



SIP Intercom Module

ICO module 01

EN

User Manual



ver. 02.2021

Table of Contents

1. Safety	4
2. Installation Guide	7
2.1 Use POE or external Power Adapter	7
2.2 Install	7
2.2.1 Button instruction	7
2.2.2 Confirm the connection	9
2.3 Appendix Table	10
2.3.1 Common command mode	10
2.3.2 Function key LED state	10
3. Basic Introduction	11
3.1 WEB configuration	11
3.2 SIP Configurations	11
4. Basic Function	12
4.1 Making Calls	12
4.2 Answering Calls	12
4.3 End of the Call	13
4.4 Auto-Answering	14
4.5 DND	15
4.6 Call Waiting	16
5. Advance Function	17
5.1 Intercom	17
5.2 MCAST	18
5.3 Hotspot	19
6. Web Configurations	21
6.1 Web Page Authentication	21
6.2 System >> Information	21
6.3 System >> Account	22
6.4 System >> Configurations	22
6.5 System >> Upgrade	23
6.6 System >> Auto Provision	23
6.7 System >> FDMS	26
6.8 System >> Tools	27
6.9 Network >> Basic	28
6.10 Network >> Advanced	30
6.11 Network >> VPN	32
6.12 Network >> Web Filter	33

6.13	Line >> SIP	34
6.14	Line >> Basic Settings	37
6.15	Line >> SIP Hotspot	38
6.16	Intercom settings >> Blacklist	39
6.17	Intercom settings >> Features	39
6.18	Intercom Setting >> Audio	41
6.19	Intercom Setting >> Video	42
6.20	Intercom Setting >> MCAST	44
6.21	Intercom Setting >> action URL	45
6.22	Intercom Setting >> Time/Date	46
6.23	Intercom Setting >> Trusted Certificates	47
6.24	Intercom Setting >> Device Certificates	48
6.25	Security Settings	49
6.26	Function Key >> Function Key Settings	51
6.26.1	Key Event	51
6.26.2	Hot Key	52
6.26.3	Multicast	53
6.26.4	PTT	54
6.26.5	Advanced Settings	55
7.	Trouble Shooting	56
7.1	Get device system information	56
7.2	Reboot device	56
7.3	Device factory reset	56
7.4	Network Packets Capture	56
7.5	Common Trouble Cases	57

List of tables

Table 1.	Button instruction	10
Table 2.	Common command mode	12
Table 3.	Function key LED state	12
Table 4.	Intercom	19
Table 5.	MCAST	20
Table 6.	SIP Hotspot	21
Table 7.	Auto provision	26
Table 8.	FDMS	28
Table 9.	Auto provision	30
Table 10.	Network Setting	33
Table 11.	SIP	36
Table 12.	Line Basic Setting	40
Table 13.	Common device function Settings on the web page	42
Table 14.	Voice Settings on web pages	43
Table 15.	Video Setting	45
Table 16.	MCAST parameters	46
Table 17.	Action URL	47
Table 18.	Time/Date	48
Table 19.	Alert/Security Settings	51
Table 20.	Function Key Settings	53
Table 21.	Hot Key Settings	54
Table 22.	Multicast Settings	55
Table 23.	Advanced Settings	57
Table 25.	Common Trouble Cases	59

List of drawings

Picture 1.	Button instruction	9
Picture 2.	Connected graphs	11
Picture 3.	WEB Login	13
Picture 4.	SIP Line Configuration	13
Picture 5.	Function Setting	14
Picture 6.	Function Setting	15
Picture 7.	Enable Auto Answer	16
Picture 8.	Set DND Option	17
Picture 9.	Enable DND	17

Picture 10.	Set DND Option	18
Picture 11.	WEB Intercom	19
Picture 12.	MCAST	20
Picture 13.	SIP Hotspot	22
Picture 14.	WEB Account	24
Picture 15.	System Setting	24
Picture 16.	Upgrade	25
Picture 17.	Auto provision	25
Picture 18.	FDMS	28
Picture 19.	Tools	29
Picture 20.	Network Basic Setting	30
Picture 21.	Network Setting	32
Picture 22.	VPN	34
Picture 23.	WEB Filter Table	35
Picture 24.	SIP	36
Picture 25.	Network Basic	39
Picture 26.	Line Basic Setting	39
Picture 27.	SIP Hotspot	40
Picture 28.	Blacklist	41
Picture 29.	Feature	41
Picture 30.	Audio	43
Picture 31.	Video Setting	44
Picture 32.	MCAST	46
Picture 33.	Action URL	47
Picture 34.	Time/Date	48
Picture 35.	Trusted Certificates	49
Picture 36.	Device Certificates	50
Picture 37.	Alert/Security Settings	51
Picture 38.	Function Key Settings	53
Picture 39.	Hot Key Settings	54
Picture 40.	Multicast Settings	55
Picture 41.	PTT Settings	56
Picture 42.	Advanced Settings	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 not 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. Installation Guide

2.1 Use POE or external Power Adapter

Intercom, called as 'the device' hereafter, supports two power supply modes, power supply from external power adapter or over Ethernet (POE) complied switch.

POE power supply saves the space and cost of providing the device additional power outlet. With a POE switch, the device can be powered through a single Ethernet cable which is also used for data transmission. By attaching UPS system to POE switch, the device can keep working at power outage just like traditional PSTN telephone which is powered by the telephone line.

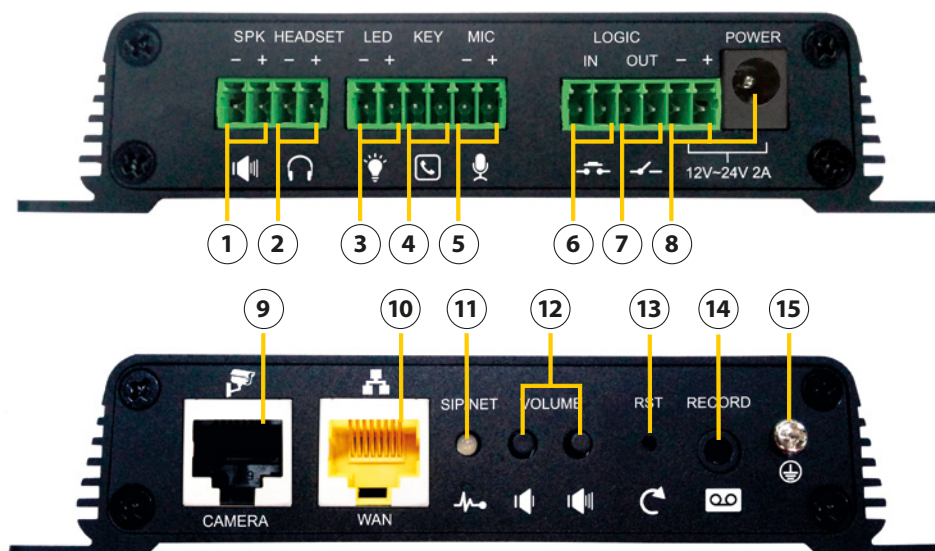
For users who do not have POE equipment, the traditional power adaptor should be used. If the device is connected to both PoE switch and external power adapter, intercom will get power supply from PoE switch in priority, and change to external power adapter once the PoE power supply fails.

Please use the power adapter supplied by Ambient System and the POE switch met the specifications to ensure the device work properly.

2.2 Install

Before you start using the device, please install the following.

2.2.1 Button instruction



Picture 1. Button instruction

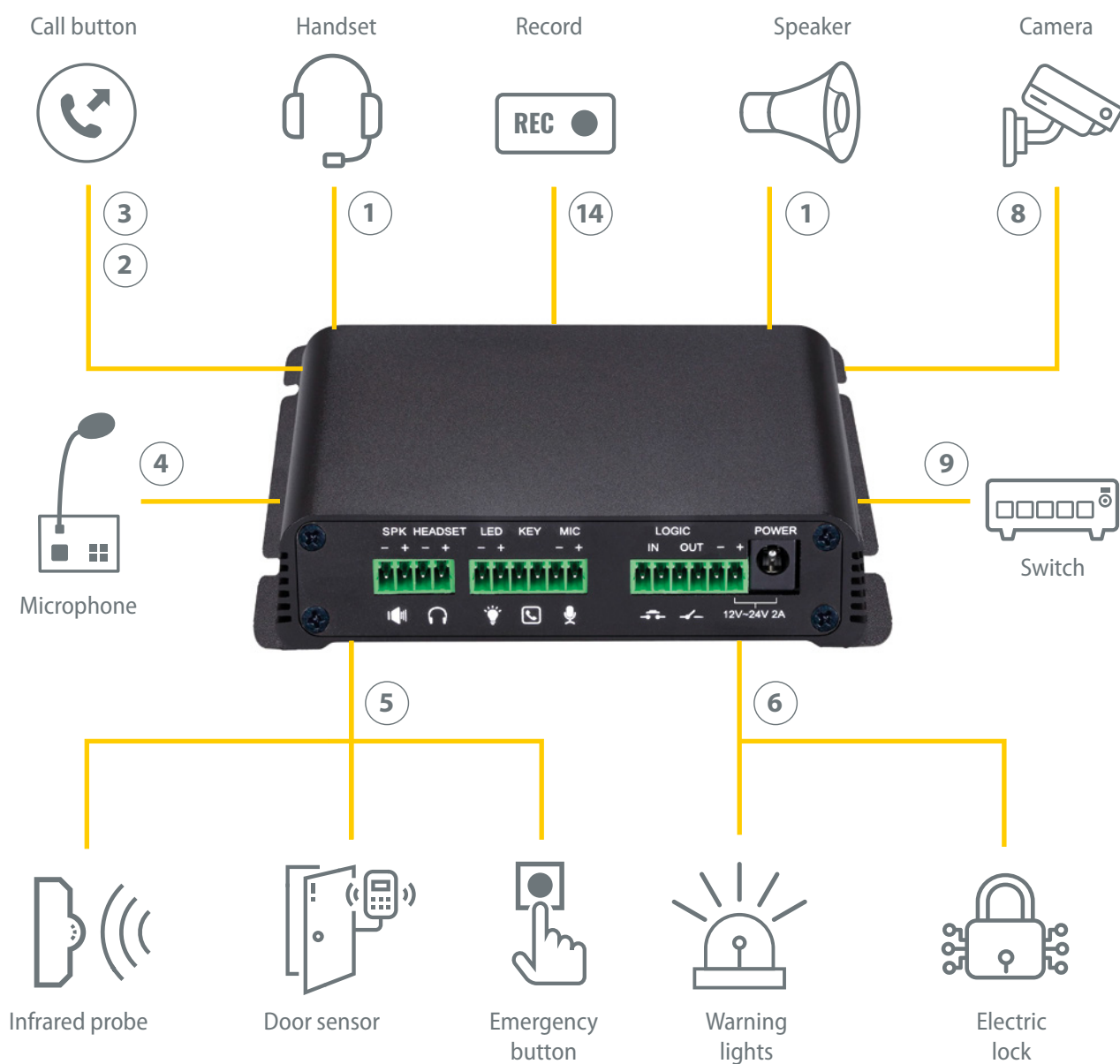
The image above shows the key layout of the device. Each button provides its own specific function. The user can refer to the instructions for the keys in the illustration in this section to operate the device.

Table 1. Button instruction

Label	Explanation
1 Speaker interface	According to the device input voltage adaptive output maximum power; 4 Ω speaker, POE / 10 W, 12 V / 10 W, 18 V / 20 W, 24 V / 30 W. The greater the horn impedance, the smaller the output power. Suggested wire diameter: 18 AWG or larger diameter.
2 Headset interface	Speaker audio line signal output impedance 32 Ohm, single ended output voltage 1.2 V, used for external headphones or active speakers
3 LED interface	Output 5 V voltage 5 mA current, can be an external LED, indicating the network status, call status, registration status.
4 Function key interface	Connection switch, you can log on page set the call number or IP address.
5 Microphone interface	Recommend the use of 2.2K Ohm impedance electret condenser microphone, sensitivity: -38 dB, bias voltage 2.2 V. Microphone signal cable it is recommended to use a shielded cable and do not connect the shield cable to the grounding screw, improve anti-interference.
6 Switch input interface	Connect an infrared probe or emergency switch or Doorsensor and other switch components.
7 Switch output interface	Corresponding to the short-circuit input interface, login device security page settings, you can control the alarm light, electric locks and other equipment; with the adjacent 8 power port connection for external equipment power supply.
8 Power input interface	12 V ~ 24 V 2 A input, according to the input voltage to determine the maximum output power amplifier.
9 Camera interface	Standard RJ45 interface, connect the original camera, the proposed use of five or five sub-network cable.
10 Ethernet interface	WAN port, standard RJ45 interface, 10 / 100M adaptive, support POE input, it is recommended to use five or super five network cable.
11 Registration/Network LED	Indicates network status, call status, registration status. Fast flashing: network anomaly or SIP account exception. Slow flashing: during a call. Always bright: successful registration.
12 Volume control key	When device is idle, the button is used to adjust the volume of ringtone, when the device is in call, the button is used to adjust call volume and when device is having broadcast, the button is used to adjust broadcast volume.
13 Restore factory key	Press and hold for 3 seconds to flash the device to restart and restore the factory settings.
14 Recording output interface	The local microphone voice and call voice mixed output, suitable for computer and other equipment recording.
15 Grounding screw	When intercom external part is connected to metal shell or panel, please connect the external part to this interface, in order to prevent static electricity or other interferences which may affect the device's normal working.

