

MyPBX

SOHO V4/V5

Administrator's Guide

Version 70.19.0.23

Yeastar Technology Co., Ltd.

Table of Contents

1. Introduction	5
1.1 Features	5
1.2 Hardware Specifications.....	6
2. System Setup	8
2.1 Connection Drawing	8
2.2 Connecting Ethernet Line	8
2.3 Supplying Power	8
3 Administrator Login.....	10
4 Status.....	13
4.1 Line Status.....	13
4.1.1 Extension Status.....	13
4.1.2 Trunk Status	14
4.2 System Status.....	15
4.2.1 System Info	15
4.2.2 Network Status.....	15
5 System	16
5.1 Network Preferences	16
5.1.1 LAN Settings	16
5.1.2 DHCP Server	17
5.1.3 VLAN Settings	18
5.1.4 VPN Settings.....	19
5.1.5 DDNS Settings.....	20
5.1.6 Static Route	21
5.2 Security Settings	22
5.2.1 Security Center.....	22
5.2.2 Firewall Rules	23
5.2.3 IP Blacklist.....	26
5.2.4 AMI Settings	27
5.2.5 Database Grant	27
5.2.6 Alert Settings	28
5.3 LDAP Server.....	31
5.3.1 LDAP Server.....	31
5.4 Storage Management	32
5.4.1 External Storage	32
5.5 System Preferences.....	35
5.5.1 Password Settings.....	35
5.5.2 Date and Time.....	37
5.5.3 Firmware Update	37
5.5.4 Backup and Restore.....	38
5.5.5 Reset and Reboot.....	39
6 PBX	40
6.1 Extensions	40

6.1.1 FXS/VoIP Extensions.....	40
6.1.2 Phone Provisioning	51
6.2 Trunks	60
6.2.1 Physical Trunk	60
6.2.2 VoIP Trunk.....	67
6.3 Outbound Call Control	77
6.3.1 Outbound Routes	77
6.3.2 Speed Dial Settings.....	80
6.4 Inbound Call Control	80
6.4.1 IVR.....	81
6.4.2 Ring Groups	84
6.4.3 Queues	86
6.4.4 Conferences.....	90
6.4.5 Inbound Routes	91
6.5 Audio Settings	97
6.5.1 Custom Prompts	97
6.5.2 Music on Hold Prompts.....	98
6.5.3 System Prompts Settings	99
6.6 Basic Settings.....	100
6.6.1 General Preferences	100
6.6.2 Business Hours.....	103
6.6.3 Feature Codes	104
6.6.4 Voicemail Settings.....	107
6.7 Advanced Settings	111
6.7.1 SIP Settings.....	111
6.7.2 IAX Settings.....	118
6.7.3 Blacklist	119
6.7.4 Callback Settings	120
6.7.5 DNIS Settings	122
6.7.6 DISA.....	122
6.7.5 PIN User Settings.....	123
6.7.8 PIN Settings.....	125
6.7.9 Paging Groups.....	126
6.7.10 Certificates.....	127
7 Reports.....	128
7.1 Call Logs.....	128
7.2 System Logs	128
8 Logout.....	130
9. Use MyPBX	130
9.1 Make outbound calls.....	130
Sample Routing via VoIP Trunk.....	131
9.2 Incoming call.....	134
Sample Routing to an IVR.....	134
APPENDIX A FAQ.....	136

APPENDIX B How to Configure External Storage	137
APPENDIX C How to Configure NAT Setting.....	139
APPENDIX D How to Use Auto Provision.....	141
APPENDIX E How Do I Configure Distinctive Ring Tones	145
APPENDIX F How to Use DID.....	147
APPENDIX G How to Use BLF Key to Choose the PSTN Line.....	151
APPENDIX H MyPBX Security Configuration Guide	152
APPENDIX I How to Use TLS in MyPBX.....	179
I.1 How to register IP phones to MyPBX via TLS	179
I.2 How to register SIP trunk to VoIP provider via TLS	203
APPENDIX J How to use LDAP	205

1. Introduction

MyPBX SOHO—IP-PBX for Small Business/Home Office

MyPBX SOHO is a standalone embedded hybrid PBX for small businesses and remote branch offices of larger organizations. MyPBX also offers a hybrid solution (a combination of VoIP applications using legacy telecom equipment) alternative for enterprises who are not yet ready to migrate to a complete VoIP solution.

***Note: This guide applies to MyPBX SOHO V4/V5, the hardware pictures in this document are for MyPBX SOHO V5.**

1.1 Features

• Alert	• Follow me
• Auto-provision	• HTTPS
• Blacklist	• Integrated built-in packet capture tools
• BLF Support	• Interactive Voice Response (IVR)
• Blind Transfer	• Intercom/Zone Intercom
• Call Back	• L2TP
• Call Detail Records(CDR)	• LDAP
• Call Forward	• Mobility Extension
• Call Parking	• Multiple administrators
• Call Pickup	• Music On Hold
• Call Recording	• Music On Transfer
• Call Routing	• Open VPN
• Call transfer	• Paging/Zone Paging
• Call Transfer	• PIN Users
• Call Waiting	• QoS
• Caller ID	• Queue
• Conference	• Ring Group
• Database Grant	• Route by Caller ID
• DDNS	• Security Center
• Define Office Time	• Skype Integration (Skype Connect)
• Dial by Name	• Speed Dial
• DIDs	• Spy functions
• Direct Inward System Access (DISA)	• Static Route
• Distinctive Ringtone	• T.38
• Do Not Disturb(DND)	• Three-way Calling

- External Storage

- VLAN

- Firewalls

- Voicemail

For more info, please click:

<http://www.yeastar.com/products/MyPBX-SOHO.asp>

1.2 Hardware Specifications

1) Front Panel



Figure 1-1 MyPBX SOHO V5 Front Panel Picture

No.	Identification
①	Green LED indicates the power connection is normal.
②	Green LED indicates the server system is in working order
③	Green LED indicates the system is ready.
④	Green LED indicates the Internet interface is in use
⑤	Red LED stands for FXO port Orange LED indicates presence of a BRI port. Green LED stands for FXS port Red LED blinks: FXO port isn't connected to PSTN line. Alternately blinks Red and Green: FXO port has an incoming call. Alternately blinks Red and Green fast: FXO port is in a call. Alternately blinks Green and Red: FXS port is ringing. Alternately blinks Green and Red fast: FXS port is in a call.

2) Rear Panel



Figure 1-2 MyPBX SOHO V5 Rear Panel

2. System Setup

2.1 Connection Drawing

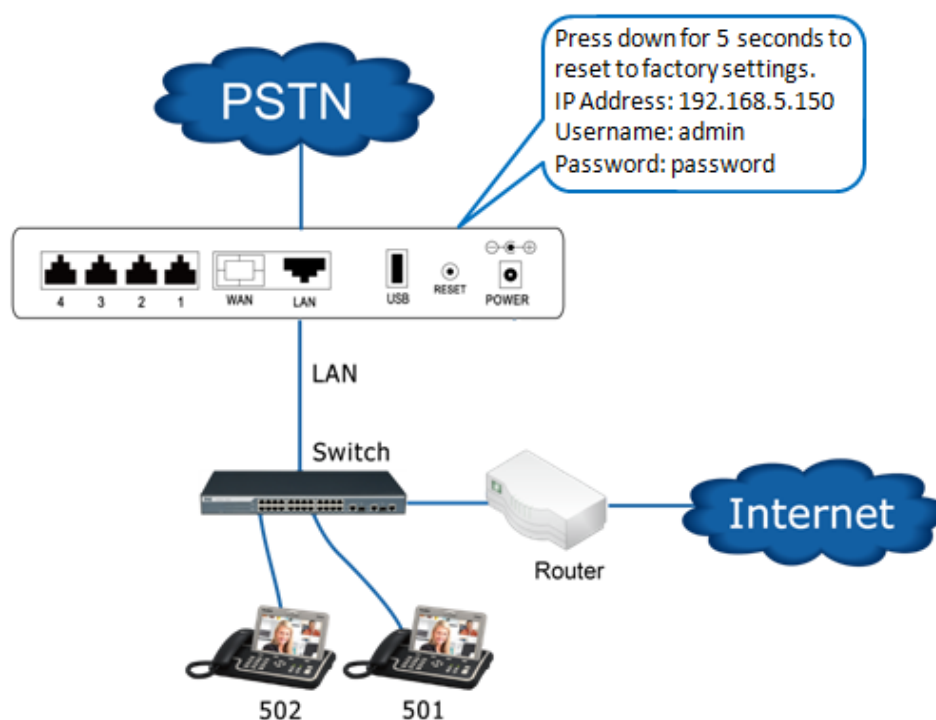


Figure 2-1

2.2 Connecting Ethernet Line

MyPBX provides two 10/100M Ethernet ports with RJ45 interface and LED indicator. Plug Ethernet line into MyPBX's Ethernet port, and then connect the other end of the Ethernet line with a hub, switch, router, LAN or WAN. Once connected, check the status of the LED indicator. A yellow LED indicates the port is in the connection process, and a green LED indicates the port is properly connected.

2.3 Supplying Power

MyPBX utilizes the high-performance switch power supply, which supplies the required power for the unit.

AC Input: 100~240V

DC Output: 12V, 1A

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

1. Connect the small end of the power cable to the power input port on the MyPBX back panel, and plug the other end of the cable into a 100VAC power outlet.
2. Check the Power LED on the front panel. A solid green LED indicates that power is being supplied correctly.

3. Administrator Login

From your web browser, input the IP address of the MyPBX server.

If this is the first time you are configuring MyPBX, please use the default settings as below (your PC should be in the same local network with MyPBX):

IP Address: <http://192.168.5.150>

Username: **admin**

Password: **password**

In this example, the IP address is 192.168.5.143

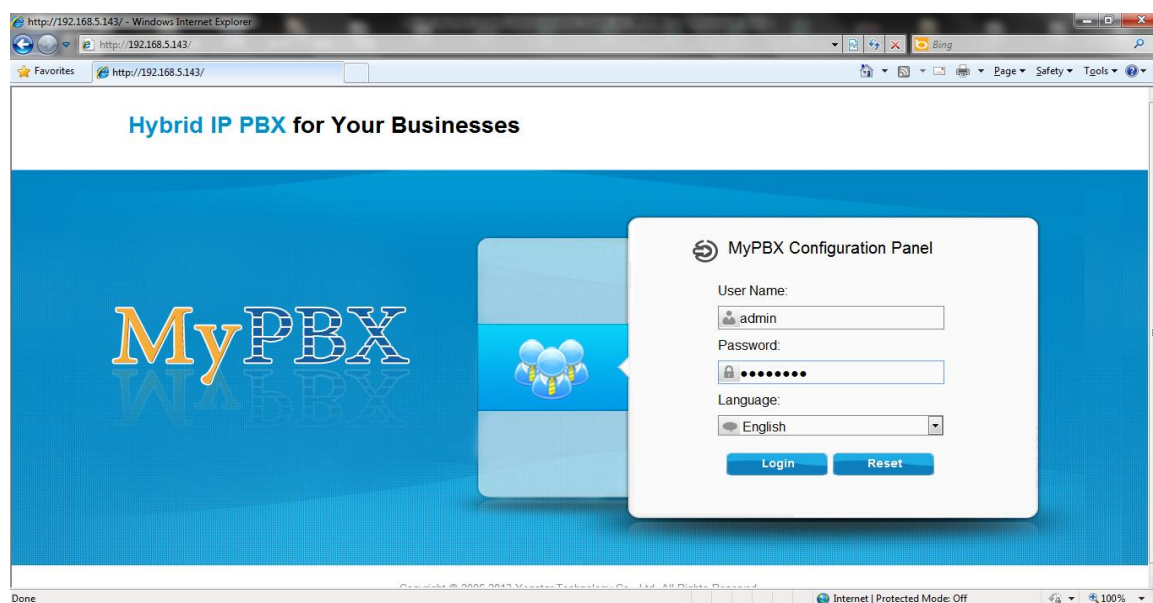


Figure 3-1

This is the welcome page of MyPBX SOHO after successful login.

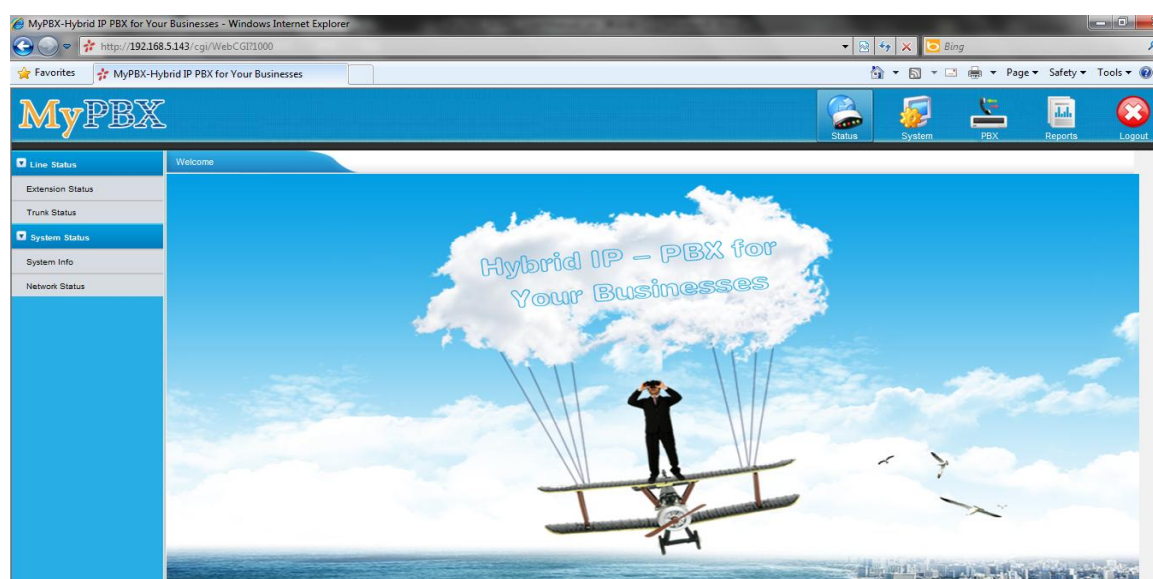


Figure 3-2

You can also login via HTTPS protocol

Like `https://192.168.5.147`, you will see a prompt that is a certificate problem. Click "Continue to ...", then you can login after entering user and password. HTTPS is HTTP over SSL, and it is safer than HTTP.

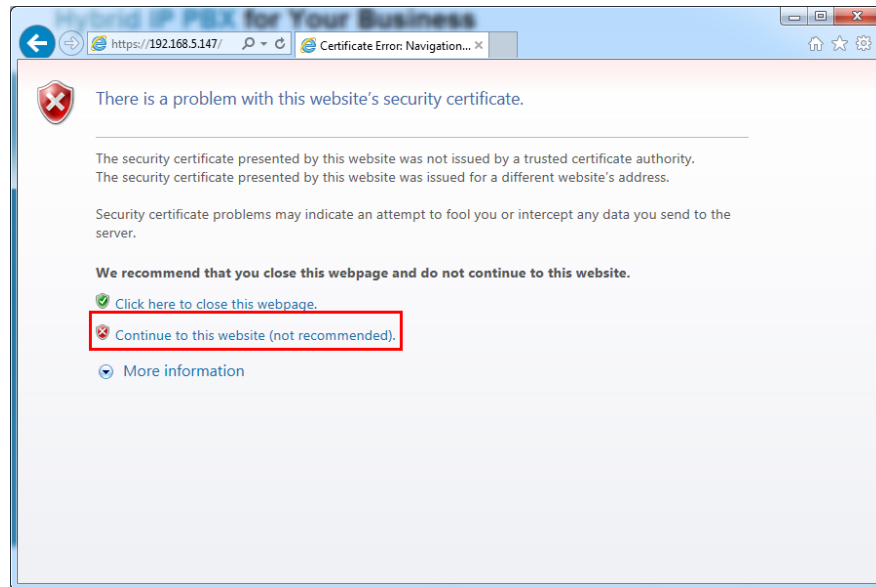


Figure 3-3

Note:

MyPBX firmware upgrade follow-up

- Reboot the device twice to make the new firmware take effect
 - Clean the cache and cookies of the browser before login.
 - There is a compatibility issue with IE11. Configure IE11 browser "Compatibility View Settings", add MyPBX IP address, and check "Display Intranet sites in Compatibility View" and "Use Microsoft compatibility lists".
- See the following picture. MyPBX IP is 192.168.5.147 in this example.

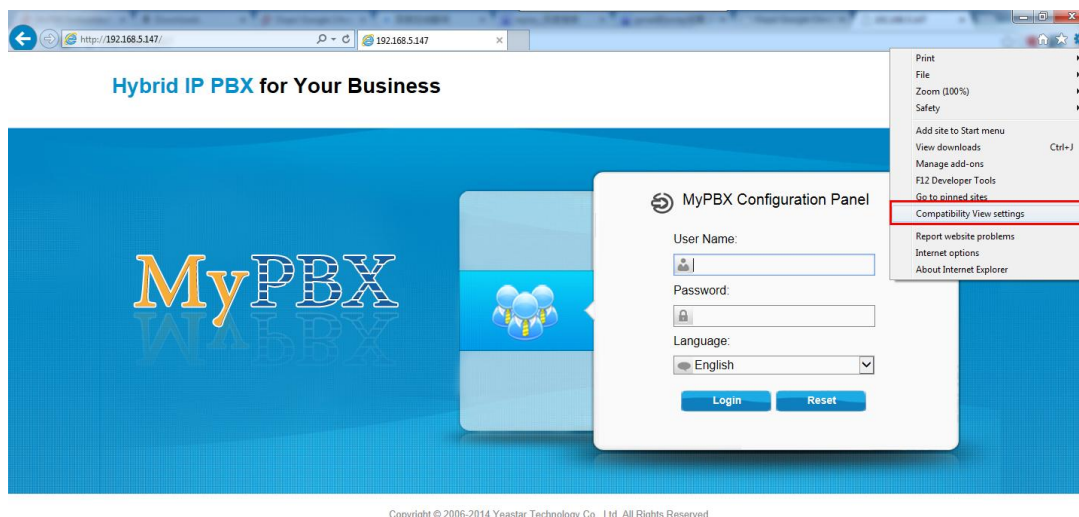


Figure 3-4

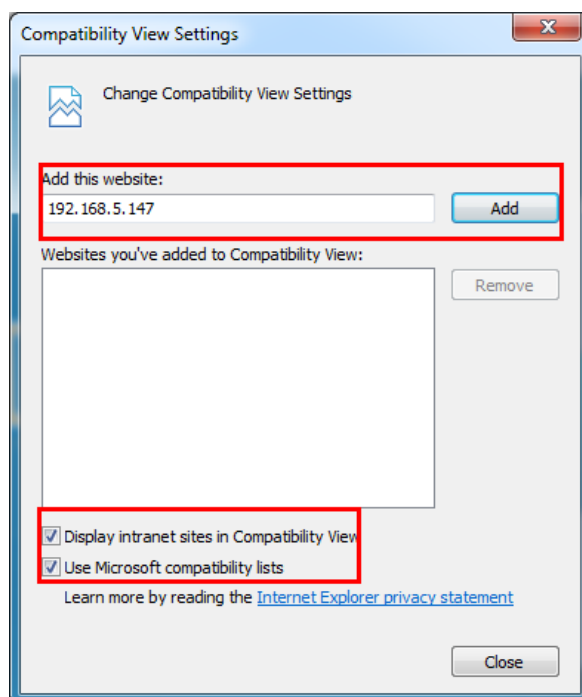


Figure 3-5

4. Status



Click  to start to check the status of MyPBX SOHO. We can check the status of extensions, trunks, and network and system information.

4.1 Line Status

In this page, we can check the status of extensions and trunks

4.1.1 Extension Status

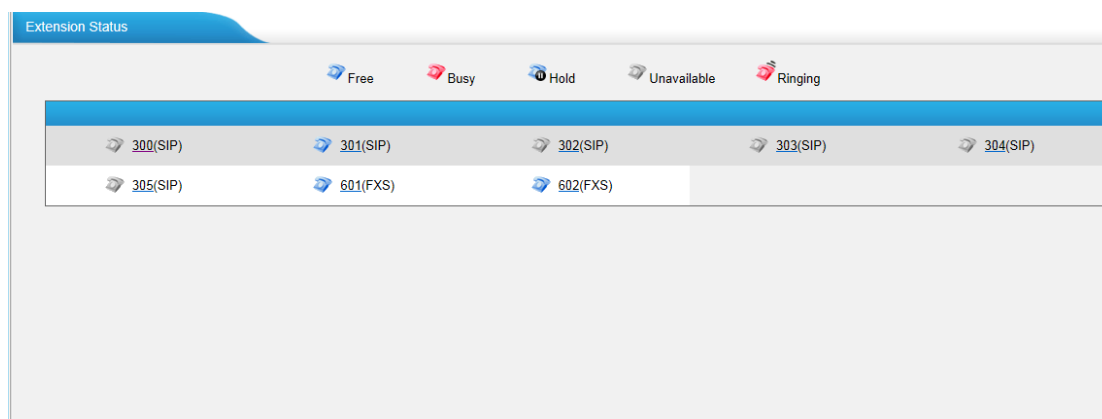


Figure 4-1

MyPBX Status Description:

Extensions:

- 1)  : Extension is unavailable
- 2)  : Extension is idle
- 3)  : Extension is ringing
- 4)  : Extension is busy
- 5)  : Extension is on hold

4.1.2 Trunk Status

Trunk Status					
Status	Trunk Name	Type	User Name	Port/Hostname/IP	Reachability
Registered	Yeastar	SIP	5012	192.168.5.101	OK
OK (1 ms)	Support	SP-SIP		192.168.4.142	OK (1 ms)
Idle	pstn4	FXO		Port 4	
OK	BriTrunk1	BRI		Port 1	
OK	BriTrunk2	BRI		Port 2	

Figure 4-2

Trunks:

VoIP Trunk:

Status

Unregistered: Trunk registration failed.

Registered: Successful registration, trunk is ready for use.

Request Send: Registering.

Waiting: Waiting for authentication.

Service Provider:

Status

OK: Successful registration, trunk is ready for use.

Unreachable: The trunk is unreachable.

Failed: Trunk registration failed.

FXO Trunk:

Status

Idle: The port is idle.

Busy: The port is in use.

Disconnected: The port hasn't connected to the PSTN line.

More detail message, please refer to the LED indication of front panel.

BRI Trunk:

Status

Ok: The ports connect correctly.

Disconnected: The port hasn't connected to the BRI line

4.2 System Status

In this page, we can check the status of MyPBX system, including the hardware, firmware version and the network status.

4.2.1 System Info

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

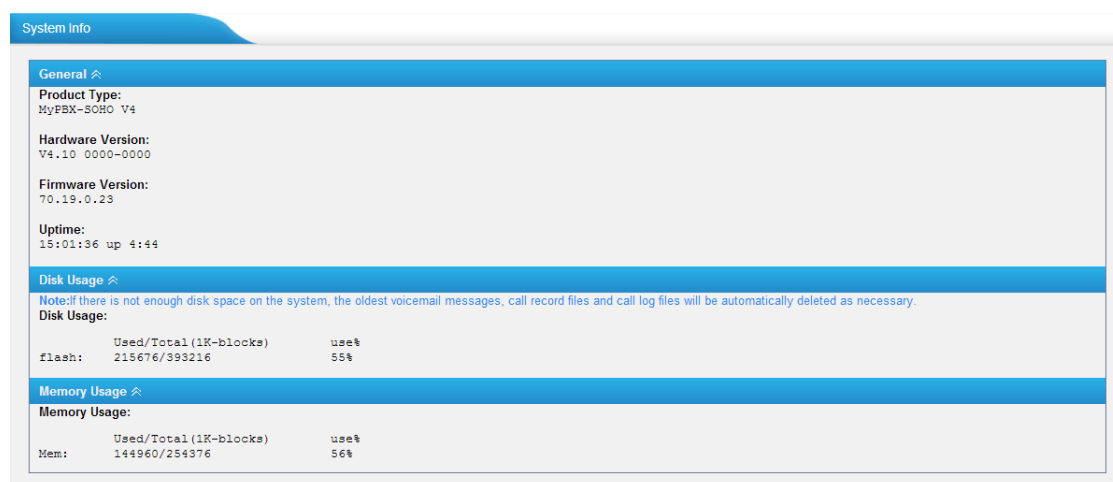


Figure 4-3

4.2.2 Network Status

In this page, the IP address of LAN port will appear. If OpenVPN and VLAN are configured well, they will be displayed here, too.

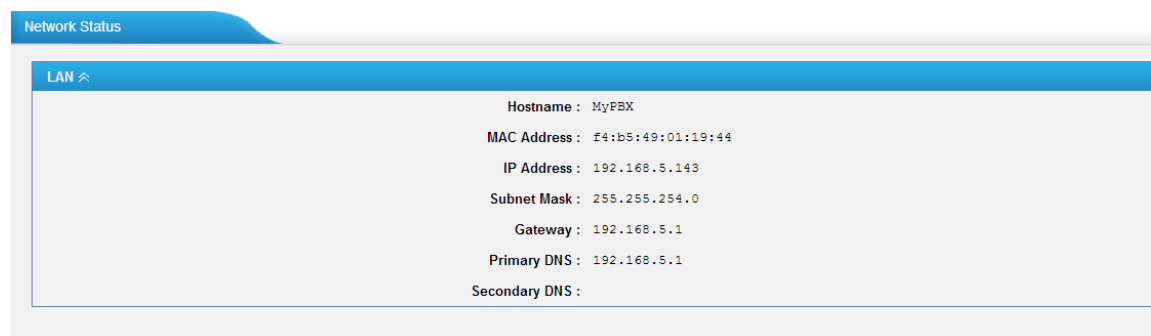


Figure 4-4

5. System

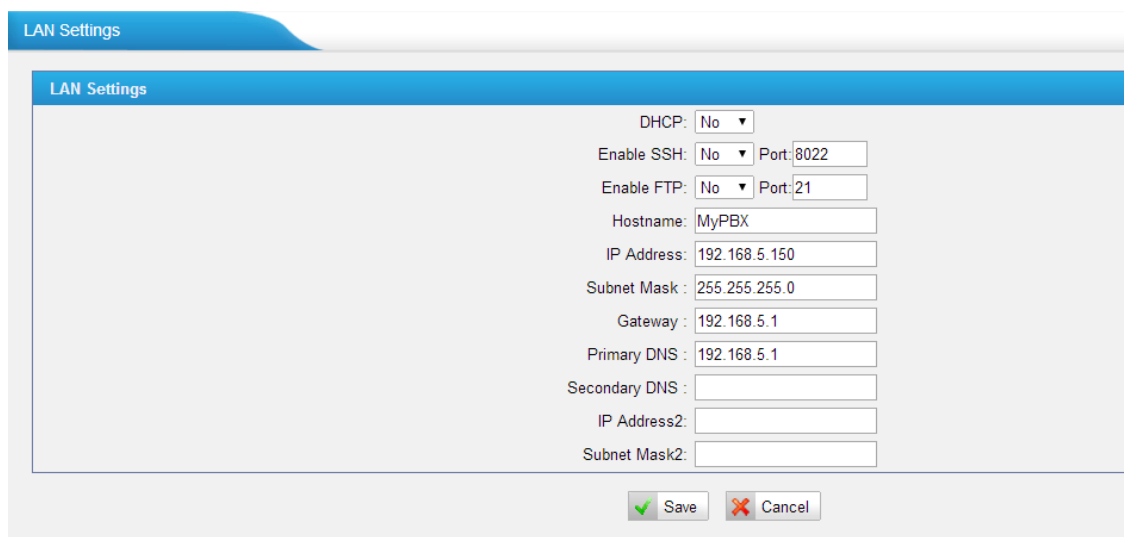


Click  to access.

In this page, we can configure the network settings, firewall settings, storage management and some other settings like firmware update.

5.1 Network Preferences

5.1.1 LAN Settings



LAN Settings	
DHCP:	No
Enable SSH:	No Port: 8022
Enable FTP:	No Port: 21
Hostname:	MyPBX
IP Address:	192.168.5.150
Subnet Mask :	255.255.255.0
Gateway :	192.168.5.1
Primary DNS :	192.168.5.1
Secondary DNS :	
IP Address2:	
Subnet Mask2:	

Figure 5-1

•DHCP

If this option is set, MyPBX will use DHCP to get an available IP address from your local network. Not recommended as without the right IP address you cannot access MyPBX.

•Enable SSH

This is the advanced way to access the device; you can use the software “putty” to access the device. In the SSH access, you can do more advanced setting and debug, it’s disabled by default.

•**Port:** the default is 8022; you can change it.

•Hostname

Set the host name for MyPBX.

•IP Address

Set the IP Address for MyPBX.

A static IP address for MyPBX is recommended.

•Subnet Mask

Set the subnet mask for MyPBX.

•Gateway

Set the gateway for MyPBX.

•Primary DNS

Set the primary DNS for MyPBX.

•Secondary DNS

Set the secondary DNS for MyPBX.

•IP Address2

Set the second IP Address for MyPBX.

•Subnet Mask2

Set the second subnet mask for MyPBX.

5.1.2 DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network. You can set a local network NTP server for MyPBX here, too.

Note: MyPBX SOHO can be working as a DHCP server, but cannot be regarded as a router.

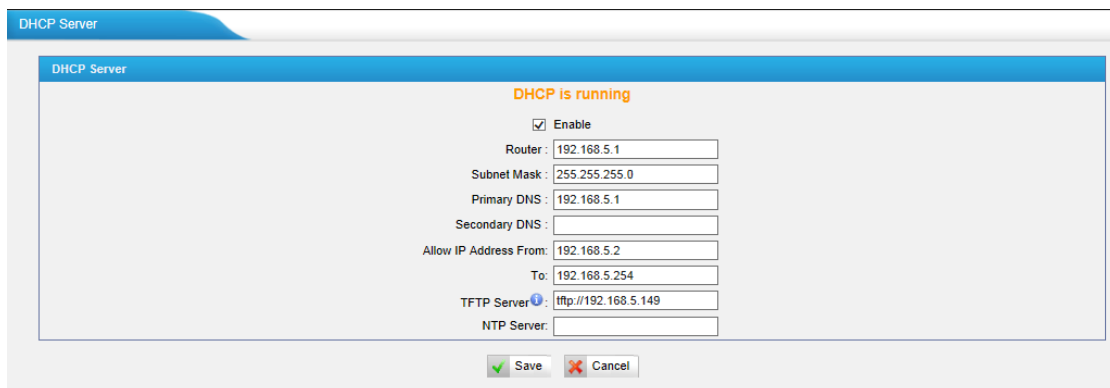


Figure 5-2

5.1.3 VLAN Settings

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

Note:

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

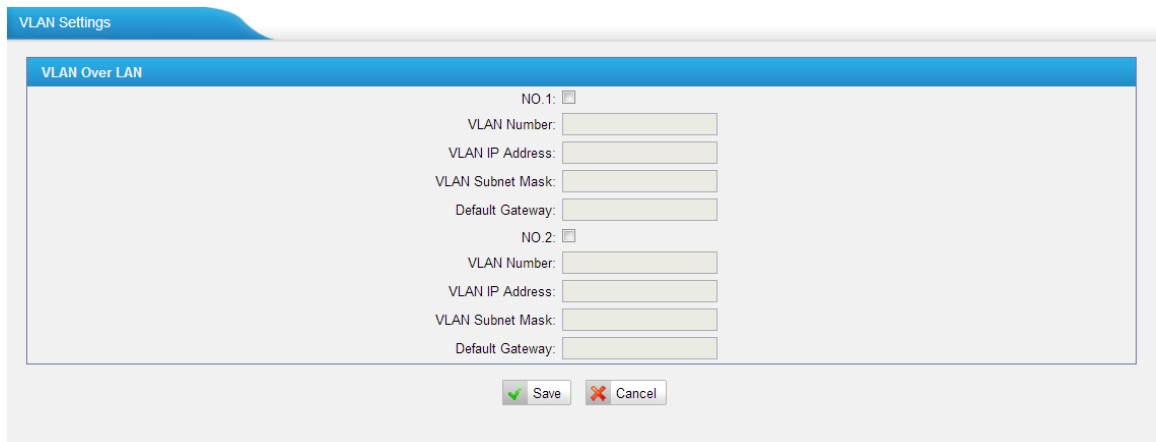


Figure 5-3

VLAN Over LAN

•NO.1

Click the NO.1 you can edit the first VLAN over LAN.

•VLAN Number

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

•VLAN IP Address

Set the IP Address for MyPBX VLAN over LAN.

•VLAN Subnet Mask

Set the Subnet Mask for MyPBX VLAN over LAN.

•Default Gateway

Set the Default Gateway for MyPBX VLAN over LAN

•NO.2

Click the NO.2 you can edit the first VLAN over LAN.

•VLAN Number

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

•VLAN IP Address

Set the IP Address for MyPBX VLAN over LAN.

•VLAN Subnet Mask

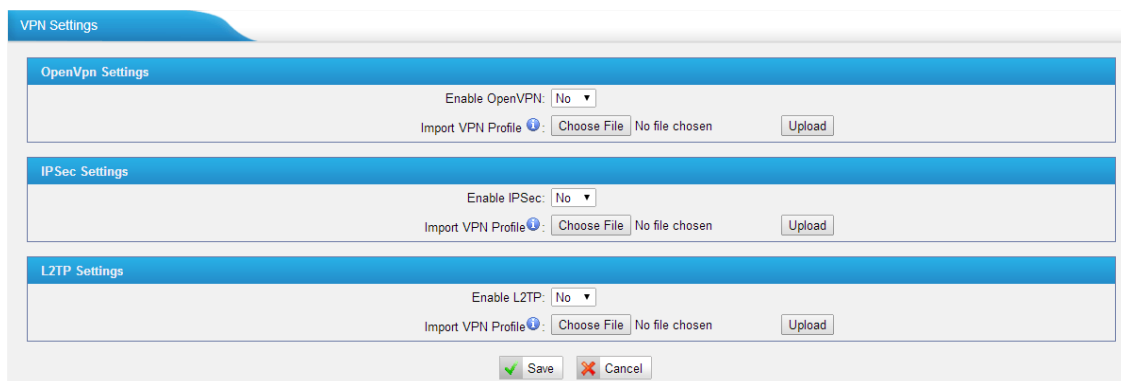
Set the Subnet Mask for MyPBX VLAN over LAN.

•Default Gateway

Set the Default Gateway for MyPBX VLAN over LAN.

5.1.4 VPN Settings

A virtual private network (VPN) is a method of computer networking—typically using the public Internet—that allows users to privately share information between remote locations, or between a remote location and a business home network. A VPN can provide secure information transport by authenticating users, and encrypting data to prevent unauthorized persons from reading the information transmitted. The VPN can be used to send any kind of network traffic securely. MyPBX supports OpenVPN, IPSec and L2TP.



The screenshot shows the 'VPN Settings' page in the MyPBX administrator interface. It features three distinct configuration sections: 'OpenVpn Settings', 'IPSec Settings', and 'L2TP Settings'. Each section includes a dropdown menu to 'Enable' the respective service, which is currently set to 'No'. Below each enable toggle is an 'Import VPN Profile' button with a small file icon, followed by a 'Choose File' button and an 'Upload' button. The 'No file chosen' text is visible next to the 'Choose File' buttons. At the bottom of the page, there are 'Save' and 'Cancel' buttons.

Figure 5-4

•Enable OpenVPN**•Import VPN Profile**

Import configuration file of OpenVPN. Don't configure "user" and "group" in the "config" file.

•Enable IPSec**•Import VPN Profile**

Import configuration file of IPSec. There can be only one "lan" in the "conf" file.

•Enable L2TP

•Import VPN Profile

Import configuration file of L2TP. There can be only one "conn" in the "conf" file.

Note: for more details about the above VPN settings, please contact our technical support.

5.1.5 DDNS Settings

DDNS(Dynamic DNS) is a method/protocol/network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a Domain Name System (DNS) name server to change, in real time, the active DNS configuration of its configured hostnames, addresses or other information.

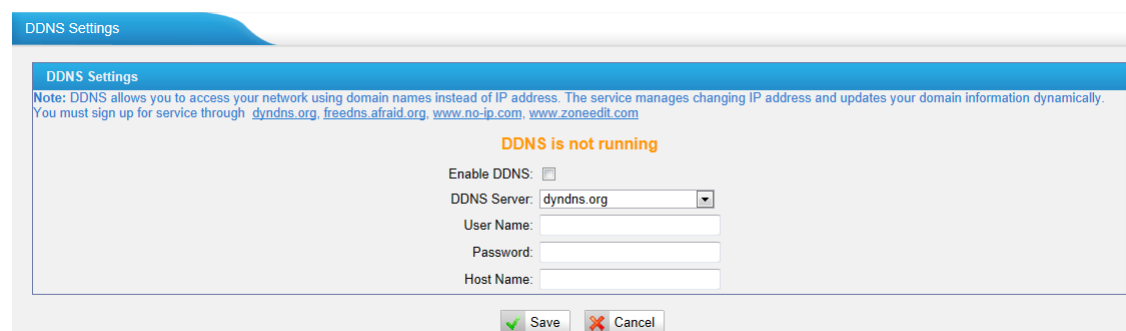


Figure 5-5

•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.

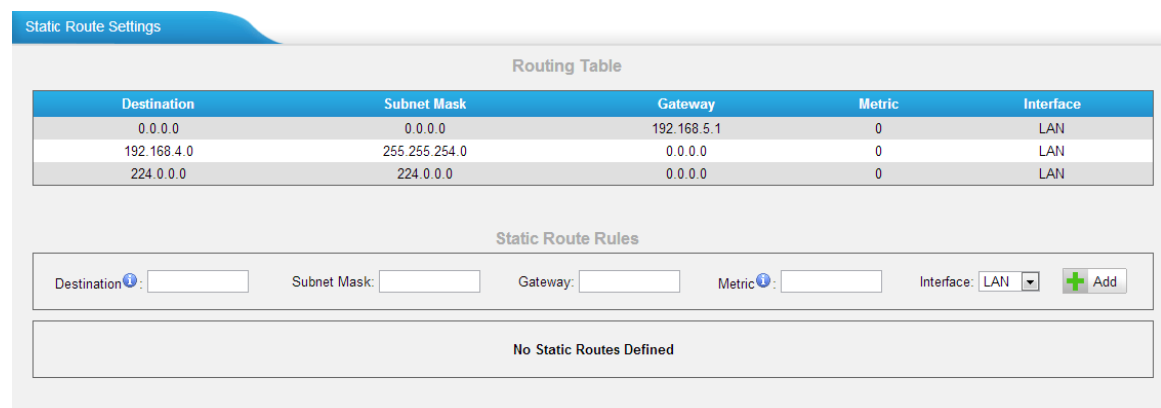
•Host Name

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

5.1.6 Static Route

MyPBX 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 MyPBX to force it goes out through different gateway when accessing different Internet. The default gateway priority of MyPBX from high to low is OpenVPN→WAN port→LAN port.



Destination	Subnet Mask	Gateway	Metric	Interface
0.0.0.0	0.0.0.0	192.168.5.1	0	LAN
192.168.4.0	255.255.254.0	0.0.0.0	0	LAN
224.0.0.0	224.0.0.0	0.0.0.0	0	LAN

Static Route Rules

Destination: Subnet Mask: Gateway: Metric: Interface: LAN

No Static Routes Defined

Figure 5-6

1) Route table

The current route rules of MyPBX

•Destination

The destination network to be accessed by MyPBX

•Subnet Mask

Specify the destination network portion.

•Gateway

Define which gateway MyPBX 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.

2) Static Route Rules

You can add new static route rules here.

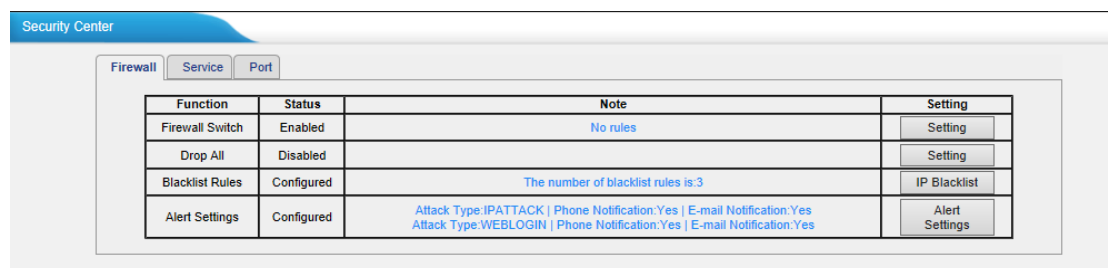
5.2 Security Settings

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.

5.2.1 Security Center

You can check MyPBX security configuration in "Security Center" page. And also, you can enter the relevant security settings page rapidly.

Firewall:

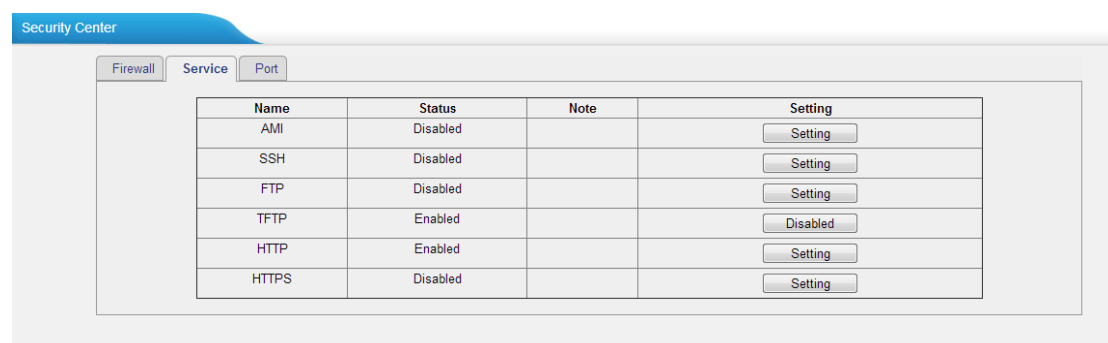


Function	Status	Note	Setting
Firewall Switch	Enabled	No rules	Setting
Drop All	Disabled		Setting
Blacklist Rules	Configured	The number of blacklist rules is 3	IP Blacklist
Alert Settings	Configured	Attack Type:IPATTACK Phone Notification:Yes E-mail Notification:Yes Attack Type:WEBLOGIN Phone Notification:Yes E-mail Notification:Yes	Alert Settings

Figure 5-7 Security Center-Firewall

In the "Firewall" tab, you can check firewall configuration and alert settings. By clicking the relevant button, you can enter the configuration page directly.

Service:



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

Figure 5-8 Security Center-Service

In "Service" tab, you can check AMI/SSH/TFTP status. For AMI/SSH, you can

enter the according page by clicking the button in "Setting" column. For TFTP, you can directly disable or enable it.

Port:

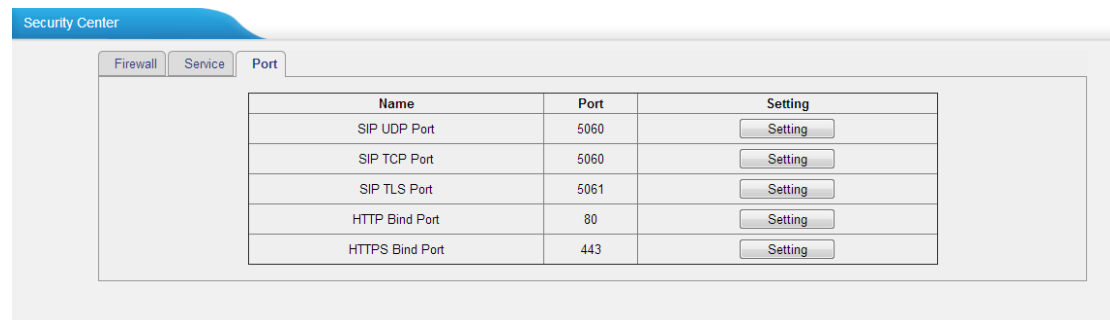


Figure 5-9 Security Center-Port

In "Port" tab, you can check SIP port and HTTP port. You can also enter the relevant page by clicking the button in "Setting" column.

5.2.2 Firewall Rules

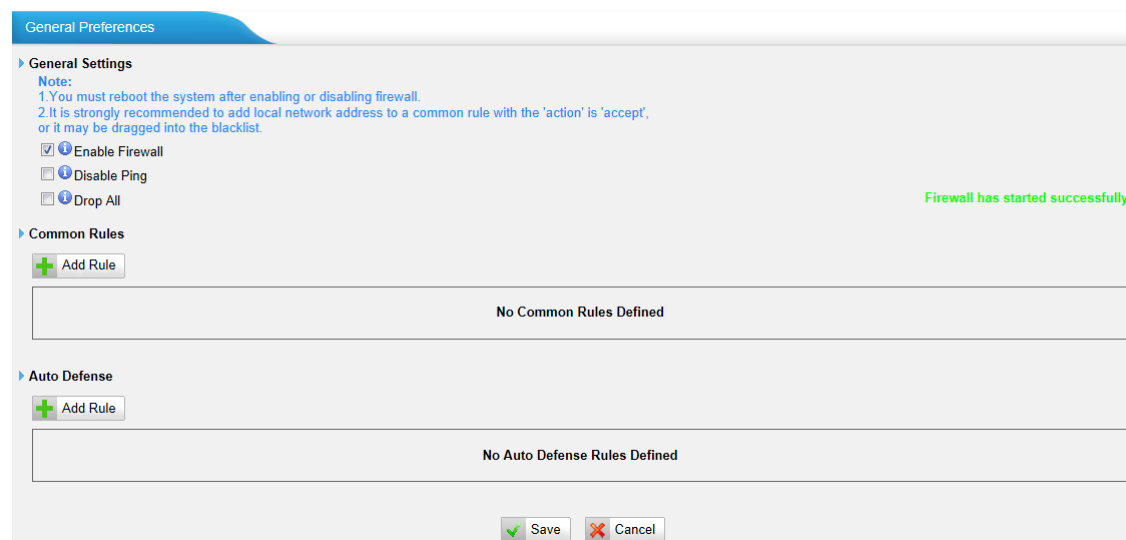


Figure 5-10 Firewall Settings

1) General Settings

•Enable Firewall

Enable the firewall to protect the device.

•Disable Ping

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

•Drop All

When you enable "Drop All" feature, system will drop all packets or connection from other hosts if there are no other rules defined. To avoid locking the devices,

at least one "TCP" accept common rule must be created for port used for SSH access, port used for HTTP access and port used for CGI access.

2) Common Rules

There is no default rule; you can create them as required.

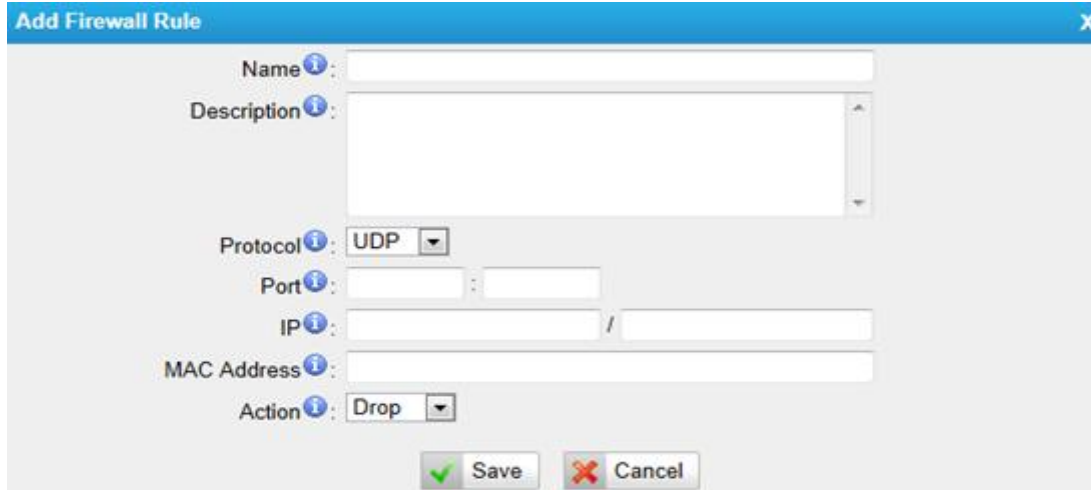


Figure 5-11 Add Common Rules

•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. 216.207.245.47/255.255.255.255 for IP 216.207.245.47

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.

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.

•Action

Accept: Accept the access from remote hosts.

Drop: Drop the access from remote hosts.

Ignore: Ignore the access.

3) Auto Defense

By default, there is no rule.

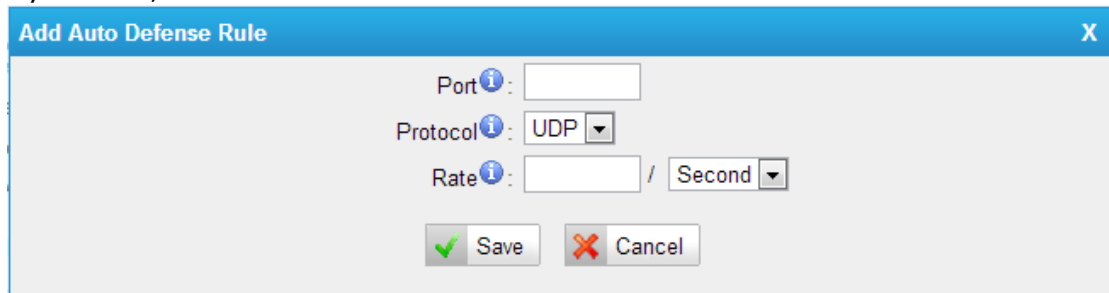
A screenshot of a web-based configuration window titled "Add Auto Defense Rule". The window has a blue header bar with the title and a close button (X). The main area is light gray and contains three input fields: "Port" with an information icon and a text box, "Protocol" with an information icon, a dropdown menu showing "UDP", and "Rate" with an information icon, a text box, a slash, and a dropdown menu showing "Second". At the bottom, there are two buttons: "Save" with a green checkmark icon and "Cancel" with a red X icon.

Figure 5-12 Add Auto Defense Rule

Port

The port you want to auto defense, for example, 8022.

Protocol:

Select the protocol. You can select UDP or TCP.

Rate:

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

For example, if you configure it as below:

Port: 8022

Protocol: TCP

Rate: 10/min

Then, it means maximum 10 TCP connections can be handled in 1 minute. The 11th connection will be dropped.

5.2.3 IP Blacklist

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

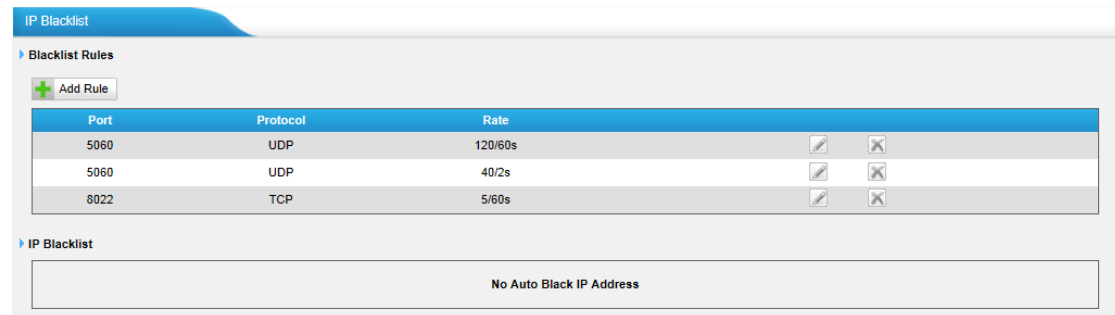


Figure 5-13 IP Blacklist Settings Page

1) Blacklist rules

You can add the rules for IP blacklist rate as you wish.

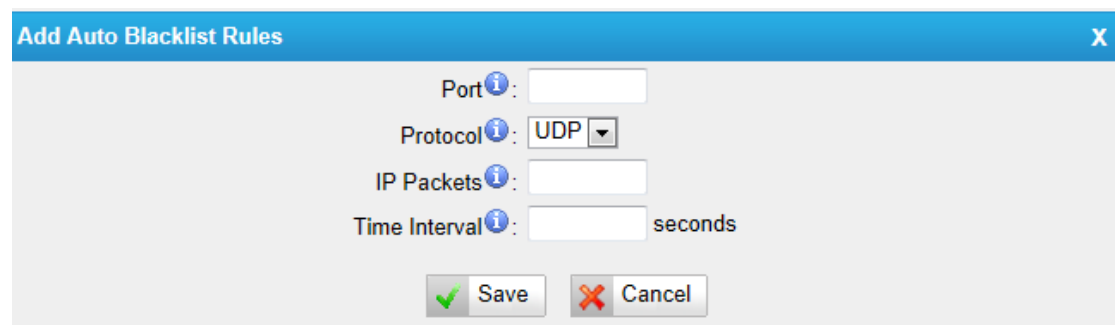


Figure 5-14 Add Blacklist Rule

•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 delete it as you wish.

5.2.4 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 MyPBX using AMI interface. It is disabled by default. If necessary, you can enable it.

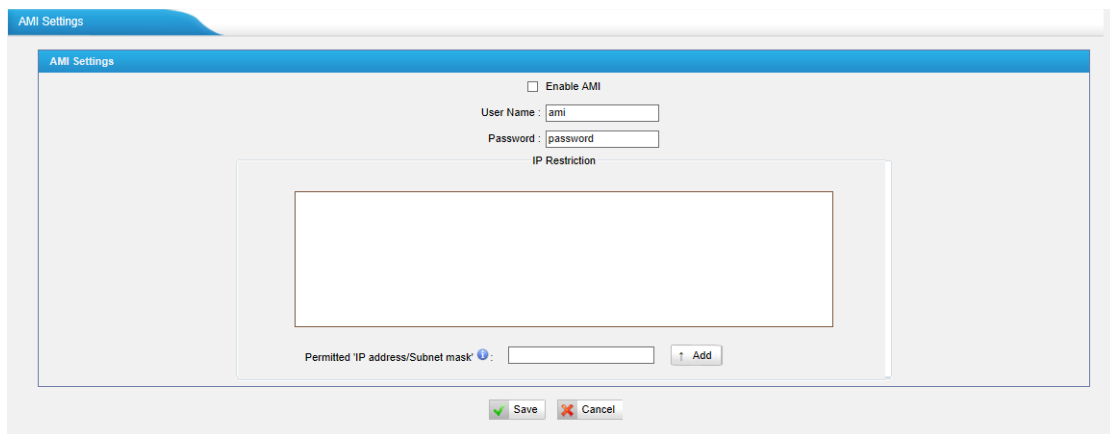


Figure 5-15 AMI Settings

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

IP Restriction: you can set which IP can log in MyPBX AMI interface

5.2.5 Database Grant

SOHO are using MySQL database from 14.18.0.22. The 3rd party software can access MySQL via internet. Before that, you need to grant the authority to the database user.

After entering "Database Grant" page, clicking "Add", you can add a database user, set user password and grant authority.

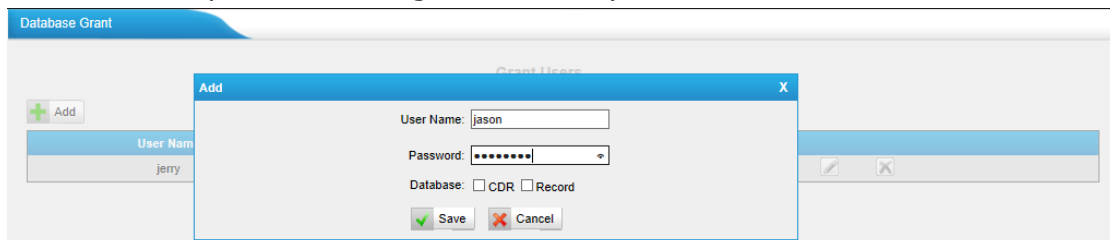


Figure 5-16 Database Grant

Username/password: The 3rd party can use this username and password to access the MySQL.

Database: there are 2 options, CDR and Record. If you choose CDR, then this user has authority to check CDR database; if you choose Record, then the user has authority to check which call has been recorded automatically.

5.2.6 Alert Settings

If the device is attacked, the system will notify users the alert via call or E-mail. The attack modes include IP attack and Web Login.

For more details on the system security configuration, please refer to

[APPENDIX H MyPBX Security Configuration Guide.](#)

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

Figure 5-17 Alert Settings

1. IPATTACK

When the system is attacked by IP address, the firewall will add the IP to auto IP Blacklist and notify the user if it match the protection rule.

1) Phone Notification Settings

•PHONE Notification

Whether enable phone notification.

•Number

The numbers could be set for alert notification; users can setup multiple extension and outbound phone numbers. Please separate them by “;”.

Example: “500;9911”, if the extension has configured Follow Me Settings, the call would go to the forwarded number directly.

•Attempts

The attempts to dial a phone number when there is no answer.

•Interval

The interval between each attempt to dial the phone number. Must be greater than 3 seconds, the default value is 10 seconds.

•Prompt

Users will hear the prompt while receiving the phone notification.

2) E-mail Notification Settings

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

•E-mail Notification

Whether to enable E-mail Notification or not

•Recipient's Name

The recipients for the alert notification, and multiple email addresses are allowed, please separate them by ";".

Example: jerry@yeastar.com; jason@yeastar.com, 456@sina.com .

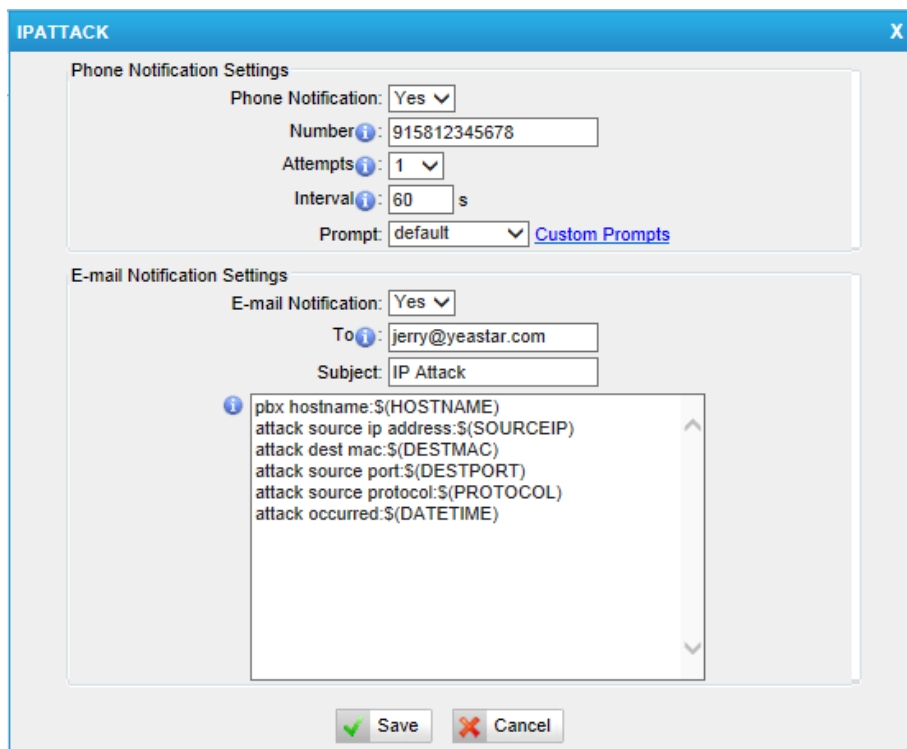
•Subject

The subject of the alert email.

•Email Content

Text content supports predefined variables. Variable names and corresponding instructions are as follows:

\$(HOSTNAME)	Host name
\$(LOCALIP)	Local IP address
\$(SOURCEIP)	Attack source IP address
\$(DATETIME)	Occurred
\$(USERNAME)	User name (WEBLOGIN effective)
\$(DESTMAC)	Attacks destination MAC (IPATTACK effective)
\$(DESTPORT)	Attacks destination Port number (IPATTACK effective)
\$(PROTOCOL)	Protocol type (IPATTACK effective)
\$(INTERFACE)	Network interface name (IPATTACK effective)



IPATTACK

Phone Notification Settings

Phone Notification: Yes

Number: 915812345678

Attempts: 1

Interval: 60 s

Prompt: default [Custom Prompts](#)

E-mail Notification Settings

E-mail Notification: Yes

To: jerry@yeastar.com

Subject: IP Attack

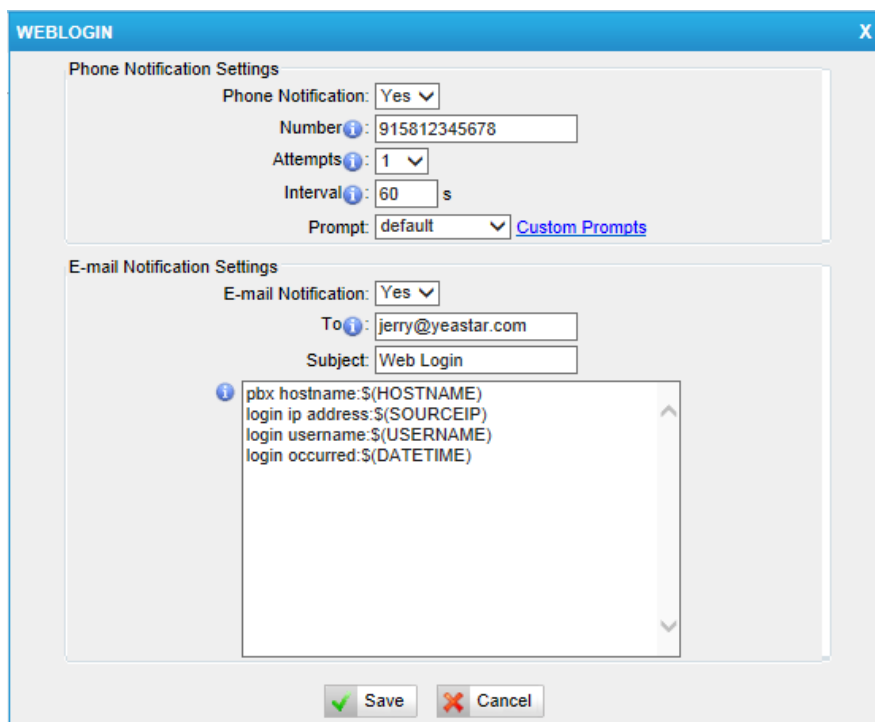
pbx hostname:\$(HOSTNAME)
 attack source ip address:\$(SOURCEIP)
 attack dest mac:\$(DESTMAC)
 attack source port:\$(DESTPORT)
 attack source protocol:\$(PROTOCOL)
 attack occurred:\$(DATETIME)

Save Cancel

Figure 5-18 IP Attack Configuration

2. WEBLOGIN

Web Login Alert Notification: Enter the password incorrectly five times to login MyPBX Web interface will be considered as an attack, the system will limit the IP login within 10 minutes and notify the user.



WEBLOGIN

Phone Notification Settings

Phone Notification: Yes

Number: 915812345678

Attempts: 1

Interval: 60 s

Prompt: default [Custom Prompts](#)

E-mail Notification Settings

E-mail Notification: Yes

To: jerry@yeastar.com

Subject: Web Login

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

Save Cancel

Figure 5-19 Web Login Alert Setting

5.3 LDAP Server

5.3.1 LDAP Server

LDAP is used as a phone book on MyPBX so that you can search a key word from your IP phone. The key word can be a name, a mobile number, an email or other key words in the phonebook.

Note:

It requires that the IP phone should support LDAP feature.

1) LDAP Settings

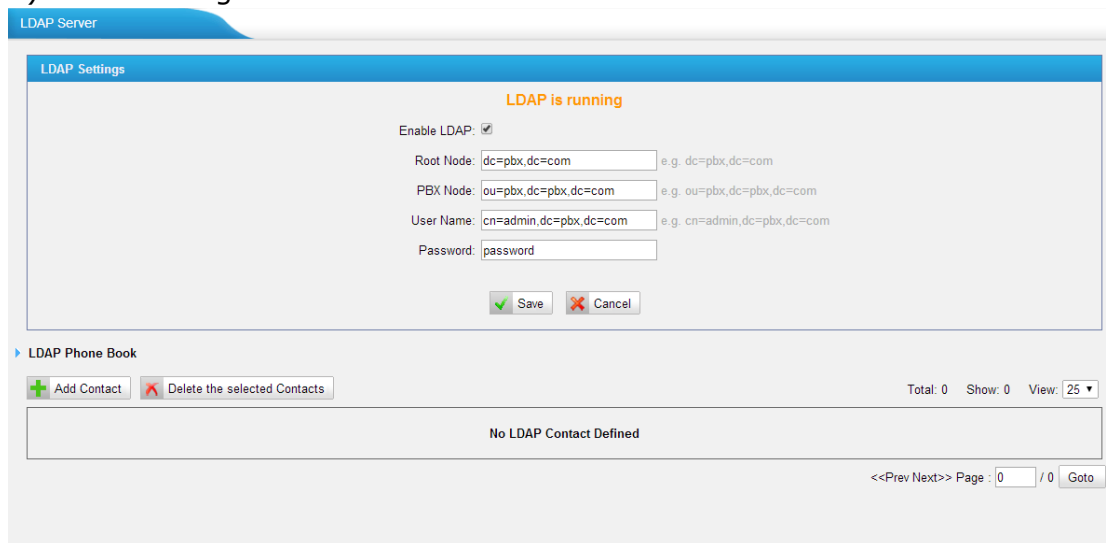


Figure 5-20 LDAP Server page

•Enable LDAP

Enable LDAP to use LDAP on your IP phone.

•Root Node

A root node for this LDAP, e.g. dc=pbx, dc=com.

•PBX Node

A pbx node for this LDAP, e.g. ou=pbx, dc=pbx, dc=com.

•User Name

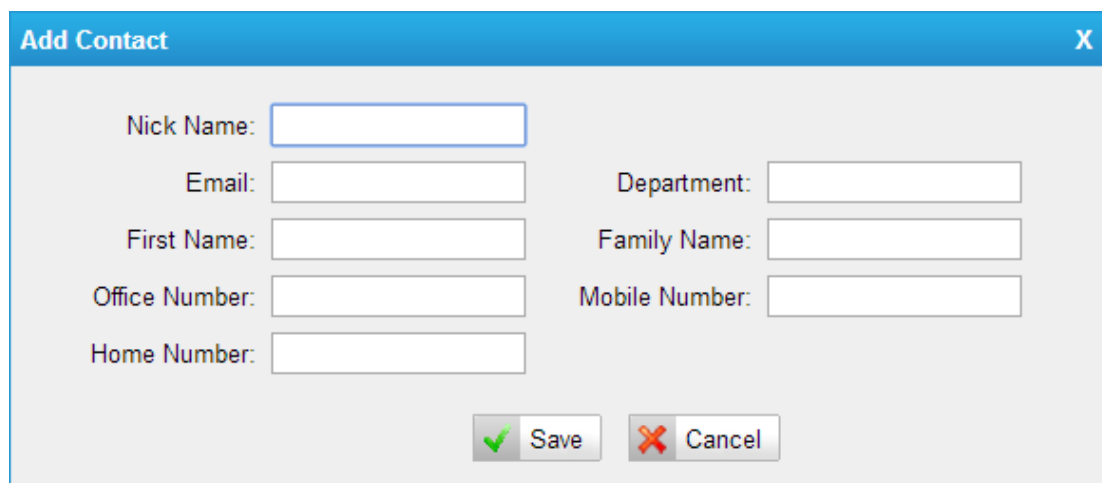
A user for this LDAP, e.g. cn=admin, dc=pbx, dc=com

•Password

A password used to access LDAP.

2) Add Contact

In Add Contact you can create them as required.



The image shows a 'Add Contact' dialog box with a blue header bar containing the title 'Add Contact' and a close button 'X'. The main area is light gray and contains several text input fields arranged in two columns. The left column includes 'Nick Name:', 'Email:', 'First Name:', 'Office Number:', and 'Home Number:'. The right column includes 'Department:', 'Family Name:', and 'Mobile Number:'. At the bottom center, there are two buttons: a green checkmark icon followed by 'Save', and a red 'X' icon followed by 'Cancel'.

