



**OpenVox Communication Co Ltd**



# iAG200/400 Series Analog Gateway User Manual

Version 1.0



## OpenVox Communication Co Ltd

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

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

**Business Contact:** [sales@openvox.cn](mailto:sales@openvox.cn)

**Technical Support:** [support@openvox.cn](mailto:support@openvox.cn)

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

**URL:** [www.openvox.cn](http://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	11/04/2022	First Version

## Contents

1. Overview .....	7
1.1 What is iAG Series Analog Gateway? .....	7
1.2 Sample Application .....	7
1.3 Product Appearance .....	8
1.4 Main Features .....	9
1.5 Physical Information .....	10
1.6 Software .....	10
2. System .....	11
2.1 Status .....	11
2.2 Time .....	11
2.3 Login Settings .....	12
2.4 General .....	14
2.5 Tools .....	15
2.6 Information .....	17
3. Analog .....	18
3.1 Channel Settings .....	18
3.2 Pickup .....	20
3.3 Dial Matching Table .....	21
3.4 Advanced .....	22
3.5 Special Function Keys .....	24
3.6 FXS Settings .....	25
3.7 Driver .....	27
4. VoIP .....	29
4.1 SIP Endpoints .....	29
4.2 FXS Batch Binding SIP .....	37
4.3 Batch Create SIP .....	38
4.4 Advanced SIP Settings .....	39
4.5 Sip Account Security .....	47
5. Routing .....	48

5.1 Call Routing Rules .....	48
5.2 Groups .....	52
5.3 Batch Create Rules .....	53
6. Network .....	54
6.1 Network Settings .....	54
6.2 VPN Settings .....	56
6.3 DDNS Settings .....	56
6.4 Toolkit .....	57
6.5 Security Settings .....	59
6.6 Security Rules .....	59
7. Advanced .....	60
7.1 Asterisk API .....	60
7.2 Asterisk CLI .....	62
7.3 Asterisk File Editor .....	63
7.4 Cloud Management .....	63
7.5 TR069 .....	64
7.6 SNMP .....	65
7.7 Auto Provision .....	65
8. Logs .....	66
8.1 Log Settings .....	66
8.2 CDR .....	69

# 1. Overview

## 1.1 What is iAG Series Analog Gateway?

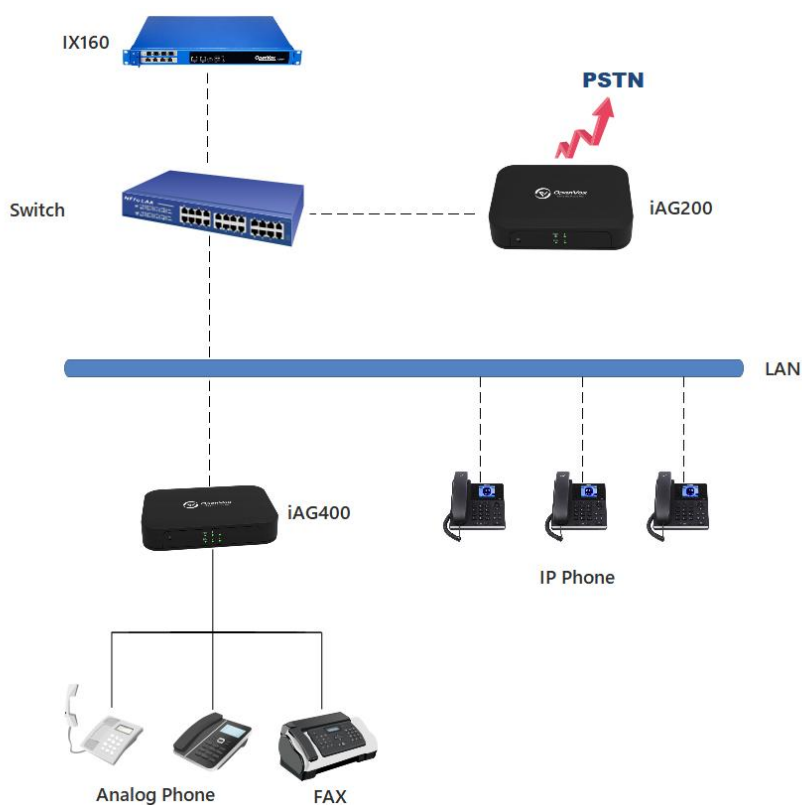
OpenVox iAG200/400 Analog Gateway, a new product of the iAG Series, is specially designed for SMBs and SOHOs. With friendly GUI and unique modular design, users may easily setup their customized gateway. Also secondary development can be completed through AMI (Asterisk Management Interface).

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

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

## 1.2 Sample Application

Figure 1-2-1 Topological Graph



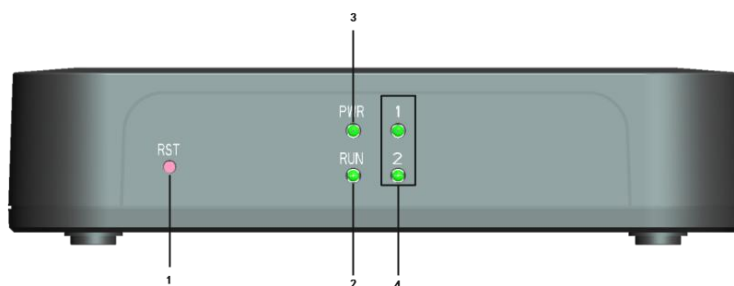
## 1.3 Product Appearance

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

**Figure 1-3-1 Product Appearance**



**Figure 1-3-2 Front Panel**



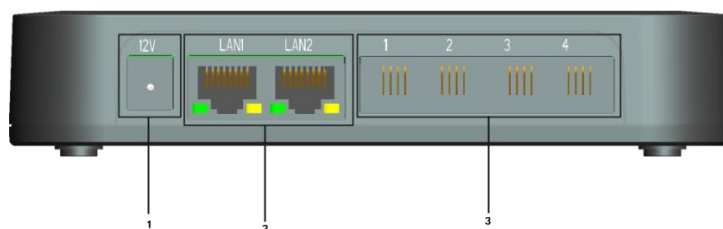
1: Reset Button

2: Running Indicator

2: Power Indicator

3: Analog Telephone Interfaces and corresponding Channels State Indicators

**Figure 1-3-3 Back Panel**



1: Power Interface

2: Ethernet Ports and Indicators

3: Analog Interface



## 1.4 Main Features

### System Features

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

### Telephony Features

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

### SIP Features

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

### Network

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

## 1.5 Physical Information

**Table 1-5-1 Description of Physical Information**

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

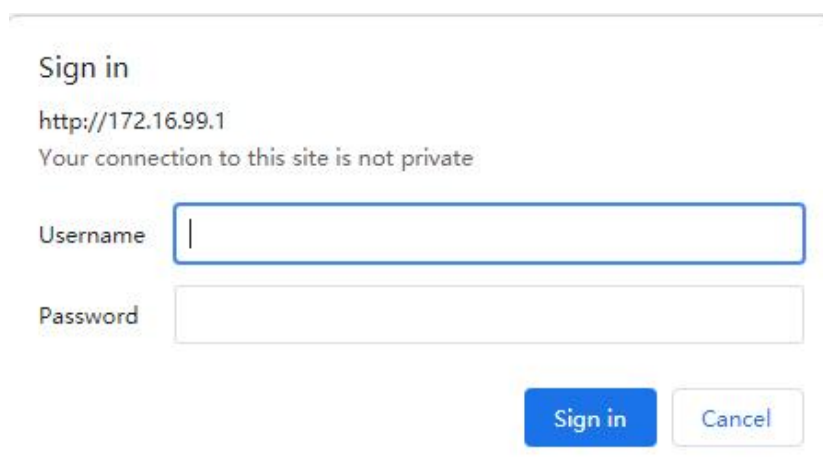
## 1.6 Software

**Default IP:** 172.16.99.1

**Username:** admin

**Password:** admin

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

**Figure 1-6-1 Login Interface**

Sign in

http://172.16.99.1

Your connection to this site is not private

Username

Password

## 2. System

### 2.1 Status

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

**Figure 2-1-1 System Status**

Port	Name	Type	Line Status/Sip Account	Port Status	Voltage
1	port-1	FXS	Connected	OnHook	48
2	port-2	FXS	Connected	OnHook	48
3	port-3	FXS	Connected	OnHook	48
4	port-4	FXS	Connected	OnHook	48

