

i23

IP Voice Access User Manual



Wall mounted



In-wall

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

| | | |
|-----------|-------------------------------------------------------|-----------|
| A. | PRODUCT INTRODUCTION | 5 |
| 1. | APPEARANCE OF THE PRODUCT | 5 |
| 2. | DESCRIPTION | 6 |
| B. | START USING | 7 |
| 1. | CONFIRM THE CONNECTION | 7 |
| 1) | Power port | 7 |
| 2) | Electric-lock and indoor switch port | 7 |
| 3) | Driving mode of electric-lock(Default in active mode) | 7 |
| 4) | Wiring instructions | 8 |
| 2. | QUICK SETTING | 9 |
| C. | BASIC OPERATION | 10 |
| 1. | ANSWER A CALL | 10 |
| 2. | CALL | 10 |
| 3. | END CALL | 10 |
| 4. | CALL RECORD | 10 |
| 5. | OPEN THE DOOR OPERATION | 10 |
| D. | PAGE SETTINGS | 11 |
| 1. | BROWSER CONFIGURATION | 11 |
| 2. | PASSWORD CONFIGURATION | 11 |
| 3. | CONFIGURATION VIA WEB | 12 |
| (1) | BASIC | 12 |
| a) | STATUS | 12 |
| b) | WIZARD | 13 |
| c) | LANGUAGE | 14 |
| d) | TIME&DATE | 14 |
| (2) | NETWORK | 16 |
| a) | WAN | 16 |
| b) | LAN | 18 |
| c) | QoS&VLAN | 18 |
| d) | WEB FILTER | 20 |
| e) | FIREWALL | 21 |
| f) | VPN | 22 |
| g) | SECURITY | 24 |
| (3) | VOIP | 25 |

| | | |
|-----|---------------------------|----|
| a) | SIP | 25 |
| b) | STUN..... | 28 |
| (4) | INTERCOM | 30 |
| a) | AUDIO..... | 30 |
| b) | FEATURE | 31 |
| c) | MCAST | 33 |
| d) | Action URL | 36 |
| (5) | DOOR PHONE..... | 36 |
| a) | FUNCTION KEY | 36 |
| b) | DOOR PHONE..... | 39 |
| c) | DOOR CARD | 41 |
| d) | DOOR ACCESS | 43 |
| e) | DOOR LOG | 45 |
| (6) | MAINTENANCE..... | 46 |
| a) | AUTO PROVISION | 46 |
| b) | SYSLOG | 48 |
| c) | CONFIG | 49 |
| d) | UPDATE..... | 50 |
| e) | ACCESS..... | 51 |
| f) | REBOOT | 51 |
| (7) | LOGOUT | 52 |
| E. | APPENDIX | 53 |
| 1. | TECHNICAL PARAMETERS..... | 53 |
| 2. | BASIC FUNCTIONS | 54 |
| 3. | SCHEMATIC DIAGRAM | 54 |
| F. | OTHER INSTRUCTIONS..... | 55 |
| 1. | OPEN DOOR MODES | 55 |
| 2. | MANAGEMENT OF CARD | 56 |

A. Product introduction

i23 voice access is a full digital network door phone, with its core part adopting 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.

i23 voice access supports entrance guard control, voice intercom, ID card and keypad remote to open the door.

1. Appearance of the product










Wall mounted



In-wall

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

B. 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 port


Power supply ways: 12v/DC or POE.

| CN1 | |
|-----------|-----|
| 1 | 2 |
| +12V | GND |
| 12V 1A/DC | |



2) Electric-lock and indoor switch port

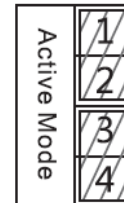
| J2 | | | | |
|---------------|-------|----------------------|-----|----|
| 1 | 2 | 3 | 4 | 5 |
| S_IN | S_OUT | NC | COM | NO |
| Indoor switch | | Electric-lock switch | | |



3) Driving mode of electric-lock(Default in active mode)



Jumper in passive mode



Jumper in active mode

【Note】 When the device is in active mode, it can drive 12V/700mA 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).

4) Wiring instructions

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

| Driving Mode | | Electric lock | | Jumper port | Connections |
|--------------|---------|---------------|----|-------------|----------------------------------------------------------------------------------------------------|
| Active | Passive | NO | NC | | |
| √ | | √ | | | <p>Indoor switch No electricity when open the door</p> |
| √ | | | √ | | <p>Indoor switch When the power to open the door</p> |
| | √ | √ | | | <p>Indoor switch Electric lock (normally open type) No electricity when open the door</p> |
| | √ | | √ | | <p>Indoor switch Electric lock (normally closed type) When the power to open the door</p> |
| | √ | √ | | | <p>Indoor switch Electric lock (normally open) Without power to open the door</p> |

2. Quick Setting

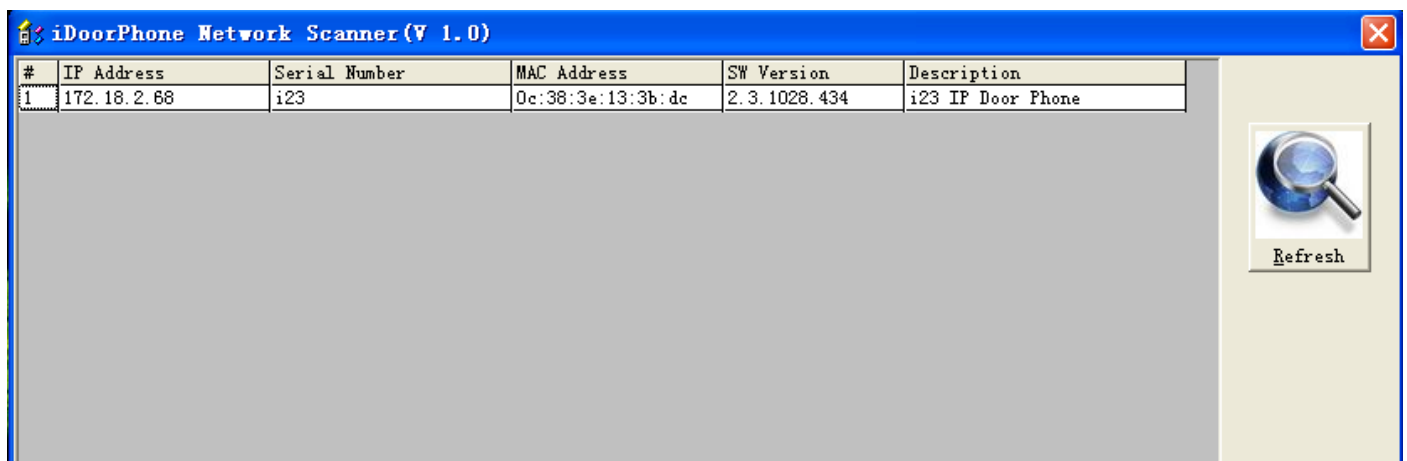
The product provides a complete function and parameter setting. Users may need to have the network and SIP protocol knowledge to understand the meaning represented by all parameters. In order to let equipment users enjoy the high quality of voice service and low cost advantage brought by the device immediately, 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.

Note: when power on, 30s waiting is needed for device running.

- Log on to the WEB device configuration.
- In a SIP page configuration service account, user name, parameters that are required for server address register.
- You can set DSS key in the Webpage(functions key settings -> function key).
- You can set function parameters in the Webpage (Intercom-> feature).



C. 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. Call record

The device provides 900 call records. When the storage space is exhausted, it will cover the first call records. When the device is powered down or reboot, call records will be removed.

You can view the call records in the web page (Door phone/Door log)

5. 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://host/cgi-bin/ConfigManApp.com?key=F_LOCK&code=openCode", "openCode" is the remote control code to open the door.

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.

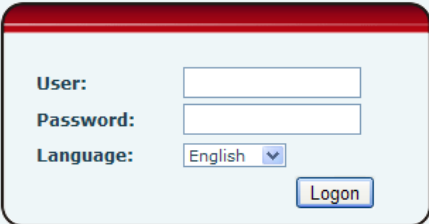
When door has been opened, the device will play sirens sound to prompt.

D. Page settings

1. Browser configuration

When the device and your computer are successfully connected to the network, enter the IP address of the device on the browser as `http://xxx.xxx.xxx.xxx/` 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 elements:

- 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.

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

2. Password Configuration

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

- Default user with general level:
 - ◆ Username: guest
 - ◆ Password: guest
- Default user with root level:
 - ◆ Username: admin
 - ◆ Password: admin

