



**We Focus · We Deliver**

## **CooVox Series V2 User Manual(Admin)**

## Contents

<b>SAFETY NOTICE .....</b>	<b>5</b>
<b>1 OVERVIEW .....</b>	<b>7</b>
1.1 BRIEF INTRODUCTION OF COOVOX SERIES	7
1.2 MAIN FEATURES	8
1.3 MODULES	10
1.4 MECHANICAL DESIGN	11
1.4.1 <i>CooVox-U20</i> .....	11
1.4.2 <i>CooVox-U50</i> .....	12
1.5 MODEL COMPARISON TABLE	13
1.6 ENVIRONMENTAL REQUIREMENTS	13
1.7 PACKAGE CONTENTS	13
1.8 COMPATIBLE ENDPOINTS	13
<b>2 GETTING STARTED .....</b>	<b>15</b>
2.1 CONNECT COOVOX IPPBX TO YOUR LAN	15
2.1.1 <i>System Login</i> .....	15
2.1.2 <i>Configure Network Profiles</i> .....	17
2.2 USER EXTENSIONS	18
2.2.1 <i>New Extensions</i> .....	18
2.2.2 <i>Other Extension Ranges</i> .....	19
2.3 IP EXTENSION REGISTRATION	19
2.3.1 <i>Desktop IP phones</i> .....	19
2.3.2 <i>Softphone on Windows PC</i> .....	20
2.3.3 <i>Softphone on Android phone, iPhone or iPad</i> .....	21
2.4 PHONE PROVISIONING	22
2.4.1 <i>Phone Provisioning by PnP</i> .....	22
2.4.2 <i>Phone Provisioning by DHCP</i> .....	24
2.5 ANALOG EXTENSIONS	24
2.6 EXTENSION STATUS	24
2.7 ADVANCED EXTENSION CONFIGURATIONS	25
2.7.1 <i>Edit Properties of One Extension</i> .....	25
2.7.2 <i>Search Extension</i> .....	27
2.7.3 <i>Edit Properties of Multiple Extensions</i> .....	27
2.7.4 <i>Upload/Download Extensions</i> .....	29
<b>3 IPPBX BASIC .....</b>	<b>30</b>
3.1 TRUNKS	30
3.1.1 <i>VoIP Trunks</i> .....	30
3.1.2 <i>FXO and GSM Trunks</i> .....	32

3.2	OUTBOUND ROUTES	34
3.2.1	<i>Dial Rules</i> .....	34
3.2.2	<i>Dial Plans</i> .....	36
3.3	INBOUND CONTROL	37
3.3.1	<i>Inbound Destinations</i> .....	37
3.3.2	<i>IVR</i> .....	38
3.3.3	<i>Ring Group</i> .....	40
3.3.4	<i>Call Queue</i> .....	41
3.3.5	<i>Time Based Rules</i> .....	43
3.3.6	<i>Office Closed Timing</i> .....	44
3.3.7	<i>Inbound Routes</i> .....	45
<b>4.</b>	<b>IPPBX ADVANCED</b> .....	<b>47</b>
4.1	GLOBAL IPPBX ADVANCED SETTINGS	47
4.1.1	<i>General</i> .....	47
4.1.2	<i>Global Analog Settings</i> .....	48
4.1.3	<i>Global SIP Settings</i> .....	50
4.1.4	<i>Global IAX Settings</i> .....	52
4.2	VIRTUAL FAX	54
4.2.1	<i>Receive Fax</i> .....	54
4.2.2	<i>Send Fax</i> .....	55
4.3	VOICEMAIL	56
4.3.1	<i>General Voicemail Options</i> .....	56
4.3.2	<i>Playback Voicemail on the phone</i> .....	57
4.3.4	<i>Voicemail to Email</i> .....	57
4.3.5	<i>Playback Voicemail from Web GUI</i> .....	59
4.4	CONFERENCE	60
4.4.1	<i>Static Conference</i> .....	60
4.4.2	<i>Dynamic Conference</i> .....	61
4.5	MUSIC SETTINGS	62
4.6	DISA	63
4.7	FOLLOW ME	64
4.8	CALL FORWARD	65
4.8.1	<i>Configure from the Web</i> .....	65
4.8.2	<i>Configure from the Phone</i> .....	66
4.9	CALL TRANSFER	67
4.10	ONE NUMBER STATIONS	68
4.11	PAGING AND INTERCOM	69
4.12	WEB EXTENSIONS	70
4.13	PIN SETS	71
4.14	CALL RECORDING	72
4.14.1	<i>Record All Calls</i> .....	72
4.14.2	<i>One Touch Recording</i> .....	73
4.15	SMART DID	73
4.16	CALLBACK	75

4.17 PHONE BOOK	76
4.18 LDAP SERVER	77
4.18.1 LDAP Server Settings.....	77
4.18.2 Synchronize Contacts with LDAP Server.....	77
4.18.3 LDAP Client Settings.....	78
4.19 FEATURE CODES	79
<b>5. NETWORK SETTINGS .....</b>	<b>82</b>
5.1 NETWORK BASIC	82
5.1.1 IPv4 Settings .....	82
5.1.2 IPv6 Settings .....	84
5.1.3 VLAN Settings .....	84
5.2 STATIC ROUTING	85
5.3 VPN	86
5.3.1 L2TP VPN.....	86
5.3.2 PPTP VPN.....	88
5.3.3 OpenVPN .....	90
5.3.4 IPSec VPN.....	92
5.3.5 N2N VPN Client.....	95
5.4 DHCP SERVER	95
5.4.1 DHCP Service.....	95
5.4.2 DHCP Client List.....	96
5.4.3 Static Mac.....	96
5.5 DDNS	97
5.6 SNMPV2	98
5.7 TR069	99
5.8 TROUBLESHOOTING	99
5.8.1 Ping.....	99
5.8.2 Traceroute.....	100
<b>6. REPORTS .....</b>	<b>101</b>
6.1 REGISTER STATUS	101
6.1.1 SIP User Status.....	101
6.1.2 IAX2 User Status.....	101
6.1.3 SIP Trunk Status.....	102
6.1.4 IAX2 Trunk Status.....	102
6.2 FAX LIST	103
6.3 RECORD LIST	104
6.3.1 Call Recording.....	104
6.3.2 Conference.....	104
6.3.3 One Touch Recording.....	105
6.3.4 Call Recording Playback.....	105
6.4 CALL LOGS	106
6.5 SYSTEM LOGS	107

<b>7. SECURITY .....</b>	<b>108</b>
7.1 FIREWALL	108
7.2 SERVICE	110
7.3 ALLOWED ADDRESS	111
<b>8.SYSTEM ADVANCED .....</b>	<b>113</b>
8.1 TIME SETTINGS	113
8.1.1 NTP.....	113
8.1.2 Manual Time Set .....	114
8.2 DATA STORAGE	114
8.2.1 USB Data Storage.....	114
8.2.2 FTP Data Storage.....	115
8.3 MANAGEMENT	117
8.3.1 Change Password .....	117
8.3.2 Set System Voice Prompts.....	117
8.4 BACKUP	118
8.4.1 TAKE A BACKUP	118
8.4.2 UPLOAD BACKUP FILE	119
8.5 RESET & REBOOT	119
8.5.1 Reset .....	120
8.5.2 Reboot.....	120
8.6 UPGRADE	121
8.6.1 Web Upgrade .....	121
8.6.2 TFTP Upgrade.....	121
8.7 ADDONS	123
8.7.1 CooBill .....	123
8.7.2 CooCall.....	124

## Safety Notice

Please read the following safety notices before installing or using this IP PBX. They are crucial for safe and reliable operation of the device. Failure to follow the instructions contained in this document may result in damage to your PBX and void the manufacturer's warranty.

1. Please use the external power supply which is included in the package. Other power supplies may cause damage to the device, affect performance or induce noise.
2. Before using the external power supply in the package, please check your building power voltage. Connecting to Inaccurate power voltage may cause fire and damage.
3. Please do not damage the power cord. If the power cord or plug is impaired, do not use it. Connecting a damaged power cord may cause fire or electric shock.
4. Ensure the plug-socket combination is accessible even after the PBX is installed. In order to service the PBX it will need to be disconnected from the power source.
5. Do not drop, knock or shake the device. Rough handling can break internal circuit boards.
6. Do not install the device in places where there is direct sunlight. Also do not place the device on carpets or cushions. Doing so may cause the device to malfunction or cause a fire.
7. Avoid exposing the device to high temperature (above 40°C), low temperature (below -10°C) or high humidity. Doing so could cause damage and will void the manufacturer warranty.
8. Avoid letting the device come in contact with water or any liquid which would damage the device.
9. Do not attempt to open the device. Non-expert handling of the device could cause damage and will immediately void the manufacturer warranty.
10. Consult your authorized dealer for assistance with any issues or questions you may have.
11. Do not use harsh chemicals, cleaning solvents, or strong detergents to clean the device.

12. Wipe the device with a soft cloth that has been slightly dampened in a mild soap and water solution.
13. If you suspect your device has been struck by lightning, do not touch the device, power plug or phone line. Call your authorized dealer for assistance to avoid the possibility of electric shock.
14. Ensure the PBX is installed in a well-ventilated room to avoid overheating and damaging the device.
15. Before you work on any equipment, be aware of any hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents if you are in a situation that could cause bodily injury.

# 1 Overview

## 1.1 Brief Introduction of CooVox Series

CooVox Series IP Phone System is the most innovative solution for VoIP telecommunication in the SMB (Small and Medium-sized Business) market. They provide not only traditional PBX functionality such as automated attendant and voicemail, but also offer many advanced telephony features, including remote extensions, remote office connection, IVR, call recording, call detail records(CDR). All of these can serve to greatly enhance business operations at reduced operational cost.

CooVox Series IP PBXs(V2) is now available in two model variants: U20 and U50.

Each model is introduced below:

CooVox-U20 has 2 analog ports installed onboard by default. The available options are detailed below:

	FXS	FXO	GSM
<b>CooVox-U20</b>	1	1	Optional
	0	2	Optional

CooVox-U50 consists of two main components:

- U50 Main Case
- Modules

There are 2 slots in the system and modules can be utilized as in the following table.

U50 Slot U50 Module	Slot 1	Slot 2
4FXS	✓	✓
4FXO	✓	✓
2FXOS	✓	✓
2GSM	✓	✓
4GSM	✓	✓
2WCDMA	✓	✓
4WCDMA	✓	✓










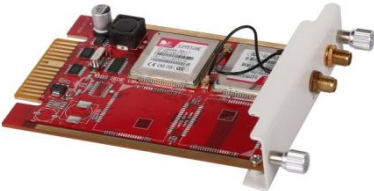



## 1.2 Main Features

1. Black List
2. BLF(Busy Lamp Field)
3. Caller ID
4. Call Detail Records (20000 records)
5. Call Center Queues (20)/ Callback
6. Call Parking/ Call Forward/ Call Transfer/ Call Waiting
7. Call Record /Ring Group Record/ Call Queue Record
8. Conference Bridge (20 Conferences)
9. DISA (Direct Inward System Access) /Paging and Intercom
10. DID/Smart DID/ DOD
11. Dial by Name
12. DHCP Server
13. Do Not Disturb(DND)
14. DDNS(Dyndns.org /No-ip.com /zoneedit.com/ freedns.afraid.org/  
www.oray.com/ 3322.org)
15. Audio Codec: G.722/ G.711-Ulaw/ G.711-Alaw/ G.726/ G.729/ GSM/ SPEEX
16. Video Codec: H.261/ H.263 / H.263+ / H.264
17. Flexible Dial Plan
18. IP Phone Feature Code
19. IPv4 / IPv6
20. One Number Stations
21. Music On Hold
22. Phonebook/LDAP (5000 contacts)
23. Ring Group
24. Speed Dial
25. Skype for SIP
26. SIP/ IAX Extension Registration
27. SNMPv2
28. Static /DHCP /PPPoE Network Access
29. System Backup
30. T.38 Pass-through
31. USB Mobile Hard Disk Record (Scalable)
32. Video Call
33. Voicemail
34. Virtual Fax
35. VPN Server (L2TP / PPTP / OpenVPN/ IPSec, up to 20 connections for VPN clients)
36. VPN Client (L2TP / PPTP / OpenVPN / N2N/ IPSec)

37. Web-based Administration and configuration
38. Extension User Portal
39. Webdial/ WebRTC
40. IP Phone Provisioning (Akuvox/ Cisco/ Escene/ Fanvil/ Grandstream/ Htek/ Yealink IP Phone)

### 1.3 Modules

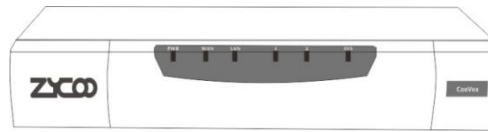
			
2FXS	2FXO	1FXOS	1GSM
			
4FXS Module		4FXO Module	
			
2FXOS Module		2GSM Module	
			
4GSM Module		2WCDMA	
			
4WCDMA			

**Notice:**

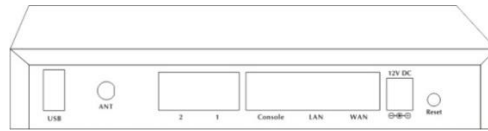
- 1) ZYCOO Module cards will only function in CooVox IP PBX from ZYCOO;
- 2) Module cards for CooVox-U50 are packed separately but contained in the same package as the CooVox system.

## 1.4 Mechanical Design

### 1.4.1 CooVox-U20



CooVox-U20 Front Panel



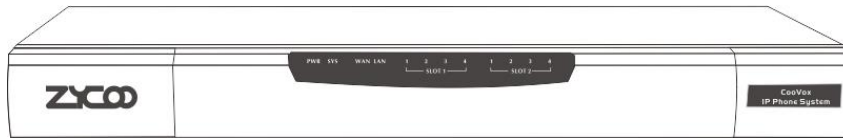
CooVox-U20 Rear Panel

- 1 \* Reset Button
- 1 \* Power Interface (*DC 12V 2A*)
- 2 \* Ethernet Interface (WAN/LAN:10/100Mbps)
- 2 \* Analog Ports(FXO/FXS)
- 1 \* ANT Port (GSM)
- 1 \* USB Interface (for storage)
- 1 \* Console Interface

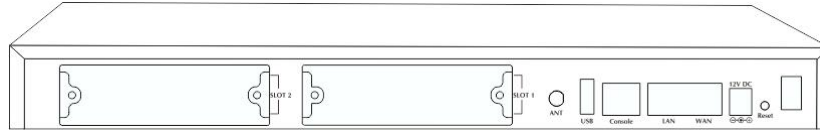
#### U20 LED Indication

LED Label	Function	Status	Indication
PWR	Power Status	On	Power on
		Off	Power off
SYS	System Status	On	System initiating
		Blink	System is functioning
		Off	System failure
WAN	WAN Status	On	Connected but no data transmitting
		Blink	Data transmitting
		Off	Disconnected
LAN	LAN Status	On	Connected but no data transmitting
		Blink	Data transmitting
		Off	Disconnected
1	FXO Status	Red	Channel available
		Blink	Channel ringing
		Off	Channel failure
2	FXS Status	Green	Channel available
		Blink	Channel ringing
		Off	Channel failure

## 1.4.2 CooVox-U50



CooVox-U50 Front Panel



CooVox-U50 Rear Panel

- 1 \* Reset Button
- 1 \* Power Port (DC 12V 2A)
- 2 \* Ethernet Interface (WAN/LAN:10/100Mbps)
- 1 \* USB Interface
- 1 \* Console Interface

Applicable module for slot1 &2: Analog/ GSM/ WCDMA Module Cards

### U50 LED Indications

LED Label	Function	Status	Indication	
PWR	Power Status	On	Power on	
		Off	Power off	
SYS	System Status	On	System initiating	
		Blink	System is functioning	
		Off	System failure	
WAN	WAN Data Status	On	Connected but no data transmitting	
		Blink	Data transmitting	
		Off	Disconnected	
LAN	LAN Data Status	On	Connected but no data transmitting	
		Blink	Data transmitting	
		Off	Disconnected	
1-4 (SLOT1/2)	SLOT 1/2 Status	FXS	Green	Channel available
			Blink	Channel ringing
			Off	Channel failure
		FXO	Red	Channel available
			Blink	Channel ringing
			Off	Channel failure
GSM	Red	Channel available		

			Blink	Channel ringing
			Off	Channel failure
		WCDMA	Red	Channel available
			Blink	Channel ringing
			Off	Channel failure

## 1.5 Model Comparison Table

Items		CooVox-U20	CooVox-U50
System Capacity	Concurrent Calls	15	30
	Extension Users	30	100
	Voicemail and Recording	36,000 mins (.gsm)	36,000 mins (.gsm)
		4000 mins (.wav)	4000 mins (.wav)
	Conference Rooms	20	20
Hardware Capacity	SDRAM	512MB DDR3	1GB DDR3
	Memory (default)	8GB SD card	8GB SD card

## 1.6 Environmental Requirements

Operating Temperature: 0 °C ~40 °C

Storage Temperature: -20 °C ~ 55 °C

Humidity: 5~95% Non-Condensing

## 1.7 Package Contents

<b>CooVox Main Case</b>	1
<b>Power Adaptor</b>	1
<b>Ethernet Cable</b>	1
<b>Quick Installation Guide</b>	1
<b>Warranty Card</b>	1
<b>Rack Mount Ear</b>	2
<b>Screws</b>	10

## 1.8 Compatible Endpoints

- Any SIP compatible IP Phone (Desktop Phones and Soft Phones for Windows, Linux, iOS and also Android platforms). Desktop phone examples include: CooFone Series and ZP Series IP Phones provided by ZYCOO, and also CISCO, Grandstream, Yealink, Polycom, Snom, Akuvox, Escene, Favil, HTEK etc. Soft Phone examples include 3CX,

CooCall, Linphone, X-Lite, Zoiper etc.

- IAX compatible endpoints, for example, CooFoneIP Phones provided by ZYCOO and also Zoiper softphone.
- Analog Phones and Fax Machines
- Web Extensions (WebRTC)

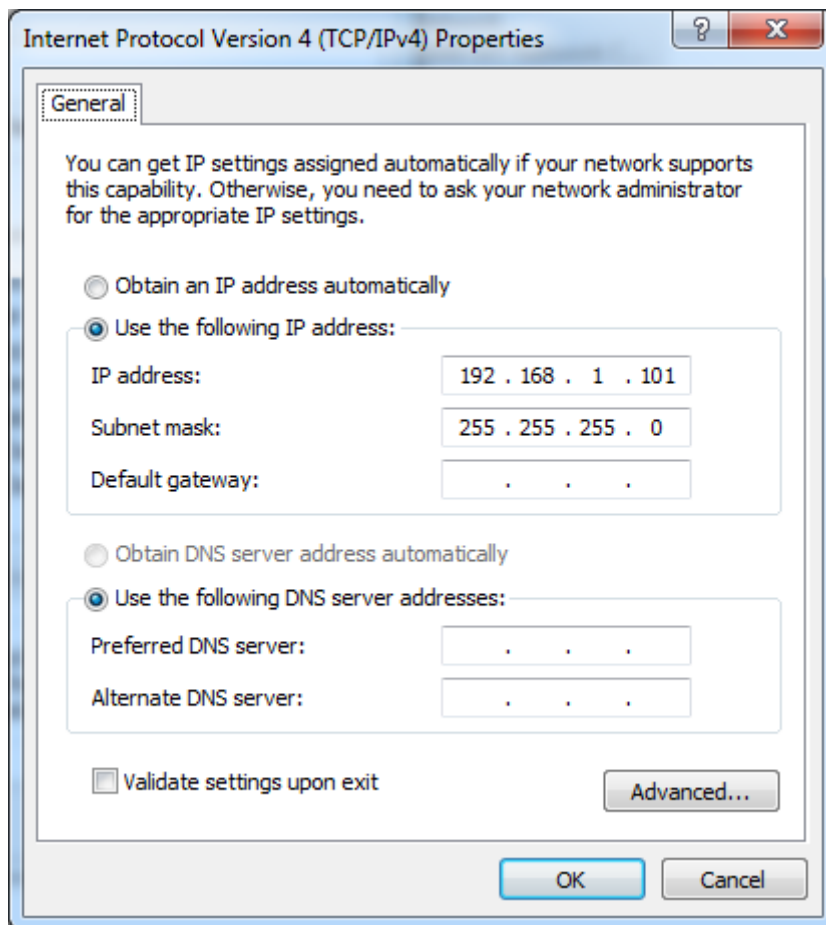
## 2 Getting Started

### 2.1 Connect CooVox IPPBX to your LAN

#### 2.1.1 System Login

CooVox series IPPBXs are preconfigured with a static IP address of 192.168.1.100 on the devices WAN port (192.168.10.100 on LAN port). If your network is configured with a different IP range to the CooVox system default address, then you will need to change the IP address to something more appropriate before connecting to your local LAN.

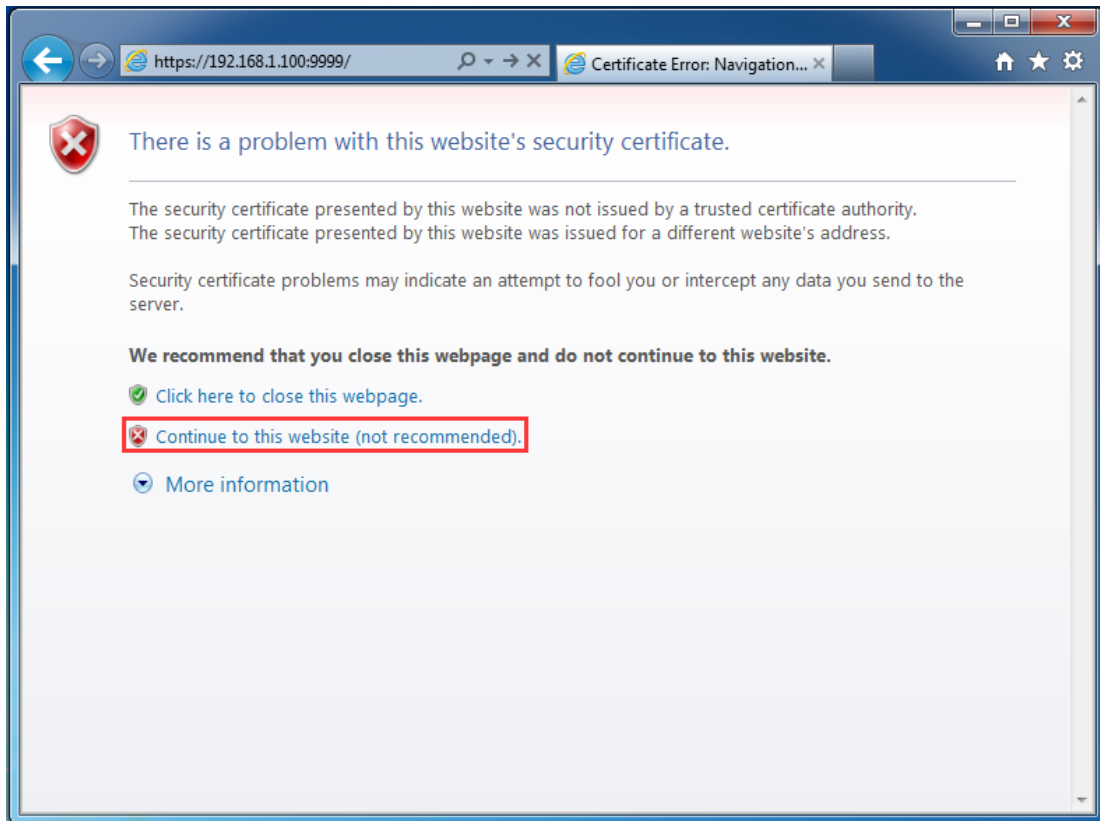
Please connect your PC directly to the WAN interface of the IPPBX and change the network profile of the PC to an IP address of 192.168.1.101 and Subnet mask of 255.255.255.0.



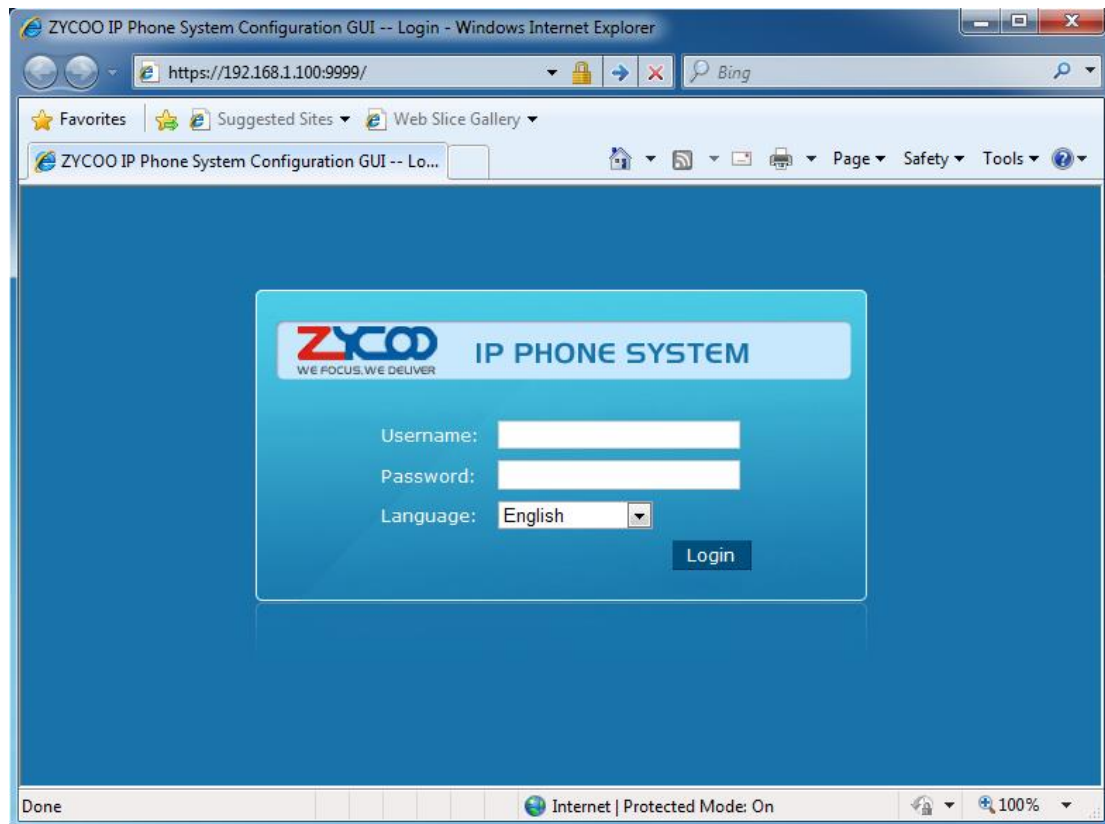
Now you can access the Web interface by inputting <https://192.168.1.100:9999> into your Internet browser address bar and pressing Enter.

You'll now be presented with a Certificate Error notice as below, please click "Continue to this website..." and you will be directed to the login page. Please ensure your IE browser version is at least version 9 or you may not be able to access the web interface.





Login page appears as below:



Type in the default username: admin, and default password: admin to login. After successful login, you will be notified to change the default admin password. Please follow the instructions within the notice to do this. To ensure the device is secure, the admin

password must be complex so please set a strong password that uses a combination of letters, numbers and also special characters.

**Notice:**

1. *CooVox Series IPPBX Web GUI supports the following 11 languages:  
English, Chinese, Arabic, Persian, Portuguese, Italian, French, Spanish, Russian, Turkish and Thai.  
You can select your native language or if this is not available then the most familiar one to login. We are continuously adding more languages to meet the needs of our customers from all around the world.*
2. *Extension number can be used to login to the CooVox IPPBX Web GUI, for more details please check the **CooVox V2 user manual (Ext.User)**.*
3. *Operator user can login to the CooVox IPPBX Web GUI to monitor the system status and check call logs and faxes. Login username is operator and password is password.*

### 2.1.2 Configure Network Profiles

Navigate to Web Menu *Network Settings-->Network->IPv4 Settings*.

