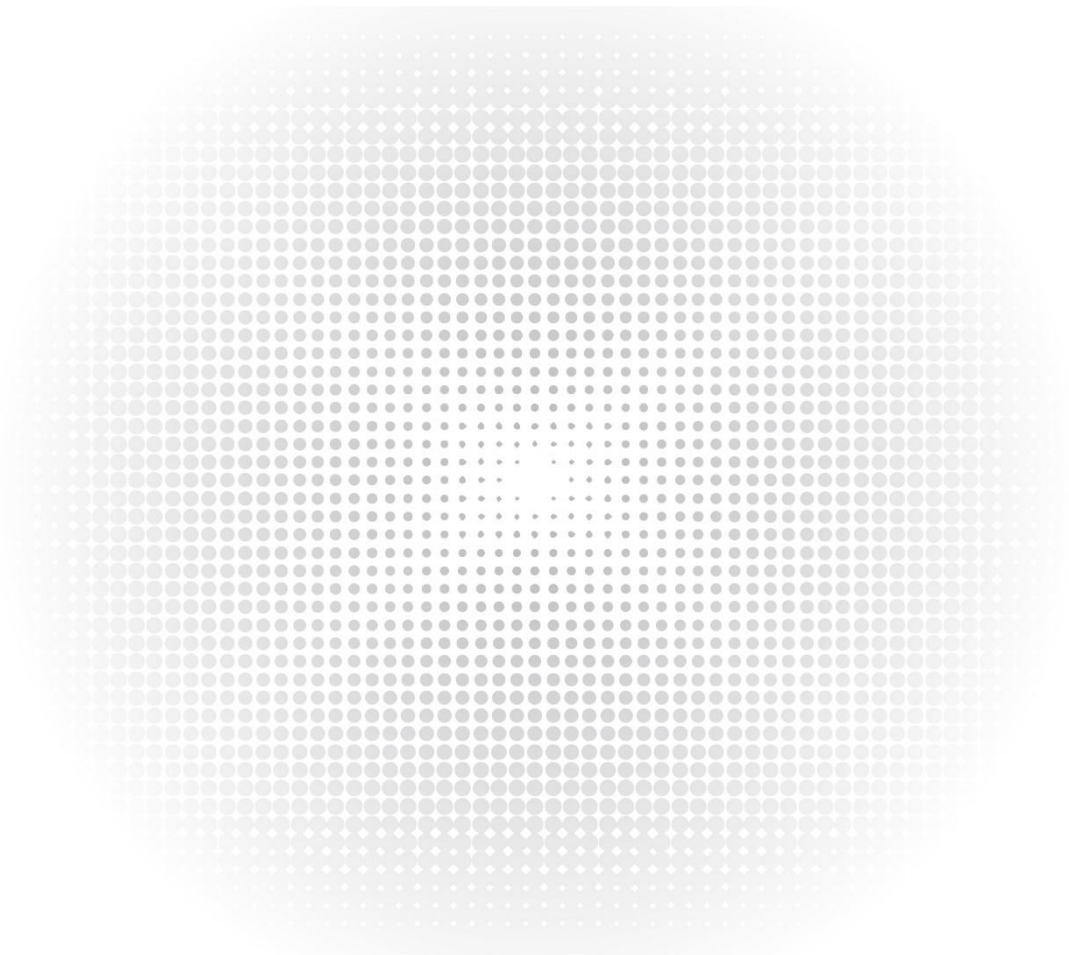


IP PBXs User Manual

Models: PBX-C301, PBX-C302, PBX-C503



Contents

1 Safety Notice	1
2 Overview	2
2.1 Brief Introduction	2
2.2 Modules	2
2.3 Mechanical Design	5
2.3.1 PBX-C301	5
2.3.2 PBX-C302 and PBX-C503	6
2.4 Key Features	8
2.5 Environmental Requirements	8
3 Getting Started	9
3.1 Quick Setup Wizard	9
4 Extensions	15
4.1 Departments	15
4.2 IP Extensions	16
4.3 Analog Extensions	20
5 Inbound Control	22
5.1 IVR	22
5.2 Call Queue	23
5.3 Time Conditions	26
5.4 Inbound Routes	28
5.5 Direct Routing	29
5.6 Inbound Fax	30
5.7 Blacklist	31
6 Outbound Control	32
6.1 Trunks	32
6.1.1 FXO/GSM Trunks	32
6.1.2 E1 Trunks	33
6.1.3 BRI Trunks	34
6.1.4 SIP Trunks	35
6.2 Dial Rules	38
6.3 Dial Permissions	39
6.4 Outbound Fax	41
6.5 PIN Sets	41
7 Audio Library	42
7.1 Music On Hold	42
7.2 IVR Prompts	42
7.3 Custom Prompts	43
8 Advanced Features	44
8.1 Call Forward	44
8.2 Follow Me	44
8.3 Wake Up Call	45

8.4 Conference	46
8.5 Paging & Intercom	46
8.6 Smart DID	47
8.7 Phonebook	48
8.8 LDAP	48
8.9 Callback	48
8.10 Whitelist	49
9 Preferences	51
9.1 Global PBX Options	51
9.2 VoIP Advanced	52
9.3 Analog Settings	54
9.4 Voicemail Settings	56
9.5 Module Settings	56
9.5.1 E1 PRI Signaling	57
9.5.2 T1 PRI Signaling	58
9.5.3 MFC/R2 Signaling	58
9.5.4 SS7 Signaling	59
9.5.5 BRI Settings	60
10 Feature Codes	62
10.1 Voicemail feature codes	62
10.2 Call Pickup feature codes	62
10.3 Call Parking feature codes	62
10.4 Call Transfer feature codes	63
10.5 Blacklist feature codes	63
10.6 Call Spy feature codes	64
10.7 Call Queue feature codes	64
10.8 Conference feature codes	64
10.9 Wakeup call feature codes	65
10.10 Call Forward feature codes	65
10.11 DND feature codes	66
10.12 Office Closed feature codes	66
10.13 Other feature codes	67
11 Reports	68
11.1 Call Logs	68
11.2 Call Recordings	68
11.2.1 Call Recordings	68
11.2.2 Conference Recordings	69
11.2.3 One Touch Recordings	70
11.3 System Logs	70
11.3.1 Fax Logs	70
11.3.2 Web Access Logs	70
11.3.3 Advanced Logs	71
12 System	72
12.1 Storage	72
12.1.1 USB Storage	72

12.1.2 FTP Storage.....	73
12.1.3 System Storage.....	74
12.2 Region and Time	75
12.3 Network Settings	75
12.3.1 Network Profiles	75
12.3.2 IPv6	76
12.3.3 Local Domain Name Service	77
12.3.4 VLAN	77
12.3.5 VPN	78
12.3.6 Static Routing	91
12.3.7 DHCP Server	92
12.3.8 DDNS	93
12.3.9 SNMP	94
12.4 Security Center	94
12.4.1 Firewall	94
12.4.2 Intrusion Detection and Prevention	96
12.4.3 IP Blacklist.....	97
12.4.4 IP Whitelist	97
12.5 Email Services	98
12.5.1 Mail Server Settings	98
12.5.2 Voicemail to Email Settings	99
12.5.3 Fax to Email Settings.....	100
12.5.4 Email Notifications.....	100
13 Maintenance	101
13.1 Users	101
13.1.1 Admin User	101
13.1.2 Operator User	101
13.1.3 API User	101
13.1.4 Conference Manager	101
13.1.5 Root User	102
13.2 Upgrade	102
13.3 Diagnostic	103
13.3.1 PING	103
13.3.2 Traceroute	103
13.3.3 Ethernet Capture	104
13.3.4 Channel Monitor	104
13.3.5 Remote Management	105
13.4 Backup	105
13.5 Reboot and Reset	105
13.5.1 Reboot.....	105
13.5.2 Reset.....	106
14 Addons	107
14.1 Proxy	107

1 Safety Notice

Please read the following safety notices before installing or using this IPPBX. 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 IPPBX and voidance of the warranty.

1. Please use the external power supply which is included in the package. Any other power supply may cause damage to the unit, affecting 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 or 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 unit is installed. In order to maintain the unit, it will need to be disconnected from the power source.
5. Do not drop, knock or shake the unit. Rough handling can break internal circuit boards.
6. Do not install the unit in places where there is direct sunlight. Also do not place the unit on carpets or cushions. Otherwise it may cause the unit malfunction or cause fire.
7. Avoid exposing the unit to high temperature (above 40°C), low temperature (below -10°C) or high humidity. Otherwise it could cause damage and will void the warranty.
8. Avoid letting the unit in contact with water or any other liquid which would damage the unit.
9. Do not attempt to open the device. Non-expert handling of the device could cause damage and will void the warranty.
10. Do not use harsh chemicals, cleaning solvents, or strong detergents to clean the unit.
11. Clean the unit with a soft cloth that has been slightly dampened in a mild soap and water solution.
12. Ensure the unit is installed in a well-ventilated room to avoid overheating.
13. Before you work on any equipment, be aware of any hazards involved in electrical circuitry and be familiar with standard practices for preventing accidents if you are in a situation that could cause physical injury.

2 Overview

2.1 Brief Introduction

IP PBX is the most innovative solution for VoIP telecommunications 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.

2.2 Modules

- 4FXO Module



4FXO module provides 4 FXO interfaces for connecting PSTN lines provided by the telecom. It can be installed on two slots of PBX-C301, PBX-C302 and PBX-C503 and provides maximal 8 FXO interfaces.

- 4FXS Module



4FXS module provides 4 FXS interfaces for connecting fax machines or analog phones. It can be installed on two slots of PBX-C301, PBX-C302 and PBX-C503 and provides maximal 8 FXS interfaces.

- 2FXOS Module



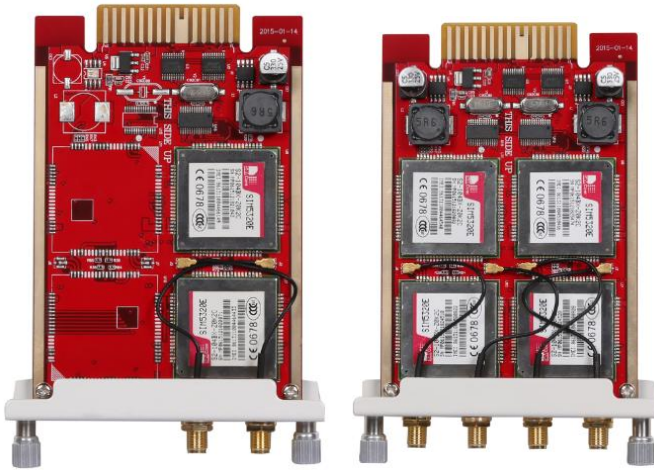
2FXOS module provides 2 FXO and 2 FXS interfaces, it can be installed on two slots of the PBX-C301, PBX-C302 and PBX-C503. With 2FXOS module installed it enables to IPPBX system with FXO to FXS lifeline feature, when there's power failure, you may still use the analog phone to make and receive phone calls.

- 2GSM/4GSM Module



2GSM/4GSM module provides 2/4 GSM channels, it can be installed on PBX-C301, PBX-C302 and PBX-C503 for making and receiving phone calls from GSM network. It is designed with SIM900 for global market, SIM900 is a quad-band GSM engine that works on frequencies GSM 850MHz, EGSM 900MHz, DCS 1800MHz and PCS 1900MHz.

- 2WCDMA/4WCDMA Module



2WCDMA/4WCDMA module provides 2/4 GSM/3G voice channels, it can be installed on PBX-C301, PBX-C302 and PBX-C503 for making and receiving phone calls from GSM/3G network. It is designed with SIM5320 series module for global market, SIM5320 is Dual-Band WCDMA and Quadband GSM engine that works on frequencies UMTS 850MHz, UMTS 900MHz, UMTS 1900MHz, UMTS 2100MHz, GSM 850MHz, EGSM 900MHz, DCS 1800MHz and PCS 1900MHz.

Notice

WCDMA modules for IPPBXs are only used for voice phone calls, they CANNOT be used for data transmission from 3G network.

- 4BRI Module



4BRI module provides 4 BRI interfaces which can be configured to work in NT or TE mode. It can be installed on PBX-C302 and PBX-C503 but not PBX-C301.

On PBX-C302 and PBX-C503 only one 4BRI module can be installed. And if it' s going to be installed with other modules (4FXO, 4FXS, 2FXOS, 2/4GSM, 2/4WCDMA modules), it should be installed on SLOT2. 4BRI cannot be installed with E1 module on the same PBX-C302 or PBX-C503.

- E1/T1 Module

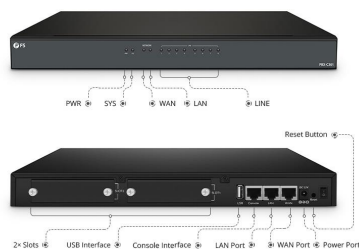


The E1/T1 module provided a RJ48 interface which could be configured to work in E1 (PRI-NET, PRI-CPE, R2, SS7 signaling) and T1 mode. You can install 2 E1/T1 modules on both PBX-C302 and PBX-C503. If it's going to be installed with other modules (4FXO, 4FXS, 2FXOS, 2/4GSM, 2/4WCDMA) it should be installed on SLOT2. And E1/T1 module cannot be installed with BRI module on the same PBX-C302 or PBX-C503.

2.3 Mechanical Design

2.3.1 PBX-C301

- Hardware configurations



PBX-C301

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

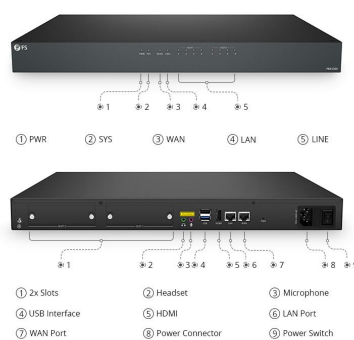
Applicable module for SLOT1 &2: FXO/FXS/ GSM/ WCDMA Module Cards

- PBX-C302 LED Indications

Identification	Indication	Status	Specification	
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
			Off	Channel failure
		FXO	Red	Channel available
			Off	Channel failure
		GSM	Red	Channel available
			Off	Channel failure
		WCDMA	Red	Channel available
			Off	Channel failure

2.3.2 PBX-C302 and PBX-C503

- Hardware Configurations



- PBX-C503 Front View

No.	Name	Specification
1-5	LED Indicators	Indicate the system activity and interface connection status.

- PBX-C503 Back View

No.	Name	Specification
1	1-24 FXO/FXS Ports	For connecting PSTN/Analog phone/Fax machine.
2	Headser	For external paging.
3	Microphone	For external paging.
4	USB Port	For USB keyboard or USB storage.
5	HDMI Port	For video output.
6	LAN Port	10/100/1000 Mbps.
7	WAN Port	10/100/1000 Mbps.
8	Power Connector	100~240V AC power.
9	Power Switch	Switch the power on or off.

- PBX-C302 and PBX-C503 LED Indication

Identification	Indication	Status		Specification	
PWR	Power States	Green		Power On	
		Off		Power Off	
SYS	System States	Wink		System is Running	
		Off		System Booting or Failed	
WAN/LAN	WAN/LAN Interface States	Wink		Data Transmitting	
		Off		No Data Transmitting	
1-4 (SLOT1/2)	Slot1 and Slot2 States	FXS		Green	Channel Loading Succeed
				Off	Channel Loading Failure
		FXO		Red	Channel Loading Succeed
				Off	Channel Loading Failure
		GSM/WCDMA		Red	Channel Loading Succeed
				Off	Channel Loading Failure
		E1/T1 (PRI/R2)	L1	Red	Module Loading Succeed
				Off	Module Loading Failure
			L2/L3	Red/Off	CPE Signaling
				Green/Off	NET Signaling
				Off/Red	SS7 Signaling
				Off/Green	R2 Signaling
			L4	Green	Connected (No Alarm)
				Red	Disconnected (Alarm)
		BRI		Red	TE Mode
				Green	NT Mode
				Off	Module Loading Failure

Notice

PBX-C302 and PBX-C503 share the same hardware architecture, except C503 has been equipped with a 500GB hard drive for internal storage.