3. Configuration via WEB

(1) BASIC

a) STATUS

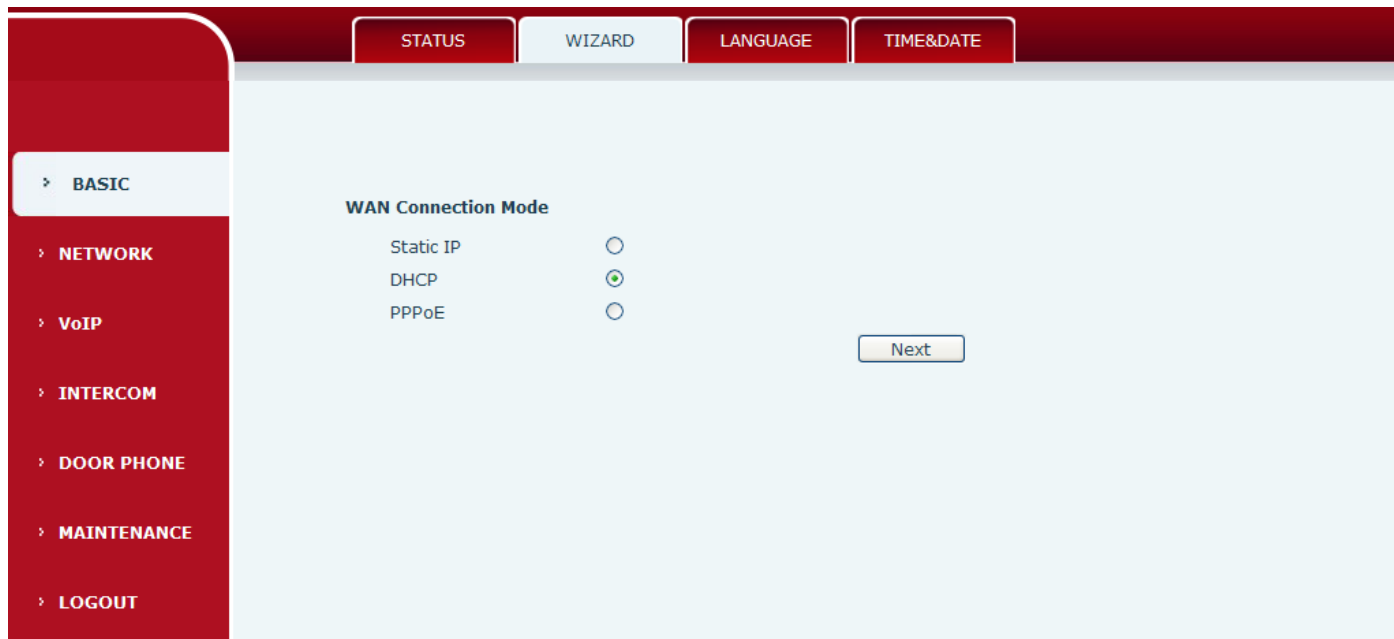
The screenshot shows the Fanvil web interface. On the left is a red sidebar with a menu containing: > BASIC, > NETWORK, > VoIP, > INTERCOM, > DOOR PHONE, > MAINTENANCE, and > LOGOUT. The main content area has a top navigation bar with tabs: STATUS, WIZARD, LANGUAGE, and TIME&DATE. The STATUS tab is selected. Below the tabs, there are two sections: 'Network' and 'Accounts'. The 'Network' section is divided into 'WAN' and 'LAN' columns. The 'Accounts' section lists two SIP lines.

| Network | |
|-----------------|-------------------|
| WAN | LAN |
| Connection Mode | DHCP |
| MAC Address | 0c:38:3e:13:3b:dc |
| IP Address | 172.18.2.127 |
| IP Gateway | 172.18.1.1 |
| IP Address | 192.168.10.1 |
| DHCP Service | Enabled |
| Bridge Mode | Disabled |

| Accounts | |
|------------|------------------|
| SIP Line 1 | @:5060 Unapplied |
| SIP Line 2 | @:5060 Unapplied |

| Status | |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Field Name | Explanation |
| Network | Shows the configuration information for WAN and LAN port, including connection mode of WAN port (Static, DHCP, PPPoE), MAC address, IP address of WAN port and LAN port, DHCP server, status for LAN port (ENABLED or DISABLED). |
| Accounts | Shows the phone numbers and registration status for the 2 SIP LINES. |

b) WIZARD



| Wizard | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Field Name | Explanation |
| Select the appropriate network mode. The equipment supports three network modes: | |
| Static IP mode | The parameters of a Static IP connection must be provided by your ISP. |
| DHCP mode | In this mode, network parameter information will be obtained automatically from a DHCP server. |
| PPPoE mode | In this mode, you must enter your ADSL account and password. |
| Static IP mode is selected; Click <Next> to go to Quick SIP Settings, Click Back to return to the Wizard screen. | |
| After selecting DHCP and clicking NEXT, the Quick SIP Settings screen will appear. Click Back to return to the Wizard screen. Click <Next> to go to the Summary screen. | |
| If PPPoE is selected, this screen will appear. Enter the information provided by the ISP. Click <Next> to go to Quick SIP Setting. Click Back to return to the Wizard screen. | |

c) LANGUAGE

Set the current language.

STATUS WIZARD **LANGUAGE** TIME&DATE

> BASIC
> NETWORK
> VoIP

Language

Language Selection English

Apply

d) TIME&DATE

Set the time zone and SNTP (Simple Network Time Protocol) server on this page. Daylight Saving Time configuration and Manual Time and Date entry can also be done in this page.

STATUS WIZARD LANGUAGE **TIME&DATE**

System Current Time

2015-08-19 11:00:26

Simple Network Time Protocol (SNTP) Settings

Enable SNTP

Enable DHCP Time

Primary Server 0.pool.ntp.org

Secondary Server time.nist.gov

Timezone (GMT+08:00)Beijing,Chongqing,Hong Kong,Urumqi

Resync Period 60 second(s)

12-Hour Clock

Apply

Daylight Saving Time Settings

Enable

Offset 60 minutes(s)

Month March Week 5 Day Sunday

Hour 2 Minute 0

Apply

Manual Time Settings

Year

Month

Day

Hour

Minute

Apply

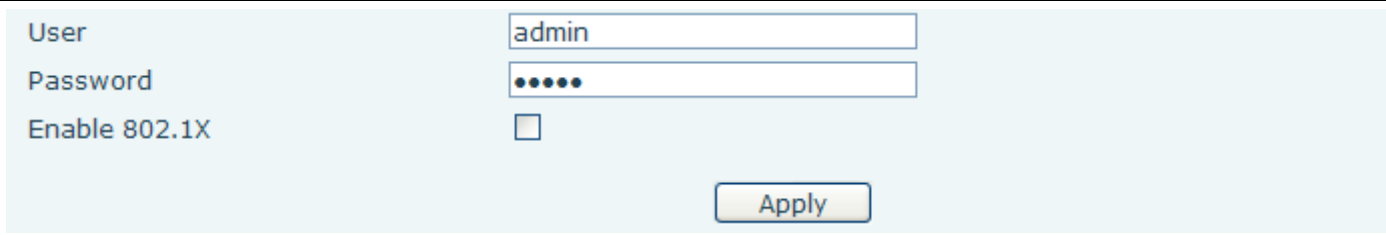
> BASIC
> NETWORK
> VoIP
> INTERCOM
> DOOR PHONE
> MAINTENANCE
> LOGOUT

| Time&Date | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Field Name | Explanation |
| System Current Time | |
| Display the current time | |
| Simple Network Time Protocol (SNTP) Settings | |
| Enable SNTP | Enable or Disable SNTP |
| Enable DHCP Time | If this is enabled, equipment will synchronize time with DHCP server |
| Primary Server | IP address of Primary SNTP Server |
| Secondary Server | IP address of Secondary SNTP Server |
| Time zone | Local Time Zone |
| Resync Period | Time between resync to SNTP server. Default is 60 seconds. |
| 12-Hour Clock | If checked, clock is 12 hour mode. If unchecked, 24 hour mode. Default is 24 hour mode. |
| Daylight Saving Time Settings | |
| Enable | Enable daylight saving time |
| Offset | DST offset. Default is 60 minutes |
| Month | Start and end month for DST |
| Week | Start and end week for DST |
| Day | Start and end day for DST |
| Hour | Start and end hour for DST |
| Minute | Start and end minute for DST |
| Manual Time Settings | |
| Enter the values for the current year, month, day, hour and minute. All values are required. Be sure to disable SNTP service before entering manual time and date. | |

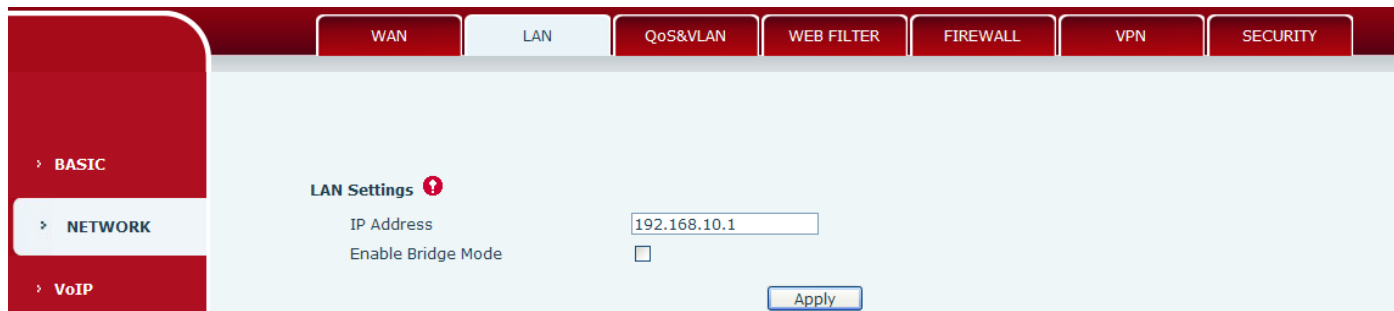
(2) NETWORK

a) WAN

| Field Name | Explanation |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| WAN Status | |
| Active IP address | The current IP address of the equipment |
| Current subnet mask | The current Subnet Mask |
| Current IP gateway | The current Gateway IP address |
| MAC address | The MAC address of the equipment |
| MAC Timestamp | Get the MAC address of time. |
| WAN Settings | |
| Select the appropriate network mode. The equipment supports three network modes: | |
| Static | Network parameters must be entered manually and will not change. All parameters are provided by the ISP. |

