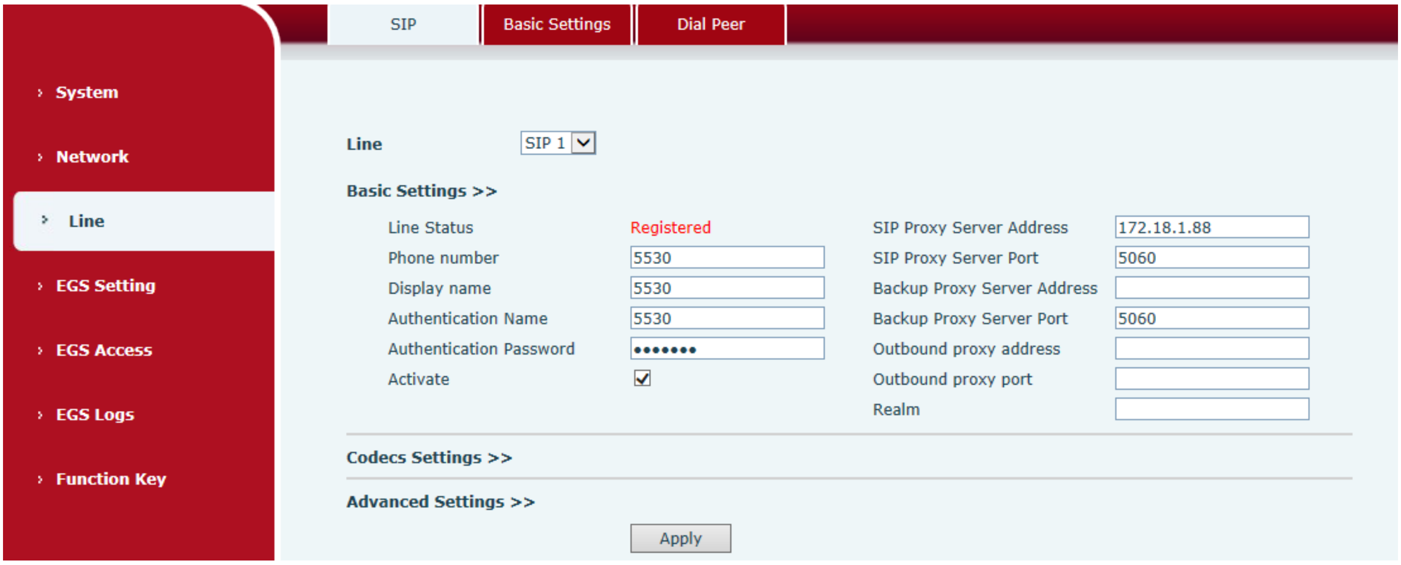
OpenVPN Configuration file:	client.ovpn	N/A	Upload	Delete
CA Root Certification:	ca.crt	N/A	Upload	Delete
Client Certification:	client.crt	N/A	Upload	Delete
Client Key:	client.key	N/A	Upload	Delete

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
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

You can configure a SIP server on this page.



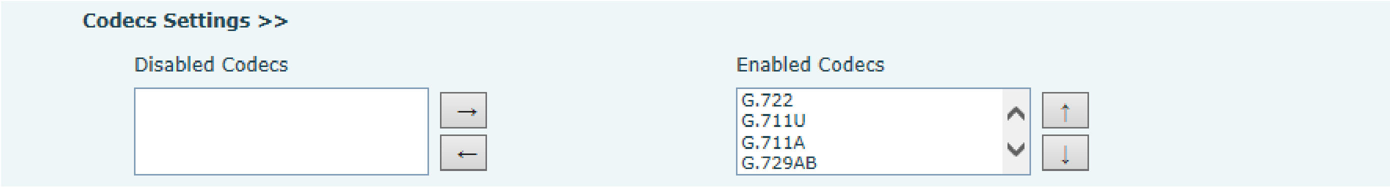
Line SIP 1

Basic Settings >>

Line Status	Registered	SIP Proxy Server Address	172.18.1.88
Phone number	5530	SIP Proxy Server Port	5060
Display name	5530	Backup Proxy Server Address	
Authentication Name	5530	Backup Proxy Server Port	5060
Authentication Password	•••••••	Outbound proxy address	
Activate	☑	Outbound proxy port	
		Realm	

Codecs Settings >>

Advanced Settings >>

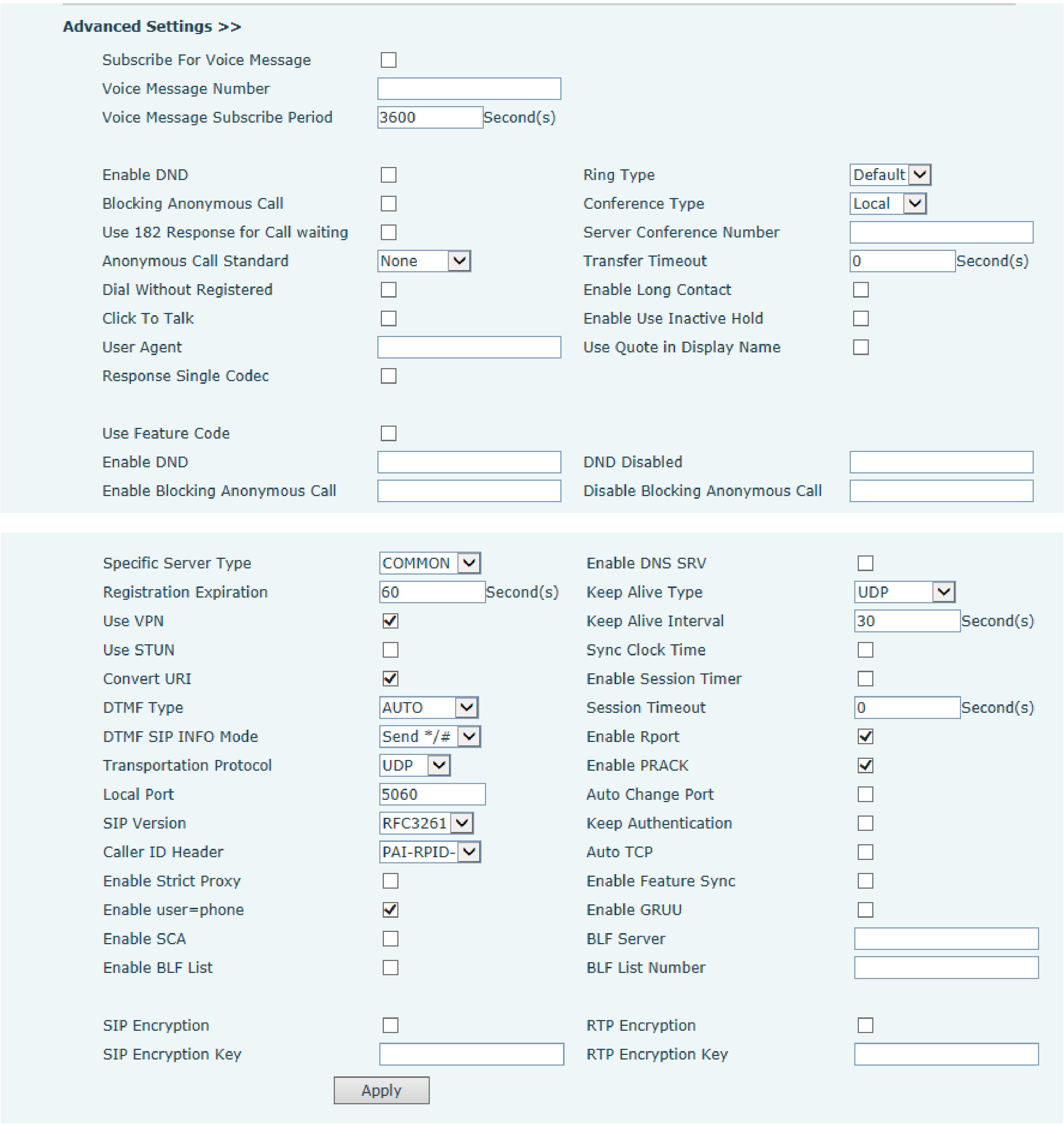


Codecs Settings >>

Disabled Codecs

Enabled Codecs

G.722
G.711U
G.711A
G.729AB



Advanced Settings >>

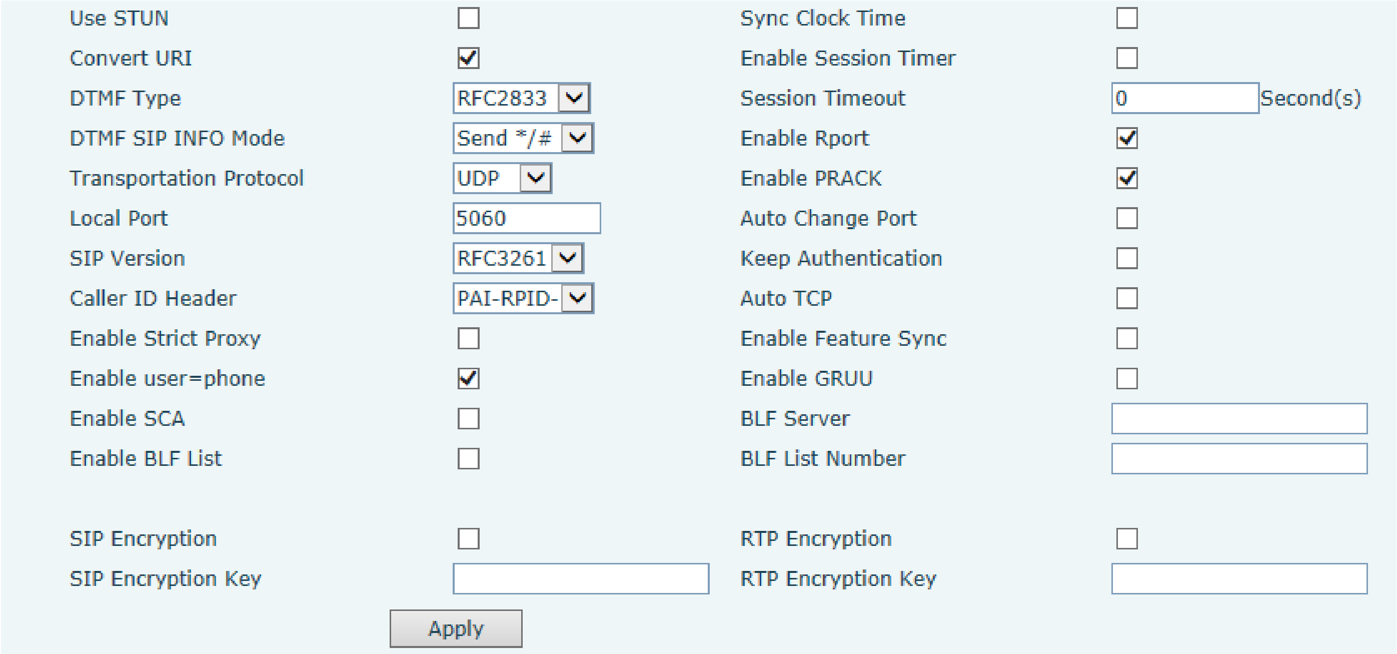
Subscribe For Voice Message	□
Voice Message Number	
Voice Message Subscribe Period	3600 Second(s)

