SIP Video Intercom i18S

USER MANUAL

V1.0

Wall mounting

Flush mounting

www.fanvil.com

Document VER	Firmware VER	Explanation	Time
V1.0	2.1.1.3390	Initial issue	20180208
V1.1	2.1.1.3445	Change some description	20180514

Safety Notices

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

Table of Content

A. Product introduction........6

1. Appearance of the product........6

2. Description........6

B. Start Using........7

1. Confirm the connection........7

1) Power port........7

2) Power, Security functions Input, Security functions Output port........7

3) Wiring instructions........7

2. Quick Setting........8

C. Basic operation........8

1. Answer a call........8

2. Call........9

3. End Call........9

D. Page settings........9

1. Browser configuration........9

2. Password Configuration........9

3. Configuration via WEB........10

(1) System........10

a) Information........10

b) Account........11

c) Configurations........12

d) Upgrade........12

e) Auto Provision........13

f) FDMS........13

g)Tools........16

(2) network........17

a) Basic........17

b) VPN........19

(3) Line........20

a) SIP........20

b) Basic Settings........25

(4) Intercom settings........26

a) Features........26

b) Audio........27

c) Video........29

d) MCAST........32

e) Action URL........35

f) Time/Date..36
(5) Security settings 37
(6) Function Key..39
E. Appendix..41
1. Technical parameters 41
2. Basic functions..42
3. Schematic diagram 42
4. The broadcast terminal configuration notice..43

A.Product introduction

i18S Voice Access is a digital network door phone. Its core part adopts mature VoIP solution (Broadcom chip), which can perform stably and reliably, it is hands-free, adopting digital full-duplex mode. The voice is loud and clear. It has a series of advantages, such as generous appearance, comfortable keypad and low power consumption, etc. i31S is easy to install. It is solid and durable.

1. Appearance of the product

Single button **Dual button**

2. Description

Picture	Description	Function
	DSS Key LED	Network error: Blink with 2s Network running: Off Registration failed: Blink with 6s Registration succeeded: On

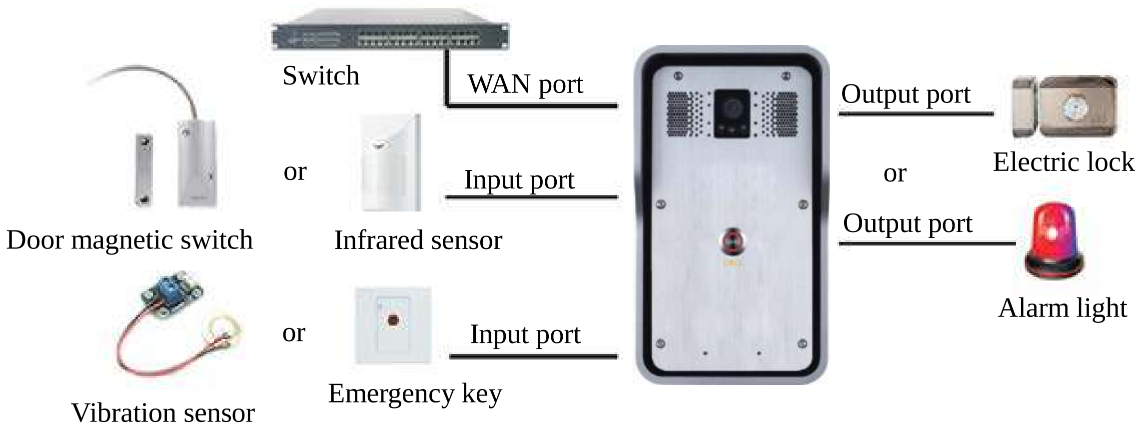
B.Start Using

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

1. Confirm the connection

Please confirm the power cord, network cable, electric lock control line connected and the boot-up is normal. (Check the network state of light)

1) Power port



2) Power, Security functions Input, Security functions Output port

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		Security functions Output port			Security functions Input port		

3) Wiring instructions

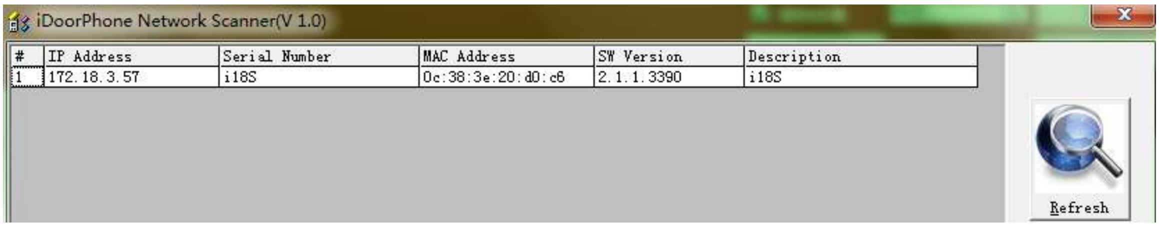
- NO: Normally Open Contact.
- COM: Common Contact.
- NC: Normally Close Contact.

2. Quick Setting

The product provides completed functions 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 let 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 complicated knowledge of SIP protocols.

In prior to this step, please make sure your broadband Internet online can work normally and complete the connection of the network hardware. The product default factory setting of network mode is STATIC IP. Before the entering of Web setting, pls connec the PC to the same LAN network with i18S or set the network segment of PC's Static IP address in the same segment of i18S.

- The default IP address is static IP address: 192.168.1.128. User can also use the software"iDoorPhoneNetworkScanner.exe" to find the IP address of the device. (download address http://download.fanvil.com/tool/iDoorPhoneNetworkScanner.exe)
- **Note:** Waiting for 30s to run the device when it is power on.
- Login to the WEB to configure the device
- Configure the service account, user name, server registered address and other parameters on the web page of SIP.
- Set DSS key in the Webpage (Intercom -> function key).
- Set function parameters in the Webpage (Safeguarding).



C.Basic operation

1. Answer a call

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

2. Call

Configure shortcut key as hot key then setup a number. The configured number will be called when user press the shortcut key.

3. End Call

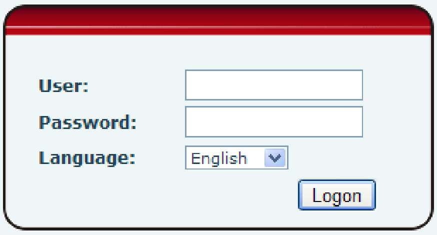
Enable the DSS key to hang up the call.

D.Page settings

1. Browser configuration

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

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



After configuring the equipment, remember to click SAVE under the Maintenance tab. If this is not done, the equipment will lose the modifications when it has been rebooted.

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

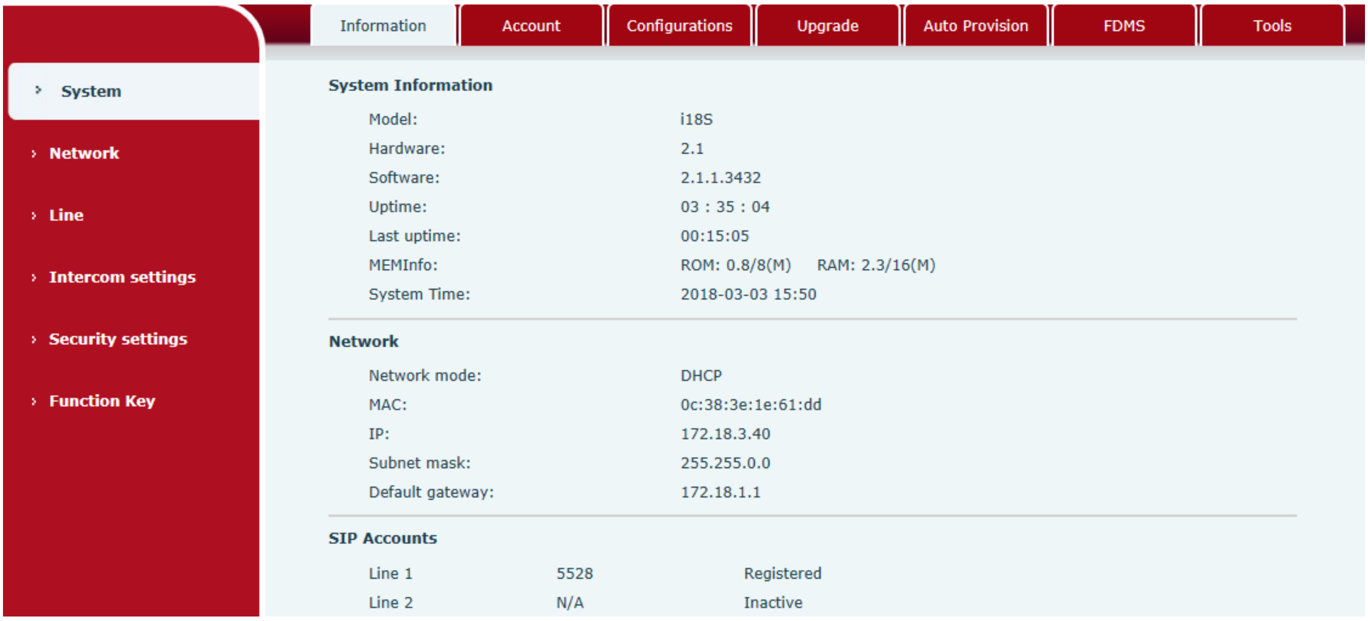
- Default user with general level:
  - Username: guest
  - Password: guest