Figure 5-21 Add Contact

If you want to know how to use LDAP, please refer to [***Appendix J***](#)

5.4 Storage Management

5.4.1 External Storage

The External Storage feature is used to extend storage space. Once configured, the files (voicemail, call recording files) created before the configured days will be moved to the Net-Disk.

Note: The shared folder must be based on Windows Operation System. And if it's windows Vista/2008/7, please add "Everyone" into the shared account list.

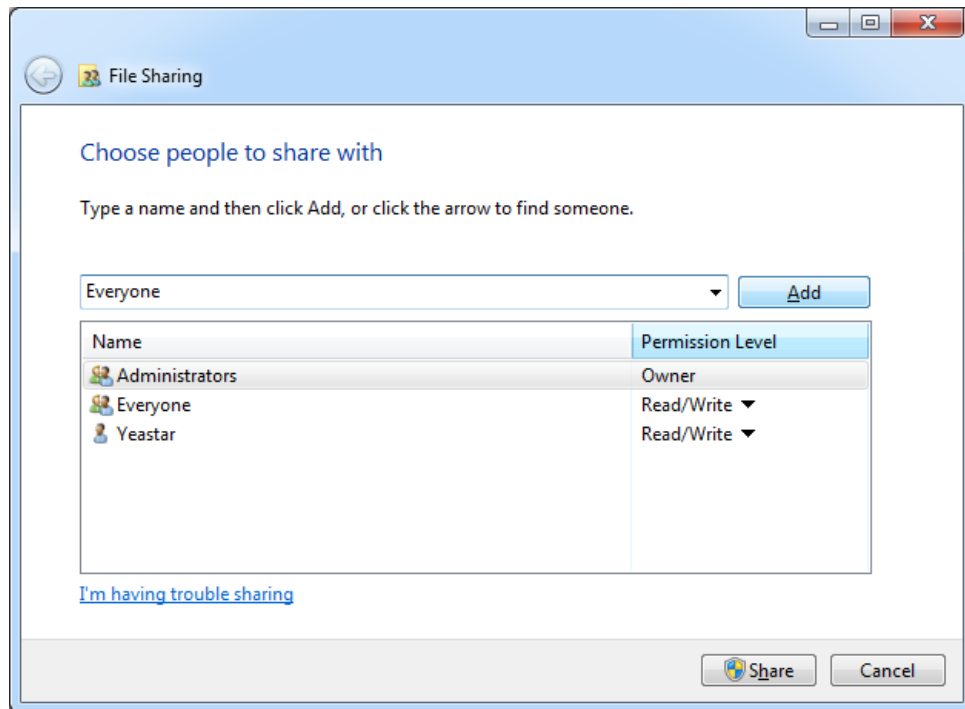


Figure 5-22

Before external storage can be properly configured, an SMB share folder accessible from MyPBX must be set up on a Windows based machine. Once that has been set up, please follow the steps below.

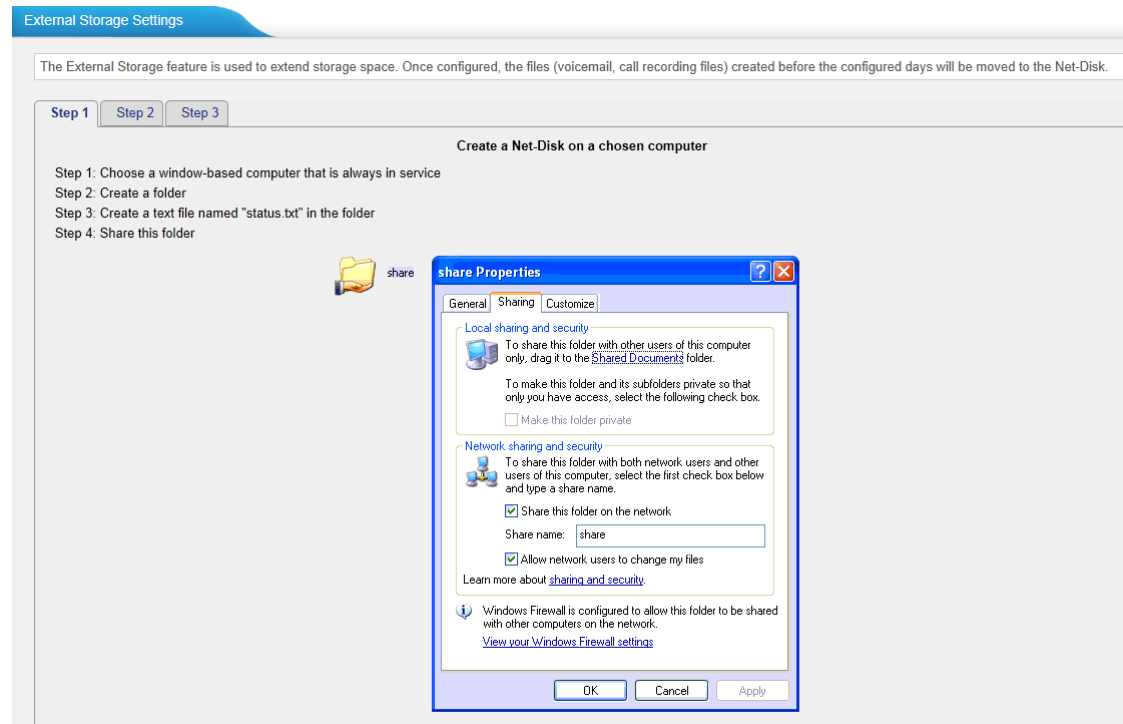


Figure 5-23

Step 1: Choose a window-based computer that is always in service

Step 2: Create a folder

Step 3: Create a text file named "status.txt" in the folder

Step 4: Share this folder

Then we need input the Net-Disk information in step2 page.

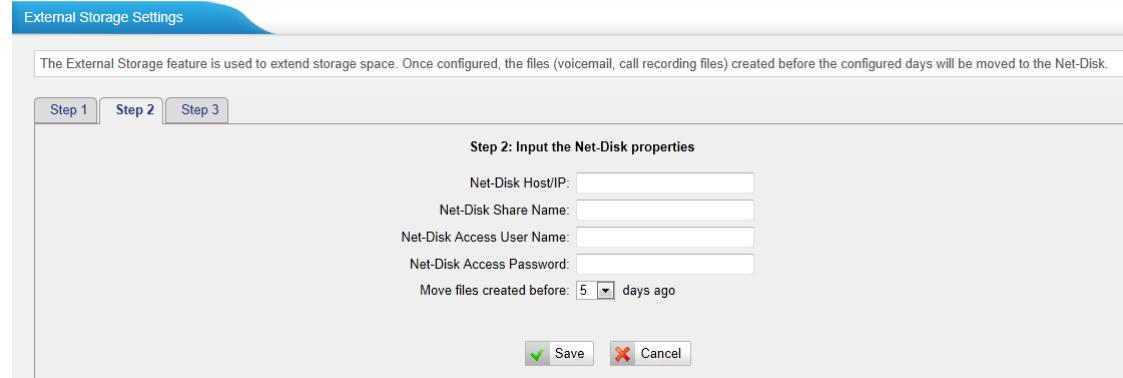


Figure 5-24

Net-Disk Host/IP: Change this to the IP address of the computer where backup files will be stored.

Net-Disk Share Name: Change this to the name of the shared folder where backups will be stored.

Net-Disk Share Username: The user name used to log into the network share. Leave this blank if it is not required

Net-Disk Share Password: The password used to log into the network share. Leave this blank if it is not required

If the configuration is correct, open the Windows share folder you will see the MyPBX backup files and folders has been created. If the contents of the backup folder look similar to step3 page, then you have successfully configured external storage on the MyPBX unit.

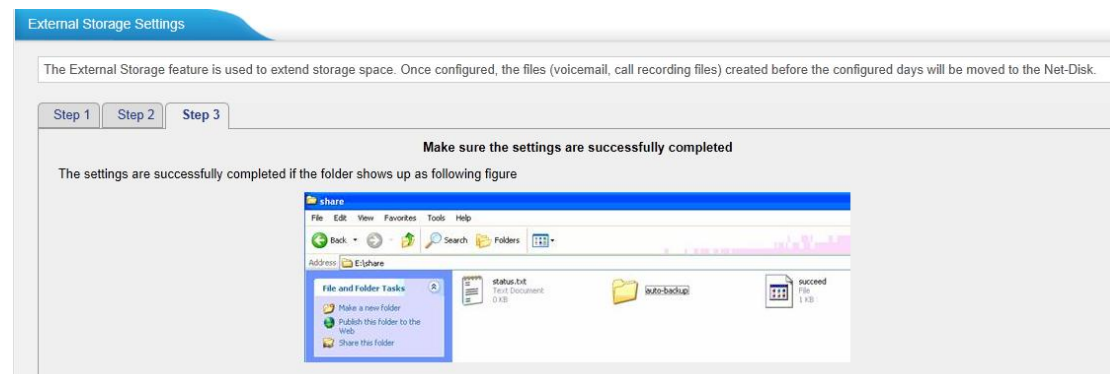


Figure 5-25

5.5 System Preferences

In this page, we can set other system preferences, like the password for admin account, system date and time, firmware update, hot standby, backup and restore, reset and reboot.

5.5.1 Password Settings

MyPBX has 3 accounts: admin, user, and cdr. User and cdr account is disabled by default.

Admin account:

The default password for account "admin" is "password". To change the password, select "admin" in "User", enter the old password and new password, and click "Save". The system will then prompt you to re-login using your new password.

After you enter the new password, MyPBX will prompt the password strength. It is recommended that you use numbers, upper-case letters, and lower-case letters to increase the security.

When you log in MyPBX using "admin" account, you can enable "user" and "cdr" account; also, you can change their passwords.

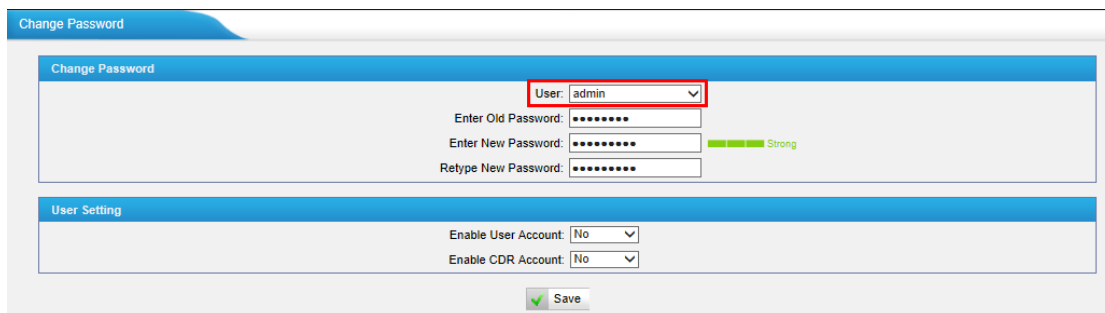
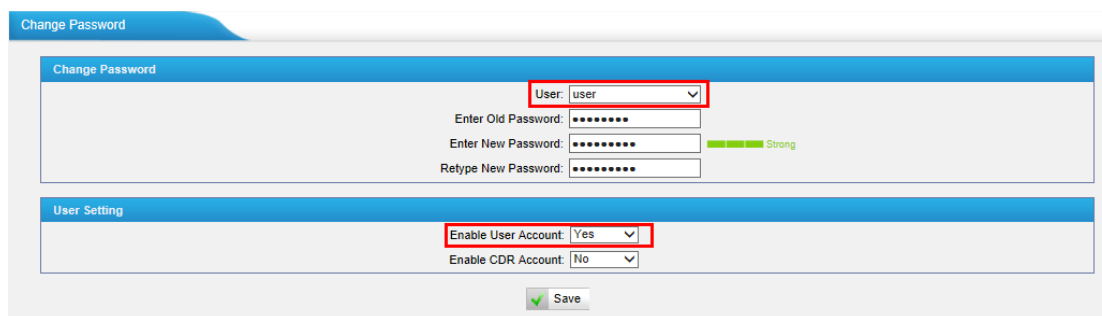


Figure 5-26

User account:

User account is disabled by default and its default password is "password". When enabling "user" account for the first time, MyPBX will ask you to change "user" password. If you don't change it, you can't enable "user" account. To change the password, select "user" in "User", enter the old password and new password, and click "Save". The system will then prompt you to re-login using your new password.

After you enter the new password, MyPBX will prompt the password strength. It is recommended that you use numbers, upper-case letters, and lower-case letters to increase the security.



The screenshot shows the 'Change Password' page in the MyPBX administrator interface. The 'User' dropdown menu is set to 'user'. Below it, there are three password input fields: 'Enter Old Password', 'Enter New Password', and 'Retype New Password'. A green strength indicator shows 'Strong'. In the 'User Setting' section below, the 'Enable User Account' dropdown is set to 'Yes', and the 'Enable CDR Account' dropdown is set to 'No'. A 'Save' button is at the bottom.

Figure 5-27

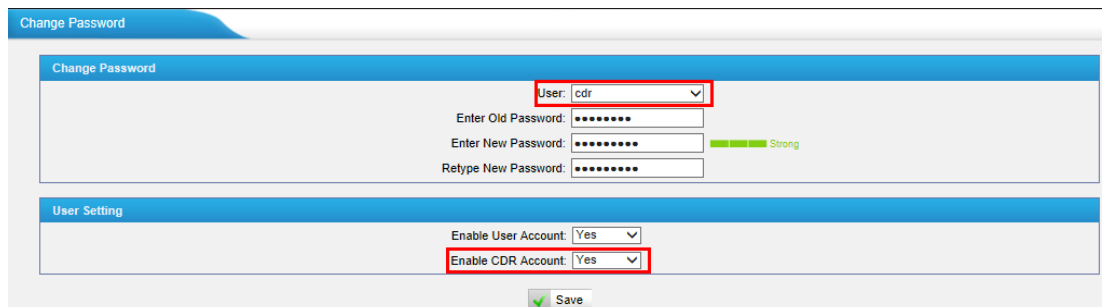
After enabling "user" account, you can log in MyPBX using "user". "user" account can change its own password.

CDR account:

"cdr" account is disabled by default and its default password is "password". You can enable it after you log in MyPBX using "admin" account.

To change the password, select "cdr" in "User", enter the old password and new password, and click "Save". The system will then prompt you to re-login using your new password.

After you enter the new password, MyPBX will prompt the password strength. It is recommended that you use numbers, upper-case letters, and lower-case letters to increase the security.



The screenshot shows the 'Change Password' page in the MyPBX administrator interface. The 'User' dropdown menu is set to 'cdr'. Below it, there are three password input fields: 'Enter Old Password', 'Enter New Password', and 'Retype New Password'. A green strength indicator shows 'Strong'. In the 'User Setting' section below, the 'Enable User Account' dropdown is set to 'Yes', and the 'Enable CDR Account' dropdown is set to 'Yes'. A 'Save' button is at the bottom.

Figure 5-28

After enabling "cdr" account, you can log in MyPBX using "cdr". "cdr" account can change its own password.

5.5.2 Date and Time

Set the date and time for MyPBX.

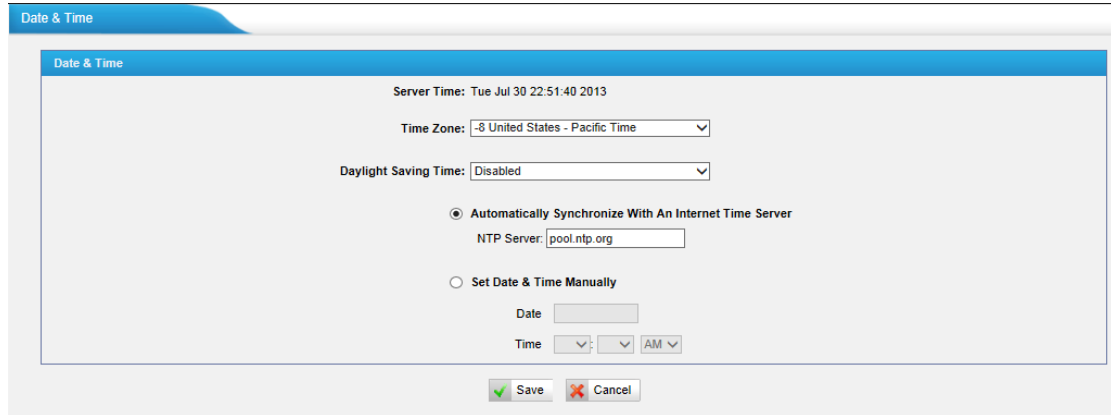


Figure 5-29

•Time Zone

You can choose your time zone here.

•Daylight Saving Time

Set the mode to Automatic or disabled

•Automatically Synchronize With an Internet Time Server

Input the NTP server so that MyPBX will update the time automatically

•Set Date & Time Manually

You can set the time to your local right time manually here

5.5.3 Firmware Update

Upgrading of the firmware is possible through the Administrator web interface using a TFTP Server or an HTTP URL.

Enter your TFTP Server IP address and firmware file name, then click start to update the firmware

Notes:

1. If "Reset configuration to Factory Defaults" is enabled, the system will restore to factory default settings.
2. When updating the firmware, please don't turn off the power. Or the system will get damaged.
3. For more information on the steps of updating the firmware, please refer to this link:

http://www.yeastar.com/download/MyPBX-SOHO/MyPBX_SOHO_FirmwareUpg

rade_en.pdf

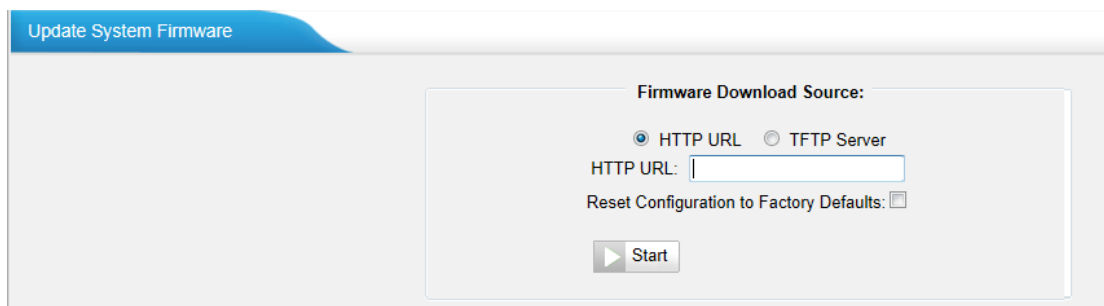


Figure 5-30

5.5.4 Backup and Restore

We can back up the configurations before resetting MyPBX SOHO to factory defaults, and then restore it using this package. The backup created on MyPBX is encrypted with file format ".bak".

Notes:

1. Only configurations, custom prompts will be backed up, the voicemail and recording files are not included.
2. When you have updated the firmware version, it's not recommended to restore using old package.

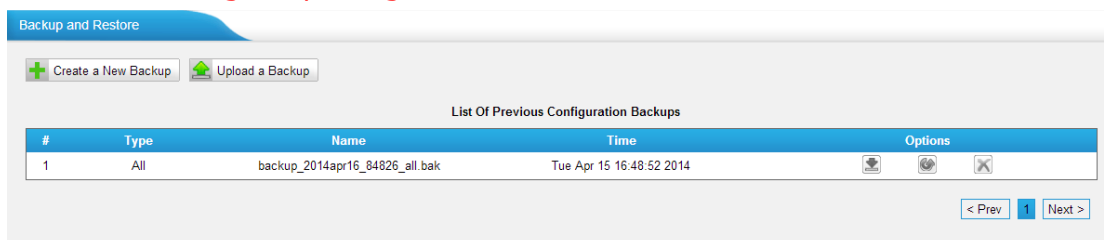


Figure 5-31

-Create a New Backup

Users are able to create a new backup for "All" or for separate backup extensions.

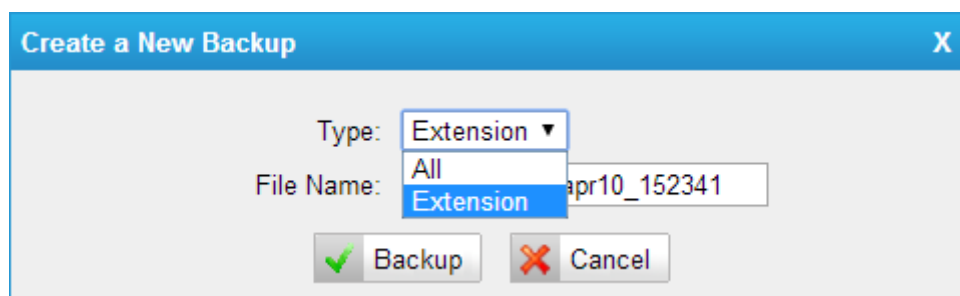


Figure 5-32

•Upload a Backup

Users are able to upload backup for "All" or for separate extensions.

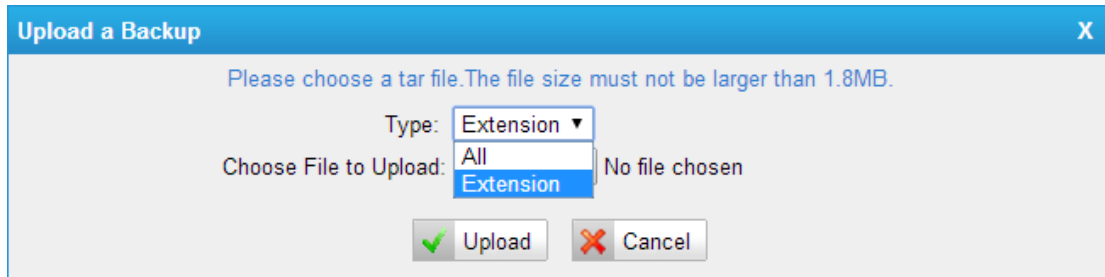


Figure 5-33

5.5.5 Reset and Reboot

We can reset or reboot MyPBX SOHO via web directly in this page.

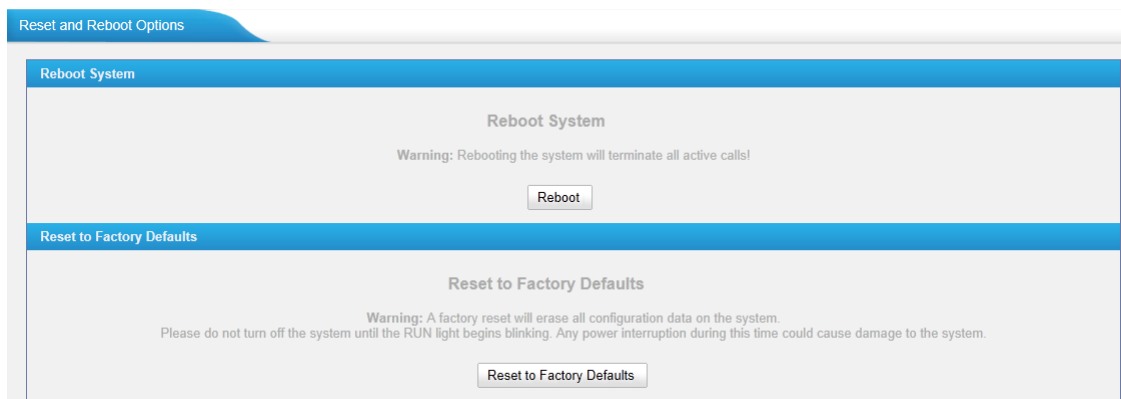


Figure 5-34

•Reboot System

Warning: Rebooting the system will terminate all active calls!

•Reset to Factory Defaults

Warning: A factory reset will erase all configuration data on the system. Please do not turn off the system until the RUN light begins blinking. Any power interruption during this time could cause damage to the system.

6. PBX



Click  to access "PBX" tab.

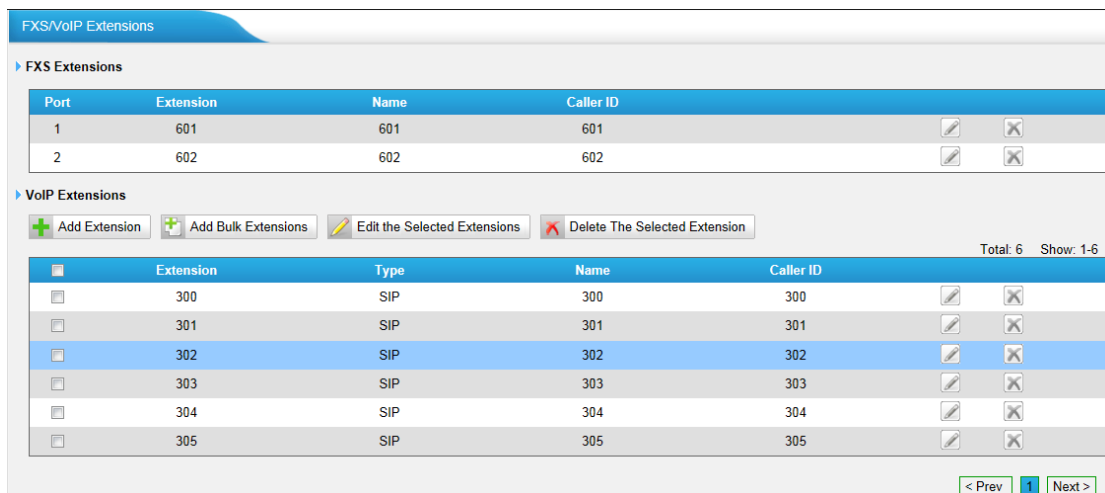
In this page, we can configure the settings of extension, trunk, inbound call control, outbound call control, audio settings and the others. After configuration, we can make or receive calls as expected.

6.1 Extensions

In this page, we can configure the extensions' details and provision the supported models automatically.

6.1.1 FXS/VoIP Extensions

There are three types of extensions supported in MyPBX SOHO V5: SIP, IAX and analog extension.



FXS/VoIP Extensions

▶ **FXS Extensions**

Port	Extension	Name	Caller ID		
1	601	601	601		
2	602	602	602		

▶ **VoIP Extensions**

 Add Extension
  Add Bulk Extensions
  Edit the Selected Extensions
  Delete The Selected Extension

Total: 6 Show: 1-6

	Extension	Type	Name	Caller ID		
☐	300	SIP	300	300		
☐	301	SIP	301	301		
☒	302	SIP	302	302		
☐	303	SIP	303	303		
☐	304	SIP	304	304		
☐	305	SIP	305	305		

< Prev 1 Next >

Figure 6-1

FXS Extensions

FXS Extensions

Port	Extension	Name	Caller ID		
1	601	601	601		
2	602	602	602		

Figure 6-2 FXS

There are two analog extensions in MyPBX SOHO V5 if S2 module is installed, to modify the extension number, please delete it first, and then recreate it again.

1) General

Edit Extension - 601

General
Other Settings

General

Extension: 601
Port: 3
Name: 601
Caller ID: 601

Voicemail

☒ Enable Voicemail
Voicemail Access PIN #: 601

Mail Setting

☐ Enable Send Voicemail
Email Address:

Note: Please ensure that the section 'SMTP Settings for Voicemail'(in the 'Voicemail Settings') have been properly configured before using this feature.

Flash

Hook Flash Detection: 1000 ms

Group

Pickup Group:

Call Duration Setting

Max Call Duration: s

Save
Cancel

Figure 6-3

•Extension

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

•Port

The extension correspond port.

•Name

A character-based name for this user, e.g. "Bob Jones".

•Caller ID

The Caller ID (CID) string will be used when this user calls another internal user.

2) Voicemail

•Enable Voicemail

Check this box if the user should have a voicemail account.

•Voicemail Access PIN #

Voicemail Password for this extension, e.g. "1234".

3) Mail Setting

•Enable Send Voicemail

Once enabled, the voicemail will be sent to the email address below as an attachment.

•Send Voicemail to Email Address

This option defines whether or not voicemails/Fax is sent to the Email address as an attachment.

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

4) Flash

•Hook Flash Detection

Sets the amount of time, in milliseconds, that must pass since the last hook-flash event received by MyPBX before it will recognize a second event. If a second event occurs in less time than defined by Hook Flash Detection, then MyPBX will ignore the event. The default value of Flash is 1000ms, and it can be configured in 1ms increments.

5) Group

•Pickup Group

If this extension belongs to a pickup group, any calls that ring this extension can be picked up by other extensions in the same pickup group by dialing the Call Pickup feature code (the default is *4).

Note: *4 is the default setting, it can be changed under Feature Codes -> General -> Call Pickup.

6) Call Duration Settings

Setup the max cull duration for every call of this extension, but it's only valid for outbound calls. Enter "0" or leave this blank empty, the value would be equal to the max call duration configured in the Option Settings page.

Note: this setting will not be valid for internal calls.

Other Settings

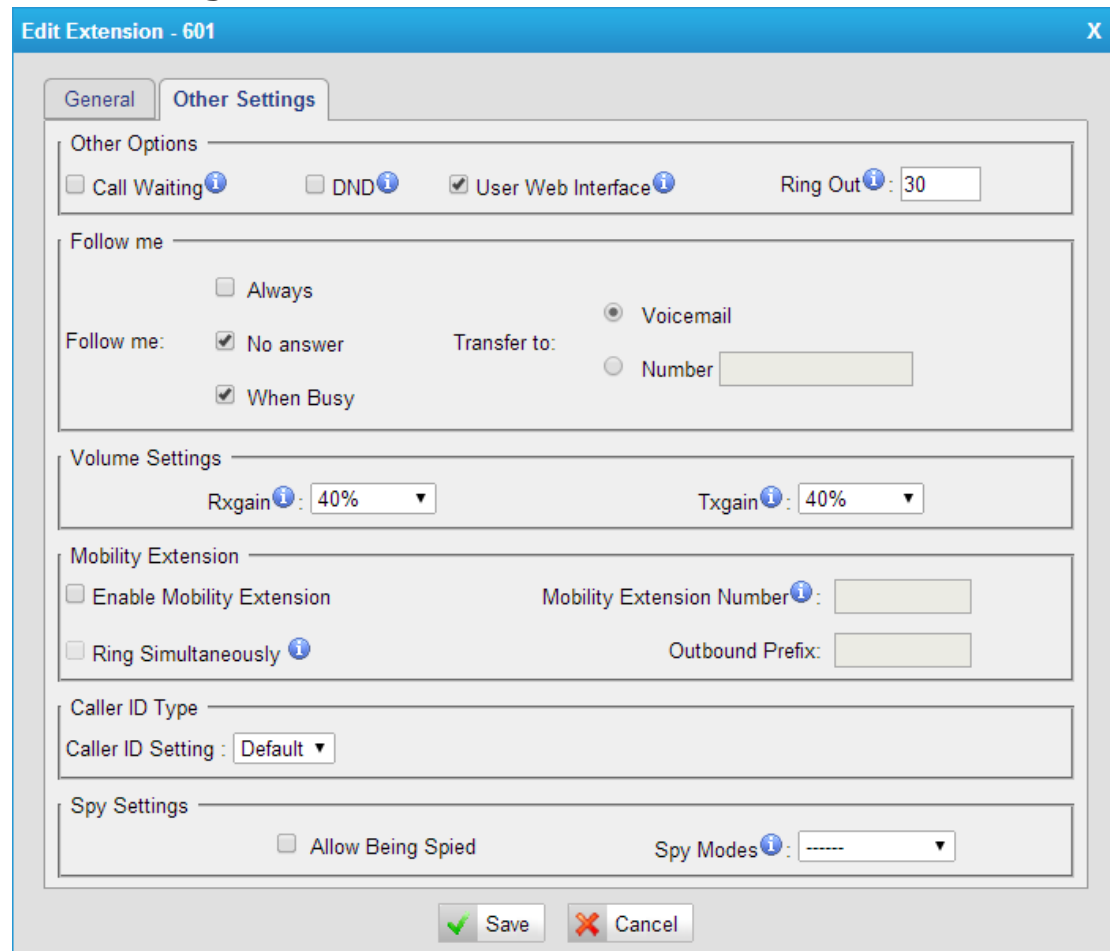


Figure 6-4

7) Other options

•Call Waiting

Check this option if the extension should have Call Waiting capability. If this option is checked, the "When busy" follow me options will not be available.

•DND

Don't Disturb.

•User Web Interface

Check this option to allow the user to log in to the MyPBX User Web interface, which can be used to access voicemail and extension recordings. Users may log in the MyPBX User Web interface by using their extension number and voicemail PIN as the user name and password respectively.

•Ring Out

Check this option if you want to custom the ring time. Tone will stop over the time defined.

8) Follow me (Call Forwarding)

This function sets inbound call forwarding on an extension. An administrator can configure Follow Me for this extension.

9) Volume Settings

Rxgain: The Volume sent to FXS extension.

Txgain: The Volume sent out by the FXS extension

10) Mobility Extension

MyPBX allows you to use your mobile phone as an extension. If you set your mobile phone as a mobility extension and then you call MyPBX with this mobile phone, you will hear a dial tone. MyPBX will recognize your call as a call from an extension. You can dial the number of other extensions (your caller ID will be the number of your extension) or dial out via outbound routes just like dialing from your extension.

Note: If callback is enabled in the inbound route, the mobility extension function of this inbound route will be disabled.

Enable Mobility Extension

Enable this feature.

•Mobility Extension Number

When you dial the server with this number, the mobile phone gets the permission of the extension. For example: dialing the other extensions, playing the voicemail.

•Ring Simultaneously

When the extension has an incoming call, it rings its mobility extension simultaneously.

•Outbound Prefix

Fill in proper prefix of mobile number so that it can match an outbound route to dial the mobility extension. For example, if you set the prefix 9, it will send "9+ mobility extension number" to the outbound route.

11) Call ID type

•Call ID Setting

Normally, you choose the "default" option except for using MyPBX in Japan, in

which case you should choose "Japan".

12) Spy Settings

MyPBX allows extension to monitor/barge in other conversation. Once this feature is enabled, the extension has the ability to monitor/barge in other calls using the feature codes for each spy mode. Refer to "Feature Codes" section for more information.

•spy modes

There are 4 spy modes available:

General spy: you have the permission to use the following 3 modes.

Normal spy: you can only hear the call, but can't talk.

Whisper spy: you can hear the call, and can talk with the monitored extension.

Barge spy: you can hear the call and talk with them both.

Note: for example, if 500 want to monitor extension 501, we need to enable the "allow being spied" for 501, and choose the spy mode for extension 500. Then pick up 500 and dial "feature codes + 501" to start monitoring when 501 is in a call

If 500 choose "normal spy", it should dial "*90501" to start monitoring.

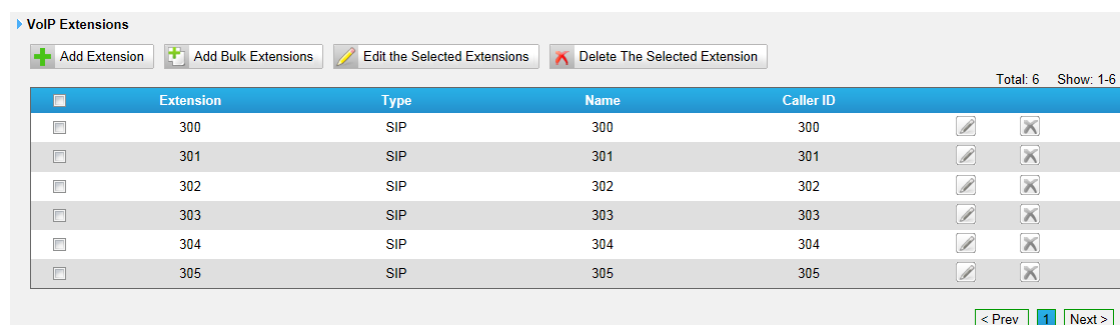
If 500 choose "whisper spy", it should dial "*91501" to start monitoring.

If 500 choose "barge spy", it should dial "*92501" to start monitoring.

If 500 choose "general spy", it can dial "*90501", "*91501" or "*92501" to start monitoring.

VoIP Extensions

A VoIP extension is a SIP/IAX Account that allows an IP Phone or an IP soft phone client to register on MyPBX.



Extension	Type	Name	Caller ID
300	SIP	300	300
301	SIP	301	301
302	SIP	302	302
303	SIP	303	303
304	SIP	304	304
305	SIP	305	305

Figure 6-5

We can click "Add extension" to start.

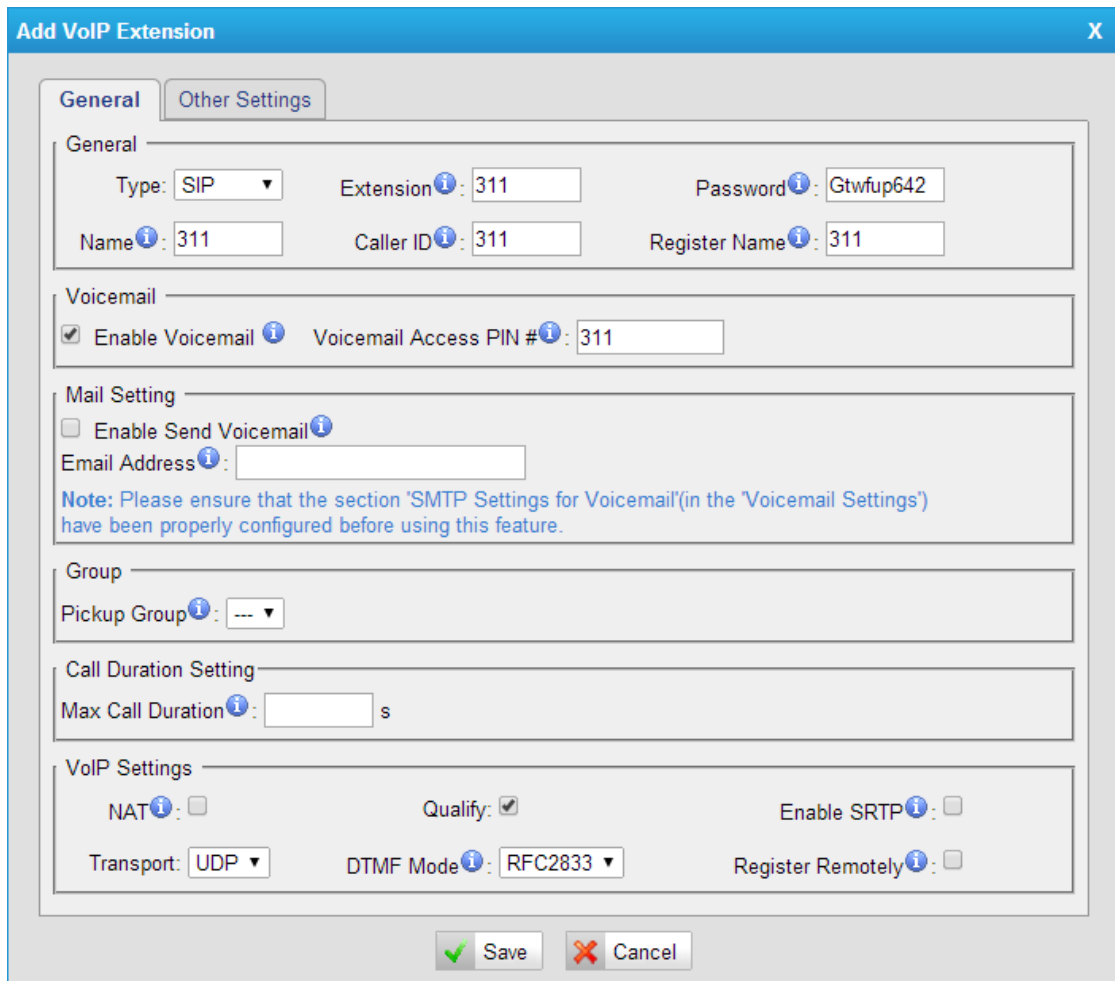


Figure 6-6

1) General

•Type

Extension type: SIP, IAX or SIP/IAX.

SIP—The extension sends and receives calls using the VoIP protocol SIP.

IAX—The extension sends and receives calls using the VoIP protocol IAX.

•Extension

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

•Password

The password for this extension, but it is not a fixed one. When you add new extension, a random and robust password will be generated like "Gtwfup642".

•Name

A character-based name for this user, e.g. "Bob Jones".

•Caller ID

The Caller ID will be used when this user calls another internal extension.

•Register Name

It is for extension registration validation. Users will not be able register the extension if the authorization name is incorrect even though the username and password are correct.

2) Voicemail

•Enable Voicemail

Check this box if the user should have a voicemail account.

•Voicemail Access PIN

The voicemail password for this extension, e.g. "1234".

3) Mail Setting

This option defines whether or not voicemails or faxes are sent to an Email Address as an attachment.

•Enable Send Voicemail

Once enabled, the voicemail will be sent to email as an attachment.

•Email Address

Email address used to receive the voicemail or Fax.

Note: Please ensure that the section "SMTP Settings For Voicemail" (in the "Voicemail Settings") has been properly configured before using this feature.

4) Group

•Pickup Group

If this extension belongs to a pickup group, any calls that ring this extension can be picked up by other extensions in the same pickup group by dialing the Call Pickup feature code (the default is *4).

Note: *4 is the default setting, it can be changed under Feature Codes -> General -> Call Pickup.

5) Call Duration Settings

Set up the max call duration for every call of this extension, but it's only valid for outbound calls. Enter "0" or leave this blank empty, the value would be equal to the max call duration configured in the Option Settings page.

Note: This setting will not be valid for internal calls.

6) VoIP Settings

•NAT

This setting should be used when the system is using a public IP address to communicate 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.

•Qualify

Send check alive packets to IP phones.

•Enable SRTP

Enable extension for SRTP (RTP Encryption).

•Transport

This will be the transport method used by the extension. The options are UDP (default) or TCP or TLS.

•DTMF Mode—RFC2833, Info, Inband, Auto.

•Remote Register

Allow to register remote extensions.

If you enable "Remote Register", the extension password must include uppercase letters, lowercase letters, and digits.

This option is used to enhance the system security, it's disabled by default.

More details for the system security configuration, please refer to [APPENDIX H MyPBX Security Configuration Guide](#)

Other Options

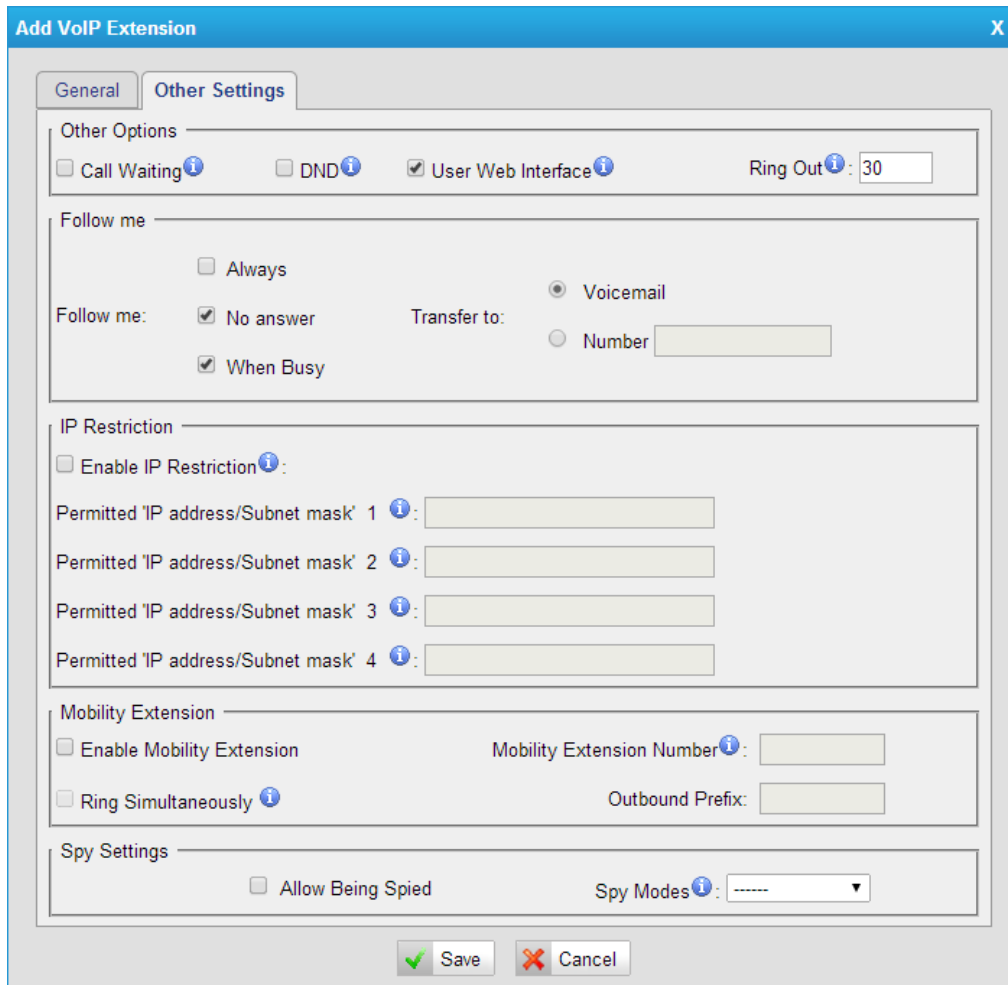


Figure 6-7

7) Other Options

.Call Waiting

Check this option if the extension should have Call Waiting capability. If this option is checked, the "When busy" follow me options will not be available. The call waiting function of IP phone has higher priority than MyPBX's call waiting function.

.DND

Don Not Disturb. When DND is enabled for an extension, the extension will not be available.

.User Web Interface

Check this option to allow the user to login to the MyPBX User Web interface, which can be used to check voicemail and extension recordings. Users may log in MyPBX User Web interface by using their extension number and voicemail PIN as the user name and password respectively.

.Ring Out

Check this option if you want to customize the ring time. Ring tone will stop over the time defined.

8) Follow me (Call Forwarding)

Call forwarding for an extension can be configured here. The administrator can configure Follow Me option for this extension. If you want to transfer the call to an outbound number, please follow the dial pattern of outbound route filled in the outbound number.

For example: forwarding a call to your mobile phone number 123456789, and the dial pattern of outbound route is "9.", you should fill in 9123456789 here.

9) IP Restriction

•Enable IP Restriction

Check this option to enhance the VoIP security for MyPBX. If this option is enabled, only the permitted IP/Subnet mask will be able to register this extension number. In this way, the VoIP security will be enhanced.

For more details on the system security configuration, please refer to

[APPENDIX H MyPBX Security Configuration Guide](#).

•Permitted "IP address/Subnet mask"

The input format should be "IP address" + "/" + "Subnet mask".

E.g. "192.168.5.100/255.255.255.255" means only the device whose IP address is 192.168.5.100 is allowed to register this extension number.

E.g. "192.168.5.0/255.255.255.0" means only the device whose IP address is 192.168.5.XXX is allowed to register this extension number.

10) Mobility Extension

MyPBX allows you to use your mobile phone as an extension. If you set your mobile phone as a mobility extension and then you call MyPBX with this mobile phone, you will hear a dial tone. MyPBX will recognize your call as a call from an extension. You can dial the number of other extensions (your caller ID will be the number of your extension) or dial out via outbound routes just like dialing from your extension.

Note: If callback is enabled in the inbound route, the mobility extension function of this inbound route will be disabled.

•Enable Mobility Extension

Enable this feature.

•Mobility Extension Number

When you dial the server with this number, the mobile phone gets the permission of the extension. For example: dialing the other extension, playing the voicemail.

•Ring Simultaneously

When the extension has an incoming call, it rings mobile simultaneously.

•Outbound Prefix

Fill in proper prefix of mobile number so that it can match an outbound route to dial the mobility extension. For example, if you set the prefix 9, it will send "9+ mobility extension number" to the outbound route.

11) Spy Settings

MyPBX allows extension to monitor/barge in other conversation. Once this feature is enabled, the extension has the ability to monitor/barge in other calls using the feature codes for each spy mode. Refer to "Feature Codes" section for more information.

•spy modes

There are 4 spy modes available:

General spy: you have the permission to use the following 3 modes.

Normal spy: you can only hear the call, but can't talk.

Whisper spy: you can hear the call, and can talk with the monitored extension.

Barge spy: you can hear the call and talk with them both.

Note: for example, if 500 want to monitor extension 501, we need to enable the "allow being spied" for 501, and choose the spy mode for extension 500. Then pick up 500 and dial "feature codes + 501" to start monitoring when 501 is in a call.

If 500 choose "normal spy", it should dial "*90501" to start monitoring.

If 500 choose "whisper spy", it should dial "*91501" to start monitoring.

If 500 choose "barge spy", it should dial "*92501" to start monitoring.

If 500 choose "general spy", it can dial "*90501", "*91501" or "*92501" to start monitoring.

6.1.2 Phone Provisioning

The Auto Provision sub menu provides users a method to Auto Provision IP Phone after the Express Setup process.

Note: Auto Provision functions fully test with these models:

Yealink (T12, T18, T19, T20, T21, T22, T26, T28, T32, T38, T41, T42, T46, W52P, VP530, VP-2009)

Snom (300, 320, 360, 370)

Polycom (IP 6000, IP 7000, IP 32X, IP33X, IP430, IP450, IP550, IP560, VVX1500)

Cisco (IP7940, IP7960)

Aastra (9480i, 9480i-CT, 6730i, 6731i, 6737i, 6753i, 6755i, 6757i, 6757i CT)

GrandStream (GXP1450, GXP2100, GXP2110, GXP2120)

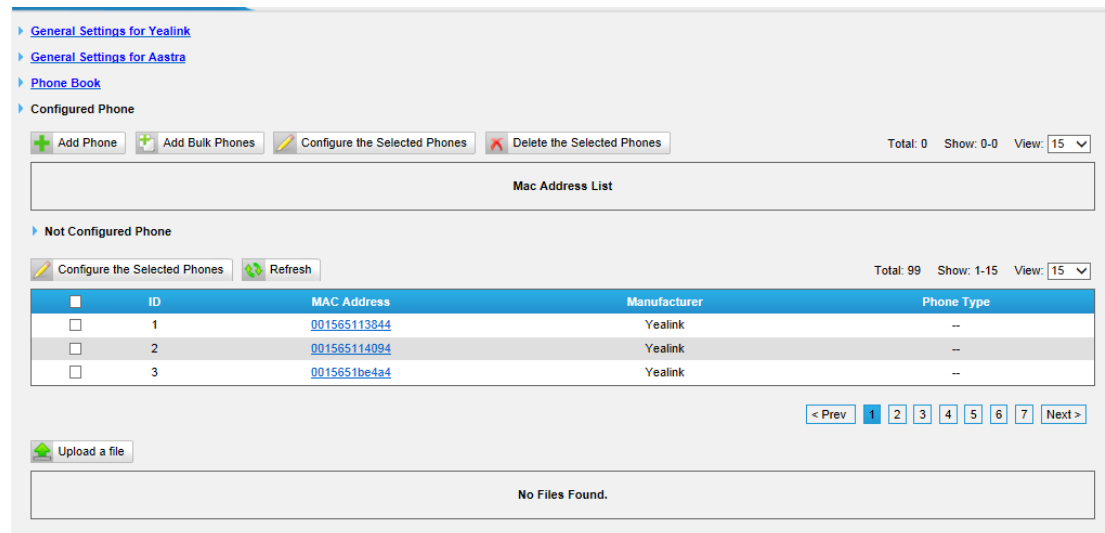
Escene (ES220, ES320, ES330, ES410, ES620)

Fanvil (C56, C58, C60, C62)

Panasonic (UT113, UT123, UT133, UT136, UT248, UT670, TGP500, TGP550)

News:

When provisioning Yealink, Grandstream, Fanvil, Snom IP phone, MyPBX is not needed to be set as the only DHCP server any more.



General Settings for Yealink

General Settings for Aastra

Phone Book

Configured Phone

Add Phone Add Bulk Phones Configure the Selected Phones Delete the Selected Phones Total: 0 Show: 0-0 View: 15

Mac Address List

Not Configured Phone

Configure the Selected Phones Refresh Total: 99 Show: 1-15 View: 15

ID	MAC Address	Manufacturer	Phone Type
1	001585113844	Yealink	--
2	001585114094	Yealink	--
3	0015851be4a4	Yealink	--

< Prev 1 2 3 4 5 6 7 Next >

Upload a file

No Files Found.

Figure 6-8

6.1.2.1 General Settings for Yealink

In this page, you can configure the general settings before provisioning Yealink IP phones, including the items like general preferences, codecs, remote phone book and firmware upgrade.

Note: if firmware download server is enabled, IP phone will update the firmware automatically according to the version and server you have configured during the provision process.

General Settings for Yealink

[Go Back to Phone Provisioning](#)

General Preferences | Codecs | Remote Phone Book | Firmware Download Server

Language: English

Web server Type: HTTP&HTTPS

Admin Password: ☒ Fixed ☐ Prefix

admin

Time Zone: +8 China(Beijing)

Primary NTP Server: cn.pool.ntp.org

Secondary NTP Server: cn.pool.ntp.org

Daylight Saving Time: Disabled

Time Format: 12 Hour

Date Format: WWW MMM DD

Voicemail: Yes

PNP URL: ☒ Automatic ☐ Custom

Figure 6-9

6.1.2.2 Aastra General Settings

In this page, you can configure the general settings before provisioning Aastra IP phones, including the items like general preferences, program keys configuration, soft keys configuration.

General Settings for Aastra

[Go Back to Phone Provisioning](#)

General Preferences | Programkeys Configuration | Softkeys Configuration

Local Dial Plan: 91x|92xx|[4-8]xxxxxxxx|Sixx

Send Dial Plan Terminator: ☐ Enable

Time and Date Setting

Time Server1:

Time Server2:

Auto-Resync

Resync Mode: none

Resync Time: 00:00

Figure 6-10

6.1.2.3 Phone book

You can add your contacts here and when you use phone provisioning; the IP phone will download the phone book.

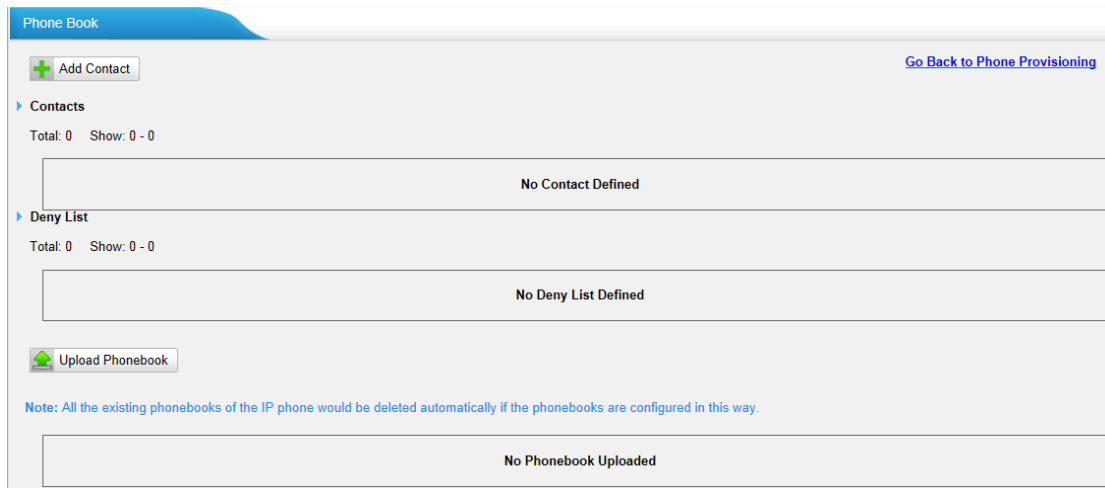


Figure 6-11

1) Add Contact

•Type

There are three types: None, VIP and Deny list (Blacklist).

•Group

There are 5 groups: None, Friends, Family, Work, Colleagues list.

•Nick Name

You can set a nick name for this number.

•Favorite

Only works with snom phone.

•Organization

Input the organization of this contact. Only works with snom phone.

•Title

Input the title of this contact. Only works with snom phone.

•Email

Input the email of this contact. Only works with snom phone.

•Birthday

Input the birthday of this contact. Only works with snom phone.

•First Name

Input the first name of this contact. Only works with snom phone.

•Family Name

Input the family of this contact. Only works with snom phone.

•Office Number

Input the office number here

•Mobile Number

Input the mobile number here

•Home Number

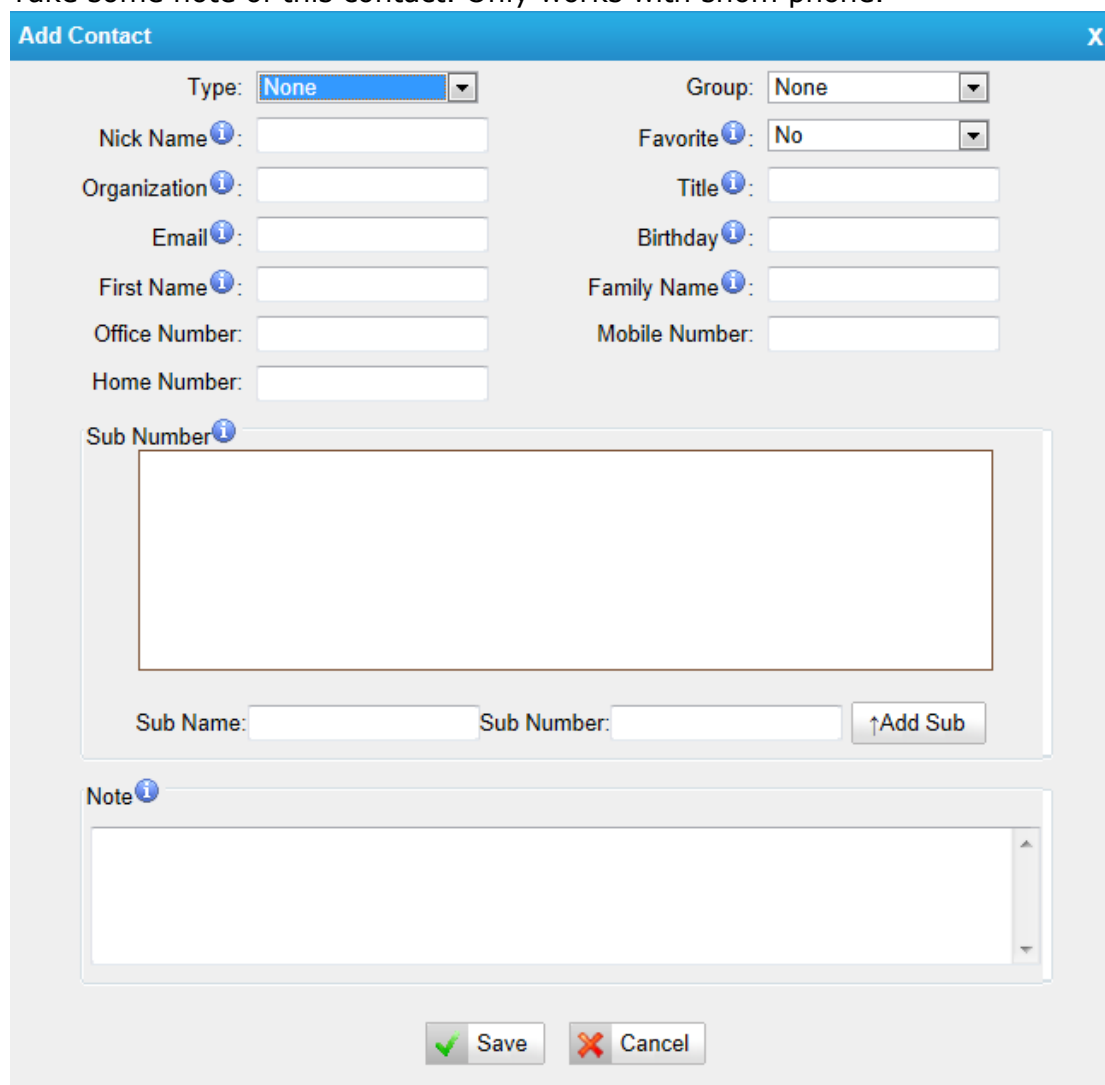
Input the home number here

•Sub Number

Add sub number of this contact. Only works with snom phone.

•Note

Take some note of this contact. Only works with snom phone.



The image shows a web-based form titled "Add Contact" with a blue header bar and a close button (X) in the top right corner. The form is organized into two main columns of input fields. The left column includes: "Type" (a dropdown menu set to "None"), "Nick Name" (text input), "Organization" (text input), "Email" (text input), "First Name" (text input), "Office Number" (text input), and "Home Number" (text input). The right column includes: "Group" (a dropdown menu set to "None"), "Favorite" (a dropdown menu set to "No"), "Title" (text input), "Birthday" (text input), "Family Name" (text input), and "Mobile Number" (text input). Below these columns is a "Sub Number" section, which features a large empty text area, a "Sub Name" text input, a "Sub Number" text input, and an "Add Sub" button. At the bottom of the form is a "Note" section with a large text area. The form concludes with "Save" and "Cancel" buttons at the bottom center.

Figure 6-12

2) Upload Phonebook

You can upload a phonebook before auto provision, which will be provisioned to the IP phone when using auto provision feature to configure your IP phones. The format of phonebook should be *.xml.

Note: All the existing phonebooks of the IP phone will be replaced automatically if the phonebooks are configured in this way.

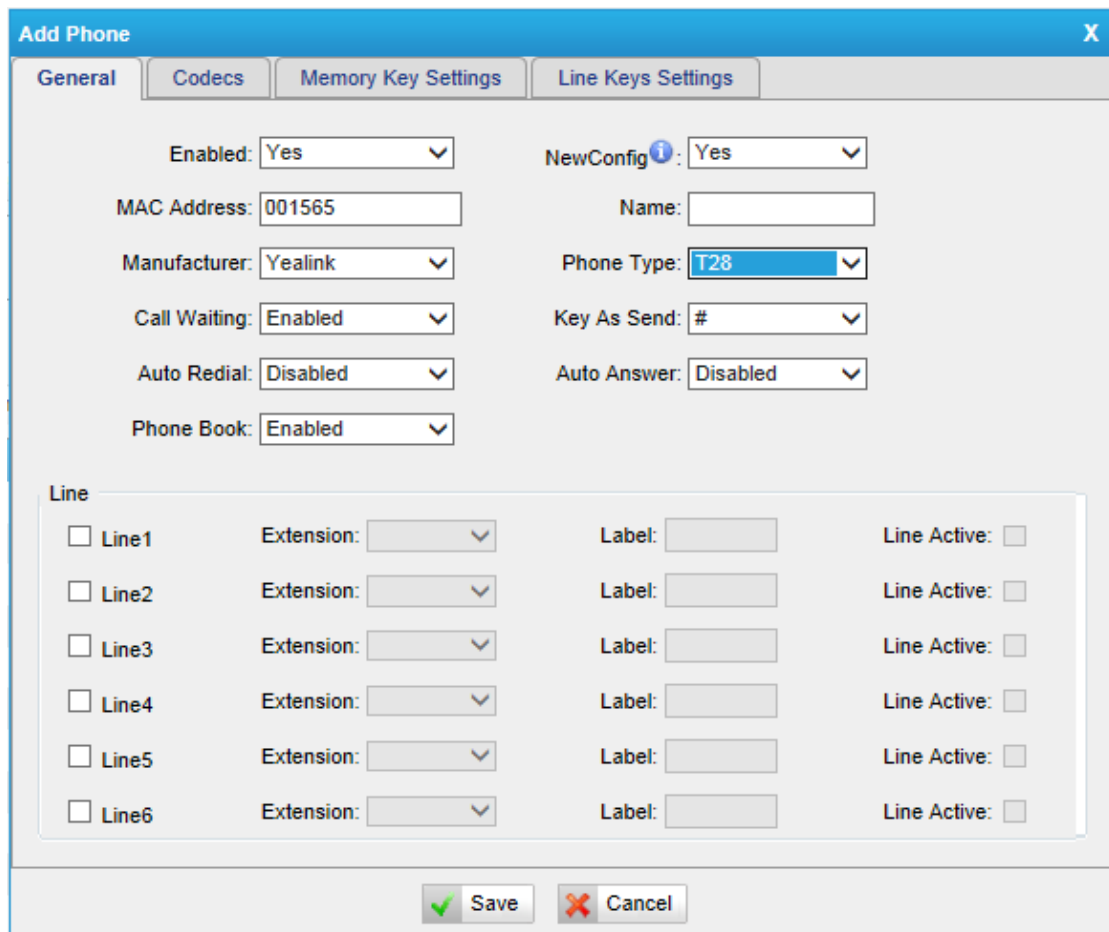
6.1.2.4 Configure phone

Let's take provisioning Yealink phone as an example.

There are two modes to create new phones: create new phones in webpage and upload the IP Phone's configuration file.

Add new phone via webpage

Click "Add Phone" and fill in the corresponding information in the pop-up window.



Add Phone			
General			
Enabled:	Yes	NewConfig:	Yes
MAC Address:	001565	Name:	
Manufacturer:	Yealink	Phone Type:	T28
Call Waiting:	Enabled	Key As Send:	#
Auto Redial:	Disabled	Auto Answer:	Disabled
Phone Book:	Enabled		
Line			
☐ Line1	Extension:	Label:	Line Active: ☐
☐ Line2	Extension:	Label:	Line Active: ☐
☐ Line3	Extension:	Label:	Line Active: ☐
☐ Line4	Extension:	Label:	Line Active: ☐
☐ Line5	Extension:	Label:	Line Active: ☐
☐ Line6	Extension:	Label:	Line Active: ☐
Save Cancel			

Figure 6-13

1) General

•Enabled

Choose yes or no to enable or disable this extension.

•New Config

If your IP phone's firmware version is above x.70.x.x, you should select "Yes". Or else, it should be "No".

• MAC address

Input the MAC address of the IP phone.

•Name

Put the name of this Phone here.

•Manufacturer

You can choose the Manufacturer of the IP phone.

•Phone Type

Choose the model of your phone. Only for snom phone.

•Call Waiting

This call feature allows your phone to accept other incoming calls to an extension already in an active call.

•Key as Send

Configure a key as the send key, you choose #, * or disable this feature

•Auto redial

Enable or disable the auto redial for the IP Phone.

•Auto answer

Enable or disable auto answer for the IP phone.

•Phone book

Enable or disable the feature of phone book for the IP phone.

•Line

You can set each line of IP phone for the account you want, active or not.

Extension: Select the extension number for IP Phone.

Label: It is shown on the LCD for users to identify the account.

Line Active: You can choose on/off to enable/disable the account respectively.

2) Codecs

In this page, we can set the codecs for the IP phone.