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	



Use STUN	□	Sync Clock Time	□
Convert URI	☑	Enable Session Timer	□
DTMF Type	RFC2833	Session Timeout	0 Second(s)
DTMF SIP INFO Mode	Send */#	Enable Rport	☑
Transportation Protocol	UDP	Enable PRACK	☑
Local Port	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.
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 Password	Enter the authentication password of the service account
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 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 remove them from the list.	
Advanced Settings	
Call Forward Unconditional	Enable unconditional call forward, all incoming calls will be forwarded to the number specified in the next field
Call Forward Number for Unconditional	Set the number of unconditional call forward

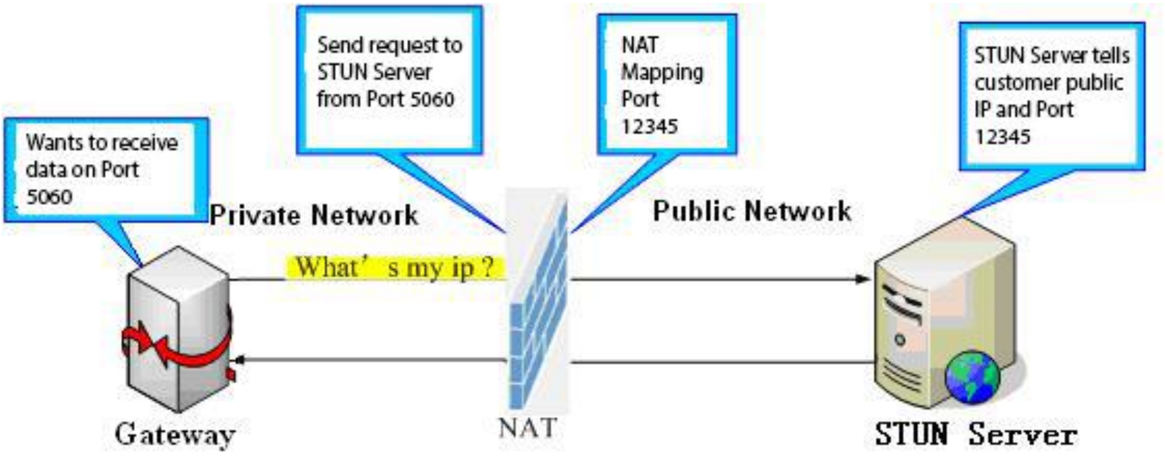
Call Forward on Busy	Enable call forward on busy, when the phone is busy, any incoming call will be forwarded to the number specified in the next field
Call Forward Number for Busy	Set the number of call forward on busy
Call Forward on No Answer	Enable call forward on no answer, when an incoming call is not answered within the configured delay time, the call will be forwarded to the number specified in the next field
Call Forward Number for No Answer	Set the number of call forward on no answer
Call Forward Delay for No Answer	Set the delay time of not answered call before being forwarded
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 the delay time
Auto Answering Delay	Set the delay for incoming call before the system automatically answered it
Subscribe For Voice Message	Enable the device to subscribe a voice message waiting notification, if enabled, the device will receive notification from the server if there is voice message waiting on the server
Voice Message Number	Set the number for retrieving voice message
Voice Message Subscribe Period	Set the interval of voice message notification subscription
Enable Hotline	Enable hotline configuration, the device will dial to the specific number immediately at audio channel opened by off-hook handset or turn on hands-free speaker or headphone
Hotline Number	Set the hotline dialing number
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.
Use Quote in Display Name	Whether to add quote in display name
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

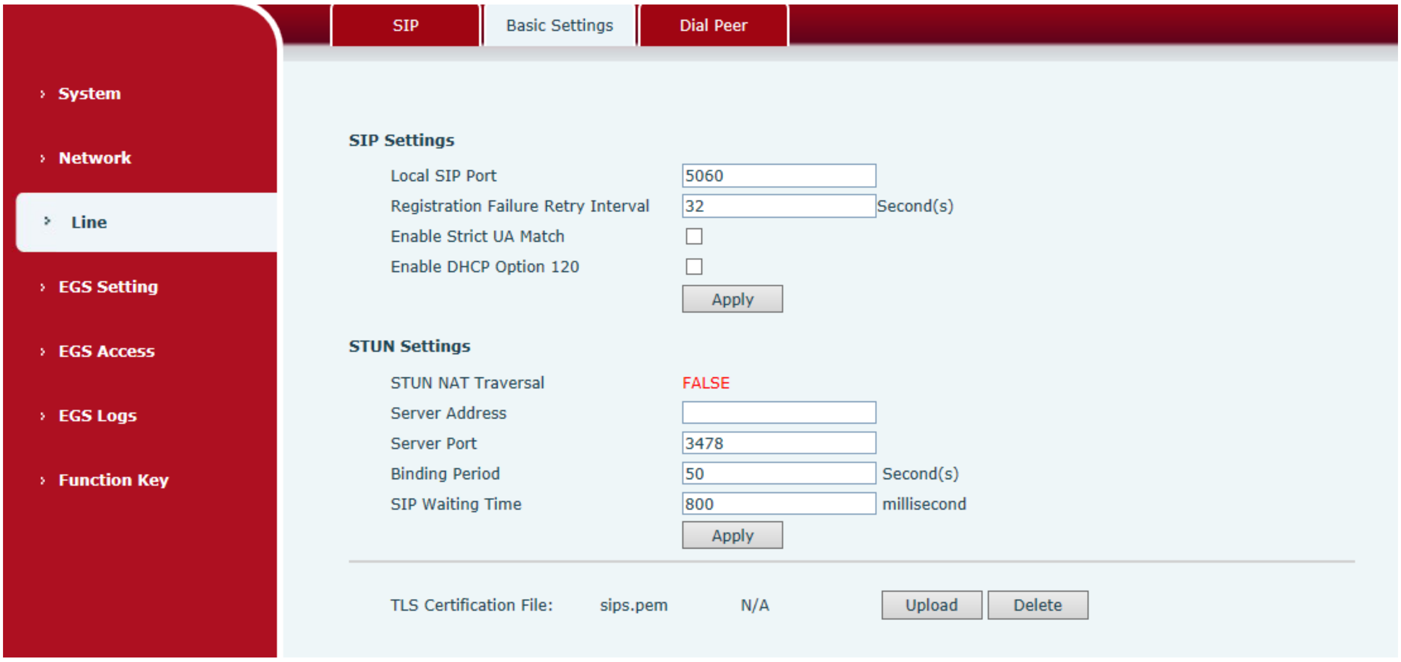
Server Conference Number	Set the conference room number when conference type is set to be Server
Transfer Timeout	Set the timeout of call transfer process
Enable Long Contact	Allow more parameters in contact field per RFC 3840
Enable Missed Call Log	If enabled, the phone will save missed calls into the call history record.
Response Single Codec	If setting enabled, the device will use single codec in response to an incoming call request
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
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 BLF List	Enable/Disable BLF List
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
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
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)
BLF Server	The registered server will receive the subscription package from ordinary application of BLF phone. Please enter the BLF server, if the sever does not support subscription package, the registered server and subscription server will be separated.
BLF List Number	BLF List allows one BLF key to monitor the status of a group. Multiple BLF 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.


Wants to receive data on Port 5060
Send request to STUN Server from Port 5060
NAT Mapping Port 12345
STUN Server tells customer public IP and Port 12345
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	□	
	Apply	

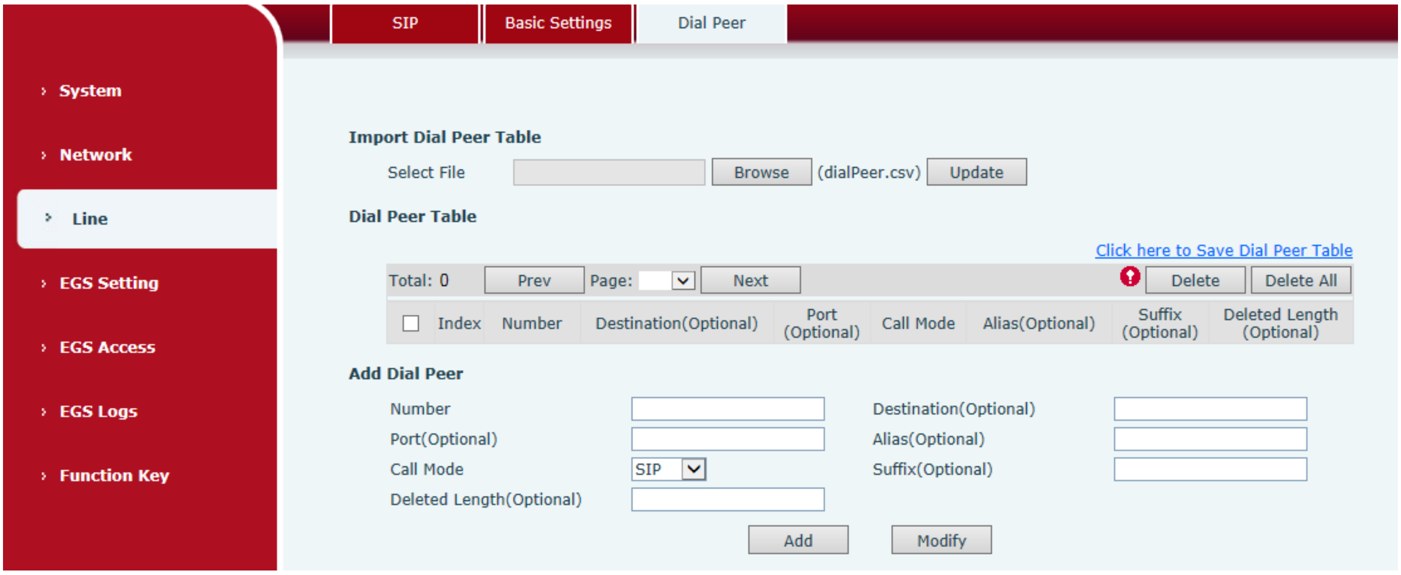
STUN Settings

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

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.
Registration Failure Retry Interval	Set the retry interval of SIP REGISTRATION when registration failed.
Enable Strict UA Match	Enable or disable Strict UA Match
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, 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.	

