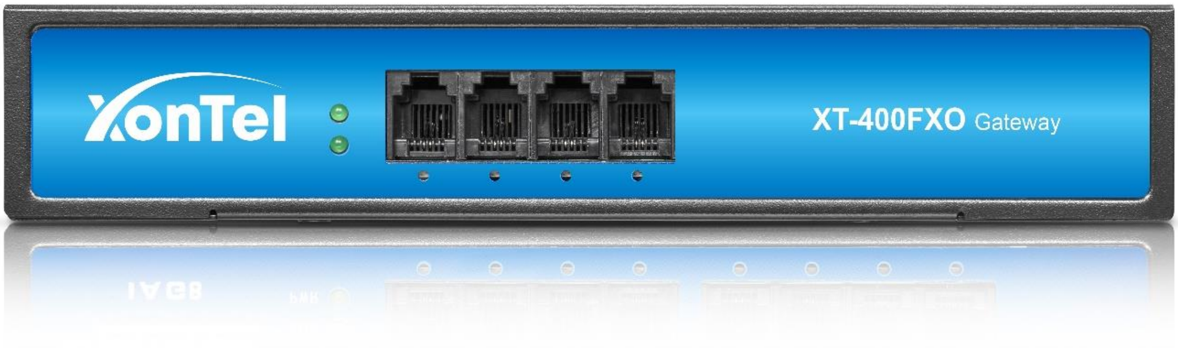
XT-400FXO Analog Gateway User Manual



Thank You for Choosing XonTel Products!

Confidentiality

Information contained herein is of a highly sensitive nature and is confidential and proprietary to XonTel 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 XonTel

Disclaimer

XonTel 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. XonTel 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 XonTel to ensure you have the latest version of this document.

Contents

1. Overview

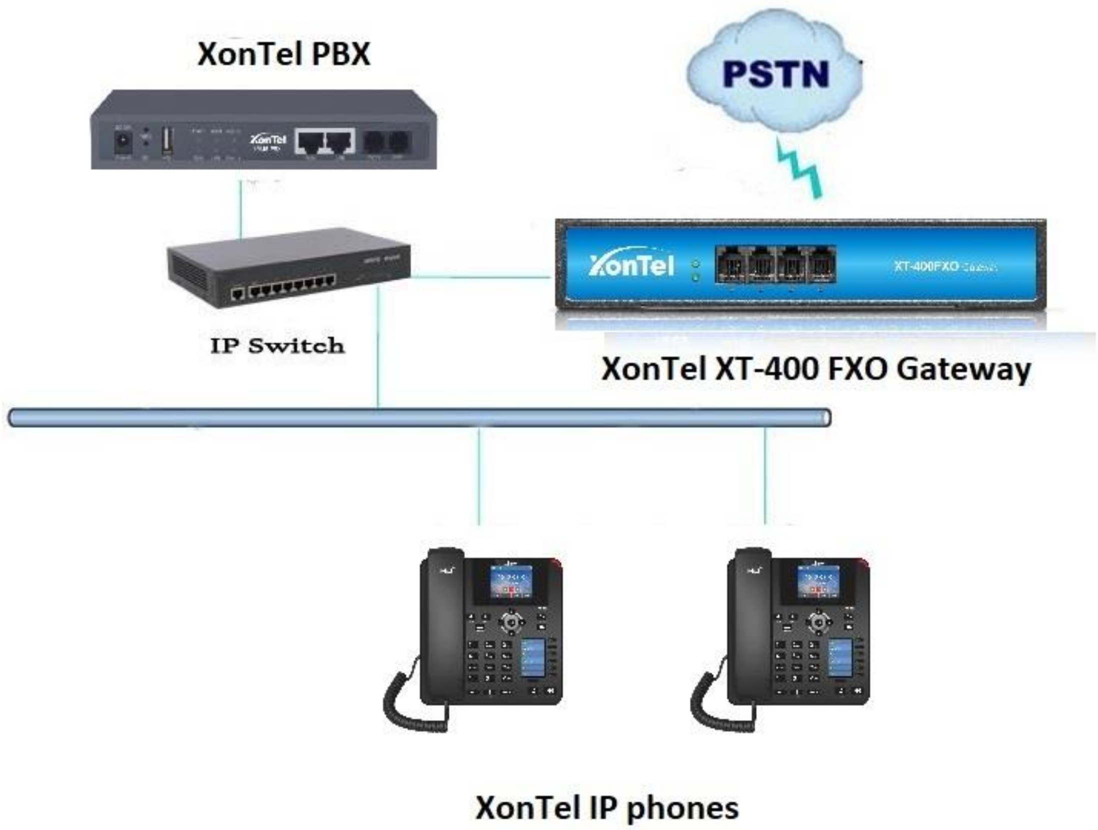
What is XT-400FXO Analog Gateway?

XonTel XT-400FXO Analog Gateway, an upgrade product of the XonTel 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 XT-400FXO Gateway is with 4 FXO ports for 4 PSTN lines.

The XT-400FXO Analog Gateway are developed for interconnecting a wide selection of codecs including G.711A, G.711U, G.729A, G.722, G.726, iLBC. XT-400FXO Gateway 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.

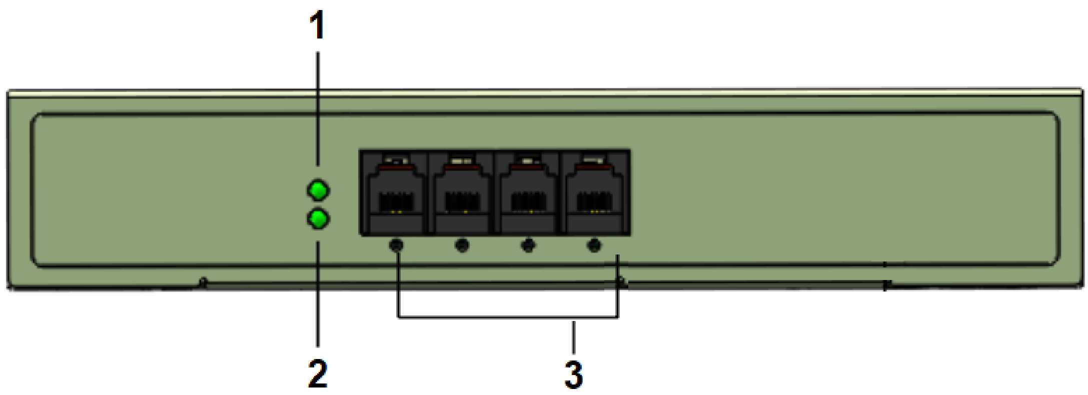
Sample Application

Figure 1-2-1 Topological Graph



Product Appearance

The picture below is appearance of XonTel XT-400FXO Analog Gateway.



1: Power Indicator

2: System LED

3: Analog Telephone Interfaces and corresponding Channels State Indicators

Figure 1-3-3 Back Panel

1: Power interface

2: Reset button

3: Ethernet ports and indicators

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.
- 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, 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 Echo cancellation, Jitter buffer.

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.

Physical Information

Description of Physical Information

Weight	637g
Size	19cm*3.5cm*14.2cm
Temperature	-20~70°C (Storage)
	0~50°C (Operation)

Operation humidity	10%~90% non-condensing
Power source	12V DC/2A
Max power	12W

Software

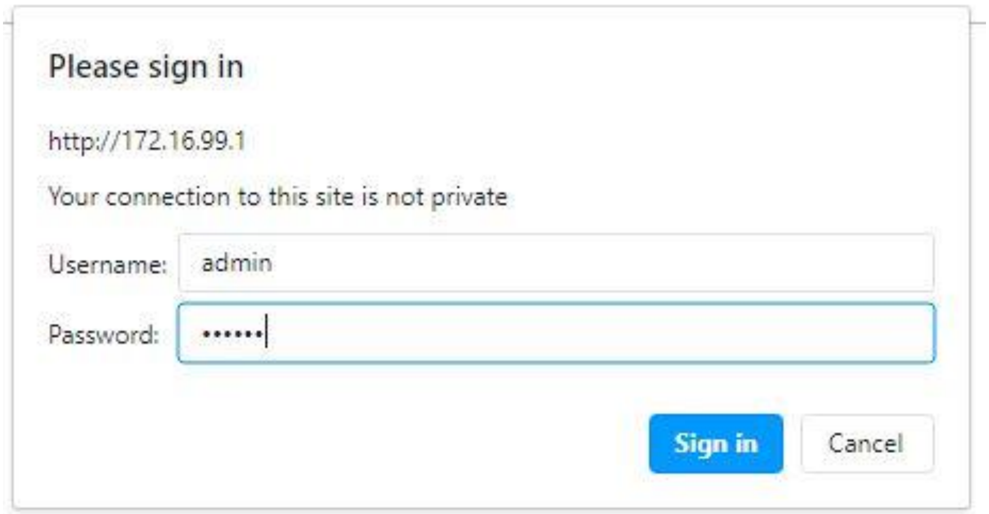
LAN2 Default IP: 172.16.99.1

Username: admin

Password: xontel

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

Login Interface

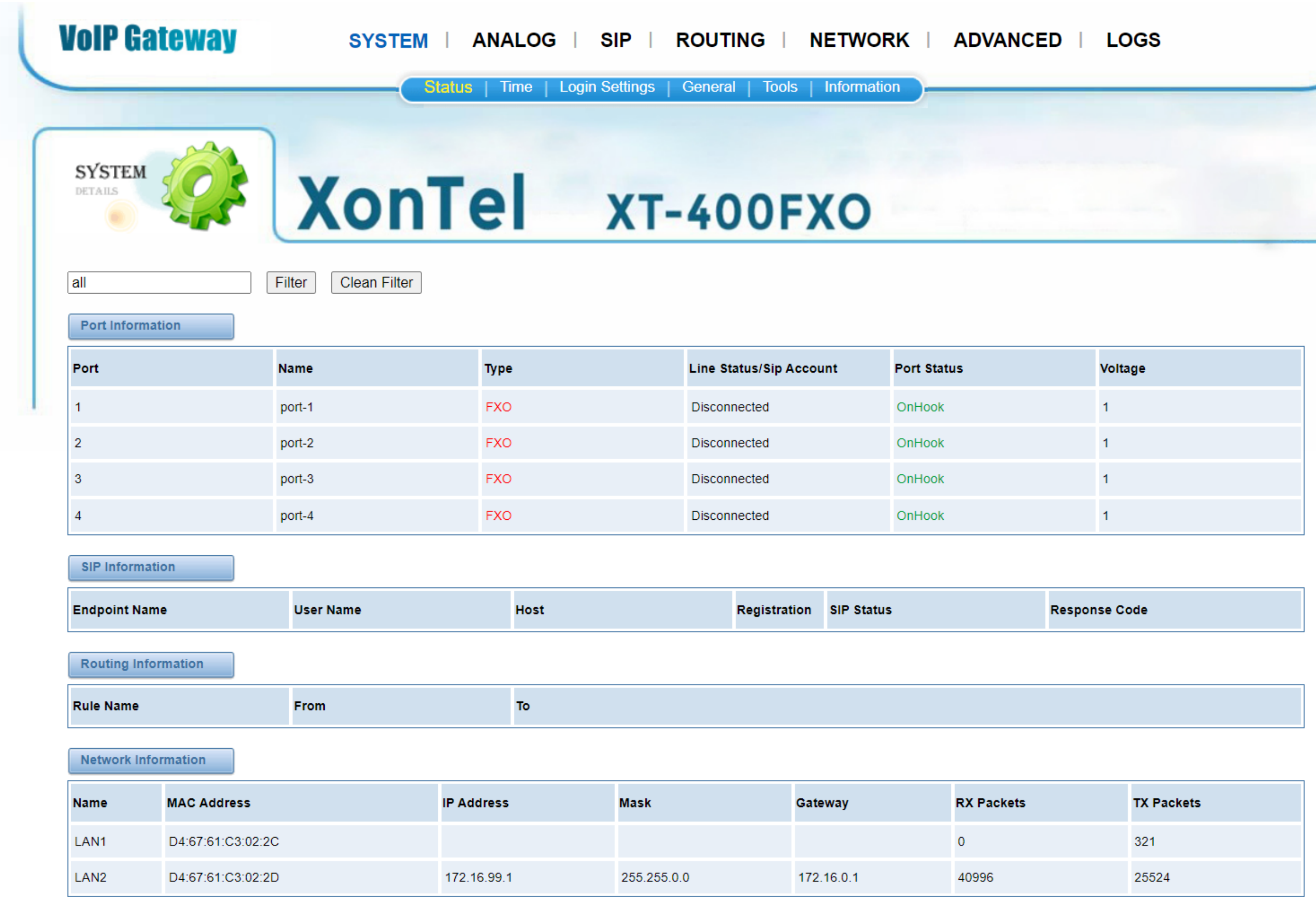


2. System

Status

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

Figure 2-1-1 System Status



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.

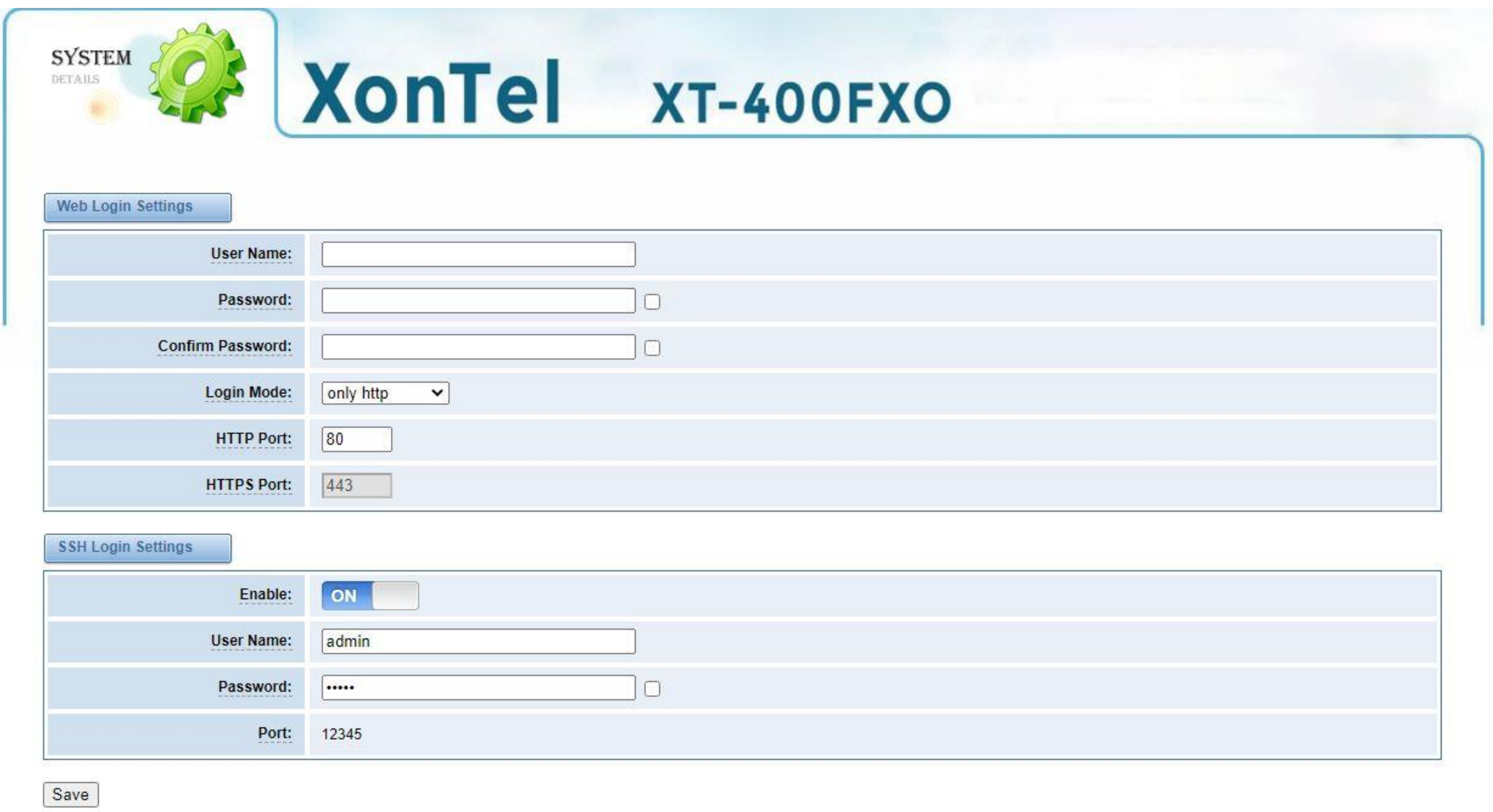
Login Settings

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 is "-_+. < >&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

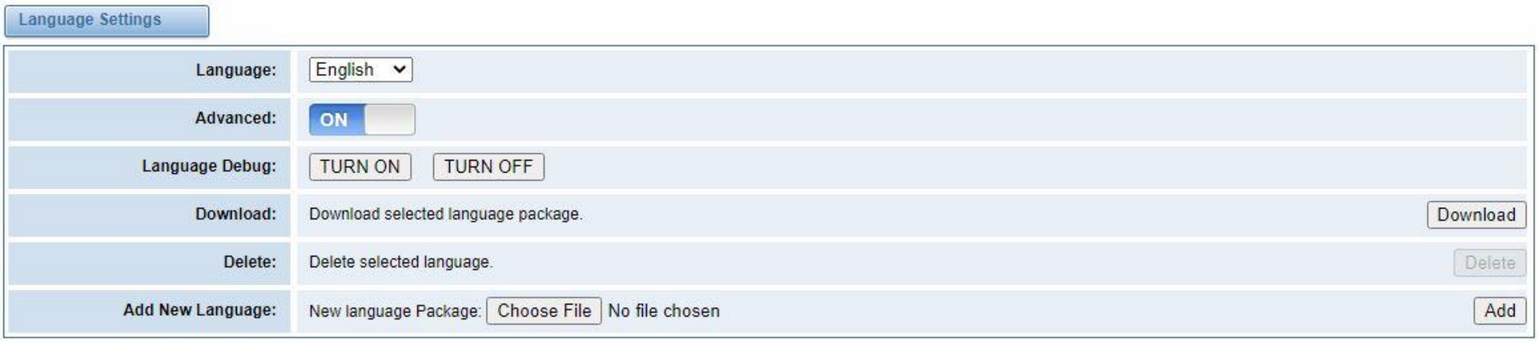


General

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.

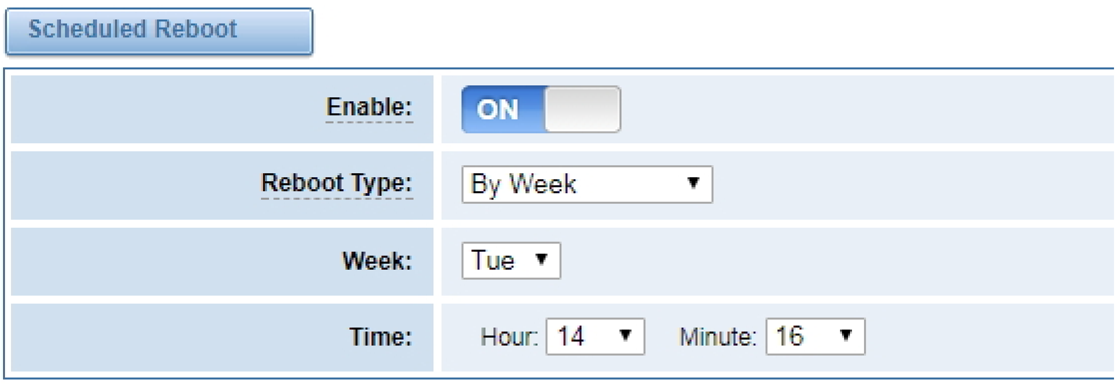
Figure 2-4-1 Language Settings



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



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

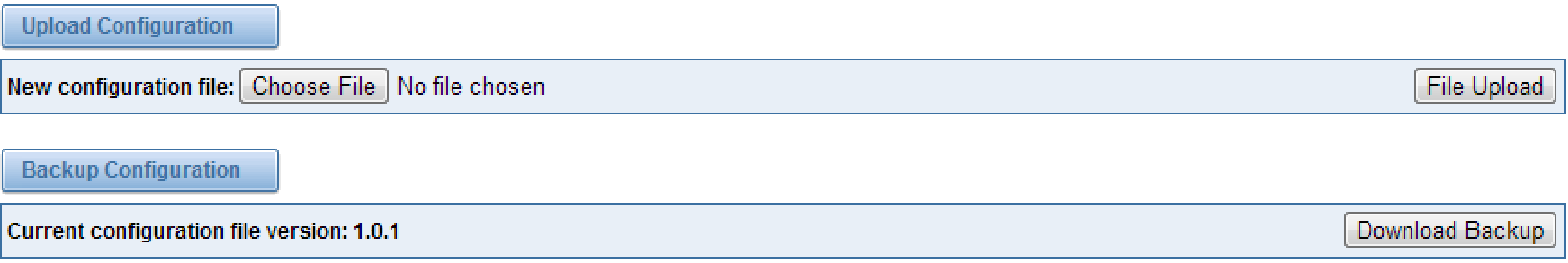
Options	Definition
System Reboot	This will turn off your gateway and then turn it back on. This will drop all current calls.
Asterisk Reboot	This will restart Asterisk and drop all current calls.

