NeoGate

TG200
User Manual

Version 5.10.0.87

Well

Table of Contents

1. Introduction

NeoGate-GSM Gateway for Maximum Efficiency & Cost Savings

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

1.1 Features

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

1.2 Hardware Specification

1.2.1 Exterior Appearance

1) Front Side

Figure 1-1 NeoGate Front Panel Picture

No.	Identifying
①Power	Green shining: Connected, correct function. Green flashing: Device error. No light: Disconnected, malfunction.
②RUN	Green Light: Indicates the server system is in working order
③Ready	Green Light: Indicates the system is ready.
④Port2	Red Light: stands for GSM port LED – Red and Green (fast blink): GSM port is in talking.
⑤Port1	Red Light: stands for GSM port LED – Red and Green (fast blink): GSM port is in talking.

2) Back Side

Figure 1-2 NeoGate Back Side Picture

2. System set up

2.1 SIM Card Placement

Lift off the SIM card holder on the backside, insert the SIM card and replace the holder, securing the latch.

Note1: Remember to set call forwarding, call barring, preferential network(s), SMS centre and similar provider and SIM card services in your mobile phone before inserting the SIM card in NeoGate.

Note2: Disconnect NeoGate from the power supply before inserting the SIM cards.

2.2 Antenna Connection

NeoGate is equipped with two antenna connector for all the GSM modules. The external antenna should always be installed vertically 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 the connection process, and a green LED indicates the port is properly connected.

2.4 Power Supply Connection

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

AC Input: 100~240V

DC Output: 12V,1A

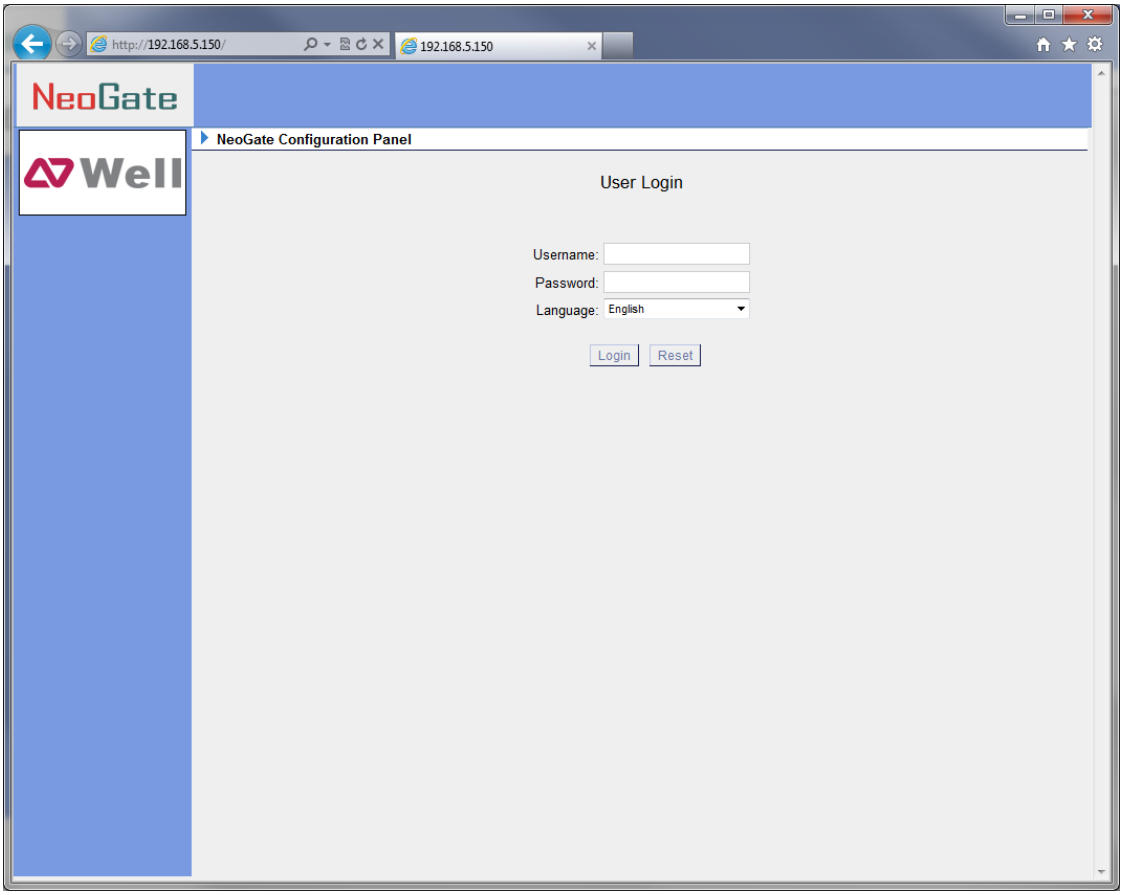
Please follow the steps below to connect the NeoGate unit to a power outlet:

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. NeoGate Configuration

3.1 Manager Login

From your web browser, input the IP address of the NeoGate server.
If this is the first time you are configuring NeoGate, please use the default settings below:
IP Address: http://192.168.5.150
Username: admin
Password: password



3.2 GSM Settings

3.2.1 Module List

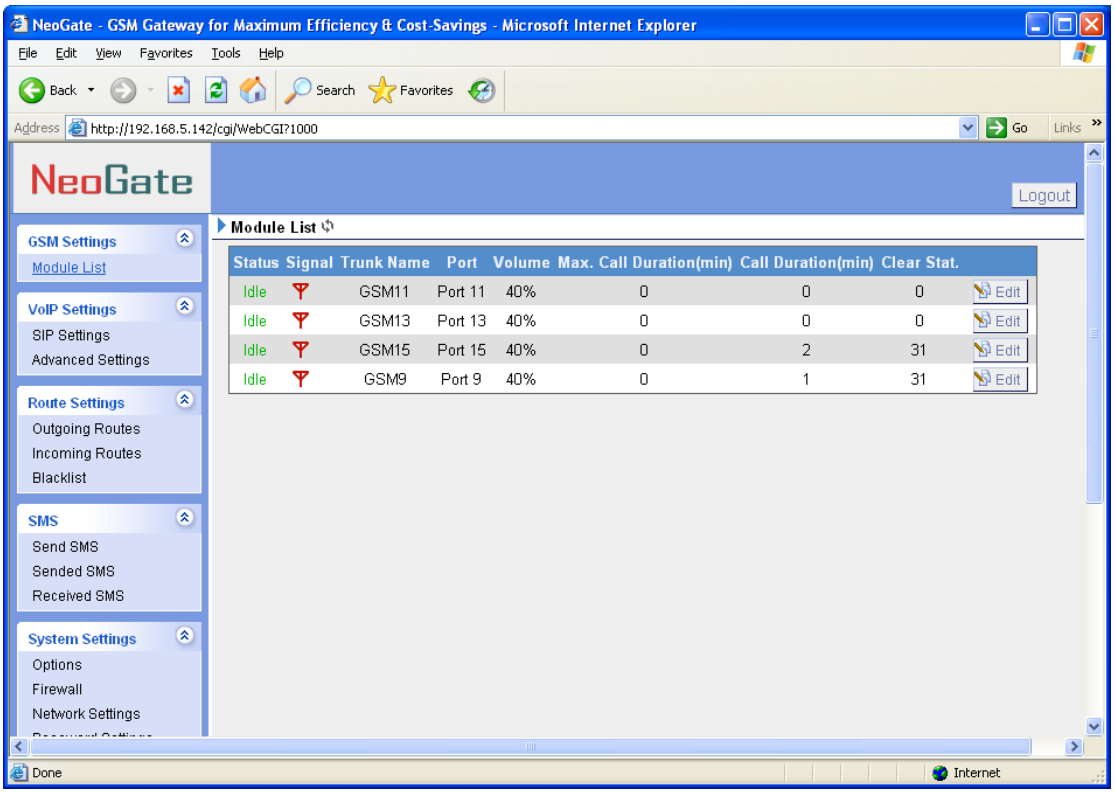


Figure 3-2

NeoGate Status Description:

Status

Idle: The port is idle.

Busy: The port is in use.

Error: The port has not inserted the SIM Card.

Signal

: No signal.

: Poor.

: Average.

: Good.

: Excellent.

3.2.2 GSM Settings

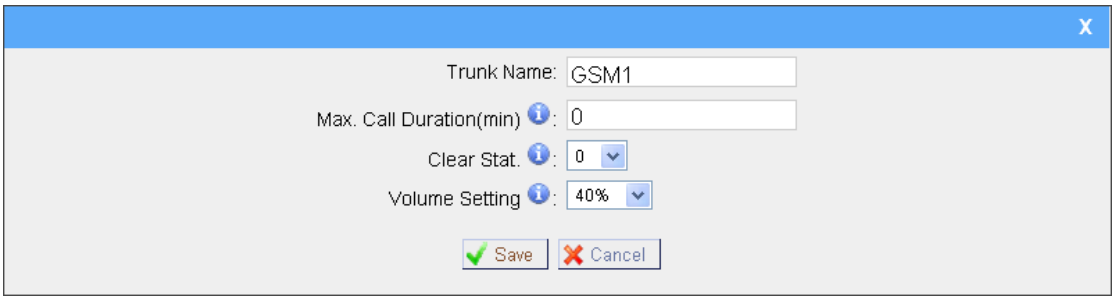


Figure 3-3

Trunk Name: A name of this Trunk. Ex: 'GSM1' etc.
Max. Call Duration (min)/Per Month: Defines the maximum call duration within a month through this SIM card. (0 it means unlimited)
Clear Stat: Set the day in a month, in this day system will automate reset the SIM card's Max Call Duration to 0 min, (if selected 0, it means disable this functions)
Volume Setting: Define the volume of this GSM Trunk.

3.3 VoIP Settings

3.3.1 SIP Settings

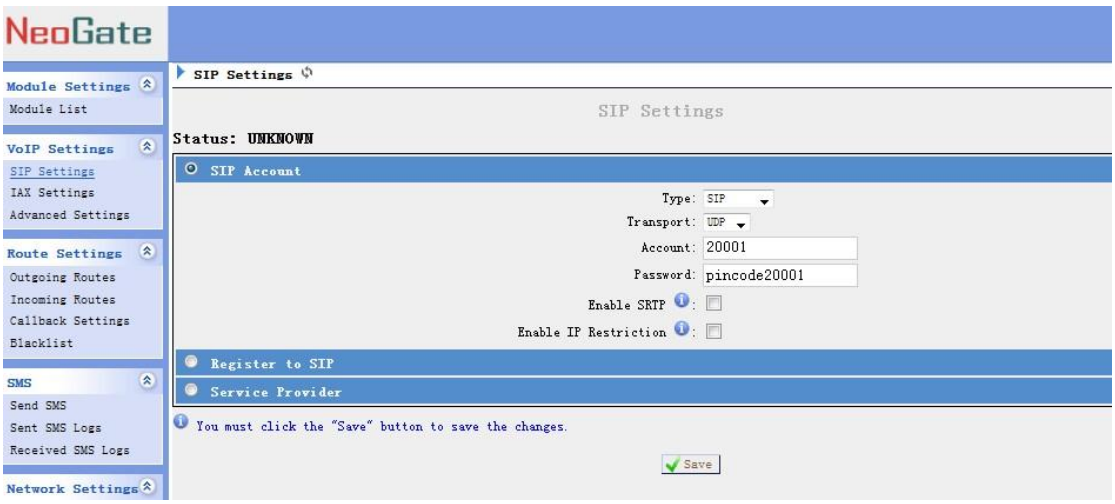


Figure 3-4

3.3.1.1 SIP Account

It is an SIP Account that allows an IP Phone, IP Soft- Phone client, IPPBX and soft switch to register on NeoGate.

