



# Secure your CooVox-V2 IP phone system

Firmware version v2.1.4

## Contents

Introduction.....	1
1 Upgrade your firmware to v2.1.4 .....	2
2 Always use strong passwords.....	2
2.1 Secure Web Admin user password.....	2
2.2 Secure operator user password .....	3
2.3 Secure extension passwords .....	4
2.4 Secure root password.....	5
3 Make sure your ZYCOO IPPBX system is placed behind NAT .....	5
4 Protect outbound calls .....	6
4.1 Implementing Pin Set for outbound dialing rules .....	6
4.2 Use obscure dial patterns.....	7
4.3 Set time conditions for the dialing rules .....	8
4.4 Limit call credits.....	8
5 Permit IP .....	8
6 Allowed Addresses and Fail2Ban.....	9
6.1 Fail2Ban .....	9
6.2 Allowed Addresses .....	10
6 Firewall Settings .....	11
6.1 Drop All.....	11
6.2 Common Rules.....	13
6.3 Auto Defense .....	15
6.4 Rejected IP.....	15
7 Conclusion .....	15

## Introduction

VoIP is not like the public switched telephone network (PSTN) which is circuit switched, it's an application running on the Internet, and therefore inherits the Internet's security issues, so securing VoIP has many challenges.

ZYCOO IP phone system is just like any other computer on your network that is connected to the Internet, can be targeted by malicious users and hackers. We had done our efforts to secure our IP phone system on software aspects. But depending on different deployment scenarios the security risks are not the same. It requires constant attention, and continuous work-in-progress to keep your IP phone system safe.

There are some basic common sense steps that you can perform that will safeguard your system from the most common of attacks. Please take a few minutes to go over this guide and check if your CooVox IPPBX system could be a target of malicious users and hackers, if yes, then please correct the configurations as instructed.

# 1 Upgrade your firmware to v2.1.4

Now we've released new firmware for CooVox-V2 (currently U20V2 and U50 V2) version v2.1.4. This firmware update is very important for you to upgrade your CooVox-V2 IPPBX system to fix some potential security vulnerabilities exist in the previous firmware versions.

If your firmware version is v2.1.4 or higher than v2.1.4 then please skip this chapter and go on with [chapter 2 Always use strong passwords](#).

Please download v2.1.4 firmware from the links below:

CooVox-U20V2: <http://www.zycoo.com/files/upload/CooVox-U20V2-firmware-v2.1.4.zip>

CooVox-U50V2: <http://www.zycoo.com/files/upload/CooVox-U50V2-firmware-v2.1.4.zip>

After downloading you'll get a .zip compressed package, please unzip it with WinRAR and please read the changelogs and notices before upgrading to v2.1.4.

## 2 Always use strong passwords

One of the simplest and yet most effective ways to secure your ZYCOO IPPBX is to ensure the use of strong passwords. Which passwords do I need to secure?

- Web Admin password.
- Operator password
- Extension password.
- SSH root password.

What type of password is strong enough?

ZYCOO defines a strong password as being one with a combination of uppercase letters, lowercase letters, numbers, and special characters such as \$, #, or \* and should be at least 10 characters long.

### 2.1 Secure Web Admin user password

By default, the factory settings for the Web Admin user are username admin and password admin. This allows our customers easier access on first use. However, this combination should NEVER be used on a production CooVox IPPBX. Please change it on web menu *System-> Management* page.

Change Password	
Username:	_____
Password:	_____
New Username: admin	_____
New Password:	_____
Retype New Password:	_____
<input type="button" value="Apply"/>	

First, specify your current username and password and then specify a new password in the “New Password” field and confirm the new password by retyping in “Retype New Password” field.

Finally, click on the “Apply” button to change the Admin user password.

As you can see, there’s a blank field with the label “New Username”, which means you can also change the Admin username (partially) as well. To do this, you need to add some characters following “admin”, for example “adminZol6”, instead of a creating a completely new username. Changing username is optional but does increase security.

After applying your new username/password here, you’ll be redirected to the login page to login with your new credentials.

