We make everyday life safer

SIP Intercom Station

ICO EMERGENCY 01

EN

User Manual

ver. 12.2021

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

Table of Contents

1. Safety

	Danger! **High risk:** This symbol indicates an imminently hazardous situation such as "Dangerous Voltage" inside the product. If not avoided, this will result in an electrical shock, serious bodily injury, or death.
	Warning! **Medium risk:** Indicates a potentially hazardous situation. If not avoided, this could result in minor or moderate bodily injury.
	Caution! **Low risk:** Indicates a potentially hazardous situation. If not avoided, this could result in property damage or risk of damage to the unit.

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

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

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

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

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

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

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

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

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

Note for power connections

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

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

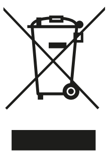
This label may appear on the bottom of the apparatus due to space limitations.

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

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

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

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



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

Only used at altitude not exceeding 2000 m.

Only used in non-tropical climate regions.

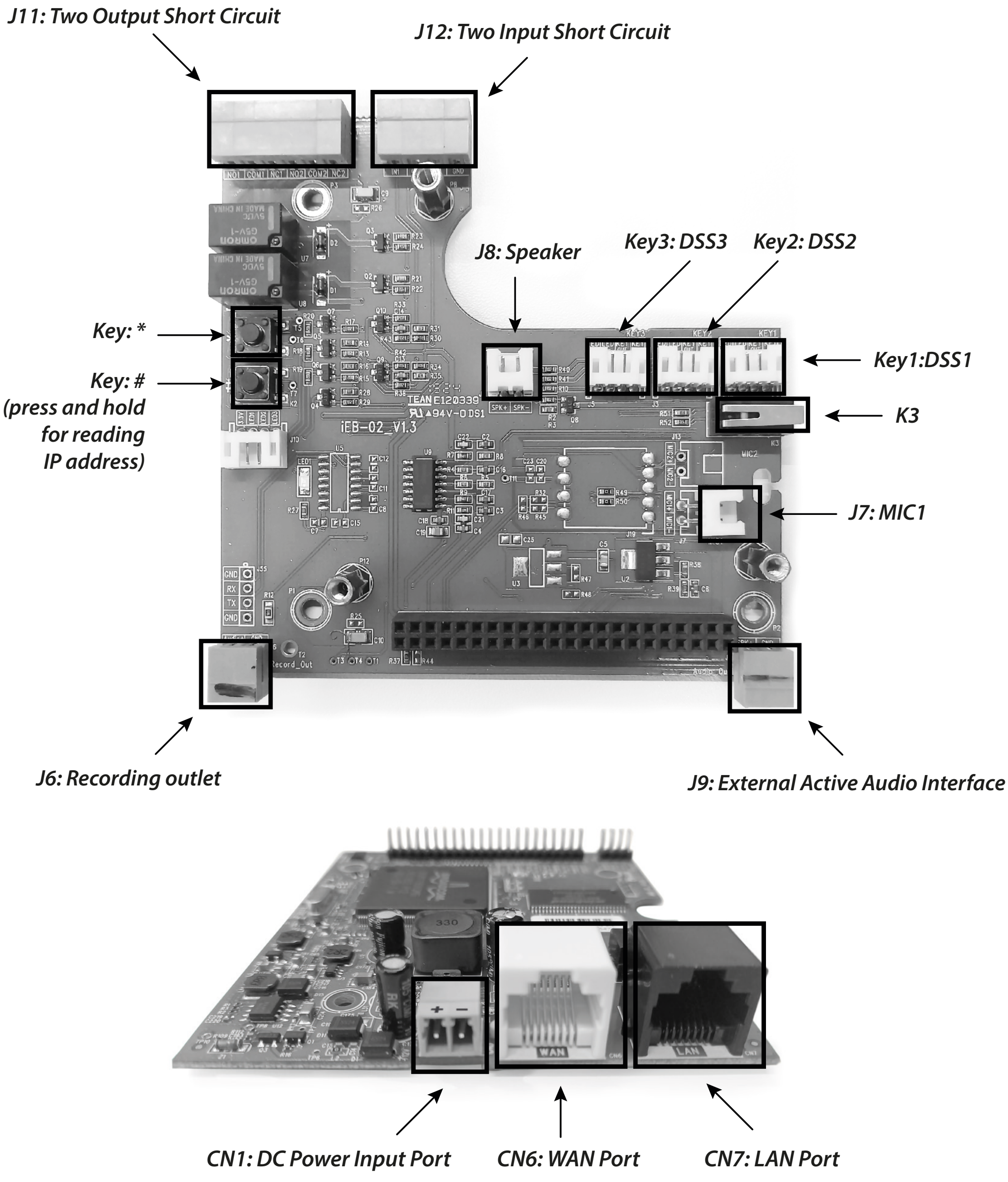
2. Overview

ICO EMERGENCY is an intercom designed to ensure high-quality communication with the highest priority in emergency situations, a special button located behind the breakable glass reduces the number of accidental connections, The intercom can establish a conversation between the reporting person and the facility security room or directly with the security services, thus shortening reaction time to an event to a minimum. In addition to the alarm button, it also has from 1 to 3 standard buttons, used for normal object communication. Intercom has 3 versions of mounting: plasterboard, flush and wall mount.

3. Installation Guide

3.1 Interfaces Speceification

3.1.1 Network and power supply schematics



Picture 1. Schematics for network and power supply

3.1.2 Port description

Table 1. Port description and feature

Port	Description	Feature
CN1	DC Power Input Port	Input Range: +10~+14V/1.5A DC (Notice: Plus and minus connection of the power)
CN6	WAN Port	10M/100M Adaptive Ethernet port, connected to the network
CN7	LAN Port	10M/100M Adaptive Ethetnet port, connected to the computer (which can be configured to routing mode, or to bridge mode)
J9	External Active Speakers Port	One is the audio signal line, one is the GND line (Please connect to the GND line, otherwise there will be noise)
J8	Audio Recording Output Port	By mixing equipment and remote call voice output. One is the audio signal line, one is the GND line (Please connect to the GND line, otherwise there will be noise)
Key1 / Key2 / Key3	DSS Key Port (programmable keys)	Function keys. Here can be difined hot keys, function keys (such as hanging up, hands-free), multicast keys
J11	Output Control Port	Used to control electric locks, alarm lamp and other, Rated voltage: 12 VDC , Max DC: 1A/24 VDC Max AC: 0,5A / 125 VAC
J12	Short Circuit Input Detection Port	Used to connect to infrared detector, magnetic switch, vibration sensor and other input devices
K3	Tamper Switch	To prevent the remove of host. Need to be reset server or web after the alarm ring

3.2 Use POE or external Power Adapter

Intercom supports two power supply methods, external power adapter and Ethernet (POE) switch power supply mechanism.

The POE power supply mode saves space and the cost of additional power sockets. Intercom is connected to the POE switch through a network cable to play the role of power supply and data transmission. By connecting to the POE switch of the UPS system, the intercom can continue to work even if the power is cut off, just like a traditional PSTN phone powered by a telephone line.

Users who do not have POE equipment can also use traditional power adapters. If the intercom is connected to the POE switch and the power adapter at the same time, the POE power supply is preferred. If the POE power supply fails, it will be switched to the power adapter.

In order to ensure the normal operation of the equipment, please use the power adapter specified by Ambient System and the POE switch that meets the equipment standard.

3.2.1 Common Command Mode

Table 2. Common command mode

Action	Description
IP Broadcast under standby mode	In standby, long press the speed dial key 10, there will be a beep and the indicator will flash quickly for 5 seconds, 5 seconds. Press the speed dial key once inside, the beep sound stops and the IP is automatically reported.
Switch network mode	In the standby mode, press and hold the speed dial button for 10 seconds, there will be a beep and the indicator will flash quickly for 5 seconds. Within 5 seconds, quickly press the speed dial key three times 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, report IP after successful switching.

3.2.2 Function Key LED State

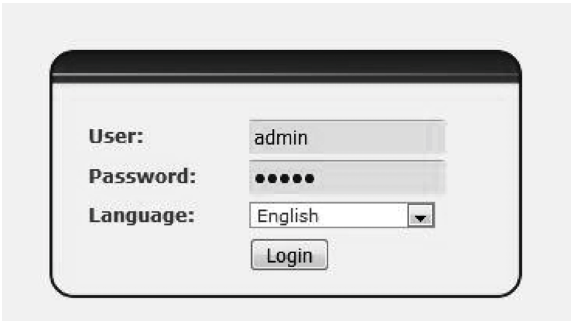
Table 3. Function key LED state

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

4. User Getting Started

4.1 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://192.168.1.128 and you can see the login interface of the web page management.



Picture 2. WEB login

⚠ *The username and password should be correct to log in to the web page. The default username and password are "admin"*

4.2 SIP Configuration

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.

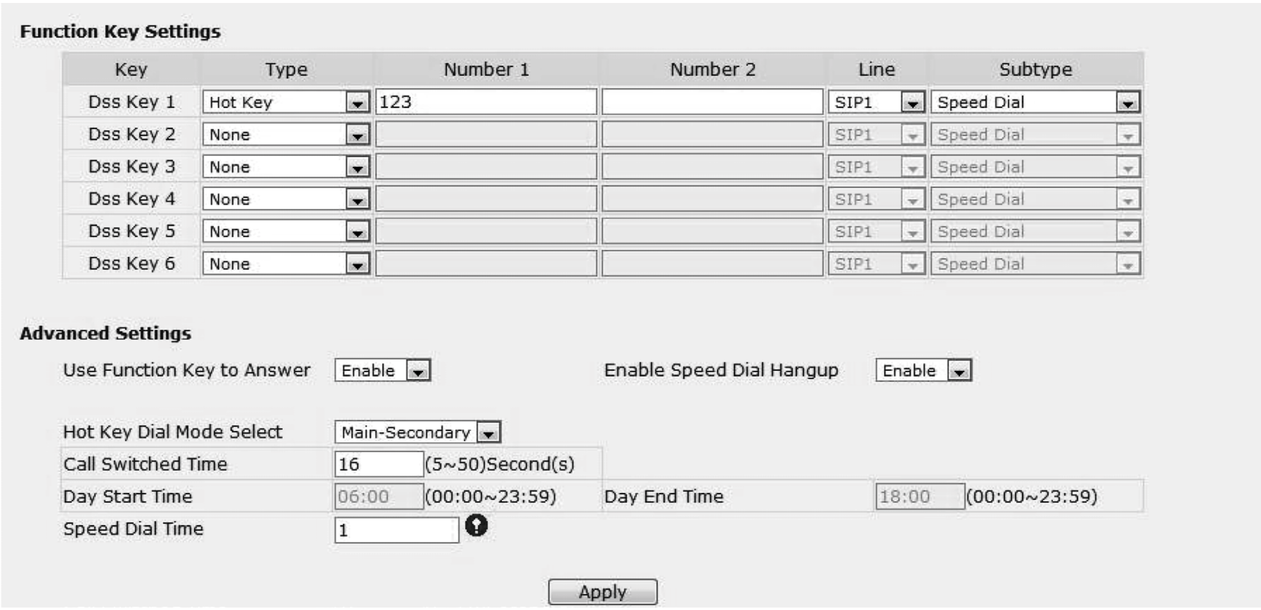
» WEB interface: After login into the phone page, enter [Line] >> [SIP] and select SIP1/SIP2 for configuration, click apply to complete registration after configuration, as shown below:

Picture 3. SIP registration

5. Basic Functions

5.1 Making calls

After setting the shortcut key as Hot key and setting the number, press the shortcut key to immediately call out the set number, the settings are as follows:



Picture 4. Hotkey setting

⚠ *See detailed configuration instructions 7.25 Function Key*

5.2 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.

5.3 End of the Call

Function Key Settings

Key	Type	Number 1	Number 2	Line	Subtype
Dss Key 1	Key Event			SIP1	Release
Dss Key 2	None			SIP1	Speed Dial
Dss Key 3	None			SIP1	Speed Dial
Dss Key 4	None			SIP1	Speed Dial
Dss Key 5	None			SIP1	Speed Dial
Dss Key 6	None			SIP1	Speed Dial

Picture 5. Function key 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 7.25 Function Key.*

5.4 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 Setting] >> [Features], Enable auto answer, set mode and auto answer time and click submit.

