NeoGate TA1610

User Manual

Version 40.18.0.11

Yeastar Information Technology Co. Ltd

Table of Contents

Introduction

NeoGate TA1610/2410/3210 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

● 16/24/32 FXO ports
● Fully compliant with SIP and IAX2
● Flexible calling rules
● Configurable VoIP Server templates
● Codec: G.711 a/u-law, G.722, G.726, G.729a, GSM,ADPCM, Speex
● Echo Cancellation: ITU-T G.168 LEC
● Web-based GUI for easy configuration and management
● Excellent interoperability with a wide range of IP equipment

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

NeoGate TA1610/2410/3210 FXO Gateway features 16/24/32 FXO interfaces for connection of PSTN and PBX extension 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_Series_Installation_Guide_en.pdf

Application Description

Connect IPPBX and NeoGate TA FXO Gateway

NeoGate TA FXO gateway is a solution to extend FXO ports for your IPPBX. Two modes are available for you to connect IPPBX and NeoGate TA FXO gateway, we call them VoIP mode and SPS (Service Provider SIP)/SPX (Service Provider IAX) mode.

VoIP Mode:

The FXO port will be registered as one the VoIP server's SIP extensions if "Enable Register" is checked on VoIP Server template.Select the VoIP Server template on the FXO port page, and fill in the information like SIP username and password. After registeration, if you want to call from IPPBX, you should call the registered SIP account, and NeoGate TA will route the call to the PSTN line.

SPS/SPX Mode:

If "Enable Register" is not checked, the FXO 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. If you want to call from IPPBX, the number you dial should match the dial pattern set on IPPBX outbound route. After receiving the call, NeoGate will forward it on the FXO line to the destination number.

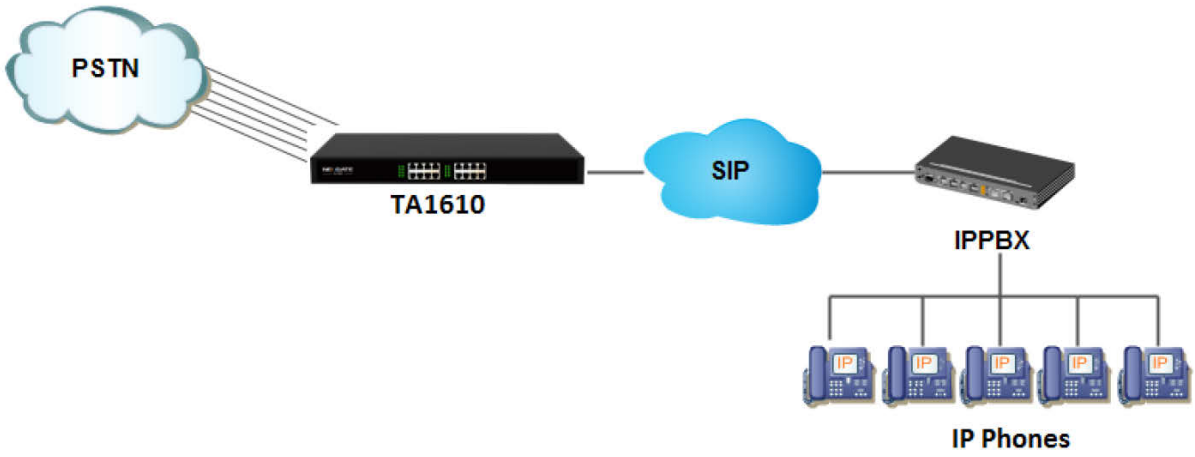


Figure II-1 Connect TA1610 and IPPBX

For incoming calls from the PSTN to NeoGate TA, NeoGate TA will forward the call to a configured SIP extension or to an inbound destination of IPPBX like IVR.

Connect NeoGate TA FXO Gateway and FXS Gateway

NeoGate TA FXO gateway can be connected to a FXS gateway using SPS/SPX Mode. Imagine this, the FXO gateway is set up in Site A, and the FXS gateway in Site B. People in Site B can make and receive calls using the local PSTN lines (which is connnected to Site A's provoider). With this solution, you can call a local number using a local PSTN line wherever you are.

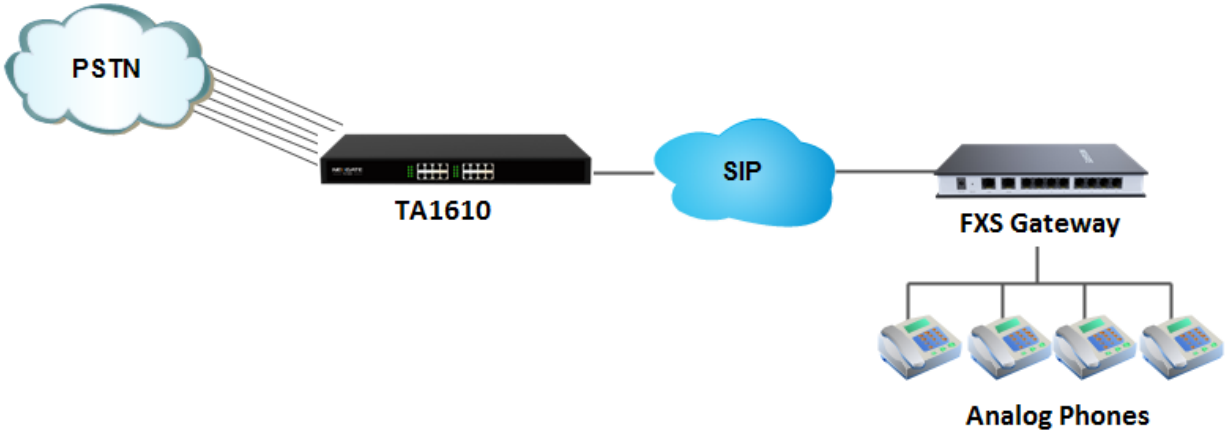


Figure II-2 Connect TA1610 and FXS Gateway

Configuration Guide

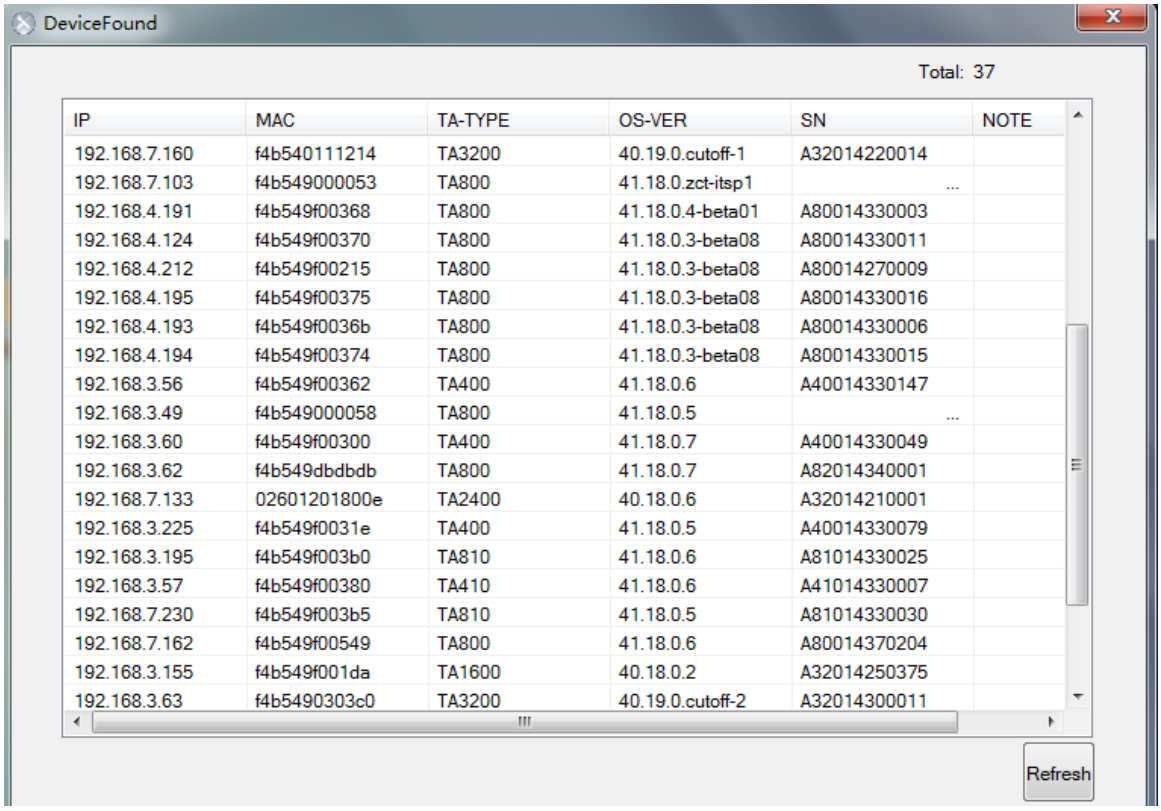
1. Login

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. Download a DeviceFound tool from Yeastar website: FindTA.rar
2. Run the DeviceFound.exe software.
3. The detected NeoGate TA devices in the local network will appear in the window.
4. Find the TA device's IP address by the device's MAC address or the SN.



IP	MAC	TA-TYPE	OS-VER	SN	NOTE
192.168.7.160	f4b540111214	TA3200	40.19.0.cutoff-1	A32014220014	
192.168.7.103	f4b549000053	TA800	41.18.0.zct-itsp1	...	
192.168.4.191	f4b549f00368	TA800	41.18.0.4-beta01	A80014330003	
192.168.4.124	f4b549f00370	TA800	41.18.0.3-beta08	A80014330011	
192.168.4.212	f4b549f00215	TA800	41.18.0.3-beta08	A80014270009	
192.168.4.195	f4b549f00375	TA800	41.18.0.3-beta08	A80014330016	
192.168.4.193	f4b549f0036b	TA800	41.18.0.3-beta08	A80014330006	
192.168.4.194	f4b549f00374	TA800	41.18.0.3-beta08	A80014330015	
192.168.3.56	f4b549f00362	TA400	41.18.0.6	A40014330147	
192.168.3.49	f4b549000058	TA800	41.18.0.5	...	
192.168.3.60	f4b549f00300	TA400	41.18.0.7	A40014330049	
192.168.3.62	f4b549dbdbdb	TA800	41.18.0.7	A82014340001	
192.168.7.133	02601201800e	TA2400	40.18.0.6	A32014210001	
192.168.3.225	f4b549f0031e	TA400	41.18.0.5	A40014330079	
192.168.3.195	f4b549f003b0	TA810	41.18.0.6	A81014330025	
192.168.3.57	f4b549f00380	TA410	41.18.0.6	A41014330007	
192.168.7.230	f4b549f003b5	TA810	41.18.0.5	A81014330030	
192.168.7.162	f4b549f00549	TA800	41.18.0.6	A80014370204	
192.168.3.155	f4b549f001da	TA1600	40.18.0.2	A32014250375	
192.168.3.63	f4b5490303c0	TA3200	40.19.0.cutoff-2	A32014300011	

Figure III-1-1 Device Found Software

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 192.168.3.199, the model is TA1610.

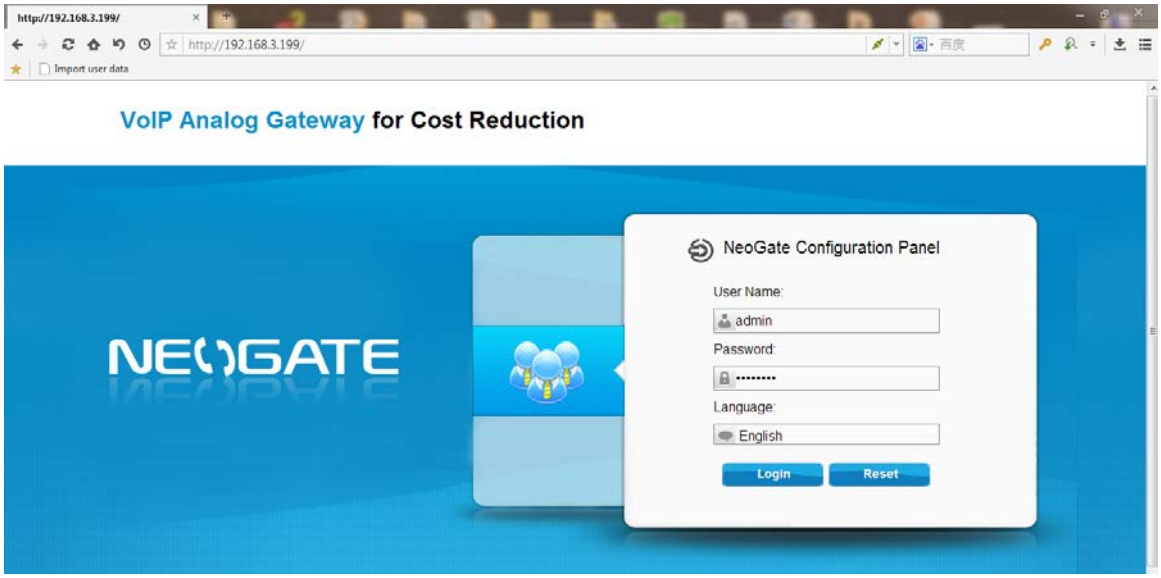


Figure III-1-2 NeoGate TA Login page

Click "Login" to get the welcome page.

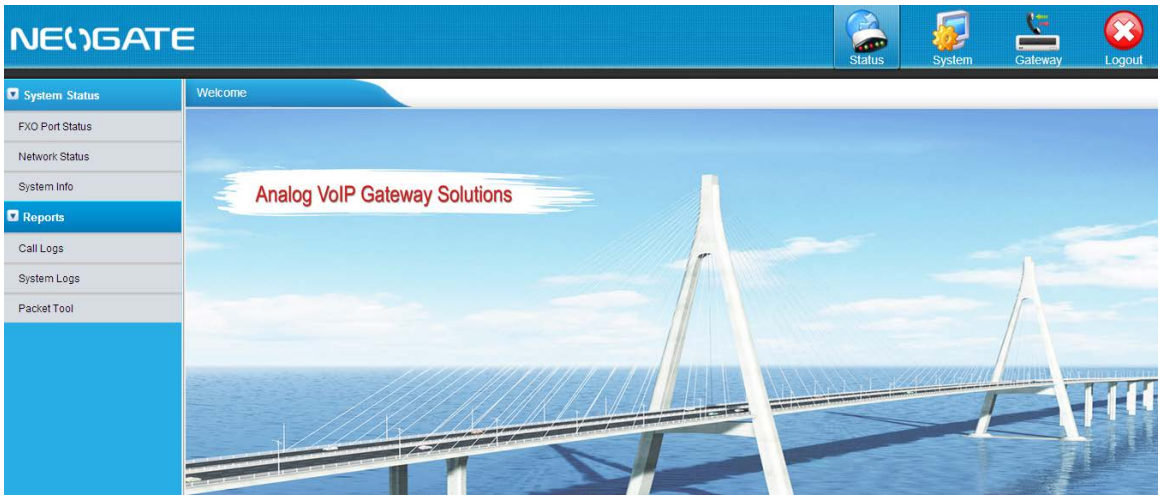


Figure III-1-3 Login NeoGate TA

2. Status

Click 

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

FXO Port Status

Port	UP/Down	(Voip) Status	(FXO) Status
1	Up	OK	Idle
2	Up	OK	Disconnected
3	Up	OK	Disconnected
4	Up	OK	Disconnected
5	Up	OK	Disconnected
6	Up	OK	Disconnected
7	Up	OK	Disconnected
8	Up	OK	Disconnected

Figure III-2-1FXO Port Status

Up/Down:

Up/Down	Description
Up	The FXO interface works well.
Down	The FXO interface is broken.

