We make everyday life safer

SIP Intercom Station

ABT-IC-1 / ABT-IC-K1

EN **User Manual**

ver. 08.2020

www.ambientsystem.eu

Ambient System Sp. z o.o.
ul. Bysewska 27 | 80-298 Gdańsk | Poland

Table of Contents

1. Safety 4

2. Product introduction 7
2.1 Appearance of the product 7
2.2 Description 8

3. Start Using 9
3.1 Confirm the connection 9
3.1.1 Power, Electric Lock, Indoor switch port 9
3.1.2 Driving mode of electric-lock (Default in Passive mode) 9
3.1.3 Wiring instructions 10
3.2 Quick Setting 11

4. Basic operation 12
4.1 Answer a call 12
4.2 Call 12
4.3 End call 12

5. Page settings 13
5.1 Browser configuration 13
5.2 Password Configuration 13
5.3 Configuration via WEB 14
5.3.1 System 14
5.3.1.1 Information 14
5.3.1.2 Account 15
5.3.1.3 Configurations 16
5.3.1.4 Upgrade 17
5.3.1.5 Auto Provision 18
5.3.1.6 FDMS 21
5.3.1.7 Tools 22
5.3.2 Network 24
5.3.2.1 Basic 24
5.3.2.2 Advanced 25
5.3.2.3 VPN 27
5.3.3 Line 29
5.3.3.1 SIP 29
5.3.3.2 Basic Settings 33
5.3.3.3 Dial Peer 35
5.3.4 EGS Setting 37
5.3.4.1 Features 37
5.3.4.2 Audio 40

5.3.4.3 Video 41
5.3.4.4 MCAST 42
5.3.4.5 Action URL 45
5.3.4.6 Time/Date 46
5.3.5 EGS Access 47
5.3.6 EGS Logs 49
5.3.7 Door Lock 50
5.3.8 Function Key 51
5.3.9 Alert 53

6. Appendix 54
6.1 Technical parameters 54
6.2 Basic functions 55
6.3 Schematic diagram 56

7. Other instructions 57
7.1 Open door modes 57
7.2 Management of card 57

1. Safety

Danger!
High risk: This symbol indicates an imminently hazardous situation such as "Dangerous Voltage" inside the product. If not avoided, this will result in an electrical shock, serious bodily injury, or death.

Warning!
Medium risk: Indicates a potentially hazardous situation.
If not avoided, this could result in minor or moderate bodily injury.

Caution!
Low risk: Indicates a potentially hazardous situation.
If not avoided, this could result in property damage or risk of damage to the unit.

1. **Read these instructions.** All the safety and operating instructions should be read before the apparatus or system is operated.
2. **Keep these instructions.** The important safety instructions and operating instructions should be retained for future reference.
3. **Heed all warnings.** All warnings on the apparatus and in the operating instructions should be adhered to.
4. **Follow all instructions.** All instructions for installation or use/operating should be followed.
5. **Do no use this apparatus near water.** Do not use this apparatus near water or a moist environment – for example, near a bath tub, wash bowl, kitchen sink, or laundry tub, in a wet basement, near a swimming pool, in an unprotected outdoor installation, or any area which is classified as a wet location.
6. **Clean only with dry cloth.** Unplug the apparatus from the outlet before cleaning. Do not use liquid cleaners or aerosol cleaners.
7. **Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.** Openings in the enclosure, if any, are provided for ventilation and to ensure reliable operation of the apparatus and to protect it from overheating. These openings must not be blocked or covered. This apparatus should not be placed in a built-in installation unless proper ventilation is provided or the manufacturer's instructions have been adhered to.
8. **Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat or in direct sunlight.**
9. **No naked flame sources, such as lighted candles, should be placed on the apparatus.**
10. **Do not defeat the safety purpose of the polarized or ground-type plug.** A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wider blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
11. **Protect the power cord from being walked on or pinched particularly at plug, convenience receptacles, and the point where they exit from the apparatus.**
12. **Only use attachments/accessories specified by the manufacturer.** Any mounting of the apparatus should follow the manufacturer's instructions, and should use a mounting accessory recommended by the manufacturer.
13. **Use only with the cart, stand, tripod, bracket or table specified by the manufacturer, or sold with the apparatus.** When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over. Quick stops, excessive force, and uneven surfaces may cause the appliance and cart combination to overturn.
14. **Unplug this apparatus during lighting storms or when unused for long periods of time.** Not applicable when special functions are to be maintained, such as evacuation systems.

15. **Refer all servicing to qualified service personnel.** Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
16. **Avoid mechanical shocks.** Strong impacts and shocks may damage the device. Transport the device carefully and avoid dropping it.
17. **The apparatus shall not be exposed to dripping or splashing and that no objects filled with liquid, such as vases, shall be placed on the apparatus.**
18. **Batteries (battery pack or batteries installed) shall not be exposed to excessive heat such as sunshine, fire or the like.**

Caution!
Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type. Dispose of used batteries according to the environmental law and procedures.

19. **Professional installation only.** Do not use this equipment in residential applications.
20. **Condensation.** In order to avoid condensation; wait a few hours before turning on the equipment when it is transported from a cold to a warm space.
21. **Hearing damage.** For apparatus with audio output, to prevent possible hearing damage, do not listen at high volume levels for long periods.
22. **Do not disassemble the device or attempt to repair or modify it.** The device does not include user replaceable components inside the chassis. Opening the chassis and unauthorized repairs will void the warranty. Unauthorized substitutions may result in fire, electric shock or other hazards.
23. **Safety check.** Upon completion of any service or repairs to this apparatus, ask the service technician to perform safety checks to determine that the apparatus is in proper operating condition.

Danger!
Overloading – do not overload outlets and extension cords as this can result in a risk of fire or electric shock.

24. **Power sources.** This apparatus should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power supply you plan to use, consult your appliance dealer or local power company. For apparatuses intended to operate from battery power, or other sources, refer to the operating instructions.
25. **Power lines.** An outdoor system should not be located in the vicinity of overhead power lines or other electric light or power circuits, or where it can fall into such power lines or circuits. When installing an outdoor system, extreme care should be taken to keep from touching such power lines or circuits, as contact with them might be fatal.

Danger!
Object and Liquid entry – never push objects of any kind into this apparatus through openings as they may touch dangerous voltage points or short-out parts that could result in a fire or electric shock. Never spill liquid of any kind on the apparatus.

26. **Protective grounding.** An apparatus with class I construction shall be connected to a power outlet socket with a protective grounding connection.

    Protective earthing. An apparatus with class I construction shall be connected to a mains socket outlet with a protective earthing connection.

Note for power connections

» For permanently connected equipment, a readily operable mains plug or all-pole mains switch shall be external to the equipment and in accordance with all applicable installation rules.

» For pluggable equipment, the socket-outlet shall be installed near the equipment and shall be easily accessible.

This label may appear on the bottom of the apparatus due to space limitations.

Caution!
To reduce the risk of electrical shock, DO NOT open covers. Refer servicing to qualified service personnel only.

Warning!
To prevent fire or shock hazard, do not expose units to rain or moisture.

Warning!
Installation should be performed by qualified service personnel only in accordance with the National Electrical Code or applicable local codes.

Warning!
Power disconnect: If the apparatus is mains powered and a power supply cord set is provided, the disconnect device is the mains plug of the power cord set.
If an AC DC adapter is provided and the mains plug that is part of the direct plug in device, the AC DC adapter is the disconnect device. The socket outlet shall be near the apparatus and shall be easily accessible.

Old electrical and electronic appliances
Electrical or electronic devices that are no longer serviceable must be collected separately and sent for environmentally compatible recycling (in accordance with the European Waste Electrical and Electronic Equipment Directive).
To dispose of old electrical or electronic devices, you should use the return and collection systems put in place in the country concerned.

Only used at altitude not exceeding 2000 m.

Only used in non-tropical climate regions.

2. Product introduction

ABT-IC-1 and ABT-IC-K1 SIP intercom stations are a full digital network door phones, with its core part adopts mature VoIP solution (Broadcom chip), stable and reliable performance, hands-free adopting digital full-duplex mode, voice loud and clear, generous appearance, solid durable, easy for installation, comfortable keypad and low power consumption.

ABT-IC-1 and ABT-IC-K1 SIP intercom stations supports entrance guard control, voice intercom, RFID/IC card and keypad remote to open the door.

2.1 Appearance of the product

SIP Intercom Stations: ABT-IC-1 and ABT-IC-K1

2.2 Description

Buttons and icons	Description	Function
	Numeric keyboard	Input password to open the door or to call.
	Programmable key	Can be set to a variety of functions, in order to meet the needs of different occasions
	Lock Status	Door unlocking: On Door locking: Off
	Call status	Standby: Off Call Holding: Blink with 1s Calls: On
	Ring status	Standby: Off Ringing: On
	Network/SIP Registration	Network error: Blink with 1s Network running: Off Registration failed: Blink with 3s Registration succeeded: On

3. Start Using

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

3.1 Confirm the connection

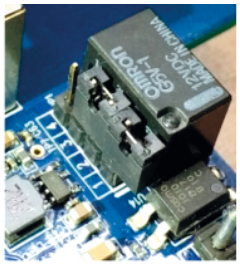
Confirm whether the equipment of the power cord, network cable, electric lock control line connection and the boot-up is normal. (Check the network state of light)

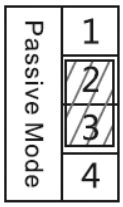
3.1.1 Power, Electric Lock, Indoor switch port

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

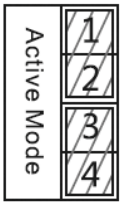
CN7						
1	**2**	**3**	**4**	**5**	**6**	**7**
+12V	VSS	NC	COM	NO	S_IN	S_OUT
12V 1A/DC		Electric-lock switch			Indoor switch	

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





Jumper in passive mode



Jumper in active mode

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

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

» When using the active mode, it is 12V DC in output.

» When using the passive mode, output is short control (normally open mode or normally close mode).

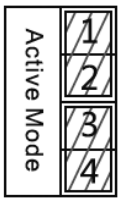
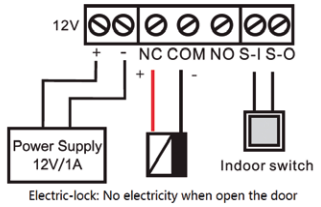
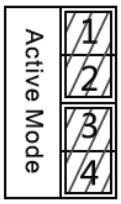
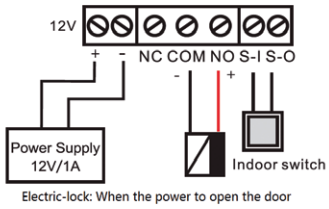
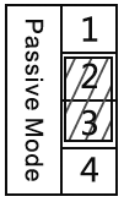
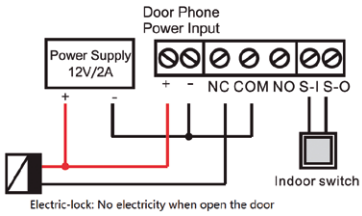
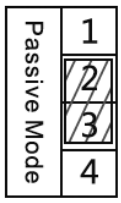
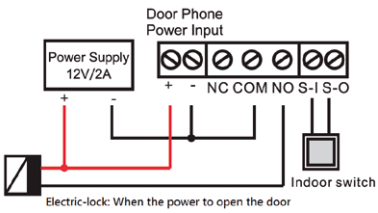
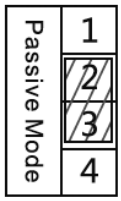
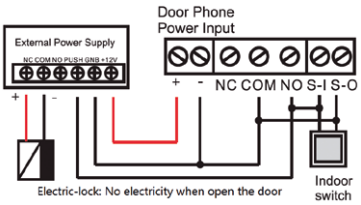
3.1.3 Wiring instructions

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

» NO: Normally Open Contact.

» COM: Common Contact.

» NC: Normally Close Contact.

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

3.2 Quick Setting

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

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

» Press and hold "#" key for 3 seconds and the door phone will report the IP address by voice.

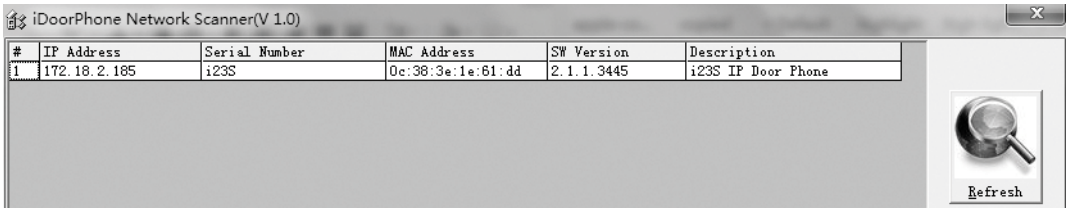
» **NOTE:** Waiting for 30s to run the device when it is power on.

» Log in to the WEB device configuration.

» In a Line page configuration service account, user name, parameters that are required for server address register.

» You can set DSS key in the Function key page.

» You can set Door Phone parameters in the Webpage (EGS Setting-> Features).



4. Basic operation

4.1 Answer a call

By default, the incoming call will be answered automatically without any ringing.

User MAY want to hear ring before answer the incoming call. This could be configured under: EGS setting -> Features -> Basic Settings -> Auto Answer timeout. This parameter is the ringing time.

Auto answered could be disabled under: EGS setting -> Features -> Basic settings -> Enable auto Answer.

4.2 Call

There are 2 options to place a call:

1. Press * to enter dialing mode, then type in the number and press * to send the call immediately.
   Here the feature of "pressing * to send the call" could be disabled by the option press * to send under EGS setting -> Features -> Basic Settings
   Another 2 important options are dial Fixed Length to Send and send Length. When user is typing in the number under dialing mode on keypad, device will check the length of number after every new digit was typed. Once the length matches the parameter send Length, the number will be called immediately. If this feature is disabled, user will need to wait auto dial out time seconds before the call is sending out.
2. By pressing the DSS key, the preconfigured number will be called. The option is under Function Key -> Function Key settings. The type is hot key, subtype is Speed dial. There are 2 numbers available here, the number 1 will be called first, if number 1 is not answered, the call will be transferred to number2.

4.3 End call

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

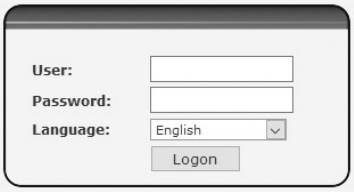
1. Release the processing call
2. Reject the incoming call when it's ringing

5. Page settings

5.1 Browser configuration

When the device and your computer are successfully connected to the network, enter the IP address of the device on the browser as http://xxx.xxx.xxx.xxx/ and you can see the login interface of the web page management.