c) Dial Peer



Total: 0

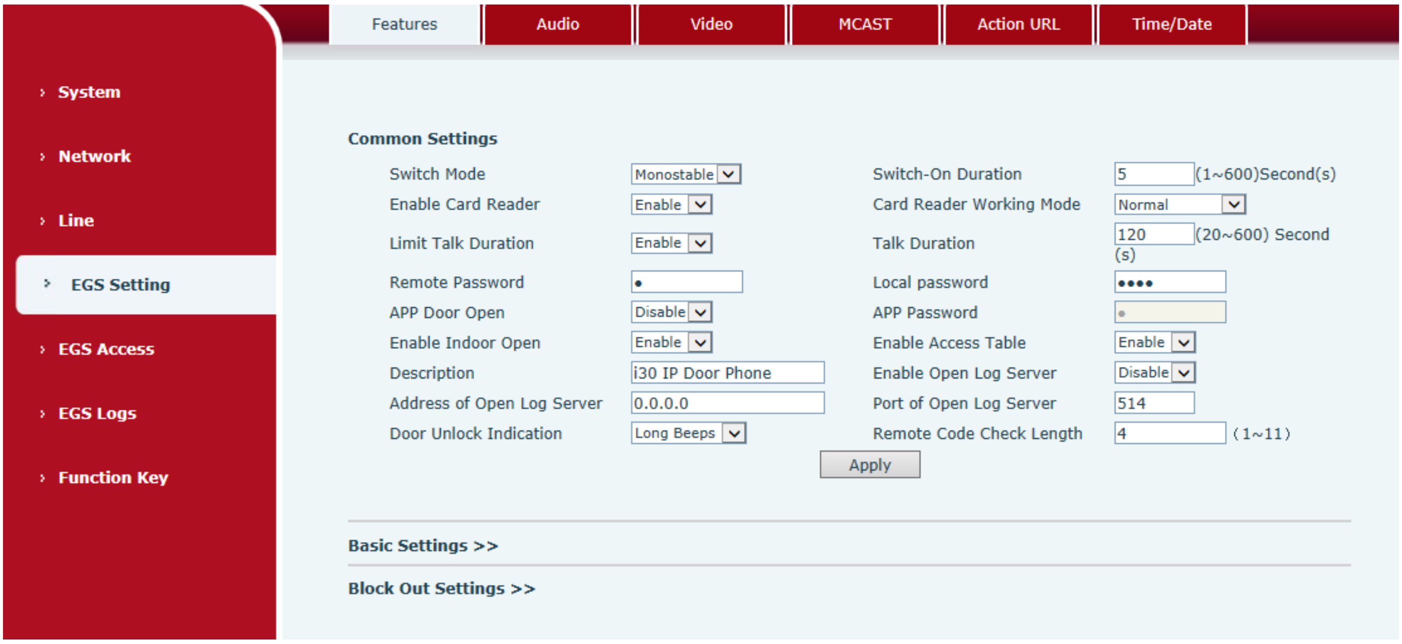
Call Mode: SIP

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	In order 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 of 30 bits; also supports the use of x format and range of numbers.
Destination	Configure the destination address and, if 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 5060v
Alias	Configure aliases, this is an optional item: the replacement number used when the prefix is prefixed, and no alias when 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 / IAX2;
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

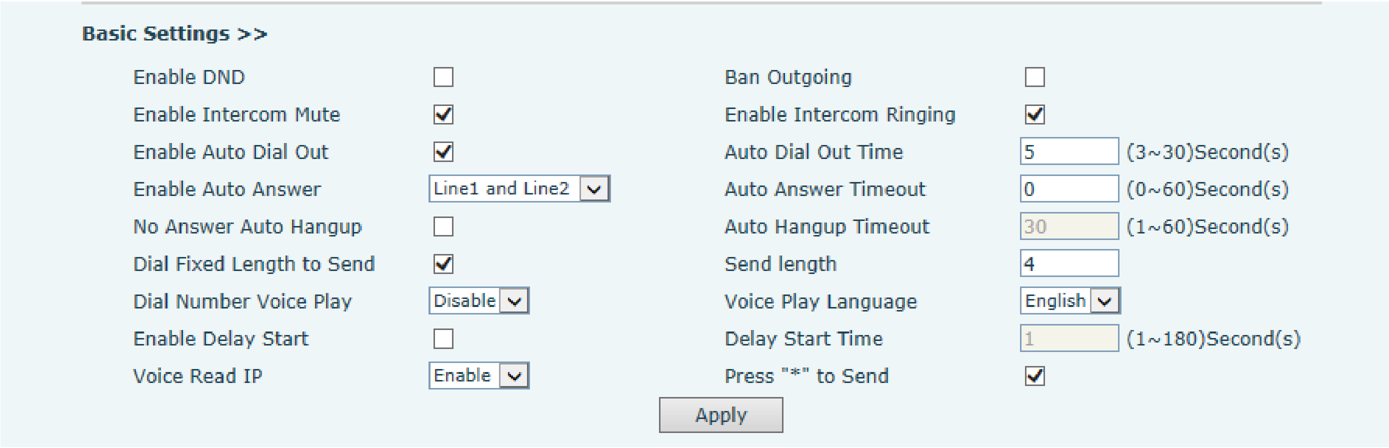


Common Settings

Switch Mode	Monostable	Switch-On Duration	5 (1~600)Second(s)
Enable Card Reader	Enable	Card Reader Working Mode	Normal
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	i30 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）

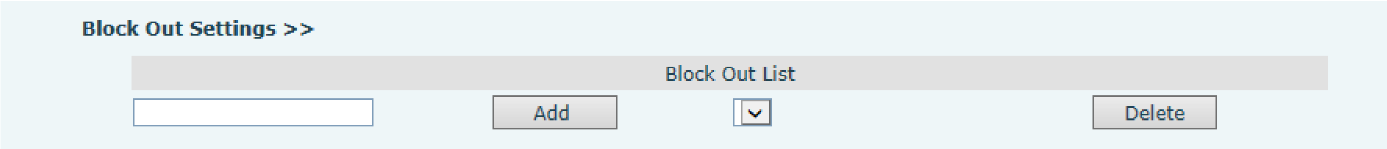
Basic Settings >>

Block Out Settings >>



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	Line1 and Line2	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

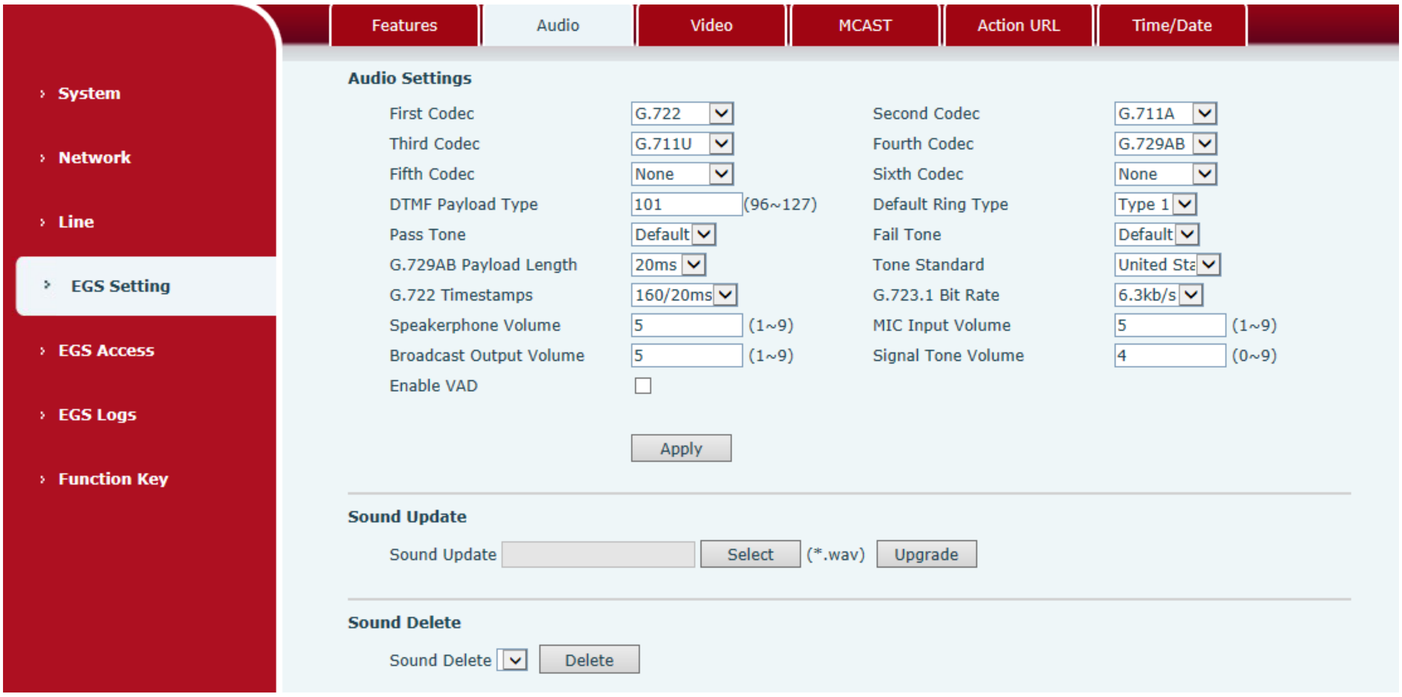
Features	
Field Name	**Explanation**
Common Settings	
Switch Mode	Monostable: there is only one fixed action status for door unlocking. Bistable: there are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After changed, the status would be kept. Initial Value is Monostable
Switch-On Duration	Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial Value is 5 seconds.
Enable Card Reader	Enable or disable card reader for RFID cards.
Card Reader Working Mode	Set ID card stats: Normal: This is the work mode, after the slot card can to open the door. Card Issuing: This is the issuing mode, after the slot card can to add ID cards. Card Revoking: This is the revoking mode, after the slot card can to delete ID cards.
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 “i31S 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 type 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.	

a) 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

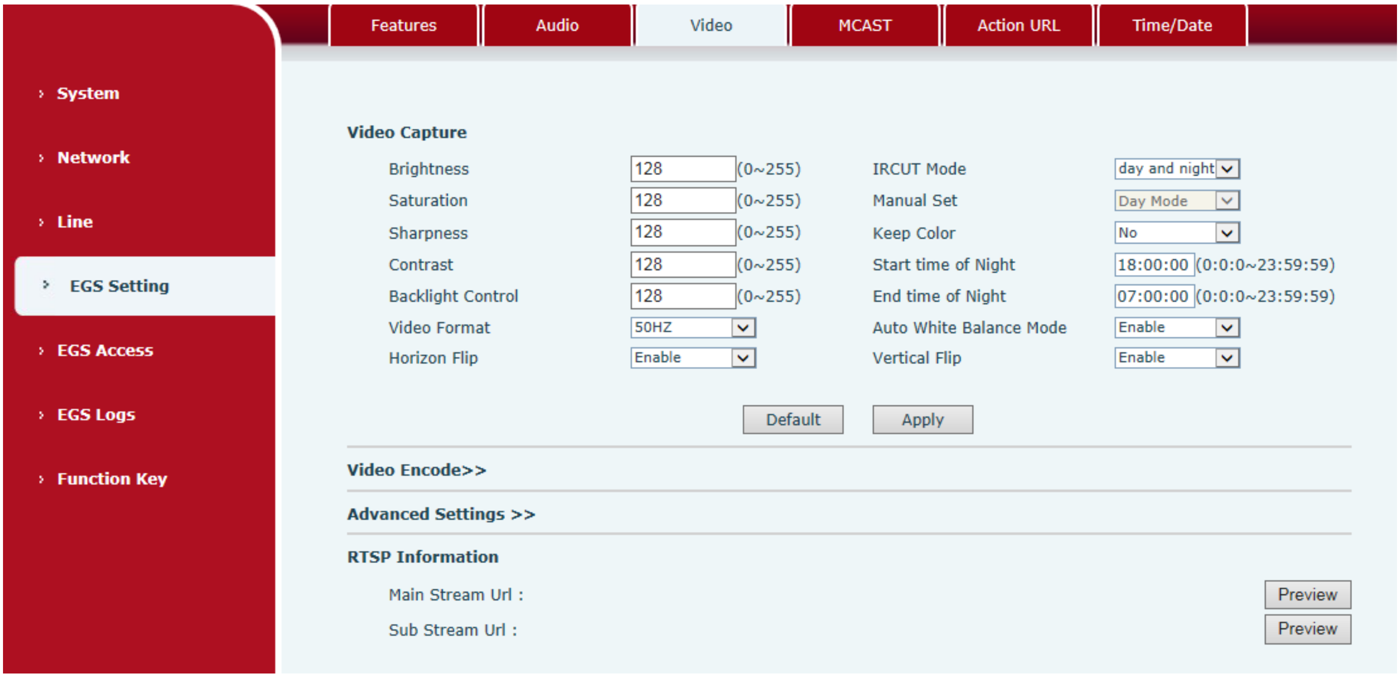
Sound Delete

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.
G.729AB Payload Length	G.729AB Payload length – adjust 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 call volume level.
MIC Input Volume	Set the MIC call volume level.
Broadcast Output Volume	Set the broadcast output volume level.
Signal Tone Volume	Set the audio signal 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 msec.

b) Video

This page allows you to set the video encoding and video capture and other information.



