OpenVox Communication Co Ltd

Analog Gateway User Manual

Version 1.0

OpenVox Communication Co Ltd

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

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

Business Contact: sales@openvox.cn

Technical Support: support@openvox.cn

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

URL: www.openvox.cn

Thank You for Choosing OpenVox Products!

Confidentiality

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

Disclaimer

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

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

Trademarks

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

Revise History

Version	Release Date	Description
1.0	22/12/2017	First Version

Contents

1. Overview

What is Analog Gateway Series?

OpenVox Analog Gateway Series is an open source asterisk-based Analog VoIP Gateway solution for SMBs and SOHOs. With friendly GUI and unique modular design, users may easily setup their customized Gateway. Also secondary development can be completed through AMI (Asterisk Management Interface).

The Modular Design Analog Gateway Series are developed for interconnecting the PSTN networks with a wide selection of codecs and signaling protocol, including G.711A, G.711U, G.729, G.722, G.723, ILBC to quickly reduce communication expenses and maximize cost-savings.

The Analog Gateway Series use standard SIP protocol and compatible with Leading IMS/NGN platform, IPPBX and SIP servers, support most of the VoIP operating platforms such as Asterisk, Elastix, 3CX, FreeSWITCH , Broadsoft etc.

Sample Application

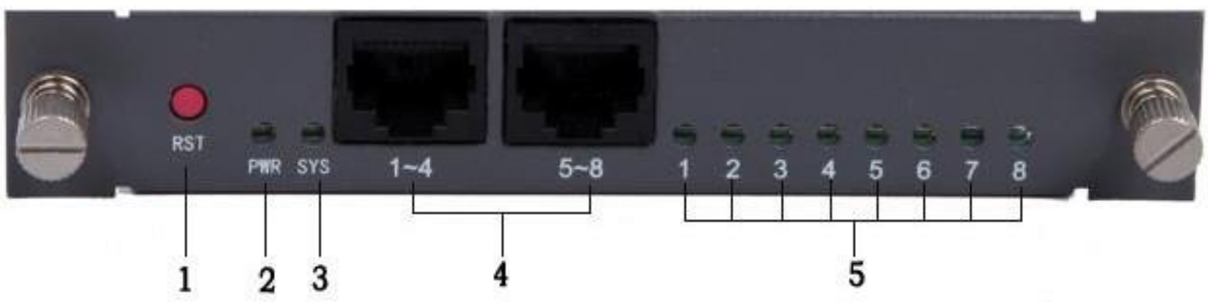
Figure 1-2-1 Topological Graph

Product Appearance

The picture below is appearance of Analog Series Gateway.

Figure 1-3-1 Product Appearance

Figure 1-3-2 Front Panel



1: Reset button

2: Power Indicator

3: System LED

4: Analog Telephone Interface (2)

5: Channels State Indicator

Main Features

➢ Modular design

- Based on Asterisk®
- Editable Asterisk® configuration file
- Support T.38 fax relay and T.30 fax transparent, can continually fax multiple page
- Echo cancellation and Static jitter buffer
- Wide selection of codecs and signaling protocol
- DTMF relay
- Ring cadence and frequency setting
- MWI(Message waiting indicator)
- DHCP , DNS/DDNS, NAT Network
- VAG and CNG
- All hot-swap
- Stable performance, flexible dialing, friendly GUI
- Two-year time warranty

Physical Information

Table 1-5-1 Description of Physical Information

Weight	200g
Size	22cm*2cm*12cm
Temperature	-40~125°C (Storage)
	0~50°C (Operation)
Operation humidity	10%~90% non-condensing
Power source	12V DC/2A
Max power	11W

Software

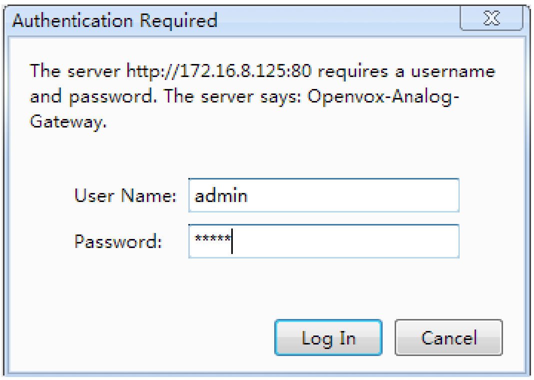
Default IP: 172.16.99.1

Username: admin

Password: admin

Please enter the default IP in your browser to scan and configure the module you want. Now we offer you two RJ45 Network ports to access to your gateway on the board, ETH1 and ETH2. ETH1 only can enter the ip of slot 1, and ETH2 can access every slot. You can choose either of them, that depends on your demand.

Figure 1-6-1 Login Interface



2. System

Status

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

Figure 2-1-1 System Status

Port Information

Port	Name	Type	Line Status/Sip Account	Port Status
1	board-1-port1	FXO	Disconnected	OnHook
2	board-1-port2	FXO	Disconnected	OnHook
3	board-1-port3	FXO	Disconnected	OnHook
4	board-1-port4	FXO	Disconnected	OnHook
5	board-1-port5	FXS	8005	OnHook
6	board-1-port6	FXS	8006	OnHook
7	board-1-port7	FXS	8007	OnHook
8	board-1-port8	FXS	8008	OnHook

SIP Information

Endpoint Name	User Name	Host	Registration	SIP Status	Response Code
9001	9001	172.16.8.250	server	OK	
9002	9002	172.16.8.250	server	OK	
9003	9003	(Unspecified)	server	UNKNOWN	
9004	9004	172.16.8.250	server	OK	
9000	9000	172.16.208.33	client	Registered	200 OK
8005	8005	172.16.208.33	client	Registered	200 OK
8006	8006	172.16.208.33	client	Registered	200 OK
8007	8007	172.16.208.33	client	Registered	200 OK
8008	8008	172.16.208.33	client	Registered	200 OK

Routing Information

Rule Name	From	To

Network Information

Name	MAC Address	IP Address	Mask	Gateway	RX Packets	TX Packets
LAN	A0:98:05:01:51:76	172.16.80.16	255.255.0.0	172.16.0.1	83463	3704

Time

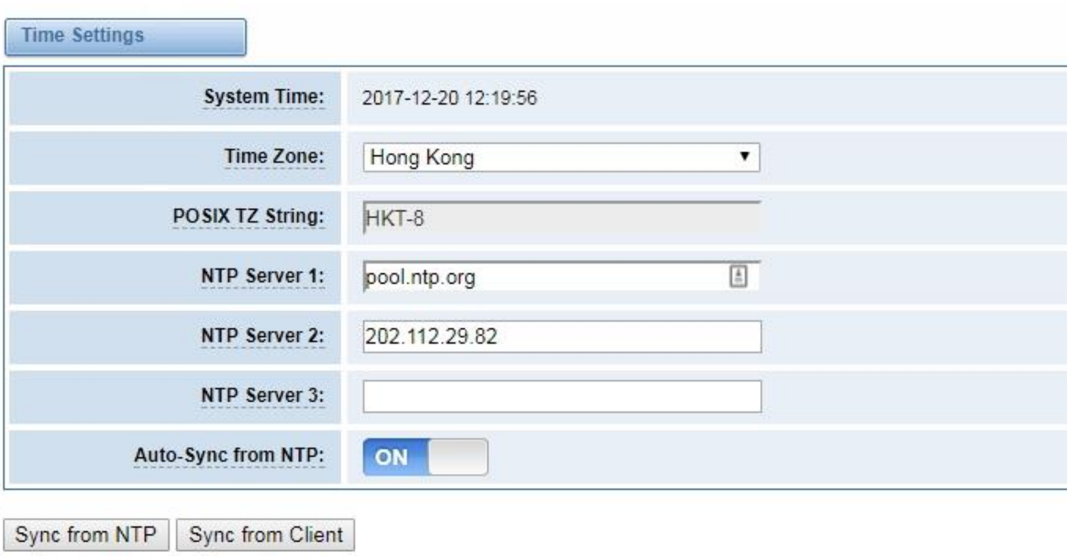
Table 2-2-1 Description of Time Settings

Options	**Definition**
System Time	Your gateway system time.
Time Zone	The world time zone. Please select the one which is the same or the

	closest as your city.
POSIX TZ String	Posix time zone strings.
NTP Server 1	Time server domain or hostname. For example, [time.asia.apple.com].
NTP Server 2	The first reserved NTP server. For example, [time.windows.com].
NTP Server 3	The second reserved NTP server. For example, [time.nist.gov].
Auto-Sync from NTP	Whether enable automatically synchronize from NTP server or not. ON is enable, OFF is disable this function.
Sync from NTP	Sync time from NTP server.
Sync from Client	Sync time from local machine.

For example, you can configure like this:

Figure 2-2-1 Time Settings



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

Login Settings

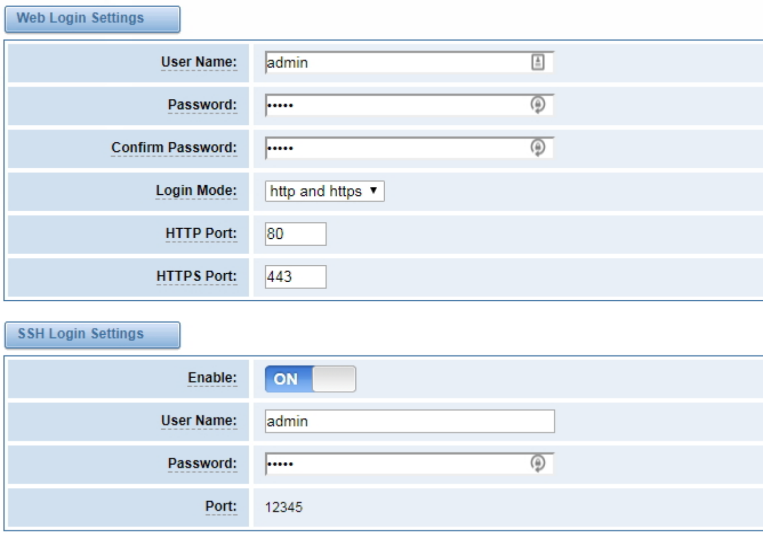
Your gateway doesn't have administration role. All you can do here is to reset what new username and password to manage your gateway. And it has all privileges to operate your gateway. You can modify both your "Web Login

Settings" and "SSH Login Settings". If you have changed these settings, you don't need to log out, just rewriting your new user name and password will be OK.

