



NeoGate TG Series User Manual

Version 1.2

Date: March 12th,2015

Yeastar Information Technology Co. Ltd

Table of Contents

1. Introduction	4
1.1 FEATURES	4
1.2 HARDWARE SPECIFICATION	5
2. System setup	7
2.1 SIM CARD PLACEMENT	7
2.2 ANTENNA CONNECTION	7
2.3 ETHERNET LINE CONNECTION	8
2.4 POWER SUPPLY CONNECTION	8
3 Administrator Login	8
4. Status	9
4.1 SYSTEM STATUS	10
4.1.1 <i>Trunk status</i>	10
4.1.2 <i>Network status</i>	11
4.1.3 <i>System info</i>	11
4.2 REPORTS	12
4.2.1 <i>Call logs</i>	12
4.2.2 <i>System logs</i>	12
5. System	13
5.1 NETWORK PREFERENCES	13
5.1.1 <i>LAN Settings</i>	13
5.1.2 <i>VLAN Settings</i>	14
5.1.3 <i>VPN Settings</i>	15
5.1.3 <i>DDNS Settings</i>	15
5.1.4 <i>Static Route</i>	16
5.2 SECURITY CENTER	17
5.2.1 <i>Security Center</i>	17
5.2.2 <i>Alert settings</i>	18
5.2.3 <i>Certificates</i>	21
5.2.4 <i>Firewall Rules</i>	22
5.2.5 <i>IP Blacklist</i>	23
5.3 SYSTEM PREFERENCES	24
5.3.1 <i>Password settings</i>	24
5.3.2 <i>Date and Time</i>	25
5.3.3 <i>Custom Prompts</i>	25
5.3.4 <i>Email settings</i>	26
5.3.5 <i>Firmware Update</i>	27
5.3.6 <i>Backup and Restore</i>	28
5.3.7 <i>Reset and Reboot</i>	29
6 SMS	30

6.1 SEND SMS.....	30
6.2 SMS CONTACTS.....	30
6.3 OUTBOX	31
6.4 INBOX.....	31
6.5 USSD	32
6.6 API SETTINGS	32
7 Gateway	34
7.1 MOBILE LIST	34
7.1.1 <i>Mobile List</i>	34
7.1.2 <i>Module Group</i>	37
7.1.3 <i>Call Waiting</i>	38
7.1.4 <i>Follow me</i>	39
7.2 VoIP SETTINGS	40
7.2.1 <i>VoIP trunk</i>	40
7.2.2 <i>Trunk Group</i>	46
7.2.3 <i>SIP Settings</i>	46
7.2.4 <i>IAX Settings</i>	52
7.2.5 <i>General Preferences</i>	52
7.3 ROUTES SETTINGS	53
7.3.1 <i>Mobile to IP</i>	53
7.3.2 <i>IP to Mobile</i>	56
7.3.3 <i>Blacklist</i>	58
7.3.4 <i>Callback Settings</i>	58
8 Applications.....	61

1. Introduction

NeoGate TG Gateway for Maximum Efficiency & Cost Savings

NeoGate is a device for connecting Mobile Network to VoIP Network directly, which can support two-way communication: Mobile to VoIP or VoIP to Mobile. It is the best solution ever to connect IP-based telephone systems, soft switches, and IP-PBXs to Mobile network.



NeoGate TG Gateway supports GSM, UMTS and CDMA network (TG1600 does not support UMTS now).




1.1 Features

• SIP proxy Registrar for IP phones included
• Incoming call routing
• Outgoing call routing
• SMS sending and receiving (WEB interface)
• USSD API
• Call Back
• LCR (Least Cost Routing)
• Top voice quality (EFR super sound)
• Simple Web based configuration
• Easy to integrate
• Easy to install

For more information, please click:
<http://www.yeastar.com/Products/Products.asp>

1.2 Hardware Specification

Model	Channels	Appearance
NeoGate TG100	1	 <p>The NeoGate TG100 is a compact, black, rectangular wireless router. It features a single antenna on the right side. The front panel includes a power jack, a LAN port, and a reset button. The brand name 'NeoGate' is printed on the top surface.</p>
NeoGate TG200	2	 <p>The NeoGate TG200 is a larger, black, rectangular wireless router. It features a single antenna on the right side. The front panel includes a power jack, a power button, a reset button, a LAN port, and two LAN ports labeled 1 and 2. The brand name 'NEOGATE TG200' is printed on the front.</p>

<p>NeoGate TG400</p>	<p>4</p>	 <p>The image shows the NeoGate TG400 device, a black rectangular unit with a single antenna on top. The front panel features the NeoGate logo, a power button, a reset button, a power LED, a run LED, an Ethernet port, and two RJ45 ports labeled 1 and 2, each with a green status LED.</p>
<p>NeoGate TG800</p>	<p>8</p>	 <p>The image shows the NeoGate TG800 device, a black rectangular unit with two antennas on top. The front panel features the NeoGate logo, a power button, a reset button, a power LED, a run LED, two Ethernet ports, and four RJ45 ports labeled 1 through 4, each with a green status LED.</p>
<p>NeoGate TG1600</p>	<p>16</p>	 <p>The image shows the NeoGate TG1600 device, a black rectangular unit with 16 RJ45 ports on the front panel, numbered 1 through 16. Each port has a yellow LED indicator. The front panel also includes a power button, a reset button, a power LED, and a run LED.</p>

2. System Setup

2.1 SIM Card Placement

Insert the SIM card on the front panel directly before powering on NeoGate. To remove this card, press the button on the left side, the card will pop directly. If you are using NeoGate TG100, you should open the box before installing SIM card on the board directly.

Notes:

1. The SIM card should be mini-SIM (2FF).
2. Please cut off the power before installing SIM card. You can also log in Web interface to power this module off separately.

2.2 Antenna Connection

NeoGate is equipped with antenna connector for all the GSM/UTMTS/CDMA modules. The external antenna should be installed vertically always on a site with a good wireless signal.

2.3 Ethernet Line Connection

NeoGate provides two 10/100M Ethernet ports with RJ45 interface and LED indicator. Plug Ethernet line into NeoGate's Ethernet port, and then connect the other end of the Ethernet line with a hub, switch, router, LAN or WAN. Once connected, check the status of the LED indicator. A yellow LED indicates the port is in 100M mode, if it's dark, the speed is 10M. Green LED indicates the port is properly connected, if it's flickering, it means data transmission.

2.4 Power Supply Connection

NeoGate utilizes the high-performance switch power, which supplies enough voltage and electrical energy required by NeoGate system.

AC Input: 100~240V

DC Output: 12V, 1A

Please follow the steps below to connect the NeoGate unit to a power outlet:

1. Connect the small end of the power cable to the power input port on the NeoGate back panel, and plug the other end of the cable into a 100VAC power outlet.
2. Check the Power LED on the front panel. A solid green LED indicates that power is being supplied correctly.

3 Administrator Login

Open your Web browser and input the IP address of the NeoGate server. If this is the first time you configure NeoGate, please use the default settings below:

IP Address: <http://192.168.5.150>

Username: **admin**

Password: **password**

In this example, the IP address is 192.168.2.135, the model is TG800.

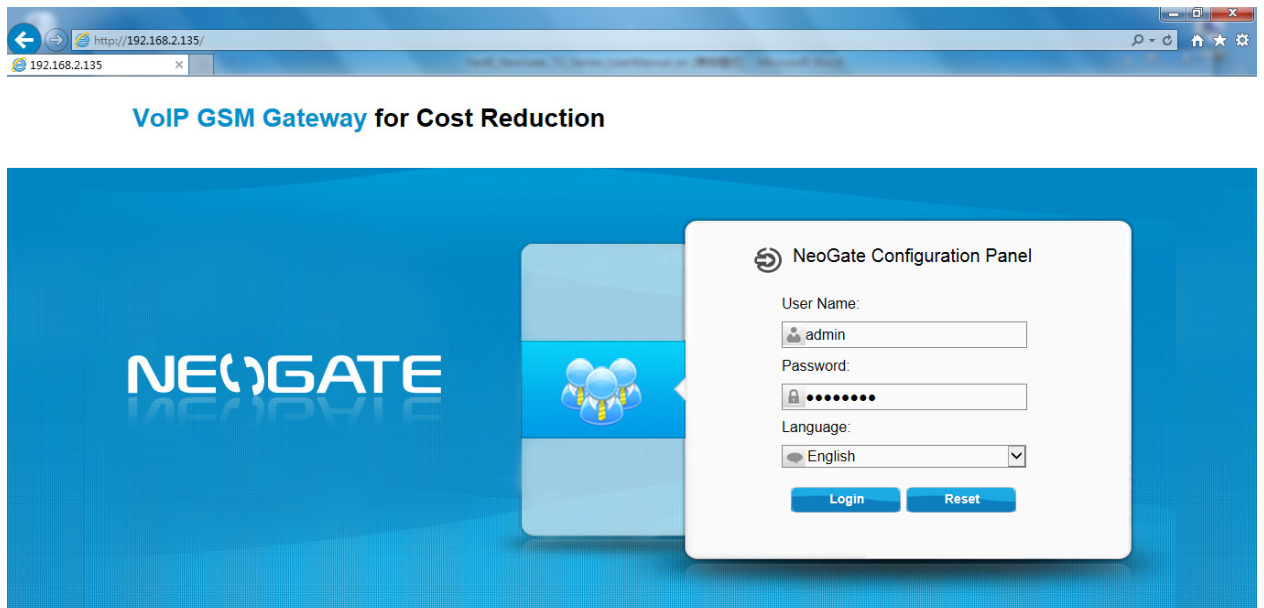


Figure 3-1


Click Login to get the welcome page.



Figure 3-2

4. Status



Click  to check the status of NeoGate TG, including the system status and the detailed reports.

4.1 System Status

In this page, we can check the status of the system, including trunk status, network status and system information.

4.1.1 Trunk status

Port	Trunk Name	Status	Signal	Carrier	Available Duration
1	GSM1	Idle	📶	CHINA MOBILE	Unlimited
2	GSM2	Busy	📶	CHINA MOBILE	Unlimited
3	GSM3	Busy	📶	CHINA MOBILE	Unlimited
4	GSM4	Idle	📶	CHINA MOBILE	Unlimited
5	GSM5	Idle	📶	CHINA MOBILE	Unlimited
6	GSM6	Failed	Please Insert SIM Card	--	Unlimited
7	GSM7	Failed	Please Insert SIM Card	--	Unlimited
8	GSM8	Idle	📶	CHINA MOBILE	Unlimited

Status	Trunk Name	Type	User Name	Hostname/IP	Reachability
OK (1 ms)	162sps	SP-SIP		192.168.5.162	OK (1 ms)

Status	Account	Type
Registered	20001	SIP
Registered	20002	SIP
Registered	20000	IAX

Figure 4-1

NeoGate Status Description:

GSM/UTMTS/CDMA Tunk:

Status	Description
Idle	The port is idle
Busy	The port is in use
Failed	The port has not inserted the SIM Card

Signal	Description
📶	No signal
📶	Poor
📶	Average
📶	Good
📶	Excellent

VoIP Trunk:

Status	Description
Unregistered	Trunk registration failed
Registered	Successful registration, trunk is ready for use

Request Sent	Registering
Waiting	Waiting for authentication

Service Provider:

Status	Description
OK	Successful registration, trunk is ready for use
Unreachable	The trunk is unreachable.
Failed	Trunk registration failed.

4.1.2 Network status

In this page, the IP address of LAN port will appear with their status.

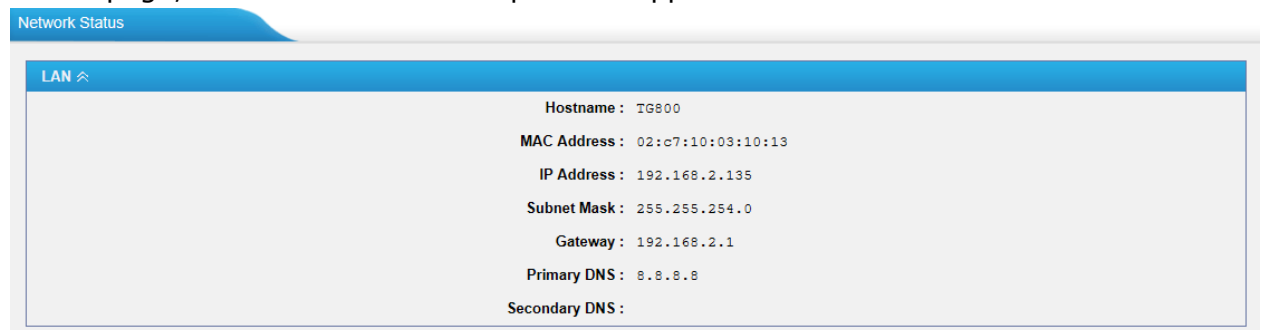


Figure 4-2

If you VLAN or OpenVPN are configured, you can check the status in this page also.

4.1.3 System info

In this page, we can check the hardware/firmware version, or the disk usage of NeoGate TG.

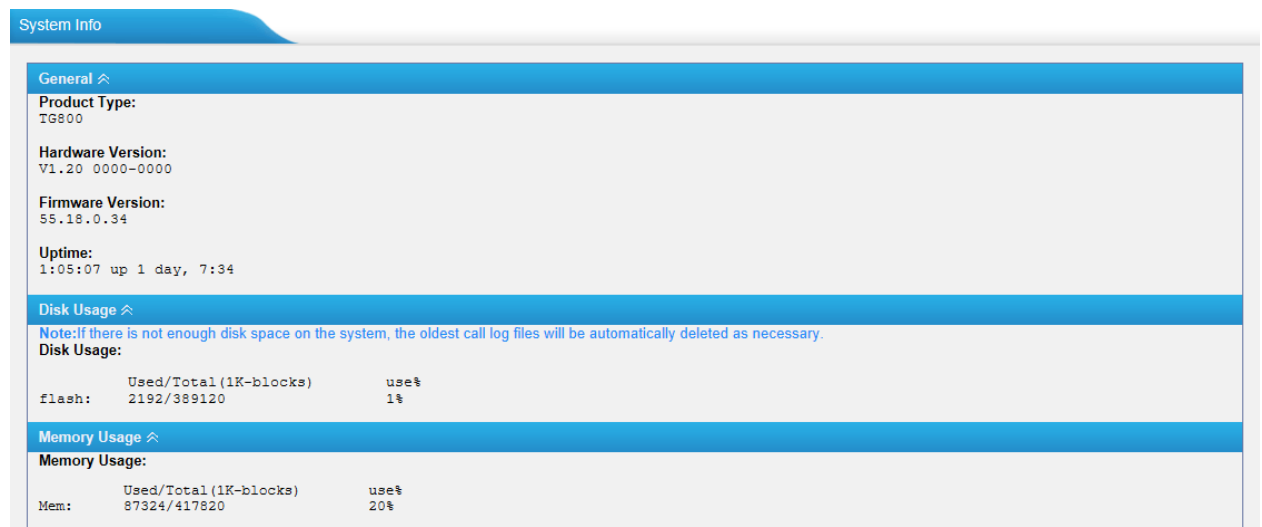


Figure 4-3

4.2 Reports

In this page, we can check the call detailed log and system log, which is used to debug.

4.2.1 Call logs

The call log captures all call details, including call time, caller number, callee number, call type, call duration, etc. An administrator can search and filter call data by call date, caller/callee, trunk, duration, billing duration, status, or communication type.

The screenshot shows the 'Call Logs' interface. At the top, there are search filters: Start Date (03 Nov 2013), End Date (03 Nov 2013), Caller/Callee, Trunk (All), Duration, Billing Duration, Status (All), and Communication Type (All). A 'Start Searching' button is present. Below the filters are buttons for 'Download the records' and 'Delete the records'. A summary bar shows 'Total: 3170', 'Show: 1-25', and 'View: 25'. The main part of the interface is a table with the following columns: Time, Caller, Callee, Source Trunk, Destination Trunk, Duration, Billing Duration, Status, and Communication Type. The table contains 15 rows of call records.

