TA FXS Gateway

User Manual

Version 40.18.0.1

Yeastar Technology Co., Ltd.

Table of Contents

Introduction

NeoGate TA FXS Analog VoIP Gateways are cutting-edge products that connect legacy telephones, fax machines and PBX systems with IP telephony networks and IP-based PBX systems. Featuring rich functionalities and easy configuration, NeoGate TA is ideal for small and medium enterprises that wish to integrate a traditional phone system into IP-based system. NeoGate TA helps them to preserve previous investment on legacy telephone system and reduce communication costs significantly with the true benefits of VoIP.

Features

● 4/8/16/24/32 FXS ports
● Fully compliant with SIP and IAX2
● Dial Pattern of outgoing calls
● Hunt Group
● Configurable VoIP Server templates
● Reliable fax performance with T.38
● 3-party Conference
● Inter-port Calling
● Call Hold
● Blind Transfer
● Attended Transfer
● Support RADIUS protocol

For more information, please click:
http://www.yeastar.com/Products/Products.asp#NeoGateTA

NeoGate TA FXS Gateway features 4, 8, 16, 24, 32 FXS interfaces for analog phones/fax machines and one 10/100 Mbps LAN port.
For more information about the NeoGate TA hardware specification and how to install the NeoGate TA, please refer to the document below:

http://www.yeastar.com/download/PartI_NeoGate_TA_FXS_Gateway_Installation_Guide_en.pdf

Part I. Configuration Guide

1. Login

The NeoGate TA attempts to contact a DHCP server in your network to obtain valid network settings (e.g., the IP address, subnet mask, default gateway address and DNS address) by default.

Please enable DHCP Server in your network to obtain the NeoGate IP address.

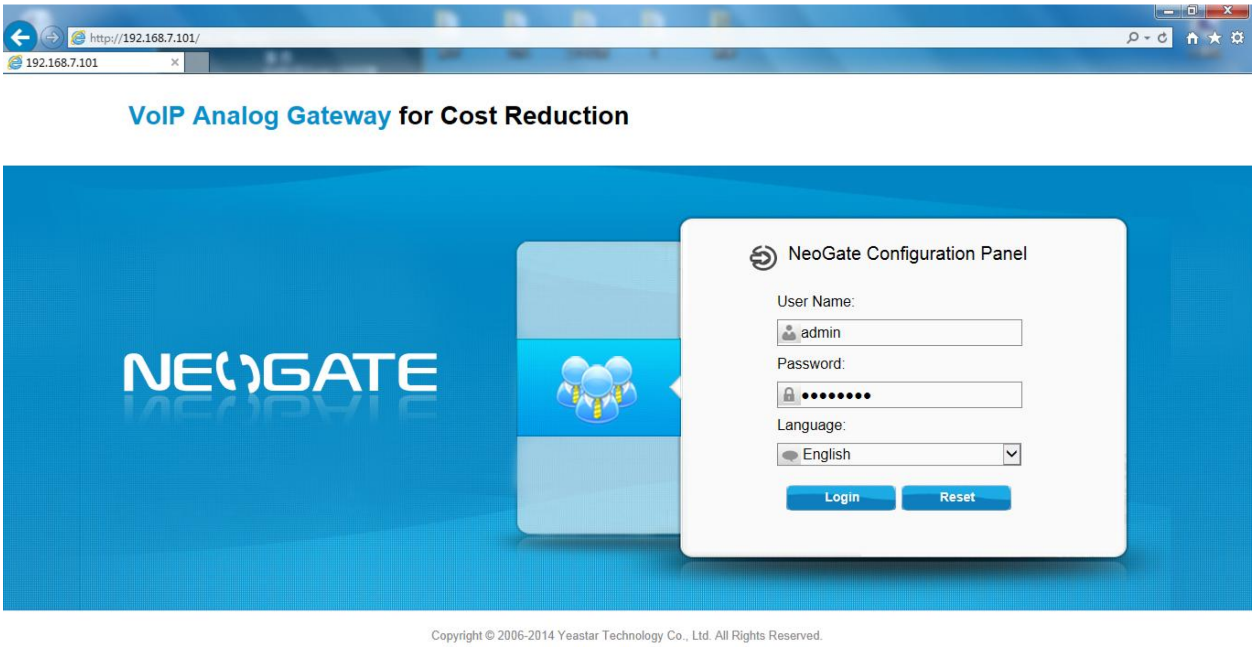
How to check NeoGate TA IP address:

1. Pick up the analog phone, then access the voice menu prompt by dialing "***".
2. Dial "**1**" to check the IP address.
3. Dial "**2**" for web access address.

Logging On:

After entering the IP address in the web browser, users will see a log-in screen.
Check the default settings below:
Username: admin
Password: password

In this example, the IP address is 192.168.7.101, the model is TA2400.



http://192.168.7.101/

VoIP Analog Gateway for Cost Reduction

NeoGate Configuration Panel

User Name: admin

Password: ••••••••

Language: English

192.168.7.101
NEOGATE
Login
Reset
Copyright © 2006-2014 Yeastar Technology Co., Ltd. All Rights Reserved.

Figure 1-1 NeoGate TA Login page

Click "Login" to get the welcome page.

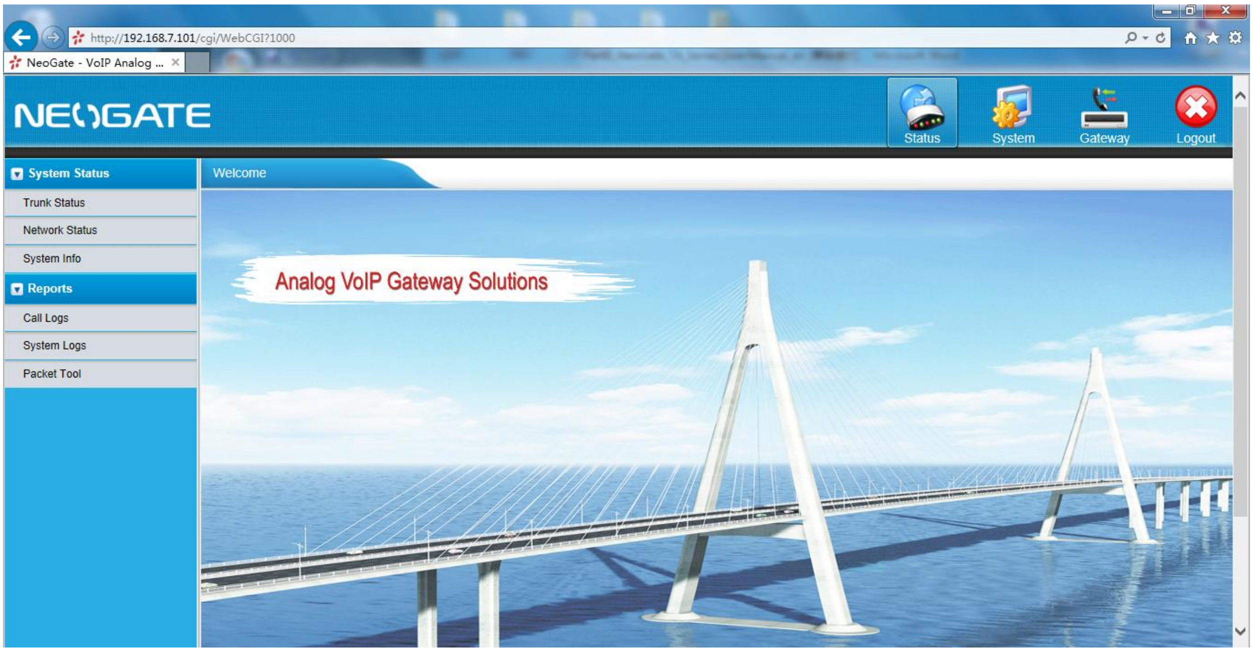


Figure 1-2 Login NeoGate TA

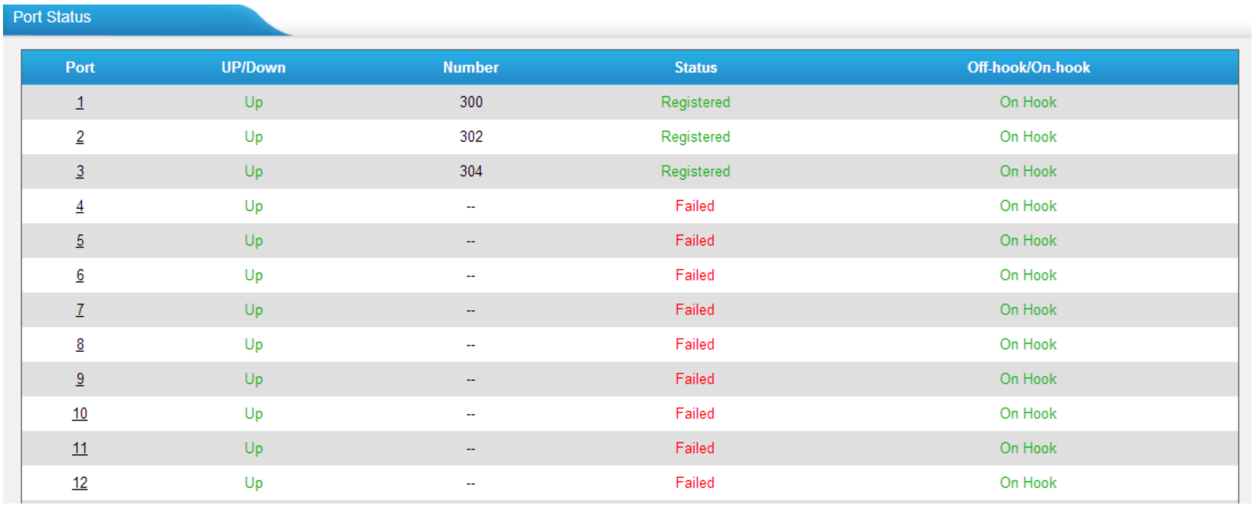
2. Status

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

2.1 System Status

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

2.1.1 Port Status



Port Status

Port	UP/Down	Number	Status	Off-hook/On-hook
1	Up	300	Registered	On Hook
2	Up	302	Registered	On Hook
3	Up	304	Registered	On Hook
4	Up	--	Failed	On Hook
5	Up	--	Failed	On Hook
6	Up	--	Failed	On Hook
7	Up	--	Failed	On Hook
8	Up	--	Failed	On Hook
9	Up	--	Failed	On Hook
10	Up	--	Failed	On Hook
11	Up	--	Failed	On Hook
12	Up	--	Failed	On Hook

Figure 2-1 FXS Port Status

NeoGate TA Status Description:

Port Status:

Up/Down	Description
up	The FXS module works well.
down	The FXS module is broken.

Status:

1) FXS ports registered as VoIP trunk

Status	Description
Registered	Successful registration, trunk is ready for use
Rejected	Trunk registration failed.
Request Send	Registering.
Wating	Waiting for authentication.

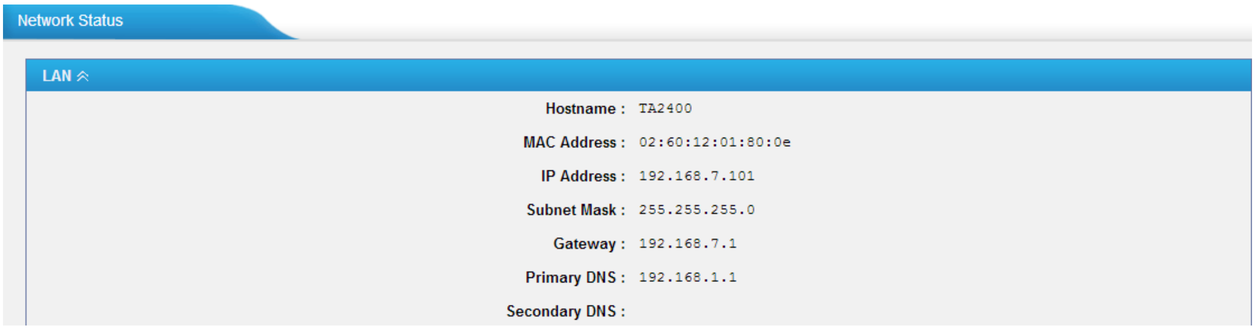
2) FXS ports registered as Service Provider SIP (IAX) trunk

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

Hook	Description
On Hook	The FXS port is idle.
Off Hook	The FXS port is busy.

2.1.2 Network status

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



Network Status

LAN

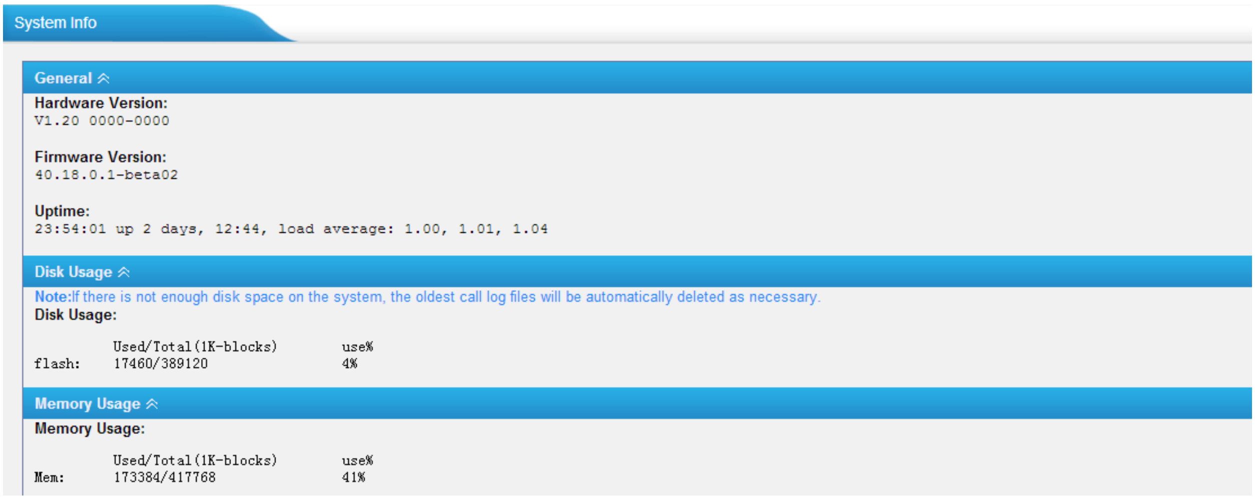
Hostname : TA2400
MAC Address : 02:60:12:01:80:0e
IP Address : 192.168.7.101
Subnet Mask : 255.255.255.0
Gateway : 192.168.7.1
Primary DNS : 192.168.1.1
Secondary DNS :

Figure 2-2 Network Status

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

2.1.3 System Info

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



System Info

General

Hardware Version:
V1.20 0000-0000

Firmware Version:
40.18.0.1-beta02

Uptime:
23:54:01 up 2 days, 12:44, load average: 1.00, 1.01, 1.04

Disk Usage

Note:If there is not enough disk space on the system, the oldest call log files will be automatically deleted as necessary.

Disk Usage:

```
          Used/Total(1K-blocks)        use%
flash:    17460/389120                 4%
```

Memory Usage

Memory Usage:

```
          Used/Total(1K-blocks)        use%
Mem:      173384/417768                41%
```

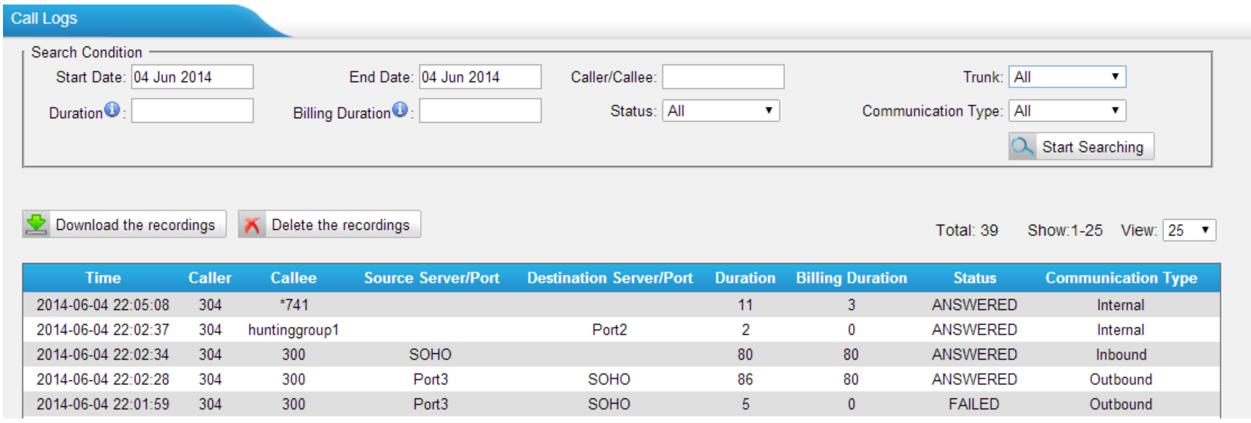
Figure 2-3 System Info

2.2 Reports

In this page, we can check the call detailed log, system log, and use the packet tool to debug the system when needed.

2.2.1 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.



Call Logs

Search Condition

Start Date: 04 Jun 2014 End Date: 04 Jun 2014 Caller/Callee: Trunk: All

Duration: Billing Duration: Status: All Communication Type: All

Start Searching

Download the recordings Delete the recordings

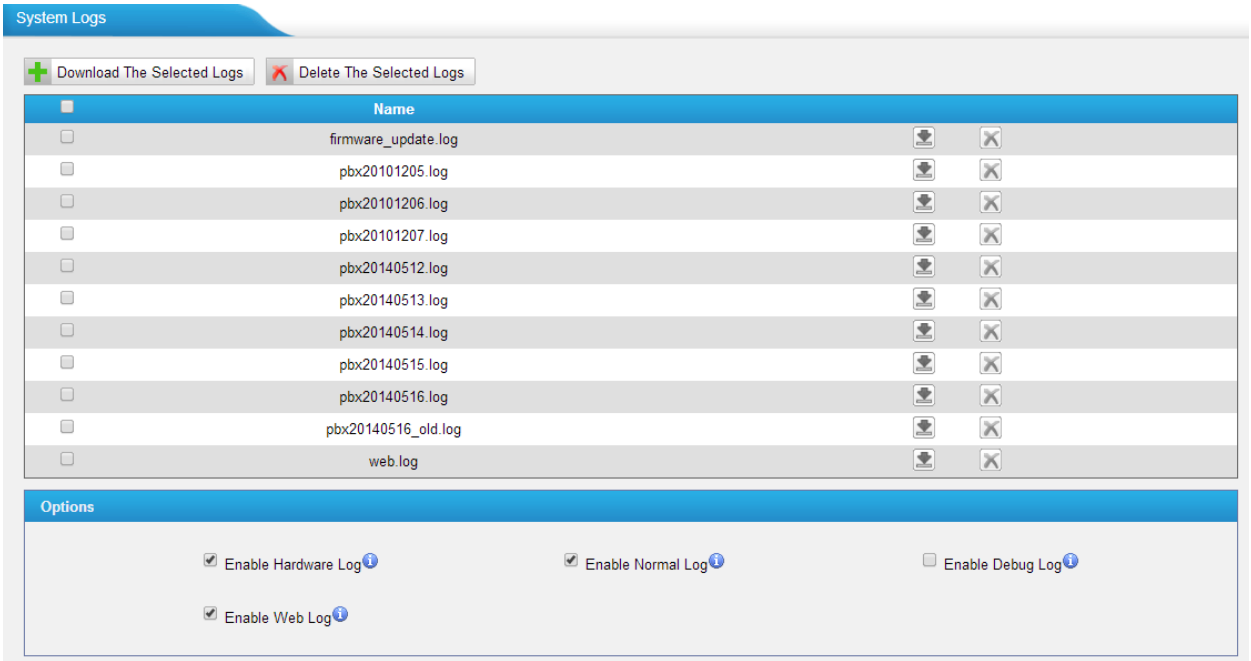
Total: 39 Show:1-25 View: 25

Time	Caller	Callee	Source Server/Port	Destination Server/Port	Duration	Billing Duration	Status	Communication Type
2014-06-04 22:05:08	304	*741			11	3	ANSWERED	Internal
2014-06-04 22:02:37	304	huntinggroup1		Port2	2	0	ANSWERED	Internal
2014-06-04 22:02:34	304	300	SOHO		80	80	ANSWERED	Inbound
2014-06-04 22:02:28	304	300	Port3	SOHO	86	80	ANSWERED	Outbound
2014-06-04 22:01:59	304	300	Port3	SOHO	5	0	FAILED	Outbound

Figure 2-4 Call Logs

2.2.2 System Logs

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



System Logs

Download The Selected Logs Delete The Selected Logs

□	Name
□	firmware_update.log
□	pbx20101205.log
□	pbx20101206.log
□	pbx20101207.log
□	pbx20140512.log
□	pbx20140513.log
□	pbx20140514.log
□	pbx20140515.log
□	pbx20140516.log
□	pbx20140516_old.log
□	web.log

Options

☑ Enable Hardware Log ☑ Enable Normal Log □ Enable Debug Log

☑ Enable Web Log

Figure 2-5 System Logs

Options

·Enable Hardware Log

Save the information of hardware; (up to 4 log files)

·Enable Normal Log
Save the prompt information; (up to 16 log files)

·Enable Web Log
Save the history of web operations (up to 2 log files)

·Enable Debug Log
Save debug information (up to 2 log files)

2.2.3 Packet Tool

This feature is used to capture packets for technician. Integrate packet capture tool "Wireshark" in NeoGate.
Users also could specify the destination IP address and port to get the packets.