2.4 Key Features

- | | |
|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| ✓ BLF(Busy Lamp Field) | ✓ Blacklist (blacklist the last caller) |
| ✓ Caller ID | ✓ Smart DID |
| ✓ DND(Do Not Disturb) | ✓ Quick Setup Wizard |
| ✓ WebRTC | ✓ Flexible Dial Permissions |
| ✓ Extension User Portal | ✓ Feature Codes |
| ✓ Call Detail Records (500,000 records) | ✓ Wakeup Call |
| ✓ Call Center Queues | ✓ One Number Stations |
| ✓ Call Parking | ✓ Music On Hold |
| ✓ Call Forward | ✓ Phonebook/LDAP(10,000 contacts) |
| ✓ Call Transfer | ✓ Department (ring group, pickup group) |
| ✓ Call Waiting | ✓ Phone Provisioning |
| ✓ Call Recording | ✓ Expansion Box Provisioning |
| ✓ One Touch Recording | ✓ Speed Dial |
| ✓ Video Call | ✓ Time Conditions |
| ✓ Voicemail | ✓ SIP/IAX Extension Registration |
| ✓ Virtual Fax | ✓ Static/DHCP Network Access |
| ✓ Conference Bridge (10 Conferences) | ✓ System Backup |
| ✓ DISA (Direct Inward System Access) | ✓ T.38 Fax Pass-through |
| ✓ Paging and Intercom | ✓ USB Extended Storage (Scalable) |
| ✓ Direct Inbound Routing | ✓ GeoIP Security Policy |
| ✓ Audio Codec: G.722/ G.711-ULaw/ G.711-ALaw/ G.726/ G.729/ GSM/ SPEEX/Opus | |
| ✓ Video Codec: H.261/ H.263 / H.263+ /H.264/VP8 | |
| ✓ VPN Server (PPTP/OpenVPN, support 10 VPN clients) | |
| ✓ VPN Client (PPTP/OpenVPN) | |
| ✓ DDNS(Dyndns.org/No-ip.com/zoneedit.com/ freedns.afraid.org/www.oray.com/ 3322.org) | |
| ✓ IP Phone Provisioning (Akuvox, Cisco, Escene, Fanvil, Flying Voice, Grandstream, Htek, MOCET, Snom, Yealink) | |

2.5 Environmental Requirements

Operating Temperature: 0 °C ~40 °C

Storage Temperature: -20 °C ~ 55 °C

Humidity: 5~95% Non-Condensing

3 Getting Started

3.1 Quick Setup Wizard

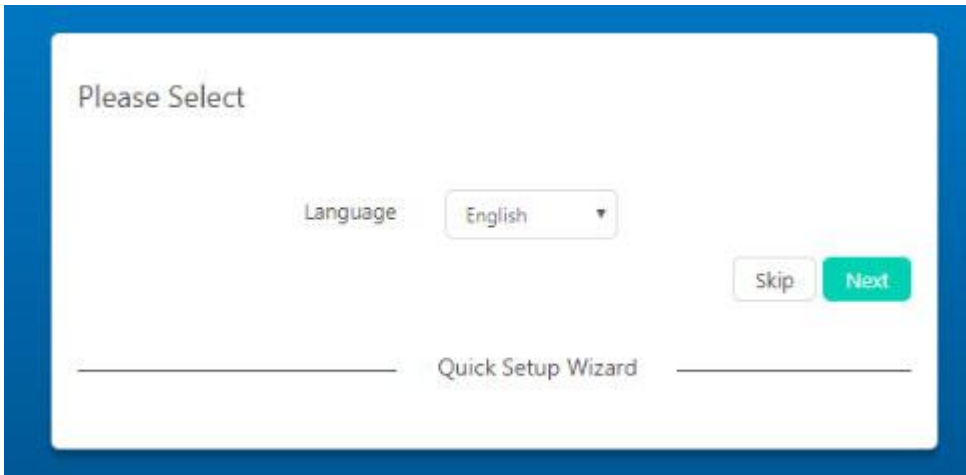
Quick Setup Wizard is especially designed on v3.0.0 software for IPPBXs to help you quickly and easily setup your IPPBX system within minutes.



When you open the Web UI of a new unit with factory default settings, Quick Setup Wizard will be presented. You may follow the wizard to complete some basic settings or you may skip the wizard and login with default credentials.

Username: admin

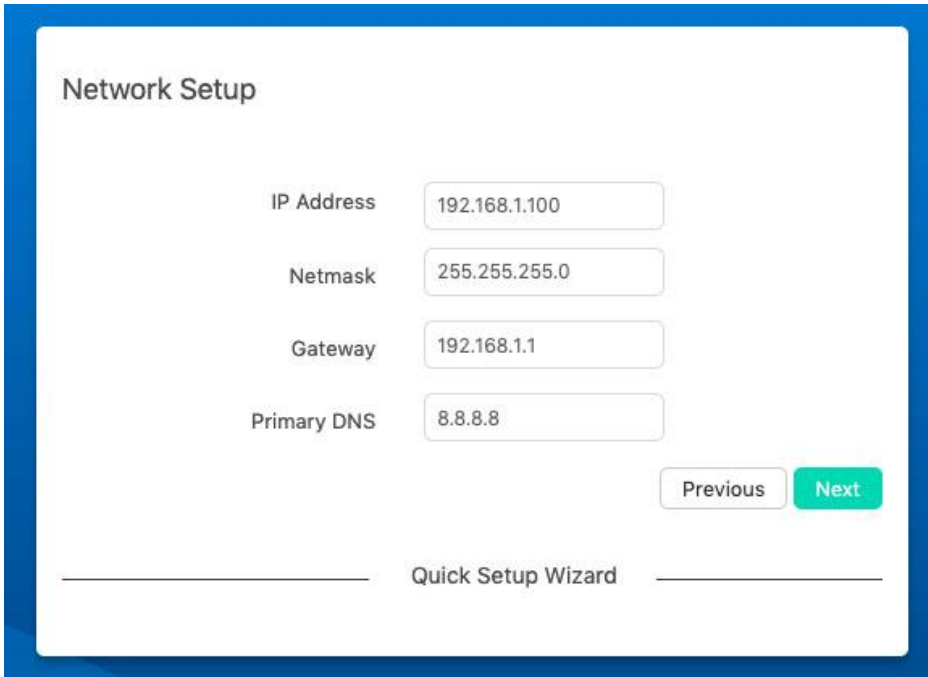
Password: admin

- Step 1: Wizard Language



You may skip the wizard here by clicking on  button. Or choose your native language to begin with the wizard, if it's not in the list then choose one that you familiar with. Once done, please click on  button to continue.

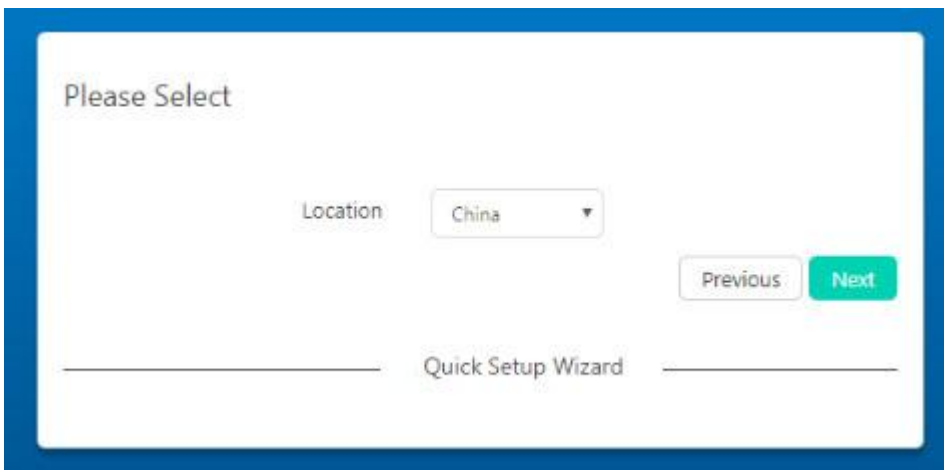
- Step 2: Network Settings



The screenshot shows the 'Network Setup' screen of the Quick Setup Wizard. It features four input fields for network configuration: IP Address (192.168.1.100), Netmask (255.255.255.0), Gateway (192.168.1.1), and Primary DNS (8.8.8.8). Below these fields are 'Previous' and 'Next' buttons. The 'Next' button is highlighted in green. At the bottom, the text 'Quick Setup Wizard' is centered between two horizontal lines.

Change the network profiles per your local LAN environment. Once done, please click on  button to continue.

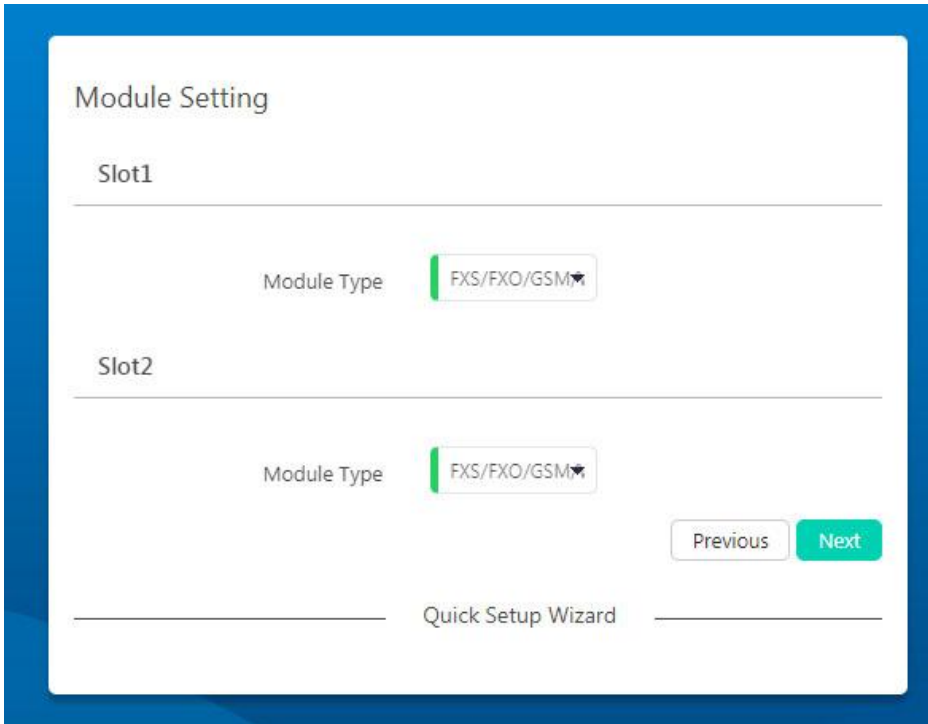
- Step 3: Location



The screenshot shows the 'Please Select' screen of the Quick Setup Wizard. It features a 'Location' dropdown menu with 'China' selected. Below the dropdown are 'Previous' and 'Next' buttons. The 'Next' button is highlighted in green. At the bottom, the text 'Quick Setup Wizard' is centered between two horizontal lines.

Select the country/region you live in, the location you selected will also tell the IPPBX system which time zone and tone zone you want the IPPBX to use. And some other regional settings will be defined as well.

- Step 4: Module Settings



The screenshot shows the 'Module Setting' page of the Quick Setup Wizard. It features two sections, 'Slot1' and 'Slot2', each with a 'Module Type' dropdown menu currently set to 'FXS/FXO/GSM'. At the bottom right, there are 'Previous' and 'Next' buttons. The page is framed by a blue border and has a white background.

This step is only for PBX-C302 and PBX-C503. If you have installed FXS/FXO/GSM/WCDMA modules on both Slots then just simply click on **Next** button to continue. If you have installed E1/T1/BRI modules, please select the module type accordingly. For more configurations please refer to Module Settings.

- Step 5: Create Departments and Extensions

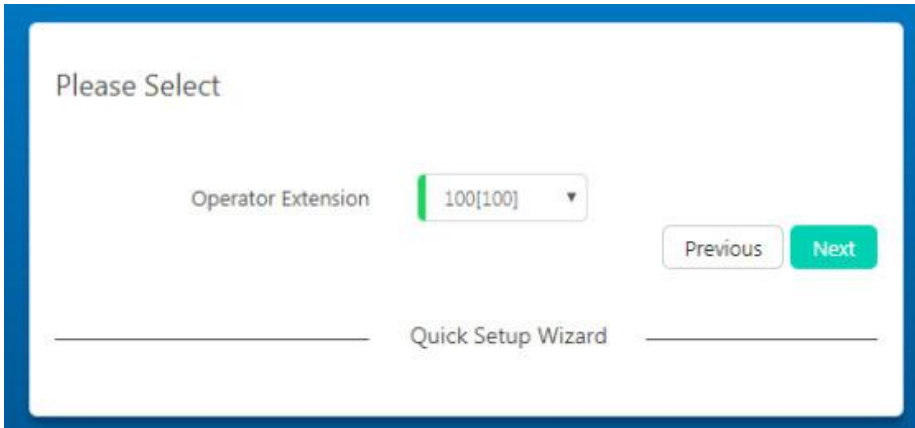


The screenshot shows the 'Departments' page of the Quick Setup Wizard. It contains three input fields: 'Department Name' (with value 'dpt1'), 'Extension Count' (with value '10'), and 'Department Extension' (with value '0400'). Below these is an 'Add' button. Further down is a 'Start Extension' input field with the value '100'. A notice states: 'Notice: Only 100 user extension supported on this unit.' At the bottom right are 'Previous' and 'Next' buttons. The page is framed by a blue border and has a white background.

According to your company organization structure you can add departments and extensions here for each department.

Specify the department name and number of the members, then click on **Add** button to add another department the same way. Once done, specify a start extension number and click on **Next** button to continue.

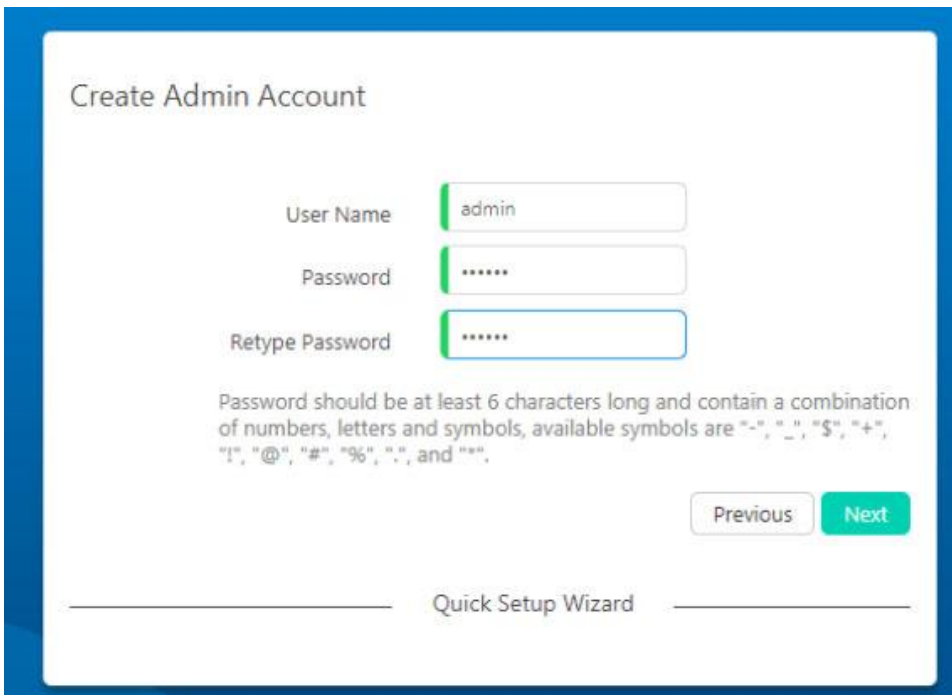
- Step 6: Specify Operator Extension



The screenshot shows a web interface titled "Please Select". It features a dropdown menu labeled "Operator Extension" with the value "100[100]" selected. To the right of the dropdown are two buttons: "Previous" and "Next". At the bottom of the form, the text "Quick Setup Wizard" is centered between two horizontal lines.

The operator extension is usually the extension number of the company receptionist or secretary. Please specify the extension number here, in certain circumstances calls will be sent directly to this extension for information.

- Step 7: Create Admin Account



The screenshot shows a web interface titled "Create Admin Account". It contains three input fields: "User Name" with the value "admin", "Password" with masked characters "*****", and "Retype Password" with masked characters "*****". Below these fields is a text instruction: "Password should be at least 6 characters long and contain a combination of numbers, letters and symbols, available symbols are '-', '_', '\$', '+', '[', ']', '@', '#', '%', '&', and '*'". To the right of the instruction are two buttons: "Previous" and "Next". At the bottom of the form, the text "Quick Setup Wizard" is centered between two horizontal lines.