Time	Caller	Callee	Source Trunk	Destination Trunk	Duration	Billing Duration	Status	Communication Type
2013-11-03 19:53:42	404	10086	162sps	GSM2	91	88	ANSWERED	IP->GSM
2013-11-03 19:53:07	405	10086	162sps	GSM1	42	38	ANSWERED	IP->GSM
2013-11-03 19:52:54	408	10086	162sps	GSM8	91	87	ANSWERED	IP->GSM
2013-11-03 19:52:40	403	10086	162sps	GSM5	91	88	ANSWERED	IP->GSM
2013-11-03 19:52:28	406	10086	162sps	GSM4	80	77	ANSWERED	IP->GSM
2013-11-03 19:51:55	407	10086	162sps	GSM3	91	88	ANSWERED	IP->GSM
2013-11-03 19:51:44	404	10086	162sps	GSM2	91	87	ANSWERED	IP->GSM
2013-11-03 19:51:23	403	10086	162sps	GSM1	43	40	ANSWERED	IP->GSM
2013-11-03 19:50:41	405	10086	162sps	GSM8	80	76	ANSWERED	IP->GSM
2013-11-03 19:50:17	408	10086	162sps	GSM5	91	87	ANSWERED	IP->GSM
2013-11-03 19:50:15	406	10086	162sps	GSM4	80	77	ANSWERED	IP->GSM
2013-11-03 19:49:47	404	10086	162sps	GSM3	91	88	ANSWERED	IP->GSM
2013-11-03 19:49:19	403	10086	162sps	GSM2	91	88	ANSWERED	IP->GSM
2013-11-03 19:48:56	407	10086	162sps	GSM1	47	43	ANSWERED	IP->GSM

Figure 4-4

4.2.2 System logs


You can download and delete the system logs of NeoGate TG.

The screenshot shows the 'System Logs' interface. At the top, there are buttons for 'Download The Selected Logs' and 'Delete The Selected Logs'. Below this is a table with columns 'Name' and 'Type'. One log entry is visible: 'web.log' with type 'Web'. Below the table are 'Options' for logging: 'Enable Hardware Log', 'Enable Normal Log', 'Enable Debug Log', and 'Enable Web Log' (which is checked). At the bottom is a 'Packet Capture Tool' section with a status 'Packet Capture Stopped', input fields for 'IP:' and 'Port:', and buttons for 'Start', 'Stop', and 'Download'. At the very bottom are 'Save' and 'Cancel' buttons.

Figure 4-5

5. System



Click  to access. In this page, we can configure the network settings, firewall rules and some system preferences.

5.1 Network Preferences

5.1.1 LAN Settings

The screenshot shows the 'LAN Settings' page with the 'General Settings' section expanded. The configuration is as follows:

Setting	Value
DHCP	No
Enable SSH	Yes
Port	8022
Hostname	TG800
IP Address	192.168.2.135
Subnet Mask	255.255.254.0
Gateway	192.168.2.1
Primary DNS	8.8.8.8
Secondary DNS	
IP Address2	
Subnet Mask2	

Figure 5-1

Items	Description
DHCP	If this option is set as yes, NeoGate TG will act as DHCP client to get an available IP address from your local network. We don't recommend enabling this, as without the right IP address you cannot access NeoGate TG.
Enable SSH	This is the advanced way to access the device. You can use the software putty to access the device. In the SSH access, you can do more advanced setting and debug. It's disabled by default. We don't recommend enabling it if not needed.
Port	The default is 8022; you can change it to another one.
Hostname	Set the host name for NeoGate TG
IP Address	Set the IP Address for NeoGate TG, It is recommended to configure a static IP address for NeoGate TG
Subnet Mask	Set the subnet mask for NeoGate TG
Gateway	Set the gateway for NeoGate TG
Primary DNS	Set the primary DNS for NeoGate TG.
Secondary DNS	Set the secondary DNS for NeoGate TG

IP Address2	Set the second IP Address for NeoGate TG
Subnet Mask2	Set the second subnet mask for NeoGate TG

5.1.2 VLAN Settings

A VLAN (Virtual LAN) is a logical local area network (or LAN) that extends beyond a single traditional LAN to a group of LAN segments, given specific configurations.

Note:

NeoGate TG is not the VLAN server, a 3-layer switch is still needed, please configure the VLAN information there first, then input the details in NeoGate TG, so that the packages via NeoGate TG will be added the VLAN label before sending to that switch.

The screenshot shows a web interface titled "VLAN Settings" with a sub-section "VLAN Over LAN". It contains two configuration sections, NO.1 and NO.2. Each section has a checkbox to select it, followed by four input fields: "VLAN Number", "VLAN IP Address", "VLAN Subnet Mask", and "Default Gateway". At the bottom of the interface are "Save" and "Cancel" buttons.

Figure 5-2

Items	Description
NO.1	Click the NO.1 you can edit the first VLAN over LAN
VLAN Number	The VLAN Number is a unique value you assign to each VLAN on a single device
VLAN IP Address	Set the IP Address for NeoGate TG VLAN over LAN.
VLAN Subnet Mask	Set the Subnet Mask for NeoGate TG VLAN over LAN.
Default Gateway	Set the Default Gateway for NeoGate TG VLAN over LAN
NO.2	Click the NO.2 you can edit the first VLAN over LAN.
VLAN Number	.The VLAN Number is a unique value you assign to each VLAN on a single device.
VLAN IP Address	Set the IP Address for NeoGate TG VLAN over LAN.
VLAN Subnet Mask	Set the Subnet Mask for NeoGate TG VLAN over LAN.
Default Gateway	Set the Default Gateway for NeoGate TG VLAN over LAN.

5.1.3 VPN Settings

A virtual private network (VPN) is a method of computer networking--typically using the public internet--that allows users to privately share information between remote locations, or between a remote location and a business' home network. A VPN can provide secure information transport by authenticating users, and encrypting data to prevent unauthorized persons from reading the information transmitted. The VPN can be used to send any kind of network traffic securely. NeoGate TG supports OpenVPN.

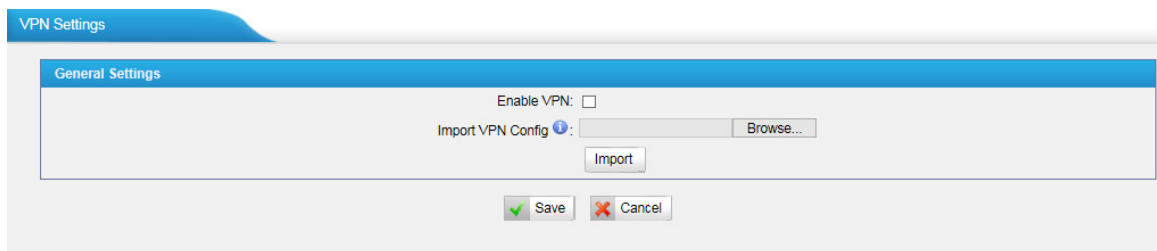


Figure 5-3

•Enable VPN

•Import VPN Config

Import configuration file of OpenVPN.

Notes:

1. Don't configure "user" and "group" in the "config" file. You can get the config package from the OpenVPN provider.
2. NeoGate TG works as VPN client mode only.

5.1.3 DDNS Settings

DDNS(Dynamic DNS) is a method / protocol / network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a Domain Name System (DNS) name server to change, in real time, the active DNS configuration of its configured hostnames, addresses or other information.

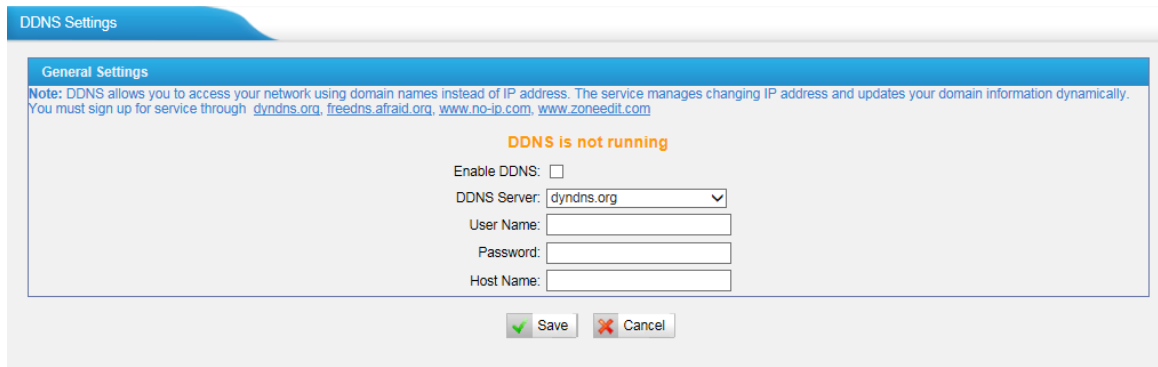


Figure 5-4

Enable DDNS

Items	Description
DDNS Server	Select the DDNS server you sign up for service.
User Name	User name the DDNS server provides you.
Password	User account’s password.
Host Name	The host name you have got from the DDNS server

Note: DDNS allows you to access your network using domain names instead of IP address. The service manages changing IP address and updates your domain information dynamically. You must sign up for service through dyndns.org, freedns.afraid.org, www.no-ip.com, www.zoneedit.com

5.1.4 Static Route

NeoGate TG will have more than one internet connection in some situations but it has only one default gateway. You will need to set some Static Route for NeoGate TG to force it to go out through different gateway when access to different internet.

The default gateway priority of NeoGate TG from high to low is VPN/VLAN → LAN port.

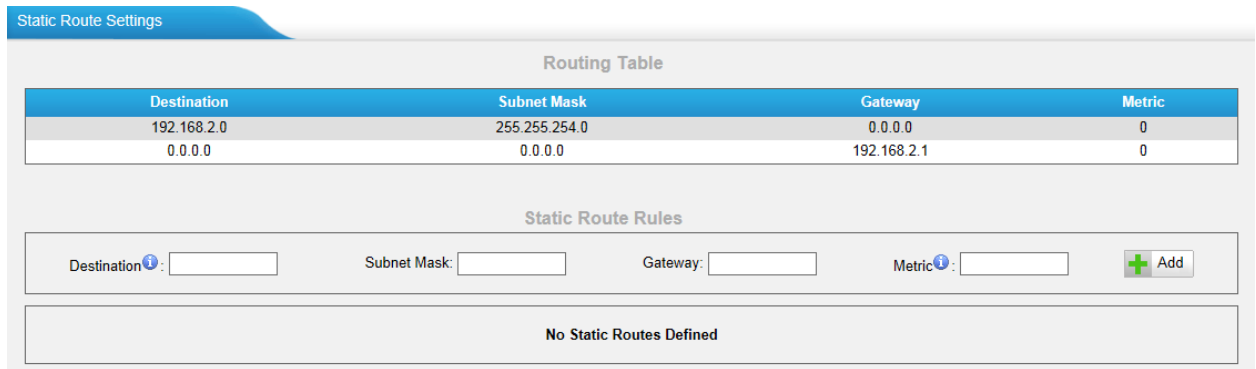


Figure 5-5

1) Route Table

The current route rules of NeoGate TG.

2) Static Route Rules

You can add new static route rules here.

Items	Description
Destination	The destination network to be accessed to by NeoGate TG.
Subnet Mask	Specify the destination network portion.
Gateway	Define which gateway NeoGate TG will go through when access to the destination network.
Metric	The cost of a route is calculated by using what are called routing metric. Routing metrics are assigned to routes by routing protocols to provide measurable statistic which can be used to judge how useful (how low cost) a route is.
Interface	Define which internet port to go through.

5.2 Security Center

5.2.1 Security Center

You can check NeoGate TG security configuration in "Security Center" page. And also, you can enter the relevant security settings page rapidly.

Firewall:

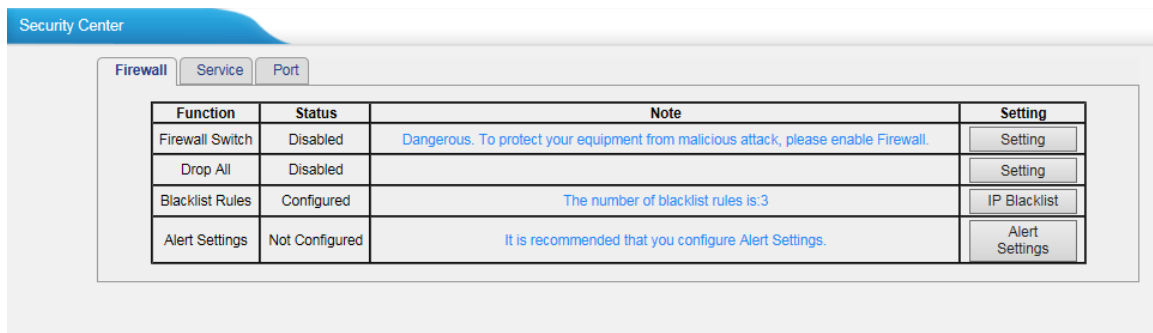


Figure 5-6

In the "Firewall" tab, you can check firewall configuration and alert settings. By

clicking the relevant button, you can enter the configuration page directly.

Service:

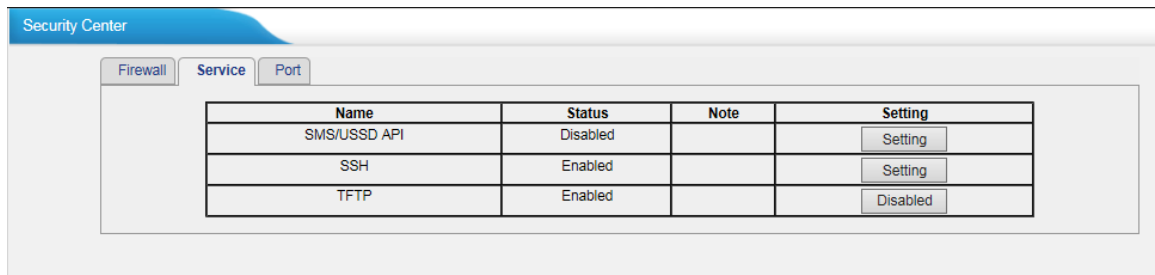


Figure 5-7

In "Service" tab, you can check SMS/USSD API /SSH/TFTP status. For SMS/USSD API, you can enter the according page by clicking the button in "Setting" column. For TFTP, you can directly disable or enable it.

Port:

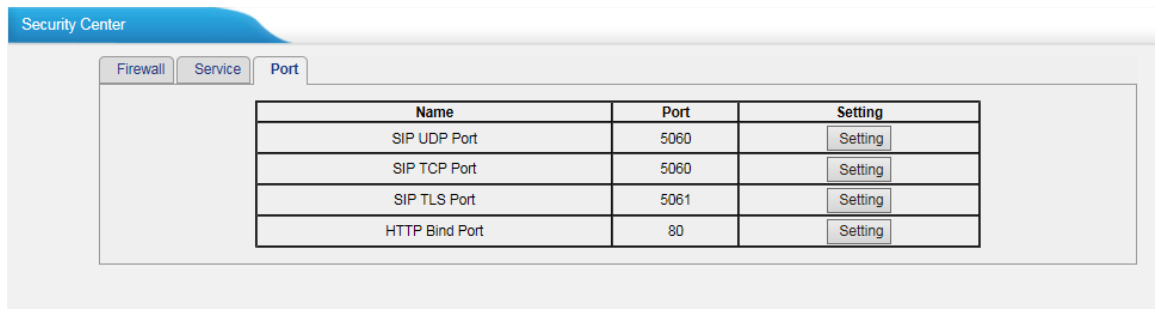


Figure 5-8

In "Port" tab, you can check SIP port and HTTP port. You can also enter the relevant page by clicking the button in "Setting" column. We recommend changing the default port for security.

5.2.2 Alert settings

If the device is under attack, the system will alert users via call or E-mail. The attack modes include IP attack and Web Login.

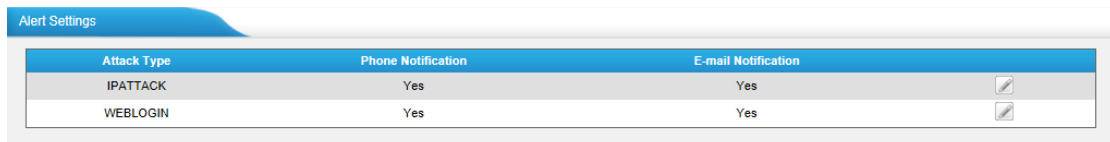


Figure 5-9

1. IPATTACK

When the system is attacked by IP address, the firewall will add the IP to auto IP Blacklist and notify the user if it match the protection rule.

1) Phone Notification Settings

Items	Description
PHONE Notification	Whether enable phone notification
Number	The numbers could be set for alert notification, users can setup multiple extension and outbound phone numbers. Please separate them by ";". Example: "500;9911", if the extension has configured Follow Me Settings, the call would go to the forwarded number directly.
Port	Choose the GSM/UTMTS/CDMA port to dial alert call.
Attempts	The attempts to dial a phone number when there is no answer.
Interval	The interval between each attempt to dial the phone number. Must be longer than 3 seconds, the default value is 60 seconds.
Prompt	Users will hear the prompt while receiving the phone notification.