- Default user with root level:
  - Username: admin
  - Password: admin

3. Configuration via WEB

(1) System

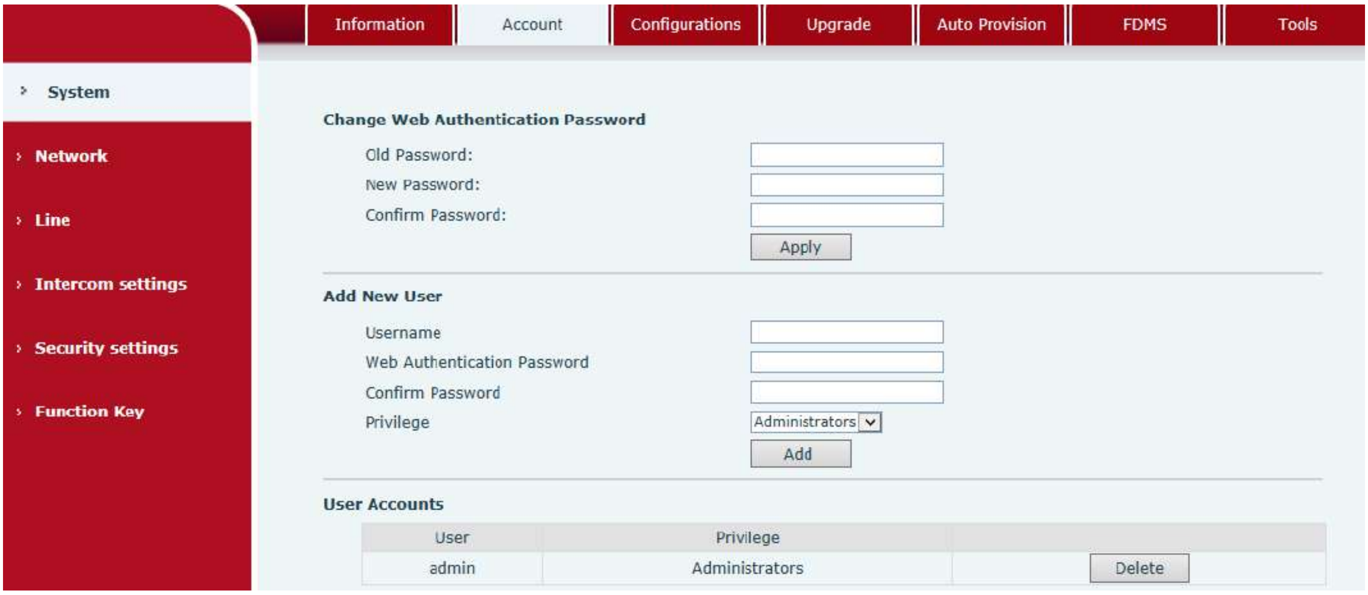
a) Information



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

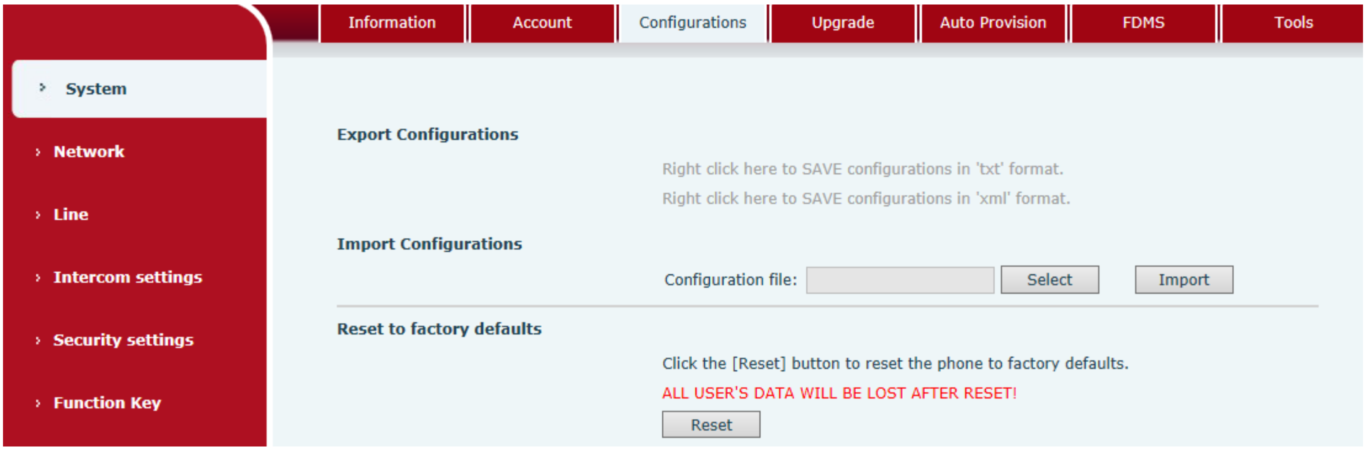
b) Account

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



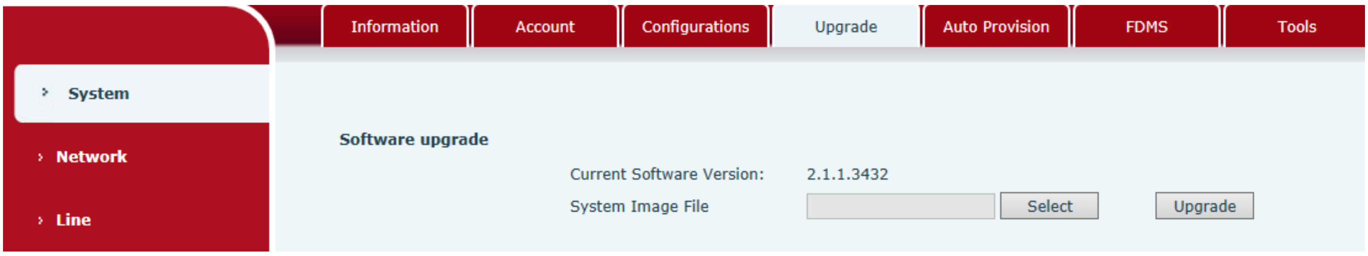
Account	
Field Name	**Explanation**
Change Web Authentication Password	
You Can modify the login password to the account	
Add New User	
You can add new user	
User Accounts	
Show the existing user information	

c) Configurations



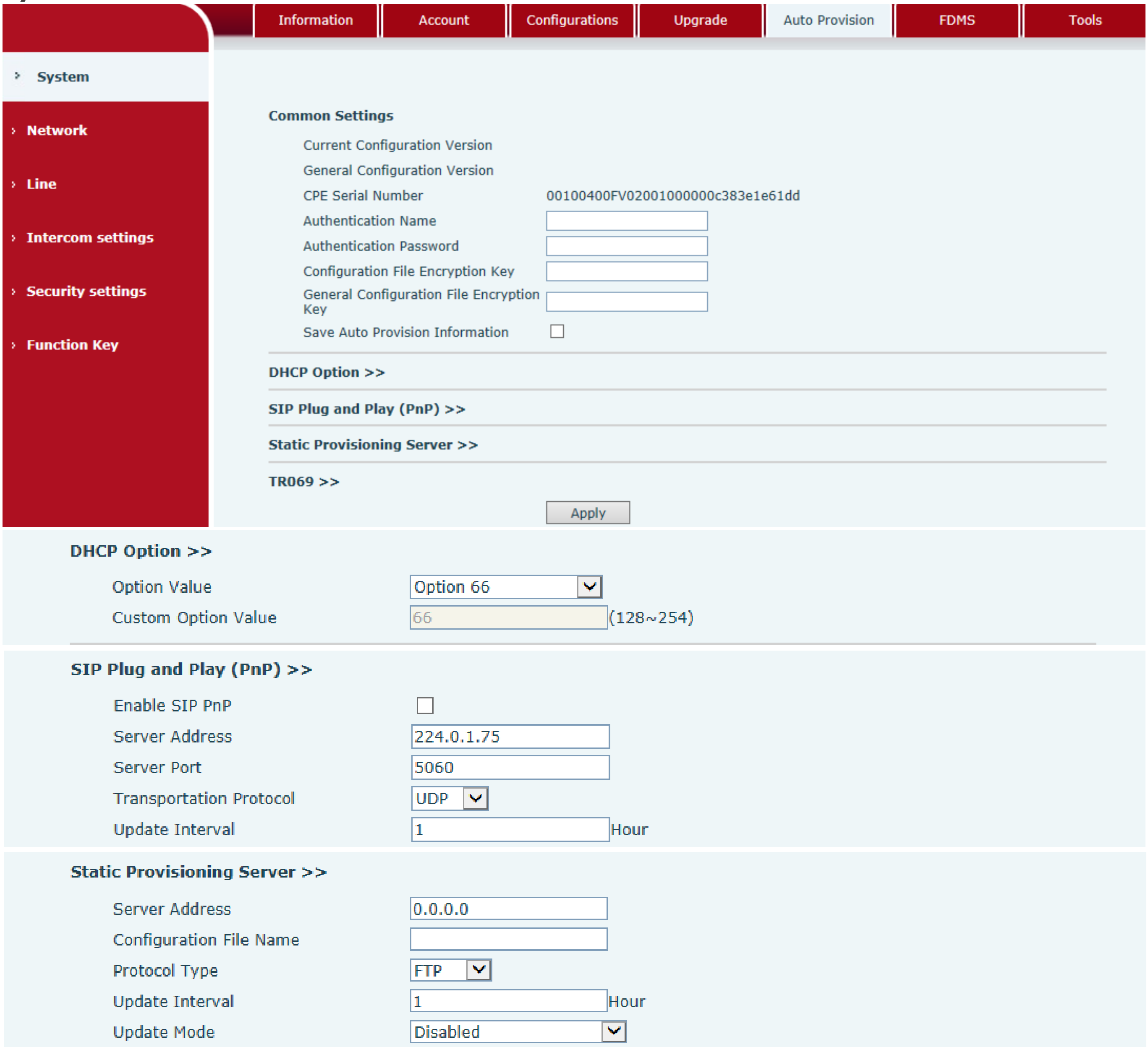
Configurations	
Field Name	**Explanation**
Export Configurations	Save the equipment configuration to a txt or xml file. Please Right click on the choice and then choose “Save Link As.”
Import Configurations	Browse to the config file, and press Update to load it to the equipment.
Reset to factory defaults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

d) Upgrade



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

e) Auto Provision

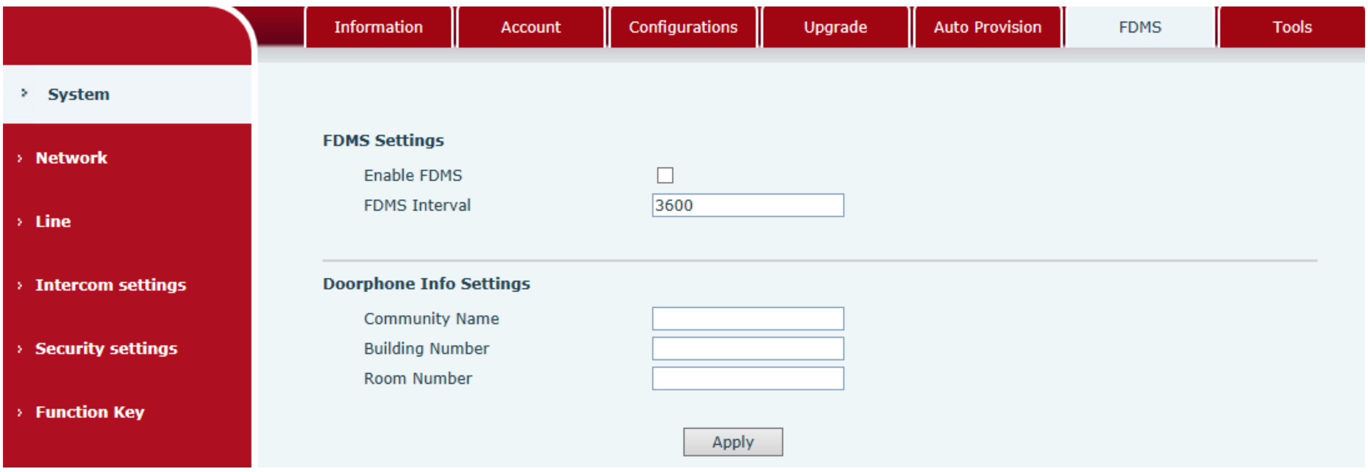


Auto Provision	
Field Name	**Explanation**
Common Settings	
Current Configuration Version	Show the current config file's version. If the version of configuration downloaded is higher than this, the configuration will be upgraded. If the endpoints confirm the configuration by the Digest method, the configuration 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 understand 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.