### 2.2 Time

**Table 2-2-1 Description of Time Settings**

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

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

For example, you can configure like this:

**Figure 2-2-1 Time Settings**

### Time Settings

System Time:	2022-04-02 12:11:43
Time Zone:	Chongqing
POSIX TZ String:	CST-8
NTP Server 1:	ntp1.aliyun.com
NTP Server 2:	pool.ntp.org
NTP Server 3:	time.nist.gov
Auto-Sync from NTP:	<input checked="" type="checkbox"/>

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

## 2.3 Login Settings

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

Table 2-3-1 Description of Login Settings

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

Figure 2-3-1 Login Settings

The screenshot displays the OpenVox web management interface. On the left is a dark blue sidebar with a search icon and a menu containing: System, Status, Time, Login Settings (highlighted), General, Tools, Information, Analog, Voip, Routing, Network, Advanced, and Logs. The main content area is titled 'Login Settings' and contains three sections:

- Web Login Settings:**
  - User Name:
  - Password:
  - Confirm Password:
  - Login Mode:
  - HTTP Port:
  - HTTPS Port:
- SSH Login Settings:**
  - Enable:
  - User Name:
  - Password:
  - Port:
- HTTPS Certificate:**
  - Certificate Upload:

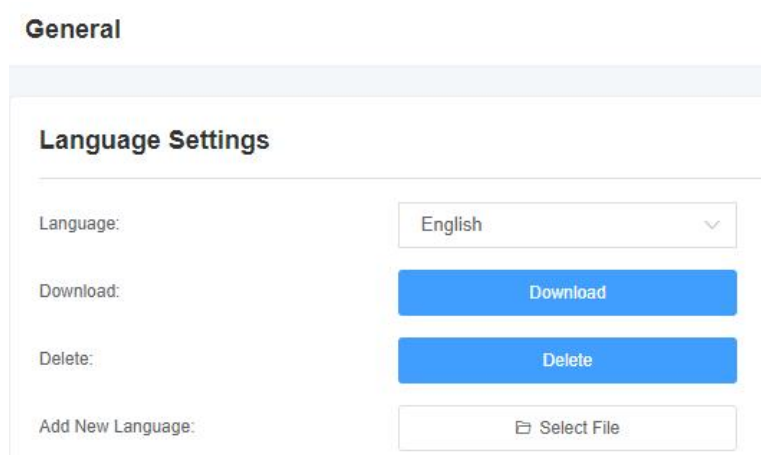
**Notice:** Whenever you do some changes, do not forget to save your configuration.

## 2.4 General

### 2.4.1 Language Settings

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

**Figure 2-4-1 Language Settings**



**General**

**Language Settings**

Language: English

Download: Download

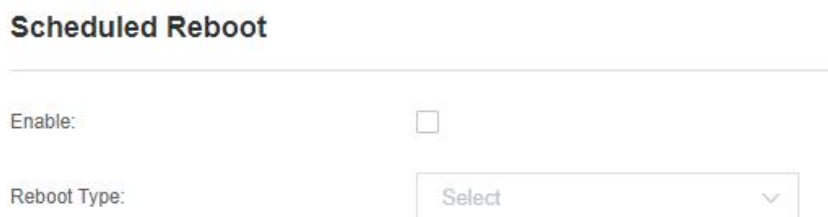
Delete: Delete

Add New Language: Select File

### 2.4.2 Scheduled Reboot

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

**Figure 2-4-2 Reboot Types**



**Scheduled Reboot**

Enable:

Reboot Type: Select

## 2.5 Tools

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

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

**Figure 2-5-1 Reboot Prompt**



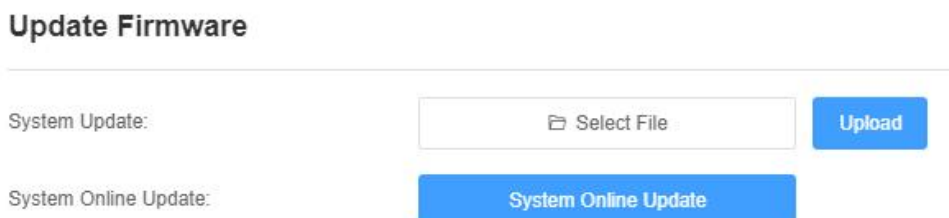
**Notice:** When you confirm the restart, the system will automatically end all current calls.

**Table 2-5-1 Instruction of reboots**

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

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

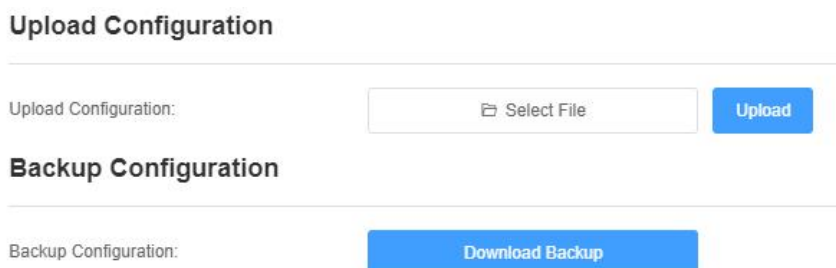
**Figure 2-5-2 Update Firmware**



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

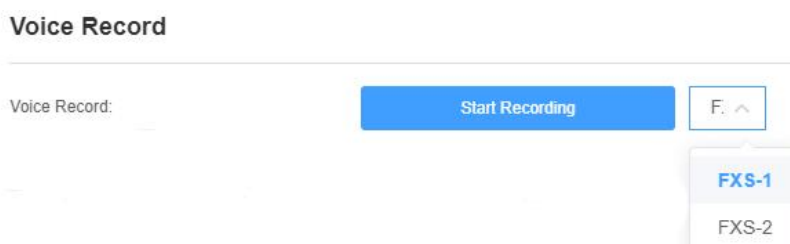
**Notice:** It will take effect only if the version of the configuration file and the current firmware version are the same.

**Figure 2-5-3 Upload and Backup**



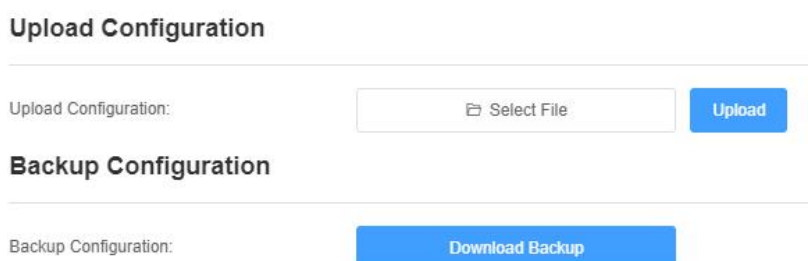
4. If you want to record the voice of the gateway, you can choose "Voice Record". Choose the port which you want to record, and then select "Start Recording".

**Figure 2-5-4 Voice Record**



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

**Figure 2-5-4 Factory Reset**



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



## 2.6 Information

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

**Figure 2-6-1 System Information**

System Information	
Product Name:	IAG400
Serial Number:	DB6110741F12462D
Software Version:	1.0.0
Hardware Version:	1.0.0
Slot Number:	1
Storage Usage:	392.0K/6.3M (6%)
Memory Usage:	54.3118 % <a href="#">Memory Clean</a>
Build Time:	2022-03-24 06:24:20
Contact Address:	Room 624, 6/F, TsingHua Information Port, QingQing Road, LongHua Street, LongHua District, ShenZhen
Tel:	+86-755-82535461
Fax:	+86-755-83823074
E-Mail:	<a href="mailto:support@openvox.cn">support@openvox.cn</a>
Web Site:	<a href="http://www.openvox.cn">http://www.openvox.cn</a>
System Time:	2022-04-02 13:50:35
System Uptime:	2 days 02:10:50

### 3. Analog

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

#### 3.1 Channel Settings

Figure 3-1-1 Channel System

Channel Settings Save

Port	Type	Name	Line Status/Sip Account	Port Status	Hour Call Count	Daily Call Count	Daily Answer Count	Call Status	Actions
1	FXS	port-1	none	OnHook	0	0	0	Unlimited	Edit
2	FXS	port-2	none	OnHook	0	0	0	Unlimited	Edit
3	FXS	port-3	none	OnHook	0	0	0	Unlimited	Edit
4	FXS	port-4	none	OnHook	0	0	0	Unlimited	Edit