·IP
Specify the destination IP address to get the packets.

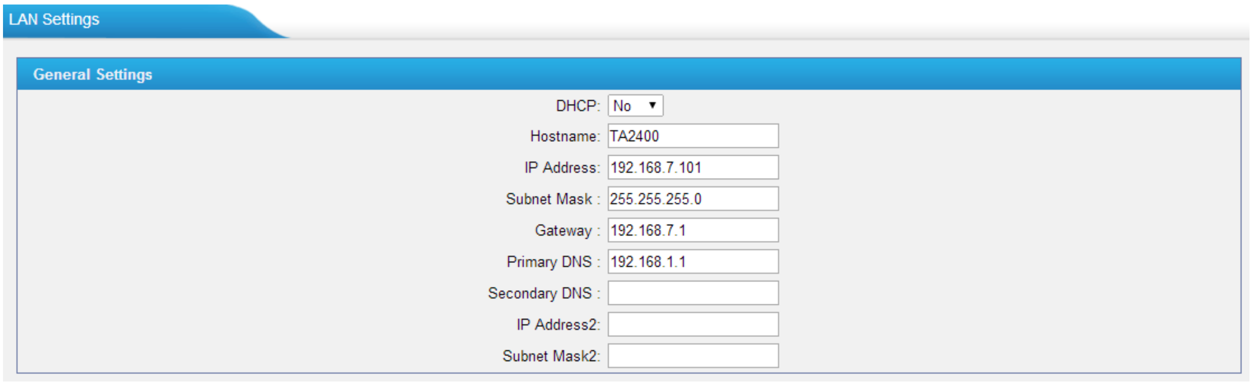
·Port
Specify the destination Port to get the packets.

3. System

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

3.1 Network Preferences

3.1.1 LAN Settings



LAN Settings

General Settings

DHCP:	No
Hostname:	TA2400
IP Address:	192.168.7.101
Subnet Mask :	255.255.255.0
Gateway :	192.168.7.1
Primary DNS :	192.168.1.1
Secondary DNS :	
IP Address2:	
Subnet Mask2:	

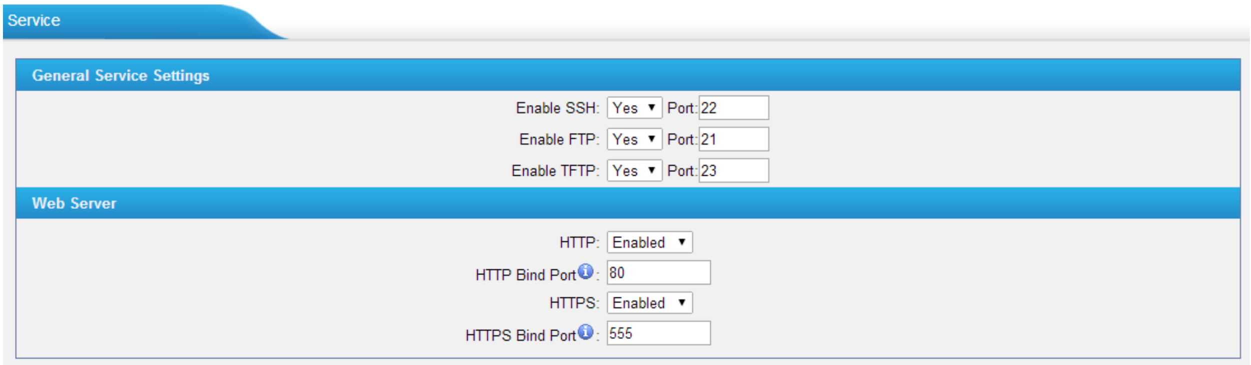
Figure 3-1 LAN Settings

Table 3-1 Description of LAN Settings

Items	Description
DHCP	If this option is set as yes, NeoGate TA will act as DHCP client to get an available IP address from your local network.
Hostname	Set the host name for NeoGate TA
IP Address	Set the IP Address for NeoGate TA. It is recommended that you configure a static IP address for NeoGate TA.
Subnet Mask	Set the subnet mask for NeoGate TA
Gateway	Set the gateway for NeoGate TA
Primary DNS	Set the primary DNS for NeoGate TA.
Secondary DNS	Set the secondary DNS for NeoGate TA
IP Address2	Set the second IP Address for NeoGate TA
Subnet Mask2	Set the second subnet mask for NeoGate TA

3.1.2 Service

The administrator can manage all the access methods on NeoGate TA on the "Service" page.


Service

General Service Settings

Enable SSH: Yes Port: 22

Enable FTP: Yes Port: 21

Enable TFTP: Yes Port: 23

Web Server

HTTP: Enabled

HTTP Bind Port: 80

HTTPS: Enabled

HTTPS Bind Port: 555

Figure 3-2 Service Settings

Table 3-2 Description of Service Settings

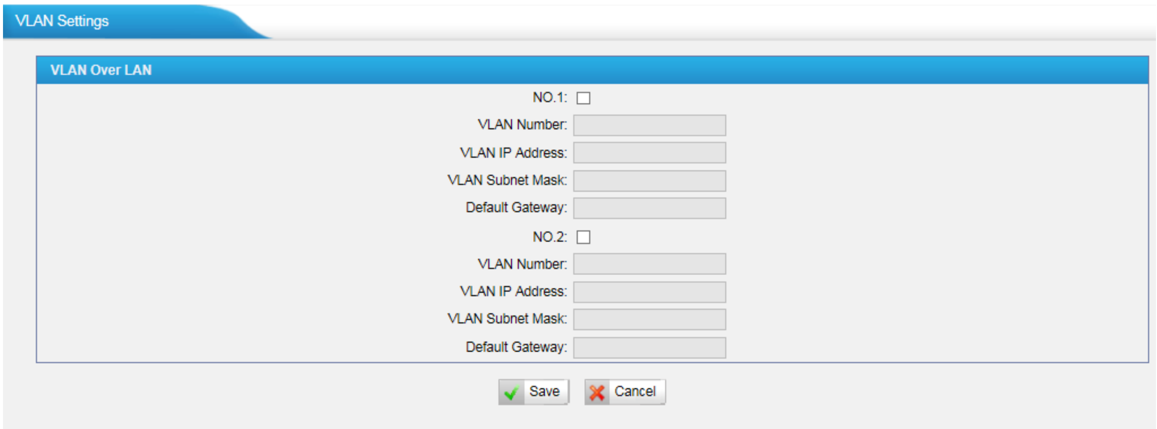
Items	Description
SSH	By using SSH, you can log in to NeoGate and run commands. It's disabled by default. We don't recommend enabling it if not needed. The default port for SSH is 8022;
FTP	FTP access; The default port is 21.
TFTP	TFTP access; The default port is 23.
HTTP	HTTP web access; The default port is 80.
HTTPS	HTTPS web access, it is disabled by default, and you can enable it to get safer web access.

3.1.3 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 TA 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 TA, so that the packages via NeoGate TA will be added the VLAN label before sending to that switch.



VLAN Settings

VLAN Over LAN

NO.1: □

VLAN Number:

VLAN IP Address:

VLAN Subnet Mask:

Default Gateway:

NO.2: □

VLAN Number:

VLAN IP Address:

VLAN Subnet Mask:

Default Gateway:

Figure 3-3 VLAN Settings

Table 3-3 Description of VLAN Settings

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 TA VLAN over LAN.
VLAN Subnet Mask	Set the Subnet Mask for NeoGate TA VLAN over LAN.
Default Gateway	Set the Default Gateway for NeoGate TA 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 TA VLAN over LAN.
VLAN Subnet Mask	Set the Subnet Mask for NeoGate TA VLAN over LAN.
Default Gateway	Set the Default Gateway for NeoGate TA VLAN over LAN.

3.1.4 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 TA supports OpenVPN.

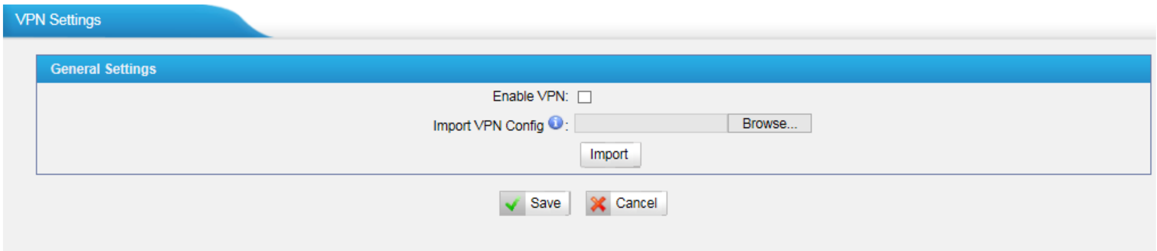


Figure 3-4 VPN Settings

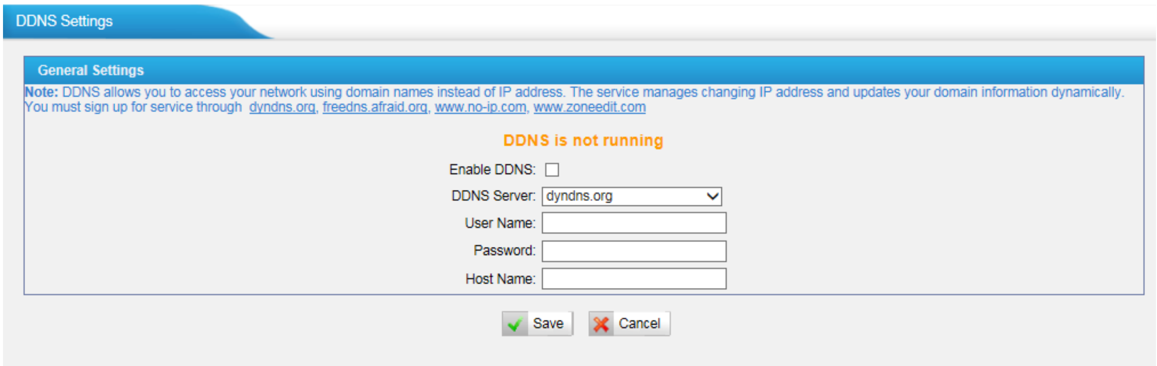
·Enable VPN

·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 TA works as VPN client mode only.

3.1.5 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.



DDNS Settings

General Settings

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

DDNS is not running

Enable DDNS: □

DDNS Server: dyndns.org

User Name:

Password:

Host Name:

Figure 3-5 DDNS Settings

Table 3-4 Description of DDNS Settings

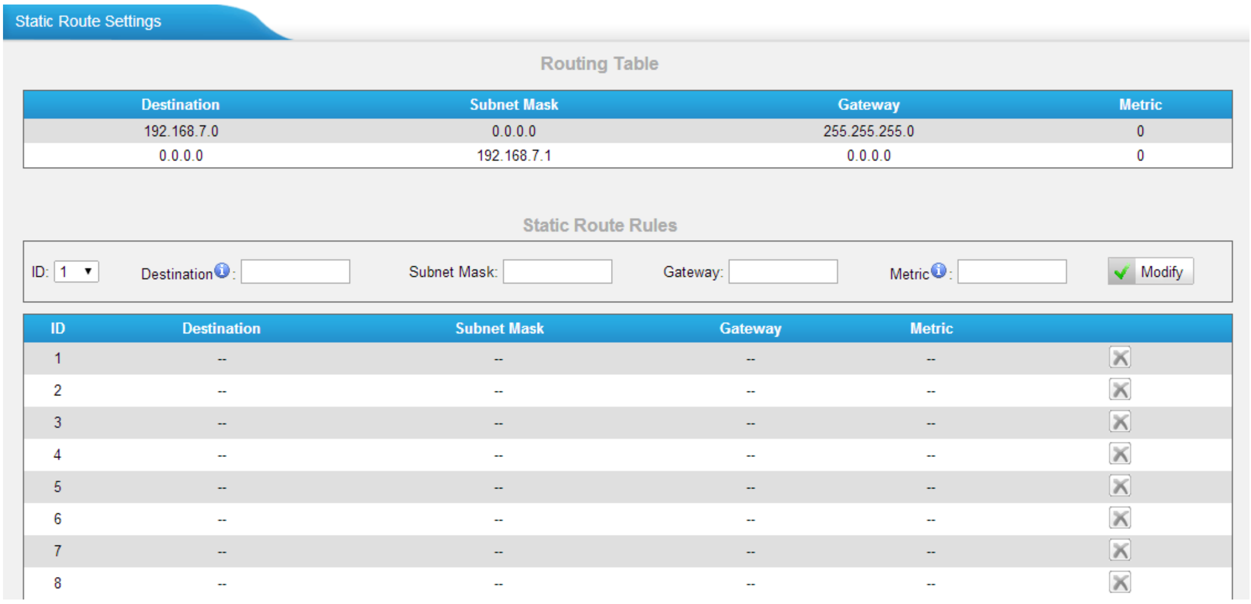
Items	Description
DDNS Server	Select the DDNS server you sign up for service.
User Name	User name the DDNS server provides you.
Password	User account’s password.
Host Name	The host name you have got from the DDNS server

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.

3.1.6 Static Route

NeoGate TA 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 TA to force it to go out through different gateway when accessing to different internet.

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



Static Route Settings

Routing Table

Destination	Subnet Mask	Gateway	Metric
192.168.7.0	0.0.0.0	255.255.255.0	0
0.0.0.0	192.168.7.1	0.0.0.0	0

Static Route Rules

ID: 1 Destination: Subnet Mask: Gateway: Metric: Modify

ID	Destination	Subnet Mask	Gateway	Metric	
1	--	--	--	--	☒
2	--	--	--	--	☒
3	--	--	--	--	☒
4	--	--	--	--	☒
5	--	--	--	--	☒
6	--	--	--	--	☒
7	--	--	--	--	☒
8	--	--	--	--	☒

Figure 3-6 Static Route

1) Route Table

The current route rules of NeoGate TA.

2) Static Route Rules

You can add new static route rules here.

Table 3-5 Description of Static Route Settings

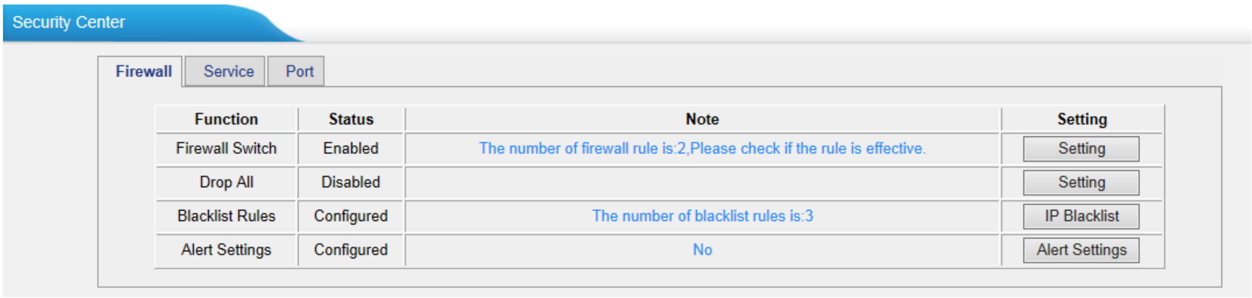
Items	Description
Destination	The destination network to be accessed to by NeoGate TA.
Subnet Mask	Specify the destination network portion.
Gateway	Define which gateway NeoGate TA will go through when accessing the destination network.
Metric	The cost of a route is calculated by using what are called 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.

3.2 Security Center

3.2.1 Security Center

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

Firewall:

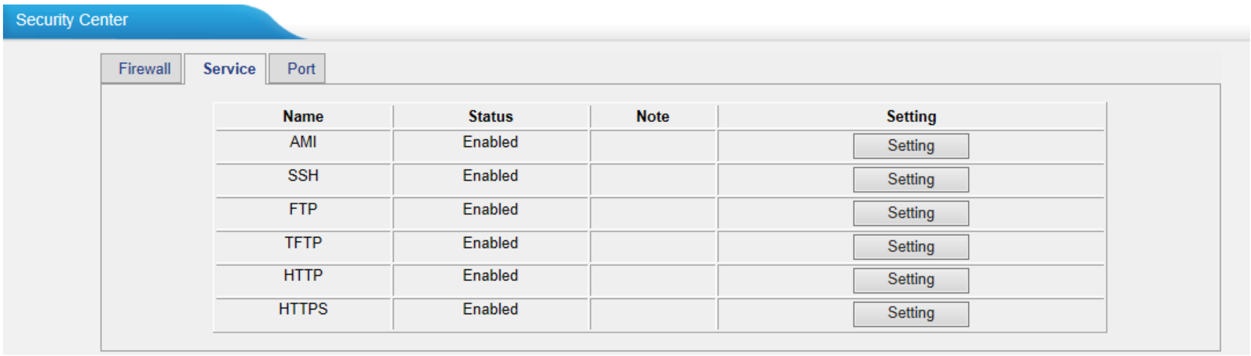


Function	Status	Note	Setting
Firewall Switch	Enabled	The number of firewall rule is:2,Please check if the rule is effective.	Setting
Drop All	Disabled		Setting
Blacklist Rules	Configured	The number of blacklist rules is:3	IP Blacklist
Alert Settings	Configured	No	Alert Settings

Figure 3-7 Firewall

In the “Firewall” tab, you can check firewall configuration and alert settings. You can enter the configuration page directly by clicking the relevant button.

Service:

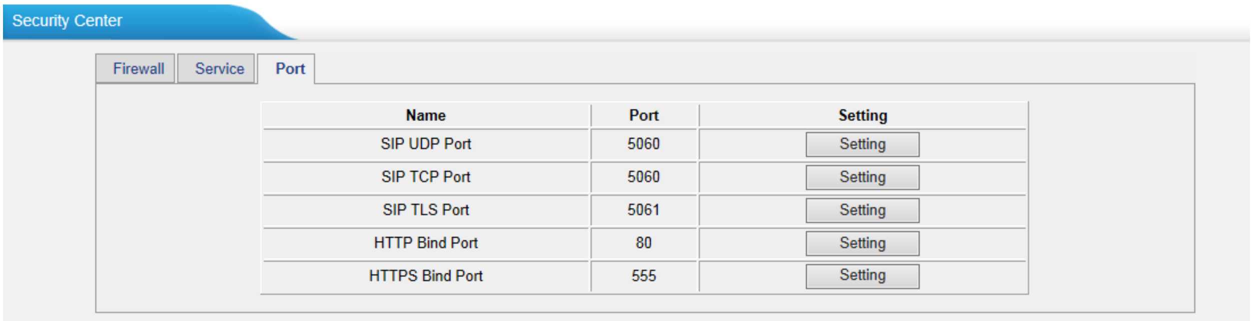


Name	Status	Note	Setting
AMI	Enabled		Setting
SSH	Enabled		Setting
FTP	Enabled		Setting
TFTP	Enabled		Setting
HTTP	Enabled		Setting
HTTPS	Enabled		Setting

Figure 3-8 Service

In “Service” tab, you can check AMI /SSH/FTP/TFTP/HTTP/HTTPS status. You can enter the configuration page directly by clicking the relevant button.

Port:



Name	Port	Setting
SIP UDP Port	5060	Setting
SIP TCP Port	5060	Setting
SIP TLS Port	5061	Setting
HTTP Bind Port	80	Setting
HTTPS Bind Port	555	Setting

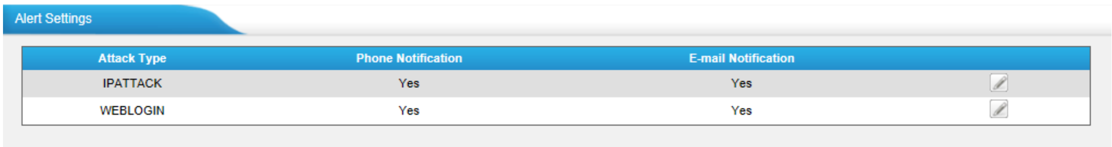
Figure 3-9 Port

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

3.2.2 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.



