



TA3210 User Manual



Sales Tel: +86-592-5503309
E-mail: sales@yeastar.com
Support Tel: +86-592-5503301
E-mail: support@yeastar.com
Web: <http://www.yeastar.com>

Version: 40.19.0.15
Revised: May 11, 2023

Copyright

Copyright 2006-2023 Yeastar Information Technology Co., Ltd. All rights reserved.

No parts of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, photocopying, recording, or otherwise, for any purpose, without the express written permission of Yeastar Information Technology Co., Ltd. Under the law, reproducing includes translating into another language or format.

Declaration of Conformity



Hereby, Yeastar Information Technology Co., Ltd. declares that TA3210 is in conformity with the essential requirements and other relevant provisions of the CE, FCC.

Warranty

The information in this document is subject to change without notice.

Yeastar Information Technology Co., Ltd. makes no warranty of any kind with regard to this guide, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Yeastar Information Technology Co., Ltd. shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance or use of this guide.

WEEE Warning



In accordance with the requirements of council directive 2002/96/EC on Waste of Electrical and Electronic Equipment (WEEE), ensure that at end-of-life you separate this product from other waste and scrap and deliver to the WEEE collection system in your country for recycling.

Contents

| | |
|----------------------------------|-----------|
| About This Guide | 5 |
| Getting Started | 6 |
| Accessing Web GUI | 6 |
| Web Configuration Panel | 7 |
| Application Description | 7 |
| FXO Port Settings | 10 |
| FXO Port Settings | 10 |
| Port Group | 15 |
| VoIP Settings | 16 |
| VoIP Trunk | 16 |
| Trunk Group | 21 |
| SIP Settings | 22 |
| IAX Settings | 27 |
| Routes Settings | 28 |
| IP->Port | 28 |
| Port->IP/Port | 30 |
| Blacklist | 32 |
| Callback Settings | 32 |
| Gateway Settings | 34 |
| General Preferences | 34 |
| Audio Settings | 35 |
| Custom Prompts | 35 |
| Advanced Settings | 36 |
| Tone Zone Settings | 36 |
| DTMF Settings | 37 |
| Network Preferences | 38 |
| LAN Settings | 38 |
| Service | 39 |
| VLAN Settings | 40 |
| VPN Settings | 41 |
| DDNS Settings | 41 |
| Static Route | 42 |
| SNMP Settings | 44 |

| | |
|---------------------------------|-----------|
| Security Center | 45 |
| Security Center | 45 |
| Alert Settings | 46 |
| AMI Settings | 48 |
| Certificates | 49 |
| Firewall Rules | 50 |
| IP Blacklist | 52 |
| System Preferences | 54 |
| Password Settings | 54 |
| Date and Time | 55 |
| Auto Provision Settings | 55 |
| Firmware Update | 58 |
| Upgrade through HTTP | 59 |
| Upgrade through TFTP | 59 |
| Backup and Restore | 61 |
| Reset and Reboot | 61 |
| Status | 62 |
| Port/Trunk Status | 62 |
| Network status | 63 |
| System Info | 64 |
| Reports | 65 |
| Call Logs | 65 |
| System Logs | 65 |
| Packet Tool | 66 |
| Port Monitor Tool | 66 |

About This Guide

Yeastar TA3210 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, TA3210 is ideal for small and medium enterprises that wish to integrate a traditional phone system into IP-based system. TA3210 helps them to preserve previous investment on legacy telephone system and reduce communication costs significantly with the true benefits of VoIP.

Audience

This manual will help you learn how to operate and manage your TA3210 FXO Analog VoIP Gateway. In this guide, we describe every detail on the functionality and configuration of TA3210. We begin by assuming that you are interested in TA3210 and familiar with networking and other IT disciplines.

Safety when working with electricity



- Do not open the device when the device is powered on.
- Do not work on the device, connect or disconnect cables when lightning strikes.
- Switch off the power before plugging or unplugging the cables.
- Disconnect all telecommunication network connectors and cable distribution system connectors before power off the TA3210.

Features Highlights

- 32 FXO ports
- Fully compliant with SIP and IAX2
- Flexible calling rules
- Configurable VoIP Server templates
- Codec: G.711 (a-law/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:

<https://www.yeastar.com/voip-gateways/>

Getting Started

In this chapter, we guide you through the basic steps to start with a new TA3210:

- [Accessing Web GUI](#)
- [Web Configuration Panel](#)
- [Application Description](#)

Accessing Web GUI

The TA3210 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 TA3210 IP address.

How to check TA3210 IP address:

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

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**

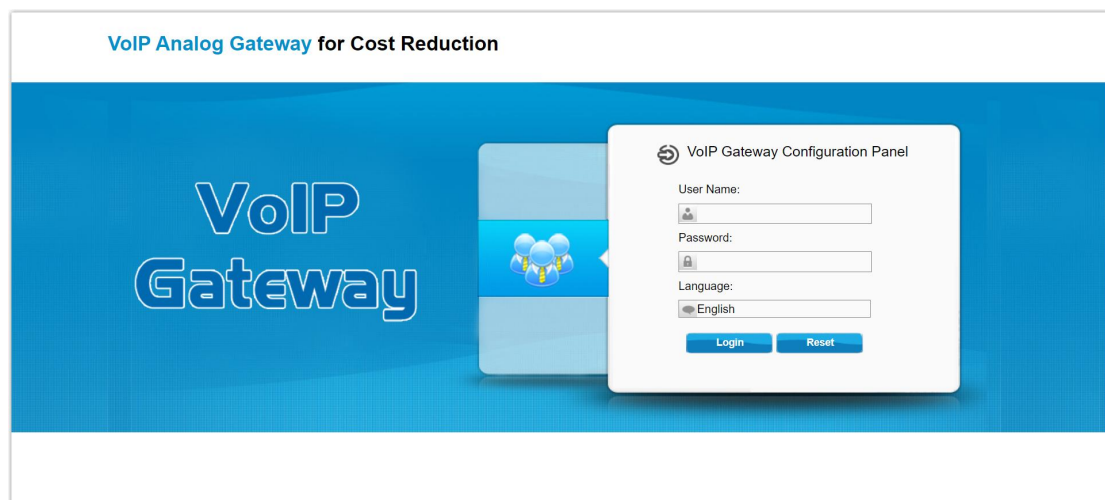


Figure 1-1 TA3210 Login page

Web Configuration Panel

There are 4 main sections on the Web Configuration Panel for users to check the TA3210's status and configure it.

- **Status:** check System Status, Port Status, Trunk Status, Network Status, call logs, and system logs, etc.
- **System:** configure Network Settings, Security related Settings, System Date and Time, Password, Backup and Restore, etc.
- **Gateway:** configure FXO ports, gateway settings and SIP settings, etc.
- **Logout:** log out TA3210.

Note: After saving the changes, remember to click the “Apply changes” button on the upper right corner of the Web GUI to make the changes take effect.

Application Description

Connect IPPBX and TA FXO Gateway

Yeastar TA 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 TA3210 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 TA3210. SPS Mode is recommended.

Account Mode:

Create one SIP account on TA3210, and take the SIP account to register one SIP trunk on your SIP server. Then TA3210 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 TA3210, 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 TA3210, choose a PSTN trunk or PSTN trunk group in the field “Call Source”, and choose the SIP account in the field “Call Destination”.
- 3) When a call comes to PSTN trunk on TA3210, 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 through PSTN trunk on TA3210 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 TA3210 as a VoIP trunk. In this way, TA3210 and your SIP server are connected.

➤ **Calls from SIP to PSTN**

- 1) Configure a IP-> Port route on TA3210; 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 TA3210. 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 TA3210, 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 TA3210, 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 TA3210 to connect to your SIP server. Add another Service Provider SIP trunk on your SIP server, connecting to TA3210.

➤ **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 TA3210, 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 TA3210, 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 TA3210, 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 TA3210 route.

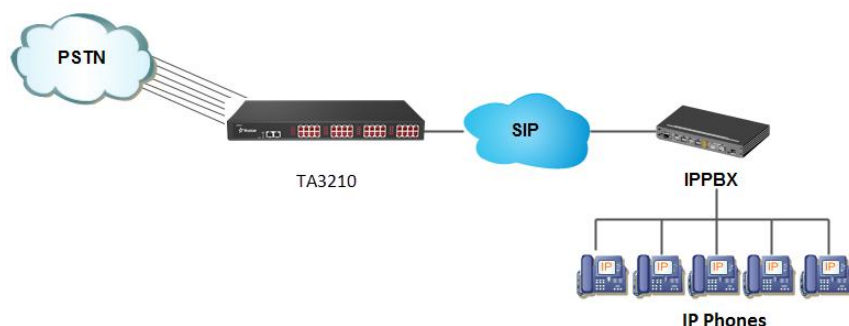


Figure 2-1 Connect IPPBX and TA FXO Gateway

For incoming calls from the PSTN to TA3210, TA3210 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.

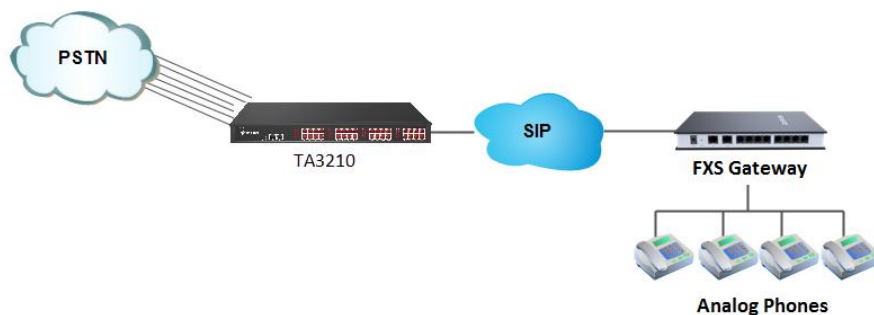


Figure 2-2 Connect TA FXO Gateway and FXS Gateway

FXO Port Settings

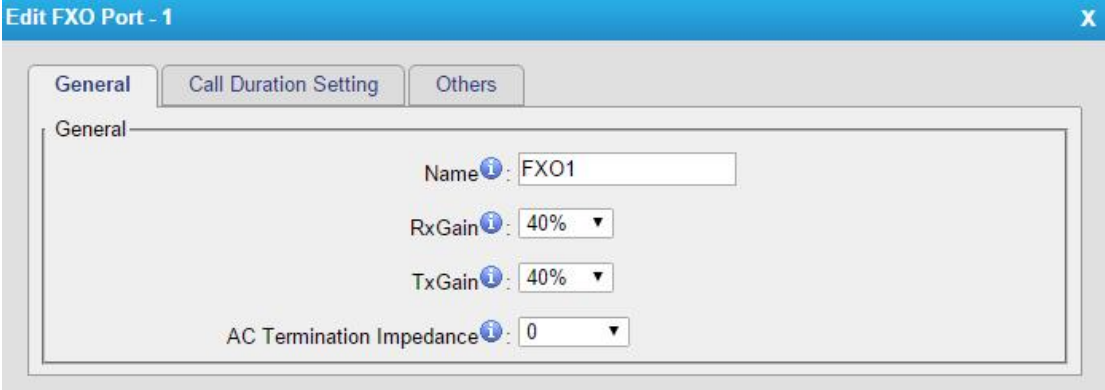
This chapter explains how to configure FXO port on TA3210, go to **Gateway**→ **Port List**→ **FXO Port List** page to configure the FXO ports.

- [FXO Port Settings](#)
- [Port Group](#)

FXO Port Settings

Click "Edit" button  to configure the FXO port.

1) General Settings



The screenshot shows a web-based configuration window titled "Edit FXO Port - 1". It has three tabs: "General", "Call Duration Setting", and "Others". The "General" tab is active. Inside the "General" tab, there are four configuration items, each with an information icon (i) to its left: "Name" is set to "FXO1"; "RxGain" is set to "40%"; "TxGain" is set to "40%"; and "AC Termination Impedance" is set to "0".