| Field Name | Explanation |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. | |
| 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. | |
| 802.1X Settings | |
|  | |
| User | 802.1X user account |
| Password | 802.1X password |
| Enable 802.1X | Enable or Disable 802.1X |
| Service port Settings | |
| Web Server Type | Specify Web Server Type – HTTP or HTTPS |
| HTTP Port | Port for web browser access. Default value is 80. To enhance security, change this from the default. Setting this port to 0 will disable HTTP access. Example: The IP address is 192.168.1.70 and the port value is 8090, the accessing address is http://192.168.1.70:8090. |
| HTTPS Port | Port for HTTPS access. Before using HTTPS, an HTTPS authentication certification must be downloaded into the equipment. Default value is 443. To enhance security, change this from the default. |
| Telnet Port | Port for Telnet access. The default is 23. |
| RTP Port Range Start | Set the beginning value for RTP Ports. Ports are dynamically allocated. |
| RTP Port Quantity | Set the maximum quantity of RTP Ports. The default is 200. |
| Note: <ol style="list-style-type: none"> Any changes made on this page require a reboot to become active. It is suggested that changes to HTTP Port and Telnet ports be values greater than 1024. Values less than 1024 are reserved. If the HTTP port is set to 0, HTTP service will be disabled. | |

b) LAN

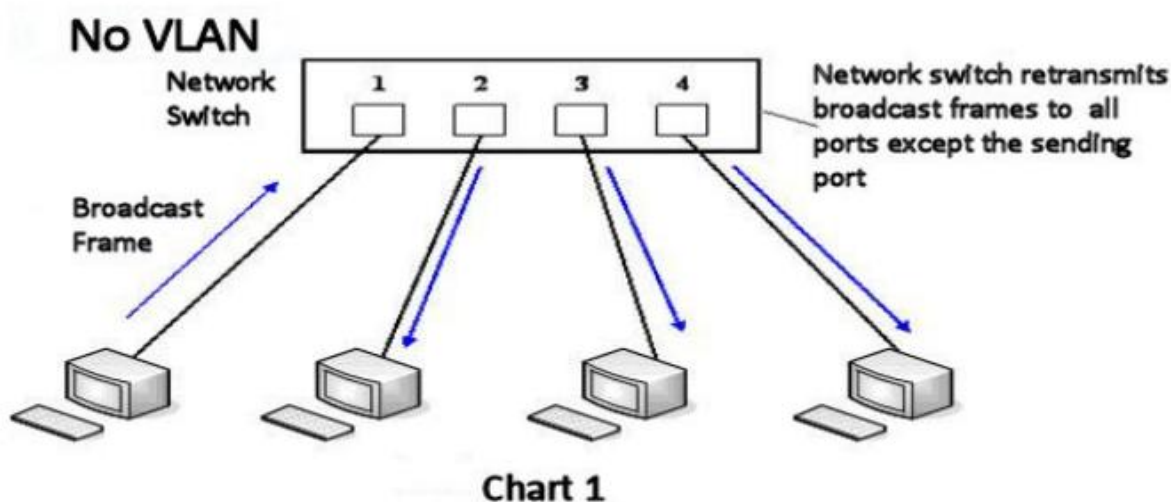


| LAN | |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Field Name | Explanation |
| IP Address | LAN static IP |
| Enable bridge mode | If Bridge Mode is activated, the equipment will not provide an IP address for the LAN port. Instead, the LAN and WAN will be part of the same network. If this is activated, clicking Apply, will cause the equipment reboot. |
| Note: If bridge mode is chosen, static LAN configuration will be disabled automatically. | |

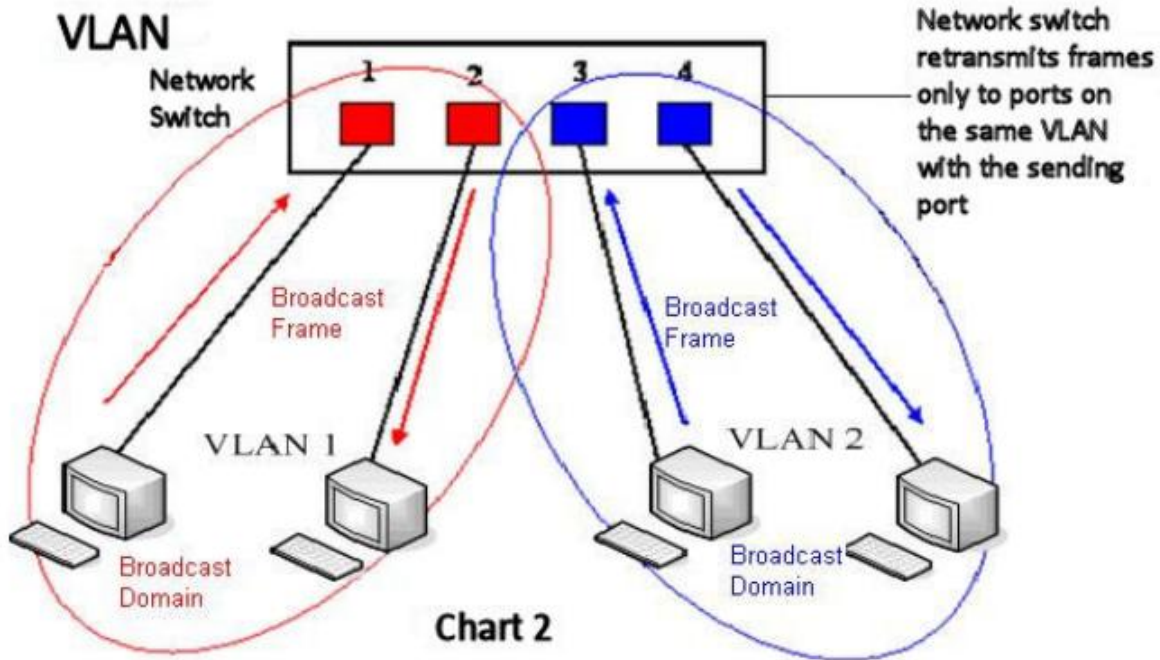
c) QoS&VLAN

The equipment supports 802.1Q/P protocol and DiffServ configuration. Use of a Virtual LAN (VLAN) allows voice and data traffic to be separated.

- Chart 1 shows a network switch with no VLAN. Any broadcast frames will be transmitted to all other ports. For example, frames broadcast from Port 1 will be sent to Ports 2, 3, and 4.



- Chart 2 shows an example with two VLANs indicated by red and blue. In this example, frames broadcast from Port 1 will only go to Port 2 since Ports 3 and 4 are in a different VLAN. VLANs can be used to divide a network by restricting the transmission of broadcast frames.



Note: In practice, VLANs are distinguished by the use of VLAN IDs.

| WAN | LAN | QoS&VLAN | WEB FILTER | FIREWALL | VPN | SECURITY |
|-----|-----|----------|------------|----------|-----|----------|
|-----|-----|----------|------------|----------|-----|----------|

- BASIC
- NETWORK
- VoIP
- INTERCOM
- DOOR PHONE
- MAINTENANCE
- LOGOUT

Link Layer Discovery Protocol (LLDP) Settings

Enable LLDP ! Packet Interval(1~3600) second(s)

Enable Learning Function

Quality of Service (QoS) Settings

Enable DSCP SIP DSCP (0~63)

Audio RTP DSCP (0~63)

WAN Port VLAN Settings

Enable WAN Port VLAN WAN Port VLAN ID (0~4095)

SIP 802.1P Priority (0~7) Audio 802.1P Priority (0~7)

LAN Port VLAN Settings

LAN Port VLAN Mode LAN Port VLAN ID (0~4095)

| QoS&VLAN | |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Field Name | Explanation |
| Link Layer Discovery Protocol (LLDP) Settings | |
| Enable LLDP | Enable or Disable Link Layer Discovery Protocol (LLDP) |
| Enable Learning Function | Enables the telephone to synchronize its VLAN data with the Network Switch. The telephone will automatically synchronize DSCP, 802.1p, and VLAN ID values even if these values differ from those provided by the LLDP server. |
| Packet Interval | The time interval for sending LLDP Packets |
| Quality of Service (QoS) Settings | |
| Enable DSCP | Enable or Disable Differentiated Services Code Point (DSCP) |
| Audio RTP DSCP | Specify the value of the Audio DSCP in decimal |
| SIP DSCP | Specify the value of the SIP DSCP in decimal |
| WAN Port VLAN Settings | |
| Enable WAN Port VLAN | Enable or Disable WAN Port VLAN |
| WAN Port VLAN ID | Specify the value of the WAN Port VLAN ID. Range is 0-4095 |
| SIP 802.1P Priority | Specify the value of the signal 802.1p priority. Range is 0-7 |
| Audio 802.1P Priority | Specify the value of the voice 802.1p priority. Range is 0-7 |
| LAN Port VLAN Settings | |
| LAN Port VLAN Mode | Follow WAN: LAN Port ID is same as WAN ID. Disable: Disable Port VALN Enable: Specify a VLAN ID for the LAN port which is different from WAN ID |
| LAN Port VLAN ID | Used when the VLAN ID is different from WAN ID. Range is 0-4095 |

d) WEB FILTER

The screenshot displays the 'WEB FILTER' configuration page in the Fanvil interface. The top navigation bar includes tabs for WAN, LAN, QoS&VLAN, WEB FILTER (active), FIREWALL, VPN, and SECURITY. The left sidebar shows a menu with options: BASIC, NETWORK (active), VoIP, INTERCOM, and DOOR PHONE. The main content area is titled 'Web Filter Table' and contains a table with columns for Start IP Address, End IP Address, and Option. Below the table is a 'Web Filter Table Settings' section with input fields for Start IP Address and End IP Address, and an 'Add' button. At the bottom is a 'Web Filter Setting' section with a checkbox for 'Enable Web Filter' and an 'Apply' button.

| |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web filter |
| The Web filter is used to limit access to the equipment. When the web filter is enabled, only the IP addresses between the start IP and end IP can access the equipment. |
| Web Filter Table |
| Web page access allows display the IP network list. |
| Web Filter Table Settings |
| Beginning and Ending IP Address for MMI Filter, Click add this filter range to the Web Filter Table. |
| Web Filter Setting |
| Select to enable MMI Filter. Click <apply> Make filter settings effective. |
| Note: Be sure that the filter range includes the IP address of the configuration computer. |