Limit Talk Duration	Disable	Talk Duration	120 (20~600) Second(s)
DND Mode	Phone	Ban Outgoing	☐
Enable Call Waiting	☑	Enable Call Waiting Tone	☑
Enable Intercom	☑	Enable Intercom Barge	☑
Enable Intercom Mute	☑		
Enable Auto Dial Out	☑	Auto Dial Out Time	5 (3~30)Second(s)
Enable Auto Answer	Lines and IP Call	Auto Answer Timeout	0 (0~60)Second(s)
Dial Fixed Length to Send	☑	Send length	4
Voice Read IP	Enable	System Language	English
Description		Enable DND	☐
HangUp Delay	3 Second(s)(1~60)	Call Timeout	90 (1~3600)Second(s)
Dial Number Voice Play	Disable	Ring Timeout	120 (1~3600)Second(s)
Hotline Number		Hotline Delay	0 (0~9)Second(s)

Apply

Picture 6. 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)

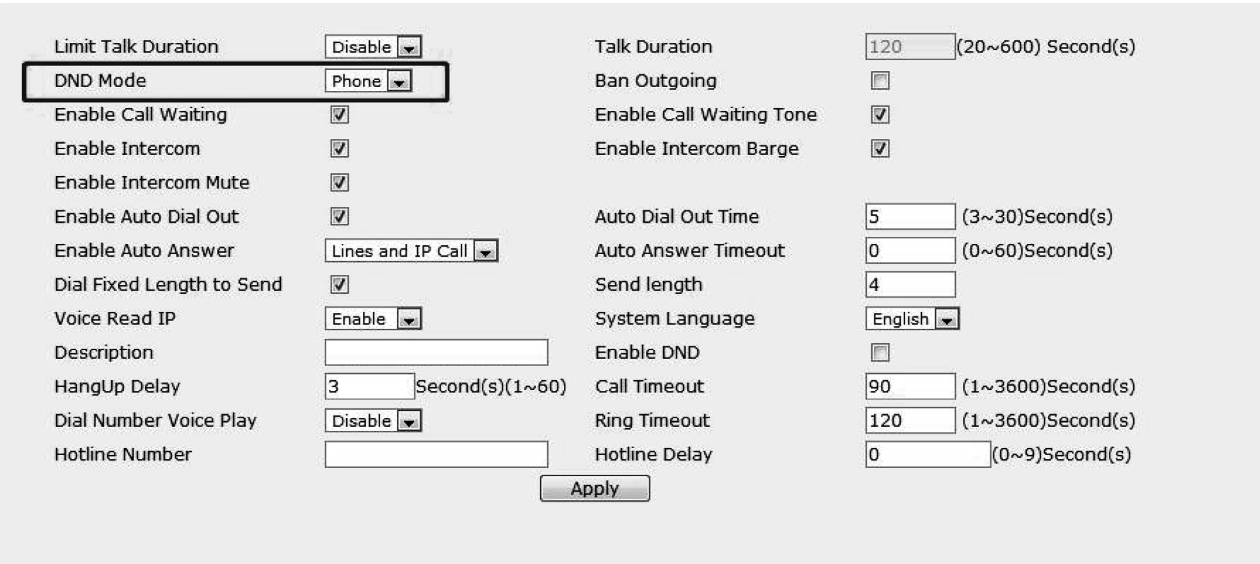
The range can be set to 0~60s , and the call will be answered automatically when the timeout is set.

5.5 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:

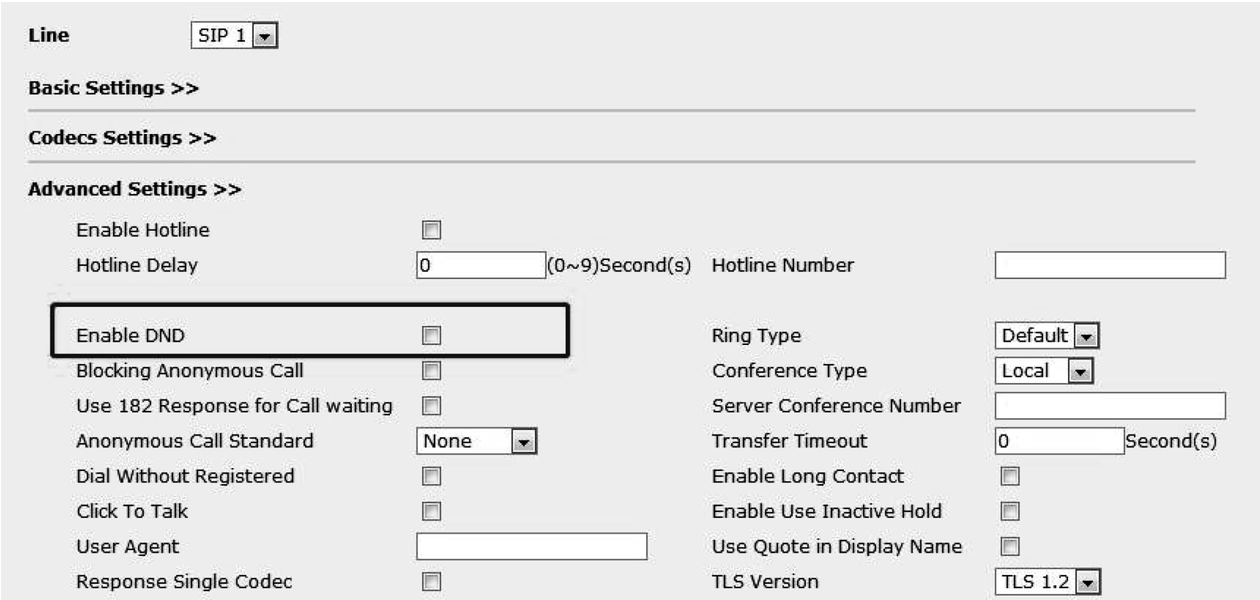
» Web interface: enter [Intercom Setting] >> [Features], set the DND Mode to phone and Enable DND.



Picture 7. Set DND option

Turn on/off the DND of a specific line of the device, as follows:

» enter [Line] >> [SIP], choose a Line and enter [Line] >> [Advanced settings], Enable DND.



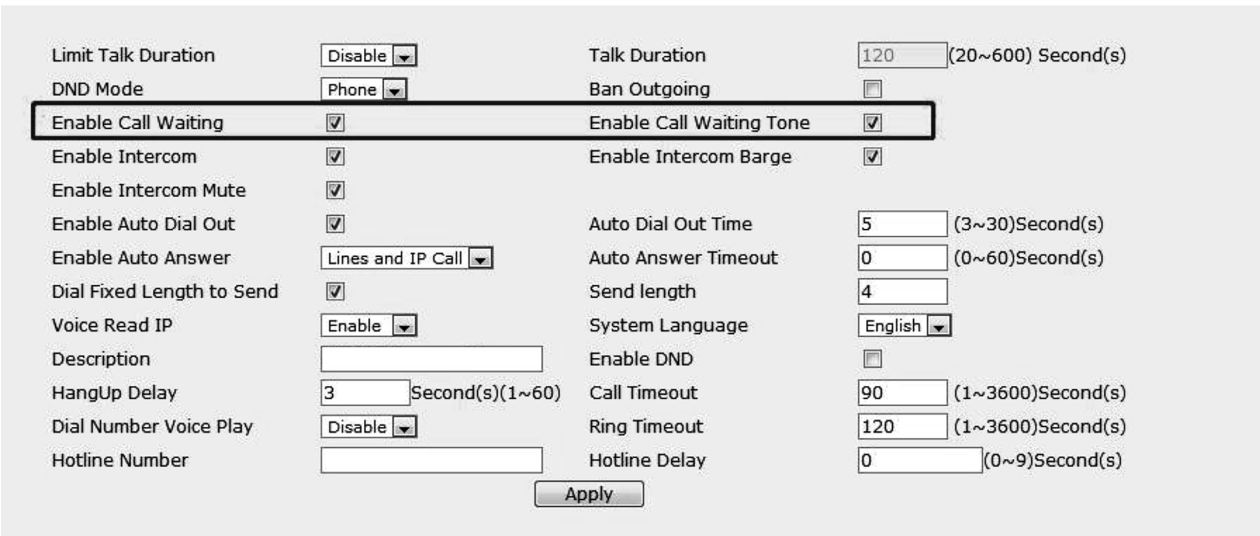
Picture 8. Enable do not disturb on a certain line

5.6 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 during a call, the device will sound a beep-beep tone.

Users can enable/disable call waiting in the device interface and the web interface.

- Web interface: enter [Intercom Setting] >> [Features], enable/disable call waiting, enable/disable call waiting tone.

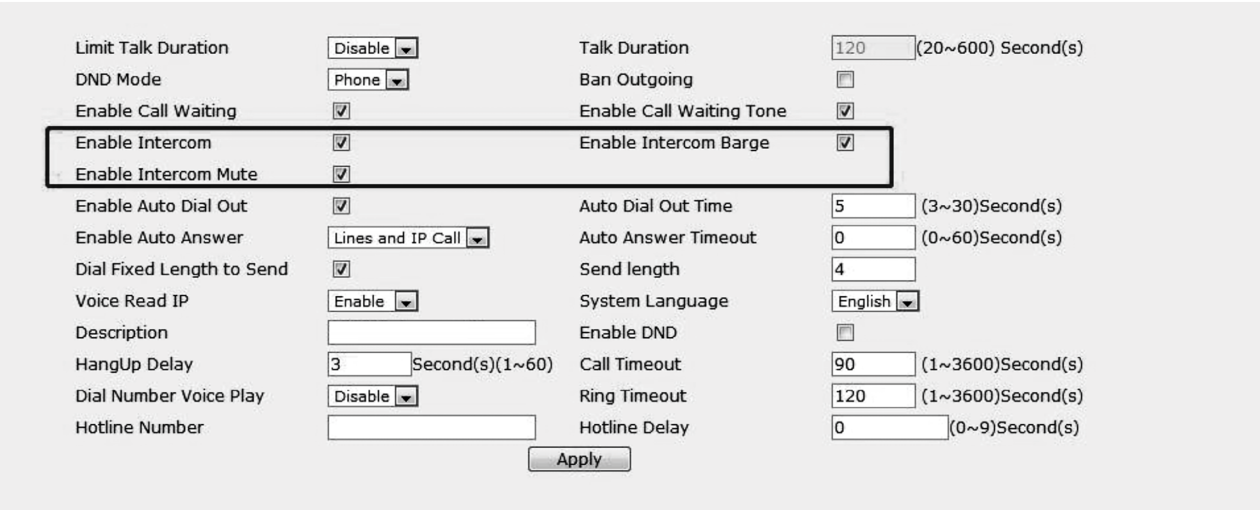


Picture 9. Web page setting call waiting

6. Advanced Functions

6.1 Intercom

When there is an intercom call, the device can answer it automatically.



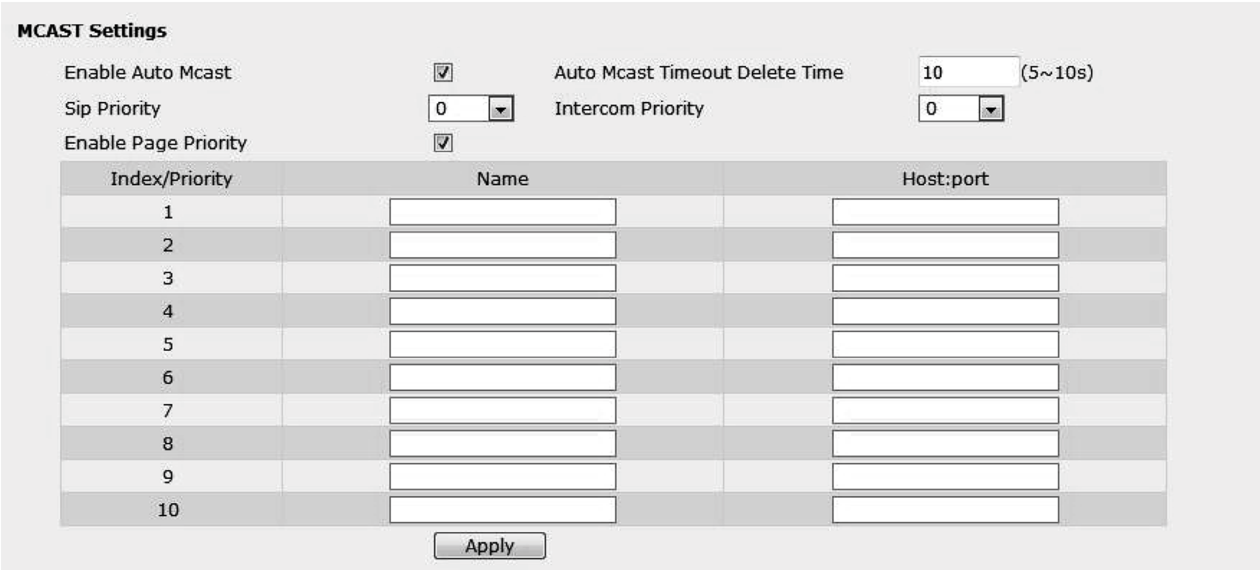
Picture 10. Web intercom

Table 4. Intercom

Parameters	Description
Enable intercom	When the intercom system is enabled, the device will accept the SIP header Call-Info of the incoming call request instruction to answer the phone automatically.
Enable intercom barge	Automatically answer the call in intercom mode during the call, if the current call is in intercom mode, refuse to answer the new intercom mode.
Enable intercom mute	Turn on the mute function during an intercom mode call.