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



5.2 Password Configuration

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

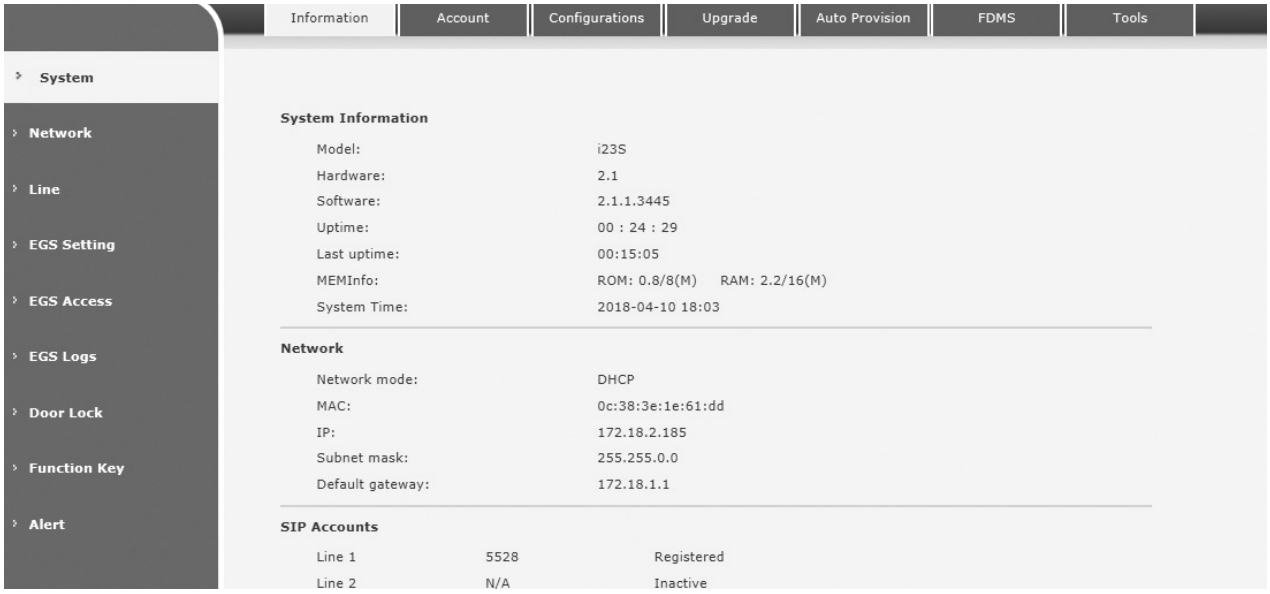
» Default user with general level: The default is not set, are free to add.

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

5.3 Configuration via WEB

5.3.1 System

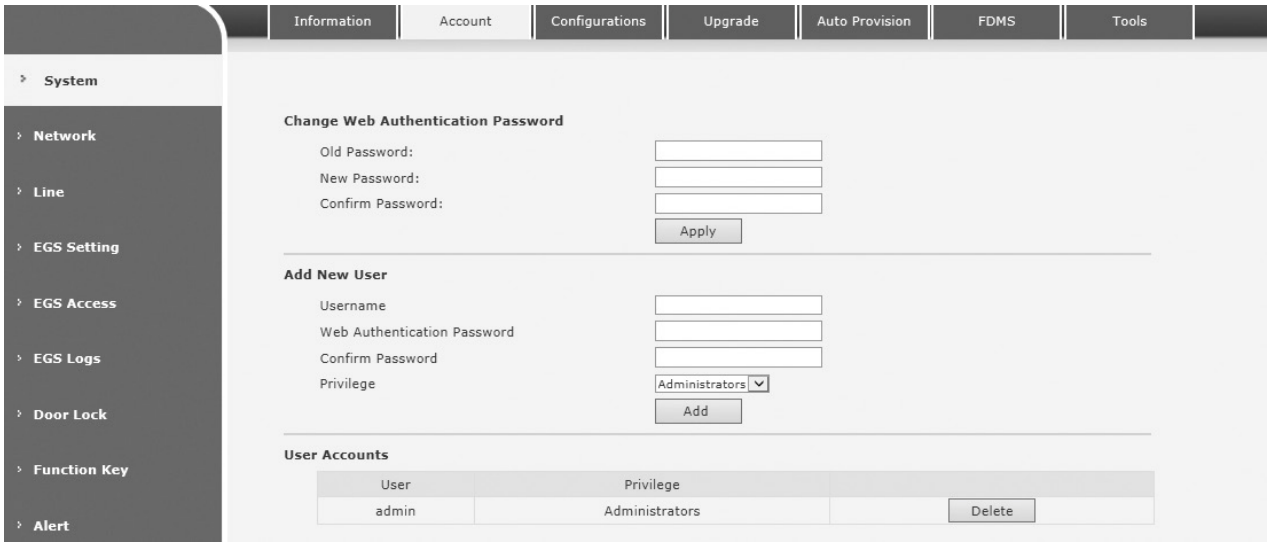
5.3.1.1 Information



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

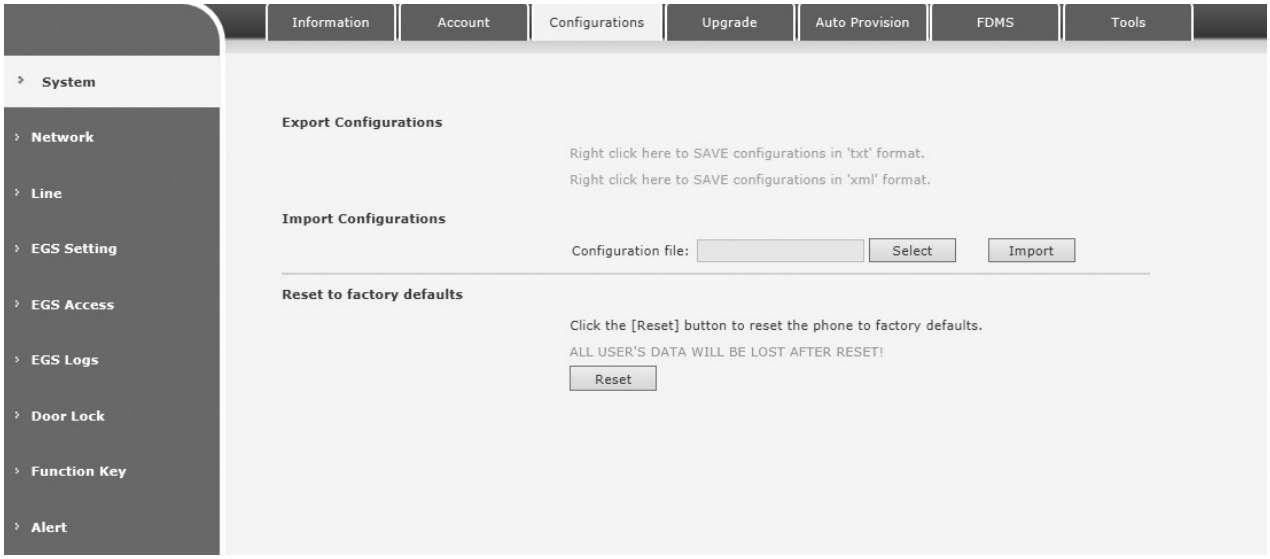
5.3.1.2 *Account*

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



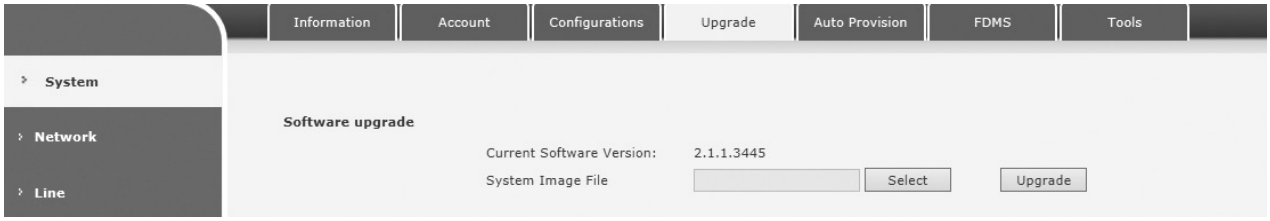
Account	
Field Name	**Explanation**
Change Web Authentication Password	You Can modify the login password to the account
Add New User	You can add new user
User Accounts	Show the existing user information

5.3.1.3 Configurations



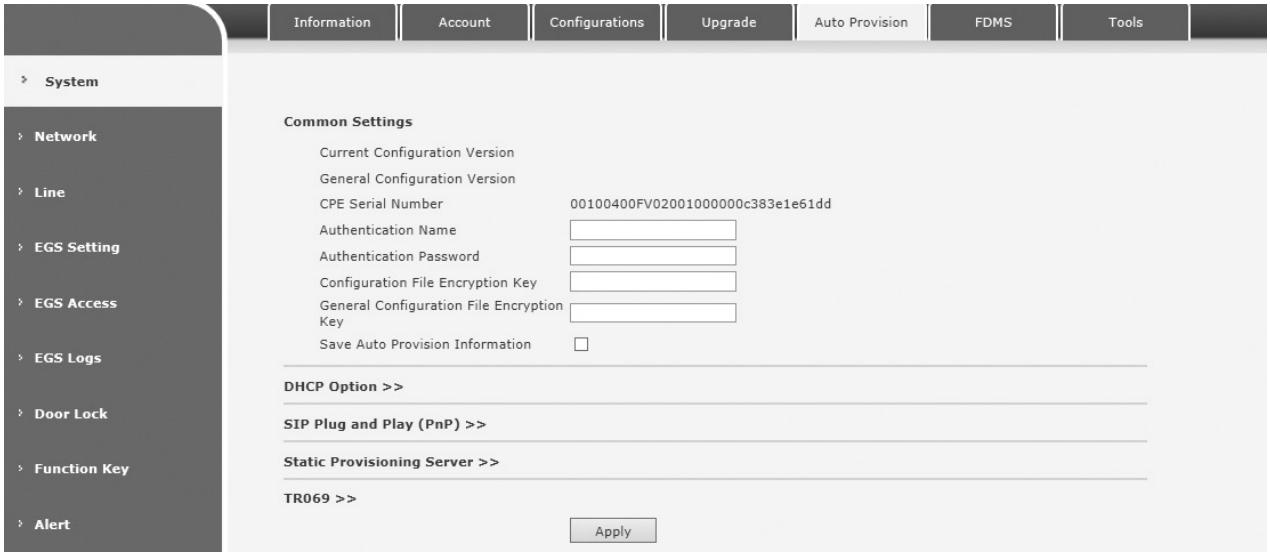
Configurations	
Field Name	**Explanation**
Export Configurations	Save the equipment configuration to a txt or xml file. Please note to Right click on the choice and then choose “Save Link As.”
Import Configurations	Browse to the config file, and press Update to load it to the equipment.
Reset to factory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

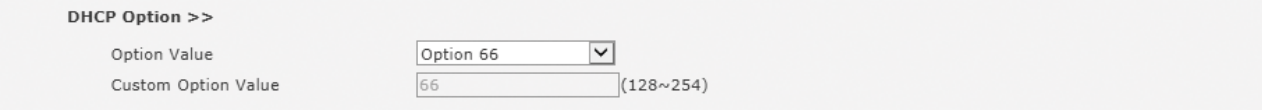
5.3.1.4 *Upgrade*

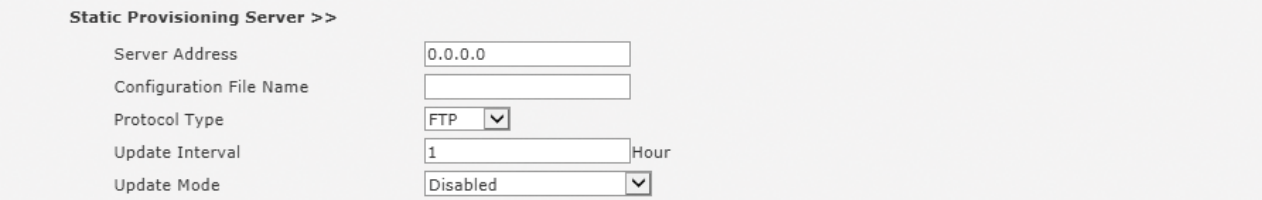


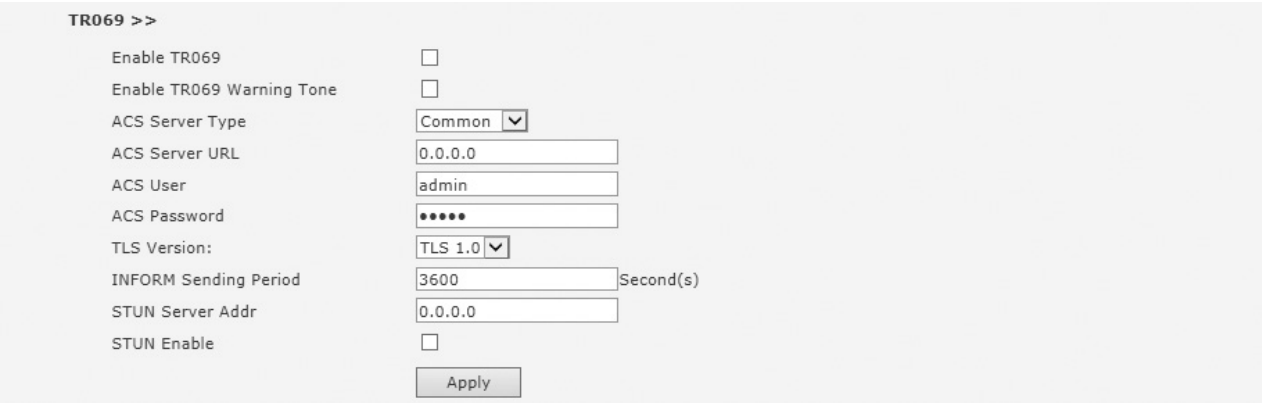
Upgrade	
Field Name	**Explanation**
Software upgrade	Browse to the firmware, and press Update to load it to the equipment.

