



TA410/810
User Manual

Version 41.19.0.15

Yeastar Information Technology Co. Ltd

Contents

Contents	2
Introduction	4
Application Description	5
Configuration Guide	9
1. Login	9
2. Status	11
2.1 System Status.....	11
2.1.1 Port Status.....	11
2.1.2 Network status.....	12
2.1.3 System Info	12
2.2 Reports	12
2.2.1 Call Logs	13
2.2.2 System Logs.....	13
2.2.3 Packet Monitor Tool	14
3. System	15
3.1 Network Preferences.....	15
3.1.1 LAN Settings.....	15
3.1.2 Service	16
3.1.3 VLAN Settings	16
3.1.4 VPN Settings	17
3.1.5 DDNS Settings	18
3.1.6 Static Route	19
3.2 Security Center	20
3.2.1 Security Center.....	20
3.2.2 Alert settings.....	21
3.2.3 AMI Settings	24
3.2.4 Certificates	25
3.2.5 Firewall Rules	26
3.2.6 IP Blacklist.....	27
3.3 System Preferences.....	28
3.3.1 Password settings	28
3.3.2 Date and Time	29
3.3.3 Email Settings.....	29
3.3.5 Auto Provision Settings.....	30
3.3.6 Firmware Update	32
3.3.7 Backup and Restore	33
3.3.8 Reset and Reboot.....	33
4. Gateway	34

4.1 FXO Port List	34
4.1.1 FXO Port List.....	34
4.1.2 Port Group.....	37
4.2 VoIP Settings	38
4.2.1 VoIP Trunk.....	38
4.2.2 Trunk Group.....	40
4.2.3 SIP Settings.....	41
4.2.4 IAX Settings.....	46
4.3 Routes Settings.....	47
4.3.1 IP->Port.....	47
4.3.2 IP->Port	49
4.3.3 Blacklist	51
4.3.3 Callback Settings	51
4.4 Gateway Settings.....	52
4.4.1 General Preferences.....	52
4.5 Audio Settings.....	53
4.5.1 Custom Prompts.....	53
4.6 Advanced Settings	54
4.6.1 Tone Zone Settings.....	54
4.5.1 DTMF Settings.....	55

Introduction

YeastarTA410/810 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, TA410/810 is ideal for small and medium enterprises that wish to integrate a traditional phone system into IP-based system. TA410/810 helps them to preserve previous investment on legacy telephone system and reduce communication costs significantly with the true benefits of VoIP.

Features

● 4/8 FXO ports
● Fully compliant with SIP and IAX2
● Flexible calling rules
● Configurable VoIP Server templates
● Codec: G.711 a/u-law, G.722, G.723,G.726, G.729A/B, GSM,ADPCM
● 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>

Yeastar TA410/810 FXO Gateway features 4, 8 FXO interfaces for connection of PSTN and PBX extension and one 10/100 Mbps LAN port.

For more information about the Yeastar TA hardware specification and how to install the Yeastar 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 TA FXO Gateway

YeastarTA FXO gateway is a solution to extend FXO ports for your IPPBX.

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

Three modes are available for you to connect your SIP server and TA410/810 gateway. We call them SIP Account Mode, VoIP Mode and SPS (Service Provider SIP) Mode. You can choose any one of the 3 modes to connect your SIP server and TA410/810. SPS Mode is recommended.

Account Mode:

Create one SIP account on TA410/810, and take the SIP account to register one SIP trunk on your SIP server. Then TA410/810 and your SIP server are connected by the account.

➤ **Calls from SIP to PSTN**

- 1) Create one outbound route on your SIP sever, and select the SIP trunk you have registered just now.
- 2) Configure a "IP->Port" route on TA410/10, choose the SIP account in the field "Call Source", and choose a PSTN trunk or PSTN trunk group in the field "Call Destination".
- 3) Make a call from your SIP Server and the call should match the outbound route dial rules.

➤ **Calls from PSTN to SIP**

- 1) Create an inbound route on your SIP server, and select the SIP trunk you have registered just now.
- 2) Configure a "Port->IP" route on TA410/810, choose a PSTN trunk or PSTN trunk group in the field "Call Source", and choose the SIP account in the filed "Call Destination".
- 3) When a call comes to PSTN trunk on TA410/810, the call will be routed to the destination of the SIP server inbound route.

➤ **Register SIP account on IP phone**

With account mode, you can directly take the SIP account to register on your SIP phone or softphone; then make calls from softphone though PSTN trunk on TA410/810 and receive incoming calls on your SIP phone or softphone. In this way, you don't have to set up any SIP server.

VoIP Mode

Take a SIP account from your SIP server, and register it on TA410/810 as a VoIP trunk. In this way, TA410/80 and your SIP server are connected.

➤ **Calls from SIP to PSTN**

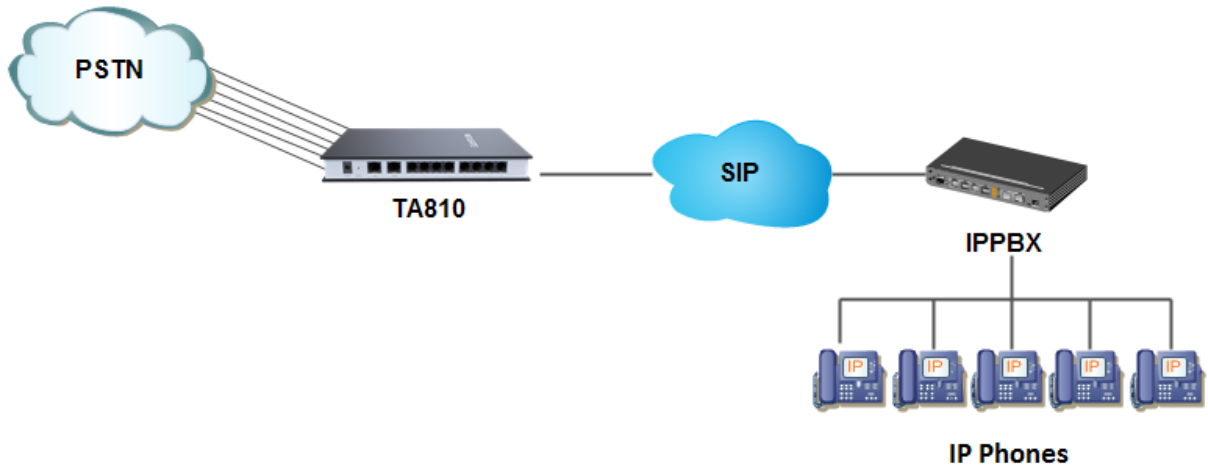
- 1) Configure a IP-> Port route on TA410/810; choose the VoIP trunk in the field “Call Source”, and choose PSTN trunk in the field “Call Destination”. **Enable Two-stage Dialing** on the route.
 - 2) Make a call from your SIP server, dial the SIP account number which is registered on TA410/810. You will hear a dial tone, then dial the external number out through PSTN trunk.
- **Calls from PSTN to SIP**
- 1) Configure a Port->IP route on TA410/TA810, choose PSTN trunk in the field “Call Source”, and choose the SIP trunk in the field “Call Destination”.
 - 2) When an incoming call reaches PSTN trunk on TA410/810, you will hear a dial tone, then dial an extension number of the SIP server.

SPS Mode(Recommended)

Create a Service Provider SIP trunk on TA410/810 to connect to your SIP server. Add another Service Provider SIP trunk on your SIP server, connecting to TA410/810.

- **Calls from SIP to PSTN**
- 1) Create one outbound route on your SIP sever, and select the SIP trunk you have created just now.
 - 2) Configure a IP->Port route on TA410/810, choose the SPS trunk in the field “Call Source”, and choose PSTN trunk in the field “Call Destination”.
 - 3) Make a call from your SIP Server and the call should match the outbound route dial rules.
- **Calls from PSTN to SIP**
- 1) Configure a Port->IP route on TA410/810, choose PSTN trunk in the field “Call Source”, and choose the SPS trunk in the field “Call Destination”.
 - 2) Create one inbound route on your SIP server and select the SIP trunk created just now.
 - 3) When an incoming call reaches PSTN trunk on TA41/810, You will hear a dial tone, then dial an extension number of the SIP Server, it will be routed to the destination of the SIP server inbound route.

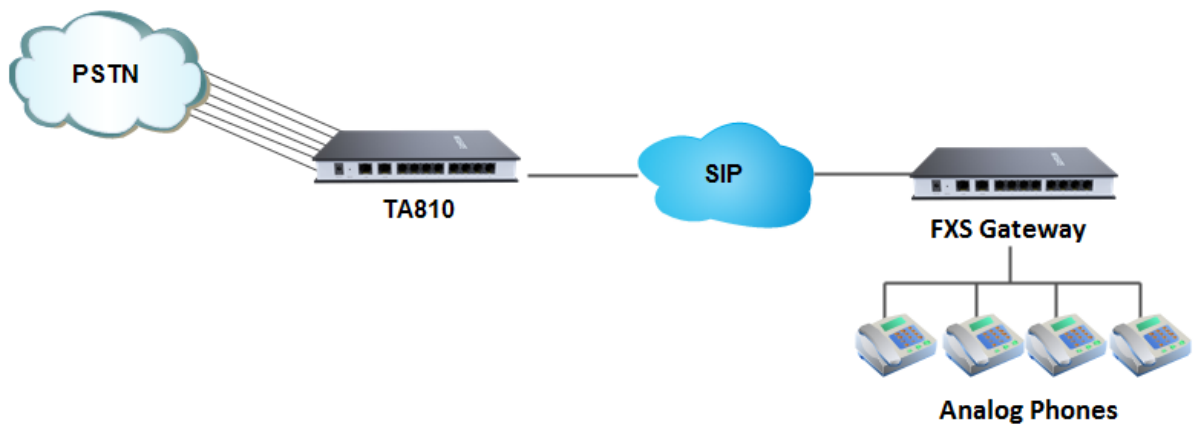
Note:if you want the call to go directly to the destination number of your SIP server, you don't have to create an inbound route on SIP server, instead set a **Hotline** number on TA410/810 route.



