# ESI Access

## ESI A64v Access Device User's Guide

Compatible with SIP and ONVIF protocols, the AC64v Access Device integrates access control, intercom, and security protection. Featuring an aluminum alloy design and a lighted numeric keypad, the AC64v delivers a high-quality robust appearance. The IP66 and IK07 ratings make the AC64v water, dust and impact resistant in most outdoor environments. The AC64v allows users to make audio/video calls via a speed-dial button and a 2 Mega-pixel camera and achieve access control by different methods such as RFID and password. An array of input and output interfaces allows the AC64v to be easily integrated with other security devices. The AC64v is ideal for apartments, commercial buildings, communities, industrial parks and more.

# Directory

## Safety

Read the following safety notices before installing or using this unit. They are crucial for the safe and reliable operation of the device.

- Use a quality power supply or a PoE supply that meets PoE standards.
- Verify that building power and wiring are good. Inaccurate power voltage or faulty wiring may cause fire and damage.
- Do not damaged cords or cables as they may cause fire or electric shock.
- Do not handle the device roughly.
- Do not install the device in places where there is direct sunlight. Also do not put the device on carpets or cushions. It may cause overheating, fire or failure.
- Before using the product, confirm that the temperature and humidity of the environment meet the working requirements of the product. See datasheet.
- Avoid getting the device wet.
- Only allow a licensed access expert to install the device so that local code is met.
- Do not use harsh chemicals, cleaning solvents, or strong detergents to clean it. Wipe it with a soft cloth that has been slightly dampened in a mild soap and water solution.
- Do not install the device in a poorly ventilated area.
- Before installing any equipment, be familiar with building layout and electrical hazards.

# Overview

Compatible with SIP and ONVIF protocols, the AC64v Access Device integrates access control, intercom, and security protection. Featuring an aluminum alloy design and a lighted numeric keypad, the AC64v delivers a high-quality robust appearance. The IP66 and IK07 ratings make the AC64v water, dust and impact resistant in most outdoor environments. The AC64v allows users to make audio/video calls via a speed-dial button and a 2 Mega-pixel camera and achieve access control by different methods such as RFID and password. An array of input and output interfaces allows the AC64v to be easily integrated with other security devices. The AC64v is ideal for apartments, commercial buildings, communities, industrial parks and more.

# Installation

## *Use PoE or external Power Adapter*

The ESI AC64v supports two power supply modes, power supply from external power adapter or Power over Ethernet (PoE) compliant 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 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 a PoE switch and power adapter at the same time, the power adapter will be used in priority and will switch to PoE power supply once it fails.

Use a quality power adapter or a PoE switch that meets standard PoE specifications to ensure proper function.

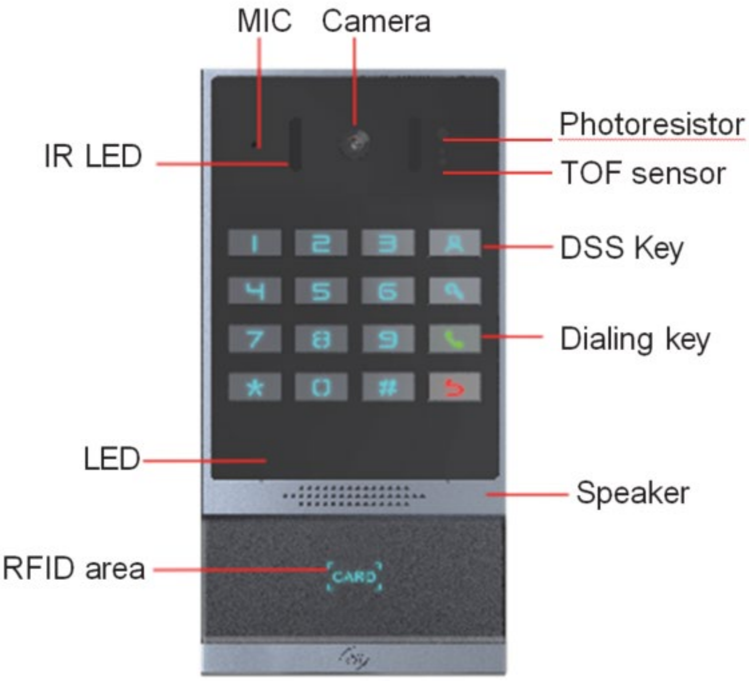
## *IP Address Reporting*

| Action behavior | Description |
|---|---|
| Standby report IP | In standby mode, long press the speed dial button for 3 seconds, there will be a 5 second tone. Press the speed dial button once within 5 seconds. The tone will stop automatically then announce IP.<br>Press the button in the upper right corner 👤. |
| Switch network mode | In the standby mode, long-press the speed dial button for 3 seconds and the beep will last for 5 seconds. Within 5 seconds, press the speed dial button three times quickly to switch to the network mode.<br>If there is no IP at present, switch to the default static IP (192.168.1.128).<br>Then switch to DHCP mode when it is the default static IP (192.168.1.128)<br>When DHCP gets to IP, then do not switch and report the IP directly. Report the IP after the successful switch |
| Voice loop mode | After you press the speed dial button twice, the device enters the voice loopback mode. After you press the MIC speaker, you can check the voice related problems. After you press the speed dial button again, you can exit the voice loopback mode |

## *LED status*

| Indicator status | Meaning |
|---|---|
| Steady green | Standby (No registration, normal network) |
| Steady cyan | Registration success |
| Cyan light flash | talking/Calling/going |
| Red slow flash | Registration failed |
| Red slow flash | Network anomaly |
| Orange light flash | Upgrade and restore factory |
| Steady | Standby |
| Flashing 1s | A credit card |

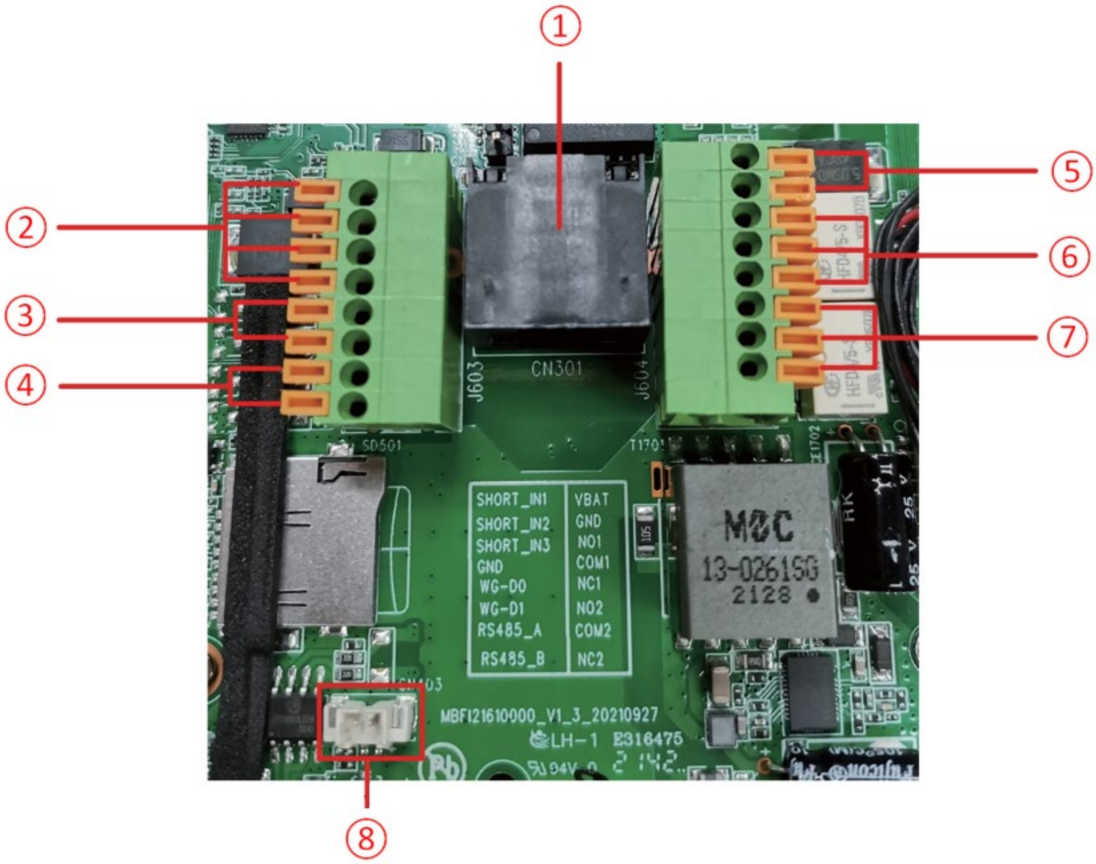
### *Front Panel*



| Name | Description |
|---|---|
| Camera | Video signal acquisition and transmission |
| MIC | Audio acquisition |
| DSS key | For speed dial, multicast, intercom, IP broadcast and other functions |
| RFID area | Swipe identification cards |
| Speaker | Play sound |
| Photo resistor | Detects light levels |
| ToF sensor | Senses the distance of an object |
| IR LED | Helps illuminate objects in low light situations |
| LED | For Status |
| Dialing key | Press to send the dialed number |

## *Connections*

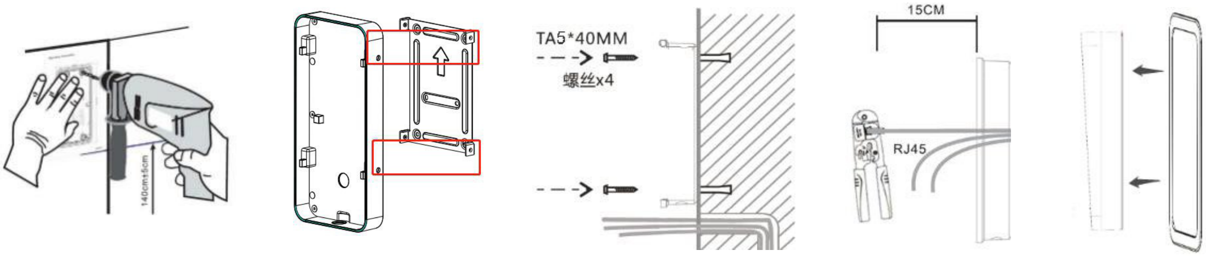
Open the rear case of the device, there is a row of terminal blocks for connecting the power supply, electric lock control, etc. The connection is as follows:



| SN | Description |
|---|---|
| ① | Ethernet interface: standard RJ45 interface, 10/100M adaptive, it is recommended to use five or five types of network cable |
| ② | Two groups of short-circuit input detection interfaces: for connecting switches, infrared probes, door magnets, vibration sensors and other input devices |
| ③ | Wiegand interface |
| ④ | RS485 interface |
| ⑤ | Power interface: 12V/1A input. VBAT=positive. GND=negative. |
| ⑥、⑦ | Two groups of short-circuit output control interface: used to control electric locks, alarms, etc. |
| ⑧ | Line out interface. For accessibility aids for the deaf |

### *Wall Mounting*

1. Draw the installation holes on the wall according to the installation dimension drawing provided. Use an electric drill to make the vacant place, after drilling the hole, remove the installation dimension drawing, and use a hammer to drive the plastic plug into the drilled hole;
2. Use a screwdriver to loosen the 4 screws on the back, separate the back shell from the wall bracket, and lock the screws on the back of the device at the same time;
3. Align the screw holes of the wall bracket with the holes made on the wall, and fix it to the wall with the supplied screws;
4. Pass all the wires through the silicone plug in the middle of the bottom shell. All wires need to reserve a length of 8 inches (20cm).
5. Hang the device and the wall bracket tightly from top to bottom, and tighten the screws at the bottom



**Device IP address**

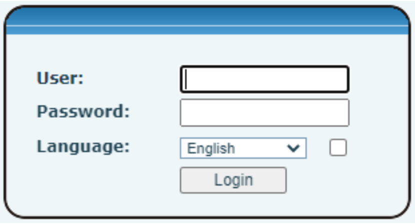
Method 1: Connect the speaker, press and hold the speed-dial button for 3 seconds (30 seconds after power on), wait for the speaker to beep. Press the speed-dial button within 5 seconds, and the device will automatically announce the IP address by voice.

Method 2: Press and hold the speed-dial button for 3 seconds, wait for the speaker to beep, press the speed-dial button three times within 5 seconds, and the device will automatically announce the IP address by voice after successfully switching to the network mode.

| **Default configuration** | | | |
|---|---|---|---|
| DHCP mode | Default enable | Static IP | 192.168.1.128 |
| Voice read IP address | Press and hold the speed-dial button for 3 seconds, press the speed dial button one times within 5 seconds. | Server port | 80 |

## 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.



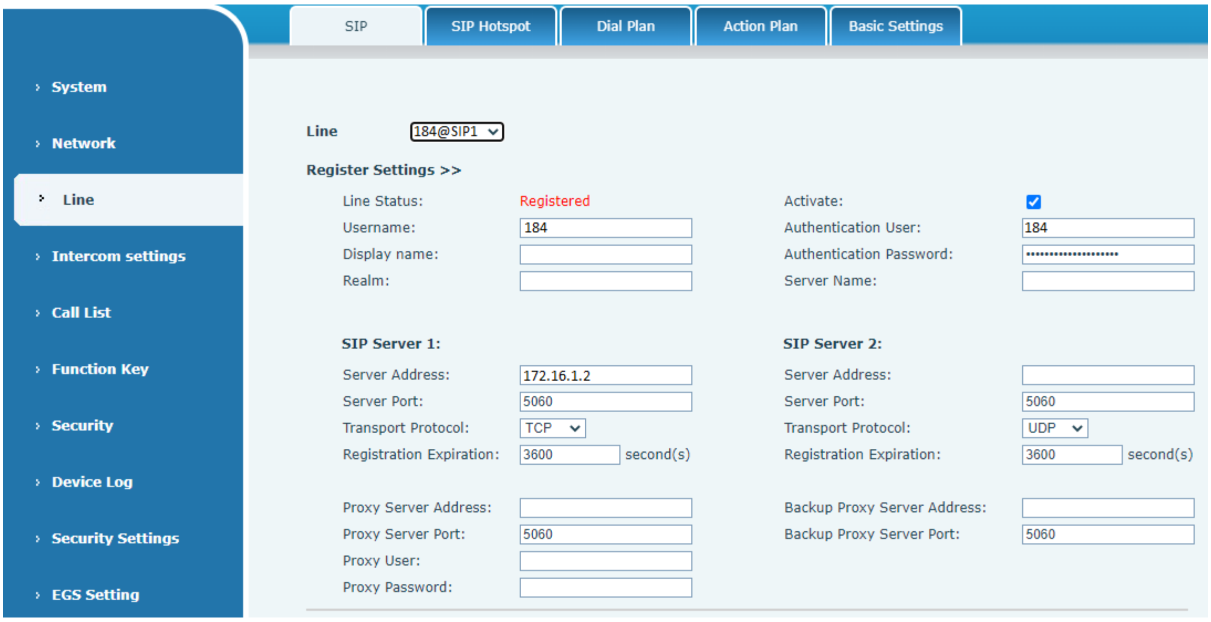
Enter the username and password to log in to the web page. The default username and password are **admin / admin** for eSIP and **admin / SIPstn@ESI** for eCloud.

## *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:



Line: 184@SIP1

Register Settings >>

Line Status: Registered
Username: 184
Display name:
Realm:
Activate: ☑
Authentication User: 184
Authentication Password: ••••••••••••••••••••
Server Name:

SIP Server 1:
Server Address: 172.16.1.2
Server Port: 5060
Transport Protocol: TCP
Registration Expiration: 3600 second(s)

SIP Server 2:
Server Address:
Server Port: 5060
Transport Protocol: UDP
Registration Expiration: 3600 second(s)

Proxy Server Address:
Proxy Server Port: 5060
Proxy User:
Proxy Password:

Backup Proxy Server Address:
Backup Proxy Server Port: 5060

## *Door opening operation*

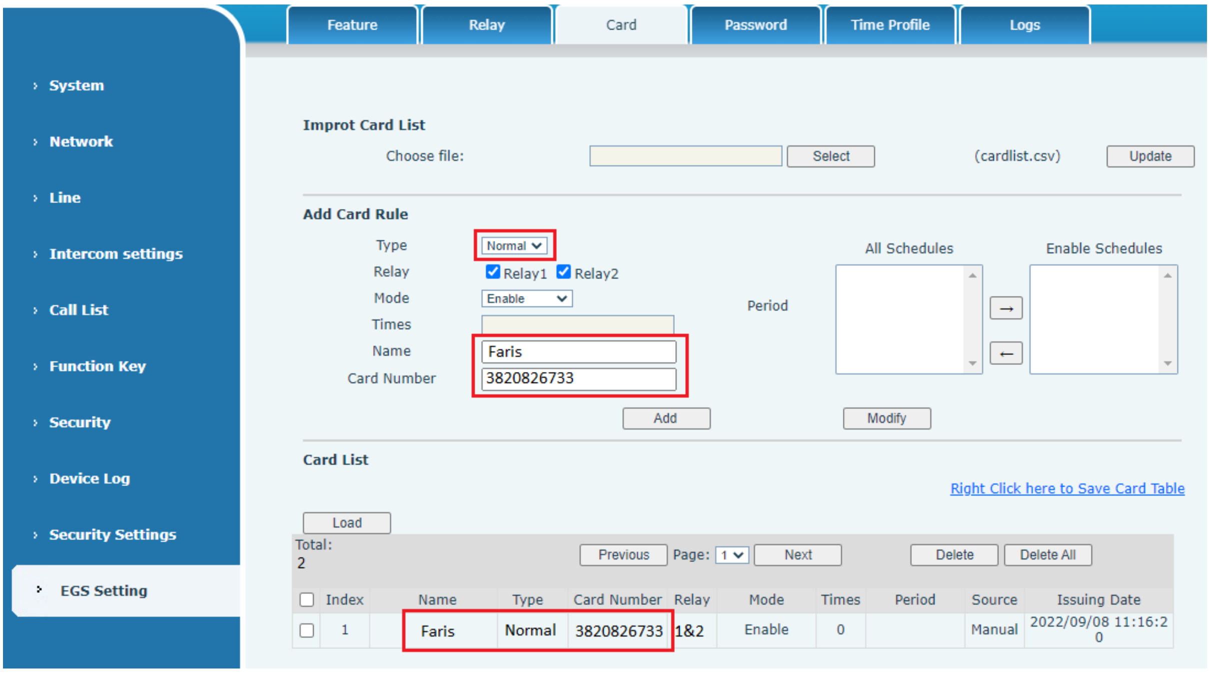
Unlock the door in the following five ways:

1. Open the door by swiping the RFID card, which supports IC card and ID card.
2. The access control helps to call owner, and the owner enters the remote opening password to open the door.
3. The other device helps to call the door phone, enters the corresponding remote authentication code, and opens the door after timeout or the password check length is reached (the authentication code shall be configured in the access list).
4. The door can be opened through the indoor door button when the door phone is in any state.
5. Timed door opening: automatically opens the door in a predetermined time period by setting a timed task.

## *Door open settings*

### Swipe card to open the door

- Access control settings on web page→EGS Setting→Add Card Rule. Select "Type" (Normal card provides open door function, Add card and Del card provides add and delete card function. Default Normal card)
- Enter your name and card number (just enter the first 10 digits of the card number), and clicking "Add" to add the card to the list.
- Tap the card reading area of the device with the configured ID card CARD to open the door.



**Improt Card List**

Choose file: (cardlist.csv)

**Add Card Rule**

Type: Normal

Relay: ☑ Relay1 ☑ Relay2

Mode: Enable

Times:

Name: Faris

Card Number: 3820826733

**Card List**

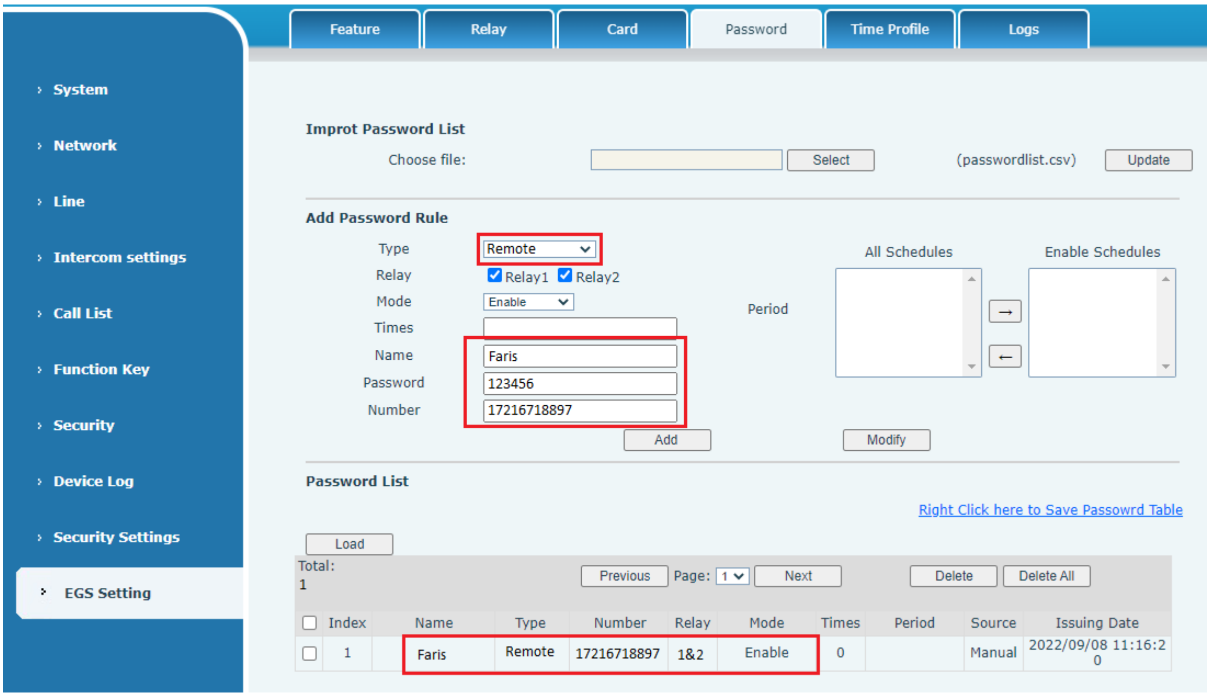
Total: 2

Page: 1

| □ | Index | Name | Type | Card Number | Relay | Mode | Times | Period | Source | Issuing Date |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | Faris | Normal | 3820826733 | 1&2 | Enable | 0 | | Manual | 2022/09/08 11:16:20 |

## Remote Password Door Opening

- Set access control on the web page→ EGS Setting→Password→ Add password rule→ Select "Remote".
- Enter your name, password and number, add to the password list.
- The owner answers the access control call and enters password to open the door for a visitor. Default password is *.



Improt Password List

Choose file: (passwordlist.csv)

Add Password Rule

|  |  |
|---|---|
| Type | Remote |
| Relay | ☑ Relay1 ☑ Relay2 |
| Mode | Enable |
| Times |  |
| Name | Faris |
| Password | 123456 |
| Number | 17216718897 |

Period All Schedules Enable Schedules

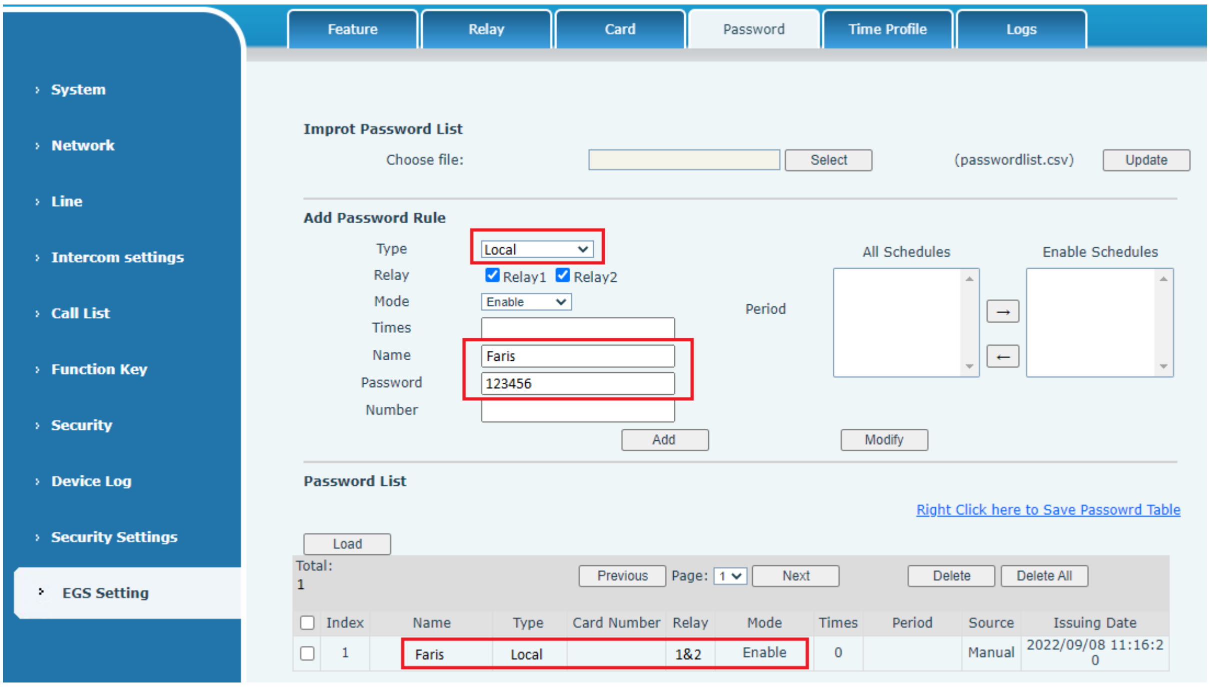
Password List

Total: 1 Page: 1

| ☐ | Index | Name | Type | Number | Relay | Mode | Times | Period | Source | Issuing Date |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | Faris | Remote | 17216718897 | 1&2 | Enable | 0 |  | Manual | 2022/09/08 11:16:20 |

## Local Password to Open Door

- Configure access on Web→EGS Setting →Password → Add password rule → Select "Local ".
- Enter your name and password to the password list.
- Owners and visitors can open the door by entering "6789" (default password) or "123456" (new password) by using the keypad.



Improt Password List

Choose file: (passwordlist.csv)

Add Password Rule

|  |  |
|---|---|
| Type | Local |
| Relay | ☑ Relay1 ☑ Relay2 |
| Mode | Enable |
| Times |  |
| Name | Faris |
| Password | 123456 |
| Number |  |

Period All Schedules Enable Schedules

Password List

Total: 1 Page: 1

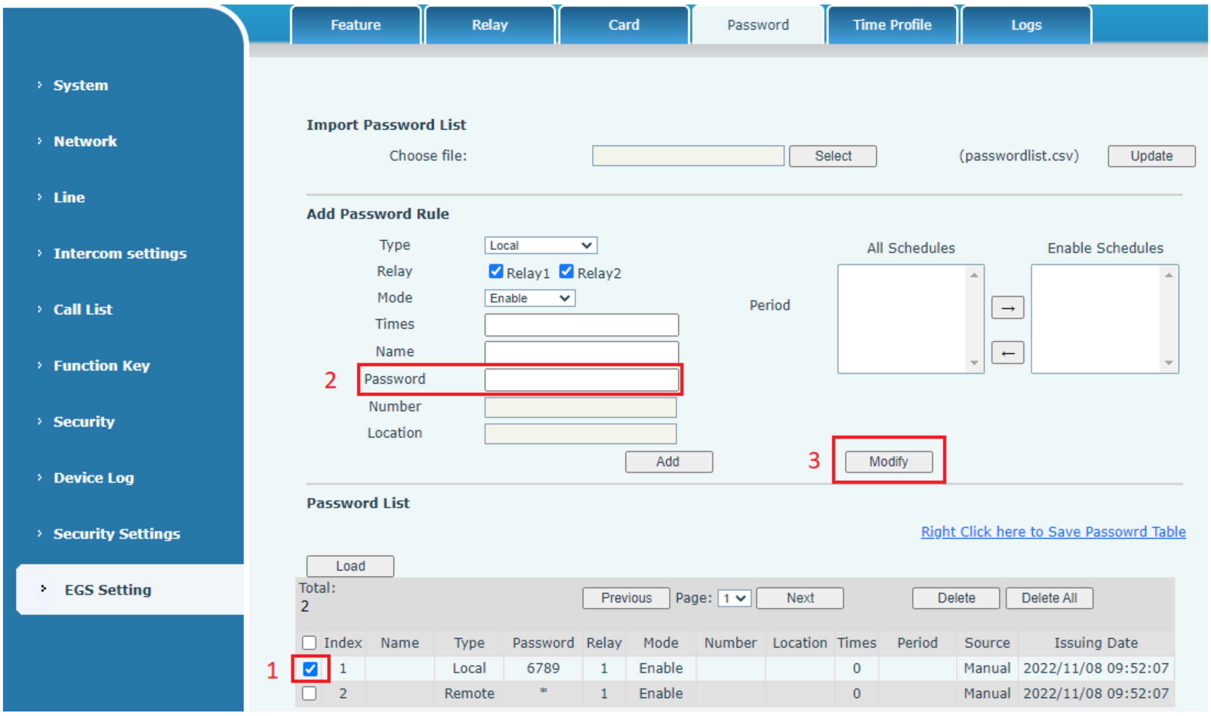
| ☐ | Index | Name | Type | Card Number | Relay | Mode | Times | Period | Source | Issuing Date |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | Faris | Local |  | 1&2 | Enable | 0 |  | Manual | 2022/09/08 11:16:20 |

## Change default password

The default local password is 6789 and the default remote password is *.

