OpenVox Communication Co Ltd

iAG200/400 Series Analog Gateway User Manual

Version 1.0

OpenVox Communication Co Ltd

Address: Room 624, 6/F, Tsinghua Information Port, Book Building, Qingxiang Road, Longhua Street, Longhua District, Shenzhen, Guangdong, China 518109

Tel: +86-755-66630978, 82535461, 82535362

Business Contact: sales@openvox.cn

Technical Support: support@openvox.cn

Business Hours: 09:00-18:00(GMT+8) from Monday to Friday

URL: www.openvoxtech.com

Thank You for Choosing OpenVox Products!

Confidentiality

Information contained herein is of a highly sensitive nature and is confidential and proprietary to OpenVox Inc. No part may be distributed, reproduced or disclosed orally or in written form to any party other than the direct recipients without the express written consent of OpenVox Inc.

Disclaimer

OpenVox Inc. reserves the right to modify the design, characteristics, and products at any time without notification or obligation and shall not be held liable for any error or damage of any kind resulting from the use of this document.

OpenVox has made every effort to ensure that the information contained in this document is accurate and complete; however, the contents of this document are subject to revision without notice. Please contact OpenVox to ensure you have the latest version of this document.

Trademarks

All other trademarks mentioned in this document are the property of their respective owners.

Revise History

Version	Release Date	Description
1.0	11/04/2022	First Version

Contents

1. Overview

1.1 What is iAG Series Analog Gateway?

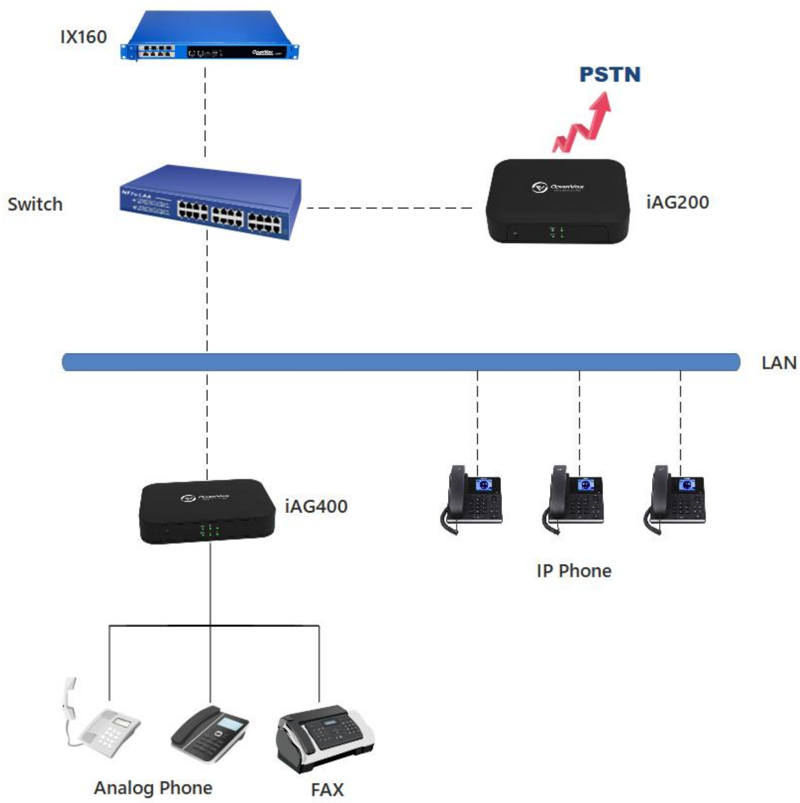
OpenVox iAG200/400 Analog Gateway, a new product of the iAG Series, is specially designed for SMBs and SOHOs. With friendly GUI and unique modular design, users may easily setup their customized gateway. Also secondary development can be completed through AMI (Asterisk Management Interface).

The iAG200/400 Analog Gateways are comprised of five models: iAG200-OS with 1 FXS and 1 FXO ports, iAG200-S with 2 FXS ports, iAG200-O with 2 FXO ports, iAG400-S with 4 FXS ports, iAG400-O with 4 FXO ports.

The iAG200/400 Analog Gateways are developed for interconnecting a wide selection of codecs including G.711A, G.711U, G.729A, G.722, G.726, iLBC. iAG200/400 use standard SIP protocol and compatible with leading VoIP platform, IPPBX and SIP servers, such as Asterisk, Issabel, 3CX, FreeSWITCH, BroadSoft and VOS VoIP operating platform.

1.2 Sample Application

Figure 1-2-1 Topological Graph

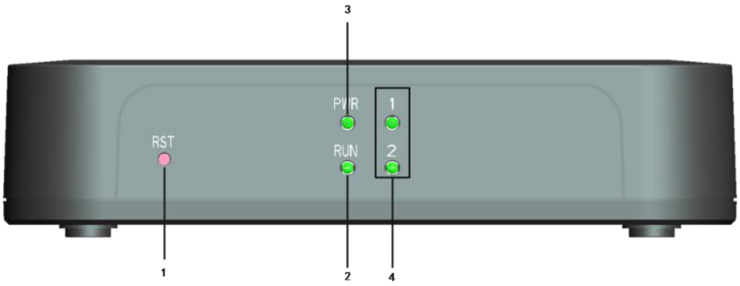


1.3 Product Appearance

The picture below is appearance of iAG200/400 Series Analog Gateway.

Figure 1-3-1 Product Appearance

Figure 1-3-2 Front Panel



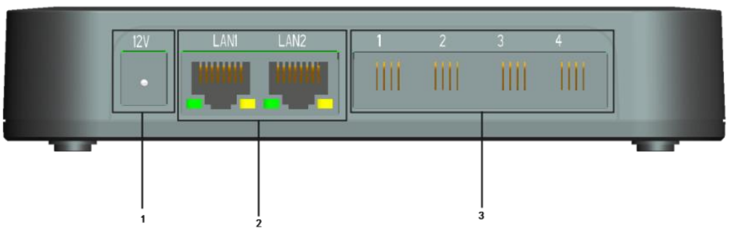
1: Reset Button

2: Running Indicator

2: Power Indicator

3: Analog Telephone Interfaces and corresponding Channels State Indicators

Figure 1-3-3 Back Panel



1: Power Interface

2: Ethernet Ports and Indicators

3: Analog Interface

1.4 Main Features

System Features

- NTP time synchronization and client time synchronization
- Support modify username and password for web login
- Update firmware online, backup/restore configuration file
- Abundant Log Info, Automatically Reboot, Call status display
- Language selection (Chinese/English)
- Open API interface (AMI), support for custom scripts, dialplans
- Support SSH remote operation and restore the factory settings

Telephony Features

- Support Volume adjustment, Gain adjustment, call transfer, call hold, call waiting, call forward, Caller ID display
- Three way calling, Call transfer, Dial-up matching table
- Support T.38 fax relay and T.30 fax transparent, FSK and DTMF signaling
- Support Ring cadence and frequency setting, WMI (Message Waiting Indicator)
- Support Echo cancellation, Jitter buffer
- Support customizable DISA and other applications

SIP Features

- Support add, modify & delete SIP Accounts, batch add, modify & delete SIP Accounts
- Support multiple SIP registrations: Anonymous, Endpoint registers with this gateway, This gateway registers with the endpoint
- SIP accounts can be registered to multiple servers

Network

- Network type： Static IP, Dynamic
- Support DDNS, DNS, DHCP, DTMF relay, NAT
- Telnet, HTTP, HTTPS, SSH
- VPN client
- Network Toolbox

1.5 Physical Information

Table 1-5-1 Description of Physical Information

	iAG200	iAG400
Weight	160g	176g
Size	125mm*85mm*28.7mm	150mm*100mm*28.7mm
Temperature	-20~70°C (Storage)	
	0~50°C (Operation)	
Operation humidity	10%~90% non-condensing	
Power source	12V DC/2A	
Max power	6W	8W

1.6 Software

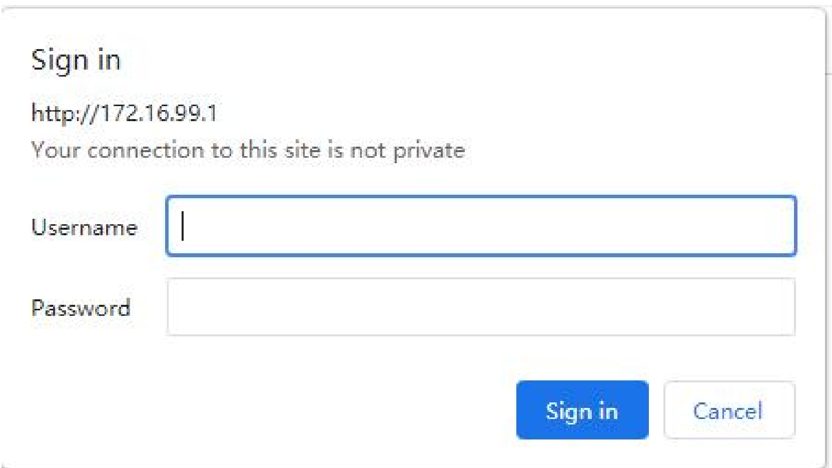
Default IP: 172.16.99.1

Username: admin

Password: admin

Please enter the default IP in your browser to scan and configure the module you want.

Figure 1-6-1 Login Interface

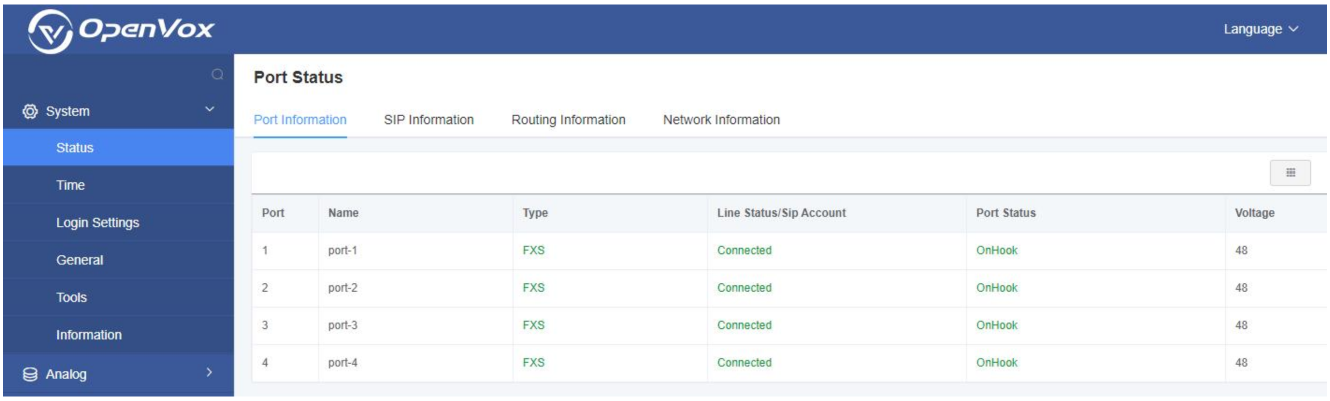


2. System

2.1 Status

On the “Status” page, you will see Port/SIP/Routing/Network information and status.

Figure 2-1-1 System Status



2.2 Time

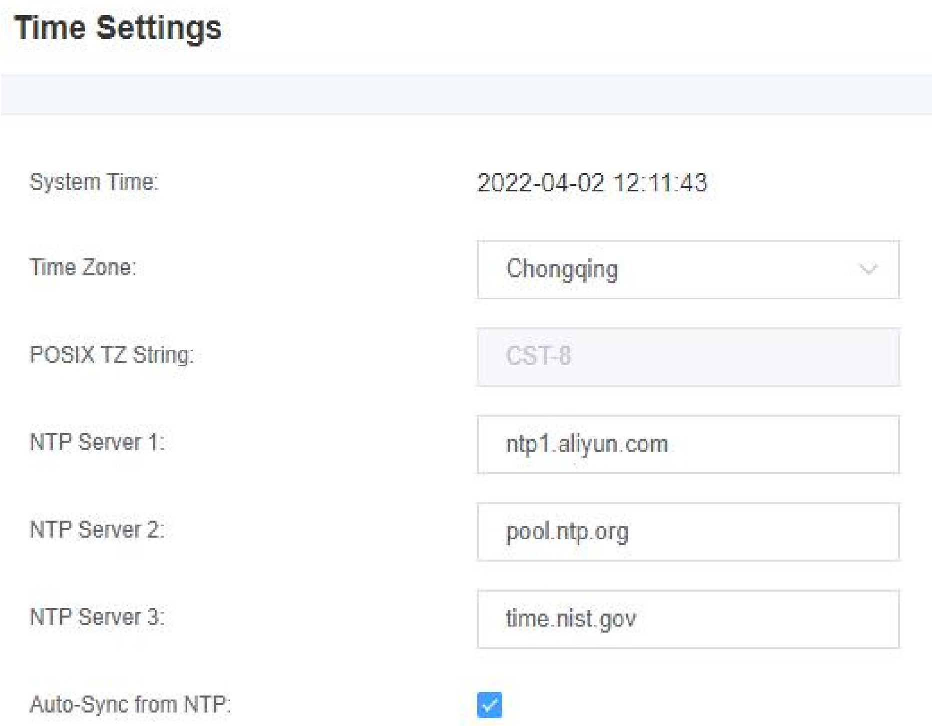
Table 2-2-1 Description of Time Settings

Options	**Definition**
System Time	Your gateway system time.
Time Zone	The world time zone. Please select the one which is the same or the closest as your city.
POSIX TZ String	Posix time zone strings.
NTP Server 1	Time server domain or hostname. For example, [time.asia.apple.com].
NTP Server 2	The first reserved NTP server. For example, [time.windows.com].
NTP Server 3	The second reserved NTP server. For example, [time.nist.gov].
Auto-Sync from NTP	Whether enable automatically synchronize from NTP server or not. ON

	is enable, OFF is disable this function.
Sync from NTP	Sync time from NTP server.
Sync from Client	Sync time from local machine.

For example, you can configure like this:

Figure 2-2-1 Time Settings



You can set your gateway time Sync from NTP or Sync from Client by pressing different buttons.

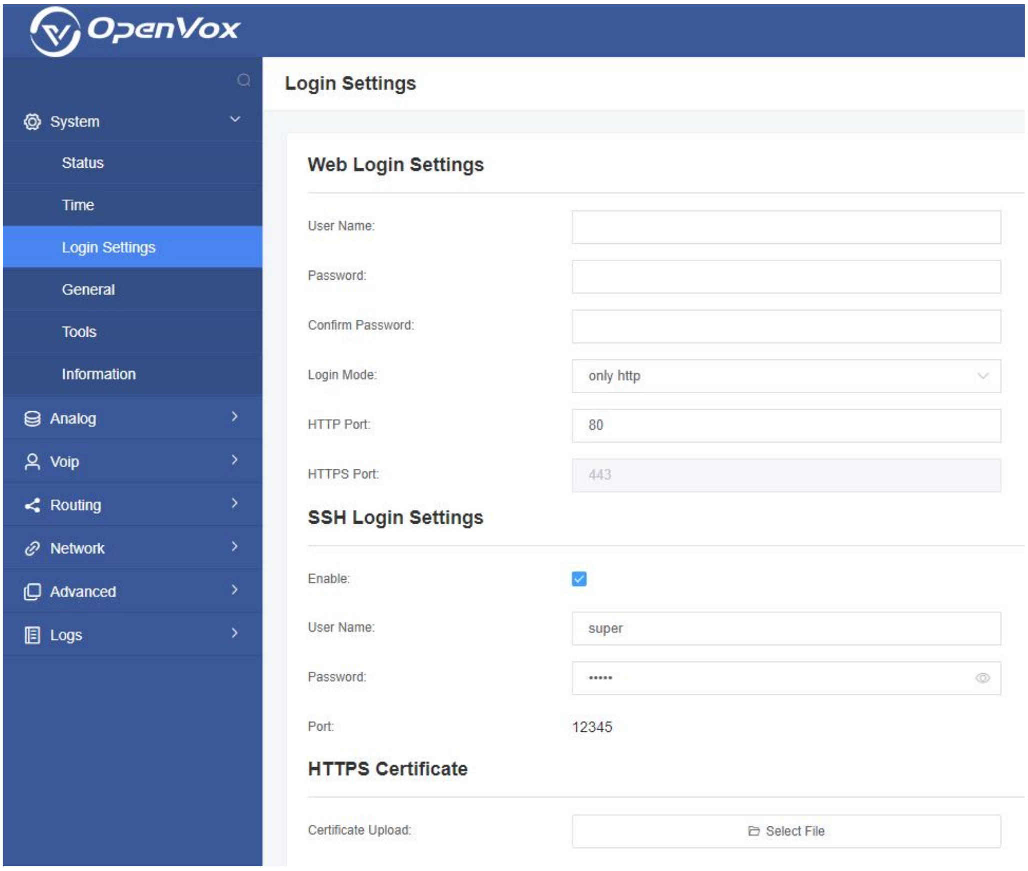
2.3 Login Settings

Your gateway doesn't have administration role. All you can do here is to reset what new username and password to manage your gateway. And it has all privileges to operate your gateway. You can modify both your "Web Login Settings" and "SSH Login Settings". If you have changed these settings, you don't need to log out, just rewriting your new user name and password will be OK.

Table 2-3-1 Description of Login Settings

Options	**Definition**
User Name	Define your username and password to manage your gateway, without space here. Allowed characters "-_+. < >&0-9a-zA-Z". Length: 1-32 characters.
Password	Allowed characters "-_+. < >&0-9a-zA-Z". Length: 4-32 characters.
Confirm Password	Please input the same password as 'Password' above.
Login Mode	Select the mode of login.
HTTP Port	Specify the web server port number.
HTTPS Port	Specify the web server port number.
Port	SSH login port number.

Figure 2-3-1 Login Settings



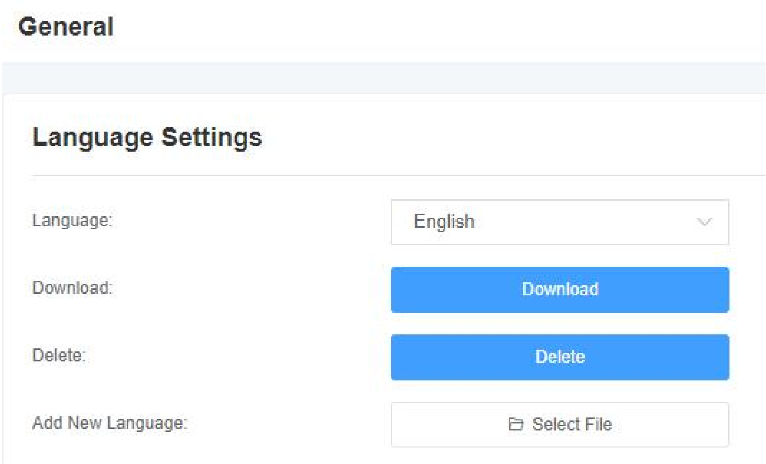
Notice: Whenever you do some changes, do not forget to save your configuration.

2.4 General

2.4.1 Language Settings

You can choose different languages for your system. If you want to change language, you can switch “Advanced” on, then “Download” your current language package. After that, you can modify the package with the language you need. Then upload your modified packages, “Choose File” and “Add”, those will be ok.

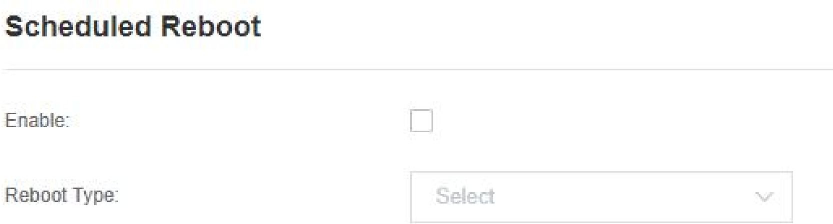
Figure 2-4-1 Language Settings



2.4.2 Scheduled Reboot

You can enable the automatic restart function to make your gateway restart after working for a certain period of time to achieve higher work efficiency.

Figure 2-4-2 Reboot Types

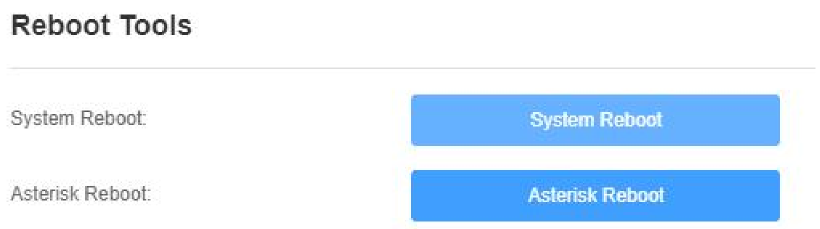


2.5 Tools

On the "Tools" page, users can restart the gateway, upgrade firmware, upload and backup configuration files, and factory restore.

