OpenVox Communication Co Ltd

SWG-2016/32 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	10/5/2018	Full text

Contents

1. Overview

1.1 What is SWG-2016/32？

OpenVox SWG-2016/32 series wireless gateways include SWG-2016 G/C/L and SWG-2032 G/C/L, which can provides 16/32 GSM/CDMA/WCDMA/LTE channels. They can bring you excellent HD voice service with multiple codecs, including G.711U, G.711A, GSM, G.722, G.723, G.726, G.729, and also flexible SMS service with multiple SMS API. The SWG-2016/32 series gateways are perfect compatible with Asterisk, 3CX, FreePBX, FreeSWITCH SIP server and VOS VoIP system platform. It can provides users with more diverse telecommunications access methods and helps users reduce communication costs.

1.2 Product Introduction

The SWG-2016/32 series gateways are available in a variety of models, and each model supports a different number of ports and frequency bands. The following table shows:

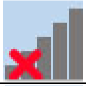
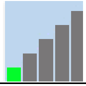
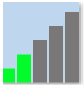
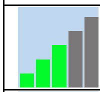
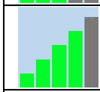
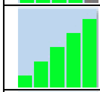
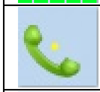
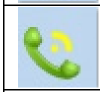
Model	Module	Ports	Network Interface	Band	USB	TF	Console
SWG-2016C	CDMA	16	2	CDMA 2000: 800MHz	1	1	1
SWG-2016G	GSM	16	2	GSM: 850/900/1800/1900MHz	1	1	1
SWG-2016L	LTE	16	2	China/India LTE FDD: B1/B3/B5/B8 LTE TDD: B38/B39/B40/B41 WCDMA: B1/B8 TD-SCDMA: B34/B39 CDMA: BC0 GSM: 900/1800MHz	1	1	1

				Europe/Middle East/Africa/ Korea/Thailand LTE FDD: B1/B3/B5/B7/B8/B20 LTE TDD: B38/B40/B41 WCDMA: B1/B5/B8 GSM: B3/B8			
SWG-2032C	CDMA	32	2	CDMA 2000: 800MHz	1	1	1
SWG-2032G	GSM	32	2	GSM: 850/900/1800/1900MHz	1	1	1
SWG-2032L	LTE	32	2	China/India LTE FDD: B1/B3/B5/B8 LTE TDD: B38/B39/B40/B41 WCDMA: B1/B8 TD-SCDMA: B34/B39 CDMA: BC0 GSM: 900/1800MHz	1	1	1
				Europe/Middle East/Africa/ Korea/Thailand LTE FDD: B1/B3/B5/B7/B8/B20 LTE TDD: B38/B40/B41 WCDMA: B1/B5/B8 GSM: B3/B8			

1.3 Application

1.3.1 LCD And Buttons

LED Indicator/Icon/Buttons	Color/ Icon	Staus
Display Icon		Module Initiating,Disable

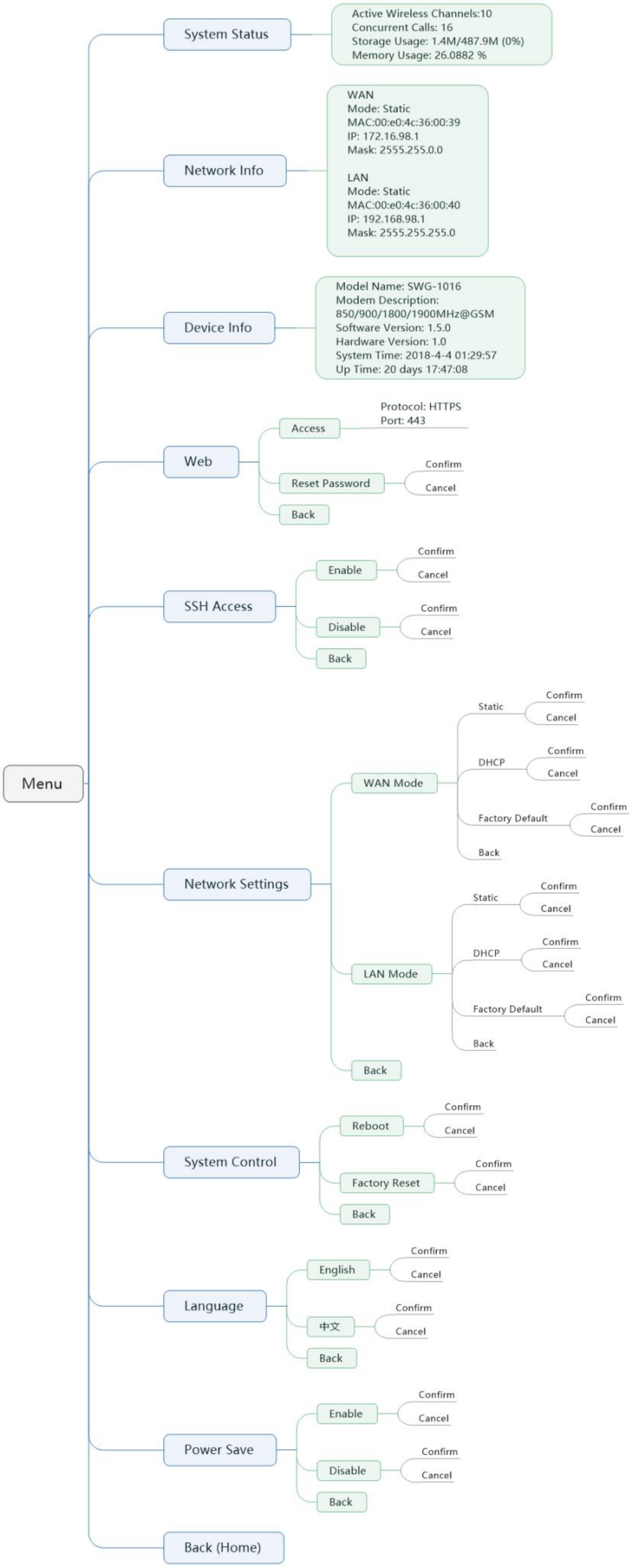
		No SIM Card
		Searching for Signal
		One grid Signal
		Two grid Signal
		Three grid Signal
		four grid Signal
		fives grid Signal
		Worst Signal Quality During a Call
		Medium Signal Quality During a Call
		Best Signal Quality During a Call
Network Status LED	Green and Flash	Network Connected
PWR	Always Green	Power on
POWER Button	OFF	Power down
	ON	Power on
RST Button	--	Press and hold the RST button for 3-5 seconds. The display jumps to the "System Booting" page to restart the system.

1.3.2 Multifunction button

1. [▲] : Press this key to flip up

2. OK :
   - Press this key in the signal interface - enter the menu
   - Press this key in the menu interface – Confrim
   - Press this key if it is Non-signal interface and there is no return option in the current interface - Back
3. [▼] : Press this key to flip down
4. Press any key in the signal interface to enter the menu interface.
5. If no button is operated within 20S, return to the main interface.

The main factions are as follows:



1.3.3 Console

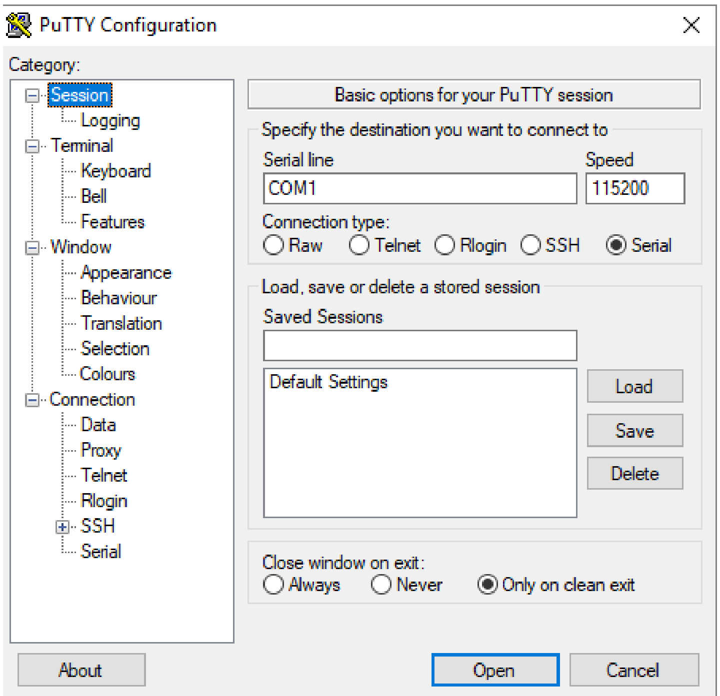
To ensure easy maintenance, SWG-2016/32 series gateway devices provide a serial port with a baud rate of 115200 bps. Users can connect to the computer through RJ45 to USB cable for maintenance related configuration.

Login device:

Step 1: Prepare the following serial cable (baud rate: 115200bps)

Step 2: Connect the USB port of the serial cable to the PC; connect the RJ45 port to the console port of the device.

Step 3: Configure the login software



After the above configuration, click "Open" to enter the device's background page. Use the same login name and password as SSH to enter the system.

1.4 Main Features

- Based on Asterisk®
- Wide selection of codecs and signaling protocol
- Support SMS sending, receiving, group sending
- Support transferring SMS to E-mail
- Support SMS remotely controlling gateway
- Support USSD service
- Support PIN identification
- Support unlimited routing rules and flexible routing settings
- SIM cards are all hot-swap
- Stable performance, flexible dialing, friendly GUI

1.5 Physical Information

- Size(No antenna and hanging ears): 440mm*44mm*300mm
- LCD dimension:2.4"
- LCD resolution ratio: 240*400
- LAN port:1
- WAN port:1
- USB Interface:1
- TF Infterface:1
- SIM Cards: hot-swap
- Operation Temperature: 0~40°C
- Storage Temperature: -20~70°C
- Operation humidity:10% ~ 90% non-condensing

1.6 Software

- Default IP:172.16.98.1
- Username:admin
- Passward:admin

For first time, you can access SWG-1016C using default IP 172.16.98.1. Then configure the module as you want.

2. System

2.1 Status

On the "Status" page, you will find all Modules, SIP, IAX2, Routing and Network information.

Figure 2-1 Systm Status

Module Information

Port	Signal	BER	Carrier	Registration Status	PDD(s)	ACD(s)	ASR(%)	Module Status	Remain Time
cdma-1.1		-1	CHINA TELECOM	Registered (Home network)	1	0	0	READY	No Limit
cdma-1.2(18002548416)		-1	CHINA TELECOM	Registered (Home network)	2	16	100	READY	No Limit
cdma-1.3		-1	CHINA TELECOM	Registered (Home network)	0	0	0	READY	No Limit
cdma-1.4		-1	CHINA TELECOM	Registered (Home network)	2	3	100	READY	No Limit
cdma-1.5		-1	CHINA TELECOM	Registered (Home network)	4	28	100	READY	No Limit
cdma-1.6		-1	CHINA TELECOM	Registered (Home network)	2	4	100	READY	No Limit
cdma-1.7		-1	CHINA TELECOM	Registered (Home network)	0	0	0	READY	No Limit
cdma-1.8		-1	CHINA TELECOM	Registered (Home network)	0	0	0	READY	No Limit
cdma-1.9		-1		Undetected SIM Card	0	0	0		No Limit
cdma-1.10		-1	CHINA TELECOM	Registered (Home network)	0	0	0	READY	No Limit
cdma-1.11		-1	CHINA TELECOM	Registered (Home network)	0	0	0	READY	No Limit
cdma-1.12		-1		Undetected SIM Card	0	0	0		No Limit
cdma-1.13		-1		Undetected SIM Card	0	0	0		No Limit
cdma-1.14		-1	CHINA TELECOM	Registered (Home network)	0	0	0	READY	No Limit
cdma-1.15		-1	CHINA TELECOM	Registered (Home network)	0	0	0	READY	No Limit
cdma-1.16		-1	CHINA TELECOM	Registered (Home network)	2	10	100	READY	No Limit

SIP Information

Endpoint Name	User Name	Host	Registration	SIP Status
1234	1234	172.16.80.216	server	OK (12 ms)
8888	8888	172.16.33.102	none	Unmonitored
9999	9999	172.16.33.102	client	No Authentication

IAX2 Information

Endpoint Name	User Name	Host	Registration	IAX2 Status
1002	1002	172.16.80.216	server	OK (38 ms)
1003	1003	172.16.33.102	none	OK (104 ms)
1004	1004	172.16.33.102	client	OK (103 ms)

Routing Information

Rule Name	From	To	Rules
OUT	sip-1234	grp-ALL	
IN	grp-ALL	custom-playback	

Network Information

Name	MAC Address	IP Address	Mask	Gateway	RX Packets	TX Packets
LAN	00:E0:4C:36:00:35	172.16.6.130	255.255.0.0	172.16.0.1	602327	157145

Table 2-1 Description of System Status

Options	**Definition**
Port	Number of each ports.
Signal	Display the signal strength of in each channels of gateway.
BER	Bit Error Rate.
Carrier	Display the network carrier of current SIM card.
Registration Status	Indicates the registration status of current module.
PDD	Post Dial Delay (PDD) is experienced by the originating customer as the time from the sending of the final dialed digit to the point at which they hear ring tone or other in-band information.Where the originating network is required to play an announcement before completing the call then this definition of PDD excludes the duration of such announcements.
ACD	The Average Call Duration (ACD) is calculated by taking the sum of billable seconds (bill sec) of answered calls and dividing it by the number of these answered calls.
ASR	Answer Seizure Ratio is a measure of network quality. Its calculated by taking the number of successfully answered calls and dividing by the total number of calls attempted. Since busy signals and other rejections by the called number count as call failures, the ASR value can vary depending on user

	behavior. ModuleStatus Show the status of port, include blank space and “READY”. Black space means it is unavailable here and “Ready” means the port is available
Module Status	Display the status of the port. "Ready" means registering and "READY" means port is available
Remain Time	This value is multiplied by to step length is a rest call time.

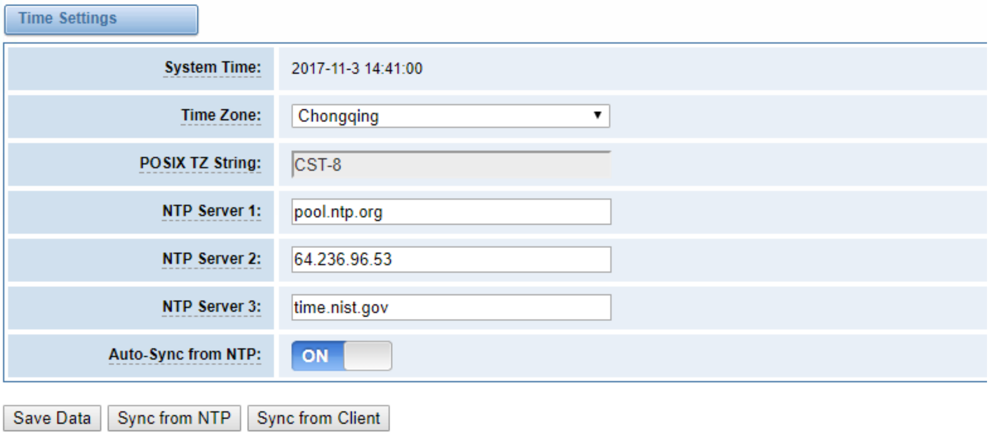
2.2 Time

Table 2-2 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].
Save Data	Save the Modify of the time settings
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 Time Settings



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

2.3 Login Settings

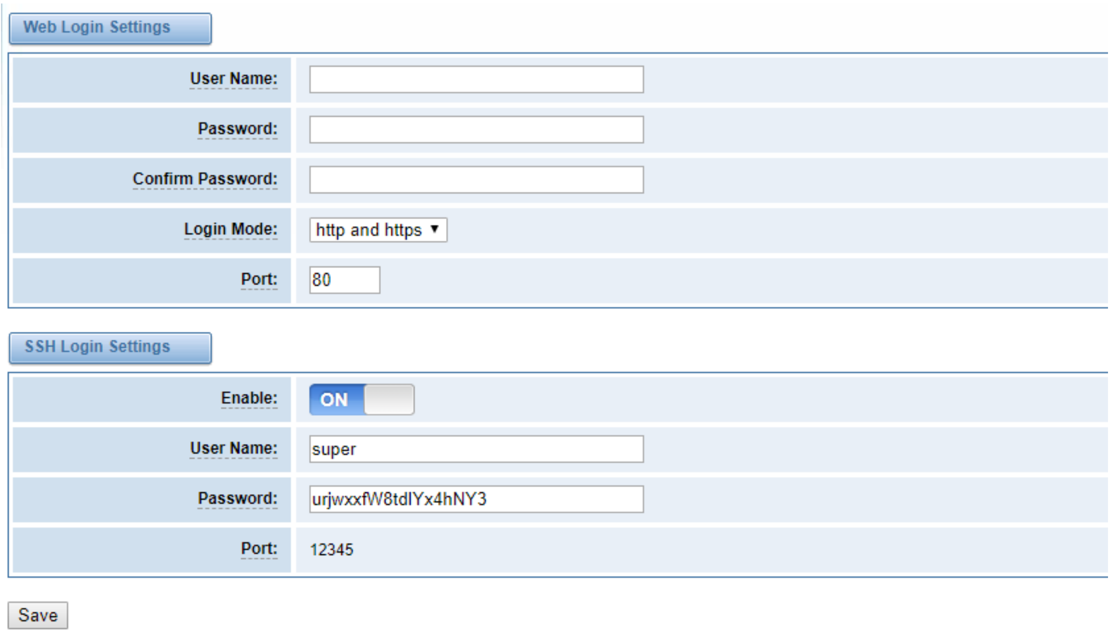
You can modify “Web Login Settings” and “SSH Login Settings”. If you have changed these settings, you don’t need to log out, just rewriting your new user name and password will be OK. Also you can specify the web server port number. Normally, the default web login mode is "http and https." For security, you can switch to “only https”.

Table 2-3 Description of Login Settings

Options	Definition
User Name	Define your username and password to manage your gateway 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	http and https: You can access gateway via link: http://gatewayIP or https://gatewayIP https: You can only access gateway via link: https://gatewayIP
Port	Specify the web server port number.

For example, you can configure like this:

Figure 2-3 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”.

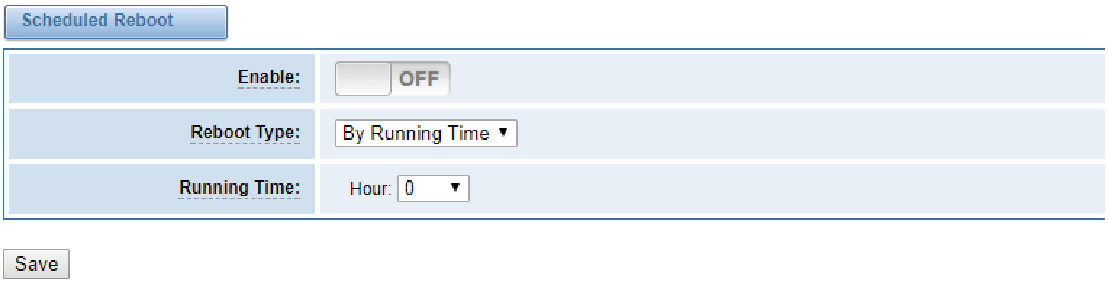
For example:

Figure 2-4 Language Settings

2.4.2 Scheduled Reboot

If switch it on, you can manage your gateway to reboot automatically as you like. There are four reboot types for you to choose, “By Day, By Week, By Month and By Running Time”.

Figure 2-5 Reboot Type



If use your system frequently, you can set this enable, it can helps system work more efficient.

2.5 Tools and Information

2.5.1 Reboot Tools

You can choose system reboot and asterisk reboot separately.

Figure 2-6 Reboot Tools

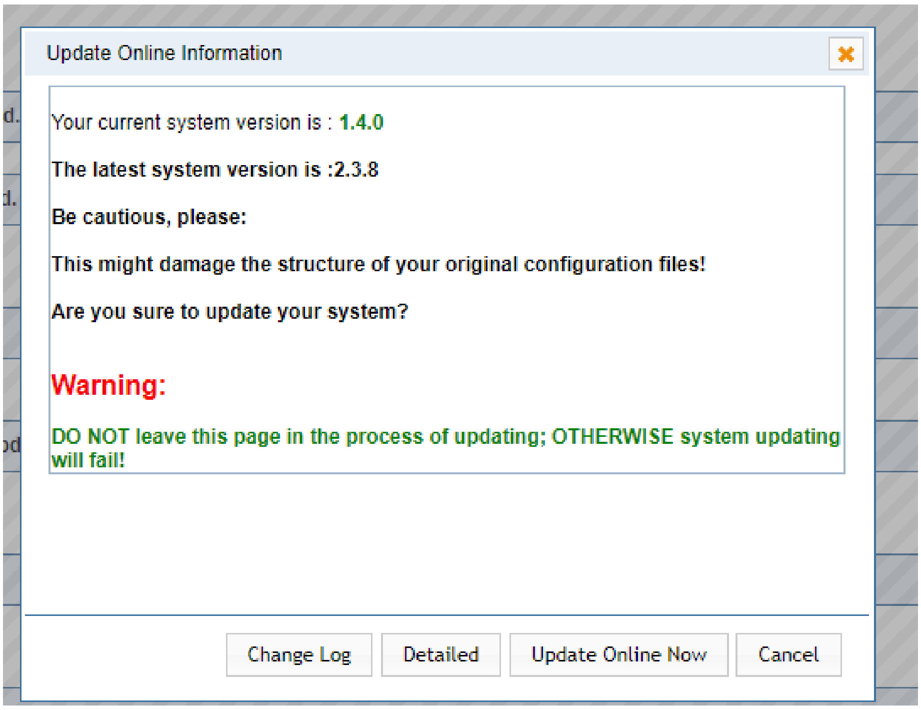
If you press "OK", your system will reboot and all current calls will be dropped. Asterisk Reboot is the same.

2.5.2 Update Firmware

We offer 2 kinds of update types for you, you can choose System Update or System Online Update.

If you choose System Online Update,you will see the following information:

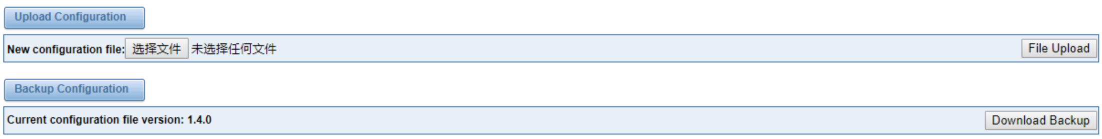
figure 2-7 Update Firmware



2.5.3 Upload and Backup Configuration

If you want to update your system and remain your previous configuration, you can first backup configuration, then you can upload configuration directly. That will be very convenient for you.

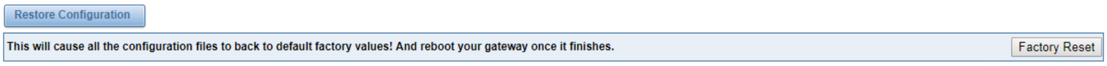
Figure 2-8 Upload and Backup Configuration



2.5.4 Restore Configuration

Sometimes there is something wrong with your gateway that you don't know how to solve it, mostly you will select factory reset. Then you just need to press a button, your gateway will be reset to the factory status.