Figure 3-1 FXO Port General Settings

Table 3-1 Description of FXO Port General Settings

| Item | 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) |

| Item | Description |
|------|-----------------------------------|
| | 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 |

2) Call Duration Settings

The screenshot shows the 'Edit FXO Port - 1' configuration window with the 'Call Duration Setting' tab selected. The settings are as follows:

- Single Call Max Duration:** 0 min
- Round up duration:** 60 s
- Max. Call Duration:** 0 s
- Enable Clear Stat:** No
- Balance Alarm Settings:**
 - Alarm threshold:** (empty) s
 - Port:** Port1 - FXO1
 - Number:** (empty)
 - Prompt:** alert.wav (with a link to Custom Prompts)
 - E-mail Notification:** No

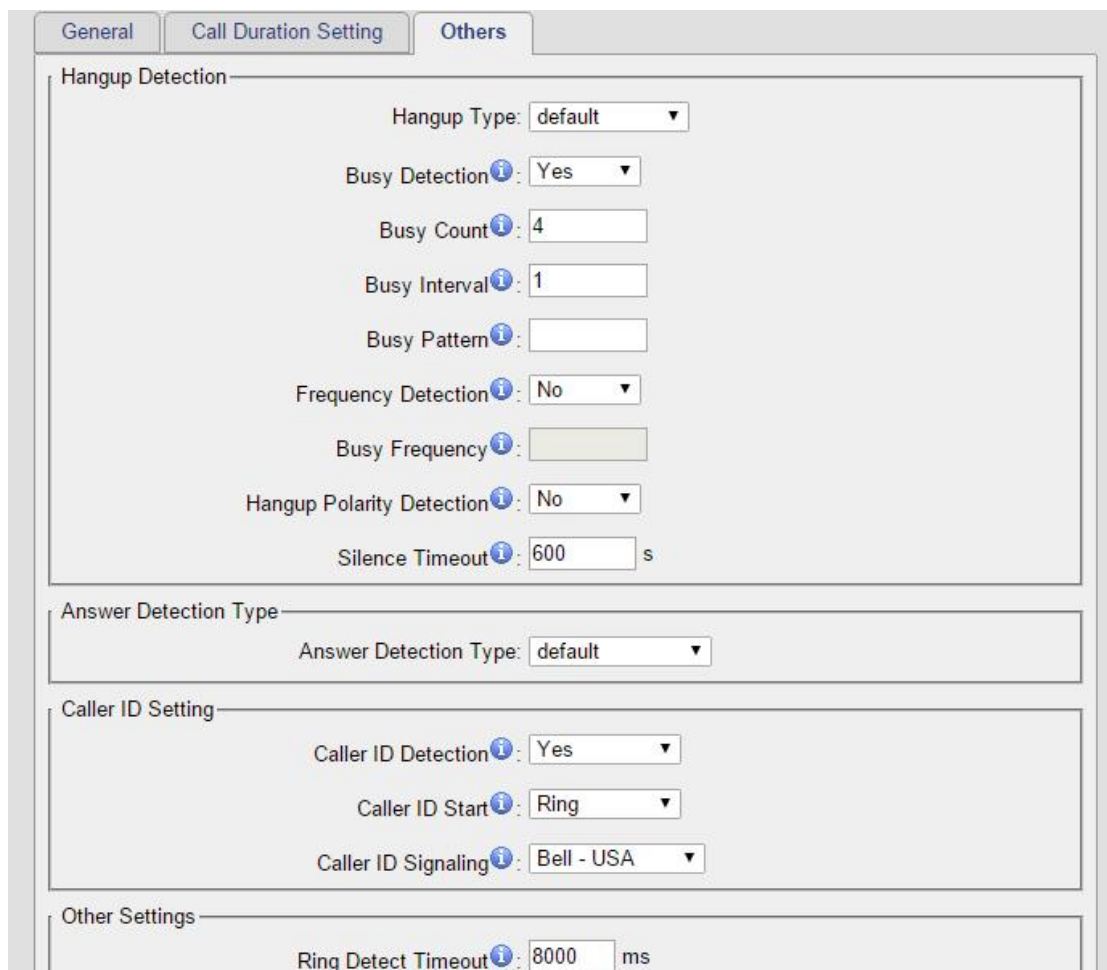
Figure 3-2 FXO Port Call Duration Setting

Table 3-2 Description of FXO Port Call Duration Settings

| Item | 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. | If enabled, you need to set the date and time to |

| Item | Description |
|------------------------|--|
| | clear the call duration status each day/week/month. |
| Balance Alarm Settings | When “Max. Call Duration” is configured as 0 (no limit), this feature is disabled. |
| Alarm threshold(min) | Configure the time duration when TA3210 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 Notification | Specify the email address to receive the alarm email, and define the alert email content. Note: Please make sure SMTP test is successful in “Email settings” page before configuring this. |

3) Other Settings



The screenshot displays the 'Others' configuration tab in the TA3210 interface. It is organized into several sections:

- Hangup Detection:**
 - Hangup Type: default
 - Busy Detection: Yes
 - Busy Count: 4
 - Busy Interval: 1
 - Busy Pattern: (empty field)
 - Frequency Detection: No
 - Busy Frequency: (empty field)
 - Hangup Polarity Detection: No
 - Silence Timeout: 600 s
- Answer Detection Type:**
 - Answer Detection Type: default
- Caller ID Setting:**
 - Caller ID Detection: Yes
 - Caller ID Start: Ring
 - Caller ID Signaling: Bell - USA
- Other Settings:**
 - Ring Detect Timeout: 8000 ms

Figure 3-3 FXO Port Other Settings

Table 3-3 Description of FXO Port Other Settings

| Item | 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. Select which type to detect the call as answered.</p> <ol style="list-style-type: none"> 1) Default: TA3210 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 TA3210 starts to bill. 3) Ringback Tone: If you choose this option, TA3210 will charge the call according to PSTN ringback tone detection. When the "ring duration" or the "ring interval duration" detected on TA3210 is larger than the standard or custom parameters, the call is detected as ANSWERED. <p>*Standard parameters: when you configure the "Tone Zone</p> |

| Item | Description |
|----------------------------|--|
| | 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 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.

Edit Port Group - 1

Group ID: 1

Group Name: g

Strategy: Round-robin

Group Members

| Available FXO Port | | Selected |
|--------------------|----|-------------|
| | »» | FXO1(Port1) |
| | → | FXO2(Port2) |
| | ← | FXO3(Port3) |
| | «« | FXO4(Port4) |
| | | FXO5(Port5) |
| | | FXO6(Port6) |
| | | FXO7(Port7) |
| | | FXO8(Port8) |

Figure 3-4 Port Group

VoIP Settings

To integrate with other IPPBX, we need to configure the VoIP settings in TA FXO Gateway to set up VoIP trunk (SIP and IAX). In this chapter, we introduce the following settings:

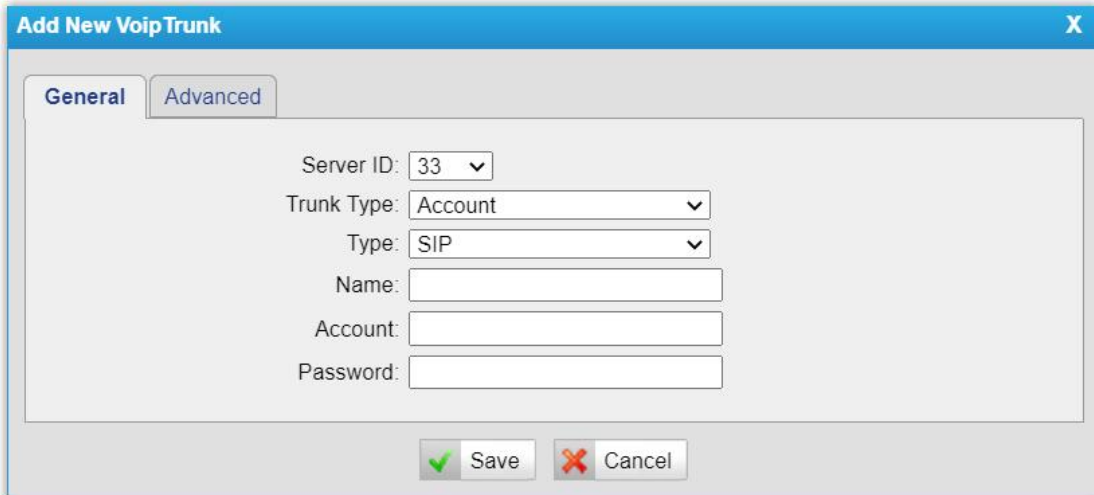
- VoIP Trunk
- Trunk Group
- SIP Settings
- IAX Settings

VoIP Trunk

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

1) Account

It's an SIP account created in TA3210 so that the other devices can register SIP trunk at their side using these information.



The screenshot shows a window titled "Add New Voip Trunk" with a close button (X) in the top right corner. It has two tabs: "General" (selected) and "Advanced". The "General" tab contains the following fields:

- Server ID: 33 (dropdown menu)
- Trunk Type: Account (dropdown menu)
- Type: SIP (dropdown menu)
- Name: (text input field)
- Account: (text input field)
- Password: (text input field)

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

Figure 4-1 Account

Table 4-1 Description of Account Settings

| Item | Description |
|----------------|--------------------------------------|
| General | |
| Server ID | The unique ID for the trunk. |
| Trunk Type | Choose the type of trunk, "Account". |
| Type | Choose the protocol of trunk. |
| Name | Define the name. |
| Account | Define the Account number. |
| Password | Set a password for this account. |

| Item | Description |
|-----------------------|---|
| Advanced | |
| Keep Alive Type | <p>Select the method of heartbeat detection.</p> <ul style="list-style-type: none"> ● Disable: TA gateway do not send packets to the server for heartbeat detection. ● Options: TA gateway sends OPTIONS packets to the VoIP server to check if the server is online. ● Notify: TA gateway sends NOTIFY packets to the VoIP server to check if the server is online. |
| Keep Alive Interval | Define the period of time between consecutive keep-alive packets. |
| NAT | This setting should be used when the system is using a public IP address, communicating with devices hidden behind a NAT device (such as a broadband router). If you have one-way audio problems, you usually have problems with your NAT configuration or your firewall's support of SIP and/or RTP ports. |
| Enable SRTP | Whether to enable SRTP. If enabled, the IPPBX also needs to enable SRTP. |
| Transport | Set the transport protocol. You can set it as UDP, TCP, or TLS. |
| DTMF Mode | Set the default mode for sending DTMF. You can set it as rfc2833, info, inband, or auto. |
| Enable IP Restriction | Once enabled, only the below 'permitted IP address/Subnet mask' will be able to register this account number. In this way, the VoIP security will be enhanced. |

2) VoIP Trunk

It's a SIP trunk configured in TA3210 to register to the SIP provider, please make sure this trunk works properly in advance with provider before configuring TA3210.

Figure 4-2 VoIP Trunk Settings

Table 4-2 Description of VoIP Trunk Settings

| Item | Description |
|--------------------|---|
| General | |
| Server ID | The unique ID for the trunk. |
| Trunk Type | Choose the type of trunk, "Trunk". |
| Type | Choose the protocol of 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. |

| Item | Description |
|------------------------------|--|
| Advanced | |
| From User | This field is generally not required to be configured. However, it can be set if the service provider has special username requirements in the "From" field. |
| Online Number | Define the online number that expected by 'Skype Connect' and some other SIP service providers. Leave this field blank if it is not required. |
| Keep Alive Type | <p>Select the method of heartbeat detection.</p> <ul style="list-style-type: none"> ● Disable: TA gateway do not send packets to the server for heartbeat detection. ● Options: TA gateway sends OPTIONS packets to the VoIP server to check if the server is online. ● Notify: TA gateway sends NOTIFY packets to the VoIP server to check if the server is online. |
| Keep Alive Interval | Define the period of time between consecutive keep-alive packets. |
| Maximum Channels | Define maximum number of concurrent calls supported by the trunk. This settings is only valid to outbound calls. Leave it blank for no limit. |
| Realm | <p>A realm defines the protection space. It must be globally unique; usually it is the same with domain name.</p> <p>For example, when registering to China Mobile, the realm value should be 'ims.fj.chinamobile.com'. Fill in a realm, so that the password will be encrypted in the configuration file.</p> |
| Caller ID | Display this number when making calls. This feature needs the service provider to support. |
| Authenticating Incoming Call | Decide whether to authenticate the incoming calls. |
| Enable SRTP | Whether to enable SRTP. If enabled, the IPPBX also needs to enable SRTP. |
| Enable Outbound Proxy Server | Whether to use an outbound proxy server. Contact your service providers to check if they support outbound proxy, then configure outbound proxy settings under their |

| Item | Description |
|-------------------------|--|
| | guidance. |
| FirstCodec ~ FifthCodec | Set the codec priority of the line, please confirm with your service provider before modifying this item, so as to match the settings that they support. |
| Transport | Set the transport protocol. You can set it as UDP, TCP, or TLS. |
| DTMF Mode | Set the default mode for sending DTMF. You can set it as rfc2833, info, inband, or auto. |
| DOD Settings | Set the outbound caller ID that will be displayed on the called party's phone. |

