



OpenVox Communication Co Ltd



SWG-M20X Series Wireless Gateways 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!

Copyright

Copyright© 2020 OpenVox Inc. All rights reserved. No part of this document may be reproduced without prior written permission.

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.

Statement

This document applies to all SWG-M20X series gateways, including GSM/WCDMA/LTE. Different types of gateways may have functional differences. For details, please contact OpenVox sales or technical support.

Trademarks

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

Revision History

Version	Date	Detail
1.0	2019/10/15	Initial

Contents

1. Overview	4
1.1 What is SWG-M20X Series Wireless Gateways?	4
1.2 Product Introduction	4
1.3 Main Features	5
1.4 Physical Information	7
1.5 Software	7
2. System	9
2.1 Status	9
2.2 Time	11
2.3 Login Settings	12
2.4 General	13
2.5 Tools and Information	14
2.6 Setting Wizard	17
3. Module	18
3.1 Module Settings	18
3.2 Call Forwarding	23
3.3 Call Waiting	24
3.4 Simbank	25
3.5 DTMF	26
3.6 BCCH	27
3.7 Toolkit	28
3.8 Module Update	29
3.9 Call and SMS Limit	30
4. VOIP	36
4.1 VOIP Endpoints	36
4.1.1 Add New SIP Endpoint	36

4.1.2 Add New IAX2 Endpoint.....	44
4.2 Batch SIP Endpoints	49
4.3 Advanced SIP Settings	51
4.4 Advanced IAX2 Settings	59
4.5 SIP Account Security	65
5. Routing	67
5.1 Call Routing Rules.....	67
5.2 Groups.....	71
5.3 Batch Creating rules	71
5.4 MNP Settings.....	73
5.5 Routing Blacklist	73
6. SMS	74
6.1 General.....	74
6.2 SMS Sender	80
6.3 SMS Inbox.....	80
6.4 SMS Outbox.....	81
6.5 SMS Forwarding	82
7. Network.....	83
7.1 LAN Settings	83
7.2 WAN Settings	84
7.3 VPN Settings.....	85
7.4 DDNS Settings	85
7.5 Toolkit.....	86
7.6 Firewall Settings	87
7.7 Security Rules.....	88
7.8 SIP Capture.....	89
8. Advances	90
8.1 Asterisk API	90

8.2 Asterisk CLI	92
8.3 Asterisk File Editor.....	93
8.4 Internet	93
8.5 Cloud Management	94
8.6 Balance.....	95
8.7 Phone Number	96
9. Logs	97

1. Overview

1.1 What is SWG-M20X Series Wireless Gateways?

OpenVox SWG-20X series wireless gateways include SWG-202 G/W/L and SWG-204 G/W/L. They can bring you excellent HD voice service with multiple codecs, including G.711U, G.711A, GSM, G.722, G.726, G.729, and also flexible SMS service with multiple SMS API. The SWG-20X 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-20X 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
SWG-202G	GSM	2	2	GSM:850/900/1800/1900MHz
SWG-204G		4		
SWG-202W	WCDMA	2		Europe UMTS: 900/2100MHz GSM: 900/1800MHz
SWG-204W		4		America UMTS: 850/1900MHz GSM: 850/900/1800/1900MHz

				Thailand UMTS: 850/2100MHz GSM: 850/900/1800/1900MHz
SWG-202L	LTE	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
SWG-204L		4		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 Australia/New Zealand/Taiwan/Brazil LTE FDD: B1/B2/B3/B4/B5/B7/B8/B28 LTE TDD: B40 WCDMA: B1/B2/B5/B8 GSM: B2/B3/B5/B8

1.3 Main Features

VoIP Characters

- Support SIP, IAX2 Protocol
- Add, Modify & Delete SIP/IAX2 Trunk
- SIP/IAX2 Registration with Domain

- SIP V2.0 RFC3261 Compliance
- DTMF Mode: RFC2833/Inband/SIP Info
- Multiple SIP/IAX2 Registrations modes
- Abundant Codecs: G.711A, G.711U, G.729, G.722, G.726, GSM

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

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

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 Remotely Controlling Gateway
- SMS Bulk Transceiver, Sent to Email and Automatically Resend
- SMS Coding/Detecting Automatically Identification
- SMS Forwarding and Quick Reply
- USSD transceiver
- Outbound
- Automatically Reboot
- Support MMP
- Support for custom scripts, dial plans
- Support OpenVox cloud manage

1.4 Physical Information

- LAN port:1
- WAN port: 1
- SIM Cards: hot-swap
- Operation Temperature: 0~40°C
- Operation humidity:10% ~ 90% non-condensing
- Storage Temperature: -20~70°C

1.5 Software

LAN:

- Default IP: 172.16.98.1
- Username: admin
- Password: admin

For the first time, you can access SWG-20X by using default IP 172.16.98.1; if you use the default login name and password, you will be prompted to change the password each time you log in. If you have modified it, you will not be prompted.

If you use WAN to connect the device, the WAN port uses DHCP by default. Please use the display to view the IP address assigned by the WAN to access the device. Use the default login name and password—admin/admin to log in to the device.

2. System

2.1 Status

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

Figure 2-1-1 System Status

Module Information											
Port	Type	Signal	Band	BER	Carrier	Registration Status	PDD(s)	ACD(s)	ASR(%)	Module Status	Remain Time
1.1	GSM			-1		Undetected SIM Card	0	0	0		No Limit
1.2	GSM			-1		Undetected SIM Card	0	0	0		No Limit
1.3	GSM			-1		Undetected SIM Card	0	0	0		No Limit
1.4	GSM			-1		Undetected SIM Card	0	0	0		No Limit
2.5	LTE			-1		Not registered	0	0	0	INIT	No Limit
2.6	LTE			-1		Undetected SIM Card	0	0	0		No Limit
2.7	LTE			-1		Undetected SIM Card	0	0	0		No Limit
2.8	LTE			-1		Undetected SIM Card	0	0	0		No Limit

SIP Information				
Endpoint Name	User Name	Host	Registration	SIP Status
10028	anonymous	172.16.208.33	none	Unmonitored
2111	test	(Unspecified)	server	UNKNOWN

IAX2 Information				
Endpoint Name	User Name	Host	Registration	IAX2 Status
2133	2133	172.16.208.33	client	UNREACHABLE

Routing Information				
Rule Name	From	To	Rules	
incoming	grp-all	iax-2133		
gsm-1.12sip	gsm-1.1	sip-10028		
sip2gsm-1.1	sip-10028	gsm-1.1	Dial_pattern (+)[/101]	
sip2lte-2.5	sip-10028	lte-2.5	Dial_pattern (+)[/200]	
outgoing	sip-2111	gsm-1.2		
test	sip-10028	lte-2.6	Dial_pattern (+1)[/]	

Network Information						
Name	MAC Address	IP Address	Mask	Gateway	RX Packets	TX Packets
LAN	A0:98:05:0A:2D:F7	172.16.6.108	255.255.0.0	172.16.0.1	1646	147

Table 2-1-1 Description of System Status

Option	Definition
Port	Number of each ports. GSM port starts with "gsm-", Such as: gsm-1.1;4G port starts with "lte-", Such as: lte-2.5.
Signal	Display the signal strength of each channels of gateway.

Band	GSM/ LTE
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 the time from the point at which the final dialed digit is sent until they hear a ringtone or other in-band message. In the case where the originating network needs to play a notification before the call is completed, the definition of the PDD excludes the duration of such notification.
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 attempted calls. Since busy signals and other rejections by the called number count as call failures, the ASR value can depend on user behavior.
Module Status	Display the status of the port. "A space" means the port is unavailable. "INIT" means registering and "READY" means the port is available.
Remain Time	Multiply this value by the step size as the limit call time.

2.2 Time

Table 2-2-1 Definition 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].
Automatic Sync from NTP	Whether to enable automatic sync time from NTP. On (enable), OFF (disable).
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 Setting

Time Settings	
System Time:	2019-4-1 12:25:55
Time Zone:	Chongqing ▼
POSIX TZ String:	CST-8
NTP Server 1:	pool.ntp.org
NTP Server 2:	64.236.96.53
NTP Server 3:	ntp1.aliyun.com
Auto-Sync from NTP:	☒ ON
Save Data Sync from NTP Sync from Client	

You can synchronize the gateway time in different ways: Sync from NTP or Sync from Client by pressing different buttons.

2.3 Login Settings

The new gateway has no administration privileges, all you can do is reset a username and password to manage your gateway. The username and password have all the permissions to operate the gateway. 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 username 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 2-3-1 Definition of Login Settings

Options	Definition
User Name	Define your username to manage your gateway. Allowed characters "-_+. < > & 0-9a-zA-Z". Length: 1-32 characters.
Password	Define your password to manage your gateway Allowed

	characters "-_+. < > & 0-9a-zA-Z". Length: 1-32 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.

Figure 2-3-1 Login Settings

Web Login Settings

User Name:

admin123

Password:

Confirm Password:

Login Mode:

http and https ▾

http and https

only https

Port:

SSH Login Settings

Enable:

ON

User Name:

super

Password:

super

Port:

12345

2.4 General

You can choose different languages for your system. If you want to change the 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 2-4-1 Language Settings

Language Settings	
Language:	English ▼
Advanced:	☒ ON
Language Debug:	☒ TURN ON ☐ TURN OFF
Download:	Download selected language package. Download
Delete:	Delete selected language. Delete
Add New Language:	New language Package: 选择文件 未选择任何文件 Add

If you 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 or By Running Time.

Figure 2-4-2 Reboot Type

Scheduled Reboot	
Enable:	☐ OFF
Reboot Type:	By Running Time ▼
Running Time:	Hour: 0 ▼

You can set this enable if you use your system frequently, it can help your system work more efficiently.

2.5 Tools and Information

Reboot Tools

You can choose system reboot or asterisk reboot separately. The new version of the gateway retains two file systems. Clicking "System Switch" will reboot the system and switch to another file system.

Figure 2-5-1 Reboot Tools

WirelessGateway SWG-2008		SYSTEM 来自 172.16.6.108		WORK ADVANCED LOGS	
		Are you sure to reboot your gateway now? You will lose all data in memory!		确定 取消	
SYSTEM DETAILS		Free Communication			
Reboot Tools		OpenVox Solution			
Reboot the gateway and all the current calls will be dropped.		System Reboot			
Reboot the asterisk and all the current calls will be dropped.		Asterisk Reboot			
Reboot the gateway and all the current calls will be dropped.		System Switch			

If you press "OK", the system will restart and the current call will be hung up. The same as the Asterisk Reboot.

Update Firmware

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

Figure 2-5-2 Update Firmware

Update Firmware	
New system file:	选择文件 未选择任何文件
System Update	
New system file is downloaded from official website and update system.	
System Online Update	

Upload and Backup Configuration

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

Figure 2-5-3 Upload and Backup Configuration

Upload Configuration	
New configuration file:	选择文件 未选择任何文件
File Upload	
Backup Configuration	
Current configuration file version: 2.1.0	
Download Backup	

Voice Record

Select a module to record the voice, the maximum duration of the recording is 3 minutes. When the recording time exceeds 3 minutes, the recording file will be automatically downloaded.

Figure 2-5-4 Voice Record

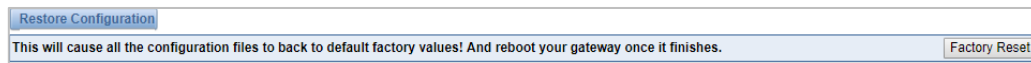
Voice Record	
Select a module to recode voice.	gsm-1.1 ▼
Start Recording	

Restore Configuration

Sometimes there is something wrong with your gateway that you don't know how to solve it. Mostly you can select factory reset, you just need to press a button and your

gateway will be reset to the factory status.

Figure 2-5-5 Restore Configuration



System 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 other useful information.

Figure 2-5-6 System Information

Product Name:	SWG-2008
GSM Model Description:	GSM: 850/900/1800/1900MHz
LTE Model Description:	LTE FDD: B1/B3/B5/B8 LTE TDD: B38/B39/B40/B41 TD-SCDMA: B34/B39 CDMA: BC0 WCDMA: 900/2100MHz GSM: 900/1800MHz
Software Version:	2.1.0
Hardware Version:	1.0
Slot Number:	1
Storage Usage:	40.5M/487.9M (9%)
Memory Usage:	21.3297 % Memory Clean
Build Time:	2019-03-06 17:19:31
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:	615
System Time:	2019-4-1 14:17:38
System Uptime:	0 days 00:02:20

2.6 Setting Wizard

According to the boot, you can change the password, set the time, network, and create SIP terminals and routes quickly.

Figure 2-6-1 Setting Wizard

The screenshot displays the 'Setup Wizard' window. At the top, a progress bar shows six steps: 1. Change Password (active), 2. Select Time Zone, 3. Network Settings, 4. SIP Endpoints, 5. Destination, and 6. Summary. The main content area is titled 'Change Password' and contains three input fields: 'New Username:', 'New Password:', and 'Confirm Password:'. Below these fields, a list of password rules is provided: 'The password must meet the following rules: 1. At least eight characters. 2. At least one number. 3. At least one lowercase letter. 4. At least one uppercase letter.' At the bottom of the window, there are two buttons: 'Next' (highlighted in blue) and 'Quit'.

3. Module

You can see the information of SIM card on this page.

3.1 Module Settings

Figure 3-1-1 Module Settings

Port	Type	Carrier	Registration Status	Module Status	Actions
1.1	GSM		Undetected SIM Card		 
1.2	GSM		Undetected SIM Card		 
1.3	GSM		Undetected SIM Card		 
1.4	GSM		Undetected SIM Card		 
2.5	LTE		Not registered	INIT	 
2.6	LTE		Undetected SIM Card		 
2.7	LTE		Undetected SIM Card		 
2.8	LTE		Undetected SIM Card		 

On this page, you can see the information of the module status, click the  button to configure the port.