Figure 2-9 Restore Configuration



2.6 Information

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

Figure 2-10 Information

Model Name:	SWG-1016
Modem Description:	800MHz@CDMA 2000
Software Version:	1.4.0
Hardware Version:	1.0
Slot Number:	1
Storage Usage:	516.0K/487.9M (0%)
Memory Usage:	25.884 % Memory Clean
Build Time:	2017-11-07 10:53:01
Contact Address:	10/F, Building 6-A, Baoneng Science and Technology Industrial Park, Longhua New District, Shenzhen, Guangdong,China
Tel:	+86-755-82535461
Fax:	+86-755-83823074
E-Mail:	support@openvox.cn
Web Site:	http://www.openvox.cn
Rebooting Counts:	51
System Time:	2017-11-7 13:56:25
System Uptime:	0 days 01:29:04

3. MODULE

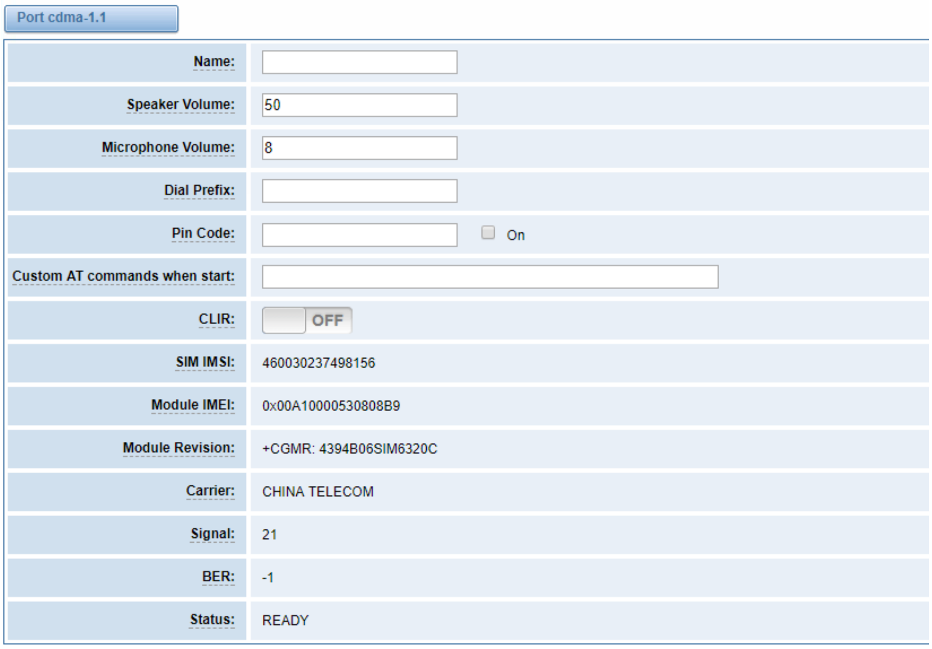
3.1 MODULE Settings

Figure 3-1 Module Settings

Port	Carrier	Registration Status	Module Status	Actions
cdma-1.1	CHINA TELECOM	Registered (Home network)	READY	
cdma-1.2(18002548416)	CHINA TELECOM	Registered (Home network)	READY	
cdma-1.3	CHINA TELECOM	Registered (Home network)	READY	
cdma-1.4	CHINA TELECOM	Registered (Home network)	READY	
cdma-1.5	CHINA TELECOM	Registered (Home network)	READY	
cdma-1.6	CHINA TELECOM	Registered (Home network)	READY	
cdma-1.7	CHINA TELECOM	Registered (Home network)	READY	
cdma-1.8	CHINA TELECOM	Registered (Home network)	READY	
cdma-1.9		Undetected SIM Card		
cdma-1.10	CHINA TELECOM	Registered (Home network)	READY	
cdma-1.11	CHINA TELECOM	Registered (Home network)	READY	
cdma-1.12		Undetected SIM Card		
cdma-1.13		Undetected SIM Card		
cdma-1.14	CHINA TELECOM	Registered (Home network)	READY	
cdma-1.15	CHINA TELECOM	Registered (Home network)	READY	
cdma-1.16	CHINA TELECOM	Registered (Home network)	READY	

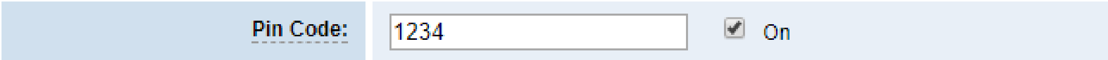
On this page, you can see your SIM Card information and module status,click action button to configure the port.

Figure 3-2 Port Configuration



If you have set your **Pin Code**, you can check on like this:

Figure 3-3 PIN Code Application



If you want to hide your number when you call out, you can just switch **CLIR** “ON” (Of course you need your operator’s support)

Figure 3-4 CLIR Application

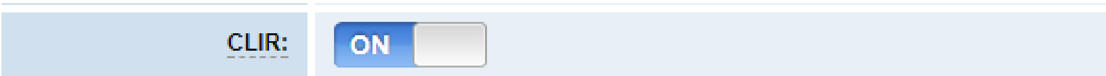


Table 3-1 Definition of Module Settings

Options	Definition
Name	The alias of the each port. Input name without space here. Allowed characters "-_+.<>&0-9a-zA-Z".Length: 1-32 characters.
Speaker Volume	The speaker volume level, the range is 0-100. This will adjust the loud speaker volume level by an AT command.
Microphone Volume	The microphone volume, range is: 0-15. This will change the microphone gain level by an AT command.
Dial Prefix	The prefix number of outgoing calls from this channel
PIN Code	Personal identification numbers of SIM card. PIN code can be modified to prevent SIM card from being stolen.
Custom AT commads when start	User custom AT commands when start system, use “|” to split AT command.
CLIR	Caller ID restriction, this function is used to hidden caller ID of SIM card number. The gateway will add ‘#31#’ in front of mobile number. This function must support by Operator.

SMS Center Number	Your SMS center number of your local carrier.
Module IMEI	Only CDMA module does not support modifying IMEI

3.1.1 Call Duration Limit Settings

Now we can offer you two types of call duration limit, you can choose “Single Call Duration Limit” or “Call Duration Limitation” to control your calling time

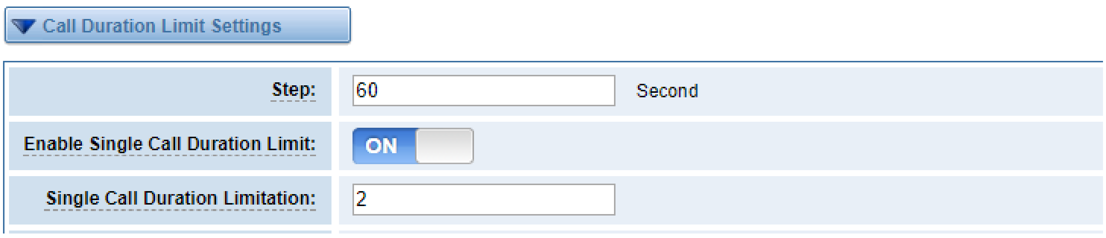
Single Call Duration Limit: This will limit the time of each call.

First you need to switch “Enable” on, then you can set “Step” and “Single Call Duration Limitation” any digits you want. When you make a call by this port, it will limit your calling time within the product of

Step * Single Call Duration Limitation

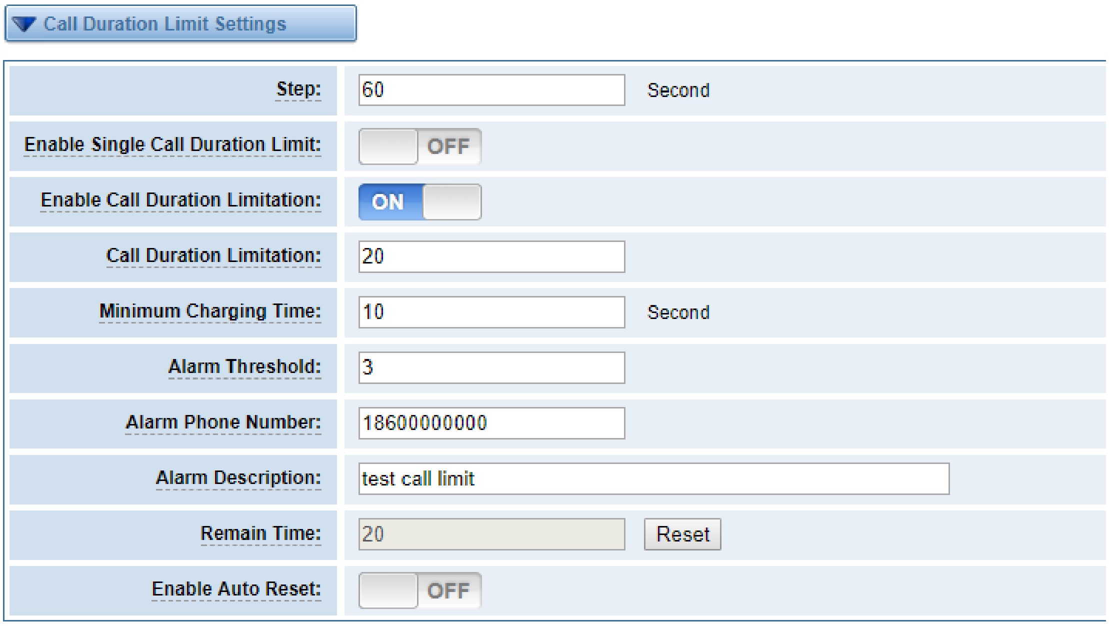
And if your calling time overtops the value above, the system will hang up this call.

Figure 3-5 Single Settings



Call Duration Limitation: This will limit your total calling time of this port. If remain time is 0, it will not send calls through this port.

Figure 3-6 Call Duration Limitation Settings



The same algorithm with single time limitation, the total calling time of this port can't beyond the product of "Step" and "Call Duration Limitation".

If the duration of a call is less than "Minimum Charging Time", it will be not included in "Call Duration".

You can set a digit for "Alarm Threshold", when the call minutes less than this value, the gateway will send alarm info to designated phone.

You can enable your Auto Reset, then choose by day, by week, or by month.

Figure 3-7 Auto Reset Settings

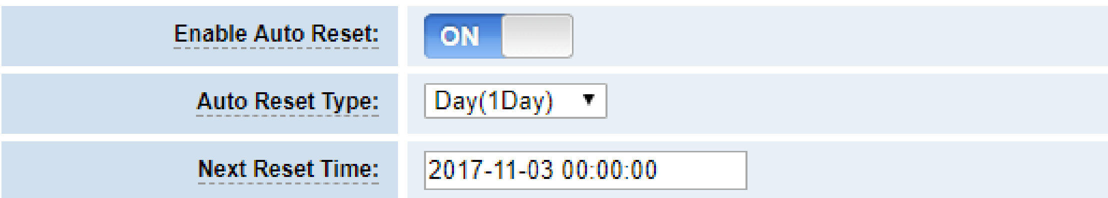


Table 3-2 Description of Call Duration Limit Settings

Options	Definition

Step	Step length value range is 1-999s, step length multiplied by time of single call just said a single call duration time allowed.
Enable Single Call Duration Limit	Definite maximum call duration for single call. Example: if Time of single call set to 10, the call will be disconnected after talking 10*step seconds.
Enable Call Duration Limitation	This function is to limit the total call duration of channel. The max call duration is between 1 to 999999 minutes.
Minimum Charging Time	A single call over this time, Module side of the operators began to collect fees, unit for seconds.
Alarm Threshold	Define a threshold value of call minutes, while the call minutes less than this value, the gateway will send alarm information to designated phone.
Alarm Description	Alarm port information description, which will be sent to user mobile phone with alarm information.
Alarm Phone Number	Receiving alarm phone number, user will received alarm message from gateway.
Enable Auto Reset	Automatic restore remaining talk time, that is, get total call minutes of each channel.
Auto Reset Type	Reset call minutes by date, by week, by month.
Next Reset Time	Defined next reset date, system will count start from that date and work as Reset Period setting

You can save your configuration to other ports.

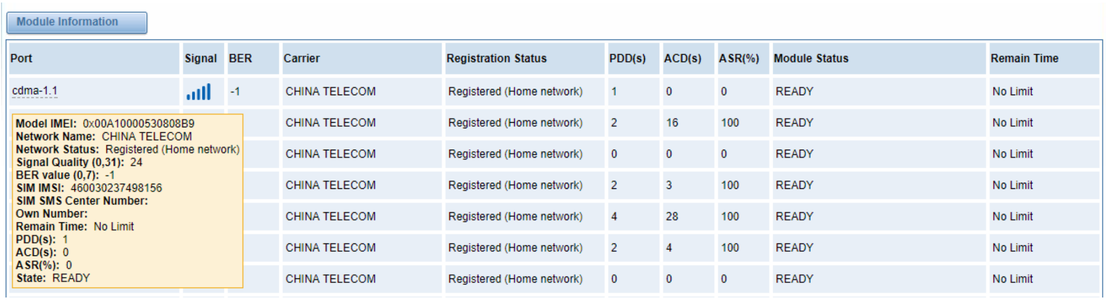
Figure 3-8 Save to Other Ports

If you have set like this, you will see many  on the Web GUI, you can set whether to check.

Notice: When you do some changes, you need to Save and Apply, then "Remain Time" will show as you set.

Your calling status will show on the main interface.

Figure 3-9 Module Information



Module Information

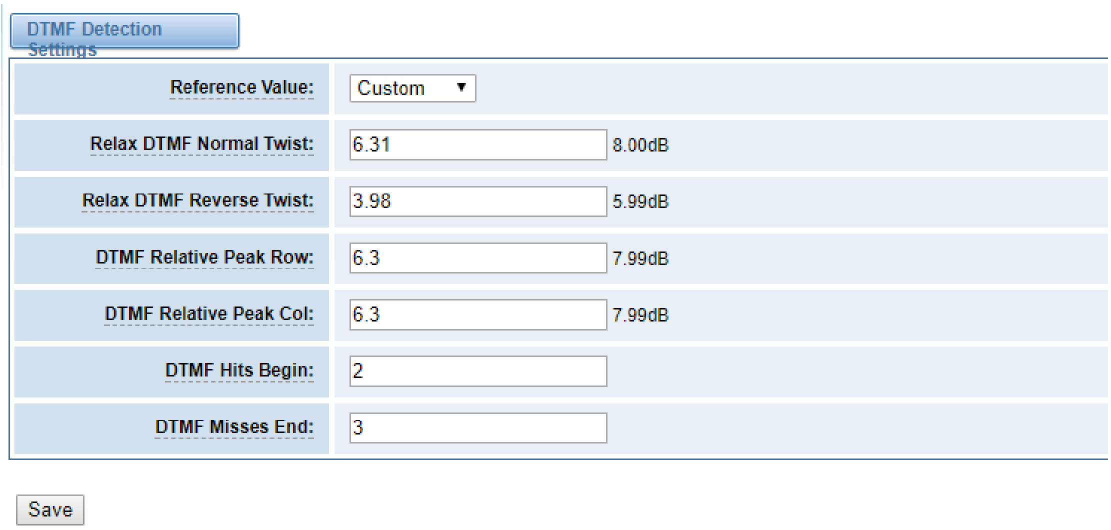
Port	Signal	BER	Carrier	Registration Status	PDD(s)	ACD(s)	ASR(%)	Module Status	Remain Time
cdma-1.1		-1	CHINA TELECOM	Registered (Home network)	1	0	0	READY	No Limit
			CHINA TELECOM	Registered (Home network)	2	16	100	READY	No Limit
			CHINA TELECOM	Registered (Home network)	0	0	0	READY	No Limit
			CHINA TELECOM	Registered (Home network)	2	3	100	READY	No Limit
			CHINA TELECOM	Registered (Home network)	4	28	100	READY	No Limit
			CHINA TELECOM	Registered (Home network)	2	4	100	READY	No Limit
			CHINA TELECOM	Registered (Home network)	0	0	0	READY	No Limit

Model IMEI: 0x00A10000530808B9
Network Name: CHINA TELECOM
Network Status: Registered (Home network)
Signal Quality (0,31): 24
BER value (0,7): -1
SIM IMSI: 460030237498156
SIM SMS Center Number:
Own Number:
Remain Time: No Limit
PDD(s): 1
ACD(s): 0
ASR(%): 0
State: READY

3.2 DTMF

You can do some DTMF Detection Settings if you choose "MODULE –> DTMF".

Figure 3-10 DTMF Detection Settings



Notice: If you don't have special need, you don't have to modify these settings. You can just choose "Default".

Table 3-3 Description of DTMF Detection Settings

Options	**Definition**
DTMF Normal Twist and Reverse Twist	It is the difference in power between the row and column energies. Normal Twist is where the Column energy is greater than the Row energy. Reverse Twist is where the Row energy

	is greater.
DTMF Relative Peak Row	The value is the smaller and the detection is easier. If you lost some numbers, you can try to put the value down. The adjustment range is 0.02 at a time.
DTMF Relative Peak Col	The value is smaller and the detection is easier. If you lost some numbers, you can try to put the value down. The adjustment range is 0.1 at a time.
DTMF Hits Begin	Sampling matching value. You can choose 2 or 3.
DTMF Misses End	The time interval between the two digits you input. Adjust the speed of input. The smaller value represents the shorter intervals.

3.3 Toolkit

You can get USSD information, send AT command and check number with this module. When you have a debug of the module, AT command is useful.

Figure 3-11 Function Options

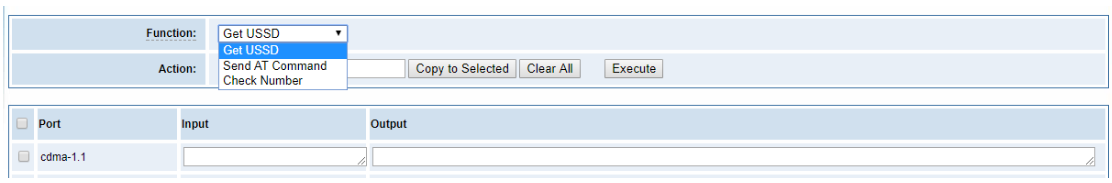


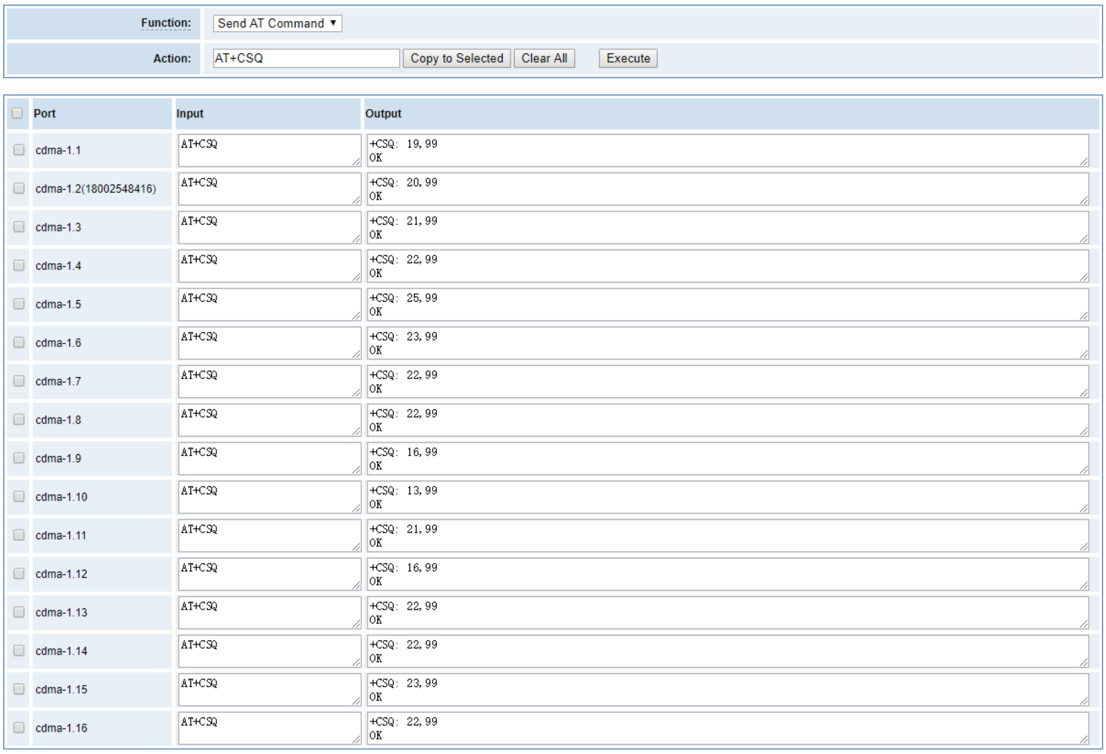
Table 3-4 Description of Definition of Functions

Options	Definition
Check Number	Enter a known number (like your mobile phone) to check what number it is of the SIM card. Click "Execute", then the gateway will dial to the number you already input. It only rings for one time and hangs up at once. Not generating telephone charge during this procedure.

Get USSD	Enter a specific USSD number (For example,*142# to check your SIM card's balance. This USSD number is might be different from different carriers) to get the USSD information. The gateway will try to get by AT commands.
AT Command	To perform some specific AT commands. This is useful when you have a debug of the modem. e.g. perform [AT+CSQ] to check what signal qualify it is. In AT commands, there is no difference between “a” and “A”

If you want to send AT command, first you should input your command, then select certain ports and choose “**Copy to Selected**”, finally choose “**Execute**”.

Figure 3-12 AT Command Example



Function: Send AT Command

Action: AT+CSQ Copy to Selected Clear All Execute

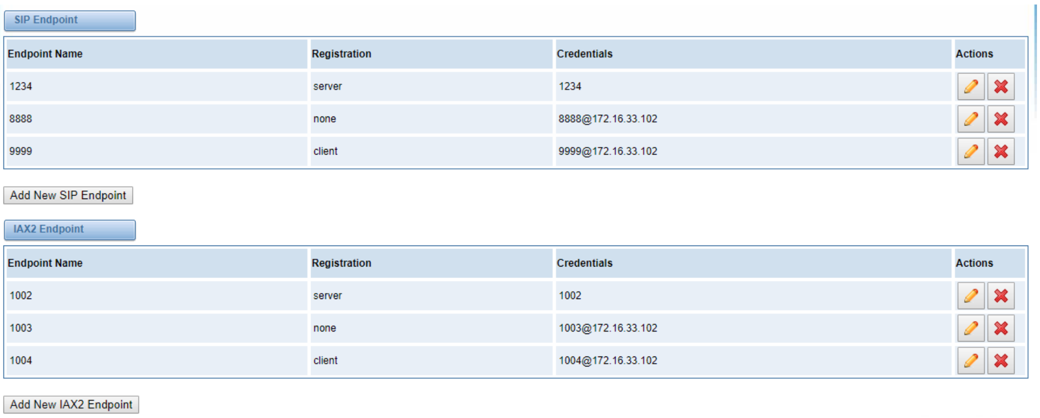
Port	Input	Output
cdma-1.1	AT+CSQ	+CSQ: 19, 99 OK
cdma-1.2(18002548416)	AT+CSQ	+CSQ: 20, 99 OK
cdma-1.3	AT+CSQ	+CSQ: 21, 99 OK
cdma-1.4	AT+CSQ	+CSQ: 22, 99 OK
cdma-1.5	AT+CSQ	+CSQ: 25, 99 OK
cdma-1.6	AT+CSQ	+CSQ: 23, 99 OK
cdma-1.7	AT+CSQ	+CSQ: 22, 99 OK
cdma-1.8	AT+CSQ	+CSQ: 22, 99 OK
cdma-1.9	AT+CSQ	+CSQ: 16, 99 OK
cdma-1.10	AT+CSQ	+CSQ: 13, 99 OK
cdma-1.11	AT+CSQ	+CSQ: 21, 99 OK
cdma-1.12	AT+CSQ	+CSQ: 16, 99 OK
cdma-1.13	AT+CSQ	+CSQ: 22, 99 OK
cdma-1.14	AT+CSQ	+CSQ: 22, 99 OK
cdma-1.15	AT+CSQ	+CSQ: 23, 99 OK
cdma-1.16	AT+CSQ	+CSQ: 22, 99 OK

4. VOIP

4.1 VOIP Endpoints

This page shows everything about your SIP&IAX2, you can see status of each SIP&IAX2.