To update your system, click on “ **File Upload** “ to choose the XT-400FXO gateway firmware file from your PC then click on “ **System Update “**

Figure 2-5-2 Update Firmware

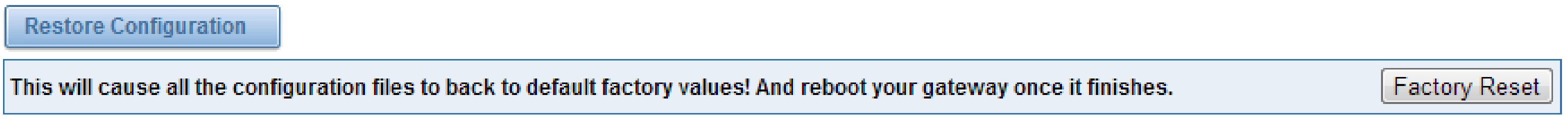
If you want to store your previous configuration, you can first backup configuration, then you can upload configuration directly. That will be very convenient for you. Notice, the version of backup and current firmware should be same, otherwise, it would not take effect.

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 XonTel 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:	XT-400FXO
Serial Number:	DB69B0641F192828
Software Version:	1.1.16
Hardware Version:	1.0.0
Slot Number:	1
Storage Usage:	360.0K/6.3M (6%)
Memory Usage:	64.7429 % Memory Clean
Build Time:	2020-12-15 10:28:39
System Time:	2020-12-15 06:07:24
System Uptime:	0 days 00:38:52

3. Analog

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

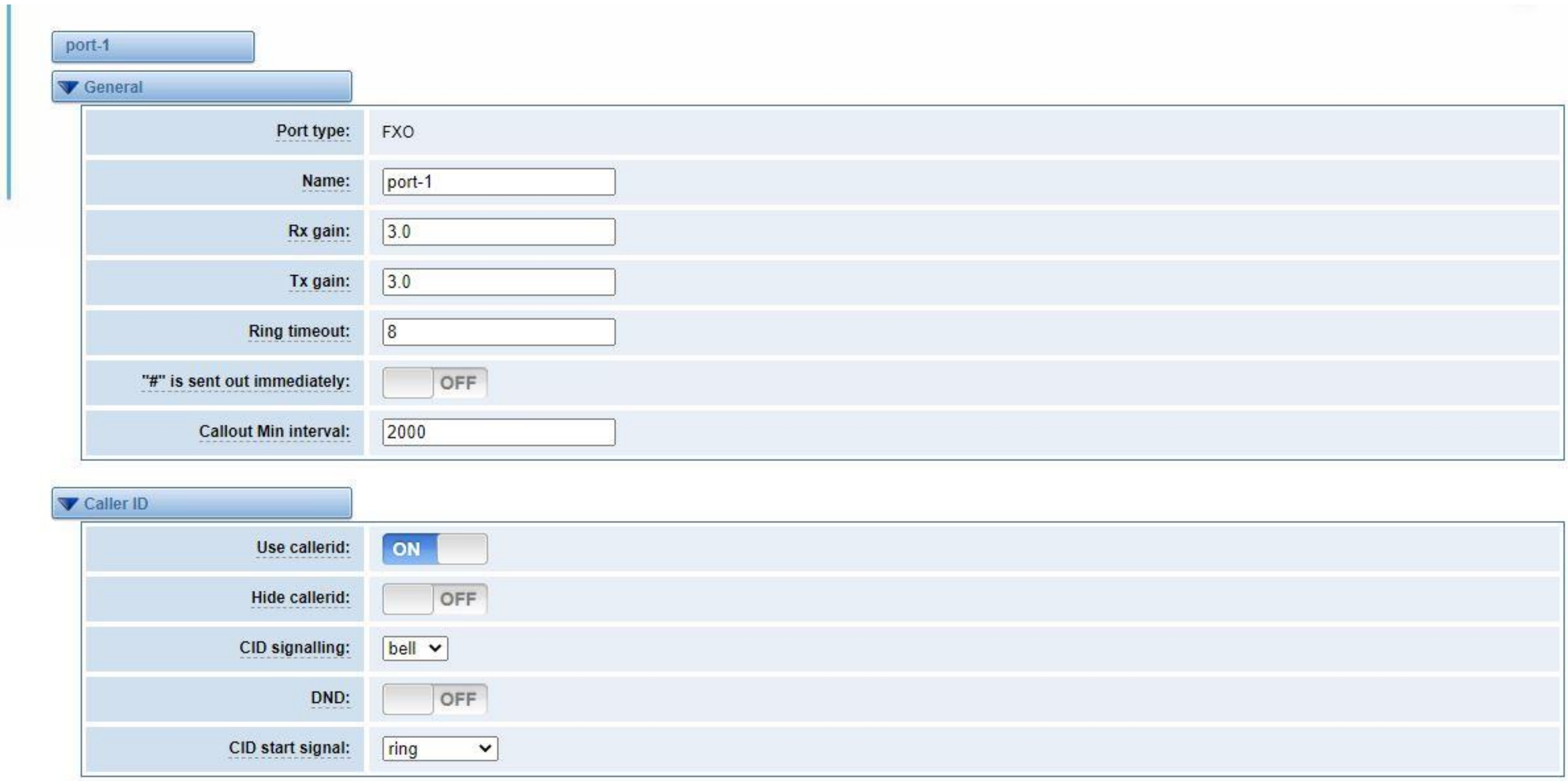
Channel Settings

Figure 3-1-1 Channel System

Port	Type	Name	Line Status/Sip Account	Port Status	Hour Call Count	Daily Call Count	Daily Answer Count	Call Status	Actions
1	FXO	port-1	Disconnected	OnHook	0	0	0	Unlimited	
2	FXO	port-2	Disconnected	OnHook	0	0	0	Unlimited	
3	FXO	port-3	Disconnected	OnHook	0	0	0	Unlimited	
4	FXO	port-4	Disconnected	OnHook	0	0	0	Unlimited	

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

Figure 3-1-2 FXO Port Configure



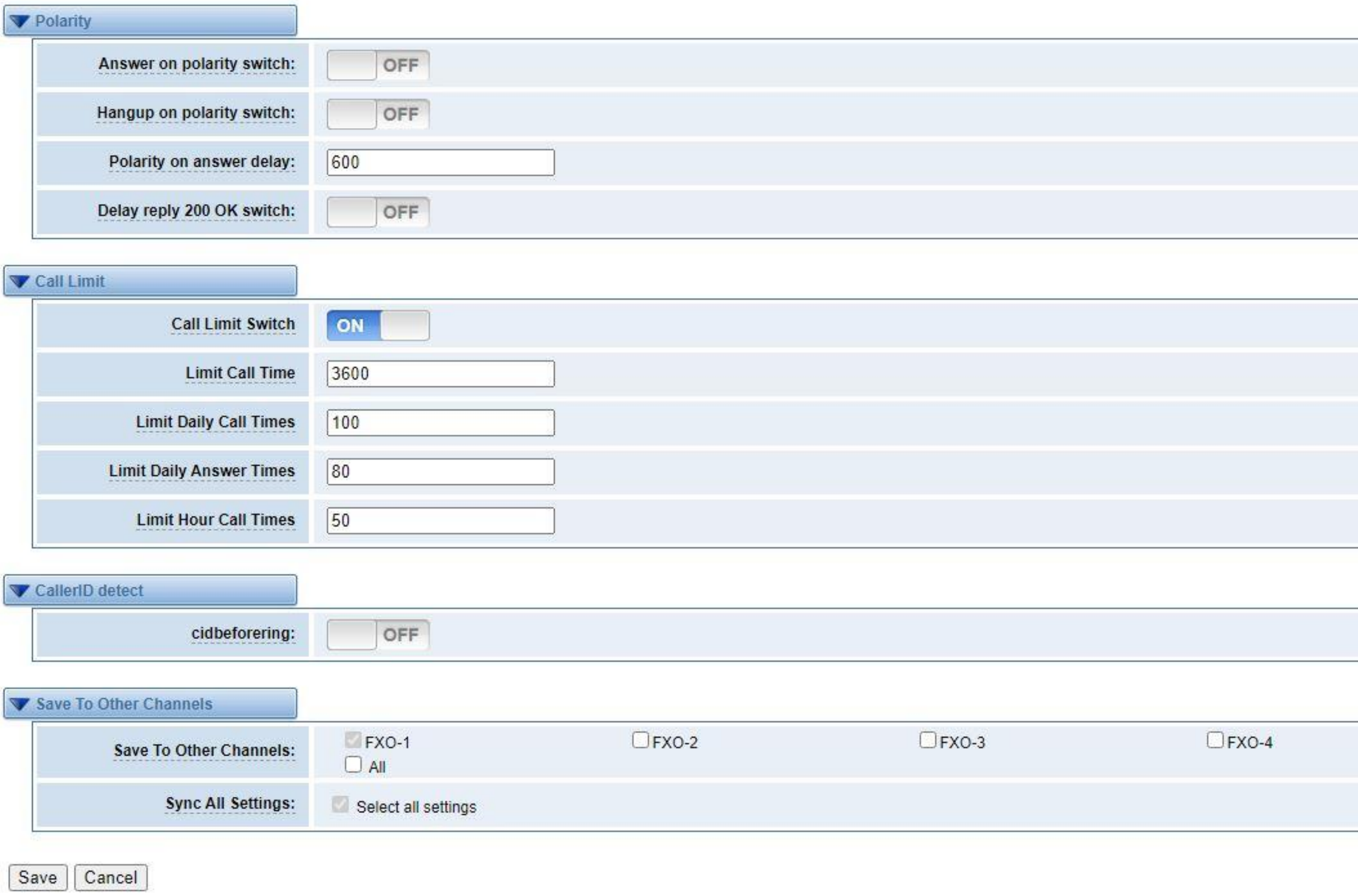


Table 3-1-1 Definition of FXO port settings

Options	**Definition**
Port-type	Read only, auto detected by the gateway.
Name	FXO port name.
Rx gain	Set the rx gain in dB. Range from -20.0dB to 6.0dB, in 0.1 dB increments.
Tx gain	Set the tx gain in dB, Range from -20.0dB to 6.0dB, in 0.1 dB increments.
Ring timeout	Set the ring timeout in seconds.
"#" is sent out immediately:	When pressing " # ", the call will be sent immediately.
Callout Min interval	Call out minimum interval. Range from 400-10000ms. Default is 2000ms
Use calledid	Use caller ID or not.
Hide callerid	Whether or not to hide outgoing caller ID.

CID signalling	Type of caller ID signaling in use
DND	Enable or disable do not disturb function
CID start signal	Set the signals of start of caller ID • ring: a ring signals the start (default). • polarity: polrity reversal signals the start. • polarity_IN: polrity reversal signals the start, for India. • dtmf: suitable in Denmark, Sweden, and Holland.
Answer on polarity switch	Use polarity reversal to mark when a outgoing call is answered by the remote party.
Hangup on polarity switch	In some countries, polarity reversal is used to signal the disconnect of phone line. If this option is selected, the call will be considered “hang-up “ on a polarity reversal.
Polarity on answer delay	Minimal time period (ms) between the answer polarity switch and hangup polarity switch. Default is 600ms.
Delay reply 200 OK switch	It is invalid when start polarity. Default is Off. • On: Delay timer in seconds to replay 200 ok • Off: Immedialtely replay 200 ok
Call Limit Switch	Enable or disable call limit. Default is Off.
cidbeforering	Save to handle irregular CID function.
Save To Other Channels	Save channel parameters to other channels synchronously.

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

Advanced Settings

Figure 3-3-1 General Configuration

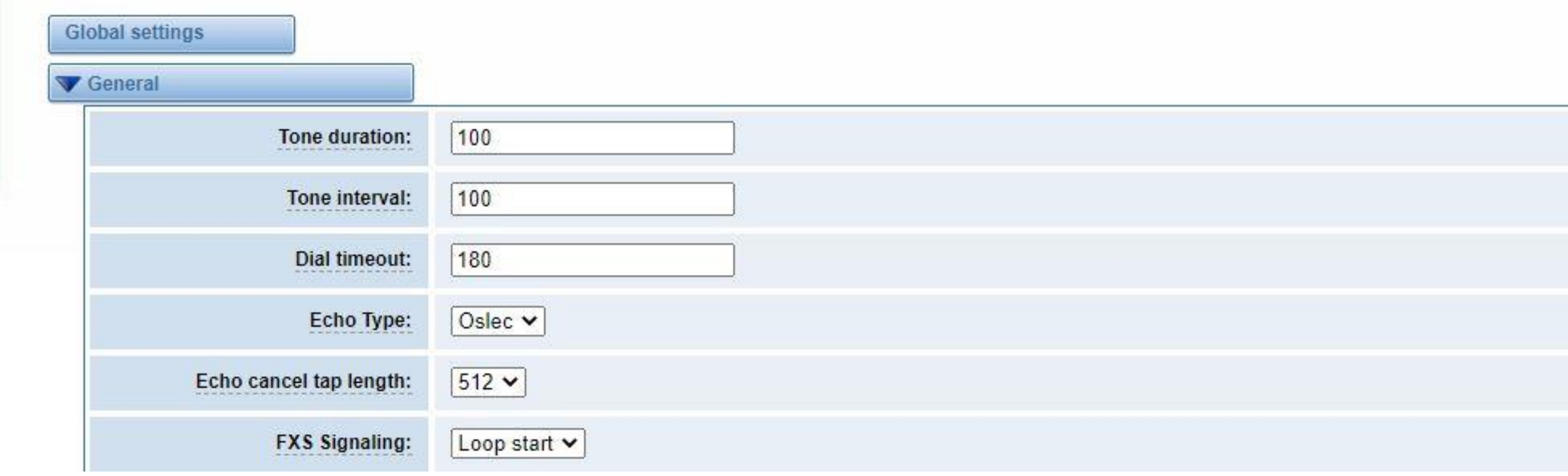


Table 3-3-1 Instruction of General

Options	**Definition**
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)
Dial timeout	Specifies the number of seconds we attempt to dial the specified devices.
Codec	Set the global encoding : mulaw, alaw.
Echo Type	Set the echo type (Oslec or Aec).
Echo cancel tap length	Hardware echo canceler tap length.
FXS signaling	Set the FXS signaling (Loop start or Kewlstart.

Figure 3-3-2 Fax Configuration

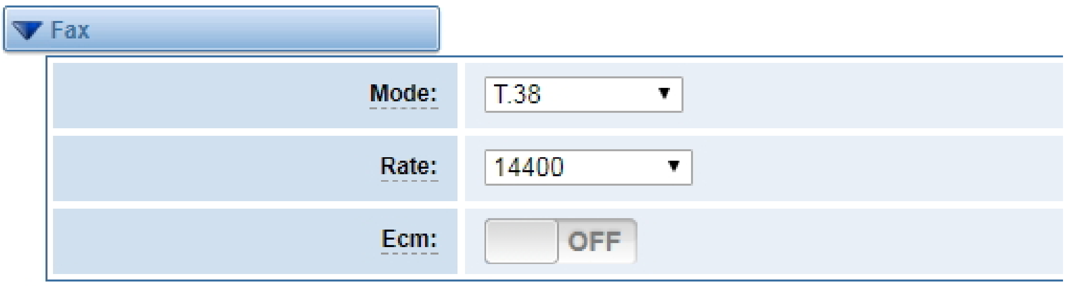


Table 3-3-2 Definition of Fax

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 3-3-3 Country Configuration

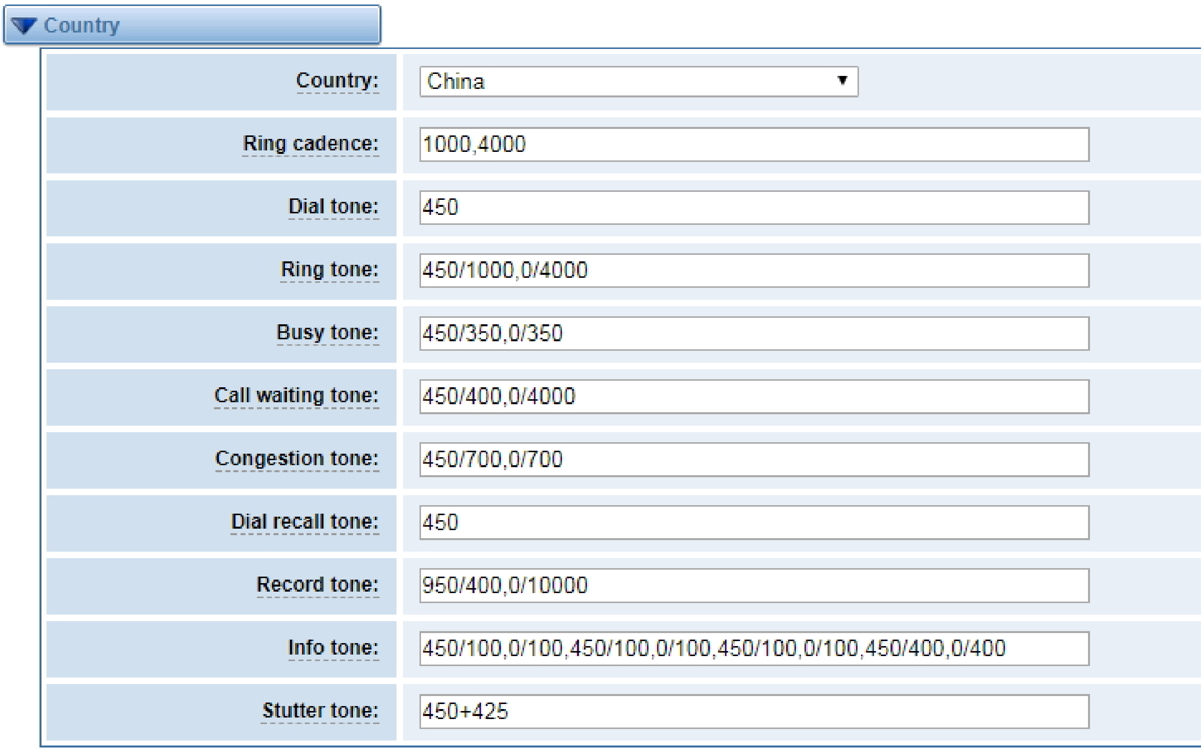


Table 3-3-3 Definition of Country

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.)