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

Figure 3-1-2 FXO Port Configure

Edit Port FXO-1

**General**

Port type: FXO

Name: port-1

Ring timeout: 8

"M" is sent out immediately:

Callout Min interval: 2000

**Caller ID**

Use callerid:

Hide callerid:

CID signalling: bell

DND:

CID start signal: ring

**Polarity**

Answer on polarity switch:

Hangup on polarity switch:

Polarity on answer delay: 600

Delay reply 200 OK switch:

Delay reply 200 OK timer: 8

**Call Limit**

Call Limit Switch:

Limit Call Time: 0

Limit Daily Call Times: 0

Limit Daily Answer Times: 0

Limit Hour Call Times: 0

**CallerID detect**

cidbeforeing:

**Save To Other Channels**

All

FXO-1

FXO-2

FXO-3

FXO-4

Figure 3-1-3 FXS Port Configure

**Edit Port FXS-1**

---

**General**

Port type: FXS

Name:

Ring timeout:

Sip Account:

---

**Caller ID**

Caller ID:

Full name:

Internal Exten Number:

CID signalling:

DND:

---

**Polarity**

Answer on polarity switch:

Hangup on polarity switch:

---

**Call feature**

Call waiting:

Three way calling:

Call transfer:

Call forward:

Call forward number:

Registered Call On Busy:

---

**Call Limit**

Call Limit Switch:

Limit Call Time:

Limit Daily Call Times:

Limit Daily Answer Times:

Limit Hour Call Times:

---

**Save To Other Channels**

All

FXS-1       FXS-2       FXS-3       FXS-4

## 3.2 Pickup

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

**Figure 3-2-1 Pickup Settings**

**Pickup Settings**

Enable:

Time Out:

Number:

FXS-1: Disabled ▾ Time Out:  Number:

FXS-2: Disabled ▾ Time Out:  Number:

FXS-3: Disabled ▾ Time Out:  Number:

FXS-4: Disabled ▾ Time Out:  Number:

**Table 3-2-1 Definition of Pickup**

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

## 3.3 Dial Matching Table

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

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

**Figure 3-3-1 Port Configure**

**Dial Matching Table**
Save

---

<pre> _01[3-578]XXXXXXXX _010XXXXXXXX _02XXXXXXXX _0[3-9]XXXXXXXX _11[02-9] _111XX _123XX _95105XXX _9[56]XXX _100XX _10[1-9] _12[0-24-9] _1[3-578]XXXXXXXX _[235-7]XXXXXXXX _[48][1-9]XXXXXX _[48]0[1-9]XXXXXX _[48]00XXXXXXXX _XXXXXXXX. _#XX _*XX _## _.X.</pre>	<p>Dial Matching rule may be numbers, letters, or combinations thereof. If an rule is prefixed by a '_' character, it is interpreted as a pattern rather than a literal. In patterns, some characters have special meanings:</p> <p style="margin-left: 20px;">X - any digit from 0-9  Z - any digit from 1-9  N - any digit from 2-9  [1235-9] - any digit in the brackets (in this example, 1, 2, 3, 5, 6, 7, 8, 9)  ! - wildcard, causes the matching process to complete as soon as it can unambiguously determine that no other matches are possible</p> <p>For example, the rule _NXXXXXX would match normal 7 digit dialings, while _!NXXXXXXXX would represent an area code plus phone number preceded by a one.</p>
---	--

## 3.4 Advanced

### 3.4.1 General

**Figure 3-4-1 General Configuration**

#### General

Dial timeout:	<input type="text" value="180"/>		
Tone duration:	<input type="text" value="100"/>	Tone interval:	<input type="text" value="100"/>
Echo cancel:	<input checked="" type="checkbox"/>		
FXS Signaling:	<input type="text" value="Loop start"/>		

**Table 3-4-1 Instruction of General**

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

### 3.4.2 Fax

**Figure 3-4-4 Fax Configuration**

<b>Fax</b>		
Mode:	<input type="text" value="T.38"/>	Rate: <input type="text" value="14400"/>
Ecm:	<input type="checkbox"/>	

**Table 3-4-4 Definition of Fax**

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

### 3.4.3 Country

**Figure 3-4-5 Country Configuration**

#### Country

Country:	China <span style="float: right;">▼</span>
Ring cadence:	1000,4000
Dial tone:	450
Ring tone:	450/1000,0/4000
Busy tone:	450/350,0/350
Call waiting tone:	450/400,0/4000
Congestion tone:	450/700,0/700
Dial recall tone:	450
Record tone:	950/400,0/10000
Info tone:	450/100,0/100,450/100,0/100,450/100,0/100,450/400,0/400
Stutter tone:	450+425

**Table 3-4-5 Definition of Country**

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

## 3.5 Special Function Keys

**Figure 3-5-1 Function keys**

**Function Keys**

None Keys Blind Transfer:

Blind Transfer:

Asked Transfer:



## 3.6 FXS Settings

Figure 3-6-1 Caller ID

**Caller ID**

---

The pattern of sending CID:

Waiting time before sending CID:

Flash/Wink:

Min flash time:

Max flash time:

"#" as Ending Dial Key:

Display extension number:

Table 3-4-2 Definition of Caller ID

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

**Figure 3-6-2 Other Parameters****Caller ID**

offhook-antishake:

64

**Table 3-4-2 Definition of Other Parameters**

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

## 3.7 Driver

### 3.7.1 General

**Figure 3-7-1 General**

**General**

---

Codec:

Impedance:

**Table 3-7-1 Definition of General**

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

### 3.7.2 CallerID Detect

**Figure 3-7-2 CallerID Detect**

**CallerID detect**

---

cidbeforeing:

cidbuflen:

cutcidbufheadlen:

fixedtimepolarity:

**Table 3-7-2 Definition of CallerID Detect**

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

### 3.7.3 Hardware Gain

**Figure 3-7-3 Hardware Gain**

#### Hardware gain

FXO Rx gain:	<input type="text" value="0"/>
FXO Tx gain:	<input type="text" value="0"/>
FXS Rx gain:	<input type="text" value="0"/> ▼
FXS Tx gain:	<input type="text" value="0"/> ▼

**Table 3-7-3 Instruction of Hardware gain**

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

## 4. VoIP

### 4.1 SIP Endpoints

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

**Figure 4-1-1 SIP Status**

**SIP Endpoints**

Add Delete

<input type="checkbox"/>	Endpoint Name	Registration	Credentials	SIP Enable	Actions
<input type="checkbox"/>	8100	server	8100	Enabled	Edit Delete
<input type="checkbox"/>	8101	server	8101	Enabled	Edit Delete
<input type="checkbox"/>	8102	server	8102	Enabled	Edit Delete
<input type="checkbox"/>	8103	server	8103	Enabled	Edit Delete

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

#### 4.1.1 Main Endpoint Settings

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

You can configure as follows:

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

**Figure 4-1-2 Main Endpoint Settings - None**

**Main Endpoint Settings**

SIP Enable:

Name:

User Name:   Anonymous

Registration:

Backup Hostname or IP Address:

Transport:

SUBSCRIBE for MWI:

STUN Switch:

Password:

Hostname or IP Address:

Port:

NAT Traversal:

VOS Encryption:

Priority Match:

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

**Figure 4-1-3 Main Endpoint Settings - Server**

**Main Endpoint Settings**

SIP Enable:

Name:

User Name:   Anonymous

Registration:

Backup Hostname or IP Address:

Transport:

SUBSCRIBE for MWI:

STUN Switch:

Password:

Hostname or IP Address:

Port:

NAT Traversal:

VOS Encryption:

Priority Match:

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

**Figure 4-1-4 Main Endpoint Settings - Client**

**Main Endpoint Settings**

SIP Enable:

Name:

User Name:   Anonymous

Registration:

Backup Hostname or IP Address:

Transport:

SUBSCRIBE for MWI:

STUN Switch:

Password:

Hostname or IP Address:

Port:

NAT Traversal:

VOS Encryption:

Priority Match:

**Table 4-1-1 Definition of Endpoint Settings**

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

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

## 4.1.2 Advanced: Registration Options

Figure 4-1-5 Registration Options

### Advanced:Registration Options

Authentication User:	<input type="text"/>	Register Extension:	<input type="text"/>	<input checked="" type="checkbox"/> Readonly	
Register User:	<input type="text" value="301"/>	<input checked="" type="checkbox"/> Readonly	From User:	<input type="text" value="301"/>	<input checked="" type="checkbox"/> Readonly
From Domain:	<input type="text" value="172.16.66.15"/>	Qualify:	<input type="text" value="Yes"/>		
Qualify Frequency:	<input type="text" value="60"/>	Outbound Proxy:	<input type="text"/>	<input type="text" value="50"/>	
Custom Registry:	<input type="checkbox"/>				
Registry String:	<input type="text"/>				
Enable Outboundproxy to Host:	<input type="checkbox"/>				

Table 4-1-2 Definition of Registration Options

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



## 4.1.3 Call Settings

Figure 4-1-6 Definition of Call Settings

**Edit SIP Endpoint** Save

Main Endpoint Settings **Call Settings** Media Settings

---

**DTMF Settings**

DTMF Mode:

**Call Limit**

Call Limit:

**Caller ID Settings**

Trust Remote-Party-ID:  Send Remote-Party-ID:

Remote Party ID Format:  Caller ID Presentation:

Table 4-1-3 Definition of Call Settings

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

## 4.1.4 Advanced: Signaling Settings

Figure 4-1-7 Definition of Signaling Settings

### Advanced:Signaling Settings

Progress Inband:	<input type="text" value="Never"/>	Allow Overlap Dialing:	<input type="text" value="No"/>
Append user:	<input type="text" value="No"/>	Add Q.850 Reason Headers:	<input type="text" value="No"/>
Honor SDP Version:	<input type="text" value="Yes"/>	Allow Transfers:	<input type="text" value="Yes"/>
Allow Promiscuous Redirects:	<input type="text" value="No"/>	Max Forwards:	<input type="text" value="70"/>
Send TRYING on REGISTER:	<input type="text" value="No"/>		

Table 4-1-4 Definition of Signaling Options

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

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 promiscredirect when redirects are made to the local system will cause loops since this gateway is incapable of performing a "hairpin" call.
Max Forwards	Setting for the SIP Max-Forwards header (loop prevention).
Send TRYING on REGISTER	Send a 100 Trying when the endpoint registers.

## 4.1.5 Advanced: Timer Settings

**Figure 4-1-8 Definition of Timer Settings**

### Advanced:Timer Settings

Default T1 Timer:	<input type="text" value="500"/>	Call Setup Timer:	<input type="text" value="32000"/>
Session Timers:	<input type="text" value="Accept"/>	Minimum Session Refresh Interval:	<input type="text" value="90"/>
Maximum Session Refresh Interval:	<input type="text" value="1800"/>	Session Refresher:	<input type="text" value="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 500ms or the measured run-trip time between the gateway and the device if you have qualify=yes for the device.
Call Setup Timer	If a provisional response is not received in this amount of time, the call will auto-congest. Defaults to 64 times the default T1 timer.
Session Timers	Session-Timers feature operates in the following three modes: Originate, request and run session-timers always; Accept, run session-timers only when requested by other UA; Refuse, do not run session timers in any case.
Minimum Session Refresh Interval	Minimum session refresh interval in seconds. Default is 90secs.
Maximum Session Refresh Interval	Maximum session refresh interval in seconds. Defaults to 1800secs.
Session Refresher	The session refresher, uac or uas. Defaults to uas.

## 4.1.6 Media Settings

**Table 4-1-6 Definition of Media Settings**

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

## 4.2 FXS Batch Binding SIP

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

**Notice:** this is only used when “Client” work mode.

**Figure 4-2-1 FXS Batch Binding SIP**

**FXS Batch Binding SIP** Save

Select File Upload Download Samples

<input type="checkbox"/>	Port	Port Name	User Name	Password	Hostname or IP Address	Port	VOS Encryption	Codec Priority	Support Codec
<input checked="" type="checkbox"/>			<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Nc ▾	G.711 u-ls ▾	all ▾
<input type="checkbox"/>	1	port-1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Nc ▾	G.711 u-ls ▾	all ▾
<input type="checkbox"/>	2	port-2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Nc ▾	G.711 u-ls ▾	all ▾
<input type="checkbox"/>	3	port-3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Nc ▾	G.711 u-ls ▾	all ▾
<input type="checkbox"/>	4	port-4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Nc ▾	G.711 u-ls ▾	all ▾

Batch  AutoPassword

## 4.3 Batch Create SIP

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

**Figure 4-3-1 Batch SIP Endpoints**

**Batch Create SIP** Save

<input type="checkbox"/>	Port	User Name	Password	Host	Port	VOS Encrytion
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Client <input type="text"/>
<input type="checkbox"/>	1	301	Pbx	172.16.99.46	<input type="text"/>	Client <input type="text"/>
<input type="checkbox"/>	2	302	Pbx	172.16.99.46	<input type="text"/>	Client <input type="text"/>
<input type="checkbox"/>	3	303	Pbx	172.16.99.46	<input type="text"/>	Client <input type="text"/>
<input type="checkbox"/>	4	304	Pbx	172.16.99.46	<input type="text"/>	Client <input type="text"/>

AutoPassword

## 4.4 Advanced SIP Settings

### 4.4.1 Networking

**Figure 4-4-1 Definition of Networking Options**

**Advanced SIP Settings** Save

[Networking](#) [Parsing and Compatibility](#) [Security and Media](#)

---

**General**

UDP Bind Port:	<input type="text" value="5060"/>	Enable TCP:	<input type="text" value="No"/>
TCP Bind Port:	<input type="text" value="5060"/>	TCP Authentication Timeout:	<input type="text"/>
TCP Authentication Limit:	<input type="text"/>	Enable Hostname Lookup:	<input type="text" value="No"/>
SIP Match Order:	<input type="text" value="From"/> <input type="text" value="To"/>		

**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	<p>Enable DNS SRV lookups on outbound calls .</p> <p>Note: the gateway only uses the first host in SRV records Disabling DNS SRV lookups disables the ability to place SIP calls based on domain names to some other SIP users on the Internet Sepcifying a port in a SIP peer definition or when dialing outbound calls with supress SRV lookups for that peer or call.</p>

## 4.4.2 NAT Settings

**Figure 4-4-2 Definition of NAT Settings**

**NAT Settings**

---

Local Network:

Local Network List:

Subscribe Network Change Event:  Match External Address Locally:

Dynamic Exclude Static:  Externally Mapped TCP Port:

External Address:   Auto Update

External Hostname:

Hostname Refresh Interval:

**Table 4-4-2 Definition of NAT Settings**

Options	Definition
Local Network	<p>Format:192.168.0.0/255.255.0.0 or 172.16.0.0./12.</p> <p>A list of IP address or IP ranges which are located inside a NATed network.</p> <p>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.</p>
Local Network List	Local IP address list that you added.
Subscribe Network Change Event	<p>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.</p> <p>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.</p>
Match External Address Locally	Only substitute the externaddr or externhost setting if it matches
Dynamic Exclude Static	Disallow all dynamic hosts from registering as any IP address. Used for statically defined hosts. This helps avoid the configuration error of allowing your users to



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

### 4.4.3 STUN Settings

**Figure 4-4-3 Definition of STUN Settings**

#### STUN Settings

Enable:	<input type="checkbox"/>	Server Port:	<input type="text" value="3478"/>
Refresh Request Interval:	<input type="text" value="30"/>	Server IP Address/Domain Name:	<input type="text" value="stun.xten.com"/>

**Table 4-4-3 Definition of STUN Settings**

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

## 4.4.4 RTP Settings

Figure 4-4-4 Definition of RTP Settings

### RTP Settings

Start of RTP Port Range:	<input type="text" value="30000"/>	End of RTP port Range:	<input type="text" value="40000"/>
RTP Timeout:	<input type="text" value="20"/>		

Table 4-4-4 Definition of NAT Settings Options

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

## 4.4.5 Parsing and Compatibility

Figure 4-4-5 Definition of Parsing and Compatibility

**Advanced SIP Settings**

Networking   Parsing and Compatibility   Security and Media

Save

---

**General**

Strict RFC Interpretation:       Send Compact Headers:

SDP Owner:       Matching Priority:

**SIP Methods**

Disallowed SIP Methods:

<input type="checkbox"/> ACK	<input type="checkbox"/> BYE	<input type="checkbox"/> CANCEL
<input type="checkbox"/> INFO	<input type="checkbox"/> INVITE	<input type="checkbox"/> MESSAGE
<input type="checkbox"/> NOTIFY	<input type="checkbox"/> OPTIONS	<input type="checkbox"/> PRACK
<input type="checkbox"/> PUBLISH	<input type="checkbox"/> REFER	<input type="checkbox"/> REGISTER
<input type="checkbox"/> SUBSCRIBE	<input type="checkbox"/> UPDATE	

Hangup Cause Code:

**Caller ID**

Shrink Caller ID:

SIP From:

Set CallerID:

**Callee ID**

SIP To:

Callee ID:

Allow Options None Exten:

**Timer Configuration**

Maximum Registration Expiry:       Minimum Registration Expiry:

Default Registration Expiry:

**Outbound Registrations**

Registration Timeout:       Number of Registration Attempts:

**Table 4-4-5 Definition of Parsing and Compatibility**

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

## 4.4.6 Security and Media

**Figure 4-4-6 Definition of Parsing and Compatibility**

**Advanced SIP Settings**

Networking   Parsing and Compatibility   Security and Media

---

**Authentication Settings**

Match Auth Username:    Realm:

Use Domain as Realm:    Always Auth Reject:

Authenticate Options Requests:

Allow Guest Calling:

**ISDN Media Settings**

Premature Media:

**RTP for SIP**

directmedia:

**QoS/ToS**

TOS for SIP Packets:    TOS for RTP Packets:

**Table 4-4-6 Instruction of Security and Media**

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

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

## 4.5 Sip Account Security

This analog gateway support TLS protocol 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 provided by the server.

**Figure 4-5-1 TLS settings**

**SIP Account Security** Save

---

**TLS Setting**

TLS Enable:       TLS Verify Server:

Port:       TLS Client Method:

---

**TLS Key**

Type	Key Name	IP Address	Organization	Password	Operation
Client	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Create

---

**Key Files**

Upload the pem file:

Upload the crt file:

File Name	File Size	Actions
No Data		

**Table 4-5-1 Instruction of TLS**

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

## 5. Routing

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

### 5.1 Call Routing Rules

**Figure 5-1-1 Routing Rules**

<input type="checkbox"/>	Rule Name	Order	From	To	Actions
<input type="checkbox"/>	in	1	fxs-10	fxs-17	Edit Delete
<input type="checkbox"/>	out	2	sip-8110	sip-8119	Edit Delete

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

**Figure 5-1-2 Example of Setup Routing Rule**

**Call Routing Rule**

Routing Name:

Send Call Through:

Call Comes in From:

Force Answer:

**DISA Settings**

Authentication:

DISA Timeout:

Secondary Dialing:

Max Password Digits:

Password:



**Table 5-1-1 Definition of Call Routing Rule**

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

**Figure 5-1-3 Advance Routing Rule**

Advance Routing Rule

**Callee/CallerID Manipulation**

Callee Dial Pattern:

Caller Dial Pattern:

[Add More Dial Pattern Fields](#)

**Time Patterns that will use this Route**

Time to start:  Any Time

Month Day start:

Time to finish:  Any Time

Month Day finish:

Week Day start:

Month start:

Week Day finish:

Month finish:

[Add More Time Pattern Fields](#)

**Change Rules**

Forward Number:

Dialing Delay:

Custom Context:

T.38 Gateway Mode:

**Fallover Call Through Number**

[Add a Fallover Call Through Provider](#)

Table 5-1-3 Definition of Advance Routing Rule

Options	Definition
CalleeID/callerID Manipulation	<p>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).</p> <p>X matches any digit from 0-9</p> <p>Z matches any digit from 1-9</p> <p>N matches any digit from 2-9</p> <p>[1237-9]matches any digit in the brackets (example: 1,2,3,7,8,9)</p> <p><b>*matches one or more digits</b></p> <p>Prepend&lt;add prefix&gt;: The number added when the pattern matches successfully. If the dialed number matches the pattern specified in the subsequent column, the number will be added before being sent to the trunk.</p> <p>Prefix: Removed when the pattern is matched successfully. The dialed number is matched with the pattern specified in the subsequent column. Once the match is successful, the prefix will be removed from the number before being sent to the trunk.</p> <p>Match Pattern: The dialed number will be compared with the number in the " prefix + " this matching pattern. Once the match is successful, the matched pattern part of the dial will be sent to the trunks.</p> <p>SDfR&lt;Delete digits from the right&gt;: The number of digits to be deleted from the right end of the number. If this value of this item exceeds the length of the current number, the entire number will be deleted.</p> <p>RDfR&lt;Reserved digits from the right&gt;: The reserved digits from the right.</p> <p>StA&lt;Add Suffix&gt;: Add this number from the right end of the current number.</p> <p>Caller Name &lt;caller display name&gt;: Set your favorite caller name before sending this call to the terminal, allowing the use of local languages, such as Chinese and Latin.</p>
Time Patterns	Time mode setting of routing rules.

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

## 5.2 Groups

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

Figure 5-2-1 Group Rules

Group Name	Type	Policy	Members	Actions
test	SIP	Ascending	sip-,sip-112,sip-8100,sip-8101,sip-8102,sip-8103,sip-8104,sip-8105,sip-8106,sip-8107,sip-8108,sip-8109,sip-8110,sip-8111,sip-8112,sip-8113,sip-8114,sip-8115,sip-8116,sip-8117,sip-8118,sip-8119,sip-8120,sip-8121,sip-8122,sip-8123,sip-8124,sip-8125,sip-8126,sip-8127,sip-8128,sip-8129,sip-8130,sip-8131	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

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

Figure 5-2-2 Create a Group

**Routing Groups**

Group Name:

Type:

Policy:

Members:

All

<input type="checkbox"/> sip-	<input type="checkbox"/> sip-112	<input type="checkbox"/> sip-8100	<input type="checkbox"/> sip-8101	<input type="checkbox"/> sip-8102	<input type="checkbox"/> sip-8103
<input type="checkbox"/> sip-8104	<input type="checkbox"/> sip-8105	<input type="checkbox"/> sip-8106	<input type="checkbox"/> sip-8107	<input type="checkbox"/> sip-8108	<input type="checkbox"/> sip-8109
<input type="checkbox"/> sip-8110	<input type="checkbox"/> sip-8111	<input type="checkbox"/> sip-8112	<input type="checkbox"/> sip-8113	<input type="checkbox"/> sip-8114	<input type="checkbox"/> sip-8115
<input type="checkbox"/> sip-8116	<input type="checkbox"/> sip-8117	<input type="checkbox"/> sip-8118	<input type="checkbox"/> sip-8119	<input type="checkbox"/> sip-8120	<input type="checkbox"/> sip-8121
<input type="checkbox"/> sip-8122	<input type="checkbox"/> sip-8123	<input type="checkbox"/> sip-8124	<input type="checkbox"/> sip-8125	<input type="checkbox"/> sip-8126	<input type="checkbox"/> sip-8127
<input type="checkbox"/> sip-8128	<input type="checkbox"/> sip-8129	<input type="checkbox"/> sip-8130	<input type="checkbox"/> sip-8131		

Must set.

**Figure 5-2-3 Modify a Group**

**Routing Groups**

Routing Groups

Group Name:

Type:

Policy:

Members:

- All
- sip-
- sip-112
- sip-8100
- sip-8101
- sip-8102
- sip-8103
- sip-8104
- sip-8105
- sip-8106
- sip-8107
- sip-8108
- sip-8109
- sip-8110
- sip-8111
- sip-8112
- sip-8113
- sip-8114
- sip-8115
- sip-8116
- sip-8117
- sip-8118
- sip-8119
- sip-8120
- sip-8121
- sip-8122
- sip-8123
- sip-8124
- sip-8125
- sip-8126
- sip-8127
- sip-8128
- sip-8129
- sip-8130
- sip-8131

**Table 5-2-1 Definition of Routing Groups**

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

### 5.3 Batch Create Rules

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

**Figure 5-3-1 Batch Create Rules**

**Batch Create Rules**

<input type="checkbox"/>	Port	Forward Number	<input type="button" value="Increment"/>	<input type="button" value="Copy"/>	SIP Endpoints	<input type="button" value="Increment"/>	<input type="button" value="Copy"/>	Caller ID	<input type="button" value="Increment"/>	<input type="button" value="Copy"/>
<input type="checkbox"/>		<input type="text"/>			none			<input type="text"/>		
<input type="checkbox"/>	FXO-1	<input type="text"/>			none			<input type="text"/>		
<input type="checkbox"/>	FXO-2	<input type="text"/>			none			<input type="text"/>		
<input type="checkbox"/>	FXO-3	<input type="text"/>			none			<input type="text"/>		
<input type="checkbox"/>	FXO-4	<input type="text"/>			none			<input type="text"/>		

