i20T

IP Voice Access User Manual

Safety Notices

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

Directory

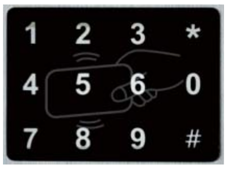
A. Product introduction

Voice Intercom i20T voice entrance guard is a full digital network door phone，its core part adopt mature VoIP solution(Broadcom1190 chipset), stable and reliable performance, Hands-free adopting digital full-duplex mode, Voice loud and clear, generous appearance, solid durable, easy for installation, comfortable keypad, low power consumption.

i20T voice entrance guard support entrance guard control, Voice Intercom, ID card and keypad remote to open the door.

1. Appearance of the product

2. Button description

Buttom	Description	Function
	digit keyboard	enter the password to open the door or make a calling
	Programmable keyboard	Can be set to a variety of functions, to meet the needs of different occasions
	call status indicators	standby-light off ring-2 sec.glitter hold/be hold-1sec. Glitter communication by telephone-long bright
	power led(left)	Long bright after power supply
	Network and SIP status indicator light(right)	network failure 1 sec. glitter network normal light off registration failure 3 sec. glitter registration succeed long bright

B. Start Using

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

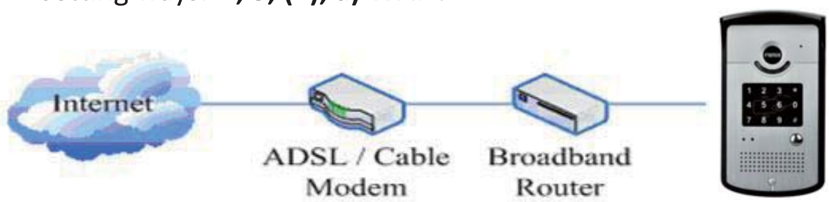
1. Connecting the power supply and the network

1) Connecting network

In prior to this step, please check if your network can work normally and have capacity of broadband internet access.

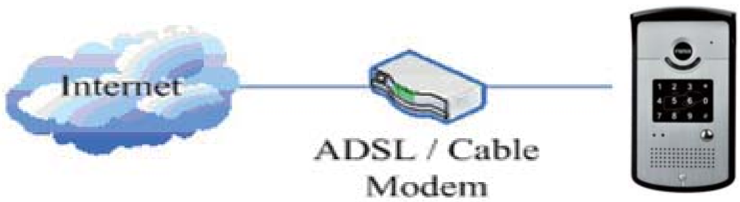
- **Broadband Router**

  Connect one end of the network cable to the intercom WAN port, the other end is connected to your broadband router's LAN port, so that the completion of the network hardware connections. In most cases, you must configure your network settings to DHCP mode. Please refer to the detailed setting ways: **D, 3, (2), a) WAN.**



- **No Broadband Router**

  Connect one end of the network cable to the intercom WAN port, the other end is connected to the broadband modem to your LAN port, so that the completion of the network hardware connections. In most cases, if you are using the cable broadband, you must configure your network settings to DHCP mode; if you are using the ADSL, you must configure your network settings to PPPoE mode. Please refer to the detailed setting ways: **D, 3, (2), a) WAN.**

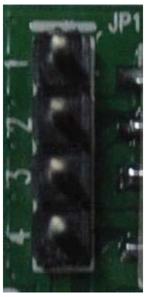


2) Connecting power supply

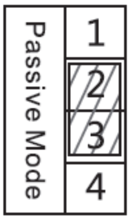
i20T voice access can use 12V/DC power supply or an external power supply in POE mode. When using POE mode, please make sure the network support POE, access network power supply can be achieved.

CN7						
1	**2**	**3**	**4**	**5**	**6**	**7**
+12V	-12V	NC	COM	NO	S_I	S_O
12V 1A/DC		Electric Lock			Indoor switch	

3) Electric Lock Connection Driver Option

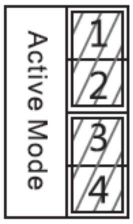


JP1



Jumper in passive mode

JP1



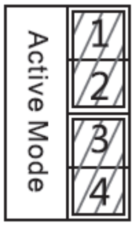
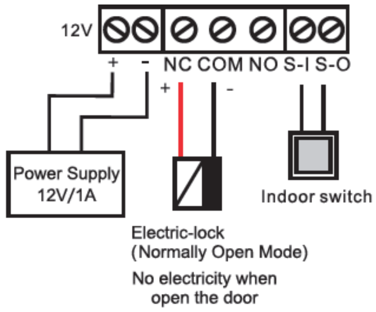
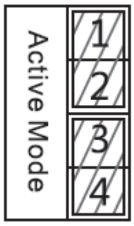
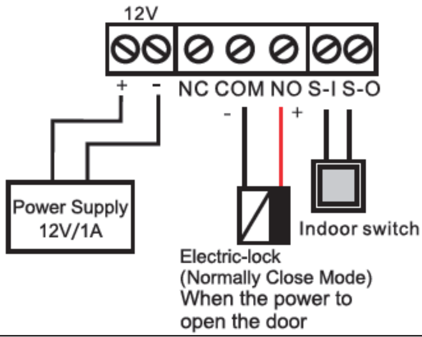
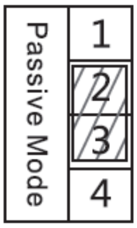
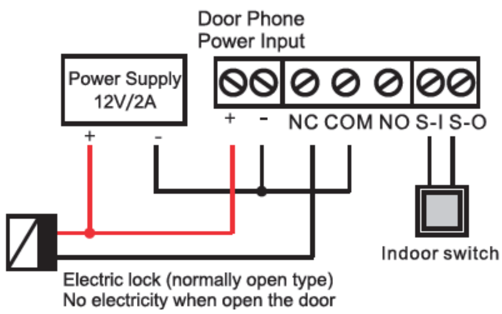
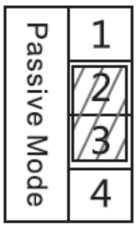
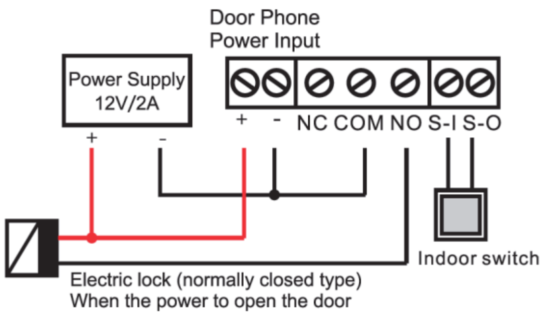
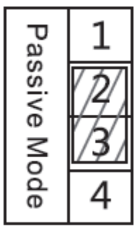
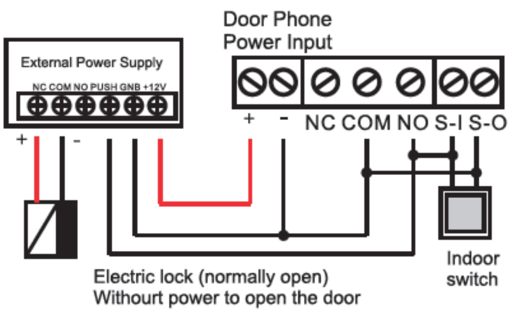
Jumper in active mode

[Notice]When electric current of the electric lock is lower than 500mA/12V, it uses the internal driven mode, by the POE or 12V DC to control the electric lock; When the electric current of the electric lock is higher than 500mA/12V, it uses the external driven mode, use specialized DC power to control the electric lock.

4) Wiring instructions

Relay connection description

- NO: Under the idle state is disconnected (normally open);
- COM: Contactor of the Relay (middle);
- NC: Under the idle state is connected (normally close).

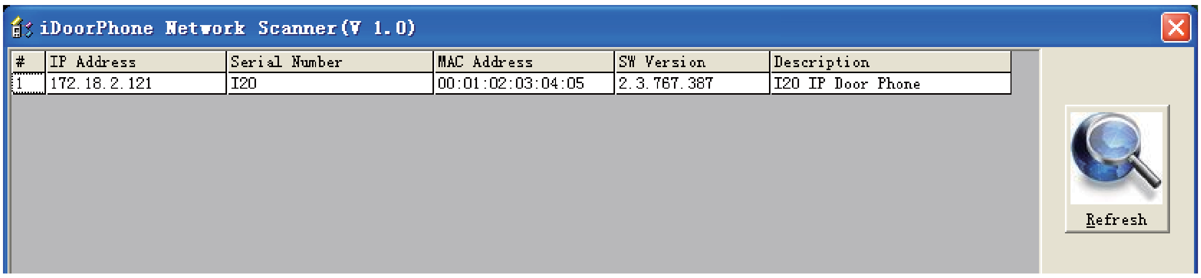
Driving Mode		Electric lock		Jumper	Connections
Active	Passive	NO	NC	JP1	
√		√			
√			√		
	√	√			
	√		√		
	√	√			

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.

- A long press # key 3 seconds, automatic voice playing device's IP address, or use the "iDoorPhoneNetworkScanner.exe " software to find the IP address of the device;
- 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);



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

3. End call

Enable Release key hang up to end call.

4. Call record

The device provides 300 call recording, 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 (Basic->call log)

5. Open the door operation

Through the following four ways to open the door:

1) Local open the door 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 and press # key to open the door (access code to be included in the list to access configuration).

4) Through the RFID CARDS to open the door.

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

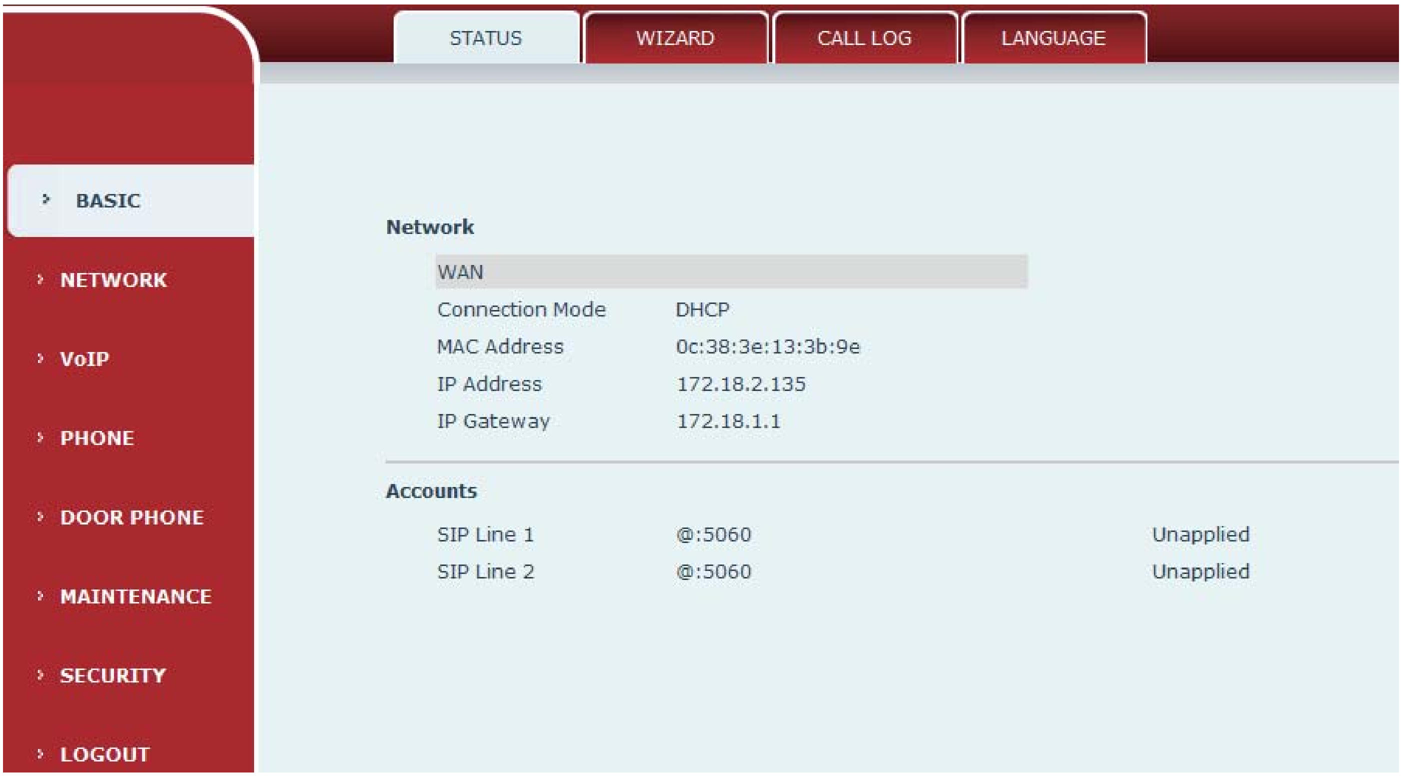
There are two levels of access: root level and general level. A user with root level access can browse and set all configuration parameters, while a user with general level can set all configuration parameters except server parameters for SIP.

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

3. Configuration via WEB

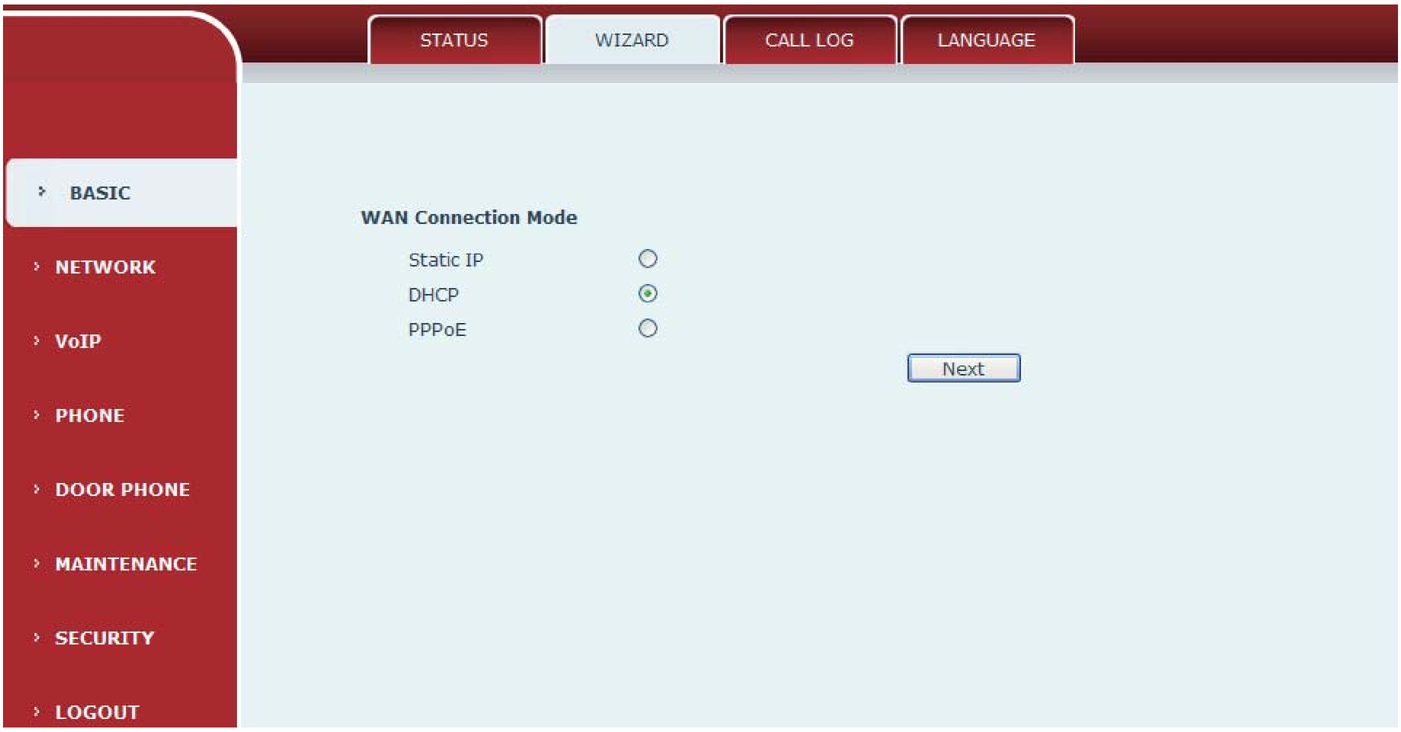
(1) BASIC

a) STATUS



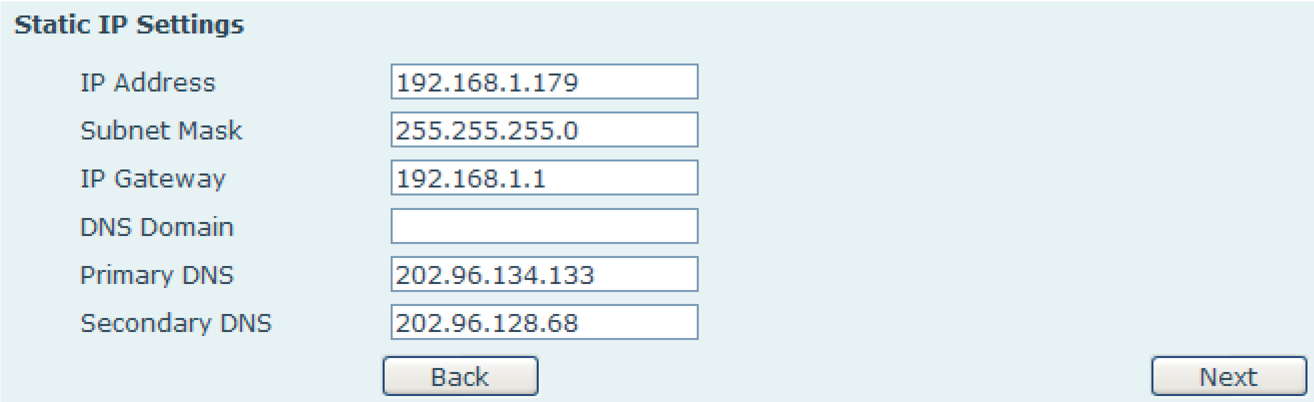
Status	
Field Name	**Explanation**
Network	Shows the configuration information for WAN and LAN port, including connection mode of WAN port (Static, DHCP, PPPoE),MAC address, IP address of WAN port.
Accounts	Shows the phone numbers and registration status for the 2 SIP LINES and 1 IAX2 server.

b) WIZARD



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

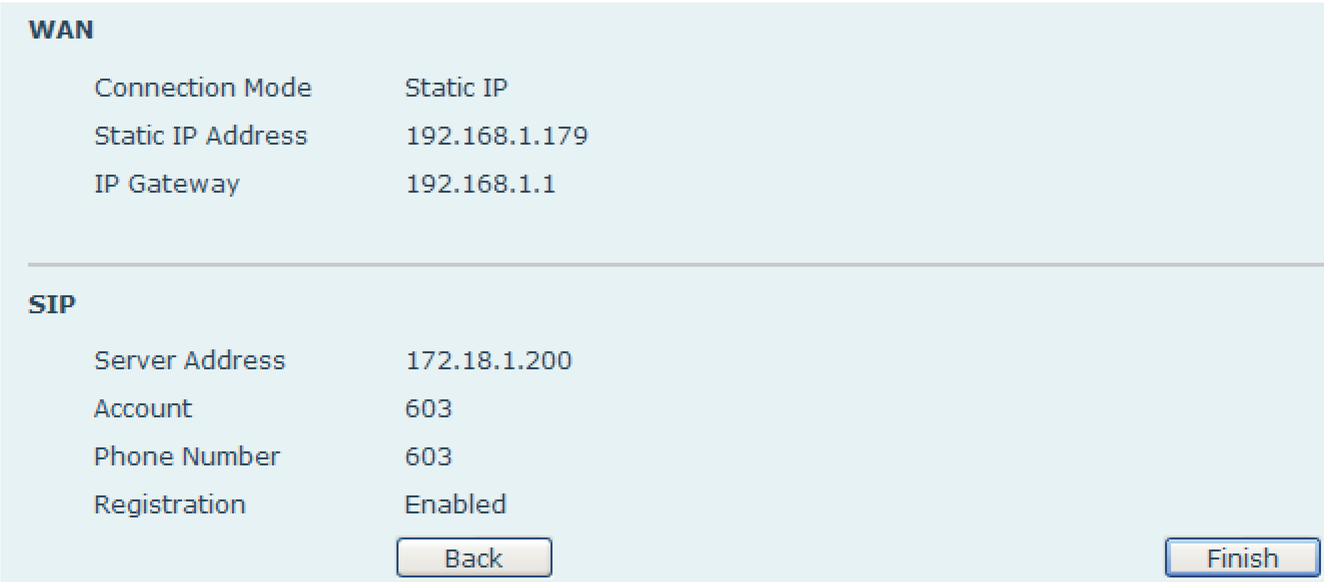
Field Name	Explanation



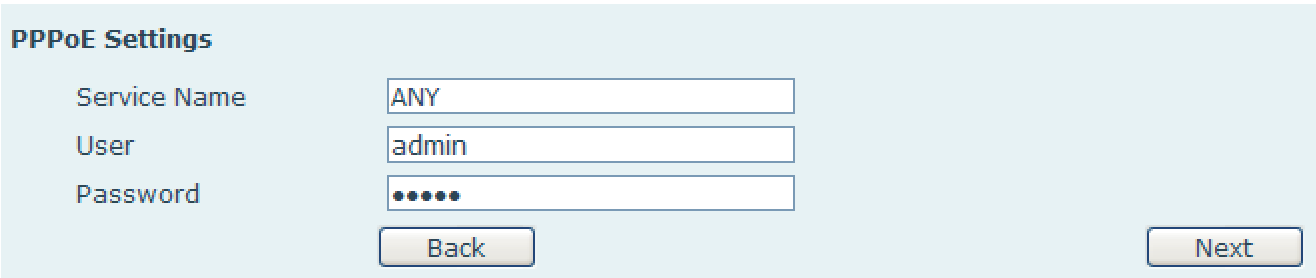
Field Name	Explanation
Static IP address	Please enter the Static IP address
Subnet Mask	Please enter the Subnet Mask
IP Gateway	Please enter the IP Gateway
DNS Domain	Set the DNS domain suffix. When the user enter the domain name DNS address cannot be resolved, the domain equipment to resolve in the domain name.
Primary DNS	Please enter the Primary DNS server address
Secondary DNS	Please enter the Secondary DNS server address
Quick SIP Settings	

Field Name	Explanation
Display Name	The name shown in caller ID
Server Address	SIP server address either IP address or URI
Server Port	SIP server port (usually 5060)
User	Login name or Authentication ID。
Password	SIP password
SIP User	Phone number
Enable Registration	Submits registration information. Normally checked

Field Name	Explanation
Displays detailed information for manual configuration.	