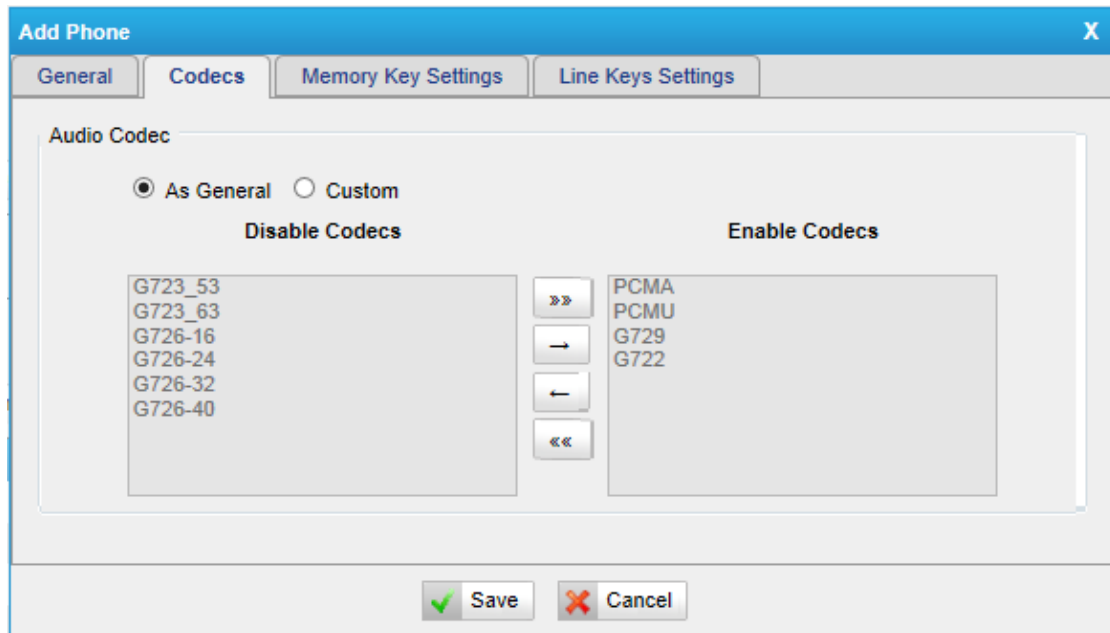
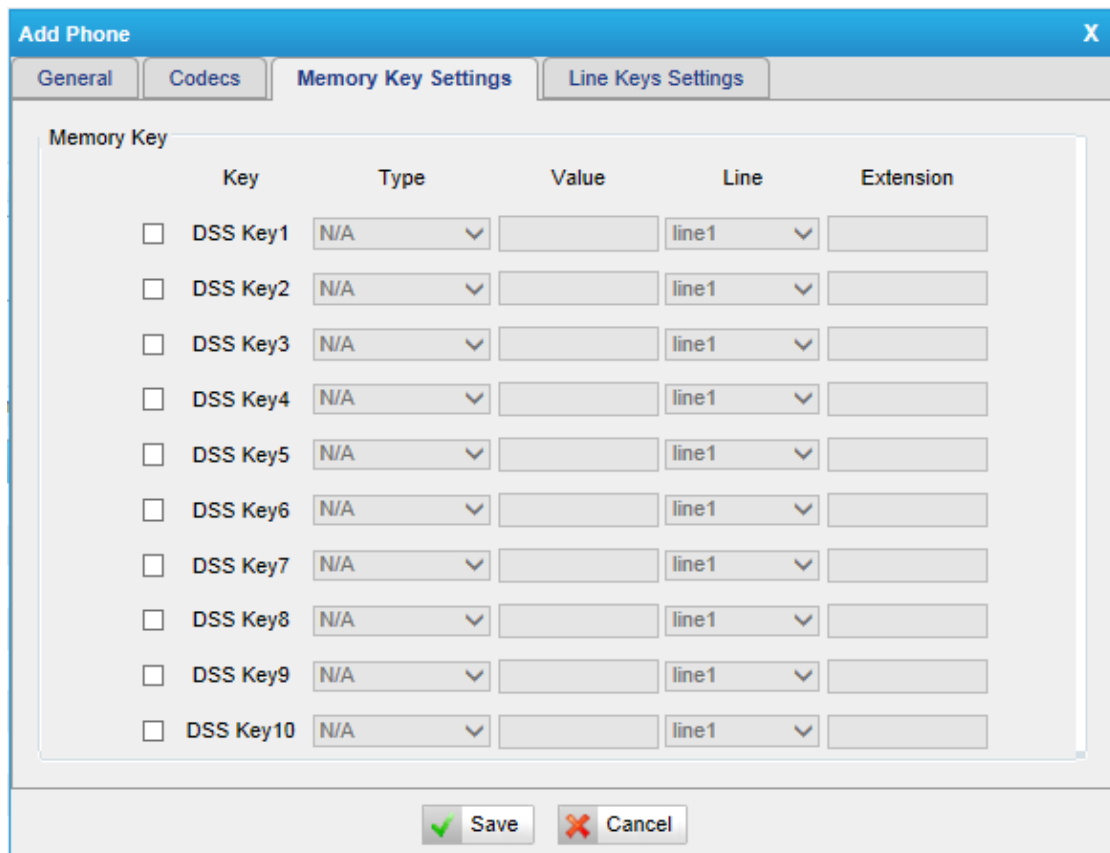


Figure 6-14

3) Memory key settings

In this page, we can configure the DSS keys of the IP phone one by one.

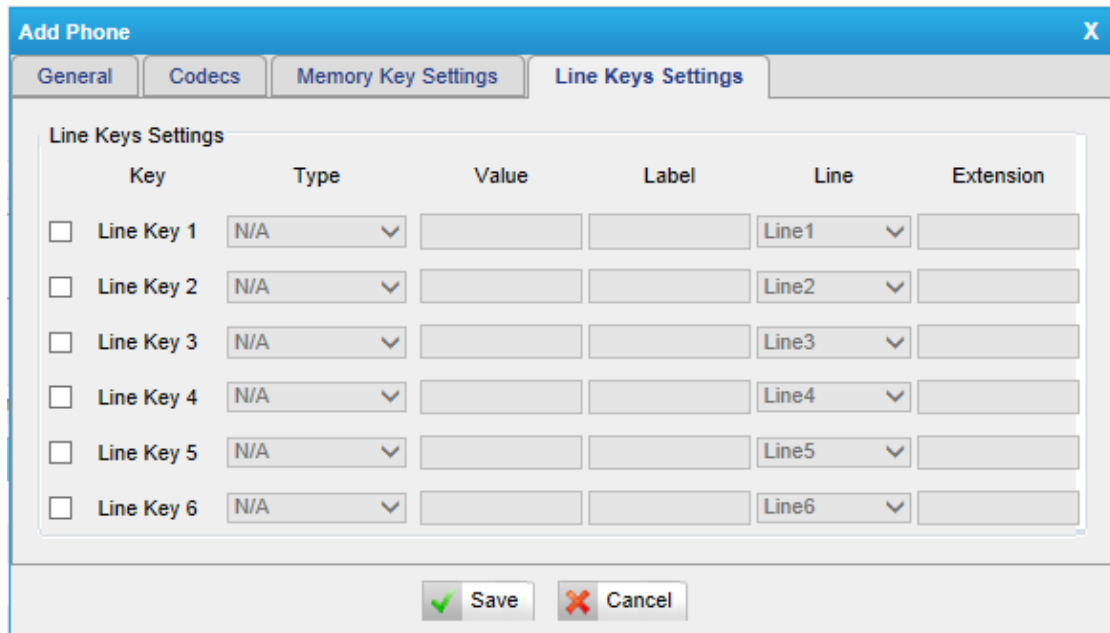


	Key	Type	Value	Line	Extension
☐	DSS Key1	N/A		line1	
☐	DSS Key2	N/A		line1	
☐	DSS Key3	N/A		line1	
☐	DSS Key4	N/A		line1	
☐	DSS Key5	N/A		line1	
☐	DSS Key6	N/A		line1	
☐	DSS Key7	N/A		line1	
☐	DSS Key8	N/A		line1	
☐	DSS Key9	N/A		line1	
☐	DSS Key10	N/A		line1	

Figure 6-15

4) Line keys settings

We can configure the line key settings for this IP phone.

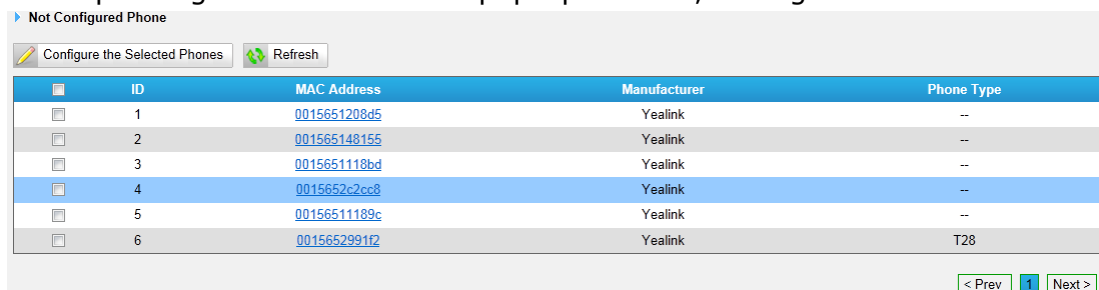


Key	Type	Value	Label	Line	Extension
☐ Line Key 1	N/A			Line1	
☐ Line Key 2	N/A			Line2	
☐ Line Key 3	N/A			Line3	
☐ Line Key 4	N/A			Line4	
☐ Line Key 5	N/A			Line5	
☐ Line Key 6	N/A			Line6	

Figure 6-16

6.1.2.4 Not configured phone

In this section, MyPBX will scan all the supported IP phones and display them here. We can click the "MAC address" of an IP phone and input the corresponding information in the pop-up window, like figure 6-13.



ID	MAC Address	Manufacturer	Phone Type
1	0015651208d5	Yealink	--
2	001565148155	Yealink	--
3	0015651118bd	Yealink	--
4	0015652c2cc8	Yealink	--
5	00156511189c	Yealink	--
6	0015652991f2	Yealink	T28

Figure 6-17

6.1.2.5 Upload a file

Click "Upload a file" and choose the configuration file of IP phone in the popup window.

Note: the file format must be

Yealink: .cfg file

Snom: .htm file

Grandstream: .xml file

Please edit the configuration files in advance before uploading.

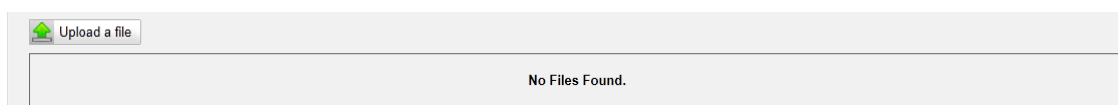


Figure 6-18

6.2 Trunks

6.2.1 Physical Trunk

Multiple physical trunks are supported in MyPBX SOHO V5, like BRI, PSTN. Please make sure you have installed the modules inside before you use the relevant physical trunk. BRI trunk requires B2 module, and PSTN trunk requires the O2 module.

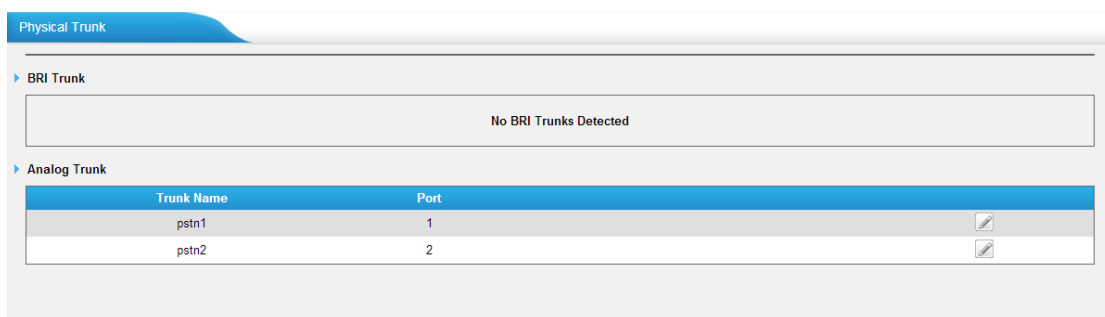


Figure 6-19

BRI Trunk

Basic Rate Interface (BRI, 2B+D, 2B1D) is an Integrated Services Digital Network (ISDN) configuration intended primarily for use in subscriber lines similar to those that have long been used for plain old telephone service. The BRI configuration provides 2 bearer channels (B channels) at 64 kbit/s each and 1 data channel (D channel) at 16 kbit/s. The B channels are used for voice or user data, and the D channel is used for any combination of data, control/signalling, and X.25 packet networking.

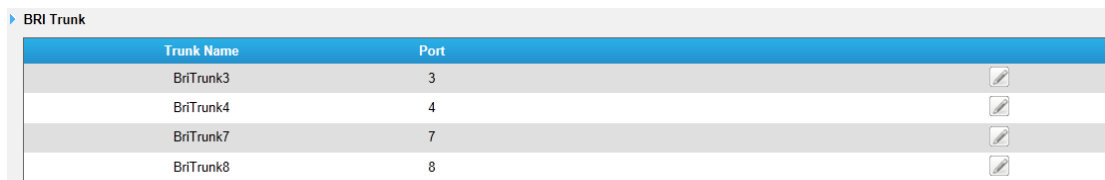


Figure 6-20

Click edit to configure the details of BRI trunks.

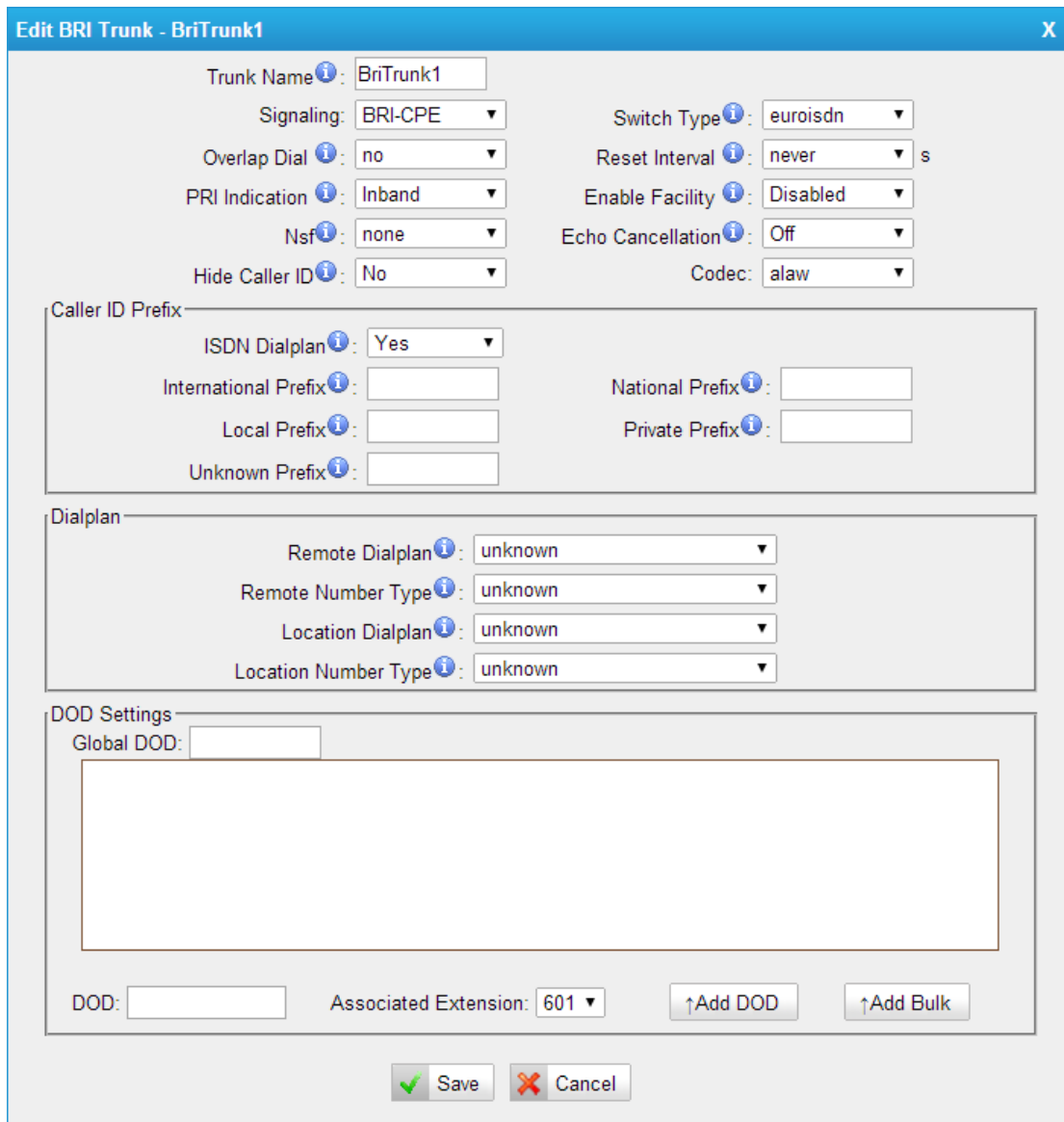


Figure 6-21

•Trunk Name

A unique label used to identify this trunk when listed in outbound rules, incoming rules, etc. E.g. "BriTrunk1"

•Signaling

Signaling method

BRI-CPE: ISDN BRI in TE mode and Point to Point.

BRI-CPE-PTMP: ISDN BRI in TE mode and Point to multi Point.

BRI-NET: ISDN BRI in NET mode and Point to Point.

BRI-NET-PTMP: ISDN BRI in NET mode and Point to multi Point.

•Switch Type

National: National ISDN type2 (common in the US)

ni1: National ISDN type 1

dms100: Nortel DMS100

4ess: AT&T 4ESS

5ess: Lucent 5ESS

euroisdn: EuroISDN

qsig: D-channel signaling protocol at Q reference point for PBX networking.

•Over Lap Dial

Define whether MyPBX can dial this switch using overlap digits or not. If you need Direct Dial-in (DDI; in German "Durchwahl") you should change this to yes, then MyPBX will wait after the last digit it receives.

•Reset interval

Set the time in seconds between restart of unused channels. Some PBXs don't like channel restarts. So set the interval to a very long interval e.g. 100000000 or "never" to disable entirely. If you are in Israel, the following is important: As Bezeq in Israel doesn't like the B-Channel resets happening on the lines, it is best to set the reset interval to "never" when installing a box in Israel. Our past experience also shows that this parameter may also cause issues on local switches in the UK and China.

•PRI Indication

Tells how Device should indicate Busy() and Congestion() to the switch/user. Accepted values are:

inband: Device plays indication tones without answering; not available on all PRI/BRI subscription lines .

outofband: Device disconnects with busy/congestion information code so the switch will play the indication tones to the caller. Busy() will now do same as setting PRI_CAUSE=17 and Hangup().

•Enable Facility

To enable transmission of facility-based ISDN supplementary services (such as caller name from CPE over facility).

•NSF

Used with AT&T PRIs. If outbound calls are being rejected due to "Mandatory information element missing" and the missing IE is 0x20, then you need this setting.

•Echo Cancellation

Disable or enable echo cancellation; it is recommended not to turn this off.

•Hide Caller ID

If you want others to see your CID, please disable this option.

•Codec

You can choose alaw or ulaw.

1) Caller ID Prefix

•ISDN Dialplan

These settings are set to make the caller ID prefix work according to information sent from the E1 provider. ISDN telephony numbering plan Recommendation E.164.

•International Prefix

When there are international calls coming in via this BRI trunk, the International Prefix you have set here will be added before the CID. So you can know this is an international call before you answer it.

•National Prefix

When there are national calls coming in via this BRI trunk, the National Prefix you have set here will be added before the CID. So you can know this is a national call before you answer it.

•Local Prefix

When there are Local calls coming in via this BRI trunk, the Local Prefix you have set here will be added before the CID. So you can know this is a local call before you answer it.

•Private Prefix

When there are Private calls coming in via this BRI trunk, the Private Prefix you have set here will be added before the CID. So you can know this is a Private call before you answer it.

•Unknown Prefix

When there are calls with unknown number coming via this BRI trunk, the Unknown Prefix you set here will be shown as the caller ID.

2) Dialplan

•Remote Dialplan

Calling number type

•Remote Number Type

Calling number identification

•Location Dialplan

Called number type

•Location Number Type

Called number identification

3) DOD Setting

•Global DOD

Global direct outward dialing number.

•DOD

Direct Outward Dialing Number.

•Associated Extension

The extension make call out via BRI Trunk will display the associated DOD.

•Add DOD

Add DOD for one associated extension.

•Add Bulk DOD



Figure 6-22

Add bulk DOD for bulk extensions in ascending sequence with the "Begin DOD" you fill in. For example, if the Associated Extensions are 100, 101, 102, 103, 104, 105 with "Begin DOD" as 5500100, the corresponding DOD will be 5500100, 5500101, 5500102, 5500103, 5500104, and 5500105.

PSTN trunk

The public switched telephone network (PSTN) is the network of the world's public circuit-switched telephone networks.

▶ Analog Trunk

Trunk Name	Port	
pstn13	13	
pstn14	14	

Figure 6-23

Click edit to configure more details.

Edit Analog Trunk - pstn8 X

Trunk Name : pstn8

Volume Setting : 40% ▼

Hangup Detection

Busy Detection : Yes ▼

Busy Count : 4

Busy Interval : 1

Busy Pattern :

Frequency Detection : No ▼

Busy Frequency :

Hangup Polarity Reversal Detection : No ▼

Answer Detection

Answer Detection: ▼

Caller ID Setting

Caller ID Start : Ring ▼ Caller ID Signaling : Bell - USA ▼

Caller ID Detection : Yes ▼

 Save  Cancel

Figure 6-24

•Trunk Name

A unique label used to identify this trunk when listed in outbound rules, incoming rules, etc. E.g. "pstn5".

•Volume Setting

Used to modify the volume level of this trunk. Normally, this setting does not need to be changed.

1) Hangup Detection

•Busy Detection

Busy Detection is used to detect far end hang-up or for detecting a busy signal. Select "Yes" to turn this feature on.

•Busy Count

If Busy Detection is enabled, it is also possible to specify how many busy tones to wait for before disconnecting the call. The default is 4, but better results can be achieved if set to 6 or even 8. Remember, the higher the number, the more time will be required to release a channel. A higher setting lowers the probability that you will encounter random hang-ups.

•Busy Interval

The busy detection interval

•Busy Pattern

If Busy Detection is enabled, it is also possible to specify the cadence of your busy signal. In many Countries, it is 500msec on, 500msec off. Without Busy Pattern specified, MyPBX will accept any regular sound-silence pattern that repeats <Busy Count> times as a busy signal. If you specify Busy Pattern, then MyPBX will further check the length of the tone and silence, which will further reduce the chance of a false positive disconnection.

•Frequency Detection

Used for Frequency Detection (Enable detecting the busy signal frequency or not).

•Busy Frequency

If the Frequency Detection is enabled, you must specify the local frequency.

•Hangup Polarity Reversal Detection

The call will be considered as "hang up" on a polarity reversal.

2) Answer Detection

•Answer Detection

Answer Detection settings are configured for accurate billing. If the PSTN trunk sends polarity after answering the call, users can choose "Polarity Detection"; or else choose "Ring Detection", and configure the detailed settings according to the PSTN line ring tone.

3) Caller ID setting

•Caller ID Start

This option allows you to define the start of a Caller ID signal:

Ring: Start when a ring is received (Caller ID Signaling: Bell_USA, DTMF).

Polarity: Start when a polarity reversal is started (Caller ID Signaling: V23_UK, V23_JP, DTMF).

Before Ring: Start before a ring is received (Caller ID Signaling: DTMF).

•Caller ID Signaling

This option defines the type of Caller ID signaling to use. It can be set to one of the following:

Bell: bell202 as used in the United States

v23_UK: suitable in the UK

v23_Japan: suitable in Japan

v23-Japan pure: suitable in Japan

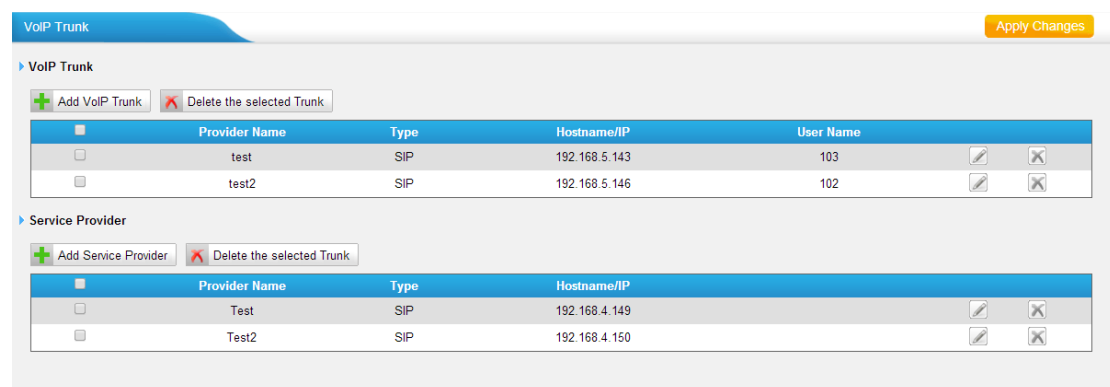
DTMF: suitable in Denmark, Sweden, and Holland

•Caller ID Detection

For FXO trunks, this option forces MyPBX to clarify Caller ID incoming calls.

6.2.2 VoIP Trunk

There are two types of VoIP trunk in MyPBX: SIP and IAX, in this page, we can also configure the "service provider" trunk, which doesn't need the use name and password for authorization, when you have bought a trunk from provide with IP address only, please choose "Service Provider" trunk .



Provider Name	Type	Hostname/IP	User Name
test	SIP	192.168.5.143	103
test2	SIP	192.168.5.146	102

Provider Name	Type	Hostname/IP
Test	SIP	192.168.4.149
Test2	SIP	192.168.4.150

Figure 6-25

6.2.2.1 VoIP Trunk

In this page, we can configure VoIP trunk (SIP/ IAX) you have got from provider with the authorization name and password.

VoIP Trunk

[+ Add VoIP Trunk](#) [X Delete the selected Trunk](#)

	Provider Name	Type	Hostname/IP	User Name		
☐	test	SIP	192.168.5.143	103		
☐	test2	SIP	192.168.5.146	102		

Figure 6-26

1) Add VoIP Trunk

Input the correct SIP information (provided by VoIP provider). Inaccurate information will prevent the trunk from registering. You can delete multiple trunks at once as required.

Add VoIP trunk X

Type: SIP ▼

Provider Name:

Hostname/IP: :

Domain:

User Name:

Authorization Name:

Password:

From User:

Online Number :

Maximum Channels :

Caller ID :

Realm :

☐ Enable Outbound Proxy Server

Transport: UDP ▼ ☐ Enable SRTP ☐ Qualify: ☒

DTMF Mode: rfc2833 ▼

DOD Settings

DOD: Associated Extension: 601 ▼ [↑Add DOD](#) [↑Add Bulk](#)

[✓ Save](#) [✗ Cancel](#)

Figure 6-27

•Type

SIP—Identifies whether the trunk sends and receives calls using the VoIP protocol SIP.

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

•Domain

VoIP provider's server domain name.

•Username

Username of the SIP account. Used for SIP trunk registration.

•Authorization name

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

•Password

Password of the SIP account.

•From User

All outgoing calls from this SIP Trunk will use the From User (In this case the account name for SIP Registration) in From Header of the SIP Invite package. Keep this field blank if not needed

•Online number

Define the online number that expected by "Skype Connect" and some other SIP service providers. Leave this field blank if not needed.

•Maximum Channels

Control the maximum number of outbound channels (simultaneous calls) that can be used on this trunk. Inbound calls are not counted against the maximum. Set as 0 to specify no maximum.

•Caller ID

Specify the caller ID to use when making outbound calls over this trunk. The caller ID set in the "extension" page will override the caller ID set in the "VoIP trunk" page. Please note that not all the service providers support this feature. Contact your service provider for more information.

•Outbound Proxy Server

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

•Realm

Realm is a string to be displayed to users so they know which username and password to use.

•Codecs

Define the codec for this SIP trunk and its priority

Note: To change the codec type and priority of this trunk, please create it first, it will appear when you edit it again.

•Transport

This will be the transport method used by the SIP Trunk. This method is given by the SIP trunk provider. The options are UDP (default) or TCP or TLS.

•Enable SRTP

Define if SRTP is enabled for this trunk.

•Qualify

Send check alive packets to the SIP provider.

•DTMF mode

Set default mode for sending DTMF of this trunk. Default setting: rfc2833

•DOD

DOD (Direct Outward Dialing) means the caller ID displayed when dialing out. Before configuring this, please make sure the provider supports this feature.

•Associated Extension

The extension making call out via SIP Trunk will display the associated DOD.

•Add DOD

Add DOD for one associated extension.

•Add Bulk DOD



Figure 6-28

Add bulk DOD for bulk extensions in ascending sequence with the "Begin DOD" you fill in. For example, if the Associated Extensions are 100, 101, 102, 103, 104, 105 with "Begin DOD" as 5500100, the corresponding DOD will be 5500100, 5500101, 5500102, 5500103, 5500104, and 5500105.

2) Add IAX trunk

Input the correct IAX information (provided by VoIP provider). Inaccurate information will prevent the trunk from registering.

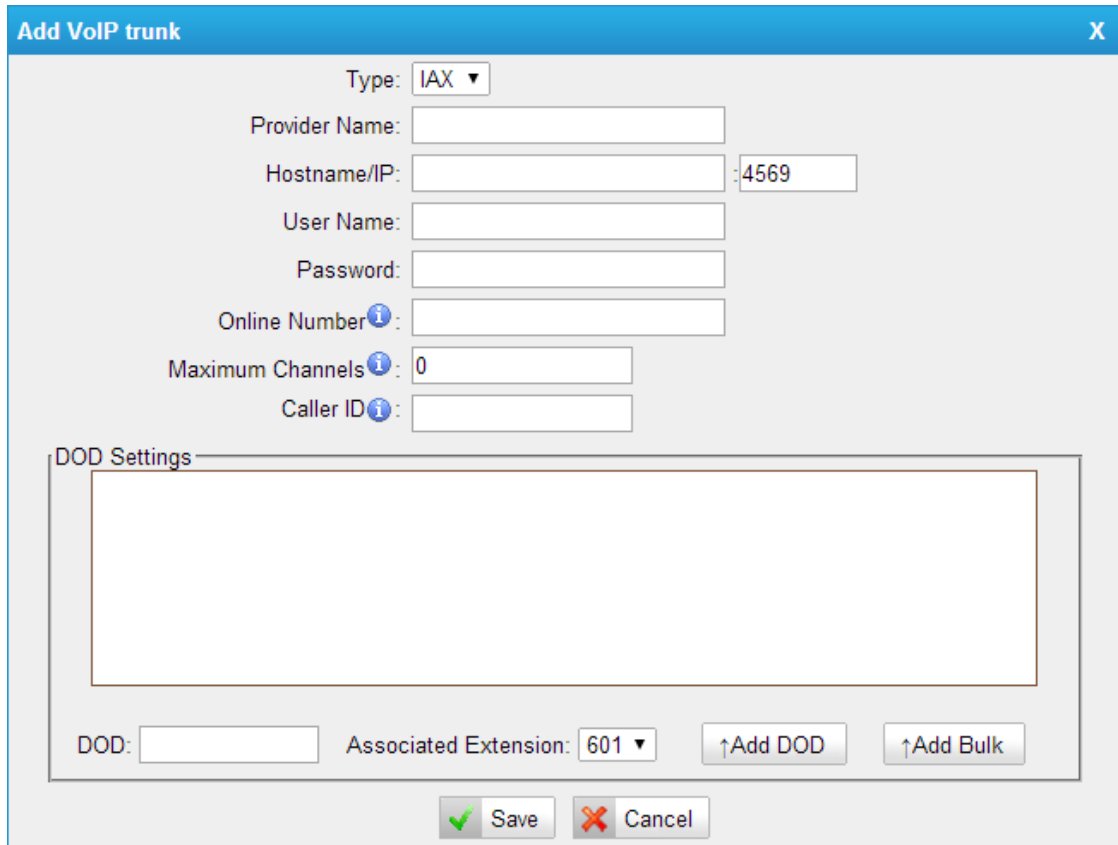


Figure 6-29

•Type

IAX—Identifies whether the trunk sends and receives calls by using the VoIP protocol IAX.

•Provider Name

A unique label to help you identify this trunk when listed in outbound rules, incoming rules etc. E.g. "yeastar2".

•Hostname/IP

Service provider's hostname or IP address. 4569 is the standard port number used by IAX protocol. Don't change this part if it is not required.

•Username

Username of IAX account; Used for IAX trunk registration.

•Password

Password of IAX account

•Online number

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

•Maximum Channels

Control the maximum number of outbound channels (simultaneous calls) that can be used on this trunk. Inbound calls are not counted against the maximum. Set as 0 to specify no maximum.

•Caller ID

Specify the caller ID to use when making outbound calls over this trunk. The caller ID set in the "extension" page will override the caller ID setting in the "VoIP trunk" page. Please note that not all the service providers support this feature. Contact your service provider for more information.

•DOD

DOD (Direct Outward Dialing) means the caller ID displayed when dialing out. Before configuring this, please make sure the provider supports this feature

•Associated Extension

The extension making call out via IAX Trunk will display the associated DOD.

•Add DOD

Add DOD for one associated extension.

•Add Bulk DOD

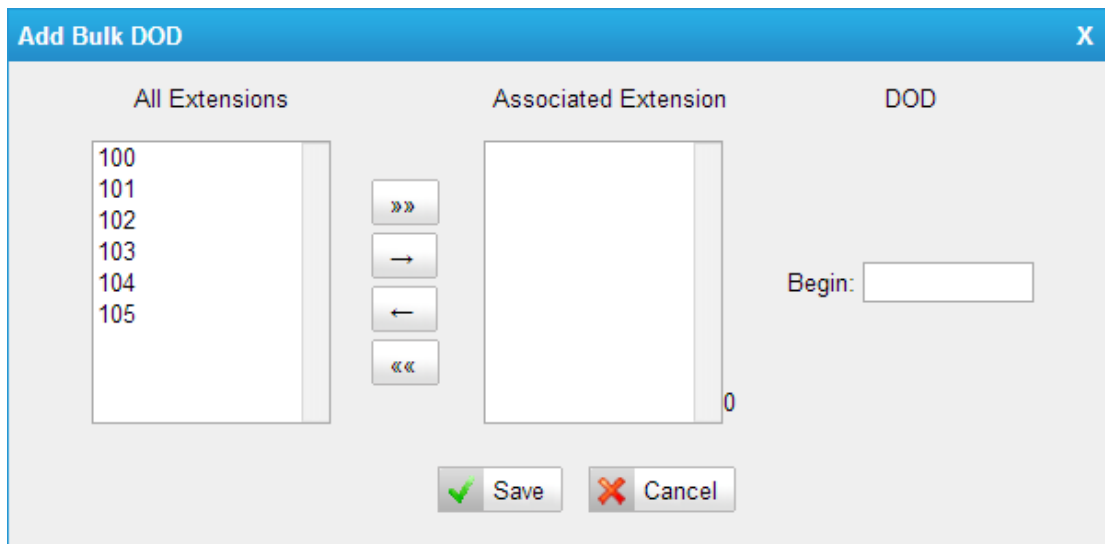


Figure 6-30

Add bulk DOD for bulk extensions in ascending sequence with the "Begin DOD" you fill in. For example, if the Associated Extensions are 100, 101, 102, 103, 104, 105 with "Begin DOD" as 5500100, the corresponding DOD will be 5500100, 5500101, 5500102, 5500103, 5500104, and 5500105.

6.2.2.2 Service Provider

In this page, we can configure Service Provider.

You can add Service Provider as required. And also you can delete multiple trunks at once by ticking the checkbox as required.

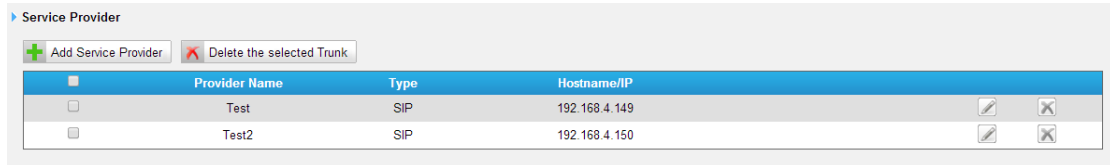
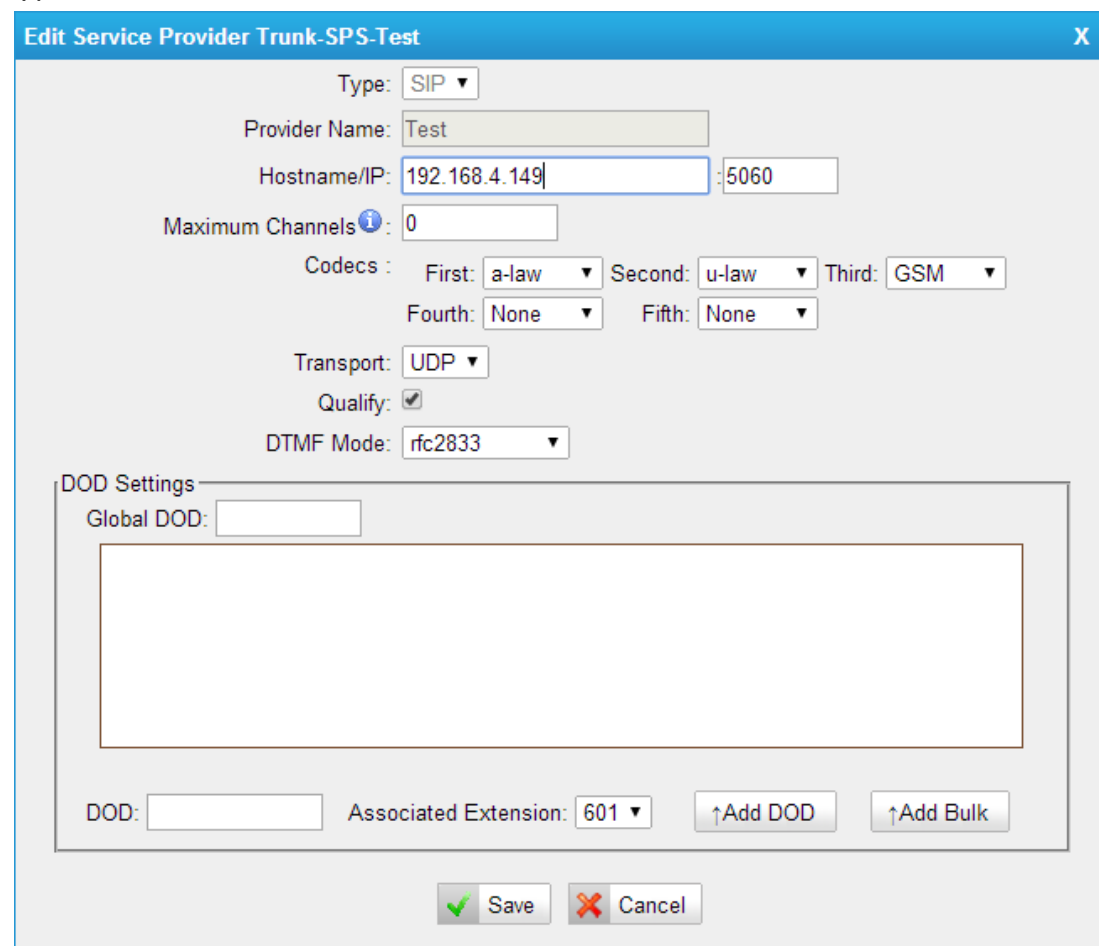


Figure 6-31

Below is service provider trunk (peer to peer mode), which authorize using IP address only. If you have got a trunk with IP address only, please choose this type.



Edit Service Provider Trunk-SPS-Test

Type: SIP

Provider Name: Test

Hostname/IP: 192.168.4.149 : 5060

Maximum Channels: 0

Codecs: First: a-law Second: u-law Third: GSM Fourth: None Fifth: None

Transport: UDP

Qualify: ☒

DTMF Mode: rfc2833

DOD Settings

Global DOD:

DOD: Associated Extension: 601

Buttons: Add DOD, Add Bulk, Save, Cancel

Figure 6-32

•Type

SIP or IAX

SIP – Identifies whether the trunk sends and receives calls by using the VoIP

protocol SIP.

IAX – Identifies whether the trunk sends and receives calls by using the VoIP protocol IAX.

•Provider Name

A unique label would help to you identify this trunk. E.g. "Provider2".

•Hostname/IP

Service provider's hostname or IP address.

Note: 5060 is the standard port number used by SIP protocol, 4569 is the standard port number used by IAX protocol. Don't change this part if it is not required.

•Maximum Channels

Control the maximum number of outbound channels (simultaneous calls) that can be used on this trunk. Inbound calls are not counted against the maximum. Leave blank to specify no maximum.

•Codecs

Define the codec for this SIP trunk and its priority

Note: codec can only display when editing it after creating the trunk.

•Transport

This will be the transport method used by the SIP Trunk. This method is given by the SIP trunk provider. The options are UDP (default) or TCP or TLS.

•Qualify

Send check alive packets to the SIP provider.

•DTMF mode

Set default mode for sending DTMF of this trunk. Default setting: rfc2833.

•DOD

DOD (Direct Outward Dialing) means the caller ID displayed when dialing out. Before configuring this, please make sure the provider supports this feature.

•Associated Extension

The extension making call out via this Trunk will display the associated DOD.

•Add DOD

Add DOD for one associated extension.

•Add Bulk DOD



The dialog box titled "Add Bulk DOD" contains three columns: "All Extensions", "Associated Extension", and "DOD". The "All Extensions" column is a list box containing the numbers 100, 101, 102, 103, 104, and 105. The "Associated Extension" column is an empty list box with a "0" at the bottom right. Between these two columns are four buttons: a double right arrow (»»), a single right arrow (→), a single left arrow (←), and a double left arrow (««). To the right of the "Associated Extension" column is a "Begin:" label followed by an empty text input field. At the bottom of the dialog are two buttons: a green checkmark icon followed by the text "Save", and a red X icon followed by the text "Cancel".

Figure 6-33

Add bulk DOD for bulk extensions in ascending sequence with the "Begin DOD" you fill in. For example, if the Associated Extensions are 100, 101, 102, 103, 104, 105 with "Begin DOD" as 5500100, the corresponding DOD will be 5500100, 5500101, 5500102, 5500103, 5500104, and 5500105.

6.3 Outbound Call Control

6.3.1 Outbound Routes

In this page, we can configure the outbound rules to control the outgoing calls.

Notes:

1. The max number of outbound route is 32.
2. If the dial patterns are the same in several routes, MyPBX will choose the available routes from top to the last one.
3. When you have created a new extension, please edit the outbound route so that it can dial out too.

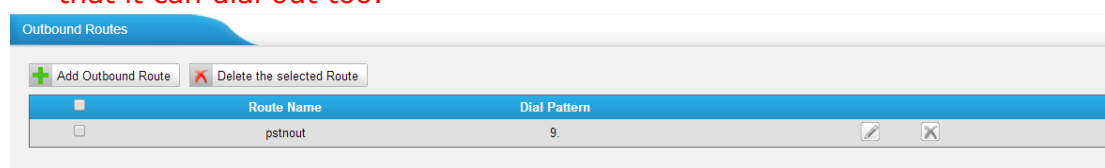


Figure 6-34

We can create outbound route or use the default route "pstnout" (dial 9+numbers to dial out). Also you can delete multiple outbound routes at once as required.

Edit Outbound Route - pstnout
X

Route Name: pstnout

Password:
[PIN Settings](#)

T.38 Support: No

Rmemory Hunt: No

Office Hours:

Dial Patterns

Dial Pattern

Strip

Prepend

9.

1

+

Add

X

Member Extensions

Available Extensions

Selected

»»

→

←

««

300(SIP)
301(SIP)
302(SIP)
303(SIP)
304(SIP)
305(SIP)
603(FXS)
604(FXS)

Member Trunks

Available Trunks

Selected

»»

→

←

««

pstn1(FXO)
pstn2(FXO)
test(SIP)

192.168.5.145(SIP)

✓ Save

✗ Cancel

Figure 6-35

•Route Name

Name of this Outbound Route. E.g. "Local" or "Long Distance".

•Password

The route password can be used to protect this route from being accessed without a password. You can choose one of the passwords in the PIN list that you can click the "Pin Settings" to edit it in "Pin Settings" page.

T.38 Support:

Enable T38 fax in this outbound route (Only for SIP Trunk).

•Rrmemory Hunt

Round robin with memory, remembers which trunk was used last time, and then use the next available trunk to call out.

•Office Hours

When a specific office hour is selected, this outbound route can only be used during this office hour, and can't be used in non-office hours.

•Dial Pattern

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

X: Any Digit from 0-9

Z: Any Digit from 1-9

N: Any Digit from 2-9

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

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

The "!" will match none remaining digits, and causes the matching process to complete as soon as it can be determined that no other matches are possible.

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

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

•Strip

Allows the user to specify the number of digits that will be stripped from the front of the phone number before the call is placed. For example, if users must press 0 before dialing a phone number, one digit should be stripped from the dial string before the call is placed.

•Prepend

These digits 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.

•Add

Add multiple dial patterns in this outbound route.

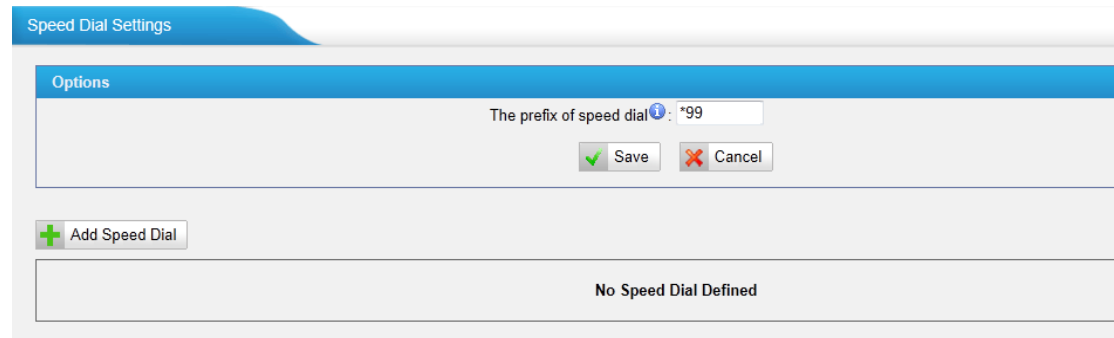
•Member Extensions

Define the extensions that will be permitted to use this outbound route.

•Member Trunks

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

6.3.2 Speed Dial Settings



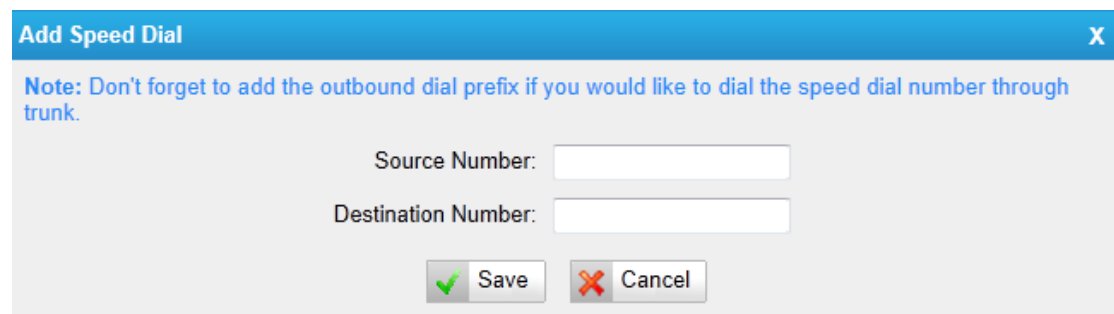
The screenshot shows the 'Speed Dial Settings' window. It has a blue header with the title 'Speed Dial Settings'. Below the header is a section titled 'Options'. Inside 'Options', there is a text input field labeled 'The prefix of speed dial' with the value '*99'. Below the input field are two buttons: 'Save' (with a green checkmark icon) and 'Cancel' (with a red X icon). Below the 'Options' section is a button labeled '+ Add Speed Dial'. Below this button is a large empty rectangular area with the text 'No Speed Dial Defined' centered at the bottom.

Figure 6-36

1) Options

•The prefix of speed dial

The prefix should be dialed before the speed dial number. The default is *99.



The screenshot shows the 'Add Speed Dial' dialog box. It has a blue header with the title 'Add Speed Dial' and a close button (X) on the right. Below the header is a note in blue text: 'Note: Don't forget to add the outbound dial prefix if you would like to dial the speed dial number through trunk.' Below the note are two text input fields: 'Source Number:' and 'Destination Number:'. Below the input fields are two buttons: 'Save' (with a green checkmark icon) and 'Cancel' (with a red X icon).

Figure 6-37

2) Add new speed dial.

•Source Number

The speed dial number.

•Destination Number

The number you want to call.

E.g. the source number is "123". The destination number is 5503305. The prefix number is *99. You can use an extension with any type to dial *99123, then it will call the number 5503305.

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

6.4 Inbound Call Control

In this page, we can configure the details of IVR, ring group, queue and inbound routes.

6.4.1 IVR

When there's an inbound call aims at Auto Attendant, MyPBX will play an IVR recording and route the caller to the requested destination (for example, "Welcome to XX company, for sales press 1, for technical support press 2, for operator press 0", etc.). The system will transfer the call to corresponding extension according to DTMF digits input by the user.

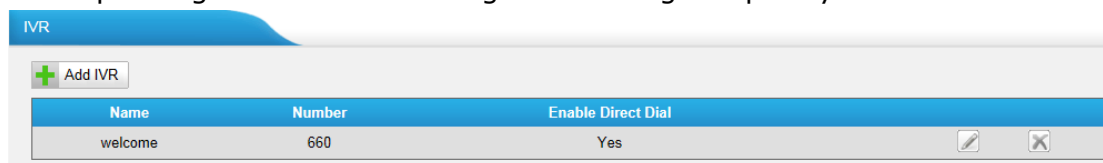
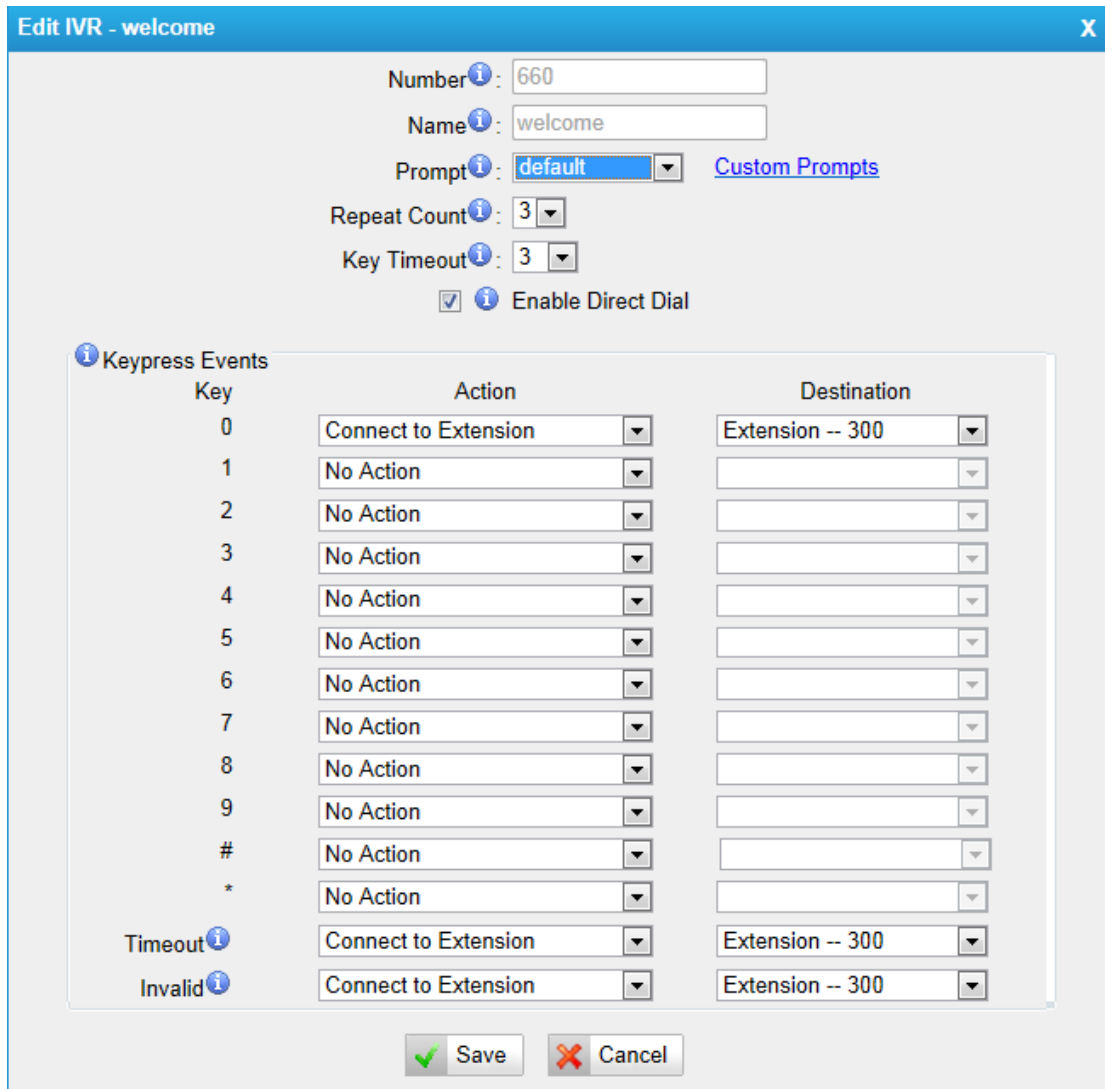


Figure 6-38

There is a default IVR here, we can edit it directly or add IVR by yourself.



Number: 660

Name: welcome

Prompt: default [Custom Prompts](#)

Repeat Count: 3

Key Timeout: 3

☒ Enable Direct Dial

Key	Action	Destination
0	Connect to Extension	Extension -- 300
1	No Action	
2	No Action	
3	No Action	
4	No Action	
5	No Action	
6	No Action	
7	No Action	
8	No Action	
9	No Action	
#	No Action	
*	No Action	
Timeout	Connect to Extension	Extension -- 300
Invalid	Connect to Extension	Extension -- 300

Save Cancel

Figure 6-39

•Number

MyPBX treats IVR as an extension; you can dial this extension number to reach the IVR from internal extensions.

•Name

A name for the IVR.

•Prompt

The prompt recording that will be played when this IVR is reached.

•Repeat Count

The number of times that the selected IVR prompt will be played.

•Key Timeout

Wait for the user to enter a new extension for a specified number of seconds.

•Enable Direct Dial

Allow the caller to dial other extensions number directly.

•Key Press Events

A list of actions that can be performed depending on the digit dialed by the user.

•Key

The Key pressed when the callers hear the IVR prompt.

•Action

When the callers press the corresponding key, the action that MyPBX will execute.

No Action: Do nothing

Connect to Extension: Connect the call to an extension.

Connect to Voicemail: Connect the call to the voicemail of an extension.

Connect to RingGroup: Connect the call to a ringgroup.

Connect to IVR: Connect the call to an IVR.

Connect to Conference Room: Connect the call to a conference room.

Connect to DISA: Connect the call to a DISA.

Connect to Queue: Connect the call to a queue.

Connect to Faxes: Connect the call to Faxes of extensions.

Dial by Name: The callers can dial the name of an extension to connect to the corresponding extension.

Hung up: Hang up the call.

•Destination

Where will MyPBX route the call when the action occurs.

•Time Out

Define the timeout action. A timeout occurs after the IVR prompt has finished playing for the number of times specified by the "Repeat Count" field.

•Invalid

Define the invalid action. The invalid action is triggered if the user enters a DTMF digit that is not defined for this IVR.

6.4.2 Ring Groups

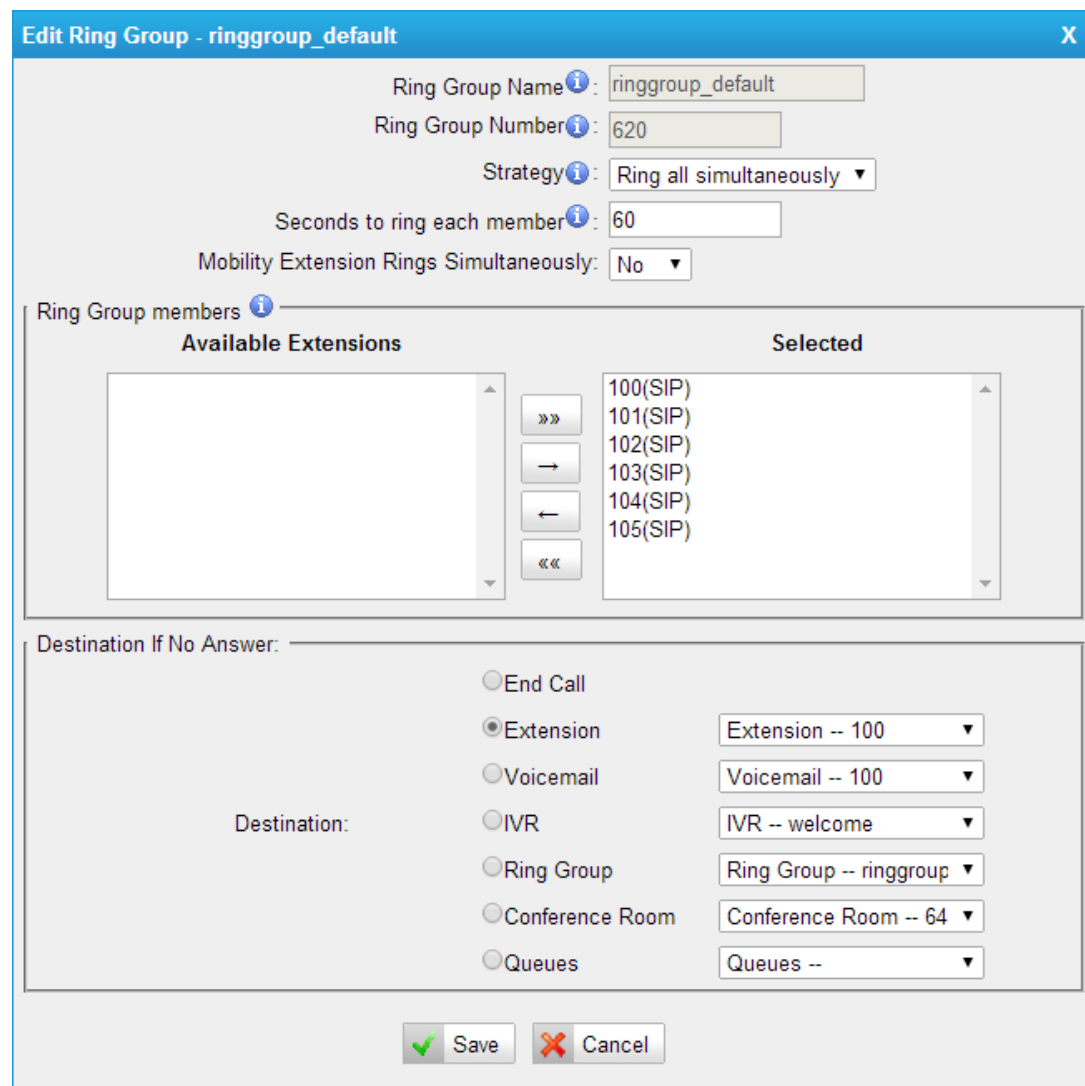
Ring groups can be configured to balance the call traffic for multiple users and give callers a higher level of availability for incoming calls. Multiple ring methods and voicemail are supported.

Note: follow me feature in extension page will not take effect when it's ringing as an agent.



Figure 6-40

There is a default ringgroup, you can edit it or create a new one



Edit Ring Group - ringgroup_default

Ring Group Name: ringgroup_default

Ring Group Number: 620

Strategy: Ring all simultaneously

Seconds to ring each member: 60

Mobility Extension Rings Simultaneously: No

Ring Group members

Available Extensions

Selected

100(SIP)
101(SIP)
102(SIP)
103(SIP)
104(SIP)
105(SIP)

Destination If No Answer:

☐ End Call
☒ Extension
☐ Voicemail
☐ IVR
☐ Ring Group
☐ Conference Room
☐ Queues

Extension -- 100
 Voicemail -- 100
 IVR -- welcome
 Ring Group -- ringgroup
 Conference Room -- 64
 Queues --

Save Cancel

Figure 6-41

•Ring Group Name

This option defines a name for this group, e.g. "Sales". "Ring Group Name" is a label to help you identify this group in the group list.

•Ring Group Number

This option defines the numbered extension that can be dialed to reach this group.

•Strategy

This option sets the Ringing Strategy for this Group. The options are as follows:

1. Ring All Simultaneously: Ring all available Extensions simultaneously.
2. Ring Sequentially: Ring each extension in the group one at a time.

•Mobility Extension Rings Simultaneously

If set to yes, when the extension in the Ring group is called, the associated mobility extension will ring simultaneously. Beforehand, the option of "Rings Simultaneously" should be ticked in the extension settings.

•Seconds to ring each member

1. If the strategy is "Ring All Simultaneously", it means the number of seconds to ring this group before routing the call according to the "Destination if No Answer" settings.
2. If the strategy is "Ring Sequentially", it means the number of seconds to ring a single extension before moving onto the next one.

•Ring Group Members

An extension can be made a member of this ring group by moving it into the "Selected" box.

•Destination If No Answer

When all members on this group fail to answer the call, system will handle the call according to the selected destination.

6.4.3 Queues

Call Queues give users (e.g. call centers) an efficient means to have their calls answered in the order they were received to deliver top tier customer service.

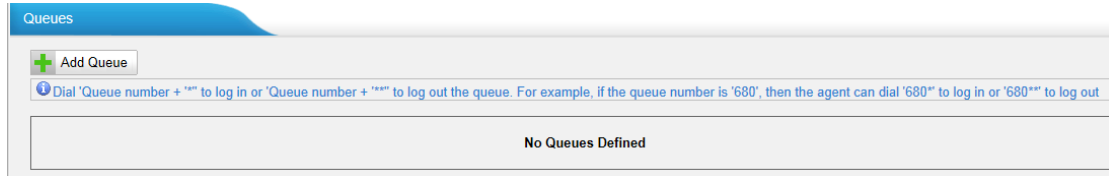


Figure 6-42

Call queues allow calls to be sequenced to one or more agents.

Notes:

1. Dial "Queue number + '*'" to log in or "Queue number + '**'" to log out the queue. For example, if the queue number is "680", then agent can dial "680*" to log in or "680**" to log out.
2. Follow me feature in extension page will not take effect when it's ringing as an agent of queue.

Add Queue
X

Queue Name: 680
Queue Number: 680
Queue Password:
Queue Agent Timeout: 30
Queue Max Wait Time: 1800
Queue Ring Strategy: ringall

Agents

Available Agents

Selected

300(SIP)
301(SIP)
302(SIP)
303(SIP)
304(SIP)
305(SIP)
601(FXS)
602(FXS)

»»
→
←
««

Caller Position Announcements

Announce Position: Yes
Announce Hold Time: Yes
Frequency: 30 seconds

Periodic Announcements

Prompt: [Custom Prompts](#)
Frequency: 30 seconds

Events

Key: ---
Action: End Call
Destination:

Failover-Destination

Action: End Call
Destination:

Others

Music On Hold: calmriver [Music on Hold Prompts](#)
Leave When Empty: Yes
Join Empty: No
Agent Announcement:
Join Announcement:
Retry: 30
Wrap-up Time: 30

Save Cancel

Figure 6-43

•Queue Name

A name for the Queue.

•Queue Number

Use this number to dial into the queue, or transfer callers to this number to put them into the queue.

•Queue Password

You can require agents to enter a password before they can log in to this queue.

•Queue Agent Timeout

The number of seconds an agent's phone can ring before we consider it a timeout.

•Queue Max Wait Time

The maximum number of seconds a caller can wait in a queue before being pulled out (0 for unlimited).

•Queue Ring Strategy

This option sets the Ringing Strategy for this Queue. The options are

RingAll: Ring all available Agents simultaneously until one answers.

LeastRecent: Ring the Agent which was least recently called.

FewestCalls: Ring the Agent with the fewest completed calls.

Random: Ring a Random Agent.

RRmemory: Round Robin with Memory, Remembers where it left off in the last ring pass.

1) Agents

This selection shows all users. Selecting a user here makes them an agent of the current queue.

2) Caller Position Announcements

•Announce Position

Announce position of caller in the queue

•Announce Hold Time

Enabling this option causes MyPBX to announce the hold time to the caller periodically based on the frequency timer. Either yes or no; hold time will not be announced if <1 minute.

•Frequency

How often to announce queue position and estimated hold time.

Note: "0 seconds" means disabling the announcement.

3) Periodic Announcements

•Prompt

Select a prompt file to play periodically.

•Frequency

How often to announce a prompt to the caller.

4) Events

If a caller presses the key while waiting in the queue, this setting selects which action should process the key press.

5) Failover-Destination

Define the failover action. A failover occurs after the user reach the Queue max wait time.

6) Others

•Music on Hold

Select the "Music on Hold" Class for this Queue.

•Leave When Empty

This option controls whether callers already on hold are forced out of a queue that has no agents. There are two options.

Yes: Callers are forced out of a queue when no agents are logged in.

No: Callers will remain in a queue with no agents.

•Join Empty

This option controls whether callers can join a call queue that has no agents. There are two options,

Yes: Callers can join a call queue without agents or only unavailable agents

No: Callers cannot join a queue when there are no agents in the queue.

The default option is No.

•Agent Announcement

Announcement played to the Agent prior to bridging in the caller.

•Join Announcement

Announcement played to callers once prior to joining the queue.

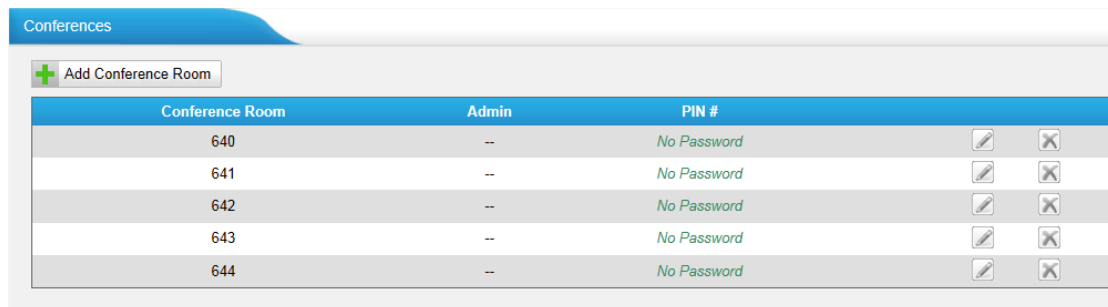
•Retry

The number of seconds we wait before trying all the phones again.

•Wrap-up time

How many seconds after the completion of a call an Agent will have before the Queue can ring them with a new call. The default is 30.

6.4.4 Conferences



Conference Room	Admin	PIN #		
640	--	No Password		
641	--	No Password		
642	--	No Password		
643	--	No Password		
644	--	No Password		

Figure 6-44

Conference Calls increase employee efficiency and productivity, and provide a more cost-effective way to hold meetings. Conference agents can dial * to access the settings options and the admin can kick the last user out and can lock the conference room.

•Extension

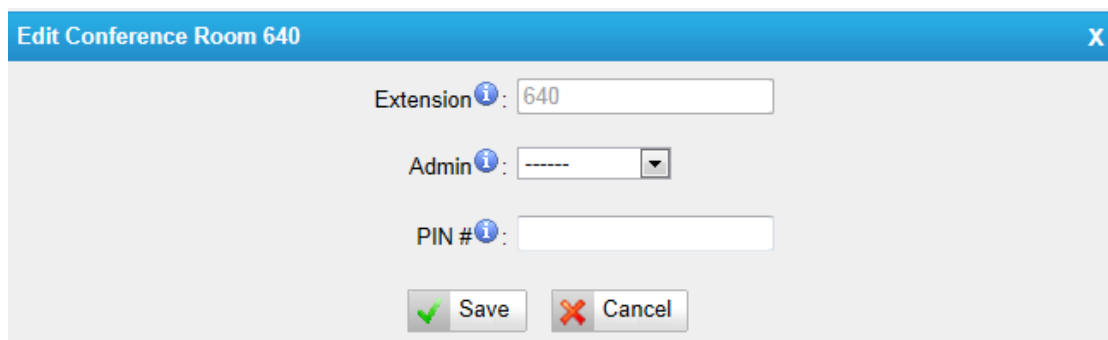
This is the number dialed to reach this Conference Room.

•Admin

Admin can kick a user out and can lock the conference room.

•PIN

Set a PIN that must be entered in order to access this conference room (e.g. 1234).



Edit Conference Room 640 X

Extension :

Admin : 

PIN # :

 Save  Cancel

Figure 6-45 Add/Edit Conference Room

6.4.5 Inbound Routes

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

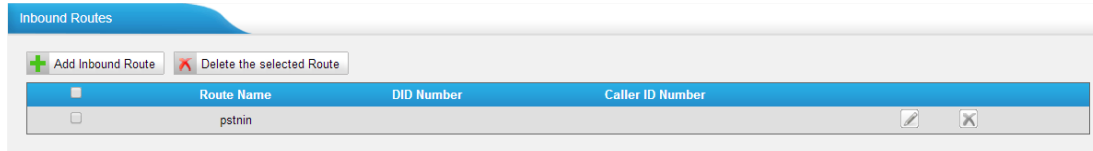


Figure 6-46 Inbound Route List

There is a default inbound route for all the trunks and set IVR as the destination, you can edit it or create a new one for your demands or you can delete multiple outbound routes at once as required. When an incoming call arrives, the system will first check "fax detection", then "Holidays", at last "Business Days".

