i30 SIP Video Door Phone

User Manual V1.0

Document VER	Firmware VER	Explanation	Time
V1.0	2.1.1.2545	Initial issue	20161117

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

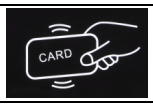
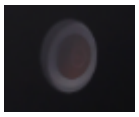
I. Product introduction

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

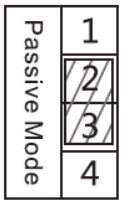
- Confirm whether the equipment of the power cord, network cable, electric lock control line connection and the boot-up is normal. (Check the network state of light)

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 active mode)



Jumper in passive mode

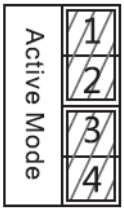
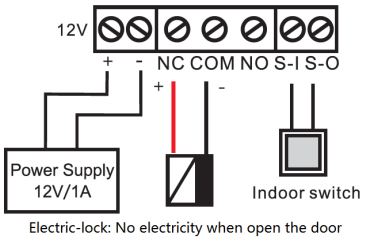
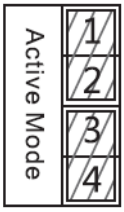
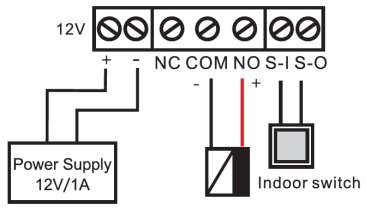
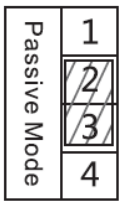
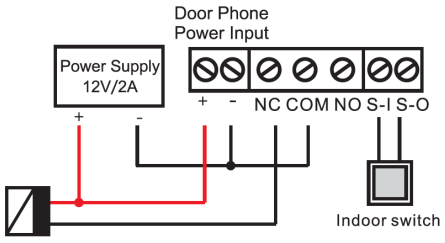
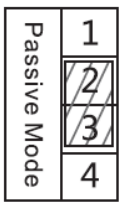
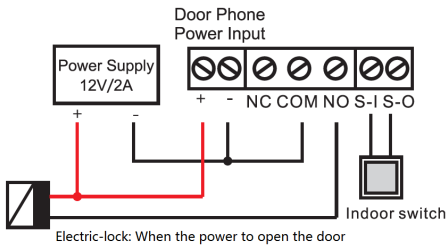
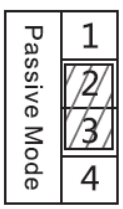
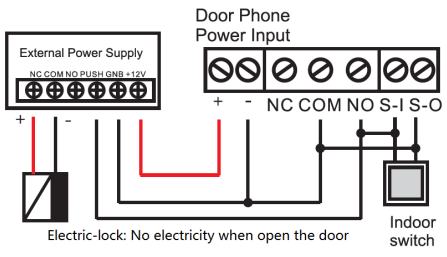
Jumper in active mode

【Note】When the device is in active mode, it can drive 12V/700mA switch output maximum（maximally）; if the electric-lock needs power supply over 12V/70mA, 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.

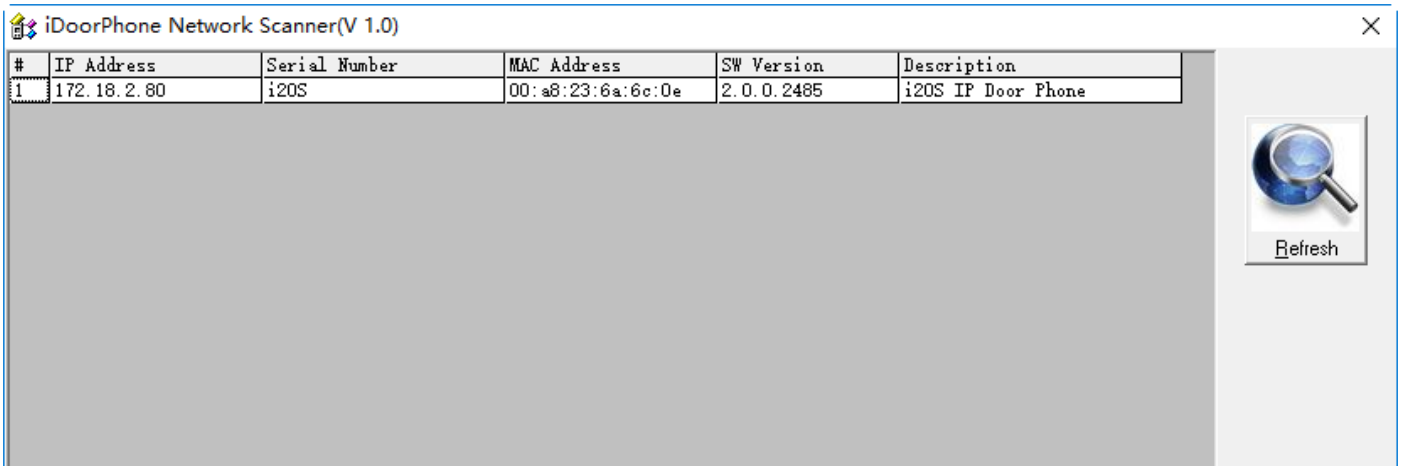
Driving Mode		Electric lock		Jumper port	Connections
Active	Passive	No electricity when open	When the power to open		
√					 Electric-lock: No electricity when open the door
√			√		 Electric-lock: When the power to open the door
	√	√			 Electric-lock: No electricity when open the door
	√		√		 Electric-lock: When the power to open the door
	√	√			 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.
- **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).



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.

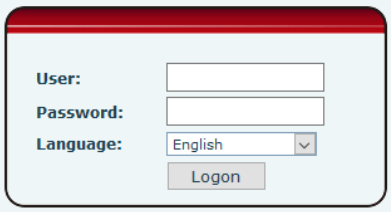
When door has been opened, the device would play sirens sound to prompt guests.

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

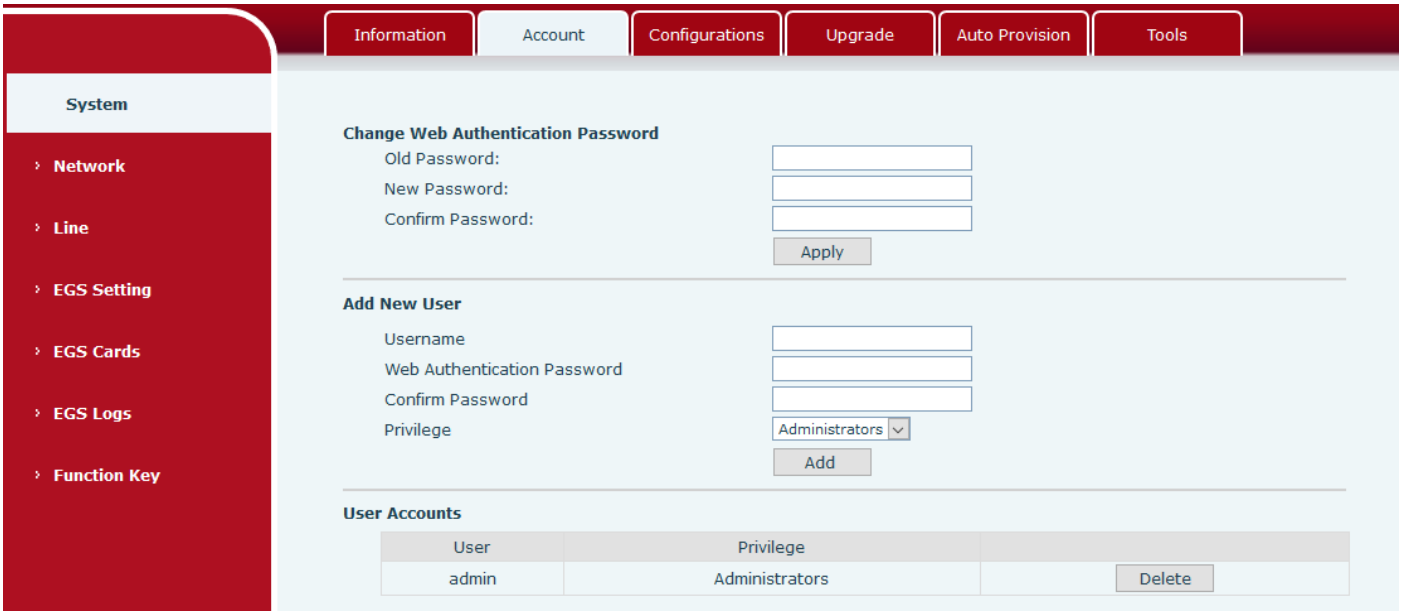
(1) System

a) Information

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.

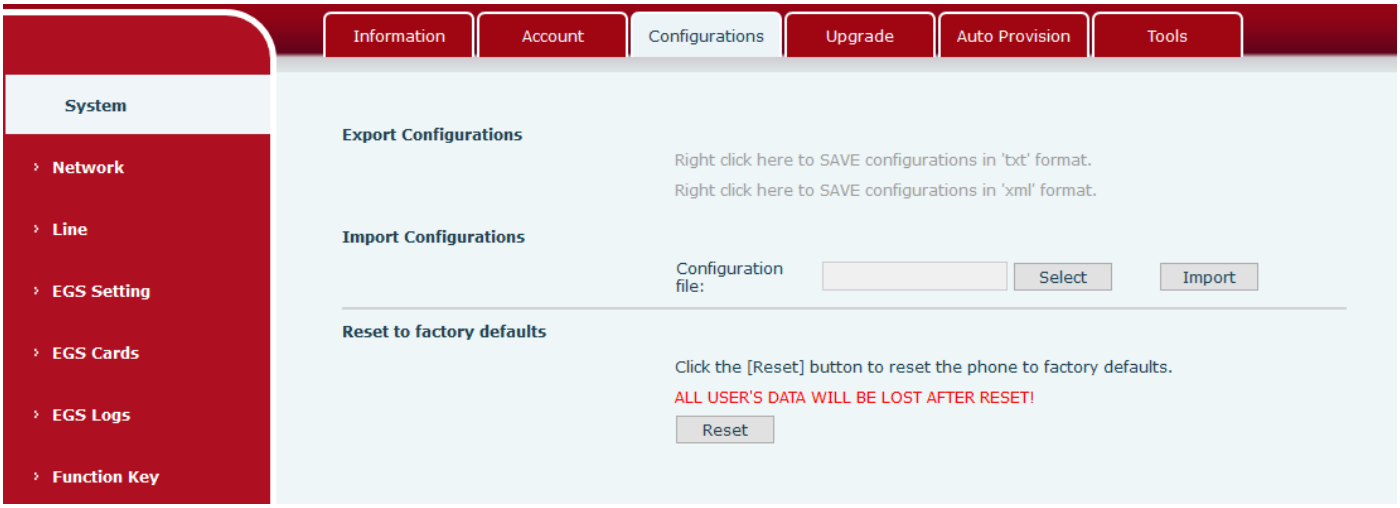
b) Account

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



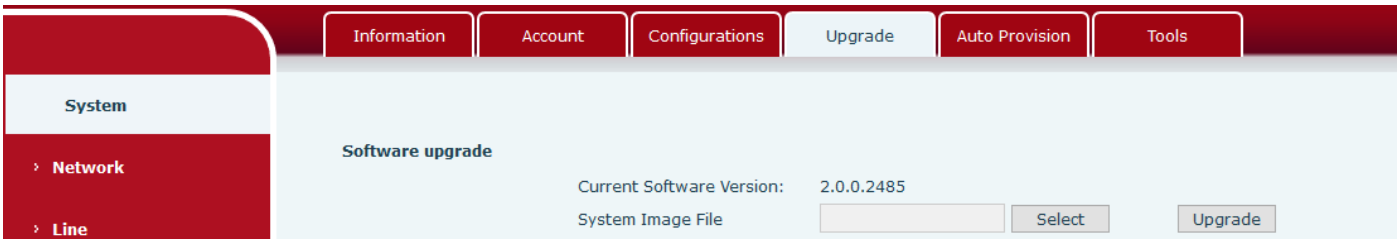
Account	
Field Name	**Explanation**
Change Web Authentication Password	
You can modify the login password of the account	
Add New User	
You can add new user	
User Accounts	
Show the existed user accounts' information	

c) Configurations



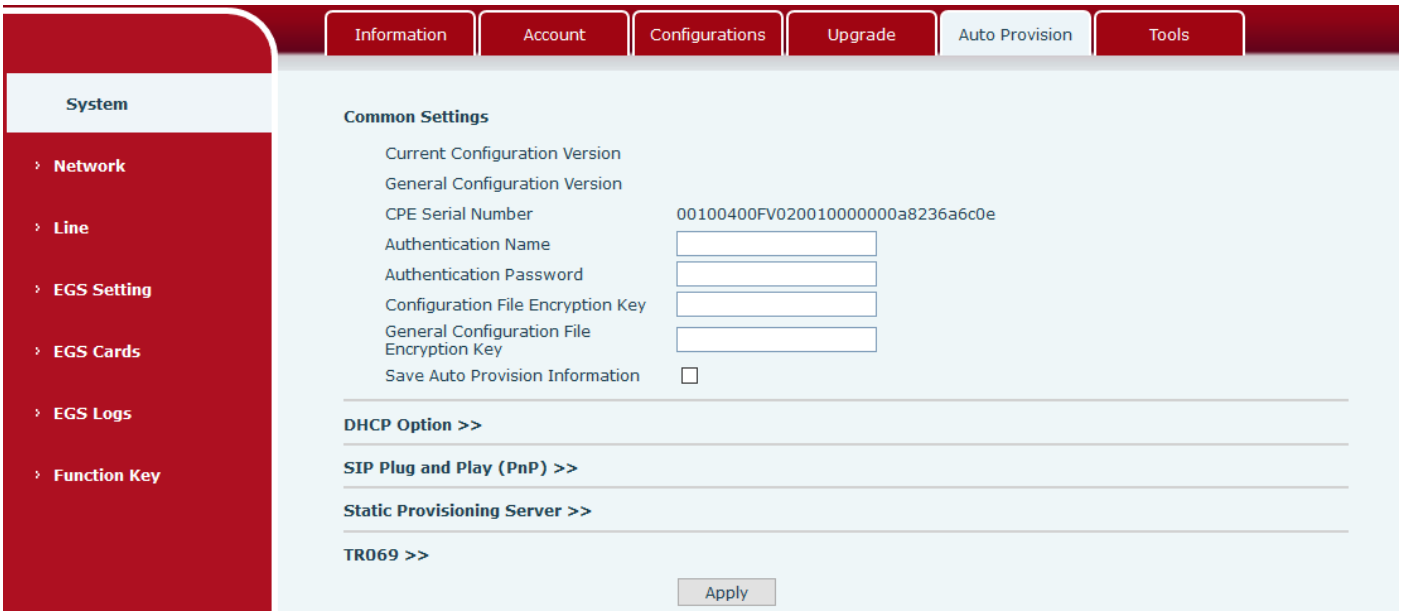
Configurations	
Field Name	**Explanation**
Export Configurations	Save the equipment configuration to a txt or xml file. Please right click on the choice and then choose "Save Link As."
Import Configurations	Find the config file, and press **Update** to load it to the equipment.
Reset to factory defaults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