FXO

Figure 3-4-1 FXO settings

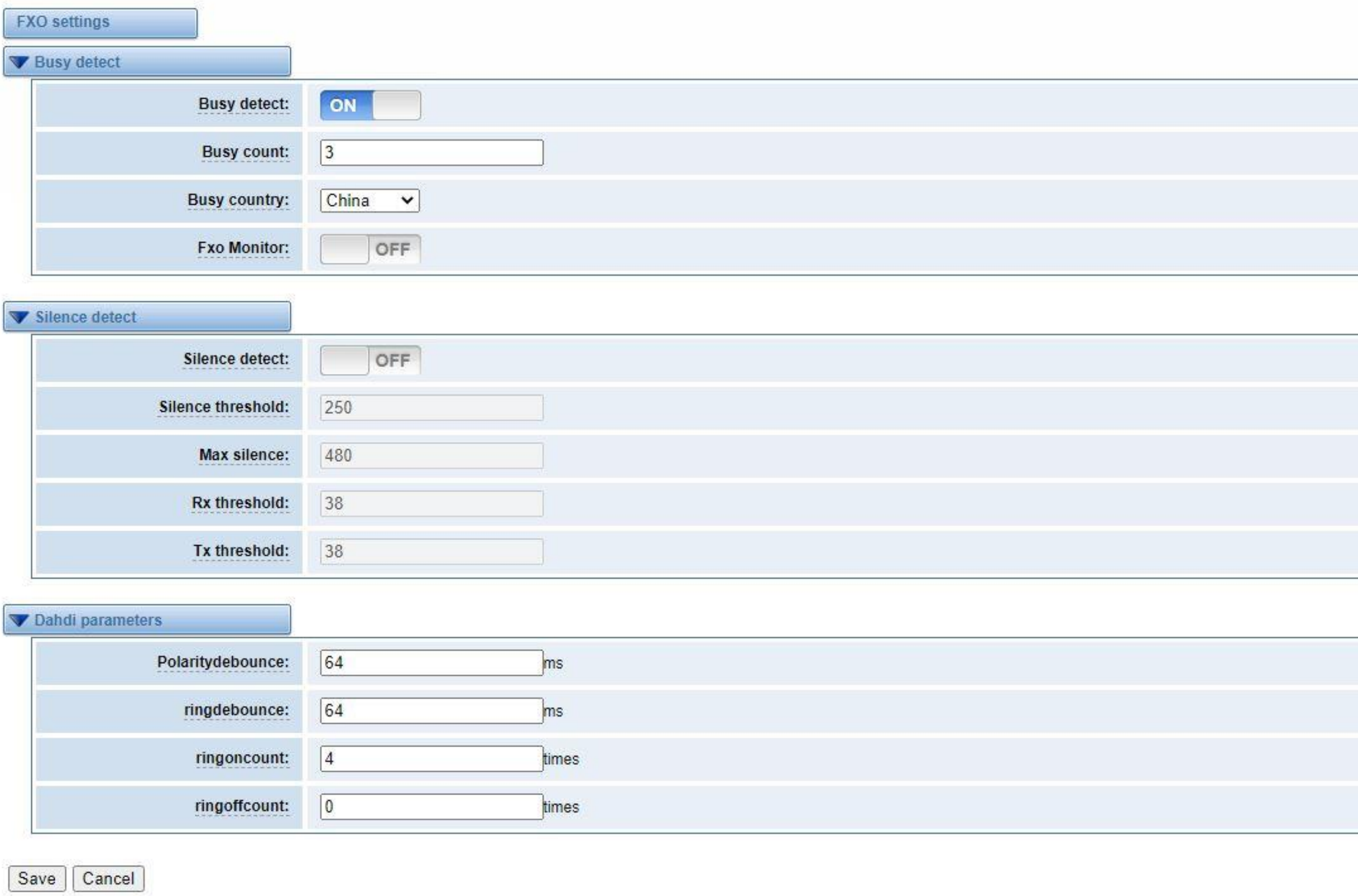


Table 3-4-1 Definition of FXO settings

Options	**Definition**
Busy detect	Enable or disable busy detection. Busy detect used for detecting busy signal or far end hang-up.
Busy count	Configure the number of busy tones the user will hear before hanging up the call when **Busy detect** is enabled.
Busy country	Select country for tone settings.
FXO Monitor	Enable or disable FXO monitor function.
Silence detect	Enable or disable silence detection function.
Silence threshold	What we consider silence: The lower, the more sensitive. Range: 100ms to 500ms. Default is 250ms.
Max silence	How silence threshold of silence before hanging up. (Eg: 16 is 250ms * 16=4s). Range: 2 to 1020(200ms to 512s).
Rx threshold	Rx threshold range: -20dbm0 to -40dbm0, default 38 (-38dbm0), all values are understood to be negative.
Tx threshold	Tx threshold range: -20dbm0 to -40dbm0, default 38 (-38dbm0), all values are understood to be negative.
Polaritydebounce	The time of polaritydebounce. Range from 0ms to 2048ms, default is 64ms.
Ringdebounce	The time of ringdebounce. Range from 0ms to 2048ms, default is 64ms.
ringoncount	Counting the times of ring on. Range from 0 to 128.
ringoffcount	Counting the times of ring off. Range from 0 to 128, default is 0.

Driver

Figure 3-5-1 Driver settings

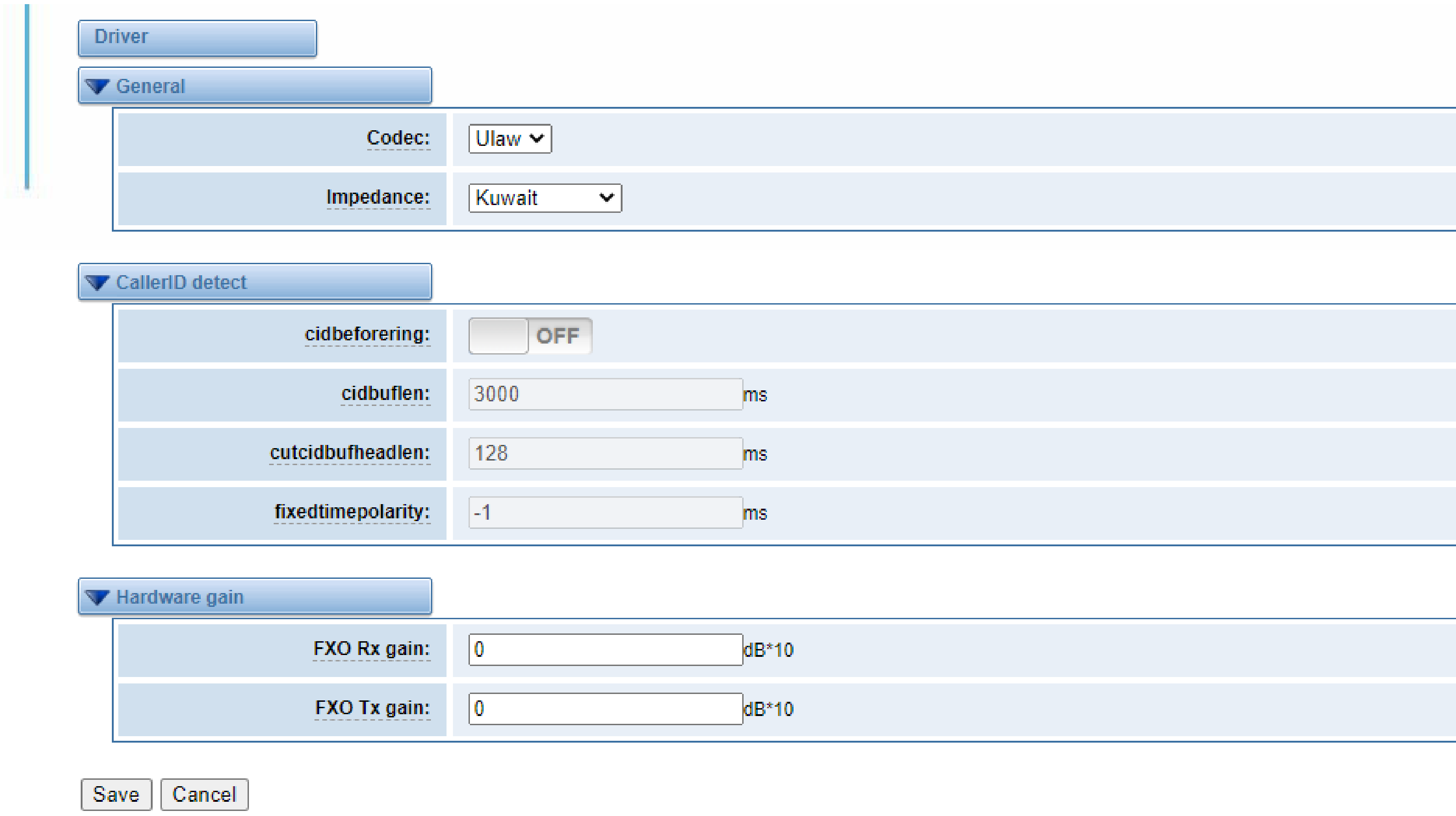


Table 3-5-1 Definition of Driver settings

Options	**Definition**
Codec	Set the global encoding that will be used in gateway (ulaw, alaw).
Impedance	Configuration for impedance.
cidbeforering	Switch to handle irregular CID function.
cidbuflen	CID media stream length byte size.
cutcidbufheadlen	CID media header length byte size.
fixedtimepolarity	Transmit polarity line reversal signal delay time.
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.

4. SIP

SIP Endpoints

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

Figure 4-1-1 SIP Status

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.

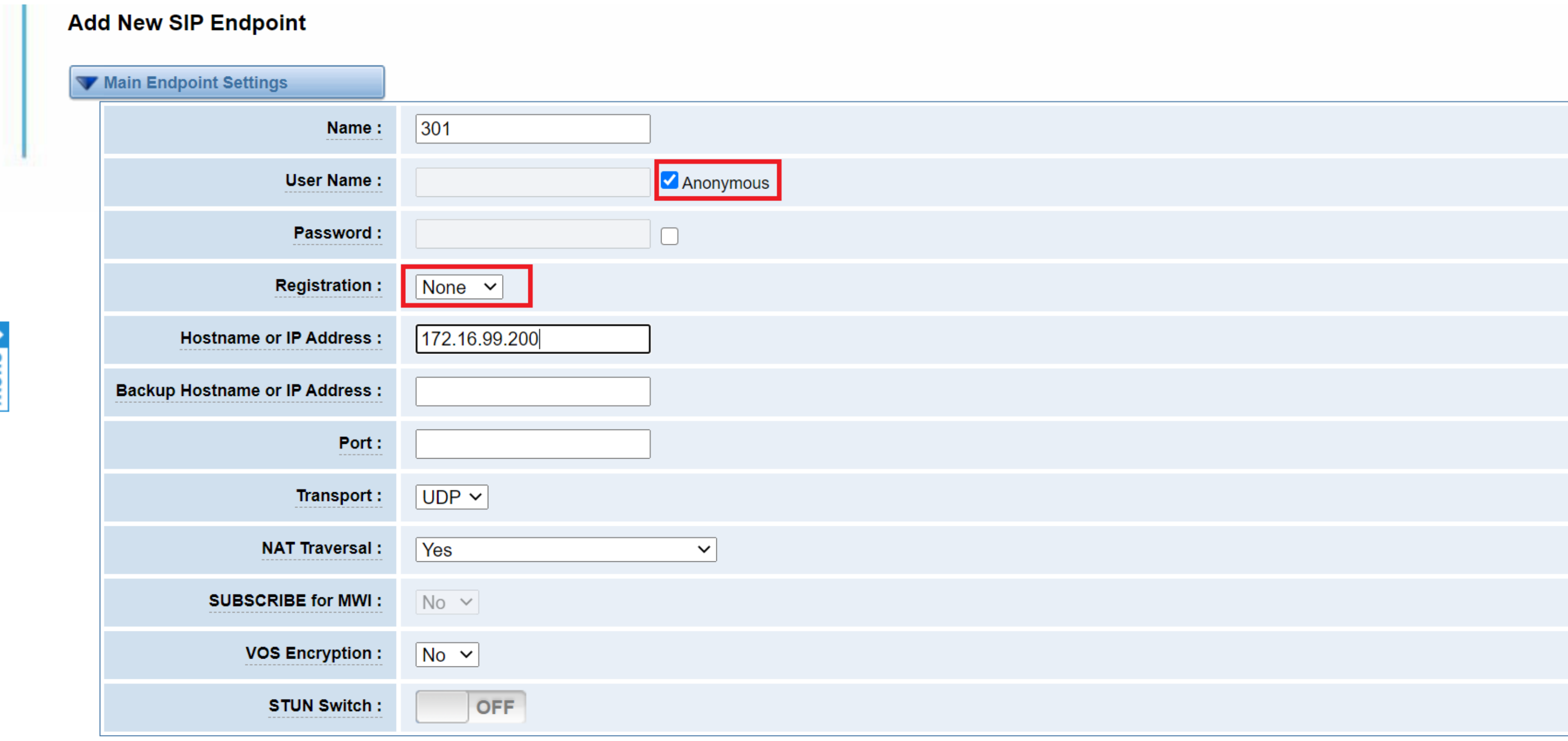
Main Endpoint Settings

There are 3 kinds of registration types for choose. You can choose " **Anonymous, Server or Client** ".

You can configure as follows:

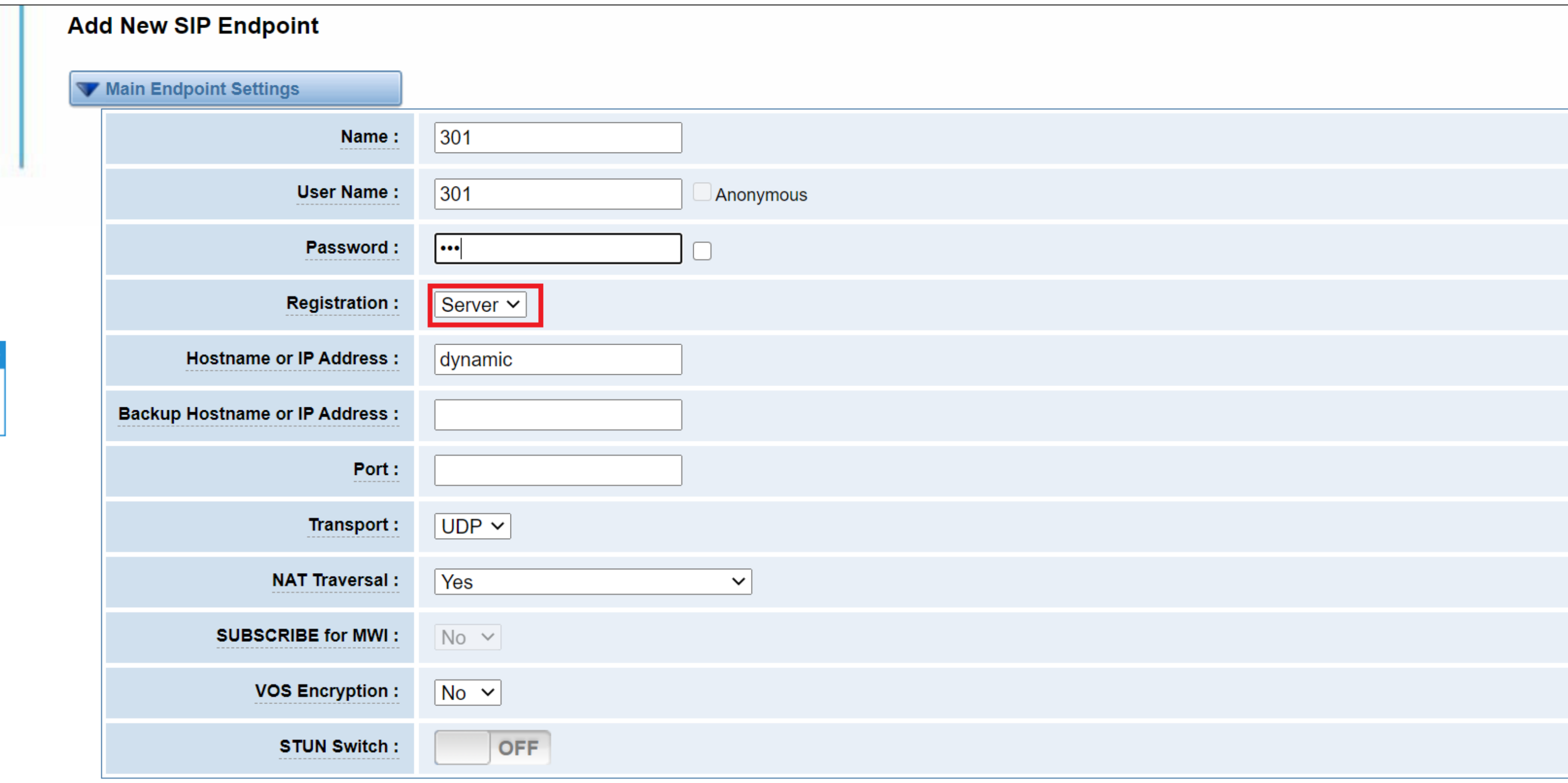
If you set up a SIP endpoint by registration " **None** " to a server, then you can't register other SIP endpoints to this server. (If you add other SIP endpoints, this will cause Out-band Routes and Trunks confused.)

Figure 4-1-2 Anonymous Registration



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

Figure 4-1-3 Register to Gateway



Also you can choose registration by " **Client** ", it's the same with "None", except name and password.

Figure 4-1-4 Register to Server

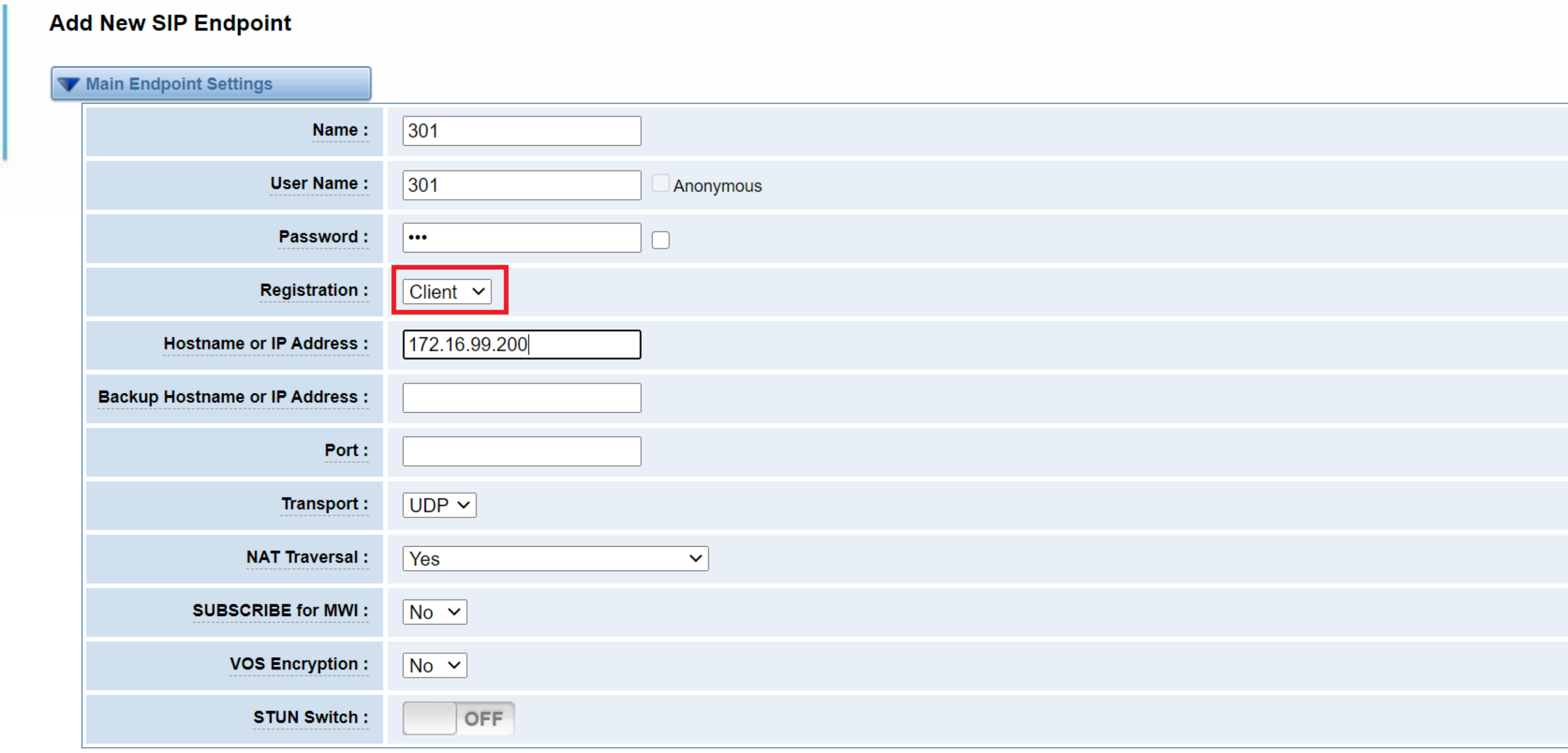


Table 4-1-1 Definition of SIP Options

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; **Server**---When register as this type, it means the FXO gateway acts as a SIP server, and SIP endpoints register to the gateway; **Client**---When register as this type, it means the FXO 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.
Backup Hostname or IP Address	Backup IP address or hostname of the endpoint.

Port	The port number the gateway will connect to at this endpoint.
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 sidesays to use it and perform comedia RTP handling.
SUBSCRIBE for MWI	Enable or disable subscribe to receive MWI.
VOS Encryption	Enable or disable VOS encryption.
STUN Switch	You need to turn the stun switch on the SIP advanced setting page to take effect.