For incoming calls from the PSTN to TA410/810, TA410/810 will forward the call to a configured SIP extension or to an inbound destination of IPPBX like IVR.

Connect TA FXO Gateway and FXS Gateway

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 connected to Site A's provider). With this solution, you can call a local number using a local PSTN line wherever you are.



Configuration Guide

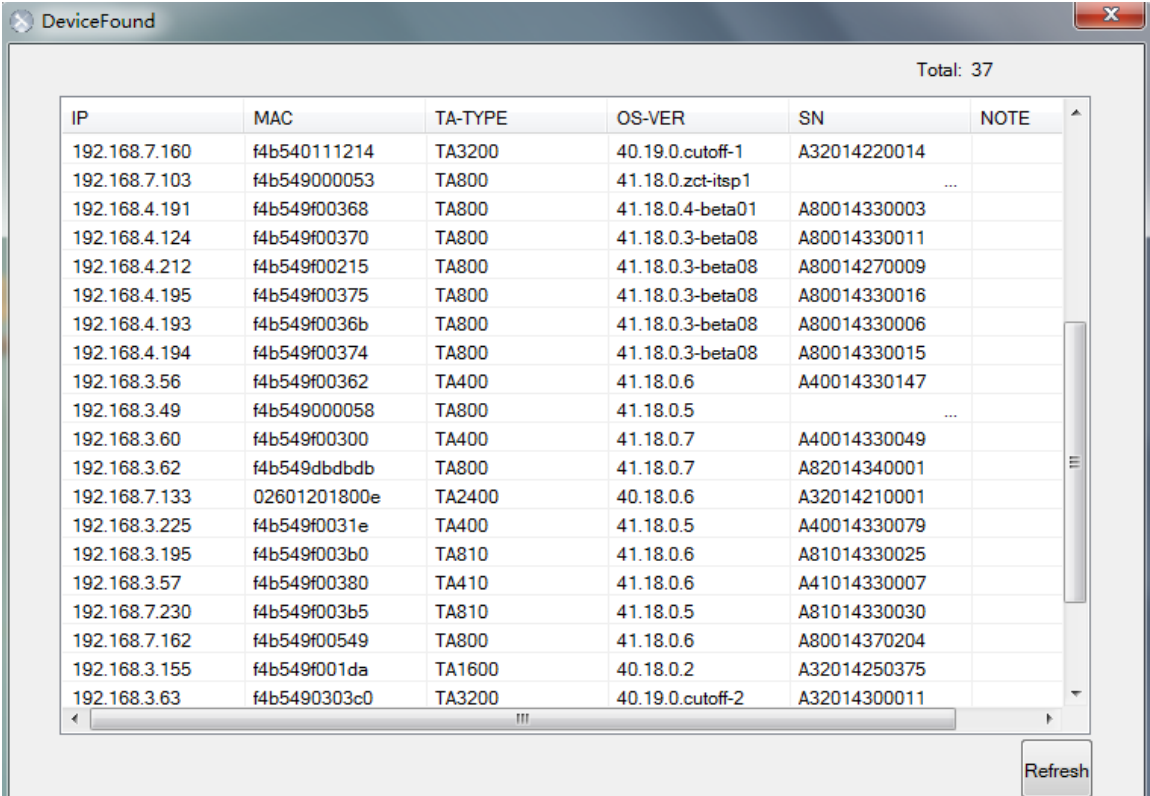
1. Login

The TA gateway 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 TA40/810 IP address.

How to check TA410/810 IP address:

1. Download a DeviceFound tool from Yeastar website: [FindTA.rar](#)
2. Run the DeviceFound.exe software.
3. The detected 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.



The screenshot shows the DeviceFound application window with a table of detected devices. The table has columns for IP, MAC, TA-TYPE, OS-VER, SN, and NOTE. The total number of devices found is 37. A Refresh button is located at the bottom right of the window.

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	

Figure1-1 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 192.168.10.125, the model is TA810.

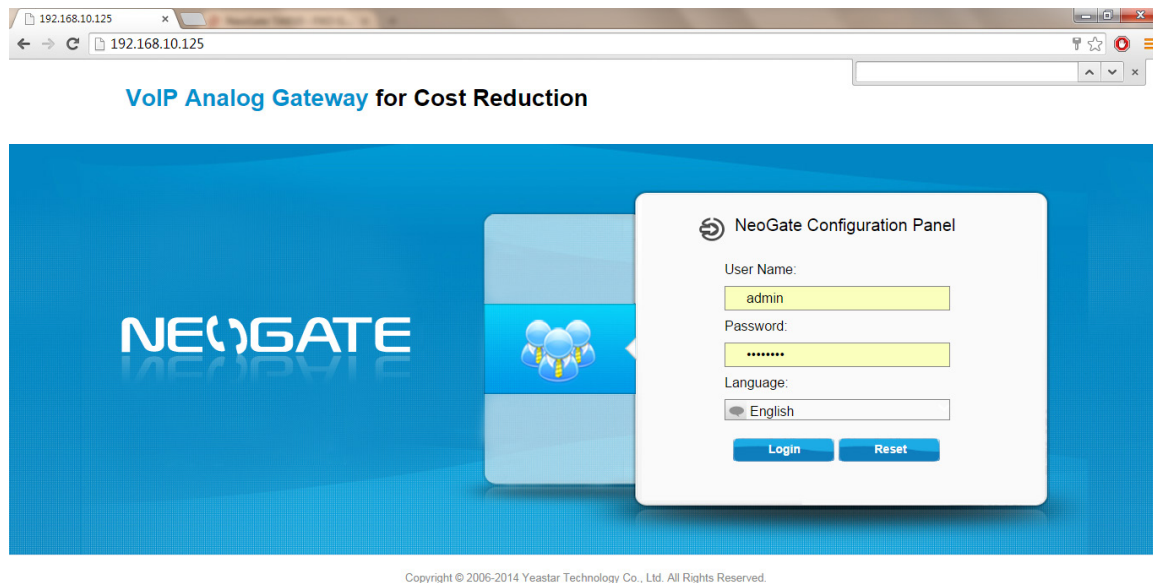


Figure1-2 TA Login page

Click "Login" to get the welcome page.

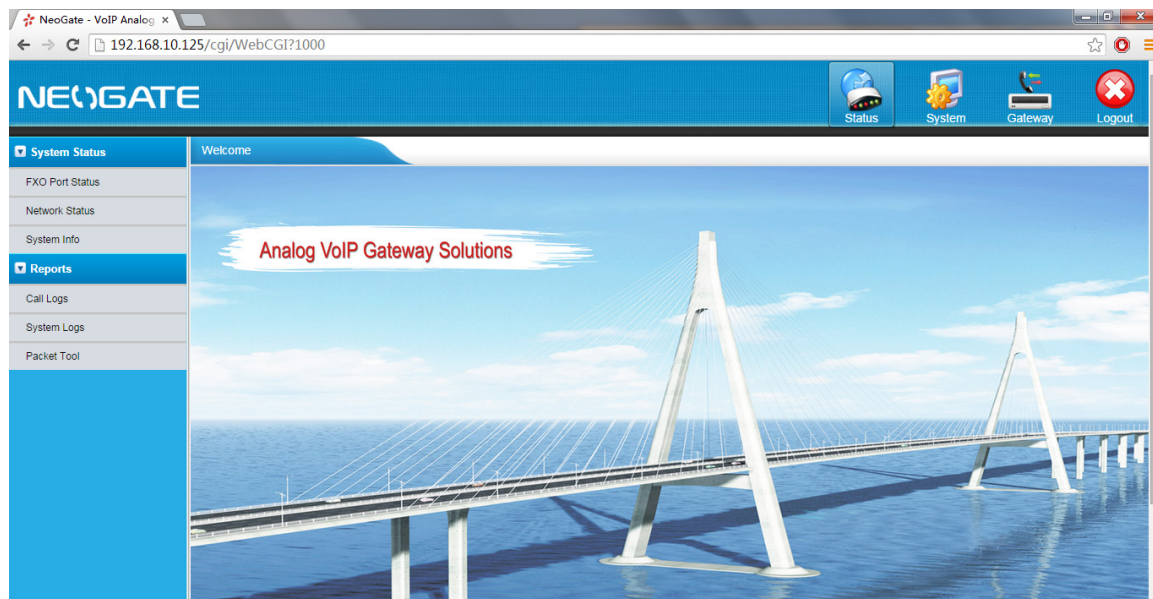



Figure1-3 Login TA

2. Status



Click  to check the status of 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	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 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.