6.2 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 11. 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.
Priority	The priority defined in the current call, 1 is the highest priority and 10 is the lowest.
Enable page prority	Regardless of which of the two multicast groups is called in first, the device will receive the higher priority multicast first.
Name	Listened multicast server name.
Priority	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 DSSKY of Multicast Key which you set.
- Receive end will receive multicast call and play multicast automatically.

6.3 Hotspot

SIP hotspot is a simple utility. Its configuration is simple, can realize the function of group vibration, can expand the number of SIP account.

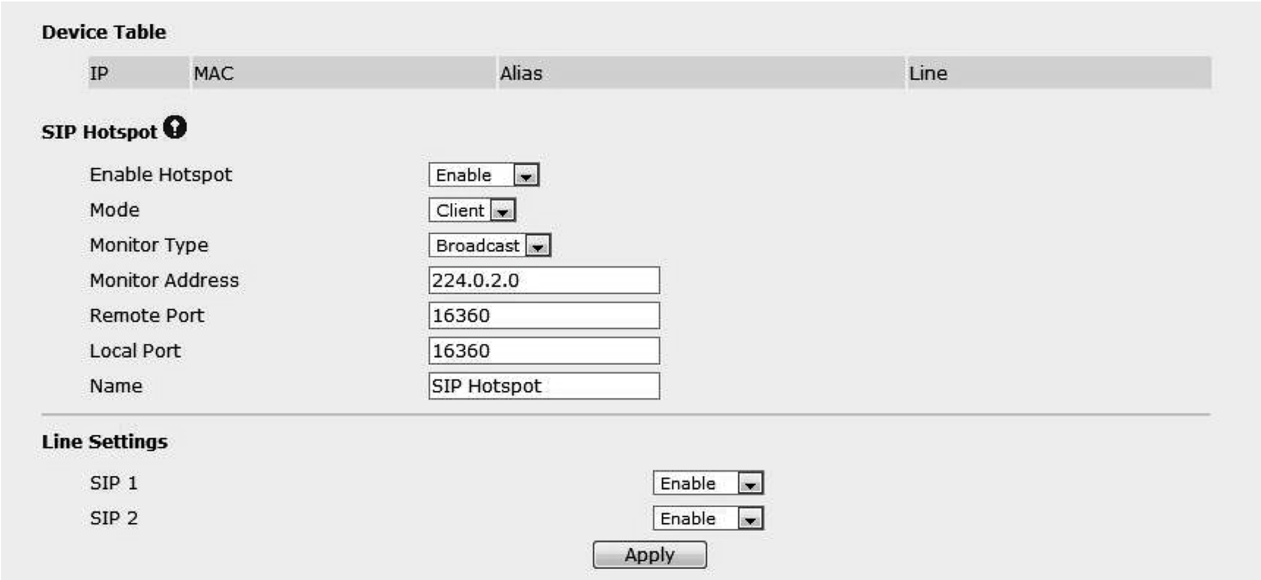
Take one device A as the SIP hotspot and the other devices (B, C) as the SIP hotspot client. When someone calls device A, devices A, B, and C will ring, and if any of them answer, the other devices will stop ringing and not be able to answer at the same time. When A B or C device is called out, it is called out with A SIP number registered with device A.

Table 6. SIP Hotspot

Parameters	Description
Enable hotspot	Set the enable hotspot option in the SIP hotspot configuration TAB to enabled.
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.



Picture 12. 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.

7. Web Configuration

7.1 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

7.2 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

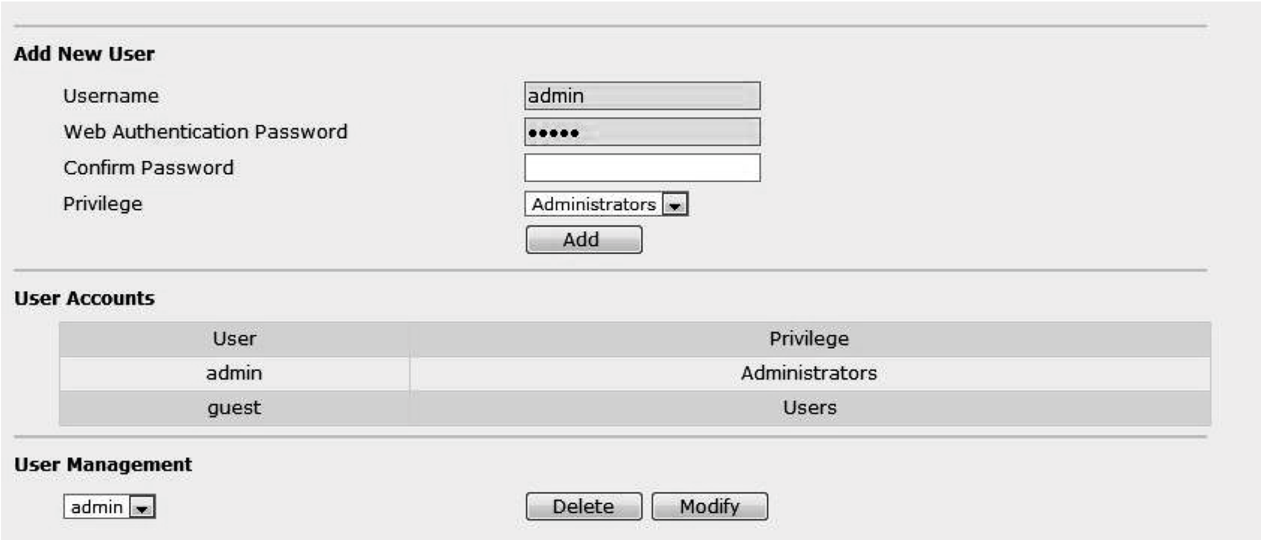
» Default Gateway

Besides, summarization of SIP account status:

» SIP User

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

7.3 System >> Account

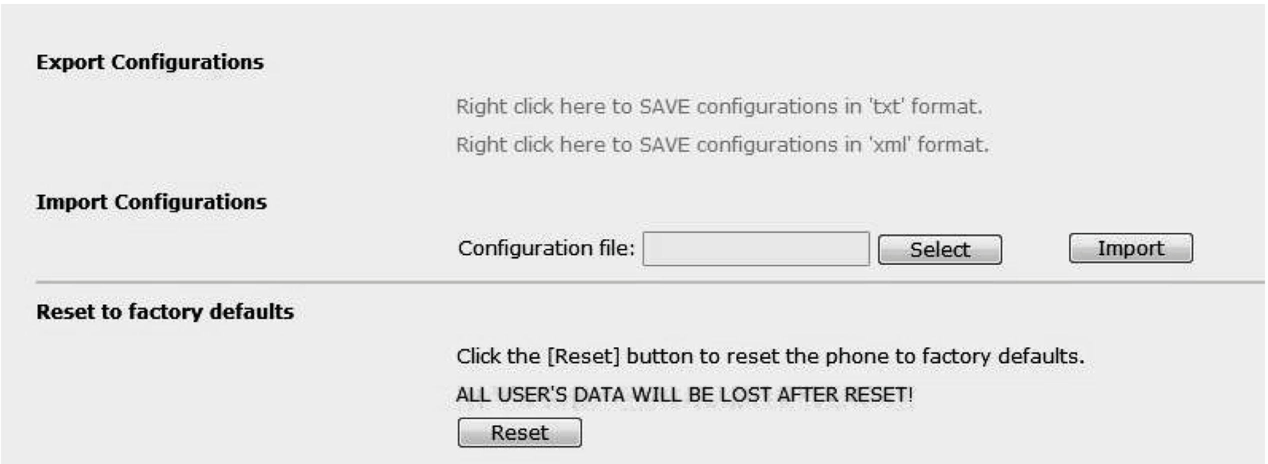


Picture 13. Web account

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.

7.4 System >> Configurations

Users with administrator rights can view, export or import device configuration on this page, and can also restore the device to factory settings.



Picture 14. System setting

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

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.

7.5 System >> Upgrade

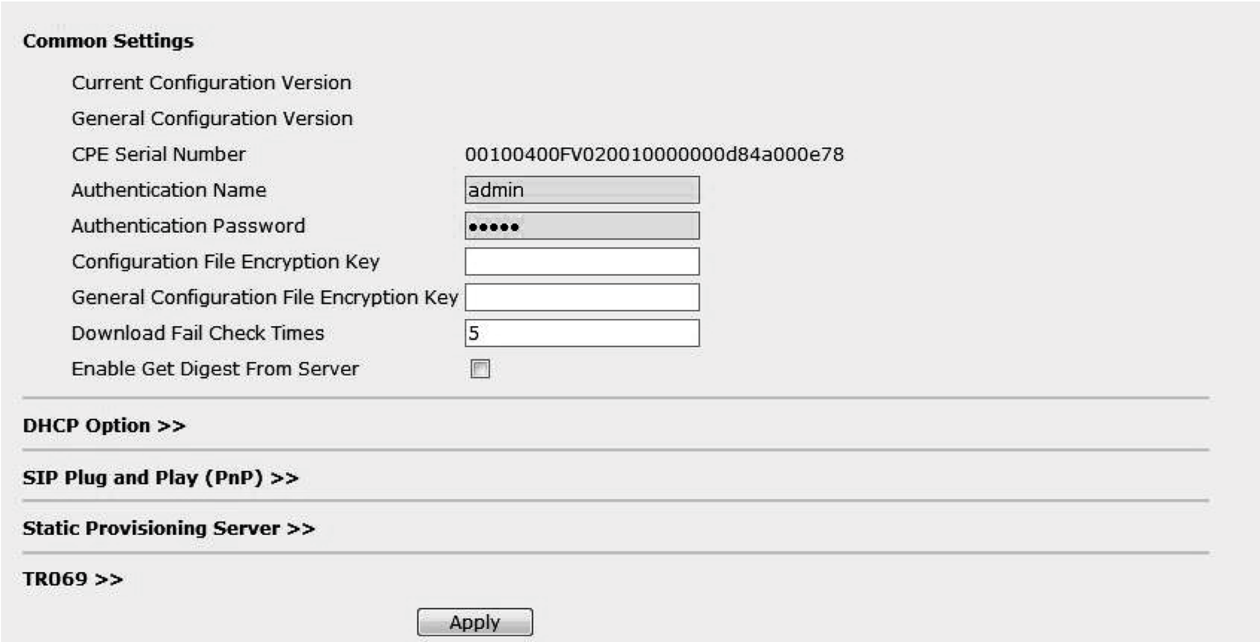
Picture 15. Upgrade

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.

7.6 System >> Auto Provision

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

Upgrade the device software version and upgrade to the new version through the web page. After the upgrade is completed, the device will automatically restart and update to the new version. Click select, select the version and click upgrade.



Picture 16. Auto provision

Intercom 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:

PNP>DHCP>TR069> Static Provisioning
Transferring protocol: FTP, TFTP, HTTP, HTTPS

Table 7. Auto provision

Parameters	Description
Basic 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.