5.3.1.5 Auto Provision





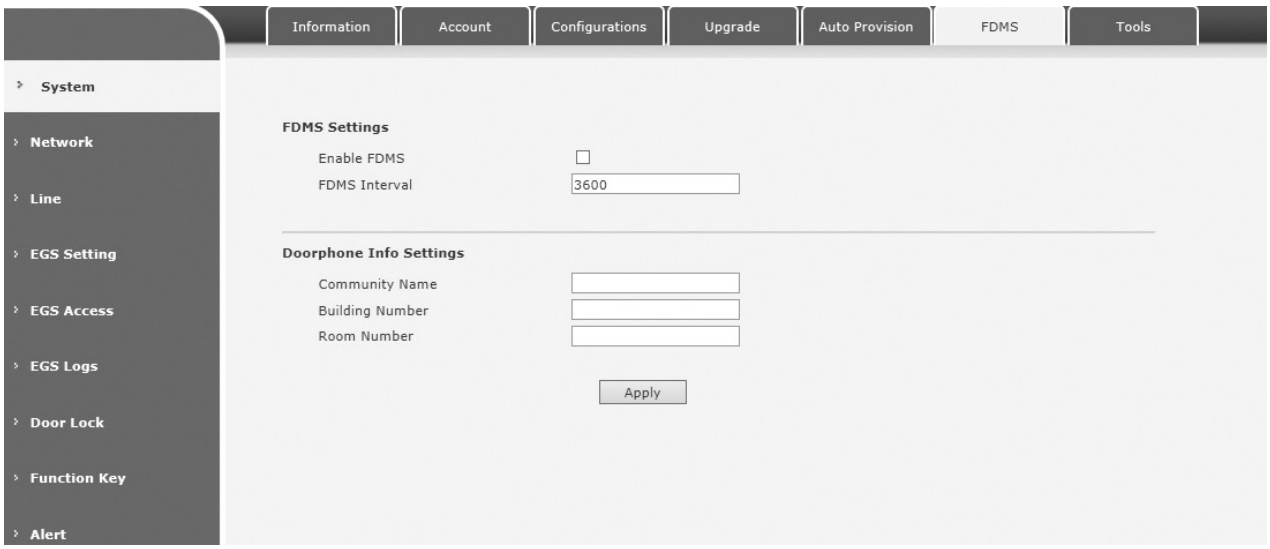




Auto Provision	
Field Name	**Explanation**
Common Settings	
Current Configuration Version	Show the current config file's version. If the version of configuration downloaded is higher than this, the configuration will be upgraded. If the endpoints confirm the configuration by the Digest method, the configuration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

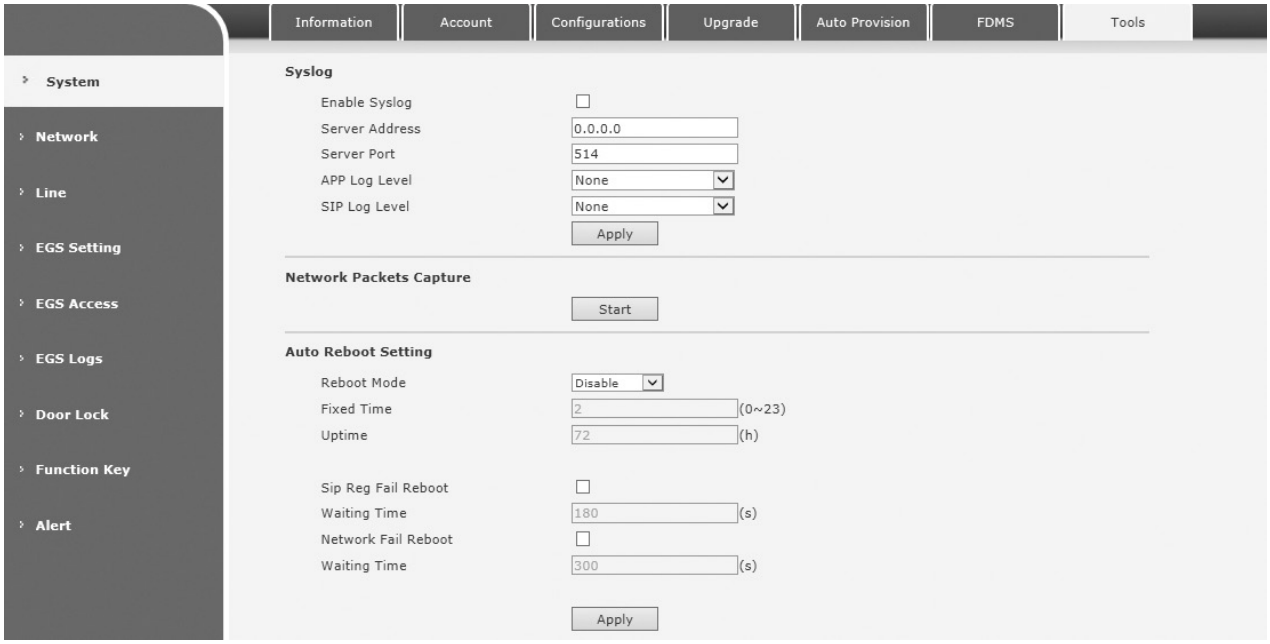
Update Interval	Specify the update interval time. Default is 1 hour.
Update Mode	1. Disable – no update 2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update interval
TR069	
Enable TR069	Enable/Disable TR069 configuration
Enable TR069 Warning Tone	Enable/Disable TR069 warning tone
ACS Server Type	Select Common or CTC ACS Server Type.
ACS Server URL	ACS Server URL.
ACS User	User name for ACS.
ACS Password	ACS Password.
TLS Version	Select the TLS transport layer security protocol version, in accordance with the service version
INFORM Sending Period	Time between transmissions of “Inform” Unit is seconds.
STUN Server Addr	Set STUN Server IP address
STUN Enable	Enable/Disable STUN

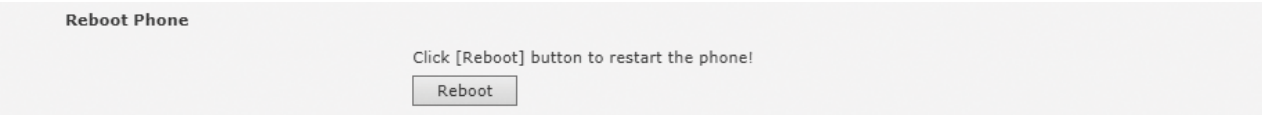
5.3.1.6 FDMS



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

5.3.1.7 Tools





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

There are 8 levels of debug information:

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

» Level 1: alert; Action must be taken immediately.

» Level 2: critical; System is probably working incorrectly.

» Level 3: error; System may not work correctly.

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

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

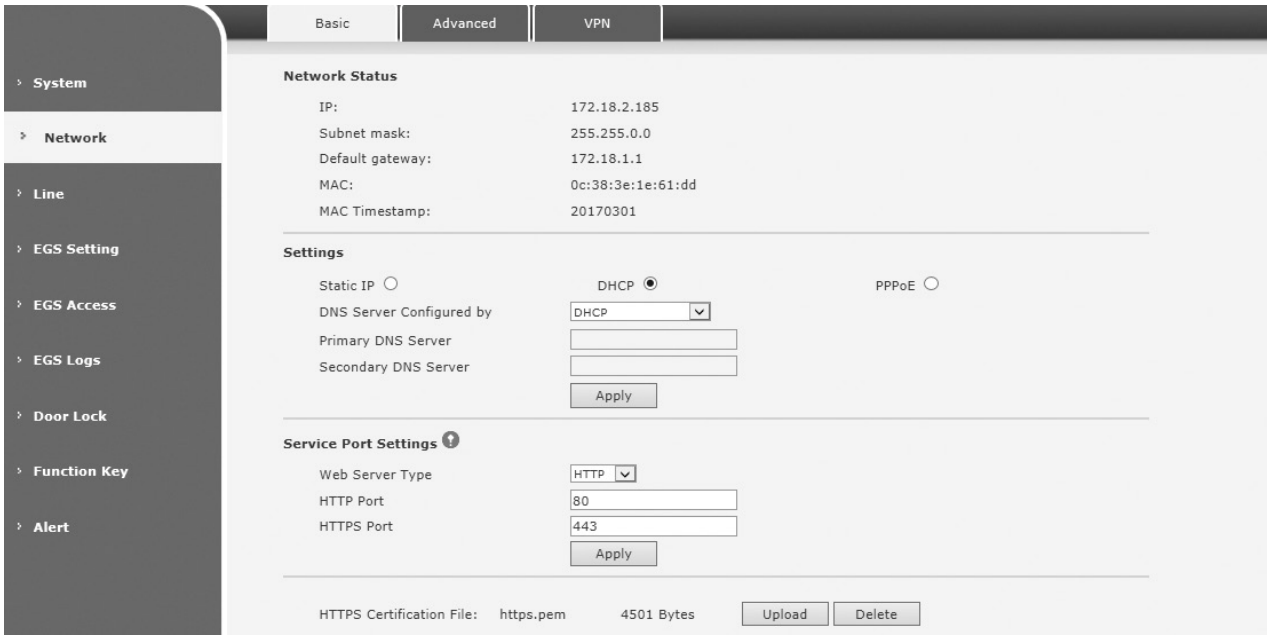
» Level 6: Informational; It is the normal daily messages.

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

Tools	
Field Name	**Explanation**
Syslog	
Enable Syslog	Enable or disable system log.
Server Address	System log server IP address.
Server Port	System log server port.
APP Log Level	Set the level of APP log.
SIP Log Level	Set the level of SIP log.
Network Packets Capture	Capture a packet stream from the equipment. This is normally used to troubleshoot problems.
Auto Reboot Setting	Configure the restart mode and restart time of the device and restart it to restore the device to its best state.
Reboot Phone	Some configuration modifications require a reboot to become effective. Clicking the Reboot button will lead to reboot immediately. NOTE: Be sure to save the configuration before rebooting.

5.3.2 Network

5.3.2.1 Basic



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 of time.
Settings	Select the appropriate network mode. The equipment supports three network modes:
Static IP	Network parameters must be entered manually and will not change. All parameters are provided by the ISP.
DHCP	Network parameters are provided automatically by a DHCP server.
PPPoE	Account and Password must be input manually. These are provided by your ISP.
If Static IP is chosen, the screen below will appear. Enter values provided by the ISP.	
DNS Server Configured by	Select the Configured mode of the DNS Server.

Primary DNS Server	Enter the server address of the Primary DNS.
Secondary DNS Server	Enter the server address of the Secondary DNS.

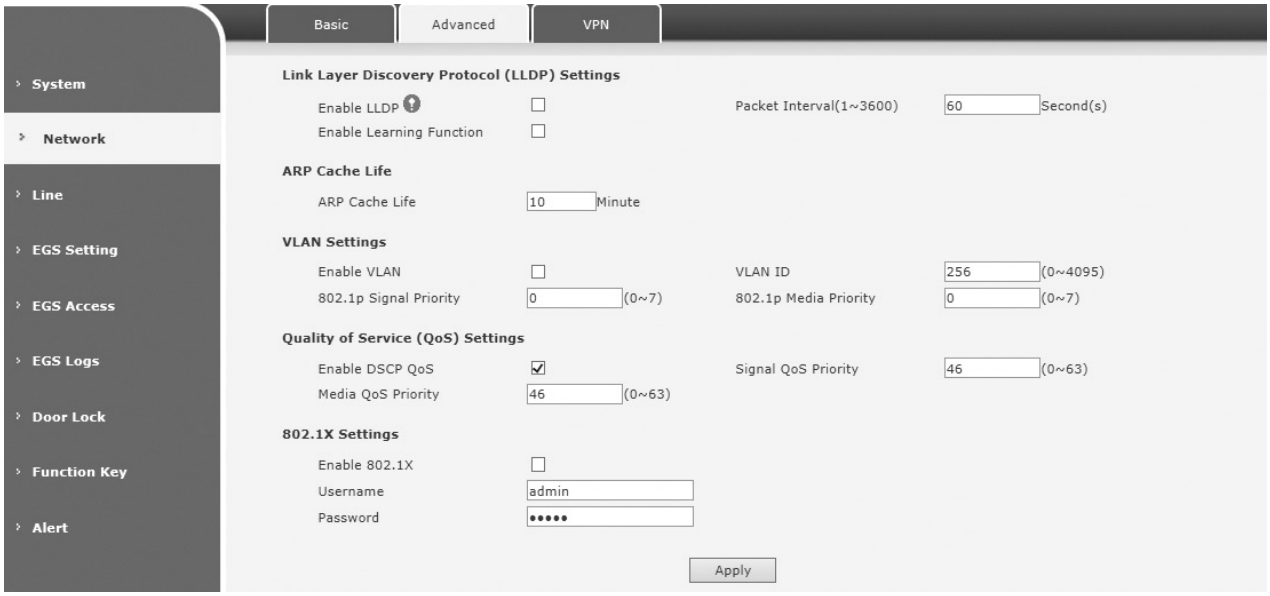
Click the APPLY button after entering the new settings. The equipment will save the new settings and apply them.
If a new IP address was entered for the equipment, it must be used to login to the phone after clicking the APPLY button.

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

NOTE:

1. Any changes made on this page require a reboot to become active.
2. It is suggested that the make the values bigger than 1024 if users change the port to HTTPS.
   Values less than 1024 are reserved.
3. If the HTTP port is set to 0, HTTP service will be disabled.