The screenshot shows the 'Network Status' page with a 'LAN' section expanded. The configuration details are as follows:

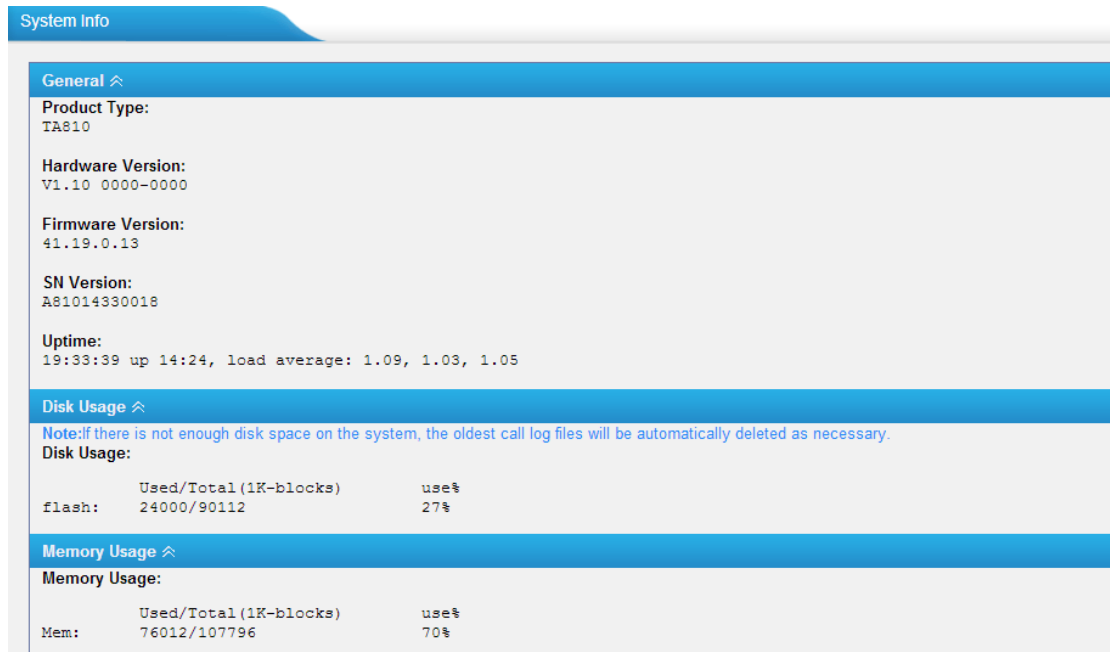
Hostname :	TA810
Type :	Static IP Address
MAC Address :	f4:b5:49:f0:03:a9
IP Address :	192.168.10.125
Subnet Mask :	255.255.255.0
Gateway :	192.168.10.1
Primary DNS :	8.8.8.8
Secondary DNS :	

Figure 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 TA.



The screenshot shows the 'System Info' page with the 'General' section expanded. The information is as follows:

General

- Product Type: TA810
- Hardware Version: V1.10 0000-0000
- Firmware Version: 41.19.0.13
- SN Version: A81014330018
- Uptime: 19:33:39 up 14:24, load average: 1.09, 1.03, 1.05

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:	24000/90112	27%

Memory Usage

Memory Usage:		
	Used/Total (1K-blocks)	use%
Mem:	76012/107796	70%

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.

The screenshot shows the 'Call Logs' interface. At the top, there is a 'Search Condition' section with the following fields: Start Date (04 Jun 2014), End Date (04 Jun 2014), Caller/Callee (empty), Trunk (All), Duration (empty), Billing Duration (empty), Status (All), and Communication Type (All). A 'Start Searching' button is located to the right of these fields. Below the search section, there are two buttons: 'Download the recordings' and 'Delete the recordings'. To the right of these buttons, it says 'Total: 39 Show: 1-25 View: 25'. Below this is a table with the following columns: Time, Caller, Callee, Source Server/Port, Destination Server/Port, Duration, Billing Duration, Status, and Communication Type. The table contains five rows of call records.

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		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 TA.

The screenshot shows the 'System Logs' interface. At the top, there are two buttons: 'Download The Selected Logs' and 'Delete The Selected Logs'. Below this is a table with the following columns: Name, Download, and Delete. The table contains ten rows of log files. Below the table is an 'Options' section with four checkboxes: 'Enable Hardware Log', 'Enable Normal Log', 'Enable Debug Log', and 'Enable Web Log'.

Name	Download	Delete
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 Monitor Tool

This feature is used to capture packets for technician. Integrate packet capture tool “Wireshark” is integrated in TA410/810.

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

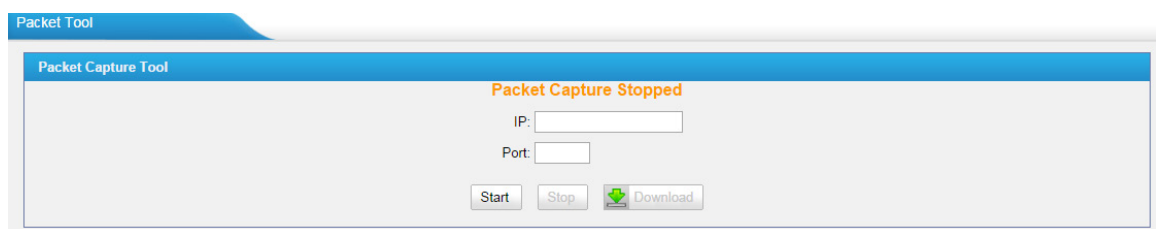


Figure 2-6 Packet Tool

·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

The screenshot shows the 'LAN Settings' page with the 'General Settings' tab selected. The 'Mode' is set to 'Static IP Address'. The following fields are visible:

- Hostname: TA810
- Mode: Static IP Address
- IP Address: 192.168.10.125
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.10.1
- Primary DNS: 8.8.8.8
- Secondary DNS: (empty)
- IP Address2: (empty)
- Subnet Mask2: (empty)

Figure 3-1 Static IP Address Mode

Table 3-1 Description of LAN Settings

Items	Description
Hostname	Set the host name for TA
Static IP Address	Set the TA's IP address as a static IP
IP Address	Set the IP Address for TA. It is recommended that you configure a static IP address for TA.
Subnet Mask	Set the subnet mask for TA
Gateway	Set the gateway for TA
Primary DNS	Set the primary DNS for TA.
Secondary DNS	Set the secondary DNS for TA
IP Address2	Set the second IP Address for TA
Subnet Mask2	Set the second subnet mask for TA

The screenshot shows the 'LAN Settings' page with the 'General Settings' tab selected. The 'Mode' is set to 'DHCP'. The following fields are visible:

- Hostname: TA810
- Mode: DHCP

Figure 3-2 DHCP Mode

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

The screenshot shows the 'LAN Settings' page with a sub-section for 'General Settings'. It contains the following fields:

- Hostname: TA810
- Mode: PPPoE (dropdown menu)
- User Name: (empty text box)
- Password: (empty text box)

Figure 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 TA on the "Service" page.

The screenshot shows the 'Service' page with two sections:

- General Service Settings:**
 - Enable SSH: Yes (dropdown) Port: 8022
 - Enable FTP: Yes (dropdown) Port: 21
- Web Server:**
 - HTTP: Enabled (dropdown)
 - HTTP Bind Port: 80
 - HTTPS: Disabled (dropdown)
 - HTTPS Bind Port: 443

Figure 3-4 Service Settings

Table 3-2 Description of Service Settings

Items	Description
SSH	By using SSH, you can log in to TA410/810 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:

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

The screenshot shows a web-based configuration interface for VLAN settings. The main window is titled 'VLAN Settings' and contains a sub-section 'VLAN Over LAN'. This section is divided into two numbered entries, NO.1 and NO.2. Each entry starts with a checkbox. Below each checkbox are four text input fields: 'VLAN Number', 'VLAN IP Address', 'VLAN Subnet Mask', and 'Default Gateway'. At the bottom of the configuration area, there are two buttons: a green 'Save' button and a red 'Cancel' button.

Figure 3-5 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 TA gateway VLAN over LAN.
VLAN Subnet Mask	Set the Subnet Mask for TA gateway VLAN over LAN.
Default Gateway	Set the Default Gateway for TA gateway 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 TA410/810 VLAN over LAN.
VLAN Subnet Mask	Set the Subnet Mask for TA410/810 VLAN over LAN.
Default Gateway	Set the Default Gateway for TA410/810 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. TA410/810 supports OpenVPN.

VPN Settings

General Settings

Enable VPN:

Import VPN Config: Browse...

Import

Save Cancel

Figure 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. TA410/810 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:

User Name:

Password:

Host Name:

Save Cancel

Figure 3-7 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

TA410/810 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 TA410/810 to force it to go out through different gateway when accessing to different internet.

The default gateway priority of TA410/810 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:

ID	Destination	Subnet Mask	Gateway	Metric	
1	--	--	--	--	<input type="button" value="X"/>
2	--	--	--	--	<input type="button" value="X"/>
3	--	--	--	--	<input type="button" value="X"/>
4	--	--	--	--	<input type="button" value="X"/>
5	--	--	--	--	<input type="button" value="X"/>
6	--	--	--	--	<input type="button" value="X"/>
7	--	--	--	--	<input type="button" value="X"/>
8	--	--	--	--	<input type="button" value="X"/>

Figure 3-8 Static Route

1) Route Table

The current route rules of TA410/810.

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 TA410/810.
Subnet Mask	Specify the destination network portion.
Gateway	Define which gateway TA410/810 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 TA410/810TA security configuration in “Security Center” page. And also, you can enter the relevant security settings page rapidly.

