

# i31S IP Video DoorPhone User Manual V2.0



| Document VER | Firmware VER | Explanation   | Time     |
|--------------|--------------|---|----------|
| V1.0         | 2.1.1.2898   | Initial issue   | 20170629 |
| V2.0         | 2.1.1.2898   | Change company address and add IP scan tool download address in QIG | 20171027 |
|              |              |   |          |
|              |              |   |          |
|              |              |   |          |

#### FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

#### FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and consider removing the no-collocation statement.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

#### Caution!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## Safety Notices

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

## Directory

|     |  |    |
|-----|--|----|
| I   | Product introduction.....                                    | 6  |
| 1.  | Appearance of the product .....                              | 6  |
| 2.  | Description.....   | 6  |
| II  | Start Using.....   | 7  |
| 1.  | Confirm the connection .....                                 | 7  |
| 1)  | Power, Electric Lock, Indoor switch port.....                | 7  |
| 2)  | Driving mode of electric-lock(Default in Passive mode) ..... | 7  |
| 3)  | Wiring instructions .....                                    | 8  |
| 2.  | Quick Setting.....   | 9  |
| III | Basic operation .....  | 10 |
| 1.  | Answer a call .....  | 10 |
| 2.  | Call.....  | 10 |
| 3.  | End call.....  | 10 |
| 4.  | Open the door operation .....                                | 10 |
| IV  | Page settings.....   | 11 |
| 1.  | Browser configuration .....                                  | 11 |
| 2.  | Password Configuration.....                                  | 11 |
| 3.  | Configuration via WEB .....                                  | 12 |
| (1) | System .....   | 12 |
| a)  | Information .....  | 12 |
| b)  | Account .....  | 13 |
| c)  | Configurations.....  | 14 |
| d)  | Upgrade.....   | 14 |
| e)  | Auto Provision .....   | 15 |
| f)  | Tools.....   | 17 |
| (2) | Network.....   | 19 |
| a)  | Basic .....  | 19 |
| b)  | VPN .....  | 20 |
| (3) | Line.....  | 22 |
| a)  | SIP .....  | 22 |
| b)  | Basic Settings.....  | 26 |
| (4) | EGS Setting .....  | 29 |
| a)  | Features.....  | 29 |

|                               |    |
|-------------------------------|----|
| b) Audio.....                 | 32 |
| c) Video .....                | 34 |
| d) MCAST.....                 | 36 |
| e) Action URL .....           | 39 |
| f) Time/Date .....            | 39 |
| (5) EGS Access .....          | 41 |
| (6) EGS Logs .....            | 43 |
| (7) Function Key .....        | 44 |
| (8) Alert .....               | 46 |
| V Appendix .....              | 49 |
| 1. Technical parameters ..... | 49 |
| 2. Basic functions .....      | 50 |
| 3. Schematic diagram .....    | 50 |
| VI Other instructions.....    | 51 |
| 1. Open door modes.....       | 51 |
| 2. Management of card .....   | 51 |

## I Product introduction

i31S voice access is a full digital network door phone, with its core part adopts mature VoIP solution (Broadcom chip), stable and reliable performance, hands-free adopting digital full-duplex mode, voice loud and clear, generous appearance, solid durable, easy for installation, comfortable keypad and low power consumption.





i31S voice access supports entrance guard control, voice intercom, ID card and keypad remote to open the door.

### 1. Appearance of the product



### 2. Description

| Buttons and icons | Description       | Function  |
|-------------------|-------------------|---|
|                   | Numeric keyboard  | Input password to open the door or to call.   |
|                   | programmable keys | Can be set to a variety of functions, in order to meet the needs of different occasions |
|                   | induction zone    | RFID induction area   |
|                   | Camera            | Video signal acquisition and transmission   |

|   |                          |  |
|---|--------------------------|--|
|  | Lock Status              | Door unlocking: On<br>Door locking: Off  |
|  | Call status              | Standby: Off<br>Call Holding: Blink with 1s<br>Calls: On   |
|  | Ring status              | Standby: Off<br>Ringing: On  |
|  | Network/SIP Registration | Network error: Blink with 1s<br>Network running: Off<br>Registration failed: Blink with 3s<br>Registration succeeded: On |

## II Start Using

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


### 1. Confirm the connection

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

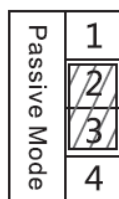
#### 1) Power, Electric Lock, Indoor switch port

Voice access the power supply ways: 12v/DC or POE.

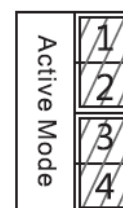
| CN7       |     |                      |     |    |               |       |
|-----------|-----|----------------------|-----|----|---------------|-------|
| 1         | 2   | 3                    | 4   | 5  | 6             | 7     |
| +12V      | VSS | NC                   | COM | NO | S_IN        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



#### 2) Driving mode of electric-lock(Default in Passive mode)



Jumper in passive mode



Jumper in active mode

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

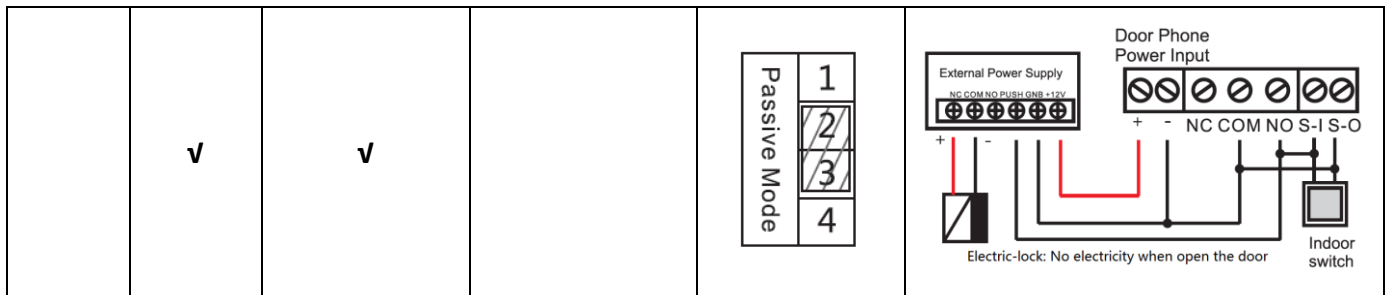
- When using the active mode, it is 12V DC in output.
- When using the passive mode, output is short control (normally open mode or normally close mode).

### 3) Wiring instructions

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

| Driving Mode |         | Electric lock            |                        | Jumper port | Connections   |
|--------------|---------|--------------------------|------------------------|-------------|---|
| Active       | Passive | No electricity when open | When the power to open |             |   |
| √            |         | √                        |                        |             | <p>Electric-lock: No electricity when open the door</p> |
| √            |         |                          | √                      |             | <p>Electric-lock: When the power to open the door</p>   |
|              | √       | √                        |                        |             | <p>Electric-lock: No electricity when open the door</p> |
|              | √       |                          | √                      |             | <p>Electric-lock: When the power to open the door</p>   |



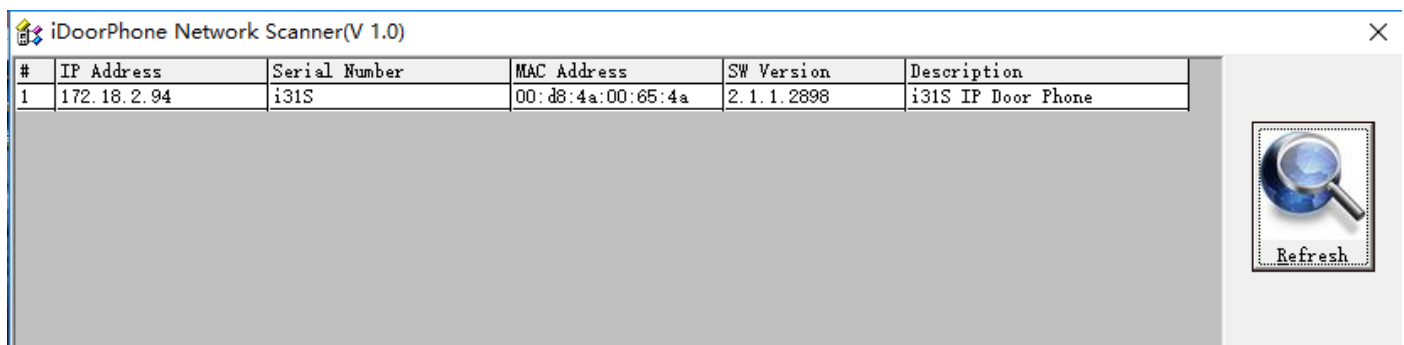


## 2. Quick Setting

The product provides a complete function and parameter setting. Users may need to have the network and SIP protocol knowledge to understand the meaning represented by all parameters. In order to let equipment users enjoy the high quality of voice service and low cost advantage brought by the device immediately, here we list some basic but compulsory setting options in this section to let users know how to operate without understanding such complex SIP protocols.

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

- Press and hold “#” key for 3 seconds and the door phone will report the IP address by voice, or use the "iDoorPhoneNetworkScanner.exe" software to find the IP address of the device.  
(Download address <http://download.fanvil.com/tool/iDoorPhoneNetworkScanner.exe> )
- **Note:** when power on, 30s waiting is needed for device running.
- Log on to the WEB device configuration.
- In a Line page configuration service account, user name, parameters that are required for server address register.
- You can set DSS key in the Function key page.
- You can set Door Phone parameters in the Webpage (EGS Setting-> Features).



## III Basic operation

### 1. Answer a call

When a call comes in, the device will answer automatically. If you cancel auto answer feature and set auto answer time, you will hear the bell ring at the set time and the device will auto answer after a timeout.

### 2. Call

Configure shortcut key as hot key and setup a number, then press shortcut key can call the configured number.

### 3. End call

Enable Release key hang up to end call.

### 4. Open the door operation

Through the following seven ways to open the door:

- 1) Input password on the keyboard to open the door.
- 2) Access to call the owner and the owner enter the remote password to open the door.
- 3) Owner/other equipment call the access control and enter the access code to open the door. (access code should be included in the list of access configuration, and enable for remote calls to open the door)
- 4) Swipe the RFID cards to open the door.
- 5) By means of indoor switch to open the door.
- 6) Private access code to open the door.

Enable for local authentication, and set private access code. Input the access code directly under standby mode to open the door. In this way, the door log will record corresponding card number and user name.

- 7) Active URL control command to open the door.

URL is "http://user:pwd@host/cgi-bin/ConfigManApp.com?key=F\_LOCK&code=openCode"

- a. User and pwd is Web the user name and password.
- b. "openCode" is the remote control code to open the door.

Example: "http://admin:admin@172.18.3.25/cgi-bin/ConfigManApp.com?key=\*"

If access code is input correctly, the device will play sirens sound to prompt access control and the remote user, while input error by low-frequency short chirp.

Password input successfully followed by high-frequency sirens sound, while input error is followed by

high-frequency short chirp.