Figure 3-1-2 Port Configuration

Port gsm-1.1

Name:	
Speaker Volume:	50
Microphone Volume:	8
Dial Prefix:	
Pin Code:	☐ On
Custom AT commands when start:	
STK flag:	☐ OFF
CLIR:	☐ OFF
SMS Center Number:	Modify
Band:	All Band(850/900/1800/1900MHz) ▼
SIM IMSI:	
Module IMEI:	Modify
Module Revision:	
Carrier:	
Bind Carrier:	Auto ▼ List Carrier
Signal:	-1
BER:	-1
Status:	
GSM Voice Codec:	ERROR ▼
CLCC:	☒ ON
AT Timeout:	10 s

▶ Save To Other Ports

You can choose different bands in the options.

Figure 3-1-3 Band binding

Band:	All Band(850/900/1800/1900MHz) ▼
SIM IMSI:	All Band(850/900/1800/1900MHz)
Module IMEI:	EGSM(850/900MHz)
Module Revision:	DCS(1800MHz)
	PCS(1900MHz)
	EGSM DCS(850/900/1800MHz)
	GSM850 PCS(850/1900MHz)

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

Figure 3-1-4 PIN Code Application

Pin Code:	123456	☒ On
-----------	--------	--

Then enter the password and the system will recognize the number of the SIM card. It can help you prevent the SIM card from being stolen and increase the safety factor. 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 3-1-5 CLIR Application

CLIR:	☒ ON
-------	--

OpenVox GSM/3G Gateway supports optional GSM voice codec. For more details, you can see the picture below:

Figure 3-1-6 GSM Voice Codec

Band:	auto	MHz ▼
SIM IMSI:	FR	
Module IMEI:	HR	
Module Revision:	EFR	
Carrier:	AMR_FR	
Bind Carrier:	AMR_HR	
Signal:	FR&EFR, FR	
BER:	EFR&FR, EFR	
Status:	EFR&HR, EFR	
GSM Voice Codec:	EFR&AMR_FR, EFR	
	AMR_FR&FR, AMR_FR	
	AMR_FR&HR, AMR_FR	
	AMR_FR&EFR, AMR_FR	
	AMR_HR&FR, AMR_HR	
	AMR_HR&HR, AMR_HR	
	AMR_HR&EFR, AMR_HR	

IMEI Modification

We also provide IMEI automatically modified performance.

Figure 3-1-7 Automatic IMEI modification

Module IMEI:	352840039592814	Modify
--------------	-----------------	--------

If you want to modify the IMEI number, log in to the gateway to modify the IP address as follows. Input <http://gatewayIP/cgi-bin/php/gsm-autoimei.php> in your browser. Then log in to the web page and you will see the setting as “Enable” as “ON” as shown below. Otherwise, the IMEI number cannot be modified.

Figure 3-1-8 IMEI Modification

▼ Automatic Change IMEI	
Port:	☒ lte-1.1 ☒ lte-1.2 ☒ lte-1.3 ☒ lte-1.4 ☒ gsm-2.5 ☒ gsm-2.6 ☒ gsm-2.7 ☒ gsm-2.8 ☒ All
Enable:	☒ ON
Interval:	1800 Second
Immediately:	☒ modify IMEI immediately
Force:	☒ Modify IMEI no matter whether the channel state is ready or not.
▶ Auto-IMEI Advanced	

You can choose to modify one , more ports or all ports, and you can set the automatic modification interval by filling in the required time.

Figure 3-1-9 Time Interval

Interval:	1800	Second
-----------	------	--------

If you select "Modify IMEI now", the changes will take effect immediately. If you select "Force", the system will hang up the current call and modify the IMEI.

Click the button **▼ Auto-IMEI Advanced** to set it. There are two ways to modify the IMEI: manual modification or automatic generation.

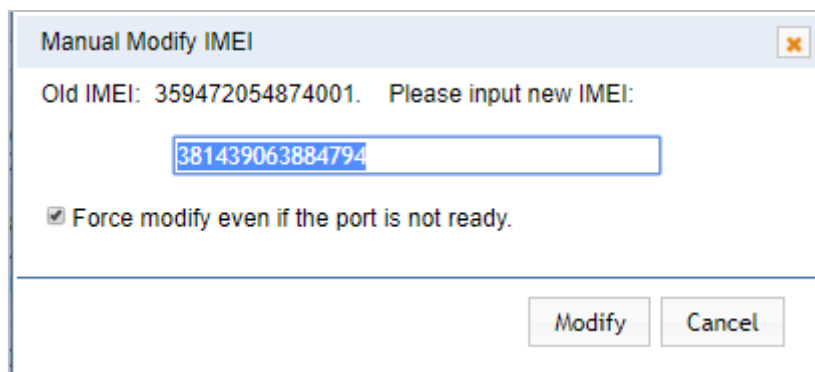
Figure 3-1-10 Advanced Setting

▼ Auto-IMEI Advanced							
IMEI Number Setting	TAC(6 digit)	FAC(2 digit)	SNR(6 digit)	SP(1 digit)		Current IMEI	Action
Set to All				Autogeneration		None	Set to All
gsm-1.1	35xxxx	0x	xxxxxx	Autogeneration		352840039592814	Manual
gsm-1.2	35xxxx	0x	xxxxxx	Autogeneration		352794018702565	Manual
gsm-1.3	35xxxx	0x	xxxxxx	Autogeneration		357720013455078	Manual
gsm-1.4	35xxxx	0x	xxxxxx	Autogeneration		358415039164809	Manual
lte-2.5	35xxxx	0x	xxxxxx	Autogeneration			Manual
lte-2.6	35xxxx	0x	xxxxxx	Autogeneration		359472054874001	Manual
lte-2.7	35xxxx	0x	xxxxxx	Autogeneration		352018070983487	Manual
lte-2.8	35xxxx	0x	xxxxxx	Autogeneration		867732033402132	Manual

As you can see, each port is set to any number. "X" means any number from 0-9. All you have to do is fill in all the lines and click "Set All". Click "Save", the current IMEI will change, this is automatically generated.

If you want to set the IMEI to a specific value, click on "Modify" and enter a new IMEI as required.

Figure 3-1-11 Manually set IMEI



After the configuration is completed, click "Back Home" to return to the gateway interface.

Table 3-1-1 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 range of the speaker volume level is 0-100. This will adjust the loud speaker volume level by an AT command.
Microphone Volume	The range of the microphone volume is: 0-15. This will change the microphone volume level by an AT command
Dial Prefix	The number prefix of the outbound call through the GSM channel.

PIN Code	Personal identification numbers of SIM card. PIN code can be modified to prevent SIM card from being stolen.
Custom AT commands when start	Use “ ” to split AT command when user use custom AT commands to start system.
CLIR	Caller ID restriction, this function is used to hide the caller ID of the SIM card number. The gateway will add ‘#31#’ in front of the mobile number. This function must be operated by a professional operator.
SMS Center Number	Your SMS center number of your local carrier.
Module IMEI	Press the Modify button to automatically modify.

Save settings to other ports:

Figure 3-1-12 Save to port

Save To Other Ports				
Save To Other Ports:	☐ gsm-1.1	☐ gsm-1.2	☐ gsm-1.3	☐ gsm-1.4
	☐ All			
Sync All Settings:	☒ Select all settings			

Your call status will be displayed on the main screen.

Figure 3-1-13 Module Information

Port	Type	Signal	Band	BER	Carrier
1.1	GSM			-1	
Model IMEI: 352840039592814 Network Name: Network Status: Undetected SIM Card Signal Quality (0,31): -1 BER value (0,7): -1 SIM IMSI: SIM SMS Center Number: Own Number: Phone Number: Remain Time: No Limit PDD(s): 0 ACD(s): 0 ASR(%): 0 State:				-1	
				-1	
				-1	
				-1	
				-1	
				-1	
				-1	
				-1	

3.2 Call Forwarding

Sometimes it's not convenient for you to answer the call. If you don't want to lose some important calls, you can choose call forwarding. There are different kinds of call types for you to choose, Such as call forwarding unconditional, call forwarding no reply, call forwarding busy and call forward on not reachable. If you want to cancel the call forwarding settings, you can choose to cancel all.

Figure 3-2-1 Call Forwarding

☐	Port	Select	Call Type	Call Number	Status	
☐	gsm-1.1	☐	Call Forwarding Unconditional			
		☐	☐	Call Forwarding No Reply		
			☐	Call Forwarding Busy		
			☐	Call Forward on Not Reachable		
			☐	Cancel All		
☐	gsm-1.2	☐	Call Forwarding Unconditional			
		☐	☐	Call Forwarding No Reply		
			☐	Call Forwarding Busy		
			☐	Call Forward on Not Reachable		
			☐	Cancel All		
☐	gsm-1.3	☒	Call Forwarding Unconditional			
		☐	☐	Call Forwarding No Reply		
			☐	Call Forwarding Busy		
			☐	Call Forward on Not Reachable		
			☐	Cancel All		
☐	gsm-1.4	☐	Call Forwarding Unconditional			
		☐	☐	Call Forwarding No Reply		
			☐	Call Forwarding Busy		
			☐	Call Forward on Not Reachable		
			☐	Cancel All		
☐	lte-2.5	☐	Call Forwarding Unconditional			
		☐	☐	Call Forwarding No Reply		
			☐	Call Forwarding Busy		
			☐	Call Forward on Not Reachable		
			☐	Cancel All		

3.3 Call Waiting

You can switch the Call Waiting Function of the SIM card on/off in the port on this page.

Figure 3-3-1 Call Waiting

☐	Port	☐ ON ☐ OFF (Call Waiting Function)	Status
☐	gsm-1.1	☐ ON ☐ OFF	
☐	gsm-1.2	☐ ON ☐ OFF	
☐	gsm-1.3	☐ ON ☐ OFF	
☐	gsm-1.4	☐ ON ☐ OFF	
☐	lte-2.5	☐ ON ☐ OFF	
☐	lte-2.6	☐ ON ☐ OFF	
☐	lte-2.7	☐ ON ☐ OFF	
☐	lte-2.8	☐ ON ☐ OFF	

Table 3-3-1 Definition of Call Waiting

Options	Definition
Switch on call waiting	Choose the port you want to set, switch to "On" and

	click the "Settings" button.
Switch off call waiting	Choose the port you want to set, switch to "Off" and click the "Settings" button.
Status	It will display the results of your execution.
Settings	Used to switch the call waiting function on or off.
Query	Used to query the status of call waiting, observe whether the port that sets the call waiting is open or closed.

3.4 Simbank

If you want to use the SWG series wireless gateway with Simbank, go to the MODULE -> Simbank interface and set the parameters of the gateway. As shown in the figure, the Simemusvr Switch is opened and the Serial Number is automatically generated for registration of the gateway on the Simbank. Select Normal in the Network Mode, and click "Save" to save the running parameters.

Figure 3-4-1 Simbank Options

The screenshot shows a web-based configuration page titled 'Simbank Options'. It contains four main configuration rows: 'Simemusvr Switch' with a toggle set to 'ON', 'Serial Number' with a text field containing '4BGDMAMV', 'Net Mode' with a dropdown menu set to 'Normal', and 'Simbank Server IP' with a text field containing '172.16.6.103'. A 'Save' button is located at the bottom left of the form.

Table 3-4-1 Definition of Simbank Options

Options	Definition
Simemusvr Switch	The switch of using remote SIM card, you cannot use local card after opening.

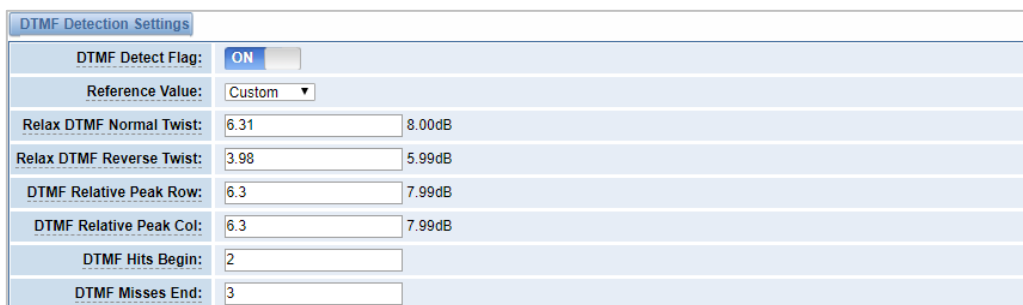
Serial Number	Serial number, unique.
Net Mode	Network mode, Normal for local connection, OPlink for external network.
Simbank Server IP	Simbank IP.

After the above settings are completed, the gateway is successfully registered, and Simbank will assign the SIM card to it remotely.

3.5 DTMF

You can do some DTMF Detection Settings if you choose “MODULE → DTMF”.

Figure 3-5-1 DTMF Detection Settings



DTMF Detection Settings		
DTMF Detect Flag:	ON	
Reference Value:	Custom ▼	
Relax DTMF Normal Twist:	6.31	8.00dB
Relax DTMF Reverse Twist:	3.98	5.99dB
DTMF Relative Peak Row:	6.3	7.99dB
DTMF Relative Peak Col:	6.3	7.99dB
DTMF Hits Begin:	2	
DTMF Misses End:	3	

Notice: You don't have to modify these settings if you don't have special need. You can just choose “Default”.

Table 3-5-1 Definition of DTMF Detection Settings

Options	Definition
DTMF Normal Twist and Reverse Twist	It is the power difference between the row and the 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 smaller the value, the easier the detection. 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 smaller the value, the easier the detection. 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	Simple match value, choose 2 or 3.
DTMF Misses End	The time interval between the two numbers you entered. Adjust the speed of input. The smaller value represents the shorter intervals.