Advanced: Registration Options

Figure 4-1-5 Advanced: Regitration Options

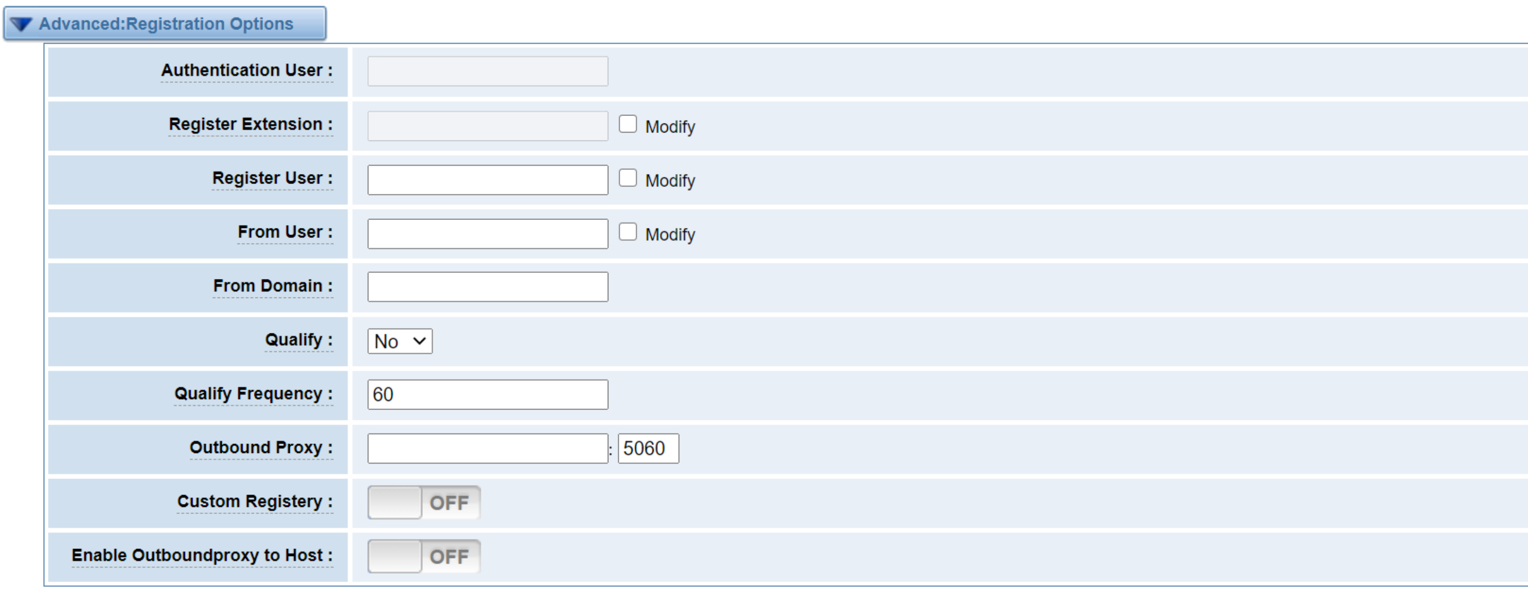


Table 4-1-2 Definition of Registration Options

Options	**Definition**
Authentication User	A username to use only for registration.
Register Extension	When Gateway registers as a SIP user agent to a SIP proxy (provider), calls from this provider connect to this local extension.
Register User	A register username to use for registration.
From User	A username to identify the gateway to this endpoint.
From Domain	A domain to identify the gateway to 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

Figure 4-1-6 Advanced: Regitration Options

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

Figure 4-1-7 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

Figure 4-1-8 Advanced: Timer Settings

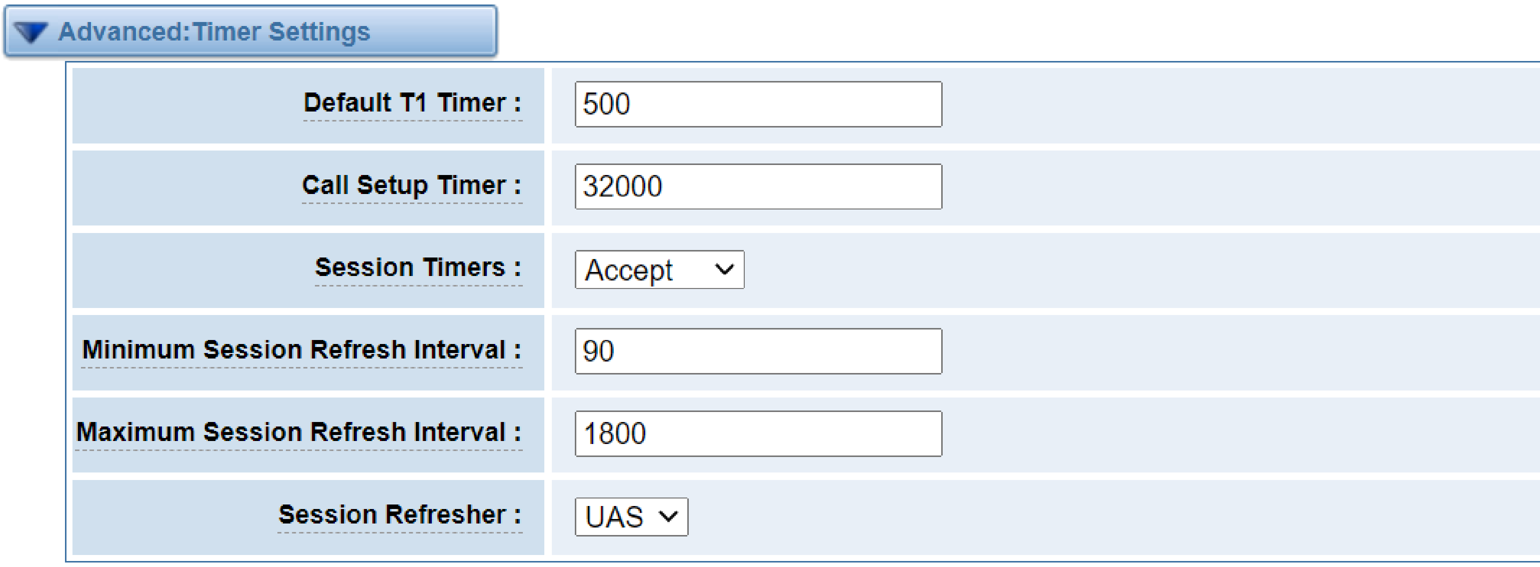


Table 4-1-5 Definition of Timer Options

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

Media Settings

Figure 4-1-9 Media Settings

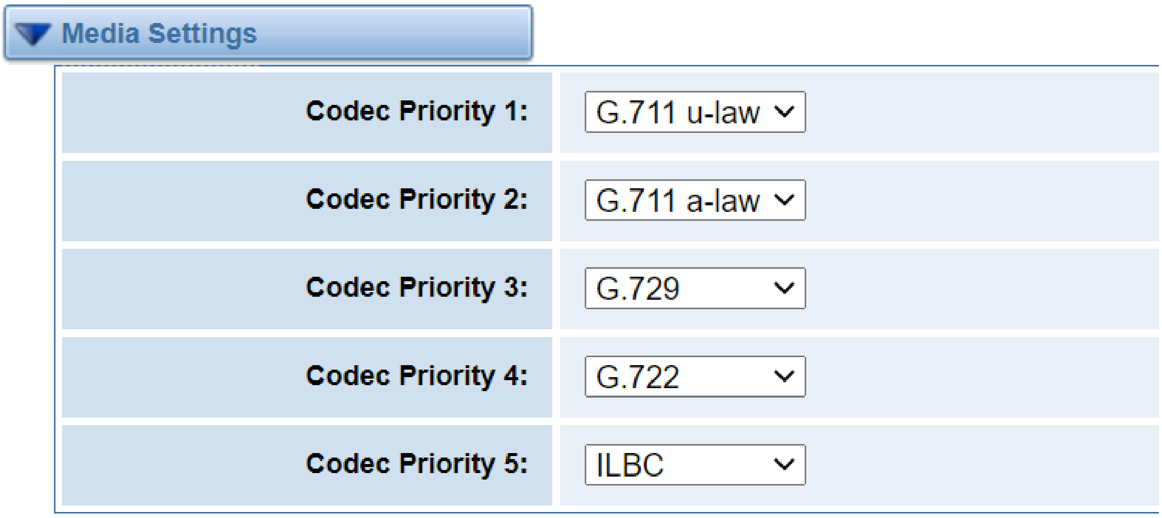


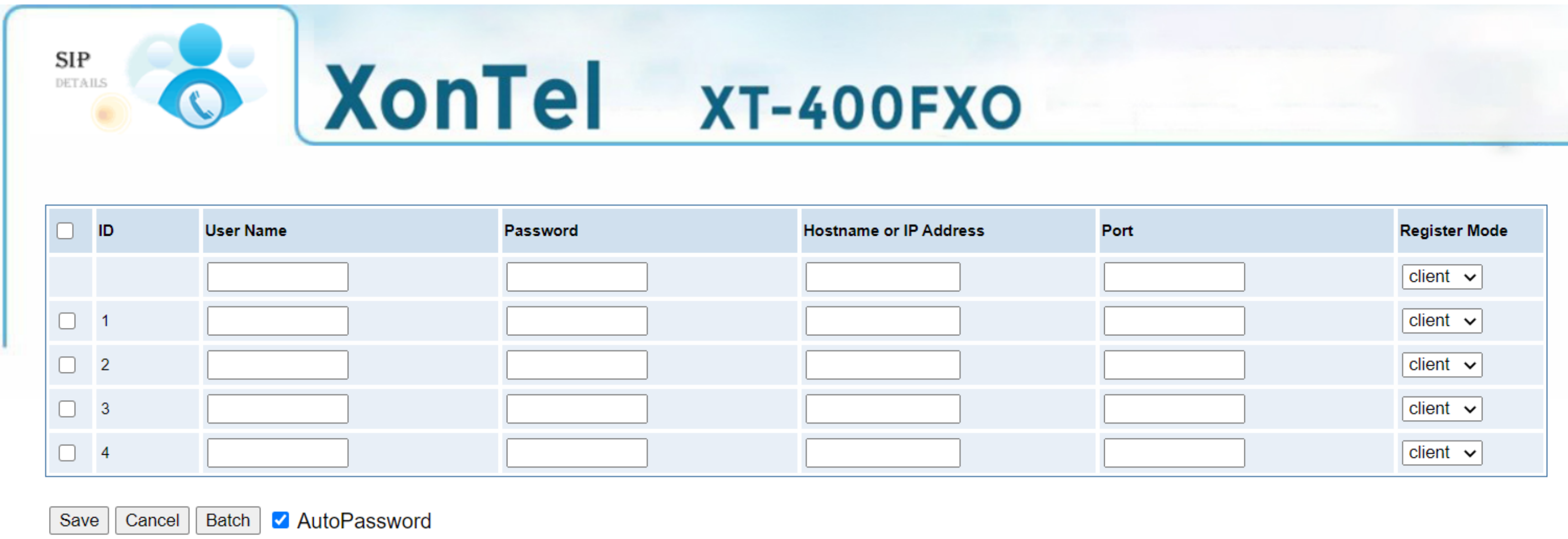
Table 4-1-6 Definition of Media Settings

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

Batch Create SIP

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

Figure 4-2-1 Batch SIP Endpoints



Advanced SIP Settings

Networking

Figure 4-3-1 Networking Options

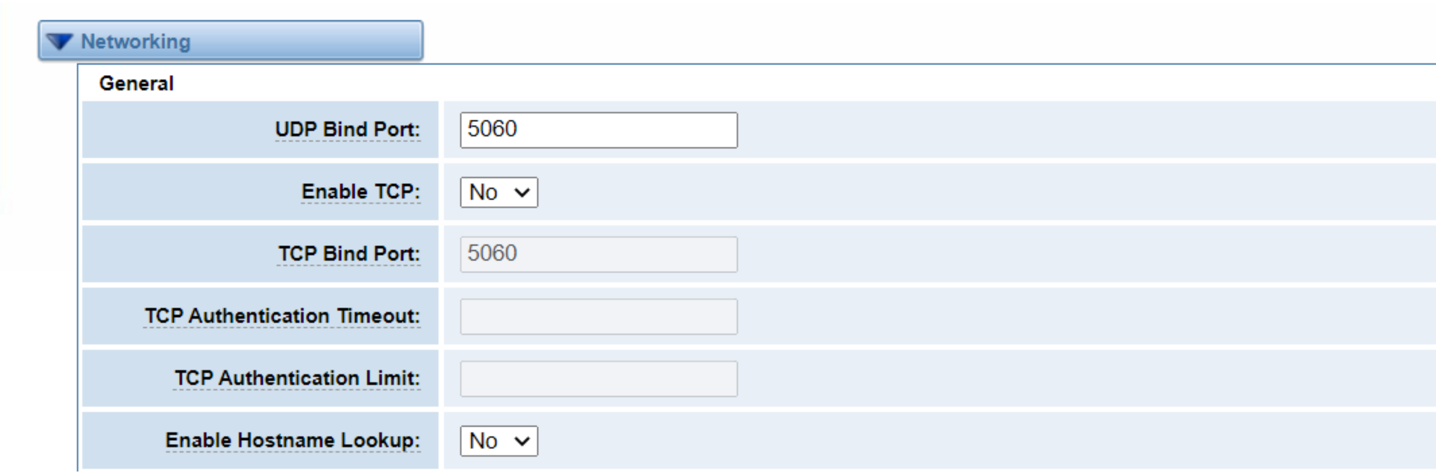


Table 4-3-1 Definition of Networking Options

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

Figure 4-3-2 NAT Settings

Table 4-3-2 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.

STUN Settings

Figure 4-3-3 STUN Settings

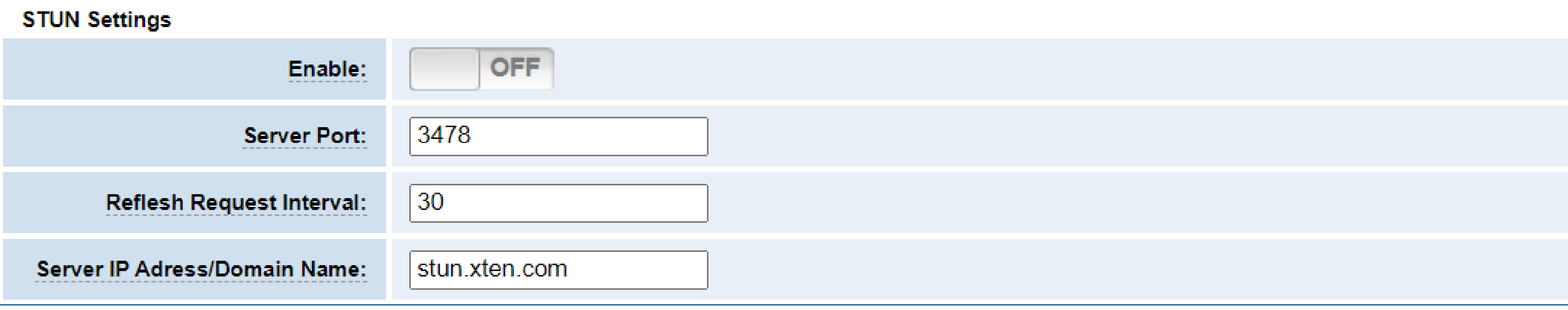


Table 4-3-3 Definition of Stun Settings Options

Options	Definition
Enable	Enable or disable STUN settings.
Server port	STUN server port.
Reflesh Request Interval	Reflesh Request Interval of the STUN server
Server IP Address/Domain Name	Address or domain of the STUN server

RTP Settings

Figure 4-3-4 RTP Settings

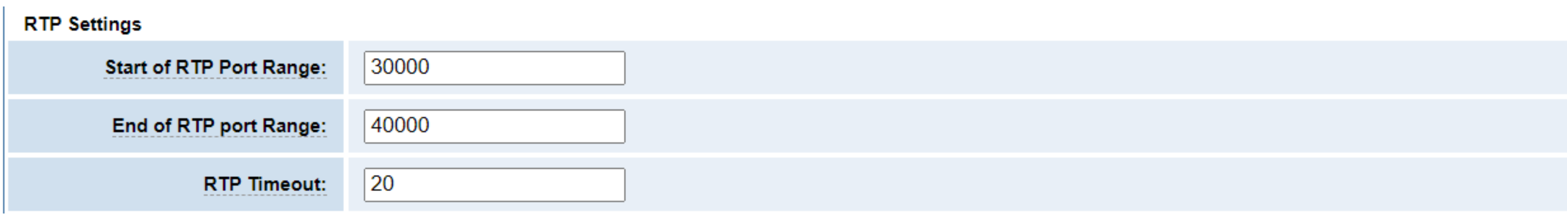


Table 4-3-4 Definition of NAT Settings Options

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

Parsing and Compatibility

Figure 4-3-5 Parsing and Compatibility Settings

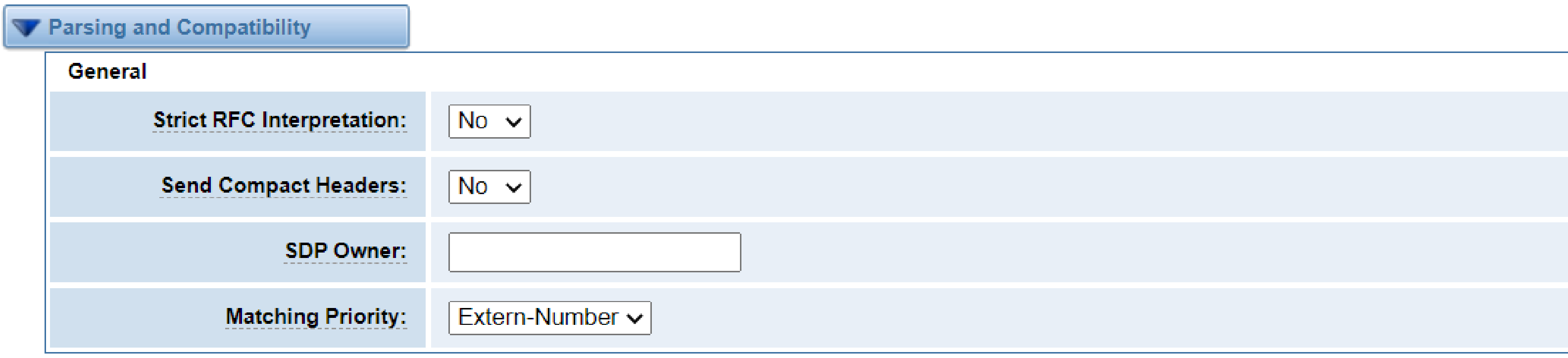


Table 4-3-5 Instruction of Parsing and Compatibility

Options	Definition
Strict RFC Interpretation	Check header tags, character conversion in URIs, and multiline headers for strict SIP compatibility.
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.
Matching Priority	Set matching priority for the gateway (From-Number / Extern-Number).
Disallowed SIP Methods	The external hostname (and optional TCP port) of the NAT.
Hangup Cause Code	Set FXO gateway hangup cause code.

Caller ID and Callee ID

Figure 4-3-6 Caller ID and Callee ID Settings

Table 4-3-6 Instruction Caller ID and Callee ID

Caller ID	
Options	**Definition**
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.
SIP From	Set SIP from type (Name or Number)
Callee ID	
Options	**Definition**
SIP To	Callee ID transfer (Tel/Tel or Tel/User).
Callee ID	Default is **EXTEN**. Eg: When selecting **SIP To**, Name is Jason and Number is 401, To mode is: “Jason”<sip:401@172.16.6.239;transport=UDP>

Timer Configuration

Figure 4-3-7 Timer configuration Settings

Table 4-3-7 Instruction of Timer configuration

Options	Definition
Maximum Registration Expiry	Maximum allowed time in seconds of incoming registrations and subscriptions.
Minimum Registration Expiry	Minimum lengeth of registration/subscriptions in seconds
Default Registration Expiry	Default length of incoming/outgoing registration in seconds.