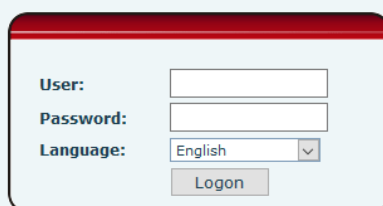
When door has been opened, the device will play sirens sound to prompt.

## IV Page settings

### 1. Browser configuration

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

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



The image shows a login form with the following fields and controls:

- User:** A text input field.
- Password:** A text input field.
- Language:** A dropdown menu currently set to "English".
- Logon:** A button to submit the login information.

### 2. Password Configuration

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

- Default user with general level: The default is not set, are free to add.
- Default user with root level:
  - ◆ User name: admin
  - ◆ Password: admin

## 3. Configuration via WEB

### (1) System

#### a) Information

The screenshot shows the Fanvil web interface with the 'Information' tab selected. The left sidebar contains a menu with options: System, Network, Line, EGS Setting, EGS Access, EGS Logs, Function Key, and Alert. The main content area is divided into three sections:

- System Information:**
  - Model: i31S
  - Hardware: 2.1
  - Software: 2.1.1.2898
  - Uptime: 21 : 00 : 35
  - Last uptime: 513:11:04
  - MEMInfo: ROM: 0.8/8(M) RAM: 2/16(M)
- Network:**
  - Network mode: DHCP
  - MAC: 00:a8:23:6a:6d:9e
  - IP: 172.18.2.131
  - Subnet mask: 255.255.0.0
  - Default gateway: 172.18.1.1
- SIP Accounts:**

| Line   | Account | Status   |
|--------|---------|----------|
| Line 1 | N/A     | Inactive |
| Line 2 | N/A     | Inactive |

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

## b) Account

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

| Account  |             |
|--|-------------|
| Field Name                                       | Explanation |
| <b>Change Web Authentication Password</b>        |             |
| You Can modify the login password to the account |             |
| <b>Add New User</b>                              |             |
| You can add new user                             |             |
| <b>User Accounts</b>                             |             |
| Show the existing user information               |             |

## c) Configurations

### Configurations

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

## d) Upgrade

### Upgrade

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

## e) Auto Provision

| Auto Provision                            |  |
|---|--|
| Field Name                                | Explanation  |
| <b>Common Settings</b>                    |  |
| Current Configuration Version             | Show the current config file's version. If the version of configuration downloaded is higher than this, the configuration will be upgraded. If the endpoints confirm the configuration by the Digest method, the configuration will not be upgraded unless it differs from the current configuration |
| General Configuration Version             | Show the common config file's version. If the configuration downloaded and this configuration is the same, the auto provision will stop. If the endpoints confirm the configuration by the Digest method, the configuration will not be upgraded unless it differs from the current configuration.   |
| CPE Serial Number                         | Serial number of the equipment   |
| Authentication Name                       | Username for configuration server. Used for FTP/HTTP/HTTPS. If this is blank the phone will use anonymous  |
| Authentication Password                   | Password for configuration server. Used for FTP/HTTP/HTTPS.  |
| Configuration File Encryption Key         | Encryption key for the configuration file  |
| General Configuration File Encryption Key | Encryption key for common configuration file   |

|                                   |  |
|-----------------------------------|--|
| Save Auto Provision Information   | Save the auto provision username and password in the phone until the server url changes  |
| <b>DHCP Option</b>                |  |
| Option Value                      | The equipment supports configuration from Option 43, Option 66, or a Custom DHCP option. It may also be disabled.  |
| Custom Option Value               | Custom option number. Must be from 128 to 254.   |
| <b>SIP Plug and Play (PnP)</b>    |  |
| Enable SIP PnP                    | If this is enabled, the equipment will send SIP SUBSCRIBE messages to a multicast address when it boots up. Any SIP server understanding that message will reply with a SIP NOTIFY message containing the Auto Provisioning Server URL where the phones can request their configuration. |
| Server Address                    | PnP Server Address   |
| Server Port                       | PnP Server Port  |
| Transportation Protocol           | PnP Transfer protocol – UDP or TCP   |
| Update Interval                   | Interval time for querying PnP server. Default is 1 hour.  |
| <b>Static Provisioning Server</b> |  |
| Server Address                    | Set FTP/TFTP/HTTP server IP address for auto update. The address can be an IP address or Domain name with subdirectory.  |
| Configuration File Name           | Specify configuration file name. The equipment will use its MAC ID as the config file name if this is blank.   |
| Protocol Type                     | Specify the Protocol type FTP, TFTP or HTTP.   |
| Update Interval                   | Specify the update interval time. Default is 1 hour.   |
| Update Mode                       | <ol style="list-style-type: none"> <li>1. Disable – no update</li> <li>2. Update after reboot – update only after reboot.</li> <li>3. Update at time interval – update at periodic update interval</li> </ol>  |
| <b>TR069</b>                      |  |
| Enable TR069                      | Enable/Disable TR069 configuration   |
| ACS Server Type                   | Select Common or CTC ACS Server Type.  |
| ACS Server URL                    | ACS Server URL.  |
| ACS User                          | User name for ACS.   |
| ACS Password                      | ACS Password.  |
| TR069 Auto Login                  | Enable/Disable TR069 Auto Login.   |
| INFORM Sending Period             | Time between transmissions of “Inform” Unit is seconds.  |



## f) FDMS

### FDMS Settings

|               |   |
|---------------|---|
| Enable FDMS   | Enable/Disable FDMS configuration   |
| FDMS Interval | The time to send sip Subscribe information to the FDMS server on a regular basis.<br>Unit seconds |

### Doorphone Info Settings

|                 |   |
|-----------------|---|
| Community Name  | The name of the community where the device is installed   |
| Building Number | The name of the building where the equipment is installed |
| Room Number     | The name of the room where the equipment is installed     |

## f) Tools

Syslog is a protocol used to record log messages using a client/server mechanism. The Syslog server receives the messages from clients, and classifies them based on priority and type. Then these messages will be written into a log by rules which the administrator has configured.

There are 8 levels of debug information.

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

Level 1: alert; Action must be taken immediately.

Level 2: critical; System is probably working incorrectly.

Level 3: error; System may not work correctly.

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

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

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

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

| Tools  |                               |
|--|-------------------------------|
| Field Name   | Explanation                   |
| <b>Syslog</b>  |                               |
| Enable Syslog  | Enable or disable system log. |
| Server Address   | System log server IP address. |
| Server Port  | System log server port.       |
| APP Log Level  | Set the level of APP log.     |
| SIP Log Level  | Set the level of SIP log.     |
| <b>Network Packets Capture</b>   |                               |
| Capture a packet stream from the equipment. This is normally used to troubleshoot problems.  |                               |
| <b>Reboot Phone</b>  |                               |
| Some configuration modifications require a reboot to become effective. Clicking the Reboot button will lead to reboot immediately. |                               |
| Note: Be sure to save the configuration before rebooting.  |                               |

## (2) Network

### a) Basic

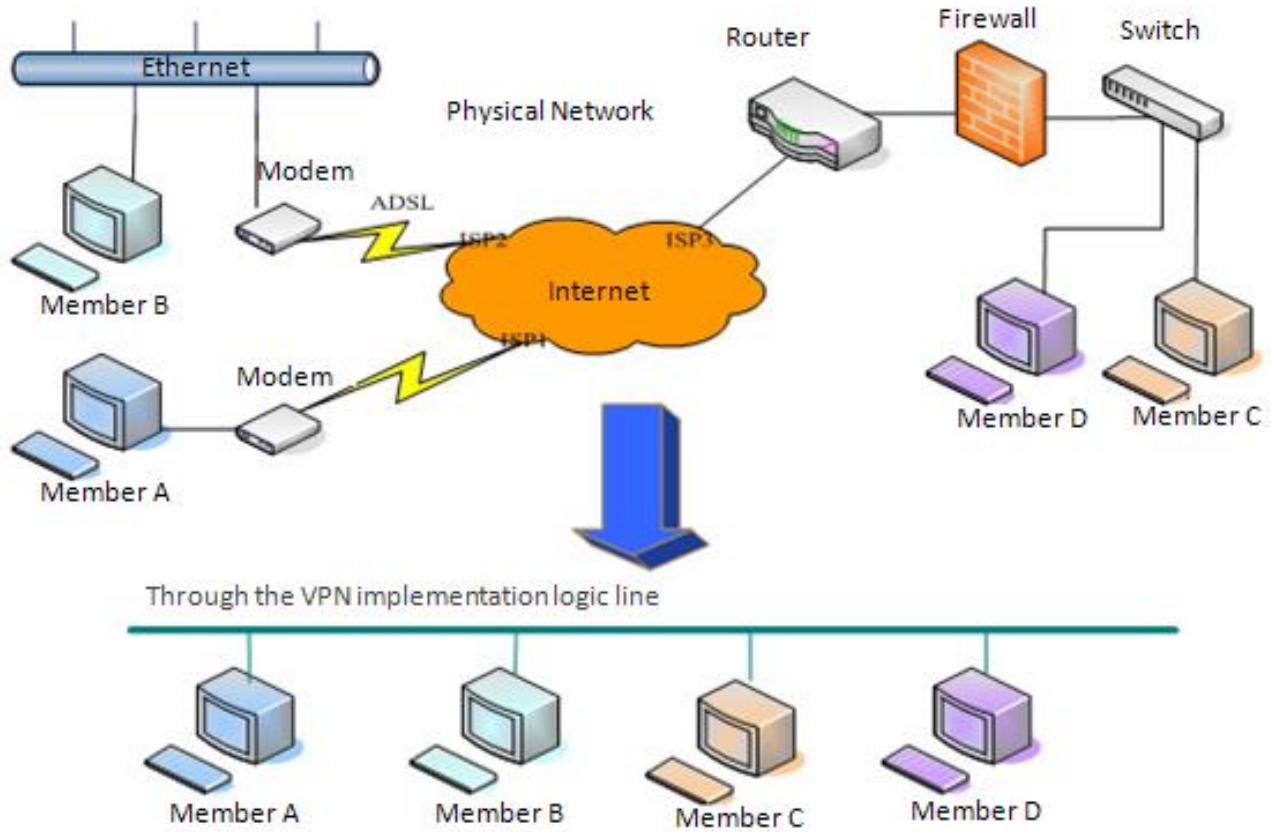
The screenshot displays the 'Basic' configuration tab for the VPN section. It is divided into three main sections: Network Status, Settings, and Service Port Settings. The Network Status section shows the current IP address, subnet mask, default gateway, and MAC address. The Settings section allows selecting a network mode (Static IP, DHCP, or PPPoE) and configuring DNS servers. The Service Port Settings section allows configuring the Web Server Type (HTTP or HTTPS) and their respective ports. An 'Apply' button is present at the end of each section. At the bottom, there is a field for the HTTPS Certification File (https.pem) with 'N/A' and 'Upload' and 'Delete' buttons.