VoIP Status:

Status	Description
OK	Successful registration, trunk is ready for use
Unreachable	The trunk is unreachable.
Request Send	Registering.
Waiting for authentication	Wrong password or user name.
Failed	Trunk registration failed.

FXO Status

Hook	Description
Idle	The FXO port is idle.
Busy	The FXO port is busy.

Disconnect	There is no line connected to the FXO port.

2.1.2 Network status

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

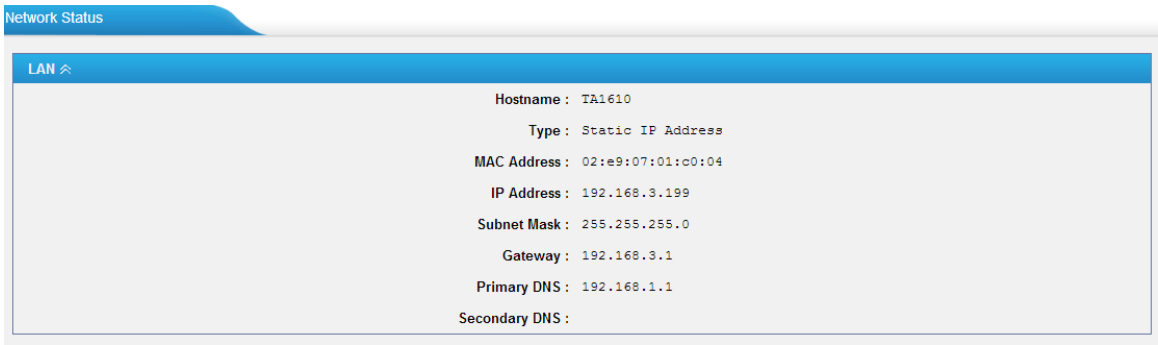


Figure III-2-2 Network Status

If your VLAN or VPN 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.

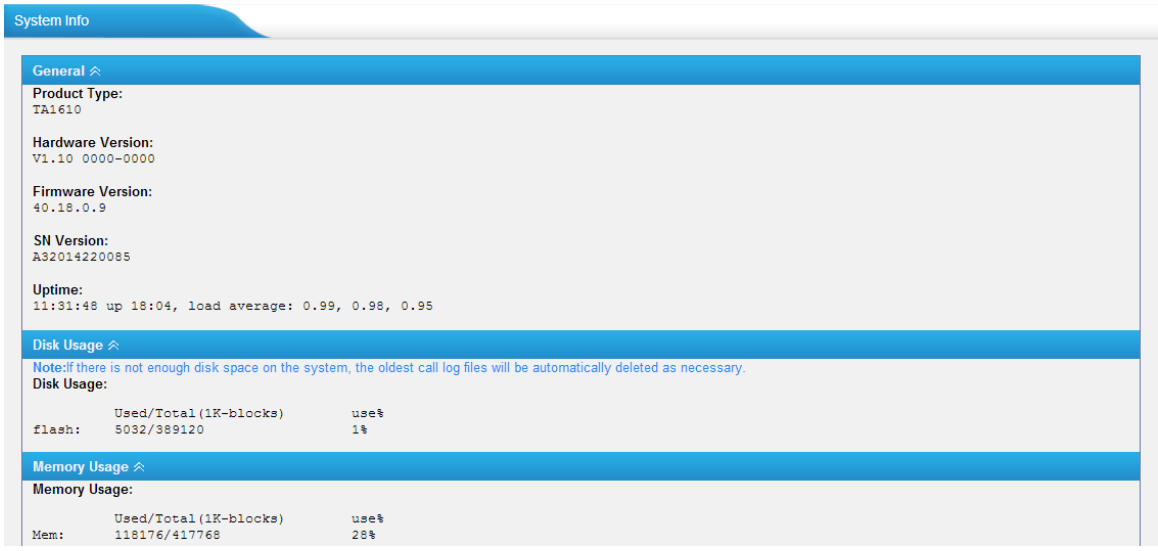


Figure III-2-3 System Info

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.

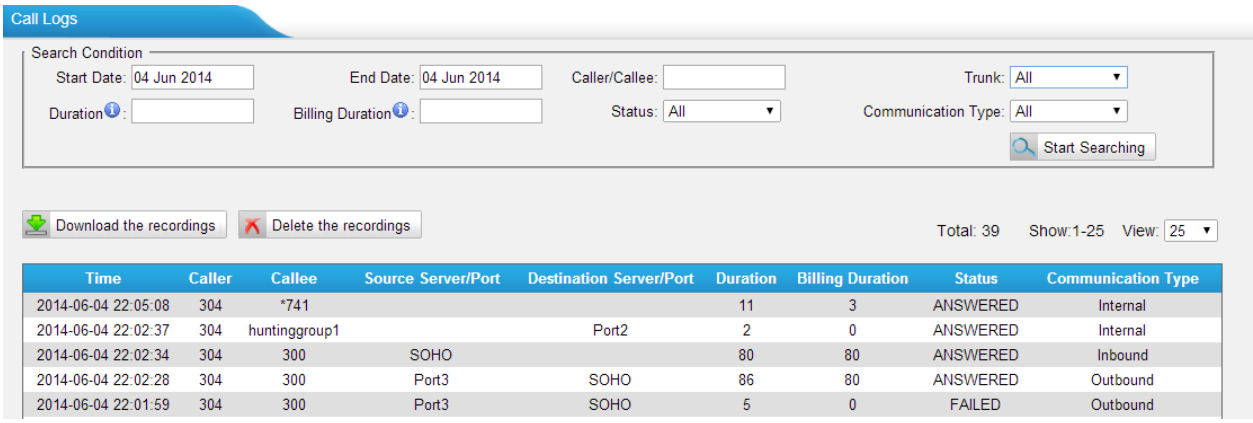


Figure III-2-4 Call Logs

2.2.2 System Logs

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

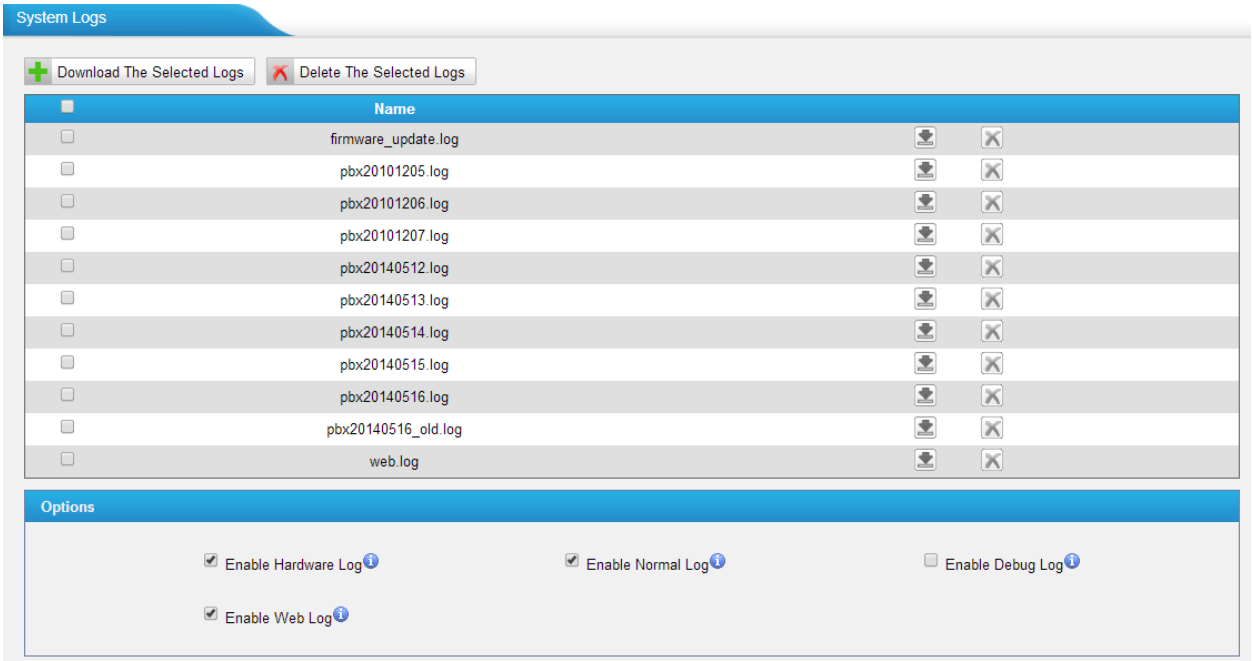


Figure III-2-5 System Logs

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” is integrated in NeoGate.

Users also could specify the destination IP address and port to get the packets.

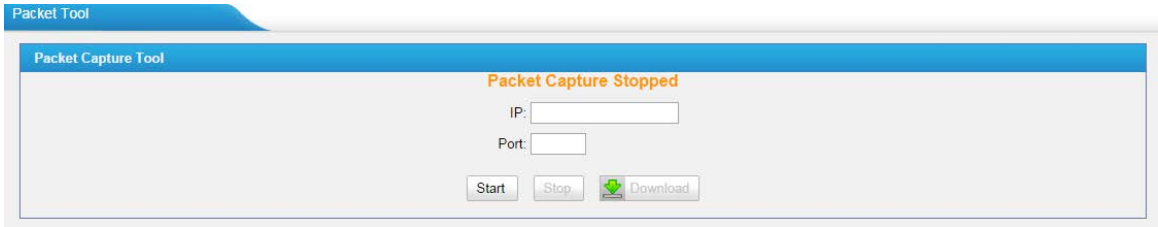


Figure III-2-6 Packet Tool

·IP

Specify the destination IP address to get the packets.

·Port

Specify the destination Port to get the packets.

3. System

Click 

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

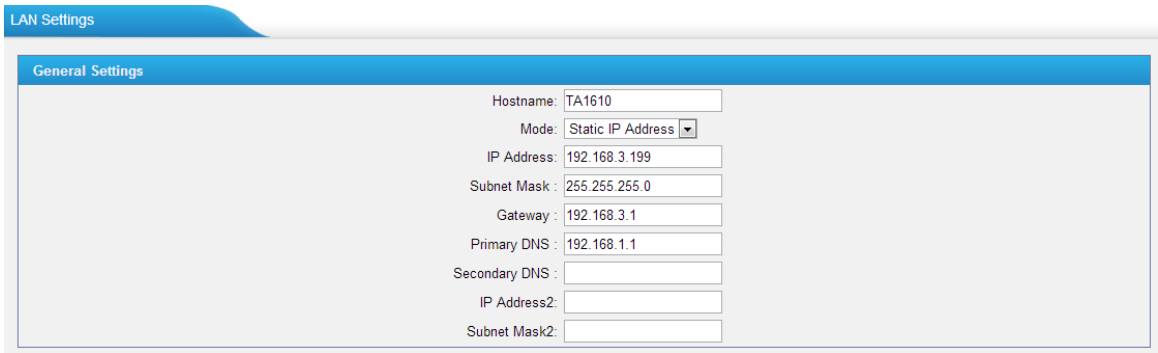


Figure III-3-1 Static IP Address Mode

Table III-3-1 Description of LAN Settings

Items	Description
Hostname	Set the host name for NeoGate TA
Static IP Address	Set the NeoGate TA's IP address as a static IP
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

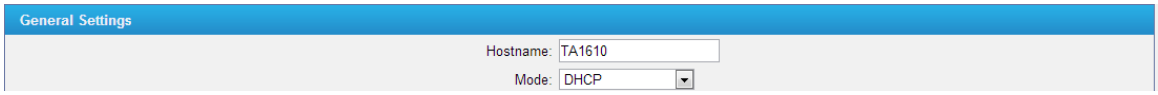


Figure III-3-2 DHCP Mode

Select DHCP mode to get network automatically from the local network.

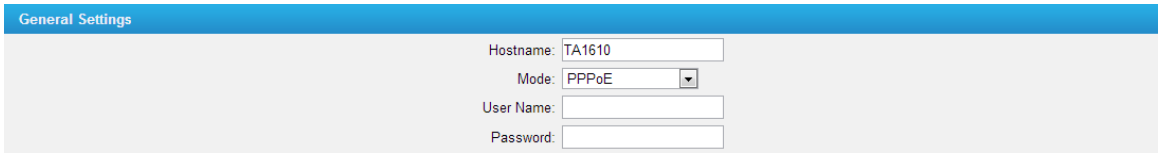


Figure III-3-3 PPPoE

Fill in user name and password to access the Internet via PPPoE.

3.1.2 Service

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

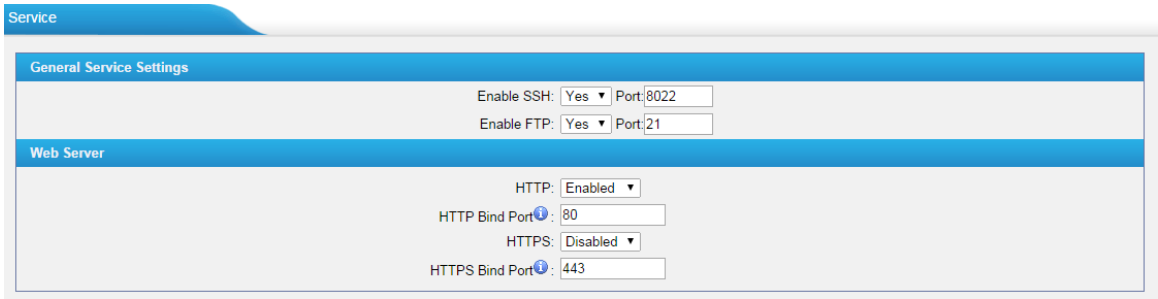


Figure III-3-4 Service Settings

Table III-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.