Table 2-3-1 Description of Login Settings

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

Figure 2-3-1 Login Settings



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

General

Language Settings

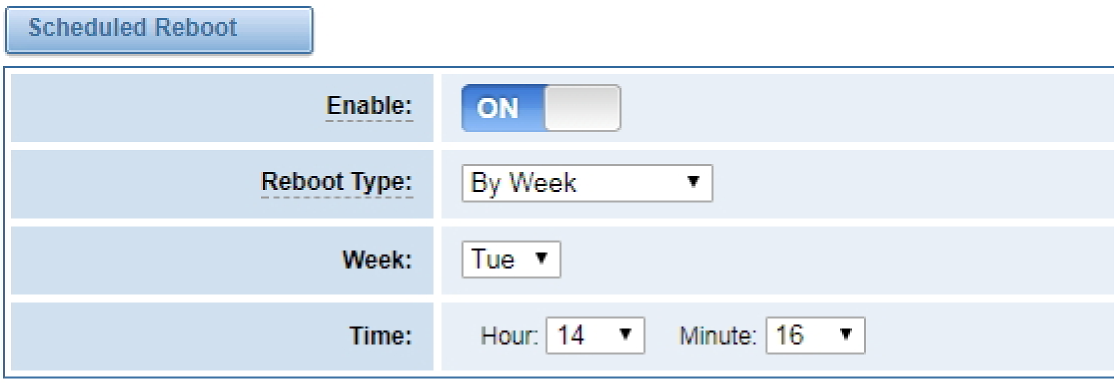
You can choose different languages for your system. If you want to change language, you can switch "Advanced" on, then "Download" your current language package. After that, you can modify the package with the language you need. Then upload your modified packages, "Choose File" and "Add", those will be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

Figure 2-4-1 Language Settings

Scheduled Reboot

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

Figure 2-4-2 Reboot Types



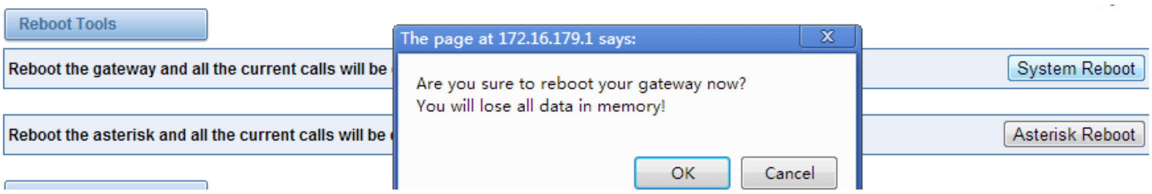
If use your system frequently, you can set this enable, it can helps system work more efficient.

Tools

On the "Tools" pages, there are reboot, update, upload, backup and restore toolkits.

You can choose system reboot and Asterisk reboot separately.

Figure 2-5-1 Reboot Prompt



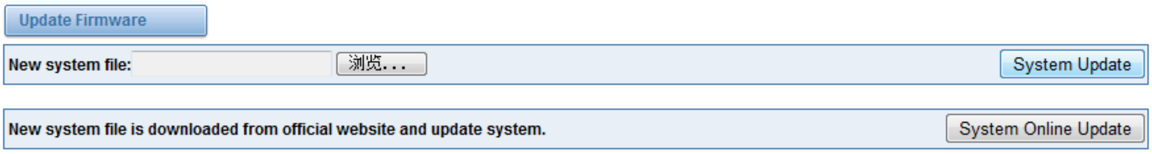
If you press "Yes", your system will reboot and all current calls will be dropped. Asterisk Reboot is the same.

Table 2-5-1 Instruction of reboots

Options	Definition
System Reboot	This will turn off your gateway and then turn it back on. This will drop all current calls.
Asterisk Reboot	This will restart Asterisk and drop all current calls.

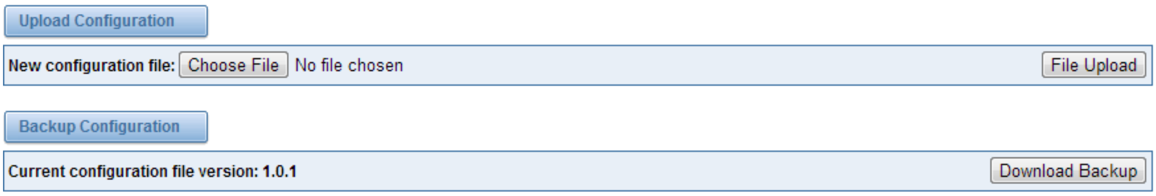
We offer two kinds of update types for you, you can choose System Update or System Online Update. System Online Update is an easier way to update your system.

Figure 2-5-2 Update Firmware



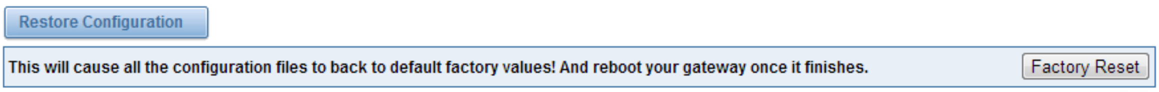
If you want to store your previous configuration, you can first backup configuration, then you can upload configuration directly. That will be very convenient for you. Notice, the version of backup and current firmware should be same, otherwise, it would not take effect.

Figure 2-5-3 Upload and Backup



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

Figure 2-5-4 Factory Reset



Information

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

Figure 2-6-1 System Information

Model Name:	VS-AGU-E2M0800
Software Version:	1.1.14
Hardware Version:	1.0.0
Slot Number:	1
Storage Usage:	1.7M/63.5M (3%)
Memory Usage:	60.3877 % Memory Clean
Build Time:	2017-12-12 16:31:16
Contact Address:	10/F, Building 6-A, Baoneng Science and Technology Industrial Park, Longhua New District, Shenzhen, Guangdong, China 518109
Tel:	+86-755-82535461
Fax:	+86-755-83823074
E-Mail:	support@openvox.cn
Web Site:	www.openvox.cn
System Time:	2017-12-20 13:51:31
System Uptime:	0 days 02:10:41

3. Analog

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

Channel Settings

Figure 3-1-1 Channel System

Port	Type	Name	Line Status/Sip Account	Port Status	Actions
1	FXO	board1-port1	Disconnected	OnHook	
2	FXO	board1-port2	Disconnected	OnHook	
3	FXO	board1-port3	Disconnected	OnHook	
4	FXO	board1-port4	Disconnected	OnHook	
5	FXS	board1-port5	8005	OnHook	
6	FXS	board1-port6	8006	OnHook	
7	FXS	board1-port7	8007	OnHook	
8	FXS	board1-port8	8008	OnHook	

On this page, you can see every port status, and click action  button to configure the port.

Figure 3-1-2 FXO Port Configure

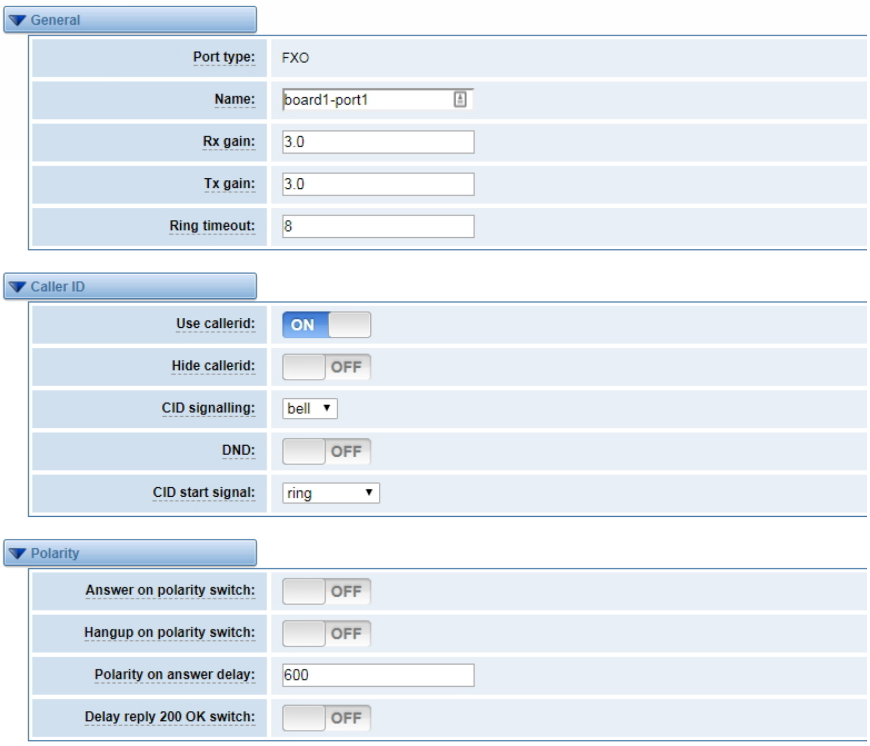
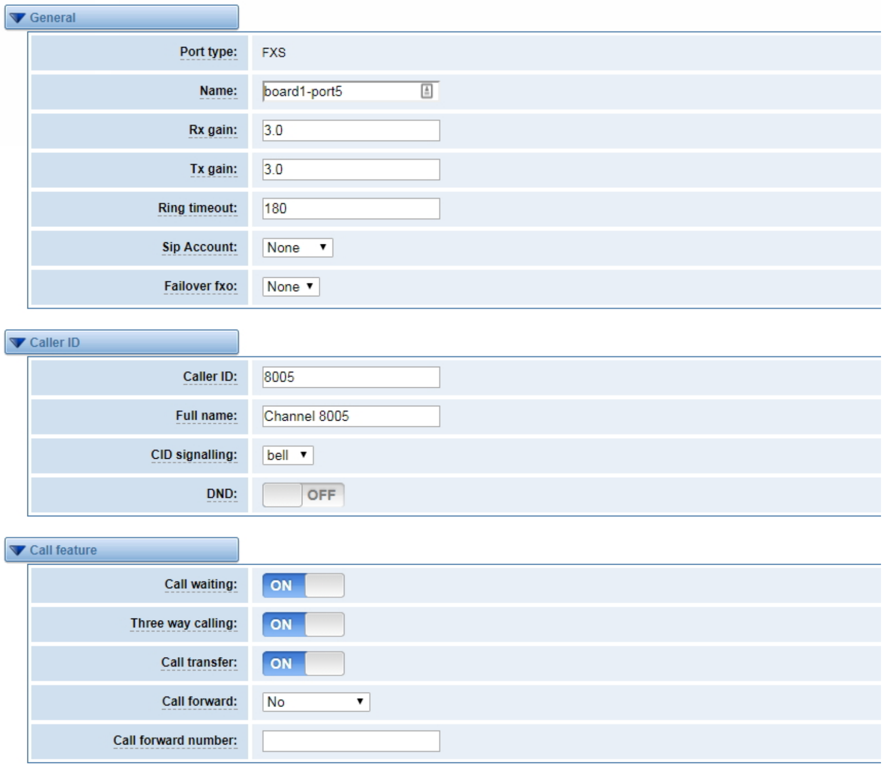


Figure 3-1-3 FXS Port Configure



Pickup Settings

Call pickup is a feature used in a telephone system that allows one to answer someone else's telephone call. You can set the “Time Out” and “Number” parameters either globally or separately for each port. The feature is accessed by pressing a special sequence of numbers which you set as “Number” parameter on the telephone set when it is enabled this function.