Admin account can be customized that you can use any user name you prefer. For security reasons, please do not use weak administrator credentials.

- Step 8: Create Operator Account

Create Operator Account

User Name

Password

Retype Password

Password should be at least 6 characters long and contain a combination of numbers, letters and symbols, available symbols are "-", "_", "\$", "+", "!", "@", "#", "%", ".", and "**".

Quick Setup Wizard

Operator account has limited permissions comparing to Admin user. It can be used by the operator user to manage extension numbers of the company, setup calling features, manage call logs and recordings.

● Step 9: Mail Server Settings

Mail Server Settings

SMTP Server ☒

Mail Service Provider

SMTP Server

Port

SSL ☒

Email


Password

Quick Setup Wizard

Mail server will be used to send out email notifications from the IPPBX system. Please select a mail service provider from the list.

Supported mail service providers' default settings will be filled in automatically. If the mail service provider of yours is not in the list

please choose “Other” .

Once done, please click on  button, now system will reboot for new settings to take effect. If PBX-C301, you’ ll have to wait around 4 minutes then refresh the page. If PBX-C302 or PBX-C503, it will take around 2 minutes to reboot, after this please refresh the page. Now you should see the login page like the screenshot shown below.



Please use the admin credentials you defined during the installation wizard to sign in.

4 Extensions

Path: **Telephony -> Extensions**

Extensions and departments should have been created during the Quick Setup Wizard process. You may manage extensions and departments here on this screen. If you have skipped the Quick Setup Wizard, you may create them here on this screen as well.

4.1 Departments

Path: **Telephony -> Extensions -> Departments**



Department concept is new on IPPBX v3 software. Extensions are grouped by your company's actual organizational structure.

A department is equal to a Pick-up group.

A department is equal to a Call groups (Ring Group).

If you have created departments and extensions from Quick Setup Wizard, you should see all your departments and extensions here.

Departments		IP Extensions		Analog Extensions		Phone Provisioning		Expansion Box	
<div>Add</div>									
Department Name	Department Extension	Department Members						Options	
dpt1	0400	Extension...	Extension...	Extension...	Extension...	Extension...	Extension...	<div><div></div><div></div></div>	
		Extension...	Extension...	Extension...	Extension...				
dpt2	0401	110[110]	111[111]	112[112]	113[113]	114[114]	115[115]	<div><div></div><div></div></div>	
		116[116]	117[117]	118[118]	119[119]				
dpt3	0402	120[120]	121[121]	122[122]	123[123]	124[124]	125[125]	<div><div></div><div></div></div>	
		126[126]							
3 Total									

If you wish to create a new department, please click on the **Add** button. Specify the department name and select member extensions then submit. If you wish to modify department settings, please click on the  button, or click on the  button to remove a department.

Edit 0400

Department Name

Ring Strategy ?

Ring All

Ring Time ?

Destination if no answer

Hangup

Select Department

Extension1[101] x

Extension2[102] x

Extension3[103] x

Extension4[104] x

Extension5[105] x

Extension6[106] x

Extension7[107] x

Extension8[108] x

Extension9[109] x

Members

Distinctive Ring

Cancel

Submit

- You may change the department name from the **Department Name** textbox.
- In the **Ring Strategy** dropdown list select a desired ring strategy of how to ring the department (Ring Group) extensions upon incoming calls.
- **Ring All:** Ring all available member extensions until one answers(default).
- **Linear:** Starting with the first member, ring the extension of each member in turn until the call is answered.
- You may adjust the ring time of each extension upon department ring group incoming calls from the **Ring Time** textbox.
- In **Destination if no answer** dropdown list select a call destination for the inbound calls when no one answers the call.
- You may add/remove members of your department from the **Select Department Members** field.
- **Distinctive Ringtone** can ring the phones with specific ringtone upon inbound calls to this department.

4.2 IP Extensions

Path: **Telephony -> Extensions -> IP Extensions**

IP extensions are user extensions that can be registered on various SIP/IAX2 endpoints, including desktop IP phones, softphone for Windows/Android/iPhone/Linux and some other endpoints that support SIP/IAX2 protocol.

<input type="text" value="Name/Number/Depart"/> <input type="button" value="Add"/> <input type="button" value="Bulk Add"/> <input type="button" value="Bulk Edit"/> <input type="button" value="Delete Selected"/> <input type="button" value="Send QR Code"/> <input type="button" value="Export Quick Register Code"/> <input type="button" value="Export Extension"/> <input type="button" value="Import Extension"/>							
<div>Per Page 10</div>							
Name	Extension Number	Outbound CID	Email	Department Name	Quick Register Code	Dial Permission	Options
John Doe	100			dpt1	566	DialPlan1	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="QR"/> <input type="button" value="Phone"/>
101	101			dpt1	110	DialPlan1	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="QR"/> <input type="button" value="Phone"/>

The extensions are created through the quick setup wizard, to check or modify the extension properties please click the  button.

Edit 100
✕

User Profiles

Features

Advanced

Enable ?

On

Name

Password (Fair) ?

VXhFS_QCeI

Email ?

Outbound CID 1 ?

Music On Hold

default

Mobile Number

Dial Permission ?

DialPlan1

Language ?

English

Outbound CID 2 ?

Cancel

Submit

- **User Name:** Alias of this extension which can be the name of the extension user.
- **Password:** The password is used for the phones to register or by the extension user to sign in the extension web portal. This can be set manually or can be generated by the IPPBX system. Auto generated password consists of numbers, letters and special characters.
- **Email:** Email address of this extension user.
- **Outbound CID (1/2):** Outbound CID will be passed to the called party while calling through the VoIP or digital trunk (E1/T1/BRI) lines, you can define 2 CIDs for each extension and choose which to be used by dial rules. By default Outbound CID1 will be used by the dial rules. There's another Outbound CID option in the trunk settings, it has higher priority than the extension Outbound CID.
- **Music On Hold:** When the user holds a call, the caller will listen to music, and the music can be set up here.
- **Mobile Number:** The mobile phone number of the extension user.
- **Dial Permission:** Defines which type of numbers the extension can dial.
- **Language:** If the extension user is not a native speaker of the system default language, you may set a different language for this user.

Edit 100



User Profiles
Features
Advanced

Voicemail ?	<input checked="" type="checkbox"/> On	Voicemail Password ?	<input type="text" value="1234"/>
Remote Extension ?	<input type="checkbox"/> Off	Simultaneous Register Count ?	<input type="text" value="1"/>
Video Call ?	<input type="checkbox"/> Off	Video Codecs ?	<input type="text" value="H.264"/>
Web Portal ?	<input checked="" type="checkbox"/> On	Call Recording ?	<input type="text" value="Disabled"/>
Call Spy ?	<input type="checkbox"/> Off	Register Expiration ?	<input type="text" value="1800"/>
Pickup Group ?	<input type="text" value="12"/>	Whitelist ?	<input type="text" value="None"/>

Cancel
Submit

- **Voicemail:** Voicemail box could be enabled or disabled for this user.
- **Voicemail Password:** The password used to access voicemail by [voicemail feature codes](#).
- **Remote Extension:** If you want the extension can be used out of the LAN, this option needs to be enabled. Before doing this, please ensure the extension uses a strong password.
- **Simultaneous Register Count:** The extensions could be registered on up to 5 different SIP endpoints at the same time, by default the value is 2. When there are already 2 registers, the 3rd register will be responded with a 403 error.
- **Video Call:** You may enable/disable video call support of this extension.
- **Video Codecs:** Supported video codecs are H.261, H.263, H.263+, H.264, VP8.
- **Web Portal:** If enabled, users can use their extension number and password to login to the IPPBX system web GUI.
- **Call Recording:** This is an automated recording option, you may choose to automatically record the inbound, outbound or both inbound and outbound calls from/to this extension.
- **Call Spy:** Call Spy feature allows the phone calls of this extension to be monitored from other extensions, please refer to [Call Spy Feature Codes](#) for how to monitor phone calls. The dial permission used by the other extension needs to be enabled with Call Spy feature in the **Internal Permissions** section, otherwise call spy won't work.
- **Register Expiration:** Default register expiration time, default value 120 seconds.
- **Pickup Group:** Setting for extension pickup group, default value is 1 (1-64), please use ‘ , ’ to separate each group for multiple groups use.
- **Whitelist:** Incoming call whitelist, only the numbers on the whitelist are allowed to call into this extension.

Edit 100



User Profiles
Features
Advanced

Transport Protocol ? UDP
DTMF Mode ? RFC 4733

SRTP ? Off
Qualify(sec.) ? 300

NAT Support ? Off
IAX Extension ? Off

Permit IP ?
Qualify Timeout(sec.) 30

Send PAI ? Off
Send RPID ? Off

RTP Timeout ? 60
Inband Progress ? On

Available Codec
GSM
G.722
G.726
Speex
Opus

⇌

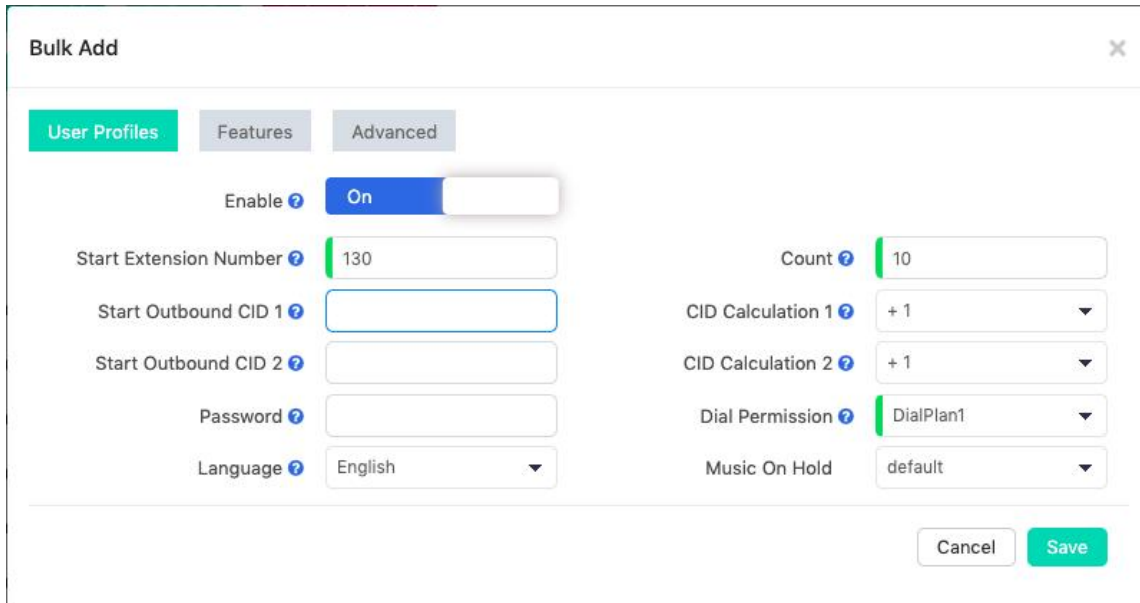
Selected Codec
Alaw
Ulaw
G.729

Cancel Submit

- **Transport Protocol:** The transport protocol to be used by SIP signaling. By default it uses UDP protocol, if you choose to use TCP or TLS please make sure the SIP IP phone or softphone uses the same protocol. Otherwise you'll get "403" error on SIP register.
- **DTMF Mode:** Defines how the system detects DTMF tones, the default setting is RFC4733, it can be changed if necessary.
- **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 SIP endpoint can also support SRTP.
- **Qualify (S):** The IPPBX system sends a SIP OPTIONS command regularly to check if the device is still online.
- **NAT Support:** Enable this option if extension user or the phone is behind a router.
- **IAX Extension:** Enable this option to activate IAX protocol support.
- **Permit IP:** Defines which IP address or network address (either private IP or public IP) is allowed to register to this extension, register coming from other addresses will be dropped.
- **Qualify Timeout (S):** If a qualify message is not responded by the SIP endpoint within the "Qualify Timeout", IP PBX system will consider the endpoint offline.
- **Send PAI:** Send the P Asserted Identity header. The P-Asserted-Identity contains the caller id information for the call on the INVITE SIP packet. Send the remote Party ID header. PAI and RPID are mutually exclusive you can set one or the other but not both.
- **Send RPID:** Send the Remote Party ID header. PAI and RPID are mutually exclusive you can set one or the other but not both.
- **RTP Timeout:** RTP timeout can be used to automatically hangup the call if no RTP traffic is received within 60 (default) seconds.
- **Inband Progress:** Set whether to send the ring tone via voice streaming.
- **Available Codec:** IPPBX system supports the following audio codecs G.711 (ulaw, alaw), G.722, G.726, G.729, GSM, Opus and Speex. You may choose the appropriate audio codecs from the **Available Codec** column and click to add to **Selected Codec** column.
- **Selected Codec:** Audio codecs you chose will be added here. The sequence of the audio codecs listed here is the sequence of the audio codecs to be used for negotiating the media of a phone call to be established.

If you want more extensions to be created or if you had skipped the quick setup wizard so no extension had been created, you may click on **Add** button to add a new extension or click on **Bulk Add** button to create bulk extensions.

The extensions' properties could be set while you are creating them.



Bulk Add

User Profiles | Features | Advanced

Enable ☒ On

Start Extension Number Count

Start Outbound CID 1 CID Calculation 1

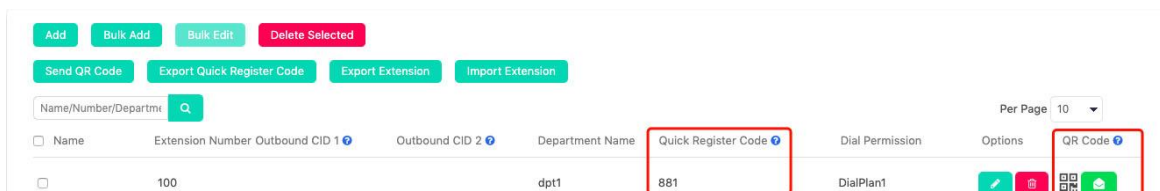
Start Outbound CID 2 CID Calculation 2

Password Dial Permission

Language Music On Hold

Cancel **Save**

- Define a **Start Extension Number** and the number of extensions to be created in the **Count** field.
- If you want to associate outbound CID numbers to the extensions, you'll need to specify the first CID number in the **Start Outbound CID (1/2)** field and in the **CID Calculation** field specify the calculating of the following CID numbers. Otherwise leave these fields blank.
- In the **Password** field you may leave it blank so the created extensions will use random passwords or you can define a password so the created extensions will share the same password.
- As for other options, you may configure accordingly per your demands. The features/options configured will be applied to all newly created extensions.
- As you can see there's a **QR code** and a **Quick Register Code** for each of the extensions.









Add Bulk Add Bulk Edit Delete Selected Send QR Code Export Quick Register Code Export Extension Import Extension							
Name/Number/Departm <input type="text" value=""/>							
<input type="checkbox"/> Name	Extension Number	Outbound CID 1	Outbound CID 2	Department Name	Quick Register Code	Dial Permission	Options <input type="text" value="Per Page 10"/>
<input type="checkbox"/>	100			dpt1	881	DialPlan1	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

4.3 Analog Extensions

Path: **Telephony -> Extensions -> Analog Extensions**

Analog extensions are generated automatically by the IPPBX system if FXS interfaces are detected. All you have to do is attaching analog phones or fax machine to the FXS interface, the analog extensions can be used directly for phone calls, no more additional settings required.

Departments		IP Extensions	Analog Extensions	Phone Provisioning		Expansion Box
Channel 	Extension 	Name	Department Name	Call Recordings	Dial Permission	Options
5	005	005		Disabled	DialPlan1	
6	006	006		Disabled	DialPlan1	
7	007	007		Disabled	DialPlan1	
8	008	008		Disabled	DialPlan1	
4 Total						

The **Channel** column and **Extension** column list the FXS interfaces and the corresponding extension numbers which are generated automatically by the IPPBX system.

You may click on the  button to change settings if necessary.

Edit 003

✕

Extension

003

Alias

003

Outbound CID ?

Operator

Call Recording ?

Disabled

Language ?

English

Dial Permission ?

DialPlan1

Input Volume ?

-10 0 10

Output Volume ?