## 6. Network

### 6.1 Network Settings

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

Figure 6-1-1 LAN Settings Interface

The screenshot displays the LAN Settings interface, organized into several sections:

- Basic Settings**: The main title of the configuration page.
- Network Type**: A dropdown menu set to "Dual".
- LAN1 Settings**:
  - Type: DHCP
  - MAC: a0:98:05:02:aa:b4
- LAN2 Settings**:
  - Type: Static
  - MAC: a0:98:05:02:aa:b5
  - Address: 172.16.99.1
  - Netmask: 255.255.0.0
  - Default Gateway: 172.16.0.1
- DNS Server**:
  - DNS Server 1: 202.96.134.133
  - DNS Server 2: 202.96.128.166
  - DNS Server 3: 8.8.8.8
  - DNS Server 4: (empty)
- Reserved Access IP**:
  - Enable:
  - Reserved Address: 192.168.99.1
  - Reserved Netmask: 255.255.255.0

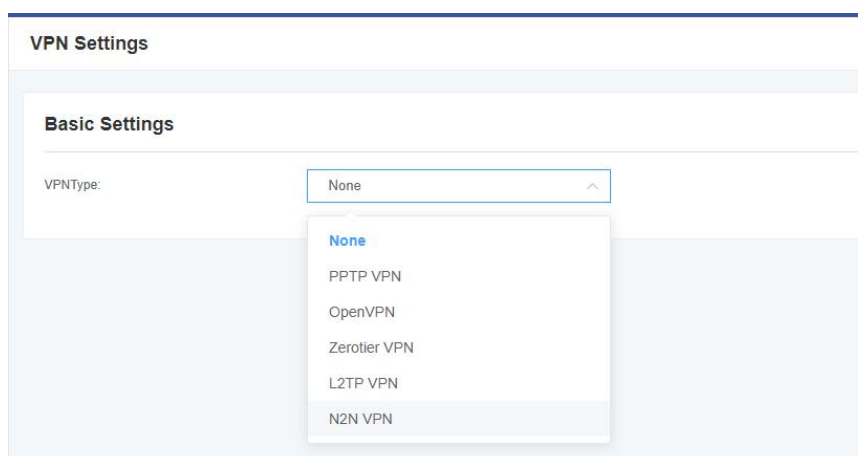
**Table 6-1-1 Definition of Network Settings**

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

## 6.2 VPN Settings

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

**Figure 6-2-1 VPN Interface**

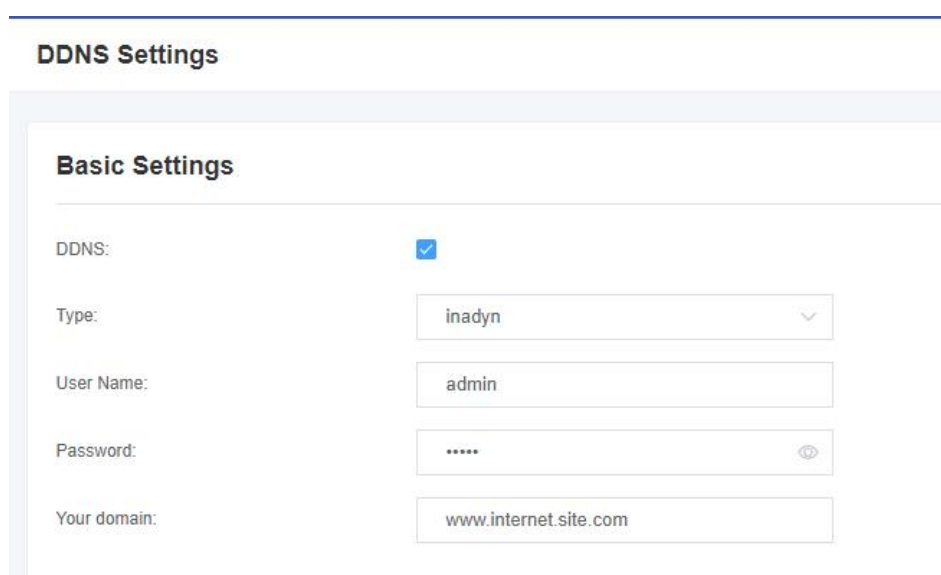


The screenshot displays the 'VPN Settings' configuration page. Under the 'Basic Settings' section, the 'VPNType:' field has a dropdown menu open. The dropdown lists the following options: 'None' (highlighted in blue), 'PPTP VPN', 'OpenVPN', 'Zerotier VPN', 'L2TP VPN', and 'N2N VPN'.

## 6.3 DDNS Settings

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

**Figure 6-3-1 DDNS Interface**



The screenshot displays the 'DDNS Settings' configuration page. Under the 'Basic Settings' section, the 'DDNS:' checkbox is checked. The 'Type:' dropdown menu is set to 'inadyn'. The 'User Name:' field contains 'admin'. The 'Password:' field contains six dots, with an eye icon to its right. The 'Your domain:' field contains 'www.internet.site.com'.



**Table 6-3-1 Definition of DDNS Settings**

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

## 6.4 Toolkit

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

**Figure 6-4-1 Network Connectivity Checking**

**Toolkit**

---

**Ping and Traceroute**

---

Interface:

Ping:

Traceroute:

**Figure 6-4-2 Channel Recording**

**Channel Recording**

---

Interface:

Source host:

Destination host:

Port:

Add a Tcpdump parameter option:

Figure 6-4-3 Capture Network Data

**Toolkit**

---

**Ping and Traceroute**

Interface:

Ping:

Traceroute:

---

**Channel Recording**

Interface:

Source host:

Destination host:

Port:

Add a Tcpdump parameter option:

Other Options:

Table 6-4-1 Definition of Channel Recording

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

## 6.5 Security Settings

Figure 6-5-1 Security Settings Interface

**Security Settings**

**Firewall Settings**

Firewall Enable:

Ping Enable:

**White List Settings**

White List Enable:

List IP Settings:

**Black List Settings**

Black List Enable:

List IP Settings:

## 6.6 Security Rules

Figure 6-6-1 Security Rules Interface

**Security Rules**

Rule Name:

Protocol:

Port:

IP / MASK:

Actions:

## 7. Advanced

### 7.1 Asterisk API

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

**Figure 7-1-1 API Interface**

**Asterisk API**

**General**

Enable:

Port: 5038

**Manager**

Manager Name:  Manager secret:

Deny:  Permit:

**Rights**

System:	<input checked="" type="checkbox"/> read	<input checked="" type="checkbox"/> write	Call:	<input checked="" type="checkbox"/> read	<input checked="" type="checkbox"/> write
Log:	<input checked="" type="checkbox"/> read	<input checked="" type="checkbox"/> write	Verbose:	<input checked="" type="checkbox"/> read	<input checked="" type="checkbox"/> write
Command:	<input type="checkbox"/> read	<input checked="" type="checkbox"/> write	Agent:	<input checked="" type="checkbox"/> read	<input checked="" type="checkbox"/> write
User:	<input checked="" type="checkbox"/> read	<input checked="" type="checkbox"/> write	Config:	<input checked="" type="checkbox"/> read	<input checked="" type="checkbox"/> write
DTMF:	<input checked="" type="checkbox"/> read	<input type="checkbox"/> write	Reporting:	<input checked="" type="checkbox"/> read	<input checked="" type="checkbox"/> write
CDR:	<input checked="" type="checkbox"/> read	<input type="checkbox"/> write	Dialplan:	<input checked="" type="checkbox"/> read	<input type="checkbox"/> write
Originate:	<input type="checkbox"/> read	<input checked="" type="checkbox"/> write			
All:	<input type="checkbox"/> read	<input type="checkbox"/> write			