Alert Settings

Attack Type	Phone Notification	E-mail Notification	
IPATTACK	Yes	Yes	✎
WEBLOGIN	Yes	Yes	✎

Figure 3-10 Alert Settings

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 matches the protection rule.

1) Phone Notification Settings

Table 3-6 Description of Phone Notification Settings

Items	Description
PHONE Notification	Whether to enable phone notification or not.
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.
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.

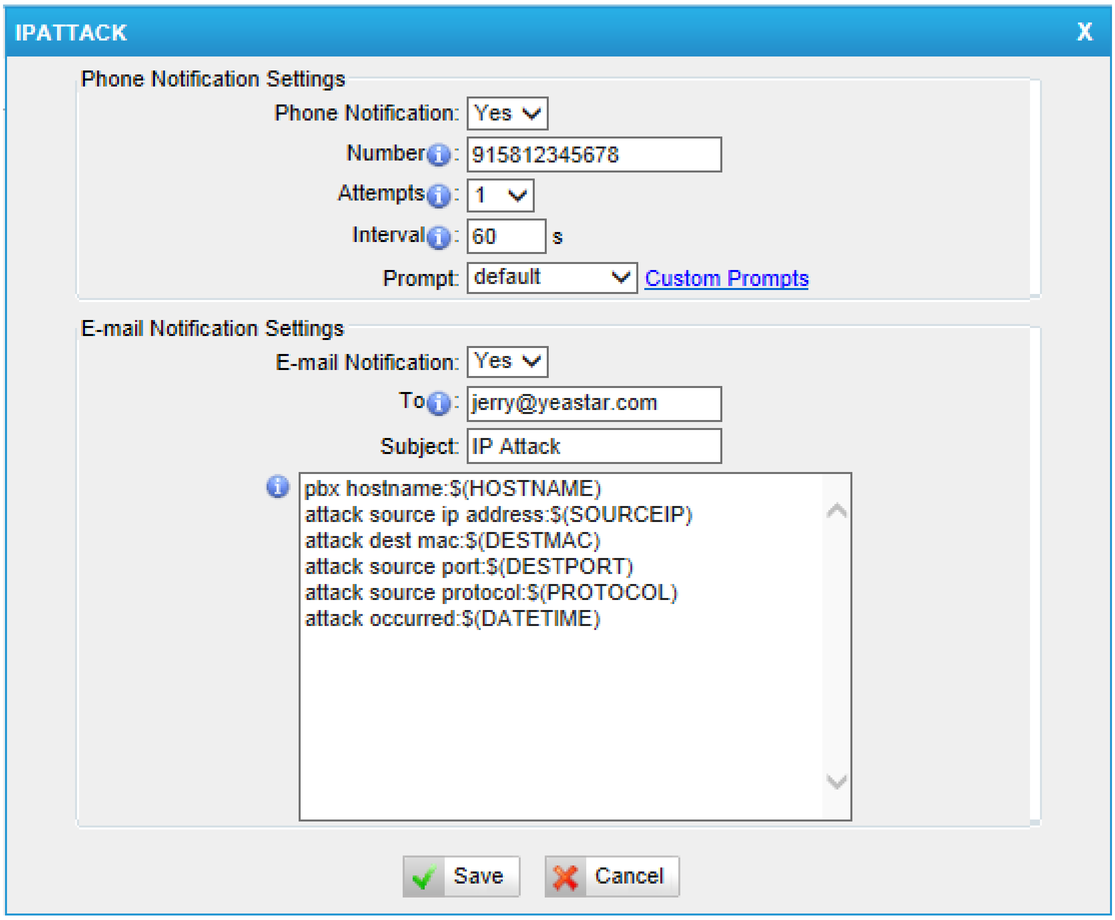
2) E-mail Notification Settings

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

Table 3-7 Description of E-mail Notification Settings

Items	Description
E-mail Notification	Whether to enable E-mail Notification or not.
Recipient's Name	The recipients for the alert notification, and multiple email addresses are allowed, please separate them by ";". E.g. jerry@yeastar.com;jason@yeastar.com,456@sina.com
Subject	The subject of the alert email.
Email Content	Text content supports 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)



Phone Notification Settings

Phone Notification: Yes

Number: 915812345678

Attempts: 1

Interval: 60 s

Prompt: default

E-mail Notification Settings

E-mail Notification: Yes

To: jerry@yeastar.com

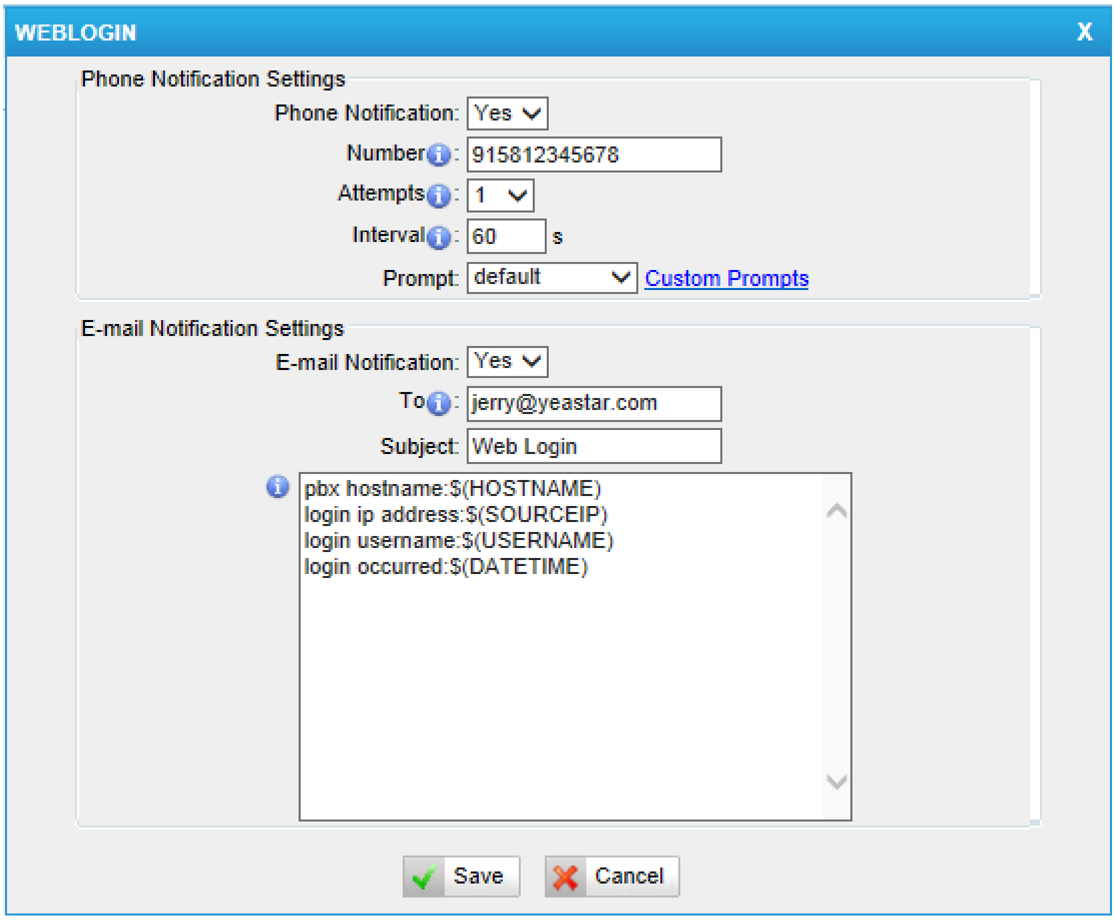
Subject: IP Attack

```
pbx hostname:$(HOSTNAME)
attack source ip address:$(SOURCEIP)
attack dest mac:$(DESTMAC)
attack source port:$(DESTPORT)
attack source protocol:$(PROTOCOL)
attack occurred:$(DATETIME)
```

Figure 3-11 IP ATTACK Alert

2. WEBLOGIN

Web Login Alert Notification: entering the wrong password consecutively for five times when logging in NeoGate TA Web interface will be deemed as an attack, the system will limit the IP login within 10 minutes and notify the user.



Phone Notification Settings

Phone Notification: Yes

Number: 915812345678

Attempts: 1

Interval: 60 s

Prompt: default

E-mail Notification Settings

E-mail Notification: Yes

To: jerry@yeastar.com

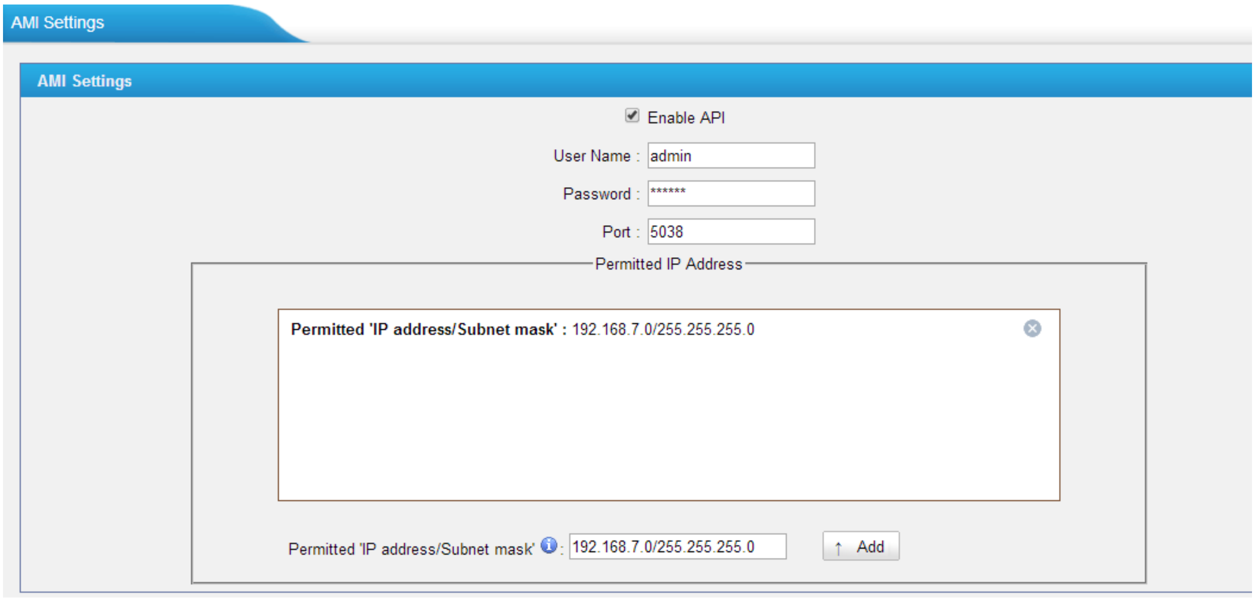
Subject: Web Login

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

Figure 3-12 WEBLOGIN Alert

3.2.3 AMI Settings

The Asterisk Manager Interface (AMI) is a system monitoring and management interface provided by Asterisk. It allows live monitoring of events that occur in the system, as well enabling you to request that Asterisk perform some action. The actions that are available are wide-ranging and include things such as returning status information and originating new calls. Many interesting applications have been developed on top of Asterisk that take advantage of the AMI as their primary interface to Asterisk.
There are two main types of messages on the Asterisk Manager Interface: manager events and manager actions.
The 3rd party software can work with NeoGate TA using AMI interface. It is disabled by default. If necessary, you can enable it.



AMI Settings

AMI Settings

☑ Enable API

User Name : admin

Password : ******

Port : 5038

Permitted IP Address

Permitted 'IP address/Subnet mask' : 192.168.7.0/255.255.255.0

Permitted 'IP address/Subnet mask' : 192.168.7.0/255.255.255.0

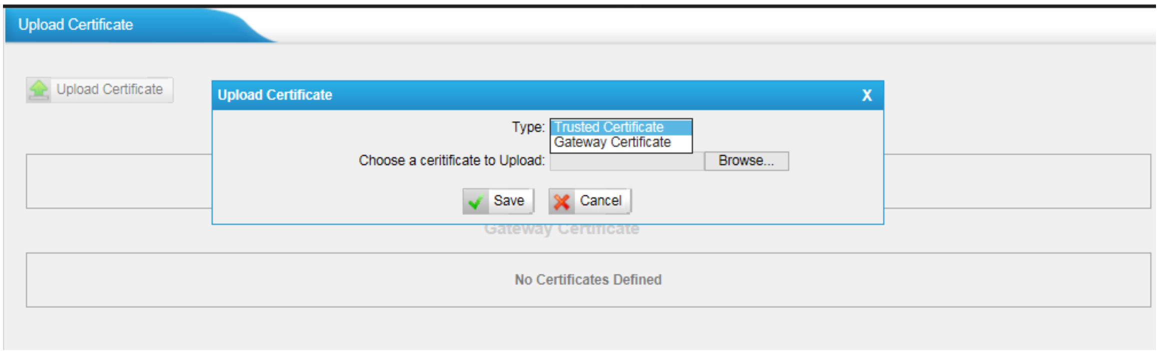
Figure 3-13 AMI Settings

Username & password: after enabling AMI, you can use this username and password to log in NeoGate TA AMI.

Permitted "IP address/Subnet mask": you can set which IP can log in NeoGate TA AMI interface.

3.2.4 Certificates

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



Upload Certificate

Upload Certificate

Type: Trusted Certificate / Gateway Certificate

Choose a ceritificate to Upload:

Gateway Certificate

No Certificates Defined

Figure 3-14 Certificates

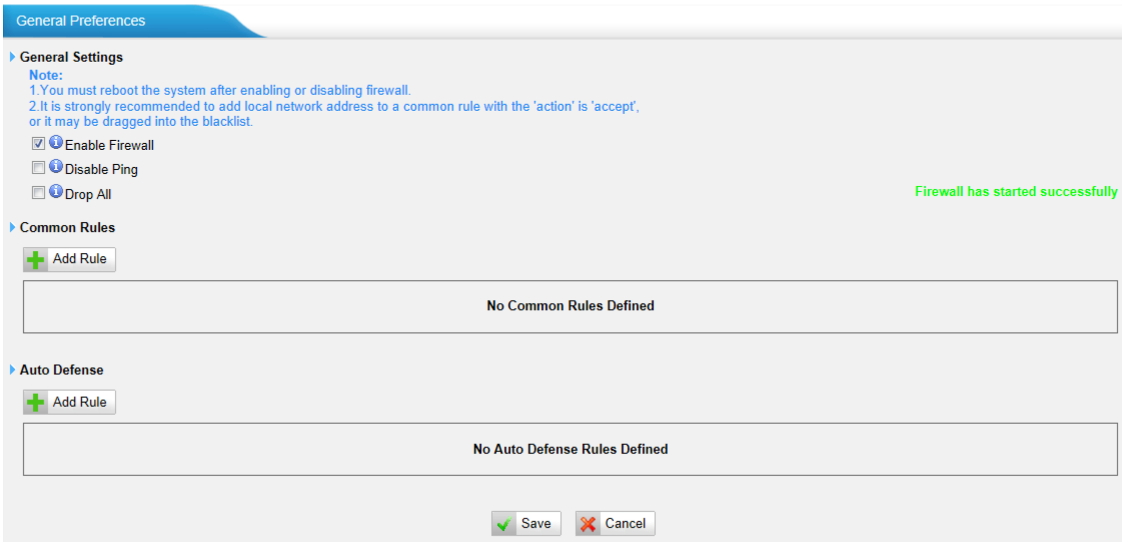
Trusted Certificate

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 TA. If IPPBX enables “TLS Verify server”, you should also upload this certificate on IPPBX.

3.2.5 Firewall Rules



General Preferences

General Settings

Note:
1.You must reboot the system after enabling or disabling firewall.
2.It is strongly recommended to add local network address to a common rule with the 'action' is 'accept', or it may be dragged into the blacklist.

☑ Enable Firewall
□ Disable Ping
□ Drop All

Firewall has started successfully

Common Rules

Add Rule

No Common Rules Defined

Auto Defense

Add Rule

No Auto Defense Rules Defined

Save Cancel

Figure 3-15 Firewall Rules

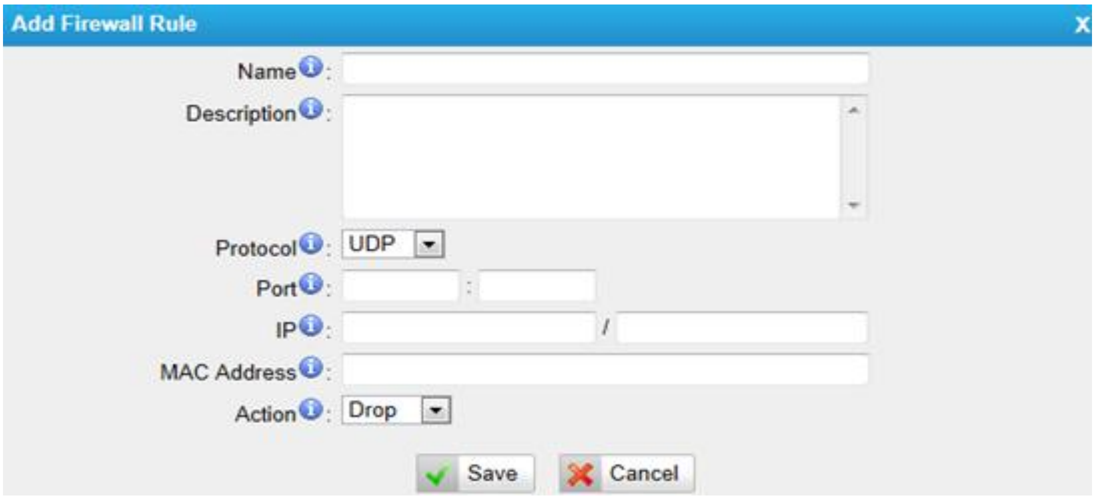
1) General Settings

Table 3-8 Description of Firewall General Settings

Items	Description
Enable Firewall	Enable the firewall to protect the device. You should reboot the device to make the firewall run.
Disable Ping	Enable this item to drop net ping from remote hosts.
Drop All	When you enable "Drop All" feature, the 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.



Add Firewall Rule

Name:	
Description:	
Protocol:	UDP
Port:	:
IP:	/
MAC Address:	
Action:	Drop

Save Cancel

Figure 3-16 Common Rule

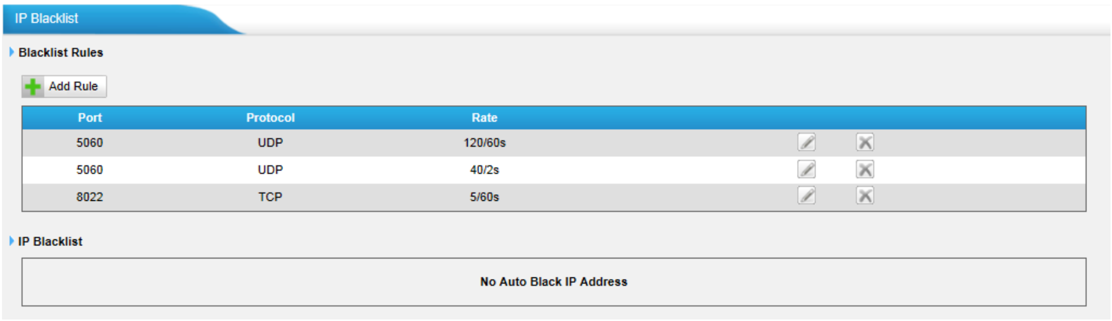
Table 3-9 Description of Common Rule Settings

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 E.g. 192.168.5.100/255.255.255.255 for IP 192.168.5.100 E.g. 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.