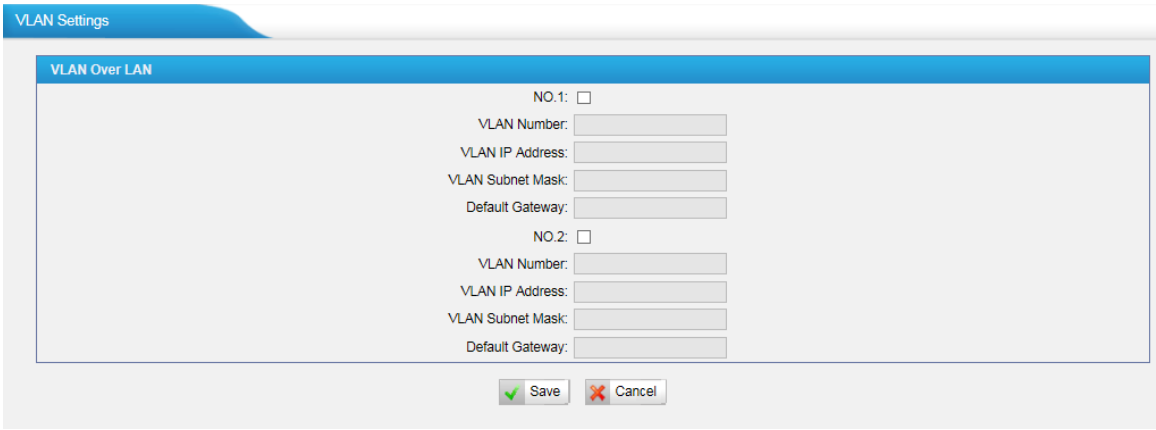


Figure III-3-5 VLAN Settings

Table III-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 networkingtypically using the public internetthat 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.

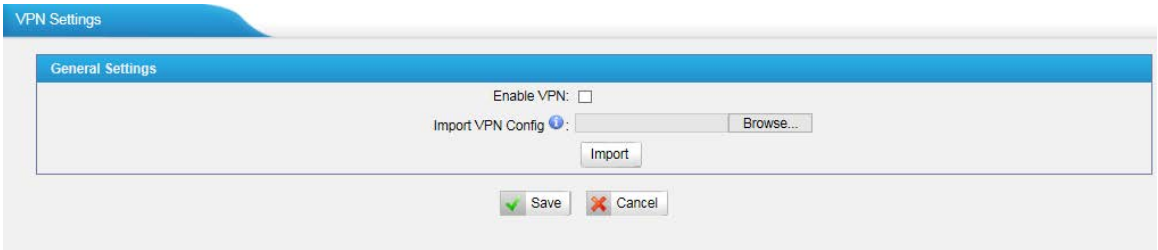


Figure III-3-6 VPN Settings

·Enable VPN

·Import VPN Config

Import configuration file of OpenVPN.

Notes:

1. Uncomment “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.

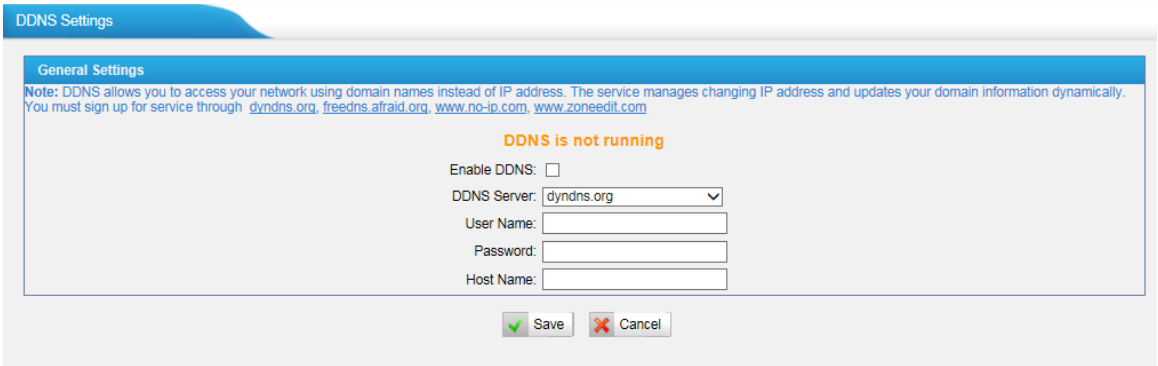


Figure III-3-7 DDNS Settings

Table III-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.

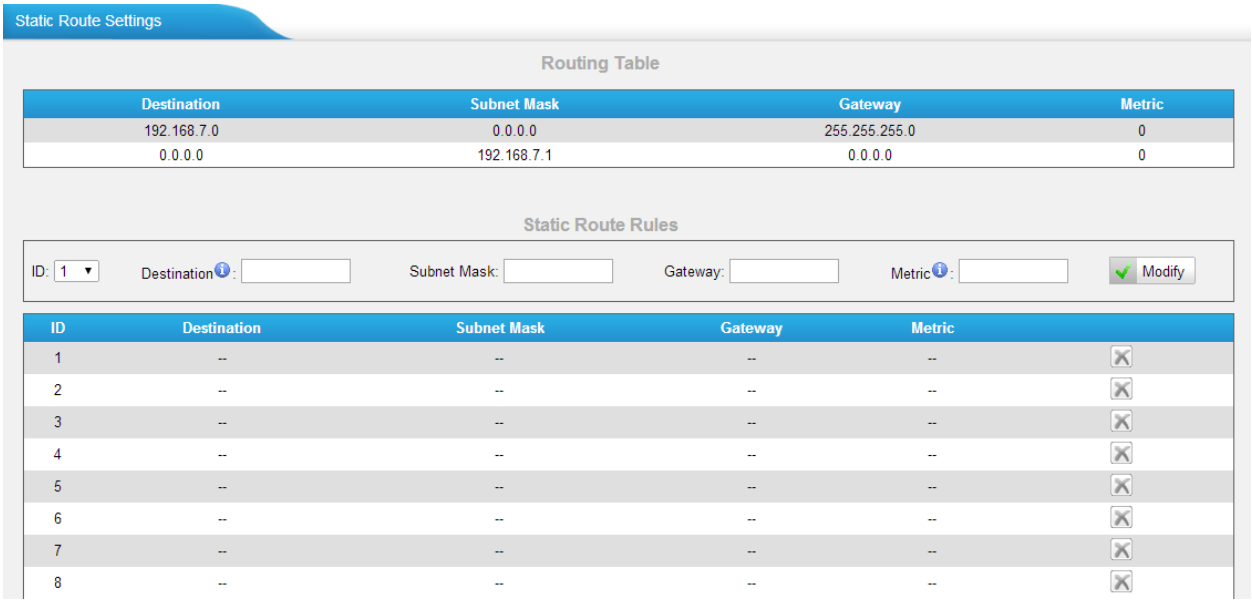


Figure III-3-8 Static Route

1) Route Table

The current route rules of NeoGate TA.

2) Static Route Rules

You can add new static route rules here.

Table III-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.

3.1.7 SNMP Settings

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. NeoGate TA gateway supports three versions: V1, V2C and V3.

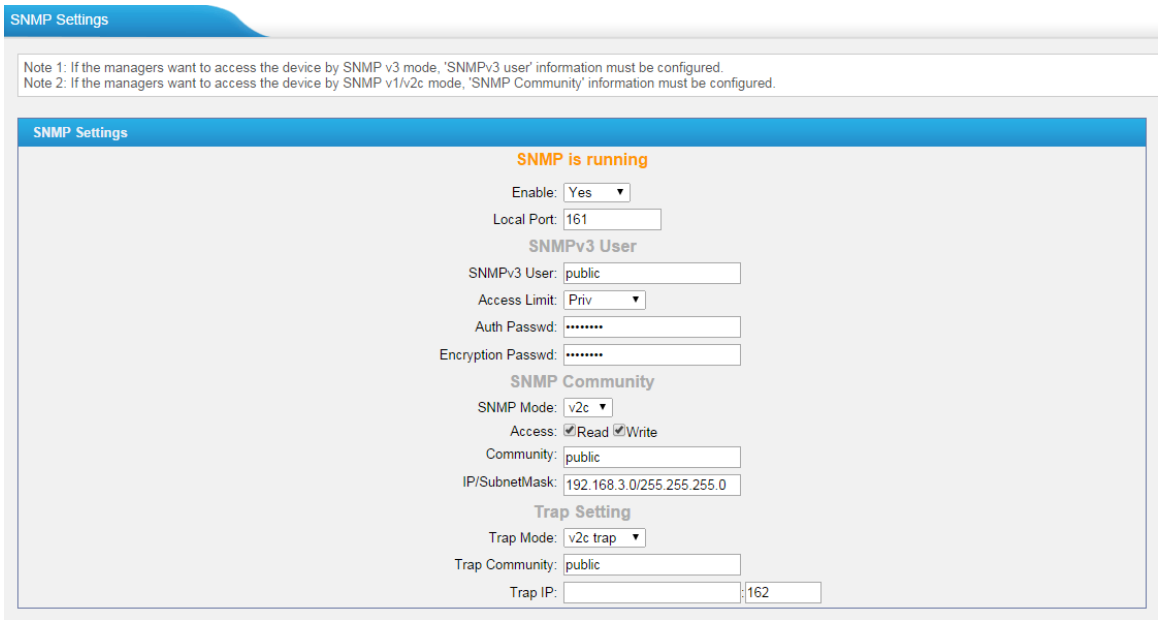


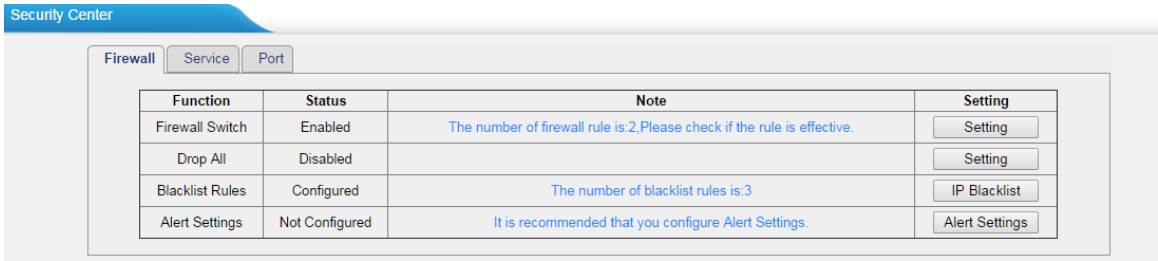
Figure III-3-9 SNMP Settings

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:

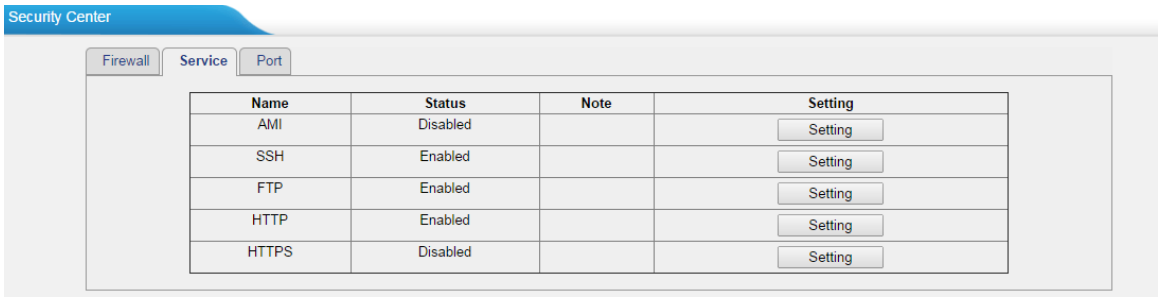


Function	Status	Note	Setting
Firewall Switch	Enabled	The number of firewall rule is:2,Please check if the rule is effective.	Setting
Drop All	Disabled		Setting
Blacklist Rules	Configured	The number of blacklist rules is:3	IP Blacklist
Alert Settings	Not Configured	It is recommended that you configure Alert Settings.	Alert Settings

Figure III-3-10 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:

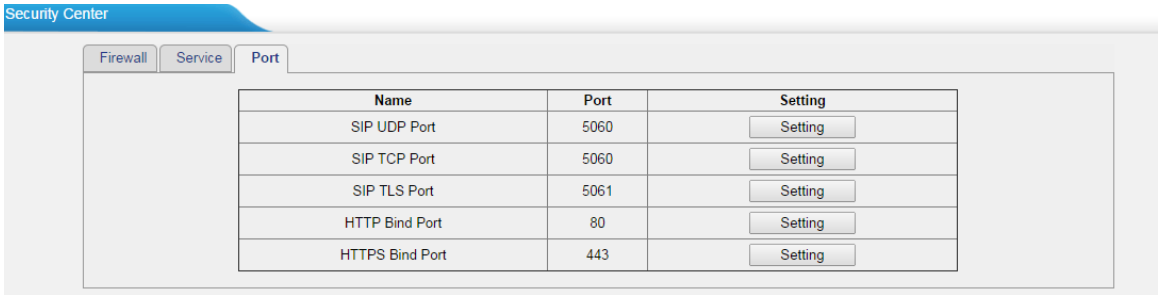


Name	Status	Note	Setting
AMI	Disabled		Setting
SSH	Enabled		Setting
FTP	Enabled		Setting
HTTP	Enabled		Setting
HTTPS	Disabled		Setting

Figure III-3-11 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	443	Setting

Figure III-3-12 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.