Outbound Registrations

Figure 4-3-8 Outbound Registrations Settings

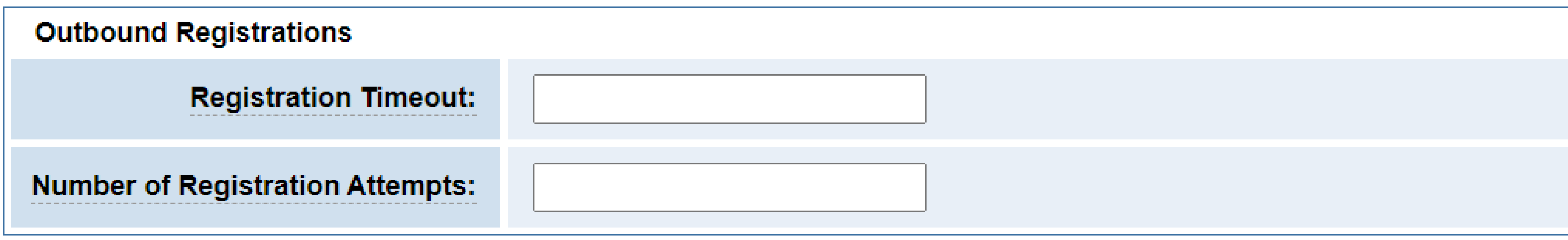


Table 4-3-8 Definition of Outbound Registrations

Options	**Definition**
Registration Timeout	How often in seconds to try registration calls.
Number of Registration Attempts	Number of regiteration attemps before giving up. 0=continue forever, hammer the other server until it accepts the registration

Security

Figure 4-3-9 Security Settings

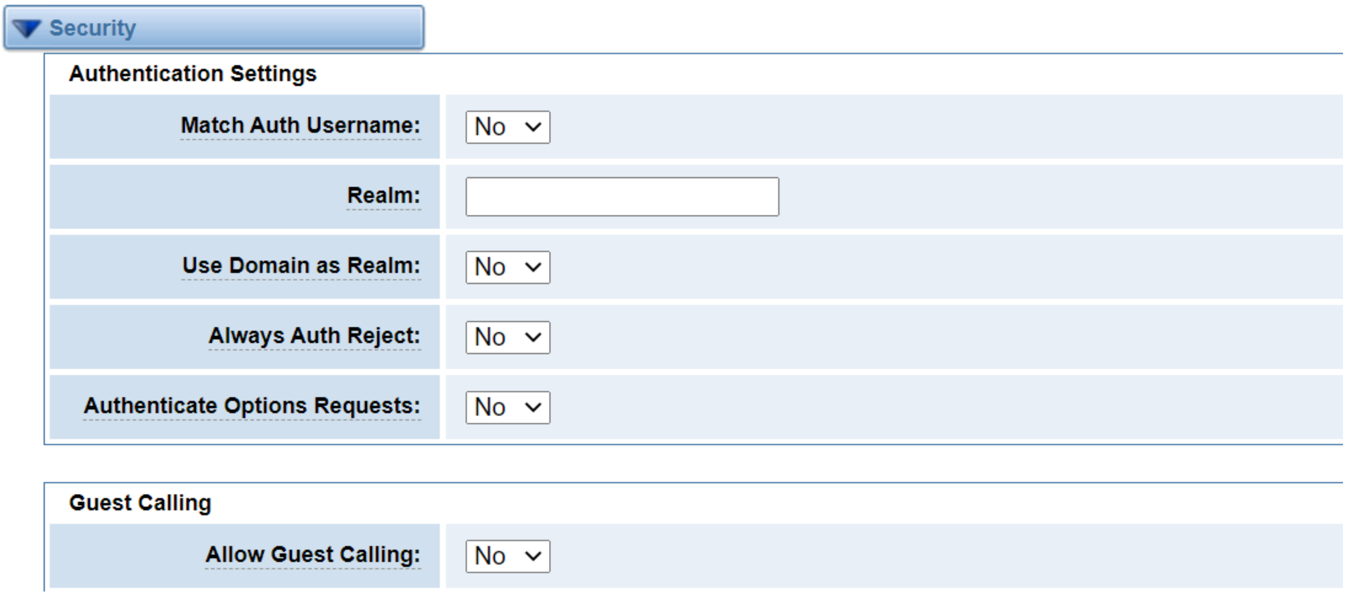


Table 4-3-9 Definition of Secutity settings

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

Figure 4-3-10 Media Settings

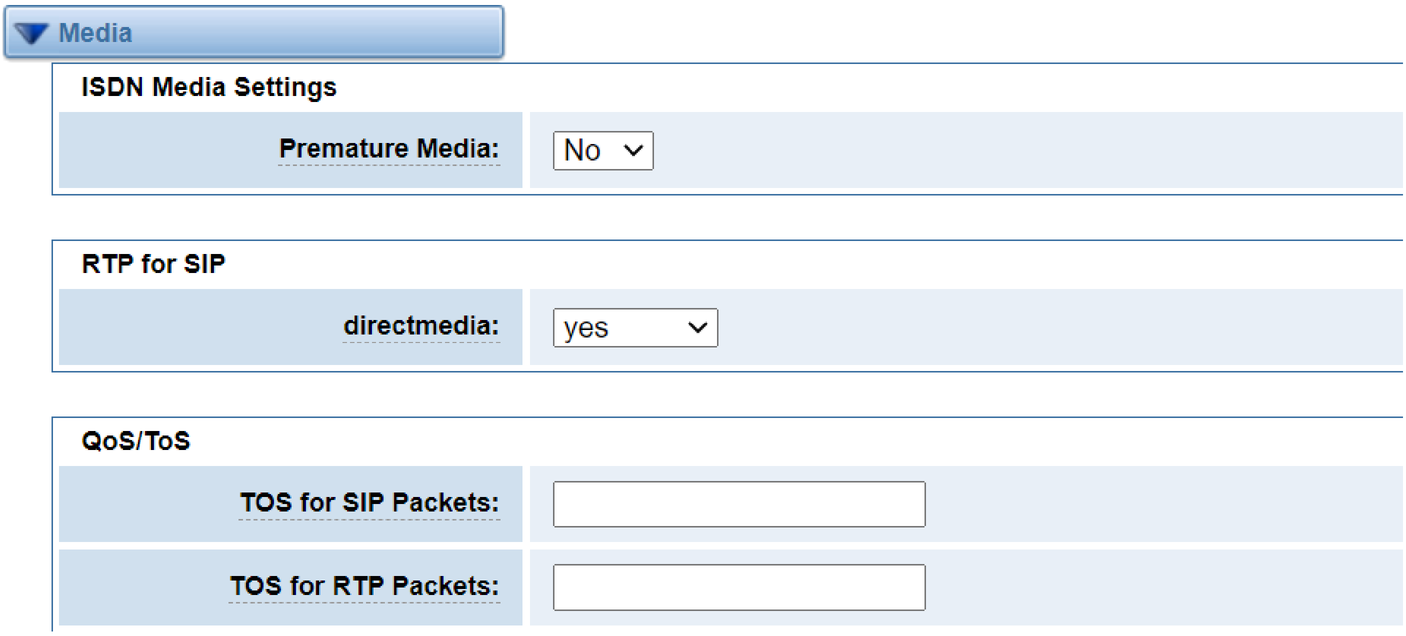


Table 4-3-10 Instruction of Media

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.
directmedia	Redirect the RTP media stream to go directly from the caller to the callee or not.
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 work 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 4-4-1 TLS settings

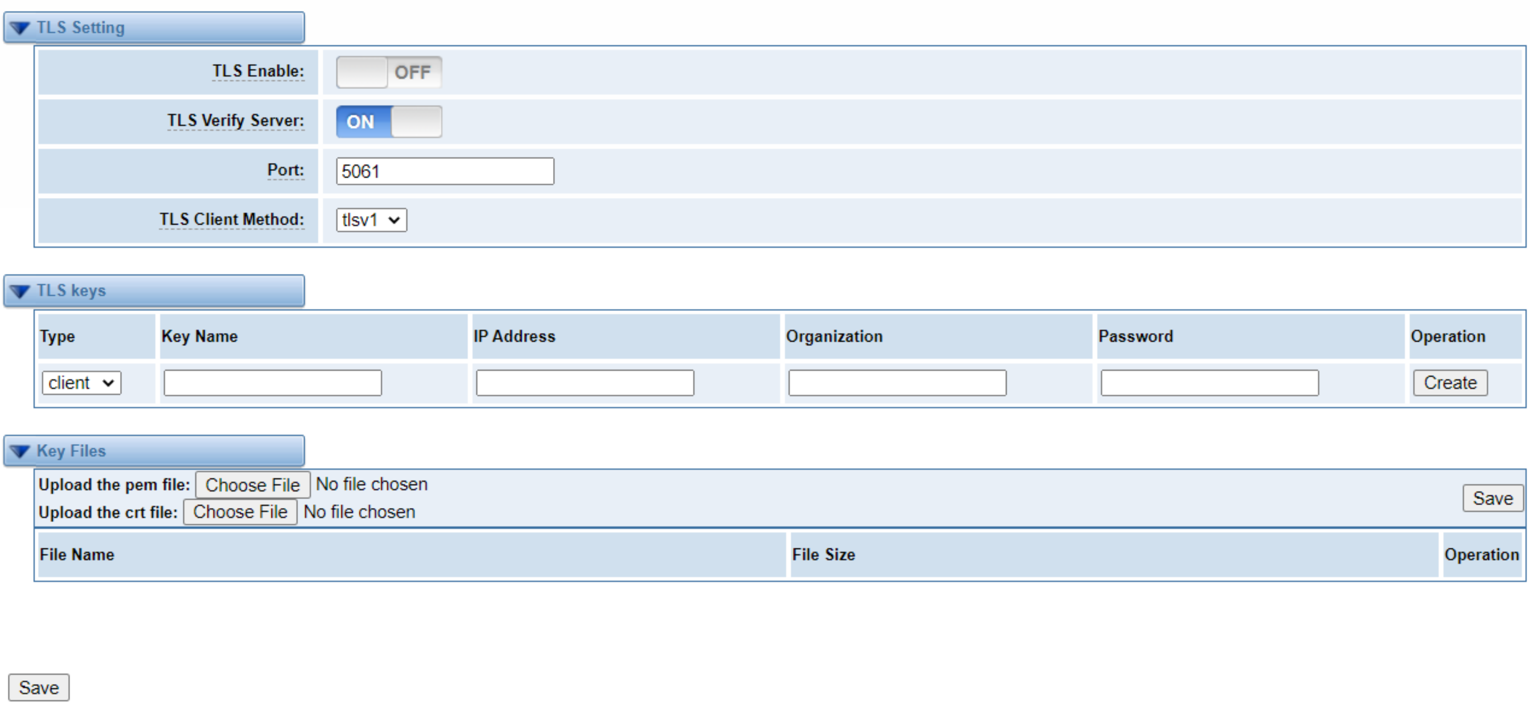


Table 4-4-1 Instruction of TLS

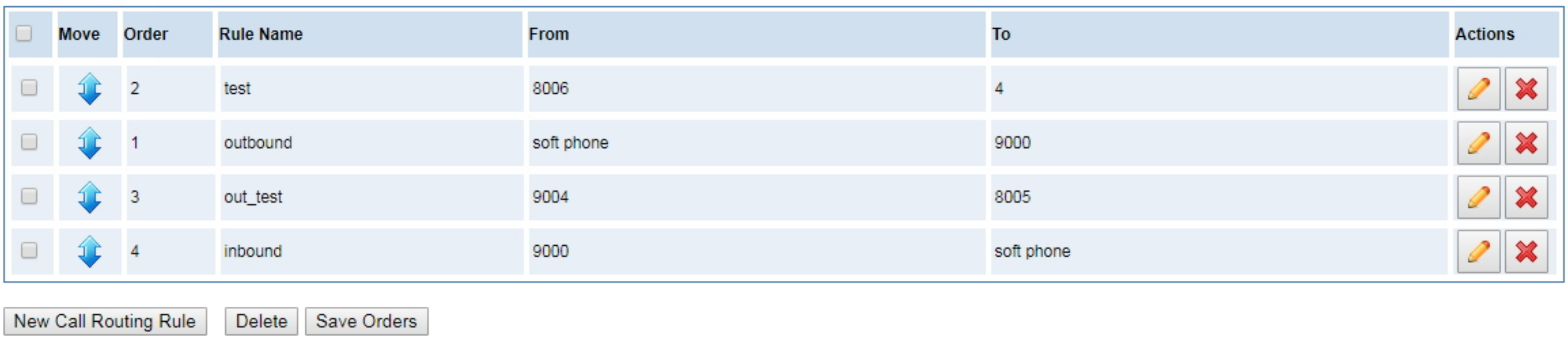
Options	Definition
TLS Enable	Enable or disable DTLS-SRTP support.
TLS Verify Server	Enable or disable tls verify server(default is no).
Port	Specify the port for remote connection.
TLS Client Method	Values include tlsv1, sslv3, sslv2, specify protocol for outbound client connections, default is sslv2.

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 supports DID function The gateway support trunk group and trunk priority management.

Call Routing Rules

Figure 5-1-1 Routing Rules



	Move	Order	Rule Name	From	To	Actions
		2	test	8006	4	
		1	outbound	soft phone	9000	
		3	out_test	9004	8005	
		4	inbound	9000	soft phone	

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.

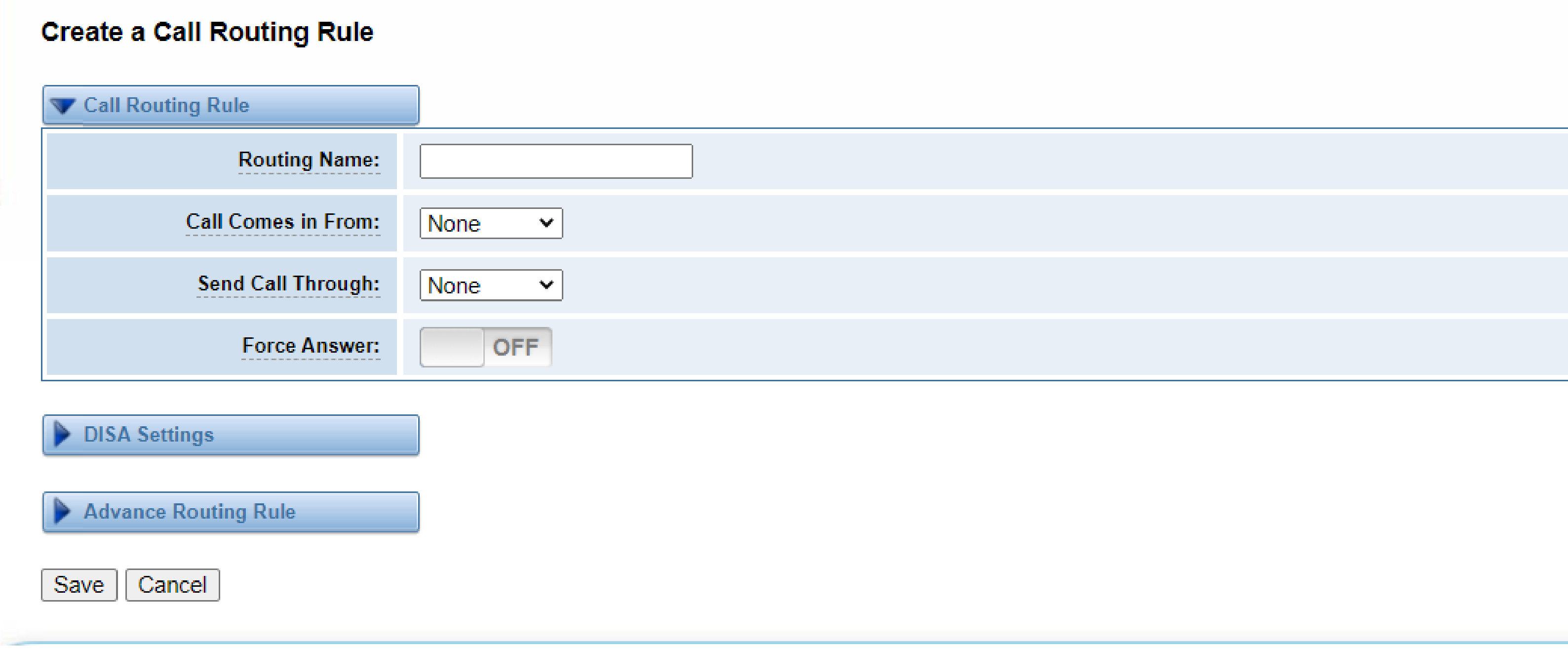
There is an example for routing rules number conversion, it transforms calling, called number at the same time. Suppose you want eleven numbers start at 159 to call the eleven numbers of start at 136. Calling transform delete the three numbers from left, then writing number 086 as prefix, delete the 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, ‘SIP2FXO’ or ‘FXO2SIP’).
Call Comes in From	The launching point of incoming calls.
Send Call Through	The destination to receive the incoming calls.
Force Answer	Enable or disable force answer option.

Figure 5-1-3 DISA Settings

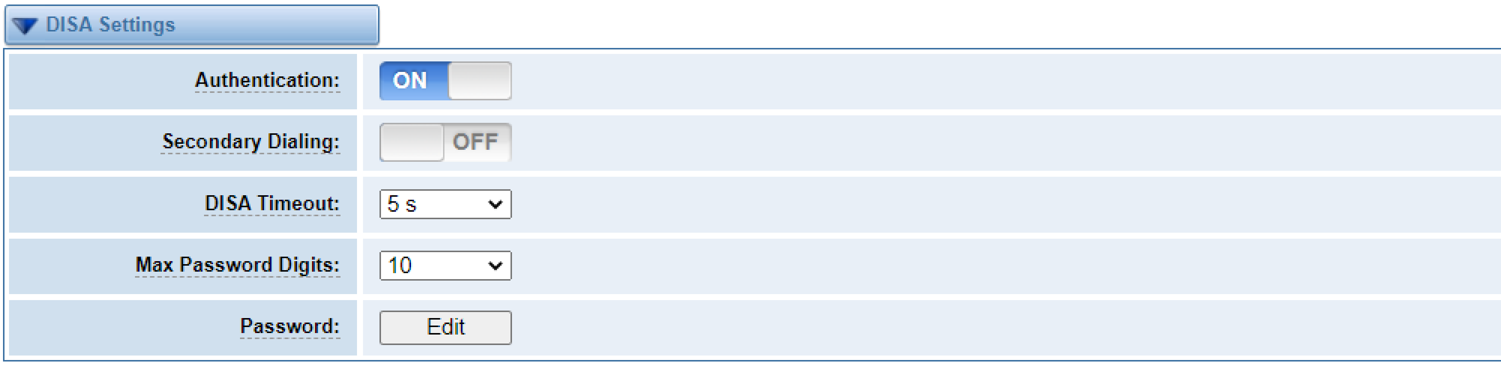


Table 5-1-3 Definition of DISA settings

Options	Definition
Authentication	Enable or disable password authentication.
Secondary Dialing	Enable or disable secondary dialing.
DISA Timeout	Select the timeout range from 1 second to 10 seconds.
Max Password Digits	Restrict the max length password dgits.
Password	Click the button “ **Edit** “ to edit DISA authentication password.

