

i31

IP Video Door Phone 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. 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).
3. 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.
4. 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.
5. 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.
6. Please use this product with normal usage and operating, in bad posture for a long time to use this product may affect your health.
7. 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 CONNECTED..... | 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 | 12 |
| c) | LANGUAGE..... | 13 |
| d) | TIME&DATE..... | 14 |
| (2) | NETWORK | 15 |
| a) | WAN | 15 |
| b) | QoS&VLAN..... | 17 |
| c) | WEB FILTER | 19 |
| d) | SECURITY | 20 |
| (3) | VOIP..... | 20 |
| a) | SIP | 20 |
| b) | STUN..... | 23 |
| (4) | INTERCOM | 25 |

| | | |
|-----|------------------------------------------------------------------------|----|
| a) | FUNCTION KEY | 25 |
| b) | MEDIA..... | 27 |
| c) | DND | 29 |
| d) | FEATURE | 30 |
| e) | MCAST | 31 |
| f) | Action URL | 34 |
| (5) | SAFEGUARDING (Only fully functional version support this feature)..... | 34 |
| (6) | DOOR PHONE..... | 37 |
| a) | DOOR PHONE..... | 37 |
| b) | DOOR CARD | 39 |
| c) | DOOR ACCESS | 40 |
| d) | DOOR LOG | 42 |
| (7) | MAINTENANCE..... | 43 |
| a) | AUTO PROVISION | 43 |
| b) | SYSLOG | 45 |
| c) | CONFIG | 46 |
| d) | UPDATE..... | 47 |
| e) | ACCESS..... | 48 |
| f) | REBOOT | 48 |
| (8) | LOGOUT | 49 |
| E. | APPENDIX | 50 |
| 1. | TECHNICAL PARAMETERS..... | 50 |
| 2. | BASIC FUNCTIONS | 51 |
| 3. | SCHEMATIC DIAGRAM | 51 |
| F. | OTHER INSTRUCTIONS..... | 52 |
| 1. | OPEN DOOR MODES | 52 |
| 2. | MANAGEMENT OF CARD | 53 |

A. Product introduction

I31 is a full digital network door phone, its core part adopt mature VoIP solution(Broadcom chipset), stable and reliable performance, Hands-free adopting digital full-duplex mode, Voice loud and clear, video clear, generous appearance, solid durable, easy for installation, comfortable keypad, low power consumption.

I31 support entrance guard control, Video intercom, keyboard, ID card and remote to open the door, and other functions.

1. Appearance of the product



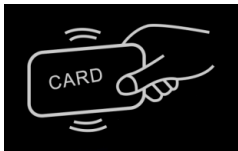






Wall mounted



In-wall

2. Description

| Buttons and icons | Description | Function |
|-------------------------------------------------------------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------|
|  | Numeric keyboard | Input password to open the door or calls. |
|  | 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 equipment, please make the following installation:


1. Confirm connected

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

1) Power port


Power supply ways: 12v/DC or POE.

| CN16 | |
|-----------|-----|
| 1 | 2 |
| +12V | GND |
| 12V 1A/DC | |

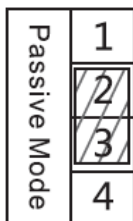


2) Electric-lock and indoor switch port

| CN6 | | | | |
|---------------|-------|----------------------|-----|----|
| 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 in active mode, device can drive 12V/700mA switch output maximum, to which a standard electric-lock or another compatible electrical appliance can be connected.

- When use the active mode, it is 12V DC in output.
- When use 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 | | Driving Mode | | Jumper port | Connections |
|--------------|---------|--------------|----|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active | Passive | NO | NC | | |
| √ | | √ | | <div>Active Mode</div> | <p>Door Phone Power Input 12V</p> <p>Power Supply 12V/1A</p> <p>Indoor switch</p> <p>Electric lock (Normally open type)</p> <p>No electricity when open the door</p> |
| √ | | | √ | <div>Active Mode</div> | <p>Door Phone Power Input 12V</p> <p>Power Supply 12V/1A</p> <p>Indoor switch</p> <p>Electric lock (Normally closed type)</p> <p>When the power to open the door</p> |
| | √ | √ | | <div>Passive Mode</div> | <p>Door Phone Power Input</p> <p>Power Supply 12V/2A</p> <p>Indoor switch</p> <p>Electric lock (normally open type)</p> <p>No electricity when open the door</p> |
| | √ | | √ | <div>Passive Mode</div> | <p>Door Phone Power Input</p> <p>Power Supply 12V/2A</p> <p>Indoor switch</p> <p>Electric lock (normally closed type)</p> <p>When the power to open the door</p> |
| | √ | √ | | <div>Passive Mode</div> | <p>Door Phone dedicated power supply NC COM NO PUSH GND +12V</p> <p>Door Phone Power Input 12V</p> <p>Indoor switch</p> <p>Electric lock (normally open)</p> <p>Without power to open the door</p> |

2. Quick Setting

The product Provide a complete function and parameter setting, users may need to have the network and SIP protocol knowledge for understanding the meaning represented by all parameters. In order to let equipment users can quickly enjoy the high quality speech brought by the IP Phone services and low cost advantage, we especially lists the basic and must set options in this section, which let users can real-time started without understanding complex SIP protocols.

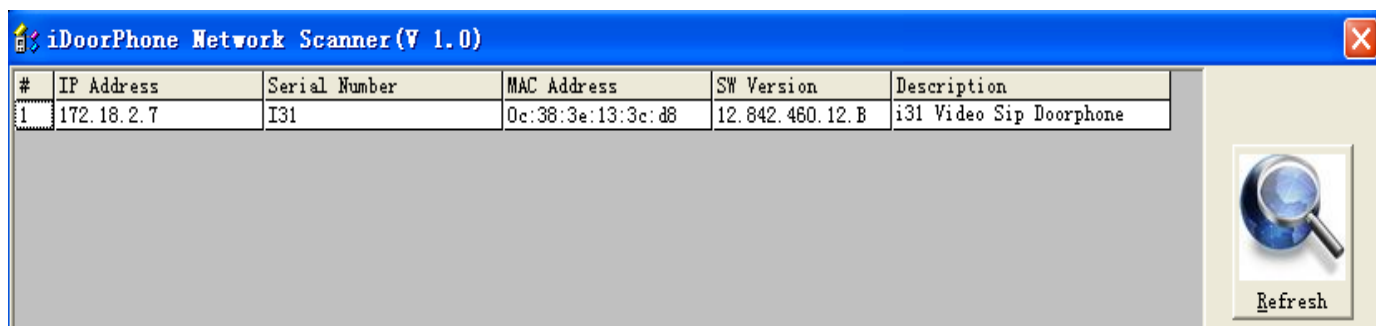
In prior to this step, please make sure your broadband Internet online can be normal operation, and complete the connection of the network hardware. The product factory default network mode is DHCP. Thus, only connect equipment with DHCP network environment then network can be automatically connected.