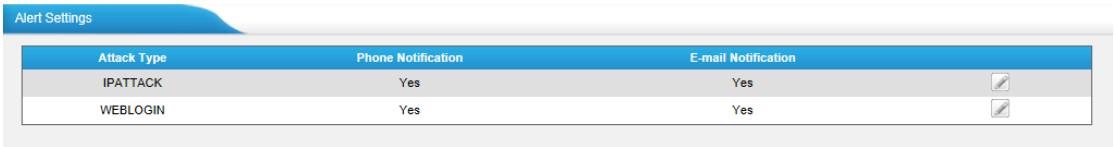


Figure III-3-13 Alert Settings

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 III-3-6 Description ofPhone 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 longerthan 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 III-3-7 Description ofE-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)

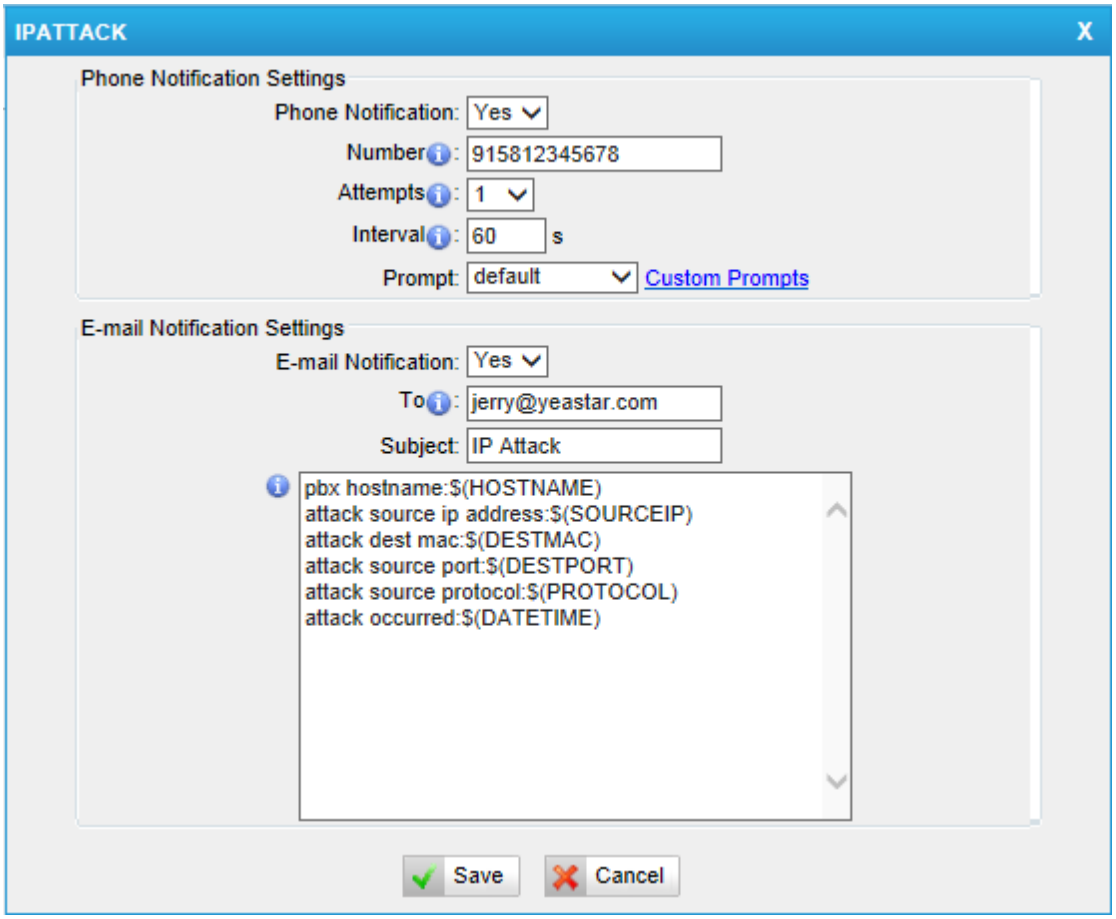


Figure III-3-14 IP ATTACK Alert

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.

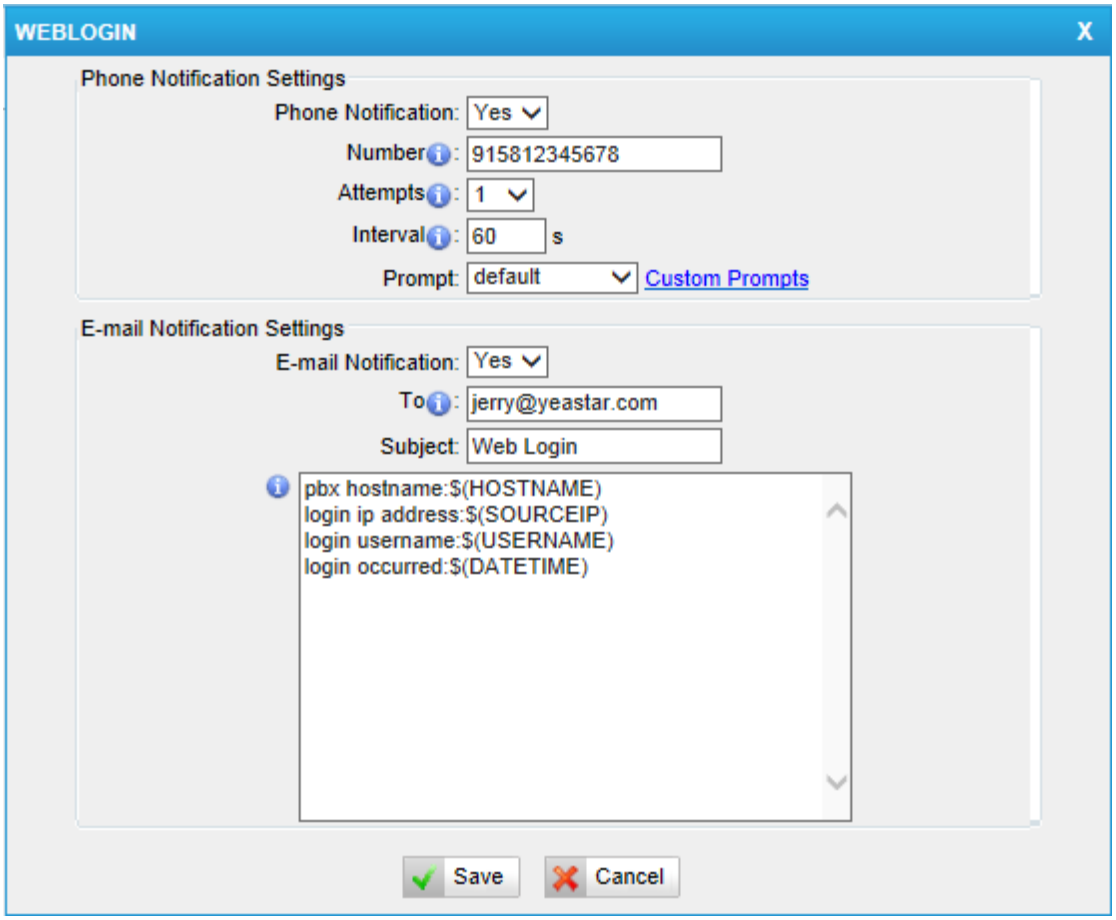


Figure III-3-15 WEBLOGIN Alert

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 as 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.

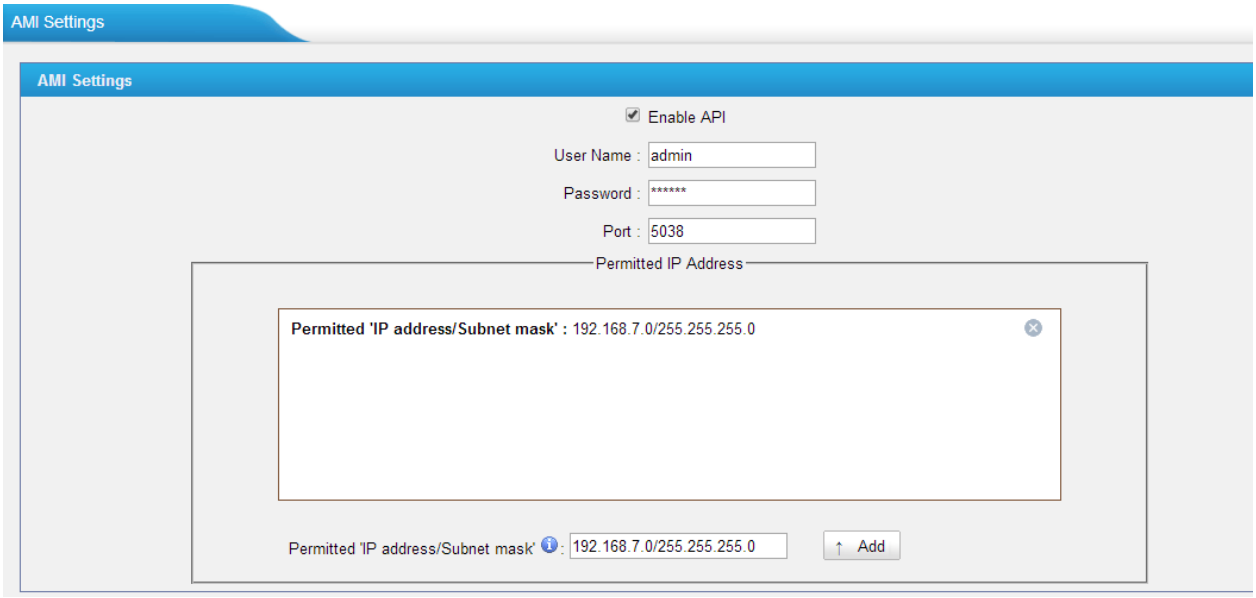


Figure III-3-16 AMI Settings

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.

3.2.4Certificates

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

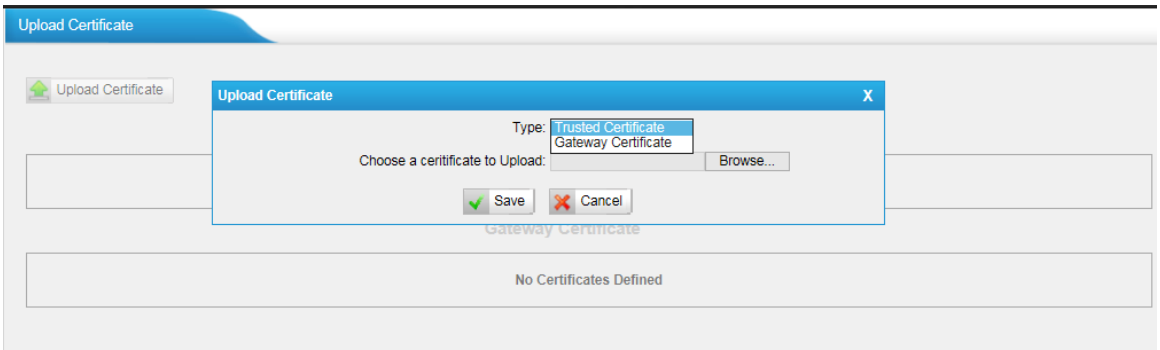


Figure III-3-17 Certificates

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

Figure III-3-18 Firewall Rules

1) General Settings

Table III-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 oneas required.

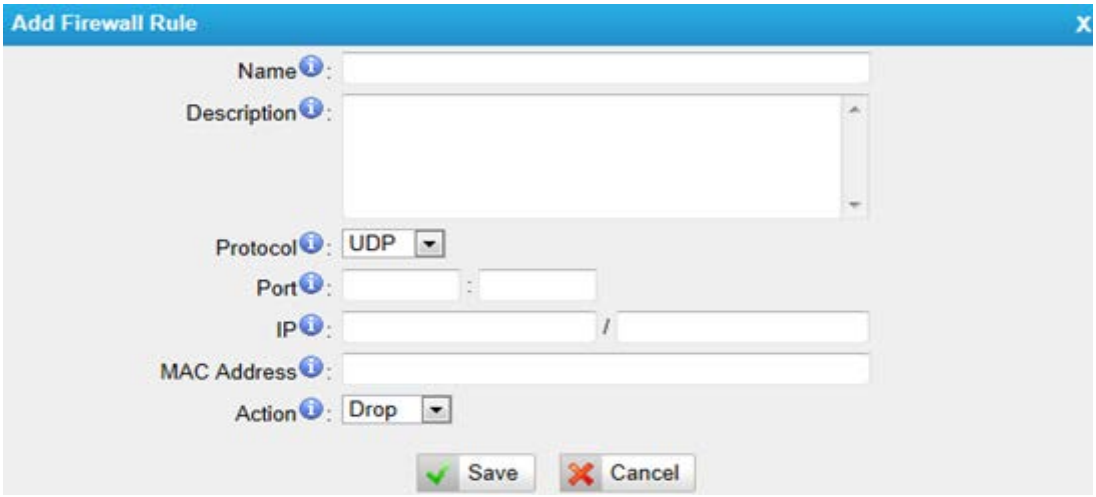


Figure III-3-19 Common Rule

Table III-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 ablack IP address and beblocked automatically.

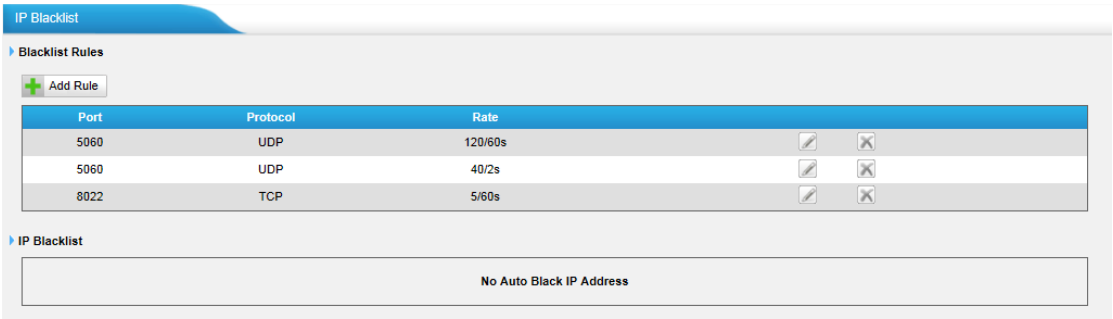


Figure III-3-20 IP Blacklist

1) Blacklist rules

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

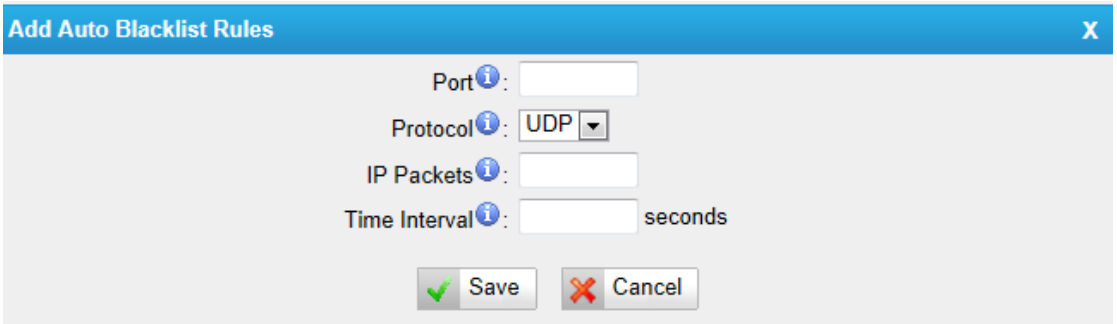


Figure III-3-21 Auto Blacklist Rule

Table III-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 youwish.

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.

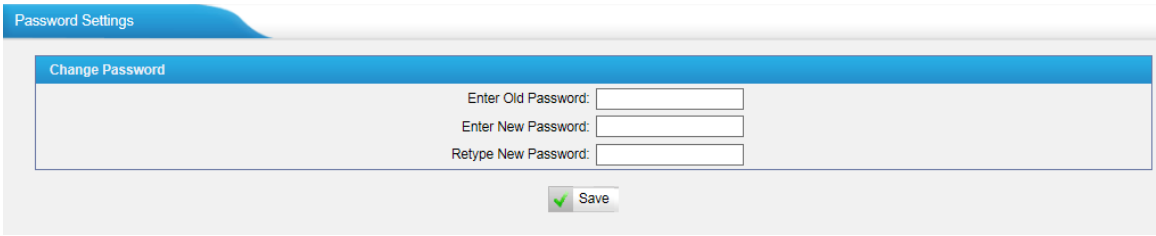


Figure III-3-22 Password Settings

3.3.2 Date and Time

Set the date and time for NeoGate TA.