Firewall:

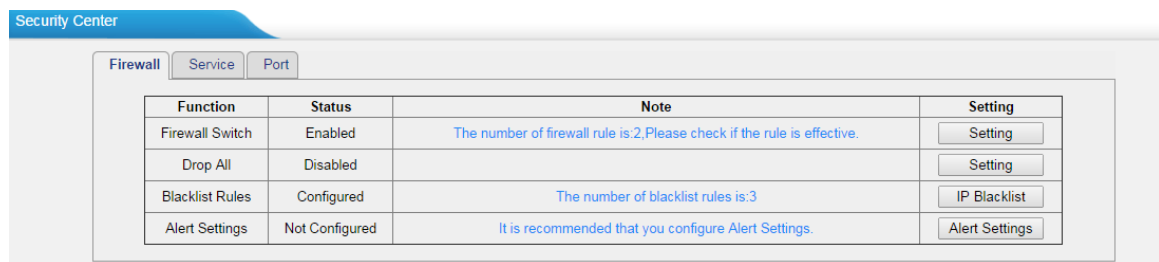


Figure 3-10 Firewall

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:

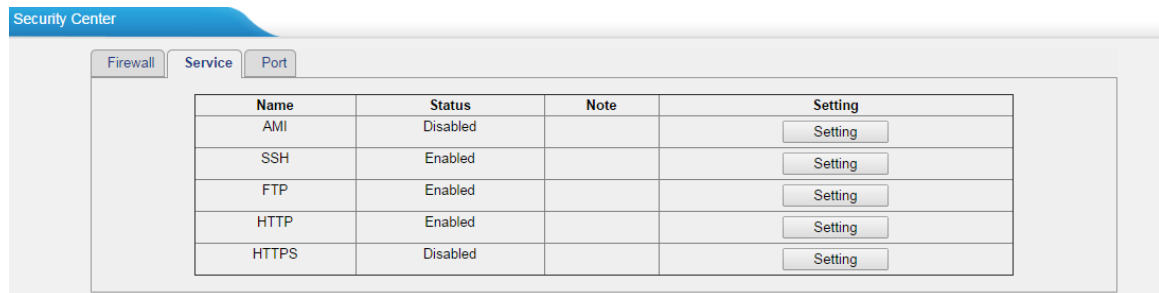


Figure 3-11 Service

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 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.

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

Figure 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 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.

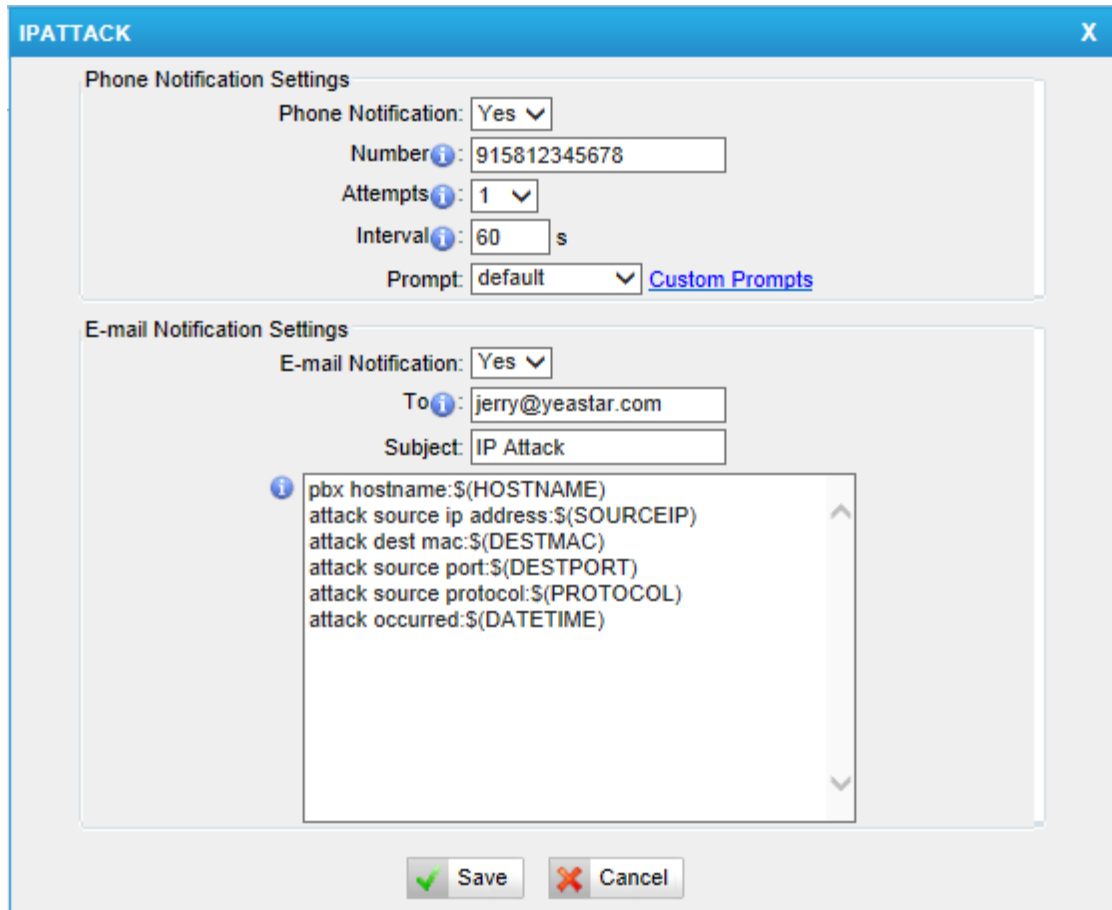
Prompt	Users will hear the prompt while receiving the phone notification.
--------	--

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)



The screenshot shows a configuration window titled "IPATTACK" with a close button (X) in the top right corner. The window is divided into two main sections: "Phone Notification Settings" and "E-mail Notification Settings".

Phone Notification Settings:

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

E-mail Notification Settings:

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

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

Figure 3-14 IP ATTACK Alert

2. WEBLOGIN

Web Login Alert Notification: entering the wrong password consecutively for five times when logging in TA410/810 Web interface will be deemed as an attack, the system will limit the IP login within 10 minutes and notify the user.

The screenshot shows a window titled "WEBLOGIN" with a close button (X) in the top right corner. The window is divided into two main sections: "Phone Notification Settings" and "E-mail Notification Settings".

Phone Notification Settings:

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

E-mail Notification Settings:

- E-mail Notification: Yes (dropdown menu)
- To: jerry@yeastar.com (text input field)
- Subject: Web Login (text input field)
- Message body (text area):


```
pbx hostname:${HOSTNAME}
login ip address:${SOURCEIP}
login username:${USERNAME}
login occurred:${DATETIME}
```

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

Figure 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 TA410/810TA using AMI interface. It is disabled by default. If necessary, you can enable it.

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 3-16 AMI Settings

Username & password: after enabling AMI, you can use this username and password to log in TA410/810 AMI.

Permitted "IP address/Subnet mask": you can set which IP can log in TA410/810 AMI interface.

3.2.4 Certificates

TA410/810 can support TLS trunk. Before you register TLS trunk to TA410/810, you should upload certificates first.

Upload Certificate

Upload Certificate

Type: Trusted Certificate
Gateway Certificate

Choose a certificate to Upload:

Gateway Certificate

No Certificates Defined

Figure 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 TA410/810. If IPPBX enables "TLS Verify

server”, you should also upload this certificate on IPPBX.

3.2.5 Firewall Rules

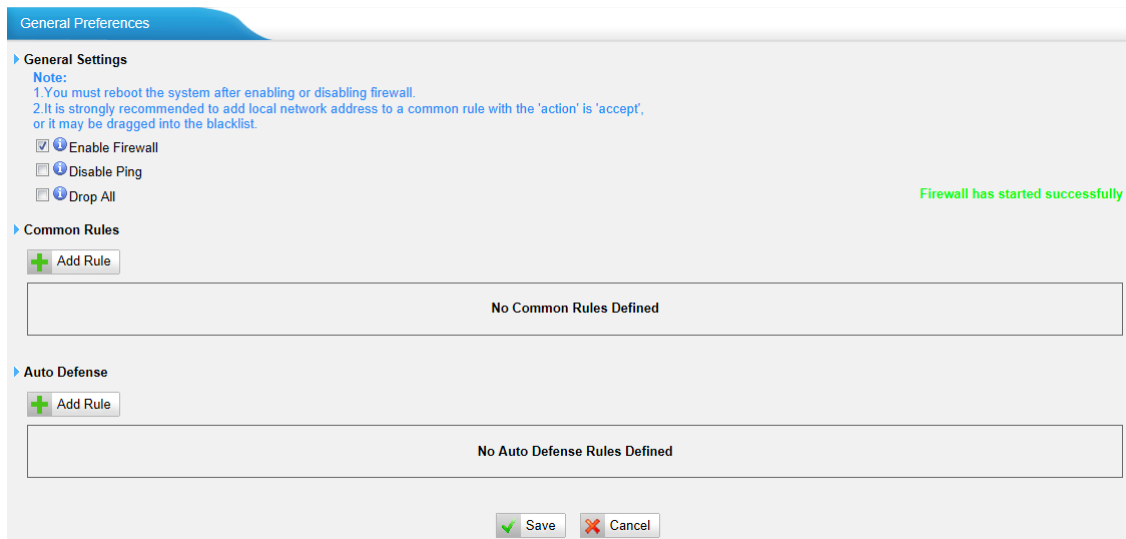


Figure 3-18 Firewall Rules

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.

Figure 3-19 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.