Figure 5-1-4 Advance Routing Rule

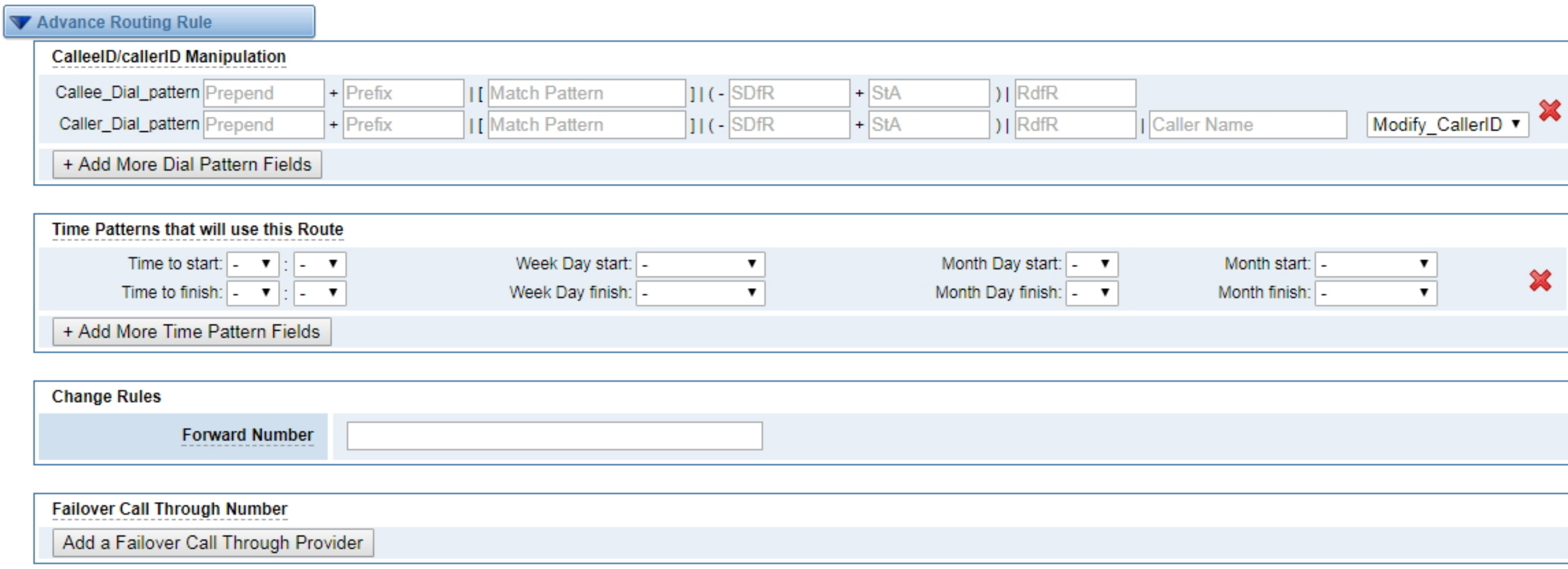


Table 5-1-4 Definition of Advance Routing Rule

Options	Definition
CalleeID/callerID Manipulation	A Dial Pattern is a unique set of digits that will select this route and send the call to the designated trunks. If a dialed pattern matches this route, no subsequent routes will be tried. If Time Groups are enabled, subsequent routes will be checked for matches outside of the designated time(s). X matches any digit from 0-9 Z matches any digit from 1-9 N matches any digit from 2-9 [1237-9] matches any digit in the brackets (example: 1,2,3,7,8,9) matches one or more 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.
Dialing Delay	The action of send callee ID will be delayed when you are creating a calling.
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

You can click 

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

Figure 5-2-2 Create a Group

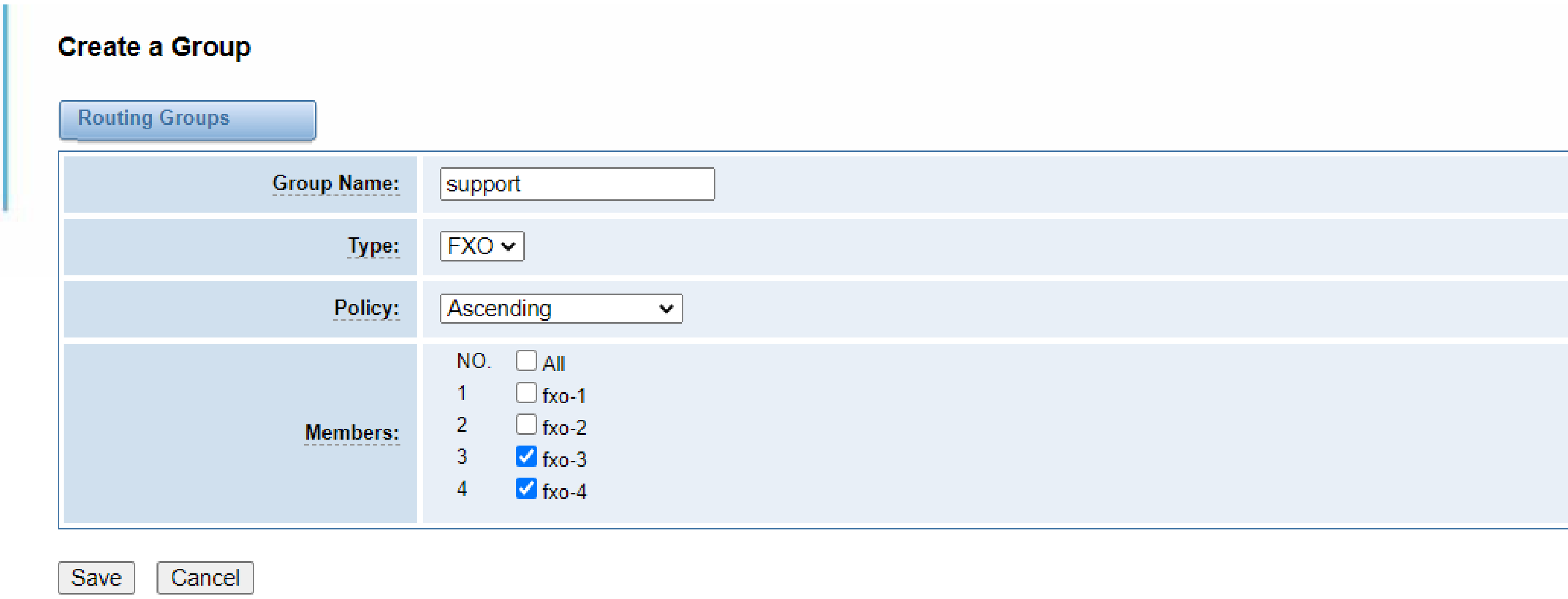


Figure 5-2-3 Modify a Group

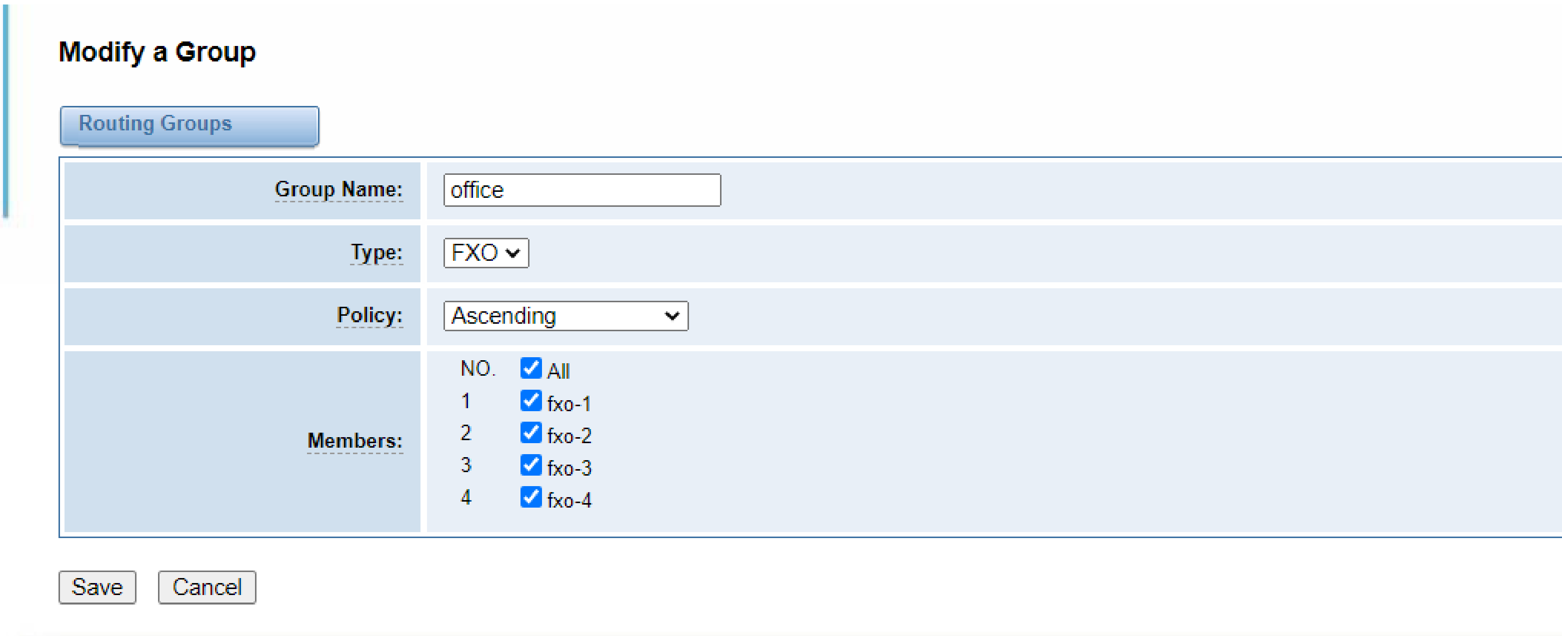


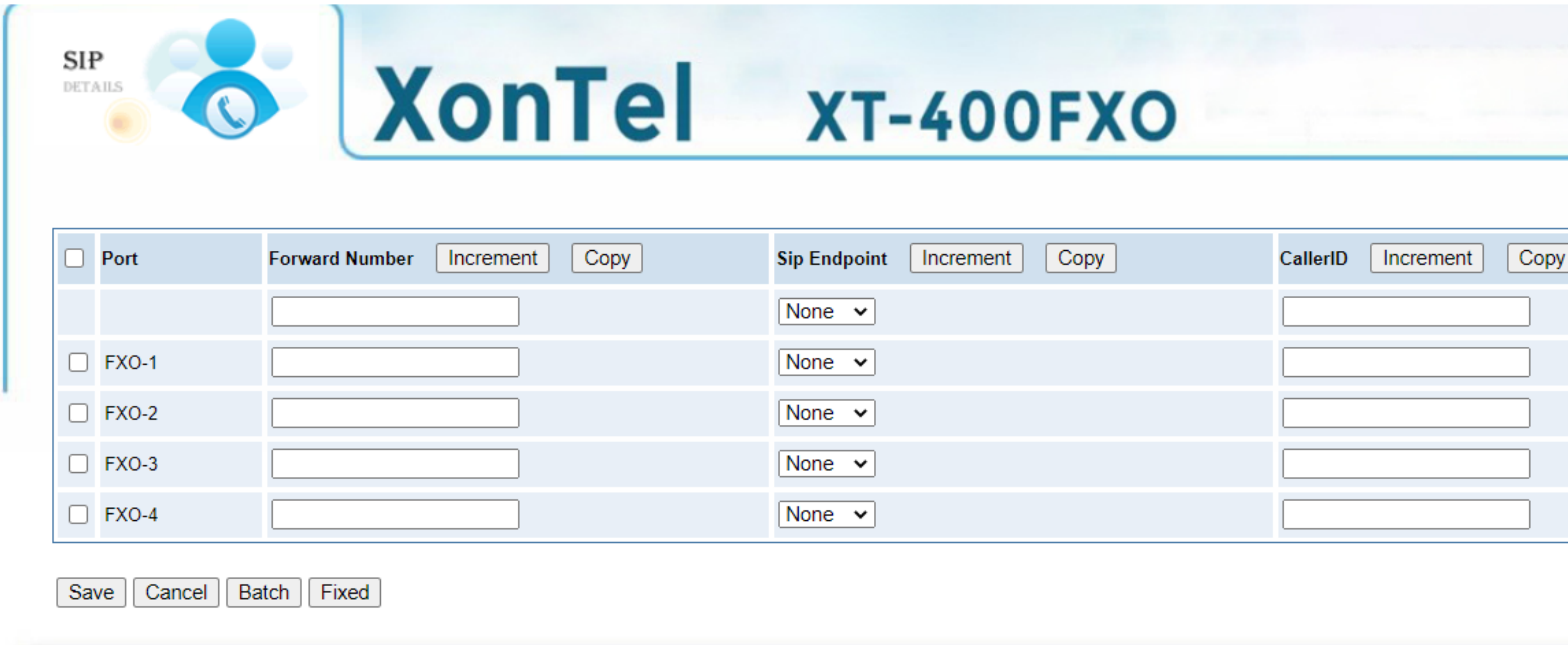
Table 5-2-1 Definition of Routing Groups

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').
Type	Group type (FXO or SIP).
Policy	Policy type (Ascending, Aescending, Roundrobin and Reverse roundrobin)
Members	Select FXO ports members for this group.

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



Advanced

Figure 5-4-1 Routing advanced settings

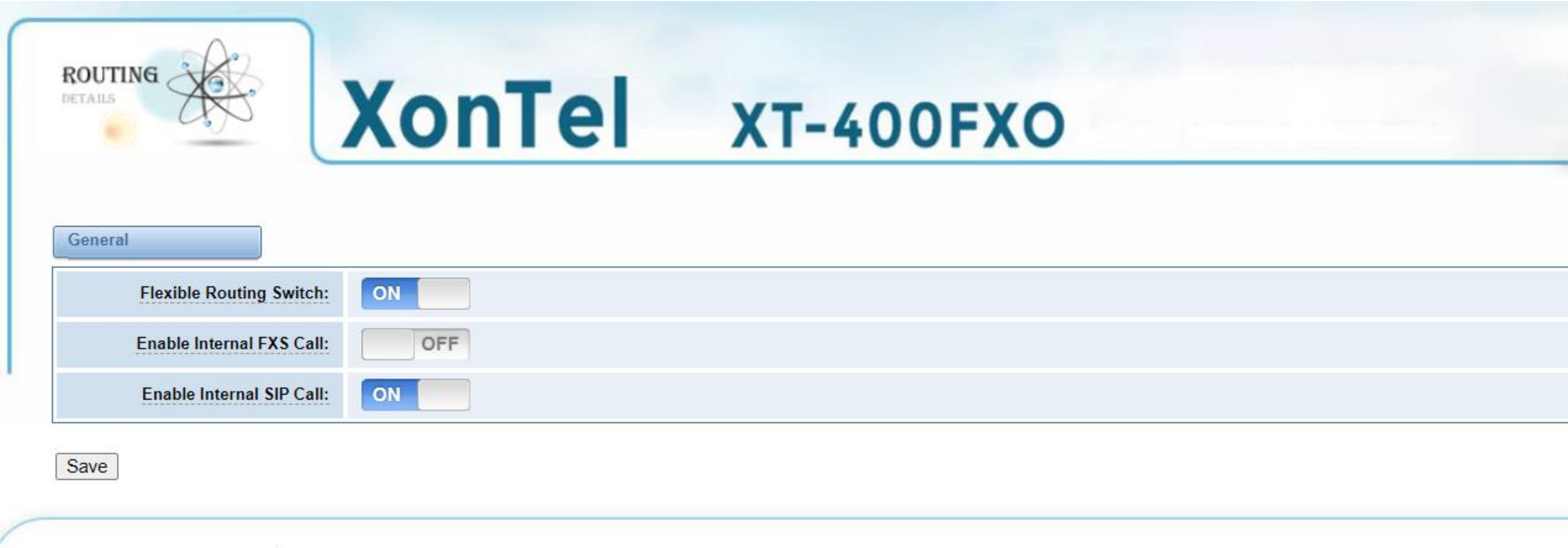


Table 5-4-1 Definition of Routing advanced settings

Options	**Definition**
Flexible Routing Switch	If you enable this option, you can enable “ **Internal FXS Call** “ option.
Enable Internal SIP Call	Enable or disable internal SIP call

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

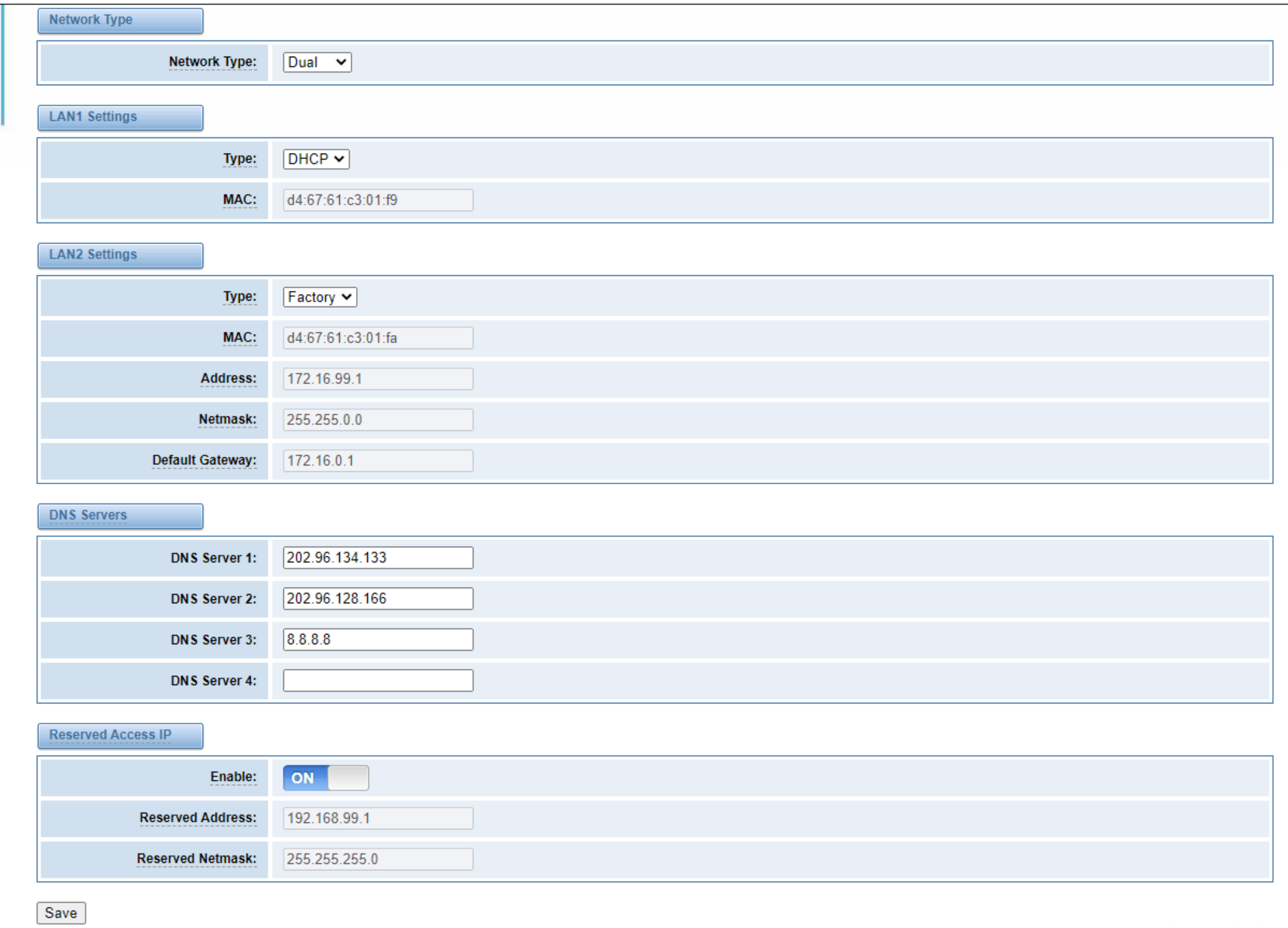


Table 6-1-1 Definition of Network Settings

Options	Definition
Network Type	Select the Ethernet mode. **Bridge**: LAN2 port interface will be used for uplink connection. LAN1 port interface will be used as bridge for PC connection. **Dual**: the two Ethernet interfaces will use different IP addresses. Assign two IP addresses in thismode.
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 FXO gateway.
Netmask	The subnet mask of your FXO gateway.
Default Gateway	Default getaway IP address.
DNS Servers	A list of DNS IP address. Basically this info is from your local network service provider.
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 FXO gatewayIP address.