- 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 settings DSS key in the Webpage(functions key settings -> function key).

You can settings function parameters in the Webpage (Intercom-> feature).



| # | IP Address | Serial Number | MAC Address | SW Version | Description |
|---|------------|---------------|-------------------|-----------------|-------------------------|
| 1 | 172.18.2.7 | I31 | 0c:38:3e:13:3c:d8 | 12.842.460.12.B | i31 Video Sip Doorphone |

C. Basic operation

1. Answer a call

When calling come, the device automatically answer, in cancel automatic answer and settings automatic answer time, will hear the bell in the set time, automatic answer after a timeout.

2. Call

Configuration shortcut (key1) as hot key and setup a number, then press shortcut keys 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, will cover the first call records. When the device is powered down or reboot, call records will be removed.

You can view the three call records in the Webpage (Door phone/Door log)

5. Open the door operation

Through the following seven ways to open the door:

- 1) On the keyboard input password to open the door.
- 2) Access to call the owner; enter the remote to open the door by the owner password to open the door.
- 3) Owner/call access control of other equipment and enter the access code to open the door. (access code to be included in the list to access configuration, and enable for remote calls to open the door)
- 4) Through 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. Under the standby directly input the access code to open the door.

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

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

Access code input correct prompt sowing sirens prompt access control and the remote user, input error by short low frequency chirp.

Password successfully by high-frequency sirens sound prompt, input error is short by high frequency chirp.

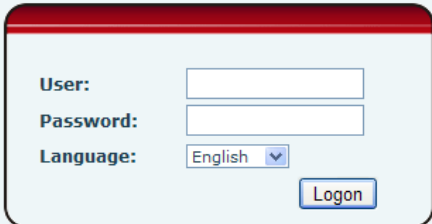
When the door opened by playing sirens sound prompt.

D. Page settings

1. Browser configuration

When the device and your computer successfully connected to the network, the on browsers enter the IP address of the device. You can see the Webpage management interface the login screen.

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



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 is rebooted.

2. Password Configuration

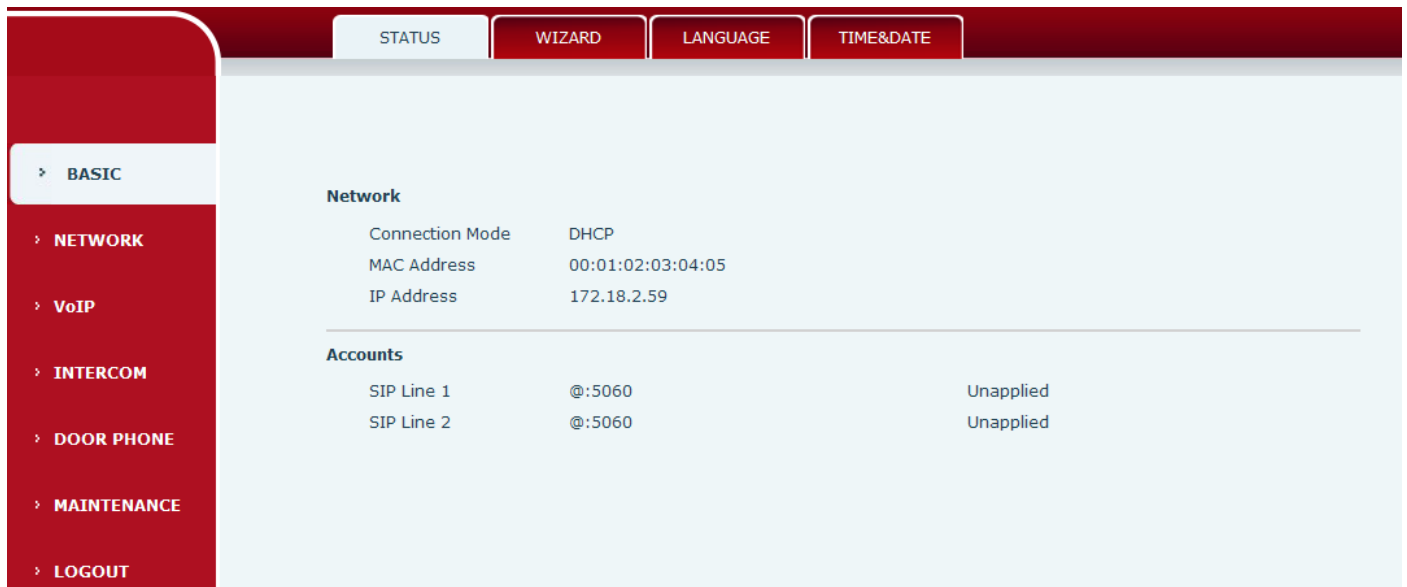
There are two levels of access: root level and general level. A user with root level access can browse and set all configuration parameters, while a user with general level can set all configuration parameters except server parameters for SIP.

- 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



STATUS | WIZARD | LANGUAGE | TIME&DATE

› BASIC

› NETWORK

› VoIP

› INTERCOM

› DOOR PHONE

› MAINTENANCE

› LOGOUT

Network

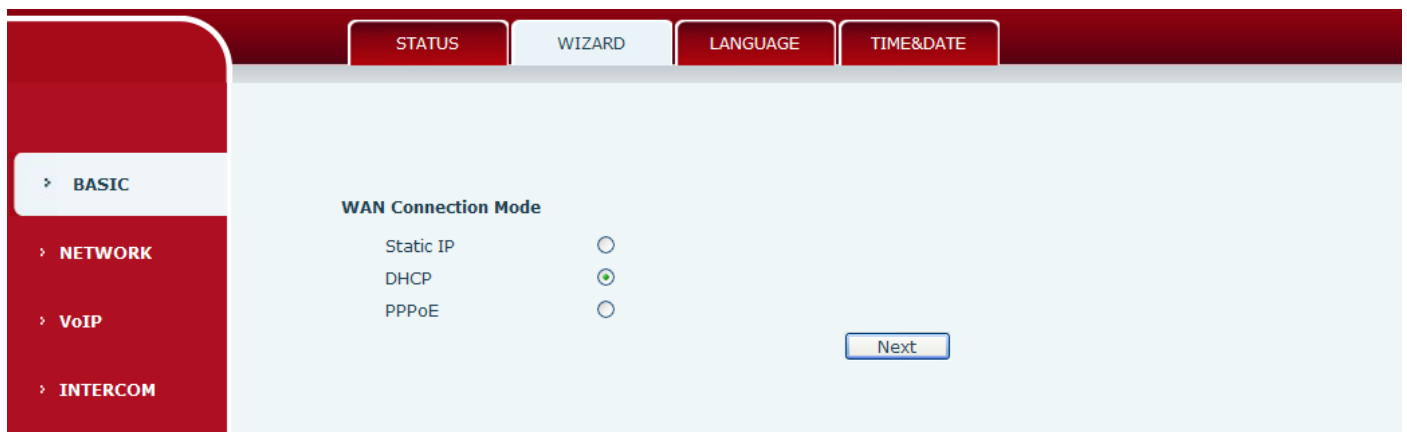
| | |
|-----------------|-------------------|
| Connection Mode | DHCP |
| MAC Address | 00:01:02:03:04:05 |
| IP Address | 172.18.2.59 |