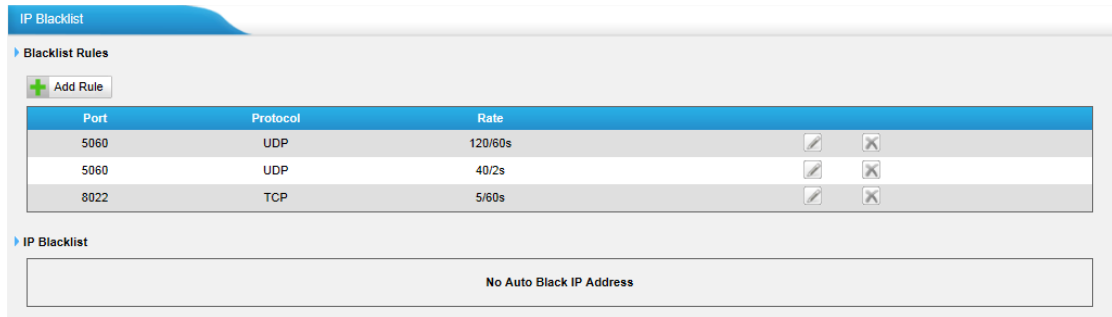


Figure 3-20 IP Blacklist

1) Blacklist rules

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

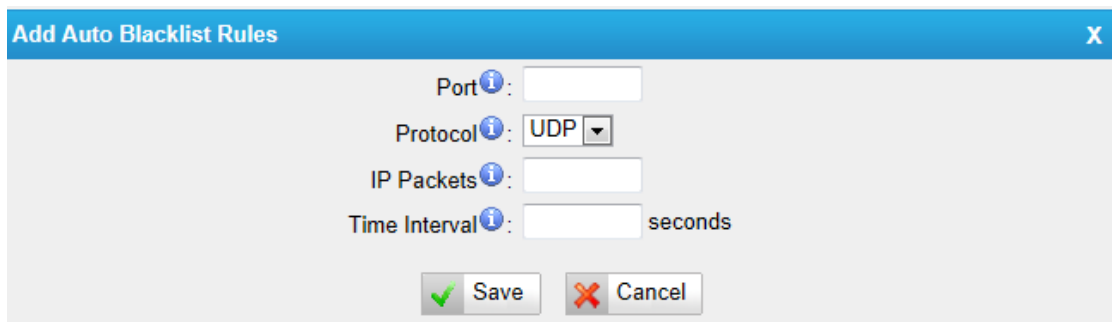


Figure 3-21 Auto Blacklist Rule

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.

Figure 3-22 Password Settings

3.3.2 Date and Time

Set the date and time for TA410/810.

Figure 3-23 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 TA410/810 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.

The screenshot shows the 'Email Settings' window with a sub-section for 'SMTP Settings for Email'. A note at the top states: 'Note: If you would like to send email when system alert or balance alarm occurs, please configure this section.' The settings include:

- E-mail Address: mypbx@sina.com
- Password: [Redacted]
- SMTP Server: smtp.sina.com
- Port: 25
- Use SSL/TLS to send secure message to server: [Unchecked]

 Buttons for 'Test SMTP Settings', 'Save', and 'Cancel' are visible at the bottom.

Figure 3-24 Email Settings

Table 3-12 Description of SMTP Settings

Items	Description
E-mail Address	The E-mail Address that TA410/810 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 TA410/810 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.

3.3.5 Auto Provision Settings

Three Methods are supported for Auto Provision: PNP, DHCP and you can manually configure a server URL to get the configuration file from the server.

The screenshot shows the 'Provision's Way' configuration section with three dropdown menus:

- PNP: Yes
- DHCP: No
- Server URL: No

Figure 3-25 Auto Provision Methods

PNP and **DHCP** modes work along with MyPBX "NeoGate Provisioning". Firstly, users need to configure TA410/810 on MyPBX "NeoGate Provisioning" page. Then TA410/810 will find and get the configuration file from MyPBX during boots up.

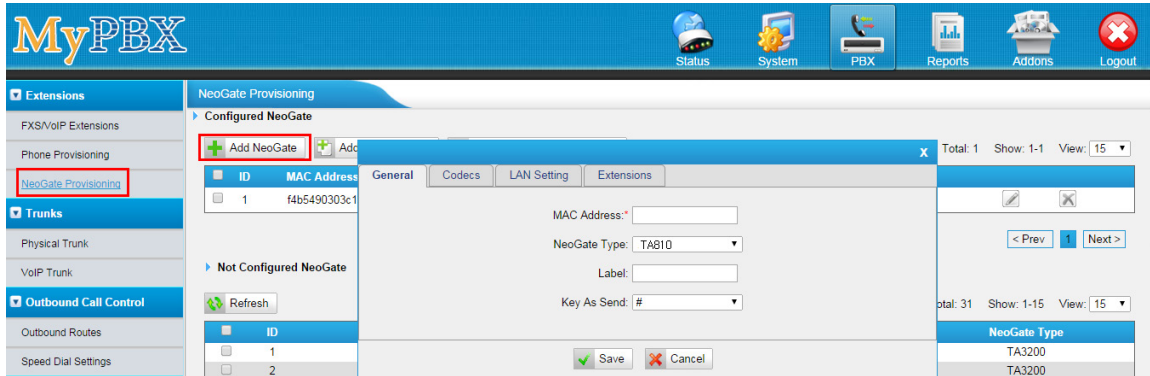


Figure 3-26 MyPBX NeoGate Provisioning

If you use **DHCP** mode to do auto provision, you should enable DHCP Server on MyPBX to make it as a DHCP server. (System→Network Preferences→DHCP Server).

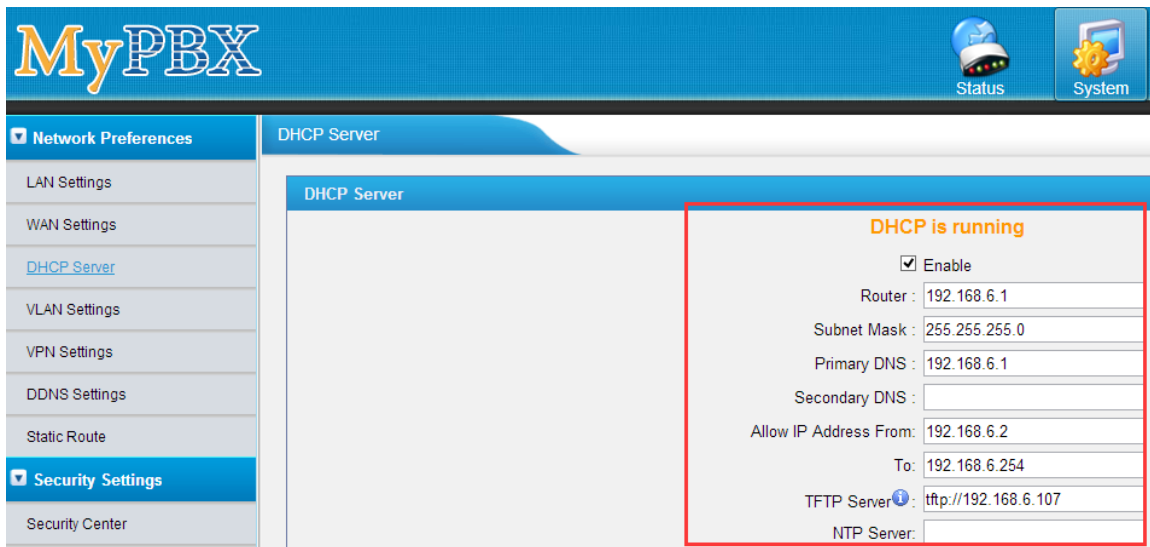


Figure 3-27 Set MyPBX as a DHCP Server

Then select DHCP mode on LAN settings page to make TA410/810 as a DHCP client.

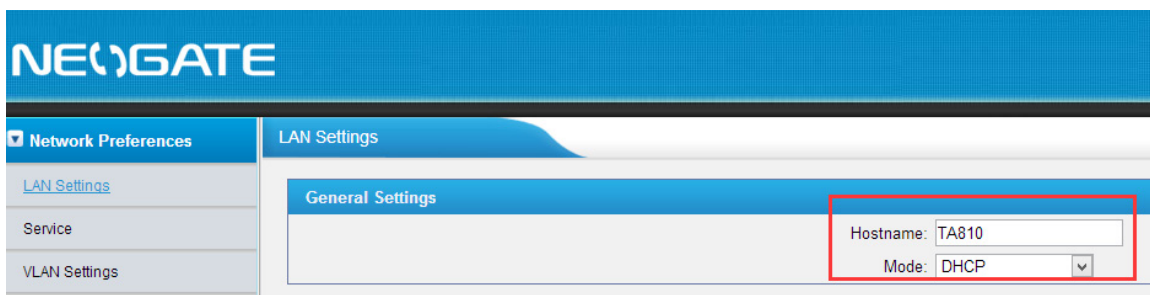


Figure 3-28 Set TA410/810 as a DHCP Client

Another way to do auto provision is to download configuration file from the configured server URL. Fill in the URL, user name, password, and set the time, TA410/810 will get the configuration file from the server automatically and regularly.

Note: if there is no user name and password for the server, leave these fields blank.

The screenshot shows two configuration sections. The 'Server Settings' section includes fields for 'Server URL', 'User Name', and 'Password', each with an information icon. Below these are two radio button options: 'Interval of time' (set to 180 Minute) and 'Specified time' (set to Everyday 00:00). The 'Other' section includes an 'AES Key' field and an 'Always Apply' dropdown menu set to 'No'.

Figure 3-29 Server Address

Other Settings for Auto Provision

- AES Key:**
 If the configuration file is encrypted by AES key, you need to fill the key in this field.
- Always Apply:**
 Whether to check the new configuration and apply to TA410/810.

3.3.6 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:

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

The screenshot shows the 'Update System Firmware' section. It features a 'Firmware Download Source' section with two radio buttons: 'HTTP URL' (selected) and 'TFTP Server'. Below this is an 'HTTP URL' input field and a 'Reset Configuration to Factory Defaults' checkbox. A 'Start' button is located at the bottom of the configuration area.

Figure 3-30 Firmware Update

3.3.7 Backup and Restore

We can back up the configurations before resetting TA410/810 to factory defaults, and then restore it on this package.