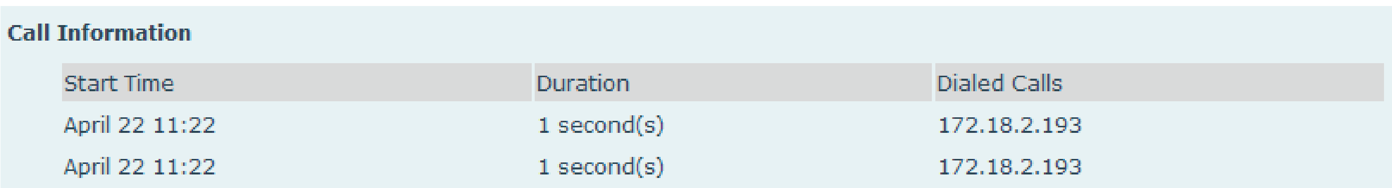
After selecting DHCP and clicking NEXT, the Quick SIP Settings screen will appear. Click Back to return to the Wizard screen. Click Next to go to the Summary screen.	
If PPPoE is selected, this screen will appear. Enter the information provided by the ISP. Click Next to go to Quick SIP Setting. Click Back to return to the Wizard screen.	



Service Name	PPPoE Service name, Usually the default value.
User	ADSL user account
Password	ADSL password
Click Finish button to save settings and reboot. After the reboot, SIP calls can be made.	

c) CALL LOG

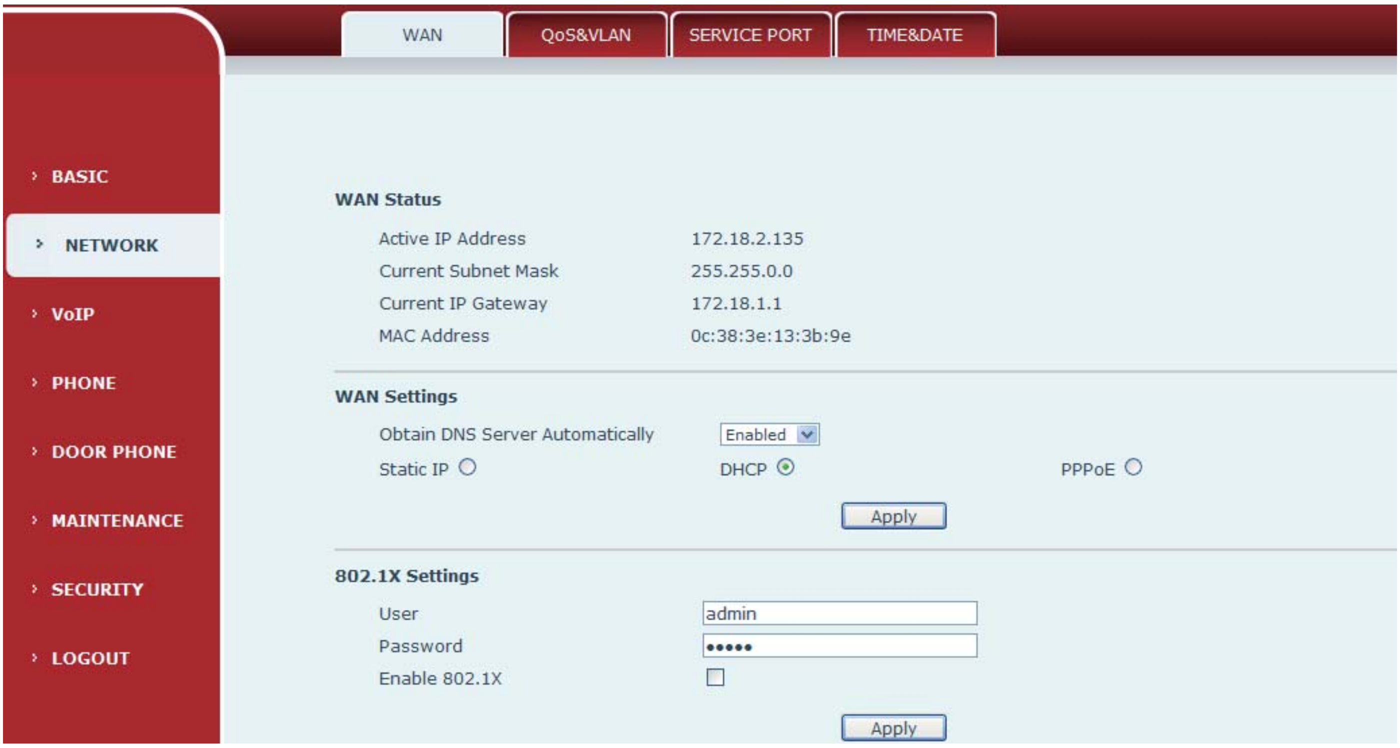
Outgoing call logs can be seen on this page

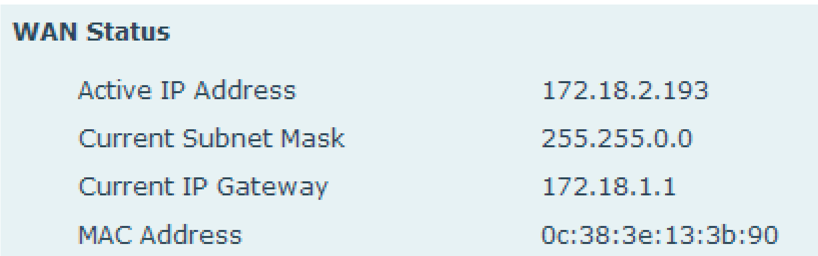


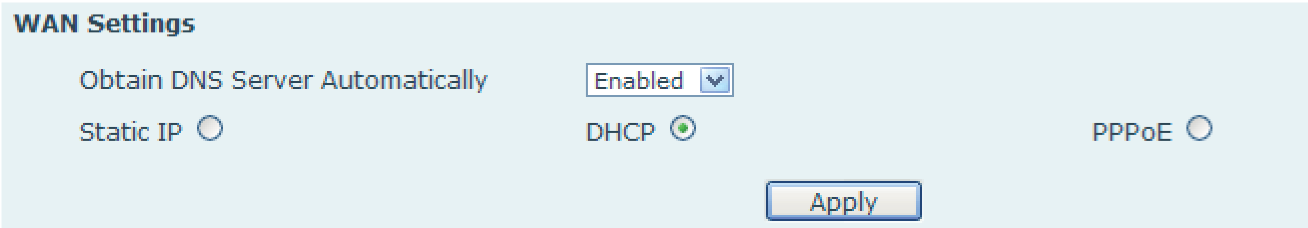
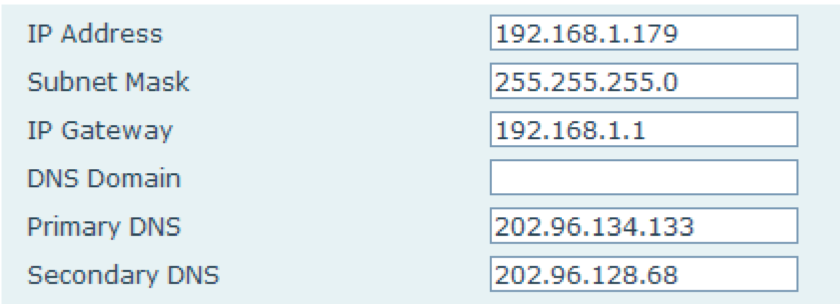
Call log	
Field Name	**Explanation**
Start time	Start time of the outgoing call
Duration	Duration of the outgoing call
Dialed calls	Account, protocol, and line of the outgoing call
Call type	Placed, Missed, Received

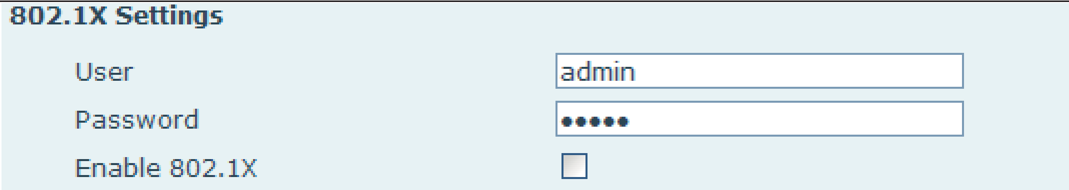
(2) NETWORK

a) WAN



WAN	
Field Name	**Explanation**
	
Active IP address	The current IP address of the equipment

Field Name	Explanation
Current subnet mask	The current Subnet Mask
Current IP gateway	The current Gateway IP address
MAC address	The MAC address of the equipment
	
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.	
	
Static IP address	Please enter the Static IP address
Subnet mask	Please enter the Subnet Mask
Gateway	Please enter the IP Gateway
DNS Domain	Set the DNS domain suffix. When the user enter the domain name DNS address cannot be resolved, the domain equipment to resolve in the domain name.
Primary DNS	Please enter the Primary DNS server address
Secondary DNS	Please enter the Secondary DNS server address

Field Name	Explanation
802.1X Settings	
	
User	802.1X user account
Password	802.1X password
Enable 812.1X	Open/Close 812.1X
After entering the new settings, click the APPLY button. The equipment will save the new settings and apply them. If a new IP address was entered for the equipment, it must be used to login to the phone after clicking the APPLY button.	

b) 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.

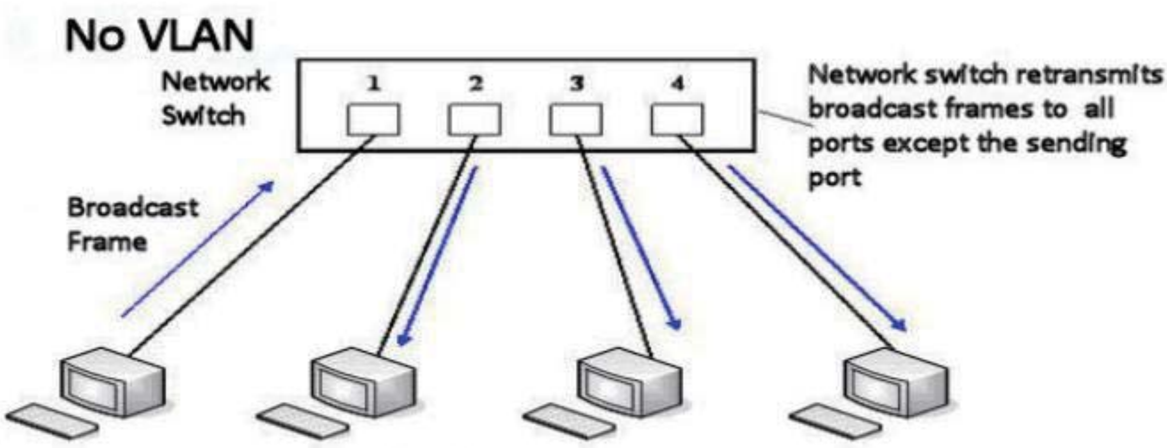
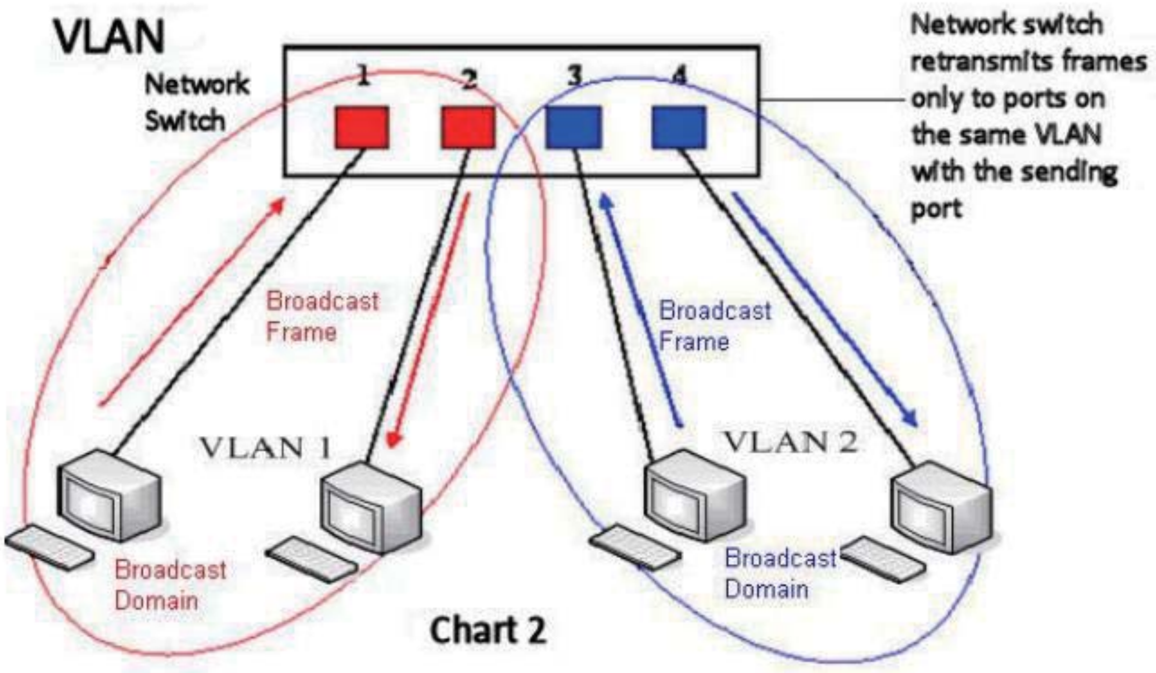
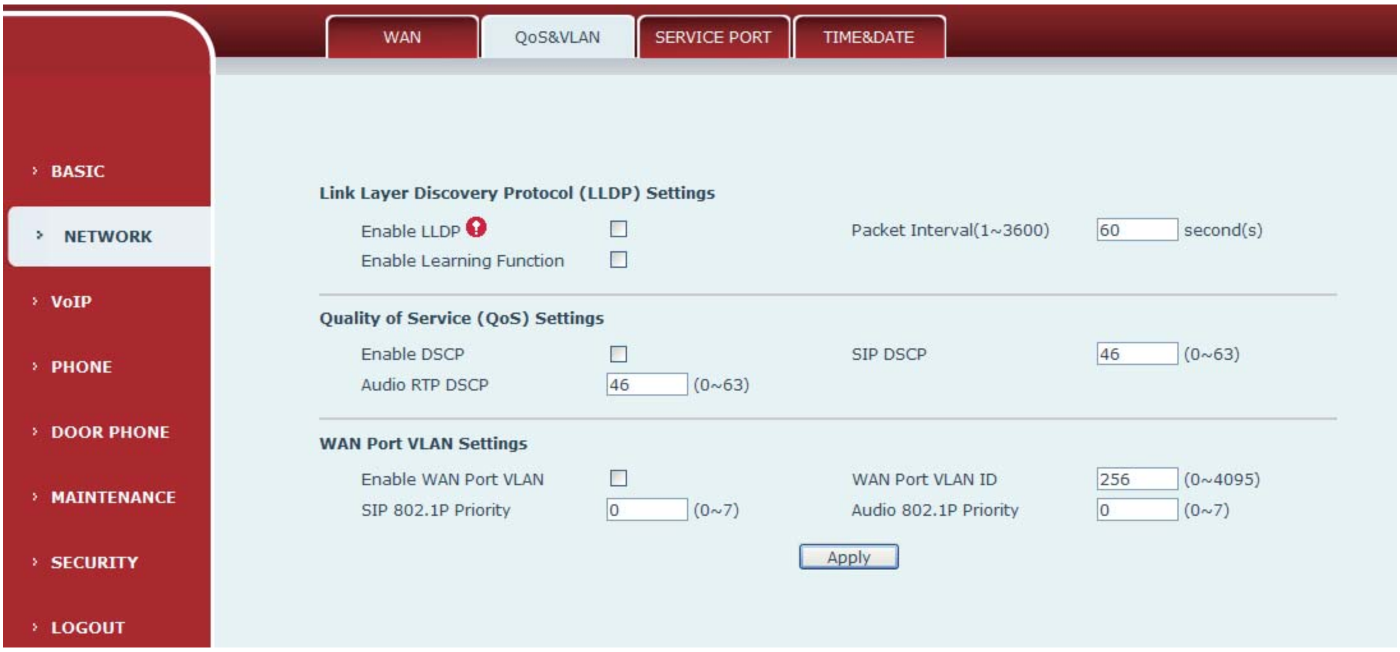


Chart 1

- 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.



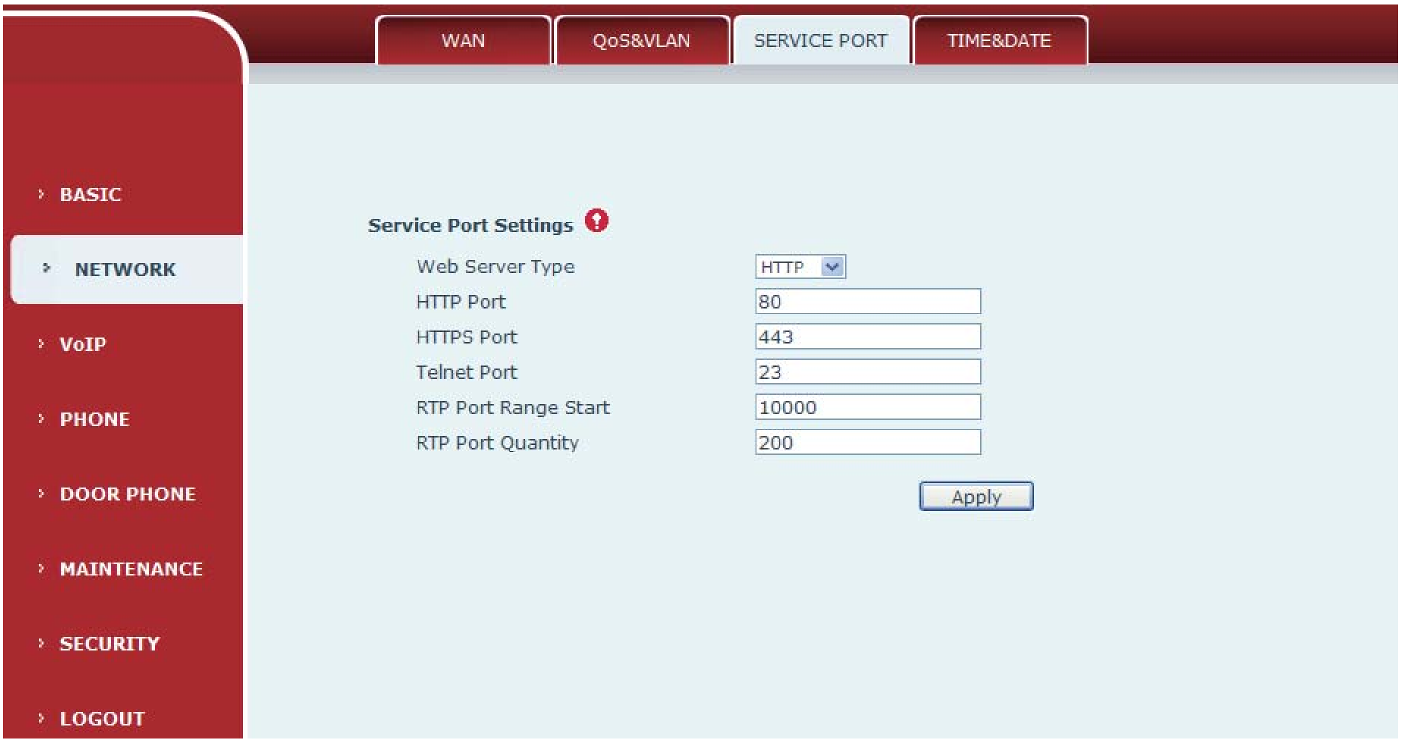
Note: In practice, VLANs are distinguished by the use of VLAN IDs.