Accounts

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

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

b) WIZARD



STATUS | WIZARD | LANGUAGE | TIME&DATE

› BASIC

› NETWORK

› VoIP

› INTERCOM

WAN Connection Mode

Static IP ☐

DHCP ☒

PPPoE ☐

Next

| 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.

The screenshot displays the Fanvil web interface for the LANGUAGE configuration page. The interface features a red sidebar on the left with navigation links: BASIC, NETWORK, VoIP, and INTERCOM. The top navigation bar includes STATUS, WIZARD, LANGUAGE (selected), and TIME&DATE. The main content area shows the 'Language' configuration section. It includes a 'Language Selection' label and a dropdown menu currently set to 'English'. An 'Apply' button is located at the bottom right of the configuration area.

d) TIME&DATE

Set the time zone and SNTP (Simple Network Time Protocol) server on this page to automatically obtain time and daylight saving time, manual time and date entry are also done on this page.

| Time&Date | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| Field Name | Explanation |
| System Current Time | |
| Display the current time | |
| Simple Network Time Protocol (SNTP) Settings | |
| Enable SNTP | Enable or Disable SNTP |
| Primary Server | IP address of Primary SNTP Server |
| Time zone | Local Time Zone |
| Time Format | Configuration time format, the default is 24 hours. |
| Date Format | Configure date display format, the default is (date) (month) (year) |
| Date Separator | Configure the date separator |
| 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

> BASIC

> NETWORK

> VoIP

> INTERCOM

> DOOR PHONE

> MAINTENANCE

> LOGOUT

WAN

QoS&VLAN

WEB FILTER

SECURITY

WAN Status

| | |
|---------------------|-------------------|
| Active IP Address | 172.18.2.59 |
| Current Subnet Mask | 255.255.0.0 |
| Current IP Gateway | 172.18.1.1 |
| MAC Address | 00:01:02:03:04:05 |

WAN Settings

Enable Vendor Identifier

Disabled

Vendor Identifier

Fanvil-I31

Static IP

☐

DHCP

☒

Obtain DNS Server Automatically

Enabled

PPPoE

☐

Apply

802.1X Settings

802.1x Mode

Off

Identity

admin

Password

•••••

CA Certificate

Browse

Upload

Device Certificate

Browse

Upload

Apply


➤ BASIC

➤ NETWORK


➤ VoIP

➤ INTERCOM

➤ DOOR PHONE

Service Port Settings 

Web Server Type

HTTP 

HTTP Port

80

HTTPS Port

443

Telnet Port

23

RTP Port Range Start

10000

RTP Port Quantity

200

Apply

| 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 |

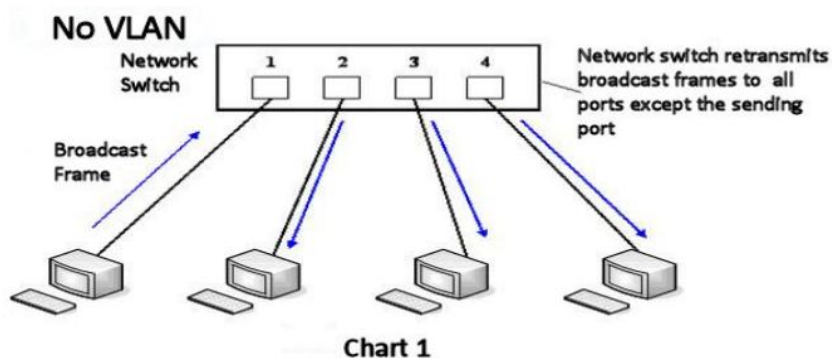
| Field Name | Explanation |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| WAN Settings | |
| Enable Vendor Identifier | Enable or disable Vendor Identifier |
| Vendor Identifier | Configure display Vendor Identifier |
| 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. |
| 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. | |
| <p>NOTE:</p> <ol style="list-style-type: none"> 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. If the system is starting use DHCP to obtain IP and the network address of the DHCP Server and system of LAN network address is the same, then the system after receive DHCP IP, add the LAN network address the last one plus one, and change the distribution of the LAN DHCP Server IP address; If the system started, And then WAN access DHCP, and the network address of the DHCP server distribution and the same LAN, WAN will be unable to get IP access networks. | |
| 802.1X Settings | |
| <div> <div>802.1X Settings</div> <div> <div>802.1x Mode</div> <div>Off</div> </div> <div> <div>Identity</div> <div>admin</div> </div> <div> <div>Password</div> <div>•••••</div> </div> <div> <div>CA Certificate</div> <div></div> <div>Browse</div> <div>Upload</div> </div> <div> <div>Device Certificate</div> <div></div> <div>Browse</div> <div>Upload</div> </div> <div>Apply</div> </div> | |
| User | 802.1X user account |
| Password | 802.1X password |
| Enable 812.1X | Enable or Disable 812.1X |
| CA Certificate | Choose the CA Certificate and then click upload to upgrade |
| Device Certificate | Choose the Device Certificate and then click upload to upgrade |

| Field Name | Explanation |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. | |