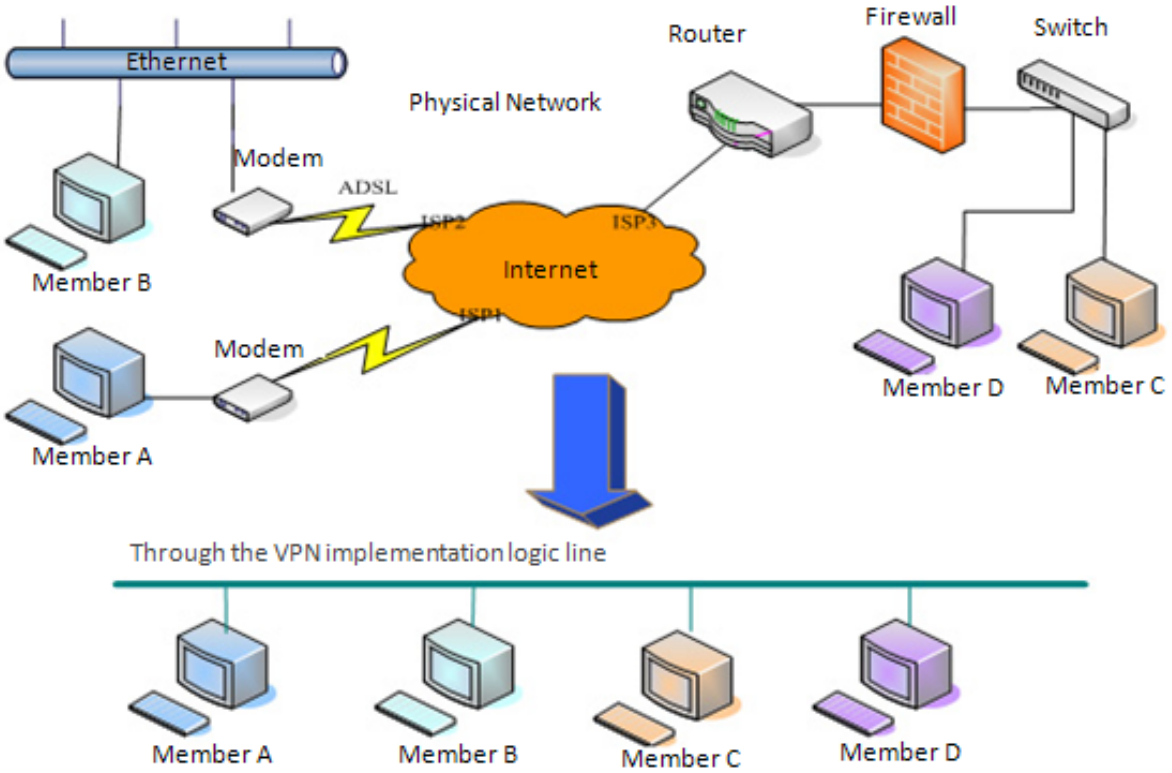
5.3.2.2 Advanced

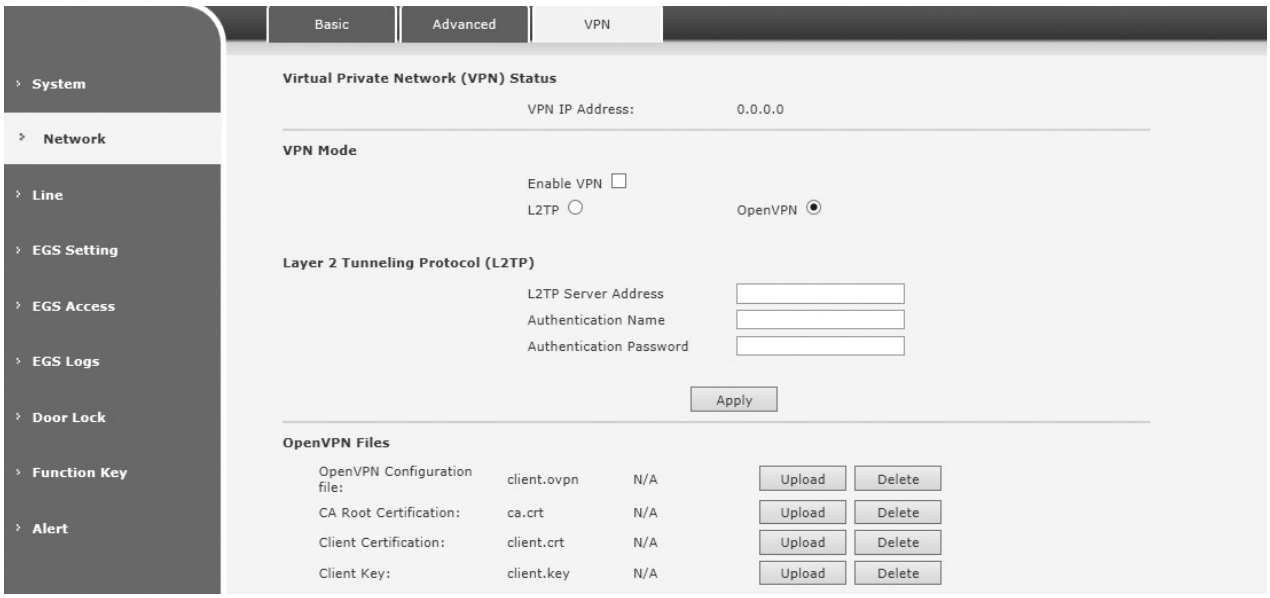


Advanced	
Field Name	**Explanation**
Link Layer Discovery Protocol (LLDP) Settings	
Enable LLDP	Enable the device to send LLDP packets.
Packet Interval (1~3600)	The time interval of device sending packet. The default value is 60s.
Enable Learning Function	Open the device to learn LLDP function, after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

5.3.2.3 VPN

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



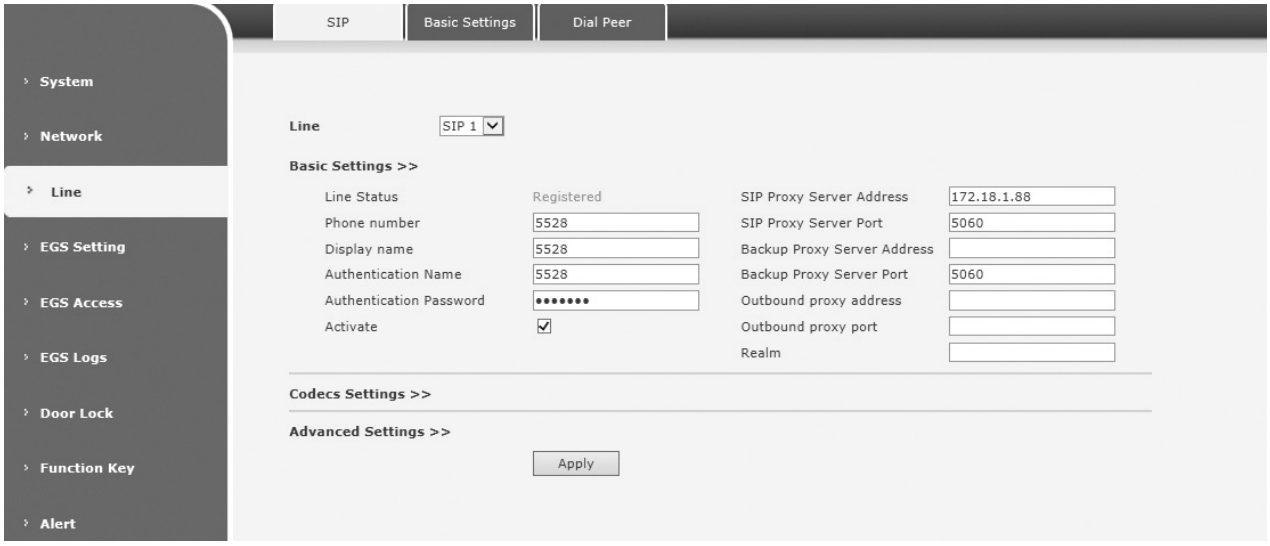


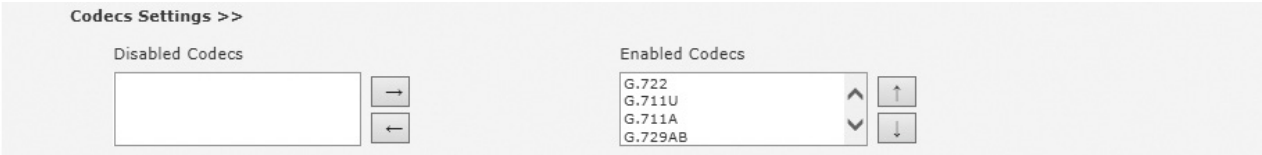
VPN	
Field Name	**Explanation**
VPN Status	
VPN IP Address	Show the current VPN IP address.
VPN Mode	
Enable VPN	Enable/Disable VPN.
L2TP	Select Layer 2 Tunneling Protocol
OpenVPN	Select OpenVPN Protocol. (Only one protocol may be activated. After the selection is made, the configuration should be saved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

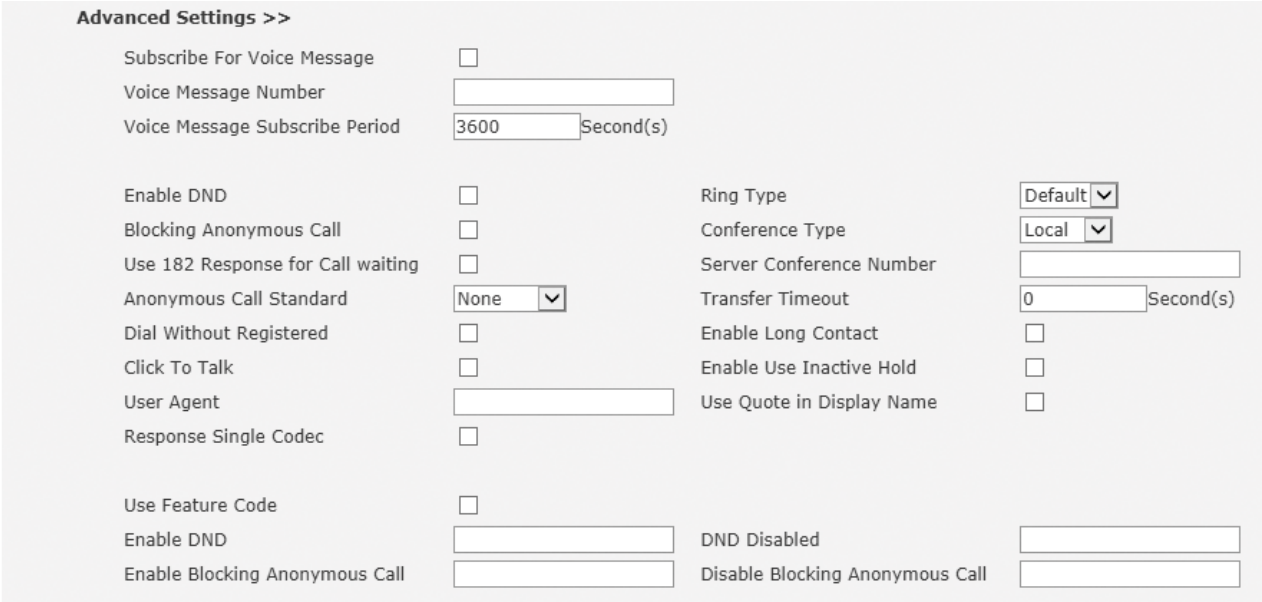
5.3.3 Line

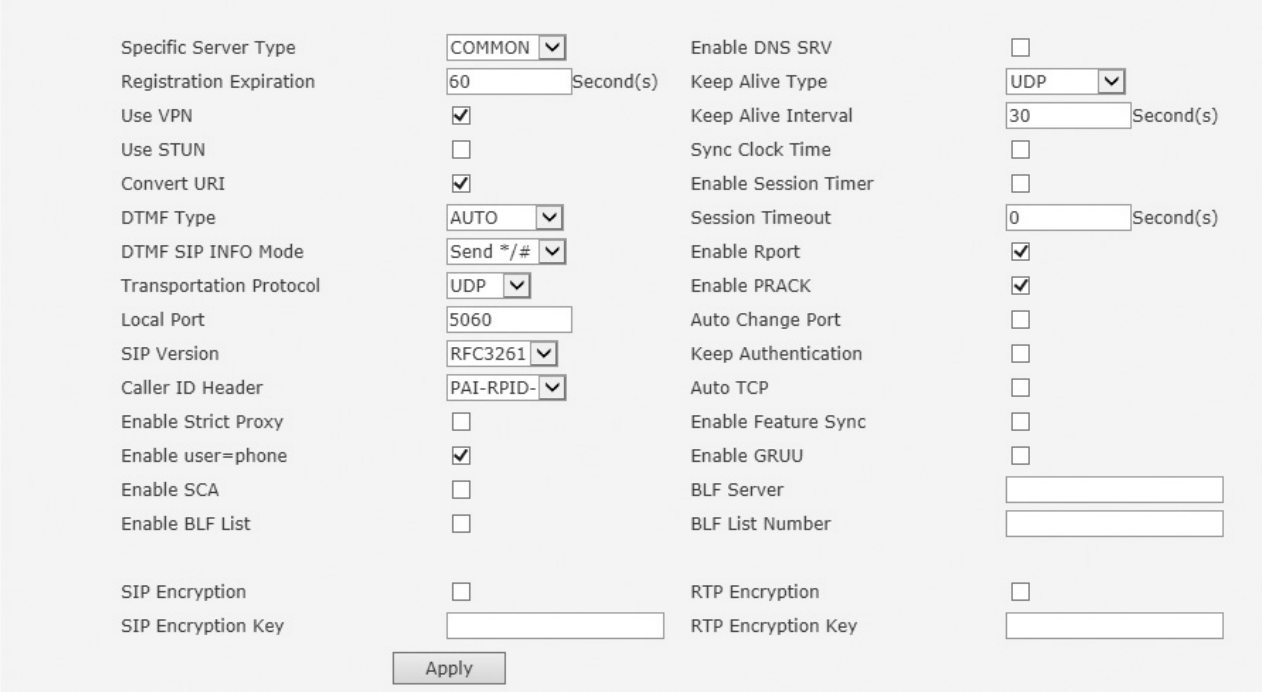
5.3.3.1 SIP

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

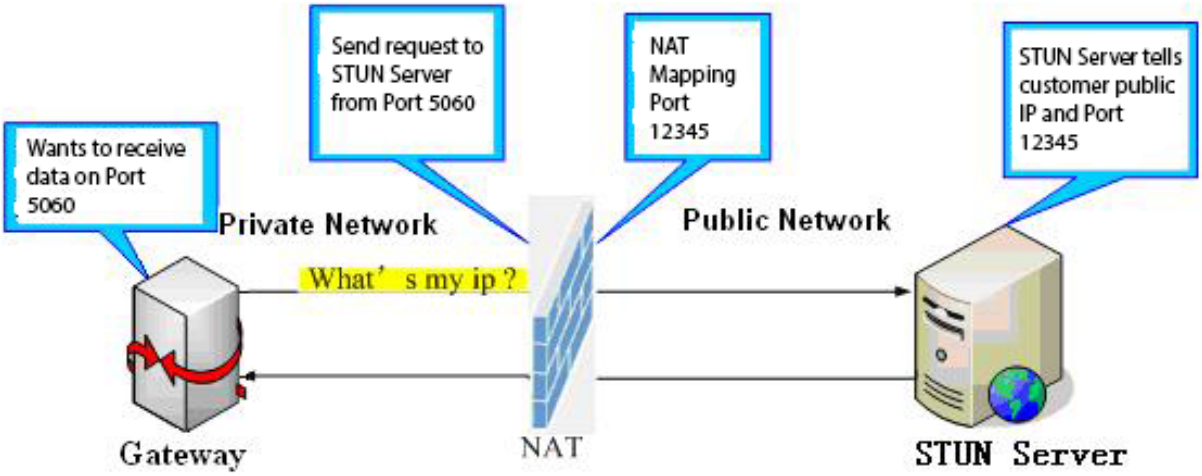
Activate	Whether the service of the line should be activated
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server
SIP Proxy Server Port	Enter the SIP proxy server port, default is 5060
Outbound proxy address	Enter the IP or FQDN address of outbound proxy server which are provided by the service provider
Outbound proxy port	Enter the outbound proxy port, default is 5060
Realm	Enter the SIP domain if requested by the service provider
Codecs Settings	Set the priority and availability of the codecs by adding or removing them from the list.
Advanced Settings	
Subscribe For Voice Message	Enable the device to subscribe a voice message of waiting notification, if it is enabled, the device will receive notification from the server when there is voice message waiting on the server
Voice Message Number	Set the number for retrieving voice message
Voice Message Subscribe Period	Set the interval of voice message notification subscription
Enable DND	Enable Do-not-disturb, any incoming call to this line will be rejected automatically
Blocking Anonymous Call	Reject any incoming call without presenting caller ID
Use 182 Response for Call waiting	Set the device to use 182 response code at call waiting response
Anonymous Call Standard	Set the standard to be used for anonymous
Dial Without Registered	Set call out by proxy without registration
Click To Talk	Set Click To Talk
User Agent	Set the user agent, the default is Model with Software Version.
Response Single Codec	If setting is enabled, the device will use single codec in responding to an incoming call request
Ring Type	Set the ring tone type for the line
Conference Type	Set the type of call conference, Local = set up call conference by the device itself, maximum supports two remote parties, Server = set up call conference by dialing to a conference room on the server
Server Conference Number	Set the conference room number when conference type is set to be Server
Transfer Timeout	Set the timeout of call transfer process.
Enable Long Contact	Allow more parameters in contact field per RFC 3840.
Enable Use Inactive Hold	When Inactive Hold is enabled, the caller's SIP packet will with Inactive fields on the condition of holding a call.
Use Quote in Display Name	Whether to add quote in display name.