QoS&VLAN	
Field Name	**Explanation**
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
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 8021.p priority. Range is 0-7
Audio 802.1P Priority	Specify the value of the voice 802.1p priority. Range is 0-7

c) SERVICE PORT

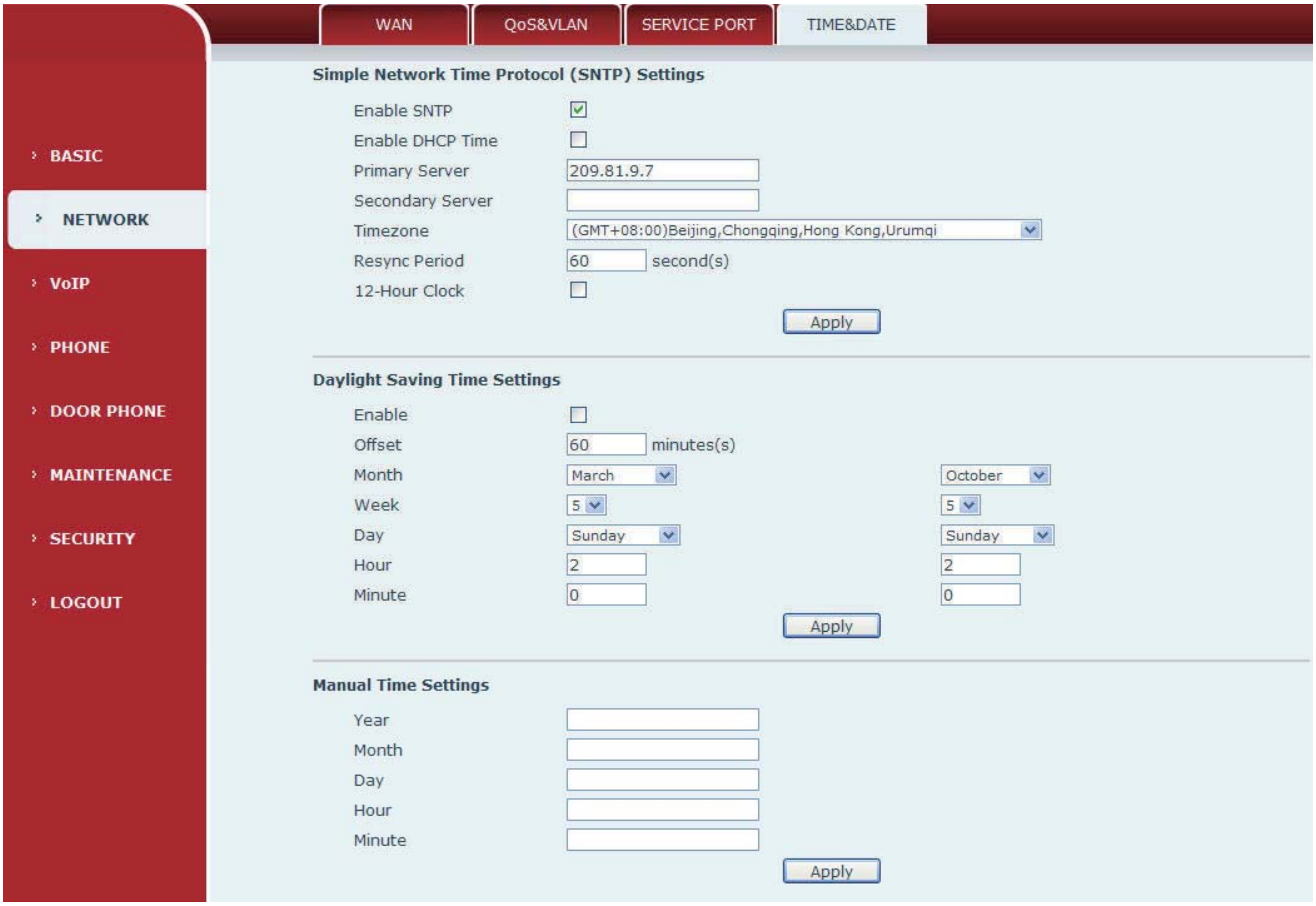
Set the port values for Telnet/HTTP/RTP on this page.



Service port	
Field Name	**Explanation**
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: 1) Any changes made on this page require a reboot to become active. 2) It is suggested that changes to HTTP Port and Telnet ports be values greater than 1024.Values less than 1024 are reserved. 3) If the HTTP port is set to 0, HTTP service will be disabled.	

d) TIME&DATE

Set the time zone and SNTP (Simple Network Time Protocol) server on this page. Daylight savings time configuration and manual time and date entry are also done on this page.



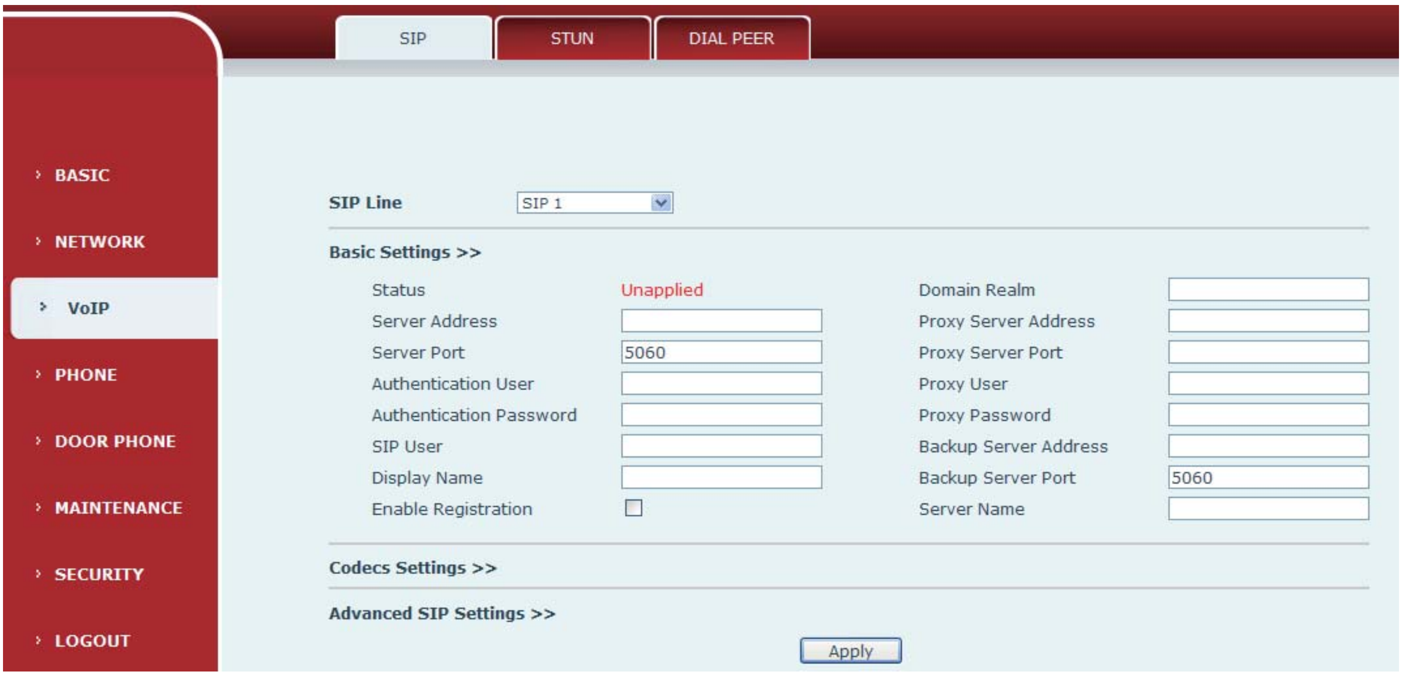
TIME&DATE	
Field Name	**Explanation**
SNTP Settings	
Enable SNTP	Enable or Disable SNTP
DHCP Time	If this is enabled, equipment will synchronize time with DHCP server
Primary Server	IP address of Primary SNTP Server
Secondary Server	IP address of Secondary SNTP Server
Time zone	Local Time Zone
Resync Period	Time between resync to SNTP server. Default is 60 seconds.
12-Hour Clock	If checked, clock is 12 hour mode. If unchecked, 24 hour mode. Default is 24 hour mode.

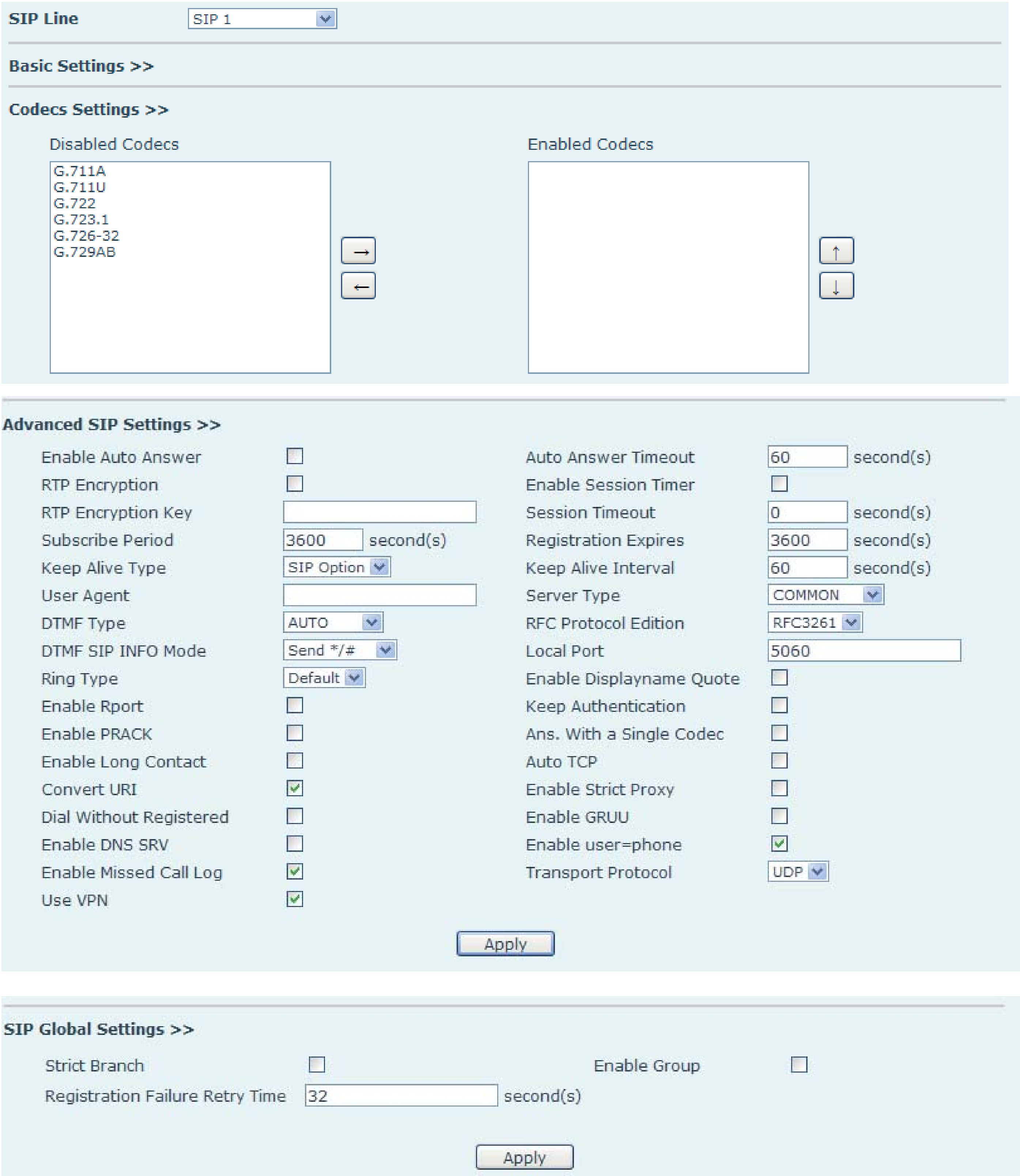
Field Name	Explanation
Daylight Saving Time Settings	
Enable	Enable daylight saving time
Offset(minutes)	DST offset. Default is 60 minutes
Month	Start and end month for DST
Week	Start and end week for DST
Day	Start and end day for DST
Hour	Start and end hour for DST
Minute	Start and end minute for DST
Manual Time Settings	
Enter the values for the current year, month, day, hour and minute. All values are required. Be sure to disable SNTP service before entering manual time and date.	

(3) VOIP

a) SIP

Configure a SIP server on this page




SIP Line
SIP 1
Basic Settings >>
Codecs Settings >>
Disabled Codecs
G.711A
G.711U
G.722
G.723.1
G.726-32
G.729AB
Enabled Codecs
Advanced SIP Settings >>
Enable Auto Answer
RTP Encryption
RTP Encryption Key
Subscribe Period
3600
second(s)
Keep Alive Type
SIP Option
User Agent
DTMF Type
AUTO
DTMF SIP INFO Mode
Send */#
Ring Type
Default
Enable Rport
Enable PRACK
Enable Long Contact
Convert URI
Dial Without Registered
Enable DNS SRV
Enable Missed Call Log
Use VPN
Auto Answer Timeout
60
second(s)
Enable Session Timer
Session Timeout
0
second(s)
Registration Expires
3600
second(s)
Keep Alive Interval
60
second(s)
Server Type
COMMON
RFC Protocol Edition
RFC3261
Local Port
5060
Enable Displayname Quote
Keep Authentication
Ans. With a Single Codec
Auto TCP
Enable Strict Proxy
Enable GRUU
Enable user=phone
Transport Protocol
UDP
Apply
SIP Global Settings >>
Strict Branch
Enable Group
Registration Failure Retry Time
32
second(s)
Apply

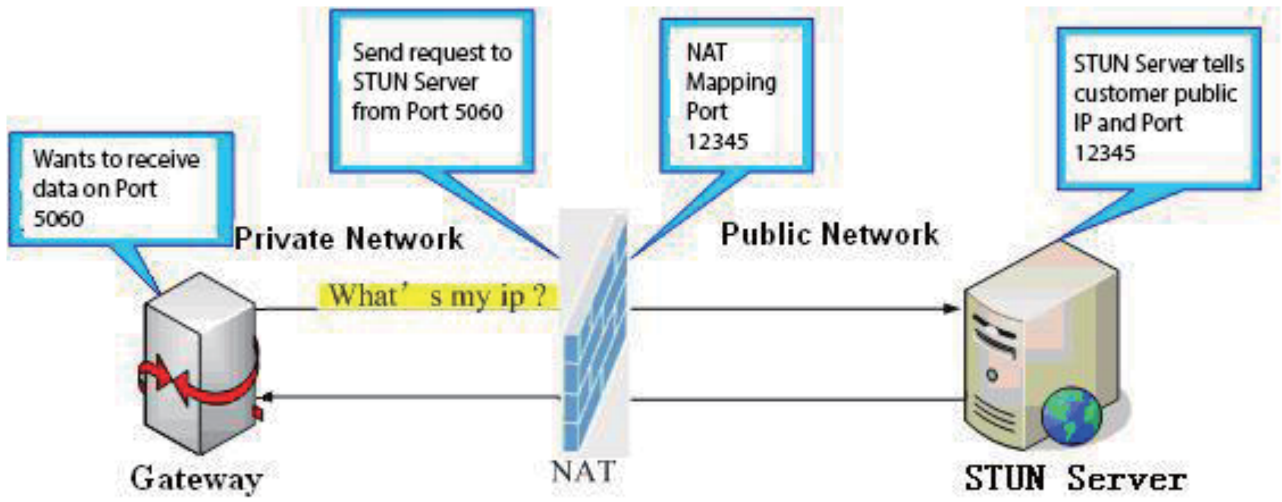
SIP	
Field Name	**Explanation**
Choose the sip line to configured (SIP 1 – SIP2). Click the dropdown arrow to select the line.	
Basic Settings	
Status	Shows registration status. If the registration is successful will display has been registered, not successful display not registered, the wrong password 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.
User	SIP account name (Login ID).
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.
Domain Realm	SIP Domain if different than the SIP Registrar Server.
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 Proxy server address	Backup SIP Server Address or URI (This server will be used if the primary server is unavailable)
Backup Proxy server port	Backup SIP Server Port
Server name	Name of SIP Backup server
Codecs Settings	
Disable Codecs /Enable Codecs	Click on the desired codec to select it. Then click the Left/right arrow to move to the Enabled or Disabled List. Use the Up/Down arrow to change the priority of enabled codecs.
Advanced SIP Settings	
Enable Auto Answer	Activate Auto Answer mode.
RTP Encryption	Enable/Disable RTP Encryption.
RTP Encryption Key	Enable/Disable RTP Encryption key.