## 2.2 Secure operator user password

After upgrading your CooVox-V2 IPPBX to firmware version v2.1.4 on the *System->Management* page an option to activate/deactivate Operator user will be added.

Change Password	
<b>Administrator:</b>	
Username:	_____
Password:	_____
New Username: admin	_____
New Password:	_____
Retype New Password:	_____
<input type="button" value="Apply"/>	
<b>Operator:</b>	
Enable:	<input type="checkbox"/>
Username: operator	_____
Password:	_____
<input type="button" value="Apply"/>	

By default it’s been disabled, if you want to activate Operator user a random password will be generate here. You can use this password or you can change it, but please do make the password strong enough.

Operator user password also can be changed on Operator user portal. On the login page please login with username “operator” and the password given on admin web page, then you are able to change the password on *Change Password* page.

● Operator	Management	<div style="border: 1px solid #ccc; padding: 10px;"> <div style="background-color: #e0e0e0; text-align: center; padding: 5px;"><b>Change Password</b></div> <div style="text-align: center; margin-top: 10px;">           Password: _____            New Password: _____            Retype New Password: _____         </div> <div style="text-align: center; margin-top: 10px;"> <input type="button" value="Apply"/> </div> </div>
● Register Status		
● Fax List		
● Record List		
● Call Logs		
● <span style="border: 2px solid red; padding: 2px;">Change Password</span>		

### 2.3 Secure extension passwords

Extension passwords are often targeted by hackers and therefore it is important that you understand how ZYCOO deals with extension passwords.

- By default, the preconfigured extensions of the IPPBX system are set with default randomly generated passwords.
- If you create a single new extension then you still get a random password.
- If you choose bulk-add new extensions, then you have the option to set a unique password or random passwords to all the new extensions.

In all the scenarios, **it's recommended that you use random passwords.**

As we can see from below snapshot:

General			
SIP:	<input checked="" type="checkbox"/>	IAX2:	<input type="checkbox"/>
Name:	<input type="text" value="809"/>	Extension:	<input type="text" value="809"/>
Password:	<input type="text" value="4WIIxNM8T!"/>	Outbound CID:	<input type="text"/>
DialPlan:	<input type="text" value="DialPlan1"/>	Analog Phone:	<input type="text" value="None"/>

The randomly generated password consists of 10 different characters including uppercase letters, lowercase letters, numbers, and special characters. They are strong enough to protect your extensions from hackers and malicious users.

If your existing extensions' passwords are in one of the below conditions please change the passwords immediately, or please delete them and re-generate the extensions with random passwords.

- ☞ Extensions share the same password
- ☞ Passwords contains company name, a person's name or something that makes sense
- ☞ Passwords less than 6 characters
- ☞ Passwords with only letters or digits

Another thing that related to extension password is that after upgrading to firmware version v2.1.4 you should use the extension password instead of voicemail password to login in extension user web portal.

## 2.4 Secure root password

You can login to the Linux console/command prompt of the IPPBX system using the username root and the root password (the last 8 characters of the IPPBX MAC address). Normally you would do this via SSH. However, for security reasons, SSH has been disabled by default.

You can find out SSH service settings on Web menu *Security->Service* page.

Service Settings

**Service Settings**

Enable SSH:  Port:

Remote SSH Administration:

HTTPS Port:

Remote HTTPS Administration:

It is highly recommended that you keep SSH disabled. If you are familiar with Linux command line and wish to use SSH access to manage and debug your IPPBX system, you can enable it here but please ensure that you change the root password immediately.

To change root password please execute the below command:

```
# passwd root
```

```
Enter new UNIX password:
```

```
Retype new UNIX password:
```

```
passwd: password updated successfully
```

### Notice:

Root user has full administration priority to your IPPBX system. Please keep root user credentials absolutely safe. Only activate SSH access when needed, do NOT forget to disable it after SSH session is closed.

## 3 Make sure your ZYCOO IPPBX system is placed behind NAT

Place your IP PBX on a LAN with Network Address Translation (NAT). NAT basically gives your IP PBX a private IP Address and makes it much more difficult to gain access to from the internet.