Do the following steps to change the default password.

- Go to EGS Settings > Password.
- Select the password to edit (1).
- Enter new password (2).
- Click Modify (3).



Type: Local
Relay: ☑ Relay1 ☑ Relay2
Mode: Enable
Times:
Name:
Password:
Number:
Location:

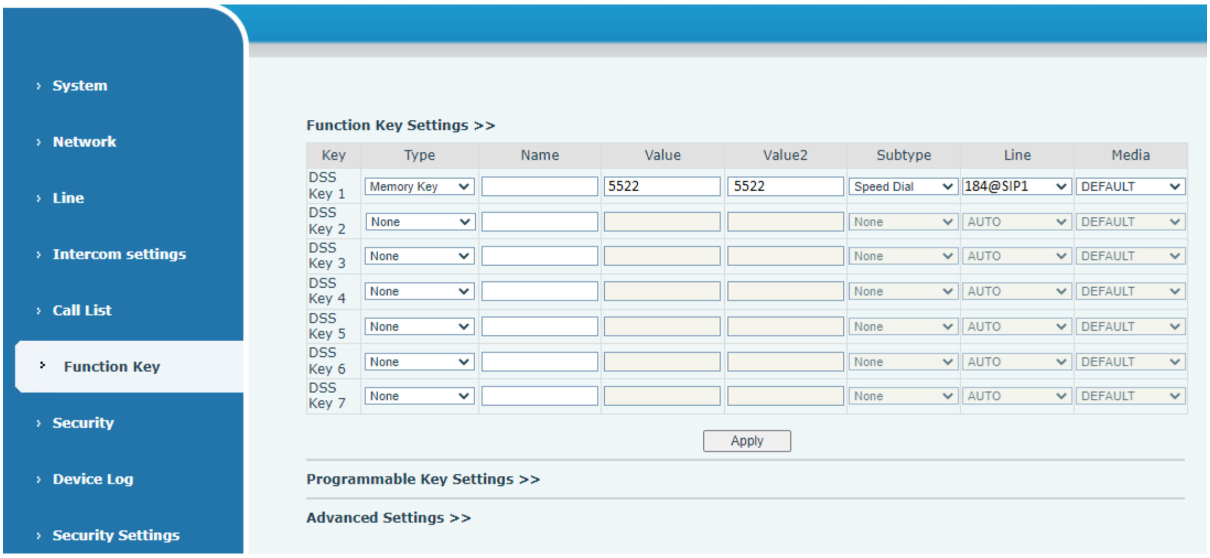
Total:
2

| □ | Index | Name | Type | Password | Relay | Mode | Number | Location | Times | Period | Source | Issuing Date |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | 1 | | Local | 6789 | 1 | Enable | | | 0 | | Manual | 2022/11/08 09:52:07 |
| □ | 2 | | Remote | * | 1 | Enable | | | 0 | | Manual | 2022/11/08 09:52:07 |

The default password can also be deleted by selecting it and then by clicking Delete

# Calling

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 >>

| Key | Type | Name | Value | Value2 | Subtype | Line | Media |
|---|---|---|---|---|---|---|---|
| DSS Key 1 | Memory Key | | 5522 | 5522 | Speed Dial | 184@SIP1 | DEFAULT |
| DSS Key 2 | None | | | | None | AUTO | DEFAULT |
| DSS Key 3 | None | | | | None | AUTO | DEFAULT |
| DSS Key 4 | None | | | | None | AUTO | DEFAULT |
| DSS Key 5 | None | | | | None | AUTO | DEFAULT |
| DSS Key 6 | None | | | | None | AUTO | DEFAULT |
| DSS Key 7 | None | | | | None | AUTO | DEFAULT |

Programmable Key Settings >>

Advanced Settings >>

See detailed configuration instructions Function Key.

After setting the speed dial according to the above settings, the AC64v access device can directly dial the set number by pressing the Management Center button 👤.

You can also press the dial button first☎, then enter the number you want to call, and automatically call after timeout.

## 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.

## End the Call

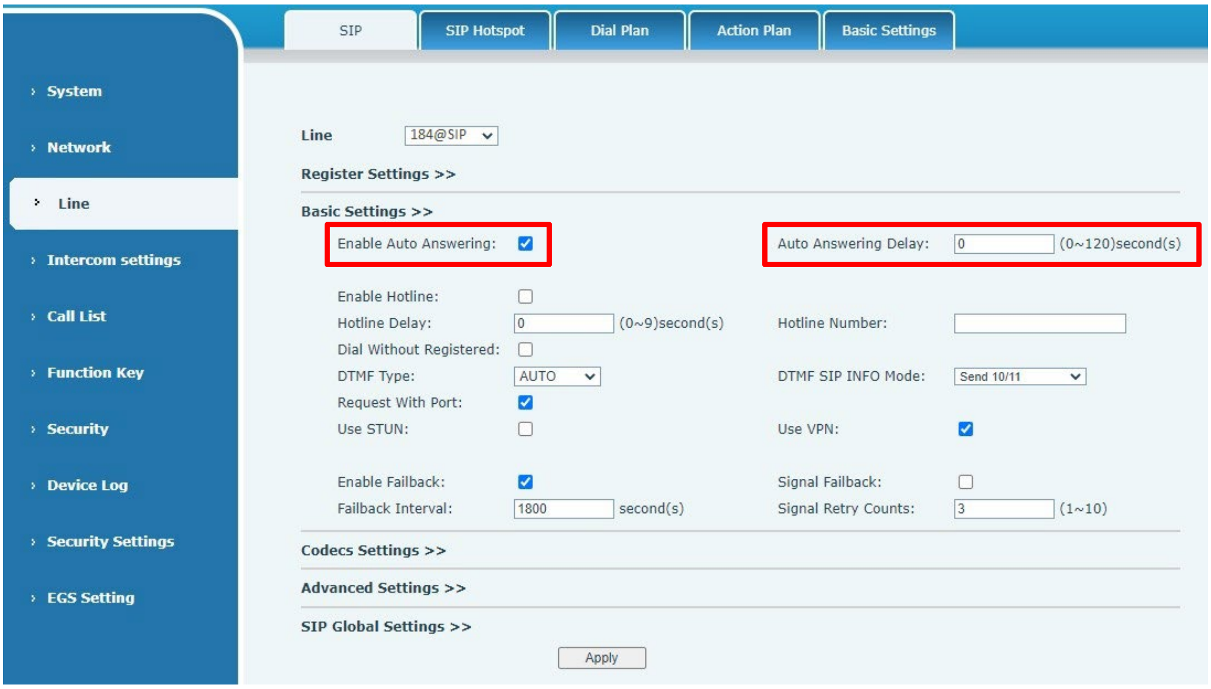
You can hang up the call through the Release key (you can set the function key as the Release key) or turn on the speed dial button to hang up the call. See detailed configuration instructions Function Key.

The back button ↩ can also be used to hang up the call.

## Auto Answer

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 [**Line**] >> [**SIP**], Enable auto answer and set auto answer time and click submit.



Line: 184@SIP

Register Settings >>

Basic Settings >>

Enable Auto Answering: ☑ | Auto Answering Delay: 0 (0~120)second(s)

| | | | |
|---|---|---|---|
| Enable Hotline: | □ | | |
| Hotline Delay: | 0 (0~9)second(s) | Hotline Number: | |
| Dial Without Registered: | □ | | |
| DTMF Type: | AUTO | DTMF SIP INFO Mode: | Send 10/11 |
| Request With Port: | ☑ | | |
| Use STUN: | □ | Use VPN: | ☑ |
| Enable Failback: | ☑ | Signal Failback: | □ |
| Failback Interval: | 1800 second(s) | Signal Retry Counts: | 3 (1~10) |

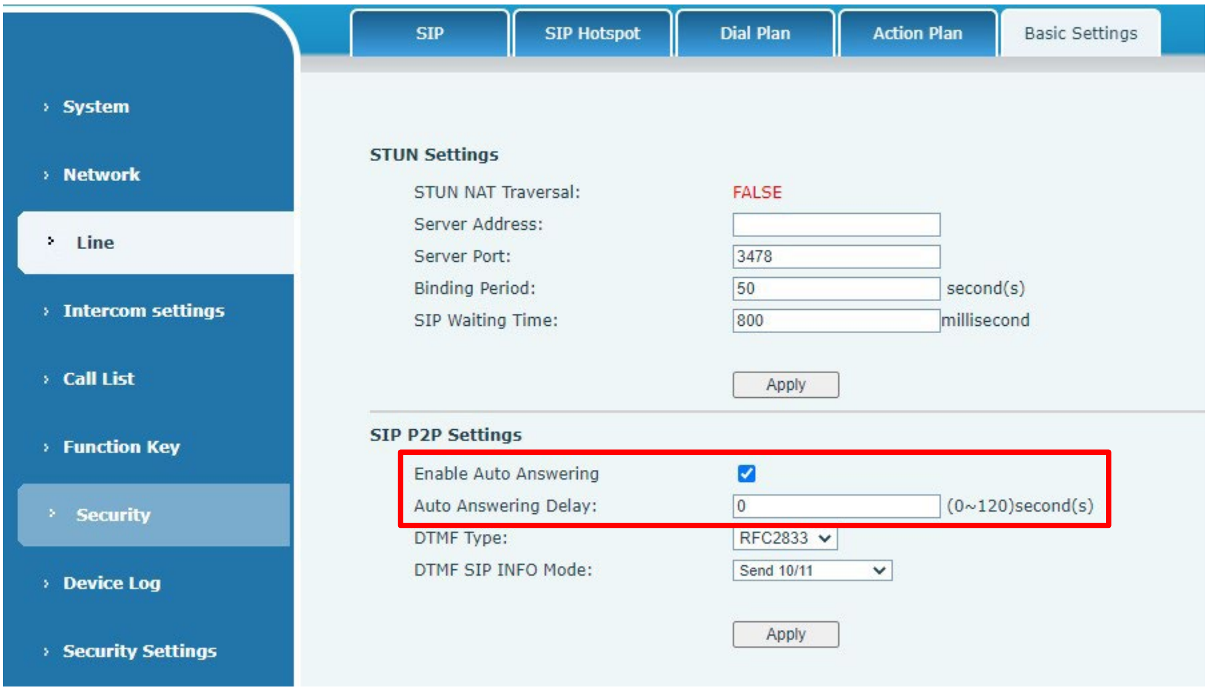
Codecs Settings >>

Advanced Settings >>

SIP Global Settings >>

SIP P2P auto answering：

Enter [**Line**] >> [**Basic settings**], Enable auto answer and set auto answer time and click submit. Auto Answer timeout is 0-120 seconds.



STUN Settings

| | |
|---|---|
| STUN NAT Traversal: | FALSE |
| Server Address: | |
| Server Port: | 3478 |
| Binding Period: | 50 second(s) |
| SIP Waiting Time: | 800 millisecond |

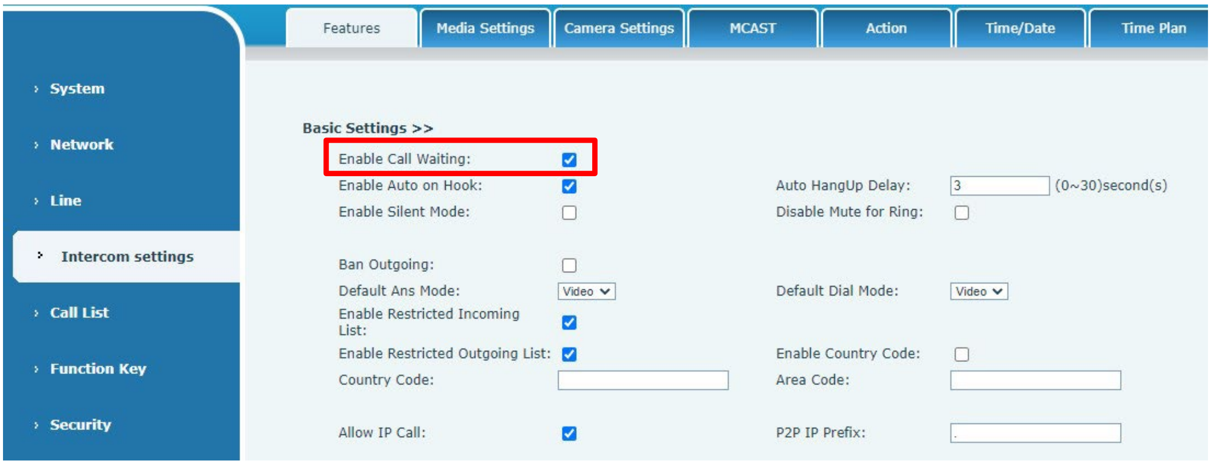
SIP P2P Settings

| | |
|---|---|
| Enable Auto Answering | ☑ |
| Auto Answering Delay: | 0 (0~120)second(s) |
| DTMF Type: | RFC2833 |
| DTMF SIP INFO Mode: | Send 10/11 |

The range can be set to 0~120 seconds and the call will be answered automatically after timeout.

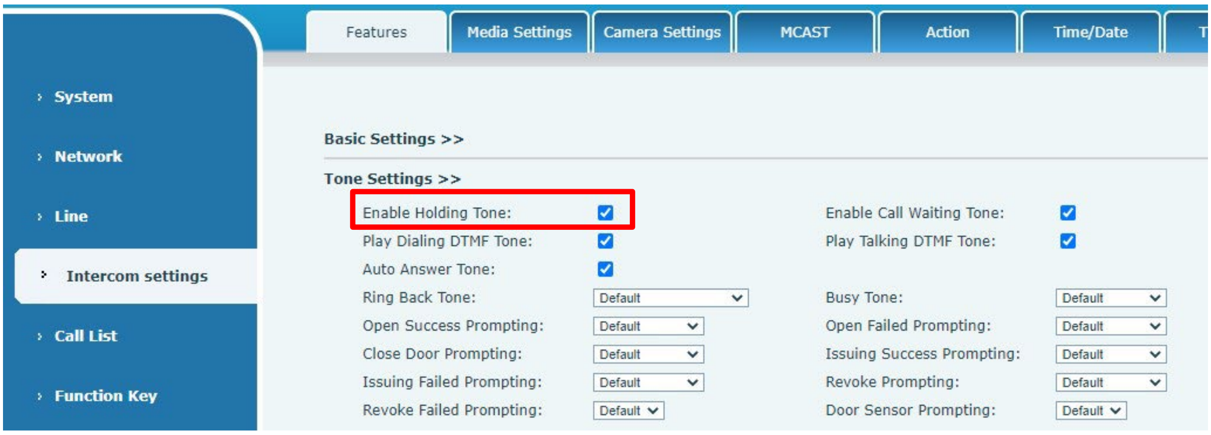
## Call Waiting

- 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.



Basic Settings >>

Enable Call Waiting: ☑
Enable Auto on Hook: ☑
Auto HangUp Delay: 3 (0~30)second(s)
Enable Silent Mode: □
Disable Mute for Ring: □
Ban Outgoing: □
Default Ans Mode: Video
Default Dial Mode: Video
Enable Restricted Incoming List: ☑
Enable Restricted Outgoing List: ☑
Enable Country Code: □
Country Code:
Area Code:
Allow IP Call: ☑
P2P IP Prefix: .



Basic Settings >>

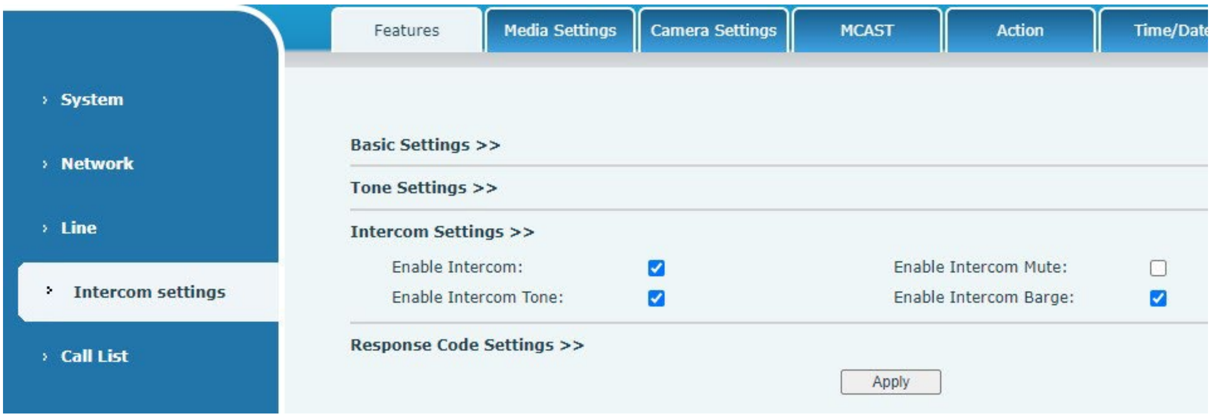
Tone Settings >>

Enable Holding Tone: ☑
Enable Call Waiting Tone: ☑
Play Dialing DTMF Tone: ☑
Play Talking DTMF Tone: ☑
Auto Answer Tone: ☑
Ring Back Tone: Default
Busy Tone: Default
Open Success Prompting: Default
Open Failed Prompting: Default
Close Door Prompting: Default
Issuing Success Prompting: Default
Issuing Failed Prompting: Default
Revoke Prompting: Default
Revoke Failed Prompting: Default
Door Sensor Prompting: Default

# Advanced Function

## *Intercom*

The device can answer intercom calls automatically.



Basic Settings >>

Tone Settings >>

Intercom Settings >>

Enable Intercom: ☑ Enable Intercom Mute: □

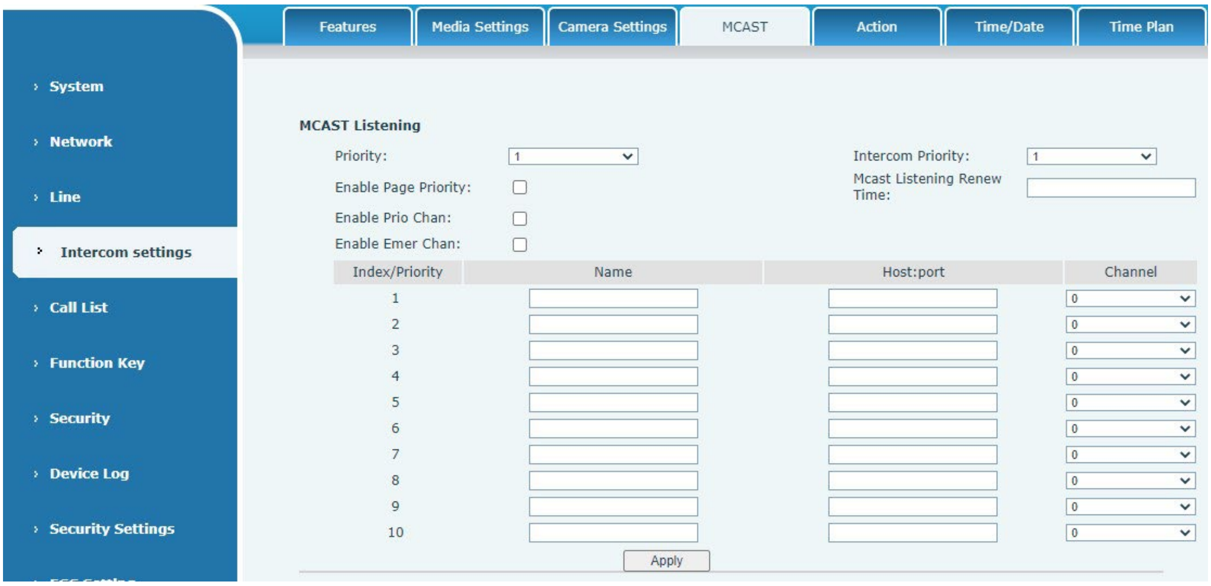
Enable Intercom Tone: ☑ Enable Intercom Barge: ☑

Response Code Settings >>

| Parameters | Description |
|---|---|
| Enable Intercom | When the intercom system is enabled, the device will accept the SIP header call info of the Call request Command automatically |
| Enable Intercom Barge | If the option is enabled, device 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 intercom 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. |

## *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.



MCAST Listening

Priority: 1 Intercom Priority: 1

Enable Page Priority: □ Mcast Listening Renew Time:

Enable Prio Chan: □

Enable Emer Chan: □

| Index/Priority | Name | Host:port | Channel |
|---|---|---|---|
| 1 | | | 0 |
| 2 | | | 0 |
| 3 | | | 0 |
| 4 | | | 0 |
| 5 | | | 0 |
| 6 | | | 0 |
| 7 | | | 0 |
| 8 | | | 0 |
| 9 | | | 0 |
| 10 | | | 0 |

| 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.

**MCAST Dynamic：**

Description: send multicast configuration information through SIP notify signaling. After receiving the message, the device configures it to the system for multicast monitoring or cancels multicast monitoring in the system.

## *Hotspot*

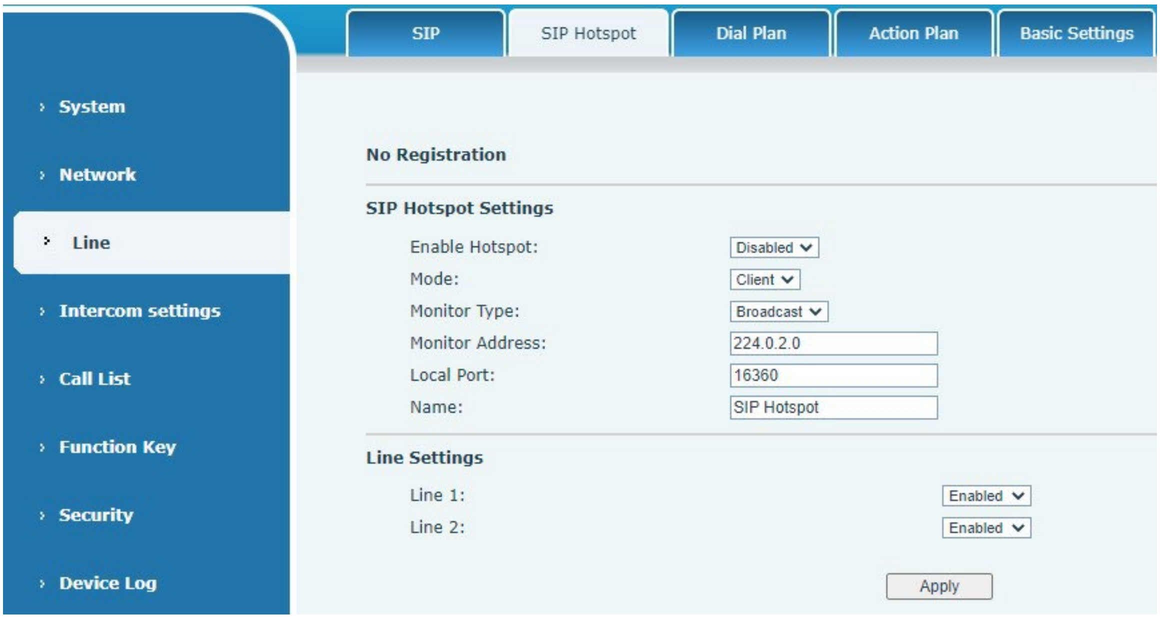
SIP hotspot is a simple utility. Its configuration is simple, which can realize the function of group vibration and expand the quantity of sip account. Take one device A as the SIP hotspot and the other devices (B, C) as the SIP hotspot client. When someone calls device A, devices A, B, and C will ring, 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.

| 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.



No Registration

SIP Hotspot Settings

Enable Hotspot: Disabled
Mode: Client
Monitor Type: Broadcast
Monitor Address: 224.0.2.0
Local Port: 16360
Name: SIP Hotspot

Line Settings

Line 1: Enabled
Line 2: Enabled

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” webpage).

Calling internal extension:

- The hotspot server and client can dial each other (example: extension 1 dials extension 0)

# Web Configurations

## *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.

## *System >> Information*

User can get the device information in this page including,

- Model
- Hardware
- Software
- Uptime
- Last uptime
- MEMInfo
- System time

And summarization of network status,

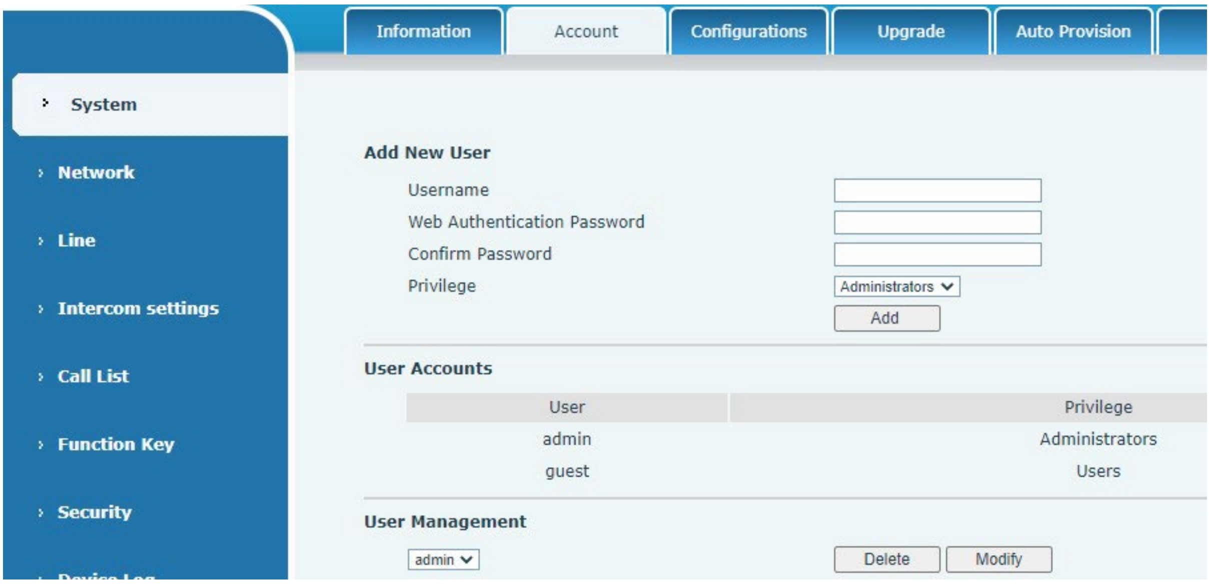
- Network Mode
- MAC
- IP
- Subnet mask
- Default getaway

Besides, summarization of SIP account status,

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

## *System >> 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.



Add New User

| | |
|---|---|
| Username | |
| Web Authentication Password | |
| Confirm Password | |
| Privilege | Administrators |

User Accounts

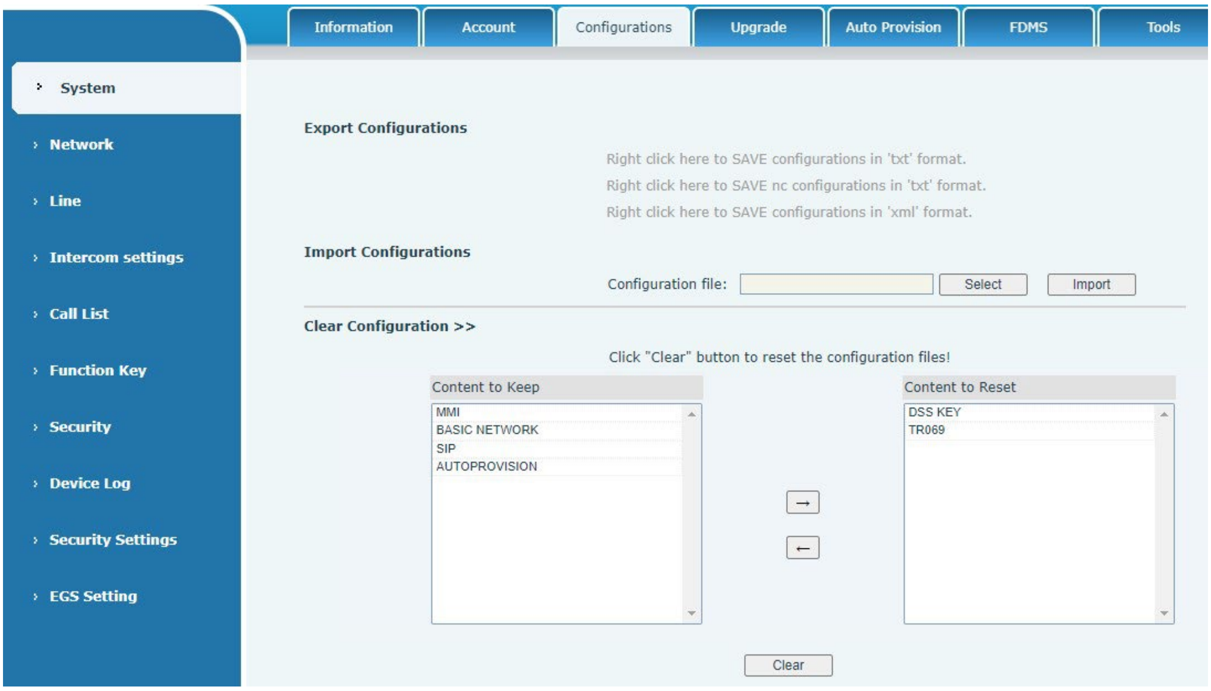
| User | Privilege |
|---|---|
| admin | Administrators |
| guest | Users |

User Management

admin

## *System >> Configurations*

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 here to SAVE configurations in 'txt' format.