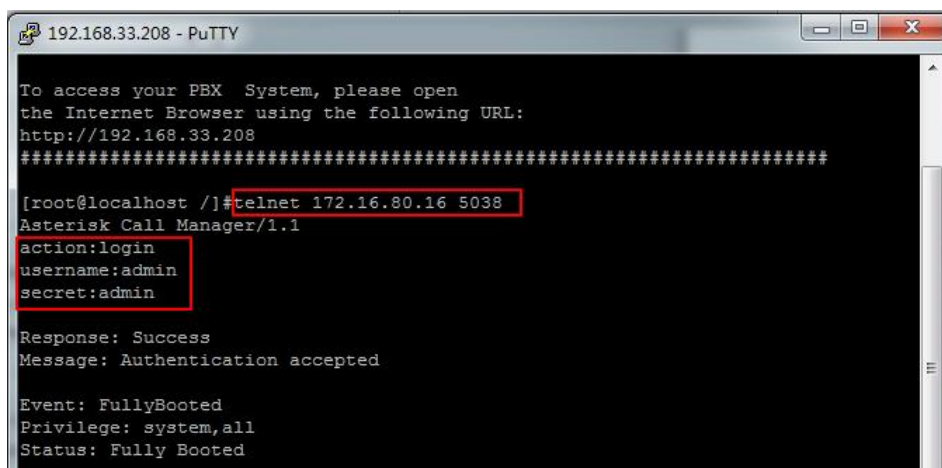
**Table 7-1-1 Definition of Asterisk API**

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

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

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

**Figure 7-1-2 Putty Access**



```

192.168.33.208 - PuTTY
To access your PBX System, please open
the Internet Browser using the following URL:
http://192.168.33.208
*****
[root@localhost ~]#telnet 172.16.80.16 5038
Asterisk Call Manager/1.1
action:login
username:admin
secret:admin

Response: Success
Message: Authentication accepted

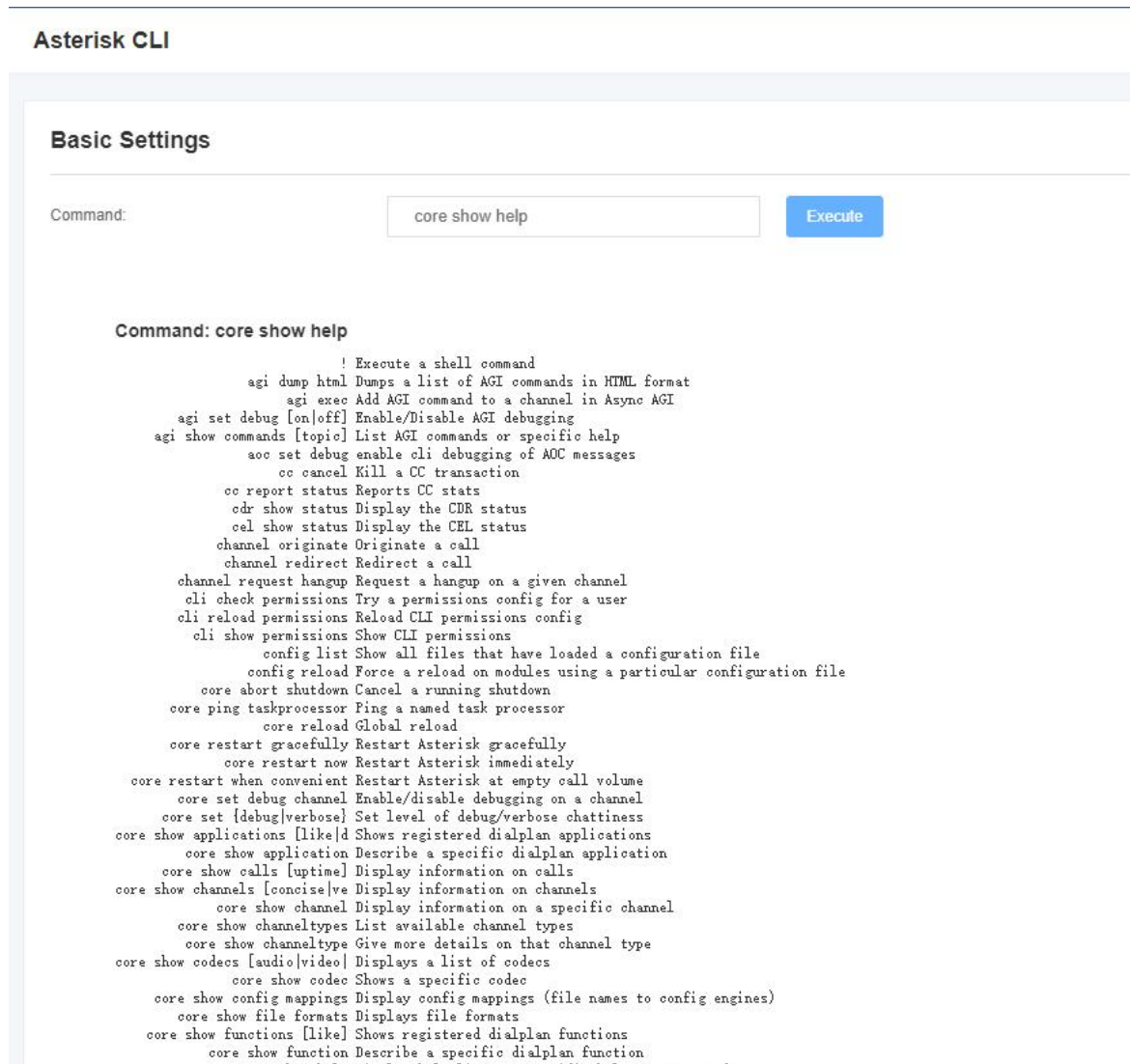
Event: FullyBooted
Privilege: system,all
Status: Fully Booted

```

## 7.2 Asterisk CLI

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

**Figure 7-2-1 Asterisk Command Interface**



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

**Table 7-2-1 Definition of Asterisk CLI**

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

## 7.3 Asterisk File Editor

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

**Figure 7-3-1 Configuration Files List**

**Asterisk File Editor**

File Name	File Size	Actions
asterisk.conf	279	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
astmanager.conf	0	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
astmanproxy.conf	445	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
cdr.conf	572	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
cdr_sqlite3_custom.conf	708	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
chan_dahdi.conf	255	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
chan_magneto.conf	142	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
company_info.conf	190	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
dahdi-channels.conf	14812	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
dahdi_groups.conf	0	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Total 50    10/page    < 1 2 3 4 5 >    Go to 1

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

## 7.4 Cloud Management

**Figure 7-4-1 Cloud Management Interface**

**Cloud**

**General**

Enable Cloud Service:

Choose Service:

Account:

Password:

Don't have an account? [Sign up](#)

## 7.5 TR069

Figure 7-4-1 TR069 Interface


**TR069 Settings**

**General**

TR069:

Server:

User Name:

Password:  

Provisioning code:

Model Name:

Periodic inform enable:

Periodic inform interval:

Connection request URL:

Connection request username:

Connection request password:

Connection Status: **Failed to Connect**



## 7.6 SNMP

Figure 7-4-1 SNMP Interface

**General**
Save

**SNMP Parameter**

SNMP Enable: <input type="checkbox"/>	System Contact: <input style="width: 80%;" type="text"/>
System Location: <input style="width: 80%;" type="text"/>	Support SNMP Version: <input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input checked="" type="checkbox"/> v3
SNMP Version: <input type="text" value="v1"/>	

**Community Configuration(V1)**

Security Name: <input style="width: 80%;" type="text" value="notConfigUser"/>	Souce: <input style="width: 80%;" type="text" value="default"/>
Community: <input style="width: 80%;" type="text" value="public"/>	

**Group Configuration(V1)**

Group: <input style="width: 80%;" type="text" value="notConfigGroup"/>	Security Name: <input style="width: 80%;" type="text" value="notConfigUser"/>
--	---

**View Configuration(V1)**

ViewName: <input style="width: 80%;" type="text" value="allview"/>	ViewType: <input type="text" value="included"/>
ViewSubtree: <input style="width: 80%;" type="text" value=".1"/>	ViewMask: <input style="width: 80%;" type="text"/>

**Access Configuration(V1)**

Group: <input style="width: 80%;" type="text" value="notConfigGroup"/>	read: <input type="text" value="notConfigGroup"/>
write: <input type="text" value="none"/>	Notify: <input type="text" value="none"/>

## 7.7 Auto Provision

Figure 7-4-1 Auto Provision Interface

**Auto Provision Settings**

Firmware Enable:	<input type="checkbox"/>
Configuration Enable:	<input checked="" type="checkbox"/>
DHCP Option 66:	<input checked="" type="checkbox"/>
Auto Config Server URL:	<input style="width: 80%;" type="text"/>
Upgrade Mode:	<input type="text" value="Immediately"/>