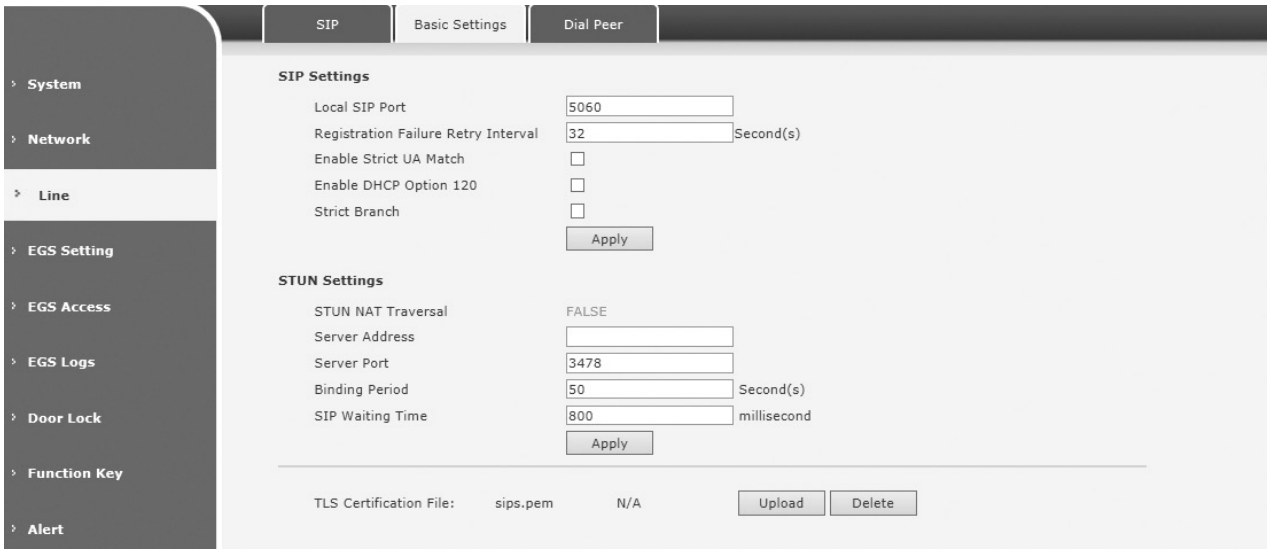
Use Feature Code	When this setting is enabled, the features in this section will not be handled by the device itself but by the server instead. In order to control the enabling of the features, the device will send feature code to the server by dialing the number specified in each feature code field.
Specific Server Type	Set the line to collaborate with specific server type.
Registration Expiration	Set the SIP expiration interval.
Use VPN	Set the line to use VPN restrict route.
Use STUN	Set the line to use STUN for NAT traversal.
Convert URI	Convert not digit and alphabet characters to %hh hex code.
DTMF Type	Set the DTMF type to be used for the line.
DTMF SIP INFO Mode	Set the SIP INFO mode to send '*' and '#' or '10' and '11'.
Transportation Protocol	Set the line to use TCP or UDP for SIP transmission.
Local Port	Set the Local Port.
SIP Version	Set the SIP version.
Caller ID Header	Set the Caller ID Header.
Enable Strict Proxy	Enables the use of strict routing. When the phone receives packets from the server, it will use the source IP address, not the address in via field.
Enable user = phone	Sets user = phone in SIP messages.
Enable SCA	Enable/Disable SCA (Shared Call Appearance)
Enable DNS SRV	Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list.
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole opened.
Keep Alive Interval	Set the keep alive packet transmitting interval.
Sync Clock Time	Synchronize with server time.
Enable Session Timer	Set the line to enable call ending by session timer refreshment. The call session will be ended if there is not new session timer event update received after the timeout period.
Session Timeout	Set the session timer timeout period.
Enable rPort	Set the line to add rPort in SIP headers.
Enable PRACK	Set the line to support PRACK SIP message.
Auto Change Port	Enable/Disable Auto Change Port.
Keep Authentication	Keep the authentication parameters from previous authentication.
Auto TCP	Using TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes.
Enable Feature Sync	Feature Sycn with server.
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)

RTP Encryption	Enable RTP encryption such that RTP transmission will be encrypted.
RTP Encryption Key	Set the pass phrase for RTP encryption.

5.3.3.2 Basic Settings

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



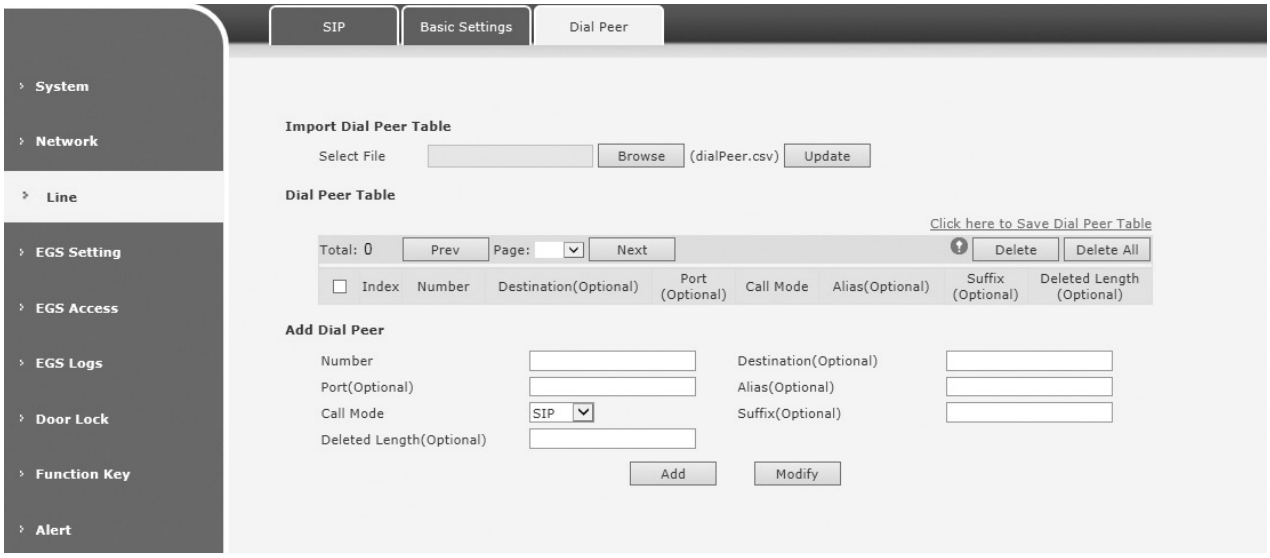


Basic Settings	
Field Name	**Explanation**
SIP Settings	
Local SIP Port	Set the local SIP port used to send/receive SIP messages.
Registration Failure Retry Interval	Set the retry interval of SIP REGISTRATION when registration failed.
Enable Strict UA Match	Enable or disable Strict UA Match
Enable DHCP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

NOTE:
The SIP STUN is used to achieve the SIP penetration of NAT, and the realization of a service, when the 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.

5.3.3.3 *Dial Peer*

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



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

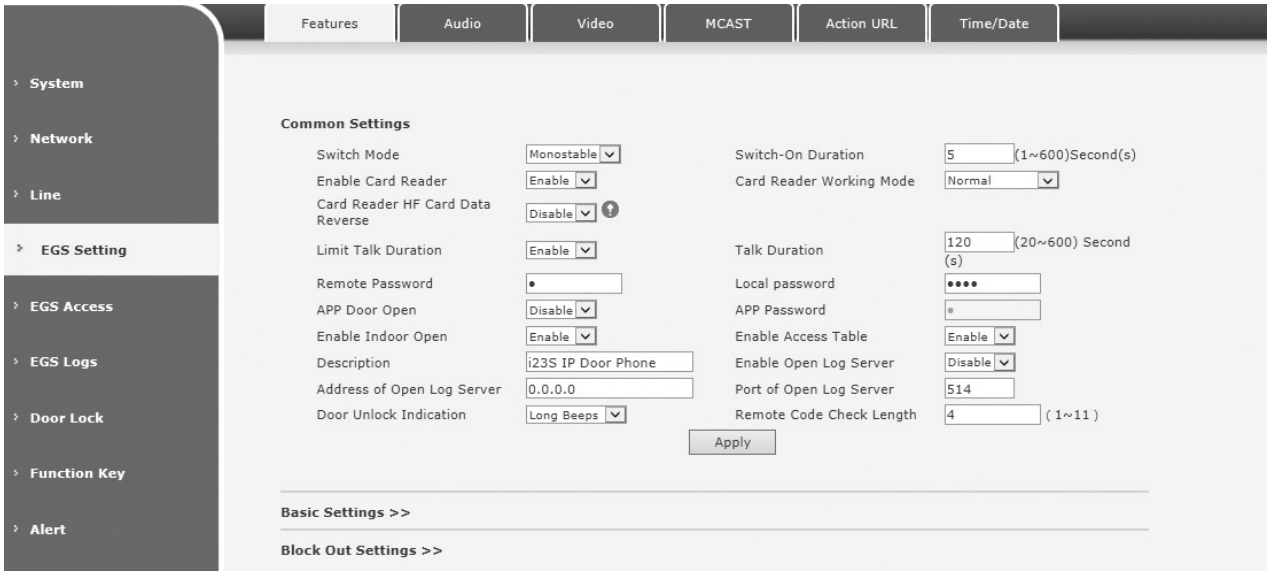
NOTE: aliases are divided into four types and must be combined with the replacement length:

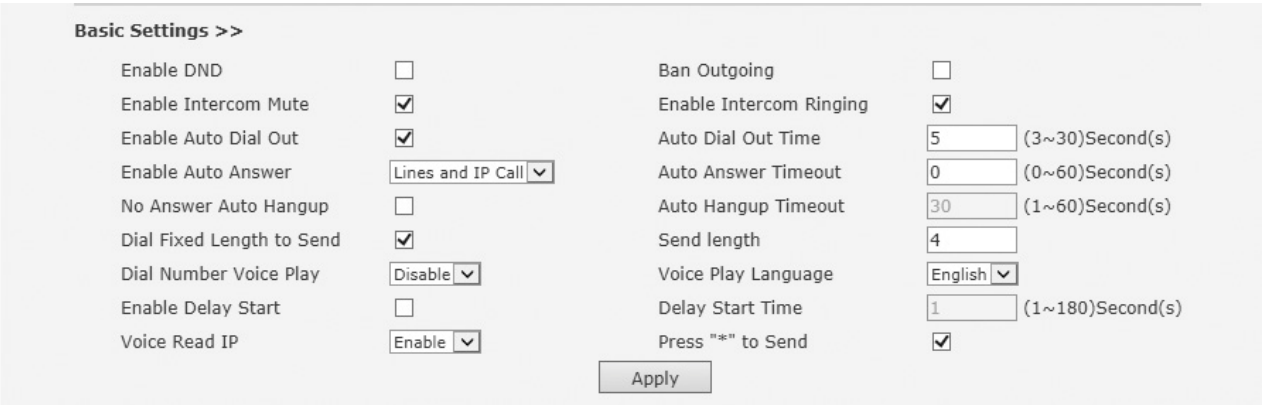
1. add: xxx, add xxx before the number. This can help users save dialing length;
2. all: xxx, all replaced by xxx; can achieve speed dial, such as user configuration dial-up 1, then by configuring all: number to change the actual call out the number;
3. del, delete the number before the n bit, n by the replacement length set;
4. rep: xxx, the number n before the number is replaced by xxx, n is set by the replacement length. For example, if the user wants to dial the PSTN (010-62281493) through the floor service provided by the VoIP operator, and the actual call should be 010-62281493, then we can configure the called number 9T, then rep: 010, and then delete the length Set to 1. Then all users call the 9 at the beginning of the phone will be replaced with 010 + number sent. To facilitate the user to call the habit of thinking mode;

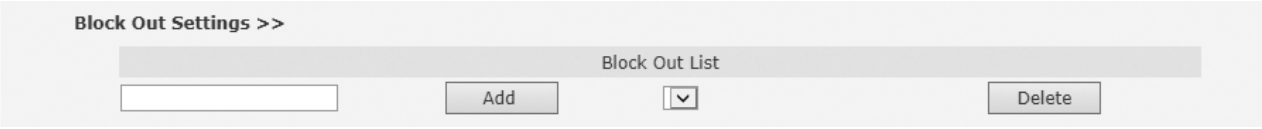
Call Mode	Configuration selection of different signaling protocols, SIP;
Suffix	Configure the suffix, this is optional configuration items: that is, after the dial-up number to add this suffix, no configuration shows no suffix;
Deleted Length	Configure the replacement / delete length, the number entered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