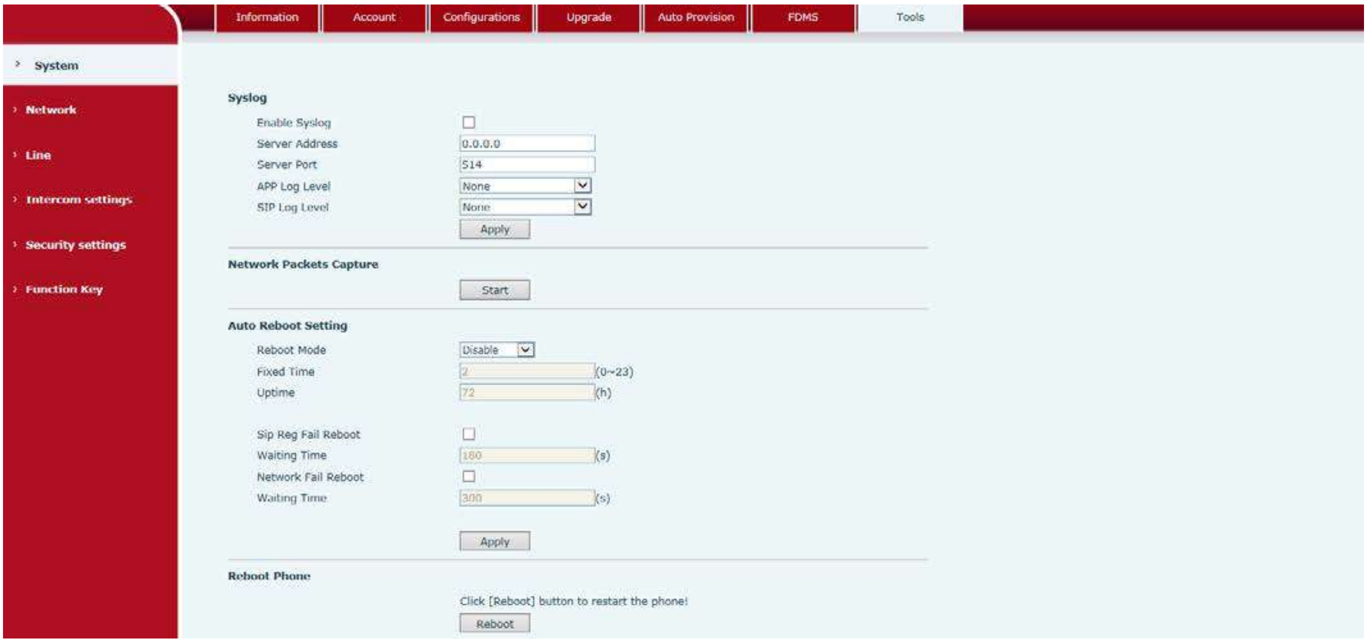
	3. Update at time interval – update at periodic update interval
TR069	
Enable TR069	Enable/Disable TR069 configuration
ACS Server Type	Select Common or CTC ACS Server Type.
ACS Server URL	ACS Server URL.
ACS User	User name for ACS.
ACS Password	ACS Password.
TR069 Auto Login	Enable/Disable TR069 Auto Login.
INFORM Sending Period	Time between transmissions of “Inform” is 3600 seconds.

f) FDMS



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

g) Tools



Syslog 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 work incorrectly.

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.

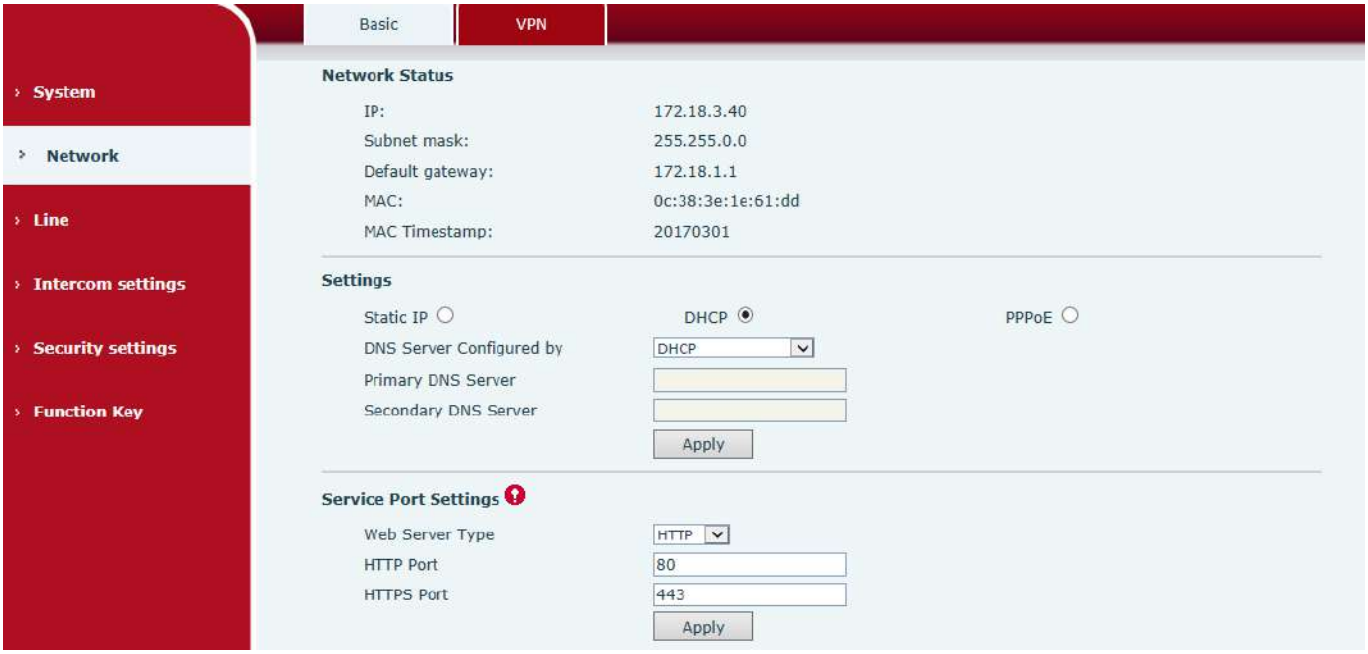
Level 7: debug; Debug messages normally used by system designer. This level can only be displayed via telnet.

Tools	
Field Name	**Explanation**
Syslog	
Enable	Enable or disable system log.

Syslog	
Server Address	System log server IP address.
Server Port	System log server port.
APP Log Level	Set the level of APP log.
SIP Log Level	Set the level of SIP log.
Network Packets Capture	
Capture a packet stream from the equipment. This is normally used to troubleshoot problems.	
Reboot Phone	
Some configuration modifications require a reboot to become effective. Clicking the Reboot button will lead to reboot immediately. Note: Be sure to save the configuration before rebooting.	

(2) network

a) Basic



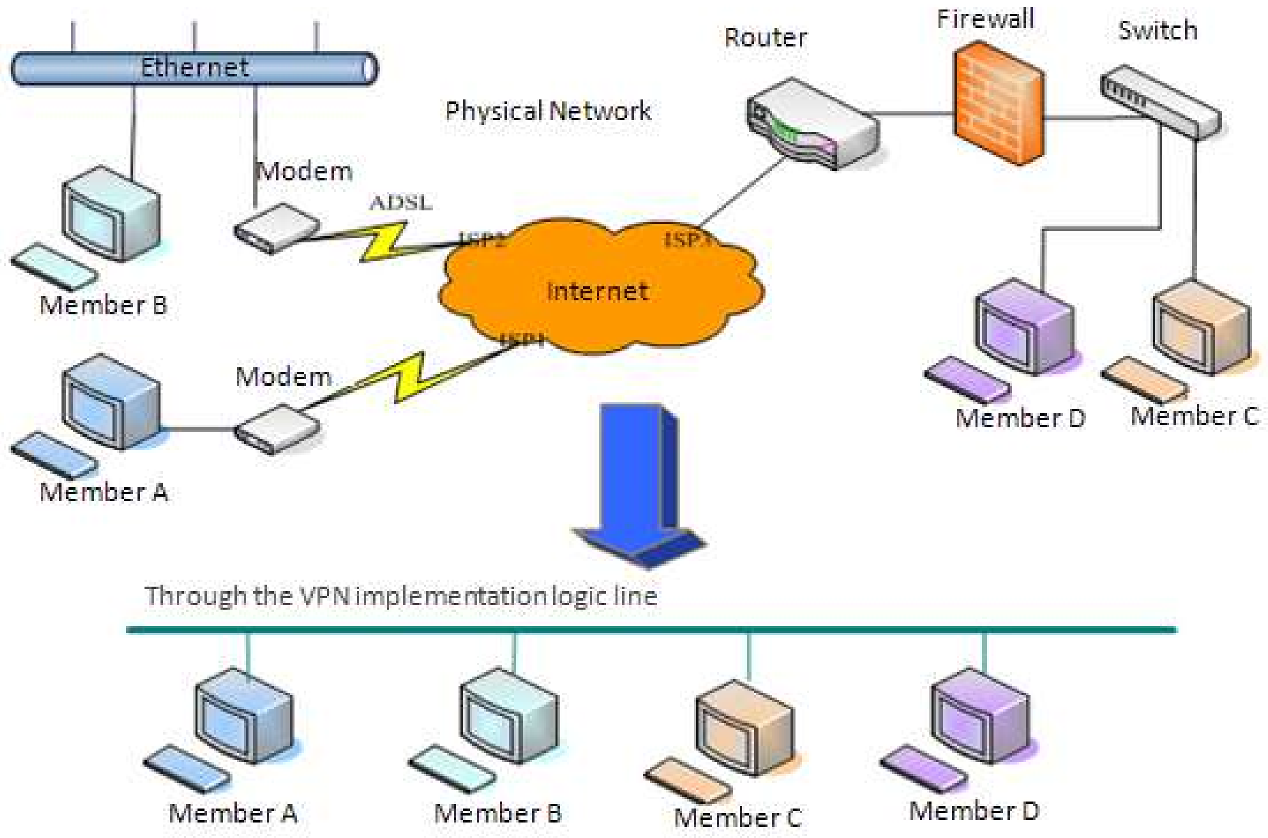
Field Name	Explanation
Network Status	
IP	The current IP address of the equipment