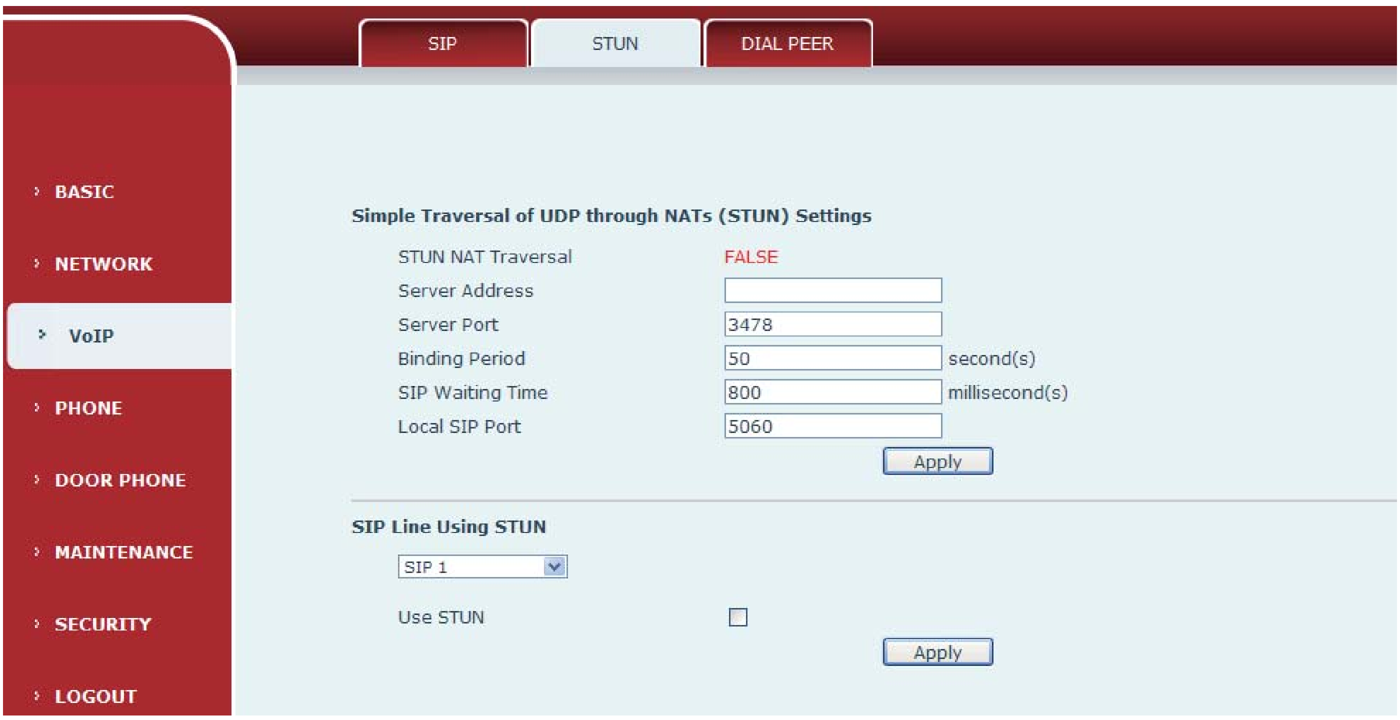
Field Name	Explanation
Subscribe Period	Time interval between MWI Subscribe Messages.
Keep Alive Type	Specifies the NAT keep alive type. If SIP Option is selected, the equipment will send SIP Option sip messages to the server every NAT Keep Alive Period. The server will then respond with 200 OK. If UDP is selected, the equipment will send a UDP message to the server every NAT Keep Alive Period.
User Agent	Set SIP User Agent value.
DTMF Type	DTMF sending mode. There are four modes: ● In-band ● RFC2833 ● SIP_INFO ● AUTO Different VoIP Service providers may require different modes.
DTMF SIP INFO Mode	You can chose Send 10/11 or Send */#
Ring Type	Set ring tone. There are 9 standard options and 3 user options.
Enable Rport	Enable/Disable support for NAT traversal via RFC3581 (Rport).
Enable PRACK	Enable or disable SIP PRACK function. Default is OFF. It is suggested this be used.
Enable Long Contact	Allow more parameters in contact field per RFC 3840
Convert URI	Converts # to %23 when sending URI information.
Dial Without Registered	Allow outgoing calls without registration.
Enable DNS SRV	Enable support RFC2782
Enable Missed Call Log	If enabled, the phone will save missed calls into the call history record.
Use VPN	Enable SIP use VPN for every line individually, not all of them
Auto Answer Timeout	Set Auto Answer Timeout
Enable Session Timer	If enabled, this will refresh the SIP session timer per RFC4028.
Session Timeout	Refresh interval if Session Timer is enabled.
Registration Expires	SIP re-registration time. Default is 3600 seconds. If the server requests a different time, the phone will change to that value.
Keep Alive Interval	Set the NAT Keep Alive interval. Default is 60 seconds
Server Type	Configures phone for unique requirements of selected server.

Field Name	Explanation
RFC 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.
Enable Display name Quote	Puts quotation marks around the display-name in SIP messages. For servers that require this.
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
Ans. With a Single Codec	If enabled phone will respond to incoming calls with only one codec.
Auto TCP	Force the use of TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes
Enable Strict Proxy	Enables the use of strict routing. When the phone receives packets from the server it will use the source IP address, not the address in via field.
Enable GRUU	Support for Globally Routable User-Agent URI (GRUU)
Enable user=phone	Sets user=phone in SIP messages. For compatibility with servers that require this.
Transport Protocol	Configuration using the transport protocol, TCP, TLS or UDP, the default is UDP.
SIP Global Settings	
Strict Branch	Enable Strict Branch - The value of the branch must be after”z9hG4bK” in the VIA field of the INVITE message received, or the phone will not respond to the INVITE. Note: This will affect all lines
Enable Group	Enable SIP Group Backup. This will affect all lines
Registration Failure Retry Time	Registration failures retry time – If registrations fails, the phone will attempt to register again after registration failure retry time. This will affect all lines

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.





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
Select the SIP account configuration the first few lines, two lines are available. The selection switch to the line account configuration.	
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.	

c) DIAL PEER

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

- Substitution – Assume that it is desired to place a direct IP call to IP address 192.168.119.Using this feature, 156 can be substituted for 192.168.1.119.

Dial Peer Table

Number	Destination	Port	Mode	Alias	Suffix	Deleted Length
156	192.168.1.119	5060	SIP	no alias	no suffix	0

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

Dial Peer Table

Number	Destination	Port	Mode	Alias	Suffix	Deleted Length
1T	0.0.0.0	5060	SIP	no alias	no suffix	0

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

  x – Matches any single digit that is dialed.

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

Dial Peer Table

Number	Destination	Port	Mode	Alias	Suffix	Deleted Length
13xxxxxxxxx	0.0.0.0	5060	SIP	no alias	no suffix	0
13[5-9]xxxxxxxx	0.0.0.0	5060	SIP	no alias	no suffix	0

1 We can also realize the equipment at the same time, using a different account, without switching fast call, will make the following specific configuration.

Dial Peer Table

Number	Destination	Port	Mode	Alias	Suffix	Deleted Length
13xxxxxxxxx	0.0.0.0	5060	SIP	no alias	no suffix	0
13[5-9]xxxxxxxx	0.0.0.0	5060	SIP	no alias	no suffix	0
156	192.168.1.119	5060	SIP	no alias	no suffix	0
1T	0.0.0.0	5060	SIP	no alias	no suffix	0

Add Dial Peer

Phone Number

Destination(Optional)

Port(Optional)

Alias(Optional)

Call Mode SIP

Suffix(Optional)

Deleted Length(Optional)

Apply

Dial Peer Option

13xxxxxxxxx Delete Modify

<table>
<tr><th colspan="2">DIAL PEER</th></tr>
<tr><th>Field Name</th><th>Explanation</th></tr>
<tr><td>Phone Number</td><td>There are two types of matching: Full Matching or Prefix Matching.
In Full matching, the entire phone number is entered and then mapped per the Dial Peer rules.
In prefix matching, only part of the number is entered followed by T. The mapping with then take place whenever these digits are dialed. Prefix mode supports a maximum of 30 digits.</td></tr>
<tr><td>Destination(Optional)</td><td>Set Destination address. This is optional. For a peer to peer call, enter the destination IP address or domain name. To use a dial rule on the SIP2 line, enter 0.0.0.2. For SIP3 enter 0.0.0.3</td></tr>
<tr><td>Port(Optional)</td><td>Set the Signaling port, the default is 5060.</td></tr>
<tr><td>Alias(Optional)</td><td>Set the Alias. This is the text to be added, replaced, or deleted. It is optional.</td></tr>
<tr><td colspan="2">Note: There are four types of aliases.
1) Add: xxx – xxx will be dialed before any phone number.
2) All: xxx – xxx will replace the phone number.
3) Del: The characters will be deleted from the phone number.
4) Rep: xxx – xxx will be substituted for the specified characters.</td></tr>
<tr><td>Alias(Optional)</td><td>Protocol configuration option, the default is SIP</td></tr>
<tr><td>Suffix(Optional)</td><td>Characters to be added at the end of the phone number. This is optional.</td></tr>
<tr><td>Deleted Length(Optional)</td><td>Sets the number of characters to be deleted. For example, if this is set to 3, the phone will delete the first 3 digits of the phone number. This is optional.</td></tr>
<tr><td colspan="2">Here's how to realize multiple accounts at the same time using the configuration number IP configuration:
<table>
<tr><th>Number</th><th>Destination</th><th>Port</th><th>Mode</th><th>Alias</th><th>Suffix</th><th>Deleted Length</th></tr>
<tr><td>9T</td><td>0.0.0.0</td><td>5060</td><td>SIP</td><td>del</td><td>no suffix</td><td>1</td></tr>
<tr><td>8T</td><td>0.0.0.0</td><td>5060</td><td>SIP</td><td>del</td><td>no suffix</td><td>1</td></tr>
</table>
9T mapping shows that when the user to configure the SIP1 server, and the user registration, all through the SIP1 call number to dial 9;
8T mapping shows that when the user to configure the SIP2 server, and the user registration, all through the SIP2 call number to dial 8;</td></tr>
</table>

The following for each alias types for example:

Web Interface	Explanation	Example
Phone Number: 9T Destination(Optional): 255.255.255.255 Port(Optional): Alias(Optional): del Call Mode: SIP Suffix(Optional): Deleted Length(Optional): 1	Set phone number, Destination, Alias and Delete Length. Phone number is XXXT; Destination is 255.255.255.255 (0.0.0.2) and Alias is del. Any phone number that begins with XXX will be sent via SIP2 after the first several digits are deleted depending on the delete length.	Dial “93333” The SIP2 server will receive “3333”
Phone Number: 2 Destination(Optional): Port(Optional): Alias(Optional): all:33334444 Call Mode: SIP Suffix(Optional): Deleted Length(Optional): 1	This creates a speed dial function. Dialing “2”, will cause the entire alias number to be sent out.	Dial “2” The SIP1 server will receive 33334444
Phone Number: 8T Destination(Optional): Port(Optional): Alias(Optional): add:0755 Call Mode: SIP Suffix(Optional): Deleted Length(Optional): 1	The equipment will add the alias to the end of the dialed number if the dialed number matches the template in the Phone Number box.	Dial “8309“ The SIP1 server will receive “07558309”
Phone Number: 010T Destination(Optional): Port(Optional): Alias(Optional): rep:0866 Call Mode: SIP Suffix(Optional): Deleted Length(Optional): 3	Set Phone Number, Alias and Delete Length. Phone number is XXXT and Alias is rep: xxx If the dialed phone number starts with the digits in the Phone Number box, the matching digits will be replaced by the alias number.	Dial “0106228” The SIP1 server will receive “86106228”
Phone Number: 147 Destination(Optional): Port(Optional): Alias(Optional): Call Mode: SIP Suffix(Optional): 0011 Deleted Length(Optional):	If the dialed phone number starts with the digits in the Phone Number box, the phone will send out the dialed phone number and add the suffix number.	Dial “147” The SIP1 server will receive “1470011”

(4) PHONE

a) AUDIO

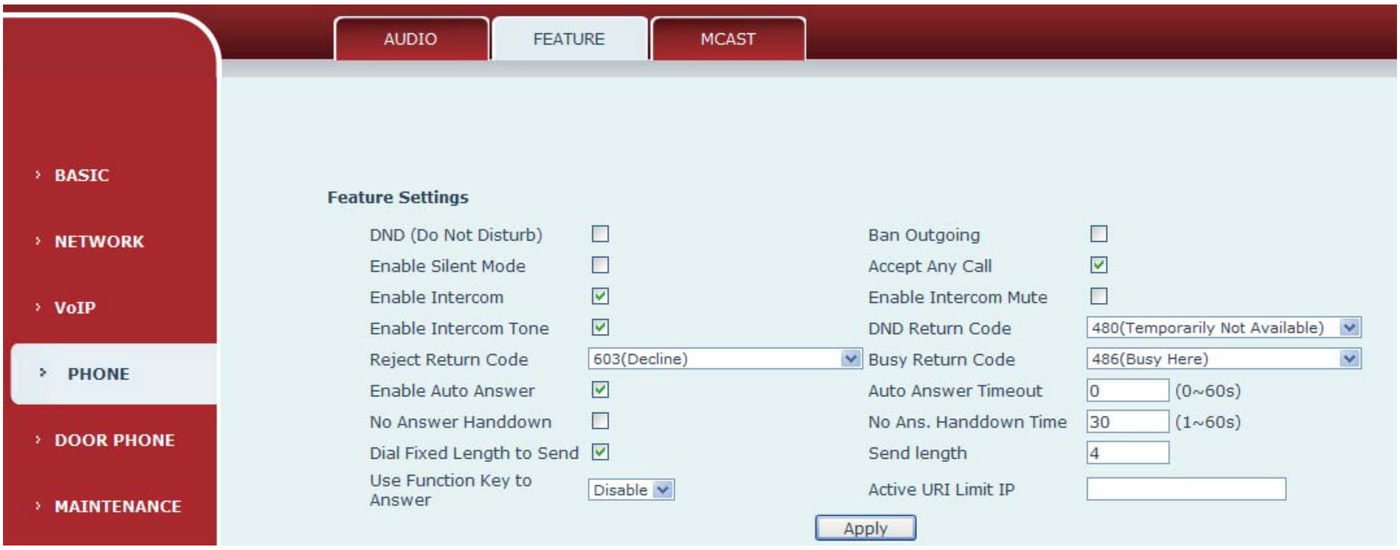
Through this page the user can set the speech coding, input and output, etc.

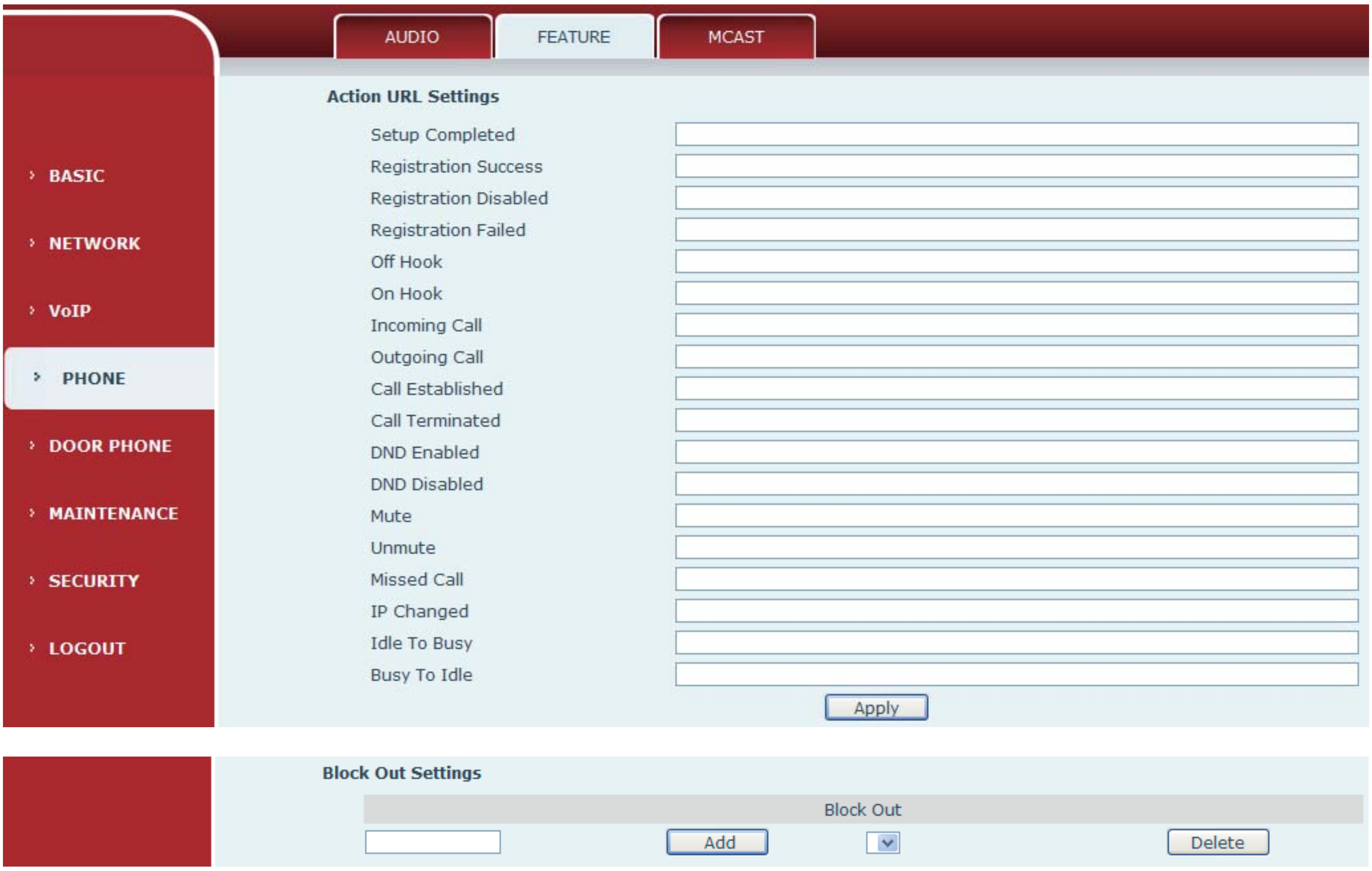
Audio	
Field Name	**Explanation**
First Codec	The first codec choice: G.711A/U, G.722, G.723, G.729, G.726
Second Codec	The second codec choice: G.711A/U, G.722, G.723, G.729, G.726, None
Third Codec	The third codec choice: G.711A/U, G.722, G.723, G.729, G.726, None
Fourth Codec	The forth codec choice: G.711A/U, G.722, G.723, G.729, G.726, None
Fifth Codec	The fifth codec choice G.711A/U, G.722, G.723, G.729, G.726, None
Sixth Codec	The sixth codec choice G.711A/U, G.722, G.723, G.729, G.726, None
DTMF Payload Type	The RTP Payload type that indicates DTMF. Default is 101
Default Ring Type	Ring Sound – There are 9 standard types and 3 User types
G.729AB Payload Length	G.729 Payload Length – Adjusts from 10 – 60 mSec
Tone Standard	Select tone plan for the country of operation
G.722 Timestamps	Choices are 160/20ms or 320/20ms

Field Name	Explanation
G.723.1 Bit Rate	Choices are 5.3kb/s or 6.3kb/s
Enable VAD	Enable or disable Voice Activity Detection (VAD). If VAD is enabled, G729 Payload length cannot be set greater than 20 mSec.
Volume Settings	
MIC Input Volume	MIC Input Volume levels
Hands-free Output Volume	Hands-free Output Volume levels
Ring Volume	Speaker Ring Volume levels
Codec Gain Settings	
Hands-free Hardware MIC Gain	Settings Hands-free Hardware MIC Gain
Hands-free Hardware Speakerphone Gain	Settings hands-free Hardware Speakerphone Gain

b) FEATURE

c) This page configures various features such as Hotline, Call Transfer, Call Waiting and Block Out.