1. The analog gateway supports individual "System Reboot" or "Asterisk Reboot". You can choose "System Reboot" and "Asterisk Reboot" separately.

Figure 2-5-1 Reboot Prompt



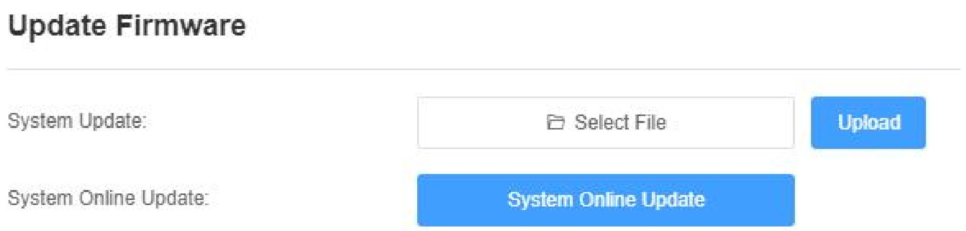
Notice: When you confirm the restart, the system will automatically end all current calls.

Table 2-5-1 Instruction of reboots

Options	Definition
System Reboot	The option will restart your gateway and cut off all current sessions.
Asterisk Reboot	The option will restart Asterisk and cut off all current sessions.

2. The analog gateway provides two firmware upgrade methods, you can choose "System Update" or "System Online Update". To select the system upgrade, you need to download the relevant firmware from the OpenVox website first. The "System Online Update" is an easier way to update your system with one-click.

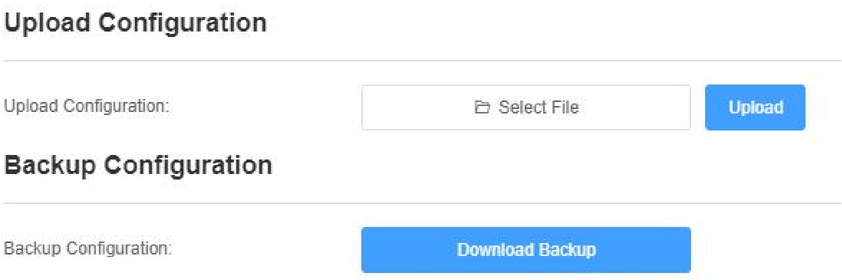
Figure 2-5-2 Update Firmware



3. After configuring your gateway, you can download the current configuration file. When you need to configure other gateways of the same model or restore the gateway to factory settings, you can choose to upload this backup configuration file without the need to reconfigure the gateway .

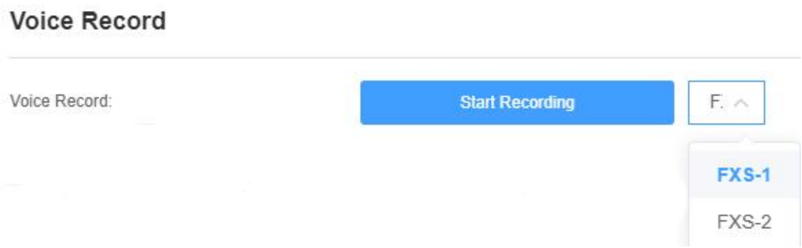
Notice: It will take effect only if the version of the configuration file and the current firmware version are the same.

Figure 2-5-3 Upload and Backup



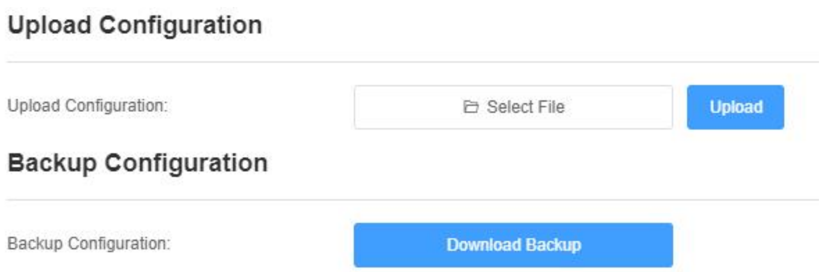
4. If you want to record the voice of the gateway, you can choose "Voice Record". Choose the port which you want to record, and then select "Start Recording".

Figure 2-5-4 Voice Record



5. Sometimes there is something wrong with your gateway that you don't know how to solve it, mostly you will select "Factory Reset".

Figure 2-5-4 Factory Reset

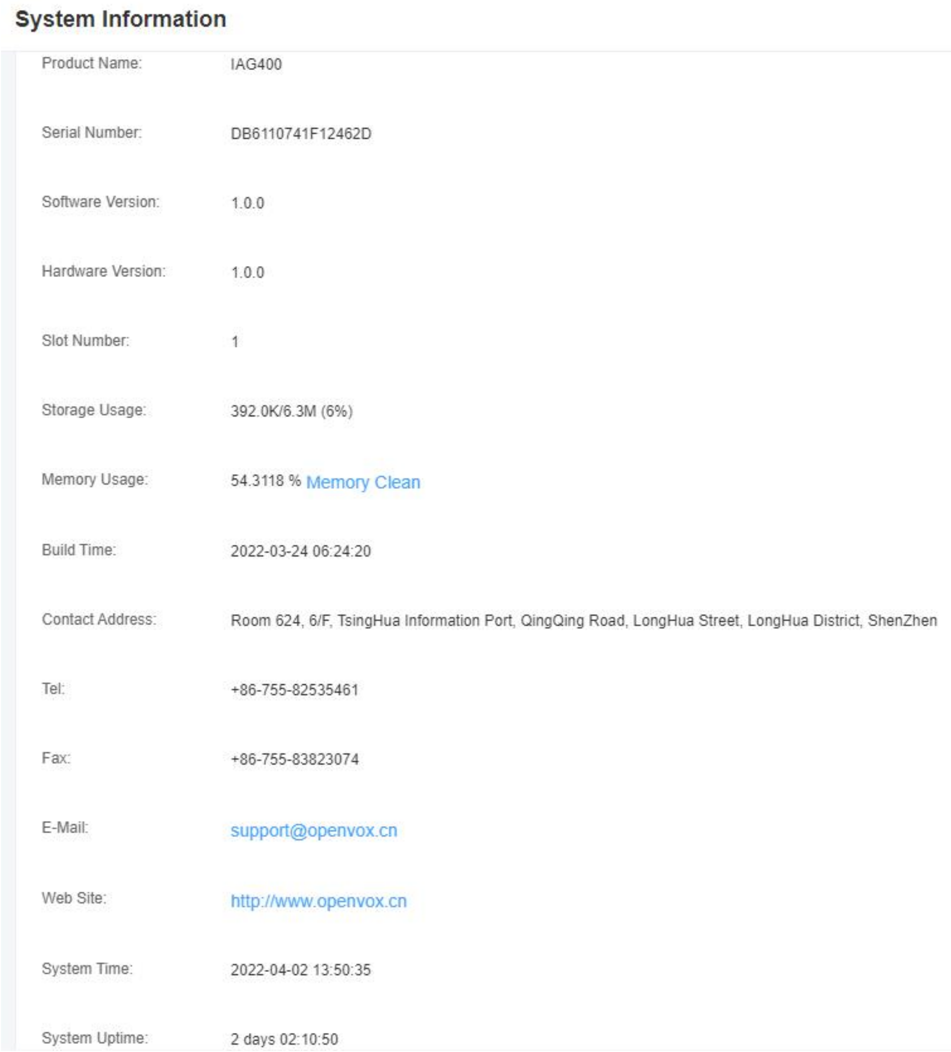


Notice: You can restore the gateway to factory settings by dialing. Connect the phone to the FXS port of the gateway and dial "*1*2*3*4" , then it will restore the gateway to factory settings.

2.6 Information

On the “Information” page, there shows some basic information about the analog gateway. You can see software and hardware version, storage usage, memory usage and some help information.

Figure 2-6-1 System Information

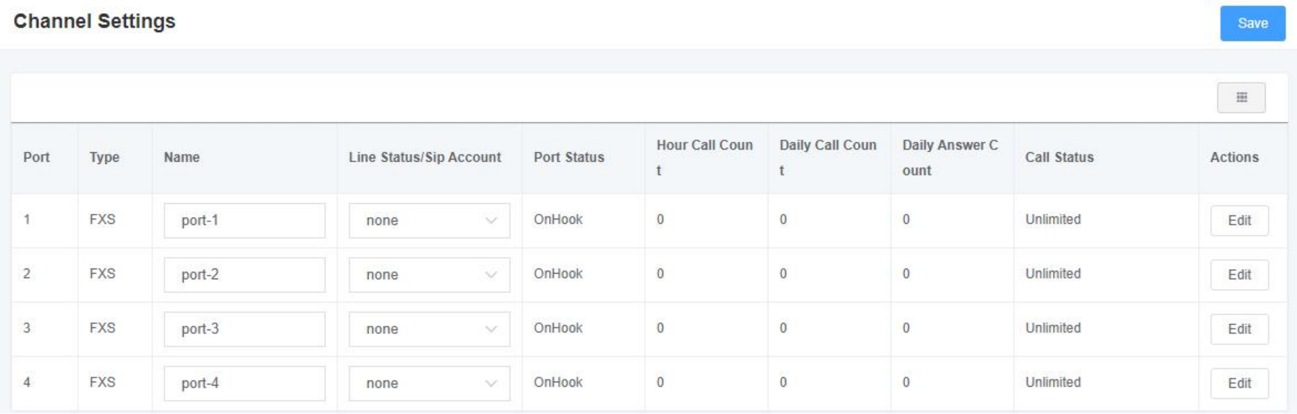


3. Analog

You can see much information about your ports on this page.

3.1 Channel Settings

Figure 3-1-1 Channel System



Click the “Edit” button to modify the corresponding port information.

Figure 3-1-2 FXO Port Configure

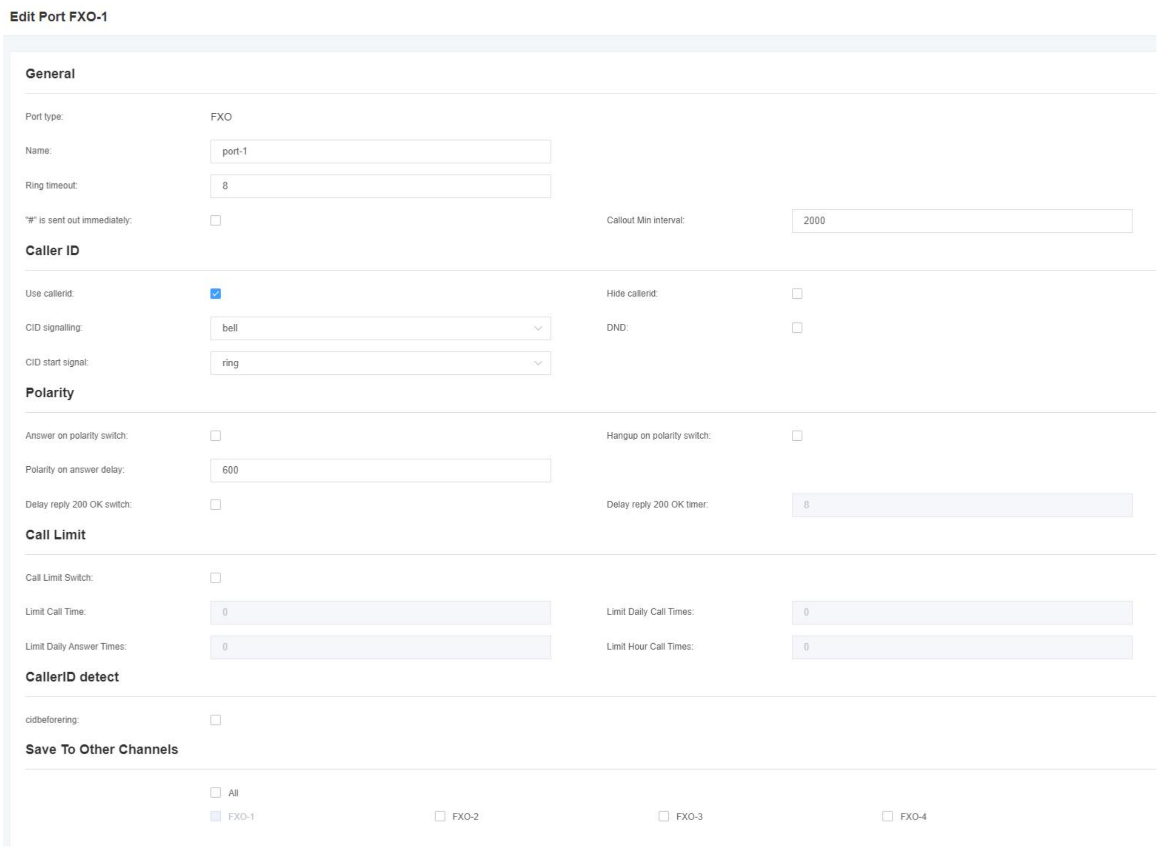
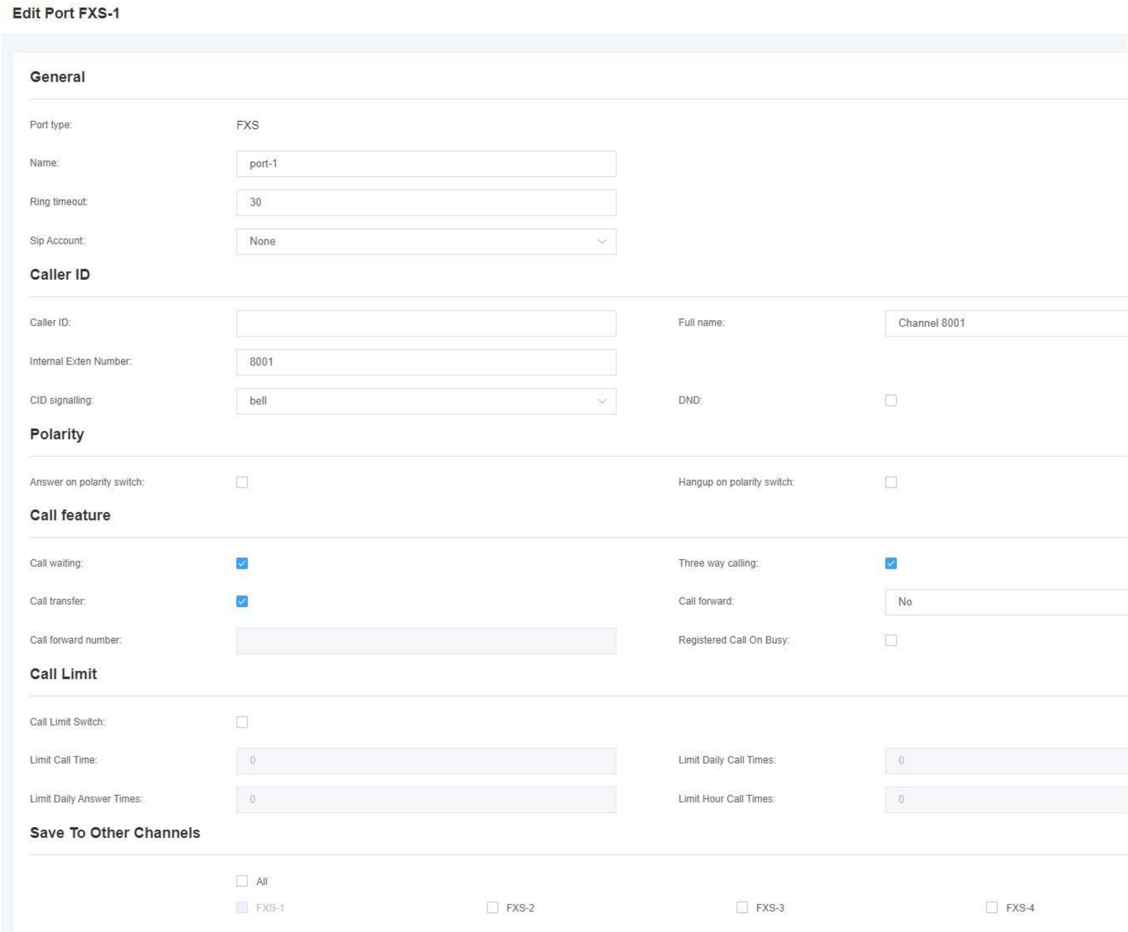


Figure 3-1-3 FXS Port Configure



3.2 Pickup

Call pick-up is a feature used in a telephone system, which allows one to answer someone else's telephone call. You can set the “Time Out” and “Number” parameters either globally or separately for each port. The function is accessed by dialing a series of specific numbers, provided that you enable this function and set the "number" parameter correctly.

Figure 3-2-1 Pickup Settings

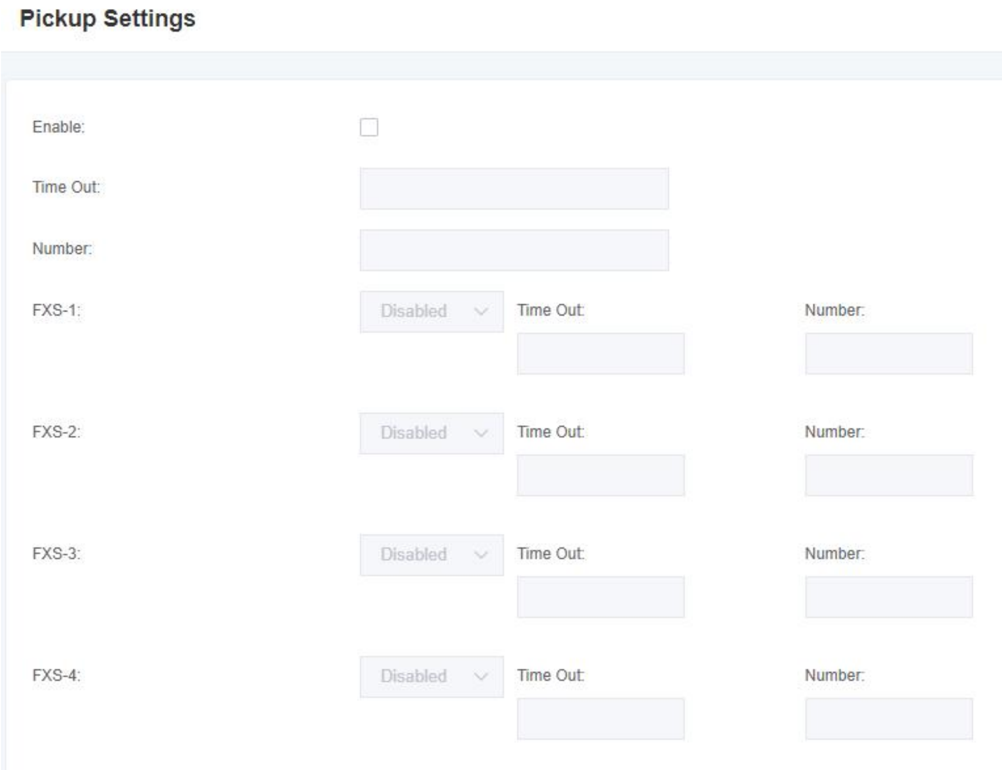


Table 3-2-1 Definition of Pickup

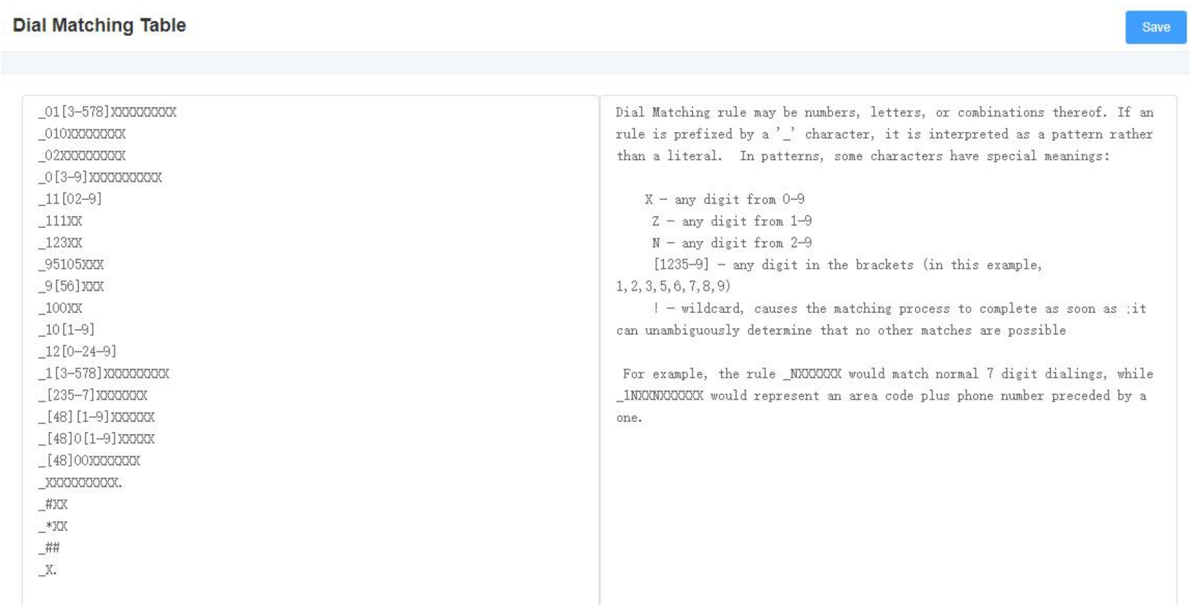
Options	**Definition**
Enable	ON(enabled), OFF(disabled)
Time Out	Set the timeout, in milliseconds (ms).Note: You can only enter numbers.
Number	Pickup number

3.3 Dial Matching Table

The dial matching table is used to effectively judge whether the received number sequence is complete so that it can be sent in time.