CooVox IPPBX WAN interface can be configured to operate in Static, DHCP or PPPoE mode. In the majority of deployment scenario's it is standard practice to configure the unit in Static mode. DHCP and PPPoE will be described later in [chapter 5](#).

To configure your CooVox system in Static mode, you must assign an available static IP address along with corresponding subnet mask, gateway and DNS to the WAN interface of the CooVox IPPBX. For example, you could assign an IP address of 192.168.1.254, Subnet Mask: 255.255.255.0, Gateway: 192.168.1.1, DNS: 8.8.8.8.

Network

IPv4 Settings	IPv6 Settings	VLAN Settings
<b>WAN Port Setup</b>		
IP Assign: <span>Static</span>		
IP Address: <u>192.168.1.254</u>		
Subnet Mask: <u>255.255.255.0</u>		
Gateway: <u>192.168.1.1</u>		
Primary DNS: <u>8.8.8.8</u>		
Alternative DNS: <u>4.4.4.4</u>		
<b>LAN Port Setup</b>		
IP Address: <u>192.168.10.100</u> Subnet Mask: <u>255.255.255.0</u>		
<input type="checkbox"/> IP AddressV1: _____      Subnet MaskV1: _____		
<input type="checkbox"/> IP AddressV2: _____      Subnet MaskV2: _____		
<span>Save</span> <span>Cancel</span>		

After modifications are complete, please click the "Save" button to save the configuration. You will now be presented with a dialog box asking you to reboot the system to make the changes effective. Please reboot the system and once complete you can connect the IPPBX to your local LAN switch.

## 2.2 User extensions

Navigate to web menu *Basic->Extensions*.

This page lists all user extensions on CooVox V2 system. Here you can add/bulk add, delete/bulk delete user extensions and also edit/bulk edit the user extension properties. By default, 10 extension numbers within the range of 800 to 809 have been created for you to use.

Extensions

Extensions
Upload/Download Extensions

Extension:  Search Show All

New User
Batch Add
Edit Selected
Delete Selected

**Extensions**

<input type="checkbox"/>	Name	Extension	Port	Protocol	DialPlan	Outbound CID	Options
<input type="checkbox"/>	1 800	800	--	SIP	DialPlan1		<a href="#">Edit</a>
<input type="checkbox"/>	2 801	801	--	SIP	DialPlan1		<a href="#">Edit</a>
<input type="checkbox"/>	3 802	802	--	SIP	DialPlan1		<a href="#">Edit</a>
<input type="checkbox"/>	4 803	803	--	SIP	DialPlan1		<a href="#">Edit</a>
<input type="checkbox"/>	5 804	804	--	SIP	DialPlan1		<a href="#">Edit</a>
<input type="checkbox"/>	6 805	805	--	SIP	DialPlan1		<a href="#">Edit</a>
<input type="checkbox"/>	7 806	806	--	SIP	DialPlan1		<a href="#">Edit</a>
<input type="checkbox"/>	8 807	807	--	SIP	DialPlan1		<a href="#">Edit</a>
<input type="checkbox"/>	9 808	808	--	SIP	DialPlan1		<a href="#">Edit</a>
<input type="checkbox"/>	10 809	809	--	SIP	DialPlan1		<a href="#">Edit</a>

### 2.2.1 New Extensions

You can add further extensions one by one by clicking the “New User” button or bulk add extensions by clicking “Batch Add” button and completing the popup shown below.

**Batch Add** X

Extension Start:  Extension End:

DialPlan:  Password:(Random )

Save
Cancel

- **Extension Start/Extension End:** These two fields define the new extension range to be generated.
- **DialPlan:** Select a dial plan for the new extensions.
- **Password:** A secure random password consisting of numbers, letters and special characters is the recommended choice and can be selected by selecting the “Random” checkbox. Alternatively, you can specify the same password for all new extensions. If you choose this option then please ensure a secure password is set.

## 2.2.2 Other Extension Ranges

We have limited the user extension number range in the CooVox IPPBX to be between 800 and 899. If you require more extensions or you want extensions in other number ranges then you need to change the extension range before you can add new extensions.

Please navigate to web menu *Advanced->Options->General*.

In the "Extension Preferences" section you can change the user extension range.

Extension Preferences	
User Extensions	<u>400</u> to <u>499</u>
Conference Extensions	<u>900</u> to <u>909</u>
IVR Extensions	<u>610</u> to <u>629</u>
Queue Extensions	<u>630</u> to <u>639</u>
Ring Group Extensions	<u>640</u> to <u>659</u>
Paging Group Extensions	<u>660</u> to <u>679</u>
Web Extensions	<u>680</u> to <u>699</u>

In the above example, the user extension range has been changed to be between 400 to 499. If you now go back to the extension page you'll be able to add new extensions within this range.

## 2.3 IP Extension Registration

### 2.3.1 Desktop IP phones

The following example details how to register a Zycoo CooFone IP phone on your CooVox IPPBX system.

#### Step 1:

Press the softkey "Status" beneath the phone screen, here you can see the IP Address of the IP phone.

#### Step 2:

Open the IP phone web interface by entering the phone IP address into the web browser address bar.

#### Step 3:

Default login credentials are username admin and password admin.

#### Step 4:

After successful login, navigate to the phone web menu VOIP->SIP, and register an extension number as below example.

SIP Line		SIP 1	
<b>Basic Settings &gt;&gt;</b>			
Status	Registered	Domain Realm	
Server Address	192.168.1.254	Proxy Server Address	
Server Port	5060	Proxy Server Port	
Authentication User	402	Proxy User	
Authentication Password	*****	Proxy Password	
SIP User	402	Backup Proxy Server Address	
Display Name	John Doe	Backup Proxy Server Port	5060
Enable Registration	<input checked="" type="checkbox"/>	Server Name	

- **Server Address:** IP address of the CooVox IPPBX.
- **Server Port:** SIP service port number, by default this is 5060 and does not require changing.
- **Authentication User:** User extension number from the CooVox IPPBX user extension page.
- **Authentication Password:** The password of the extension.
- **SIP User:** The same as Authentication user.
- **Display Name:** Name of the extension user.
- **Enable Registration:** Only when enabled here will the phone register to CooVox IPPBX as an extension.

### 2.3.2 Softphone on Windows PC

Softphones including 3CX, Bria, Zoiper and many other softphone APPs all work well with CooVox V2 IPPBX. Below is an example of registering Zoiper to CooVox IPPBX system as an extension from your Windows PC.

#### Step 1:

Download Zoiper from <http://www.zoiper.com/>.

#### Step 2:


Install and run Zoiper on your Windows device.

#### Step 3:

Click menu "Settings" and select "Create a new account" and select "SIP" protocol and click Next.

#### Step 4:

Complete the register credentials as in the example below:



Account wizard

Credentials

user / user@host 402

Password ●●●●●●●●

Domain / Outbound proxy 192.168.1.254

← BACK NEXT →

**Step 5:**

Click Next to complete the registration process.

### 2.3.3 Softphone on Android phone, iPhone or iPad


The majority of softphones detailed previously in this section have mobile editions for both Android and iOS platforms. You can download these apps and install them from your mobile phone APP Store.

Below is an example of how to register Zoiper softphone to Coovox IPPBX as an extension from your iPhone:

**Step 1:**

Run Zoiper on your iPhone and tap  menu.

**Step 2:**

Tap  Accounts menu.


**Step 3:**

Tap  to create a new account.

**Step 4:**

You will be asked "Do you already have an account(username and password)?" tap "Yes" and then tap "Manual configuration" to continue.

**Step 5:**

Tap  SIP account to configure the account as in the below example:

### Step 6:

After entering the register credentials, tap "Register" to register to CooVox IPPBX system as an extension.

## 2.4 Phone Provisioning

If you plan to deploy a large number of IP phones, phone provisioning is a useful feature as it can reduce the time and effort required to deploy phone extensions. There are 2 methods to auto provision your IP phones, DHCP and PnP.

### 2.4.1 Phone Provisioning by PnP

Navigate to web menu *Advanced->Phone Provisioning*.

Here on this page you can see the term "PnP", which refers to Plug and Play. By using this technique you don't have to undertake any configurations directly on the IP phones, but instead only some minimized configurations on the IPPBX system. After this configuration is complete you can plug the phones to your LAN and once they start up, they are ready for phone calls through the IPPBX system.

Click on "PnP Settings" tab.

Plug and Play(PnP) Settings

On this page, tick "Enable" to enable PnP feature.

- **Interface:** Select WAN or LAN depending on which interface you have connected the IPPBX to your local LAN.

- **Custom URL:** Custom URL tells the IP phones where to obtain the configuration files for auto provisioning. You should read your IP phone user manual to determine which kind of files it requires for auto provisioning. Then you create/upload these files to a FTP/TFTP/HTTP server for the phones to download. The URL can be IP address or domain name with subdirectory.

For example: [http://192.168.1.2/phones/\\${MAC}.conf](http://192.168.1.2/phones/${MAC}.conf). With "Custom URL" configured, you don't have to add phones from the "Phone Settings" tab.

- **Multicasting Address:** IP phones which support PnP can use multicast discovery of SIP Registrar. Multicast registrations are addressed to the well-known "all SIP servers" multicast address "sip.mcast.net" (224.0.1.75 for IPv4).
- **Port:** SIP signaling port, default is 5060.

**Notice:**

*Phone provisioning only works for IP phones that are in the same LAN where the CooVox IPPBX is deployed.*

After enabling PnP feature, click on "Phone Settings" tab and click "New Phones" to generate the configuration files for the phones to be added to the IPPBX system.

The screenshot shows a 'New Phone' configuration dialog box. It has a title bar with 'New Phone' and a close button 'X'. The dialog is split into two sections: 'General' and 'Advanced'. In the 'General' section, there is an 'Enable' checkbox which is checked. Below it, 'Manufacturer' is a dropdown menu showing 'Zycoo', and 'Type' is a dropdown menu showing 'D30'. The 'MAC' field contains the text '68692e021e7d'. In the 'Advanced' section, 'Line1' is a dropdown menu showing 'Extension: 401', and 'Label' is a text field containing 'John Doe'. At the bottom of the dialog are two buttons: 'Save' (green) and 'Cancel' (orange).

- **Manufacturer:** Manufacturer of the IP phone, currently, CooVox V2 supports phone provisioning phones from the following manufacturers: Zycoo, Grandstream, Yealink, Escene, AkuVox, Htek, Cisco, MOCET and Fanvil.
- **Model:** You must specify the exact model number of the phone, even if the phone is from the same manufacturer. This is because different models require different configuration files.
- **MAC:** CooVox IPPBX uses the MAC address of the phone to identify it on the local LAN as part of the provisioning process and it essential that you enter the correct MAC address for your IP Phone
- **Extension:** The extension number selected here will be auto configured to the phone with the MAC address given above.
- **Label:** Specify the user name of the phone.

Once you have added your new IP Phone(s) as described above, configuration files will be generated in the background of the IPPBX system. You can now connect the phone(s) to



your LAN and once the phone(s) have booted up they will download configuration files from the IPPBX system and complete auto configuration with the extension numbers you provided.

## 2.4.2 Phone Provisioning by DHCP

If you want to auto provision your IP phones using DHCP, please make sure they support DHCP option 66.

Please navigate to web menu: *Network Settings->DHCP Server* to enable DHCP service for the IP phones first. Please refer to [chapter 5.4](#).

Once DHCP is enabled you can add the phones in the same way as instructed above in Phone Provisioning by PnP section, however, enabling PnP is not required in this scenario.

### Notice:

*If you are going to enable DHCP service on the CooVox IPPBX system, please ensure there is no other DHCP server in the same LAN. If possible you can put the IPPBX and IP phones in a separate VLAN.*

## 2.5 Analog Extensions

If your CooVox IPPBX is equipped with an FXS port then you can configure an analog extension on your IPPBX system. This can be an ordinary analog phone or it can be a fax machine for sending and receiving faxes. The green LED indicates the RJ11 interface is FXS, you should connect the analog phone/fax machine to the FXS port of the IPPBX.

Navigate to web menu: *Basic->Extensions*, click "New User" button to add an analog extension.

New		X	
<b>General</b>			
SIP:	<input checked="" type="checkbox"/>	IAX2:	<input type="checkbox"/>
Name:	411	Extension:	411
Password:	UdTQ1P#@4g	Outbound CID:	
DialPlan:	DialPlan1	Analog Phone:	Port 2
<b>Voicemail</b>			

In the "Analog Phone" dropdown list, select an FXS port number for this new extension. This will allow the analog phone/fax machine connected to this port to be assigned with this extension number. The phone can now make and receive phone calls in the same manner SIP/IAX extensions do.

## 2.6 Extension Status

You can check the status of all extensions configured on your CooVox IPPBX via the *Operator* page "Operator" section.

Operator

Extensions				
Idle	Ringing	InUse	Hold	UnAvailable
401 401(SIP)	402 402(SIP)	403 403(SIP)	404 404(SIP)	405 405(SIP)
406 406(SIP)	407 407(SIP)	408 408(SIP)	409 409(SIP)	410 410(SIP)
Total:10		Online:3		Current Call(s):0

Here in this section, you can view real-time status of all extensions. Including idle(online), ringing, in use and also on hold.

## 2.7 Advanced Extension Configurations

### 2.7.1 Edit Properties of One Extension

On the *Basic->Extension* page, you can click the "Edit" button to edit the properties of one 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:

**Video Options**

Video Call:   H.261  H.263  H.263+  H.264

**Audio Codecs**

g722  
g726  
gsm  
speex

→  
←  
<<

alaw  
ulaw  
g729

Disallowed
Allowed

Below are the explanations for the configuration options:

#### General

- **SIP**: Tick the checkbox to activate SIP protocol.
- **IAX2**: Tick the checkbox to activate IAX2 protocol.
- **Name**: Alias of this extension which can be the name of the extension user.
- **Extension**: Number of this user extension.

- **Password:** The password used for the phones to register. This can be set manually or can be generated by the IPPBX system. Auto generated password consists of numbers, letters and special characters. If this is an analog extension then password is of no use as analog phones are not required to register.
- **Outbound CID:** Choose a number to show to the external called party. This feature only works with SIP trunks if the ITSP(Internet Telephony Service Provider) allows this number to be passed.
- **DialPlan:** Defines which type of numbers the extension can dial.
- **Analog Phone:** The FXS port number. An analog phone attached to this port will use this extension number.

### Voicemail

- **Enable:** Activate voicemail service for this extension.
- **Password:** Password for extension user to access the voicemail facilities.
- **Delete VMail:** Delete voice messages if the system has sent the message to user via email.
- **Email:** Email address of this extension user.

### Other Options

- **Web Manager:** If enabled, users can use their extension number and voicemail password to login to the IPPBX system web GUI.
- **Agent:** If enabled, this user extension can be a call queue agent.
- **Call Waiting:** With this option enabled, busy extensions will hear the call-waiting tone, and can use hook-flash to switch between callers. This option is only for analog extensions, for IP extensions you have to configure this feature directly on the IP phones.
- **Allow Been Spied:** Enable this option to allow other extension users the ability to spy on the phone calls of this extension by using feature codes.
- **Pickup Group:** Define a pickup group for this extension, extensions in the same pickup group can help pickup an incoming call on other ringing extensions in the same pickup group using feature code \*8. Available values are from 0 to 63.
- **Mobility Extension:** An external number can be specified here e.g. your mobile phone number. If you now call the IPPBX using the mobile phone specified, you will hear a dial tone and will have full access to the IPPBX system functionalities just as a standard extension user does.
- **Mobility Extension Number:** When "Mobility Extension" as described above is enabled, enter your external phone number here.

### VoIP Settings

- **NAT:** Check this option if extension user or the phone is located behind a router.
- **Transport:** Choose UDP, TCP or TLS as the transport protocol for SIP signaling.

- **SRTP:** Secure Real-time Transport Protocol(SRTP) encrypts the RTP traffic to secure your VoIP phone calls. Before enabling this option you need to ensure the end point can also support SRTP.
- **DTMF Mode:** Defines how the system detects DTMF tones, the default setting is rfc2833, it can be changed if necessary.
- **Permit IP:** Defines which IP address or network address is allowed to register to this extension number, other addresses will be unable to register. Addresses can be private or public IP Addresses.

### Video Options

- **Video Call:** Tick the checkbox to enable video call support. Supported video codecs are H.261, H.263, H.263+, H.264.

### Audio Codecs

CooVox V2 supported audio codecs are ulaw, alaw, G.722, G.726, G.729, GSM and Speex. Enable the ones you require by moving the audio codecs to the "Allowed" column.

## 2.7.2 Search Extension

If there are too many extensions on the extensions page, it is difficult to locate a single extension number to edit its properties, you can search by specifying the extension number and clicking "Search" button.

Extension: 405

**Extensions**

<input type="checkbox"/>	Name	Extension	Port	Protocol	DialPlan	Outbound CID	Options
<input type="checkbox"/>	1 405	405	--	SIP	DialPlan1		<a href="#">Edit</a>

## 2.7.3 Edit Properties of Multiple Extensions

Tick the checkboxes of the extensions you wish to edit, and click "Edit Selected" button and you are able to edit the options as below:

**Edit Selected** X

**General**  
 Password:   DialPlan:

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

**Other Options**  
 Web Manager:   Agent:   
 Pickup Group:

**VoIP Settings**  
 NAT:   Transport:   SRTP:   
 DTMF Mode:   Permit IP:

**Video Options**  
 Video Call:   H.261  H.263  H.263+  H.264

**Audio Codecs**  
Disallowed:   
Allowed:

If configured here, the selected extensions will have the same properties with the exception of the extension numbers.

**Notice:**

*Here you are configuring mutual parameters for the selected extensions, if you provide an IP address here in the "Permit IP" field, then only the unique endpoint with this IP can register to these extensions. Only consider this if these selected extensions are for an individual gateway or a remote office, otherwise please do not configure here or please specify a network address.*

## 2.7.4 Upload/Download Extensions

The upload/download extensions feature can be used to backup or bulk add extensions of the IPPBX system using text files. Supported file formats are CSV and TXT.

Click on the "Upload/Download Extensions" tab on *Basic->Extensions* page and you will see the menu as below:

Upload/Download Extensions

[Extensions](#) [Upload/Download Extensions](#)

**Upload Extensions**

Please choose file to upload:  No file chosen

**Download Extensions Template**

**Extensions Template**

Right Click here to Save as Template File (.csv)

Right Click here to Save as Template File (.txt)

**Download Extensions(.csv)**

- **Upload Extensions:** Here you can upload .csv or .txt file to generate extensions.
- **Download Extensions Template:** Here you can download a template file in .csv or .txt format. Inside there are examples which you can follow to add your desired new extensions in the same format. Once complete, the new file can then be used to upload to Coovox IPPBX system to generate new extensions.
- **Download Extensions(.csv):** Here you can download the existing extensions in the system for backup. The downloaded CSV file can be used for extension list recovery.

## 3 IPPBX Basic

### 3.1 Trunks

A trunk on an IPPBX system is essential for extensions to be able to make outbound phone calls. Coovox V2 IPPBX system currently supports FXO, GSM, WCDMA and VoIP trunks for outbound calls. (PRI and BRI trunks will be supported by other new models)

If your IPPBX system is equipped with FXO ports then you can attach the PSTN(Public Switched Telephone Network) lines to the FXO ports for the extensions to make phone calls through the local telephone company. If your system is equipped with GSM modules or WCDMA modules then you are able to make phone calls through your mobile carrier network.

#### 3.1.1 VoIP Trunks

Asterisk PBX can register as a SIP user agent to a SIP proxy (provider). If you have subscribed to a VoIP service from an ITSP, then with the account details provided by them you can configure a VoIP trunk on your Coovox IPPBX system for the user extensions to share and make outbound phone calls.

Navigate to web menu *Basic->Trunks*. Click "New VoIP Trunk" button and complete the account details provided to setup the trunk as in the example below.

The screenshot shows a 'New VoIP Trunk' configuration window with the following fields and values:

- Description: International
- Protocol: SIP
- Peer Mode:
- Host: gw1.sip.us :5060
- Maximum Channels\*: 0
- Prefix:
- Outbound CID:
- Without Authentication
- Username: 525274xxxx
- Authuser: 525274xxxx
- Password: .....
- Advanced Options
  - Fromdomain: gw1.sip.us
  - Insecure: port,invite
  - Fromuser: 525274xxxx
  - Qualify(sec): 2
  - DID Number:
  - Transport: UDP
  - DTMF Mode: RFC2833
  - NAT:
  - SRTP:
  - Auto Fax Detection:
  - Context: Default
  - Language: Default
- Audio Codecs**
  - ulaw  alaw  G.722  G.729  G.726  GSM  Speex
- Video Codes**
  - H.261  H.263  H.263+  H.264

Buttons: Save, Cancel

- **Description:** A name for this trunk.

- **Protocol:** SIP or IAX2 protocol.
- **Peer Mode:** If enabled then Host blank will be hidden. Peer mode requires only that the authorization matches rather than the IP address.
- **Host:** The SIP server domain or IP address.
- **Maximum Channels:** Maximum calls that can be made through this trunk at the same time, 0 means unlimited.
- **Prefix:** The prefix number you enter here will be added in front of any number you dial via this trunk. This feature is seldom required so please leave this field blank.
- **Caller ID:** The number you want to display to the called party.
- **Without Authentication:** If the service provider doesn't require a username and password for this account to register to their server then you can enable this option.
- **Username:** Username provided by VoIP Provider.
- **Authuser:** The optional authorization user for the SIP server
- **Password:** Password provided by VoIP Provider.

#### Advanced Options

- **Domain:** Your service provider's domain name.
- **Insecure:** Default value is "port, invite" ; "port"--Allow matching of peer by IP address without matching port number; "invite"-- Do not require authentication of incoming INVITEs.
- **From User:** fromuser=yourusername; Many SIP providers require this.
- **Qualify(sec):** Asterisk sends a SIP OPTIONS command regularly to check that the device is still online. Default value is 2(sec).
- **DID number:** Self defined, and can be used to setup number DID.
- **Transport:** Default transport type for SIP messages.
- **DTMF Mode:** Used to inform the system how to detect the DTMF(Dual Tone Multi Frequency) key press. Choices are inband, rfc2833, or info. By default we use RFC2833.
- **NAT:** With this option enabled, Asterisk may override the address/port information specified in the SIP/SDP messages, and use the information (sender address) supplied by the network stack instead. This feature is often required when there is a firewall located between the PBX and the service provider.
- **Context:** Custom dial plan for this trunk, by default it uses the "default" dial plan. Configure only if this trunk is for branch office integration, so calls coming from the other side can dial out from this IPPBX trunk directly. DO NOT change unless you fully understand how this feature works.
- **Language:** You can choose a desired language of the system voice prompts to play to the incoming calls from this trunk. For example, if the call is not answered or the user is busy the IPPBX system will notify the caller to leave a voice message in the language you set.



- **Audio Codecs:** Select the audio codec/codecs the provider can support.
- **Video Codecs:** If the ITSP supports video calls then you can enable compatible video codecs here for video phone calls.

With the exception of configuration options related to your service provider and your account details, please do not change the trunk advanced parameters if you are not familiar with them. After the SIP trunk is successfully added you can see it listed here on this page.

List of Trunks					New VoIP Trunk
	Provider Name	Type	Hostname/IP	Username	Options
1	International	SIP	gw1.sip.us	525274xxxx	<a href="#">Edit</a> <a href="#">Delete</a>

By clicking "Edit" you can modify the trunk settings and by clicking "Delete" you can remove this trunk from the IPPBX system.

### 3.1.2 FXO and GSM Trunks

#### FXO Trunks

On the IPPBX front panel, red LED indicates the RJ11 interface is FXO. You should attach the telephone wire from your telecom socket to the FXO ports. Once connected you should be able to see the connection status on *Operator* page "FXO/FXS/GSM Ports" section.

FXO/FXS/GSM Ports				
Status	Signal Strength	Type	Port	BLF Label
Connected		FXO	1	Channel1
Connected		FXO	2	Channel2
Connected		FXO	3	Channel3
Connected		FXO	4	Channel4
Disconnected		FXO	5	Channel5
Connected		FXO	6	Channel6
Connected		FXO	7	Channel7
Connected		FXO	8	Channel8

To be able to make calls on your FXO interface you will first need to create a trunk(s). To create a trunk you need to navigate to web menu *Basic->Trunks->FXO/GSM Trunks*. Click "New FXO/GSM Trunk" button and you'll see the available port numbers that can be used.

Edit
X

Description:

Lines: **FXO:**  1  2  3  4  5  6  7  8

Prefix:

**Advanced Options**

Call Method:

Busy Detection:  Busy Count:

Input Volume:  Output Volume:

Call Progress:  Progress Zone:

Busy Pattern:  Language:

Answer on Polarity Switch:

Hangup on Polarity Switch:

Auto Fax Detection:

- **Description:** A name for this FXO trunk.
- **Lines:** Available FXO and GSM ports.
- **Prefix:** The prefix number you enter here will be added in front of any number you dial via this trunk. This feature is seldom required so please leave this field blank.
- **Call Method:** If in this trunk you have more than 1 FXO/GSM ports selected, then this parameter defines how to use these ports for outbound phone calls.
- **Busy Detection:** Enable busy tone detection, it is also possible to specify how many busy tones to wait for before hanging up.
- **Busy Count:** Specify how many busy tones to wait for before hanging up, configurable only if Busy Detection is enabled.
- **Input Volume:** The volume of the incoming calls from FXO channel/channels.
- **Output Volume:** The volume of the outgoing calls from FXO channel/channels.
- **Call Progress:** If enabled, call progress attempts to determine answer, busy, and ringing on phone lines. This feature is HIGHLY EXPERIMENTAL and can easily detect false answers and therefore can prove unreliable.
- **Progress Zone:** Progress zone also affects the pattern used for busy detection, only effective when Call Progress in turned on.
- **Busy Pattern:** If busy detection is enabled, it is also possible to specify the cadence of your busy signal.
- **Language:** You can choose a desired language of the system voice prompts to play to the incoming calls from this trunk. For example, if the call is not answered or the user is busy the IPPBX system will notify the caller to leave a voice message in the language you set.
- **Answer on Polarity Switch:** When enabled, FXO (FXS signaled) ports watch for a polarity reversal to mark when an outgoing call is answered by the remote party.
- **Hangup on Polarity Switch:** In certain countries, a polarity reversal is used to signal the disconnection of a phone line. If the "hangup on polarity switch" option is selected, the call will be considered "hung up" on a polarity reversal.

When creating a FXO trunk, if you are not competent with the advanced options then please do not configure or change the default values.

### GSM Trunk

If you have ordered GSM or WCDMA modules for your CooVox U50V2 IPPBX, the user extensions will be able to make and receive phone calls from the mobile network.

You first have to insert SIM cards into the SIM slots of the GSM/WCDMA modules and then install the modules to the U50 IPPBX module slots. Antennas should be properly installed and placed in open space for better signal reception. After completing the above, power on the U50 IPPBX and you'll be able to configure GSM/WCDMA trunks in exactly the same way as you configure FXO trunks.