-10 0 10

Cancel

Submit

- **Extension number** can be defined per your requirements.
- **Alias** can be defined to identify this analog extension.
- **Outbound CID** displays the number externally through digital trunk.
- **Call Recording** could be enabled to record Inbound, Outbound or Both direction phone calls if necessary.
- The **Language** option determines the language of the system prompts that the user will listen to/hear.
- **Dial Permission** controls which dial rules the user can use to make phone calls.
- **Input Volume** could be used to adjust the input gain of this analog extension.
- **Output Volume** could be used to adjust the output gain of this analog extension.

5 Inbound Control

Path: **Telephony -> Inbound Control**

The Inbound Control section is where you define how 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.

5.1 IVR

Path: **Telephony -> Inbound Control -> 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,".

Before configuring IVR menus you will first need to create inbound call destinations, for example, **Extensions**, **Departments** (ring groups), **IVR prompts**, **Call Queues**, etc.

If you want to create multi-layer IVR menus, you may need to create the sub-layers at first.

In order to create an IVR menu, please click on the  button, you'll see a popup dialog as below:

Add

Name

Welcome-1

Number ?

0601

Voice Prompts ?

welcome

Loop Count ?

1

Dial Extension ?

On

Dial Permission ?

Extension

Language ?

Default

Press Key Timeout(s)

3

Events ?

Invalid Key

Hangup

No Press

Hangup

Press 0

Extension

003[003]

Press 1

Extension

Please Select

Cancel

Submit

- In the **Name** field a name is required to identify this IVR menu.
- In the **Number** field a number had been created for this IVR menu for user being able to dial this number and test the IVR options.
- In **Voice Prompts** drop-down list, select a pre-recorded voice prompts for this IVR menu. The prompts will be played to the callers as they enter the IVR. The voice prompts must be uploaded or recorded from the **Audio Library -> IVR Prompts** page.
- In **Loop Count** drop-down list, select the number of times to playback this IVR prompts before callers pressing a key.
- **Dial Extension** switch could be enabled for callers to dial specific numbers upon this IVR menu if they already knew which number should be dialed, so the callers don't have to listen to all the options of this IVR.

- If **Dial Extension** is enabled a default **Dial Permission** named **Extension** will be applied for callers being able to dial internal extensions upon this IVR menu, if you wish callers could dial some more numbers you may select another dial permission here. (Not Recommended)
- **Language** option determines which language of system voice prompts the callers will hear if they landed on some inbound destinations that will play system voice prompts via this IVR menu, voicemail for example.
- **Press Key Timeout(s)**: The maximum interval time in seconds between pressing two keys.
- **Events** are the IVR options to be configured according to the instructions you have specified in the selected IVR prompts. Available key presses could be set from **0** to **9**, ***** and **#**. If the caller presses the key which are not specified and it will be handled by the "Invalid Key" option. And if the caller didn't press any key during the whole IVR process, the call will be handled by the "No Press" option.

5.2 Call Queue

Path: **Telephony -> Inbound Control -> 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 create a call queue, please click on the  button, a popup window will show up as below:

Add
✕

General Settings
Advanced Settings
Announcements

Call Queue Name
Support

Queue Number ?
0301

Ring Strategy ?
Ring All

Music On Hold ?
default

Agent Penalty ?
On

Static Agents ?
100[100] ✕ 101[101] ✕ 102[102] ✕

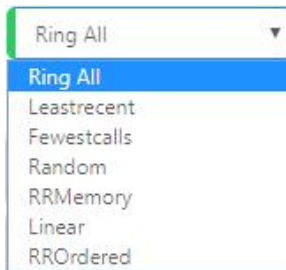
Dynamic Agents ?
103[103] ✕ 104[104] ✕ 105[105] ✕

Destination if no answer
Hangup

Cancel
Submit

First please complete the **General Settings**.

- In **Call Queue Name** field specify a name to identify this queue.
- In **Queue Number** field a default number is given. The number could be changed within the Paging Group Extension Number Range listed on **Telephony -> Preferences -> Global PBX Options** page, Extension Ranges section.
- **Ring Strategy** sets the method how you wish the queue agent extensions to ring when there's incoming call to this queue.

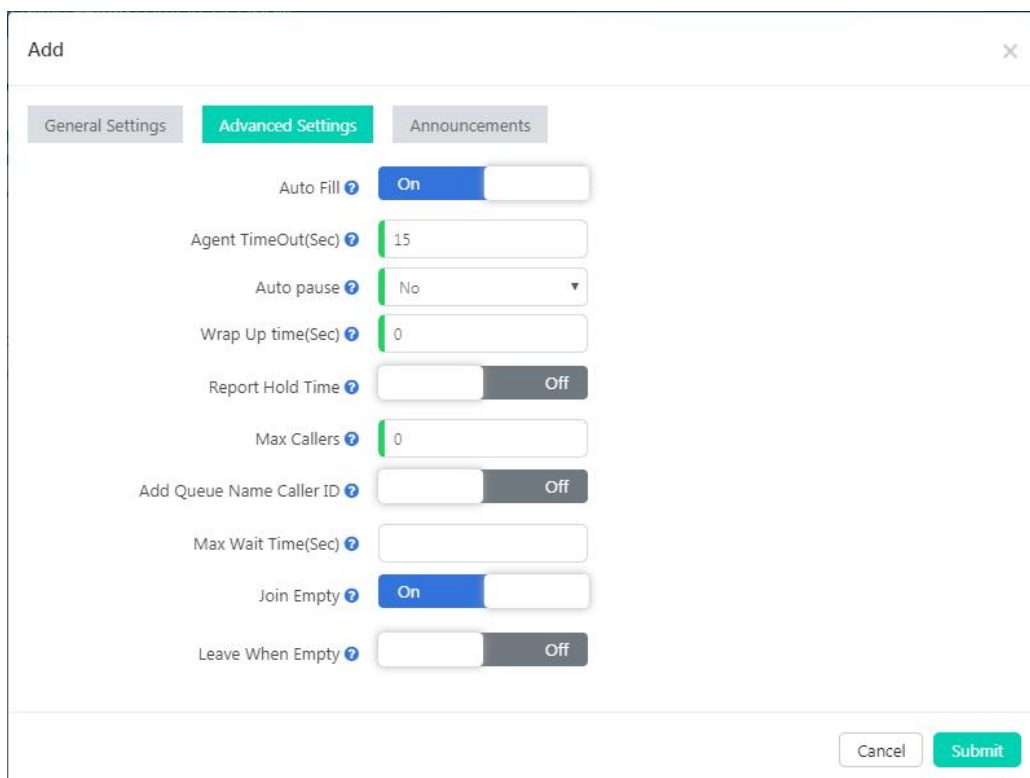


Ring All

- Ring All
- Leastrecent
- Fewestcalls
- Random
- RRMemory
- Linear
- RROrdered

- **Ring All:** Ring all available agents until one answers(default).
- **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:** The system remembers which agent was last called and begins the round robin with the next agent.
- **Linear:** Starting with the first agent, ring the extension of each agent in turn until the call is answered.
- **RROrdered:** Same as RRMemory, except the queue member order is preserved.
- In the **Music On Hold** drop-down list select a music folder as hold music when callers are waiting in the queue.
- After **Agent Penalty** is enabled, and the Ring Strategy is on the Linear mode, the incoming calls in the queue will ring the agents in the order of the static agent extension numbers list.
- **Static Agents** are extensions that are assumed to always be in the queue. Static agents do not need to “log in” to the queue, and cannot “log out” of the queue.
- **Dynamic Agents** are extensions that can log in and out of the queue. Extensions selected here will NOT automatically be logged in to the queue.
- **Destination if no answer** sets the final destination for the callers if no one answers the call when they were in the queue.

More advanced options for call queue is available, please click on [Advanced Settings](#) button to show advanced options, they are optional but might be useful to improve the callers' experiences.



Add

General Settings **Advanced Settings** Announcements

Auto Fill ☒ On

Agent TimeOut(Sec)

Auto pause

Wrap Up time(Sec)

Report Hold Time Off

Max Callers

Add Queue Name Caller ID Off

Max Wait Time(Sec)

Join Empty ☒ On

Leave When Empty Off

Cancel Submit

- **Auto Fill** if it's set to be Yes, and multiple agents are available, the PBX will send one call to each waiting agent (depending on the

ring strategy). Otherwise, it will hold all calls while it tries to find an agent for the top call in the queue, making the other callers wait.

- **Agent TimeOut** specifies the number of seconds to ring an agent's extension before sending the call to the next Agent (based on Ring Strategy).
- If an agent's extension rings and the agent fails to answer the call, **Auto Pause** option can automatically pause that agent to stop them receiving further calls from the queue.
- **Wrap Up time** is the amount of time in seconds that an agent has to complete work on a call after which the call is disconnected.
- If **Report Hold Time** is enabled, it will report to the agent about how long the caller had been waiting in the queue.
- The value of **Max Callers** limits the maximum amount of callers can wait in the queue (Default is 0 -- unlimited). When the maximum number of callers in the queue is reached, subsequent callers will be sent to the **If no answer** destination.
- If **Add Queue Name Caller ID** option is enabled, when an incoming call is distributed to an agent the queue name 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. This feature is helpful if an agent belongs to multiple call queues.
- Calls that have been waiting in the queue for **Max Wait Time(Sec)** will be sent to the **If no answer** destination. If left blank, there will not be any time limitation of waiting time.
- **Join Empty** option allows callers to enter the queue when no agents are available. If this option is not enabled, callers will not be able to enter the queue without available agents - callers will be sent to the **If no answer** destination.
- **Leave When Empty** option if it's enabled 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 no answer destination. This option cannot be used with Join Empty at the same time.

You may set the system to playback announcements to the callers while they are waiting in the queue. Please click on the [Announcements](#) button to setup customized announcements.

Add
×

General Settings
Advanced Settings
Announcements

Caller Position Announcements

Announce Hold Time ?
Once ▼

Announce Position ?
Off

Broadcast Frequency(Sec) ?
30

Periodic Announcements

Repeat Frequency(Sec) ?
0

Announcements Prompts ?
▼

Cancel
Submit

- **Caller Position Announcements** is used to tell the callers how they've been waiting and the position in the queue.
 - **Announce Hold Time:** Announce to the callers of the time they have been waiting, the first minute callers waiting in the queue will not hear such announcements.
 - **Announce Position:** If set to be Yes, the system will announce the position of the caller is currently waiting in the queue.
 - **Broadcast Frequency(Sec):** To defines how often to announce queue position and estimate hold time.
- **Periodic Announcements** can be used to periodically playback a voice prompts to the callers waiting in the queue.
 - Repeat Frequency(Sec): The time interval to repeat this periodic announcements.
 - Announcements Prompts: To select a voice prompts to be periodically played to the waiting callers.

After setting up call queue, you may use internal extensions (non-agent extensions) to call the queue number to verify the queue settings.

5.3 Time Conditions

Path: **Telephony -> Inbound Control -> Time Conditions**

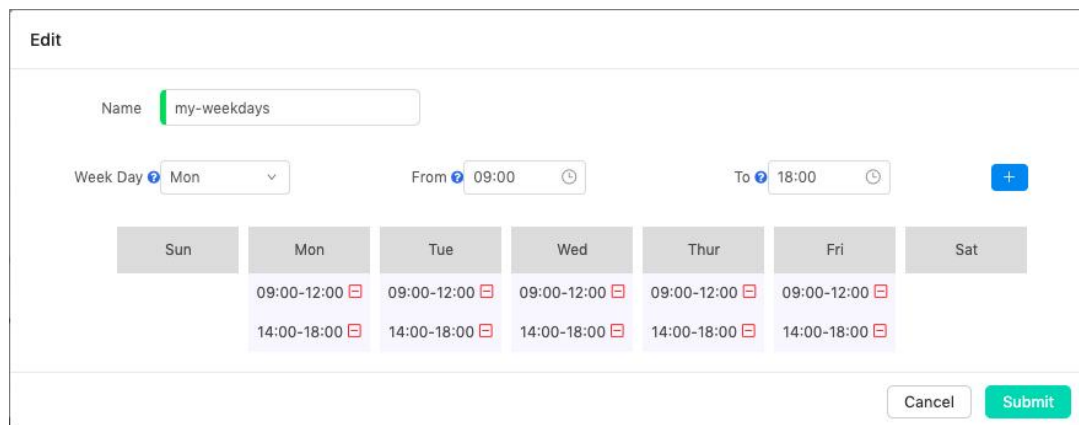
Time conditions in IPPBX allow you to control what happens to inbound calls both during and outside (weekends/holidays) normal business hours.

Time condition settings include Time Rule, Weekday and Holiday settings.

- Time Rule:
- Weekdays:
- Holidays:

To create a time rule you need first set up weekdays and holidays.

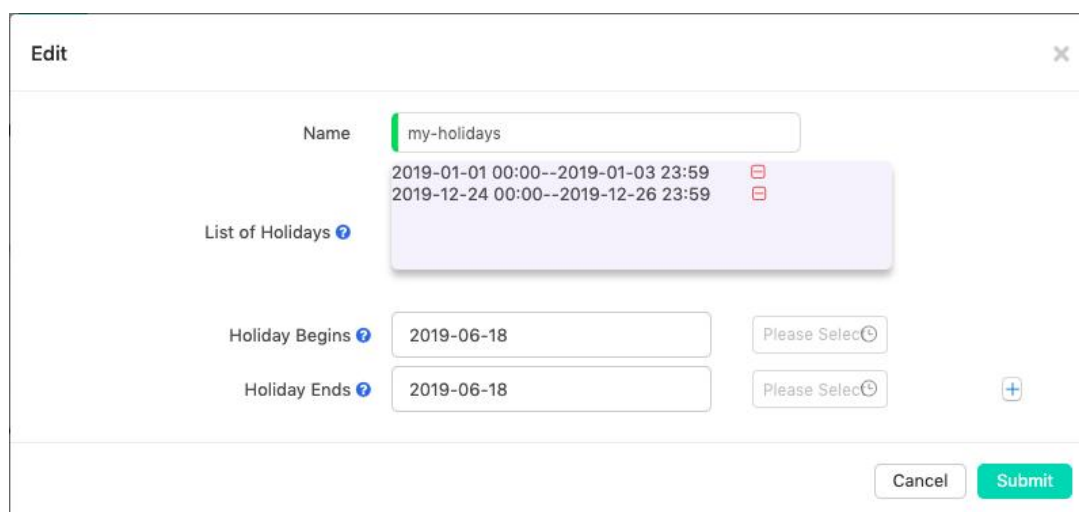
To set up weekdays you may modify the default one or create a new one by clicking on **Add** button.



The screenshot shows the 'Edit' form for a time condition named 'my-weekdays'. It includes a 'Week Day' dropdown set to 'Mon', 'From' and 'To' time pickers set to '09:00' and '18:00' respectively, and a calendar grid. The calendar grid shows time slots for Monday through Friday from 09:00-12:00 and 14:00-18:00. There are 'Cancel' and 'Submit' buttons at the bottom right.

This example shows the company opens from Monday to Friday. On each weekday, it opens from 9 am to 12 pm, after a 2-hour break then opens from 2 pm to 6 pm. Any other time duration unspecified will be considered as non-business hours.

In order to exclude holidays from the weekdays, you'll also have to set up holidays.



The screenshot shows the 'Edit' form for a time condition named 'my-holidays'. It includes a 'List of Holidays' section with a dropdown menu showing two holiday periods: '2019-01-01 00:00--2019-01-03 23:59' and '2019-12-24 00:00--2019-12-26 23:59'. Below this are 'Holiday Begins' and 'Holiday Ends' fields, both set to '2019-06-18', with 'Please Select' buttons next to them. There are 'Cancel' and 'Submit' buttons at the bottom right.

Please ensure you add all upcoming holidays to the holiday list.

Now you have all prerequisites to set up a time rule.

Add

Name
my-time-rule

Weekdays
my-weekdays

Business Hours
IVR
biz-hrs[0601]

Non-business Hours
IVR
no-biz[0602]

Holidays
my-holidays

Holiday destination
IVR
no-biz[0602]

Cancel
Submit

Now you could apply this time rule to the [Inbound Routes](#).

In the above example, there are only business hours and non-business hours for inbound calls. If you want inbound calls during your holidays to be handled by a holiday IVR, you could setup another IVR dedicated for holidays. And if you want to setup a time rule for noon-break, you can do it follow the instructions below.

In **Weekdays** section, setup noon-breaks for each weekday.