The correct use of the dial matching table can help shorten the turn-on time of phone call.

Figure 3-3-1 Port Configure



3.4 Advanced

3.4.1 General

Figure 3-4-1 General Configuration

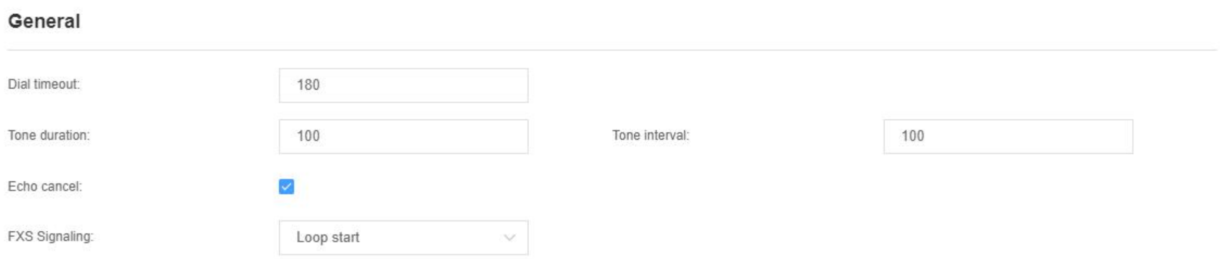


Table 3-4-1 Instruction of General

Options	**Definition**
Dial timeout	Specifies the number of seconds we attempt to dial the specified devices.
Tone duration	How long generated tones (DTMF and MF) will be played on the channel. (in milliseconds)
Tone interval	How long between tone and tone will be played on the channel.(in milliseconds).
Echo cancel	Choose enable echo cancellation or not.
FXS signaling	Default Loop start, busy tone is generated, Kewlstart, power is off, no busy tone is generated

3.4.2 Fax

Figure 3-4-4 Fax Configuration

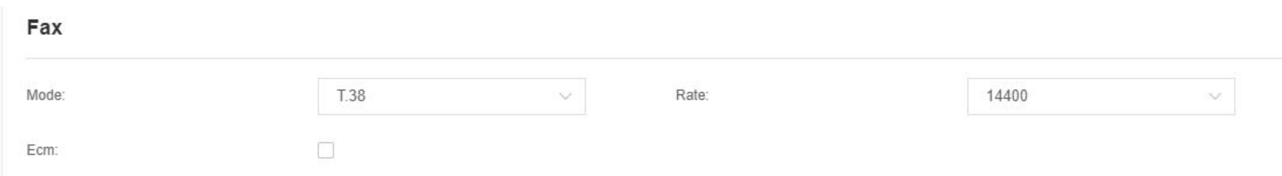


Table 3-4-4 Definition of Fax

Options	Definition
Mode	Set the transmission mode.
Rate	Set the rate of sending and receiving.
Ecm	Enable/disable T.30 ECM (error correction mode) by default.

3.4.3 Country

Figure 3-4-5 Country Configuration

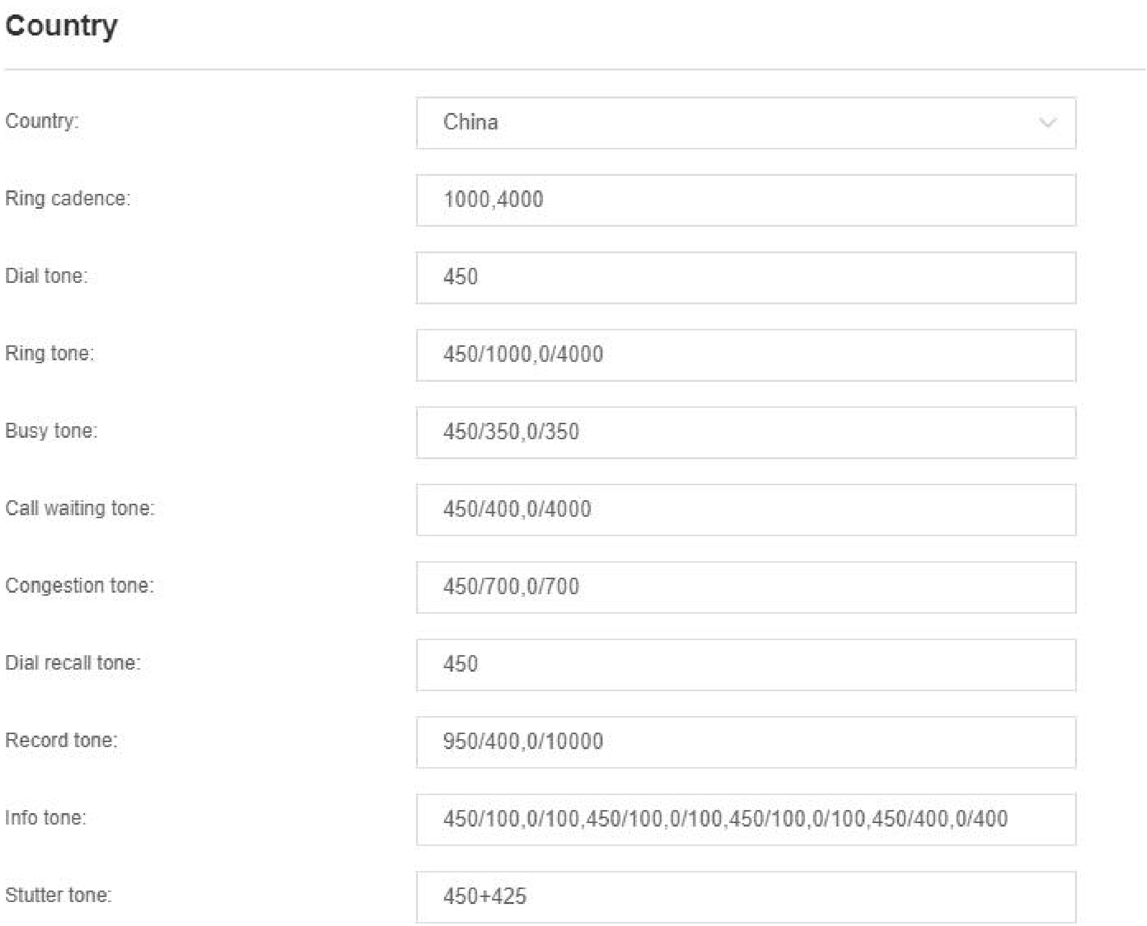
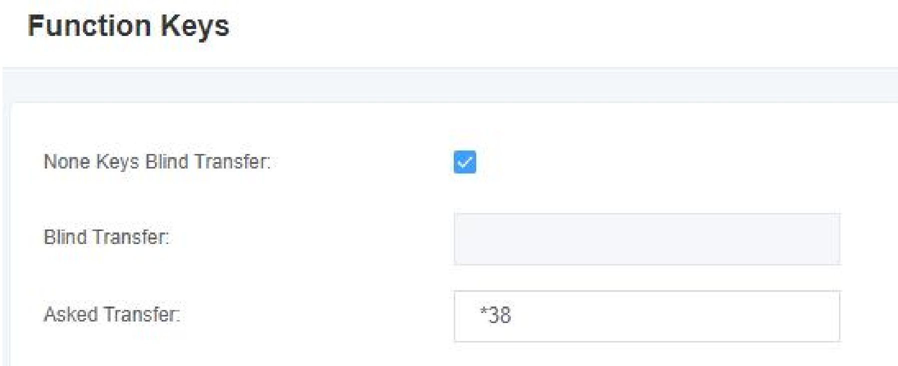


Table 3-4-5 Definition of Country

Options	Definition
Country	Configuration for location specific tone indications.
Ring cadence	List of durations the physical bell rings.
Dial tone	Set of tones to be played when one picks up the hook.
Ring tone	Set of tones to be played when the receiving end is ringing.
Busy tone	Set of tones played when the receiving end is busy.
Call waiting tone	Set of tones played when there is a call waiting in the background.
Congestion tone	Set of tones played when there is some congestion.
Dial recall tone	Many phone systems play a recall dial tone after hook flash.
Record tone	Set of tones played when call recording is in progress.
Info tone	Set of tones played with special information messages (e.g., number is out of service.)

3.5 Special Function Keys

Figure 3-5-1 Function keys



3.6 FXS Settings

Figure 3-6-1 Caller ID

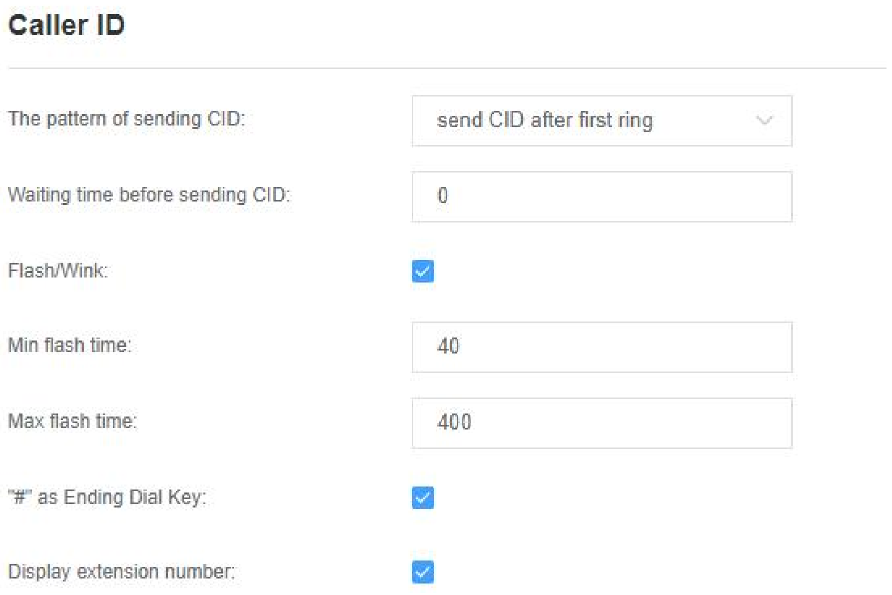


Table 3-4-2 Definition of Caller ID

Options	Definition
The pattern of sending CID	Some countries(UK) have ring tones with different ring tones(ring-ring), which means the caller ID needs to be set later on, and not just after the first ring, as per the default(1).
Waiting time before sending CID	How long we will waiting before sending the CID on the channel.(in milliseconds).
Flash/Wink	Turn on/off Flash/Wink.
Min flash time	Min flash time. (in milliseconds). Range: 1-100.
Max flash time	Max flash time. (in milliseconds). Range:100-3000.
“#” as Ending Dial Key	Turn on/off Ending Dial Key.
Display extension number	Turn on/off display extension number.

Figure 3-6-2 Other Parameters

Table 3-4-2 Definition of Other Parameters

Options	Definition
Offhook-antishake	The anti-jitter delay value when the gateway FXS port detects the off-hook signal. The setting value is from 32ms to 2048ms (multiple of 32) and the default value is 64ms.

3.7 Driver

3.7.1 General

Figure 3-7-1 General

Table 3-7-1 Definition of General

Options	Definition
Codec	Set the global encoding: ulaw, alaw.
Impedance	Configuration for impedance.

3.7.2 CallerID Detect

Figure 3-7-2 CallerID Detect

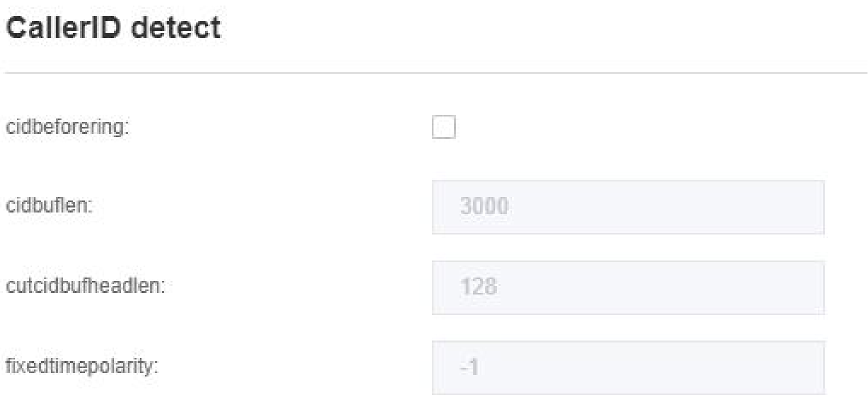


Table 3-7-2 Definition of CallerID Detect

Options	Definition
cidbeforering	Swith to handle irregular CID function.
cidbuflen	CID media stream length byte size.
cutcidbufheadlen	CID media stream header length byte size.
fixedtimepolarity	Transmit polarity line reversal signal delay time.

3.7.3 Hardware Gain

Figure 3-7-3 Hardware Gain

Table 3-7-3 Instruction of Hardware gain

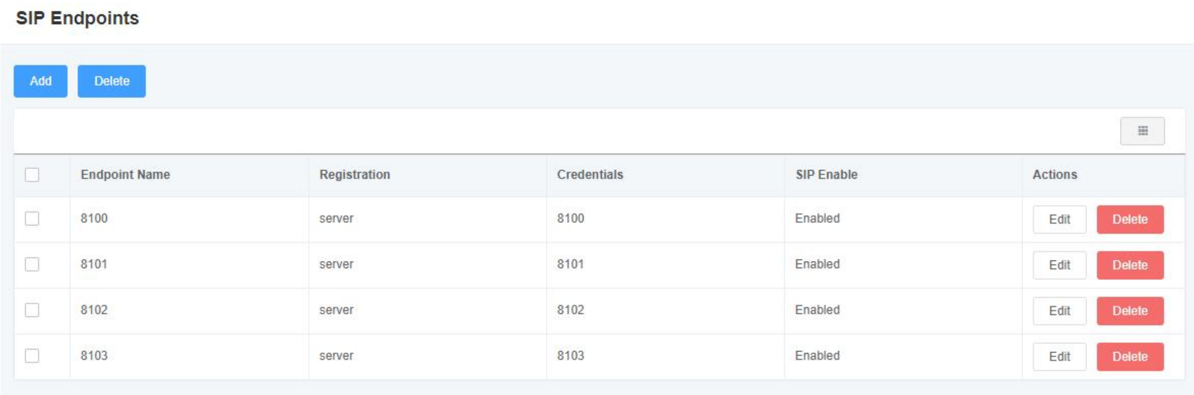
Options	Definition
FXO Rx gain	Set FXO to IP gain. Range: from -150 to 120, the default is 0.
FXO Tx gain	Set FXO to terminal gain. Range: from -150 to 120, the default is 0.
FXS Rx gain	Set FXS to IP gain. Range: -35, 0 or 35. the default is 0.
FXS Tx gain	Set FXS to terminal gain. Range: -35, 0 or 35. the default is 0.

4. VoIP

4.1 SIP Endpoints

On this page, the status information about the SIP account is displayed.

Figure 4-1-1 SIP Status



Click the "Add" button to add a new SIP endpoint, and if you want to modify existed endpoints, you can click "Edit" button.

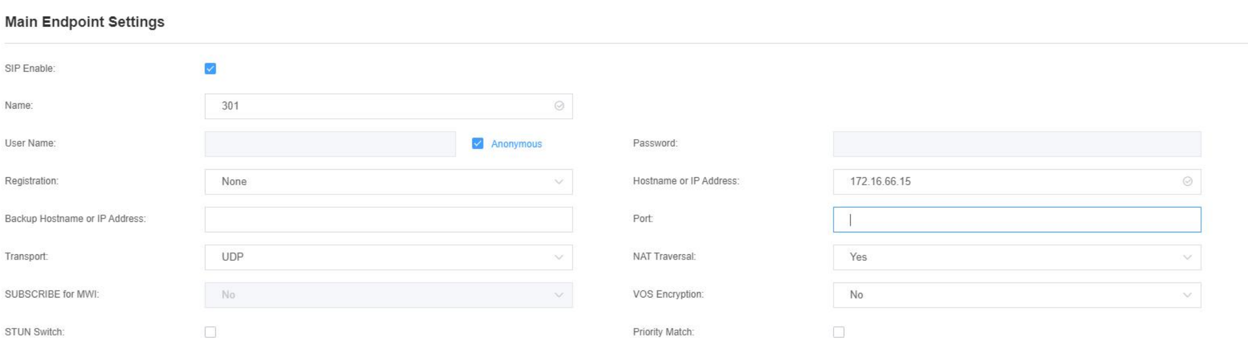
4.1.1 Main Endpoint Settings

There are 3 kinds of registration types for choose. You can choose "None, Client or Server".

You can configure as follows:

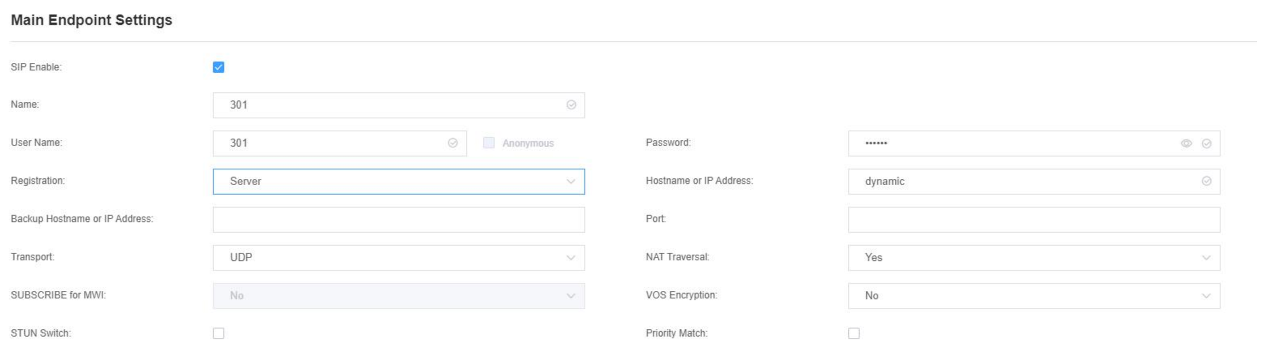
1. If you set up a SIP endpoint by registration "None" to a server, then you can't register other SIP endpoints to this server. (If you add other SIP endpoints, this will cause Out-band Routes and Trunks confused.)

Figure 4-1-2 Main Endpoint Settings - None



2. For convenience, we have designed a method that you can register your SIP endpoint to your gateway, thus your gateway just work as a server.

Figure 4-1-3 Main Endpoint Settings - Server



3. Also you can choose to register by “Client”, it’s the same with “None”, except name and password.

Figure 4-1-4 Main Endpoint Settings - Client

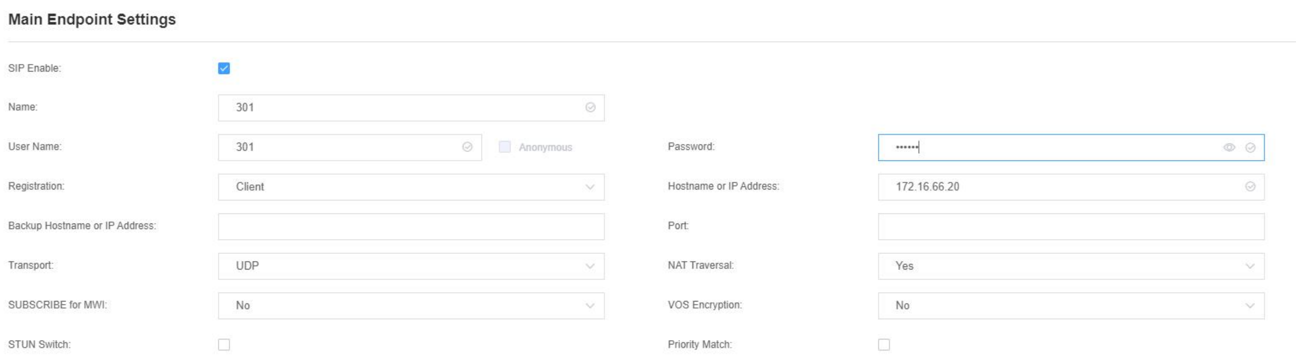


Table 4-1-1 Definition of Endpoint Settings

Options	**Definition**
Name	A name which is able to read. And it’s only used for user’s reference.
Username	Username for authentication between the endpoint and the gateway. Allowed characters: "-_+.<>&0-9a-zA-Z". Length: 1-32 characters.
Password	The password for authentication between the endpoint and the gateway, allowing letters.
Registration	None---Anonymous registration; Server---When register as this type, it means the gateway acts as a SIP server, and the SIP endpoints should register to the gateway; Client---When register as this type, it means the gateway acts as a client, and the endpoint

	should register to a SIP server;
Hostname or IP Address	IP address or hostname of the endpoint or 'dynamic' (if the endpoint has a dynamic IP address). This will require registration.
Transport	Set possible transmission types and order of use for outgoing transmissions. When you use various transport protocols：UDP, TCP, TLS，the transmission type enabled for the first time is only used for outgoing messages until registration occurs. If the endpoint requires another transmission type during the registration process, the first transmission type may be changed to another transmission type.
NAT Traversal	Addresses NAT-related issues in incoming SIP or media sessions. No --- Use Rport if the remote side says to use it. Force Rport on --- Force Rport to always be on. Yes --- Force Rport to always be on and perform comedia RTP handling. Rport if requested and comedia --- Use Rport if the remote side says to use it and perform comedia RTP handling.