## GSM and WCDMA Specifications

Module	Working Frequencies
2GSM	GSM/GPRS 850/900/1800/1900MHz
4GSM	GSM/GPRS 850/900/1800/1900MHz
2WCDMA	Quad-band: GSM850, EGSM 900, DCS 1800, PCS 1900. SIM5320A: Dual-Band UMTS 850/1900MHz SIM5320E: Dual-Band UMTS 900/2100MHz SIM5320J: Dual-Band UMTS 850(800)/2100MHz
4WCDMA	

## 3.2 Outbound Routes

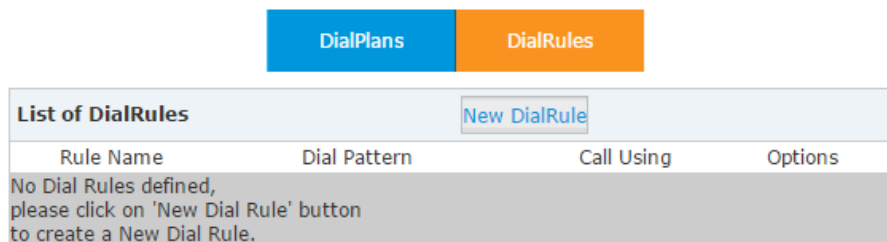
Outbound Routes allow you to define a set of dial rules that tell your CooVox IPPBX which Trunks (phone lines) to use when people dial external telephone numbers. A simple installation will direct CooVox IPPBX to send all calls to a single trunk. However, a complex setup could have for example an outbound route for emergency calls, another outbound route for local calls, another for long distance calls, and perhaps even another for international calls.

With all of the above possibilities, you may have to configure several trunks on your CooVox IPPBX system and therefore you will need to configure several dial rules and maybe also several dial plans.

### 3.2.1 Dial Rules

Navigate to web menu *Basic->Outbound Routes->DialRules*.

DialRules



By default there are no existing dial rules configured in the IPPBX system. You need to click “[New DialRule](#)” button to add a new dial rule.

**New DialRule** X

Rule Name: Domestic

PIN Set:  forDialRule Record in CDR:

Call Duration Limit: \_\_\_\_\_ seconds

Time Rule:

Place this call through:

Available Trunks Selected Trunks

Custom Pattern: 9XXX

Z Any digit from 1 to 9  
N Any digit from 2 to 9  
X Any digit from 0 to 9  
. Any number of additional digits

Delete 1 digits prefix from the front and auto-add digit \_\_\_\_\_ before dialing

Save Cancel

- **Rule Name:** A name for this dial rule.
- **PIN Set:** A collection of PIN codes for granting outbound phone calls. See [chapter 4.13](#).
- **Record in CDR:** Record the PIN codes used for outbound phone calls along with the user extension number and the dialed numbers in to the call logs.
- **Call Duration Limit:** Specify the maximum call time using this dial rule.
- **Time Rule:** Set a time condition when this dial rule can be used.
- **Available Trunks:** All existing trunks in the IPPBX system.
- **Selected Trunks:** Trunk/Trunks that can be used by this dial rule.
- **Custom Pattern:** Dial patterns act like a filter for matching numbers dialed with trunks. The various patterns you can enter are similar to Asterisk's definition of them:
  - X — Refers to any digit between 0 and 9
  - N — Refers to any digit between 2 and 9
  - Z — Any digit that is not zero. (E.g. 1 to 9)
  - . — Wildcard. Match any number of anything. Must match \*something\*.
- **Delete \_\_\_\_\_ digits prefix from the front and auto-add \_\_\_\_\_ digit before dialing:** The first blank allows you to strip some digit/digits before dialing out, here if required, you need to complete the number of digits to delete. The second blank is to prepend some digit/digits before dialing out, here you need to fill in the exact number of digits to be added in front of the dialed number. For example a user dialing 912345678 using the dial rule example above, the prefix 9 at the first digit will be removed, and 00 will be added, so eventually the number called will actually be 0012345678.

### 3.2.2 Dial Plans

Navigate to web menu *Basic->Outbound Routes->DialPlans.*

DialPlans

DialPlans
DialRules

List of DialPlans				New DialPlan
Default	DialPlan Name	Rules	Options	
<input checked="" type="checkbox"/>	1 DialPlan1	Ring Groups, Call Queues, Paging and Intercom, IVR, Conferences, Extensions, DISA, Directory, Spy	<a href="#">Edit</a>	<a href="#">Delete</a>

A default dial plan already exists in the IPPBX system. For most installations you just have to click "Edit" button on the default dial plan "DialPlan1" and tick on all dial rules to enable them, now extension users will be able to call any destinations using the trunk lines of the IPPBX system.

Edit X

DialPlan Name: DialPlan1

Include External Calling Rules

- International
- Domestic

Include Internal Calling Rules

- Ring Groups
- Call Queues
- Paging and Intercom
- IVR
- Conferences
- Extensions
- DISA
- Directory
- Spy

Save
Cancel

Calling rules in the left column are for external calls and calling rules in the right column are for internal calling. If you want to restrict some users from calling out through specific trunk lines or you don't want them to be able to call certain internal destinations, you can create a new dial plan by clicking the "New DialPlan" button.

**New DialPlan** X

DialPlan Name: DialPlan2

Include External Calling Rules

- International
- Domestic

Include Internal Calling Rules

- Ring Groups
- Call Queues
- Paging and Intercom
- IVR
- Conferences
- Extensions
- DISA
- Directory
- Spy

Save Cancel

In the new dial plan you should disable the rules you don't want others to use and save. After this, go to the extension configuration page and give the extension a different dial plan which ensures the restrictions you made take effect.

### 3.3 Inbound Control

The Inbound Control section is where you define how Coovox IPPBX system handles incoming calls. Typically, you determine the phone number that outside callers have called (DID Number) and then indicate which extension, Ring Group, Voicemail, or other destination to which the call should be directed.

#### 3.3.1 Inbound Destinations

A call destination in Coovox IPPBX system might be an IVR menu that instructs the callers to press certain digits to route their calls, a queue to wait for specific telephone services, a ring group to call a number of user extensions, or virtually any other type of process to route the call in whatever way is desired. A call may have several destinations throughout its lifespan.

Below is a list of call destinations available in Coovox IPPBX system:

- Extension
- Voicemail
- IVR
- Ring Group
- Paging Group
- Conference
- Call Queue

- DISA
- Time Rule
- FAX
- Dial By Name
- Hangup

### 3.3.2 IVR

IVR, or interactive voice response, is responsible for the menus people hear and respond to when they call up a company or business and hear the words for example: "press 1 for sales, press 2 for marketing, press 0 to speak to the operator,".

#### IVR Prompts

To configure an IVR menu on CooVox IPPBX system you'll first need to record your IVR prompts, these IVR prompts will communicate to the callers the menu options that they have e.g. press one for sales.

Navigate to web menu: *Inbound Control->IVR Prompts*

On this page you can delete the default voice prompts and click "New Voice" button to record a new voice prompts from a designated extension.

The screenshot shows a modal window titled "New Voice" with a close button (X) in the top right corner. Inside the window, there are three input fields: "File Name:" with the text "office\_hours", "Format:" with a dropdown menu showing "WAV (16-bit)", and "Extension used for recording:" with a dropdown menu showing "402". Below these fields are two buttons: a green "Record" button and an orange "Cancel" button.

Click "Record" button and the extension will ring, pickup the extension and speak to record your message. Once recording is complete your voice prompts will be listed on this page. There is another way to add voice prompts to the system, click "Upload Voice Prompts" tab.

The screenshot shows a page titled "Upload IVR Prompts". At the top, there are two tabs: "IVR Prompts" (blue) and "Upload IVR Prompts" (orange). Below the tabs is a light blue header with the text "Upload IVR Prompts". Underneath, there is a red note: "Note: The sound file must be mp3, wav(16bit/8000Hz/Mono), gsm, ulaw or alaw! The size is limited in 15MB!". Below the note, it says "Please choose file to upload:" followed by a "Choose File" button and the text "No file chosen". At the bottom, there is a green "Upload" button.

Here you can select a pre-recorded voice prompts file from your operating system to upload and once complete your file will be listed on *Voice Prompts* page. Now you can use your file to setup your personalized IVR menu.

## IVR menu

Navigate to web menu: *Inbound Control->IVR*.

Click "New IVR" button to add an IVR menu.

Key	Action
0	Goto Extension ▼ 401(401) ▼
1	Goto Ring Group ▼ sales ▼
2	Goto Ring Group ▼ marketing ▼
3	Disabled ▼
4	Disabled ▼
5	Disabled ▼
6	Disabled ▼
7	Disabled ▼
8	Disabled ▼
9	Disabled ▼
*	Disabled ▼
#	Disabled ▼
t	Goto Extension ▼ 401(401) ▼
i	Goto Extension ▼ 401(401) ▼

Let's look at the above example where your IVR message says "Press 1 for sales, press 2 for marketing, press 0 for operator". If the caller is on the IVR menu, and after they hear the voice prompts they press 1 then the sales ring group will ring, if 2 is pressed then the Marketing ring group will ring, if 0 is pressed then will the IVR will ring the operator extension.

### IVR Settings

- **Name:** Name for this IVR menu.
- **Extension:** Extension number for the IVR, by calling this number you can access the IVR menu.

### Welcome Message

- **Please Select:** Select a voice prompts for this IVR menu.
- **Custom Prompts:** Click this button to navigate to *Inbound Control->IVR Prompts* page for new voice prompts.
- **Repeat Loops:** Define how many times to play the IVR menu to the caller.
- **Timeout:** Timeout for key pressing of each IVR loop.
- **Dial other Extensions:** If enabled, the caller can dial extension numbers directly when in the IVR.
- **Custom:** By clicking "Custom" you can set a dial plan for this IVR menu and the callers



on the IVR will be able to dial other destinations that the dial plan allows.(Not recommended)

- **Key Press Events:** Define which destination to go by pressing a key on the phone keypad. If undefined keys are pressed then they will be handled by the "i" parameter, "i" which means invalid. And "t" stands for timeout, after all IVR loops are completed without the caller pressing any key then the incoming call will be handled by "t" parameter.

### 3.3.3 Ring Group

In a ring group, an incoming call will ring the phones of everyone in the group at the same time. To configure a ring group please navigate to web menu: *Inbound Control->Ring Groups*.

Click "New Ring Group" button to add a ring group.

**Edit - sales** X

Name: sales Strategy: RingAll

Ring Group Members	Available Channels
403(SIP) 403	401(SIP) 401
404(SIP) 404	402(SIP) 402
405(SIP) 405	407(SIP) 407
406(SIP) 406	408(SIP) 408
	409(SIP) 409
	410(SIP) 410
	411(SIP) 411
	412(SIP) 412

Label: \_\_\_\_\_

Extension for this ring group: 640

Ring (each/all) for lasting time(sec): 20

**If not answered**

- Goto Extension
- Goto Voicemail
- Goto Ring Group
- Goto IVR
- Hangup

Save Cancel

The extensions in the "Available Channels" column can be added to the ring group as a ring group member.

- **Name:** Name for this ring group.
- **Strategy:** Defines how to ring the group members; selecting "RingAll" will ring all the member extensions at the same time, selecting "Ring In Order" will ring the member extensions one by one.
- **Ring Group Members:** The extensions selected to be the members of the ring group.
- **Available Channels:** All available extensions/channels can be added to the ring group.
- **Label:** Extensions can be members of multiple ring groups and therefore by giving each ring group a different label, if an incoming call rings a ring group the label will be

displayed on the phone screen along with the caller ID. Therefore a ring group member will know which ring group the call is coming from.

- **Extension for this ring group:** Reach the ring group member by calling this extension.
- **Ring (each/all) for lasting time(sec):** Ring duration of the group members.
- **If not answered:** Defines a destination to redirect incoming calls to if no one answers from within the ring group.

### 3.3.4 Call Queue

A call queue places incoming calls in line to be answered while extension users are busy with other calls. The queued calls are distributed to the next available extension user in the order received. Once a call queue has been created, it can be assigned to specific extensions and configured to feature greetings, messages, and hold music.

To configure a call queue please navigate to web menu *Inbound Control->Call Queue*.

There are 3 existing call queues pre-configured and all you have to do is click "Edit" button to configure them. If you require more call queues then click "New Call Queue" to add more.

**New** X

**Call Queue Reference:**

Queue Number: 633 Label: \_\_\_\_\_  
Ring Strategy: Random

**Agents:**

You do not have any users defined as agents!  
[click here](#) to manage users.

Queue Options:	Announcements:
Agent TimeOut(sec): 15 Auto Pause: <input type="checkbox"/> Wrap-Up-Time(sec): 10 Max Wait Time(sec): _____ Max Callers: 8 Join Empty: <input type="checkbox"/> Leave When Empty: <input type="checkbox"/> Auto Fill: <input checked="" type="checkbox"/> Report Hold Time: <input type="checkbox"/>	<b>Caller Position Announcements</b> Frequency(sec): 30 Announce Hold Time: No
	<b>Periodic Announcements</b> Repeat Frequency(sec): 0 Announcements Prompt: _____
	<b>If not answered</b> Destination: Hangup

Save Cancel

Here we can see in the "Agents" field there are no available agents to be assigned to the call queues. Click "click here" and you'll be redirected to the extension page to determine which extensions will be employed as call queue agents.

Tick the checkbox of the extension numbers which will be employed as call queue agents, then click "Edit Selected" button and tick the "Agent" option in the "Other Options" section.

**Other Options**

Web Manager:   Agent:   
 Pickup Group:

Save and go back to *Inbound Control->Call Queues* page again and now you will be able to configure the existing call queues and add new call queues with available agents.

Edit
X

**Call Queue Reference:**

Queue Number:  Label:

Ring Strategy:  ▼

**Agents:**

406 407 408 409 410

Queue Options:	Announcements:
<p>Agent TimeOut(sec): <input type="text" value="15"/></p> <p>Auto Pause: <input type="checkbox"/></p> <p>Wrap-Up-Time(sec): <input type="text" value="10"/></p> <p>Max Wait Time(sec): <input type="text"/></p> <p>Max Callers: <input type="text" value="8"/></p> <p>Join Empty: <input type="checkbox"/></p> <p>Leave When Empty: <input type="checkbox"/></p> <p>Auto Fill: <input type="checkbox"/></p> <p>Report Hold Time: <input type="checkbox"/></p>	<p><b>Caller Position Announcements</b></p> <p>Frequency(sec): <input type="text" value="30"/></p> <p>Announce Hold Time: <input type="text" value="Yes"/> ▼</p> <p><b>Periodic Announcements</b></p> <p>Repeat Frequency(sec): <input type="text" value="0"/></p> <p>Announcements Prompt: <input type="text"/></p> <p><b>If not answered</b></p> <p>Destination: <input type="text" value="Hangup"/> ▼</p>

- **Queue Number:** Define an extension number to identify the queue.
- **Label:** Define the label for the queue. A user can be an agent of multiple queues, by giving a label for the call queue, if an incoming call is distributed to an agent the label will be displayed on the phone screen along with the caller ID. So a call queue agent knows which call queue the call is coming from.

**Ring Strategy**

- **RingAll:** Ring all available agents until one answers(default)
- **RoundRobin:** Starting with the first agent, ring the extension of each agent in turn until the call is answered.
- **LeastRecent:** Ring the extension of the Agent who has least recently received a call
- **FewestCalls:** Ring the extension of the Agent who has taken the fewest number of calls.
- **Random:** Ring the extension of a random Agent.
- **RRmemory:** RoundRobin with Memory, like RoundRobin above, except instead of the next call starting with the first agent, the system remembers which extension was last called and begins the round robin with the next agent .
- **Agent:** Check each agent that you want to be a member of this specific Call Center



Queue.

- **Agent TimeOut(sec)**: Specify the number of seconds to ring an agent's extension before sending the call to the next Agent (based on Ring Strategy).
- **Auto Pause**: If an Agent's extension rings and the Agent fails to answer the call, automatically pause that agent to stop them receiving further calls from the queue.
- **Wrap-Up-Time(sec)**: This is the amount of time in seconds that an agent has to complete work on a call after which the call is disconnected. (Default is 0, which means no wrap-up time.)
- **Max Wait Time(sec)**: Calls that have been waiting in the queue for this number of seconds will be sent to the "If not answered" destination.
- **Max Callers**: Max number of callers who are allowed to wait in the queue. (Default is 0, which means unlimited.) when the maximum number of callers in the queue is reached, subsequent callers will be sent to the "If not answered" destination.
- **Join Empty**: Allow callers to enter the Queue when no Agents are available. If this option is not defined, callers will not be able to enter Queues without available agents - callers will be sent to the "If not answered" destination.
- **Leave When Empty**: If this option is selected and calls are still in the queue when the last agent logs out, the remaining callers in the Queue will be transferred to the "If not answered" destination. This option cannot be used with Join Empty simultaneously.
- **Auto Fill**: Callers will be distributed to Agents automatically.
- **Report Hold Time**: Report the hold time of the next caller for Agent when the Agent is answering the call.
- **Frequency(sec)**: Repeat frequency to announce the hold time for callers in the Queue. ("0" means no announcement).
- **Announce Hold Time**: Announce the hold time. Announce (yes), do not announce (no) or announce once (once), There will be no announcement when the hold time is less than 1 minute.
- **Repeat Frequency(sec)**: Interval time to play the voice menu for callers. ("0" means do not play).
- **Announcement Prompt**: Select an IVR prompt to be used as the Announcements Prompt.

### 3.3.5 Time Based Rules

Many businesses have fixed working hours where they know for example that they are only open Monday to Friday between 9am and 5pm and will be closed for business at all other times. Time conditions in CooVox IPPBX allow you to control what happens to inbound calls both during and outside normal business hours.

Navigate to web menu: *Inbound Control->Time Based Rules.*

Click "New Time Rule" to add a time condition for the system:

**New Time Rule** X

Rule Name: workdays

**Time & Date Conditions**

Start Time: 09 : 00 End Time: 17 : 00  
 Start Day: Mon End Day: Fri  
 Start Date: 01 End Date: 31  
 Start Month: Jan End Month: Dec

**Destination**

if time matches: IVR -- office-hours  
 if time does not match: IVR -- closed time

Save Cancel

Here you configure the time and date of your business hours. If you receive a call where the time matches then the inbound call will be directed to "office-hours" IVR menu. If the time does not match then the inbound call will be directed to "closed time" IVR menu.

### 3.3.6 Office Closed Timing

Office closed timing is an extending of time based rules, you can manually activate office closed timing by feature code. This feature allows much more flexible time conditions to be temporarily applied for the offices which may have some unscheduled businesses and activities off the time table of the time based rule/rules.

For example, the office opens in the morning but there's an event in the afternoon and by then nobody will be able to answer phone calls. You can direct the inbound calls to an extension's voicemail or the closed time IVR.

**Enable Office Closed Timing**

Enable Office Closed Timing: \*81 Disable Office Closed Timing: \*081  
 Destination: Voicemail 800  
Save Cancel  
 Status: Enable

- **Enable Office Closed Timing:** By dialing the feature code on the phone, you can activate office closed timing. (Default is \*81)
- **Disable Office Closed Timing:** By dialing the feature code on the phone, you can deactivate office closed timing. (Default is \*081)
- **Destination:** The destination of the inbound calls while office closed timing is activated. It needs to be pre-configured before you can use this feature.
- **Save:** Save the settings of office closed timing.
- **Cancel:** Cancel the settings.
- **Status:** Status of office closed timing, "Enabled" or "Disabled".

### 3.3.7 Inbound Routes

#### General

For both FXO channels and VoIP channels, you can define default inbound destinations. If you don't want the inbound calls to always go to an IVR menu, ring group or extension, then you can use a time rule to handle the inbound calls.

**From FXO/GSM Channels**

Distinctive Ring Tone: ;info=domestic

Destination: Goto Time Rule Time Rule -- TimeRule

**From VoIP Channels**

Distinctive Ring Tone: ;info=international

Destination: Goto Time Rule Time Rule -- TimeRule

Save Cancel

#### Port DIDs

If some of the FXO/GSM ports are dedicated to a specific calling service and you want them handling differently to your generic service then you can configure "Port DIDs" here.

**New Port DID**

Port: FXO Port 1 Label: VIP

Destination: Goto Extension 401(401)

Save Cancel

For the above example, all inbound calls from FXO port 1 will be directed to extension number 401. General inbound control will still work with other ports which have not been configured with port DIDs.

#### Number DIDs

Number DID is only for inbound control of VoIP channels and not FXO channels. If you have a VoIP trunk for outbound and inbound phone calls, then your service provider will issue you with a DID number with which people can call you on.

Click "Number DIDs" tab and click "New Number DID" button to add a number DID rule:

**New Number DID**

DID Number: 51097214 Label: Inquiry

Destination: Goto Extension 410(410)

Save Cancel


In this example, if the caller calls your DID number 51097214 the call will go directly to

extension 410, general inbound control will not work with this DID number. If you experience problems setting inbound DID then please check with your service provider to confirm the exact DID number that the service provider is passing to the CooVox IPPBX.

### DOD Settings

DOD is also known as direct outward dialing, by specifying the number of an external caller in the CooVox IPPBX system, when this caller calls in, this call can be directed to a destination directly without restriction of time rule or IVR.

Click DOD Settings tab and click New DOD to add a record.



The screenshot shows a web form titled "New DOD" with a close button "X" in the top right corner. The form contains two input fields: "DOD Number:" with the value "02885337096" and "Destination:" with a dropdown menu showing "Goto Extension" and a text box containing "405(405)". Below the fields are two buttons: "Save" and "Cancel".

For this example, if the caller 02885337096 calls the office number, the call will go directly to extension 405.

## 4. IPPBX Advanced

### 4.1 Global IPPBX Advanced Settings

#### 4.1.1 General

Navigate to web menu *Advanced->Options->General*.

Here on this page you can configure some global options for all user extensions. In the "Local Extension Settings" section you can view the below options that can be configured.

#### Local Extension Settings

**Local Extension Settings**

Operator Extension:

Global Ring Time Set(sec):

Enable Transfer:

Enable Attended Transfer Caller ID:

Enable Music On Ringback:

Auto-Answer:  Fax Detect Time:

Web Dial Auto-Answer:

Record Format:

Call Forward CID:

P-Preferred-Identity:

- **Operator Extension:** Choose an extension to be operator extension. When an incoming call has been directed to voicemail, then by pressing '0' the caller will be put through to the operator extension.
- **Global Ring Time Set(sec):** If not specifically configured, an incoming call will ring the extension for the time given here.
- **Enable Transfer:** If enabled, the extension users will be able to perform call transfers.
- **Enable Attended Transfer Caller ID:** Normally if you use feature code \*2(This will be introduced in chapter [4.18](#)) to transfer a call to another extension, the extension user only sees your extension number as caller ID but not the actual caller ID, by enabling this option the real caller ID will be passed to the user extension.
- **Enable Music On Ringback:** If enabled, callers will hear music instead of ringback tone when calling other extensions.
- **Auto-Answer:** Auto-answer enables the IPPBX to automatically answer the inbound calls from analog ports.
- **Fax Detect Time:** If auto-answer enabled, you are able to configure the fax auto detection time here.



- **Web Dial Auto-Answer:** Enable/disable auto answer of the extension numbers while dialing from Web GUI.
- **Record Format:** Choose GSM or WAV as the call recording format.
- **Call Forward CID:** Allow passing the real caller ID to the forwarded number.
- **P-Preferred-Identity:** The P-Preferred-Identity header is used among trusted SIP entities (typically intermediaries) to carry the identity of the user sending a SIP message as it was verified by authentication.

### Default Settings for New User

Default Settings for New User			
SIP: <input checked="" type="checkbox"/>	IAX2: <input type="checkbox"/>	Web Manager: <input type="checkbox"/>	Call Waiting: <input checked="" type="checkbox"/>
Agent: <input type="checkbox"/>	Voicemail: <input checked="" type="checkbox"/>	Delete VMail: <input type="checkbox"/>	VM Password: <u>1234</u>
NAT: <input type="checkbox"/>	Transport: <u>UDP</u> ▼	SRTSP: <input type="checkbox"/>	
<b>Audio Codecs</b>			
<input checked="" type="checkbox"/> ulaw	<input checked="" type="checkbox"/> alaw	<input type="checkbox"/> G.722	<input checked="" type="checkbox"/> G.729
		<input type="checkbox"/> G.726	<input type="checkbox"/> GSM
			<input type="checkbox"/> Speex

In this section, options are defined for the creation of new extensions. If you have one of the options enabled, then so will any newly created extensions.

### Extension Preferences

Extension Preferences	
User Extensions	<u>401</u> to <u>499</u>
Conference Extensions	<u>900</u> to <u>909</u>
IVR Extensions	<u>610</u> to <u>629</u>
Queue Extensions	<u>630</u> to <u>639</u>
Ring Group Extensions	<u>640</u> to <u>659</u>
Paging Group Extensions	<u>660</u> to <u>679</u>
Web Extensions	<u>680</u> to <u>699</u>
<input type="button" value="Reset"/>	

The user extension number and system extension number ranges are defined here to avoid any conflicts within the CooVox V2 IPPBX system. You can modify these number ranges according to your requirements.

#### 4.1.2 Global Analog Settings

Global Analog Settings are used for configuring the CooVox V2 IPPBX system to seamlessly work with the telephone lines from your telecommunications provider.

Navigate to web menu *Advanced->Options->Global Analog Settings*.

#### Caller ID Detect

Caller ID Detect	
Caller ID Detection:	<input checked="" type="checkbox"/>
Caller ID Signaling:	<u>Bell-US</u> ▼
Caller ID Start:	<u>Ring</u> ▼
CID Buffer Length:	<u>2500</u> ▼

These options are used to teach the CooVox IPPBX system how to detect caller

identity(caller ID) from the PSTN lines on FXO ports.

- **Caller ID Detection:** Enable/Disable Caller ID Detection.
- **Caller ID Signaling:** The signaling type applied on the PSTN lines to pass caller ID.  
Bell-US—Also known as Bellcore FSK. Used in the Canada, China, Hong Kong and US.  
DTMF—Dual Tone Multi-Frequency. Used in Denmark, Finland and Sweden.  
V23—Mostly used in UK.  
V23-Japan—Mostly used in Japan.
- **Caller ID Start:** Defines when the caller ID starts.  
Ring—Caller ID starts when a ring is received.  
Polarity—Caller ID starts when polarity reversal starts.  
Polarity(India)—Can be used in India.  
Before Ring—Caller ID starts before a ring received.
- **CID Buffer Length:** The buffer length can be used to store caller ID info.

## General

General	
Opermode:	FCC
Tone Zone:	China
Ring Timeout(s):	8
Relax DTMF:	<input type="checkbox"/>
Send Caller ID After:	1
Echo Cancel:	<input checked="" type="checkbox"/>
Echo Training:	no (yes/no/number)

- **Opermode:** Set the Opermode for FXO Ports.
- **ToneZone:** Select the tone zone of your country.
- **Ring Timeout(s):** FXO (FXS signaled) devices must have a timeout to determine if it should hang up before the line is answered. This value can be tweaked to shorten how long it takes before DAHDI considers a non-ringing line to have hung-up.
- **Relax DTMF:** Helps DTMF signal detection.
- **Send Caller ID After:** Certain countries (UK) have ring tones with different ring tones (ring-ring), which means the caller ID needs to be set later on, and not just after the first ring, as per the default (1).
- **Echo Cancel:** Enable/Disable software Echo Cancel algorithm.
- **Echo Training:** Enabling echo training will cause the PBX system to mute the channel, send an impulse, and use the impulse response to pre-train the echo canceller so it can start out with a much closer idea of the actual echo. Value may be "yes", "no", or a number of milliseconds to delay before training (default = 400). This option does not apply to hardware echo cancellers.

### 4.1.3 Global SIP Settings

Global SIP settings allow you to configure some general and advanced options for the IP-PBX system global SIP preferences. Navigate to web menu *Advanced->Options->SIP Settings*.