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

7.7 System >> Tools

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

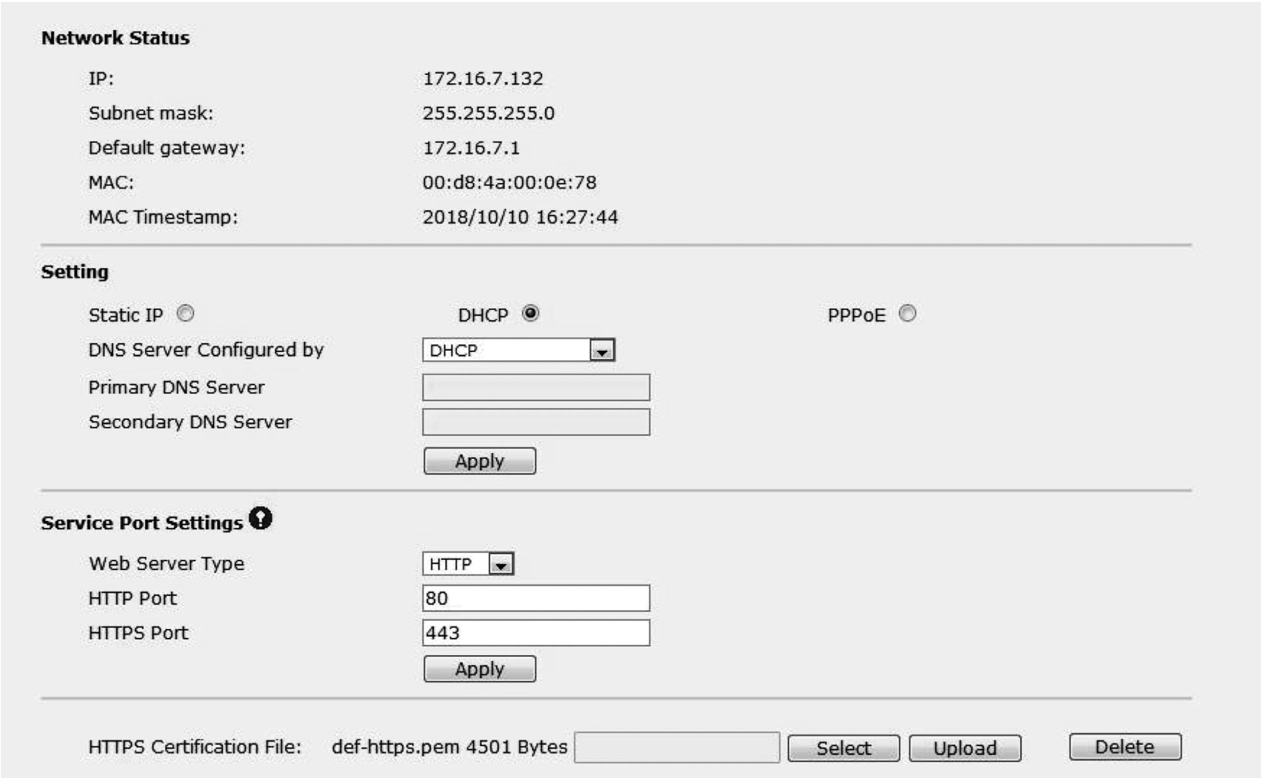
Picture 17. Tools

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 technical support.

7.8 Network >> Basic

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



Picture 18. Network basic settings

Table 8. 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.

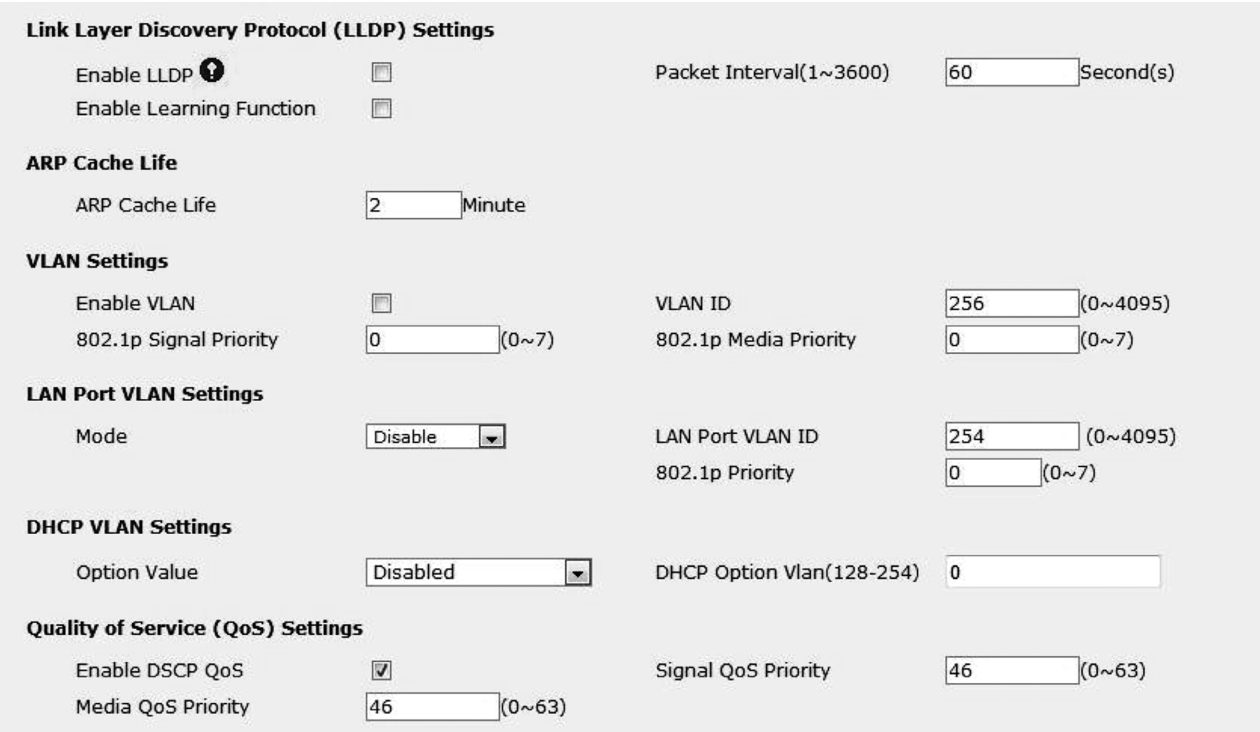
PPPoE	Account and Password must be input manually. These are provided by your ISP.
If Static IP is chosen, the screen below will appear. Enter values provided by the ISP.	
DNS Server Configured by	Select the Configured mode of the DNS Server.
Primary DNS Server	Enter the server address of the Primary 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.

7.9 Network >> Advanced



Picture 19. Basic network settings

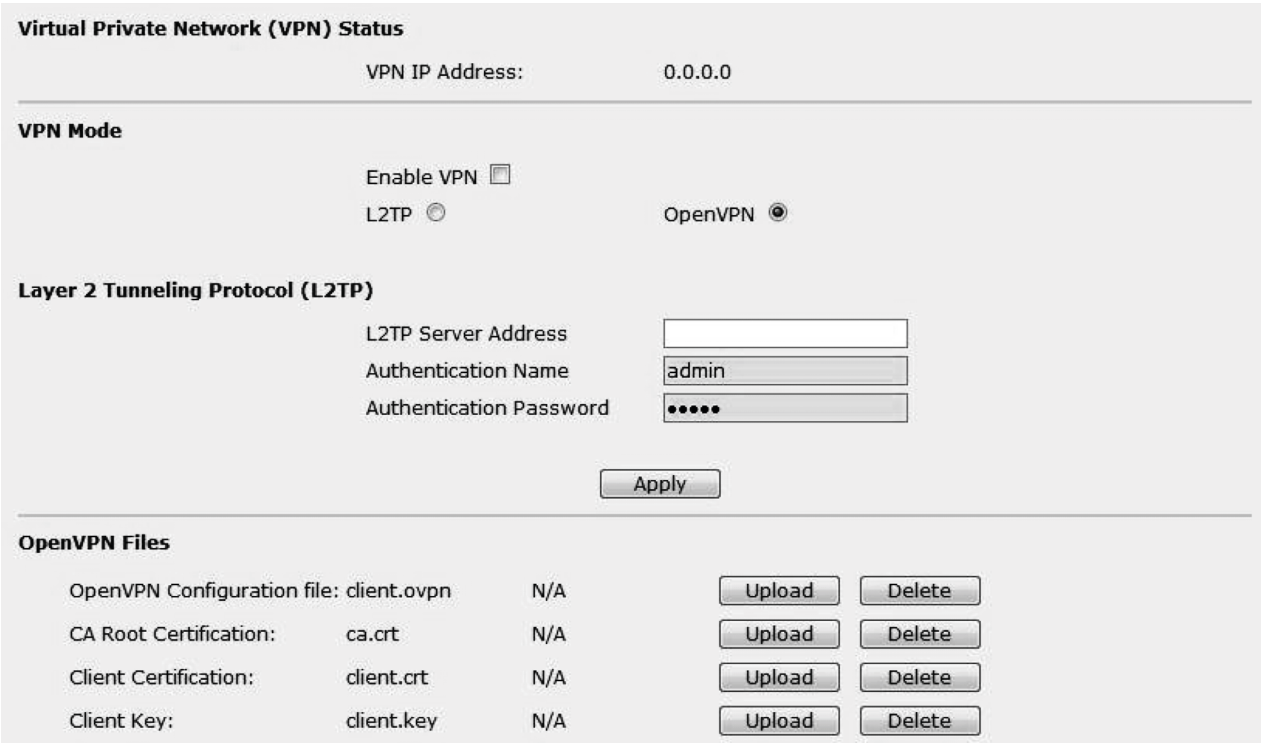
Network advanced Settings are typically configured by IT administrators to improve the quality of device service.

Picture 20. Basic network parameters

Field Name	Explanation
LLDP Settings	
Report	Enable LLDP
Interval	LLDP requests interval time
Learning	Apply the learned VLAN ID to the phone configuration
QoS Settings	
QoS Mode	Voice quality assurance (off by default)
DHCP VLAN Settings	
Parameter value	128-254, get the VLAN value through DHCP
WAN VLAN	
WAN VLAN	WAN port VLAN configuration

LAN VLAN	
LAN VLAN	LAN port VLAN configuration

7.10 Network >> VPN



Picture 21. 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

⚠ *NOTICE! 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.

<u>OpenVPN</u>

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:

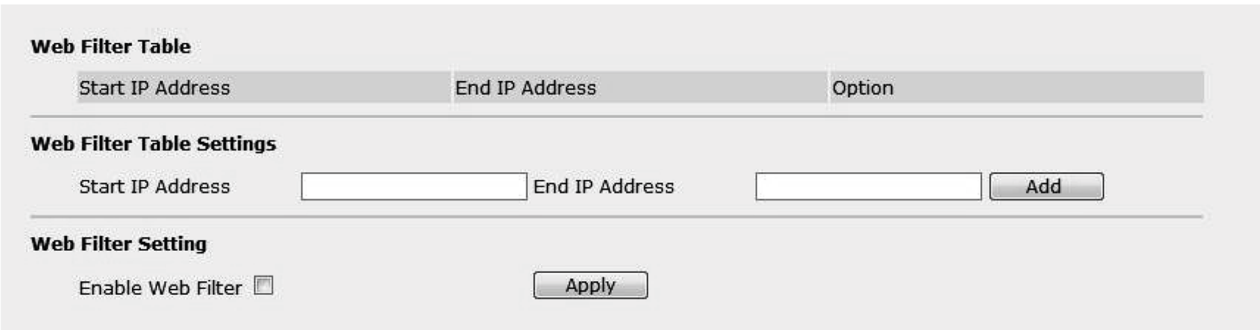
- OpenVPN Configuration file: client.ovpn
- CA Root Certification: ca.crt
- Client Certification: client.crt
- Client Key: client.key

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.

7.11 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.



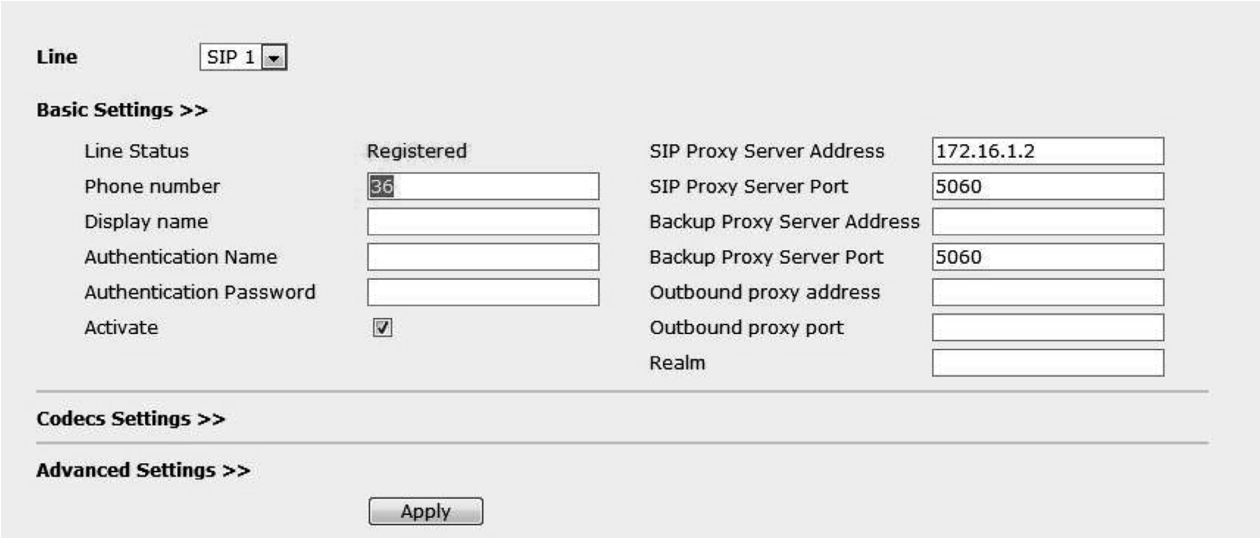
Picture 22. Web filter table

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.*

7.12 Line >> SIP

Configure the service configuration for the wire on this page.