| Field Name  | Explanation  |
|---|--|
| <b>Network Status</b>   |  |
| IP  | The current IP address of the equipment  |
| Subnet mask   | The current Subnet Mask  |
| Default gateway   | The current Gateway IP address   |
| MAC   | The MAC address of the equipment   |
| MAC Timestamp   | Get the MAC address of time.   |
| <b>Settings</b>   |  |
| Select the appropriate network mode. The equipment supports three network modes:        |  |
| Static IP   | Network parameters must be entered manually and will not change. All parameters are provided by the ISP. |
| DHCP  | Network parameters are provided automatically by a DHCP server.  |
| PPPoE   | Account and Password must be input manually. These are provided by your ISP.                             |
| If Static IP is chosen, the screen below will appear. Enter values provided by the ISP. |  |
| DNS Server Configured by  | Select the Configured mode of the DNS Server.  |
| Primary DNS Server  | Enter the server address of the Primary DNS.   |

|  |   |
|--|---|
| Secondary DNS Server   | Enter the server address of the Secondary DNS.  |
| After entering the new settings, click the APPLY button. The equipment will save the new settings and apply them. If a new IP address was entered for the equipment, it must be used to login to the phone after clicking the APPLY button.  |   |
| <b>Service Port Settings</b>   |   |
| Web Server Type  | Specify Web Server Type – HTTP or HTTPS   |
| HTTP Port  | Port for web browser access. Default value is 80. To enhance security, change this from the default. Setting this port to 0 will disable HTTP access.<br>Example: The IP address is 192.168.1.70 and the port value is 8090, the accessing address is http://192.168.1.70:8090. |
| HTTPS Port   | Port for HTTPS access. Before using https, an https authentication certification must be downloaded into the equipment.<br>Default value is 443. To enhance security, change this from the default.   |
| <p>Note:</p> <ol style="list-style-type: none"> <li>1) Any changes made on this page require a reboot to become active.</li> <li>2) It is suggested that changes to HTTP Port be values greater than 1024. Values less than 1024 are reserved.</li> <li>3) If the HTTP port is set to 0, HTTP service will be disabled.</li> </ol> |   |

## b) VPN

The device supports remote connection via VPN. It supports both Layer 2 Tunneling Protocol (L2TP) and OpenVPN protocol. This allows users at remote locations on the public network to make secure connections to local networks.



- > System
- > Network
- > Line
- > EGS Setting
- > EGS Access
- > EGS Logs
- > Function Key
- > Alert

Basic

VPN

### Virtual Private Network (VPN) Status

VPN IP Address: 0.0.0.0

---

**VPN Mode**

Enable VPN

L2TP  OpenVPN

**Layer 2 Tunneling Protocol (L2TP)**

L2TP Server Address

Authentication Name

Authentication Password

---

**OpenVPN Files**

|                             |             |     |                                       |                                       |
|-----------------------------|-------------|-----|---------------------------------------|---------------------------------------|
| OpenVPN Configuration file: | client.ovpn | N/A | <input type="button" value="Upload"/> | <input type="button" value="Delete"/> |
| CA Root Certification:      | ca.crt      | N/A | <input type="button" value="Upload"/> | <input type="button" value="Delete"/> |
| Client Certification:       | client.crt  | N/A | <input type="button" value="Upload"/> | <input type="button" value="Delete"/> |
| Client Key:                 | client.key  | N/A | <input type="button" value="Upload"/> | <input type="button" value="Delete"/> |

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

## (3) Line

### a) SIP

Configure a SIP server on this page.

The screenshot displays the Fanvil web interface for configuring a SIP line. The interface is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with the following items: System, Network, Line (selected), EGS Setting, EGS Access, EGS Logs, Function Key, and Alert. The main content area has a top navigation bar with tabs for SIP, Basic Settings, and Dial Peer. The 'SIP' tab is active, and the 'Line' dropdown is set to 'SIP 1'. Below this, the 'Basic Settings >>' section is expanded, showing the following configuration options:

- Line Status: Inactive
- Phone number:
- Display name:
- Authentication Name:
- Authentication Password:
- Activate:
- SIP Proxy Server Address:
- SIP Proxy Server Port:
- Backup Proxy Server Address:
- Backup Proxy Server Port:
- Outbound proxy address:
- Outbound proxy port:
- Realm:

Below the 'Basic Settings' section, there are links for 'Codecs Settings >>' and 'Advanced Settings >>'. An 'Apply' button is located at the bottom of the configuration area.

## Codecs Settings >>

Disabled Codecs



Enabled Codecs



## Advanced Settings >>

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

|                         |   |                      |   |
|-------------------------|---|----------------------|---|
| Specific Server Type    | <input type="text" value="COMMON"/>       | Enable DNS SRV       | <input type="checkbox"/>                  |
| Registration Expiration | <input type="text" value="60"/> Second(s) | Keep Alive Type      | <input type="text" value="UDP"/>          |
| Use VPN                 | <input checked="" type="checkbox"/>       | Keep Alive Interval  | <input type="text" value="30"/> Second(s) |
| Use STUN                | <input type="checkbox"/>                  | Sync Clock Time      | <input type="checkbox"/>                  |
| Convert URI             | <input checked="" type="checkbox"/>       | Enable Session Timer | <input type="checkbox"/>                  |
| DTMF Type               | <input type="text" value="AUTO"/>         | Session Timeout      | <input type="text" value="0"/> Second(s)  |
| DTMF SIP INFO Mode      | <input type="text" value="Send */#"/>     | Enable Rport         | <input checked="" type="checkbox"/>       |
| Transportation Protocol | <input type="text" value="UDP"/>          | Enable PRACK         | <input checked="" type="checkbox"/>       |
| Local Port              | <input type="text" value="5060"/>         | Auto Change Port     | <input type="checkbox"/>                  |
| SIP Version             | <input type="text" value="RFC3261"/>      | Keep Authentication  | <input type="checkbox"/>                  |
| Caller ID Header        | <input type="text" value="PAI-RPID-I"/>   | Auto TCP             | <input type="checkbox"/>                  |
| Enable Strict Proxy     | <input type="checkbox"/>                  | Enable Feature Sync  | <input type="checkbox"/>                  |
| Enable user=phone       | <input checked="" type="checkbox"/>       | Enable GRUU          | <input type="checkbox"/>                  |
| Enable SCA              | <input type="checkbox"/>                  | BLF Server           | <input type="text"/>                      |
| Enable BLF List         | <input type="checkbox"/>                  | BLF List Number      | <input type="text"/>                      |
| SIP Encryption          | <input type="checkbox"/>                  | RTP Encryption       | <input type="checkbox"/>                  |
| SIP Encryption Key      | <input type="text"/>                      | RTP Encryption Key   | <input type="text"/>                      |

Apply

| SIP   |   |
|---|---|
| Field Name  | Explanation   |
| <b>Basic Settings</b> (Choose the SIP line to configured)                               |   |
| Line Status   | Display the current line status at page loading. To get the up to date line status, user has to refresh the page manually.  |
| Username  | Enter the username of the service account.  |
| Display name  | Enter the display name to be sent in a call request.  |
| Authentication Name   | Enter the authentication name of the service account  |
| Authentication Password   | Enter the authentication password of the service account  |
| Activate  | Whether the service of the line should be activated   |
| SIP Proxy Server Address  | Enter the IP or FQDN address of the SIP proxy server  |
| SIP Proxy Server Port   | Enter the SIP proxy server port, default is 5060  |
| Outbound proxy address  | Enter the IP or FQDN address of outbound proxy server provided by the service provider  |
| Outbound proxy port   | Enter the outbound proxy port, default is 5060  |
| Realm   | Enter the SIP domain if requested by the service provider   |
| <b>Codecs Settings</b>  |   |
| Set the priority and availability of the codecs by adding or remove them from the list. |   |
| <b>Advanced Settings</b>  |   |
| Subscribe For Voice Message   | Enable the device to subscribe a voice message waiting notification, if enabled, the device will receive notification from the server if there is voice message waiting on the server |
| Voice Message Number  | Set the number for retrieving voice message   |
| Voice Message Subscribe Period  | Set the interval of voice message notification subscription   |
| Enable DND  | Enable Do-not-disturb, any incoming call to this line will be rejected automatically  |
| Blocking Anonymous Call   | Reject any incoming call without presenting caller ID   |
| Use 182 Response for Call waiting   | Set the device to use 182 response code at call waiting response  |
| Anonymous Call Standard   | Set the standard to be used for anonymous   |
| Dial Without Registered   | Set call out by proxy without registration  |
| Click To Talk   | Set Click To Talk   |
| User Agent  | Set the user agent, the default is Model with Software Version.   |

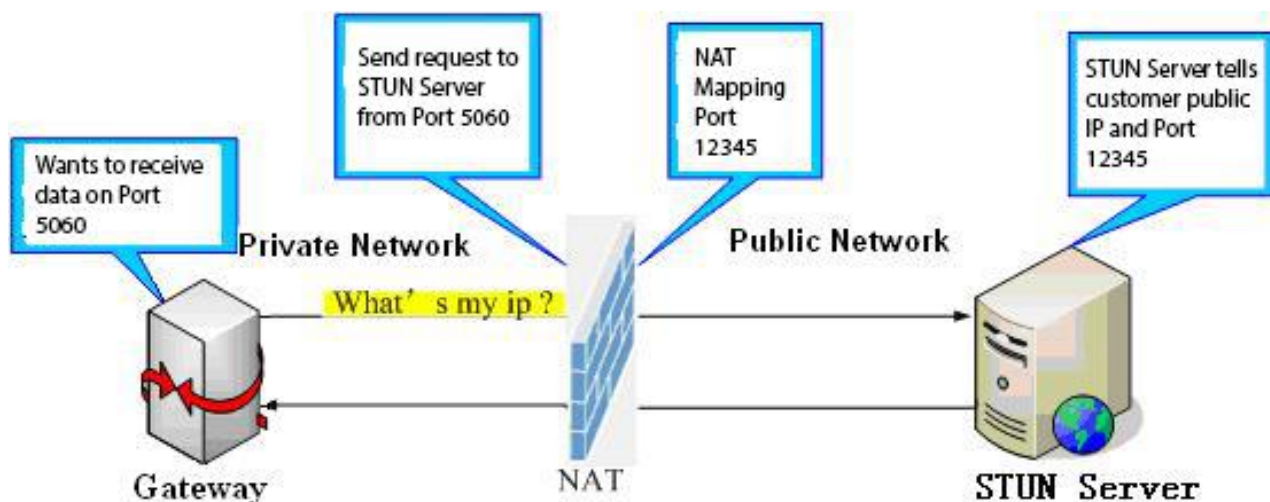


|                           |  |
|---------------------------|--|
| Response Single Codec     | If setting enabled, the device will use single codec in response to an incoming call request   |
| Ring Type                 | Set the ring tone type for the line  |
| Conference Type           | Set the type of call conference, Local=set up call conference by the device itself, maximum supports two remote parties, Server=set up call conference by dialing to a conference room on the server   |
| Server Conference Number  | Set the conference room number when conference type is set to be Server  |
| Transfer Timeout          | Set the timeout of call transfer process   |
| Enable Long Contact       | Allow more parameters in contact field per RFC 3840  |
| Use Quote in Display Name | Whether to add quote in display name   |
| Use Feature Code          | When this setting is enabled, the features in this section will not be handled by the device itself but by the server instead. In order to control the enabling of the features, the device will send feature code to the server by dialing the number specified in each feature code field. |
| Specific Server Type      | Set the line to collaborate with specific server type  |
| Registration Expiration   | Set the SIP expiration interval  |
| Use VPN                   | Set the line to use VPN restrict route   |
| Use STUN                  | Set the line to use STUN for NAT traversal   |
| Convert URI               | Convert not digit and alphabet characters to %hh hex code  |
| DTMF Type                 | Set the DTMF type to be used for the line  |
| DTMF SIP INFO Mode        | Set the SIP INFO mode to send '*' and '#' or '10' and '11'   |
| Transportation Protocol   | Set the line to use TCP or UDP for SIP transmission  |
| Local Port                | Set the Local Port   |
| SIP Version               | Set the SIP version  |
| Caller ID Header          | Set the Caller ID Header   |
| Enable Strict Proxy       | Enables the use of strict routing. When the phone receives packets from the server, it will use the source IP address, not the address in via field.   |
| Enable user=phone         | Sets user=phone in SIP messages.   |
| Enable SCA                | Enable/Disable SCA (Shared Call Appearance )   |
| Enable BLF List           | Enable/Disable BLF List  |
| Enable DNS SRV            | Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list  |
| Keep Alive Type           | Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole opened  |
| Keep Alive Interval       | Set the keep alive packet transmitting interval  |