Figure 3-2-1 Pickup Configure

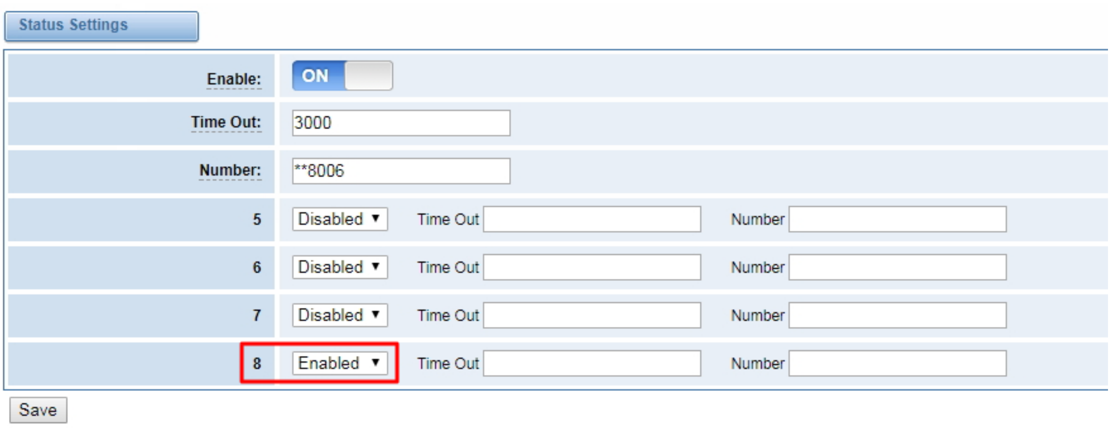


Table 3-2-1 Definition of Pickup

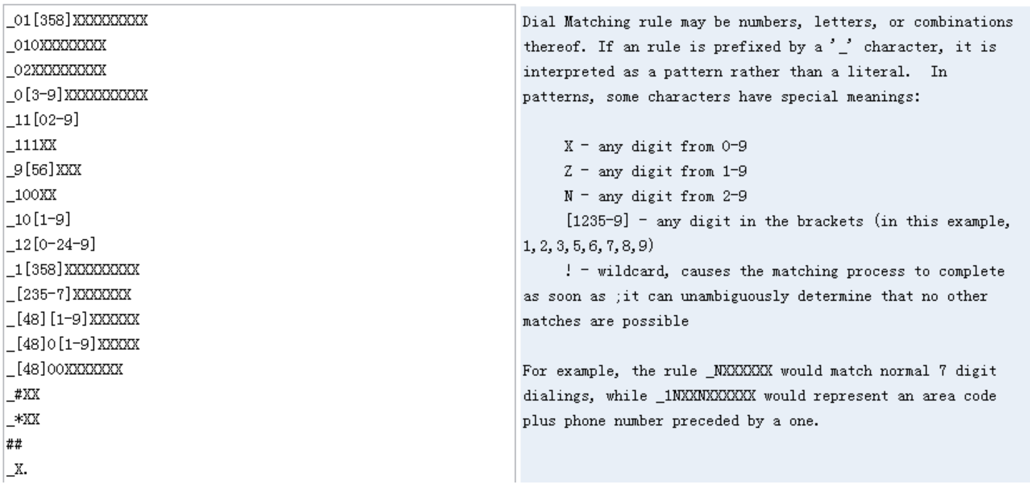
Options	Definition
Enable	ON(enabled),OFF(disabled)
Time Out	Set the timeout, in milliseconds (ms).Note: You can only enter numbers.
Number	Pickup number

Dial Matching Table

Dialing rules is used to effectively judge whether the received number sequence is complete, in order to timely end receiving number and send out number

The correct use of dial-up rules, helps to shorten the turn-on time of phone call

Figure 3-3-1 Port Configure



Advanced Settings

Figure 3-4-1 General Configuration

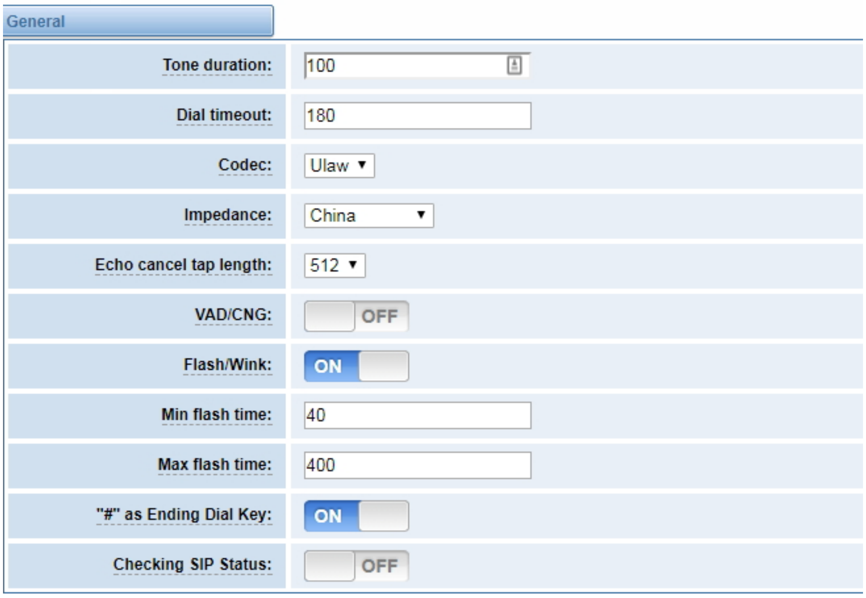


Table 3-4-1 Instruction of General

Options	**Definition**
Tone duration	How long generated tones (DTMF and MF) will be played on the channel. (in milliseconds)
Dial timeout	Specifies the number of seconds we attempt to dial the specified devices.
Codec	Set the global encoding : mulaw, alaw.
Impedance	Configuration for impedance.
Echo cancel tap length	Hardware echo canceler tap length.
VAD/CNG	Turn on/off VAD/CNG.
Flash/Wink	Turn on/off Flash/wink.
Max flash time	Max flash time.(in milliseconds).
“#”as Ending Dial Key	Turn on/off Ending Dial Key.
Checking SIP Status	Turn on/off SIP Account registration status checking.

Figure 3-4-2 Caller ID

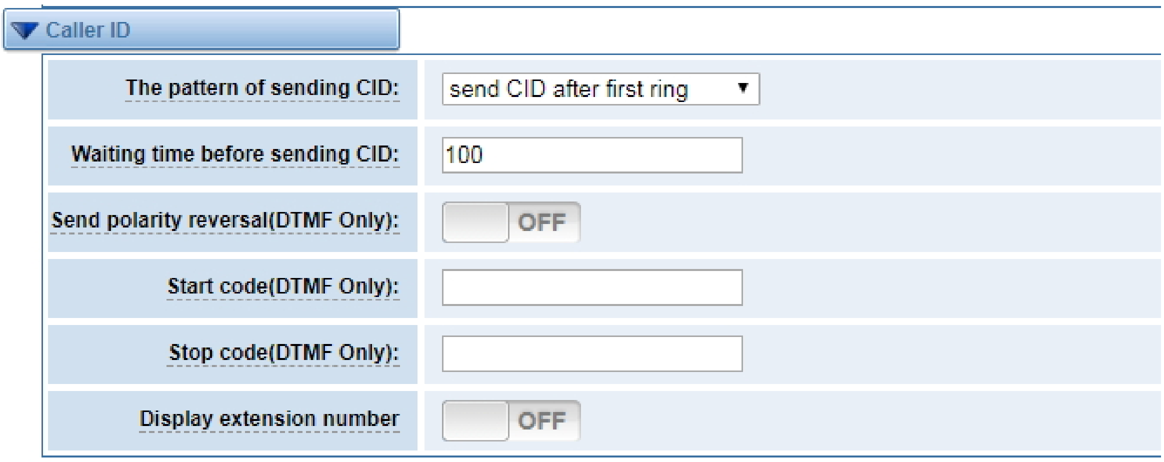


Table 3-4-2 Instruction of Caller ID

Options	Definition
The pattern of sending CID	Some countries(UK) have ring tones with different ring tones(ring-ring), which means the caller ID needs to be set later on, and not just after the first ring, as per the default(1).
Waiting time before sending CID	How long we will waiting before sending the CID on the channel.(in milliseconds).
Sending polarity reversal(DTMF Only)	Send polarity reversal before sending the CID on the channel.
Start code(DTMF Only)	Start code.
Stop code(DTMF Only)	Stop code.

Figure 3-4-3 Hardware Gain

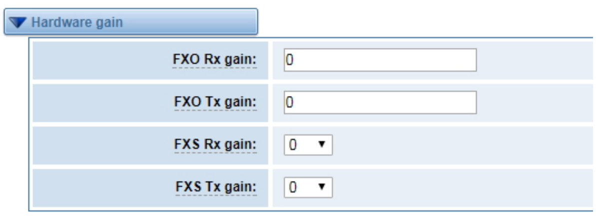


Table 3-4-3 Instruction of Hardware gain

Options	Definition
FXS Rx gain	Set the FXS port Rx gain. Range: from -150 to 120. Select -35, 0 or 35.
FXS Tx gain	Set the FXS port Tx gain. Range: from -150 to 120. Select -35, 0 or 35.

Figure 3-4-4 Fax Configuration

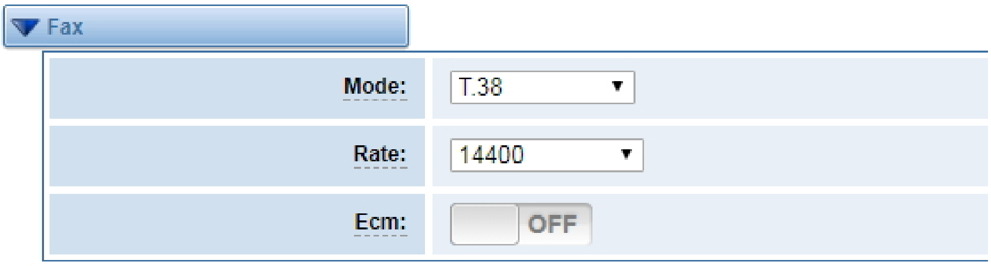


Table 3-4-4 Definition of Fax

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

Figure 3-4-5 Country Configuration

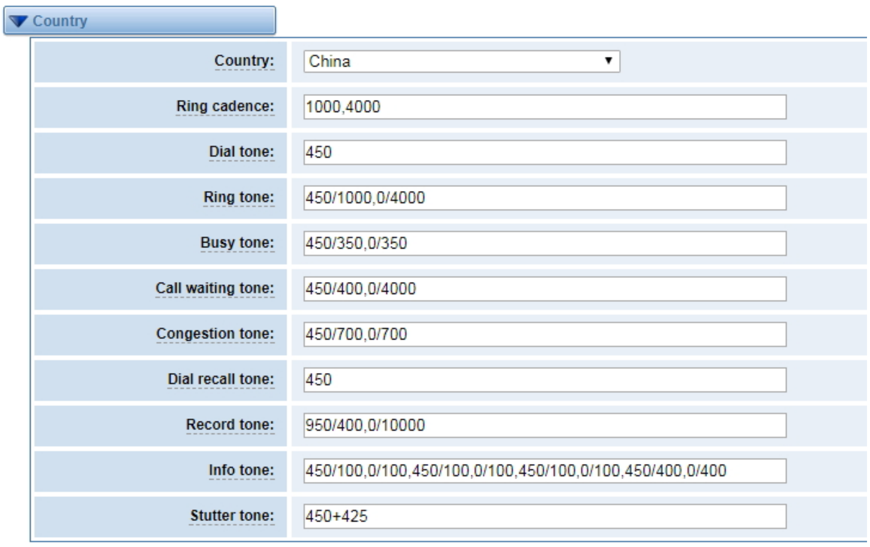
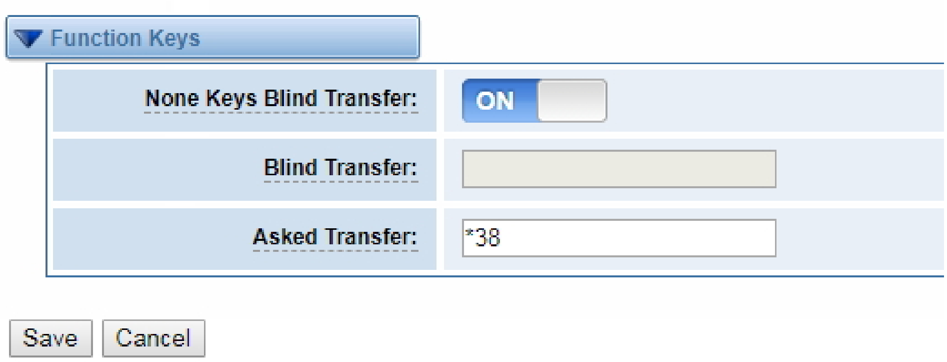