Add

Name
noon-break

Week Day
Fri
From
09:00
To
18:00

Sun
Mon
Tue
Wed
Thur
Fri
Sat

12:00-14:00
12:00-14:00
12:00-14:00
12:00-14:00
12:00-14:00

Cancel
Submit

Then create a new time rule as below.

Add

Name
noon-break

Weekdays
noon-break

Business Hours
IVR
noon-break-ivr[0603]

Non-business Hours
Time Rules
my-time-rule

Holidays
None

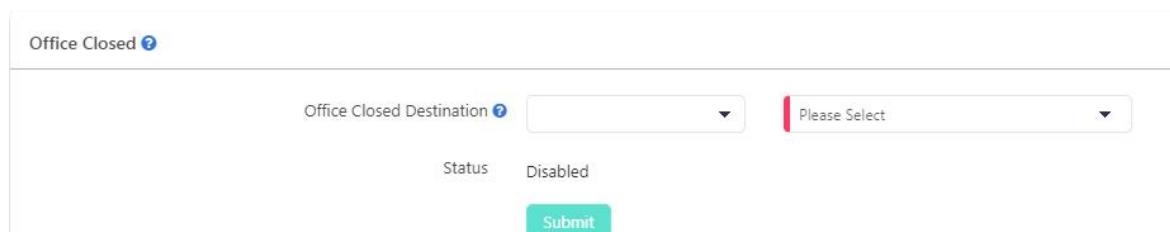
Cancel
Submit


In **Weekdays** field please select noon-break, and in **Business Hours** field please select a noon-break IVR or some other destination. In **Non-business Hours** field select the main time rule you have configured. And you should select **None** in the **Holidays** field. Then finally apply the noon-break time rule for inbound route settings.


5.4 Inbound Routes

Path: **Telephony -> Inbound Control -> Inbound Routes**

The Inbound Routes settings tell your IPPBX system where to send those inbound calls coming in from the trunks. Calls can be sent to a variety of destinations, including extensions, departments (ring groups), call queues, IVRs, DISAs, conferences, paging groups, voicemail, fax, etc.



Office Closed 





Office Closed Destination 

Status Disabled

Office Closed is an extending of time conditions, you can manually activate Office Closed 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 conditions. For the Office Closed feature codes and instructions, please refer to [Feature Codes](#).

Office Closed Destination is the destination of the inbound calls to be directed to while Office Closed timing is activated. You may select the destination per your requirements.

The Inbound Routes are configured per each trunk. You may set different inbound destinations for different trunks.

Trunk Name	Destination Type	Inbound Destination	Distinctive Ringtone	Options
<input type="checkbox"/> Trunk Name				
<input type="checkbox"/> FXO-1	Time Rules	my-time-rule		
<input type="checkbox"/> FXO-2	Time Rules	my-time-rule		
<input type="checkbox"/> FXO-3	Time Rules	my-time-rule		
<input type="checkbox"/> FXO-4	Time Rules	my-time-rule		

0 Selected / 4 Total

Please click on  button to configure inbound routes for each trunk.



Edit FXO-1 

Inbound Destination 

Distinctive Ringtone 

In the Inbound Destination field select a desired inbound destination for inbound calls from this trunk.

Distinctive Ringtone is optional, if needed, you may specify the ringtone name of the phone, so when the callers call in from this trunk the phone will ring this specific ringtone. It requires the phone support distinctive ringtone feature.

This is how you configure inbound routes for a trunk, you may configure the same inbound routes for other trunks or use different inbound route settings per your requirements.

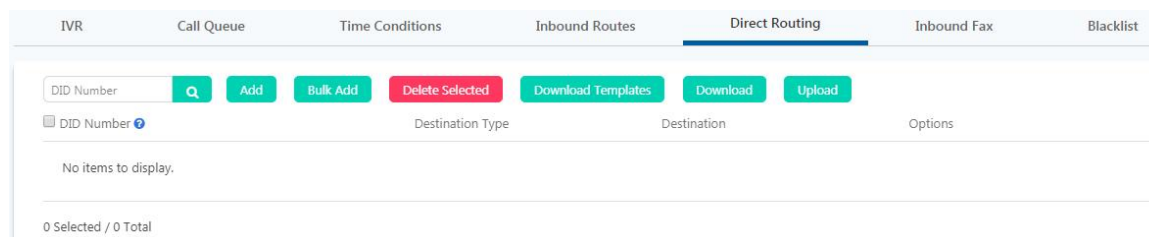
5.5 Direct Routing

Path: **Telephony -> Inbound Control -> Direct Routing**

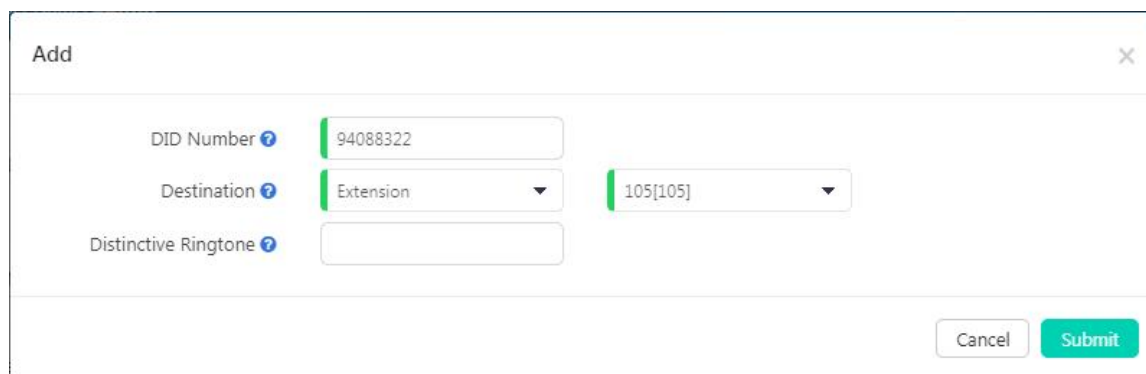
You may set up Direct Routing based on the DID numbers of your VoIP/E1/T1/BRI trunk lines and the phone numbers of the external callers. Direct Routing has higher priority than time conditions (unless the inbound destination is a time rule) and other general inbound routes.

Direct Routing based on DID numbers will cause the inbound calls which dialed the specified DID number to a specific call destination without the limitation of any other inbound settings.

To add a Direct Routing rule based on DID number, please click on the "Add" button as shown below.



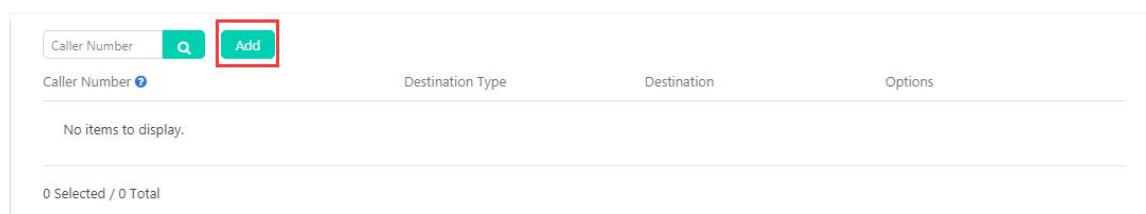
In the popup window, specify one of your DID numbers, and assign a call destination for all inbound calls by calling this DID number.



In the above example, 94088322 is one of your DID numbers, you may configure it with an extension number, when someone calls this number the call will then directly go to the selected extension.

In the **Distinctive Ringtone** field you may specify the ringtone name of the phone, so when the callers call the DID number and the call goes to this extension the phone will ring this specific ringtone. It requires the phone support distinctive ringtone feature.

To add a Direct Routing rule base on the caller's number, please click "Add" button as shown below.



In the popup window, specify the caller's number, and assign a call destination for inbound calls from this external phone number.

Add

Caller Number ?
69032354

Destination ?
Extension
106[106]

Cancel
Submit

Once this Direct Routing is created, all phone calls coming from the number 69032354 will then all go to extension 106, no matter when and from which trunk the call is coming in.

5.6 Inbound Fax

Virtual Fax feature on IPPBX system has the ability to automatically detect incoming fax and send the fax to one of the destinations as below:

- **Save to System**
- **Send as Email**
- **Fax Machine**

If the **Fax Destination** is set to **Save in System**.

Inbound Fax Settings

Fax Destination ?
Save to System

Submit

The received faxes will be saved in the IPPBX system internal storage. Admin user and operator user are able to check faxes on **Reports** -> **System Logging** -> **Fax Logs** page.

If the **Fax Destination** is set to **Send as Email**.

Inbound Fax Settings

Fax Destination ?
Send as Email

johndoe@gmail.com

Submit
Add Email

You'll have to give at least one Email address for the IPPBX to send the receive faxes to this Email address. Each fax will be attached to the Email in .tif format. And you can setup up to 5 email addresses as the fax receiver.

If your IPPBX system has been equipped with FXS ports, you may set the **Fax Destination** to **Fax Machine**.

Inbound Fax Settings

Fax Destination ?
Fax Machine

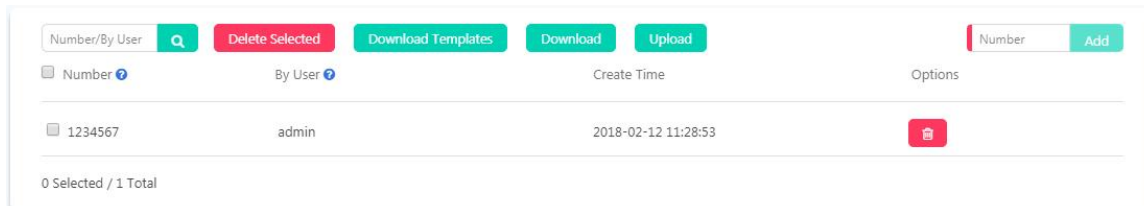
Please Select
005
006
007
008

In the dropdown list, select the analog (FXS port) extension number which has the fax machine attached. When inbound fax detected, it will be directed to the fax machine.

5.7 Blacklist

Path: **Telephony -> Inbound Control -> Blacklist**

Blacklist feature allows you to create a list of numbers that are not allowed to call in to the IPPBX system. Blacklist could be managed by both the admin user and operator user. The extension user could also add numbers to the system blacklist by using [Blacklist Feature Codes](#).



The screenshot shows the Blacklist management interface. At the top, there is a search bar labeled 'Number/By User' with a magnifying glass icon. To its right are buttons: 'Delete Selected' (red), 'Download Templates' (green), 'Download' (green), and 'Upload' (green). Further right is a text input field labeled 'Number' with an 'Add' button (green). Below these are columns: 'Number', 'By User', 'Create Time', and 'Options'. A table with one row is visible, containing the number '1234567', the user 'admin', the time '2018-02-12 11:28:53', and a red trash icon. At the bottom left, it says '0 Selected / 1 Total'.

By specifying a number in the top right number blank, you may add a number to the system blacklist.

To add blacklist numbers by using a template file, please click on [Download Templates](#) button to download the template file and edit with MS Excel, once done upload it from this page, the numbers you added in the template file will be added to the system blacklist.

If you want to share the blacklist numbers on other IPPBX systems, you may download it by clicking the [Download](#) button to download all blacklist numbers in a file and upload on other IPPBX systems.

6 Outbound Control

By default if you've not configured any outbound control settings, the extension users are not able to make outbound phone calls yet. Please follow the instructions of this chapter to configure the IPPBX system for outbound phone calls.





6.1 Trunks


A trunk on an IPPBX system is essential for extensions to be able to make outbound phone calls. On IPPBX system, the trunks will be detected and generated automatically at the first time of the system initialization.

6.1.1 FXO/GSM Trunks

Path: **Telephony -> Outbound Control -> 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.

Physical Trunks Bulk Edit			
Trunk Name	Remark	Type	Options
<input type="checkbox"/> FXO-1		Analog	
<input type="checkbox"/> FXO-2		Analog	
<input type="checkbox"/> FXO-3		Analog	
<input type="checkbox"/> FXO-4		Analog	
0 Selected / 4 Total			

If needed you may edit the trunk settings by click on the  button, or you may select the same type of trunks and click on Bulk Edit button to edit settings of the trunks together.

Edit FXO-1

Call Recording ?
Disabled

Output Volume ?
-10 0 10

Input Volume ?
-10 0 10

Answer Polarity Detection ?
Off

Hangup Polarity Detection ?
Off

Fax Detect ?
Off

Caller ID Signaling ?
Default

Remark

Prompts Language ?
English

Busy Count ?
3

Busy Pattern ?

Busy Detection ?
On

Quick Send Number ?
Off

Caller ID Start ?
Default

Cancel Submit

Select the parameters you want to configure before modifying them. Usually if the trunks are working fine please do not change these settings.






- **Call recording:** To enable or disable call recording on the trunk/trunks. To enable recording you have options to record inbound calls only, outbound calls only or both inbound and outbound calls.
- **Output Volume:** Sets the volume of the outgoing calls from the FXO channels.

- **Input Volume:** Sets the volume of the incoming calls from the FXO channels.
- **Answer Polarity Detection:** When enabled, FXO (FXS signaled) ports watch for a polarity reversal to mark when an outgoing call is answered by the remote party.
- **Hangup Polarity Detection:** In certain countries, a polarity reversal is used to signal the disconnection of a phone line. If enabled, the calls will be considered "hang up" on a polarity reversal.
- **Fax Detect:** Enable or disable fax auto detection on this trunk.
- **Caller ID Signaling:** Setup caller ID signaling for this trunk line instead of using global caller ID signaling.
- **Prompts 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.
- **Busy Count:** Specify how many busy tones to wait for before hanging up, and it's configurable only if Busy Detection is enabled.
- **Busy Pattern:** If busy detection is enabled, it is also possible to specify the cadence of your busy signal.
- **Busy Detection:** Enable busy tone detection, it is also possible to specify how many busy tones to wait for before hanging up.
- **Quick Send Number:** When enabled, your calls will get through faster, as all numbers sent through this trunk will always be added with "#" at the end, it will cause the carrier to switch the calls immediately instead of waiting till digits timeout.
- **Caller ID Start:** Caller ID detection option for this trunk instead of using global settings. For more information please refer to [Analog Settings](#).

6.1.2 E1 Trunks

Path: **Telephony -> Outbound Control -> Trunks**

If your PBX-C302 or PBX-C503 IPPBX system has E1 module installed, you'll have an E1 trunk available for inbound and outbound phone calls.

Physical Trunks Bulk Edit			
Trunk Name	Remark	Type	Options
<input type="checkbox"/> FXO-32		Analog	
<input type="checkbox"/> FXO-33		Analog	
<input type="checkbox"/> FXO-34		Analog	
<input type="checkbox"/> FXO-35		Analog	
<input type="checkbox"/> PRI-1		Digital	

0 Selected / 5 Total

Click on the  button to configure the E1 (PRI) trunk when needed.

Edit PRI-1

Remark

Call Recording ?

Disabled

Outbound CID

Pri Indication

Inband

Prompts Language ?

English

Dial Permission

Default

Quick Send Number ?

Off

Overlap Dial

Yes

Reset Interval

3600

Switch Type

EuroISDN (common in Europe)

Fax Detect ?

On

Preferred Outbound CID ?

Extension

Cancel









Submit

- **Call recording:** To enable or disable call recording on the trunk/trunks. To enable recording you have options to record inbound calls only, outbound calls only or both inbound and outbound calls.
- **Overlap Dial:** Overlap dialing mode (sending overlap digits).
- **Outbound CID:** The number you want to display to the called party.
- **Reset Interval:** To set the time in seconds between restart of unused B channels.
- **Pri Indication:** To enable this to report Busy and Congestion on a PRI using out-of-band notification.
- **Switch Type:** To set the type of PRI switch being used by the telephony provider.
- **Prompts Language:** Custom a system voice prompts language for the callers calling in from this trunk.
- **Fax Detect:** Enable/disable fax detection on this trunk.
- **Dial Permission:** Custom dial permission for this trunk, by default it uses the "Extension" dial permission. Configure only if this trunk is used for PBX 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.
- **Preferred outbound CID:** To set preferred outbound CID of this trunk of the extensions.
- **Quick Send Number:** When enabled, your calls will get through faster, as all numbers sent through this trunk will always be added with "#" at the end, it will cause the carrier to switch the calls immediately instead of waiting till digits timeout.

6.1.3 BRI Trunks

Path: **Telephony -> Outbound Control -> Trunks**

If your PBX-C302 or PBX-C503 IPPBX system has 4BRI module installed, you'll have 4 BRI trunks available for inbound and outbound phone calls.