Video Capture

Brightness 128 (0~255)

Saturation 128 (0~255)

Sharpness 128 (0~255)

Contrast 128 (0~255)

Backlight Control 128 (0~255)

Video Format 50HZ

Horizon Flip Enable

IRCUT Mode day and night

Manual Set Day Mode

Keep Color No

Start time of Night 18:00:00 (0:0:0~23:59:59)

End time of Night 07:00:00 (0:0:0~23:59:59)

Auto White Balance Mode Enable

Vertical Flip Enable

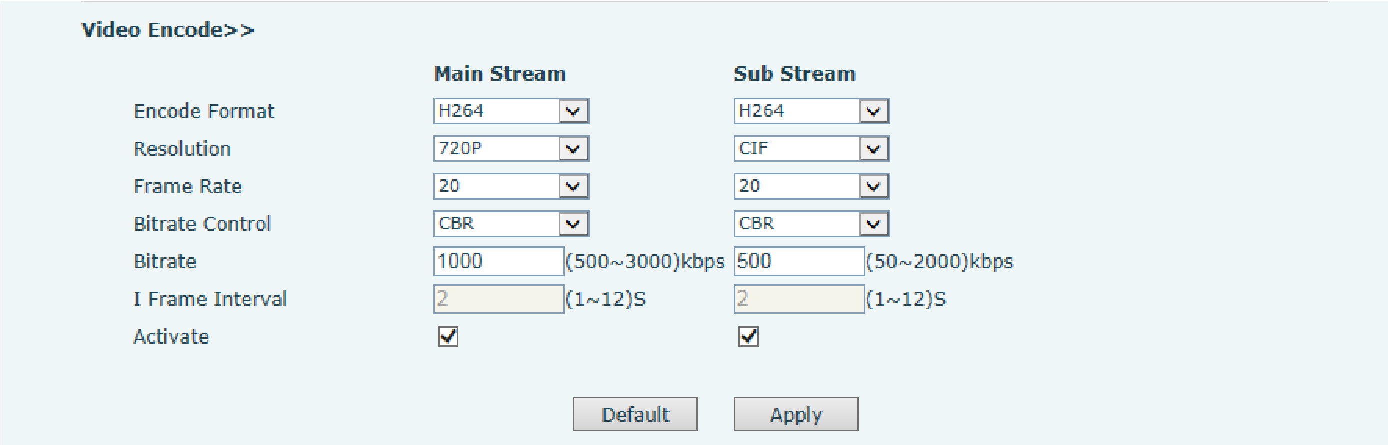
Video Encode>>

Advanced Settings >>

RTSP Information

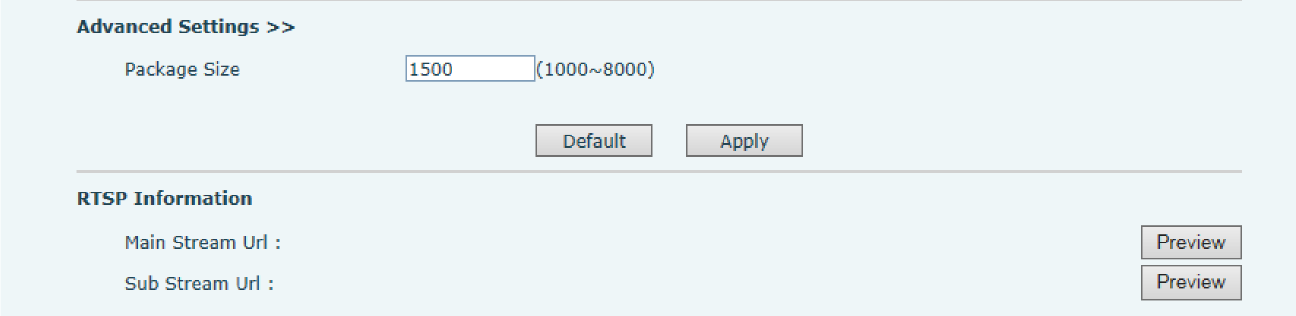
Main Stream Url :

Sub Stream Url :



Video Encode>>

	Main Stream	Sub Stream
Encode Format	H264	H264
Resolution	720P	CIF
Frame Rate	20	20
Bitrate Control	CBR	CBR
Bitrate	1000 (500~3000)kbps	500 (50~2000)kbps
I Frame Interval	2 (1~12)S	2 (1~12)S
Activate	☑	☑



Advanced Settings >>

Package Size: 1500 (1000~8000)

RTSP Information

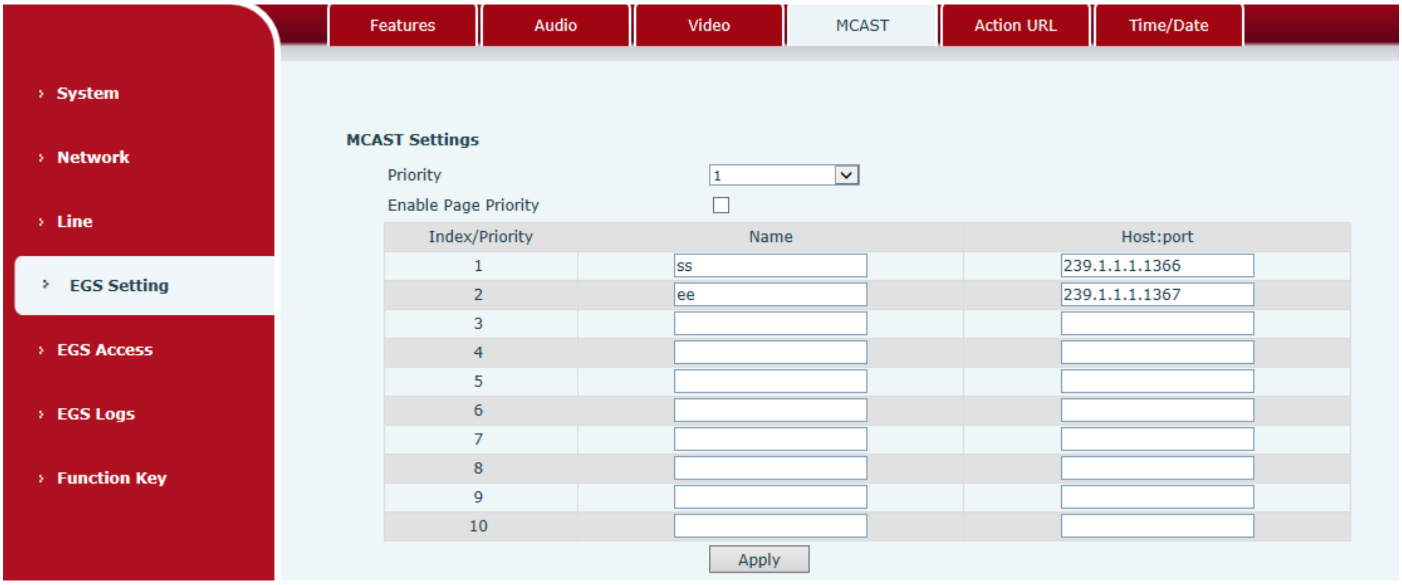
Main Stream Url :

Sub Stream Url :

Video	
Field Name	**Explanation**
Video Capture	
Brightness	Adjust the video brightness level
Saturation	Adjust the video color purity, the higher the value is , the more vivid colors might be displayed
Sharpness	Adjust video clarity
Contrast	Adjust the video brightness ratio
Backlight Control	Video background brightness
Video Format	Based on the using power frequency , common frequency is 50Hz
Horizon Flip	The video is flipped horizontally
Brightness	Adjust video brightness
IRCUT Mode	Day & night Mode: The camera automatically switches to black and white in "Night Start Time" and "Night End Time" (under black and white mode, you can see things in a dark environment) Auto Mode: IRCUT switches according to the actual ambient light level of the camera Manual Mode: the user need to manually select the camera day / night mode, night mode is black and white反向被动模式：IRCUT滤光片切换

Manual Set	You need to manually select the camera day / night mode, night mode is black and white
Keep Color	Select whether or not the camera is remained as colorized
Start time of Night	IR-Cut Day and night mode, the camera switches to black and white start time
End time of Night	IR-Cut day and night mode, the camera switches to black and white end time
Auto White Balance Mode	The camera automatically adjusts the video image based on ambient light
Video Encode	
Encode Format	Only H.264 encoding format is supported
Resolution	Main stream: support 720P Sub-stream: you can select CIF (352 * 288), D1 (720 * 576)
Frame Rate	The larger the value is, the more coherent the video would be got; not recommend adjusted.
Bitrate Control	CBR: If the code rate (bandwidth) is insufficient, it is preferred. VBR: Image quality is preferred, not recommended.
Bitrate	It is proportional to video file size, not recommend adjusted.
I Frame Interval	The greater the value is, the worse the video quality would be, otherwise the better video quality would be; not recommend adjusted.
Activate	When you selected it, the stream is enabled, otherwise disabled
Advanced Setup	
Package Size	Video data package size
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

c) MCAST



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
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 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, the device monitors and plays 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.