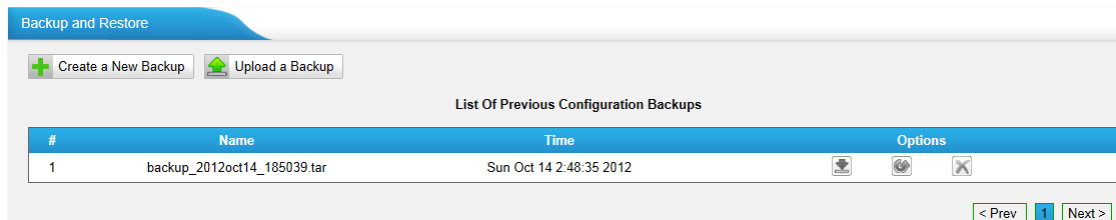


Figure 3-31 Backup and Restore

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.

3.3.8 Reset and Reboot

We can reset or reboot TA410/810 directly in this page.

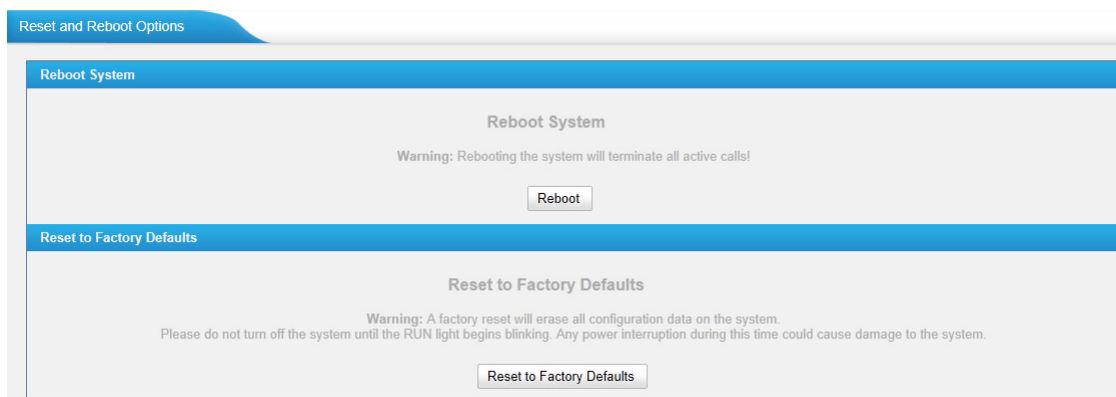


Figure 3-32 Reset and Reboot

·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

All the FXO ports are listed here. You can edit each FXO port by clicking the "Edit" button.

>General

Table4-1 Description of FXO Port General Settings

Items	Description
Name	The trunk Name.
RX Gain	The receive volume. The default setting is 40%.
TX Gain	The transmit volume. The default setting is 40%.
AC Termination Impedance	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) 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

> Call Duration Settings

Table4-2 Description of FXO Port Call Duration Settings

Items	Description
Single Call Max Duration(min)	Configure the duration of each call, it's 0 by default, which means no limit.
Round up Duration	Once the value of Billing Unit is changed, the "Round Up Duration" will be cleared, "Call Duration" will also change accordingly.
Max. Call Duration(min)	Defines the maximum number of billing unit called within a month through the trunk. To disable this limitation set the value at 0.
Enable Clear Stat.	The date to clean the duration status each month.
Balance Alarm Settings	When Max. Call Duration(min) is configured a 0 (no limit), this feature is disabled.
Alarm threshold(min)	Configure the time duration when TA410/810 will send the alarm message. The value must be less than "Max Call Duration".
Port	Choose the port to dial the alarm call.
Number	The number to receive the alarm call.
Prompt	The prompt played during the alarm call, you can customize the prompts as your wish.
E-mail	The email address to receive the alarm email. Note: please make sure SMTP test is successful in "Email settings" page before configuring this.

> Other Settings

Table4-3 Description of FXO Port Other Settings

Items	Description	
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	<p>Answer Detection settings are configured for accurate billing.</p> <p>Select which type to detect the call as answered.</p> <p>1) Default. TA410/810 will start to charge once you grab the PSTN trunk to call out, whether the call is answered or not.</p> <p>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 TA410/810 starts to bill.</p> <p>3) Ringback Tone: If you choose this option, TA410/810 will charge the call according to PSTN ring back tone detection. When the "ring duration" or the "ring interval duration" detected on TA410/810 is larger than the standard or custom parameters, the call is detected as ANSWERED.</p> <p>*Standard parameters: when you configure the "Tone Zone Settings" you get the country's standard tone parameters.</p>
	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	Max pause between the two ring tones.

	Duration	
	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.

4.1.2 Port Group

Port group is a feature that allows you to define specific PSTN trunks to a group. A trunk group can be used in a route. When a call is coming or going through the route, an available trunk would be selected in the trunk group. There are two ring strategies supported for Port Group:

- Round-Robin: select the next available port in line.
- Least Used: select the port that is least used.

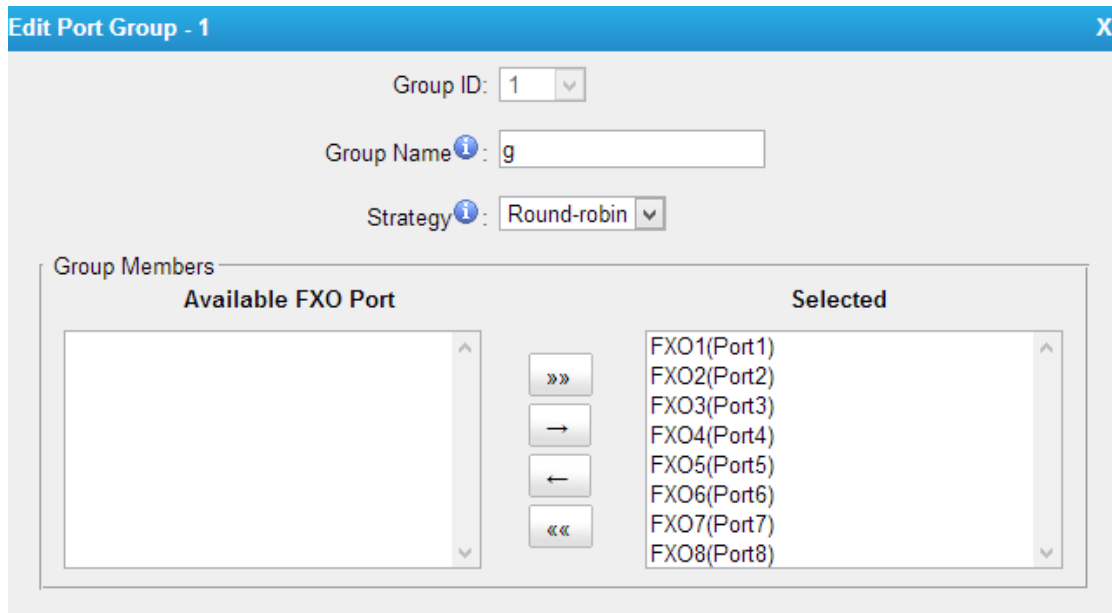


Figure4-1 Port Group

4.2 VoIP Settings

To integrate with other IPPBX, we need to configure the VoIP settings in TA410/810 to setup VoIP trunk (SIP and IAX).

4.2.1 VoIP Trunk

There are 3 types of trunks listed in this page, Account, Trunk and Service Provider.

VoIP Trunks							
VoIP Trunks							
+ Add VoIP Trunk							
Name	Type	Transport	Hostname/IP	Max. Call Duration(min)	Call Duration(min)	Clear Stat.	
1000	Account	udp	--	0	8	0	
1001	Account	udp	--	0	0	0	
PBX	VoIP Trunk	udp	192.168.6.31	0	0	0	

Figure 4-2 VoIP Trunk

1) Account

It's an SIP account created in TA410/810 so that the other devices can register SIP trunk at their side using these information.

Figure 4-3 Account

Table 4-4 Description of Account Settings

Items	Description
Trunk Type	Choose the type of trunk, "Account".
Name	Define the name.
Account	Define the Account number.
Password	Set a password for this account.

2) VoIP Trunk

It's a SIP trunk configured in TA410/810 to register to the SIP provider, please make sure this trunk works properly in advance with provider before configuring TA410/TA810.

Figure 4-4 VoIP Trunk Settings

Table 4-5 Description of VoIP Trunk Settings

Items	Description
Trunk Type	Choose the type of trunk, "VoIP Trunk".
Provider Name	A unique label to help you identify this trunk when listed in outbound rules, incoming rules etc. E.g. "yeastar".

Hostname/IP	Service provider's hostname or IP address. Note: 5060 is the standard port number used by SIP protocol. Don't change this part if it is not required.
Domain	VoIP provider's server domain name or IP address.
User Name	User name of SIP account provided from the SIP Server provider.
Authorization Name	Authorization Name of SIP account provided from the SIP Server provider.
Password	Password of the SIP account.

3) Service Provider

This is service provider trunk (peer to peer mode) which authorized using IP address only.

Figure 4-5 Service Provider Trunk Settings

Table 4-6 Description of Service Provider Trunk Settings

Items	Description
Trunk Type	Choose the type of trunk, "Service Provider".
Provider Name	A unique label to help you identify this trunk when listed in outbound rules, incoming rules etc. E.g. "yeastar".
Hostname/IP	Service provider's hostname or IP address. Note: 5060 is the standard port number used by SIP protocol. Don't change this part if it is not required.

4.2.2 Trunk Group

Trunk group is a feature that allows you to define specific SIP trunks to a group. A trunk group can be used in a route. When a call is coming or going through the route, an available trunk would be selected in the trunk group.

Figure 4-6 Trunk Group

4.2.3 SIP Settings

This is the SIP settings in TA410/810, including General settings, NAT, Codecs, QoS, Response Code, and advanced settings.