3.2.6 IP Blacklist

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



IP Blacklist

Blacklist Rules

Port	Protocol	Rate
5060	UDP	120/60s
5060	UDP	40/2s
8022	TCP	5/60s

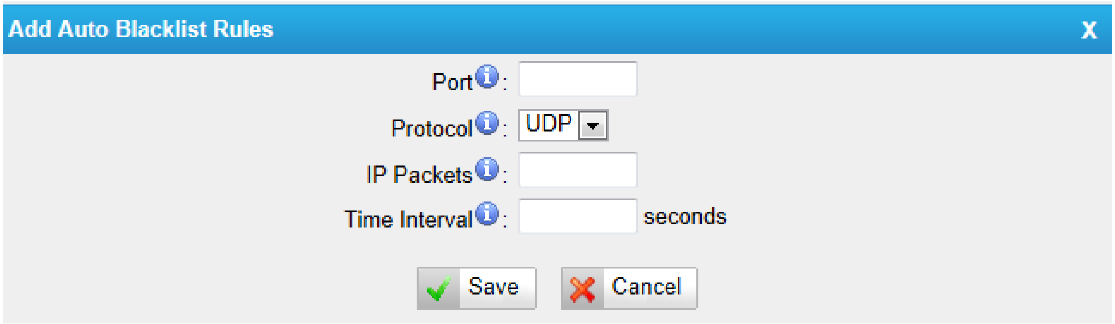
IP Blacklist

No Auto Black IP Address

Figure 3-17 IP Blacklist

1) Blacklist rules

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



Add Auto Blacklist Rules

Port:

Protocol: UDP

IP Packets:

Time Interval: seconds

Figure 3-18 Auto Blacklist Rule

Table 3-10 Description of Auto Blacklist Rule Settings

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

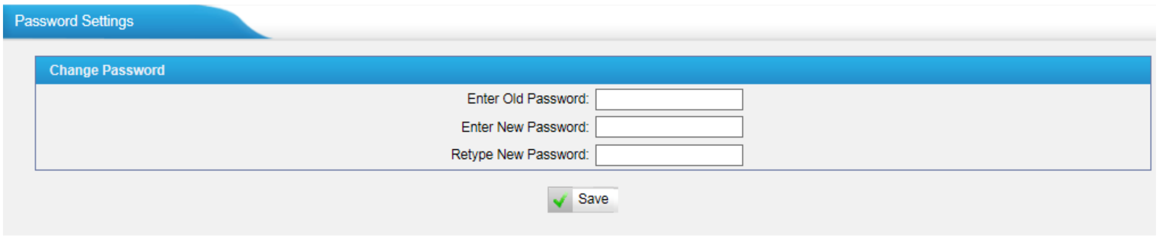
The blocked IP address will display here, you can edit or delete it as you wish.

3.3 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.

3.3.1 Password settings

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



Password Settings

Change Password

Enter Old Password:

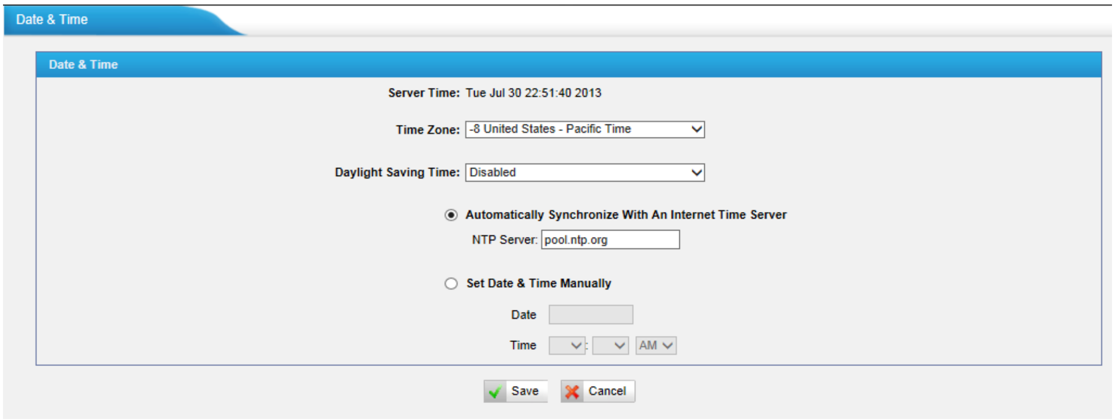
Enter New Password:

Retype New Password:

Figure 3-19 Password Settings

3.3.2 Date and Time

Set the date and time for NeoGate TA.



Date & Time

Date & Time

Server Time: Tue Jul 30 22:51:40 2013

Time Zone: -8 United States - Pacific Time

Daylight Saving Time: Disabled

● Automatically Synchronize With An Internet Time Server

NTP Server: pool.ntp.org

○ Set Date & Time Manually

Date

Time : AM

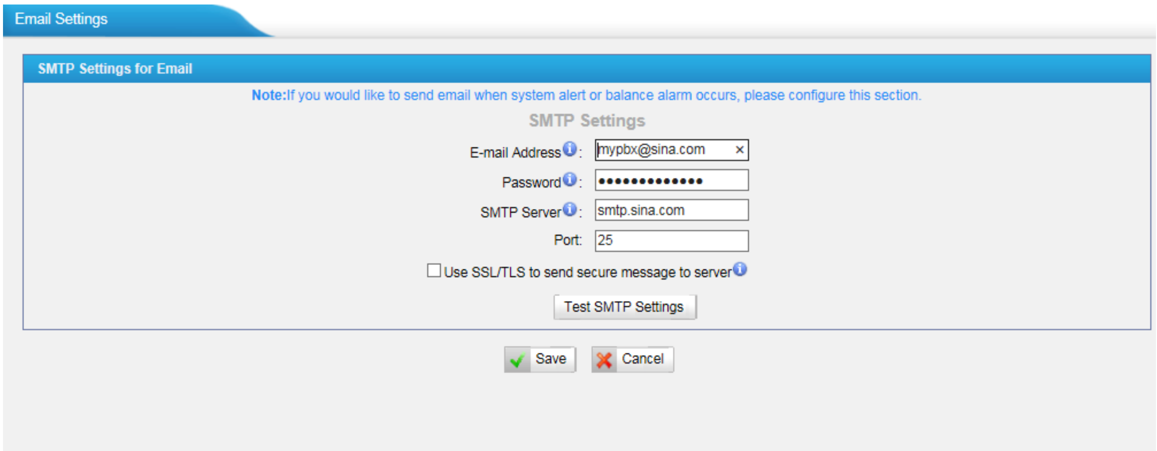
Figure 3-20 Date & Time

Table 3-11 Description of Date & Time Settings

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 TA will update the time automatically.
Set Date & Time Manually	You can set the time to your local time manually here.

3.3.3 Email Settings

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


Email Settings

SMTP Settings for Email

Note:If you would like to send email when system alert or balance alarm occurs, please configure this section.

SMTP Settings

E-mail Address: mypbx@sina.com

Password: ••••••••••••••

SMTP Server: smtp.sina.com

Port: 25

□ Use SSL/TLS to send secure message to server

Figure 3-25 Email Settings

Table 3-12 Description of SMTP Settings

Items	Description
E-mail Address	The E-mail Address that NeoGate TA 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 TA 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.

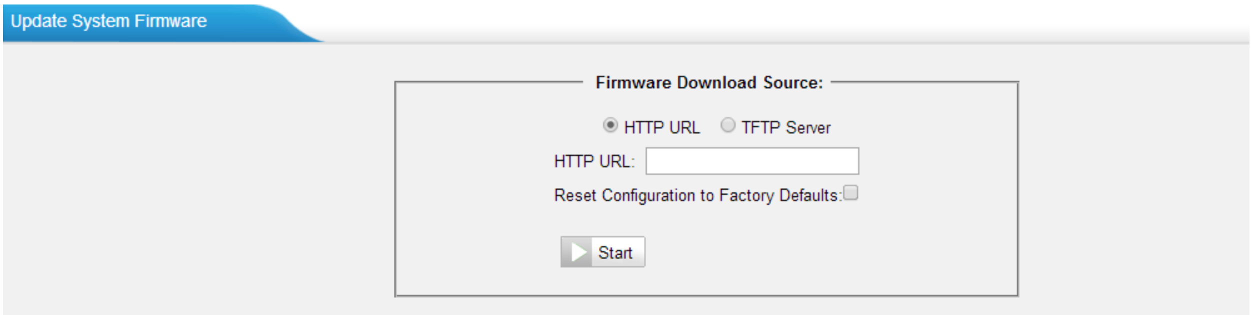
After filling out the above information, you can click on the "Test Account Settings" button to check whether the setup is OK.

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 if the network is proper.

3.3.4 Firmware Update

Firmware upgrading 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 "Reset configuration to Factory Defaults" is enabled, the system will restore to factory default settings.
2. When updating the firmware, please don't turn off the power. Or the system will get damaged.



Update System Firmware

Firmware Download Source:

● HTTP URL ○ TFTP Server

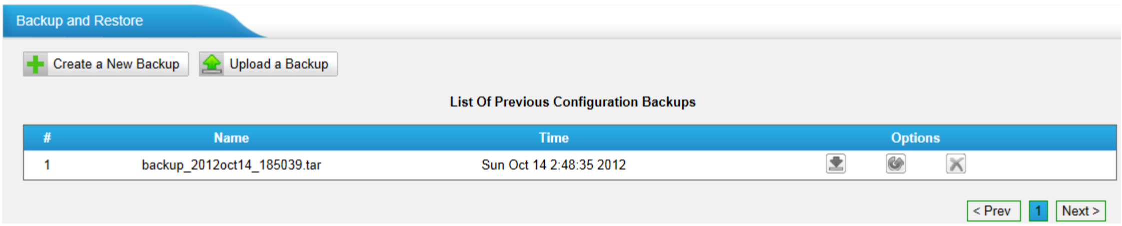
HTTP URL:

Reset Configuration to Factory Defaults: □

Figure 3-26 Firmware Update

3.3.5 Backup and Restore

We can back up the configurations before resetting NeoGate TA to factory defaults, and then restore it on this package.



Backup and Restore

List Of Previous Configuration Backups

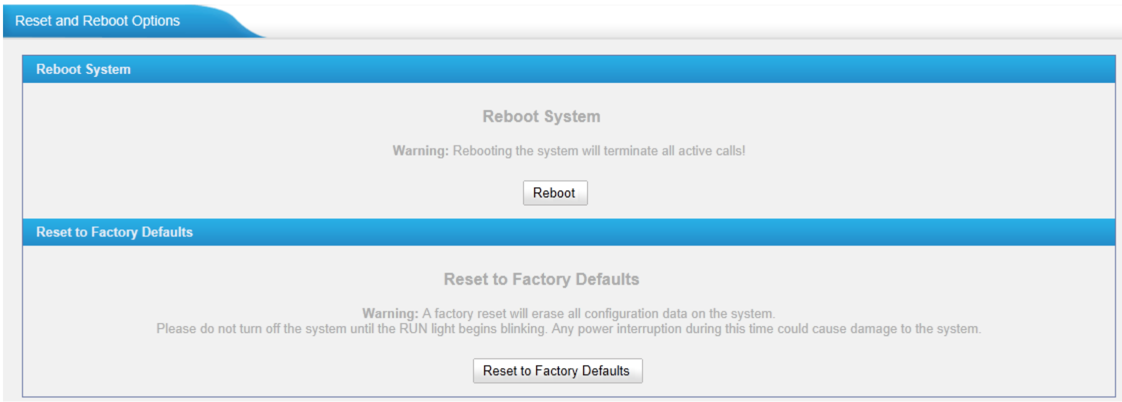
#	Name	Time	Options
1	backup_2012oct14_185039.tar	Sun Oct 14 2:48:35 2012	

Figure 3-27 Backup and Restore

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

3.3.6 Reset and Reboot

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



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 3-28 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.

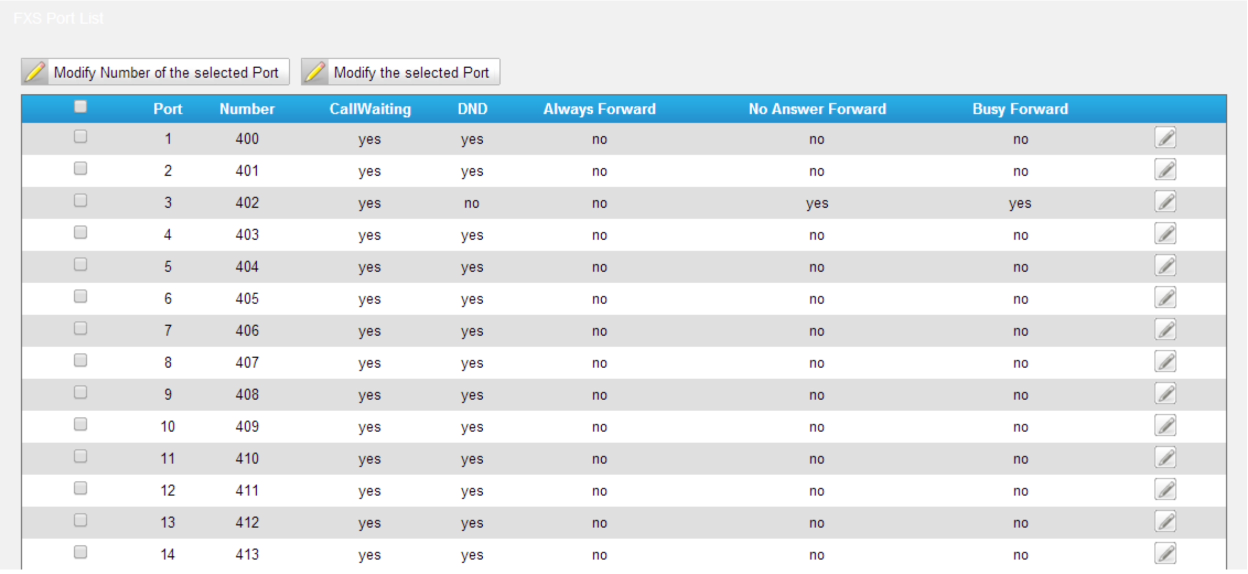
4. Gateway

Click Gateway to access the gateway configuration page. Users can configure the details of FXS ports, VoIP settings, gateway settings and advanced settings.

4.1 FXS Port List

4.1.1 FXS Port List

All the FXS ports are listed here. You can edit each FXS port by clicking the "Edit" button. Batch editing the FXS ports number and batch editing FXS ports are available.



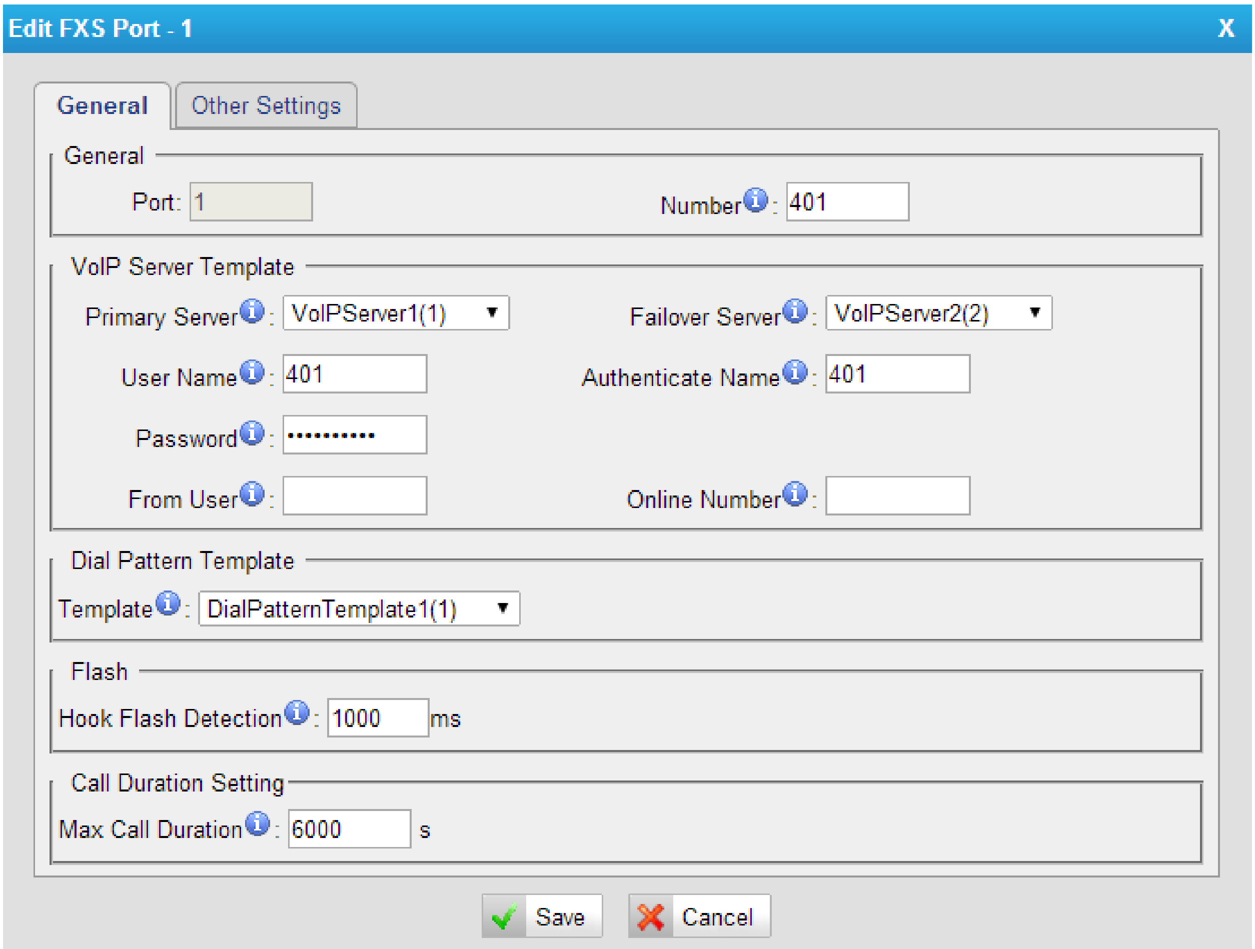
FXS Port List

□	Port	Number	CallWaiting	DND	Always Forward	No Answer Forward	Busy Forward	
□	1	400	yes	yes	no	no	no	✎
□	2	401	yes	yes	no	no	no	✎
□	3	402	yes	no	no	yes	yes	✎
□	4	403	yes	yes	no	no	no	✎
□	5	404	yes	yes	no	no	no	✎
□	6	405	yes	yes	no	no	no	✎
□	7	406	yes	yes	no	no	no	✎
□	8	407	yes	yes	no	no	no	✎
□	9	408	yes	yes	no	no	no	✎
□	10	409	yes	yes	no	no	no	✎
□	11	410	yes	yes	no	no	no	✎
□	12	411	yes	yes	no	no	no	✎
□	13	412	yes	yes	no	no	no	✎
□	14	413	yes	yes	no	no	no	✎

Figure 4-1 FXS Port List

1) Edit the FXS port

Click "Edit" button ✎ to configure the FXS port.