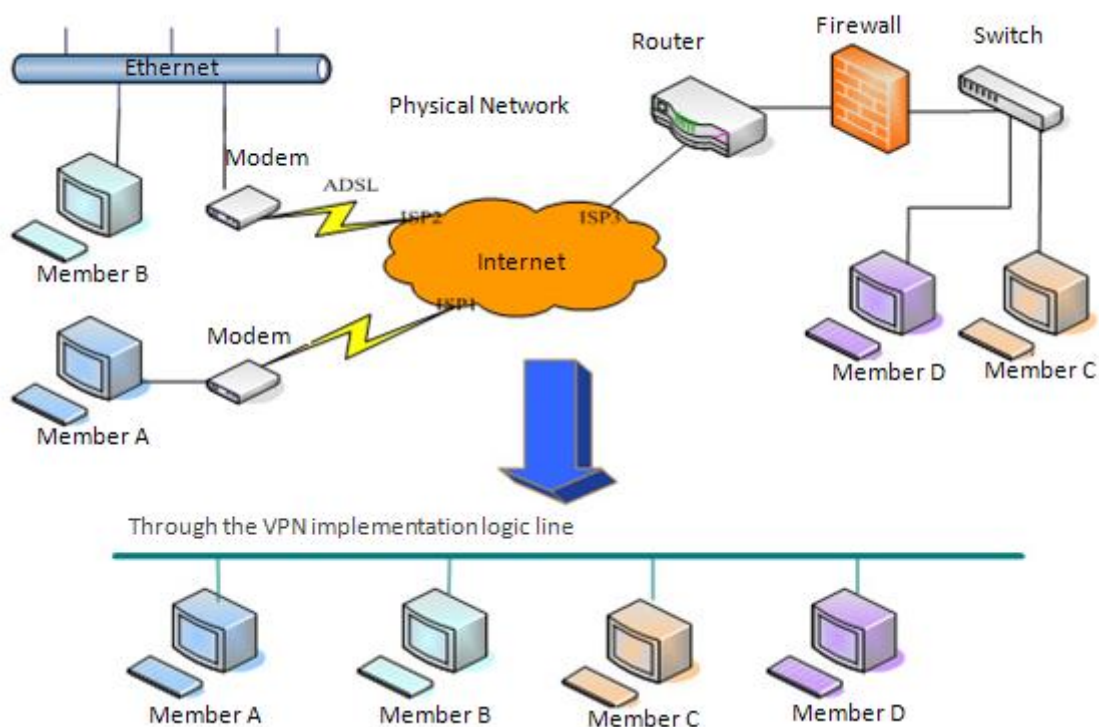
e) FIREWALL

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| Firewall | |
| Firewall rules can be used to prevent unauthorized Internet users from accessing private networks connected to this phone (input rule), or prevent unauthorized devices connected to this phone from accessing the Internet (output rule). Each rule type supports a maximum of 10 items. | |
| Firewall Rules Settings | |
| Enable Input Rules | Enable rules limiting access from the Internet. |
| Enable Output Rules | Enable rules limiting access to the Internet. |

| Field Name | Explanation |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Firewall Settings | |
| Input / Output | Specify if the current rule is input or output. |
| Deny/Permit | Specify if the current rule is Deny or Permit. |
| Protocol | Filter protocol type (TCP/ UDP/ ICMP/ IP) |
| Port Range | Set the filter Port range |
| Source Address | Set source address. It can be a single IP address or use * as a wild card. For example: 192.168.1.14 or *.*.*.14. |
| Destination Address | Set destination address. It can be a single IP address or use * as a wild card. For example: 192.168.1.14 or *.*.*.14. |
| Source Mask | Set the source address mask. For example: 255.255.255.255 points to one host while 255.255.255.0 points to a C type network. |
| Destination Mask | Set the destination address mask. For example: 255.255.255.255 points to one host while 255.255.255.0 points to a C type network. |

f) 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.



| Field Name | Explanation |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Virtual Private Network (VPN) Status | |
| VPN IP | Shows the current VPN IP address. |
| VPN Mode | |
| Enable VPN | Enable/Disable VPN. |
| L2TP | Select Layer 2 Tunneling Protocol |
| Open VPN | Select OpenVPN Protocol. (Only one protocol may be activated. After the selection is made, the configuration should be saved and the phone be rebooted.) |
| Layer 2 Tunneling Protocol (L2TP) | |
| VPN Server address | Set VPN L2TP Server IP address. |
| VPN user | Set User Name access to VPN L2TP Server. |
| VPN password | Set Password access to VPN L2TP Server. |

g) SECURITY

| Field Name | Explanation |
|----------------------|----------------------------------------------------------------------------|
| Update Security File | Select the security file to be updated. Click the Update button to update. |
| Delete Security File | Select the security file to be deleted. Click the Delete button to Delete. |
| SIP TLS Files | Show SIP TLS authentication certificate. |
| HTTPS Files | Show HTTPS authentication certificate. |
| OpenVPN Files | Show OpenVPN File authentication certificate file. |

(3) VOIP

a) SIP

Configure a SIP server on this page.

SIP STUN

SIP Line: SIP 1

Basic Settings >>

Status: Unapplied

Server Address:

Server Port: 5060

Authentication User:

Authentication Password:

SIP User:

Display Name:

Enable Registration:

Advanced SIP Settings >>

Apply

SIP Global Settings >>

Advanced SIP Settings >>

| | | | |
|-----------------------|--------------------------|--------------------------|-------------------------------------|
| Proxy Server Address | <input type="text"/> | Proxy Server Port | <input type="text"/> |
| Proxy User | <input type="text"/> | Proxy Password | <input type="text"/> |
| Backup Server Address | <input type="text"/> | Backup Server Port | 5060 |
| Domain Realm | <input type="text"/> | Server Name | <input type="text"/> |
| RTP Encryption | <input type="checkbox"/> | Enable Session Timer | <input type="checkbox"/> |
| Registration Expires | 60 second(s) | Session Timeout | 0 second(s) |
| Keep Alive Type | SIP Option | Keep Alive Interval | 60 second(s) |
| User Agent | <input type="text"/> | Server Type | COMMON |
| DTMF Type | AUTO | RFC Protocol Edition | RFC3261 |
| DTMF SIP INFO Mode | Send */# | Local Port | 5060 |
| Enable Rport | <input type="checkbox"/> | Keep Authentication | <input type="checkbox"/> |
| Enable PRACK | <input type="checkbox"/> | Ans. With a Single Codec | <input type="checkbox"/> |
| Enable Strict Proxy | <input type="checkbox"/> | Auto TCP | <input type="checkbox"/> |
| Enable DNS SRV | <input type="checkbox"/> | Use VPN | <input checked="" type="checkbox"/> |
| Transport Protocol | UDP | | |

Apply

SIP Global Settings >>

| | | | |
|---------------------------------|-------------------------------------------|------------------|-------------------------------------------------------------|
| Strict Branch | <input type="checkbox"/> | Enable Group | <input type="checkbox"/> |
| Registration Failure Retry Time | <input type="text" value="32"/> second | DND Return Code | <input type="text" value="480(Temporarily Not Available)"/> |
| Reject Return Code | <input type="text" value="603(Decline)"/> | Busy Return Code | <input type="text" value="486(Busy Here)"/> |

Apply

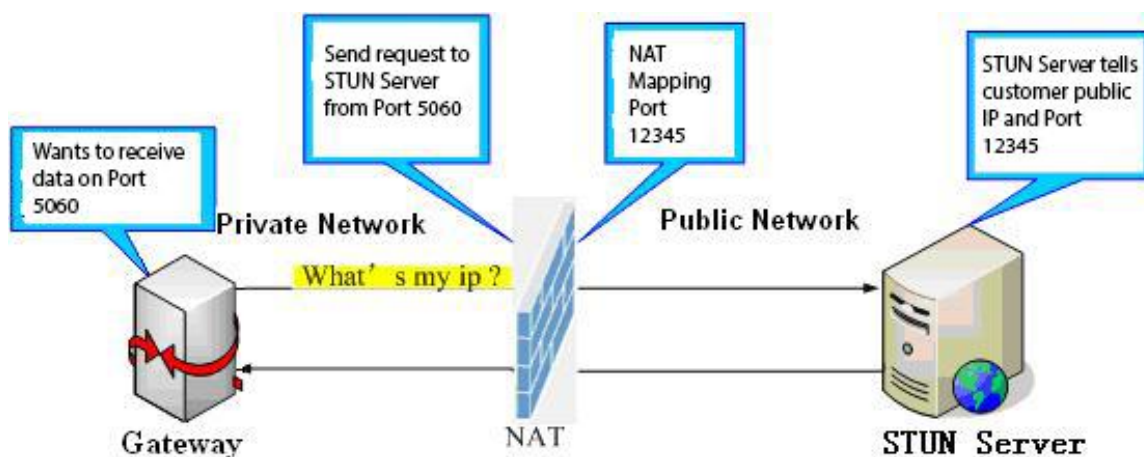
| SIP | |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Field Name | Explanation |
| Basic Settings (Choose the SIP line to configured) | |
| Status | Shows registration status. If the registration is successful done, it will display "has been registered", otherwise will display "not registered". The wrong password will display "403 errors" and account number failure will display "timeout". |
| Server Address | SIP server IP address or URI. |
| Server Port | SIP server port. Default is 5060. |
| Authentication User | SIP account name (Login ID). |
| Authentication Password | SIP registration password. |
| SIP User | Phone number assigned by VoIP service provider. Equipment will not register if there is no phone number configured. |
| Display Name | Set the display name. This name is shown on Caller ID. |
| Enable Registration | Check to submit registration information. |
| Advanced SIP Settings | |
| Proxy Server Address | SIP proxy server IP address or URI, (This is normally the same as the SIP Registrar Server) |
| Proxy Server Port | SIP Proxy server port. Normally 5060. |
| Proxy User | SIP Proxy server account. |
| Proxy Password | SIP Proxy server password. |
| Backup Server Address | Backup SIP Server Address or URI (This server will be used if the primary server is unavailable) |
| Backup Server Port | Backup SIP Server Port. |
| Domain Realm | SIP Domain if different than the SIP Register Server. |
| Server Name | Name of SIP Backup server |