d) Upgrade



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

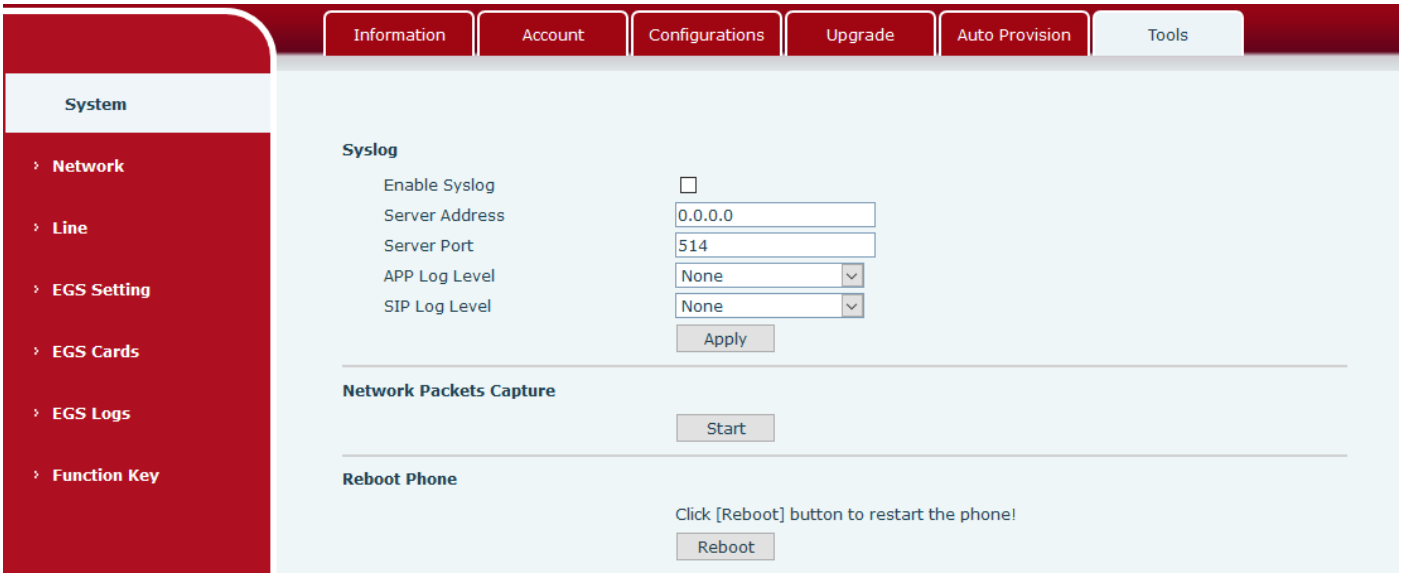
e) Auto Provision



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) Tools



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

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's time.
Settings	
Select the appropriate network mode. The equipment supports three network modes:	
Static IP	Network parameters must be entered manually and would 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 would 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 would save the new settings and apply them. If a new IP address was entered for the equipment, it must be used to login to the phone after clicking the **Apply** button.	

b) Advanced

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

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

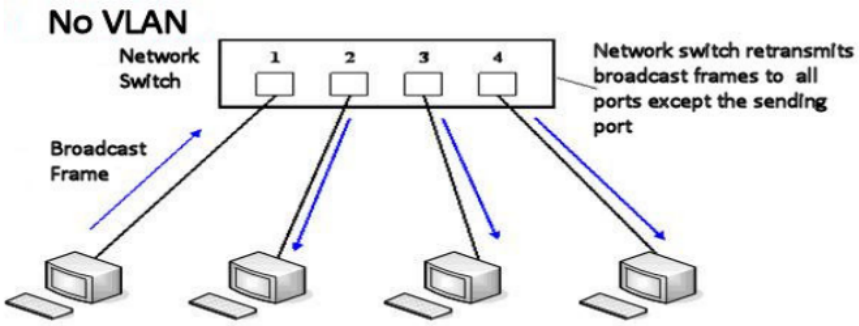


Chart 1

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

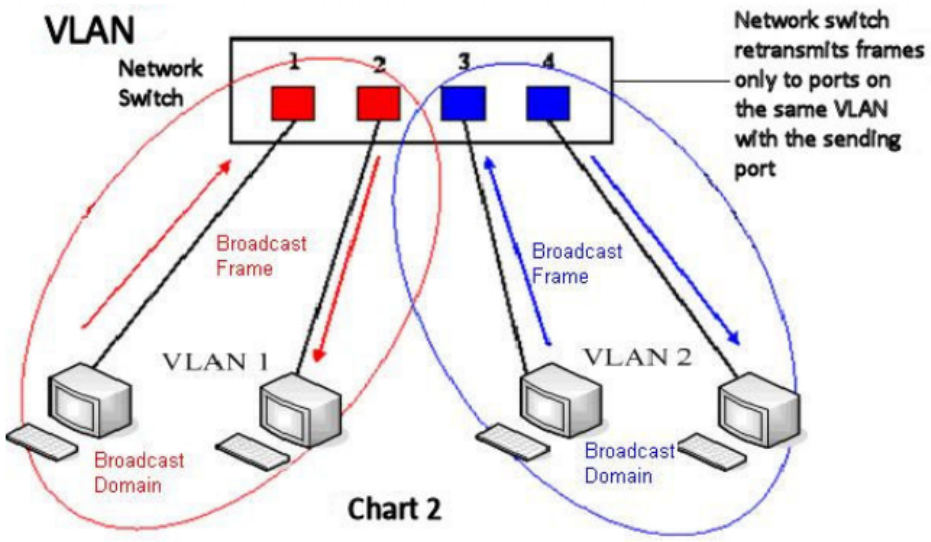
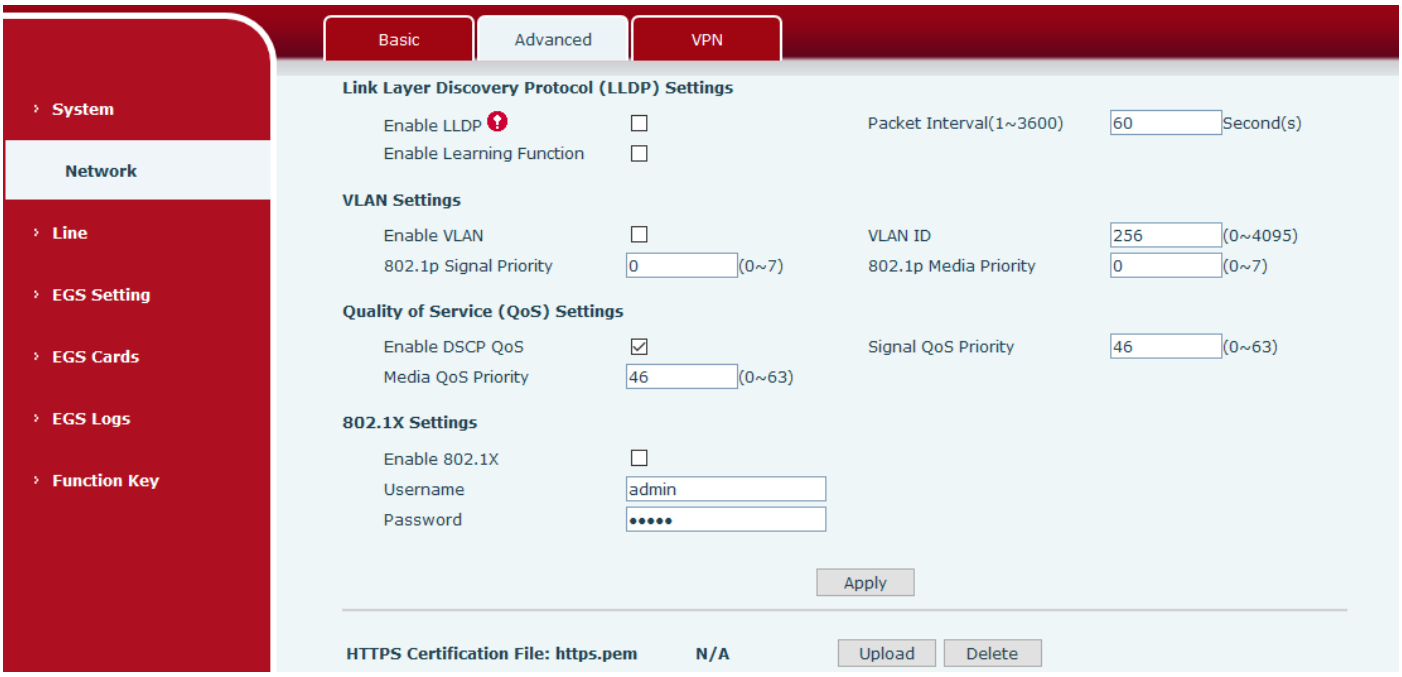
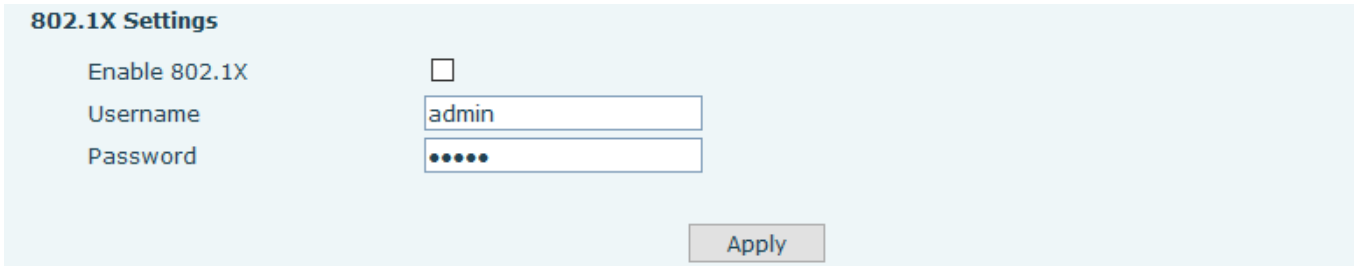