5.3.4 EGS Setting

5.3.4.1 Features





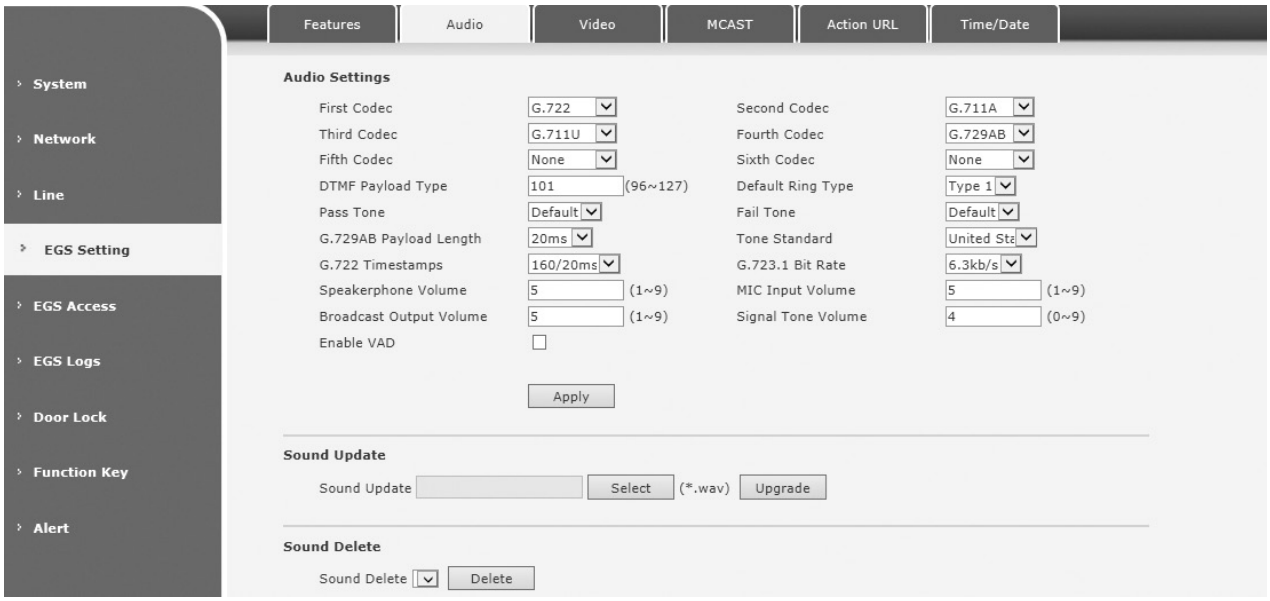


Features	
Field Name	**Explanation**
Common Settings	
Switch Mode	Monostable: there is only one fixed action status for door unlocking. See "Switch-On Duration" too. Bistable: there are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After changed, the status would be kept. default Value is Monostable.
Switch-On Duration	Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Default Value is 5 seconds.
Enable Card Reader	Enable or disable card reader for RFID/IC cards.
Card Reader Working Mode	Set RFID/IC card stats: » Normal: This is the work mode, in which user can use the authorized card can to open the door. » Card Issuing: This is the issuing mode; the swiped card will be added in access list automatically. User could edit other parameters under EGS access. » Card Revoking: This is the revoking mode; the swiped card will be deleted from Access List.
Card Reader HF Card Data Reverse	Set the format of HF card to make the data sequence reverse to meet with specific card.
Limit Talk Duration	If enabled, calls would be forced ended after talking time is up.
Talk Duration	The call will be ended automatically when time up. Initial Value is 120 seconds
Remote Password	Remote door unlocking password. Initial Value is "*".
Local password	Local door unlocking password via keypad, the default password length is 4. Initial Value is "6789".
APP Door Open	Enable or disable the APP Door Open.
APP password	APP door unlocking password. Initial Value is "*".
Enable Indoor Open	Enable or disable to use indoor switch to unlock the door.
Enable Access Table	Enable Access Table: enter <Access Code> for opening door during calls. Disable Access Table: enter <Remote Password> for opening door during calls. Default Enable.
Description	Device description displayed on IP scanning tool software. Initial Value is "i23S IP Door Phone".
Enable Open Log Server	Enable or disable to connect with log server.
Address of Open Log Server	Log server address (IP or domain name)
Port of Open Log Server	Log server port (0-65535), Initial Value is 514.
Door Unlock Indication	Indication tone for door unlocked. There are 3 types of tone: silent/short beeps/long beeps.

Remote Code Check Length	The remote access code length would be restricted with it. If the input access code length is matched with it, system would check it immediately. Initial Value is 4.
Basic Settings	
Enable DND	DND might be disabled phone for all SIP lines, or line for SIP individually. But the outgoing calls will not be affected.
Ban Outgoing	If enabled, no outgoing calls can be made.
Enable Intercom Mute	If enabled, mutes incoming calls during an intercom call.
Enable Intercom Ringing	If enabled, plays intercom ring tone to alert to an intercom call.
Enable Auto Dial Out	Enable Auto Dial Out.
Auto Dial Out Time	Set Auto Dial Out Time.
Enable Auto Answer	Enable Auto Answer function.
Auto Answer Timeout	Set Auto Answer Timeout.
No Answer Auto Hangup	Enable automatically hang up when no answer.
Auto Hangup Timeout	Configuration in a set time, automatically hang up when no answer.
Dial Fixed Length to Send	Enable or disable dial fixed length to send.
Send length	The number will be sent to the server after the specified numbers of digits are dialed.
Dial Number Voice Play	Configuration Open / Close Dial Number Voice Play.
Voice Play Language	Set language of the voice prompt.
Enable Delay Start	Enable or disable the start delay.
Delay Start Time	Set start delay time.
Voice Read IP	Enable or disable voice broadcast IP address.
Press “*” to Send	Enable or disable the Press “*” to Send, Initial Value is enable.
Block Out Settings	
Add or delete blocked numbers – enter the prefix of numbers which should not be dialed by the phone. For example, if 001 is entered, the phone would not dial any number beginning with 001. X and x are wildcards which match single digit. For example, if 4xxx or 4XXX is entered, the phone would not dial any 4 digits numbers beginning with 4. It would dial numbers beginning with 4 which are longer or shorter than 4 digits.	

5.3.4.2 Audio

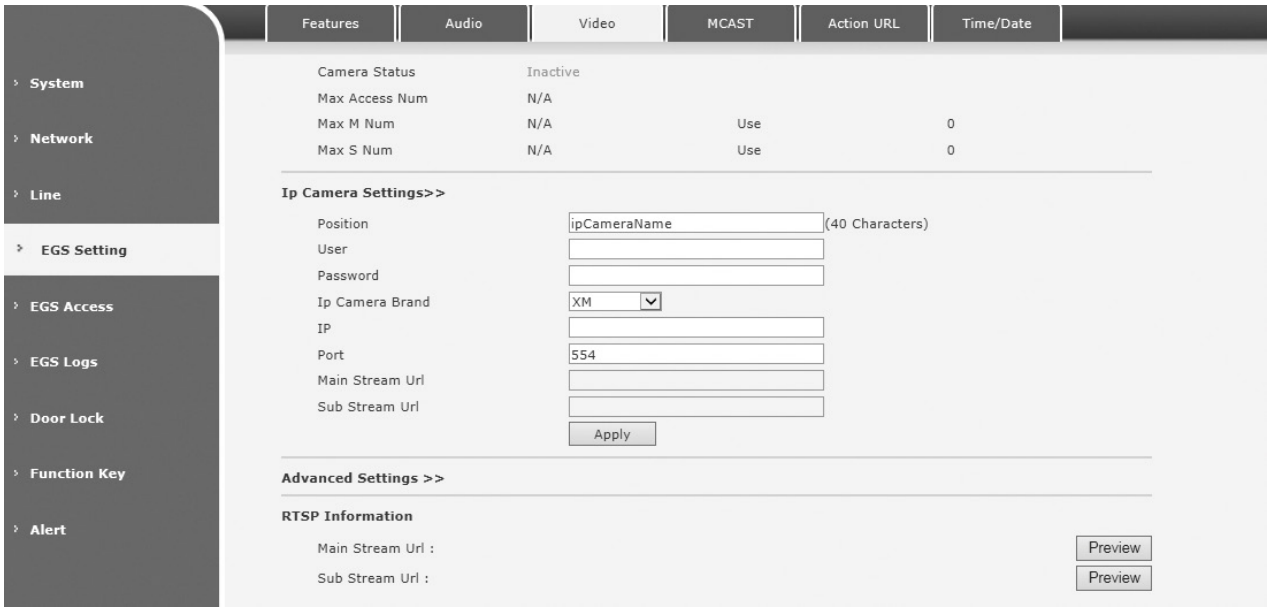
This page configures audio parameters such as voice codec, speak volume, mic volume and ringer volume.



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.
Pass Tone	When the door opened successfully, the device will play the correct tone set by the user.
Fail Tone	When the door fails to open, the terminal will play an error tone set by the user.
G.729AB Payload Length	G.729AB Payload Length – Adjusts from 10 – 60 ms.
Tone Standard	Configure tone standard area.
G.722 Timestamps	Choices are 160/20ms or 320/20ms.
G.723.1 Bit Rate	Choices are 5.3kb/s or 6.3kb/s.
Speakerphone Volume	Set the speaker calls the volume level.
MIC Input Volume	Set the MIC calls the volume level.
Broadcast Output Volume	Set the broadcast the output volume level.
Signal Tone Volume	Set the audio signal the output volume level.
Enable VAD	Enable or disable Voice Activity Detection (VAD). If VAD is enabled, G729 Payload length cannot be set greater than 20 ms.

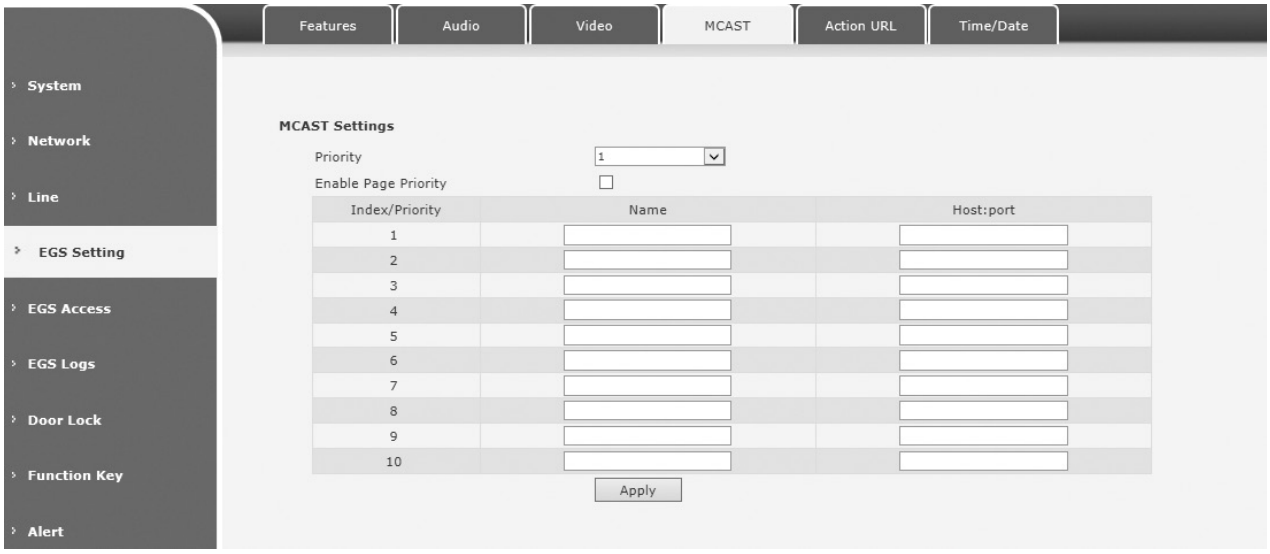
5.3.4.3 *Video*

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



Video	
Field Name	**Explanation**
Camera Status	Display the relevant information of the camera, including maximum access, maximum stream, maximum sub stream, and the status.
IP Camera Settings	
Position	Set IP Camera Name.
User name	External camera login required account.
Password	External camera login password required.
IP Camera Brand	Select the camera manufacturers.
IP address	IP address of the camera, please use the camera matching scan tool to obtain the IP address.
Port	Camera port number.
Advanced Settings	
Video Direction	Select the transport type of the video stream.
H.264 Payload Type	Set the payload type of H.264.
RTSP information	Click [Apply], the connection automatically shows the camera does not show the reverse.
Preview	Copy and paste the main stream or sub-stream URL into the VLC player, or click [Preview] to display the current camera video.

5.3.4.4 MCAST



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

MCAST Settings

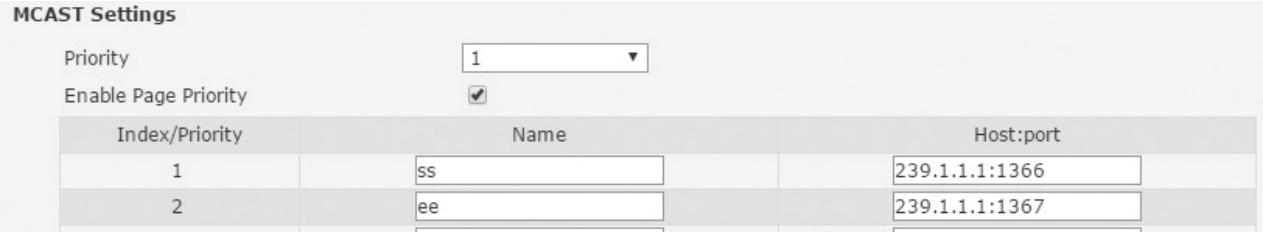
Equipment can be set up to monitor up to 10 different multicast addresses, which is used to receive the multicast RTP stream sent by the multicast address.

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

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

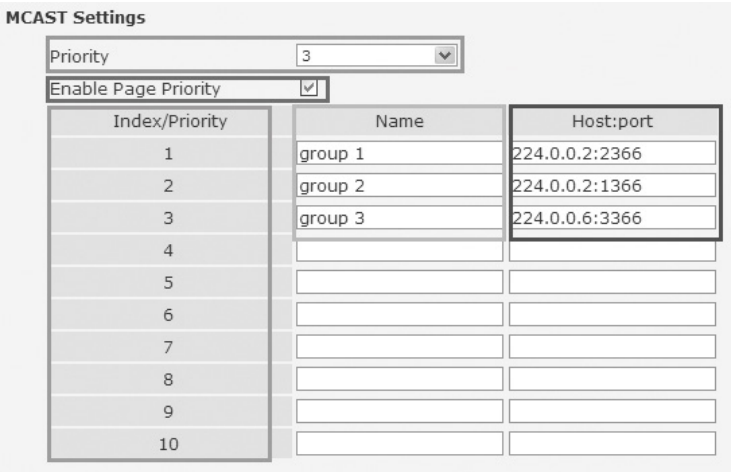
» **The options are as follows:**
  - 1-10: To definite the priority of the common calls, 1 is the top level while 10 is the lowest
  - Disable: ignore all incoming multicast RTP stream
  - Enable the page priority:
    Page priority determines the device how to deal with the new receiving multicast RTP stream when it is in multicast session currently. When Page priority switch is enabled, the device will automatically ignore the low priority multicast RTP stream but receive top-level priority multicast RTP stream, and keep the current multicast session in state; If it is not enabled, the device will automatically ignore all receiving multicast RTP stream.

» **Web Settings**:



The multicast SS priority is higher than that of EE, which is the highest priority.
NOTE: when pressing the multicast key for multicast session, both multicast sender and receiver will beep.

Listener configuration



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

» **Purple part (host: port)**
It is a set of addresses and ports to listen, separated by a colon.

» **Pink part (index / priority)**
Multicast is a sign of listening, but also the monitoring multicast priority. The smaller number refers to higher priority.

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

› The purpose of setting monitoring multicast "Group 1" or "Group 2" or "Group 3" launched a multicast call.