Table 3-4-5 Definition of Country

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

Special Function Keys

Figure 3-5-1 Function keys



4. SIP

SIP Endpoints

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

Figure 4-1-1 SIP Status

	Endpoint Name	Registration	Credentials	Actions
	8000	client	8000@172.16.80.134	
	8001	client	8001@172.16.80.134	
	8002	client	8002@172.16.80.134	
	8003	client	8003@172.16.80.134	
	8004	client	8004@172.16.80.134	
	8005	client	8005@172.16.80.134	
	8006	client	8006@172.16.80.134	
	8007	client	8007@172.16.80.134	

Add New SIP Endpoint Delete

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

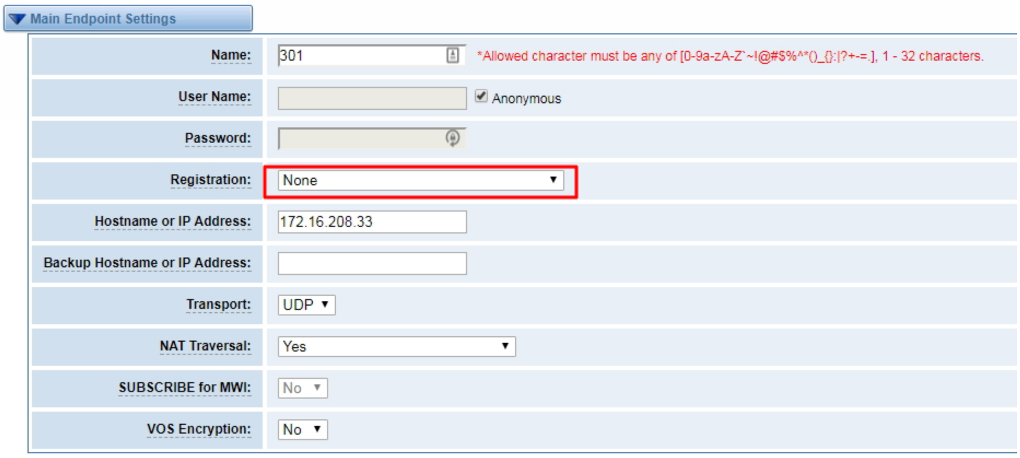
Main Endpoint Settings

There are 3 kinds of registration types for choose. You can choose "Anonymous, Endpoint registers with this gateway or This gateway registers with the endpoint".

You can configure as follows:

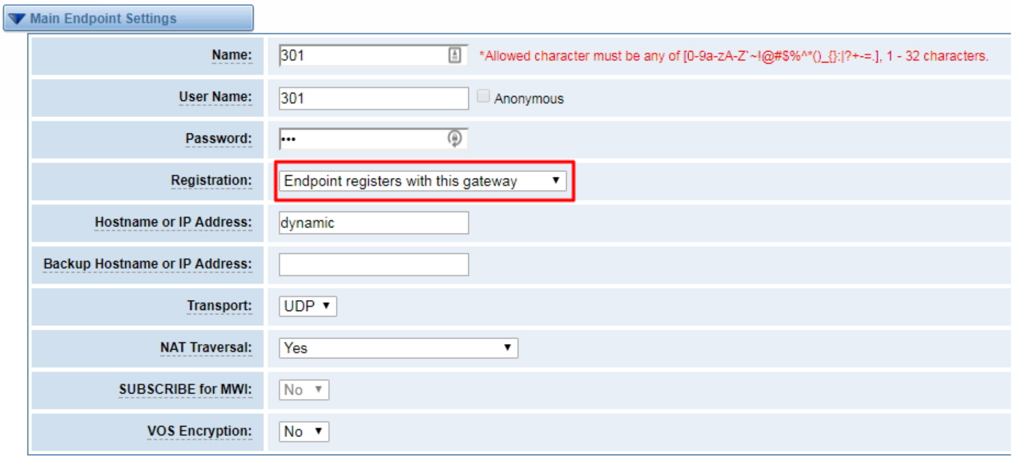
If you set up a SIP endpoint by registration "None" to a server, then you can't register other SIP endpoints to this server. (If you add other SIP endpoints, this will cause Out-band Routes and Trunks confused.)

Figure 4-1-2 Anonymous Registration



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

Figure 4-1-3 Register to Gateway



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

Figure 4-1-4 Register to Server

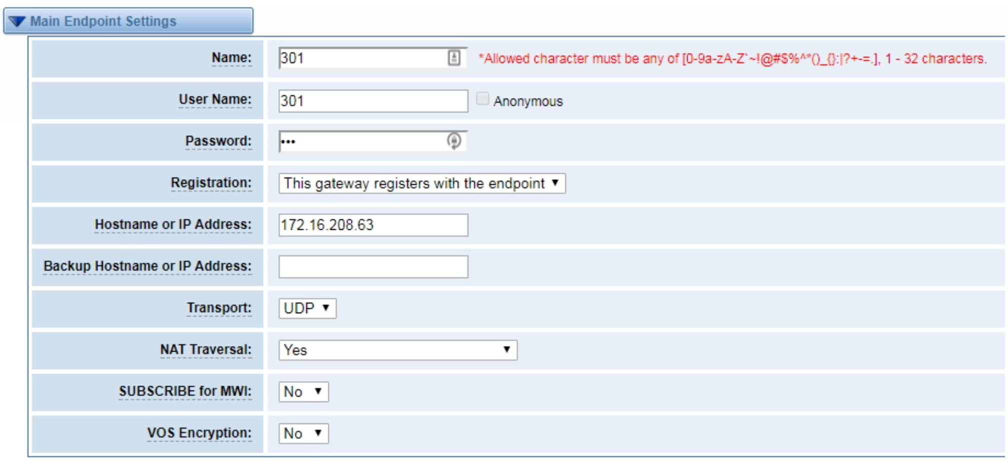


Table 4-1-1 Definition of SIP Options

Options	Definition
Name	A name which is able to read by human. And it's only used for user's reference.
Username	User Name the endpoint will use to authenticate with the gateway.
Password	Password the endpoint will use to authenticate with the gateway. Allowed characters.
Registration	**None**---Not registering; **Endpoint registers with this gateway**---When register as this type, it means the GSM gateway acts as a SIP server, and SIP endpoints register to the gateway; **This gateway registers with the endpoint**---When register as this type, it means the GSM gateway acts as a client, and the endpoint should be register to a SIP server;
Hostname or IP Address	IP address or hostname of the endpoint or 'dynamic' if the endpoint has a dynamic IP address. This will require registration.
Transport	This sets the possible transport types for outgoing. Order of usage, when the respective transport protocols are enabled, is UDP, TCP, TLS. The first enabled transport type is only used for outbound messages until a Registration takes place. During the peer Registration the transport type may change to another supported type if the peer requests so.
NAT Traversal	Addresses NAT-related issues in incoming SIP or media sessions. **No**---Use Rport if the remote side says to use it. **Force Rport on**---Force Rport to always be on. **Yes**---Force Rport to always be on and perform comedia RTP handling. **Rport if requested and comedia**---Use Rport if the remote side says to use it and perform comedia RTP handling.

Advanced: Registration Options

Table 4-1-2 Definition of Registration Options

Options	**Definition**
Authentication User	A username to use only for registration.
Register Extension	When Gateway registers as a SIP user agent to a SIP proxy (provider), calls from this provider connect to this local extension.
From User	A username to identify the gateway to this endpoint.
From Domain	A domain to identify the gateway to this endpoint.
Remote Secret	A password which is only used if the gateway registers to the remote side.
Port	The port number the gateway will connect to at this endpoint.
Quality	Whether or not to check the endpoint's connection status.
Qualify Frequency	How often, in seconds, to check the endpoint's connection status.
Outbound Proxy	A proxy to which the gateway will send all outbound signaling instead of sending signaling directly to endpoints.
Custom Registery	Custom Registery On / Off.
Enable Outboundproxy to Host	Outboundproxy to Host On / Off.

Call Settings

Table 4-1-3 Definition of Call Options

Options	**Definition**
DTMF Mode	Set default DTMF Mode for sending DTMF. Default: rfc2833. Other options: 'info', SIP INFO message (application/dtmf-relay); 'Inband', Inband audio (require 64kbit codec -alaw, ulaw).
Call Limit	Setting a call-limit will cause calls above the limit not to be accepted.

Trust Remote-Party-ID	Whether or not the Remote-Party-ID header should be trusted.
Send Remote-Party-ID	Whether or not to send the Remote-Party-ID header.
Remote Party ID Format	How to set the Remote-Party-ID header: from Remote-Party-ID or from P-Asserted-Identity.
Caller ID Presentation	Whether or not to display Caller ID.

Advanced: Signaling Settings

Table 4-1-4 Definition of Signaling Options

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

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

Advanced: Timer Settings

Table 4-1-5 Definition of Timer Options

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

Maximum Session Refresh Interval	Maximum session refresh interval in seconds. Defaults to 1800secs.
Session Refresher	The session refresher, uac or uas. Defaults to uas.

Media Settings

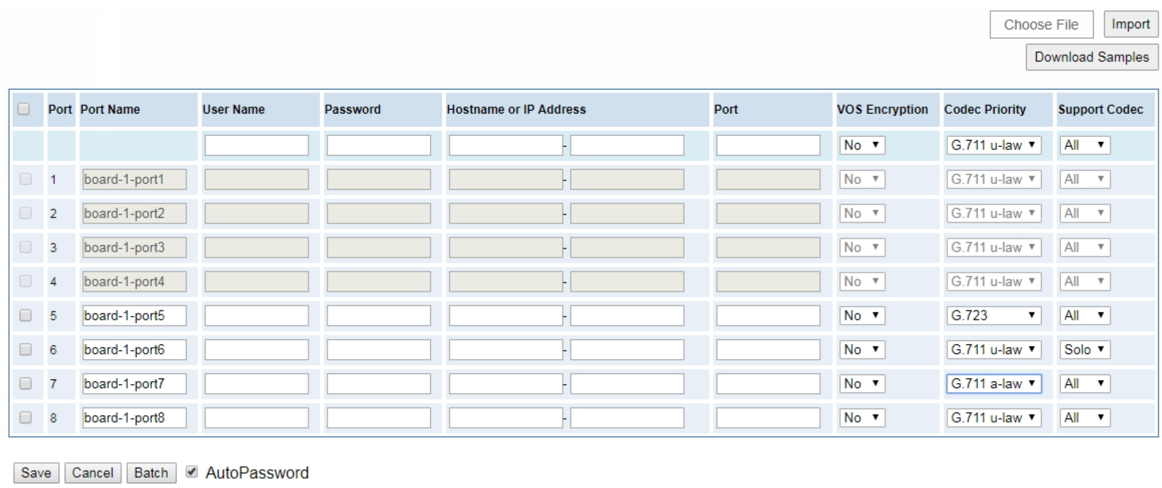
Table 4-1-6 Definition of Media Settings

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

FXS Batch Binding SIP

If you want binding batch Sip accounts to FXS port, you can configure this page. Look out: this is only used when “This gateway registers with the endpoint” work mode.