| Field Name | Explanation |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SIP Encryption | Enable/Disable SIP Encryption. |
| Enable Session Timer | If enabled, this will refresh the SIP session timer per RFC4028. |
| Registration Expires | SIP re-registration time. Default is 60 seconds. If the server requests a different time, the phone will change to that value. |
| Session Timeout | Refresh interval if Session Timer is enabled. |
| Keep Alive Type | Specifies the NAT keep alive type. If SIP Option is selected, the equipment will send SIP Option SIP messages to the server every NAT Keep Alive Period. The server will then respond with 200 OK. If UDP is selected, the equipment will send a UDP message to the server every NAT Keep Alive Period. |
| Keep Alive Interval | Set the NAT Keep Alive interval. Default is 60 seconds |
| User Agent | Set SIP User Agent value. |
| Server Type | Configures phone for unique requirements of selected server. |
| DTMF Type | DTMF sending mode. There are four modes: <ul style="list-style-type: none"> ● In-band ● RFC2833 ● SIP_INFO ● AUTO Different VoIP Service providers may require different modes. |
| RFC Protocol Edition | Select SIP protocol version RFC3261 or RFC2543. Default is RFC3261. Used for servers which only support RFC2543. |
| DTMF SIP INFO Mode | You can chose Send 10/11 or Send */# |
| Local Port | SIP port. Default is 5060. |
| Enable Rport | Enable/Disable support for NAT traversal via RFC3581 (Rport). |
| Keep Authentication | Enable /disable registration with authentication. It will use the last authentication field which passed authentication by server. This will decrease the load on the server if enabled |
| Enable PRACK | Enable or disable SIP PRACK function. Default is OFF. It is suggested this be used. |
| Ans. With a Single Codec | If enabled phone will respond to incoming calls with only one codec. |
| 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. |
| Auto TCP | Force the use of TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes |

| Field Name | Explanation |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable DNS SRV | Enables use of DNS SRV records |
| Use VPN | Enable SIP use VPN for every line individually, not all of them |
| Transport Protocol | Configuration using the transport protocol, TCP, TLS or UDP, the default is UDP. |
| SIP Global Settings | |
| Strict Branch | Enable Strict Branch - The value of the branch must be after "z9hG4bK" in the VIA field of the INVITE message received, or the phone will not respond to the INVITE. Note: This will affect all lines |
| Enable Group | Enable SIP Group Backup. This will affect all lines |
| Registration Failure Retry Time | Registration failures retry time – If registrations fails, the phone will attempt to register again after registration failure retry time. This will affect all lines |
| DND Return Code | Specify SIP Code returned for DND. Default is 480 - Temporarily Not Available. |
| Reject Return Code | Specify SIP Code returned for Rejected call. Default is 603 – Decline. |
| Busy Return Code | Specify SIP Code returned for Busy. Default is 486 – Busy Here. |

b) STUN

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
STUN

- > BASIC
- > NETWORK
- > VoIP
- > INTERCOM
- > DOOR PHONE
- > MAINTENANCE
- > LOGOUT

Simple Traversal of UDP through NATs (STUN) Settings

| | | |
|--------------------|-------|-------------------------------------------------|
| 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(s) |
| Local SIP Port | | <input type="text" value="5060"/> |

SIP Line Using STUN

Use STUN

| STUN | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Field Name | Explanation |
| STUN NAT Traversal | Shows whether or not STUN NAT Traversal was successful. |
| 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. |
| Local SIP Port | Port configure the local SIP signaling |
| SIP Line Using STUN (SIP1 or SIP2) | |
| Use STUN | Enable/Disable STUN on the selected line. |
| 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. | |

(4) INTERCOM

a) AUDIO

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

The screenshot shows the 'AUDIO' configuration page in the Fanvil web interface. The sidebar on the left lists navigation options: BASIC, NETWORK, VoIP, INTERCOM (highlighted), DOOR PHONE, MAINTENANCE, and LOGOUT. The main content area is divided into three sections:

- Audio Settings:**
 - First Codec: G.711A
 - Second Codec: G.711U
 - Third Codec: G.722
 - Fourth Codec: G.729AB
 - DTMF Payload Type: 101 (96~127)
 - Default Ring Type: Type 1
 - G.729AB Payload Length: 20ms
 - Tone Standard: United States
 - G.722 Timestamps: 160/20ms
 - G.723.1 Bit Rate: 6.3kb/s
 - Enable VAD:
- Talk Volume Settings:**
 - SPK Output Volume: 5 (1~9)
 - MIC Input Volume: 2 (1~9)
- Media Volume Settings:**
 - Broadcast Output Volume: 5 (1~9)
 - Signal Tone Volume: 7 (0~9)

An 'Apply' button is located at the bottom right of the configuration area.

| Field Name | Explanation |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Audio Settings | |
| 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. |
| Enable VAD | Enable or disable Voice Activity Detection (VAD). If VAD is enabled, G729 Payload length cannot be set greater than 20 mSec. |

| Field Name | Explanation |
|------------------------------|-----------------------------------------------|
| Talk Volume Settings | |
| SPK Output Volume | Set the speaker calls the volume level. |
| MIC Input Volume | Set the MIC calls the volume level. |
| Media Volume Settings | |
| Broadcast Output Volume | Set the broadcast the output volume level. |
| Signal Tone Volume | Set the audio signal the output volume level. |

b) FEATURE

| Feature | |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Field Name | Explanation |
| Feature Settings | |
| DND (Do Not Disturb) | DND might be disabled phone for all SIP lines, or line for SIP individually. But the outgoing calls will not be affected |
| Ban Outgoing | If enabled, no outgoing calls can be made. |

| Field Name | Explanation |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Enable Intercom Mute | If enabled, mutes incoming calls during an intercom call. |
| Enable Intercom Tone | If enabled, plays intercom ring tone to alert to an intercom call. |
| Enable Auto Answer | Enable Auto Answer function |
| Auto Answer Timeout | Set Auto Answer Timeout |
| No Answer Handdown | Enable automatically hang up when no answer |
| No Answer Handdown Time | 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. |
| Enable Speed Dial Handdown | Enable Speed Dial Hand Up function |
| Dial Number Voice Play | Configuration Open / Close Dial Number Voice Play |
| Use Function Key to Answer | Configure whether to enable the function keys, is disabled by default. |
| Block Out Settings | |
| <p>Add or Delete Blocked numbers – Enter the prefix of numbers which should not be dialled by the phone. For example, if 001 is entered, the phone will not dial any numbers beginning with 001.</p> <p>X and x are wildcards which match single digits. For example, if 4xxx or 4XXX is entered, the phone will not dial any 4 digit numbers beginning with 4. It will dial numbers beginning with 4 which are longer or shorter than 4 digits.</p> | |

c) MCAST

MCAST Settings

Priority: 1

Enable Page Priority:

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

Apply

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

MCAST Settings

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

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

- **Priority:**

In the drop-down box to choose priority of ordinary calls the priority, if the priority of the incoming flows of multicast RTP, lower precedence than the current common calls, device will automatically ignore the group RTP stream. If the priority of the incoming flow of multicast RTP is higher than the current common calls priority, device will automatically receive the group RTP stream, and keep the current common calls in state. You can also choose to disable in the receiving threshold drop-down box, the device will automatically ignore all local network multicast RTP 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 | ss | 239.1.1.1:1366 |
| 2 | ee | 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 | group 1 | 224.0.0.2:2366 |
| 2 | group 2 | 224.0.0.2:1366 |
| 3 | group 3 | 224.0.0.6:3366 |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

- **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.

d) Action URL

Action URL 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`

(5) DOOR PHONE

a) FUNCTION KEY

| Key | Type | Number 1 | Number 2 | Line | Subtype |
|-----------|-----------|----------|----------|------|------------|
| DSS Key 1 | Key Event | | | SIP1 | OK |
| DSS Key 2 | None | | | SIP1 | Speed Dial |
| DSS Key 3 | None | | | SIP1 | Speed Dial |
| DSS Key 4 | None | | | SIP1 | Speed Dial |

➤ Key Event Settings

Set the key type to the Key Event.

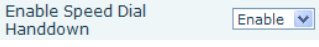
| Key | Type | Number 1 | Number 2 | Line | Subtype |
|-----------|-----------|----------|----------|------|------------|
| DSS Key 1 | Key Event | | | SIP1 | OK |
| DSS Key 2 | None | | | SIP1 | None |
| DSS Key 3 | Hot Key | | | SIP1 | Dial |
| DSS Key 4 | Line | | | SIP1 | Release |
| | Key Event | | | SIP1 | OK |
| | Multicast | | | SIP1 | Handfree |
| | None | | | SIP1 | Speed Dial |

| DSS key type | Subtype | Usage |
|--------------|----------|--------------------------------------------|
| Key Event | None | Not responding |
| | Dial | Dial function |
| | Release | End calls |
| | OK | Identify key |
| | Handfree | The hand-free key(with hook dial, hang up) |

➤ Hot key Settings

Enter the phone number in the input box, when you press the shortcut key, equipment will dial set telephone number. This button can also be used to set the IP address, press the shortcut key IP direct dial call.

| Key | Type | Number 1 | Number 2 | Line | Subtype |
|-----------|-----------|----------|----------|------|------------|
| DSS Key 1 | Hot Key | | | SIP1 | Speed Dial |
| DSS Key 2 | None | | | SIP1 | Speed Dial |
| DSS Key 3 | Hot Key | | | SIP1 | Intercom |
| DSS Key 4 | Line | | | SIP1 | Speed Dial |
| | Key Event | | | SIP1 | Speed Dial |
| | Multicast | | | SIP1 | Speed Dial |
| | None | | | SIP1 | Speed Dial |

| DSS key type | Number | Line | Subtype | Usage |
|--------------|------------------------------------------------|-------------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hot Key | Fill the called party's SIP account or address | The SIP account corresponding lines | Speed Dial | In Speed dial mode, with  can define whether this call is allowed to be hang up by re-press the speed dial |
| | | | Intercom | In Intercom mode, if the caller's IP phone support intercom feature, can realize auto answer |

➤ Multicast Settings

Multicast function is launched will voice messages sent to set the multicast address, all equipment to monitor the group multicast address can receive sponsors speech information, etc. Using multicast functionality can be simple and convenient to send notice to each member in the multicast.