2.2.2 Confirm the connection

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



Picture 2. Connected graphs

2.3 Appendix Table

2.3.1 Common command mode

Table 2. Common command mode

Action	Description
Standby to IP	Wait for captain to press volume down button 3s to report IP.
Switching network mode	In standby mode, long press the volume button for 10 seconds, and there will be a beep sound and the indicator light will flash for 5 seconds. Within 5 seconds, press the volume up button for three times continuously to switch the network mode. Network status is static or PPPoE mode will be switched to DHCP mode; When the network is DHCP mode, it will be switched to static IP 192.168.1.128, and IP will be reported after successful switch.

2.3.2 Function key LED state

Table 3. Function key LED state

Type	LED	State
Line/network	Quick flashing	Registration failed/ network abnormal
	Normally on	Successfully registered
	Slow flashing	In call

3. Basic Introduction

3.1 WEB 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.



Picture 3. WEB Login

The username and password should be correct to log in to the web page. **The default username and password are "admin".** For the specific details of the operation of the web page, please refer to section 6 – [Web Configurations](#).

3.2 SIP Configurations

At least one SIP line should be configured properly to enable the telephony service. The line configuration is like a virtualized SIM card. Just like a SIM card on a mobile phone, it stores the service provider and the account information used for registration and authentication. When the device is applied with the configuration, it will register the device to the service provider with the server's address and user's authentication as stored in the configurations.

The SIP line configuration should be set via the WEB configuration page by entering the correct information such as phone number, authentication name/password, SIP server address, server port, etc. which are provided by the SIP server administrator.

- » **WEB interface:** After login into the phone page, enter **[Line]** >> **[SIP]** and select **SIP1/SIP2** for configuration, click apply to complete registration after configuration, as shown below:



Picture 4. SIP Line Configuration

4. Basic Function

4.1 Making Calls

After setting the function key to Hot key and setting the number, press the function key to immediately call out the set number, as shown below:

Function Key Settings

☐ Input port Multiplexing as DSS Key2

Key	Type	Number 1	Number 2	Line	Subtype
DSS Key 1	Hot Key	125		SIP1	Speed Dial
DSS Key 2	None			SIP1	Speed Dial

Advanced Settings

Use Function Key to Answer ☐ Enable

Enable Speed Dial Hangup ☐ Enable

Hot Key Dial Mode Select ☐ Day-Night

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

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

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

Apply

Picture 5. Function Setting

See detailed configuration instructions – [9.26 Function Key](#)

4.2 Answering Calls

After setting up the automatic answer and setting up the automatic answer time, it will hear the ringing bell within the set time and automatically answer the call after timeout. Cancel automatic answering. When a call comes in, you will hear the ringing bell and will not answer the phone over time.

4.3 End of the Call

Function Key Settings

☐ Input port Multiplexing as DSS Key2

Key	Type	Number 1	Number 2	Line	Subtype
DSS Key 1	Key Event			SIP1	Release
DSS Key 2	None			SIP1	Speed Dial

Advanced Settings

 Use Function Key to Answer

 Enable Speed Dial Hangup

 Hot Key Dial Mode Select

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

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

Picture 6. Function Setting

You can hang up the call through the Release key (you can set the function key as the Release key) or turn on the speed dial button to hang up the call. See detailed configuration instructions [9.26 Function Key](#).

4.4 Auto-Answering

The user can turn off the auto-answer function (enabled by default) on the device webpage, and the ring tone will be heard after the shutdown, and the auto-answer will not time out.

» **Web interface:** enter [Intercom Settings] >> [Features], Enable auto answer, set mode and auto answer time and click submit.

System

Network

Line

Intercom settings

Security settings

Function Key

Features

Audio

Video

MCAST

Action URL

Time/Date

Trusted Certificates

Device Certificates

Limit Talk Duration

Disable

DND Mode

Phone

Enable Call Waiting

☒

Enable Intercom

☒

Enable Intercom Mute

☒

Enable Auto Dial Out

☒

Enable Auto Answer

Lines and IP Call

No Answer Auto Hangup

☐

Dial Fixed Length to Send

☒

Voice Read IP

Enable

Description

IP Intercom Pho

Enable Headset

☒

Talk Duration

120

(20~600) Second(s)

Ban Outgoing

☐

Enable Call Waiting Tone

☒

Enable Intercom Barge

☒

Enable Intercom Ringing

☒

Auto Dial Out Time

5

(3~30)Second(s)

Auto Answer Timeout

0

(0~60)Second(s)

Auto Hangup Timeout

30

(1~60)Second(s)

Send length

4

System Language

English

Enable DND

☐

Apply

Picture 7. Enable Auto Answer

» **Auto Answer mode:**

- › Disable: Turn off the automatic answer function, the device has a call, ring, will not time out to answer automatically.
- › Line1: Line 1 has an automatic call timeout.
- › Line2: Line 2 has an automatic call timeout.
- › Line1 and Line2: Line 1 and line 2 have an automatic call timeout.
- › Lines and IP Call: Line and IP direct dial call timeout automatically answer.

» **Auto Answer Timeout (0~60)**

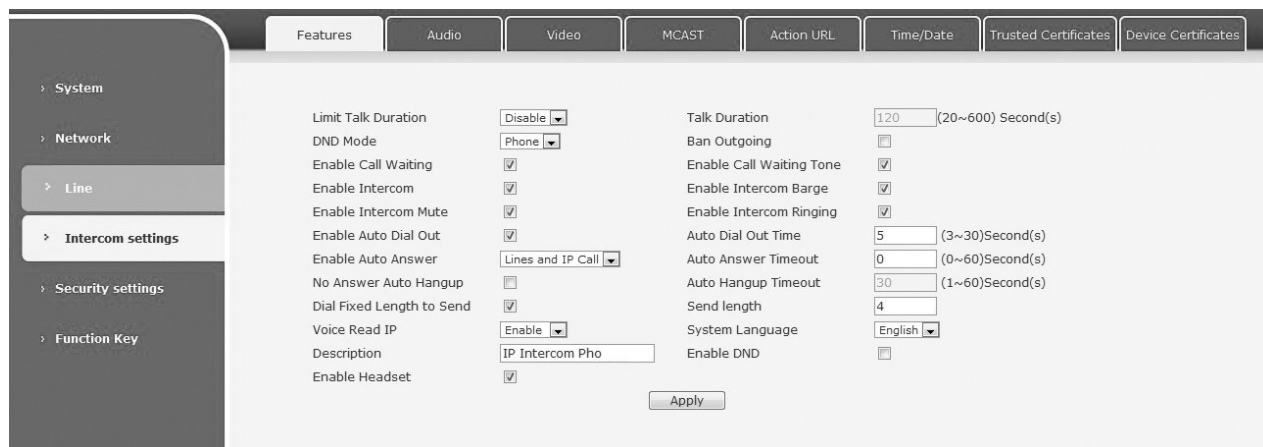
The range can be set to 0~60s, and the call will be answered automatically when the timeout is set.

4.5 DND

Users can turn on the do-not-disturb (DND) feature on the device's web page to reject incoming calls (including call waiting). Do not disturb can be set by the SIP line respectively on/off.

Turn on/off all lines of the device without interruption by the following methods:

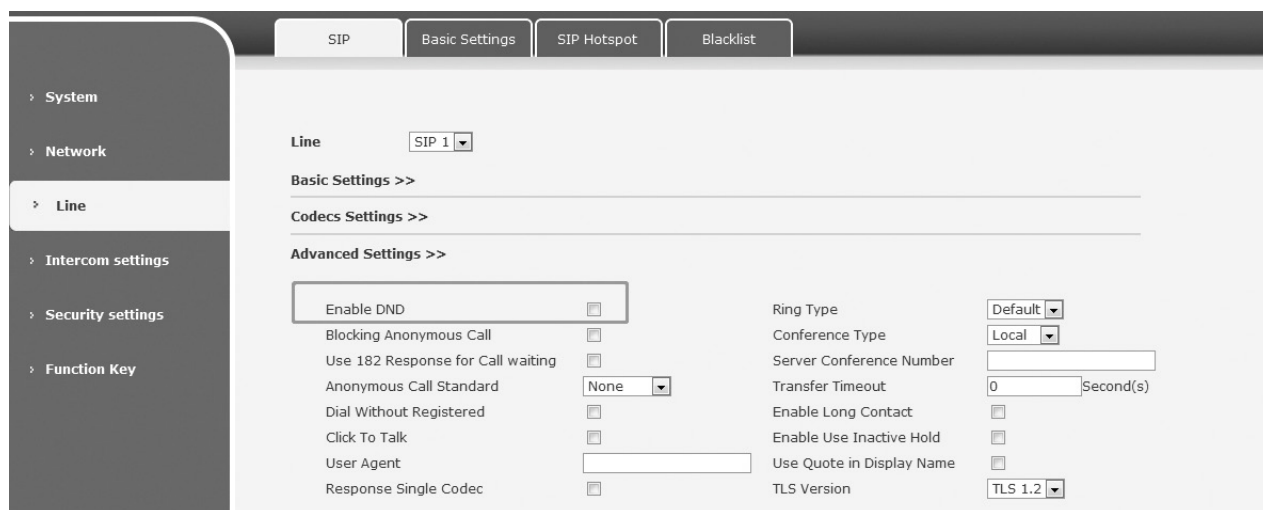
- » **Web interface:** enter [Intercom Settings] >> [Features], set the DND Mode to phone and Enable DND.



Picture 8. Set DND Option

Turn on/off the interruption free method for the specific line of the device, as follows:

- » **Web interface:** enter [Line] >> [SIP], choose a Line and enter [Line] >> [Advanced settings], Enable DND.



Picture 9. Enable DND

4.6 Call Waiting

- » Enable call waiting: new calls can be accepted during a call.
- » Disable call waiting: new calls will be automatically rejected and a busy signal will be prompted
- » Enable call waiting tone: when you receive a new call on the line, the device will beep. Users can enable/disable call waiting in the device interface and the web interface.
- » Web interface: enter **[Intercom Settings]** >> **[Features]**, enable/disable call waiting, enable/disable call waiting tone.

The screenshot displays the web interface of the SIP Intercom Module, specifically the 'Features' configuration page. On the left, a sidebar menu lists categories: System, Network, Line, Intercom settings (highlighted), Security settings, and Function Key. The main content area is divided into two columns of settings. In the left column, 'Limit Talk Duration' is set to 'Disable', 'DND Mode' is 'Phone', 'Enable Call Waiting' is checked, 'Enable Intercom' is checked, 'Enable Intercom Mute' is checked, 'Enable Auto Dial Out' is checked, 'Enable Auto Answer' is set to 'Lines and IP Call', 'No Answer Auto Hangup' is unchecked, 'Dial Fixed Length to Send' is checked, 'Voice Read IP' is set to 'Enable', 'Description' is 'IP Intercom Pho', and 'Enable Headset' is checked. In the right column, 'Talk Duration' is '120' (20~600) Second(s), 'Ban Outgoing' is unchecked, 'Enable Call Waiting Tone' is checked, 'Enable Intercom Barge' is checked, 'Enable Intercom Ringing' is checked, 'Auto Dial Out Time' is '5' (3~30)Second(s), 'Auto Answer Timeout' is '0' (0~60)Second(s), 'Auto Hangup Timeout' is '30' (1~60)Second(s), 'Send length' is '4', 'System Language' is 'English', and 'Enable DND' is unchecked. An 'Apply' button is located at the bottom right of the settings area.