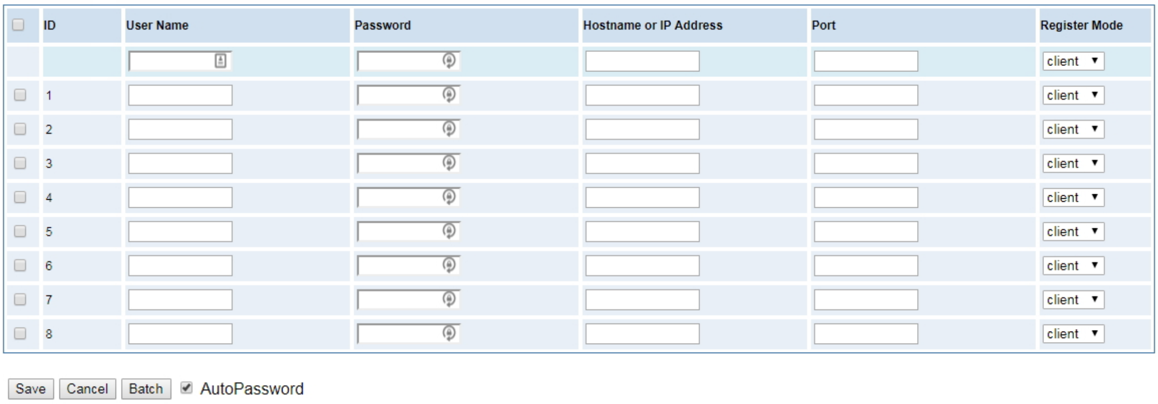
Figure 4-2-1 FXS Batch Binding SIP



Batch Create SIP

If you want add batch Sip accounts, you can configure this page. You can choose all the register mode.

Figure 4-3-1 Batch SIP Endpoints



Advanced SIP Settings

Networking

Table 4-4-1 Definition of Networking Options

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

	outbound calls with suppress SRV lookups for that peer or call.

NAT Settings

Table 4-4-2 Definition of NAT Settings

Options	**Definition**
Local Network	Format:192.168.0.0/255.255.0.0 or 172.16.0.0./12. A list of IP address or IP ranges which are located inside a NATed network. This gateway will replace the internal IP address in SIP and SDP messages with the external IP address when a NAT exists between the gateway and other endpoints.
Local Network List	Local IP address list that you added.
Subscribe Network Change Event	Through the use of the test_stun_monitor module, the gateway has the ability to detect when the perceived external network address has changed. When the stun_monitor is installed and configured, chan_sip will renew all outbound registrations when the monitor detects any sort of network change has occurred. By default this option is enabled, but only takes effect once res_stun_monitor is configured. If res_stun_monitor is enabled and you wish to not generate all outbound registrations on a network change, use the option below to disable this feature.
Match External Address Locally	Only substitute the externaddr or externhost setting if it matches
Dynamic Exclude Static	Disallow all dynamic hosts from registering as any IP address. Used for staticly defined hosts. This helps avoid the configuration error of allowing your users to register at the same address as a SIP provider.
Externally Mapped TCP Port	The externally mapped TCP port, when the gateway is behind a static NAT or PAT
External Address	The external address (and optional TCP port) of the NAT. External Address = hostname[:port] specifies a static address[:port] to be used in SIP and SDP messages.Examples: External Address = 12.34.56.78

	External Address = 12.34.56.78:9900
External Hostname	The external hostname (and optional TCP port) of the NAT. External Hostname = hostname[:port] is similar to External Address. Examples: External Hostname = foo.dyndns.net
Hostname Refresh Interval	How often to perform a hostname lookup. This can be useful when your NAT device lets you choose the port mapping, but the IP address is dynamic. Beware, you might suffer from service disruption when the name server resolution fails.

RTP Settings

Table 4-4-3 Definition of NAT Settings Options

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

Parsing and Compatibility

Table 4-4-4 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	The external hostname (and optional TCP port) of the NAT.

Methods	
Shrink Caller ID	The shrinkcallerid function removes '(', ' ', ')', non-trailing '.', and '-' not in square brackets. For example, the caller id value 555.5555 becomes 5555555 when this option is enabled. Disabling this option results in no modification of the caller id value, which is necessary when the caller id represents something that must be preserved. By default this option is on.
Maximum Registration Expiry	Maximum allowed time of incoming registrations and subscriptions (seconds).
Minimum Registration Expiry	Minimum length of registrations/subscriptions (default 60).
Default Registration Expiry	Default length of incoming/outgoing registration.
Registration Timeout	How often, in seconds, to retry registration calls. Default 20 seconds.
Number of Registration Attempts Enter '0' for unlimited	Number of registration attempts before we give up. 0 = continue forever, hammering the other server until it accepts the registration. Default is 0 tries, continue forever.

Security

Table 4-4-5 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. Realms MUST be globally unique according to RFC 3261. Set this to your host name or domain name.

Use Domain as Realm	Use the domain from the SIP Domains setting as the realm. In this case, the realm will be based on the request 'to' or 'from' header and should match one of the domain. Otherwise, the configured 'realm' value will be used.
Always Auth Reject	When an incoming INVITE or REGISTER is to be rejected, for any reason, always reject with an identical response equivalent to valid username and invalid password/hash instead of letting the requester know whether there was a matching user or peer for their request. This reduces the ability of an attacker to scan for valid SIP usernames. This option is set to 'yes' by default.
Authenticate Options Requests	Enabling this option will authenticate OPTIONS requests just like INVITE requests are. By default this option is disabled.
Allow Guest Calling	Allow or reject guest calls (default is yes, to allow). If your gateway is connected to the Internet and you allow guest calls, you want to check which services you offer everyone out there, by enabling them in the default context.

Media

Table 4-4-6 Instruction of Media

Options	Definition
Premature Media	Some ISDN links send empty media frames before the call is in ringing or progress state. The SIP channel will then send 183 indicating early media which will be empty - thus users get no ring signal. Setting this to "yes" will stop any media before we have call progress (meaning the SIP channel will not send 183 Session Progress for early media). Default is 'yes'. Also make sure that the SIP peer is configured with progressinband=never. In order for 'noanswer' applications to work, you need to run the progress()

	application in the priority before the app.
TOS for SIP Packets	Sets type of service for SIP packets
TOS for RTP Packets	Sets type of service for RTP packets

Sip Account Security

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

Figure 4-5-1 TLS settings

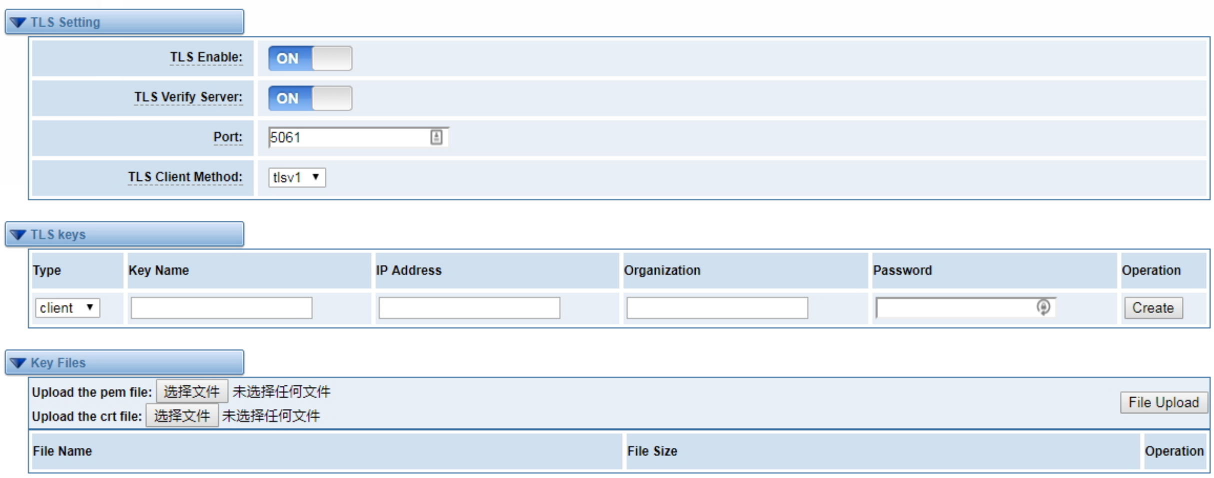


Table 4-5-1 Instruction of TLS

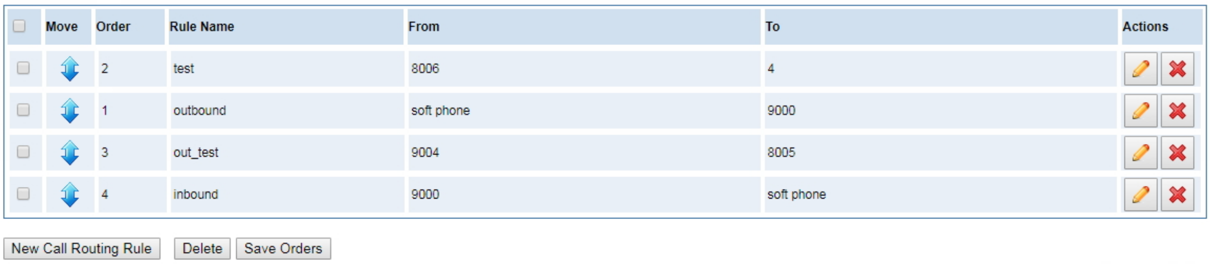
Options	**Definition**
TLS Enable	Enable or disable DTLS-SRTP support.
TLS Verify Server	Enable or disable tls verify server(default is no).
Port	Specify the port for remote connection.
TLS Client Method	Values include tlsv1, sslv3, sslv2, Specify protocol for outbound client connections, default is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

5. Routing

The gateway embraces the flexible and friendly routing settings for user. It supports up to 512 routing rules and about 100 pairs of calleeID/callerID manipulations can be set in a rule. It support DID function The gateway support trunk group and trunk priority management.

Call Routing Rules

Figure 5-1-1 Routing Rules



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

There is an example for routing rules number conversion, it transform calling, called number at the same time. Suppose you want eleven numbers start at 159 to call the eleven numbers of start at 136. Calling transform delete the three numbers from left, then writing number 086 as prefix, delete the last four numbers, and then add number 0755 at the end, it will show caller name is China Telecom. Called transform adds 086 as prefix, and Change the last two number to 88.

Figure 5-1-1

processing rules	prepend	prefix	Match pattern	SdfR	StA	RdfR	Caller Name
Calling Transformation	086	159	xxxxxxxx	4	0755		China telecom
Called transformation	086	136	xxxxxxx	2	88		N/A

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

Figure 5-1-2 Example of Setup Routing Rule

The figure above realizes that calls from "support" SIP endpoint switch you have registered will be transferred to Port-1. When "Call Comes in From" is 1001, "prepend", "prefix" and "match pattern" in "Advanced Routing Rule" are ineffective, and just "CallerID" option is available.

Table 5-1-2 Definition of Call Routing Rule

Options	Definition
Routing Name	The name of this route. Should be used to describe what types of calls this route matches (for example, 'SIP2GSM' or 'GSM2SIP').
Call Comes in From	The launching point of incoming calls.
Send Call Through	The destination to receive the incoming calls.