3) Service Provider

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

The screenshot shows a window titled "Add New Voip Trunk" with a close button (X) in the top right corner. It has two tabs: "General" (selected) and "Advanced". The "General" tab contains the following fields:

- Server ID: 33 (dropdown menu)
- Trunk Type: Service Provider (dropdown menu)
- Type: SIP (dropdown menu)
- Provider Name: (empty text field)
- Hostname/IP: (empty text field) : 5060 (text field)

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

Figure 4-3 Service Provider Trunk Settings

Table 4-3 Description of Service Provider Trunk Settings

| Item | Description |
|----------------|---|
| General | |
| Server ID | The unique ID for the trunk. |
| Trunk Type | Choose the type of trunk, "Service Provider". |
| Type | Choose the protocol of 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. |

| Item | Description |
|-------------------------|--|
| Advanced | |
| Keep Alive Type | Select the method of heartbeat detection. <ul style="list-style-type: none"> ● Disable: TA gateway do not send packets to the server for heartbeat detection. ● Options: TA gateway sends OPTIONS packets to the VoIP server to check if the server is online. ● Notify: TA gateway sends NOTIFY packets to the VoIP server to check if the server is online |
| Keep Alive Interval | Define the period of time between consecutive keep-alive packets. |
| Maximum Channels | Define maximum number of concurrent calls supported by the trunk. This settings is only valid to outbound calls. Leave it blank for no limit. |
| FirstCodec ~ FifthCodec | Set the codec priority of the line, please confirm with your service provider before modifying this item, so as to match the settings that they support. |
| Transport | Set the transport protocol. You can set it as UDP, TCP, or TLS. |
| DTMF Mode | Set the default mode for sending DTMF. You can set it as rfc2833, info, inband, or auto. |
| DOD Settings | Set the outbound caller ID that will be displayed on the called party's phone. |

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.

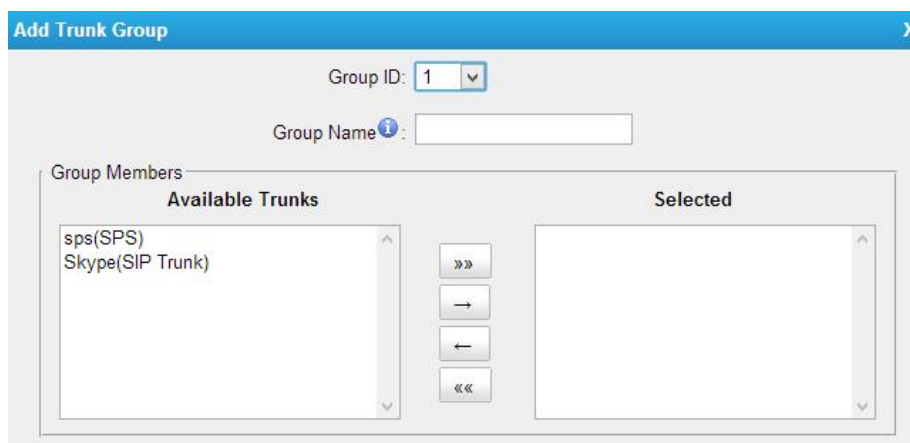


Figure 4-4 Trunk Group

SIP Settings

It is wise to leave the default setting as provided on this page. However, for a few fields, you need to change them to suit your situation.

1) General

The screenshot shows the 'SIP Settings' window with the 'General' tab selected. The settings are as follows:

- UDP Port: 5060
- Enable Random Port: Yes
- Random Port Update Interval: 24 Hour
- Enable TCP Port: 5060
- Enable TLS Port: 5061
- TLS Verify Server: No
- TLS Ignore Common Name: Yes
- TLS Client Method: sslv2
- RTP Port Start: 10000
- RTP Port End: 12000
- DTMF Mode: rfc2833
- Max Registration/Subscription Time: 3600
- Min Registration/Subscription Time: 60
- Default Incoming/Outgoing Registration Time: 120
- Register Attempts: 0
- Register Timeout: 20
- Calling Channel Codec Priority: Yes
- DNS SRV Look Up: No
- User Agent:

Figure 4-5 SIP General Settings

Table 4-4 Description of SIP General Settings

| Item | 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 TA FXO Gateway as a TLS client, whether or not to verify server'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 TA FXO Gateway 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 | Maximum duration (in seconds) of a SIP registration. |

| Item | Description |
|---|--|
| Registration/Subscription Time | 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. |
| MWI Subscription Expiry Time | Expiry time for outgoing MWI subscriptions. |
| 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, TA FXO Gateway will follow the priority order in your SIP/SPS trunks. |
| 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 "TA FXO Gateway"; you can change it if needed. |

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 4-6 NAT Settings

Table 4-5 Description of SIP NAT Settings

| Item | 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. |
| STUN Port | The STUN port. |
| 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 | If an external host has been supplied, you may specify how often the system will perform a DNS query on this host. This value is specified in seconds. |
| Local Network Identification | Used to identify the local network using a network number/subnet mask pair when the system is behind a NAT or firewall. Some examples of this are as follows: "192.168.0.0/255.255.0.0": All RFC 1918 addresses are local networks; "10.0.0.0/255.0.0.0": Also RFC1918; "172.16.0.0/12": Another RFC1918 with CIDR notation; "169.254.0.0/255.255.0.0": Zero conf local network. Please refer to RFC1918 for more information. |
| NAT Mode | Global NAT configuration for the system; the options for this setting are as follows: Yes = Use NAT. Ignore address information in the SIP/SDP headers and reply to the sender's IP address/port. No = Use NAT mode only according to RFC3581. Never = Never attempt NAT mode or RFC3581 support. Route = Use NAT but do not include rport in headers. |
| Allow RTP Re-invite | By default, the system will route media streams from SIP endpoints through itself. Enabling this option causes the system to attempt to negotiate the endpoints to route packets to each other directly, bypassing the system. It is not always possible for the system to negotiate endpoint-to-endpoint media routing. |

3) Codecs

You can choose the allowed codec in TA3210, 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

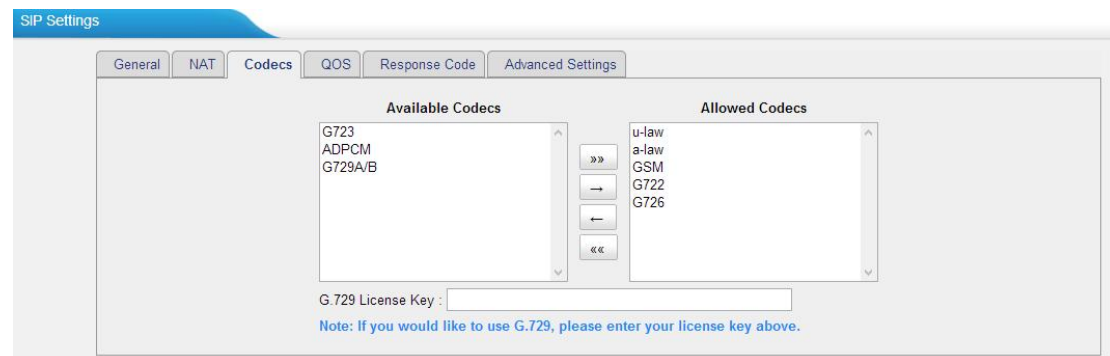


Figure 4-7 Codecs

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.

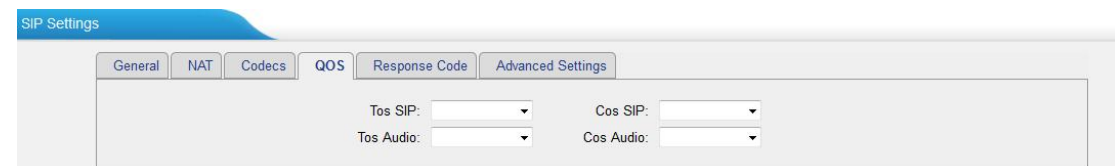


Figure 4-8 Qos

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

5) Response Code

You can change the response code on TA FXO Gateway 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.

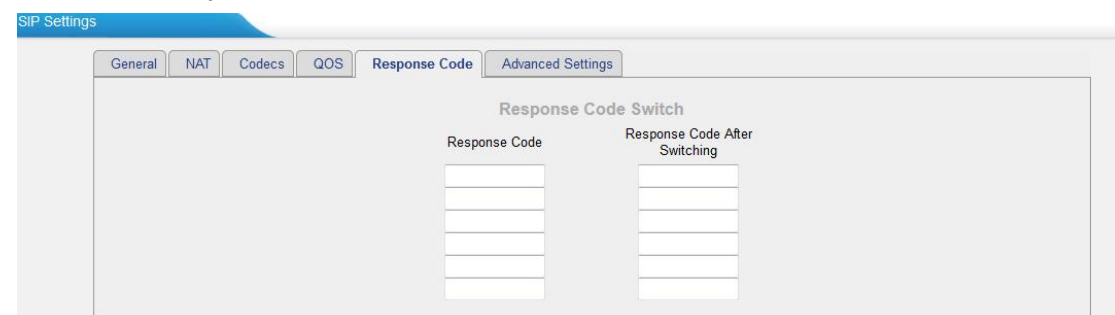


Figure 4-9 Response Code

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

SIP Settings

General NAT Codecs QOS Response Code **Advanced Settings**

From Field: From

To Field: To

180 Ringing: ☐

Remote Party ID: ☐ send ☐ trust

Allow Guest: No

Pedantic: No

Alwaysauthreject: Yes

OPTIONS Response 200: Yes

Session-timers: Accept

Session-expires: 1800 s

Session-minse: 90 s

Session-refresher: Uas

Figure 4-10 SIP Advanced Settings

Table 4-6 Description of SIP Advanced Settings

| Item | Description |
|----------------------|--|
| From Field | Decide from which header field will the gateway retrieve Caller ID. |
| To Field | Decide from which header field will the gateway get to match the DID (Inbound Direct Number). |
| 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 TA FXO Gateway rejects "Register" or "Invite" packets, TA FXO Gateway always respond the packets using "SIP404 NOT FOUND". It's recommended that it is enabled for security reason. |
| OPTIONS Response 200 | If set to yes, the response to an OPTIONS is always 200OK. |
| Session-timers | Enable session-timer mode, default: yes. If you find the call is cut off every 15 minutes every time, please disable this. |
| Session-expires | The max refresh interval |
| Session-minse | The min refresh interval, which mustn't be shorter than 90s. |
| Session-refresher | Choose the session-refresher, the default is Uas. |

IAX Settings

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

The screenshot shows the 'IAX Settings' window with two tabs: 'General' and 'Codecs'. The 'General' tab contains the following settings:

- UDP Port: 4569
- Bandwidth: Low (dropdown menu)
- Minimum Registration/Subscription Time: 60
- Maximum Registration/Subscription Time: 1200

The 'Codecs' tab is currently inactive. At the bottom of the window, the 'Allowed Codecs' section shows the following options:

- ☒ u-law
- ☒ a-law
- ☒ GSM
- ☐ G726
- ☐ ADPCM
- ☐ G729A/B
- ☐ G723

Figure 4-11 IAX Settings

Table 4-7 Description of IAX Settings

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

Routes Settings

After connecting Yeastar TA3210 gateway with the VoIP server, you need to configure the routes settings on TA3210 to route the calls through the gateway. In this chapter, we introduce the following sections:

- [IP->Port](#)
- [Port->IP/Port](#)
- [Blacklist](#)
- [Callback Settings](#)

IP->Port

Configure IP->Port routes to control calls from your SIP server to TA3210 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.