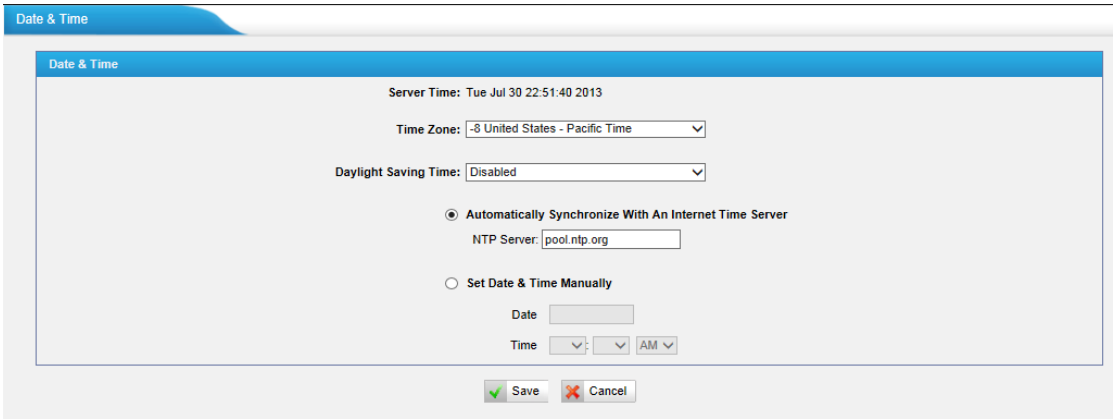


Figure III-3-23 Date & Time

Table III-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.

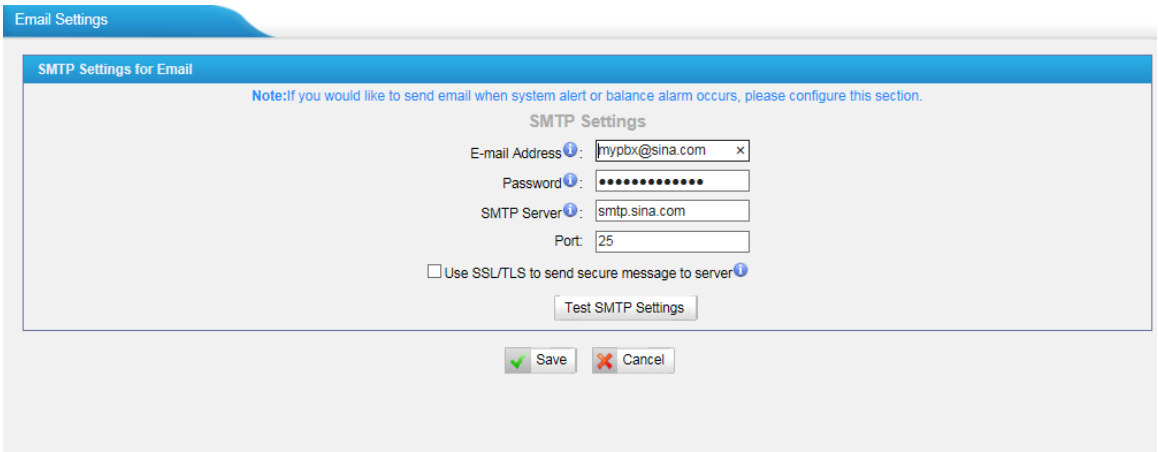


Figure III-3-24 Email Settings

Table III-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 TAwill 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.

3.3.5 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.

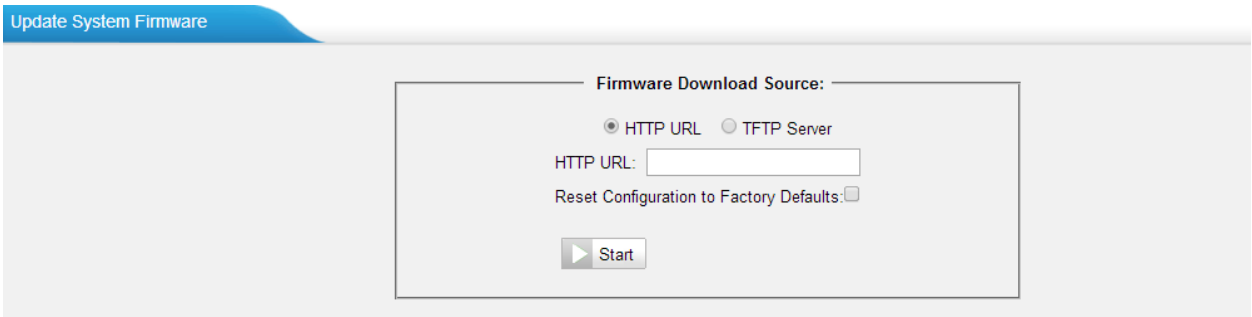


Figure III-3-31 Firmware Update

3.3.6 Backup and Restore

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

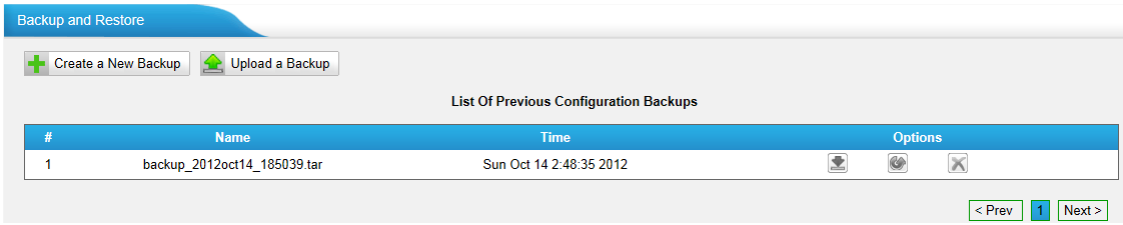


Figure III-3-32 Backup and Restore

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.

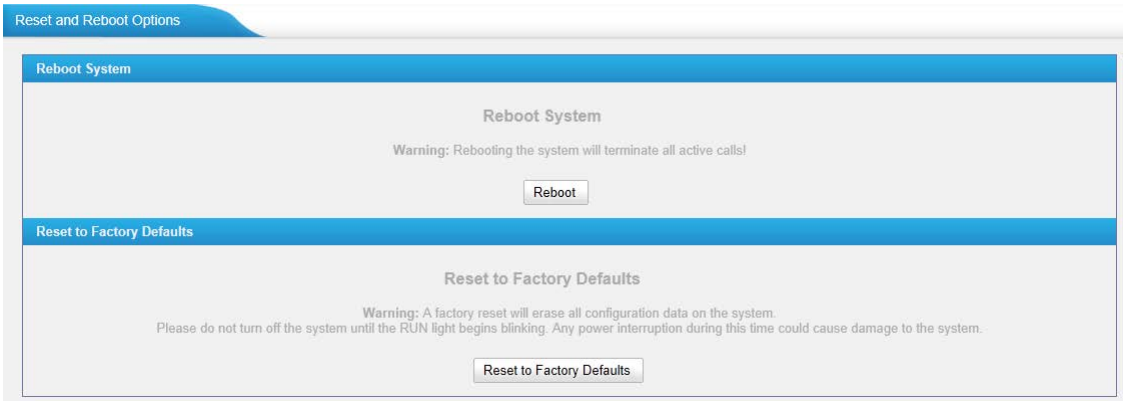


Figure III-3-33 Reset and Reboot

·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 

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

4.1 FXO Port List

4.1.1 FXO Port List

1) Edit the FXS port

Click "Edit" button  to configure the FXS port.

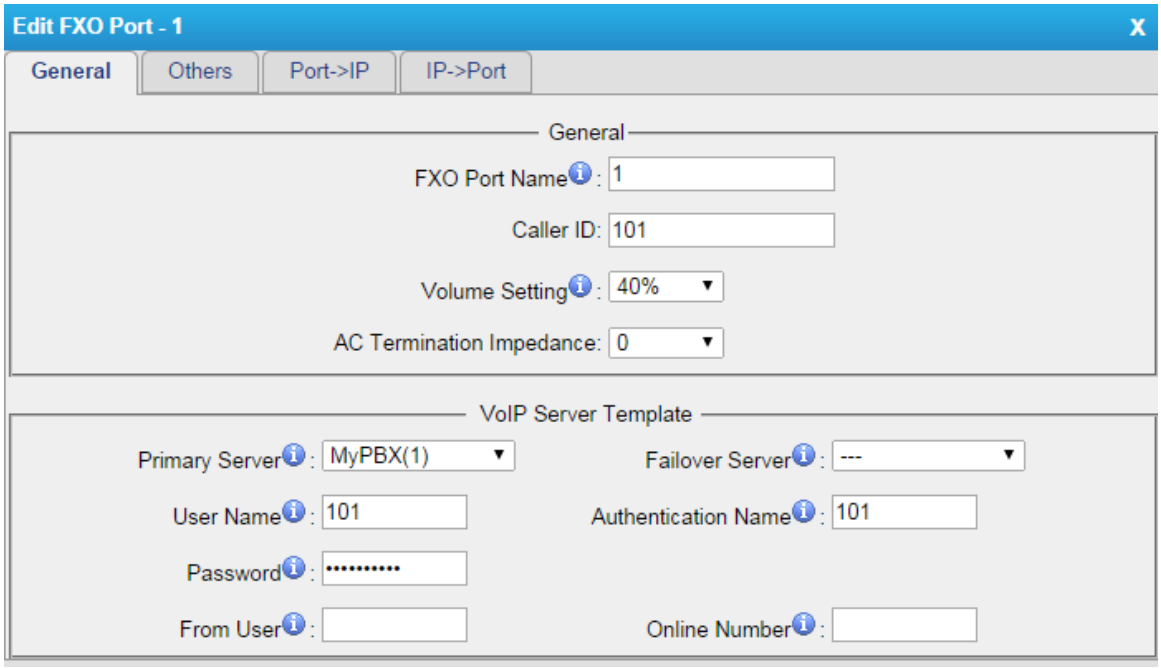


Figure III-4-1General Settings

>General

Table III-4-1 Description of FXO Port General Settings

Items		Description
General	FXO Port Name	The corresponding port.
	Caller ID	User account number.
	Volume Settings	Configure the volume for the FXO port, the default setting is 40%.
		Select the impedance of the analog line connected to the FXO port. Here is the impedance value for the settings: 0 - 600 Ohm (North American)

	AC Termination Impedance	1 - 900 Ohm 2 - 270 Ohm + (750 Ohm || 150nF) and 275 Ohm + (780 Ohm || 150nF) 3 - 220 Ohm + (820 Ohm || 120nF) and 220 Ohm + (820 Ohm || 115nF) 4 - 370 Ohm + (620 Ohm || 310nF) 5 - 320 Ohm + (1050 Ohm || 230nF) 6 - 370 Ohm + (820 Ohm || 110nF) 7 - 275 Ohm + (78 Ohm || 150 nF) 8 - 120 Ohm + (820 Ohm || 110 nF) 9 - 350 Ohm + (1000 Ohm || 210nF) 10 - 0 Ohm + (900 Ohm || 30nF) 11 - 600 Ohm + 2.16 uF 12 - 900 Ohm + 1 uF 13 - 900 Ohm + 2.16 uF 14 - 600 Ohm + 1 uF 15 - Global complex impedance
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.

> Other Settings

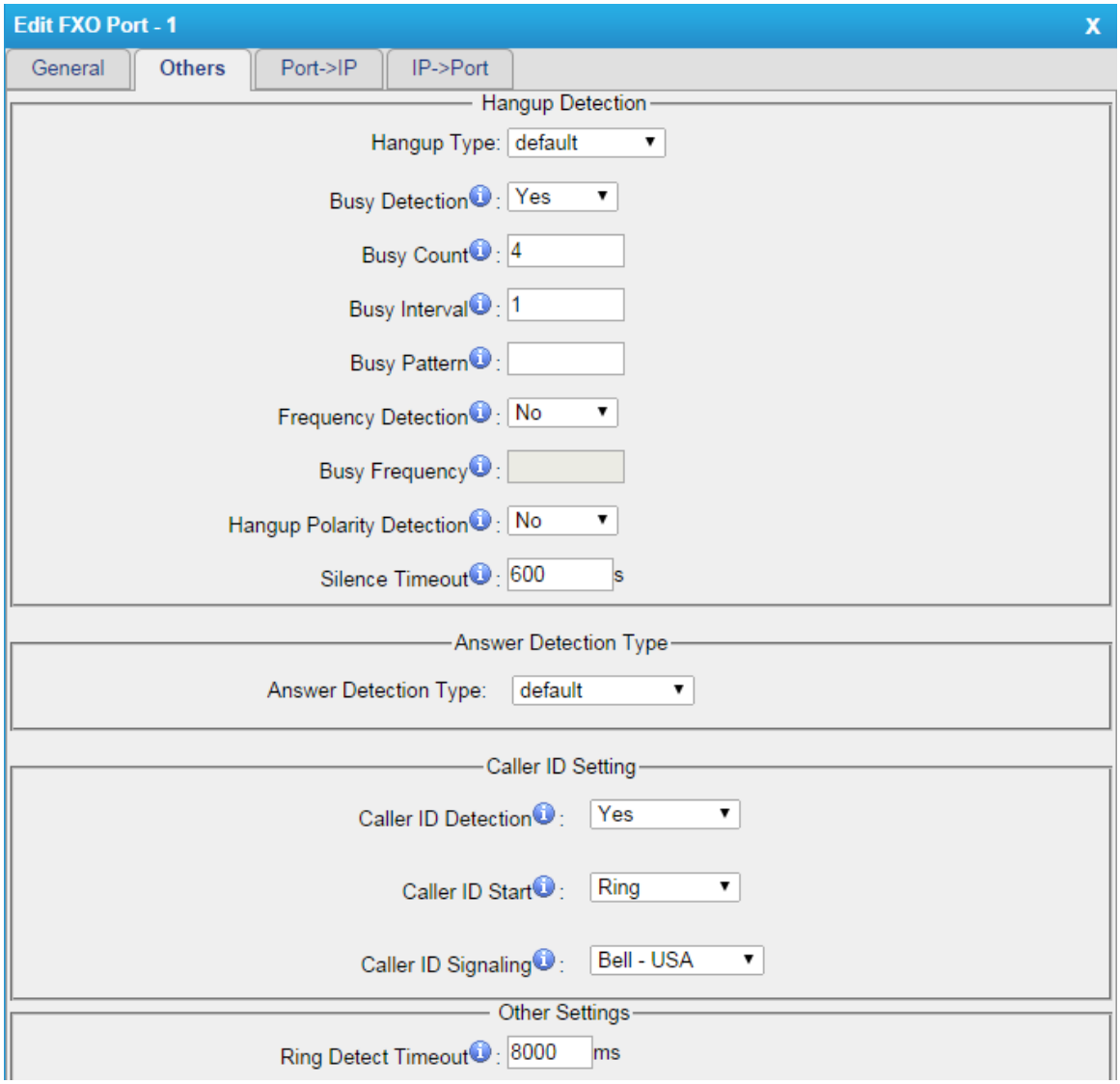


Figure III-4-2FXO Port Other Settings

Table III-4-2 Description of FXO Port Other Settings

Hangup Detection	Hangup Type	Select which kind of hangup type will be used to detect the call and hang up.
	Busy Detection	Enable or disable Busy Detection. It is used for detecting far end hangup or busy signal.