·Type

Choose the type(SIP, IAX, SIP/IAX)

·Transport

Choose the protocol of the transport(UDP, TCP and TLS).

·Account

The numbered extension, i.e. 1234, that will be associated with this particular User / Phone.

·Password

The password for this extension, Ex: '12t3f6'.

·Enable SRTP

Enable SRTP for this account.

·Enable IP Restriction

Enable the restriction function .

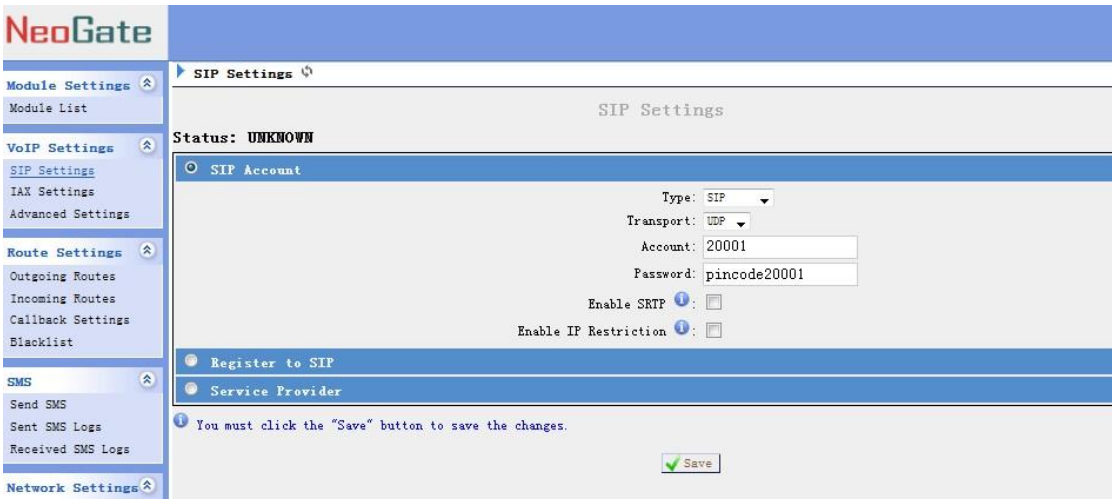


Figure 3-5

3.3.1.2 Register to SIP

'Register to SIP', It use to register to SIP Server or SIP Proxy.

·Type

Choose the type(SIP, IAX)

·Transport

Choose the protocol of the transport(UDP, TCP and TLS).

·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.

·Username

Username of SIP account. Used for SIP trunk registration.

.Authorization name

Used for SIP authentication. Leave this blank if not required.

·Password

Password of SIP account.

.From User

All outgoing calls from this SIP Trunk will use the From User (In this case the account name for SIP Registration) in From Header of the SIP Invite.

.Online number

Define the online number that expected by 'Skype Connect' and some other SIP service providers. Leave this field blank if it's no required.

·Outbound Proxy Server

A proxy that receives requests from a client, even though which may not be the server resolved by the Request-URI.

·Enable SRTP

Enable SRT

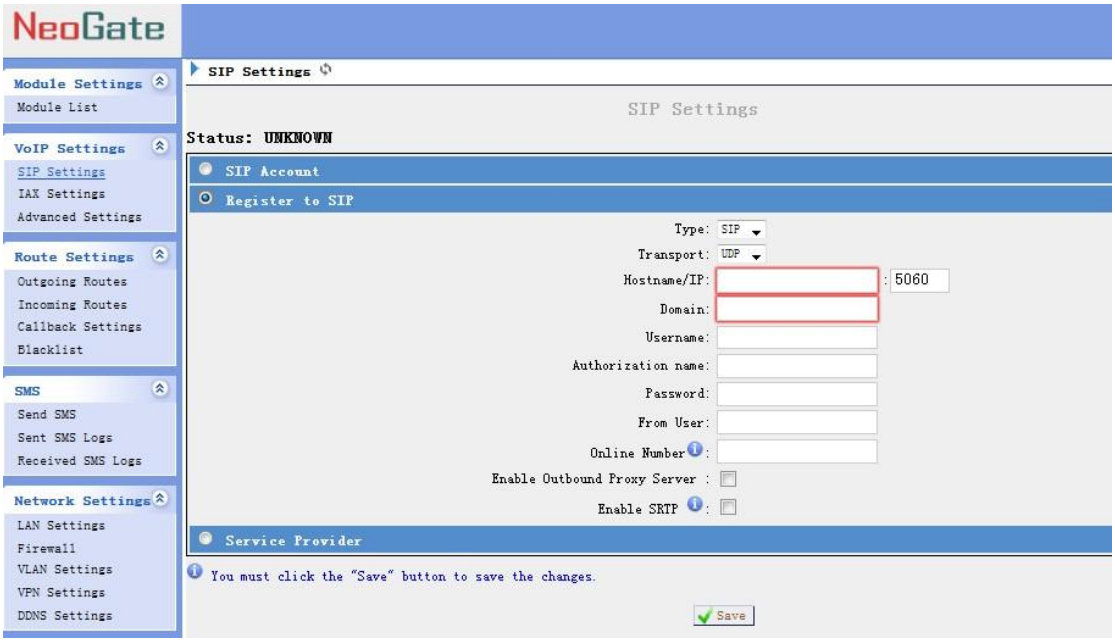


Figure 3-6

3.3.1.3 Service Provider

·Type

Choose the type(SIP, IAX)

·Transport

Choose the protocol of the transport(UDP, TCP and TLS).

·Hostname/IP

Service provider's hostname or IP address.

Note: 5060 is the standard port number used by SIP protocol. Don't change this part if it is not required.

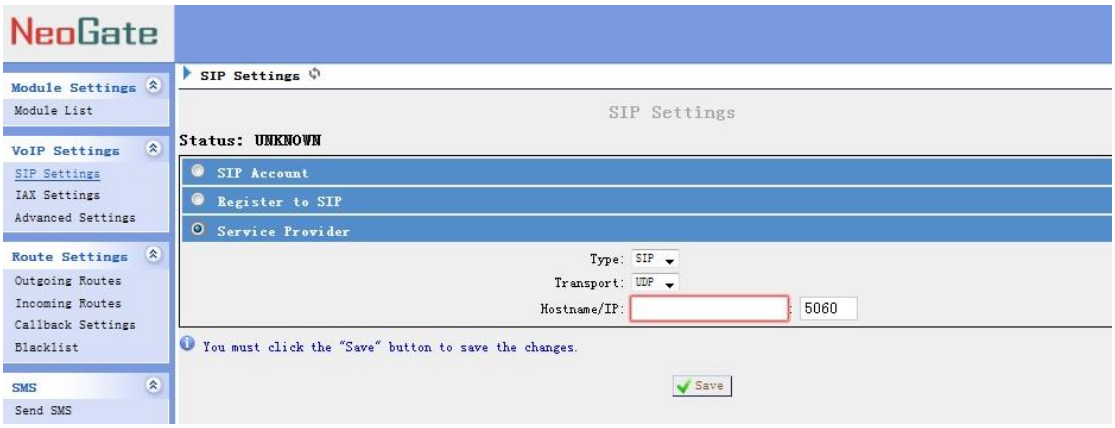


Figure 3-7

3.3.2 IAX Settings

1) General

·Bind Port

The port used for IAX

·Bandwidth

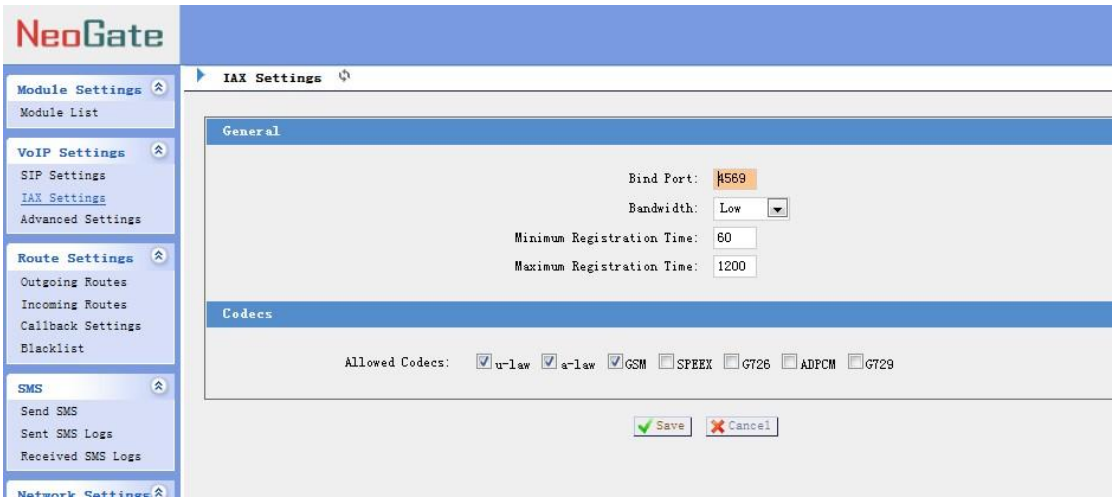
Choose the Bandwidth(Low, Medium, High)

·Minimum Registration Time

·Maximum Registration Time

1) Codecs

Tick the Codecs allowed.



3.3.3 Advanced Settings

1) General

·UDP Port

Port use for sip registrations, Default is 5060.

·TCP Port
Port use for sip registrations, Default is 5060.

·TLS Port
Port use for sip registrations, Default is 5061.

·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 Time
Minimum duration (in seconds) of a SIP registration. Default is 60 seconds.

·Default Incoming/Outgoing Registration Time
Default Incoming/Outgoing Registration Time: Default is 30 seconds.

·Register Attempts
The number of SIP REGISTER messages to send to a SIP Registrar before giving up. Default is 4 (no limit).