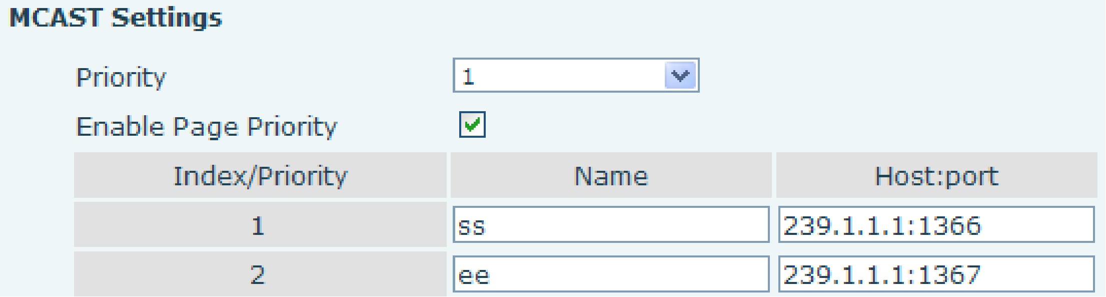
- Priority:

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

- 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 streams
  - ✧ Enable the page priority:

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

- Web Settings:



MCAST Settings

Priority: 1

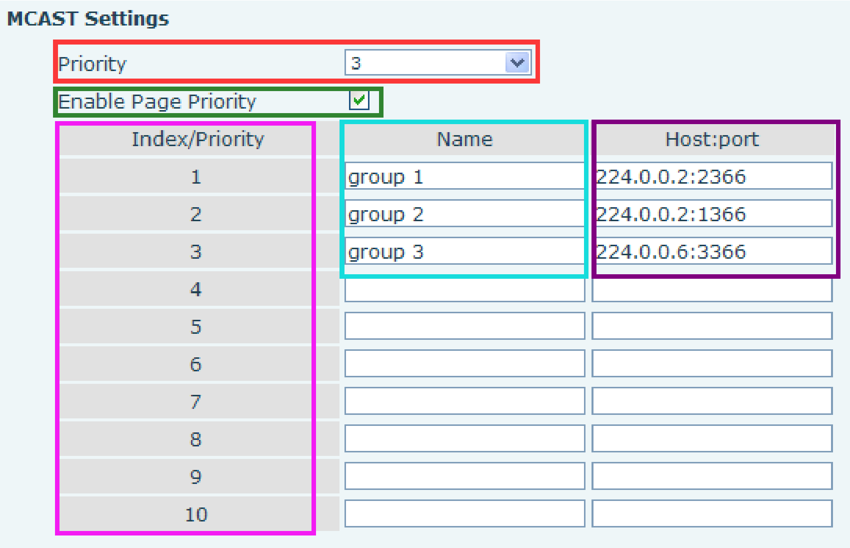
Enable Page Priority: ☑

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; ss has the highest priority.

Note: when you press the multicast key for multicast session, both multicast sender and receiver would 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 would be displayed on the screen when you answer the multicast. If you have not set, the screen would 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 higher priority. The followings would explain how to use this option:

- ✧ The purpose of setting monitoring multicast "Group 1" or "Group 2" or "Group 3" is to launch a multicast call.
- ✧ All equipment has one or more common non multicast communication.
- ✧ When you set the priority as disabled, any level of multicast would not be answered , multicast call is rejected.
- ✧ when you set the priority as some value, only the multicast higher than the priority can come in. If you set the priority as 3, group 2 and group 3 would be rejected, for its priority level is equal to 3 and less than 3; multicast 1 priority is set up with 2, higher than ordinary call priority, device can answer the multicast message, at the same time, holding the other call.

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

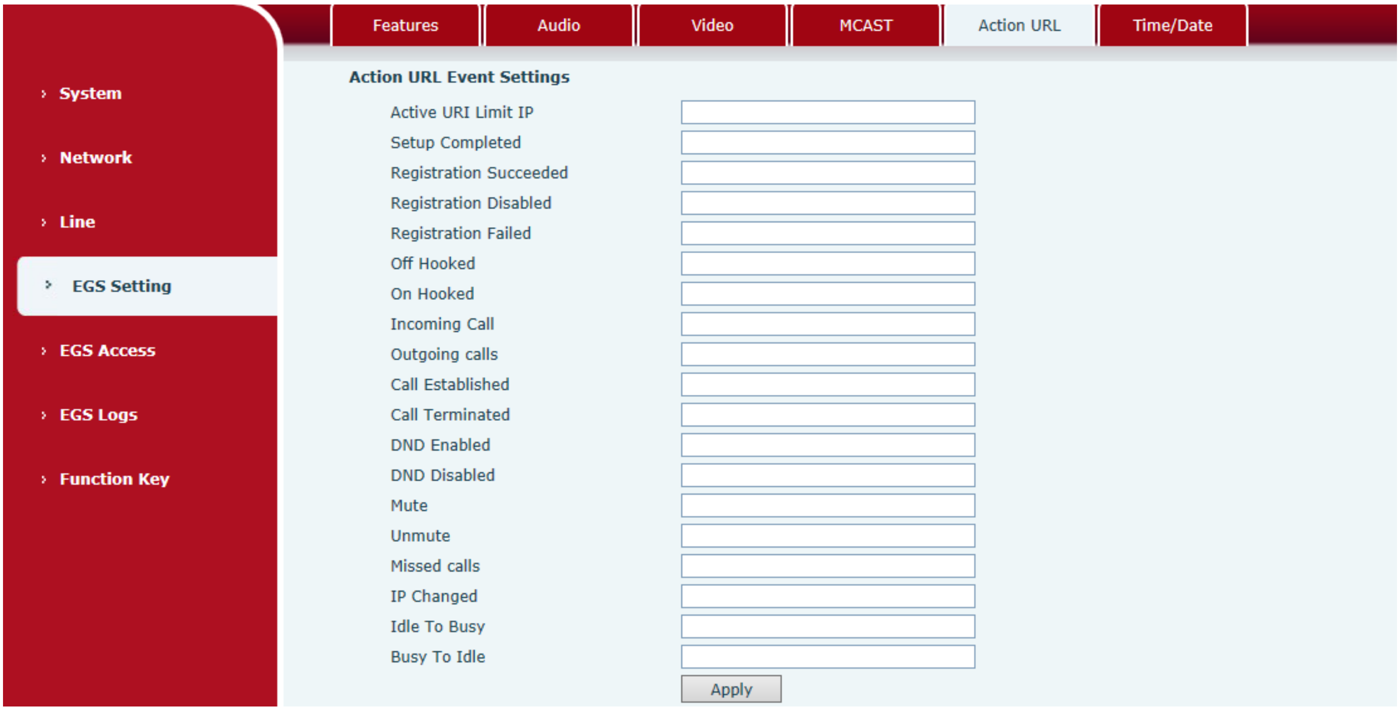
 Set whether to open multicast comparison function, multicast priority is pink part number. Following explains how to use:

- ✧ The purpose of setting monitoring multicast "group 1" or “group 3”is listening "group of 1" or “group 3”multicast call of multicast address.
- ✧ The device has a path or multi-path multicast calls, such as listening to "multicast information group 2".
- ✧ If multicast is a new "group 1", and because the priority of group 1" is 2, higher than the current call priority 3 of “group 2”, so multicast call would come in.
- ✧ If multicast is a new "group 3", and because the priority of group 3" is 4, lower than the current call priority 3 of “group 2”, the device would listen to the “group 1” and maintain the "group 2".

Multicast service

- **Send:** when you configure the item, pressing the corresponding key on the equipment shell, equipment would directly enter the Talking interface; the premise is to ensure no current multicast call and three-way conference, so the multicast can be established.
- **Monitor:** IP port and priority are configured to monitor the device, when the call is initiated by multicast and the call is successful; the device would directly enter the Talking interface.

d) 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

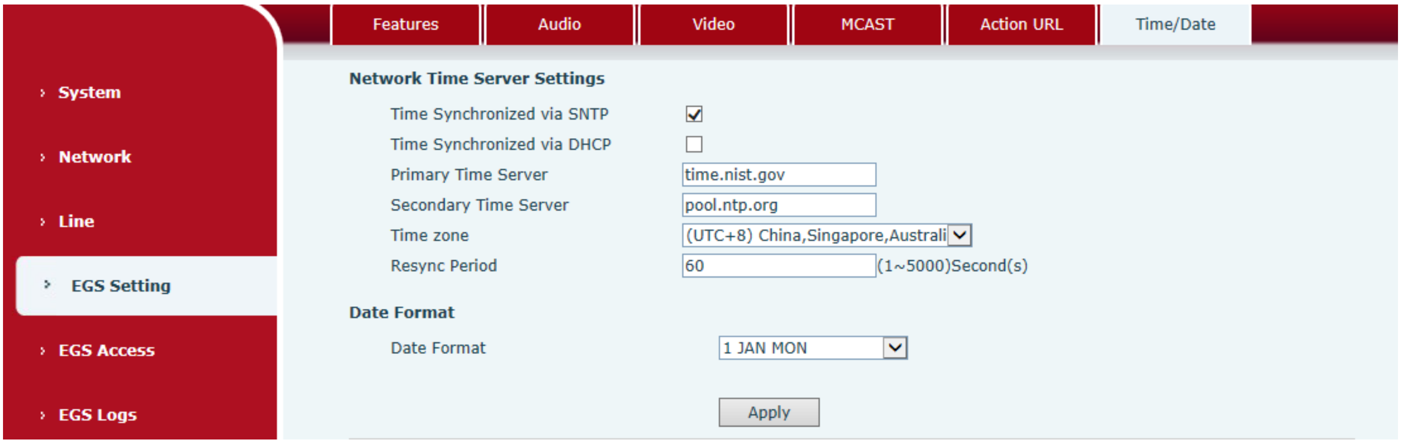
IP Changed

Idle To Busy

Busy To Idle

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



Network Time Server Settings

Time Synchronized via SNTP ☑

Time Synchronized via DHCP ☐

Primary Time Server: time.nist.gov

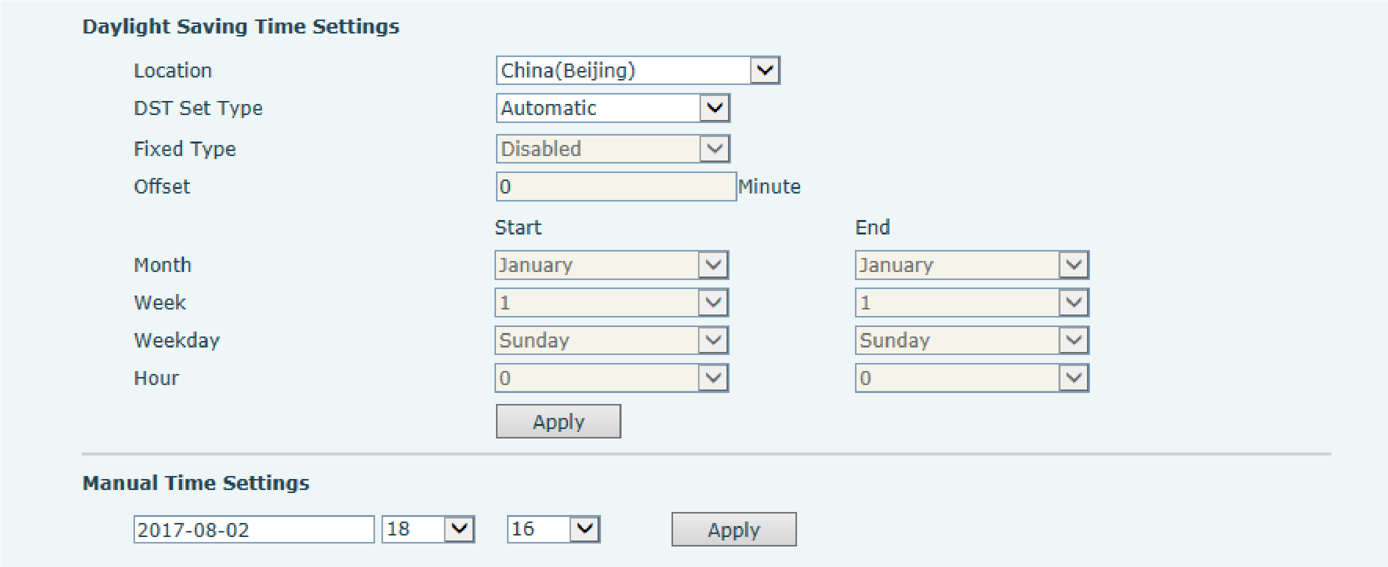
Secondary Time Server: pool.ntp.org

Time zone: (UTC+8) China,Singapore,Australi

Resync Period: 60 (1~5000)Second(s)