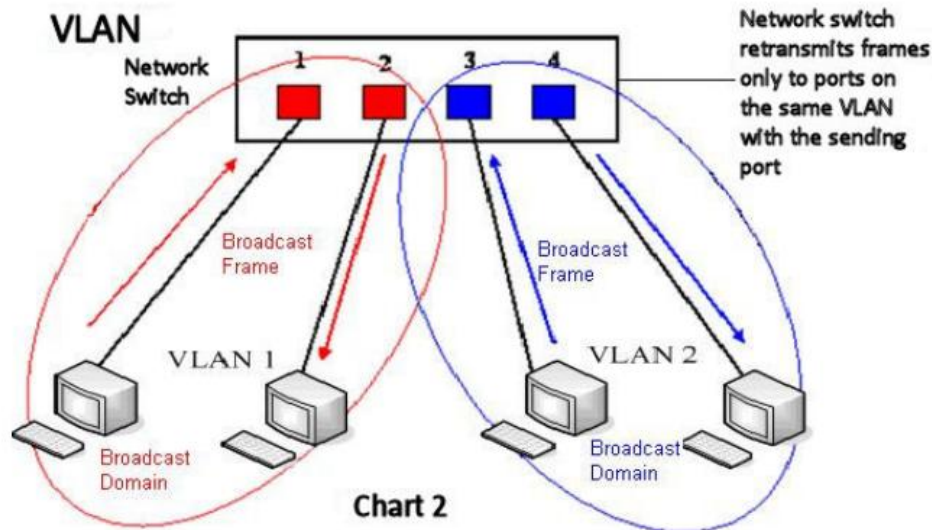
b) QoS&VLAN

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, and 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
QoS&VLAN
WEB FILTER
SECURITY

BASIC
NETWORK
VoIP
INTERCOM
DOOR PHONE
MAINTENANCE
LOGOUT

Link Layer Discovery Protocol (LLDP) Settings

Enable LLDP
☐

Enable Learning Function
☐

Packet Interval(1~3600)
second(s)

Quality of Service (QoS) Settings

Enable DSCP
☐

Audio RTP DSCP
(0~63)

SIP DSCP
(0~63)

Video RTP DSCP
(0~63)

WAN Port VLAN Settings

Enable WAN Port VLAN
☐

802.1P Priority
(0~7)

WAN 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 |

| Field Name | Explanation |
|------------------------------------------|---------------------------------------------------------------|
| 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 |

c) WEB FILTER

| |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 |
| Webpage 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. |

d) 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. |

(3) VOIP

a) SIP

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 | <input type="text" value="5060"/> |
| Domain Realm | <input type="text"/> | Server Name | <input type="text"/> |
| RTP Encryption | <input type="checkbox"/> | Enable Session Timer | <input type="checkbox"/> |
| Registration Expires | <input type="text" value="3600"/> second(s) | Session Timeout | <input type="text" value="0"/> second(s) |
| Keep Alive Type | <input type="text" value="UDP"/> | Keep Alive Interval | <input type="text" value="60"/> second(s) |
| User Agent | <input type="text" value="Voip Phone 1.0"/> | Server Type | <input type="text" value="COMMON"/> |
| DTMF Type | <input type="text" value="RFC2833"/> | RFC Protocol Edition | <input type="text" value="RFC3261"/> |
| Local Port | <input type="text" value="5060"/> | Transport Protocol | <input type="text" value="UDP"/> |
| Enable Rport | <input checked="" type="checkbox"/> | Keep Authentication | <input type="checkbox"/> |
| Enable PRACK | <input type="checkbox"/> | Ans. With A Single Codec | <input type="checkbox"/> |
| Enable Strict Proxy | <input checked="" type="checkbox"/> | Auto TCP | <input type="checkbox"/> |
| Enable DNS SRV | <input type="checkbox"/> | | |

Apply

SIP Global Settings >>

| | | | |
|------------------------|---------------------------------------------|---------------------------------|---------------------------------------------|
| Strict Branch | <input type="checkbox"/> | Enable Group | <input type="checkbox"/> |
| Enable RFC4475 | <input checked="" type="checkbox"/> | Registration Failure Retry Time | <input type="text" value="32"/> second(s) |
| Enable Strict UA Match | <input type="checkbox"/> | DND Return Code | <input type="text" value="486(Busy Here)"/> |
| Reject Return Code | <input type="text" value="486(Busy Here)"/> | Busy Return Code | <input type="text" value="486(Busy Here)"/> |

Apply

SIP

| Field Name | Explanation |
|------------|-------------|
|------------|-------------|

Basic Settings (Choose the sip line to configured)

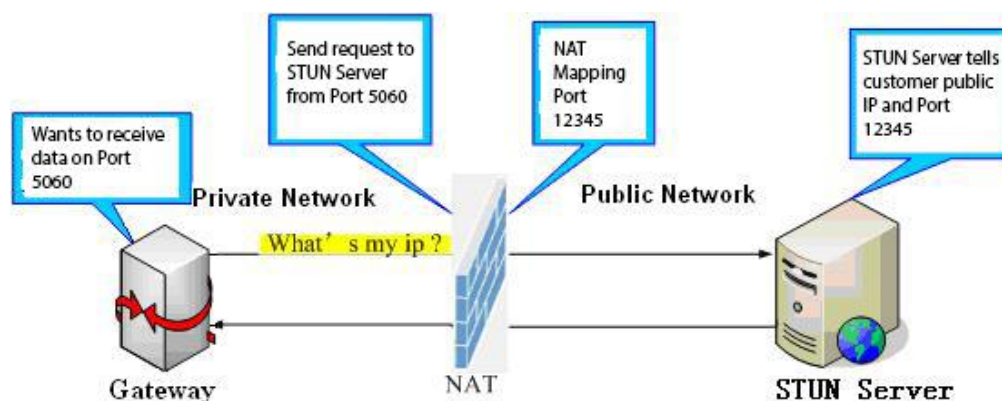
| | |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status | Shows registration status. If the registration is successful will display has been registered, not successful display not registered, the wrong password is displayed 403 errors, account number failure 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. |

| Field Name | Explanation |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 Registrar Server. |
| Server Name | Name of SIP Backup server |
| RTP Encryption | Enable/Disable RTP 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. |
| Protocol Edition | Select SIP protocol version RFC3261 or RFC2543. Default is RFC3261. Used for servers which only support RFC2543. |
| Local Port | SIP port. Default is 5060. |

| Field Name | Explanation |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Transport Protocol | Configuration using the transport protocol, TCP, TLS or UDP, the default is UDP. |
| 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 |
| Enable DNS SRV | Enables use of DNS SRV records |
| 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 |
| Enable RFC4475 | Enable or disable RFC4475, default is enable. |
| 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 |
| Enable Strict UA Match | Enable or disable Strict UA Match |
| 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

Server Port

3478

Binding Period

50

second(s)

SIP Waiting Time

800

millisecond(s)

Local SIP Port

5060

Apply

SIP Line Using STUN

SIP 1

Use STUN

☐

Apply

STUN

| Field Name | Explanation |
|-------------------------------------------|-----------------------------------------------------------------------------------------------|
| STUN NAT Traversal | Shows whether or not STUN NAT Transversal 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) FUNCTION KEY

1-4 programmable key in phone software (depend on hardware), you can configure different feature on each key. You can ref to below indications for each feature. default is NA, means without any feature settings.

| Key | Type | Number 1 | Number 2 | Line | Subtype | Media |
|-------|---------|----------|---------------|------|------------|---------|
| DSS 1 | Hot Key | 602 | 192.168.2.100 | SIP1 | Speed Dial | DEFAULT |
| DSS 2 | None | | | SIP1 | None | DEFAULT |
| DSS 3 | None | | | SIP1 | None | DEFAULT |
| DSS 4 | None | | | SIP1 | None | DEFAULT |

Apply

➤ Key Event Settings

Set the key type to the Key Event.