Through the DSS Key configuration multicast calling WEB is as follows:

| Key | Type | Number 1 | Number 2 | Line | Subtype |
|-----------|-----------|----------|----------|------|----------|
| DSS Key 1 | Multicast | | | SIP1 | G.711A |
| DSS Key 2 | None | | | SIP1 | G.711A |
| DSS Key 3 | Hot Key | | | SIP1 | G.711U |
| DSS Key 4 | Line | | | SIP1 | G.722 |
| | Key Event | | | SIP1 | G.723.1 |
| | Multicast | | | SIP1 | G.726-32 |
| | None | | | SIP1 | G.729AB |

| DSS key type | Number | Subtype | Usage |
|--------------|--------------------------------------------------------------------------|----------|---------------------------------|
| Multicast | Set the host IP address and port number, the middle 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

Device through the DSS Key configuration of multicast address and port and started coding; set by WEB to monitor the multicast address and port; device sends a multicast, listens to the address of the device can receive the multicast content.

✧ calling configuration

The call is already exists, and three party or initiated multicast communication, so it will not be able to launch a new multicast call.

b) DOOR PHONE

FUNCTION KEY
DOOR PHONE
DOOR CARD
DOOR ACCESS
DOOR LOG

- > BASIC
- > NETWORK
- > VoIP
- > INTERCOM
- > DOOR PHONE
- > MAINTENANCE
- > LOGOUT

EGS Settings

| | | | |
|--------------------------|--------------------------------------------------|---------------------------------|---------------------------------------------------|
| Switch Mode | <input type="text" value="monostable"/> | Keypad Mode | <input type="text" value="Dial and Password"/> |
| Switch-On Duration | <input type="text" value="5"/> (1~600 seconds) | Talk Duration | <input type="text" value="120"/> (20~600 seconds) |
| Remote Password | <input type="text" value="*"/> | Local Password | <input type="text" value="6789"/> |
| Description | <input type="text" value="i23 IP Door Phone"/> | Enable Access Table | <input type="text" value="Enable"/> |
| Hot Key Dial Mode Select | <input type="text" value="Main-Secondary"/> | Call Switched Time | <input type="text" value="16"/> (5~50 seconds) |
| 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="text" value="Disable"/> | Enable Indoor Open | <input type="text" value="Enable"/> |
| Enable Card Reader | <input type="text" value="Enable"/> | Limit Talk Duration | <input type="text" value="Enable"/> |
| Door Unlock Indication | <input type="text" value="Long beeps"/> | Remote Access Code Check Length | <input type="text" value="4"/> (1~6) |

Tamper Alarm Settings

| | |
|---------------------------------------|-------------------------------------------|
| <input type="checkbox"/> Tamper Alarm | <input type="button" value="Reset"/> |
| Alarm command | <input type="text" value="Tamper_Alarm"/> |
| Server Address | <input type="text" value="0.0.0.0"/> |
| Reset command | <input type="text" value="Tamper_Reset"/> |
| Tamper Alarm Ring | <input type="text" value="default"/> |

| Field Name | Explanation | Initial Value |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| EGS Settings | | |
| Switch Mode | Monostable: there is only one fixed action status for door unlocking. Bistable: there are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After changed, the status would be kept. | Monostable |
| Keypad Mode | Only password: password input only, dialing would be forbidden. Password+dialing: password input is default. Dialing mode is as below if you want. <ul style="list-style-type: none"> ● key for off hook to dialing mode, # key for hang up. ● Time out or length match for number sending when dialing mode. * Key to enter the dial, the # key to hang up. | Password+dialing |
| Switch-On Duration | Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. | 5 seconds |
| Talk Duration | The call will be ended automatically when time up. | 120 seconds |
| Remote Password | Remote door unlocking password. | * |
| Local Password | Local door unlocking password via keypad, the default password length is 4. | 6789 |
| Description | Device description displayed on IP scanning tool software. | i23 IP door phone |

| Field Name | Explanation | Initial Value |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| Enable Access Table | Enable Access Table: enter <Access Code> for opening door during calls. Disable Access Table: enter <Remote Password> for opening door during calls. | Enable |
| Hot Key Dialed Mode Selection | <Primary /Secondary>mode allow system to call primary extension first, if there were no answer, it would cancel the call and then call secondary extension automatically. <Day/Night>mode allow system to check the calling time is belong to Day or Night time, and then decide to call the number 1 or number 2 automatically. Users just press speed dial key once. | Primary /secondary |
| Call Switched Time | The period between hot key dialing to the first and second number. | 16 seconds |
| Day Start Time | The start time of the Day When you select<Day/Night>mode | 06:00 |
| Day End Time | The end time of the day When you select <Day/Night>mode | 18:00 |
| Address of Log Server | Log server address(IP or domain name) | 0.0.0.0 |
| Port of Log Server | Log server port(0-65535) | 514 |
| Enable Log Server | Enable or disable to connect with log server | Disable |
| Enable Indoor Open | Enable or disable to use indoor switch to unlock the door. | Enable |
| Enable Card Reader | Enable or disable card reader for RFID cards. | Enable |
| Limit Talk Duration | If enabled, calls would be forced ended after talking time is up. | Enable |
| Door Unlock Indication | Indication tone for door unlocked. There are 3 type of tone: silent/short beeps/long beeps. | Long beeps |
| Remote Access 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. | 4 |

| Field Name | Explanation |
|------------------------------|-----------------------------------------------------------------------------------------------|
| Tamper Alarm Settings | |
| Tamper Alarm | When the selection is enabled, the tamper detection enabled |
| Reset | Directly stop the alarm from equipment in the Webpage |
| 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 |
| Server Address | Configure remote response server address |
| Tamper alarm ring | When the detected someone tampering the equipment, plays the corresponding ringtone or alarm |

c) DOOR CARD

FUNCTION KEY | **DOOR PHONE** | **DOOR CARD** | **DOOR ACCESS** | **DOOR LOG**

Door Card Table

Total: 0 Page: [Right Click here to Save Door Card Table](#)

| Index | Name | ID | <input type="checkbox"/> | Issuing Date | Card State |
|--------------------------------------|------|----|--------------------------|--------------|------------|
| <input type="button" value="Apply"/> | | | | | |

Add Door Card

ID

Import Door Card Table

Select File (doorCard.csv)

Card Reader Setting>>

State

Administrator Table>>

Add Administrator>>

Delete Administrator>>

| Door Card | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Field Name | Explanation |
| Door Card Table | |
| Index | The serial number of has been issuer cards. |
| Name | The name of has been issuer cards. |
| ID | The card number of has been issuer cards. (Note: The card is not registered in the remote access list is unable to open the door.) |
| Issuing Date | The issuing date of has been issuer cards. |
| Card State | To have been issuer cards the state. |
| Delete | Click <delete>, will delete the door card list within the selected ID cards. |
| Delete All | Click <Delete All>, to delete all door card lists. |
| Export door card table | Right Click here to Save Door Card Table Right-click it and select save target to your computer. |
| Add Door Card | |
| The input RFID card numbers the top 10, for example, 0004111806, click <add>. | |
| Import Door Card Table | |
| Click the <Browse> to choose to import door card list file (doorCard.csv), click <Update> can be batch import. | |
| Card Reader Setting | |
| Set ID card stats: Normal: This is the work mode, after the slot card can to open the door. Card Issuing: This is the issuing mode, after the slot card can to add ID cards. Card Revoking: This is the revoking mode, after the slot card can to delete ID cards. | |
| Administrator Table | |
| The show admin card the ID, Date and Type. | |
| Add Administrator | |
| ID: admin card the card number. Type: Issuer and Revoking. Entrance guard in normal state, brush card(issuing card) entrance guard into the issuing state, and then brush to add a card, the card is added to the database, add swipe again after card(issuing card) entrance guard returned to normal. Delete card operation and issuing card the same. Can release at most 10 cards, 500 copies of ordinary cards. Note: in the issuing state to delete brush card is invalid, and vice versa. | |
| Delete Administrator | |
| Choose to delete the card number, then press <delete>. | |

d) DOOR ACCESS

FUNCTION KEY
DOOR PHONE
DOOR CARD
DOOR ACCESS
DOOR LOG

- > BASIC
- > NETWORK
- > VoIP
- > INTERCOM
- > DOOR PHONE
- > MAINTENANCE
- > LOGOUT

Access Table

Total: 0 Page: ▼ Pre Next Delete ⚠ Delete All [Right Click here to Save Access Table](#)

| Index | Name | ID | Department | Position | location | Number | Fwd Number | Access Code | Double Auth | Access by Call | Access by Psw | Profile | Type | <input type="checkbox"/> |
|-------|------|----|------------|----------|----------|--------|------------|-------------|-------------|----------------|---------------|---------|------|--------------------------|
| | | | | | | | | | | | | | | |