Edit FXS Port - 1

General | Other Settings

General

Port: 1

Number: 401

VoIP Server Template

Primary Server: VoIPServer1(1)

Failover Server: VoIPServer2(2)

User Name: 401

Authenticate Name: 401

Password: ••••••••••

From User:

Online Number:

Dial Pattern Template

Template: DialPatternTemplate1(1)

Flash

Hook Flash Detection: 1000 ms

Call Duration Setting

Max Call Duration: 6000 s

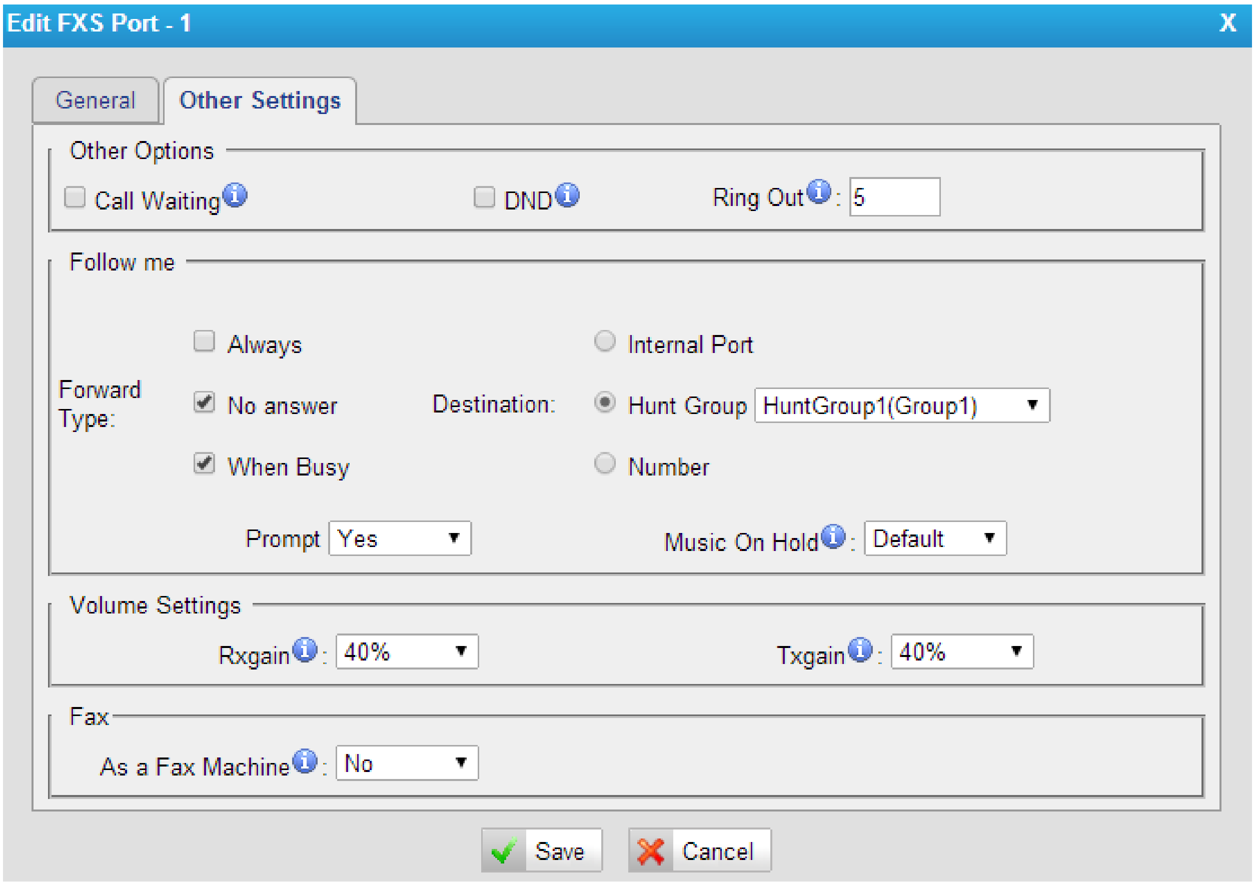
Figure 4-2 Edit FXS Port

> General

Table 4-1 Description of FXS Port General Settings

Items		Description
General	Port	The corresponding port.
	Number	User account number.
VoIP Serer Template	Primary Server	Choose the Primary VoIP server, where the account will be registered.
	Failover Server	Choose the failover server for the account. This server will be used if the primary server is unavailable.
	User Name	Username of the account. Used for VoIP trunk registration. The user name should be entered if the "Enable Register" is checked on the VoIP Server.
	Authentication Name	Used for SIP authentication. The authentication name should be entered if "Enable Register" is checked on the VoIP Server.
	Password	Password of the SIP account. The password should be entered if "Enable Register" is checked on the VoIP Server.
	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 package. Keep this field blank if not needed.
	Online Number	Define the online number that expected by "Skype Connect" and some other SIP service providers. Leave this field blank if not needed.
Dial Pattern Template		The account will be allowed to make outbound calls according to the selected template.
Flash		Sets the amount of time, in milliseconds, that a hook flash must remain depressed in order for the system to consider it as a valid flash event. Default: 1000ms.
Call Duration Setting		Set up the max cull duration for every call of this user, but it's only valid for outbound calls. Enter "0" or leave this blank empty, the value would be equal to the max call duration configured in the General Preferences settings page. **Note**: This setting will not be valid for internal calls.

> Other Settings



Edit FXS Port - 1

Other Options

□ Call Waiting   □ DND   Ring Out: 5

Follow me

Forward Type: □ Always ☑ No answer ☑ When Busy

Destination: ○ Internal Port ● Hunt Group HuntGroup1(Group1) ○ Number

Prompt: Yes   Music On Hold: Default

Volume Settings

Rxgain: 40%   Txgain: 40%

Fax

As a Fax Machine: No

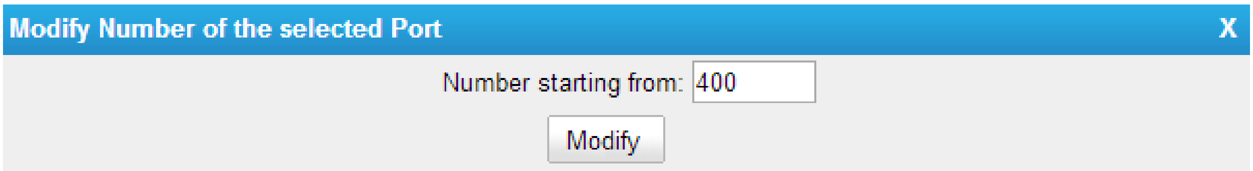
Figure 4-3 FXS Port Other Settings

Table 4-2 Description of FXS Port Other Settings

Items	Description
Call Waiting	Check this option if the extension should have Call Waiting capability. If this option is checked, the “When busy” follow me options will not be available.
DND	Don’t Disturb. When DND is enabled for an extension, the extension will not be available.
Ring Out	Check this option if you want to customize the ring time. Ring tone will stop over the time defined.
Follow me	Call forwarding for an extension can be configured here. You can also configure call forwarding to a hunt group. Prompt: whether the prompt is played or not when the call is transfered. Music On Hold: choose the on hold music.
Volume Settings	Settings for the FXS port volume. Rxgain: adjust receive gain. Txgain: adjust transmit gain.
Fax	If the FXS port is connected to a Fax machine, this option should be checked.

2) Batch Edit Number of FXS Ports

Select the FXS ports, and click the button "Modify Number of the selected Port" Modify Number of the selected Port , you can modify the number of the FXS ports in bulk.



Modify Number of the selected Port X

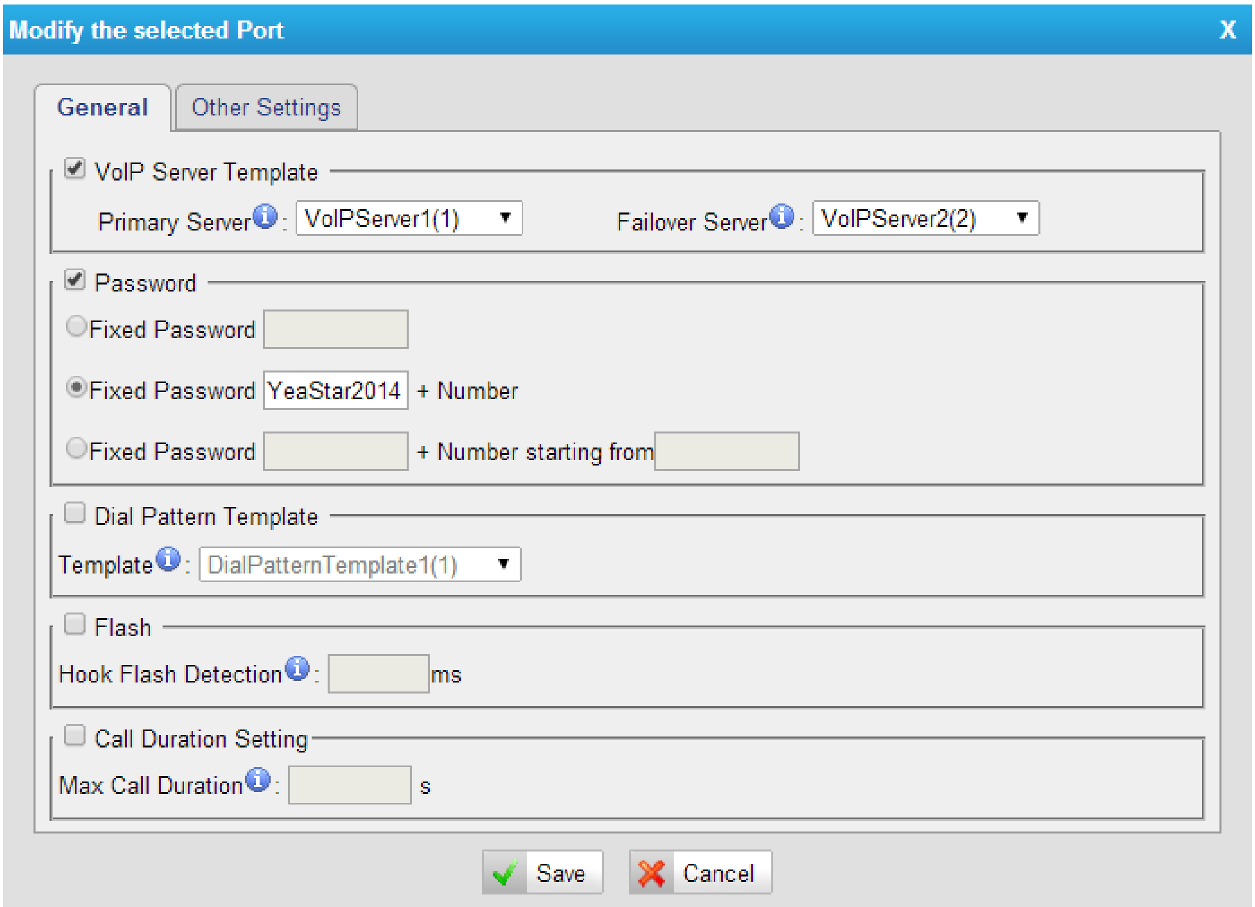
Number starting from: 400

Figure 4-4 Batch Edit Number of FXS Ports

3) Batch Edit FXS Ports

You can also modify the selected FXS ports in bulk by clicking the button "Modify the selected Port" Modify the selected Port .

Check the options that you want to edit. Options that are not checked and modified will remain the default settings.



Modify the selected Port X

☑ VoIP Server Template

Primary Server: VoIPServer1(1) ▼   Failover Server: VoIPServer2(2) ▼

☑ Password

○ Fixed Password

● Fixed Password YeaStar2014 + Number

○ Fixed Password + Number starting from

□ Dial Pattern Template

Template: DialPatternTemplate1(1) ▼

□ Flash

Hook Flash Detection: ms

□ Call Duration Setting

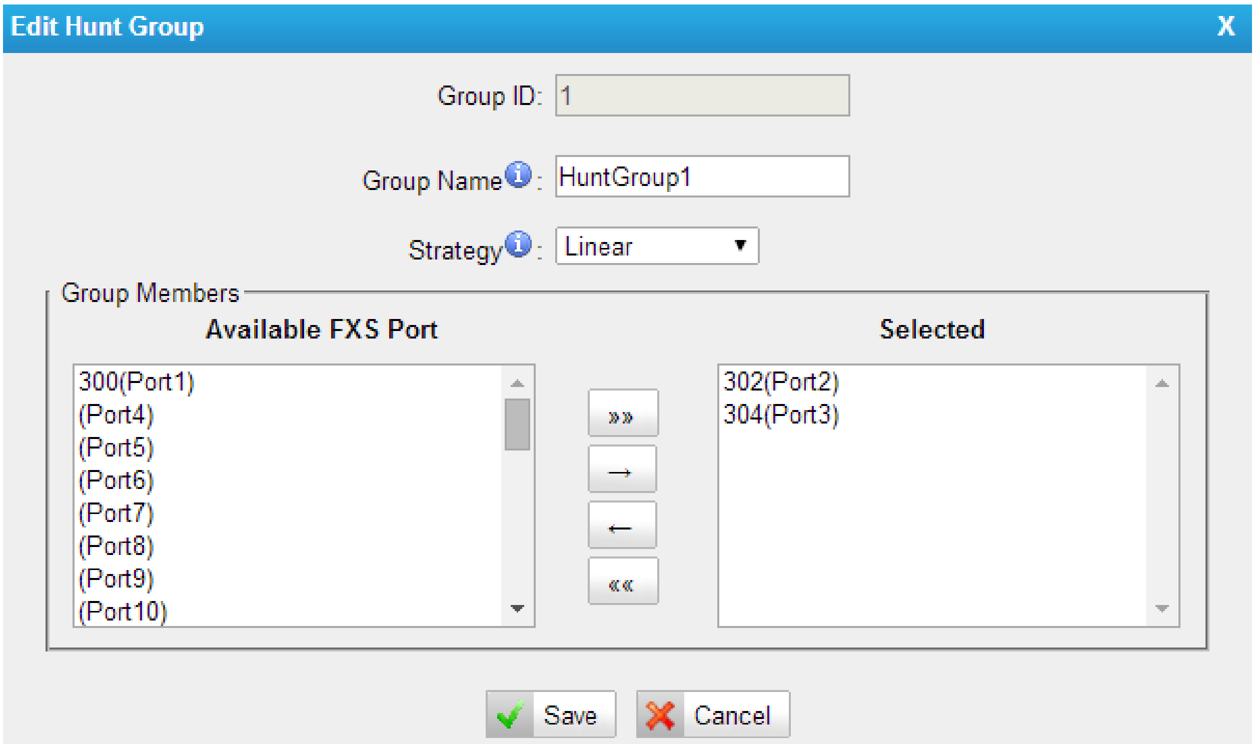
Max Call Duration: s

Figure 4-5 Batch Edit FXS ports

4.1.2 Hunt Group

Hunt group is a feature that allows a call reaching multiple FXS ports. The FXS ports will act as a single group, called a hunt group. The number of hunt groups is limited by the number of ports each NeoGate TA model has. For example, there are 24 hunt groups on NeoGate TA2400.

Hunt group will be chosen when configuring the FXS port "Follow Me". The hunt group will work when a call reaches the FXS port associated user which is busy or no answer.



Edit Hunt Group

Group ID: 1

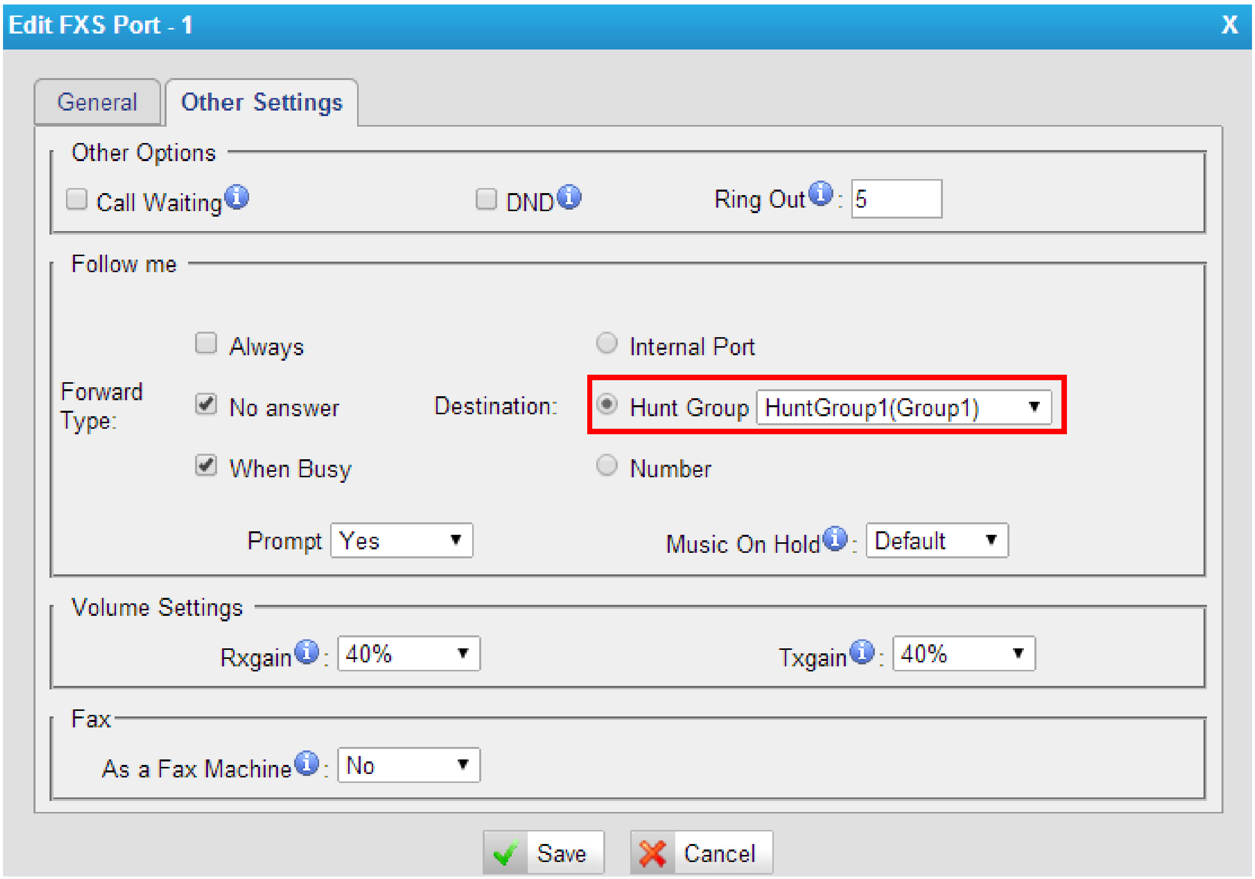
Group Name: HuntGroup1

Strategy: Linear

Group Members

Available FXS Port	Selected
300(Port1)	302(Port2)
(Port4)	304(Port3)
(Port5)	
(Port6)	
(Port7)	
(Port8)	
(Port9)	
(Port10)	

Figure 4-6 Hunt Group



Edit FXS Port - 1

General | Other Settings

Other Options

☐ Call Waiting ☐ DND Ring Out: 5

Follow me

Forward Type: ☐ Always ☑ No answer ☑ When Busy

Destination: ○ Internal Port ● Hunt Group HuntGroup1(Group1) ○ Number

Prompt Yes

Music On Hold: Default

Volume Settings

Rxgain: 40% Txgain: 40%

Fax

As a Fax Machine: No

Figure 4-7 Set Hount Group on "FXS Port" Page

There are 3 strategies for hunt group on NeoGate TA.

- Simultaneous

All the FXS users will ring at the same time.

- Circular

In circular hunting, the calls are processed "round-robin". If a call is delivered to FXS port1, the next call will go to 2, the next to 3. The succession throughout each of the FXS users even if one of the previous local users becomes free. When the end of the hunting group is reached, the hunting starts over at the first local users.

- Linear

Linear hunting is also referred to serial hunting. In linear hunting, calls are always delivered to the first FXS users, unless it is busy, then the second, third, and so on.

4.2 VoIP Settings

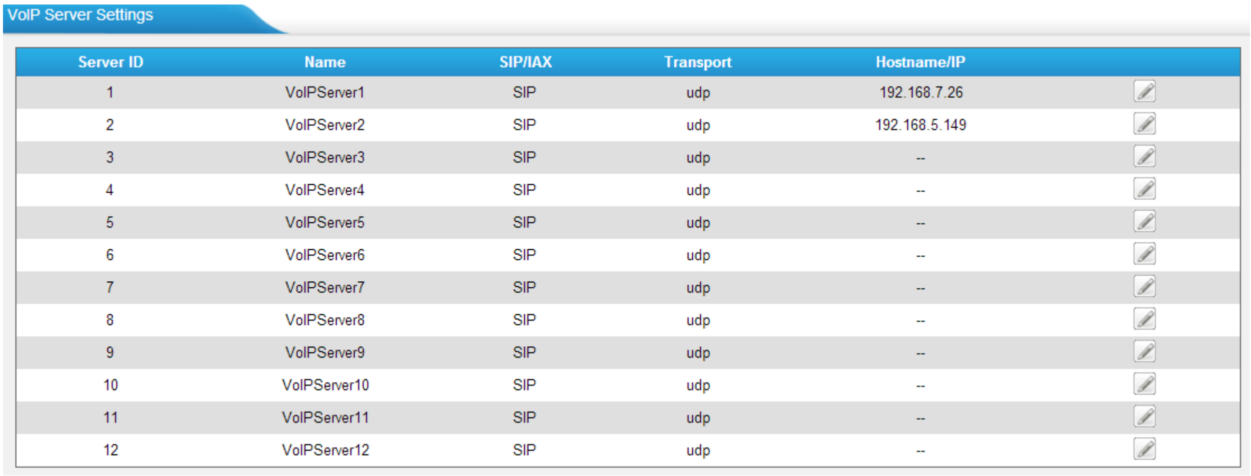
To integrate with other IPPBX, we need to configure the VoIP settings in NeoGate TA to set up VoIP trunk (SIP and IAX).

4.2.1 VoIP Server Settings

There are some configurable VoIP(SIP/IAX) Server templates on this page. The number of VoIP Server templates is the half of FXS ports on NeoGate. The VoIP server settings help the FXS ports to register to the VoIP server. Once configured, the templates can be chosen on FXS port setting page.
Two modes are available for the VoIP server, we call them VoIP mode and SPS(Service Provider SIP)/SPX(Service Provider IAX) mode.