#### General

General	
<input type="checkbox"/> Enable	UDP Port: <u>5060</u>
<input type="checkbox"/> Enable	TCP Port: <u>5060</u>
	TLS Port: <u>5061</u>
	Start RTP Port: <u>10001</u>
	End RTP Port: <u>10500</u>
	DTMF Mode: <u>Auto</u> ▼
	Allow Guest: <input type="checkbox"/>
	Max Registration/Subscription Time(sec): <u>3600</u>
	Min Registration/Subscription Time(sec): <u>60</u>
	Default Incoming/Outgoing Registration Time(sec): <u>60</u>

- **UDP Port:** SIP over UDP service port. By default Zycoo IPPBX system uses UDP as SIP transmission protocol. Port number can be changed here if required.
- **TCP Port:** By ticking the "Enable" checkbox you can enable global SIP TCP support. To register a SIP extension over TCP protocol, you'll have to select TCP transport on the extension configure page, please refer to [chapter 2.7.1](#).
- **TLS Port:** By ticking the "Enable" checkbox you can enable global SIP TLS support. To register a SIP extension over TLS protocol, you'll have to select TLS transport on the extension configuration page, please refer to [chapter 2.7.1](#).
- **Start RTP Port/End RTP Port:** The UDP ports used by Coovox IPPBX system to carry RTP voice stream. Do not change the port numbers or you may encounter audio issue with phone calls.
- **DTMF Mode:** The DTMF mode specifies how touch tones will be transmitted to the other side of the call. Possible values for this field are rfc2833, inband, info, and auto.
- **Allow Guest:** This setting determines if anonymous callers are permitted to place calls to the Coovox IPPBX system. For security precautions please do not enable this option.
- **Max Registration/Subscription Time(sec):** Maximum allowed time of incoming registrations and subscriptions (seconds).
- **Min Registration/Subscription Time(sec):** Minimum length of registrations/subscriptions.
- **Default Incoming/Outgoing Registration Time(sec):** Default length of incoming/outgoing registration.

## NAT Support

When the CooVox IPPBX system is behind a NAT device and needs to communicate to the outside. It needs to know whether it is talking to someone "inside" or "outside" of the NATted network. For example, if you are going to deploy remote extensions you have to tell the CooVox IPPBX system which network address/addresses are from inside and which are from outside. Below is an example configuration.

NAT Support	
External IP:	<u>117.176.159.157</u>
External Host:	<u>117.176.159.157</u>
External Refresh(sec):	<u>10</u>
Local Network Address:	<u>192.168.1.0/255.255.255</u>
Local Network Address:	<u>192.168.10.0/255.255.255</u>
Local Network Address:	<u>  </u>

- **External IP:** Your static public IP address or domain name.
- **External Host:** This is similar to "External IP" except that the hostname is looked up every "External Refresh" seconds(default 10's).
- **External Refresh(sec):** The refresh interval of the "External Host".
- **Local Network Address:** Your local network address/addresses.

### Notice:

*If you have one-way audio or no audio issue on the remote extensions then this most probably means that NAT support is not properly configured. Please check your configurations [here](#).*

## Type of Service

Asterisk supports different QoS settings at the application level for various protocols on both signaling and media. The Type of Service (TOS) byte can be set on outgoing IP packets for various protocols. The TOS byte is used by the network to provide some level of Quality of Service (QoS) even if the network is congested with other traffic.

Type of Service	
TOS for Signaling packets:	CS3 ▾
TOS for RTP audio packets:	ef ▾
TOS for RTP video packets:	AF41 ▾
COS Priority for Signaling packets:	3 ▾
COS Priority for RTP audio packets:	5 ▾
COS Priority for RTP video packets:	4 ▾
DNS SRV Look Up:	<input type="checkbox"/>
Relax DTMF:	<input checked="" type="checkbox"/>
RTP TimeOut(sec):	<u>                  </u>
RTP Hold TimeOut(sec):	<u>                  </u>
Add 'user=phone' to URI:	<input type="checkbox"/>
UserAgent:	<u>VOIP</u>

- **TOS for Signaling Packets:** Sets TOS for SIP packets.
- **TOS for RTP audio packets:** Sets TOS for RTP audio packets.
- **TOS for RTP video packets:** Sets TOS for RTP video packets.
- **COS Priority for Signaling packets:** Sets 802.1p priority for SIP packets.
- **COS Priority for RTP audio packets:** Sets 802.1p priority for RTP audio packets.
- **COS Priority for RTP video packets:** Sets 802.1p priority for RTP video packets.
- **DNS SRV Look Up:** Enable DNS SRV lookups on outbound calls.
- **Relax DTMF:** Relax DTMF handling.
- **RTP TimeOut(sec):** Terminate call if there is 60 seconds of no RTP or RTCP activity on the audio channel when we're not on hold. This feature enables the ability to hangup a call in the case of a phone disappearing from the network, for instance if the phone loses power.
- **RTP Hold TimeOut(sec):** Terminate call if 300 seconds of no RTP or RTCP activity on the audio channel when on hold.
- **Add 'user=phone' to URI:** Enable this option if the SIP provider requires ";user=phone" on URI.
- **UserAgent:** Allows you to change the user agent string. The default user agent string also contains the Asterisk version. If you don't want to expose this, change the user agent string here.

### Outbound SIP Registrations

The "Outbound SIP Registrations" configures the register behaviors of CooVox IPPBX system when registering as a client to the other SIP servers.

Outbound SIP Registrations
Register TimeOut(sec): <u>30</u>
Register Attempts: <u>10</u>

- **Register TimeOut(sec):** Retry registration every 30 seconds (default).
- **Register Attempts:** Number of registration attempts before the IPPBX system give up. Default is 10 and 0 means continue forever.

### 4.1.4 Global IAX Settings

Navigate to web menu *Advanced->Options->IAX2 Settings*.

General
UDP Port: <u>4569</u>
Bandwidth: <u>low</u> ▼
Max Registration/Subscription Time(sec): <u>1200</u>
Min Registration/Subscription Time(sec): <u>60</u>

- **UDP Port:** IAX2 signaling and media port, the default is 4569.
- **Bandwidth:** Specify bandwidth of low, medium, or high to control which codecs are used in general.
- **Max Registration/Subscription Time(sec):** Maximum amount of time that IAX peers can request as a registration expiration interval (in seconds).
- **Min Registration/Subscription Time(sec):** Minimum amount of time that IAX peers can request as a registration expiration interval (in seconds).

## 4.2 Virtual Fax

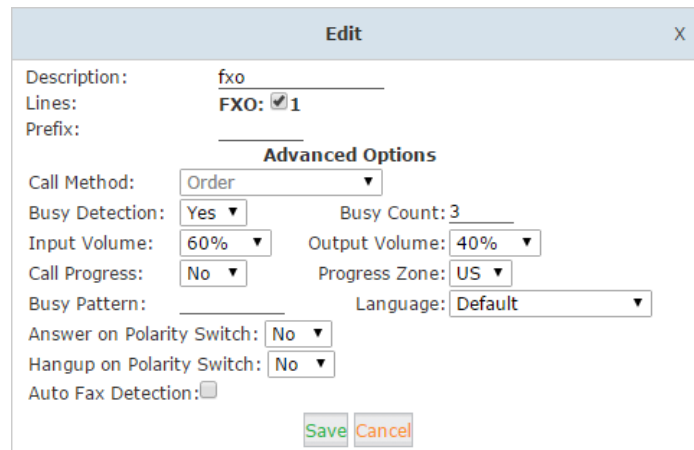
CooVox IPPBX system has the ability to auto detect incoming faxes and send the received faxes to a user's email box. If you don't wish to send the fax by email then faxes can be saved to a user's extension account.

### Notice:

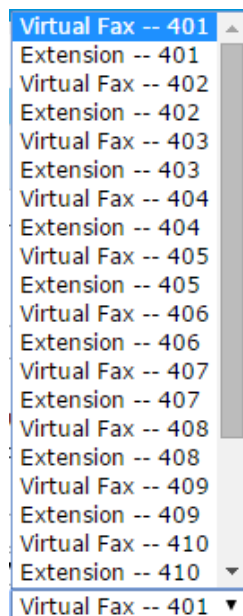
Please enable Virtual Fax services on *Virtual Fax* page first, and then follow the instructions below to configure.

### 4.2.1 Receive Fax

CooVox IPPBX system detects incoming faxes from the trunks. To configure CooVox IPPBX to auto detect incoming faxes please navigate to web menu *Basic->Trunks*.



Click on "Edit" to edit the trunk(either analog or VoIP trunk) that you want to configure fax auto detection on. Find the "Auto Fax Detection" option and tick the checkbox. You'll see a dropdown list from which you can select any extensions to direct the detected faxes to.



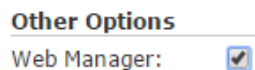
If you want the IPPBX system to send the received faxes to an email address(Fax to Email) then please select an extension number starting with "Virtual Fax". Then navigate to *Basic->Extension* page to specify the email address in "Email(Fax/Voicemail)"section. If you require that the received fax is stored in the IPPBX system only then you should select a virtual fax extension without specifying the email address. Finally, if you want the incoming fax to be handled by a fax machine, please select the extension number assigned to the fax machine.

**Notice:**

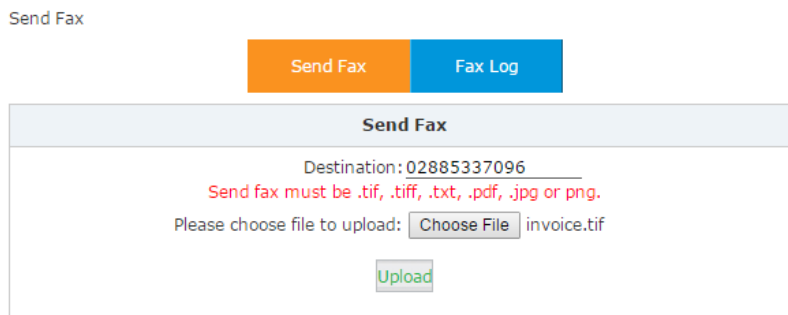
If you are configuring Fax to Email, you also have to configure the SMTP service before it will work. Please refer to [chapter 4.3.4](#).

### 4.2.2 Send Fax

To send a fax you must first login to the CooVox IPPBX web interface with an extension number and the voicemail password for this extension. Before doing this please ensure this extension has the "Web Manager" option enabled on the extension configure page.

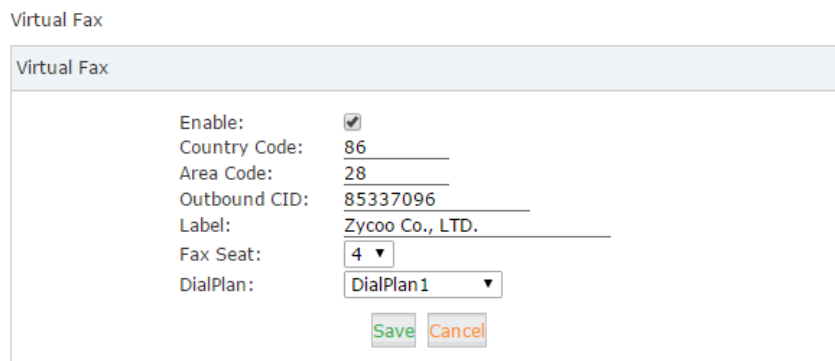


After login, navigate to the *Send Fax* page.



Enter the fax number and click on "Choose File" to locate the file you are planning to send, upload the file and then send the fax.

There are some optional options for outbound faxes, please navigate to web menu *Advanced->Virtual Fax*.



- **Enable:** Enable Virtual fax feature for receiving and sending faxes.



- **Country Code:** Enter your country code here.(Optional)
- **Area Code:** Enter your Area Code here.(Optional)
- **Outbound CID:** Only works if the outbound fax is to be sent through VoIP trunks. The other side receives your fax with this number.
- **Label:** Define custom information to be printed to the header of the fax pages.
- **Fax Seat:** Defines how many users can send fax at the same time.
- **DialPlan:** A dial plan to send faxes.

## 4.3 VoiceMail

### 4.3.1 General Voicemail Options

Voice mail allows callers to leave messages for subscribers (user extensions) of the IPPBX system when they are unable to answer the incoming calls.

#### VoiceMail Reference

VoiceMail Reference	
Max Greeting Time(sec):	30
Dial "0" for Operator:	<input checked="" type="checkbox"/>

- **Max Greeting Time(sec):** Maximum voicemail box greeting message duration.
- **Dial "0" for Operator:** If this option is enabled then callers will be able to dial "0" to transfer out of voicemail to the Operator.

#### Voice Message Options

Voice Message Options	
Message Format:	WAV (16-bit) ▼
Maximum Messages:	100 ▼
Max Message Time(min):	2 ▼
Min Message Time(sec):	2 ▼

- **Message Format:** The audio file format to be used for the recording.
- **Maximum Messages:** The maximum amount of voice messages for each extension.
- **Max Message Time(min):** The maximum time duration of an individual voicemail message.
- **Min Message Time(sec):** The minimum time duration of an individual voicemail message. Default minimum duration is 2 seconds, which means voice messages which are less than 2seconds will be ignored by the IPPBX system.

#### Playback Options

Playback Options	
<input checked="" type="checkbox"/>	Say Message CallerID
<input checked="" type="checkbox"/>	Say Message Duration
<input type="checkbox"/>	Play Envelope
<input type="checkbox"/>	Allow Users to Review

These options are for voicemail message playback.

- **Say Message CallerID:** Announce the Caller ID of the caller who left this message before playing the voice message.
- **Say Message Duration:** Announce the message duration before playing the voice message.
- **Play Envelope:** Announce the date, time and caller ID for the voicemail message.
- **Allow Users to Review:** If enabled, this option will allow users to review the voice message.

### 4.3.2 Playback Voicemail on the phone

Navigate to web menu *Advanced->Feature Codes*.

On this page, you'll find two feature codes that can be used for checking voicemail.

**Voicemail Main Menu:** \*60

**Check Extension Voicemail:** \*61

Dial \*60 and you will enter the main menu of voicemail feature, by specifying the extension number and voicemail password of the required extension then you can check its voicemail and you can do this for any extension by following the system voice guidance.

By dialing \*61 from an extension and entering the voicemail password for this extension you can follow the voice guidance to check voicemail of your own extension. Or alternatively, you can configure some advanced options for your voicemail box.

### 4.3.4 Voicemail to Email

To send received voicemail messages to the user's email box, you need to configure SMTP support, Email format and specify email addresses for the extension users.

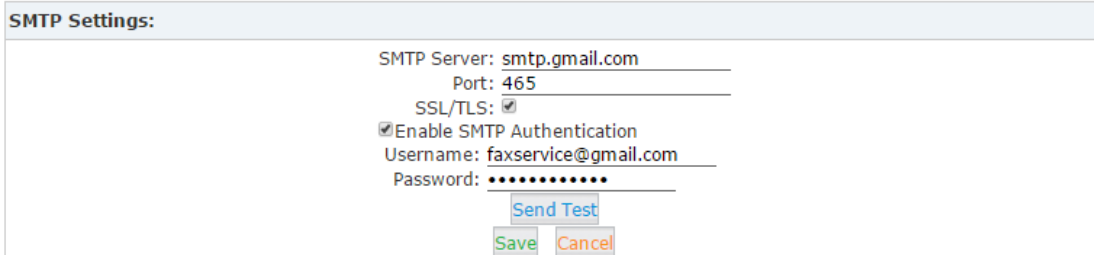
#### Step1:

#### SMTP Settings

Navigate to web menu: *Advanced->SMTP Settings*.

Define an email account to be used by the system which will send emails with voicemail messages attached to the extension users' email boxes.

SMTP Settings



SMTP Settings:

SMTP Server:

Port:

SSL/TLS:

Enable SMTP Authentication

Username:

Password:

- **SMTP Server:** SMTP server domain, for example: smtp.gmail.com, smtp.tom.com.
- **Port:** Default SMTP service port is 25, but if you are using SSL/TLS then please use

port 465.

- **SSL/TLS:** Encrypts a communication channel between the Coovox IPPBX system and the SMTP server.
- **Enable SMTP Authentication:** If your SMTP server requires authentication then please enable this option and configure the following.
- **Username:** The email account.
- **Password:** The password for this email account.
- **Send Test:** Click "Send Test" to send a test email to see if SMTP is working correctly. If it is working then you'll receive an email sent by the IPPBX system.

## Step 2:

### Email Settings

Navigate to web menu: *Advanced->Voicemail->Email Settings.*

On this page you can define the email content that will be sent to the extension users' email boxes.

Email Settings

General Email Settings

### Template for Voicemail Emails

Attach voicemail to email

Sender Name IP Phone System

From faxservice@gmail.com

Subject New Voicemail from \${VM\_CALLERID}

Message Hello \${VM\_NAME}, you received a message lasting \${VM\_DUR} at \${VM\_DATE} from, (\${VM\_CALLERID}).

Save Cancel

**Template Variables:**  
\${VM\_NAME} : Recipient's first name and last name  
\${VM\_DUR} : The duration of the voicemail message  
\${VM\_MAILBOX} : The recipient's extension  
\${VM\_CALLERID} : The Caller ID of the person who left the message  
\${VM\_MSGNUM} : The message number in your mailbox  
\${VM\_DATE} : The date and time the message was left

- **Attach voicemail to email:** If enabled, the system will send any voice message files received to the extension users' email box.
- **Sender Name:** Alias for the SMTP email account.
- **From:** The email account from SMTP settings.
- **Subject:** The subject of the email sent by Coovox IPPBX system.
- **Message:** The content of the email, describes the details of the voicemail message received.
- **Template Variables:** These variables can be used to acquire details of the voicemail messages, which can then be used in the message field to compose the email content.

### Step3:

#### Email Address

Go to the extension details for the user and specify the email address where messages for this user should be sent.

The screenshot shows a configuration window titled 'Edit' with a close button 'X'. It has two main sections: 'General' and 'Voicemail'.  
**General:**  
 SIP:  IAX2:   
 Name: 401 Extension: 401  
 Password: 123456 Outbound CID:  
 DialPlan: DialPlan1 Analog Phone: None  
**Voicemail:**  
 Enable:  Password: 1234  
 Delete VMail:  Email(Fax/Voicemail): example@gmail.com

Once these 3 configuration steps are complete, if user extension 401 receives a new voicemail message then the IPPBX system will send this voicemail message to [example@gmail.com](mailto:example@gmail.com).

#### 4.3.5 Playback Voicemail from Web GUI

An extension user can login to the web interface with their extension number and voicemail password if "Web Manager" option is enabled on their extensions.

Navigate to *Voicemail List* page.

Voicemail

Field: New  Field: New

<input type="checkbox"/>	Caller ID	Date	Duration(sec)	Options
<input type="checkbox"/>	1 "403" <403>	Sat Jan 2 13:47:31 2010	15	<input type="button" value="Play"/> <input type="button" value="Delete"/>

Here on this page you can see all newly received voice messages displayed.

By clicking "Play" button you will be presented with a dialog box that gives you two options to playback this message.

The screenshot shows a dialog box titled 'Play' with a close button 'X'. It contains:  
 Type 1:   
 Type 2: Extension used for playing: 401  
 Buttons:

By clicking button you can playback this message directly from the web interface. By selecting an extension number and clicking on the "Play" button you can playback this message from the selected extension.

## 4.4 Conference

Conferences allow two or more callers to be joined together so that all parties on the call can hear one another. Conferences are also referred as Conference Bridges or Conference Rooms.

On CooVox V2 IPPBX system, you can create up to 20 conference rooms. There are 3 default conference rooms preconfigured for you.

### 4.4.1 Static Conference

Navigate to web menu *Advanced->Conference*. You can click "New Conference" button to add a new conference room or click "Edit" button on the existing conference room to change the properties.

Edit		X
<b>Conference Number</b>		
Room Extension:	900	
<b>Conference Password</b>		
Guest Password:	1234	
Administrator Password:	2345	
<b>Conference Options</b>		
Conference DialPlan	Internal	▼
<input type="checkbox"/>	Play hold music for first caller	
<input type="checkbox"/>	Enable caller menu	
<input type="checkbox"/>	Announce callers	
<input type="checkbox"/>	Record conference	
<input type="checkbox"/>	Quiet Mode	
<input type="checkbox"/>	Close the conference when last administrator exits	
<input type="checkbox"/>	Leader Wait	
Save		Cancel

#### Conference number

- **Room Extension:** Call this extension number to enter the conference room.

#### Conference Password

- **Guest Password:** If callers use this password to enter the conference then they are ordinary participants.
- **Administrator Password:** If callers use this password to enter the conference then they are administrators and have advanced conference menu features such as inviting people to participate in the conference.

#### Conference Options

- **Conference DialPlan:** Conference admin can use this dialplan to invite other participants.

- **Play hold music for first caller:** Plays the hold music for the first participant in the conference until another participant enters the conference.
- **Enable caller menu:** Check this option to allow the conference admin to access the conference menu by pressing "\*" on the phone.
- **Announce Callers:** Announce all the participants in the room when a new participant enters the conference room.
- **Record Conference:** Record this conference(Recording format is wav). The recorded conference can be searched within *Report->Record List->Conference* page. Please see [chapter 6.3.2](#).
- **Quiet Mode:** If this option is checked then the system will not give any announcement when participants enter or leave the conference.
- **Close the conference when last administrator exits:** If this option is checked then the conference will be terminated when the last administrator exits.
- **Leader Wait:** Wait until the conference leader(administrator) enters the conference before starting the conference.

#### 4.4.2 Dynamic Conference

CooVox IPPBX system allows you to press a key sequence(feature code) to create a conference during a live call.

Please navigate to web menu *Advanced->Feature Codes*. You can see the feature codes available for conference feature.

##### Conferences

Invite Participant:	0
Create Conference:	*0
Return to conference with participant:	**
Return to conference without participant:	*#

- **Invite Participant:** When in a static conference room or a dynamic conference room, if the conference administrator presses 0 they will get a dial tone to invite others to participate in this conference.
- **Create Conference:** During a live call the extension user can press \*0 to create a dynamic conference room. The other side will automatically enter the conference as an ordinary participant while the extension user who created this conference will be requested to enter the conference password to enter.
- **Return to conference with participant:** While using the conference menu to invite other people, you can dial \*\* to return to the conference with invited party.
- **Return to conference without participant:** If the invited party doesn't want to participate in the conference you can press \*# to return to the conference without the invited party.

##### Notice:

*After a dynamic conference is created, in reality you have entered a static conference room (by default 900 is the first available conference room). You are able to use conference admin menu to invite others to the conference also others can dial 900 to enter this conference.*

## 4.5 Music Settings

Music Settings, or Music On Hold(MOH) as it is more commonly known on an IPPBX system allows audio files (such as WAV or MP3 files) to be uploaded to the IPPBX system and played back when a caller is placed on hold or is waiting in a queue.

Navigate to web menu *Advanced->Music Settings*.

Music Settings

Music Settings Music Management

**Music On Hold Reference**

Music: Music 1 ▾

**Music On Ringback Reference**

Music: Music 2 ▾

**Music On Queue Reference**

Music: Music 3 ▾

Save Cancel

- **Music On Hold Reference:** Audio files in this selected folder will play to the party which is on hold.
- **Music On Ringback Reference:** Audio files in this folder will be played instead of playing ringback tone to the caller.
- **Music On Queue Reference:** Audio files in this folder will be played when the caller is waiting in a call queue.

There are 10 folders for music files, by default the first 3 folders are preloaded with music files which you may wish to choose. However, if you want to upload your own audio files please click "Music Management" tab.

Music Management

Music Settings Music Management

**Music Management**

Select Music Directory: Music 1 ▾ Load

Files: ▾ Delete

**Upload Music File**

Select Music Directory: Music 1 ▾

Note: The sound file must be mp3, wav(16bit/8000Hz/Mono), gsm, ulaw or alaw!  
The size is limited in 15MB!

Please choose file to upload: Choose File No file chosen

Upload

In the Music Management section, you can select a music folder and click "Load" button to check which audio files are inside this folder. By clicking "Delete" button you can delete the existing audio files.

In the Upload Music File section, you can select a music folder and browse your PC file system to select your preferred audio file and click “Upload” button to upload the audio file. If there are more than one audio file in the same music folder, they will be played at random.

**Notice:**

*CooVox IPPBX system can adopt MP3, wav(16bit, 8000Hz, mono), gsm, ulaw and alaw audio file format.*

## 4.6 DISA

Direct inward system access(DISA) allows an outside caller to dial directly into the PBX system and access the system's features and facilities remotely.

This is useful if you want people to be able to for example take advantage of the low rate for international calls that you have available on your system, or to allow outside callers to be able to use the paging or intercom features of the system. Always protect this feature with strong password/passwords, the passwords need to be set on *Advanced->Pin Sets* page which will be introduced in [Chapter 4.13](#).

Navigate to web menu *Advanced->DISA*. Click on “New DISA” button to create a new DISA call target.

**New DISA** X

Name:

PIN Set:  Without PIN

Record in CDR:

Response Timeout(sec):

Digit Timeout(sec):

Extension for this DISA(Optional):

**Allow Outbound Route**

Select DialPlan

- **Name:** Alias of the DISA call target.
- **PIN Set:** A set of pin codes used to authorize all callers using the system features and facilities.
- **Without PIN:** If enabled, callers will not be required to enter any pin code to be able to use the system features (Not recommended).
- **Record in CDR:** The pin code that is used will be stored into call logs and can therefore be traced on *Report->Call Logs* page.
- **Response Timeout(sec):**The maximum waiting duration before hanging up if the dialed number is incomplete or invalid. Defaulted 10 seconds
- **Digit Timeout(sec):**The maximum interval time between digits when typing extension number. Defaulted 5 seconds.



- **Extension for this DISA(Optional)**: If you want to access DISA by dialing an extension, you can define an extension number for this DISA.
- **Select DialPlan**: Select a dial plan for this DISA so callers will be able to make outbound phone calls using the trunks on the IPPBX system.

**Notice:**

After a new DISA is created, it can be included in the inbound control section as a call destination. But this is not recommended as it is not safe because all callers can possibly access DISA functionality. A better option is to configure DOD settings ([Chapter 3.3.6](#)) for the numbers which you want to be able to access DISA.

## 4.7 Follow Me

The Follow Me feature allows you to set a list of numbers that you may possibly be contacted on. Therefore, if someone calls your extension and you are not available then follow me will work through the list calling each of the numbers in turn until you are contacted or the list is exhausted.

To configure follow me, navigate to web menu *Advanced->Follow Me*. Click on “[New Follow Me](#)” to configure follow me for an extension.

The screenshot shows a web-based configuration window titled "New Follow Me". It has a close button in the top right corner. The "Extension:" field is a dropdown menu currently showing "401 (401)". Below it, the "Ring lasting for" field is set to "20" seconds. The "Follow Me List:" is a text area containing three lines of text: "402,20", "913880424687,20", and "985337096,20". At the bottom of the window are two buttons: "Save" and "Cancel".

- **Extension**: Select the extension number which will be configured with follow me.
- **Ring lasting for 20 seconds**: Define how long to ring the extension before the call is forwarded out. By default, this is 20 seconds.
- **Follow Me List**: The list of numbers to forward the calls to. Each line is written with the format “number,time”, “number” is one of the number to forward the calls to, “time” defines how long to ring this number. They are separated with a comma without space. Numbers are called in sequence.

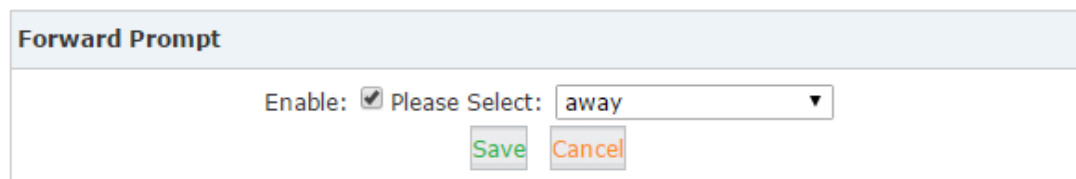
## 4.8 Call Forward

### 4.8.1 Configure from the Web

This feature allows calls to an extension to be automatically forwarded to a specific internal extension or external phone number.

Before configuring call forward you can enable the IPPBX system to play a voice prompt before the call is forwarded. This voice prompts can be recorded or uploaded from the *Inbound Control->IVR Prompts* page.