	Busy Count	If Busy Detection is enabled, it is also possible to specify how many busy tones to wait for before hanging up. The default is 4, but better results can be achieved if this setting is set as 6 or 8. Higher value requires more time for detection, but lower the probability that a false detection may occur.
	Busy Interval	Set the busy detection interval.
	Busy Pattern	If Busy Detection is enabled, you need to specify the cadence of the busy signal. If a busy pattern is not specified, the system will accept any repeating sound-silence pattern as a busy signal. If a busy pattern is specified, then the system will check the length of the sound and the silence patterns, which will further reduce the chance of a false positive.
	Frequency Detection	Enable or disable Frequency Detection, it is used for frequency detection.
	Busy Frequency	If Frequency Detection is enabled, you must specify the local frequency.
	Hangup Polarity Detection	Enable or disable Polarity Detection. The call will be considered as “hang up” on a polarity reversal.
	Silence Timeout	Define the ring out value for this port.
Answer Detection Type	Answer Detection Type	Answer Detection settings are configured for accurate billing. Select which type to detect the call as answered. 1) Default. NeoGate TA will start to charge once you grab the PSTN trunk to call out, whether the call is answered or not. 2) Polarity Detection: If the PSTN line supports polarity, you can choose "Polarity detection". When the callee answers the call, the provider will send a polarity signal, and then NeoGate TA starts to bill. 3) Ringback Tone: If you choose this option, NeoGate TA will charge the call according to PSTN ring back tone detection. When the "ring duration" or the "ring interval duration" detected on NeoGate TA is larger than the standard or custom parameters, the call is detected as ANSWERED.

		*Standard parameters: when you configure the "Tone Zone Settings" you get the country's standard tone parameters.
	Custom Ring Tone	Enable or disable Custom Ring Tone. If the custom ring tone is enabled, you need to configure the following settings according to the ringback signal.
	Max Ring Duration	Max duration of the ring tone.
	Max Ring Interval Duration	Max pause between the two ring tones.
	Min Ring Detection	Enable Min Ring Detection, which is useful for complex situations, like when jitter or noise occurs on the PSTN line. Generally it is disabled.
	Min Ring Duration	Min duration of the received tone.
	Min Ring Interval Duration	Min pause between the two received tones.
Caller ID Setting	Caller ID Detection	Enable or disable caller ID detection.
	Caller ID Start	This option allows one to define the start of a caller ID signal. Ring: start to detect when a ring is received Polarity: start to detect when a polarity reversal is started Before Ring: start to detect before a ring tone
	Caller ID Signaling	This option defines the type of caller ID signaling to use. Bell-USA: US standard V23-UK: UK standard V23-Japan: Japanese standard V23-Japan Pure: Japanese standard DTMF: DTMF signal Please check with your PSTN service provider to configure Caller ID Settings. If you don't know how to configure, please contact Yeastar support.
Other Settings	Ring Detect Timeout	There should be a timeout to determine if there is a hang up before the line is answered. Range from 3000 to 8000. Default is 8000 ms.

Port→IP

On this page, you can specify how to route the calls from PSTN trunk to IPPBX. There are two modes for you to configure that.

1) Simple Mode

All you need to configure in simple mode is to choose the dial pattern template.

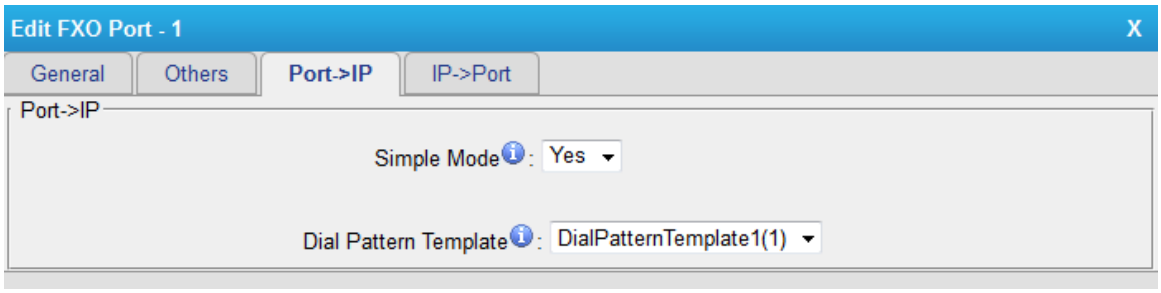


Figure III-4-3 Port→IP Simple Mode

2) Advanced Mode

When Simple Mode is set to "No", you can check the advanced settings.

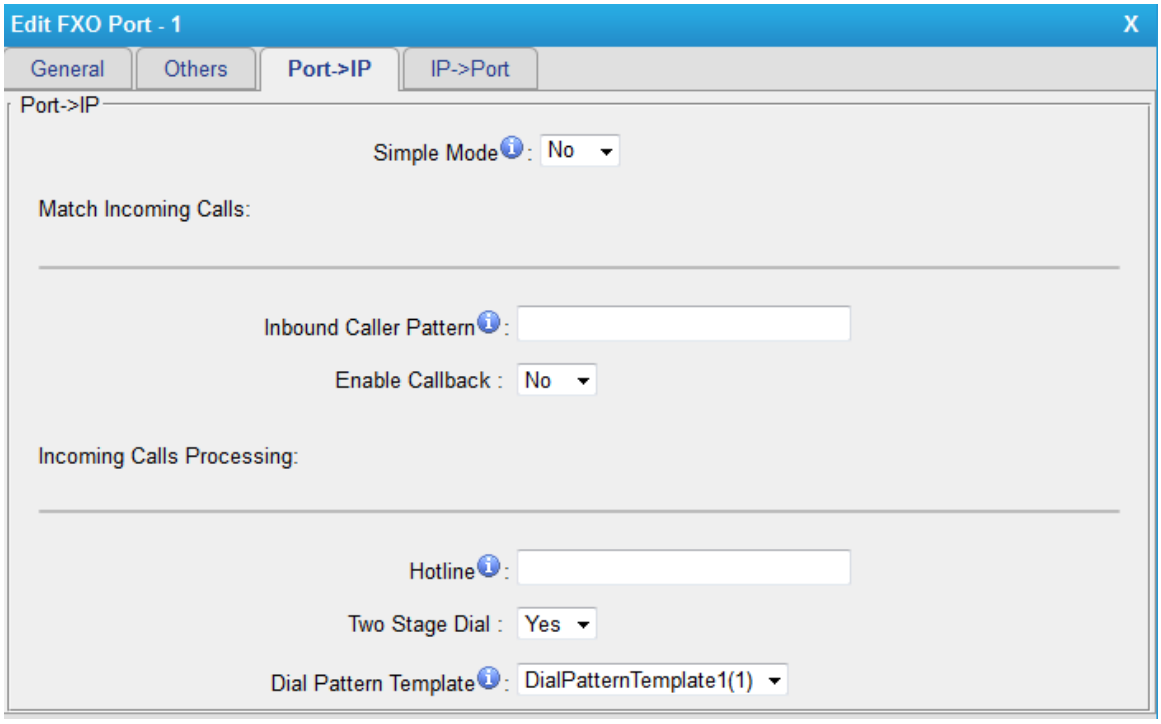


Figure III-4-4 Port→IP Advanced Mode

Table III-4-3 Port→IP Settings

Items	Description
Inbound Caller Pattern	Match the prefix of caller ID for incoming calls. Hover the pointer over to read tips.
Enable Call Back	Choose whether call back is enabled. NeoGate TA allows

	caller A to dial an inbound route number, and after hearing the ring, A can hang up the call to cut off the call, then NeoGate TA will call back to A.
Hotline	Set the hotline number. If hotline number is configured, TA will route the incoming call to the hotline number directly.
Two Stage Dial	Enable it to get the customized two stage dial tone before dialing out, it's disabled by default.
Dial Pattern Template	Choose the Dial Pattern template.

IP→Port

On this page, you can configure how to route the calls from VoIP trunk to a PSTN number.

1) Simple Mode

All you need to configure in simple mode is to choose the dial pattern template. NeoGate TA will allow all incoming calls and route the calls to the destination without any modification.

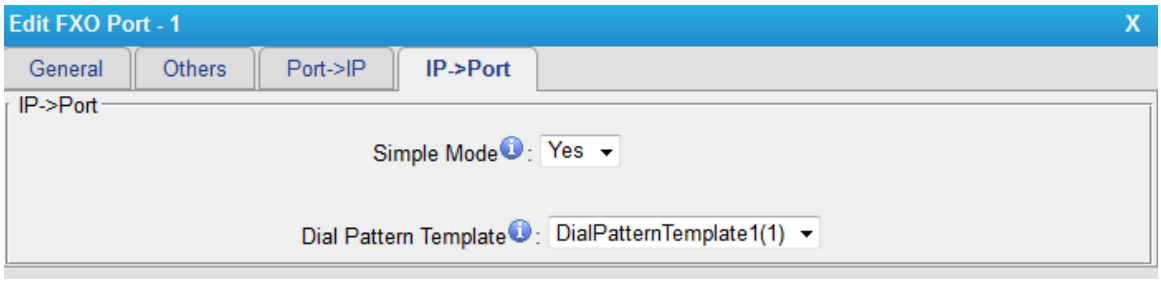


Figure III-4-5 IP→Port Simple Mode

2) Advanced Mode

When Simple Mode is set as "No", you can check the advanced settings.

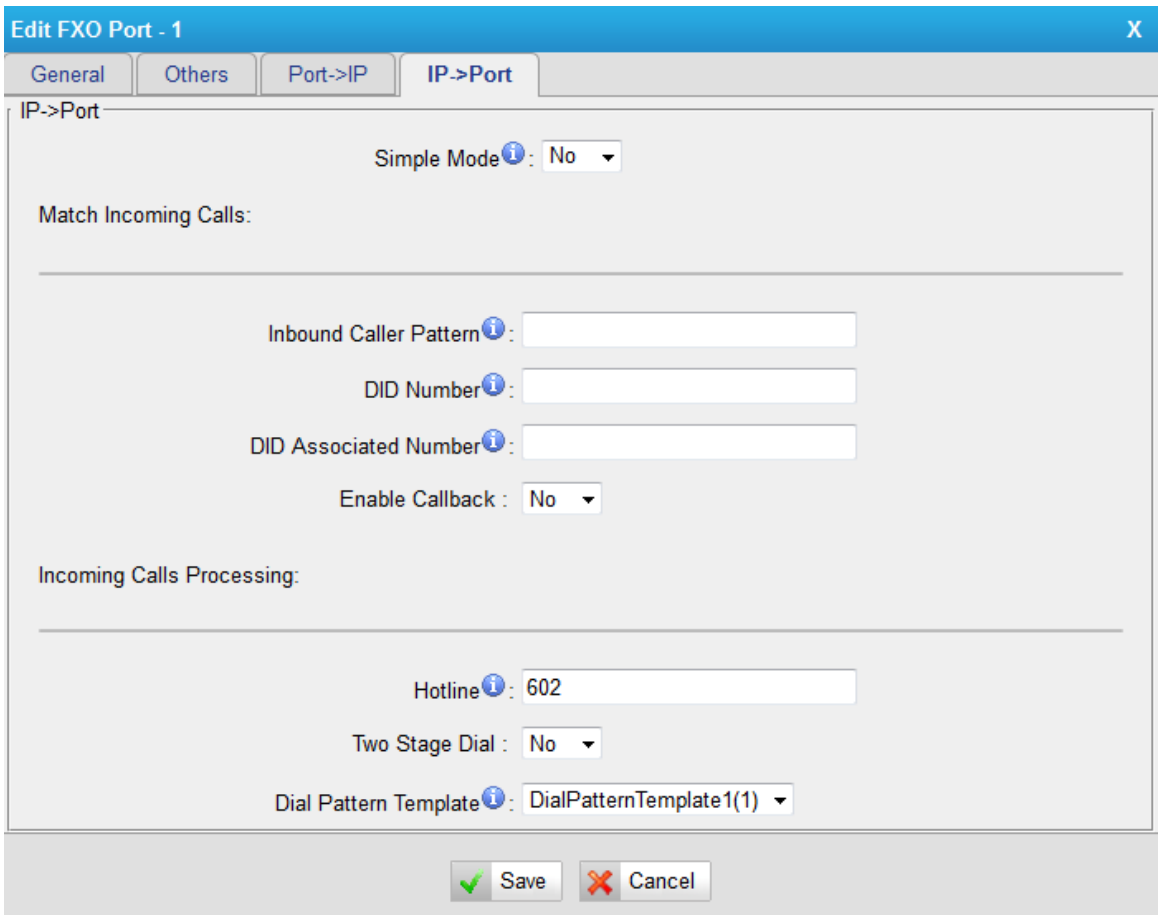


Figure III-4-6 IP→Port Advanced Mode

Table III-4-4 IP→Port Settings

Items	Description
Inbound Caller Pattern	Match the prefix of caller ID for incoming calls. Hover the pointer over to read tips.
DID Number	Define the expected DID Number if this trunk passes DID on incoming calls. Leave this field blank to match calls with any or no DID info. You can also use pattern matching to match a range of numbers.
DID Associated Number	Define the extension for DID number. You can only input number and "-" in this field, and the format can be xxx or xxx-xxx. The count of the number must be only one or equal the count of the DID number.
Enable Call Back	Choose whether call back is enabled. NeoGate TA allows caller A to dial an inbound route number, and after hearing the ring, Acan hang up the call cut off the call, then NeoGate TA will call back to A.
Hotline	Set the hotline number. If hotline number is configured, TA will route the incoming call to the hotline number directly.

Two Stage Dial	Enable it to get the customized two stage dial tone before dialing out, it's disabled by default.
Dial Pattern Template	Choose the Dial Pattern template.