Chart 2

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

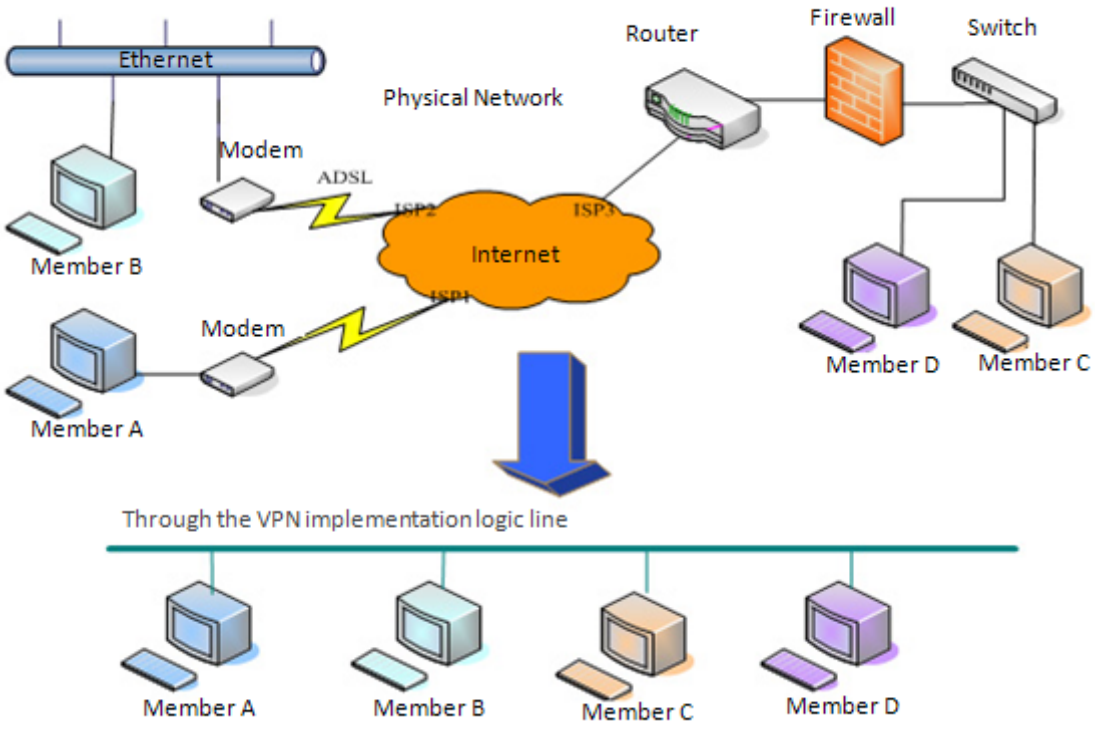


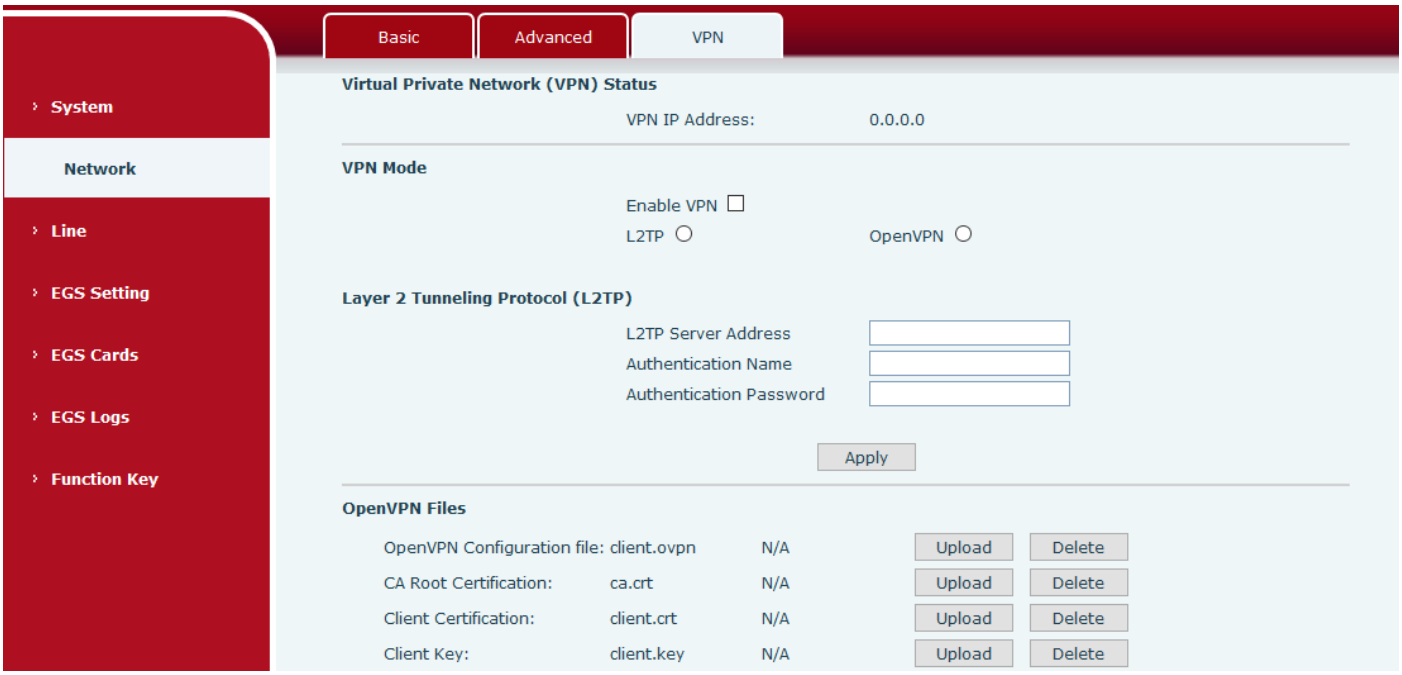
Advanced	
Field Name	**Explanation**
Link Layer Discovery Protocol (LLDP) Settings	
Enable LLDP	Enable or Disable Link Layer Discovery Protocol (LLDP)
Enable Learning Function	Enables the telephone to synchronize its VLAN data with the Network Switch. The telephone would automatically synchronize DSCP,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

802.1X Settings	
	
Enable 802.1X	Enable or Disable 812.1X
Username	802.1X user account
Password	802.1X password
HTTPS Certification File	
Upload or delete HTTPS Certification File	

c) VPN

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



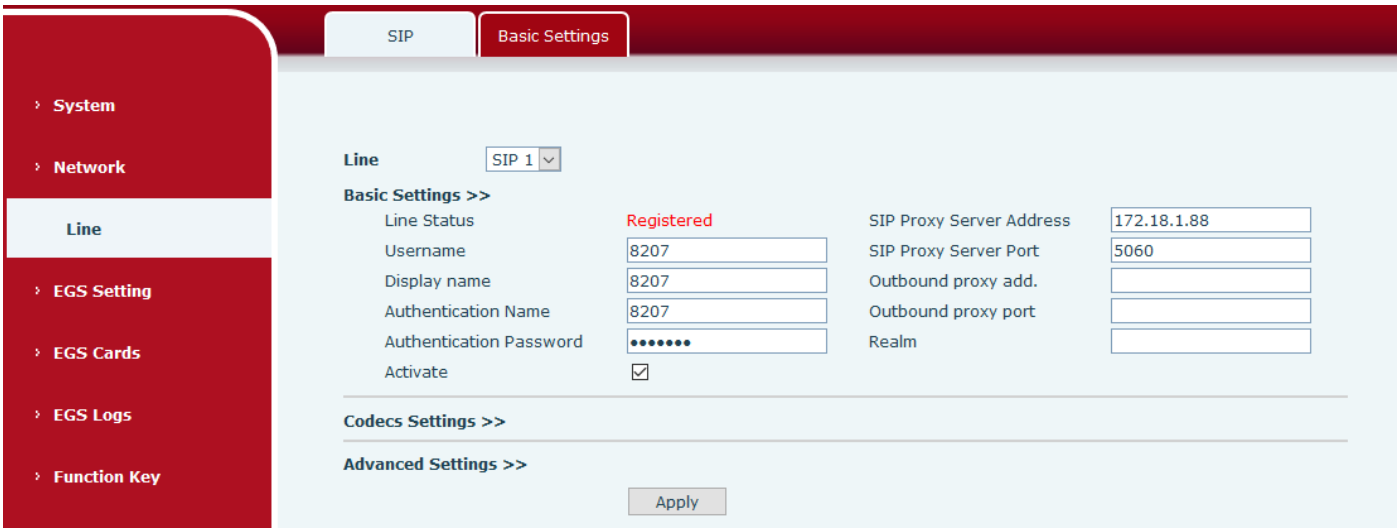


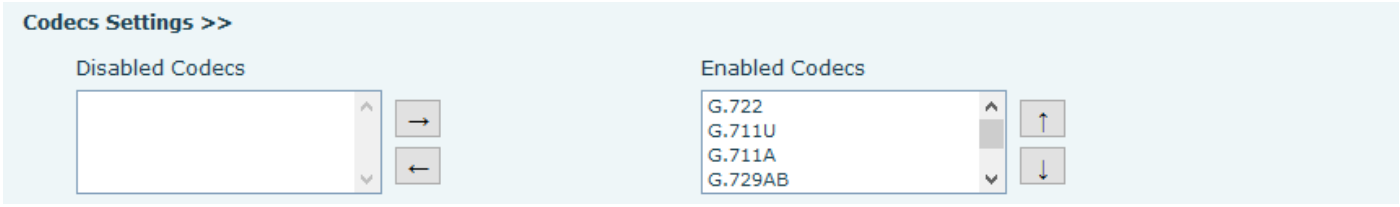
Field Name	Explanation
VPN IP Address	Shows the current VPN IP address.
VPN Mode	
Enable VPN	Enable/Disable VPN.
L2TP	Select Layer 2 Tunneling Protocol
OpenVPN	Select OpenVPN Protocol. (Only one protocol may be activated. After the selection is made, the configuration should be saved and the phone be 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	

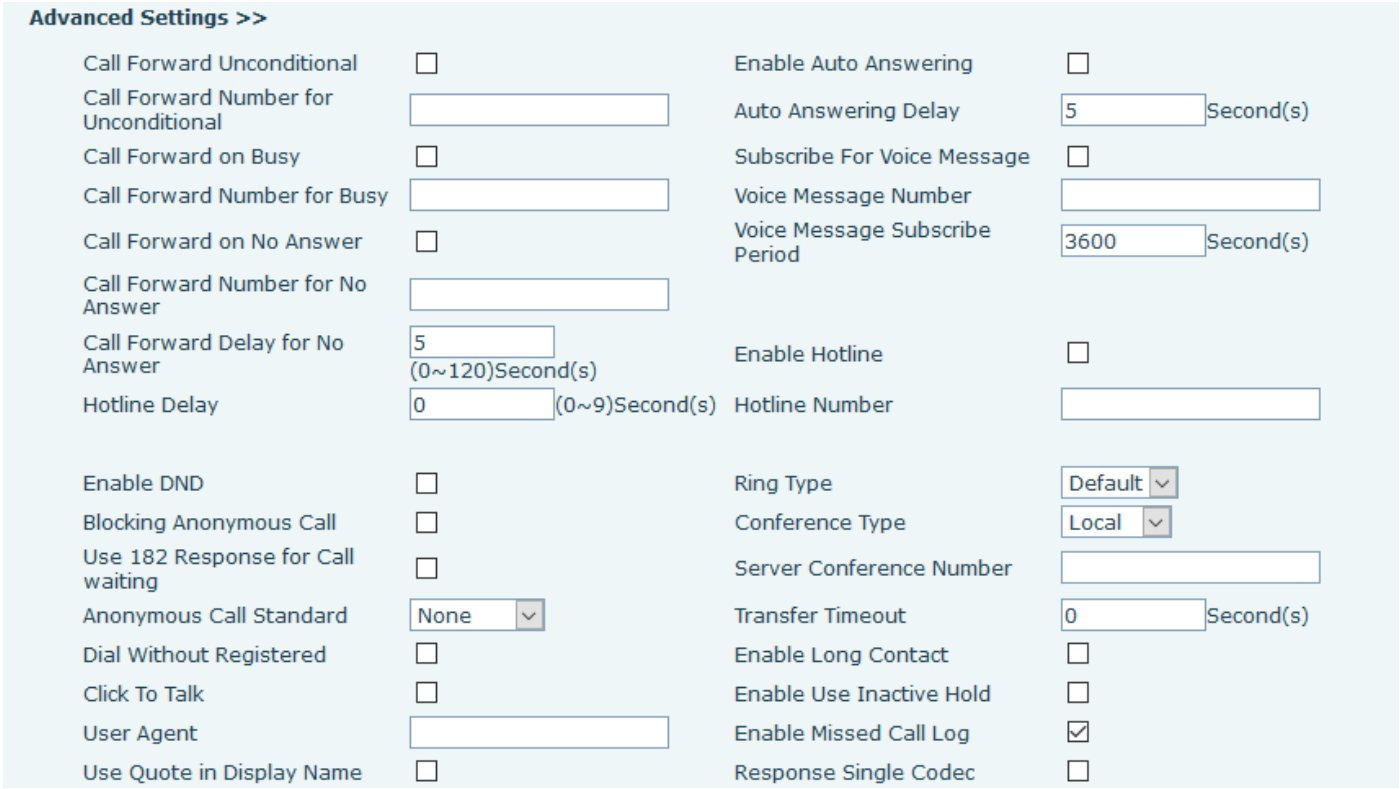
(3) Line

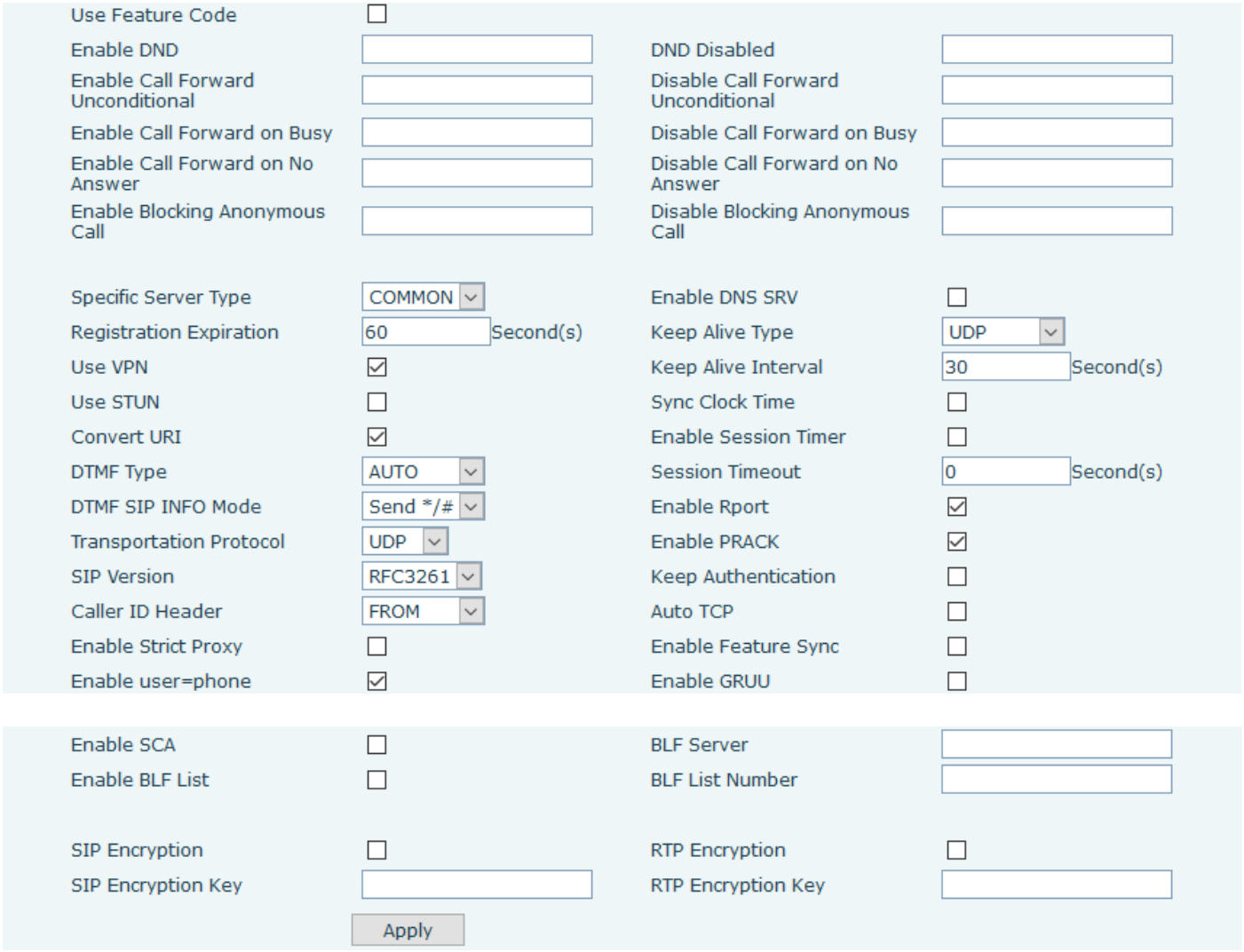
a) SIP

You can configure a SIP server on this page.