Right click here to SAVE nc configurations in 'txt' format.

Right click here to SAVE configurations in 'xml' format.

Import Configurations

Configuration file: Select Import

Clear Configuration >>

Click "Clear" button to reset the configuration files!

Content to Keep: MMI, BASIC NETWORK, SIP, AUTOPROVISION

Content to Reset: DSS KEY, TR069

→ ← Clear

### Export Configurations

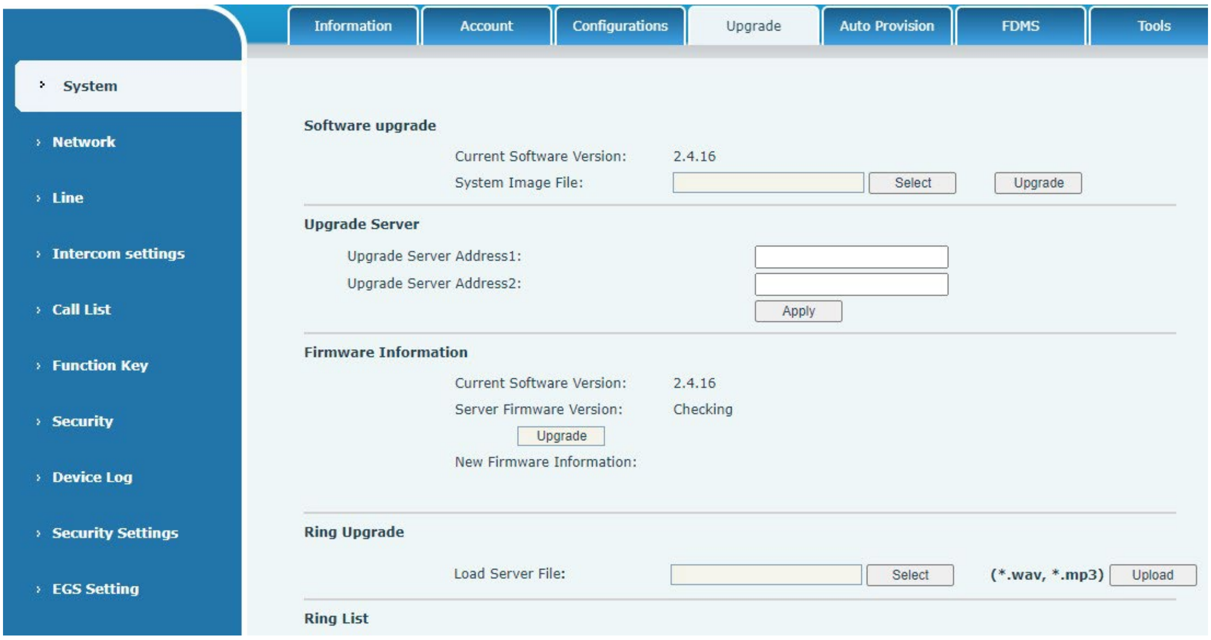
Right click to select target save as, that is, to download the device's configuration file, suffix “.txt”. (note: profile export requires administrator privileges)

- **Import Configurations**
  Import the configuration file of Settings. The device will restart automatically after successful import, and the configuration will take effect after restart
- **Clear Configurations**
  Select the module in the configuration file to clear. SIP: account configuration. AUTOPROVISION: automatically upgrades the configuration TR069:TR069 related configuration MMI: MMI module, including authentication user information, web access protocol, etc. DSS Key: DSS Key configuration
- **Clear Tables**
  Select the local data table to be cleared, all selected by default.
- **Reset Phone**

  The phone data will be cleared, including configuration and database tables.

## *System >> 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. Upgrade the ringtone. Supports wav and MP3 format.



Software upgrade

Current Software Version: 2.4.16

System Image File:

Upgrade Server

Upgrade Server Address1:

Upgrade Server Address2:

Firmware Information

Current Software Version: 2.4.16

Server Firmware Version: Checking

New Firmware Information:

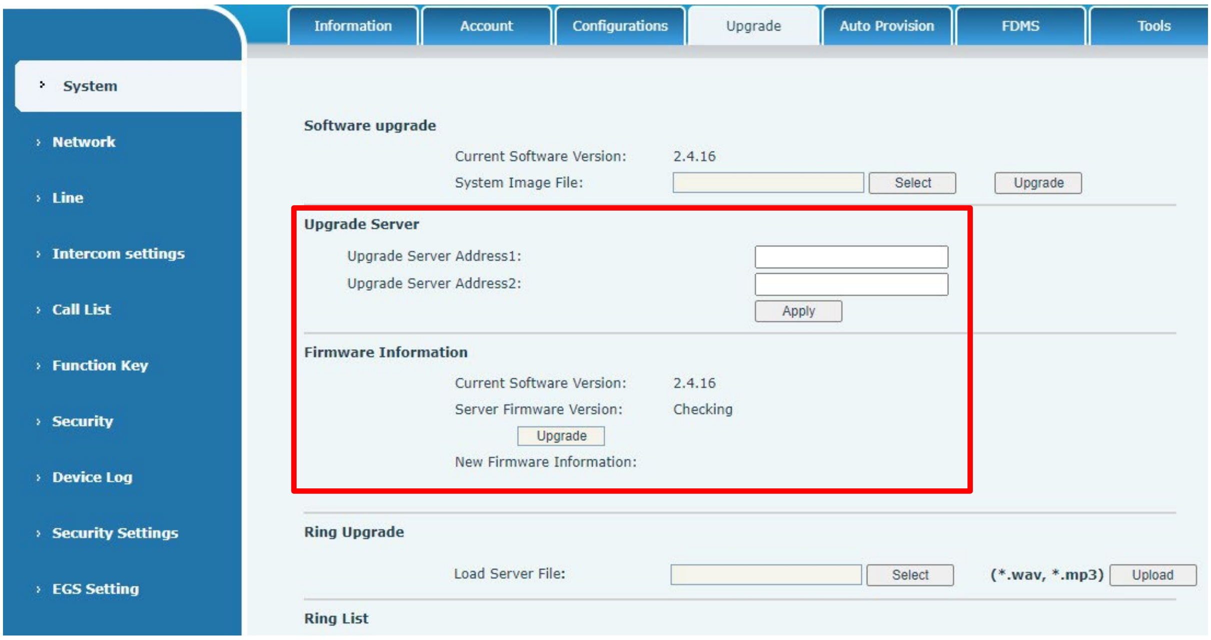
Ring Upgrade

Load Server File: (*.wav, *.mp3)

Ring List

**Firmware Upgrade：**

- Web page： Login phone web page, go to **System** >> **Upgrade**.



Software upgrade

Current Software Version: 2.4.16

System Image File:

Upgrade Server

Upgrade Server Address1:

Upgrade Server Address2:

Firmware Information

Current Software Version: 2.4.16

Server Firmware Version: Checking

New Firmware Information:

Ring Upgrade

Load Server File: (*.wav, *.mp3)

Ring List

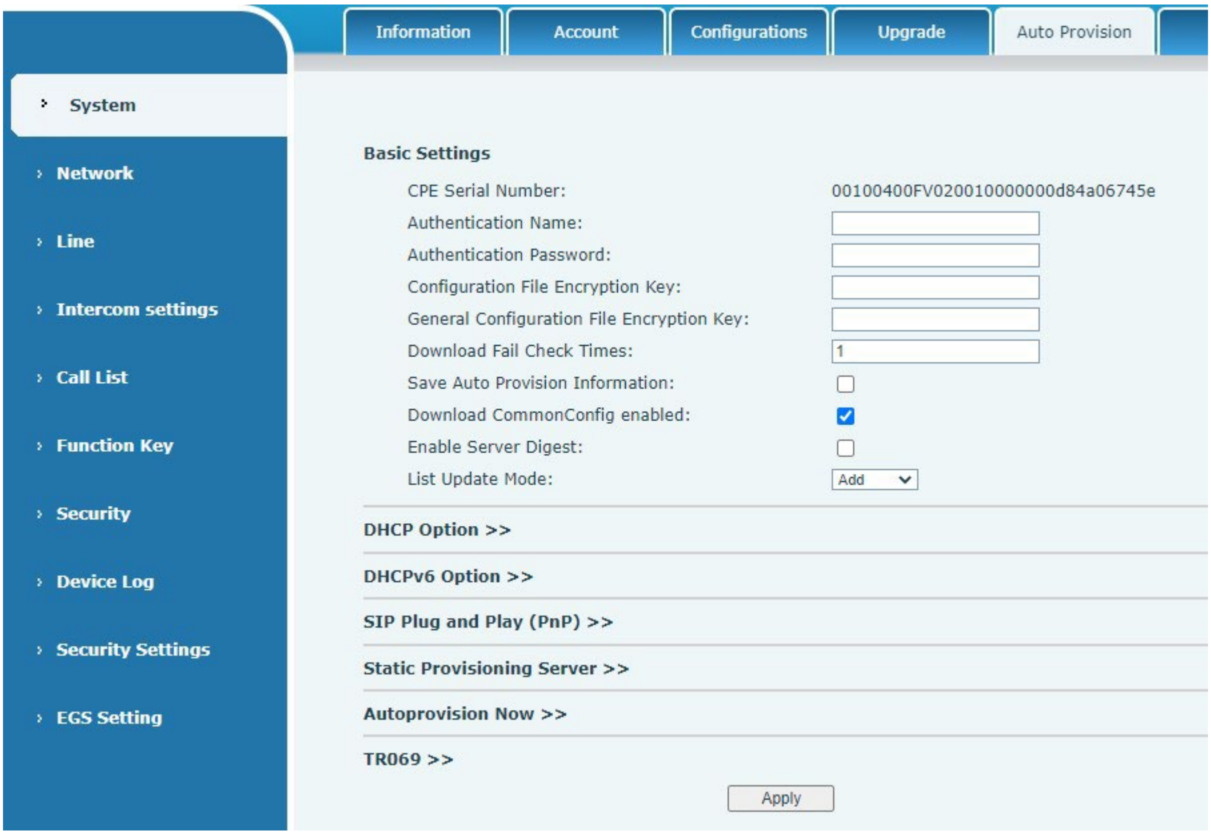
| Parameter | Description |
|---|---|
| **Upgrade server** | |
| Enable Auto Upgrade | Enable automatic upgrade, If there is a new version txt and new software firmware on the server, phone will show a prompt upgrade message after Update Interval. |
| Upgrade Server Address1 | Set available upgrade server address. |

| | |
|---|---|
| Upgrade Server Address2 | Set available upgrade server address. |
| Update Interval | Set Update Interval. |
| **Firmware Information** | |
| Current Software Version | It will show Current Software Version. |
| Server Firmware Version | It will show Server Firmware Version. |
| [Upgrade] button | If there is a new version txt and new software firmware on the server, the page will display version information and upgrade button will become available;<br>Click [Upgrade] button to upgrade the new firmware. |
| New version description information | When there is a corresponding TXT file and version on the server side, the TXT and version information will be displayed under the new version description information. |

- The file requested from the server is a TXT file called vendor_model_hw10.txt.Hw followed by the hardware version number, it will be written as hw10 if no difference on hardware. All Spaces in the filename are replaced by underline.
- The URL requested by the phone is HTTP:// server address/vendor_Model_hw10.txt ：　The new version and the requested file should be placed in the download directory of the HTTP server.
- TXT file format must be UTF-8
- vendor_model_hw10.TXT.  The file format is as follows：
  Version=1.6.3 #Firmware
  Firmware=xxx/xxx.z
  #URL，　Relative paths are supported and absolute paths are possible, distinguished by the presence of protocol headers.
  BuildTime=2018.09.11 20:00
  Info=TXT|XML
  Xxxxx Xxxxx Xxxxx Xxxxx
- After the interval of update cycle arrives, if the server has available files and versions, the phone will prompt as shown below. Click [view] to check the version information and upgrade.

## *System >> Auto Provision*

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



Basic Settings

| | |
|---|---|
| CPE Serial Number: | 00100400FV020010000000d84a06745e |
| Authentication Name: | |
| Authentication Password: | |
| Configuration File Encryption Key: | |
| General Configuration File Encryption Key: | |
| Download Fail Check Times: | 1 |
| Save Auto Provision Information: | □ |
| Download CommonConfig enabled: | ☑ |
| Enable Server Digest: | □ |
| List Update Mode: | Add |

DHCP Option >>

DHCPv6 Option >>

SIP Plug and Play (PnP) >>

Static Provisioning Server >>

Autoprovision Now >>

TR069 >>

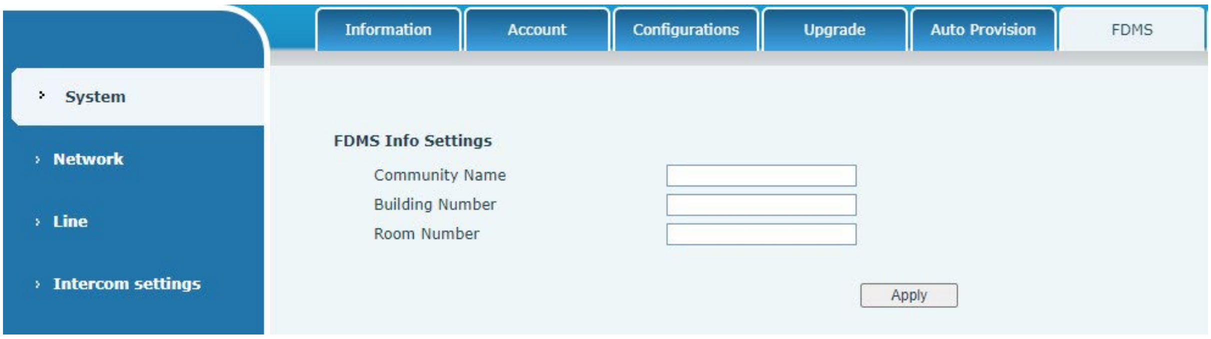
Devices support SIP PnP, DHCP options, Static provision, TR069. If all of the 4 methods are enabled, the priority from high to low as follows: PNP>DHCP>TR069> Static Provisioning.

Transferring protocol: FTP、 TFTP、 HTTP、 HTTPS

| Auto Provision | |
|---|---|
| **Parameters** | **Description** |
| **Basic settings** | |
| CPE Serial Number | Display the device SN |
| Authentication Name | The user name of provision server |
| Authentication Password | The password of provision server |
| Configuration File Encryption Key | If the device configuration file is encrypted , user should add the encryption key here |
| General Configuration File Encryption Key | If the common configuration file is encrypted, user should add the encryption key here |
| Save Auto Provision Information | Save the HTTP/HTTPS/FTP user name and password. If the provision URL is kept, the information will be kept. |
| Download Common Config enabled | Whether phone will download the common configuration file. |
| 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 | Configure DHCP option, DHCP option supports DHCP custom option \| DHCP option 66 \| DHCP option 43, 3 methods to get the provision URL. The default is Option 66. |
| Custom Option Value | Custom Option value is allowed from 128 to 254. The option value must be same as server define. |
| Enable DHCP Option 120 | Use Option120 to get the SIP server address from DHCP server. |
| **DHCPv6 Option** | |
| Option Value | Configure DHCPv6 option, DHCPv6 option supports custom option 66, option 43, 3 methods to get the provision URL. The default is Disable. |
| 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 enabled, 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 | Provisioning server address. Support both IP address and domain address. |
| 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.<br>1. Disabled.<br>2. Update after reboot.<br>3. Update after interval. |
| **Static Provisioning Server** | |
| **TR069** | |
| Enable TR069 | Enable TR069 after selection |
| 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) |
| Enable TR069 Warning Tone | If TR069 is enabled, there will be a prompt tone when connecting. |
| TLS Version | TLS Version |
| STUN server address | Enter the STUN address |
| Enable the STUN | Enable the STUN |

## System >> FDMS



FDMS Info Settings

Community Name

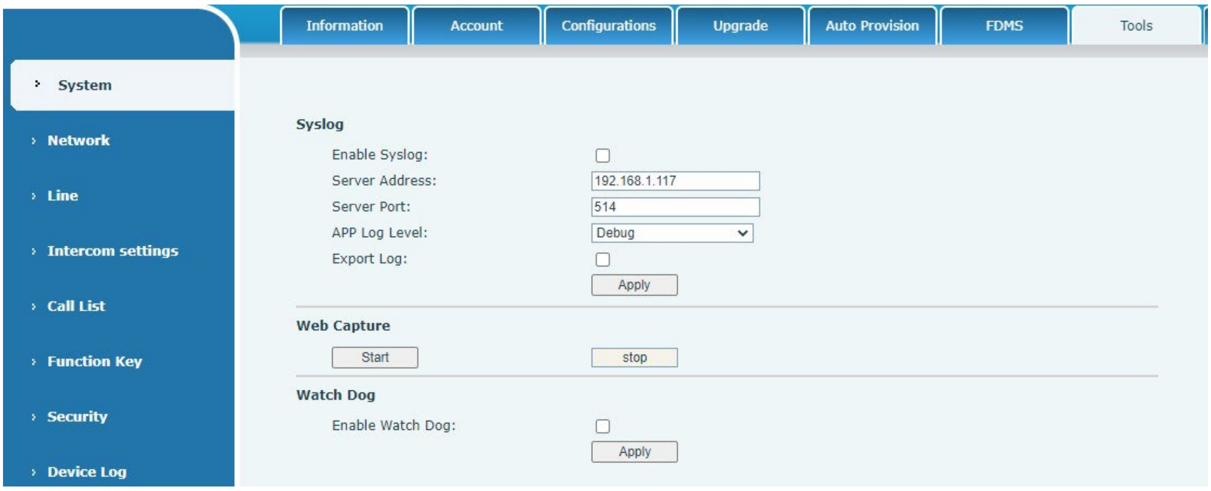
Building Number

Room Number

| FDMS information Settings | |
|---|---|
| Community Name | Name of equipment installation community |
| Building Number | Name of equipment installation building |
| Room Number | Equipment installation room name |

## System >> 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.



Syslog

Enable Syslog: □

Server Address: 192.168.1.117

Server Port: 514

APP Log Level: Debug

Export Log: □

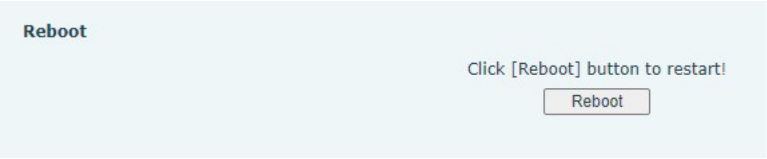
Web Capture

Watch Dog

Enable Watch Dog: □

## System >> Reboot

This page can restart the device.

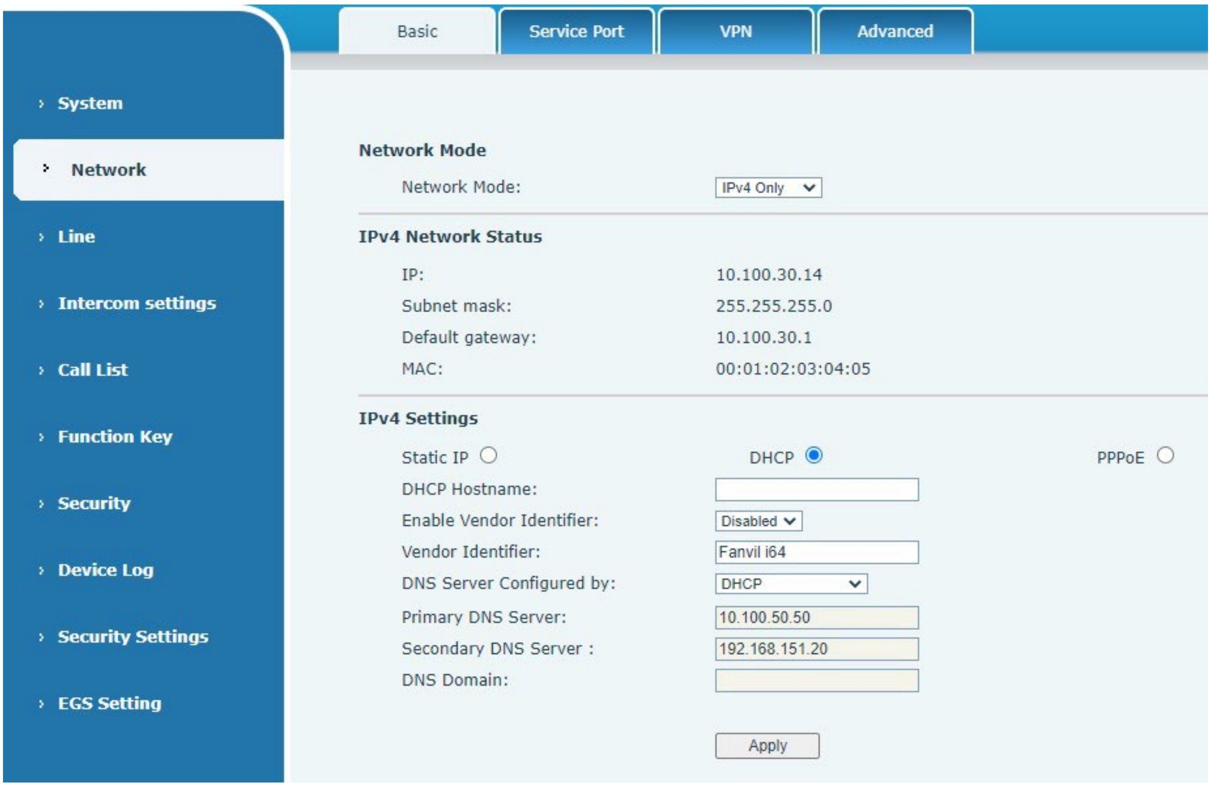


Reboot

Click [Reboot] button to restart!

## *Network >> Basic*

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



**Network Mode**

Network Mode: IPv4 Only

**IPv4 Network Status**

IP: 10.100.30.14

Subnet mask: 255.255.255.0

Default gateway: 10.100.30.1

MAC: 00:01:02:03:04:05

**IPv4 Settings**

Static IP ○ DHCP ● PPPoE ○

DHCP Hostname:

Enable Vendor Identifier: Disabled

Vendor Identifier: Fanvil i64

DNS Server Configured by: DHCP

Primary DNS Server: 10.100.50.50

Secondary DNS Server : 192.168.151.20

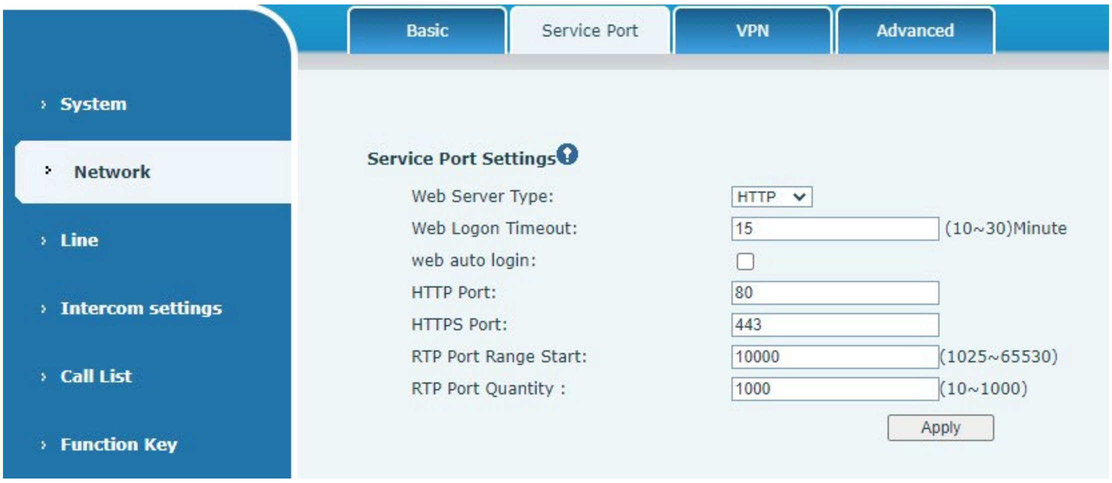
DNS Domain:

| Field Name | Explanation |
|---|---|
| **IPv4 Network Status** | |
| IP | The current IP address of the device |
| Subnet mask | The current Subnet Mask |
| Default gateway | The current Gateway IP address |
| MAC | The MAC address of the device |
| **IPv4 Settings** | |
| **Settings** | |
| Select the appropriate network mode. The device supports three network modes: | |
| Static IP | Network parameters must be entered manually and will not be changed. All parameters are provided by the ISP. |
| DHCP | Network parameters are provided automatically by a DHCP server. |
| If Static IP is chosen, 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. |
| DNS Domain | Enter the domain of the DNS. |
| attention：<br>1. After setting the parameters, click Apply to take effect.<br>2. If you change the IP address, the webpage will no longer respond. Enter the new IP address in web browser to access the device.<br>3. If the device uses DHCP to obtain IP, 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 device 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

## *Network >> Service Port*

This page provides the settings of webpage login protocol, protocol port and RTP port.

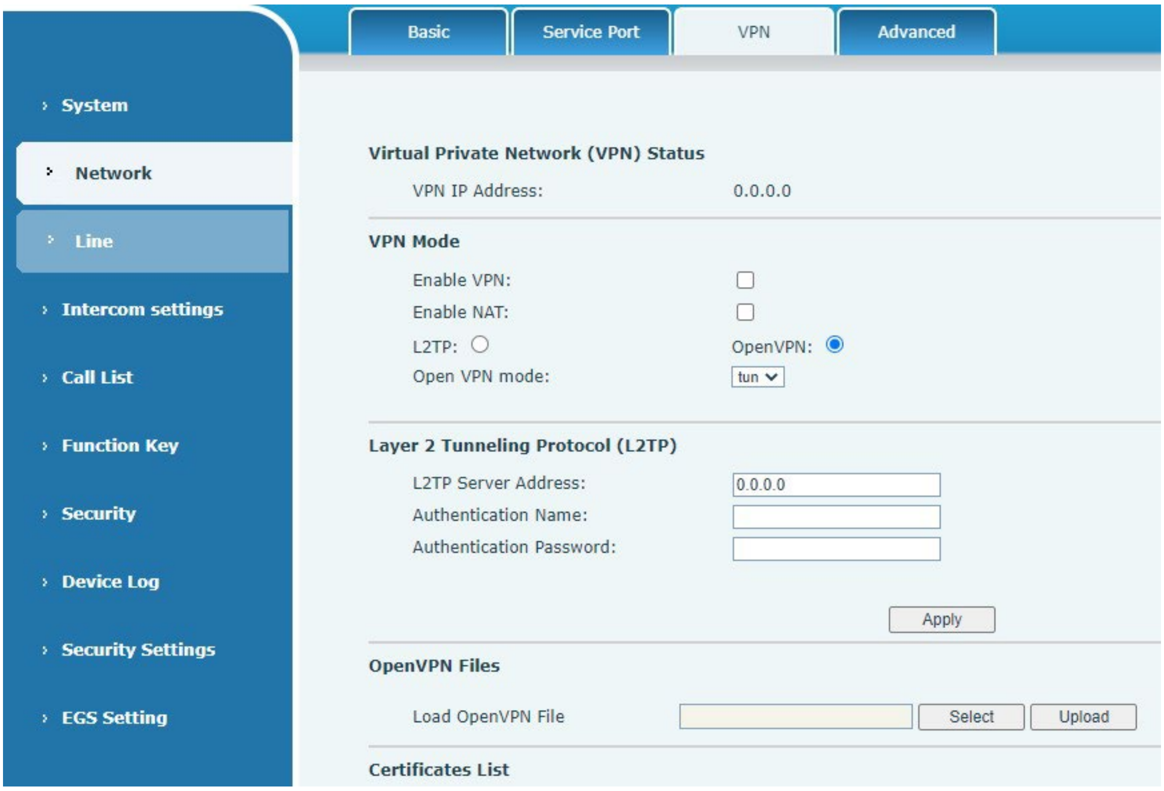


Service Port Settings

Web Server Type: HTTP
Web Logon Timeout: 15 (10~30)Minute
web auto login: □
HTTP Port: 80
HTTPS Port: 443
RTP Port Range Start: 10000 (1025~65530)
RTP Port Quantity : 1000 (10~1000)

| Parameter | Description |
|---|---|
| Web server type | Restart after setting takes effect. Optional web login as HTTP/HTTPS |
| Web login timeout | The default is 15 minutes, the timeout will automatically log out of the login page, and you need to log in again |
| Web page automatic login | No need to enter the user name and password after the timeout, it will automatically log in to the web page. |
| HTTP port | The default is 80, if you want security, you can set another port such as: 8080, web page login: HTTP://ip:8080 |
| HTTPS port | The default is 443, same as HTTP port usage |
| RTP port start range | The value range is 1025-65535. The value of rtp port starts from the initial value set. Each time a call is made, the value of the voice and video ports is increased by 2 |
| RTP port quantity | Number of calls |

## *Network >> VPN*



**Virtual Private Network (VPN) Status**

VPN IP Address: 0.0.0.0

**VPN Mode**

Enable VPN: □

Enable NAT: □

L2TP: ○ OpenVPN: ●

Open VPN mode: tun

**Layer 2 Tunneling Protocol (L2TP)**

L2TP Server Address: 0.0.0.0

Authentication Name:

Authentication Password:

**OpenVPN Files**

Load OpenVPN File

**Certificates List**

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, use OpenVPN instead.