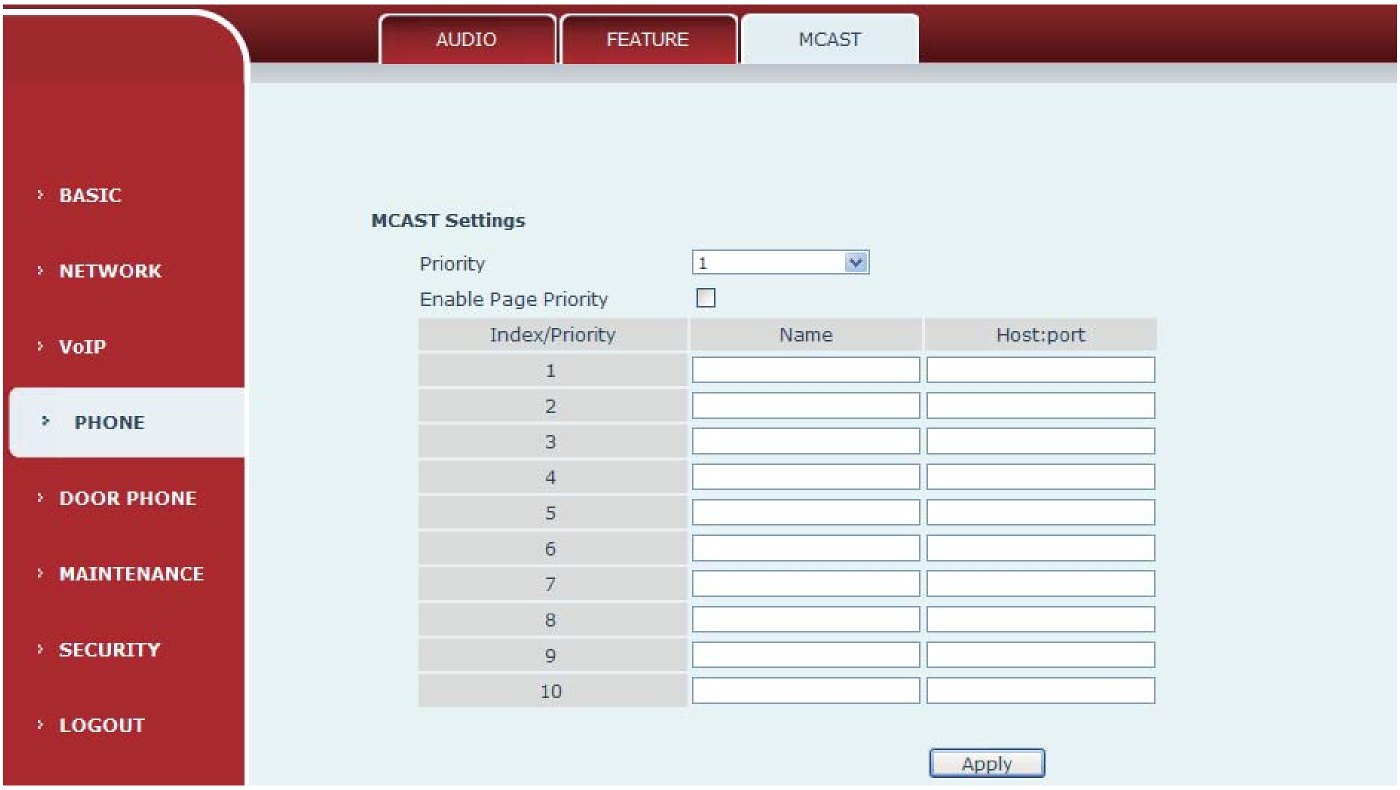




Feature	
Field Name	**Explanation**
Feature Settings	
DND (Do Not Disturb)	DND might be disabled, phone for all SIP lines, or line for SIP individually.
Ban Outgoing	If enabled, no outgoing calls can be made.
Enable Silent Mode	If enabled, the equipment will not ring to indicate a new call. Instead, the light below the key pad will blink to indicate a new call.
Accept Any Call	If enabled, the equipment will accept a call even if the called number does not belong to the phone.
Enable Intercom	If enabled, allows intercom calls.
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.
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.
Enable Auto Answer	Enable Auto Answer function
Auto Answer Timeout	Set Auto Answer Timeout

Field Name	Explanation
No Answer Handdown	Enable no answer when hang up automatically
No Ans. Handdown Time	Configuration in a set time, automatically hang up no answer
Dial Fixed Length to Send	Enable Dial fixed length at to send
Send length	Configured to receive number length; The default is 4, after the user dial four number, the device will automatically breathe out the four number
Use Function Key to Answer	Configure whether to enable the function keys, is disabled by default.
Active URI Limit IP	IP address of the server for the Action URL messages described below.
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	
Block Out Settings	
Add or Delete Blocked numbers – Enter the prefix of numbers which should not be dialed by the phone. For example, if 001 is entered, the phone will not dial any numbers beginning with 001. X and x are wildcards which match single digits. For example, if 4xxx or 4XXX is entered, the phone will not dial any 4 digit numbers beginning with 4. It will dial numbers beginning with 4 which are longer or shorter than 4 digits.	

d) MCAST



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.

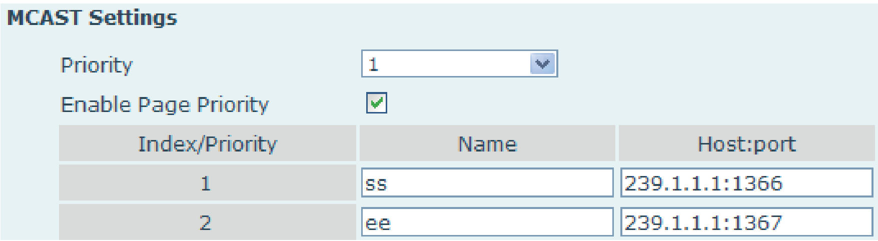
In the Web interface setting change equipment receiving multicast RTP stream processing mode are: set the ordinary priority and enable page priority.

- 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: 1

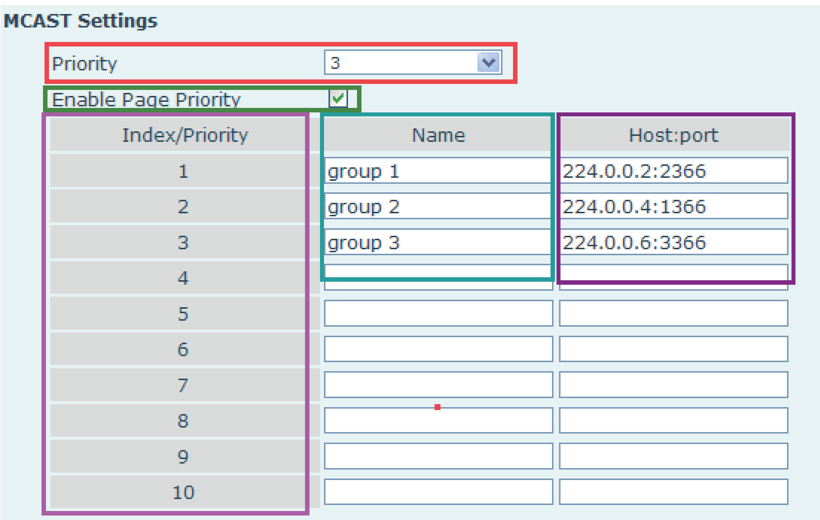
Enable Page Priority: ☑

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: 3

Enable Page Priority: ☑

Index/Priority	Name	Host:port
1	group 1	224.0.0.2:2366
2	group 2	224.0.0.4:1366
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".

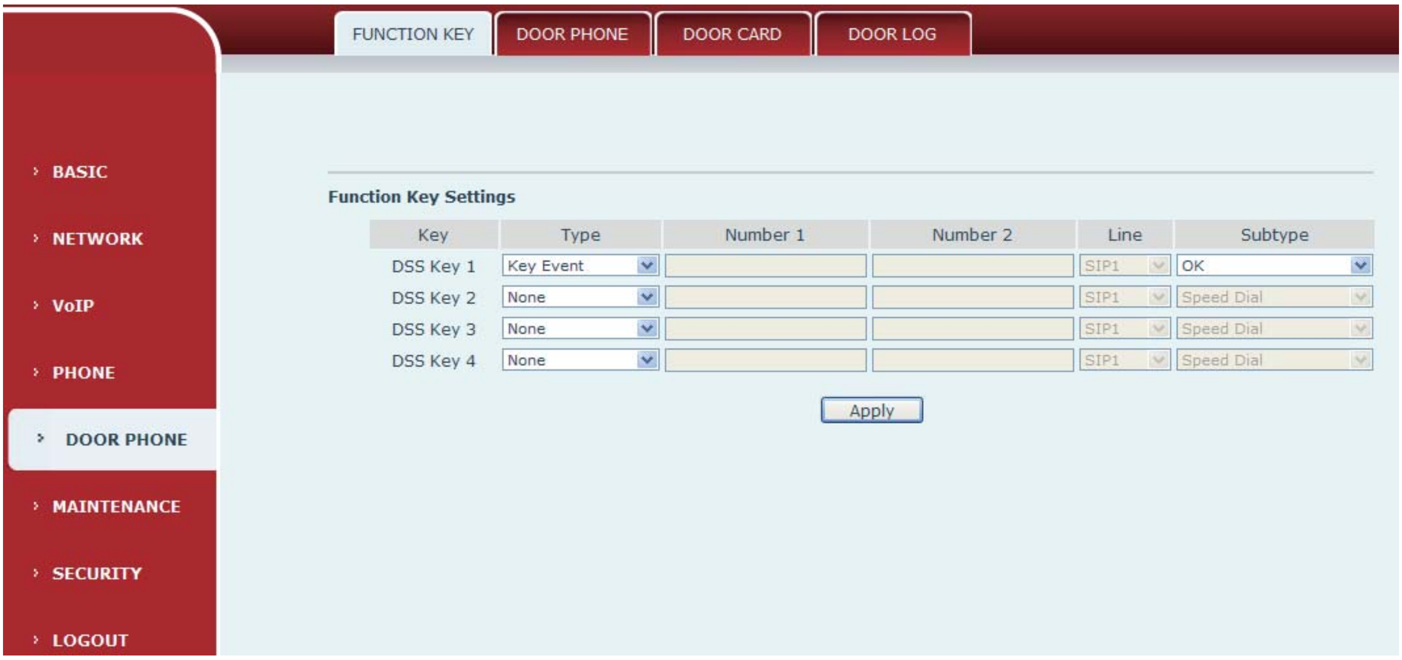
Multicast service

- **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.
- **L monitor:** IP port and priority configuration monitoring device, when the call is initiated and incoming multicast, directly into the Talking interface equipment.

(5) DOOR PHONE

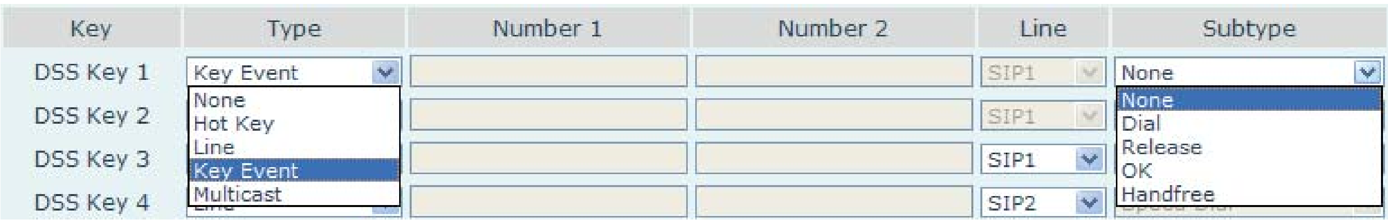
a) FUNCTION KEY

The equipment has four programmable keys (depending on the hardware configuration), you can set different for each key function respectively, the list below you can set up some of the functions and the related introduction, every button by default is N/A, namely the default doesn't set any function.



➢ **Key Event Settings**

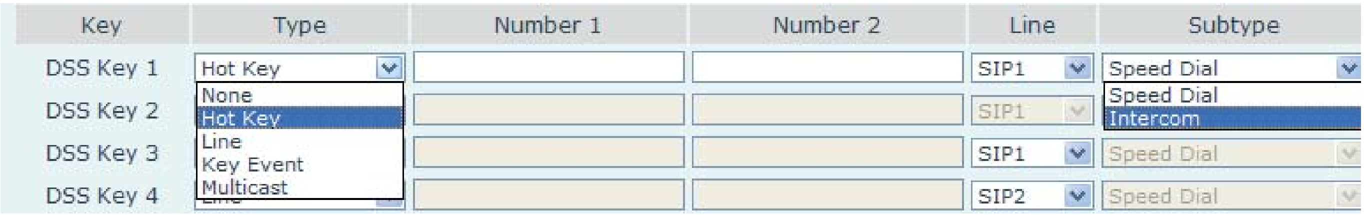
The Subtype configuration of Hot key.



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)

H 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.

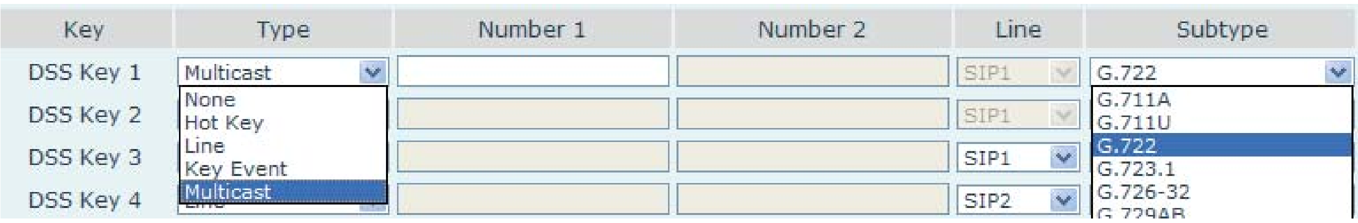


DSS key type	Number	Line	Subtype	Usage
Hot key	Fill the called party's SIP account or address	The SIP account corresponding lines	Speed Dial	In Speed dial mode, with Enable Speed Dial Handdown [Enable] can define whether this call is allowed to be hang up by re-press the speed dial
			Intercom	In Intercom 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:



DSS key type	Number	Subtype	Usage
Multicast	Set the host IP address and port number, the middle separated by a colon	G.711A	Narrowband speech coding (4Khz)
		G.711U	
		G.722	Wideband speech coding (7Khz)
		G.723.1	Narrowband speech coding (4Khz)
		G.726-32	
		G.729AB	

✧ operation mechanism

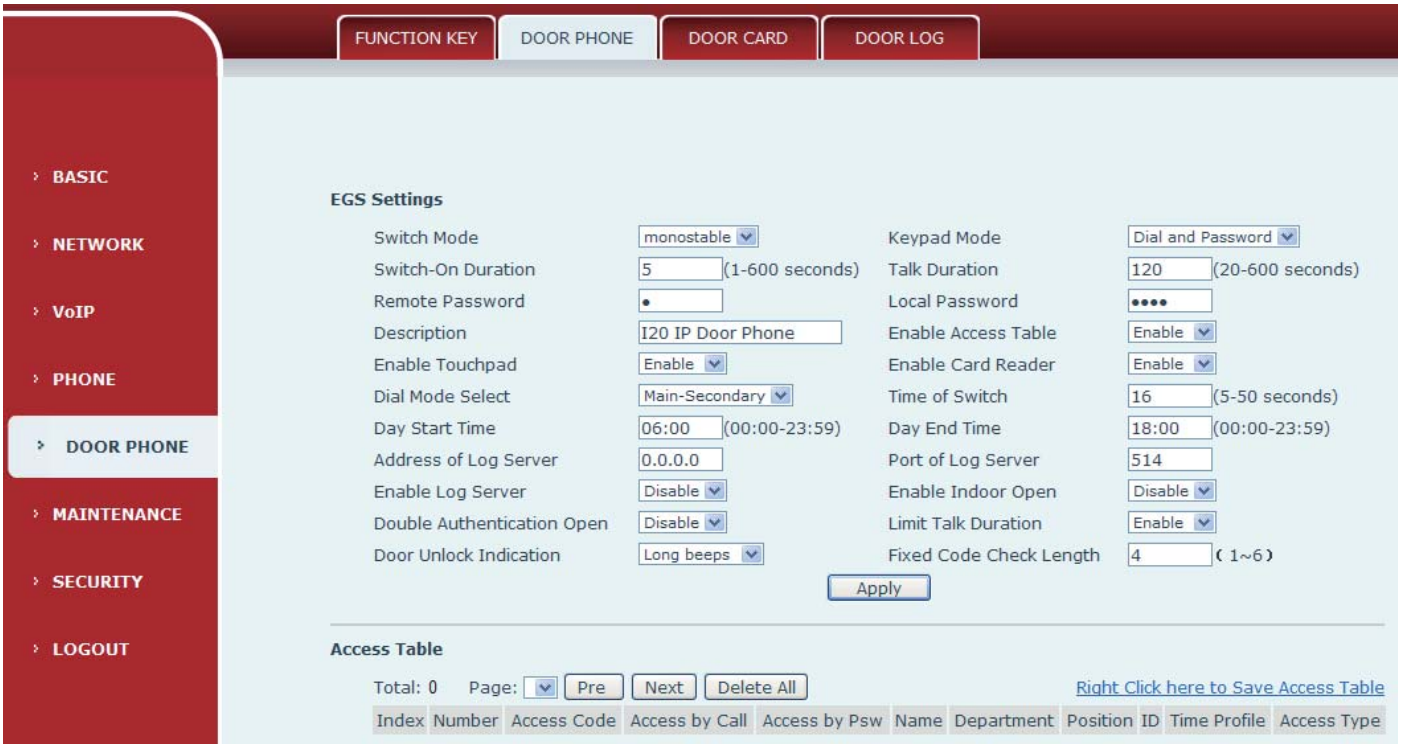
Device through the DSS Key configuration of multicast address and port and started coding; set by WEB to monitor the multicast address and port; device sends a multicast, listens to the address of the device can receive the multicast content.

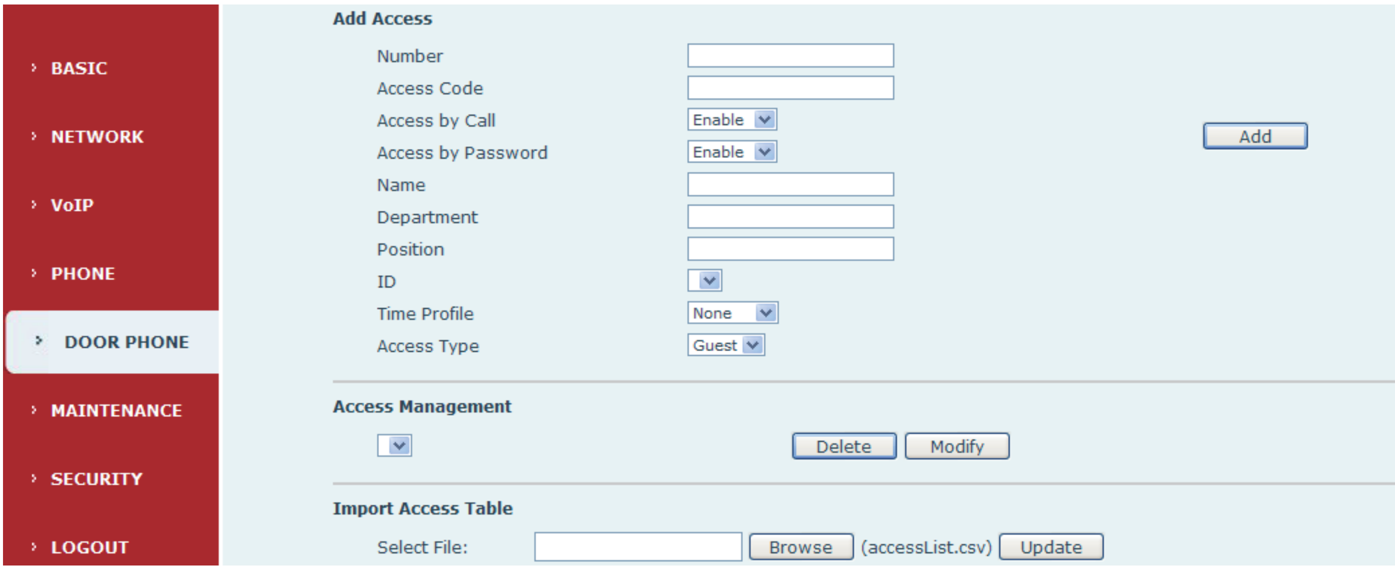
✧ calling configuration

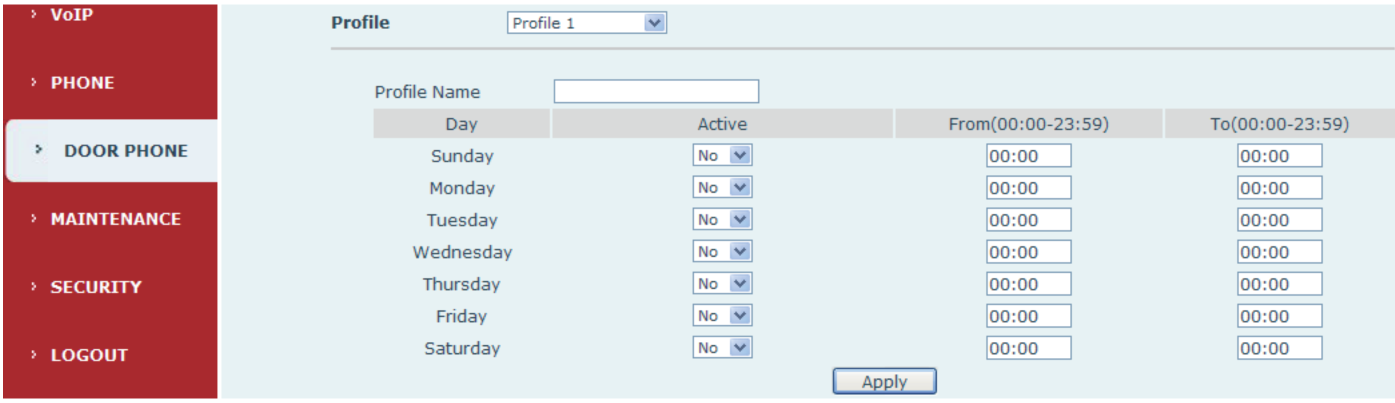
The call is already exists, and three party or initiated multicast communication, so it will not be able to launch a new multicast call.

b) DOOR PHONE

Entrance guard page used to configure the parameters of the entrance guard, access management personnel.