VoIP Mode:
The FXS port will be registered as one the VoIP server's SIP extensions if "Enable Register" is checked on VoIP Server template.

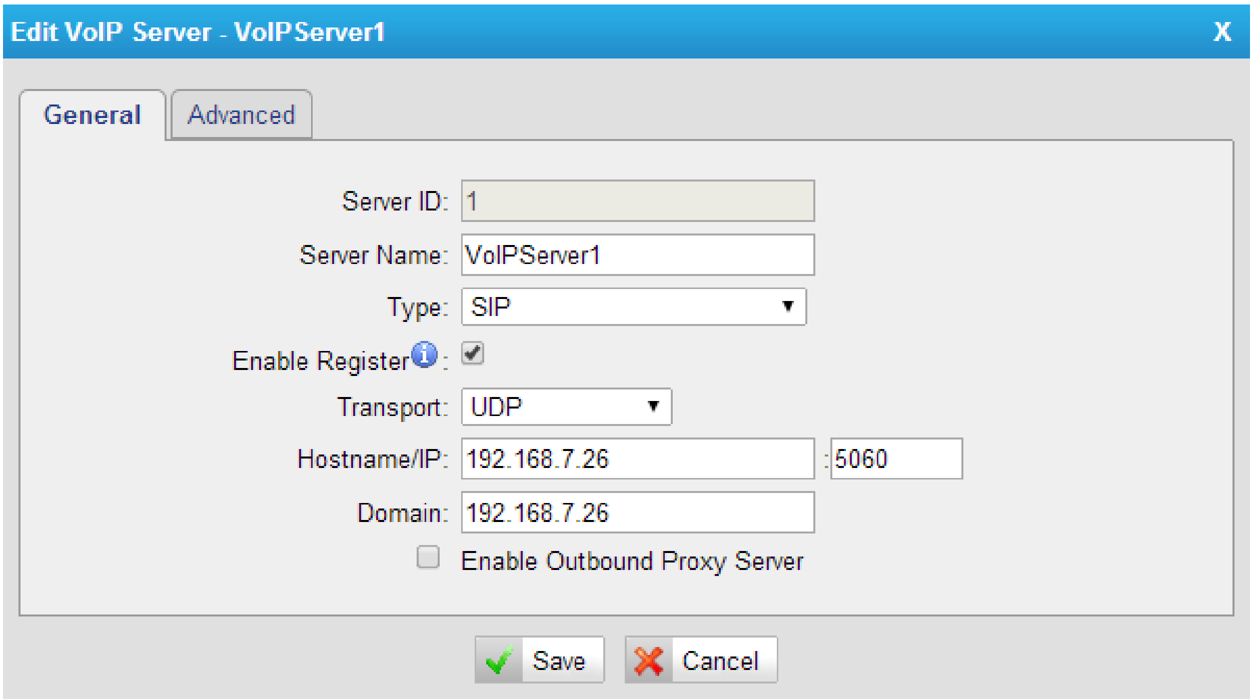
SPS/SPX Mode:
If "Enable Register" is not checked, the FXS port will be registered as a SPS/SPX trunk to the VoIP Server. One SPS/SPX trunk to NeoGate TA also should be created on the VoIP Server.



VoIP Server Settings

Server ID	Name	SIP/IAX	Transport	Hostname/IP	
1	VoIPServer1	SIP	udp	192.168.7.26	✎
2	VoIPServer2	SIP	udp	192.168.5.149	✎
3	VoIPServer3	SIP	udp	--	✎
4	VoIPServer4	SIP	udp	--	✎
5	VoIPServer5	SIP	udp	--	✎
6	VoIPServer6	SIP	udp	--	✎
7	VoIPServer7	SIP	udp	--	✎
8	VoIPServer8	SIP	udp	--	✎
9	VoIPServer9	SIP	udp	--	✎
10	VoIPServer10	SIP	udp	--	✎
11	VoIPServer11	SIP	udp	--	✎
12	VoIPServer12	SIP	udp	--	✎

Figure 4-8 VoIP Server



Edit VoIP Server - VoIPServer1

Server ID: 1

Server Name: VoIPServer1

Type: SIP

Enable Register: ☑

Transport: UDP

Hostname/IP: 192.168.7.26 : 5060

Domain: 192.168.7.26

☐ Enable Outbound Proxy Server

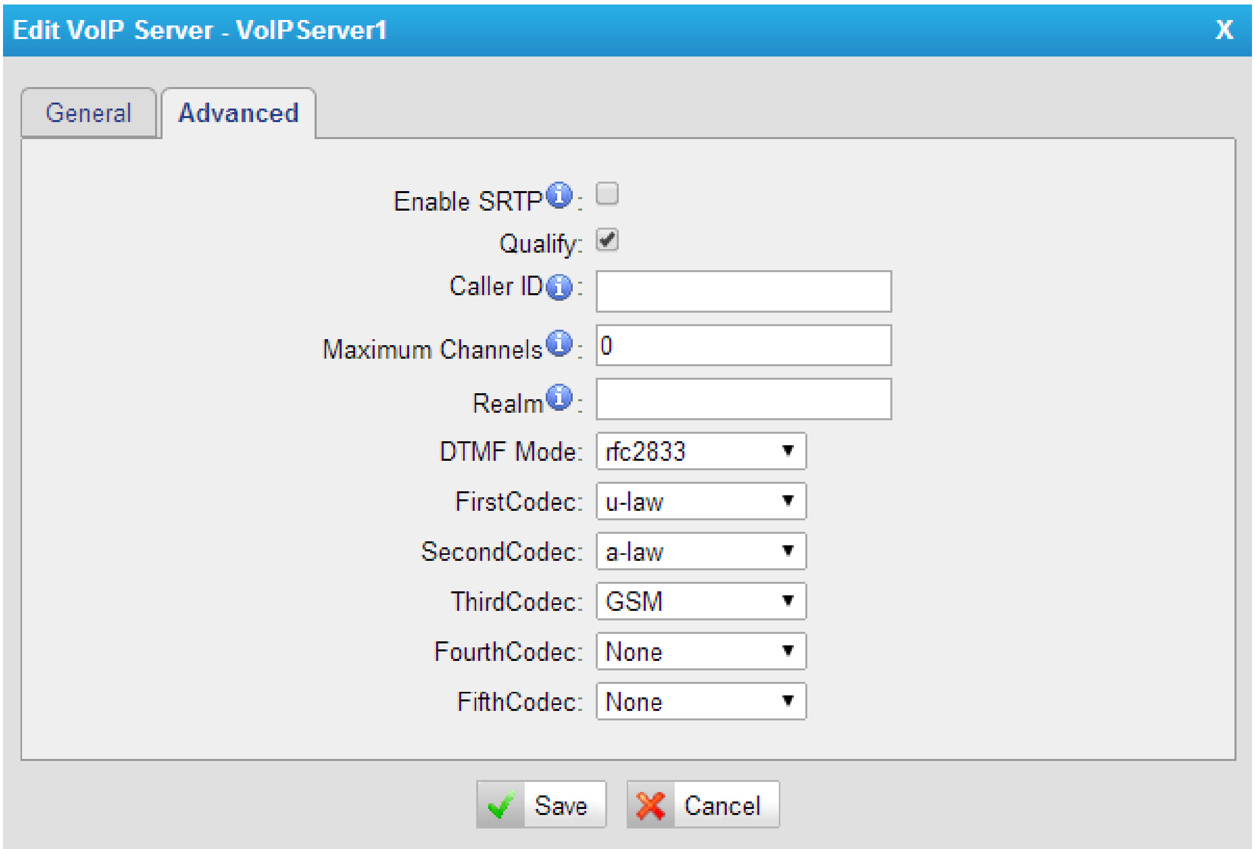
Figure 4-9 VoIP Server Settings

> General

Table 4-3 Description of VoIP Server General Settings

Items	Description
Server ID	The ID for the VoIP server template.
Server Name	The name for the VoIP server template.
Type	Choose the type of the VoIP server, SIP or IAX.
Enabel Register	Do not check "Enable Register", if you want to register the FXS port as a Service Provider SIP (IAX) trunk to the VoIP Server. One Service Provider SIP (IAX) trunk to NeoGate TA also should be created on the VoIP Server. Check "Enable Register" if you want to register the FXS port as an extension of the VoIP server. You will need to enter the relevant user name, password, etc in the FXS port page when using this template.
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), TCP ,and TLS.
Hostname/IP	VoIP server 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 server hostname. An IP address also can be filled here.
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.

> Advanced



Enable SRTP: □

Qualify: ☑

Caller ID:

Maximum Channels: 0

Realm:

DTMF Mode: rfc2833

FirstCodec: u-law

SecondCodec: a-law

ThirdCodec: GSM

FourthCodec: None

FifthCodec: None

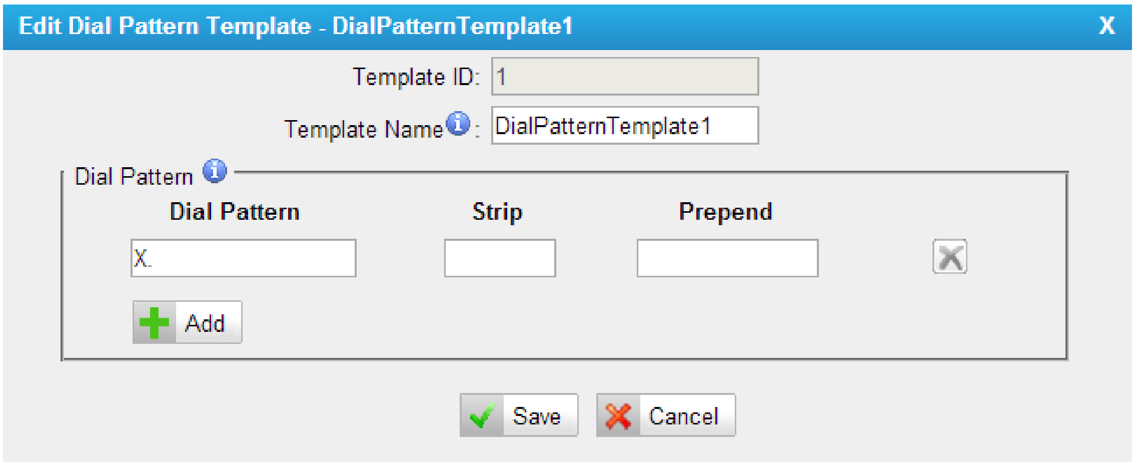
Figure 4-10 VoIP Server Advanced Settings

Table 4-4 Description of VoIP Server Advanced Settings

Items	Description
Enable SRTP	Define if SRTP is enabled for this VoIP server.
Qualify	Send check alive packets to the SIP provider.
Caller ID	Specify the caller ID to use when making outbound calls over this VoIP server.
Maxmum Channels	Control the maximum number of simultaneous calls. Set as 0 to specify no maximum.
Realm	Realm is a string to be displayed to users so they know which username and password to use.
DTMF Mode	Set default mode for sending DTMF of this trunk. Default setting: rfc2833
Codec	Define the codec for this sip trunk and its priority

4.2.2 Dial Pattern Template

Dial pattern template specifying how to route the calls from FXS ports to VoIP server extensions or external numbers. The number of dial pattern templates is limited by the number of ports each NeoGate TA model has.



Edit Dial Pattern Template - DialPatternTemplate1

Template ID: 1

Template Name: DialPatternTemplate1

Dial Pattern

Dial Pattern	Strip	Prepend
X.		

Figure 4-11 Dial Pattern Template

Table 4-5 Description of Dial Pattern Template Settings

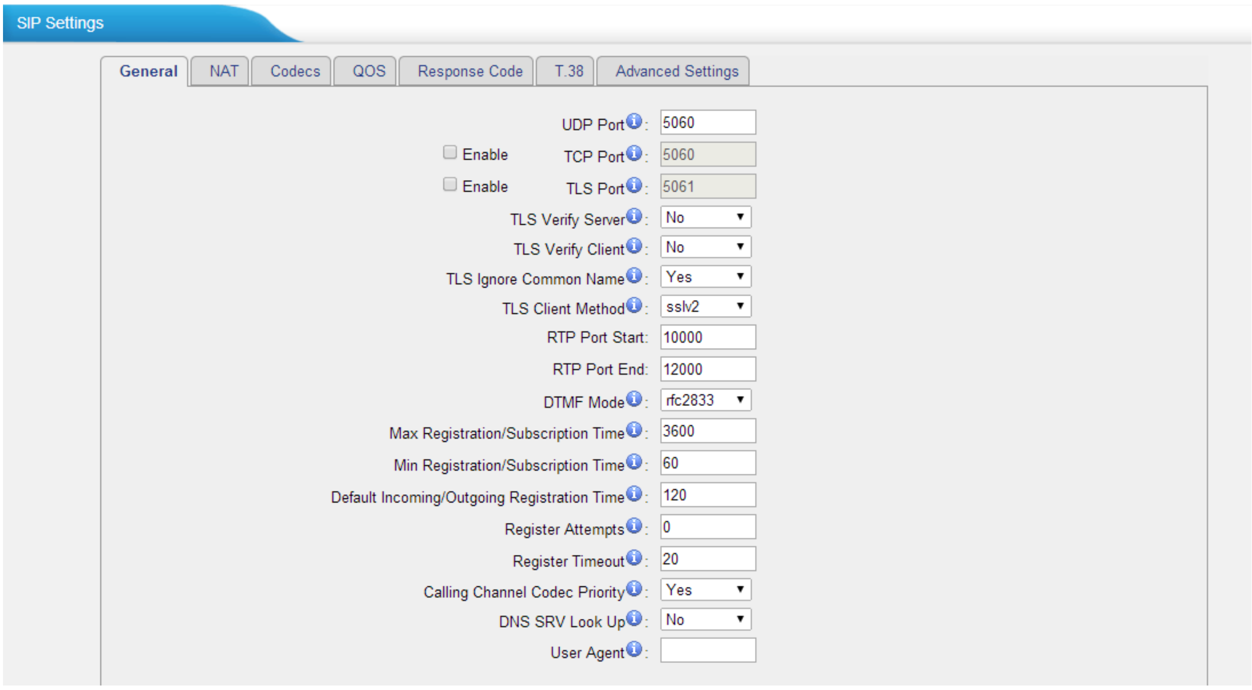
Items	Description
Template ID	The ID for this template.
Template Name	A name for this template.
Dial Pattern	Calls from the FXS port should match the dial pattern set on this template, or the call cannot be established. Hover the pointer over ⓘ to read tips.
Strip	Allows the user to specify the number of digits that will be stripped from the front of the phone number before the call is placed.
Prepend	The digits will be appended to the phone number before the call is placed.

DTMF Mode	Set default mode for sending DTMF of this trunk. Default setting: rfc2833.
Codec	Define the codec for this sip trunk and its priority.

4.2.3 SIP Settings

This is the SIP settings in NeoGate, including General settings, NAT, Codecs, Qos, Response Code, T.38, and advanced settings.

1) General



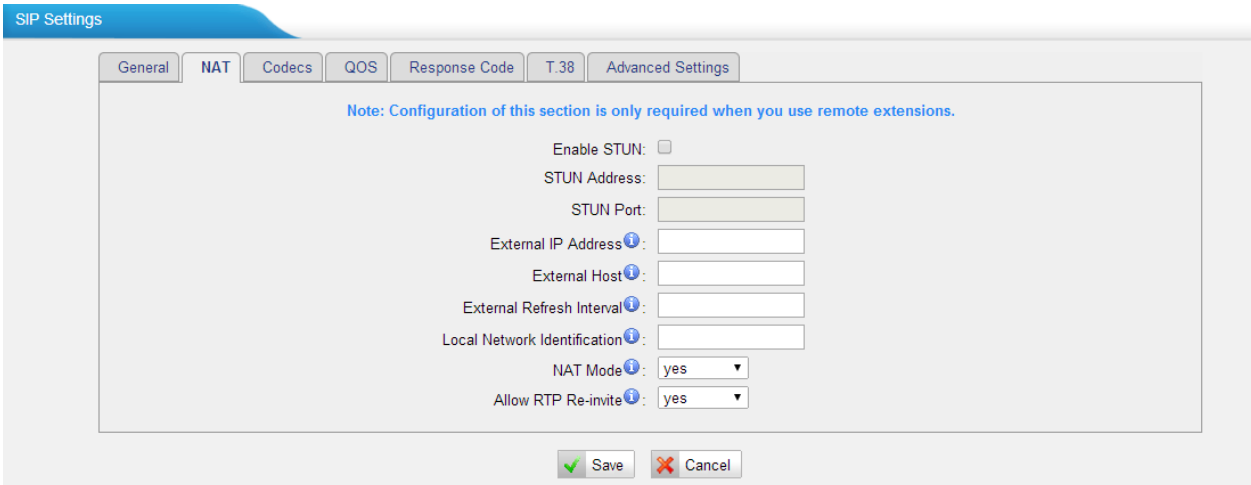
UDP Port: 5060
□ Enable TCP Port: 5060
□ Enable TLS Port: 5061
TLS Verify Server: No
TLS Verify Client: No
TLS Ignore Common Name: Yes
TLS Client Method: sslv2
RTP Port Start: 10000
RTP Port End: 12000
DTMF Mode: rfc2833
Max Registration/Subscription Time: 3600
Min Registration/Subscription Time: 60
Default Incoming/Outgoing Registration Time: 120
Register Attempts: 0
Register Timeout: 20
Calling Channel Codec Priority: Yes
DNS SRV Look Up: No
User Agent:

Figure 4-12 SIP General Settings

Table 4-6 Description of SIP General Settings

Items	Description
UDP Port	Port used for SIP registrations. The default is 5060.
TCP Port	Port used for SIP registrations. The default is 5060.
TLS Port	Port used for SIP registrations. The default is 5061.
TLS Verify Server	When using NeoGate TA as a TLS client, whether or not to verify server's certificate. It is "No" by default.
TLS Verify Client	When using NeoGate TA 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 TA as TLS client, specify the protocol for outbound TLS connections. You can select it as tlsv1, sslv2 or sslv3.
RTP Port Start	Beginning of the RTP port range.
RTP Port End	End of the RTP port range.
DTMF Mode	Set the default mode for sending DTMF. Default setting: rfc2833
Max Registration/Subscription Time	Maximum duration (in seconds) of a SIP registration. The default is 3600 seconds.
Min Registration/Subscription Time	Minimum duration (in seconds) of a SIP registration. The default is 60 seconds.
Default Incoming/Outgoing Registration Time	Default Incoming/Outgoing Registration Time: the 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. The default is 0 (no limit).
Register Timeout	Number of seconds to wait for a response from a SIP Registrar before classifying the register has timed out. The 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 preferentially. If not, NeoGate TA will follow the priority order in your SIP/SPS trunks.
Video Support	Support SIP video or no. The 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 TA"; you can change it if needed.

2) NAT



Note: Configuration of this section is only required when you use remote extensions.

Enable STUN: □

STUN Address:

STUN Port:

External IP Address:

External Host:

External Refresh Interval:

Local Network Identification:

NAT Mode: yes

Allow RTP Re-invite: yes

Figure 4-13 NAT Settings

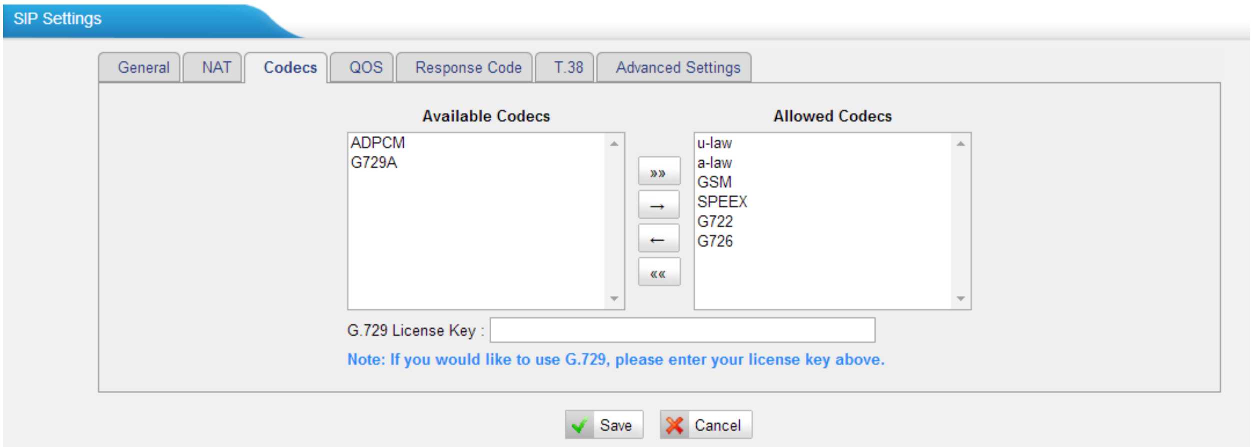
Table 4-7 Description of SIP General Settings

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 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) Codecs

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



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

Figure 4-14 Codecs

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.