·Register Timeout
Number of seconds to wait for a response from a SIP Registrar before timed out. Default is 20 seconds.

·Max. Channels
Control the maximum number of outbound channels (simultaneous calls) that can be used. Inbound calls are not counted against the maximum.

2) NAT
Note: Configuration of this section is only required when using remote extensions.

·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 be used with this system. Please contact your ISP for more information.

·External Refresh Interval

If an external host has been supplied, you may specify how often the system will perform a DNS query on this host. This value is specified in seconds.

·Local Network Identification

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 report in headers.

·Allow RTP Reinvite

By default, the system will route media steams 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）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.

4）Codecs

A codec is a compression or decompression algorithm that used in the transmission of voice packets over a network or the Internet.

u-law: A PSTN standard codec, used in North America, that provides very good voice quality and consumes 64kbit/s in each direction (receiving and transmitting) of a VoIP call.

a-law: A PSTN standard codec, used outside of North America, that provides very good voice quality and consumes 64kbit/s in each direction (receiving and transmitting) of a VoIP call.

GSM: A wireless standard codec, used worldwide, that provides adequate voice quality and consumes 13.3kbit/s in each direction (receiving and transmitting) of a VoIP call. GSM is supported by many VoIP phones.

SPEEX: SPEEX is an Open Source/Free Software patent-free audio compression format designed for speech. The SPEEX Project aims to lower the barrier of entry for voice applications by providing a free alternative to expensive proprietary speech codec. Moreover, SPEEX is well-adapted to Internet applications and provides useful features that are not present in most other codec.

G.726: A PSTN codec, used worldwide, that provides good voice quality and consumes 32kbit/s in each direction (receiving and transmitting) of a VoIP call. G.726 is supported by some VoIP phones.

ADPCM, G.729.

Note: If you would like to use G.729, please enter your license.

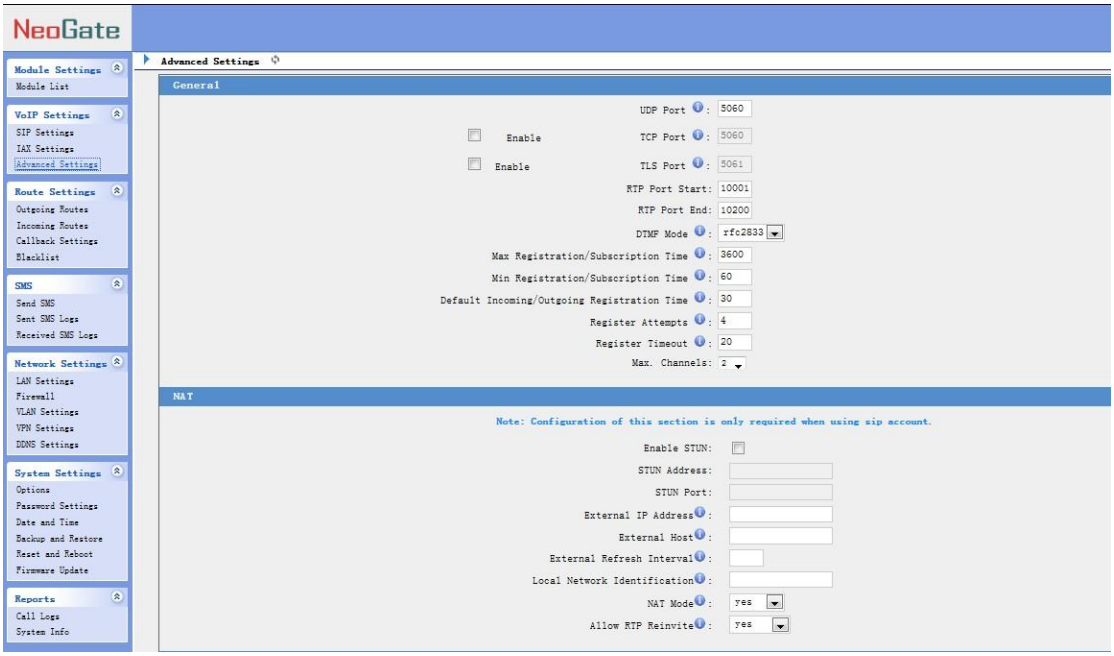


Figure 3-8

3.4 Route Settings

3.4.1 Outgoing Routes

Outbound routing mainly works for guides outgoing calls to go through trunks.

Click 'New Outbound Route' and fill in the corresponding information in the popup window.

1）General

·Route Name

Name of this Outbound Route. ex: 'Local' or 'Long Distance' etc.

·Dial Pattern

Outbound calls that match this dial pattern will use this outbound route. There are a number of dial pattern characters that have special meanings:

X : Any Digit from 0-9

Z : Any Digit from 1-9

N : Any Digit from 2-9

[12345-9] : Any digit in the brackets (in this example, 1,2,3,4,5,6,7,8,9)

The '**.**' Character will match any remaining digits. For example, 9011. will match any phone number that starts with 9011, excluding 9011 itself.

The '**!**' will match any remaining digits, and causes the matching process to complete as soon as it can be determined that no other matches are possible.

Example 1: **NXXXXXX** will match any 7 digits phone number.

Example 2: **1NXXNXXXXX** will match a phone number starting with a 1, followed by a 3-digit area code, and then 6 digit number.

·Strip

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. For example, if users must press 0 before dialing a phone number, one digit should be stripped from the dial string before the call is placed.

·Prepend these digits before dialing

These digits will be prepended to the phone number before the call is placed. For example, if a trunk requires 10 digit dialing, but users are more comfortable with 7 digit dialing, this field could be used to prepend a 3 digit area code to all 7 digit phone numbers before calls are placed. When using analog trunks, a 'w' character may also be prepended to provide a slight delay before dialing.

·Direct Number

All the outgoing calls through this route will call to this phone number directly.

·Strategy

Define the strategy to select trunk.
Default: Select the trunk from the first.
Sequence: Select the trunk next the last used.
Balance: Select the trunk last recently used.

·Time

The scope of time which is allowed to make calls via this route.

·Days of week

The days in a week when is allowed to make calls via this route.

·Generate Virtual Ring

The system can generate the virtual ring when you use this route.

·Member Trunks

Define the trunks that can be used for this outbound route.

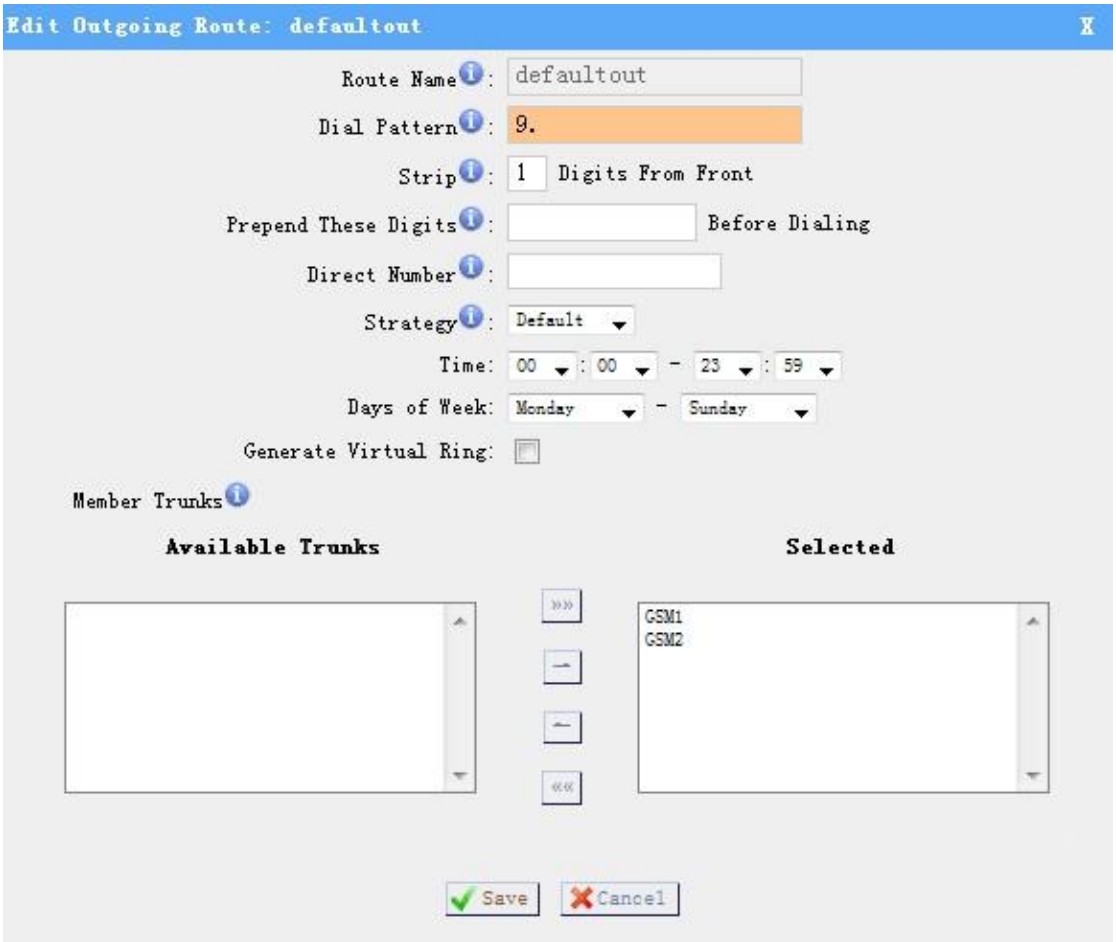


Figure 3-9

3.4.2 Incoming Routes

Inbound routing processes incoming call traffic to destination during office hours or outside office hours.

1）General

·Route Name

A name of this inbound route. ex: 'callin' etc.

·Caller ID Number

Define the Caller ID Number to be matched on incoming calls. Leave this field blank to match any or no CID info.

You can also use a pattern match (e.g. 2[345]X) to match a range of numbers. The following patterns may be used:

X : Any Digit from 0-9

Z : Any Digit from 1-9

N : Any Digit from 2-9

[12345-9] : Any digit in the brackets (in this example, 1,2,3,4,5,6,7,8,9)

The '**.**' Character will match any remaining digits. For example, 9011. will match any phone number that starts with 9011, excluding 9011 itself.

The '**!**' will match any remaining digits, and causes the matching process to complete as soon as it can be determined that no other matches are possible.

Example 1: **NXXXXXX** will match any 7 digits phone number.
Example 2: **1NXXNXXXXX** will match a phone number starting with a 1, followed by a 3-digit area code, and then 6 digit number.

·Direct Number
All the incoming calls through this route will call to this phone number directly.
Note: Only 'SIP Settings' use 'Register to SIP' and 'Service Provider' mode can support this function.
·Auto Callback
You can enable the auto callback function here.