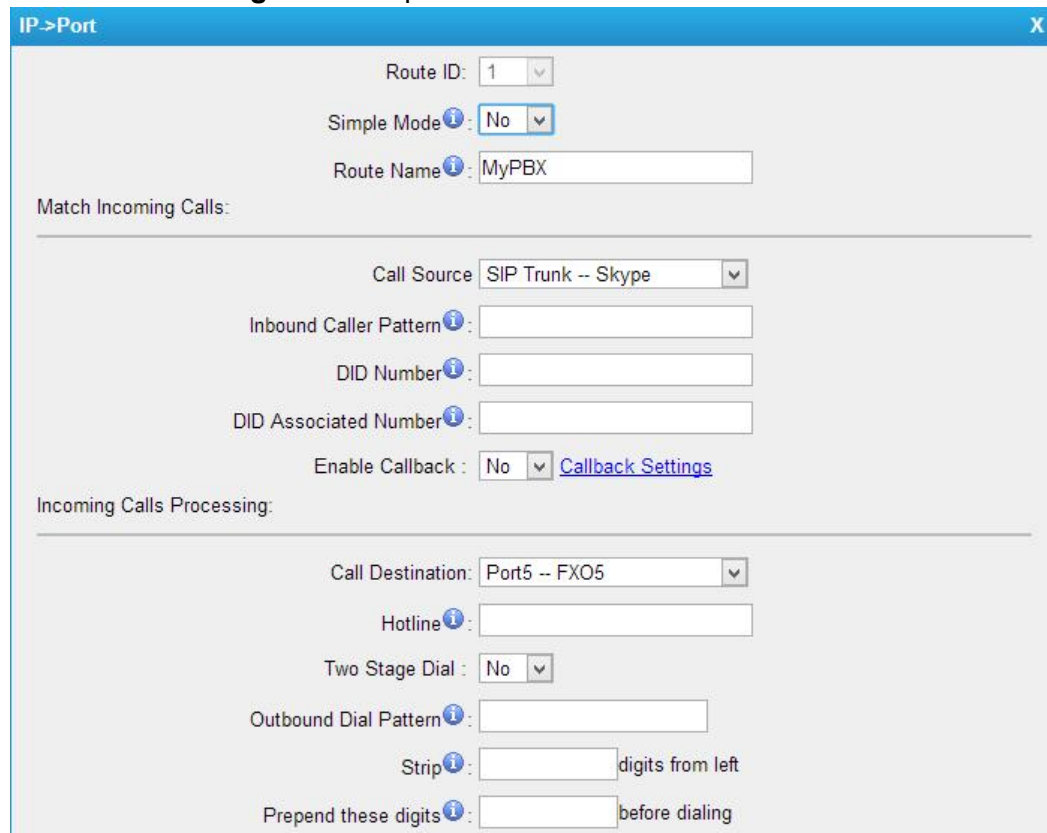
Figure 5-1 Simple Mode Route

Table 5-1 Description of Simple Mode Route

| Item | Description |
|------------------|---|
| Route Name | Define the route name. |
| Call Source | Choose the trunk or trunk group for the incoming calls. |
| Call Destination | Choose the FXO port or port 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.



IP->Port

Route ID: 1

Simple Mode: No

Route Name: MyPBX

Match Incoming Calls:

Call Source: SIP Trunk -- Skype

Inbound Caller Pattern:

DID Number:

DID Associated Number:

Enable Callback: No [Callback Settings](#)

Incoming Calls Processing:

Call Destination: Port5 -- FXO5

Hotline:

Two Stage Dial: No

Outbound Dial Pattern:

Strip: digits from left

Prepend these digits: before dialing

Figure 5-2 Detailed Mode Route

Table 5-2 Description of Match Incoming Calls Settings

| Item | 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. |
| Enable Callback | If the caller hangs up after calling in when Callback is enabled, the TA FXO gateway will call back from that line and then send the call to the outgoing trunk. For more information, please configure the " Callback Settings ". |

Table 5-3 Description of Handle Matched Incoming Calls Settings

| Item | Description |
|-----------------------|---|
| Call Destination | Choose the FXO port or port 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 Dial | 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. |

Port->IP/Port

Port->IP/Port routes are used to control incoming calls to PSTN trunks on TA3210 and route the calls to your SIP server or another PSTN trunk on TA3210.

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.

The screenshot shows the 'Add Port->IP/Port Route' configuration window. The fields are as follows:

- Route ID: 2
- Simple Mode: Yes
- Route Name: Elastix
- Match Incoming Calls:
 - Call Source: Port1 -- FXO1
- Incoming Calls Processing:
 - Call Destination: SPS -- sps
 - Hotline: (empty)
- Buttons: Save, Cancel

Figure 5-3 Simple Mode Route

Table 5-4 Description of Simple Mode Route

| Item | Description |
|------------------|---|
| Route Name | Define the route name. |
| Call Source | Choose the FXO port or port 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 5-4 Detailed Mode Route

Table 5-4 Description of Match Incoming Calls Settings

| Item | 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 | If the caller hangs up after calling in when Callback is enabled, the TA FXO gateway will call back from that line and then send the call to the outgoing trunk. For more information, please configure the " Callback Settings ". |

Table 5-5 Description of Handle Matched Incoming Calls Settings

| Item | 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. |

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.

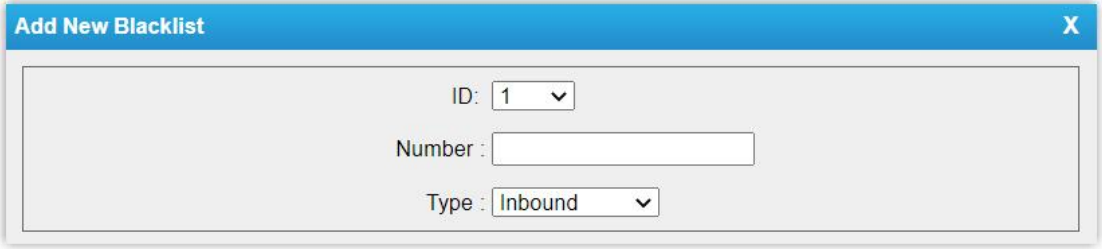


Figure 5-5 Blacklist

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.

Callback Settings

Callback Number Settings

Note:
1. If you'd like to use callback feature, please make sure that it's enabled on the [IP->Port](#) / [Port->IP/Port](#) setting panel.
2. No callback rules need to be set if the trunk is able to call back with the caller ID directly.

☒ Allow All Numbers ⓘ

+ Add Callback Number

✖ Delete The Selected

| <input type="checkbox"/> | ID | Callback Number |
|--------------------------|----|-----------------|
| <input type="checkbox"/> | 1 | 1589293883 |

Callback Rules Settings

+ Add Callback Rules

✖ Delete The Selected

No Callback Rules Defined

Figure 5-6 Callback Settings

Gateway Settings

This chapter explains Gateway settings, which can be applied globally to TA3210. The gateway settings can be configured under **Gateway**→ **Gateway Settings**.

- **General Preferences**

General Preferences

Figure 6-1 General Preferences

Table 6-1 General Preferences

| Item | Description |
|-------------------------|--|
| 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. |

Audio Settings

This chapter explains prompt settings on TA3210.

- Custom Prompts

Custom Prompts

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

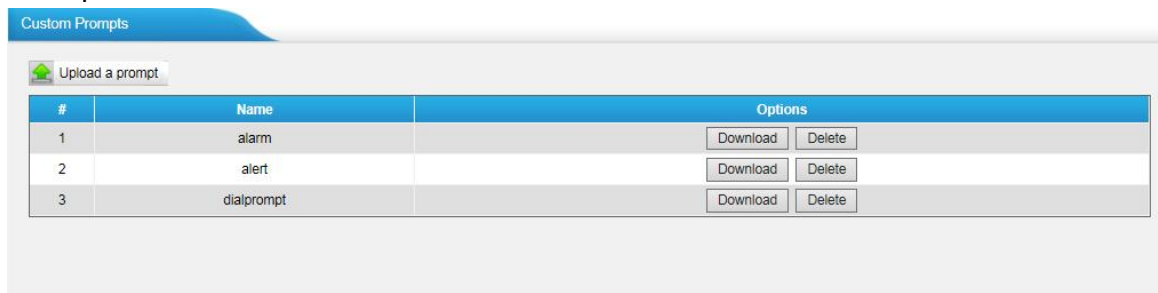


Figure 7-1 Custom Prompts

The administrator can upload prompts by doing the following:

- 1) Click “Upload Prompt”.
- 2) Click “Choose File” to choose the desired prompt.
- 3) Click “Upload” to upload the selected prompt.

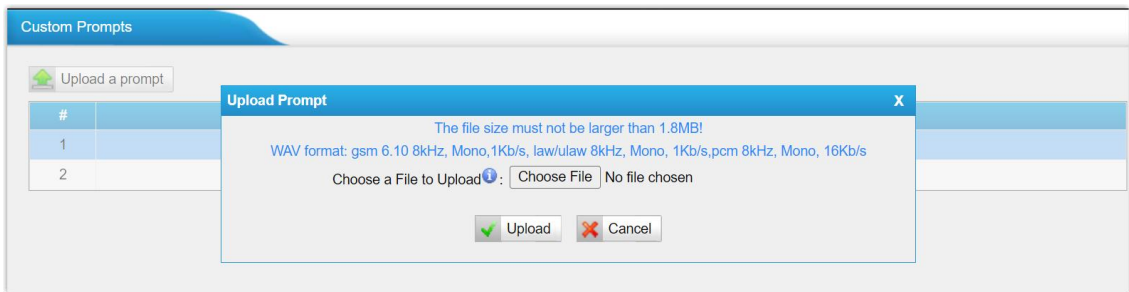


Figure 7-2 Upload A Prompt

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

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

Advanced Settings

This chapter explains SIP settings and Distinctive Ringtones.

- [Tone Zone Settings](#)
- [DTMF Settings](#)

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' page with the 'Country/Region' dropdown set to 'United States / North America'. The settings are as follows:

| Setting | Value |
|-------------------|---|
| Country/Region | 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 8-1 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 TA FXO Gateway:

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

The screenshot shows the 'Tone Zone Settings' page with the 'Country/Region' dropdown set to 'Customize Tones'. The settings are as follows:

| Setting | Value |
|-------------------|-----------------|
| Country/Region | Customize Tones |
| Ring Cadence | |
| Dial Tone | |
| Ringback Tone | |
| Busy Tone | |
| Call-Waiting Tone | |
| Congestion Tone | |
| 2nd Dial Tone | |

Figure 8-2 Customize Tones

Table 8-1 Description of Tone Zone Settings

| Item | Description |
|----------------|---|
| Country/Region | 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 |

| Item | Description |
|-------------------|--|
| | 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. |

DTMF Settings

DTMF signal sent from TA3210 to the receiver can be set on this page.

DTMF Settings

DTMF Settings

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

Use Default Volume: Yes

Digit Volume: -10,-10 dB

Figure 8-3 DTMF Settings

- Digit Length and Dial Pause Between Digit: 100.100 (ms)
- Use Default Volume: Whether to use the default volume. The default volume is -10,-10 (dB).
- Digit Volume: Customize digit volume if the Use Default Volume is set to No.

Network Preferences



This chapter explains network settings on TA3210. Click the main menu **System** on the top of the Web GUI to check the network settings.

- [LAN Settings](#)
- [Service](#)
- [VLAN Settings](#)
- [VPN Settings](#)
- [DDNS Settings](#)
- [Static Route](#)
- [SNMP Settings](#)

LAN Settings

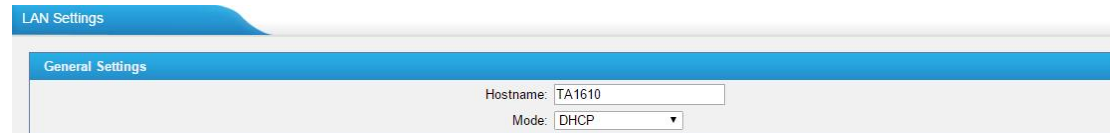
After successfully logging in the TA3210 Web GUI for the first time, you can go to **System**→**Network Preferences**→**LAN Settings** to configure the network for TA3210.

Figure 9-1 LAN Settings -- Static IP Address Mode

Table 9-1 LAN Settings -- Description of Static IP Address Mode Parameters

| Item | Description |
|-------------|---|
| Hostname | Set the host name for TA3210. |
| Mode | Choose the network mode: <ul style="list-style-type: none"> • Static IP Address • DHCP • PPPoE |
| IP Address | Set the IP Address for TA3210. |
| Subnet Mask | Set the subnet mask for TA3210. |
| Gateway | Set the gateway for TA3210. |
| Primary DNS | Set the primary DNS for TA3210. |


| | |
|---------------|--|
| Secondary DNS | Set the secondary DNS for TA3210. |
| IP Address2 | Set the second IP Address for TA3210. |
| Subnet Mask2 | Set the second subnet mask for TA3210. |



The screenshot shows the 'LAN Settings' window with the 'General Settings' tab selected. The 'Hostname' field is set to 'TA1610' and the 'Mode' dropdown is set to 'DHCP'.