However, sometimes remote extensions/offices and remote management to the IPPBX system is unavoidable. Remote extensions and remote office require opening SIP port 5060 and RTP ports 10000 to 10500 to the Internet (more details please check the [Remote Extensions and Remote Offices Manual](#)), and remote web management requires web port 9999 to be opened. Doing this will expose your IPPBX system to the Internet and hackers may gain access to the IPPBX system.

If you decided to open ports 5060 and 10000 to 10500 please make sure you have changed all extension passwords and the new extension passwords are strong enough. Please see chapter

### [2.3 Secure extension passwords.](#)

If you are going to open port 9999 please make sure you have changed Admin user password and Operator password. Please see chapter [2.1 Change Admin user password](#) and [2.2 Secure operator user password](#). And we strongly recommend you DO NOT open port 9999 to the Internet, if you have to do this please DO close this port after remote management is done.

## 4 Protect outbound calls

Below are some techniques that can be used to protect outbound calls.

- Implementing Pin Set for the dialing rules
- Use obscure dial patterns
- Set time conditions for the dialing rules
- Limit call credits on your trunks

It is highly recommended using at least one of the above techniques to authorize outbound calls especially calls to the high-cost and international calling destinations.

Obscure dial patterns and PIN codes will only be shared within the company even if the hackers got SIP registration to the IPPBX system they don't know how to place calls out.

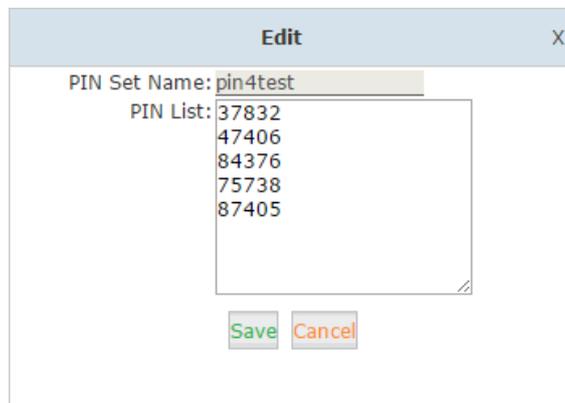
Set time conditions for the dialing rules will only allow outbound calls in certain time period during a day, for example, the time condition will only allow outbound calls in office hours while the office is closed no calls can be made.

Please go on with the detailed instructions below.

### 4.1 Implementing Pin Set for outbound dialing rules

Pin Set is a collection of PIN codes. For example, you can define a PIN Set with 5 PIN codes and give each PIN code to an extension user, if the PIN Set is being used with a dialing rule then only the users with PIN codes that can dial out.

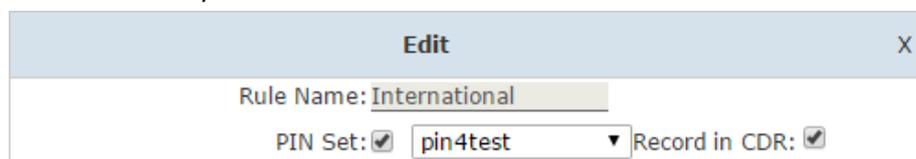
To define a PIN Set please navigate to web menu *Advanced->PIN Sets* page, and click on "New PIN Set" to define a PIN Set.



The image shows a web-based dialog box titled "Edit" with a close button (X) in the top right corner. Inside the dialog, there is a text input field for "PIN Set Name" containing the text "pin4test". Below this is a text area for "PIN List" containing the following PIN codes: 37832, 47406, 84376, 75738, and 87405. At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

Once a PIN Set has been defined you can activate it on the dialing rules. Please navigate to web menu *Basic->Outbound Routes->Dial Rules* page, click on “Edit” button of the dial rule you want to implement PIN Set or create a new dial rule by clicking on “New Dial Rule” button.