2) E-mail Notification Settings

Note: Please ensure that all voicemail settings are properly configured on the System Settings -> Voicemail Settings page before using this feature.

Items	Description
E-mail Notification	Whether enable E-mail Notification
Recipient's Name	The recipients for the alert notification, and multiple email addresses are allowed, please separate them by ";". Example: jerry@yeastar.com;jason@yeastar.com, 456@sina.com
Subject	The subject of the alert email.
Email Content	Text content support for predefined variables. Variable names and corresponding instructions are as follows: gateway hostname:\$(HOSTNAME) attack source ip address:\$(SOURCEIP) attack dest mac:\$(DESTMAC) attack source port:\$(DESTPORT) attack source protocol:\$(PROTOCOL) attack occurred:\$(DATETIME)

The screenshot shows a configuration window titled "IPATTACK" with two main sections: "Phone Notification Settings" and "E-mail Notification Settings".

Phone Notification Settings:

- Phone Notification: Yes (dropdown)
- Number: 915812345678 (text input)
- Attempts: 1 (dropdown)
- Interval: 60 s (text input)
- Prompt: default (dropdown) with a link to "Custom Prompts"

E-mail Notification Settings:

- E-mail Notification: Yes (dropdown)
- To: jerry@yeastar.com (text input)
- Subject: IP Attack (text input)
- Message body (text area):
pbx hostname:\$(HOSTNAME)
attack source ip address:\$(SOURCEIP)
attack dest mac:\$(DESTMAC)
attack source port:\$(DESTPORT)
attack source protocol:\$(PROTOCOL)
attack occurred:\$(DATETIME)

At the bottom of the window are "Save" and "Cancel" buttons.

Figure 5-10

2. WEBLOGIN

Web Login Alert Notification: Enter the password incorrectly five times to login NeoGate TG Web interface will be as attack, the system will limit the IP login within 10 minutes and notify the user.

The screenshot shows a window titled "WEBLOGIN" with two sections: "Phone Notification Settings" and "E-mail Notification Settings".

Phone Notification Settings:

- Phone Notification: Yes (dropdown)
- Number: 915812345678 (text input)
- Attempts: 1 (dropdown)
- Interval: 60 s (text input)
- Prompt: default (dropdown) with a link to "Custom Prompts"

E-mail Notification Settings:

- E-mail Notification: Yes (dropdown)
- To: jerry@yeastar.com (text input)
- Subject: Web Login (text input)
- Body template (text area):


```
pbx hostname:$(HOSTNAME)
login ip address:$(SOURCEIP)
login username:$(USERNAME)
login occurred:$(DATETIME)
```

At the bottom are "Save" and "Cancel" buttons.

Figure 5-11

5.2.3 Certificates

NeoGate TG can support TLS trunk. Before you register TLS trunk to NeoGate TG, you should upload certificates first.

The screenshot shows the "Upload Certificate" dialog box. It has a "Type" dropdown menu with "Trusted Certificate" selected. Below it is a "Choose a certificate to Upload:" label and a "Browse..." button. At the bottom are "Save" and "Cancel" buttons. The background shows a table with the header "Gateway Certificate" and the text "No Certificates Defined".

Figure 5-12

Trusted Certificate

This certificate is a CA certificate. When selecting "TLS Verify Client" as "Yes", you should upload a CA. The relevant IPPBX should also have this certificate.

Gateway Certificate

This certificate is server certificate. No matter selecting "TLS Verify Client" as "Yes" or "NO", you should upload this certificate to NeoGate TG. If IPPBX enables "TLS Verify server", you should also upload this certificate on IPPBX.

5.2.4 Firewall Rules

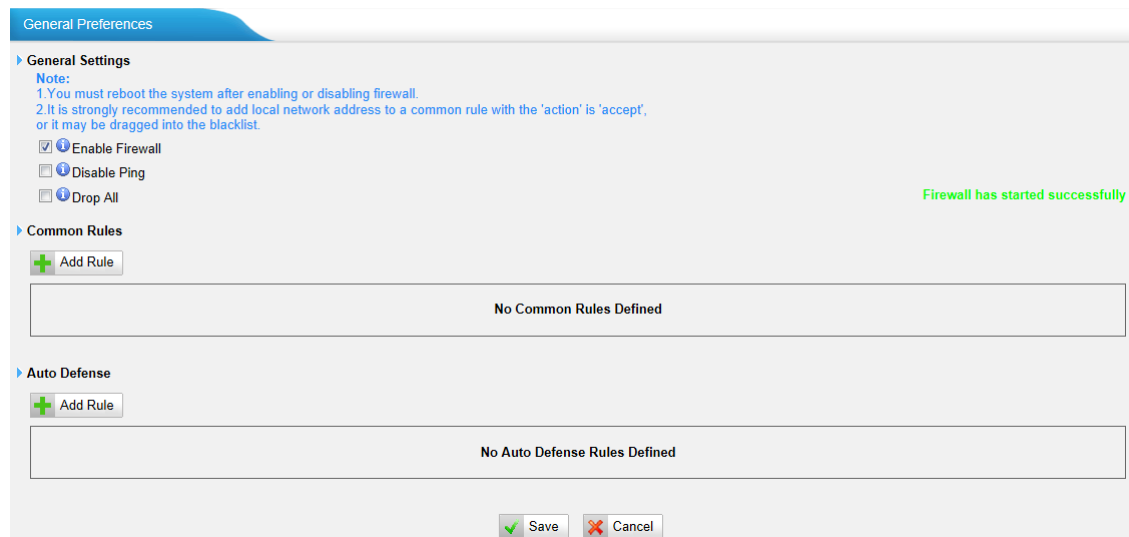


Figure 5-13

1) General Settings

Items	Description
Enable Firewall	Enable the firewall to protect the device. You should reboot the device to make the firewall run successfully.
Disable Ping	Enable this item to drop net ping from remote hosts.
Drop All	When you enable "Drop All" feature, system will drop all packets or connection from other hosts if there are no other rules defined. To avoid locking the devices, at least one "TCP" accept common rule must be created for port used for SSH access, port used for HTTP access and port sued for CGI access.

2) Common Rules

There is no default rule; you can create one as required.

Figure 5-14

Items	Description
Name	A name for this rule, e.g. "HTTP".
Description	Simple description for this rule. E.g.: Accept the specific host to access the web interface for configuration.
Protocol	The protocols for this rule.
Port	Initial port should be on the left and end port should be on the right. The end port must be equal to or greater than start port.
IP	The IP address for this rule. The format of IP address is: IP/mask Ex: 192.168.5.100/255.255.255.255 for IP 192.168.5.100 Ex:192.168.5.0/255.255.255.0 for IP from 192.168.5.0 to 192.168.5.255 .
MAC Address	The format of MAC Address is XX:XX:XX:XX:XX:XX, X means 0~9 or A~F in hex, the A~F are not case sensitive.
Action	Accept: Accept the access from remote hosts. Drop: Drop the access from remote hosts. Ignore: Ignore the access.

Note: The MAC address will be changed when it's a remote device, so it will not be working to filter using MAC for remote devices.

5.2.5 IP Blacklist

You can set some packets accept speed rules here. When a IP address which hasn't been accepted in common rules sends packets faster than the allowed speed, it will be set as black IP address and blocked automatically.

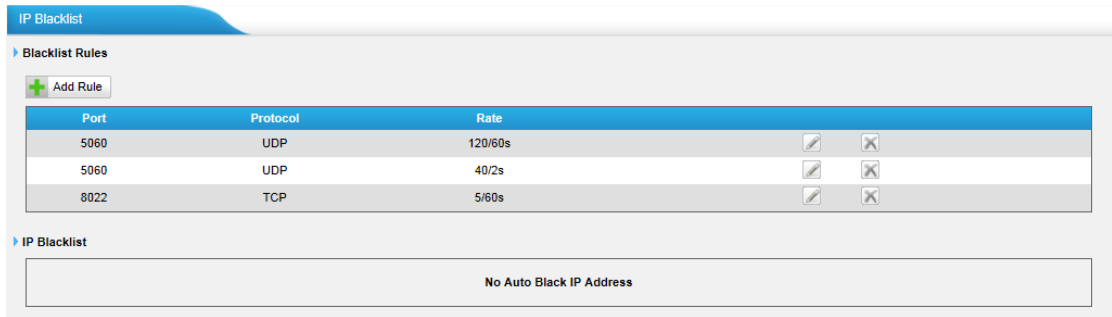


Figure 5-15

1) Blacklist rules

We can add the rules for IP blacklist rate as demanded.

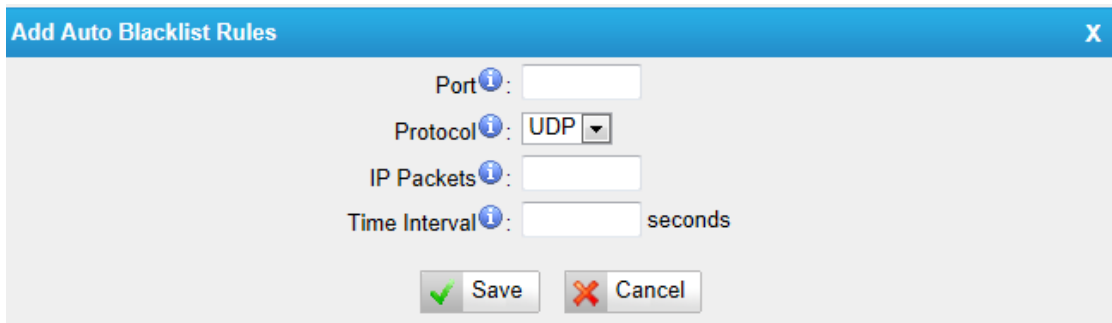


Figure 5-16

Items	Description
Port	Auto defense port
Protocol	Auto defense protocol. TCP or UDP.
IP Packets	Allowed IP packets number in the specific time interval.
Time interval	The time interval to receive IP packets. For example, IP packets 90, time interval 60 means 90 IP packets are allowed in 60 seconds.

2) IP blacklist

The blocked IP address will display here, you can edit or delete it as your wish.

5.3 System Preferences

In this page, we can set other system preferences, like the password for admin account, system date and time, firmware update, backup and restore, reset and reboot.

5.3.1 Password settings

The default password is "password". To change the password, enter the new password and click update. The system will then prompt you re-login using your

new password.

The screenshot shows a web interface for 'Password Settings'. At the top, there is a blue header with the text 'Password Settings'. Below this is a white box with a blue title bar that says 'Change Password'. Inside this box, there are three input fields: 'Enter Old Password:', 'Enter New Password:', and 'Retype New Password:'. Below the input fields is a green 'Save' button with a checkmark icon.

Figure 5-17

5.3.2 Date and Time

Set the date and time for NeoGate TG.

The screenshot shows a web interface for 'Date & Time' settings. At the top, there is a blue header with the text 'Date & Time'. Below this is a white box with a blue title bar that says 'Date & Time'. Inside this box, the 'Server Time' is displayed as 'Tue Jul 30 22:51:40 2013'. There are two dropdown menus: 'Time Zone' set to '-8 United States - Pacific Time' and 'Daylight Saving Time' set to 'Disabled'. There are two radio button options: 'Automatically Synchronize With An Internet Time Server' (which is selected) and 'Set Date & Time Manually'. Under the selected option, there is an 'NTP Server' input field with 'pool.ntp.org' entered. Under the 'Set Date & Time Manually' option, there are 'Date' and 'Time' input fields. At the bottom, there are green 'Save' and red 'Cancel' buttons.

Figure 5-18

Items	Description
Time Zone	You can choose your time zone here.
Daylight Saving Time	Set the mode to Automatic or disabled
Automatically Synchronize With an Internet Time Server	Input the NTP server so that NeoGate TG will update the time automatically
Set Date & Time Manually	You can set the time to your local right time manually here

5.3.3 Custom Prompts

We can upload the prompts in this page; you can also download it and save it as a backup.

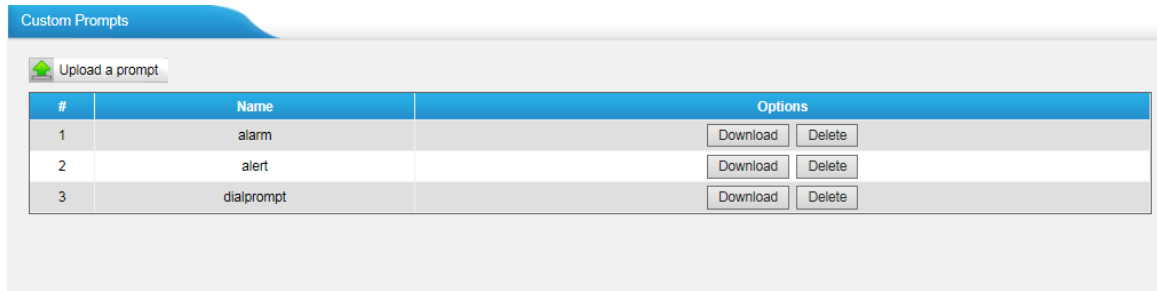


Figure 5-19

The administrator can upload prompts by doing the following:

- 1) Click "Upload Prompt".
- 2) Click "Browse" to choose the desired prompt.
- 3) Click "Upload" to upload the selected prompt.

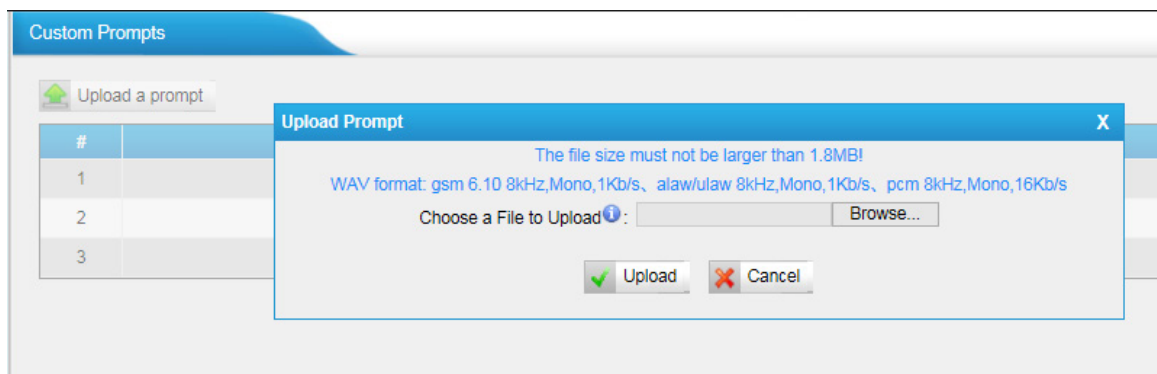


Figure 5-20

Note: The file size must not be larger than 1.8 MB, and the file must be WAV format:

- GSM 6.10 8 kHz, Mono, 1 Kb/s;
- Alaw/Ulaw 8 kHz, Mono, 1 Kb/s;
- PCM 8 kHz, Mono, 16 Kb/s.

5.3.4 Email settings

To send the SMS or system alert to email address, please configure the Email settings first, and make sure SMTP test is successful.

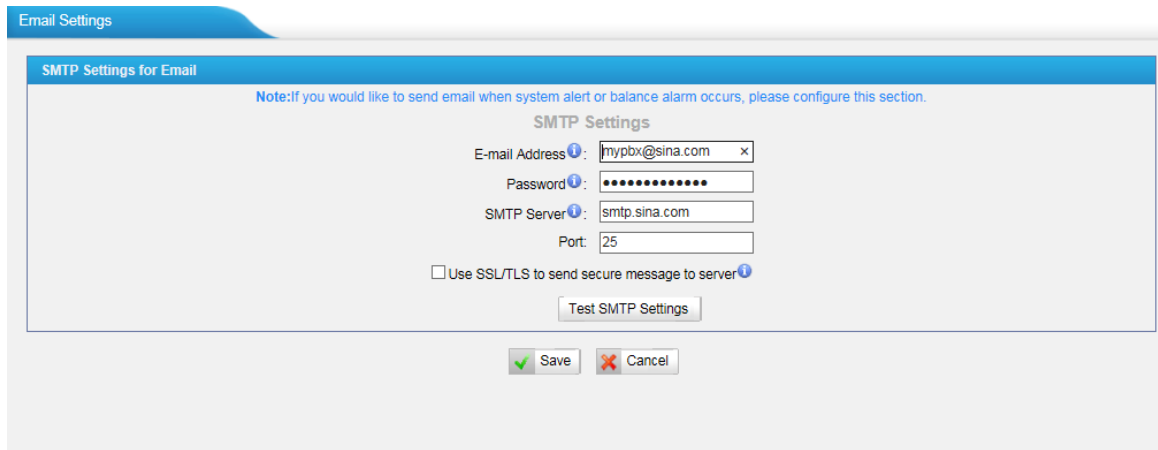


Figure 5-21

Items	Description
E-mail Address	The E-mail Address that NeoGate TG will use to send voicemail.
Password	The password for the email address used above
SMTP Server	The IP address or hostname of an SMTP server that the NeoGate TG will connect to in order to send voicemail messages via email, i.e. mail.yourcompany.com.
Port	SMTP Port: the default value is 25.
Use SSL/TLS to send secure message to server	If the server of sending email needs to authenticate the sender, you need to enable this Note: Must be selected for Gmail or exchange server.