|                      |  |
|----------------------|--|
| Enable Session Timer | Set the line to enable call ending by session timer refreshment. The call session will be ended if there is not new session timer event update received after the timeout period   |
| Session Timeout      | Set the session timer timeout period   |
| Enable Rport         | Set the line to add rport in SIP headers   |
| Enable PRACK         | Set the line to support PRACK SIP message  |
| Enable DNS SRV       | Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list  |
| Auto Change Port     | Enable/Disable Auto Change Port  |
| Keep Authentication  | Keep the authentication parameters from previous authentication  |
| Auto TCP             | Using TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes   |
| Enable Feature Sync  | Feature Syncn with server  |
| Enable GRUU          | Support Globally Routable User-Agent URI (GRUU)  |
| BLF Server           | The registered server will receive the subscription package from ordinary application of BLF phone.<br>Please enter the BLF server, if the sever does not support subscription package, the registered server and subscription server will be separated. |
| BLF List Number      | BLF List allows one BLF key to monitor the status of a group. Multiple BLF lists are supported.  |
| SIP Encryption       | Enable SIP encryption such that SIP transmission will be encrypted   |
| SIP Encryption Key   | Set the pass phrase for SIP encryption   |
| RTP Encryption       | Enable RTP encryption such that RTP transmission will be encrypted   |
| RTP Encryption Key   | Set the pass phrase for RTP encryption   |

## b) Basic Settings

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



|   | SIP                                  | Basic Settings                       | Dial Peer   |
|---|--------------------------------------|--------------------------------------|---|
| <ul style="list-style-type: none"> <li>&gt; System</li> <li>&gt; Network</li> <li>&gt; Line</li> <li>&gt; EGS Setting</li> <li>&gt; EGS Access</li> <li>&gt; EGS Logs</li> <li>&gt; Function Key</li> <li>&gt; Alert</li> </ul> | <b>SIP Settings</b>                  |                                      |   |
|   | Local SIP Port                       | <input type="text" value="5060"/>    |   |
|   | Registration Failure Retry Interval  | <input type="text" value="32"/>      | Second(s)   |
|   | Enable Strict UA Match               | <input type="checkbox"/>             |   |
|   | Enable DHCP Option 120               | <input type="checkbox"/>             |   |
|   |                                      | <input type="button" value="Apply"/> |   |
|   | <b>STUN Settings</b>                 |                                      |   |
|   | STUN NAT Traversal                   | FALSE                                |   |
|   | Server Address                       | <input type="text"/>                 |   |
|   | Server Port                          | <input type="text" value="3478"/>    |   |
| Binding Period  | <input type="text" value="50"/>      | Second(s)                            |   |
| SIP Waiting Time  | <input type="text" value="800"/>     | millisecond                          |   |
|   | <input type="button" value="Apply"/> |                                      |   |
| TLS Certification File:   | sips.pem                             | N/A                                  | <input type="button" value="Upload"/> <input type="button" value="Delete"/> |

| Basic Settings                      |  |
|-------------------------------------|--|
| Field Name                          | Explanation  |
| <b>SIP Settings</b>                 |  |
| Local SIP Port                      | Set the local SIP port used to send/receive SIP messages.            |
| Registration Failure Retry Interval | Set the retry interval of SIP REGISTRATION when registration failed. |
| Enable Strict UA Match              | Enable or disable Strict UA Match                                    |
| <b>STUN Settings</b>                |  |
| Server Address                      | STUN Server IP address   |
| Server Port                         | STUN Server Port – Default is 3478.                                  |

|  |   |
|--|---|
| Binding Period   | STUN blinding period – STUN packets are sent at this interval to keep the NAT mapping active. |
| SIP Waiting Time   | Waiting time for SIP. This will vary depending on the network.                                |
| <b>TLS Certification File</b>  |   |
| Upload or delete the TLS certification file used for encrypted SIP transmission.   |   |
| Note: the SIP STUN is used to achieve the SIP penetration of NAT, is the realization of a service, when the equipment configuration of the STUN server IP and port (usually the default is 3478), and select the Use Stun SIP server, the use of NAT equipment to achieve penetration. |   |

## C) Dial Peer

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

| Import Dial peer Table |  |
|------------------------|--|
| Field Name             | Explanation  |
| Select File            | Select an existing dialing rule file. The file type must be a .CSV   |
| Add Dial Peer          |  |
| Number                 | In order to add an outgoing call number, the outgoing call number can be divided into two types: one is the exact match, and after the exact match, if the number is exactly the same as the user dialing the called number, the device will use the IP address of this number mapping or (This is the area code prefix function of the PSTN). If the number matches the N-bit (prefix number length) of the called number, the device uses the IP address or configuration mapped to this number. Make a call. Configuration prefix matching needs to be followed by a prefix number to match the exact match number; the longest support of 30 bits; also supports the use of x format and range of numbers. |

|  |  |
|--|--|
| Destination  | Configure the destination address and, if configured as a point-to-point call, write the peer IP address directly. Can also be set to domain name, by the device DNS server to resolve the specific IP address. If it is not configured, the IP address is 0.0.0.0. This is an optional configuration item |
| Port   | Configure the signaling port of the other party. This is an optional configuration item. The default is 5060   |
| Alias  | Configure aliases, this is an optional item: the replacement number used when the prefix is prefixed, and no alias when configured   |
| <p>Note: aliases are divided into four types and must be combined with the replacement length:</p> <p>1) add: xxx, add xxx before the number. This can help users save dialing length;</p> <p>2) all: xxx, all replaced by xxx; can achieve speed dial, such as user configuration dial-up 1, then by configuring all: number to change the actual call out the number;</p> <p>3) del, delete the number before the n bit, n by the replacement length set;</p> <p>4) rep: xxx, the number n before the number is replaced by xxx, n is set by the replacement length. For example, if the user wants to dial the PSTN (010-62281493) through the floor service provided by the VoIP operator, and the actual call should be 010-62281493, then we can configure the called number 9T, then rep: 010, and then delete the length Set to 1. Then all users call the 9 at the beginning of the phone will be replaced with 010 + number sent. To facilitate the user to call the habit of thinking mode;</p> |  |
| Call Mode  | Configuration selection of different signaling protocols, SIP;   |
| Suffix   | Configure the suffix, this is optional configuration items: that is, after the dial-up number to add this suffix, no configuration shows no suffix;  |
| Deleted Length   | Configure the replacement / delete length, the number entered by the user is replaced / deleted by this length; this is an optional configuration item;  |

## (4) EGS Setting

### a) Features

Features
Audio
Video
MCAST
Action URL
Time/Date

- > System
- > Network
- > Line
- > EGS Setting
- > EGS Access
- > EGS Logs
- > Function Key
- > Alert

### Common Settings

|                            |              |                          |           |                    |
|----------------------------|--------------|--------------------------|-----------|--------------------|
| Switch Mode                | Monostable ▼ | Switch-On Duration       | 5         | (1~600)Second(s)   |
| Enable Card Reader         | Enable ▼     | Card Reader Working Mode | Normal ▼  |                    |
| Limit Talk Duration        | Enable ▼     | Talk Duration            | 120       | (20~600) Second(s) |
| Remote Password            | •••••        |                          |           |                    |
| APP Door Open              | Disable ▼    | Local password           | •••••     |                    |
| Enable Indoor Open         | Enable ▼     | APP Password             | •••••     |                    |
| Description                | 后门131S(5523) |                          |           |                    |
| Address of Open Log Server | 0.0.0.0      |                          |           |                    |
| Door Unlock Indication     | Long Beeps ▼ | Enable Access Table      | Enable ▼  |                    |
|                            |              | Enable Open Log Server   | Disable ▼ |                    |
|                            |              | Port of Open Log Server  | 514       |                    |
|                            |              | Remote Code Check Length | 4 (1~11)  |                    |

---

[Basic Settings >>](#)

---

[Block Out Settings >>](#)

### Basic Settings >>

|                           |                                     |                         |                                     |
|---------------------------|-------------------------------------|-------------------------|-------------------------------------|
| Enable DND                | <input type="checkbox"/>            | Ban Outgoing            | <input type="checkbox"/>            |
| Enable Intercom Mute      | <input checked="" type="checkbox"/> | Enable Intercom Ringing | <input checked="" type="checkbox"/> |
| Enable Auto Dial Out      | <input checked="" type="checkbox"/> | Auto Dial Out Time      | 5 (3~30)Second(s)                   |
| Enable Auto Answer        | Lines and IP Call ▼                 | Auto Answer Timeout     | 0 (0~60)Second(s)                   |
| No Answer Auto Hangup     | <input type="checkbox"/>            | Auto Hangup Timeout     | 30 (1~60)Second(s)                  |
| Dial Fixed Length to Send | <input checked="" type="checkbox"/> | Send length             | 4                                   |
| Dial Number Voice Play    | Disable ▼                           | Voice Play Language     | English ▼                           |
| Enable Delay Start        | <input type="checkbox"/>            | Delay Start Time        | 1 (1~180)Second(s)                  |
| Voice Read IP             | Enable ▼                            | Press "*" to Send       | <input checked="" type="checkbox"/> |