SIP	
Field Name	**Explanation**
Basic Settings (Choose the SIP line to configured)	
Line Status	Display the current line status after 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

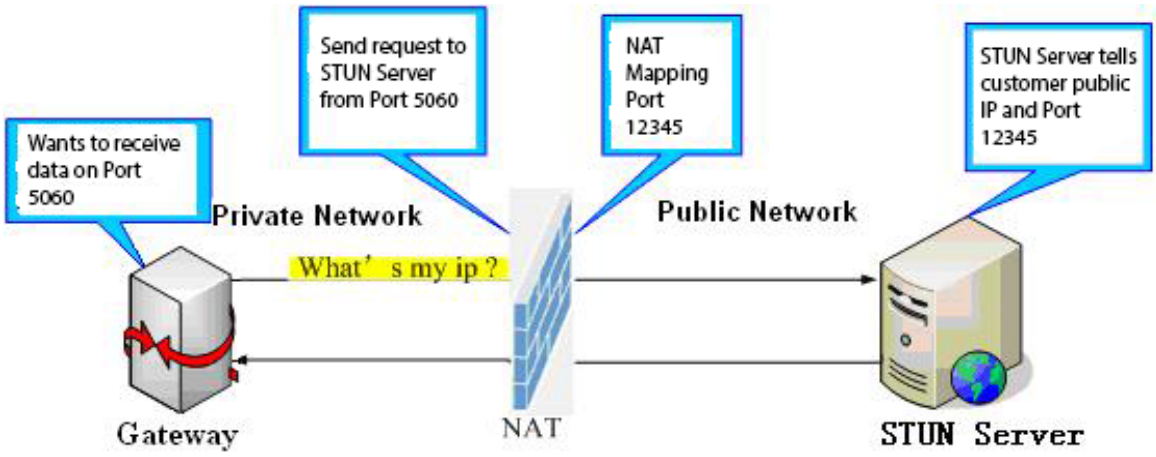
SIP Proxy Server Port	Enter the SIP proxy server port, default is 5060
Outbound proxy address	Enter the IP or FQDN address of outbound proxy server provided by the service provider
Outbound proxy port	Enter the outbound proxy port, default is 5060
Realm	Enter the SIP domain if it is needed by the service provider
Codecs Settings	
Set the priority and availability of the codecs by adding or removing them from the list.	
Advanced Settings	
Call Forward Unconditional	Enable unconditional call forwarding, all incoming calls would be forwarded to the number specified in the next field
Call Forward Number for Unconditional	Set the number of unconditional call forwarding
Call Forward on Busy	Enable call forward on busy, when the phone is busy, any incoming call would be forwarded to the number specified in the next field
Call Forward Number for Busy	Set the number of call forwarding when the I30 is 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 would 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 dial it
Enable Auto Answering	Enable auto-answering, the incoming calls would be answered automatically after the delay time
Auto Answering Delay	Set the delay for incoming call before the system automatically answered answer it
Subscribe For Voice Message	Enable the device to subscribe a voice message waiting notification, if you enable it , the device would 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 period of voice message notification subscription
Enable Hotline	Enable hotline configuration, the device would dial to the specific number immediately at audio channel opened by off-hook or turning on hands-free speaker or headphone

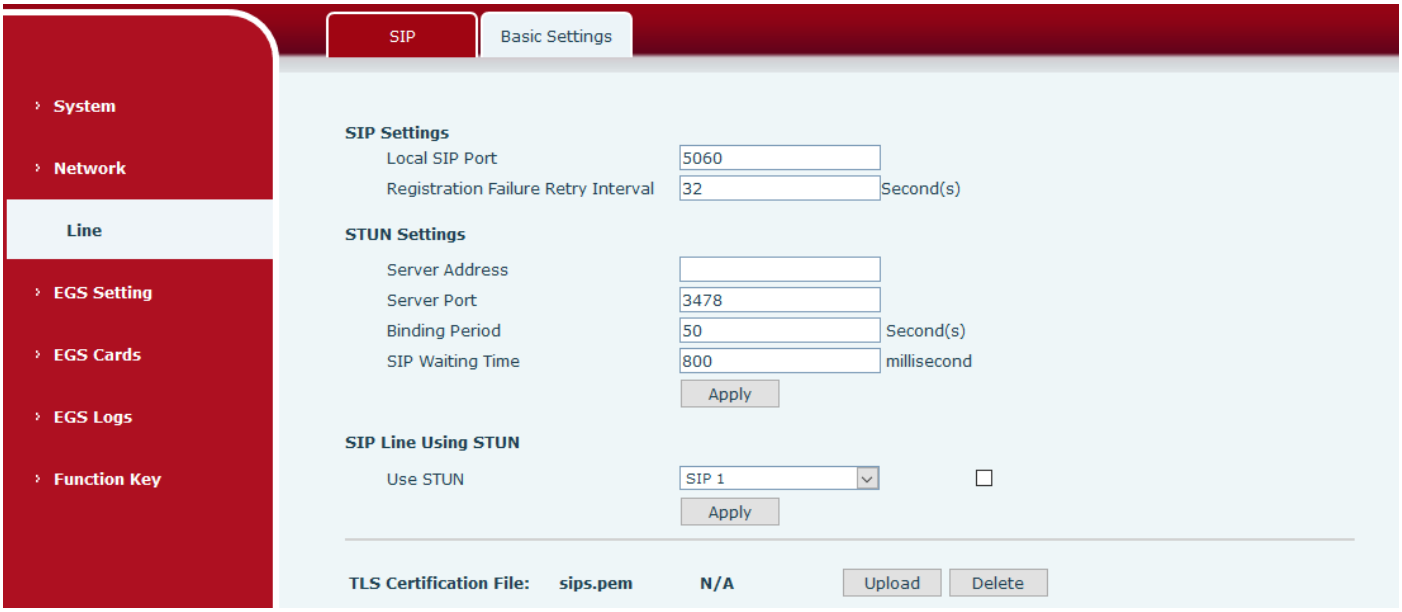
Hotline Number	Set the hotline dialing number
Enable DND	Enable Do-not-disturb, any incoming call on this line would be rejected automatically
Blocking Anonymous Call	Reject any incoming call without presenting caller ID
Use 182 Response for Call waiting	Set the device to use 182 response code at call waiting response
Anonymous Call Standard	Set the standard to be used for anonymous call
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; I30 maximally 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 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 it is enabled, the phone would save missed calls into the call history record.
Response Single Codec	If it is enabled, the device would use single codec in response to an incoming call request
Use Feature Code	When this setting is enabled, the features in this section would not be handled by the device itself but by the server instead. In order to control the authorization of the features, the device would 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 period
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 would 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 would 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 would be ended if there is not new session timer event updating 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 of previous authentication
Auto TCP	Using TCP protocol to guarantee usability of transport when SIP messages have more than 1500 bytes
Enable Feature Sync	Feature Sync with server
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)
BLF Server	The registered server would 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 would 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 would be encrypted
SIP Encryption Key	Set the pass phrase for SIP encryption
RTP Encryption	Enable RTP encryption such that RTP transmission would be encrypted
RTP Encryption Key	Set the pass phrase for RTP encryption

b) Basic Settings

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



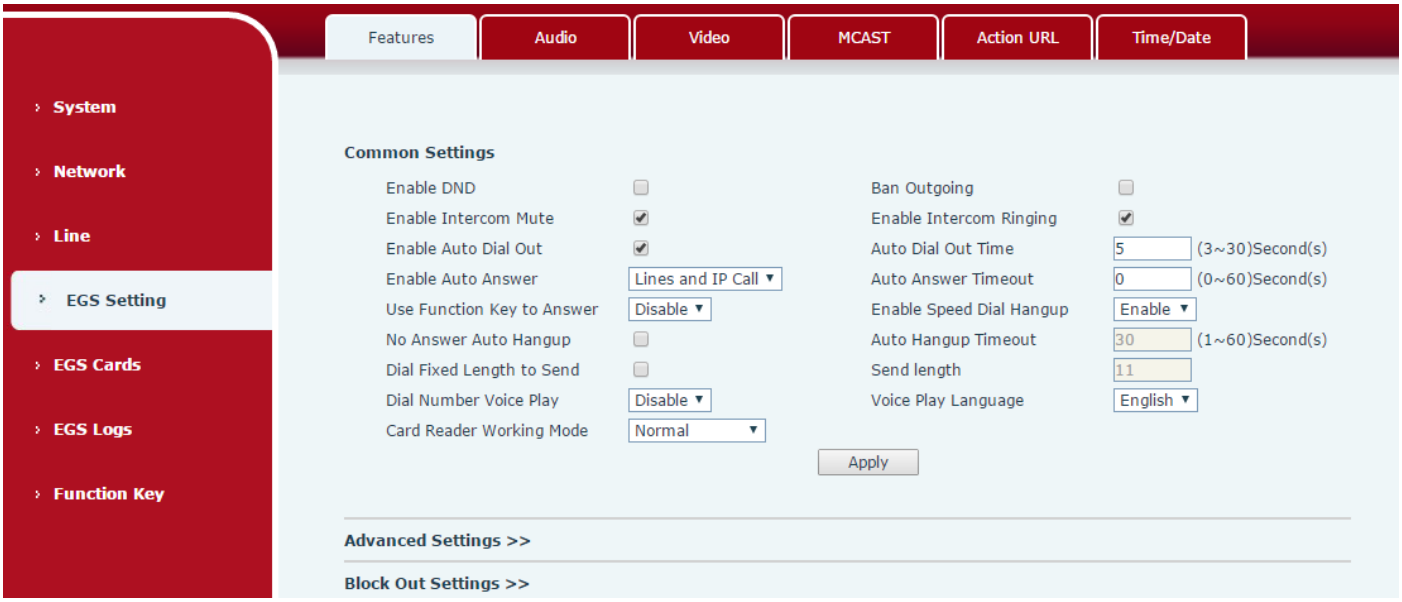


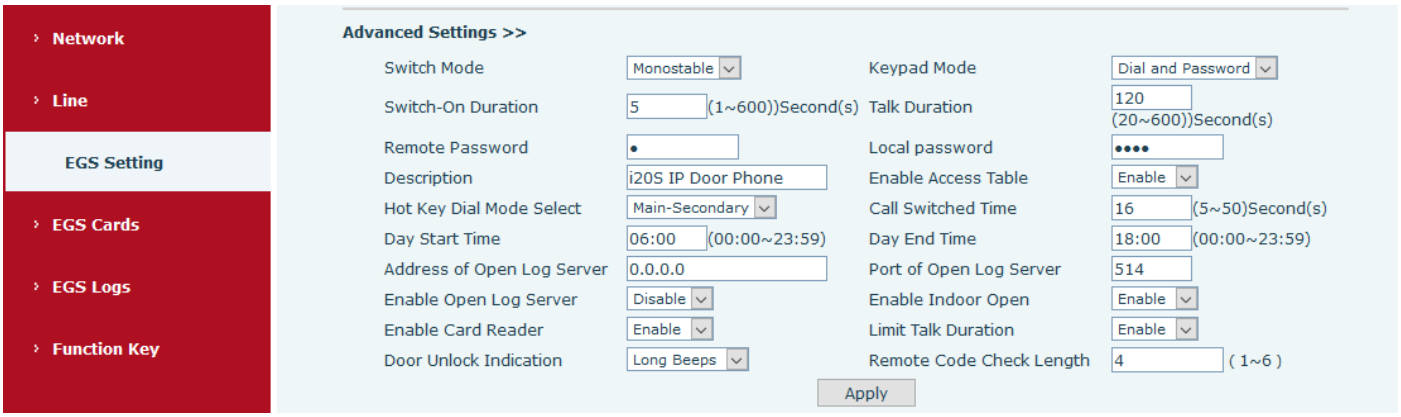
Basic Settings	
Field Name	**Explanation**
SIP Settings	
Local SIP Port	Set the local SIP port used to send/receive SIP messages.
Registration Failure Retry Interval	Set the retry interval of SIP registration when registration failed.
STUN Settings	
Server Address	STUN Server IP address

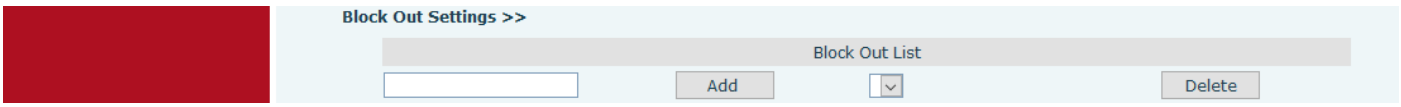
Server Port	STUN Server Port – Default is 3478.
Binding Period	STUN blinding period – STUN packets are sent once every this period to keep the NAT mapping active.
SIP Waiting Time	Waiting time for SIP. This would vary depending on the network.
SIP Line Using STUN(SIP1 or SIP2)	
Use STUN	Enable/Disable STUN on the selected line.
TLS Certification File	
Upload or delete the TLS certification file used for encrypting SIP transmission.	
Note: the SIP STUN is used to achieve the penetration of SIP NAT; it is a realization of service, when the equipment is configured the STUN server IP and port (usually the default is 3478), and selected “Use Stun SIP server”, you can make common SIP equipment achieve penetration.	