Figure 4-1 SIP&IAX2 Endpoints



4.1.1 Add New SIP Endpoint

Main SIP Endpoint Settings:

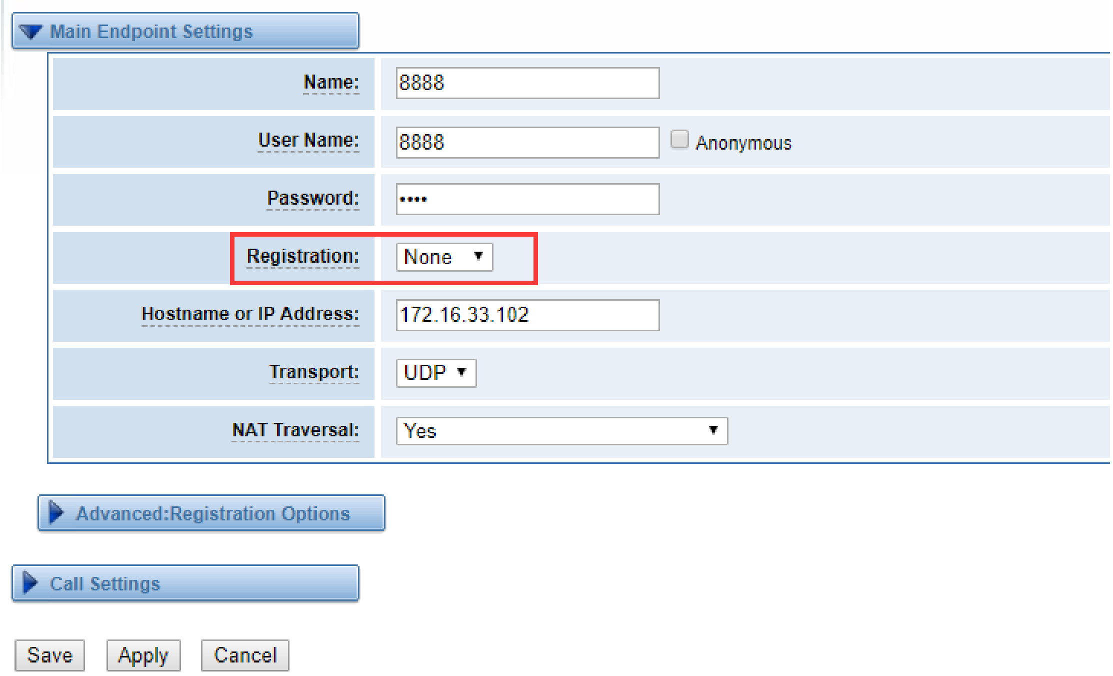
You can click Add New SIP Endpoint button to add a new SIP endpoint, and if you want to modify existed endpoints, you can click  button.

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

You can configure as follows:

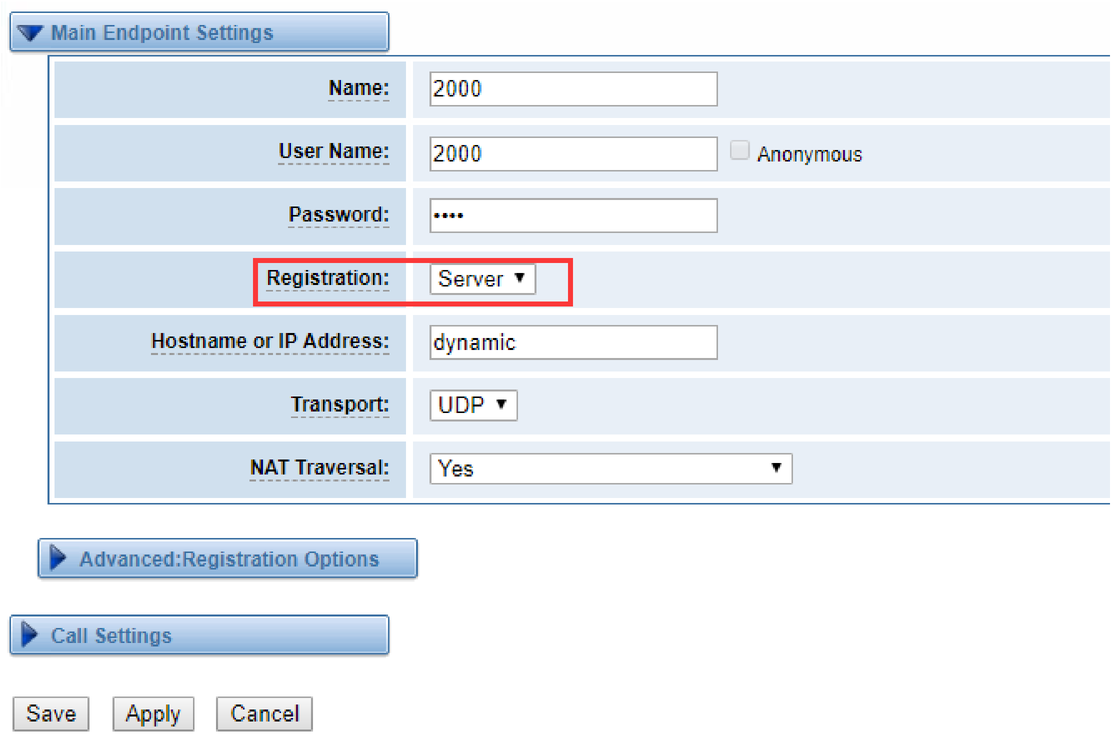
If you set up a SIP endpoint by registration “None” to a server, then you can’t register other SIP endpoints to this server. (If you add other SIP endpoints, this will cause Out-band Routes and Trunks confused.)

Figure 4-2 None Registration



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 4-3 Server



Also you can choose registration by "This gateway registers with the endpoint", it's the same with "None", except name and password.

Figure 4-4 Client

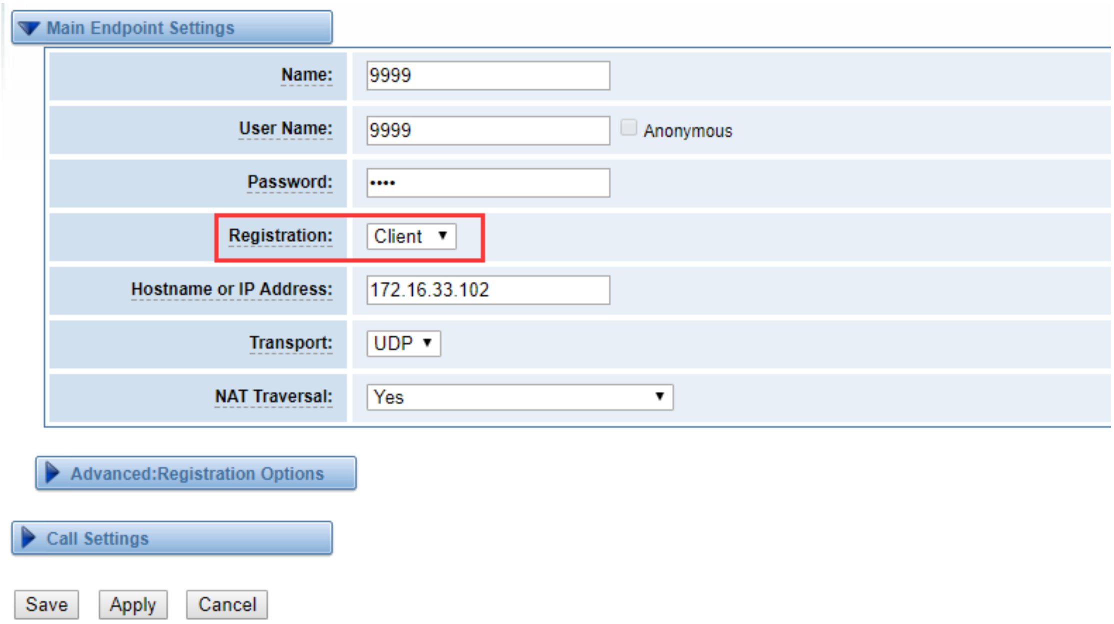


Table 4-1 Definiton of SIP Options

Options	**Definition**
Name	Display name
Username	Register name in your SIP server
Password	Authenticating with the gateway and characters are allowed.
Registration	**None** --- Not registering; **Server** --- When register as this type, it means the gateway acts as a SIP server, and SIP endpoints register to the gateway; **Client** --- When register as this type, it means the gateway acts as a client, and the endpoint should be 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	This sets the possible transport types for outgoing. Order of usage, when the respective transport protocols are enabled, is

	UDP, TCP, TLS. The first enabled transport type is only used for outbound messages until a Registration takes place. During the peer Registration, the transport type may change to another supported type if the peer requests so.
NAT Traversal	**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.

Advanced——Registration Options

Figure 4-5 Advanced Registration Options

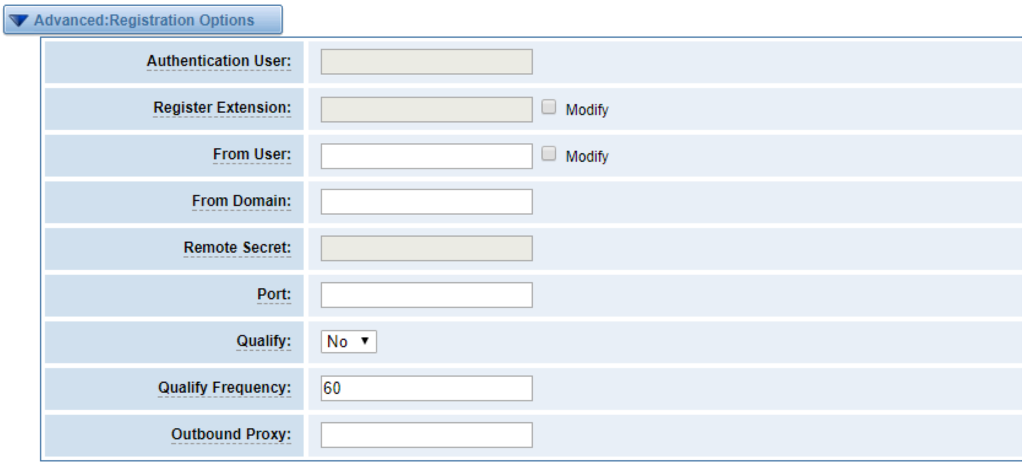


Table 4-2 Definition of Registration Options

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.

From User	A username to identify the gateway to this endpoint.
From Domain	A domain to identify the gateway to this endpoint.
Remote Secret	A password which is only used if the gateway registers to the remote side.
Port	The port number the gateway will connect to at 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 signalling instead of sending signalling dirrectly to endpoints.

Call Settings

Figure 4-6 Call Settings

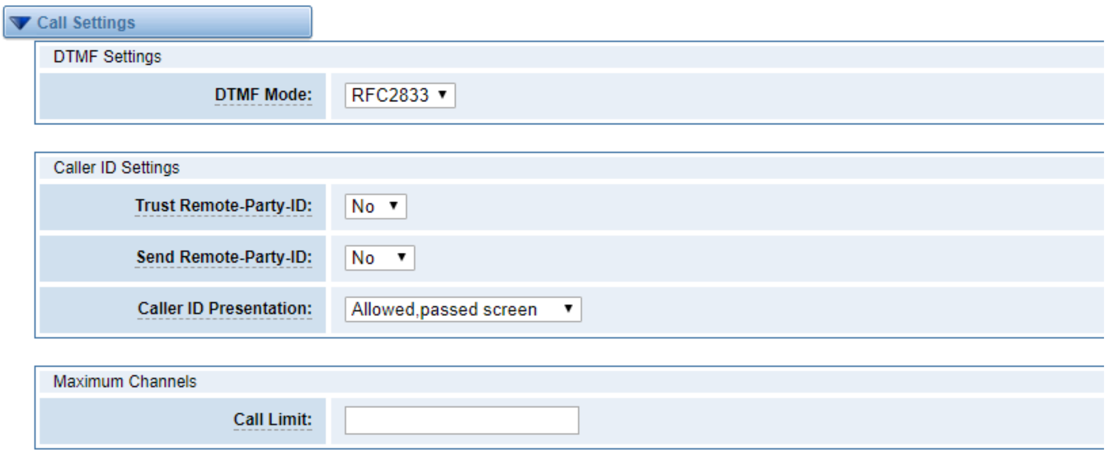


Table 4-3 Definition of Call Options

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).

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.
Call Limit	Usually used when this sip work as a trunk. To limit number of maximum channels supported by the sip trunk.

Advanced:——Signaling Settings

Figure 4-7 Signaling Settings

Table 4-4 Definition of Signaling Options

Options	**Definition**
Progress Inband	Whether there is ringing tone. Never: Indicates that incoming calls are never applicable. Optional values: yes / no / never. Default: yes
Append user=phone to URI	Whether or not to Add 'user = phone' to UPIS to include a valid phone number in the URI.

Add Q.850 Reason Headers	If it is available, Whether or not to add a reason header and use it.
Honor SDP Version	Whether or not to display Caller ID.
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.
Outbound Proxy	A proxy to which the gateway will send all outbound signaling instead of sending signaling directly to endpoints.

Advanced——Timer Settings

Figure 4-8 Timer Settings

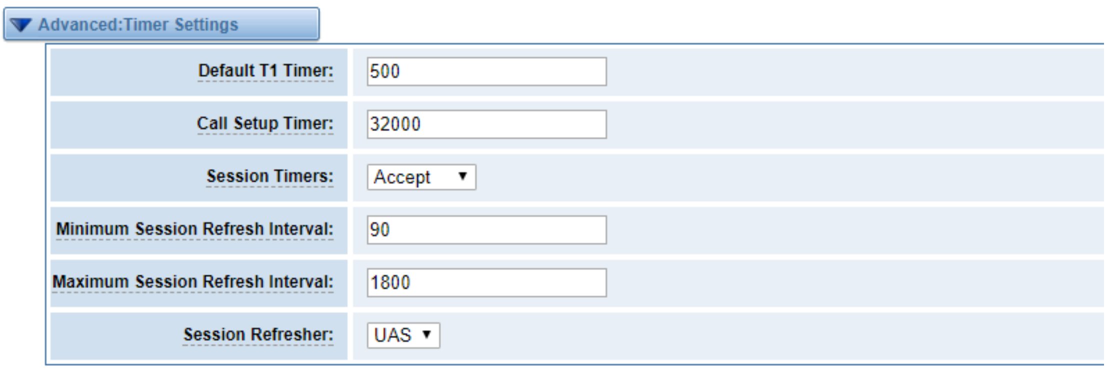
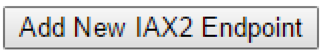


Table 4-5 Definition of Timer Options

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	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.

4.1.2 Add New IAX2 Endpoint

You can click 

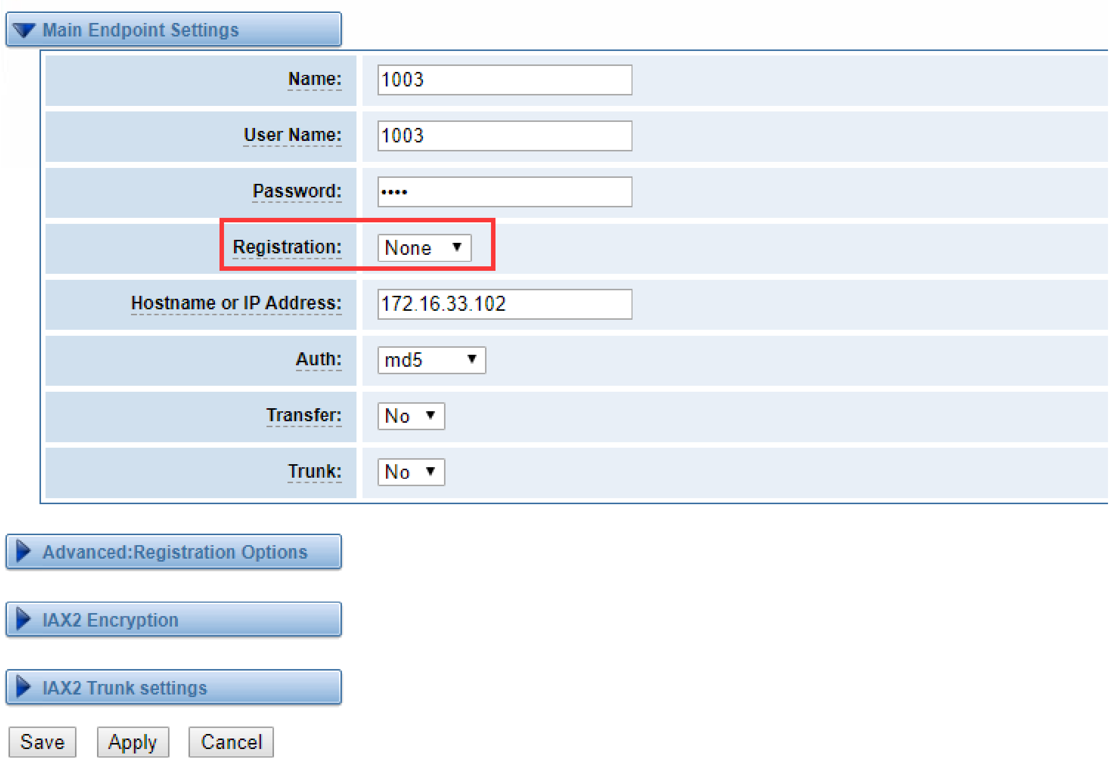
button to add a new IAX2 endpoint, and if you want to modify existed endpoints, you can click  button.

There are 3 kinds of registration types for choose. You can choose None, Endpoint registers with this gateway(work as a Server) or This gateway registers with the endpoint(work as a Client).

You can configure as follows:

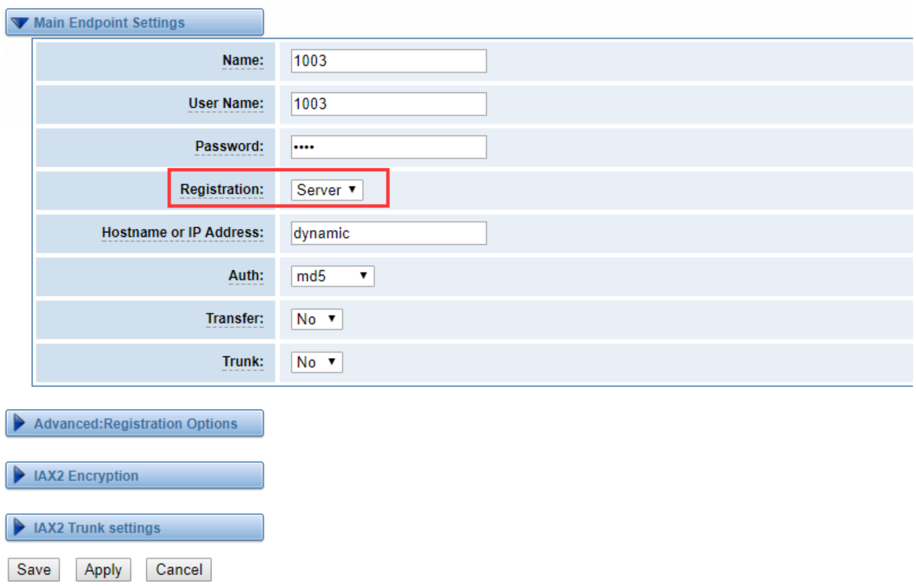
If you set up a IAx2 endpoint by registration "None" to a server, then you can't register other IAX2 endpoints to this server, just authenticate the username and password.

Figure 4-9 None Registrarion



For convenience, we have designed a method that you can register your IAX2 endpoint to your gateway, thus your gateway just work as a server.

Figure 4-10 Server



Also you can choose registration by “This gateway registers with the endpoint”, it will work as a Client.

Figure 4-11 Client

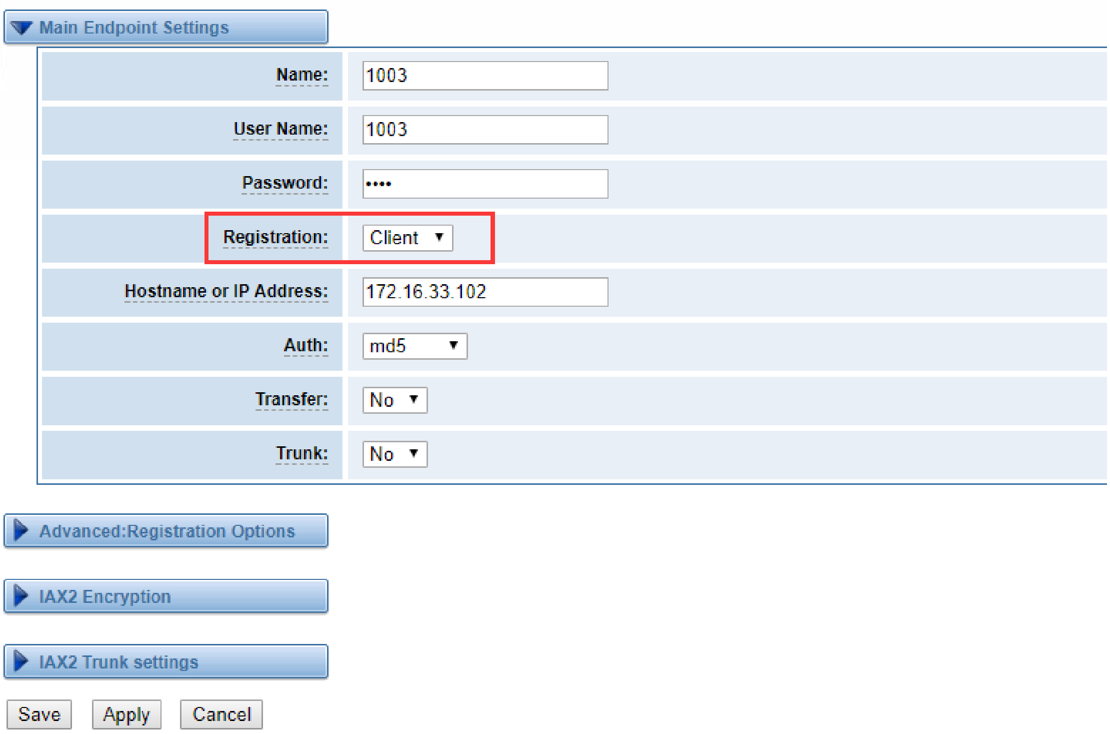


Table 4-6 Definition of IAX2 Options

Options	**Definition**
Name	Display name
Username	Authenication name in your IAX2 server
Password	Authenticating with the gateway and characters are allowed.
Registration	**None** --- Not registering; **Endpoint registers with this gateway** --- When register as this type, it means the gateway acts as a IAX2 server, and IAX2 endpoints register to the gateway; **This gateway registers with the endpoint** --- When register as this type, it means the gateway acts as a IAX2 client, and the endpoint should be register to a IAX2 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.
Auth	There are three authentication methods that are

	supported: md5, plaintext and rsa. The least secure is "plaintext", which sends passwords cleartext across the net. "md5" uses a challenge/response md5 sum arrangement, but still requires both ends have plain text access to the secret. "rsa" allows unidirectional secret knowledge through public/private keys.If "rsa" authentication is used, "inkeys" is a list of acceptable public keys on the local system that can be used to authenticate the remote peer, separated by the ":" character. "outkey" is a single, private key to use to authenticate to the other side.
Transfer	This application allows you to transfer calls.
Trunk	**"trunk=yes"** Purpose: To obtain a better chart of actual bandwidth usage per codec as seen "on-the-wire" when using IAX2 trunking between two Asterisk telephony servers.