### Block Out Settings >>

Block Out List

▼

| Features               |  |
|------------------------|--|
| Field Name             | Explanation  |
| <b>Common Settings</b> |  |
| Switch 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.<br>Each action might be triggered and changed to the other status. After changed, the status would be kept.<br>Initial Value is Monostable |
| Switch-On Duration     | Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial Value is 5 seconds.   |

|                            |   |
|----------------------------|---|
| Enable Card Reader         | Enable or disable card reader for RFID cards.   |
| Card Reader Working Mode   | Set ID card stats:<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. |
| Limit Talk Duration        | If enabled, calls would be forced ended after talking time is up.   |
| Talk Duration              | The call will be ended automatically when time up. Initial Value is 120 seconds   |
| Remote Password            | Remote door unlocking password. Initial Value is “*”.   |
| Local password             | Local door unlocking password via keypad, the default password length is 4. Initial Value is “6789”.  |
| APP Door Open              | Enable or disable the APP Door Open   |
| APP password               | APP door unlocking password. Initial Value is “*” .   |
| Enable Indoor Open         | Enable or disable to use indoor switch to unlock the door.  |
| Enable Access Table        | Enable Access Table: enter <Access Code> for opening door during calls.<br>Disable Access Table: enter <Remote Password> for opening door during calls.<br>Default Enable.  |
| Description                | Device description displayed on IP scanning tool software. Initial Value is “i31S IP Door Phone”.   |
| Enable Open Log Server     | Enable or disable to connect with log server  |
| Address of Open Log Server | Log server address(IP or domain name)   |
| Port of Open Log Server    | Log server port (0-65535) , Initial Value is 514.   |
| Door Unlock Indication     | Indication tone for door unlocked. There are 3 type of tone: silent/short beeps/long beeps.   |
| Remote Code Check Length   | The remote access code length would be restricted with it. If the input access code length is matched with it, system would check it immediately. Initial Value is 4.   |
| <b>Basic Settings</b>      |   |
| Enable DND                 | DND might be disabled phone for all SIP lines, or line for SIP individually. But the outgoing calls will not be affected  |
| Ban Outgoing               | If enabled, no outgoing calls can be made.  |
| Enable Intercom Mute       | If enabled, mutes incoming calls during an intercom call.   |
| Enable Intercom Ringing    | If enabled, plays intercom ring tone to alert to an intercom call.  |

|   |   |
|---|---|
| Enable Auto Dial Out  | Enable Auto Dial Out  |
| Auto Dial Out Time  | Set Auto Dial Out Time  |
| Enable Auto Answer  | Enable Auto Answer function   |
| Auto Answer Timeout   | Set Auto Answer Timeout   |
| No Answer Auto Hangup   | Enable automatically hang up when no answer   |
| Auto Hangup Timeout   | Configuration in a set time, automatically hang up when no answer                       |
| Dial Fixed Length to Send   | Enable or disable dial fixed length to send.  |
| Send length   | The number will be sent to the server after the specified numbers of digits are dialed. |
| Dial Number Voice Play  | Configuration Open / Close Dial Number Voice Play                                       |
| Voice Play Language   | Set language of the voice prompt  |
| Enable Delay Start  | Enable or disable the start delay   |
| Delay Start Time  | Set start delay time  |
| Voice Read IP   | Enable or disable voice broadcast IP address  |
| Press "*" to Send   | Enable or disable the Press "*" to Send, Initial Value is enable                        |
| <b>Block Out Settings</b>   |   |
| <p>Add or delete blocked numbers – enter the prefix of numbers which should not be dialed by the phone. For example, if 001 is entered, the phone would not dial any number beginning with 001.</p> <p>X and x are wildcards which match single digit. For example, if 4xxx or 4XXX is entered, the phone would not dial any 4 digits numbers beginning with 4. It would dial numbers beginning with 4 which are longer or shorter than 4 digits.</p> |   |

## b) Audio

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



Features
Audio
Video
MCAST
Action URL
Time/Date

- > System
- > Network
- > Line
- > EGS Setting
- > EGS Access
- > EGS Logs
- > Function Key
- > Alert

### Audio Settings

|                         |                          |                    |               |
|-------------------------|--------------------------|--------------------|---------------|
| First Codec             | G.722                    | Second Codec       | G.711A        |
| Third Codec             | G.711U                   | Fourth Codec       | G.729AB       |
| Fifth Codec             | None                     | Sixth Codec        | None          |
| DTMF Payload Type       | 101 (96~127)             | Default Ring Type  | Type 1        |
| Pass Tone               | Default                  | Fail Tone          | Default       |
| G.729AB Payload Length  | 20ms                     | Tone Standard      | United States |
| G.722 Timestamps        | 160/20ms                 | G.723.1 Bit Rate   | 6.3kb/s       |
| Speakerphone Volume     | 5 (1~9)                  | MIC Input Volume   | 5 (1~9)       |
| Broadcast Output Volume | 5 (1~9)                  | Signal Tone Volume | 4 (0~9)       |
| Enable VAD              | <input type="checkbox"/> |                    |               |

---

### Sound Update

Sound Update   (\*.wav)

---

### Sound Delete

Sound Delete

| Audio Setting           |  |
|-------------------------|--|
| Field Name              | Explanation  |
| First Codec             | The first codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB  |
| Second Codec            | The second codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, None   |
| Third Codec             | The third codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, None  |
| Fourth Codec            | The forth codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, None  |
| DTMF Payload Type       | The RTP Payload type that indicates DTMF. Default is 101   |
| Default Ring Type       | Ring Sound – There are 9 standard types and 3 User types.  |
| G.729AB Payload Length  | G.729AB Payload Length – Adjusts from 10 – 60 mSec.  |
| Tone Standard           | Configure tone standard area.  |
| G.722 Timestamps        | Choices are 160/20ms or 320/20ms.  |
| G.723.1 Bit Rate        | Choices are 5.3kb/s or 6.3kb/s.  |
| Speakerphone Volume     | Set the speaker calls the volume level.  |
| MIC Input Volume        | Set the MIC calls the volume level.  |
| Broadcast Output Volume | Set the broadcast the output volume level.   |
| Signal Tone Volume      | Set the audio signal the output volume level.  |
| Enable VAD              | Enable or disable Voice Activity Detection (VAD). If VAD is enabled, G729 Payload length cannot be set greater than 20 mSec. |

## c) Video

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

| Video                |  |
|----------------------|--|
| Field Name           | Explanation  |
| <b>Video Capture</b> |  |
| IRCUt Mode           | Auto: IRCUT switches according to the actual ambient light level of the camera<br>Synchronization: The switching of the IRCUT is determined by the actual brightness of the IR lamp.   |
| Day/Night Mode       | Automatic: automatically switches according to the DNC Threshold and the brightness of the actual environment where the camera is located<br>Day Mode: The camera's video screen is always colored, if there is IR-cut will be synchronized to switch.<br>Night Mode: the camera's video screen is always black and white, if there is IR-cut will be synchronized switch. |
| White Balance        | Automatic: Automatically adjusts according to the actual environment in which the camera is located.<br>Outdoor: installed in the outdoor preferred.<br>Indoor: installed in the room preferred.   |
| Horizon Flip         | The video is flipped horizontally  |
| Anti Flicker         | Enable the option. In a fluorescent environment can eliminate the video horizontal scroll  |
| Vertical Flip        | The video is flipped horizontally  |
| IR Swap              | IR-cut filter switch   |

|                         |  |
|-------------------------|--|
| DNC Threshold           | In the Day / Night mode Auto option, the color switching black and white threshold is set  |
| Backlight Compensation  | In front of a very strong background light can see people or objects clearly   |
| AutoFill Sensitivity    | In the environment changes in light and shade, the higher the sensitivity the faster the video changes                               |
| Fill Light              | Enable or disable Fill Light   |
| <b>Video Encode</b>     |  |
| Encode Format           | Only H.264 encoding format is supported  |
| Resolution              | Main stream: support 720P<br>Sub-stream: you can select CIF (352 * 288), D1 (720 * 576)  |
| Frame Rate              | The larger the value is, the more coherent the video would be got; not recommend adjusted.   |
| Bitrate Control         | CBR: If the code rate (bandwidth) is insufficient, it is preferred.<br>VBR: Image quality is preferred, not recommended.             |
| Quality                 | Video quality adjustment, the better the quality needs to transfer faster  |
| Bit rate                | It is proportional to video file size, not recommend adjusted.   |
| I Frame Interval        | The greater the value is, the worse the video quality would be, otherwise the better video quality would be; not recommend adjusted. |
| Activate                | When you selected it, the stream is enabled, otherwise disabled  |
| <b>RTSP Information</b> |  |
| Main Stream Url         | Access the main address of RTSP  |
| Sub Stream Url          | Access the child address of RTSP   |

## d) MCAST

**MCAST Settings**

Priority:

Enable Page Priority:

| Index/Priority | Name                 | Host:port            |
|----------------|----------------------|----------------------|
| 1              | <input type="text"/> | <input type="text"/> |
| 2              | <input type="text"/> | <input type="text"/> |
| 3              | <input type="text"/> | <input type="text"/> |
| 4              | <input type="text"/> | <input type="text"/> |
| 5              | <input type="text"/> | <input type="text"/> |
| 6              | <input type="text"/> | <input type="text"/> |
| 7              | <input type="text"/> | <input type="text"/> |
| 8              | <input type="text"/> | <input type="text"/> |
| 9              | <input type="text"/> | <input type="text"/> |
| 10             | <input type="text"/> | <input type="text"/> |

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

### MCAST Settings

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

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

- **Priority:**

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

- The options are as follows:

- ✧ 1-10: To definite the priority of the common calls, 1 is the top level while 10 is the lowest
- ✧ Disable: ignore all incoming multicast RTP stream
- ✧ Enable the page priority:

Page priority determines the device how to deal with the new receiving multicast RTP stream when it is in multicast session currently. When Page priority switch is enabled, the device will automatically ignore the low priority multicast RTP stream but receive top-level priority multicast RTP

stream, and keep the current multicast session in state; If it is not enabled, the device will automatically ignore all receiving multicast RTP stream.

- **Web Settings:**

**MCAST Settings**

Priority

Enable Page Priority

| Index/Priority | Name                            | Host:port                                   |
|----------------|---------------------------------|---|
| 1              | <input type="text" value="ss"/> | <input type="text" value="239.1.1.1:1366"/> |
| 2              | <input type="text" value="ee"/> | <input type="text" value="239.1.1.1:1367"/> |

The multicast SS priority is higher than that of EE, which is the highest priority.

Note: when pressing the multicast key for multicast session, both multicast sender and receiver will beep.

### Listener configuration

**MCAST Settings**

Priority

Enable Page Priority

| Index/Priority | Name                                 | Host:port                                   |
|----------------|--------------------------------------|---|
| 1              | <input type="text" value="group 1"/> | <input type="text" value="224.0.0.2:2366"/> |
| 2              | <input type="text" value="group 2"/> | <input type="text" value="224.0.0.2:1366"/> |
| 3              | <input type="text" value="group 3"/> | <input type="text" value="224.0.0.6:3366"/> |
| 4              | <input type="text"/>                 | <input type="text"/>                        |
| 5              | <input type="text"/>                 | <input type="text"/>                        |
| 6              | <input type="text"/>                 | <input type="text"/>                        |
| 7              | <input type="text"/>                 | <input type="text"/>                        |
| 8              | <input type="text"/>                 | <input type="text"/>                        |
| 9              | <input type="text"/>                 | <input type="text"/>                        |
| 10             | <input type="text"/>                 | <input type="text"/>                        |

- **Blue part (name)**

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

- **Purple part (host: port)**

It is a set of addresses and ports to listen, separated by a colon.