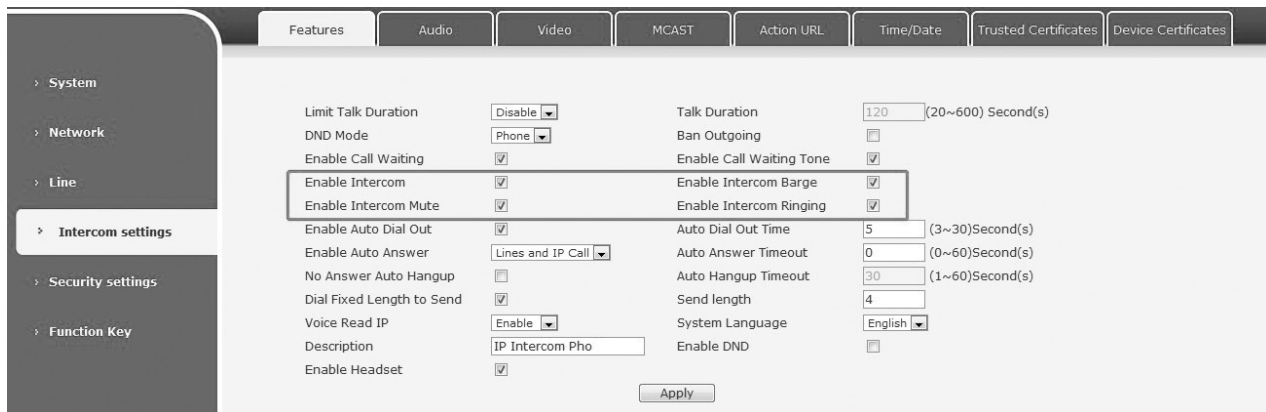
Feature	Value
Limit Talk Duration	Disable
DND Mode	Phone
Enable Call Waiting	☒
Enable Intercom	☒
Enable Intercom Mute	☒
Enable Auto Dial Out	☒
Enable Auto Answer	Lines and IP Call
No Answer Auto Hangup	☐
Dial Fixed Length to Send	☒
Voice Read IP	Enable
Description	IP Intercom Pho
Enable Headset	☒
Talk Duration	120 (20~600) Second(s)
Ban Outgoing	☐
Enable Call Waiting Tone	☒
Enable Intercom Barge	☒
Enable Intercom Ringing	☒
Auto Dial Out Time	5 (3~30)Second(s)
Auto Answer Timeout	0 (0~60)Second(s)
Auto Hangup Timeout	30 (1~60)Second(s)
Send length	4
System Language	English
Enable DND	☐

Picture 10. Set DND Option

5. Advance Function

5.1 Intercom

The equipment can answer intercom calls automatically.



Feature	Value
Limit Talk Duration	Disable
DND Mode	Phone
Enable Call Waiting	☒
Enable Intercom	☒
Enable Intercom Mute	☒
Enable Auto Dial Out	☒
Enable Auto Answer	Lines and IP Call
No Answer Auto Hangup	☐
Dial Fixed Length to Send	☒
Voice Read IP	Enable
Description	IP Intercom Pho
Enable Headset	☒
Talk Duration	120 (20~600) Second(s)
Ban Outgoing	☐
Enable Call Waiting Tone	☒
Enable Intercom Barge	☒
Enable Intercom Ringing	☒
Auto Dial Out Time	5 (3~30)Second(s)
Auto Answer Timeout	0 (0~60)Second(s)
Auto Hangup Timeout	30 (1~60)Second(s)
Send length	4
System Language	English
Enable DND	☐

Picture 11. WEB Intercom

Table 4. Intercom

Parameters	Description
Enable Intercom	When the intercom system is enabled, the device will accept the SIP header call-info of the Call request Command automatic call.
Enable Intercom Barge	If the option is enabled, intercom will answer the intercom call automatically while it is in a normal call, and it will reject new intercom call if there is already one intercome call.
Enable Intercom Mute	Enable mute during intercom mode.
Enable Intercom Ringing	If the incoming call is intercom call, the device plays the intercom tone.

5.2 MCAST

This feature allows user to make some kind of broadcast call to people who are in multicast group. User can configure a multicast DSS Key on the phone, which allows user to send a Real Time Transport Protocol (RTP) stream to the pre-configured multicast address without involving SIP signaling. You can also configure the phone to receive an RTP stream from pre-configured multicast listening address without involving SIP signaling. You can specify up to 10 multicast listening addresses.

Picture 12. MCAST

Table 5. MCAST

Parameters	Description
Enable Auto Mcast	Send the multicast configuration information by Sip Notify signaling, and the device will configure the information to the system for multicast listening or cancel the multicast listening in the system after receiving the information .
Auto Mcast Timeout Delete Time	When a multicast call does not end normally, but for some reason the device can no longer receive a multicast RTP packet, this configuration cancels the listening after a specified time.
SIP Priority	Defines the priority in the current call, with 1 being the highest priority and 10 the lowest.
Intercom Priority	Compared with multicast and SIP priority, high priority is pluggable and low priority is rejected.
Enable Page Priority	Regardless of which of the two multicast groups is called in first, the device will receive the higher priority multicast first.
Enable Mcast Tone	When enabled, play the prompt sound when receiving multicast.
Name	Listened multicast server name.
Host:port	Listened multicast server's multicast IP address and port.

Multicast:

- » Go to web page of [Function Key] >> [Function Key], select the type to multicast, set the multicast address, and select the codec.
- » Click Apply.
- » Set up the name, host and port of the receiving multicast on the web page of [Intercom Settings] >> [MCAST].
- » Press the DSSKey of Multicast Key which you set.
- » Receive end will receive multicast call and play multicast automatically.

5.3 Hotspot

SIP hotspot is a simple utility. Its configuration is simple, which can realize the function of group vibration and expand the quantity of sip account. Take one device A as the SIP hotspot and the other devices (B, C) as the SIP hotspot client. When someone calls device A, devices A, B, and C will ring, and if any of them answer, the other devices will stop ringing and not be able to answer at the same time. When A B or C device is called out, it is called out with A SIP number registered with device A.

Table 6. SIP Hotspot

Parameters	Description
Enable Hotspot	Enable or disable hotspot.
Mode	This device can only be used as a client.
Monitor Type	The monitoring type can be broadcast or multicast. If you want to restrict broadcast packets in the network, you can choose multicast. The type of monitoring on the server side and the client side must be the same, for example, when the device on the client side is selected for multicast, the device on the SIP hotspot server side must also be set for multicast.
Monitor Address	The multicast address used by the client and server when the monitoring type is multicast. If broadcasting is used, this address does not need to be configured, and the system will communicate by default using the broadcast address of the device's wan port IP.
Remote Port	Fill in a custom hotspot communication port. The server and client ports need to be consistent.
Name	Fill in the name of the SIP hotspot. This configuration is used to identify different hotspots on the network to avoid connection conflicts.
Line Settings	Sets whether to enable the SIP hotspot function on the corresponding SIP line.

Client Settings:

As a SIP hotspot client, there is no need to set up a SIP account, which is automatically acquired and configured when the device is enabled. Just change the mode to "client" and the other options are set in the same way as the hotspot.

The screenshot shows the web interface for the SIP Intercom Module. On the left is a sidebar menu with options: System, Network, Line (selected), Intercom settings, Security settings, and Function Key. The top navigation bar has tabs: SIP, Basic Settings, SIP Hotspot (active), and Blacklist. The main content area is titled 'SIP Hotspot' and contains two sections: 'Device Table' and 'Line Settings'.

Device Table

IP	MAC	Alias	Line
----	-----	-------	------

SIP Hotspot

Enable Hotspot:

Mode:

Monitor Type:

Monitor Address:

Remote Port:

Local Port:

Name:

Line Settings

SIP 1:

SIP 2:

Picture 13. SIP Hotspot

The device is the hotspot server, and the default extension is 0. The device ACTS as a client, and the extension number is increased from 1 (the extension number can be viewed through the [SIP hotspot] page of the webpage).

Calling internal extension:

- » The hotspot server and client can dial each other through the extension number before.
- » Extension 1 dials extension 0.

6. Web Configurations

6.1 Web Page Authentication

Users can log into the device's web page to manage user device information and operate the device. Users must provide the correct user name and password to log in. If the password is entered incorrectly three times, it will be locked and can be entered again after 5 minutes.

The details are as follows:

- » If an IP is logged in more than the specified number of times with a different user name, it will be locked.
- » If a user name logs in more than a specified number of times on a different IP, it is also locked.

6.2 System >> Information

User can get the system information of the device in this page including:

- » Model
- » Hardware Version
- » Software Version
- » Uptime
- » Last uptime
- » MEMInfo
- » System Time

And summarization of network status:

- » Network Mode
- » MAC Address
- » IP
- » Subnet Mask
- » Default Gateway

Besides, summarization of SIP account status:

- » SIP User
- » SIP account status (Registered / Unapplied / Trying / Timeout)

6.3 System >> Account

The screenshot shows the 'Account' tab in the 'System' menu. It features a sidebar with navigation options: System, Network, Line, Intercom settings, Security settings, and Function Key. The main content area is divided into three sections: 'Add New User' with input fields for Username, Web Authentication Password, Confirm Password, and a Privilege dropdown set to 'Administrators'; 'User Accounts' with a table listing 'admin' (Administrators) and 'guest' (Users); and 'User Management' with a dropdown showing 'admin' and 'Delete'/'Modify' buttons.

User	Privilege
admin	Administrators
guest	Users

Picture 14. WEB Account

On this page the user can change the password for the login page.
Users with administrator rights can also add or delete users, manage users, and set permissions and passwords for new users.

6.4 System >> Configurations

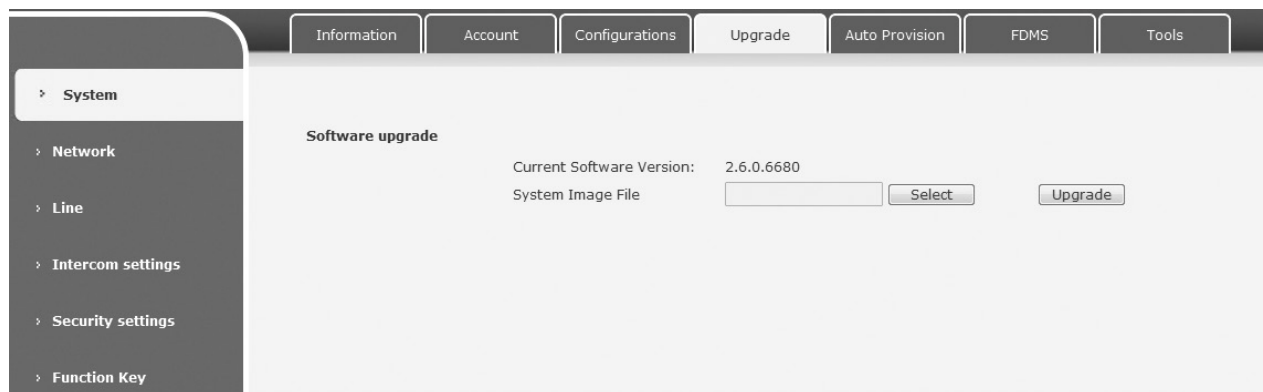
On this page, users with administrator privileges can view, export, or import the phone configuration, or restore the phone to factory Settings.

The screenshot shows the 'Configurations' tab in the 'System' menu. It features a sidebar with navigation options: System, Network, Line, Intercom settings, Security settings, and Function Key. The main content area is divided into three sections: 'Export Configurations' with instructions to right-click to save configurations in 'txt' or 'xml' format; 'Import Configurations' with a 'Configuration file:' input field and 'Select'/'Import' buttons; and 'Reset to factory defaults' with a 'Reset' button and a warning that all user data will be lost.

Picture 15. System Setting

- » **Export Configurations:** Right click to select target save as, that is, to download the device's configuration file, suffix ".txt". (note: profile export requires administrator privileges)
- » **Import Configurations:** Import the configuration file of Settings. The device will restart automatically after successful import, and the configuration will take effect after restart
- » **Reset Phone:** The phone data will be cleared, including configuration and database tables.

6.5 System >> Upgrade



Information Account Configurations **Upgrade** Auto Provision FDMS Tools

> System

> Network

> Line

> Intercom settings

> Security settings

> Function Key

Software upgrade

Current Software Version: 2.6.0.6680

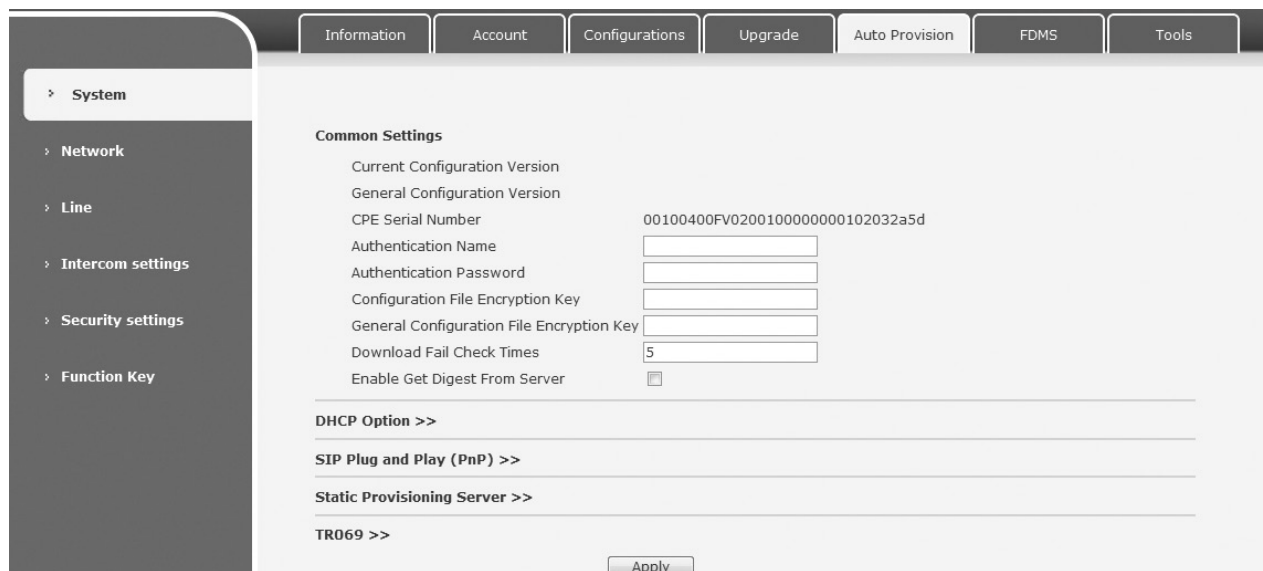
System Image File

Picture 16. Upgrade

Upgrade the software version of the device, and upgrade to the new version through the webpage. After the upgrade, the device will automatically restart and update to the new version.
Click select, select the version and then click upgrade.