2) Member Trunks
This area allows you to select which trunks will be member trunks for this route. To make a trunk a member of this route, please move it to the 'Selected' box.

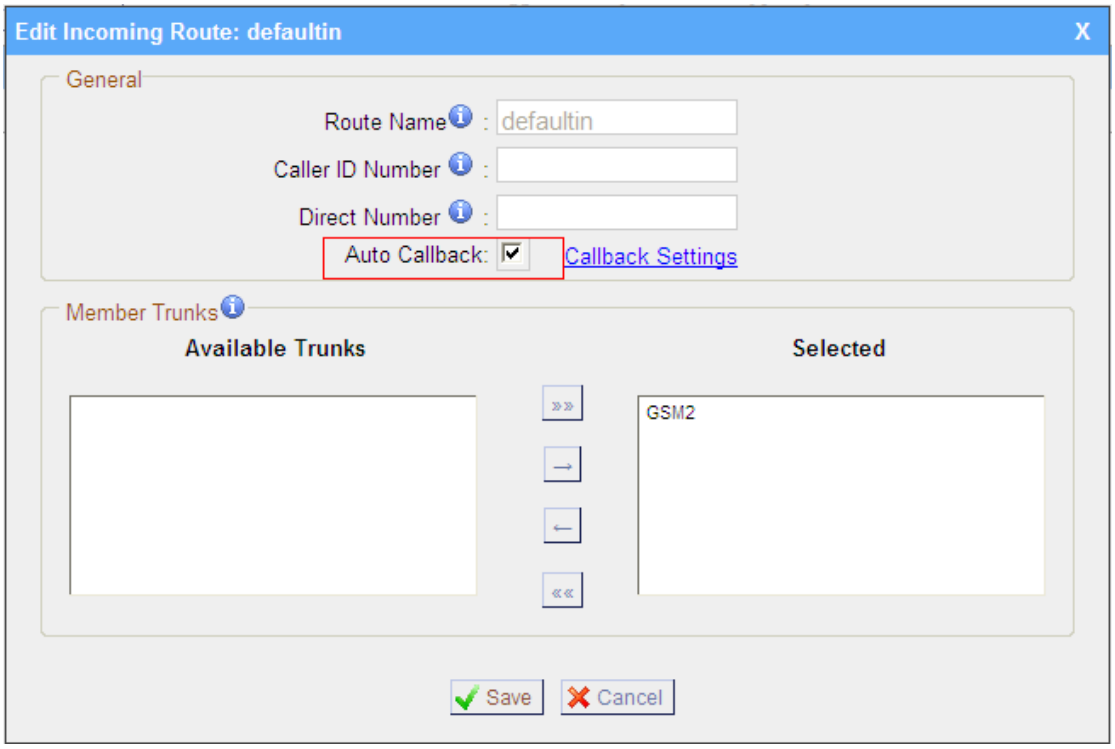


Figure 3-10

3.4.3 Callback Settings

NeoGate allows caller A to dial the number of the SIM card inserted in NeoGate, and after hearing the ring back tone, A can hang up the call or wait for NeoGate to cut off the call, then NeoGate will call A with this SIM card. When A pick up the

call, A can dial the number he wants to call; NeoGate will forward this call to SIP server.

If user wants to use this function, please follow those steps.

Step1: **Enable Auto Callback**.

Incoming Routes -> Tick Auto Callback and choose the trunk.

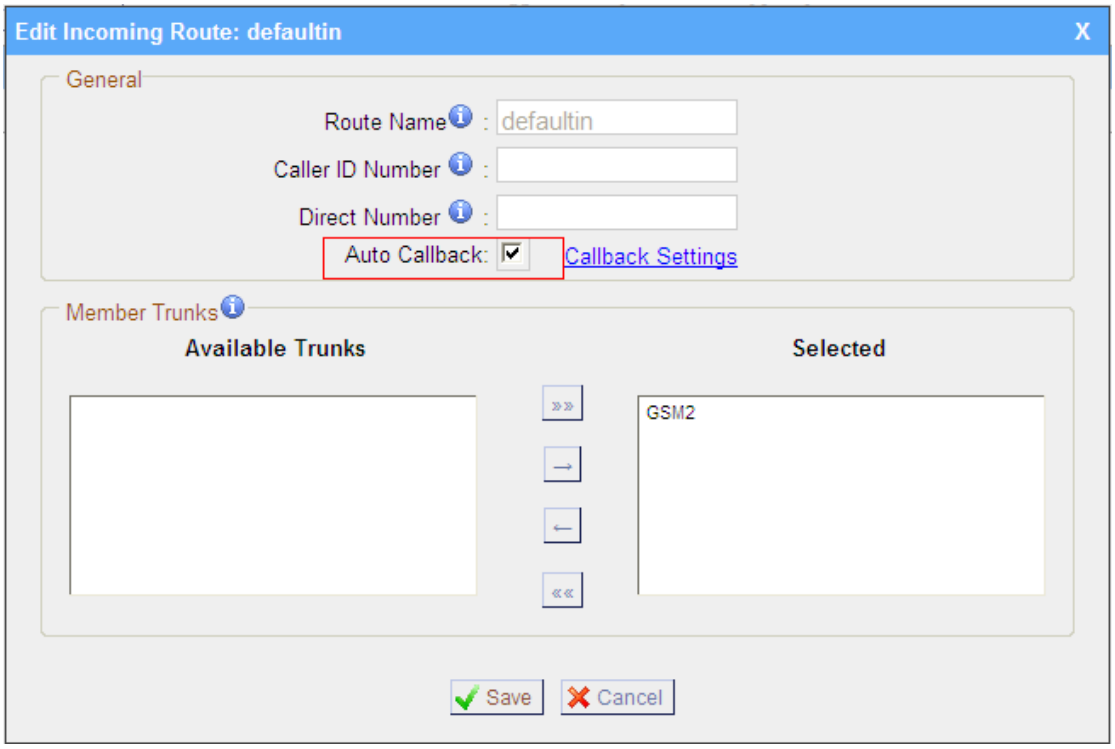


Figure 3-11

Step2: Configure the Callback number

Callback Settings -> Click 'New Callback number', and fill in the phone number in the pop-up windows.

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

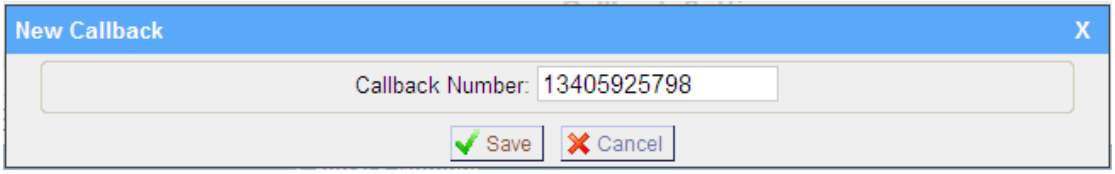


Figure 3-12

Step3: Test.

In this case, configure the SIP Settings as the picture below.

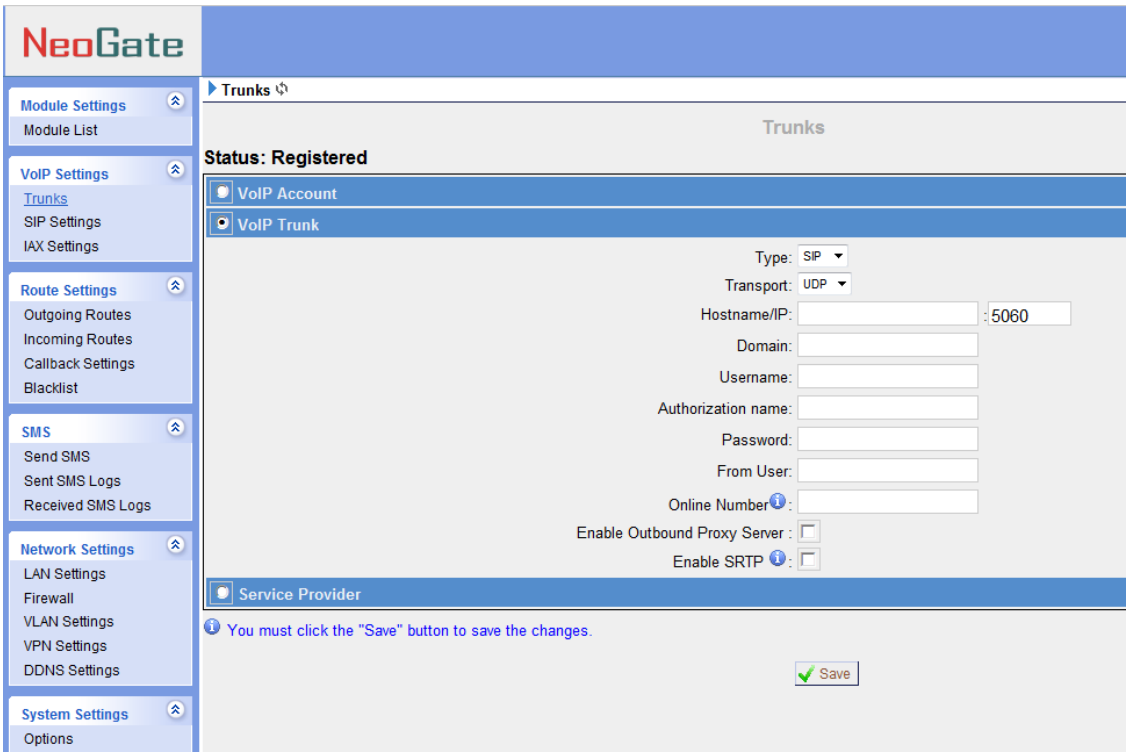


Figure 3-13

Test:

Use mobile phone (whose number is 13405925798 which has already been added in the call back number) to call the SIM card inserted in the NeoGate. After hanging up the call, NeoGate will use SIM card to call user's mobile phone number. You pick up the call and then you can dial the number you want to call.

Note: Please ensure that the SIP account you set with NeoGate would allow you to call out directly.

3.4.4 Blacklist

Number Blacklist is used to block an incoming call you do not want to answer and block outgoing call.

If the incoming call or outgoing call number is registered in the number blacklist, the caller will hear the following: "The number you have dialed is not in service. Please check the number and try again". The system will then disconnect the call.