1) General

Figure 4-7 SIP General Settings

Table 4-7 Description of SIP General Settings

Items	Description
UDP Port	Port used for SIP registrations. The default is 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 TA410/810 as a TLS client, whether or not to verify server's certificate. It is "No" by default.
TLS Verify Client	When using TA410/810 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 TA410/810 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, TA410/810 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.
------------	---

2) NAT

SIP Settings

General NAT Codecs QOS Response Code Advanced Settings

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:

Allow RTP Re-invite:

Figure 4-8 NAT Settings

Table 4-8 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

	<p>and reply to the sender's IP address/port.</p> <p>No = Use NAT mode only according to RFC3581.</p> <p>Never = Never attempt NAT mode or RFC3581 support.</p> <p>Route = Use NAT but do not include rport in headers.</p>
Allow RTP Reinvite	<p>By default, the system will route media streams from SIP endpoints through itself. Enabling this option causes the system to attempt to negotiate the endpoints to route packets to each other directly, bypassing the system. It is not always possible for the system to negotiate endpoint-to-endpoint media routing.</p>

3) Codecs

We can choose the allowed codec in TA410/810, 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

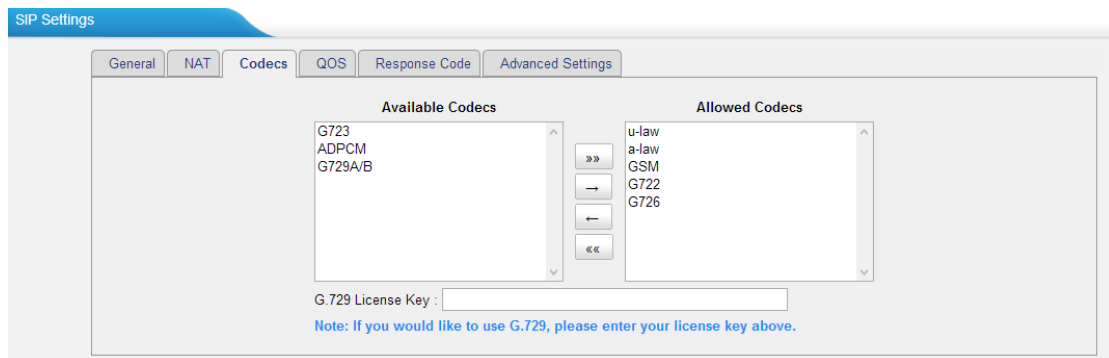


Figure 4-9 Codecs

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.

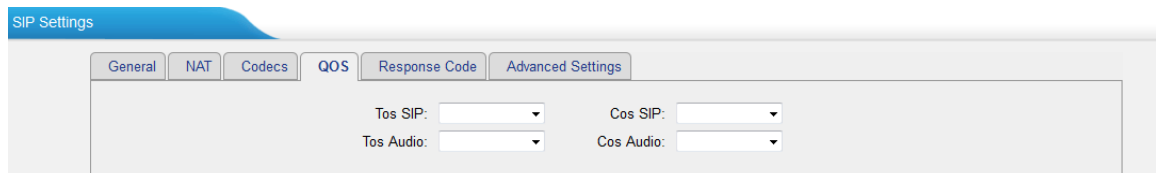


Figure 4-10 Qos

Note: It's recommended that you configure the QoS in your router or switch instead of TA410/810 side.

5) Response Code

You can change the response code on TA410/810 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.

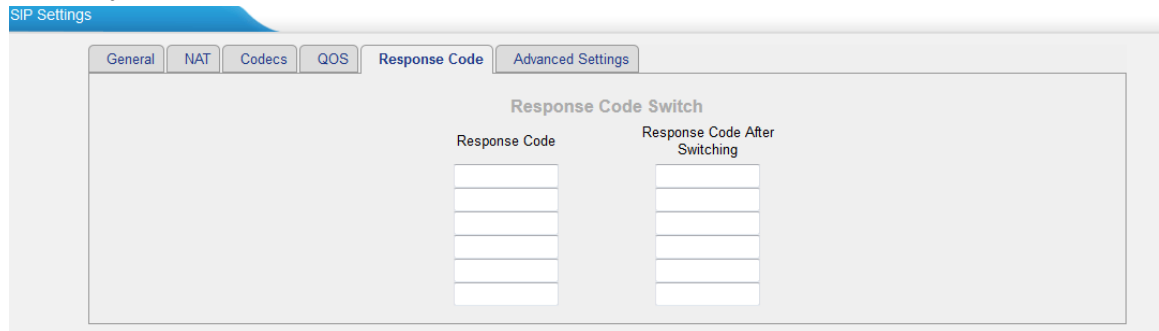


Figure 4-11 Response Code

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

6) Advanced Settings

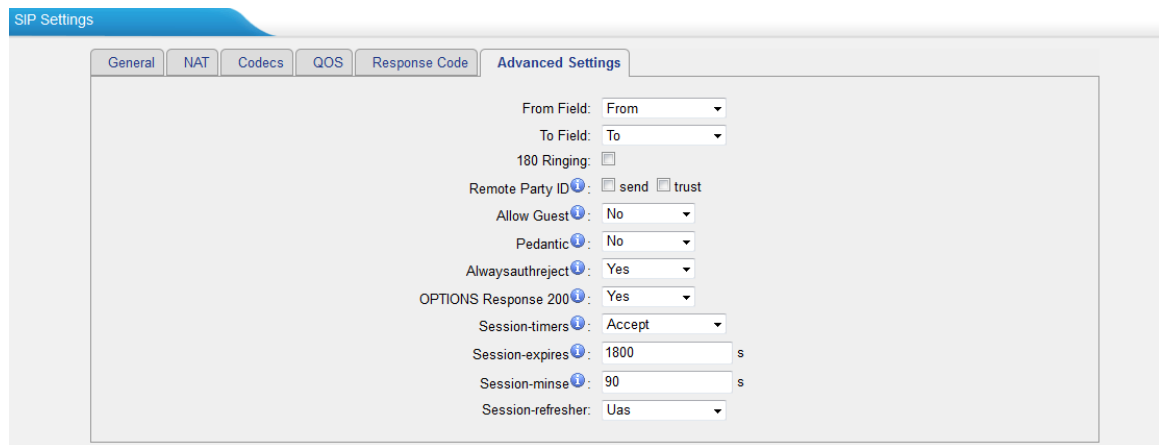


Figure 4-12 SIP Advanced Settings

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 TA410/810 rejects "Register"

	or “Invite” packets, TA410/81 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 TA410/810 or register IAX trunk to another IAX server. It’s supported by the asterisk-based IPPBX.

Figure 4-13 IAX Settings

Table 4-10 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 Routes Settings

4.3.1 IP->Port

Configure IP->Port routes to control calls from your SIP server to TA410/810 FXO ports.

Click “Edit” to check the route details, there are two modes for you.

1) Simple Mode

Choose “Yes” for Simple Mode, the simple mode configuration page appears as below.

Figure 4-14 Simple Mode Route

Table 4-11 Description of Simple Mode Route

Items	Description
Route Name	Define the route name.
Call Source	Choose the trunk or trunk group for the incoming calls.
Call Destination	Choose the trunk or trunk group to route the incoming calls to.
Hotline	Dial the number directly, The dial pattern is ignored.

2) Detail Mode

Choose “No” for Simple Mode, you will see the detailed configuration page as the following picture shows. Detailed settings for **Match Incoming Calls** and **Handle Matched Incoming Calls** are provided in Detailed Mode.

The screenshot shows a configuration window titled "IP->Port" with a close button (X) in the top right corner. The window is divided into several sections:

- Route Information:**
 - Route ID: 1 (dropdown)
 - Simple Mode: No (dropdown)
 - Route Name: MyPBX (text input)
- Match Incoming Calls:**
 - Call Source: SIP Trunk -- Skype (dropdown)
 - Inbound Caller Pattern: (text input)
 - DID Number: (text input)
 - DID Associated Number: (text input)
 - Enable Callback: No (dropdown) with a link to [Callback Settings](#)
- Incoming Calls Processing:**
 - Call Destination: Port5 -- FXO5 (dropdown)
 - Hotline: (text input)
 - Two Stage Dial: No (dropdown)
 - Outbound Dial Pattern: (text input)
 - Strip: (text input) digits from left
 - Prepend these digits: (text input) before dialing

Figure 4-15 Detailed Mode Route

Table 4-12 Description of Match Incoming Calls Settings

Items	Description
Call Source	Choose the trunk or trunk group for the incoming calls.
Inbound Caller Pattern	Match the prefix of caller ID for incoming calls.
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 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.

Table 4-13 Description of Handle Matched Incoming Calls Settings

Items	Description
Call Destination	Choose the trunk or trunk group to route the incoming calls to.
Hotline	Direct number to the SIP Server. The parameter is ignored

	if a SIP Account is selected on this route.
Two-stage Dialing	Enable or Disable Two-stage Dialing.
Outbound Dial Pattern	Outbound calls that match this dial pattern will use this outbound route.
Strip	Allows the user to specify the number of digits that will be stripped from the front of the phone number before the call is placed. For example, if users must press 0 before dialing a phone number, one digit should be stripped from the dial string before the call is placed.
Prepend	These digits will be prepended to the phone number before the call is placed. For example, if a trunk requires 10-digit dialing, but users are more comfortable with 7-digit dialing, this field could be used to prepend a 3-digit area code to all 7-digit phone numbers before calls are placed.

4.3.2 IP->Port

Port->IP/Port routes are used to control incoming calls to PSTN trunks on TA410/810 and route the calls to your SIP server or another PSTN trunk on TA410/810.

Click “Edit” to check the route details, there are two modes for you.

1) Simple Mode

Choose “Yes” for Simple Mode, the simple mode configuration page appears as below.