Date Format

Date Format: 1 JAN MON



Daylight Saving Time Settings

Location	China(Beijing)	
DST Set Type	Automatic	
Fixed Type	Disabled	
Offset	0 Minute	
	Start	End
Month	January	January
Week	1	1
Weekday	Sunday	Sunday
Hour	0	0

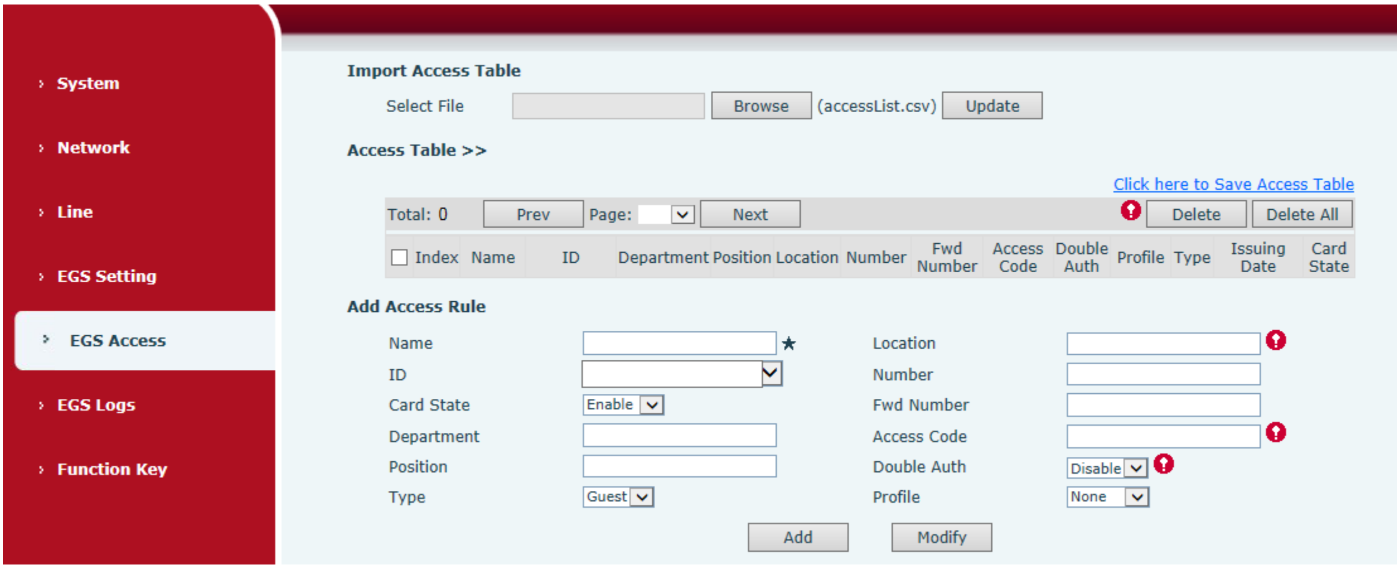
Manual Time Settings

2017-08-02 18 16

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 would 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 according to specific area
DST Set Type	Select automatic DST according to the preset rules of DST, or you can manually input rules
Offset	The DST offset time
Month Start	The DST start month
Week Start	The DST start week
Weekday Start	The DST start weekday
Hour Start	The DST start hour
Month End	The DST end month

Week End	The DST end week
Weekday End	The DST end weekday
Hour End	The DST end hour
Manual Time Settings	
The time might be set manually, needed user to disable SNTP service first.	

(5) EGS Access



Import Access Table

Select File (accessList.csv)

Access Table >>

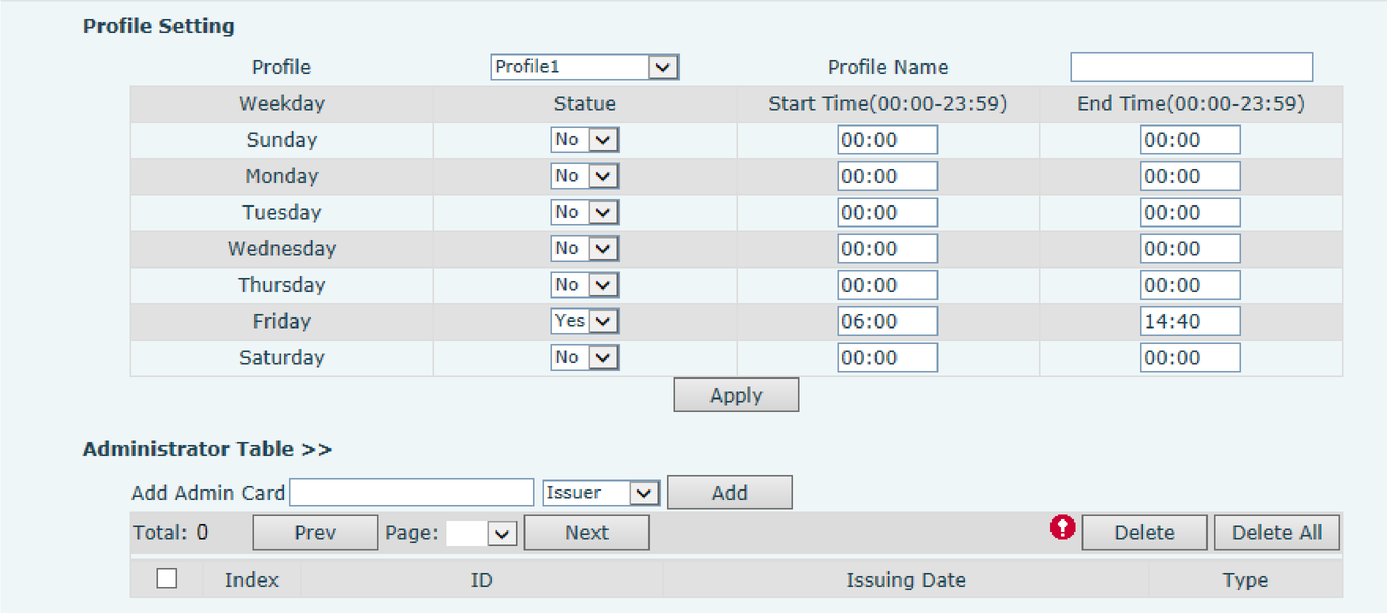
Click here to Save Access Table

Total: 0 Page:

□	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



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	Yes	06:00	14:40
Saturday	No	00:00	00:00

Administrator Table >>

Add Admin Card Issuer

Total: 0 Page:

□	Index	ID	Issuing Date	Type

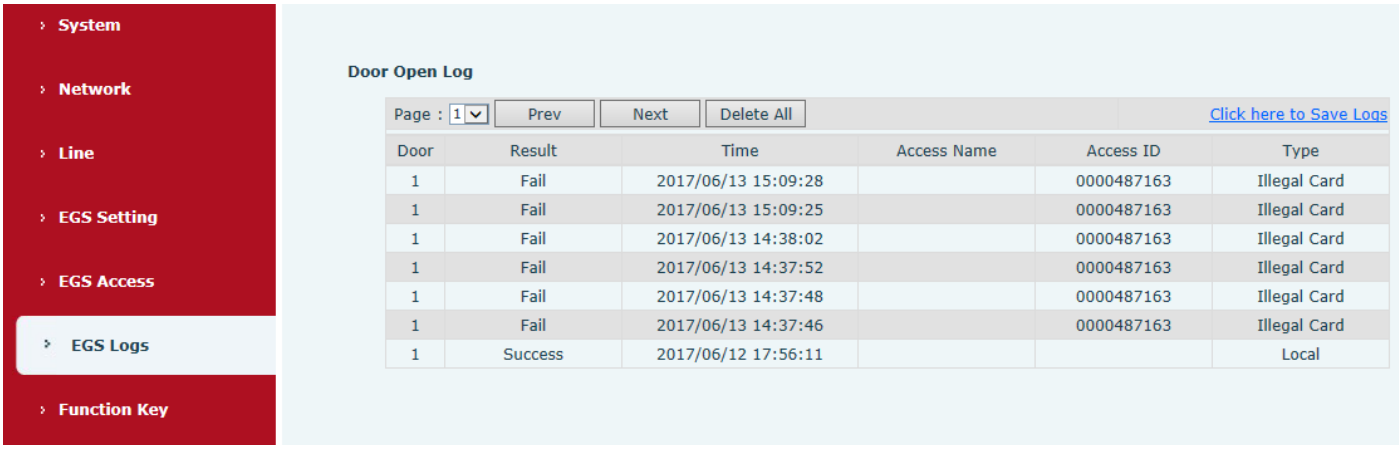
EGS Access	
Field Name	**Explanation**
Import Access Table	
Click the <Browse> to choose to import remote access list file (access List.csv) and then clicking <Update>	

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 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, 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 admin card list of the selected ID cards.
Delete All	Click <Delete All>, to delete all admin card lists.

(6) EGS Logs

According to open event log, can record up to 20W open event, after more than cover the old records. Click here to Save Logs Right click on the links to select save target as the door log can export CSV format.

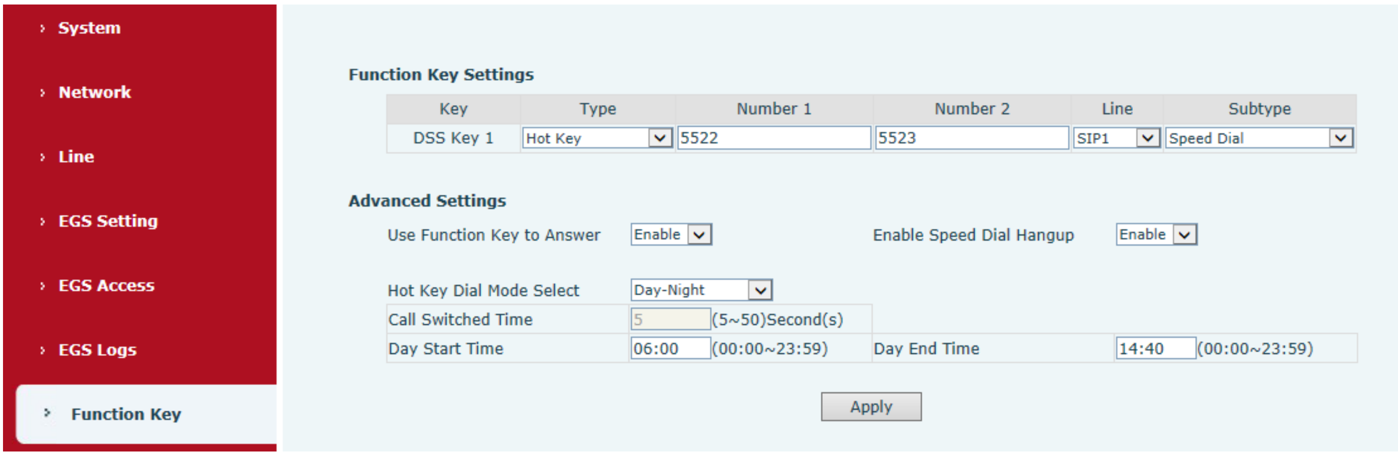


Door	Result	Time	Access Name	Access ID	Type
1	Fail	2017/06/13 15:09:28		0000487163	Illegal Card
1	Fail	2017/06/13 15:09:25		0000487163	Illegal Card
1	Fail	2017/06/13 14:38:02		0000487163	Illegal Card
1	Fail	2017/06/13 14:37:52		0000487163	Illegal Card
1	Fail	2017/06/13 14:37:48		0000487163	Illegal Card
1	Fail	2017/06/13 14:37:46		0000487163	Illegal Card
1	Success	2017/06/12 17:56:11			Local