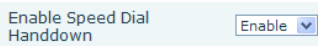
| Key | Type | Number 1 | Number 2 | Line | Subtype | Media |
|-------|-----------|----------|----------|------|----------|---------|
| DSS 1 | Key Event | | | SIP1 | None | DEFAULT |
| DSS 2 | None | | | SIP1 | None | DEFAULT |
| DSS 3 | Hot Key | | | SIP1 | Redial | DEFAULT |
| DSS 4 | Key Event |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

| 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 | Media |
|-------|-----------|----------|----------|------|------------|---------|
| DSS 1 | Hot Key | | | SIP1 | Speed Dial | DEFAULT |
| DSS 2 | None | | | SIP1 | Speed Dial | DEFAULT |
| DSS 3 | Hot Key | | | SIP1 | Intercom | DEFAULT |
| DSS 4 | Key Event | | | SIP1 | None | DEFAULT |
| | Multicast | | | | | |
| | None | | | SIP1 | None | DEFAULT |

| 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 | Media |
|-------|-----------|----------|----------|------|---------|---------|
| DSS 1 | Multicast | | | SIP1 | G.711A | DEFAULT |
| DSS 2 | None | | | SIP1 | G.711A | DEFAULT |
| DSS 3 | Hot Key | | | SIP1 | G.711U | DEFAULT |
| DSS 4 | Key Event | | | SIP1 | G.722 | DEFAULT |
| | Multicast | | | | G.723.1 | |
| | None | | | SIP1 | G.729AB | DEFAULT |

| 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) MEDIA

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

FUNCTION KEY

MEDIA

DND

FEATURE

MCAST

Action URL

> BASIC

> NETWORK

> VoIP

> INTERCOM

> DOOR PHONE

> MAINTENANCE

> LOGOUT

Audio Settings

First Codec

G.711A

Second Codec

G.711U

Third Codec

G.722

Fourth Codec

G.729AB

DTMF Payload Type

101

(96~127)

AMR Payload Type

108

(96~127)

ILBC Payload Type

97

(96~127)

ILBC Payload Length

20ms

G.723.1 Bit Rate

6.3kb/s

G.729AB Payload Length

20ms

SPK Output Volume

7

(1~7)

Broadcast Output Volume

5

(1~7)

Signal Tone Volume

3

(1~7)

Enable VAD

Video Settings

Video Codec

H.264

H.264 Payload Type

117

(96~127)

Video Bit Rate

2Mbps

Video Frame Rate

30fps

Video Resolution

VGA(640*480)

Display Mosaic Frames

RTP Control Protocol(RTCP) Settings

CNAME user:

CNAME host

Apply

> VoIP

> INTERCOM

> DOOR PHONE

> MAINTENANCE

> LOGOUT

Sound Update

Sound Update:

Browser

(*.mp3,*.wav)

Update

Sound Delete

Sound Delete:

Delete

Sound Settings

NAME

SIZE

Apply

| 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 |

| Field Name | Explanation |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DTMF Payload Type | The RTP Payload type that indicates DTMF. Default is 101 |
| AMR Payload Type | Set the AMR Payload type, Numerical based on between 96-127. |
| ILBC Payload Type | Set the ILBC Payload type, Numerical based on between 96-127. |
| ILBC Payload length | Set the ILBC payload length. |
| G.723.1 Bit Rate | Choices are 5.3kb/s or 6.3kb/s. |
| G.729AB Payload Length | G.729AB Payload Length – Adjusts from 10 – 60 mSec. |
| SPK Output Volume | Set the speaker 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. |
| Video Settings | |
| Video Codec | Set the video codec used in video call (H.263, H.264) |
| H.264 Payload Type | Set the H.264 Payload type, Numerical based on between 96-127. |
| Video Bit Rate | Set the bandwidth of video call |
| Video Frame Rate | Set the video frame rate |
| Video Resolution | Set the video resolution, QCIF(176*144), CIF(352*288), VGA(640*480), 4CIF(704*576), 720P(1280x720). Note: 720P only on the four nuclear phone support, And need to choose above 2M of the bandwidth. |
| Display Mosaic Frames | Enable or Disable display mosaic |

| Field Name | Explanation |
|-----------------------------------------------------------|----------------|
| RTP Control Protocol(RTCP) Settings | |
| CNAME user | Set CNAME user |
| CNAME host | Set CNAME host |
| Sound Update | |
| Choose the ring tone files and then click update to apply | |
| Sound Delete | |
| Delete the ring tone file | |
| Sound Settings | |
| Set the ring tong files format is .mp3 and .wav | |

c) DND

| Field Name | Explanation |
|-----------------------------|---------------------------------------|
| DND Methods Settings | |
| DND option | Set the DND option, default is phone. |
| DND Line Settings | |
| SIP1 | Enable or Disable sip1 DND |
| SIP2 | Enable or Disable sip2 DND |
| DND Global Settings | |
| Enable DND Timer | Enable or disable DND timer |
| DND Timer | Set the DND time |
| Enable White List DND | Enable or disable white list DND |

d) FEATURE

FUNCTION KEY

MEDIA

DND

FEATURE

MCAST

Action URL

BASIC

NETWORK

VoIP

INTERCOM

DOOR PHONE

MAINTENANCE

LOGOUT

Feature Settings

Ban Outgoing

☐

Speed Dial Action

HangUp

Enable Telnet

☐

Select Your Tone

United states

Enable Intercom Mute

☐

Enable Intercom Tone

☒

Default Ans Mode

video

Default Dial Mode

video

Enable Auto Answer

Line1 and Line2

Auto Answer Timeout

0

(0~60s)

Call Switched Time

16

(5~50s)

Dial Fixed Length

200

to Send

☐

Apply

| Feature | |
|-------------------------|-----------------------------------------------------------------------------------------|
| Field Name | Explanation |
| Feature Settings | |
| Ban Outgoing | If enabled, no outgoing calls can be made. |
| Speed Dial Action | Default is Speed Dial Hand-down function |
| Enable Telnet | Enable or disable Telnet |
| Select your Tone | Standard configuration signal sound. |
| 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. |
| Default Ans Mode | Set answer mode, default is video . |
| Default Dial Mode | Set dial mode, default is video. |
| Enable Auto Answer | Enable or disable auto answer. |
| Enable Auto Answer | Enable or disable auto answer. |
| Call Switched Time | Set the call switched time. |
| Auto Answer Timeout | Set the auto answer time |
| Dial Fixed Length | The number will be sent to the server after the specified numbers of digits are dialed. |
| Description | device IP description |

e) MCAST

MCAST Settings

Normal Call 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"/> |

Using multicast functionality can be simple and convenient to send notice to each member of the multicast, through setting the multicast key on the device, sending multicast RTP stream to pre-configured multicast address. By on the device configuration monitoring multicast address, listen to and play the group multicast address send RTP stream.