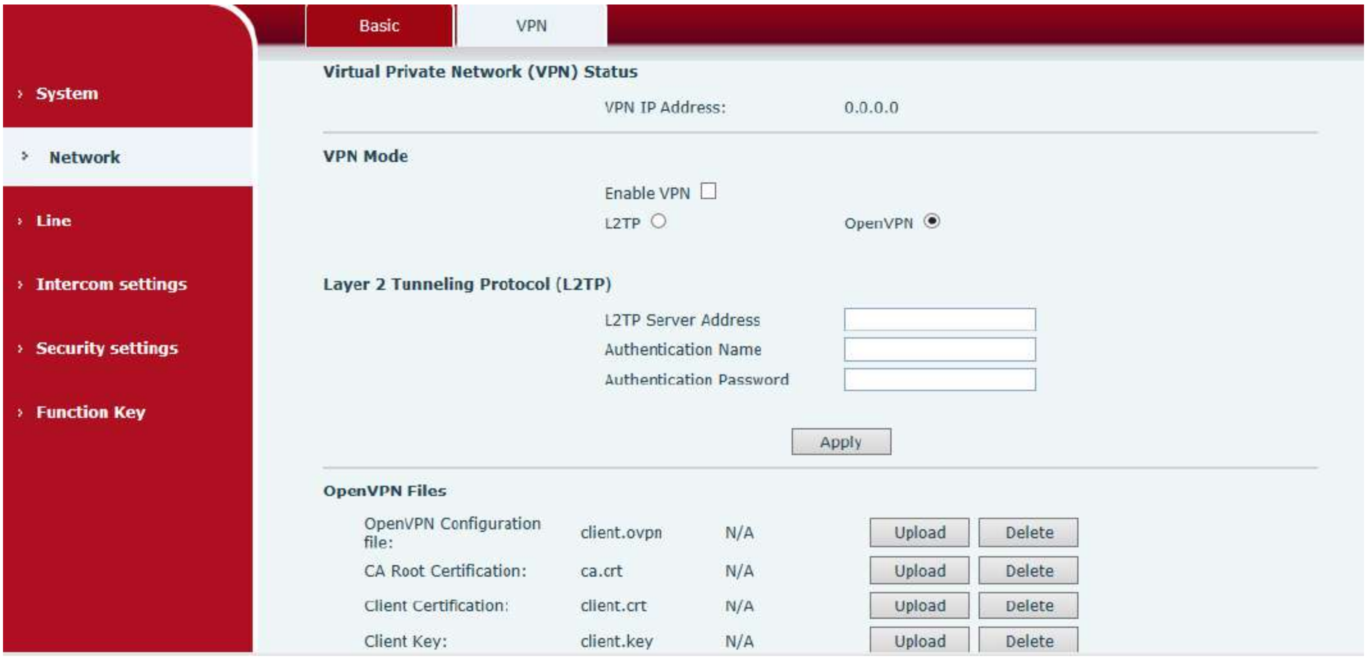
Subnet mask	The current Subnet Mask
Default gateway	The current Gateway IP address
MAC	The MAC address of the equipment
MAC Timestamp	Get the MAC address of time.
Settings	
Select the appropriate network mode. The equipment supports three network modes:	
Static IP	Network parameters must be entered manually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

3) If the HTTP port is set to 0, HTTP service will be disabled.

b) VPN

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



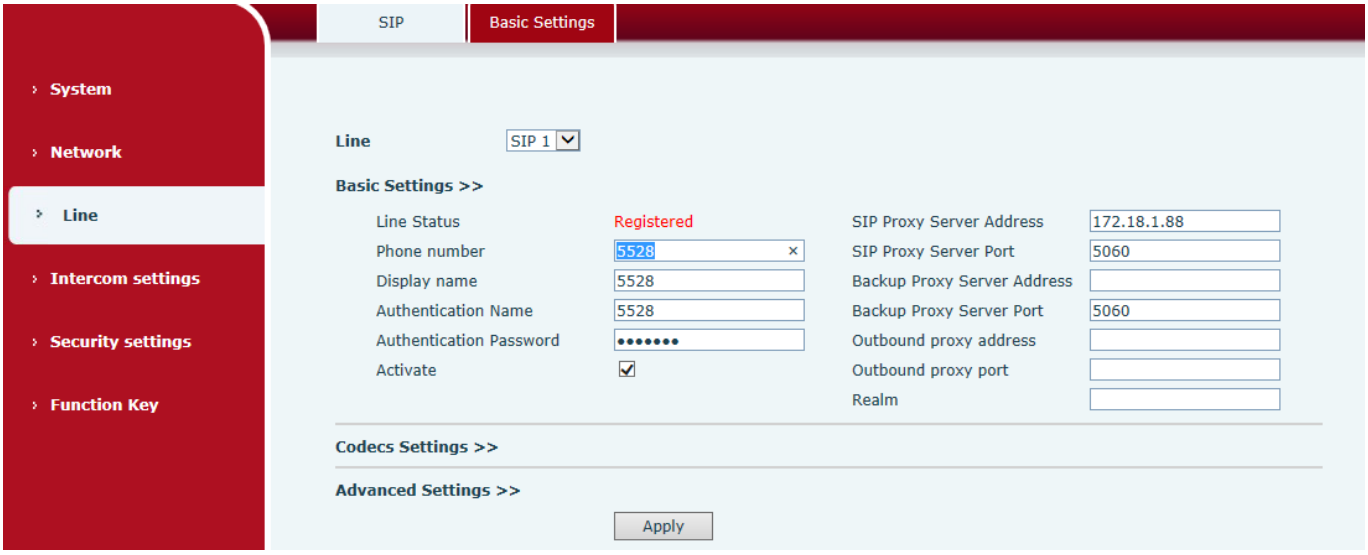


Field Name	Explanation
VPN IP Address	Shows the current VPN IP address.
VPN Mode	
Enable VPN	Enable/Disable VPN.
L2TP	Select Layer 2 Tunneling Protocol
OpenVPN	Select OpenVPN Protocol. (Only one protocol may be activated. After the selection is made, the configuration should be saved and the phone be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

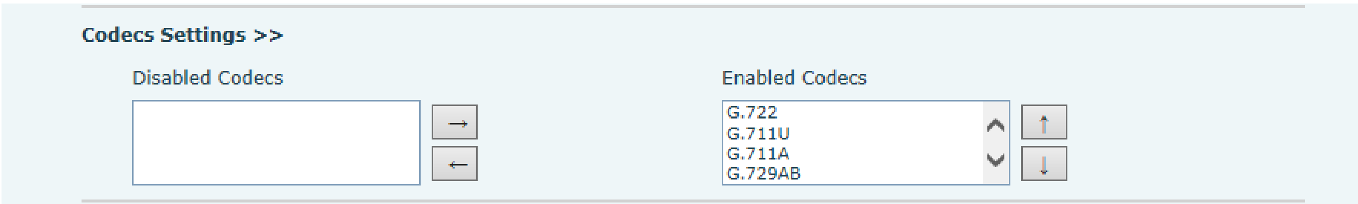
(3) Line

a) SIP

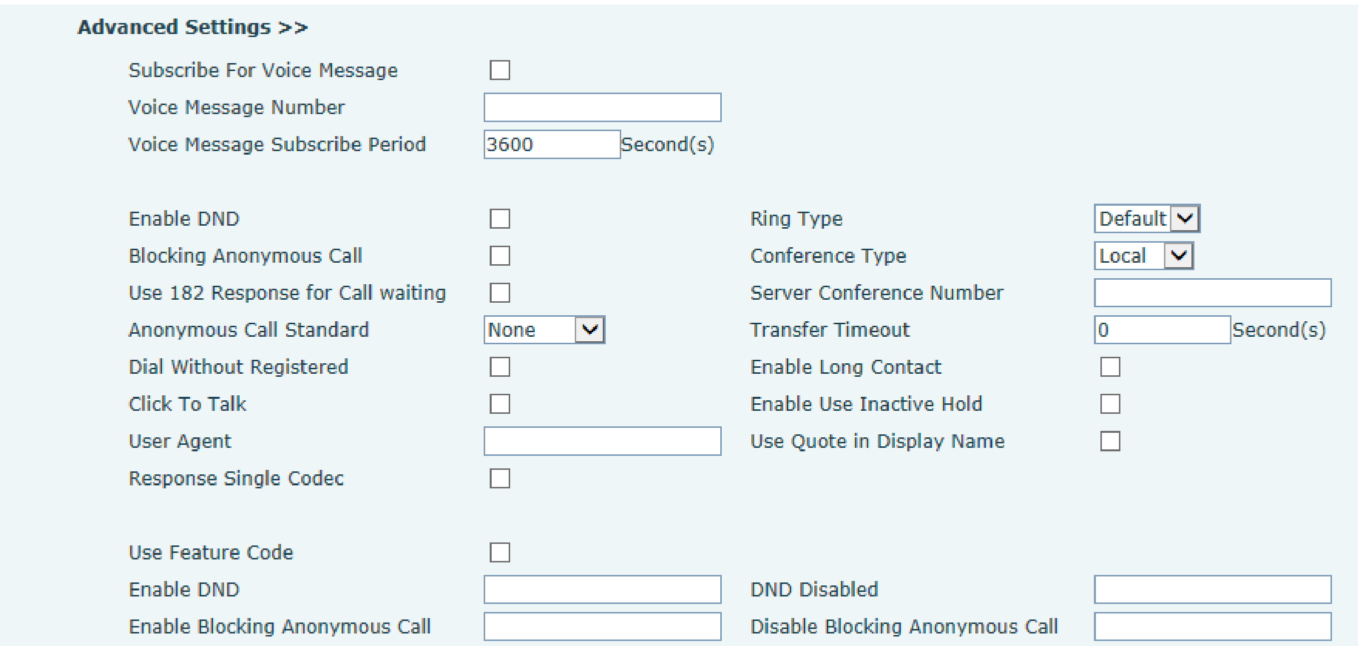
Configure a SIP server on this page.