Figure 5-1-3 Advance Routing Rule

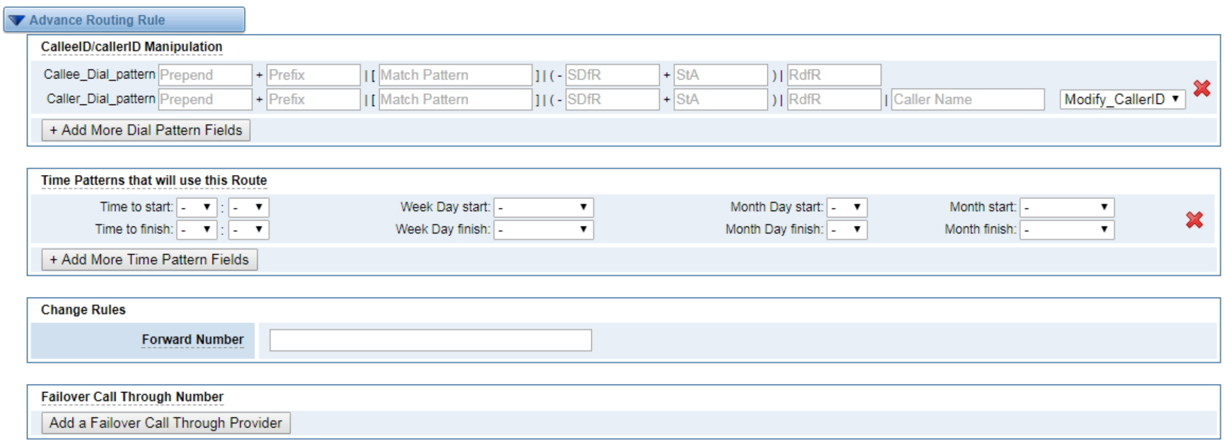


Table 5-1-3 Definition of Advance Routing Rule

Options	Definition
CalleeID/callerID Manipulation	A Dial Pattern is a unique set of digits that will select this route and send the call to the designated trunks. If a dialed pattern matches this route, no subsequent routes will be tried. If Time Groups are enabled, subsequent routes will be checked for matches outside of the designated time(s). X matches any digit from 0-9 Z matches any digit from 1-9 N matches any digit from 2-9 [1237-9]matches any digit in the brackets (example: 1,2,3,7,8,9) . 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. Mach 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. SDfR(Stripped Digits from Right): The amount of digits to be deleted from the right end of the number. If the value of this item exceeds the length of the current number, the whole number will be deleted. RDfR(Reserved Digits from Right): The amount of digits to be resevered from the right end of the number. If the value of this item under the length of the current number, the whole number will be reserverd. StA(Suffix to Add): Designated information to be added to the right end of the current number. Caller Name: What caller name would you like to set before sending this call to the

	endpoint. Disabled Caller Number Change : Disable the caller number change, and fixed caller number match pattern.
Time Patterns that will use this Route	Time Patterns that will use this Route help
Forward Number	What destination number will you dial? This is very useful when you have a transfer call.
Failover Call Through Number	The gateway will attempt to send the call out each of these in the order you specify.

Groups

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

Figure 5-2-1 Group Rules

Group Name	Type	Policy	Members	Actions
all	fxo	roundrobin	1, 2, 3, 4, 5, 6, 7, 8	
SIP	sip	roundrobin	987, 1002, 980, 981, 982, 983, 984, 985, 986	

New Group

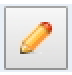
You can click New Group button to set new group, and if you want to modify existed group, you can click  button.

Figure 5-2-2 Create a Group

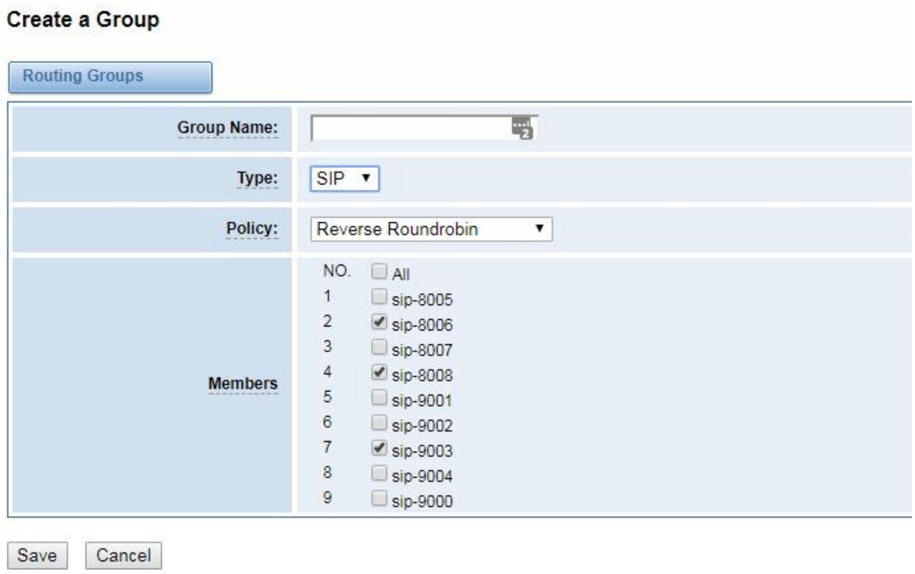


Figure 5-2-3 Modify a Group

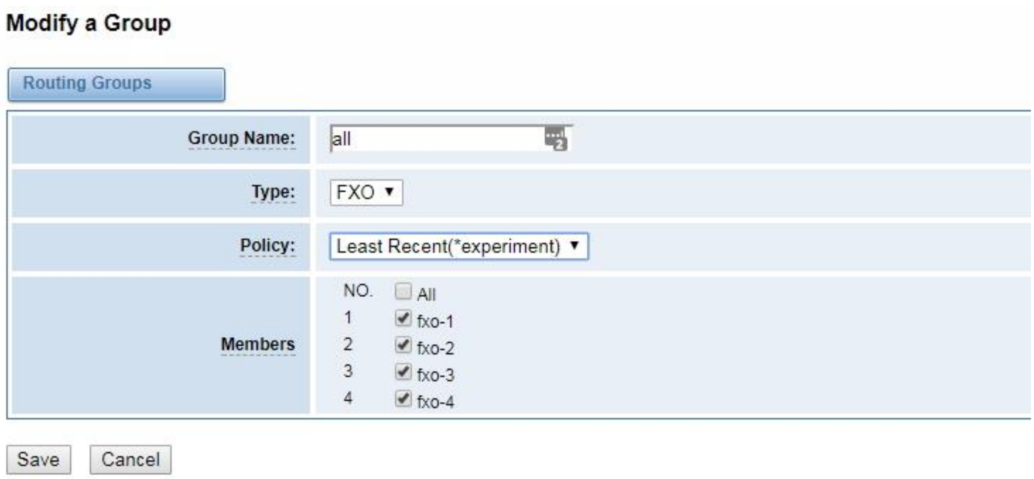


Table 5-2-1 Definition of Routing Groups

Options	Definition
Group Name	The mean of this route. Should be used to describe what types of calls this route match (for example, 'sip1 TO port1' or 'port1 To sip2').

Batch Create Rules

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

Figure 5-3-1 Batch Create Rules

Port	Forward Number	Sip Endpoint	CallerID
FXO-1		None	
FXO-2		None	
FXO-3		None	
FXO-4		None	

Save Cancel

6. Network

On “Network” page, there are “Network Settings”, “VPN Settings”, “DDNS Settings”, and “Toolkit”.

Network Settings

There are three types of LAN port IP, Factory, Static and DHCP. Factory is the default type, and it is 172.16.99.1. When you Choose LAN IPv4 type is “Factory”, this page is not editable.

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

Figure 6-1-1 LAN Settings Interface

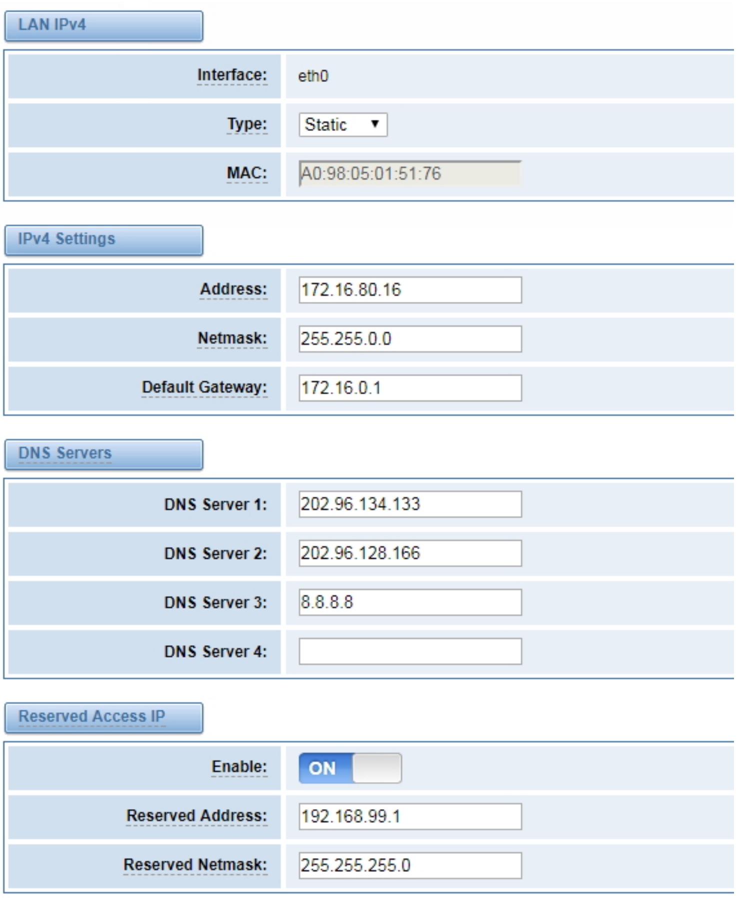


Table 6-1-1 Definition of Network Settings

Options	Definition

Interface	The name of network interface.
Type	The method to get IP. Factory: Getting IP address by Slot Number (System → information to check slot number). Static: manually set up your gateway IP. DHCP: automatically get IP from your local LAN.
MAC	Physical address of your network interface.
Address	The IP address of your gateway.
Netmask	The subnet mask of your gateway.
Default Gateway	Default getaway IP address.
Reserved Access IP	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.
Enable	A switch to enable the reserved IP address or not. ON(enabled), OFF(disabled)
Reserved Address	The reserved IP address for this gateway.
Reserved Netmask	The subnet mask of the reserved IP address.

Basically this info is from your local network service provider, and you can fill in four DNS servers.