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

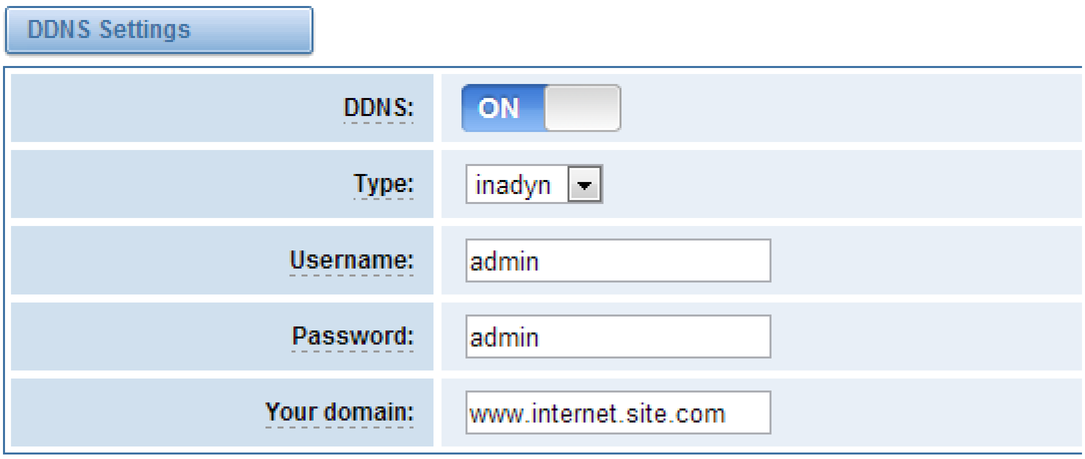


Table 6-3-1 Definition of DDNS Settings

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

Toolkit

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

Figure 6-4-1 Network Connectivity Checking

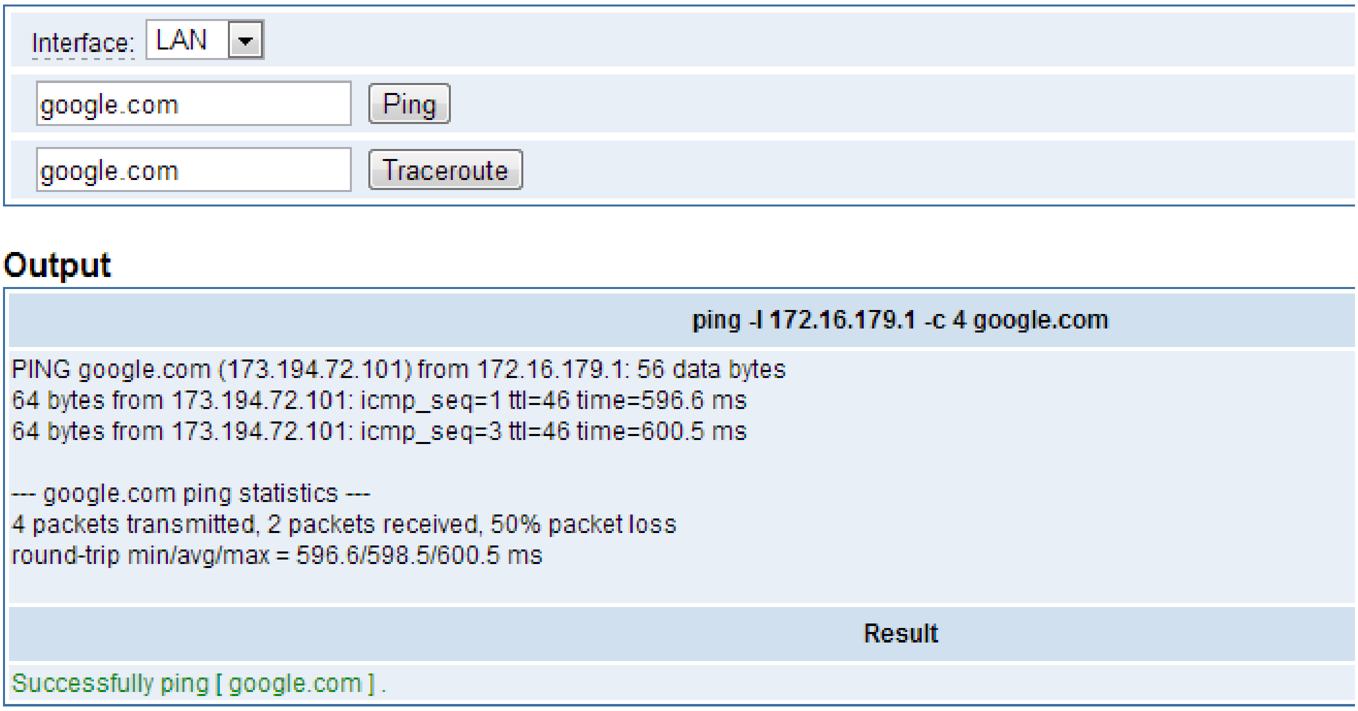


Figure 6-4-2 Channel Recording

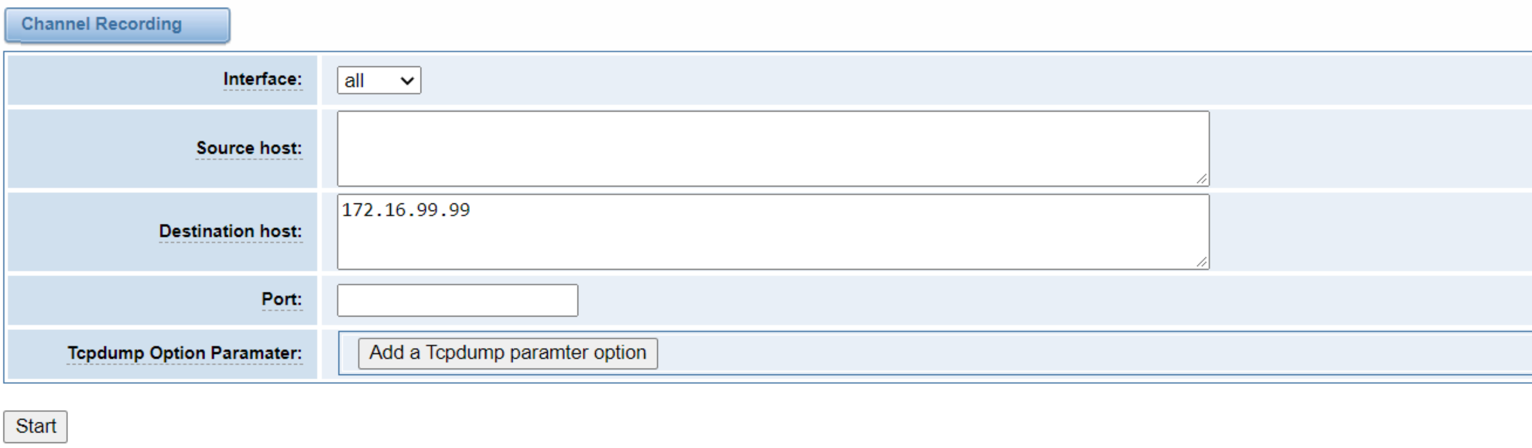


Figure 6-4-3 Capture Network Data

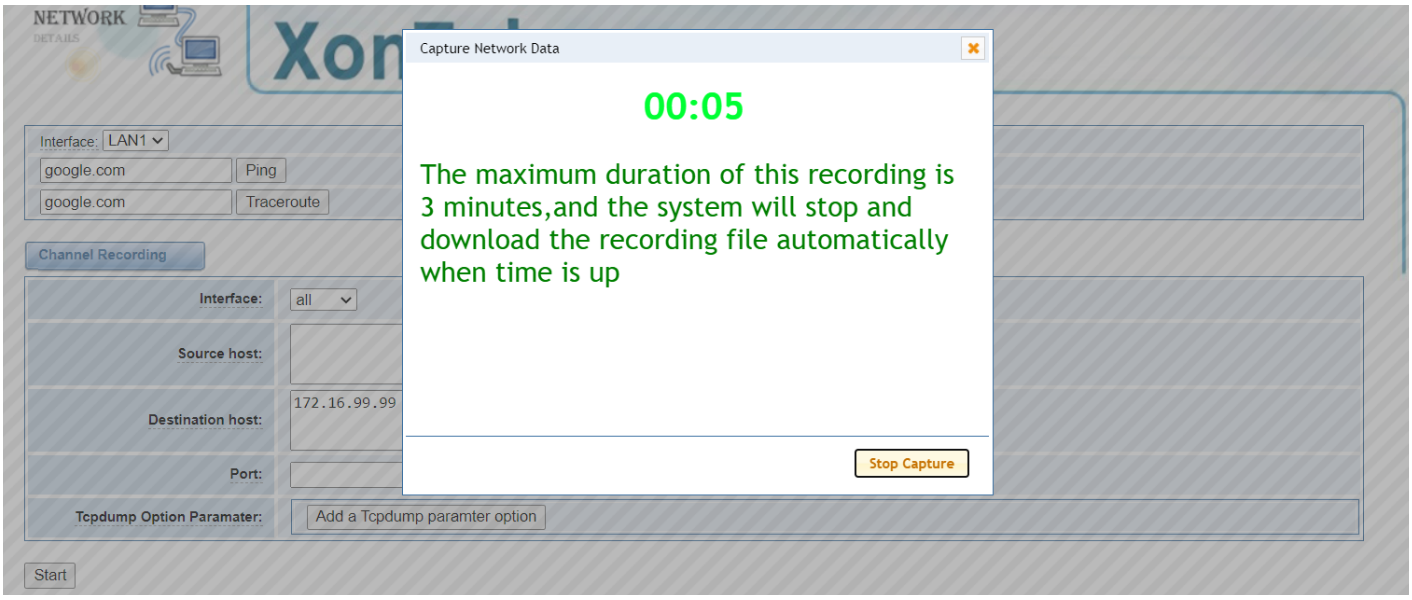


Table 6-4-1 Definition of Channel Recording

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
Tcpdump Option Parameter	The tool of tcpdump capture network data by parameter option specified.

Security Settings

Figure 6-5-1 Network security settings

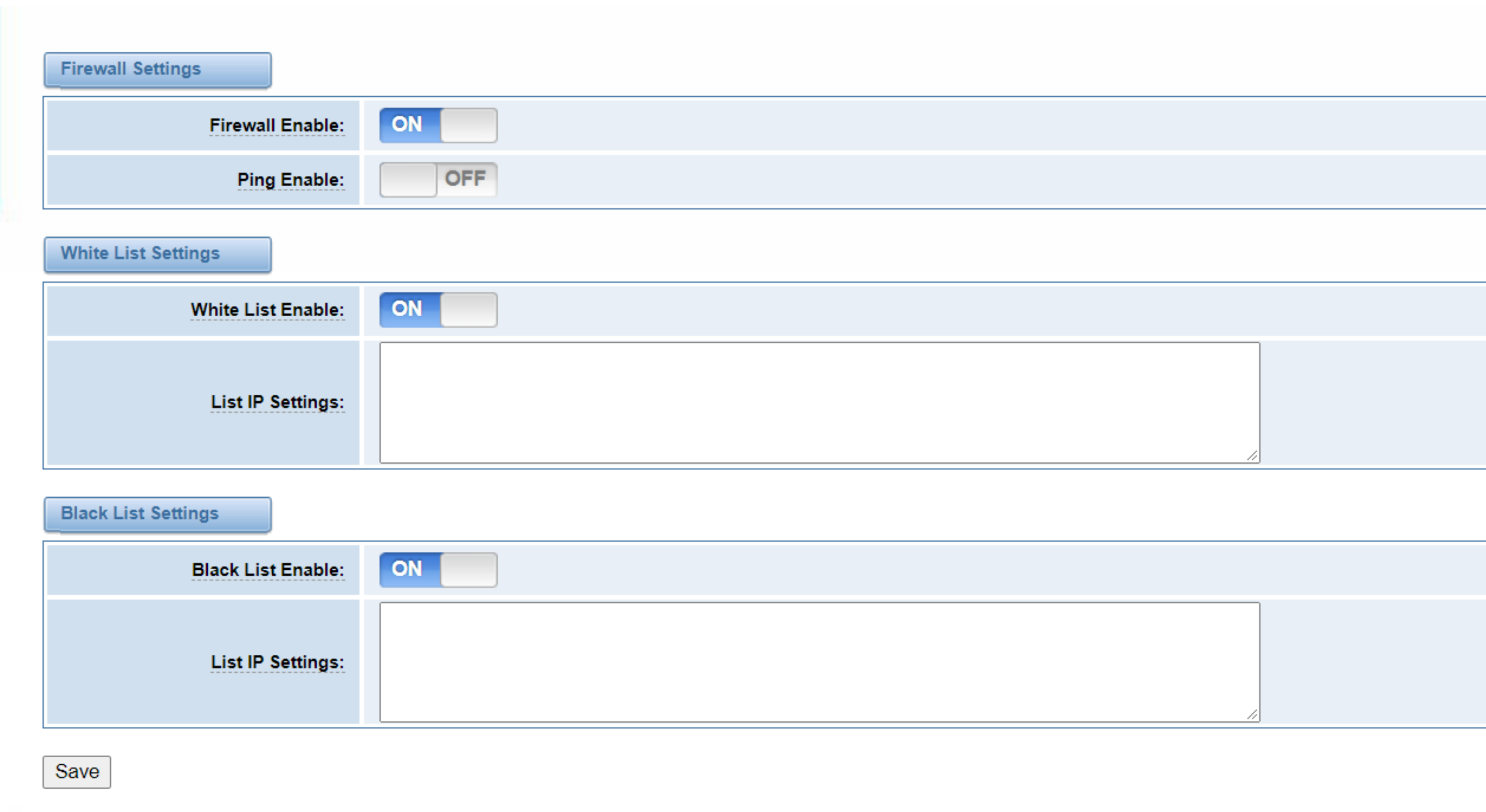


Table 6-5-1 Definition of network security settings

Options	**Definition**
Firewall Enable	Enable or disable firewall option in the FXO gateway.
Disable Ping	If you enable this option the FXO gateway will disable Ping response.
Whitelist Enable	If you enable this option, you can add approved list of IP addresses that have permission to access your FXO gateway.
Blacklist Enable	If you enable this option, you can add a list of IP addresses that will be blocked or cant access your FXO gateway.

Security Rules

From this page you can add the security rules in your FXO Gateway as shown below.

Figure 6-6-1 Security rules settings

Figure 6-6-2 Create new security rule

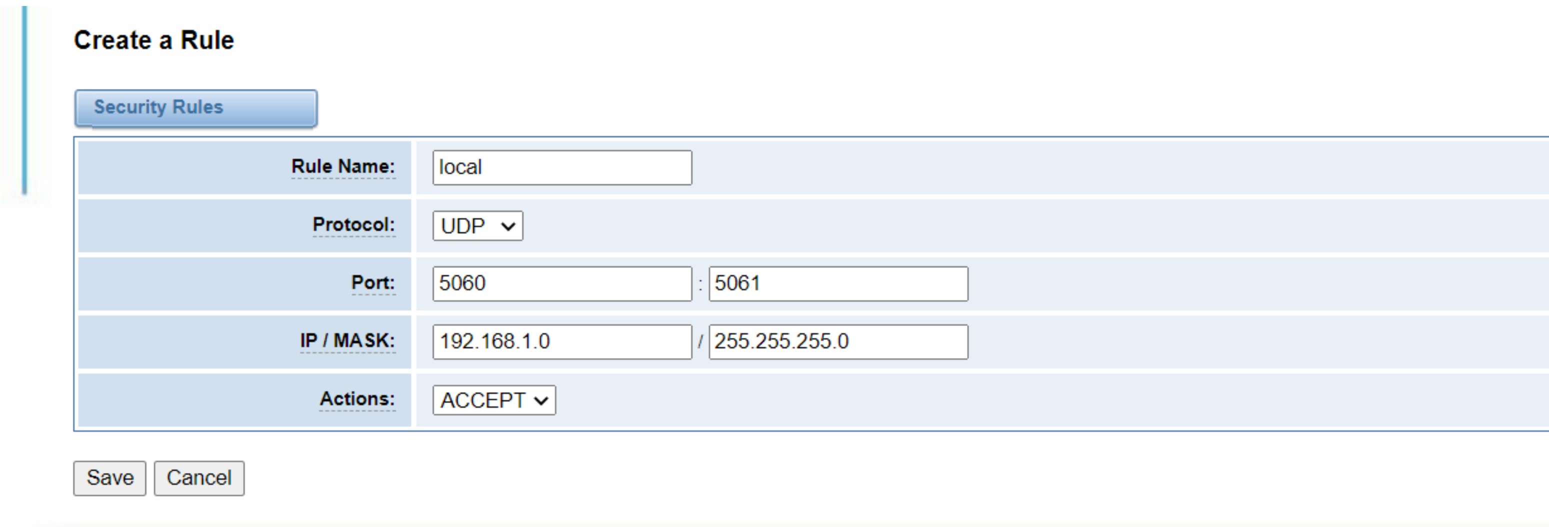


Table 6-5-1 Definition of security rules

Options	**Definition**
Rule name	Set a name for the created security rule.
Protocol	Choose the protocol (UDP, TCP, ICMP).

Port	Set the range of ports.
IP / Mask	The format for IP is IP / Mask. Confirm the range by IP and mask.
Action	Choose the action for the firewall rule (Accept, Drop).

7. Advanced

Asterisk API

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

Figure 7-1-1 API Interface

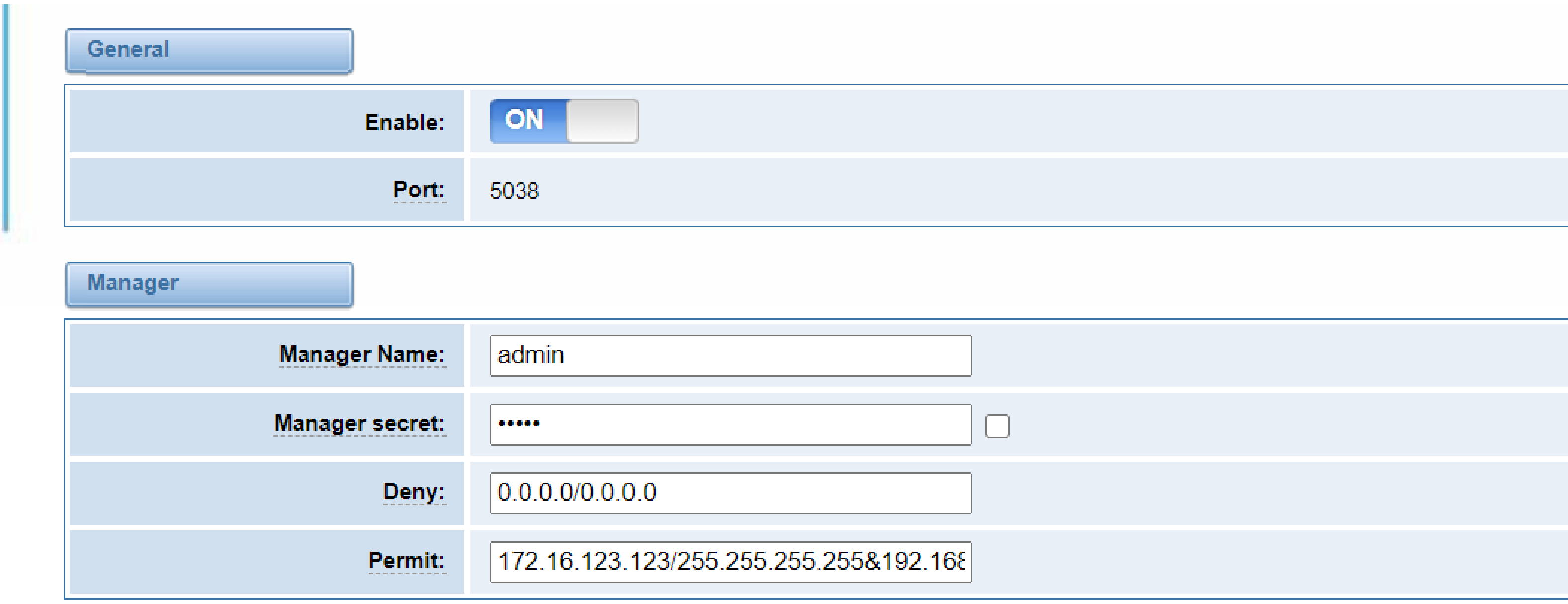


Figure 7-1-2 Permissions for API Interface

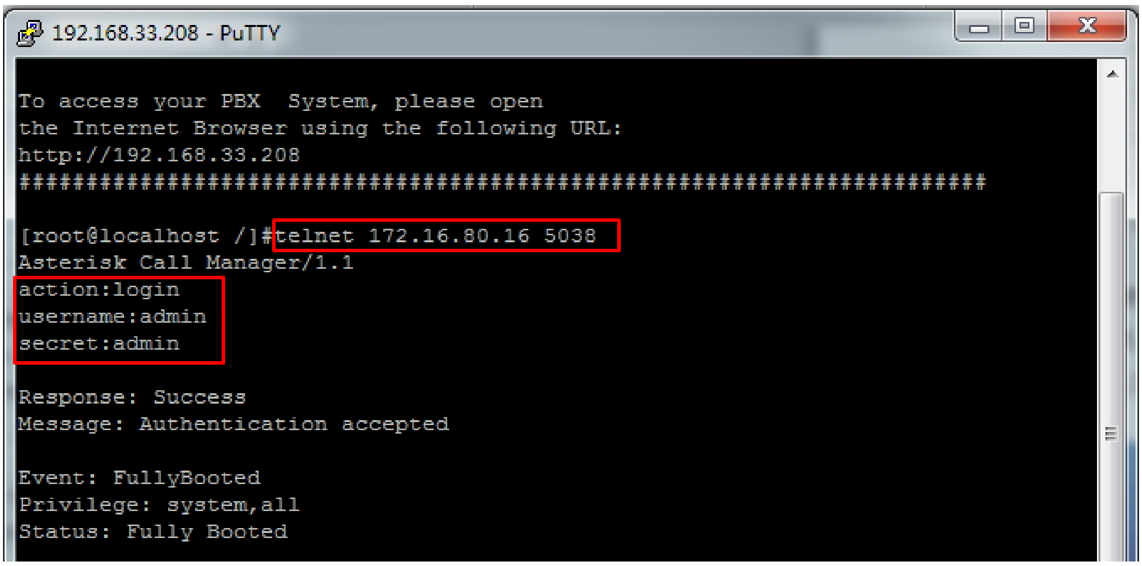
Table 7-1-1 Definition of Asterisk API

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 & 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 & 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