MCAST Settings

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

In the Web interface setting change equipment receiving multicast RTP stream processing mode are: 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 flow. 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: The definition of common call priority, 1 is the most advanced, most low 10
- ✧ Disable: ignore all incoming stream multicast RTP
- ✧ Enable the page priority:

Page determines the priority equipment current in multicast session, how to deal with the new receiving multicast RTP stream, enabling the Page switch priority, the device will automatically ignore the low priority of multicast RTP stream, receive priority multicast RTP stream, and keep the current multicast session in state; If is not enabled, the device will automatically ignores all receive 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, the highest priority.

Note: when a multicast session key by multicast, 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)**

The "group of 1" and "2" and "3" are you setting monitoring multicast name, answer time is displayed on the screen, if you do not set the screen will display the IP: port directly.

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

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 the number of higher priority.

- **Red part (priority)**

Is the general call, non multicast call priority, the smaller the number of high priority, the following will explain how to use this option:

- ✧ The purpose of setting monitoring multicast "group 1" or "2" or "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

f) Action URL

| | FUNCTION KEY | MEDIA | DND | FEATURE | MCAST | Action URL |
|----------------------------|--------------|-------|-----|---------|-------|--------------------------------------|
| Action URL Settings | | | | | | |
| Active URI Limit IP | | | | | | <input type="text"/> |
| Setup Completed | | | | | | <input type="text"/> |
| Registration Success | | | | | | <input type="text"/> |
| Registration Disabled | | | | | | <input type="text"/> |
| Registration Failed | | | | | | <input type="text"/> |
| Off Hook | | | | | | <input type="text"/> |
| On Hook | | | | | | <input type="text"/> |
| Incoming Call | | | | | | <input type="text"/> |
| Outgoing Call | | | | | | <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 Call | | | | | | <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 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) SAFEGUARDING (Only fully functional version support this feature)

| Input Settings | | | |
|-----------------------------------------------|-----------------------------------------------------|-----------------------------------------------|-----------------------------------------------------|
| <input checked="" type="checkbox"/> Input 1 : | | <input checked="" type="checkbox"/> Input 2 : | |
| Trigger Mode | Low Level Trigger(Close Trigger) | Trigger Mode | Low Level Trigger(Close Trigger) |
| Response Mode | <input checked="" type="checkbox"/> Remote Response | Response Mode | <input checked="" type="checkbox"/> Remote Response |

| Output Settings | | | |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-------------------------|
| <input checked="" type="checkbox"/> Output 1 : | | <input checked="" type="checkbox"/> Output 2 : | |
| Output Level | High Level(NO:closed) | Output Duration | 5 (1~600) s |
| Output Trigger Mode | <input checked="" type="checkbox"/> Input 1 Trigger <input checked="" type="checkbox"/> Remote DTMF Trigger <input checked="" type="checkbox"/> Remote SMS Trigger <input checked="" type="checkbox"/> Call State Trigger <input checked="" type="checkbox"/> Emergency Key Trigger | <input type="checkbox"/> Input 2 Trigger 1234 ALERT=OUT1_SOS Talking | Output Last By Duration |
| <input checked="" type="checkbox"/> Output 2 : | | <input checked="" type="checkbox"/> Output 2 : | |
| Output Level | High Level(NO:closed) | Output Duration | 5 (1~600) s |
| Output Trigger Mode | <input type="checkbox"/> Input 1 Trigger <input checked="" type="checkbox"/> Remote DTMF Trigger <input checked="" type="checkbox"/> Remote SMS Trigger <input checked="" type="checkbox"/> Call State Trigger <input checked="" type="checkbox"/> Emergency Key Trigger | <input checked="" type="checkbox"/> Input 2 Trigger 5678 ALERT=OUT2_SOS Talking | Output Last By Duration |

Tamper Alarm Settings

☐ Tamper Alarm
 Alarm command

Reset command

Server & Trigger Ring Type Settings

Server Address

Input 1 Trigger Ring

Input 2 Trigger Ring

Remote DTMF Trigger Ring

Remote SMS Trigger Ring

Tamper Alarm Ring

Alarm Ring Duration
 (1~600) s

| Security Settings | |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Field Name | Explanation |
| Input settings | |
| Input 1 | Open / Close Input port1 |
| 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. |
| Response Mode | Open /Close Input port1 the Remote Response |
| Input 2 | Open /Close Input port2 |
| Trigger Mode | When choosing the low level trigger (closed trigger), detect the input port 2 (low level) closed trigger. |
| | When choosing the high level trigger (disconnected trigger), detect the input port 2 (high level) disconnected trigger. |
| Response Mode | Open /Close Input port2 the Remote Response |
| Output Settings | |
| Output 1/2 | Open/close, Output 1/Output 2 |
| 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. |
| Output Trigger Mode: There are many kinds of trigger modes, multiple choices. | |
| Input port1 trigger | When the input port1 meet to trigger condition, the output port1 will trigger(The Port level time change, By < Output Duration > control) |
| Input port2 trigger | When the input port2 meet to trigger condition, the output port2 will trigger(The Port level time change, By < Output Duration > control) |

| Field Name | Explanation | |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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) | |
| Emergency key 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) | |
| Tamper Alarm Settings | | |
| 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 | Directly stop the alarm from equipment in the Webpage | |
| Server & Trigger Ring Type Settings | | |
| Server Address | Configure remote response server address(including remote response server address and tamper alarm server address) | |
| Input 1 trigger ring | When the input port 1 triggering condition is satisfied, the corresponding ring tone or alarm | |
| Input 2 trigger ring | When the input port 2 triggering condition is satisfied, the corresponding ring tone or alarm | |
| Remote DTMF trigger ring | When received the remote DTMF command, whether to output the ringtone | |
| Remote SMS trigger ring | When receiving the remote SMS instructions, whether to output the ringtone | |
| Tamper alarm ring | When the detected someone tampering the equipment, plays the corresponding ringtone or alarm | |
| Alarm ring duration | duration of alarm ring(not including tamper alarm) | |