4.1.2 Advanced: Registration Options

Figure 4-1-5 Registration Options

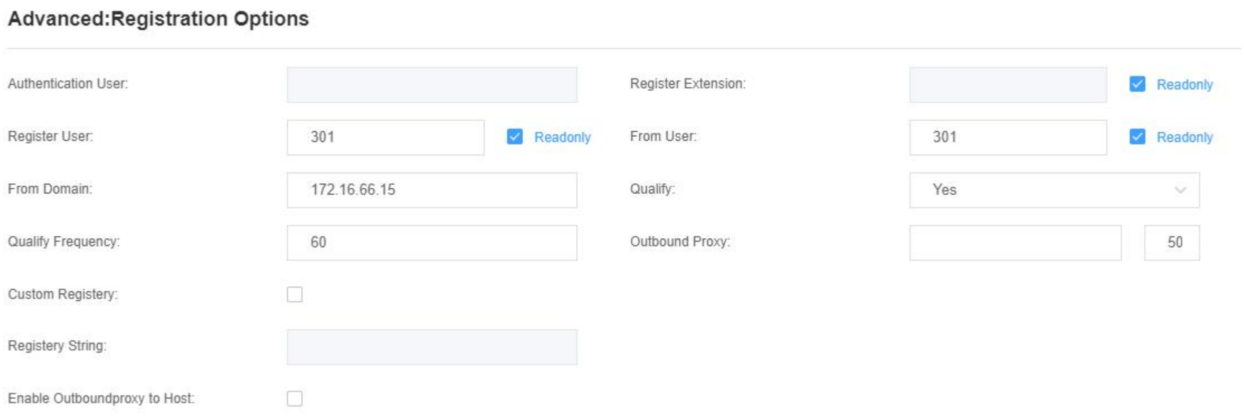


Table 4-1-2 Definition of Registration Options

Options	**Definition**
Authentication User	A username to use only for registration.
Register Extension	When Gateway registers as a SIP user agent to a SIP proxy (provider), calls from this provider connect to this local extension.
Register User	The register username, is the user in “register => user[:secret[:authuser]]@host[:port][/extension]”
From User	A username to identify the gateway to this endpoint.
From Domain	A domain to identify the gateway to this endpoint.
Qualify	Whether or not to check the endpoint's connection status.
Qualify Frequency	How often, in seconds, to check the endpoint's connection status.
Outbound Proxy	A proxy to which the gateway will send all outbound signaling instead of sending signaling directly to endpoints.
Custom Registery	Custom Registery On / Off.
Enable Outboundproxy to Host	Outboundproxy to Host On / Off.

4.1.3 Call Settings

Figure 4-1-6 Definition of Call Settings

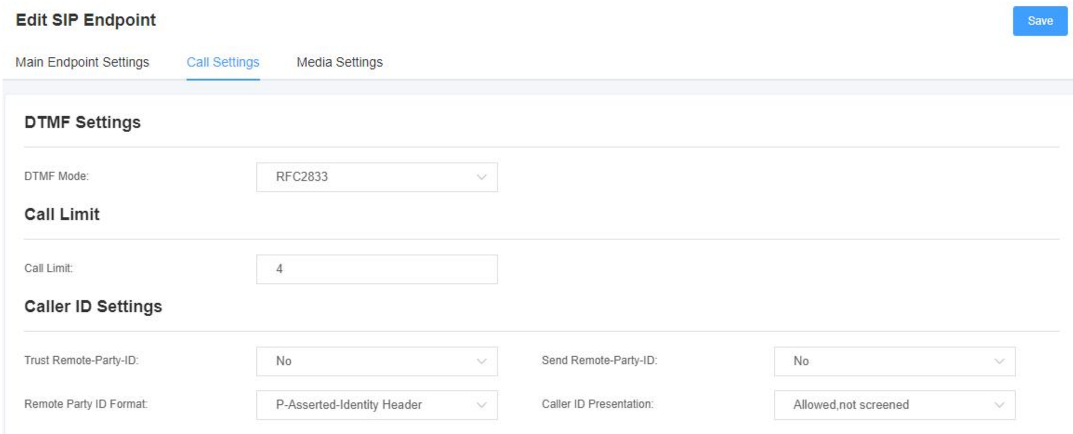


Table 4-1-3 Definition of Call Settings

Options	**Definition**
DTMF Mode	Set default DTMF Mode for sending DTMF. Default: rfc2833. Other options: 'info', SIP INFO message (application/dtmf-relay); 'Inband', Inband audio (require 64kbit codec -alaw, ulaw).
Call Limit	Setting a call-limit will cause calls above the limit not to be accepted.
Trust Remote-Party-ID	Whether or not the Remote-Party-ID header should be trusted.
Send Remote-Party-ID	Whether or not to send the Remote-Party-ID header.
Remote Party ID Format	How to set the Remote-Party-ID header: from Remote-Party-ID or from P-Asserted-Identity.
Caller ID Presentation	Whether or not to display Caller ID.

4.1.4 Advanced: Signaling Settings

Figure 4-1-7 Definition of Signaling Settings

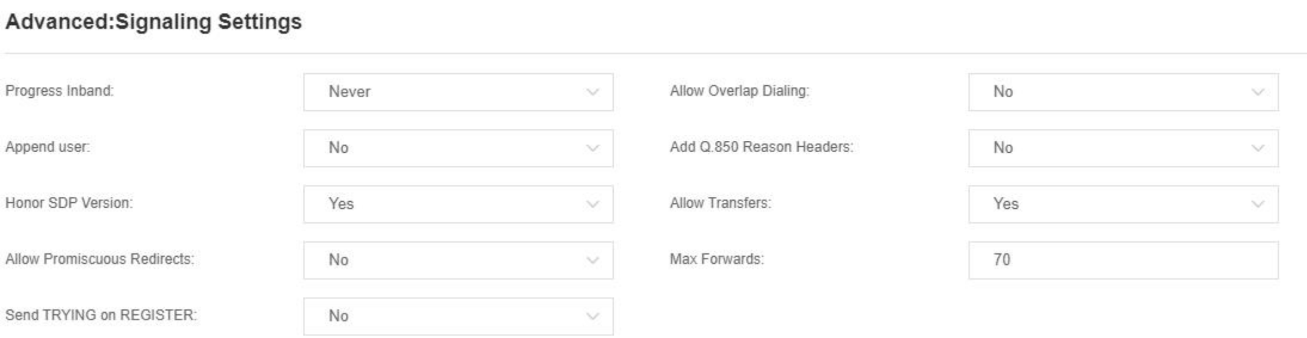


Table 4-1-4 Definition of Signaling Options

Options	**Definition**
Progress Inband	If we should generate in-band ringing. Always use 'never' to never use in-band signaling, even in cases where some buggy devices might not render it. Valid values: yes, no never. Default: never.
Allow Overlap Dialing	Allow Overlap Dialing: Whether or not to allow overlap dialing. Disabled by default.
Append user=phone to URI	Whether or not to add '; user=phone' to URIs that contain a valid phone number.
Add Q.850 Reason Headers	Whether or not to add Reason header and to use it if it is available.
Honor SDP Version	By default, the gateway will honor the session version number in SDP packets and will only modify the SDP session if the version number changes. Turn this option off to force the gateway to ignore the SDP session version number and treat all SDP data as new data. This is required for devices that send non-standard SDP packets (observed with Microsoft OCS). By default this option is on.

Allow Transfers	Whether or not to globally enable transfers. Choosing 'no' will disable all transfers (unless enabled in peers or users). Default is enabled.
Allow Promiscuous Redirects	Whether or not to allow 302 or REDIR to non-local SIP address. Note that promiscredir when redirects are made to the local system will cause loops since this gateway is incapable of performing a "hairpin" call.
Max Forwards	Setting for the SIP Max-Forwards header (loop prevention).
Send TRYING on REGISTER	Send a 100 Trying when the endpoint registers.

4.1.5 Advanced: Timer Settings

Figure 4-1-8 Definition of Timer Settings

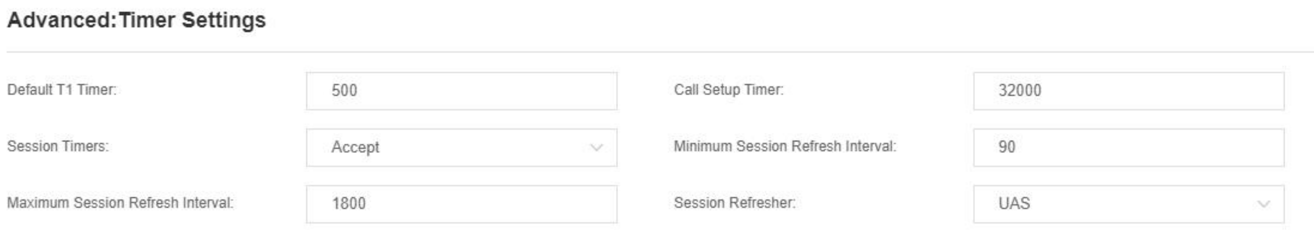


Table 4-1-5 Definition of Timer Options

Options	Definition
Default T1 Timer	This timer is used primarily in INVITE transactions. The default for Timer T1 is 500ms or the measured run-trip time between the gateway and the device if you have qualify=yes for the device.
Call Setup Timer	If a provisional response is not received in this amount of time, the call will auto-congest. Defaults to 64 times the default T1 timer.
Session Timers	Session-Timers feature operates in the following three modes: Originate, request and run session-timers always; Accept, run session-timers only when requested by other UA; Refuse, do not run session timers in any case.
Minimum Session Refresh Interval	Minimum session refresh interval in seconds. Default is 90secs.
Maximum Session Refresh Interval	Maximum session refresh interval in seconds. Defaults to 1800secs.
Session Refresher	The session refresher, uac or uas. Defaults to uas.

4.1.6 Media Settings

Table 4-1-6 Definition of Media Settings

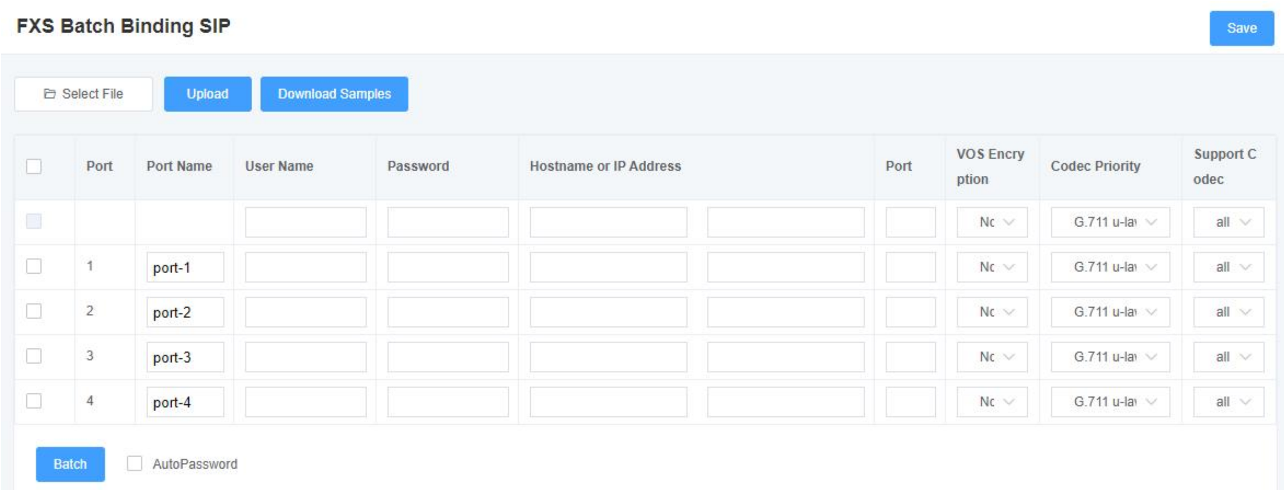
Options	**Definition**
Media Settings	Select codec from the drop down list. Codecs should be different for each Codec Priority.

4.2 FXS Batch Binding SIP

If you want to bind sip accounts in batches on the FXS port, you can configure this page.

Notice: this is only used when "Client" work mode.

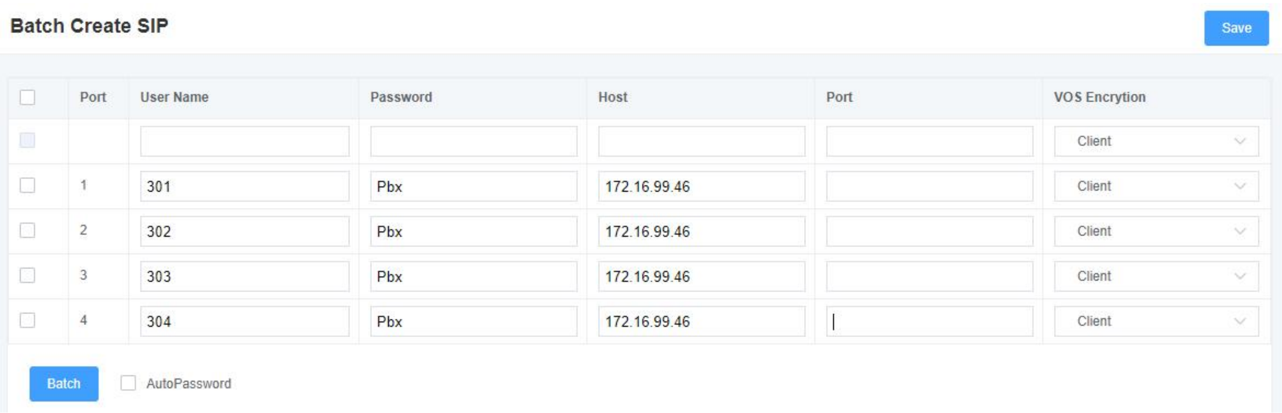
Figure 4-2-1 FXS Batch Binding SIP



4.3 Batch Create SIP

On this interface, users can create multiple SIP accounts at one time. You can choose any registration mode.

Figure 4-3-1 Batch SIP Endpoints



4.4 Advanced SIP Settings

4.4.1 Networking

Figure 4-4-1 Definition of Networking Options

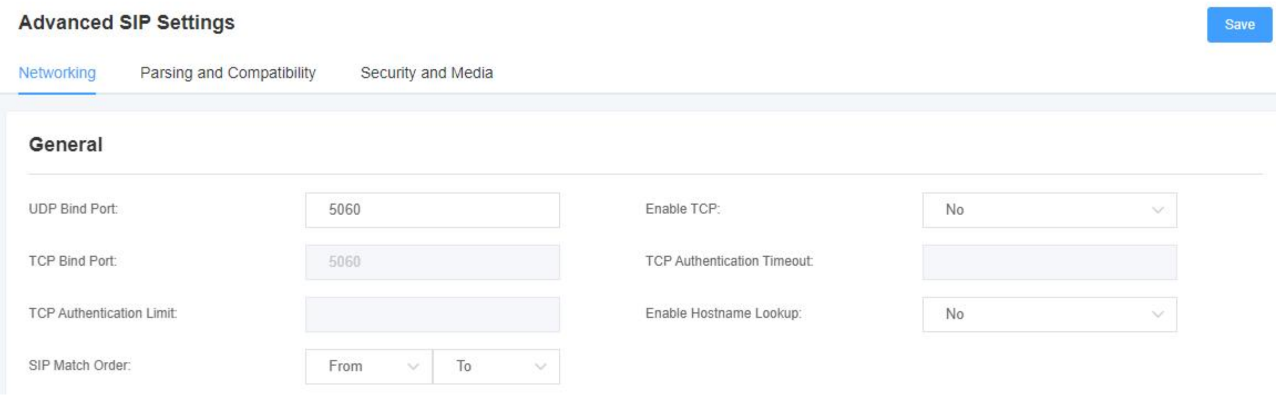


Table 4-4-1 Definition of Networking Options

Options	**Definition**
UDP Bind Port	Choose a port on which to listen for UDP traffic.
Enable TCP	Enable server for incoming TCP connection (default is no).
TCP Bind Port	Choose a port on which to listen for TCP traffic.
TCP Authentication Timeout	The maximum number of seconds a client has to authenticate. If the client does not authenticate before this timeout expires, the client will be disconnected.(default value is: 30 seconds).
TCP Authentication Limit	The maximum number of unauthenticated sessions that will be allowed to connect at any given time(default is:50).
Enable Hostname Lookup	Enable DNS SRV lookups on outbound calls . Note: the gateway only uses the first host in SRV records Disabling DNS SRV lookups disables the ability to place SIP calls based on domain names to some other SIP users on the Internet Sepcifying a port in a SIP peer definition or when dialing outbound calls with supress SRV lookups for that peer or call.

4.4.2 NAT Settings

Figure 4-4-2 Definition of NAT Settings

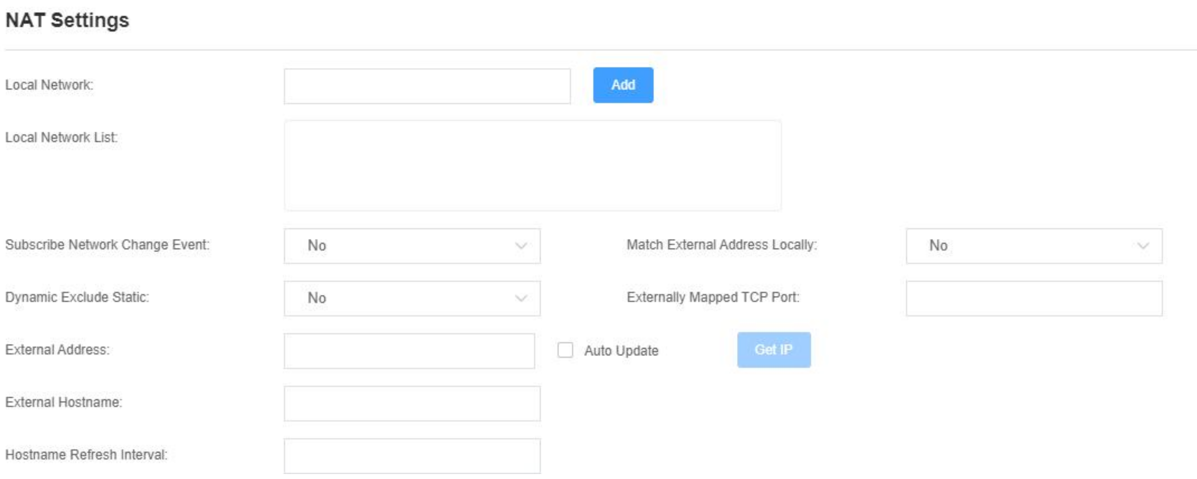


Table 4-4-2 Definition of NAT Settings

Options	Definition
Local Network	Format:192.168.0.0/255.255.0.0 or 172.16.0.0./12. A list of IP address or IP ranges which are located inside a NATed network. This gateway will replace the internal IP address in SIP and SDP messages with the external IP address when a NAT exists between the gateway and other endpoints.
Local Network List	Local IP address list that you added.
Subscribe Network Change Event	Through the use of the test_stun_monitor module, the gateway has the ability to detect when the perceived external network address has changed. When the stun_monitor is installed and configured, chan_sip will renew all outbound registrations when the monitor detects any sort of network change has occurred. By default this option is enabled, but only takes effect once res_stun_monitor is configured. If res_stun_monitor is enabled and you wish to not generate all outbound registrations on a network change, use the option below to disable this feature.
Match External Address Locally	Only substitute the externaddr or externhost setting if it matches
Dynamic Exclude Static	Disallow all dynamic hosts from registering as any IP address. Used for staticly defined hosts. This helps avoid the configuration error of allowing your users to

	register at the same address as a SIP provider.
Externally Mapped TCP Port	The externally mapped TCP port, when the gateway is behind a static NAT or PAT.
External Address	The external address (and optional TCP port) of the NAT. External Address = hostname[:port] specifies a static address[:port] to be used in SIP and SDP messages. Examples: External Address = 12.34.56.78 External Address = 12.34.56.78:9900
External Hostname	The external hostname (and optional TCP port) of the NAT. External Hostname = hostname[:port] is similar to "External Address". Examples: External Hostname = foo.dyndns.net
Hostname Refresh Interval	How often to perform a hostname lookup. This can be useful when your NAT device lets you choose the port mapping, but the IP address is dynamic. Beware, you might suffer from service disruption when the name server resolution fails.