To establish a L2TP connection, users should log in to the device web portal, open page [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 to the VPN automatically when the device boots up every time until user disable it. Sometimes, if the VPN connection does not established immediately, user may try to reboot the device and check if VPN connection established after reboot.

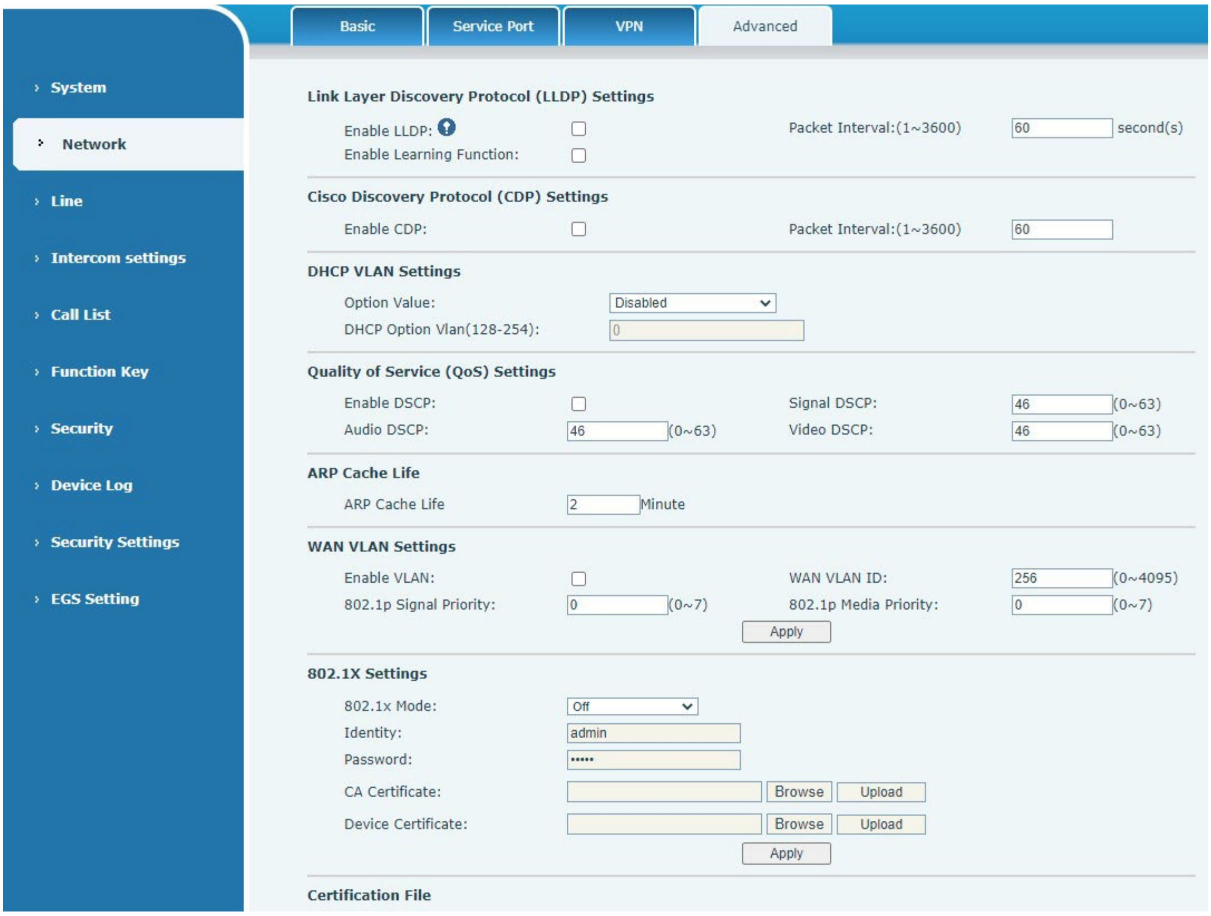
- **OpenVPN**

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 then uploads these files to the device in the web page [Network] -> [VPN], Section OpenVPN Files. Then user should check “Enable VPN” and select “OpenVPN” in VPN Mode and click “Apply” to enable OpenVPN connection. The connection will be re-established every time the device is rebooted, or until user disables it manually.

## *Network >> Advanced*



Link Layer Discovery Protocol (LLDP) Settings

Enable LLDP: □ Packet Interval:(1~3600) 60 second(s)
Enable Learning Function: □

Cisco Discovery Protocol (CDP) Settings

Enable CDP: □ Packet Interval:(1~3600) 60

DHCP VLAN Settings

Option Value: Disabled
DHCP Option Vlan(128-254): 0

Quality of Service (QoS) Settings

Enable DSCP: □ Signal DSCP: 46 (0~63)
Audio DSCP: 46 (0~63) Video DSCP: 46 (0~63)

ARP Cache Life

ARP Cache Life 2 Minute

WAN VLAN Settings

Enable VLAN: □ WAN VLAN ID: 256 (0~4095)
802.1p Signal Priority: 0 (0~7) 802.1p Media Priority: 0 (0~7)
Apply

802.1X Settings

802.1x Mode: Off
Identity: admin
Password: •••••
CA Certificate: Browse Upload
Device Certificate: Browse Upload
Apply

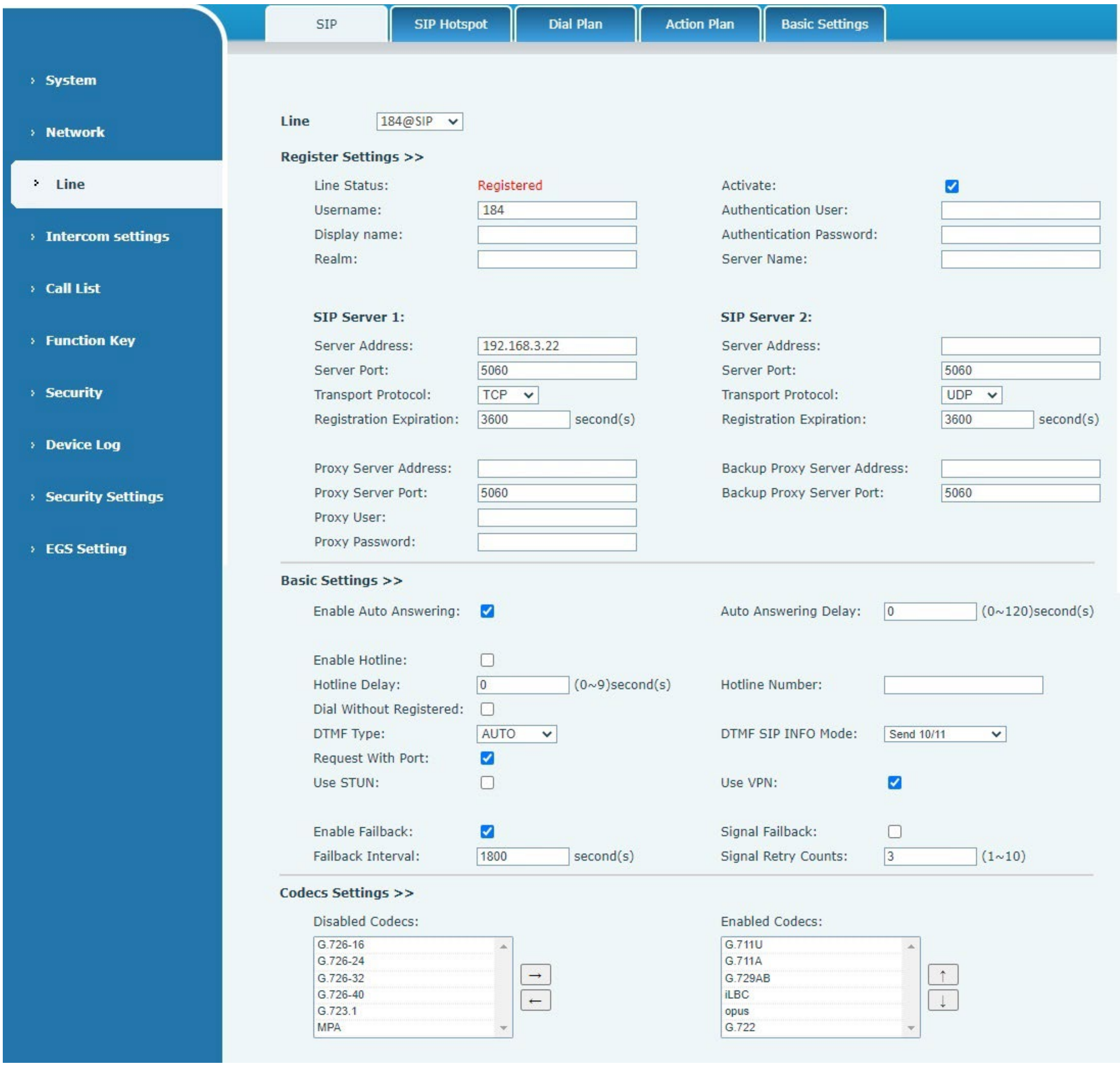
Certification File

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

| 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 |

## *Line >> SIP*



Line: 184@SIP

Register Settings >>

Line Status: Registered
Activate: ☑
Username: 184
Authentication User:
Display name:
Authentication Password:
Realm:
Server Name:

SIP Server 1:
Server Address: 192.168.3.22
Server Port: 5060
Transport Protocol: TCP
Registration Expiration: 3600 second(s)

SIP Server 2:
Server Address:
Server Port: 5060
Transport Protocol: UDP
Registration Expiration: 3600 second(s)

Proxy Server Address:
Proxy Server Port: 5060
Proxy User:
Proxy Password:
Backup Proxy Server Address:
Backup Proxy Server Port: 5060

Basic Settings >>

Enable Auto Answering: ☑
Auto Answering Delay: 0 (0~120)second(s)
Enable Hotline: □
Hotline Delay: 0 (0~9)second(s)
Hotline Number:
Dial Without Registered: □
DTMF Type: AUTO
DTMF SIP INFO Mode: Send 10/11
Request With Port: ☑
Use STUN: □
Use VPN: ☑
Enable Failback: ☑
Failback Interval: 1800 second(s)
Signal Failback: □
Signal Retry Counts: 3 (1~10)

Codecs Settings >>

Disabled Codecs: G.726-16, G.726-24, G.726-32, G.726-40, G.723.1, MPA
Enabled Codecs: G.711U, G.711A, G.729AB, iLBC, opus, G.722

| Parameters | Description |
|---|---|
| **Register Settings** | |
| 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. |
| Activate | Whether the service of the line should be activated |

| | |
|---|---|
| Username | Enter the username of the service account. |
| Authentication User | Enter the authentication user of the service account |
| Display Name | Enter the display name to be sent in a call request. |
| Authentication Password | Enter the authentication password of the service account |
| Realm | Enter the SIP domain if requested by the service provider |
| Server Name | Input server name. |
| **SIP Server 1** | |
| Server Address | Enter the IP or FQDN address of the SIP server |
| Server Port | Enter the SIP server port, default is 5060 |
| Transport Protocol | Set up the SIP transport line using TCP or UDP or TLS. |
| Registration Expiration | Set SIP expiration date. |
| **SIP Server 2** | |
| Server Address | Enter the IP or FQDN address of the SIP server |
| Server Port | Enter the SIP server port, default is 5060 |
| Transport Protocol | Set up the SIP transport line using TCP or UDP or TLS. |
| Registration Expiration | Set SIP expiration date. |
| SIP Proxy Server Address | Enter the IP or FQDN address of the SIP proxy server. |
| Proxy Server Port | Enter the SIP proxy server port, default is 5060. |
| Proxy User | Enter the SIP proxy user. |
| Proxy Password | Enter the SIP proxy password. |
| Backup Proxy Server Address | Enter the IP or FQDN address of the backup proxy server. |
| Backup Proxy Server Port | Enter the backup proxy server port, default is 5060. |
| **Basic Settings** | |
| Enable Auto Answering | Enable auto-answering, the incoming calls will be answered automatically after the delay time |
| Auto Answering Delay | Set the delay for incoming call before the device automatically answered it |
| Enable Hotline | Enable hotline configuration, the device will dial to the specific number immediately at audio channel opened by off-hook handset or turn on hands-free speaker or headphone |
| Hotline Delay | Set the delay for hotline before the device automatically dials it |
| Hotline Number | Set the hotline dialing number |
| Dial Without Registered | Set call out by proxy without registration |
| Enable Missed Call Log | If enabled, the phone will save missed calls into the call history record. |
| DTMF Type | Set the DTMF type to be used for the line |
| Use VPN | Set the line to use VPN restrict route |
| Use STUN | Set the line to use STUN for NAT traversal |
| Enable Failback | Whether to switch to the primary server when it is available. |
| Failback Interval | A Register message is used to periodically detect the time interval for the availability of the main Proxy. |
| Signal Failback | Multiple proxy cases, whether to allow the invite/register request to also execute failback. |
| Signal Retry Counts | The number of attempts that the SIP Request considers proxy unavailable under multiple proxy scenarios. |

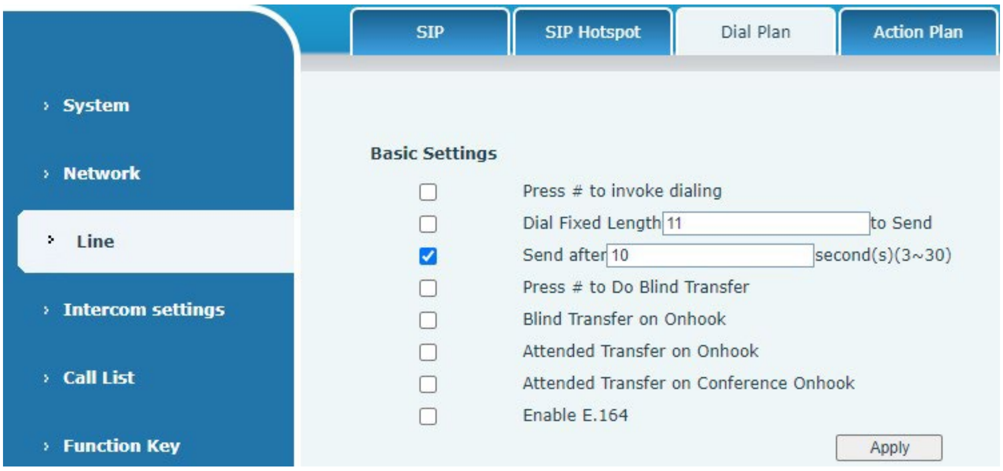
| | |
|---|---|
| **Codecs Settings** | Set the priority and availability of the codecs by adding or remove them from the list. |
| **Advanced Settings** | |
| Use Feature Code | When this setting is enabled, the features in this section will not be handled by the device itself but by the server instead. In order to control the enabling of the features, the device will send feature code to the server by dialing the number specified in each feature code field. |
| Enable Blocking Anonymous Call | Set the feature code to dial to the server |
| Disable Blocking Anonymous Call | Set the feature code to dial to the server |
| Call Waiting On Code | Set the feature code to dial to the server |
| Call Waiting Off Code | Set the feature code to dial to the server |
| Send Anonymous on Code | Set the feature code to dial to the server |
| Send Anonymous Off Code | Set the feature code to dial to the server |
| Enable Session Timer | Set the line to enable call ending by session timer refresh.<br>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 |
| BLF Server | The registered server will receive the subscription package from ordinary application of BLF phone.<br>Enter the BLF server, if the sever does not support subscription package, the registered server and subscription server will be separated. |
| 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 |
| Keep Authentication | Keep the authentication parameters from previous authentication |
| Blocking Anonymous Call | Reject any incoming call without presenting caller ID |
| User Agent | Set the user agent, the default is Model with Software Version. |
| Specific Server Type | Set the line to collaborate with specific server type |
| SIP Version | Set the SIP version |
| Anonymous Call Standard | Set the standard to be used for anonymous |
| Local Port | Set the local port |
| Ring Type | Set the ring tone type for the line |
| Enable user=phone | Sets user=phone in SIP messages. |
| Use Tel Call | Set use telephone call |
| Auto TCP | Using TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes |
| Enable Rport | Set the line to add rport in SIP headers |
| Enable PRACK | Set the line to support PRACK SIP message |
| DNS Mode | Select DNS mode, A, SRV, NAPTR |
| Enable Long Contact | Allow more parameters in contact field per RFC 3840 |
| 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. |
| Convert URI | Convert not digit and alphabet characters to %hh hex code |

| | |
|---|---|
| Use Quote in Display Name | Whether to add quote in display name, i.e. “VoIP” vs VoIP |
| Enable GRUU | Support Globally Routable User-Agent URI (GRUU) |
| Sync Clock Time | Time Sync with server |
| Enable Inactive Hold | With the post-call hold capture package enabled, you can see that in the INVITE package, SDP is inactive. |
| Caller ID Header | Set the Caller ID Header |
| Use 182 Response for Call waiting | Set the device to use 182 response code at call waiting response |
| Enable Feature Sync | Feature Sync with server |
| Enable SCA | Enable/Disable SCA ( Shared Call Appearance ) |
| CallPark Number | Set the CallPark number. |
| Server Expire | Set the timeout to use the server. |
| TLS Version | Choose TLS Version. |
| uaCSTA Number | Set uaCSTA Number. |
| Enable Click to Talk | With the use of special server, click to call out directly after enabling. |
| Enable Chgport | Whether port updates are enabled. |
| Intercom Number | Set Intercom Number. |
| Unregister On Boot | Whether to enable logout function. |
| Enable MAC Header | Whether to open the registration of SIP package with user agent with MAC or not. |
| Enable Register MAC Header | Whether to open the registration is user agent with MAC or not. |
| PTime(ms) | Set whether to bring ptime field, default no. |
| **SIP Global Settings** | |
| Strict Branch | Set up to strictly match the Branch field. |
| Enable Group | Set open group. |
| Enable RFC4475 | Set to enable RFC4475. |
| Enable Strict UA Match | Enable strict UA matching. |
| Registration Failure Retry Time | Set the registration failure retry time. |
| Local SIP Port | Modify the phone SIP port. |
| Enable uaCSTA | Set to enable the uaCSTA function. |

## *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 Hotspot for details.

## *Line >> Dial Plan*



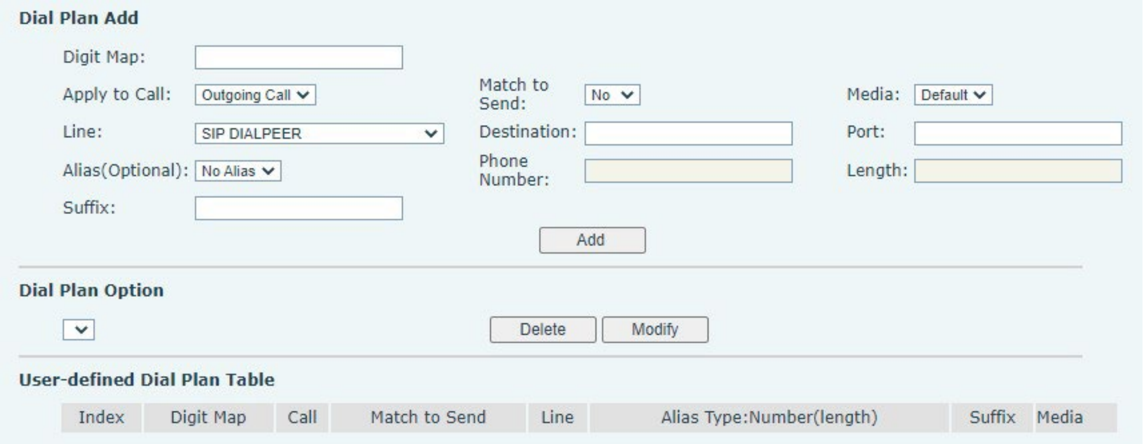
**Basic Settings**

- ☐ Press # to invoke dialing
- ☐ Dial Fixed Length 11 to Send
- ☑ Send after 10 second(s)(3~30)
- ☐ Press # to Do Blind Transfer
- ☐ Blind Transfer on Onhook
- ☐ Attended Transfer on Onhook
- ☐ Attended Transfer on Conference Onhook
- ☐ Enable E.164

Apply

| Parameters | Description |
|---|---|
| Press # to invoke dialing | The user dials the other party's number and then adds the # to dial out; |
| Dial Fixed Length | The number entered by the user is automatically dialed out when it reaches a fixed length |
| Timeout dial | The device dials automatically after timeout |

### Dial Plan Add:



**Dial Plan Add**

| | | | | | |
|---|---|---|---|---|---|
| Digit Map: | | | | | |
| Apply to Call: | Outgoing Call | Match to Send: | No | Media: | Default |
| Line: | SIP DIALPEER | Destination: | | Port: | |
| Alias(Optional): | No Alias | Phone Number: | | Length: | |
| Suffix: | | | | | |

Add

**Dial Plan Option**

Delete Modify

**User-defined Dial Plan Table**

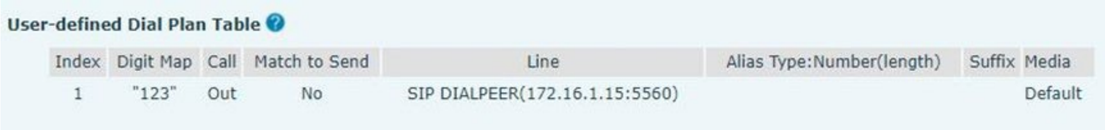
| Index | Digit Map | Call | Match to Send | Line | Alias Type:Number(length) | Suffix | Media |
|---|---|---|---|---|---|---|---|

| Parameters | Description |
|---|---|
| Dial rule | There are two types of matching: Full Matching or Prefix Matching. In Full matching, the entire phone number is entered and then mapped per the Dial Peer rules.<br>In prefix matching, only part of the number is entered followed by T. The mapping will then take place whenever these digits are dialed.  Prefix mode supports a maximum of 30 digits. |
| Note: Two different special characters are used.<br>• x -- Matches any single digit that is dialed.<br>• [ ] -- Specifies a range of numbers to be matched. It may be a range, a list of ranges separated by commas, or a list of digits. | |
| Destination | Set Destination address. This is for IP direct. |
| Port | Set the Signal port, and the default is 5060 for SIP. |

| | |
|---|---|
| Alias | Set the Alias. This is the text to be added, replaced or deleted. It is an optional item. |
| Note: There are four types of aliases.<br>• all: xxx – xxx will replace the phone number.<br>• add: xxx – xxx will be dialed before any phone number.<br>• del –The characters will be deleted from the phone number.<br>• rep: xxx – xxx will be substituted for the specified characters. | |
| Suffix | Characters to be added at the end of the phone number. It is an optional item. |
| Length | Set the number of characters to be deleted. For example, if this is set to 3, the phone will delete the first 3 digits of the phone number. It is an optional item. |

This feature allows the user to create rules to make dialing easier. There are several different options for dialing rules. The examples below will show how this can be used.

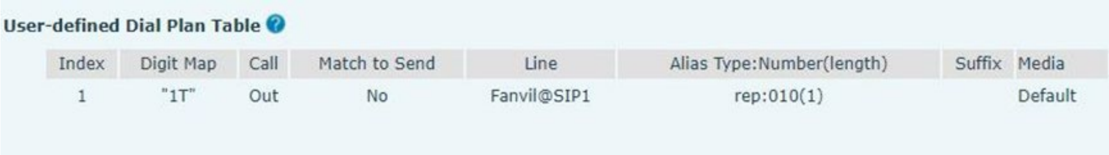
**Example 1**: All Substitution -- Assume that it is desired to place a direct IP call to IP address 172.168.2.208. Using this feature, 123 can be substituted for 172.168.2.208.



User-defined Dial Plan Table

| Index | Digit Map | Call | Match to Send | Line | Alias Type:Number(length) | Suffix | Media |
|---|---|---|---|---|---|---|---|
| 1 | "123" | Out | No | SIP DIALPEER(172.16.1.15:5560) | | | Default |

**Example 2**: Partial Substitution -- To dial a long-distance call to Beijing requires dialing area code 010 before the local phone number.  Using this feature 1 can be substituted for 010. For example, to call 62213123 would only require dialing 162213123 instead of 01062213123.



User-defined Dial Plan Table

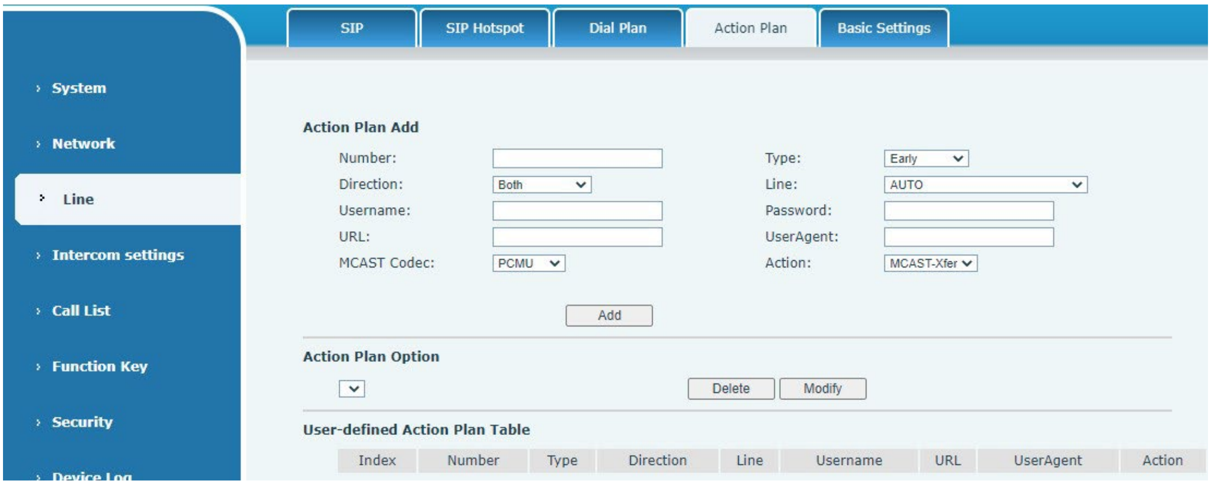
| Index | Digit Map | Call | Match to Send | Line | Alias Type:Number(length) | Suffix | Media |
|---|---|---|---|---|---|---|---|
| 1 | "1T" | Out | No | Fanvil@SIP1 | rep:010(1) | | Default |

**Example 3**: Addition -- Two examples are shown. In the first case, it is assumed that 0 must be dialed before any 11-digit number beginning with 13. In the second case, it is assumed that 0 must be dialed before any 11-digit number beginning with 135, 136, 137, 138, or 139. Two different special characters are used.

x -- Matches any single digit that is dialed.

[] -- Specifies a range of numbers to be matched. It may be a range, a list of ranges separated by commas, or a list of digits.