6.6 System >> Auto Provision

Webpage: Login and go to [System] >> [Auto provision].



Information Account Configurations Upgrade **Auto Provision** FDMS Tools

> System

> Network

> Line

> Intercom settings

> Security settings

> Function Key

Common Settings

Current Configuration Version

General Configuration Version

CPE Serial Number 00100400FV0200100000000102032a5d

Authentication Name

Authentication Password

Configuration File Encryption Key

General Configuration File Encryption Key

Download Fail Check Times

Enable Get Digest From Server ☐

DHCP Option >>

SIP Plug and Play (PnP) >>

Static Provisioning Server >>

TR069 >>

Picture 17. Auto provision

Ambient System devices support SIP PnP, DHCP options, Static provision, TR069. If all of the 4 methods are enabled, the priority from high to low as below.

Table 7. Auto provision

Parameters	Description
Basic settings	
Current Configuration Version	Shows the current config file's version. If the version of the downloaded configuration file is same with this one, the configuration file will not be applied. If the device confirm the configuration by the Digest method, once the configuration of server is modified or the device's configurations are different from server's, the device will download and apply the configurations.
General Configuration Version	Shows the common config file's version. If the version of the downloaded configuration file is same with this one, the configuration file will not be applied. If the device confirm the configuration by the Digest method, once the configuration of server is modified or the device's configurations are different from server's, the device will download and apply the configurations.
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.
Download Fail Check Times	The default value is 5. If the download configuration fails, it will be downloaded 5 times.
Enable Get Digest From Server	When the feature is enable, if the configuration of server is changed, phone will download and update.
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.
Enable DHCP Option 120	Set the SIP server address through DHCP option 120.
SIP Plug and Play (PnP)	
Enable SIP PnP	Whether enable PnP or not. If PnP is enable, phone will send a SIP SUBSCRIBE message with broadcast method. Any server can support the feature will respond and send a Notify with URL to phone. Phone could get the configuration file with the URL.
Server Address	Broadcast address. As default, it is 224.0.0.0.
Server Port	PnP port
Transport Protocol	PnP protocol, TCP or UDP
Update Interval	PnP message interval

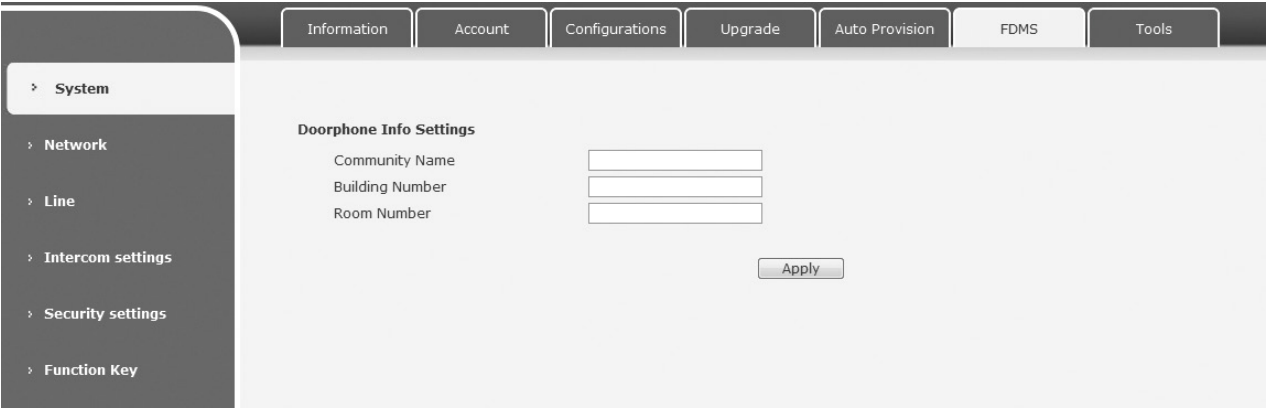
Static Provisioning Server

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	The configuration file name. If it is empty, phone will request the common file and device file which is named as its MAC address. The file name could be a common name, \$mac.cfg, \$input.cfg. The file format supports CFG / TXT / XML.
Protocol Type	Transferring protocol type, supports FTP / TFTP / HTTP and HTTPS.
Update Interval	Configuration file update interval time. As default it is 1, means phone will check the update every 1 hour.
Update Mode	Provision Mode: 1. Disabled. 2. Update after reboot. 3. Update after interval.

TR069

Enable TR069	Enable TR069 after selection
Enable TR069 Warning Tone	If TR069 is enabled, there will be a prompt tone when connecting
ACS Server Type	There are 2 options Serve type, common and CTC
ACS Server URL	ACS server address
ACS User	ACS server username (up to is 59 character)
ACS Password	ACS server password (up to is 59 character)
STUN server address	Enter the STUN address
Enable the STUN	Enable the STUN
TLS Version	TLS Version

6.7 System >> FDMS



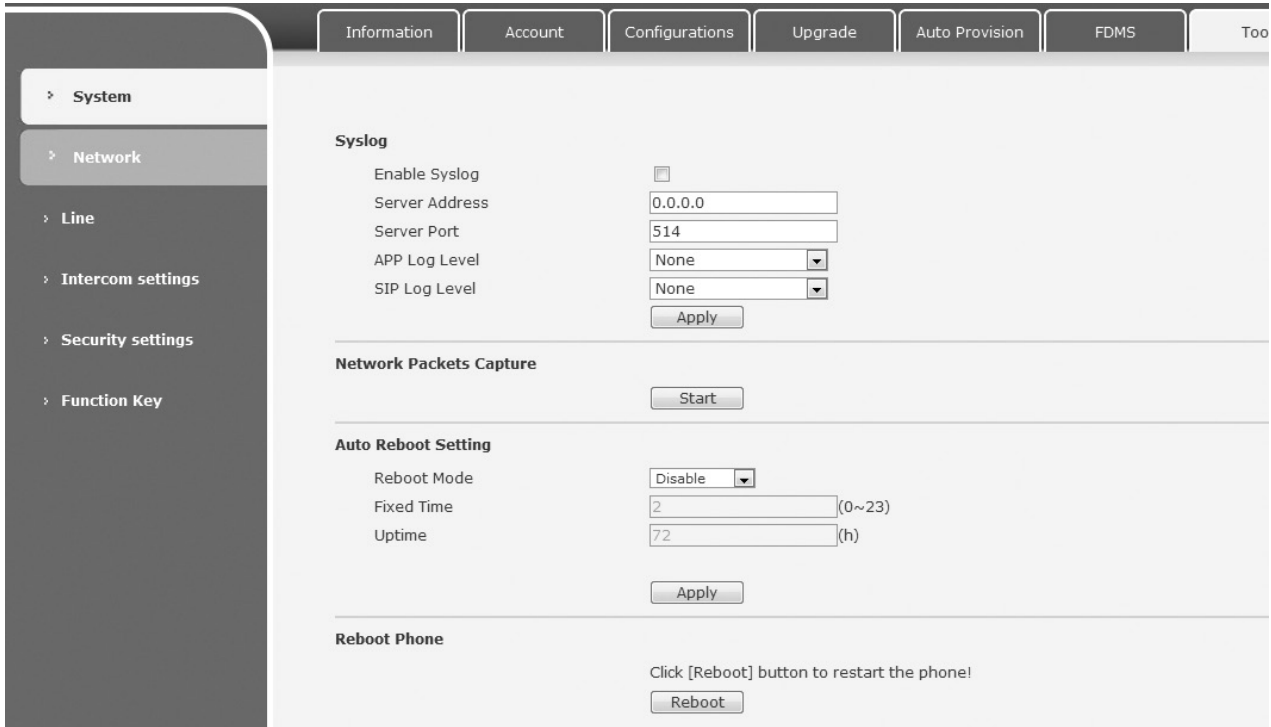
Picture 18. FDMS

Table 8. FDMS

FDMS information Settings	
Community designations	Name of equipment installation community
Building a movie theatre	Name of equipment installation building
Room number	Equipment installation room name

6.8 System >> Tools

This page gives the user the tools to solve the problem.



The screenshot shows the 'Tools' section of the Ambient System interface. The left sidebar contains a menu with 'System' selected, and 'Network' expanded. The main content area has tabs for 'Information', 'Account', 'Configurations', 'Upgrade', 'Auto Provision', 'FDMS', and 'Tools'. The 'Tools' tab is active, displaying four sections:

- Syslog:** Includes a checkbox for 'Enable Syslog', text input for 'Server Address' (0.0.0.0), text input for 'Server Port' (514), dropdowns for 'APP Log Level' (None) and 'SIP Log Level' (None), and an 'Apply' button.
- Network Packets Capture:** Includes a 'Start' button.
- Auto Reboot Setting:** Includes a dropdown for 'Reboot Mode' (Disable), text input for 'Fixed Time' (2) with a range '(0~23)', text input for 'Uptime' (72) with a unit '(h)', and an 'Apply' button.
- Reboot Phone:** Includes a text instruction 'Click [Reboot] button to restart the phone!' and a 'Reboot' button.

Picture 19. Tools

Syslog: When enabled, set the syslog software address, and log information of the device will be recorded in the syslog software during operation. If there is any problem, log information can be analyzed by Ambient System technical support.

Auto Reboot Setting

Reboot Mode:

- » Disable: It will not restart at set time after disabled
- » Fixed Time: In the range of 0~24 (h), restart will be conducted at the setting point every day after the setting is completed
- » Uptime: **Set the maximum** length to 3 bits and restart at run time

For other details, please refer to [section 7 – trouble shooting](#).

6.9 Network >> Basic

This page allows users to configure network connection types and parameters.

The screenshot displays the 'Network Basic Setting' page. On the left is a sidebar with navigation links: System, Network (selected), Line, Intercom settings, Security settings, and Function Key. The main content area has tabs for Basic, Advanced, VPN, and Web Filter. Under the 'Basic' tab, the 'Network Status' section shows: IP: 172.16.12.104, Subnet mask: 255.255.255.0, Default gateway: 172.16.12.1, MAC: 00:01:02:03:2a:5d, and MAC Timestamp: 20160714. The 'Setting' section has radio buttons for Static IP, DHCP (selected), and PPPoE. Below are fields for DNS Server Configured by (DHCP), Primary DNS Server, and Secondary DNS Server, with an 'Apply' button. The 'Service Port Settings' section has a dropdown for Web Server Type (HTTP), and input fields for HTTP Port (80) and HTTPS Port (443), with an 'Apply' button. At the bottom, there's a section for 'HTTPS Certification File' showing 'https.pem' (4501 Bytes) with 'Upload' and 'Delete' buttons.

Picture 20. Network Basic Setting

Table 9. Auto provision

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 Time stamp	Display the time when the device gets the MAC address.
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.

attention:

1. After setting the parameters, click [Apply] to take effect.
2. If you change the IP address, the webpage will no longer responds, please enter the new IP address in web browser to access the device.
3. If the system USES DHCP to obtain IP when device boots up, and the network address of the DHCP Server is the same as the network address of the system LAN, then after the system obtains the DHCP IP, it will add 1 to the last bit of the network address of LAN and modify the IP address segment of the DHCP Server of LAN. If the DHCP access is reconnected to the WAN after the system is started, and the network address assigned by the DHCP server is the same as that of the LAN, then the WAN will not be able to obtain IP access to the network

Service Port Settings

Web Server Type	Specify Web Server Type – HTTP or HTTPS.
HTTP Port	Port for web browser access. Default value is 80. To enhance security, change this from the default. Setting this port to 0 will disable HTTP access. Example: The IP address is 192.168.1.70 and the port value is 8090, the accessing address is http://192.168.1.70:8090.
HTTPS Port	Default value is 443. To enhance security, change this from the default.

6.10 Network >> Advanced

The screenshot displays the 'Advanced' network configuration page for the SIP Intercom Module. The left sidebar shows a navigation menu with 'System' and 'Network' expanded. The main content area is divided into several sections for configuring network protocols and services.