3.6 BCCH

Figure 3-6-1 BCCH Settings

		0			1			2			3			4			5			6				
Port	Mode	LAC	BCCH	dbm	LAC	BCCH	dbm	LAC	BCCH	dbm	LAC	BCCH	dbm	LAC	BCCH	dbm	LAC	BCCH	dbm	LAC	BCCH	dbm	Status	Detail
gsm-1.1	default																							Detail
gsm-1.2	default																							Detail
gsm-1.3	default																							Detail
gsm-1.4	default																							Detail

Get Current State Search Cell

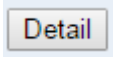
The BCCH mode can be changed by clicking the  button.

Figure 3-6-2 BCCH Mode

gsm-1.1
Port: gsm-1.1
BCCH Mode: Default
Apply To All Ports:

Index	MCC	MNC	LAC	CID	BCCH	Receive Level	Lock

Get Current State Search Cell Save Apply Cancel

3.7 Toolkit

You can get USSD information, send AT command or check the number of this module. The AT command is very helpful for you when debugging a module.

Figure 3-7-1 Function Options

The screenshot shows a web-based interface for the OpenVox Toolkit. At the top, there is a 'Function:' dropdown menu with 'Get USSD' selected. Below it, an 'Action:' dropdown menu also has 'Get USSD' selected. To the right of these dropdowns are three buttons: 'Copy to Selected', 'Clear All', and 'Execute'. Below the action menu is a table with three columns: 'Port', 'Input', and 'Output'. The 'Port' column lists eight ports: gsm-1.1, gsm-1.2, gsm-1.3, gsm-1.4, lte-2.5, lte-2.6, lte-2.7, and lte-2.8. Each port has a corresponding empty input field and an empty output field.

Table 3-7-1 Description of Definition of Functions

Options	Definition
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. It is useful when you have a debug of the modem. For example, perform [AT+CSQ] to check what signal qualify it is. In AT commands, there is no difference between "a" and "A" (case insensitive).
Check Number	Enter a known number (like your mobile phone number) 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.
--	---

If you want to send an AT command, enter the command, select a port first and then select "Copy to selected", and finally click "Execute".

Figure 3-7-2 AT Command Example

Function: Send AT Command ▼		
Action: AT+CSQ Copy to Selected Clear All Execute		
☐ Port	Input	Output
☒ gsm-1.1	AT+CSQ	
☒ gsm-1.2	AT+CSQ	
☐ gsm-1.3		
☐ gsm-1.4		
☐ lte-2.5		
☐ lte-2.6		
☐ lte-2.7		
☐ lte-2.8		

3.8 Module Update

You can update the module version or update the microcontroller by yourself on this page.

Figure 3-8-1 Module Update

Module Update			
Port:	☐ gsm-1.1 ☐ gsm-1.2 ☐ gsm-1.3 ☐ gsm-1.4		
	☐ lte-2.5 ☐ lte-2.6 ☐ lte-2.7 ☐ lte-2.8		
	☐ All ☐ Show All		
Module Update file:	选择文件 未选择任何文件 Update		
MCU Update			
Port:	☐ gsm-1 & gsm-2 ☐ gsm-3 & gsm-4 ☐ lte-5 & lte-6 ☐ lte-7 & lte-8		
	☐ All ☐ Show All		
MCU Update file:	选择文件 未选择任何文件 Update		

3.9 Call and SMS Limit

Click the edit button to set call restrictions, lock cards, and SMS restrictions. You can also view statistics on call/sms sent here.

Figure 3-9-1 Call and SMS Limit

Port	Type	Call Status	Lock Status	Mark Status	SMS Status	Actions
1.1	GSM	Unlimited 	Unlocked 	Unmarked	Unlimited	
1.2	GSM	Unlimited 	Unlocked 	Unmarked	Unlimited	
1.3	GSM	Unlimited 	Unlocked 	Unmarked	Unlimited	
1.4	GSM	Unlimited 	Unlocked 	Unmarked	Unlimited	
2.5	LTE	Unlimited 	Unlocked 	Unmarked	Unlimited	
2.6	LTE	Unlimited 	Unlocked 	Unmarked	Unlimited	
2.7	LTE	Unlimited 	Unlocked 	Unmarked	Unlimited	
2.8	LTE	Unlimited 	Unlocked 	Unmarked	Unlimited	

Port	Type	Hour Call Count	Daily Call Count	Daily Answer Count	Call Failed Count	Call Duration
1.1	GSM	0	0	0	0	0
1.2	GSM	0	0	0	0	0
1.3	GSM	0	0	0	0	0
1.4	GSM	0	0	0	0	0
2.5	LTE	0	0	0	0	0
2.6	LTE	0	0	0	0	0
2.7	LTE	0	0	0	0	0
2.8	LTE	0	0	0	0	0

SMS Sending Statistics						
☐ Port	Type	SMS count of the day	Daily limit	SMS count of the month	Monthly limit	Monthly recovery date
☐ 1.1	GSM	0	0	0	0	0
☐ 1.2	GSM	0	0	0	0	0
☐ 1.3	GSM	0	0	0	0	0
☐ 1.4	GSM	0	0	0	0	0
☐ 2.5	LTE	0	0	0	0	0
☐ 2.6	LTE	0	0	0	0	0
☐ 2.7	LTE	0	0	0	0	0
☐ 2.8	LTE	0	0	0	0	0
		Clear zero		Clear zero		

Call Limit

You can limit the number of daily calls, number of days connected, and number of hours of calls for the selected channel.

Figure 3-9-2 Call Limit

Call Limit (gsm-1.1)	
Call Limit Switch:	☒ ON
Limit Daily Call Times:	0
Limit Daily Answer Times:	0
Limit Hour Call Times:	0

Call Limit Time

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

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 through this port, your calling time will be limited.

Single Call Duration Limitation: If your calling time exceeds the set value, the system will hang up the call. Multiplying the step size by a single call time is to allow a single call duration.

Figure 3-9-3 Single Settings

Call Limit Time	
Call Time Limit Switch:	☒ ON
Step:	60 Second
Enable Single Call Duration Limit:	☒ ON
Single Call Duration Limitation:	0
Enable Call Duration Limitation:	☐ OFF

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 3-9-4 Call Duration Limitation Settings

Call Limit Time	
Call Time Limit Switch:	☒ ON
Step:	60 Second
Enable Single Call Duration Limit:	☒ ON
Single Call Duration Limitation:	0
Enable Call Duration Limitation:	☒ ON
Call Duration Limitation:	10
Minimum Charging Time:	30 Second
Alarm Threshold:	2
Alarm Phone Number:	18610001000
Alarm Description:	test
Remain Time:	0 Reset
Enable Auto Reset:	☒ ON
Auto Reset Type:	Week(7Day) ▼
Next Reset Time:	2019-04-01 16:29:35

The same as the algorithm for the single call duration limit, the total call time of the port cannot exceed the product of the "Step" and the "Call Duration Limitation". The Minimum Billing Time value must be less than the step size.

You can set a value for the Alarm Threshold. When the remaining call duration of the

port reaches the set value, the gateway will send alarm info to the designated phone. You can also turn on enable auto reset, which can be selected from one day, one week or one month. After the automatic reset time is reached, the remaining call duration is reset to the set total call duration.

Figure 3-9-5 Auto Reset Settings

Enable Auto Reset:	☒ ON
Auto Reset Type:	Week(7Day) ▼
Next Reset Time:	2019-04-01 16:29:35

Table 3-9-1 Description of Call Duration Limit Settings

Options	Definition
Step	The value range of the step length is 1-999s. Multiplying the step size by a single call time is to allow a single call duration.
Enable Single Call Duration Limit	The value of the single call duration limit, ranging from 1-999999. The step size multiplied by the single talk time is the single call duration.
Enable Call Duration Limitation	The value of the total call duration limit, in the range of 1-999999. The step size multiplied by the total talk time is the total call duration.
Minimum Charging Time	After a period of conversation, the operator starts billing, in seconds. This value must be less than the step size.
Alarm Threshold	The threshold for the duration of the call. When the duration of the call is equal or less than this value, the gateway will send an alert message to the specified phone number via SMS (only once before the total call duration is reset). This value must be less than the call duration limit.

Alarm Phone Number	User will received alarm message from the gateway when receiving alarm phone number.
Alarm Description	The alarm port information description sends the alarm information to the user's phone.
Remaining call duration	Multiplying this value by the step size is the remaining call duration.
Enable Auto Reset	The remaining talk time is automatically restored, that is, the total number of minutes of the call is restored.
Auto Reset Type	Reset call minutes by date, by week, by month.
Next Reset Time	Define the next reset date. The system will count from that date and be set as a reset period.

Lock Card

The lock card detection switch is a switch function of the lock card. After opening, the call failure lock card condition parameter needs to be set. After the lock card condition is reached, the SIM card is disabled and cannot be allocated for use unless the card is removed, the gateway is restarted, and the manual is unlocked (Duration limit requires manual reset), turn off the lock card function, etc.

Figure 3-9-6 Lock Card

Lock Sim	
Lock Detect Switch:	☒ ON
Mark Switch:	☒ ON
Call Failed Mark Count:	3
Call Failed Lock Switch:	☒ ON
Call Failed Lock Count:	3
SMS Send Detection Switch:	☒ ON
SMS Send Detection Count:	10
Send Sms Number:	13810001000
Sms Message:	test s
Testing SMS report:	☒ ON

Table 3-9-3 Description of Lock Card

Options	Definition
Call Failed Mark Count	The number of consecutive calls failed to reach the number of settings, making the port.
Called Failed Lock Count	Lock the port after the number of successive call failures reaches the set number, restrict the port expiration, and no longer select the port expiration in the group policy.
SMS Send Detection Switch	After opening, when the number of successive call failures reaches the set value, send message to check whether the port is available; if the message send successfully, it will clear the number of successive call failures; if the message fails, it will limit the port's outgoing.
Testing SMS report	When closed, the successful sending of message indicates that the port is available; when opened, the successful sending of message and the receipt of message report indicate that the port is available.

SMS Limit

Figure 3-9-7 SMS Limit

SMS Limit	
SMS Limit Switch	☒ ON
SMS Limit Success Flag	☒ ON
Day Limit SMS Count	0
Month Limit SMS Count	5
SMS Clean Date	1 ▼

Table 3-9-4 Definition of SMS Limit

Options	Definition
SMS Limit Success Flag	When closed, no matter whether the message is sent successfully or not, the number of messages is counted; When opened, the number of messages is counted when the message is sent successfully.
Day Limit SMS Count	Limit the number of SMS sent daily, the default value is 0, indicating unlimited.
Month Limit SMS Count	Limit the number of SMS sent per month, the default value is 0, indicating unlimited.
SMS Clean Date	The number of messages sent monthly is automatically cleared at 0 points, 0 minutes and 0 seconds on the set date.

4. VOIP

4.1 VOIP Endpoints

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

Figure 4-1 SIP&IAX2 Endpoints

SIP Endpoint

☐	Endpoint Name	Registration	Credentials	Actions
☐	10028	none	anonymous@172.16.208.33	 
☐	2111	server	test	 

Add New SIP EndpointDelete

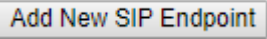
IAX2 Endpoint

☐	Endpoint Name	Registration	Credentials	Actions
☐	2133	client	2133@172.16.208.33	 

Add New IAX2 EndpointDelete

4.1.1 Add New SIP Endpoint

Main SIP Endpoint Settings:

You can click  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 you to 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 4-1-1 None Registration

Main Endpoint Settings	
Name:	6666
User Name:	☒ Anonymous
Password:	
Registration:	None
Hostname or IP Address:	172.16.200.20
Transport:	UDP
NAT Traversal:	Yes

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 4-1-2 Server Registration

The screenshot shows the 'Main Endpoint Settings' form. The fields are: Name (10027), User Name (10027) with an 'Anonymous' checkbox, Password (masked with dots), Registration (Server, highlighted with a red box), Hostname or IP Address (dynamic), Transport (UDP), and NAT Traversal (Yes).

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

Figure 4-1-3 Client Registration

The screenshot shows the 'Main Endpoint Settings' form. The fields are: Name (10027), User Name (10027) with an 'Anonymous' checkbox, Password (masked with dots), Registration (Client, highlighted with a red box), Hostname or IP Address (172.16.80.16), Transport (UDP), and NAT Traversal (Yes).

Table 4-1-1 Definition of SIP Options

Options	Definition
Name	A name is easier to understand, only for reference, does not participate in SIP authentication.
Username	Register name in your SIP server.
Password	Authenticating with the gateway and characters are allowed.
Registration	Whether the terminal registers with the gateway or the gateway registers with the terminal.

	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. Notice: If you entered the domain name and changed the DNS, you must restart asterisk.
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 report if the remote needs it. Force Report on—Force report on. Yes --- Force the report to open and perform commedia RTP processing. Report if requested and commedia --- If the remote needs it, use report and perform commedia RTP processing.

Advanced: Registration Options

Figure 4-1-4 Advanced Registration Options

The screenshot shows the 'Advanced:Registration' configuration page. It contains the following fields and options:

- Authentication User:** 108
- Register Extension:** 108 ☐ Modify
- Register User:** 108 ☐ Modify
- Contact User:** ☒ Modify
- From User:** ☐ Modify
- From Domain:**
- Port:** 5060
- Quality:** No ▾
- Qualify Frequency:** 60
- Outbound Proxy:** :
- Custom Registry:** ☐ OFF
- Enable Outboundproxy to Host:** ☐ OFF

Table 4-1-2 Definition of Registration Options

Options	Definition
Authentication User	Just a username used when registering.
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	Register user name, it is the user of register => user[:secret[:authuser]]@host[:port][[/extension]].
Contact User	e.g. When the Contact User is 402 Contact: sip:402@172.16.6.123:5060;transport=UDP.
From User	A username to identify the gateway to this endpoint.
From Domain	A domain to identify the gateway to this endpoint.
Port	The port number used by the gateway to link the peer.