Picture 23. SIP

Table 9. SIP

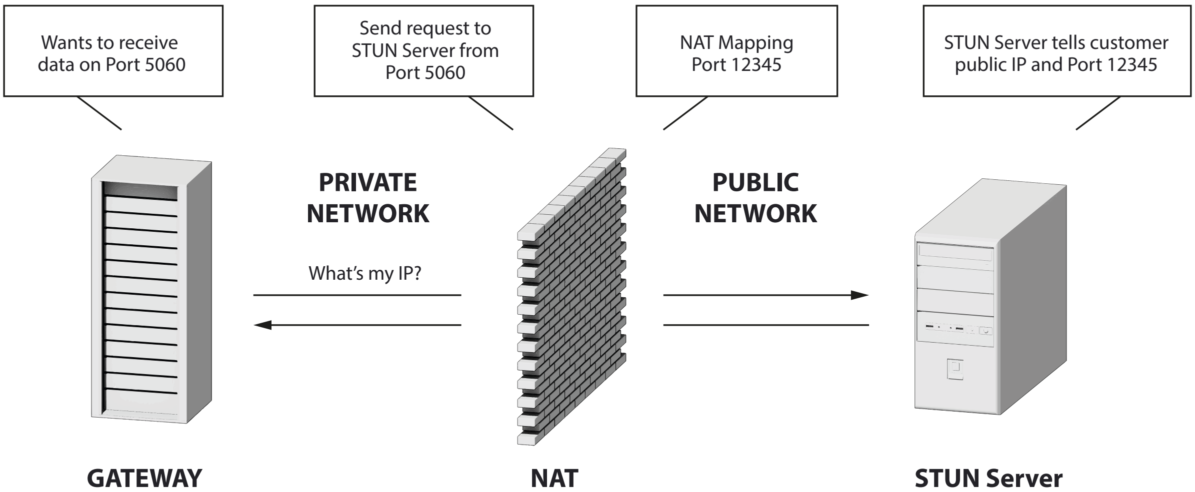
Field Name	Explanation
Basic settings (Choose the SIP line to configured)	
Line Status	Display the current line status at page loading. To get the up to date line status, user has to refresh the page manually.
Username	Enter the username of the service account.
Display name	Enter the display name to 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.	

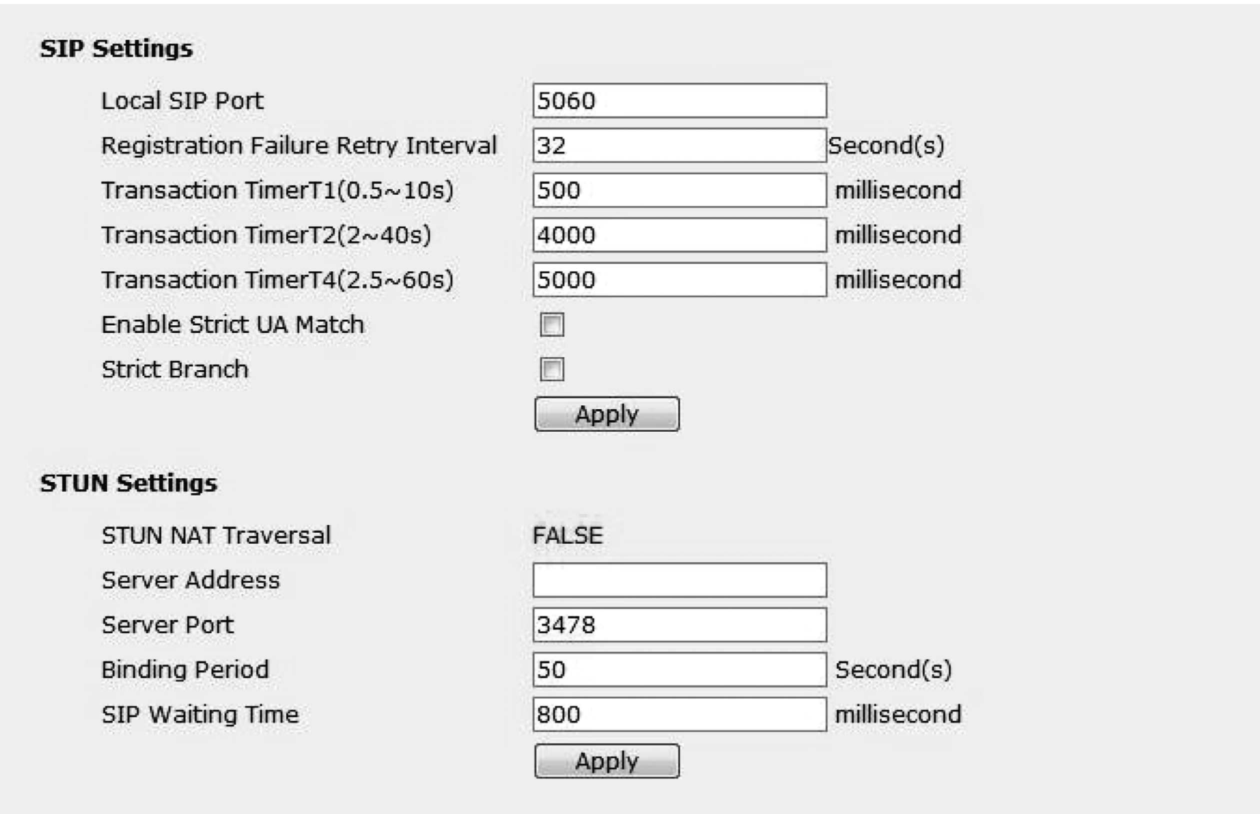
Advanced Settings	
Subscribe For Voice Message	Enable the device to subscribe a voice message waiting notification, if enabled, the device will receive notification from the server if there is voice message waiting on the server.
Voice Message Number	Set the number for retrieving voice message.
Voice 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 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.
Use Quote in Display Name	Whether to add quote in display name.
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 Report	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.
With Mac field	When enabled, all SIP messages strip Mac fields.
Register with the Mac field	When enabled, register the message ribbon Mac field.

7.13 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.





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 24. Line basic setting

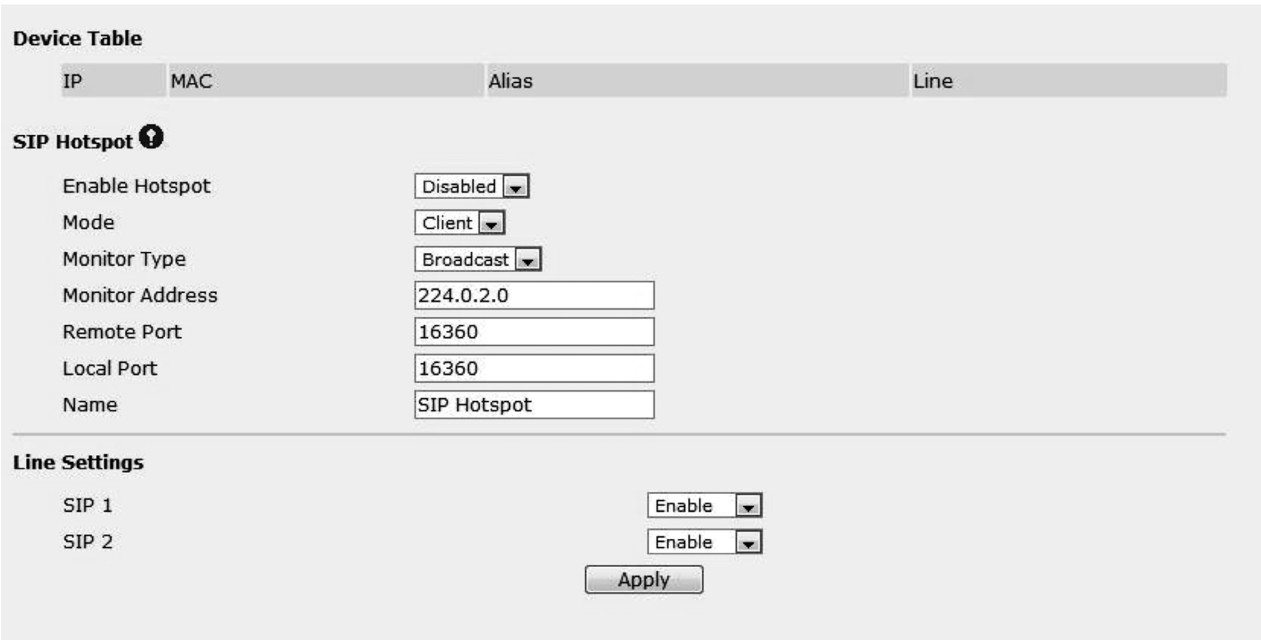
Table 10. Line Basic Setting

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.

7.14 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.*

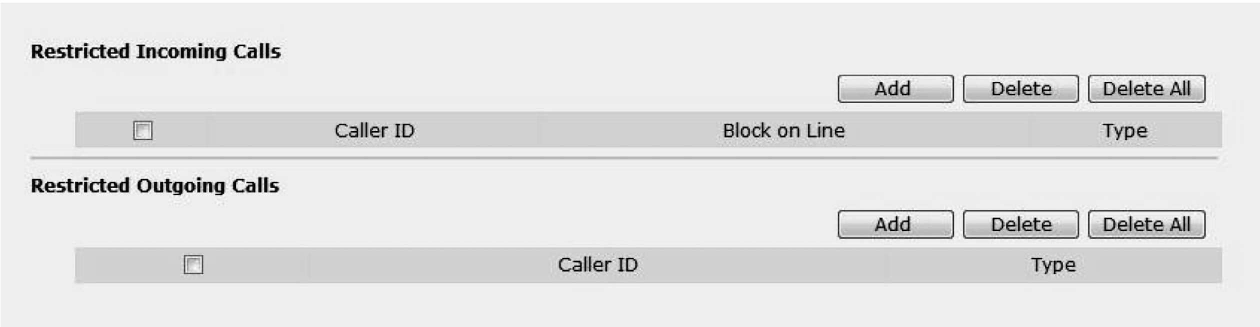


Picture 25. SIP Hotspot

7.15 Line >> Blacklist

Web page to add call limit function, you can set the number or prefix to limit calls. The rules are as follows:

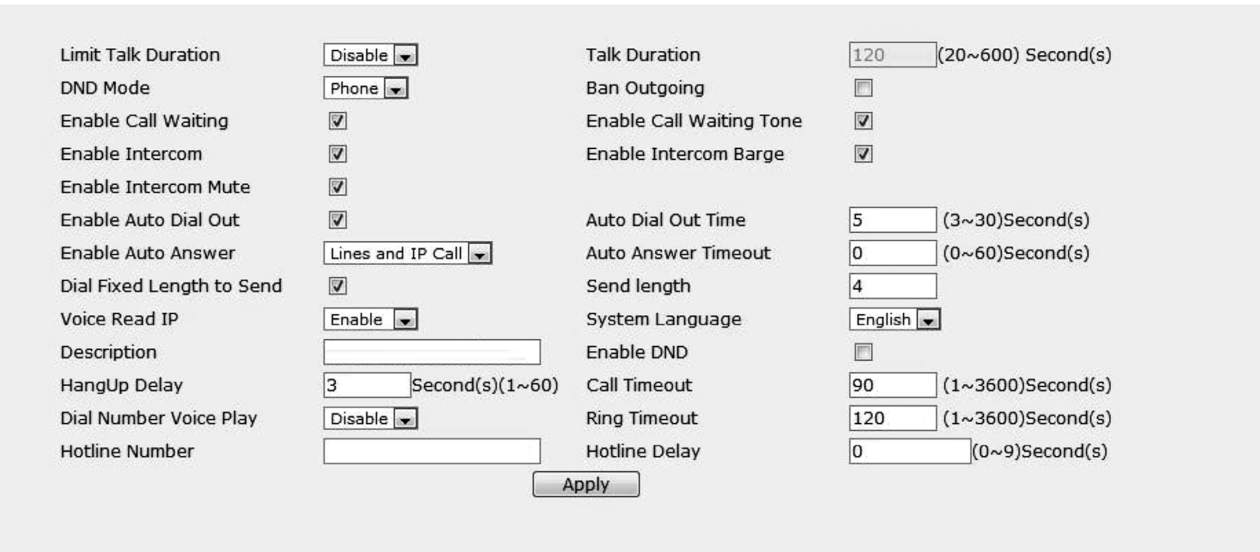
Add x, type number, x cannot call. Add x, type prefix, then the number beginning with x cannot call.
X could be a number or an IP. To add a whitelist rule, the number /IP should be preceded by a "-", followed by a ". ",
After addition, only the number in the whitelist is allowed to call, and the number outside the whitelist is refused.