Physical Trunks Bulk Edit			
Trunk Name	Remark	Type	Options
<input type="checkbox"/> FXO-13		Analog	
<input type="checkbox"/> FXO-14		Analog	
<input type="checkbox"/> FXO-15		Analog	
<input type="checkbox"/> FXO-16		Analog	
<input type="checkbox"/> BRI-1		Digital	
<input type="checkbox"/> BRI-2		Digital	
<input type="checkbox"/> BRI-3		Digital	
<input type="checkbox"/> BRI-4		Digital	
0 Selected / 8 Total			

Click on the  button to configure the BRI trunk when needed.

Edit BRI-1

Remark	<input type="text"/>	Overlap Dial	<input type="text" value="Yes"/>
Call Recording	<input type="text" value="Disabled"/>	Reset Interval	<input type="text" value="3600"/>
Outbound CID	<input type="text"/>	Switch Type	<input type="text" value="EuroISDN (common in Europe)"/>
Pri Indication	<input type="text" value="Inband"/>	Fax Detect	<input type="text" value="On"/>
Prompts Language	<input type="text" value="中文"/>	Preferred Outbound CID	<input type="text" value="Extension"/>
Dial Permission	<input type="text" value="Default"/>		

Cancel
Submit

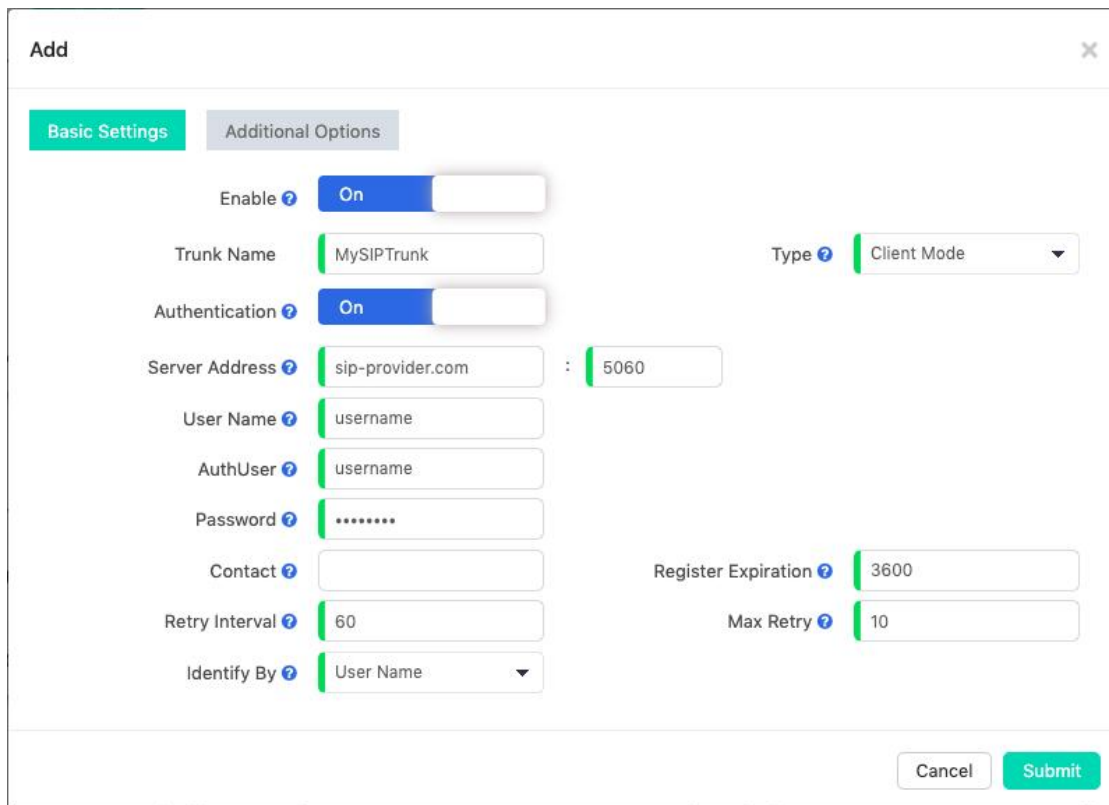
- **Call recording:** To enable or disable call recording on the trunk/trunks. To enable recording you have options to record inbound calls only, outbound calls only or both inbound and outbound calls.
- **Overlap Dial:** Overlap dialing mode (sending overlap digits).
- **Outbound CID:** The number you want to display to the called party.
- **Reset Interval:** To set the time in seconds between restart of unused B channels.
- **Pri Indication:** To enable this to report Busy and Congestion on a BRI using out-of-band notification.
- **Switch Type:** To set the type of PRI switch being used by the telephony provider.
- **Prompts Language:** Custom a system voice prompts language for the callers calling in from this trunk.
- **Fax Detect:** To enable/disable fax detection on this trunk.
- **Dial Permission:** Custom dial permission for this trunk, by default it uses the "Extension" dial permission. Configure only if this trunk is used for PBX 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.
- **Preferred outbound CID:** To set preferred outbound CID of this trunk of the extensions.

6.1.4 SIP Trunks

Path: **Telephony -> Outbound Control -> Trunks**

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

To implement your SIP trunk account on the IPPBX system, you'll need to create a SIP trunk.



Most of the trunk settings will be given by the service provider, settings that are not mentioned by the provider you may leave them blank or use default values.

- **Enable:** The trunk will be active and usable only if it's enabled.
- **Authentication:** If the service provider doesn't require a username and password for this account to register to their server then you can disable this option.
- **Server Address:** The SIP server domain or IP address.
- **User Name:** Username provided by SIP Provider.
- **AuthUser:** AuthUser is the optional authorization user for the SIP server.
- **Password:** Password provided by SIP Provider.
- **Contact:** Contact user to use in an outbound call request through this trunk.
- **Retry Interval:** Once registration expired, retry interval is the number of seconds system will wait before attempting to send another register request to the server.
- **Identify By:** Identify by the user name and domain or the Authorization username.
- **Type:** In practical applications, client mode SIP trunks are the most commonly used to connect to the SIP providers for low cost, long distance and international phone calls, while server mode is only used when users want to do SIP trunking between IPPBXs.
- **Registration Expiration:** Expiration time of registration in seconds.
- **Max Retry:** Defines how many times the IPPBX system will attempt to register to the server before permanently giving up.

More advanced settings.

Add

Basic Settings
Additional Options

Fax Detect ? ☐ Off

SRTP ? ☐ Off

Client URI ?

Server URI ?

AOR Contact ?

Call Recording ? Disabled

From User ?

From Domain ?

DTMF Mode ? Auto

Send PAI ☒ On

RTP Timeout ? 60

Qualify ? 120

NAT Support ? ☐ Off

Transport Protocol ? UDP

Prompts Language ? English

Simultaneous Call ?

Preferred Outbound CID ? Extension

Outbound CID ?

Dial Permission ? Default

Video Codecs ? None

Send RPID ☐ Off

Available Codec

GSM

G.722

G.726

Speex

Opus

Selected Codec

Ulaw

Alaw

G.729

Cancel Submit

- **Fax Detect:** Enable/disable fax detection on this trunk.
- **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.
- **Client URI:** Client SIP URI used when attempting outbound registration (e.g. SIP:1234567890@sip.example.com:5060).
- **Server URI:** SIP URI of the server to register against (e.g. sip:sip.example.com:5060).
- **AOR Contact:** Address of records, it uses the same format as the client URI.
- **Call Recording:** Enable/disable call recording on this trunk. If enabled, all phone calls going in or out will all be recorded.
- **From User:** Username to use in "From" header for sending outbound call requests to this trunk.
- **From Domain:** Your service provider's domain name.
- **DTMF Mode:** Used to inform the system how to detect the DTMF key press. Choices are Inband, rfc4733, SIP info and Auto.
- **Send PAI:** Send the P Asserted Identity header. The P-Asserted-Identity contains the caller id information for the call on the INVITE SIP packet. PAI and RPID are mutually exclusive you can set one or the other but not both.
- **RTP Timeout:** RTP Timeout can be used to automatically hangup the call if not RTP traffic is received within 60 (default) seconds.
- **Qualify:** Qualify will cause the server sending SIP OPTIONS command regularly to check that the device is still online.
- **NAT Support:** 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.

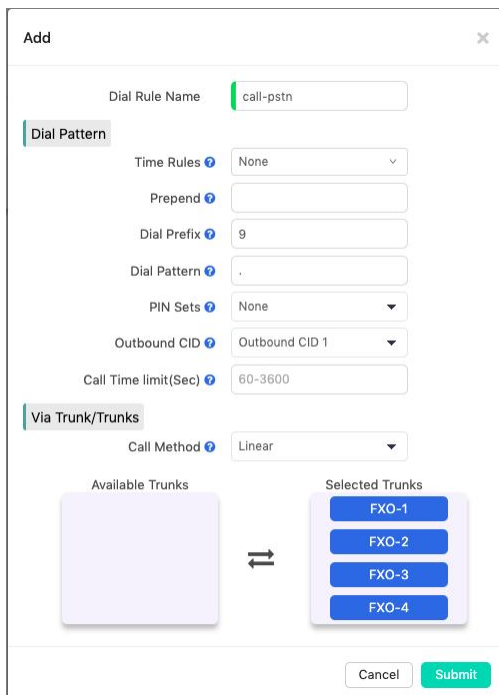
- **Transport Protocol:** To set the VoIP trunk to use UDP, TCP or TLS as the transport protocol, in most cases the providers use UDP as default transport protocol.
- **Prompts Language:** You can choose a desired language of the system voice prompts to play for the incoming calls from this trunk. For 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.
- **Simultaneous Calls:** This option will limit the number of simultaneous outbound calls can be made through this trunk, leave it blank as not limited.
- **Preferred Outbound CID:** To set preferred outbound CID of this trunk of the extensions.
- **Outbound CID:** The number you want to display to the called party while dialing out through this trunk. It depends on the service provider whether it works or not.
- **Dial Permission:** Custom dial permission for this trunk, by default it uses the "default" dial permission. 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.
- **Video Codecs:** If the ITSP supports video calls then you can enable compatible video codecs here for video phone calls.
- **Send RPID:** Send the Remote Party ID header. PAI and RPID are mutually exclusive you can set one or the other but not both.
- **Available Codec:** IPPBX system supports the following audio codecs G.711 (ulaw, alaw), G.722, G.726, G.729, GSM, Opus and Speex. You may choose the appropriate audio codecs from here and click to add to Selected Codec.
- **Selected Codec:** Audio codecs you chose will be added here. The sequence of the audio codecs listed here is the sequence of the audio codecs to be used for negotiating the media of a phone call to be established.

6.2 Dial Rules

Path: **Telephony -> Outbound Control -> Trunks**

On the IPPBX system you can setup different dial rules, for users to dial numbers in different format/pattern and cause the IPPBX system to call out through different trunk lines. For example, users dial the numbers with a prefix 9 to call out through the CO lines (land lines). Or dial the numbers with a prefix 00 to call out through the VoIP lines (SIP trunks).

Click on  button to create a dial rule, below is an example dial rule.



- First of all in the **Dial Rule Name** field specify a name to identify this dial rule.
- In the **Time Rules** dropdown list, you may select a time condition for this dial rule, so this dial rule will only be available to be used at business hours.
- **Prepend** option is used to always add specific digit/digits in front of the actual dialed number after the **Dial Prefix** is deleted. These extra digits will be sent along with the actual number to the service provider to exchange. For example, if you want to always add an area code in front of the dialed number, you can specify the area code in front of the dialed number, you can specify the area code here, otherwise leave this field blank.
- **Dial Prefix** is the first digit users have to dial while they want to make calls through the trunk/trunks selected in this dial rule. The system will strip the prefix from the number that is sent to the trunk.
- **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*.
- **Pin Set** is a collection of PIN codes for granting outbound phone calls.
- **Outbound CID**: Choose between Outbound CID1 and Outbound CID2 to send to the called party. When the extension user make outbound phone calls by using this dial rule, the chosen outbound CID number will be used. So in the below **Selected Trunks** field VoIP or E1/T1/BRI trunks need to be used, and the service provider need to support users passing outbound CIDs.
- **Call Time Limit**: The limited time of call conversation can be made while using this dial rule. The limitation can be set from 60 to 3600 seconds.
- **Call Method** sets how to use the selected trunks for outbound phone calls.
 - **Linear**: Always take the first available trunk, if the first trunk is busy it will try the second trunk, if the second trunk is busy it will try the third, and so on.
 - **Linear Cycle**: Always take the next trunk, the trunk which the last had taken will not be used, it will call out through the next one directly.
- Double click one of the trunks or drag-and-drop to move the trunks from **Available Trunks** field to **Selected Trunks** field. The selected trunks will be used by this dial rule for outbound phone calls.

Notice

If you want all users to use the same dial rule for outbound phone calls, a dial prefix may not be necessary. But please make sure all available trunks should be included in the **Selected Trunks** field, otherwise unselected trunks will never be used.


If you want to set different dial rules please make sure the dial rules use different dial prefixes.

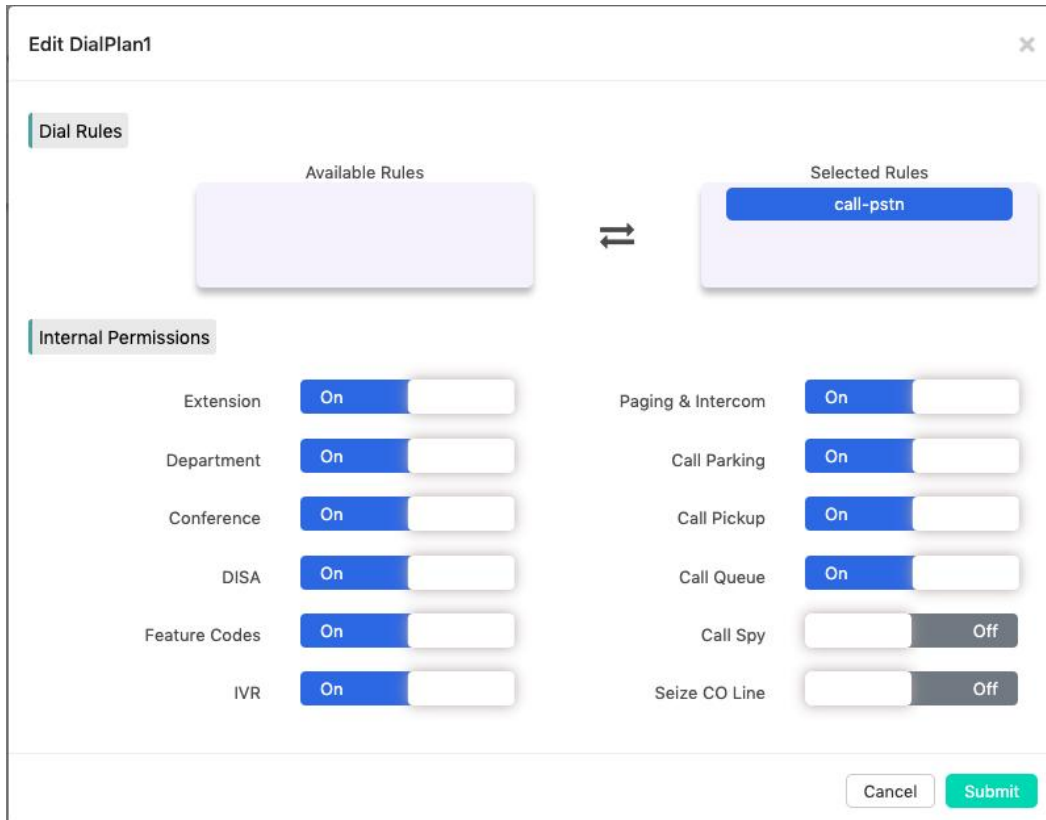
6.3 Dial Permissions

Path: **Telephony -> Outbound Control -> Dial Permissions**

A dial permission consists of outbound dial permissions (dial rules) and internal dial permissions. Each extension number had been assigned with a dial permission. Dial rules are created for dial outbound phone calls, internal dial permissions are used for controlling extension number from using local phone system features.

You may create several different dial permissions. By assigning the extension numbers with different dial permissions you may limit the extension users to dial certain outbound phone calls and use certain local phone system features.

Click on  button to create a new dial permission or you may use the default dial permission.