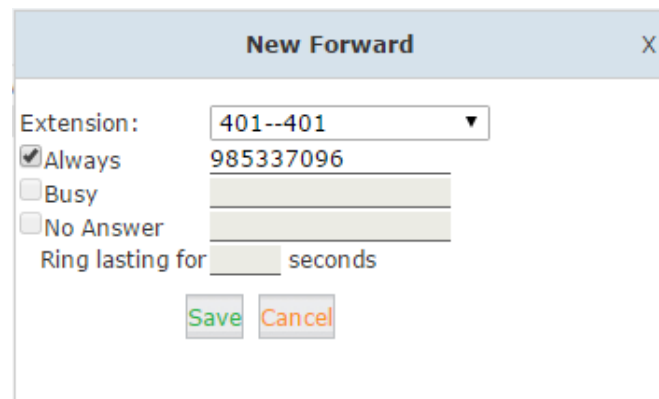
Once the voice prompt file is ready you can navigate to web menu *Advanced->Call Forward* and enable the system to play back the voice prompt before the incoming call is forwarded.



**Forward Prompt**

Enable:  Please Select:

After the voice prompt is set, click "New Forward" button to set call forward for an extension.



**New Forward** X

Extension:

Always

Busy

No Answer

Ring lasting for  seconds

- **Always:** Unconditionally forward the incoming calls.
- **Busy:** Forward the incoming calls only if the extension is busy.
- **No Answer:** Forward the incoming call only if the extension didn't answer.
- **Ring lasting for \_\_\_\_ seconds:** Only configurable for "No Answer" option. It defines how long to ring the extension before forwarding if the extension didn't answer.

**Notice:**

1. If you are forwarding a call to an external phone number then please ensure that you add a prefix in front of the number if your system requires a prefix to dial out.
2. The forward condition "Always" is mutually exclusive to "Busy" and "No Answer".

#### 4.8.2 Configure from the Phone

Navigate to web menu *Advanced->Feature Codes*.

You'll see feature codes for call forward as follows:

##### Call Forward

Enable Forward All Calls:	<u>*71</u>
Disable Forward All Calls:	<u>*071</u>
Enable Forward on Busy:	<u>*72</u>
Disable Forward on Busy:	<u>*072</u>
Enable Forward on No Answer:	<u>*73</u>
Disable Forward on No Answer:	<u>*073</u>

With these feature codes, you can activate or deactivate call forward directly from your phones without configuration on the Web GUI.

For example, a Coovox IPPBX requires prefix 9 to call outbound, and the number you want to forward the calls to is 85337096.

- Activate always call forward: Dial \*71985337096, press 1 to confirm.
- Deactivate always call forward: Dial \*071.
- Activate call forward on busy: Dial \*72985337096, press 1 to confirm.
- Deactivate call forward on busy: Dial \*072.
- Activate call forward no answer: Dial \*73985337096, press 1 to confirm.
- Deactivate call forward no answer: Dial \*073.

## 4.9 Call Transfer

Call Transfer is used to transfer a call in progress to some other destination. There are two types of call transfer.

- **Attended call transfer** - Where the call is placed on hold, a call is placed to another party, and a conversation can take place privately before the caller on hold is connected to the new destination. It is also referred to as "Supervised Call Transfer".
- **Blind call transfer** - Where the call is transferred to the other destinations without intervention (the other destination could ring out and may not be answered for instance).

Navigate to web menu *Advanced->Feature Codes*. You'll see the feature code for call transfer as below:

### Transfer

Blind Transfer: #  
Attended Transfer: \*2  
Disconnect Call: \*  
Timeout for answer on attended transfer(sec): 15

- **Blind Transfer:** In a live call, an extension user can press # key and the IPPBX system prompts "Transfer", you then enter the number to transfer to, this call will be transferred instantly and the user can hangup. If the transferred number doesn't answer this call then it will ring back to the extension user.
- **Attended Transfer:** In a live call, extension user can press \*2 and the IPPBX system prompts "Transfer", you then enter the number to transfer to, after someone answers your call, you can introduce this call and hangup at which point the call is transferred.
- **Disconnect Call:** In an attended transfer if the other side doesn't want to take the call to be transferred, you can press \* to disconnect with them and get back to the caller.
- **Timeout for answer on attended transfer(sec):** In an attended transfer, if the third party rang for 15 seconds without answering, the extension user will go back to the caller and the transfer is terminated.

## 4.10 One Number Stations

One Number Stations is an innovative IPPBX feature unique to Zycoco IPPBX. With one number stations feature, you can have the same extension number in several different locations.

One number stations feature can put several extension numbers in the same "group", a main number can be selected from the members and when an incoming call is made to the main number, it will ring all the member extensions including the main number. Any extension with the group calling other extensions will display only the main number.

Navigate to web menu *Advanced->One Number Stations*. Click "New One Number Stations" button to create a one number stations group.

The screenshot shows a web interface titled "New One Number Stations". It features two vertical lists of extension numbers. The left list, labeled "ONS Group Members", contains 407, 408, and 409. The right list, labeled "Extensions", contains 403, 404, 405, 406, 410, 411, 412, and 413. Between the lists are two arrow buttons: a left-pointing arrow and a right-pointing arrow. Below the lists, there is a "Main Extension" dropdown menu currently showing "407" and a "Ring lasting for" input field with the value "20". At the bottom of the form are "Save" and "Cancel" buttons.

Select the extensions from the "Extensions" column to the "ONS Group Members" column. In the "Main Extension" dropdown list select an extension to be the main extension number. Next click "Save" and you'll have a new one number stations group.

In this example, no matter whether 407, 408 or 409 makes a call, other extensions only see the calling number as extension 407, while any calls made to 407 will result in all 3 extensions ringing.

As you can see on this page there's a feature code Switch Station available.

The screenshot shows a configuration field for "Switch Station". It consists of a text input box containing the asterisk code "\*1", followed by "Save" and "Cancel" buttons.

This feature code is used to switch extension during a phone call. For example, if an inbound call called extension 407 and the one number stations member 408 answered this call, you can press \*1 from extension 407 or 409 to switch this live call to 407 or 409, then 408 will be disconnected.

## 4.11 Paging and Intercom

The Paging and Intercom feature allows you to use your phone system as an intercom system, provided that your endpoints (phone devices) support this functionality. The Paging and Intercom feature allows you to define a number (just like an extension or Ring Group number) that will simultaneously page a group of devices. For example, in a small office, you might define a paging group that allows any user to dial 699, allowing them to page the entire office. You can also use the feature code \*50/\*51 to page/intercom a single extension, by dialing \*50/\*51 followed by the extension number.

Navigate to web menu *Advanced->Paging and Intercom*. Click "New Paging and Intercom" button to add a new paging group.

The screenshot shows a 'New' dialog box with the following fields and controls:

- Paging Extension:** 660
- Description:** managers
- Paging Group Members:** 401(SIP) 401, 402(SIP) 402, 403(SIP) 402, 404(SIP) 404, 405(SIP) 405
- Device List:** 406(SIP) 406, 407(SIP) 407, 408(SIP) 408, 409(SIP) 409, 410(SIP) 410, 411(SIP) 411, 412(SIP) 412, 412(IAX2) 412
- Duplex:**
- Buttons:** Save, Cancel

- **Paging Extension:** The extension number for this paging group, by calling this extension number you can reach the group members.
- **Description:** Description of this paging group.
- **Duplex:** If enabled, the group members can talk back to the caller.

By calling the paging extension number, all group member phones will auto answer in speaker mode (requires that the IP phones support auto answer feature), the caller can now make a brief announcement to the group members.

## 4.12 Web Extensions

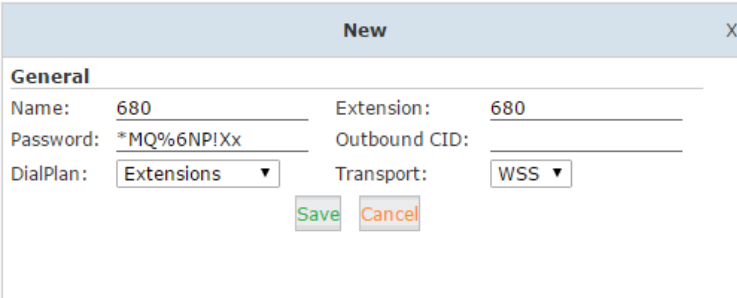
Web Extension is a new feature that makes use of WebRTC technology. You can use any web browser that supports WebRTC to register an extension number to your CooVox V2 IPPBX system without any plugins.

To register the first Web extensions please follow the steps below:

### Step 1:

#### Create a Web Extension

To create a web extension, navigate to web menu *Advanced->Web Extensions*. Click on "New User" button to add a new UAE web extension.



General			
Name:	680	Extension:	680
Password:	*MQ%6NP!Xx	Outbound CID:	
DialPlan:	Extensions	Transport:	WSS

- **Name:** Username of this web extension.
- **Extension:** Extension number of this web extension.
- **Password:** Password for registration of this web extension.
- **Outbound CID:** Only works if the call was placed out through VoIP trunks.
- **DialPlan:** Defines which type of numbers the web extension can dial.
- **Transport:** WS or WSS.
- **WS:** WS (WebSocket) Protocol which is an independent TCP-based protocol providing full-duplex communication channels over a single TCP connection. The WebSocket protocol was standardized by the IETF as RFC 6455 in 2011, and the WebSocket API in Web IDL is being standardized by the W3C.
- **WSS:** WSS (WebSockets over SSL/TLS), like HTTPS, WSS is encrypted and we strongly recommend the secure wss:// protocol over the insecure ws:// transport. A variety of attacks against WebSockets are almost impossible if the transport is secured.

### Step 2:

#### Upgrade Web extension patch

As you can see, web extensions use different protocols for signaling and media (WS/WSS) and they are not ordinary SIP/IAX2 extension that can use IP phones or softphones to register so must be treated differently.

Download WebRTC patch from the links below:

U20V2: [http://zycoco.com/html/U20\\_V2.html](http://zycoco.com/html/U20_V2.html)

U50V2: [http://zycoco.com/html/U50\\_V2.html](http://zycoco.com/html/U50_V2.html)

### Step 3:

#### Register a Web Extension

After completing the upgrade process (see [chapter 8.6](#)) you can access the WebRTC extension register interface. Open your web browser and enter URL <https://192.168.1.254:9999/webrtc> (192.168.1.254 should be your IPPBX IP address) you will see the web extension register interface. Please complete the register credentials as below:

Name	i.e. Homer Simpson	?
John Doe		
SIP URI	i.e. sip:homer@your-domain.com	?
6800@192.168.1.254		
SIP password		?
.....		
WS URI	i.e. wss://your-domain.com:8089/ws	?
wss://192.168.1.254:8089/ws		

[advanced settings](#)

Next, press Enter and the web extension will be registered and is ready for phone calls just like any other standard extension.

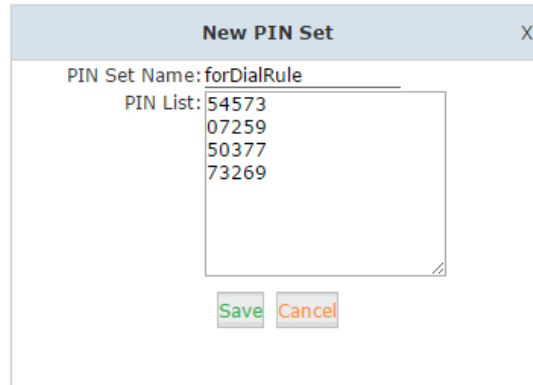
WebRTC can even be adapted to the enterprise website which can help an enterprise serve their customers with direct voice communication via their website. For more advanced WebRTC settings please refer to the WebRTC manual.

#### 4.13 Pin Sets

Pin sets can be used to secure your IPPBX system phone services and in particular for outbound dial rules and DISA.

Navigate to web menu *Advanced->PIN Sets*. Click on "New PIN Set" button to create a collection of PIN codes.





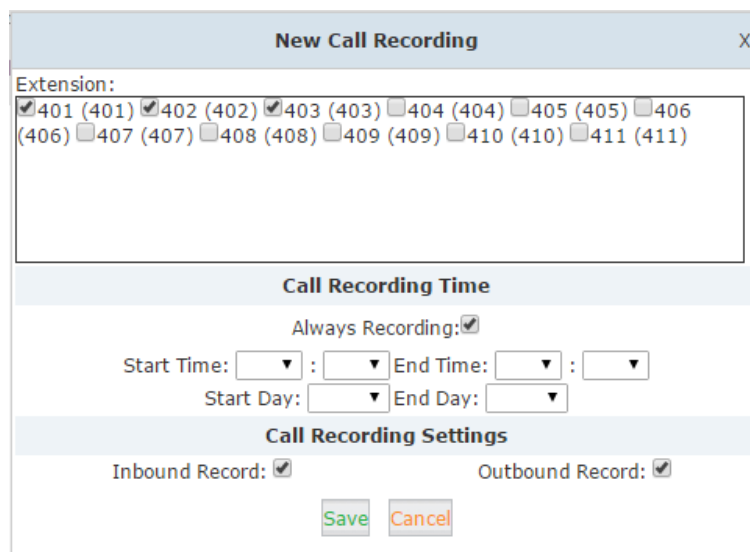
Each line is a PIN code, press Enter to add the next PIN code without any symbols.

## 4.14 Call Recording

CooVox IPPBX system has built-in ability to record calls. No additional software is required for recording calls. When CooVox IPPBX system records a call, both sides of the call are recorded and written out to a file for playback on a computer. Call recording can be used to ensure call quality, or to keep calls for later review. CooVox IPPBX provides the ability to record all of the calls, or to selectively record calls.

### 4.14.1 Record All Calls

Navigate to web menu *Advanced->Call Recording*. Click “[New Call Recording](#)” to activate call recording for the extensions you want calls to be recorded.



- **Extension:** Select the extensions which you want their calls to be recorded.
- **Always Recording:** If enabled, all calls from the above selected extensions will be recorded regardless when the calls were made and received.

- **Start Time, End Time, Start Day, End Day:** If Always Recording is unnecessary then you can specify which time durations in a week to record all calls from the above selected extensions.
- **Inbound Record:** Enable to record all inbound calls.
- **Outbound Record:** Enable to record all outbound calls.

The recordings can be searched on *Report->Record List->Call Recording* page. Please see [chapter 6.3.1.](#)

#### 4.14.2 One Touch Recording

One Touch Recording is also known as Record on Demand. It allows users to record phone calls selectively.

Navigate to web menu *Advanced->Feature Code*. Here on this page you can see the one touch recording feature code as below:

**One Touch Recording**  
One Touch Recording: \*1 \_\_\_\_\_

In a live call conversation, an extension user can use feature code \*1 to record this call. With this feature, you don't have to configure recording all calls for the extensions which may cause heavy system resource use if some call recordings are not required.

The one touch recordings can be searched from *Report->Record List->One Touch Recording* page. Please see [chapter 6.3.3.](#)

#### 4.15 Smart DID

CooVox IPPBX system has the ability to route an inbound call directly to an extension if the extension had previously tried to call the number but the call was unanswered. It is convenient for the called party to make a call back and be directly routed to the extension that called them without going through the IVR menu or reception desk.

Navigate to web menu *Advanced->Smart DID*. Tick the "Enable" checkbox to enable Smart DID functionality.

Smart DID

**Smart DID**

Enable:

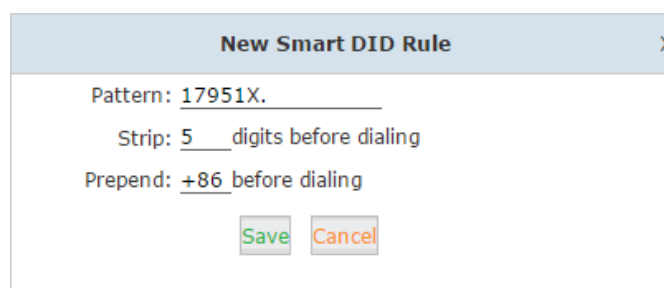
Save
Cancel

Smart DID Rules List		<a href="#">New Smart DID Rule</a>	
Pattern	Strip	Prepend	Options
1	X.		<span style="border: 1px solid #ccc; padding: 2px 5px;">Edit</span> <span style="border: 1px solid #ccc; padding: 2px 5px; margin-left: 5px;">Delete</span>

There is a default Smart DID rule which enables all outbound calls to be monitored by the

Smart DID feature. If the call is not answered by the called party, then the called number will be stored into the Asterisk database with the extension number which made this call. If the called party does make a callback to the IPPBX system then the call can automatically be directed to the extension number.

If you don't want all outbound calls monitored by Smart DID, you can modify the existing rule or click "[New Smart DID Rule](#)" to add your custom rule/rules. An example of this is detailed below:



The screenshot shows a dialog box titled "New Smart DID Rule" with a close button (X) in the top right corner. The dialog contains three input fields: "Pattern: 17951X.", "Strip: 5 digits before dialing", and "Prepend: +86 before dialing". Below these fields are two buttons: "Save" (green) and "Cancel" (orange).

- **Pattern:** Defines the number format which would be dialed.
- **Strip:** Remove some digits from the front of the dialed number.
- **Prepend:** Prepend some digits in front of the dialed number after manipulated by the "Strip" option.

The numbers to be dialed will start with prefix 17951 and if they call back, the expected numbers will have +86 in front of them instead of the 5-digit prefix 17951. In such a situation, the outbound and inbound numbers are not the same, you'll need the "Strip" and "Prepend" options to manipulate the dialed numbers to make sure it can match the "same" number when it calls back. If the numbers to be called and the numbers to be received are the same, then you don't have to configure these 2 options. Alternatively, you can configure only one of these 2 options, it will all depend on your actual requirements.

For example, the extension user 401 wishes to call 85337096, and the carrier requires a prefix 17951 to ensure the rate is much cheaper. The user will dial 1795185337096 to place this call. If the called party misses this call then the IPPBX system will store this number +8685337096 with extension number 401 into its database. Later on, if the called party tries to call back, the IPPBX system gets +8685337096 as the caller ID and matches this from its database, once successfully matched, this call will be automatically directed to extension 401.

**Notice:**

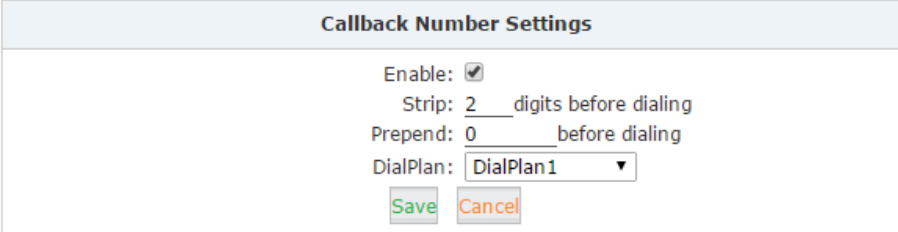
1. The records for Smart DID functionality in the system database will be erased every day at midnight. This means this is a dynamic effective feature and is only designed to handle callbacks made within the same day as the original call.
2. In the "[Pattern](#)" field, patterns can be used in the same way as the patterns used to manipulate dialed number in the dial rules. Please refer to [chapter 3.2.1](#).
3. Due to the mechanism of how Asterisk works, at this time Smart DID only works with VoIP trunks and does not work with FXO or GSM/ WCDMA trunks.

## 4.16 Callback

Callback is to allow a company employee who needs to make a call from their personal phone to call the IPPBX, the IPPBX calls them back and the cost of any future outbound calls are at the companies expense.

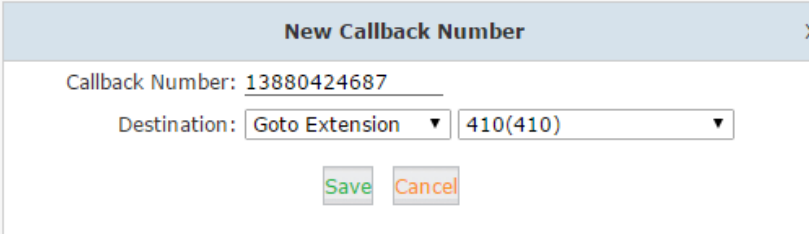
Navigate to web menu *Advanced->Call Back*.

Callback Number Settings



- **Enable:** Check the checkbox to enable call back feature.
- **Strip:** The received caller ID might have some additional digits in front of it and it will not be possible for you to call back directly, you can specify here to remove some digits before calling back.
- **Prepend:** After the number has been manipulated by the "Strip" option, you can use this option to add some extra digits in front before calling back.
- **DialPlan:** Choose an appropriate dial plan to make sure the IPPBX system has the permissions for outbound calling.

Click "New Callback Number" to add a call back number.



- **Callback Number:** The number which will be used to call into the IPPBX system and will be handled by the Callback feature.
- **Destination:** An extension or another call destination which will be used to call the callback number.

In the above example, if the caller 13880424687 called the IPPBX system, IPPBX will disconnect this call and make a call back to this number using extension 410.

In the call back destination field you can even set the destination to a conference, call queue or DISA, so the callers can access these functionalities all at the companies expense.

## 4.17 Phone Book

The phone book on the CooVox IPPBX system is similar to a contact list on a cellular phone. You can add the contacts to the IPPBX system from *Advanced->Phone Book* page. To do this Click "New Contact" to create a new contact record.

X
Create Contact

Name:

Phone Number:

Speed Dial:

- **Name:** Contact name.
- **Phone Number:** Phone number of the contact.
- **Speed Dial:** Speed dial number which can be used to call this contact from another extension.

After contacts have been created they will be listed here on this page.

Phone Book

Phone Book					<input type="button" value="Import"/>	<input type="button" value="Export"/>	<input type="button" value="Delete All"/>	<input type="button" value="Sync LDAP"/>
The prefix of speed dial: <input type="text" value="*99"/>					<input type="button" value="Save"/>	<input type="button" value="Cancel"/>		
Field: <input type="text" value="Name"/>		<input type="text"/>	<input type="button" value="Filter"/>		<input type="button" value="Create Contact"/>		<input type="button" value="Delete Selected"/>	
	Name	Phone Number	Speed Dial	Options				
<input type="checkbox"/>	1 John Doe	73459203	01	<input type="button" value="Call"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		

Here on this page you also have some additional advanced options for the phone book and LDAP configurations.

- **Import:** You can import a contact list from .txt or .csv files.
- **Export:** Export the current contact list as .csv file.
- **Delete All:** Delete all contacts.
- **Sync LDAP:** Synchronize the contacts to an LDAP server.
- **The prefix for speed dial:** Using this feature code with the speed dial code of a contact you can call the contact without knowing their exact number.
- **Filter:** Search contacts by contact name, phone number or speed dial code.
- **Create Contact:** Create a new contact record.
- **Delete Selected:** Delete the selected contacts.
- **Call:** Assign an extension to call this contact.
- **Edit:** Edit the information of this contact.
- **Delete:** Delete this contact.

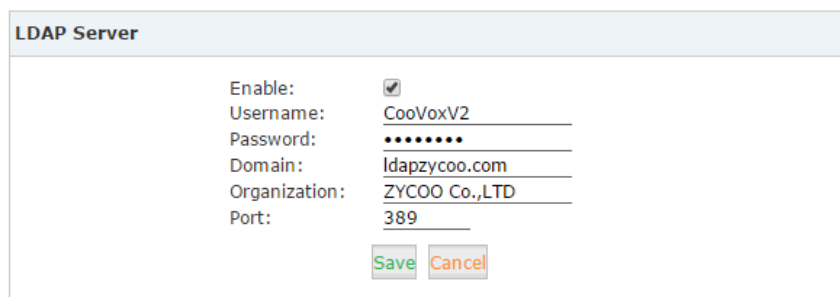
## 4.18 LDAP Server

### 4.18.1 LDAP Server Settings

LDAP(Lightweight Directory Access Protocol) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an IP network. An LDAP server has been embedded into CooVox IP PBX which is mainly used to centralized and manage the phonebook. LDAP server has generated the phonebook based on created extensions by default.

Navigate to web menu *Advanced->LDAP Server*.

LDAP Server

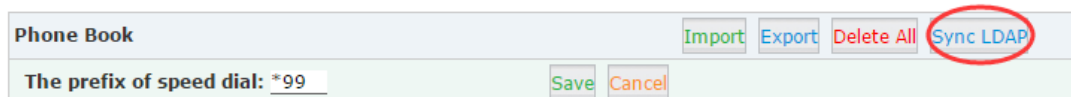


- **Enable:** Enable/Disable LDAP Service.
- **Username:** Define the username of the server administrator (e.g.: manager). This setting will be used on the IP Phone.
- **Password:** Define the password of the server administrator. This setting will be used on the IP Phone.
- **Domain:** Define a domain for the LDAP server (e.g.: ldapdomain.com).This setting will be used on the IP Phone.
- **Organization:** Define an organization to describe the members recorded by LDAP (e.g.: zycoo.ltd). This setting will be used on the IP Phone.
- **Port:** LDAP service port, the default port number is 389.

### 4.18.2 Synchronize Contacts with LDAP Server

Navigate to web menu *Advanced->Phone Book*. Click on the "Sync LDAP" button to synchronize contacts with LDAP server.

Phone Book



### 4.18.3 LDAP Client Settings

After enabling the LDAP server, you need configure a client. For example: ZYCOO D60 IP Phone. Open the web interface of the IP Phone on your browser, navigate to web menu *Phone->Remote Contact->LDAP Settings*.

#### LDAP Settings

LDAP LDAP 1

Display Title	<input type="text" value="ZYCOO"/>	Version	<span style="border: 1px solid black; padding: 2px;">Version 3</span>
Server Address	<input type="text" value="192.168.1.254"/>	Server Port	<input type="text" value="389"/>
Authentication	<span style="border: 1px solid black; padding: 2px;">Simple</span>	Line	<span style="border: 1px solid black; padding: 2px;">Auto</span>
Username	<input type="text" value="cn=CooVoxV2,dc=ldapzy"/>	Password	<input type="password" value="*****"/>
Search Base	<input type="text" value="dc=ldapzycoo.com"/>	Enable Calling Search	<input type="checkbox"/>
Telephone	<input type="text" value="telephoneNumber"/>	Mobile	<input type="text" value="mobile"/>
Other	<input type="text" value="home"/>	Display Name	<input type="text" value="cn"/>

- **LDAP:** Select LDAP server to connect
- **Display Title:** Define a title for the LDAP server, this will be displayed on the phone's screen.
- **Version:** Select the LDAP Version. Default is Version 3.
- **Server Address:** Configure the server domain or IP
- **Server Port:** Configure the server port. Default is 389.
- **Authentication:** Select authentication method, including None, Simple, Digest-MD5 and CRAM-MD5.
- **Line:** Select SIP lines for outbound calls with different LDAP servers
- **Username/Password:** Configure the username and password for the LDAP server. (Please refer to the settings of LDAP server, username format: cn=CooVoxV2, dc=ldapzycoo.com.)
- **Search Base:** Configure the position where the search begins. (This corresponds to the domain setting of LDAP server.)
- **Enable Calling Search:** You can search or update the other party's name in the call if you enable calling search.
- **Telephone/Mobile/Other/Display Name:** Configure the contact information, including display name, telephone number, mobile number and other number.

## 4.19 Feature Codes

Feature codes allow you to set the special codes that users can dial to access various features.

Navigate to web menu *Advanced->Feature Codes*.

### Call Parking

#### Call Parking

Extension to Dial for Parking Calls: 700  
Extension Range to Park Calls: 701-720  
Call Parking Time(sec): 45  
Enable Call Park BLF notification:

A Parking Lot allows anyone who has received a call to park the call on an extension, allowing any other user to access the parked call. Typically, you receive the call, transfer it to extension 700, and then listen as the system tells you where you can pick up the call (usually extension 701). Anyone else on your Coovox IPPBX system can now dial 701 to pick-up the parked call.

A call can be parked for a maximum of 45 seconds as per the definition of "Call Parking Time", if nobody picks this call up then it will go back to the extension which parked it. The "Enable Call Park BLF Notification" enables the parked extensions 701-720 to be monitored by BLF keys, so if there's a call that is parked, the extension user will be able to see it from the BLF panel.