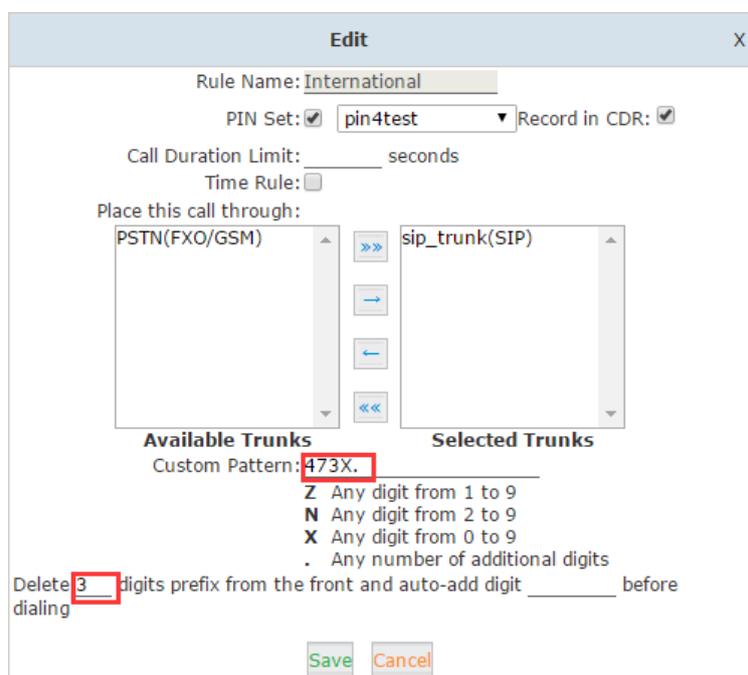
Like the snapshot below enable PIN Set and select the PIN Set in the dropdown list. The “Record in CDR” option is to store the PIN codes to the call logs if they have been used to place an outbound call successfully.



With PIN Set implemented, when an outbound call is in process the caller will be asked to enter a PIN code, if one of the PIN codes from the PIN Set has been entered then this call will go through otherwise it will fail.

## 4.2 Use obscure dial patterns

Obscure dial patterns means using complicated dial prefix to place an outbound call. You have to do it on *Basic->Outbound Routes->Dial Rules* page.



In the above example, a custom dial pattern is given as “473X.” this pattern means you have to dial the number with 473 in front otherwise it will not match this dial rule and no calls can go through the VOIP trunk named “sip\_trunk”.

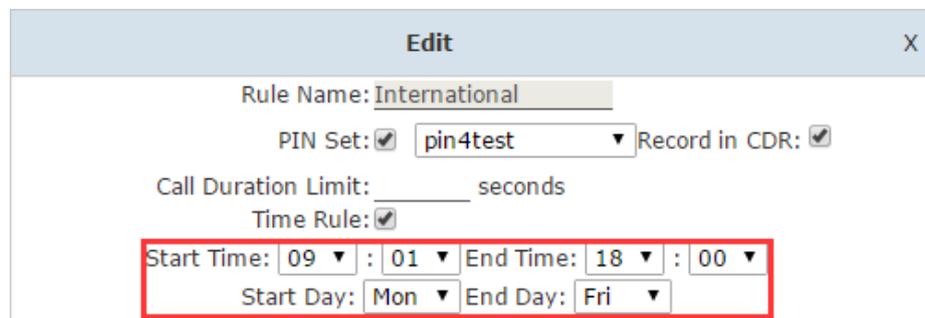
473 is a random combination which doesn’t make any sense to anybody. Please do not use prefix combinations that can be easily figured out.

After this dial rule has been matched the prefix 473 is no longer needed, you have to remove it from real number by specifying “Delete 3 digits prefix...”manipulation mechanism.

### 4.3 Set time conditions for the dialing rules

Set time condition for the dialing rules can limit the time when the dialing rules can be used for outbound phone calls.

See the example below, time rule has been enabled for the “International” dialing rule.