- In the **Dial Rules** section by moving the dial rules from the **Available Rules** field to the **Selected Rules** field to enable the dial rules in this dial permission. In the above given example, 2 dial rules had been enabled. The “call-pstn” rule is used to make phone calls through CO lines (land lines). The “call-voip” rule is used to make phone call through the SIP trunk. So if you assign this dial permission to the extension users, they will be able to make outbound phone call both through CO lines and the SIP trunk.
- In the **Internal Permissions** section by switching the internal call features on/off to enable/disable the call features.
 - **Extension:** Allow/Disallow dialing other extension numbers.
 - **Paging & Intercom:** Allow/Disallow dialing paging & intercom group numbers.
 - **Department:** Allow/Disallow dialing other department numbers.
 - **Call Parking:** Allow/Disallow answering the parked calls.
 - **Conference:** Allow/Disallow using conference feature.
 - **Call Pickup:** Allow/Disallow pickup phone calls on other extensions.
 - **DISA:** Allow/Disallow using DISA feature.
 - **Call Queue:** Allow/Disallow dialing the call queue numbers.
 - **Feature Codes:** Allow/Disallow using feature codes.
 - **Call Spy:** Allow/Disallow spying on other extensions’ phone calls.
 - **IVR:** Allow/Disallow dialing IVR extensions.
 - **Seize CO Line:** Allow/Disallow the extension user to dial the FXO trunk BLF code to seize the line and make outbound phone call directly.


By default all extensions use the default dial permission “DialPlan1”, if you have created new dial permissions, please don’t forget to assign them to the extensions from **Telephony -> Extensions -> IP Extensions** and **Telephony -> Extensions -> Analog Extensions** (if there are analog extensions) page.


6.4 Outbound Fax


Path: **Telephony -> Outbound Control -> Outbound Fax**

Virtual Fax feature on IPPBX system has the ability to send faxes.

Outbound Fax Settings

Send Fax 

Dial Permission 

Outbound CID 

- **Send Fax:** Enable or disable outbound fax function.
- **Dial Permission:** The dial permission limits what kind of numbers can be dialed, in other words, it also limits what numbers the system can be used to send fax to.
- **Outbound CID:** Pass this number to the called party while sending fax through VoIP or digital(E1/T1/BRI)lines.

Test Fax

Fax Number 


You can send a test fax to a number by inputting in the blank of **Fax Number**. This number is only used to send a test fax to verify outbound fax works.

6.5 PIN Sets


Path: **Telephony -> Outbound Control -> PIN Sets**

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

Each PIN Set consists of a series of PIN Codes.

Add 

Name

PIN List 

The PIN codes could be any digits that you want, but usually recommended it to be 3 to 5 digits meaningless numbers.

You could distribute these PIN codes out to each of the extension users or several of them to share a same PIN per your demand. If the PIN set is implemented on a dial rule or DISA, the IPPBX system will ask them to enter one of those PIN codes before they can call out.

The PIN codes also can be used to query call logs and recordings, so even if the extension user dialed a number from another extension if PIN code is used you'll know who actually made that call.

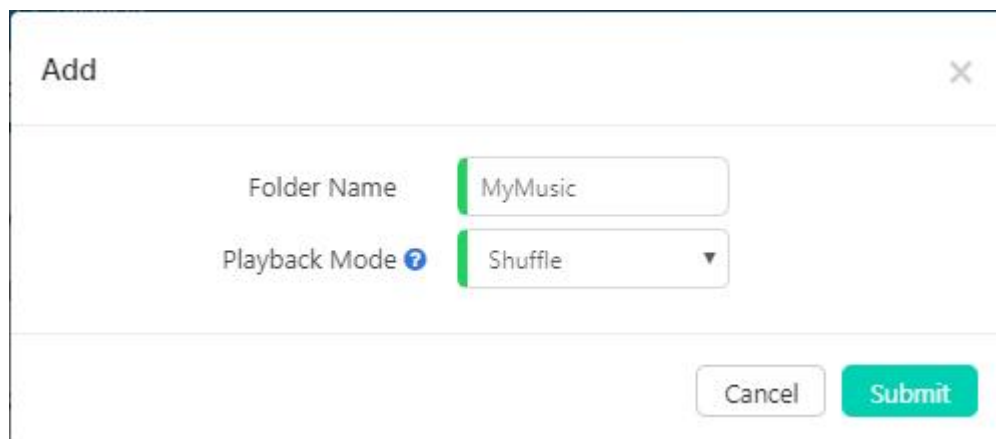
7 Audio Library

7.1 Music On Hold

Path: **Telephony -> Audio Library -> Music On Hold**

Music On Hold (MOH) is 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.

Audio files are managed by folder basis. You may use the system default MOH folder as on hold music or you may create new folders and upload your custom music files. Please first click on "Create New Folder" to create a new MOH folder.



Give this folder a name and set the playback mode as shuffle (random playback) or in turn (playback in order). Once done click on "Submit".

Now click on  button to upload audio files to the newly created folder one by one.

Supported File Format: MP3, WAV(8KHz, 16bit, Mono)

7.2 IVR Prompts

Path: **Telephony -> Audio Library -> IVR Prompts**

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

Always be sure that the recorded IVR prompts will match the options to be set up in the IVR. If you change your IVR options, don't forget to change your recording!

The IVR prompts are pre-recorded and then uploaded to the IPPBX system.

Music On Hold


























IVR Prompts

Other Custom Prompts

IVR Prompts ?

Upload


Record

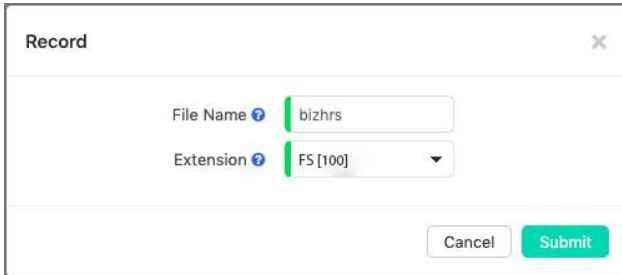
File	Format	Play ?	Options
 closed	wav	 	 
 closed_cn	wav	 	 
 welcome	wav	 	 
 welcome_cn	wav	 	 
 biz-hrs	wav	 	 

5 Total

The pre-recorded audio could be MP3 or WAV (16bit, 8KHz, Mono) format.

After uploading, you may playback on the web by clicking  button or playback on a phone by clicking on the  button.

If you want to record the voice prompts by using an IP phone extension, please click on the  button, in the pop-up dialog, please define a name for the audio file to be recorded and select an extension which will be used to do the recording.



The image shows a 'Record' dialog box with a close button (X) in the top right corner. It contains two input fields: 'File Name' with the value 'bizhrs' and 'Extension' with a dropdown menu showing 'FS [100]'. At the bottom right, there are two buttons: 'Cancel' and 'Submit'.

When done, click on Submit and the selected extension will ring. After the user pickup the phone, please follow the system voice prompts to complete the recording. When recording is done, the newly recorded audio will be listed on this page and ready to be used for setup IVR.

7.3 Custom Prompts

Path: **Telephony -> Audio Library -> Other Custom Prompts**

Custom prompts are to be used by call queue, call forward and some other advanced features, where customized voice prompts required.

You could record the voice prompts in MP3 or WAV (16bit, 8000Hz, mono) format and upload here. Then when you setup call queue periodic announcements you could select the customized voice prompts, or when you setup call forward notify message you could set the IPPBX system to notify callers before forwarding their calls.


8 Advanced Features

8.1 Call Forward

Path: **Telephony -> Advanced Features -> Call Forward**

Call forward allows calls to an extension to be forwarded to a specific internal extension number or an external phone number. According to different application scenario, the forward type can be set as Forward All, Forward on Busy, Forward When Unavailable, No Answer and Busy, or No Answer and Unavailable.

Advanced Options

Notify Caller before Forwarding  Off

[Save](#)

- **Notify Caller before Forwarding** option allows you to choose a voice prompts to be played to the caller to notify caller that the call will be forwarded. The voice prompts is uploaded from **Telephony -> Audio Library -> Other Custom Prompts** page. If this option is not enabled, the call will be forwarded without notifying the caller.

To configure call forward please click on the [Add](#) button. And follow the explanations to complete the configurations as below.

Add

Extension Number

100(John Doe)

Forward Type

Forward On Busy

Destination

965302385

Enable





On

Cancel
Submit

- In the **Extension Number** drop-down list select the extension to be configured with call forward.
- In **Forward Type** drop-down list select the condition of when to forward the incoming calls.
- In the **Destination** field specify the number to receive the forwarded phone calls. If it's another internal extension number, just fill in with that extension number. If it's an external number, you'll have to specify the dial prefix in front of the actual number. In this case, the actual number is 65302385, the dial prefix is 9.

In the forward list, you may disable or enable items based on requirements.

[Add](#)
[Activate Selected](#)
[Deactivate Selected](#)
[Delete Selected](#)

Extension	Forward Type	Destination	Options
104	Always	105	  <div>Off</div>
131	Always	965302387	  <div>On</div>

0 Selected / 2 Total

Call forward could be configured by Admin user and the operator user, and even by extension user from extension user web portal or by extension users from their phones by feature codes, please refer to [Call Forward feature codes](#).

8.2 Follow Me

Path: **Telephony -> Advanced Features -> Follow Me**

The Follow Me feature allows you to set a list of numbers for an extension number that the extension user may possibly be contacted on. Therefore, if someone calls the extension and the user is not available then Follow Me will work through the list calling each of the

numbers in turn until the user is contacted or the list is exhausted.

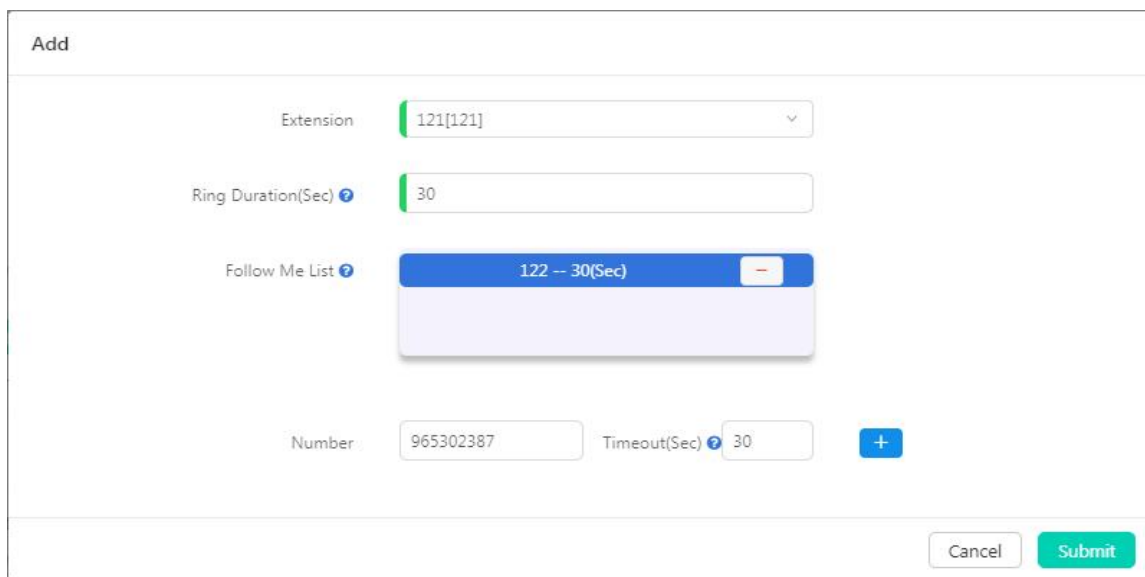
Before configuring Follow Me there are 2 advanced options you may want to know about.



The 'Configure' window shows two toggle switches: 'Always Take Call' is set to 'On' and 'Record Caller Name' is set to 'Off'. A green 'Save' button is at the bottom.

- **Always Take Call:** If enabled the forwarded call will be answered directly by a destination number, if disabled, when the forwarded call reaches the destination number, IPPBX system will give the destination number choices to decline or answer the call.
- **Record Caller Name:** Ask the caller to say his/her name and record the name, so it can be announced to each destination number.

Add a follow me feature like below.



The 'Add' window contains the following fields: 'Extension' (dropdown menu showing '121[121]'), 'Ring Duration(Sec)' (input field with '30'), 'Follow Me List' (a list box containing '122 -- 30(Sec)' with a minus button), 'Number' (input field with '965302387'), and 'Timeout(Sec)' (input field with '30' and a plus button). At the bottom right are 'Cancel' and 'Submit' buttons.


- Select the **Extension** which will be configured with Follow Me.
- **Ring Duration (Sec):** To set the time in seconds to ring the extension before Follow Me process starts.
- **Follow Me List:** The list of numbers to be reached in order.
- **Number and Timeout (Sec):** The number to be reached and the time to ring this number before trying the next one. If the number is an external number, don't forget to add a dial prefix in front of it.

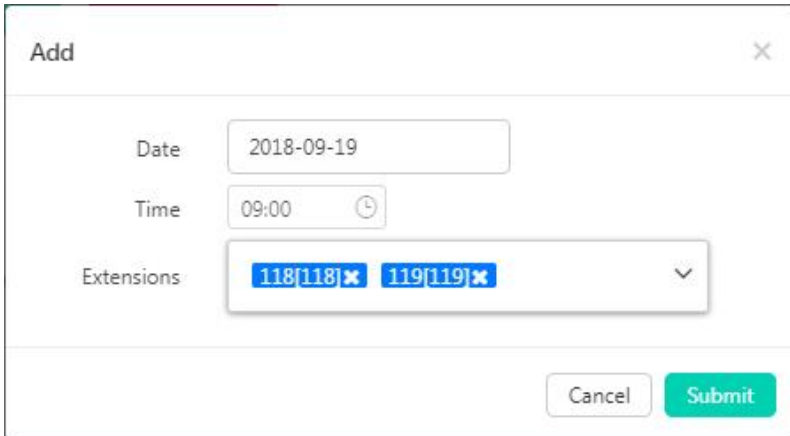
Take the above settings as example, when extension 121 gets an incoming call, if it's not answered in 30 seconds, the call will be forwarded firstly to 122 and ring this extension for 30 seconds, if still not answered, it will try number 65302387 (9 is the dial prefix, not part of the number) for another 30 seconds. If extension 122 answered the call then 65302387 will not be called. If the call didn't answer by any of the numbers listed in **Follow Me List**, the Follow Me process will end and the caller will be disconnected.

8.3 Wake Up Call

Path: **Telephony -> Advanced Features -> Wake Up Calls**

Wake Up Call feature could be used to schedule reminders to the user extensions. Wakeup calls could be scheduled by admin user from admin Web interface, by operator user from operator Web interface, or could be scheduled by extension users by dialing [Wake Up Call feature codes](#).

To schedule a wakeup call from admin user Web interface, please click on  button, in the popup window set the time of the wakeup call and select the extension/extensions to be called at the scheduled time point.



- Click on **Date** field to schedule the date for the wakeup call.
- Click on **Time** field to schedule the time for the wakeup call.
- In **Extensions** field you could select one or more extensions as you want.

When it's time for wakeup call, IPPBX system will ring the selected extension/extensions. After user answering the wakeup call, IPPBX system will let user "**Confirm**" wakeup call. If user press a key to confirm wakeup call then the schedule is completed.

If a wakeup call is not answered, system will try to ring back in the next minute, and will retry 2 times, after which system will consider the wakeup call completed.

8.4 Conference

Path: **Telephony -> Advanced Features -> 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.

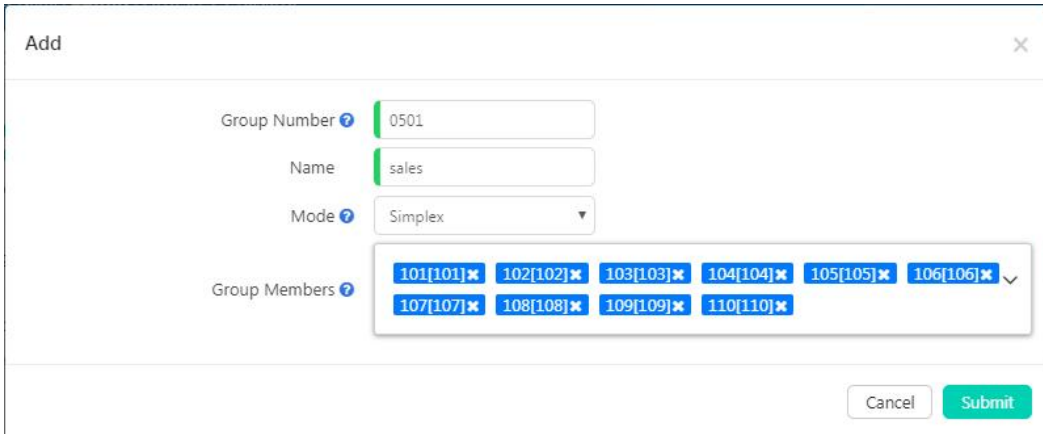
There are 10 conference numbers for internal extension users to dial to join conference calls. You can also set conference as a destination in inbound routes to allow outside callers to reach the conferences.