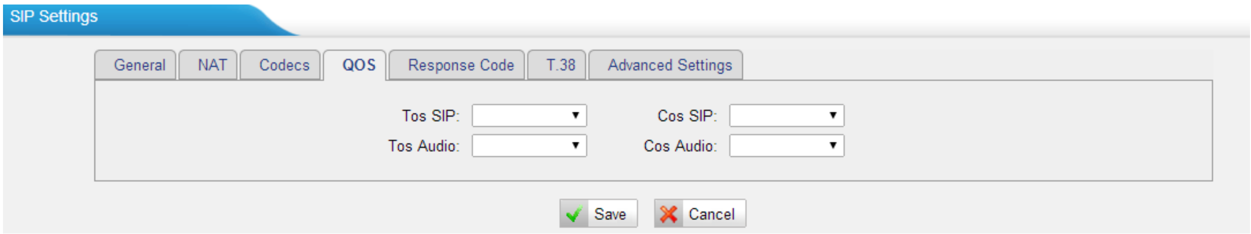


Figure 4-15 Qos

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

5) Response Code

You can change the response code on NeoGate TA to the one you want before sending it to the VoIP server. It helps the VoIP server understands better the exact call status, like busy, no response and others.

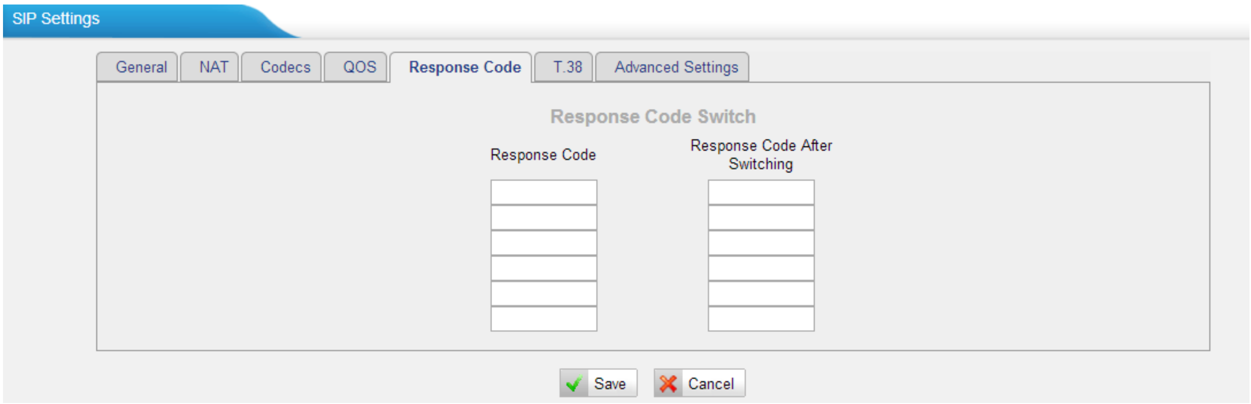
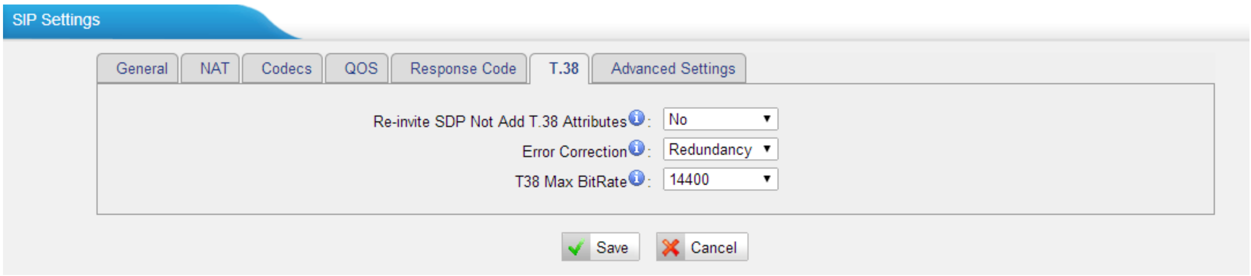


Figure 4-16 Response Code

Note: We don’t’ recommend configuing this if you are not familiar with the code of call status from the VoIP server.

6) T.38

Settings on this page is for the purpose of improving receiving and sending T.38 FAX.



Re-invite SDP Not Add T.38 Attributes: No

Error Correction: Redundancy

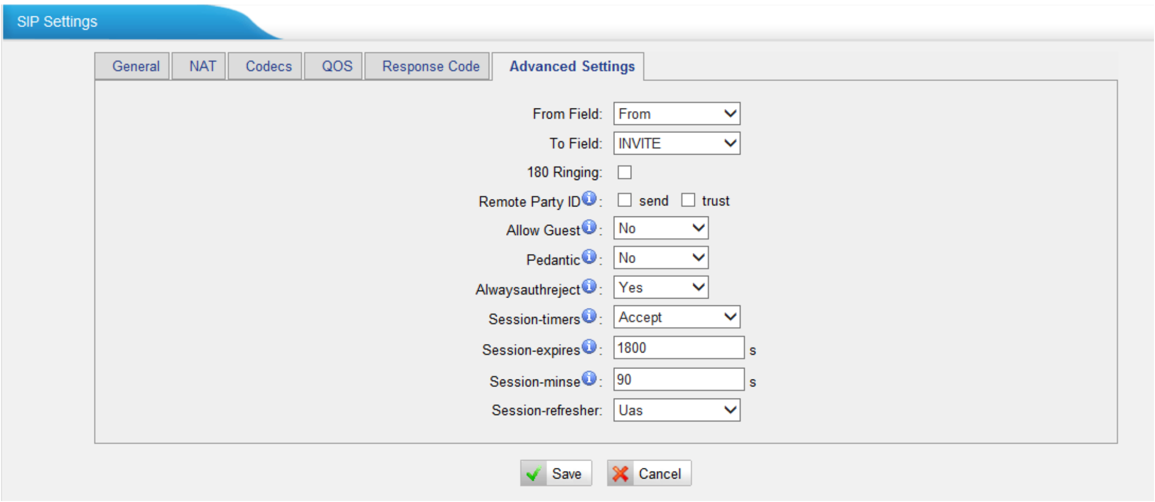
T38 Max BitRate: 14400

Figure 4-17 T.38 Settings

Table 4-8 Description of T.38 Settings

Items	Description
Re-invite SDP Not Add T.38 Attributes	If set to Yes, SDP in re-invite packet will not add T.38 attributes.
Error Correction	Re-invite SDP T38FaxUdpEc.
T.38 Max Bit Rate	Set T38 Max Bit Rate.

7) Advanced Settings



From Field: From

To Field: INVITE

180 Ringing: □

Remote Party ID: □ send □ trust

Allow Guest: No

Pedantic: No

Alwaysauthreject: Yes

Session-timers: Accept

Session-expires: 1800 s

Session-minse: 90 s

Session-refresher: Uas

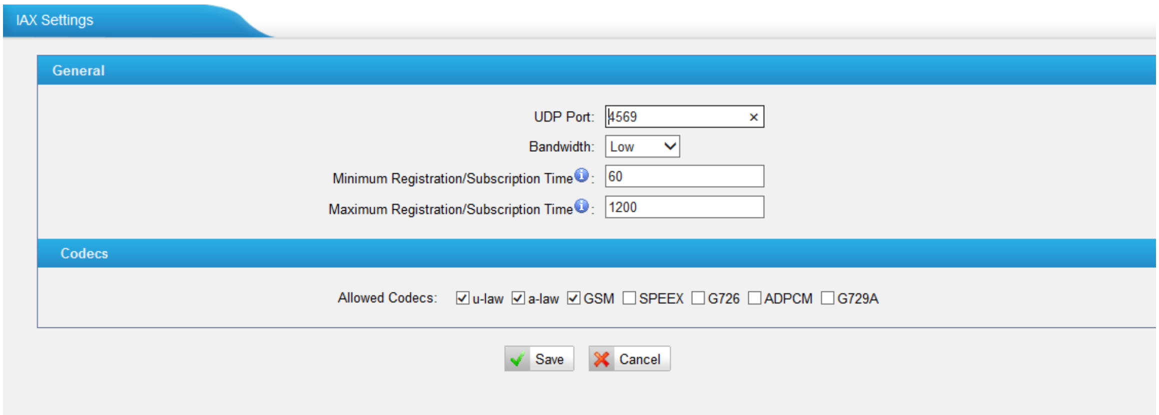
Figure 4-18 SIP Advanced Settings

Table 4-9 Description of SIP Advanced Settings

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 to send Remote-Party-ID on SIP header or not. Default: no.
Allow Guest	Whether to allow anonymous registration extension or not. Default: no. It’s recommended that it is disabled for security reason.
Pedantic	Enable pedantic parameter. Default: no.
Alwaysauthreject	If enabled, when NeoGate TA rejects “Register” or “Invite” packets, NeoGate TA always respond the packets using “SIP404 NOT FOUND”. It’s recommended that it is enabled for security reason.
Session-timers	Enable session-timer mode, default: yes. If you find 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 the session-refresher, the default is Uas.

4.2.4 IAX Settings

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



UDP Port: 4569
Bandwidth: Low
Minimum Registration/Subscription Time: 60
Maximum Registration/Subscription Time: 1200

Allowed Codecs: ☑ u-law ☑ a-law ☑ GSM □ SPEEX □ G726 □ ADPCM □ G729A

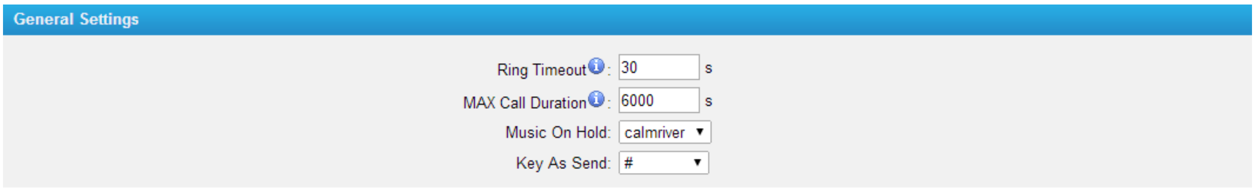
Figure 4-19 IAX Settings

Table 4-10 Description of IAX Settings

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.

4.3 Gateway Settings

4.3.1 General Preferences



General Settings

Ring Timeout: 30 s

MAX Call Duration: 6000 s

Music On Hold: calmriver

Key As Send: #

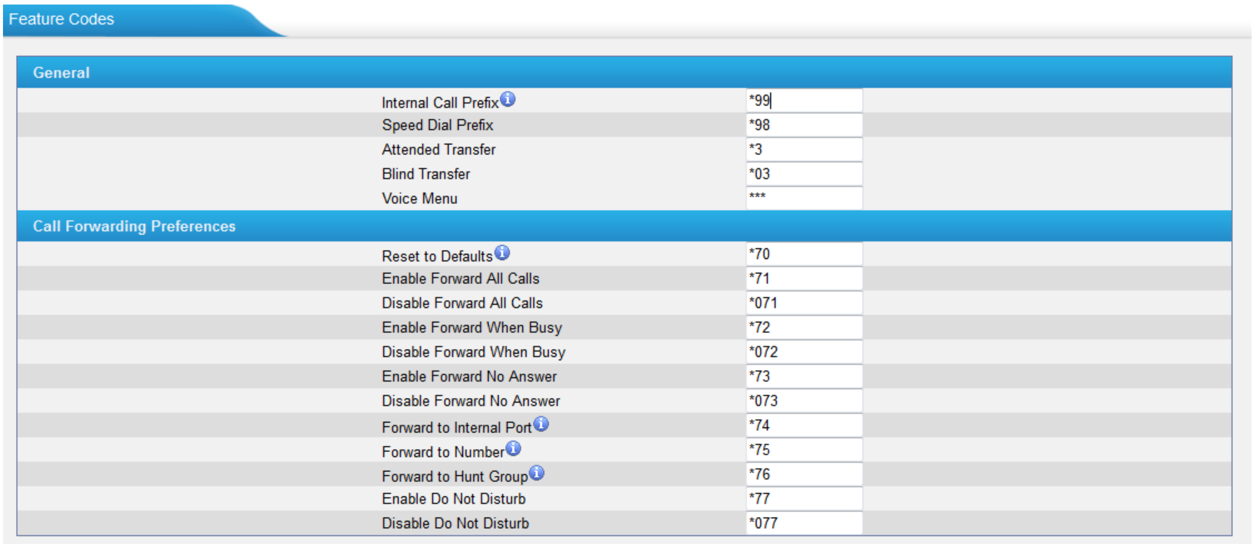
Figure 4-20 General Settings

Table 4-11 Description of General Settings

Items	Description
Ring Timeout	Number of seconds to ring a device before executing the "Follow me" configurations. This is a gloable setting for all FXS ports.
MAX Call Duration	The absolute maximum amount of time permitted for a call. A setting of 0 disables the timeout.
Music On Hold	Set hold music for the system.
Key As Send	Set the "#" or "*" to perform as a send key while dialing. Default is "#".

4.3.2 Feature Codes

There are various feature codes on NeoGate TA. The feature codes are used to acquire the gateway info or activate and inactivate supplementary services. The default feature codes are illustrated below. The parameters for feature codes are configurable.



Feature Codes

General

Internal Call Prefix	*99
Speed Dial Prefix	*98
Attended Transfer	*3
Blind Transfer	*03
Voice Menu	***

Call Forwarding Preferences

Reset to Defaults	*70
Enable Forward All Calls	*71
Disable Forward All Calls	*071
Enable Forward When Busy	*72
Disable Forward When Busy	*072
Enable Forward No Answer	*73
Disable Forward No Answer	*073
Forward to Internal Port	*74
Forward to Number	*75
Forward to Hunt Group	*76
Enable Do Not Disturb	*77
Disable Do Not Disturb	*077

Figure 4-21 Feature codecs

> General

Table 4-12 Description of General Settings

Items	Default	Description
Internal Call Prefix	*99	Dial the feature code and the FXS port number when making calls between the analog phones connected to multiple ports of the NeoGate TA without the use of a VoIP server.
Speed Dial Prefix	*98	The prefix number for applying a speed dialing. The prefix should be added ahead of the speed dial number.
Attended Transfer	*3	Users may transfer an incoming call by dialing *3 on their phone.
Blind Transfer	*03	Users may blind transfer an incoming call by dialing*03 on their phone.
Voice Menu	***	Users may enter the voice prompt menu by pressing *** on their phone.

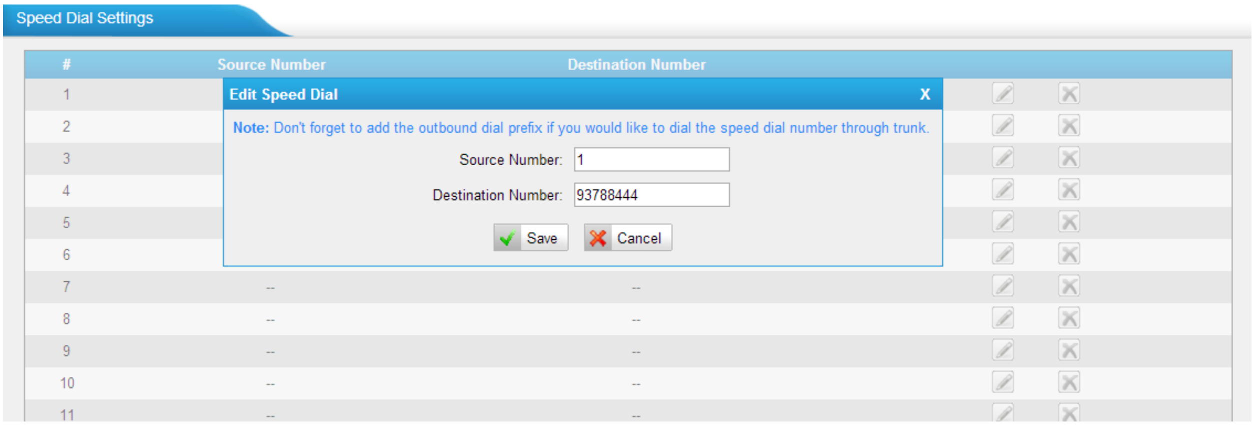
> Call Forwarding Preferences

Table 4-13 Description of Call Forwarding Preferences

Items	Default	Description
Reset to Defaults	*70	Users may reset all call forwarding defaults by calling *70 on their phone.
Enabel Forward All Calls	*71	Users may enable always forward by calling *71 on their phone.
Disable Forward All Calls	*071	Users may disable always forward by calling *071 on their phone.
Enable Forward When Busy	*72	Users may enable busy forward by dialing *72 on their phone.
Disable Forward When Busy	*072	Users may disable busy forward by calling *072 on their phone.
Enable Forward No Answer	*73	Users may enable no answer forward by calling *73 on their phone.
Disable Forward No Answer	*073	Users may disable no answer forward by calling *073 on their phone.
Forward to Internal Port	*74	Users may activate call forwarding to port by dialing this feature code, followed by the FXS port number.
Forward to Number	*75	Users may activate call forwarding by dialing this feature code, followed by the extension or phone number to forward all calls to this number. **Note**: Users may activate Forward to number by dialing *74 + phone number. E.g. by dialing *74501, all calls will be forwarded to extension 501.
Forward to Hunt Group	*76	Users may forward the call to a hunt group by calling *75 on their phone.
Enable Do Not Disturb	*77	Activate "Do Not Disturb". Once activated, the FXS port will reject all incoming calls.
Disable Do Not Disturb	*077	Disable "Do Not Disturb" for the FXS port by pressing the feature code on the phone. It will recover normal ringing upon the arrival of incoming calls.

4.3.3 Speed Dial Settings

There are 128 configurable Speed Dial templates available on NeoGate TA.



Speed Dial Settings

#	Source Number	Destination Number
1		
2		
3		
4		
5		
6		
7	--	--
8	--	--
9	--	--
10	--	--
11	--	--

Edit Speed Dial X

Note: Don't forget to add the outbound dial prefix if you would like to dial the speed dial number through trunk.

Source Number: 1

Destination Number: 93788444

Figure 4-22 Speed Dial

·Source Number

The speed dial number.

·Destination Number

The number you want to call.

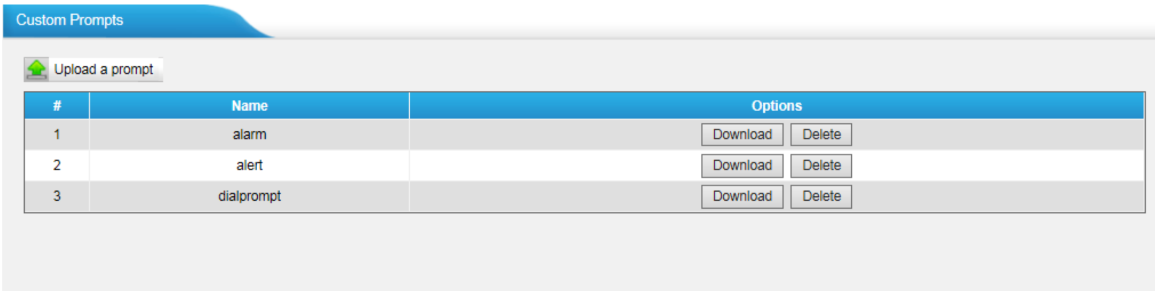
E.g. the source number is “1”. The destination number is 93788444. The prefix number is *98. You can use an extension with any type to dial *981, then it will call the number 93788444.

Note: Don’t forget to add the dial pattern according to the selected dial pattern template.