### Pickup Call

#### Pickup Call

Pickup Extension: \*8  
Pickup Specified Extension: \*\*

Pickup call option allows users to pick up calls that are not directed to them by dialing a feature code \*8 or \*\*.

"Pickup Extension: \*8" has already been introduced in [chapter 2.7.1](#), as it's related to the pickup group option of the extension settings.

While "Pickup Specified Extension: \*\*" can help pickup a call on any ringing extension. Dial \*\* followed by the extension number and you can pickup a call on a ringing extension if it is in the same pickup group as your extension or not.

### Transfer

Please see [chapter 4.9](#).

### One Touch Recording

Please see [chapter 6.3.3](#).

### Call Forward

Please see [chapter 4.8.2](#).



## Do Not Disturb

### Do Not Disturb

Enable Do Not Disturb: \*74  
Disable Do Not Disturb: \*074

With the Do Not Disturb(DND) feature enabled, an extension can make outbound phone calls but inbound calls to the extension cannot be made.

If an extension user of the CooVox IPPBX system dials \*74 from their phone, the system will play a beep sound to indicate DND has been activated.

To disable DND, simply dial \*074, another beep sound will play and DND has been deactivated.

## Spy

### Spy

Normal Spy: \*90  
Whisper Spy: \*91  
Barge Spy: \*92

Call Spy allows users to dial the spy feature codes followed by an extension number to listen to the call conversation in real-time.

- **Normal Spy:** For example, extension 410 is talking to someone on the phone, you can dial \*90410 to listen to their conversation, however, neither speaker will be able to hear you.
- **Whisper Spy:** Whisper spy is also known as coaching. For example, a new employee is talking to the customer on the phone, their supervisor can dial \*91 followed by the employee's extension number to listen to their conversation. The supervisor can talk to the new employee only without the customer hearing the conversation.
- **Barge Spy:** Barge spy is similar to an instant 3-way conference call. While an extension user is talking to someone else on the phone, you can dial \*92 followed by their extension number to talk to both of the speakers.

### Notice:

*Before call spy can be used, you have to make sure the extensions to be spied, have the "Allow Being Spied" option enabled on extension settings page.*

## Black List

### Black List

Blacklist a number: \*75  
Remove a number from the blacklist: \*075

Black list feature allows you to create a list of numbers that are not allowed to call in to the CooVox IPPBX system.

Any extension user can dial \*75 and follow the voice prompts to add the numbers to the CooVox IPPBX system black list.

To remove numbers from black list, you can dial \*075.

## Voicemail

Please see [chapter 4.3.2](#).

## Conference

Please see [chapter 4.4.2](#).

## Call Queues

### Call Queues

Pause Queue Member Extension: \*95  
Unpause Queue Member Extension: \*095

Call queue agents can dial \*95 to suspend their extension temporarily, new calls will not be distributed to their extensions, until they dial \*095 to resume.

## Others

### Others

Intercom: \*50  
Paging: \*51  
Directory: \*3

- **Intercom:** The intercom feature code allows you to intercom one extension only. You don't have to create a "Paging and Intercom" group for only one extension if you intend to intercom with only that extension.
- **Paging:** The paging feature code allows you to page one extension only. It's the same as the intercom feature code, the only difference between paging feature code and intercom feature code is by using intercom feature code both sides can talk to each other but using paging feature code, only the caller can talk to the called party.
- **Directory:** Directory is also known as dial by name. Extension users can dial \*3 and follow the voice prompts to enter the first 3 letters of another extension user's first or last name and then make a call to an extension number without knowing its extension number.

## 5. Network Settings

### 5.1 Network Basic

#### 5.1.1 IPv4 Settings

CooVox V2 IPPBX system supports static IP, DHCP and PPPoE for WAN connection, while on LAN port only static IP is supported. If you are configuring your WAN connection as static IP or DHCP, ensure WAN and LAN IP addresses are not in the same network.

#### Static

Navigate to web menu *Network Settings->Network->IPv4 Setting.*

Network

IPv4 Settings	IPv6 Settings	VLAN Settings
---------------	---------------	---------------

**WAN Port Setup**

IP Assign: Static ▾

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

Primary DNS: 8.8.8.8

Alternative DNS: 4.4.4.4

**LAN Port Setup**

IP Address: 192.168.10.254 Subnet Mask: 255.255.255.0

IP AddressV1: 192.168.5.254 Subnet MaskV1: 255.255.255.0

IP AddressV2:                      Subnet MaskV2:

Save Cancel

By default, CooVox IPPBX has been preconfigured with a static IP address of 192.168.1.100 and 192.168.10.100 on WAN and LAN interfaces respectively. If you want to use a static IP then configure required address here and include the address, netmask, gateway and DNS given by your ISP or network administrator.

For the LAN interface, you can specify 2 additional virtual IP addresses. These can be used to access other networks from the LAN port.

#### DHCP

If your Internet connection automatically provides you with a usable IP address, you can select "DHCP" on the WAN interface.

Network

IPv4 Settings	IPv6 Settings	VLAN Settings
<b>WAN Port Setup</b>		
IP Assign: <span style="border: 1px solid black; padding: 2px;">DHCP</span>		
IP Address: <input type="text" value="192.168.1.100"/>		
Subnet Mask: <input type="text" value="255.255.255.0"/>		
Gateway: <input type="text" value="192.168.1.1"/>		
Primary DNS: <input type="text" value="8.8.8.8"/>		
Alternative DNS: <input type="text" value="4.4.4.4"/>		
<b>LAN Port Setup</b>		
IP Address: <input type="text" value="192.168.10.100"/> Subnet Mask: <input type="text" value="255.255.255.0"/>		
<input type="checkbox"/> IP AddressV1: <input type="text"/> Subnet MaskV1: <input type="text"/>		
<input type="checkbox"/> IP AddressV2: <input type="text"/> Subnet MaskV2: <input type="text"/>		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

If DHCP is selected then the WAN interface will not be configurable as it obtains all its network parameters from the DHCP server. DHCP should be used cautiously as all IP extensions register to the IPPBX system through the WAN interface and as DHCP addresses can change and IP extensions need to know the address of the IPPBX at all times. It is best practice to configure WAN address with a Static IP.

### PPPoE

CooVox IPPBX can be connected to the network via ADSL modem by means of Point-to-Point Protocol over Ethernet (PPPoE)dial-up. In such a situation, extensions will subscribe to the IPPBX system through the LAN port, while WAN port can be used for remote extensions.

Network

IPv4 Settings	IPv6 Settings	VLAN Settings
<b>WAN Port Setup</b>		
IP Assign: <span style="border: 1px solid black; padding: 2px;">PPPoE</span>		
Username: <input type="text" value="CD85335361"/>		
Password: <input type="password" value="....."/>		
IP Address: <input type="text" value="192.168.1.100"/>		
Subnet Mask: <input type="text" value="255.255.255.0"/>		
Gateway: <input type="text" value="192.168.1.1"/>		
Primary DNS: <input type="text" value="8.8.8.8"/>		
Alternative DNS: <input type="text" value="4.4.4.4"/>		
<b>LAN Port Setup</b>		
IP Address: <input type="text" value="192.168.10.100"/> Subnet Mask: <input type="text" value="255.255.255.0"/>		
<input type="checkbox"/> IP AddressV1: <input type="text"/> Subnet MaskV1: <input type="text"/>		
<input type="checkbox"/> IP AddressV2: <input type="text"/> Subnet MaskV2: <input type="text"/>		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

If PPPoE is set, you have to specify the username and password given by your ISP and the IPPBX system will dial-up to the ISP and once successfully connected, you will have

Internet access on the WAN interface.

LAN port connects to your local network for internal IP extensions to register. If necessary, you can change LAN IP to suit your local network.

### 5.1.2 IPv6 Settings

IPv6(Internet Protocol Version 6) has been in development for nearly two decades. Now the next-generation protocol is ready to replace IPv4 and assume its place as the back of the Internet.

Today, major Internet service providers (ISPs), home networking equipment manufacturers, and web companies around the world are permanently enabling IPv6 for their products and services. Many organizations, institutions and universities have deployed their own networks on IPv6.

To be able to deliver VoIP calls over IPv6(SIP over IPv6), you can configure Coovox IPPBX system with IPv6 addresses to be able to deploy it in your IPv6 network infrastructure.

To do this, navigate to web menu *Network Settings->Network->IPv6 Settings*.

Network

IPv4 Settings IPv6 Settings VLAN Settings

**WAN Port Setup**

Enable:

IPv6 Address: 2001:db8:4005:80a::200e

Prefix Length: 64

Gateway: 2001:db8:4005:80a::1

Primary DNS: 2001:da8:8000:1:202:120:2:1

Alternative DNS: \_\_\_\_\_

Save Cancel

Specify your IPv6 network profile here and you will be able to connect Coovox IPPBX to your IPv6 network infrastructure.

### 5.1.3 VLAN Settings

With a layer-3 switch you can configure VLAN on Coovox IPPBX system to divide the VoIP and data traffic. Voice VLAN can ensure that phones remain working even when the data network is congested.

To set VLAN, navigate to web menu *Network Settings->Network->VLAN*. As you can see here on this page, you are able to configure 4 VLANs, 2 each for WAN or LAN port.

Network

IPv4 Settings
IPv6 Settings
VLAN Settings

**WAN VLAN 1**

Enable:

VLAN ID: 2

VLAN IP Address: 172.16.10.2

Subnet Mask: 255.255.255.0

**WAN VLAN 2**

Enable:

VLAN ID: 3

VLAN IP Address: 172.16.20.2

Subnet Mask: 255.255.255.0

**LAN VLAN 1**

Enable:

VLAN ID: 4

VLAN IP Address: 172.16.30.2

Subnet Mask: 255.255.255.0

**LAN VLAN 2**

Enable:

VLAN ID: 5

VLAN IP Address: 172.16.40.2

Subnet Mask: 255.255.255.0

Save
Cancel

Ensure VLAN IPs for VLAN1 and VLAN2 of WAN and LAN interfaces are in several different network segments.

## 5.2 Static Routing

Static Routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing protocol to forward traffic. Navigate to web menu *Network Settings->Static Routing*. Click "New Static Routing" to add a new routing record to the system.

**New Static Routing** X

Destination Network: 222.209.4.1

Subnet Mask: 255.255.255.255

Gateway: 192.168.10.1

Save
Cancel

- **Destination:** Set the IP address of destination host or network address. E.g.222.209.4.1, 192.168.10.0.
- **Gateway:** Set the gateway address.

After the new record has been manually created you can see it listed here on this page.

List of Static Routing			New Static Routing	
	Destination Network	Subnet Mask	Gateway	Options
1	222.209.4.1	255.255.255.255	192.168.10.1	<span>Edit</span> <span>Delete</span>

You can click "Edit" button to edit one of the items, or you can delete the item by clicking the "Delete" button.

Click the "Routing Table" tab and you'll see a detailed list of all the system routing rules, including default and custom ones.

Routing Table

Static Routing		Routing Table	
<b>Routing Table:</b>			
Kernel IP routing table			
Destination	Gateway	Genmask	Flags Metric Ref Use Iface
0.0.0.0	192.168.10.1	0.0.0.0	UG 0 0 0 WAN
192.168.1.0	0.0.0.0	255.255.255.0	U 0 0 0 LAN
192.168.7.0	0.0.0.0	255.255.255.0	U 0 0 0 LAN
192.168.10.0	0.0.0.0	255.255.255.0	U 0 0 0 WAN
222.209.4.1	192.168.10.1	255.255.255.255	UGH 0 0 0 WAN

## 5.3 VPN

VPN(Virtual Private Network) is mainly used for setting up long-distance and/or secured network connections. When used on Coovox IPPBX, all phone calls made and received are encrypted so it secures your remote offices/extensions' phone services. Built-in VPN Server on Coovox series is an easy way to set up a secured connection between other Coovox series IPPBXs or IP phones. You don't need to build a dedicated VPN server or buy a VPN router. This is also a workaround to avoid firewall issues when configuring remote VoIP client such as SIP protocol which is notoriously difficult to pass through a firewall due to its random port numbers to establish connection.

Coovox IP PBX supports four varieties of VPN, they are L2TP, PPTP, OpenVPN and IPSec.

### 5.3.1 L2TP VPN

#### L2TP VPN Server

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy. Here on the Coovox IPPBX system we use IPSec to do the encryption.

To configure your L2TP server, navigate to web menu *Network Settings->VPN Server*. Check the radio button of L2TP to configure L2TP VPN server.

VPN Server

VPN Server      OpenVPN Certificate Download

**VPN Server**

L2TP    PPTP    OpenVPN    IPSec

Enable:

Remote Start IP:

Remote End IP:

Local IP:

Primary DNS:

Alternative DNS:

Authentication Method:  chap    pap

Debug:

IPSec:

IPSec Local IP:

IPSec Password:

- **Enable:** Tick the checkbox to enable L2TP VPN server.
- **Remote Start IP, Remote End IP:** L2TP VPN remote network IP range, between start IP and end IP there must be less than 10 available IP addresses.
- **Local IP:** L2TP VPN local server IP address.
- **Primary DNS:** Primary DNS for VPN connection.
- **Alternate DNS:** Alternative DNS for VPN connection.
- **Authentication Method:** Select the authentication method: chap or pap.  
**pap:** Password Authenticate Protocol, PAP works like a standard login procedure; it uses static user name and password to authenticate the remote system.  
**chap:** Challenge Handshake Authentication Protocol  
CHAP takes a more sophisticated and secure approach to authentication by creating a unique challenge phrase (a randomly generated string) for each authentication.
- **Debug:** Tick to enable debug for L2TP VPN connection, debug info will be written into system logs.
- **IPSec:** Enable IPSec encryption for L2TP VPN server.
- **IPSec Local IP:** CooVox WAN IP which can access Internet.
- **IPSec Password:** Define a password for IPSec VPN client to authenticate.

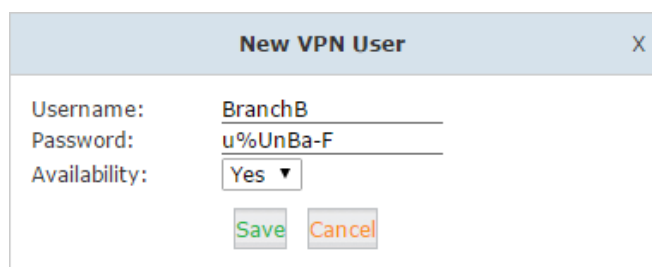
**Notice:**

*If the CooVox IPPBX system is behind NAT, you need to open ports 500, 4500 and 1701 on the router/firewall.*

For the VPN client to connect you'll need to create a VPN user account.

Click "VPN User Management" tab and click "New VPN User" button to add a VPN user account.





**New VPN User** X

Username:

Password:

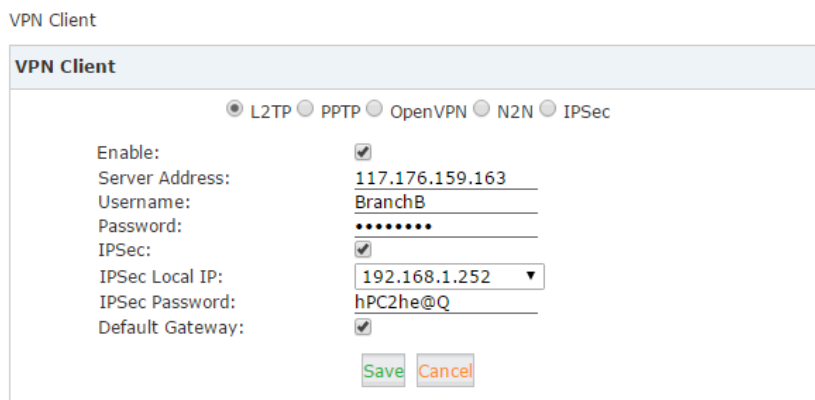
Availability:

Now the L2TP VPN client can connect to the L2TP VPN server.

### L2TP VPN Client

For example, in the branch office you are going to connect another IPPBX system to the head office using L2TP VPN.

Navigate to the web menu *Network Settings->VPN Client*. Check the radio button of L2TP to configure L2TP VPN client.



VPN Client

L2TP  PPTP  OpenVPN  N2N  IPsec

Enable:

Server Address:

Username:

Password:

IPsec:

IPsec Local IP:

IPsec Password:

Default Gateway:

- **Enable:** Tick to enable L2TP VPN client.
- **Server Address:** L2TP server public IP.
- **Username:** L2TP VPN user name given by the VPN server.
- **Password:** L2TP VPN user password given by the VPN server.
- **IPsec:** Enable IPsec support.
- **IPsec Local IP:** CooVox IPPBX WAN IP Address that can access the Internet.
- **IPsec Password:** Set according to the password specified on the server.
- **Default Gateway:** All traffic goes through the L2TP VPN connection.

### Notice:

*If connection is successfully established, the system will display as follows:*

*Status: L2TP client VPN remote IP address 172.16.0.1*

*L2TP client VPN local IP address 172.16.0.x (An IP address between 172.16.0.2 and 172.16.0.9)*

### 5.3.2 PPTP VPN

The Point-to-Point Tunneling Protocol (PPTP) uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The intended use of this protocol is to provide security levels and remote access levels comparable with typical VPN products.

## PPTP VPN Server

To configure your PPTP Server, navigate to web menu *Network Settings->VPN Server*.  
Check the radio button of PPTP to configure PPTP VPN server.

**VPN Server**

L2TP  PPTP  OpenVPN  IPSec

Enable:

Remote IP: 172.16.0.2 - 11

Local IP: 172.16.0.1

Primary DNS: 8.8.8.8

Alternative DNS: 4.4.4.4

Timeout(sec): 20

Authentication Method:  chap  pap  mschap  mschap-v2

Enable mppe128:

Debug:

- **Enable:** Tick the checkbox to enable PPTP VPN server.
- **Remote IP:** PPTP VPN remote network IP range, there must be 10 or less available IP addresses between start IP and end IP.
- **Local IP:** PPTP VPN local server IP address.
- **Primary DNS:** Primary DNS for VPN connection.
- **Alternative DNS:** Secondary DNS for VPN connection.
- **Timeout(sec):** Session timeout for PPTP tunnels.
- **Authentication Method:** Choose method/methods for the authentication of the VPN clients.

**chap:** Challenge Handshake Authentication Protocol

CHAP takes a more sophisticated and secure approach to authentication by creating a unique challenge phrase (a randomly generated string) for each authentication.

**pap:** Password Authenticate Protocol PAP works like a standard login procedure; it uses static user name and password to authenticate the remote system.

**mschap:** MS-CHAP is the Microsoft version of the Challenge-Handshake Authentication Protocol.

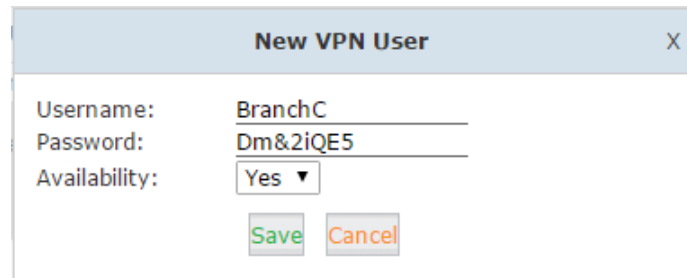
**mschap-v2:** Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2), this provides stronger security for remote access connections.

- **Enable mppe128:** Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol (PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections with 128-bit key.
- **Debug:** Tick to enable debug for PPTP VPN connection, debug information will be written into system logs.

You will need to create a VPN user account for a VPN client to be able to connect to the VPN Server.

To create an account, click "VPN User Management" tab and click "New VPN User" button

to add a VPN user account.



**New VPN User** X

Username: BranchC  
Password: Dm&2iQE5  
Availability: Yes ▾

Save Cancel

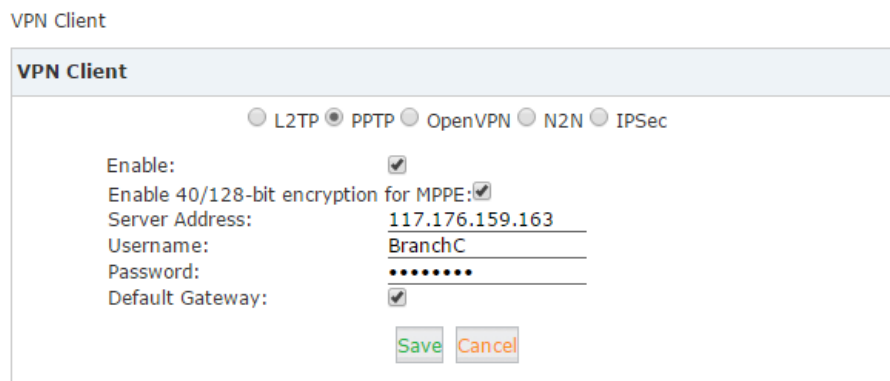
Now the PPTP VPN client will be able to connect to the PPTP VPN server.

**Notice:**

If the CooVox IPPBX system is behind NAT, you will need to open ports 1723 on the router/firewall.

**PPTP VPN Client**

To create your VPN client at the branch office site, open the CooVox IPPBX web GUI and navigate to web menu *Network Settings->VPN Client*. Check the radio button of PPTP to configure PPTP VPN client.



VPN Client

L2TP  PPTP  OpenVPN  N2N  IPSec

Enable:   
Enable 40/128-bit encryption for MPPE:   
Server Address: 117.176.159.163  
Username: BranchC  
Password: ●●●●●●  
Default Gateway:

Save Cancel

- **Enable:** Tick to enable PPTP VPN client.
- **Enable 40/148-bit encryption for MPPE:** Tick to enable 40-bit key (standard) or 128-bit key (strong) MPPE encryption schemes.
- **Server Address:** PPTP VPN server public IP.
- **Username:** PPTP VPN user name given by the VPN server.
- **Password:** PPTP VPN user password given by the VPN server.
- **Default Gateway:** All traffic goes through the L2TP VPN connection.

**Notice:**

*If connection is successfully established the system will display:*

*Status: Local IP address 172.16.0.x (An IP address between 172.16.0.2 and 172.16.0.9)*

*Remote IP address 172.16.0.1*

**5.3.3 OpenVPN**

OpenVPN is an open-source software application that implements virtual private network

(VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls. It was written by James Yonan and is published under the GNU General Public License (GPL).

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

### OpenVPN Server

To create your OpenVPN Server, navigate to web menu *Network Settings->VPN Server*. Check the radio button of OpenVPN to configure your OpenVPN server.

**VPN Server**

L2TP  PPTP  OpenVPN  IPsec

Enable:

Stealth:

Certificate: Done [Create](#) [Delete](#)

Port: 1194

Stealth Port: 443

Protocol: TCP

Device Node: TUN

Cipher: Default

Compress Lzo:

TLS-Server:

Remote Network: 172.16.0.0 / 255.255.255.0

Route: 172.16.0.0 / 255.255.255.0

Client-to-Client:

[Save](#) [Cancel](#)

- **Enable:** Tick to enable OpenVPN server.
- **Stealth:** Certain deep packet inspection firewalls might not allow OpenVPN traffic, stealth SSL tunneling can disguise your OpenVPN traffic under the HTTPS traffic which is often seen as HTTPS traffic by the DPI.
- **Certificate:** Certificate is one of the client authentication methods available in OpenVPN.
- **Port:** OpenVPN service port, the default is 1194.
- **Stealth Port:** Stealth service port, the default is 443.
- **Protocol:** You can choose either UDP or TCP. Stealth requires TCP only so if you have stealth enabled then this option is not configurable and the Server will use TCP by default.
- **Device Node:** TUN or TAP; A TAP device is a virtual Ethernet adapter, while a TUN device is a virtual point-to-point IP link.
- **Cipher:** Cipher (or cypher) is an algorithm for performing encryption or decryption.

- **Compress Lzo:** LZO is an efficient data compression library which is suitable for data de-compression in real-time.
- **TLS-Server:** TLS is an excellent choice for authentication and key exchange mechanism of OpenVPN.
- **Remote Network:** OpenVPN remote network.
- **Route:** The route entries adjust the local routing table, telling it which network to route over the VPN.
- **Client-to-Client:** Client-to-Client can enable intercommunication between clients.

### 5.3.4 IPSec VPN

Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

IPSec can be configured to operate in two different modes, Tunnel and Transport mode. Use of each mode depends on the requirements and implementation of IPSec.

#### IPSec VPN Server (Tunnel mode)

Tunnel mode is used to encrypt all traffic between secure IPSec Gateways, for example if you have two Coovox IPPBX's and each acts as an IPSec Gateway for the hosts/IP phones behind it. The WAN ports will be used to connect both Coovox systems to establish IPSec VPN connection, now all PCs or IP phones on the LAN ports can communicate with each other on both sides via a secure IPSec tunnel.

Navigate to web menu *Network Settings->VPN Server*. Check the IPSec radio button to configure IPSec VPN server.

VPN Server

The screenshot shows a web interface for configuring a VPN Server. At the top, there are two buttons: "VPN Server" (orange) and "OpenVPN Certificate Download" (blue). Below these is a form titled "VPN Server". The form has radio buttons for "L2TP", "PPTP", "OpenVPN", and "IPSec", with "IPSec" selected. The "Enable" checkbox is checked. The "Type" dropdown is set to "Tunnel". The "IPSec Local IP" is set to "117.176.159.163". The "IPSec Password" is "hPC2he@Q". The "IPSec Remote IP 1" is "192.168.1.252". The "IPSec Remote Network 1" is "192.168.200.0 / 255.255.255.0". There are empty fields for "IPSec Remote IP 2", "IPSec Remote Network 2", "IPSec Remote IP 3", and "IPSec Remote Network 3". At the bottom of the form are "Save" and "Cancel" buttons.

- **Enable:** Tick the checkbox to enable IPsec VPN server.
- **Type:** Defaults to Tunnel mode.
- **IPsec Local IP:** CooVox WAN IP, which can be used to connect to the client network.
- **IPsec Password:** Define a password for authentication of the IPsec client.
- **IPsec Remote IP:** IPsec VPN client IP. The client uses this IP to connect to IPsec server.
- **IPsec Remote Network:** Specify the IPsec VPN client LAN network address.

**Notice:**

1. If the CooVox IPPBX is behind NAT, port 500 and 4500 must be open on the router/firewall.
2. If the CooVox IPPBX is connected to the Internet via PPPoE, then IPsec Local IP needs to be the IP address assigned by PPPoE.
3. IPsec VPN server can connect 3 IPsec clients.

**IPsec VPN Client (Tunnel mode)**

On the remote site, open the web GUI of another CooVox IPPBX system and navigate to web menu to configure the VPN Client *Network Settings->VPN Client*.

On the VPN Client page choose IPsec and tick "Enable" option to enable IPsec client.

VPN Client

**VPN Client**

L2TP  PPTP  OpenVPN  N2N  IPsec

Enable:

Type:

IPsec Local IP:

Server Address:

IPsec Password:

IPsec Remote Network:  /

- **Enable:** Tick the checkbox to enable IPsec client.
- **Type:** Ensure this is the same as the IPsec server.
- **IPsec Local IP:** WAN port IP which can connect to the IPsec server.
- **Server Address:** Specify the IPsec server IP.
- **IPsec Password:** Specify the IPsec VPN password defined previously on the server.
- **IPsec Remote Network:** The IPsec VPN server LAN network address.

**Notice:**

1. After saving the configuration, the client will try to connect to the server using the details provided.
2. If connection is successfully established then the system will display "Status: 1 tunnel has been established!!!"
3. If connection fails then the system will display "Status: There's no tunnel! Reconnecting..."

**IPsec VPN server (Transport mode)**

IPsec Transport mode is used for end-to-end communications, NAT traversal is not supported with the transport mode. So if two CooVox IPPBX's are connected via IPsec transport mode, IPsec only encrypts the communication service ports, unlike Tunnel mode

which encrypts the whole LAN subnet.