Edit Inbound Route: pstnin
X

General

Route Name : pstnin
DID Number :
Extension :
Caller ID Number :
Distinctive Ringtone :
Enable Callback : No [Callback Settings](#)

Member Trunks

Available Trunks
Selected

pstn1(FXO)
pstn2(FXO)
192.168.5.145(SIP)
test(SIP)

»»
→
←
««

Business Days

Office Hours : default
Office Hours Destination : IVR IVR -- welcome
Non-office Hours Destination : IVR IVR -- welcome

During Holidays

Holiday :
Destination : End Call

Fax Detection

Destination : No Detect

Save Cancel

Figure 6-47 Add/Edit Inbound Route

1) General

•Route Name

A name for this inbound route. E.g. "pstnin".

•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. The following patterns may be used:

X: Any Digit from 0-9

Z: Any Digit from 1-9

N: Any Digit from 2-9

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

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

The "!" will match none remaining digits, and causes the matching process to complete as soon as it can be determined that no other matches are possible.

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

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

For more information, please refer to [Appendix F How to Use DID](#).

•Extension

Define the extension for DID number. This field is only valid when you use BRI, SIP, SPS or SPX trunk for this inbound router. You can only input number and "-" in this field and the format can be xxx or xxx-xxx. The count of the number must be only one or equal to the count of the DID number.

•Caller ID Number

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

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

X: Any Digit from 0-9

Z: Any Digit from 1-9

N: Any Digit from 2-9

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

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

The "!" will match none remaining digits, and causes the matching process to complete as soon as it can be determined that no other matches are possible.

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

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

•Distinctive Ringtone

MyPBX support mapping to custom ring tone files. For example, if you configure the distinctive ringing for custom ring tone to "**Family**", the ring tone will be played if the phone receives the incoming call.

•Enable Callback

You can enable the callback function of this inbound route. If you want to configure the callback function, please refer to [chapter 6.7.4](#)

How do I configure distinctive ring tones? Please refer to [APPENDIX E](#).
Currently distinctive ringtone can be compatible with Yealink and Snom phone.

2) Member Trunks

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

3) Business Days

Define where the calls will be routed during Business Days.

•Office Hours

Select one defined business days office hours.

•Office Hours Destination

Configure where to route the incoming calls during office hours.

•End Calls

Route the incoming calls to end calls, the system will auto hang up the call.

•Extension

Route the incoming calls to a specific extension.

•Voicemail

Route the incoming calls to extension's voicemail.

•IVR

Route the incoming calls to a specific IVR.

•Ring Group

Route the incoming calls to a specific Ring Group.

•Conference Room

Route the incoming calls to a specific Conference Room.

•DISA

Route the incoming calls to a specific DISA.

•Queues

Route the incoming calls to a specific Queue.

•Faxes

Route the incoming faxes to a specific extension's mail address.

Note: This function only supports T.38 faxes.

•Outbound Routes

Route the incoming calls to a specific outbound route.

This function is mainly used for the connection of two branches.

For example: Company A locates headquarters in the USA with a branch B in China. A and B both have a MyPBX phone system.

Now if staff of A would like to make a call to a telephone or mobile phone in China from the extension of A but via the FXS line of B, that can be done by this configuration.

•Non-office Hours Destination

Configure where to route the incoming calls during non-office hours.

4) During Holidays

Define where the calls will be routed during Holidays.

•Holiday

Select which defined Holiday to use. When a time is defined in both Business Days and Holidays, it will be treated as Holidays.

•Destination

Configure where to route the incoming calls during holidays.

5) Fax Detection

Configure if detecting faxes in this inbound route.

Note: Please choose IVR as the destination above before configuring fax detection (recommended).

•Destination

Configure where the faxes will be routed when faxes are detected.

•No detect

Do not detect faxes.

•Custom Email

Customize an E-mail address to receive the faxes. You should first configure the "Voicemail Settings->SMTP Settings for Voicemail" correctly before you use this option.

•Faxes

Send faxes to an extension. If choosing a FXS extension here, the fax will be

sent to the FXS port selected, you should connect a fax machine to this FXS port. If Choosing a VoIP extension, the fax will be sent to the extension's voicemail as an attachment.

Note: If you want to receive faxes with custom Email address, the "SMTP settings" of "Voicemail Settings" should be configured successfully in advance. If you want to receive faxes with E-mail address configured in VoIP extension voicemail, you should first make sure the tested email to your email address works fine.

6.5 Audio Settings

Custom prompts are supported in MyPBX, and you can change the system prompts to your local country's prompt.

6.5.1 Custom Prompts

We can record or upload the prompts in this page; you can also play it directly to confirm if it's a valid one, you can also download it and save it as a backup.

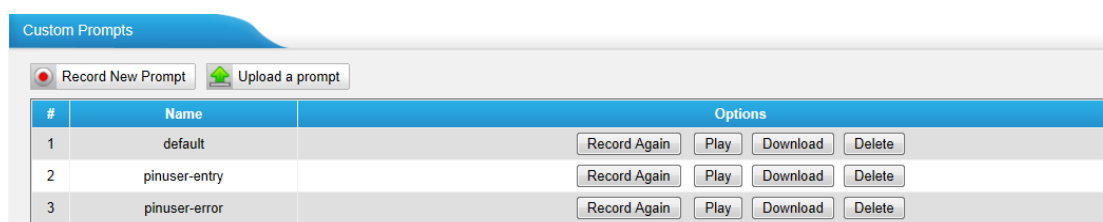


Figure 6-48

1. Record new Prompt

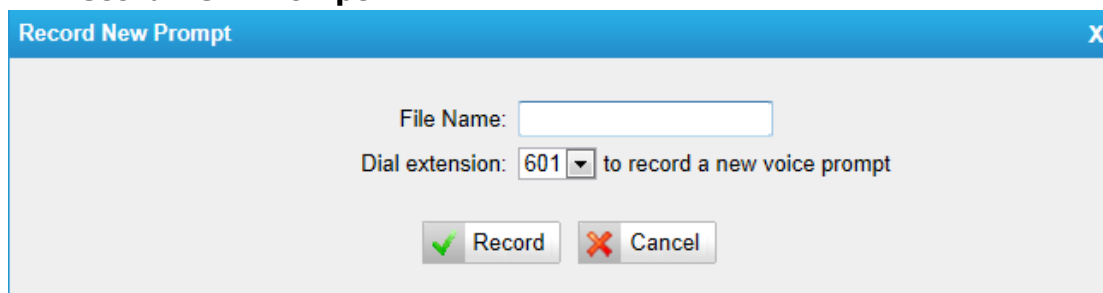


Figure 6-49

The administrator can record custom prompts by doing the following:

- 1) Click "Record New Custom Prompt".
- 2) Input the desired file name on the popup window and choose an extension to call for recording (such as 500).
- 3) Click "Record". The selected extension will ring and you can pick up the phone to start recording.

2. Upload Prompt

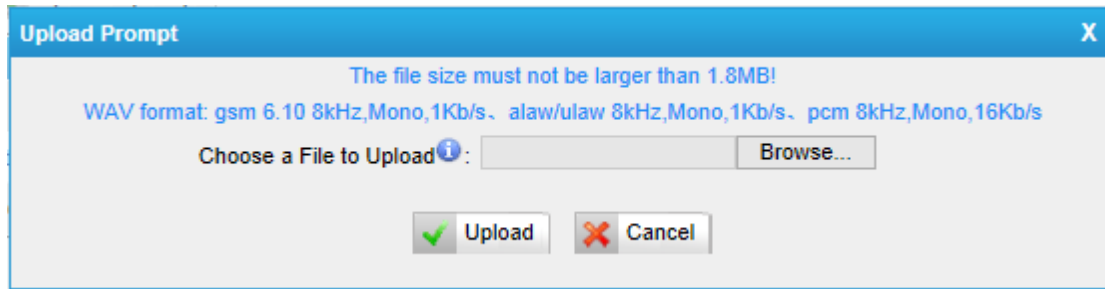


Figure 6-50

The administrator can also upload prompts by doing the following:

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

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.

6.5.2 Music on Hold Prompts

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

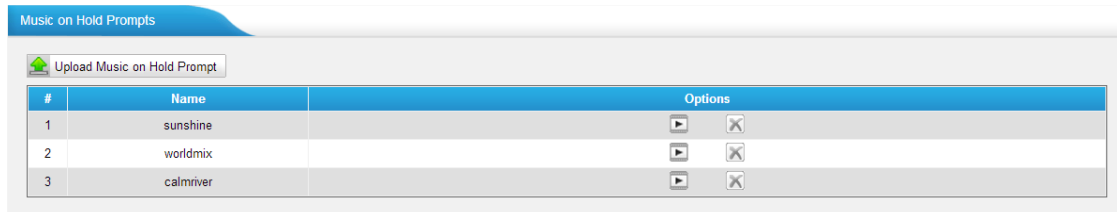


Figure 6-51

The administrator can upload on hold music as follows:

- 1) Click "Upload Music on Prompt".
- 2) Click "Browse" to choose the desired audio file.
- 3) Click "Upload" to upload the selected file.

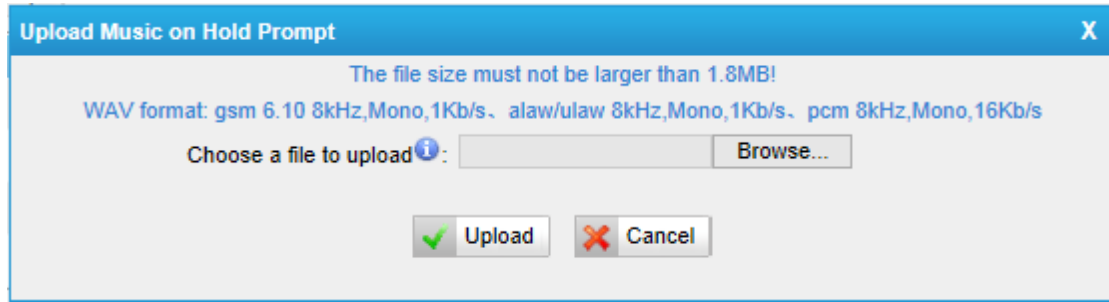


Figure 6-52

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.

6.5.3 System Prompts Settings

MyPBX have prompts of many languages. You can download the appropriate language you need. MyPBX can support American English, Australian English, Chinese, Dutch, French, Canadian French, German, Greek, Hungarian, Italian, Polish, Portuguese, Brazilian Portuguese, Russian, Spanish, Mexican Spanish, Turkish, Thai, and Korean currently.

Notes:

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

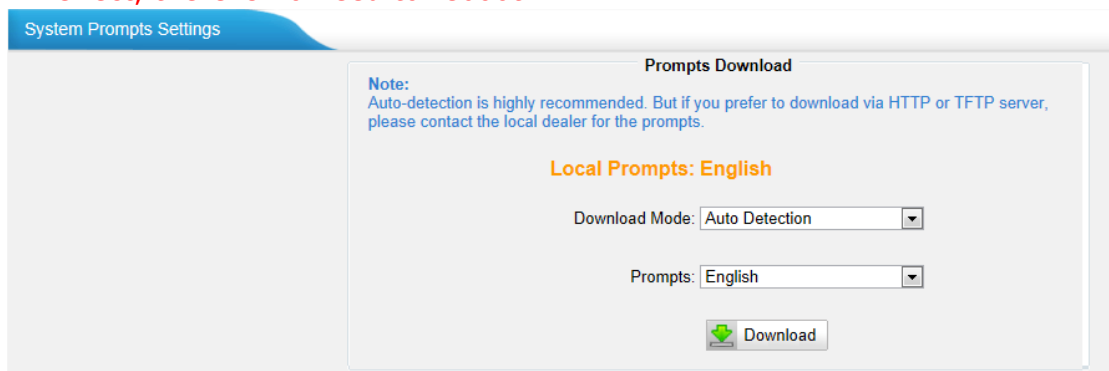


Figure 6-53

6.6 Basic Settings

There are some basic settings we need to configure MyPBX SOHO V5, like the general preferences, business hours, feature codes, voicemail settings.

6.6.1 General Preferences

In this page, there are some general settings of MyPBX.

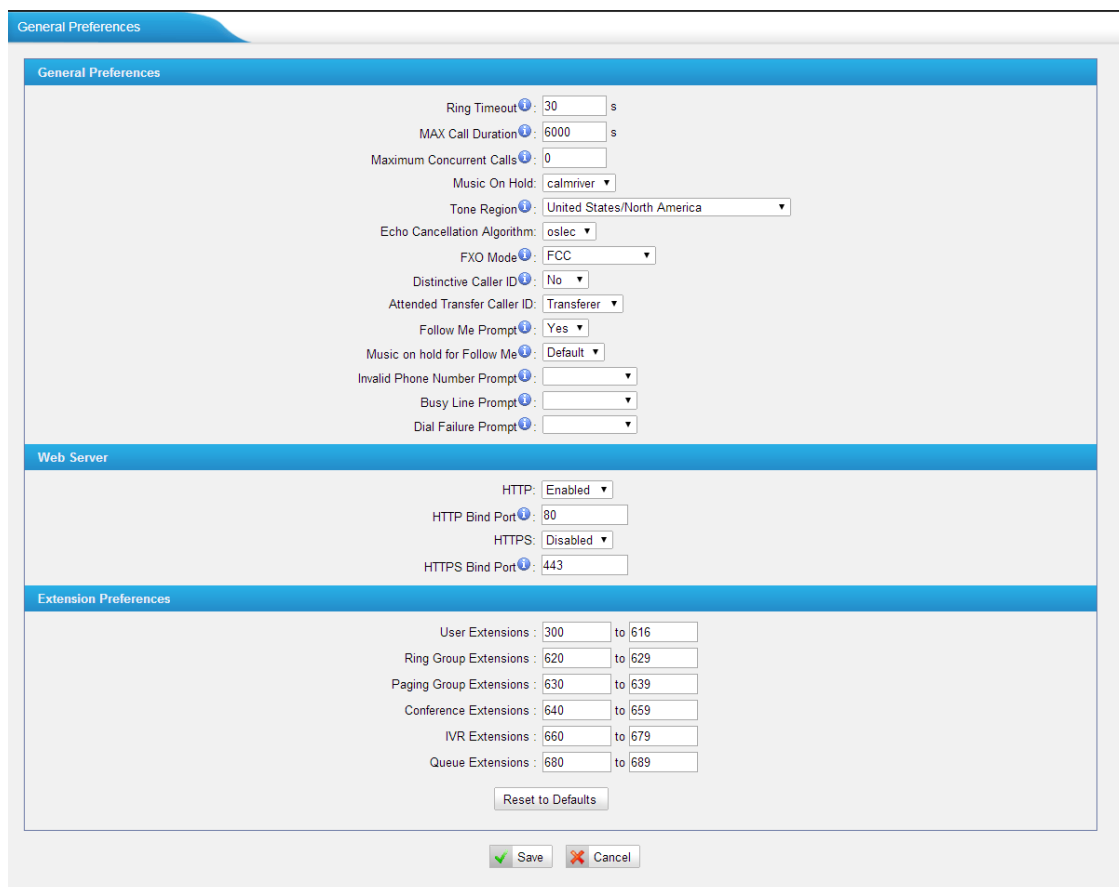


Figure 6-54

1) General

•Ring Timeout

Number of seconds to ring a device before handling the call as per the extension's Follow Me settings. The default value is 30s.

•MAX call duration

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

.Maximum concurrent calls

Maximum concurrent calls limits. The default value 0 means no limit.

•Music on hold

Used to set hold music for the system.

•Tone Region

Please select your country or nearest neighboring country to enable the default dial tone, busy tone, and ring tone for your region.

Note: please reboot the system to take effect.

•HTTP bind port/Web Access Port

Port to use for HTTP sessions; Default: 80

Note: please reboot the system to take effect.

•FXO Mode

FXO port's operation mode.

•Virtual Ring Back Tone

It's only for GSM/UMTS trunk. Once enabled, when the caller call out with GSM/UMTS trunks, the caller will only hear the virtual ring back tone generated by the system before callee answers the call.

•Distinctive Caller ID

When incoming calls are routed from ring group/queue/IVR, the caller ID displays with the name of ring group/queue/IVR, for example 5503302 (ringgroup_default).

Note: To display IVR's name, please press the key instead of the extension number directly.

•Attended Transfer Caller ID

When transferring an incoming call using the attended transfer feature code or the transfer key of IP phone, the Caller ID of transferee or transferer displayed on the screen of the callee. The default display is the Caller ID of the initiator. For example, if extension 500 makes a call to extension 501. After 501 picks up the call, 501 makes an attended transfer to extension 502. If selecting "Transferer", 502 will display the Caller ID as 500; if selecting "Transferee", 502 will display the Caller ID as 501.

•Follow Me Prompt

When set "Follow me" to "Transfer to number" on the extension page (e.g. when 500 is busy, transfer to 501), while 500 is busy, the call will be transferred to 501. If "Enable Follow Me Prompt" choosing yes, there will be prompt before

transferring the call. Otherwise, the call will be transferred directly without any prompt. Default: Yes.

•Music on Hold for Follow Me Prompt

Configure whether to play a prompt “please hold while I try to locate the person you are calling” when transferring a call through follow me settings.

•Invalid Phone Number Prompt

Configure the prompt when the dialed phone number is invalid.

•Busy Line Prompt

Configure the prompt when the dialed phone number is busy.

•Dial Failure Prompt

Configure the prompt when dial failed due to conjunction or no-available channel.

2) Web Server

•HTTP

Enable or disable HTTP session.

•HTTP Bind Port

Default port to use for HTTP session is 80.

•HTTPS

Enable or disable HTTPS session.

•HTTPS Bind Port

Default port to use for HTTPS session is 443.

Note: please reboot the system to take effect.

3) Extension Preferences

•User Extensions

The default value is 500 to 616.

•Ring Group Extensions

The default value is 620 to 629.

•Paging Group Extensions

The default value is 630 to 639.

•Conference Extensions

The default value is 640 to 659.

•IVR Extensions

The default value is 660 to 679.

•Queue Extensions

The default value is 680 to 689.

6.6.2 Business Hours

Business Hours setting including "Holidays" is used to control the incoming calls, we can configure it in this page.

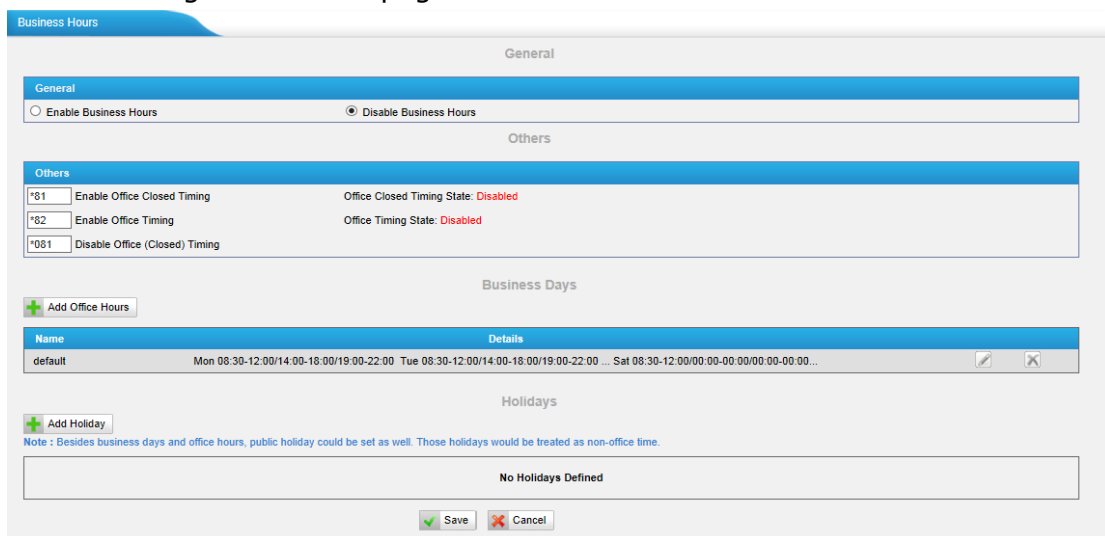


Figure 6-55

1) General

•Enable Business Hours

•disable Business Hours

2) Others

•Enable Office Closed Timing

By dialing *81 (*81 is the default code) on an extension will force the office time closed for the device whatever the general setting is.

•Enable Office Timing

By dialing *82 (*82 is the default code) on an extension will force the office time to take effect for the device whatever the general setting is.

•Disable Office closed timing

By dialing *081 (*081 is the default code) on an extension will disable the Office Closed Timing.

3) Add office hours

You can set up the business hours here.

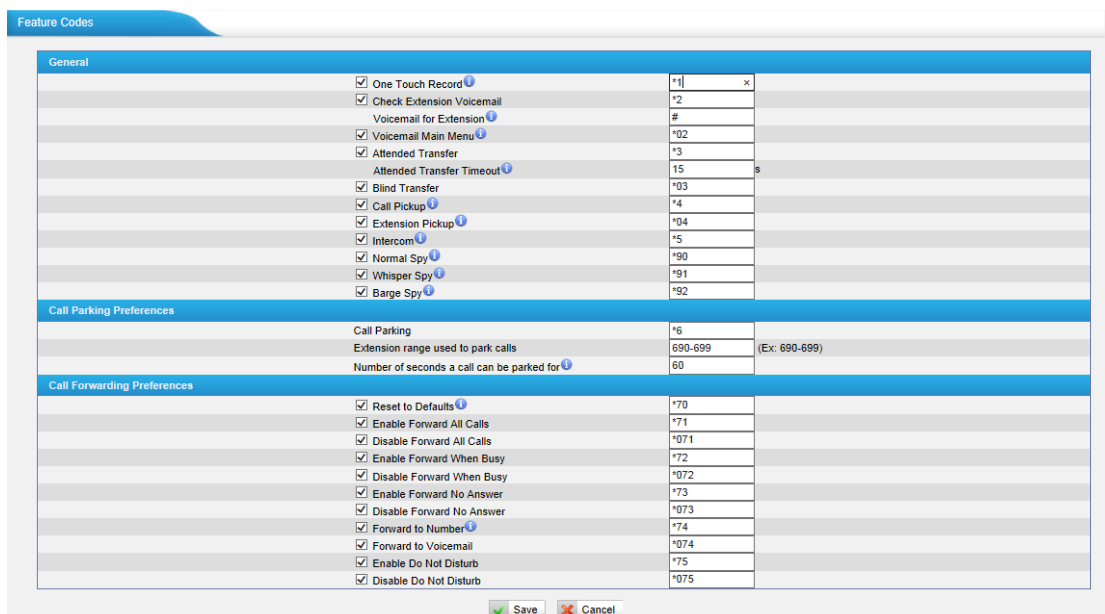
4) Add Holiday

You can set up the holidays here.

If a time period is configured as both Holidays and office hours, it will be treated as Holidays.

6.6.3 Feature Codes

There are many feature codes available in MyPBX, which allow users to dial from extension side to realize the exact feature.



Section	Feature	Code	Default
General	☒ One Touch Record	*1	x
	☒ Check Extension Voicemail	*2	
	Voicemail for Extension	#	
	☒ Voicemail Main Menu	*02	
	☒ Attended Transfer	*3	
	Attended Transfer Timeout	15	s
	☒ Blind Transfer	*03	
	☒ Call Pickup	*4	
	☒ Extension Pickup	*04	
	☒ Intercom	*5	
	☒ Normal Spy	*90	
	☒ Whisper Spy	*91	
☒ Barge Spy	*92		
Call Parking Preferences	Call Parking	*6	
	Extension range used to park calls	690-699	(Ex: 690-699)
	Number of seconds a call can be parked for	60	
Call Forwarding Preferences	☒ Reset to Defaults	*70	
	☒ Enable Forward All Calls	*71	
	☒ Disable Forward All Calls	*071	
	☒ Enable Forward When Busy	*72	
	☒ Disable Forward When Busy	*072	
	☒ Enable Forward No Answer	*73	
	☒ Disable Forward No Answer	*073	
	☒ Forward to Number	*74	
	☒ Forward to Voicemail	*074	
	☒ Enable Do Not Disturb	*75	
☒ Disable Do Not Disturb	*075		

Figure 6-56

1) General

•One Touch Record

A user may initiate or stop call recording by dialing *1 during a call. (*1 is the default setting).

•Extension for Checking Voicemail

Users can check their Voicemail by dialing *2 on their phone (*2 is the default setting).

•Voicemail for Extension

Users can leave a voicemail to other extensions by dialing # on their phone or the incoming call could be forwarded to an extension's voicemail directly. (# is the default setting).

For example, extension 500 want to leave a message for extension 501, users can use 500 dial “#501” to enter the voicemail of 501.

•Voicemail main menu

Users can go to the main menu by dialing *02 (*02 is the default setting).

•Attended Transfer

Users may transfer an incoming call by dialing *3 on their phone (*3 is the default setting).

•Attended Transfer Timeout

The timeout value of transferring a call

•Blind Transfer

Users may blind transfer an incoming call by dialing*03 on their phone (*03 is the default setting).

•Call Pickup

Users may pick up an incoming call by dialing *4 on their phone (*4 is default the setting)

•Extension Pickup

Users may pick up a specific extension's incoming call by dialing *04+extension number on their phone (*04 is the default setting)

•Intercom

Define the feature code that is used to dial an extension in intercom mode. For instance, setting this value to *5 would allow you to initiate an intercom call with extension 501 by dialing *5501.

•Normal Spy

In this mode, you can only listen to the extension being spied, for example you can dial *90501 to monitor extension 501

•Whisper Spy

In this mode you can listen/whisper to the extension being spied, for example, dialing *91501 to listen to extension 501, you can also talk with 501 too.

•Barge Spy

In this mode, you can barge in both extensions involved in the call, for example dialing *92501 to barge in and talk with extensions on both sides.

2) Call Parking Preferences

•Call Parking

User may park an incoming call on his own telephone by pressing “*6” (*6 is the default setting)

•Extension range used to park calls

User may park an incoming call on a designated extension at first and then pick up the call again on any other extensions.

•Number of seconds a call can be parked before it is recalled.

Define the time (in seconds) that a call can be parked before it is recalled to the station that parked it.

3) Call Forwarding Preferences

•Reset to Defaults

Users may reset all call forwarding defaults by calling *70 on their phone (*70 is the default setting).

Note: When reset to defaults. The call forwarding settings will be configured as follows:

Always forward: Disabled

Busy forward to Voicemail: Enabled

No answer forward to Voicemail: Enabled

Do not disturb: Disabled

•Enable Forward All Calls

Users may enable always forward by calling *71 on their phone (*71 is the default setting)

•Disable Forward All Calls

Users may disable always forward by calling *071 on their phone (*071 is the default setting)

•Enable Forward When Busy

Users may enable busy forward by dialing *72 on their phone (*72 is the default setting)

•Disable Forward When Busy

Users may disable busy forward by calling *072 on their phone (*072 is the default setting)

•Enable Forward No Answer

Users may enable no answer forward by calling *73 on their phone (*73 is the default setting)

•Disable Forward No Answer

Users may disable no answer forward by calling *073 on their phone (*072 is the default setting)

•Forward to number

Users may activate call forwarding by dialing this feature code, followed by the extension or phone number to forward all calls to this number.

Note: Users may activate Forward to number by dialing *74 + phone number. E.g. by dialing *74501, all calls will be forwarded to extension 501.

•Forward to Voicemail

Users may forward the call to Voicemail by calling *074 on their phone (*074 is the default setting)

•Enable Do Not Disturb

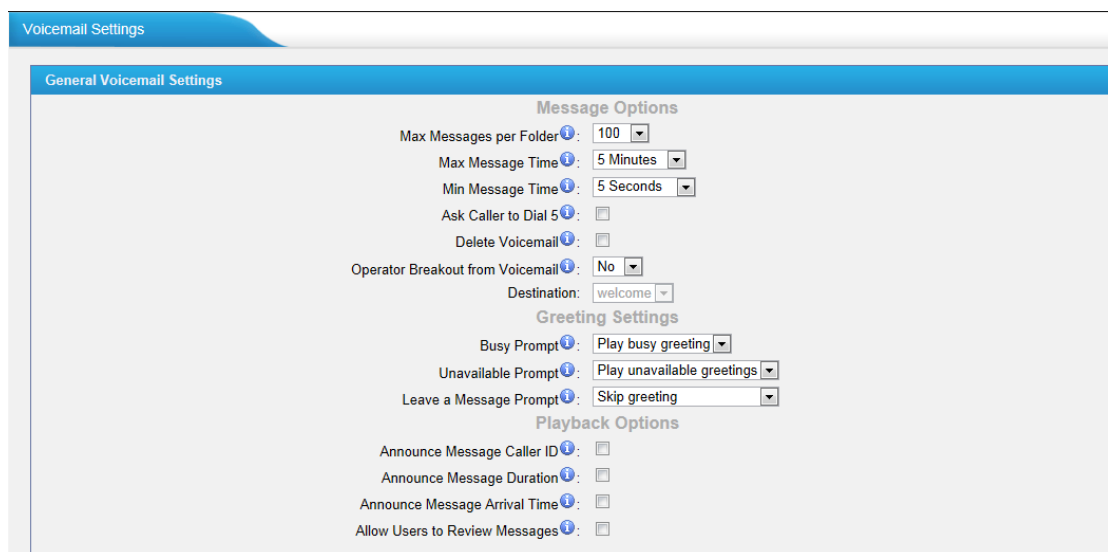
Users may enable do not disturb by calling *75 on their phone (*75 is the default setting)

•Disable Do Not Disturb

Users may disable do not disturb by calling *075 on their phone (*075 is the default setting)

6.6.4 Voicemail Settings

In this page, we can configure some settings for voicemail feature, including general voicemail settings and SMTP settings, which is used for "voicemail to email".



The screenshot displays the 'Voicemail Settings' interface. The 'General Voicemail Settings' section is active, showing the following options:

- Message Options**
 - Max Messages per Folder: 100
 - Max Message Time: 5 Minutes
 - Min Message Time: 5 Seconds
 - Ask Caller to Dial 5: ☐
 - Delete Voicemail: ☐
 - Operator Breakout from Voicemail: No
 - Destination: welcome
- Greeting Settings**
 - Busy Prompt: Play busy greeting
 - Unavailable Prompt: Play unavailable greetings
 - Leave a Message Prompt: Skip greeting
- Playback Options**
 - Announce Message Caller ID: ☐
 - Announce Message Duration: ☐
 - Announce Message Arrival Time: ☐
 - Allow Users to Review Messages: ☐

Figure 6-57

1) General Voicemail Settings

a) Message Options

•Max Messages per Folder

Set the maximum number of messages that can be stored in a single voicemail box.

•Max Message Time

Set the maximum length of a single voicemail message.

•Min Message Time

Set the minimum length of a single voicemail message. Messages below this threshold will be automatically deleted.

•Ask Caller to Dial 5

If this option is set, the caller will be prompted to press 5 before leaving a message.

•Operator Breakout from Voicemail

If this option is set, the caller can jump out of the voicemail and go to the destination (IVR) you set by dialing "0".

b) Greeting Settings

•Busy Prompt

Greeting played when the extension called is busy.

Skip greeting: Do not play a greeting.

Play busy greeting: play the extension busy greeting.

•Unavailable Prompt

Greeting played when the extension called is Unavailable.

Skip greeting: Do not play a greeting.

Play Unavailable greeting: play the extension Unavailable greeting.

•Leave a Message Prompt

Greeting played to ask the caller to dial 5 to leave a message.

Skip greeting: Do not play a greeting.

Play busy greeting: play the extension busy greeting.

Play Unavailable greeting: play the extension Unavailable greeting.

c) Playback Options

•Announce Message Caller ID

If this option is enabled, the Caller ID of the party that left the message will be played back before the voicemail message begins playing.

•Announce Message Duration

If this option is set, the duration of the message in minutes will be played back before the voicemail message begins playing.

•Announce Message Arrival Time

If this option is set, the arrival time of the message will be played back before the voicemail message begins playing.

•Allow Users to Review Messages

Allow callers to review their recorded message before sending it to voicemail.

2) SMTP Settings for Voicemail

Note: If you want to send voicemail messages as email attachments, please configure this section.

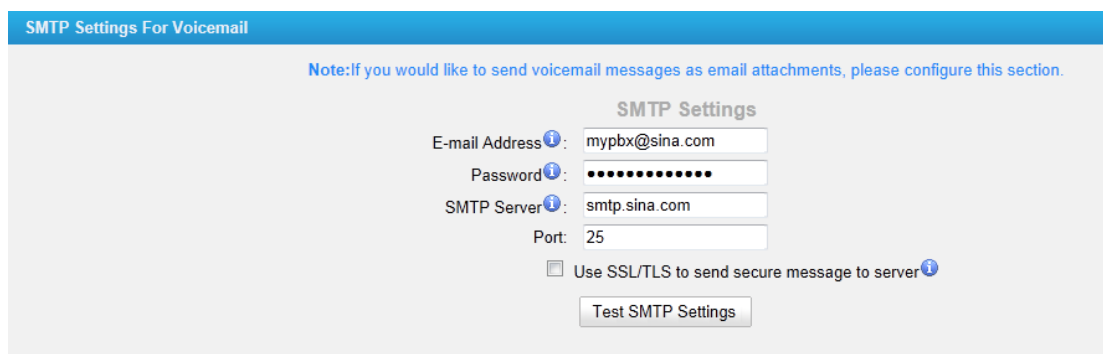


Figure 6-58

•E-mail Address

The E-mail Address that MyPBX will use to send voicemail.

•Password

The password for the email address used above

•SMTP Server

The IP address or hostname of an SMTP server that the MyPBX will connect to in order to send voicemail messages via email, e.g. mail.yourcompany.com.

•Port

SMTP Port: the default value is 25.

•Use SSL/TLS to send secure message to server

If the server of sending email needs to authenticate the sender, you need to select the check box.

Note: Must be selected for Gmail or exchange server.

After filling out the above information, you can click on the "Test Account

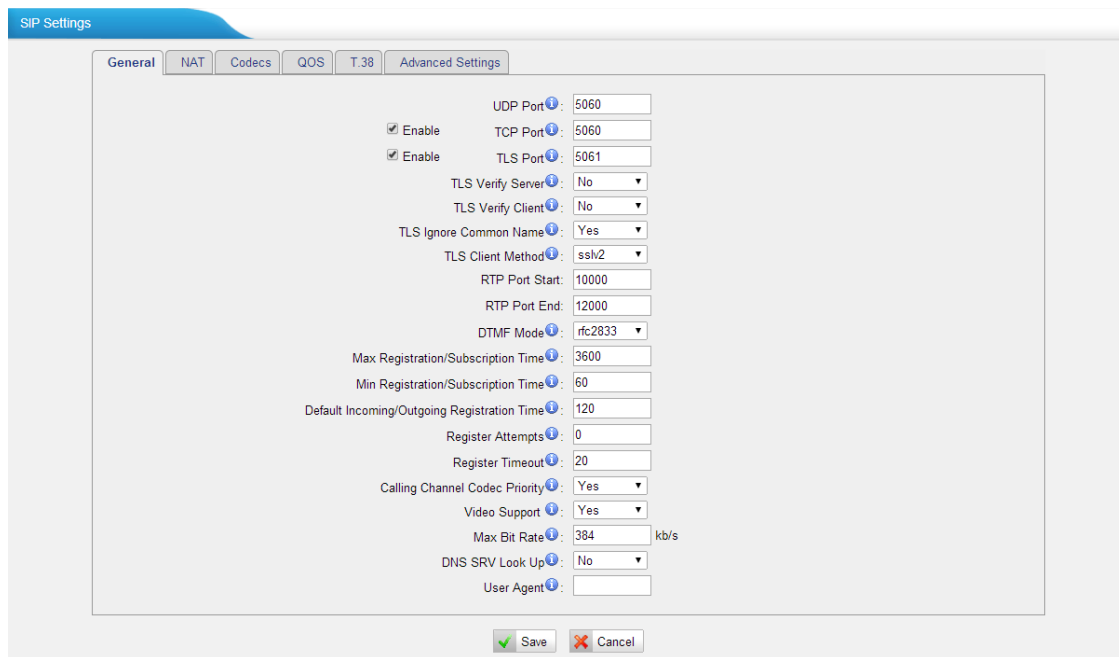
Settings" button to check whether the setup is OK.

- 1) If the test is successful, you can use the email safely.
- 2) If test failed, please check if the above information is correct or network is proper.

6.7 Advanced Settings

6.7.1 SIP Settings

1) General



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

- UDP Port: 5060
- ☒ Enable TCP Port: 5060
- ☒ Enable TLS Port: 5061
- TLS Verify Server: No
- TLS Verify Client: No
- TLS Ignore Common Name: Yes
- TLS Client Method: sslv2
- RTP Port Start: 10000
- RTP Port End: 12000
- DTMF Mode: rfc2833
- Max Registration/Subscription Time: 3600
- Min Registration/Subscription Time: 60
- Default Incoming/Outgoing Registration Time: 120
- Register Attempts: 0
- Register Timeout: 20
- Calling Channel Codec Priority: Yes
- Video Support: Yes
- Max Bit Rate: 384 kb/s
- DNS SRV Look Up: No
- User Agent:

At the bottom, there are 'Save' and 'Cancel' buttons.

Figure 6-59

•UDP Port

Port used for SIP registrations. The default is 5060.

•TCP Port

Port used for SIP registrations. The default is 5060.

•TLS Port

Port used for SIP registrations. The default is 5061.

•TLS Verify Server

When using MyPBX as a TLS client, whether or not to verify server's certificate. It is "No" by default.

•TLS Verify Client

When using MyPBX as a TLS server, whether or not to verify client's certificate. It is "No" by default.

•TLS Ignore Common Name

Set this parameter as "No", then common name must be the same with IP or

domain name.

•TLS Client Method

When using MyPBX as TLS client, specify the protocol for outbound TLS connections. You can select it as tlsv1, sslv2 or sslv3.

•RTP Port Start

Beginning of RTP port range.

•RTP Port End

End of RTP port range.

•DTMF Mode

Set default mode for sending DTMF. Default setting: rfc2833.

•Max Registration/Subscription Time

Maximum duration (in seconds) of a SIP registration. 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: Default duration (in seconds) of incoming/outgoing registration.

•Register Attempts

The number of SIP REGISTER messages to send to a SIP Registrar before giving up. Default is 0 (no limit).

•Register Timeout

Number of seconds to wait for a response from a SIP Registrar before considering 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 in preference. If not, MyPBX will follow the priority in your SIP/SPS trunks.

•Video Support

Support for SIP video or no. The default is yes.

•Max Bit Rate

Configure the max bit rate for video stream. The default: 384kb/s

•DNS SRV Look Up

Please enable this option when your SIP trunk contains more than one IP address.

•User Agent

To change the user agent parameter of asterisk, the default is "MyPBX"; you could change it if needed.

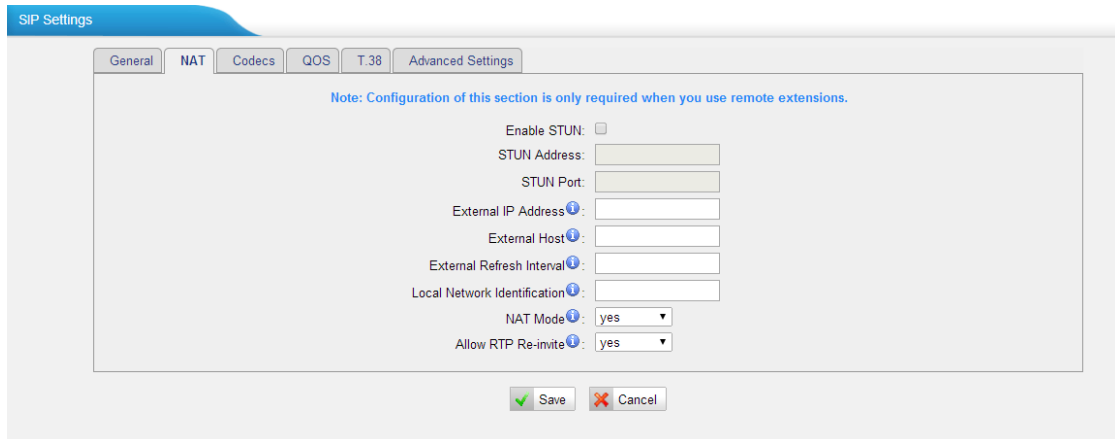
2) NAT

Figure 6-60

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

•Enable STUN

STUN (Simple Traversal of UDP through NATs) is a protocol for assisting devices behind a NAT firewall or router with their packet routing.

•STUN Address

The STUN server allows clients to find out their public address, the type of NAT they are behind and the Internet side port associated by the NAT with a particular local port. This information is used to set up UDP communication between the client and the VoIP provider and so establish a call.

•External IP Address

The IP address that will be associated with outbound SIP messages if the system is in a NAT environment.

•External Host

Alternatively you can specify an external host, and the system will perform DNS

queries periodically.

This setting is only required when your public IP address is not static. It is recommended that a static public IP address 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 Reinvite

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

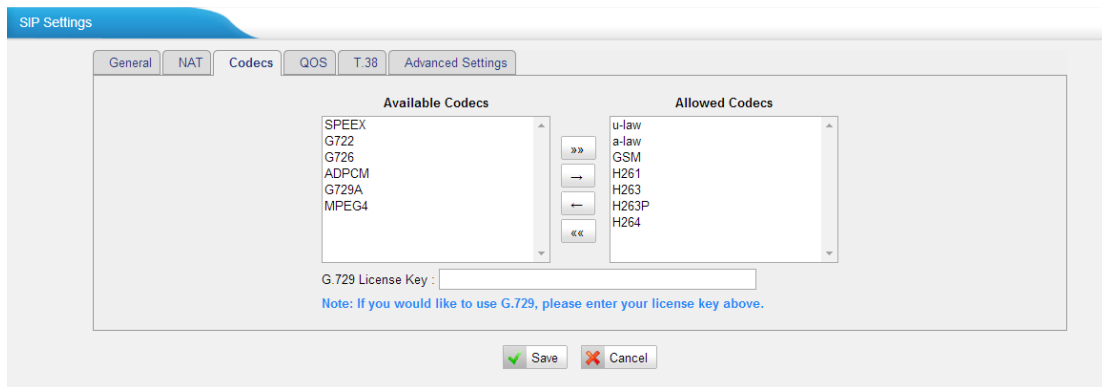


Figure 6-61

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

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

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

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

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

G.722: G.722 is a wideband speech coding algorithms which supports the bit rate of 64, 56 and 48kbps wideband. It's a broadband voice encoding of G series.

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

ADPCM, G.729A, H261, H263, H263p, H264, MPEG4.

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

4) QoS

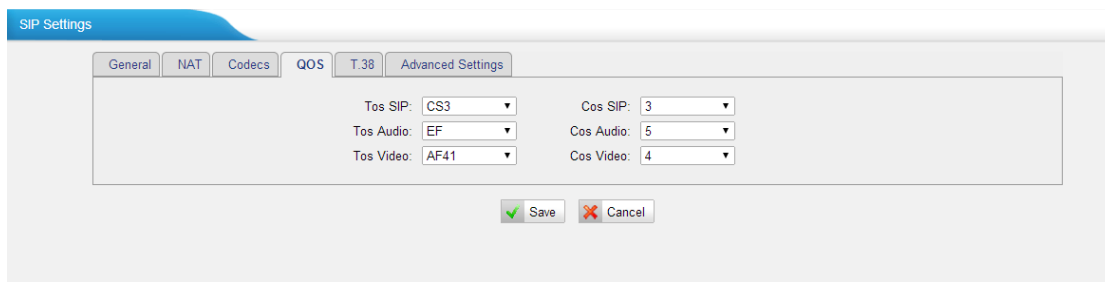


Figure 6-62

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 to interference from other lower priority traffic. When the network capacity is insufficient, QoS could provide priority to users by setting the value.

5) T.38

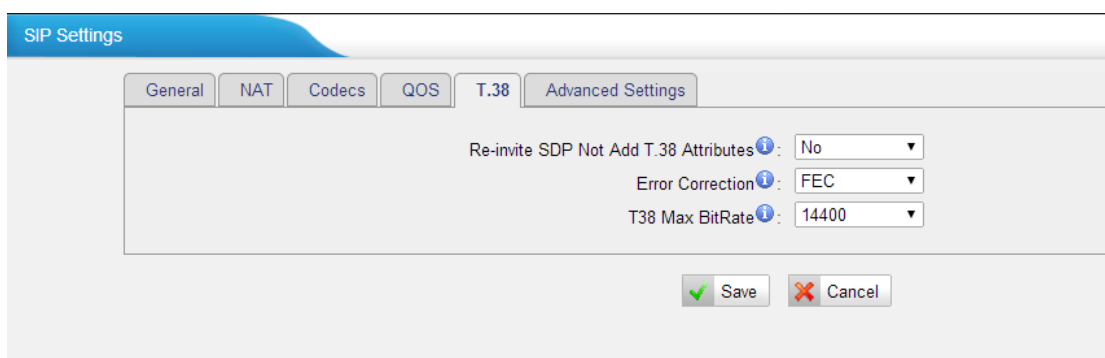


Figure 6-63

•Re-invite SDP Not Add T.38 Attributes

If set to Yes, SDP in re-invite packet will not add T.38 attributes.

•Error Correction

Re-invite SDP T38FaxUdpEc.

•T38 Max BitRate

Set T38 Max BitRate.

6) Advanced Settings

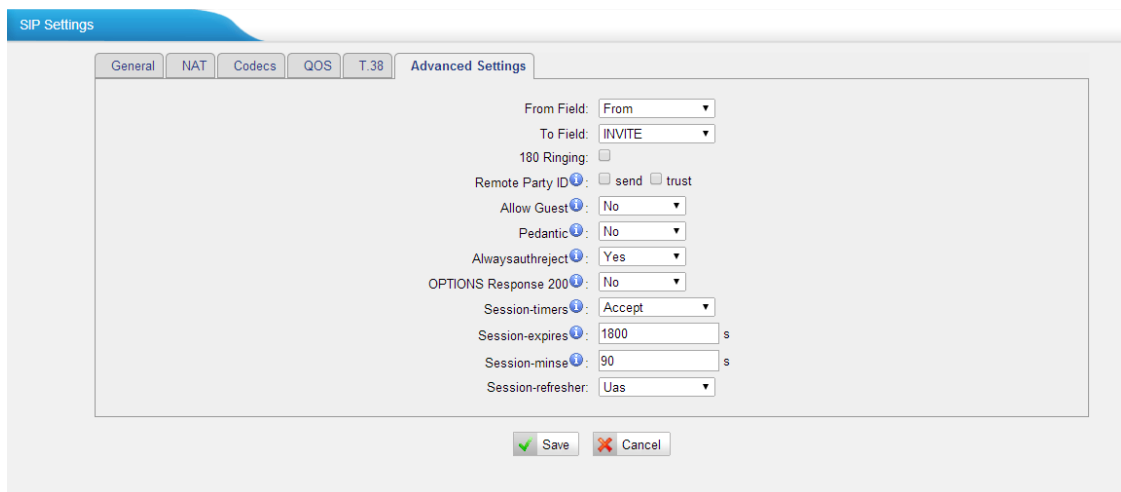


Figure 6-64

•From Field

Where to get the caller ID in SIP packet.

•To Field

Where to get the DID in SIP packet.

•180 Ringing

It is set when the telecom provider needs. Usually it is not needed.

•Remote Party ID

Whether to send Remote-Party-ID on SIP header or not. Default: no.

•Allow Guest

Whether to allow anonymous registration extension or not. Default: no.

This option is used to avoid some anonymous calls by hackers. For more details about the system security configuration, please refer to [APPENDIX B MyPBX Security Configuration Guide](#).

•Pedantic

Enable pedantic parameter. Default: no.

•Alwaysauthreject

If enabled, when MyPBX rejects "Register" or "Invite" packets, MyPBX always respond the packets using "SIP404 NOT FOUND".

•OPTIONS Response 200

If set to yes, the response to an OPTIONS is always 200 OK.

•Session -timers

Enable session-timer mode, default: yes.

•Session-expires

The max refresh interval.

•Session-minSE

The min refresh interval, which mustn't be less than 90s.

•Session-refresher

Choose session-refresher, the default is Uas.

6.7.2 IAX Settings

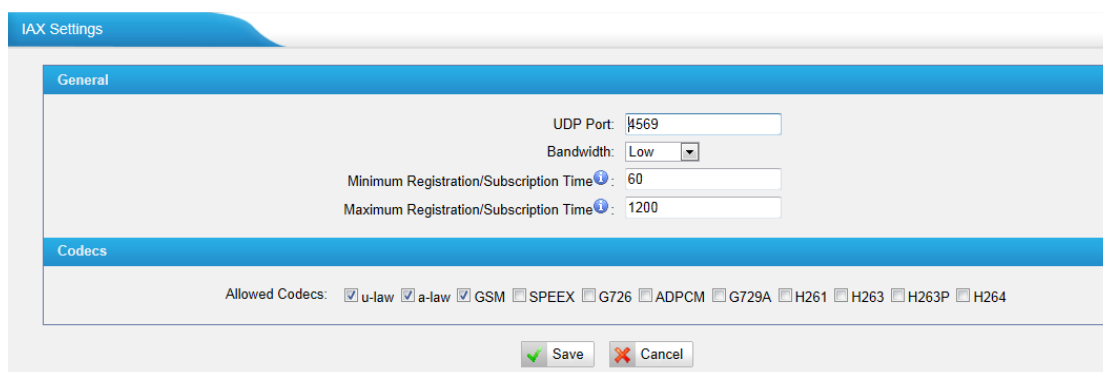


Figure 6-65

1) General

•Bind Port

Port used for IAX2 registrations. Default is 4569.

•Bandwidth

Low/medium/high with this option you can control which codec to be used.

•Min Registration Time

Minimum duration (in seconds) of an IAX2 registration. The default is 60 seconds.

•Max Registration Time

Maximum duration (in seconds) of an IAX2 registration. The default is 1200 seconds.

2) Codecs

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

u-law: A PSTN standard codec, used in North America, which provides very

good voice quality and consumes 64kbit/s in each direction (receiving and transmitting) of a VoIP call.

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

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

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

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

ADPCM, G.729A, H261, H263, H263p, H264.

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

6.7.3 Blacklist

Blacklist is used to block an incoming/outgoing call. If the number of incoming/outgoing call is registered 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.

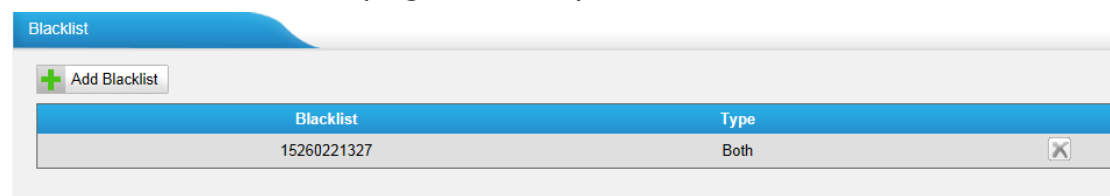
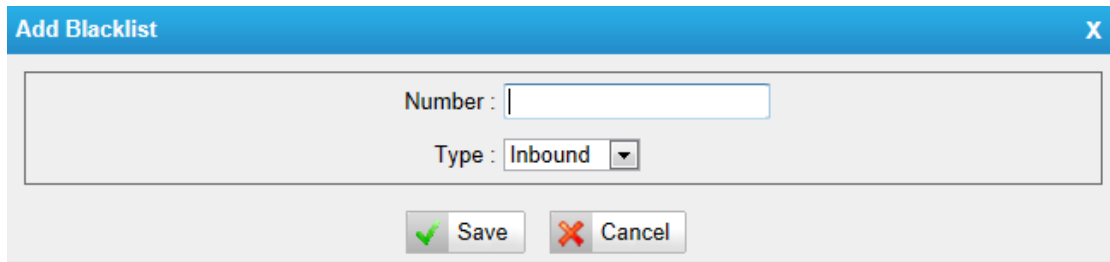


Figure 6-66

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



The 'Add Blacklist' dialog box has a blue header with the title 'Add Blacklist' and a close button 'X'. It contains a text input field labeled 'Number :', a dropdown menu labeled 'Type :' with 'Inbound' selected, and two buttons at the bottom: 'Save' with a green checkmark icon and 'Cancel' with a red X icon.

Figure 6-67

Note: Add a phone number in blacklist, such as "05921234567":

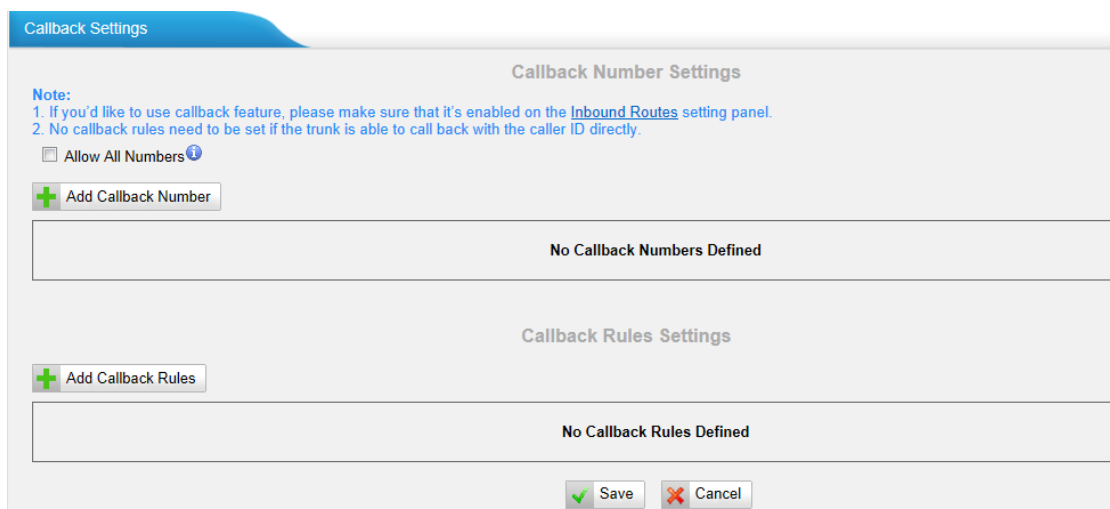
- 1) If the type is "inbound", then this number can't be called.
- 2) If the type is "outbound", then the extensions in MyPBX can't call this number.

6.7.4 Callback Settings

MyPBX allows caller A to dial an inbound route number, and after hearing the ring, A can hang up the call or wait for MyPBX to cut off the call, then MyPBX will call A with this number. When A picks up the call, A can dial the number he wants to call; MyPBX will call the number with its outbound route.

Notes:

1. If you'd like to use callback feature, please make sure it's enabled on the inbound route setting panel.
2. No callback rules needed to be set if the trunk supports call back with the caller ID directly.



The 'Callback Settings' panel has a blue header with the title 'Callback Settings'. It contains a 'Note' section with two points: '1. If you'd like to use callback feature, please make sure that it's enabled on the [Inbound Routes](#) setting panel.' and '2. No callback rules need to be set if the trunk is able to call back with the caller ID directly.' Below the note is a checkbox labeled 'Allow All Numbers' with an information icon. There are two sections: 'Add Callback Number' with a green plus icon and a button, and 'Add Callback Rules' with a green plus icon and a button. Both sections show 'No Callback Numbers Defined' and 'No Callback Rules Defined' respectively. At the bottom are 'Save' and 'Cancel' buttons.

Figure 6-68

•Allow All Numbers

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

Follow the steps below to use this function.

Step 1: Enable Callback.

Inbound Routes—Choose “Yes” on “Enable Callback” to enable this function.

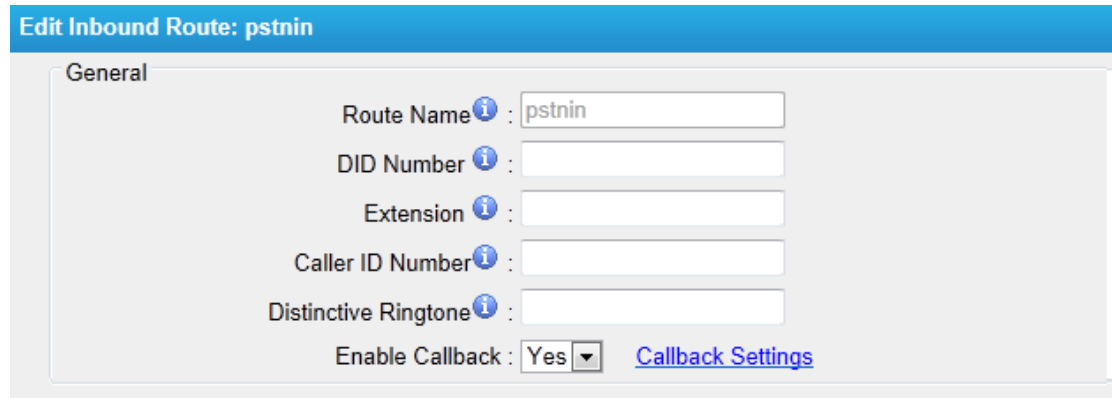


Figure 6-69

Step 2: Create Callback number.

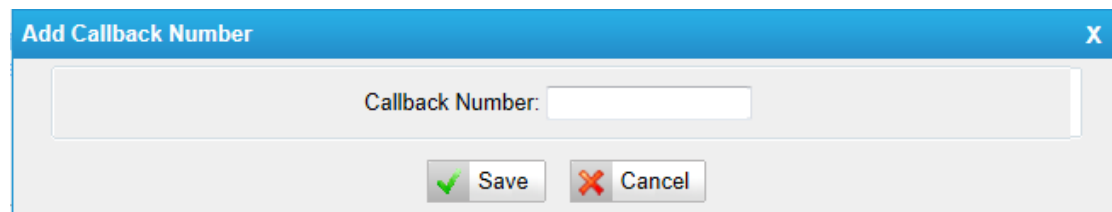


Figure 6-70

Step 3: Create Callback Rules

You will need to create callback rules when the system should strip or add digits.

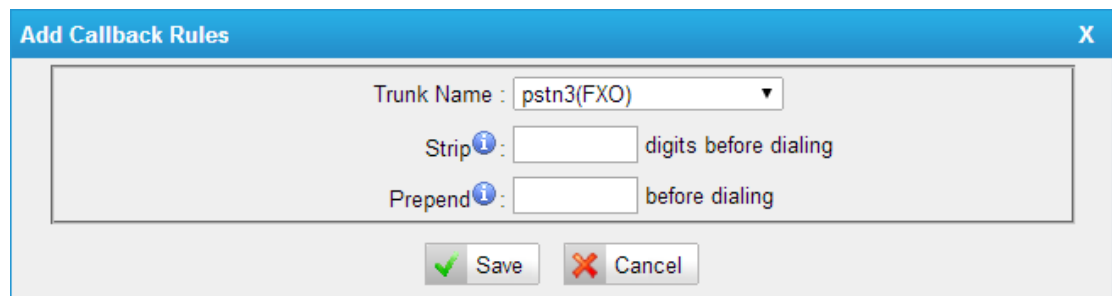


Figure 6-71

•Trunk Name

Choose the trunk with callback rules.

•Strip digits from front

Define how many digits will be stripped from the call in number before the callback is placed. For example, when you call from number 123456789 into MyPBX, the caller ID is 0123456789, but you can only call 123456789 successfully from MyPBX trunk. You should configure number 0123456789 as the call back number and strip 1 digit before the callback is placed.

•Prepend before dialing

Define digits added before a callback number before the callback is placed. For example, the call in number (Caller ID) is 123456789, MyPBX need to send 9123456789 to its trunk when calling this number. You should configure 123456789 as the callback number and add 9 before the callback is placed. You can add "w" for analog trunks for some delay too.

6.7.5 DNIS Settings

DNIS (Dialed Number Identification Service) is a telephone service that identifies for the receiver of a call the number that the caller dialed.

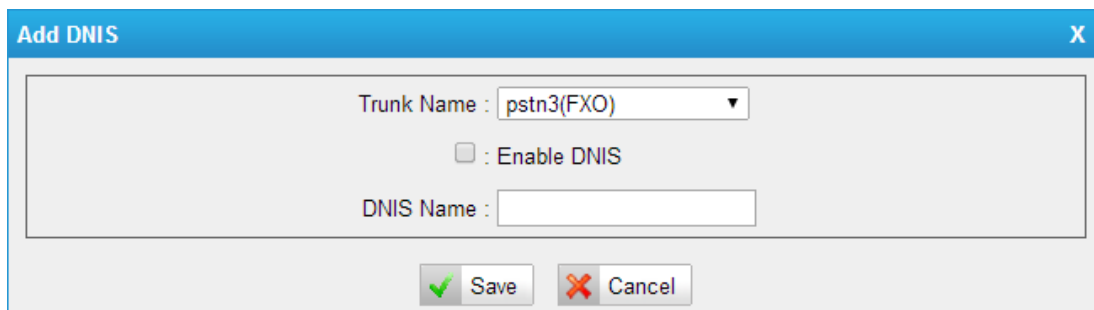


Figure 6-72

Note: If DID is not configured here, all the calls via this trunk will show the DNIS instead of the original caller ID.

6.7.6 DISA

DISA (Direct Inward System Access) allows someone calling in from outside the telephone switch (PBX) to obtain an "internal" system dial tone and make calls as if they were using one of the extensions attached to the telephone switch. To use DISA, a user calls a DISA number, which invokes the DISA application. The DISA application in turn requires the user to enter a PIN number, followed by the pound sign (#). If the PIN number is correct, the user will hear dial tone on which a call may be placed. Obviously, this type of access has serious security implications, and great care must be taken not to compromise your security.

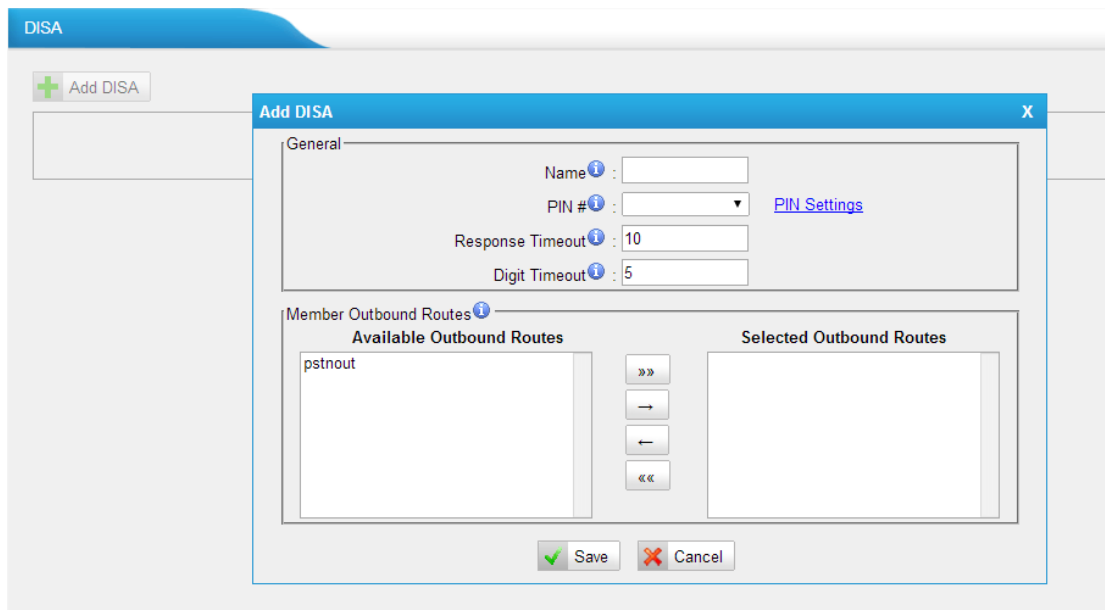


Figure 6-73

1) General

•DISA Name

Give this DISA application a name to help you identify it.

•PIN

The password for this DISA.

•PIN Settings

Click to add, delete or edit PIN list.

•Response Timeout

The maximum amount of time the system will wait before hanging up the call if the user has dialed an incomplete or invalid number. The default is 10 seconds.

•Digit Timeout

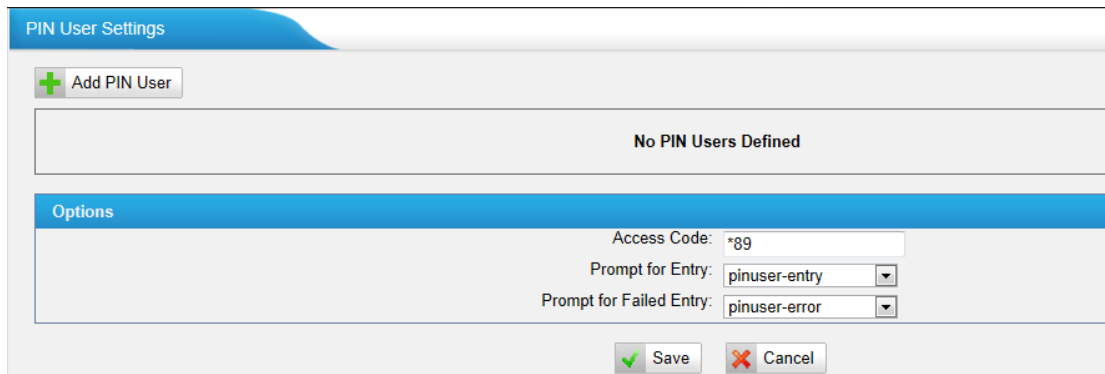
The maximum amount of time permitted between each digit when the user is dialing an extension number. The default is 5 seconds.

2) Member Outbound Routes

Used to set the outbound routes that can be accessed from this DISA.

6.7.5 PIN User Settings

PIN User is used to manage lists of PINs that can be used to access restricted features such as Outbound Routes.



The screenshot shows the 'PIN User Settings' window. At the top, there is a tab labeled 'PIN User Settings'. Below the tab, there is a button labeled '+ Add PIN User'. In the center, a message states 'No PIN Users Defined'. Below this, there is an 'Options' section with three fields: 'Access Code' with the value '*89', 'Prompt for Entry' with a dropdown menu showing 'pinuser-entry', and 'Prompt for Failed Entry' with a dropdown menu showing 'pinuser-error'. At the bottom right of the 'Options' section, there are 'Save' and 'Cancel' buttons.

Figure 6-74

1) Options

•Access Code

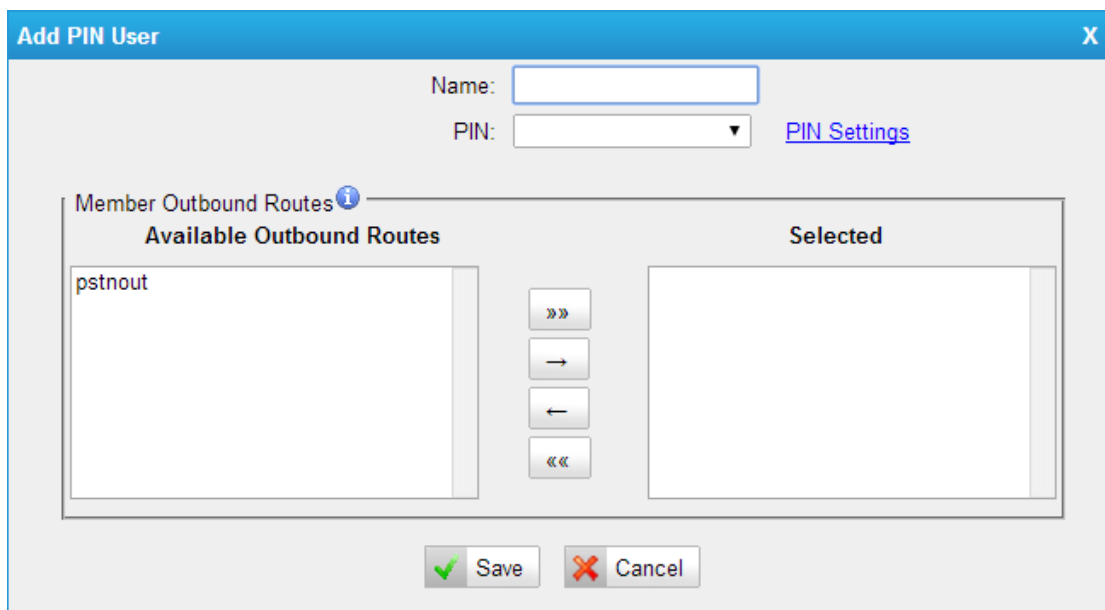
Dial this code to access PIN.