Figure 6-1-2 DNS Interface

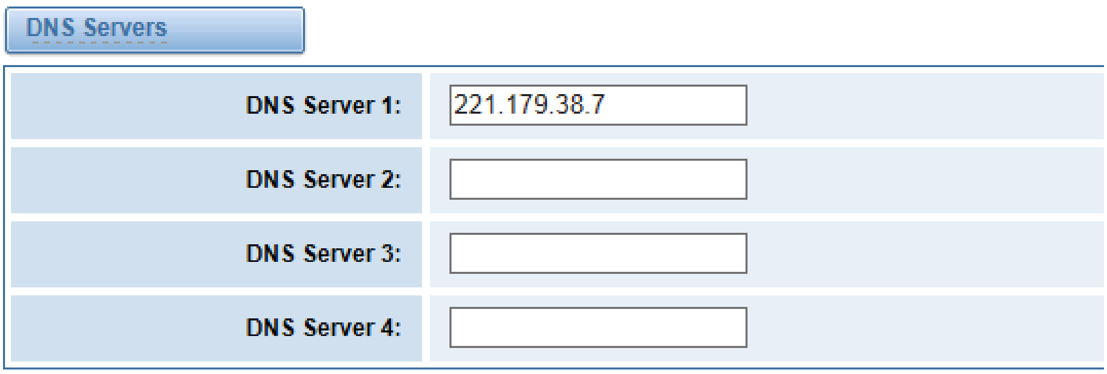


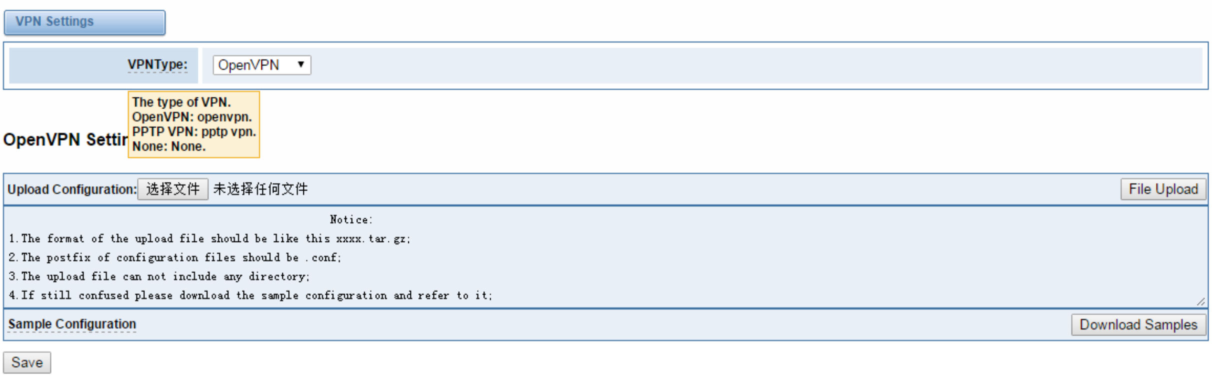
Table 6-1-2 Definition of DNS Settings

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

VPN Settings

You can upload the VPN client configuration, if success, you can see a VPN virtual network card on SYSTEM status page. About the configure format you can refer to the Notice and Sample configuration.

Figure 6-2-1 VPN Interface



DDNS Settings

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

Figure 6-3-1 DDNS Interface

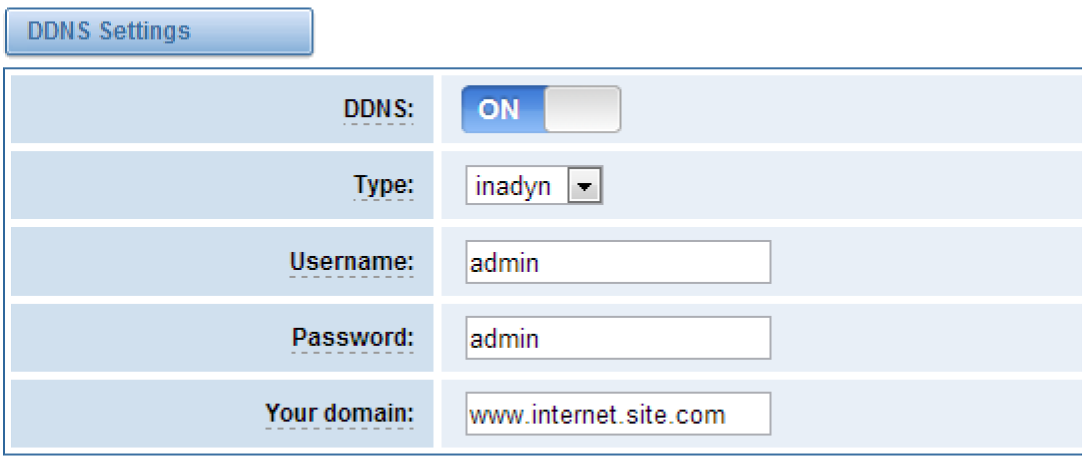


Table 6-3-1 Definition of DDNS Settings

Options	Definition
DDNS	Enable/Disable DDNS(dynamic domain name
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.

Toolkit

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

Figure 6-4-1 Network Connectivity Checking

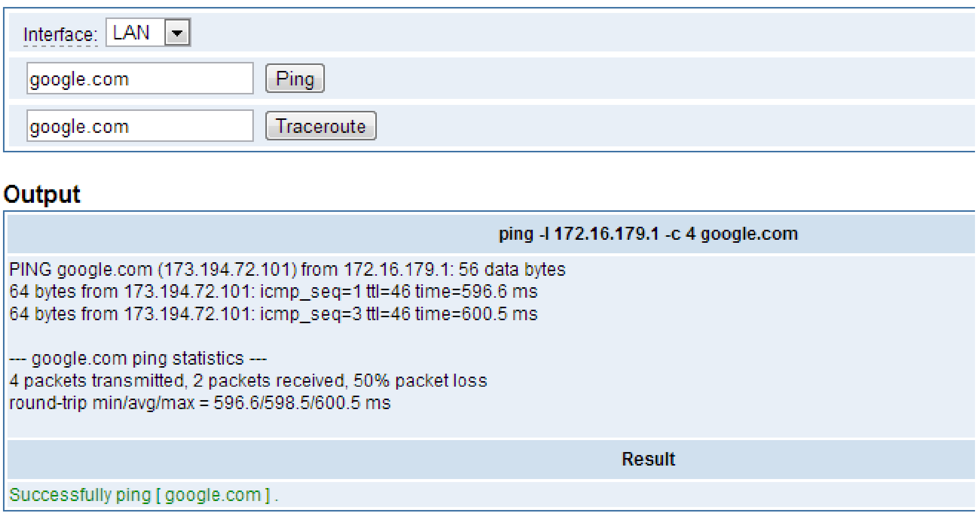


Figure 6-4-2 Channel Recording

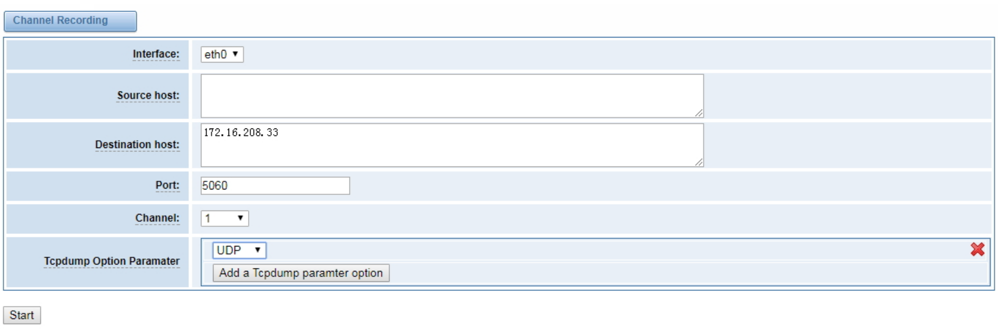


Figure 6-4-3 Capture Network Data

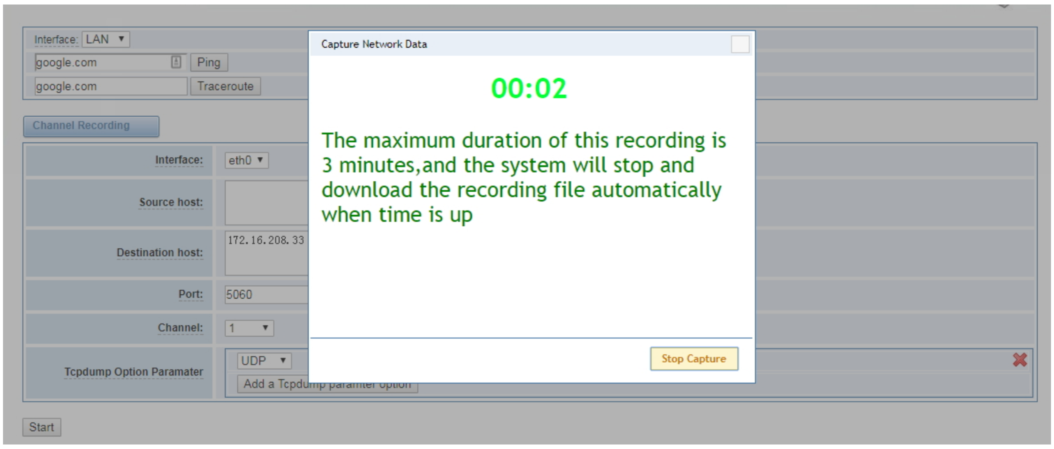


Table 6-4-1 Definition of Channel Recording

Options	**Definition**
Interface	The name of network interface.
Source host	Capture the data of source host you specified
Destination host	Capture the data of destination host you specified
Port	Capture the data of port you specified
Channel	Capture the data of channel you specified
Tcpdump Option Parameter	The tool of tcpdump capture network data by parameter option specified.

7. Advanced

Asterisk API

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

Figure 7-1-1 API Interface

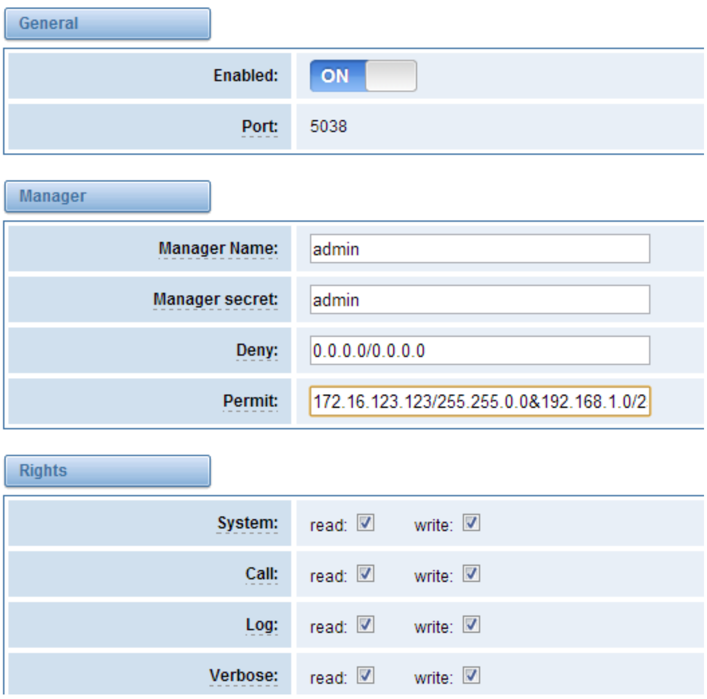


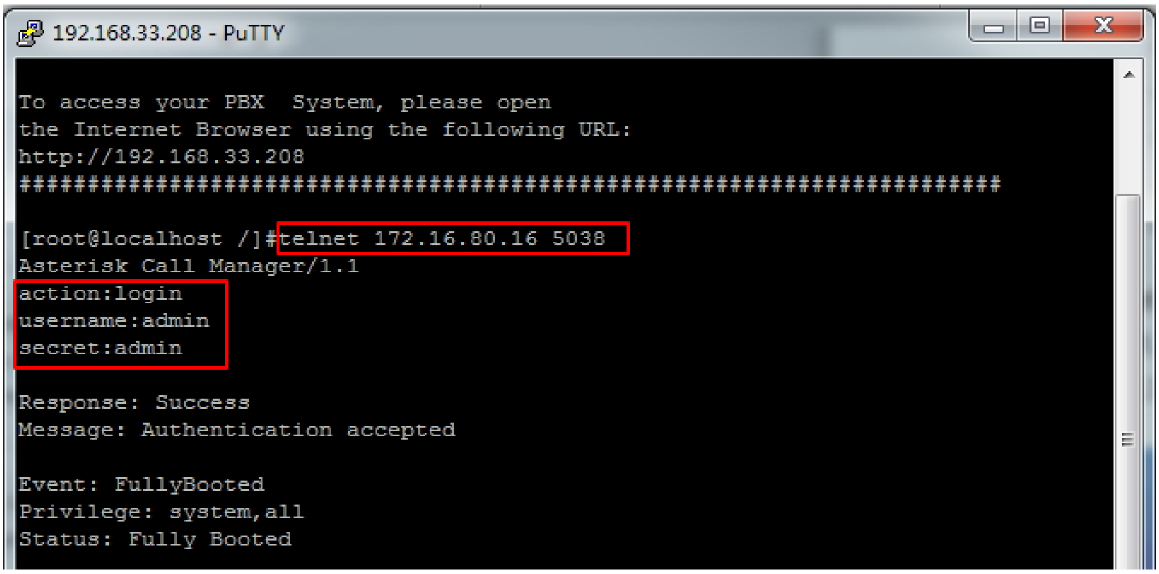
Table 7-1-1 Definition of Asterisk API

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

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

Once you set like the above figure, the host 172.16.80.16/255.255.0.0 is allowed to access the gateway API. Please refer to the following figure to access the gateway API by putty. 172.16.80.16 is the gateway's IP, and 5038 is its API port.