4.4.3 STUN Settings

Figure 4-4-3 Definition of STUN Settings

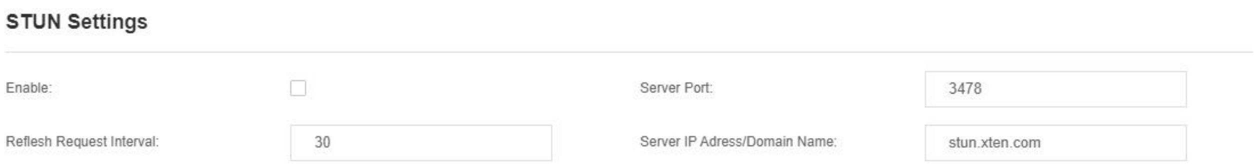


Table 4-4-3 Definition of STUN Settings

Options	**Definition**
Start	Turn on function.
Server Port	Default port 3478.
Refresh Request Interval	Time interval in seconds, default 30 seconds.
Server IP Address/Domain Name	Server address or domain name.

4.4.4 RTP Settings

Figure 4-4-4 Definition of RTP Settings

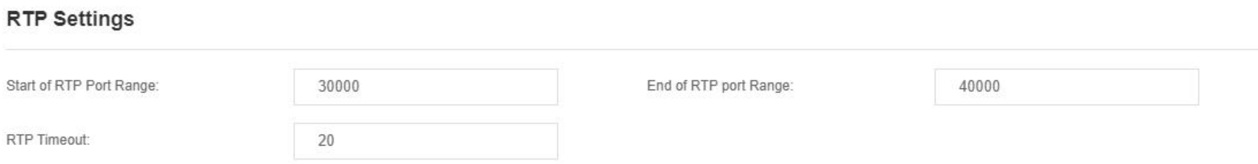


Table 4-4-4 Definition of NAT Settings Options

Options	Definition
Start of RTP Port Range	Start of range of port numbers to be used for RTP.
End of RTP port Range	End of range of port numbers to be used for RTP.
RTP Timeout	RTP Timeout

4.4.5 Parsing and Compatibility

Figure 4-4-5 Definition of Parsing and Compatibility

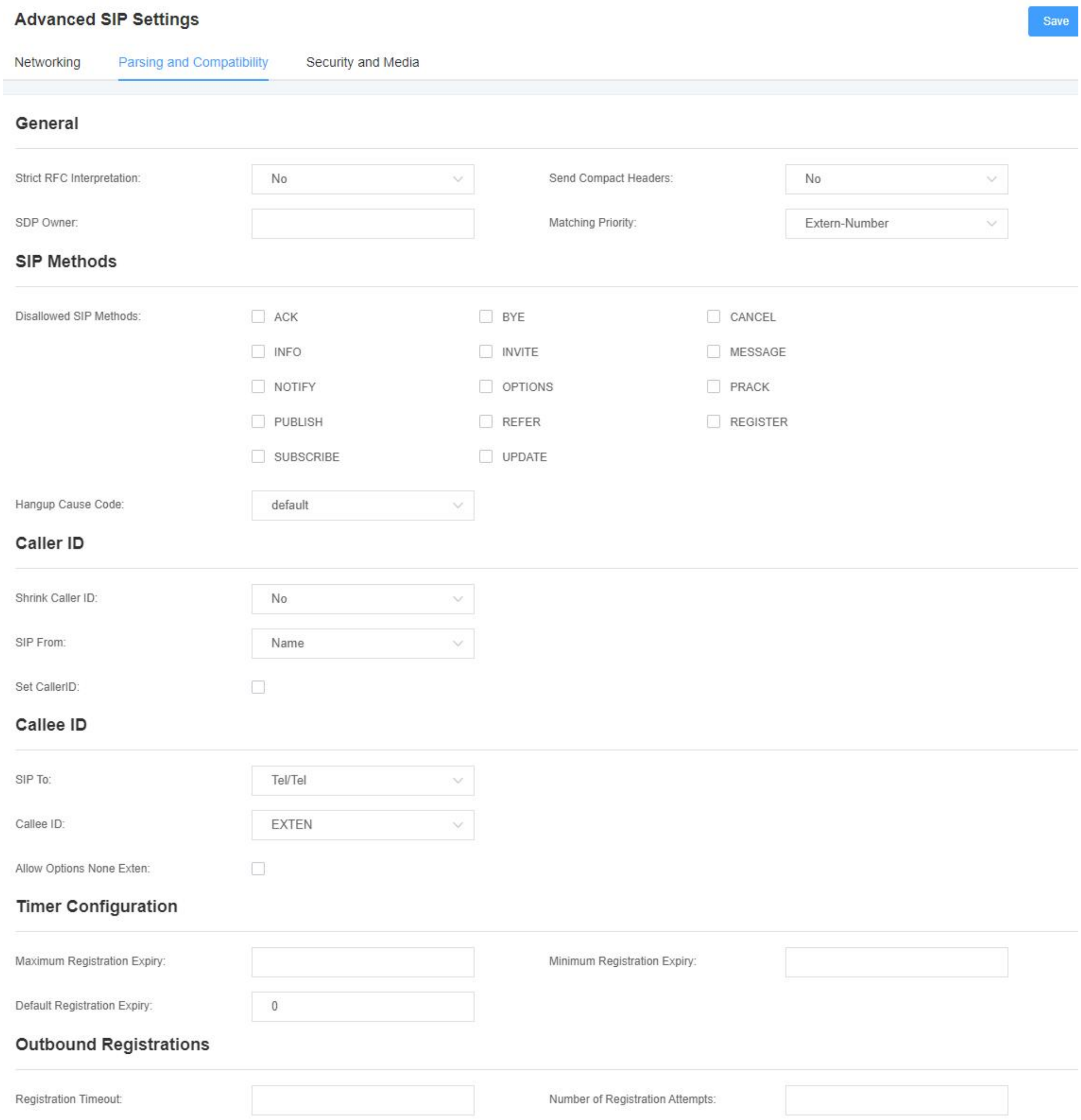


Table 4-4-5 Definition of Parsing and Compatibility

Options	**Definition**
Strict RFC Interpretation	Check header tags, character conversion in URIs, and multiline headers for strict SIP compatibility(default is yes).
Send Compact Headers	Send compact SIP headers.
SDP Owner	Allows you to change the username filed in the SDP owner string. This filed **MUST NOT** contain spaces.
Disallowed SIP Methods	The external hostname (and optional TCP port) of the NAT.
Shrink Caller ID	The shrinkcallerid function removes '(', ' ', ')', non-trailing '.', and '-' not in square brackets. For example, the caller id value 555.5555 becomes 5555555 when this option is enabled. Disabling this option results in no modification of the caller id value, which is necessary when the caller id represents something that must be preserved. By default this option is on.
Maximum Registration Expiry	Maximum allowed time of incoming registrations and subscriptions (seconds).
Minimum Registration Expiry	Minimum length of registrations/subscriptions (default 60).
Default Registration Expiry	Default length of incoming/outgoing registration.
Registration Timeout	How often, in seconds, to retry registration calls. Default 20 seconds.
Number of Registration Attempts	Number of registration attempts before we give up. 0 = continue forever, hammering the other server until it accepts the registration. Default is 0 tries, continue forever.

4.4.6 Security and Media

Figure 4-4-6 Definition of Parsing and Compatibility

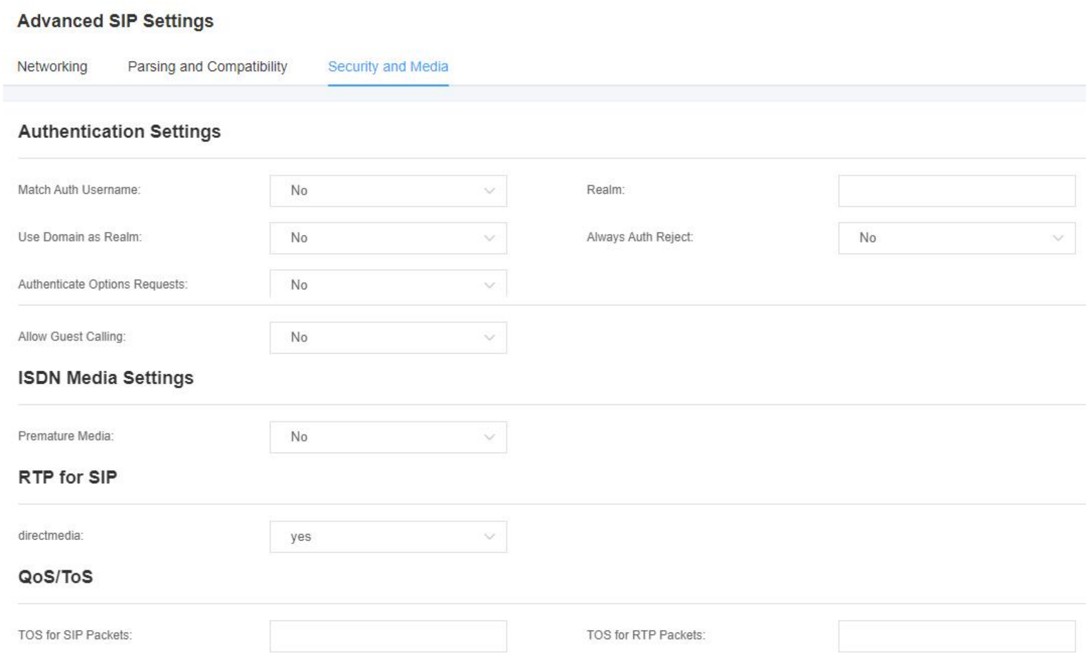


Table 4-4-6 Instruction of Security and Media

Options	**Definition**
Match Auth Username	If available, match user entry using the 'username' field from the authentication line instead of the 'from' field.
Realm	Realm for digest authentication. Realms MUST be globally unique according to RFC 3261. Set this to your host name or domain name.
Use Domain as Realm	Use the domain from the SIP Domains setting as the realm. In this case, the realm will be based on the request 'to' or 'from' header and should match one of the domain. Otherwise, the configured 'realm' value will be used.
Always Auth Reject	When an incoming INVITE or REGISTER is to be rejected, for any reason, always reject with an identical response equivalent to valid username and invalid password/hash instead of letting the requester know whether there was a matching user or peer for their request. This reduces the ability of an

	attacker to scan for valid SIP usernames. This option is set to 'yes' by default.
Authenticate Options Requests	Enabling this option will authenticate OPTIONS requests just like INVITE requests are. By default this option is disabled.
Allow Guest Calling	Allow or reject guest calls (default is yes, to allow). If your gateway is connected to the Internet and you allow guest calls, you want to check which services you offer everyone out there, by enabling them in the default context.
Premature Media	Some ISDN links send empty media frames before the call is in ringing or progress state. The SIP channel will then send 183 indicating early media which will be empty - thus users get no ring signal. Setting this to "yes" will stop any media before we have call progress (meaning the SIP channel will not send 183 Session Progress for early media). Default is 'yes'. Also make sure that the SIP peer is configured with progressinband=never. In order for 'noanswer' applications to work, you need to run the progress() application in the priority before the app.
TOS for SIP Packets	Sets type of service for SIP packets
TOS for RTP Packets	Sets type of service for RTP packets

4.5 Sip Account Security

This analog gateway support TLS protocl for encrypting calls. On the one hand, it can worked as TLS server, generate the session keys used for the secure connection. On the other hand, it also can be registered as a client, upload the key files provied by the server.

Figure 4-5-1 TLS settings

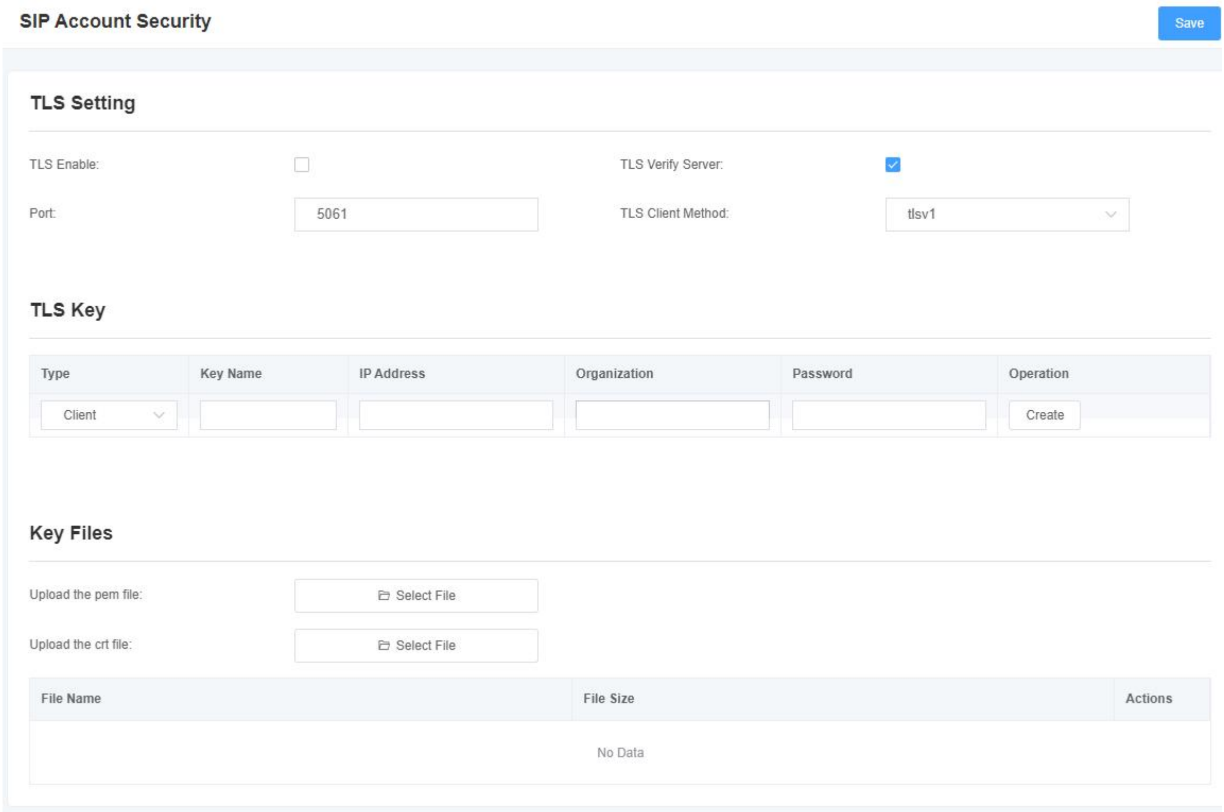


Table 4-5-1 Instruction of TLS

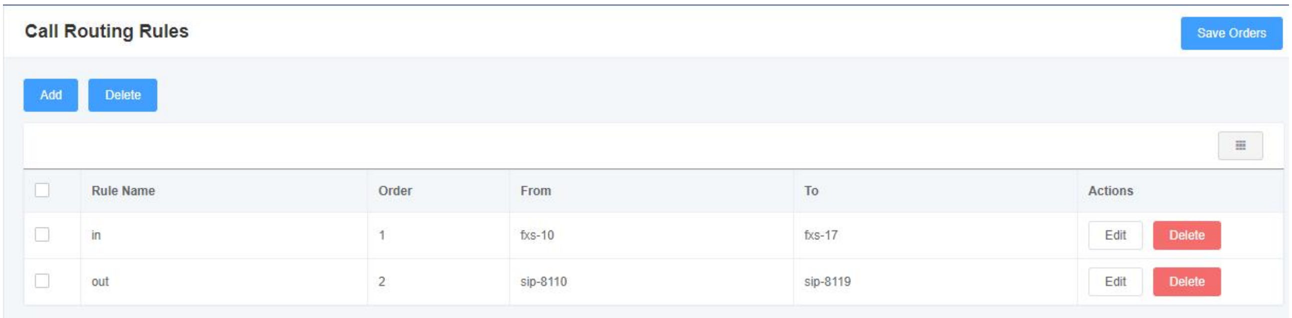
Options	Definition
TLS Enable	Enable or disable DTLS-SRTP support.
TLS Verify Server	Enable or disable tls verify server(default is no).
Port	Specify the port for remote connection.
TLS Client Method	Values include tlsv1, sslv3, sslv2, Specify protocol for outbound client connections, default is sslv2.

5. Routing

The gateway has a friendly user interface and very flexible settings. It supports up to 512 routing rules and each routing rule supports up to 100 pairs of calling/called number filtering and conversion operations. It support DID function The gateway supports trunk group and trunk priority management.

5.1 Call Routing Rules

Figure 5-1-1 Routing Rules



Click “Add”, you can set up a new routing rule. Click "Edit" to modify the routing rule, and click "Delete" to delete the routing rule.

Figure 5-1-2 Example of Setup Routing Rule

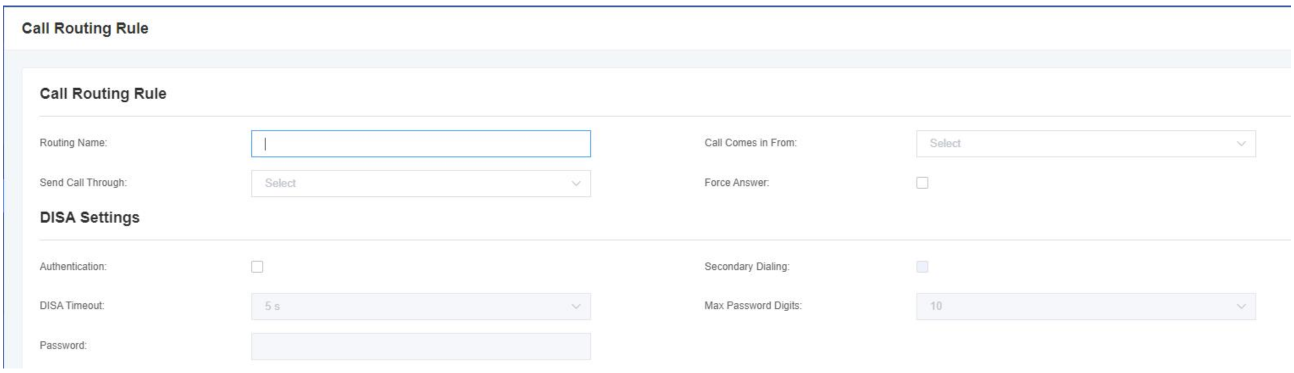


Table 5-1-1 Definition of Call Routing Rule

Options	**Definition**
Routing Name	This is a rule name. The type of match usually used to describe (for example, "sip1 TO port" or "port1 TO sip1").
Call Is From	Source of the call.
Call Delivery	The destination to receive the incoming calls.
DISA Timeout	The specific setting time of DISA timeout.
Maximum Number of Digits In Password	Set the maximum number of password digits
Password	Set a password within the specified range