•Prompt for Entry

Prompt caller to enter the PIN Number.

•Prompt for Entry Failure

Prompt the caller when an invalid PIN is entered.



The screenshot shows the 'Add PIN User' window. At the top, there is a title bar with 'Add PIN User' and a close button 'X'. Below the title bar, there are two input fields: 'Name:' and 'PIN:'. To the right of the 'PIN:' field, there is a link labeled 'PIN Settings'. Below these fields, there is a section titled 'Member Outbound Routes' with an information icon. This section contains two lists: 'Available Outbound Routes' and 'Selected'. The 'Available Outbound Routes' list contains the item 'pstnout'. Between the two lists are four buttons: '>>>', '→', '←', and '<<<'. At the bottom of the window, there are 'Save' and 'Cancel' buttons.

Figure 6-75

2) PIN User

MyPBX can store a number of PIN Users. PIN Users may be used to keep track of calls in relation to particular activities or clients. They can also be used to keep track of calls by particular users or sets of users.

- PINs entered are checked against those stored by the system. If an invalid PIN is entered, the PIN is requested again.

- The system administrator can configure certain numbers or types of numbers to require entry of a PIN before users can continue making a call to such a number.
- The system administrator can also configure to require users to enter a PIN before making any external call.

•Name

A character-based name for this PIN list, e.g. "YeastarPIN"

•PIN

The password for this PIN list

•PIN Settings

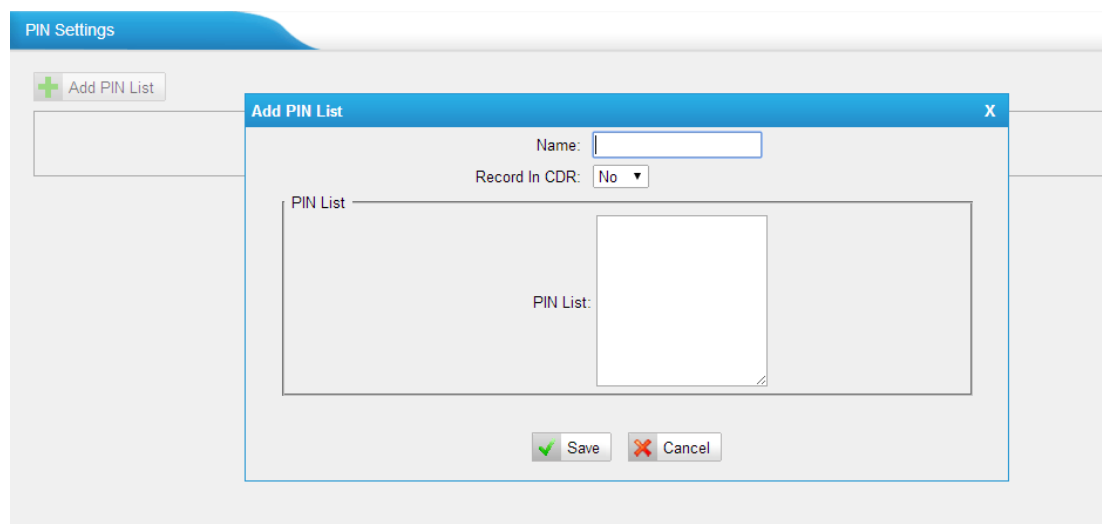
Click to add, delete or edit PIN list.

•Member Outbound Route

PIN User can use those outbound route to make call out.

6.7.8 PIN Settings

In this page users can manage all the passwords of outbound routes, PIN User, and DISA.



The screenshot shows the 'PIN Settings' page with a blue header. On the left, there is a button labeled '+ Add PIN List'. A modal dialog box titled 'Add PIN List' is open in the center. The dialog has a blue header with a close button (X). Inside the dialog, there is a 'Name:' text input field, a 'Record In CDR:' dropdown menu set to 'No', and a large text area labeled 'PIN List:'. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons with green and red icons respectively.

Figure 6-76

•Name

A character-based name for this PIN list, e.g. "YeastarPIN"

•Record in CDR

If set yes, the PIN code will be displayed in call log.

•PIN list

PIN list is a numeric field. Letters and punctuation are not allowed in this field. Fill in one PIN and if you end with enter for each PIN, you could create multiple PINs.

6.7.9 Paging Groups

Paging is used to make an announcement over the speakerphone to a phone or group of phones. Targeted phones will not ring, but instead answer immediately into speakerphone mode. Please note that this section is for configuring paging groups. If you would like to configure Intercom settings, please open the Other Settings -> Feature Codes screen.

This feature is supported by the following SIP phones:

Yealink's T28, T26, T22, T20, T10T, T9CM. Other SIP devices may also work with this feature but are not officially supported.

Note: A paging group can have a maximum of 20 members.

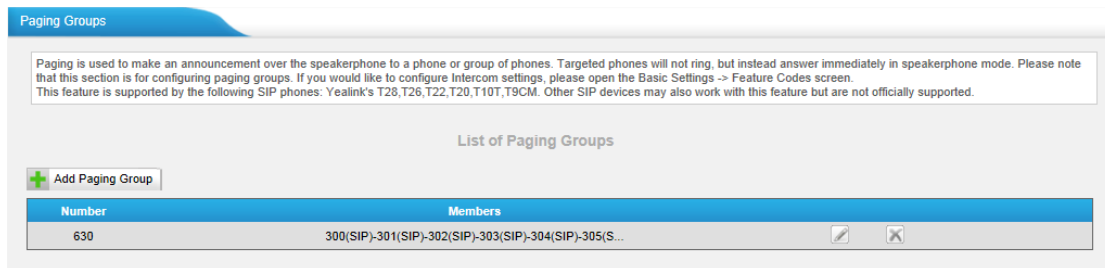


Figure 6-77

In this mode, if you dial its number, MyPBX will help to pick up those chosen members and you can talk directly without any rings.

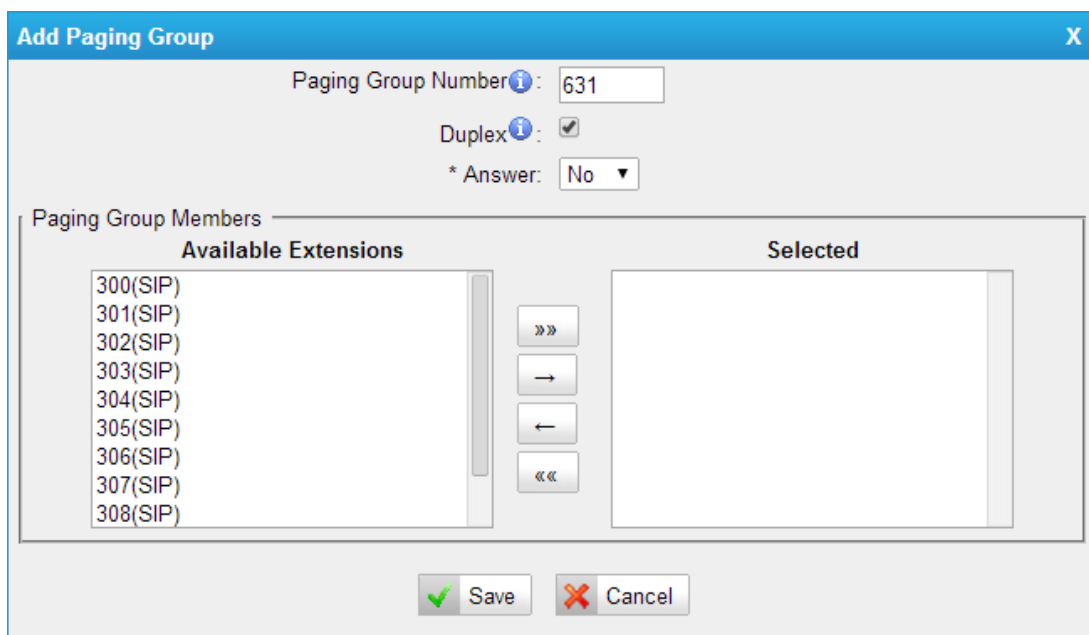


Figure 6-78

•Paging Group Number

Define the numbered extension that may be dialed to reach this group.

•Duplex

Paging is typically one way for announcements only. Checking this will make paging duplex, allowing all users in the group to talk and be heard by all.

•*Answer

If it sets Yes, any user in the group will talk with the caller when they press "*". If it sets No, users in the group can talk with each other without pressing "*".

6.7.10 Certificates

MyPBX can support TLS extension. Before you register TLS extension on IP phone, you should upload certificates first.

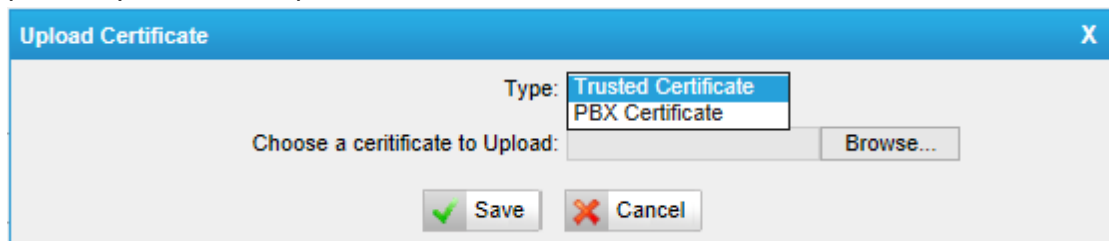


Figure 6-79

Trusted Certificate

This certificate is a CA certificate. When selecting "TLS Verify Client" as "Yes", you should upload a CA. The relevant IP phone should also have this certificate.

PBX Certificate

This certificate is server certificate. No matter selecting "TLS Verify Client" as "Yes" or "NO", you should upload this certificate to MyPBX. If IP phone enables "TLS Verify server", you should also upload the relevant CA certificate on IP phone.

7. Reports

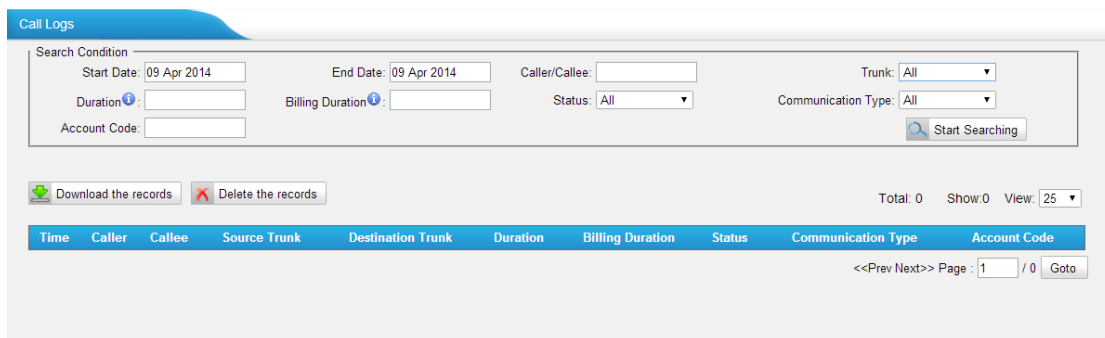


Click [Reports](#) to access.

We can check the call detailed logs for accounting and system log for debugging.

7.1 Call Logs

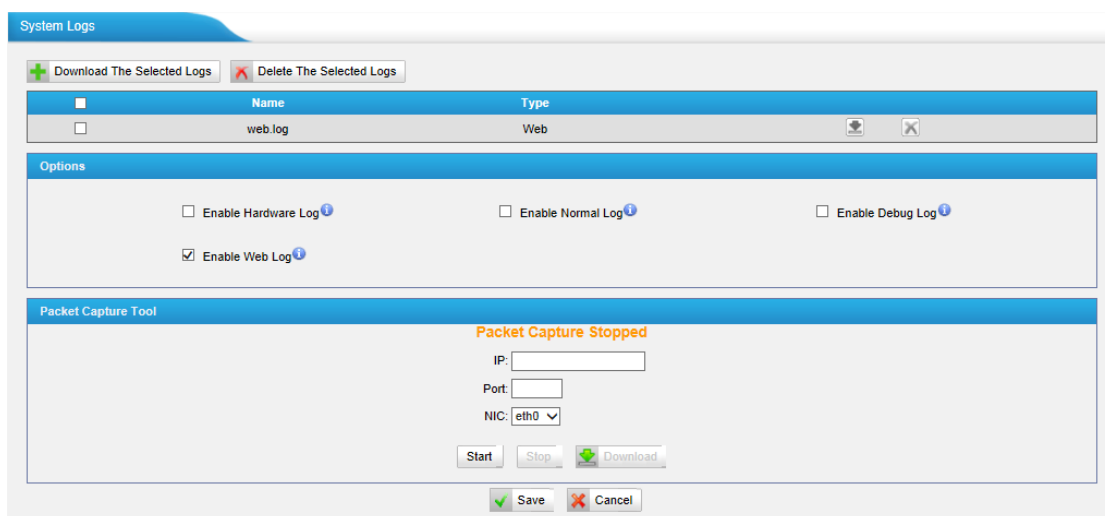
The call Log captures all call details, including call time, caller number, callee number, call type, call duration, etc. An administrator can search and filter call data by call date, caller/callee, trunk, duration, billing duration, status, communication type and Pin User.



The screenshot shows the 'Call Logs' interface. It features a search bar with fields for Start Date (09 Apr 2014), End Date (09 Apr 2014), Caller/Callee, Trunk (All), Duration, Billing Duration, Status (All), and Communication Type (All). A 'Start Searching' button is present. Below the search bar are buttons for 'Download the records' and 'Delete the records'. A summary bar shows 'Total: 0', 'Show: 0', and 'View: 25'. A table header lists columns: Time, Caller, Callee, Source Trunk, Destination Trunk, Duration, Billing Duration, Status, Communication Type, and Account Code. A pagination bar at the bottom shows '<<Prev Next>>' and 'Page: 1 / 0' with a 'Goto' button.

Figure 7-1

7.2 System Logs



The screenshot shows the 'System Logs' interface. It has buttons for 'Download The Selected Logs' and 'Delete The Selected Logs'. A table lists logs with columns 'Name' and 'Type', showing 'web.log' as 'Web'. Below the table is an 'Options' section with checkboxes for 'Enable Hardware Log', 'Enable Normal Log', 'Enable Debug Log', and 'Enable Web Log' (which is checked). At the bottom is a 'Packet Capture Tool' section with a status 'Packet Capture Stopped', fields for IP, Port, and NIC (set to eth0), and buttons for 'Start', 'Stop', 'Download', 'Save', and 'Cancel'.

Figure 7-2

You can download and delete the system logs of MyPBX.

Options

•Enable Hardware Log

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

•Enable Normal Log

Save the prompt information (up to 16 log files).

•Enable Web Log

Save the history of web operations (up to 2 log files).

•Enable Debug Log

Save debug information (up to 2 log files).

Packets Capture Tool

This feature is used by technician to capture packets. Packet capture tool "Wireshark" is integrated in MyPBX.

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

•IP

Specify the destination IP address to get the packets.

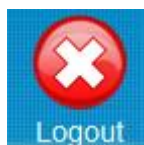
•Port

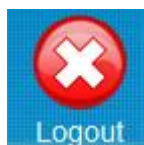
Specify the destination Port to get the packets.

•NIC

Choose the NIC (LAN or WAN) which you want to capture the packets.

8. Logout



Click  to log out safely.

9. Use MyPBX

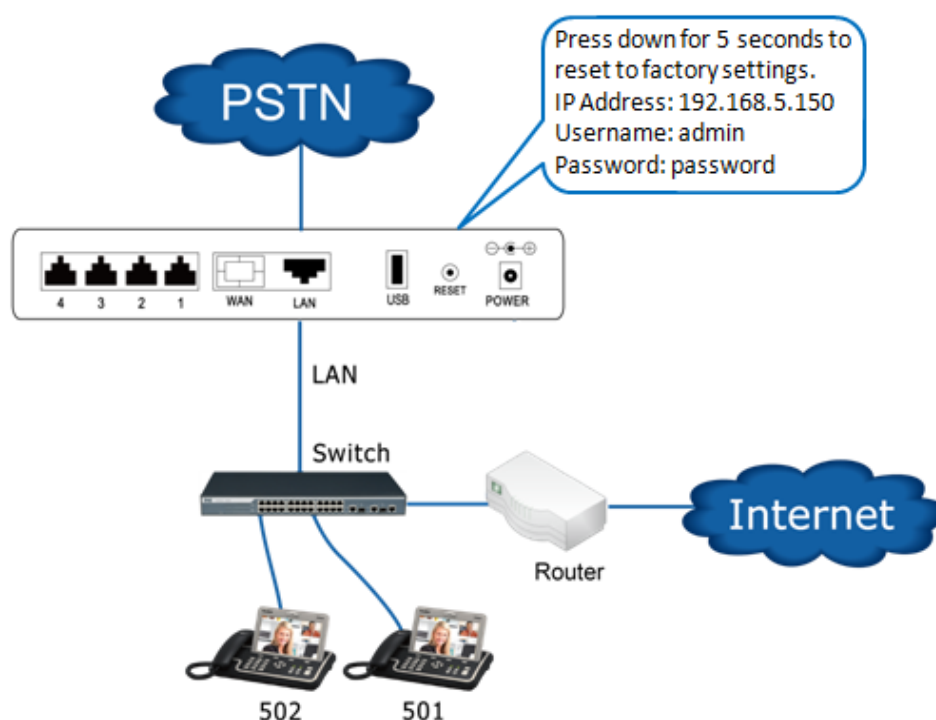


Figure 9-1

9.1 Make outbound calls

To make an outbound call, we need to add a trunk first. There are 3 types of VoIP Trunk:

- VoIP Trunk:** Connected to remote VoIP service server.
You should get an IP address with user name/ password from the provider.
- Service Provider:** Connected to service provider server.
You will get only IP address for authorization.
- Analog Trunk:** FXO ports of MyPBX, connected to a local PSTN.

•**BRI Trunk:** BRI ports of MyPBX, connected to ISDN provider

What are FXO and FXS?

FXS (Foreign exchange Station) is an interface which drives an analog telephone or FAX machine. FXS interfaces deliver power, provide ringing, and use FXO signaling. FXS interfaces are what allow you to hook telephones and other analog devices to your PBX

FXO (Foreign exchange Office) is an interface that connects to a phone line to supply your PBX with access to a public telephone network. FXO interfaces use FXS signaling. FXO interfaces allow you to connect your PBX to real analog phone lines.

Sample Routing via VoIP Trunk

Let's configure all inside extensions to dial "0" through the VoIP Trunk.

1. Add VoIP service provider

Before we do add this, please make sure you have a VoIP Trunk account.

Trunks → VoIP Trunk → SIP Trunk

Enter your account information on this page, and click Save.

Edit VoIP Trunk - VOIP_Supplier

Provider Name: VOIP_Supplier
Hostname/IP: catnextgen.com
Domain: catnextgen.com
User Name: +6621070164
Authorization Name: 6621070164@catnextgen.com
Password:
From User:
Online Number:
Maximum Channels: 0
Caller ID: +6621070164
Realm:
☒ Enable Outbound Proxy Server
Outbound Proxy Server: 202.129.61.102 Port: 5060
Codecs: First: a-law Second: u-law Third: GSM
Fourth: None Fifth: None
Transport: UDP Enable SRTP: ☐ Qualify: ☒
DTMF Mode: rfc2833

DOD Settings

DOD:
Associated Extension: 601
Add DOD

Save Cancel

Figure 9-2

2. Add Outbound Routes

As we can see from the Outbound Route of "VOIP_OUT", all phone numbers starting with 0 will have their first digit stripped off (digit 0) and will be sent to the SIP Trunk.

Add Outbound Route
X

Route Name : VOIP_OUT
Dial Pattern : 0.
Strip : digits from front
Prepend these digits : before dialing
Password :
T.38 Support : No
Rmemory Hunt : No
Office Hours :

Member Extensions

Available Extensions

Selected

300(SIP)
301(SIP)
302(SIP)
303(SIP)
304(SIP)
305(SIP)
601(FXS)
602(FXS)

Member Trunks

Available Trunks

Selected

pstn11(FXO)
pstn12(FXO)
pstn13(FXO)
pstn14(FXO)
pstn15(FXO)
pstn16(FXO)
E1Trunk1(E1)
E1Trunk2(E1)

VOIP_Supplier(SIP)

Save Cancel

Figure 9-3

Now that we have added two outbound dialing rules, any call starting with 9 will be routed to the PSTN, and any number starting with 0 will be routed to the SIP Trunk.

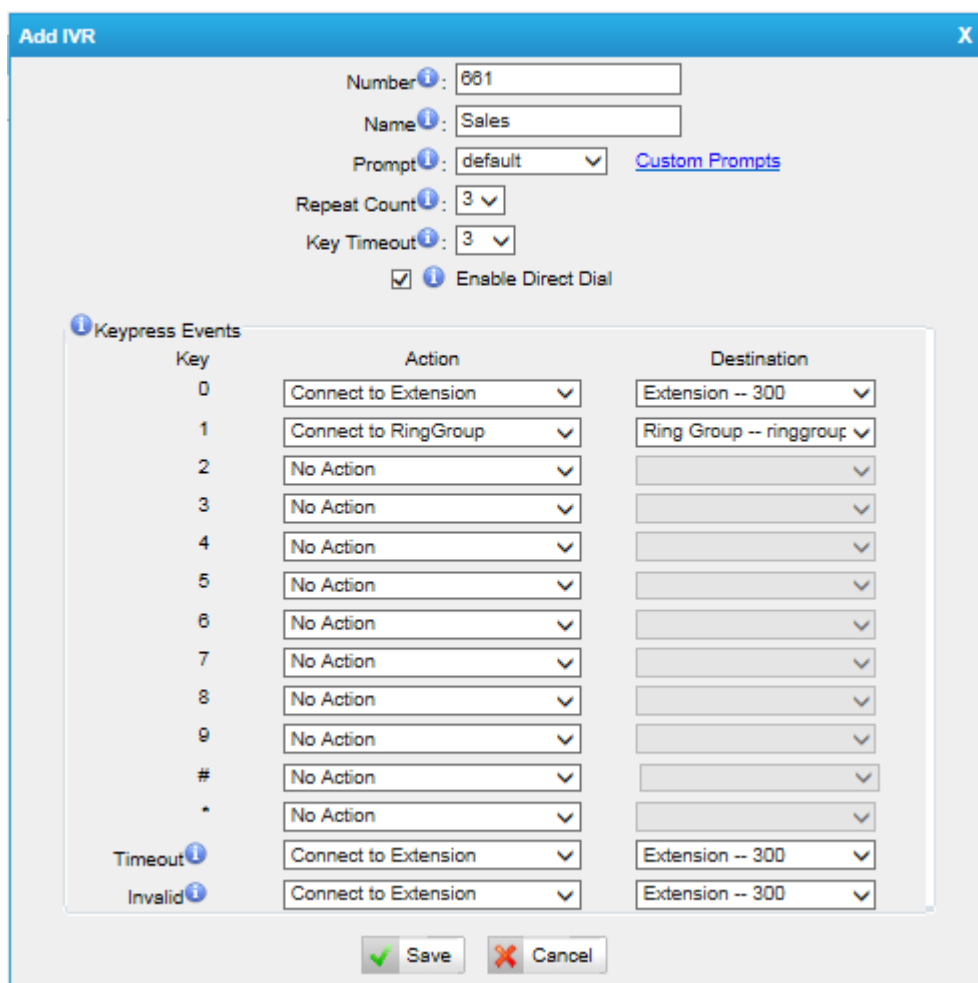
9.2 Incoming call

Sample Routing to an IVR

Let's configure an incoming call to route to the IVR. In the IVR itself, let's configure digit 0 to route the call to extension 300, and digit 1 to route the call to ringgroup.

1. Add IVR

To add a new IVR, go to IVR→ Create New IVR.



Key	Action	Destination
0	Connect to Extension	Extension -- 300
1	Connect to RingGroup	Ring Group -- ringgroup
2	No Action	
3	No Action	
4	No Action	
5	No Action	
6	No Action	
7	No Action	
8	No Action	
9	No Action	
#	No Action	
*	No Action	
Timeout	Connect to Extension	Extension -- 300
Invalid	Connect to Extension	Extension -- 300

Figure 9-4

2. Add Inbound Routes

As we can see from the Inbound Route of "VOIP_IN", all incoming calls from VoIP trunk will be sent to the IVR.

Add Inbound Route
X

General

Route Name : VOIP_IN
DID Number :
Extension :
Caller ID Number :
Distinctive Ringtone :
Enable Callback : No [Callback Settings](#)

Member Trunks

Available Trunks		Selected
pstn9(FXO)		114.132.246.190(SIP)
pstn10(FXO)		
GSM15(GSM)		
BnTrunk7(BRI)		
BnTrunk8(BRI)		
147(SPS)		
192.168.5.142(SPS)		
sps599(SPS)		

Business Days

Office Hours : default
Office Hours Destination : IVR IVR -- welcome
Non-office Hours Destination : End Call

During Holidays

Holiday :
Destination : End Call

Fax Detection

Destination : No Detect

Save Cancel

Figure 9-5

APPENDIX A FAQ

Q1. How to Register SIP device?

A1:

1) Register SIP soft phone

Download the x-lite softphone from CounterPath website

www.counterpath.com

After installing the x-lite, right click the panel and select the SIP Account setting and then configure it.

Display Name: 500

User Name: 500

Password: 500

Authorization Name: 500

Domain: 192.168.5.150

2) Register IP Phone (for example, Yealink's T28 IP Phone)

a) Connect the T28's Internet port to the switch. And it can get the IP from your route.

b) Press the "OK" key on T28 to get the IP of T28.

c) Put the IP on web browser then you can enter the T28 configure page through this IP.

d) Put the SIP extensions info on the T28 IP phones.

Display Name: 501

User Name: 501

Register Name: 501

Password: 501

SIP Server: 192.168.5.150

Use the same method register another T28 to other extension.

Q2. How do I reset MyPBX back to the factory default settings?

A2: To perform a reset, please follow the steps below:

Step 1: Press down the "Reset" button on the back of the unit for 5 seconds and watch the LEDs on the front of the MyPBX. When the status LED turns red, let go of the reset button.

Step 2: When the RUN status LED starts blinking, MyPBX will be set back to factory defaults.

Step 3: To access the configuration page, navigate to **192.168.5.150** using a Web browser. Make sure that you are on the 192.168.5.0 subnet before doing this.

Step 4: Login to the device with the username "**admin**" and the password "**password**", and reconfigure the device.

APPENDIX B How to Configure External Storage

Before External storage can be properly configured, an SMB share folder accessible from MyPBX must be set up on a Windows based machine. Once that has been set up, please follow the steps below.

Step 1 Add a new folder, rename it, and set this new folder's share Properties according to Figure B-1.

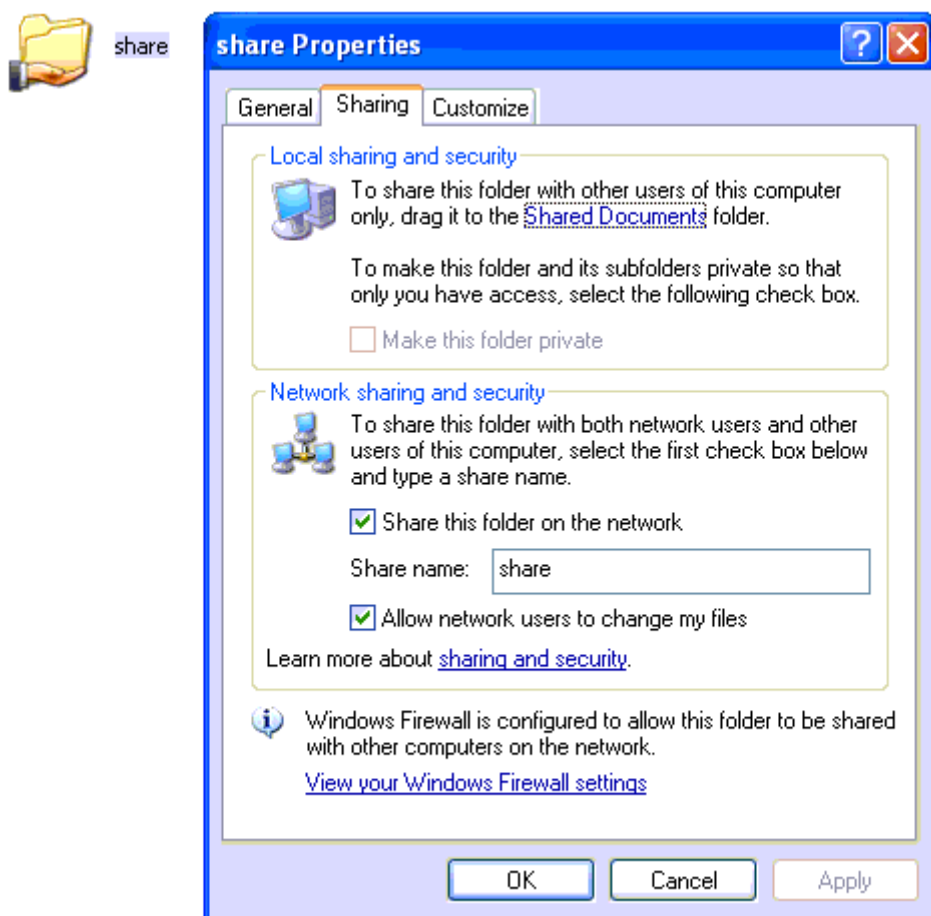


Figure B-1 Set up share Properties

Step 2 Enter the new folder and create a new text file, then rename this file to status.txt. This step is very important, DO NOT forget to create the status.txt file.

Step 3 Configure External storage settings on MyPBX to Figure B-2.

External Storage Settings

The External Storage feature is used to extend storage space. Once configured, the files(voicemail, call recording files, CDR files) created before the configured days will be moved to the Net-Disk.

Step 1: Create a Net-Disk on a chosen computer

Step 2: Input the Net-Disk properties

Net-Disk Host/IP:

Net-Disk Share Name:

Net-Disk Access Username:

Net-Disk Access Password:

Move files created before: days ago

Step 3: Save Net-Disk settings

Step 4: Make sure the settings are successfully completed

Figure B-2 External Storage Setting

Net-Disk Host/IP: Change this to the IP address of the computer where backup files will be stored.

Net-Disk Share Name: Change this to the name of the shared folder where backups will be stored.

Net-Disk Share Username: The user name used to log into the network share. Leave this blank if it is not required

Net-Disk Share Password: The password used to log into the network share. Leave this blank if it is not required

Open your Windows share folder to see if the MyPBX backup files and folders has been created. If the contents of the backup folder look similar to Figure B-3, then you have successfully configured External storage on the MyPBX unit.

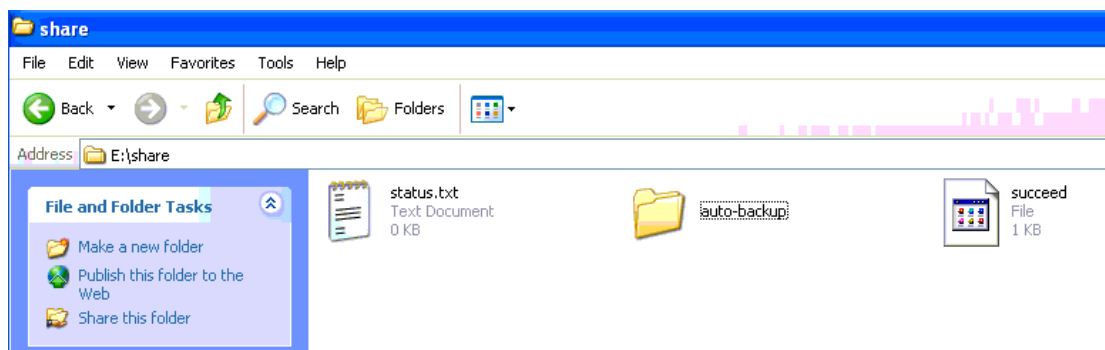


Figure B-3 External storage setting succeeds

APPENDIX C How to Configure NAT Setting

When MyPBX is behind a NAT (firewall), you need to configure NAT setting on MyPBX if you want to use a remote extension.

Please follow section **1** or **2** below depending on your network configuration.

1. If MyPBX is connected to a local network, you must set up port forwarding on your router. Specifically, you must map port 5060 (default SIP port) and port 10001-10200 (default RTP port range) as UDP ports.

Next, log in MyPBX Web GUI, go to "PBX" -> "Advanced Settings" -> "SIP Settings" -> "NAT"

External IP Address: your router's public IP address

External Host: your router's domain

External Refresh Interval: 20 seconds

Local Network Identification: 192.168.5.0/255.255.255.0 (change this according to your network configuration)

NAT mode: Yes

Allow RTP Reinvite: Yes

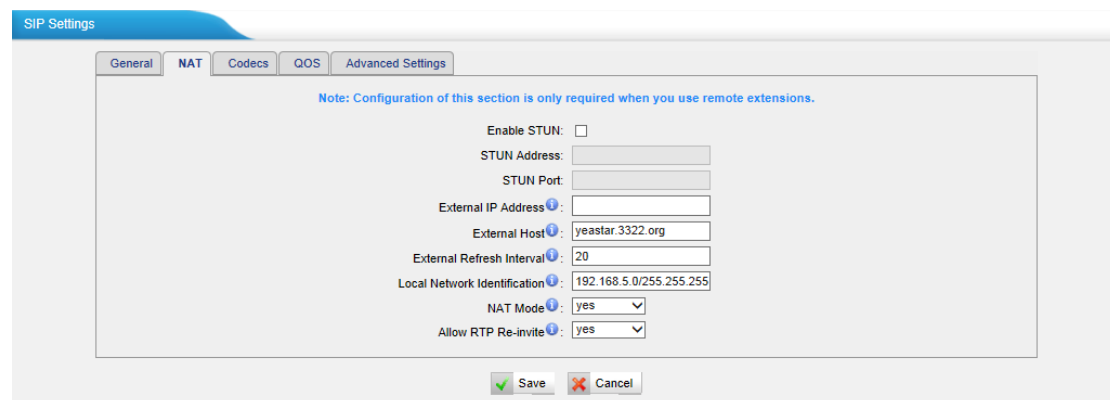


Figure C-1

Assuming that your router's host address is yeastar.3322.org, your local network is from 192.168.5.1-192.168.5.254, and the subnet Mask is 255.255.255.0, the MyPBX network settings should be configured like Figure C-2.

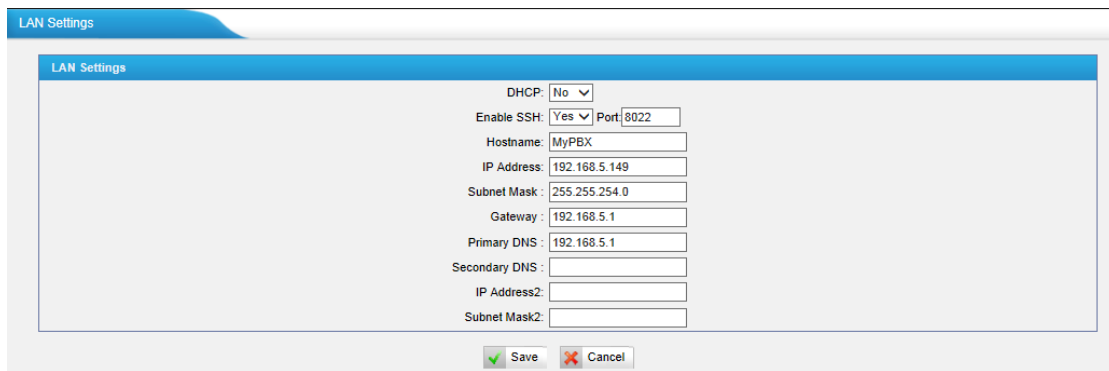


Figure C-2 MyPBX Network setting

2. If MyPBX has a public IP (i.e. is connected directly to your Internet service provider), the network settings should be configured according to Figure C-3:

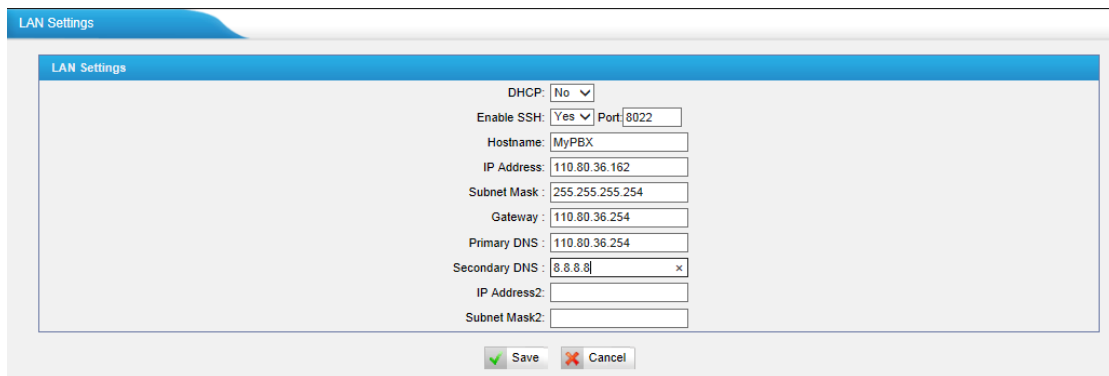


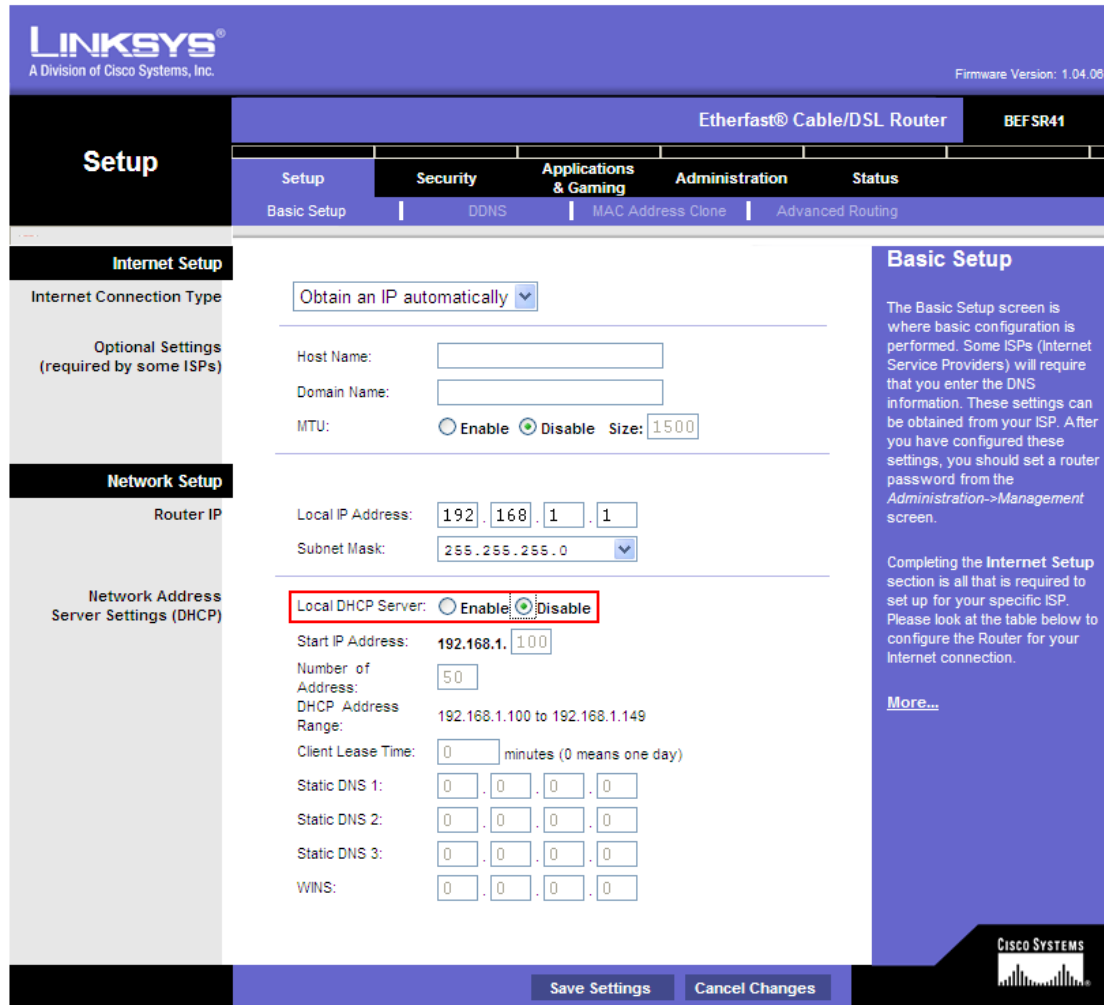
Figure C-3

Now, MyPBX has been configured as a public IP, so there is no need to configure NAT again, just leave all settings in "NAT" blank.

APPENDIX D How to Use Auto Provision

Step1. Disable DHCP Server on your local network.

E.g. Disable DHCP Server on Linksys Router.



The screenshot shows the Linksys Basic Setup page for an Etherfast Cable/DSL Router (BEFSR41). The page is divided into several sections: Internet Setup, Network Setup, and Basic Setup. The Local DHCP Server settings are highlighted with a red box, showing the 'Disable' option selected. The settings include:

- Internet Connection Type: Obtain an IP automatically
- Host Name: (empty)
- Domain Name: (empty)
- MTU: ☐ Enable ☒ Disable Size: 1500
- Local IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Local DHCP Server: ☐ Enable ☒ Disable
- Start IP Address: 192.168.1.100
- Number of Address: 50
- DHCP Address Range: 192.168.1.100 to 192.168.1.149
- Client Lease Time: 0 minutes (0 means one day)
- Static DNS 1: 0.0.0.0
- Static DNS 2: 0.0.0.0
- Static DNS 3: 0.0.0.0
- WINS: 0.0.0.0

The Basic Setup section on the right contains a description of the screen and a link to 'More...'. The bottom of the page has 'Save Settings' and 'Cancel Changes' buttons.

Figure D-1

Step2. Enable DHCP Server on MyPBX.

Login MyPBX web interface, "System" → "Network Preference" → "DHCP Server" → "Enable DHCP Server".

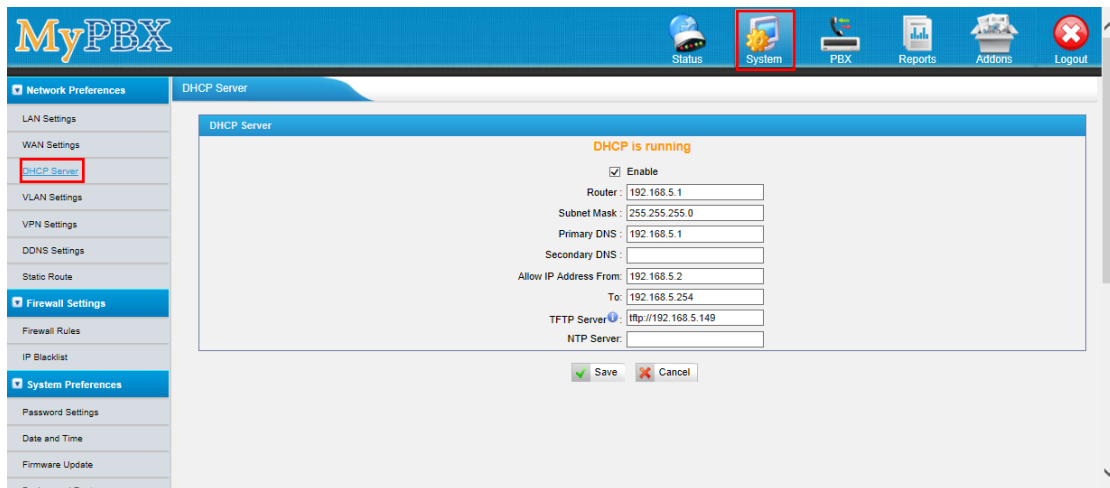


Figure D-2

Step3. Configure phones on MyPBX auto-provision page.

1. Login MyPBX web interface, "PBX" -> "Extensions" -> "Phone Provisioning" -> "Add Phone".

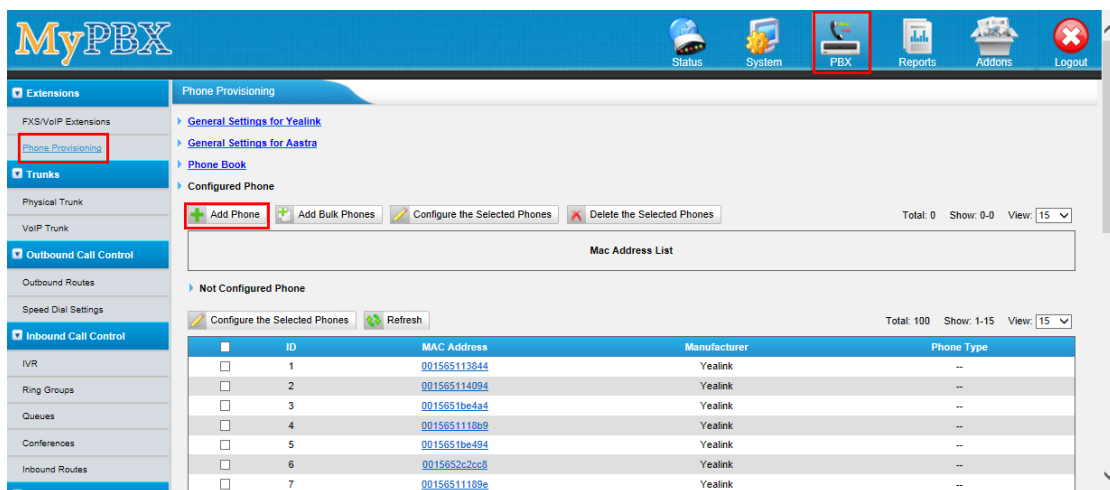


Figure D-3

2. Fill in the phone detail message on the pop-up windows.

Input IP Phone's MAC address, configure Name, Call waiting, Line, Extension, Label, Line active for the phone. And also you can configure other features on the phone, like codecs, memory keys, etc.

Add Phone
X

General
Codecs
Memory Key Settings
Line Keys Settings

Enabled: Yes
NewConfig: Yes

MAC Address: 001565
Name:

Manufacturer: Yealink
Phone Type: T28

Call Waiting: Enabled
Key As Send: #

Auto Redial: Disabled
Auto Answer: Disabled

Phone Book: Enabled

Line

☐ Line1
Extension:
Label:
Line Active:

☐ Line2
Extension:
Label:
Line Active:

☐ Line3
Extension:
Label:
Line Active:

☐ Line4
Extension:
Label:
Line Active:

☐ Line5
Extension:
Label:
Line Active:

☐ Line6
Extension:
Label:
Line Active:

Save
Cancel

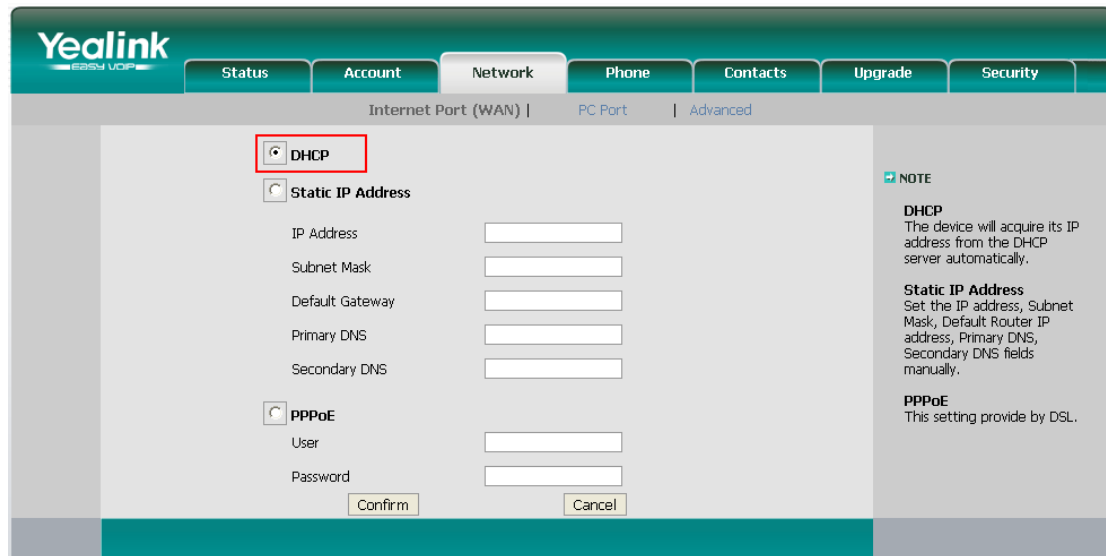
Figure D-4

Step4. Turn on the power and connect the network cable to IP Phone.

Remark: The factory default setting of DHCP for IP Phone is enabled, so you can skip this step to step 5.

If the DHCP is disabled, please follow the steps below to enable it (e.g. Yealink's IP Phone).

1. Log in IP phone's web page.
2. Enable DHCP.



Yealink easy VoIP

Status Account **Network** Phone Contacts Upgrade Security

Internet Port (WAN) | PC Port | Advanced

☒ **DHCP**

☐ **Static IP Address**

IP Address

Subnet Mask

Default Gateway

Primary DNS

Secondary DNS

☐ **PPPoE**

User

Password

NOTE

DHCP
The device will acquire its IP address from the DHCP server automatically.

Static IP Address
Set the IP address, Subnet Mask, Default Router IP address, Primary DNS, Secondary DNS fields manually.

PPPoE
This setting provide by DSL.

Figure D-5

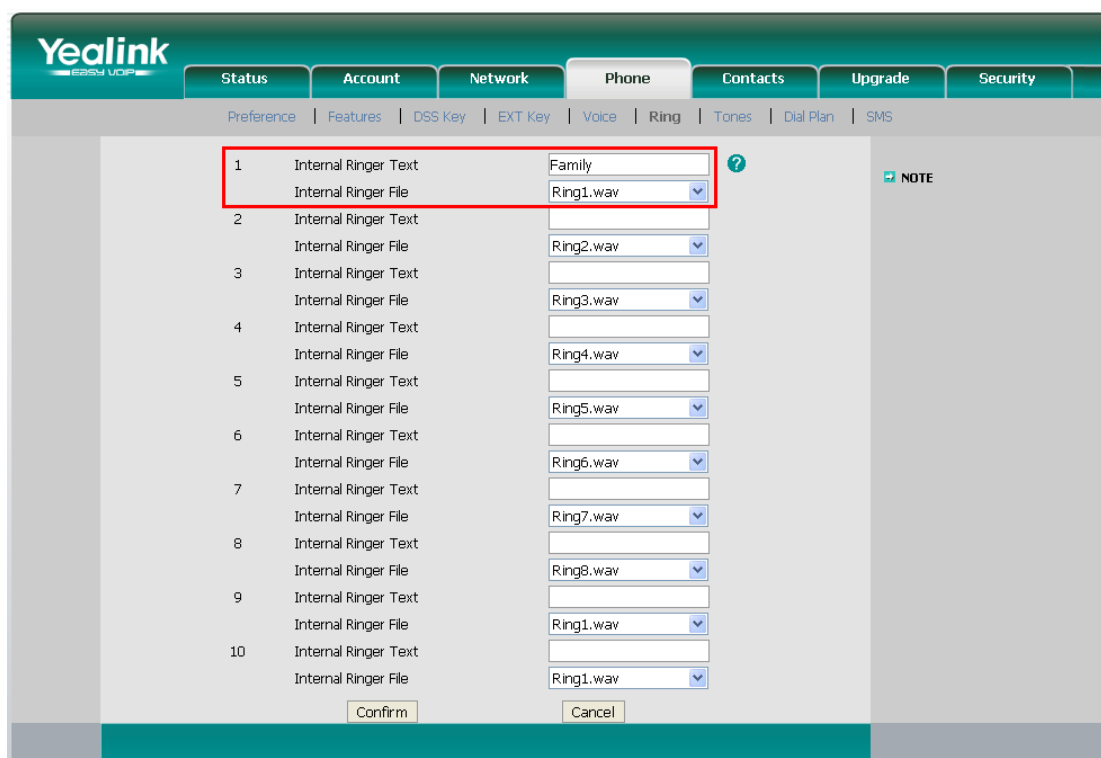
Step5. Finish.

APPENDIX E How Do I Configure Distinctive Ring Tones

Step1: On your IP phone, navigate to the Phone settings web configuration page and find the Distinctive Ring Tone section.

For each custom ring tone, enter the Internal Ringer Text (can be digits or text) to trigger the ring tone. For example, you may enter "Family".

E.g. Yealink's IP phone.



Internal Ringer Text	Internal Ringer File
1 Family	Ring1.wav
2	Ring2.wav
3	Ring3.wav
4	Ring4.wav
5	Ring5.wav
6	Ring6.wav
7	Ring7.wav
8	Ring8.wav
9	Ring1.wav
10	Ring1.wav

Figure E-1

Step2. Configure the "Distinctive Ringtone" on MyPBX.

Log in MyPBX web interface, "PBX" -> "Inbound Call Control" -> "Inbound Routes" →Edit Inbound Route, fill in the Internal Ringer Text on "Distinctive Ringtone".

Edit Inbound Route: VOIP_IN
X

General

Route Name : VOIP_IN
DID Number :
Extension :
Caller ID Number :
Distinctive Ringtone : family
Enable Callback : No [Callback Settings](#)

Member Trunks

Available Trunks		Selected
E1Trunk1(E1) 192.168.4.147(SPS)	»» → ← ««	VOIP_Supplier(SIP)

Business Days

Office Hours : default
Office Hours Destination : IVR IVR -- welcome
Non-office Hours Destination : End Call

During Holidays

Holiday :
Destination : End Call

Fax Detection

Destination : No Detect

Save Cancel

Figure E-2

Step3. Finish.

APPENDIX F How to Use DID

Direct inward dialing (DID), also called direct dial-in (DDI) in Europe and Oceania, is a feature offered by telephone companies for use with their customers' private branch exchange (PBX) systems. In DID service the telephone company provides one or more trunk lines to the customer for connection to the customer's PBX and allocates a range of telephone numbers to this line (or group of lines) and forwards all calls to such numbers via the trunk.

MyPBX support DID, you can configure DID in inbound route. Related settings: **DID Number, Extension, Destination.**

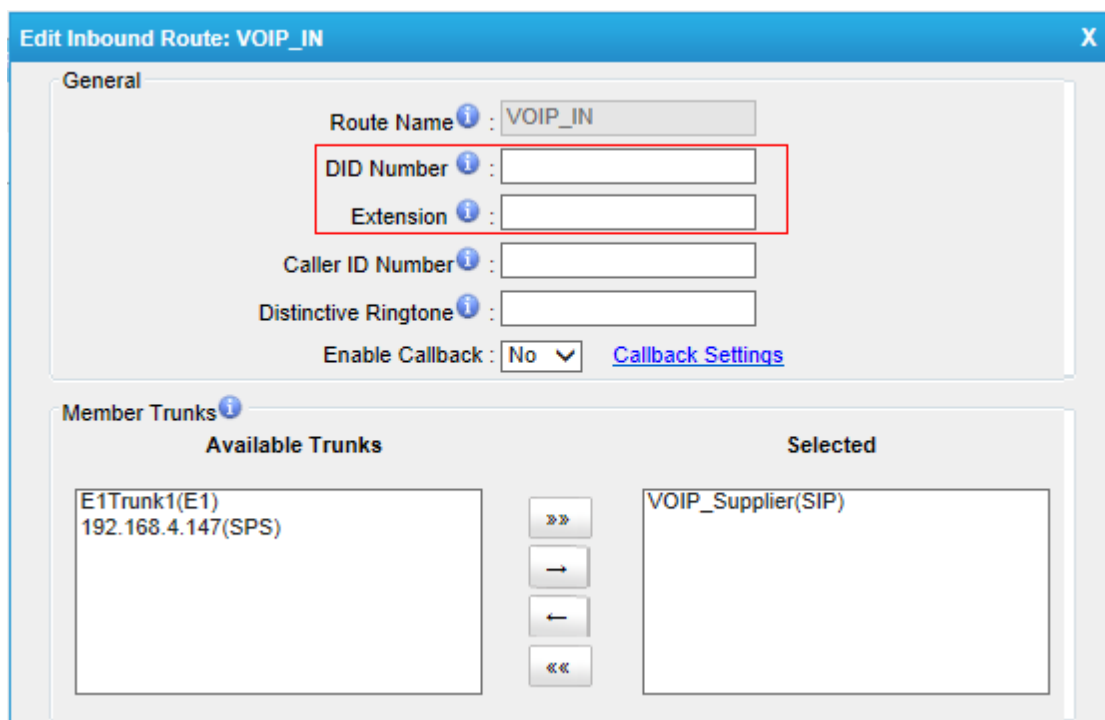


Figure F-1

•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. Only service provider, E1 trunks, BRI trunks or SIP trunks need to be configured with this setting.

You can also use pattern matching to match a range of numbers. The following patterns may be used:

X: Any Digit from 0-9

Z: Any Digit from 1-9

N: Any Digit from 2-9

[12345-9]: Any digit in the brackets (in this example, 1, 2, 3, 4, 5, 6, 7, 8, 9)
The "." Character will match any remaining digits. For example, "9011." will match any phone number that starts with "9011", excluding "9011" itself.
The "!" will match none remaining digits, and causes the matching process to complete as soon as it can be determined that no other matches are possible.

•Extension

Define the extension for DID number, this field only valid when use E1 trunk for this inbound router. You can only input number and "-" in this field, and the format can be xxx or xxx-xxx. The count of the number must be only one or equal the count of the DID number.

•Destination

If you don't set the extension, you can set the destination of the call here.

Example 1:

Step1: You set the DID number (5503XXX in this example).

Step2: You choose the destination (IVR in this example).

The configuration of this example means when the incoming call with DID number 5503XXX (7-digit numbers starting with 5503) will go to the destination IVR.

If you choose the destination, please leave the Extension form blank.

Edit Inbound Route: pstnin
X

General

Route Name : pstnin
DID Number : 5503XXX
Extension :
Caller ID Number :
Distinctive Ringtone :
Enable Callback : No [Callback Settings](#)

Member Trunks

Available Trunks		Selected
VOIP_Supplier(SIP) 192.168.4.147(SPS)	»» → ← ««	E1Trunk1(E1)

Business Days

Office Hours : default
Office Hours Destination : IVR IVR -- welcome
Non-office Hours Destination : IVR IVR -- welcome

During Holidays

Holiday :
Destination : End Call

Fax Detection

Destination : No Detect

Save Cancel

Figure F-2

Example 2:

Step1: You set the DID number (6001-6099 in this example).

Step2: You set the Extension (6001-6099 in this example).

The configuration of this example means when the incoming call with DID number 6001 to 6099 will go to the destination 6001 to 6099 (number 6001 to extension 6001, number 6002 to extension 6002).

The destination you set below will be disabled if you set the Extension.

Edit Inbound Route: VOIP_IN
X

General

Route Name : VOIP_IN
DID Number : 6001-6099
Extension : 6001-6099
Caller ID Number :
Distinctive Ringtone :
Enable Callback : No [Callback Settings](#)

Member Trunks

Available Trunks		Selected
E1Trunk1(E1) 192.168.4.147(SPS)	»» → ← ««	VOIP_Supplier(SIP)

Business Days

Office Hours : default
Office Hours Destination : IVR IVR -- welcome
Non-office Hours Destination : End Call

During Holidays

Holiday :
Destination : End Call

Fax Detection

Destination : No Detect

Save Cancel

Figure F-3

APPENDIX G How to Use BLF Key to Choose the PSTN Line

MyPBX allows you to choose the specific PSTN line to make outbound call by pressing the BLF key on the IP Phone.

Follow the steps to do the configuration with your Yealink phone.

1. We want to choose pstn1 or pstn2 to call out.

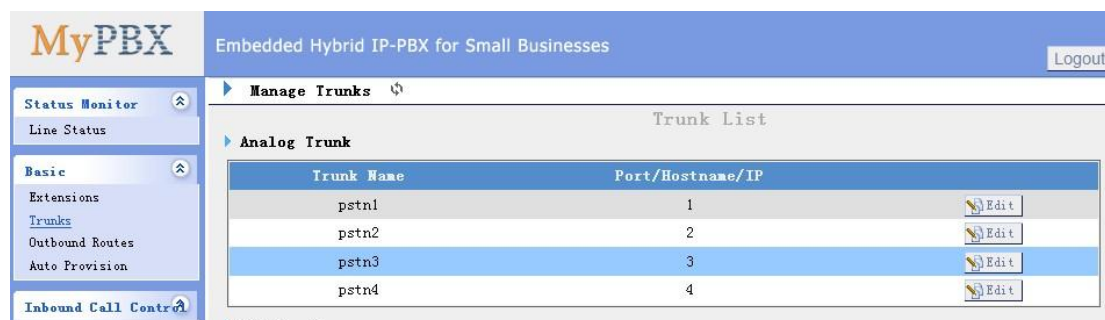


Figure G-1

2. Configure the IP Phone:



Figure G-2

Test

When you press DSS Key 1/2, the phone will connect to pstn1/pstn2 line. If pstn1/pstn2 is not busy, you will hear the dial tone. You can dial the number you want and use this line to call out then.

APPENDIX H MyPBX Security Configuration Guide

VoIP attack, although not an everyday occurrence does exist. When using VoIP, system security is undoubtedly one of the issues we care about most. But with the appropriate configuration, and some basic safety habits, we can improve the security of the telephone system. Moreover, the powerful built-in firewall function in MyPBX is adequate to enable the system to run safely and stably.

This guide will introduce the highest defense level in MyPBX, and we strongly recommend that you configure firewall and other security options according to this guide, to prevent the attack fraud and the system failure or calls loss.

Notes:

1. In this guide, the configuration options marked with "*" only exist in X.18.XX.XX and above versions.
2. We recommend upgrading the firmware to the latest edition for security purpose.
3. Don't map any port to MyPBX in router if not needed.
4. We recommend limiting the credit of VoIP trunks for international calls.

Security Center*

Security center is a new feature since x.18.0.xx, we can get an overview of basic settings like firewall, service security and port guard.

Click "System→ System Preferences→Security Center" to get the details. You can click the button to configure those one by one. You can follow the steps in this manual to configure and get the result in this page.

1. Port:

This page shows the SIP port and HTTP port, we can click "Setting" to change that.

It's recommend that the default port should be changed.

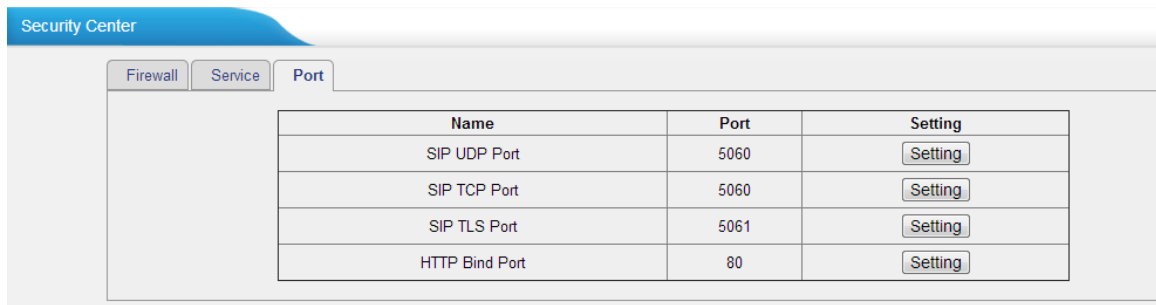


Figure H-0-1

2. Service:

This page shows the general service like AMI, SSH and TFTP, we recommend disabling them if not used.

Note: TFTP is used for phone provisioning, it's enabled by default, you can disable it after all phones are well configured.

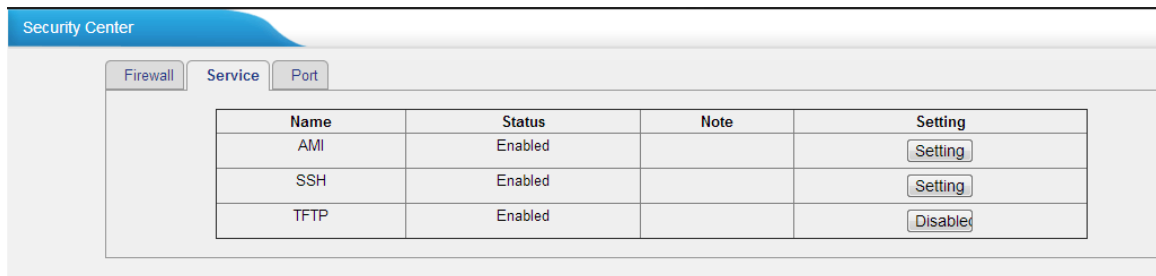


Figure H-0-2

3. Firewall:

In this page, the basic information of firewall rules are displayed. We recommend configuring it step by step following part 2 of this manual.

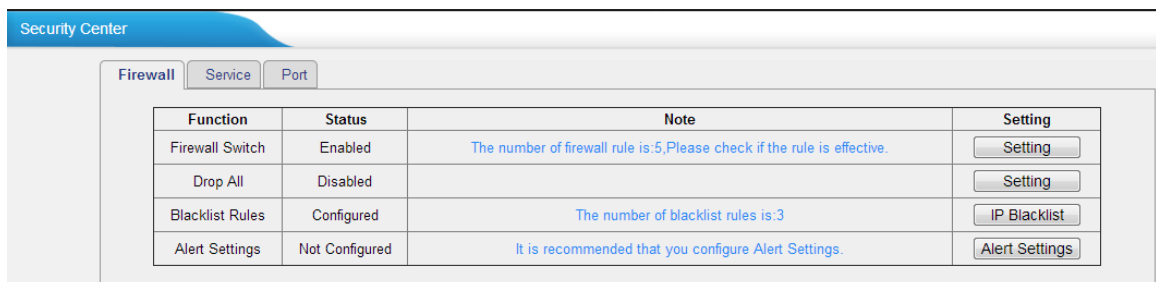


Figure H-0-3

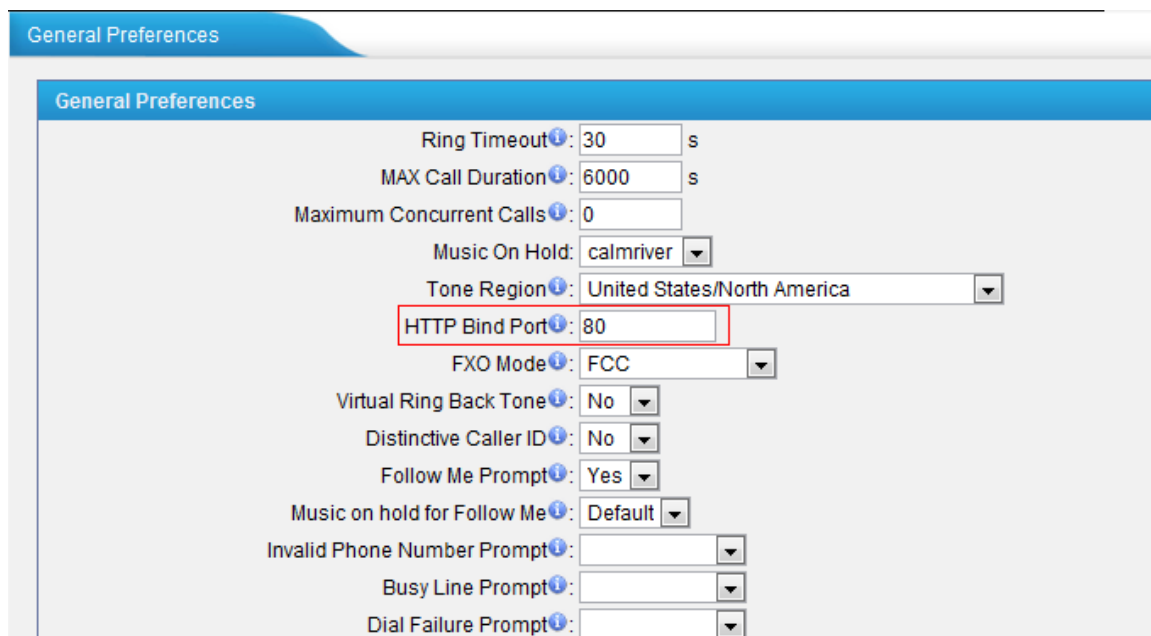
1. Ports and password enhancement

Ports and password are most important for security; we recommend changing the default ones to your own.