Section	Parameter	Value	Range/Unit
Link Layer Discovery Protocol (LLDP) Settings	Enable LLDP	☐	
	Enable Learning Function	☐	
Packet Interval	Packet Interval	60	Second(s)
ARP Cache Life	ARP Cache Life	2	Minute
VLAN Settings	Enable VLAN	☐	
	VLAN ID	256	(0~4095)
	802.1p Signal Priority	0	(0~7)
802.1p Media Priority	802.1p Media Priority	0	(0~7)
LAN Port VLAN Settings	Mode	Disable	
	LAN Port VLAN ID	254	(0~4095)
	802.1p Priority	0	(0~7)
DHCP VLAN Settings	Option Value	Disabled	
	DHCP Option Vlan(128-254)	0	
Quality of Service (QoS) Settings	Enable DSCP QoS	☒	
	Media QoS Priority	46	(0~63)
	Signal QoS Priority	46	(0~63)
802.1X Settings	Enable 802.1X	☐	
	Username	admin	

Picture 21. Network Setting

Network advanced Settings are typically configured by IT administrators to improve the quality of device service.

Table 10. Network Setting

Field Name	Explanation
LLDP Settings	
Enable LLDP	Enable or disable LLDP
Packet Interval	LLDP Send detection cycle
Enable Learning Function	Learn the discovered device information on the device
QoS Settings	
Pattern	Voice quality assurance (off by default)
DHCP VLAN Settings	
parameters values	128 – 254, Obtain the VLAN value through DHCP
WAN port virtual Wan	
WAN port virtual Wan	WAN port Settings
LAN port virtual LAN	
LAN port virtual LAN	LAN port Settings
802.1X	
Enable 802.1X	Enable or disable 802.1X
Username	Confirm Username
Password	Confirm Password

6.11 Network >> VPN

Virtual Private Network (VPN) Status			
VPN IP Address:	0.0.0.0		

VPN Mode			
Enable VPN	☒		
L2TP	☒	OpenVPN	☒

Layer 2 Tunneling Protocol (L2TP)			
L2TP Server Address			
Authentication Name	admin		
Authentication Password	•••••		
Apply			

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

Picture 22. VPN

Virtual Private Network (VPN) is a technology to allow device to create a tunneling connection to a server and becomes part of the server's network. The network transmission of the device may be routed through the VPN server.

For some users, especially enterprise users, a VPN connection might be required to be established before activate a line registration. The device supports two VPN modes, Layer 2 Transportation Protocol (L2TP) and OpenVPN.

The VPN connection must be configured and started (or stopped) from the device web portal.

» L2TP

NOTE! The device only supports non-encrypted basic authentication and non-encrypted data tunneling. For users who need data encryption, please use OpenVPN instead.

To establish a L2TP connection, users should log in to the device web portal, open webpage **[Network] >> [VPN]**. In VPN Mode, check the "Enable VPN" option and select "L2TP", then fill in the L2TP server address, Authentication Username, and Authentication Password in the L2TP section. Press "Apply" then the device will try to connect to the L2TP server.

When the VPN connection established, the VPN IP Address should be displayed in the VPN status. There may be some delay of the connection establishment. User may need to refresh the page to update the status.

Once the VPN is configured, the device will try to connect with the VPN automatically when the device boots up every time until user disable it. Sometimes, if the VPN connection does not establish immediately, user may try to reboot the device and check if VPN connection established after reboot.

» OpenVPN

To establish an OpenVPN connection, user should get the following authentication and configuration files from the OpenVPN hosting provider and name them as the following:

OpenVPN Configuration file: client.ovpn

CA Root Certification: ca.crt

Client Certification: client.crt

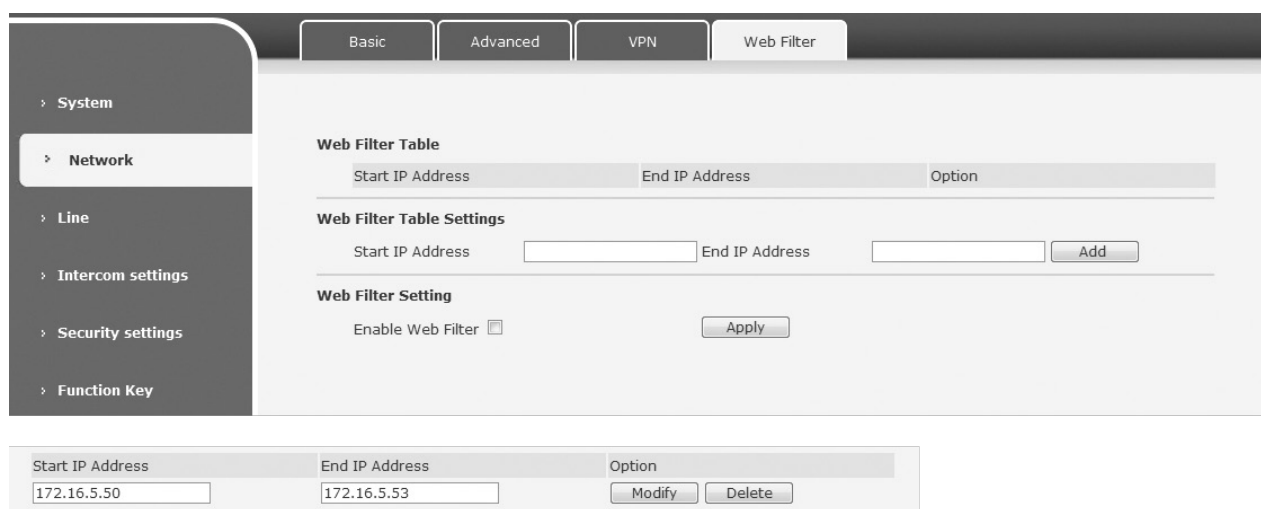
Client Key: client.key

User can upload these files to the device in the web page **[Network] >> [VPN]**, select OpenVPN Files. Then user should check "Enable VPN" and select "OpenVPN" in VPN Mode and click "Apply" to enable OpenVPN connection.

Same as L2TP connection, the connection will be established every time when system rebooted until user disable it manually.

6.12 Network >> Web Filter

A user can set up a configuration management device that allows only machines with a certain network segment IP to access the configuration management device.



Start IP Address	End IP Address	Option
172.16.5.50	172.16.5.53	Modify Delete

Picture 23. WEB Filter Table

Add and remove IP segments that are accessible; Configure the starting IP address within the start IP, end the IP address within the end IP, and click **[Add]** to submit to take effect. A large network segment can be set, or it can be divided into several network segments to add. When deleting, select the initial IP of the network segment to be deleted from the drop-down menu, and then click **[Delete]** to take effect.

Enable web page filtering; configure enable/disable web page access filtering; Click the "apply" button to take effect.

NOTE: if the device you are accessing is in the same network segment as the phone, please do not configure the filter segment of the web page to be outside your own network segment, otherwise you will not be able to log in the web page.

6.13 Line >> SIP

Configure the service configuration for the wire on this page.

The screenshot displays the SIP configuration page. On the left is a sidebar with navigation links: System, Network, Line (selected), Intercom settings, Security settings, and Function Key. The main area has tabs for SIP, Basic Settings, SIP Hotspot, and Blacklist. Under the SIP tab, there's a 'Line' dropdown set to 'SIP 1'. Below this are sections for 'Basic Settings >>', 'Codecs Settings >>', and 'Advanced Settings >>'. The 'Advanced Settings' section contains two columns of options with checkboxes, dropdowns, and text inputs. Options include Enable DND, Blocking Anonymous Call, Use 182 Response for Call waiting, Anonymous Call Standard (set to None), Dial Without Registered, Click To Talk, User Agent, Response Single Codec, Specific Server Type (set to COMMON), Registration Expiration (3600 seconds), Use VPN (checked), Use STUN (checked), Convert URI (checked), DTMF Type (set to RFC2833), DTMF SIP INFO Mode (set to Send */#), Transportation Protocol (set to UDP), Local Port (5450), Ring Type (set to Default), Conference Type (set to Local), Server Conference Number, Transfer Timeout (0 seconds), Enable Long Contact, Enable Use Inactive Hold, Use Quote in Display Name, TLS Version (set to TLS 1.2), Enable DNS SRV, Keep Alive Type (set to SIP Option), Keep Alive Interval (60 seconds), Sync Clock Time, Enable Session Timer, Session Timeout (0 seconds), Enable Rport (checked), Enable PRACK (checked), and Auto Change Port (checked).

Picture 24. SIP

Table 11. SIP

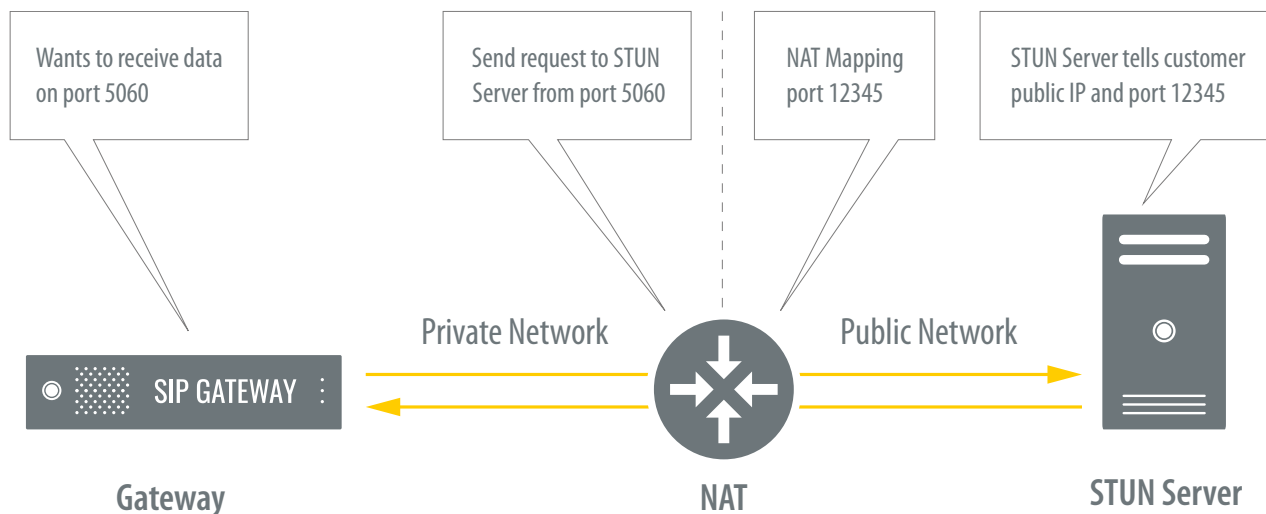
Field Name	Explanation
Basic settings (Choose the SIP line to configured)	
Line Status	Display the current line status at page loading. To get the up to date line status, user has to refresh the page manually.
Username	Enter the username of the service account.
Display name	Enter the display name to be sent in a call request.
Authentication Name	Enter the authentication name of the service account.
Authentication Password	Enter the authentication password of the service account.
Activate	Whether the service of the line should be activated.
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server.
SIP Proxy Server Port	Enter the SIP proxy server port, default is 5060.
Outbound proxy address	Enter the IP or FQDN address of outbound proxy server provided by the service provider.