The screenshot shows a dialog box titled "Edit" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Rule Name:
- PIN Set:   Record in CDR:
- Call Duration Limit: \_\_\_\_\_ seconds
- Time Rule:
- Start Time:  :  End Time:  :
- Start Day:  End Day:

The fields for Start Time, End Time, Start Day, and End Day are enclosed in a red rectangular box.

The available calling time durations are the working hours (9 am to 6 pm) out of the 5 workdays. It means when the office is closed the international phone calls are deactivated automatically.

### 4.4 Limit call credits

It's not a bad idea to ask the service provider to limit your call credit on the trunks, especially those trunks which can dial long distance and international call destinations.

If unfortunately your IPPBX system is compromised you will not have to pay tremendously overpriced phone bills.

## 5 Permit IP

Permit IP restricts the IP addresses your extensions can register on to the local subnet or even specific public IP addresses. Coovox IPPBX uses the ACL (permit/deny) mechanism for the extensions to block IP addresses. This can fend off brute force registration attempts.

On the *Basic->Extensions* page click on “Edit” button of an extension. You can specify an IP address or a network address to allow only the specified IP or network to register this extension number.

**Edit** X

---

**General**

SIP:  IAX2:   
Name:  Extension:   
Password:  Outbound CID:   
DialPlan:  Analog Phone:

**Voicemail**

Enable:  Password:   
Delete VMail:  Email(Fax/Voicemail):

**Other Options**

Web Manager:  Agent:  Call Waiting:   
Allow Being Spied:  Pickup Group:   
Mobility Extension:  Mobility Extension Number:

**VoIP Settings**

NAT:  Transport:  SRTP:   
DTMF Mode:  Permit IP:192.168.1.137/255.255.255.255

In the above example, a unique IP 192.168.1.137/255.255.255.255 has been given to user extension 800 as the Permit IP. With this setting, only the SIP endpoint with IP 192.168.1.137 that can register the extension number 800, any other endpoints with different IP cannot register even if all register credentials are correctly specified.

Permit IP also works with public IP addresses, for example 210.16.1.7/255.255.255.255.

If you want to allow a SIP endpoint from a specific network being able to register an extension number you can specify the network address, for example 192.168.1.0/255.255.255.0.

## 6 Allowed Addresses and Fail2Ban

### 6.1 Fail2Ban

There's a security regulation built-in Coovox IPPBX system which will treat all local network IP addresses as trusted IP and public IP addresses as untrusted. Trusted IP will never be blocked by the IPPBX system, untrusted IP will be blocked after certain times of illegal access attempts to the IPPBX system.

The rules are controlled by Fail2Ban on *Security->Allowed Address->Settings* page. Please see snapshot below.

Allowed Address	Settings
<b>SIP</b>	
Max Retry: <u>10</u>	
Find Time: <u>600</u> seconds	
Ban Time: <u>3600</u> seconds	
<b>IAX2</b>	
Max Retry: <u>10</u>	
Find Time: <u>600</u> seconds	
Ban Time: <u>3600</u> seconds	
<b>HTTPS</b>	
Max Retry: <u>5</u>	
Find Time: <u>600</u> seconds	
Ban Time: <u>600</u> seconds	
<b>SSH</b>	
Max Retry: <u>5</u>	
Find Time: <u>600</u> seconds	
Ban Time: <u>600</u> seconds	