(4) EGS Setting

a) Features







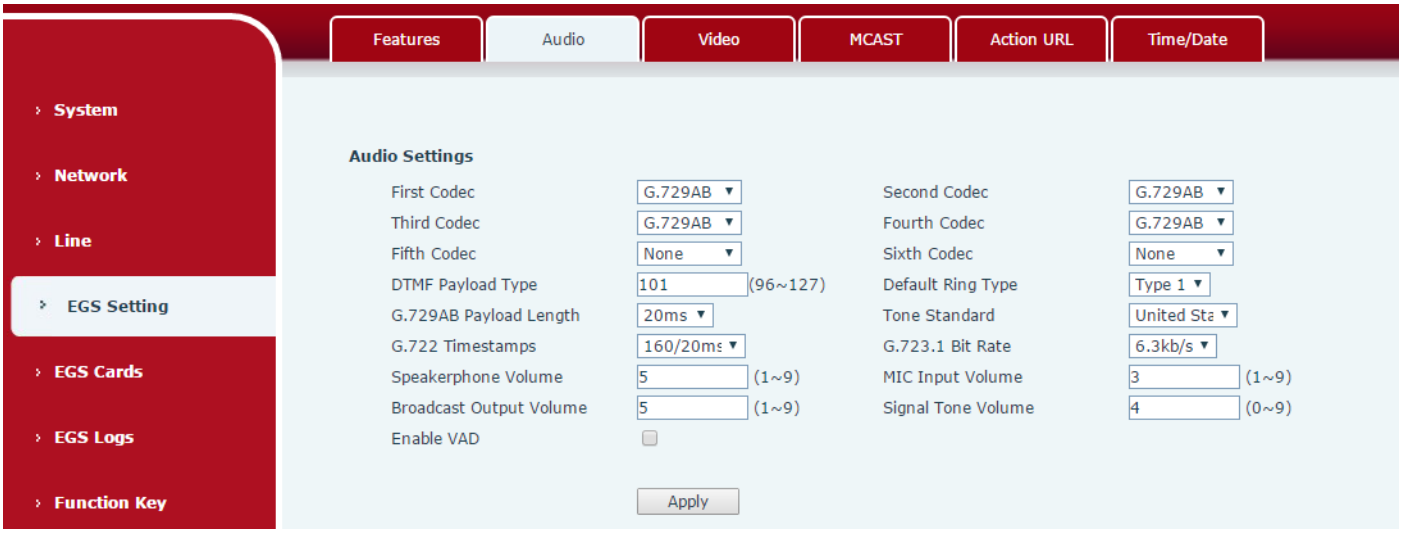
Features	
Field Name	**Explanation**
Common Settings	
Enable DND	DND feature can refuse all incoming calls for all SIP lines, or for individual SIP line. But the outgoing calls would not be affected
Ban Outgoing	If it is enabled, no outgoing calls can be made.
Enable Intercom Mute	If it is enabled, device would mute incoming calls during an intercom call.
Enable Intercom Ringing	If it is enabled, device would play intercom ring tone to alert that there is a new incoming call during 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 feature添加 when there is no answer
Auto Hangup Timeout	Configuration in a set time, the device would automatically hang up when there is no answer
Dial Fixed Length to Send	Enable or disable dial fixed length.
Send length	The number would be sent to the server after the specified digits are dialed.
Enable Speed Dial Hangup	Enable Speed Dial Hand Up function
Use Function Key to Answer	Configure whether to enable the function keys, the feature is disabled by default.
Dial Number Voice Play	Configuration Open / Close Dial Number Voice Play
Voice Play Language	Set language of the voice prompt
Card Reader Working Mode	Set ID card status: Normal: This is the work mode; swiping card can open the door. Card Issuing: This is the issuing mode; swiping card can add ID cards. Card Revoking: This is the revoking mode; swiping card can delete ID cards.

Field Name	Explanation
Advanced 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 mode is Monostable
Keypad Mode	Password+dialing: password inputting mode is default. Dialing mode is as below if you want. Only password: password input only, dialing would be forbidden. Only dialing: dial input only, you can press * key to enter the dial, the # key for hanging up. Initial mode is password and dialing.
Switch-On Duration	Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial time is 5 seconds.
Talk Duration	The call would be ended automatically when time up. Initial time is 120 seconds
Remote Password	Remote unlocking door password. Initial password is “*”.
Local password	Local unlocking door password via keypad, the default password length is 4. Initial password is “6789”.
Description	Device description displayed on IP scanning tool software. Initial description is “I30 IP Door Phone”.
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. The device enables the feature by default.
Hot Key Dial Mode Select	<Primary /Secondary>mode allow system to call primary extension first, if there is no answer, system would cancel the call and then call secondary extension automatically. <Day/Night>mode allow system to check the calling time is belong to day time or night time, and then system decides to call the number 1 or number 2 automatically. Users just press speed dial key once.
Call Switched Time	The period between hot key dialing to the first and second number. Initial time is 16 seconds.
Day Start Time	The start time of the day when you select<Day/Night>mode.
Day End Time	The end time of the day when you select <Day/Night>mode.
Address of Open Log Server	Log server address(IP or domain name)

Port of Open Log Server	Log server port (0-65535), Initial port is 514.
Enable Open Log Server	Enable or disable connecting with log server
Enable Indoor Open	Enable or disable using indoor switch to unlock the door.
Enable Card Reader	Enable or disable card reader for RFID cards.
Limit Talk Duration	If enabled, calls would be forced to end after talking time is up.
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 length is 4.
Block Out Settings	
Add or delete blocked numbers – enter the prefix of numbers which should not be dialed by the phone. For example, if 001 is entered, the phone 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.

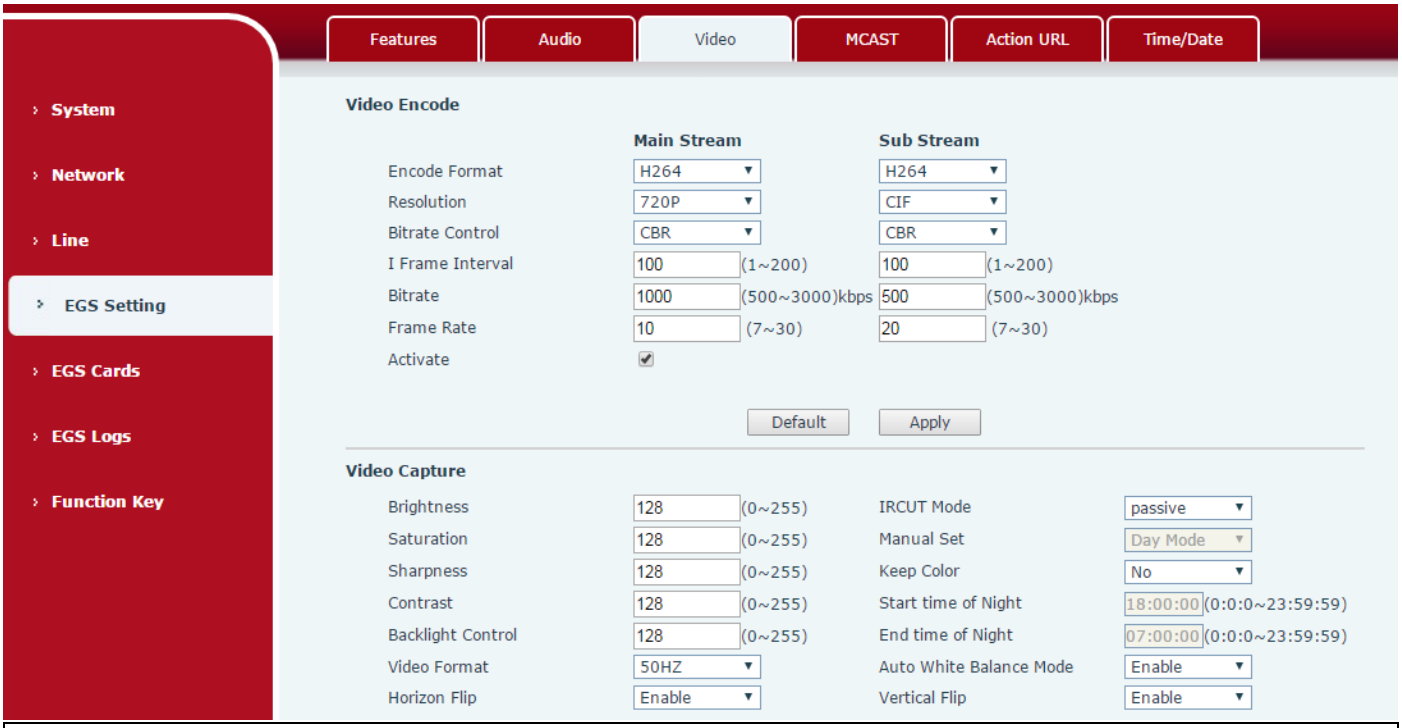


Audio Setting	
Field Name	**Explanation**
First Codec	The first codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB

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.

c) Video

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

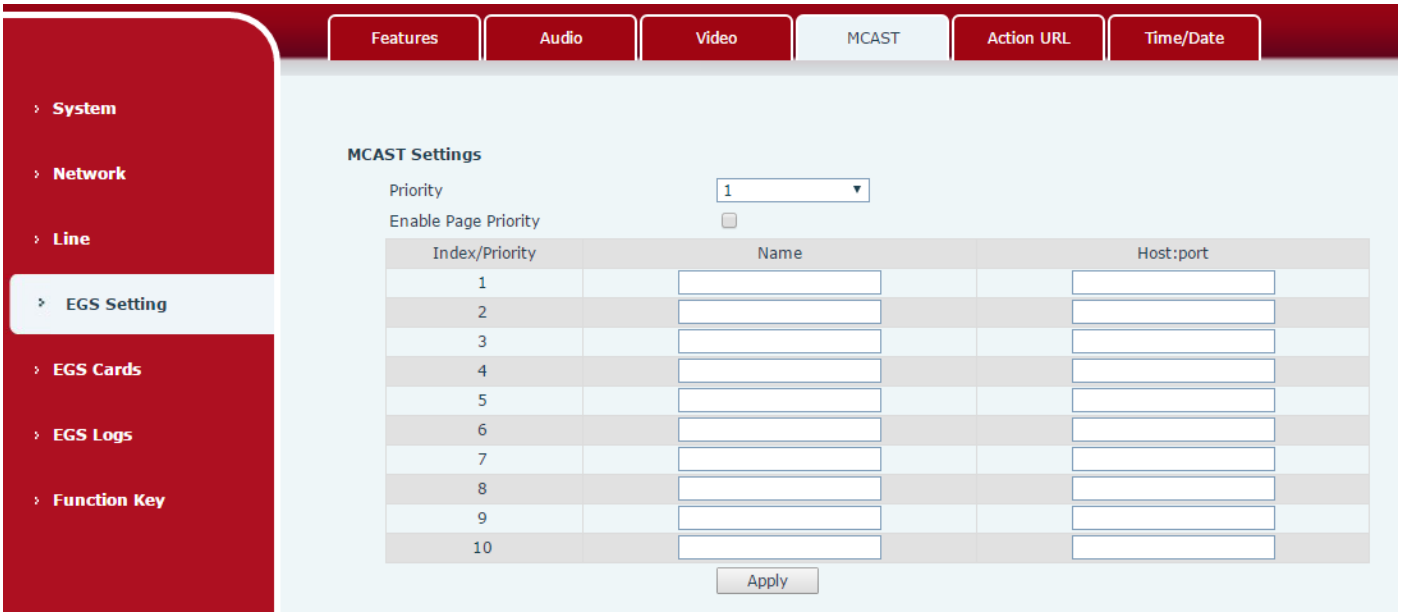


Video Encode

Field Name	Explanation
Encode	Only H.264 encoding format is supported
Resolution	Main stream: support 720P Sub-stream: you can select 360P, CIF (352 * 288), QVGA (240 * 320)
Bitrate Control	CBR: If the code rate (bandwidth) is insufficient, it is preferred. VBR: Image quality is preferred, not recommended. CVBR: greater than the minimum bit rate (bandwidth), smaller than the maximum bit rate (bandwidth), the setting is complex; the type is not recommended.
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.
Bitrate	It is proportional to video file size, not recommend adjusted.
Frame Rate	The larger the value is, the more coherent the video would be got; not recommend adjusted.
Activate	When you selected it, the main stream is enabled, otherwise disabled
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
IRCUT Mode	IR-Cut operating mode selection: **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) **Manual mode:** the user need to manually select the camera day / night mode, night mode is black and white
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	IR-Cut day and night mode, the camera switches to black and white end time

Night	
Auto White Balance Mode	The camera automatically adjusts the video image based on ambient light
Vertical Flip	The video is flipped horizontally

d) MCAST



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

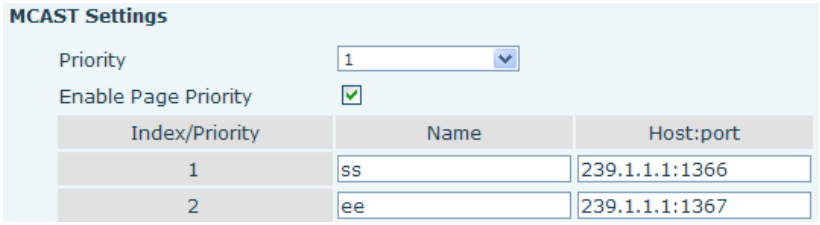
- Priority:

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.

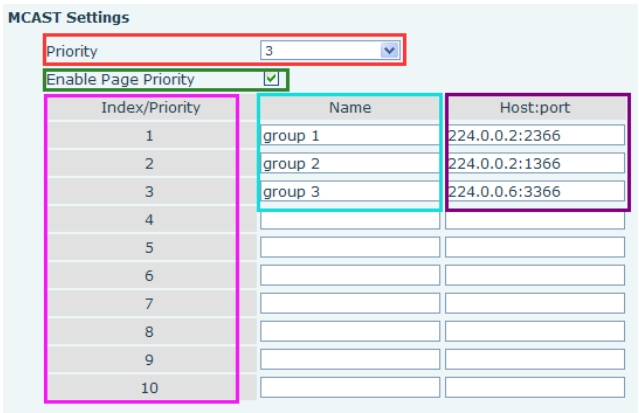
- Web Settings:



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



- **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".