Figure 9-2 LAN Settings -- DHCP Mode

Select DHCP mode to get an IP address and related network configuration automatically from the local network.



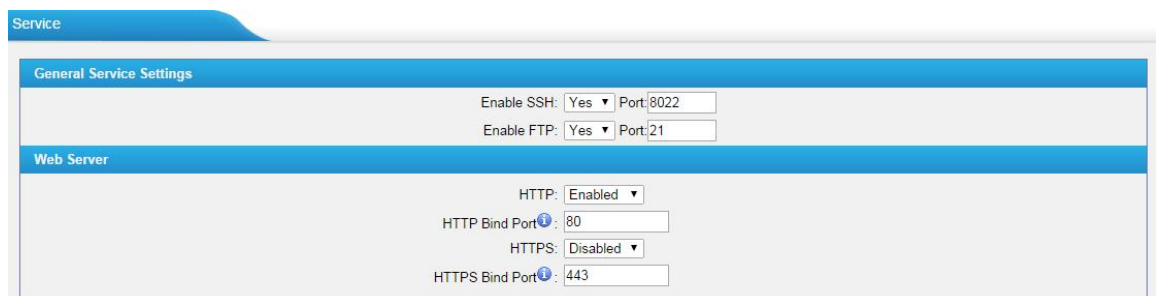
The screenshot shows the 'LAN Settings' window with the 'General Settings' tab selected. The 'Hostname' field is set to 'TA1610' and the 'Mode' dropdown is set to 'PPPoE'. The 'User Name' and 'Password' fields are empty.

Figure 9-3 LAN Settings -- PPPoE Mode

Fill in User Name and Password to access the Internet via PPPoE.

Service

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



The screenshot shows the 'Service' window with the 'General Service Settings' tab selected. The 'Enable SSH' dropdown is set to 'Yes' and the 'Port' is 8022. The 'Enable FTP' dropdown is set to 'Yes' and the 'Port' is 21. The 'Web Server' tab is also visible, showing 'HTTP' set to 'Enabled' and 'HTTP Bind Port' as 80. 'HTTPS' is set to 'Disabled' and 'HTTPS Bind Port' as 443.

Figure 9-4 Service Settings

Table 9-2 Description of Service Settings

| Item | Description |
|------|---|
| SSH | By using SSH, you can log in to TA3210 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. |

| Item | Description |
|-------|---|
| 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. |

VLAN Settings

VLAN (Virtual Local Area Network) is a group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location.

A VLAN is a broadcast domain created by switches. This means the VLAN is configured on switches, layer 3 switches. Note that some of the switches don't support VLAN.

Note: TA3210 acts as a VLAN client, a 3-layer switch is needed.

Figure 9-5 VLAN Settings

Please follow the steps below to set up VLAN on TA3210.

Step1. Create VLANs on your switch.

Step2. Allocate a VLAN ID and IP address for TA3210.

Step3. Configure VLAN settings page on TA3210.

Table 9-3 Description of VLAN Settings

| Item | Description |
|------------------|--|
| NO.1 | Select the checkbox to edit the first VLAN. |
| VLAN Number | Enter the VLAN ID. |
| VLAN IP Address | Enter the VLAN IP address. |
| VLAN Subnet Mask | Enter the subnet mask. |
| Default Gateway | Enter the gateway address. |
| NO.2 | Select the checkbox to edit the second VLAN. |
| VLAN Number | Enter the VLAN ID. |
| VLAN IP Address | Enter the VLAN IP address. |

| Item | Description |
|------------------|----------------------------|
| VLAN Subnet Mask | Enter the subnet mask. |
| Default Gateway | Enter the gateway address. |

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. TA3210 supports OpenVPN.

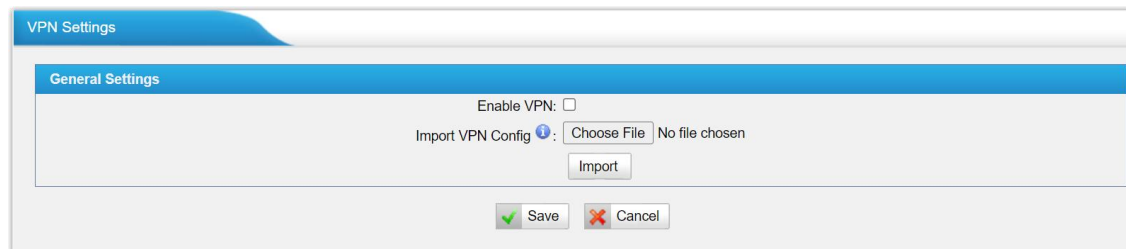


Figure 9-6 VPN Settings

- **Enable VPN**
Enable VPN feature.
- **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. TA3210 works as VPN client mode only.

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 9-7 DDNS Settings

Table 9-4 Description of DDNS Settings

| Item | Description |
|-------------|--|
| Enable DDNS | Select the checkbox to enable DDNS. |
| 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.

Static Route

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

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

Static Route Settings

Routing Table

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

Static Route Rules

ID: 1 ▼

Destination ⓘ:

Subnet Mask:

Gateway:

Metric ⓘ:

✓

Modify

| ID | Destination | Subnet Mask | Gateway | Metric | |
|----|-------------|-------------|---------|--------|--------------|
| 1 | -- | -- | -- | -- | <div>✕</div> |
| 2 | -- | -- | -- | -- | <div>✕</div> |
| 3 | -- | -- | -- | -- | <div>✕</div> |
| 4 | -- | -- | -- | -- | <div>✕</div> |
| 5 | -- | -- | -- | -- | <div>✕</div> |
| 6 | -- | -- | -- | -- | <div>✕</div> |
| 7 | -- | -- | -- | -- | <div>✕</div> |
| 8 | -- | -- | -- | -- | <div>✕</div> |

Figure 9-8 Static Route

1) Route Table

The current route rules of TA FXO Gateway.

2) Static Route Rules

You can add new static route rules here.

Table 9-4 Description of Static Route Settings

| Items | Description |
|-------------|---|
| Destination | The destination network to be accessed to by TA FXO Gateway. |
| Subnet Mask | Specify the destination network portion. |
| Gateway | Define which gateway TA FXO Gateway 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. |

SNMP Settings

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. Yeastar TA3210 gateway supports three versions: V1, V2C and V3.

SNMP Settings

Note 1: If the managers want to access the device by SNMP v3 mode, 'SNMPv3 user' information must be configured.
Note 2: If the managers want to access the device by SNMP v1/v2c mode, 'SNMP Community' information must be configured.

SNMP Settings

SNMP is not running

Enable:

Local Port:

SNMPv3 User

SNMPv3 User:

Access Limit:

SNMP Community

SNMP Mode:

Access: ☒Read ☐Write

Community:

IP/SubnetMask:


Trap Setting

Trap Mode:

Trap Community:

Trap IP:

Figure 9-9 SNMP Settings



44/66

Security Center

This chapter describes how to secure your TA3210. It is strongly recommended that users configure firewall and other security options on TA3210 to prevent the attack fraud and the system failure or calls loss.

- [Security Center](#)
- [Alert Settings](#)
- [AMI Settings](#)
- [Certificates](#)
- [Firewall Rules](#)
- [IP Blacklist](#)

Security Center

All the security settings including Firewall, Service, Port Settings in TA3210 are displayed in Security Center. Users could rapidly check and configure the relevant security settings here.

1) Firewall

In the “Firewall” tab, users could check firewall configuration and alert settings, you can enter the corresponding setting page directly by clicking the button in “Setting” column.

| Function | Status | Note | Setting |
|-----------------|----------------|---|--------------------------------|
| Firewall Switch | Disabled | Dangerous. To protect your equipment from malicious attack, please enable Firewall. | 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 10-1 Security Center -- Firewall

2) Service

In “Service” tab, you can check AMI/SSH status. For AMI/SSH, you can enter the corresponding setting page directly by clicking the button in “Setting” column.

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

Figure 10-2 Security Center -- Service

3) Port

In “Port” tab, you can check SIP port and HTTP port. you can enter the corresponding setting page directly by clicking the button in “Setting” column.

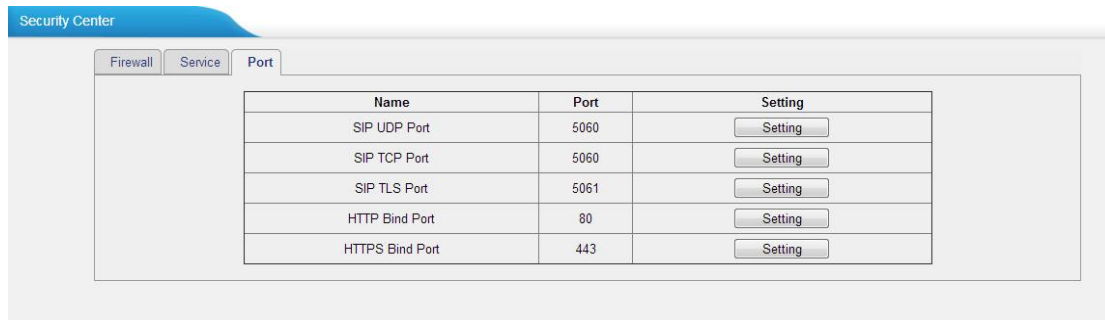


Figure 10-3 Security Center -- Port

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.

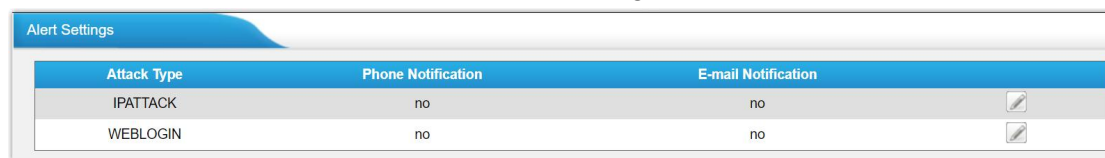


Figure 10-4 Attack Type

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

IPATTACK

Phone Notification Settings

Phone Notification: Yes ▾

Port: Port1 -- FXO1 ▾

Number ⓘ: 915812345678

Attempts ⓘ: 1 ▾

Interval ⓘ: 60 s

Prompt: alert.wav ▾ [Custom Prompts](#)

E-mail Notification Settings

E-mail Notification: Yes ▾

To ⓘ: jerry@yeastar.com

Subject: IP Attack

gateway hostname:\$(HOSTNAME)
 attack source ip address:\$(SOURCEIP)
 attack dest mac:\$(DESTMIC)
 attack source port:\$(DESTPORT)
 attack source protocol:\$(PROTOCOL)
 attack occurred:\$(DATETIME)

Figure 10-5 Alert Settings

Table 10-1 Description of Alert Settings

| Item | Description |
|------------------------------------|---|
| Phone Notification Settings | |
| Phone Notification | Whether to enable phone notification or not. |
| Port | The port that was attacked. |
| Number | The numbers could be set for alert notification; users can set up 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. |

| Item | Description |
|------------------------------------|---|
| Email Notification Settings | |
| E-mail Notification | Whether to enable E-mail Notification or not. |
| To | The recipients for the alert notification. 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:\$(DESTMACH) attack source port:\$(DESTPORT) attack source protocol:\$(PROTOCOL) attack occurred:\$(DATETIME) |

AMI Settings

The Asterisk Manager Interface (AMI) is a system monitoring and management interface provided by Asterisk. It allows live monitoring of events that occur in the system, as well enabling you to request that Asterisk perform some action. The actions that are available are wide-ranging and include things such as returning status information and originating new calls. Many interesting applications have been developed on top of Asterisk that take advantage of the AMI as their primary interface to Asterisk.

There are two main types of messages on the Asterisk Manager Interface: manager events and manager actions.

The 3rd party software can work with TA3210 using AMI interface. It is disabled by default. If necessary, you can enable it.

Figure 10-5 AMI Settings

- **User Name, Password & Port**
After enabling AMI, you can use this username and password to log in TA3210. The default port is 5038.
- **Permitted "IP address/Subnet mask"**
You can set which IP is allowed to log in TA3210 AMI interface.