Figure 5-1-3 Advance Routing Rule

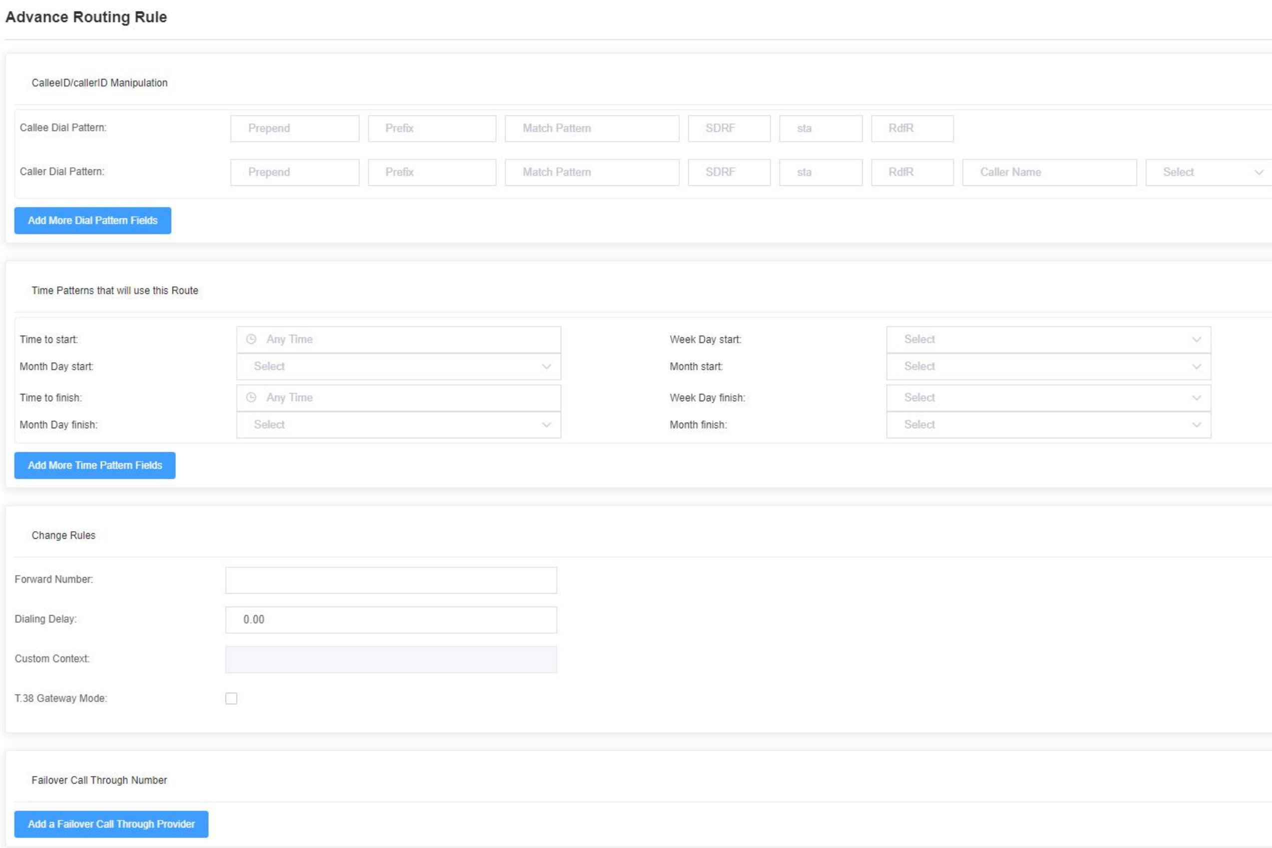


Table 5-1-3 Definition of Advance Routing Rule

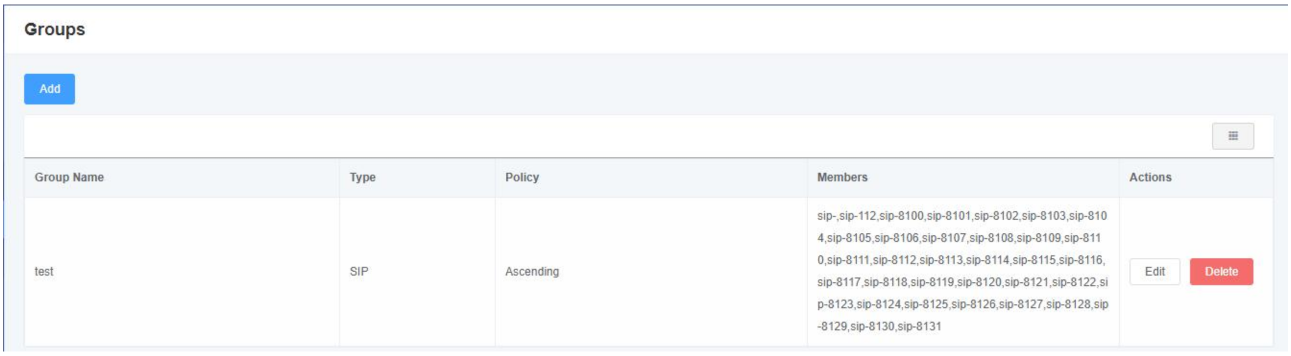
Options	Definition
CalleeID/callerID Manipulation	A Dial Pattern is a unique set of digits that will select this route and send the call to the designated trunks. If a dialed pattern matches this route, no subsequent routes will be tried. If Time Groups are enabled, subsequent routes will be checked for matches outside of the designated time(s). X matches any digit from 0-9 Z matches any digit from 1-9 N matches any digit from 2-9 [1237-9]matches any digit in the brackets (example: 1,2,3,7,8,9) ***matches one or more digits** Prepend<add prefix>: The number added when the pattern matches successfully. If the dialed number matches the pattern specified in the subsequent column, the number will be added before being sent to the trunk. Prefix: Removed when the pattern is matched successfully. The dialed number is matched with the pattern specified in the subsequent column. Once the match is successful, the prefix will be removed from the number before being sent to the trunk. Match Pattern: The dialed number will be compared with the number in the ”prefix +” this matching pattern. Once the match is successful, the matched pattern part of the dial will be sent to the trunks. SDfR<Delete digits from the right>: The number of digits to be deleted from the right end of the number. If this value of this item exceeds the length of the current number, the entire number will be deleted. RDfR<Reserved digits from the right>: The reserved digits from the right. StA<Add Suffix>: Add this number from the right end of the current number. Caller Name <caller display name>: Set your favorite caller name before sending this call to the terminal, allowing the use of local languages, such as Chinese and Latin.
Time Patterns	Time mode setting of routing rules.

that will use this Route	
Forward Number	What destination number will you dial? This is very useful when you have a transfer call.
Failover Call Through Number	The gateway will attempt to send the call out each of these in the order you specify.

5.2 Groups

Sometimes you want to make a call through one port, but you don't know if it is available, so you have to check which port is free. That would be troublesome. But with our product, you don't need to worry about it. You can combine many Ports or SIP to groups. Then if you want to make a call, it will find available port automatically.

Figure 5-2-1 Group Rules



You can click the "Add" button to set up a new group, if you want to modify an existing group, you can click the "Edit" button.

Figure 5-2-2 Create a Group

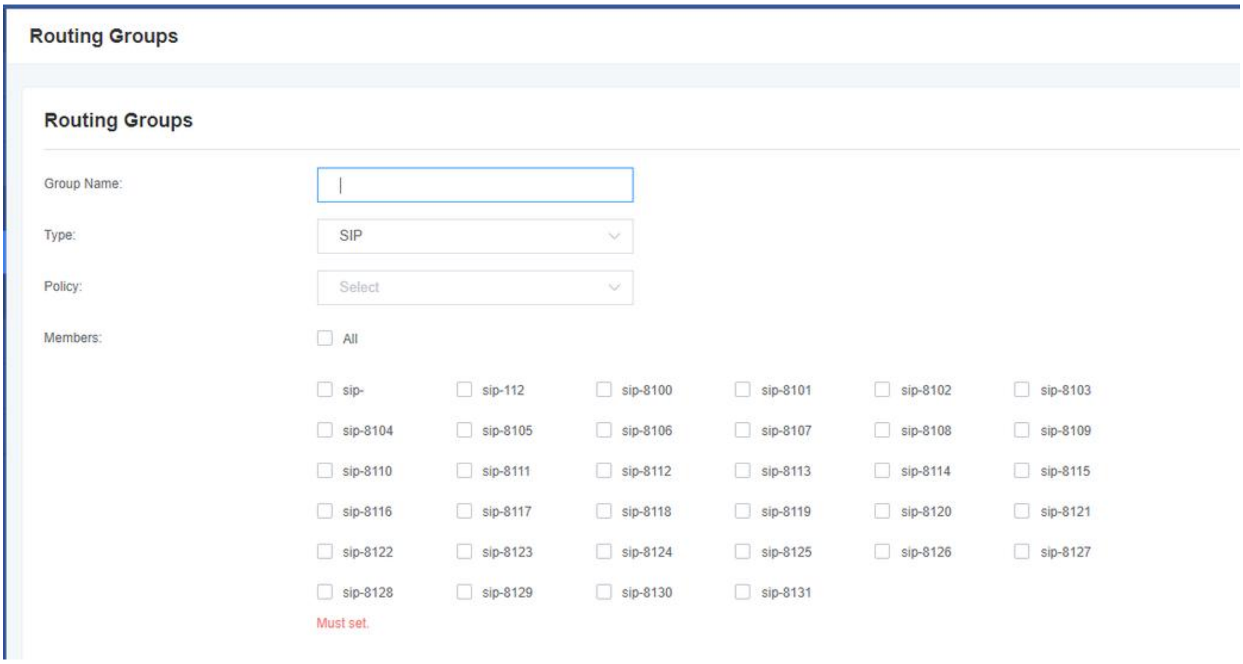


Figure 5-2-3 Modify a Group

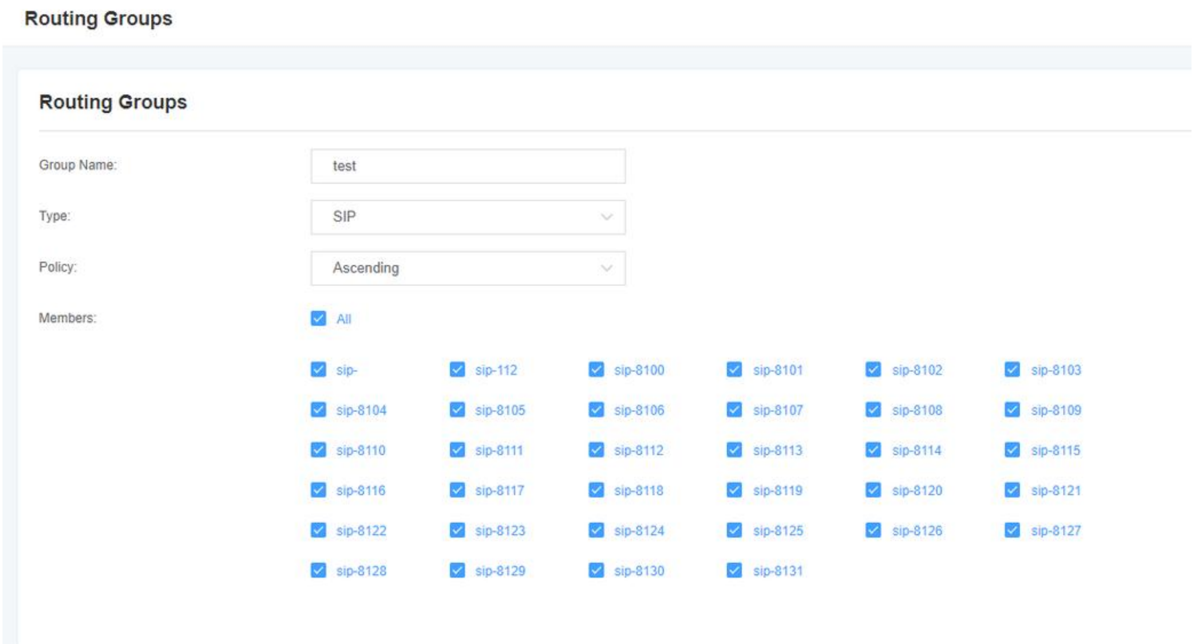


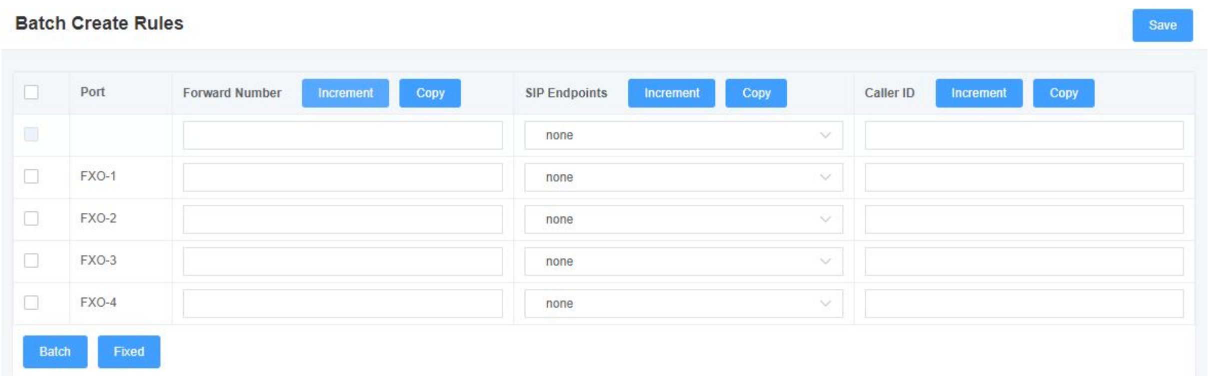
Table 5-2-1 Definition of Routing Groups

Options	**Definition**
Group Name	The name of this route. Should be used to describe what types of calls this route matches(for example, 'sip1TOport1' or 'port1TOsip2').

5.3 Batch Create Rules

If you bind telephone for each FXO port and want to establish separate call routings for them. For convenience, you can batch create call routing rules for each FXO port at once in this page.

Figure 5-3-1 Batch Create Rules



6. Network

6.1 Network Settings

There are three types of LAN port IP to choose from： Factory, Static and DHCP. The default type is: factory, the default IP is 172.16.99.1. If you forget the current IP, you can connect the phone to any FXS port of the analog gateway and dial "**" to query the current IP.

Figure 6-1-1 LAN Settings Interface

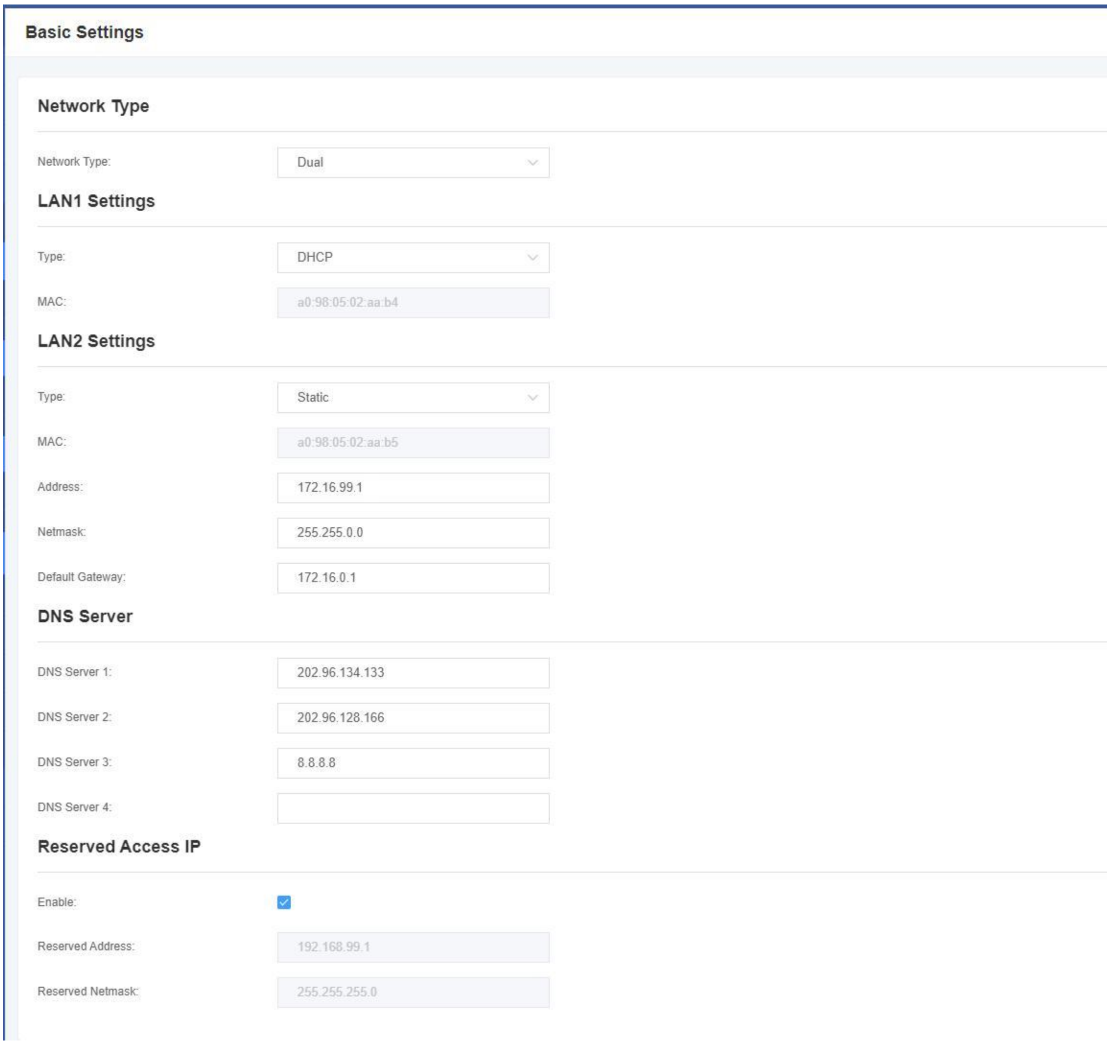


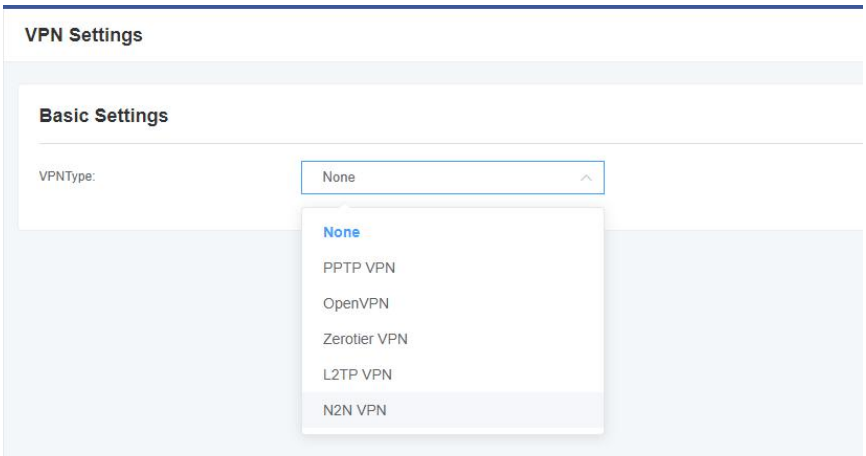
Table 6-1-1 Definition of Network Settings

Options	**Definition**
Network Type	The name of network interface.
Type	The method to get IP. Static: manually set up your gateway IP. DHCP: dynamically obtain the gateway IP address.
Address	The IP address of your gateway.
Netmask	The subnet mask of your gateway.
Default Gateway	Default getaway IP address.
Reserved Access IP	List of domain name server IP addresses. This information is mainly obtained from the local network service provider.
Enable	Enable or disable the reserved IP address switch. ON(enabled), OFF(disabled)
Reserved Address	The reserved IP address for this gateway.
Reserved Netmask	The subnet mask of the reserved IP address.

6.2 VPN Settings

You can select VPN type and upload OpenVPN client configuration file or fill in PPTP VPN account information. If successful, you can see a VPN virtual network card on the system status page. You can refer to the parameter hints and sample configuration.

Figure 6-2-1 VPN Interface



6.3 DDNS Settings

You can enable or disable DDNS (Dynamic Domain Name Server) according to your needs.

Figure 6-3-1 DDNS Interface

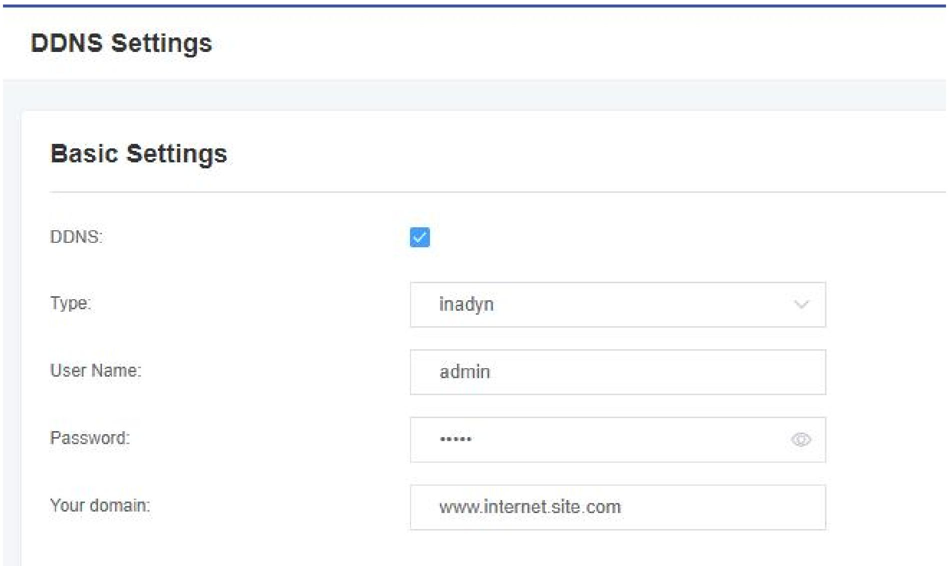


Table 6-3-1 Definition of DDNS Settings

Options	Definition
DDNS	Enable/Disable DDNS(dynamic domain name server)
Type	Set the type of DDNS server.
Username	Your DDNS account's login name.
Password	Your DDNS account's password.
Your domain	The domain to which your web server will belong.