Door phone		
Field Name	**Explanation**	**Initial Value**
Access control Settings		
Switch Mode	Monostable: there is only one action and status-open door mode; Bistable: there are two actions and statuses-open door and close door; each action might be triggered and changed to the other status; after changed, the status would be kept	monostable
Keyboard mode	Only password: there is only accepted password input; dialing would be forbidden; Password+dialing: there might be password input, dialing(* key for getting dialing tone, hang up calls; # key for confirming)	Dialing and password input
Switch-On Duration	Opened door time for monstable mode. If the time is up, door switch would be closed automatically	5 seconds
Talk Duration	After time is up, the call will be ended automatically.	120 seconds
Remote Password	Remote opening door password.	*

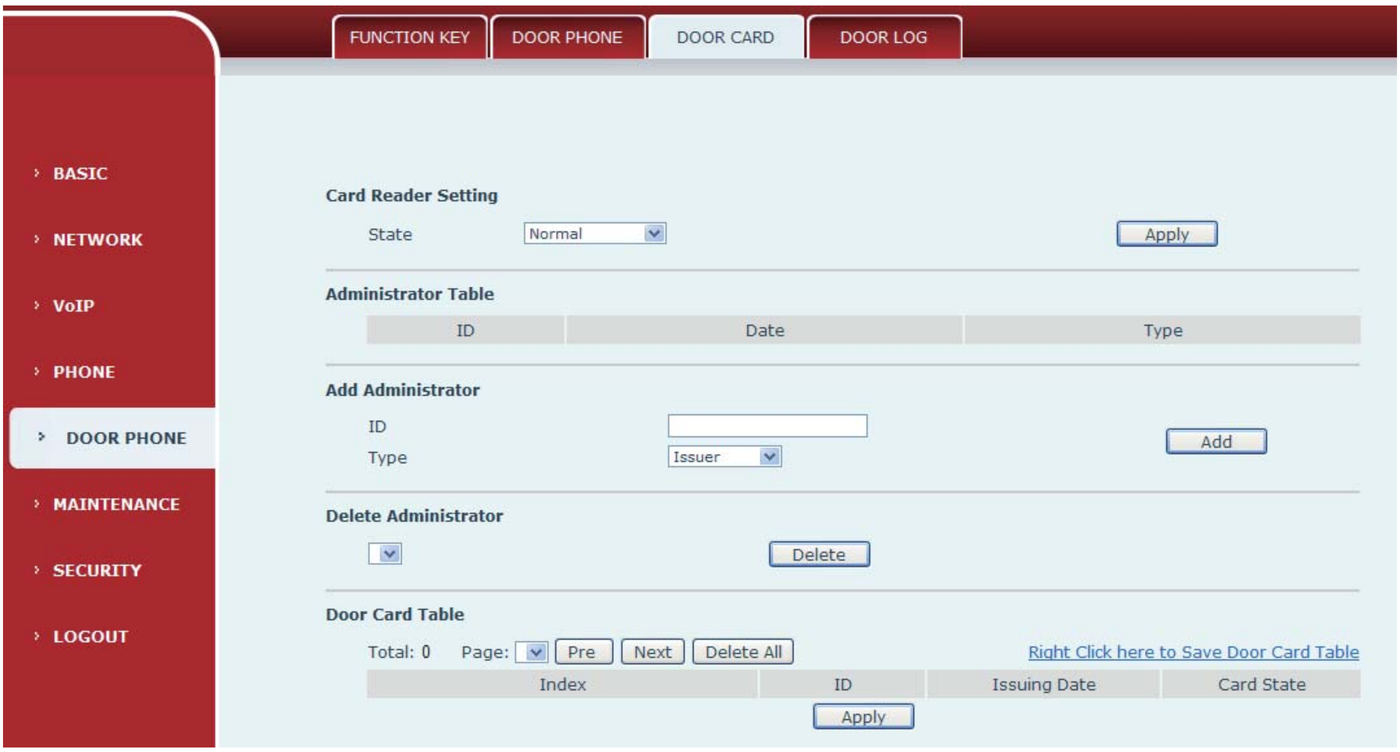
Field Name	Explanation	Initial Value
Local Password	Local opening door password via keypad, the default password length is 4	6789
Description	Displayed on IP scanner tool software	I20 IP door phone
Enable Access Table	Enable or disable remote password for opening door during calls	Enable
Enable Touchpad	Enable or disable keypad operation for dialing and password input	Enable
Enable Card Reader	Enable or disable RFID card checked	Enable
Dial Mode Select	<Primary /Secondary>mode allow system to call primary extension first, if it were no answer, 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; User just press speed dial key once;	Primary /secondary
Time of Switch	The period between one-button Call function to call the first and second number	16S
Day Start Time	When select <Day/Night>mode, the time to start Day time	06:00
Day End Time	When select <Day/Night>mode, the time to end up Day time	18:00
Address of Log Server	Log server address(IP)	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 open door with indoor switch	Disable
Double Authentication Open	If it enabled, the door would be opened only when the local password and cards checked are both correct	Disable
Limit Talk Duration	Configuration is enabled to speak timeout automatically after the call	Enable
Door Unlock Indication	Indication tone for door opened. There are 3 type of tone: silent/short beeps/long beeps	Long beeps
Fixed Code Check Length	The local password length would be restricted with it; if the input password length is matched with it, system would check it immediately	4

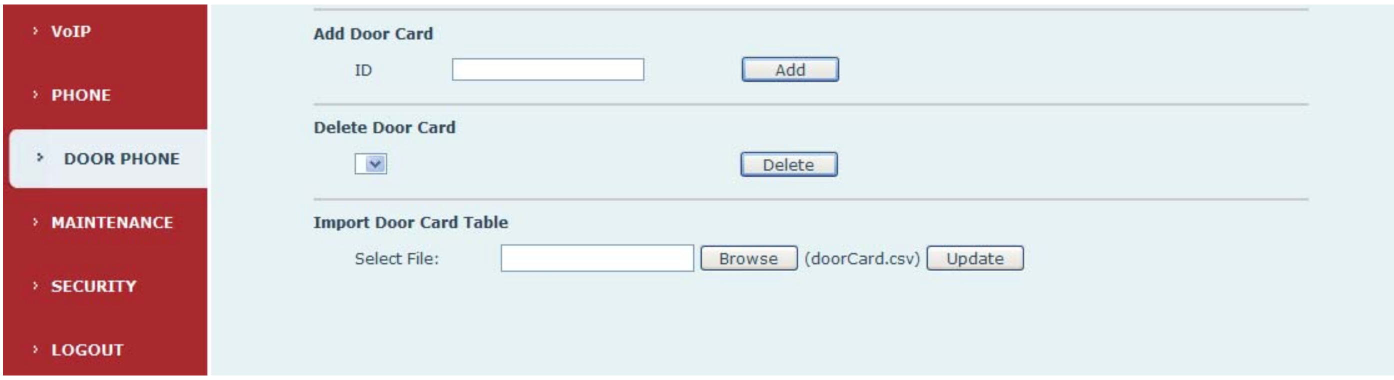
Field Name	Explanation	Initial Value
Remote Phonebook		
Index	The number has been registered number	
Number	Remote phone number	
Authentication code	Access code for visitor. When remote phone calls, if the number is in access list, you can input access code to open the door.	When IP phone calls, it needs to input authentication code to Control voice access controller.
Access by Call	Configured to enable or disable by phone to open the door	Enable
Access by Password	Configured to enable or disable by a password to open the door	Enable
Name	Card holder's name	
Department	Card holder's department	
Position	Card holder's position	
Card number	RFID's number	
Time Profile	Configuration ID card period of use time	
Type of Host	When owner calls, controller answer automatically, when visitor calls, controller mute.	
Right Click here to Save Access Table	Right Click here to Save Access Table Click the right mouse button, select save target as, then select the save location, you can keep the moment have registered good remote access list to a computer.	
Add access		
Number	Configuration access personnel call number	
Access Code	Configuration access authentication codes	
Access by Call	Configured to enable or disable by phone to open the door	Enable
Access by Password	Configured to enable or disable by a password to open the door	Enable
Name	Card holder's name	
Department	Card holder's department	
Position	Card holder's position	
ID	RFID's number	
Time Profile	The current personnel all open certification effective use of time, do not restrict [no] is 24 hours.	The default "no"
Access Type	When owner calls, controller answer automatically, when visitor calls, controller mute.	

Field Name	Explanation
Configuration after press "add" button to add a new remote access list. Remote access list personnel can call entrance guard, switch on the corresponding access code after input to open the door, or card to open the door. Can add at most 300 people to visit.	
Access Management	
Choose the need to manipulate Numbers, click "delete" button to delete the selected access personnel; Click "modify" button to modify the selected site visits. In addition to the call number cannot be modified and all the other attributes can be modified.	
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 number.	
Profile Settings	
Profile	Configuration choice period 1, 2, 3, 4
Profile Name	The name of the current period
Active	Whether startup configuration on the day of the period of management
From	Configuration the beginning of the period of time
To	Configuration of the end of the period of time

c) DOOR CARD

Entrance card Settings interface. Set the state of card reader, card issuing and delete.





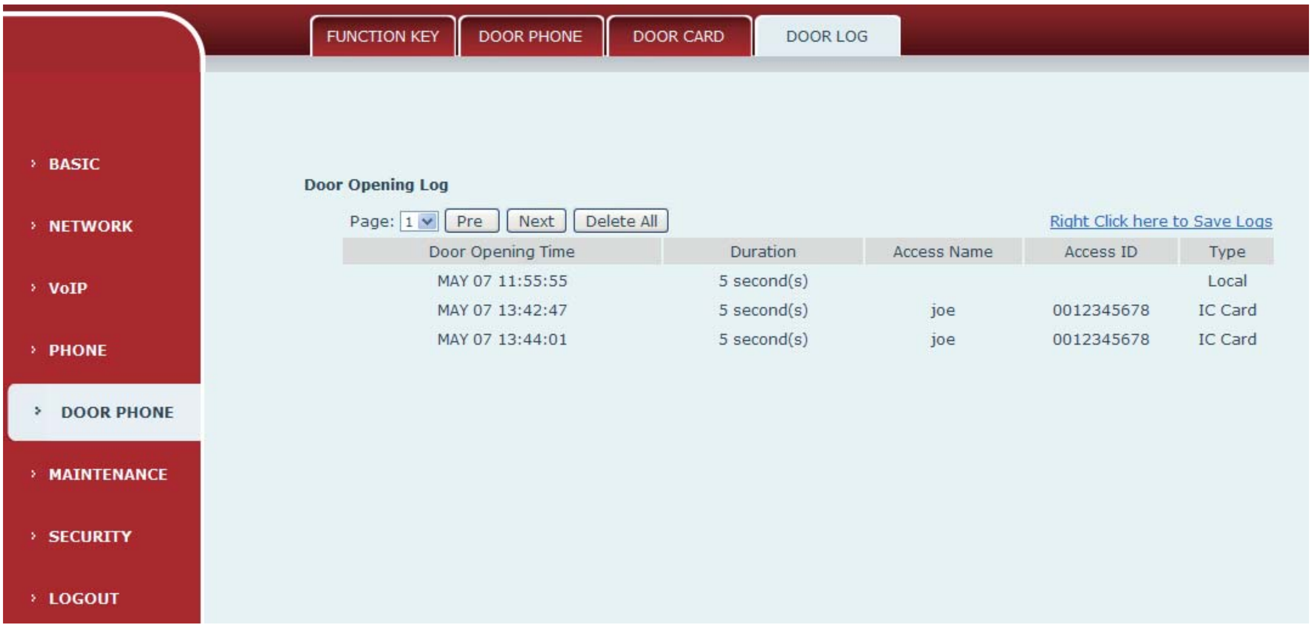
Door card settings	
Field Name	**Explanation**
Card Reader Setting	
State	Set the ID card of state: Normally, after the credit card to open the door; Card Issuing, the state of charge can put the card to be added to the database; Card Revoking, the state of charge can put the card is removed from the database.
Administrator Table	
Card data table shows card ID, Date and Type .	
Add Administrator	
Post card. ID number management kaka Type: there are two hairpins, delete card. Distributed entrance guard in normal state, brush card entrance guard into the state, then brush to add card, the card is added to the database, after joining another brush card entrance guard returned to normal. Delete card operation. Can release at most 10 card, 500 copies of an ordinary card. Note: in the issuing state to delete brush card is invalid, and vice versa.	
Delete Administrator	
Delete administrator card choose to delete the card number, then press "delete"	
Door Card Table	
Index	Credit card number
ID	Have card number (note: has the card is not registered in the remote access list is unable to open the door)
Issuing Date	The issuing time
Card State	The current status. When choose to disable this card number in the remote access list of information to be deleted, but can't open the door and registration.

Field Name	Explanation
Right Click here to Save Door Card Table	Right Click here to Save Door Card Table Right-click it and select save target as to save on your computer
Add Door Card	Manually enter entrance card number the top 10, for example, 0004111806, click "add".
Delete Door Card	Select entrance guard card to delete, click the "delete" .
Import Door Card Table	Click the "browse" to choose to import door card list file "doorCard.csv", click "update" can be batch import.

d) DOOR LOG

According to open event log, can record up to 20 w open event, after more than cover the old records.

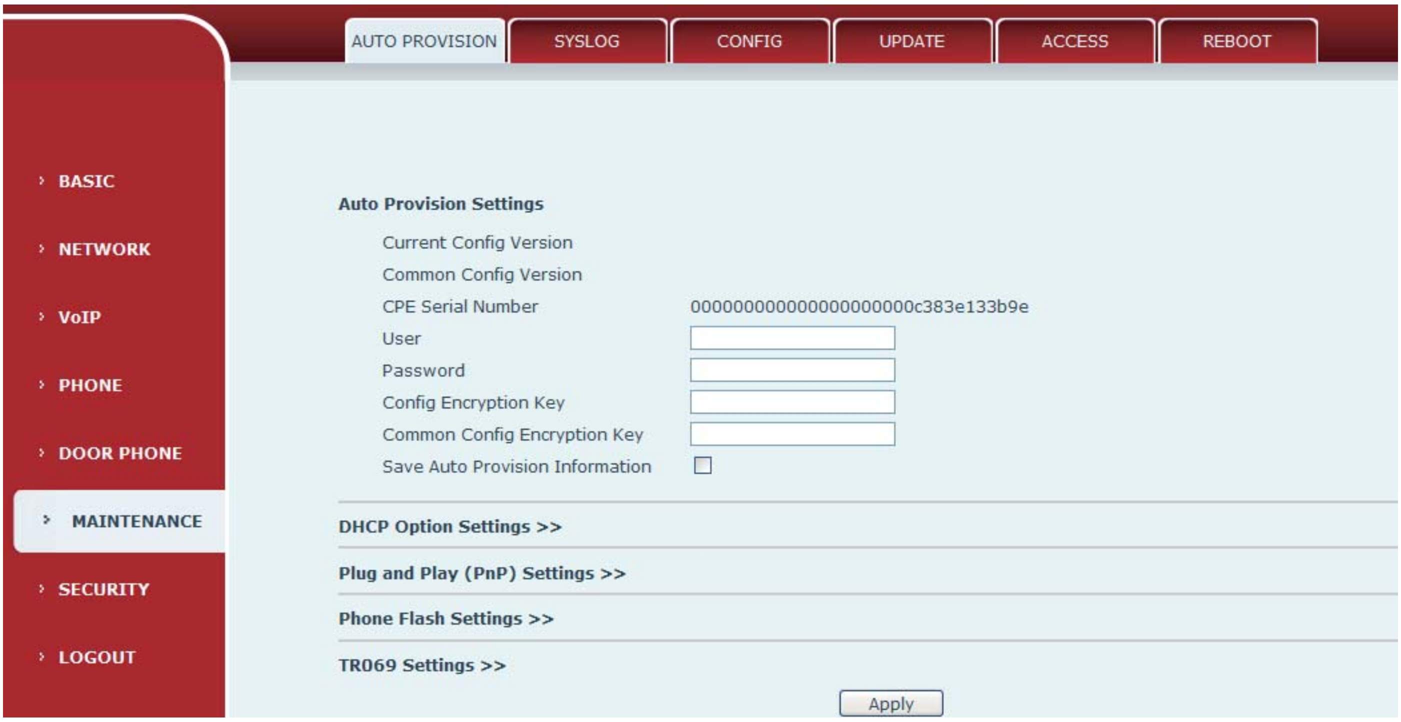
Right Click here to Save Logs Right click on the links to select save target as the door log can export CSV format.



Door log	
Field Name	**Explanation**
Door opening time	Open the door of time
Duration	Duration of open the door
Access name	If the open the door for slot card and remote display remote access registration name list.
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, slot card.

(6) MAINTENANCE

a) AUTO PROVISION



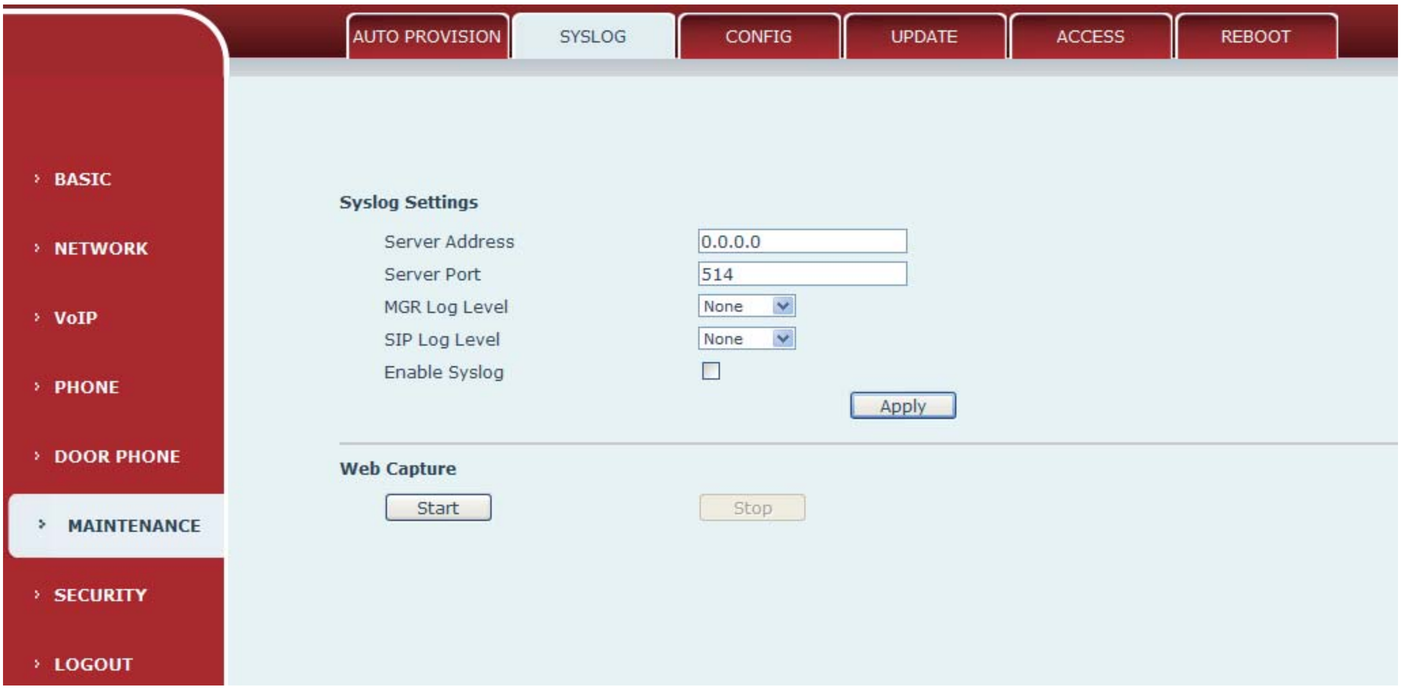
The equipment supports PnP, DHCP, and Phone Flash to obtain configuration parameters. They will be queried in the following order when the equipment boots.