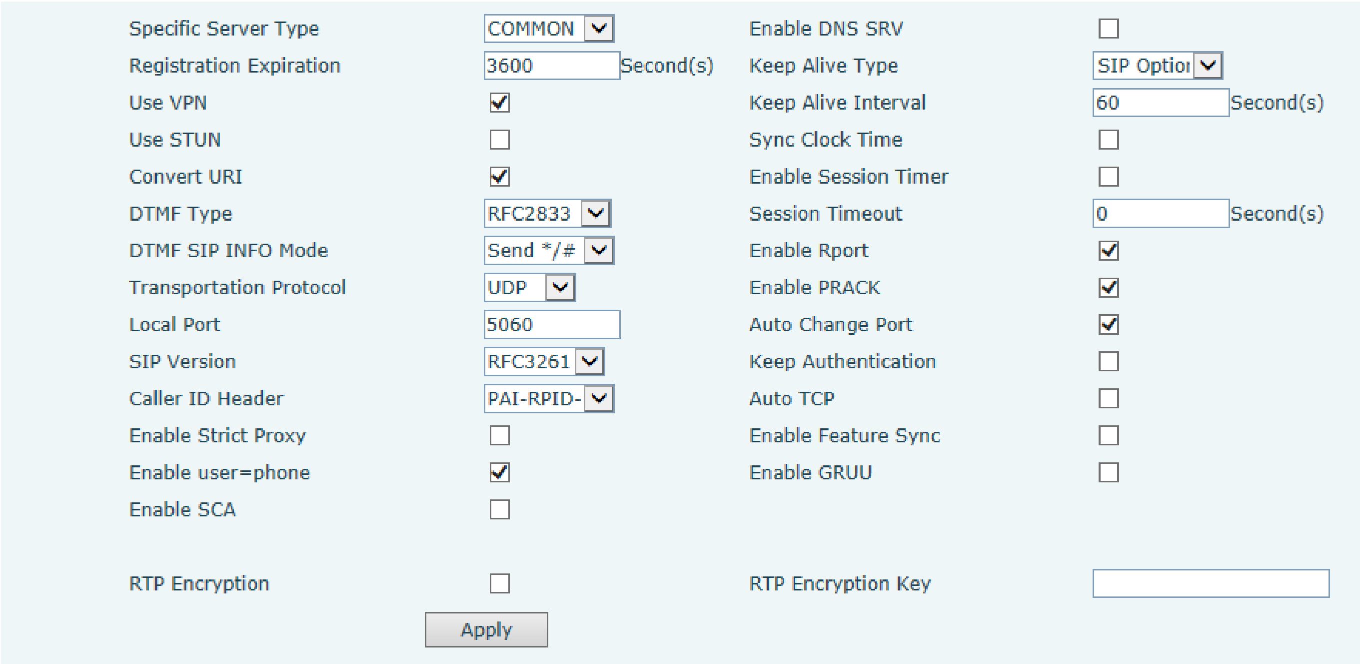
SIP
Basic Settings
System
Network
Line
Intercom settings
Security settings
Function Key
Line SIP 1
Basic Settings >>
Line Status Registered
Phone number 5528
Display name 5528
Authentication Name 5528
Authentication Password •••••••
Activate
SIP Proxy Server Address 172.18.1.88
SIP Proxy Server Port 5060
Backup Proxy Server Address
Backup Proxy Server Port 5060
Outbound proxy address
Outbound proxy port
Realm
Codecs Settings >>
Advanced Settings >>
Apply



Codecs Settings >>
Disabled Codecs
Enabled Codecs
G.722
G.711U
G.711A
G.729AB



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



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 are a few 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 are 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. 5) Other SIP error code, check SIP protocol standard, or contact support.
Username	Enter the username of the service account, assigned by IPPBX administrator, or provided by ISP provider.
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

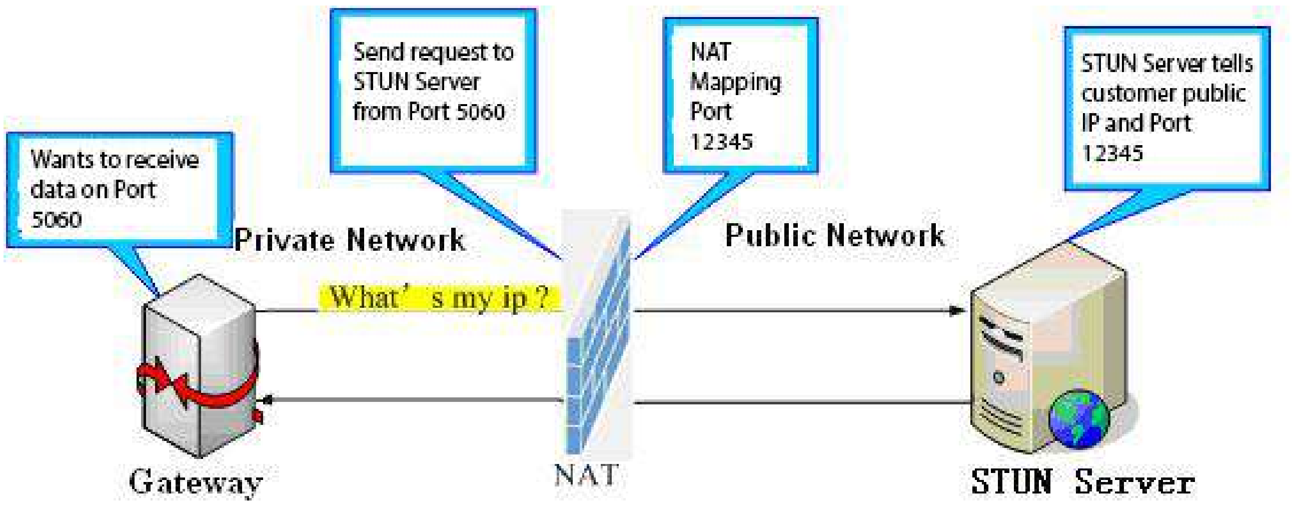
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server
SIP Proxy Server Port	Enter the SIP proxy server port, default is 5060
Outbound proxy address	Enter the IP or FQDN address of outbound proxy server provided by the service provider
Outbound proxy port	Enter the outbound proxy port, default is 5060
Realm	Enter the SIP domain if requested by the service provider
Codecs Settings	
Set the priority and availability of the codecs by adding or remove them from the list.	
Advanced Settings	
Subscribe For Voice Message	Enable the device to subscribe a voice message waiting notification, if enabled, the device will receive notification from the server if there is voice message waiting on the server
Voice Message Number	Set the number for retrieving voice message
Voice Message Subscribe Period	Set the interval of voice message notification subscription
Enable 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 enabled, the device will use single codec in response 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
Use Quote in Display	Whether to add quote in display name

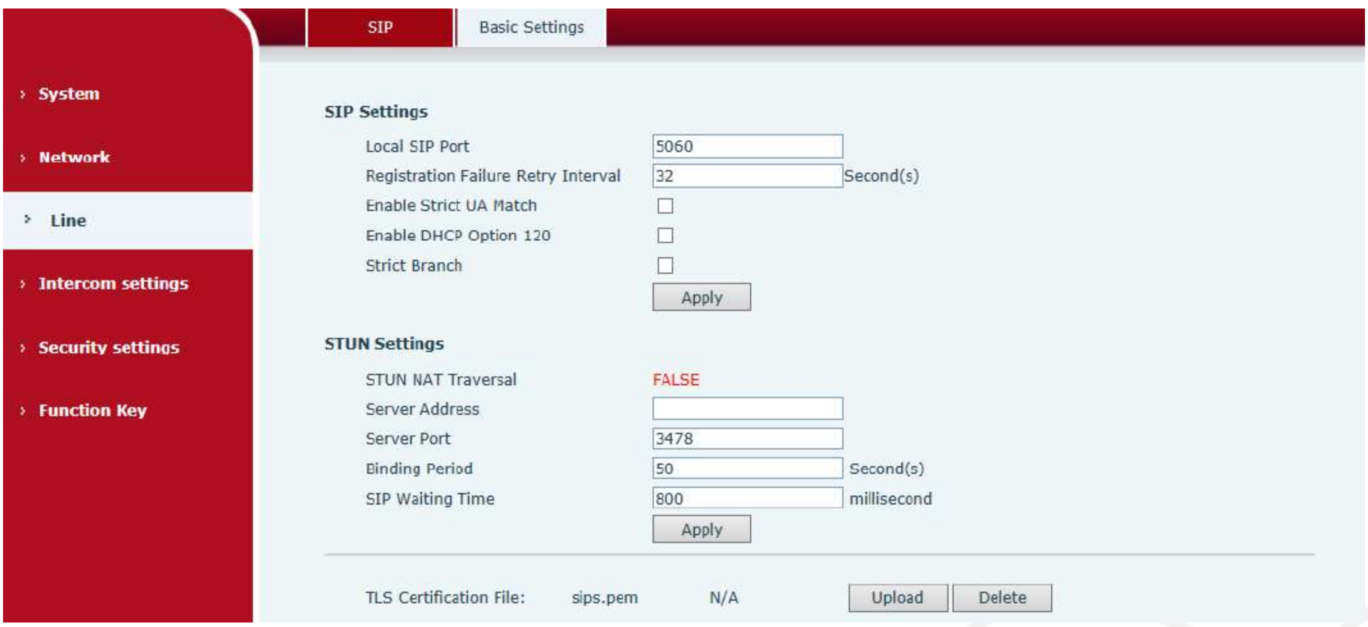
Name	
Use Feature Code	When this setting is enabled, the features in this section will not be handled by the device itself but by the server instead. In order to control the enabling of the features, the device will send feature code to the server by dialing the number specified in each feature code 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 BLF List	Enable/Disable BLF List
Enable DNS SRV	Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole opened
Keep Alive Interval	Set the keep alive packet transmitting interval
Enable Session Timer	Set the line to enable call ending by session timer refreshment. The call session will be ended if there is not new session timer event update received after the timeout period
Session Timeout	Set the session timer timeout period
Enable rport	Set the line to add rport in SIP headers
Enable PRACK	Set the line to support PRACK SIP message
Enable DNS SRV	Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list
Auto Change Port	Enable/Disable Auto Change Port
Keep Authentication	Keep the authentication parameters from previous authentication

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

b) Basic Settings

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



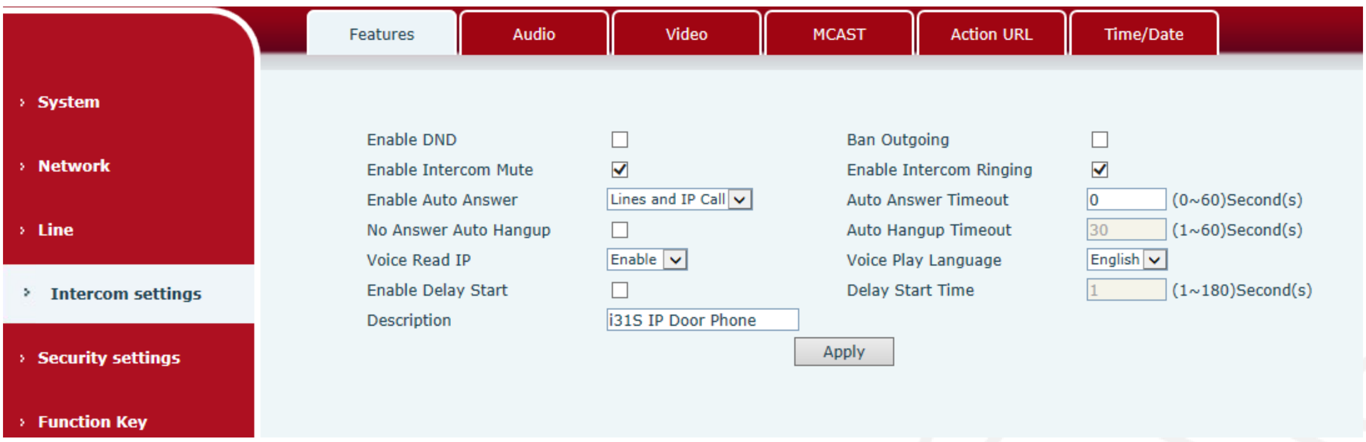


Basic Settings

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 working 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.	