6.4 Toolkit

This tool is used to detect the network connection, you can execute the Ping command on the web interface.

Figure 6-4-1 Network Connectivity Checking

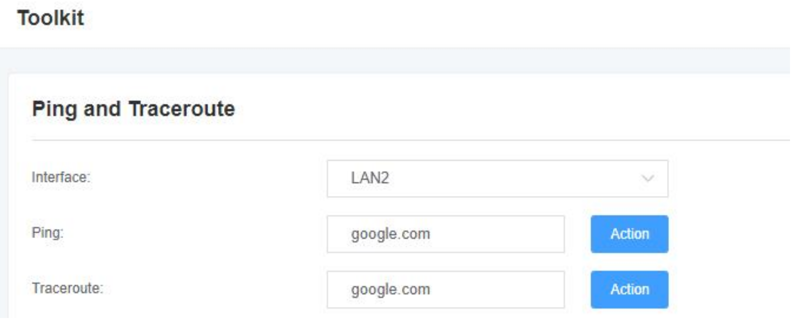


Figure 6-4-2 Channel Recording

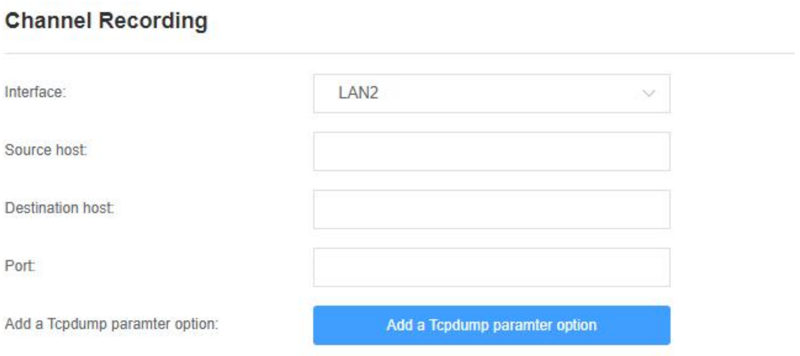


Figure 6-4-3 Capture Network Data

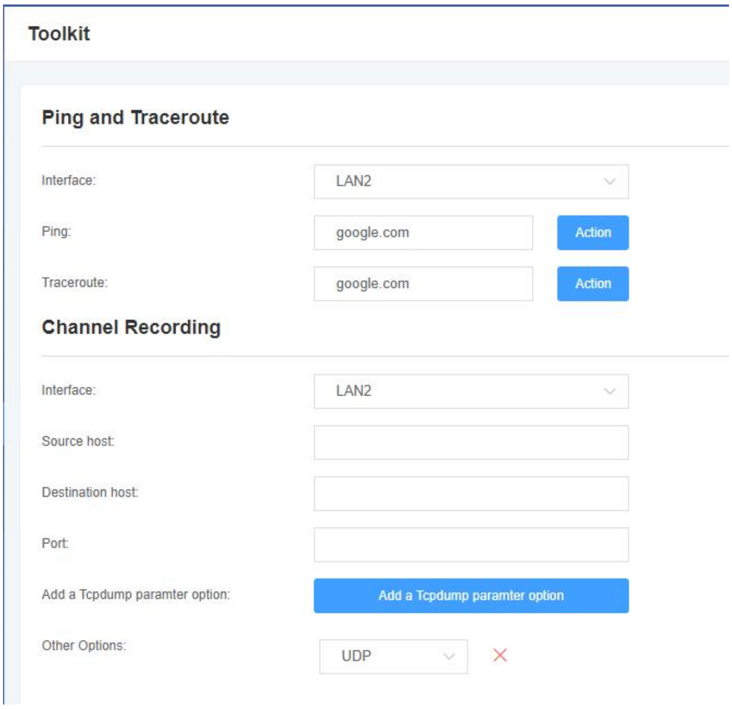
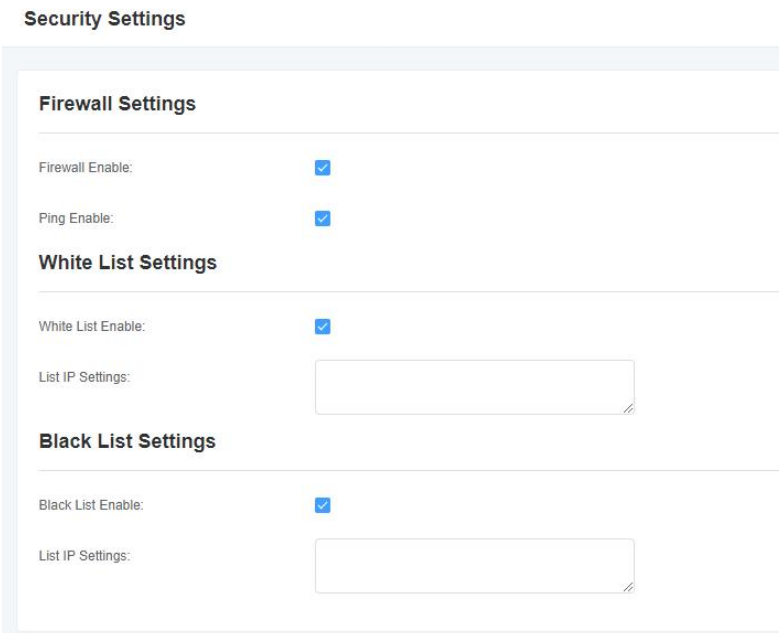


Table 6-4-1 Definition of Channel Recording

Options	**Definition**
Interface	The name of network interface.
Source host	Specify the source address of the data you want to get.
Destination host	Specify the destination address you want to get data from.
Port	Specify the port where you want to get data.
Channel	Specify the channel number you want to get data.
Tcpdump Option Parameter	The tool of tcpdump capture network data by parameter option specified.

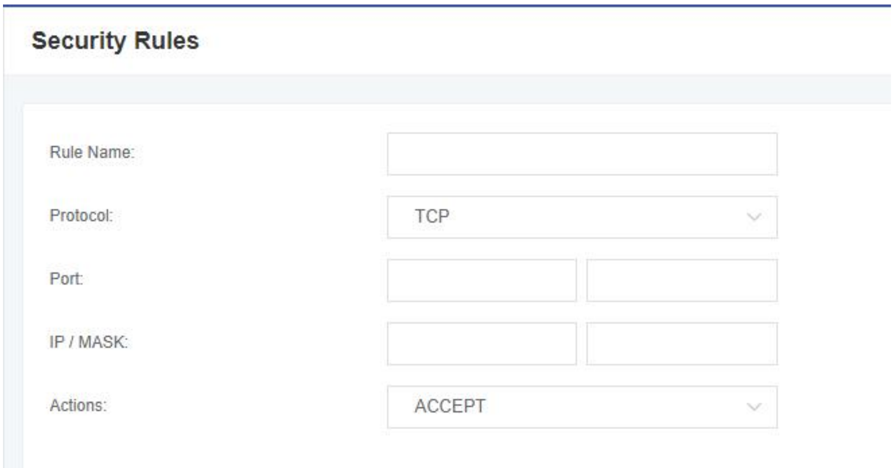
6.5 Security Settings

Figure 6-5-1 Security Settings Interface



6.6 Security Rules

Figure 6-6-1 Security Rules Interface



7. Advanced

7.1 Asterisk API

When you make “Enable” switch to “on”, this page is available.

Figure 7-1-1 API Interface

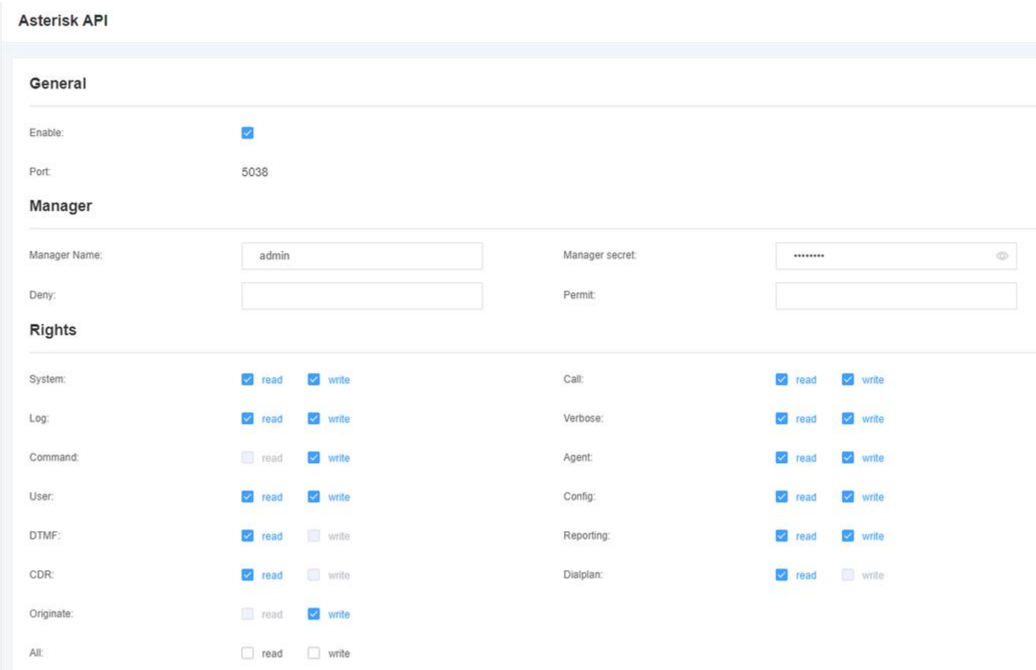


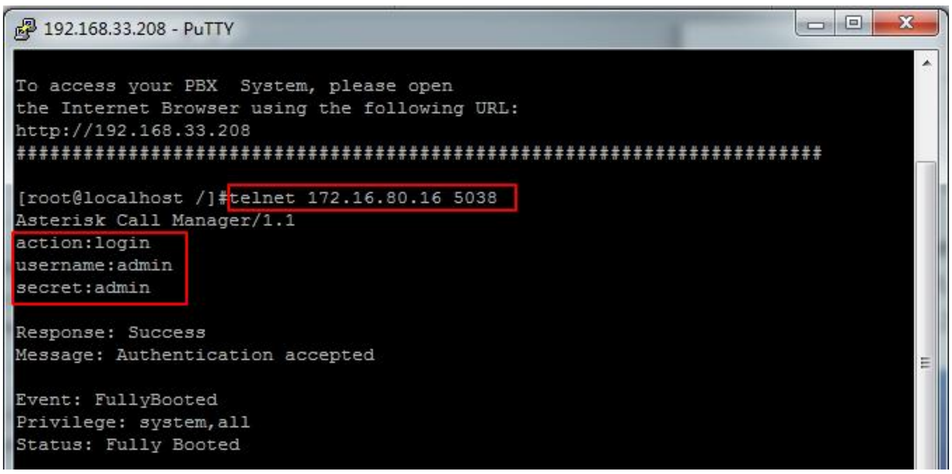
Table 7-1-1 Definition of Asterisk API

Options	**Definition**
Port	Network port number.
Manager Name	Name of the manager without space.
Manager secret	Password for the manager. Characters: Allowed characters “-_+.<>&0-9a-zA-Z”. Length:4-32 characters.
Deny	If you want to deny many hosts or networks, use char & as separator. Example: 0.0.0.0/0.0.0.0 or 192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0.
Permit	If you want to permit many hosts or network, use char & as separator.

	Example: 0.0.0.0/0.0.0.0 or 192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0
System	General information about the system and ability to run system management commands, such as Shutdown, Restart, and Reload.
Call	Information about channels and ability to set information in a running channel.
Log	Logging information. Read-only. (Defined but not yet used.)
Verbose	Verbose information. Read-only. (Defined but not yet used.)
Command	Permission to run CLI commands. Write-only.
Agent	Information about queues and agents and ability to add queue members to a queue.
User	Permission to send and receive UserEvent.
Config	Ability to read and write configuration files.
DTMF	Receive DTMF events. Read-only.
Reporting	Ability to get information about the system.
CDR	Output of cdr, manager, if loaded. Read-only.
Dialplan	Receive NewExten and Varset events. Read-only.
Originate	Permission to originate new calls. Write-only.
All	Select all or deselect all.

Refer to the above configuration diagram, the host 172.16.80.16/255.255.0.0 has been allowed to enter the gateway API, and the port number is 5038.

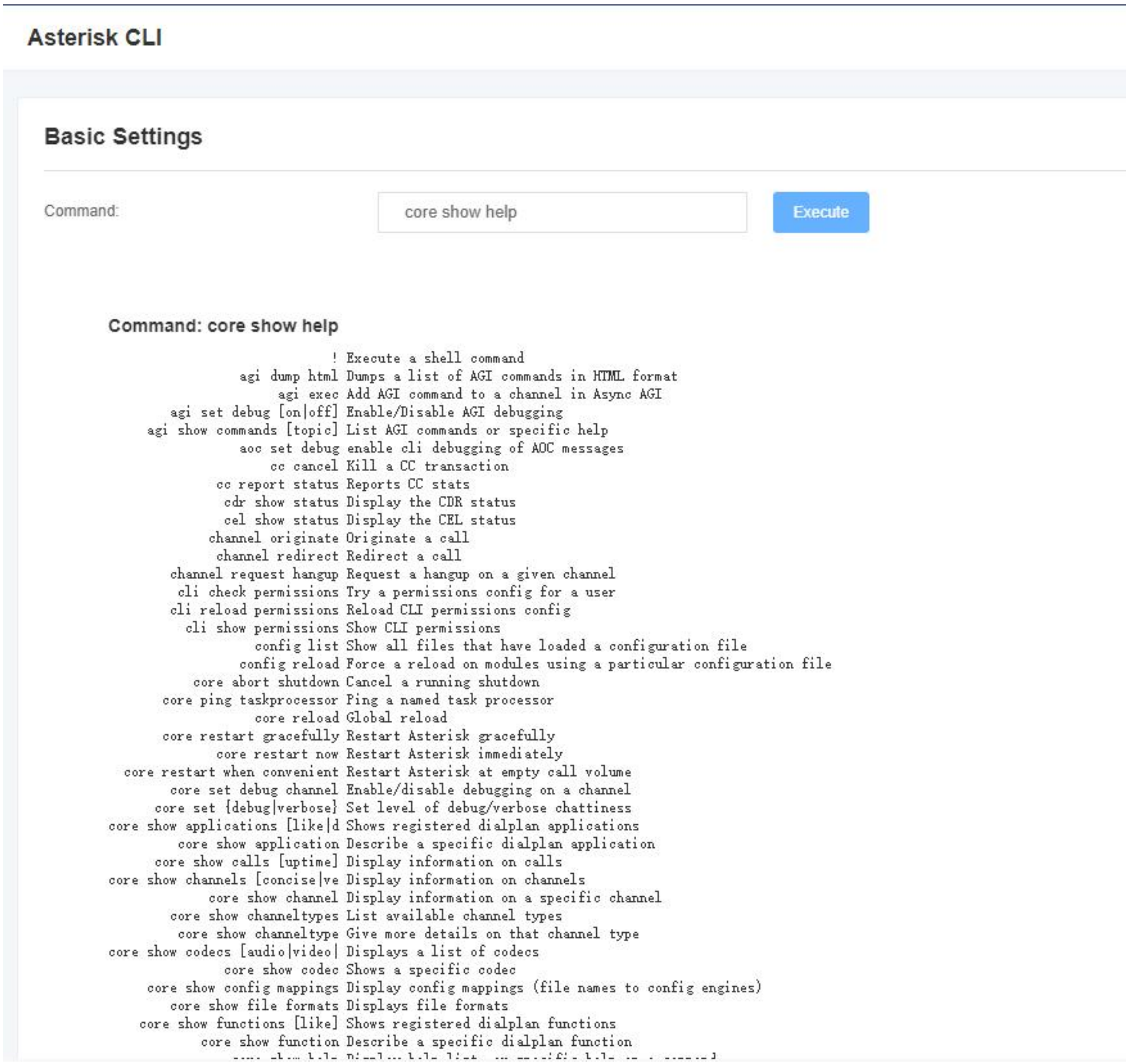
Figure 7-1-2 Putty Access



7.2 Asterisk CLI

In this page, you are allowed to run Asterisk commands.

Figure 7-2-1 Asterisk Command Interface



For example: enter "help" or "?" in the command bar, after execution, the page will prompt for executable commands, as shown in the figure above.

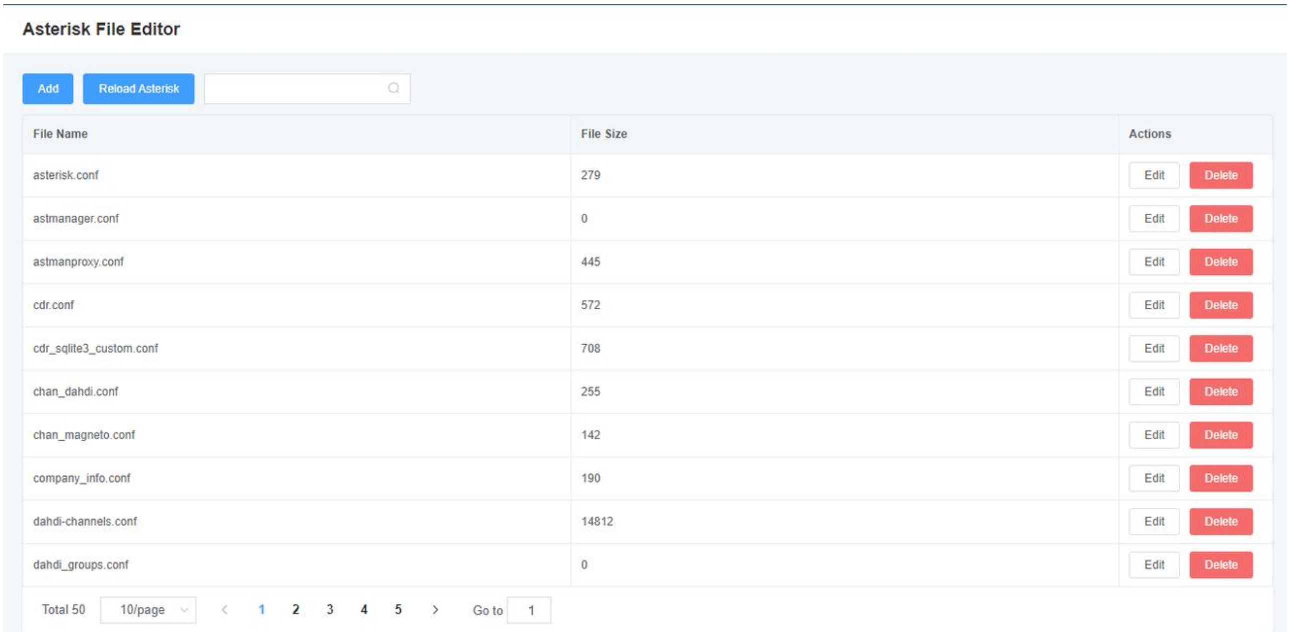
Table 7-2-1 Definition of Asterisk CLI

Options	Definition
Command	Type your Asterisk CLI commands here to check or debug your gateway.

7.3 Asterisk File Editor

On this page, you are allowed to edit and create configuration files.

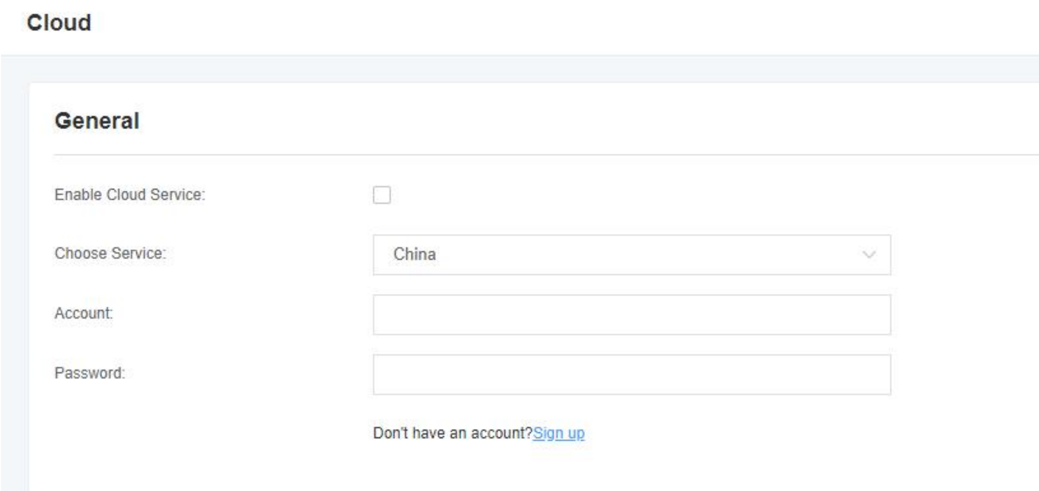
Figure 7-3-1 Configuration Files List



Notice: After modifying the configuration file, Asterisk needs to be reloaded.