Certificates

TA3210 supports TLS transport, you can configure FXO port with TLS transport. To use TLS, you should upload certificates first.

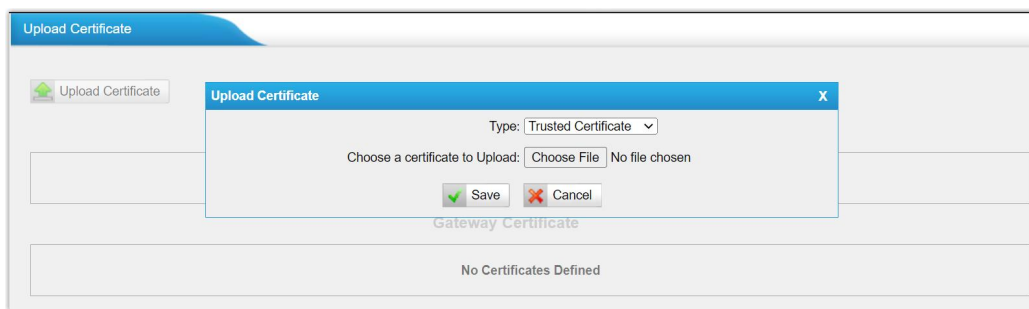


Figure 10-6 Upload Certificate

- **Trusted Certificate**
This certificate is a CA certificate. When selecting "TLS Verify Client" as "Yes", you should upload a CA. The relevant VoIP provider 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 TA3210. If the VoIP provider enables "TLS Verify server", you should also upload the relevant CA certificate on the VoIP provider.

Firewall Rules

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



Figure 10-7 Firewall Settings

1) General Settings

Table 10-2 Description of Firewall General Settings

| Item | Description |
|-----------------|--|
| Enable Firewall | Enable the firewall to protect the device. |
| 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. Note: 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.

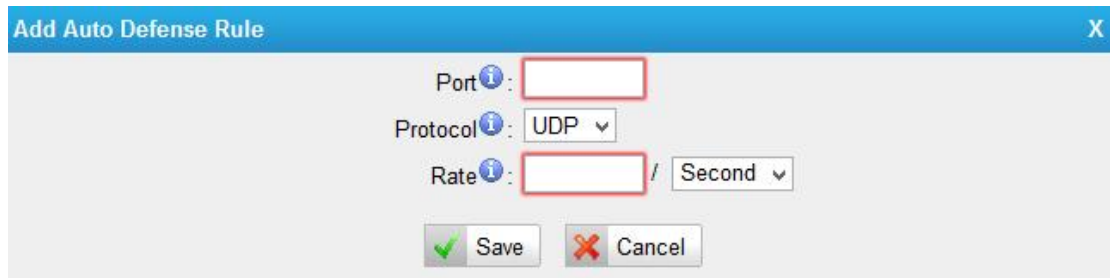
Figure 10-8 Common Rules

Table 10-3 Description of Common Rules

| Item | 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) Auto Defense



The dialog box titled "Add Auto Defense Rule" contains the following fields and controls:

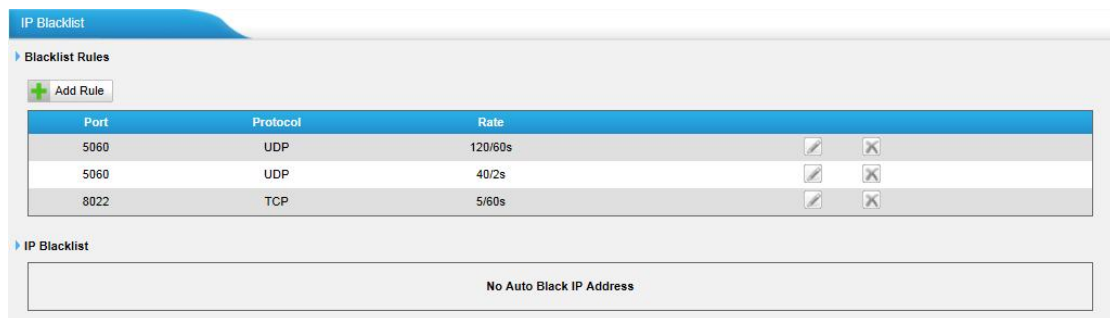
- Port:** A text input field with a red border.
- Protocol:** A dropdown menu currently set to "UDP".
- Rate:** A text input field with a red border, followed by a unit dropdown menu currently set to "Second".
- Buttons:** "Save" (with a green checkmark icon) and "Cancel" (with a red X icon).

Figure 10-9 Auto Defense
Table 10-4 Description of Auto Defense

| Items | Description |
|----------|--|
| Port | The port you want to auto defense, for example, 8022. |
| Protocol | Select the protocol. You can select UDP or TCP. |
| Rate | <p>The maximum packets or connections can be handled per unit time. For example, if you configure it as below:</p> <p>Port: 8022 Protocol: TCP Rate: 10/min</p> <p>Then, it means maximum 10 TCP connections can be handled in 1 minute. The 11th connection will be dropped.</p> |

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.



The IP Blacklist Settings Page includes the following sections:

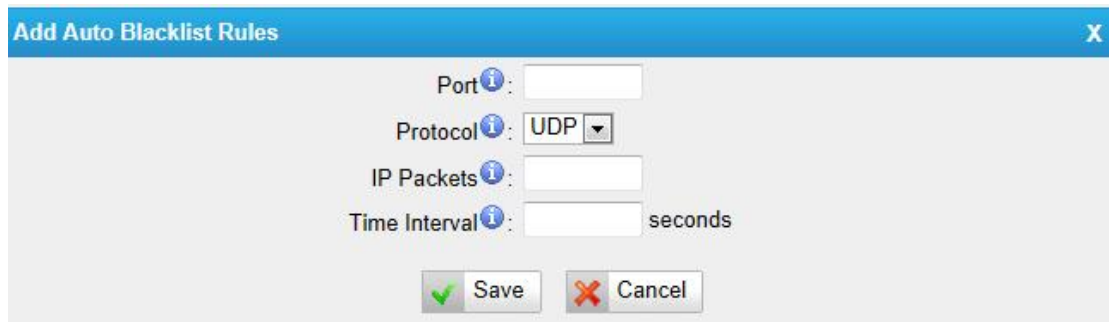
- Blacklist Rules:** A section with an "Add Rule" button and a table of existing rules.

| Port | Protocol | Rate | | |
|------|----------|---------|--|--|
| 5060 | UDP | 120/60s | | |
| 5060 | UDP | 40/2s | | |
| 8022 | TCP | 5/60s | | |
- IP Blacklist:** A section showing "No Auto Black IP Address" in a text box.

Figure 10-10 IP Blacklist Settings Page

1) Blacklist rules

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



The dialog box titled "Add Auto Blacklist Rules" contains the following fields and controls:

- Port:** A text input field.
- Protocol:** A dropdown menu currently showing "UDP".
- IP Packets:** A text input field.
- Time Interval:** A text input field followed by the label "seconds".
- Buttons:** "Save" (with a green checkmark icon) and "Cancel" (with a red X icon).

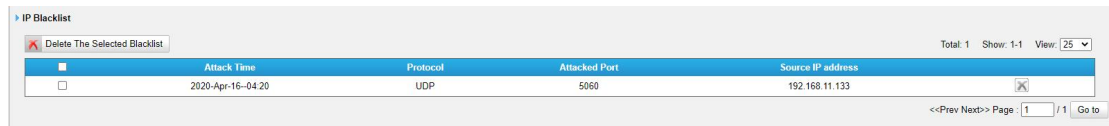
Figure 10-11 Add Blacklist Rule

Table 10-5 Description of Auto Blacklist Rules

| Item | 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.



The "IP Blacklist" table displays the following data:

| | Attack Time | Protocol | Attacked Port | Source IP address |
|--------------------------|-------------------|----------|---------------|-------------------|
| <input type="checkbox"/> | 2020-Apr-16-04:20 | UDP | 5060 | 192.168.11.133 |

Additional UI elements include a "Delete The Selected Blacklist" button, a "Total: 1" indicator, a "Show: 1-1" dropdown, a "View: 25" dropdown, and pagination controls: "<< Prev Next >> Page: 1 / 1 Go to".

System Preferences

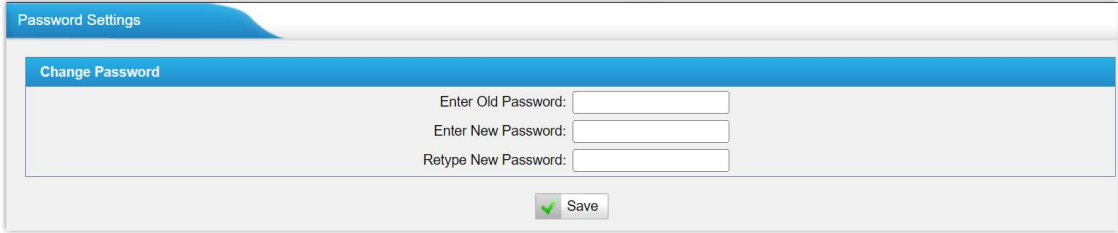
This chapter describes system maintenance settings including the followings:

- Password Settings
- Date and Time
- Email Settings
- Auto Provision Settings
- Firmware Update
- Backup and Restore
- Reset and Reboot

Password Settings

It is highly recommended to change the system's password after first login. Go to **System→System Preferences→Password Settings** to change the password.

1. Enter the old password first.
2. Enter a new password and retype the new password to confirm. The password complexity will be detected, which will help users to set a strong password and make TA3210 safer. A strong password is comprised of letters, numbers and characters.
3. Save the changes, the user will be automatically logged out.
4. Log in TA3210 using the new password.



The screenshot shows a web interface for 'Password Settings'. It features a blue header bar with the title 'Change Password'. Below the header, there are three input fields: 'Enter Old Password:', 'Enter New Password:', and 'Retype New Password:'. At the bottom of the form, there is a 'Save' button with a green checkmark icon.

Figure 11-1 Password Settings

Date and Time

Please adjust the time of TA3210 (including the time zone) consistent with your local time. Go to **System**→**System Preferences**→**Date and Time** to configure the system date and time.

The screenshot shows the 'Date & Time' configuration window. At the top, it displays the 'Server Time' as 'Tue May 05 22:28:17 2015'. Below this, there are three dropdown menus: 'Time Zone' set to '-8 United States - Pacific Time', 'Daylight Saving Time' set to 'Disabled', and a radio button selection for synchronization. The 'Automatically Synchronize With an Internet Time Server' option is selected, showing an 'NTP Server' of 'pool.ntp.org'. The 'Set Date & Time Manually' option is also present, with fields for 'Date' and 'Time' (including AM/PM selection).

Figure 11-2 Date and Time

Table 11.1 Description of Date and Time settings

| Item | Description |
|--|---|
| Time Zone | Select your current and correct time zone on TA3210. |
| Daylight Saving Time | The option is disabled by default. Enable it when necessary |
| Automatically Synchronize with an Internet Time Server | TA3210 will adjust its internal clock to a central network server. Please note the TA3210 should be able to access to the Internet if you choose this method. |
| Set Date & Time Manually | Enter the time using the numbers on your keyboard. |

Note: You have to reboot the system to make the changes take effect.

Email Settings

Set up email server to send system alert or balance alarm.

The screenshot shows the 'Email Settings' window, specifically the 'SMTP Settings for Email' section. A note at the top states: 'Note: if you would like to send system alert or balance alarm with email, please configure this section.' Below this, there are four input fields: 'E-mail Address' (mybpx@sina.com), 'Password' (masked with dots), 'SMTP Server' (smtp.sina.com), and 'Port' (25). There is an unchecked checkbox for 'Use SSL/TLS to send secure message to server'. A 'Test SMTP Settings' button is located at the bottom of the form.

Figure 11-3 Email Settings

Table 11.2 Description of Email settings

| Item | Description |
|--|--|
| E-mail Address | Enter the email address to be used to send alert emails. |
| Password | Enter the password of the email account. |
| SMTP Server | The IP address or hostname of an SMTP server that will be used to send alert as email attachments. |
| Port | Enter the port of the SMTP server. |
| Use SSL/TLS to send secure message to server | Decide whether to enable SSL/TLS encryption. It is recommended that you confirm with your mailbox provider before setting this. Note: If you are using Gmail or Exchange server, this option MUST be enabled. |

After the settings are complete, you need to test if the email server can successfully send emails by clicking "Test SMTP Settings". If the test fails, please check if the TA FXO gateway can connect to the network properly, or if the above information is correct.