Qualify	Whether to check the link status of the peer.
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 Registry	After opening, customers can customize their own registry.
Registry String	Customers can enter their own registration information. The format is:: user[:secret[:authuser]]@host[:port][/extension] e.g.: 1001@sip.com:pbx122@172.16.6.122/1001.
Enable Outbound proxy to Host	Outbound proxy to Host On / Off.

Call Settings

Figure 4-1-5 Call Settings

Call Settings

DTMF Settings

DTMF Mode: RFC2833

Caller ID Settings

Trust Remote-Party-ID: No

Send Remote-Party-ID: No

Caller ID Presentation: Allowed,passed screen

Maximum Channels

Call Limit:

Table 4-1-3 Description of DTMF Detection 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).
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 the Caller ID.
Call Limit	Usually used when this sip works as a trunk. Limit the maximum number of channels supported by sip trunks.

Advanced: Signaling Settings

Figure 4-1-6 Signaling Settings

Advanced: Signaling

Progress Inband:	Never ▼
Append user=phone to URI:	No ▼
Add Q.850 Reason Headers:	No ▼
Ignor SDP Version:	Yes ▼
Directmedia:	Yes ▼
Allow Transfers:	Yes ▼
Allow Promiscuous Redirects:	No ▼
Max Forwards:	70
Send TRYING on REGISTER:	No ▼

Table 4-1-4 Definition of Signaling Options

Options	Definition
Progress Inband	Whether the tone is ringing. Never: Indicates that the incoming calls are never applied. Option values: yes, no, never. Default: never.
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 a reason header and use it if is available.
Ignore 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. Switch 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.
Direct media	The value of parameter direct media is one of them (no, yes, nonat, update, outgoing). Default value is yes.
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. Notice: Redirecting the local system causes a loop call, which is not supported by asterisk.
Max Forwards	Setting for the SIP Max-Forwards header (loop prevention).
Send TRYING on REGISTER	Send a 100 Trying when the endpoint registers.

Advanced: Timer Settings

Figure 4-1-7 Timer Settings

▼ Advanced:Timer Settings

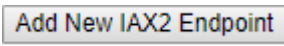
Default T1 Timer:	500
Call Setup Timer:	32000
Session Timers:	Accept ▼
Minimum Session Refresh Interval:	90
Maximum Session Refresh Interval:	1800
Session Refresher:	UAS ▼

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 500 ms 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. The default is 64*T1.
Session Timers	There are three modes for you to choose: originate, request and run session-timers always; Accept or run the session timer only when requested by another user agent; Refuse, Do not run session timers in any case.
Minimum Session Refresh Interval	Minimum session refresh interval in seconds. The default is 90 secs.
Maximum Session Refresh Interval	Maximum session refresh interval in seconds. The default is 1800secs.
Session Refresher	The session refresher, UAC or UAS. The default is 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 three registration types: None, Server or Client.

You can configure as follows:

If you set up an 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 4-1-8 None Registration

Main Endpoint Settings	
Name:	lax-test
User Name:	1001
Password:	*****
Registration:	None ▼
Hostname or IP Address:	172.16.80.92
Auth:	md5 ▼
Transfer:	No ▼
Trunk:	No ▼

For convenience, you can choose registration by “Server”, thus your gateway just work as a server.

Figure 4-1-9 Server Registration

Main Endpoint Settings	
Name:	lax-test
User Name:	1001
Password:	*****
Registration:	Server ▼
Hostname or IP Address:	dynamic
Auth:	md5 ▼
Transfer:	No ▼
Trunk:	No ▼

Also you can choose registration by “Client”, it will work as a Client.

Figure 4-1-10 Client Registration

Main Endpoint Settings	
Name:	lax-test
User Name:	1001
Password:	*****
Registration:	Client ▼
Hostname or IP Address:	172.16.80.92
Auth:	md5 ▼
Transfer:	No ▼
Trunk:	No ▼

Table 4-1-6 Definition of IAX2 Options

Options	Definition
Name	A name which is able to read by human. And it's only used for user's reference.
Username	The endpoint will use username to authenticate with the

	gateway.
Password	The endpoint will use password to authenticate with the gateway.
Registration	Whether this endpoint will register to this gateway or this gateway to the endpoint. 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. Notice: If you entered the domain name and changed the DNS, you must restart asterisk.
Auth	There are three authentication methods that are supported: md5, plaintext and rsa. The least secure is "plaintext", which sends passwords clear text across the net. 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.
Transfer	Disable or not IAX2 native transfer .
Trunk	Use IAX2 trunking with this host.

Advanced: Registration Options

Figure 4-1-11 Registration Options

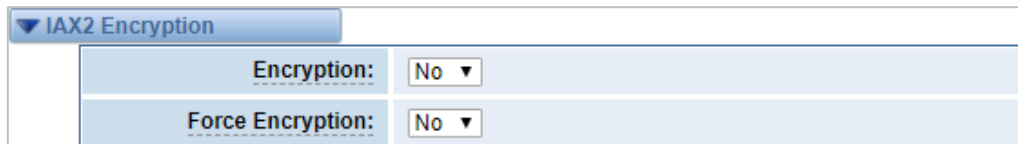
▼ Advanced:Registration Options	
Qualify:	Yes ▼
Qualify Smothing:	Yes ▼
Qualify Freq Ok:	6000
Qualify Freq Not Ok:	6000
Port:	4569
Require Call Token:	Yes ▼

Table 4-1-7 Definition of Registration Options

Options	Definition
Qualify	Whether or not to check the endpoint's connection status.
Qualify Smoothing	Use the average of the last two connection results to reduce the lag end of the misdetection. The default is no.
Qualify Freq Ok	How frequently to ping the peer when everything seems to be OK, in milliseconds
Qualify Freq Not Ok	How frequently to ping the peer when it is either, LAGGED or UNAVAILABLE, in milliseconds.
port	The port number the gateway will connect to at this endpoint. Default is 4569.

IAX2 Encryption

Figure 4-1-12 IAX2 Encryptions



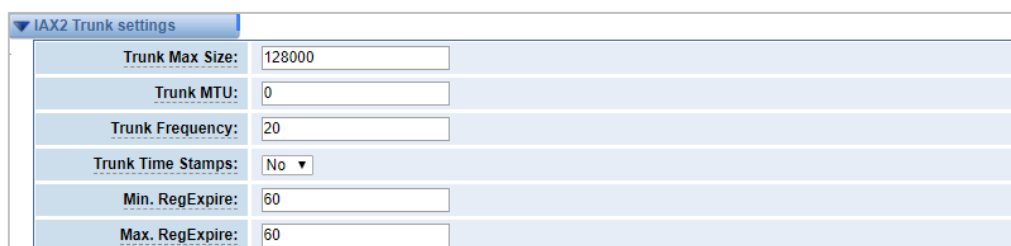
The screenshot shows a configuration window titled "IAX2 Encryption". It contains two rows of settings. The first row is labeled "Encryption:" and has a dropdown menu set to "No". The second row is labeled "Force Encryption:" and also has a dropdown menu set to "No".

Table 4-8 Definition of Encryption 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 switching this option on, encryption is automatically switch on as well. The default is no.

IAX2 Trunk Settings

Figure 4-1-13 IAX2 Trunk Settings



The screenshot shows a configuration window titled "IAX2 Trunk settings". It contains six rows of settings, each with a label and a value field. The values are: Trunk Max Size: 128000, Trunk MTU: 0, Trunk Frequency: 20, Trunk Time Stamps: No (dropdown), Min. RegExpire: 60, and Max. RegExpire: 60.

Table 4-1-9 Definition of Trunk Options

Options	Definition
Trunk Max Size	The default is 128000 bytes, which supports up to 800 calls of ulaw at 20ms a frame.

Trunk MTU	Set the maximum transmission unit for IAX2 UDP trunking.
Trunk Frequency	How frequently to send trunk messages in msec. This is 20ms by default.
Trunk Time Stamps	Ensure that frame timestamps get sent end-to-end properly.
Min. RegExpire	Minimum amounts of time that IAX2 peers can request as a registration expiration 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

On this page, you can create multiple SIP Endpoints at the same time.

Figure 4-2-1 Multiple SIP Endpoints Settings

☐	ID	User Name	Password	Hostname or IP Address	Port	Register Mode
☐						client ▼
☐	1					client ▼
☐	2					client ▼
☐	3					client ▼
☐	4					client ▼
☐	5					client ▼
☐	6					client ▼
☐	7					client ▼
☐	8					client ▼

You should select the number of SIPs to be created after you filling in the username, password, domain name or IP address, port and registration mode in the first line. You can create up to the same number of SIP endpoints as the number of device ports at a time; Then choose whether to tick “AutoPassword” button. After the above configuration is completed, click Batch Settings, and then save to create SIP endpoints in batches.

Table 4-2-1 Definition of Multiple SIP Endpoints

Options	Definition
Username	The display name is the same as the registered name on the SIP server by default.
Password	Authenticating with the gateway and characters are allowed.
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.
Port	Port number registration
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;
AutoPassword	Tick - Automatically increments based on the password entered in the first line. Do not tick- All SIP endpoints have the same password as the first one.

4.3 Advanced SIP Settings

Networking

Figure 4-3-1 Networking General

The screenshot shows the 'Networking' tab with the 'General' sub-tab selected. The configuration fields are as follows:

Field	Value
UDP Bind Port:	5060
Enable TCP:	No
TCP Bind Port:	5060
TCP Authentication Timeout:	
TCP Authentication Limit:	
Enable Hostname Lookup:	No
Enable Internal SIP Call:	No
Internal SIP Call Prefix:	

Table 4-3-1 Definition of Networking General 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. Notice: The gateway uses the first host in the SRV record. This function can be used in dial-up activation to dial SIP calls on

	the Internet via domain name.
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 S	Specify a prefix before routing the internal calls.

Figure 4-3-2 NAT Settings

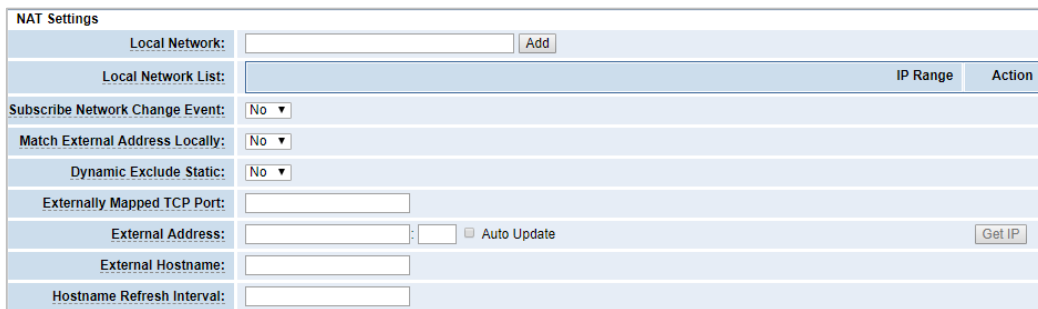


Table 4-3-2 Definition of NAT Settings Options

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 NAT 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	Add local IP address list.
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 <code>stun_monitor</code> is installed and configured, <code>chan_sip</code> will renew all outbound registrations when the monitor detects any sort of network change has occurred. By default this option is enabled, but <code>res_stun_monitor</code> only takes effect once. If <code>res_stun_monitor</code> is enabled and you don't want changes on the network to cause an outbound registration, use the option below to disable this feature.
Match Address Locally	External	Only substitute the extern address or extern host setting if it matches.
Dynamic Static	Exclude	Dynamic hosts are not allowed to register with the static host's IP address, which will avoid the same IP registration error.
Externally TCP Port	Mapped	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.
Hostname Interval	Refresh	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.

Figure 4-3-3 RTP Settings

RTP Settings	
Start of RTP Port Range:	10000
End of RTP port Range:	20000
RTP Timeout:	120

Table 4-3-3 Definition of RTP Settings Options

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

Parsing and compatibility

Figure 4-3-4 Parsing and Compatibility

Parsing and Compatibility

General

Strict RFC Interpretation:

Yes

Send Compact Headers:

No

SDP Owner:

Ring 183 Mode:

Immediately

SIP Methods

Disallowed SIP Methods

ACK

BYE

CANCEL

INFO

INVITE

MESSAGE

NOTIFY

OPTIONS

PRACK

PUBLISH

REFER

REGISTER

SUBSCRIBE

UPDATE

Hangup Cause Code:

default

Notify Unlimited:

OFF

Caller ID	
Shrink Caller ID:	No ▾
Caller ID:	SIP From ▾ Number ▾
SIP From:	Tel/Tel ▾
Callee ID	
SIP To:	Tel/Tel ▾
Callee ID:	EXTEN ▾
Permit Dialing Letters:	☐ OFF
Timer Configuration	
Maximum Registration Expiry:	
Minimum Registration Expiry:	
Default Registration Expiry:	
Outbound Registrations	
Registration Timeout:	20
Number of Registration Attempts:	0
Transform Local Port	
Client Auto Flag:	☐ OFF

Table 4-3-4 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	When a dialog is started with another SIP endpoint, the other endpoint should include an Allow header telling us what SIP methods the endpoint implements. However, some endpoints either do not include an Allow header or lie about what methods they implement. In the former case, the gateway makes the assumption that the endpoint supports all known SIP methods. If you know that your SIP endpoint does

	not provide support for a specific method, then you may provide a list of methods that your endpoint does not implement in the disallowed methods option. Note that if your endpoint is truthful with its Allow header, then there is no need to set this option.
Shrink Caller ID	The Shrink Caller Id function removes '(', ' ', ')', non-trailing '.', and '-' not in square brackets. For example, the caller id value 555.5555 becomes 5555555 when this option is enabled. By default, this option is on.
Caller ID	Default: SIP From and Number. For example: When selecting SIP From, Name is Peter and Number is 402. The From mode is: "Peter"<sip:402@172.16.6.239;transport=UDP>;tag=bd481672.
Callee ID	Default: EXTEN For example: When selecting SIP To, Name is Jason and Number is 401. The mode is: "Jason"<sip:401@172.16.6.239;transport=UDP>.
Maximum Registration Expiry	Maximum allowed time of incoming registrations and subscriptions (seconds).
Minimum Registration Expiry	Minimum length of registrations/subscriptions (default 60).
Default Registration	Default length of incoming/outgoing registration.