## Line >> Action Plan



Action Plan Add

Number:
Direction: Both
Username:
URL:
MCAST Codec: PCMU
Type: Early
Line: AUTO
Password:
UserAgent:
Action: MCAST-Xfer

Action Plan Option

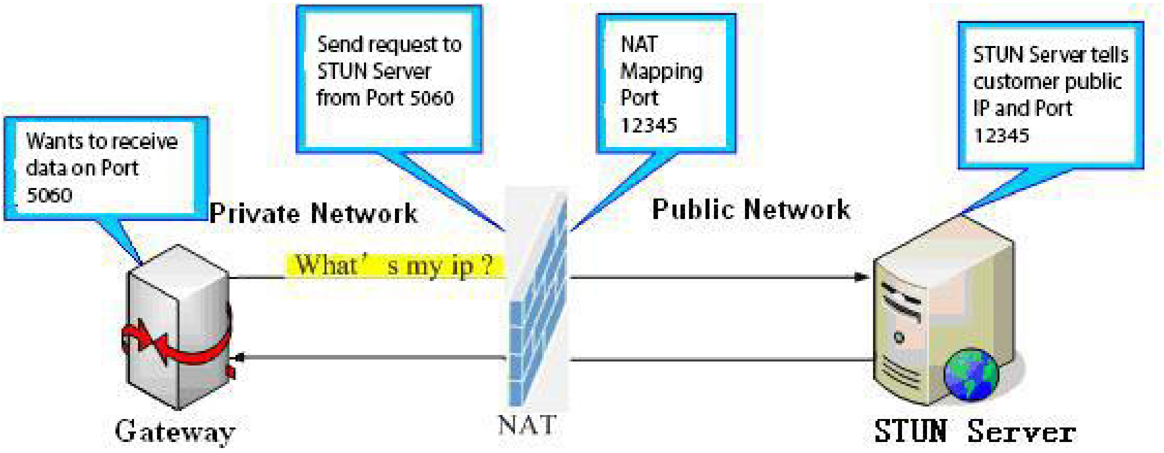
User-defined Action Plan Table

| Index | Number | Type | Direction | Line | Username | URL | UserAgent | Action |
|---|---|---|---|---|---|---|---|---|

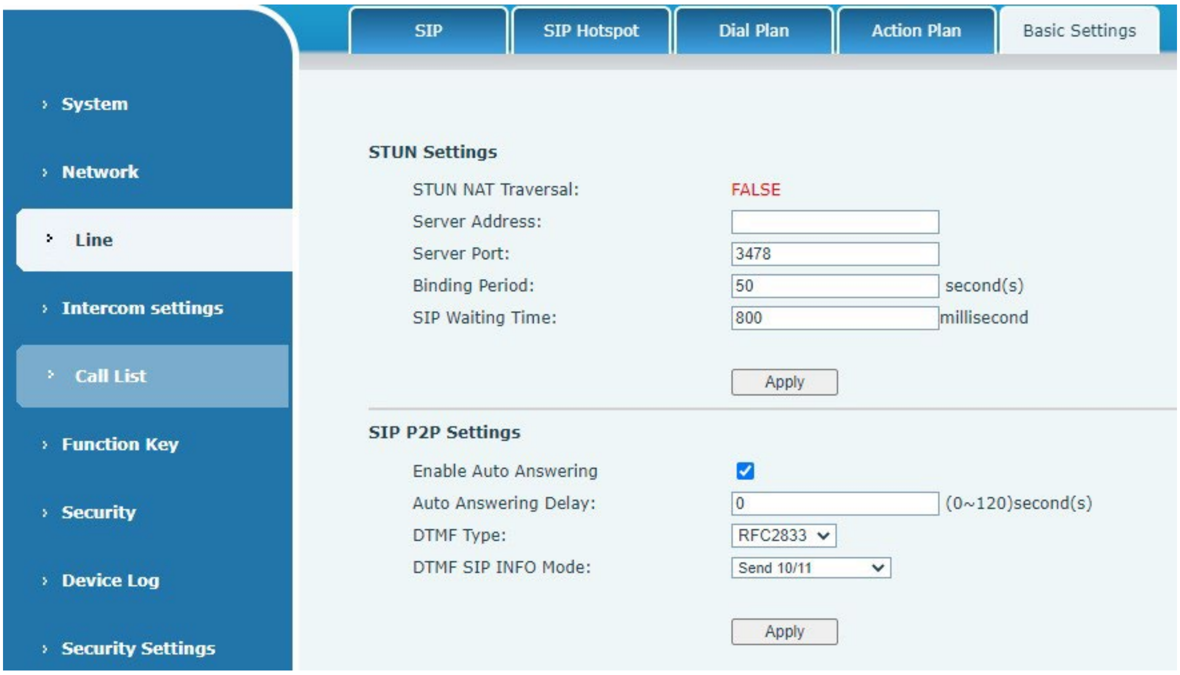
| Parameter | Description |
|---|---|
| Number | Auxiliary phone number (support video) |
| Type | Support video display on call. |
| Direction | For call mode, incoming/outgoing call displays video |
| Line | Set up outgoing lines. |
| Username | Bind the user name of the IP camera. |
| Password | Bind IP camera password. |
| URL | Video streaming information. |
| User Agent | Set user agent information |
| MCAST Codec | Set mcast codec |
| Action | Select action |

## 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 device 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.



Wants to receive data on Port 5060
Send request to STUN Server from Port 5060
NAT Mapping Port 12345
STUN Server tells customer public IP and Port 12345
Private Network
Public Network
What’ s my ip ?
Gateway
NAT
STUN Server



STUN Settings

STUN NAT Traversal: FALSE

Server Address:

Server Port: 3478

Binding Period: 50 second(s)

SIP Waiting Time: 800 millisecond

SIP P2P Settings

Enable Auto Answering ☑

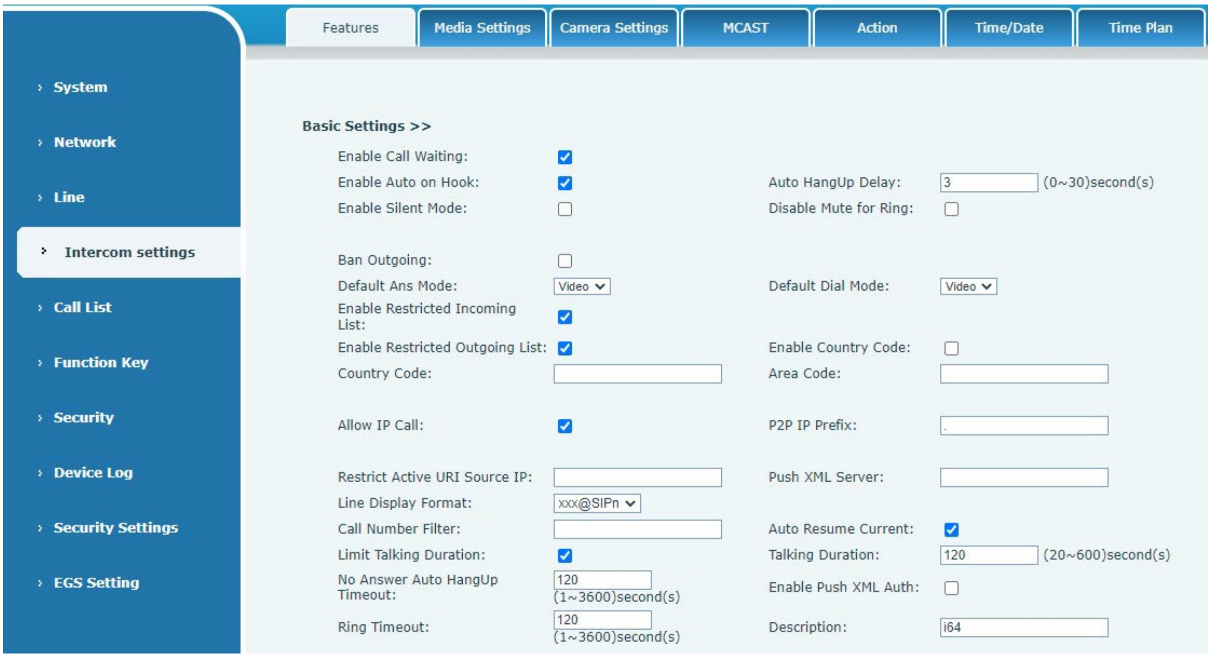
Auto Answering Delay: 0 (0~120)second(s)

DTMF Type: RFC2833

DTMF SIP INFO Mode: Send 10/11

| Parameters | Description |
|---|---|
| **STUN Settings** | |
| Server Address | Set the STUN server address |
| Server Port | Set the STUN server port, default is 3478 |
| Binding Period | Set the STUN binding period which can be used to keep the NAT pinhole opened. |
| SIP Waiting Time | Set the timeout of STUN binding before sending SIP messages |
| **SIP P2P Settings** | |
| Enable Auto Answering | Automatically answer incoming IP calls after the timeout period is enabled |
| Auto Answering Delay | Automatic answer timeout setting |
| DTMF Type | Set the DTMF type of the line. |
| DTMF SIP INFO mode | Set SIP INFO mode to send '*' and '#' or '10' and '11' |

## *Intercom settings >> Features*



Basic Settings >>

Enable Call Waiting: ☑

Enable Auto on Hook: ☑

Auto HangUp Delay: 3 (0~30)second(s)

Enable Silent Mode: □

Disable Mute for Ring: □

Ban Outgoing: □

Default Ans Mode: Video

Default Dial Mode: Video

Enable Restricted Incoming List: ☑

Enable Restricted Outgoing List: ☑

Enable Country Code: □

Country Code:

Area Code:

Allow IP Call: ☑

P2P IP Prefix: .

Restrict Active URI Source IP:

Push XML Server:

Line Display Format: xxx@SIPn

Call Number Filter:

Auto Resume Current: ☑

Limit Talking Duration: ☑

Talking Duration: 120 (20~600)second(s)

No Answer Auto HangUp Timeout: 120 (1~3600)second(s)

Enable Push XML Auth: □

Ring Timeout: 120 (1~3600)second(s)

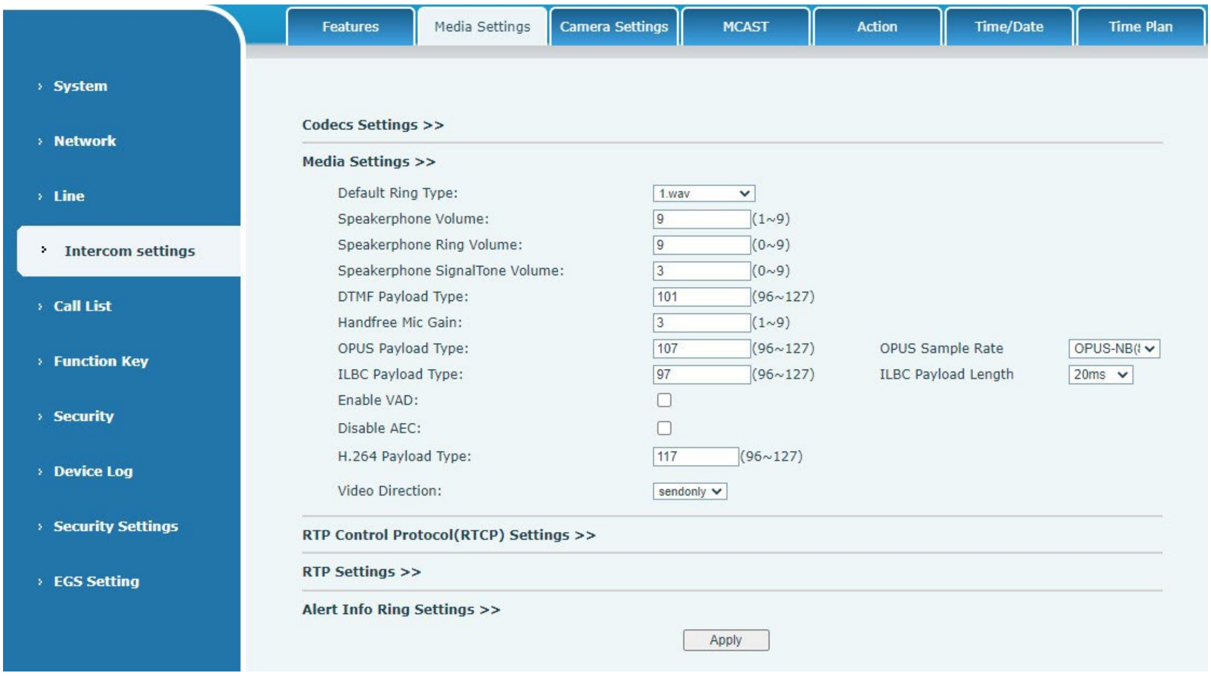
Description: i64

| **Parameters** | **Description** |
|---|---|
| **Basic Settings** | |
| Enable Call Waiting | Enable this setting to allow user to take second incoming call during an established call. Default enabled. |
| Enable Auto Handdown | The phone will hang up and return to an idle state automatically at hands-free mode |
| Auto Handdown Time | Specify Auto handdown time, the phone will hang up and return to an idle state automatically after Auto Hand down time at hands-free mode, and play dial tone Auto handdown time at handset mode |
| Enable Silent Mode | When enabled, the phone is muted, there is no ringing when calls, you can use the volume keys and mute key to unmute. |
| Disable Mute for Ring | When enabled, you cannot mute the phone. |
| Ban Outgoing | If you enable Ban Outgoing, you cannot dial out any number. |
| Default Reply Mode | Select the default mode after an incoming call, including Video and Audio |
| Default Dial Mode | Select the default mode after dialing, including Video and Audio |
| Enable Restricted Incoming List | Enable Restricted Incoming List |
| Enable Restricted Outgoing List | Enable Restricted Outgoing List |
| Enable country Code | Enable country Code |
| Country Code | Country Code |
| Area Code | Area Code |
| Allow IP Call | If enabled, user can dial out with IP address |
| P2P IP Prefix | You can set IP call prefix, for example, set P2P IP Prefix as “172.16.2.”,then input #160 using the dialpad and press dial key. It will call 172.16.2.160 automatically |

| | |
|---|---|
| Restrict Active URI Source IP | Set the device to accept Active URI command from a specific IP address. |
| Push XML Server | Configure Push XML Server. When phone receives a request, it will determine whether to display corresponding content on the phone. |
| Line Display Format | Line display format including SIPn/SIPn：xxx/xxx@SIPn |
| Call Number Filter | Configure a special character & , if the number is 78 & 9. The call will filter out & |
| Auto Resume Current | If the current path changes, the hold will automatically resume |
| Limit Talking Duration | Automatically hang up the call after enabling the time set for the call |
| Talking Duration | Call duration ,20-600s |
| No Answer Auto HangUp Timeout | If the call is not answered, the call will be automatically hung up after the timeout |
| Enable Push XML Auth | To enable push xml auth, user password is required |
| Ringing timeout | If the call is not answered, automatic hang-up after timeout |
| Show description information | Device description |
| **Tone Settings** | |
| Enable Holding Tone | When enabled, a tone plays when the call is held |
| Enable Call Waiting Tone | When enabled, a tone plays when call waiting |
| Play Dialing DTMF Tone | Play DTMF tone on the device when user presses a phone digit while dialing, default enabled. |
| Play Talking DTMF Tone | Play DTMF tone on the device when user presses a phone digits during taking, default enabled. |
| Auto-answer beep | When enabled, a beep will be heard when auto-answer is activated. |
| Tone of open door successfully | Closed: No prompt tone is played after the door is opened successfully<br>Default: Use the default prompt tone<br>Voice: built-in voice prompt by default, default is "door open successfully"<br>Support for custom door opening success prompt tone, which can be customized in system > upgrade > ringtone or after the door is opened and the ringtone file upgrades successfully |
| Tone of open door unsuccessfully | Closed: There is no prompt tone after the door fails to open<br>Default: Use the default prompt tone<br>Voice: voice prompt by default, default is "failed to open the door"<br>Supports custom door opening failure prompt tone, in the system > upgrade > ringtone, or after failing to open the door and the ringtone file upgrades unsuccessfully |
| Door closing beep | Close: no beep after closing the door.<br>Voice: default built-in voice prompt, default is "Close" Support custom door closing tone, in the system > upgrade > ringtones, after upgrading the ringtone file under the door closing available settings to use the custom tone |
| Successful card addition beep | Close: No beep after successful card addition.<br>Voice: default built-in voice prompt, default is "Card added successfully"<br>Support customizable beep for successful card addition in system > upgrade > ringtones, after upgrading the ringtone file available under successful card addition settings to use a custom tone. |

| | |
|---|---|
| Add card failure beep | Close: No beep after failed card addition.<br>Voice: default built-in voice prompt, default is "card refill failed".<br>Support customizable sound for card failure in system > upgrade > ringtones. After upgrading the ringtone file under the card failure, set to use a custom prompt |
| Successful beep for card deletion | Close: No beep after successful card deletion.<br>Voice: default voice prompt is "card deletion successful"<br>Support for customizing the successful card deletion tone. Go to System > Upgrade > Ringtone. After upgrading the ringtone file under the successful card deletion you can set to use the custom prompt. |
| Card deletion failure beep | Close: No beep after failed card deletion.<br>Voice: default voice prompt is "card deletion failed".<br>Support for customizing the card deletion failure tone in System > Upgrade > Ringtone. After upgrading the ringtone file under the card deletion failure, it can be set to use a custom prompt. |
| Magnetic door detection beep | Closed: No beep after door magnetic detection anomaly.<br>Voice: default voice prompt is "Please close the door".<br>Customized door detection tones are available under System > Upgrade > Ringtones. After upgrading the ringtone file the door detection can be set to use the customized prompt. |
| **Intercom Settings** | |
| Enable Intercom | When intercom is enabled, the device will accept the incoming call request with a SIP header of Alert-Info instruction to automatically answer the call after specific delay. |
| Enable Intercom Mute | Enable mute mode during the intercom call |
| Enable Intercom Tone | If the incoming call is intercom call, the phone plays the intercom tone |
| Enable Intercom Barge | Enable Intercom Barge by selecting it, the phone auto answers the intercom call during a call. If the current call is intercom call, the phone will reject the second intercom call |
| **Response Code Settings** | |
| Busy Response Code | Set the SIP response code on line busy |
| Reject Response Code | Set the SIP response code on call rejection |

## *Intercom settings >> Media*



Codecs Settings >>

Media Settings >>

Default Ring Type: 1.wav

Speakerphone Volume: 9 (1~9)

Speakerphone Ring Volume: 9 (0~9)

Speakerphone SignalTone Volume: 3 (0~9)

DTMF Payload Type: 101 (96~127)

Handfree Mic Gain: 3 (1~9)

OPUS Payload Type: 107 (96~127) OPUS Sample Rate OPUS-NB(

ILBC Payload Type: 97 (96~127) ILBC Payload Length 20ms

Enable VAD: ☐

Disable AEC: ☐

H.264 Payload Type: 117 (96~127)

Video Direction: sendonly

RTP Control Protocol(RTCP) Settings >>

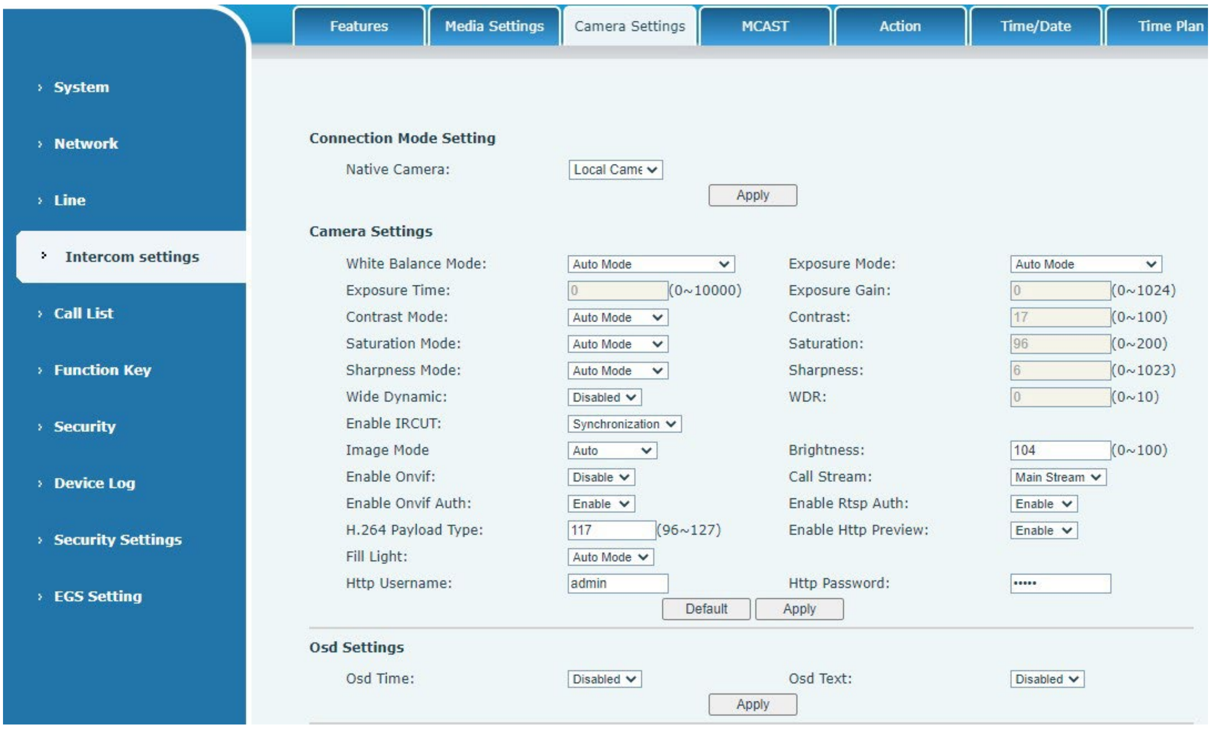
RTP Settings >>

Alert Info Ring Settings >>

| **Parameters** | **Description** |
|---|---|
| **Codecs Settings** | Select the enabled and disabled voice codecs<br>codec: G.711A/U,G.722,G.729,ILBC,opus |
| **Media Setting** | |
| Default Ring Type | Set the default ring type. If the caller ID of an incoming call was not configured with specific ring type, the default ring will be used. |
| Speakerphone Volume | Set the speakerphone volume, the value must be 1~9 |
| Speakerphone Ring Volume | Set the ring volume in the speakerphone, the value must be 1~9 |
| Speakerphone Ring Volume | Set the ring volume in the speakerphone, the value must be 1~9 |
| DTMF Payload Type | Enter the DTMF payload type, the value must be 96~127. |
| Opus payload type | Enter the opus payload type, the value must be 96~127. |
| OPUS Sample Rate | Set the opus sample rate including OPUS-NB（8KHz）,<br>OPUS-WB（16KHz） |
| ILBC Payload Type | Set the ILBC Payload Type |
| ILBC Payload Length | Set the ILBC Payload Length |
| Enable VAD | Enable Voice Activity Detection. When enabled, the device will suppress the audio transmission with artificial comfort noise signal to save the bandwidth. |
| H.264Payload Type | Set the H264 Payload Type. The value must be 96~127. |
| **RTP Control Protocol(RTCP) Settings** | |
| CNAME user | Set CNAME user |
| CNAME host | Set CNAME host |
| **RTP Settings** | |
| RTP keep alive | Hold the call and send the packet after 30s |
| **Alert Info Ring Settings** | |
| Value | Set the value to specify the ring type. |
| Ring Type | Type1-Type9 |

## *Intercom settings>>Camera Settings*

Configure camera related parameters and adjust video coding related settings.



Connection Mode Setting

Native Camera: Local Came

Camera Settings

White Balance Mode: Auto Mode
Exposure Mode: Auto Mode
Exposure Time: 0 (0~10000)
Exposure Gain: 0 (0~1024)
Contrast Mode: Auto Mode
Contrast: 17 (0~100)
Saturation Mode: Auto Mode
Saturation: 96 (0~200)
Sharpness Mode: Auto Mode
Sharpness: 6 (0~1023)
Wide Dynamic: Disabled
WDR: 0 (0~10)
Enable IRCUT: Synchronization
Image Mode: Auto
Brightness: 104 (0~100)
Enable Onvif: Disable
Call Stream: Main Stream
Enable Onvif Auth: Enable
Enable Rtsp Auth: Enable
H.264 Payload Type: 117 (96~127)
Enable Http Preview: Enable
Fill Light: Auto Mode
Http Username: admin
Http Password: •••••

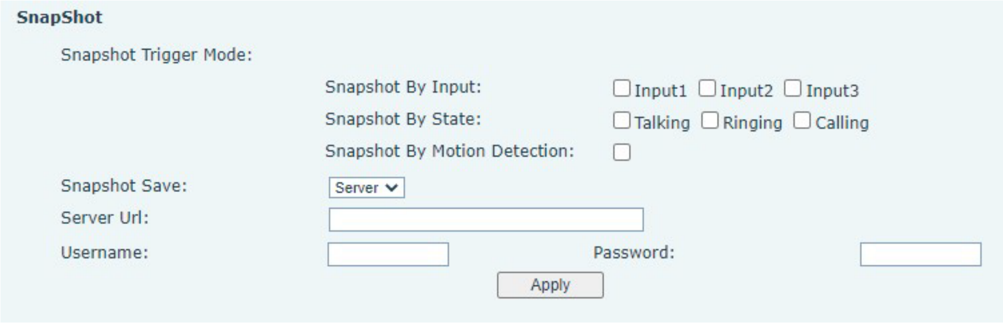
Osd Settings

Osd Time: Disabled
Osd Text: Disabled

| Parameters | Description |
|---|---|
| **Connection Mode Setting** | |
| Native Camera | **Local:** Automatically use the local camera to transmit images.<br>**External:** After setting the external camera, it will automatically use the external camera to transmit images |
| **Camera settings** | |
| White Balance Mode | **Auto mode**：The camera automatically makes the most appropriate adjustments according to the color temperature of the shooting scene, and automatically compensates for the color of the light source.<br>**Lock mode**：Fixed white balance parameters will not be automatically adjusted according to the actual color temperature.<br>**Incandescent lamp mode：**To compensate for the hue of incandescent lamps, it is suitable for use under beige light sources (bulbs, tungsten lamps, candles) and other light sources of this type.<br>**Warm light mode**：Compensate the hue of warm light, suitable for light sources with a color temperature of about 2700K Natural light mode：It can be used for white balance in outdoor shooting and has a wide range of applications.<br>**Fluorescent lamp light**：Compensate the hue of fluorescent lamps, suitable for use under fluorescent light sources (fluorescent lamps, energy-saving lamps) and other types of light sources |
| Exposure Mode | **Auto mode：** The camera automatically sets the parameters, no need for the operator to adjust.<br>**Manual exposure time：** Set the exposure time by yourself, the range is 0~10000.<br>**Manual exposure gain**：Set the exposure gain by yourself, the range is 0~1024.<br>All manual： Manually set the exposure time and gain. |

| | |
|---|---|
| Exposure Time | It refers to the time to press the shutter. Increasing the exposure time can increase the signal-to-noise ratio and make the image clear. The longer the time, the more the sum of photons to the CCD\CMOS surface, the brighter the captured image will be, but if it is overexposed, the photo will be too bright and lose the image details; if it is underexposed, the photo will be too dark. |
| Exposure Gain | It refers to the amplification gain of the analog signal after double sampling, but the noise signal is also amplified in the process of amplifying the image signal. The gain is generally only used when the signal is weak, but you do not want to increase the exposure time. |
| Contrast Mode | **Auto mode**：The camera automatically sets the contrast according to the environment, no need for the operator to adjust.<br>**Manual mode**：Manually set the camera's contrast parameters. |
| Contrast | Contrast refers to the contrast between light and dark in the picture. Increase the contrast, the brighter areas will be brighter and the darker areas will be darker, and the contrast between light and dark will increase. |
| Saturation Mode | **Auto mode**：The camera automatically sets the saturation according to the environment, without the need for the operator to adjust.<br>**Manual mode**：Manually set the camera's saturation parameters. |
| Saturation | Saturation refers to the color. Adjusting the saturation will change the color. The greater the adjustment, the more distorted the image color. Adjusting the saturation is only suitable for pictures with insufficient colors. When the saturation is adjusted to the lowest, the image will lose its color and become a black and white image. |
| Sharpness Mode | **Auto mode**：The camera automatically sets the sharpness according to the environment, no need for the operator to adjust.<br>**Manual mode**：Manually set the sharpness parameters of the camera. |
| Sharpness | Sharpness is an indicator that reflects the sharpness of the image plane and the sharpness of the edges of the image. If you increase the sharpness, the contrast of the details on the image plane is also higher and it looks clearer. |
| Wide dynamic | Enable or disable wide dynamic. Turning on wide dynamic allows the camera to see the image in a very strong contrast |
| Wide dynamic range | Set image brightness by yourself, range 0~10. |
| Enable IRCUT | Enable/Disable IRCUT |
| Image mode | **Daytime** (color): The camera transmits color images when there is sufficient light during the day.<br>**Night** (black and white): The camera transmits black and white images when there is insufficient light at night.<br>**Automatic**: The camera transmits color images when the light is sufficient during the day according to the light sensitivity, and transmits black and white images when the light is insufficient at night |
| Brightness | Set the image brightness by yourself, the range is 0~100 |
| Enable Onvif | Enable or disable the onvif protocol, after enabling it, the device can be discovered through a recorder that supports ONVIF |
| Call Stream | Main stream or sub stream used in video call |
| Enable Onvif Auth | Authentication is required when using onvif protocol (with username and password) |

| | |
|---|---|
| Enable Rtsp Auth | When using rtsp protocol, whether authentication is required (with username and password) |
| H.264 Payload Type | Set the load type of h.264, the range is 96~127 |
| **Osd Settings** | |
| Osd Time | Turn on/off the date display of the camera image interface. |
| Osd Text | Enable/disable the text display of the camera image interface. |
| **Video Codecs** | |
| H264 Video Stream | Support H.264 encoding format |
| Bitrate Control | **VBR**：Video call will adapt to the bit rate of the opposite end, so that the video effect is better.<br>**CBR**：The video call will not change according to the bit rate set by it. |
| Resolution | Support 1080P，720P，4CIF,VGA,CIF,QVGA |
| Frame Rate (fps) | The larger the value is, the more fluent the video is, and the higher the requirement for network bandwidth is; adjustment is not recommended |
| BitRate | It refers to the data flow used by video files in unit time, also known as code rate or code flow rate. Generally speaking, sampling rate is the most important part of picture quality control in video coding. Generally, the unit we use is KB/s or MB/s |
| I Frame Interval | The larger the value, the worse the video quality, otherwise the better the video quality; adjustment is not recommended. |
| **RTSP Information** | |
| Main Stream Url | Display the main stream URL address |
| Sub Stream Url | Display the sub stream URL address |
| **Snapshot** | |
| Input trigger | Select the input port that triggers the capture |
| Call trigger | Select the call status that triggers the capture |
| Movement detection trigger | Whether to enable monitoring capture |
| Saving Method of Capture | Set how to save the captured image, including: server, Storage Card, Server and Storage Card |
| Server address | Enter the server address |
| Username | Enter a username |
| Password | Enter a password |