Advanced——Registration Options

Figure 4-12 Registration Options

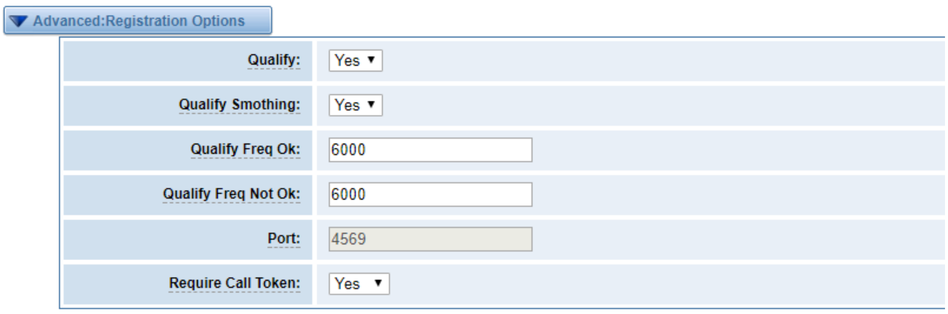


Table 4-7 Definition of Registration Options

Options	**Definition**
Qualify, Qualify Freq Ok, Qualify Freq Not Ok	The qualify, qualifyfreqok and qualifyfreqnotok settings are used to determine the status availability of an IAX peer. If a peer is consdered to be in a reachable (OK or LAGGED) state, it is queried for availability every "qualifyfreqok" milliseconds. If it is

	considered to be in an UNREACHABLE state, it is queried for availability every "qualifyfreqnotok" milliseconds.The qualify= setting turns the qualify system on (if the "yes" or xxx options are used) or off (if qualify=no, which is by default). The millisecond value of the qualify= setting specifies the maximum response time of the availability acknowledgement before the peer is considered to be in a "LAGGED" state.
Qualify Smothing	Use an average of the last two PONG result to reduce falsely detected LAGGED host. The default is 'no'.
Port	The port number the gateway will connect to at this endpoint.

IAX2 Encryption

Figure 4-13 IAX2 Encryption

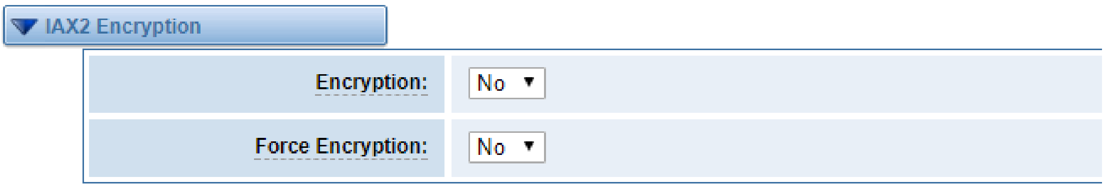


Table 4-8 Definition of Encrytion Options

Options	**Definition**
Encryption	Enable IAX2 encryption. The default is no.
Force Encryption	Force encryption insures no connection is established unless both sides support encryption. By turning this option on, encryption is automatically; turned on as well. The default is no

IAX2 Trunk Settings

Figure 4-14 IAX2Trunk Settings

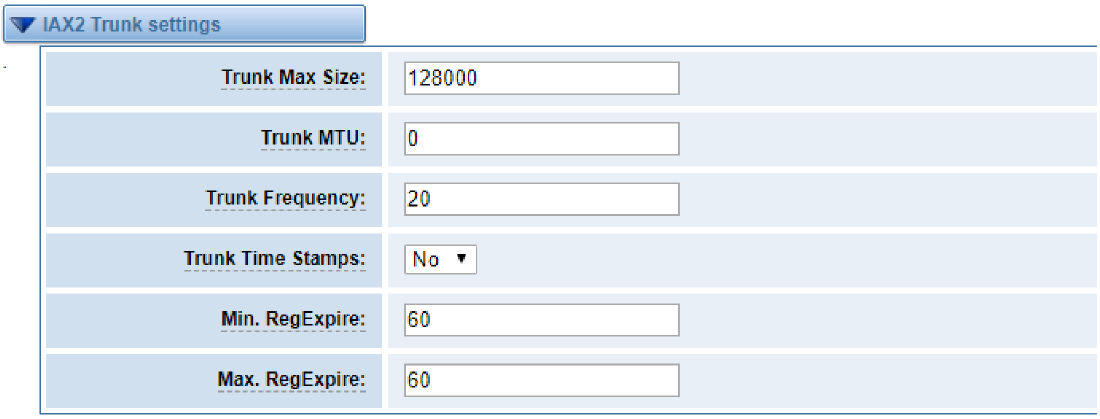


Table 4-9 Definition of Trunk Options

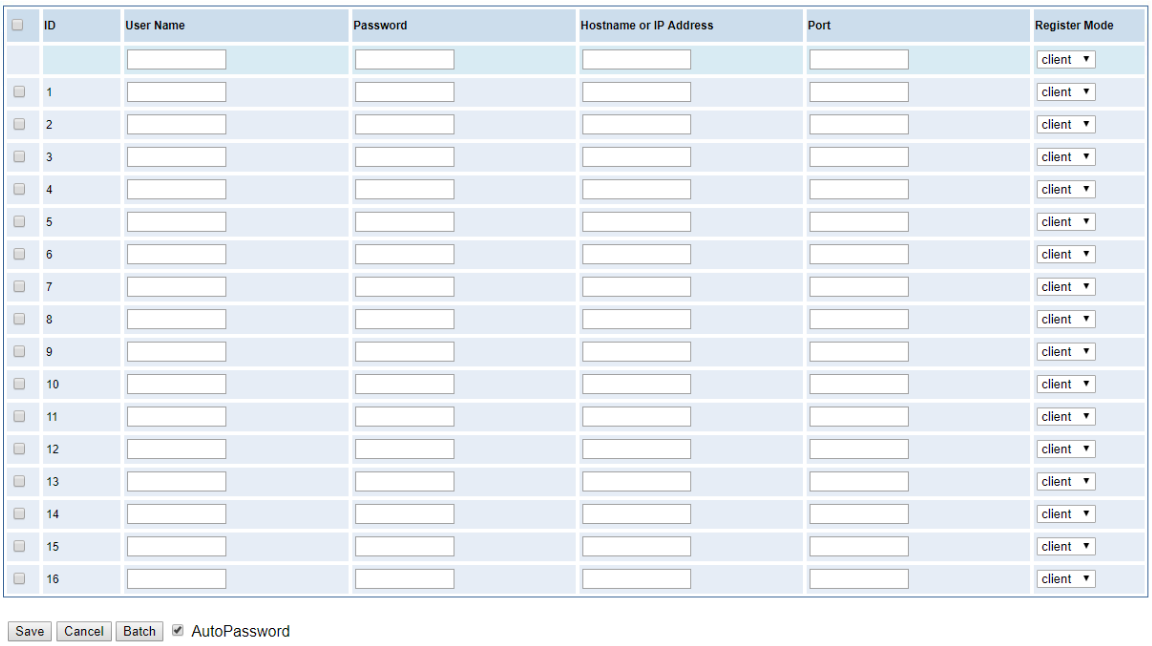
Options	Definition
Trunk Max Size	Defaults to 128000 bytes, which supports up to 800; calls of ulaw at 20ms a frame.
Trunk MTU	With a large amount of traffic on IAX2 trunk, there is a risk of bad voice quality when allowing the Linux system to handle fragmentation of UDP packets. Depending on the side of each payload, allowing the OS to handle fragmentation may not be very efficient. This setting sets the maximum transmission unit for AIX2 UDP trunking. The default is 1240 bytes which means if a trunk's payload is over 1240 bytes for every 20ms it will be broken into multiple 1240 bytes messages. Zero disables this functionality and let's the OS handle fragmentation.
Trunk Frequency	How frequently to send trunk msgs (in ms). This is 20ms by default.
Trunk Time Stamps	Should we send timestamps for the individual sub_frames within trunk frames? There is a small bandwith use for these (less than 1kbps/call), but they ensure that frame timestamps get sent end-to-end

	properly. If both ends of all your trunks go directly to TDM, _and_your trunkfreq equals the frame length for your codecs, you can probably suppress these. The receiver must also need to have it enabled.
Min. RegExpire	Minimum amounts of time that IAX2 peers can request as a registration interval (in seconds).
Max. RegExpire	Maximum amounts of time that IAX2 peers can request as a registration expiration interval(in seconds).

4.2 Batch SIP Endpoints

In this page,you can generate multiple SIP Extentations at the same time

Figure 4-15 Multiple SIP Extentations Settings



You can fill in the user name, password, domain name or IP address, port, and registration mode on the firt line and select the number of SIPs to be created. You can create up to the same number of SIP endpoints as the number of device ports at a time. After the above configuration, click Batch Setup and save it to create SIP endpoints in batches.

Table 4-10 Definition of Multiple SIP Extentations

Options	**Definition**

Name	Display name
Username	Register name in your SIP server
Password	Authenticating with the gateway and characters are allowed.
Registration	**None** --- Not registering; **Server** --- When register as this type, it means the gateway acts as a SIP server, and SIP endpoints register to the gateway; **Client** --- When register as this type, it means the gateway acts as a client, and the endpoint should be 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.
AutoPassword	Tick - Automatically increments based on the password entered in the first lineDo not check - All SIP endpoints have the same password as the first one.

4.3 Advanced SIP Settings

4.3.1 Networking

Networking General

Figure 4-16 Networking General

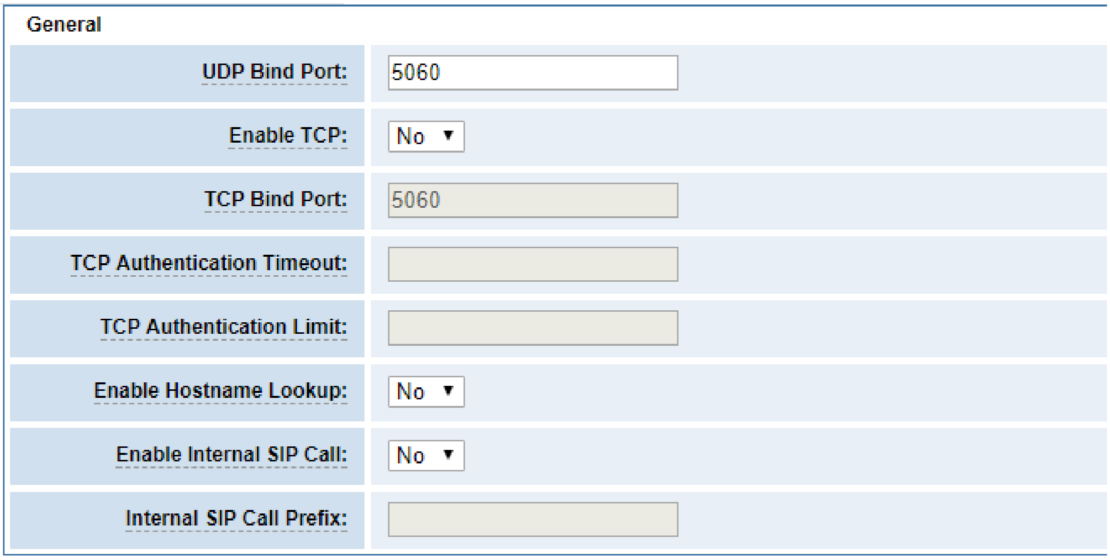


Table 4-11 Definition of Networking General Optiongs

Options	**Definition**
UDP Bind Port	UDP Bind Port
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 specifying a port in a SIP peer definition or when dialing outbound calls with suppress SRV lookups for that peer or call.
Enable Internal SIP Call	Whether enable the internal SIP calls or not when you select the registration option "Endpoint registers with this gateway".

Internal SIP Call Prefix	Specify a prefix before routing the internal calls.

NAT Settings

Figure 4-17 NAT Settings

Table 4-12 Definition of NAT Settings Options

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 statically 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 Hostname	The external hostname (and optional TCP port) of the NAT.
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.

RTP Settings

Figure 4-18 RTP Settings

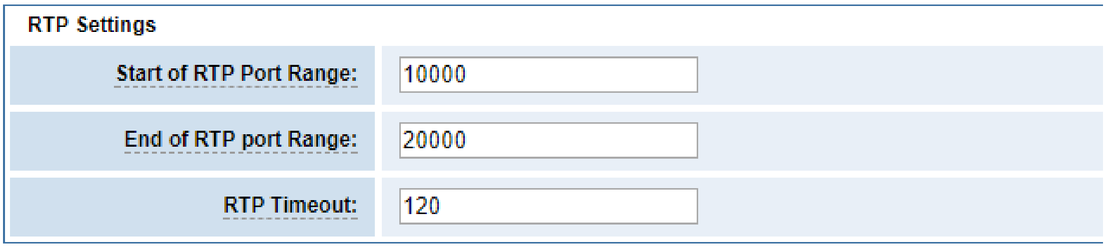
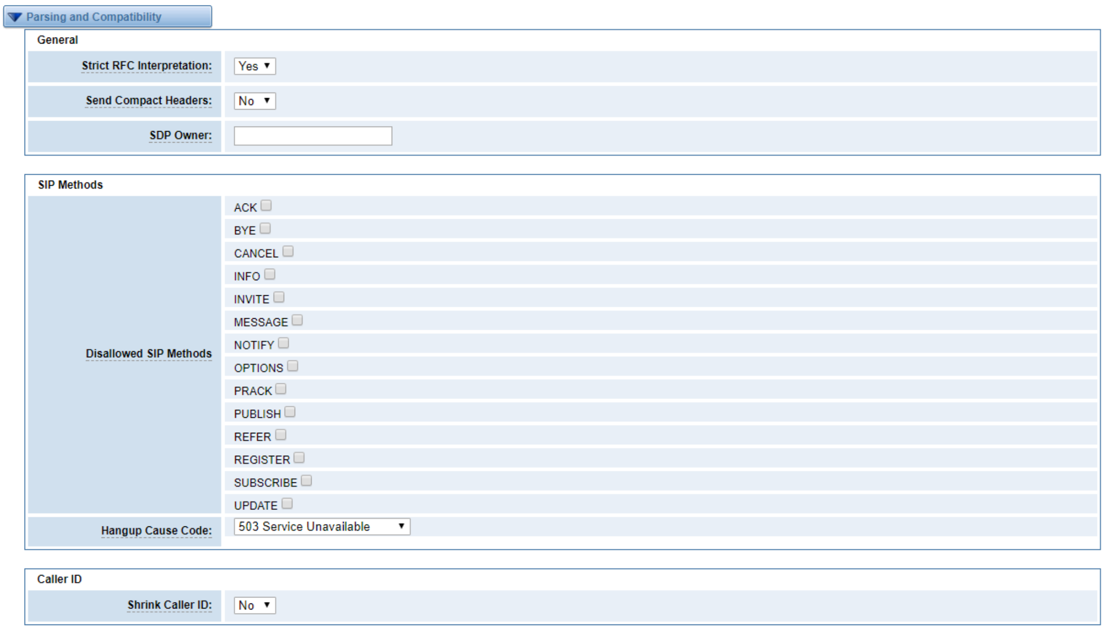


Table 4-13 Definition of RTP Settings Options

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 port numbers to be used for RTP
RTPTimeout	RTP Timeout retransmission time

4.3.2 Paesing and Compatibility

Figure 4-19 Paesing and Compatibility



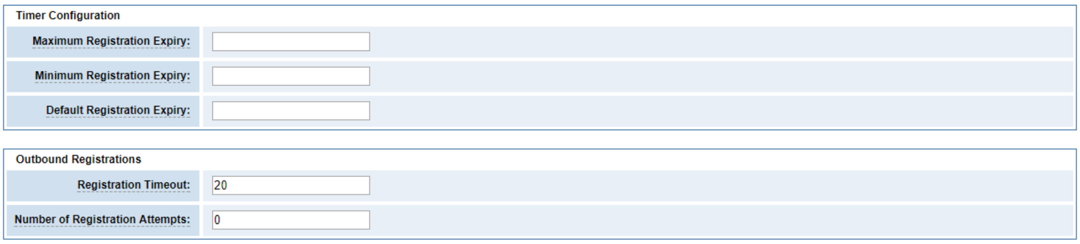


Table 4-14 Instruction of Parsing and Compatibility

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 Enter '0' for unlimited 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.

4.3.3 Security

Figure 4-20 Security Settings

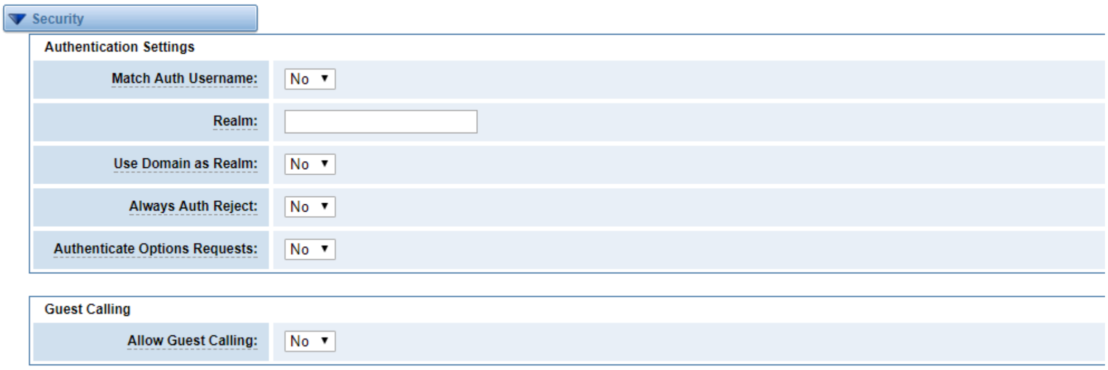


Table 4-15 Instruction of Security

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.

4.3.4 Media

Figure 4-22 Media Settings

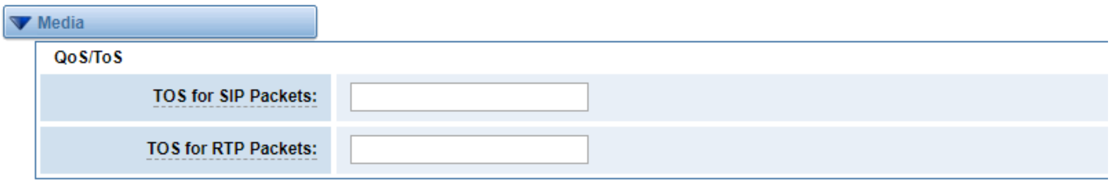


Table 4-16 Instruction of Media

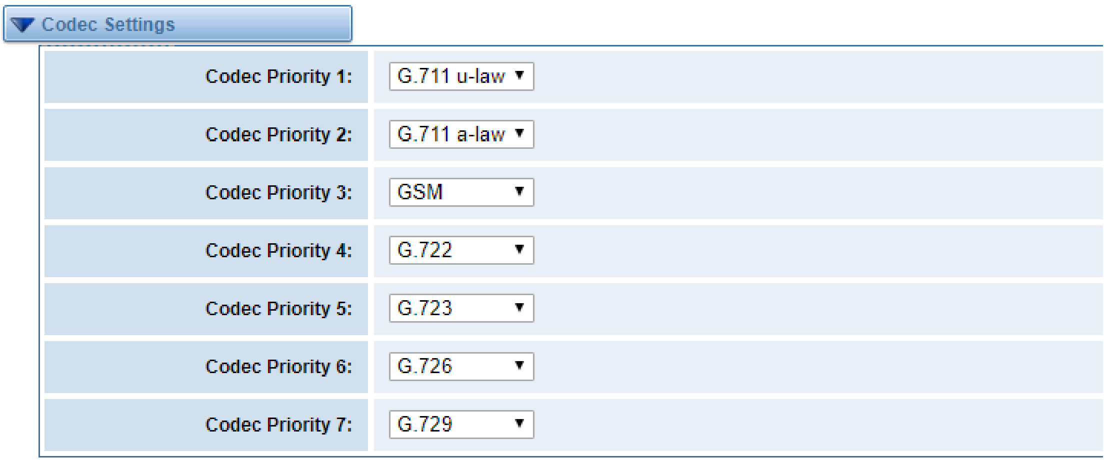
Options	Definition
Premature Media	Some ISDN links send empty media frames before the call is in ringing or progress state. The SIP channel will then send 183 indicating early media which will be empty - thus users get no ring signal. Setting this to "yes" will stop any media before we have call progress (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

4.3.5 Codec Settings

Select codecs from the list below.

Figure 4-22 Codec Settings



4.4 Advanced IAX2 Settings

4.4.1 General Settings

Figure 4-23 General Settings

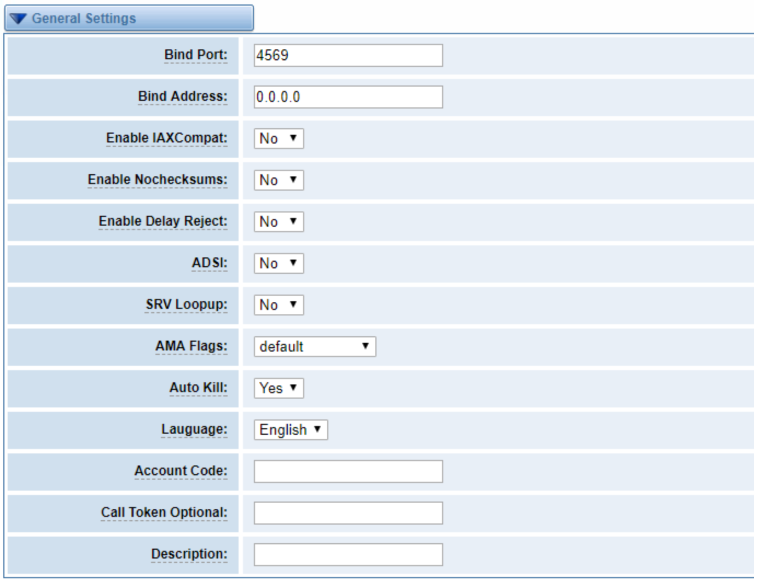


Table 4-17 Instruction of General

Options	**Definition**
Bind Port	Bind port and bindaddr may be specified
Enable IAXCompat	More than once to bind to multiple addresses, but the first will be the default.
Enable Nochecksums	Set iaxcompat to yes if you plan to use layered switches or some other scenario which may cause some delay when doing a lookup in the dialplan. It incurs a small performance hit to enable it. This option cause Asterisk to spawn a separate thread when it receives an IAX DPREQ (Dialplan Request) instead of blocking while it waits for a response.
Enable Delay Reject	Disable UDP checksums (if no checksums is set, then no checksums will be calculated/checked on system supporting the feature)

ADSI	ADSI (Analog Display Services Interface) can be enable if you have (or may have) ADSI compatible CPE equipment.
SRV Loopup	Whether or not to perform an SRV lookup on outbound calls
AMA Flags	You may specify a global default AMA flag for iaxtel calls. These flags are used in the generation of call detail records.
autokill	If we don't get ACK to our NEW within 2000ms,and autokill is set to yes, then we cancel the whole thing(that's enough time for one retransmission only).This is used to keep things from stalling for a long time for a host that is not available for bad connections.
Language	You may specify a global default language for users. This can be specified also on a per-user basis. If omitted, will fallback to English(en)
Account Code	You may specify a default account for Call Detail Records (CDRs) in addition specifying on a per-user basis.