Outbound proxy port	Enter the outbound proxy port, default is 5060.
Realm	Enter the SIP domain if requested by the service provider.
Codecs Settings	
Set the priority and availability of the codecs by adding or remove them from the list.	
Advanced Settings	
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 dialling to a conference room on the server.
Server Conference Number	Set the conference room number when conference type is set to be server.
Enable Long Contact	Allow more parameters in contact field per RFC 3840.
Enable use inactive hold	Active capture package SDP is inactive, while the hold is sendrecv. Active capture package has no response of 400, etc. Hold the hair inactive. After closing the grab packet, you can see that the DSP is sendonly and the hold is sendrecv.
TLS version	TLS version.
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 sending mode, there are four types: › In-band › RFC2833 › SIP_INFO › AUTO › Different service providers may offer different models

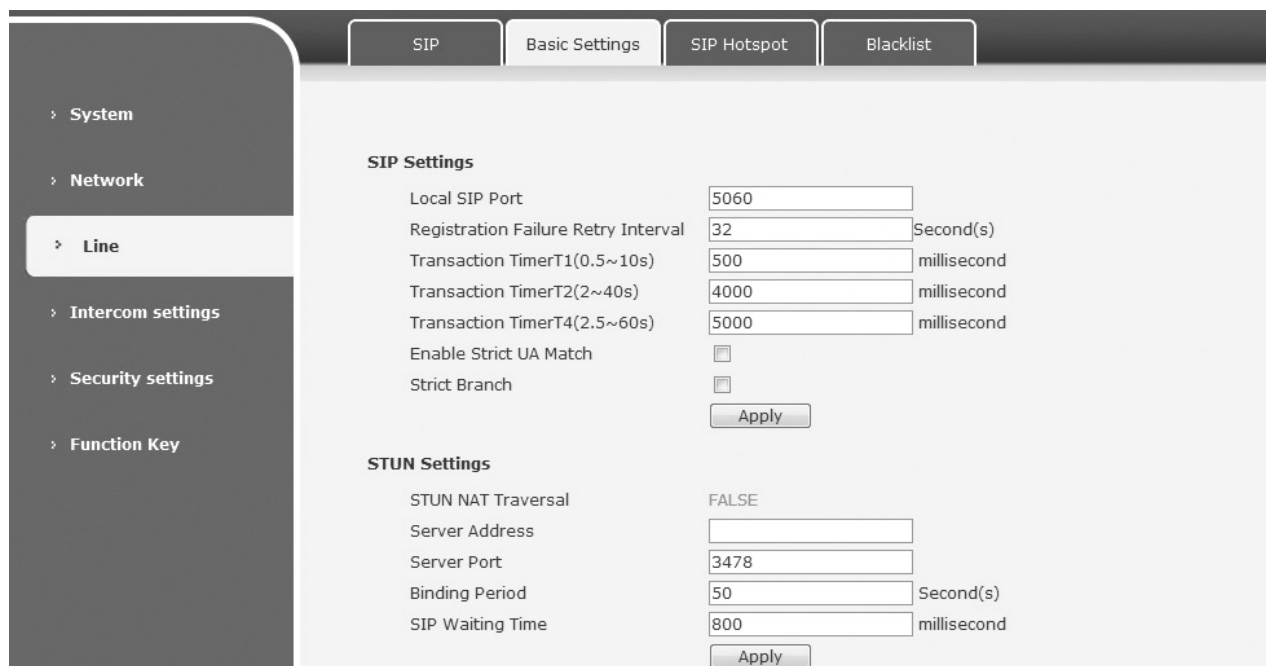
DTMF SIP INFO Mode	When the device's DTMF type is set to SIP_INFO The DTMF_SIP_INFO type is configured to send */#, and when the device presses the */# key, the actual value sent is */#; Configured to send 10/11, when the device presses the */# key, the actual value sent is 10/11.
Transportation Protocol	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.
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 GRUU	Support Globally Routable User-Agent URI (GRUU).
RTP Encryption	Set the pass phrase for RTP encryption.
Enable MAC Header	When enabled, all SIP messages strip Mac fields.
Enable Register MAC Header	When enabled, register the message ribbon Mac field.

6.14 Line >> 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.



Picture 25. Network Basic



The screenshot shows the 'Line Basic Setting' interface. The sidebar on the left contains the following navigation items: System, Network, Line (highlighted), Intercom settings, Security settings, and Function Key. The main content area is divided into two sections: SIP Settings and STUN Settings.

SIP Settings

Local SIP Port	5060
Registration Failure Retry Interval	32 Second(s)
Transaction TimerT1(0.5~10s)	500 millisecond
Transaction TimerT2(2~40s)	4000 millisecond
Transaction TimerT4(2.5~60s)	5000 millisecond
Enable Strict UA Match	☐
Strict Branch	☐

Apply

STUN Settings

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

Apply

Picture 26. Line Basic Setting

Table 12. Line Basic Setting

Field Name	Explanation
SIP Settings	
Local SIP Port	Set the local SIP port used to send/receive SIP messages.
Registration Failure Retry Interval	Set the retry interval of SIP REGISTRATION when registration failed.
Enable Strict UA Match	Enable or disable Strict UA Match.
STUN Settings	
Server Address	STUN Server IP address.
Server Port	STUN Server Port – Default is 3478.
Binding Period	STUN blinding period – STUN packets are sent at this interval to keep the NAT mapping active.
SIP Waiting Time	Waiting time for SIP. This will vary depending on the network.

6.15 Line >> SIP Hotspot

SIP hotspot is a simple and practical function. It is simple to configure, can realize the function of group vibration, and can expand the number of SIP accounts.

See [section 5.3 Hotspot](#) for details.

The screenshot shows the 'SIP Hotspot' configuration page. The sidebar on the left contains a tree view with 'System', 'Network', 'Line', 'Intercom settings', 'Security settings', and 'Function Key'. The 'Line' item is selected. The main content area has four tabs: 'SIP', 'Basic Settings', 'SIP Hotspot', and 'Blacklist'. The 'SIP Hotspot' tab is active. It contains a 'Device Table' with columns 'IP', 'MAC', 'Alias', and 'Line'. Below the table is the 'SIP Hotspot' configuration section, which includes the following settings:

- Enable Hotspot:
- Mode:
- Monitor Type:
- Monitor Address:
- Remote Port:
- Local Port:
- Name:

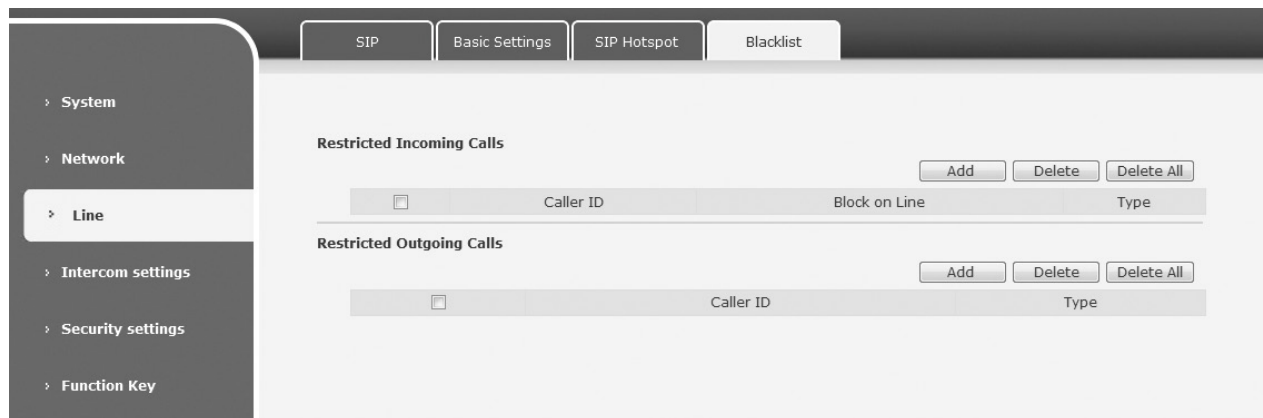
Below these settings is the 'Line Settings' section, which includes:

- SIP 1:
- SIP 2:
-

Picture 27. SIP Hotspot

6.16 Intercom settings >> Blacklist

Web page to add call limit function, you can set the number or prefix to limit calls. The rules are as follows:
 Add x, type number, x cannot call. Add x, type prefix, then the number beginning with x cannot call.
 X could be a number or an IP. To add a whitelist rule, the number /IP should be preceded by a "-", followed by a ".",
 After addition, only the number in the whitelist is allowed to call, and the number outside the whitelist is refused.

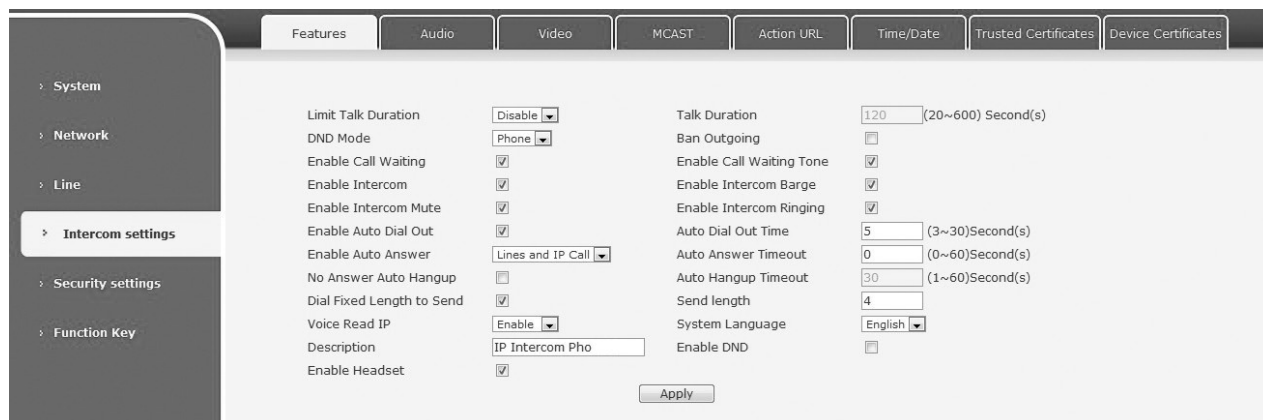


The screenshot shows the 'Blacklist' tab in the configuration menu. It contains two sections: 'Restricted Incoming Calls' and 'Restricted Outgoing Calls'. Each section has a table with columns for 'Caller ID', 'Block on Line', and 'Type'. There are 'Add', 'Delete', and 'Delete All' buttons for each section. The 'Line' menu item is highlighted in the left sidebar.

Picture 28. Blacklist

6.17 Intercom settings >> Features

Configure intercom Settings.



The screenshot shows the 'Features' tab in the configuration menu. It contains various settings for intercom functionality, including 'Limit Talk Duration', 'DND Mode', 'Enable Call Waiting', 'Enable Intercom', 'Enable Intercom Mute', 'Enable Auto Dial Out', 'Enable Auto Answer', 'No Answer Auto Hangup', 'Dial Fixed Length to Send', 'Voice Read IP', 'Description', 'Enable Headset', 'Talk Duration', 'Ban Outgoing', 'Enable Call Waiting Tone', 'Enable Intercom Barge', 'Enable Intercom Ringing', 'Auto Dial Out Time', 'Auto Answer Timeout', 'Auto Hangup Timeout', 'Send length', 'System Language', and 'Enable DND'. Each setting has a corresponding input field or checkbox. The 'Intercom settings' menu item is highlighted in the left sidebar.

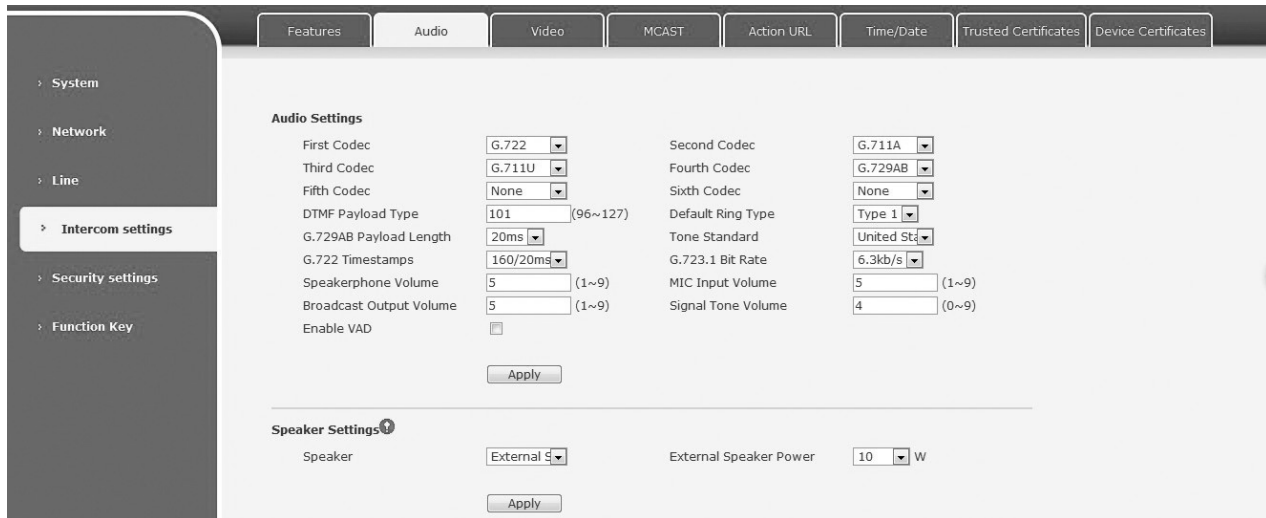
Picture 29. Feature

Table 13. Common device function Settings on the web page

Field Name	Explanation
Basic Settings	
Limit Talk Duration	If user enables the option, intercom will hang up the call automatically while talk duration is achieved.
Talk Duration	Time out to hang up.
DND (Do Not Disturb)	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 Call Waiting	The default value is enabled. Allow users to answer the second call while maintaining the call.
Enable Call Waiting Tone	The default value is enabled. When enabled, the call waiting tone can be heard while waiting for a call. If this function is turned off, when waiting for a call, the beep will not be heard.
Enable Intercom	When the intercom system is enabled, the device will accept the SIP header call-info of the Call request. Command automatic call.
Enable Intercom Barge	Automatically answer calls in intercom mode during a call if the current call is intercom mode. Type, refused to answer the new intercom mode.
Enable Intercom Mute	If enabled, mutes incoming calls during an intercom call.
Enable Intercom Tone	If enabled, plays intercom ring tone to alert to an intercom call.
Enable Auto Dial Out	Enable Auto Dial Out when timeout.
Auto Dial Out Time	Configure waiting time for timeout dialling.
Enable Auto Answer	Enable Auto Answer function.
Auto Answer Timeout	Set Auto Answer Timeout.
Auto Hangup Timeout	Set the time of no answer auto hangs up..
Dial Fixed Length to Send	Configure to enable/disable fixed-length automatic dial-out numbers.
Voice Read IP	Turn on or off device voice broadcast IP address.
System Language	Language for configuring voice prompts.
Description	Description information displayed on IP scan tool software or FDMS. The default is "intercom".
Enable Headset	Active speaker and SPK output when enabled, SPK only when off.