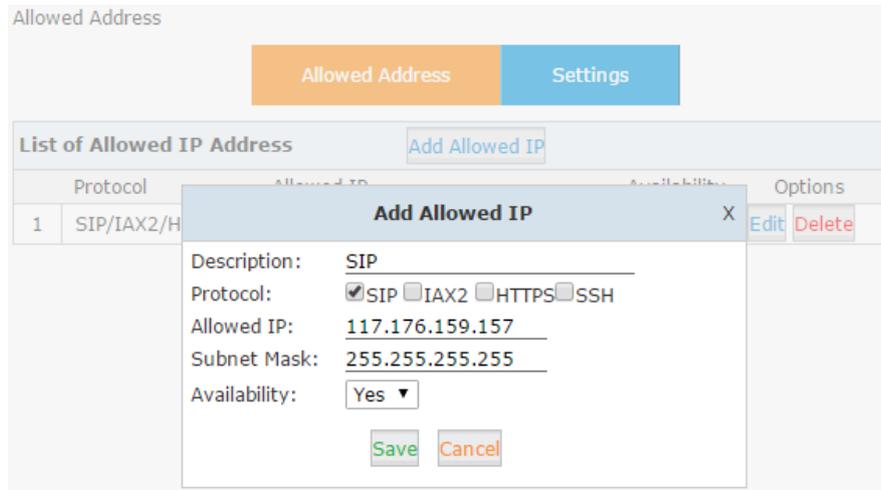
These settings will safeguard SIP register, IAX2 register, HTTPS web access and SSH access. SIP and IAX2 only allow 10 times of illegal register attempts within 10 minutes, if exceeded then the IP addresses of the illegal users will be banned for 3600 seconds (one hour). For HTTPS and SSH only 5 chances within 10 minutes, if failed to enter the correct login credentials the illegal users' IP address will be blocked for 10 minutes.

These rules can be changed according to your wishes.

## 6.2 Allowed Addresses

Allowed address is like a whitelist which allows you to specify public IP addresses to the IPPBX system to bypass the Fail2Ban security rule mentioned above and also bypass the firewall rules which will be introduced in chapter [6 Firewall Settings](#).

To add public IP addresses to allowed address list please go to *Security->Allowed Address* page. Click on "Add Allowed IP" button to specify the IP addresses that you are going to unconditionally allow access to the IPPBX system.



Those public IP addresses added here will never be banned by the IPPBX system if they access the specified service. But access the services not specified will still be regulated by the security rules.

## 6 Firewall Settings

In the firewall section you can manually configure some rules to ban or grant certain IP addresses access to the IPPBX system. Also you can set some rules for the IPPBX to auto defense some brutal attacks.

To configure firewall settings please navigate to Web menu *Security->Firewall* page.

### 6.1 Drop All

In the General section there are options to enable/disable firewall functionalities, enable/disable ping response and enable/disable drop all packets.

Firewall

General		
Enable Firewall: <input checked="" type="checkbox"/>	Disable Ping: <input checked="" type="checkbox"/>	Drop All: <input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Drop all causes the IPPBX system drop all packets sent from others, if you decide to enable drop all, you should know exactly which devices/endpoints are allowed to access the IPPBX system and configure the permit rules in the Common Rules section. After the permit rules have been added then you can enable drop all to block any other communications with the IPPBX system. Below is an example of configuring drop all on the Coovox IPPBX system.

#### Step 1: Enable Web GUI access for specific IP address/addresses

The first priority is adding a rule to allow an IP address or a network to be able to access the Web

GUI. Please click "Add Rule" in the Common Rules section to add a permit rule which allows someone to be able to access the Web GUI.

The screenshot shows a dialog box titled "Add Rule" with a close button (X) in the top right corner. The form contains the following fields and values:

- Name: web
- Description: admin web gui access
- Protocol: TCP
- Port: 9999 - 9999
- IP: 192.168.1.0 /255.255.255.0
- Note: Set a network segment(10.10.10.0/255.255.255.0) or a network address(10.10.10.124/255.255.255.255)
- MAC: (empty)
- Action: ACCEPT
- Buttons: Save, Cancel

### Step 2: Enable SIP signaling

In the Common Rules section click "Add Rule" to enable SIP signaling in the local network.

The screenshot shows a dialog box titled "Add Rule" with a close button (X) in the top right corner. The form contains the following fields and values:

- Name: sip
- Description: local SIP signaling
- Protocol: UDP
- Port: 5060 - 5060
- IP: 192.168.1.0 /255.255.255.0
- Note: Set a network segment(10.10.10.0/255.255.255.0) or a network address(10.10.10.124/255.255.255.255)
- MAC: (empty)
- Action: ACCEPT
- Buttons: Save, Cancel

### Step 3: Enable local RTP transmission

In the Common Rules section click "Add Rule" to enable RTP transmission in the local network.