4.4.2 Music on Hold

Figure 4-24 Music on Hold Settings

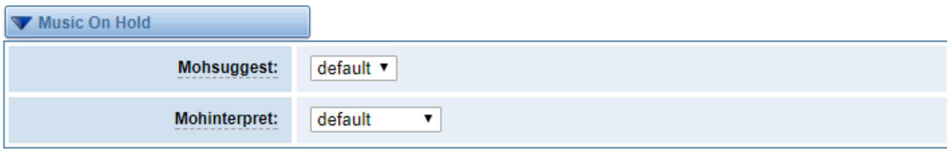


Table 4-18 Instruction of Music on Hold

Options	**Definition**
Mohsuggest	The 'Mohsuggest' option specifies which music on hold class to suggest to the peer channel when this channel place the peer on hold. It may be specified globally or on a per-user or per-peer basis.

Mohinterpret	You may specify a global default language for users. This can be specified also on a per-user basis. If omitted, will fall back to English(en)

4.4.3 Instruction of Codec Settings

Figure 4-25 Codec Settings

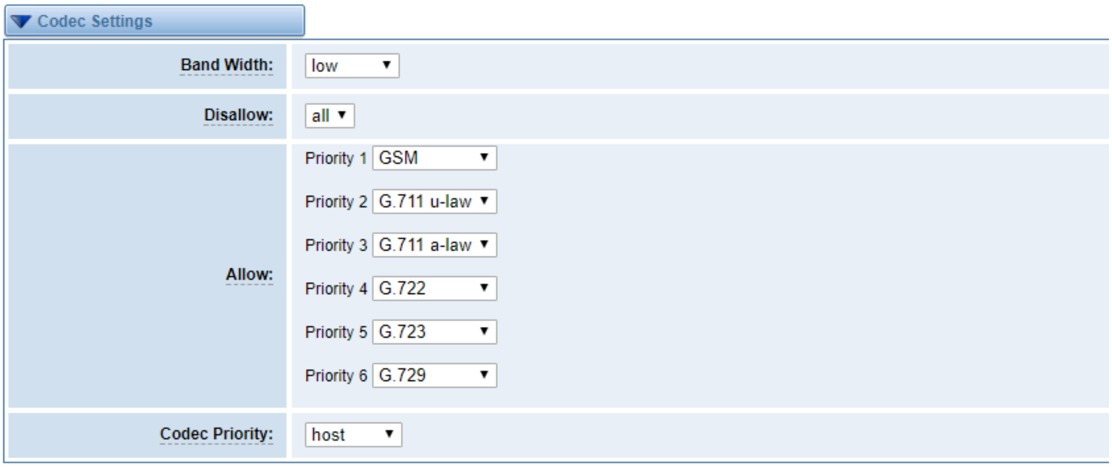


Table 4-19 Instruction of Codec Settings

Options	**Definition**
Band Width	Specify bandwith of low, medium, or high to control which codes are used in general
Disallow	Fine tune codes here using “allow” and “disallow” clause with specific codes
Allow	Fine tune codes here using “allow” and “disallow” clause with specific codes
Codec Priority	Codec priority controls the codec negotiation of an inbound IAX2 call. This option is inherited to all user entity separately which will override the setting in general.

4.4.4 Jitter Buffer Settings

Figure 4-26 Jitter Buffer

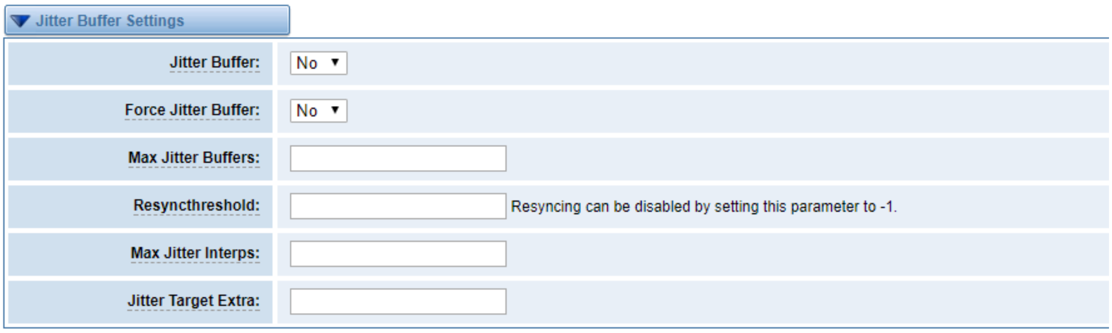


Table 4-20 Instruction of Jitter Buffer

Options	**Definition**
Jitter Buffer	Global default as to whether you want the jitter buffer at all
Force Jitter Buffer	In the ideal world, when we bridge VoIP channels we don't want to jitter buffering on the switch, since the endpoints can each handle this. However, some endpoints may have poor jitter buffers themselves, so this option will force to always jitter buffer, even in this case.
Max Jitter Buffers	A maximum size for the jitter buffer
Resyncthreshold	When the jitter buffer notice a significant change in delay that continue over a few frames, it will resync, assuming that the change in delay was caused by a timestamping mix-up. The threshold for noticing a change in delay is measured as twice the measured jitter plus this resync threshold.
Max Jitter Interps	The maximum number of interpolation frames the jitter buffer should return in a row. Since some clients do not send CNG/DTX frames to indicate silence, the jitter buffer will assume silence has begun after returning this many interpolations. This prevents interpolating throughout a long silence.

Jitter Target Extra	Number of milliseconds by which the new jitter buffer will pad its size. The default is 40, so without modification, the new jitter buffer will set its size to the jitter value may help if your network normally has low jitter, but occasionally has spikes.

4.4.5 Misc Settings

Figure 4-27 Misc Settings

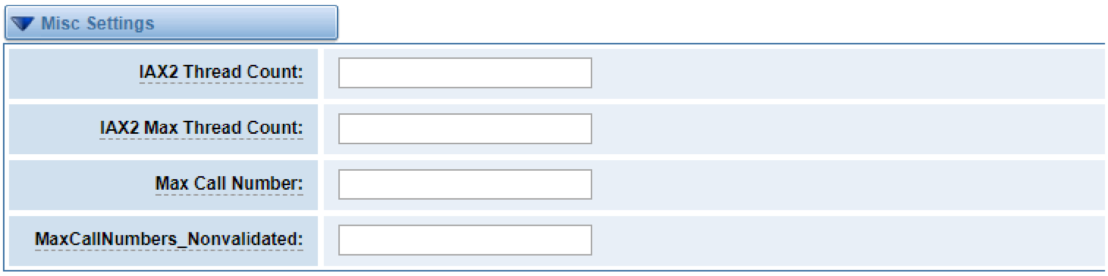


Table 4-21 Instruction of Misc Settings

Options	**Definition**
IAX Thread Count	Establishes the number of iax helper thread to handle I/O
IAX Max Thread Count	Establishes the number of extra dynamic threads that may by spawned to handle I/O
Max Call Number	The 'maxcallnumbers' option limits the amount of call numbers allowed for each individual remote IP address. Once an IP address reaches its call number limit, no more new connections are allowed until the previous ones close. This option can be used in a peer definition as well, but only takes effect for the IP of a dynamic peer after it completes registration.
MaxCallNumbers_Nonvalidated	The 'maxcallnumbers-nonvalidated' is used to set the combined number of call numbers that can be allocated for connections where call token validation has been disabled.

	Unlike the ‘maxcallnumbers’ option, this limit is not separate for each individual IP address. Any connection resulting in a non-call token validated call number being allocated contributes to this limit. For use cases, see the call should be sufficient in most cases.

4.4.6 Quality of Service

Figure 4-28 Quality of Service

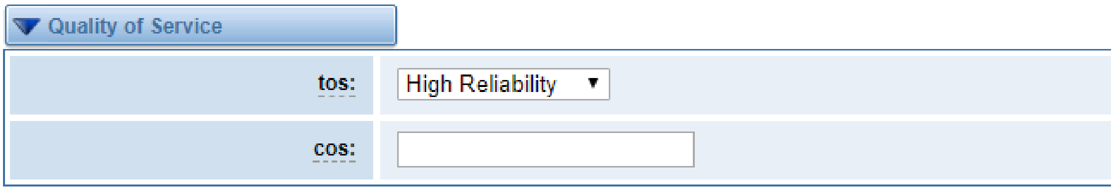
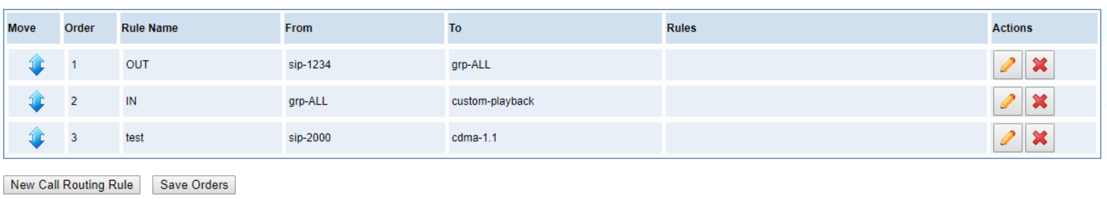


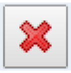
Table 4-22 Instruction of Quality of Service

Options	**Definition**
Tos	Type of service
Cos	Class of service

5. Routing

Figure 5-1 Routing Rules

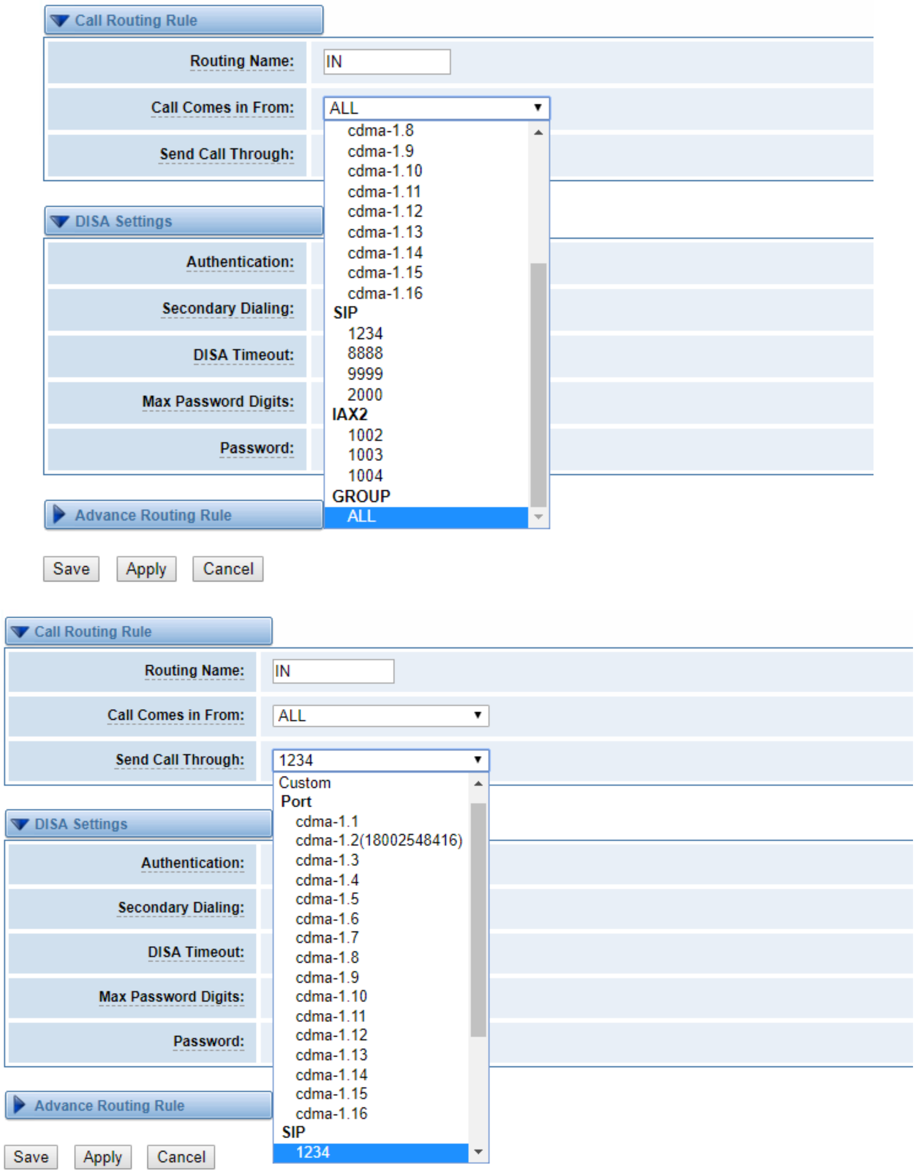


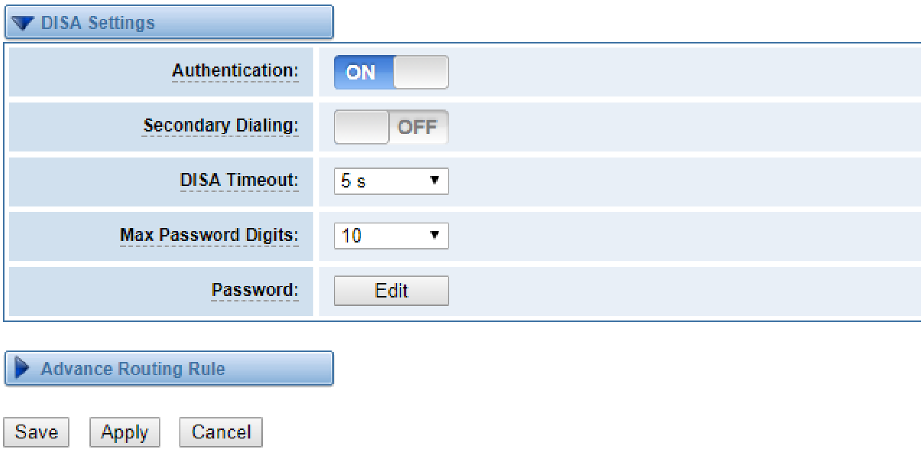
You are allowed to set up new routing rule by New Call Routing Rule , and after setting routing rules, move rules’ order by pulling up and down, click button to edit the routing and  to delete it. Finally click the Save Orders button to save what you set.

Call Routing Rule:

You can click New Call Routing Rule button to set up your routings.

Figure 5-2 Example of Set up Routing Rule





The figure above shows that all the phones in the group ALL are transferred to the SIP-1234 terminal.

Table 5-1 Definition of Routing Options

Options	**Definition**
Routing Name	The name of this route. Should be used to describe what types of calls this route matches (for example, 'SIP2CDMA' or 'CDAM2SIP').
Call Comes in From	The launching point of incoming calls.
Send Call Through	The destination to receive the incoming calls.

Table 5-2 Description of Advanced Routing Rule

Options	**Definition**
Dial Patterns that will use this Route	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). Rules: X matches any digit from 0-9 Z matches any digit from 1-9 N matches any digit from 2-9

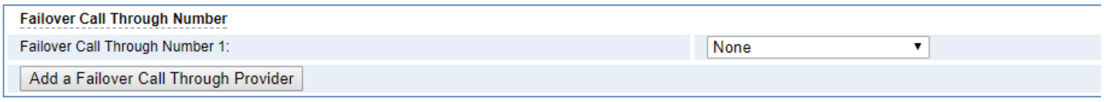
	[1237-9] matches any digit in the brackets (example: 1,2,3,7,8,9) . wildcard: matches one or more dialed digits. prepend: Digits to prepend to a successful match If the dialed number matches the patterns specified by the subsequent columns, then this will be prepended before sending to the trunks prefix: Prefix to remove on a successful match The dialed number is compared to this and the subsequent columns for a match. Upon a match, this prefix is removed from the dialed number before sending it to the trunks. match pattern: The dialed number will be compared against the prefix + this match pattern. Upon a match, the match pattern portion of the dialed number will be sent to the trunks CallerID: If CallerID is supplied, the dialed number will only match the prefix + match pattern if the CallerID has been transmitted matches this. When extensions make outbound calls, the CallerID will be their extension number and NOT their Outbound CID. The above special matching sequences can be used for CallerID matching similar to other number matches.
Set the Caller ID Name to	What caller ID name would you like to set before sending this call to the endpoint.
Forward Number	What destination number will you dial? This is very useful when you have a transfer call.
Custom Context	User-defined dialing rules
Failover Call Through Number	The gateway will attempt to send the call out each of these in the order you specify. You can create various time routes

	and use these time conditions to limit some specific calls.

Figure 5-3 Time Patterns that will use this Route

If you configure like this, then from January to March, from the first day to the last day of these months, from Monday to Thursday, from 00:00 to 02:00, during this time (meet all above time conditions), all calls will follow this route. And the time will synchronize with your Sever time.

Figure 5-4 Failover Call Through Number

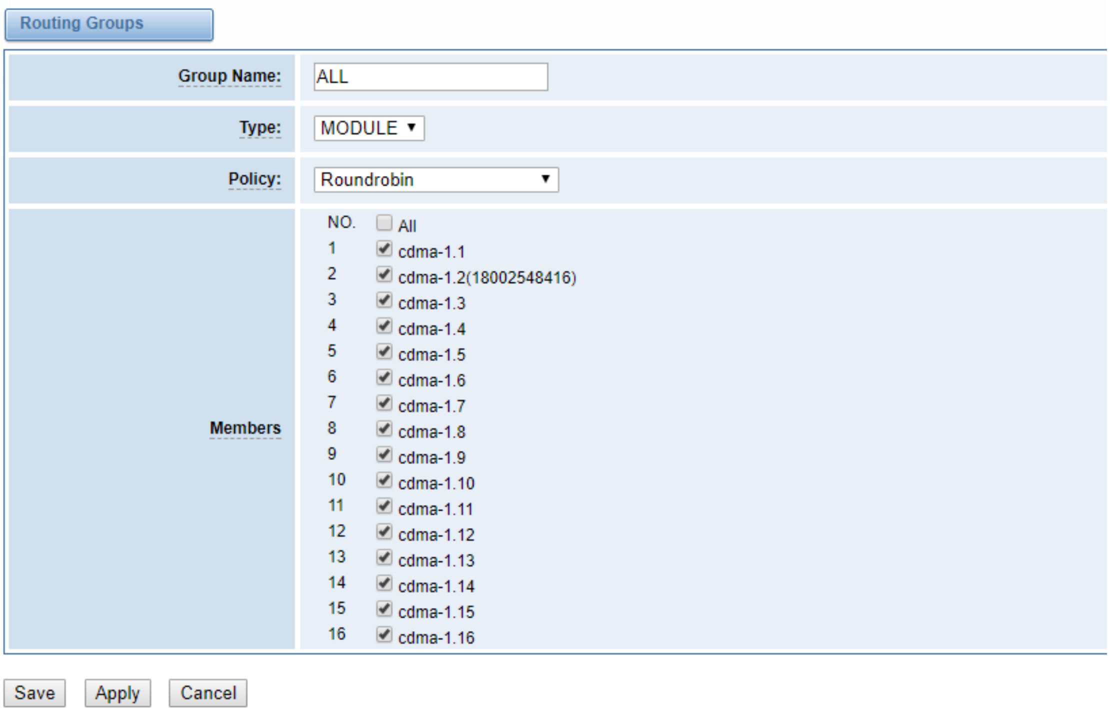


You can add one or more “Failover Call Through Numbers”.

5.1 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 Port or SIP to groups. Then if you want to make a call, it will find available port automatically.

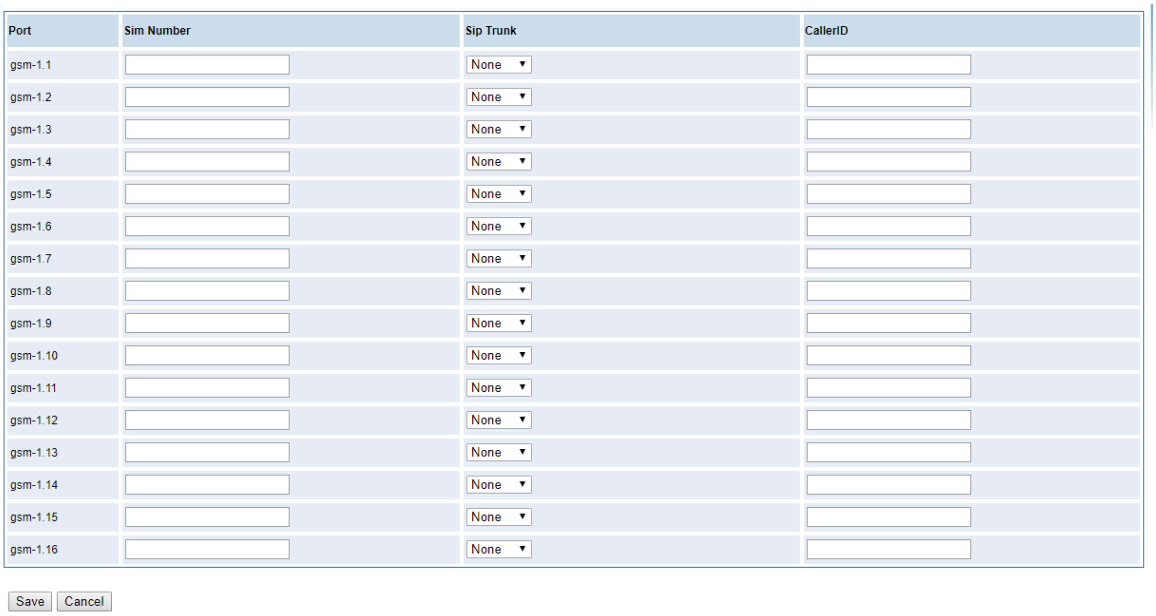
Figure 5-5 Routing Group



5.2 Batch Creating rules

This page can generate multiple routing rules at the same time

Figure 5-6 Batch Creating rules Group



You can configure the SIM Number, SIP trunk and calling Number for each port.And then, click "save" to batch creating multiple Routing rules.By an attention, the SIP trunk must be configures and the SIM number and calling Number can be emply.

Table 5-3 Description of Advanced Routing Rule

Options	**Definition**
Forward Number	What destination number will you dial? This is very useful when you have a transfer call.
SIP Trunk	Inbound and outbound calls through designated SIP trunks
Set the Caller ID Name to	What caller ID name would you like to set before sending this call to the endpoint.

5.3 MNP Settings

Mobile Number Portability allows switching between mobile phone operators without changing the mobile number. Sounds simple, but there are loads of tasks performed behind the scene at the operator end.

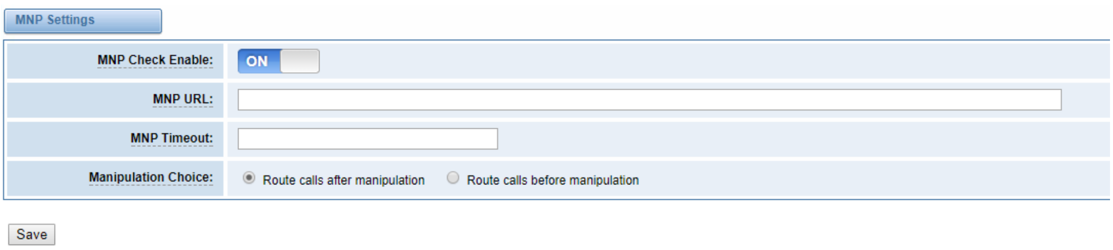
The URL is shown in the password string way. So please type the url in other place such a txt file, check it, then copy it to the gateway. The outgoing number in the url should be replaced by the variables **${num}**.