(4) Intercom settings

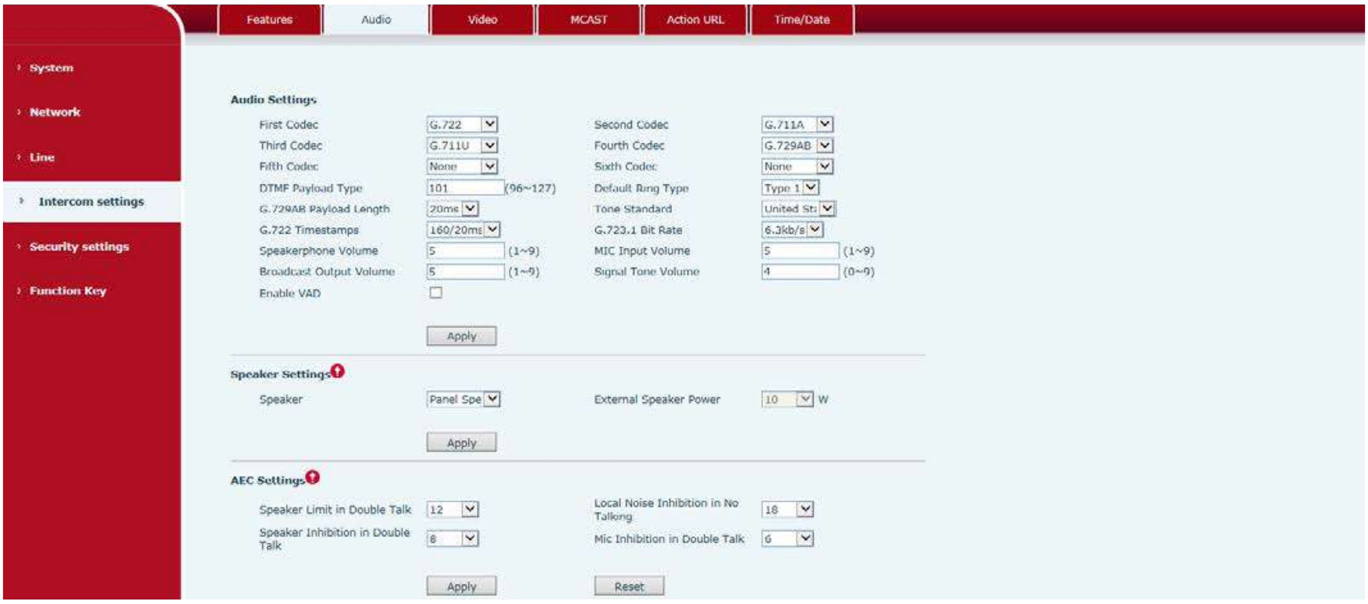
a) Features



Features	
Field Name	**Explanation**
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 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
Voice Read IP	Enable or disable voice broadcast IP address
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
Description	Device description displayed on IP scanning tool software. Initial Value is "i18S".

b) Audio

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

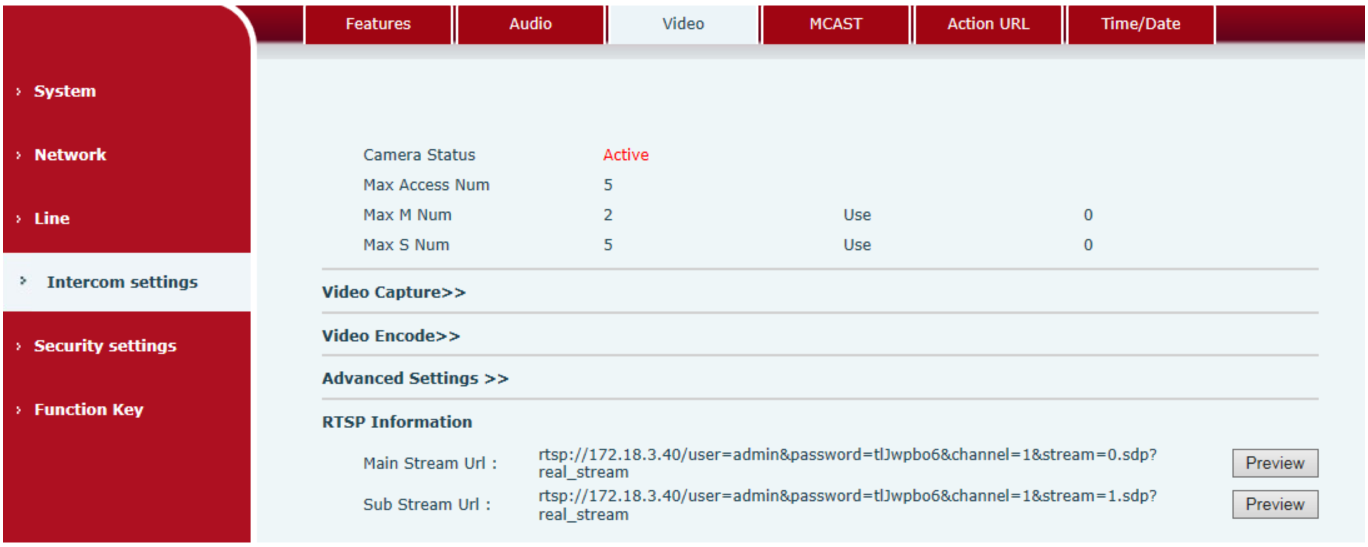


Audio Setting	
Field Name	**Explanation**
First Codec	The first codec choice: G.711A/u, G.722，G.723.1, G.729AB，G.726-32
Second Codec	The second codec choice: G.711A/u, G.722，G.723.1, G.729AB，G.726-32, None
Third Codec	The third codec choice: G.711A/u, G.722，G.723.1, G.729AB，G.726-32, None
Fourth Codec	The forth codec choice: G.711A/u, G.722，G.723.1, G.729AB，G.726-32, None
DTMF Payload Type	The RTP Payload type that indicates DTMF. Default is 101
Default Ring Type	Ring Sound – There are 9 standard types and 3 User types.
G.729AB Payload Length	G.729AB Payload Length – Adjusts from 10 – 60 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.
Speaker Settings	

These settings are only for the devices which support multiple output power. Be aware of that, the selected output power must be less than the real output power of the external speak, otherwise the external speak might be damaged.	
Speaker	The embedded speaker can be set to use static output power mode, and the external speak can be set as 10W, 20W, 30W output power. NOTE: this device support embedded speaker
External Speaker Power	Set the external speaker power, it must be lower than the real power of the external speaker, otherwise the external speaker might be damaged.
AEC Settings	
Speaker Limit in Double Talk	Limit maximum volume of the speaker while it's in the two-way conversation, the bigger the value, the loader the volume allowed.
Local Noise Inhibition in No Talking	While there's no talking on the conversation, the background noise will be inhibited, this value determined how much it's inhibited. The higher the value, the more background noise will be inhibited. It's not recommended to set it too big, because there will be more background noise while talking in the conversation.
Speaker Inhibition in Double Talk	Set the speaker inhibition while it's in the two-way conversation, the higher of the inhibition value, the smaller of the volume.
Mic Inhibition in Double Talk	Set the MIC inhibition while it's in the two-way conversation, the higher of the inhibition value, the smaller of the volume.

c) Video

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

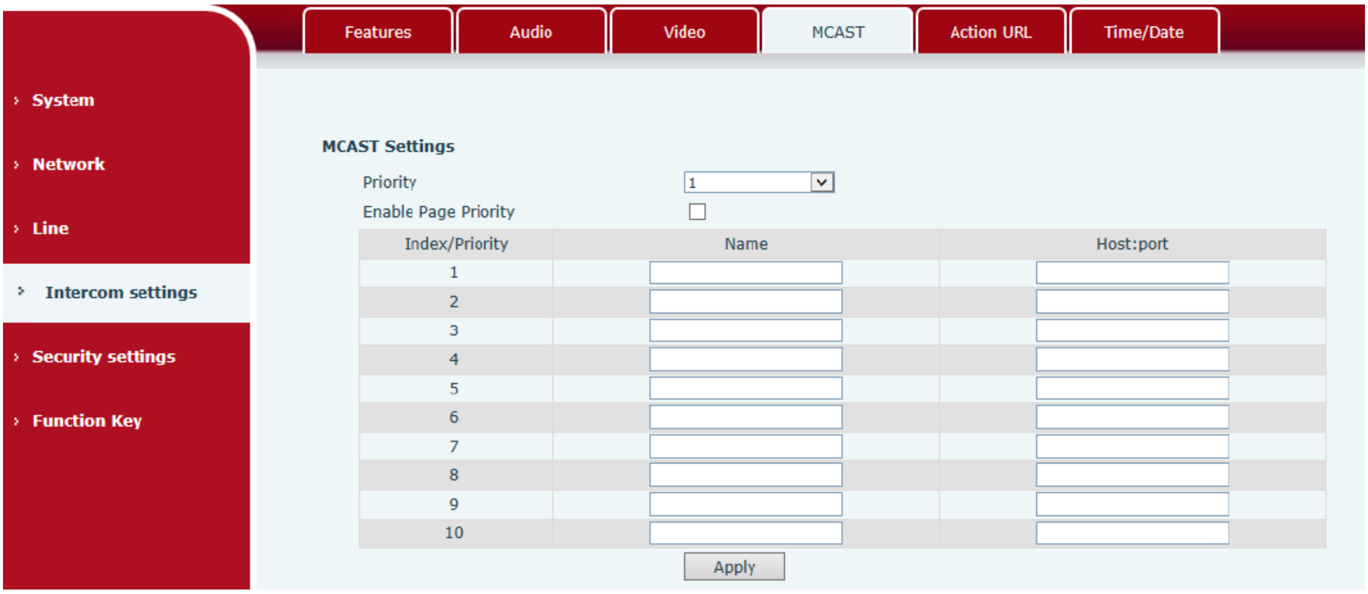


Video	
Field Name	**Explanation**
Camera Status: Display the relevant information of the camera, including maximum access, maximum stream, maximum sub stream, and the status.	
Video Capture	
IRCUT Mode	Auto: IRCUT switches according to the actual ambient light level of the camera Synchronization: The switching of the IRCUT is determined by the actual brightness of the IR lamp.