After filling out the above information, you can click on the "Test Account Settings" button to check whether the setup is OK.

- 1) If the test is successful, you can use the email safely.
- 2) If test failed, please check if the above information is correct or network is proper.

5.3.5 Firmware Update

Upgrading of the firmware is possible through the Administrator Web interface using a TFTP Server or an HTTP URL.

Enter your TFTP Server IP address and firmware file location, then click start to update the firmware

Notes:

1. If enabled "Reset configuration to Factory Defaults", System will restore to factory default settings.
2. When update the firmware, please don't turn off the power. Or the system will get damaged.

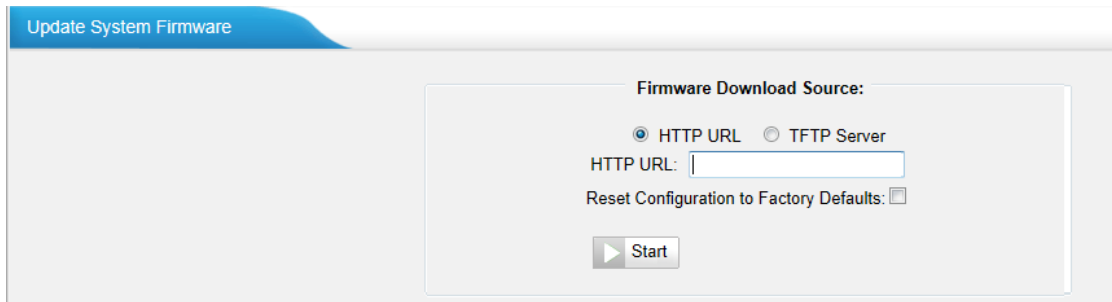


Figure 5-22

5.3.6 Backup and Restore

We can backup up the configurations before reset NeoGate TG to factory defaults, and then restore it using this package.

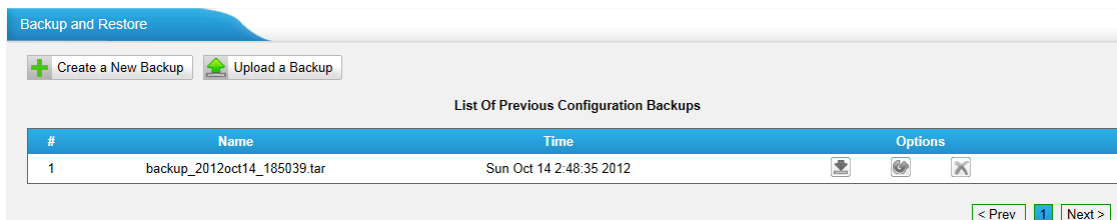


Figure 5-23

Notes:

1. Only configurations, custom prompts will be backed up.
2. When you have updated the firmware version, it's not recommended to restore using old package.

5.3.7 Reset and Reboot

We can reset or reboot NeoGate TG directly in this page.

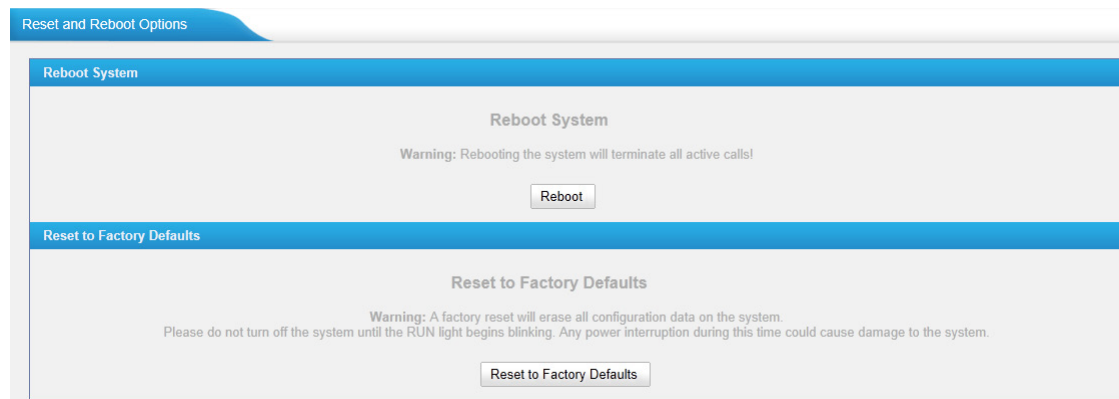


Figure 5-24

•Reboot System


Warning: Rebooting the system will terminate all active calls!

•Reset to Factory Defaults

Warning: A factory reset will erase all configuration data on the system. Please do not turn off the system until the RUN light begins blinking. Any power interruption during this time could cause damage to the system.

6 SMS



Click  to access the SMS page, it has the powerful SMS toolkit like send/receive SMS, USSD, and SMS API. We can also check the status of SMS that we sent.

6.1 Send SMS

In this page, we can send the SMS directly via GSM/UTMTS/CDMA port directly.

Figure 6-1

Items	Description
Country code	Choose the country code of yours, if you cannot find the code for you, just ignore it and add the code before number in "destiation" field to send SMS.
Destination	Input the destination number to send the SMS to, you can also choose the contact directly by name or Group.
Select Port	Choose the channel to send the SMS
Content	Input the content of SMS, the max characters can reach 300. If the length you send is longer than 160, the SMS will be cut into 2 pieces at provider side.

6.2 SMS Contacts

We can add the contact in NeoGate TG to send the SMS, then we can choose the contact by name or Group before sending SMS.

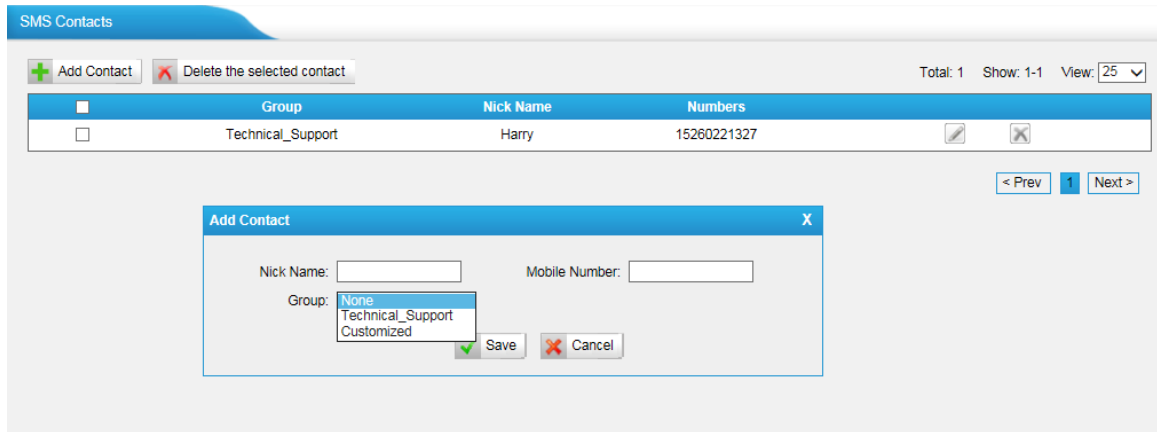


Figure 6-2

To customize the Group name, just choose "Customized", then input the group name, the special characters like blank is not allowed. You can input "_" instead.

6.3 Outbox

To check the SMS we sent, we can check it in outbox page, there are some filters for searching the SMS we want. We can also check the status of email below.

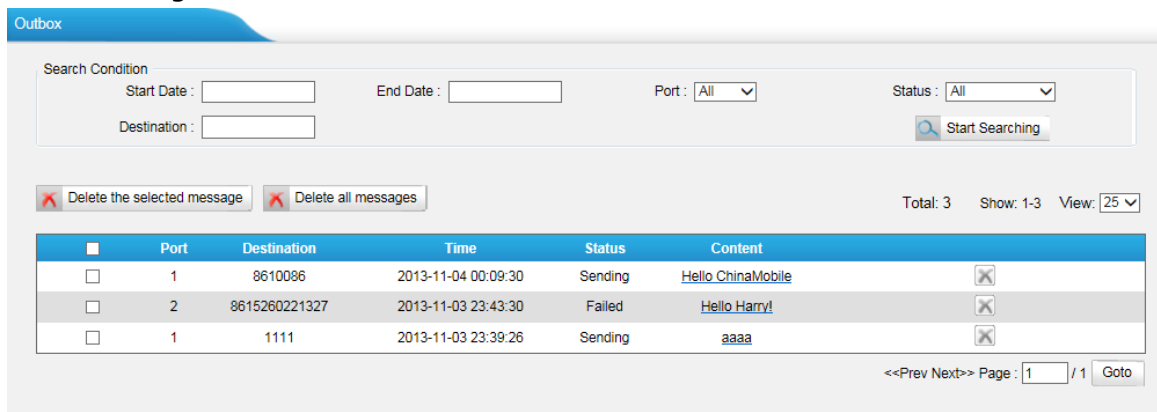


Figure 6-3

6.4 Inbox

NeoGate TG can check the incoming SMS also in this page; we can search SMS via filters like date, port and read status etc. We can also reply this SMS directly in this page via the same port.

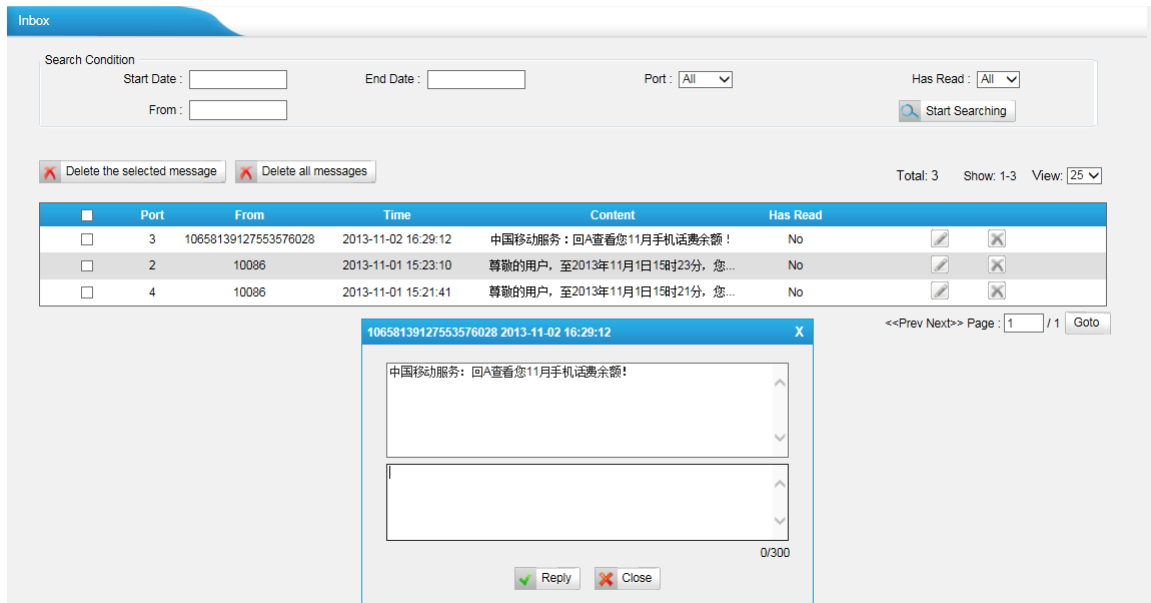


Figure 6-4

6.5 USSD

Unstructured Supplementary Service Data (USSD) is a protocol used by GSM/UTMTS/CDMA cellular telephones to communicate with the service provider's computers. USSD can be used for WAP browsing, prepaid callback service, mobile-money services, location-based content services, menu-based information services, and as part of configuring the phone on the network.

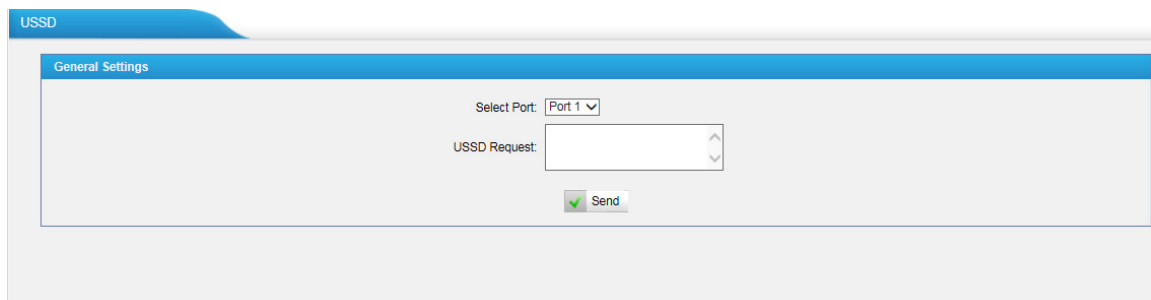


Figure 6-5

Choose the SIM port to send the request to carrier for the services.

6.6 API Settings

To send and receive SMS, it's supported connect to NeoGate TG using third party software via API, then he can send and receive SMS without login Web interface.

The screenshot shows a web interface titled "API Settings" with a sub-section "Send SMS and USSD API". At the top right of this section is a checkbox labeled "Enable API". Below it are two text input fields: "User Name" containing "apiuser" and "Password" containing "apipass". Underneath these is a section titled "Permitted IP Address" which contains a large empty rectangular box. At the bottom of this box is a label "Permitted 'IP address/Subnet mask'" followed by a small blue information icon, a text input field, and an "Add" button with an upward arrow. At the very bottom of the interface are two buttons: "Save" with a green checkmark icon and "Cancel" with a red X icon.


Figure 6-6

Enable API first, define the user name and password. You can set up the IP restriction for some special IP, the software can connect to NeoGate TG via the IP only.

We recommend configuring "Permitted 'IP address/Subnet mask'" for security.

7 Gateway



Click  to access the gateway configuration page. We can configure the details of GSM/UTMTS/CDMA trunks, VoIP trunks and the call routing rules.

7.1 Mobile List

7.1.1 Mobile List

All the GSM/UTMTS/CDMA modules will be listed here, edit each to the settings as you wish, and power off or reboot this module (Port) separately.

Port	Trunk Name	Type	Single Call Max Duration (min)	Max. Call Duration (min)	Call Duration (min)	Power On/Off	Reboot Module	
1	GSM1	GSM	0	0	2335	Power Off	Reboot	
2	GSM2	GSM	0	0	3922	Power Off	Reboot	
3	GSM3	GSM	0	0	3900	Power Off	Reboot	
4	GSM4	GSM	0	0	3909	Power Off	Reboot	
5	GSM5	GSM	0	0	2804	Power Off	Reboot	
6	GSM6	GSM	0	0	0	Power Off	Reboot	
7	GSM7	GSM	0	0	0	Power Off	Reboot	
8	GSM8	GSM	0	0	2736	Power Off	Reboot	

Figure 7-1

Click edit to configure the GSM/UTMTS/CDMA channels.

X
Edit GSM Trunk - GSM1

General

Call Duration Settings

Advanced Settings

Trunk Name (i):

Mobile Number:

CLIR (i): No v

RxGain (i): 60% v

TxGain (i): 40% v

Call Progress Tone: No v

Save
 Cancel

Figure 7-2

1) General

Items	Description
Trunk name	Design the name of this trunk, it will display in mobile list and trunk status page.
Mobile number	Input the mobile number here to take a note only.
CLIR	Calling Line Identification Restriction. If you want to hide your mobile number, you can enable it. It's disabled by default. Note: Please contact the SIM carrier to confirm if it's supported in advance.
RxGain	To adjust the received volume, please configure this one. No need to change it if the volume is fine. It's 60% by default.
TxGain	To adjust the transmit volume, please configure this one. No need to change it if the volume is fine . It's 40% by default
Call Progress Tone	When dialing from SIP to GSM/UTMTS/CDMA, during the trying period at SIM carrier side, it's completely silent in SIP side. Enable this to get a virtual ring back tone.