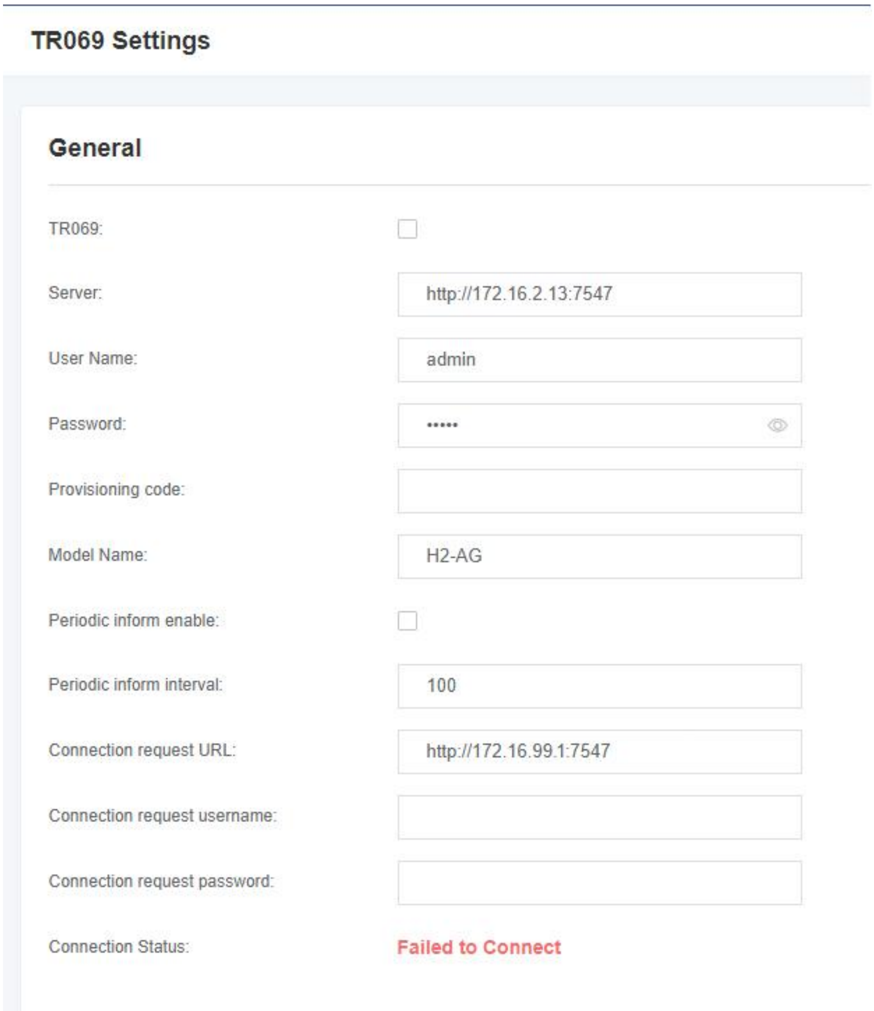
7.4 Cloud Management

Figure 7-4-1 Cloud Management Interface



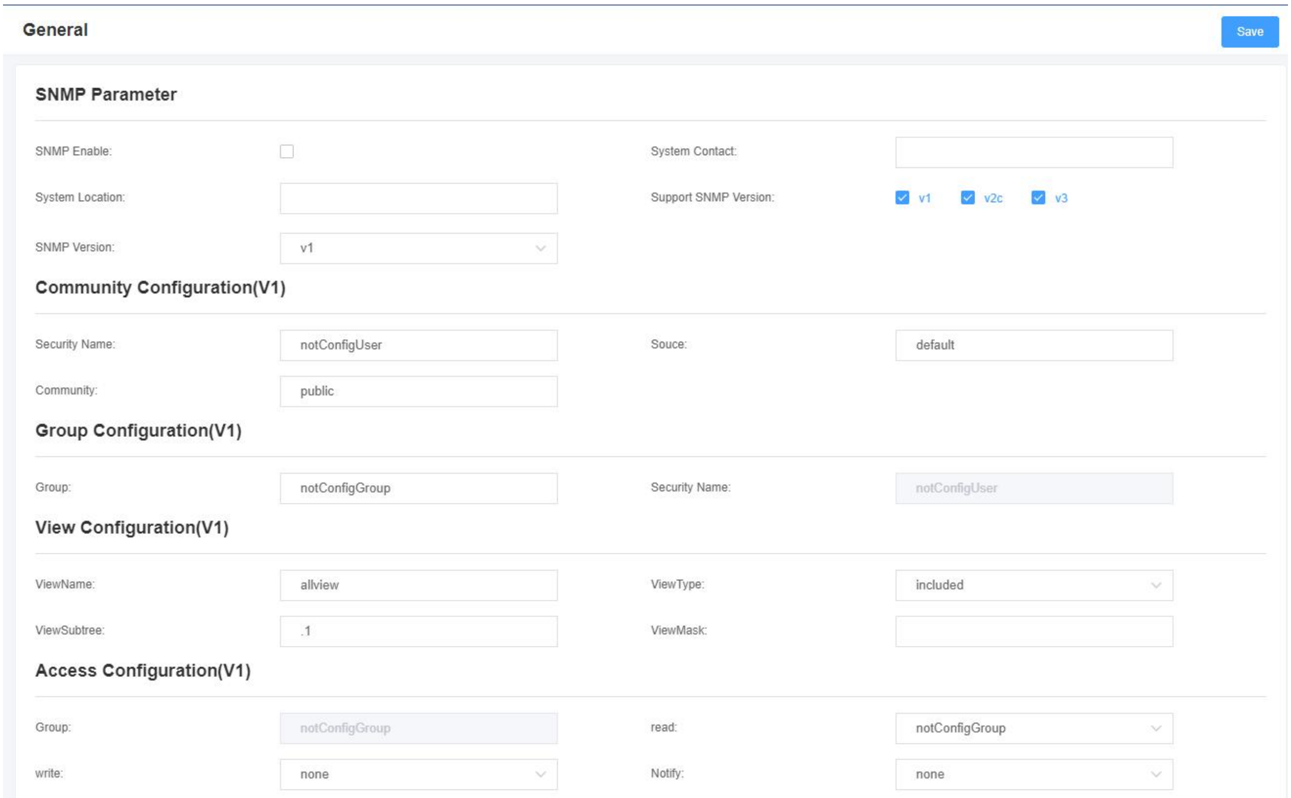
7.5 TR069

Figure 7-4-1 TR069 Interface



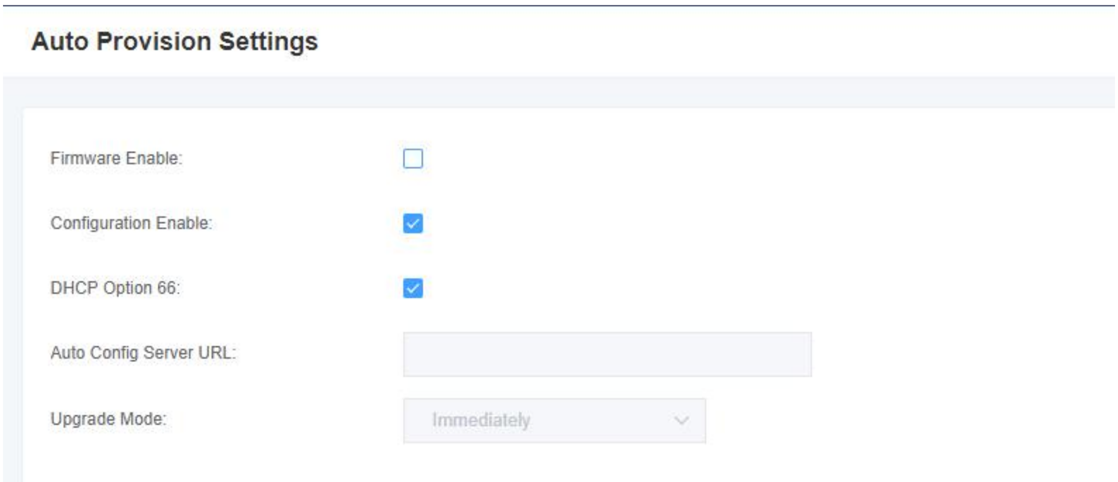
7.6 SNMP

Figure 7-4-1 SNMP Interface



7.7 Auto Provision

Figure 7-4-1 Auto Provision Interface



8. Logs

8.1 Log Settings

On the log setting interface, open the corresponding log option, and you can view different logs in the corresponding interface. Take the system log as an example.

Figure 8-1-1 Logs Settings

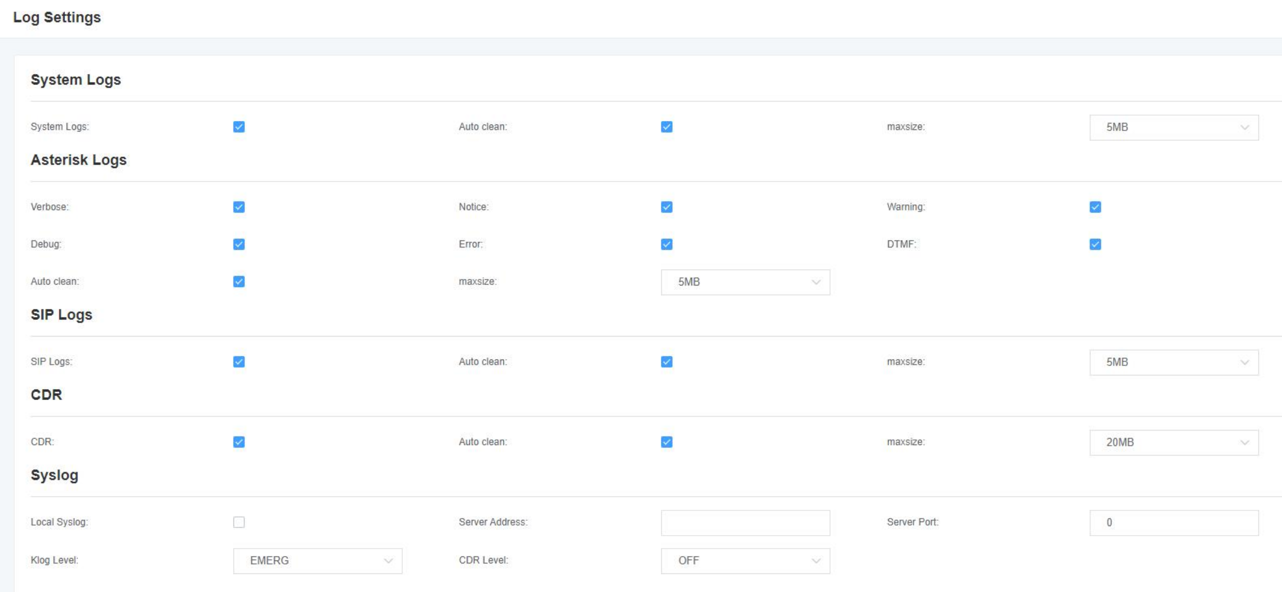


Figure 8-1-2 System Logs Output

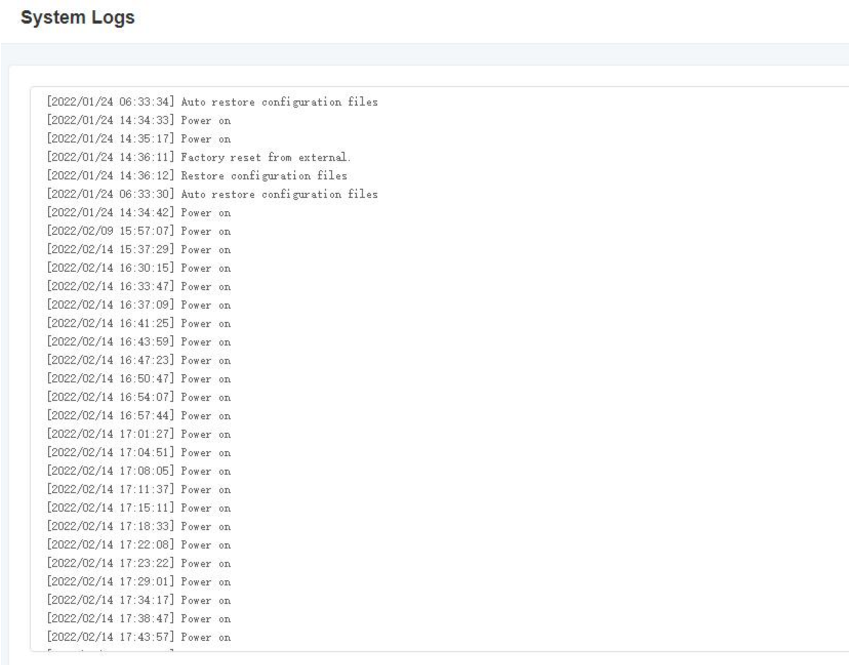


Figure 8-1-3 Asterisk Logs Output

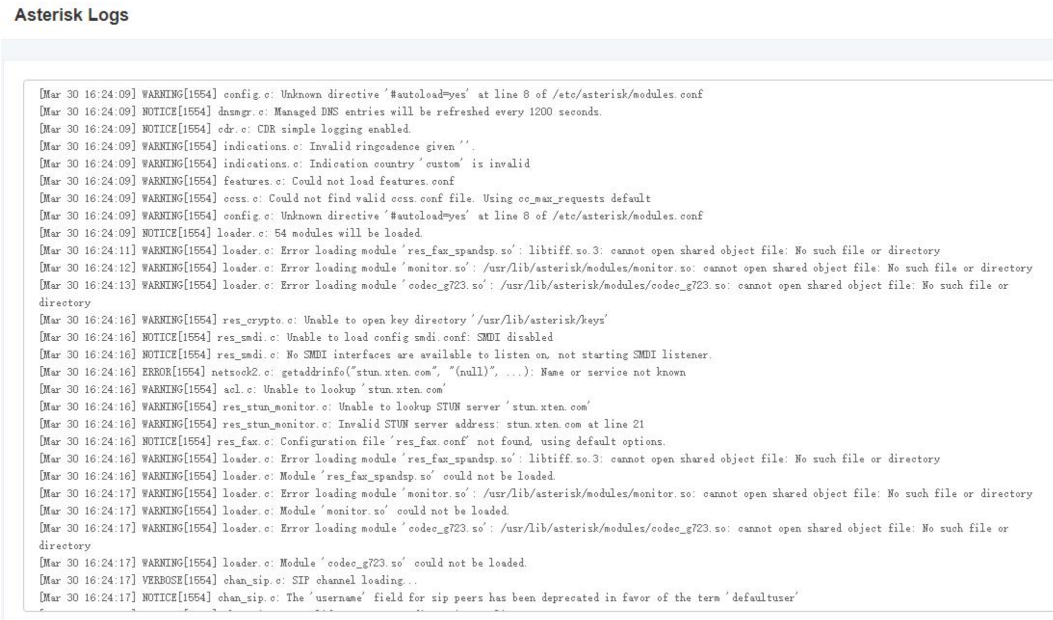


Figure 8-1-4 SIP Logs Output

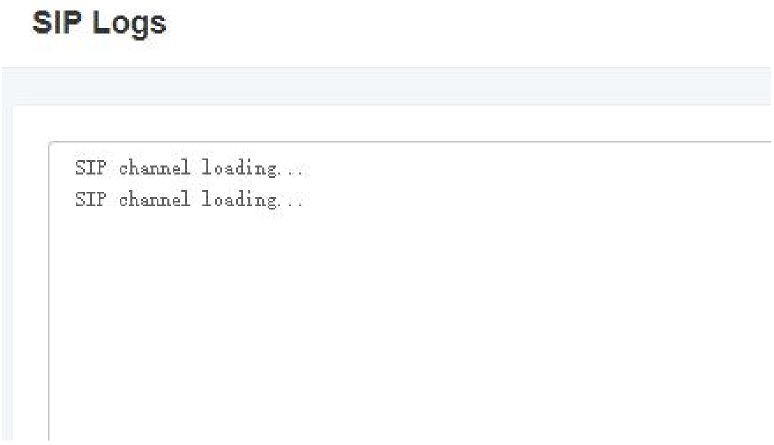


Table 8-1-1 Definition of LOG

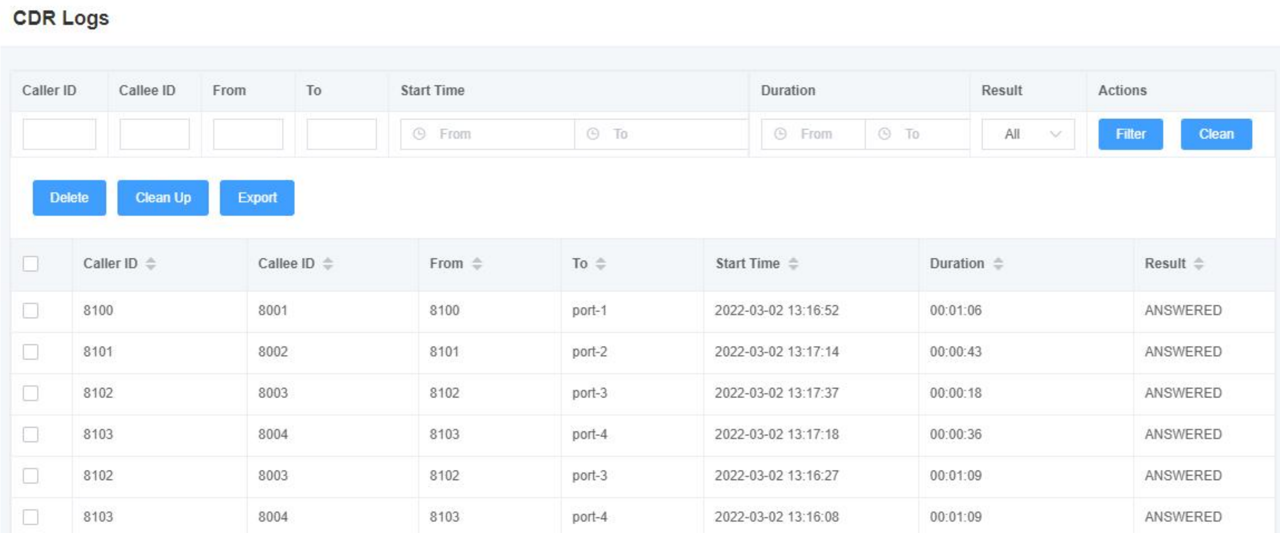
Options	**Definition**
System Logs	Whether to enable the system log.
Auto clean (System Logs)	Switch on: when the size of log file reaches the max size, the system will cut a half of the file. New logs will be retained. Switch off: logs will remain, and the file size will increase gradually. default on, max size=1MB.
Verbose	Asterisk console verbose message switch.
Notice	Asterisk console notice message switch.
Warning	Asterisk console warning message switch.

Debug	Asterisk console debug message switch.
Error	Asterisk console error message switch.
DTMF	Asterisk console DTMF info switch.
Auto clean: (asterisk logs)	Switch on: when the size of log file reaches the max size, the system will cut a half of the file. New logs will be retained. Switch off: logs will remain, and the file size will increase gradually. default on, max size=100KB.
SIP Logs:	Whether to enable the SIP log.
Auto clean: (SIP logs)	Switch on: when the size of log file reaches the max size,the system will cut a half of the file. New logs will be retained. Switch off: logs will remain, and the file size will increase gradually. default on, default size=100KB.
Call Detail Record	Displaying Call Detail Records for each channel.
Auto clean: (Call Detail Record)	Switch on: when the size of log file reaches the max size,the system will cut a half of the file. New logs will be retained. Switch off: logs will remain, and the file size will increase gradually. default on, default size=20MB.

8.2 CDR

You can browse the details of each call record on this page. If you need to search for a specific record, you can use the filter function.

Figure 8-3-1 Call Detail Record



Caller ID	Callee ID	From	To	Start Time	Duration	Result
8100	8001	8100	port-1	2022-03-02 13:16:52	00:01:06	ANSWERED
8101	8002	8101	port-2	2022-03-02 13:17:14	00:00:43	ANSWERED
8102	8003	8102	port-3	2022-03-02 13:17:37	00:00:18	ANSWERED
8103	8004	8103	port-4	2022-03-02 13:17:18	00:00:36	ANSWERED
8102	8003	8102	port-3	2022-03-02 13:16:27	00:01:09	ANSWERED
8103	8004	8103	port-4	2022-03-02 13:16:08	00:01:09	ANSWERED