Day/Night Mode	Automatic: automatically switches according to the DNC Threshold and the brightness of the actual environment where the camera is located Day Mode: The camera's video screen is always colored, if there is IR-cut will be synchronized to switch. Night Mode: the camera's video screen is always black and white, if there is IR-cut will be synchronized switch.
White Balance	Automatic: Automatically adjusts according to the actual environment in which the camera is located. Outdoor: installed in the outdoor preferred. Indoor: installed in the room preferred.
Horizon Flip	The video is flipped horizontally
Anti Flicker	Enable the option. In a fluorescent environment can eliminate the video horizontal scroll
Vertical Flip	The video is flipped horizontally
IR Swap	IR-cut filter switch
DNC Threshold	In the Day / Night mode Auto option, the color switching black and white threshold is set
Backlight Compensation	In front of a very strong background light can see people or objects clearly
AutoFill Sensitivity	In the environment changes in light and shade, the higher the sensitivity the faster the video changes
wide Dynamic	Set wide dynamic
Wide Dynamic Upper Limit	Change the brightness of the background image, the higher the brighter.
Fill Light	Enable or disable Fill Light
Video Encode	
Encode Format	Only H.264 encoding format is supported
Resolution	Main stream: support 720P Sub-stream: you can select CIF (352 * 288), D1 (720 * 576)
Frame Rate	The larger the value is, the more coherent the video would be got; not recommend adjusted.
Bitrate Control	CBR: If the code rate (bandwidth) is insufficient, it is preferred. VBR: Image quality is preferred, not recommended.
Quality	Video quality adjustment, the better the quality needs to transfer faster
Bit rate	It is proportional to video file size, not recommend adjusted.
I Frame Interval	The greater the value is, the worse the video quality would be, otherwise the better video quality would be; not recommend adjusted.
Activate	When you selected it, the stream is enabled, otherwise disabled
Encode Static config	

Select the video codec type, it's recommended to use "Base Line" to stay the same as the video output or stream receiver.	
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	
Main Stream Url	Access the main address of RTSP
Sub Stream Url	Access the child address of RTSP

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, 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 address, used to receive the multicast RTP stream sent by the multicast address.

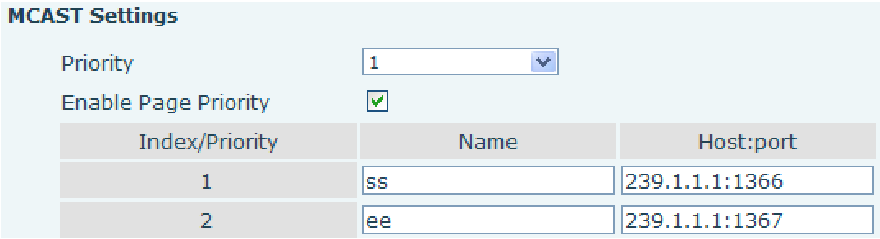
Here are the ways to change equipment receiving multicast RTP stream processing mode in the Web interface: set the ordinary priority and enable page priority.

- 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 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 stream
  - ✧ Enable the page priority:

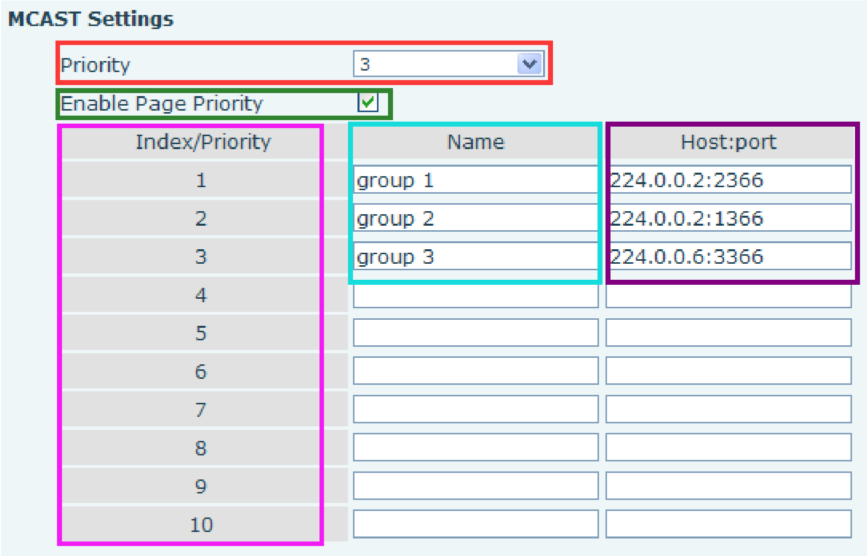
    Page priority determines the device how to deal with the new receiving multicast RTP stream when it is in multicast session currently. When Page priority switch is enabled, the device will automatically ignore the low priority multicast RTP stream but receive top-level priority multicast RTP stream and keep the current multicast session in state; If it is not enabled, the device will automatically ignore all receiving multicast RTP streams.
- 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 the names of the monitoring multicast which you set. 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 higher priority. The followings will explain how to use this option:

✧ The purpose of setting monitoring multicast "Group 1" or "Group 2" or "Group 3" is able to launch a multicast call.

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

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

✧ When you set the Priority to a value, only higher than the priority of multicast can get access. If you set the Priority is 3, group 2 and group 3 for priority level equal to 3 or less than 3 were rejected, 1 priority is 2 higher than ordinary call priority. Device can answer the multicast message and hold the other call at the same time

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

✧ User can set whether to open more priority to be is the priority of multicast, Multicast is the pink part number. Explain how to use:

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

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

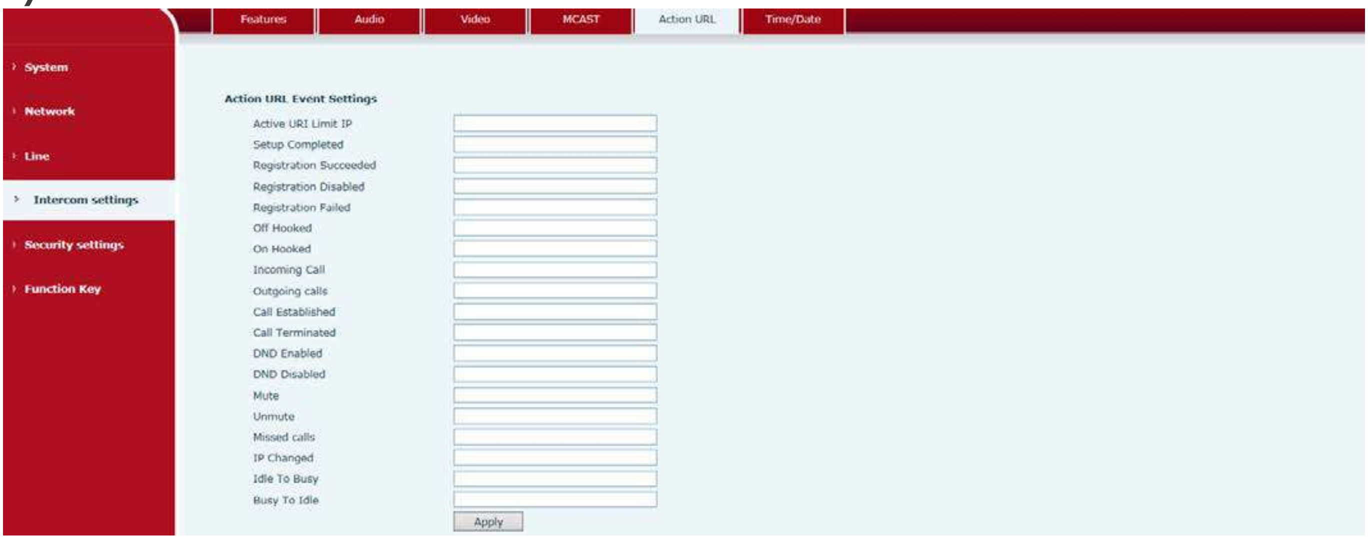
✧ If multicast is a new "group of 1", then the call will come in. Because "the priority group 1" is 2, higher than the current call "priority group 2" 3

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

Multicast service

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

e) Action URL

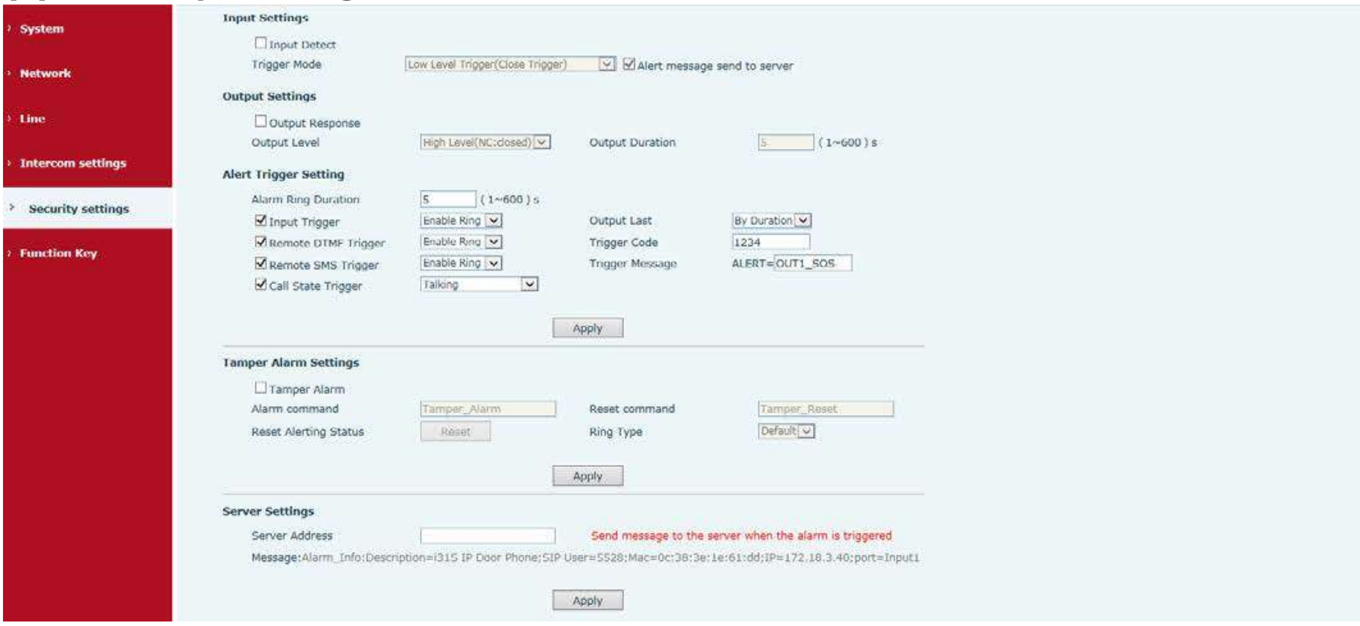


Action URL Settings
URL for various actions is performed by the phone. These actions are recorded and sent as xml files to the server. Sample format is http://InternalServer /FileName.xml

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 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.	