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

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

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

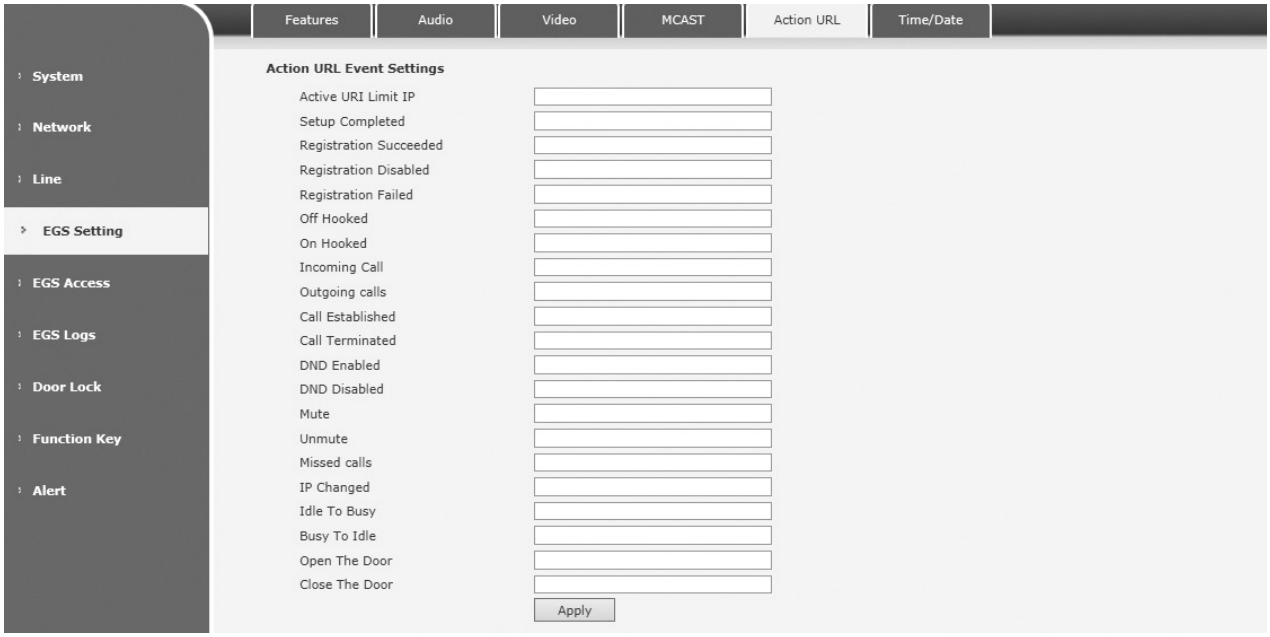
» **Green part (Enable Page priority)**
Set whether to open more priority is the priority of multicast, multicast is pink part number.
Explain how to use:
  › The purpose of setting monitoring multicast “group 1” or “3” set up listening “group of 1” or “3” multicast address multicast call.
  › All equipment has been a path or multi-path multicast phone, such as listening to “multicast information group 2”.
  › If multicast is a new “group of 1”, because “the priority group 1” is 2, higher than the current call “priority group 2” 3, so multicast call will can come in.
  › If multicast is a new “group of 3”, because “the priority group 3” is 4, lower than the current call “priority group 2” 3, “1” will listen to the equipment and maintain the “group of 2”.

Multicast service

» **Send:** when configured ok, our key press shell on the corresponding equipment, equipment directly into the Talking interface, the premise is to ensure no current multicast call and 3-way of the case, the multicast can be established.

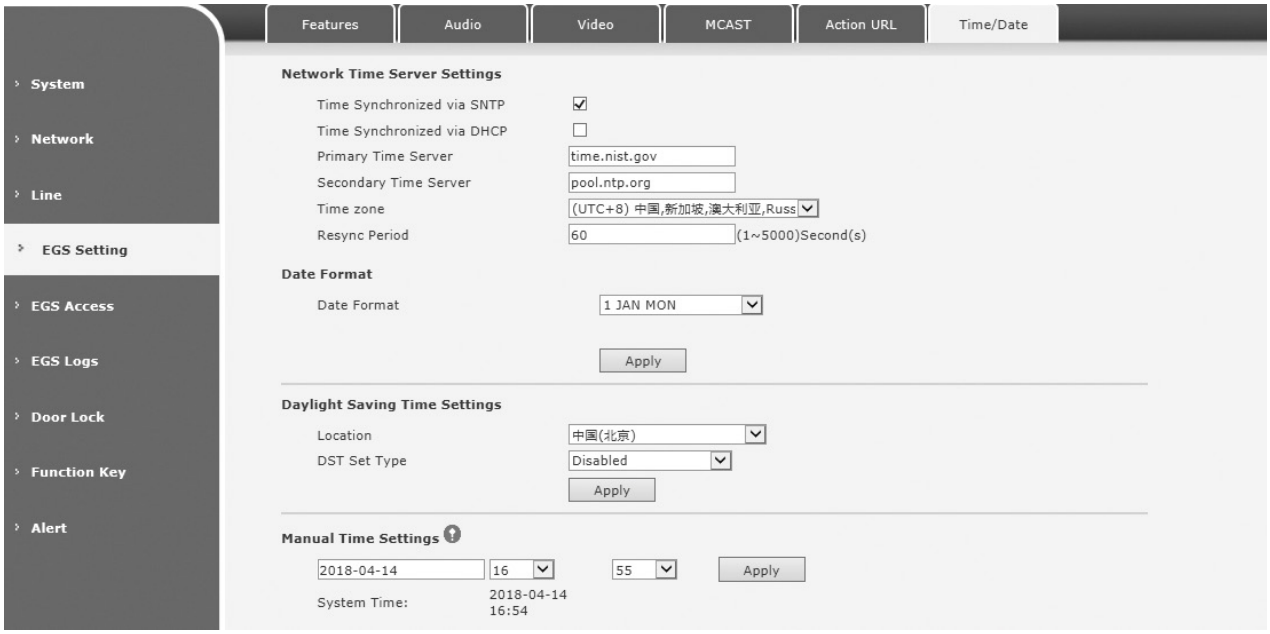
» **Monitor:** IP port and priority configuration monitoring device, when the call is initiated and incoming multicast, directly into the Talking interface equipment.

5.3.4.5 Action URL



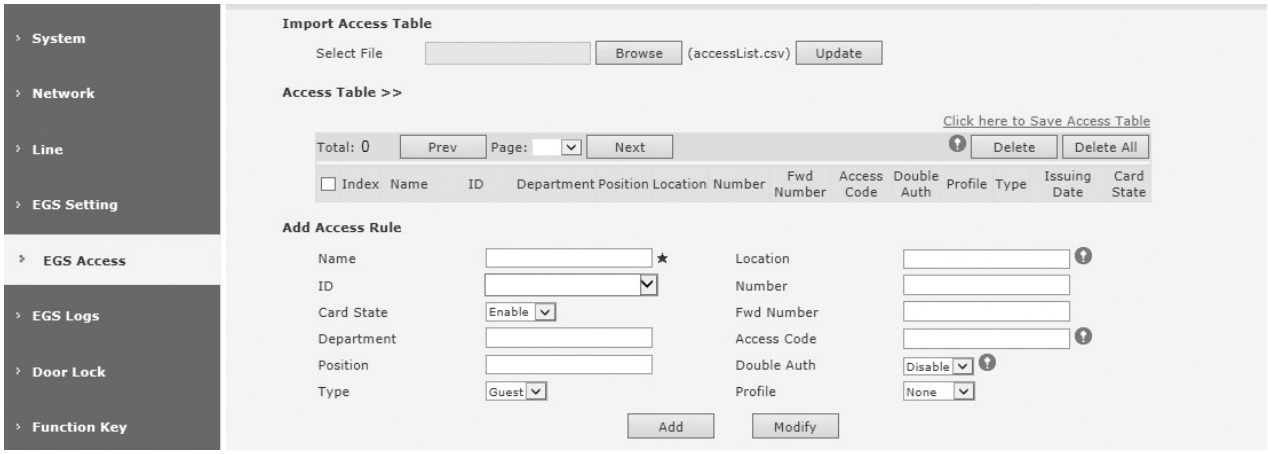
Action URL	
Field Name	**Explanation**
Action URL Event Settings	URL for various actions performed by the phone. These actions are recorded and sent as xml files to the server. Sample format is: http://InternalServer /FileName.xml

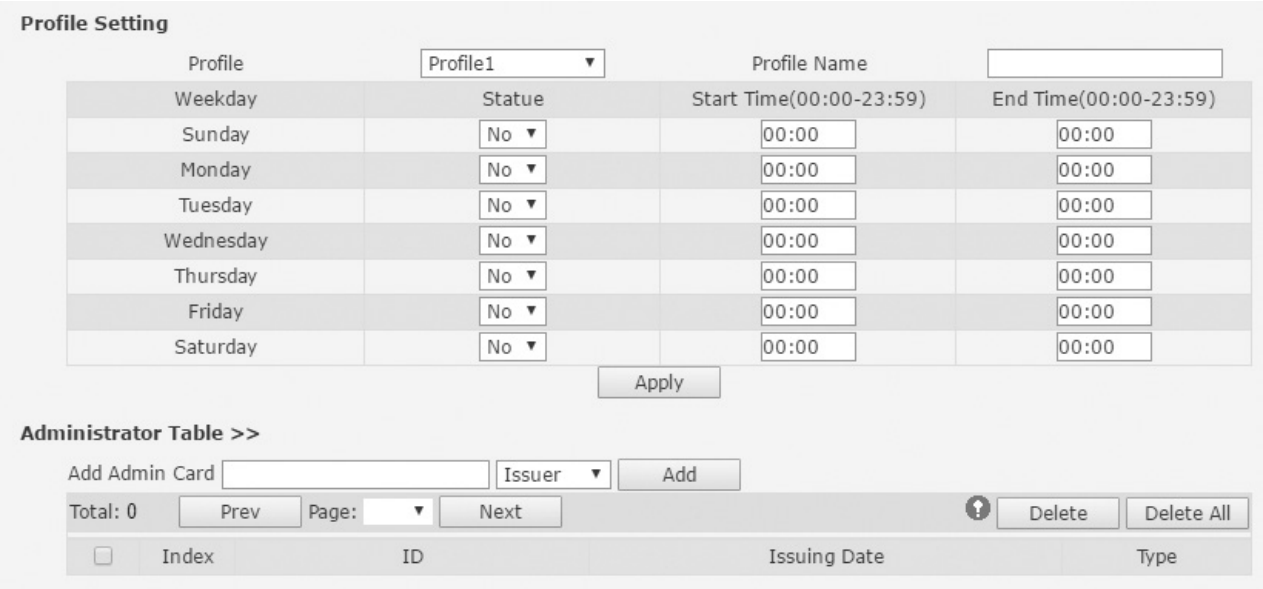
5.3.4.6 Time/Date



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 will try to connect to secondary time server to get time synchronization.
Time zone	Select the time zone
Resync Period	Time of re-synchronization with time server
Date Format	
Date Format	Select the time/date display format
Daylight Saving Time Settings	
Location	Select the user's time zone specific area
DST Set Type	Select automatic DST according to the preset rules of DST, or the manually input rules
Manual Time Settings	The time set by hand, need to disable SNTP service first.

5.3.5 EGS Access





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

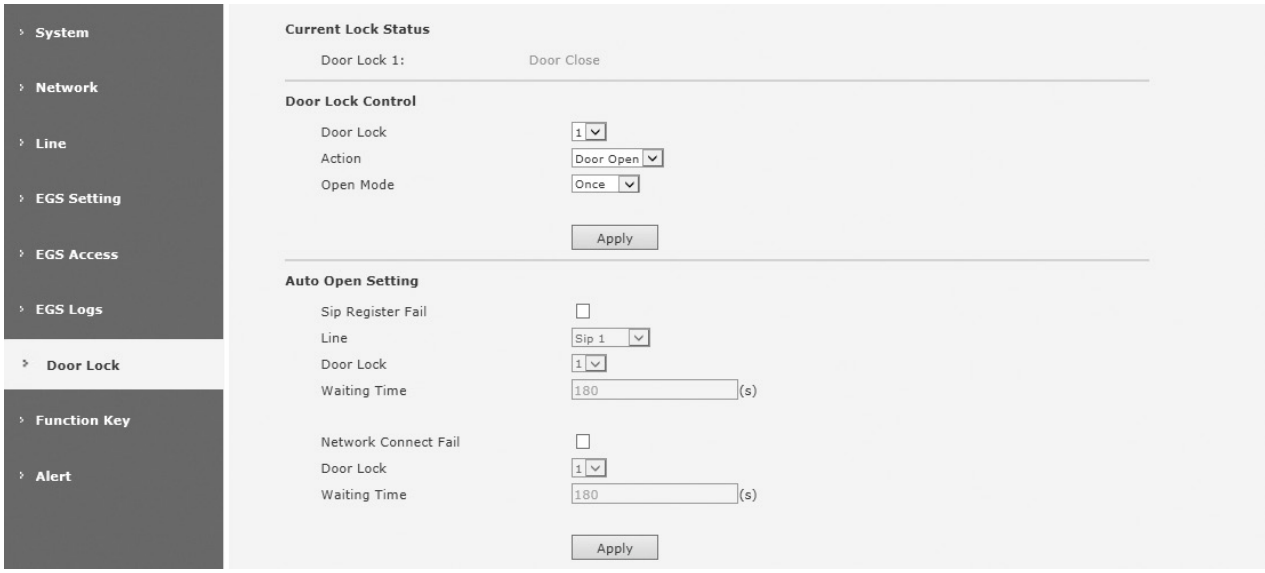
Number	User phone number
Card State	Enable or disable holder's RFID card
Fwd Number	Call forwarding number when above phone number is unavailable.
Department	Card holder's department
Access Code	1. When the door phone answers the call from the corresponding <Phone Num> user, then the <Phone Num> user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

5.3.6 EGS Logs

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

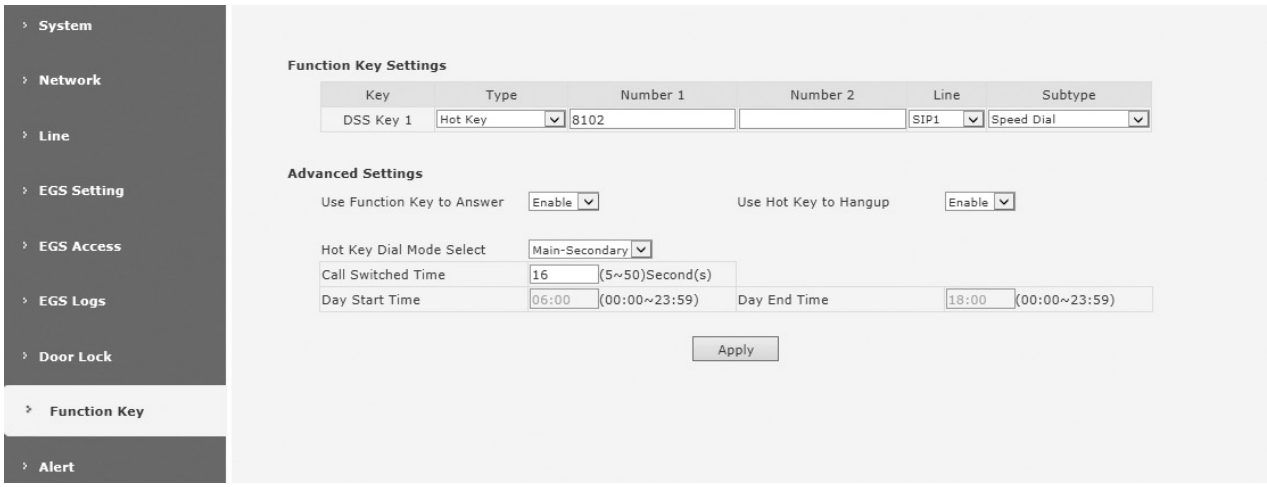
EGS Logs	
Field Name	**Explanation**
Door Open Log	
Result	Show the results of the open the door (Succeeded or Failed)
Time	The time of opening door.
Access Name	If the door was opened by swipe card or remote unlocking door, the device would display remote access name.
Access ID	1. If the opening door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