Here is an example of the MNP url:

https://s1.bichara.com.br:8181/chkporta.php?user=832700&pwd=sdsfdg&tn=8388166902

The 8388166902 is the outgoing phone number, when config the MNP url, should replce it with ${num}. Then it turns to https://s1.bichara.com.br:8181/chkporta.php?user=832700&pwd=sdsfdg&tn=${num}。

Figrue 5-7 MNP Settings

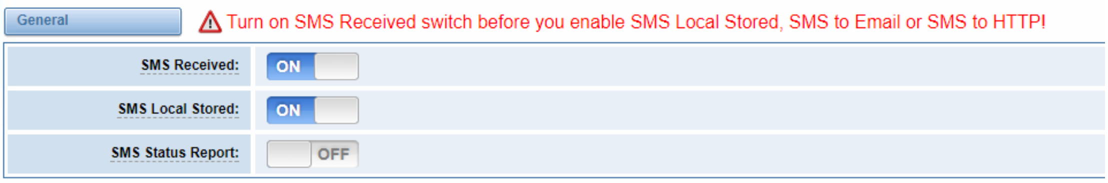


6. SMS

6.1 General

You can choose enable SMS Received, SMS Local Strored and SMS Status Report or not.

Figure 6-1 SMS Settings



6.1.1 Sender Options

You can change sender options here, include resend, times of resend.

Figure 6-2 Sender Options

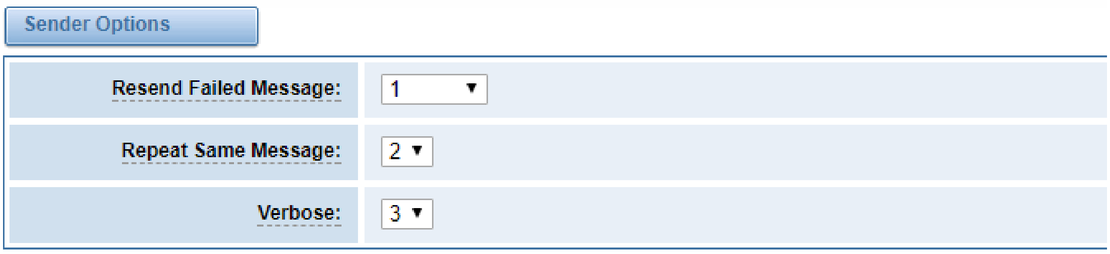


Table 6-1 Description of Sender Options

Options	**Definition**
Resend Failed Message	The times that you will attempt to resend your failed message.
Repeat Same Message	The times that you will resend the same message.

6.1.2 SMS to Email

This is a tool that makes it available for you to email account to transmit the SMS to other email boxes. The following settings realize that received SMS through openvpnvoip@gmail.com transmit to openvpnvoip@yahoo.com.cn, openvpnvoip@hotmail.com and support@openvox.cn

Figure 6-3 SMS to Email

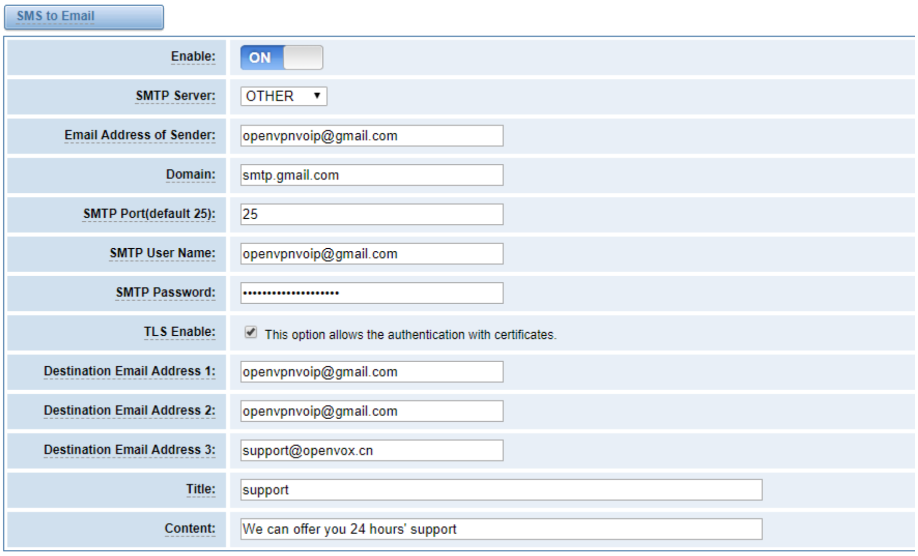


Table6-2 Types of E-mail Box

E-mail Box Type	SMTP Server	SMTP Port	SMTP Security Connectivity
Gmail	smtp.gmail.com	587	√
HotMail	smtp.live.com	587	√
Yahoo!	smtp.mail.yahoo.co.in	587	×
e-mail	smtp.163.com	25	×

Table6-3 Definition of SMS to E-mail

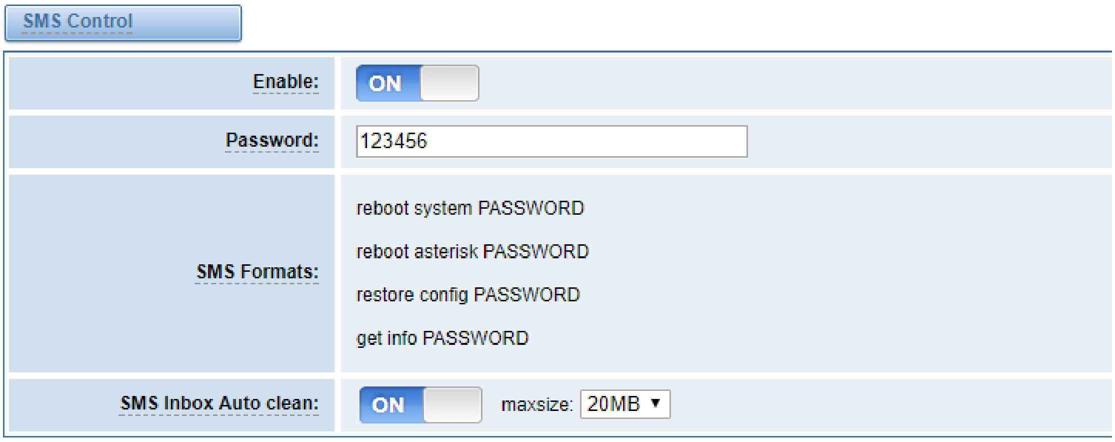
Options	Definition
Enable	When you choose on, the following options are available, otherwise, unavailable.

Email Address of Sender	To set the email address of an available email account. For example, openvpnvoip@gmail.com.
Domain	To set outgoing mail server. e.g. smtp.gmail.com
SMTP Port	To set port number of outgoing mail server. (Default is 25)
SMTP User Name	The login name of your existing email account. This option might be different from your email address. Some email client doesn't need the email postfix
SMTP Password	The password to login your existing email.
TLS Enable	When you choose Yahoo and 163 free e-mails, this option is not available.
SMTP Server	To set outgoing mail server. e.g. mail.openvox.cn.
Destination Email Address1	The first email address to receive the inbox message.
Destination Email Address2	The second email address to receive the inbox message.
Destination Email Address3	The third email address to receive the inbox message.

6.1.3 SMS Control

Allowing endpoints to send some specific KEY WORDS and corresponding PASSWORD to operate the gateway and message is case-sensitive. In default, this function is disabled.

Figure 6-4 SMS Control



For example, SMS control password is 123456 which has nothing to do with the login password, you can send “get info 123456” to the module’s phone number to get your gateway’s IP information.

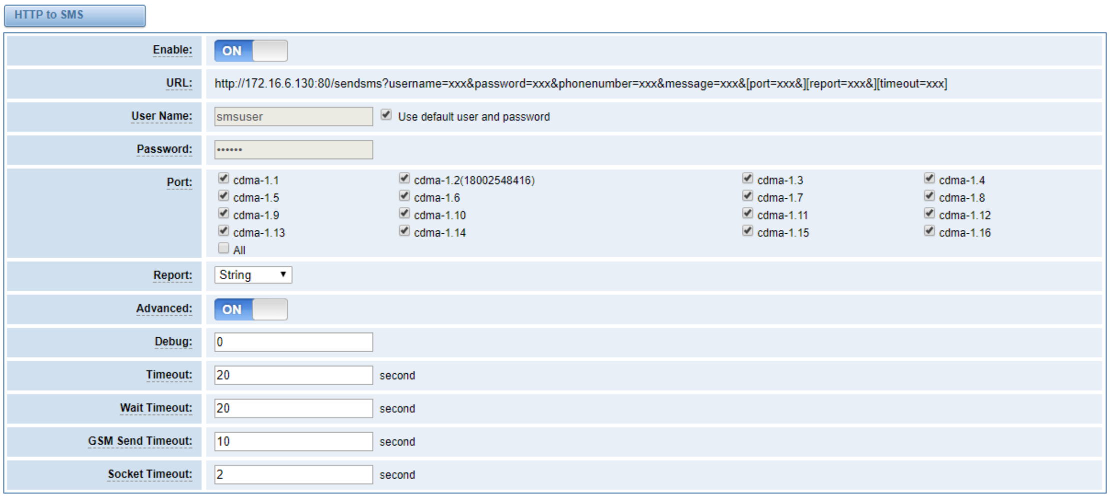
Table 6-4 Definition of SMS Control

Options	**Definition**
Enable	ON(enable), OFF(disable)
Password	The password to confirm that SMS makes the gateway rebooted, shut down, restored configuration files and get info on this gateway.
SMS Format	For example, the message formats: reboot system PASSWORD: To reboot your whole gateway. The PASSWORD is referring to the PASSWORD you set up from option “PASSWORD” above. Reboot asterisk PASSWORD: To restart your gateway core. Restore configs PASSWORD: To reset the configuration files back to the default factory settings. Get info PASSWORD: To get your gateway IP address

SMS inbox Auto clean	switch on: When the size of the SMS inbox record file reaches the max size, the system will cut a half of the file. New record will be retained. switch off: SMS record will remain, and the file size will increase gradually. default on, max size = 20 MB

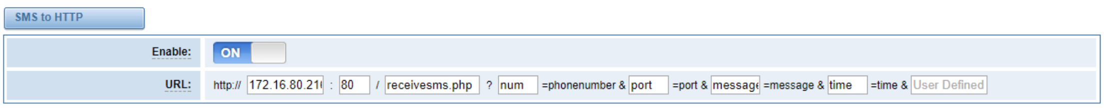
6.1.4 HTTP to SMS

Figure 6-5 HTTP to SMS



6.1.5 SMS to HTTP

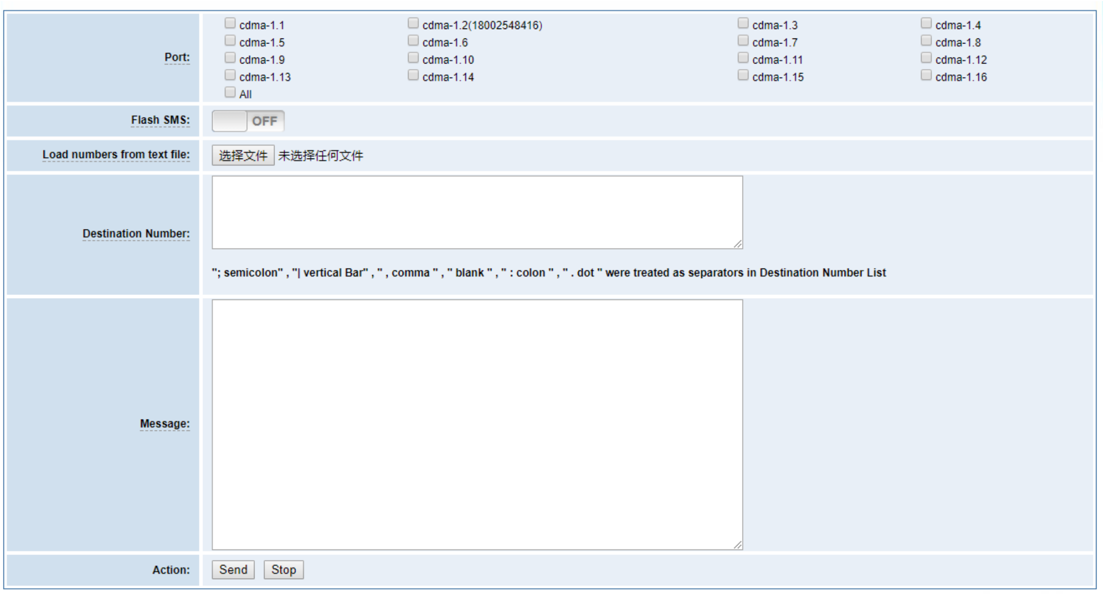
Figure 6-6 SMS to HTTP Settings



6.2 SMS Sender

You can choose one or more ports to send SMS to the destination number, different numbers should be separated by symbols: '\r', '\n', space character, semicolon and comma. Then you can see much feedback information.

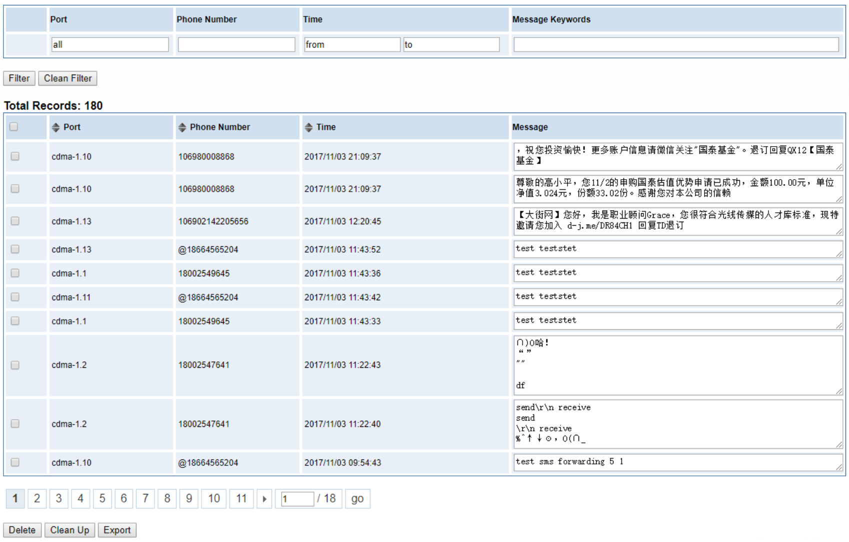
Figure 6-7 SMS Sender



6.3 SMS Inbox

On this page, you are allowed to scan, delete, clean up, and export each port's received SMS. Also you are allowed to check messages by port, phone number, time order and message keywords.

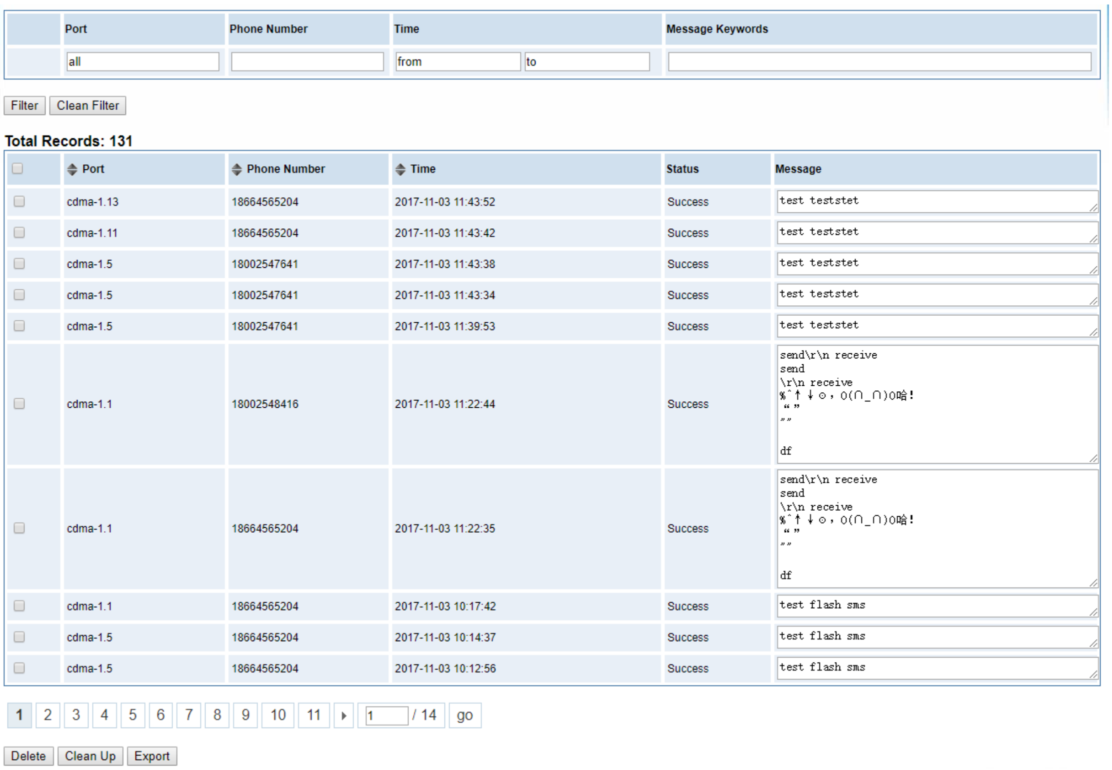
Figure 6-8 SMS Inbox



6.4 SMS Outbox

On this page, you are allowed to scan, delete, clean up, and export each port's received SMS. Also you are allowed to check messages by port, phone number, time order and message keywords.

Figure 6-9 SMS Outbox

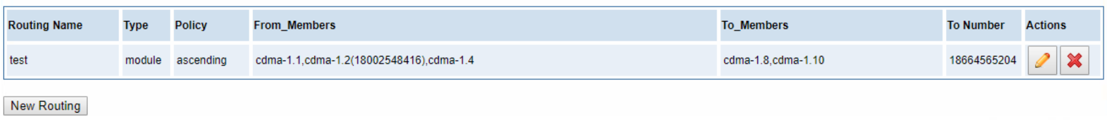


6.5 SMS Forwarding

Using this feature, you can forward incoming sms to your mobile. You can click New Routing button to add new routing.

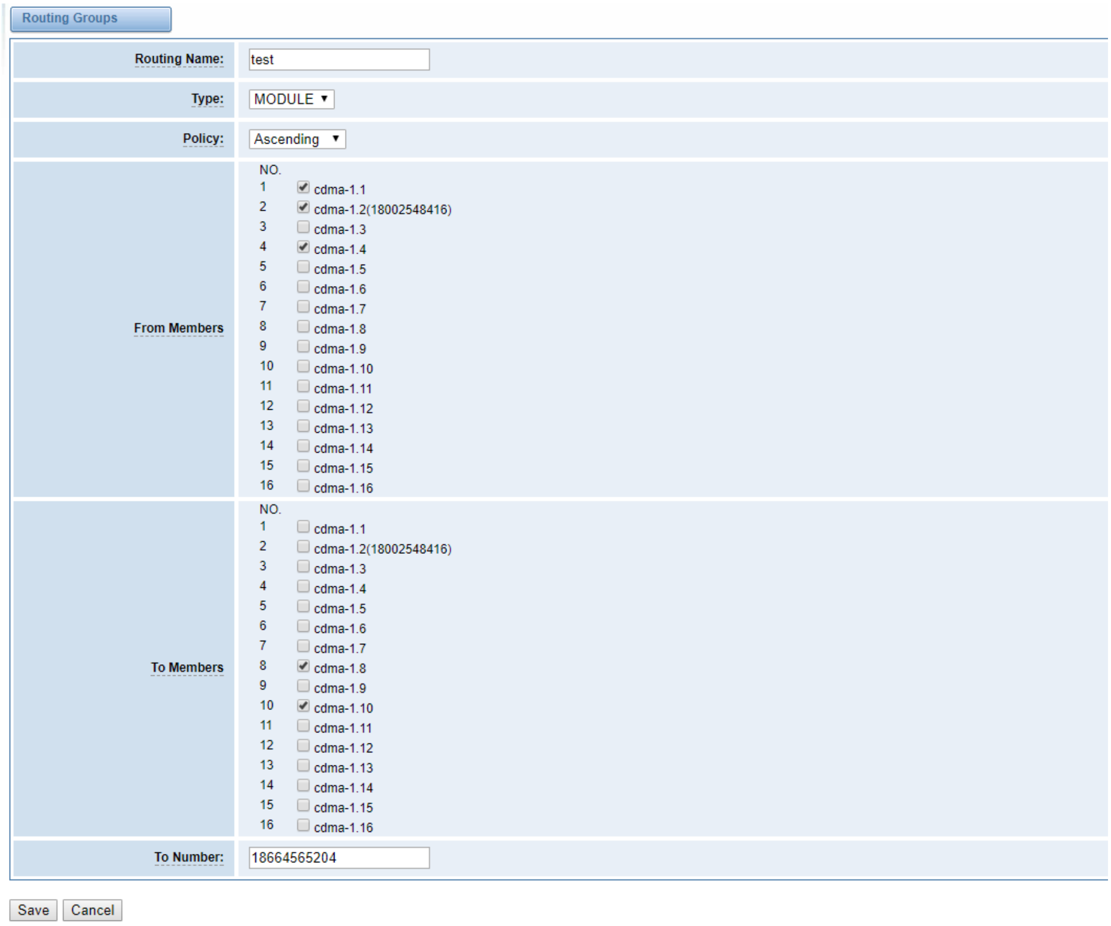
Such as:

Figure 6-10 SMS Forwarding Rules



SMS received by cdma-1.1 and cdma-1.2, cdma-1.4, will be transfered to phone number 18664565204 through port cdma-1.8 or cdma-1.10.

Figure 6-11 Create a Routing



For "ascending" Policy, if you choose 2 or more ports members, it will use first available port to transfer sms. For this case, if cdma-1.8 is availble, it will always use cdma-1.8 to trnasfer sms; Otherwise, it will use cdma-1.10 to transfer sms.

7. Network

7.1 LAN Settings

There are three types of LAN port IP, Factory, Static and DHCP. Factory is the default type, and it is 172.16.98.1. When you Choose LAN IPv4 type is “Factory”, this page is not editable.

A reserved IP address to access in case your gateway IP is not available. Remember to set a similar network segment with the following address of your local PC.