6.18 Intercom Setting >> Audio

Change voice Settings.



Picture 30. Audio

Table 14. Voice Settings on web pages

Field Name	Explanation
Basic Settings	
First Codec	The first codec choice: G.711A/u, G.722, G.723, G.729, G.726-32
Second Codec	The second codec choice: G.711A/u, G.722, G.723, G.729, G.726-32
Third Codec	The third codec choice: G.711A/u, G.722, G.723, G.729, G.726-32
Fourth Codec	The forth codec choice: G.711A/u, G.722, G.723, G.729, G.726-32
Five Codec	The Five codec choice: G.711A/u, G.722, G.723, G.729, G.726-32
Six Codec	The Six codec choice: G.711A/u, G.722, G.723, G.729, G.726-32
DTMF Payload Type	The RTP Payload type that indicates DTMF. Default is 101.
Default Ring Type	Ring sound – there are 9 standard types and 3 user types.
G.729AB Payload Length	G.729AB Payload length – adjust from 10 – 60 msec.
G.723.1 Bit Rate	Configure signal tone standard area.
G.722 Timestamps	Select a timestamp for the g. 722 encoding, optional 160/20 ms,320/20 ms.
G.723.1 Bit Rate	Select the rate of G723, optional 5.3 kb/s,6.3 kb/s.
Speakerphone Volume	Configure speakerphone volume level.
MIC Input Volume	Configure the call volume level for the microphone.
Broadcast Output Volume	Configure the output volume level for broadcast.
Signal Tone Volume	Configure the output volume level of the signal sound.

Enable VAD	Mute detection; If VAD is enabled, the payload length of g.729 should not be greater than 20 ms.
Player Settings	
Player	The player has two modes of choice, panel speaker or external speaker. "Panel horn" means that both the speaker and the microphone are installed in the same shell and are mainly used for intercom. At this time, the sound effect of two-way intercom is required to be better. Therefore, the output power of the speaker needs to be optimized to ensure the sound effect of intercom. "External speaker" refers to the external speaker, microphone and speaker are separately deployed, at this time the broadcast sound requirements are larger.
External speaker power	External speaker power can only be selected in the "external speaker" mode, 10 W / 20 W / 30 W respectively. At this time, the impedance of the speaker used is 4 ohms. Note that the corresponding power supply is POE (or 12 VDC) / 18VDC / 24VDC 2A power supply.
AEC Settings	
AEC Settings	Provide adjustment parameter Settings for different power connection states.
Sound Update/Delete	
Sound Update	Optional.wav suffix ring tone upgrade.
Sound Delete	The upgraded ringtone is shown in the delete list and can be optionally deleted.
Alert Info Ring Settings	
The value of notification information 1 to 10	Sets the value to specify the ringtone type.
Ring Type	Type1-Type9

6.19 Intercom Setting >> Video

The screenshot displays the 'Video' configuration page of the SIP Intercom Module. The interface includes a top navigation bar with tabs for Features, Audio, Video, MCAST, Action URL, Time/Date, Trusted Certificates, and Device Certificates. A left sidebar contains a menu with options: System, Network, Line, Intercom settings (selected), Security settings, and Function Key. The main content area is divided into several sections. The 'Camera Status' section shows 'Inactive'. Below it is a table with three rows: 'Max Access Num' (N/A), 'Max M Num' (N/A), and 'Max S Num' (N/A), each with a 'Use' column and a value of '0'. The 'Ip Camera Connect Settings' section features a 'Connect Mode' dropdown menu set to 'External' and an 'Apply' button. The 'Ip Camera Settings>>' section contains the following fields: 'ipCameraName' (text input, 40 Characters), 'User' (text input, admin), 'Password' (password input, masked with dots), 'Ip Camera Brand' (dropdown menu, XM), 'IP' (text input), 'Port' (text input, 554), 'Main Stream Url' (text input), 'Sub Stream Url' (text input), 'User Agent' (text input), and 'H.264 Stream No SPS&PPS' (checkbox). An 'Apply' button is located at the bottom of this section.

Picture 31. Video Setting

Table 15. Video Setting

Field Name	Explanation
Camera Settings (external mode)	
Connection Mode	Select external, click submit, and restart the device.
Name	Camera name.
User name	External camera login name.
Password	External camera login password.
Camera type	Select camera manufacturer.
IP address	Camera IP address, please use the camera matching scan tool to get the IP address.
Port	Camera port number.
Main Stream Url	After user submit the camera information and apply the changes, if the device connects external camera successfully, the page will display the main stream URL directly, or the information is blank.
Sub Stream Url	After user submit the camera information and apply the changes, if the device connects external camera successfully, the page will display the sub stream URL directly, or the information is blank. If the IP camera user used is not in the list, and user select CUSTOMER as IP camera brand, he also need input the main stream URL manually.
Advanced Settings	
Video Direction	Sendonly: establish video call, and the SDP packet in the invite packet is Sendonly; Sendrecv: to create a call, the SDP package in the invite package is Sendrecv.
RTSP Over TCP	The RTSP goes over the TCP protocol.
H.264 Payload Type	Set the h. 264 Payload type. The range is between 96 and 127. The default is 117.
Default Call Stream	Optional main stream and substream.
RTSP Information	
Main Stream Url	Display the main stream URL address.
Sub Stream Url	Display the sub stream URL address.

6.20 Intercom Setting >> 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.

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

Picture 32. MCAST

Table 16. MCAST parameters

Field Name	Explanation
Enable Auto Mcast	SIP Notify information is used to issue mcast configurations, after device receives the information, it can finish the configurations to listen the mcast or cancel mcast listening.
Auto Mcast Timeout Delete Time	When a multicast call does not end normally, but for some reason the device can no longer receive the multicast RTP packets, enable this option will make the device cancel listening after a specified period.
SIP priority	Defines the priority in the current call, with 1 being the highest priority and 10 the lowest.
Broadcast priority	Compared with multicast and SIP priority, higher priority is pluggable and low priority is rejected.
Enable Page Priority	Two multicasts, regardless of who first calls in, the device will accept the multicast with higher priority.
Multicast prompt tone	When enabled, play the prompt sound first when receiving multicast.
Name	Listened multicast server name.
Host: port	Listened multicast server's multicast IP address and port.

6.22 Intercom Setting >> Time/Date

Users can configure the device's time Settings on this page.

The screenshot shows the 'Time/Date' configuration page in the SIP Intercom Module web interface. The sidebar on the left lists navigation options: System, Network, Line, Intercom settings (selected), Security settings, and Function Key. The main content area is titled 'Time/Date' and contains two sections: 'Network Time Server Settings' and 'Daylight Saving Time Settings'. The 'Network Time Server Settings' section includes checkboxes for 'Time Synchronized via SNTP' (checked) and 'Time Synchronized via DHCP' (unchecked). It also has input fields for 'Primary Time Server' (time.nist.gov), 'Secondary Time Server' (pool.ntp.org), a 'Time zone' dropdown (set to '(UTC+8) China, Singapore, Australia'), and a 'Resync Period' input (60 seconds). The 'Daylight Saving Time Settings' section includes a 'Location' dropdown (China(Beijing)), a 'DST Set Type' dropdown (Automatic), a 'Fixed Type' dropdown (Disabled), an 'Offset' input (0 minutes), and a table for 'Start' and 'End' dates with dropdowns for Month, Week, Weekday, and Hour. Both sections have an 'Apply' button at the bottom.

Picture 34. Time/Date

Table 18. 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
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.
Offset	The DST offset time.
Month Start	The DST start month .

Week Start	The DST start week
Weekday Start	The DST start weekday
Hour Start	The DST start hour
Month End	The DST end month
Week End	The DST end week
Weekday End	The DST end weekday
Hour End	The DST end hour

Manual Time Settings

To set the time manually, you need to disable the SNTP service first, and you need to fill in and submit each item of year, month, day, hour and minute in the figure above to make the manual settings successful.

System time: Display system time and its source (SIP automatic get > SNTP automatic get > manual manual setting) .

6.23 Intercom Setting >> Trusted Certificates

User can upload and delete the uploaded certificates in certificate management page.

Update Trusted Certificates File

Load Trusted Certificates File

Delete Trusted Certificates File

Select Trusted Certificates File

Trusted Certificates File

File Name	Issued To	Issued By	Expiration	File Size

Trusted Certificates Settings

CA Certificates

Picture 35. Trusted Certificates

6.24 Intercom Setting >> Device Certificates

User can upload and delete the uploaded certificates for device in device certificates page.

Device Certificates

Device Certificates

Custom Certificates

Apply

Import Certificates

Load Device Certificates File

Select

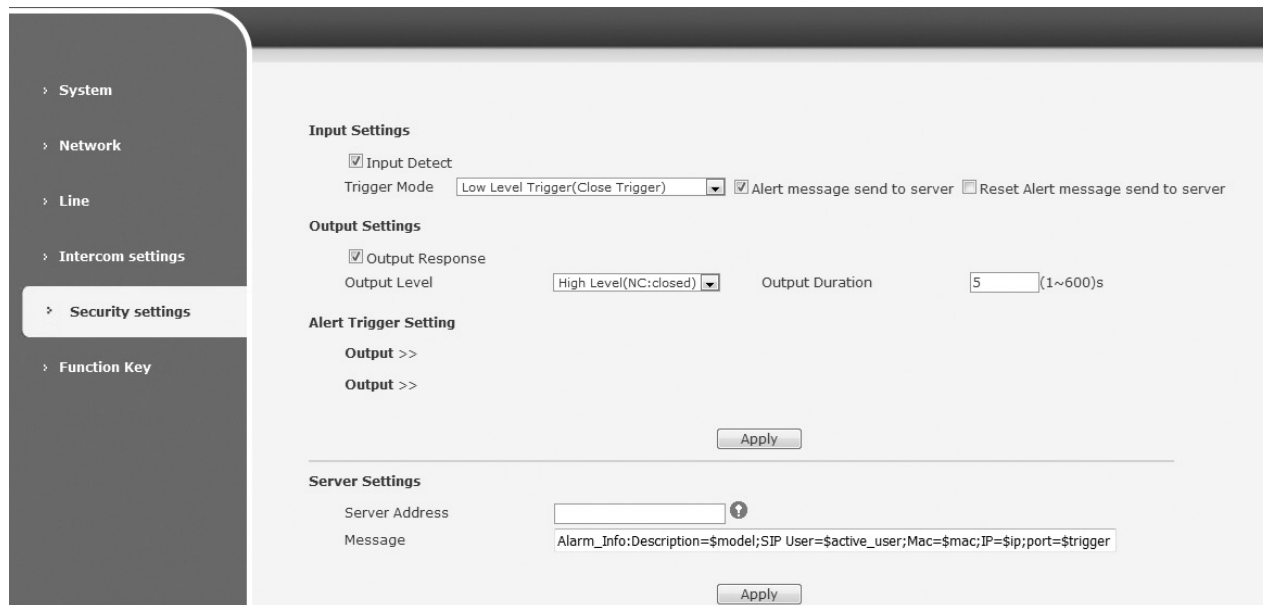
Upload

Certification File

Index	File Name	Issued To	Issued By	Expiration	File Size
					Delete

Picture 36. Device Certificates

6.25 Security Settings



Picture 37. Alert/Security Settings

Table 19. Alert/Security Settings

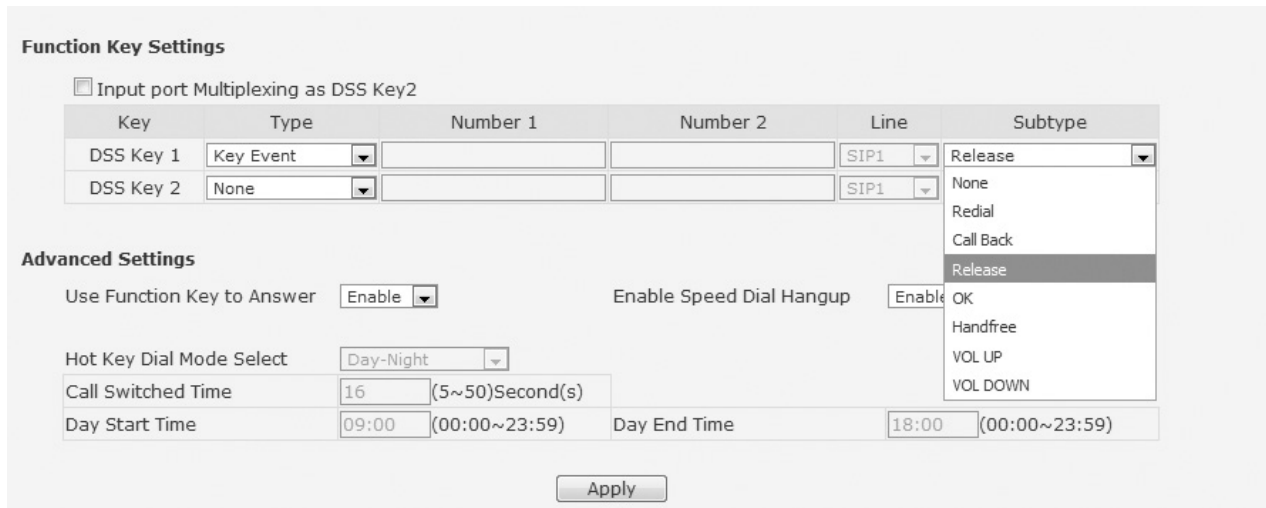
Field Name	Explanation
Input settings	
Input Detect	Enable or disable Input Detect.
Trigger Mode	When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger.
	When choosing the high level trigger (disconnected trigger), detect the input port (high level) disconnected trigger.
Alert message send to server	Set the Alert message send to server.
Reset Alert message send to server	Enable or disable sending reset messages to the server.
Output Settings	
Output Response	Enable or disable Output Response.
Output Level	When choosing the low level trigger (NO: normally open), when meet the trigger condition, trigger the NO port disconnected.
	When choosing the high level trigger (NC: normally close), when meet the trigger condition, trigger the NO port close.
Output Duration	The duration of the changes in the output port, default value is 5 seconds.