Picture 26. Blacklist

7.16 Intercom Settings >> Function Settings

Configure the intercom function settings.



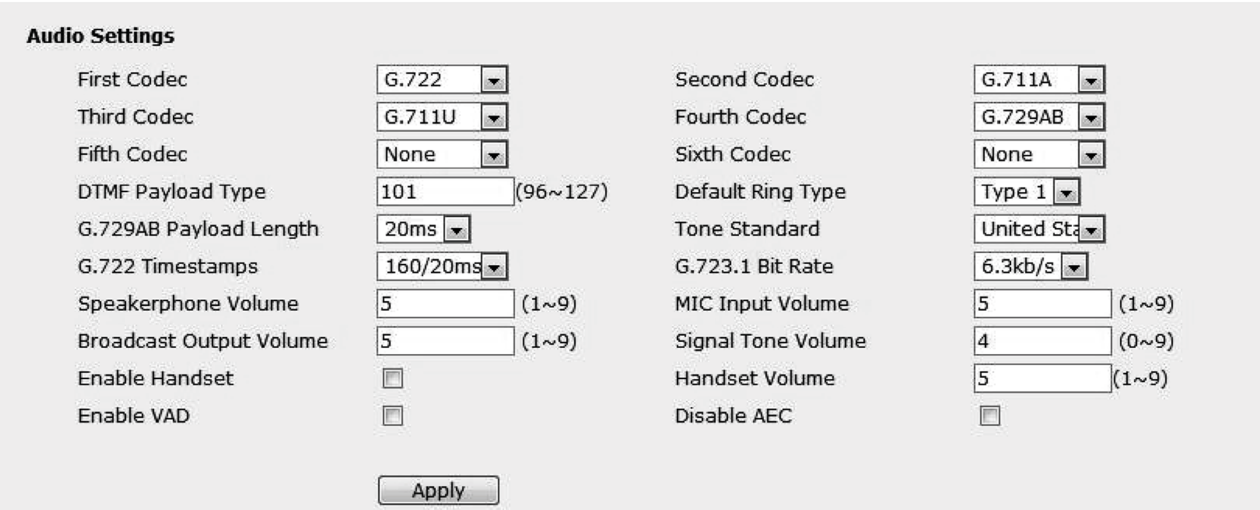
Picture 27. Function settings

Table 11. Common device function settings on the web page

Field Name	Explanation
General Settings	
Limit call duration	After enabling, hang up the call after timeout.
Call time	Hang up after timeout.
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.
Turn on intercom	When the intercom system is enabled, the device will accept the SIP header Call-Info of the incoming call request instruction to answer the phone automatically.
The second intercom answering	Automatically answer the call in intercom mode during the call, if the current call is in intercom mode, refuse to answer the new intercom mode.
Mute the intercom	If enabled, mutes incoming calls during an intercom call.
Turn on intercom ringing	When the intercom mode is configured, the incoming call will hear a ringing tone.
Turn on timeout dialing time	The system will automatically dial after timeout.
Turn on auto answer	Configure to turn on the auto answer function.
Auto answer time	Configure auto answer time.
Hang up automatically if no answer	Configure to enable automatic hangup when no answer.
Auto hang up timeout	Configure to hang up automatically when there is no answer within a set time.
Fixed length dial of receiving number	When enabled, the number entered by the user reaches a fixed length and automatically dials out.
Report IP	Turn on or off the device's voice broadcast IP address.
System language	Configure the language of the voice prompt.
Description	Descriptive information displayed on the IP scanning tool software.
Auto hang up time	Configure the automatic hang-up time, if it is in hands-free mode, the device will automatically return to standby after the auto handdown time is exceeded.

7.17 Intercom Settings >> Voice Settings

Change voice settings.



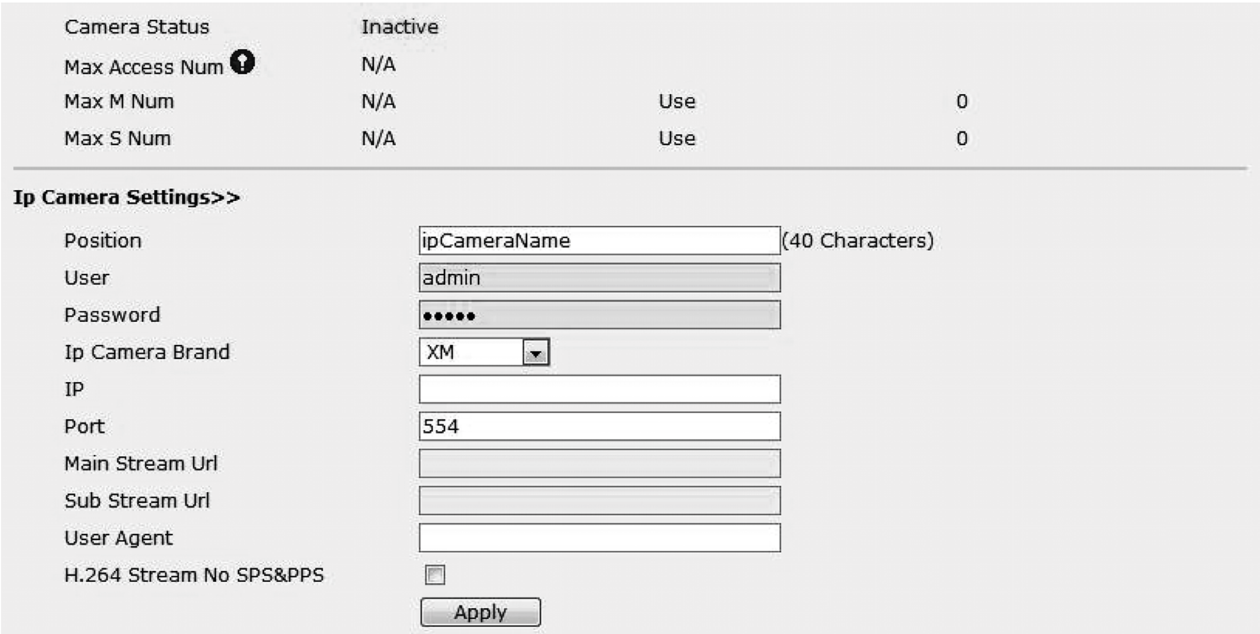
Picture 28. Audio settings

Table 12. Audio settings

Field Name	Explanation
Basic Settings	
Codec	Select DSP priority speech coding algorithm, including: 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.
Preset ringtone type	Configure the default ringtone.
G.729AB Payload Length	Configure the length of the G.729AB voice coding payload.
Signal Tone Standard	Configure signal tone standard area.
G.722 Timestamp	Select time stamp for G.722 encoding, 160/20ms and 320/20ms can be selected.
G.723.1 Bit Rate	For G723 rate selection, you can choose 5.3kb/s and 6.3kb/s.
Hands-free Volume Setting	Configure hands-free call volume level.
Microphone Input Volume	Configure the call volume level for the microphone.
Broadcast Output Volume	Configure the output volume level when broadcasting.
Signal Tone Volume	Configure the output volume level of the signal sound.
Enable Voice Activity Detection	Mute detection; if VAD is enabled, G.729 payload length cannot be set greater than 20ms.
Ringtone Upgrade/Delete	
Ringtone Upgrade	Optional ringtone upgrade with .wav suffix
Ringtone Delete	The upgraded ringtones are displayed in the delete list and can be deleted selectively.

Incoming Call Designated Ring Type Setting (Alert-info)	
The value of notification information 1 to 10	Sets the value to specify the ringtone type.
Ring Type	Type1-Type9

7.18 Intercom Setting >> Video Settings



Picture 29. Video settings

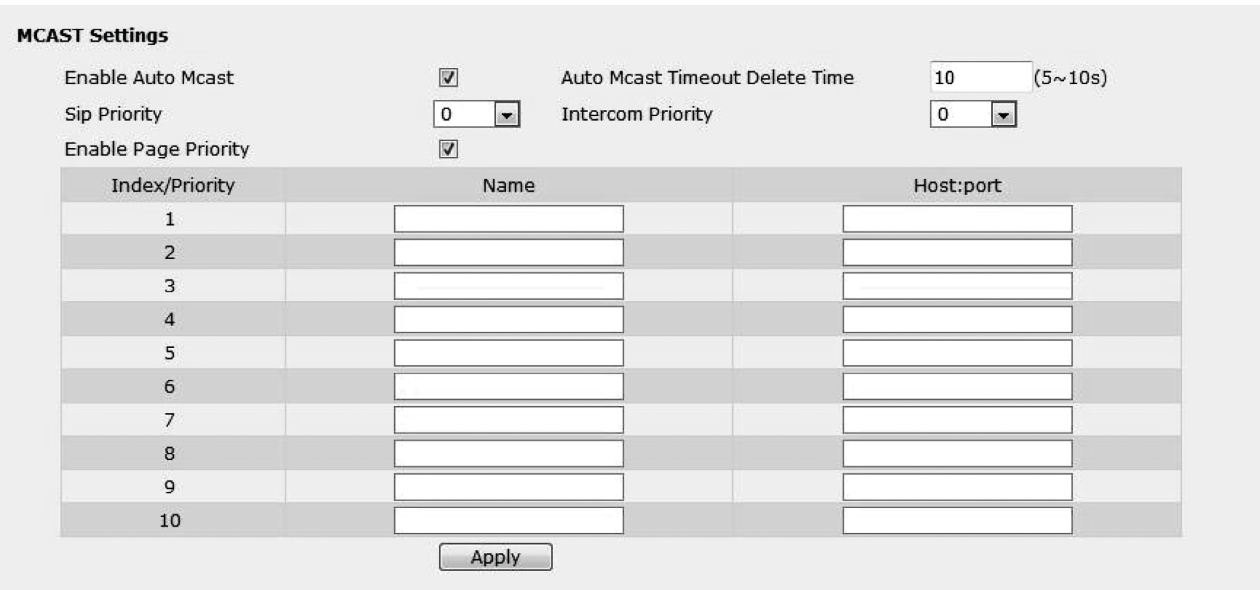
Table 13. Video Setting

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	Click Submit, the camera Url information will be automatically displayed if the connection is successful, and it will not be displayed if it fails.
Sub Stream Url	Click Submit, the camera Url information will be automatically displayed if the connection is successful, and it will not be displayed if it fails.
H.264 stream without SPS&PPS	Compatible with cameras without SPS&PPS, can display video normally.
Advanced Settings	
Video Direction	Sendonly: establish video call, and the SDP packet in the invite packet is Sendonly.
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	Access the main address of RTSP.
Sub Stream Url	Access the child address of RTSP.

7.19 Intercom Setting >> Multicast

The multicast function can be used to send announcements to each member of the multicast simply and conveniently. By setting the multicast key on the device, the multicast RTP stream can be sent to the pre-configured multicast address. By configuring the monitoring multicast address on the device, the RTP stream sent by the multicast address is monitored and played.