- **Pink part (index / priority)**

Multicast is a sign of listening, but also the monitoring multicast priority. The smaller number refers to higher priority.

- **Red part (priority)**

It is the general call, non multicast call priority. The smaller number refers to high priority. The followings will explain how to use this option:

- ✧ The purpose of setting monitoring multicast "Group 1" or "Group 2" or "Group 3" launched a multicast call.
- ✧ All equipment has one or more common non multicast communication.
- ✧ When you set the Priority for the disable, multicast any level will not answer, multicast call is rejected.
- ✧ when you set the Priority to a value, only higher than the priority of multicast can come in, if you set the Priority is 3, group 2 and group 3 for priority level equal to 3 and less than 3 were rejected, 1 priority is 2 higher than ordinary call priority device can answer the multicast message at the same time, keep the hold the other call.

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

Set whether to open more priority is the priority of multicast, multicast is pink part number. Explain how to use:

- ✧ The purpose of setting monitoring multicast "group 1" or "3" set up listening "group of 1" or "3" multicast address multicast call.
- ✧ All equipment has been a path or multi-path multicast phone, such as listening to "multicast information group 2".
- ✧ If multicast is a new "group of 1", because "the priority group 1" is 2, higher than the current call "priority group 2" 3, so multicast call will can come in.
- ✧ If multicast is a new "group of 3", because "the priority group 3" is 4, lower than the current call "priority group 2" 3, "1" will listen to the equipment and maintain the "group of 2".

## Multicast service

- **Send:** when configured ok, our key press shell on the corresponding equipment, equipment directly into the Talking interface, the premise is to ensure no current multicast call and 3-way of the case, the multicast can be established.
- **Lmonitor:** IP port and priority configuration monitoring device, when the call is initiated and incoming multicast, directly into the Talking interface equipment.

## e) Action URL

|  | Features                         | Audio                | Video | MCAST | Action URL | Time/Date |
|--|----------------------------------|----------------------|-------|-------|------------|-----------|
| <ul style="list-style-type: none"> <li>&gt; System</li> <li>&gt; Network</li> <li>&gt; Line</li> <li style="background-color: #f0f0f0;">&gt; EGS Setting</li> <li>&gt; EGS Access</li> <li>&gt; EGS Logs</li> <li>&gt; Function Key</li> <li>&gt; Alert</li> </ul> | <b>Action URL Event Settings</b> |                      |       |       |            |           |
|  | Active URI Limit IP              | <input type="text"/> |       |       |            |           |
|  | Setup Completed                  | <input type="text"/> |       |       |            |           |
|  | Registration Succeeded           | <input type="text"/> |       |       |            |           |
|  | Registration Disabled            | <input type="text"/> |       |       |            |           |
|  | Registration Failed              | <input type="text"/> |       |       |            |           |
|  | Off Hooked                       | <input type="text"/> |       |       |            |           |
|  | On Hooked                        | <input type="text"/> |       |       |            |           |
|  | Incoming Call                    | <input type="text"/> |       |       |            |           |
|  | Outgoing calls                   | <input type="text"/> |       |       |            |           |
|  | Call Established                 | <input type="text"/> |       |       |            |           |
|  | Call Terminated                  | <input type="text"/> |       |       |            |           |
|  | DND Enabled                      | <input type="text"/> |       |       |            |           |
|  | DND Disabled                     | <input type="text"/> |       |       |            |           |
|  | Mute                             | <input type="text"/> |       |       |            |           |
|  | Unmute                           | <input type="text"/> |       |       |            |           |
|  | Missed calls                     | <input type="text"/> |       |       |            |           |
|  | IP Changed                       | <input type="text"/> |       |       |            |           |
| Idle To Busy   | <input type="text"/>             |                      |       |       |            |           |
| Busy To Idle   | <input type="text"/>             |                      |       |       |            |           |
| <input type="button" value="Apply"/>   |                                  |                      |       |       |            |           |

### 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`

## f) Time/Date

|   | Features                             | Audio  | Video | MCAST | Action URL | Time/Date |
|---|--------------------------------------|--|-------|-------|------------|-----------|
| <ul style="list-style-type: none"> <li>&gt; System</li> <li>&gt; Network</li> <li>&gt; Line</li> <li style="background-color: #f0f0f0;">&gt; EGS Setting</li> <li>&gt; EGS Access</li> <li>&gt; EGS Logs</li> </ul> | <b>Network Time Server Settings</b>  |  |       |       |            |           |
|   | Time Synchronized via SNTP           | <input checked="" type="checkbox"/>                            |       |       |            |           |
|   | Time Synchronized via DHCP           | <input type="checkbox"/>                                       |       |       |            |           |
|   | Primary Time Server                  | <input type="text" value="time.nist.gov"/>                     |       |       |            |           |
|   | Secondary Time Server                | <input type="text" value="pool.ntp.org"/>                      |       |       |            |           |
|   | Time zone                            | <input type="text" value="(UTC+8) China,Singapore,Australia"/> |       |       |            |           |
|   | Resync Period                        | <input type="text" value="60"/> (1~5000)Second(s)              |       |       |            |           |
|   | <b>Date Format</b>                   |  |       |       |            |           |
|   | Date Format                          | <input type="text" value="1 JAN MON"/>                         |       |       |            |           |
|   | <input type="button" value="Apply"/> |  |       |       |            |           |

> Line

> EGS Setting

> EGS Access

> EGS Logs

> Function Key

> Alert

### Daylight Saving Time Settings

Location:

DST Set Type:

Fixed Type:

Offset:  Minute

Start:

End:

---

### Manual Time Settings

| Time/Date                            |   |
|--------------------------------------|---|
| Field Name                           | Explanation   |
| <b>Network Time Server Settings</b>  |   |
| 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   |
| <b>Date Format</b>                   |   |
| Date Format                          | Select the time/date display format   |
| <b>Daylight Saving Time Settings</b> |   |
| 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 |
| <b>Manual Time Settings</b>                               |                  |
| The time set by hand, need to disable SNTP service first. |                  |
| <b>Daylight Saving Time Settings</b>                      |                  |

## (5) EGS Access

- > System
- > Network
- > Line
- > EGS Setting
- > EGS Access
- > EGS Logs
- > Function Key
- > Alert

**Import Access Table**

Select File   (accessList.csv)

**Access Table >>**

[Click here to Save Access Table](#)

Total: 0  Page:

| <input type="checkbox"/>   | Index | Name                                | ID | Department | Position    | Location | Number                               | Fwd Number | Access Code | Double Auth | Profile | Type                               | Issuing Date | Card State |
|--|-------|-------------------------------------|----|------------|-------------|----------|--------------------------------------|------------|-------------|-------------|---------|------------------------------------|--------------|------------|
| <b>Add Access Rule</b>   |       |                                     |    |            |             |          |                                      |            |             |             |         |                                    |              |            |
| Name   |       | <input type="text"/>                |    |            | Location    |          | <input type="text"/>                 |            |             | Number      |         | <input type="text"/>               |              |            |
| ID   |       | <input type="text"/>                |    |            | Fwd Number  |          | <input type="text"/>                 |            |             | Access Code |         | <input type="text"/>               |              |            |
| Card State   |       | <input type="text" value="Enable"/> |    |            | Double Auth |          | <input type="text" value="Disable"/> |            |             | Profile     |         | <input type="text" value="None"/>  |              |            |
| Department   |       | <input type="text"/>                |    |            | Position    |          | <input type="text"/>                 |            |             | Type        |         | <input type="text" value="Guest"/> |              |            |
| <input type="button" value="Add"/> <input type="button" value="Modify"/> |       |                                     |    |            |             |          |                                      |            |             |             |         |                                    |              |            |

**Profile Setting**

Profile  Profile Name

| Weekday   | Statue                          | Start Time(00:00-23:59)            | End Time(00:00-23:59)              |
|-----------|---------------------------------|------------------------------------|------------------------------------|
| Sunday    | <input type="text" value="No"/> | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |
| Monday    | <input type="text" value="No"/> | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |
| Tuesday   | <input type="text" value="No"/> | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |
| Wednesday | <input type="text" value="No"/> | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |
| Thursday  | <input type="text" value="No"/> | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |
| Friday    | <input type="text" value="No"/> | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |
| Saturday  | <input type="text" value="No"/> | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |

**Administrator Table >>**

Add Admin Card  Issuer

Total: 0  Page:

| <input type="checkbox"/> | Index | ID | Issuing Date | Type |
|--------------------------|-------|----|--------------|------|
|--------------------------|-------|----|--------------|------|

|                            |                    |
|----------------------------|--------------------|
| <b>EGS Access</b>          |                    |
| <b>Field Name</b>          | <b>Explanation</b> |
| <b>Import Access Table</b> |                    |

Click the <Browse> to choose to import remote access list file (access List.csv) and then clicking <Update> can batch import remote access rule.

## Access Table

According to entrance guard access rules have been added, you can choose single or multiple rules on this list to delete operation.

## Add Access Rule

|                 |  |
|-----------------|--|
| Name(necessary) | User name  |
| Location        | Virtual extension number, used to make position call instead of real number. It might be taken with unit number, or room number.   |
| ID              | RFID card number. You can manually fill in the first 10 digits of the card number or select the existing card number   |
| Number          | User phone number  |
| Card State      | Enable or disable holder's RFID card   |
| Fwd Number      | Call forwarding number when above phone number is unavailable.   |
| Department      | Card holder's department   |
| Access Code     | 1/ When the door phone answers the call from the corresponding <Phone Num> user, then the <Phone Num> user can input the access code via keypad to unlock the door remotely.<br>2/ The user's private password should be input via keypad for local door unlocking. The private password format is <b>Location * Access Code</b> . |
| Position        | Card holder's position   |
| Double Auth     | When the feature is enabled, private password inputting and RFID reading must be matched simultaneously for door unlocking.  |
| Type            | Host: the door phone would answer all call automatically.<br>Guest: the door phone would ring for incoming call, if the auto answer is disabled.   |
| Profile         | It is valid for user access rules (including RFID, access code, etc) within corresponding time section. If NONE is selected, the feature would be taken effect all day.  |

## Profile Setting

|              |   |
|--------------|---|
| Profile      | There are 4 sections for time profile configuration   |
| Profile Name | The name of profile to help administrator to remember the time definition   |
| Status       | If it is yes, the time profile would be taken effect. Other time sections not included in the profiles would not allow users to open door |
| Start Time   | The start time of section   |
| End Time     | The end time of section   |

## Administrator Table

|                |  |
|----------------|--|
| Add Admin Card | You should input the top 10 digits of RFID card numbers. for example, 0004111806, selected the type of admin card , click <add>. |
|----------------|--|

Type: Issuer and revocation

When entrance guard is in normal state, swipe card (issuing card) would make entrance guard into the issuing state, and then you can swipe a new card, which the card would be added into the database; when you swipe the issuing card again after cards added done, entrance guard would return to normal state. Delete card operation is the same with issuing card.