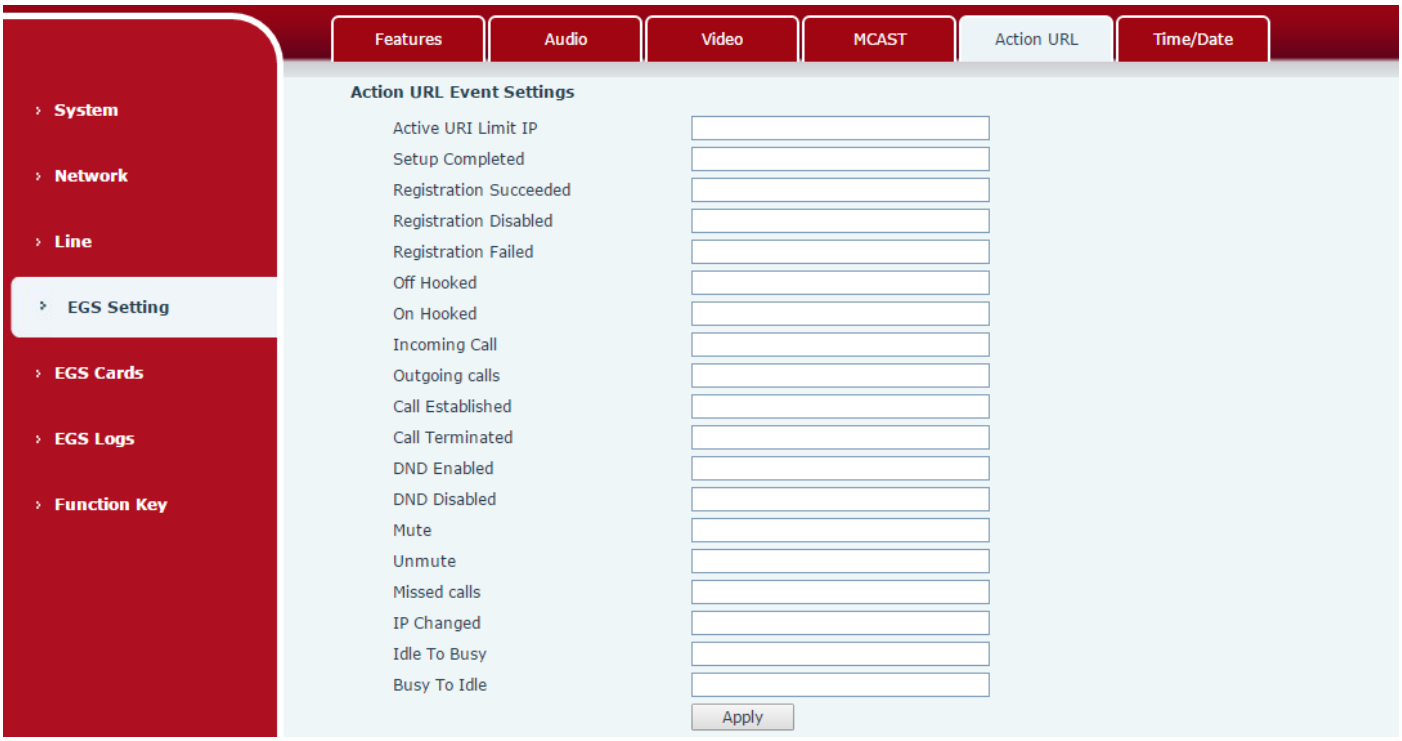
✧ If multicast is a new "group 1", and because the priority of group 1" is 2, higher than the current call priority 3 of “group 2”, so multicast call would come in.

✧ 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

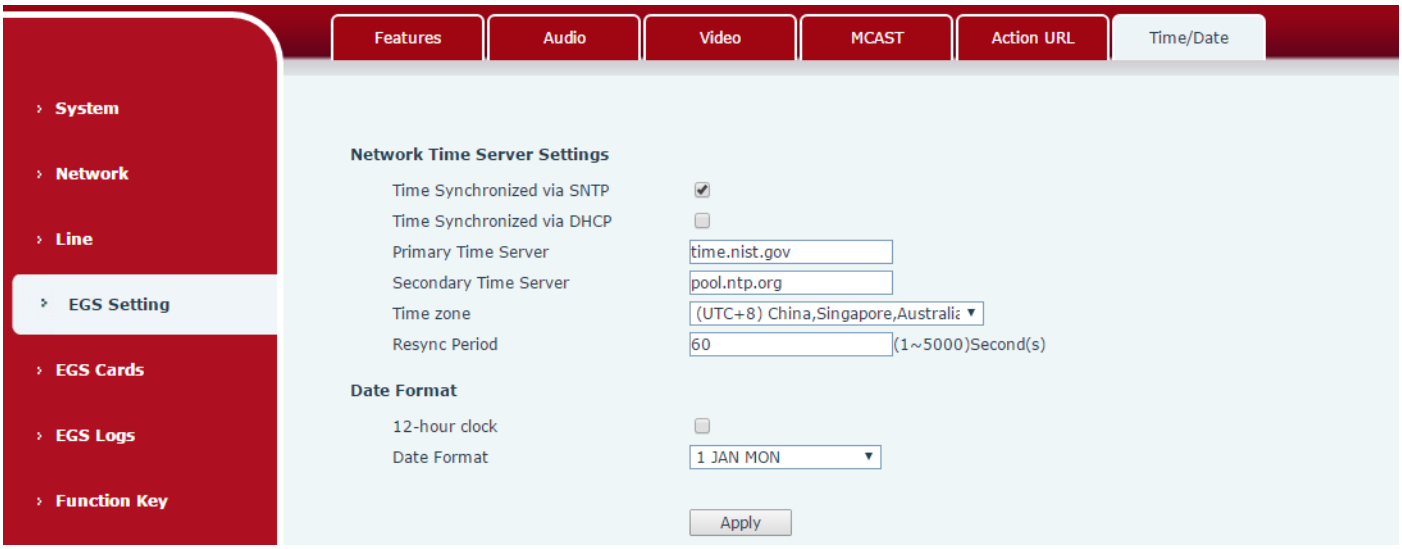
- **Send:** when you configure the item, pressing the corresponding key on the equipment shell, equipment would directly enter the Talking interface; the premise is to ensure no current multicast call and three-way conference, so the multicast can be established.
- **Monitor:** IP port and priority are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

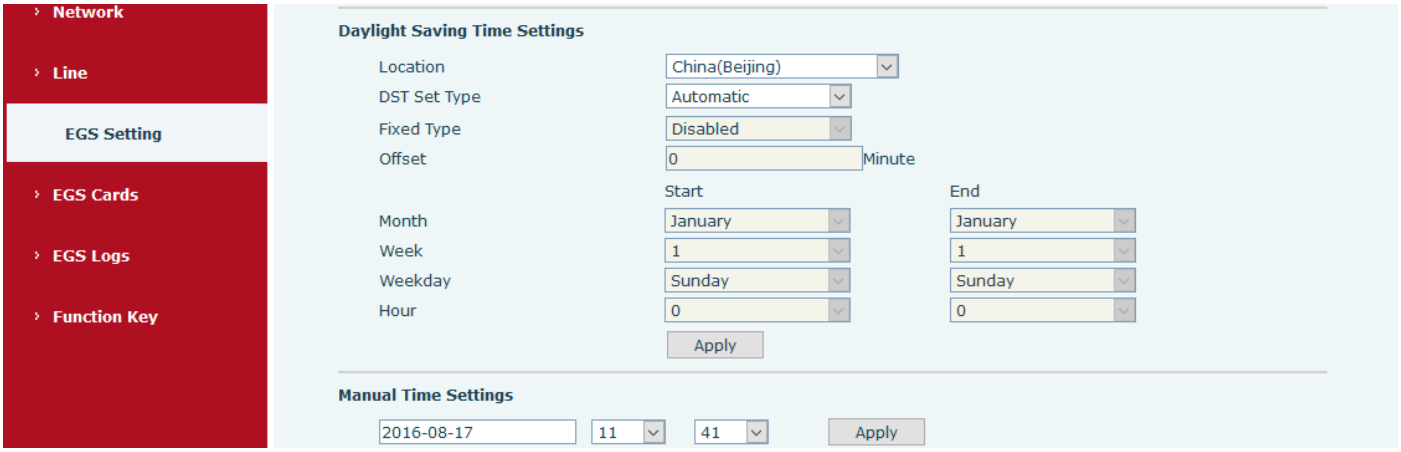
e) Action URL



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



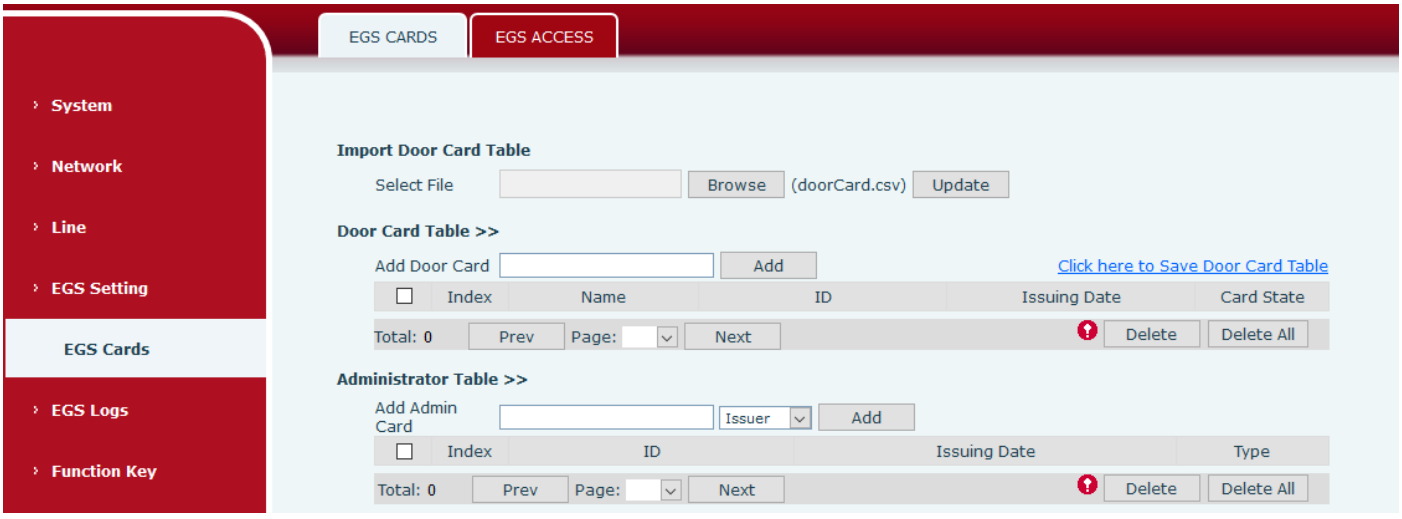


Time/Date	
Field Name	**Explanation**
Network Time Server Settings	
Time Synchronized via SNTP	Enable time-sync through SNTP protocol
Time Synchronized via DHCP	Enable time-sync through DHCP protocol
Primary Time Server	Set primary time server address
Secondary Time Server	Set secondary time server address, 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	

12-hour clock	Set the time display in 12-hour mode
Date Format	Select the time/date display format
Daylight Saving Time Settings	
Location	Select the user's time zone 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 Cards

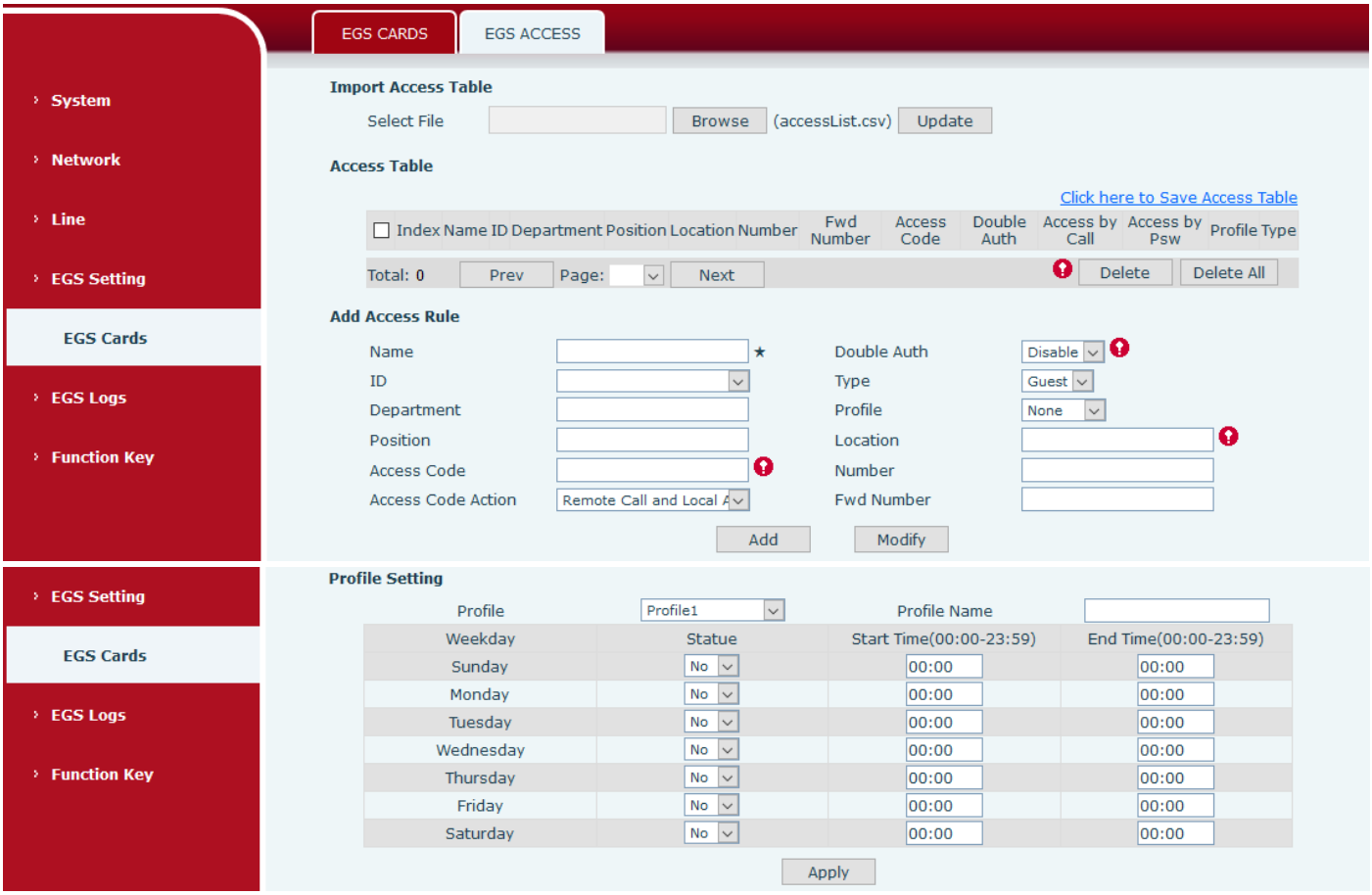
a) EGS Cards



EGS Cards	
Field Name	**Explanation**
Import Door Card Table	
Click <Browse> to choose importing door card list file (doorCard.csv); click <Update> can batch import.	