Alert Trigger Setting		
Input trigger	When the input port meets the trigger condition, the output port will be triggered (The trigger duration is controlled by option Output Duration).	
DTMF output Duration	By duration	Port switch amount change time, press < output duration > control.
	By Calling	By call state control, after the end of the call, port to return the default state.
Remote DTMF trigger	Receive the DTMF password sent by the remote device. If it is correct, trigger the corresponding output port. You can choose to enable or disable ringtones.	
DTMF trigger code	During the call, the receiving terminal device sends a DTMF password, and if it is correct, the corresponding output port is triggered. The default is 1234.	
reset code	After receiving the corresponding instruction, the test device will reset the state and stop playing the corresponding ringtone.	
Active Url triggers	When device receives the active URI trigger message sent by the remote device and if it is correct, the corresponding output port will be triggered. You can choose to enable or disable ringtones.	
Trigger message	When the test device receives the right trigger message, the output port will be triggered.	
Reset message	When the test device receives the right reset message, the device will reset its status and stop playing the corresponding ringtone.	
Remote SMS trigger	Enable or disable remote SMS triggering. You can choose to enable or disable ringtones.	
Trigger Message Alert	Send instructions on remote devices or servers, ALERT= [set instructions], if correct, trigger the corresponding port output.	
Call State Trigger	Continued triggering the output port by device's call status. For example, When the call triggers the output port, the output will be triggered while the call status does not change. 1. Talking 2. Talking and Ringing 3. Ringing 4. Calling 5. Calling and Talking 6. Calling and Talking (dialling) 7. Calling and Ringing 8. Calling and Ringing (called) 9. Calling, Ringing and Talking	
Server Settings		
Server Address	Send message to the server when the alarm is triggered. Message format: Alarm Info: Description = intercom;SIP User= Mac= 00:a8:34:68:23:d1 IP= 172.18.90.235 port=Input1	

6.26 Function Key >> Function Key Settings

6.26.1 Key Event

The speed dial key type could be set as Key Event.



Function Key Settings

☐ Input port Multiplexing as DSS Key2

Key	Type	Number 1	Number 2	Line	Subtype
DSS Key 1	Key Event			SIP1	Release
DSS Key 2	None			SIP1	None

Advanced Settings

Use Function Key to Answer:

Enable Speed Dial Hangup:

Hot Key Dial Mode Select:

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

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

Picture 38. Function Key Settings

Table 20. Function Key Settings

Type	Subtype	Usage
Key Event	None	No responding
	Release	Delete password input, cancel dialling input and end call
	OK	Confirm key
	Call Back	The user can redial the last number dialled
	Redial	Call the nearest missed number
	Handfree	Use as a hands-free button
	VOL UP	Turn up volume
	VOL DOWN	Turn down volume

6.26.2 Hot Key

When the speed dial key is set as Hot Key, the device will dial pre-set telephone number. The number option can also be configured with IP address. User can press the speed dial button to make direct IP call.

Function Key Settings

☐ Input port Multiplexing as DSS Key2

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

Advanced Settings

Use Function Key to Answer

Enable

Enable Speed Dial Hangup

Enable

Hot Key Dial Mode Select

Day-Night

Call Switched Time

16

(5~50)Second(s)

Day Start Time

09:00

(00:00~23:59)

Day End Time

18:00

(00:00~23:59)

Apply

Picture 39. Hot Key Settings

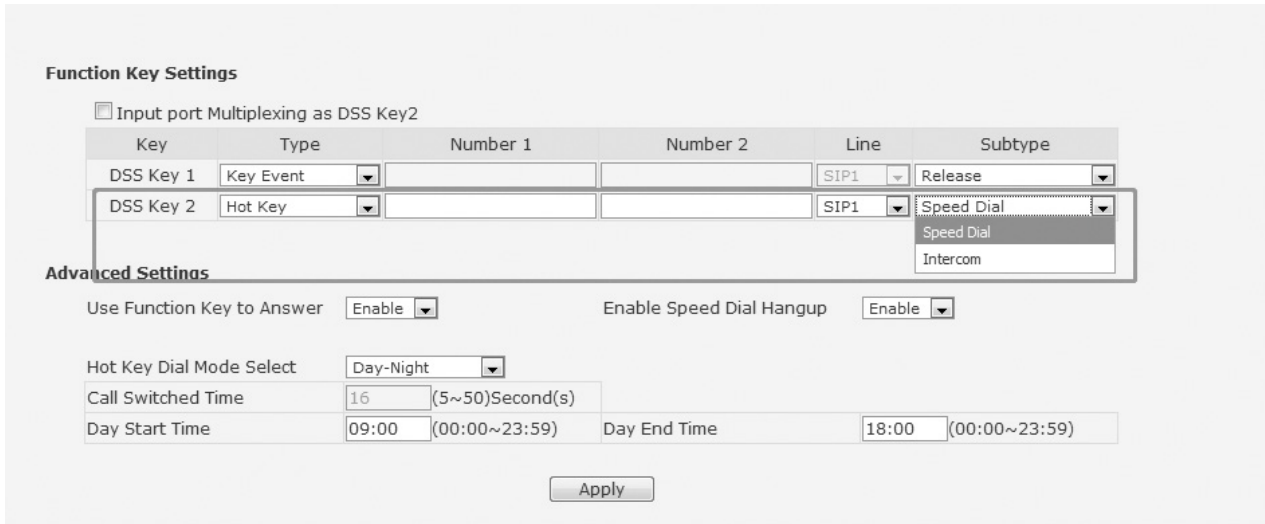
Table 21. Hot Key Settings

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.

6.26.3 Multicast

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

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



Picture 40. Multicast Settings

Table 22. Multicast Settings

Type	Number	Subtype	Usage
Multicast	Set the host IP address and port number, they must be separated by a colon (The IP address range is 224.0.0.0 to 239.255.255.255, and the port number is preferably set between 1024 and 65535).	G.711A	Narrowband speech coding (4 KHz)
		G.711U	
		G.722	Wideband speech coding (7 KHz)
		G.723.1	Narrowband speech coding (4 KHz)
		G.726-32	
		G.729AB	

6.26.4 PTT

Keep pressing the shortcut key set to make a call, release it and hang up.

Function Key Settings

☐ Input port Multiplexing as DSS Key2

Key	Type	Number 1	Number 2	Line	Subtype
DSS Key 1	Key Event			SIP1	Release
DSS Key 2	PTT			SIP1	Speed Dial

Advanced Settings

Use Function Key to Answer

Enable

Enable Speed Dial Hangup

Enable

Hot Key Dial Mode Select

Day-Night

Call Switched Time

16

(5~50)Second(s)

Day Start Time

09:00

(00:00~23:59)

Day End Time

18:00

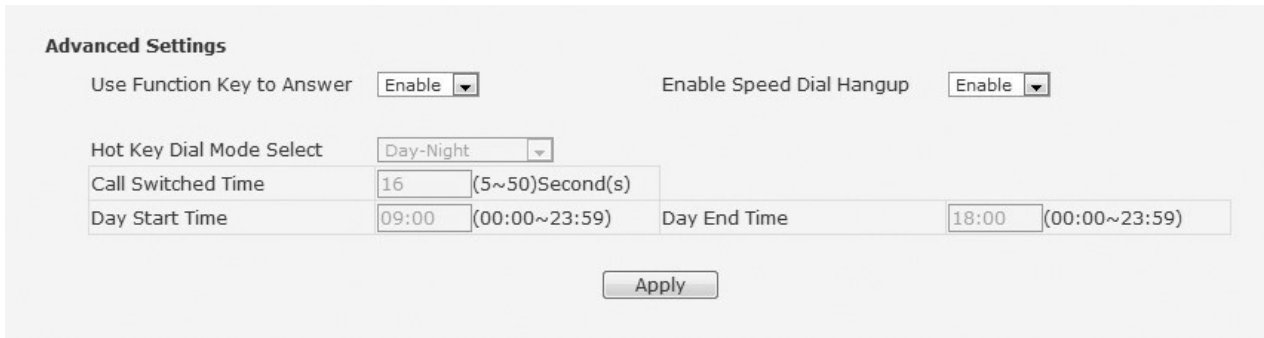
(00:00~23:59)

Apply

Picture 41. PTT Settings

6.26.5 Advanced Settings

Keep pressing the shortcut key set to make a call, release it and hang up.



Advanced Settings

Use Function Key to Answer

Enable Speed Dial Hangup

Hot Key Dial Mode Select

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

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

Picture 42. Advanced Settings

Table 23. Advanced Settings

Field Name	Explanation
Input port is multiplexed as function key 2	Enable or disable the input port to be multiplexed as speed dial button 2.
Use Function Key to Answer	Enable or disable shortcuts to answer calls.
Enable Speed Dial Hang up	Enable or disable shortcuts to hang up calls.
Hot Key Dial Mode Select	Number 1 call number 2 mode selection. < Main / Secondary > : If the first number is not answered within the set time, the second number will be automatically switched. < Day / Night >: The system time is automatically detected during the call. If it is daytime, the first number is called, otherwise the second number is called.
Call Switched Time	Set number 1 to call number 2 time, default 16 seconds.
Day Start Time	The start time of the day when the <Day/Night> mode is defined. Default "06:00".
Day End Time	The end time of the day when the <Day/Night> mode is defined. Default "18:00".

7. Trouble Shooting

When the device is not working properly, users can try the following methods to restore the device to normal operation or collect relevant information to send a problem report to the Ambient System technical support mailbox.

7.1 Get device system information

Users can obtain information through the **[System] >> [Information]** option on the device webpage. The following information will be provided:

Device information (model, software and hardware version) and Internet Information etc.

7.2 Reboot device

The user can restart the device through the webpage, click **[System] >> [Tools] >> [Reboot Phone]** and Click **[Reboot]** button, or directly unplug the power to restart the device.

7.3 Device factory reset

Restoring the factory settings will delete all configuration, database and configuration files on the device and the device will be restored to the factory default state.

To restore the factory settings, you need to log in to the webpage **[System] >> [Configuration]**, and click **[Reset]** button, the device will return to the factory default state.

7.4 Network Packets Capture

In order to obtain the data packet of the device, the user needs to log in to the webpage of the device, open the webpage **[System] >> [Tools]**, and click the **[Start]** option in the "Network Packets Capture". A message will pop up asking the user to save the captured file. At this time, the user can perform related operations, such as starting/deactivating the line or making a call, and clicking the **[Stop]** button on the webpage after completion. Network packets during the device are saved in a file. Users can analyze the packet or send it to the Ambient System Technical Support mailbox.

7.5 Common Trouble Cases

Table 25. Common Trouble Cases

Trouble Case	Solution
Device could not boot up	1. If the device enters "POST mode" (the SIP/NET and function button indicators are always on), the device system is damaged. Please contact your location technical support to help you restore your equipment system. 2. If the device enters "POST mode" (the SIP/NET and function button indicators are always on), the device system is damaged. Please contact your location technical support to help you restore your equipment system.
Device could not register to a service provider	1. Please check if the device is connected to the network. The network cable must be connected to the  [Network] interface instead of the  [Camera] interface. 2. If the network connection is good, please check your line configuration again. If all configurations are correct, contact your service provider for support, or follow the instructions in "10.4 Network Data Capture" to obtain a registered network packet and send it to the Ambient System Support Email to help analyze the issue.

>



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