The device can support up to 10 admin cards, 1000 copies of ordinary cards.

Note: in the issuing state, swiping deleted card is invalid.

Shows the ID, Issuing Date and Type of admin card

|            |  |
|------------|--|
| Delete     | Clicking <Delete> would delete the admin card list of the selected ID cards. |
| Delete All | Click <Delete All>, to delete all admin card lists.                          |

## (6) EGS Logs

According to open event log, can record up to 20W open event, after more than cover the old records. [Click here to Save Logs](#) Right click on the links to select save target as the door log can export CSV format.

The screenshot shows the 'Door Open Log' interface. On the left is a navigation menu with 'EGS Logs' highlighted. The main content area displays a table of log entries. At the top of the table area, there are controls for 'Page' (set to 1), 'Prev', 'Next', and 'Delete All', along with a link 'Click here to Save Logs'.

| Door | Result | Time                | Access Name | Access ID  | Type         |
|------|--------|---------------------|-------------|------------|--------------|
| 1    | Fail   | 2017/06/28 14:58:46 |             | 0005340786 | Illegal Card |
| 1    | Fail   | 2017/06/28 14:58:45 |             | 0005340791 | Illegal Card |
| 1    | Fail   | 2017/06/28 14:58:44 |             | 0005340791 | Illegal Card |
| 1    | Fail   | 2017/06/28 14:58:43 |             | 0005322743 | Illegal Card |
| 1    | Fail   | 2017/06/28 14:58:41 |             | 0005322748 | Illegal Card |
| 1    | Fail   | 2017/06/28 14:58:39 |             | 0005322753 | Illegal Card |
| 1    | Fail   | 2017/06/28 14:58:38 |             | 0005323101 | Illegal Card |
| 1    | Fail   | 2017/06/28 14:58:36 |             | 0005323101 | Illegal Card |
| 1    | Fail   | 2017/06/28 14:58:34 |             | 0005323096 | Illegal Card |
| 1    | Fail   | 2017/06/28 14:58:30 |             | 0005380528 | Illegal Card |
| 1    | Fail   | 2017/06/28 14:58:27 |             | 0005380523 | Illegal Card |
| 1    | Fail   | 2017/06/28 14:58:24 |             | 0005380518 | Illegal Card |

| Field Name           | Explanation   |
|----------------------|---|
| <b>Door Open Log</b> |   |
| Result               | Show the results of the open the door ( Succeeded or Failed)  |
| Time                 | The time of opening door.   |
| Access Name          | If the door was opened by swipe card or remote unlocking door, the device would display remote access name. |
| Access ID            | 1. If the opening door method is swiping card, it would display the card number                             |

|      |  |
|------|--|
|      | <p>2. If the opening door way is remote access, it would display the remote extension's number.</p> <p>3. If the opening door way is local access, there is no display information.</p>  |
| Type | <p>Open type: 1. Local, 2. Remote, 3. Brush card (Temporary Card, Valid Card and Illegal Card).</p> <p>Note: there are three kinds of brushing card feedback results.</p> <ol style="list-style-type: none"> <li>1. Temporary Card (only added ) the card number, without adding other rules )</li> <li>2. Valid Card (added access rules)</li> <li>3. Illegal Card (Did not add information)</li> </ol> |

## (7) Function Key

### ➤ Key Event

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

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

## ➤ Hot Key

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

| Key                                  | Type      | Number 1             | Number 2             | Line   | Subtype                                |
|--------------------------------------|-----------|----------------------|----------------------|--------|--|
| DSS Key 1                            | Hot Key ▼ | <input type="text"/> | <input type="text"/> | SIP1 ▼ | Speed Dial ▼<br>Speed Dial<br>Intercom |
| <input type="button" value="Apply"/> |           |                      |                      |        |  |

| Type    | Number  | Line                                | Subtype    | Usage   |
|---------|---|-------------------------------------|------------|---|
| Hot Key | Fill the called party's SIP account or IP address | The SIP account corresponding lines | Speed Dial | Using Speed Dial mode together with <a href="#">Enable Speed Dial Hangup</a> <input type="button" value="Enable"/> , can define whether this call is allowed to be hung up by re-pressing the speed dial key. |
|         |   |                                     | Intercom   | In Intercom mode, if the caller's IP phone supports Intercom feature, the device can automatically answer the Intercom calls  |

## ➤ Multicast

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

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

| Key                                  | Type        | Number 1             | Number 2             | Line   | Subtype  |
|--------------------------------------|-------------|----------------------|----------------------|--------|--|
| DSS Key 1                            | Multicast ▼ | <input type="text"/> | <input type="text"/> | SIP1 ▼ | G.722 ▼<br>G.711A<br>G.711U<br>G.722<br>G.723.1<br>G.726-32<br>G.729AB |
| <input type="button" value="Apply"/> |             |                      |                      |        |  |

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

✧ operation mechanism

You can define the DSS Key configuration with multicast address, port and used codec. The device can configure via WEB to monitor the multicast address and port. When the device make a multicast, all devices monitoring the address can receive the multicast data.

✧ calling configuration

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

## (8) Alert

**Input Settings**

Input Detect  
 Trigger Mode: Low Level Trigger(Close Trigger)  Alert message send to server

**Output Settings**

Output Response  
 Output Level: High Level(NO:closed) Output Duration: 5 ( 1~600 ) s

**Alert Trigger Setting**

Alarm Ring Duration: 5 ( 1~600 ) s  
 Input Trigger: Disable Ring  
 Remote DTMF Trigger: Enable Ring  
 Remote SMS Trigger: Disable Ring  
 Call State Trigger: Talking  
 DTMF Output Last: By Duration  
 DTMF Trigger Code: 1234  
 Trigger Message Format: ALERT=OUT1\_SOS

Apply

### Tamper Alarm Settings

Tamper Alarm

Alarm command: Tamper\_Alarm  
 Reset Alerting Status: Reset  
 Reset command: Tamper\_Reset  
 Ring Type: Default

Apply

### Server Settings

Server Address:  Send message to the server when the alarm is triggered  
 Message: Alarm\_Info:Description=后门i31S(5523);SIP User=5523;Mac=00:a8:23:6a:6d:9e;IP=172.18.2.131;port=Input1

Apply

| Field Name            | Explanation                    |
|-----------------------|--------------------------------|
| <b>Input settings</b> |                                |
| Input Detect          | Enable or disable Input Detect |

|   |  |   |
|---|--|---|
| Trigger Mode  | When choosing the low level trigger (closed trigger), detect the input port 1 (low level) closed trigger.  |   |
|   | When choosing the high level trigger (disconnected trigger), detect the input port 1 (high level) disconnected trigger.  |   |
| Alert message send to server  | Set the Alert message send to server   |   |
| <b>Output Settings</b>  |  |   |
| Output Response   | Enable or disable Output Response  |   |
| Output Level  | When choosing the low level trigger (NO: normally open), when meet the trigger condition, trigger the NO port disconnected.  |   |
|   | When choosing the high level trigger (NO: normally close), when meet the trigger condition, trigger the NO port close.   |   |
| Output Duration   | Changes in port, the duration of. The default is 5 seconds.  |   |
| <b>Alert Trigger Setting</b>  |  |   |
| Alarm Ring Duration   | Set the Alarm Ring Duration. The default is 5 seconds.   |   |
| Trigger Mode: "Input trigger", "Remote DTMF trigger", "Remote SMS trigger", "Call state trigger".<br>Call status triggering: there are four triggering modes of Talking / Talking and Ringing / Ringing / Calling |  |   |
| Input trigger   | When the input port meet to trigger condition, the output port will trigger(The Port level time change, By < Output Duration > control)                                  |   |
| Remote DTMF trigger   | By duration  | Received the terminal equipment to send the DTMF password, if correct, which triggers the corresponding output port (The Port level time change, By < Output Duration > control)  |
|   | By Calling State   | During the call, receive the terminal equipment to send the DTMF password, if correct, which triggers the corresponding output port (The Port level time change, (By call state control, after the end of the call, port to return the default state) |
| Remote SMS trigger  | In the remote device or server to send instructions to ALERT=[instructions], if correct, which triggers the corresponding output port                                    |   |
| Call state trigger  | When the emergency call button to trigger the equipment shell, which triggers the corresponding output port(after the end of the call, port to return the default state) |   |
| Trigger Message Format  | Send instructions on remote devices or servers, ALERT=[set instructions], if correct, trigger the corresponding port output.   |   |
| <b>Tamper Alarm Settings</b>  |  |   |
| Tamper Alarm  | When the selection is enabled, the tamper detection enabled  |   |

|                       |   |
|-----------------------|---|
| Alarm command         | When detected someone tampering the equipment, will be sent alarm to the corresponding server |
| Reset command         | When the equipment receives the command of reset from server, the equipment will stop alarm   |
| Reset Alerting Status | Directly stop the alarm from equipment in the Webpage   |
| Ring Type             | Set the Ring Type   |