2) Call Duration Settings

In this page we can configure the duration of this channel, you can also enable the blank alarm when the time is beyond the value you have pre-configured.

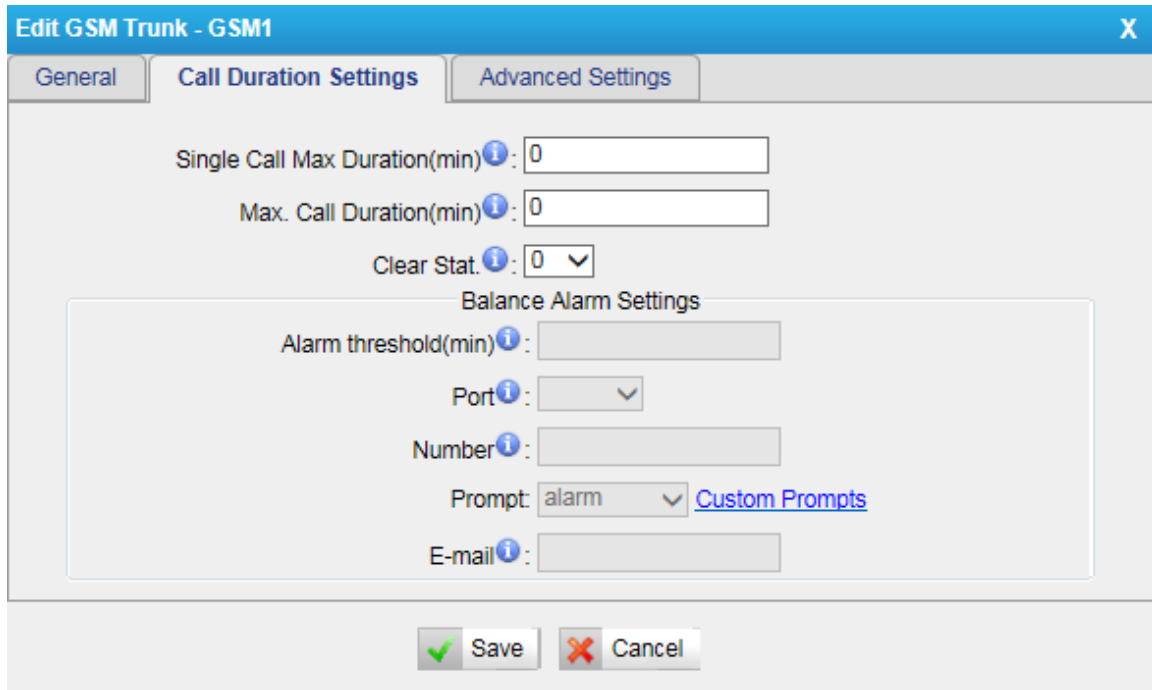


Figure 7-3

Items	Description
Single Call Max Duration(min)	Configure the duration of each call, it's 0 by default, which means no limit.
Max. Call Duration(min)	Configure the max duration of this GSM/UTMTS/CDMA port, it's 0 by default, which means no limit.
Clear Stat.	The date to clean the duration status each month.
Balance Alarm Settings	When Max. Call Duration(min) is configured a 0 (no limit), this feature is disabled.
Alarm threshold(min)	Cofigure the time duration when NeoGate TG will send the alarm message. The value must be less than "Max Call Duration".
Port	Choose the port to dial the alarm call.
Number	The number to receive the alarm call.
Prompt	The prompt played during the alarm call,you can customize the prompts as your wish.
E-mail	The email address to receive the alarm email. Note: please make sure SMTP test is successful in "Email settings" page before configuring this.

3) Advanced settings.

Edit GSM Trunk - GSM1

General | Call Duration Settings | **Advanced Settings**

IMEI: 013227009598602

IMSI: 460003290311575

SMS Center: +8613800200500

Carrier: Automatic Manual

CHINA MOBILE ▾

Band: Default ▾

PIN Code:

Warning: Be careful. If you failed to enter your correct PIN code 3 times in succession, SIM card will be blocked.

Save Cancel

Figure 7-4

Items	Description
IMEI	International Mobile Equipment Identity of this module, it's not changeable.
IMSI	International Mobile Subscriber Identification of SIM card, it's not changeable.
SMS Center	The SMS center of this SIM card, NeoGate will generate this by default. You can also input the number here for the carrier if it's not the default one.
Carrier	The carrier connected by default. You can also choose manual mode if this SIM card is supported by several carriers.
Band	The band of this SIM card, you can choose PGSM900, DCS1800, PCS1900, EGSM900/DCS1800, GSM850/PCS1900
PIN Code	The PIN code of this SIM card, if it's disabled by cellphone, just keep it blank here. Warning: Be careful. If you failed to enter your correct PIN code 3 times in succession, the SIM card will be blocked.

7.1.2 Module Group

To route the call to a GSM/UTMTS/CDMA channels group, and dial out by the strategy we chose, NeoGate can route the call in advanced method depending on your needs.

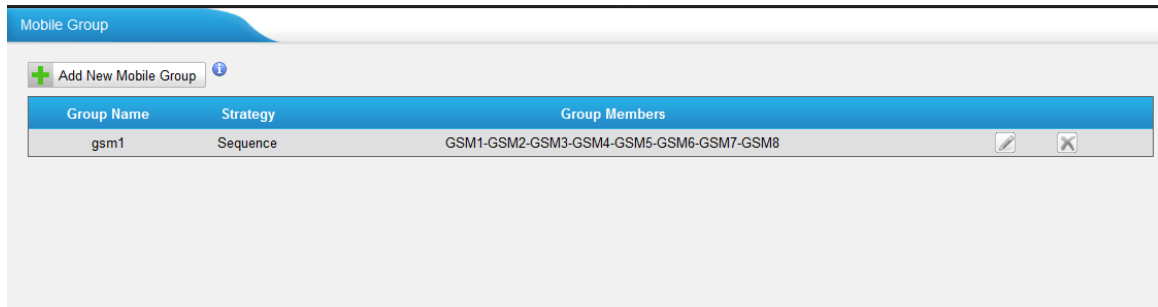


Figure 7-5

You can create new mobile group or edit the default one.

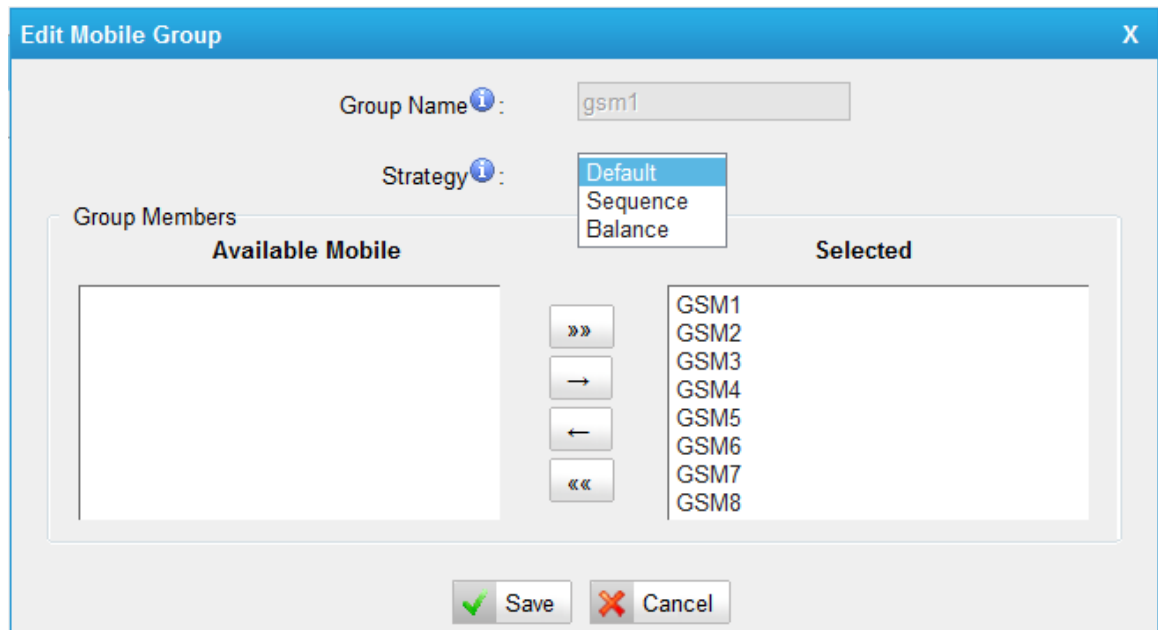


Figure 7-6

Items	Description
Group Name	Design the group name of this mobile group
Strategy	Choose the strategy of how to use these GSM/UTMTS/CDMA channels. Default: The first channel will be used first always, when it's busy, NeoGate TG will choose the next one. Sequence: The whole channels will be used one by one. Balance: These channels will be balanced used .
Group Members	The channels selected to right side will be a member of this mobile group.

7.1.3 Call Waiting

Call waiting is a feature supported by SIM carrier, when there is a second call dialing into this SIM card, there will be waiting tone instead of hang up or do

follow me.

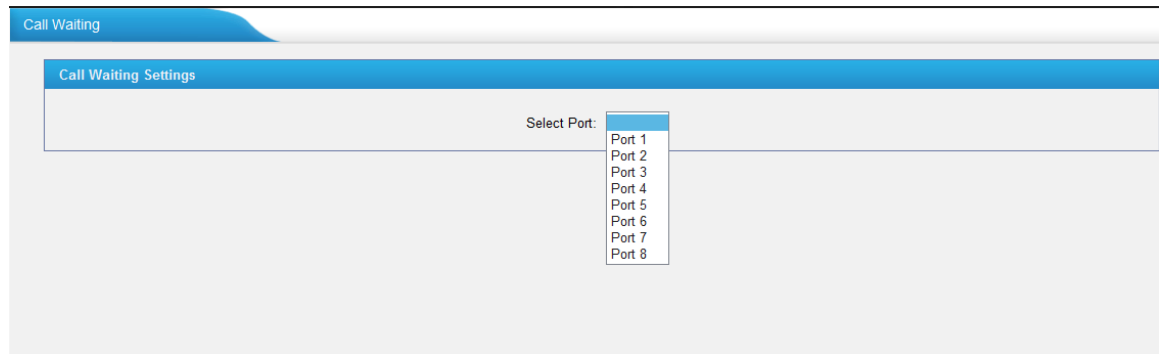


Figure 7-7

Choose the port to set up call waiting, NeoGate will contact the SIM carrier to define if call waiting is supported. If yes, a window will pop up allowing you to enable or disable call waiting.

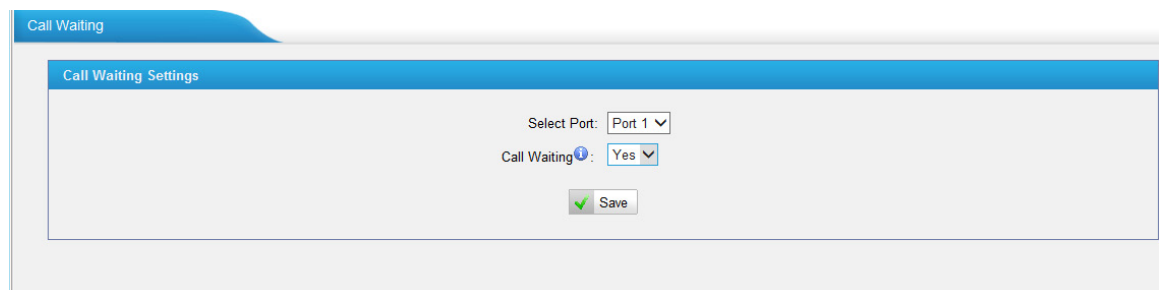


Figure 7-8

Notes:

1. It takes several seconds to contact SIM carrier to get the call waiting status.
2. When call waiting is enabled, follow me will not work.

7.1.4 Follow me

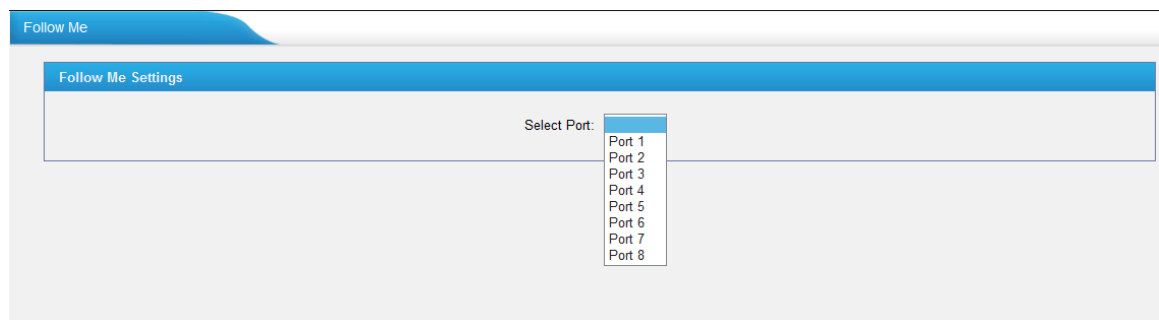


Figure 7-9

Choose the available port to set up follow me, NeoGate will contact the SIM carrier to confirm if follow me is supported. If yes, a window will pop up allowing you to configure the details.

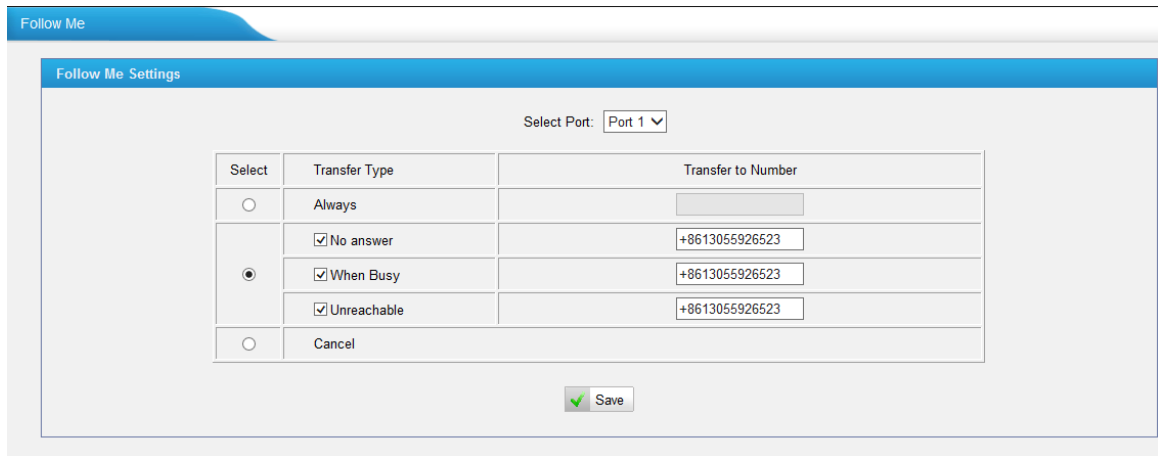


Figure 7-10

We can choose the transfer type, input the number you want to transfer the call, just make sure the number you input there is reachable. When a call arrived, the call will be transferred to that number.

Notes:

1. It takes several seconds to contact SIM carrier to get the status of follow me feature.
2. The follow me feature needs the support of SIM carrier.

7.2 VoIP Settings

To integrate with other IPPBX, we need to configure the VoIP settings in NeoGate TG to set up VoIP trunk (SIP and IAX).

7.2.1 VoIP trunk

There are 3 types in VoIP trunk page. We can create VoIP account, VoIP trunk, service provider trunk here.