Navigate to web menu *Network Settings->VPN Server*. Check the IPsec radio button.

VPN Server

VPN Server

L2TP  PPTP  OpenVPN  IPsec

Enable:

Type: Transport

IPSec Local IP: 117.176.159.163

IPSec Password: hPC2he@Q

Save Cancel

- **Enable:** Tick the checkbox to enable IPsec VPN server.
- **Type:** Select Transport mode.
- **IPsec Local IP:** Coovox IPPBX WAN IP.(This is the same as configuring in Tunnel mode)
- **IPsec Password:** Define a password for authentication of the IPsec client.

### IPsec VPN Client(Transport mode)

On the remote site, open the client IPPBX web GUI and navigate to web menu *Network Settings->VPN Client*. Check the radio button of IPsec.

VPN Client

VPN Client

L2TP  PPTP  OpenVPN  N2N  IPsec

Enable:

Type: Transport

IPSec Local IP: 192.168.1.252

Server Address: 117.176.159.163

IPSec Password: hPC2he@Q

Save Cancel

- **Enable:** Tick the checkbox to enable IPsec VPN client.
- **Type:** Ensure this is the same as the IPsec VPN server.
- **IPsec Local IP:** Coovox IPPBX WAN IP which can connect to the IPsec server.
- **Server Address:** IPsec VPN server IP.
- **IPsec Password:** Specify the IPsec VPN password defined previously on the server.

### Notice:

*If a successful connection is established, then the system will display "Status: 2 tunnels have been established!!!". Because the Coovox IPPBX system encrypts all service ports over UDP and TCP protocols, this means there will be 2 tunnels established.*

### 5.3.5 N2N VPN Client

N2N is an open source Layer 2 over Layer 3 VPN application which utilizes a peer-to-peer architecture for network membership and routing.

On CooVox IPPBX system we support N2N VPN client, to configure the N2N VPN client, please navigate to web menu *Network Settings->VPN Client*. Check the radio button of N2N VPN and configure the client info.

VPN Client

**VPN Client**

L2TP  PPTP  OpenVPN  N2N  IPSec

Enable:

Server Address:

Port:

Local IP:

Subnet Mask:

Local Port:

Username:

Password:

- **Enable:** Tick this checkbox to enable N2N VPN client.
- **Server Address:** N2N server(supernode) IP address.
- **Port:** N2N service port number. This is 82 by default.
- **Local IP:** VPN local IP.
- **Subnet Mask:** Netmask of the VPN network.
- **Local Port:** N2N local service port.
- **Username/Password:** Used for the N2N server to authorize the connection.

### 5.4 DHCP Server

DHCP(Dynamic Host Configuration Protocol)is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

With DHCP, computers/IP phones request IP addresses and networking parameters automatically from CooVox IPPBX WAN/LAN port which saves administrators a lot of time when compared with having to configure these settings manually.

#### 5.4.1 DHCP Service

Navigate to web menu *Network Settings->DHCP Server*.



DHCP Server

DHCP Server
DHCP Client List
Static MAC

**DHCP Server Settings**

Enable:

Interface: WAN ▾

Start IP: 192.168.1.101

End IP: 192.168.1.199

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

Primary DNS: 192.168.1.1

Lease Time(min): 1440

TFTP Server:

Save
Cancel

- **Enable:** Enable DHCP service.
- **Interface:** Choose the network port to implement DHCP service.
- **Start IP, End IP:** Specify the DHCP IP address pool.
- **Subnet Mask:** Netmask to be assigned to client devices.
- **Gateway:** Gateway address to be assigned to client devices.
- **Primary DNS:** DNS to be assigned to client devices.
- **Lease Time(min):** Duration for DHCP server to lease an address to a new device. When the lease expires, the DHCP server might assign the IP address to a different device. Default value is 1440 minutes.
- **TFTP Server:** Input the TFTP server address if required which may be used to auto provision your IP phones.

### 5.4.2 DHCP Client List

Navigate to *Network Settings->DHCP Server->DHCP Client List* and you will see a list of all devices receiving their IP address from the Coovox IPPBX system.

DHCP Client List

DHCP Server
DHCP Client List
Static MAC

**DHCP Client List:**

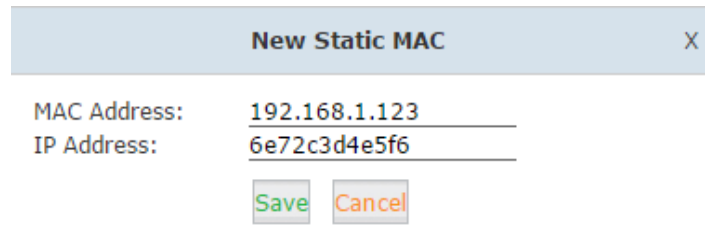
Mac Address	IP Address	Host Name	Expires in
00:0b:82:71:b3:17	192.168.1.157		23:08:17

### 5.4.3 Static Mac

Static MAC is a useful feature which ensures the DHCP service on Coovox IPPBX always assigns the same IP address to a specific computer or IP phone on your LAN. To be more specific, the DHCP service assigns this static IP to a unique MAC address assigned to each NIC on your LAN.

To create a static Mac, navigate to web menu *Network Settings->DHCP Server->Static*

MAC. Click "New Static MAC" to add a record to the CooVox IPPBX system.



The screenshot shows a web-based configuration window titled "New Static MAC". It features two input fields: "MAC Address:" containing the value "192.168.1.123" and "IP Address:" containing the value "6e72c3d4e5f6". Below these fields are two buttons, "Save" and "Cancel". The window has a light blue header and a close button in the top right corner.

In this example, the IP address 192.168.1.123 will always be assigned to the device with MAC address 6E:72:C3:D4:E5:F6, lease time will not apply to this IP Address.

## 5.5 DDNS

Unlike DNS that only works with static IP addresses, DDNS (Dynamic Domain Name Server) is designed to also support dynamic IP addresses, such as those assigned by a DHCP server.

Built-in DDNS feature on CooVox IPPBX system only requires you to sign up with a Dynamic DNS provider, then with the domain name they provide which maps your IP address on the Internet, you can access CooVox IPPBX and also other services within your LAN via the domain name without needing to know your Dynamic public IP Address.

After setting DDNS, CooVox IP PBX phone services can be accessed from remote site via the domain name which your DDNS provider supplied you. Also remote management is possible, even without a static public IP.

CooVox IPPBX system supports the following DDNS service providers:

- <http://dyn.com/>
- <http://www.noip.com/>
- <http://www.zoneedit.com/>
- <http://www.oray.com/>
- <http://www.3322.net>
- <http://freedns.afraid.org/>

Sign up to one of these DDNS service providers' website and subscribe a dynamic domain name. Once you have your account details, navigate to web menu *Network Settings* -> *DDNS Settings*.

#### DDNS Settings

DDNS Settings	
Enable:	<input checked="" type="checkbox"/>
DDNS Server:	<input type="text" value="dyndns.org"/>
Username:	<input type="text" value="zycootech"/>
Password:	<input type="password" value="*****"/>
Domain:	<input type="text" value="zycootech.dyndns.org"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- **Enable:** Tick to enable DDNS service.
- **DDNS Server:** Select the DDNS service provider which you have subscribed to.
- **Username:** Username you subscribed to the service provider.
- **Password:** Password you used to sign up to the service provider.
- **Domain:** Your domain name.

After completing the above, please configure port forwarding on your router/firewall, then you'll be able to remote access CooVox IPPBX services from the internet using this dynamic domain. For example, you can port forward port number 9999 and then you can access the CooVox IPPBX web interface using the URL: <http://zycootech.dyndns.org:9999>.

## 5.6 SNMPv2

Simple Network Management Protocol (SNMP) is an Internet-standard protocol that is widely used in network management systems to monitor network-attached devices for conditions (Alerts) that warrant administrative attention.

#### SNMPv2 Settings

Read Only	
Enable:	<input checked="" type="checkbox"/>
RO Community:	<input type="text" value="public"/>
RO Network:	<input type="text" value="192.168.10.0"/> / <input type="text" value="24"/>

Read and Write	
Enable:	<input checked="" type="checkbox"/>
RW Community:	<input type="text" value="private"/>
RW Network:	<input type="text" value="192.168.1.0"/> / <input type="text" value="24"/>

With the above configurations, the network 192.168.1.0 can read and write(modify) the system configurations through the web interface, while the network 192.168.10.0 can only read but cannot modify anything.

## 5.7 TR069

TR069 (Technical Report 069) is a Broadband Forum (formerly known as DSL Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

To configure TR069, navigate to web menu *Network Settings->TR069*.

TR069 Settings	
Enable:	<input checked="" type="checkbox"/>
CPE to ACS URL:	<input type="text" value="http://192.168.1.69/acs"/>
ACS Authentication Mode:	<input type="text" value="BASIC"/>
ACS Username:	<input type="text" value="user"/>
ACS Password:	<input type="text" value="123456"/>
CPE Inform Interval(sec):	<input type="text" value="42200"/>
ACS to CPE URL:	<input type="text" value="http://192.168.1.78:7547"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- **Enable:** Enable TR069 service
- **CPE to ACS URL:** Input URL to visit ACS, which is used by PBX to connect ACS via CPE WAN management protocol (CWMP)
- **ACS Authentication Mode:** Select ACS Authentication Mode: NONE/ BASIC/ DIGEST
- **ACS Username:** When the PBX sends a request to ACS, ACS will provide username to the authorized PBX.
- **ACS Password:** When the PBX sends a request to ACS, ACS will provide password to the authorized PBX.
- **CPE Inform Interval (sec):** Interval for CPE to connect ACS.
- **ACS to CPE URL:** Input URL to visit CPE. Format: http://IP:port(7547).

## 5.8 Troubleshooting

We have included two tools for troubleshooting network problems and they allow you to check the network reachability, ping and traceroute. With these tools you'll get an outside view of your network response time and network topology, which allows you to track down possible errors more easily.

### 5.8.1 Ping

The ping command is a very common method for troubleshooting the accessibility of devices. It uses a series of Internet Control Message Protocol (ICMP) Echo messages to determine:

- Whether a remote host is active or inactive.
- The round-trip delay in communicating with the host.
- Packet loss.

### Troubleshooting

Ping
Traceroute

Ping 192.168.1.2      Packets: 4      Run Stop

```

PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_req=1 ttl=128 time=0.979 ms
64 bytes from 192.168.1.2: icmp_req=2 ttl=128 time=0.952 ms
64 bytes from 192.168.1.2: icmp_req=3 ttl=128 time=0.870 ms
64 bytes from 192.168.1.2: icmp_req=4 ttl=128 time=0.910 ms

--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.870/0.927/0.979/0.055 ms
    
```

First specify the domain or IP of the host you want to contact and then define how many packets are to be sent, finally click the “Run” button and the command begins to process. You will receive results output from the system indicating the reachability of the destination.

### 5.8.2 Traceroute

The traceroute command is used to discover the routes that packets actually take when traveling to their destination.

Click “Traceroute” tab and specify the domain or IP address that you want to lookup and then click the “Run” button to start the process.

Ping
Traceroute

Traceroute 8.8.8.8      Run Stop

```

traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 38 byte packets
 1 192.168.1.253 (192.168.1.253)  9.090 ms  2.339 ms  1.364 ms
 2 117.176.159.129 (117.176.159.129)  2.953 ms  3.768 ms  3.141 ms
 3 221.182.42.129 (221.182.42.129)  7.828 ms  3.642 ms  3.220 ms
 4 * * *
 5 * 221.183.19.45 (221.183.19.45)  3.036 ms  2.875 ms
 6 221.176.20.137 (221.176.20.137)  42.682 ms  42.717 ms  42.592 ms
 7 221.176.24.2 (221.176.24.2)  89.873 ms  38.681 ms  38.080 ms
 8 221.183.15.14 (221.183.15.14)  202.732 ms  202.97.15.9 (202.97.15.9)
 9 202.97.60.134 (202.97.60.134)  209.421 ms  210.220 ms  207.741 ms
10 * * *
11 * 202.97.60.82 (202.97.60.82)  210.967 ms  210.754 ms
12 202.97.61.118 (202.97.61.118)  209.741 ms  209.814 ms  212.201 ms
13 202.97.62.214 (202.97.62.214)  47.344 ms  43.307 ms  44.187 ms
14 209.85.241.56 (209.85.241.56)  43.452 ms  209.85.241.58 (209.85.241.58)
15 216.239.40.13 (216.239.40.13)  45.787 ms  209.85.142.185 (209.85.142.185)
16 216.239.57.239 (216.239.57.239)  77.555 ms  209.85.253.89 (209.85.253.89)
17 64.233.175.205 (64.233.175.205)  109.890 ms  72.14.237.171 (72.14.237.171)
18 * * *
19 google-public-dns-a.google.com (8.8.8.8)  75.043 ms  86.514 ms  72.94
    
```

After the process has completed the system will notify you that “Trace Complete” and you can view which routes the packets have taken before reaching their final destination.

## 6. Reports

### 6.1 Register Status

On the register status page you are able to check the extension and SIP/IAX2 trunk status intuitively. You can view from which IP an extension is registered and you can also see the connection state, for example how much delay there is between the IPPBX system and the end point.

#### 6.1.1 SIP User Status

Navigate to web menu *Report->Register Status->SIP User Status.*

Register Status [🔗](#)

SIP Users Status		IAX2 Users Status		SIP Trunks Status		IAX2 Trunks Status	
SIP Users Status							
Name	Extension	IP	NAT	ACL	Port	Status	
401	401	N/A	No	No	N/A	Unregistered	
402	402	192.168.7.32	No	No	5060	Registered (4 ms)	
403	403	192.168.7.147	No	No	45290	Registered (5 ms)	
404	404	N/A	No	No	N/A	Unregistered	
405	405	N/A	No	No	N/A	Unregistered	
406	406	N/A	No	No	N/A	Unregistered	
407	407	N/A	No	No	N/A	Unregistered	
408	408	N/A	No	No	N/A	Unregistered	
409	409	192.168.7.147	No	No	39480	Registered (4 ms)	
410	410	N/A	No	No	N/A	Unregistered	
411	411	N/A	No	No	N/A	Unregistered	
John Doe	682	N/A	Yes	No	N/A	Unregistered	

Here on this page you can see the SIP/IAX2 extensions, web extensions and also the register status of trunk users. Only a trunk that is configured as peer mode will be listed here.

#### Status and Description

- **Registered:** Registration success.
- **Unregistered:** Registration failure or unapplied.
- **Unreachable:** Network issue.
- **Timeout:** Register request timeout.

#### 6.1.2 IAX2 User Status

To view IAX2 user status, navigate to web menu *Report->Register Status->IAX2 Users Status.*

Register Status [↗](#)

SIP Users Status		IAX2 Users Status		SIP Trunks Status		IAX2 Trunks Status	
<b>IAX2 Users Status</b>							
Name	Extension	IP	Port	Reachability			
412	412	192.168.7.32	4569	Registered (2 ms)			
413	413	N/A	N/A	Unregistered			

### Status and Description

- **Registered:** Registration success.
- **Unregistered:** Registration failure or unapplied.
- **Unreachable:** Network issue.
- **Timeout:** Register request timeout.

#### 6.1.3 SIP Trunk Status

To view SIP trunk status, navigate to web menu *Report->Register Status->SIP Trunk Status*.

Register Status [↗](#)

SIP Users Status		IAX2 Users Status		SIP Trunks Status		IAX2 Trunks Status	
<b>SIP Trunks Status</b>							
Username	Hostname/IP			Status			
5252742452	gw1.sip.us:5060			Registered			
61921248	183.62.205.209:5060			Registered			

Here you can see all your outbound SIP trunks' status.

### Status and Description

- **Registered:** Successfully registered to the service provider and ready for phone calls.
- **Request Sent:** In this status, it's most probable that the network is totally unreachable to the SIP server. Please make sure network setting on the IPPBX system are correct.
- **Waiting for Authentication:** If "Waiting for Authentication" then most probably the register request has already been received by the server side but cannot authenticate the register request due to incorrect credentials. Please double check your credentials.
- **Failed:** After trying to register within a certain time period without success, you get "Failed" on the trunk status.

#### 6.1.4 IAX2 Trunk Status

To view IAX2 trunk status, navigate to web menu *Report->Register Status->IAX2 Trunk Status*.

Register Status

SIP Users Status	IAX2 Users Status	SIP Trunks Status	IAX2 Trunks Status
------------------	-------------------	-------------------	--------------------

IAX2 Trunks Status		
Username	Hostname/IP	Status
asterisk	192.168.7.146:4569	Registered

Here you can see all of your outbound IAX2 trunks' status.

### Status and Description

- **Registered**: Successfully registered to the service provider and ready for phone calls.
- **Request Sent**: If in this status, it's most probable that the network is totally unreachable to the service provider. Please make sure network setting on the IPPBX system are correct.
- **Waiting for Authentication**: If "Waiting for Authentication" then most probably the register request has already been received by the server side but cannot authenticate the register request due to incorrect credentials. Please double check the credentials again.
- **Failed**: After unsuccessfully trying to register within a certain time period, you will see "Failed" on the trunk status.

## 6.2 FAX List

Navigate to web menu *Report->FAX List*. You can search any fax received by the IPPBX system.

Fax List

Start Date:	Nov ▼	12 ▼	2015 ▼	Field:	Caller ID ▼	<input type="text"/>	<input type="button" value="Filter"/>
End Date:	Dec ▼	12 ▼	2015 ▼				
Caller ID	Destination	Date	File Name	Status			
02037085791	800	12/04/15 13:15	fax000000007.tif	Done			
01085790903	800	11/24/15 20:37	fax000000006.tif	Done			
01085790903	800	11/20/15 16:26	fax000000005.tif	Done			
02082303466	800	11/18/15 16:06	fax000000004.tif	Done			
051786244043	800	11/12/15 09:52	fax000000002.tif	Done			

In the "Start Date" and "End Date" fields specify a time duration, and click "Filter" and you'll be able to view all faxes received during this time period. If you specified a "Caller ID" or "Destination ID" in the "Field" blank then you can get the fax sent/receive by a specific number in this time period.

Faxes can be downloaded to your PC hard drive by clicking the button.



## 6.3 Record List

### 6.3.1 Call Recording

On the web page *Report ->Record List*. You are able to search all recorded call conversations if you have configured the extension to be always recorded.

Call Recording

Call Recording
Conferences
One Touch Recording

Extension:	402 <span style="color: red;">Delete</span>	Field:	Caller ID		
Start Date:	Dec 21 2015	End Date:	Dec 21 2015	<span style="border: 1px solid #ccc; padding: 2px;">Filter</span>	
<b>List of Recording Files</b>			<span style="color: red;">Delete Selected</span>		
<input type="checkbox"/>	Caller ID	Destination ID	Date	Duration(sec)	Options
<input type="checkbox"/>	1 402	403	2015/12/21 12:00:21	40	<span style="background-color: #d9ead3; padding: 2px;">Play</span> <span style="background-color: #d9ead3; padding: 2px;">Delete</span> <span style="color: blue;">⬇</span>
<input type="checkbox"/>	2 402	402	2015/12/21 11:46:40	7	<span style="background-color: #d9ead3; padding: 2px;">Play</span> <span style="background-color: #d9ead3; padding: 2px;">Delete</span> <span style="color: blue;">⬇</span>
<input type="checkbox"/>	3 402	403	2015/12/21 11:46:33	2	<span style="background-color: #d9ead3; padding: 2px;">Play</span> <span style="background-color: #d9ead3; padding: 2px;">Delete</span> <span style="color: blue;">⬇</span>

- **Extension:** Select an extension number to search the recordings of this extension.
- **Delete:** Delete all recordings from the selected extension number.
- **Field:** Filter the recordings by specifying caller ID or destination ID. For example, if you select "Caller ID" and specify number 401, you will get back the recordings of the calls made by extension 401; if you select "Destination ID" and specify number 401, you get back the recordings of the calls which called extension 401.
- **Start Date/End Date:** Search recordings made during this time period.
- **Delete Selected:** Delete the select recording items.
- **Caller ID:** Caller ID of this recorded call.
- **Destination ID:** The number that was called.
- **Date:** Exact time when this call recording began.
- **Duration(sec):** Duration of the recording.
- **Options:** Playback, delete and download options for the recorded files.
- **Play:** You can playback the recordings directly on the web page or playback on a specific phone.

### 6.3.2 Conference

All recorded conferences can be found here on *Report->Record List->Conference* page.

Conferences

Call Recording
Conferences
One Touch Recording

Start Date:	Dec 21 2015	End Date:	Dec 21 2015	<span style="border: 1px solid #ccc; padding: 2px;">Filter</span>
<b>List of Conference Record Files</b>			<span style="color: red;">Delete Selected</span>	
<input type="checkbox"/>	Conference Room	Date	Options	
<input type="checkbox"/>	1 900	2015/12/21 14:52:39	<span style="background-color: #d9ead3; padding: 2px;">Play</span> <span style="background-color: #d9ead3; padding: 2px;">Delete</span> <span style="color: blue;">⬇</span>	

- **Start Date/End Date:** Specify a time duration to search the recorded conferences.

- **Delete Selected:** Delete the selected searched results.
- **Delete All:** Delete all searched results.
- **Conference Room:** The number of the recorded conference.
- **Date:** Exact time when the conference began.
- **Options:** Playback, delete or download the recording file.
- **Play:** Playback the recordings directly on the web page or playback on a specific phone.
- **Delete:** Delete the recorded audio file.

### 6.3.3 One Touch Recording

Call recordings recorded by one touch recording feature code \*1 and can be found on *Report-> Record List->One Touch Recording* page.

One Touch Recording

Call Recording
Conferences
One Touch Recording

Extension:  Delete

Start Date:    End Date:    Filter

Delete Selected

	Caller ID	Destination ID	Date	Options
<input type="checkbox"/>	1 402	403	2015/12/21 14:49:15	<span style="color: green; font-weight: bold;">Play</span> <span style="color: red; font-weight: bold;">Delete</span> <span style="color: blue; font-weight: bold;">⬇</span>

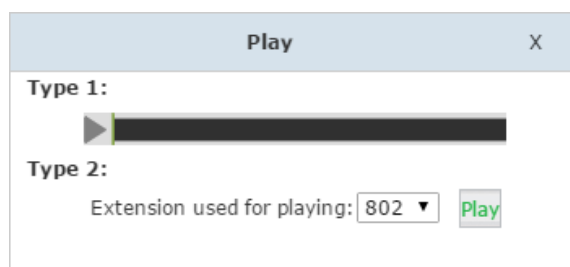
- **Extension:** Extensions that used one touch recording to record calls will be listed here.
- **Delete:** Delete all recordings for the selected extension number.
- **Start Date/End Date:** Search the recordings during this time period.
- **Delete Selected:** Delete the select recording items.
- **Caller ID:** Caller ID of this recorded call.
- **Destination ID:** The number the caller called.
- **Date:** The exact time when this call began.
- **Play:** Playback, delete and download options of the recording files.
- **Delete:** Delete the recorded audio file.


### 6.3.4 Call Recording Playback

On Coovox IPPBX system, there are two ways to playback recordings.

- Playback on the web interface
- Playback on a specific phone

By clicking the "Play" button on a call recording file you'll see a dialog box like below:



With "Type 1", you can click the  button you can playback the recording directly on the web interface.

With "Type 2", you can specify an extension number and click on "Play" and then the extension will ring and you can pickup the call and the recording will play on the phone.

## 6.4 Call Logs

Call logs are also known as CDR(Call Detailed Records), on the call logs page you can check records for any call that went through the IPPBX system.

Navigate to web menu *Report->Call Logs* and by specifying the time duration and/or Caller ID/Destination ID/Account you can find the call records that you require.

Call Logs

Call Start	Caller ID	Destination ID	Account Code	Duration(sec)	Disposition
2015-12-21 16:35:56	402 <402>	013880424687	50377	240	Answered
2015-12-21 16:33:41	402 <402>	013880424687		43	Answered
2015-12-21 16:08:49	402 <402>	785756211		252	Answered
2015-12-21 16:06:00	85337096 <85337096>	402		55	Answered
2015-12-21 14:52:35	404 <404>	conference		2031	Answered
2015-12-21 14:52:49	402 <402>	conference		2014	Answered
2015-12-21 14:53:07	402 <402>	conference		56	Answered
2015-12-21 14:50:02	404 <404>	conference		42	Answered
2015-12-21 14:50:28	402 <402>	conference		12	Answered
2015-12-21 14:49:15	402 <402>	402		22	Answered
2015-12-21 12:00:21	402 <402>	402		40	Answered
2015-12-21 11:46:40	402 <402>	402		7	Answered
2015-12-21 11:46:33	402 <402>	403		2	Answered

Total:13  Per Page Pages: <<  >>

- **Start Date/End Date:** Define the searching time period by "Start Date" and "End Date".
- **Field:** Search criteria.  
  - Caller ID:** Search by the caller number.
  - Destination ID:** Search by the called number.
  - Account Code:** Search within the pin code which was used for outbound dialing.
- **Download:** Download the search results.
- **Delete:** Delete the search results.
- **Call Start:** The exact time when this call began.
- **Caller ID:** The number of the caller.(By clicking on the number you can add this number to the IPPBX system phone book.)

- **Destination ID:** The number which has been called.(By clicking on the number you can add this number to the IPPBX system phone book.)
- **Account Code:** The pin code that was used for outbound dialing.
- **Duration:** The duration of this phone call.
- **Disposition:** How the calls have been handled. Either answered, no answer or failed.

## 6.5 System Logs

These logs are IPPBX journals which store all system activities. They can be used for debug purpose if the system is running into exception. Please do not enable these logs if the system is functioning properly as debug information creates large log files which consume space and also utilize system resources.

In the CooVox IPPBX system, there are 4 kinds of log files.

- **System Log:** System Logs store all system events.
- **PBX Log:** PBX Logs store all Asterisk events.
- **PBX Debug Log:** Asterisk debug logs.
- **Access Log:** Web and SSH access logs.

To enable these logs for the IPPBX system, please navigate to web menu *Report->System Logs*. And enable the logs by ticking the corresponding checkboxes.

System Logs

System Logs	
Enable System Log:	<input checked="" type="checkbox"/>
Enable PBX Log:	<input checked="" type="checkbox"/>
Enable PBX Debug Log:	<input checked="" type="checkbox"/>
Enable Access Log:	<input checked="" type="checkbox"/>

After checking the checkboxes please click "Save" and the log files will be generated.

List of Logs		Download Selected		Delete Selected	
<input type="checkbox"/>	Name	Type	Options		
<input type="checkbox"/>	1 debug20151221.log	Debug Log	Delete	Download	
<input type="checkbox"/>	2 login201512.log	Login Log	Delete	Download	
<input type="checkbox"/>	3 pbx20151221.log	PBX Log	Delete	Download	
<input type="checkbox"/>	4 sys20151221.log	System Log	Delete	Download	

Each day there will be a new log file generated for each of the log types. Enable them only if you are familiar with these logs for troubleshooting purposes.

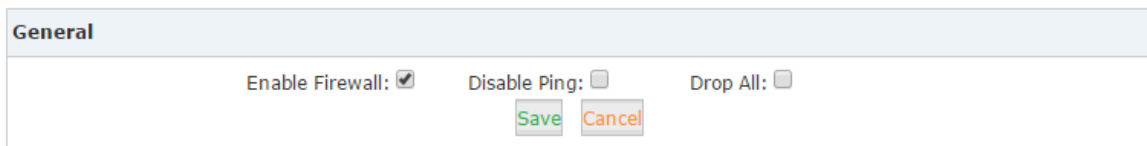
# 7. Security

## 7.1 Firewall

CooVox IPPBX system has been preconfigured with a built-in firewall which prevents your IP phone system from unauthorized access, phone calls and certain other attacks.

To manage the firewall, navigate to web menu *Security->Firewall*.