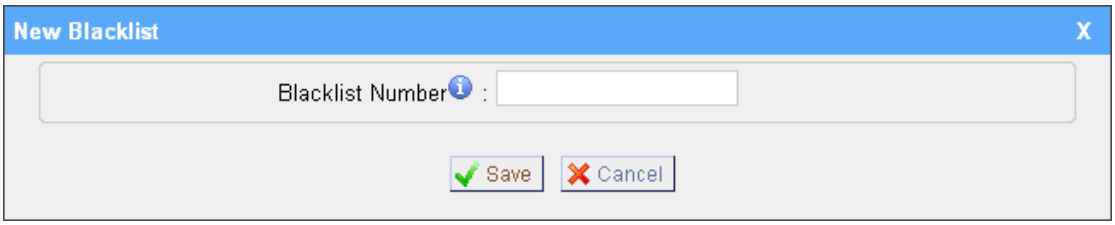


Figure 3-14

3.5 SMS

3.5.1 Send SMS

Users can send the SMS in this page.
Note: Please select corresponding Calling Code when sending SMS. If the Calling Code isn't available in the list, please input it before the Destination Number. The format is: Country Code + Destination Number. (e.g.:In '861380592xxxx','86' is the Calling Code of China, and '1380592xxxx' is Destination Number.)
Calling Code: please select corresponding Calling Code when sending SMS. If the Calling Code isn't available in the list, please input it before the Destination Number.
Destination: destination number.
Port: the port use to send SMS.
Content: content use to send out. (Max character is 300).

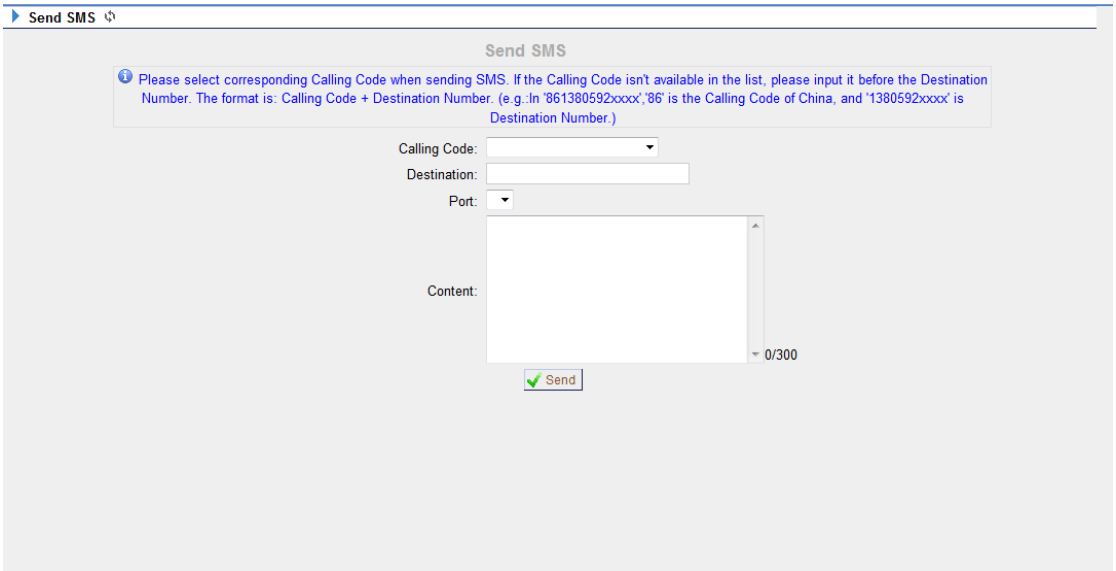


Figure 3-15

3.5.2 Sent SMS Logs

The Sent SMS logs capture all sent SMS details, including Account, Port, Destination, Time and Content.
Note: the maximum amount of messages sent that can be saved are 500.

3.5.3 Received SMS Logs

The Received SMS logs capture all received SMS details, including Port, From, Time and Content.

Note: The maximum amount of messages received that can be saved are 500.

3.6 Network Settings

3.6.2 LAN Setting

·DHCP
If this option is set, NeoGate will use DHCP to get an available IP address from your local network. Not recommended.

·Enable SSH
This is the advance way to access the device, you can use the putty software to access the device. In the SSH access, you can do more advance setting and debug.

·Port: the default is 8022,

·Hostname
Set the host name for NeoGate.

·IP Address
Set the IP Address for NeoGate.

·Subnet Mask
Set the subnet mask for NeoGate.

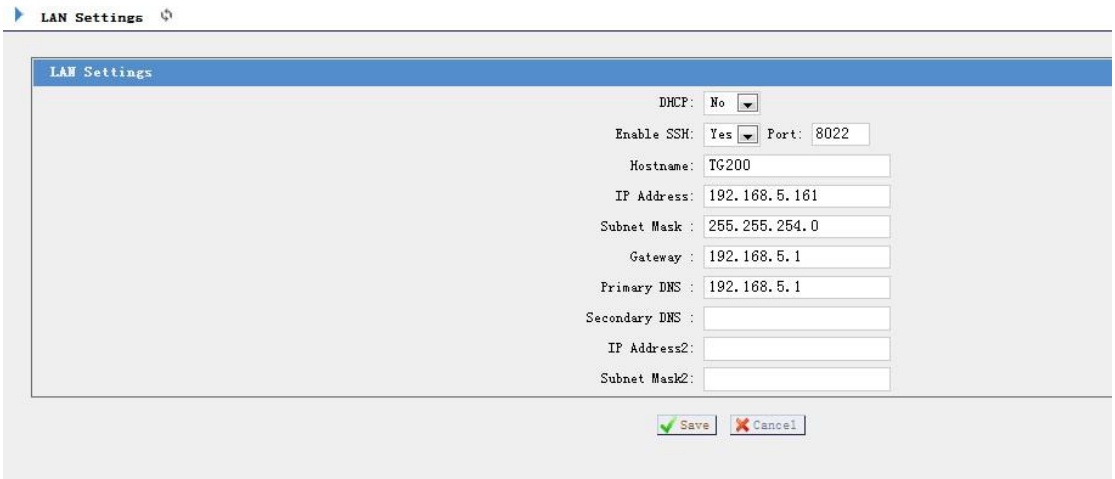
·Gateway
Set the gateway for NeoGate.

·Primary DNS
Set the primary DNS for NeoGate.

·Secondary DNS
Set the secondary DNS for NeoGate.

·IP Address2
Set the 2nd IP Address for NeoGate.

·Subnet Mask2
Set the 2nd subnet mask for NeoGate.



3.6.2 Firewall

Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

1) Enable Firewall

Enable the firewall to protect the device.

2) Common Rules

·Name

A name of this rule, e.g. 'HTTP'.

·Description

Simple description for this rule. eg: Accept the specific host to access the web interface for configuration.

·Protocol

The protocols of 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: 216.207.245.47/255.255.255.255 for ip 216.207.245.47

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.

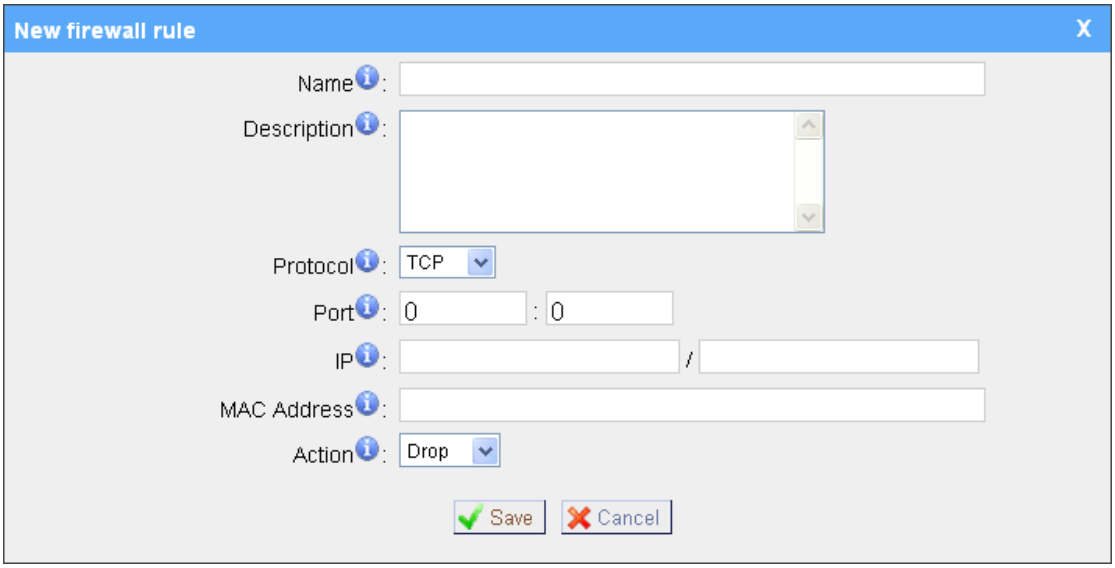


Figure 3-17

3) Auto Defense

·Port

Auto defense port, e.g.: 8022.

·Protocol

Auto defense protocol, TCP or UDP.

·Rate

The maximum packets or connections can be handled per unit time.
E.g.: (Port: 8022 Protocol: TCP Rate: 10/minute) means maximum 10 TCP connection to port 8022 can be handled per minute, the eleventh connection will be refused directly.

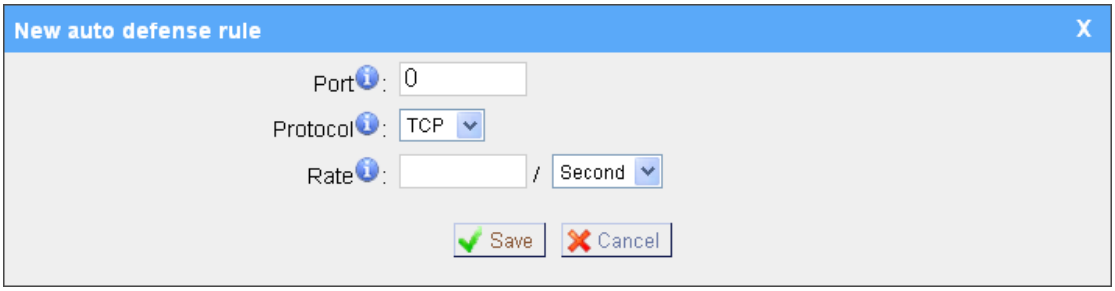


Figure 3-18

4) SIP Defense

·Port

The port used for SIP protocol.

·Protocol

Choose the protocol need to be protect, etc: UDP.

·SIP Packets

The SIP packets allowed in specific time interval.

·Time Interval

The time interval to receive SIP packets.

For example, SIP packets 90, time interval 60 means 90 SIP packets are allowed in 60 seconds.