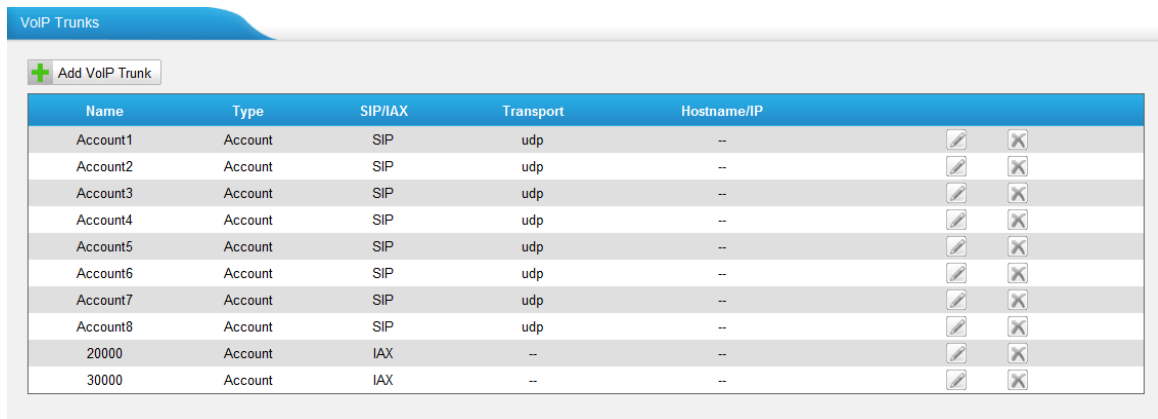


Figure 7-11

1) VoIP account

Figure 7-12

Items	Description
Trunk type	Account mode will allow IP phone or IPPBX to register using this account to NeoGate
Type	Choose type of this account, SIP, IAX, or SIP/IAX
Name	Define the name for this account
Account	Define the number for this account
Password	Define the password for this account

Figure 7-13

Items	Description
Enable SRTP	Secure Real-time Transport Protocol, if it's enabled, the same setting should be enabled in IP phone side.
Qualify	Send check alive packets to IP phones, when it's disabled, NeoGate will ignore the reachability and the

	status of this account will be unmonitored.
Transport	This will be the transport method used by the extension. The options are UDP (default) or TCP or TLS.
DTMF Mode	RFC2833, Info, Inband, Auto.

2) VoIP Trunk

In this mode, you can register NeoGate TG to provider via the trunk details with authorization details.

The screenshot shows a dialog box titled "Add New Trunk" with two tabs: "General" and "Advanced". The "Advanced" tab is selected. The form contains the following fields:

- Trunk Type: Trunk (dropdown)
- Type: SIP (dropdown)
- Provider Name: [text input]
- Hostname/IP: [text input] : 5060 (text input)
- Domain: [text input]
- User Name: [text input]
- Authorization Name: [text input]
- Password: [text input]

At the bottom of the dialog, there are two buttons: "Save" (with a green checkmark icon) and "Cancel" (with a red X icon).

Figure 7-14

Items	Description
Trunk Type	Choose trunk mode to register to provider
Type	Choose the type of this trunk, SIP or IAX
Provider Name	Input the name of provider
Hostname/IP	Service provider’s hostname or IP address, 5060 is the standard port number used by SIP protocol. Don’t change this part if it is not required.
Domain	VoIP provider’s server domain name
User Name	Username of SIP account
Authorization Name	Used for SIP authentication, it’s the same as user name generally.
Password	Password of SIP account

Add New Trunk [X]

General | **Advanced**

From User:

Online Number ⁱ:

Maximum Channels ⁱ:

Caller ID ⁱ:

Enable SRTP ⁱ:

Qualify:

Enable Outbound Proxy Server

FirstCodec:

SecondCodec:

ThirdCodec:

FourthCodec:

FifthCodec:

Transport:

DTMF Mode:

DOD Settings

DOD: Associated Number:

Figure 7-15

Items	Description
From User	All outgoing calls from this SIP Trunk will use the From User in From Header of the SIP Invite package. Keep this field blank if not needed.
Online Number	Define the online number for "Skype Connect" and some other SIP service providers. Leave this field blank if not needed.
Maximum Channels	Control the maximum number of simultaneous calls, set as 0 to specify no limit.
Caller ID	Specify the caller ID to use when making outbound calls

	over this trunk.
Enable SRTP	Define if SRTP is enabled for this trunk, it depends on provider's configuration.
Qualify	Send check alive packets to the SIP provider.
Enable outbound proxy server	A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI.
Codec	Define the codec for this SIP trunk and its priority
Transport	This will be the transport method used by the SIP Trunk. This method is given by the SIP trunk provider. The options are UDP (default) or TCP or TLS.
DTMF Mode	Set default mode for sending DTMF of this trunk. Default setting: rfc2833
DOD settings	DOD (Direct Outward Dialing) means the caller ID displayed when dialing out, before configure this, and please make sure the provider supports this feature.

3) Service provider

This is service provider trunk (peer to peer mode), which uses IP address only. If you have got a trunk with only IP address, please choose this type.

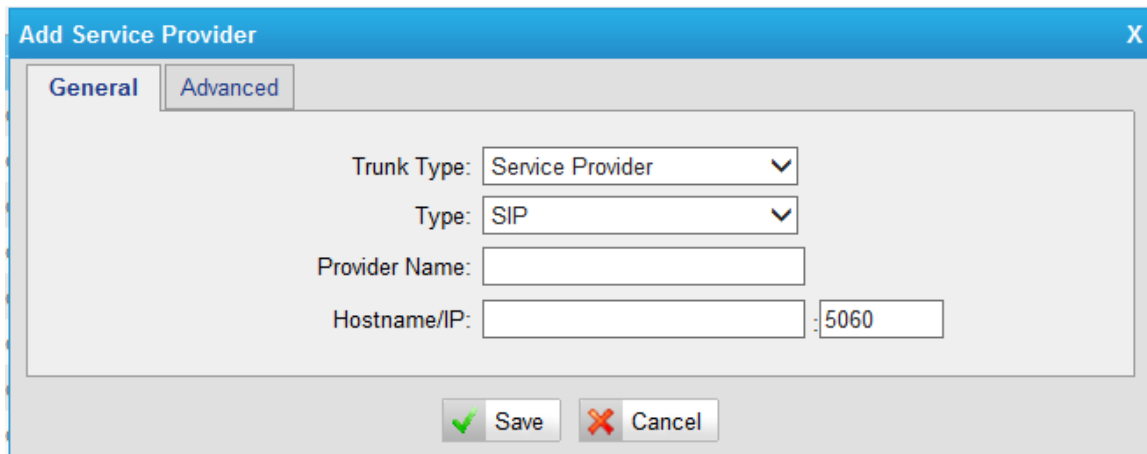


Figure 7-16

Items	Description
Trunk Type	Choose trunk mode to register to provider
Type	Choose the type of this trunk, SIP or IAX
Provider Name	Input the name of provider
Hostname/IP	Service provider's hostname or IP address, 5060 is the standard port number used by SIP protocol. Don't change this part if it is not required.

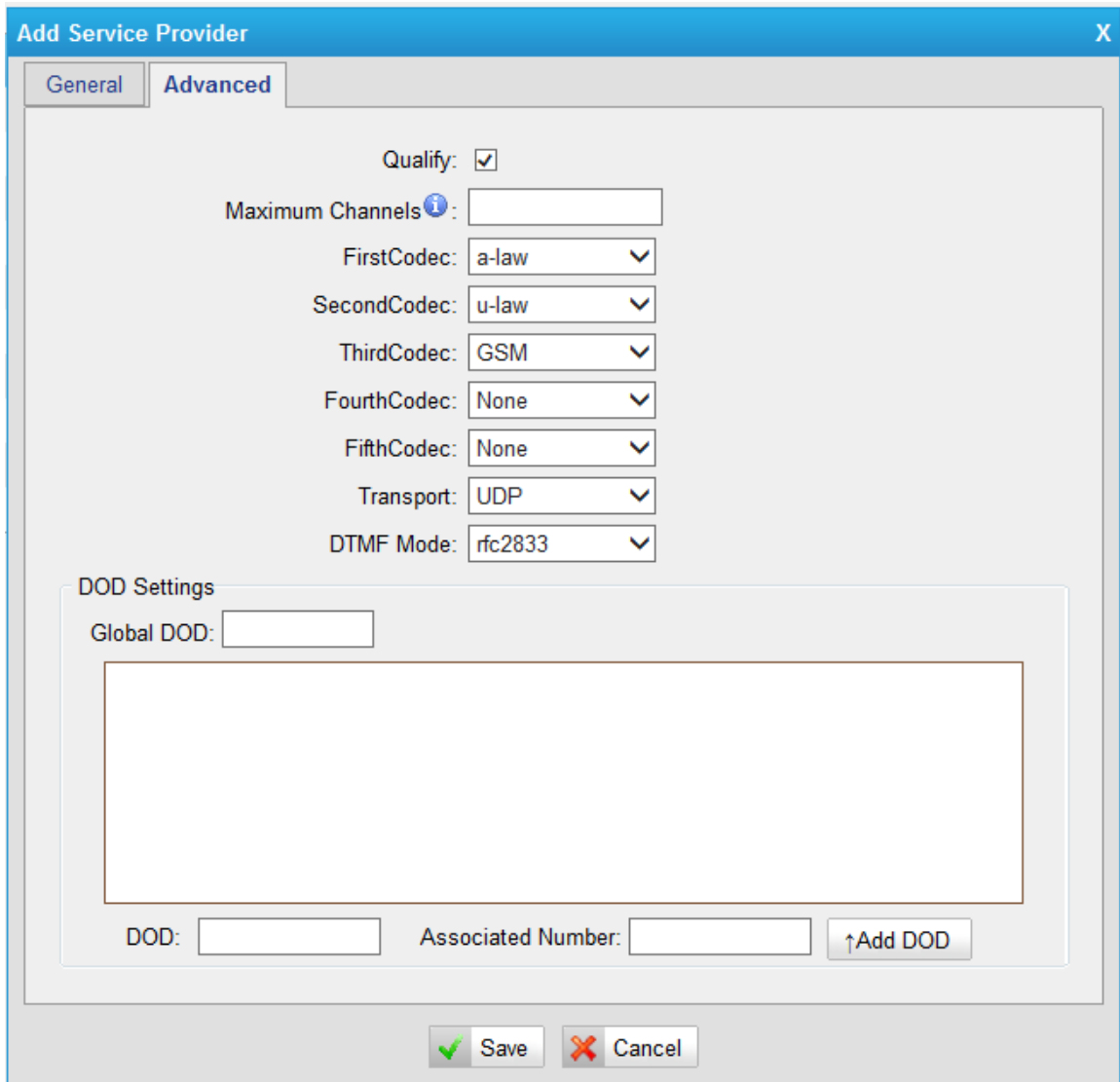


Figure 7-17

Items	Description
Qualify	Send check alive packets to the SIP provider.
Maximum Channels	Controls the maximum number of simultaneous calls, set as 0 to specify no limit
Codec	Define the codec for this SIP trunk and its priority
Transport	This will be the transport method used by the SIP Trunk. This method is given by the SIP trunk provider. The options are UDP (default) or TCP or TLS.
DTMF Mode	Set default mode for sending DTMF of this trunk. Default setting: rfc2833
DOD settings	DOD (Direct Outward Dialing) means the caller ID displayed when dialing out, before configure this, and please make sure the provider supports this feature.

7.2.2 Trunk Group

To route the call from GSM/UTMTS/CDMA trunk to VoIP trunk group, we can create trunk group in this page.

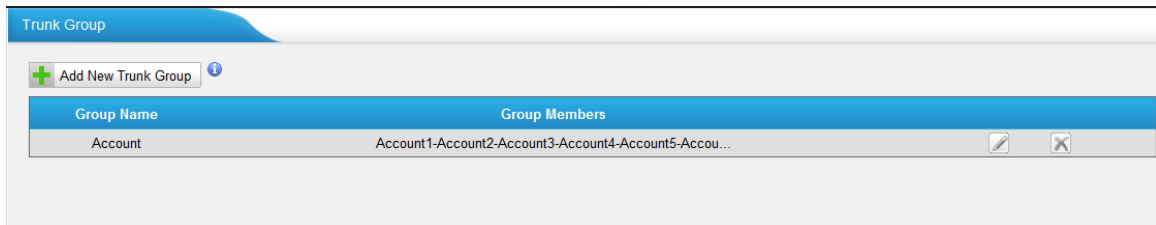


Figure 7-18

Click "Add New Trunk Group" to add a new one, or edit the default one. All the VoIP trunk will be listed here, we can choose the desired trunks to the right side as a group.

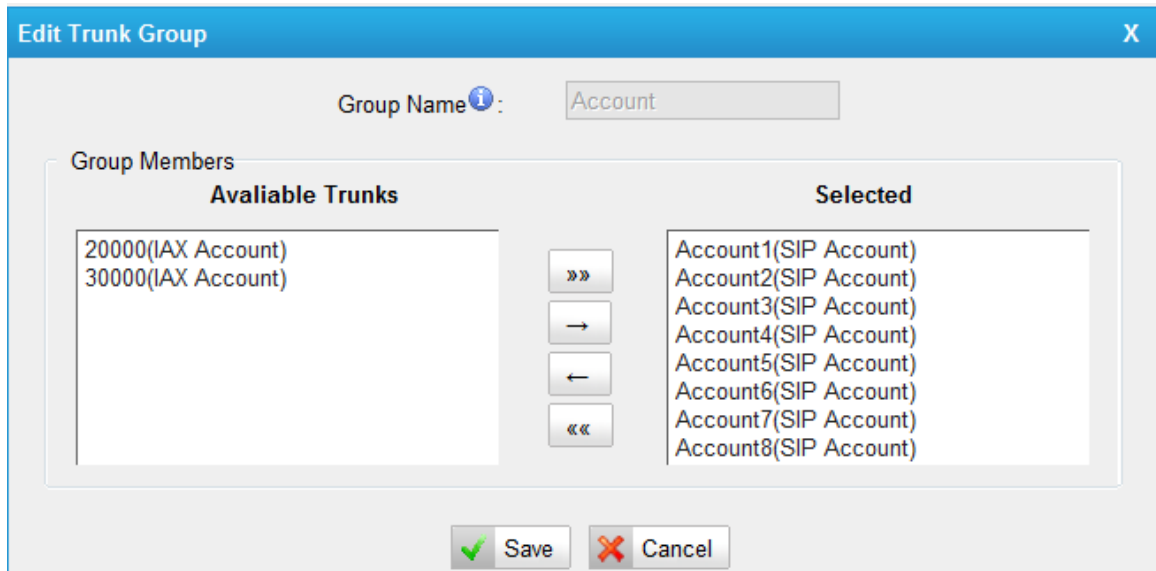


Figure 7-19

7.2.3 SIP Settings

This is the SIP settings in NeoGate, including General settings, NAT, Codecs, Qos, Response code and Advanced settings.