Expiry	
Registration Timeout	How often, in seconds, to retry registration calls. Default 20 seconds.
Number of Registration	Number of registration attempts before we give up.

Security

Figure 4-3-5 Security Settings

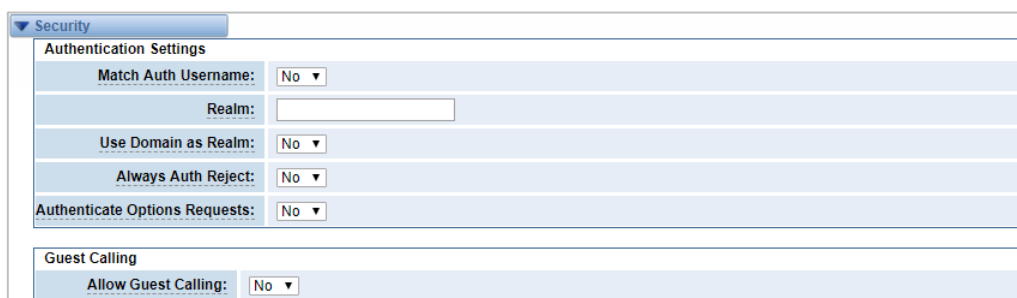


Table 4-3-5 Instruction of Security

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. All realms must be globally unique according to the RFC3261 standard and can generally be set to hostname or domain name.
Use Domain as Realm	Use the domain from the SIP Domains setting as the realm.
Always Auth Reject	When an INVITE or REGISTER request is rejected for any reason, the same reason is always used, the username is legal but the password is incorrect. It does not tell the

	requester whether there is this user or peer, which will reduce the possibility of the attacker scanning the SIP account. This parameter is enabled 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 customer calls (default yes, allowed). If your gateway is connected to the Internet and allows customers to call, you want to check which services are available to everyone, by enabling them in the default context.

Media

Figure 4-3-6 Media Settings



The screenshot shows a web interface for Media Settings. Under the 'Media' tab, there is a section for 'QoS/ToS'. It contains two input fields: 'TOS for SIP Packets:' and 'TOS for RTP Packets:'. Both fields are currently empty.

Table 4-3-6 Instruction of Media

Options	Definition
TOS for SIP Packets	Sets type of service for SIP packets.
TOS for RTP Packets	Sets type of service for RTP packets.

Codec Settings

Select codecs from the list below.

Figure 4-3-7 Codec Settings

▼ Codec Settings	
Codec Priority 1:	G.711 u-law ▼
Codec Priority 2:	G.711 a-law ▼
Codec Priority 3:	GSM ▼
Codec Priority 4:	G.722 ▼
Codec Priority 5:	G.723 ▼
Codec Priority 6:	G.726 ▼
Codec Priority 7:	G.729 ▼

4.4 Advanced IAX2 Settings

General Settings

Figure 4-4-1 General Settings

▼ General Settings	
Bind Port:	4569
Bind Address:	0.0.0.0
Enable IAXCompat:	No ▼
Enable Nochecksums:	No ▼
Enable Delay Reject:	No ▼
ADSI:	No ▼
SRV Loopup:	No ▼
AMA Flags:	default ▼
Auto Kill:	Yes ▼
Language:	English ▼
Account Code:	
Call Token Optional:	
Description:	

Table 4-4-1 Instruction of General

Options	Definition
Bind Port	Bind port and bindaddr may be specified.
Enable	Set laxcompat to yes if you need to use a tiered switch, or if

IAXCompat	some of the latency may occur when performing a lookup in a dial plan, otherwise enabling it will result in a small performance conflict.
Enable Nochecksums	Disable UDP checksums (if Nochecksums is set, then Nochecksums will be calculated/checked on systems supporting this feature).
ADIS	ADSI (Analog Display Services Interface) can be enabled if you have (or may have) ADSI compatible CPE equipment.
SRV Lookup	Whether or not to perform an SRV lookup on outbound calls.
AMA Flags	You may specify a global default AMA flag for IAX internal calls. These flags are used in the generation of call detail records.
Auto Kill	If we don't get ACK to our NEW within 2000ms, and Auto Kill 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, However, this function is not friendly in the case of poor connection status.
Language	You may specify a global default language for users. This can be specified also on a per-user basis. If you ignore this item, it will use the default English language.
Account Code	You may specify a default account for Call Detail Records (CDRs) in addition to specifying on a per-user basis.

Music on Hold

Figure 4-4-2 Music on Hold Settings

▼ Music On Hold	
Mohsuggest:	default ▼
Mohinterpret:	default ▼

Table 4-4-2 Instruction of Music on Hold

Options	Definition
Mohsuggest	Specifies the type of waiting music that plays while the channel is on hold. It can specify global settings or be specified by the user or each peer.
Mohinterpret	Set the content of the channel playback when the phone is suspended. If it is "default", the music specified in the dialing rules will be played in the channel when the phone hangs. If it is "transfer", it will be replaced by a message signal.

Instruction of Codec Settings

Figure 4-4-3 Codec Settings

▼ Codec Settings	
Band Width:	low ▼
Disallow:	all ▼
Allow:	Priority 1 GSM ▼
	Priority 2 G.711 u-law ▼
	Priority 3 G.711 a-law ▼
	Priority 4 G.722 ▼
	Priority 5 G.723 ▼
	Priority 6 G.729 ▼
Codec Priority:	host ▼

Table 4-4-3 Instruction of Codec Settings

Options	Definition
Band Width	Specify bandwidth of low, medium, or high to control which codes are used in general.
Disallow	Adjust the type of codec to be switched off.
Allow	Adjust the type of codec to be switched on and the priority.
Codec Priority	Codec priority controls the codec negotiation of an inbound IAX2 call. This option is inherited to all user entities. It can also be defined in each user entity separately which will override the setting in general.

Jitter Buffer Settings

Figure 4-4-4 Jitter Buffer



▼ Jitter Buffer Settings	
Jitter Buffer:	No ▼
Force Jitter Buffer:	No ▼
Max Jitter Buffers:	
Resyncthreshold:	Resyncing can be disabled by setting this parameter to -1.
Max Jitter Interps:	
Jitter Target Extra:	

Table 4-4-4 Instruction of Jitter Buffer

Options	Definition
Jitter Buffer	Whether to set a global buffer should be enabled by an unstable network environment, generally you do not need. Because the terminal device buffers the jitter processing. The default is "no".

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. The default is "no".
Max Jitter Buffers	A maximum size for the jitter buffer.
Resyncthreshold	When the jitter buffer notices a significant change in delay that continues 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. Resyncing can be disabled by setting this parameter to -1.
Max Jitter Interps	The maximum number of interpolation frames the jitter buffer should return in a row.
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 plus 40 milliseconds. Increasing this value may help if your network normally has low jitter, but occasionally has spikes.

Misc Settings

Figure 4-4-5 Misc Settings

▼ Misc Settings	
IAX2 Thread Count:	
IAX2 Max Thread Count:	
Max Call Number:	
MaxCallNumbers_Nonvalidated:	

Table 4-4-5 Instruction of Misc Settings

Options	Definition
IAX Thread Count	Establishes the number of IAX helper threads to handle I/O
IAX2 Max Thread Count	Establishes the number of extra dynamic threads that may be spawned to handle I/O.
Max Call Number	The 'Max Call Numbers' 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 ' Max Call Number ' 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 token user guide. This option's default value of 8192 should be sufficient in most cases.

Quality of Service

Figure 4-4-6 Quality of Service

▼ Quality of Service	
tos:	High Reliability ▼
cos:	

Table 4-4-6 Instruction of Quality of Service

Options	Definition
TOS	Type of service.
COS	Class of service.

4.5 SIP Account Security

The SIP account security module greatly enhances the security of the system. The wireless gateway supports TLS encrypted calls (sip), which requires sip phone support.

Figure 4-5-1 SIP Account Security

▼ TLS Setting						
TLS Enable:		☒				
TLS Verify Server:		☒				
Port:		5061				
TLS Client Method:		tlsv1 ▼				
▼ TLS keys						
Type	Key Name	IP Address	Organization	Password	Operation	
client ▼					Create	
▼ Key Files						
Upload the pem file:		选择文件 未选择任何文件				File Upload
Upload the crt file:		选择文件 未选择任何文件				
File Name		File Size		Operation		

You need to understand its rules when using TLS. The following table shows the setting parameters of TLS.

Table 4-5-1 Parameters of TLS settings

Options	Definition
TLS Enable	Enable or disable DTLS-SRTP support.
TLS Verify Server	If set it off, there is no need to verify the server certificate when the client is operating. If you do not have a server CA certificate, you can disable authentication to connect without the need for a TLS CA file.
Port	TLS port SIP registration, default port 5061.
TLS Client Method	Values include tlsv1, sslv3, sslv2, which specify the protocol for the outbound client connection. The default is sslv2.

Enter the key name, IP address, organization and password in the above settings to create a ca certificate. After mutual authentication between the client and the server, it can be accessed with a certificate.

We need to do a few basic steps:

1. Your asterisk server requires an authentication. We must create or add a certificate on the asterisk server. We need to create a digital key for our server, the server key is the key.pem file, and the certificate request is request.pem.
2. Add some configuration settings to the sip.conf file.
3. Configure the client to use TLS.

5. Routing

5.1 Call Routing Rules

Figure 5-1-1 Call Routing Rules

	Move	Order	Rule Name	From	To	Rules	Actions
☐		1	incoming	grp-all	iax-2133		
☐		2	outgoing	sip-2111	lte-1.2		
☐		3	test	sip-10028	gsm-2.6	Dial_pattern (+1[/.])	

[New Call Routing Rule](#) [Delete](#) [Save Orders](#)

You are allowed to set up new call routing rules 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 button [Save Orders](#) to save what you set.

Call Routing Rules

You can click [New Call Routing Rule](#) button to set up your routings.

Figure 5-1-2 Call Routing Rules

Call Routing Rule

Routing Name:

incoming

Call Comes in From:

all

Send Call Through:

None

DISA Settings

Any SIP

Authentication:

Port

Advance Routing Rule

lte-1.1

lte-1.2

lte-1.3

lte-1.4

gsm-2.5

gsm-2.6

gsm-2.7

gsm-2.8

SIP

8000

8001

401

GROUP

all

Save

Apply

Cancel

The figure above shows that all the phones in the group ALL are transferred to the IAX2-2133. When the "incoming source" is GSM/LTE port, "prepend", "prefix" and "match pattern" in the "Advanced Routing Rules" are invalid, and only the "CallerID" option is available.

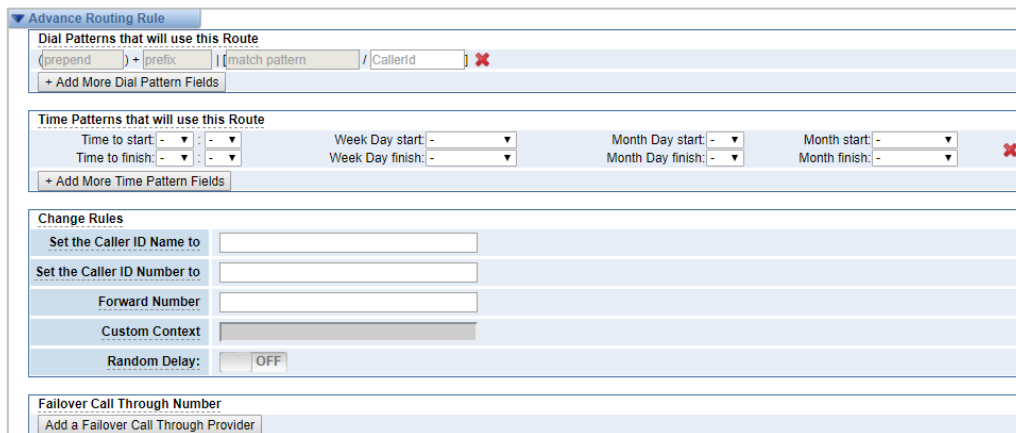
Table 5-1-1 Definition of Routing Options

Options	Definition
Routing Name	The name of this route. Should be used to describe what types of calls this route matches (for example: 'sip1TOport1' or 'port1TOsip1').
Call Comes in From	The launching point of incoming calls.
Send Call Through	The destination to receive the incoming calls.

Figure 5-1-3 DISA Settings

In the DISA Settings, you can set a Password, Authentication or Secondary Dialing.

Figure 5-1-4 Advance Routing Rule Settings



In the Advance Routing Rule Settings, you can set the function of the dial Patterns、Time Patterns、Calling, Forward, Delay and Failover.