SnapShot

Snapshot Trigger Mode:

Snapshot By Input: □ Input1 □ Input2 □ Input3

Snapshot By State: □ Talking □ Ringing □ Calling

Snapshot By Motion Detection: □

Snapshot Save: Server

Server Url:

Username: Password:

Snapshot trigger mode:

- Snapshot By Input. Select the input port to trigger the snapshot
- Snapshot By State. The snapshot is triggered when Talking, Ringing or Calling.
- Snapshot By Motion Detection. A capture is triggered when the camera detects abnormal action

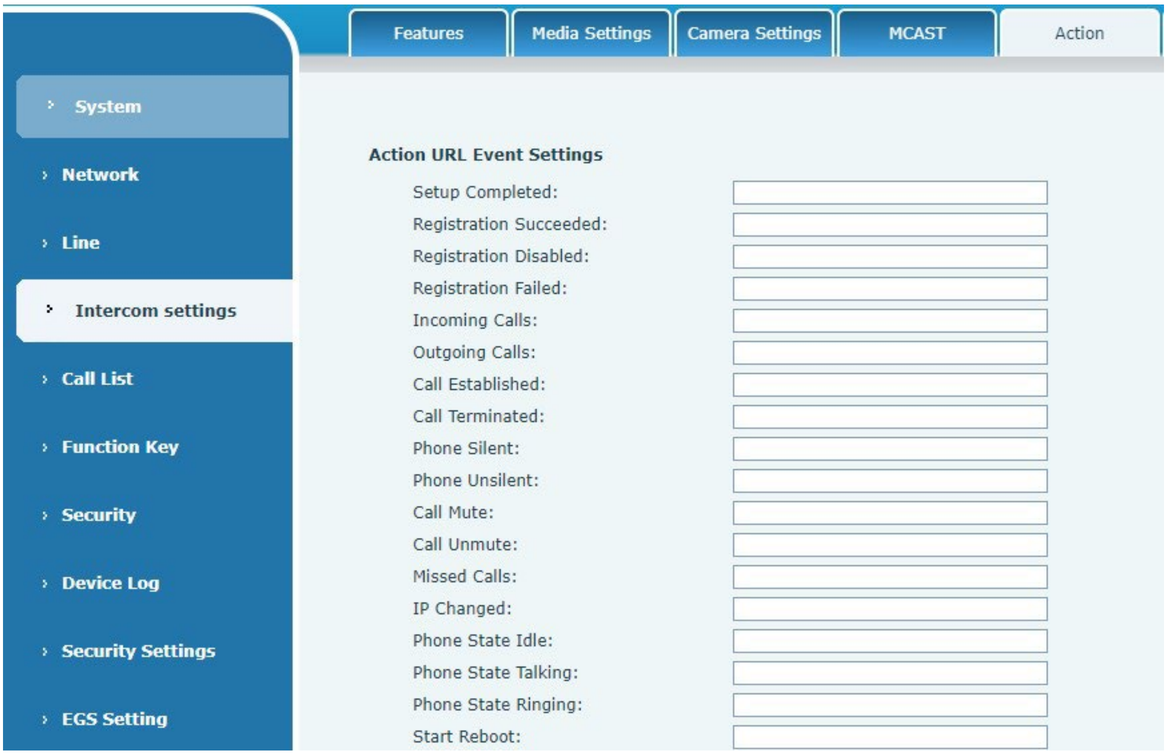
- Snapshot Save. Save the screenshot to the server or SD card.
- Server Url. Server address (Upload through FTP, TFTP, HTTP, or HTTPS).

## *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.

## *Intercom Setting >> Action URL*

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

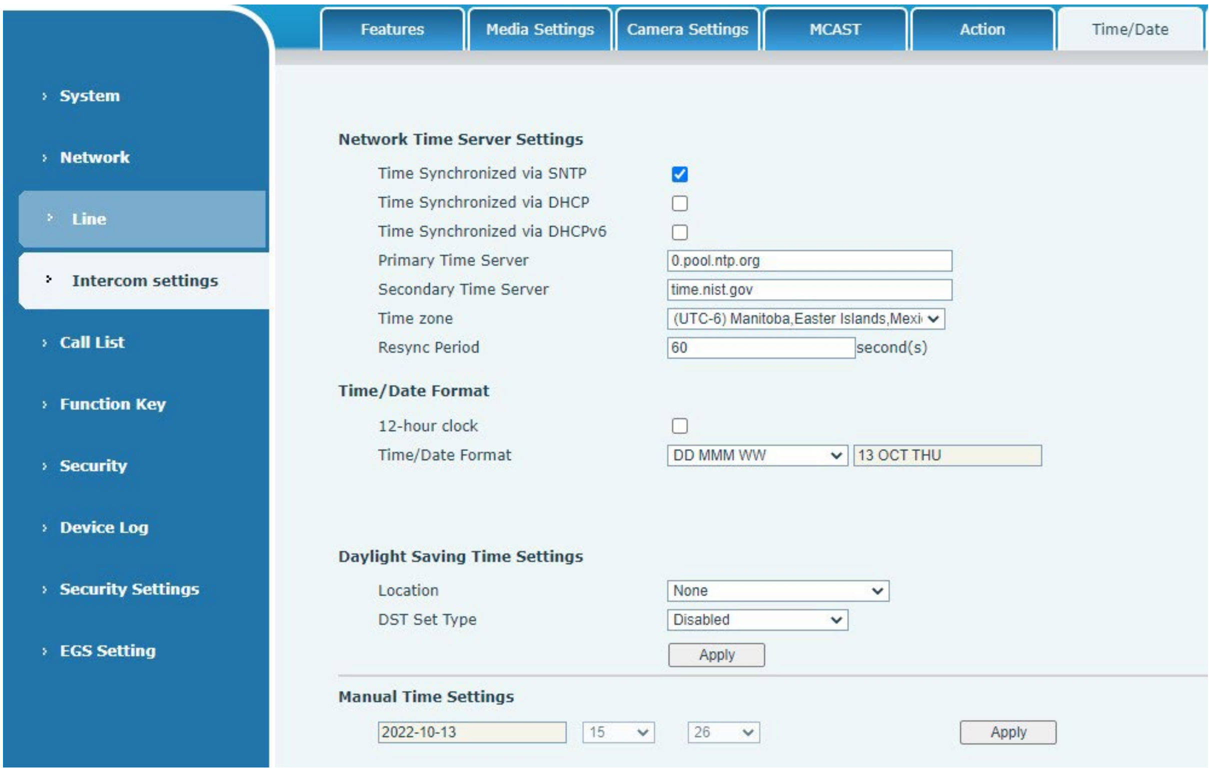


**Action URL Event Settings**

Setup Completed:
Registration Succeeded:
Registration Disabled:
Registration Failed:
Incoming Calls:
Outgoing Calls:
Call Established:
Call Terminated:
Phone Silent:
Phone Unsilent:
Call Mute:
Call Unmute:
Missed Calls:
IP Changed:
Phone State Idle:
Phone State Talking:
Phone State Ringing:
Start Reboot:

## *Intercom Setting >> Time/Date*

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



Network Time Server Settings

Time Synchronized via SNTP ☑

Time Synchronized via DHCP □

Time Synchronized via DHCPv6 □

Primary Time Server 0.pool.ntp.org

Secondary Time Server time.nist.gov

Time zone (UTC-6) Manitoba,Easter Islands,Mexi

Resync Period 60 second(s)

Time/Date Format

12-hour clock □

Time/Date Format DD MMM WW 13 OCT THU

Daylight Saving Time Settings

Location None

DST Set Type Disabled

Apply

Manual Time Settings

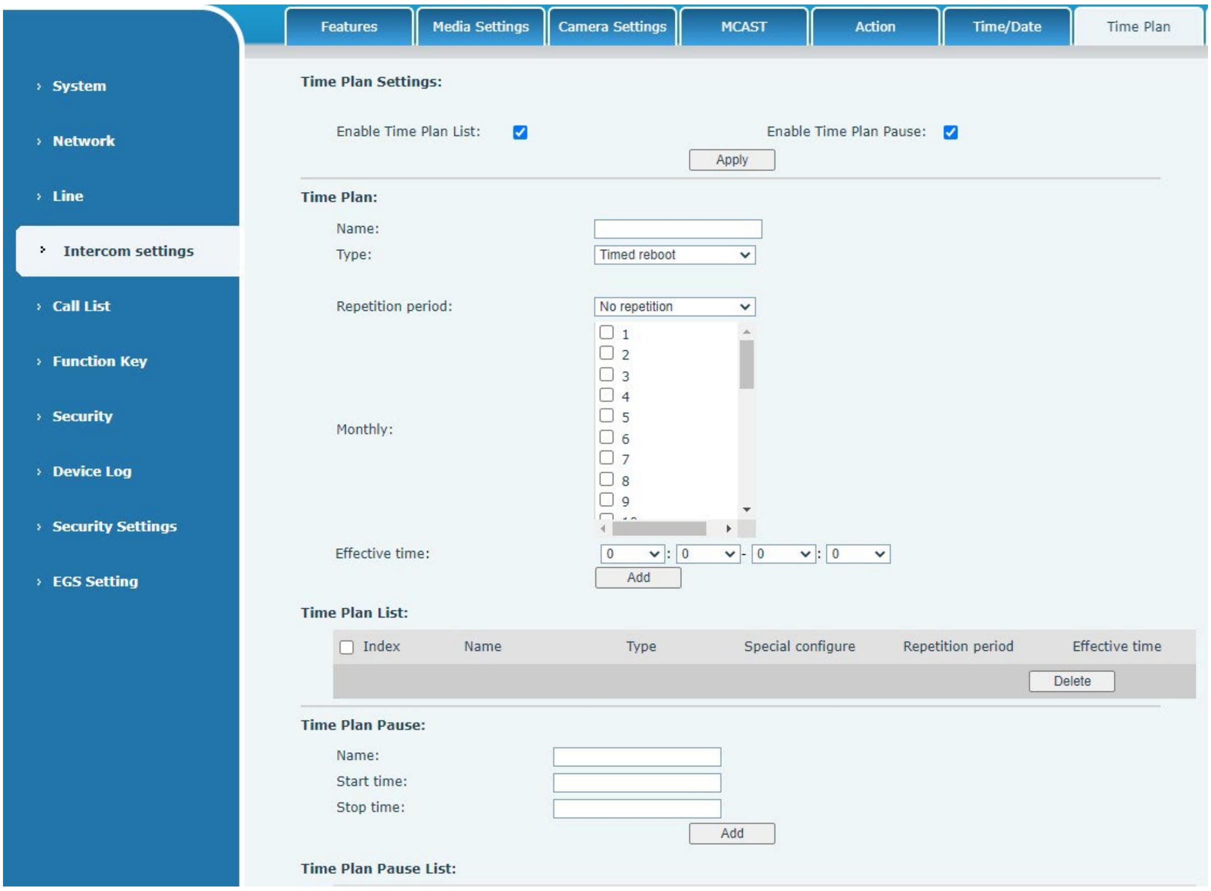
2022-10-13 15 26 Apply

| 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. | |

## *Intercom settings>>Time plan*

The user can set the time point and time period for the device to perform a certain action.



**Time Plan Settings:**

Enable Time Plan List: ☑ Enable Time Plan Pause: ☑

**Time Plan:**

Name:

Type: Timed reboot

Repetition period: No repetition

Monthly: □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9

Effective time: 0 : 0 - 0 : 0

**Time Plan List:**

| □ Index | Name | Type | Special configure | Repetition period | Effective time |
|---|---|---|---|---|---|

**Time Plan Pause:**

Name:

Start time:

Stop time:

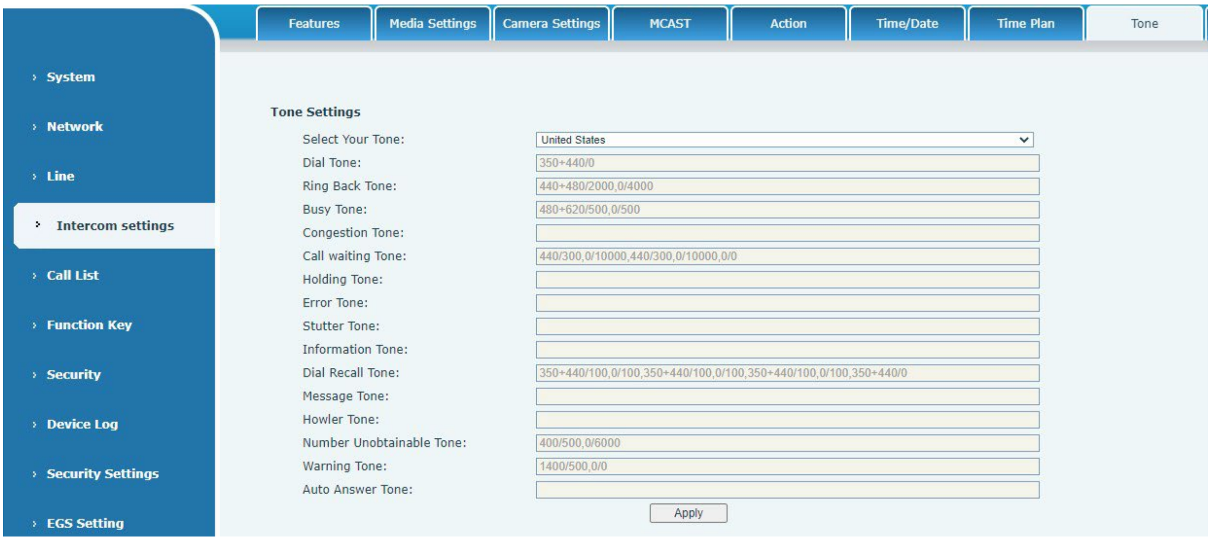
**Time Plan Pause List:**

| Parameters | Description |
|---|---|
| Name | Enter a defined action name |
| type | Timing restart, timing upgrade, timing sound detection, timing playback audio |
| Audio path | Support local<br>Local: select the audio file uploaded locally |
| Audio settings | Select the audio file you want to play, it supports trial listening, and you can play it immediately after clicking the trial listening |
| Repeat cycle | **Do not repeat**: execute once within the set time range.<br>**Daily**: Perform this operation in the same time frame every day.<br>**Weekly**: Do this in the time frame of the day of the week Monthly: the time frame of the month to perform this operation |
| Effective time | Set the time period for execution |

## *Intercom settings >> Tone*

The user can configure the prompt tone of the device on this page.

You can select the country area or customize the area. The selected area can directly appear the default information, and the customized one can modify the key tone, callback tone and other information.

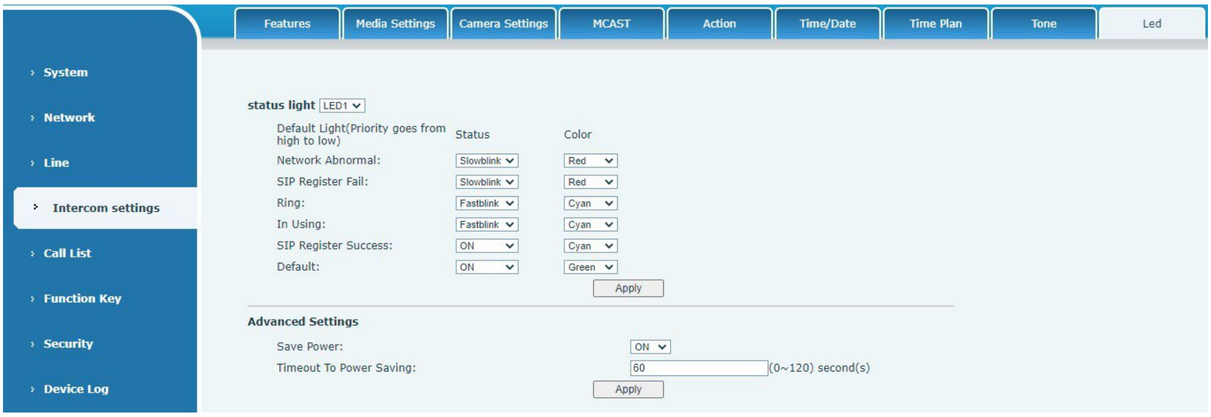


Tone Settings

| | |
|---|---|
| Select Your Tone: | United States |
| Dial Tone: | 350+440/0 |
| Ring Back Tone: | 440+480/2000,0/4000 |
| Busy Tone: | 480+620/500,0/500 |
| Congestion Tone: | |
| Call waiting Tone: | 440/300,0/10000,440/300,0/10000,0/0 |
| Holding Tone: | |
| Error Tone: | |
| Stutter Tone: | |
| Information Tone: | |
| Dial Recall Tone: | 350+440/100,0/100,350+440/100,0/100,350+440/100,0/100,350+440/0 |
| Message Tone: | |
| Howler Tone: | |
| Number Unobtainable Tone: | 400/500,0/6000 |
| Warning Tone: | 1400/500,0/0 |
| Auto Answer Tone: | |

## *Intercom settings >> Led*

The user can configure the status and color of the indicator light on this page.



status light LED1

| Default Light(Priority goes from high to low) | Status | Color |
|---|---|---|
| Network Abnormal: | Slowblink | Red |
| SIP Register Fail: | Slowblink | Red |
| Ring: | Fastblink | Cyan |
| In Using: | Fastblink | Cyan |
| SIP Register Success: | ON | Cyan |
| Default: | ON | Green |

Advanced Settings

| | |
|---|---|
| Save Power: | ON |
| Timeout To Power Saving: | 60 (0~120) second(s) |

**Status indicator:** The user can customize how the LED displays when the device is in different status.
**Energy-saving mode:** The device automatically turns off the LED when the device is not in use. The user can turn on or off the energy-saving mode.
**Energy-saving mode timeout:** The user can set the timeout of the energy-saving mode after inactivity. The default timeout is 60 seconds.

## Call list >> Call List

- Restricted Incoming Calls

It is the same as blacklist. By adding a number into the blacklist, user will no longer receive phone call from that number and it will be rejected automatically by the device until user delete it from the blacklist.

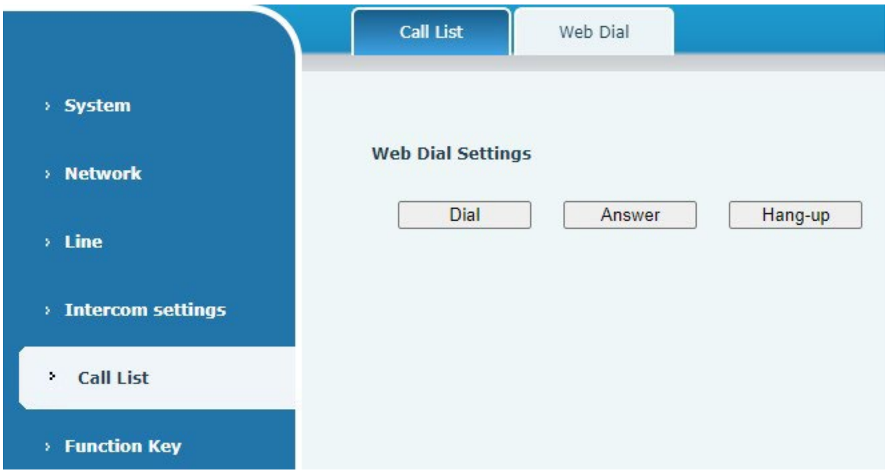
User can add specific number to be blocked, or a prefix where any numbers matched the prefix will all be blocked.

- Restrict Outgoing Call

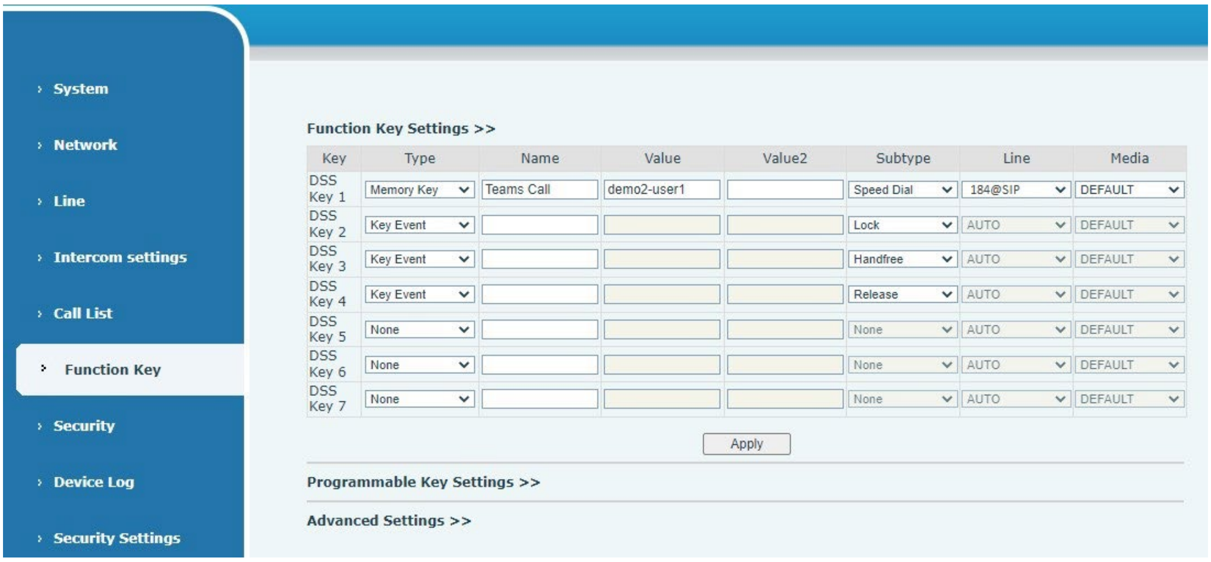
You can set the rule to restrict some numbers from dialing out, until you remove the number from the table.

## Call list >> Web Dial

Use phone web page to call, answer and hang up.



## Function key

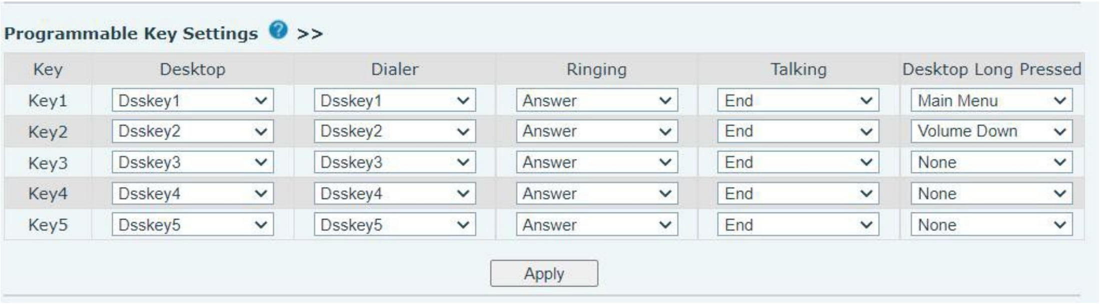


Function Key Settings >>

| Key | Type | Name | Value | Value2 | Subtype | Line | Media |
|---|---|---|---|---|---|---|---|
| DSS Key 1 | Memory Key | Teams Call | demo2-user1 | | Speed Dial | 184@SIP | DEFAULT |
| DSS Key 2 | Key Event | | | | Lock | AUTO | DEFAULT |
| DSS Key 3 | Key Event | | | | Handfree | AUTO | DEFAULT |
| DSS Key 4 | Key Event | | | | Release | AUTO | DEFAULT |
| DSS Key 5 | None | | | | None | AUTO | DEFAULT |
| DSS Key 6 | None | | | | None | AUTO | DEFAULT |
| DSS Key 7 | None | | | | None | AUTO | DEFAULT |

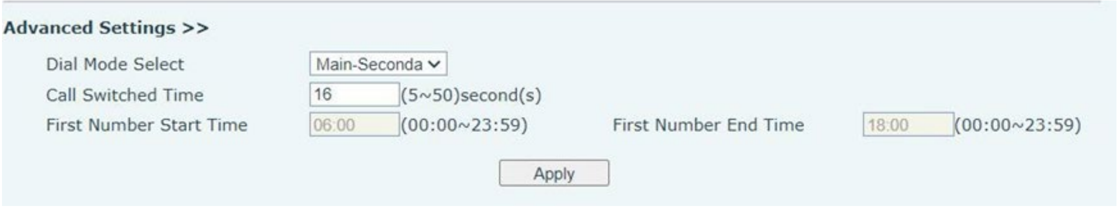
Programmable Key Settings >>

Advanced Settings >>



Programmable Key Settings >>

| Key | Desktop | Dialer | Ringing | Talking | Desktop Long Pressed |
|---|---|---|---|---|---|
| Key1 | Dsskey1 | Dsskey1 | Answer | End | Main Menu |
| Key2 | Dsskey2 | Dsskey2 | Answer | End | Volume Down |
| Key3 | Dsskey3 | Dsskey3 | Answer | End | None |
| Key4 | Dsskey4 | Dsskey4 | Answer | End | None |
| Key5 | Dsskey5 | Dsskey5 | Answer | End | None |



Advanced Settings >>

Dial Mode Select: Main-Seconda

Call Switched Time: 16 (5~50)second(s)