Figure 7-1 LAN Settings

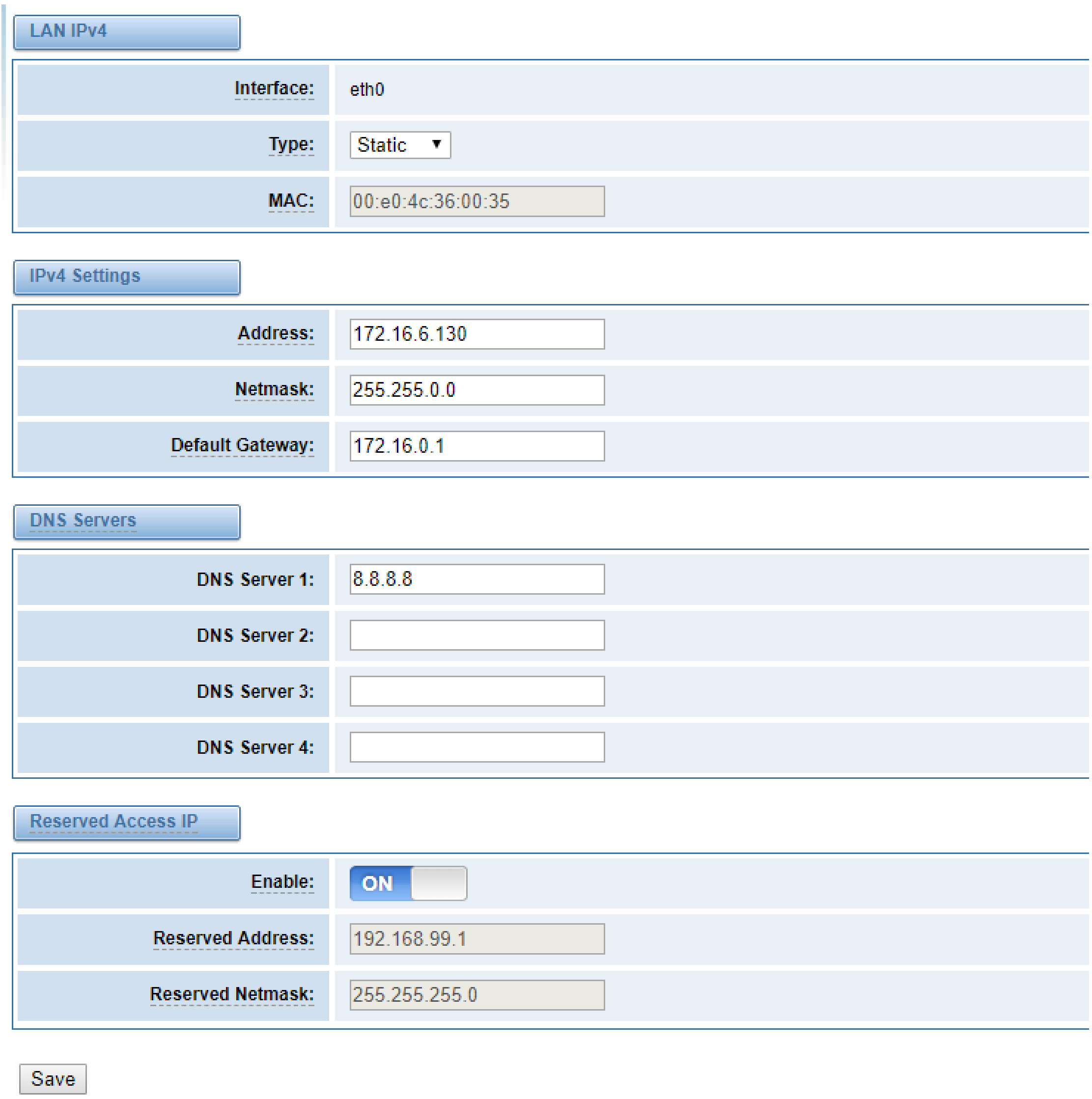


Table 7-1 Definition of LAN Settings

Options	Definition
Interface	The name of network interface.
Type	The method to get IP. Factory: Getting IP address by Slot Number (System information to check slot number). Static: manually set up your gateway IP. DHCP: automatically get IP from your local LAN.

MAC	Physical address of your network interface.
Address	The IP address of your gateway.
Netmsk	The subnet mask of your gateway.
Default Gateway	Default getaway IP address.

DNS Servers: A list of DNS IP address. Basically this info is from your local network service provider,and you can fill in four DNS servers.

7.2 WAN Settings

There are three types of WAN port IP, Disable, Static and DHCP. DHCP is the default type. When you Choose IPv4 type is "Disable" or "DCHP", this page is not editable.

Figure 7-2 WAN Settings

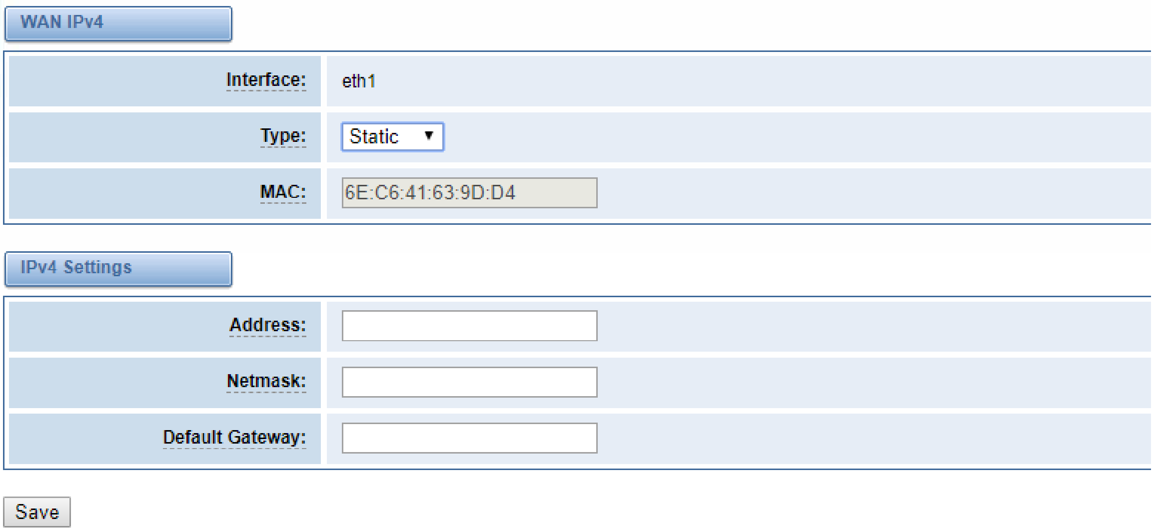


Table 7-2 Definition of WAN Settings

Options	**Definition**
Interface	The name of network interface.
Type	The method to get IP. Factory: Getting IP address by Slot Number (System information to check slot number).

	Static: manually set up your gateway IP. DHCP: automatically get IP from your local LAN.
MAC	Physical address of your network interface.
Address	The IP address of your gateway.
Netmsk	The subnet mask of your gateway.
Default Gateway	Default getaway IP address.

7.3 VPN Settings

SWG-2016/32 series gateways support PPTP VPN.

Figure 7-3 VPN Settings

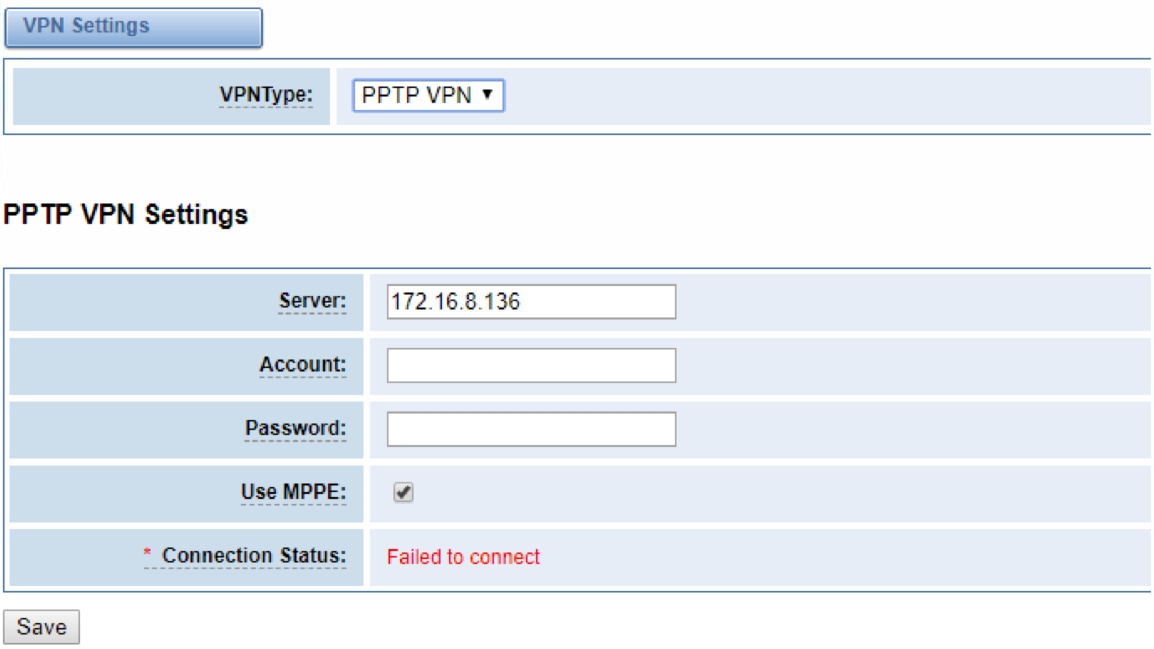


Table 7-3 Definition of VPN Settings

Options	Definition
VPN Type	None – close VPN PPTP VPN – use PPTP VPN
server	The server's IP address

Account	Server account
Password	The server's password
Use MPPE	Whether to use MPPE
Connection Status	Is it successful to connect to the server

7.4 DDNS Settings

You can enable or disable DDNS (dynamic domain name server).

Figure 7-4 DDNS Settings

Table7-4 Definition of DDNS Settings

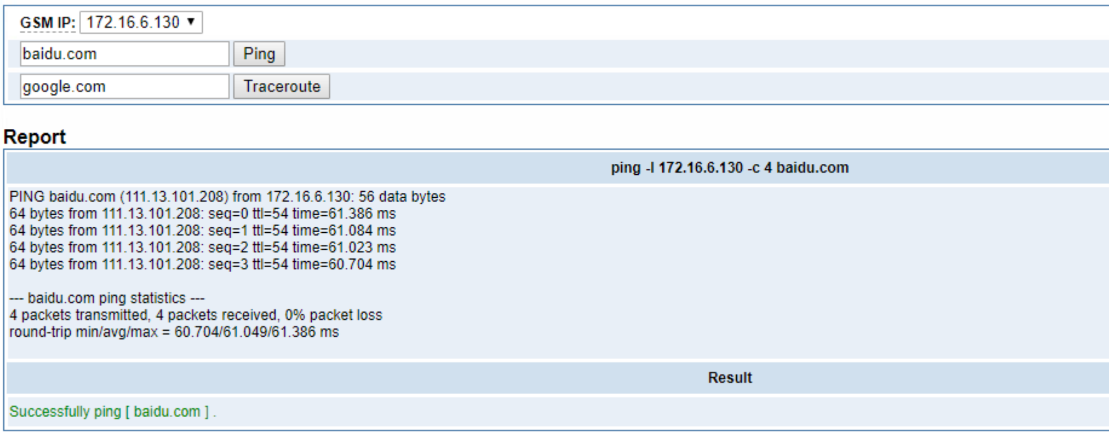
Options	**Definition**
DDNS	Enable/Disable DDNS(dynamic domain name server)
Type	Set the type of DDNS server.
Username	Your DDNS account’s login name.
Password	Your DDNS account’s password.
Your domain	The domain to which your web server will belong.

7.5 Toolkit

7.5.1 Ping and Traceroute

It is used to check network connectivity. Support Ping command on web GUI.

Figure 7-5 Toolkit



7.5.2 TCP Capture

You can capture the tcp packets on the page to facilitate locationg problems.

Figure 7-6 TCP Capture

Table7-5 Definition of DDNS Settings

Options	Definition
Inferface	You can choose eth0 or eth1
Source host	Source host IP
Destination host	Destination host IP
Port	Which port you want to capture?
Protocol	Which protocol you want to capture?

7.6 Security Settings

7.6.1 Firewall Settings

Figure 7-7 Firewall Settings

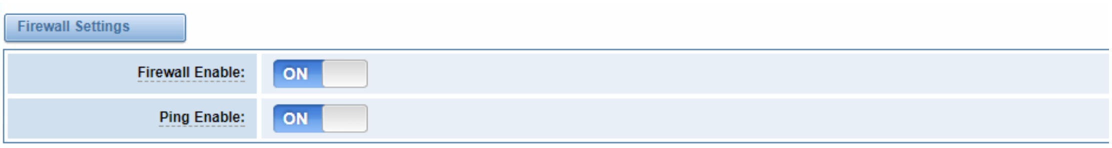


Table 7-6 Deginition of Firewall Settings

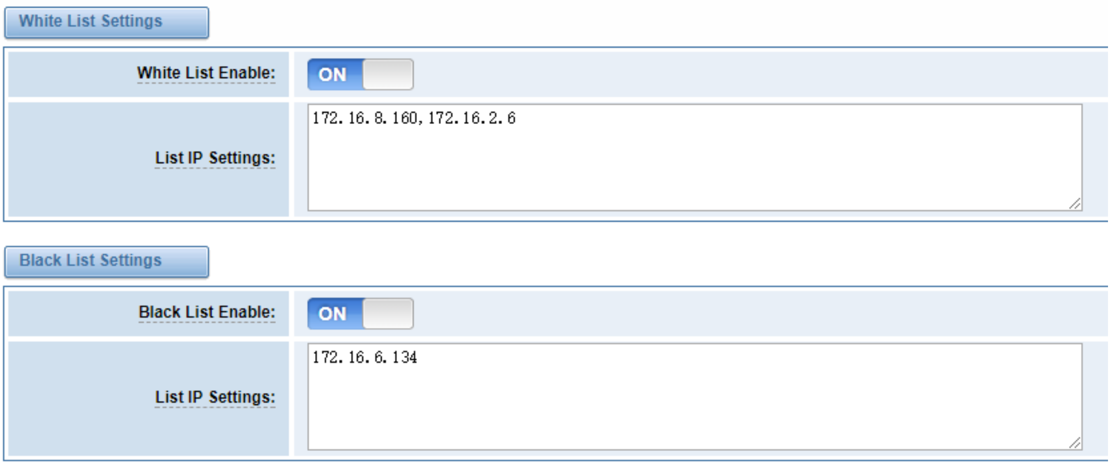
Options	Definition
Firewall Enale	If you want to use White/Black List, and security rules, you must enble this option.
Ping Enable	To disable ping or not. OFF: disable ping. This gateway will not allow to ping.

7.6.2 White/Black List Settings

White List Enbale: To enable white list or not.

List IP Settings: IPs are separated only by "," character.

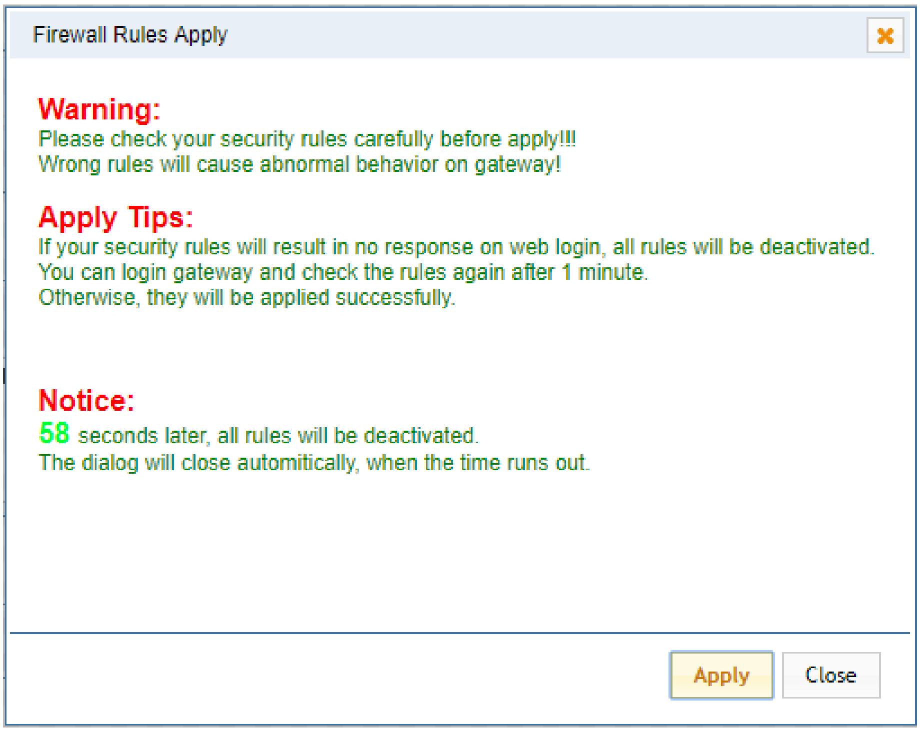
Figure 7-8 White/Black List Settings



Click "Save" button to save configration; Click "submit" button to submit and apply configuration.

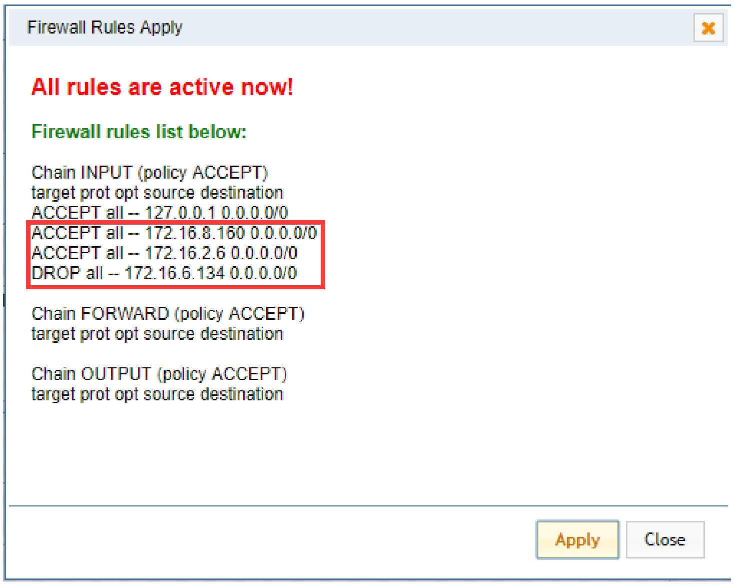
If "List IP Settings" has no problem, you will see popup window like below. Please read the warning and tips carefully. And Click "Apply" button in 1 minute. If time runs out, this window will close automatically.

Figure 7-9 Firewall Rules Apply



If you see windows like below. It means your configuration has been applied successfully.

Figure 7-10 Firewall Rules Apply



7.7 Security Rules

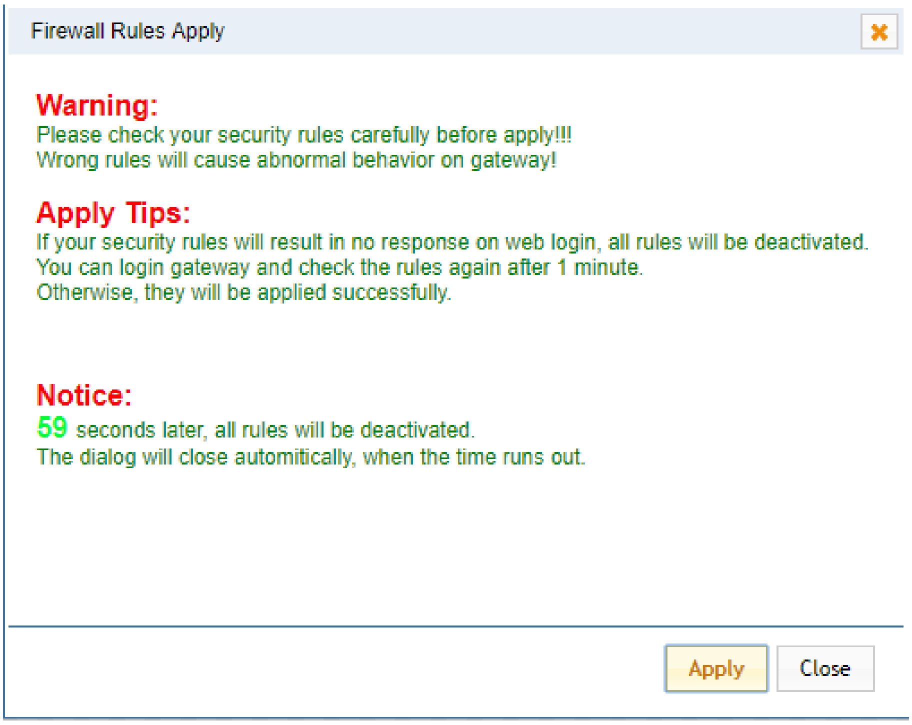
Figure 7-11 Security Rules

Rule Name	Type	Protocol	IP	Port	Actions
test1	TCP	ACCEPT	172.16.80.216/255.255.0.0	5060:5060	
test2	UDP	DROP	172.16.80.216/255.255.0.0	1000:2000	

Click "submit" button to submit and apply configuration.

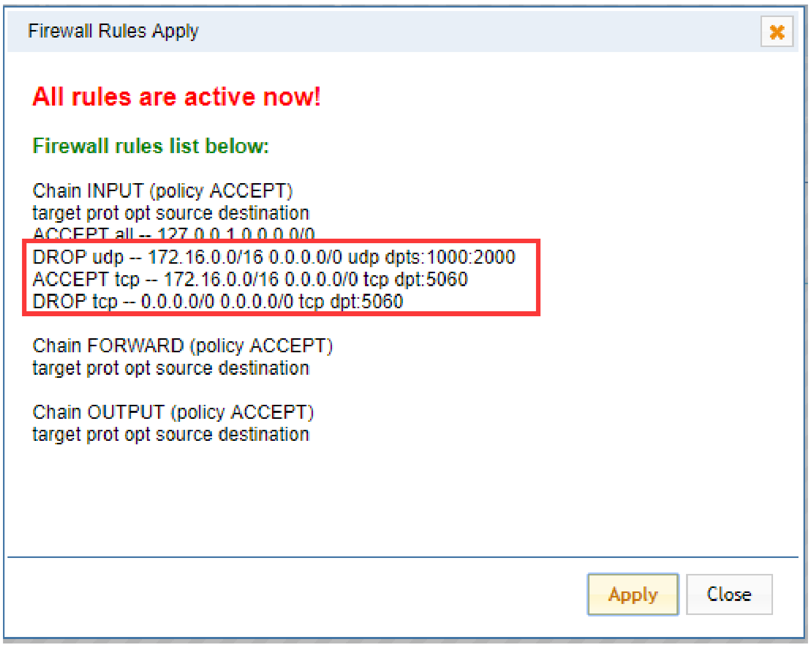
If "List IP Settings" has no problem, you will see popup window like below. Please read the warning and tips carefully. And Click "Apply" button in 1 minute. If time runs out, this window will close automatically.

Figure 7-12 Security Rules Apply



If you see windows like below. It means your configuration has been applied successfully.

Figure 7-13 Security Rules Apply



7.8 SIP Capture

You can capture the SIP packets on the page to facilitate locationg problems.