1.1 Web GUI (HTTP)

1.1.1 Change the default HTTP bind port.

PBX→Basic Settings→ General Preferences→HTTP Bind Port



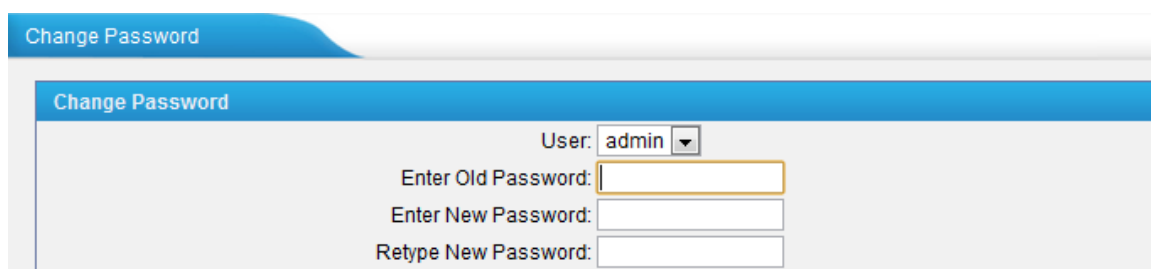
The screenshot shows the 'General Preferences' web interface. The 'HTTP Bind Port' field is highlighted with a red box and contains the value '80'. Other visible settings include Ring Timeout (30 s), MAX Call Duration (6000 s), Music On Hold (calmriver), Tone Region (United States/North America), FXO Mode (FCC), Virtual Ring Back Tone (No), Distinctive Caller ID (No), Follow Me Prompt (Yes), Music on hold for Follow Me (Default), Invalid Phone Number Prompt, Busy Line Prompt, and Dial Failure Prompt.

Figure H-1-1

We can change it to another one like 8080 for example.

1.1.2 Change the default password.

System→ System Preferences→Change Password



The screenshot shows the 'Change Password' web interface. It includes a 'User' dropdown menu set to 'admin', and three input fields: 'Enter Old Password:', 'Enter New Password:', and 'Retype New Password:'.

Figure H-1-2

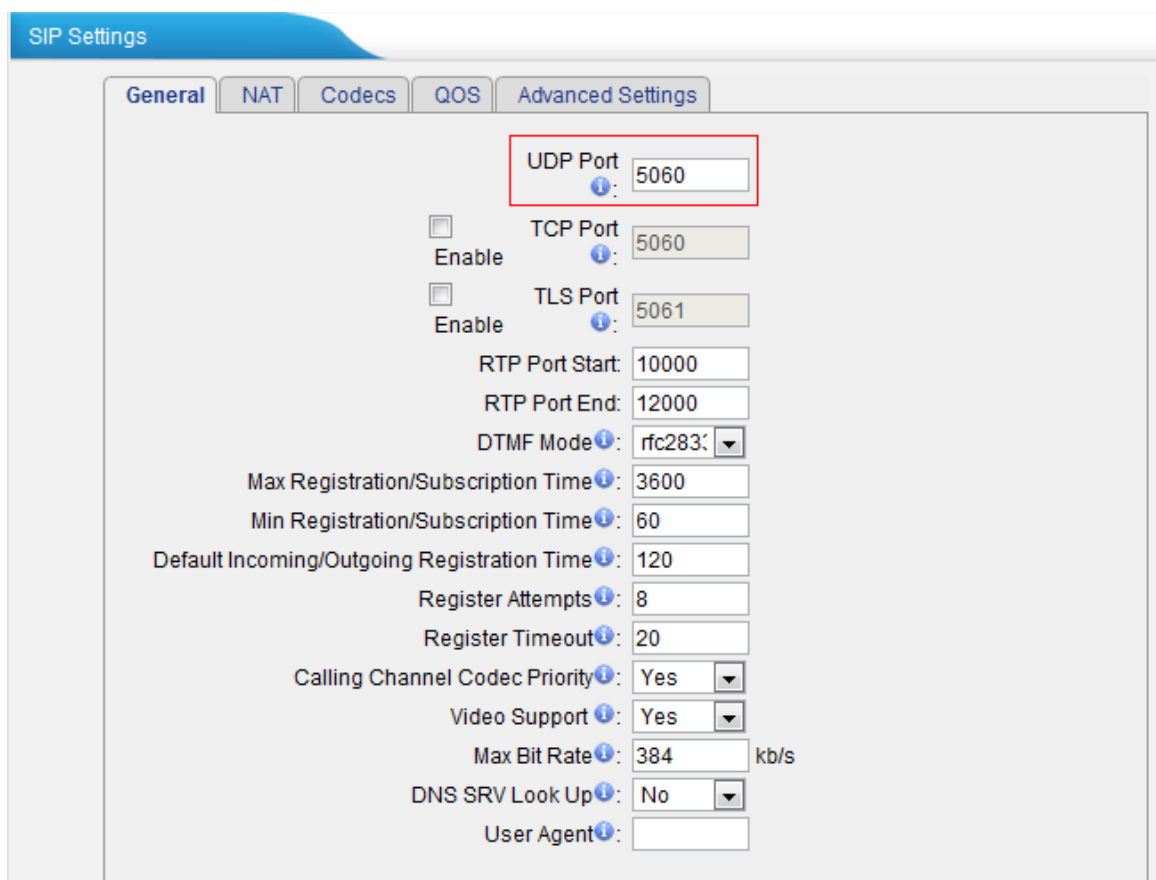
A strong password needs to be configured here for all accounts. Especially account "admin" and "user".

1.2 Extension

Hackers are always sending packages to PBX to register extension before dialing out. Extension's security is very important for users.

1.2.1 Change the default SIP Port

PBX→Basic settings→SIP Settings→General→UDP Port



SIP Settings

General NAT Codecs QOS Advanced Settings

UDP Port: 5060

☐ Enable TCP Port: 5060

☐ Enable TLS Port: 5061

RTP Port Start: 10000

RTP Port End: 12000

DTMF Mode: rfc283

Max Registration/Subscription Time: 3600

Min Registration/Subscription Time: 60

Default Incoming/Outgoing Registration Time: 120

Register Attempts: 8

Register Timeout: 20

Calling Channel Codec Priority: Yes

Video Support: Yes

Max Bit Rate: 384 kb/s

DNS SRV Look Up: No

User Agent:

Figure H-1-3

We recommend changing this to another available port, for example: 5080.

1.2.2 Change the default password

The password of the extensions is "pincode + extension number". A password with upper and lower letters and numbers is recommended. For example: AjK5Up1G.

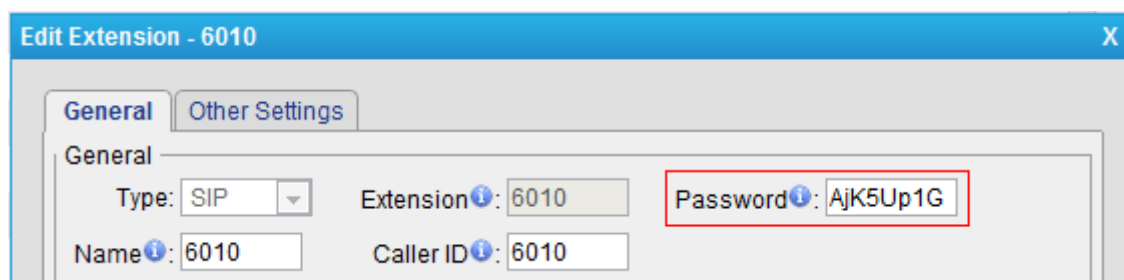


Figure H-1-4 shows the 'Edit Extension - 6010' window. The 'General' tab is selected. The 'Password' field is highlighted with a red box, showing the value 'Ajk5Up1G'.

Figure H-1-4

Note: A strong password is a MUST for remote extensions.

1.2.3. IP restriction for extensions

You can find this setting in

PBX→Extensions→FXS/VoIP Extensions→ VoIP Extensions→General→Password
When it's configured, only the permitted IP can register this extension. All the other registry requests will be denied.

The format is "IP address/Subnet mask", e.g. 192.168.5.136/255.255.255.255.
In this way, only 192.168.5.136 can register this extension 6010.

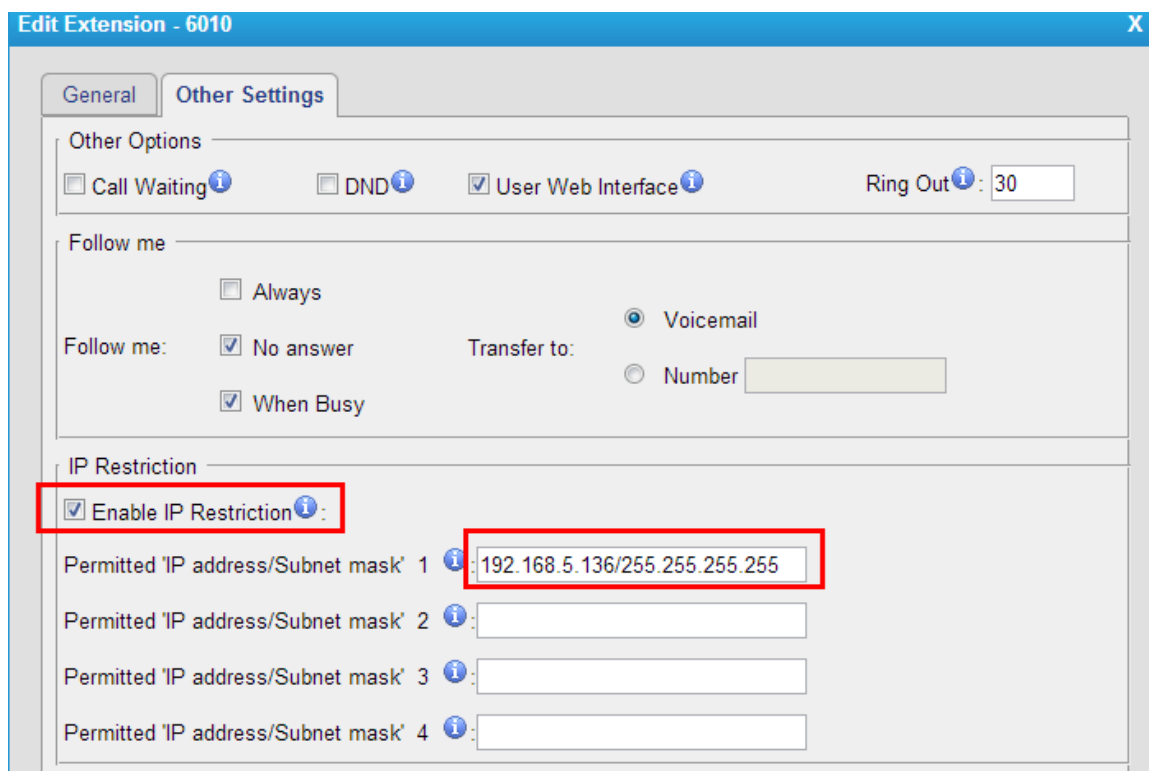


Figure H-1-5 shows the 'Edit Extension - 6010' window, 'Other Settings' tab. The 'Enable IP Restriction' checkbox is checked and highlighted with a red box. Below it, the first 'Permitted IP address/Subnet mask' field is also highlighted with a red box, showing the value '192.168.5.136/255.255.255.255'.

Figure H-1-5

Note: If it's for remote extension, a static public IP address is needed to input instead.

1.2.3 Security Configuration for Remote Extensions

PBX→Extensions→FXS/VoIP Extensions→ VoIP Extensions→General
Enable "NAT" and "Register remotely" like the picture shown below.

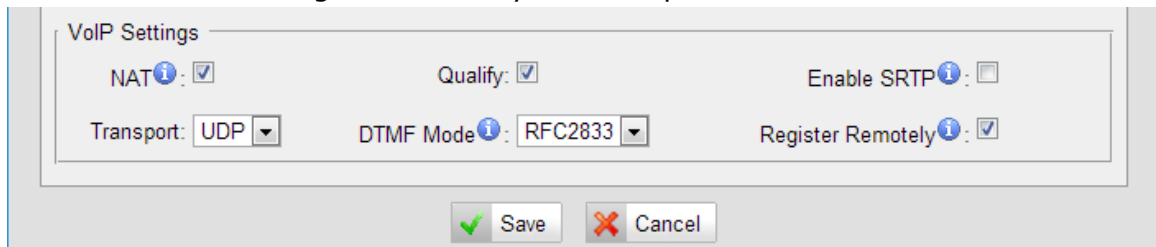


Figure H-1-6

Notes:

1. If remote registration isn't required, please disable it.
2. If extensions register to MyPBX via WAN port, please only enable "register remotely".

1.2.4 TLS registry (Optional)

Introduction

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. They use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and Voice-over-IP (VoIP).

TLS is supported in MyPBX for security SIP registry; you can also register SIP trunks to VoIP providers via TLS. We need to upload the certificate into MyPBX and the IP phones together for authorization.

Hackers send the register request to PBX for registry via UDP generally, if TLS is

enabled in MyPBX, hacker cannot register extension without the CA, the registry request will be refused directly.

Refer to [Appendix I](#) to get the detailed steps of how to use TLS in MyPBX.

Note: TLS is disabled in MyPBX by default; we need to enable it in "SIP settings" page in advance before using it.

2. Firewall configuration

Note: Please back up the configurations on Backup and Restore page before you go ahead. In the case that you lock the device, you can reset to factory default and restore the previous configurations. The example rules below work with MyPBX firmware version 2.15.xx.xx or higher versions.

The basic logic to configure firewall is "Allow all trusted IP addresses and then enable "Drop All".

Step1. Enable firewall on firewall page of MyPBX.

System→Firewall Settings → Firewall Rules→General Settings

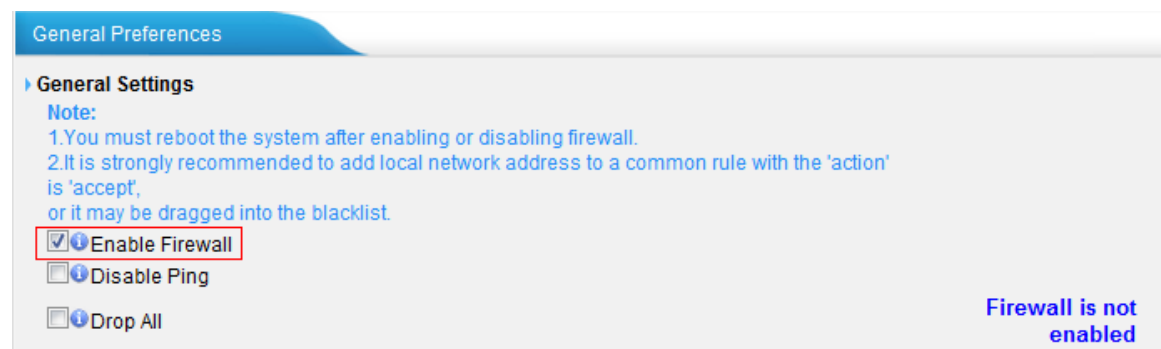


Figure H-2-1

Step2. Add common rules to accept local network access.

Create a common rule to allow all the IP addresses of the local phones to access MyPBX server. For example, the local IP range is 192.168.5.1-192.168.5.254, the configuration could be as below:

Name: LocalNetwork

Protocol: BOTH

Port: 1:65535

IP: 192.168.5.0/255.255.255.0, the format must be "IP/net mask"

Action: Accept

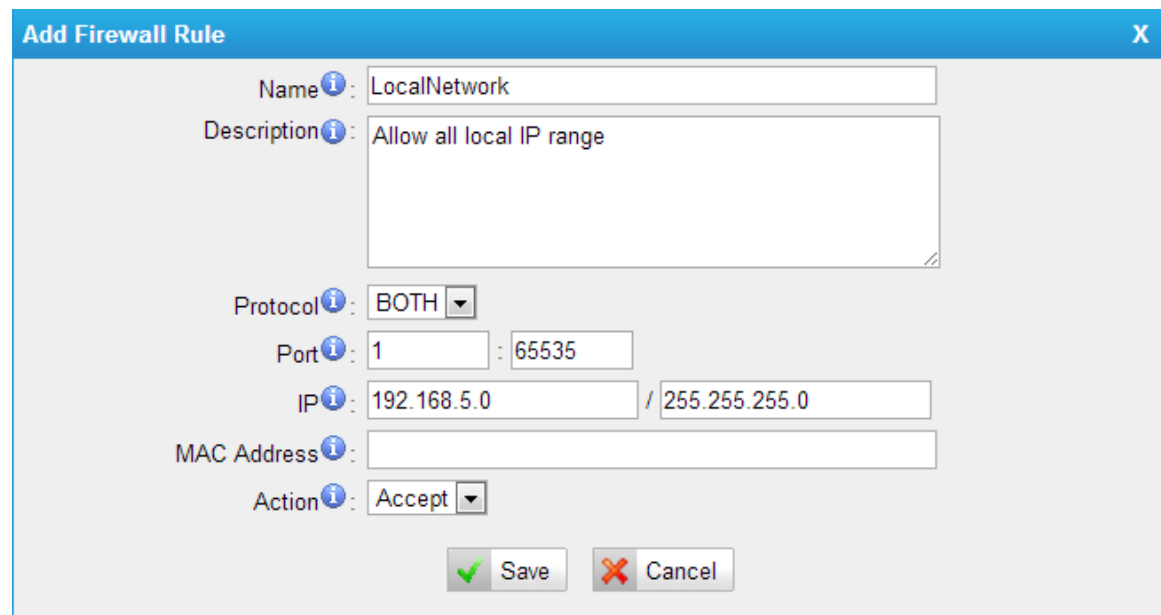


Figure H-2-2

Step3. Add common rules to allow remote administrators, extensions or devices.

For example the public IP is 110.30.25.152; we can allow all ports for this trusted IP.

Name: Remote

Protocol: BOTH

Port: 1:65535

IP: 110.30.25.152/255.255.255.255

Action: Accept

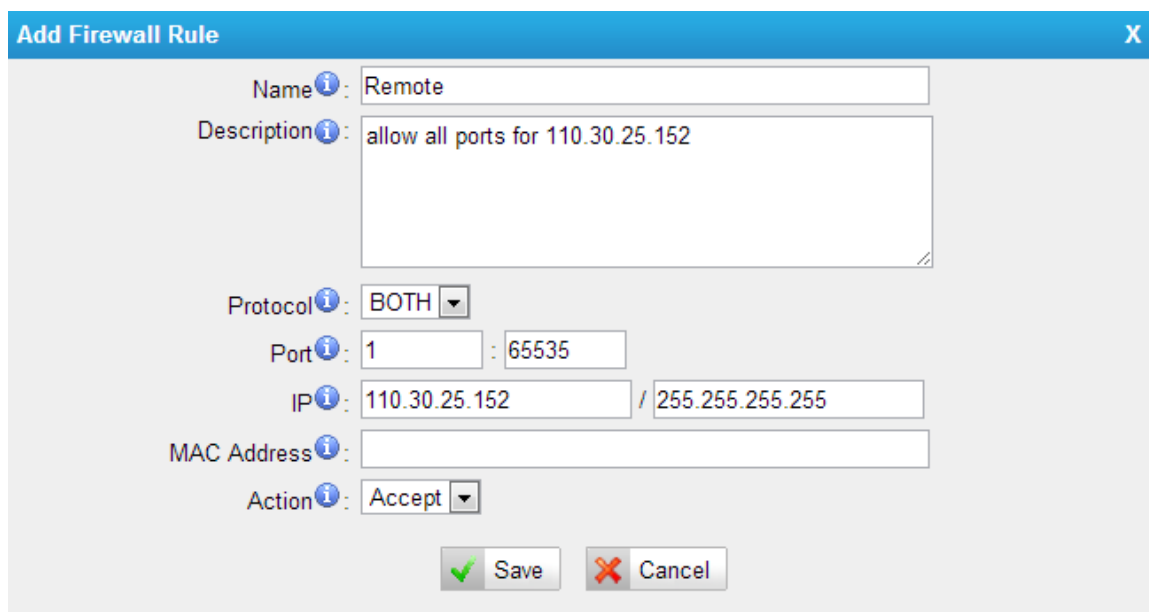


Figure H-2-3

Note: Static public IP range needs to be configured here, if it's dynamic IP address that doesn't belong to a range, there is no need to configure it, but the "Drop All" in the next step should not be ticked. The IP blacklist rules will help to protect MyPBX. We recommend getting public static IP for security purpose.

Step4. Add common rules to accept the static public IP range of VoIP provider.

The ports used to contact the SIP provider is 5060 and 10000-12000 by default, if you have changed this port range, you can input it here by yourself.

For example, the IP address is 110.111.132.6, the configurations should be two parts, one is for 5060, and the second is for RTP port: 10000-12000.

Allow registry port: 5060.

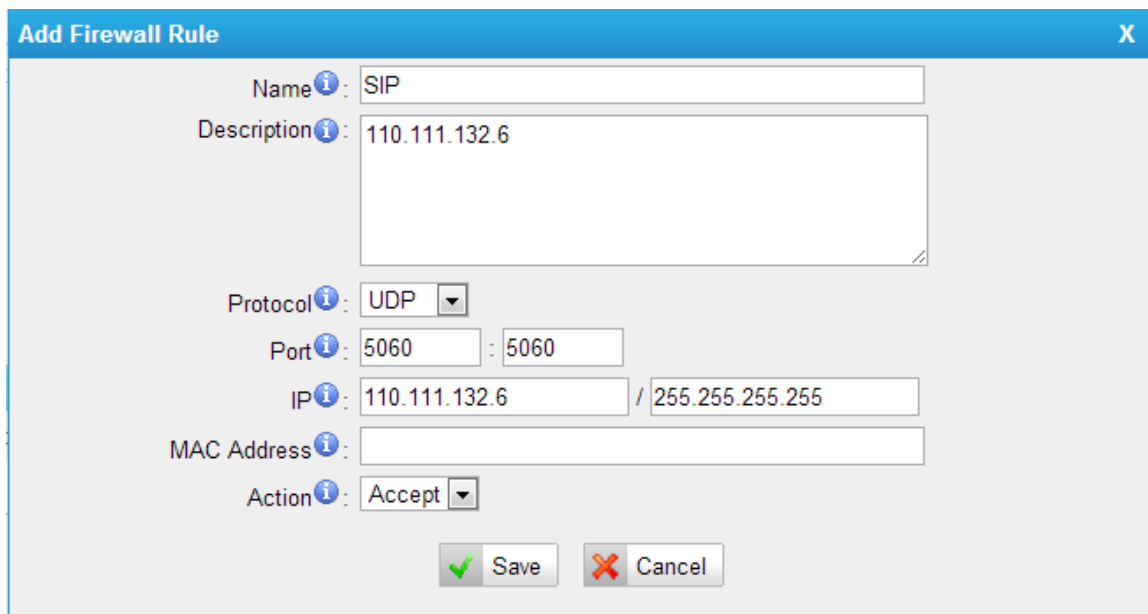
Name: SIP

Protocol: UDP

Port: 5060:5060

IP: 110.111.132.6/255.255.255.255

Action: Accept



Add Firewall Rule

Name: SIP

Description: 110.111.132.6

Protocol: UDP

Port: 5060 : 5060

IP: 110.111.132.6 / 255.255.255.255

MAC Address:

Action: Accept

Save Cancel

Figure H-2-4

Allow RTP port range:

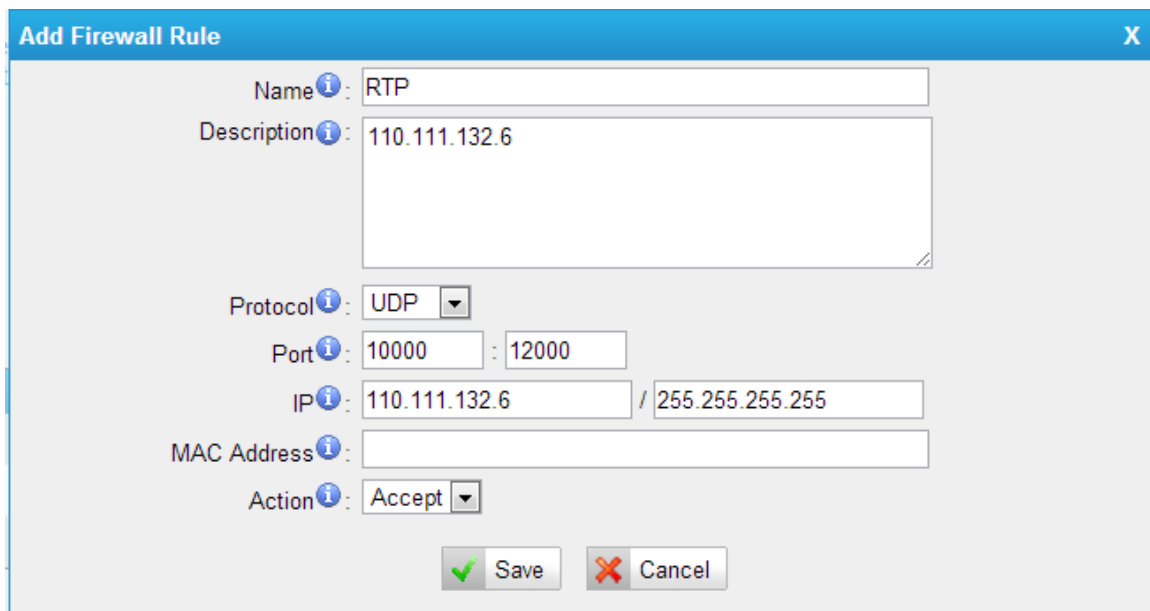
Name: RTP

Protocol: UDP

Port: 10000:12000

IP: 110.111.132.6/255.255.255.255

Action: Accept



Add Firewall Rule

Name: RTP

Description: 110.111.132.6

Protocol: UDP

Port: 10000 : 12000

IP: 110.111.132.6 / 255.255.255.255

MAC Address:

Action: Accept

Save Cancel

Figure H-2-5

Note: If the media server of SIP provider is dynamic, and we cannot collect the IP range. We can allow the RTP range for the whole IP addresss like this:

Name: RTP_ALL
Protocol: UDP
Port: 10000:12000
IP: 0.0.0.0/0.0.0.0
Action: Accept

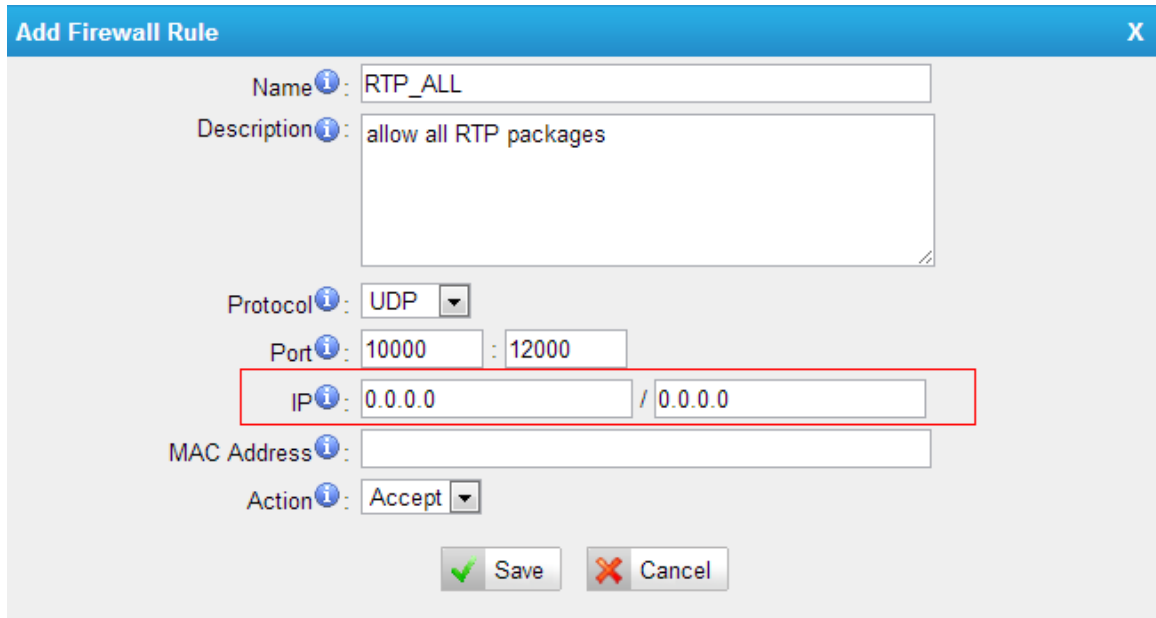


Figure H-2-6

In this case, MyPBX can get rid of one-way volume issue.

Step5. Block the web connection of the other IP address that are not added into accept list.

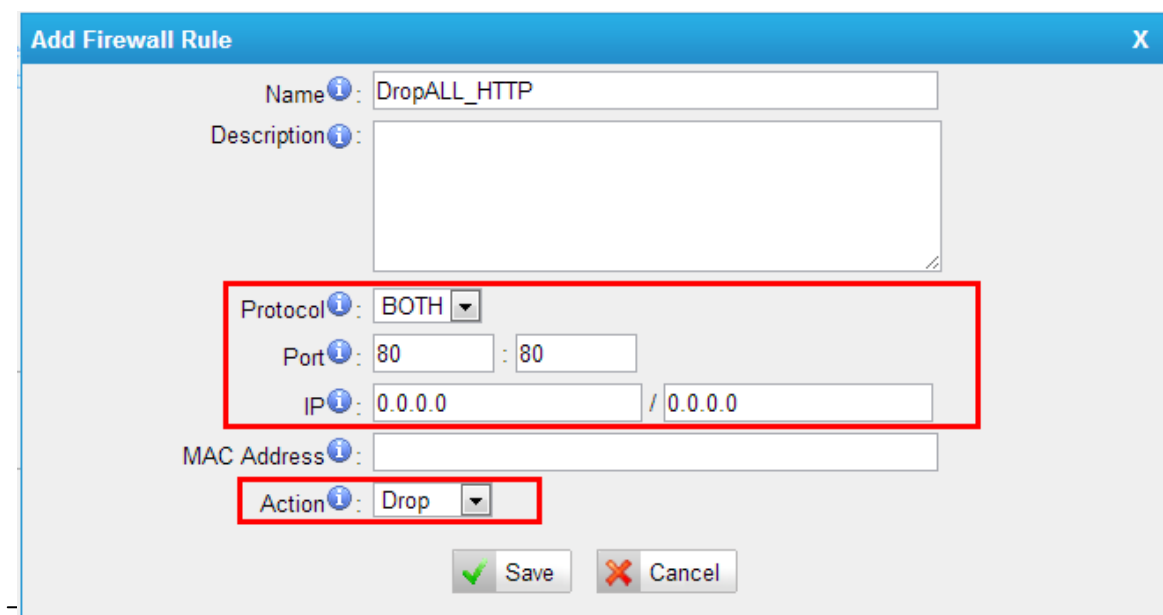


Figure H-2-7

Note: Many attacks are caused by the web access, it's highly recommend to drop the untrusted connection via web interface.

Step6. Add common rules to accept the static public IP range of NTP, SMTP, and POP server.

We recommend opening all ports for NTP, SMTP, and POP server in MyPBX's firewall, and the IP address should be a static one or it belongs to a range. If it's DynDNS, there is no need to configure this rule, but the IP blacklist should be kept, and "Drop All" should not be ticked.

For example, the SMTP server is 110.30.1.123.

Name: Allow_SMTP

Protocol: BOTH

Port: 1:65535

IP: 110.30.1.123/255.255.255.255

Action: Accept

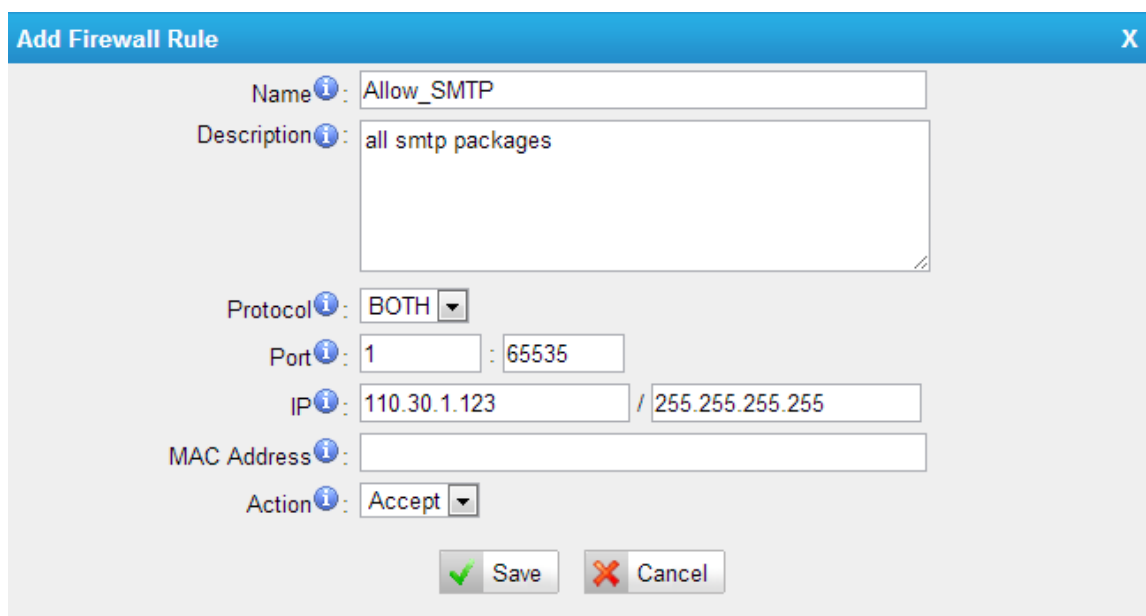


Figure H-2-7

As for the rule of NTP and POP server, you can create it one by one.

Step6. Configure auto blacklist rules

Auto blacklist rules: the Server would add the IP address to the blacklist

automatically if the number of the packets it sends exceeds the rule you configured.

Note: These 3 rules are created by MyPBX by default.

1) Add two auto blacklist rules for port: 5060.

Rule No.1:

Port: 5060

Protocol: UDP

IP Packets: 120

Time Interval: 60 seconds

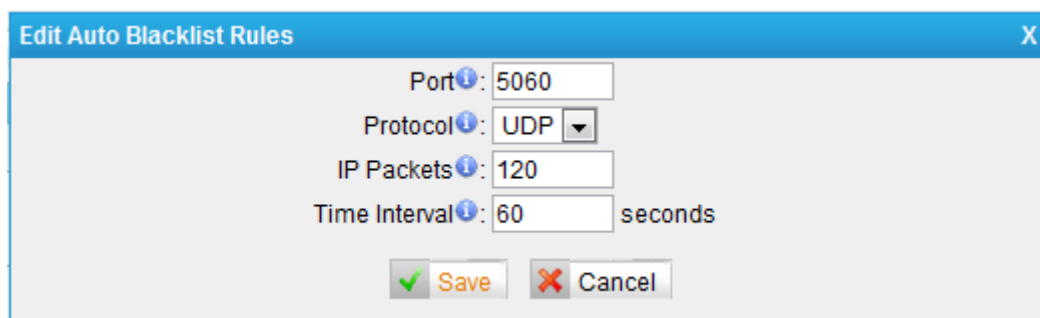


Figure H-2-8

Rule No.2:

Port: 5060

Protocol: UDP

IP Packets: 40

Time Interval: 2 seconds

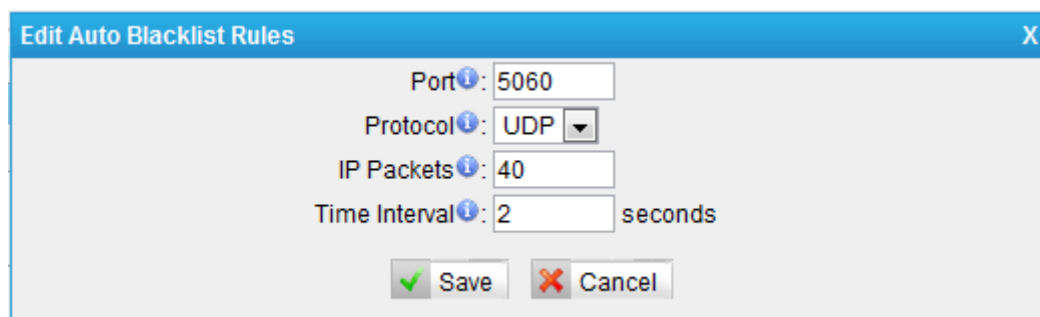


Figure H-2-9

2) Add an auto blacklist rule for Port:8022

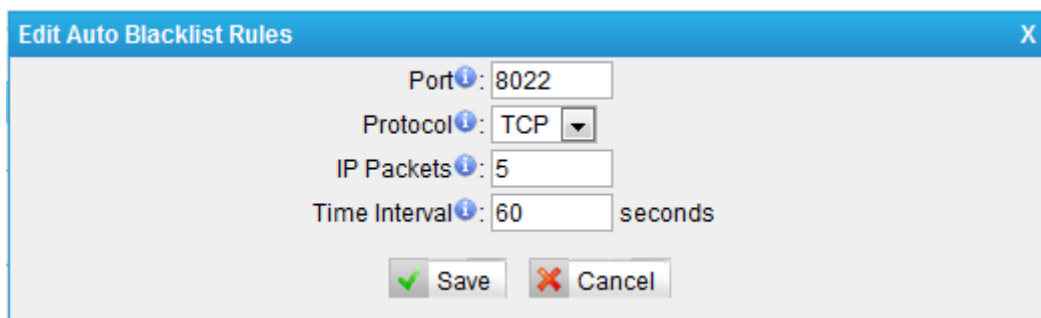
Rule No.3

Port: 8022

Protocol: TCP

IP Packets: 5

Time Interval: 60 seconds



Port: 8022

Protocol: TCP

IP Packets: 5

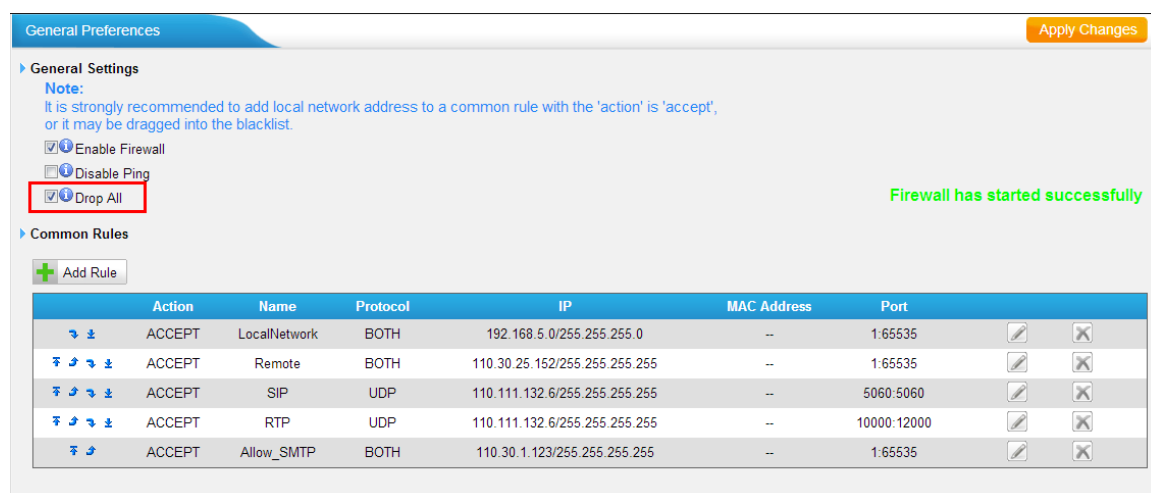
Time Interval: 60 seconds

Save Cancel

Figure H-2-10

Step 7. Enable “Drop all” (If this feature is enabled, all the packets and connection that do not match the rules would be dropped.)

Warning: Before enabling this feature, please create a rule to accept the local network access, or the server might not be accessed.



General Preferences

Apply Changes

General Settings

Note:
It is strongly recommended to add local network address to a common rule with the 'action' is 'accept', or it may be dragged into the blacklist.

☒ Enable Firewall

☐ Disable Ping

☒ Drop All

Firewall has started successfully

Common Rules

+ Add Rule

Action	Name	Protocol	IP	MAC Address	Port		
ACCEPT	LocalNetwork	BOTH	192.168.5.0/255.255.255.0	--	1.65535		
ACCEPT	Remote	BOTH	110.30.25.152/255.255.255.255	--	1.65535		
ACCEPT	SIP	UDP	110.111.132.6/255.255.255.255	--	5060:5060		
ACCEPT	RTP	UDP	110.111.132.6/255.255.255.255	--	10000:12000		
ACCEPT	Allow_SMTP	BOTH	110.30.1.123/255.255.255.255	--	1.65535		

Figure H-2-11

Notes:

1. After enabling “Drop All”, the rules of auto defense and IP blacklist will not take effect. It means except the IPs and packets which are defined in the accept rules, the other connection or packets will be dropped.
2. If “Drop All” is not enabled, please don’t remove the IP blacklist rules in case the system security hole exists.

Step 8. The configuration of firewall settings is completed. See the figure below.

General Preferences

General Settings

Note:
It is strongly recommended to add local network address to a common rule with the 'action' is 'accept', or it may be dragged into the blacklist.

☒ Enable Firewall

☐ Disable Ping

☒ Drop All

Firewall has started successfully

Common Rules

+ Add Rule

Action	Name	Protocol	IP	MAC Address	Port		
ACCEPT	LocalNetwork	BOTH	192.168.5.0/255.255.255.0	--	1:65535		
ACCEPT	Remote	BOTH	110.30.25.152/255.255.255.255	--	1:65535		
ACCEPT	SIP	UDP	110.111.132.6/255.255.255.255	--	5060:5060		
ACCEPT	RTP	UDP	110.111.132.6/255.255.255.255	--	10000:12000		
ACCEPT	Allow_SMTP	BOTH	110.30.1.123/255.255.255.255	--	1:65535		
DROP	DropALL_HTTP	BOTH	0.0.0.0/0.0.0.0	--	80:80		

Auto Defense

+ Add Rule

No Auto Defense Rules Defined

Save Cancel

Figure H-2-12

IP Blacklist Apply Changes

Blacklist Rules

+ Add Rule

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

IP Blacklist

No Auto Black IP Address

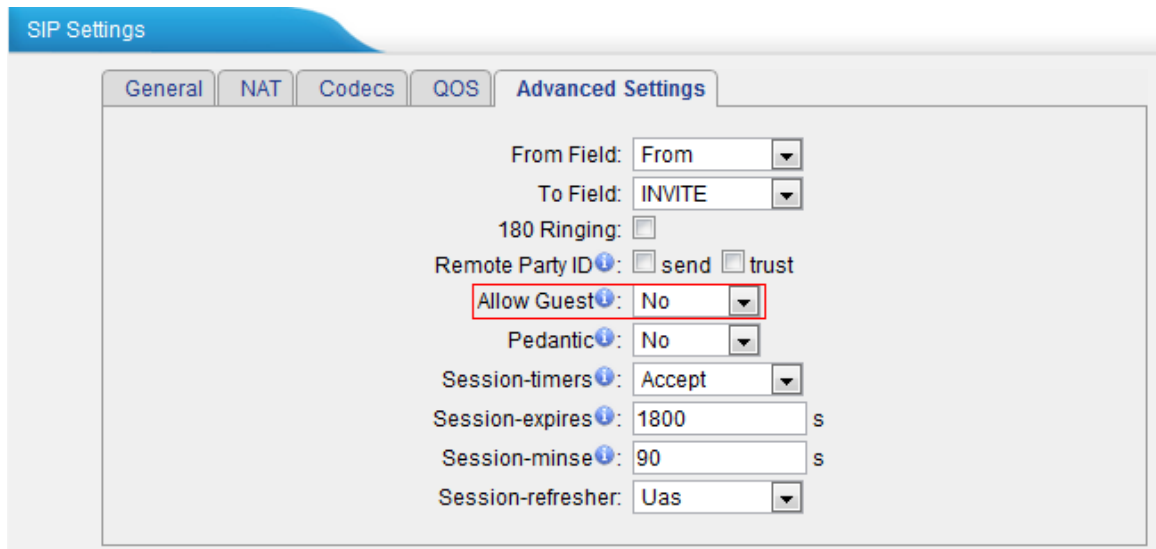
Figure H-2-13

3. Service security

3.1 Disable Guest Call

3.2 Disable Guest calls

PBX→Basic Settings→SIP Settings→Advanced Settings→Allow Guest



The screenshot shows the 'SIP Settings' window with the 'Advanced Settings' tab selected. The 'Allow Guest' dropdown menu is highlighted with a red box and is set to 'No'. Other settings visible include 'From Field' (From), 'To Field' (INVITE), '180 Ringing' (unchecked), 'Remote Party ID' (send and trust unchecked), 'Pedantic' (No), 'Session-timers' (Accept), 'Session-expires' (1800 s), 'Session-minse' (90 s), and 'Session-refresher' (Uas).

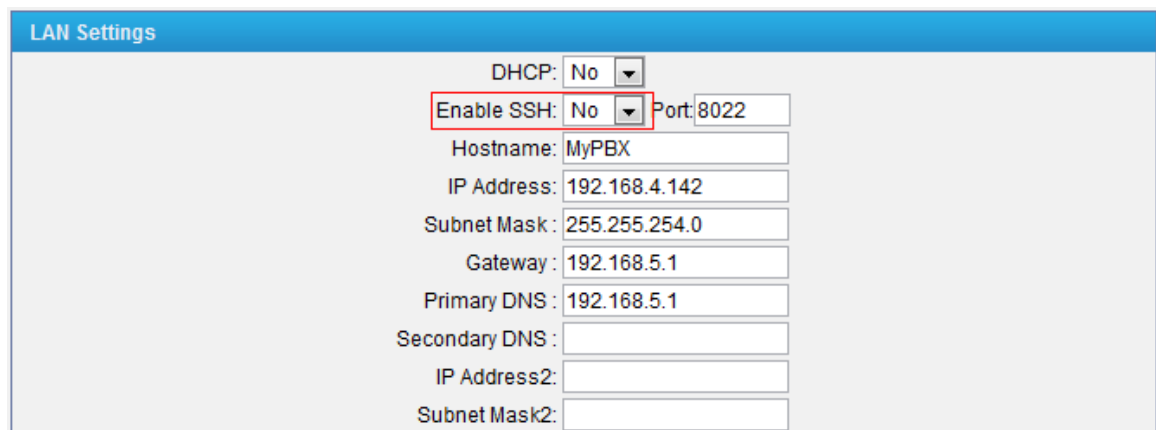
Figure H-3-1

Note: Allow Guest is disabled by default; please keep it to “No” for general use.

3.2 SSH access enhancement

3.2.1 Disable SSH

Select LAN Settings→Enable SSH. If external debugging isn’t required, please select “No”.



The screenshot shows the 'LAN Settings' window. The 'Enable SSH' dropdown menu is highlighted with a red box and is set to 'No'. Other settings visible include 'DHCP' (No), 'Port' (8022), 'Hostname' (MyPBX), 'IP Address' (192.168.4.142), 'Subnet Mask' (255.255.254.0), 'Gateway' (192.168.5.1), 'Primary DNS' (192.168.5.1), 'Secondary DNS' (empty), 'IP Address2' (empty), and 'Subnet Mask2' (empty).

Figure H-3-2

Note: SSH access is disabled by default; please keep it to “No” if not needed.

3.2.2 Change the default password for SSH

We can use the Linux command **passwd** to change the root password of MyPBX.

1. Log in via putty.exe.

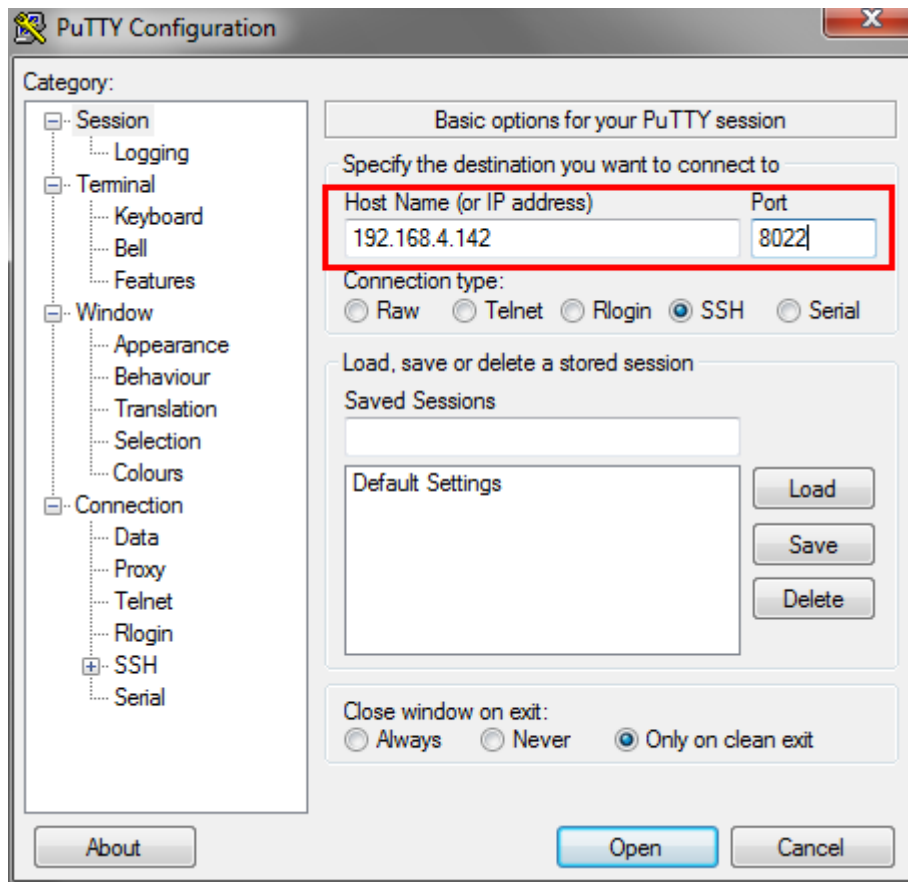


Figure H-3-3

2. The default username is **root** and the default password is **ys123456**.

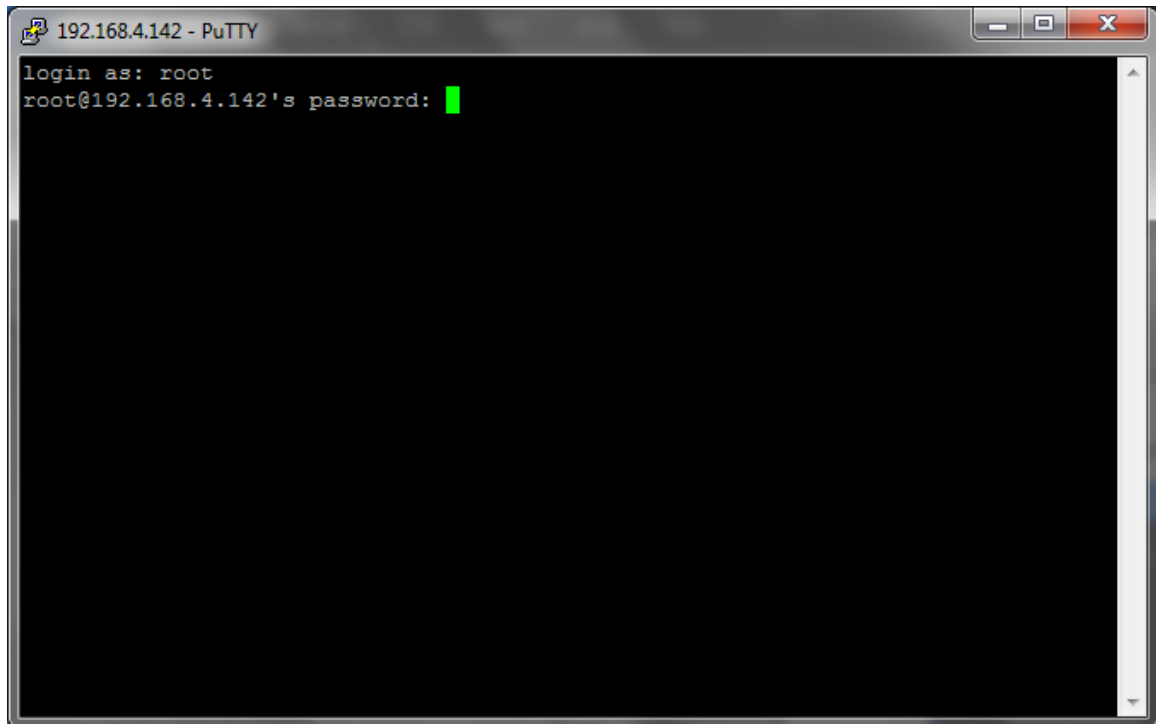


Figure H-3-4

3. Use command **passwd** to change the root's password

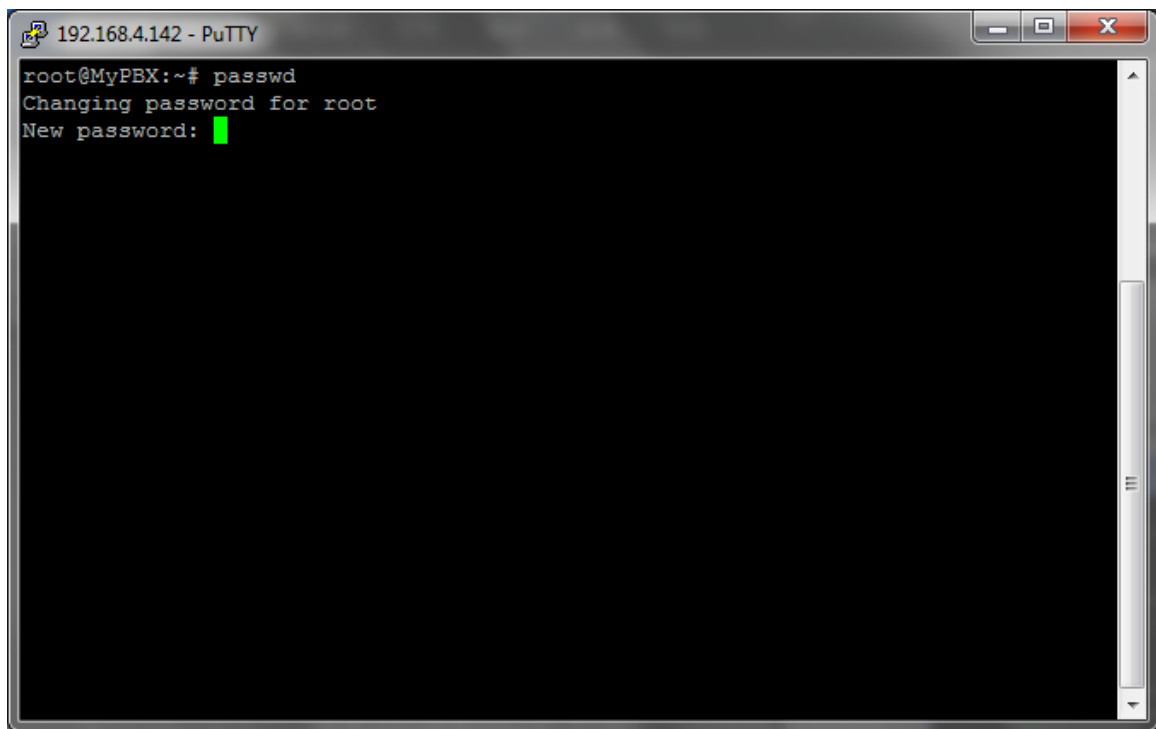


Figure H-3-5

You need to input the new password twice to take effect.

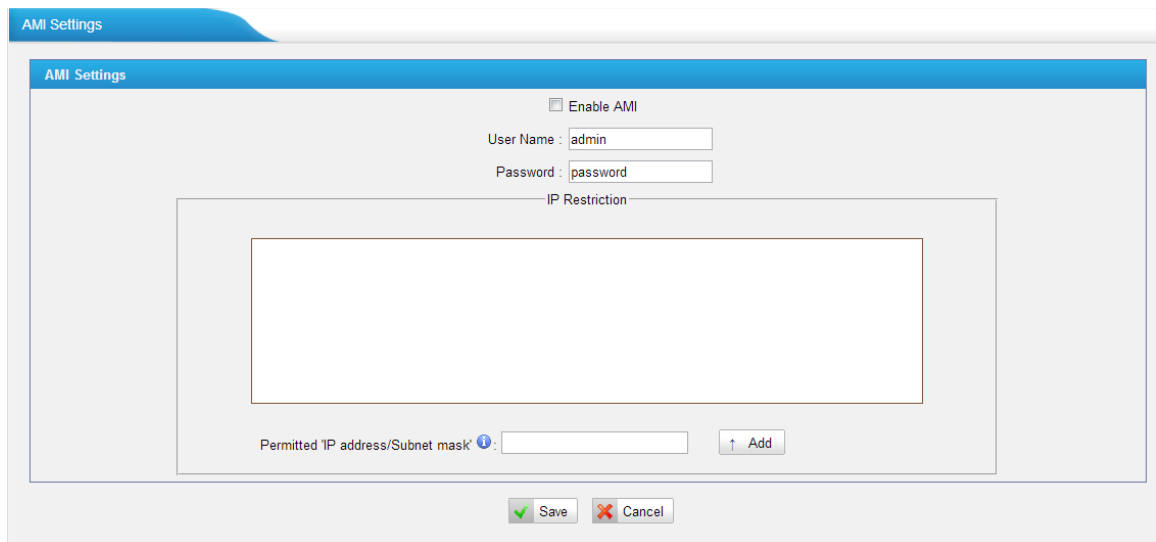
3.3 AMI settings*

The Asterisk Manager Interface (AMI) allows a client program to connect to an Asterisk instance and issue commands or read events over a TCP/IP stream. Integrators will find this particularly useful when trying to track the state of a telephony client inside Asterisk, and directing that client based on custom (and possibly dynamic) rules.

For more information, you can refer to this page:

<http://www.voip-info.org/wiki/view/Asterisk+manager+API>

Note: this feature is disabled by default; there is no need to enable it for general use. If it's enabled, please change account and configure IP restriction.



The image shows the 'AMI Settings' form in the Yeastar MyPBX SOHO V4/V5 Administrator's Guide. The form has a blue header bar with the text 'AMI Settings'. Below the header, there is a section for 'Enable AMI' with a checkbox. Underneath, there are two input fields: 'User Name' with the value 'admin' and 'Password' with the value 'password'. Below these is a section for 'IP Restriction' which contains a large empty rectangular box. At the bottom of the 'IP Restriction' section, there is a label 'Permitted IP address/Subnet mask' followed by an input field and an 'Add' button. At the very bottom of the form, there are 'Save' and 'Cancel' buttons.

Figure H-3-6

To manage the accounts to access AMI, we can configure it in AMI page directly.
Click System→System Preferences→AMI Settings.

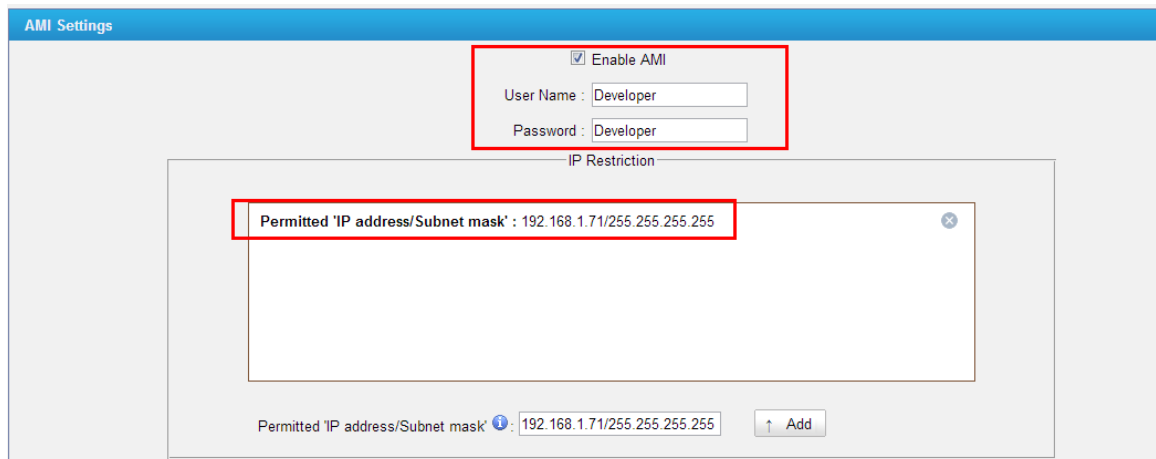
For example, the AMI account I want is:

User name: Developer

Password: Developer

The only IP address that's allowed to log in is 192.168.1.71.

We can configure it like this:

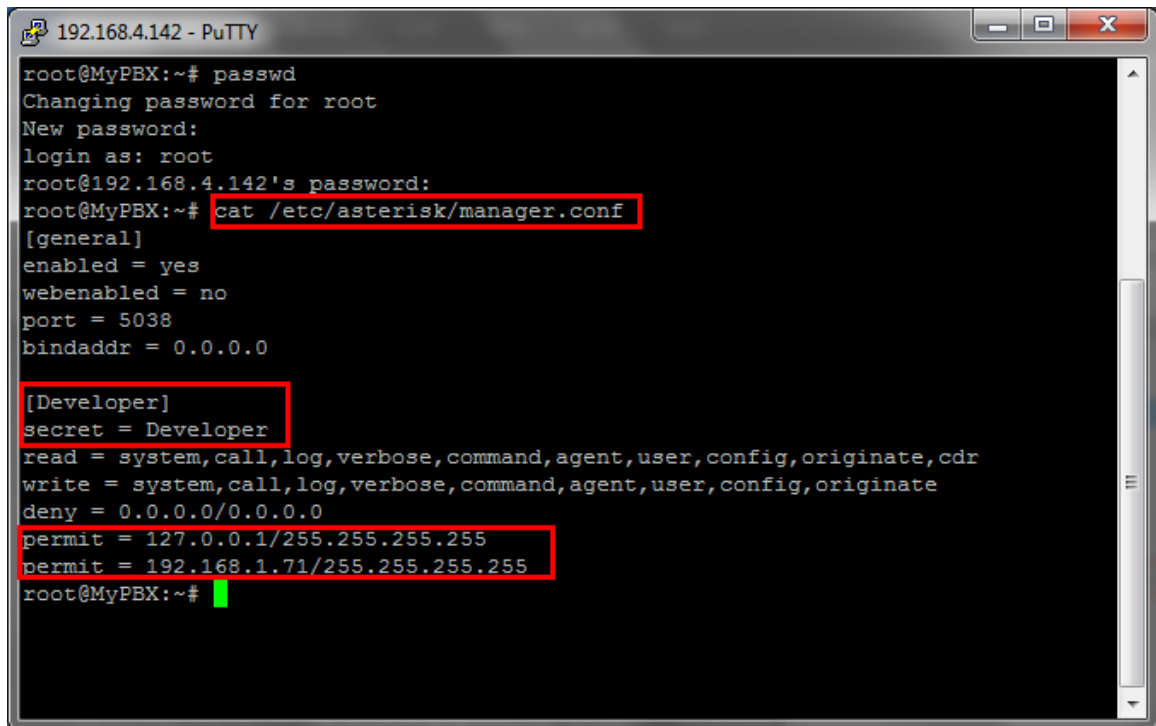


The image shows the 'AMI Settings' form with the configuration from the previous example. The 'Enable AMI' checkbox is checked. The 'User Name' field contains 'Developer' and the 'Password' field contains 'Developer'. The 'IP Restriction' section now contains a list of permitted IP addresses. The first entry is 'Permitted IP address/Subnet mask: 192.168.1.71/255.255.255.255'. Below this list, there is a label 'Permitted IP address/Subnet mask' followed by an input field containing '192.168.1.71/255.255.255.255' and an 'Add' button. The 'Save' and 'Cancel' buttons are still at the bottom.

Figure H-3-7

Save it and apply the changes.

To confirm more details, please try command "cat /etc/asterisk/manager.conf"



```

192.168.4.142 - PuTTY
root@MyPBX:~# passwd
Changing password for root
New password:
login as: root
root@192.168.4.142's password:
root@MyPBX:~# cat /etc/asterisk/manager.conf
[general]
enabled = yes
webenabled = no
port = 5038
bindaddr = 0.0.0.0

[Developer]
secret = Developer
read = system,call,log,verbose,command,agent,user,config,originate,cdr
write = system,call,log,verbose,command,agent,user,config,originate
deny = 0.0.0.0/0.0.0.0
permit = 127.0.0.1/255.255.255.255
permit = 192.168.1.71/255.255.255.255
root@MyPBX:~#

```

Figure H-3-8

3.4 TFTP*

MyPBX can work as a TFTP server when using “phone provisioning”, and this feature is enabled by default. If all the phones are well provisioned, you can disable this access to protect the configuration files of MyPBX.

Click “System→Security Center→Service” to disable it directly.

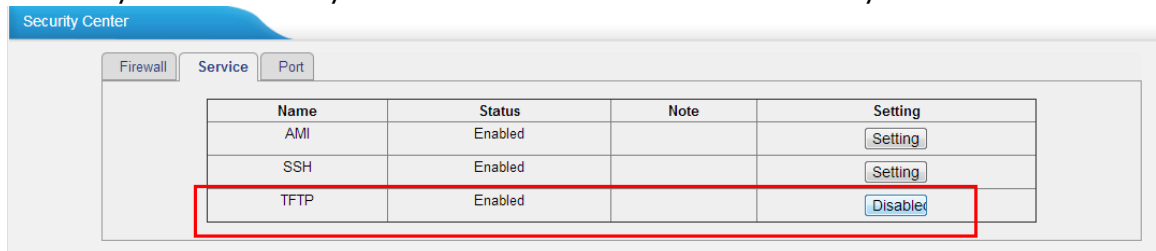


Figure H-3-9

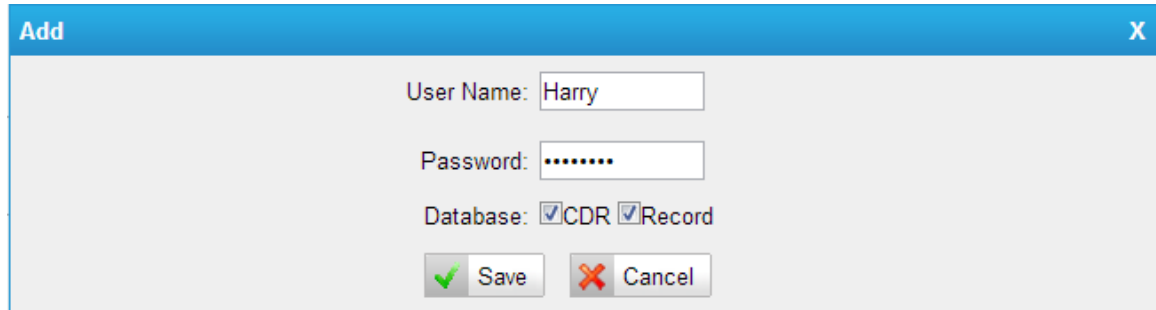
3.5 Database Grant*

MyPBX has integrated MySQL since x.18.0.xx, which provides convenience for users to manage the CDR and the Recording log. To protect the database access, we need to set up user name and password separately before login.