Add Access Rule

Name ★

ID ▼

Access Code Remote Call and Local Auth ▼ ⚠

Location ⚠

Add

Department

Position

Time Profile None ▼

Access Type Guest ▼

Double Authentication Disable ▼ ⚠

Forward Num

Phone Num

Modify

Import Access Table

Select File: Browse (accessList.csv) Update

Profile Settings

Profile Profile 1 ▼

| Profile Name | Day | Active | From(00:00-23:59) | To(00:00-23:59) |
|--------------|-----------|--------------------------------|------------------------------------|------------------------------------|
| | Sunday | No ▼ | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |
| | Monday | No ▼ | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |
| | Tuesday | No ▼ | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |
| | Wednesday | No ▼ | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |
| | Thursday | No ▼ | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |
| | Friday | No ▼ | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |
| | Saturday | No ▼ | <input type="text" value="00:00"/> | <input type="text" value="00:00"/> |

Apply

| Field Name | Explanation |
|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Table | |
| According to entrance guard access rules have been added, can choose single or multiple rules on this list to delete operation. | |
| Add Access Rule | |
| Name(necessary) | User name |
| Department | Card holder's department |
| Position | Card holder's position |
| ID | RFID card number |
| Time Profile | Valid for user access rules (including RFID, access code, etc) within corresponding time section. If NONE is selected, it would be taken effect all day. |
| Access Type | Host: the door phone would answer all call automatically. Guest: the door phone would be ringing for incoming call, if the auto answer had been disabled. |
| Access Code | 1/ When the door phone has been answering the call from below <Phone Num> user, then the <Phone Num> user can input the access code by keypad to unlock the door remotely. 2/ The user's private password for local door unlocking by door phone's keypad. |
| Double Authentication | When enabled, private password inputting and RFID reading must be matched simultaneously for door unlocking. |
| Location | Virtual extension number, used to make position call instead of real number. It might be taken with unit number, or room number. |
| Phone Num | User Phone Number |
| Forward Num | Call forwarding number when above Phone Num is unavailable. |
| Import Access Table | |
| Click the <Browse> to choose to import remote access list file (access List.csv) and then click <Update> can be batch import remote access rule. | |
| Profile Settings | |
| Time profile sections | There are 4 sections for time profile configuration |
| Profile Name | The name of profile to help administrator to remember the time definition |
| Active | If it were yes, the time profile would be taken effect. Other time section not included in the profiles would not allow users to open door |
| From | The start time of section |
| To | The end time of section |

e) DOOR LOG

According to open event log, can record up to 2 w open event, after more than cover the old records.

[Right Click here to Save Logs](#) Right click on the links to select save target as the door log can export CSV format.

The screenshot displays the Fanvil web interface. At the top, there are navigation tabs: FUNCTION KEY, DOOR PHONE, DOOR CARD, DOOR ACCESS, and DOOR LOG. The DOOR LOG tab is selected. On the left, a vertical navigation menu lists various system categories. The main content area is titled 'Door Opening Log' and contains a table with the following data:

| Door Opening Time | Duration | Access Name | Access ID | Type |
|-------------------|-------------|-------------|------------|---------|
| JAN 01 03:16:32 | 5 second(s) | | | Local |
| JAN 01 03:18:38 | 5 second(s) | joe | 0006800281 | IC Card |
| JAN 01 03:23:30 | 5 second(s) | joe | 8207 | Remote |

Below the table, there is a 'Call Information' section with a table:

| Start Time | Duration | Peer Calls | Type |
|------------|----------|------------|------|
| | | | |

| Field Name | Explanation |
|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Door Opening Log | |
| Door Opening Time | Open the door of time. |
| Duration | Duration of open the door. |
| Access Name | If is the open the door for slot card or remote, will display remote access the name. |
| Access ID | 1. If open the door way to brush card shows card number 2. If the door way to open the door for the remote display the phone number of the door. 3. If open the door way to open the door for local, no display information. |
| Type | Open type: 1. local, 2. Remote, 3. Brush card. |
| Call Information | |
| Display device call records. Including: start time, duration, call number and call type. | |

(6) MAINTENANCE

a) AUTO PROVISION

The equipment supports PnP, DHCP, and Phone Flash to obtain configuration parameters. They will be queried in the following order when the equipment boots.

DHCP option → PnP server → Phone Flash

| Field Name | Explanation |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auto Provision Settings | |
| Current Config 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 |
| Common Config 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 |
| User | Username for configuration server. Used for FTP/HTTP/HTTPS. If this is blank the phone will use anonymous |
| Password | Password for configuration server. Used for FTP/HTTP/HTTPS. |

| Field Name | Explanation |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Config Encryption Key | Encryption key for the configuration file |
| Common Config Encryption Key | Encryption key for common configuration file |
| Save Auto Provision Information | Save the auto provision username and password in the phone until the server url changes |
| DHCP Option Settings | |
| DHCP Option Setting | The equipment supports configuration from Option 43, Option 66, or a Custom DHCP option. It may also be disabled. |
| Custom DHCP Option | Custom option number. Must be from 128 to 254. |
| Plug and Play (PnP) Settings | |
| Enable 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. |
| PnP server | PnP Server Address |
| PnP port | PnP Server Port |
| PnP Transport | PnP Transfer protocol – UDP or TCP |
| PnP Interval | Interval time for querying PnP server. Default is 1 hour. |
| Phone Flash Settings | |
| Server Address | Set FTP/TFTP/HTTP server IP address for auto update. The address can be an IP address or Domain name with subdirectory. |
| Config 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"> 1. Disable – no update 2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update interval |

| Field Name | Explanation |
|-------------------------|---------------------------------------------------------|
| TR069 Settings | |
| 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. |

b) SYSLOG

The screenshot shows the Fanvil web interface with the 'SYSLOG' tab selected. On the left is a navigation menu with options: BASIC, NETWORK, VoIP, INTERCOM, DOOR PHONE, MAINTENANCE (highlighted), and LOGOUT. The main content area is titled 'Syslog Settings' and contains the following fields:

- Server Address: 0.0.0.0
- Server Port: 514
- MGR Log Level: None (dropdown)
- SIP Log Level: None (dropdown)
- Enable Syslog:

An 'Apply' button is located below the 'Enable Syslog' checkbox. Below the Syslog Settings section is a 'Web Capture' section with 'Start' and 'Stop' buttons.

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.

| Field Name | Explanation |
|----------------------------|---------------------------------------------------------------------------------------------|
| System log settings | |
| Server Address | System log server IP address. |
| Server port | System log server port. |
| MGR log level | Set the level of MGR log. |
| SIP log level | Set the level of SIP log. |
| Enable syslog | Enable or disable system log. |
| Web Capture | |
| Start | Capture a packet stream from the equipment. This is normally used to troubleshoot problems. |
| Stop | Stop capturing the packet stream |

c) CONFIG

| Field Name | Explanation |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Save Configuration | Save the current equipment configuration. Clicking this saves all configuration changes and makes them effective immediately. |
| Backup Configuration | Save the equipment configuration to a txt or xml file. Please note to Right click on the choice and then choose "Save Link As." |
| Clear Configuration | Logged in as Admin, this will restore factory default and remove all configuration information. Logged in as Guest, this will reset all configuration information except for VoIP accounts (SIP1-2) and version number. |

d) UPDATE

This page allows uploading configuration files to the equipment.

| Field Name | Explanation |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web Update | Browse to the config file, and press Update to load it to the equipment. Various types of files can be loaded here including firmware, ring tones, local phonebook and config files in either text or xml format. |

e) ACCESS

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

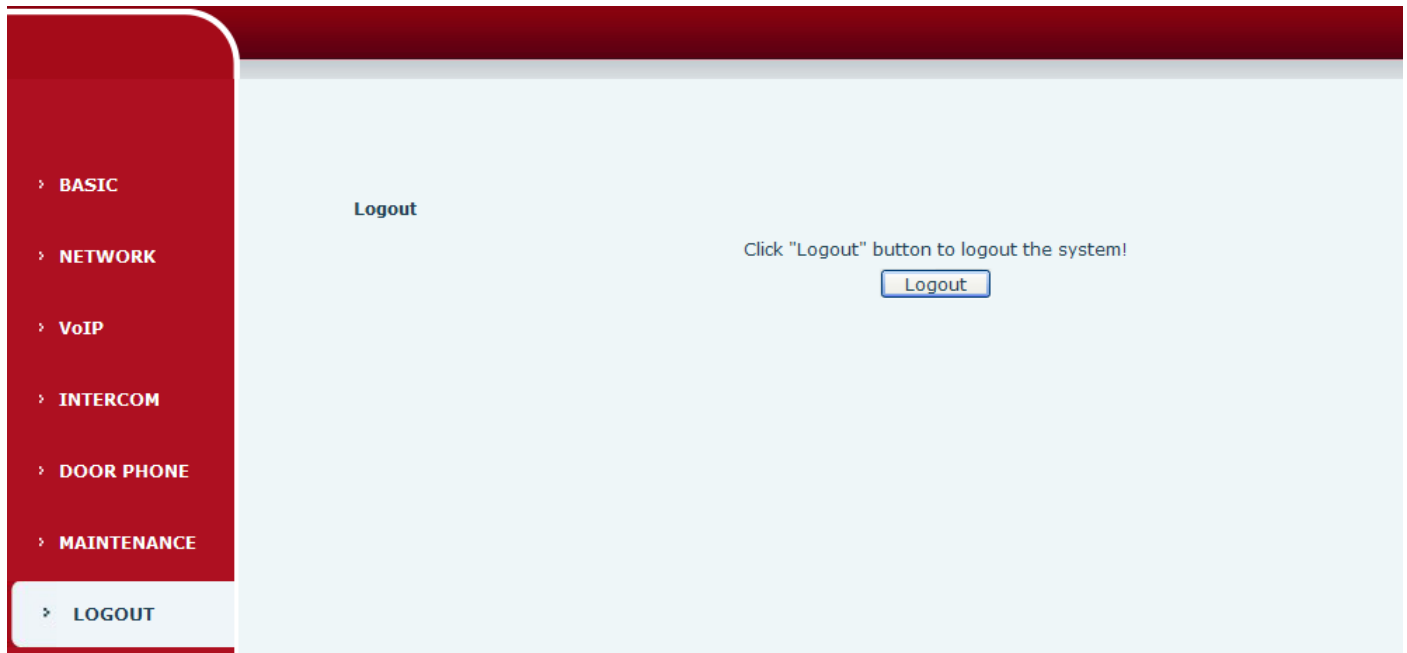
| Field Name | Explanation |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| User Settings | |
| User | shows the current user name |
| User level | Show the user level; admin user can modify the configuration. General user can only read the configuration. |
| Add User | |
| User | Set User Account name |
| Password | Set the password |
| Confirm | Confirm the password |
| User level | There are two levels. Root user can modify the configuration. General user can only read the configuration. |
| User Management | |
| Select the account and click Modify to modify the selected account. Click Delete to delete the selected account. A General user can only add another General user. | |

f) REBOOT

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.