5.3.7 Door Lock



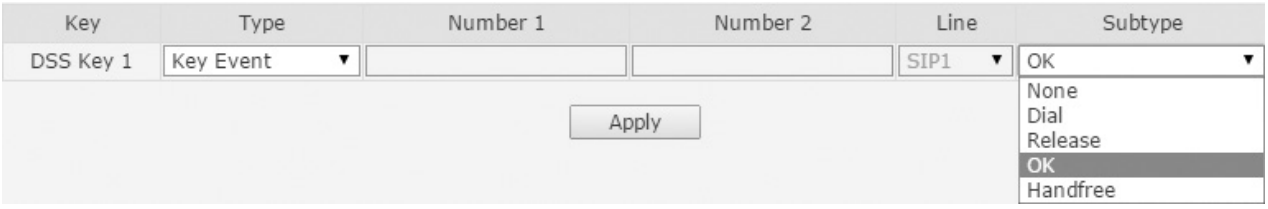
Door Lock	
Field Name	**Explanation**
Current Lock Status	
Door Lock	Display the current lock status.
Door Lock Control	
Door Lock	Door lock code
Action	Action to open/close the door
Open Mode	The action of door open mode: #1 The door will open after choose the “once” and it will return to normal status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

5.3.8 Function Key



Key Event

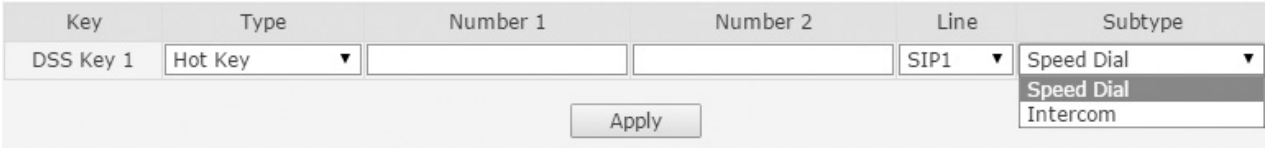
You might set up the key type with the Key Event.



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

Hot Key

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

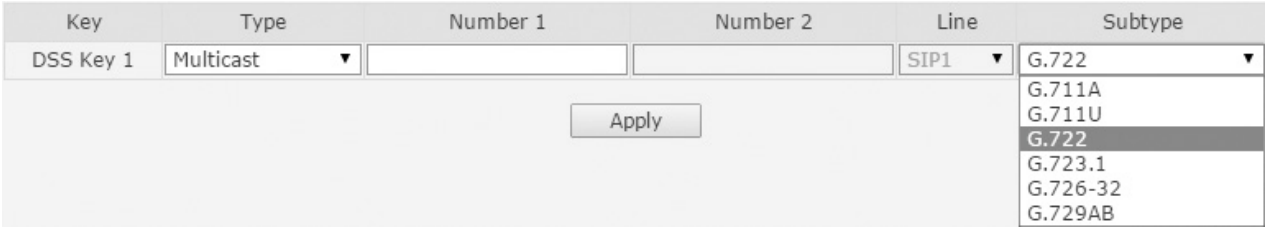


Type	Number	Line	Subtype	Usage
Hot Key	Fill the called party's SIP account or IP address	The SIP account corresponding lines	Speed Dial	Using Speed Dial mode together with Enable Speed Dial Hangup Enable, can define whether this call is allowed to be hung up by re-pressing the speed dial key.
			Intercom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

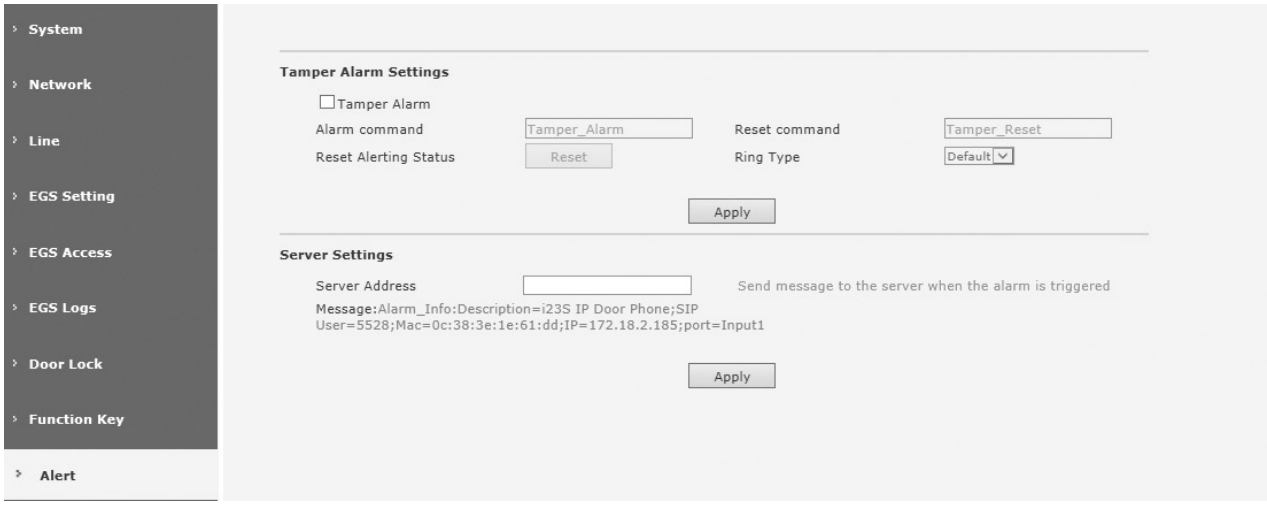


Type	Number	Subtype	Usage
Multicast	Set the host IP address and port number; they must be separated by a colon	G.711A	Narrowband speech coding (4Khz)
		G.711U	
		G.722	Wideband speech coding (7Khz)
		G.723.1	Narrowband speech coding (4Khz)
		G.726-32	
		G.729AB	

» 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 makes a multicast, all devices monitoring the address can receive the multicast data.

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

5.3.9 Alert



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

6. Appendix

6.1 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**	12 V / 650 mA DC
	WAN	10/100BASE-TX s Auto-MDIX, RJ-45
RFID/IC card reader		EM4100 (125 Khz) MIFARE One (13.56 Mhz)
Power supply mode		12 V / 1A DC or PoE
PoE		PoE
Cables		CAT5 or better
Shell Material		Cast aluminium panel, Cast aluminium back shell
Working temperature		-40°C to 70°C
Working humidity		10% – 95%
Storage temperature		-40°C to 70°C
Installation way		Wall mounted or In-wall
Dimension		Wall mounted: 223 × 130 × 74 mm In-wall: 270 × 150 × 61mm
Package size		310 × 175 × 115 mm
Equipment weight		1500 g
Gross weight		1800 g

6.2 Basic functions

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

6.3 Schematic diagram

7. Other instructions

7.1 Open door modes

Local

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

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

7.2 Management of card

Add Administrator>>

ID	0003476384	Add
Type	Issuer	

Add Administrator>>

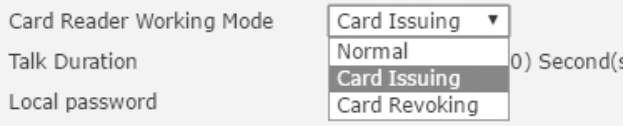
ID	0003408919	Add
Type	Revocation	

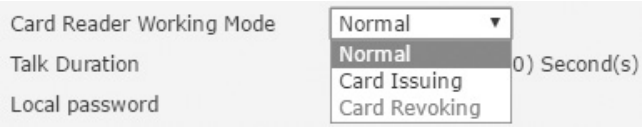
Administrator Table>>

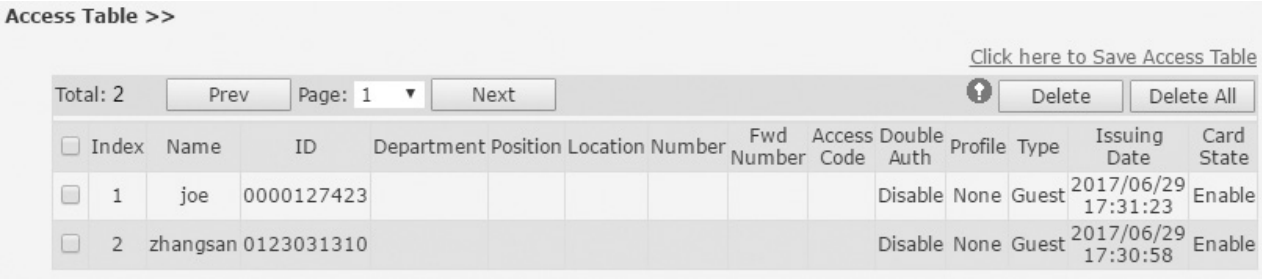
ID	Date	Type
0003476384	JAN 01 02:09:04	Issuer
0003408919	JAN 01 02:09:29	Revocation

Method 1

Used to add cards for starters typically





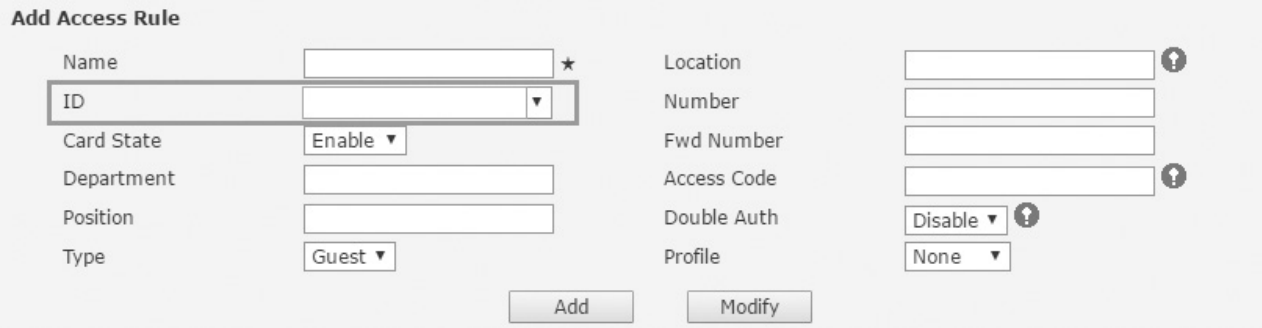


Method 2

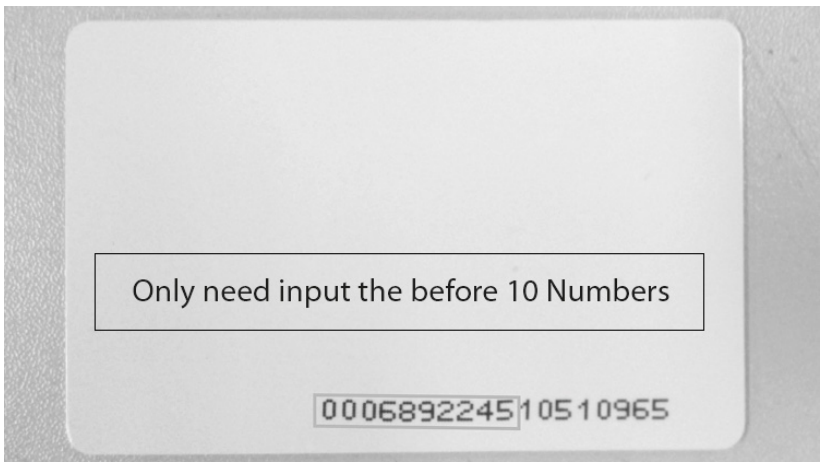
Used to add cards for professionals

Method 3

Use to add few cards

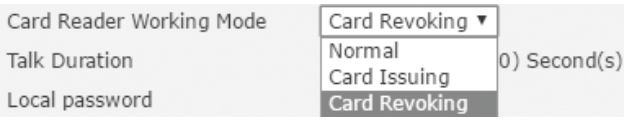


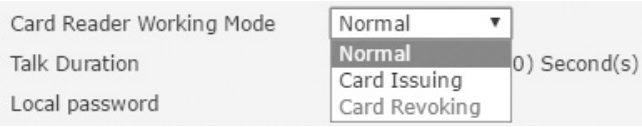
NOTE: you can also use the USB card reader connected with PC to get cards ID automatically.



Method 1

Used to batch delete cards for starters



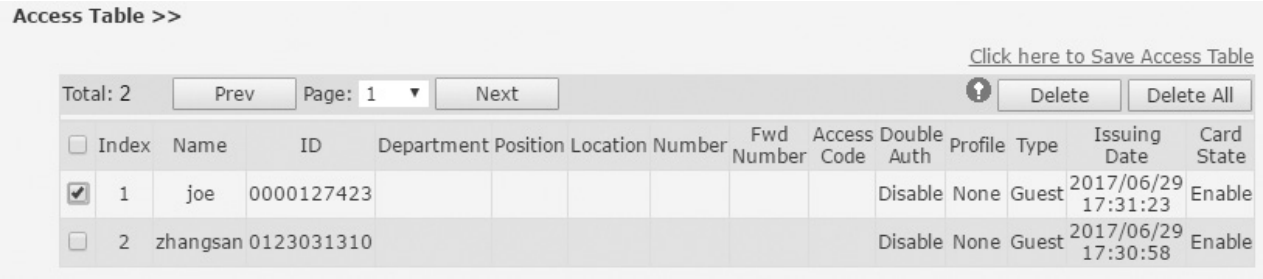


Method 2

Used to batch add cards for intermediates

Method 3

Use to batch delete cards or delete few cards



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

We make everyday life safer

Ambient System Sp. z o.o.
ul. Bysewska 27 | 80-298 Gdańsk | Poland
T: +48 58 345 51 95 | ambient@ambientsystem.eu