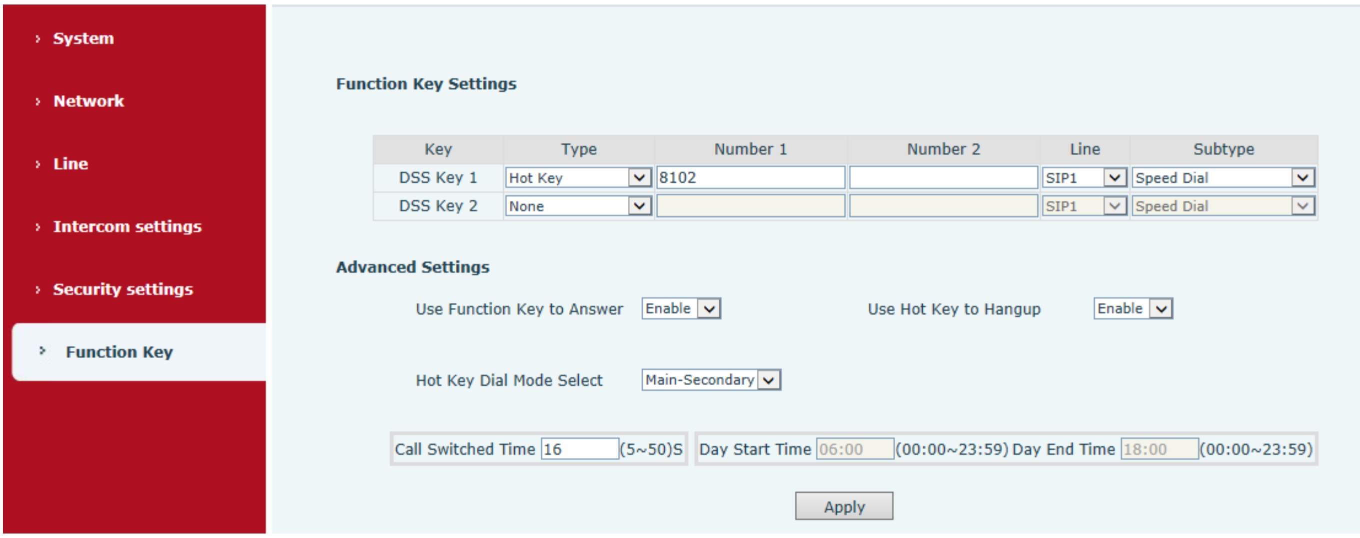
(5) Security settings



Security settings	
Field Name	**Explanation**
Input settings	
Input Detect	Enable input detection
Trigger Mode	Low Level Trigger(Close Trigger),Double short circuit detection port(If it is single port, is the low level)Detection to trigger when closed
	High Level Trigger(Disconnect Trigger),Double short circuit detection port(If it is single port, is the high level)Detection to trigger when disconnect.
Alert message send to server	When meet the input port to trigger condition, to the server sends the alarm information correspondence.
Output Settings	
Output Response	Enable output port detection
Output Level	Low Level(NO: always on)When meet the trigger condition, trigger the NO port disconnected.
	High Level(NC: always off)When meet the trigger condition, trigger the NC port close.
Output Duration	Define the output Duration change of output port.（1~600S）
Alert Trigger Setting	
Alarm Ring Duration	Define the output Duration change of output port.（1~600S）
Input Trigger	When the input port meet to trigger condition, the output port will be triggered

Remote DTMF Trigger	By Duration： Received the terminal equipment to send the DTMF password, if correct, which triggers the corresponding output port (The Port level time change, By < Output Duration> control)
	By Calling State： During the call, receive the terminal equipment to send the DTMF password, if correct, which triggers the corresponding output port (The Port level time change, by call state control, after the end of the call, port to return the default state)
Remote SMS Trigger	In the remote device or server to send instructions to ALERT=[instructions], if correct, which triggers the corresponding output port
Call State Trigger	The port output continuous time synchronization and trigger state changes, including the trigger conditions: 1, call; 2, call and singing; 3, singing; three models. (for example: the call trigger output port, will be in conversation state continued to output the corresponding level)
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
Server Settings	
Server Address	Configure remote response server address (including remote response server address and tamper alarm server address)

(6) Function Key



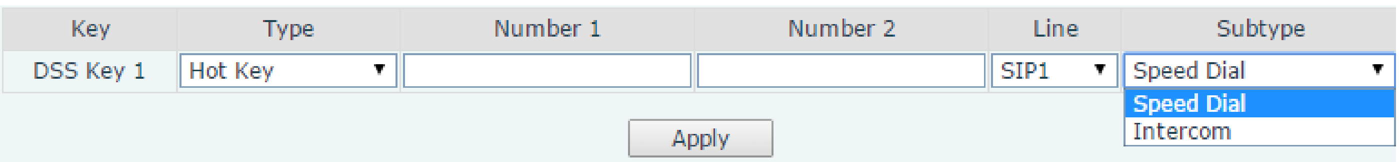
➢ Key Event

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 make a IP call directly.



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.

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 in initiated multicast communication, the device would not be able to launch a new multicast call.

E. Appendix

1. Technical parameters

Communication protocol		SIP 2.0(RFC-3261)
Main chipset		Broadcom
Key	**DSS key materials**	Stainless steel
	DSS Key	1 or 2
Speech flow	**Audio amplifier**	3W
	Volume control	Adjustable
	Full duplex speakerphone	Support (AEC)
	DTMF TYPE	In-band, Out-of-band(RFC 2833), SIP INFO
	wideband speech code	G.722
	Narrowband speech code	G711A/u, G.723.1, G.729AB, ILBC, AMR
Port	**Security linkage**	1 embedded short circuit input interface
		1 embedded short circuit output interface
	WAN	10/100BASE-TX s Auto-MDIX, RJ-45
Camera		1/3 "color CMOS, wide angle
Power supply mode		12V / 1A DC or PoE
Cables		CAT5 or better
Shell Material		Cast aluminium panel, Cast aluminium back shell
Working temperature		-40°C to 70°C
Working humidity		10% - 90%
Storage temperature		-40°C to 70°C
Installation way		Wall-mounting or Flush-mounting
Dimension		Wall-mounting: 223*130*74mm Flush-mounting: 270*150*61mm

2. Basic functions

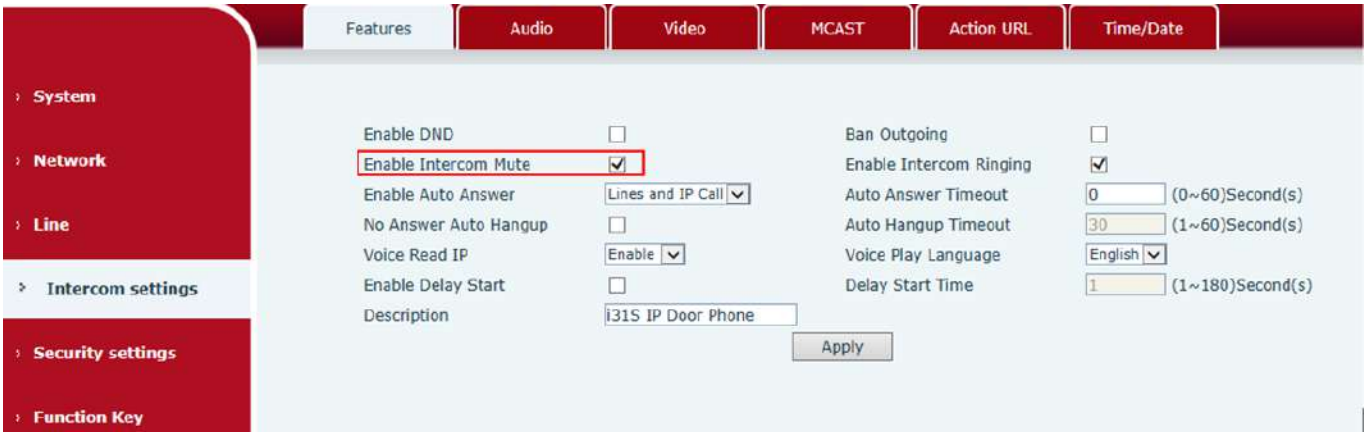
- 2 SIP Lines
- PoE Enabled
- Full-duplex speakerphone (HF)
- Intelligent DSS Keys (Speed Dial/intercom etc.)
- Wall-mounting / Flush-mounting
- Special integrated noise reduction module
- Dual microphone Omnidirectional voice pickup
- 1 embedded short circuit input interface
- 1 embedded short circuit output interface. Support 4 controlled events: remote DTMF; remote server's commands; interact with short circuit input; talking status
- Anti-tamper switch
- Record voice and video during calls (Optional)
- All in ONE: Radio and intercom, intelligent security function
- Industrial standard certifications: IP65，IK10，CE/FCC

3. Schematic diagram

4. The broadcast terminal configuration notice

✧ How to avoid an incoherency sound when the broadcast playing?

When the terminal used as broadcast, the speaker is loud. If do not set mute for microphone, the AEC (echo cancellation) of equipment will be activated, which leads the sound incoherence. In order to avoid such circumstance, when the equipment turn to use as a radio should be set as intercom mode. Then activate the intercom mute, so as to ensure the broadcast quality.



✧ How to improve broadcasting tone quality?

In order to obtain better broadcast quality, recommend the use of the HD (G.722) mode for broadcast.

Voice bandwidth will be by the narrow width (G.711) of 4 KHz, which is extended to broadband (G.722)7 KHz. When combined with the active speaker, the effect will be better.