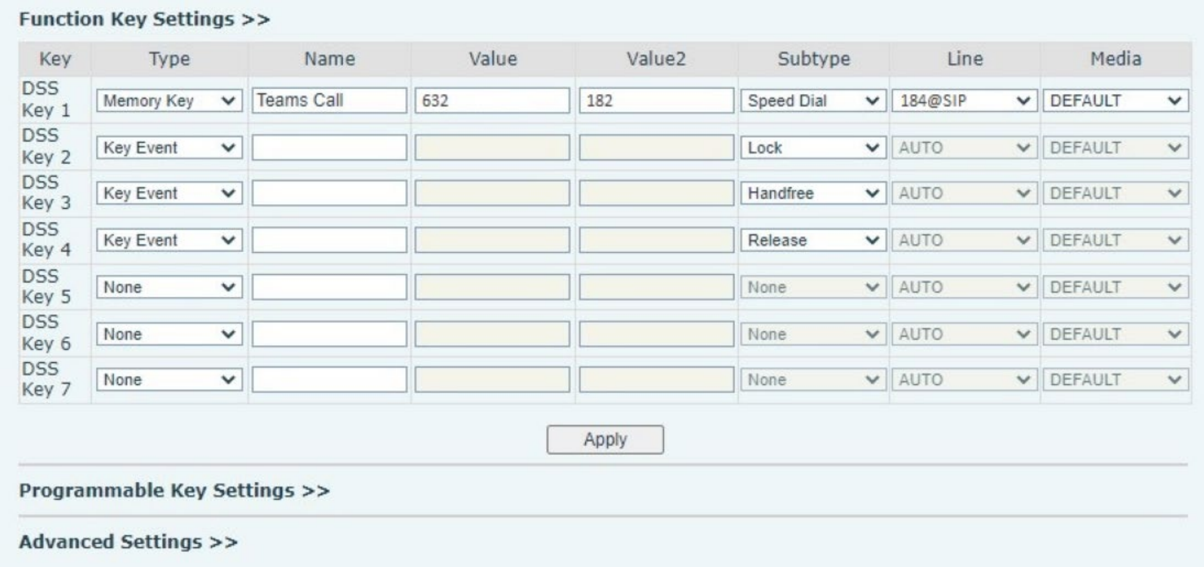
First Number Start Time: 06:00 (00:00~23:59)  First Number End Time: 18:00 (00:00~23:59)

| Parameters | Description |
|---|---|
| **Function key settings** | |
| memory | **Speed Dial**: The user can directly dial the set number. This feature is convenient for customers to dial frequent numbers.<br>**Intercom:** This feature allows the operator or secretary to quickly connect to the phone, widely used in office environments |
| Key event | The user can select a function key as the shortcut to trigger an event<br>Handfree：One-click to open the hands-free<br>Audio play：play music stored locally<br>OK：Confirm key<br>Volume Up：Increase the volume<br>Volume Down：Decrease the volume<br>Redial: redial out the last number dialed<br>Release: Hang up the call<br>Call Back: dial back the last call |
| DTMF | Press during a call to send the set DTMF |
| Mcast Paging | Configure the multicast address and voice encoding. User can initiate multicast by pressing this key |
| Action URL | The user can use a specific URL to make basic calls to the device, open the door, etc. |
| Mcast Listening | In standby, press the function key, if the RTP of the multicast is detected, the device will monitor the multicast |
| PTT | Speed dial：Press to make a call.<br>Intercom：Press to start an intercom call.<br>Multicast：Press to initiate a multicast. |
| Programmable Key Settings | |
| Desktop | None：Nothing happens when you press the speed dial Dsskey1：When it is set to dsskey1, follow the settings of dsskey1 to make call, answer, etc.<br>Dsskey2 ： When it is set to dsskey2, perform operations such as calling and answering according to the setting of dsskey2 |

| | |
|---|---|
| Dialer | None：Nothing happens when you press the speed dial Dsskey1：When it is set to dsskey1, follow the settings of dsskey1 to make call, answer, etc.<br>Dsskey2 ： When it is set to dsskey2, perform operations such as calling and answering according to the setting of dsskey2 |
| Ringing | Answer：Set to answer, when there is an incoming call, if auto answer is disabled, press the speed dial key to answer the call.<br>End: set to end, when there is an incoming call, press the speed dial button to hang up the call. |
| Talking | End: set to end, when there is a call, press the speed dial key to hang up the call.<br>Volume up: set as volume up button. When there is a call, press the speed dial button to increase the volume.<br>Volume down: set as volume up button. When there is a call, press the speed dial button to decrease the volume.<br>Dsskey1：When it is set to dsskey1, follow the settings of dsskey1 to make call, answer, etc.<br>Dsskey2 ： When it is set to dsskey2, perform operations such as calling and answering according to the setting of dsskey2 |
| Desktop Long Pressed | None: Long press the speed dial key. It does not respond.<br>Main menu: Long press the speed dial key to enter the command line mode. |
| Advanced Settings | |
| Hot Key Dial Mode Select | Number 1 call number 2 mode selection.<br><Main/Secondary>: If the first number is not answered within the set time, the second number will be automatically switched.<br><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 |

## Memory

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



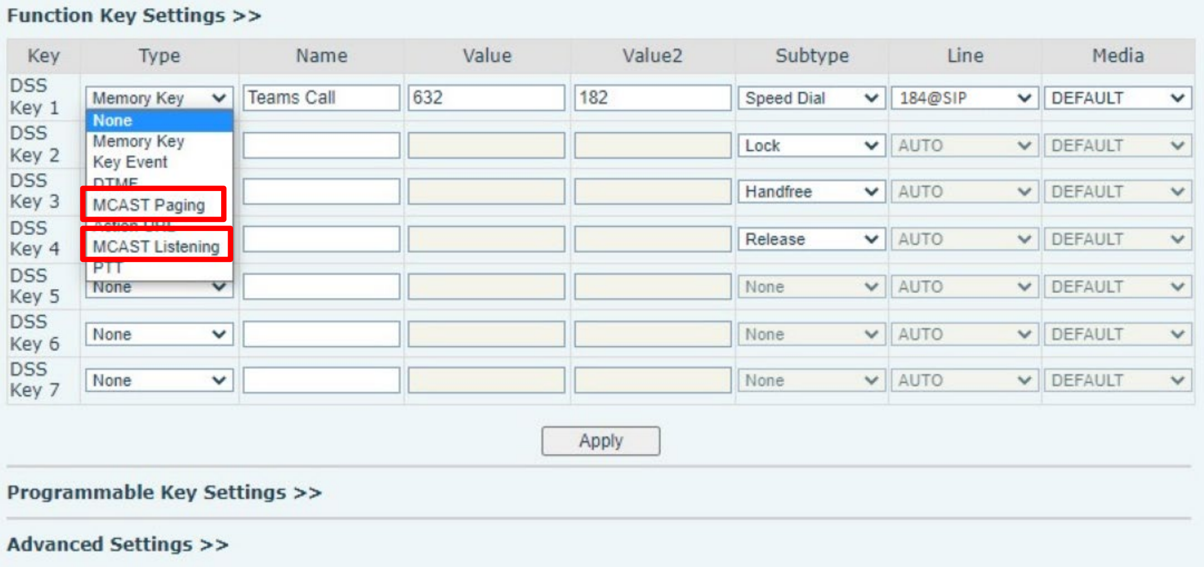
Function Key Settings >>

| Key | Type | Name | Value | Value2 | Subtype | Line | Media |
|---|---|---|---|---|---|---|---|
| DSS Key 1 | Memory Key | Teams Call | 632 | 182 | Speed Dial | 184@SIP | DEFAULT |
| DSS Key 2 | Key Event | | | | Lock | AUTO | DEFAULT |
| DSS Key 3 | Key Event | | | | Handfree | AUTO | DEFAULT |
| DSS Key 4 | Key Event | | | | Release | AUTO | DEFAULT |
| DSS Key 5 | None | | | | None | AUTO | DEFAULT |
| DSS Key 6 | None | | | | None | AUTO | DEFAULT |
| DSS Key 7 | None | | | | None | AUTO | DEFAULT |

| Type | Value | Line | Subtype | Usage |
|---|---|---|---|---|
| Memory | Fill in the SIP account or IP address of the called party | The line corresponding to the SIP account | Speed Dial | Using the speed dial mode, press the button to quickly dial the set number. |
| | | | Intercom | Using the intercom mode, when the SIP phone at the opposite end supports the intercom function, the call can be automatically answered. |

### Multicast

Multicast function delivers voice stream to configured multicast address. All equipment monitoring the multicast address can receive and play the broadcasting. Using multicast functionality would deliver voice one to multiple devices, which are in the multicast group.
The DSS Key multicast web configuration for calling party is as follows:



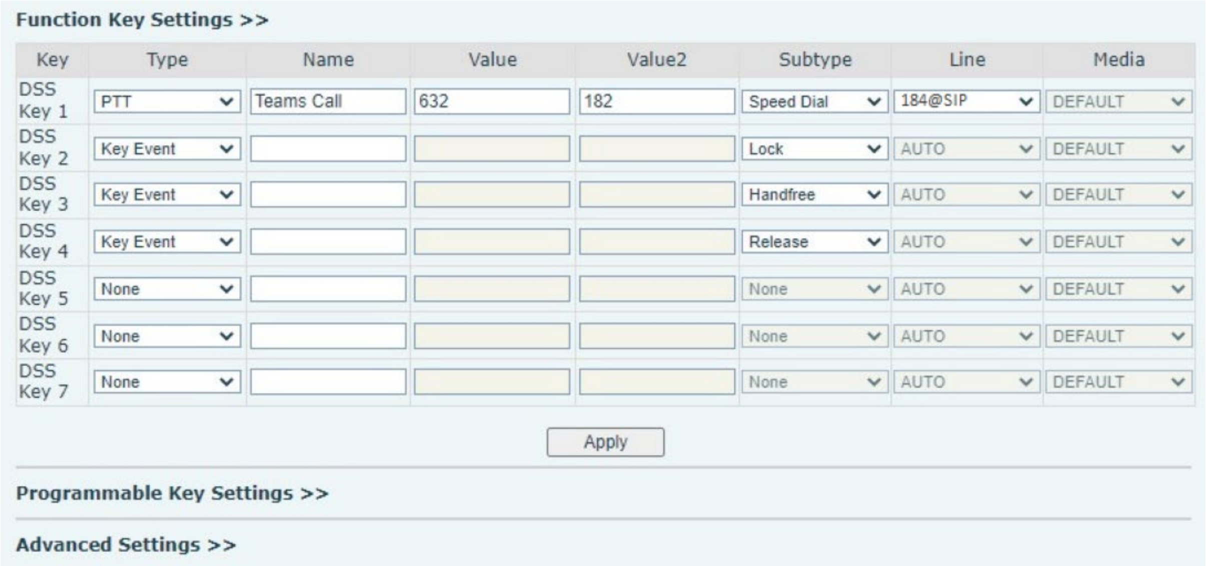
Function Key Settings >>

| Key | Type | Name | Value | Value2 | Subtype | Line | Media |
|---|---|---|---|---|---|---|---|
| DSS Key 1 | Memory Key | Teams Call | 632 | 182 | Speed Dial | 184@SIP | DEFAULT |
| DSS Key 2 | | | | | Lock | AUTO | DEFAULT |
| DSS Key 3 | | | | | Handfree | AUTO | DEFAULT |
| DSS Key 4 | | | | | Release | AUTO | DEFAULT |
| DSS Key 5 | None | | | | None | AUTO | DEFAULT |
| DSS Key 6 | None | | | | None | AUTO | DEFAULT |
| DSS Key 7 | None | | | | None | AUTO | DEFAULT |

| Type | Number | Subtype |
|---|---|---|
| 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 |
| | | G.711U |
| | | G.729AB |
| | | iLBC |
| | | opus |
| | | G.722 |

### PTT

Press and hold the shortcut key to make a call, release it and hang up.

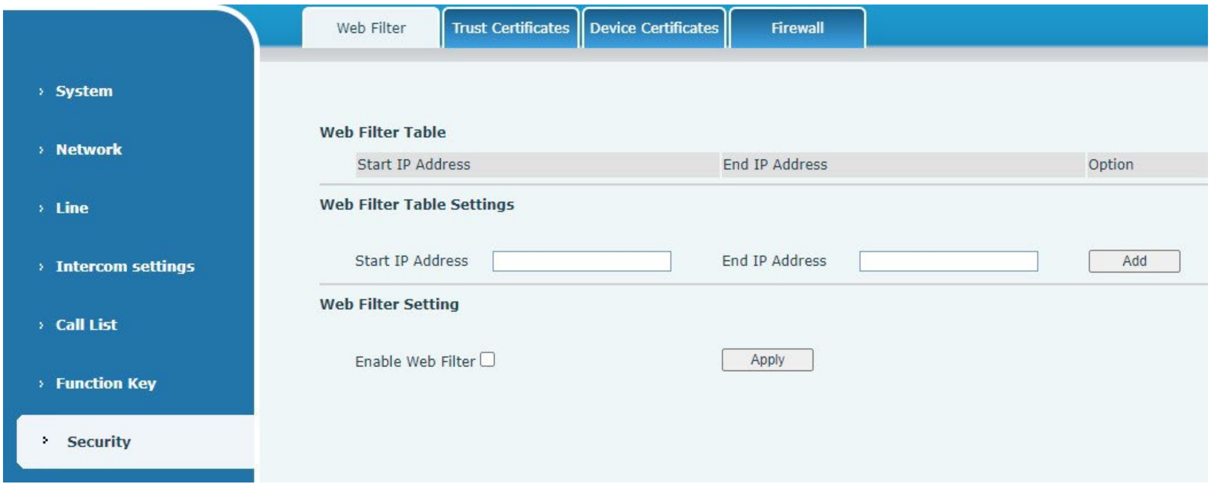


Function Key Settings >>

| Key | Type | Name | Value | Value2 | Subtype | Line | Media |
|---|---|---|---|---|---|---|---|
| DSS Key 1 | PTT | Teams Call | 632 | 182 | Speed Dial | 184@SIP | DEFAULT |
| DSS Key 2 | Key Event | | | | Lock | AUTO | DEFAULT |
| DSS Key 3 | Key Event | | | | Handfree | AUTO | DEFAULT |
| DSS Key 4 | Key Event | | | | Release | AUTO | DEFAULT |
| DSS Key 5 | None | | | | None | AUTO | DEFAULT |
| DSS Key 6 | None | | | | None | AUTO | DEFAULT |
| DSS Key 7 | None | | | | None | AUTO | DEFAULT |

## *Security >> Web filter*

Users can set up to allow only a certain network segment IP to access the device.



Web Filter Table

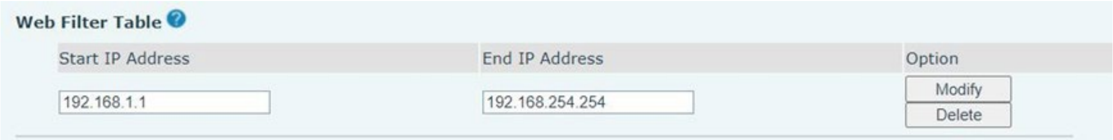
| Start IP Address | End IP Address | Option |
|---|---|---|

Web Filter Table Settings

Start IP Address End IP Address Add

Web Filter Setting

Enable Web Filter ☐ Apply



Web Filter Table

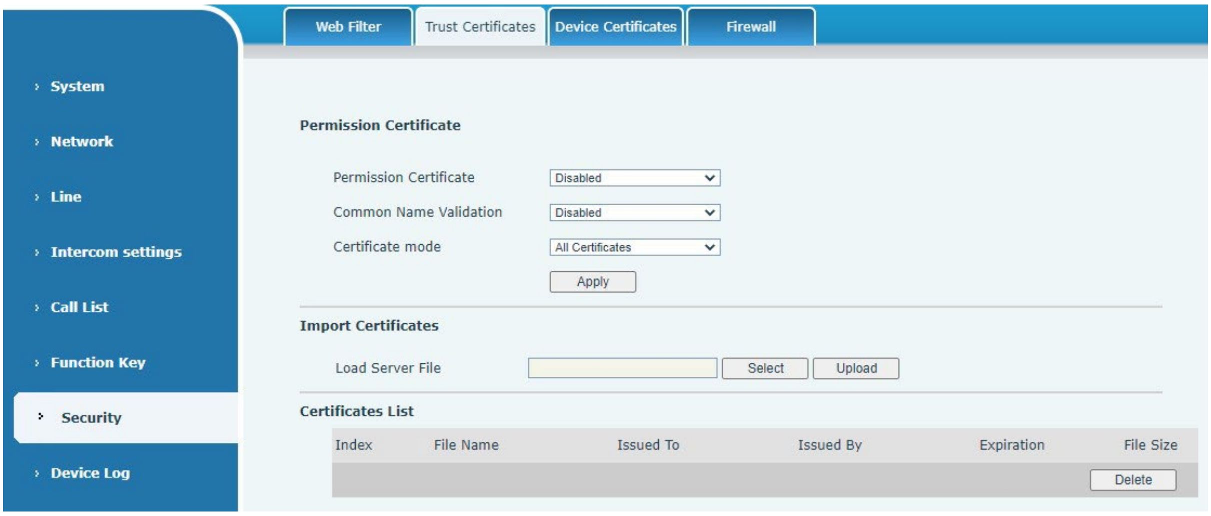
| Start IP Address | End IP Address | Option |
|---|---|---|
| 192.168.1.1 | 192.168.254.254 | Modify<br>Delete |

Add and delete the allowed IP network segments; configure the start IP address in the start IP, configure the end IP address in the end IP, and then click [Add] to add successfully. You can set a large network segment or add it into several network segments. When deleting, select the starting IP of the network segment to be deleted in the list, and then click [Delete] to take effect.
Enable web filtering: configure to enable/disable web access filtering; click the [Submit] button to take effect.

Note: If the device you access is on the same network segment, do not configure the web filtering network segment to be outside your own network segment, otherwise you will not be able to log in to the web page.

## *Security >> Trust Certificates*

Upload and delete uploaded trust certificates.



Permission Certificate

Permission Certificate: Disabled
Common Name Validation: Disabled
Certificate mode: All Certificates
Apply

Import Certificates

Load Server File: Select Upload

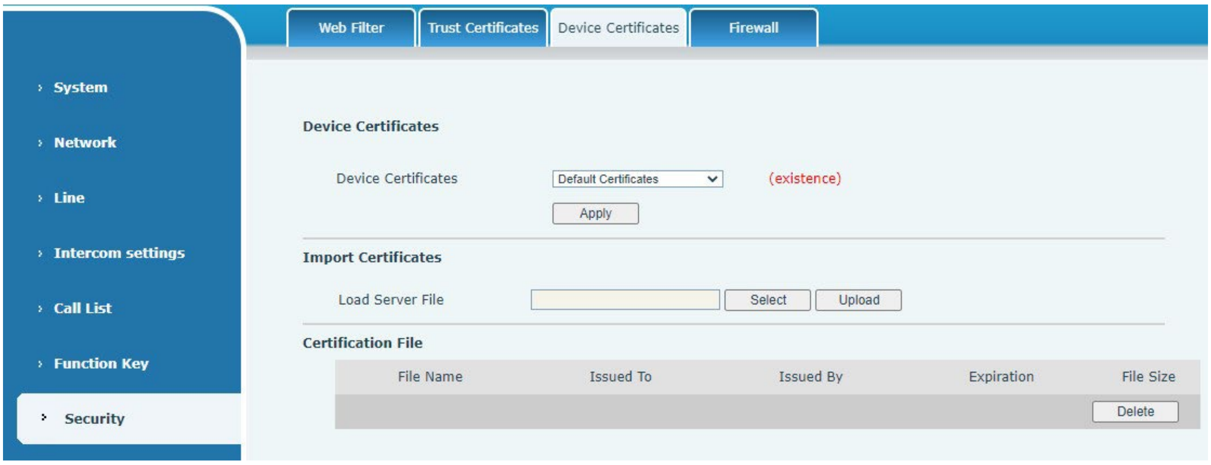
Certificates List

| Index | File Name | Issued To | Issued By | Expiration | File Size |
|---|---|---|---|---|---|

Delete

## *Security >> Device Certificates*

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



Device Certificates

Device Certificates: Default Certificates (existence)
Apply

Import Certificates

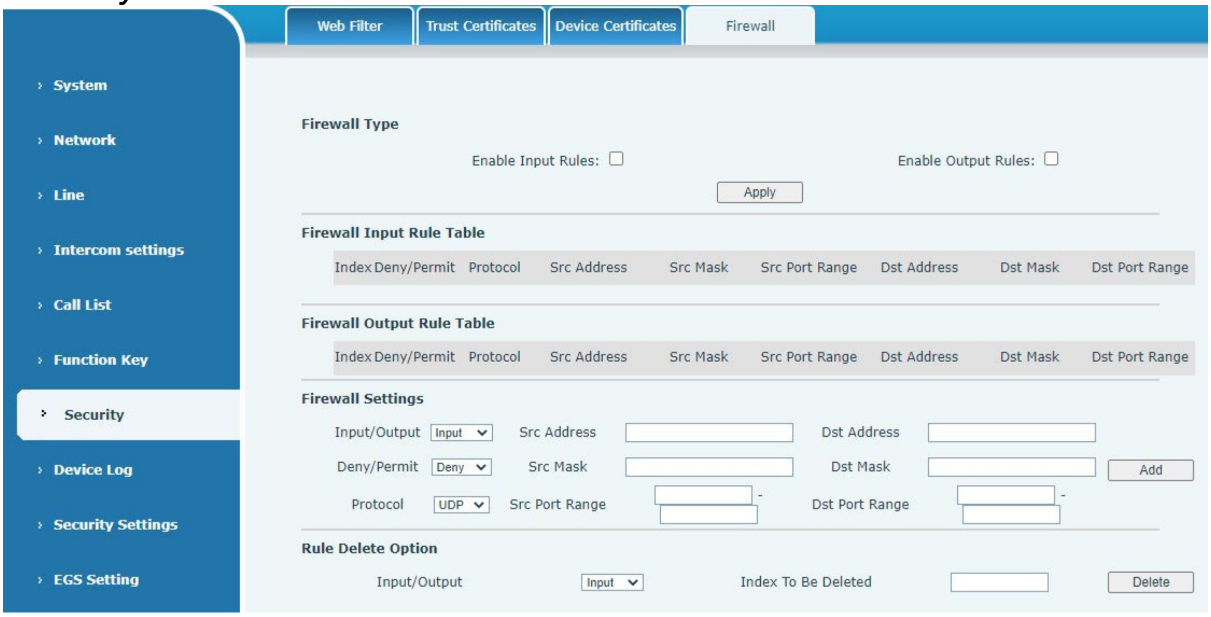
Load Server File: Select Upload

Certification File

| File Name | Issued To | Issued By | Expiration | File Size |
|---|---|---|---|---|

Delete

## *Security >> Firewall*



**Firewall Type**

Enable Input Rules: □ Enable Output Rules: □

**Firewall Input Rule Table**

| Index | Deny/Permit | Protocol | Src Address | Src Mask | Src Port Range | Dst Address | Dst Mask | Dst Port Range |
|---|---|---|---|---|---|---|---|---|

**Firewall Output Rule Table**

| Index | Deny/Permit | Protocol | Src Address | Src Mask | Src Port Range | Dst Address | Dst Mask | Dst Port Range |
|---|---|---|---|---|---|---|---|---|

**Firewall Settings**

Input/Output: Input Src Address: Dst Address:

Deny/Permit: Deny Src Mask: Dst Mask:

Protocol: UDP Src Port Range: - Dst Port Range: -

**Rule Delete Option**

Input/Output: Input Index To Be Deleted:

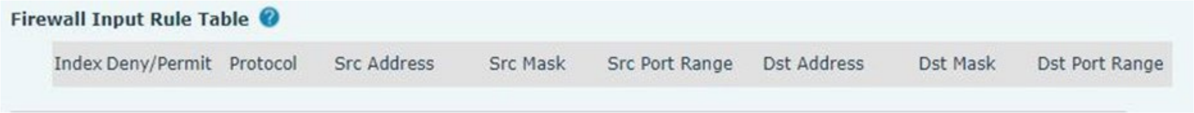
Through this page, you can set whether to enable the input and output firewalls, and at the same time, you can set the input and output rules of the firewall. Use these settings to prevent malicious network access, or restrict internal users from accessing some resources of the external network, and improve safety.

The firewall rule setting is a simple firewall module. This function supports two kinds of rules: input rules and output rules. Each rule will be assigned a serial number, and a maximum of 10 each rule can be set.

Taking into account the complexity of firewall settings, the following will illustrate with an example:

| Parameter | Description |
|---|---|
| Enable Input Rules | Enable Input Rules |
| Enable Output Rules | Enable Output Rules |
| input/output | Select the current rule as an input or output rule |
| Deny/permit | Choose a rule to deny or allow. |
| protocol | There are four types of protocols：TCP，UDP，ICMP，IP |
| Port range | Port range |
| Src Address | The source address can be the host address, network address, or all addresses 0.0.0.0; it can also be a network address similar to *.*.*.0, such as 192.168.1.0. |
| Dst Mask | The destination address can be a specific IP address or all addresses 0.0.0.0; it can also be a network address similar to *.*.*.0, such as 192.168.1.0. |
| Src Port Range | This is the source address mask. When it is configured as 255.255.255.255, it means it is a specific host. When it is set as a subnet mask of type 255.255.255.0, it means that the filter is a network segment. |
| Dst Port Range | This is the destination address mask. When it is configured as 255.255.255.255, it means it is a specific host. When it is set as a subnet mask of 255.255.255.0 type, it means that a network segment is filtered. |

After setting, click [Add], a new item will be added to the firewall output rules, as shown in the figure below:

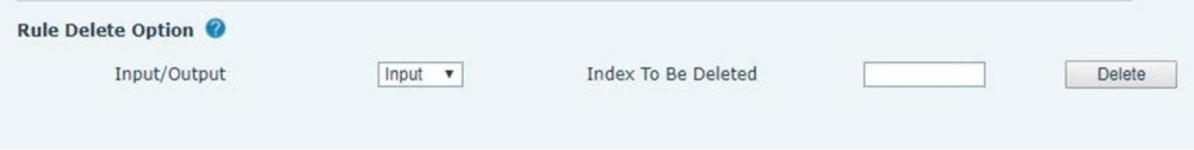


**Firewall Input Rule Table**

| Index | Deny/Permit | Protocol | Src Address | Src Mask | Src Port Range | Dst Address | Dst Mask | Dst Port Range |
|---|---|---|---|---|---|---|---|---|

Then select and click the button [Submit].

In this way, when the device runs: ping 192.168.1.118, it will not be able to send data packets to 192.168.1.118 because of the prohibition of the output rule. But ping other IPs in the 192.168.1.0 network segment can still receive the response packets from the destination host normally.



**Rule Delete Option**

Input/Output: Input ▾
Index To Be Deleted:

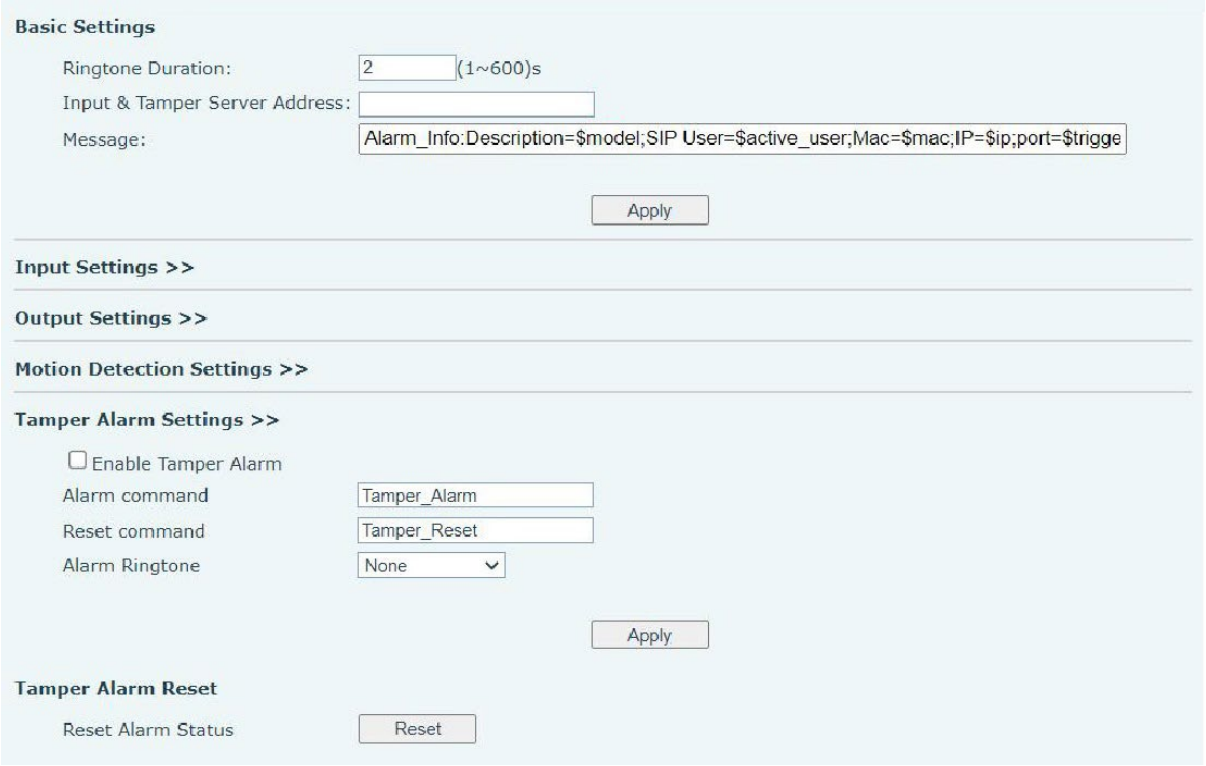
Select the list you want to delete and click [Delete] to delete the selected list.

## *Device log*

You can review the device log to help diagnose problems.

## *Security settings*

Enable Tamper: After enable, when the device is removed by force, the alarm information will be sent to the server and the alarm ring will be played. The following image is found in Security Settings.