## 8. Logs

### 8.1 Log Settings

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

**Figure 8-1-1 Logs Settings**

**Log Settings**

<b>System Logs</b>			
System Logs:	<input checked="" type="checkbox"/>	Auto clean:	<input checked="" type="checkbox"/>
		maxsize:	5MB
<b>Asterisk Logs</b>			
Verbose:	<input checked="" type="checkbox"/>	Notice:	<input checked="" type="checkbox"/>
Debug:	<input checked="" type="checkbox"/>	Error:	<input checked="" type="checkbox"/>
Auto clean:	<input checked="" type="checkbox"/>	maxsize:	5MB
		Warning:	<input checked="" type="checkbox"/>
		DTMF:	<input checked="" type="checkbox"/>
<b>SIP Logs</b>			
SIP Logs:	<input checked="" type="checkbox"/>	Auto clean:	<input checked="" type="checkbox"/>
		maxsize:	5MB
<b>CDR</b>			
CDR:	<input checked="" type="checkbox"/>	Auto clean:	<input checked="" type="checkbox"/>
		maxsize:	20MB
<b>Syslog</b>			
Local Syslog:	<input type="checkbox"/>	Server Address:	
Klog Level:	EMERG	Server Port:	0
		CDR Level:	OFF

**Figure 8-1-2 System Logs Output**

**System Logs**

```
[2022/01/24 06:33:34] Auto restore configuration files
[2022/01/24 14:34:33] Power on
[2022/01/24 14:35:17] Power on
[2022/01/24 14:36:11] Factory reset from external.
[2022/01/24 14:36:12] Restore configuration files
[2022/01/24 06:33:30] Auto restore configuration files
[2022/01/24 14:34:42] Power on
[2022/02/09 15:57:07] Power on
[2022/02/14 15:37:29] Power on
[2022/02/14 16:30:15] Power on
[2022/02/14 16:33:47] Power on
[2022/02/14 16:37:09] Power on
[2022/02/14 16:41:25] Power on
[2022/02/14 16:43:59] Power on
[2022/02/14 16:47:23] Power on
[2022/02/14 16:50:47] Power on
[2022/02/14 16:54:07] Power on
[2022/02/14 16:57:44] Power on
[2022/02/14 17:01:27] Power on
[2022/02/14 17:04:51] Power on
[2022/02/14 17:08:05] Power on
[2022/02/14 17:11:37] Power on
[2022/02/14 17:15:11] Power on
[2022/02/14 17:18:33] Power on
[2022/02/14 17:22:08] Power on
[2022/02/14 17:23:22] Power on
[2022/02/14 17:29:01] Power on
[2022/02/14 17:34:17] Power on
[2022/02/14 17:38:47] Power on
[2022/02/14 17:43:57] Power on
```

**Figure 8-1-3 Asterisk Logs Output**

**Asterisk Logs**

```

[Mar 30 16:24:09] WARNING[1654] config.c: Unknown directive '#autoload=yes' at line 8 of /etc/asterisk/modules.conf
[Mar 30 16:24:09] NOTICE[1654] dnsmgr.c: Managed DNS entries will be refreshed every 1200 seconds.
[Mar 30 16:24:09] NOTICE[1654] cdr.c: CDR simple logging enabled.
[Mar 30 16:24:09] WARNING[1654] indications.c: Invalid ringcadence given ''.
[Mar 30 16:24:09] WARNING[1654] indications.c: Indication country 'custom' is invalid
[Mar 30 16:24:09] WARNING[1654] features.c: Could not load features.conf
[Mar 30 16:24:09] WARNING[1654] ocsc.c: Could not find valid ocsc.conf file. Using oc_max_requests default
[Mar 30 16:24:09] WARNING[1654] config.c: Unknown directive '#autoload=yes' at line 8 of /etc/asterisk/modules.conf
[Mar 30 16:24:09] NOTICE[1654] loader.c: 54 modules will be loaded.
[Mar 30 16:24:11] WARNING[1654] loader.c: Error loading module 'res_fax_spandsp.so': libtiff.so.3: cannot open shared object file: No such file or directory
[Mar 30 16:24:12] WARNING[1654] loader.c: Error loading module 'monitor.so': /usr/lib/asterisk/modules/monitor.so: cannot open shared object file: No such file or directory
[Mar 30 16:24:13] WARNING[1654] loader.c: Error loading module 'codec_g723.so': /usr/lib/asterisk/modules/codec_g723.so: cannot open shared object file: No such file or directory
[Mar 30 16:24:16] WARNING[1654] res_crypto.c: Unable to open key directory '/usr/lib/asterisk/keys'
[Mar 30 16:24:16] NOTICE[1654] res_smdl.c: Unable to load config smdl.conf: SMDI disabled
[Mar 30 16:24:16] NOTICE[1654] res_smdi.c: No SMDI interfaces are available to listen on, not starting SMDI listener.
[Mar 30 16:24:16] ERROR[1654] netsock2.c: getaddrinfo("stun.xten.com", "(null)", ...): Name or service not known
[Mar 30 16:24:16] WARNING[1654] acl.c: Unable to lookup 'stun.xten.com'
[Mar 30 16:24:16] WARNING[1654] res_stun_monitor.c: Unable to lookup STUN server 'stun.xten.com'
[Mar 30 16:24:16] WARNING[1654] res_stun_monitor.c: Invalid STUN server address: stun.xten.com at line 21
[Mar 30 16:24:16] WARNING[1654] res_fax.c: Configuration file 'res_fax.conf' not found, using default options.
[Mar 30 16:24:16] WARNING[1654] loader.c: Error loading module 'res_fax_spandsp.so': libtiff.so.3: cannot open shared object file: No such file or directory
[Mar 30 16:24:16] WARNING[1654] loader.c: Module 'res_fax_spandsp.so' could not be loaded.
[Mar 30 16:24:17] WARNING[1654] loader.c: Error loading module 'monitor.so': /usr/lib/asterisk/modules/monitor.so: cannot open shared object file: No such file or directory
[Mar 30 16:24:17] WARNING[1654] loader.c: Module 'monitor.so' could not be loaded.
[Mar 30 16:24:17] WARNING[1654] loader.c: Error loading module 'codec_g723.so': /usr/lib/asterisk/modules/codec_g723.so: cannot open shared object file: No such file or directory
[Mar 30 16:24:17] WARNING[1654] loader.c: Module 'codec_g723.so' could not be loaded.
[Mar 30 16:24:17] VERBOSE[1654] chan_sip.c: SIP channel loading...
[Mar 30 16:24:17] NOTICE[1654] chan_sip.c: The 'username' field for sip peers has been deprecated in favor of the term 'defaultuser'
    
```

**Figure 8-1-4 SIP Logs Output**

**SIP Logs**

```

SIP channel loading...
SIP channel loading...
    
```

**Table 8-1-1 Definition of LOG**

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

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

## 8.2 CDR

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

**Figure 8-3-1 Call Detail Record**

**CDR Logs**

Caller ID	Callee ID	From	To	Start Time	Duration	Result	Actions
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> From <input type="text"/> To <input type="text"/>	<input type="text"/> From <input type="text"/> To <input type="text"/>	All <input type="text"/>	<input type="button" value="Filter"/> <input type="button" value="Clean"/>
<input type="button" value="Delete"/> <input type="button" value="Clean Up"/> <input type="button" value="Export"/>							
<input type="checkbox"/>	Caller ID ↕	Callee ID ↕	From ↕	To ↕	Start Time ↕	Duration ↕	Result ↕
<input type="checkbox"/>	8100	8001	8100	port-1	2022-03-02 13:16:52	00:01:06	ANSWERED
<input type="checkbox"/>	8101	8002	8101	port-2	2022-03-02 13:17:14	00:00:43	ANSWERED
<input type="checkbox"/>	8102	8003	8102	port-3	2022-03-02 13:17:37	00:00:18	ANSWERED
<input type="checkbox"/>	8103	8004	8103	port-4	2022-03-02 13:17:18	00:00:36	ANSWERED
<input type="checkbox"/>	8102	8003	8102	port-3	2022-03-02 13:16:27	00:01:09	ANSWERED
<input type="checkbox"/>	8103	8004	8103	port-4	2022-03-02 13:16:08	00:01:09	ANSWERED