2) Batch Edit Number of FXO Ports

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

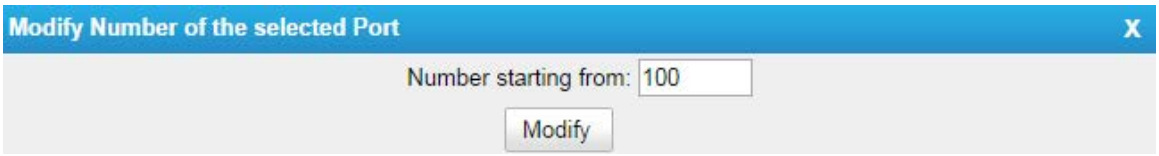


Figure III-4-7 Batch Edit Number of FXO Ports

3) Batch Edit FXO Ports

You can also modify the selected FXO 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.

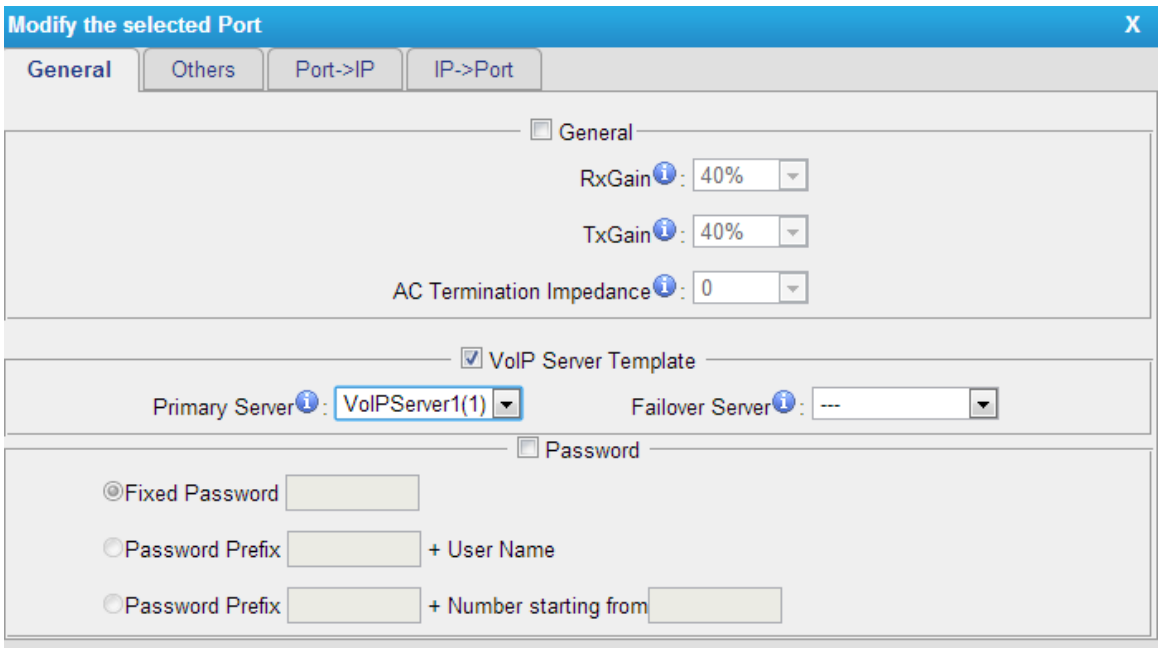


Figure III-4-8 Batch Edit FXO ports

3) Batch Reset FXO Ports

You can reset the selected FXO ports in bulk by clicking the button "Reset the selected Port" Reset the selected Port. The settings for the FXO ports will back to the default.

4.2 VoIP Settings

To integrate with other IPPBX, we need to configure the VoIP settings in NeoGate TA to setup 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 FXO ports on NeoGate. The VoIP server settings help the FXO ports to register to the VoIP server. Once configured, the templates can be chosen on FXO 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 FXO 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 FXO 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 III-4-9 VoIP Server

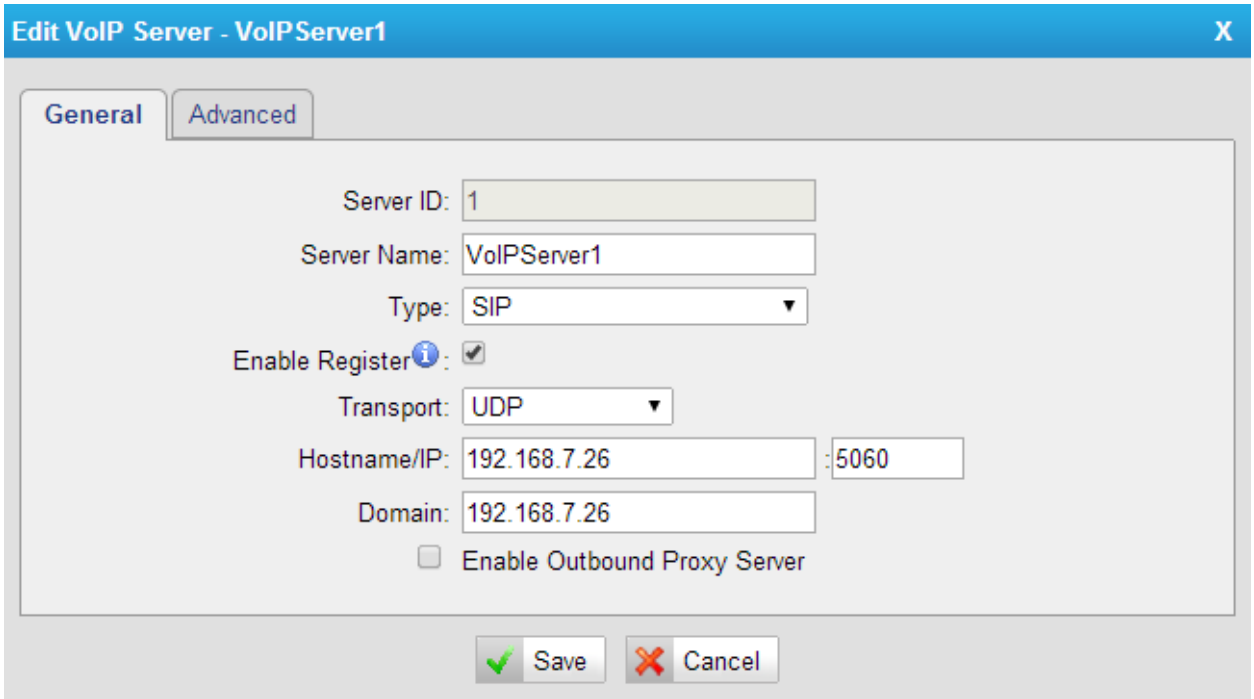


Figure III-4-10 VoIP Server Settings

> General

Table III-4-5 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 FXO 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 FXO port as an extension of the VoIP server. You will need to enter the relevant user name, password, etc in the FXO 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 host name 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 host name. 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

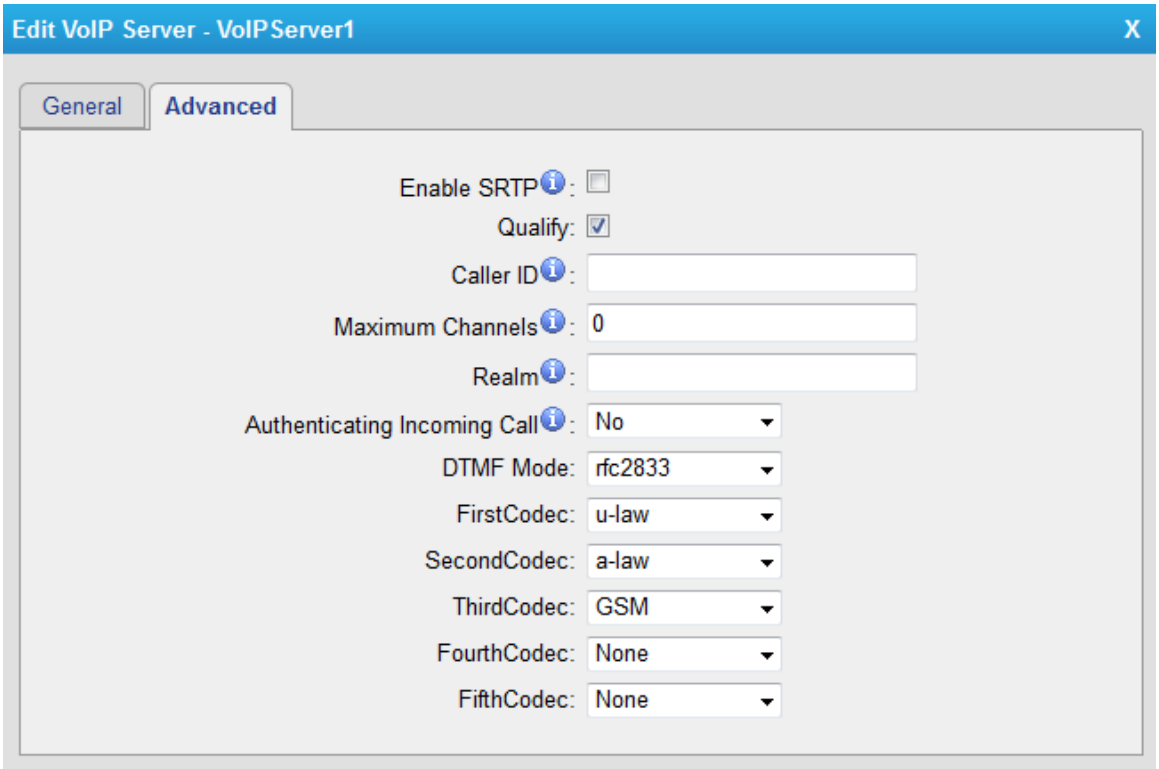


Figure III-4-11 VoIP Server Advanced Settings

Table III-4-6 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.
Authenticating Incoming Call	When an incoming call reaches TA device and sends INVITE packet to TA, TA responds 401, but the Realm info in 401 Response does not match the Realm set on TA VoIP Server, the provider will refuse to authenticate. If you set this option to No, TA will not reply a 401 Response to the provider to authenticate the incoming call.
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 FXOports 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.

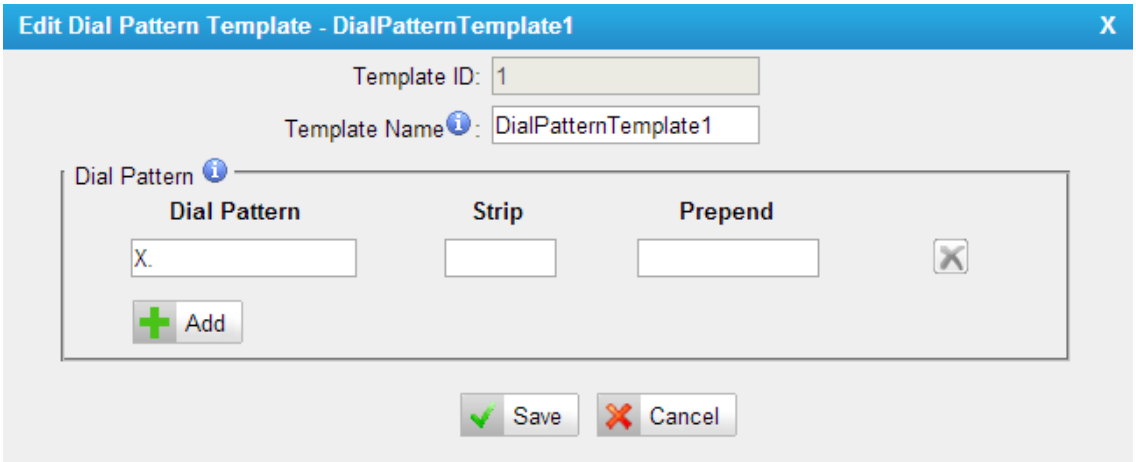


Figure III-4-12 Dial Pattern Template

Table III-4-7 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 FXO 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

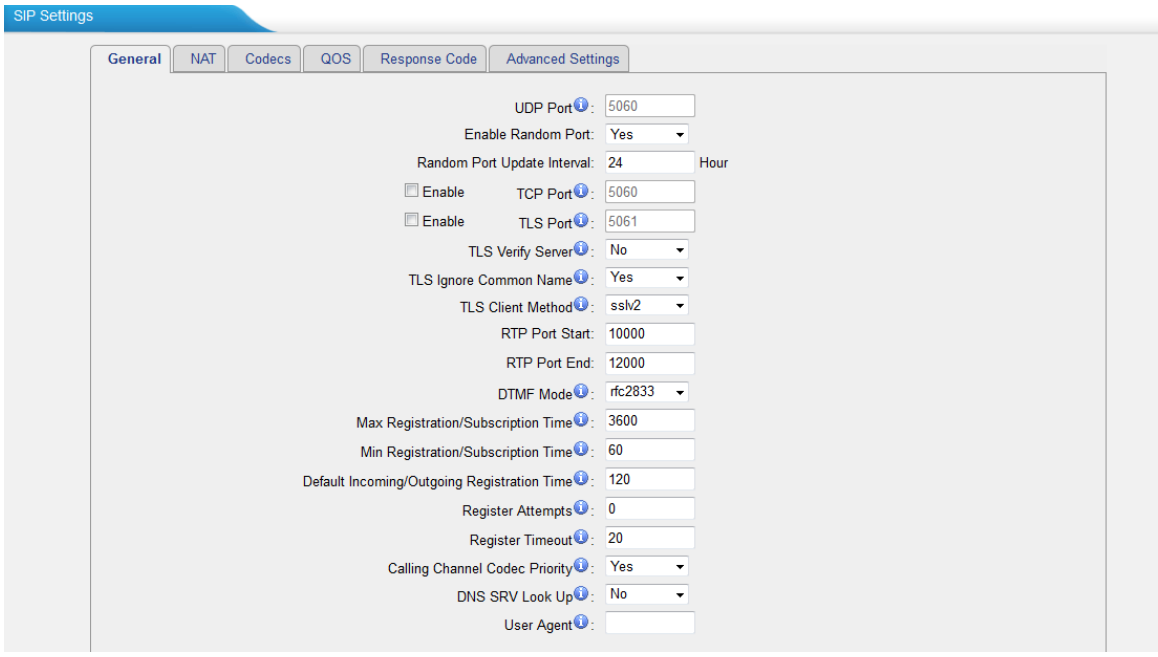


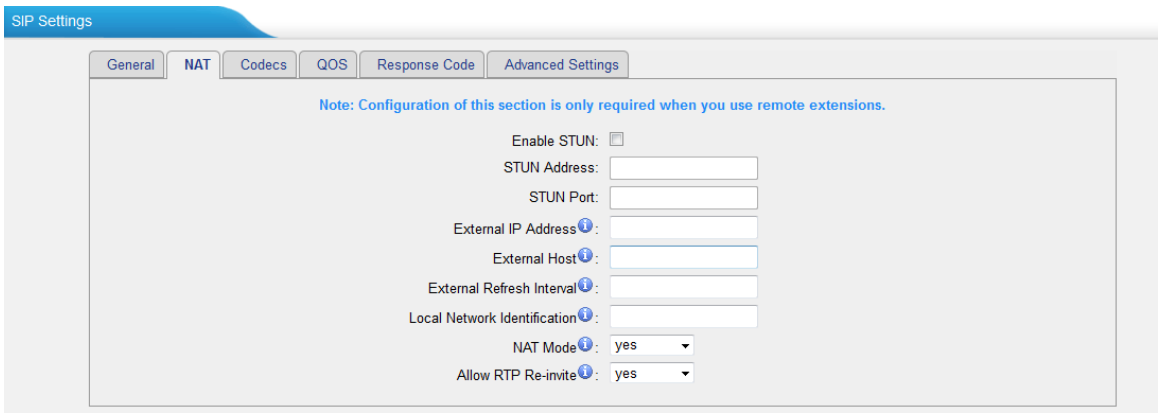
Figure III-4-13 SIP General Settings

Table III-4-8 Description of SIP General Settings

Items	Description
UDP Port	Port used for SIP registrations.The defaultis 5060.
Enable Random Port	Enable or Disable Random SIP port.
Random Port Update Interval	Set the Random Port Update Interval.
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 priorityorderin 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 canchange it if needed.