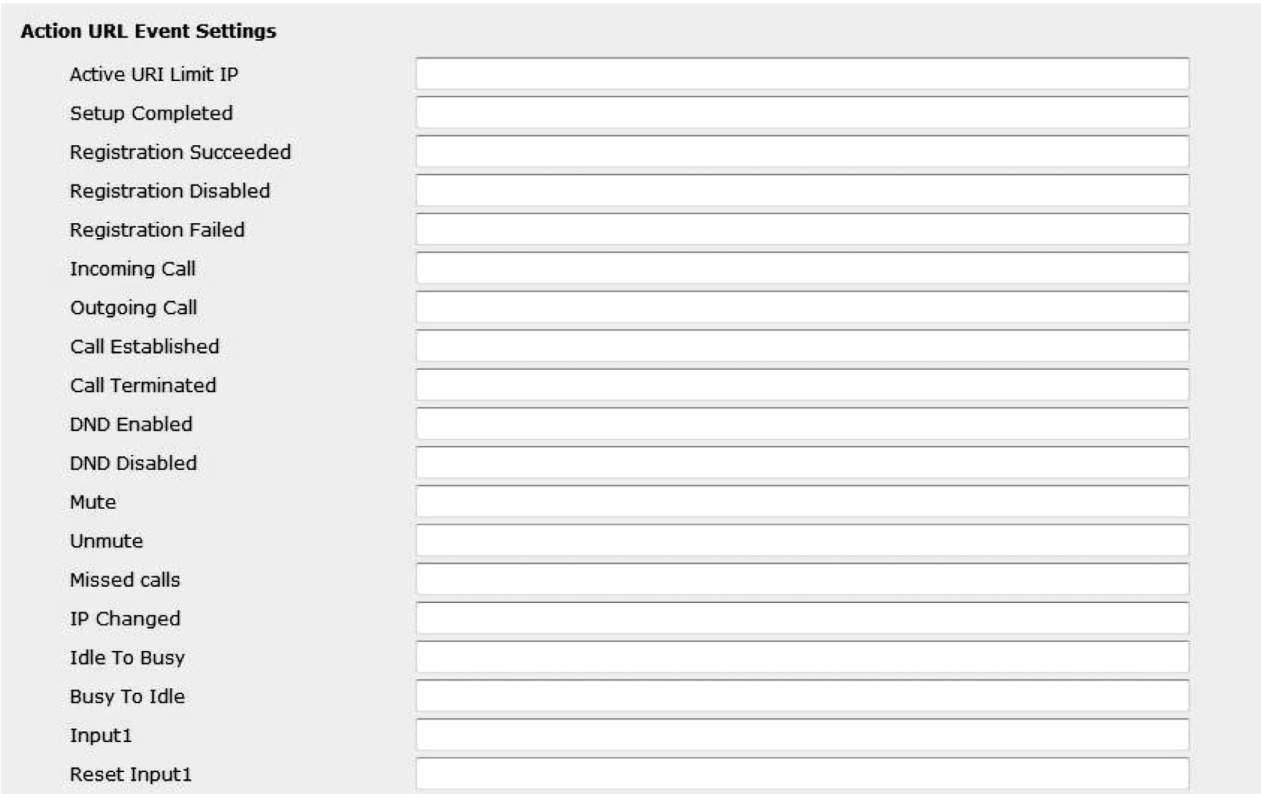


Picture 30. MCAST parameters

Table 14. MCAST parameters

Field Name	Explanation
Enable Auto Mcast	Send multicast configuration information through Sip Notify signaling. After receiving the information, the device configures it in the system for multicast monitoring or cancels multicast monitoring in the system.
Automatic Multicast Timeout Delete Time	When the multicast call does not end normally, but for some reasons, the device can no longer receive the multicast rtp packet, through this configuration, the monitoring will be cancelled after the specified time.
SIP priority	The priority defined in the current call, 1 is the highest priority, and 10 is the lowest.
Intercom priority	Compared with multicast and SIP priority, high priority can be inserted, low priority is rejected.
Enable Page Priority	Regardless of who calls in the two multicasts first, the device will give priority to the multicast with the higher priority.
Name	Listened multicast server name.
Host: port	Listened multicast server's multicast IP address and port.

7.20 Intercom Setting >> Action URL



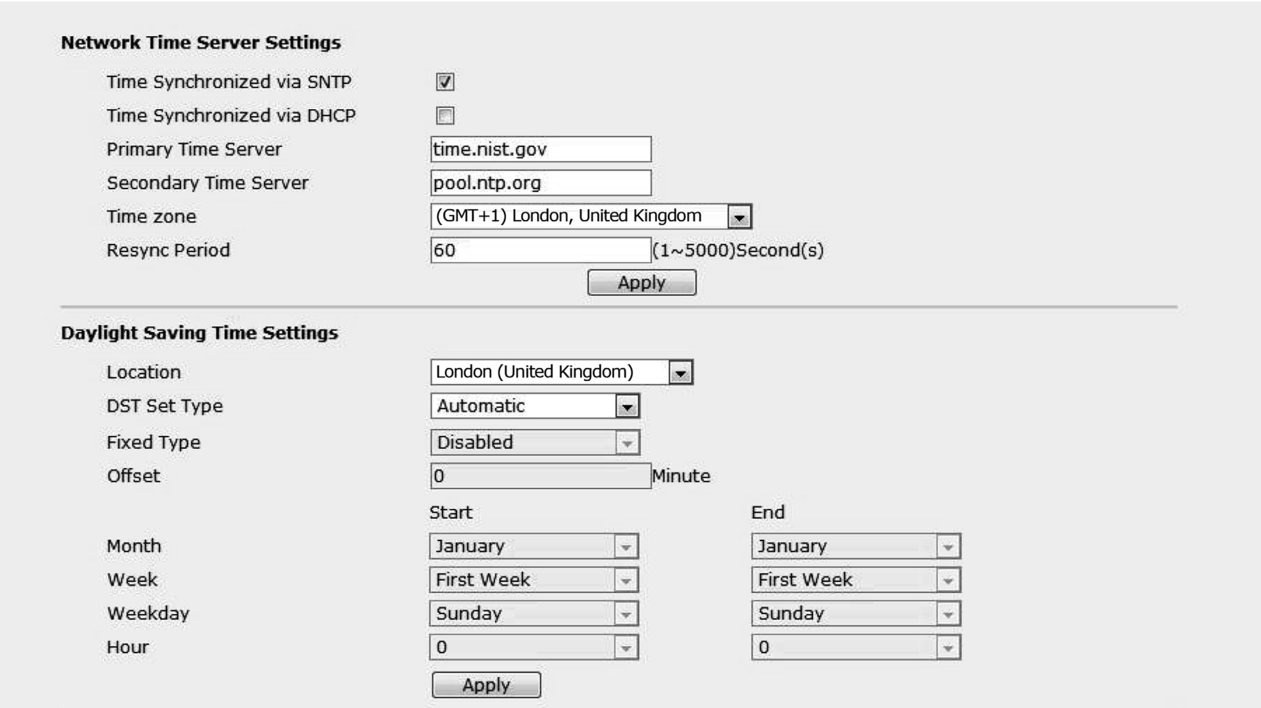
Picture 31. Action URL

Table 15. Action URL

Action URL Settings
Configure the URL for reporting actions to the server, for example, fill in the URL: http://InternalServer /FileName.xml? (Internal Server is the IP address of the server, and File Name is the xml file name of the storage device reporting action)

7.21 Intercom Setting >> Action URL

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



Picture 32. Time/Date

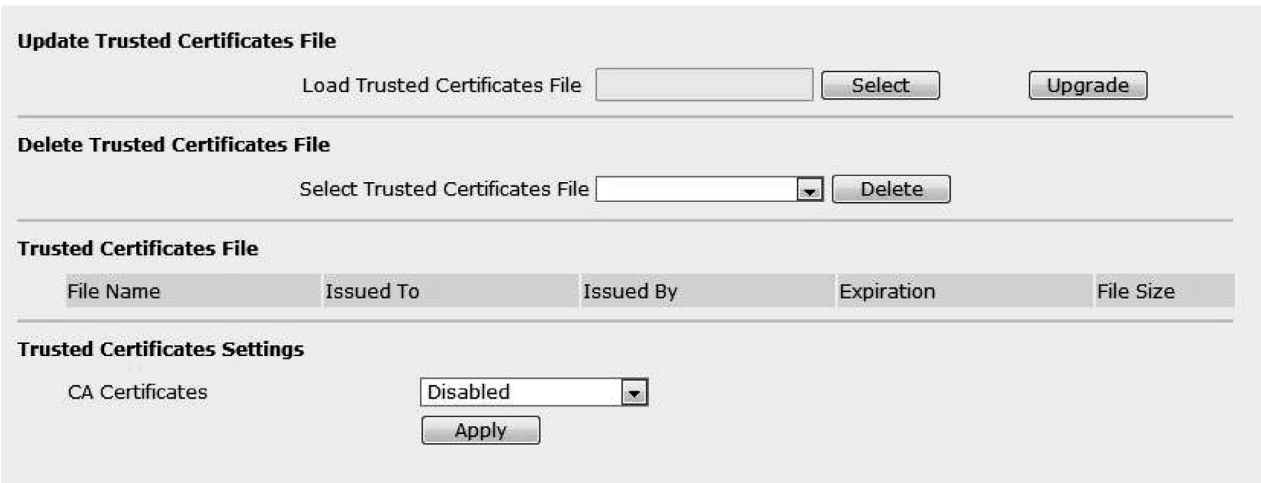
Table 16. Time/Date

Field Name	Explanation
Network Time Server Settings	
Time Synchronized via SNTP	Enable time-sync through SNTP protocol.
Time Synchronized via DHCP	Enable time-sync through DHCP protocol.
Primary Time Server	Set primary time server address.
Secondary Time Server	Set secondary time server address, when primary server is not reachable, the device 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	
Manual Time Settings	The time set by hand, need to disable SNTP service first.

7.22 Intercom Setting >> Certificate Management

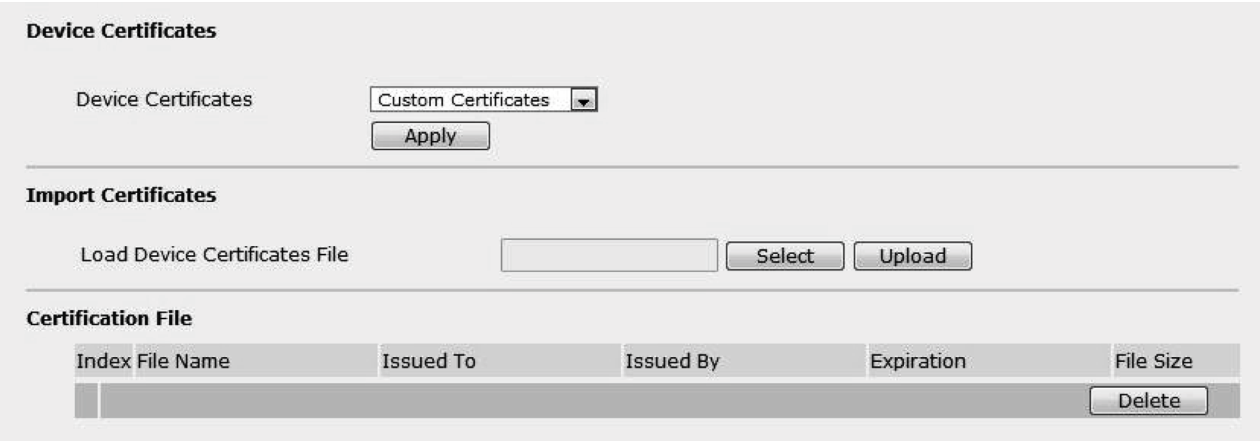
Set whether to enable the license certificate and conventional name verification, and select the certificate module.
Can upload and delete uploaded certificates.