Auto Provision Settings

Three methods are supported for Auto Provision: PNP, DHCP, and a manually-configured Server URL to get the configuration file from the server. Go to **System→System Preferences→Auto Provision Settings** to configure.

The screenshot shows a web interface for 'Auto Provision Settings'. At the top, there is a label 'Provision Method:' followed by a large rectangular box. Inside this box, there are three settings, each with a label and a dropdown menu: 'PNP: Yes', 'DHCP: No', and 'Server URL: No'. The dropdown menus are currently set to 'Yes', 'No', and 'No' respectively.

Figure 11-3 Auto Provision Methods

● PNP and DHCP Modes

PNP and **DHCP** modes work along with MyPBX "TA Provisioning". Firstly, users need to configure TA3210 on MyPBX "TA Provisioning" page. Then TA3210 will find and get the configuration file from MyPBX during boots up.

In **PNP** mode, you just need to place the TA3210 in the same IP range network with MyPBX, then you can find the TA3210 and provision it on MyPBX "TA Provisioning" page.

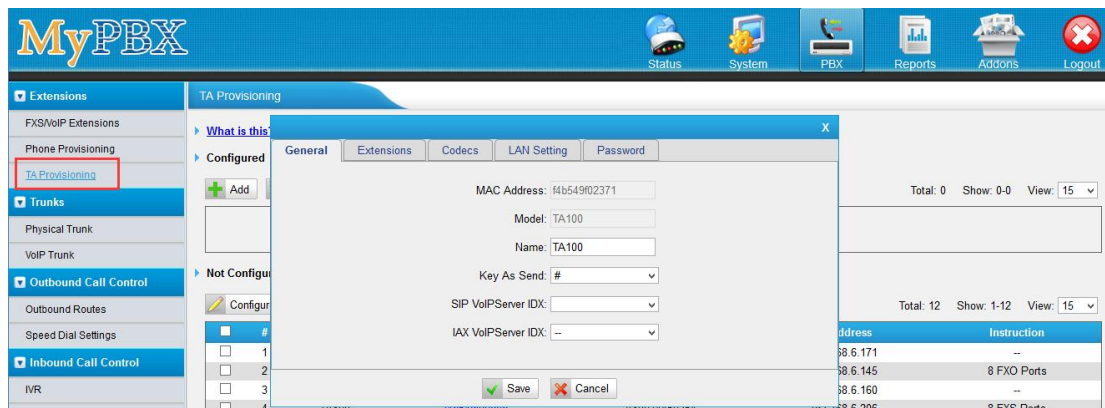


Figure 11-4 MyPBX TA Provisioning

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).

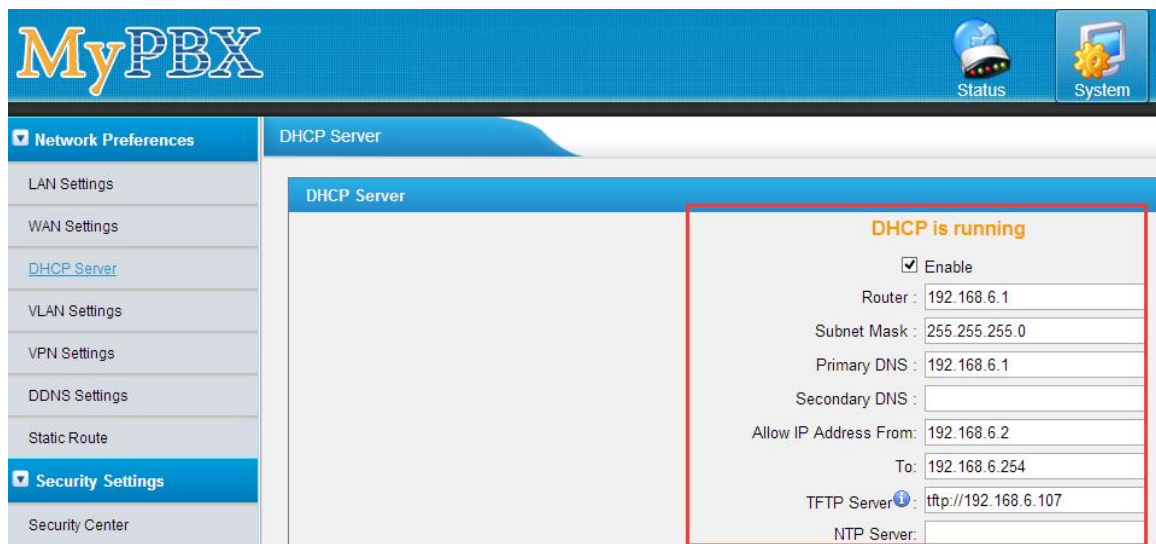


Figure 11-5 Set MyPBX as a DHCP Server

Then select DHCP mode on LAN settings page to make TA3210 as a DHCP client.

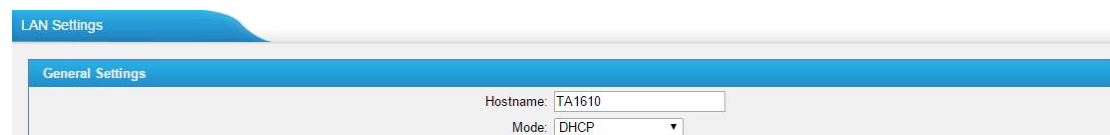


Figure 11-6 Set TA3210 as a DHCP Client

● Server URL

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, TA3210 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 a configuration window with two main sections: "Server Settings" and "Other".

Server Settings:

- Server URL: [Text input field]
- User Name: [Text input field]
- Password: [Text input field]
- Interval of time: ☐ 180 Minute
- Specified time: ☒ Everyday [Dropdown: 00] : [Dropdown: 00]

Other:

- AES Key: [Text input field]
- Always Apply: [Dropdown: No]

Figure 11-7 Auto Provisioning -- Server URL

Table 11.3 Description of Auto Provisioning Server URL Method

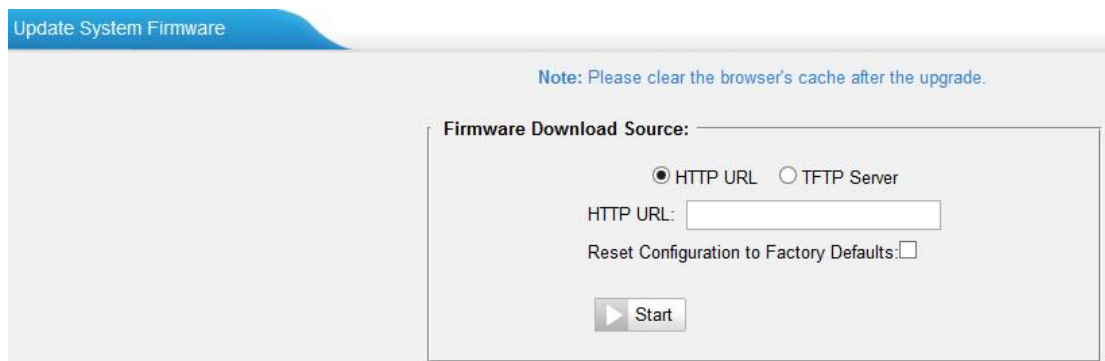
| Item | Description |
|------------------|--|
| Server URL | <p>Enter the server's URL where the gateway can download configuration file.</p> <p>Format: Support HTTP, FTP, and TFTP.</p> <ul style="list-style-type: none"> ● <code>http://{url}</code> ● <code>ftp://host[:port]/[path]</code> ● <code>tftp://host[:port]/[path]</code> |
| User Name | Enter the server's username. Leave this field blank if there is no a user name. |
| Password | Enter the server's password. Leave this field blank if there is no a password. |
| Interval of time | Set up to update the configuration file from the server at regular intervals. |
| Specified time | Set up a specific time to update the configuration file from the server. |
| AES Key | Supports AES-128-CBC. If the configuration file is encrypted by AES key, you need to fill the key in this field. |
| Always Apply | <p>Decide whether to always apply the configuration file.</p> <ul style="list-style-type: none"> ● No: The gateway will compare the current configuration file with the last updated one, if the contents are the same, then no update will be operated. ● Yes: The gateway always apply the updated configuration file. |

Firmware Update

TA3210 can be upgraded to a new firmware version via HTTP or TFTP. Please go to **System**→ **System Preferences**→ **Firmware Update** to complete the upgrade operation.

Notes:

1. If “Reset configuration to Factory Defaults” is enabled, the system will be restored to factory default settings after upgrading.
2. During upgrading, do **NOT** turn off the power. or the system will be damaged.
3. If you are trying to upgrade through HTTP, please make sure that your TA3210 is able to access external network, or it cannot access Yeastar website to get the firmware file, causing the upgrade failure.

Upgrade through HTTP URL


Update System Firmware

Note: Please clear the browser's cache after the upgrade.

Firmware Download Source:

☒ HTTP URL ☐ TFTP Server

HTTP URL:

Reset Configuration to Factory Defaults: ☐

Figure 11-8 Upgrade through HTTP

Step1. On the Firmware Upgrade page, choose **HTTP URL**.

Step2. Enter the download link of the firmware image file.

Note: The HTTP URL MUST be a **BIN** file download link.

Step3. Click “Start” to upgrade.

Upgrade through TFTP Server

Step1. Download firmware file from Yeastar website.

Step2. Create a tftp server (For example, tftpd on Windows).

- 1) Install tftpd32 software on computer.

Download link: http://tftpd32.jounin.net/tftpd32_download.html

- 2) Configure tftpd32.

On option “**Current Directory**”, click “**Browse**” button, choose the firmware file (BIN file) upgraded patch.

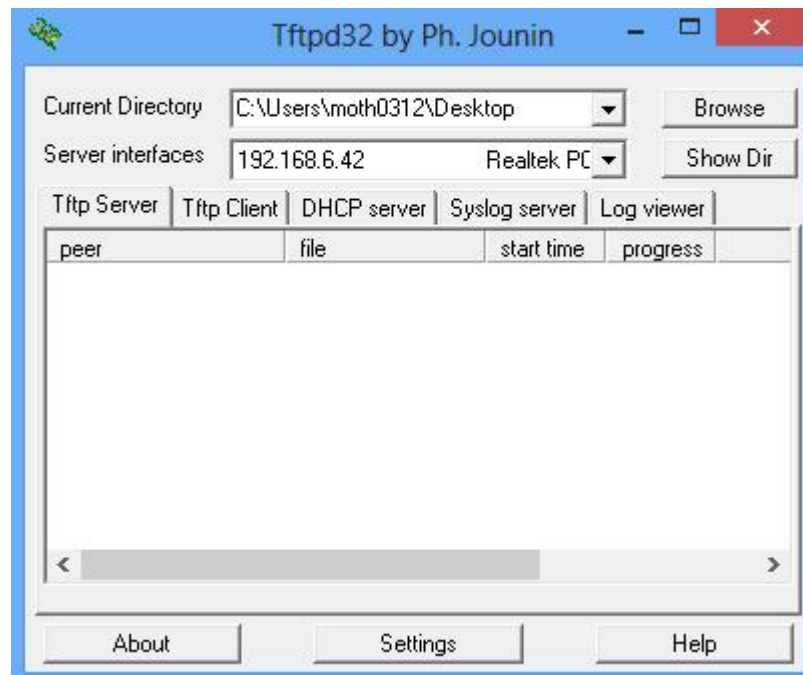


Figure 11-9 Configure Tftpd32

Step3. Log in to the TA3210 Web interface, go to **System→System Preferences→Firmware Update**, and choose “**TFTP Server**”.