### General

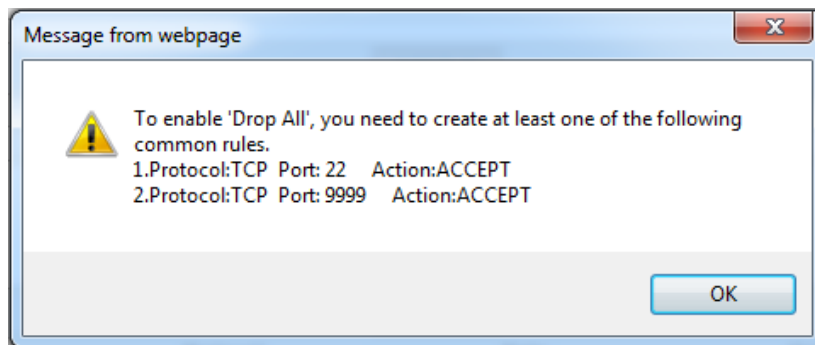


General

Enable Firewall:     Disable Ping:     Drop All:

Save    Cancel

- **Enable Firewall:** By default, the firewall is enabled. You may disable the built-in firewall by unchecking "Enable Firewall" checkbox. Only consider disabling your firewall if your CooVox IPPBX is behind a router/firewall without any port forwarding from the Internet.
- **Disable Ping:** Ignore ping request. If enabled, you cannot ping the IPPBX system.
- **Drop All:** Drop all packets sent to the IPPBX system, this will cause CooVox IPPBX system to block all communication with the outside world. Because of this, the system will prompt to add at least one grant rule on port 22(SSH) or 9999(Web) to make sure the IPPBX system is not totally unreachable.



The rule/rules can be created in the "Common Rules" section.

### Common Rules

In Common Rules section, you can configure the firewall to grant or deny an IP address or a network from communicating with the IPPBX system. Even the service port number can be specified so it can grant or deny a specific IP or network to access a specific service.

By clicking "Add Rule" button you can add a custom rule for rejecting or accepting an IP address or network address.

**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:

- **Name:** A name for this rule.
- **Description:** Optional, you may describe why this rule has been created.
- **Protocol:** Transmission protocol, UDP, TCP or UDP with TCP.
- **Port:** Service port number.
- **IP:** Can be an IP address or a network address.
- **MAC:** Action to be taken according to the Mac address of a device instead of its IP Address. This only works with devices within the same local network because Mac address are not routable.
- **Action:** Select "Drop" to block and "Accept" to grant.

### Auto Defense

CooVox IPPBX system uses Fail2Ban to perform intrusion detection, iptables is used for blocking any attack attempts.

Fail2Ban is an intrusion prevention framework written in the Python programming language. It works by reading Asterisk logs and some other logs in the IPPBX system, and uses iptables profiles to block brute-force attempts.

In the Auto Defense section you can define some custom rules to help the IPPBX system determine brute-force attempts.

Auto Defense			<a href="#">Add Rule</a>
Port	Protocol	Rate	Options
5060	UDP	40/2s	<a href="#">Edit</a> <a href="#">Delete</a>
5061	TCP	80/2s	<a href="#">Edit</a> <a href="#">Delete</a>

Click "Add Rule" button to add a new custom rule.

**Add Rule** X

Port:

Protocol:

Packets:  (1-200)

Time Interval:  seconds

In this example, it will block an IP Address that sends more than 10 packets to the port 9999 within 30 seconds, this rule will prevent brute-force attempts on the web GUI login.

### Rejected IP

Any IP address that is banned will be shown in the table of "Rejected IP". The table will show the IP address of the banned host, as well as what kind of service intrusion was detected.

Rejected IP		
Type	IP	Options
VOIP	212.83.154.178	<a href="#">Delete</a>
VOIP	173.249.158.227	<a href="#">Delete</a>
VOIP	5.189.154.148	<a href="#">Delete</a>

If a host appears incorrectly in the list of rejected IP, you can click on the "Delete" button to remove it from the list.

## 7.2 Service

Navigate to web menu *Security->Service*.

Service Settings

**Service Settings**

Enable SSH:  Port:

Remote SSH Administration:

HTTPS Port:

Remote HTTPS Administration:

As we can see here on this page, you are able to configure the SSH and HTTPS services.

- **Enable SSH:** With this option you can enable or disable SSH access to the IPPBX system. It's disabled(unchecked) by default.
- **Port:** By default, SSH service port number is 22, you can change it to any other available port number.
- **Remote SSH Administration:** If this option is checked, remote SSH access will be enabled.
- **HTTPS Port:** Web GUI service port number, the default is 9999 and you can change this to any other port number if required.
- **Remote HTTPS Administration:** If this option is checked then remote web access will

be enabled.

**Notice:**

If you want to remote access to SSH and web GUI of the IPPBX system, you can forward the corresponding ports on your router. Before doing this please ensure you have set strong passwords for root user and web admin user.

### 7.3 Allowed Address

Allowed address allows you to add IP addresses and network addresses to the IPPBX system as a whitelist. The IPs in the whitelist will always be treated as trusted IP's and will not be filtered by the firewall rules.

Navigate to web menu *Security->Allowed Address*. Click "Add New IP" button and you can add a trusted IP or network to the system IP whitelist.

Add Allowed IP		X
Description:	all	
Protocol:	<input checked="" type="checkbox"/> SIP <input checked="" type="checkbox"/> IAX2 <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> SSH	
Allowed IP:	117.176.159.157	
Subnet Mask:	255.255.255.255	
Availability:	Yes ▼	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

- **Description:** A name for this entry.
- **Protocol:** Select protocols this IP/network can access.
- **Allowed IP:** IP address or network to be trusted.
- **Subnet Mask:** Netmask for this IP or network.
- **Availability:** Choose "Yes" to activate this entry, choose "No" to deactivate.

### Settings



Allowed Address

Allowed Address	Settings
<b>SIP</b>	
Max Retry: <input type="text" value="10"/>	
Find Time: <input type="text" value="600"/> seconds	
Ban Time: <input type="text" value="3600"/> seconds	
<b>IAX2</b>	
Max Retry: <input type="text" value="10"/>	
Find Time: <input type="text" value="600"/> seconds	
Ban Time: <input type="text" value="3600"/> seconds	
<b>HTTPS</b>	
Max Retry: <input type="text" value="5"/>	
Find Time: <input type="text" value="600"/> seconds	
Ban Time: <input type="text" value="600"/> seconds	
<b>SSH</b>	
Max Retry: <input type="text" value="5"/>	
Find Time: <input type="text" value="600"/> seconds	
Ban Time: <input type="text" value="600"/> seconds	

These options are actually for Fail2Ban, the "Max Retry" limits the authentication attempts. "Find Time" defines the time duration from the first attempt to the last attempt which reaches the "Max Retry" limitation. "Ban Time" is the time in seconds the IPPBX system will block the IP which exceeds max retry.

These settings don't take effect on any allowed addresses.

## 8. System Advanced

### 8.1 Time Settings

System time is very important for the IPPBX system, especially if the CooVox IPPBX system handles inbound phone calls using time rules, then only if the system time is correct will calls be handled properly. Also, call logs and debug logs recorded to the system events use system time.

CooVox IPPBX system supports NTP (Network Time Protocol) and manual time set.

#### 8.1.1 NTP

Navigate to web menu *System->Time Settings*.

By default, CooVox IPPBX system use NTP to obtain time from Internet time servers. To configure, simply inform the IPPBX system where to find the server by specifying its domain or IP address. Also, please remember to select the correct time zone.

Time Settings

NTP     Manual Time Set

NTP Server:

Time Zone:

Once complete, click "Sync" button and the IPPBX system will attempt to synchronize the current time from the Internet. It might take a while depending on your network conditions.

After the process is complete, you'll receive a notice saying either "Sync Failed!" or "Sync Success!". If failed, then please check if the IPPBX can access the Internet or please change to another NTP server and try again.

## 8.1.2 Manual Time Set

If you want to manually set the time for the IPPBX system or for some special reason the IPPBX cannot access the Internet. You can choose to manually set the system time by checking "Manual Time Set" radio button.

Time Settings

**Time Settings**

NTP     Manual Time Set

Year: \_\_\_\_\_ (YYYY, eg: 2010)  
Month: \_\_\_\_\_ (MM, eg: 05)  
Day: \_\_\_\_\_ (DD, eg: 08)  
Hour: \_\_\_\_\_ (HH, eg: 09)  
Minute: \_\_\_\_\_ (MM, eg: 30)

Synchronize with current PC time

There are two ways to manually set a time on the system.

1. Manually input the time and date info and click "Save".
2. Synchronize the IPPBX system time with your PC time by clicking "Sync" button and then click on "Save" button.

Once "Save" is clicked the time is manually written or synchronized from the PC and will be stored into the hardware clock chip on the IPPBX motherboard.

## 8.2 Data Storage

Data storage allows you to upload your recording files, log files and voicemail messages to an FTP server through the Ethernet. If a USB drive is attached to the USB interface then the call recordings will be saved automatically to the USB drive instead of internal storage of the IPPBX system.

### 8.2.1 USB Data Storage

Plug the USB disk to the USB interface of Coovox (U20V2 and U50V2) IPPBX. Navigate to

Home page. You'll see the USB storage info like below snapshot.

Home

### System Info

<b>Network</b>			
WAN	IP: 192.168.1.7	MAC: 68:69:2E:04:18:1A	
LAN	IP: 192.168.10.100	MAC: 68:69:2E:FF:18:1A	
<b>Storage</b>			
Disk	Total:	5.3G	Used: 2.1G
Ext Disk	Total:	7.5G	Used: 129M
<b>Slot Info</b>			
SLOT 1			
1	2	3	4
FXO	FXO	FXS	FXS
SLOT 2			
1	2	3	4
GSM	GSM	N/A	N/A

Call recordings will be saved into USB drive without additional configurations. And the files can be accessed from IPPBX system Web GUI.

**Important Notice:**

- If you are using a mobile HDD please use external power supply to power the mobile HDD.**
- You can plug in the USB drive with IPPBX system in production, but please DO NOT unplug it without cut off the power.

**8.2.2 FTP Data Storage**

Utilizing your existing FTP server, you can configure the Coovox IPPBX to upload call recordings, voicemails and call log files to your FTP server. If you don't have one you can even use your Windows PC to setup an FTP server for the IPPBX system to connect to. You must however ensure that your PC is always turned on or at least available at the times when your IPPBX is going to upload files.

Data Storage

Data Storage | Data Storage Log

### Data Storage

Enable:

Server Address: 192.168.1.149

Username: U50

Password: ●●●●●●●●

Directory: /uploading

Automatically upload frequency(day): 7

Time of automatically upload: 13 : 01

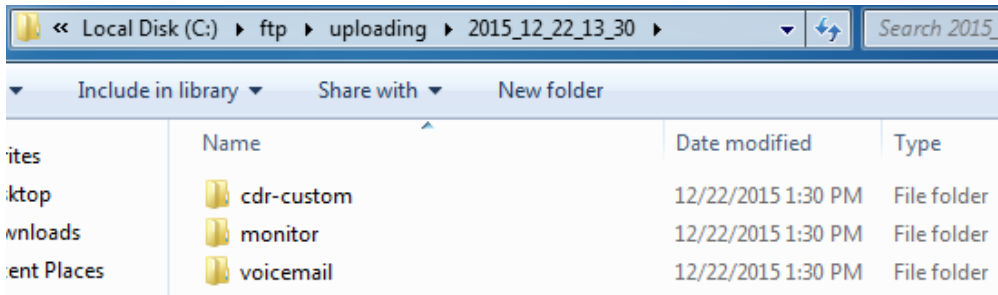
Forcibly upload when the flash storage is over: 60%

Call Recording:  Voicemail:  Call Logs:

Status: Disabled

After each upload you'll have a new folder created on your FTP server directory named by  
Copyright ©ZYCOO All Rights Reserved 115 / 127  
V2.1.2

the date and time of this upload.



**Notice:**

*After each upload, with the exception of call logs(Master.csv inside cdr-custom folder) all other files will be removed from the IPPBX system, including call recordings(files inside monitor folder) and voice messages(files inside voicemail folder). So after each upload you will only have newly generated audio files.*

## 8.3 Management

Navigate to web menu *System->Management*.

### 8.3.1 Change Password

In the "Change Password" section, you are able to change admin password, also admin username can be changed by adding extra letters following name string "admin". Operator user had been disabled by default, 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.

Management

**Change Password**

**Administrator:**  
Username: \_\_\_\_\_  
Password: \_\_\_\_\_  
New Username: admin \_\_\_\_\_  
New Password: \_\_\_\_\_  
Retype New Password: \_\_\_\_\_

**Operator:**  
Enable:   
Username: operator  
Password: \_\_\_\_\_

Once complete changing admin user credentials, click "Apply" and you'll be automatically logged out and redirected to the login page, now you are able to login with the new username and password.

And after Operator user been activated you can login with user name operator and the operator password. Operator user password also can be changed on Operator user portal. you can change the password on *Change Password* page.

### 8.3.2 Set System Voice Prompts

What are system voice prompts?

System voice prompts guide callers on for example how to place a call or how to use the IPPBX system functionality. One example is while checking voicemail the system voice prompts informs the user to enter voicemail password and in another example if you call someone and they don't answer then the system voice will ask that you should leave a message.

In the "Set Language" section you can decide in which language the system uses for the

callers.

**Set Language**

Set Voice Language: English \* [Download](#) [Delete](#)

Save

At this time, CooVox IPPBX system(firmware version 2.1.2) supports 22 different languages as the system voice prompts. They are English, English (Australia), Chinese, French, French (Canada), Spanish, Spanish (Mexico), Portuguese, Portuguese (Brazil), Italian, Persian, Arabic, Turkish, Thai, Russian, Polish, Dutch, Korea, Hungary, Vietnamese, Hebrew, Greek and Germany.

The items with \* means these languages already exist on the system while others can be downloaded here by clicking the "Download" button.

## 8.4 Backup

### 8.4.1 Take a Backup

Taking a backup on CooVox IPPBX system is the same as when you create a recovery point on your Windows system. By restoring the backup you can recover the CooVox IPPBX system configurations to the time point when it was still functioning well.

Normally the first backup should be taken when you have finished configuring the IPPBX to work for the very first time. Also, when you have applied new changes to your configuration is always a good time to take another backup.

Navigate to web menu *System->Backup*. Click "Take a Backup" button to create a backup file which will contain all current system configurations.

Backup

Backup
Upload Backup File

List of Backups		<a href="#">Take a Backup</a>
Name	Date	Options
1	backup_2015dec14_174001	Dec 14, 2015
		<span style="border: 1px solid #ccc; padding: 2px 5px; background-color: #e0e0e0;">Restore</span> <span style="margin-left: 5px; border: 1px solid #ccc; padding: 2px 5px; background-color: #e0e0e0;">Delete</span> <span style="margin-left: 5px; border: 1px solid #ccc; padding: 2px 5px; background-color: #e0e0e0;">📄</span>

Once complete, you will see the backup file listed on this page. The file is stored in the file system. At any time, by clicking "Restore" button you can restore your configurations. By clicking "Delete" button you can delete this backup. You can also download the backup to your computer hard disk drive by clicking the button.

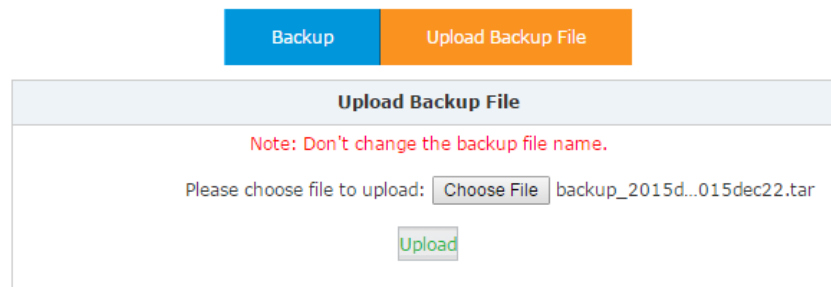
**Notice:**

If you are downloading the backup to your computer hard drive, please keep this file confidential, because this file contains web admin password, user extension password and many other sensitive information which may compromise your IPPBX system.

## 8.4.2 Upload Backup File

Click on "Upload Backup File" tab and you are able to upload a backup file from your computer hard drive.

Upload Backup File



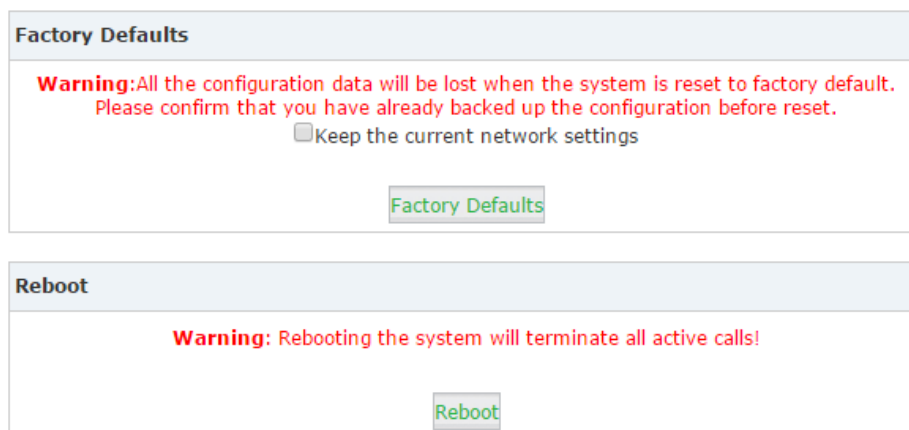
### Notice:

If you are uploading a backup from another IPPBX system, please ensure they have the same hardware configurations. It is not recommended to upload backup files to different IPPBX systems, unless you are pretty comprehensive with Zycoo IPPBX systems.

## 8.5 Reset & Reboot

Navigate to web menu *System->Reset & Reboot.*

Reset & Reboot



As you can see here on this page, you are able to reset and reboot the IPPBX system directly via web GUI.



### 8.5.1 Reset

By clicking “**Factory Defaults**” button you can reset all configurations for the IPPBX system. In addition to the configurations to be reset, recording files, voicemail messages and call logs will also be erased. So please ensure you have backed up the files you need before resetting.

The whole resetting process will be completed in 2 minutes. If you have chosen to reset network settings also, then you need to login with the default URL <https://192.168.1.100:9999>. Username and password will all be reset to admin.

### 8.5.2 Reboot

By clicking “**Reboot**” you can restart the IPPBX system, the whole process will be completed in 2 minutes.

## 8.6 Upgrade

Zycoo will update the IPPBX firmware at regular intervals for new features and bug fixes. You can visit our official website [www.zycoo.com](http://www.zycoo.com) to check the updates for your IPPBX system.

The downloaded firmware package should be in .rar or .zip format, please extract the package first and upgrade with the uImage-md5.xxx file to upgrade your IPPBX system. Navigate to web menu *System->Upgrade*. You can see there are two methods you can upgrade the IPPBX firmware, they are web upgrade and TFTP upgrade.

### 8.6.1 Web Upgrade

Upgrade

**Upgrade System Package**

WEB Upgrade       TFTP Upgrade

Restore Default Set:

Please choose file to upload:  uImage-md5.u50v2.v212

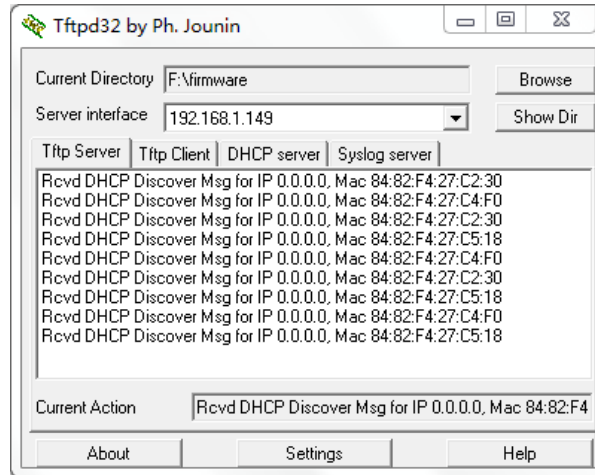
Check "WEB Upgrade" radio button and click "Browse" button to locate the new firmware in your PC hard drive. Click "Upload" and you will be asked to confirm a restart of the IPPBX system to complete the upgrade process. You can click "Yes" to continue upgrading.

**Notice:**

*The "Restore Default Set" option is used to reset the IPPBX system configurations while upgrading, You don't have to enable this option to reset the IPPBX system and only do so if you do wish to reset to default settings as it will reset all system configurations including the network profiles.*

### 8.6.2 TFTP Upgrade

If you don't have a TFTP server, you can Google tftpd32 and download this application to setup a lightweight TFTP server on your Windows.



Please click "Browse" on the TFTP application window to locate the new firmware. In the "Server Interface" dropdown list is a list of your PC network interfaces. Please select a correct interface(in the same network) which can access the IPPBX system.

On the IPPBX web GUI please check the "TFTP Upgrade" radio button, and specify the exact firmware file name in the "Enter The Package Name" blank, and in the "TFTP Server IP address" blank please specify the IP address displayed on the TFTP application window.

#### Upgrade

Please double check the file name and TFTP server IP address then click "Apply" you will be able to upgrade the firmware just like web upgrade.

## 8.7 Addons

Addons for CooVox IPPBX system are used to enhance the experience of the IPPBX system features. For now we support CooBill(billing) and CooCall(Zycoo softphone APP) addons.

### 8.7.1 CooBill

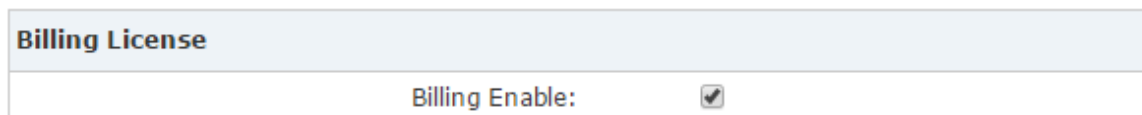
CooBill is a billing system developed by ZYCOO Europe and is designed to integrate with our CooVox Series IP Phone Systems. Its primary purpose is to aid enterprises in managing their telecommunication billing process, and allows them to access a detailed account list of daily calls or to produce bills for customers. Once integration with CooVox IP Phone Systems is complete, CooBill can be used to check billing for each extension, recharge for a selected extension, etc. Prepay and Postpay are available for flexible payment type options.

First you'll need to download CooBill client and install it on your Windows system. The download links for both Windows 32bit and 64bit versions are available at:

<http://zycoo.com/html/CooBill.html>

CooBill client can be installed on Windows Vista, Windows 7 and Windows 8, but Windows XP is not compatible.

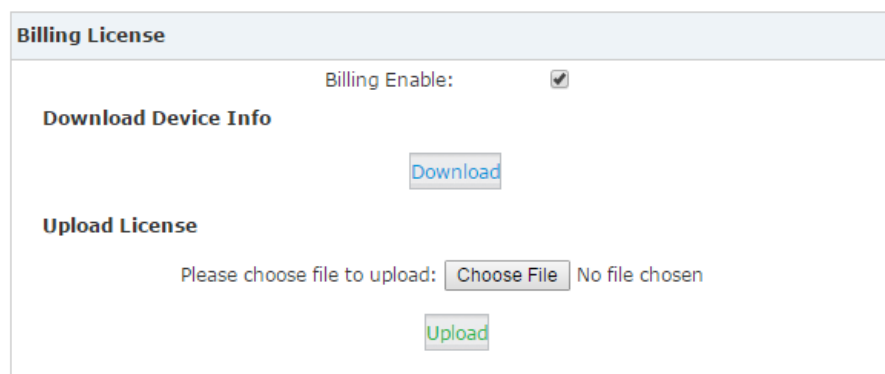
On the IPPBX system you first need to enable CooBill addon service. Navigate to web menu *System->Addons*.



The screenshot shows a web interface for configuring the Billing License. At the top, there is a header "Billing License". Below it, there is a section labeled "Billing Enable:" with a checked checkbox.

Tick "Billing Enable" checkbox, and click "Save" and you'll be able to download the license source file, please send this file to ZYCOO sales or send to ZYCOO distributor to apply license for CooBill billing system.

Addons



The screenshot shows the Billing License configuration page with the "Billing Enable" checkbox checked. Below this, there are two main sections: "Download Device Info" and "Upload License". The "Download Device Info" section has a "Download" button. The "Upload License" section has a "Please choose file to upload:" label, a "Choose File" button, and an "Upload" button.

Click the "Download" button and you can download the license source file. After you have received the license file from Zycoo you can upload it here. Once upload has completed your billing system is activated.



For configuring the CooBill client on your Windows system please refer to the link below:

[http://www.zycoo.com/files/upload/CooBill\\_Installation\\_Guide&Manual.pdf](http://www.zycoo.com/files/upload/CooBill_Installation_Guide&Manual.pdf)

**Notice:**

*Before you request your license file from Zycoo and upload it to your IPPBX system to activate billing addon, please disable billing feature temporarily. Because without configuring valid rate rules on CooBill client the IPPBX system is unable to make outbound phone calls.*

### 8.7.2 CooCall

CooCall is a free softphone APP for Android and iOS platforms which can be integrated with ZYCOO IPPBX systems. You can bring your extension with you anywhere there's an Internet connection.

CooCall provides not only basic softphone APP functionalities such as call transfer, call hold and 3-way conference call but can also achieve some features other softphone APPs cannot do by integrating with ZYCOO CooVox IPPBX system. For example, BLF, call recording retrieval and playback, voicemail retrieve and playback, phonebook integration with IPPBX system, etc.

You can download and install CooCall from your mobile phone APP store by searching keyword "CooCall". Or you can visit our web page <http://www.zycoo.com/html/CooCall.html> and scan the QR code at the bottom of this page to get the APP.

After installation, please setup your account on CooCall as detailed below:

Back User Settings Register

Primary IP Address \*  
192.168.1.100

Secondary IP Address \*  
117.176.159.157

Username \*  
408

Password \*  
•••••

Show Password

Version:1.0.0

Logs Dialer Contacts Config

- **Primary IP Address, Secondary IP Address:** Normally your IPPBX system is deployed in a private network, you may use the private IP of the IPPBX to register your extension when you are in the office. Secondary IP can be the public IP address of your office, if you are out of office, CooCall will switch to the secondary IP to register to the IPPBX system as a remote extension.
- **Username:** An extension number.
- **Password:** Password of this user extension.

Once information is complete, tap "Register" button to register to the IPPBX system. After registered, you will see "Ready to call" displayed on the "Dialer" screen. You can now make phone calls from the CooCall softphone just as you would make calls from any other IP phones.

**Notice:**

1. CooCall for iPhone works only with TCP transmission. Please enable TCP for the extensions which will be used by CooCall softphone on the extension configuration page.

VoIP Settings

NAT:  Transport: TCP SRTP:

If you are going to use this extension outside the LAN please also enable NAT.

And you have to enable global TCP transmission support too. It's on Advanced->Options->SIP Settings page.

SIP Settings

General	Analog Settings	SIP Settings	IAX2 Settings
---------	-----------------	--------------	---------------

General	
<input checked="" type="checkbox"/> Enable	UDP Port: <u>5060</u>
<input type="checkbox"/> Enable	TCP Port: <u>5060</u>
	TLS Port: <u>5061</u>

2. If you are planning to register remote extensions, you have to port forward 5060(UDP+TCP), 10001-10500(UDP) on your router/firewall. And NAT support should be enabled on Advanced->Options->SIP Settings page.

SIP Settings

General	Analog Settings	SIP Settings	IAX2 Settings
---------	-----------------	--------------	---------------

NAT Support	
External IP:	<u>117.176.159.157</u>
External Host:	<u>117.176.159.157</u>
External Refresh(sec):	<u>10</u>
Local Network Address:	<u>192.168.1.0/255.255.255.0</u>
Local Network Address:	_____
Local Network Address:	_____

Both "External IP" and "External Host" should be your public IP address, or can be your DDNS domain.