(6) DOOR PHONE

a) DOOR PHONE

DOOR PHONE
DOOR CARD
DOOR ACCESS
DOOR LOG

BASIC
NETWORK
VoIP
INTERCOM
DOOR PHONE
MAINTENANCE
LOGOUT

EGS Settings

| | | | |
|--------------------------|---------------------|---------------------------------|----------------------|
| Switch Mode | monostable | Keypad Mode | Dial and Password |
| Switch-On Duration | 5 (1~600 seconds) | Talk Duration | 120 (20~600 seconds) |
| Remote Password | * | Local Password | 6789 |
| Description | 方位后门 | Enable Access Table | Enable |
| Hot Key Dial Mode Select | Main-Secondary | Day End Time | 18:00 (00:00~23:59) |
| Day Start Time | 06:00 (00:00~23:59) | Port of Log Server | 514 |
| Address of Log Server | 0.0.0.0 | Enable Indoor Open | Enable |
| Enable Log Server | Disable | Limit Talk Duration | Enable |
| Enable Card Reader | Enable | Remote Access Code Check Length | 4 (1~6) |
| Door Unlock Indication | Long beeps | | |

Apply

| 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. | i31 Video Sip 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 |

b) DOOR CARD

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 (If you don't add rules, that will be just the temporary 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.

| 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 | |
| You can add new access rules, or select an existing project within the list to modify | |
| 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 |
| 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. | |
| 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 |

d) DOOR LOG

According to open event log, can record up to Twenty thousand 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.

Door Opening Log

Page: 1 [Pre](#) [Next](#) [Delete All](#) [Right Click here to Save Logs](#)

| Result | Door Opening Time | Duration | Access Name | Access ID | Type |
|---------|---------------------|-------------|-------------|------------|----------------|
| Success | 2015/11/12 18:15:25 | 5 second(s) | Amy | 0009479957 | valid Card |
| Success | 2015/11/12 18:14:56 | 5 second(s) | | 0009479957 | Temporary Card |
| Success | 2015/11/12 18:13:37 | 5 second(s) | | | Local |

[Export CallLogs List](#) [Right Click here to Save CallLogs](#)

| Field Name | Explanation |
|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Door Opening Log | |
| Result | Show the results of door opening |
| 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 valid ; 4 invalid. |
| Export CallLogs List | |
| Right Click here to Save CallLogs , Right-click it and select save target to your computer. | |

(7) 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. |
| Config Encryption Key | Encryption key for the configuration file |

| Field Name | Explanation |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Common Config Encryption Key | Encryption key for common configuration file |
| Download Fail Check Times | Download failed and check times |
| Save Auto Provision Information | Save the auto provision username and password in the phone until the server url changes |
| Download CommonConfig enabled | Enable or disable download commonconfig |
| Download DeviceConfig enabled | Enable or disable download deviceconfig |
| 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. |

| Field Name | Explanation |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Update Mode | 1. Disable – no update 2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update interval |
| TR069 Settings | |
| Enable TR069 | Enable/Disable TR069 configuration |
| Enable TR069 Warning Tone | Enable or disable TR069 Warning Tone |
| 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. |

b) SYSLOG

Syslog Settings

Server Address: 0.0.0.0

Server Port: 514

MGR Log Level: None

SIP Log Level: None

Enable Syslog: ☐

Apply

Web Capture

Start Stop

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

The screenshot shows the 'CONFIG' tab selected in the top navigation bar. The left sidebar lists menu items: BASIC, NETWORK, VoIP, INTERCOM, DOOR PHONE, and MAINTENANCE (highlighted). The main content area has three sections:

- Save Configuration:** A message 'Click "Save" button to save the configuration files!' with a 'Save' button below it.
- Backup Configuration:** A message 'Save all network and VoIP settings.' followed by two links: 'Right Click here to Save as Config File(.txt)' and 'Right Click here to Save as Config File(.xml)'.
- Reset Content:** A message 'Click "Clear" button to clear the Contacts CallLogs and Photos!' with a 'Clear' button below it.

This screenshot shows the 'Reset Configuration' section. It includes a message 'Click "Clear" button to reset the configuration files!'. Below this are two boxes: 'Content to Reset' containing 'Dsskey_Module' and 'DialPlan_Module', and 'Content to Keep' containing 'SIP_Module'. Between these boxes are two arrows (right and left) for moving items. A 'Clear' button is at the bottom.

| 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." |
| Reset Content | Click the "clear" button can reset phone records and photos. |
| Reset Configuration | To reset the system and Automatic restart the equipment. |

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, the user can accord need to add and remove users, can modify existing user permissions.

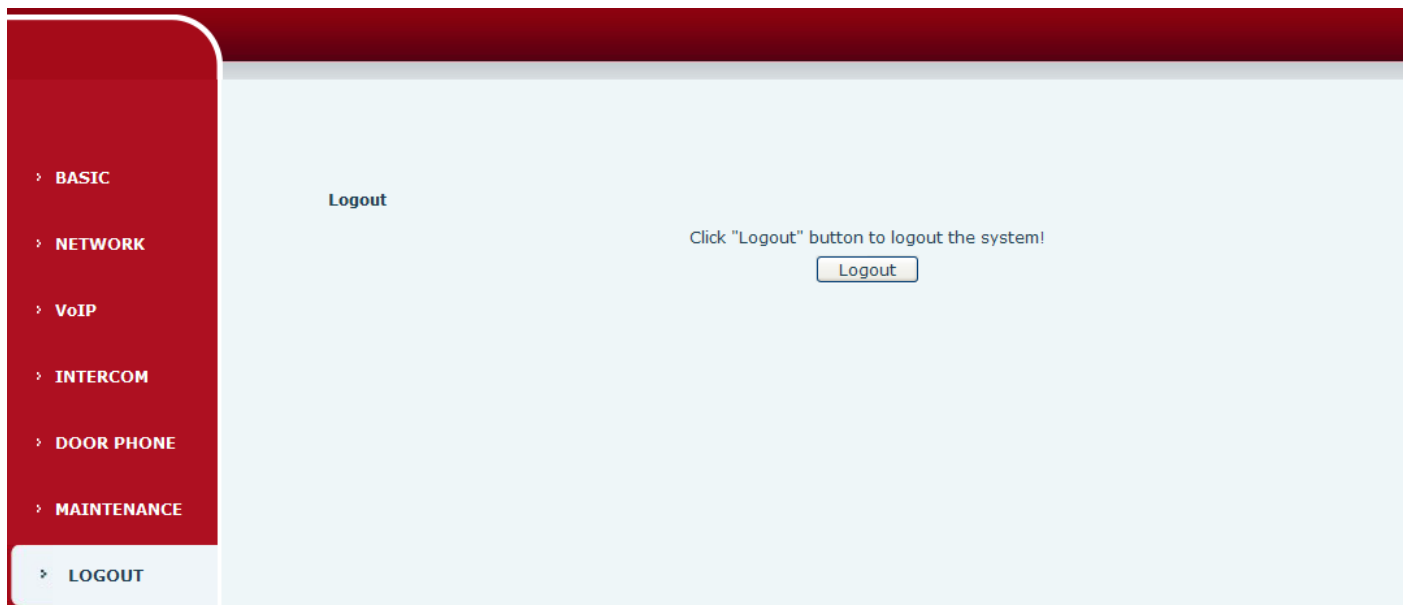
| Field Name | Explanation |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| 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 cause the equipment to reboot immediately.