Figure 4-16 Simple Mode Route

Table 4-14 Description of Simple Mode Route

Items	Description
Route Name	Define the route name.
Call Source	Choose the trunk or trunk group for the incoming calls.
Call Destination	Choose the trunk or trunk group to route the incoming calls to.
Hotline	Dial the number directly, The dial pattern is ignored.

2) Detail Mode

Choose “No” for Simple Mode, you will see the detailed configuration page as the following picture shows. Detailed settings for **Match Incoming Calls** and **Handle Matched Incoming Calls** are provided in Detailed Mode.

Port->IP/Port

Route ID: 1

Simple Mode: No

Route Name: test

Match Incoming Calls:

Call Source: Port5 -- FXO5

Inbound Caller Pattern:

Enable Callback: No [Callback Settings](#)

Incoming Calls Processing:

Call Destination: SPS -- sps

Hotline: 8000

Outbound Dial Pattern:

Strip: digits from left

Prepend these digits: before dialing

Save Cancel

Figure 4-17 Detailed Mode Route

Table 4-15 Description of Match Incoming Calls Settings

Items	Description
Call Source	Choose the trunk or trunk group for the incoming calls.
Inbound Caller Pattern	Match the prefix of caller ID for incoming calls.
Enable Callback	Whether to enable callback feature.

Table 4-16 Description of Handle Matched Incoming Calls Settings

Items	Description
Call Destination	Choose the trunk or trunk group to route the incoming calls to.
Hotline	Direct number to the SIP Server. The parameter is ignored if a SIP Account is selected on this route.
Outbound Dial Pattern	Outbound calls that match this dial pattern will use this outbound route.
Strip	Allows the user to specify the number of digits that will be stripped from the front of the phone number before the call is placed. For example, if users must press 0 before dialing a phone number, one digit should be stripped from the dial string before the call is placed.
Prepend	These digits will be prepended to the phone number before the call is placed. For example, if a trunk requires 10-digit dialing, but users are more comfortable with 7-digit dialing, this field could be used to prepend a 3-digit area code to all 7-digit phone numbers before calls are placed.

4.3.3 Blacklist

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

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

The screenshot shows a dialog box titled "Add Blacklist" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Number:". Below it is a dropdown menu labeled "Type:" with a downward arrow. The dropdown menu is open, showing three options: "Inbound" (highlighted in blue), "Outbound", and "Both". At the bottom of the dialog, there are two buttons: a "Save" button with a green checkmark icon and a "Cancel" button.

Figure 4-18 Blacklist

4.3.3 Callback Settings

- 1) If you'd like to use callback feature, please make sure it's enabled on the IP->Port or Port->IP/Port route setting panel.
- 2) No callback rules needed to be set if the trunk supports call back with the caller ID directly.
- 3) Add Callback numbers, then callback will work for the added callback numbers. Tick "Allow All Numbers", callback feature will work for all numbers.

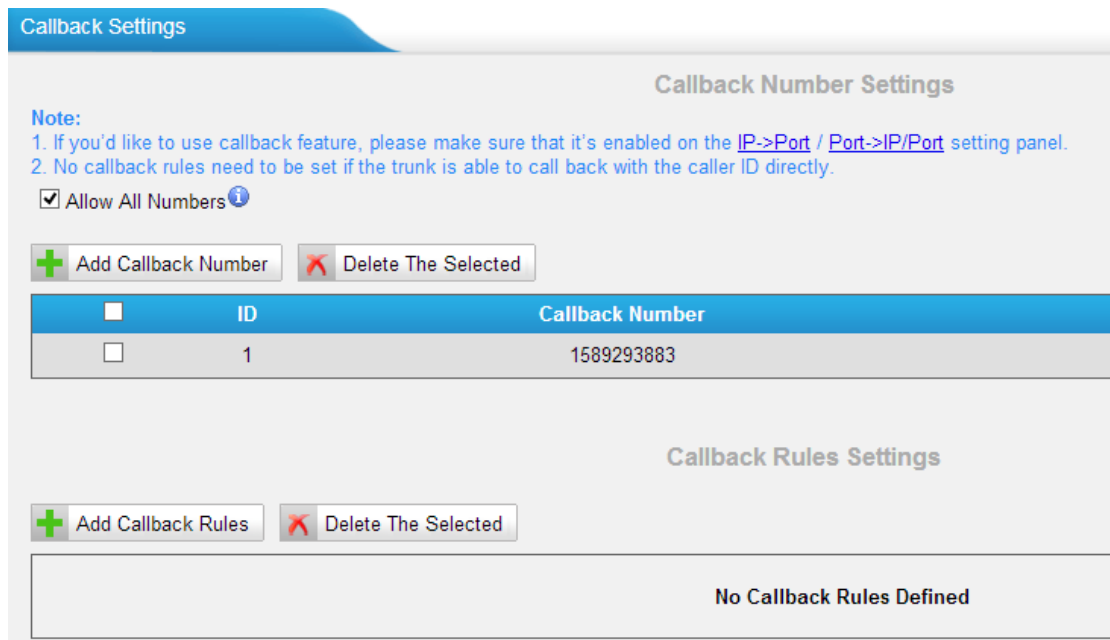


Figure 4-19 Callback Settings

4.4 Gateway Settings

4.4.1 General Preferences

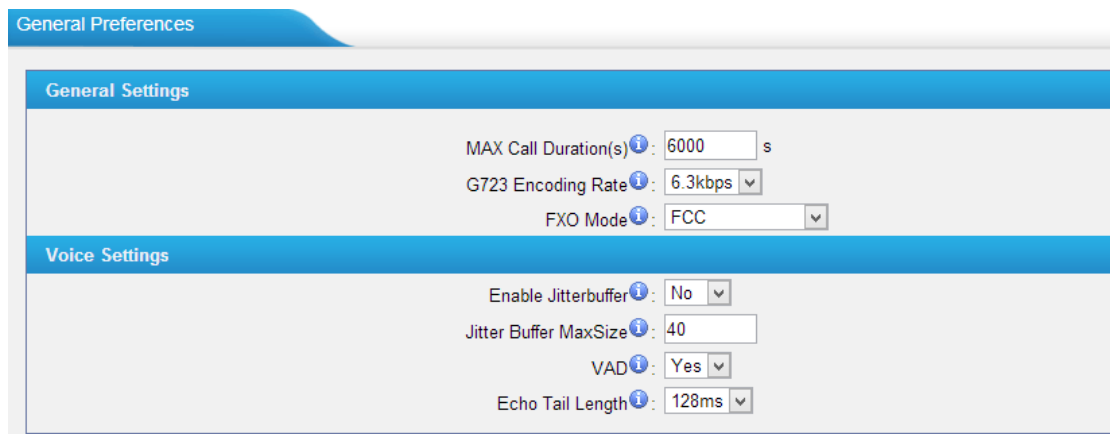


Figure 4-20 General Settings

Table4-16 Description of General Preferences

General Settings	
MAX Call Duration	The absolute maximum amount of time permitted for a call. A setting of 0 disables the timeout.
G723 Encoding Rate	Set the G723 encoding rate.
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".
Voice Settings	
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.
Jitter Buffer MaxSize	Max length of the jitter buffer in milliseconds. Default: 40.
VAD	Voice Activity Detection.
Echo Tail Length	In some cases, the echo canceller doesn't train quickly enough and there is echo at the beginning of the call which then quickly fades out.

4.5 Audio Settings

4.5.1 Custom Prompts

Upload custom prompts on this page. You can also download it and save it as a backup.

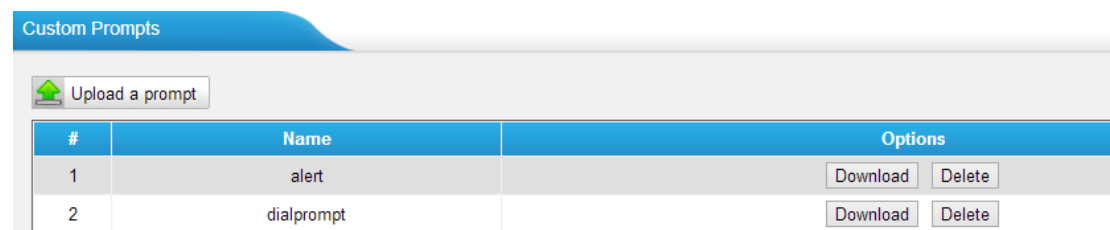


Figure 4-21 Custom Prompts

The administrator can upload prompts following the steps:

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

Note:

The file 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.

4.6 Advanced Settings

4.6.1 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 their country to get tone zone settings for the gateway.

The screenshot shows the 'Tone Zone Settings' interface. At the top, there is a blue header with the text 'Tone Zone Settings'. Below this, a dropdown menu is set to 'United States / North America'. The settings are as follows:

- 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+440

Figure 4-22 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 TA410/810:

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

The screenshot shows the 'Tone Zone Settings' interface with the 'Country' dropdown set to 'Customize Tones'. The settings fields are empty and highlighted with red boxes:

- Country: Customize Tones
- Ring Cadence: [Empty field]
- Dial Tone: [Empty field]
- Ringback Tone: [Empty field]
- Busy Tone: [Empty field]
- Call-Waiting Tone: [Empty field]
- Congestion Tone: [Empty field]
- 2nd Dial Tone: [Empty field]

Figure 4-23 Customize Tones

Table 4-17 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 TA410/810 to the receiver can be set on this page.

Digit Length and Dial Pause Between Digit: 100,100 (ms)

Default Digit Volume: -10,-10 (dB)

DTMF Settings

DTMF Settings

Digit Length And Dial Pause Between Digit: 100,100 ms

Use Default Volume: Yes

Digit Volume: -10,-10 dB

Figure 4-24 Customize Tones

[The End]