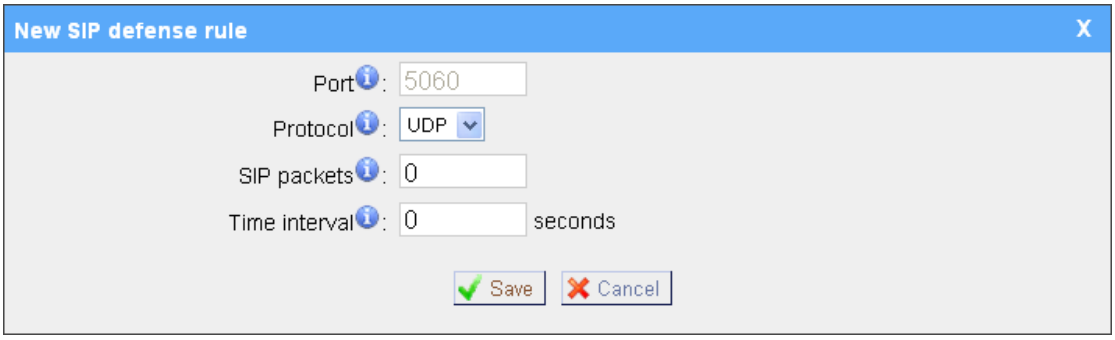


Figure 3-19

5) Other Settings

·Disable Ping

Enable this item, net ping from remote hosts will be dropped.

·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.

3.6.3 VLAN Settings

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

NeoGate supports 2 VLANs

·VLAN Number

.The VLAN Number is a unique value you assign to each VLAN on a single device.

·VLAN IP Address

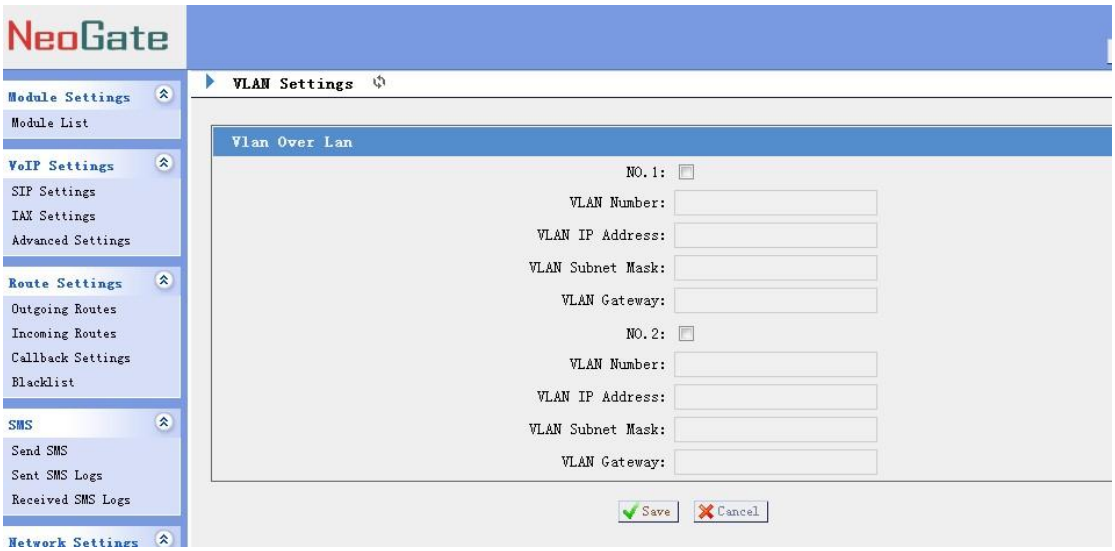
Set the IP Address for NeoGate VLAN.

·VLAN Subnet Mask

Set the Subnet Mask for NeoGate VLAN.

·VLAN Gateway

Set the Gateway for NeoGate VLAN.



3.6.4 VPN Settings

You can import VPN configuration file in Neogate to take advantage of VPN.

3.6 Network Settings

3.6.1 Options

1) General

·Ring Timeout

Number of seconds to ring a device before answering. Default value is 30s.

.MAX Call Duration

The absolute maximum amount of time permitted for a call. A setting of 0 disables the timeout. Default value is 6000s.

·HTTP Bind Port/Web Access Port

Port use for HTTP sessions. Default: 80

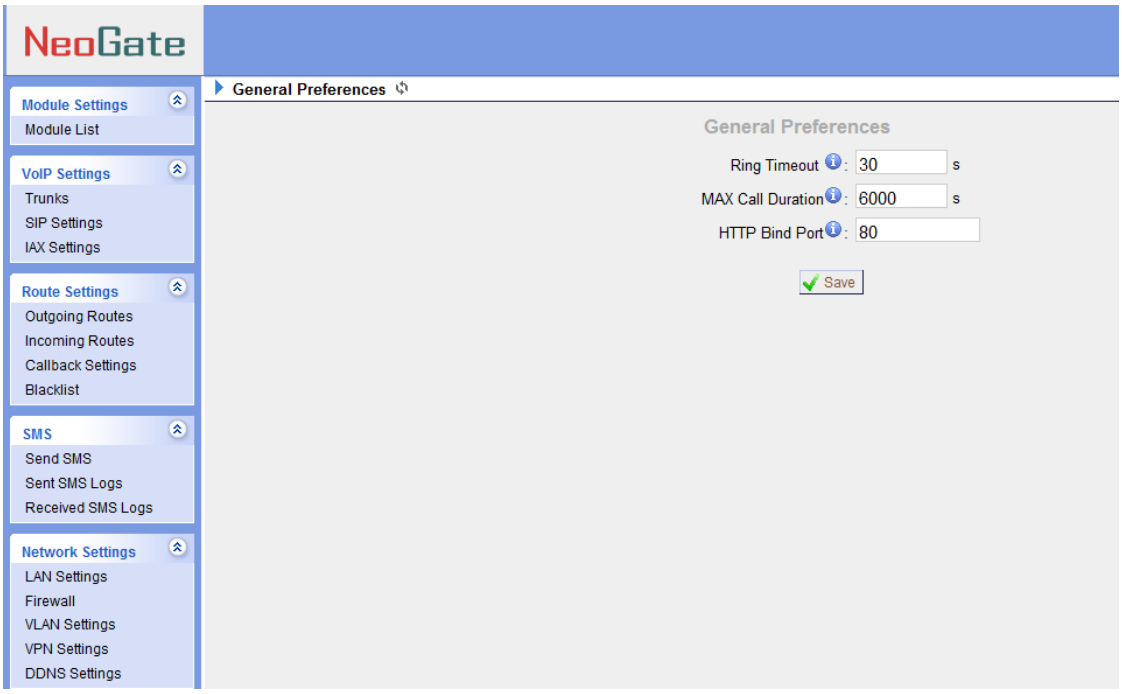


Figure 3-16

3.6.2 Firewall

Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified

security criteria.
1) Enable Firewall
Enable the firewall to protect the device.

2) Common Rules
·Name
A name of this rule, e.g. 'HTTP'.

·Description
Simple description for this rule. eg: Accept the specific host to access the web interface for configuration.

·Protocol
The protocols of 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: 216.207.245.47/255.255.255.255 for ip 216.207.245.47
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.

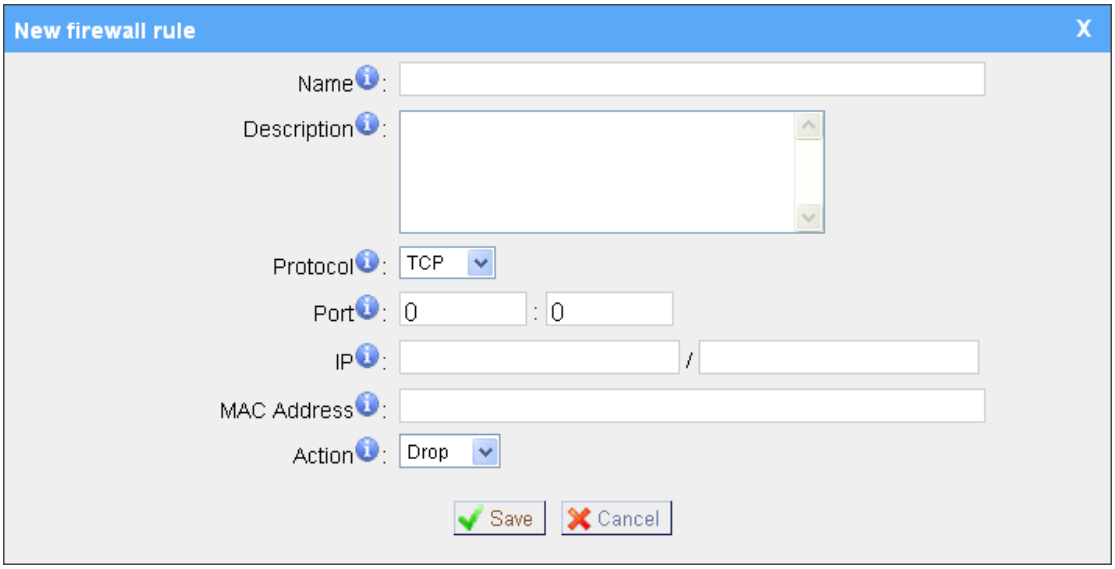


Figure 3-17

3) Auto Defense

·Port

Auto defense port, e.g.: 8022.

·Protocol

Auto defense protocol, TCP or UDP.

·Rate

The maximum packets or connections can be handled per unit time.

E.g.: (Port: 8022 Protocol: TCP Rate: 10/minute) means maximum 10 TCP connection to port 8022 can be handled per minute, the eleventh connection will be refused directly.

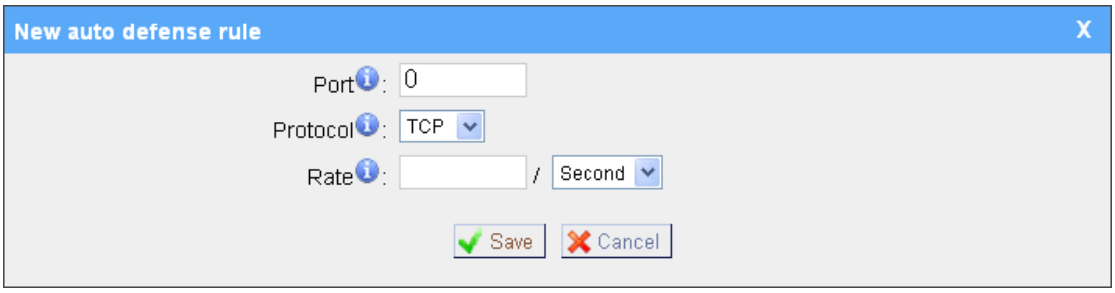


Figure 3-18

4) SIP Defense

·Port

The port used for SIP protocol.

·Protocol

Choose the protocol need to be protect, etc: UDP.

·SIP Packets

The SIP packets allowed in specific time interval.

·Time Interval

The time interval to receive SIP packets.

For example, SIP packets 90, time interval 60 means 90 SIP packets are allowed in 60 seconds.