Figure 7-1-2 Putty Access



Asterisk CLI

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

Figure 7-2-1 Asterisk Command Interface

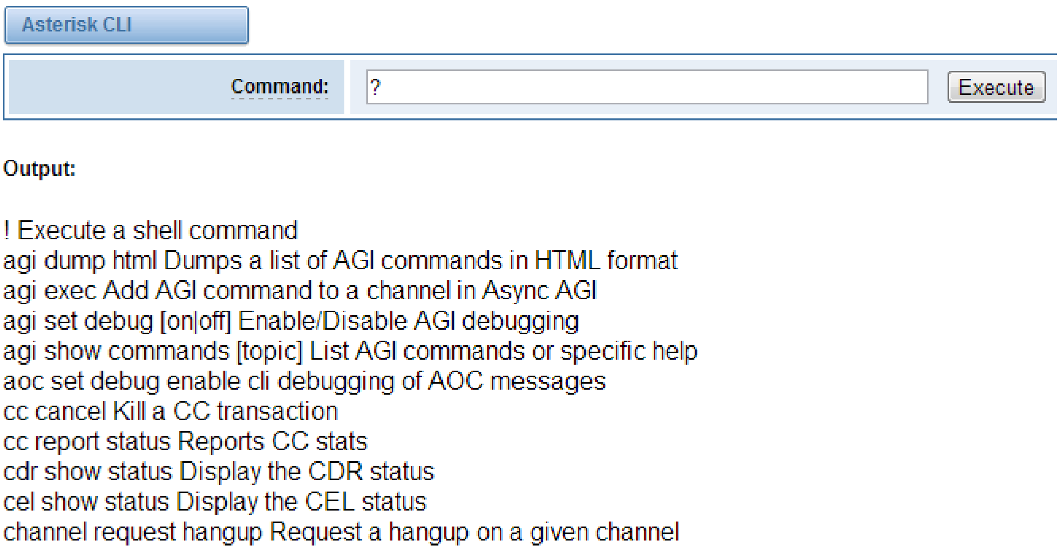


Table 7-2-1 Definition of Asterisk API

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

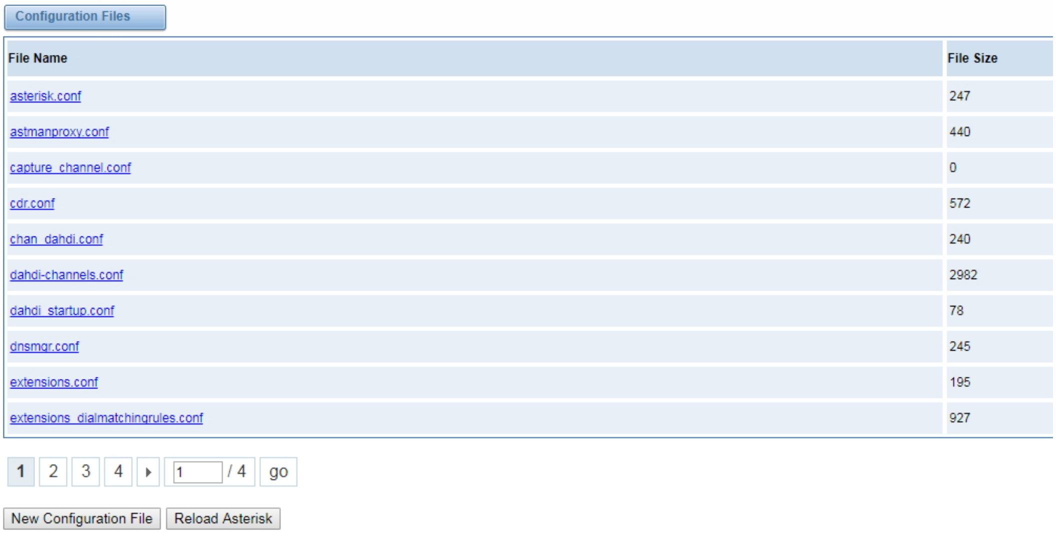
If you type “help” or “?” and execute it, the page will show you the executable commands.

Asterisk File Editor

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

Click the file to edit.

Figure 7-3-1 Configuration Files List



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

8. Logs

Log Settings

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

Figure 8-1-1 Logs Settings

Table 8-1-1 Definition of LOG

Options	Definition
System Logs	Whether enable or disable system log.
Auto clean (System Logs)	switch on : when the size of log file reaches the max size, the system will cut a half of the file. New logs will be retained. switch off : logs will remain, and the file size will increase gradually. default on, max size=1MB.
Verbose	Asterisk console verbose message switch.
Notice	Asterisk console notice message switch.
Warning	Asterisk console warning message switch.
Debug	Asterisk console debug message switch.
Error	Asterisk console error message switch.
DTMF	Asterisk console DTMF info switch.
Auto clean: (asterisk logs)	switch on : when the size of log file reaches the max size, the system will cut a half of the file. New logs will be retained. switch off : logs will remain, and the file size will increase gradually. default on, max size=100KB.
SIP Logs:	Whether enable or disable SIP log.
Auto clean: (SIP logs)	switch on : when the size of log file reaches the max size,the system will cut a half of the file. New logs will be retained. switch off : logs will remain, and the file size will increase gradually. default on, default size=100KB.
Call Detail Record	Displaying Call Detail Records for each channel.
Auto clean: (Call Detail Record)	switch on : when the size of log file reaches the max size,the system will cut a half of the file. New logs will be retained. switch off : logs will remain, and the file size will increase gradually. default on, default size=20MB.

System

Figure 8-2-1 System Logs Output

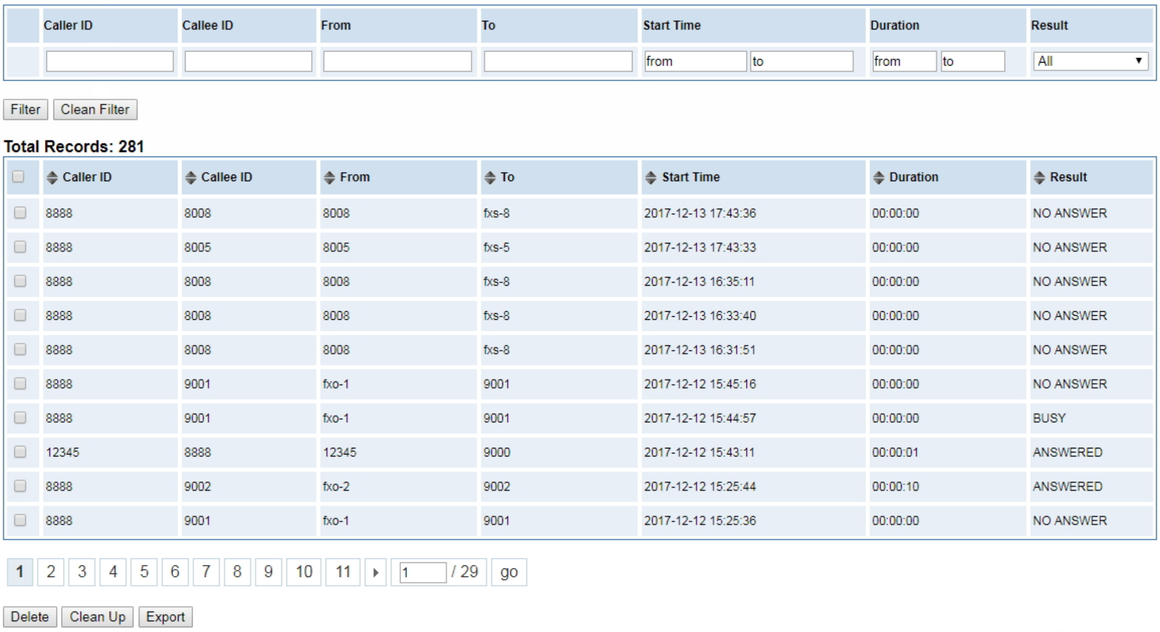
```
[1970/01/01 00:00:08] Auto restore configuration files
[1970/01/01 07:01:20] Power on
[2017/12/09 15:47:03] Restart asterisk from crontab.
[2017/12/12 10:11:43] Power off
[1970/01/01 07:01:17] Power on
[2017/12/12 15:51:00] Restore configuration files
[2017/12/12 15:51:10] Power off
[1970/01/01 00:00:08] Auto restore configuration files
[1970/01/01 07:01:19] Power on
[1970/01/01 07:01:20] Power on
[1970/01/01 07:26:44] System Update
[1970/01/01 07:26:59] Power off
[1970/01/01 07:00:10] Auto update configuration files, remain a few files.
[1970/01/01 07:01:27] Power on
[2017/12/13 11:10:05] Power off
[1970/01/01 07:01:22] Power on
[2017/12/13 13:47:43] Restore configuration files
[2017/12/13 13:47:50] Power off
[1970/01/01 00:00:08] Auto restore configuration files
[1970/01/01 07:01:25] Power on
[2017/12/14 18:29:39] Restore configuration files
[2017/12/14 18:29:46] Power off
[1970/01/01 00:00:08] Auto restore configuration files
[1970/01/01 07:01:33] Power on
[2017/12/18 15:44:08] Power on
[2017/12/18 15:53:56] System Update
[2017/12/18 15:54:15] Power off
[2017/12/18 15:55:35] Power on
[2017/12/20 11:42:01] Power on
```


Notice: The same to Asterisk Logs and SIP Logs.

CDR

You can scan every call detail records in this page. We also provide the filter for you to search some specific records.

Figure 8-3-1 Call Detail Record



Caller ID	Callee ID	From	To	Start Time	Duration	Result
8888	8008	8008	fxs-8	2017-12-13 17:43:36	00:00:00	NO ANSWER
8888	8005	8005	fxs-5	2017-12-13 17:43:33	00:00:00	NO ANSWER
8888	8008	8008	fxs-8	2017-12-13 16:35:11	00:00:00	NO ANSWER
8888	8008	8008	fxs-8	2017-12-13 16:33:40	00:00:00	NO ANSWER
8888	8008	8008	fxs-8	2017-12-13 16:31:51	00:00:00	NO ANSWER
8888	9001	fxo-1	9001	2017-12-12 15:45:16	00:00:00	NO ANSWER
8888	9001	fxo-1	9001	2017-12-12 15:44:57	00:00:00	BUSY
12345	8888	12345	9000	2017-12-12 15:43:11	00:00:01	ANSWERED
8888	9002	fxo-2	9002	2017-12-12 15:25:44	00:00:10	ANSWERED
8888	9001	fxo-1	9001	2017-12-12 15:25:36	00:00:00	NO ANSWER