2) NAT



FigureIII-4-14 NAT Settings

Table III-4-9 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 isused 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

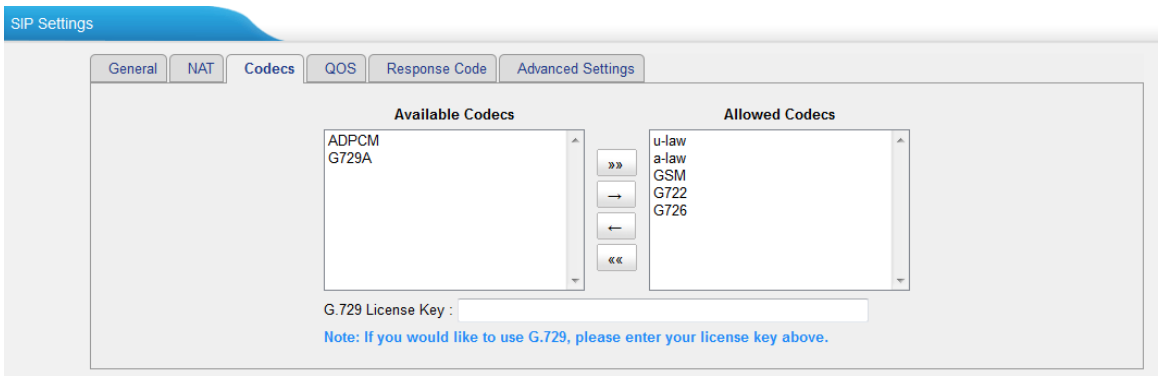


Figure III-4-15 Codecs

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.

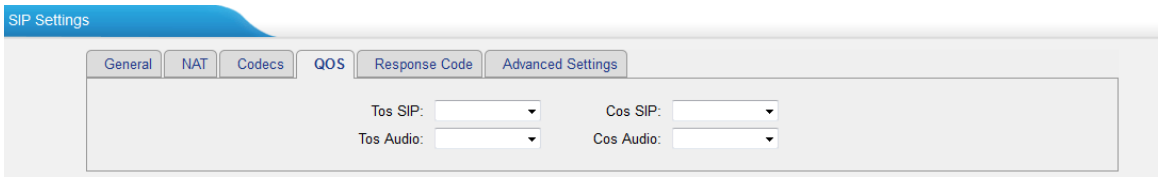


Figure III-4-14 Qos

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.

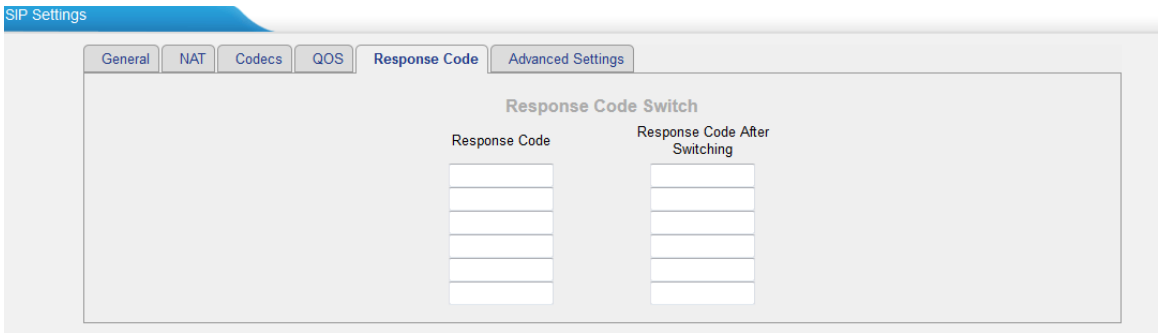


Figure III-4-16 Response Code

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

6) Advanced Settings

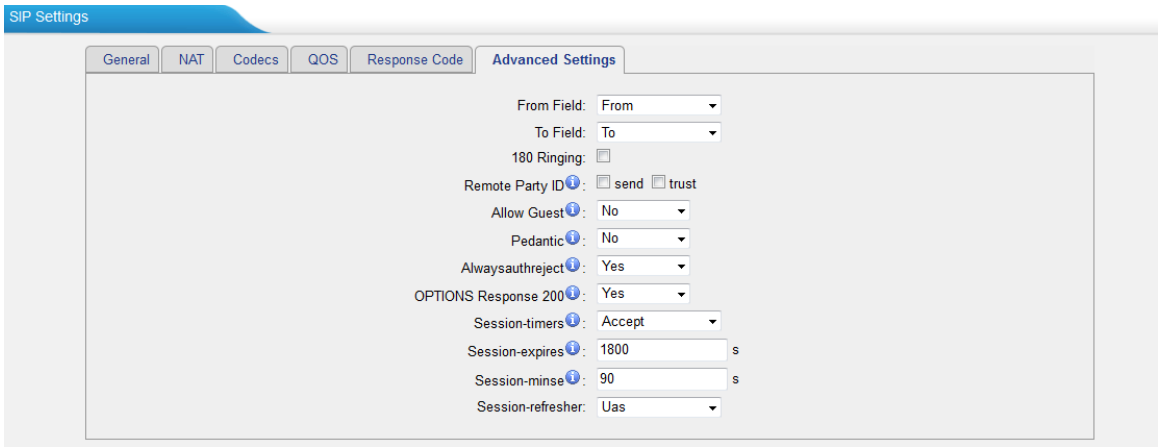


Figure III-4-17 SIP Advanced Settings

Table III-4-10 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 extensionor not. Default: no. It's

	recommendedthat 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 shorterthan 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.

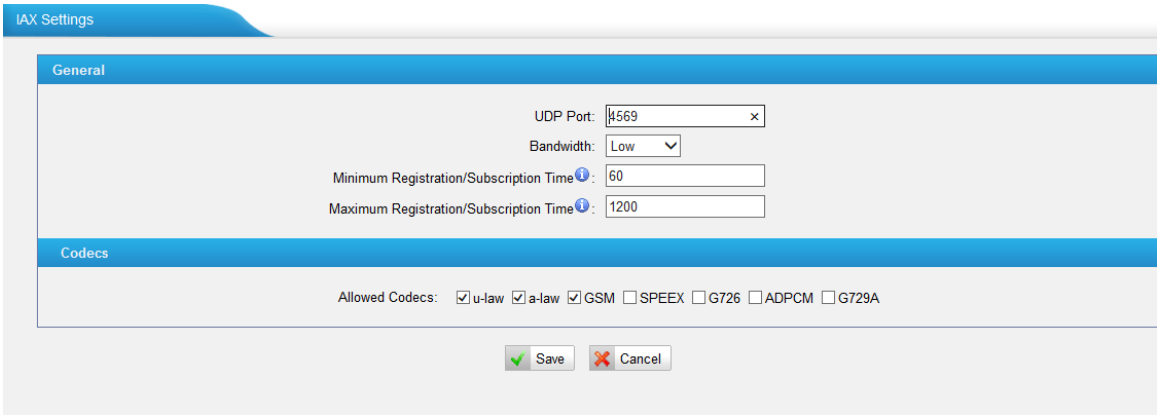


Figure III-4-18 IAX Settings

Table III-4-11 Description of IAX Settings

Items	Description
Bind Port	Port used for IAX2 registrations. The 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

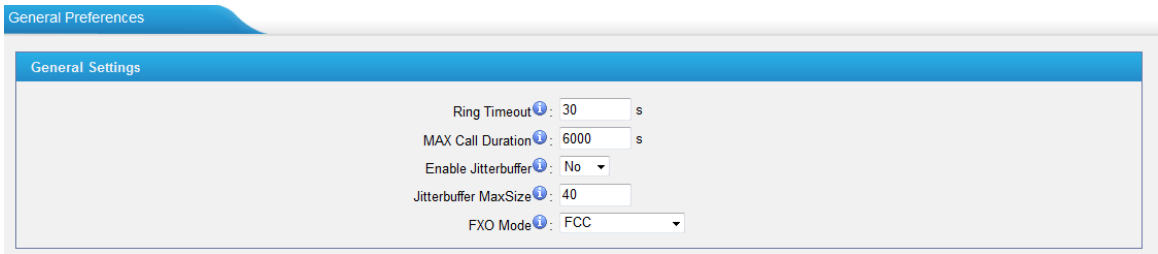


Figure III-4-19 General Settings

Table III-4-12 Description of General Settings

Items	Description
Ring Timeout	Number of seconds to ring a device before giving up.
MAX Call Duration	The absolute maximum amount of time permitted for a call. A setting of 0 disables the timeout.
Enable Jitterbuffer	Forces the use of a jitter buffer on the received side of a SIP channel. The call quality will be improved if this option is enabled.
Jitterbuffer MaxSize	Max length of the jitter buffer. Default is 40 milliseconds.
FXO Mode	Select country to set the On Hook Speed, Ringer Impedance, Ringer Threshold, Current Limiting,TIP/RING voltage adjustment, Minimum Operational Loop Current, and AC Impedance as predefined for your country's analog line characteristics. The default setting is "FCC".

4.5 Advanced Settings

4.5.1 Tone Zone Settings

Advanced ring tones for all the FXO ports can be configured on this page. There

are pre-programmed tone zone settings for some countries and regions. Users can simply find and select thier country to get tone zone settings for the gateway.

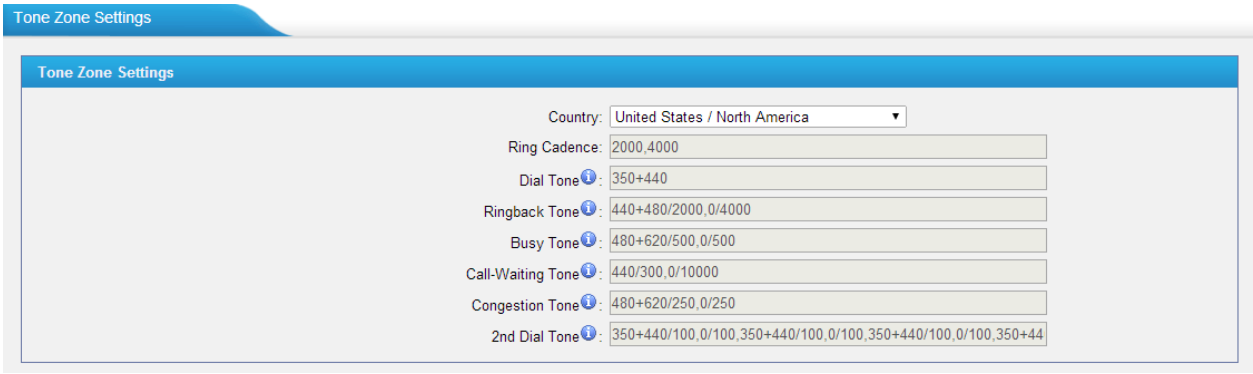


Figure III-4-20 Tone Zone Settings

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

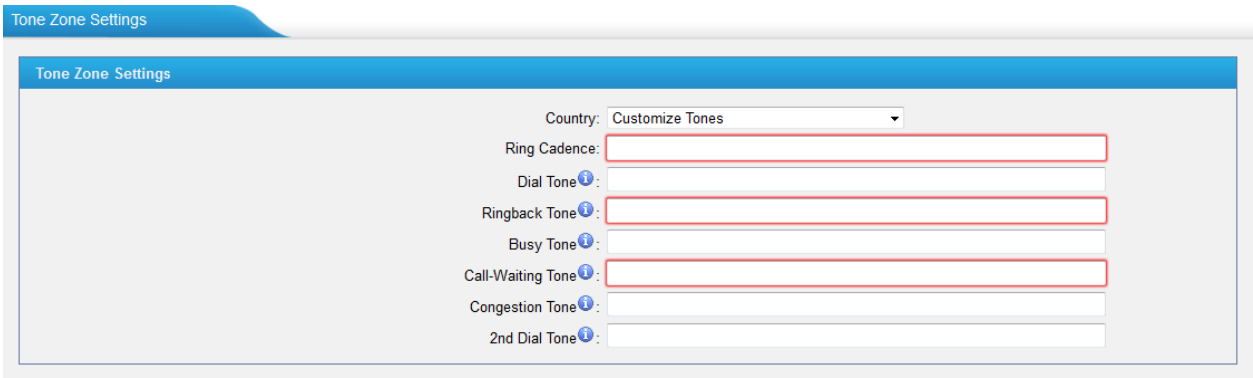


Figure III-4-21 Customize Tones

Table III-4-13 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 FXO 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.

4.5.1 DTMF Settings

DTMF signal sent from NeoGate TA to the receiver can be set on this page.
DTMF Digit Length: Default is 100ms.
DTMF Digit Volume: Range from -31 to 0 dB
DTMF Dial Pause: Default is 100ms.

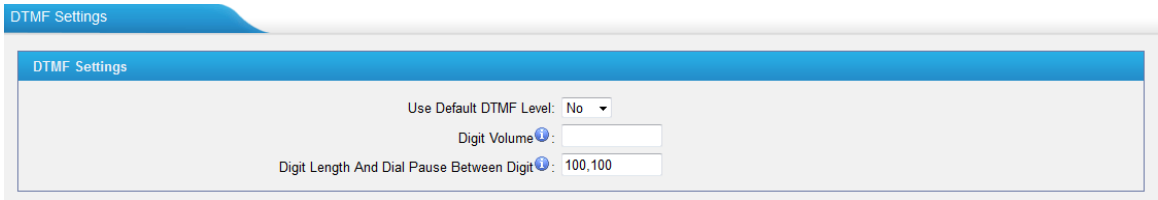


Figure III-4-22 Customize Tones

[The End]