1) General

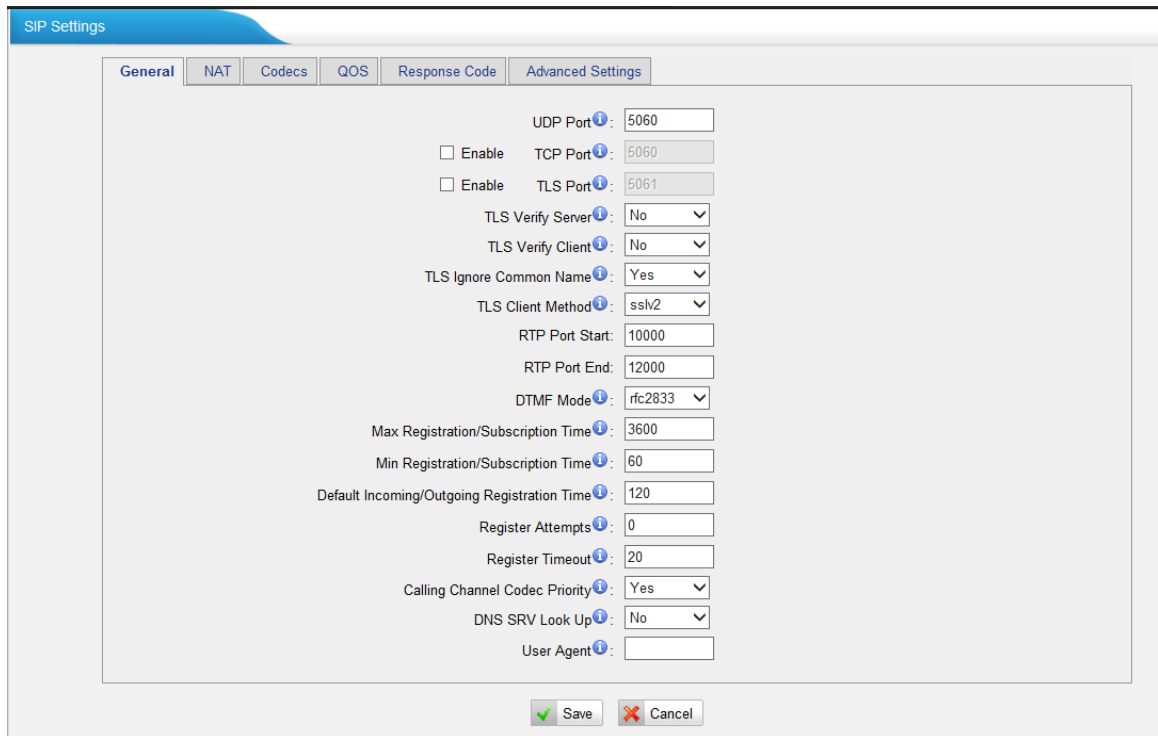


Figure 7-20

Items	Description
UDP Port	Port used for SIP registrations, Default is 5060
TCP Port	Port used for SIP registrations, Default is 5060
TLS Port	Port used for SIP registrations, Default is 5061
TLS Verify Server	When using NeoGate TG as a TLS client, whether or not to verify server’s certificate. It is “No” by default.
TLS Verify Client	When using NeoGate TG as a TLS server, whether or not to verify client’s certificate. It is “No” by default.
TLS Ignore Common Name	Set this parameter as “No”, then common name must be the same with IP or domain name.
TLS Client Method	When using NeoGate TG as TLS client, specify the protocol for outbound TLS connections. You can select it as tlsv1, sslv2 or sslv3.
RTP Port Start	Beginning of RTP port range
RTP Port End	End of RTP port range
DTMF Mode	Set default mode for sending DTMF. Default setting: rfc2833
Max Registration/Subscription Time	Maximum duration (in seconds) of a SIP registration. Default is 3600 seconds.
Min Registration/Subscription	Minimum duration (in seconds) of a SIP registration. Default is 60 seconds

Time	
Default Incoming/Outgoing Registration Time	Default Incoming/Outgoing Registration Time: Default duration (in seconds) of incoming/outgoing registration.
Register Attempts	The number of SIP REGISTER messages to send to a SIP Registrar before giving up. Default is 0 (no limit)
Register Timeout	Number of seconds to wait for a response from a SIP Registrar before timed out. Default is 20 seconds.
Calling Channel Codec Priority	Once enabled, when dialing out via SIP/SPS trunks, the codec of calling channel will be selected in preference. If not, NeoGate TG will follow the priority in your SIP/SPS trunks.
Video Support	Support for SIP video or no. Default is yes.
Max Bit Rate	Configure the max bit rate for video stream. The default: 384kb/s
DNS SRV Look Up	Please enable this option when your SIP trunk contains more than one IP address.
User Agent	To change the user agent parameter of asterisk, the default is "NeoGate TG", you can change it if needed.

2) NAT

Note: Configuration of this section is required when using remote extensions generally.

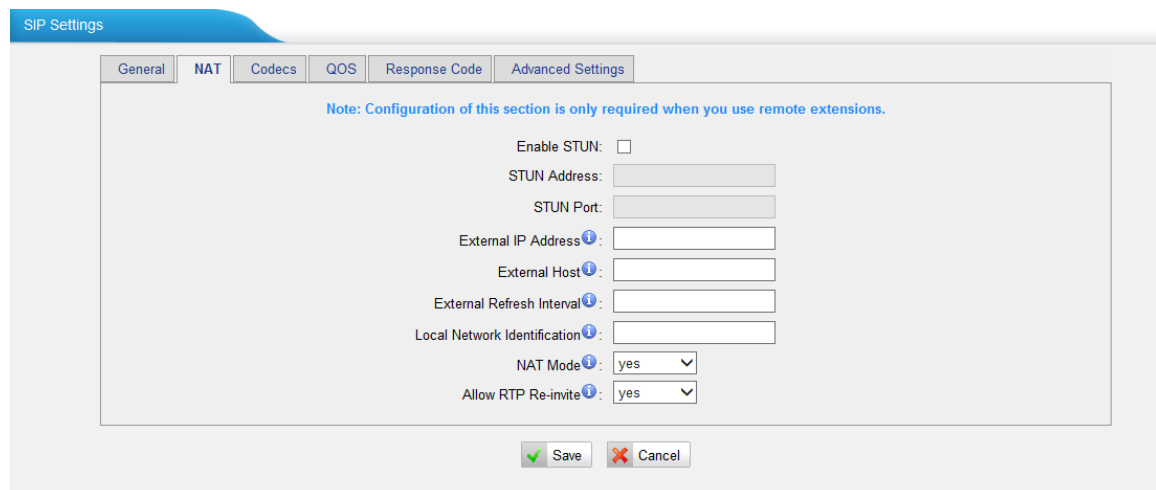


Figure 7-21

Items	Description
Enable STUN	STUN (Simple Traversal of UDP through NATs) is a protocol for assisting devices behind a NAT firewall or router with their packet routing.
STUN Address	The STUN server allows clients to find out their public address, the type of NAT they are behind and the internet side port

	associated by the NAT with a particular local port. This information is used to set up UDP communication between the client and the VOIP provider and so establish a call.
External IP Address	The IP address that will be associated with outbound SIP messages if the system is in a NAT environment.
External Host	Alternatively you can specify an external host, and the system will perform DNS queries periodically. This setting is only required when your public IP address is not static. It is recommended that a static public IP address is used with this system. Please contact your ISP for more information.
External Refresh Interval	Used to identify the local network using a network number/subnet mask pair when the system is behind a NAT or firewall. Some examples of this are as follows: "192.168.0.0/255.255.0.0": All RFC 1918 addresses are local networks; "10.0.0.0/255.0.0.0": Also RFC1918; "172.16.0.0/12": Another RFC1918 with CIDR notation; "169.254.0.0/255.255.0.0": Zero conf local network. Please refer to RFC1918 for more information.
NAT Mode	Global NAT configuration for the system; the options for this setting are as follows: Yes = Use NAT. Ignore address information in the SIP/SDP headers and reply to the sender's IP address/port. No = Use NAT mode only according to RFC3581. Never = Never attempt NAT mode or RFC3581 support. Route = Use NAT but do not include rport in headers.
Allow RTP Reinvite	By default, the system will route media streams from SIP endpoints through itself. Enabling this option causes the system to attempt to negotiate the endpoints to route packets to each other directly, bypassing the system. It is not always possible for the system to negotiate endpoint-to-endpoint media routing.

3) Codecs

We can choose the allowed codec in NeoGate TG, a codec is a compression or decompression algorithm that used in the transmission of voice packets over a network or the Internet. More information about codec, you can refer to this page: http://en.wikipedia.org/wiki/List_of_codecs

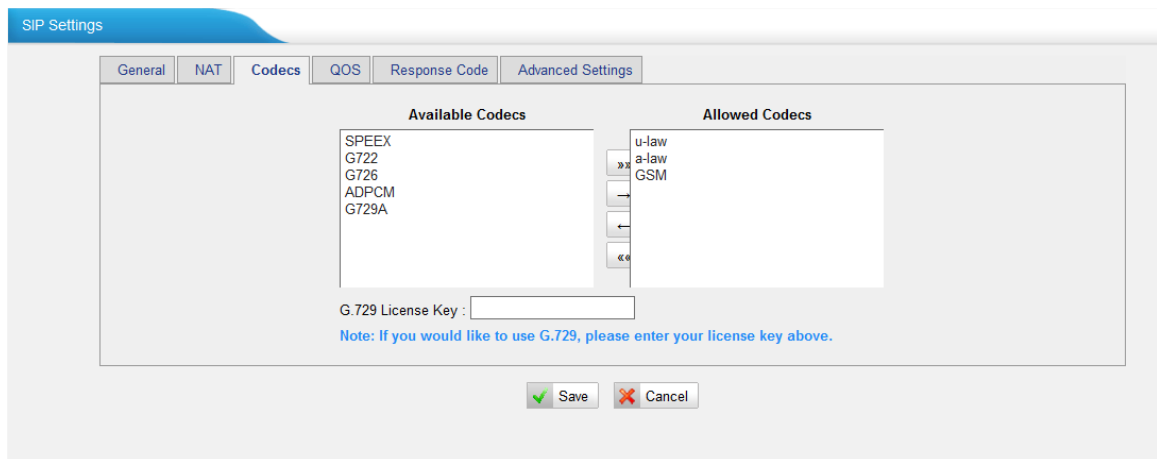


Figure 7-22

If you want to use codec G729, we recommend buying a license key and input it here.

4) QoS

QoS (Quality of Service) is a major issue in VoIP implementations. The issue is how to guarantee that packet traffic for a voice or other media connection will not be delayed or dropped due interference from other lower priority traffic. When the network capacity is insufficient, QoS could provide priority to users by setting the value.

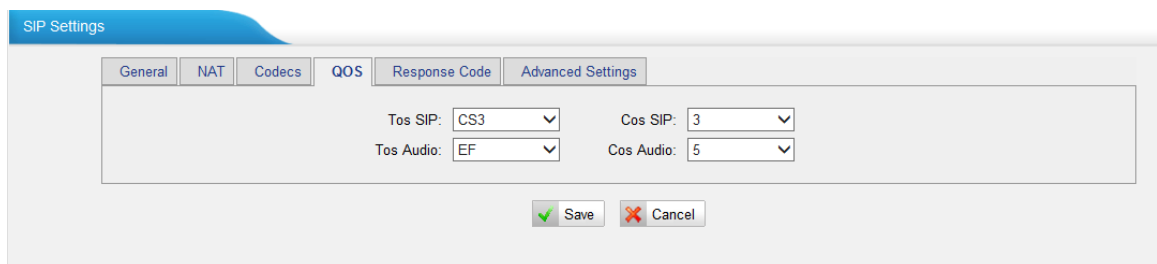


Figure 7-23

Note: It's recommended that you configure the QoS in your router or switch instead of NeoGate side.

5) Response Code

NeoGate supports to change the code from GSM/UTMTS/CDMA provider to the one you wanted before sending it back to your IPPBX, it helps the IPPBX understand better the exact call status, like busy, no response and others.

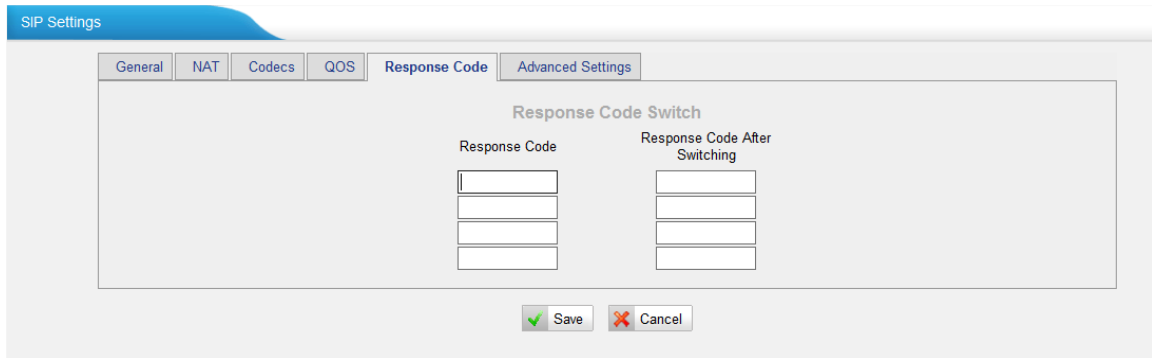


Figure 7-24

Note: We don't recommend configuring this if you are not familiar to the code of call status from mobile carrier and your IPPBX.

6) Advanced Settings

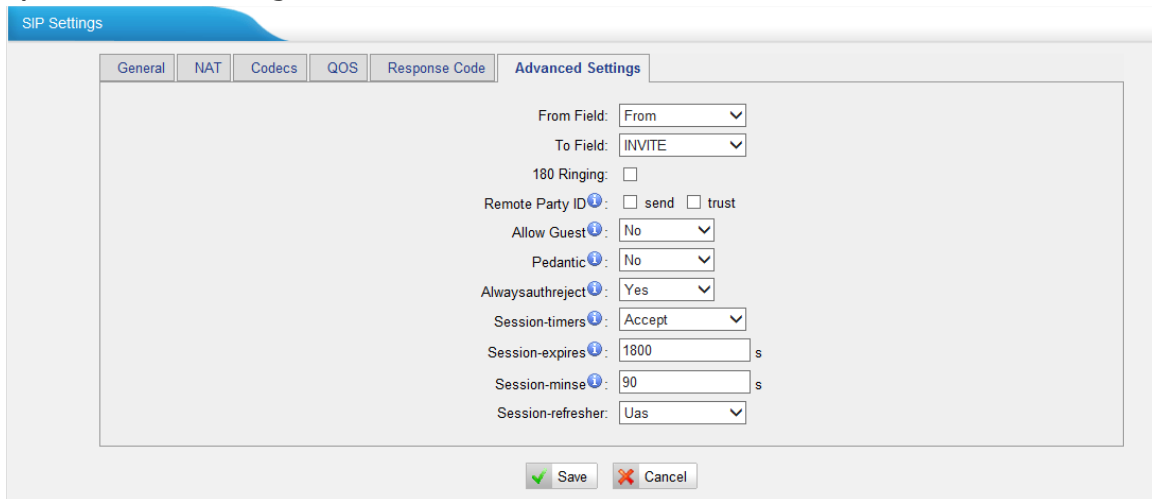


Figure 7-25

Items	Description
From Field	Where to get the caller ID in SIP packet
To Field	Where to get the DID in SIP packet
180 Ringing	It is set when the telecom provider needs. Usually it is not needed
Remote Party ID	Whether send Remote-Party-ID on SIP header. Default no.
Allow Guest	Whether allow anonymous registration extension. Default: no. It's recommended to be disabled for security.
Pedantic	Enable pedantic parameter. Default: no.
Alwaysauthreject	If enabled, when NeoGate TG rejects "Register" or "Invite" packets, NeoGate TG always respond the packets using "SIP404 NOT FOUND". It's recommended to be enabled for security.

Session -timers	Enable session-timer mode, default: yes. If you found the call is cut off every 15 minutes every time, please disable this.
Session-expires	The max refresh interval
Session-minse	The min refresh interval, which mustn't be shorter than 90s
Session-refresher	Choose session-refresher, the default is Uas

7.2.4 IAX Settings

IAX is the Internal Asterisk Exchange protocol, you can connect to NeoGate TG or register IAX trunk to another IAX server. It's supported by the asterisk-based IPPBX.

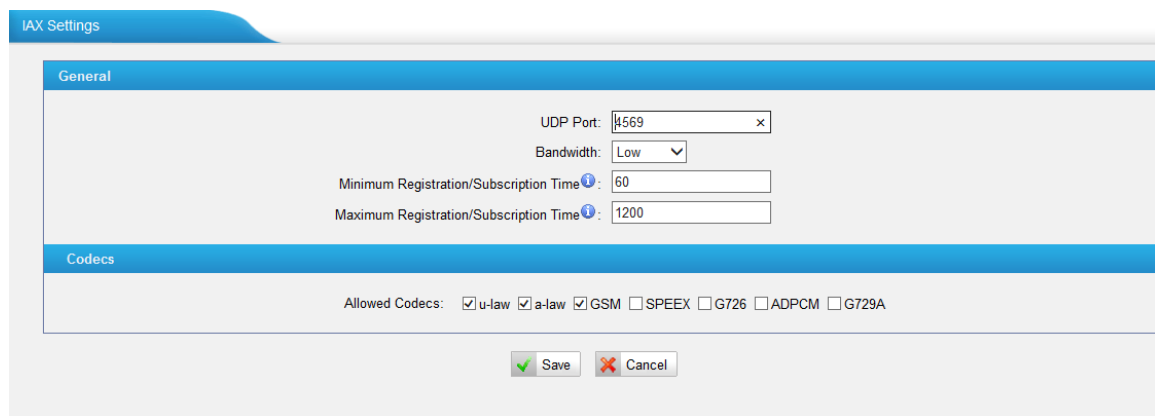


Figure 7-26

Items	Description
Bind Port	Port used for IAX2 registrations. Default is 4569.
Bandwidth	Low/medium/high with this option you can control which codec to be used.
Min Registration Time	Minimum duration (in seconds) of an IAX2 registration. Default is 60 seconds
Max Registration Time	Maximum duration (in seconds) of an IAX2 registration. Default is 1200 seconds.
Codecs	Enable the codec you want for IAX communication.