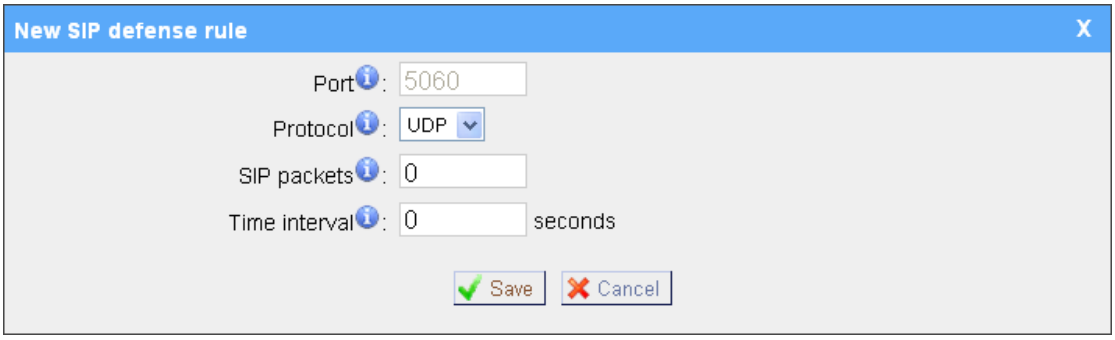


Figure 3-19

5) Other Settings

·Disable Ping

Enable this item, net ping from remote hosts will be dropped.

·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.

3.6.3 Network Setting

1) LAN

·DHCP

If this option is set, NeoGate will use DHCP to get an available IP address from your local network. Not recommended.

·Enable SSH

This is the advance way to access the device, you can use the putty software to access the device. In the SSH access, you can do more advance setting and debug.

·Port: the default is 8022,

·Hostname

Set the host name for NeoGate.

·IP Address
Set the IP Address for NeoGate.

·Subnet Mask
Set the subnet mask for NeoGate.

·Gateway
Set the gateway for NeoGate.

·Primary DNS
Set the primary DNS for NeoGate.

·Secondary DNS
Set the secondary DNS for NeoGate.

2) Advanced Settings
A VLAN is a logical local area network (or LAN) that extends beyond a single traditional LAN to a group of LAN segments, given specific configurations.
·IP Address2 and Subnet Mask2
.Configure second IP Address and Mask in this text, NeoGate can use this ip address access to another network.

·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 VLAN.

·VLAN Subnet Mask
Set the Subnet Mask for NeoGate VLAN.

·VLAN Gateway
Set the Gateway for NeoGate VLAN.

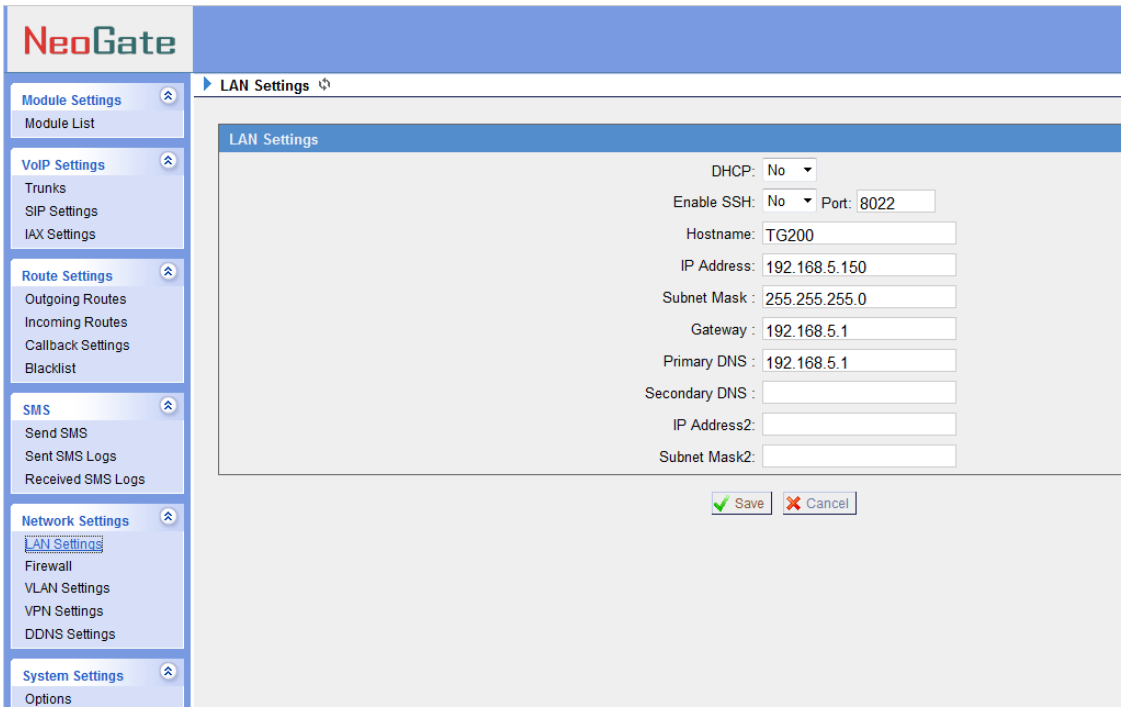


Figure 3-20

3.6.4 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.

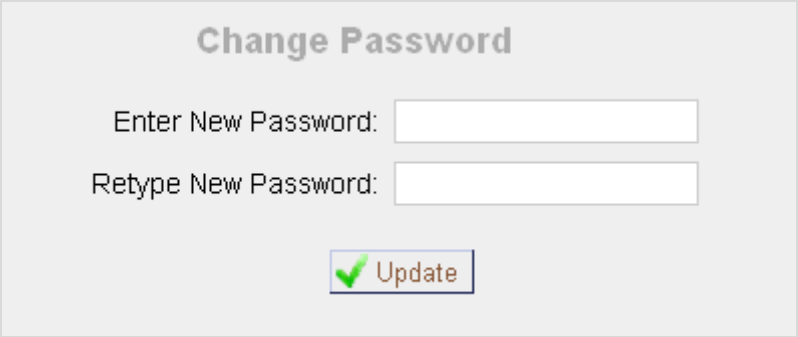


Figure 3-21

3.6.5 Date and Time

Set the date and time for NeoGate.

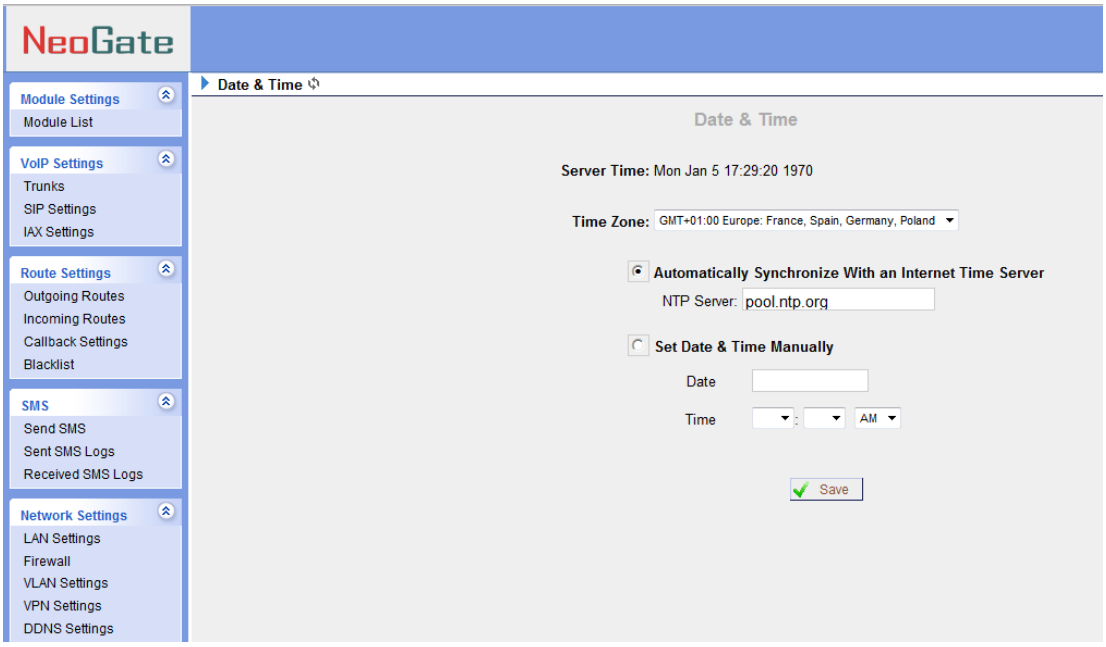


Figure 3-22

3.6.6 Backup and Restore

You can backup your configure in this page. After back up, you can see the back up in the list. You can restore the configure in this page also.
Note: the restore will only work after reboot.

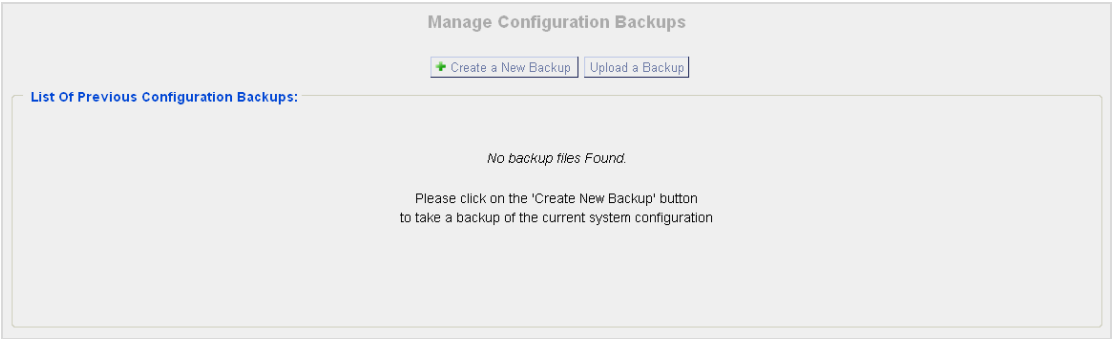


Figure 3-23

3.6.7 Reset and Reboot

·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.