#### Step 4: Enable “Drop All”

In the General section tick the checkbox of “Drop All” and click “Save”.

Firewall

Drop all should be configured cautiously and please note to ensure the permit rules have been added first from the common rules section before you enable drop all. With drop all enabled, any un-specified IP addresses cannot access any services on the CooVox IPPBX system. So you have to ensure that you fully understand what drop means before you configure and apply drop all.

## 6.2 Common Rules

Common rules are used for customize some specific rules to block/grant some IP addresses to access some specific services of the IPPBX system.

Below is an example of blocking an IP from register SIP extension:

**Add Rule** X

Name:

Description:

Protocol:

Port:  -

IP:  /

Note: Set a network segment(10.10.10.0/255.255.255.0)  
or a network address(10.10.10.124/255.255.255.255)

MAC:

Action:

Below is an example of granting an IP to access the IPPBX system through AMI:

**Add Rule** X

Name:

Description:

Protocol:

Port:  -

IP:  /

Note: Set a network segment(10.10.10.0/255.255.255.0)  
or a network address(10.10.10.124/255.255.255.255)

MAC:

Action:

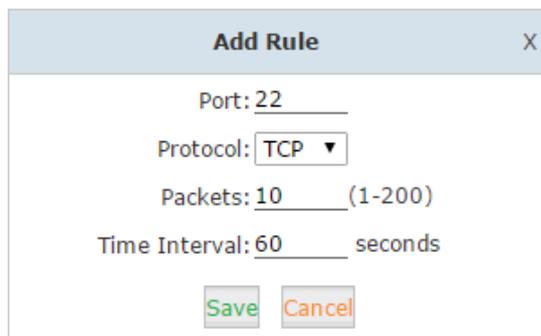
The order of common rules in the list is important. To adjust the order of the rules you can click on the or button to move the rules up or down. For example, you have configured the above rule which allows the IP 192.168.1.2 to access the AMI port 5038, but there's a default rule which denies all access attempts on this port. So you have to move your customized rule above the default rule.

Common Rules <span style="float: right;"><a href="#">Add Rule</a></span>							
	Name	Action	Protocol	Port	IP	MAC	Options
	AMI Grant	ACCEPT	TCP/UDP	5038:5038	192.168.1.2/255.255.255.255	--	<a href="#">Edit</a> <a href="#">Delete</a>
	Refuse AMI	DROP	TCP	5038:5038	--	--	<a href="#">Edit</a> <a href="#">Delete</a>
	block-sip-1	DROP	TCP/UDP	5060:5060	173.249.158.227/255.255.255.255	--	<a href="#">Edit</a> <a href="#">Delete</a>

It's the same principle as configuring drop all, you have to first add the permit rules to the list then enable drop all.

### 6.3 Auto Defense

Define an auto defense rule can prevent a specific service port from brute-force attempts attack.



For example the rule to be added shown in the above snapshot, the IPPBX system will only allow 10 packets to be received in 60 seconds on port 22, further more packets will be discarded. You can add new rules here to limit the packet rate on a specific service port.

### 6.4 Rejected IP

Rejected IP list is the blacklist of your IPPBX system.

Rejected IP		
Type	IP	Options
SSH	220.135.167.211	Delete
VOIP	94.254.225.230	Delete
VOIP	117.176.159.157	Delete
VOIP	94.254.224.206	Delete

As you can see from the above snapshot, the Coovox IPPBX will list the intruders IP addresses here with which kind of service they were trying to access.

If a friendly IP has been blocked you can remove it from the blacklist by click on "Delete".

## 7 Conclusion

To keep your Coovox IPPBX system safe you don't have to do the above all configurations. Just make sure after reading this guide and now you have the knowledge of which parts of configurations is needed to be done on your Coovox IPPBX system, then you do the necessity. Security is not a one-time effort it requires constant attention, and continuous work-in-progress to keep your IP phone system safe. So we recommend that you change passwords of the IPPBX system aperiodically and exam the security related configurations frequently.