Figure 7-14 SIP Capture

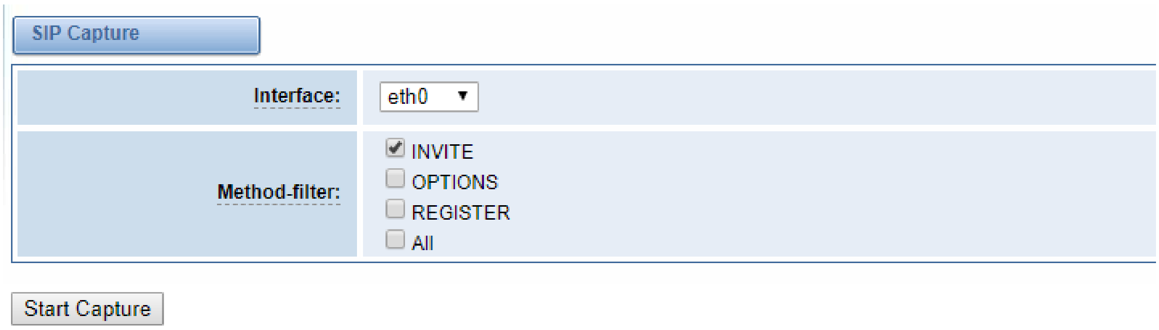


Table 7-7 SIP Capture Settings

Options	Definition
Inferface	You can choose eth0 or eth1
Method-filter	You can choose INVITE, OPTIONS and REGISTER

8. Advances

8.1 Asterisk API

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

Figure 8-1 Asterisk API

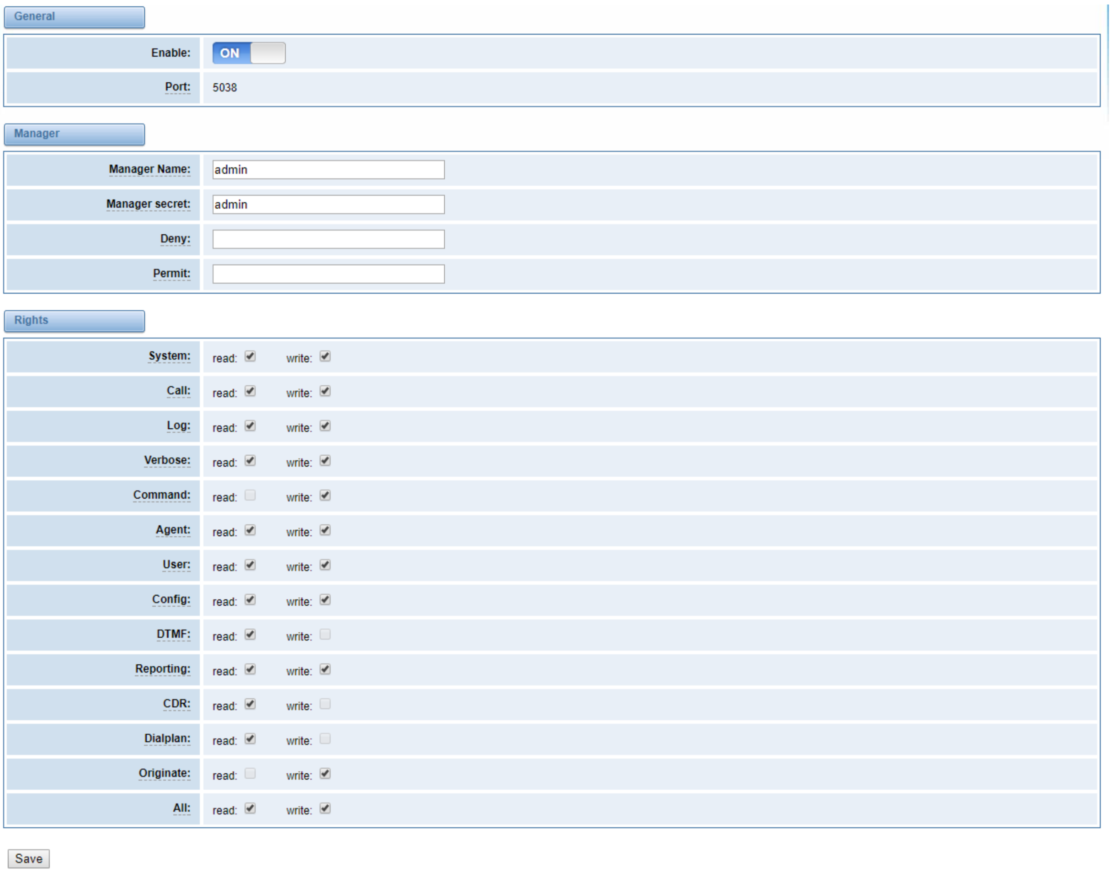


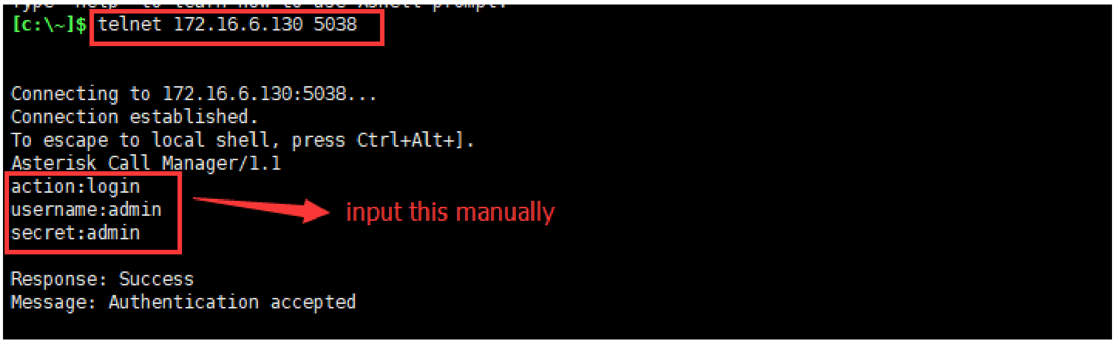
Table 8-1 Definition of Asterisk API

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.
CDR	Call records. Read-only.
Dialplan	Receive NewExten and Varset events. Read-only.
Originate	Permission to originate new calls. Write-only.
All	Select all or deselect all.

Once you set like the above figure, the host 172.16.100.110/255.255.0.0 is allowed to access the gateway API. Please refer to the following figure to access the gateway API by telnet. 172.16.179.1 is the gateway's IP, and 5038 is its API port.

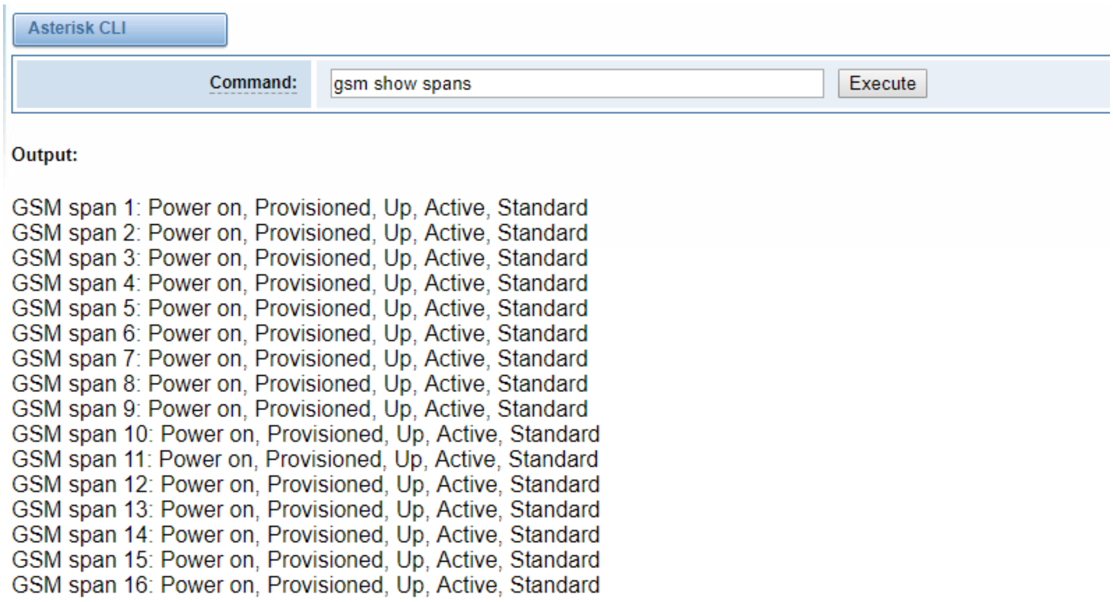
Figure 8-2 Telnet Access Gateway API



8.2 Asterisk CLI

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

Figure 8-3 Asterisk CLI



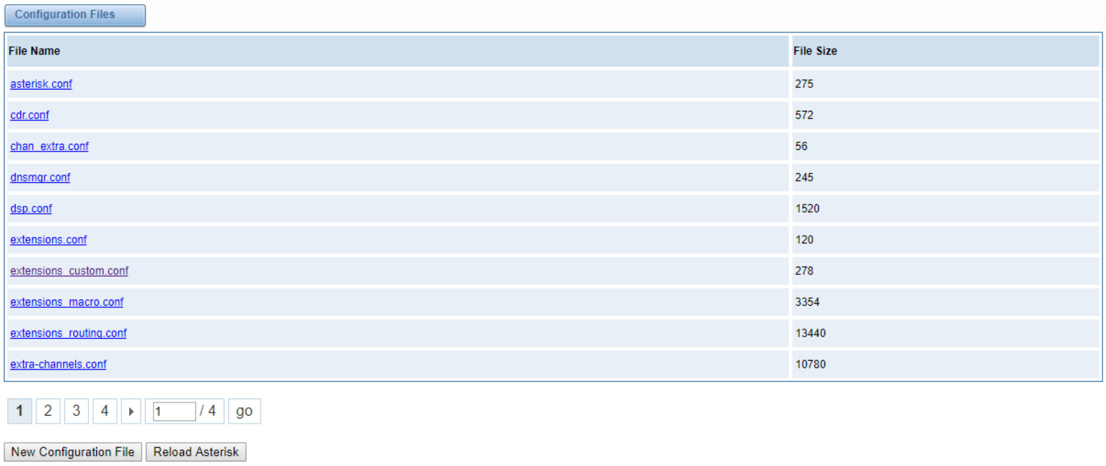
Command: Type your Asterisk CLI commands here to check or debug your gateway.

Notice: If you type “help” or “?” and execute it, the page will show you the executable commands.

8.3 Asterisk File Editor

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

Figure 8-4 Asterisk File Editor



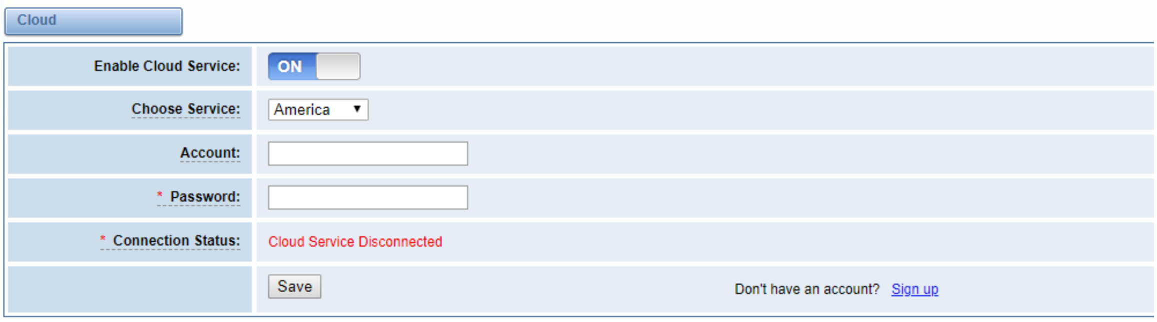
File Name	File Size
asterisk.conf	275
cdr.conf	572
chan_extra.conf	56
dnsmgr.conf	245
dsp.conf	1520
extensions.conf	120
extensions_custom.conf	278
extensions_macro.conf	3354
extensions_routing.conf	13440
extra-channels.conf	10780

Click "New Configuration File" to create a new configuration file. After editing or creating, please reload Asterisk.

8.3 Cloud Management

SWG-2016/32 series gateways support OpenVox Cloud Management.

Figure 8-5 Cloud Management



If your device is connected to the cloud management, the SSH and web pages of the gateway can be accessed through the cloud management, and it can be monitored whether the device is connected to the cloud management platform.On the cloud management platform, you can also count your device model, quantity, distribution area, and so on.

Table 8-2 Definition of Cloud Management

Options	Definition
Enable Cloud Service	Turn on/off cloud management
Choose Service	Currently supports two servers, one is China and the other is the United States.
Account	Registered account or email on the cloud management platform
Password	The password of the account registered on the cloud management platform
Connection Status	Is it currently connected to the cloud management platform?

9. Logs

On the “Log Settings” page, you should set the related logs on to scan the responding logs page. For example, set “System Logs” on like the following, then you can turn to “System” page for system logs, otherwise, system logs is unavailable. And the same with other log pages.

Figure 9-1 Log Settings

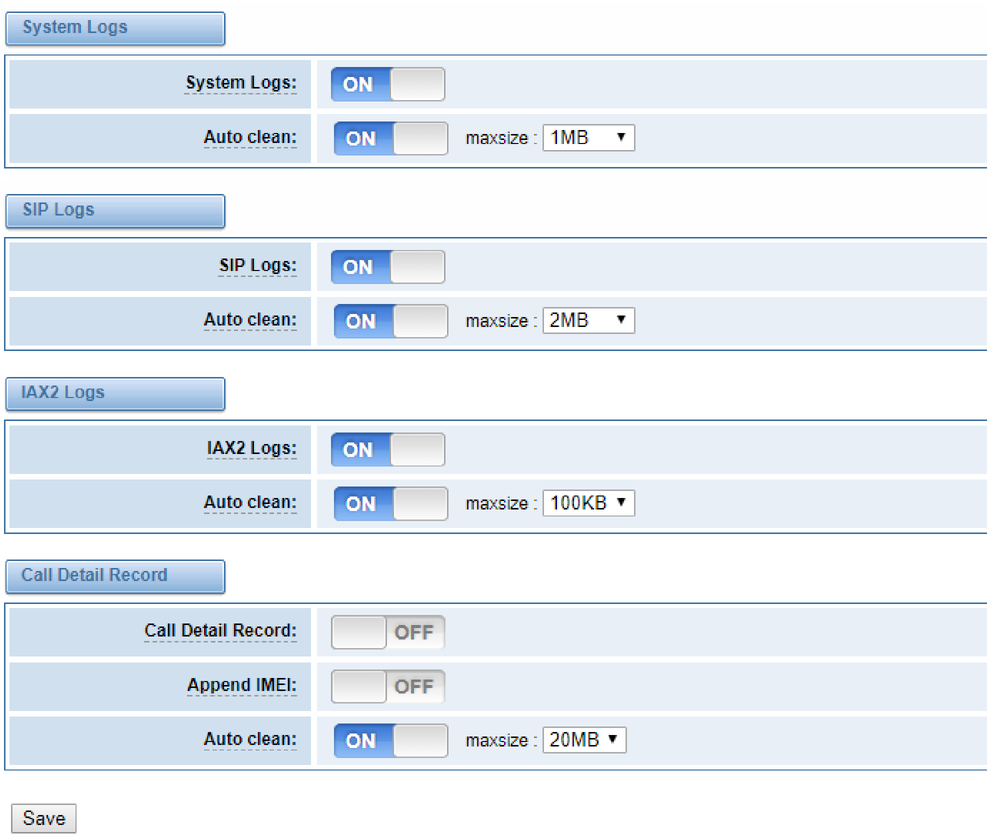
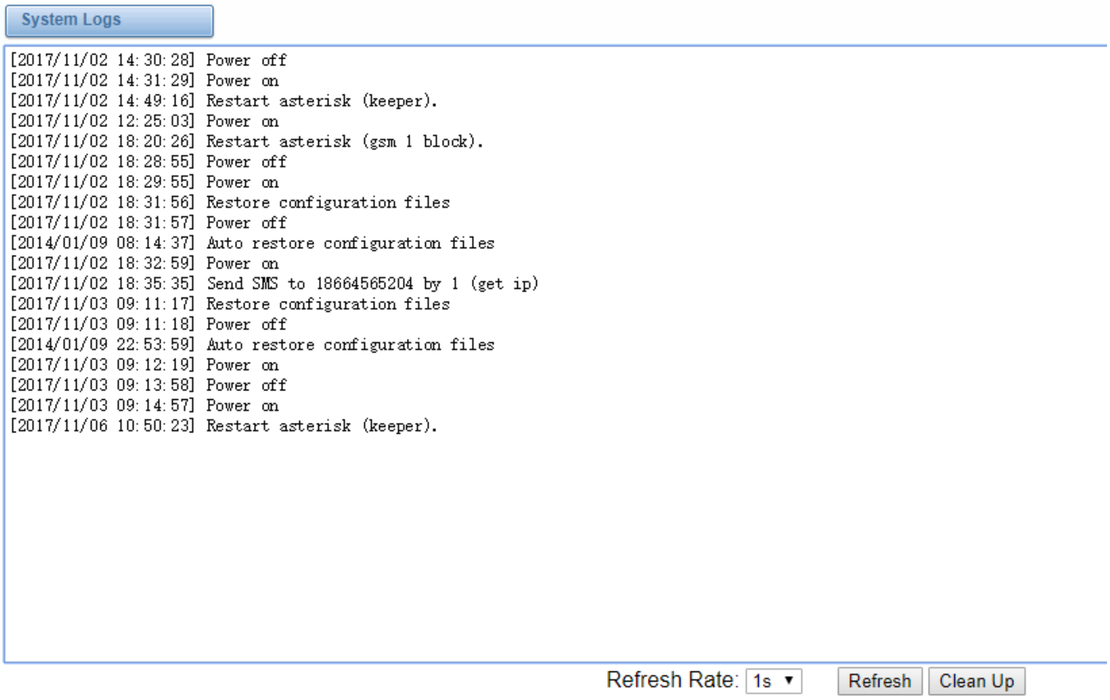
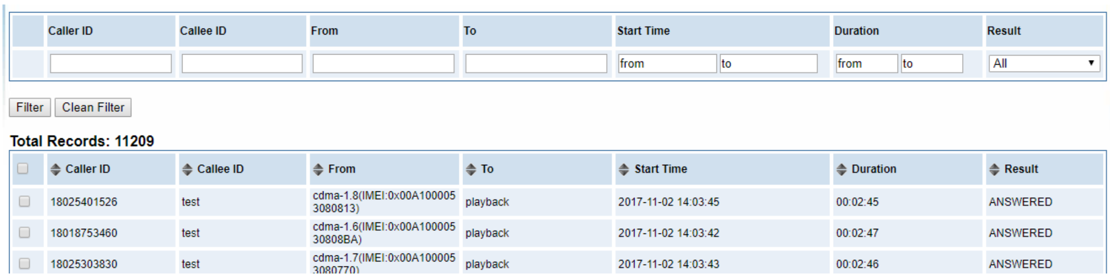


Figure 9-2 System Logs



You can scan your CDR easily on web GUI, and also you can delete, clean up or export your CDR information.

Figure 9-3 CDR Output



	Caller ID	Callee ID	From	To	Start Time	Duration	Result
					from to	from to	All

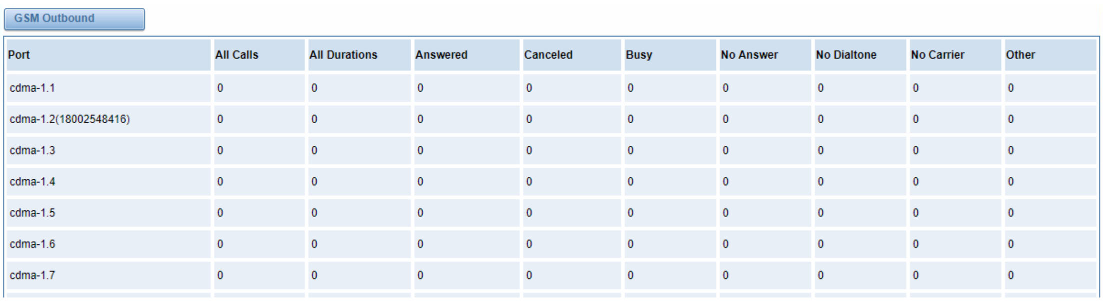
Filter Clean Filter

Total Records: 11209

	Caller ID	Callee ID	From	To	Start Time	Duration	Result
	18025401526	test	cdma-1.8(IMEI:0x00A1000053080813)	playback	2017-11-02 14:03:45	00:02:45	ANSWERED
	18018753460	test	cdma-1.6(IMEI:0x00A10000530808BA)	playback	2017-11-02 14:03:42	00:02:47	ANSWERED
	18025303830	test	cdma-1.7(IMEI:0x00A1000053080770)	playback	2017-11-02 14:03:43	00:02:46	ANSWERED

Recently we have made our LOGS display richer, you can see your Outbound of every port clearly.

Figure 9-4 Outbound



GSM Outbound

Port	All Calls	All Durations	Answered	Canceled	Busy	No Answer	No Dialtone	No Carrier	Other
cdma-1.1	0	0	0	0	0	0	0	0	0
cdma-1.2(18002548416)	0	0	0	0	0	0	0	0	0
cdma-1.3	0	0	0	0	0	0	0	0	0
cdma-1.4	0	0	0	0	0	0	0	0	0
cdma-1.5	0	0	0	0	0	0	0	0	0
cdma-1.6	0	0	0	0	0	0	0	0	0
cdma-1.7	0	0	0	0	0	0	0	0	0

Table9-1 definition of Logs

Options	Definition
System Logs	Whether enable or disable 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, maxsize=1M.
SIP Logs	Whether enable or disable 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, maxsize=100KB.
IAX Logs	Whether enable or disable IAX log.
Auto clean(IAX 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, maxsize=100KB.
Call Detail Record	Displaying Call Detail Records for each channel.
Auto clean (CDR 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=20MB.

Appendix Feature List

General Info

- LAN:1

- WAN:1
- Console:1
- USB Interface:1
- TF Interface:1
- LCD dimension:2.4"
- LCD resolution ratio: 240*400
- SIM Cards: hot-swap
- Temperature: -20~70°C (Storage)   0~40°C (Operation)
- Operation humidity: 10% ~ 90%non-condensing

VOIP Characters

- Support SIP, IAX2 Protocol
- Add, Modify & Delete SIP/IAX2 Trunk
- SIP/IAX2 Registration with Domain
- Combine Different SIP/IAX2 Trunk into Group
- DTMF Mode: RFC2833/Inband/SIPInfo
- SIP V2.0 RFC3261 Compliance
- Multiple SIP/IAX2 Registrations modes:

  None (No registration, just IP and Password authenication)

  Endpoint registers with this gateway (work as a SIP Sever)

  This gateway registers with the endpoint (work as a SIP/IAX2 client)

Network

- IPv4，UDP/TCP，DHCP，TELNET，HTTP/HTTPS，TFTP
- PPTP VPN

- HTTP/SSH（Optical Telnet）
- Ping & Traceroute Command on the Web
- Simple Security Strategy: white list, black list, security rules

System Features

- Combine Different SIP/IAX2 Trunk into Group
- CLID Display & Hide (Need operators' support)
- Random call interval
- Call Duration Limitation
- Single Call Duration Limitation
- Real Open API Protocol (based on Asterisk)
- Support DISA
- SMSC/SMS/USSD
- PIN Identification
- Optional Voice Codec
- Ports Group Management
- SMS Bulk Transceiver, Sent to Email and Automatically Resend
- SMS Coding/Detecting Automatically Identification
- SMS Remotely Controlling Gateway
- SMS Forwarding and Quick Reply
- USSD transceiver
- Outbound
- Automatically Reboot
- Support MMP
- Support for custom scripts, dialplans
- Support Openvox cloud manage

Management

- Simple and convenient configuration via Web GUI
- Support maintenance and configuration by SSH
- Support configuration files backup and upload
- Support Chinese and English page
- Firmware Update by HTTP
- Support Web and SSH login password modification
- Restore Factory Settings
- CDR(More than 200,000 Lines CDRs Storage Locally)
- System log
- SIP/IAX2 log
- TCP and SIP capture