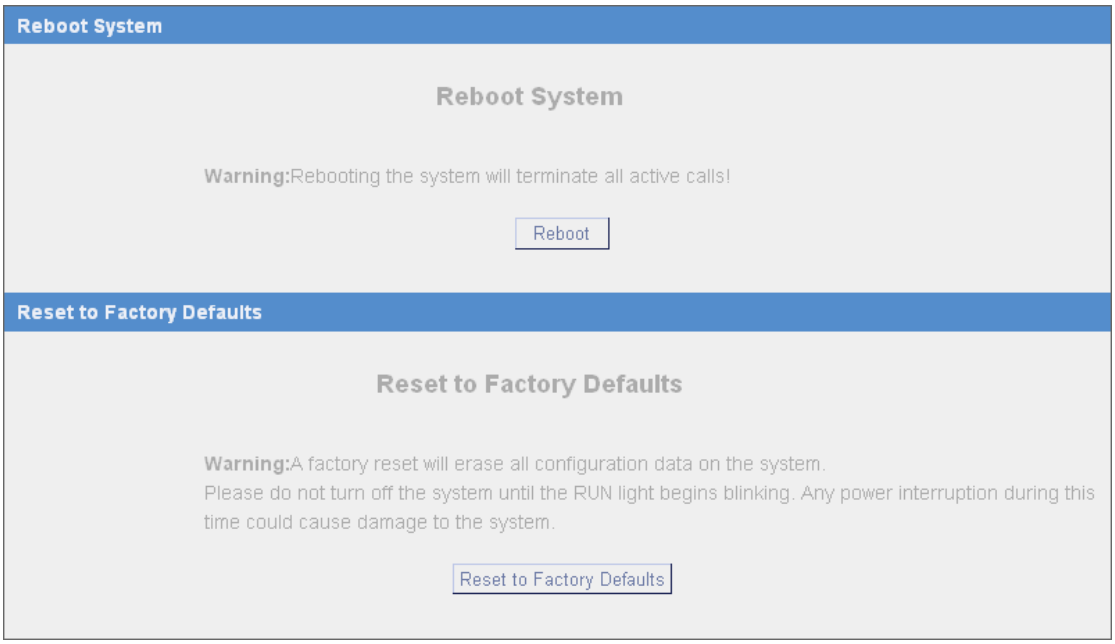


Figure 3-24

3.6.8 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.

Note:
1. If enabled 'Reset configs', System will restore to factory default settings.
2. When update the firmware, please don't turn off the power.

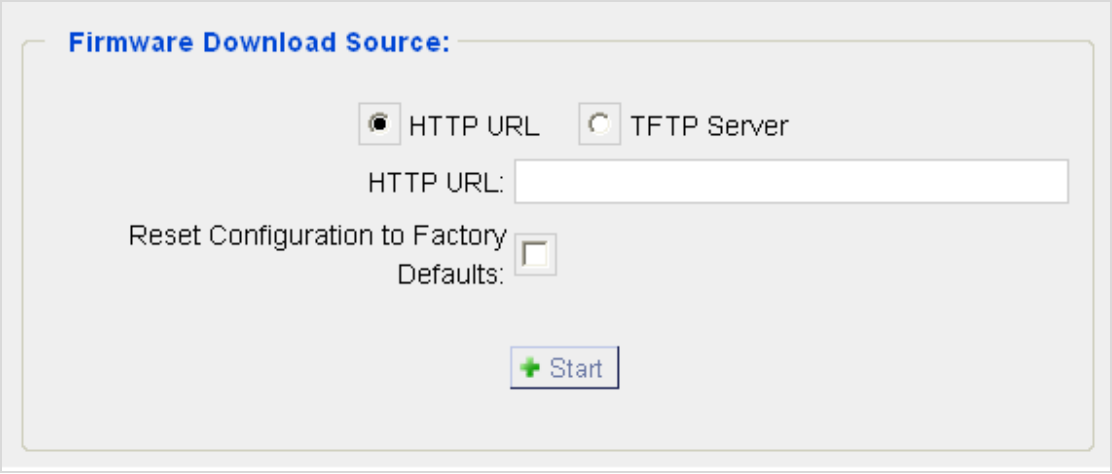


Figure 3-25

3.7 Reports

3.7.1 Call Logs

The call Log captures all call details, including Source, Destination, Start Time, End Time, Duration, Billable Duration, Disposition, Communication Type, etc. Administrator can export CDR data to a CSV file.

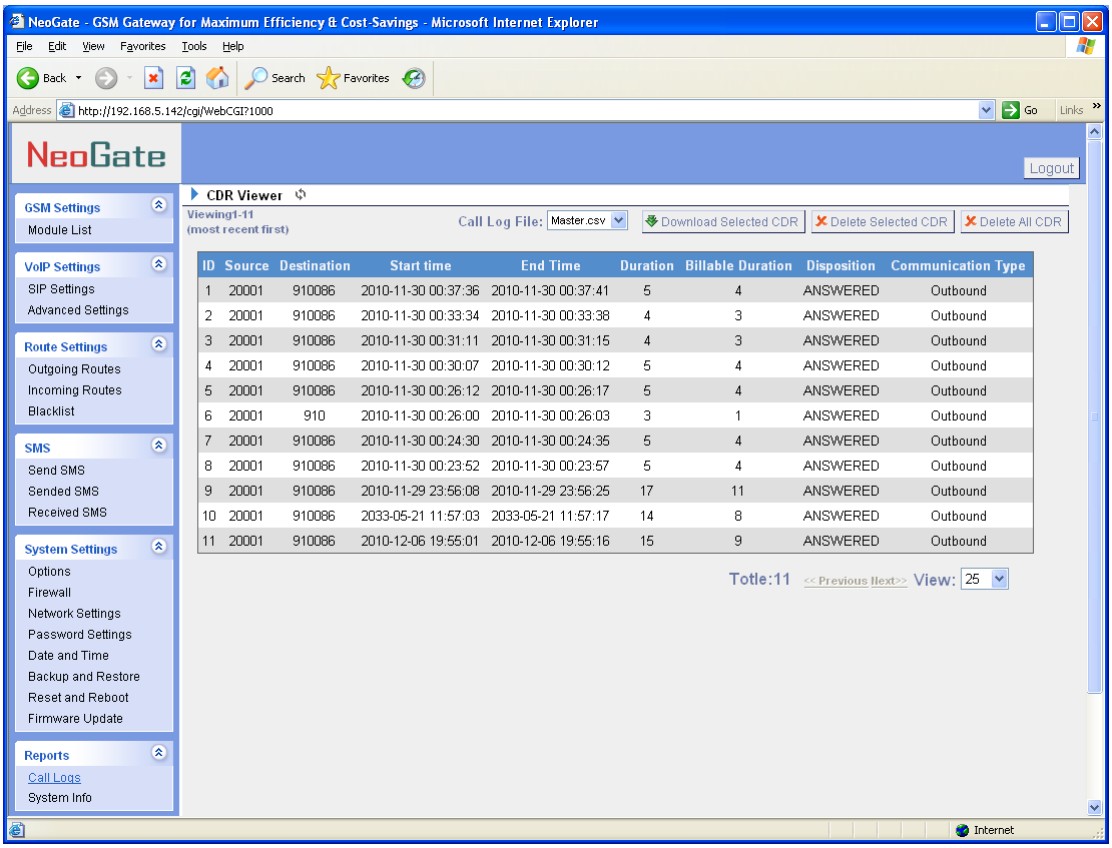


Figure 3-26

3.7.2 System Info

General:
Information about hardware version, firmware version and system uptime.

LAN:
Information about hostname, MAC address, IP address, subnet mask, gateway, Primary DNS and Secondary DNS.

Disk Usage:
Disk usage information.

Memory Usage:

Memory usage information.

Figure 3-27

4. Application

Application 1

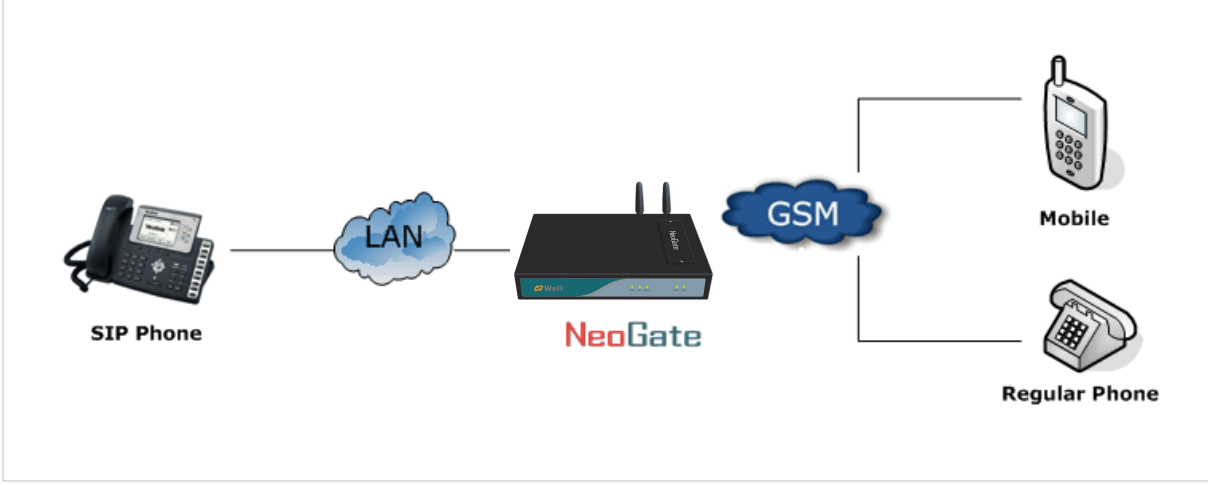


Figure 4-1

Application 2

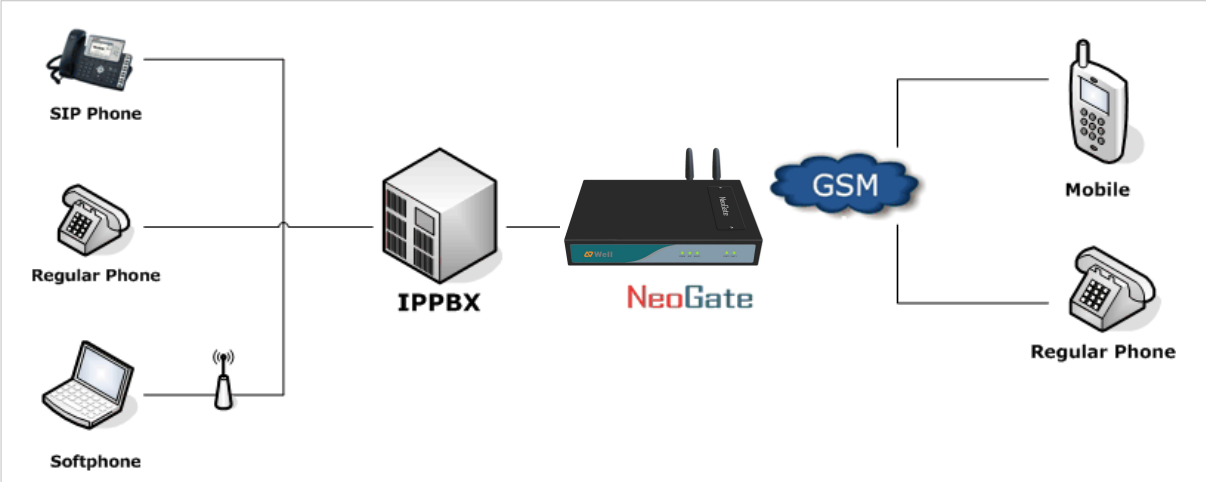


Figure 4-2

<Finish>