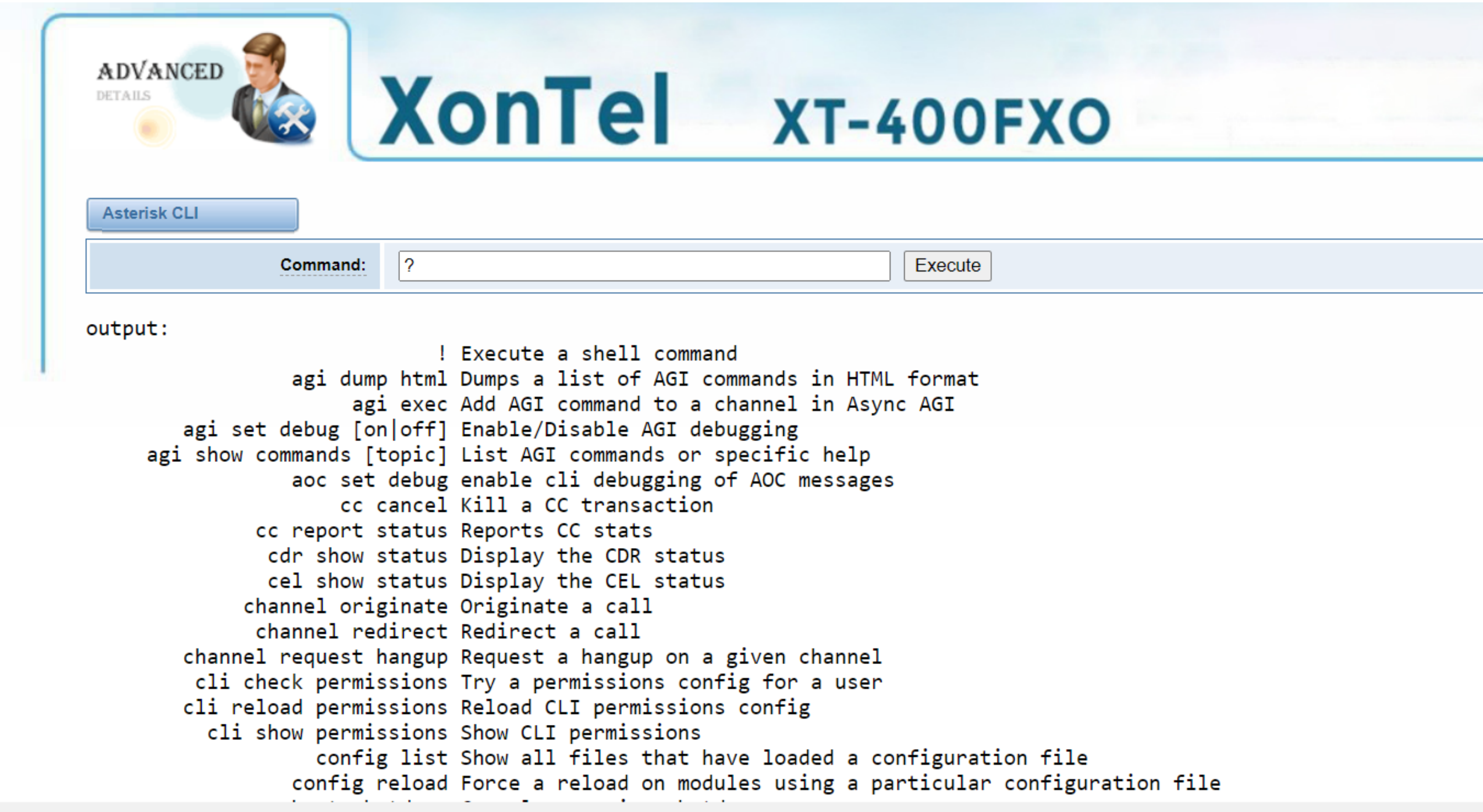


Table 7-2-1 Definition of Asterisk API

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

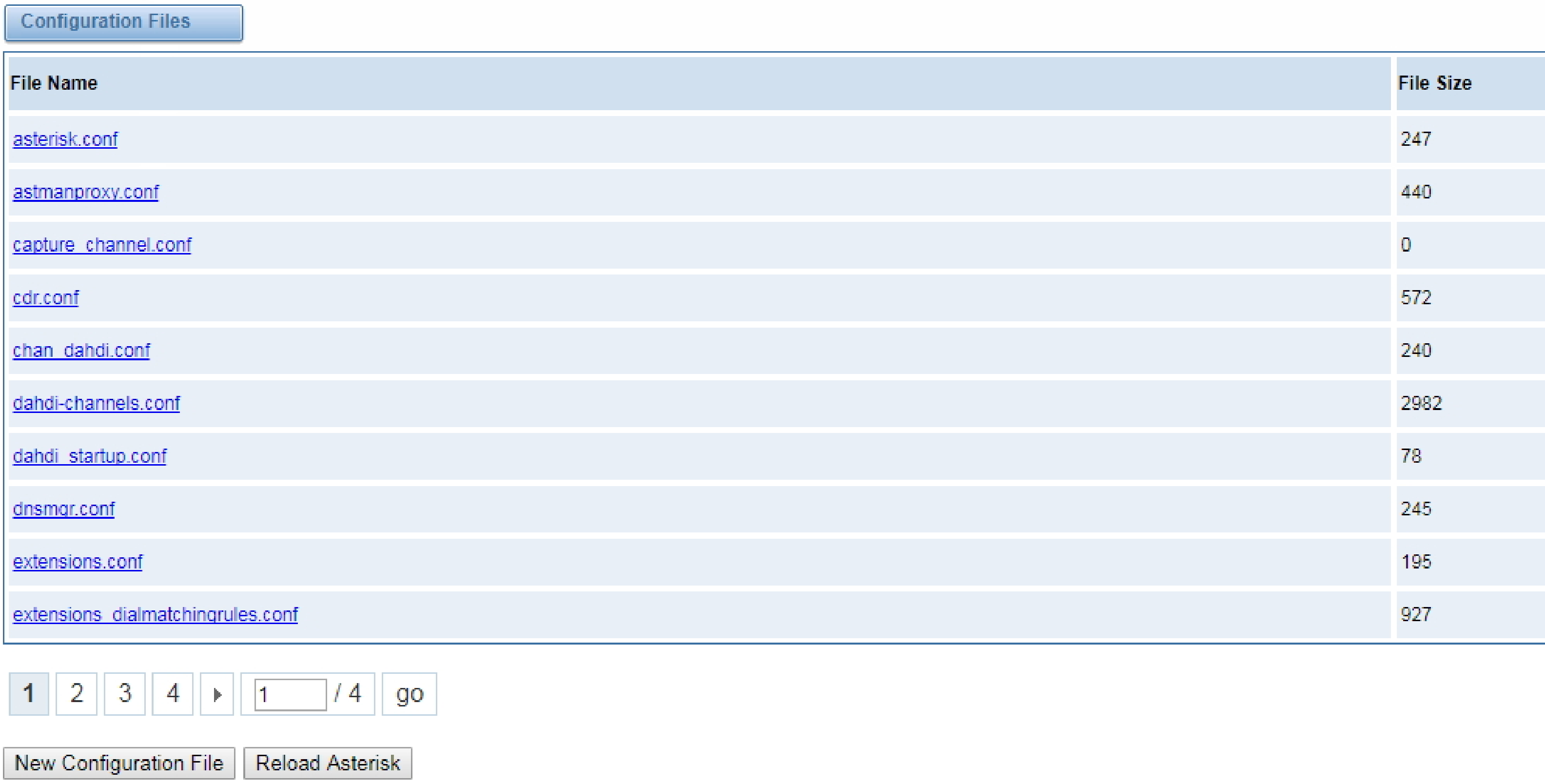
If you type “help” or “?” and execute it, the page will show you the executable commands.

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



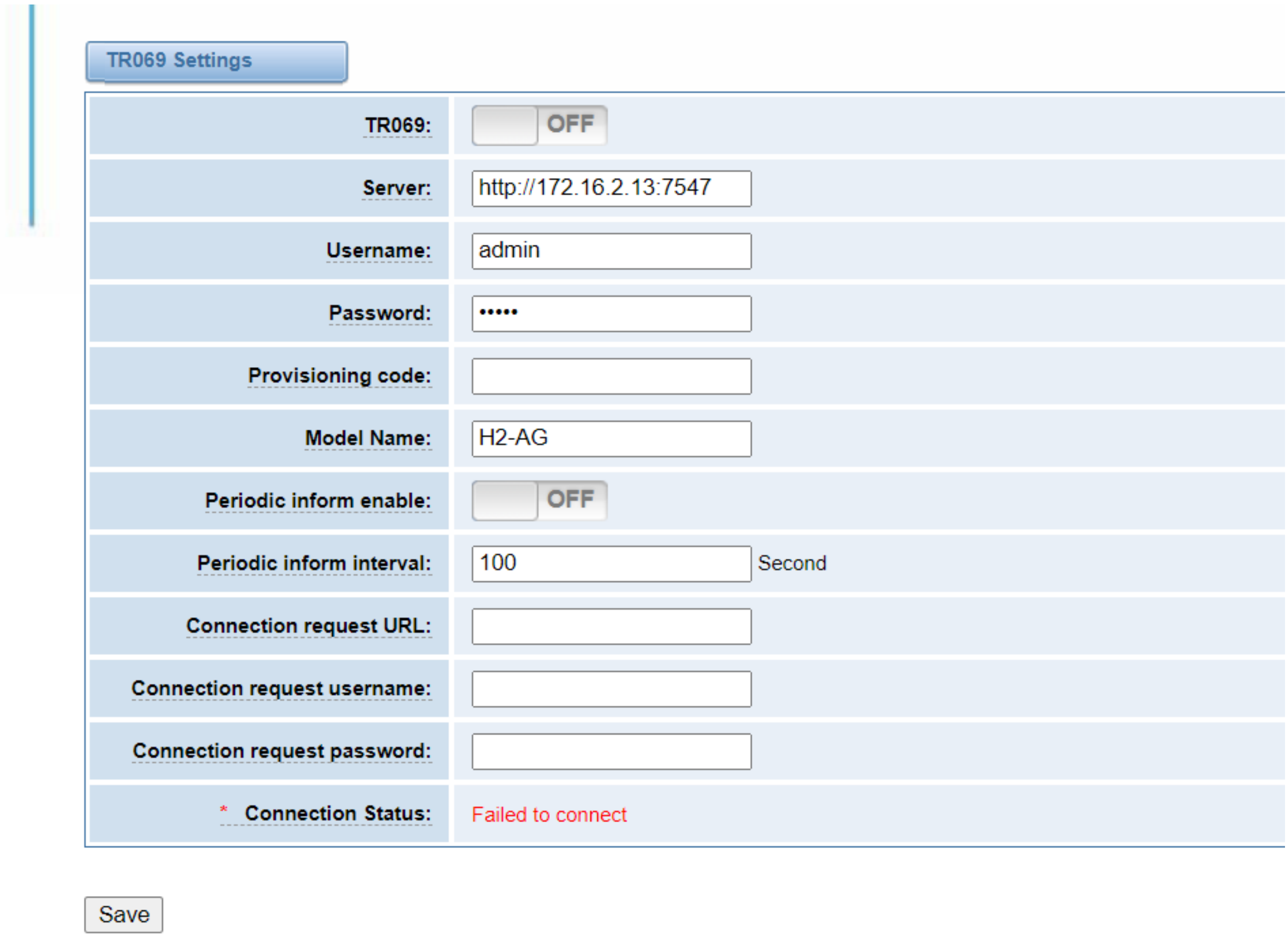
File Name	File Size
asterisk.conf	247
astmanproxy.conf	440
capture_channel.conf	0
cdr.conf	572
chan_dahdi.conf	240
dahdi-channels.conf	2982
dahdi_startup.conf	78
dnsmgr.conf	245
extensions.conf	195
extensions_dialmatchingrules.conf	927

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

TR069

XonTel XT-400FXO Gateway can be managed remotely by service provider with TR069 management protocol and is interoperable with various ACS.

Figure 7-4-1 TR069 settings



Auto Provision

XonTel XT-400FXO Gateway can be managed remotely by service provider with TR069 management protocol and is interoperable with various ACS.

Figure 7-5-1 Auto Provision settings

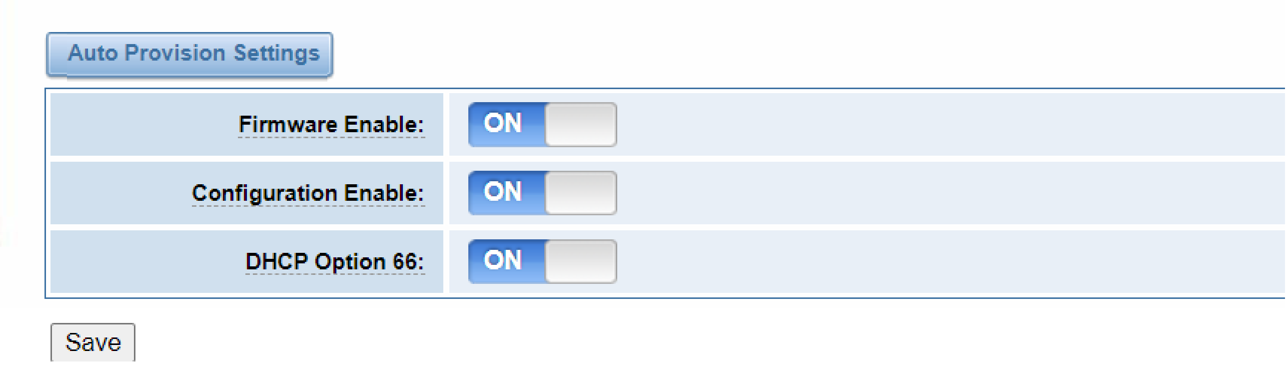


Table 7-5-1 Definition of Auto Provision settings

Options	**Definition**
Firmware Enable	Enabe or disable firmware auto provision in FXO gateway.
Configuration Enable	Enable or disable configuration auto provision in FXO gateway.
DHCP Option 66	Get asc server address from option 66 DHCP,

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 are unavailable. And the same with other log pages.

Figure 8-1-1 Logs Settings

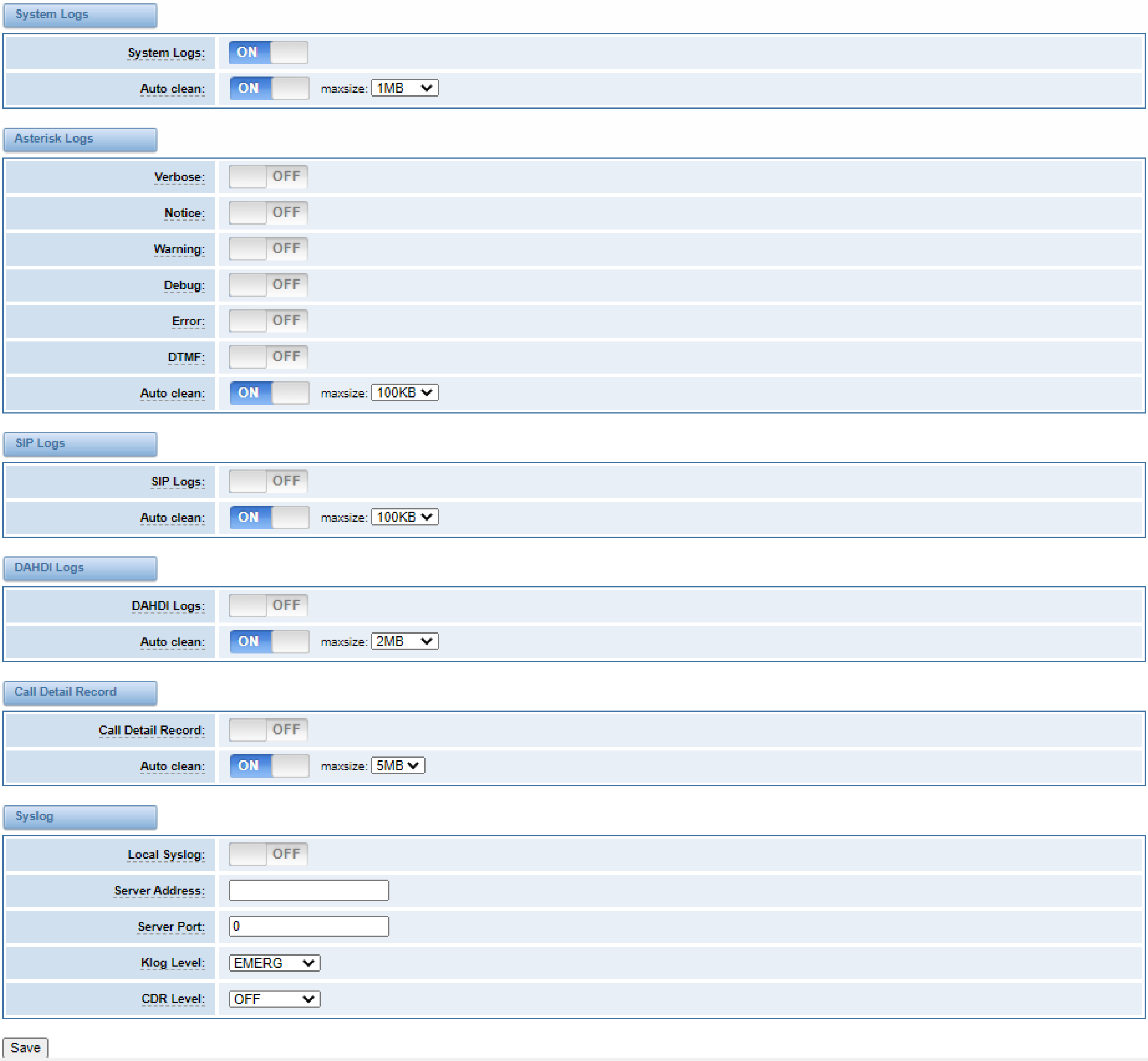


Table 8-1-1 Definition of LOG

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.
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.
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.
DAHDI Logs:	Whether enable or disable DAHDI log.
Auto clean: (DAHDI 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.
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.
Local Syslog	This action needs to set Asterisk log level in the log
Server address	Syslog server IP address, and then turn on the local syslog to take effect.
Server port	Syslog server port.
Klog level	Set the kernel log level
CDR level	Set the CDR log level.

System

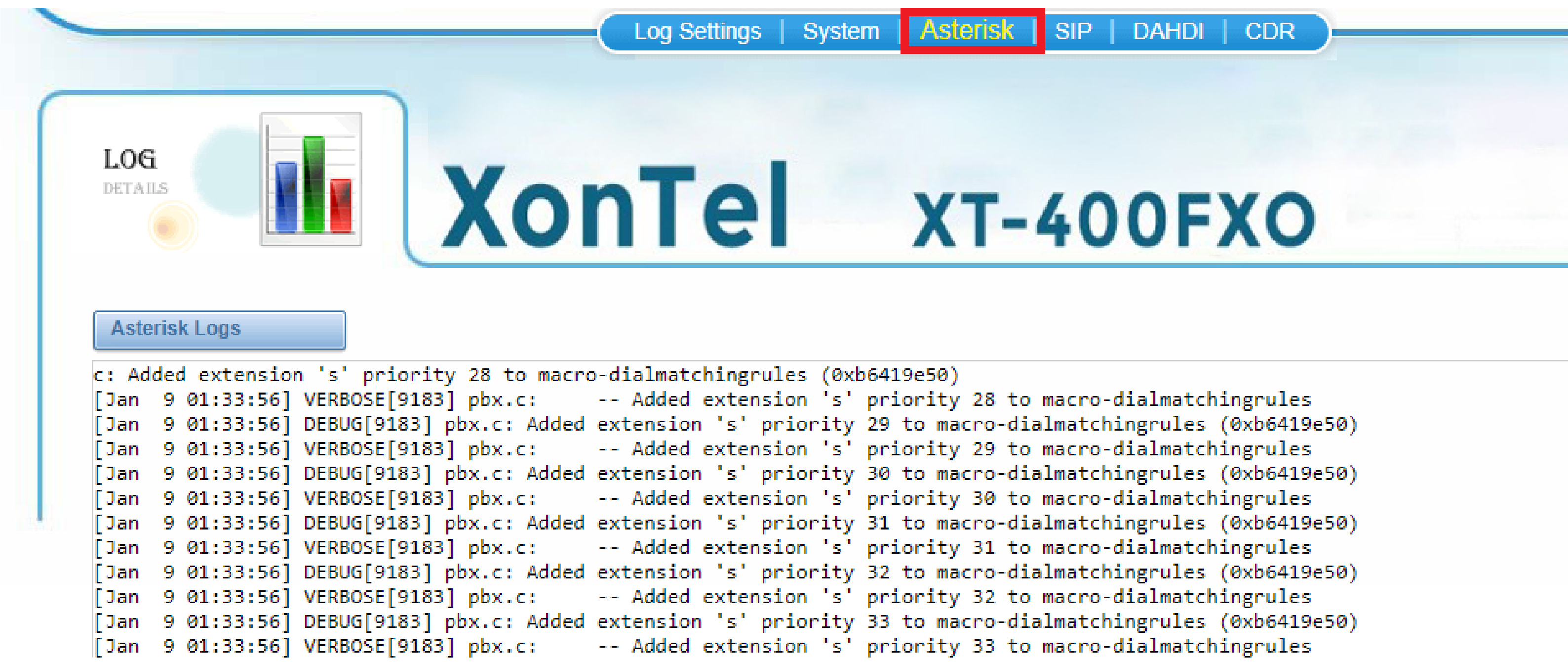
For this page you check systems logs as shown below

Figure 8-2-1 System Logs Output

Asterisk

For this page you check Asterisk logs as shown below.

Figure 8-3-1 Asterisk Logs



SIP

For this page you check SIP logs as shown below.

Figure 8-4-1 SIP Logs

DAHDI

For this page you check DAHDI logs as shown below.

Figure 8-5-1 DAHDI 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 8-6-1 Call Detail Record