Picture 33. Certificate settings

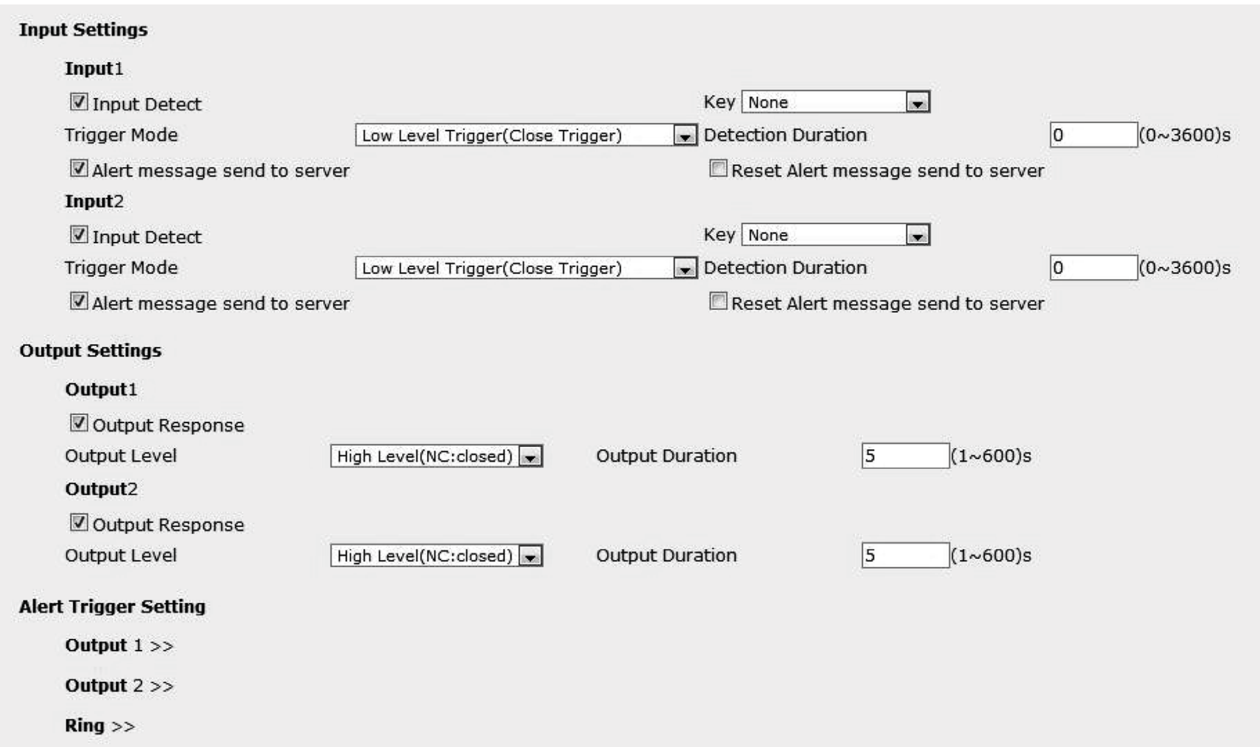
7.23 Intercom Setting >> Equipment Certificates

Select the device certificate as the default certificate and custom certificate. You can upload and delete the uploaded certificate.



Picture 34. Device certificate settings

7.24 Security Settings



Picture 35. Security settings

Table 17. Alert/Security Settings

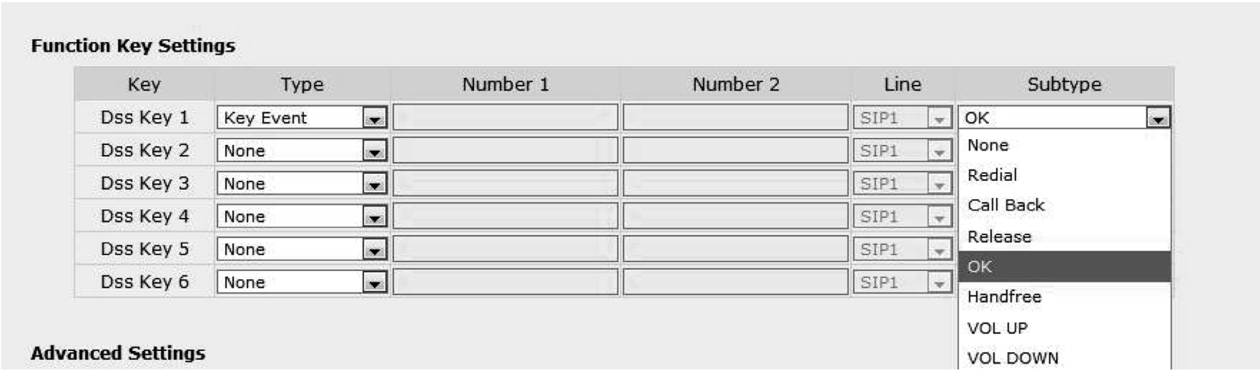
Field Name	Explanation
Input settings	
Input Detect	Enable or disable Input Detect.
Trigger Mode	When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger.
	When choosing the high level trigger (disconnected trigger), detect the input port (high level) disconnected trigger.
Alert message send to server	Set the Alert message send to server.
Send reset message to server	Enable or disable sending reset messages to the server.
Output Settings	
Output Port Response	Enable or disable Output Response.
Output Level	When low level (NO: open) is selected, when the trigger condition is met, the trigger NO port is disconnected.
	When the high level (NC: Close) is selected, the trigger NO port is closed when the trigger conditions are met.
Output Duration	The duration of the changes in the output port, default value is 5 seconds.
Alert Trigger Setting	
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 (NO: normally close), when meet the trigger condition, trigger the NO port close.
Remote DTMF Trigger	Receive the DTMF code sent by the remote device, and if it is correct, trigger the corresponding output port. You can choose to enable or disable the ringtone.
DTMF Trigger Code	During the call, the receiving terminal device sends the DTMF code, and if it is correct, the corresponding output port is triggered.
Reset Code	After receiving the corresponding instruction, the test device will reset the state and stop playing the corresponding ringtone.
Active Url Triggers	Receive the active uri sent by the remote device, and if it is correct, trigger the corresponding output port. You can choose to enable or disable the ringtone.
Trigger message	After the test equipment receives the corresponding instruction, if it is correct, it will trigger the corresponding output port.
Reset message	After receiving the corresponding instruction, the test equipment will reset the state and stop playing the corresponding ringtone.
Remote SMS trigger	Enable or disable remote SMS triggering. You can choose to enable or disable the ringtone.
Trigger Message	Send instructions on remote devices or servers, ALERT= [set instructions], if correct, trigger the corresponding output port.

Reset message	After receiving the corresponding instruction, the test equipment will reset the state and stop playing the corresponding ringtone.
Call Status Trigger	The port outputs a continuous time trigger type, including the trigger condition. For example, the call triggers the output port, and the output port will be in the call state and continue to respond) 1. Talking 2. Talking and Ringing 3. Ringing 4. Calling 5. Call and talk 6. Call and talk (caller) 7. Calling and ringing 8. Talking and ringing (called) 9. Talking and ringing 10. Call, ring and talk
Tamper Alarm Settings	
Tamper detection	If the terminal is violently demolished, the terminal is triggered to always play the set alarm ringtone.
Warning Instruction	After the alarm is triggered, the command set by the Alarm command is sent to the server at the same time.
Alarm Recovery	If you need to stop the alarm ringtone, the remote end can send a short message to the terminal. The content of the short message is the value set in the Reset command. At this time, the test terminal will stop the alarm ringtone playback.
Alarm Status Recovery	Reset to stop the playback of the ringtone.
Ring Type	Ringtone can be set to none / preset.
Server Settings	
Server Address	Configure the remote response server address (including the remote response server address and trigger alarm server address, IP:PORT, SIP number). When the input port is triggered, a short message will be sent to the server. The message format is as follows: Alarm Info: Description=ICO EMERGENCY;SIP User=;Mac=00:69:67:80:12:39;IP=172.18.2.243;port =Input1 (support variables and strings).

7.25 Function Key >> Function Key

7.25.1 Key Event

You can set the function type of these keys to Key Event, and there are multiple options for sub-types.



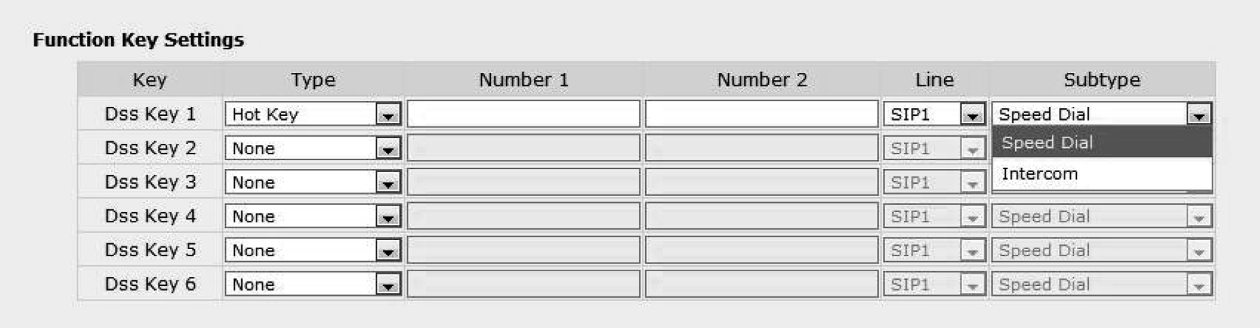
Picture 36. Function keys

Table 18. Function keys

Type	Subtype	Usage
Function Keys	None	No responding
	Redial	User can redial the last number dialed
	Call Back	Call the nearest missed number
	Release	Delete password input, cancel dialing input and end call
	OK	Identification key
	Handfree	Use as a hands-free button
	VOL UP	Turn up volume
	VOL DOWN	Turn down volume

7.25.2 Hot Key

Enter the phone number in the input box. When you press the shortcut key, the device will call out the set phone number. This button can also be used to set the IP address, press the shortcut key to make an IP direct call.



Picture 37. Hot key setting

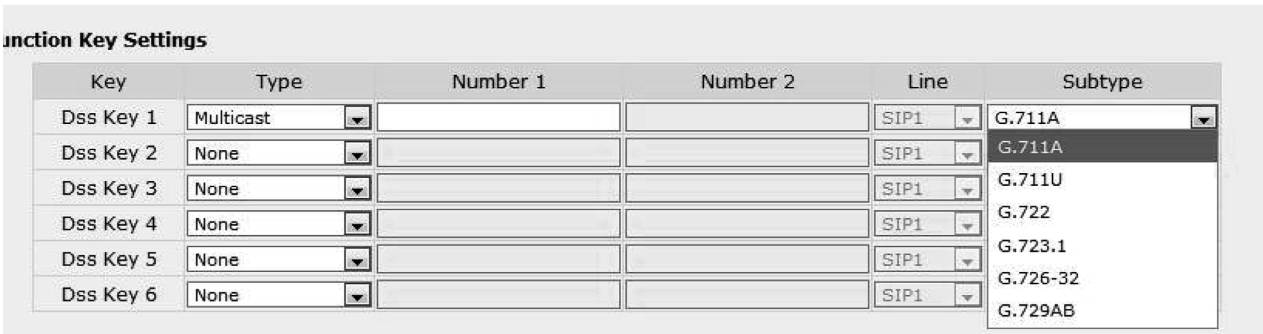
Table 19. Hot Key Settings

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.

7.25.3 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:



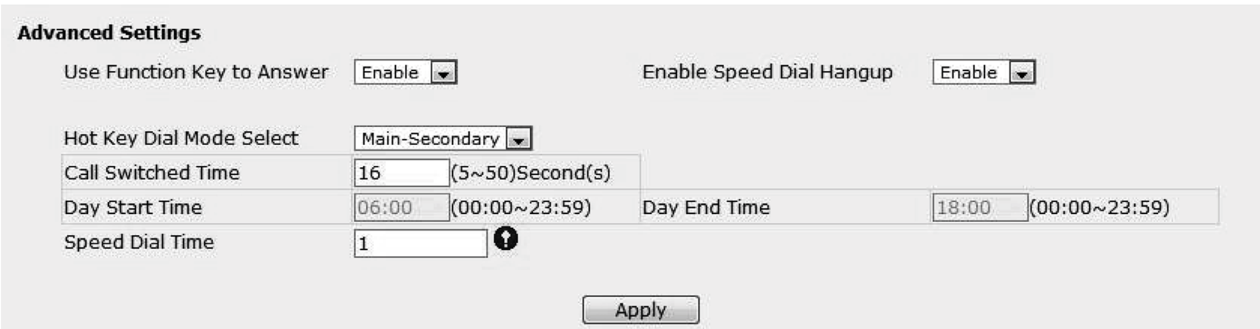
Picture 38. Multicast settings

Table 20. 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	

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

7.25.4 Advanced Settings



Picture 39. Advanced settings

Table 21. 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”.

8. 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 technical support.

8.1 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.

8.2 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.

8.3 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.

8.4 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 technical support mailbox.

8.5 Common Trouble Cases

Table 22. Common trouble cases

Trouble Case	Solution
Device could not boot up	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 [Computer] interface. 2. Please check if the device has an IP address. Check the system information. If the IP address is Negotiating..., the device has not obtained an IP address. Please check if the network configuration is correct. 3. 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.

9. List of Contents

9.1 List of Tables

9.2 List of Drawings

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