There is no account configured by default, if you need to connect the database

using third party software, you need to set up this first.

For example, username: Harry, password: Harry123

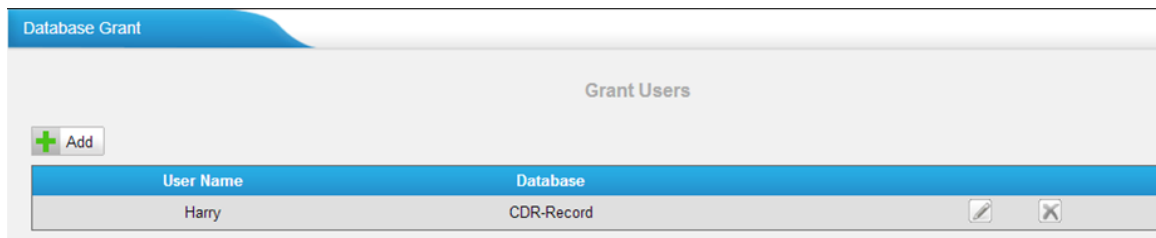


The 'Add' dialog box contains the following fields and controls:

- User Name:** A text input field containing 'Harry'.
- Password:** A password input field with masked characters (dots).
- Database:** Two checked checkboxes labeled 'CDR' and 'Record'.
- Buttons:** A green 'Save' button and a red 'Cancel' button.

Figure H-3-10

Save it and apply the changes.



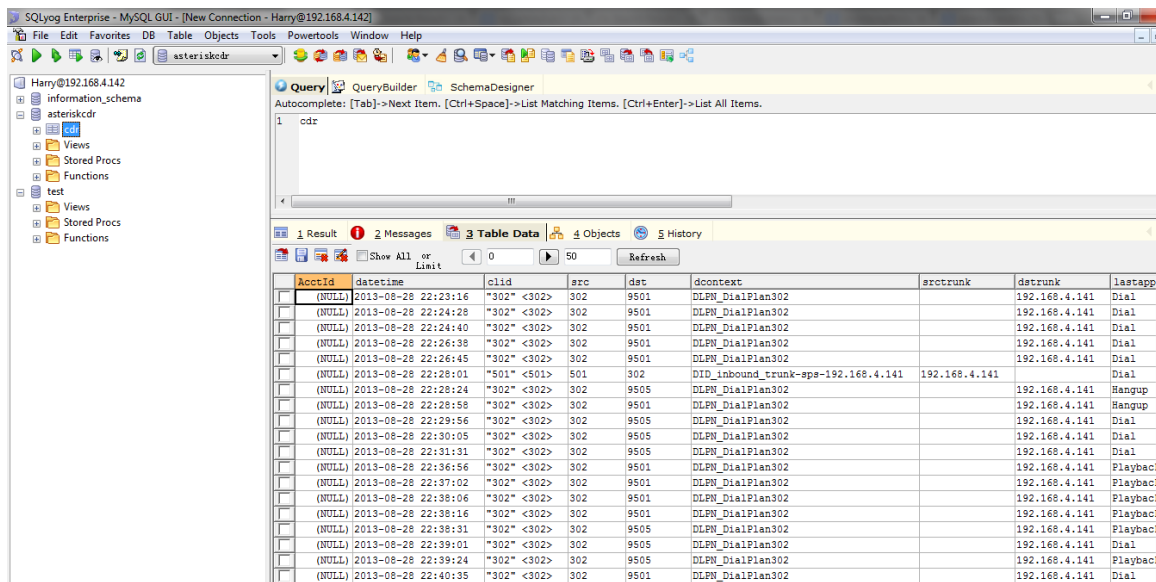
The 'Database Grant' window shows a table with the following data:

User Name	Database
Harry	CDR-Record

There is an 'Add' button with a green plus icon and a 'Grant Users' button.

Figure H-3-11

When logging in using other software, we can check the CDR.



The screenshot shows the SQLyog Enterprise interface with a query executed on the 'cdr' table. The results are displayed in a table with the following columns and data:

AccId	datetime	clid	src	dst	dcontext	srctrunk	dsttrunk	lastapp
(NULL)	2013-08-28 22:23:16	"302" <302>	302	9501	DLPN_DialPlan302		192.168.4.141	Dial
(NULL)	2013-08-28 22:24:28	"302" <302>	302	9501	DLPN_DialPlan302		192.168.4.141	Dial
(NULL)	2013-08-28 22:24:40	"302" <302>	302	9501	DLPN_DialPlan302		192.168.4.141	Dial
(NULL)	2013-08-28 22:26:38	"302" <302>	302	9501	DLPN_DialPlan302		192.168.4.141	Dial
(NULL)	2013-08-28 22:26:45	"302" <302>	302	9501	DLPN_DialPlan302		192.168.4.141	Dial
(NULL)	2013-08-28 22:28:01	"501" <501>	501	302	DTD_inbound_trunk-sps-192.168.4.141	192.168.4.141		Dial
(NULL)	2013-08-28 22:28:24	"302" <302>	302	9505	DLPN_DialPlan302		192.168.4.141	Hangup
(NULL)	2013-08-28 22:28:58	"302" <302>	302	9505	DLPN_DialPlan302		192.168.4.141	Hangup
(NULL)	2013-08-28 22:29:56	"302" <302>	302	9505	DLPN_DialPlan302		192.168.4.141	Dial
(NULL)	2013-08-28 22:30:05	"302" <302>	302	9505	DLPN_DialPlan302		192.168.4.141	Dial
(NULL)	2013-08-28 22:31:31	"302" <302>	302	9505	DLPN_DialPlan302		192.168.4.141	Dial
(NULL)	2013-08-28 22:36:56	"302" <302>	302	9501	DLPN_DialPlan302		192.168.4.141	Playbac
(NULL)	2013-08-28 22:37:02	"302" <302>	302	9501	DLPN_DialPlan302		192.168.4.141	Playbac
(NULL)	2013-08-28 22:38:06	"302" <302>	302	9501	DLPN_DialPlan302		192.168.4.141	Playbac
(NULL)	2013-08-28 22:38:16	"302" <302>	302	9501	DLPN_DialPlan302		192.168.4.141	Playbac
(NULL)	2013-08-28 22:38:31	"302" <302>	302	9505	DLPN_DialPlan302		192.168.4.141	Playbac
(NULL)	2013-08-28 22:39:01	"302" <302>	302	9505	DLPN_DialPlan302		192.168.4.141	Dial
(NULL)	2013-08-28 22:39:24	"302" <302>	302	9505	DLPN_DialPlan302		192.168.4.141	Playbac
(NULL)	2013-08-28 22:40:35	"302" <302>	302	9501	DLPN_DialPlan302		192.168.4.141	Dial

Figure H-3-12

3.6 Alert settings

After enabling alert settings, if the device is attacked, the system will notify users the alert via call or e-mail. The attack modes include IP attack and Web Login.

3.6.1 IPATTACK

When the system is attacked by some IP addresses, the firewall will add the IP to auto IP Blacklist and notify the user if it match the protection rule.

Example: Configure to notify extension 500, outbound number 5503301 and E-mail alert@yeastar.com.
configuration could be as below.

Phone Notification Settings:

Phone Notification: Yes

Number: 500;5503301

Attempts: 1

Interval: 60s

Prompt: default

Note: If there's an outbound number to notify, the number should fit the dial pattern of the outbound route.

E-mail Notification Settings:

E-mail Notification: Yes

To: alert@yeastar.com

Subject: IPAttack

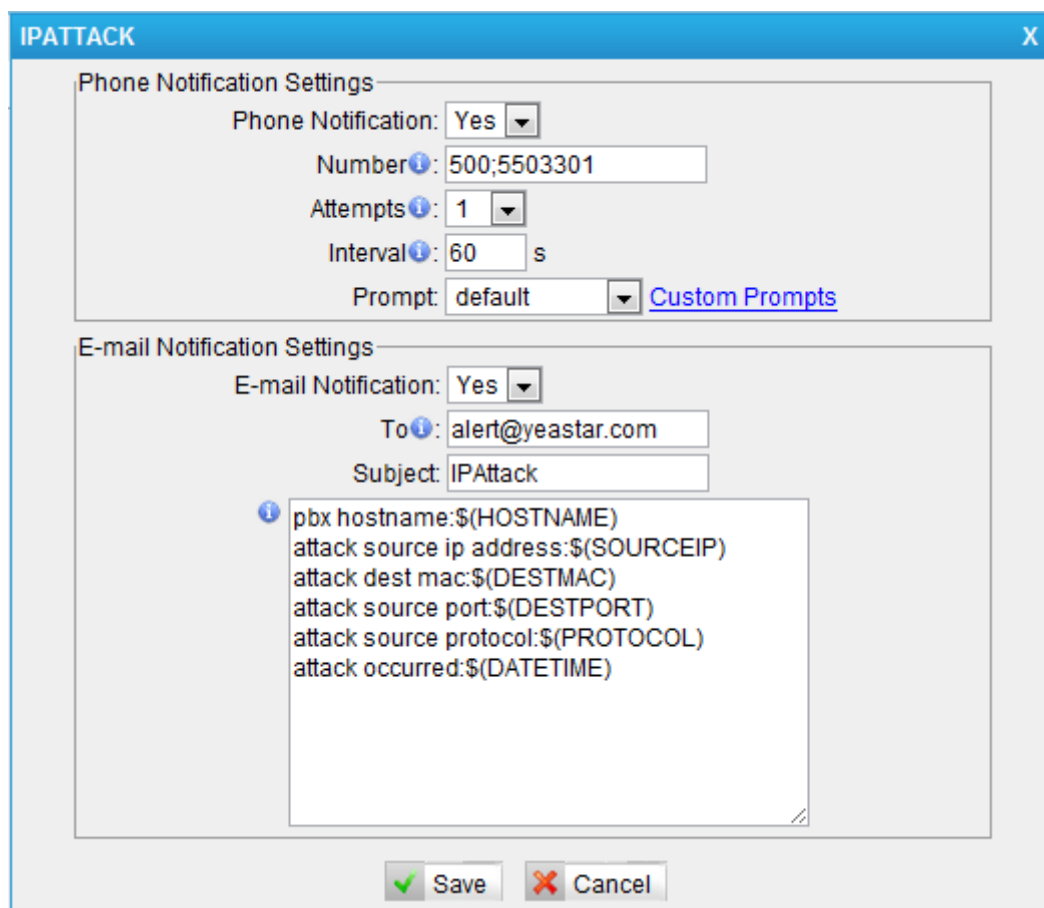


Figure H-3-13

3.6.2 WEBLOGIN

Enter the password incorrectly five times when logging in MyPBX Web interface will be deemed as attack, the system will limit the IP login within 10 minutes and notify the user.

Example: Configure to notify extension 500, outbound number 5503301 and E-mail alert@yeastar.com.
configuration could be as below.

Phone Notification Settings:
Phone Notification: Yes
Number: 500;5503301
Attempts: 1
Interval: 60s
Prompt: default

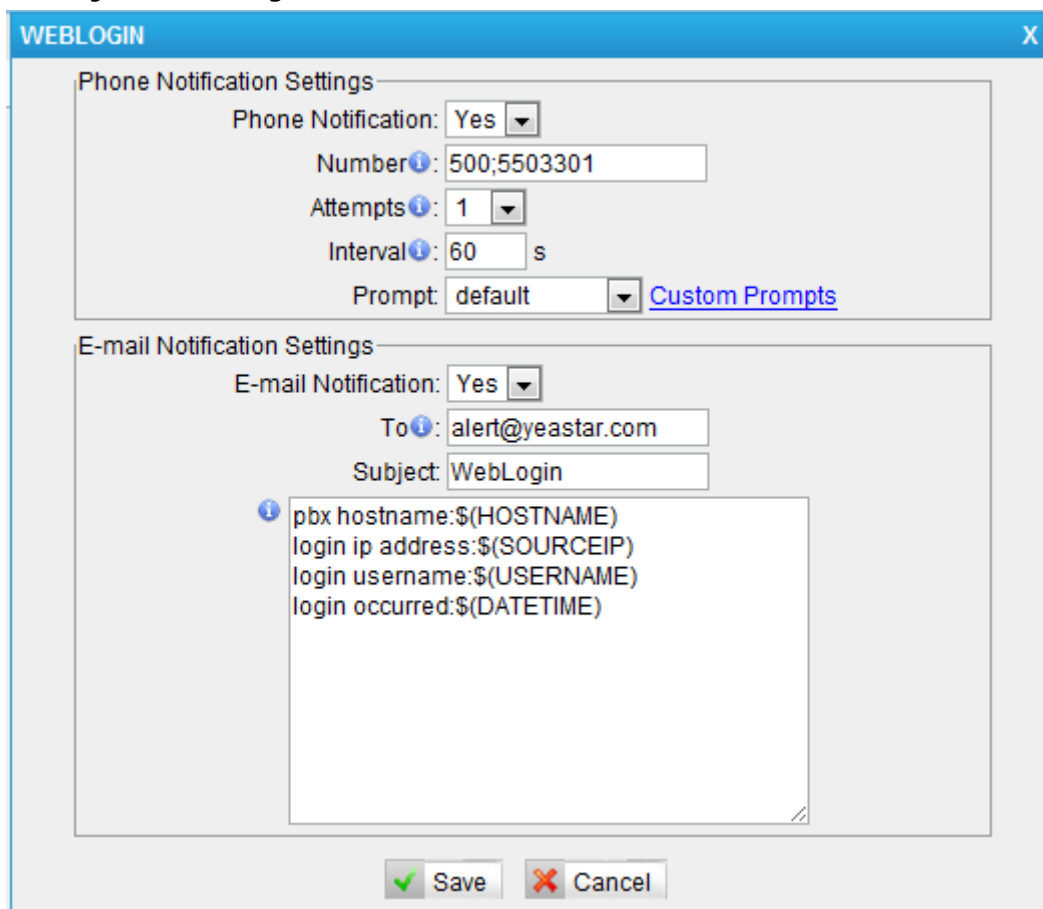
Note: If there's an outbound number to notify, the number should fit the dial pattern of the outbound route.

E-mail Notification Settings:

E-mail Notification: Yes

To: alert@yeastar.com

Subject: WebLogin



The screenshot shows a window titled "WEBLOGIN" with two sections: "Phone Notification Settings" and "E-mail Notification Settings".

Phone Notification Settings:

- Phone Notification: Yes (dropdown)
- Number: 500;5503301 (text field)
- Attempts: 1 (dropdown)
- Interval: 60 s (text field)
- Prompt: default (dropdown) with a link to [Custom Prompts](#)

E-mail Notification Settings:

- E-mail Notification: Yes (dropdown)
- To: alert@yeastar.com (text field)
- Subject: WebLogin (text field)
- Information box:
 - pbx hostname:\$(HOSTNAME)
 - login ip address:\$(SOURCEIP)
 - login username:\$(USERNAME)
 - login occurred:\$(DATETIME)

At the bottom are "Save" and "Cancel" buttons.

Figure H-3-14

4. International call limit

4.1 Limit call credit at provider side

We can ask VoIP/PSTN/ISDN provider for help to limit the credit of international calls in advance, then the hacker cannot dial international calls. Each provider has its own policy. You can also ask provider to disable international call if not needed.

4.2 Set password for international call

MyPBX allows you to configure password for outbound routes.

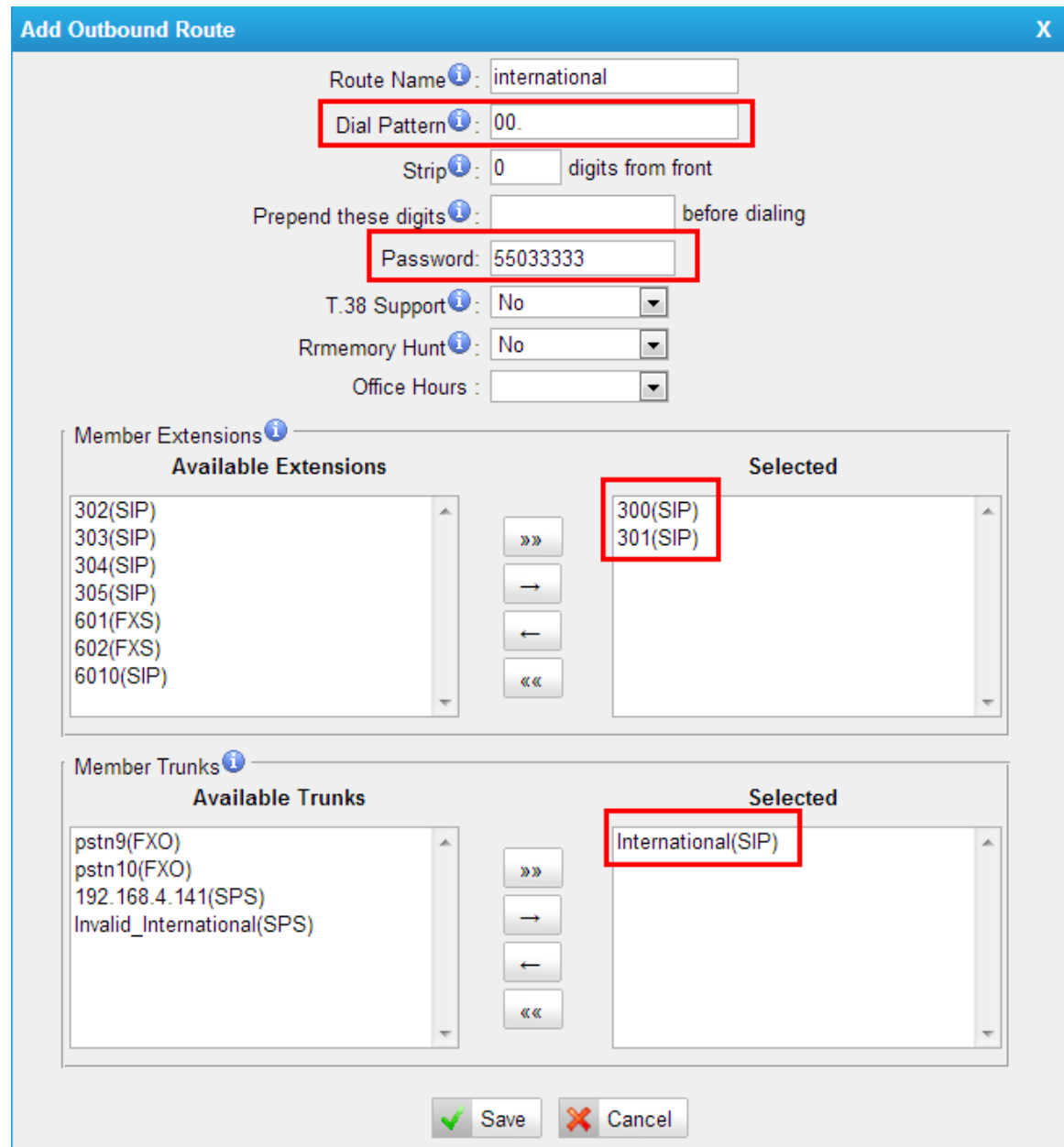
Click "PBX→Outbound Call Control→ Outbound Route".

For example, the password you need is 55033333

Dial pattern: 00. <Don't miss the dot here>

Password: 55033333

Choose the allowed extension and the trunk to the right side like this:



Add Outbound Route

Route Name: international

Dial Pattern: 00.

Strip: 0 digits from front

Prepend these digits: before dialing

Password: 55033333

T.38 Support: No

Rmemory Hunt: No

Office Hours:

Member Extensions

Available Extensions	Selected
302(SIP)	300(SIP)
303(SIP)	301(SIP)
304(SIP)	
305(SIP)	
601(FXS)	
602(FXS)	
6010(SIP)	

Member Trunks

Available Trunks	Selected
pstn9(FXO)	International(SIP)
pstn10(FXO)	
192.168.4.141(SPS)	
Invalid_International(SPS)	

Save Cancel

Figure H-4-1

Save and apply the changes, when 300 and 301 pick up headsets and dial a international number, MyPBX will ask for the password, if passed, the call will be dialed out. If not, the call will be dropped.

4.3 Disable international call in MyPBX

We can ask the provider for help to disable international calls in advance, if it's not possible, we can configure the rules in MyPBX side to drop all the international calls. Here are the detailed steps.

Step1. Create an invalid SIP trunk

Create an invalid SIP trunk in "PBX→VoIP trunk→Service Provider". The IP address can be an invalid one, like 127.0.0.1

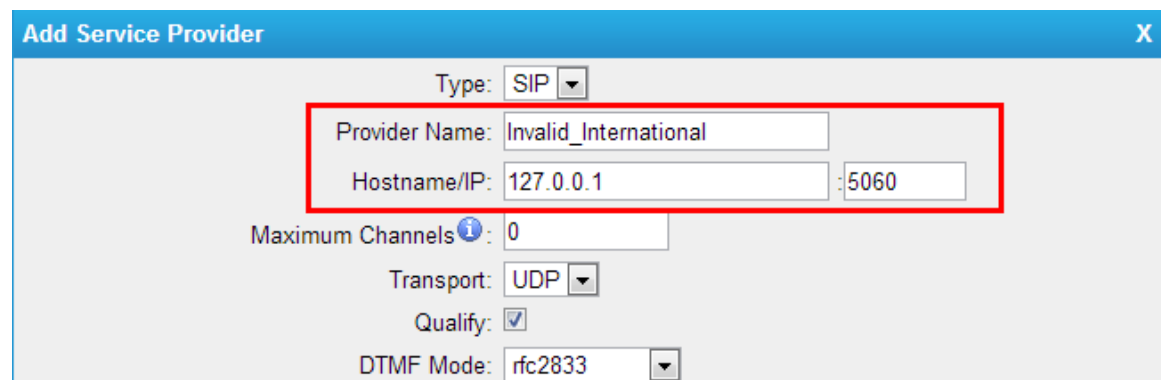


Figure H-4-2

Save it and apply the changes. The status of this trunk is unreachable of course. That's what we want.

Step2. Create an outbound route for all extensions and this trunk to route international calls.

Click "PBX→Outbound Call Control→Outbound Route", create a new one:

Name: NoInternational

Dial pattern: 00. <Don't miss that dot here>

Strip: 0

Choose all extensions and that special trunk (Invalid_international) to the right side.

Add Outbound Route

Route Name: NoInternational
Dial Pattern: 00.
Strip: 0 digits from front
Prepend these digits: before dialing
Password:
T.38 Support: No
Rmemory Hunt: No
Office Hours:

Member Extensions

Available Extensions

Selected

300(SIP)
301(SIP)
302(SIP)
303(SIP)
304(SIP)
305(SIP)
601(FXS)
602(FXS)

Member Trunks

Available Trunks

Selected

Invalid_International(SPS)

Save Cancel

Figure H-4-3

Save it and apply the changes. Then click the arrow at the left side to set it to the top.

Outbound Routes

+ Add Outbound Route

	Route Name	Dial Pattern		
↕	NoInternational	00.	✎	✕
↕ ↕ ↕ ↕	sip_out	8.	✎	✕
↕ ↕	pstnout	9.	✎	✕

Figure H-4-4

In this case, all international call requests will be routed to this invalid trunk. Ie. The call is dropped directly.

APPENDIX I How to Use TLS in MyPBX

I.1 How to register IP phones to MyPBX via TLS

MyPBX is working as a SIP server, IP phones register to MyPBX as extensions via TLS.

1. Enable TLS in MyPBX's web interface

Click "PBX→SIP settings→General" to get the settings about TLS, which is disabled by default. If you are using MyPBX SOHO, please find it in "Internal Settings→SIP Settings" page.

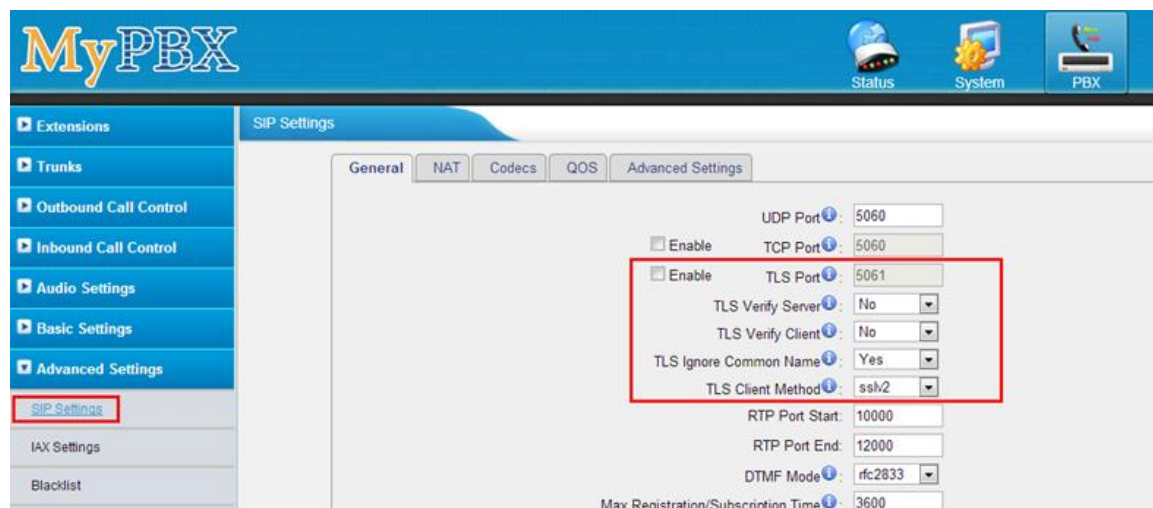


Figure I-1

•TLS Port

Port use for Sip registrations, Default is 5061.

•TLS Verify Server

When using MyPBX as a TLS client, whether or not to verify server's certificate. It is "No" by default.

•TLS Verify Client

When using MyPBX as a TLS server, whether or not to verify client's certificate. It is "No" by default.

•TLS Ignore Common Name

Set this parameter as "No", then common name must be the same with IP or domain name.

•TLS Client Method

When using MyPBX as a TLS client, specify the protocol for outbound TLS connections. You can select it as tlsv1, sslv2 or sslv3.

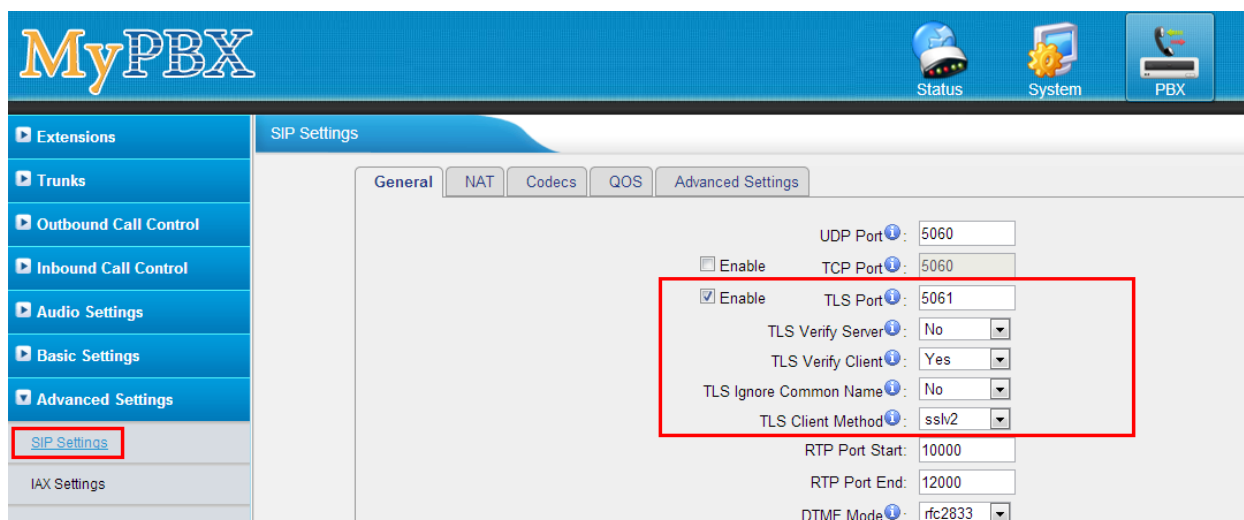


Figure I-2

Notes:

1. For security reason, we recommend enabling "TLS Verify Client" and disabling "TLS Ignore Common Name", in which case, MyPBX will verify IP phone's Certificate, the common name inside CA should be the same as its IP or domain name.
2. TLS Client Method: it's the TLS method of IP phone; you can contact the manufacturer of the IP phone to get that.
3. You need to reboot MyPBX to take effect after enabling TLS.

2. Prepare the whole certificates for TLS

Here are the certificates of MyPBX and IP phones for TLS registry as the screen shot above:

MyPBX's CA: CA.crt.

MyPBX's server certificate: asterisk.pem.

IP phone's CA: CA.crt or CA.csr.

IP phone's server certificate: client.pem.

The certificate is generated via the toolkit OpenSSL, you can compile the source package from <http://www.openssl.org/>, or download the tool used here, download link:

www.yeastar.com/download/tools/TLS_CA_Tool.rar

You can find the files inside the package like these:

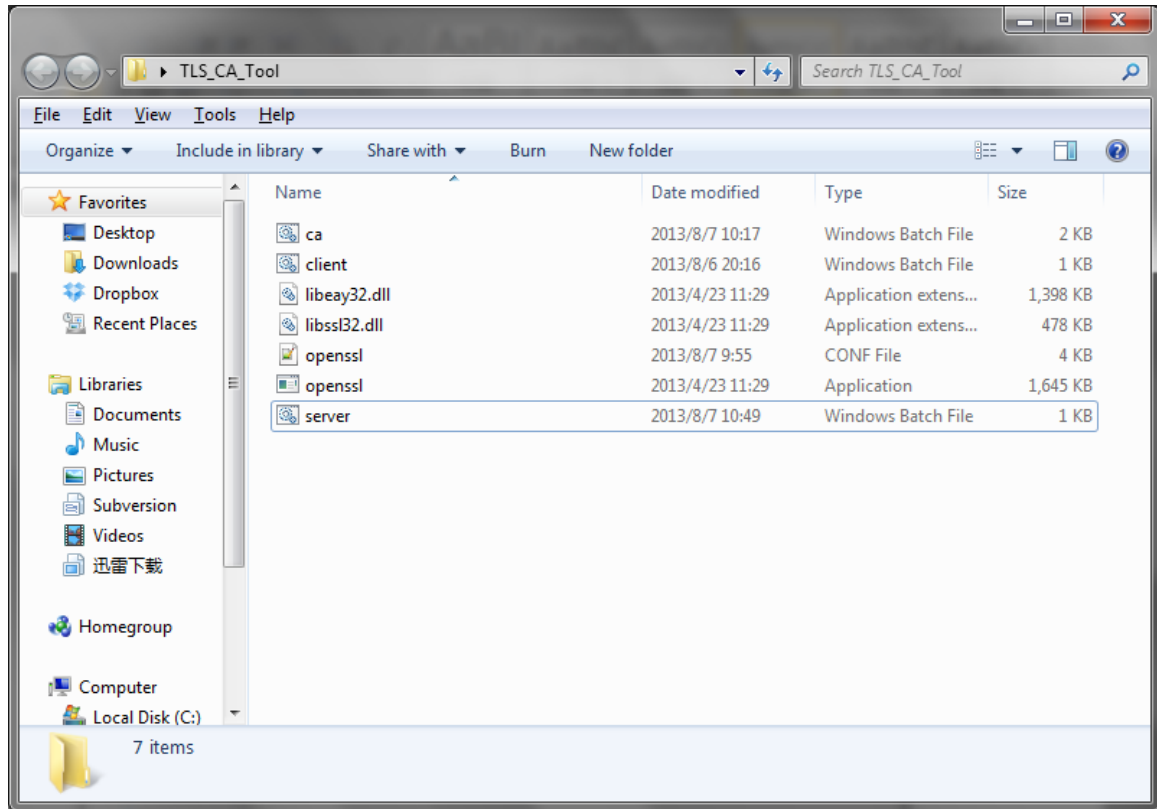


Figure I-3

Ca.bat: Make the CA.crt for IP phone and MyPBX

Client.bat: make the "client.pem", it's the "IP phone's server certificate".

Server.bat: make the "asterisk.pem", it's the "MyPBX's server certificate".

Here are the steps to make all the certificates.

Step1. Prepare MyPBX's CA: CA.crt

Double click ca.bat

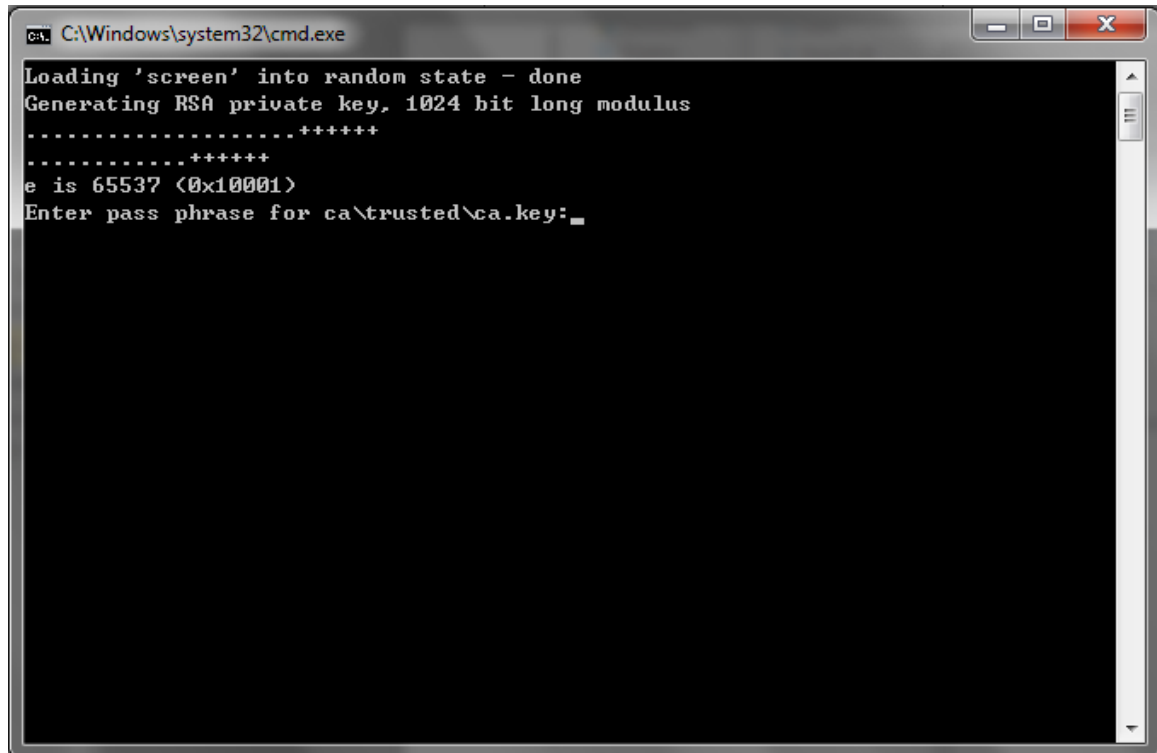
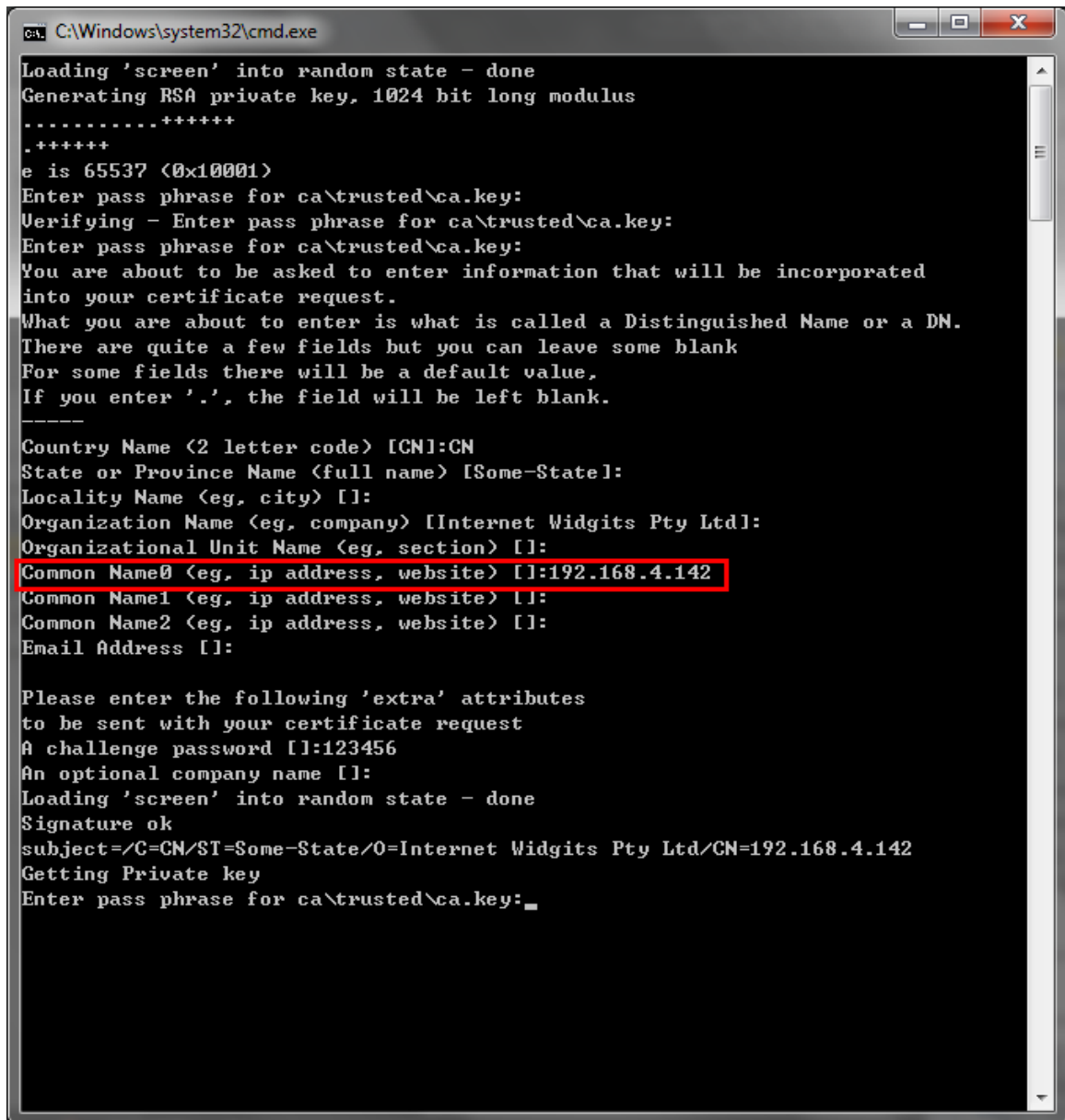


Figure I-4

Just follow the guide to input the information of MyPBX step by step.
In this example, MyPBX's IP address is 192.168.4.142.



```
C:\Windows\system32\cmd.exe
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
..+++++
e is 65537 (0x10001)
Enter pass phrase for ca\trusted\ca.key:
Verifying - Enter pass phrase for ca\trusted\ca.key:
Enter pass phrase for ca\trusted\ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:CN
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name0 (eg, ip address, website) [192.168.4.142]
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Loading 'screen' into random state - done
Signature ok
subject=/C=CN/ST=Some-State/O=Internet Widgits Pty Ltd/CN=192.168.4.142
Getting Private key
Enter pass phrase for ca\trusted\ca.key: _
```

Figure I-5

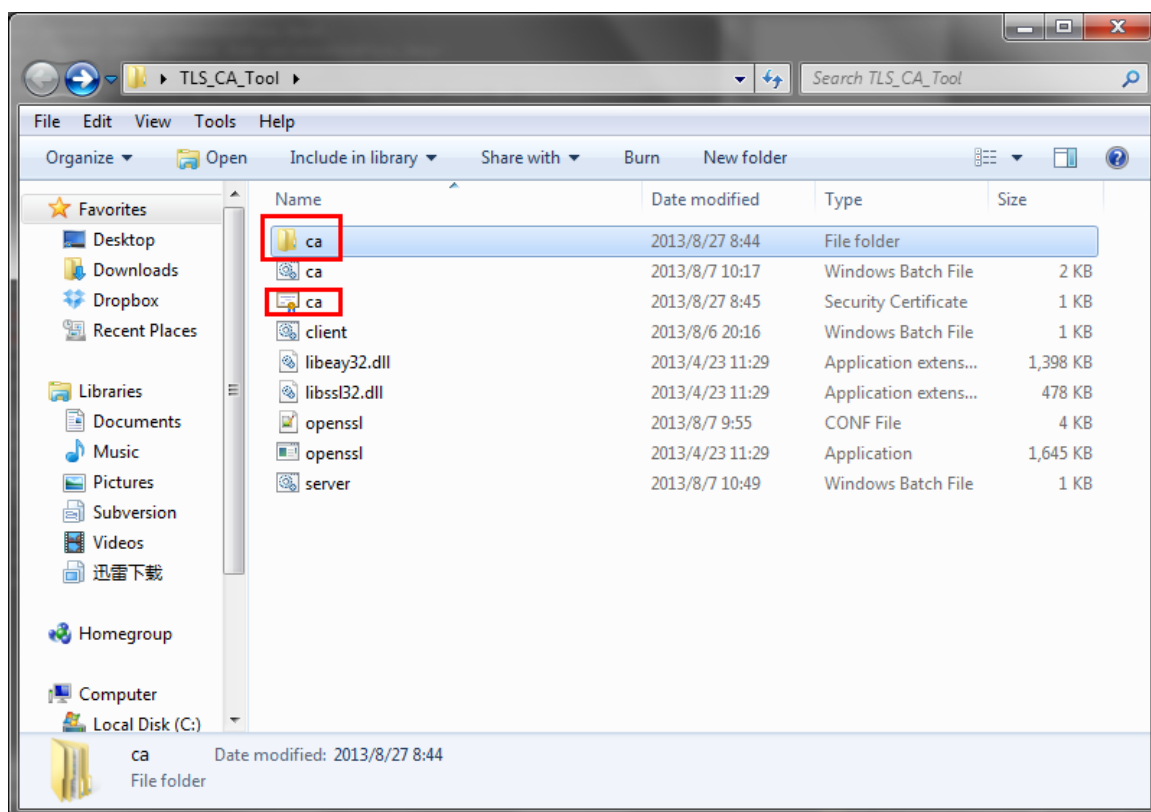


Figure I-6

This ca.crt is the same as the one in folder /TLS_CA_Tool/ca/trusted/.

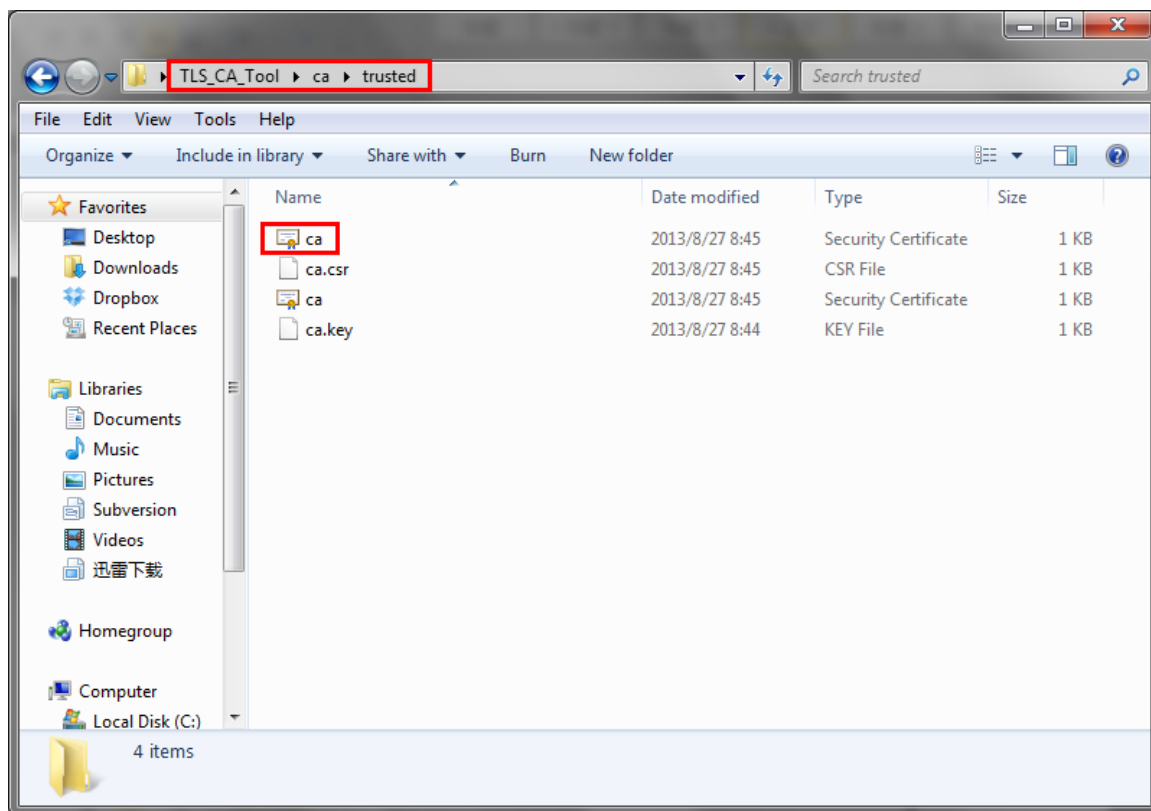


Figure I-7

MyPBX's CA: CA.crt is generated successfully.

Step2 Prepare "asterisk.pem", "MyPBX's server certificate"

We need the CA.crt and CA.key to make the server certificate.
Double click "server.bat".

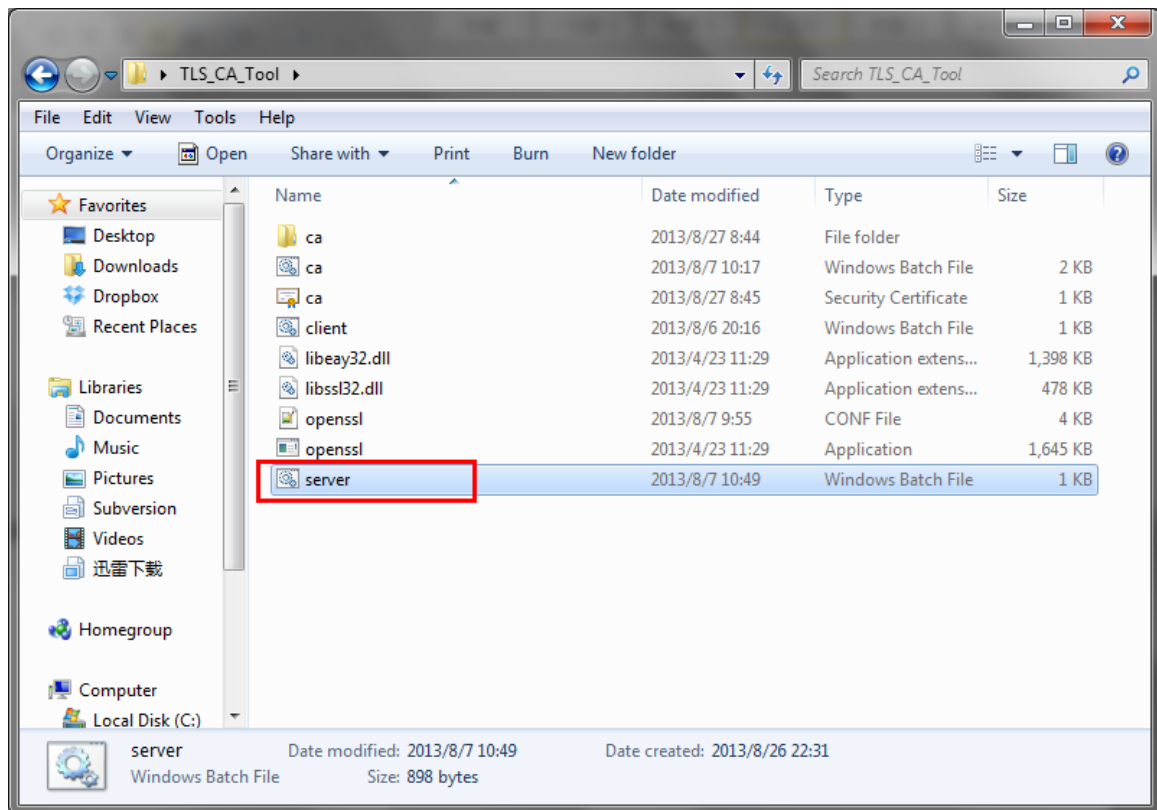
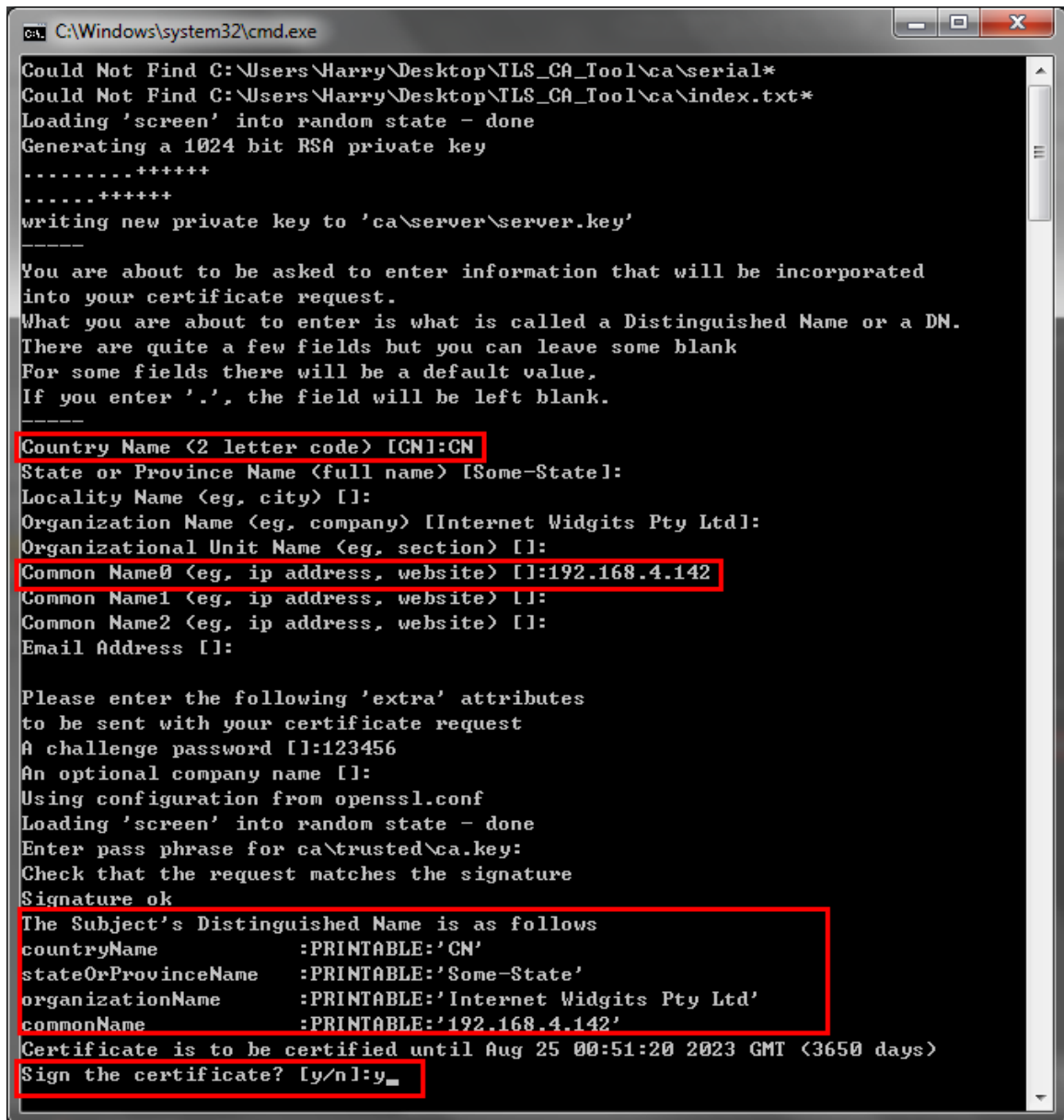


Figure I-8

Follow the guide to input information step by step, and make sure the information you have input matches the one you have input in Step1.



```
C:\Windows\system32\cmd.exe
Could Not Find C:\Users\Harry\Desktop\TLS_CA_Tool\ca\serial*
Could Not Find C:\Users\Harry\Desktop\TLS_CA_Tool\ca\index.txt*
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'ca\server\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name <2 letter code> [CN]:CN
State or Province Name <full name> [Some-State]:
Locality Name <eg, city> []:
Organization Name <eg, company> [Internet Widgits Pty Ltd]:
Organizational Unit Name <eg, section> []:
Common Name0 <eg, ip address, website> []:192.168.4.142
Common Name1 <eg, ip address, website> []:
Common Name2 <eg, ip address, website> []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Using configuration from openssl.conf
Loading 'screen' into random state - done
Enter pass phrase for ca\trusted\ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'CN'
stateOrProvinceName     :PRINTABLE:'Some-State'
organizationName        :PRINTABLE:'Internet Widgits Pty Ltd'
commonName              :PRINTABLE:'192.168.4.142'
Certificate is to be certified until Aug 25 00:51:20 2023 GMT (3650 days)
Sign the certificate? [y/n]:y
```

Figure I-9

Check the whole information then input “y” to continue. When done, you can find the asterisk.pem as the following picture shows.

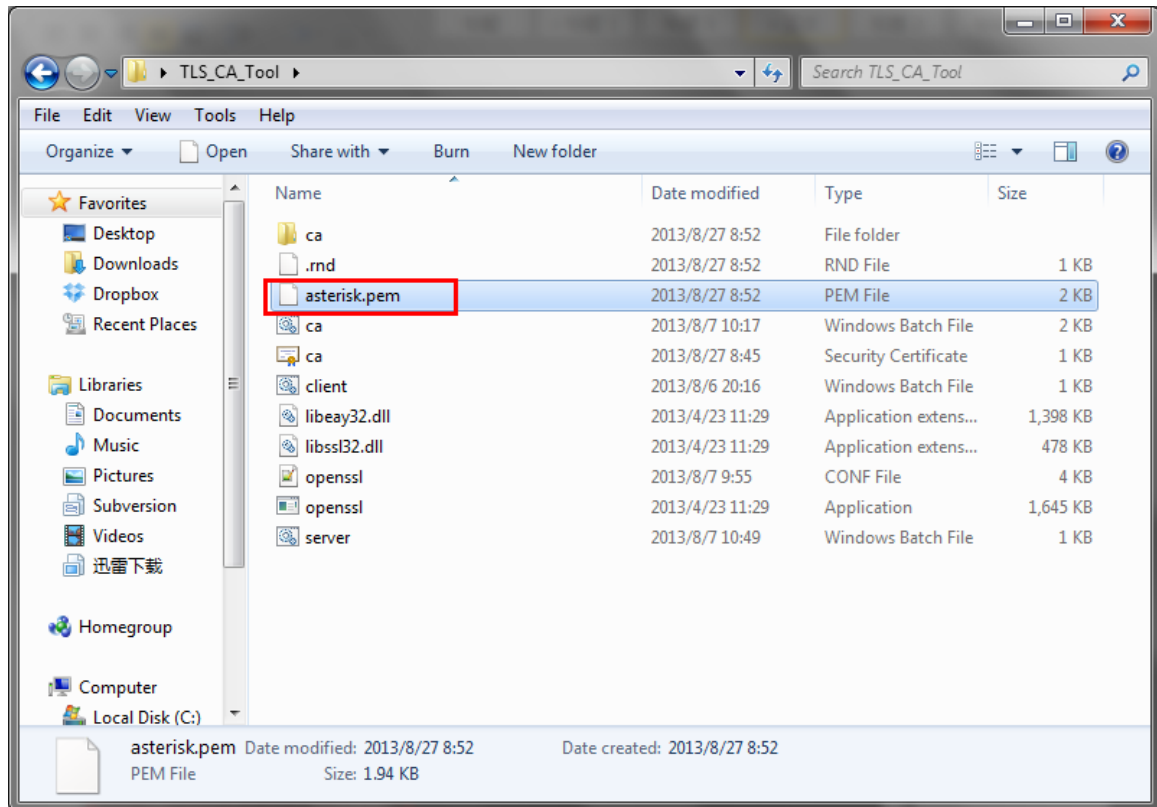


Figure I-10

asterisk.pem, the “MyPBX’s server certificate” is generated successfully.

Note: We can copy the asterisk.pem, ca.crt to another folder before making the IP phone’s certificate.

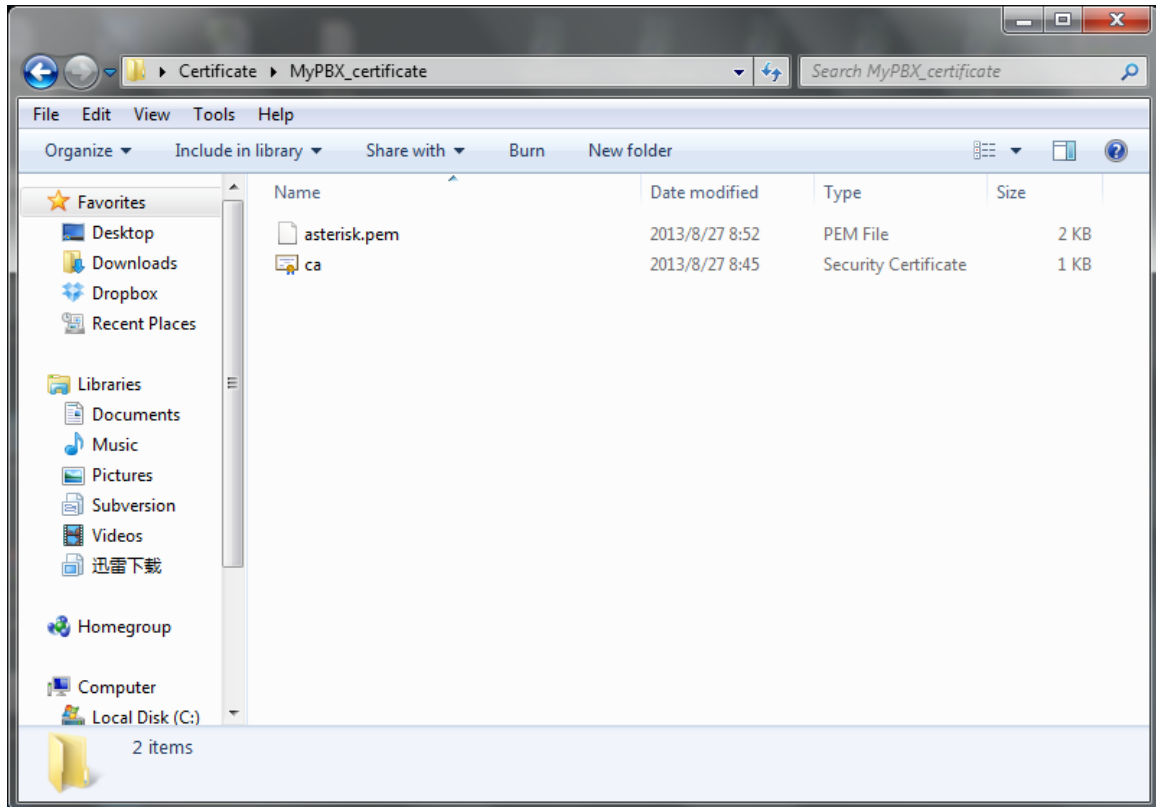


Figure I-11

Step3. Prepare the IP phone's certificate, ca.crt

Double click "ca.bat", input the information of IP phone step by step.

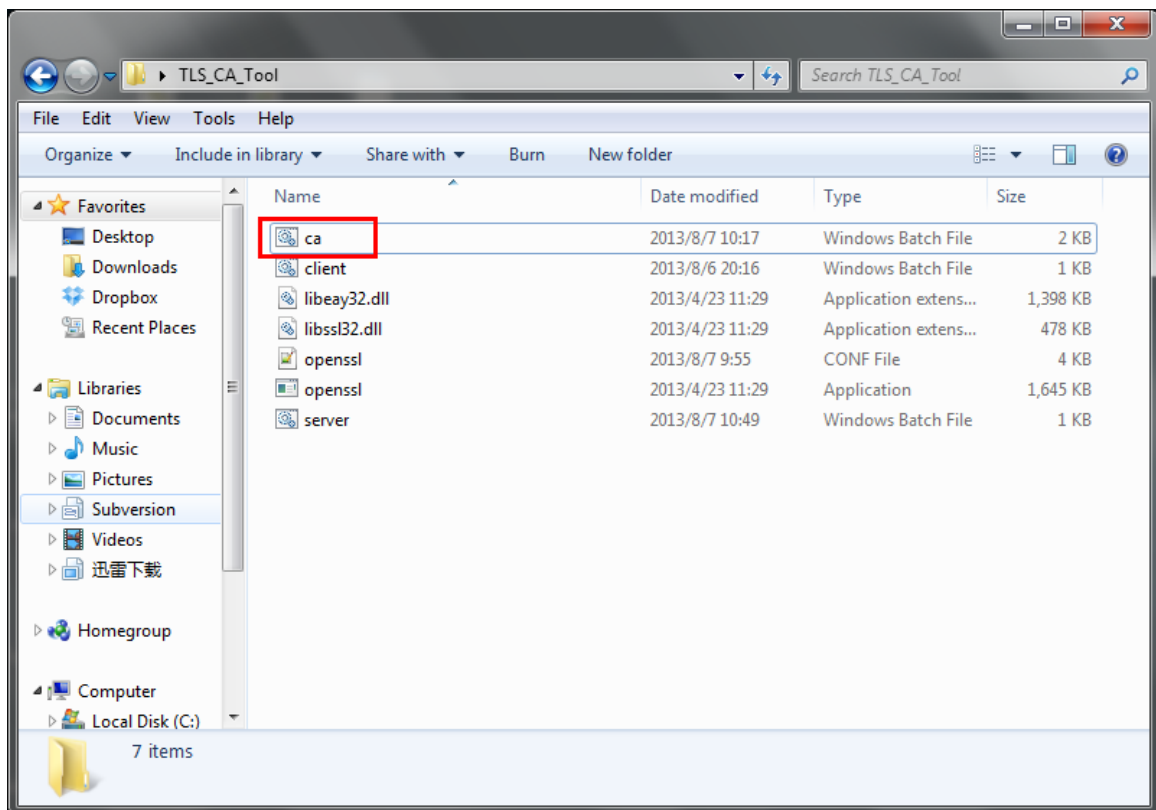
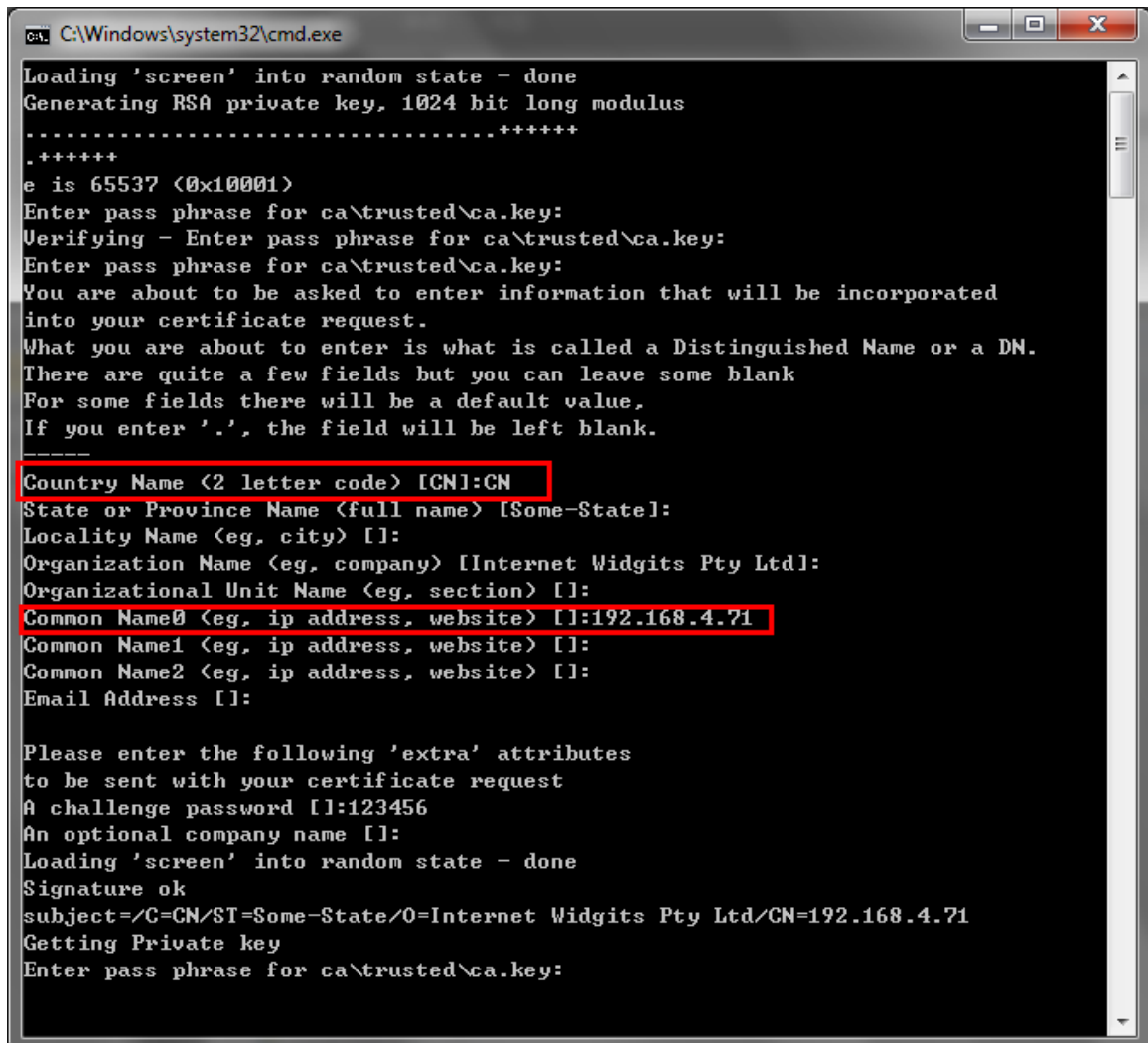


Figure I-12

In this example, the IP phone's IP address is 192.168.4.71.



```
C:\Windows\system32\cmd.exe
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
.+++++
e is 65537 (0x10001)
Enter pass phrase for ca\trusted\ca.key:
Verifying - Enter pass phrase for ca\trusted\ca.key:
Enter pass phrase for ca\trusted\ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:CN
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, ip address, website) [1:192.168.4.71]
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password [1:123456]
An optional company name []:
Loading 'screen' into random state - done
Signature ok
subject=/C=CN/ST=Some-State/O=Internet Widgits Pty Ltd/CN=192.168.4.71
Getting Private key
Enter pass phrase for ca\trusted\ca.key:
```

Figure I-13

When done, we can find the ca.crt in this folder.