## V Appendix

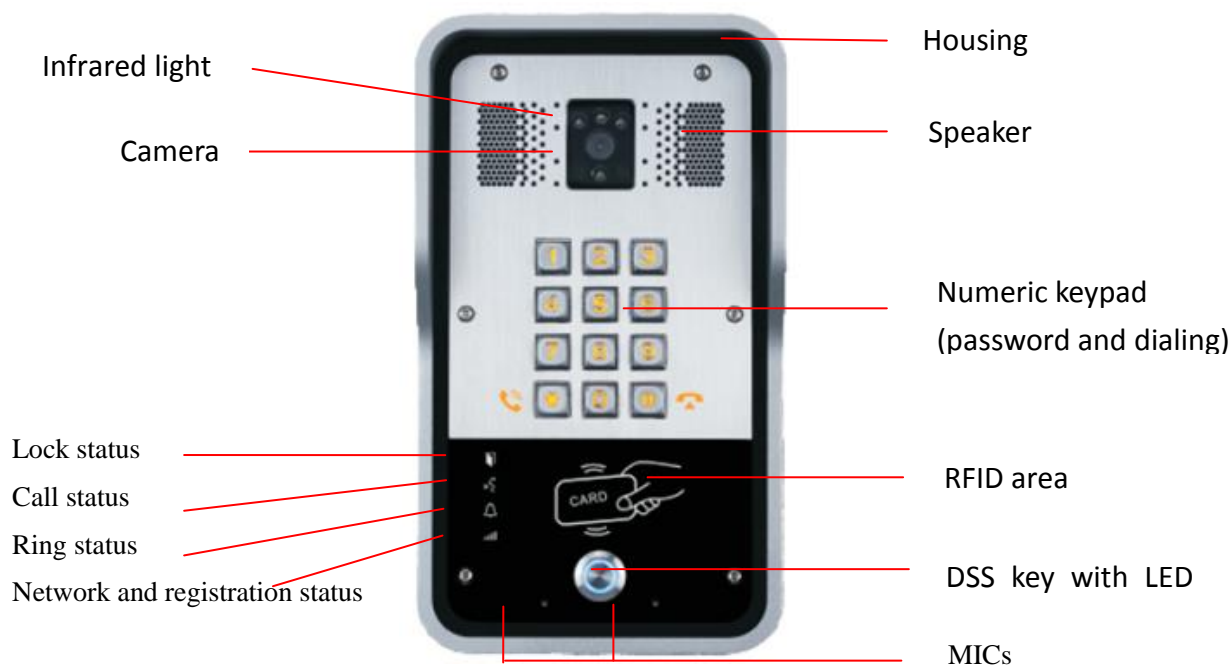
### 1. Technical parameters

|                               |                                 |   |
|-------------------------------|---------------------------------|---|
| <b>Communication protocol</b> |                                 | SIP 2.0(RFC-3261)   |
| <b>Main chipset</b>           |                                 | Broadcom  |
| <b>Keys</b>                   | <b>DSS Key</b>                  | 1 (Stainless steel)   |
|                               | <b>Numeric keyboard</b>         | Support   |
| <b>Audio</b>                  | <b>MIC</b>                      | 1   |
|                               | <b>Speaker</b>                  | 3W/4Ω   |
|                               | <b>Volume control</b>           | Adjustable  |
|                               | <b>Full duplex speakerphone</b> | Support (AEC)   |
| <b>Speech flow</b>            | <b>Protocols</b>                | RTP   |
|                               | <b>Decoding</b>                 | G.729、 G.723、 G.711、 G.722、 G.726                           |
| <b>Ports</b>                  | <b>Active Switched Output</b>   | 12V/650mA DC  |
|                               | <b>WAN</b>                      | 10/100BASE-TX s Auto-MDIX, RJ-45                            |
| <b>Camera</b>                 |                                 | 1/3 "color CMOS, 1 megapixel, wide angle                    |
| <b>RFID/IC card reader</b>    |                                 | EM4100 (125Khz)<br>MIFARE One(13.56Mhz)                     |
| <b>Power supply mode</b>      |                                 | 12V / 1A DC or PoE  |
| <b>PoE</b>                    |                                 | PoE 802.3af (Class 3 - 6.49~12.95W)                         |
| <b>Cables</b>                 |                                 | CAT5 or better  |
| <b>Shell Material</b>         |                                 | Cast aluminium panel, Cast aluminium back shell             |
| <b>Working temperature</b>    |                                 | -40°C to 70°C   |
| <b>Working humidity</b>       |                                 | 10% - 95%   |
| <b>Storage temperature</b>    |                                 | -40°C to 70°C   |
| <b>Installation way</b>       |                                 | Wall-mounting or Flush-mounting                             |
| <b>Dimension</b>              |                                 | Wall-mounting: 223*130*74mm<br>Flush-mounting: 270*150*61mm |
| <b>Package size</b>           |                                 | 310x175x115mm   |
| <b>Equipment weight</b>       |                                 | 1500g   |
| <b>Gross weight</b>           |                                 | 1800g   |

## 2. Basic functions

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

## 3. Schematic diagram



## VI Other instructions

### 1. Open door modes

#### ● Local

##### 1) Local Password

- ✧ Set <Local Password> (the default is "6789") via DOOR PHONE\DOOR PHONE as above.
- ✧ Use the device's keypad to input password and "#" key, then the door will be unlocked.

##### 2) Private access code

- ✧ Set <Add Access Rule\Access Code> and enable local authentication.
- ✧ Use the device's keypad to input access code and "#" key, then the door will be unlocked.

#### ● Remote

##### 1) Visitors call to owner

- ✧ Visitors call to owner via position speed dial or phone number. (When set the speed dial key, can press it to call direct.)
- ✧ The owner answers the call, with pressing the "\*" key to unlock the door for visitors.

##### 2) Owner calls to visitors

- ✧ Owner calls to visitors via SIP phone.
- ✧ SIP door phone answers the call automatically.
- ✧ Owner use keypad to input corresponding <Access codes> to unlock the door.

#### ● Slot cards

- ✧ Use pre assigned RFID cards to unlock the door, by touching RFID area of device.

#### ● Indoor switch

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

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

### 2. Management of card

#### ● Add Administrator

There are 2 types of Administrator cards: issuer used for adding cards, revocation used for deleting cards.

### 1) Add<Issuer admin card >

Input a card's ID, selected <Issuer> in the types and Clicked <Add>, you can add Issuer admin card.

#### Add Administrator>>

ID

Type

### 2) Add<Revocation admin card>

Input a card's ID, selected <Revocation> in the types and Clicked <Add>, you can add Revocation admin card.

#### Add Administrator>>

ID

Type

### 3) Administrator Table

#### Administrator Table>>

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

### ● Delete Administrator

Select the admin card of need to delete, click <Delete>.

#### Delete Administrator>>

### ● Add user cards

**Method 1:** used to add cards for starters typically

1) In web page < EGS Setting\Card Reader Working Mode> option, select <Card Issuing> function.

Card Reader Working Mode

Talk Duration  0) Second(s)

Local password

2) Click <Apply>, Card Reader would be entered the issuing status.

3) Use new card to touch card reader induction area, and then you might hear the confirmed indication tone from the device. Repeat step 3 to add more cards.

4) In web page <EGS Setting\Card Reader Working Mode > option, select <normal> function.

Card Reader Working Mode

Talk Duration  0) Second(s)

Local password

- 5) Click <Apply>, Card Reader would be back to the Normal status.
- 6) The issuing records can be found from the Access table list.

**Access Table >>** [Click here to Save Access Table](#)

| Total: 2                 |       | Prev     | Page: 1    | Next       |          |          | Delete | Delete All |             |             |         |       |                     |            |
|--------------------------|-------|----------|------------|------------|----------|----------|--------|------------|-------------|-------------|---------|-------|---------------------|------------|
| <input type="checkbox"/> | Index | Name     | ID         | Department | Position | Location | Number | Fwd Number | Access Code | Double Auth | Profile | Type  | Issuing Date        | Card State |
| <input type="checkbox"/> | 1     | joe      | 0000127423 |            |          |          |        |            |             | Disable     | None    | Guest | 2017/06/29 17:31:23 | Enable     |
| <input type="checkbox"/> | 2     | zhangsan | 0123031310 |            |          |          |        |            |             | Disable     | None    | Guest | 2017/06/29 17:30:58 | Enable     |

**Method 2:** used to add cards for professionals

- 1) Use <Issuer admin card> to touch card reader induction area, and it would be entered issuing card status.
- 2) Use new card to touch card reader induction area, and you might hear the confirmed indication tone from the device. Repeat step 2 to add more cards.
- 3) Use <Issuer admin card> to touch card reader induction area again, it would be back to normal working status.

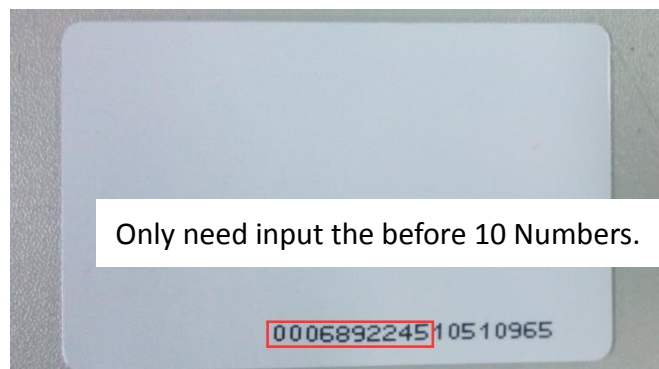
**Methods 3:** use to add few cards

- 1) Input cards number in <EGS Setting\Add Access Rule\ID> page, and then click <Add>.

**Add Access Rule**

|            |                      |   |             |                      |     |
|------------|----------------------|---|-------------|----------------------|-----|
| Name       | <input type="text"/> | ★ | Location    | <input type="text"/> | ?   |
| <b>ID</b>  | <input type="text"/> | ▼ | Number      | <input type="text"/> |     |
| Card State | Enable               | ▼ | Fwd Number  | <input type="text"/> |     |
| Department | <input type="text"/> |   | Access Code | <input type="text"/> | ?   |
| Position   | <input type="text"/> |   | Double Auth | Disable              | ▼ ? |
| Type       | Guest                | ▼ | Profile     | None                 | ▼   |

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



● **Delete user cards**

**Method 1:** used to batch delete cards for starters.

1) In web page <EGS Setting\Card Reader Working Mode> option, select <Card revoking>.

|                          |                 |              |
|--------------------------|-----------------|--------------|
| Card Reader Working Mode | Card Revoking ▾ |              |
| Talk Duration            | Normal          | 0) Second(s) |
| Local password           | Card Issuing    |              |
|                          | Card Revoking   |              |

2) Click <Apply>, Card Reader would be entered the revoking status.

3) Use card to touch card reader induction area, and you might hear the card reader confirmed indication tone. Repeat step 3 to delete more cards.

4) In web page <EGS Setting\Card Reader Working Mode >option, select <normal>.

|                          |               |              |
|--------------------------|---------------|--------------|
| Card Reader Working Mode | Normal ▾      |              |
| Talk Duration            | Normal        | 0) Second(s) |
| Local password           | Card Issuing  |              |
|                          | Card Revoking |              |

5) Click <Apply>, Card Reader would be back to the Normal status.

**Method 2:** used to batch add cards for intermediates.

1) Use < Revocation admin card> to touch card reader induction area, and it would be entered revoking card status.

2) Use the cards you want to delete from system, to touch card reader induction area, and you might hear the card reader confirmed indication tone. Repeat step 2 to delete cards.

3) Use <Revocation admin card> to touch card reader induction area, and it would be back to card read only status.

**Method 3:** use to batch delete cards or delete few cards.

1) In web page<EGS Access\Access Table>select the card ID and then click <Delete>.

**Note:** If you click <Delete All>, system will delete all the ID cards.

**Access Table >>**

[Click here to Save Access Table](#)

| Total: 2                            | Prev  | Page: 1 ▾ | Next       |            | Delete   | Delete All |        |            |             |             |         |       |                     |            |
|-------------------------------------|-------|-----------|------------|------------|----------|------------|--------|------------|-------------|-------------|---------|-------|---------------------|------------|
| <input type="checkbox"/>            | Index | Name      | ID         | Department | Position | Location   | Number | Fwd Number | Access Code | Double Auth | Profile | Type  | Issuing Date        | Card State |
| <input checked="" type="checkbox"/> | 1     | joe       | 0000127423 |            |          |            |        |            |             | Disable     | None    | Guest | 2017/06/29 17:31:23 | Enable     |
| <input type="checkbox"/>            | 2     | zhangsan  | 0123031310 |            |          |            |        |            |             | Disable     | None    | Guest | 2017/06/29 17:30:58 | Enable     |