DHCP option → PnP server →Phone Flash

Field Name	Explanation
Automatic update configuration	
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

Field Name	Explanation
Password	Password for configuration server. Used for FTP/HTTP/HTTPS.
Config Encryption Key	Encryption key for the configuration file
Common Config Encryption Key	Encryption key for common configuration file
Save Auto Provision Information	Save the auto provision username and password in the phone until the server url changes
DHCP Option Settings	
DHCP Option Setting	The equipment supports configuration from Option 43, Option 66, or a Custom DHCP option. It may also be disabled.
Custom DHCP Option	Custom option number. Must be from 128 to 254.
Plug and Play（PnP）Settings	
Enable PnP	If this is enabled, the equipment will send SIP SUBSCRIBE messages to a multicast address when it boots up. Any SIP server understanding that message will reply with a SIP NOTIFY message containing the Auto Provisioning Server URL where the phones can request their configuration.
PnP server	PnP Server Address
PnP port	PnP Server Port
PnP Transport	PnP Transfer protocol – UDP or TCP
PnP Interval	Interval time for querying PnP server. Default is 1 hour.
Phone Flash Settings	
Server Address	Set FTP/TFTP/HTTP server IP address for auto update. The address can be an IP address or Domain name with subdirectory.
Config File Name	Specify configuration file name. The equipment will use its MAC ID as the config file name if this is blank.
Protocol Type	Specify the Protocol type FTP, TFTP or HTTP.
Update Interval	Specify the update interval time. Default is 1 hour.
Update Mode	1. Disable – no update 2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update interval

b) SYSLOG



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.

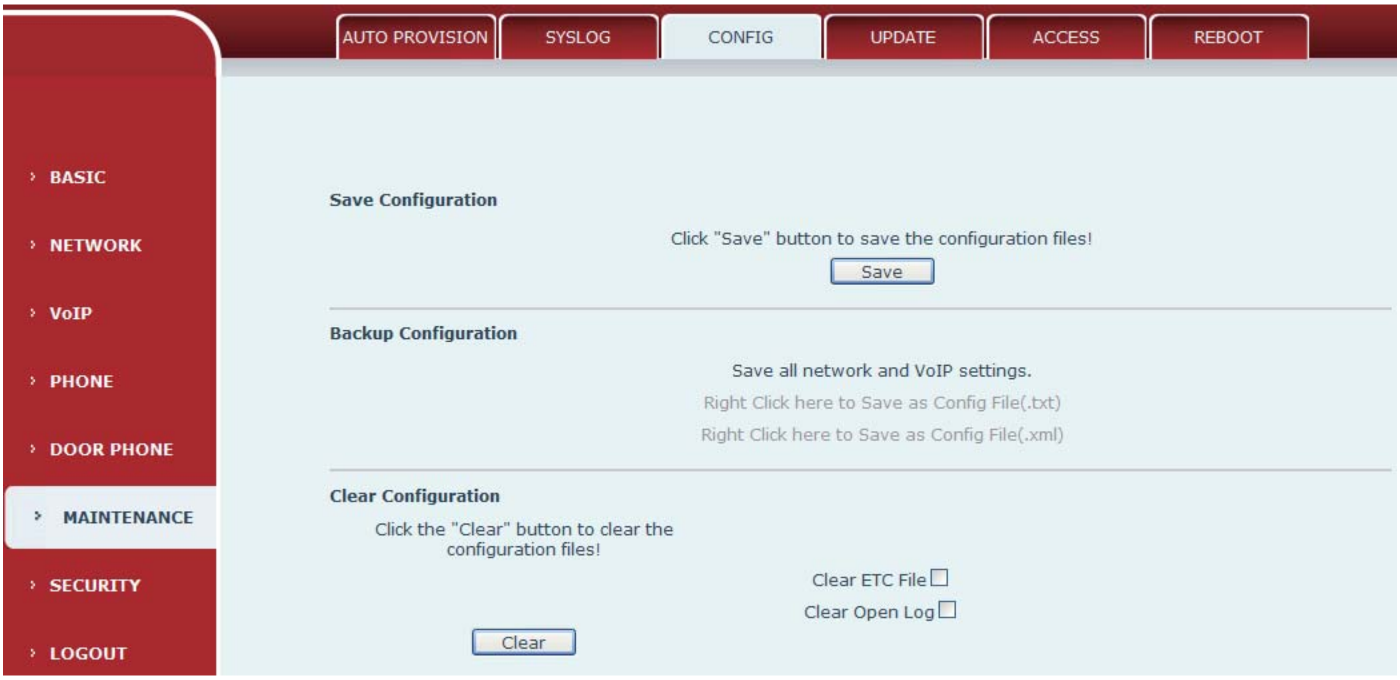
Level 6: Informational; It is the normal daily messages.

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.
IAX2 log level	Set the level of IAX2 log.
Enable system log	Enable or disable system log.

Field Name	Explanation
Web Capture	
Start	Capture a packet stream from the equipment. This is normally used to troubleshoot problems.
Stop	Stop capturing the packet stream

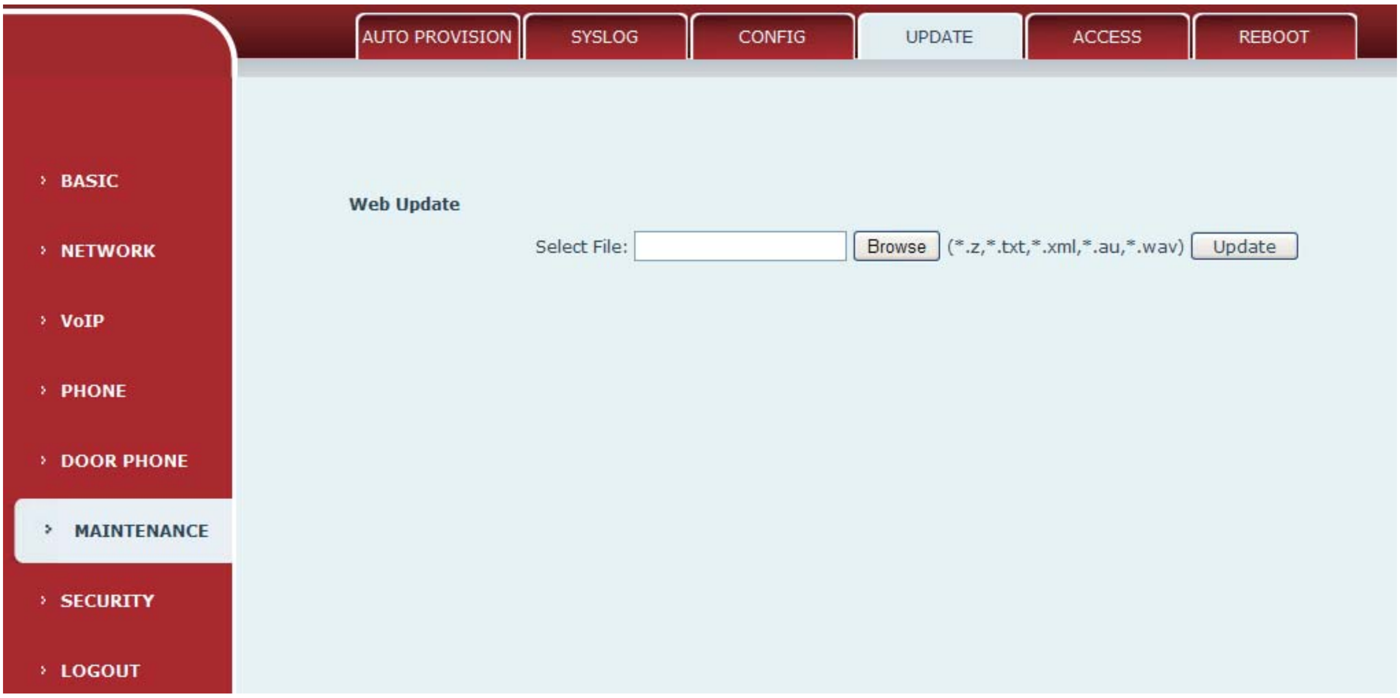
c) CONFIG



Field Name	Explanation
Save Configuration	Save the current equipment configuration. Clicking this saves all configuration changes and makes them effective immediately.
Backup Configuration	Save the equipment configuration to a txt or xml file. Please note to Right click on the choice and then choose “Save Link As.”
Clear Configuration	Logged in as Admin, this will restore factory default and remove all configuration information. Logged in as Guest, this will reset all configuration information except for VoIP accounts (SIP1-6 and IAX2) and version number.

d) UPADTE

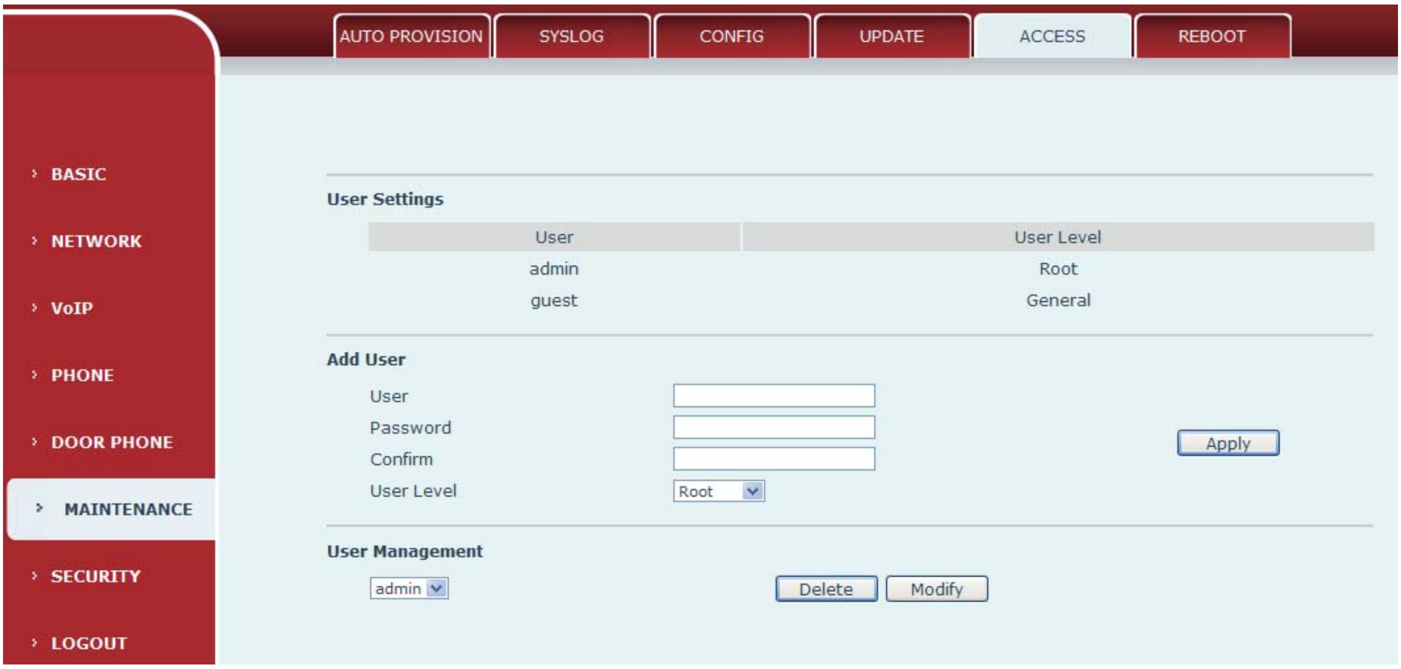
This page allows uploading configuration files to the equipment.



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.	

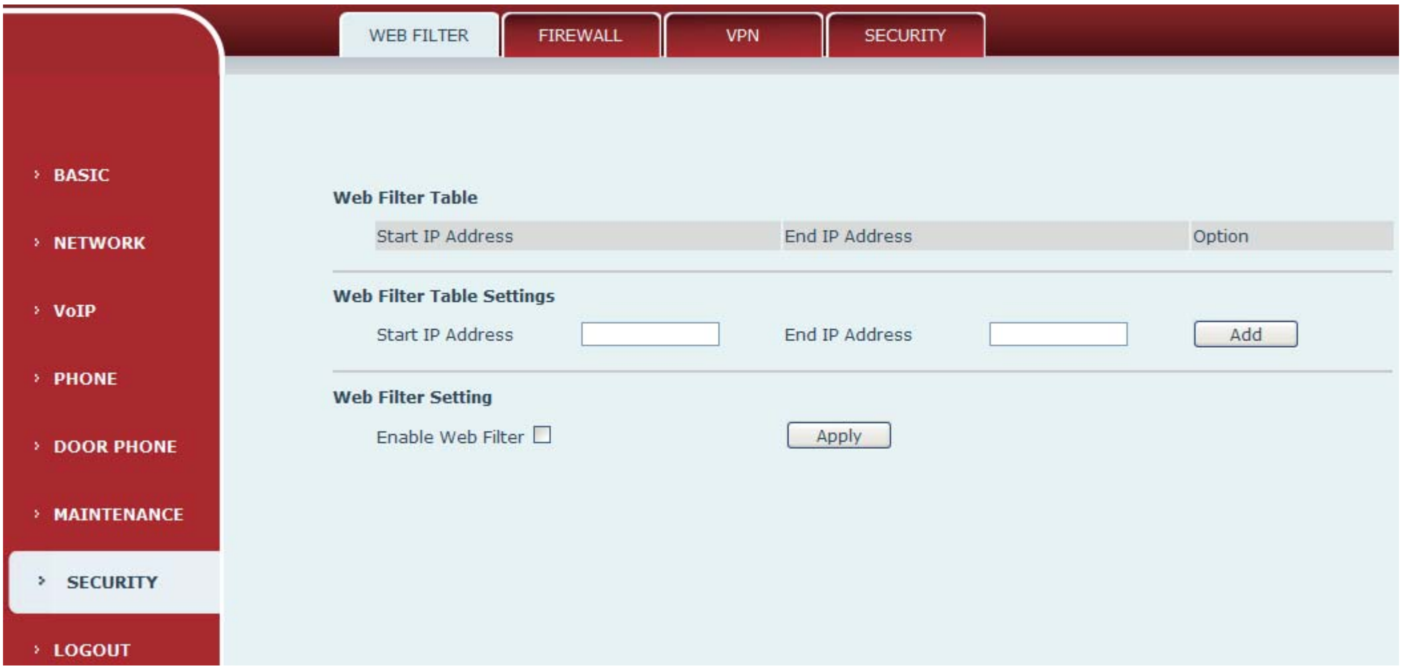
f) REBOOT

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.

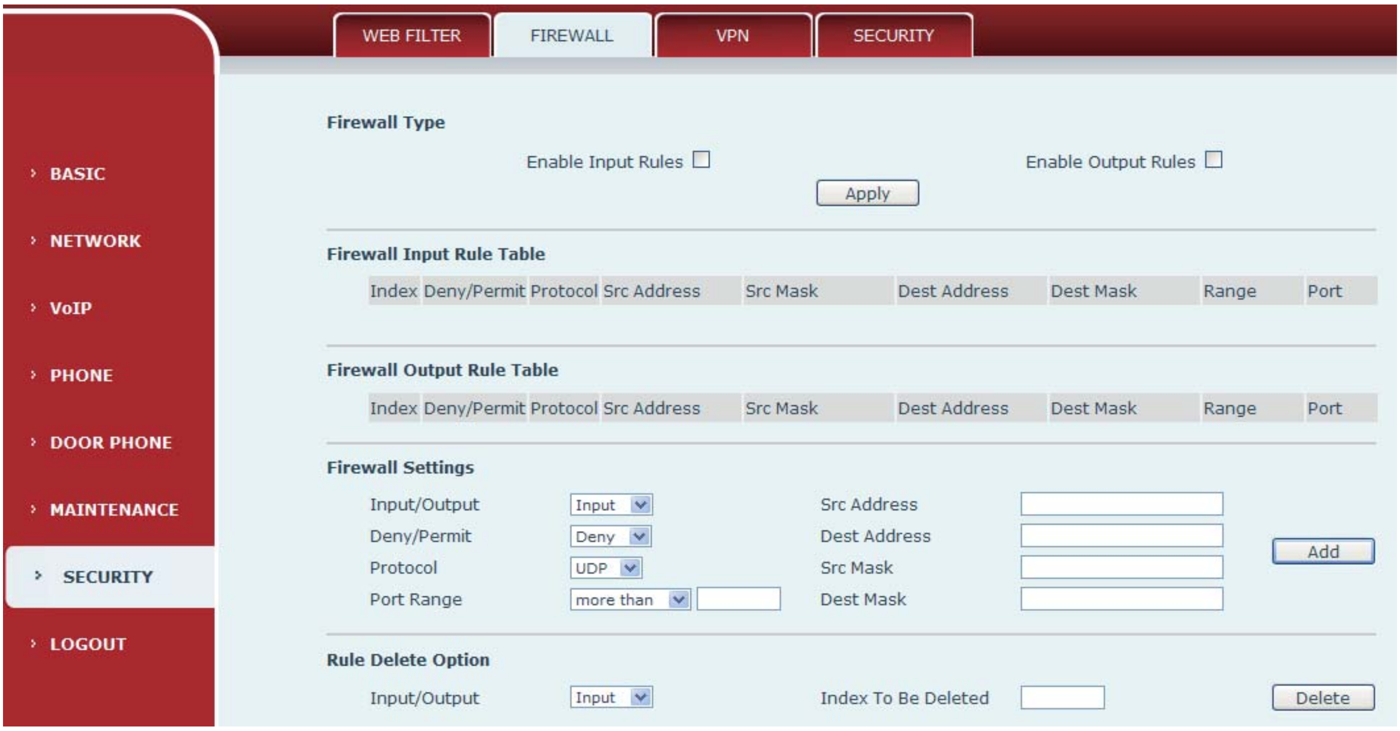
(7) SECURITY

a) 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.	
Field Name	**Explanation**
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.	