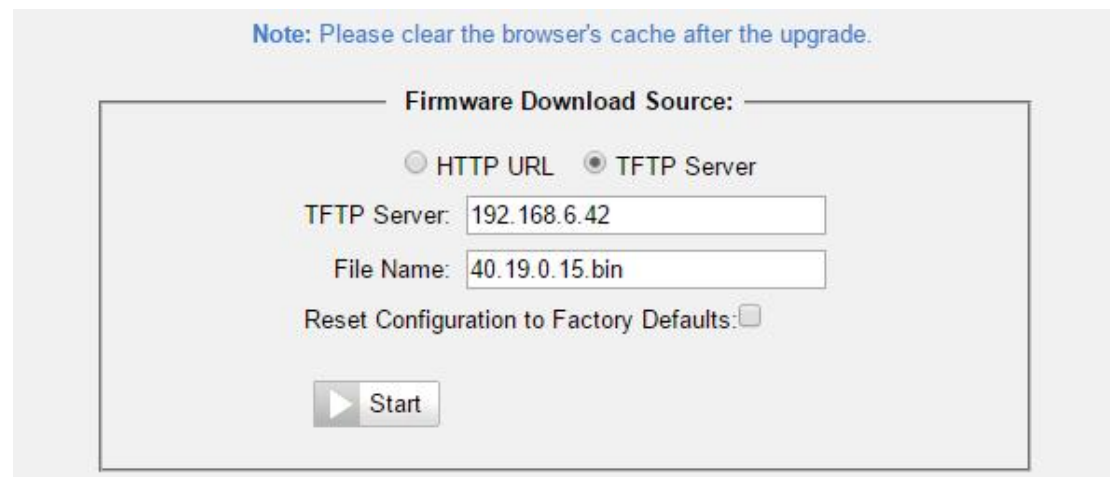


Figure 11-10 Upgrade through TFTP

- 1) TFTP Server: Fill in IP address of tftpd32 server (your PC's IP address).
- 2) File Name: Enter the name of firmware update. It should be a BIN file name.
- 3) Click “Start” to upgrade.

Backup and Restore

TA3210 provides Backup and Restore feature, which allows you to create a complete backup of TA3210 configurations to a file.


Notes:

1. When you have updated the firmware version, it's not recommended to restore using an old package.
2. Backup from an earlier version cannot be restored on TA3210 of a later version.


- **Create a New Backup**

Click  **Create a New Backup** to create a new backup.

- **Upload a Backup**

Click  **Upload a Backup** to upload a backup.

- **Restore**

To restore TA3210 configuration data, upload the backup file to TA3210 and click . Reboot the system to take effect.

Please note the current configurations will be OVERWRITTEN with the backup data.


| # | Name | Time | Options |
|---|----------------------------|-------------------------|---|
| 1 | backup_2015may9_174120.tar | Sat May 09 1:41:58 2015 |    |

Figure 11-11 Restore Backup

Reset and Reboot

You can reset and reboot the system under **System**→ **System Preferences**→ **Reset and Reboot**.

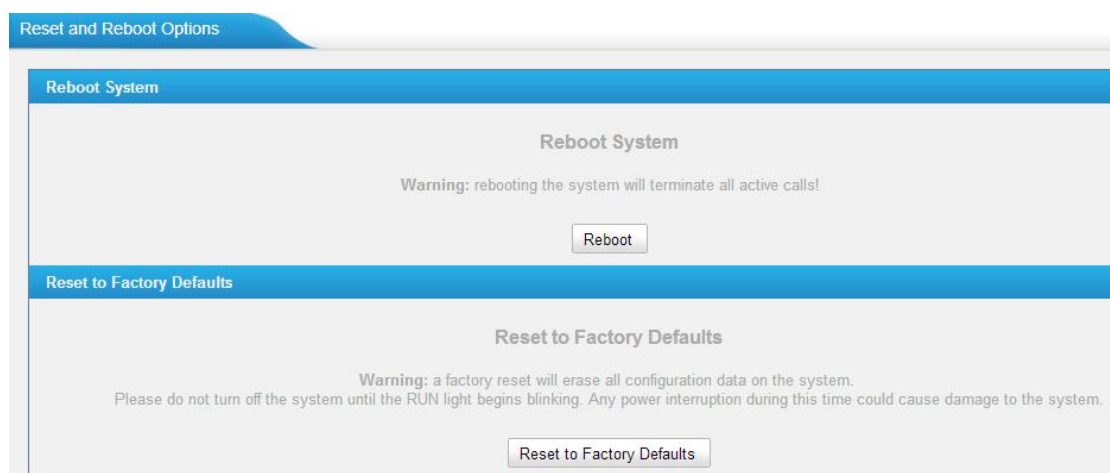


Figure 11-12 Reset and Reboot

Status

You can check the system status on **Status→System Status**, where FXO Port and trunk Status, Network Status and System Info can be checked.

- [Port/Trunk Status](#)
- [Network Status](#)
- [System Info](#)

Port/Trunk Status

Port/Trunk Status

| Port | UP/Down | Available Duration (s) | Status |
|------|---------|------------------------|--------------|
| 1 | Up | Unlimited | Disconnected |
| 2 | Up | Unlimited | Disconnected |
| 3 | Up | Unlimited | Disconnected |
| 4 | Up | Unlimited | Disconnected |
| 5 | Up | Unlimited | Disconnected |
| 6 | Up | Unlimited | Disconnected |
| 7 | Up | Unlimited | Disconnected |
| 8 | Up | Unlimited | Disconnected |

| Status | Trunk Name | Type | User Name | Hostname/IP | Reachability |
|------------|------------|--------|-----------|---------------|--------------|
| OK (11 ms) | MyPBX | SP-SIP | -- | 192.168.6.246 | OK |

| Status | Account | Type |
|--------------------|---------|------|
| No Account Defined | | |

Figure 12-1 Port/Trunk Status

➤ FXO Port Status

Table 12-1 Description of FXO Port Status

| Up/Down | |
|--|---|
| Up | The FXO module works well. |
| Down | The FXO module is broken. |
| Available Duration (s) | |
| The available duration of this PSTN trunk. | |
| Status | |
| Idle | The FXO port is idle. |
| Busy | The FXO port is busy. |
| Disconnect | There is no line connected to the FXO port. |

➤ VoIP Trunk Status

1) SIP/IAX Type

Table 12-2 Description of SIP/IAX Trunk Status

| Status | Description |
|----------------------------|--|
| Registered | Successful registration, trunk is ready for use. |
| Unregistered | Trunk registration failed. |
| Request Sent | Registering. |
| Waiting for Authentication | Wrong password. |

2) SP-SIP/IAX Type

Table 12-3 Description of SP-SIP/IAX Trunk Status

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

3) VoIP Account

Table 12-4 Description of VoIP Account Status

| Status | Description |
|--------------|---|
| Registered | The account is registered successfully on the SIP server. |
| Unregistered | Trunk registration failed. |

Network status

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

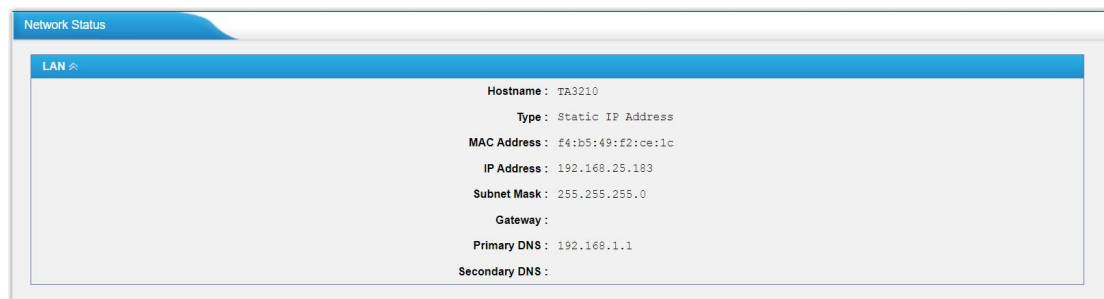


Figure 12-2 Network Status

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

System Info

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



Figure 12-3 System Info

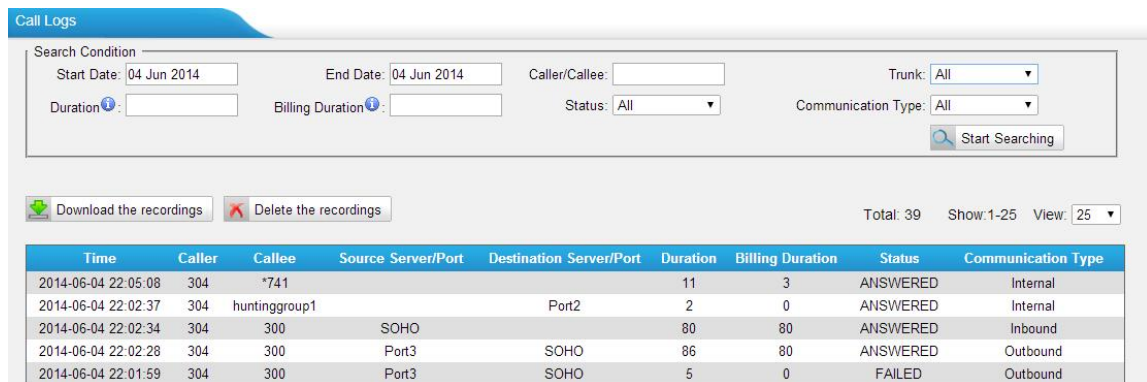
Reports

Users could check the call logs, system logs on **Status**→**Reports** page, and use the packet Tool and Port Monitor Tool to capture debug logs from TA3210.

- [Call Logs](#)
- [System Logs](#)
- [Packet Tool](#)
- [Port Monitor Tool](#)

Call Logs

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



Call Logs

Search Condition

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

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

Start Searching

Download the recordings Delete the recordings

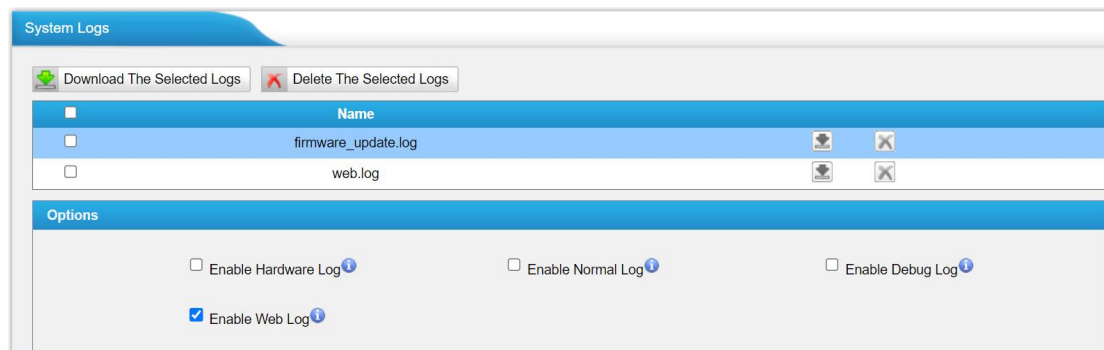
Total: 39 Show: 1-25 View: 25

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

Figure 13-1 Call Logs

System Logs

You can download and delete the system logs of TA3210.



System Logs

Download The Selected Logs Delete The Selected Logs

| Name | | |
|---------------------|--|--|
| firmware_update.log | | |
| web.log | | |

Options

☐ Enable Hardware Log
 ☐ Enable Normal Log
 ☐ Enable Debug Log
 ☒ Enable Web Log

Figure 13-2 System Logs

- **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)

Packet Tool

This feature is used to capture packets for technician. Integrate packet capture tool “Wireshark” in TA3210. Users also could specify the destination IP address and port to get the packets.

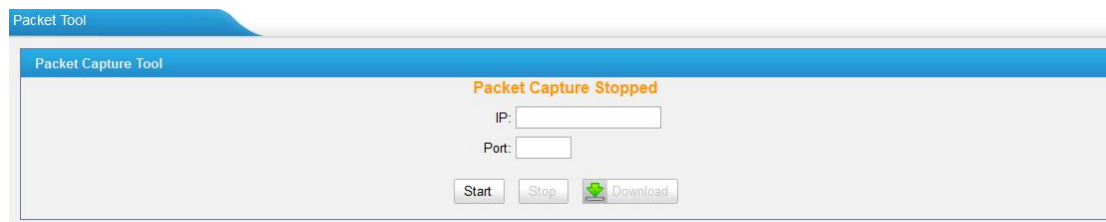


Figure 13-3 Packet Tool

- **IP**
Specify the destination IP address to get the packets.
- **Port**
Specify the destination Port to get the packets.

Port Monitor Tool

This tool is used to debug a FXO port. Select a FXO port and click “Start” to monitor the FXO port, stop monitoring by clicking “Stop” button.



Figure 13-4 Port Monitor Tool