Field Name	**Explanation**
Door Open Log	
Result	Show the results of the open the door (Succeeded or Failed)
Time	The time of opening door.
Duration	Duration of opening the 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) Function Key



Function Key Settings

Key	Type	Number 1	Number 2	Line	Subtype
DSS Key 1	Hot Key	5522	5523	SIP1	Speed Dial

Advanced Settings

Use Function Key to Answer: Enable

Enable Speed Dial Hangup: Enable

Hot Key Dial Mode Select: Day-Night

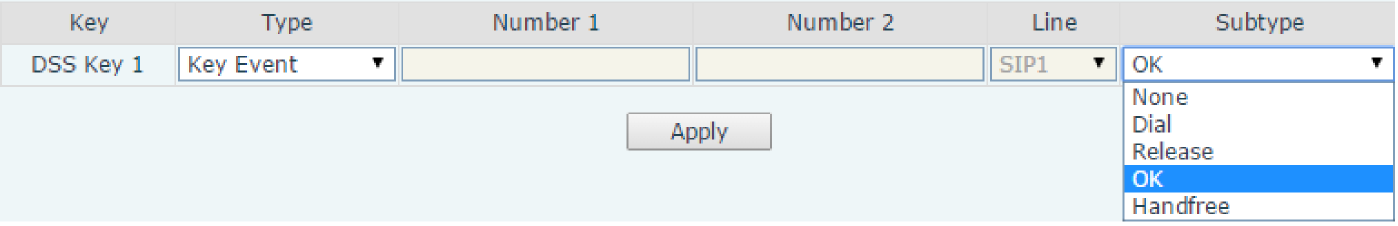
Call Switched Time: 5 (5~50)Second(s)

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

Day End Time: 14:40 (00:00~23:59)

➢ Key Event

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

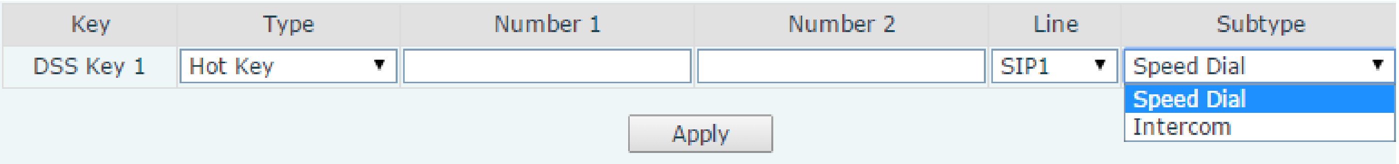


Key	Type	Number 1	Number 2	Line	Subtype
DSS Key 1	Key Event			SIP1	OK

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 a IP call.



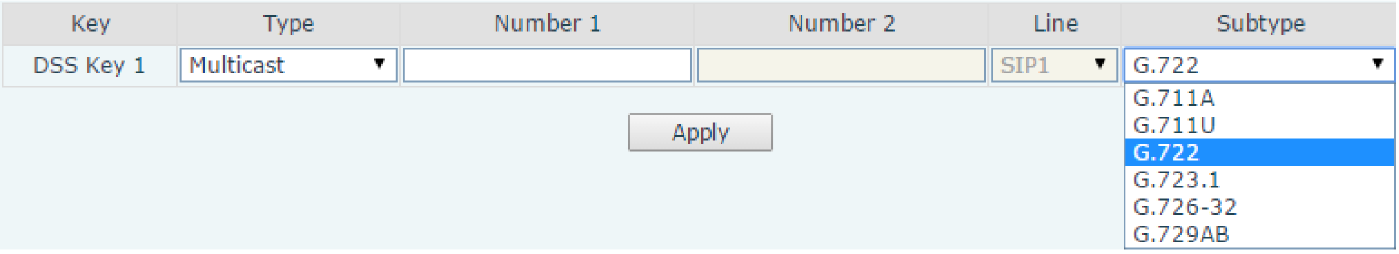
Key	Type	Number 1	Number 2	Line	Subtype
DSS Key 1	Hot Key ▼			SIP1 ▼	Speed Dial ▼

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

V. Appendix

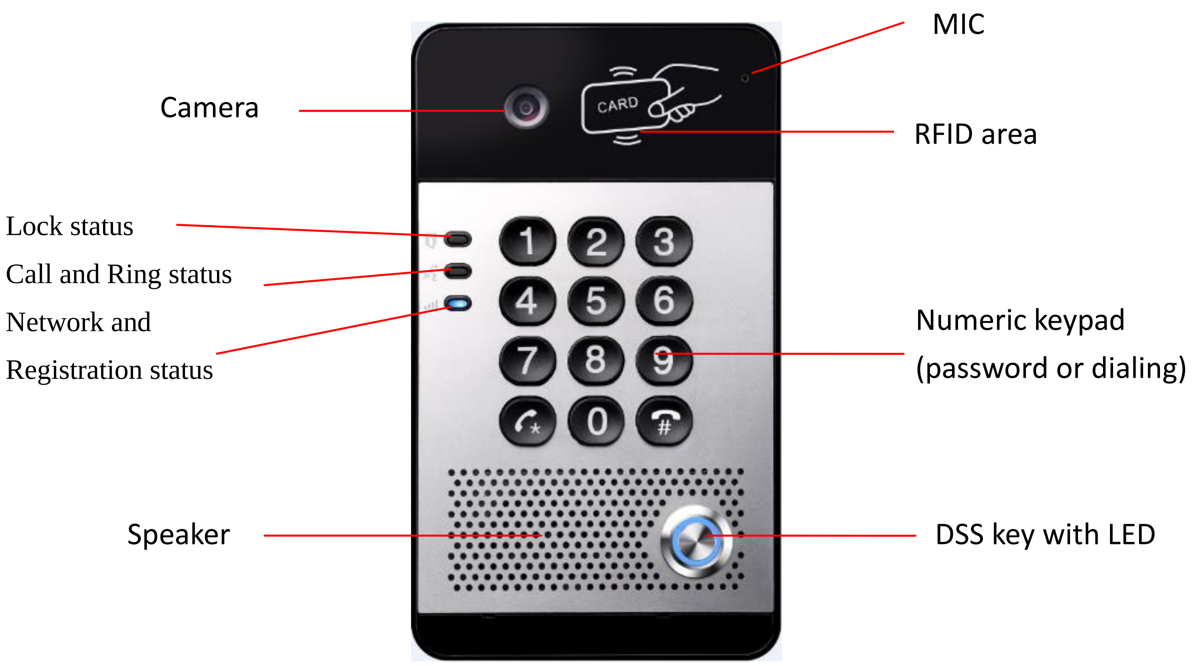
1. Technical parameters

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
Camera		1/4 "color CMOS, 1 megapixel, wide angle
RFID/IC card reader		EM4100 (125Khz) MIFARE One(13.56Mhz)
Power supply mode		12V / 1A DC or PoE
PoE		PoE 802.3af (Class 3 - 6.49~12.95W)
Cables		CAT5 or better
Shell Material		Metal panel, ABS face-piece and back shell
Working temperature		-10°C to 60°C
Working humidity		10% - 90%
Storage temperature		-40°C to 70°C
Installation way		Wall-mounting
External size		160 x 93 x 35mm
Package size		209x118x64mm
Equipment weight		330g
Gross weight		450g

2. Basic functions

- 2 SIP lines
- PoE Enabled
- Full-duplex speakerphone (HF)
- Numeric keypad (dialing pad or password input)
- Intelligent DSS Keys (Speed Dial/Intercom etc)
- Wall-mounting
- Integrated RFID Card reader
- 1 indoor switch interface
- 1 electric lock relay
- External power supply
- Door phone opening methods: call, password, RFID card, indoor switch
- Protection level: IP65, 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 EGS Setting\Feature\Advanced Settings.

✧ Input password via keypad and press the "#" key, then the door would be unlocked.

2) Private access code

✧ Set <Add Access Rule\Access Code> and enable local authentication.

✧ Input access code via keypad and press the "#" key, then the door would 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 directly)

✧ 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.

✧ SIP door phone answers the call automatically.

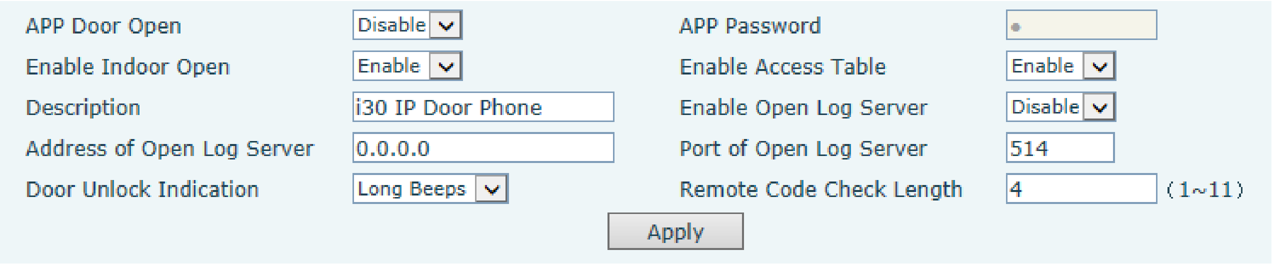
✧ Owner inputs corresponding access codes via SIP phone keypad to unlock the door.

● Swiping cards

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

● Indoor switch

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

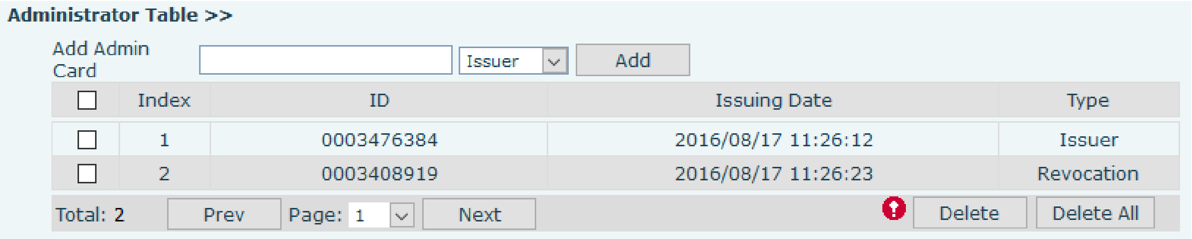


APP Door Open	Disable	APP Password	•
Enable Indoor Open	Enable	Enable Access Table	Enable
Description	i30 IP Door Phone	Enable Open Log Server	Disable
Address of Open Log Server	0.0.0.0	Port of Open Log Server	514
Door Unlock Indication	Long Beeps	Remote Code Check Length	4 (1~11)

2. Management of card

1) Administrator Table

<Issuer> and <Revocation>



Administrator Table >>

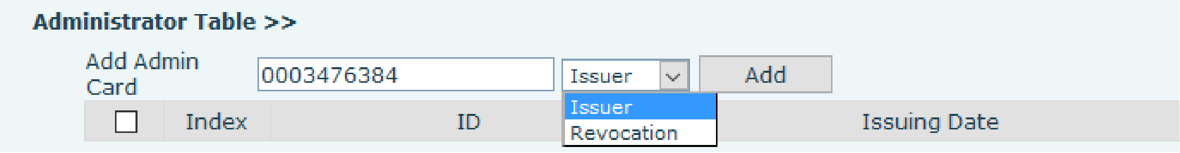
Add Admin Card

□	Index	ID	Issuing Date	Type
□	1	0003476384	2016/08/17 11:26:12	Issuer
□	2	0003408919	2016/08/17 11:26:23	Revocation

Total: 2

- **Add Administrator cards**

Input a card’s ID, selected <Issuer> or <Revocation> in the types and then click <Add>; you would add administrator card.