b) FIREWALL

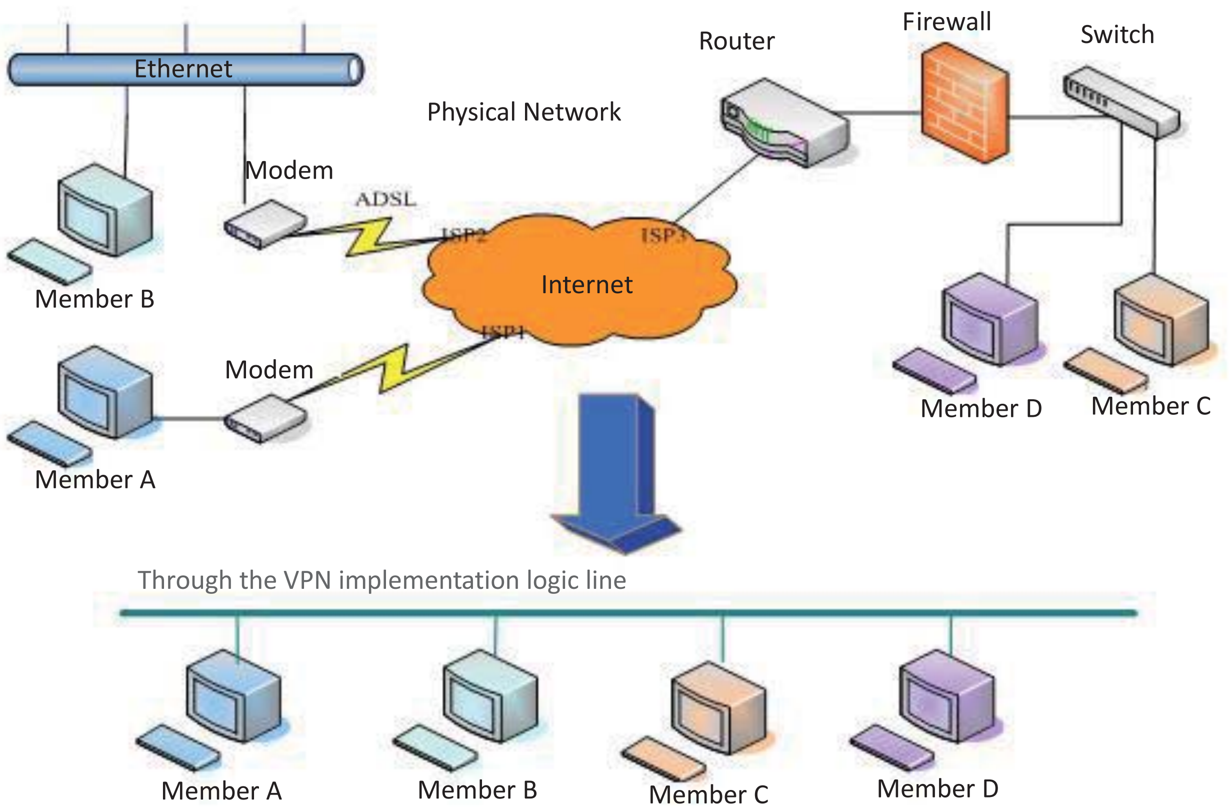


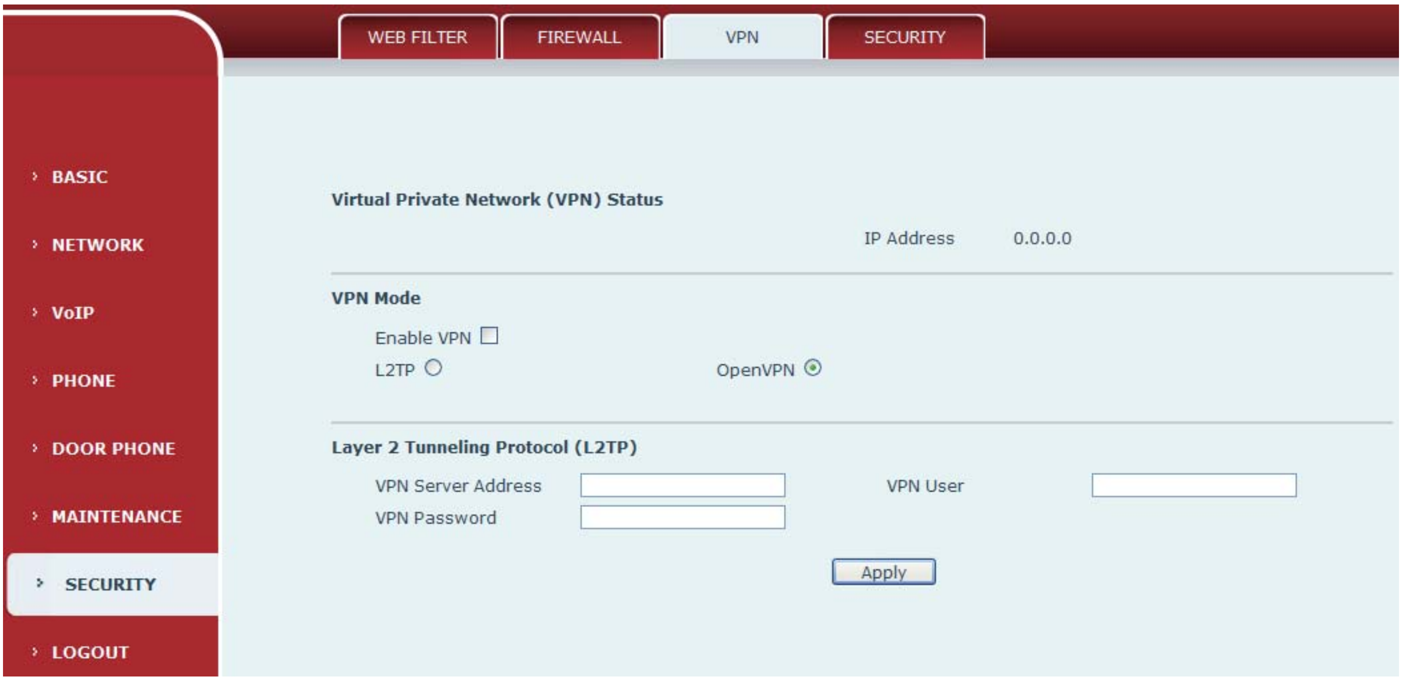
Firewall	
Firewall rules can be used to prevent unauthorized Internet users from accessing private networks connected to this phone (input rule), or prevent unauthorized devices connected to this phone from accessing the Internet (output rule). Each rule type supports a maximum of 10 items.	
Field Name	**Explanation**
Firewall Rules Settings	
Enable Input Rules	Enable rules limiting access from the Internet.
Enable Output Rules	Enable rules limiting access to the Internet.
Firewall Settings	
Input / Output	Specify if the current rule is input or output.
Deny/Permit	Specify if the current rule is Deny or Permit.
Protocol type	Filter protocol type (TCP/ UDP/ ICMP/ IP)
Port Range	Set the filter Port range
Source Address	Set source address. It can be a single IP address or use * as a wild card. For example: 192.168.1.14 or *.*.*.14.
Destination Address	Set destination address. It can be a single IP address or use * as a wild card. For example: 192.168.1.14 or *.*.*.14.

Field Name	Explanation
Source Mask	Set the source address mask. For example: 255.255.255.255 points to one host while 255.255.255.0 points to a C type network.
Destination Mask	Set the destination address mask. For example: 255.255.255.255 points to one host while 255.255.255.0 points to a C type network.

c) VPN

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



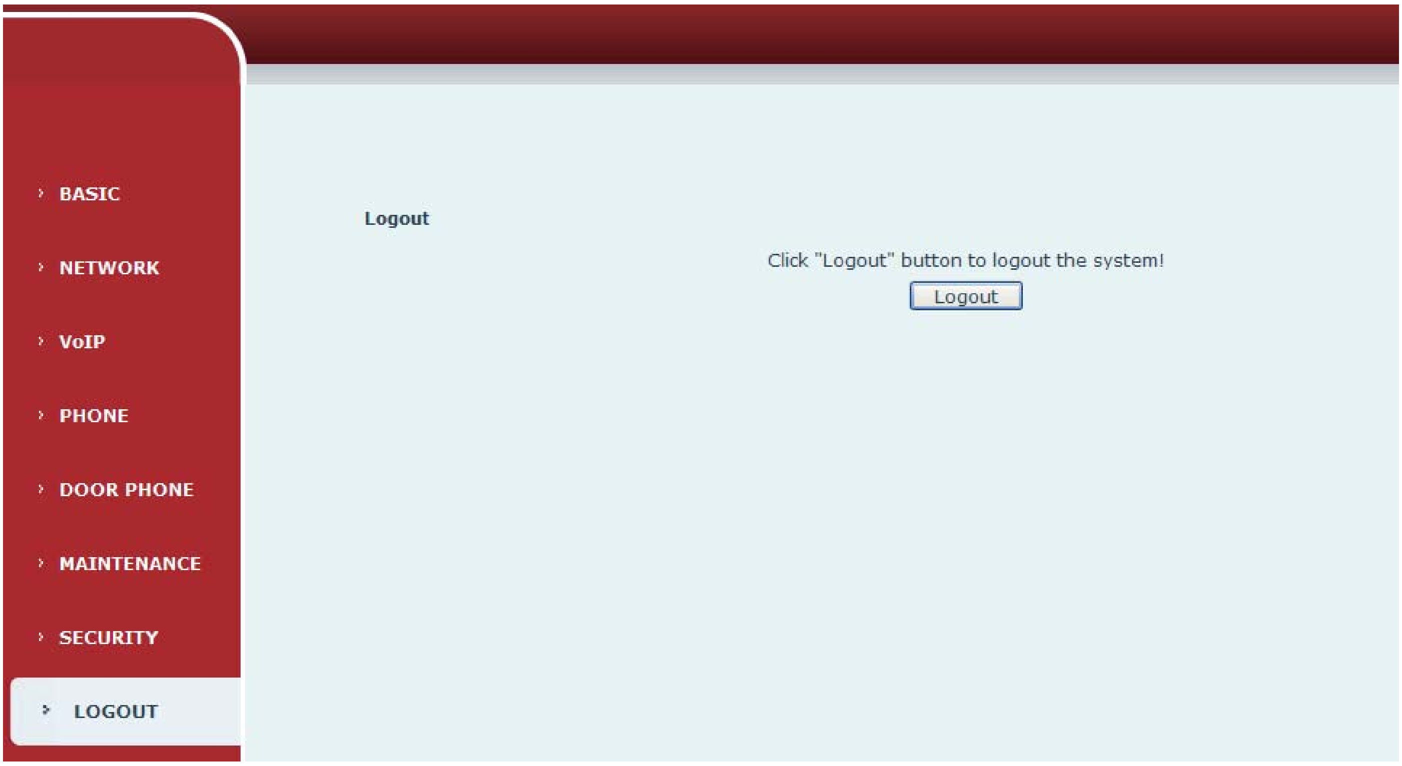


Field Name	Explanation
VPN IP	Shows the current VPN IP address.
VPN type	
Enable VPN	Enable/Disable VPN.
L2TP	Select Layer 2 Tunneling Protocol
Open VPN	Select OpenVPN Protocol. (Only one protocol may be activated. After the selection is made, the configuration should be saved and the phone rebooted.)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

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.
OpenVPN Files	Show OpenVPN File authentication certificate file.

(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		Broadcom
Key	**DSS key material**	Stainless steel
	DSS key	1
	numeric keyboard	Support
Speech flow	**Protocols**	RTP
	Decoding	G.729、G.723、G.711、G.722、G.726
	Audio amplifier	1.5W/8Ω
	Volume control	Adjustable
	Full duplex speakerphone	Support (AEC)
Port	**Passive switch(relay)**	Normally open/Normally close, support 30V DC/1A, 125V AC/0.3A max.
	Active Switched Output	12V DC /750mA
	WAN	10/100BASE-TX s Auto-MDIX, RJ-45
RFID/IC card		TK4100 (125Khz)
Power supply mode		12V±15% / 1A DC or POE
Cables		CAT5 or better
Shell Material		Aluminum alloy panel, Plastic bottom shell
Working temperature		0°C to 50°C
Working humidity		10% - 95%
Storage temperature		-40°C to 70°C
Installation way		Embedded installation
Dimension		Overall dimension: 174.5x96x44mm Package dimension: 148x80x36mm

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)
- Embedded installation
- Integrated RFID Card reader
- Integrated indoor switchgear
- Integrated one Relay
- External Power Supply
- Access control-by call, code, RFID card, indoor switch
- Industrial Standard Certifications: IP54, CE/FCC

3. Schematic diagram

F. Other instructions

1. Open door modes

- **Local**

✧ Set local password (the default is "6789") via web-door phone-door phone.

✧ Use the device's keyboard to input password and # key, and then the door opened.

- **Remote**

1) Visitors call to owner

✧ Visitors press the speed dial key to call the owner;

✧ The owner answer calls, press the "*" key open to visitors.

2) Owner calls to visitors

✧ Owner calls to visitors via SIP phone;

✧ Voice access automatically answers the call;

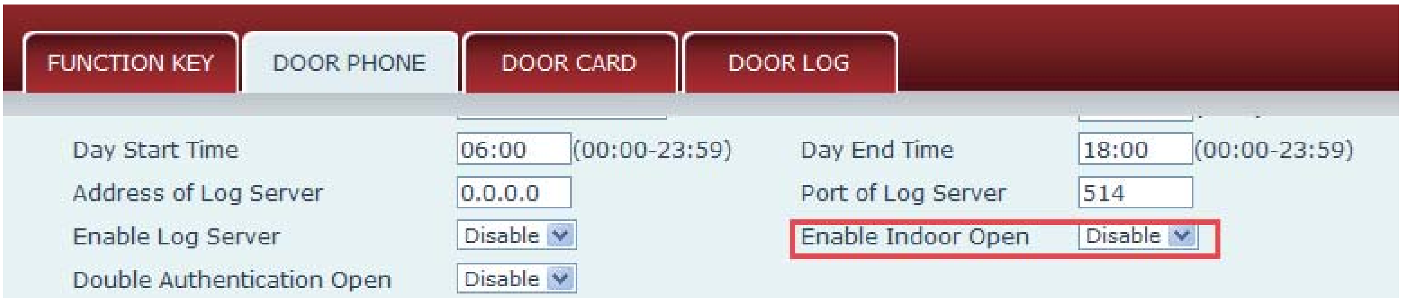
✧ Owner use keypad to input corresponding authentication codes to open the door.

- **Slot cards**

✧ Use pre assigned ID cards to touch the access control to open the door.

- **Indoor switch**

✧ Use indoor switch, which is installed and connected with access control.

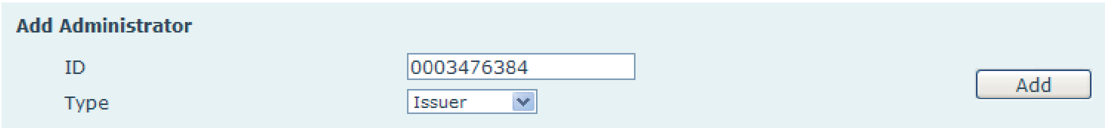


2. Management of card

- **Add Administrator**

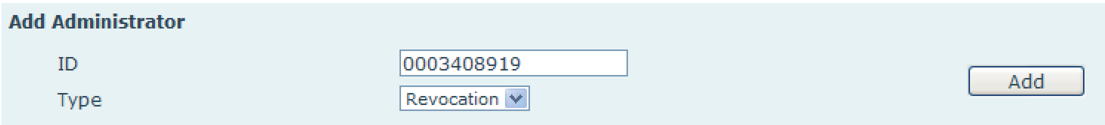
1) Add<Issuer admin card >

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



2) Add <Revocation admin card>

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



3) Administrator Table

Administrator Table

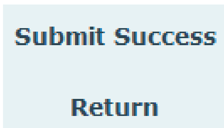
ID	Date	Type
0003476384	MAY 06 11:16:42	Issuer
0003408919	MAY 06 11:17:33	Revocation

- **Add user card**

Methods 1: used to batch add cards for starters.

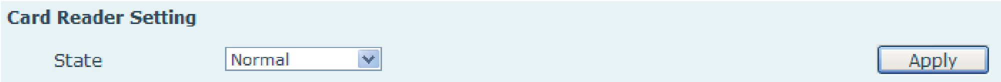
1) In web page <Card Reader Setting> option, select <Card Issuing> function;

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



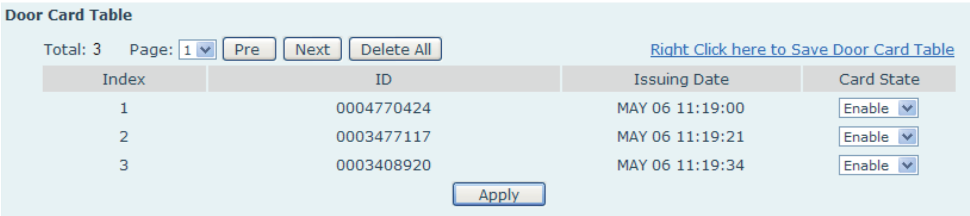
3) Use card to touch card reader induction area, and then hear the card reader confirmed indication tone. You might repeat it to add cards;

4) In web page < card reader Settings > option, select <normal> function;



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

6) The issuing records can be found on the door card list.


Door Card Table

Total: 3 Page: 1 Pre Next Delete All Right Click here to Save Door Card Table

Index	ID	Issuing Date	Card State
1	0004770424	MAY 06 11:19:00	Enable
2	0003477117	MAY 06 11:19:21	Enable
3	0003408920	MAY 06 11:19:34	Enable

Apply

Methods 2: used to batch add cards for intermediate

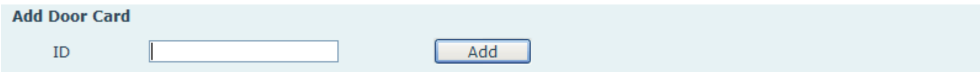
1) Use <Issuer admin card> to touch card reader induction area, and it would be entered issuing card status;

2) Use new cards to touch card reader induction area, and hear the card reader confirmed indication tone. You might repeat it to add cards.

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

Methods 3: use to add few cards

1) Input cards number in door card settings page, and then press add button.

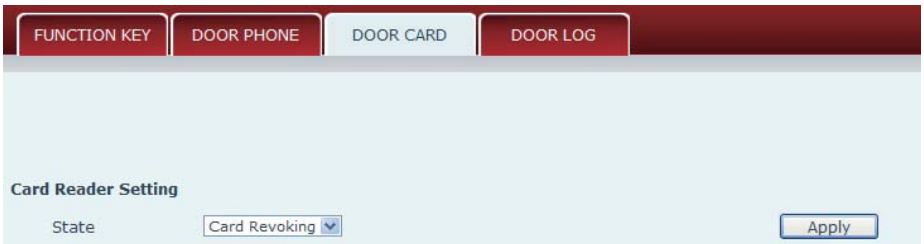


Note: you can also use the USB card reader connected with PC to get cards ID automatically.

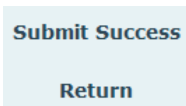
- ## Delete user card

Methods 1: used to batch delete cards for starters

1) In web page <Card Reader Setting> option, select <Card revoking>function;



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



3) Use card to touch card reader induction area, and then hear the card reader confirmed indication tone. You might repeat it to delete cards;

4) In web page < card reader Settings > option, select <normal> function;

Card Reader Setting

State	Normal	Apply

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

Methods 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 hear the card reader confirmed indication tone. You might repeat it to delete cards.

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

Methods 3: use to delete few cards

1) In web page<Delete Door card>, select the card ID and then press delete button.

Delete Door Card

0004770424	Delete

Add Remote access to data

1) Add Access

Fill with the user’s data, and then assign the user's card ID, which is configured in door card table; Click <Add>.

Add Access

Number	7289	
Access Code	8888	
Access by Call	Enable	
Access by Password	Enable	Add
Name	Xiaoming Chen	
Department	market	
Position	employee	
ID	0004770424	
Time Profile	None	
Access Type	Host	

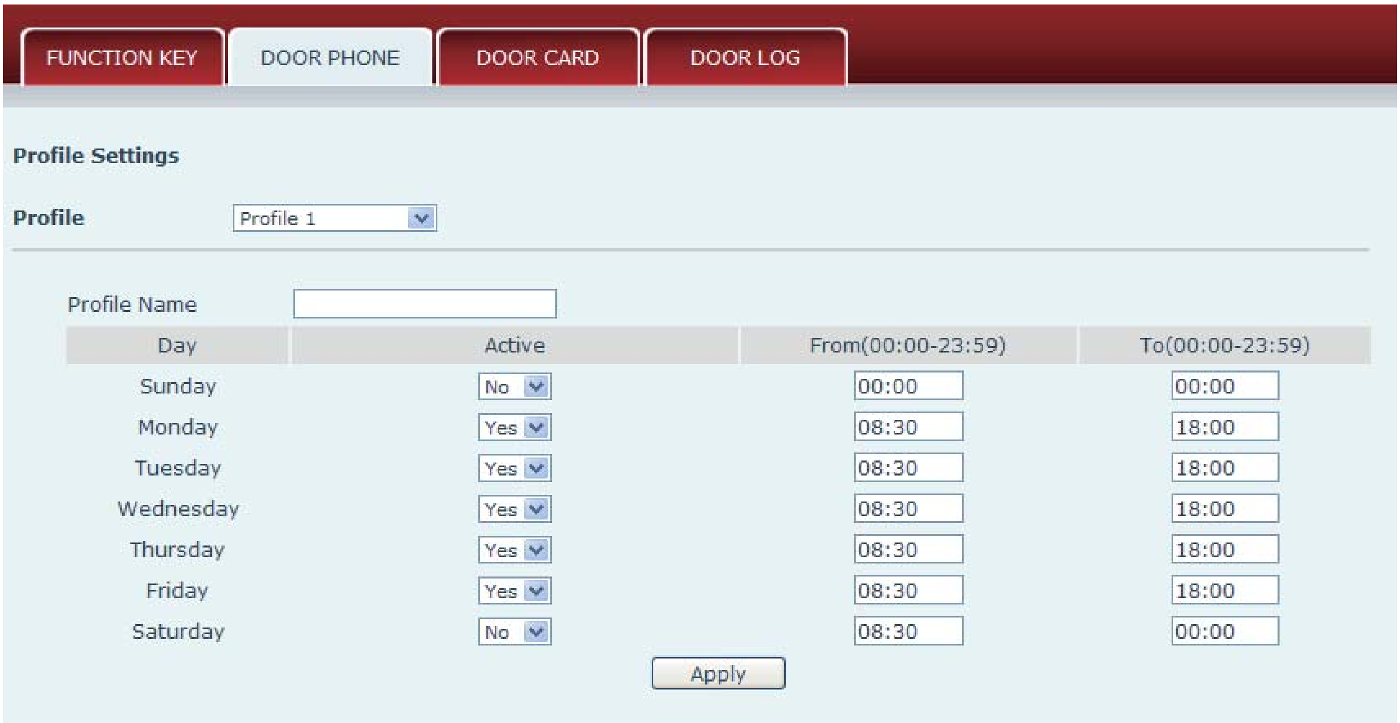
2) Access Table

Access Table

Total: 1 Page: 1 Pre Next Delete All Right Click here to Save Access Table

Index	Number	Access Code	Access by Call	Access by Psw	Name	Department	Position	ID	Time Profile	Access Type
1	7289	8888	Enable	Enable	Xiaoming Chen	employee	market	0004770424	None	Host

3) **Time Profile Settings**



Time Profile Settings	
Time profile sections	There are 4 sections for time profile configuration
Profile Name	The name of profile to help 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