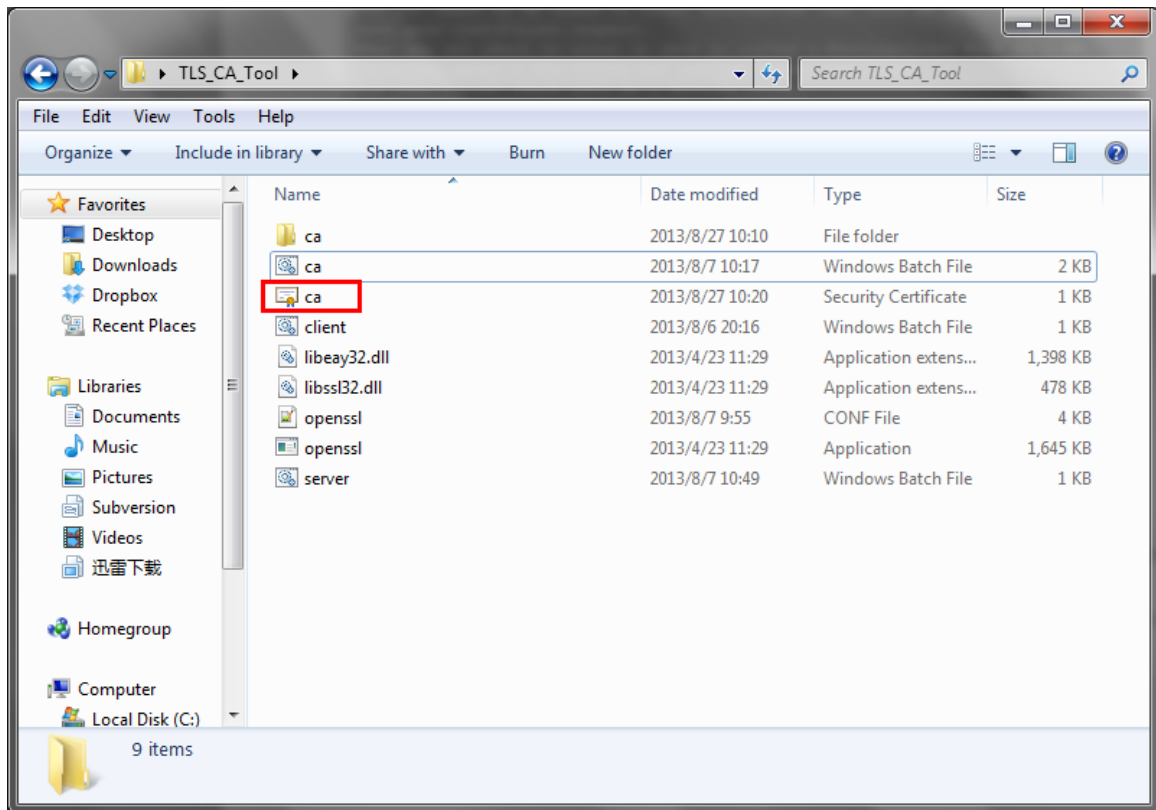


Figure I-14

The ca.crt in folder /TLS_CA_Tool/ca/trusted is the same as the above one.

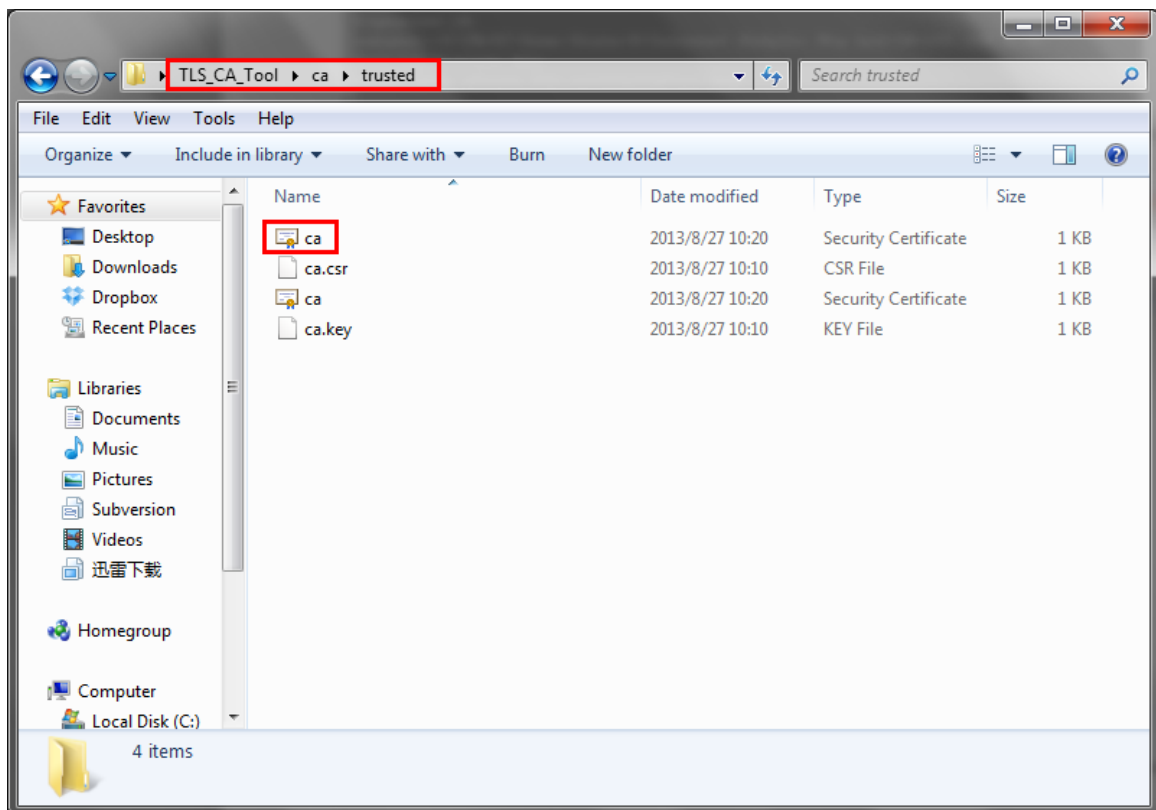


Figure I-15

The IP phone's certificate is finished.

Note: If you have got your own CA for IP phone, you can rename it to CA.crt and copy it to folder "/TLS_CA_Tool/ca/trusted" before making the "client.pem".

Step4. Prepare "client.pem", the "IP phone's server certificate".

Double click "client.bat".

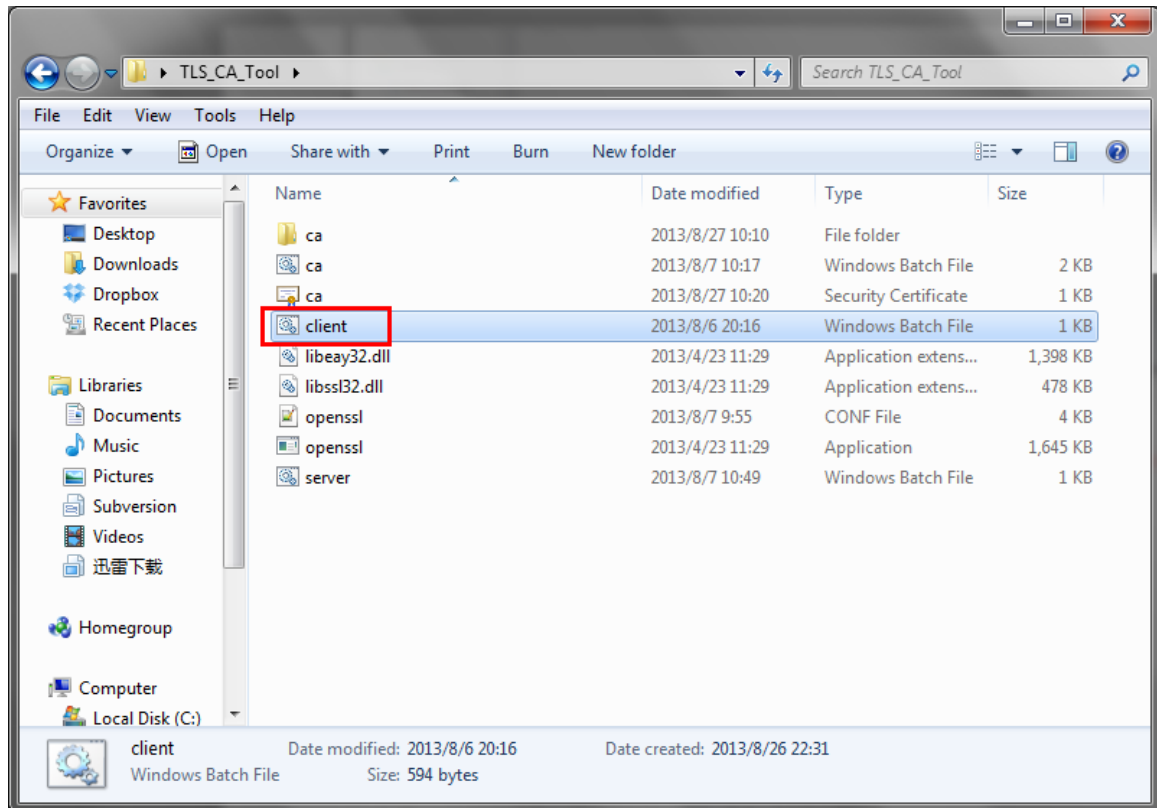


Figure I-16

Input the IP phone's information step by step in this script; make sure the content is the same as Step3.

```
C:\Windows\system32\cmd.exe
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'ca\client\client.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name <2 letter code> [CN]:CN
State or Province Name <full name> [Some-State]:
Locality Name <eg, city> []:
Organization Name <eg, company> [Internet Widgits Pty Ltd]:
Organizational Unit Name <eg, section> []:
Common Name0 <eg, ip address, website> []:192.168.4.71
Common Name1 <eg, ip address, website> []:
Common Name2 <eg, ip address, website> []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Using configuration from openssl.conf
Loading 'screen' into random state - done
Enter pass phrase for ca\trusted\ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'CN'
stateOrProvinceName     :PRINTABLE:'Some-State'
organizationName        :PRINTABLE:'Internet Widgits Pty Ltd'
commonName              :PRINTABLE:'192.168.4.71'
Certificate is to be certified until Aug 25 02:30:44 2023 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
```

Figure I-17

Confirm all the information we input before clicking “y” to finish this guide.

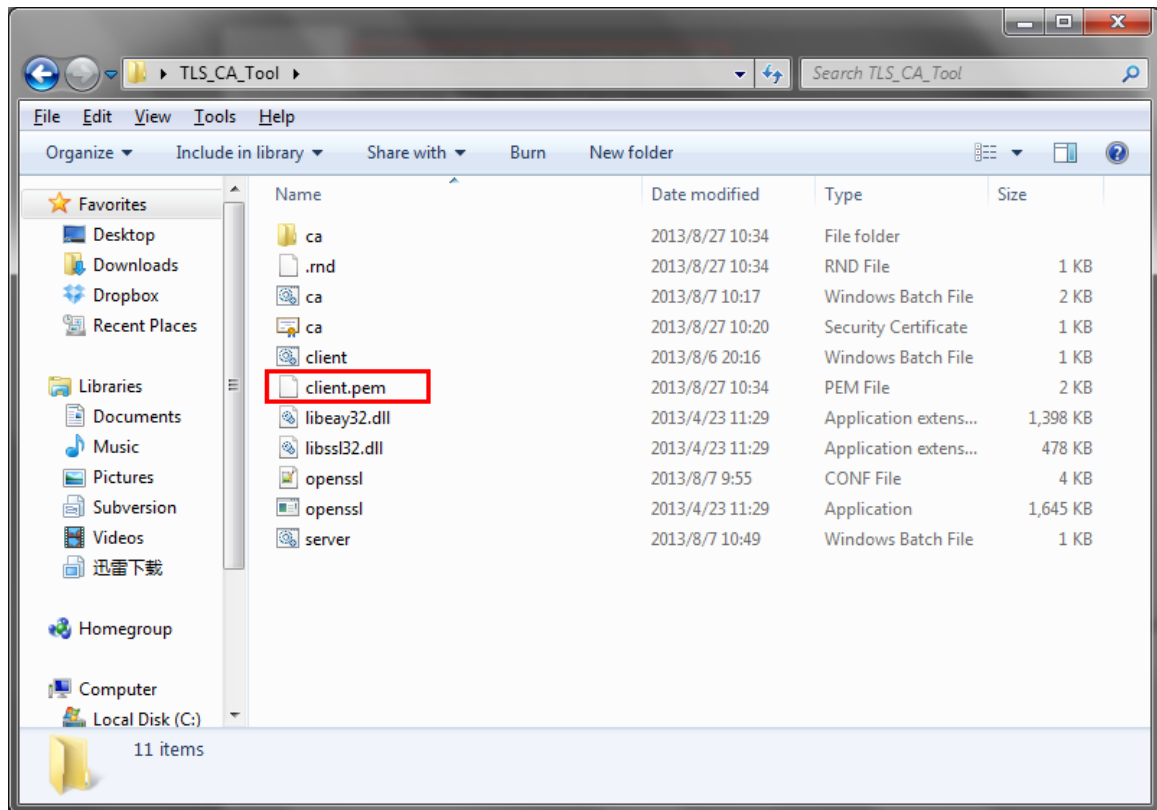


Figure I-18

The “IP phone’s server certificate” is ready.

Note: We can copy the client.pem, ca.crt to another folder before uploading.

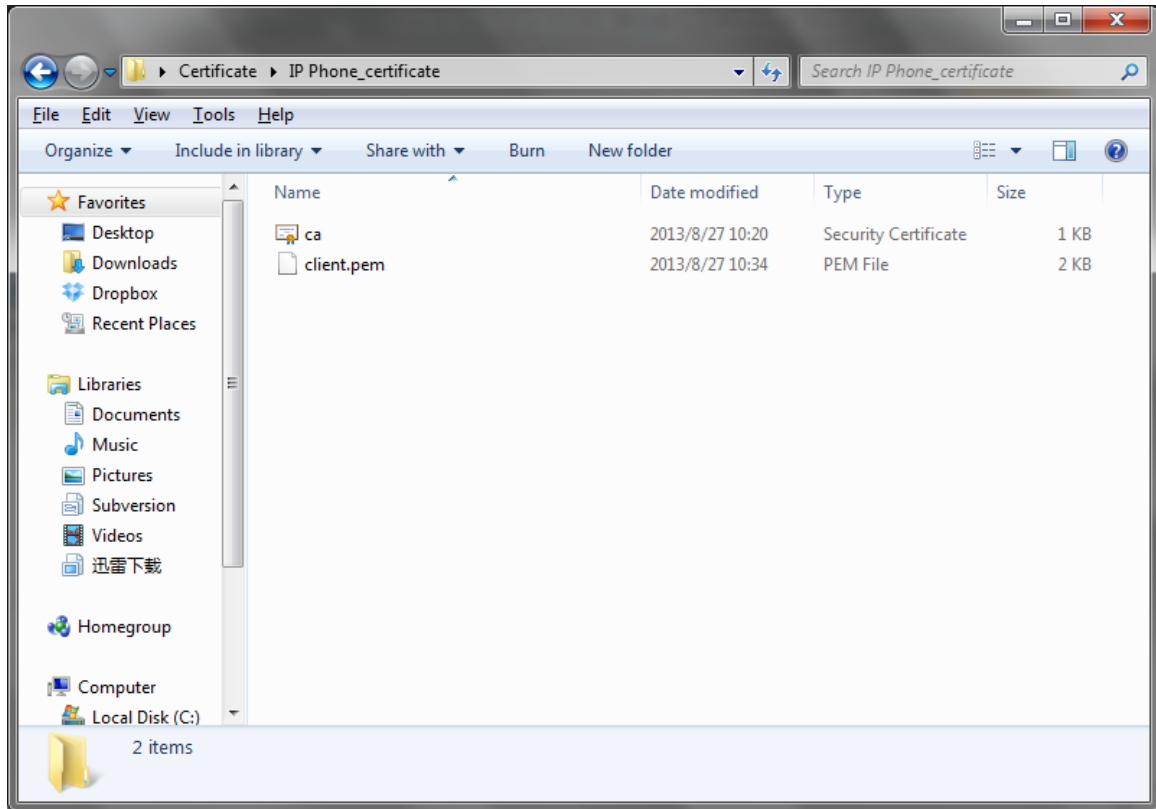


Figure I-19

All the certificates are prepared.

3. Upload certificates

3.1 Upload IP phone's certificates

In this example, IP phone's model is Yealink T28.

Step1. Upload "IP phone's server certificate" (client.pem).

Click "Security→Server Certificates" to upload client.pem

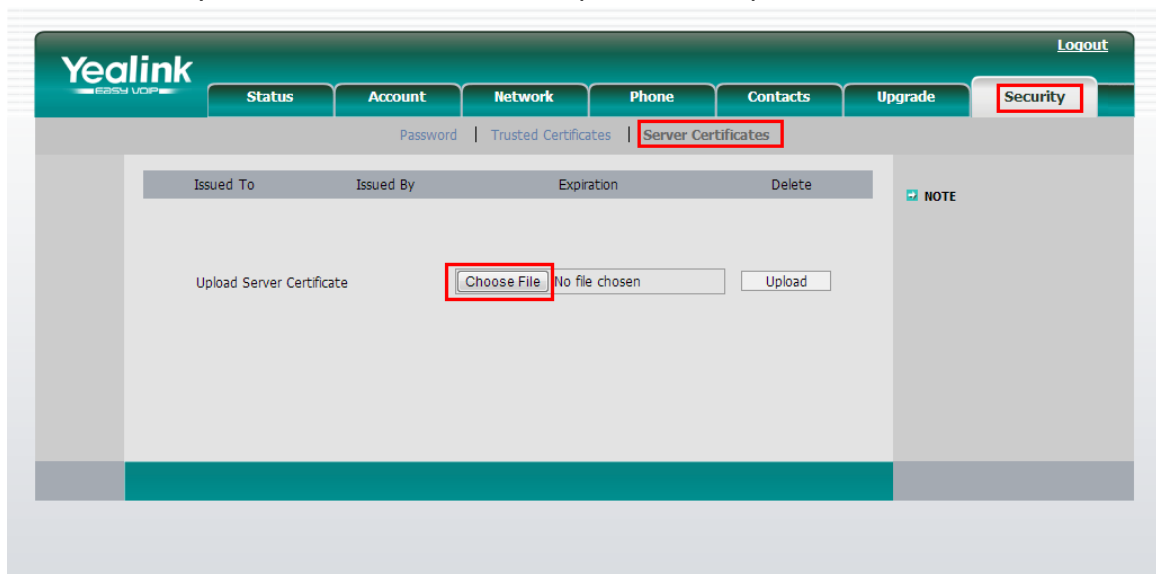


Figure I-20

Click "Choose File" and upload IP phone's server certificate. IP phone will reboot by itself when uploaded successfully to take effect.

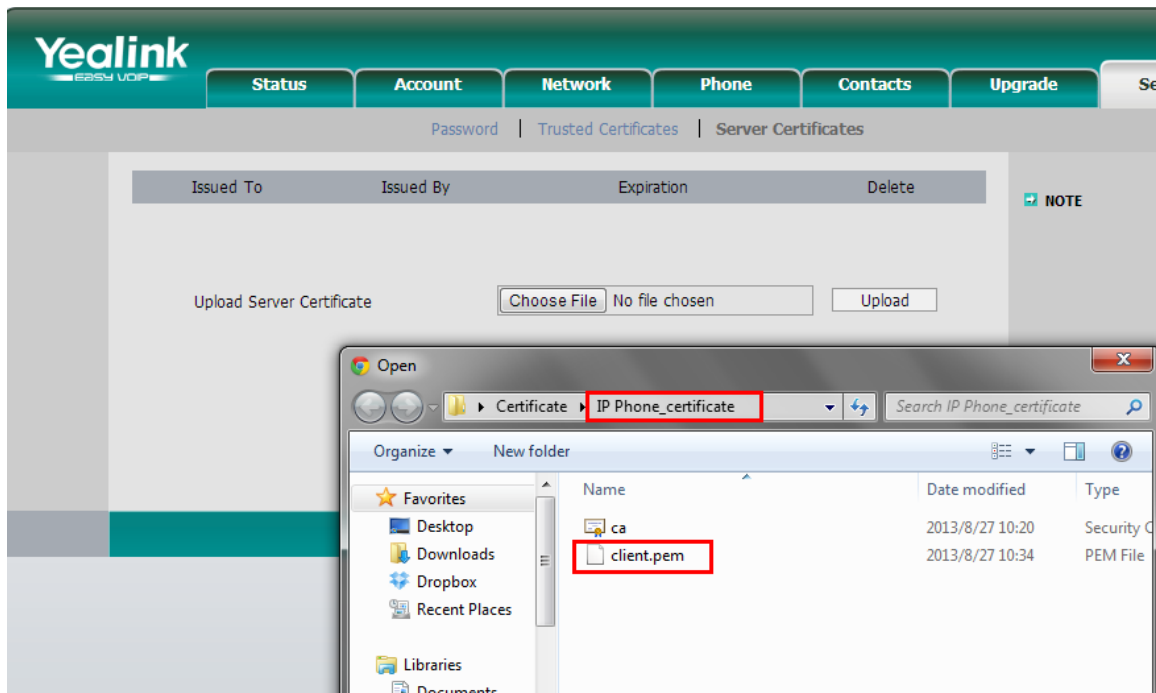


Figure I-21

When IP phone boots up again, we can check the certificate status.

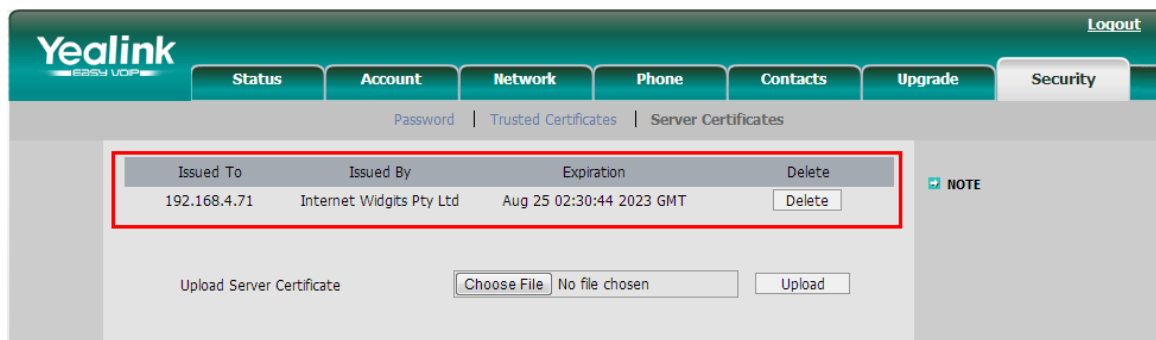


Figure I-22

Step2. Upload the trusted certificate.

The trusted certificate is the ca.crt of MyPBX. It will be sent to MyPBX during the registry process for authorization.

Click "Security→Trusted Certificates", upload MyPBX's ca.crt.

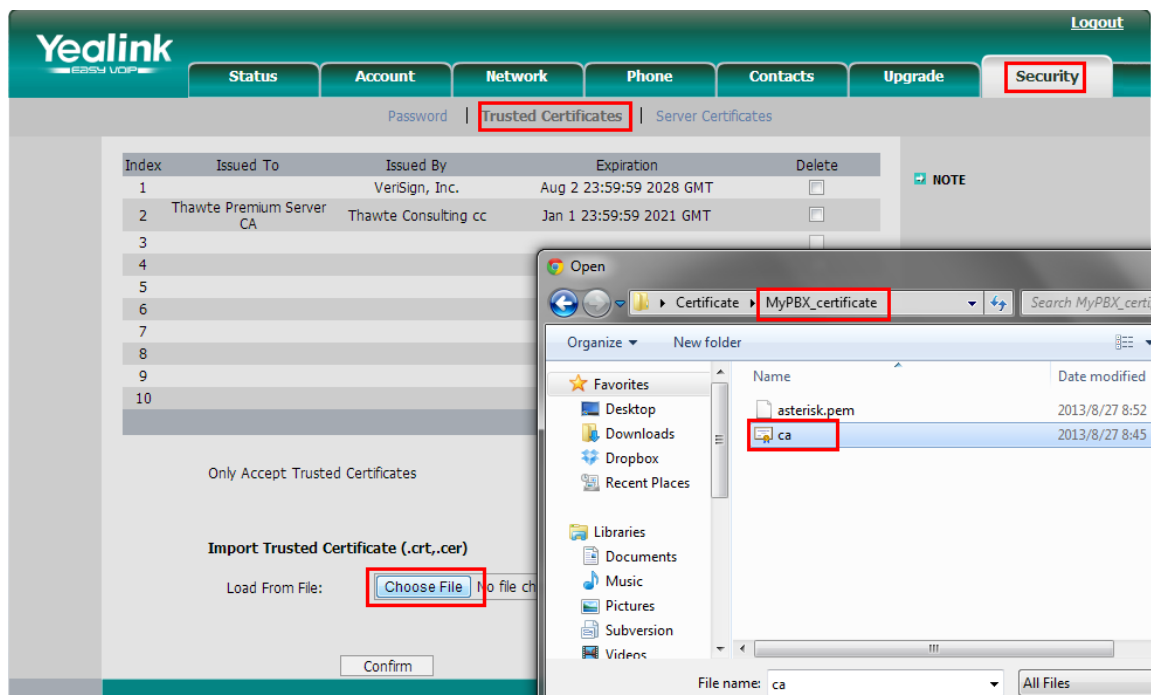


Figure I-23

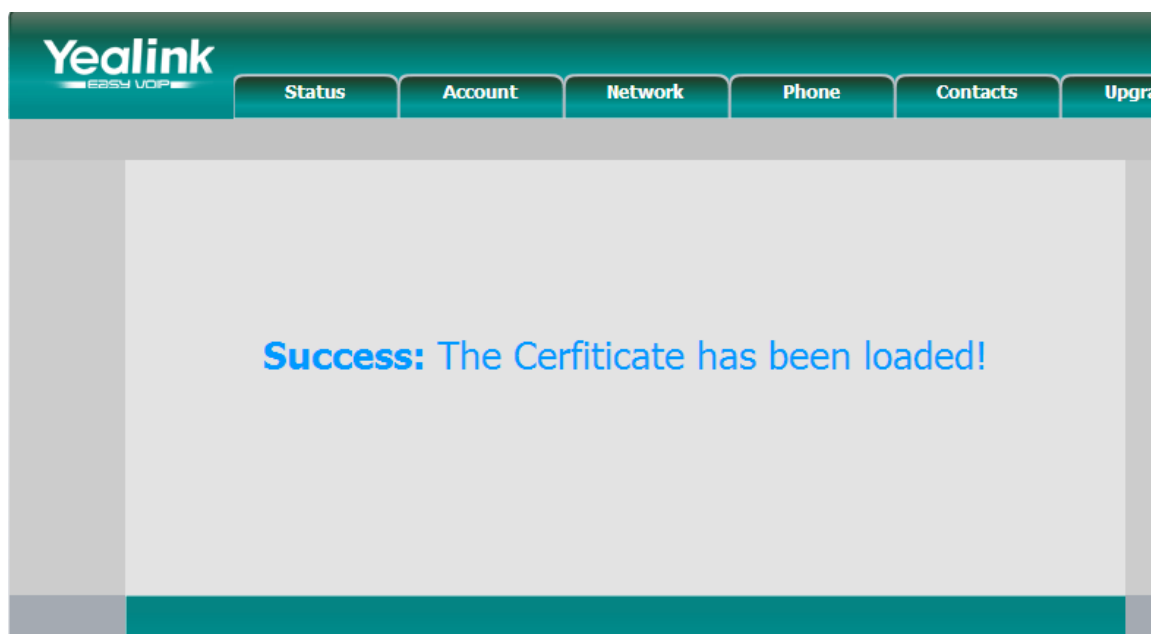


Figure I-24

When done, we can check the content of CA.crt like the picture shown below.

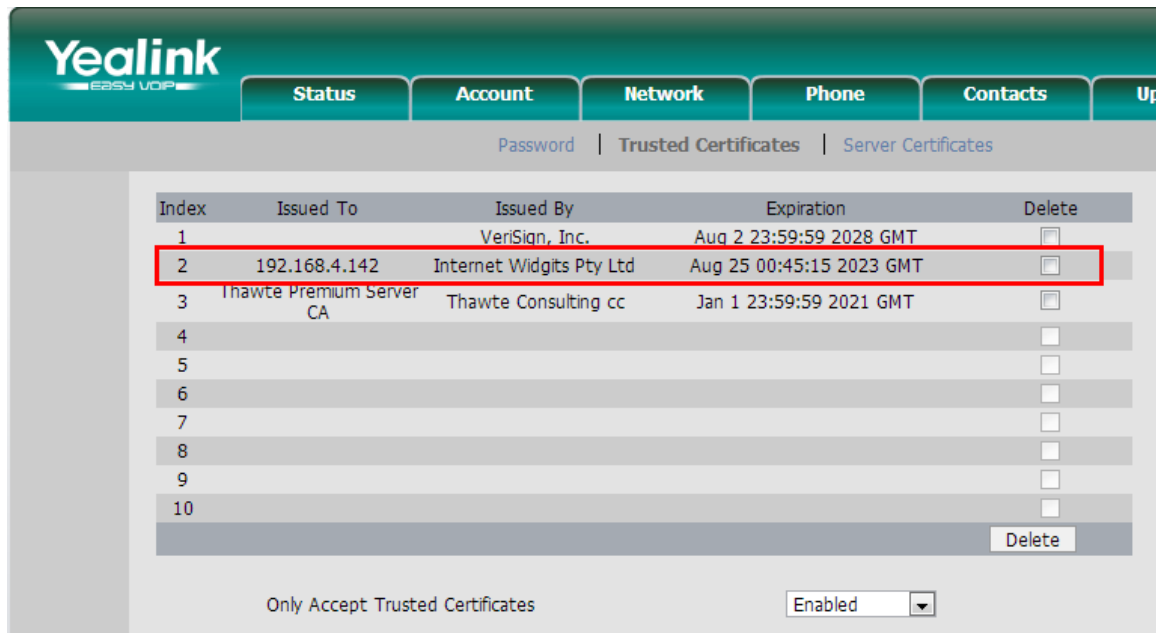


Figure I-25

The certificates in IP phone side are well uploaded.

3.2 Upload MyPBX's certificates

In this example, the model of MyPBX is MyPBX U200 (firmware version: 15.18.0.22)

Step1. Upload MyPBX's server certificate (asterisk.pem)

Click "PBX->Advanced Settings->Certificates", then click "Upload Certificates", choose "PBX Certificates" in Type windows, then upload the asterisk.pem.

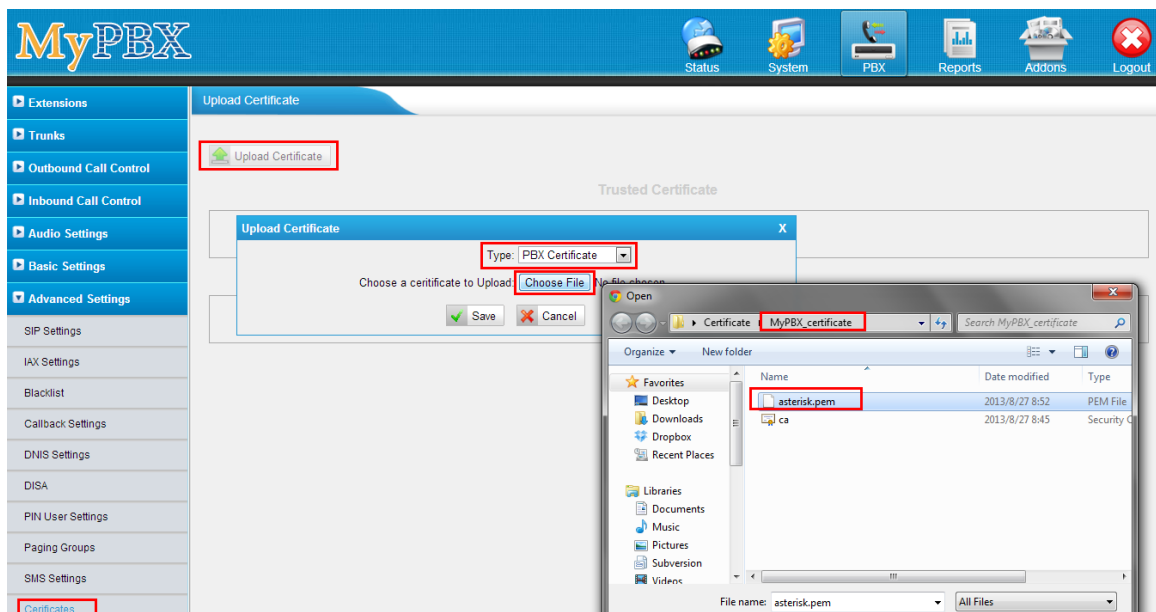


Figure I-26

Click Save to upload, you will need to reboot MyPBX to take effect.

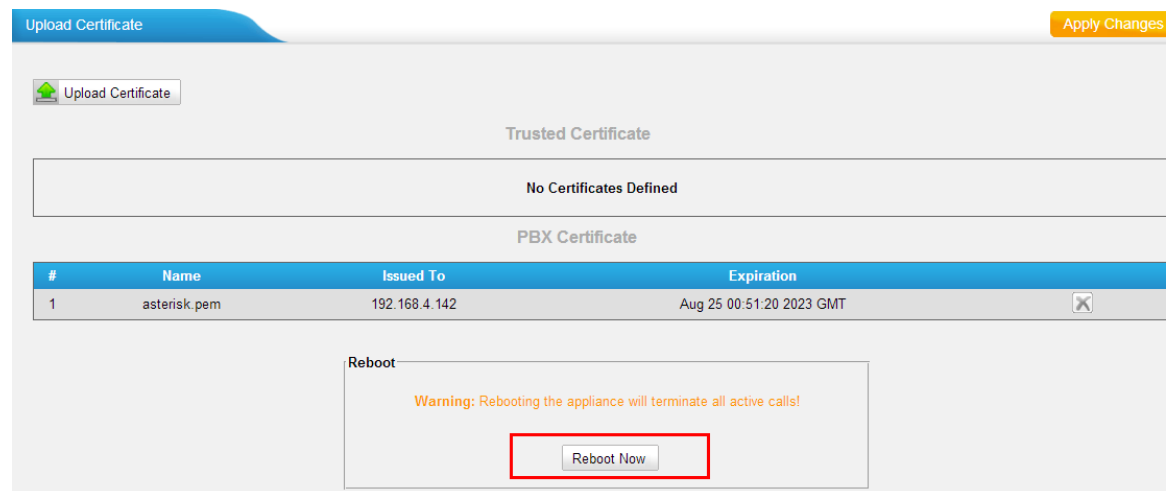


Figure I-27

Click "Reboot Now" to reboot MyPBX. When done, we can move to Step 2.

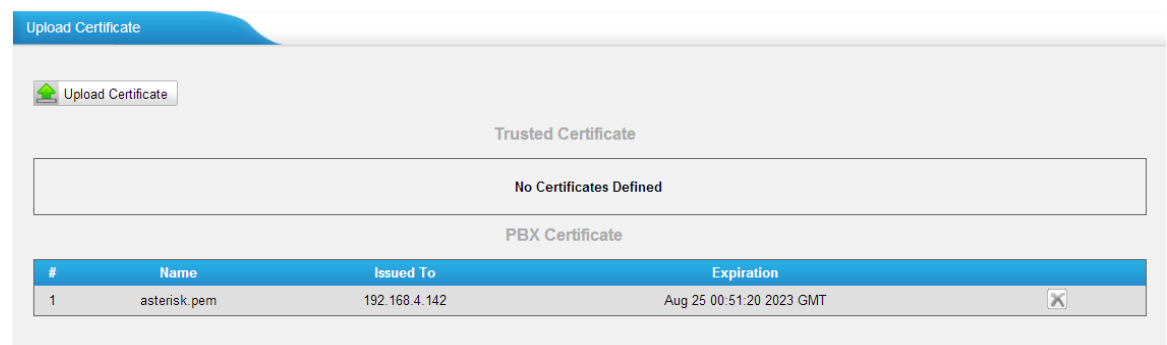


Figure I-28

Step2. Upload the trusted certificate.

The trusted certificate in MyPBX should be the ca.crt of IP phone.
Click "Upload Certificates" and choose "Trusted Certificates" in Type windows, then upload the IP phone's ca.crt.

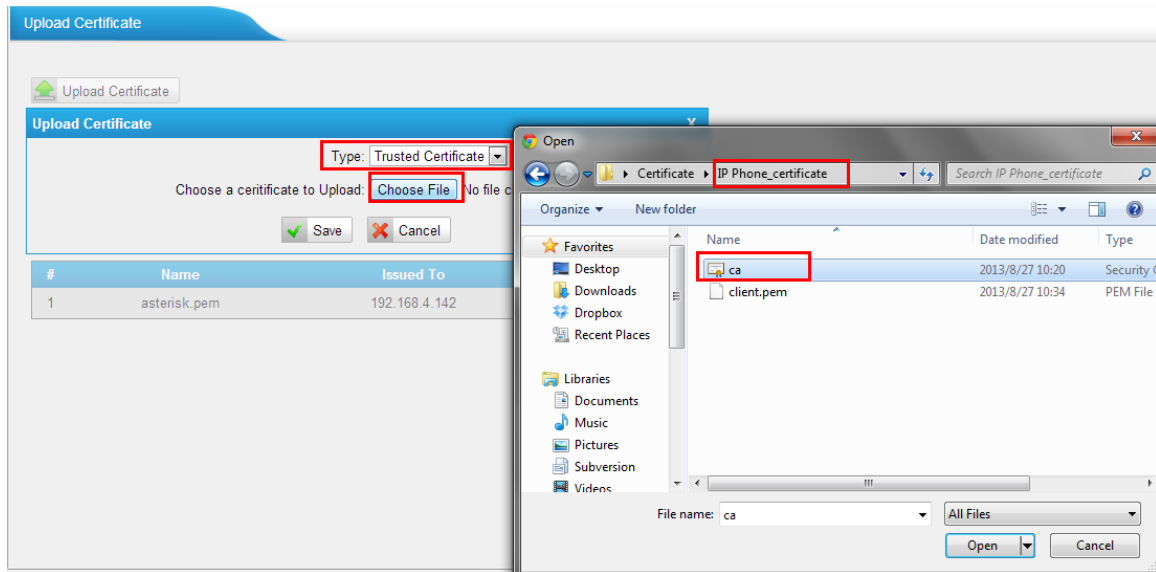


Figure I-29

Click "Save" to upload, then click "Apply Changes".

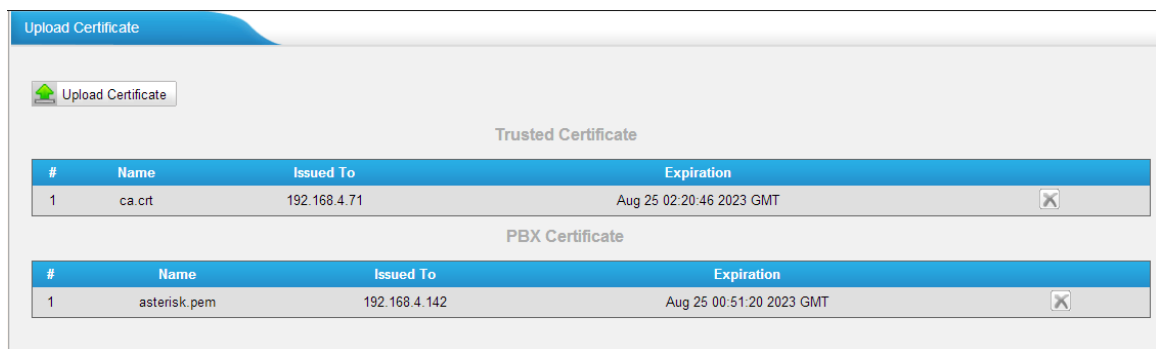


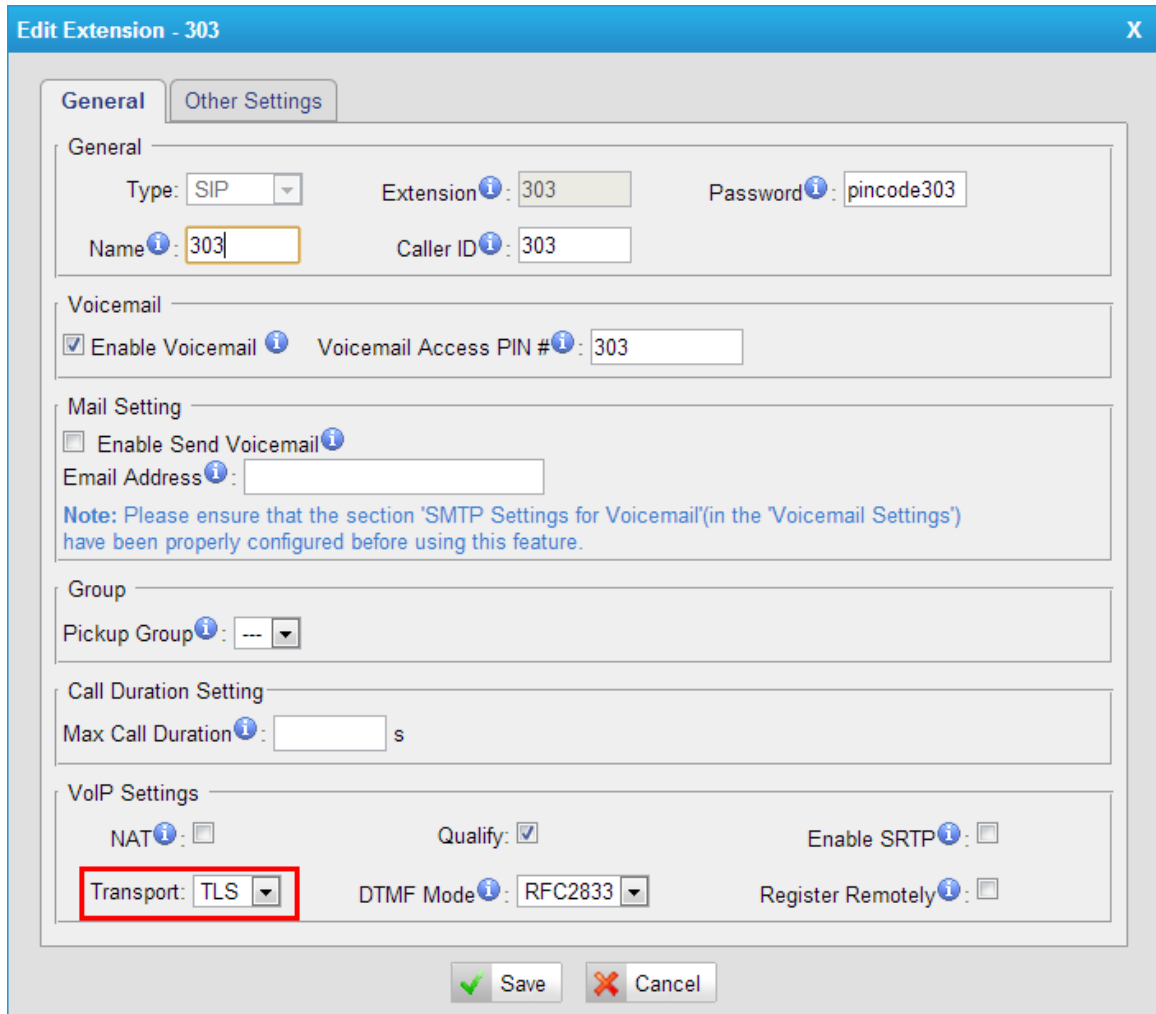
Figure I-30

The certificates in MyPBX side are well uploaded.

4 Register IP phone to MyPBX via TLS

Before registering IP phone to MyPBX, we need to create a SIP extension in MyPBX side in advance, or edit the existing one. In this example, extension number is 303.

We need to set TLS protocol in this page, click save and "Apply Changes" on Web.



Edit Extension - 303

General | Other Settings

General

Type: SIP | Extension: 303 | Password: pincode303

Name: 303 | Caller ID: 303

Voicemail

☒ Enable Voicemail | Voicemail Access PIN #: 303

Mail Setting

☐ Enable Send Voicemail

Email Address:

Note: Please ensure that the section 'SMTP Settings for Voicemail'(in the 'Voicemail Settings') have been properly configured before using this feature.

Group

Pickup Group: ---

Call Duration Setting

Max Call Duration: s

VoIP Settings

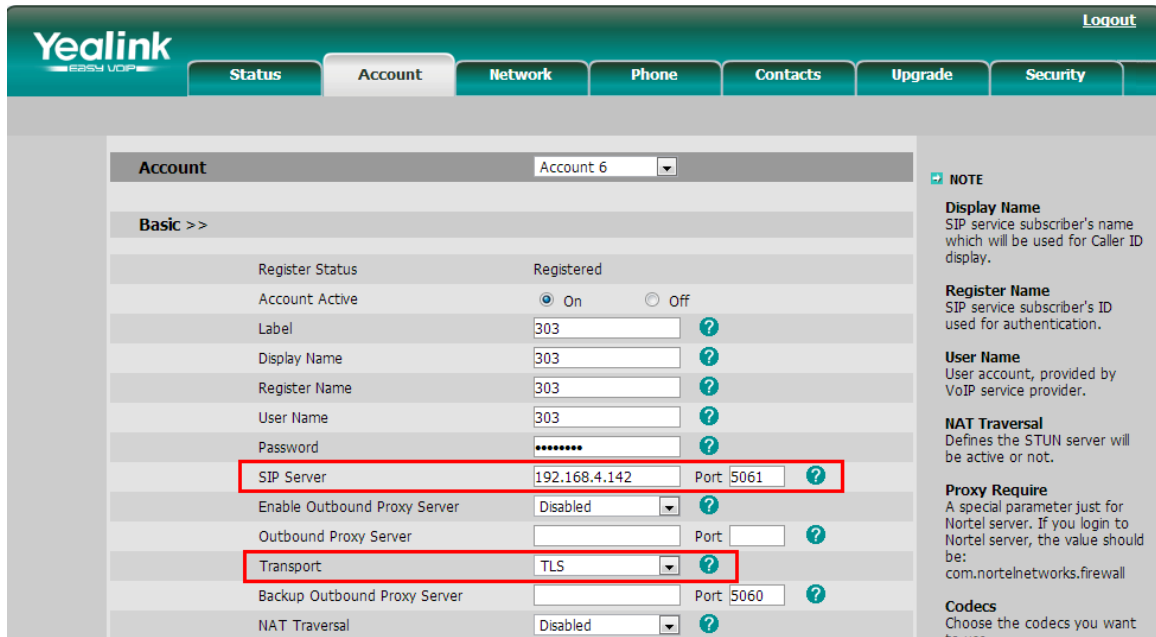
NAT: ☐ | Qualify: ☒ | Enable SRTP: ☐

Transport: TLS | DTMF Mode: RFC2833 | Register Remotely: ☐

Save | Cancel

Figure I-31

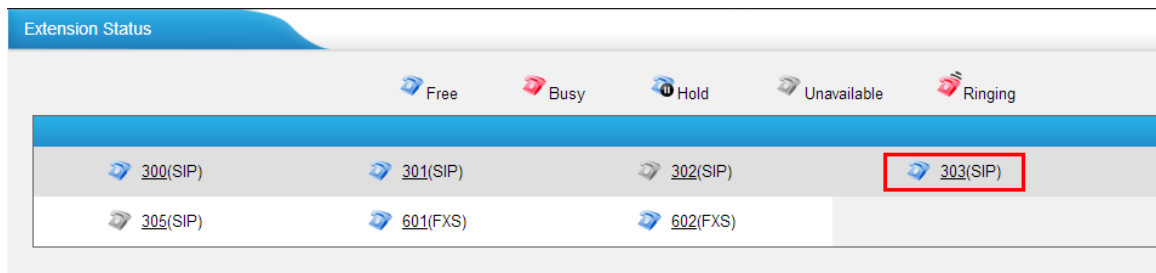
Open IP phone's configuration page, input the registry information of extension 303.



The screenshot shows the 'Account' configuration page in the Yealink MyPBX SOHO V4/V5 Administrator's Guide. The 'Account' dropdown is set to 'Account 6'. The 'Basic >>' section is expanded, showing various configuration fields. The 'SIP Server' field is set to '192.168.4.142' and the 'Port' is '5061'. The 'Transport' field is set to 'TLS'. The 'Outbound Proxy Server' and 'Backup Outbound Proxy Server' fields are empty. The 'NAT Traversal' field is set to 'Disabled'. The 'Register Status' is 'Registered'. The 'Account Active' status is 'On'. The 'Label' is '303'. The 'Display Name' is '303'. The 'Register Name' is '303'. The 'User Name' is '303'. The 'Password' is masked with '*****'. The 'NOTE' section on the right contains information about 'Display Name', 'Register Name', 'User Name', 'NAT Traversal', 'Proxy Require', and 'Codecs'.

Figure I-32

Click "Confirm" to apply the changes, then extension 303 is registered via TLS. We can also check the status in "Extension Status" page of MyPBX.



The screenshot shows the 'Extension Status' page in the Yealink MyPBX SOHO V4/V5 Administrator's Guide. The page displays a grid of extension status icons. The status icons are: Free (blue), Busy (red), Hold (blue), Unavailable (grey), and Ringing (red). The extensions are listed in a grid: 300(SIP), 301(SIP), 302(SIP), 303(SIP), 305(SIP), 601(FXS), and 602(FXS). The 303(SIP) extension is highlighted with a red box, indicating it is registered via TLS.

Figure I-33

If you have any problems about extension's registry, please run a packet trace in "Reports→System Logs→Packet Capture Tool", input IP phone's IP address, choose the eth port, then click "Start". You can register the IP phone again, then click "Stop" and download the package to analyze via Wireshark. You can also send it to us for analyzing.

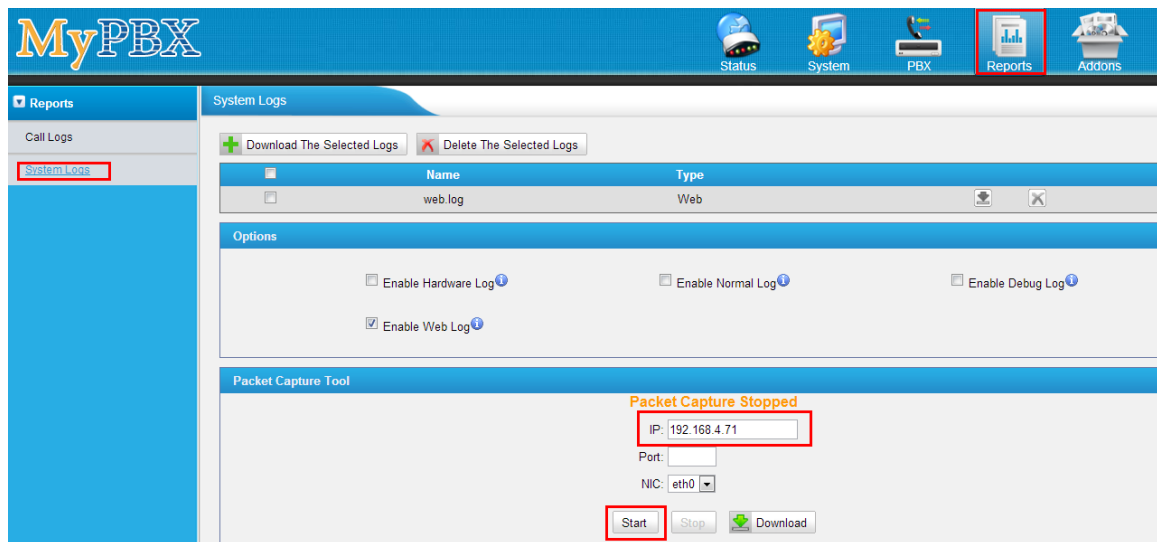
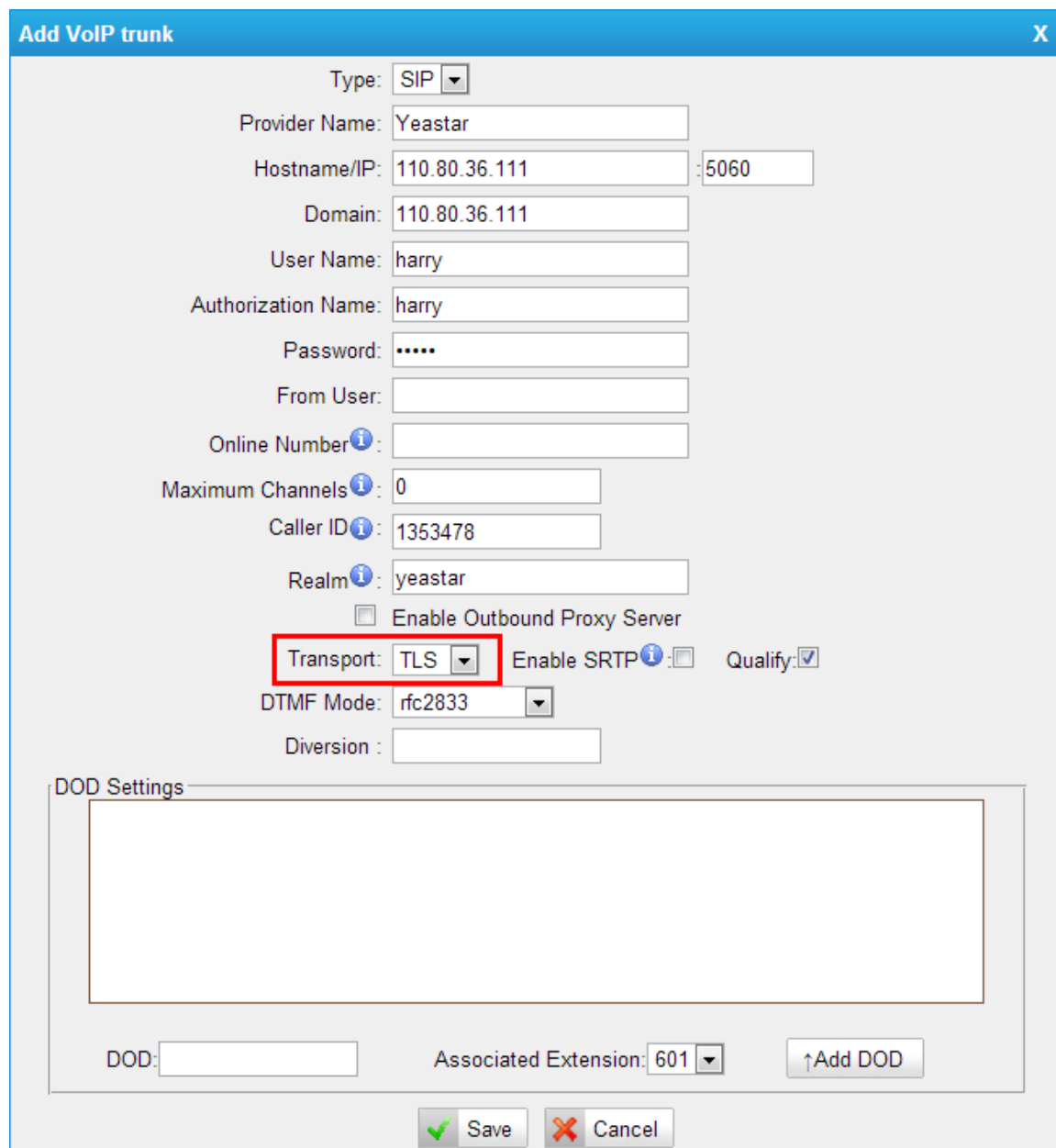


Figure I-34

I.2 How to register SIP trunk to VoIP provider via TLS

If you have got the SIP trunk from provider that is using TLS, we can configure it in MyPBX and choose TLS within the trunk, here are two examples for you.

VoIP trunk:



Add VoIP trunk

Type: SIP

Provider Name: Yeastar

Hostname/IP: 110.80.36.111 : 5060

Domain: 110.80.36.111

User Name: harry

Authorization Name: harry

Password:

From User:

Online Number:

Maximum Channels: 0

Caller ID: 1353478

Realm: yeastar

☐ Enable Outbound Proxy Server

Transport: TLS Enable SRTP: ☐ Qualify: ☒

DTMF Mode: rfc2833

Diversion:

DOD Settings

DOD:

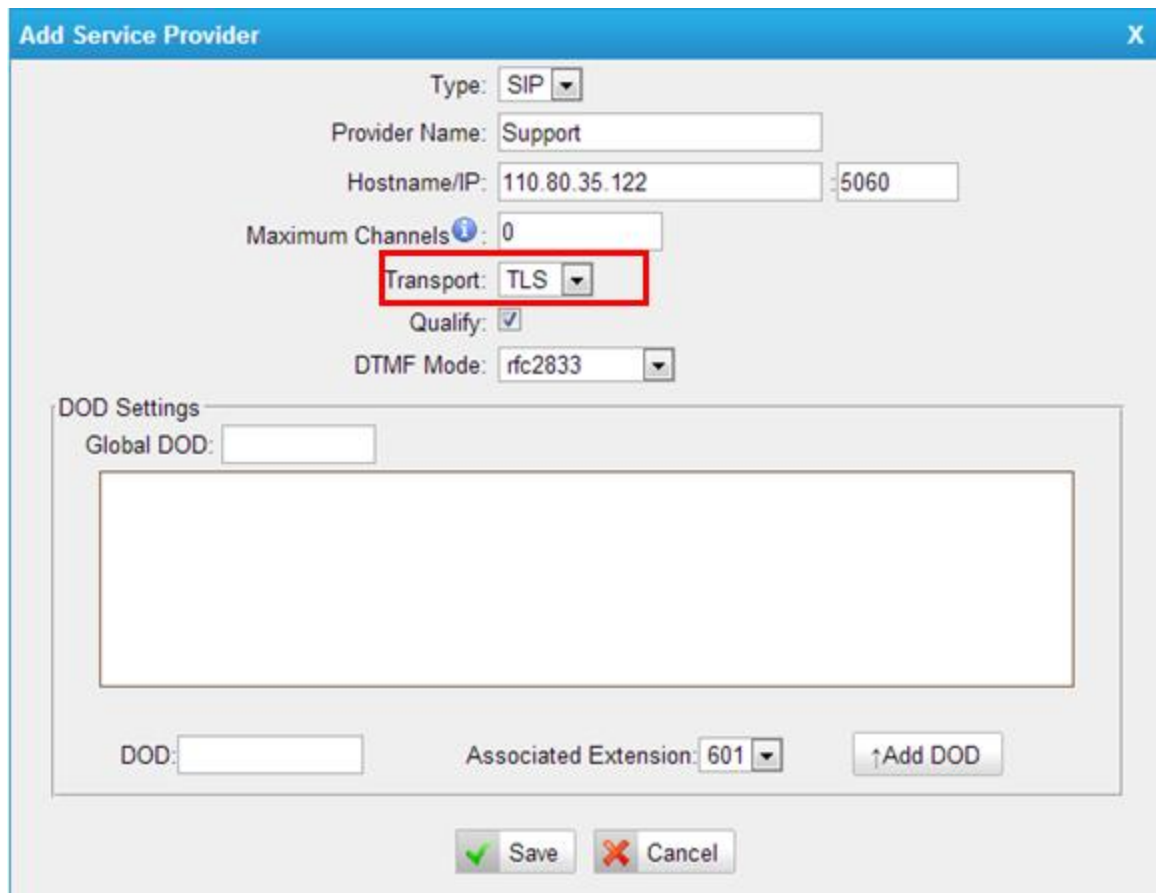
Associated Extension: 601

↑Add DOD

Save Cancel

Figure I-35

Service provider trunk (P-P).



Add Service Provider

Type: SIP

Provider Name: Support

Hostname/IP: 110.80.35.122 Port: 5060

Maximum Channels: 0

Transport: TLS

Qualify: ☒

DTMF Mode: rfc2833

DOD Settings

Global DOD:

DOD: Associated Extension: 601 Add DOD

Save Cancel

Figure I-36

If you have got problem when registering to provider via TLS, you can also run a packet trace in "System Log" page using "Packet Capture Tool", then send it to provider or us to analyze.

APPENDIX J How to use LDAP

LDAP stands for Lightweight Directory Access Protocol, which is a client-server protocol for accessing a directory service. Normally, it is used as a phone book on MyPBX so that you can search a key word from your IP phone. Here we take Yealink T-28 IP phone as an example.

1. Configuration on MyPBX.

Tick the option of "Enable LDAP", and use default configuration in the other fields.

Default configuration as below:

Root Node: dc=pbx,dc=com

PBX Node: ou=pbx,dc=pbx,dc=com

User Name: cn=admin,dc=pbx,dc=com

Password: (fill in as required)

Then you can add contact as required.

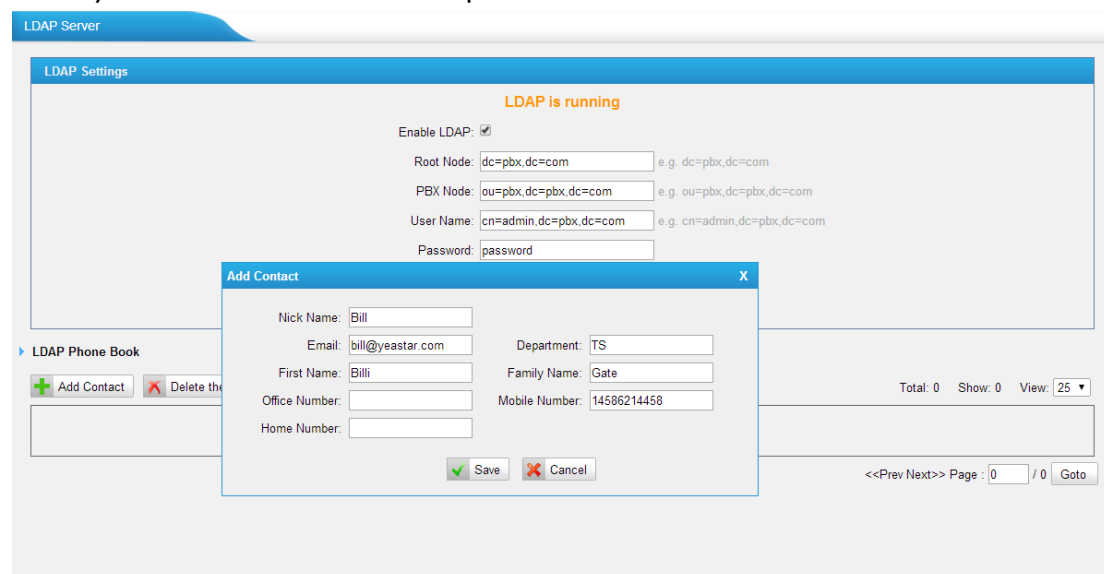
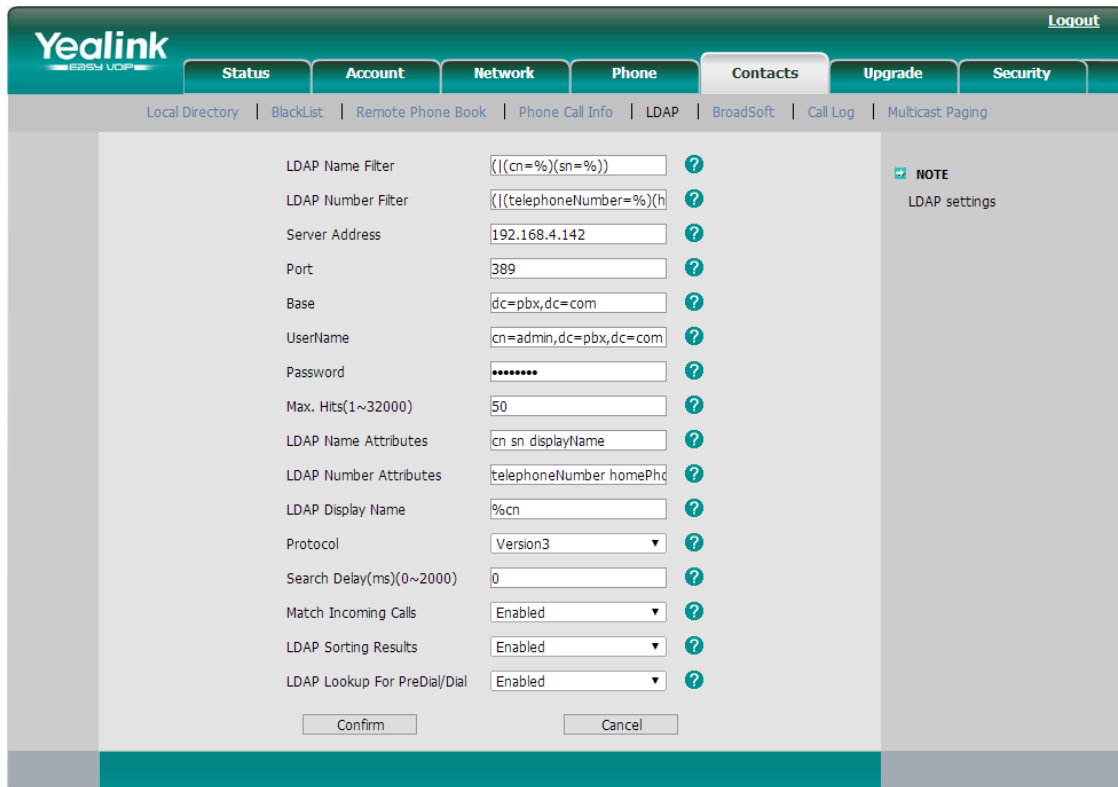


Figure K-1

2. Configuration on Yealink T-28 IP phone



Field	Value	Help
LDAP Name Filter	<code>((cn=%)(sn=%))</code>	?
LDAP Number Filter	<code>((telephoneNumber=%)(homePhone=%)(mobile=%))</code>	?
Server Address	192.168.4.142	?
Port	389	?
Base	dc=pbx,dc=com	?
UserName	cn=admin,dc=pbx,dc=com	?
Password	*****	?
Max. Hits(1~32000)	50	?
LDAP Name Attributes	cn sn displayName	?
LDAP Number Attributes	telephoneNumber homePhone	?
LDAP Display Name	%cn	?
Protocol	Version3	?
Search Delay(ms)(0~2000)	0	?
Match Incoming Calls	Enabled	?
LDAP Sorting Results	Enabled	?
LDAP Lookup For PreDial/Dial	Enabled	?

NOTE: LDAP settings

Buttons: Confirm, Cancel

Figure K-2

First fill the fields as the configuration as below:

LDAP Name Filter: `((cn=%)(sn=%))`
 LDAP Number Filter: `((telephoneNumber=%)(homePhone=%)(mobile=%))`
 Server Address: 192.168.5.142 /the IP of MyPBX/
 Port: 389
 Base: dc= yeastar,dc=cn
 User Name: cn=admin,dc=yeastar,dc=com
 Password: ***** /the password you have set on MyPBX/
 Max.Hits: 50
 LDAP Name Attributes: cn sn displayName
 LDAP Number Attributes: telephoneNumber homePhone mobile mail departmentNumber
 LDAP Display Name: %cn
 Protocol: Version 3
 Search Delay(ms)(0~2000): 0
 LDAP Lookup for Incoming Call: Enabled
 LDAP Sorting Results: Enabled
 LDAP Lookup for PreDial/Dial: Enabled

Click the "confirm" button, and the LDAP will take effect.

Then configure the DSS Key for linking to the LDAP setting.



[Logout](#)

Status

Account

Network

Phone

Contacts

Upgrade

Security

[Preference](#) | [Features](#) | [Softkey Layout](#) | [DSS Keys](#) | [EXT Key](#) | [Action URL](#) | [Voice](#) | [Ring](#) | [Tones](#) | [Dial Plan](#) | [SMS](#)

Memory Keys >> ?

Key	Type	Value	Line	Extension
DSS Key 1	LDAP		Auto	
DSS Key 2	N/A		Auto	
DSS Key 3	N/A		Auto	
DSS Key 4	N/A		Auto	
DSS Key 5	N/A		Auto	
DSS Key 6	N/A		Auto	
DSS Key 7	N/A		Auto	
DSS Key 8	N/A		Auto	
DSS Key 9	N/A		Auto	
DSS Key 10	N/A		Auto	

Line Keys >> ?

Programmable Keys >> ?

Confirm

Cancel

NOTE

Key Type

The free function key 'Types' Speed Dial, BLF, Key Event, Intercom, URL.

BLF

The button can be configured Busy Line Field function with specified account. This feature must be supported by the sip server.

Key Event

Key events are predefined shortcuts to phone and call functions.

Intercom

Enable the 'Intercom' mode and it is useful in an office environment as a quick access to connect to the operator or the secretary.

URL

This key function allows you to send HTTP requests to a web server.

Figure K-3

If you enable the "LDAP Lookup for PreDial/Dial", you can use LDAP feature either in PreDial/Dial page or by pressing DSS Key.

[Finish]