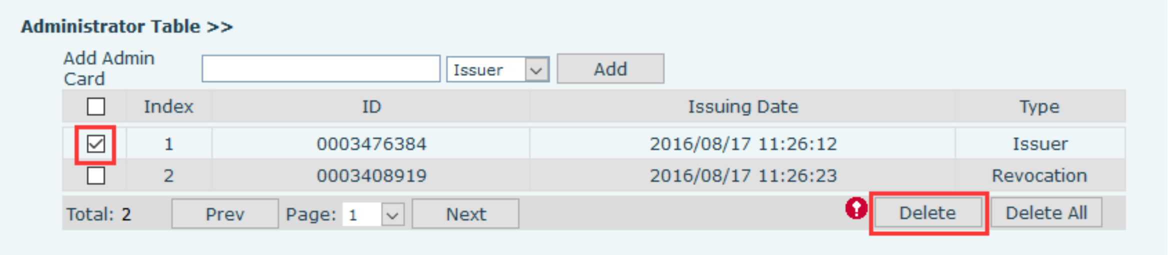
Administrator Table >>

Add Admin Card: 0003476384

□	Index	ID	Issuing Date

- **Delete Administrator cards**

Select the admin card need to be deleted, click <Delete>.



Administrator Table >>

Add Admin Card

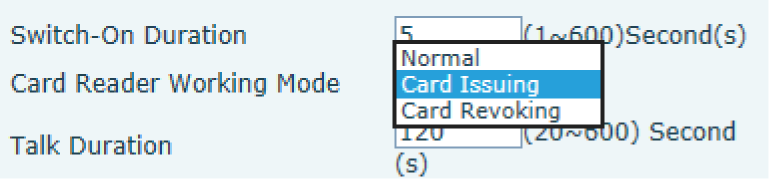
□	Index	ID	Issuing Date	Type
☑	1	0003476384	2016/08/17 11:26:12	Issuer
□	2	0003408919	2016/08/17 11:26:23	Revocation

Total: 2

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>.



Switch-On Duration: 5 (1~600)Second(s)

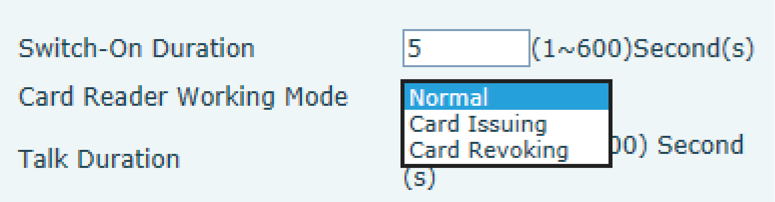
Card Reader Working Mode: Card Issuing

Talk Duration: 120 (20~600) Second (s)

✧ Click <Apply>, Card Reader would enter 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.

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



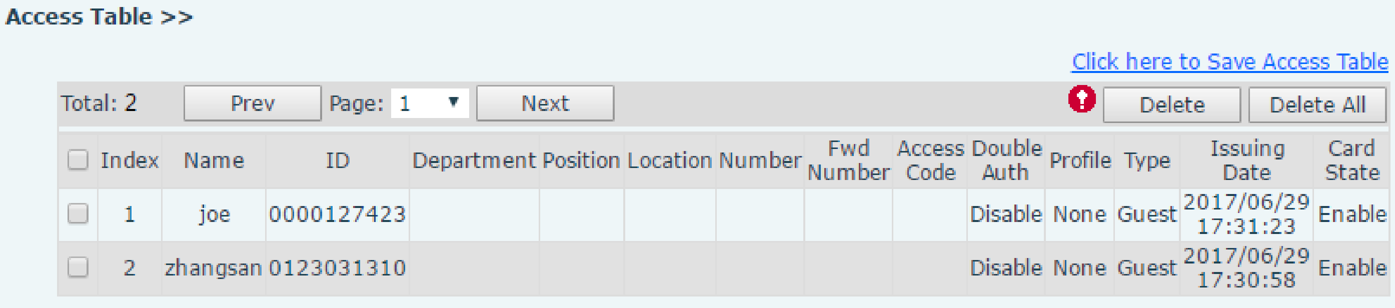
Switch-On Duration: 5 (1~600)Second(s)

Card Reader Working Mode: Normal

Talk Duration: 00) Second (s)

✧ Click <Apply>, Card Reader would back to the Normal status.

✧ The issuing records can be found from the door card table list.



Access Table >>

Click here to Save Access Table

Total: 2 | Prev | Page: 1 ▾ | Next | Delete | Delete All

□	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

- **Methods 2:** used to add cards for professionals

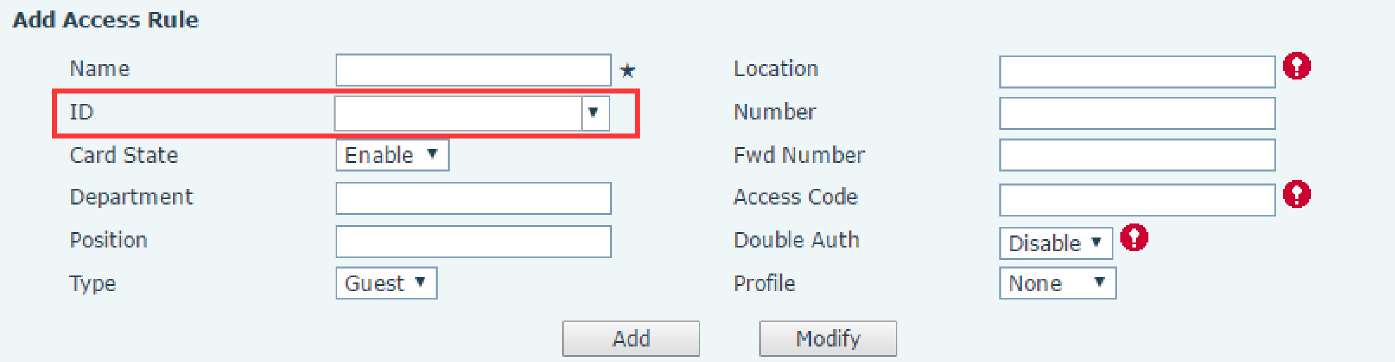
✧ Use issuer admin card to touch card reader induction area, and it would enter issuing card status.

✧ 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 go back to normal working status.

- **Method 3:** use to add few cards

✧ Input cards number in <EGS Setting\Add Access Rule\ID> page, and then click <Add>

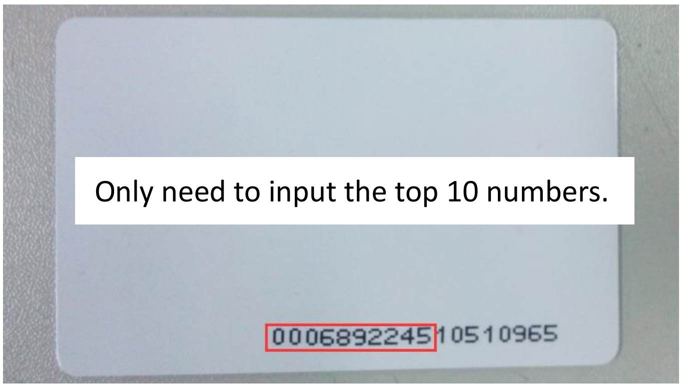


Add Access Rule

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

Add | Modify

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

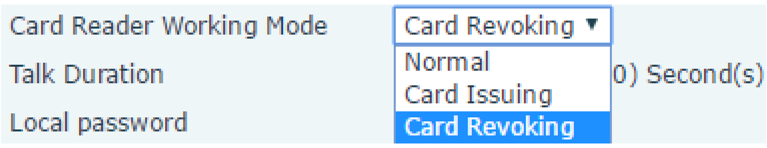


Only need to input the top 10 numbers.

3) Delete user cards

- **Method 1:** used to batch delete cards for starters.

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



Card Reader Working Mode — Card Revoking ▼

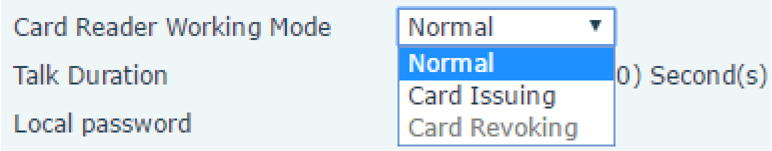
Talk Duration — 0) Second(s)

Local password

✧ Click <Apply>, card reader would enter 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.

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



Card Reader Working Mode — Normal ▼

Talk Duration — 0) Second(s)

Local password

✧ Click <Apply>, card reader would go 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 enter revoking card status.

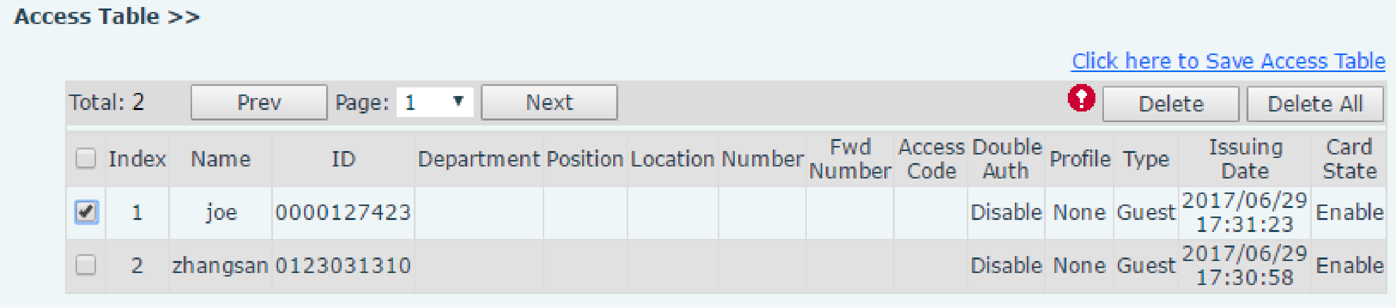
✧ Use the cards you want to delete from system to touch card reader induction area, and you might hear the card reader confirmed indication tone. Repeat step 2 to delete cards.

✧ Use revocation admin card to touch card reader induction area, and it would go back to card read only status.

- **Method 3**: bulk delete or partially delete card records

✧ In web page<EGS Cards →Door Card Table>select the card ID and then click <Delete>.

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



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