**Basic Settings**

Ringtone Duration: 2 (1~600)s
Input & Tamper Server Address:
Message: Alarm_Info:Description=$model;SIP User=$active_user;Mac=$mac;IP=$ip;port=$trigge

**Input Settings >>**

**Output Settings >>**

**Motion Detection Settings >>**

**Tamper Alarm Settings >>**

☐ Enable Tamper Alarm
Alarm command: Tamper_Alarm
Reset command: Tamper_Reset
Alarm Ringtone: None ▾

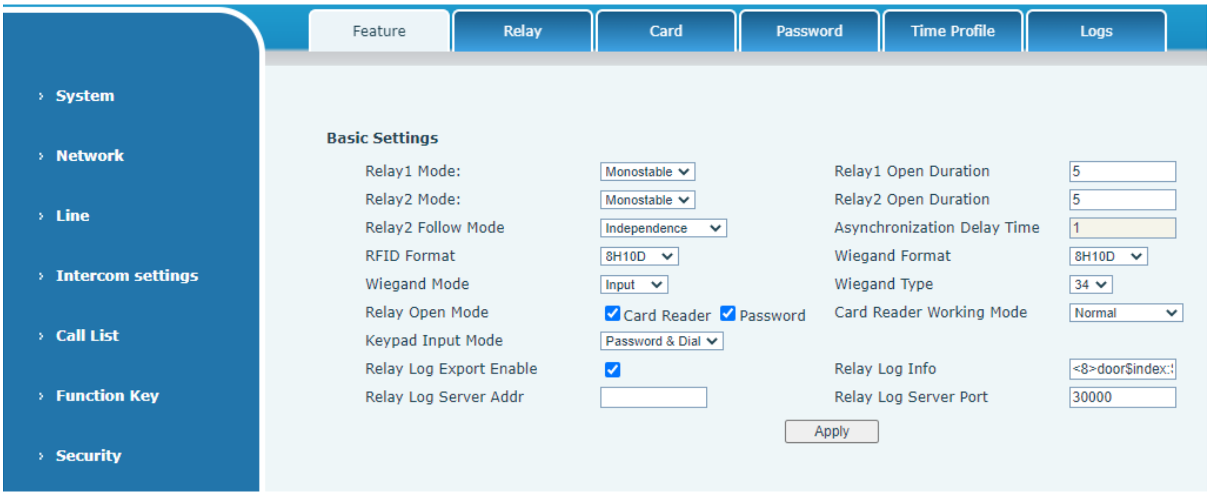
**Tamper Alarm Reset**

Reset Alarm Status

| **Security Settings** | |
|---|---|
| **Parameters** | **Description** |
| **Basic Settings** | |
| Ringtone Duration | Set the ringtone duration, default value is 2 seconds. |
| Input & Tamper Server Address | Set remote server address. The device will send message to the server when the alarm is triggered. The message format is：<br>Alarm_Info:Description=AC64v;SIP User=;Mac=0c:38:3e:3a:06:65;IP=; port=Input . |
| Message | Fill in the information to the upload server |
| **Input settings** | |
| Input | Enable or disable Input |
| Triggered by | When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger. |
| | When choosing the high level trigger (disconnect trigger), detect the input port (high level) disconnected trigger. |
| Input Duration | Set the Input change duration time, the default is 5 seconds. |
| Triggered Action | **Send SMS:** Set the alert message send to server if selected.<br>**Event:** The device will perform corresponding Dss Key configurations if any key is selected, by default the value is none.<br>**Triggered Ringtone:** Select triggered ring tone. |
| Triggered Ringtone | Ringtone selection |
| **Output Settings** | |
| Enable Logs | Enable or disable LOG |
| Triggered by DTMF Ring tone | Select the DTMF trigger ring tone. |
| Triggered by URI Ringtone | Select the URI trigger ring tone. |
| Triggered By SMS Ringtone | Select the SMS trigger ring tone. |
| Triggered By Dsskey Ringtone | Select the Dsskey trigger ring tone. |
| Output Response | Enable or disable Output Response |
| Standard Status | 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 NC port close. |
| Output Duration | Set the output change duration time, the default is 5 seconds. |
| Input trigger | When the input port meets the trigger condition, the output port will trigger (the port level time changes, controlled by <output duration>). |
| Trigger by DTMF | Enable or disable trigger by DTMF. The device will check the received DTMF sent by remote device, if it matches the DTMF trigger code, the device will trigger corresponding output port. |
| DTMF Trigger Code | Input the DTMF trigger code, default value is 1234. |
| DTMF Reset Code | Input the DTMF reset code, default value is 4321. |
| Reset By | Reset the output port mode by duration or state.<br>By duration: Reset the output port status when output duration occurs.<br>By state: Reset the output port status when device’s call state changes. |

| | |
|---|---|
| Trigger by URI | Enable or disable trigger by URI.<br>User can send commands from remote device or server to a compatible device, if the command is correct, then device will trigger corresponding output port. |
| Trigger Message | Input trigger message for trigger by URI mode. |
| Rest Message | Input reset message for trigger by URI mode. |
| Trigger by SMS | Enable or disable trigger by SMS.<br>User can send ALERT command to a compatible device, if the command is correct, then device will trigger corresponding output port. |
| Trigger SMS | Input trigger message for trigger by SMS mode. |
| Reset SMS | Input reset message for trigger by SMS mode. |
| Trigger by Input | Select the input port, when the input port meets the trigger condition, the output port will be triggered (The Port level time change, By < Output Duration > control) |
| Trigger By Call state | Select call state to trigger the output port, options are:<br>Talking: When the device’s talking status changes, trigger the output port.<br>Ringing: When the device’s ringing status changes, trigger the output port.<br>Calling: When the device’s calling status changes, trigger the output port. |
| Trigger By DssKey | Enable or disable trigger by dsskey. If any of the dsskey is selected, when the dsskey application performs, the output port will be triggered. |
| Triggered Hangup | Trigger the output port after hanging up |
| Hangup Delay | Hang up trigger delay, default 5 seconds |
| **Motion detection settings** | |
| Motion Detection Alarm | Enable or disable motion detection |
| Trigger Duration | Set the trigger delay time, the default is 3 seconds, the range: 0~3600 seconds |
| Trigger ringtone | Support ringtone selection |
| Trigger behavior:<br>Send SMS | Enable or disable the input port to send messages to the server |
| Function key | When set to dsskey1 or dsskey2, trigger dsskey to make a call, the default is none |
| **Tamper Alarm Settings** | |
| Enable Tamper Alarm | Enable tamper detection. If the device is violently dismantled, the tamper is triggered and will always play the set alarm ringtone |
| Alarm command | When detected someone tampering the device, the alarm signal will be sent to the corresponding server |
| Reset command | When the device receives the command of reset from server, the device will stop alarm |
| Alarm Ringtone | Alarm ringtone setting |
| Detachable alarm reset | |
| Reset alarm state | Reset the play of stop ringtone |

## *EGS Setting >> Features*

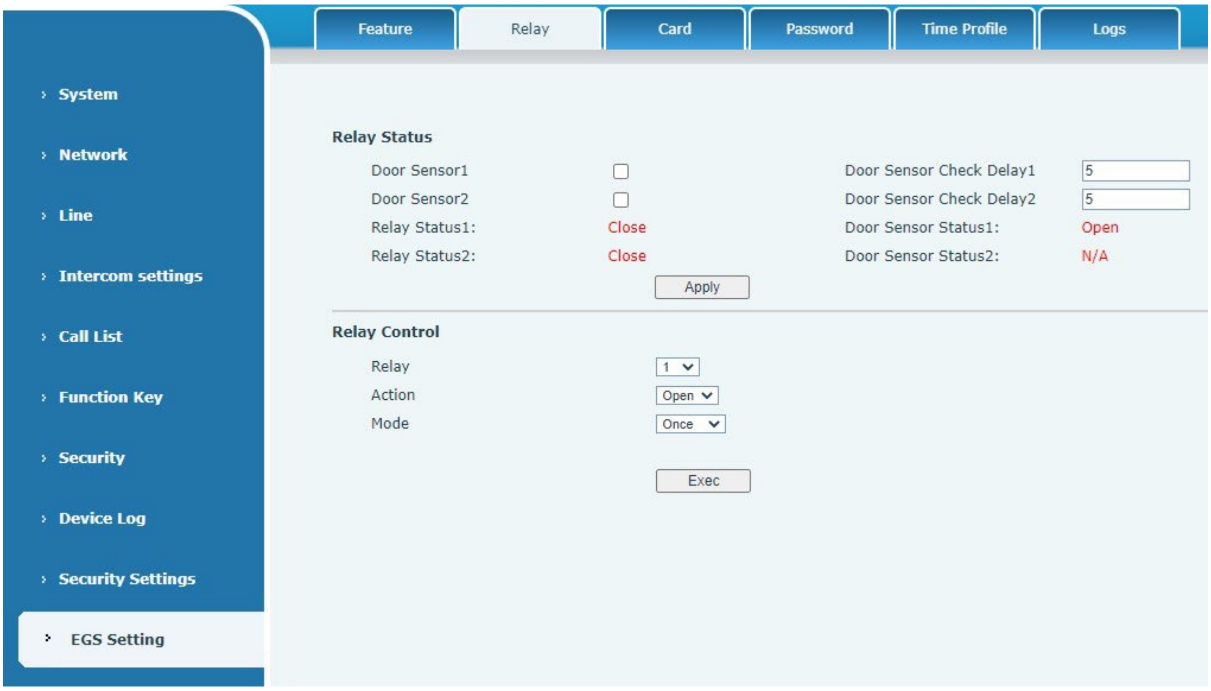


**Basic Settings**

| | | | |
|---|---|---|---|
| Relay1 Mode: | Monostable | Relay1 Open Duration | 5 |
| Relay2 Mode: | Monostable | Relay2 Open Duration | 5 |
| Relay2 Follow Mode | Independence | Asynchronization Delay Time | 1 |
| RFID Format | 8H10D | Wiegand Format | 8H10D |
| Wiegand Mode | Input | Wiegand Type | 34 |
| Relay Open Mode | ☑ Card Reader ☑ Password | Card Reader Working Mode | Normal |
| Keypad Input Mode | Password & Dial | | |
| Relay Log Export Enable | ☑ | Relay Log Info | <8>door$index: |
| Relay Log Server Addr | | Relay Log Server Port | 30000 |

| Field Name | Explanation |
|---|---|
| **Basic Settings** | |
| Relay1 Mode | Monostable: there is only one fixed action status for door unlocking.<br>Bistable: there are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After changed, the status would be kept.<br>Initial Value is Monostable |
| Relay1 Duration | Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial Value is 5 seconds. |
| Relay2 Mode | Monostable: there is only one fixed action status for door unlocking.<br>Bistable: there are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After changed, the status would be kept.<br>Initial Value is Monostable |
| Relay2 Duration | Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial Value is 5 seconds. |
| Relay2Follow mode | Independent: Open the door independently with Relay1 Synchronous: open the door at the same time as Relay1 Asynchronous: Relay1 opens after a period of time Relay2 opens |
| Asynchronous delay | The user can set the asynchronous door opening delay time of Relay1 and Relay2, the default is 1 second |
| RFID card format | Supported access control card format |
| Wiegand format | Supported Wiegand access card format |
| Wiegand mode | Optional input port or output port |
| Enable Virtual password | After enabling, the correct password will be included in the consecutively entered numbers to open the door |
| Enable Card Reader | Enable or disable card reader for RFID cards. |
| Card Reader Working Mode | Set ID card status:<br>Normal: This is the work mode, after the slot card can to open the door.<br>Card Issuing: This is the issuing mode, after the slot card can to add ID cards.<br>Card Revoking: This is the revoking mode, after the slot card can to delete ID cards. |

*EGS Setting >> Relay*



Relay Status

| | | | |
|---|---|---|---|
| Door Sensor1 | □ | Door Sensor Check Delay1 | 5 |
| Door Sensor2 | □ | Door Sensor Check Delay2 | 5 |
| Relay Status1: | Close | Door Sensor Status1: | Open |
| Relay Status2: | Close | Door Sensor Status2: | N/A |

Apply

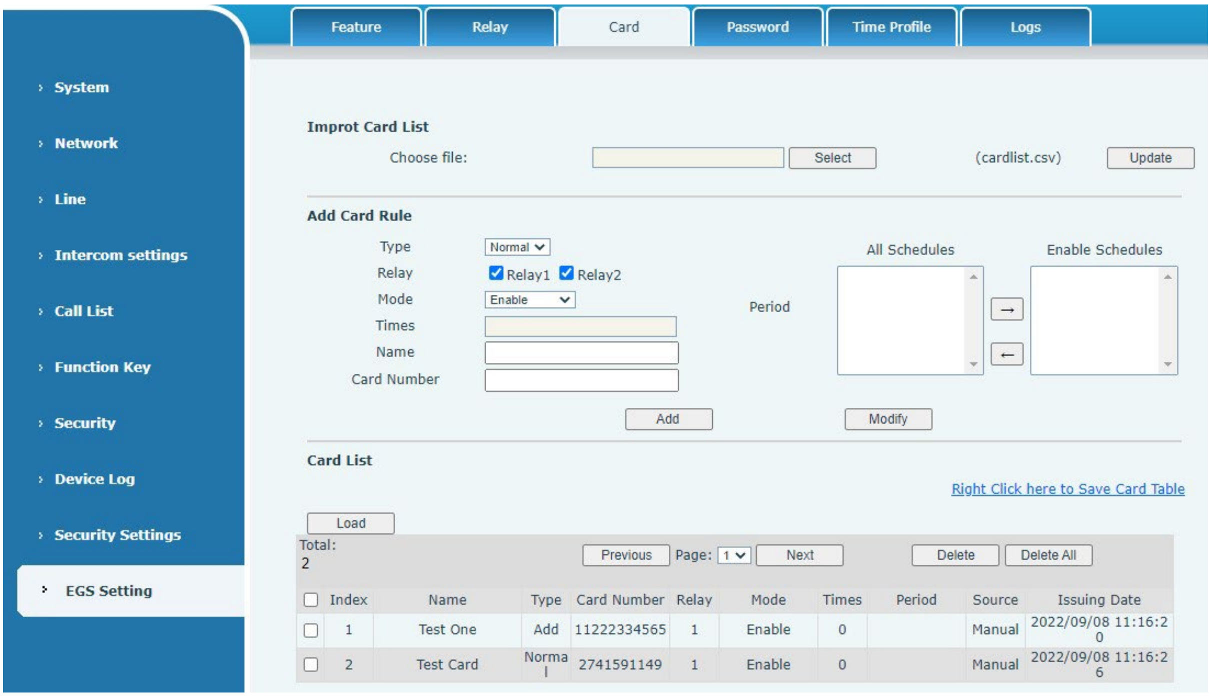
Relay Control

| | |
|---|---|
| Relay | 1 |
| Action | Open |
| Mode | Once |

Exec

| Field Name | Explanation |
|---|---|
| **Relay Status** | |
| Door Sensor1 | Enable or disable door sensor 1 |
| Door Sensor Check Delay 1 | Door Sensor1 detection delay time setting,5 seconds by default |
| Door Sensor2 | Enable or disable door status sensor 2 |
| Door Sensor Check Delay 2 | Door Sensor2 detection delay time setting,5 seconds by default |
| Lock Status 1 | Door Close/Open |
| Door Sensor Status1 | Door Close/Open |
| Lock Status 2 | Door Close/Open |
| Door Sensor Status2 | Door Close/Open |
| **Door Lock Control** | |
| Door Lock | Execute a door lock to open or close the door |
| Action | Door Open/Close |
| Open mode | Once: perform door opening action, and will be closed automatically when timeout.<br>Continue: perform the door opening action, the door will not be closed automatically and will need to be closed manually when timeout. |

# *EGS Setting >> Card*



Improt Card List

Choose file: (cardlist.csv)

Add Card Rule

Type: Normal

Relay: ☑ Relay1 ☑ Relay2

Mode: Enable

Times:

Name:

Card Number:

Period: All Schedules / Enable Schedules

Card List

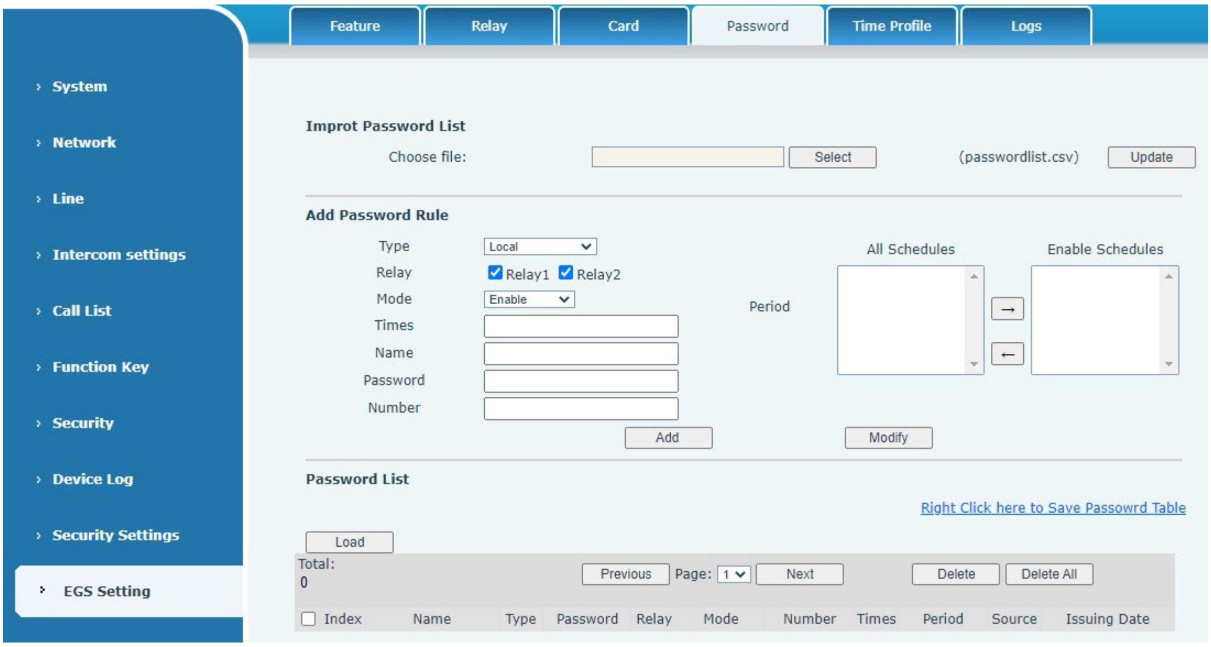
Total: 2

Page: 1

| □ | Index | Name | Type | Card Number | Relay | Mode | Times | Period | Source | Issuing Date |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | Test One | Add | 11222334565 | 1 | Enable | 0 |  | Manual | 2022/09/08 11:16:20 |
| □ | 2 | Test Card | Normal | 2741591149 | 1 | Enable | 0 |  | Manual | 2022/09/08 11:16:26 |

| Field Name | Explanation |
|---|---|
| **Import Card List** | |
| Click the <Select> to choose to import remote card list file (cardlist.csv) and then clicking <Update> can batch import remote card rule. | |
| **Add Card Rule** | |
| Type | **Normal**, namely to open the door card<br>**Add**, swipe the added card administrator card in the standby mode, the device will enter the card add mode, and then swipe the card, the card that has not been added to the card list will be added.<br>**Delete**, swipe the added card delete administrator card in standby, the device will enter the card delete mode, and then swipe the card, the added card will be deleted. |
| Relay | Swipe to open the door lock |
| Mode | Closed, swiping is unsuccessful after disabling Enable, swipe the card to take effect after enabling.<br>Time zone, swiping the card in the set time zone takes effect. |
| Times | The number of times the card can be swiped in a time period |
| Name | User name |
| Card Number | RFID card number. You can manually fill in the first 10 digits of the card number or select the existing card number |
| Period | The time to add the card, automatically generated |
| **Card List** | |
| Operation | Delete, delete all.<br>Export, support to export to csv. file. |

## *EGS Setting >> Password*



Type: Local

Relay: ☑ Relay1 ☑ Relay2

Mode: Enable

Times:

Name:

Password:

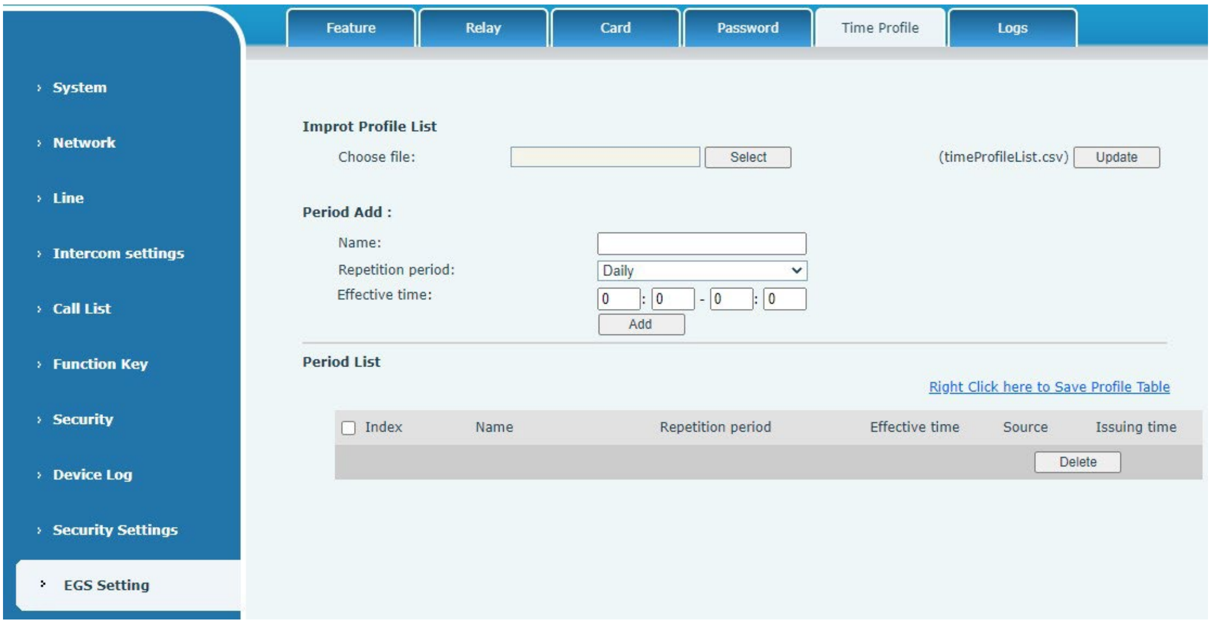
Number:

Total: 0

Page: 1

| Field Name | Explanation |
|---|---|
| **Import Password List** | |
| Click the <Select> to choose to import remote password list file (passwordlist.csv) and then clicking <Update> can batch import remote password rule. | |
| **Add Password Rule** | |
| Type | **Local**: That is, the local door opening password, enter a password that can be used to open the door.<br>**Remote**: Remote opening password, when the indoor unit calls the door device or when the door device calls the indoor unit to open the door, enter the DTMF password to open the door.<br>**Remote and local**: One password supports two door opening methods at the same time. |
| Relay | A door lock with a code |
| Mode | **Disable**, unsuccessful password opening after disabling.<br>**Enable**, after enabling the password to open the door to take effect.<br>**Time Profile**, the password to open the door takes effect during the set time profile. |
| Times | The number of times the door can be opened with a password within a given time period |
| Name | User name |
| Password | Password to open the door |
| Number | When the indoor unit calls the access control or the access control calls the indoor unit to open the door, enter the DTMF password to open the door |
| Period | Time to add the card, automatically generated |
| **Password List** | |
| Operation | **Delete**: Delete all<br>**Export**: Support to export to csv. file |

## *EGS Setting >> Time Profile*



Improt Profile List

Choose file: (timeProfileList.csv)

Period Add :

Name:

Repetition period: Daily

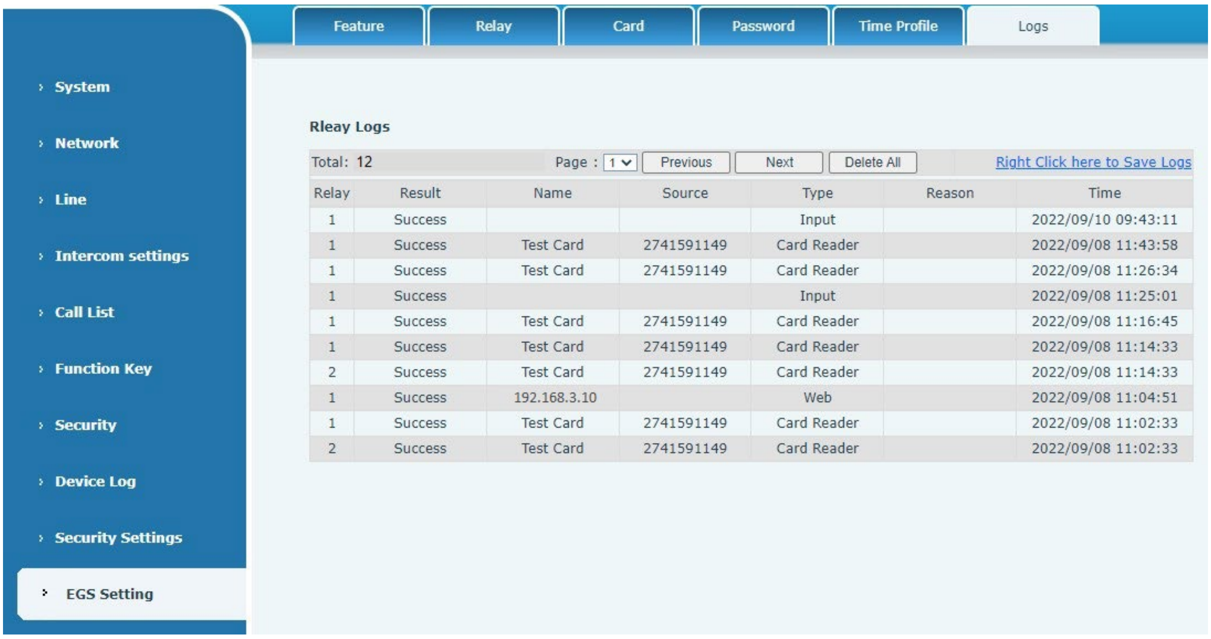
Effective time: 0 : 0 - 0 : 0

Period List

| □ Index | Name | Repetition period | Effective time | Source | Issuing time |
|---|---|---|---|---|---|

| **Field Name** | **Explanation** |
|---|---|
| **Import time list** | |
| Click the <Select> to choose to import remote Profile list file (timeProfileList.csv) and then clicking <Update> can batch import remote Period. | |
| **Period Add** | |
| Name | Set the name of the time period |
| Repetition period | **No repetition**: Opening the door in the set time period is valid, and it is invalid at other times.<br>**Daily**: It is valid to open the door in the time period set daily, and it is invalid at other times.<br>**Weekly**: It is valid to open the door in the time period set every week, and it is invalid at other times.<br>**Monthly**: Open the door in the time period set every month is valid, and it is invalid at other times. |
| Effective time | Set the effective time |

## *EGS Setting >> Logs*



Rleay Logs

Total: 12

| Relay | Result | Name | Source | Type | Reason | Time |
|---|---|---|---|---|---|---|
| 1 | Success | | | Input | | 2022/09/10 09:43:11 |
| 1 | Success | Test Card | 2741591149 | Card Reader | | 2022/09/08 11:43:58 |
| 1 | Success | Test Card | 2741591149 | Card Reader | | 2022/09/08 11:26:34 |
| 1 | Success | | | Input | | 2022/09/08 11:25:01 |
| 1 | Success | Test Card | 2741591149 | Card Reader | | 2022/09/08 11:16:45 |
| 1 | Success | Test Card | 2741591149 | Card Reader | | 2022/09/08 11:14:33 |
| 2 | Success | Test Card | 2741591149 | Card Reader | | 2022/09/08 11:14:33 |
| 1 | Success | 192.168.3.10 | | Web | | 2022/09/08 11:04:51 |
| 1 | Success | Test Card | 2741591149 | Card Reader | | 2022/09/08 11:02:33 |
| 2 | Success | Test Card | 2741591149 | Card Reader | | 2022/09/08 11:02:33 |

| Field Name | Explanation |
|---|---|
| Relay | Relay |
| Result | Display the result of a single door opening (success or failure) |
| Name | The name of the person who opened the door |
| Source | Card number or password to open the door |
| Type | Door opening type, including password, credit card |
| Reason | Reasons for failed door opening |
| Time | Opening time |

# 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 for diagnostics.

## *Get device system information*

Users can obtain information through the [**System**] >> [**Information**] option on the device webpage. The following device information will be provided: model, software and hardware version, Internet Information, etc.

## *Reboot device*

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

## *Device factory reset*

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

To restore the factory settings, go to [**System**] >> [**Configuration**] >> [**Reset Phone**] page, and click [**Reset**] button, the device will return to the factory default state.

## *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 Technical Support.

## *Get device log*

Log information is helpful when encountering abnormal problems. In order to obtain the log information of the device, the user can log on to the device web page, open the web page **[device log]**, click the "start" button, follow the steps of the problem until the problem appears, and then click the "end" button, "save" to the local for analysis or send the log to the technician to locate the problem.

## *Common Trouble Cases*

| **Trouble Case** | **Solution** |
|---|---|
| Device will not boot up | 1. The device is powered by external power supply via power adapter or PoE switch. Use standard power adapter or a PoE switch that meets standard PoE specifications and check that device is well connected to power source.<br>2. If the device enters "POST mode" (the SIP/NET and function button indicators are always on), the device is in a failed state. Contact technical support to help restore device function. |
| Device unable to register to a service provider | 1. Check if the device is connected to the network.<br>2. If the network connection is good, check your line configuration again. If all configurations are correct, contact tech support, or follow the instructions in "Network Data Capture" to obtain a registered network packet capture to help analyze the issue. |