(7) LOGOUT



Click <Logout> from the web to exit. Users need to enter their user name and password again when visit next time.

E. Appendix

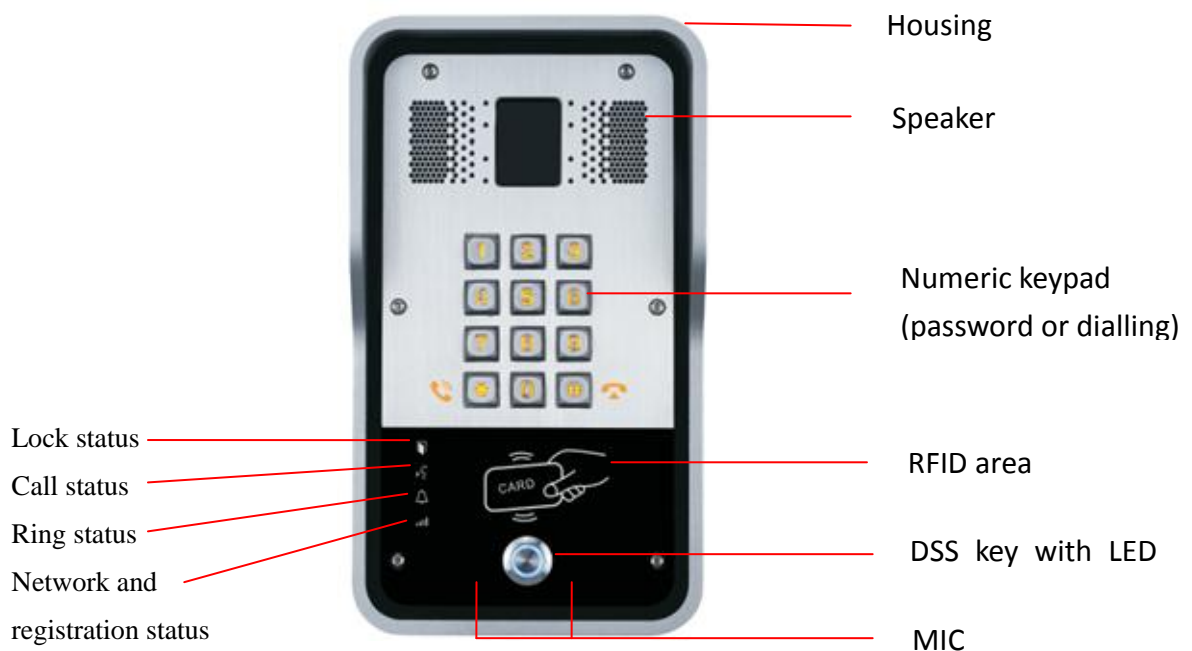
1. Technical parameters

| | | |
|-----------------------------------|---------------------------------|---------------------------------------------------------|
| Communication protocol | | SIP 2.0(RFC-3261) |
| Main chipset | | Broadcom |
| Key | DSS key materials | Stainless steel |
| | DSS Key | 1 |
| | Numeric keyboard | Support |
| Speech flow | Audio amplifier | 2.4W |
| | Volume control | Adjustable |
| | Full duplex speakerphone | Support (AEC) |
| | Protocols | RTP |
| | Decoding | G.729、 G.723、 G.711、 G.722、 G.726 |
| Port | Passive switch(relay) | Normally open/Normally close, support 30V/1A AC/DC. |
| | Active Switched Output | 12V/750mA DC |
| | External speakers | Audio output (only support to fully functional version) |
| | WAN | 10/100BASE-TX s Auto-MDIX, RJ-45 |
| | LAN | 10/100BASE-TX s Auto-MDIX, RJ-45 |
| RFID/IC card reader(relay) | | EM4100 (125Khz) MIFARE One(13.56Mhz) NFC |
| Power supply mode | | 12V / 1A DC or PoE |
| Cables | | CAT5 or better |
| Shell Material | | Cast aluminium panel, Cast aluminium back shell |
| Working temperature | | -40°C to 70°C |
| Working humidity | | 10% - 90% |
| Storage temperature | | -40°C to 70°C |
| Installation way | | Wall mounted or In-wall |
| Dimension | | Wall mounted: 225*131*73.5mm In-wall: 270*150*83mm |

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 mounted / In-wall
- Special integrated noise reduction module
- Dual microphone Omnidirectional voice pickup
- 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



F. Other instructions

1. Open door modes

● Local control

1) Local Password

- ✧ Set <Local Password> (the password is "6789" by default) via DOOR PHONE\DOOR PHONE as above.
- ✧ Input password via keypad and press the "#" key, then the door will be unlocked.

2) Private access code

- ✧ Set <Add Access Rule\Access Code> and enable local authentication.
- ✧ Input access code via keypad and press the "#" key, then the door will be unlocked.

● Remote control

1) Visitors call the owner

- ✧ Visitors can call the owner via position speed dial or phone number. (After setting the speed dial key, visitors can press it to call direct.)
- ✧ The owner answers the call and presses the "*" key to unlock the door for visitors.

2) Owner calls visitors

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

● Swip cards

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

● Indoor switch

- ✧ Press indoor switch, which is installed and connected with the 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"/> <input type="button" value="Enable"/> |
| 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 < Door card\Card Reader Setting> option, select <Card Issuing> function.

Card Reader Setting>>

State

Administrator Table>>

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

Submit Success

Return

- 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 <Door card\card reader Settings > option, select <normal> function.

Card Reader Setting>>

State Normal ▼ Apply

Normal
 Card Issuing
 Card Revoking

Administrator Table>>

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

Door Card Table

Total: 3 Page: 1 Pre Next Delete Delete All [Right Click here to Save Door Card Table](#)

| Index | Name | ID | <input type="checkbox"/> | Issuing Date | Card State |
|-------|----------|------------|--------------------------|-----------------|------------|
| 1 | zhangsan | 0004770424 | <input type="checkbox"/> | JAN 01 02:10:30 | Enable ▼ |
| 2 | joe | 0003477117 | <input type="checkbox"/> | JAN 01 02:10:44 | Enable ▼ |
| 3 | | 0003408920 | <input type="checkbox"/> | JAN 01 02:10:58 | Enable ▼ |

Apply

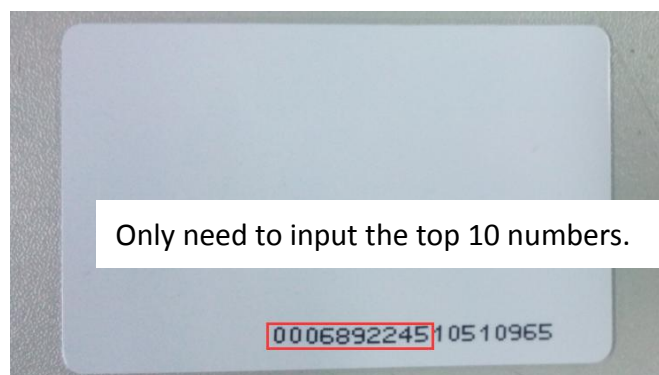
Methods 2: use to add few cards

- 1) Input cards number in door card settings page, and then click <Add>.

Add Door Card

ID Add

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



Method 3: 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.

● **Delete user cards**

Method 1: used to batch delete cards for starters.

- 1) In web page <Door card →Card Reader Setting> option, select <Card revoking>.

Card Reader Setting>>

State Card Revoking Apply

Normal
Card Issuing
Card Revoking

Administrator Table>>

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

Submit Success

Return

- 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 <Door card →card reader Settings >option, select <normal>.

Card Reader Setting>>

State Normal Apply

Normal
Card Issuing
Card Revoking

Administrator Table>>

- 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 bulk delete or partially delete card records

- 1) In web page<Door Card Table>select the card ID and then click <Apply>.

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

Door Card Table

Total: 3 Page: 1 Pre Next Delete Delete All [Right Click here to Save Door Card Table](#)

| Index | Name | ID | <input type="checkbox"/> | Issuing Date | Card State |
|-------|----------|------------|-------------------------------------|-----------------|------------|
| 1 | zhangsan | 0004770424 | <input type="checkbox"/> | JAN 01 02:10:30 | Enable |
| 2 | joe | 0003477117 | <input checked="" type="checkbox"/> | JAN 01 02:10:44 | Enable |
| 3 | | 0003408920 | <input type="checkbox"/> | JAN 01 02:10:58 | Enable |

Apply