Table 5-1-2 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 (for 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.
Set the Caller ID Number to	What caller ID number would you like to set before sending this call to the endpoint.
Forward Number	This number will be sent to target PBX or SIP Server as a DID number for inbound rule settings.
Custom Context	Custom the context of dialing rules.

Random Delay	Randomly obtain any value within the threshold interval.
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 Port or SIP to groups. Then if you want to make a call, it will find available port automatically. For the "Ascending" policy, if 2 or more port members are selected, it will use the first available port to call/access the call. In this case, if the gsm-1.1 is available, it will always use the gsm-1.1 call, otherwise, it will use gsm-1.2, and so on.

Figure 5-2-1 Routing Groups

Routing Groups

Group Name:

Type:

Policy:

Members

NO.	☐ All
1	☒ lte-1.1
2	☒ lte-1.2
3	☒ lte-1.3
4	☒ lte-1.4
5	☒ gsm-2.5
6	☒ gsm-2.6
7	☒ gsm-2.7
8	☒ gsm-2.8

Save Apply Cancel

5.3 Batch Creating rules

This page can generate multiple routing rules at the same time.

Figure 5-3-1 Batch Creating rules

Port	Sim Number	Sip Trunk	CallerID
lte-1.1	66001	10028	101
lte-1.2	66002	None	102
lte-1.3	66003	None	200
lte-1.4		None	
gsm-2.5		None	
gsm-2.6		None	
gsm-2.7		None	
gsm-2.8		None	

SIM Number: This number will be sent to target PBX or SIP Server as a DID number for inbound rule settings. If the SIM number is empty, no incoming routing is created.

The SIM number will be sent to the target PBX or SIP server as DID number, and the calling number will be set to the caller ID in the outgoing route.

Figure 5-3-2 Create an incoming route

Call Routing Rule

Routing Name: gsm-1.12sip

Call Comes in From: lte-1.1

Send Call Through: 10028

DISA Settings

Authentication: OFF

Advance Routing Rule

Dial Patterns that will use this Route

Time Patterns that will use this Route

Change Rules

Set the Caller ID Name to

Set the Caller ID Number to

Forward Number 66001

Custom Context

Random Delay: OFF

Failover Call Through Number

Add a Failover Call Through Provider

Figure 5-3-3 Create an outgoing route

Call Routing Rule

Routing Name: sip2gsm-1.1

Call Comes in From: 10028

Send Call Through: lte-1.1

DISA Settings

Authentication: OFF

Advance Routing Rule

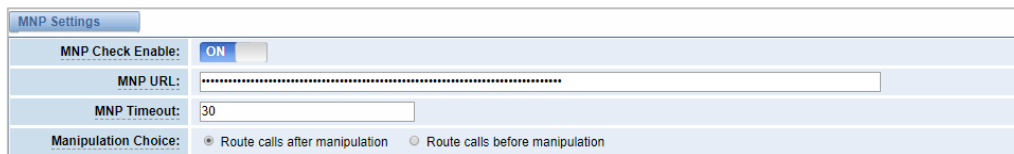
Dial Patterns that will use this Route

Time Patterns that will use this Route

5.4 MNP Settings

Mobile Number Portability allows switching between mobile phone operators without changing the mobile number.

Figure 5-4-1 MNP Settings



The URL is displayed as a password string. So please enter the URL in the format below and check if it is correct. After confirming, copy it to the gateway.

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, The outgoing number in the url should be replaced by a variable `${num}`.

When configuring MNP url, it should be replaced with `${num}`, Then paste: `https://s1.bichara.com.br:8181/chkporta.php?user=832700&pwd=sdsfdg&tn=${num}`.

5.5 Routing Blacklist

Figure 5-5-1 Routing Blacklist Settings



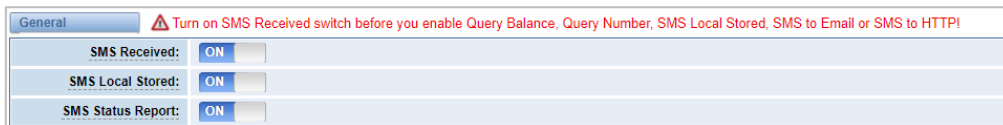
Blacklists are used to add a phone number to the blacklist or to remove a phone number from the blacklist. After opening the blacklist routing, in the incoming mode, if the calling number is in the blacklist, it will be routed to `hangup()` to end the call.

6. SMS

6.1 General

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

Figure 6-1-1 SMS Settings

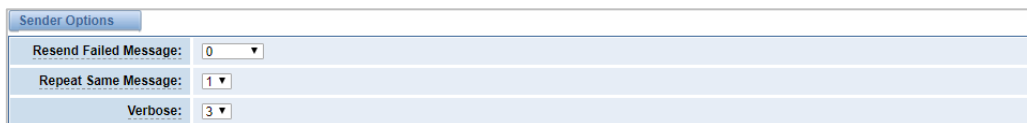


General	
⚠ Turn on SMS Received switch before you enable Query Balance, Query Number, SMS Local Stored, SMS to Email or SMS to HTTP!	
SMS Received:	☒
SMS Local Stored:	☒
SMS Status Report:	☒

Sender Options

You can change sender options here, include resend and the time of resend.

Figure 6-1-2 Sender Options



Sender Options	
Resend Failed Message:	0
Repeat Same Message:	1
Verbose:	3

Table 6-1-1 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.
Verbose	Verbose level of sending message.

SMS to Email

This is a tool that makes it available for you to email account to transmit th

e 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 6-1-3 SMS to Email

SMS to Email	
Enable:	☒ ON
SMTP Server:	OTHER ▼
Email Address of Sender:	openvpnvoip@gmail.com
Domain:	smtp.gmail.com
SMTP Port(default 25):	587
SMTP User Name:	openvpnvoip@gmail.com
SMTP Password:	*****
TLS Enable:	☒ This option allows the authentication with certificates.
Destination Email Address 1:	openvpnvoip@yahoo.com.cn
Destination Email Address 2:	openvpnvoip@hotmail.com
Destination Email Address 3:	support@openvox.cn
Title:	support
Content:	we can offer 24 hour's support

Table 6-1-2 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	×

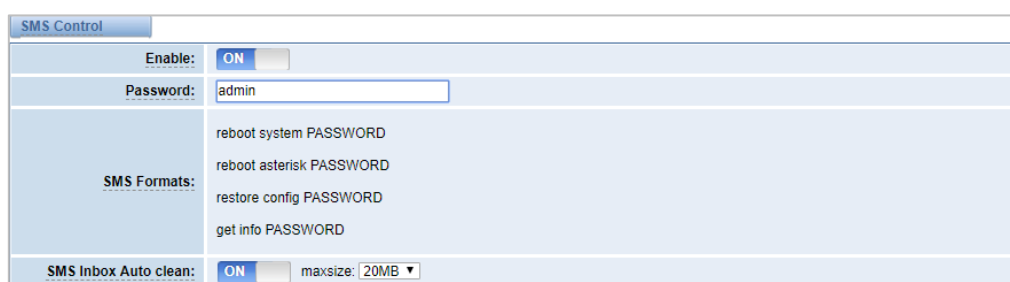
Table 6-1-3 Definition of SMS to E-mail

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

Email Address of Sender	To set the email address of an available email account. For example: <u>openvpnvoip@gmail.com</u> .
Domain	To set outgoing mail server. For example: smtp.gmail.com.
SMTP Port	To set the port number of outgoing mail server. (Default is 25)
SMTP User Name	The login name of your existing email account. 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. For example: 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.

SMS Control

It allows the endpoint to send some specific KEY WORDS and corresponding PASSWORD in response to operate the gateway. SMS is case-sensitive. In default, this function is disabled.

Figure 6-1-4 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 6-1-4 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 config 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.
--	---

HTTP to SMS

Figure 6-1-5 HTTP to SMS Settings

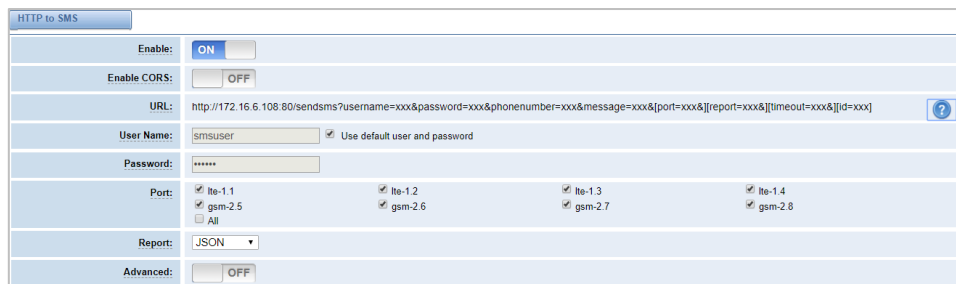


Table 6-1-5 Definition of HTTP to SMS

Options	Definition
Enable	ON (enable), OFF (disable).
Enable CORS	ON (enable), OFF (disable).
Allow Access Origin Domain	Allow source domain names or IPs that can be accessed across domains.
URL	The URL for send sms. Username: the login username for send sms. Password: the login password for send sms. Phone number: the destination telephone number. Message: the SMS contents. Port: the gsm port for send sms. For example: gsm-1.1, gsm-1.2. Report: the sending result report format.

	Timeout: how long to wait.
--	----------------------------

SMS to HTTP

Figure 6-1-6 SMS to HTTP Settings

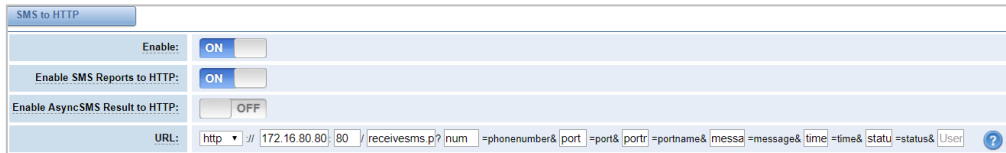


Table 6-1-6 Definition of SMS to HTTP

Options	Definition	Example
host	HTTP server IP address or domain.	172.16.6.171
port	HTTP server port.	80
param1	File path for receiving and processing the SMS data requests.	smsreceive.php
param2	The name of the parameter used to process the 'port' value.	port
param3	The name of the parameter used to process the 'port name' value.	port name
param4	The name of the parameter used to process the ' message ' value.	message
param5	The name of the parameter used to process the ' time ' value.	time

6.2 SMS Sender

Click the box to select the corresponding port number, fill in the target number and SMS content. Then you can send it. Different numbers should be separated by symbols: '\r', '\n', space character, semicolon and comma. After sending a text message, if the SMS status report is enabled, a detailed report of the SMS transmission will be displayed below.

Figure 6-2-1 SMS Sender

Port:	☐ lte-1.1 ☐ gsm-2.5 ☐ All	☐ lte-1.2 ☐ gsm-2.6	☐ lte-1.3 ☐ gsm-2.7	☐ lte-1.4 ☐ gsm-2.8
Flash SMS:	OFF			
Load numbers from text file:	选择文件 未选择任何文件			
Destination Number:	10086 "; semicolon", " vertical Bar", ", comma", " blank ", " : colon ", " . dot " were treated as separators in Destination Number List			
Message:	ye			
Action:	Send Stop			

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 6-3-1 SMS Inbox

Port	Phone Number	Time	Message Keywords
all		from to	
Filter Clean Filter			
Total Records: 170			
Port	Phone Number	Time	Message
gsm-7.27	10086	2019/04/02 12:03:33	【好网选移动，流量放心用！，猛戳 dx.10086.cn/bx1k05】尊敬的客户：您当前账户余额25.50元，下一个月结日为2019年04月22日。如需充值可点击 http://gd.10086.cn/cz 。【0元领副卡获赠10G流量： http://dx.10086.cn/yTFvY3a 】【中国移动】
gsm-7.25	10086	2019/04/02 12:03:32	【好网选移动，流量放心用！，猛戳 dx.10086.cn/bx1k05】尊敬的客户：您当前账户余额30.00元，下一个月结日为2019年04月05日。如需充值可点击 http://gd.10086.cn/cz 。【0元领副卡获赠10G流量： http://dx.10086.cn/yTFvY3a 】【中国移动】
gsm-7.28	10086	2019/04/02 12:03:32	尊敬的客户：您已欠费4.40元，已被停机。如需充值可点击 http://gd.10086.cn/cz 。【中国移动】
gsm-7.26	10086	2019/04/02 12:03:32	尊敬的客户：您已欠费1.04元，已被停机。如需充值可点击 http://gd.10086.cn/cz 。【中国移动】
lte-4.15	10086	2019/04/02 12:03:30	【好网选移动，流量放心用！，猛戳 dx.10086.cn/bx1k05】尊敬的客户：您当前账户余额23.51元，下一个月结日为2019年04月28日。如需充值可点击 http://gd.10086.cn/cz 。【0元领副卡获赠10G流量： http://dx.10086.cn/yTFvY3a 】【中国移动】
lte-4.14	10086	2019/04/02 12:03:30	【好网选移动，流量放心用！，猛戳 dx.10086.cn/bx1k05】尊敬的客户：您当前账户余额38.20元，下一个月结日为2019年04月05日。如需充值可点击 http://gd.10086.cn/cz 。【0元领副卡获赠10G流量： http://dx.10086.cn/yTFvY3a 】【中国移动】
lte-4.13	10086	2019/04/02 12:03:30	尊敬的客户：您已欠费3.60元，已被停机。如需充值可点击 http://gd.10086.cn/cz 。【中国移动】
lte-4.15	10086055	2019/04/02 09:33:21	尊敬的客户，感谢您一直以来对我司的支持，诚邀您体验我司88元畅享套餐尊享计划优惠。此套餐优惠仅需88元，即可获得一年内每月60GB国内通用流量+2000分钟国内通话分钟数。基本相当于只需支付88元/月，即可语音流量任性用。此优惠仅限受邀客户办理，数量有限办完即止，赶快点击 http://dx.10086.cn/2FFB88 抢购吧。优惠名额有限，欲购从速。如有疑问请咨询10086。【中国移动】
lte-4.13	10086	2019/04/01 11:34:31	尊敬的客户：截止01日04:56，您的号码账户余额为0元，尚需缴费3.60元，号码现已暂停使用。支付宝自动充可享充值优惠，打开支付宝APP-充值中心-自动充办理，戳此链接马上办理： http://dx.10086.cn/duanxin1 。【中国移动】
lte-4.13	10086	2019/04/01 11:10:54	尊敬的客户：04月01日因您账户余额不足扣取月结日所需扣费用5.00元，月结扣费失败导致欠费停机，为保障您的通讯服务不受影响，请及时充值开机。支付宝自动充可享充值优惠，打开支付宝APP-充值中心-自动充办理，戳此链接马上办理： http://dx.10086.cn/duanxin1 。【中国移动】
1 2 3 4 5 6 7 8 9 10 11 17 / 17 go			
Delete Clean Up Export			