4.4 Audio Settings

4.4.1 Custom Prompts

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



Custom Prompts

#	Name	Options
1	alarm	Download Delete
2	alert	Download Delete
3	dialprompt	Download Delete

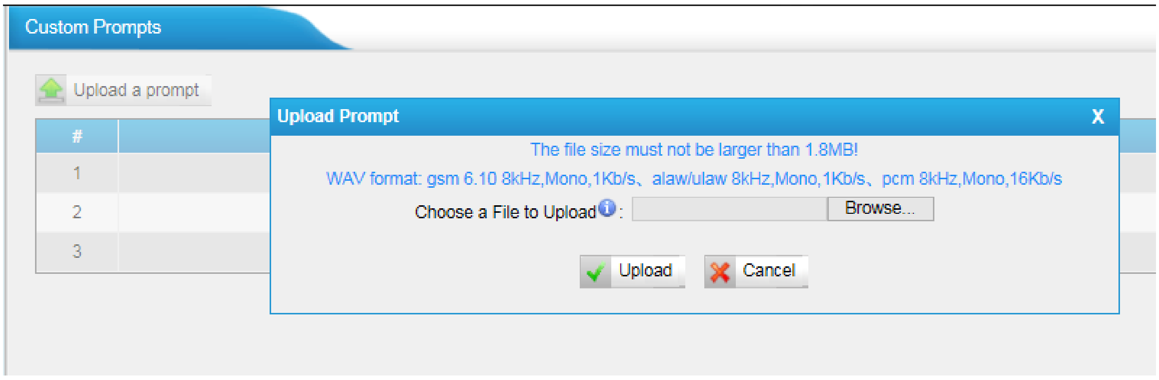
Figure 4-23 Custom Prompts

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.



Custom Prompts

Upload a prompt

#	
1	
2	
3	

Upload Prompt X

The file size must not be larger than 1.8MB!

WAV format: gsm 6.10 8kHz,Mono,1Kb/s、alaw/ulaw 8kHz,Mono,1Kb/s、pcm 8kHz,Mono,16Kb/s

Choose a File to Upload: Browse...

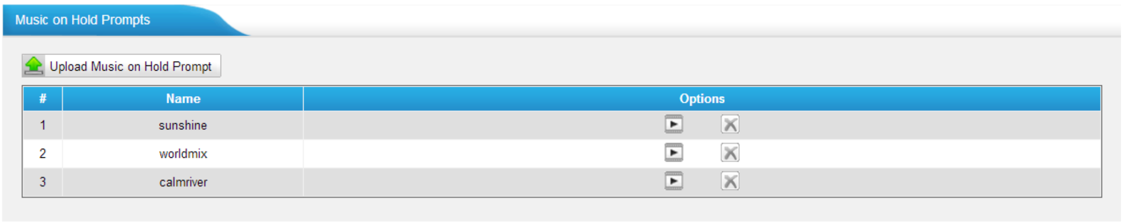
Upload Cancel

Figure 4-24 Upload A Prompt

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.

4.4.2 Music on Hold Prompts

In this page, we can upload the music on hold prompts.



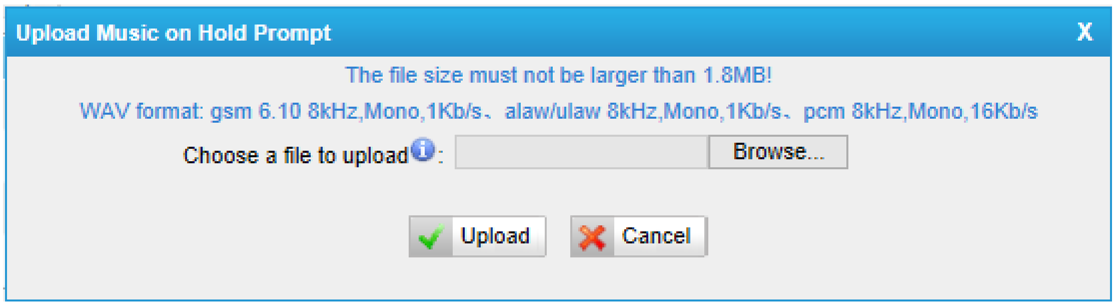
Music on Hold Prompts

Upload Music on Hold Prompt

#	Name	Options
1	sunshine	▶ ☒
2	worldmix	▶ ☒
3	calmriver	▶ ☒

Figure 4-25 Music On Hold

The administrator can upload on hold music as follows:
1) Click “Upload Music on Prompt”.
2) Click “Browse” to choose the desired audio file.
3) Click “Upload” to upload the selected file.



Upload Music on Hold Prompt X

The file size must not be larger than 1.8MB!

WAV format: gsm 6.10 8kHz,Mono,1Kb/s、alaw/ulaw 8kHz,Mono,1Kb/s、pcm 8kHz,Mono,16Kb/s

Choose a file to upload: Browse...

Upload Cancel

Figure 4-26 Upload Music on Hold Prompt

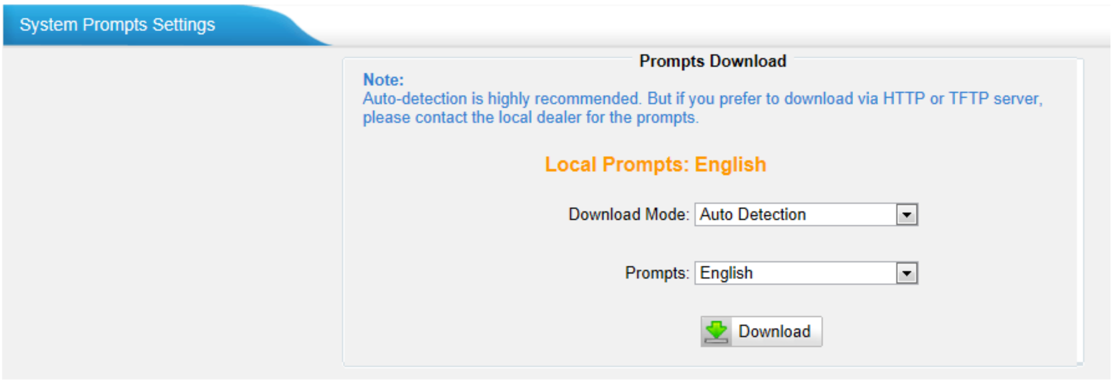
Note: The file size must not be larger than 1.8 MB, and the file must be WAV format:
GSM 6.10 8 kHz, Mono, 1 Kb/s;
Alaw/Ulaw 8 kHz, Mono, 1 Kb/s;
PCM 8 kHz, Mono, 16 Kb/s.

4.4.3 System Prompts Settings

There are multilingual system prompts on NeoGate TA. You can download the appropriate language you need. NeoGate TA can support American English, Australian English, Chinese, Dutch, French, Canadian French, German, Greek, Hungarian, Italian, Polish, Portuguese, Brazilian Portuguese, Russian, Spanish, Mexican Spanish, Turkish, Thai, and Korean currently.

Notes:

1. Auto-detection is highly recommended. But if you prefer to download via HTTP or TFTP server, please contact the local dealer for the prompts.
2. When update successfully, just click “Apply Changes” on Web then it will take effect, there is no need to reboot.



System Prompts Settings

Prompts Download

Note:
Auto-detection is highly recommended. But if you prefer to download via HTTP or TFTP server, please contact the local dealer for the prompts.

Local Prompts: English

Download Mode: Auto Detection

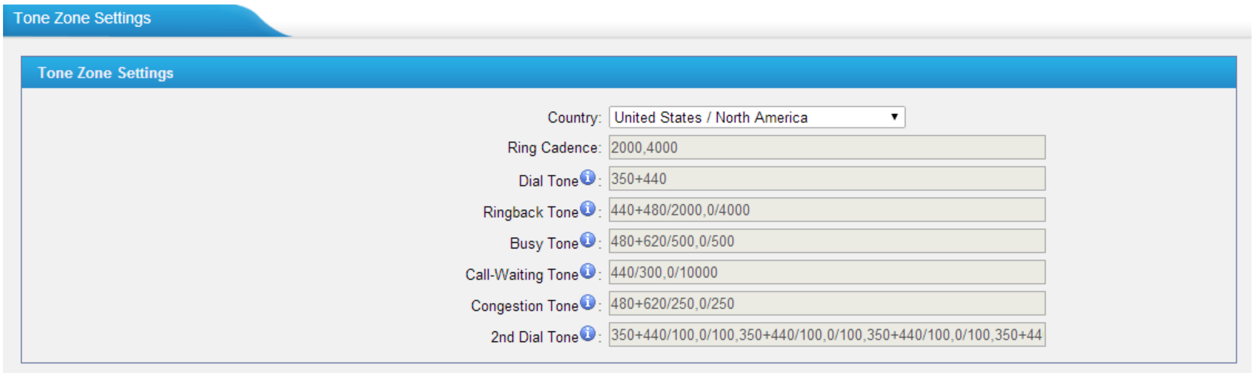
Prompts: English

Figure 4-27 System Prompts Settings Page

4.5 Advanced Settings

4.5.1 Tone Zone Settings

Advanced ring tones for all the FXS ports can be configured on this page. There are pre-grogrammed tone zone settings for some countries and regions. Users can simply find and select thier country to get tone zone settings for the gateway.



Tone Zone Settings

Tone Zone Settings

Country: United States / North America

Ring Cadence: 2000,4000

Dial Tone: 350+440

Ringback Tone: 440+480/2000,0/4000

Busy Tone: 480+620/500,0/500

Call-Waiting Tone: 440/300,0/10000

Congestion Tone: 480+620/250,0/250

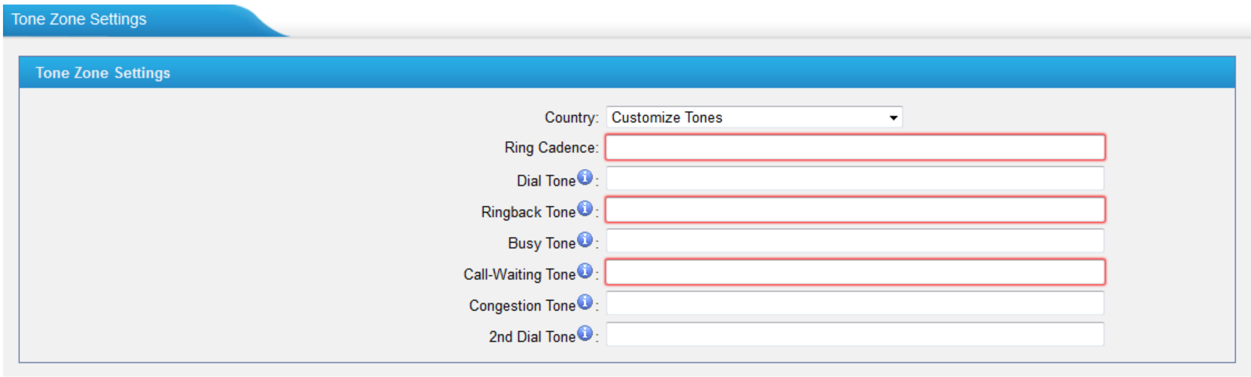
2nd Dial Tone: 350+440/100,0/100,350+440/100,0/100,350+440/100,0/100,350+44

Figure 4-28 Tone Zone Settings

Users may also configure the tone zone according to the national standard by selecting

"User custom for Tone Zone". Please refer to the document below and configure the tone zone settings on NeoGate TA:

http://www.itu.int/ITU-T/inr/forms/files/tones-0203.pdf



Tone Zone Settings

Tone Zone Settings

Country: Customize Tones

Ring Cadence:

Dial Tone:

Ringback Tone:

Busy Tone:

Call-Waiting Tone:

Congestion Tone:

2nd Dial Tone:

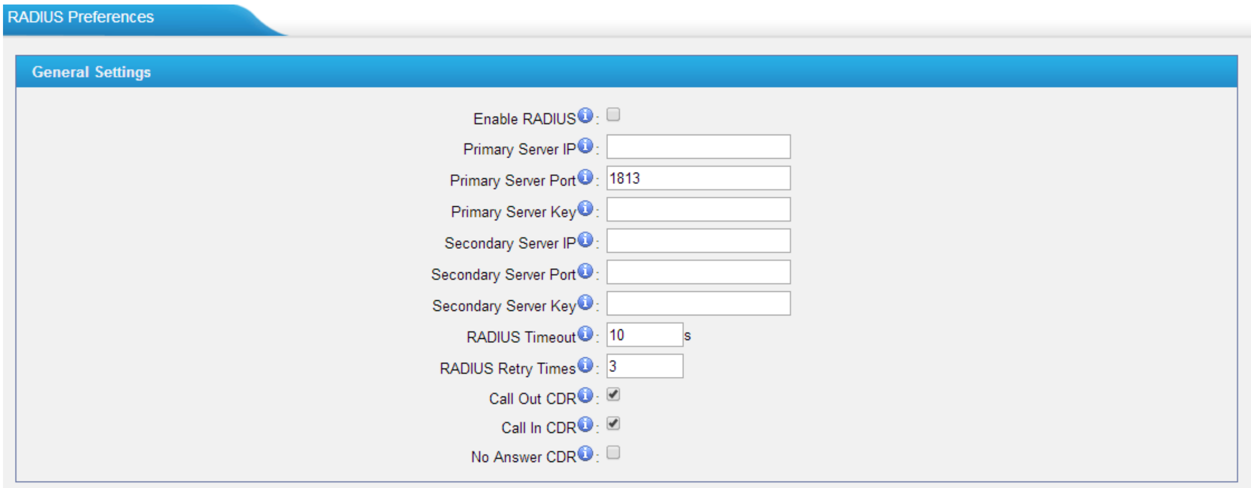
Figure 4-29 Customize Tones

Table 4-14 Description of Tone Zone Settings

Items	Description
Country	Choose the country to get pre-programmed tone zone settings or choose "User custom for Tone Zone" to configure the settings manually.
Ring Cadence	Configuration option for all FXS ports ring cadence for all incoming calls.
Dial Tone	Prompt tone of off-hook dial tone.
Ringback Tone	The tone sent to caller when ringing is on.
Busy Tone	Used for busy line prompt.
Call-Waiting Tone	Used for notification in call waiting.
Congestion Tone	Used to indicate that an invalid code has been dialed, or that all circuits (trunks) are busy and/or the call is unroutable.
2nd Dial Tone	Used for the second stage dial tone.

4.5.2 RADIUS Settings

NeoGate TA supports RADIUS (Remote Authentication Dial In User Service) protocol. RADIUS feature is mainly for billing purpose on NeoGate TA. There are primary and secondary RADIUS server configurations available. Once the primary server is unreachale, the RADIUS requests will be sent to the secondary server.



RADIUS Preferences

General Settings

Enable RADIUS: □
Primary Server IP:
Primary Server Port: 1813
Primary Server Key:
Secondary Server IP:
Secondary Server Port:
Secondary Server Key:
RADIUS Timeout: 10 s
RADIUS Retry Times: 3
Call Out CDR: ☑
Call In CDR: ☑
No Answer CDR: □

Figure 4-30

Table 4-15 Description of RADIUS Settings

Items	Description
Enable RADIUS	Enable RADIUS on NeoGate TA.
Primary Server IP	Set IP address of the primary server.
Primary Server Port	Default is 1813. Specifies the port to be used for the primary RADIUS account.
Primary Server Key	Specifies the key to be used to authenticate the RADIUS connection to the Primary server. The key is set according to the RADIUS server.
Secondry Server IP	Set IP address of the primary server. The second sever will be activated the primary one becomes unusable.
Secondry Server Port	Default is 1813. Specifies the port to be used for the second RADIUS account.
Secondry Server Key	Specifies the key to be used to authenticate the RADIUS connection to the second server. The key is set according to the RADIUS server.
RADIUS Timeout	Specifies the number of seconds to wait for a response after the RADIUS message is sent to the server. Default: 10 seconds. The retransmission will be performed if there is no response after the timeout.
RADIUS Retry Times	Specifies the number of times the RADIUS messages will send to the RADIUS server before giving up. Default: 3.
Call Out CDR	Whether to send "Call Out CDR" to RADIUS server or not.
Call In CDR	Whether to send "Call In CDR" to RADIUS server or not.
No Answer CDR	Whether to send "Call Out CDR" to RADIUS server or not.

Part II. Basic Operations

Here are instructions about how to operate on analog phones connected to NeoGate TA to use some features.

1. Inter-port Call

NeoGate TA supports inter-port calls between the phones which are connected to FXS ports of NeoGate TA. Achieve it by simply pressing the "Internal Call Extra" feature code (default *99) + the FXS port number on the phone.

Note: You need add digit 0 before the FXS port number if the port number is between 1 and 9.

For example, to make a call from the phone which is connected to NeoGate TA FXS port 1 to another phone which is connected to FXS port2, you need to dial *9902 on the phone. The user connected to port 16 can be reached by dialing *9916 on the phone.

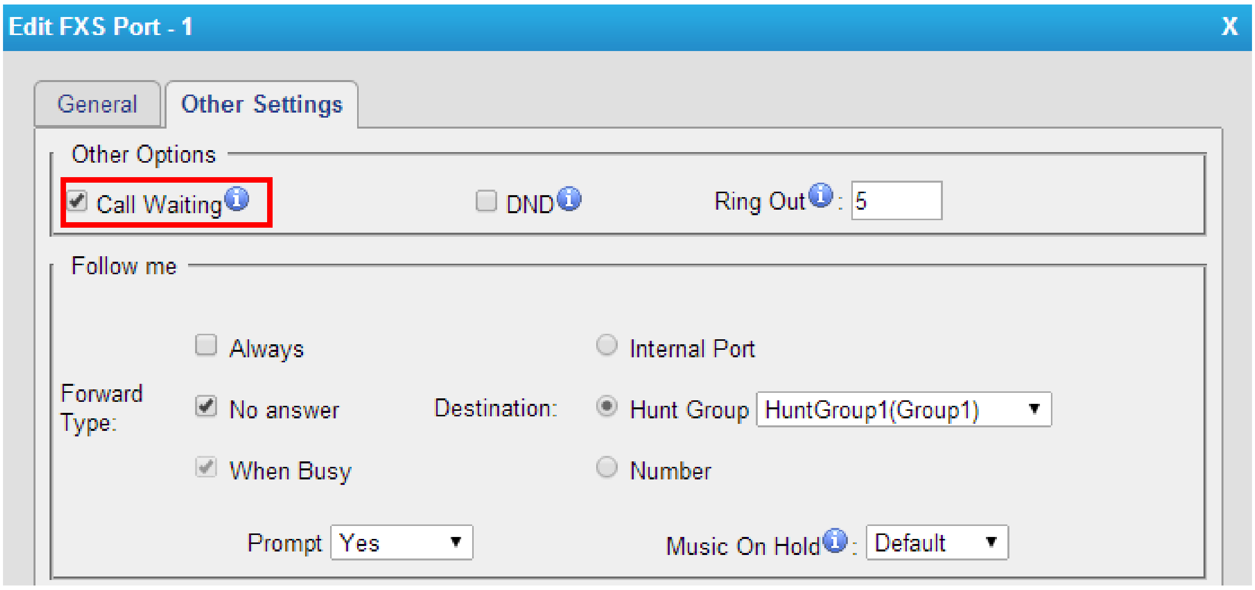
2. Call Hold

An active call can be held by pressing "flash" key on the analog phone. Press the key again to resume the call.

If there is no "flash" key on the phone, you can use "hook flash" (quickly toggle on-off hook) to hold a call. The call may be disconnected by chance if using "hook flash".

3. Call Waiting

If the call waiting is activated for the FXS port, the FXS user who is in a call can hear a call waiting tone "beep" when there is a new incoming call. The user can press "hook flash" to toggle between the active call and the incoming call.



Other Options

☑ Call Waiting □ DND Ring Out: 5

Follow me

Forward Type: □ Always ☑ No answer ☑ When Busy

Destination: ○ Internal Port ● Hunt Group HuntGroup1(Group1) ○ Number

Prompt: Yes Music On Hold: Default

Figure 1-1 Enable "Call Waiting" on FXS Port Page

4. Call Transfer

Blind transfer and attended transfer are supported on NeoGate TA. Users can achieve call transfer by pressing the feature code during the call.

Blind Transfer
Default feature code: *03
1. Dial "*03" during the call;
2. Dial the called number after hearing a prompt "transfer";
3. The call will be transferred after the number is dialed.

Attended Transfer
Default feature code: *3
1. Dial "*3" during the call;
2. Dial the called number after hearing a prompt "transfer";
3. Talk to the transfer recipient;
4. The call will be transferred after hanging up.

5. Three-party Conference

Users can make a three-party conference call on NeoGate TA.
Assuming that A and B are in the call and B wants to invite C to a conference. Please check the following steps of how to establish a conference.

1. B presses "flash" key or taps hook flash to get a dial tone; A will hear the on hold music meanwhile;
2. B dials C's number;
3. If C answers the call, then B presses "flash" key or tap hook flash, the conference will be established, including A, B, and C.
4. If there is no answer on C, A can press "flash" key or tap hook flash to resume the call with A.
5. C will be ejected if B presses "flash" key or taps flash hook during the conference call.

[End]