Door Card Table	
Add Door Card	You should input the top 10 digits of RFID card numbers, for example, 0004111806, click <add>.
Click here to Save Door Card Table	Click here to Save Door Card Table Right-click it and select saving target to your computer.
Name	The name of users who own issued cards.
ID	The card number of issued cards. (Note: The card not registered to the remote access list is unable to open the door.)
Issuing Date	The issuing date of issued cards.
Card State	The state of issued cards.
Delete	Click <Delete>, you would delete the door card list of the selected ID cards.
Delete All	Click <Delete All>, to delete all door card lists.
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: issuing and revoking 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, 500 copies of ordinary cards. Note: in the issuing state, swiping deleted card is invalid.	
Shows the ID, Date and Type of admin card	
Delete	Clicking <Delete> would delete the admin card list of the selected ID cards.
All Delete	Click <Delete All>, to delete all admin card lists.

b) EGS ACCESS

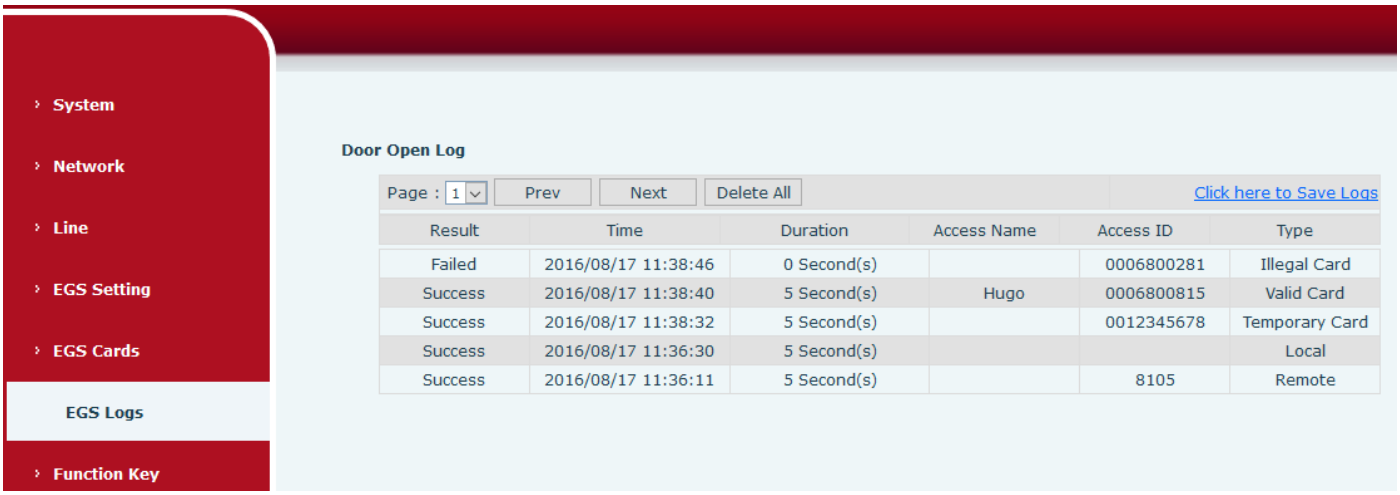


Field Name	Explanation
Import Access Table	
Click the <Browse> to choose to import remote access list file (access List.csv) and then clicking <Update> can batch import remote access rule.	
Access Table	
According to entrance guard access rules have been added, you can choose single or multiple rules on this list to delete operation.	
Add Access Rule	
Name	User name
ID	RFID card number
Department	Card holder's department
Position	Card holder's position
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.

Access Code Action	Select Access Code Action mode
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.
Location	Virtual extension number, used to make position call instead of real number. It might be taken with unit number, or room number.
Number	User phone number
Fwd Number	Call forwarding number when above phone number is unavailable.
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

(6) EGS Logs

According to open event log, the device can record up to 150 thousands open event; it would cover the old records after the records exceed 150 thousands. Click here to Save Logs Right click on the links to select saving target as the door log can export CSV format.

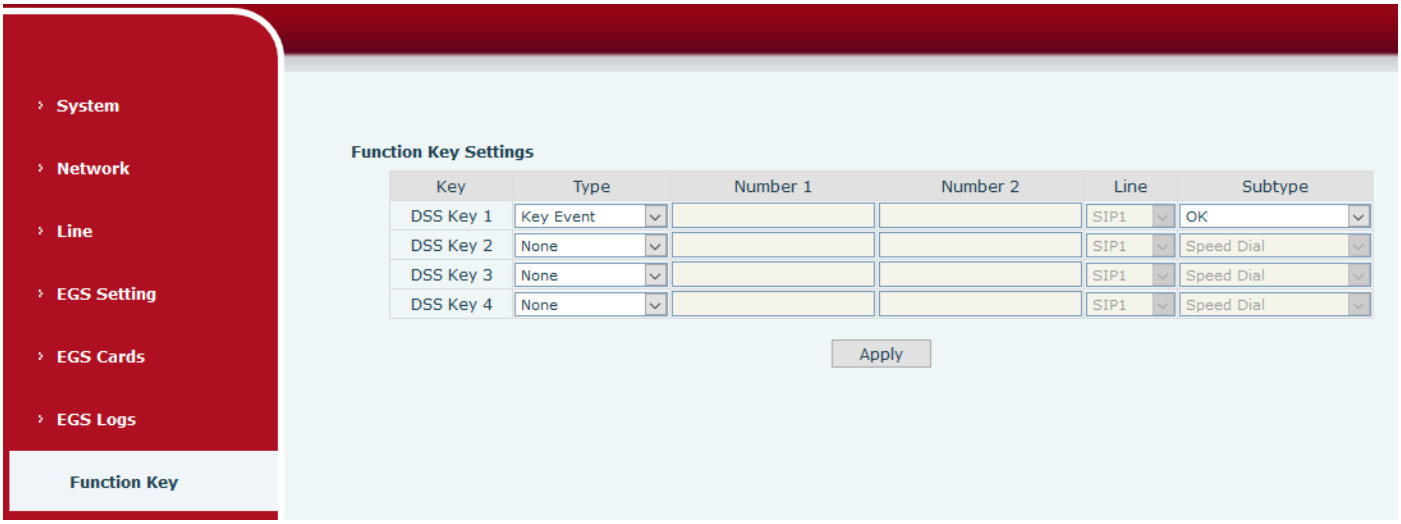


Field Name	Explanation

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)

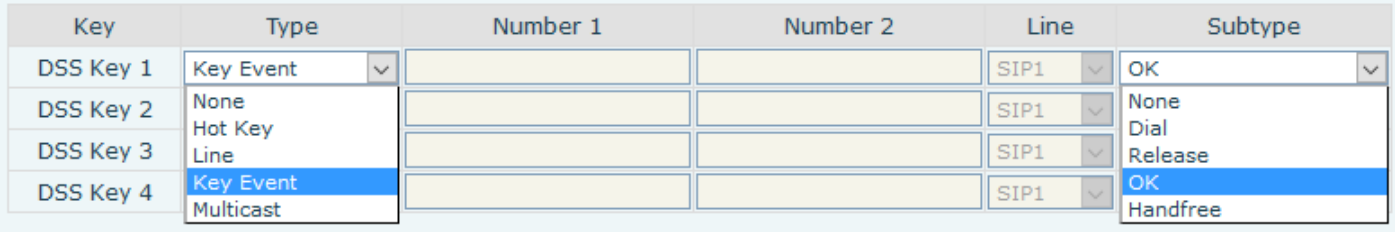
(7) Function Key

a) Function Key Settings



➢ Key Event

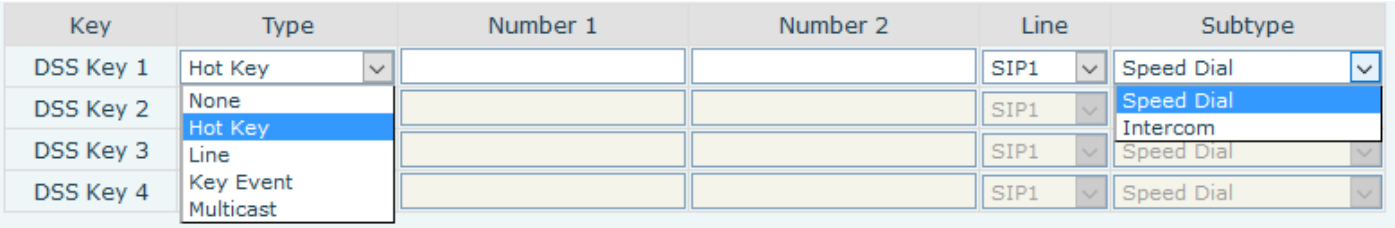
You might set up the key type with the Key Event.



Type	Subtype	Usage
Key Event	None	No responding
	Dial	Dialing function
	Release	Delete password input, cancel dialing input and end call
	OK	identification key
	Handfree	The hand-free key(with hooking dial, hanging up functions)

➢ 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.

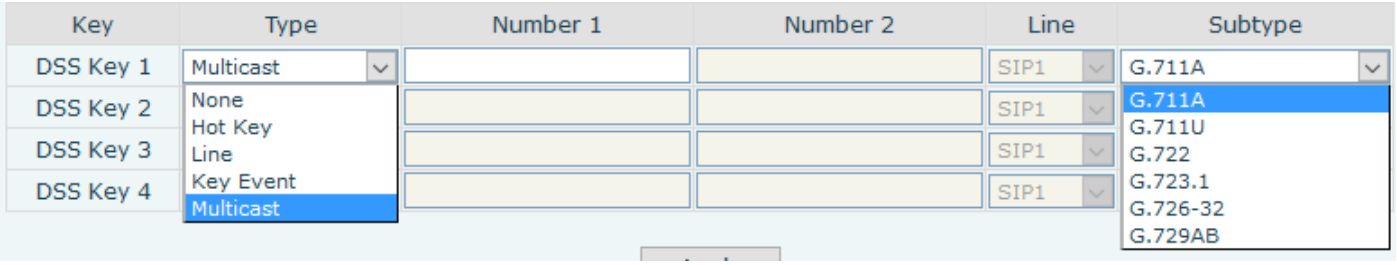


Type	Number	Line	Subtype	Usage
Hot Key	Fill the called party's SIP account or IP address	The SIP account corresponding lines	Speed Dial	Using Speed Dial mode together with Enable Speed Dial Hangup Enable, can define whether this call is allowed to be hung up by re-pressing the speed dial key.
			Intercom	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:



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

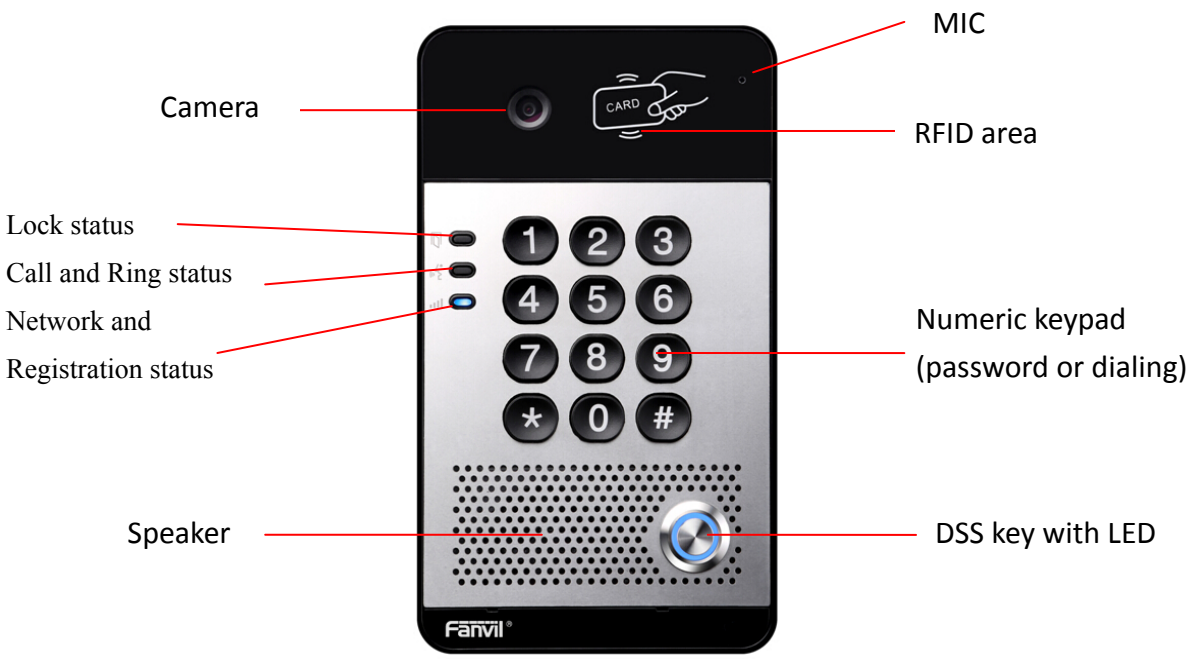
1. Technical parameters

Communication protocol		SIP 2.0(RFC-3261)
Main chipset		Broadcom
Keys	**DSS Key**	1(stainless steel)
	Numeric keyboard	Support
Audio	**MIC**	1 个
	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/700mA DC
	WAN	10/100BASE-TX s Auto-MDIX, RJ-45
Camera		1/4 "color CMOS, 1 megapixel, wide angle
RFID/IC card reader(optional)		EM4100 (125Khz) ---Standard configuration MIFARE One(13.56Mhz) ---Custom-made
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 mounted
External size		160 x 93 x 35mm
Package size		178 x 104 x 55mm
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 mounted
- 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.