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 6-4-1 SMS Outbox

Port

all

Phone Number

Time

from

to

Message Keywords

Filter

Clean Filter

Total Records: 105

	Port	Phone Number	Time	Status	Message
☐	gsm-7.27	10086	2019-04-02 14:41:15	DELIVERD	ye
☐	gsm-7.28	10086	2019-04-02 14:41:00	DELIVERD	ye
☐	gsm-7.25	10086	2019-04-02 14:41:00	DELIVERD	ye
☐	gsm-3.9	10086	2019-04-02 14:41:00	DELIVERD	ye
☐	gsm-7.26	10086	2019-04-02 14:40:59	DELIVERD	ye
☐	lte-4.14	10086	2019-04-02 14:40:52	DELIVERD	ye
☐	lte-4.15	10086	2019-04-02 14:40:52	DELIVERD	ye
☐	lte-4.13	10086	2019-04-02 14:40:47	DELIVERD	ye
☐	lte-4.16	10086	2019-04-02 14:40:47	DELIVERD	ye
☐	gsm-7.25	10086	2019-04-02 14:35:55	DELIVERD	ye

1

2

3

4

5

6

7

8

9

10

11

▶

1 / 11

go

Delete

Clean Up

Export

6.5 SMS Forwarding

Using this function, you can forward incoming SMS to your mobile. You can click

New Routing

button to add new routing. For example:

Figure 6-5-1 SMS Forwarding

Routing Name	Type	Policy	From_Members	To_Members	To Number	Actions
forward	module	ascending	lte-1.1,lte-1.2	lte-1.3,lte-1.4	13923704563	 

SMS received by lte-1.1 and lte-1.2, will be transferred to phone number 13923704563 through lte-1.3 or lte-1.4.

Figure 6-5-2 Create a Routing

Routing Groups	
Routing Name:	forward
Type:	MODULE
Policy:	Ascending
From Members	NO. 1 ☒ lte-1.1 2 ☒ lte-1.2 3 ☐ lte-1.3 4 ☐ lte-1.4 5 ☐ gsm-2.5 6 ☐ gsm-2.6 7 ☐ gsm-2.7 8 ☐ gsm-2.8
To Members	NO. 1 ☐ lte-1.1 2 ☐ lte-1.2 3 ☒ lte-1.3 4 ☒ lte-1.4 5 ☐ gsm-2.5 6 ☐ gsm-2.6 7 ☐ gsm-2.7 8 ☐ gsm-2.8
To Number:	13923704563

For "Ascending" Policy, if you choose 2 or more ports members, it will use first available port to transfer SMS. For this case, if lte-1.3 is available, it will always use lte-1.3 to transfer SMS; otherwise, it will use lte-1.4 to transfer SMS.

7. Network

7.1 LAN Settings

There are three types of LAN port IP: Factory, Static, and DHCP. The Factory is the default type with an IP of 172.16.98.1. This page is not editable when the LAN IPv4 type is selected as "Factory".

DNS Servers: A list of DNS IP address. Basically this info is from your local network service provider.

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 7-1-1 LAN Settings

LAN IPv4	
Interface:	eth0
Type:	Static ▼
MAC:	A0:98:05:0A:2D:F7

IPv4 Settings	
Address:	172.16.6.108
Netmask:	255.255.0.0
Default Gateway:	172.16.0.1

DNS Servers	
DNS Server 1:	8.8.8.8
DNS Server 2:	
DNS Server 3:	
DNS Server 4:	

Reserved Access IP	
Enable:	☐ OFF

Table 7-1-1 Definition of LAN Settings

Options	Definition
Interface	The name of the 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 Address	Physical address of your network interface.
IP Address	The IP address of your gateway.
Netmask	The subnet mask of your gateway.
Default Gateway	Default gateway IP address.

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 7-2-1 WAN Settings

WAN IPv4	
Interface:	eth1
Type:	DHCP ▼
MAC:	00:E0:4C:36:01:8F

7.3 VPN Settings

The wireless gateway provides PPTP and N2N VPN connections, which allow users to establish virtual private networks, encrypt communications, and achieve remote access.

Figure 7-3-1 PPTP VPN Settings

VPN Settings	
VPNType:	PPTP VPN ▼
PPTP VPN Settings	
Server:	172.16.8.136
Account:	
Password:	
Use MPPE:	☒
* Connection Status:	Failed to connect
Save	

Figure 7-3-2 N2N VPN Settings

VPN Settings	
VPNType:	N2N VPN ▼ PPTP VPN N2N VPN None
N2N VPN Settings	
Enable:	ON ☐
Server Address:	
Port:	
Local IP:	
Subnet Mask:	
User Name:	
Password:	
* Connection Status:	Failed to connect

7.4 DDNS Settings

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

Figure 7-4-1 DDNS Settings

DDNS Settings	
DDNS	ON ☐
Type:	inadyn ▼
User Name:	admin
Password:	*****
Your domain:	www.internet.site.com

Table 7-4-1 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.

7.5 Toolkit

Some tools for checking network connections are provided, Ping commands and route tracking are supported in the web user interface. You can set the source/destination host address, port, and protocol to capture network packets.

Figure 7-5-1 Toolkit

The screenshot displays the 'Toolkit' section of a web interface. At the top, there's a 'GSM IP' dropdown set to '172.16.6.108'. Below it are two input fields for 'www.openvox.cn' with 'Ping' and 'Traceroute' buttons. A 'Channel Recording' tab is active. The configuration section includes: 'Interface' set to 'eth0', empty 'Source host' and 'Destination host' fields, an empty 'Port' field, and 'Protocol' set to 'All'. A 'Start' button is present. The 'Report' section shows the command 'ping -I 172.16.6.108 -c 4 www.openvox.cn' and its output: 'PING www.openvox.cn (104.233.238.106) from 172.16.6.108: 56 data bytes' followed by four successful ping responses with times around 173ms. A summary line states '4 packets transmitted, 4 packets received, 0% packet loss' and 'round-trip min/avg/max = 172.117/173.026/173.900 ms'. The 'Result' section shows 'Successfully ping [www.openvox.cn]'.

GSM IP: 172.16.6.108
www.openvox.cn Ping
www.openvox.cn Traceroute
Channel Recording
Interface: eth0
Source host:
Destination host:
Port:
Protocol: All
Start
Report
ping -I 172.16.6.108 -c 4 www.openvox.cn
PING www.openvox.cn (104.233.238.106) from 172.16.6.108: 56 data bytes
64 bytes from 104.233.238.106: seq=0 ttl=51 time=172.644 ms
64 bytes from 104.233.238.106: seq=1 ttl=51 time=173.446 ms
64 bytes from 104.233.238.106: seq=2 ttl=52 time=173.900 ms
64 bytes from 104.233.238.106: seq=3 ttl=52 time=172.117 ms
--- www.openvox.cn ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 172.117/173.026/173.900 ms
Result
Successfully ping [www.openvox.cn]

7.6 Firewall Settings

Figure 7-6-1 Firewall Settings

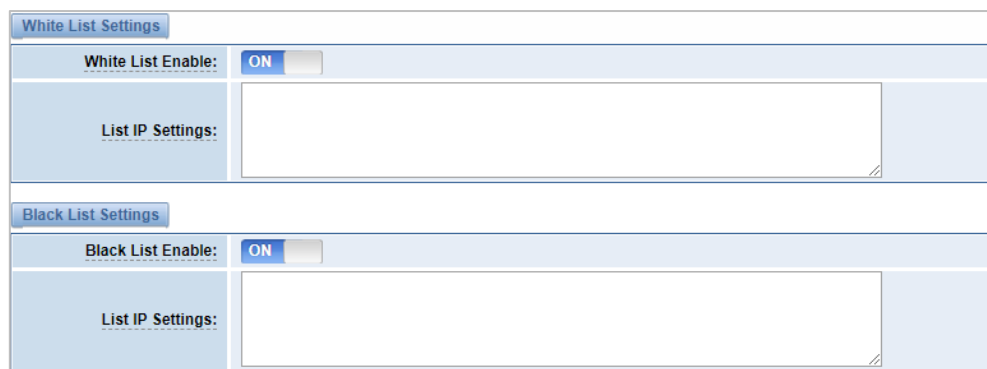


The screenshot shows the 'Firewall Settings' tab. It contains two settings: 'Firewall Enable' and 'Ping Enable'. Both settings have a toggle switch set to 'ON'.

Table 7-6-1 Definition of Firewall Settings

Options	Definition
Firewall Enable	If you want to use White/Black List, and security rules, you must enable this option.
Ping Enable	Whether to enable the Ping function. If the status is OFF: disable ping, the gateway does not allow ping.

Figure 7-6-2 White/Black List Settings



The screenshot shows the 'White List Settings' and 'Black List Settings' tabs. Each tab has a 'List IP Settings' text area. The 'White List Enable' and 'Black List Enable' toggle switches are both set to 'ON'.

Table 7-6-2 Definition of White/Black List Settings

Options	Definition
White/Black List Enable	To enable White/Black list or not.
List IP	IP is separated only by "," character.

7.7 Security Rules

Figure 7-7-1 Security Rules Settings

Rule Name	Type	Protocol	IP	Port	Actions
SIP	UDP	DROP	172.16.8.0/255.255.0.0	5060:5060	 
RTP	TCP	ACCEPT	172.16.8.0/255.255.0.0	10000:20000	 

Security Rules

Rule Name:	SIP				
Protocol:	UDP ▼				
Port:	5060		5060		
IP / MASK:	172.16.8.0		255.255.0.0		
Actions:	DROP ▼				

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 7-7-2 Security Rules Apply

Firewall Rules Apply

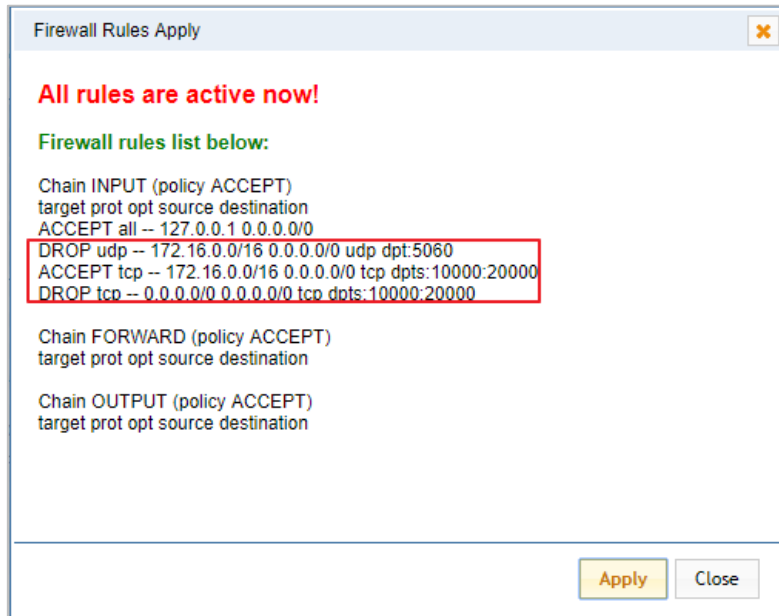
Warning:
Please check your security rules carefully before apply!!!
Wrong rules will cause abnormal behavior on gateway!

Apply Tips:
If your security rules will result in no response on web login, all rules will be deactivated.
You can login gateway and check the rules again after 1 minute.
Otherwise, they will be applied successfully.

Notice:
58 seconds later, all rules will be deactivated.
The dialog will close automatically, when the time runs out.

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

Figure 7-7-3 Figure 7-11 Security Rules Apply



7.8 SIP Capture

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

Figure 7-8-1 SIP Capture

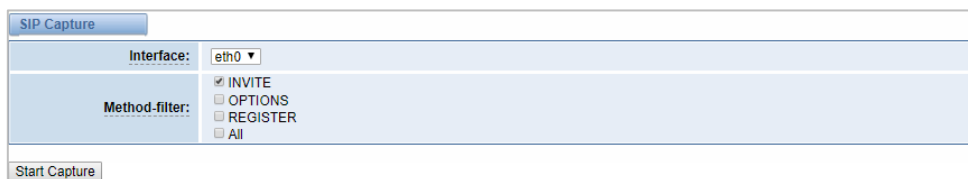


Table 7-8-1 SIP Capture Settings

Options	Definition
Interface	You can choose eth0, eth1 or eth0:0.
Method-filter	You can choose INVITE, OPTIONS, REGISTER or ALL.