7.2.5 General Preferences

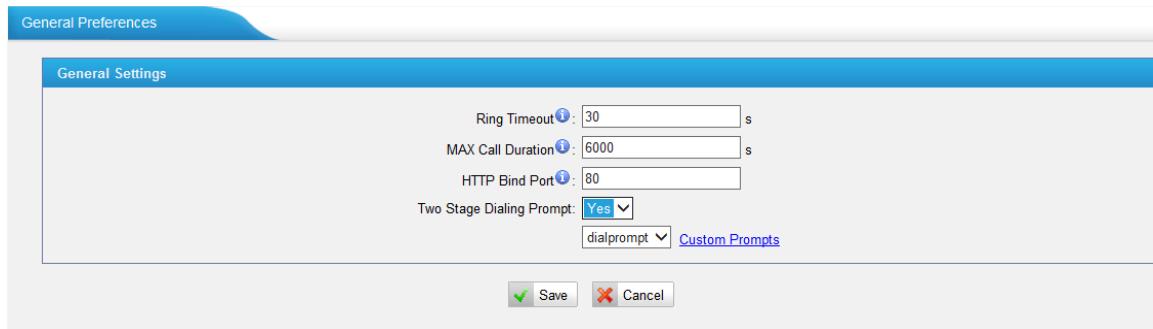


Figure 7-27

Items	Description
Ring Timeout	The global time out value for extensions, it's 30 by default.
MAX Call Duration	The global max call duration setting for all extensions, it's 6000 by default.
HTTP Bind Port	Port used for HTTP sessions; Default: 80. If you change this, please reboot to take effect.
Two Stage Dialing Prompt	Choose the customized two stage dialing prompt; it's disabled by default.

7.3 Routes Settings

To route the call to the correction destination, we should configure this page well, including the mobile to IP and IP to mobile settings.

7.3.1 Mobile to IP

This is the route page specifying how to route the calls from GSM/UTMTS/CDMA channel to IPPBX. There is a default route here, and we can create a new one or edit the old one. There are two modes for you to configure that.

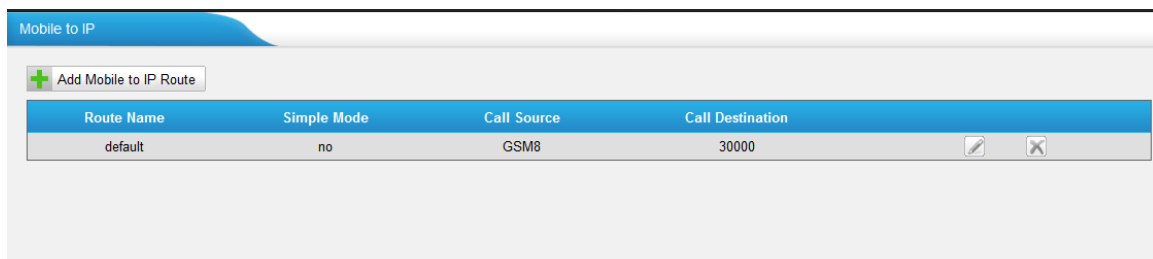


Figure 7-28

1) Simple Mode

Simple Mode *i*: Yes ▾

Route Name *i*: default

Match Incoming Calls:

Call Source Mobile -- GSM8 ▾

Incoming Calls Processing:

Call Destination: IAX Account -- 30000 ▾

Save Cancel

Figure 7-29

This is the simple mode. What we need to do is just choose the incoming source trunk and the destination trunk you want to route the call to, NeoGate will allow all incoming calls and route it to the destination trunk without any modification.

2) Advanced route

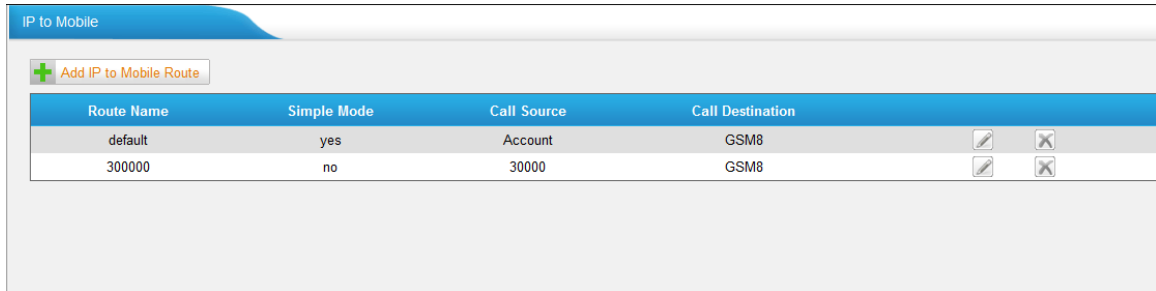
Figure 7-30

When simple mode is set as “No”, you can check the advanced settings.

Items	Description
Route name	A name for this route
Call Source	Choose the trunk where incoming call comes from
Inbound caller pattern	Match the prefix of caller ID for incoming calls. Hover the pointer over to read tips.
Enable Callback	Choose whether call back is enabled, you can configure the advanced call back settings in part: 7.3.4.
Call Destination	Choose the destination trunk to route the call to
Hotline	When it’s configred, this number will be dial via destination trunk permanently
Outbound Dial Pattern	Outbound calls that match this dial pattern will use this outbound route. Hover the pointer over to read tips.
Strip digits from front before dialing	Allow the user to specify the number of digits that will be stripped from the front of the phone number before the call is placed.
Prepend these digits before dialing	These digits will be prepended to the phone number before the call is placed

7.3.2 IP to Mobile

This is the route page specifying how to route the calls from VoIP trunk to GSM/UTMTS/CDMA channel. There is a default route here, and we can create a new one or edit the old one. There are two modes for you to configure that also.

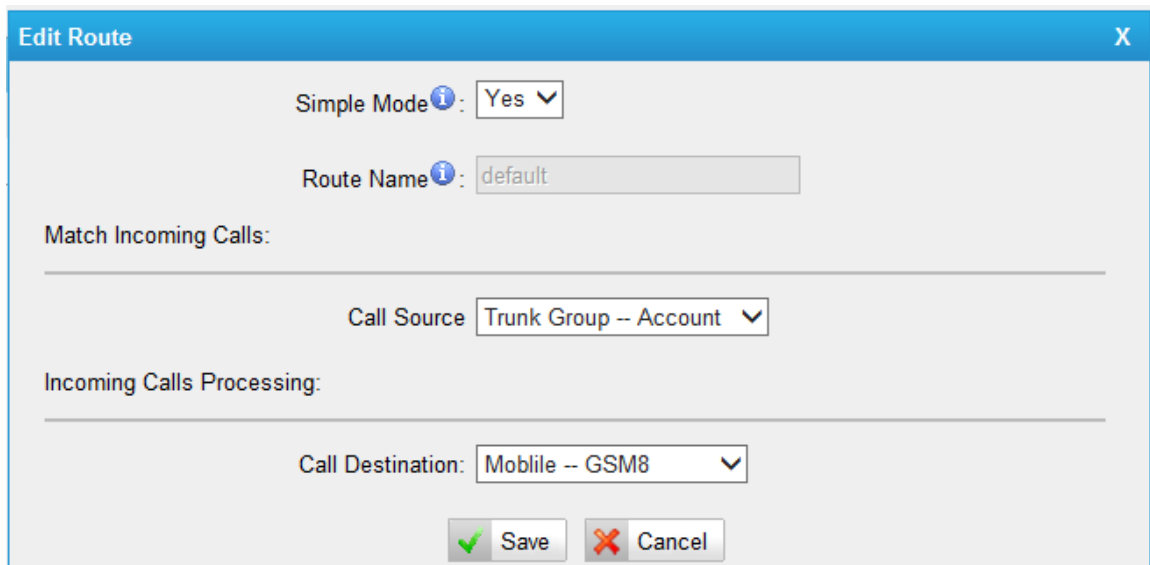


Route Name	Simple Mode	Call Source	Call Destination		
default	yes	Account	GSM8		
300000	no	30000	GSM8		

Figure 7-31

1) Simple Mode

This is the simple mode. What we need to do is just choose the incoming source trunk and the destination trunk you want to route the call to, NeoGate will allow all incoming calls and route it to destination trunk without any modification.



Edit Route [X]

Simple Mode ⓘ: Yes ▾

Route Name ⓘ: default

Match Incoming Calls:

Call Source: Trunk Group -- Account ▾

Incoming Calls Processing:

Call Destination: Mobile -- GSM8 ▾

Save Cancel

Figure 7-32

2) Advanced mode

Figure 7-33

When simple mode is set as “No”, you can check the advanced settings.

Items	Description
Route name	A name for this route
Call Source	Choose the trunk where incoming call comes from
Inbound caller pattern	Match the prefix of caller ID for incoming calls. Hover the pointer over ⓘ to read tips.
DID number	Define the expected DID Number if this trunk passes DID on incoming calls. Leave this field blank to match calls with any or no DID info. You can also use pattern matching to match a range of numbers.
DID Associated Number	Define the extension for DID number. You can only input number and “-” in this field, and the format can be xxx or xxx-xxx. The count of the number must be only one or equal the count of the DID number

Enable Callback	Choose whether call back is enabled, you can configure the advanced call back settings in part: 7.3.4.
Call Destination	Choose the destination trunk to route the call to
Hotline	When it's configred, this number will be dial via destination trunk permanently
Two stage Dial	Enable it to get the customized two stage dial tone before dial out, it's disabled by default.
Outbound Dial Pattern	Outbound calls that match this dial pattern will use this outbound route. Hover the pointer over ⓘ to read tips.
Strip digits from front before dialing	Allows the user to specify the number of digits that will be stripped from the front of the phone number before the call is placed.
Prepend these digits before dialing	These digits will be prepended to the phone number before the call is placed

7.3.3 Blacklist

Blacklist is used to block an incoming/outgoing call. If the number of incoming/outgoing call is listed in the number blacklist, the caller will hear the following prompt: "The number you have dialed is not in service. Please check the number and try again". The system will then disconnect the call.

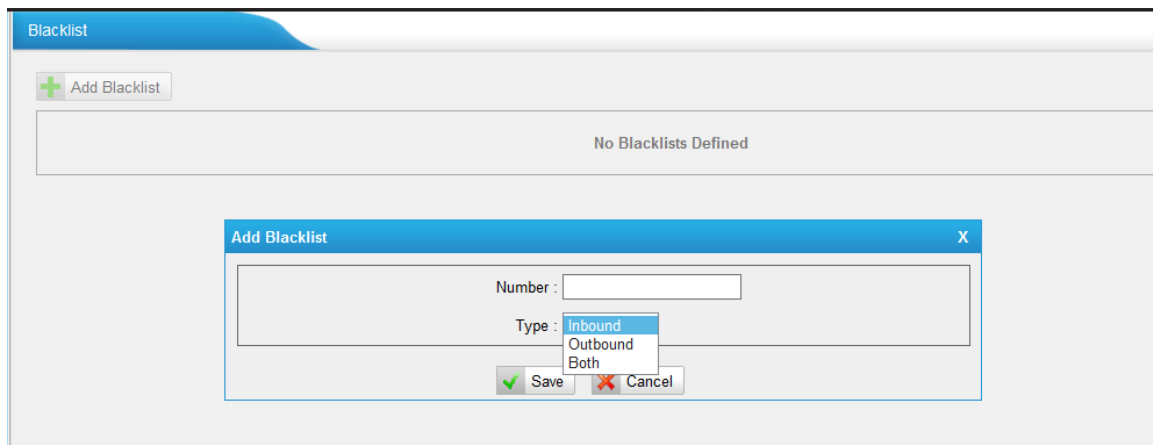


Figure 7-34

We can add a number with the type: inbound, outbound or both.

7.3.4 Callback Settings

NeoGate TG allows caller A to dial an inbound route number, and after hearing the ring, A can hang up the call or wait for NeoGate TG to cut off the call, then

NeoGate TG will call A with this number. When A picks up the call, A can dial the number he wants to call; NeoGate TG will route this call to destination trunk.

Notes:

1. If you'd like to use callback feature, please make sure it's enabled on the "Mobile to IP" or "IP to Mobile" setting panel.
2. No callback rules needed to be set if the trunk supports call back with the caller ID directly.

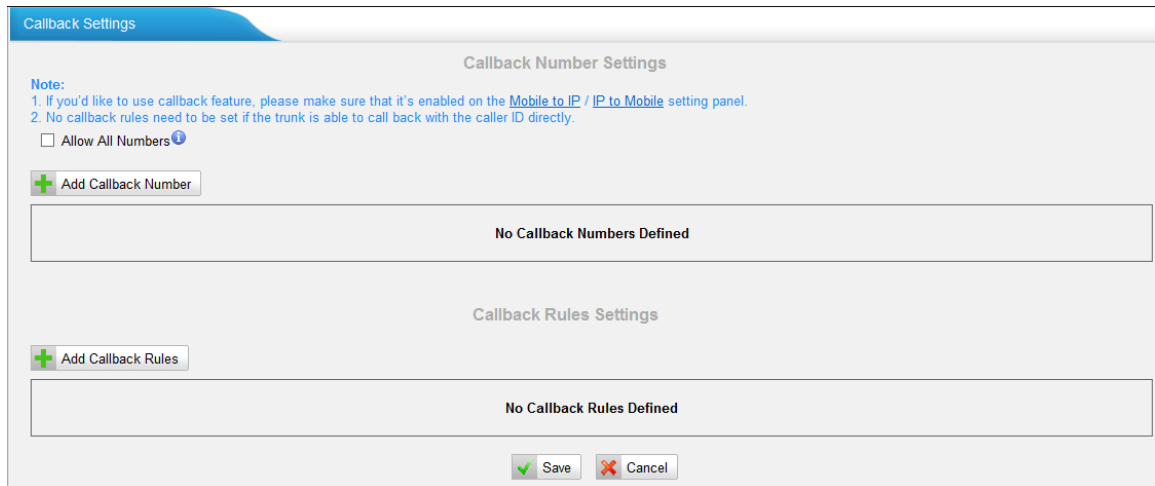


Figure 7-35

If you want to apply Callback function to all incoming numbers, please tick Allow All numbers.

Follow the step to use this function.

Step 1: Enable Callback.

On the "mobile to IP" or "IP to Mobile" setting panel—Choose "Yes" on "Enable Callback" to enable this function.

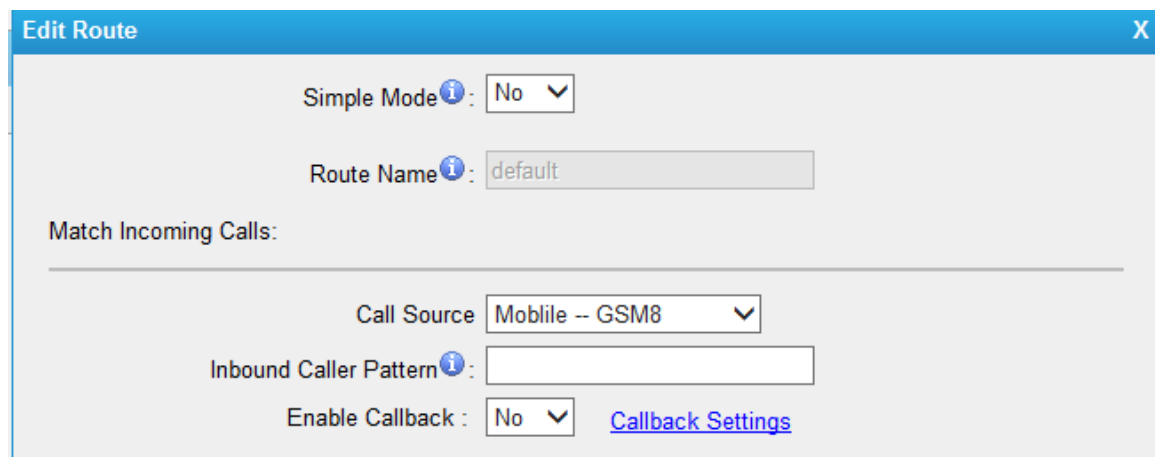


Figure 7-36

Step 2: Create Callback number

Figure 7-37

Step 3: Create Callback Rules

You will need to create callback rules when the system should strip or add digits.

Figure 7-38

Items	Description
Trunk Name	Choose the trunk with callback rules
Strip digits from front	Define how many digits will be stripped from the call in number before the callback is placed.
Prepend before dialing	Define digits added before a callback number before the callback is placed

8 Applications

Application 1



Figure 8-1

Application 2



Figure 8-2

[Finish]