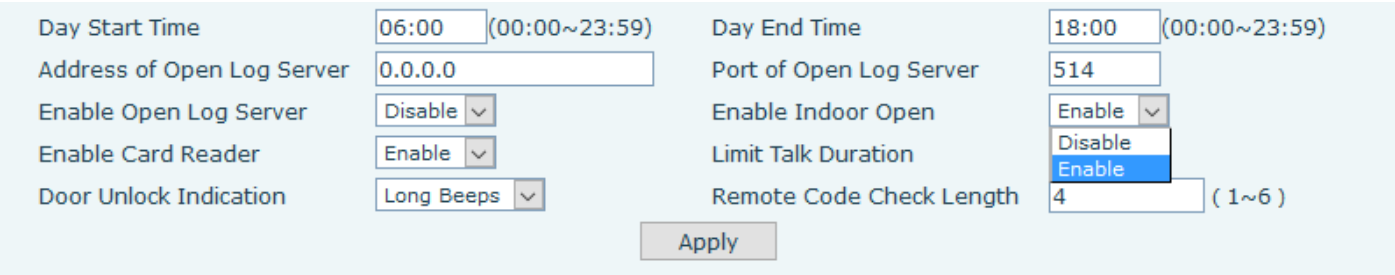
✧ Owner inputs corresponding access codes via SIP phone keypad to unlock the door.

- **Swiping cards**

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

- **Indoor switch**

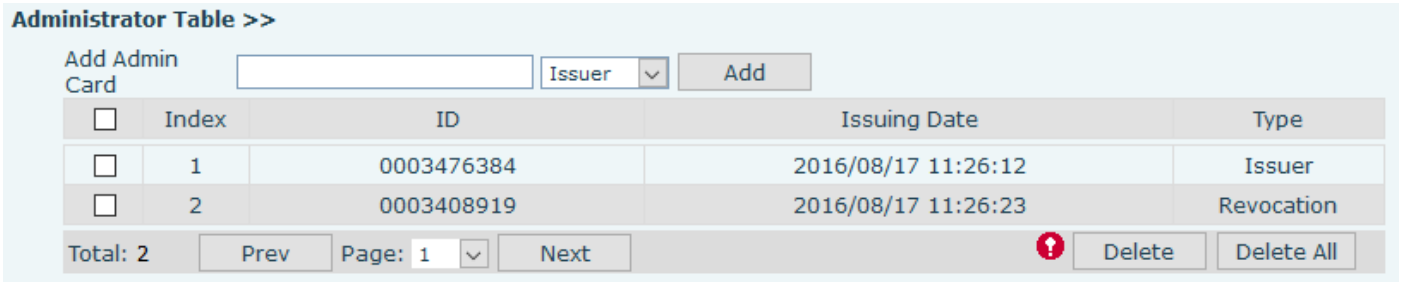
✧ Press indoor switch, which is installed and connected with the device, to unlock the door.



2. Management of card

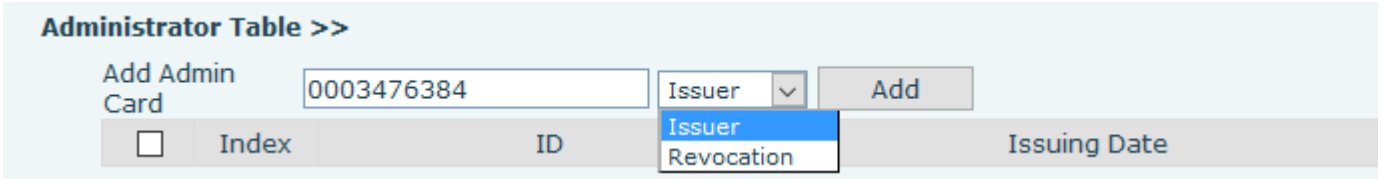
1) Administrator Table

<Issuer> and <Revocation>



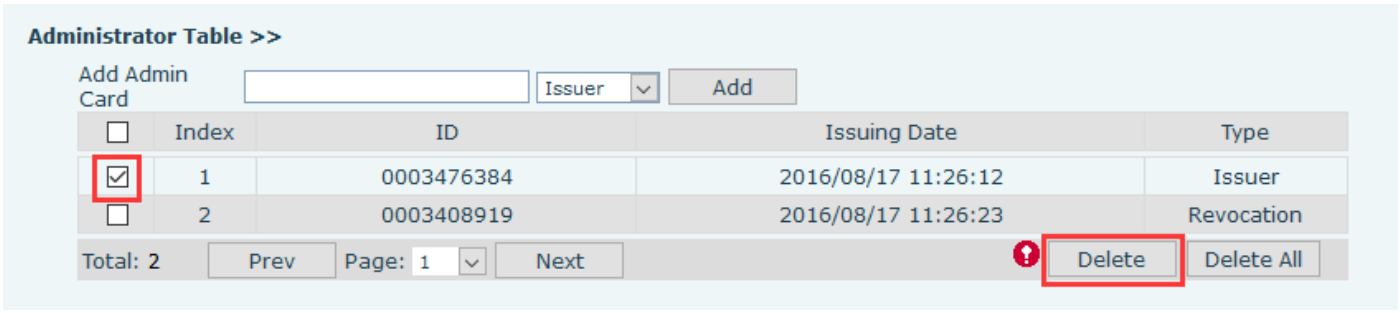
- **Add Administrator cards**

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



- **Delete Administrator cards**

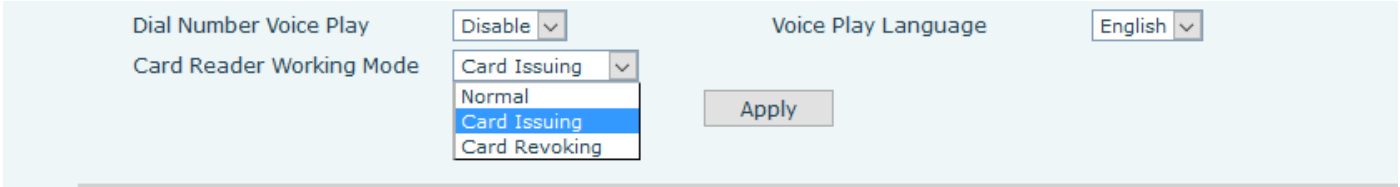
Select the admin card need to be deleted, click <Delete>.



2) Add user cards

- **Method 1**: used to add cards for starters typically

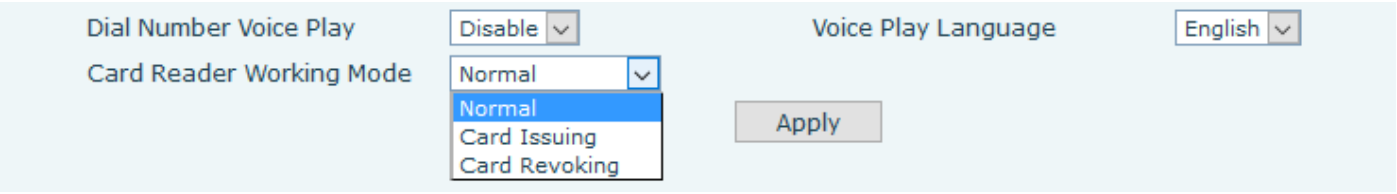
✧ In web page < EGS Setting →Features →Card Reader Working Mode > option, select <Card Issuing>.



✧ Click <Apply>, Card Reader would enter the issuing status.

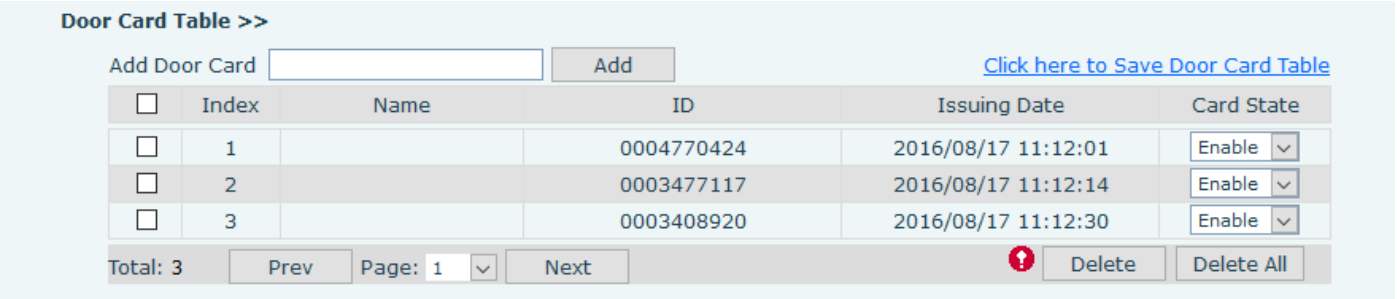
✧ Use new card to touch card reader induction area, and then you might hear the confirmed indication tone from the device. Repeat step can to add more cards.

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



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

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



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

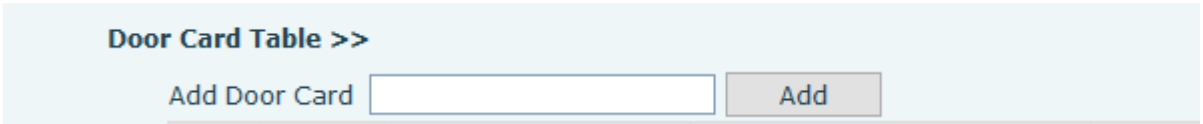
✧ Use issuer admin card to touch card reader induction area, and it would enter issuing card status.

✧ 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.

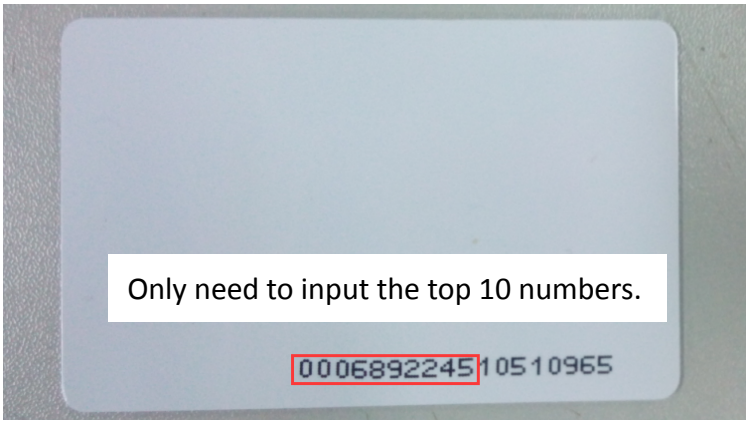
✧ Use issuer admin card to touch card reader induction area again, it would go back to normal working status.

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

✧ Input cards number in door card settings page, and then click <Add>.



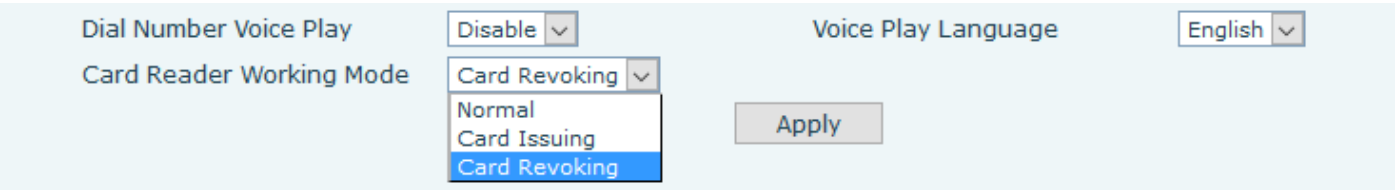
Note: you can also use the USB card reader connected with PC to get cards ID automatically.



3) Delete user cards

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

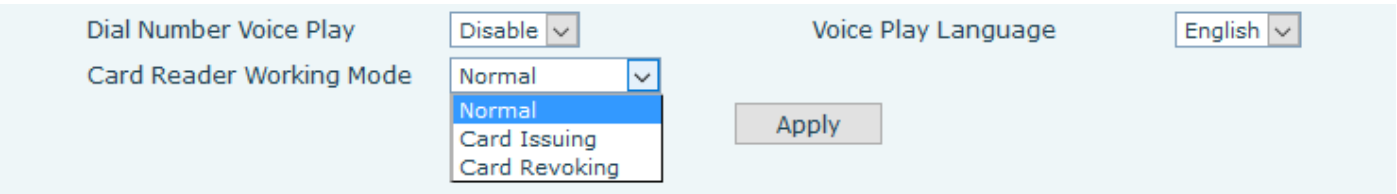
✧ In web page < EGS Setting →Features →Card Reader Working Mode > option, select <Card Revoking>.



✧ 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>.



✧ 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.