8. Advances

8.1 Asterisk API

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

Figure 8-1-1 Asterisk API

General		
Enable:	☒ ON	
Port:	5038	
Manager		
Manager Name:	admin	
Manager secret:	NS1hPs2d	
Deny:		
Permit:		
Rights		
System:	read: ☒	write: ☒
Call:	read: ☒	write: ☒
Log:	read: ☒	write: ☒
Verbose:	read: ☒	write: ☒
Command:	read: ☐	write: ☒
Agent:	read: ☒	write: ☒
User:	read: ☒	write: ☒
Config:	read: ☒	write: ☒
DTMF:	read: ☒	write: ☐
Reporting:	read: ☒	write: ☒
CDR:	read: ☒	write: ☐
Dialplan:	read: ☒	write: ☐
Originate:	read: ☐	write: ☒
All:	read: ☒	write: ☒

Table 8-1-1 Definition of Asterisk API

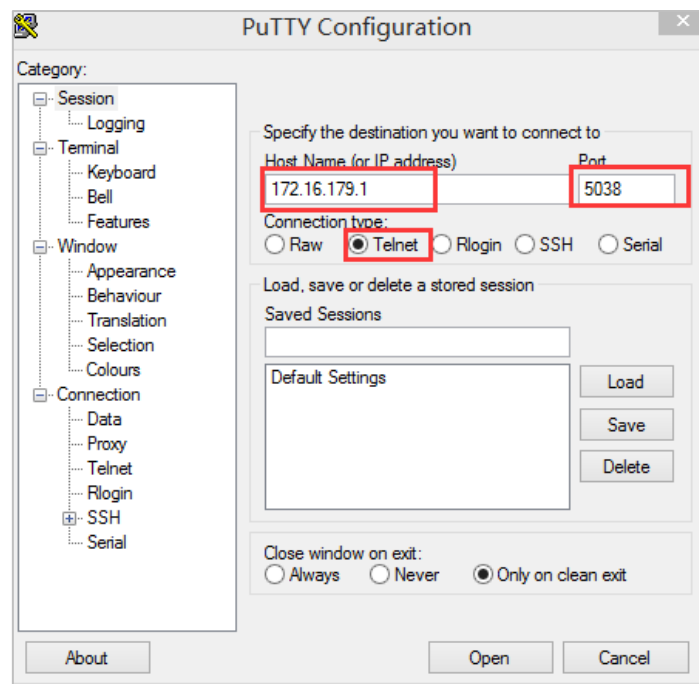
Options	Definition
Port	Network port number.
Manager Name	Name of the manager without space.
Manager secret	Password for the manager. Allowed characters: “-_.<>&0-9a-zA-Z”. Length: 4-32 characters.

Deny	If you want to deny some hosts or networks, you can use char & as separator. For example: 192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0.
Permit	If you want to permit some hosts or networks, you can use char & as separator. For example: 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	The information about channels and the setting information of the channel in use.
Log	Logging information.
Verbose	Verbose information.
Command	Permission to run CLI commands. Write-only.
Agent	The information about queues and agents and the ability to add queue members to a queue.
User	Permission to send and receive User Event.
Config	Ability to read and write configuration files.
DTMF	Receive DTMF events. Read-only.
Reporting	The ability to get information about the system.
CDR	Call records. Read-only.
Dialplan	Receive NewExten and Varset events. Read-only.

Originate	Permission to initiate new calls. Write-only.
All	Select all or deselect all.

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 8-1-2 Telnet Access Gateway API



8.2 Asterisk CLI

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

Figure 8-2-1 Asterisk CLI

Asterisk CLI

Command:

Output:

GSM span 1: Power off, Provisioned, Down, Active, Standard
GSM span 2: Power on, Provisioned, Up, Active, Standard
GSM span 3: Power on, Provisioned, Undetected SIM Card, Active, Standard
GSM span 4: Power on, Provisioned, Undetected SIM Card, Active, Standard
GSM span 5: Power on, Provisioned, Undetected SIM Card, Active, Standard
GSM span 6: Power on, Provisioned, Undetected SIM Card, Active, Standard
GSM span 7: Power on, Provisioned, Undetected SIM Card, Active, Standard
GSM span 8: Power on, Provisioned, Undetected SIM Card, Active, Standard

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 shell command.

8.3 Asterisk File Editor

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

Figure 8-3-1 Asterisk File Editor

Configuration Files

File Name	File Size
asterisk.conf	275
cdr.conf	572
cdr_syslog.conf	364
chan_extra.conf	56
dnsmgr.conf	245
dso.conf	1520
extensions.conf	120
extensions_custom.conf	0
extensions_macro.conf	5114
extensions_routing.conf	4054

1 2 3 4 ▶ 1 / 4 go

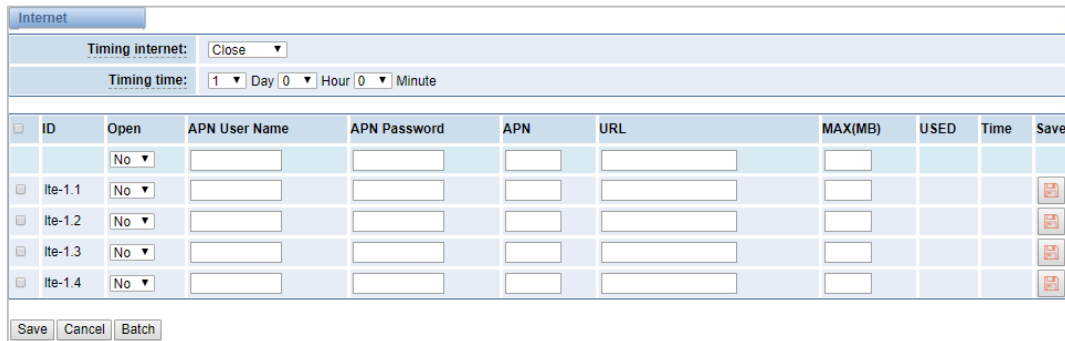
Click to create a new configuration file. After editing or creating, you should reload Asterisk.

8.4 Internet

In order to meet the requirements of some operators Package consumption flow, we provide Internet access which can be set in batches (This function is only available on

the LTE module currently. Other hardware does not support the Internet function at this time).

Figure 8-4-1 Asterisk Internet



8.5 Cloud Management

SWG and VoxStack series gateways both support OpenVox Cloud Management.

Figure 8-5-1 OpenVox Cloud Management



If your device is connected to the cloud management, the SSH and the 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 which can provide you with efficient and excellent service and experience.

Table 8-5-1 Definition of Cloud Management

Options	Definition
Enable Cloud Service	Turn on/off the 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	Whether currently connected to the cloud management platform or not.

8.6 Balance

The wireless gateway provides a balance inquiry function for users who use the SIM card in batches, it can automatically send a short message to the operator to query the current balance on the SIM card, which is convenient, fast and accurate.

Figure 8-6-1 Balance

Port	Query Type	Destination Number	Receive Number	Send Message	Matching Key	Balance	Actions
lte-1.1	SMS	10086	10086	ye	余额		
lte-1.2	SMS	10086	10086	ye	余额		
lte-1.3	SMS	10086	10086	ye	余额		
lte-1.4	SMS	10086	10086	ye	余额		
gsm-2.5	SMS	10086	10086	ye	余额		
gsm-2.6	SMS	10086	10086	ye	余额		
gsm-2.7	SMS	10086	10086	ye	余额		
gsm-2.8	SMS	10086	10086	ye	余额		

Figure 8-6-2 Balance Settings

Port lte-1.1

Query Switch: ☒ ON

Query Type: SMS

Destination Number: 10086

Receive Number: 10086

Send Message: ye

Matching Key: 余额

Registered Query: ☐ OFF

Interval: 0 Minute

Call Count Query: 0

Decimal mark: .

Kilo mark: .

The matching test

Message content: 【好网速移动，流量放心用！，猛戳 dx.10086.cn/bx1k05】尊敬的客户：您当前账户余额30.00元，下一个月结日为2019年04月05日。如需充值可点击：//gd.10086.cn/CZ。【0元领副卡获赠10G流量：http://dx.10086.cn/yjFvT3q】【中国移动】

Matching results: Test 30.00

Save To Other Ports

8.7 Phone Number

The wireless gateway also provides a number inquiry function, which can automatically send a short message to the operator to query the number of the SIM card that you use currently.

Figure 8-7-1 Phone Number

Port	Query Type	Destination Number	Receive Number	Send Message	Matching Key	PhoneNumber	Actions
lte-1.1	SMS	10086	10086	BJ	号码		
lte-1.2	SMS	10086	10086	BJ	号码		
lte-1.3	SMS	10086	10086	BJ	号码		
lte-1.4	SMS	10086	10086	BJ	号码		
gsm-2.5	SMS	10086	10086	BJ	号码		
gsm-2.6	SMS	10086	10086	BJ	号码		
gsm-2.7	SMS	10086	10086	BJ	号码		
gsm-2.8	SMS	10086	10086	BJ	号码		

Figure 8-7-2 Phone Number

Query Switch: ☒ ON

Query Type: SMS

Destination Number: 10086

Receive Number: 10086

Send Message: BJ

Matching Key: 号码

The matching test

Message content:

Matching results: Test

Save To Other Ports

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 are unavailable. Other log pages are the same.

Figure 9-1 Logs Settings

The screenshot shows the 'Logs Settings' page with four main sections: System Logs, Asterisk Logs, SIP Logs, and IAX2 Logs. Each section has a 'System Logs' toggle and an 'Auto clean' toggle with a 'maxsize' dropdown.

Section	System Logs	Auto clean	maxsize
System Logs	ON	ON	1MB
Asterisk Logs	OFF	ON	100KB
SIP Logs	OFF	ON	100KB
IAX2 Logs	OFF	ON	100KB

Table 9-1 Definition of Logs

Options	Definition
System Logs	Whether to enable the system logs or not
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 and the new logs will be retained; Switch off: logs will remain, and the file size will increase gradually. The default is on, the default maxsize is 1MB.
SIP Logs	Whether to open the sip logs or not
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 and the new logs will be retained;

	Switch off: logs will remain, and the file size will increase gradually. The default is on, the default maxsize is 100KB.
IAX Logs	Whether to open the IAX logs or not
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 and the new logs will be retained; Switch off: logs will remain, and the file size will increase gradually. The default is on, the default maxsize is 100KB.
Call Detail Record	Show Call Detail Records for each channel.
Append IMEI	Switch on: IMEI will be appended to the CDR gsm channel in 'From' or 'To'. Switch off: No appended IMEI. The default is off.
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 and the new logs will be retained; Switch off: logs will remain, and the file size will increase gradually. The default is on, the default maxsize is 10MB.

With the Syslog software, the gateway's logs and CDRs can be monitored and stored locally on the PC.

Figure 9-2 Logs Settings

Syslog	
Local Syslog:	☒ ON
Server Address:	
Server Port:	
Syslog Level:	EMERG ▼
CDR Level:	OFF ▼

Figure 9-3 System Logs

System Logs

[2014/01/01 00:01:21]	Power on.
[2019/03/09 18:18:20]	Power on.
[2019/03/09 18:22:22]	Power on.
[2019/03/09 18:26:22]	Power on.
[2019/03/09 18:30:21]	Power on.
[2014/01/01 00:01:21]	Power on.
[2019/03/09 18:38:33]	Power on.
[2019/03/09 18:42:32]	Power on.
[2019/03/09 18:46:27]	Power on.
[2019/03/09 18:50:26]	Power on.
[2014/01/01 00:01:16]	Power on.
[2019/03/09 18:58:29]	Power on.
[2019/03/09 19:02:32]	Power on.
[2014/01/01 00:01:18]	Power on.
[2019/03/09 19:10:35]	Power on.
[2019/03/09 19:14:41]	Power on.
[2019/03/09 19:18:45]	Power on.
[2019/03/09 19:22:36]	Power on.
[2019/03/09 19:26:39]	Power on.
[2014/01/01 00:01:19]	Power on.
[2019/03/09 19:34:48]	Power on.
[2019/03/09 19:38:40]	Power on.
[2014/01/01 00:01:22]	Power on.
[2019/03/09 19:46:46]	Power on.
[2014/01/01 00:01:20]	Power on.
[2019/03/09 19:54:50]	Power on.

Refresh Rate: Off Refresh Clean Up

You can easily browse your CDRs on the Web GUI, you also can delete, clean or export your CDR information.

Figure 9-4 CDR

	Caller ID	Callee ID	From	To	Start Time	Duration	Result
					from to	from to	All
Filter Clean Filter							
Total Records: 33385							
☐	Caller ID	Callee ID	From	To	Start Time	Duration	Result
☐	66376	1028@172.16.33.102	gsm-1.1	1028	1970-01-01 08:04:06	00:01:55	ANSWERED
☐	66389	1028@172.16.33.102	gsm-2.2	1028	1970-01-01 08:01:50	00:01:00	ANSWERED
☐	66390	1028@172.16.33.102	gsm-1.3	1028	1970-01-01 08:02:21	00:00:25	ANSWERED

In the new version we have enriched the LOGS display which you can see each port of the call outbound clearly.

Figure 9-5 GSM Outbound

GSM Outbound									
Port	All Calls	All Durations	Answered	Canceled	Busy	No Answer	No Dialtone	No Carrier	Other
lte-1.1	0	0	0	0	0	0	0	0	0
lte-1.2	0	0	0	0	0	0	0	0	0
lte-1.3	0	0	0	0	0	0	0	0	0
lte-1.4	0	0	0	0	0	0	0	0	0
gsm-2.5	0	0	0	0	0	0	0	0	0
gsm-2.6	0	0	0	0	0	0	0	0	0
gsm-2.7	0	0	0	0	0	0	0	0	0
gsm-2.8	0	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0	0