Note: Be sure to save the configuration before rebooting.

(8) LOGOUT



Click <Logout> from the web, visit next time when need to enter your user name and password.

E. Appendix

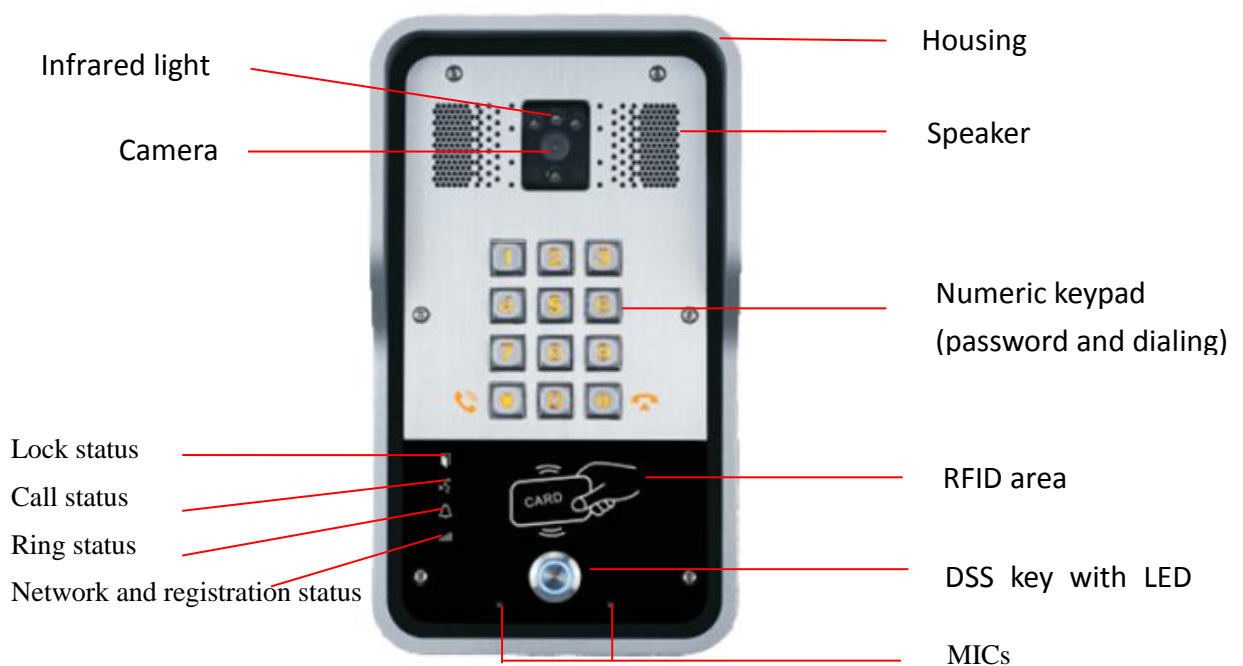
1. Technical parameters

| | | |
|-----------------------------------|---------------------------------|---------------------------------------------------------|
| Communication protocol | | SIP 2.0(RFC-3261) |
| Main chipset | | Freescall i.MX 6Quad |
| Key | DSS key materials | Stainless steel |
| | DSS Key | 1 or 2 |
| | Numeric keyboard | Support |
| Audio | Audio amplifier | 3W |
| | Volume control | Adjustable |
| | Full duplex speakerphone | Support (AEC) |
| | DTMF TYPE | In-band, Out-of-band(RFC 2833), SIP INFO |
| | wideband speech code | G.722 |
| | Narrowband speech code | G711A/u, G.723.1, G.729AB, ILBC, AMR |
| Video | Scope of broadband | 64kbps~4Mbps |
| | Video Framerate | 10~30fps |
| | resolution | CIF, QCIF, VGA, 4CIF, 720P(HD) |
| | Video Codec | H.263, H.264 |
| 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 |
| 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% - 95% |
| Storage temperature | | -40°C to 70°C |
| Installation way | | Wall mounted or In-wall |
| Dimension | | Wall mounted: 223*130*74mm In-wall: 270*150*61mm |

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

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 | <input type="text" value="0003476384"/> | <input type="button" value="Add"/> |
| Type | <input type="text" value="Issuer"/> | |

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 | <input type="text" value="0003408919"/> | <input type="button" value="Add"/> |
| Type | <input type="text" value="Revocation"/> | |

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>>

| | |
|-----------------------------------------|---------------------------------------|
| <input type="text" value="0006892245"/> | <input type="button" value="Delete"/> |
|-----------------------------------------|---------------------------------------|

● 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 | <input type="text" value="Card Issuing"/> | <input type="button" value="Apply"/> |
| | <input type="text" value="Normal"/> <input type="text" value="Card Issuing"/> <input type="text" value="Card Revoking"/> | |

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

Administrator Table>>

Normal
Card Issuing
Card Revoking

- 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

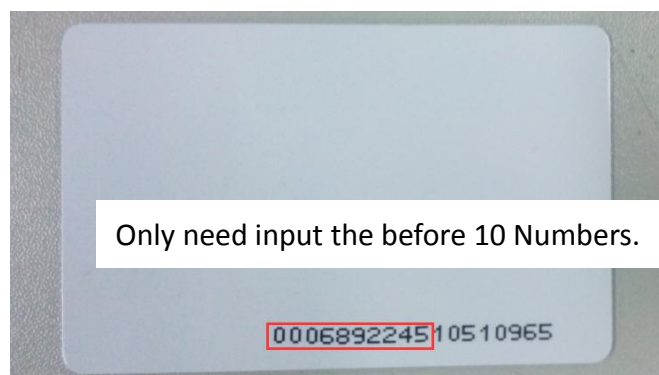
Methods 2: use to add few cards

- 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 batch delete cards or delete few cards.

- 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 cards.

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