8.5 Paging & Intercom

Path: **Telephony -> Advanced Features -> Paging & 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 an extension number that by calling the number will simultaneously page/intercom a group of phones.

To create a **Paging & Intercom** group, please click on the  button, a popup window will show up as below.



- In the **Group Number** field, a default group number is given. The number could be changed within the Paging Group Extension Number Range listed on **Telephony -> Preferences -> Global PBX Options** page, Extension Ranges section.
- In the **Name** field a name should be given to identify this paging group.
- In the **Mode** dropdown list, if "Simplex" is selected, calling the group number will page on the group members, if "Duplex", the group members are able to talk back to the caller (intercom).
- In the **Group Members** field, select the desired user extensions, make sure all extensions you selected are desktop based IP phones, otherwise if the phone is an analog one, paging/intercom will not work.

Except group paging and intercom, extension users could also paging/intercom an individual extension by using feature codes, please refer to introductions in [Other feature codes](#) section.

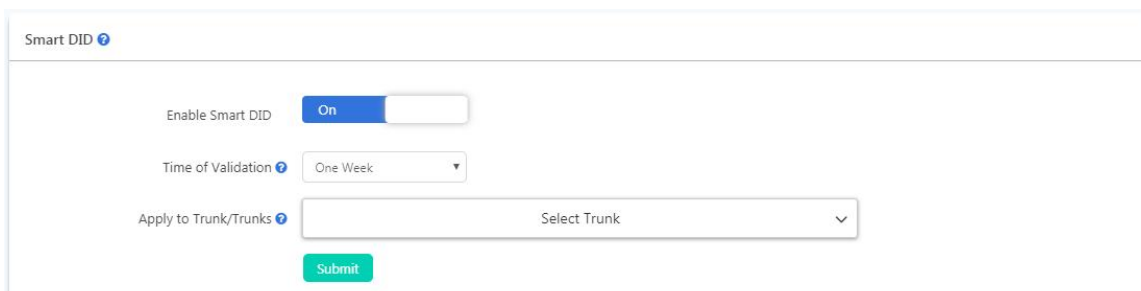
8.6 Smart DID

Path: **Telephony -> Advanced Features -> Smart DID**

With Smart DID feature, the IPPBX system has the ability to route an inbound call directly to an extension if the extension had previously called or tried to call the external number. 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.

For example, extension 100 called external number 1234567, no matter this number answered or not, when the number tries to ring back, the call will go directly to extension 100.

If you want this to happen, please use the **Enable Smart DID** switch to turn on this feature.




In **Time of Validation** dropdown list choose how long the system to save these outbound call records. When the records expired, the inbound calls will be routed according to you inbound routes settings.

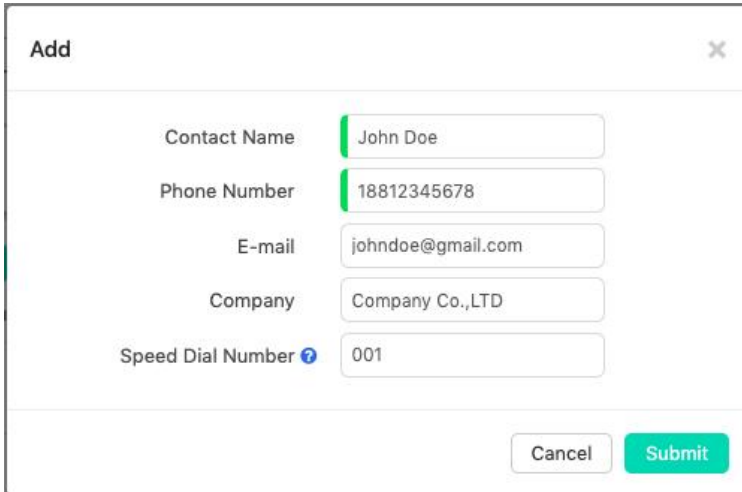
In **Apply to Trunk/Trunks** field, you have to select the trunk/trunks Smart DID feature will be applied to.

8.7 Phonebook

Path: **Telephony -> Advanced Features -> Phonebook**

Phonebook feature for IPPBX is just like a contact list on the mobile phones. You may add contacts to the IPPBX system, when the contacts calling in, on the ringing user extension phone screen will display the caller number and the contact name you have added before. If the number didn't match any contacts in the phonebook, then only caller number will be displayed on the ringing phone screen.

You may click on the  button to add a new contact from the popup window.



The image shows a 'Add' contact popup window. It has a title bar with 'Add' and a close button. The form contains five input fields: 'Contact Name' with the value 'John Doe', 'Phone Number' with '18812345678', 'E-mail' with 'johndoe@gmail.com', 'Company' with 'Company Co.,LTD', and 'Speed Dial Number' with '001'. There are 'Cancel' and 'Submit' buttons at the bottom right.

Or you may export the phonebook template file to add the contacts by MS Excel and then upload the file to generate contacts.

Contacts could be added by admin user from admin web interface, by operator from operator web interface and by extension user from extension user web portal.

A contact added by admin user and operator user is visible to all extension users, but a contact added by an extension user is only visible to the user who added it and the admin and operator user, other extensions won't be able to see it.

8.8 LDAP

Path: **Telephony -> Advanced Features -> Phonebook**

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 pre-configured on IP PBX which is mainly used to centralize manage the phonebook.

8.9 Callback

Path: **Telephony -> Advanced Features -> 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.

Options

Enable ☐ Off

Strip Prefix

Add Prefix

Dial Permission

[Save](#)

- **Enable:** Enable Call Back feature by switching the button on.
- **Strip Prefix:** 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.
- **Add Prefix:** Define digits added before calling out the numbers.
- **Dial Permission:** Choose an appropriate dial plan to make sure the IPPBX system has the permissions for outbound calling.

Click "Add" to add a call back number.

Add

Number

Destination

[Cancel](#) [Submit](#)

- **Number:** The number which will be used to call into the IPPBX system and 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 85337096 called the IPPBX system, IPPBX will disconnect this call and make a call back to this number using extension 100.

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.

8.10 Whitelist

Path: **Telephony -> Advanced Features -> Whitelist**

An extension user can set up a whitelist, only the numbers in the whitelist can dial that extension number, otherwise the call will be rejected. After establishing the whitelist, user can select the association in the 'IP Extension'.

Smart DID Phonebook Callback **Whitelist**

[Add](#)


Name	Number List	Options
No items to display.		
0 Total		

Add: add a new whitelist

Add ✕

Name

Extension

Number List 

1001, 1002, 1003, 1004

Cancel

Submit

Name: the name of the whitelist.

Number List: the system would check whether the incoming call number match with any one number on the number list. Please use ' , ' to separate multiple numbers.

9 Preferences

9.1 Global PBX Options

Path: **Telephony -> Preferences -> Global PBX Options**

Global PBX

Operator Extension ?	FS [100]
Global Ring Time(Sec) ?	30
Outbound Call Transfer ?	<input type="checkbox"/> Off
Music On Ringback ?	<input type="checkbox"/> Off
Auto Answer ?	<input type="checkbox"/> Off
PPI ?	<input type="checkbox"/> Off
Diversion ?	<input type="checkbox"/> Off
Early Media ?	<input type="checkbox"/> Off
Block Anonymous Calls ?	<input type="checkbox"/> Off
Jitter Buffer ?	<input type="checkbox"/> Off

Submit

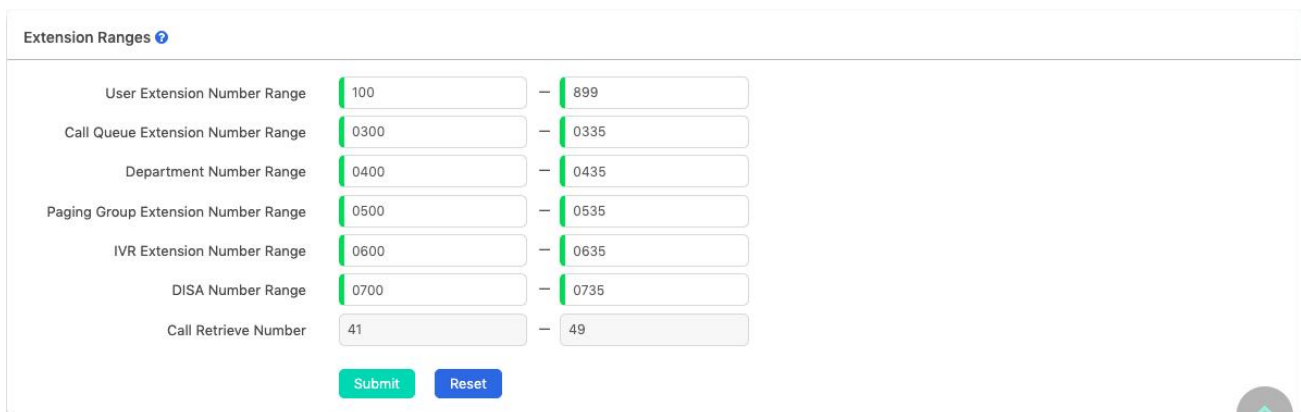
Global PBX

Operator Extension ?	None	Global Ring Time(Sec) ?	30
Outbound Call Transfer ?	<input type="checkbox"/> Off	Early Media ?	<input type="checkbox"/> Off
Music On Ringback ?	<input type="checkbox"/> Off	Music On Hold Folder	Please Select
Auto Answer ?	<input type="checkbox"/> Off	Auto Answer Time(Sec)	Please Select
Block Anonymous Calls ?	<input type="checkbox"/> Off	Jitter Buffer ?	<input type="checkbox"/> Off
Call Forward CID ?	<input type="checkbox"/> Off	Press 0 to Operator ?	<input checked="" type="checkbox"/> On
Indicate Line Busy ?	<input checked="" type="checkbox"/> On	Blind Transfer Callback ?	<input checked="" type="checkbox"/> On
Diversion ?	<input type="checkbox"/> Off	PPI ?	<input type="checkbox"/> Off
Abandoned Call Logs ?	<input type="checkbox"/> Off	SIP Header Type ?	tel

Submit

- **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:** If it's not specifically configured, an incoming call will ring the extension for the time given here.
- **Outbound Call Transfer:** Allow outbound phone calls to be transferred, if enabled it might cause phone call problem in certain situations. For example, an outbound phone call had been placed to another IVR system, the keypress might be recognized as transfer request on your own IPPBX system.
- **Early Media:** Early media is the ability of two user agents to communicate before a call is actually established.
- **Music On Ringback:** If enabled, callers will hear music instead of ringback tone when calling extensions.
- **Music On Hold Folder:** To select the music folder.

- **Auto Answer:** Auto-answer enables the IPPBX to automatically answer the inbound calls from analog ports.
- **Auto Answer Time:** The time in second after the call is auto answered.
- **Block Anonymous Calls:** If enabled, all anonymous (without caller ID) calls will be blocked by the phone system.
- **Jitter Buffer:** Jitter buffer can be used to resolve the sound distortion caused by network congestion, timing drift or route changes.
- **Call Forward CID:** The incoming call numbers are allowed to be transmitted through other digital trunks.
- **Press 0 to Operator:** Calls that are unanswered due to the disable of extension's voice mailbox, it will prompt a 'Press 0 to speak with an operator'.
- **Indicate Line Busy:** Whether to enable the announcement of 'Line Busy' when the outgoing line cannot be connected.
- **Blind Transfer Callback:** Enable the blind transfer for unanswered call to be transferred.
- **Diversion:** While forwarding/transferring a call out through SIP trunk, the actual caller number can be passed to the forwarded number with diversion option enabled, but requires the SIP trunk service provider support this feature, otherwise please disable this option.
- **PPI:** The P-Preferred-Identity (PPI) 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.
- **Abandoned Call Logs:** Whether to record the abandoned call that are in the queue into logs.
- **SIP Header Type:** The header type for PPI and Diversion.



Extension Range	Start	End
User Extension Number Range	100	899
Call Queue Extension Number Range	0300	0335
Department Number Range	0400	0435
Paging Group Extension Number Range	0500	0535
IVR Extension Number Range	0600	0635
DISA Number Range	0700	0735
Call Retrieve Number	41	49

The user extension number and system extension number ranges are defined here to avoid any conflicts within the IPPBX system. You can modify these number ranges as per your requirements. The user extension number could be 2 to 11 digits. And **Call Retrieve Number** range need to be modified from the **Feature Codes** screen.

9.2 VoIP Advanced

Path: **Telephony -> Preferences -> VoIP Advanced**

Global SIP settings allow you to configure some general and advanced options for the IPPBX system global SIP preferences.

SIP

UDP Port	<input type="text" value="5060"/>
TCP Port	<input type="text" value="5060"/>
TLS Port	<input type="text" value="5062"/>
ICE Enable	<input checked="" type="checkbox"/> On
STUN Server Address	<input type="text"/>
RTP Port Range	<input type="text" value="10001"/> — <input type="text" value="10500"/>
User Agent	<input type="text" value="IPPBX"/>
Endpoint Identifier Order	<input type="text" value="ip,username,auth_username"/>
External Media Address	<input type="text"/>
External Signaling Address	<input type="text"/>
External UDP Signaling Port	<input type="text"/>
External TCP Signaling Port	<input type="text"/>
External TLS Signaling Port	<input type="text"/>
Local Net(IP/Netmask Length) 1	<input type="text"/>
Local Net(IP/Netmask Length) 2	<input type="text"/>
Local Net(IP/Netmask Length) 3	<input type="text"/>

- **UDP Port:** SIP over UDP service port. By default IPPBX system uses UDP as SIP transmission protocol. Port number can be changed here if required. If changed on the IPPBX system, you'll also have to change on the SIP clients.
- **TCP Port:** If the phones support TCP protocol, you can register SIP extensions over TCP protocol on port 5061.
- **TLS Port:** If the phones support TLS protocol, you can register SIP extensions over TLS protocol on port 5062.
- **ICE Enable:** This is specific to clients that support NAT traversal for media via ICE, STUN, TURN. By default, please keep it enabled, otherwise WebRTC won't work, **STUN Server Address** can be left blank.
- **STUN Server Address:** By default please keep it blank, if you got available STUN server, please specify the valid server address, otherwise an invalid STUN server address will cause phone system exception.
- **RTP Port Range:** The UDP ports used by the IPPBX system to carry RTP voice stream. Do not change the port range or you may encounter audio issue with phone calls.
- **User Agent:** The default user agent string also contains the Asterisk version. If you don't want to expose it, change the user agent string here.
- **Endpoint Identifier Order:** The priority of SIP signaling user authentication type (non-professional users are not recommended to modify).
- **External Media Address:** If you want to map your IPPBX system to the Internet, you should specify the static public IP address or domain name here.
- **External Signaling Address:** This is similar to External Media Address except that the External Signaling Address is looked up regularly (every 10s).
- **External UDP Signaling Address Port:** Port number of SIP signaling with UDP transport protocol on the public network.
- **External TCP Signaling Address Port:** Port number of SIP signaling with TCP transport protocol on the public network.
- **External TLS Signaling Address Port:** Port number of SIP signaling with TLS transport protocol on the public network.
- **Local Net (IP/Netmask Length):** Your local network address/addresses.

Notice

If you are going to map your IPPBX system to the Internet, the following configurations should be done.

1. SIP port mapping on your router (one of the following: UDP: 5060; TCP: 5061; TLS: 5062).

2. RTP port mapping on your router (UDP: 10001 to 10500).
3. Specify External Media Address and External Signaling Address.
4. Specify your local network address/addresses.
5. For extensions remote registration, enable "Remote Extension" on extension edit popup window.

Mapping your IPPBX to the Internet will be risky, for security precautions please always use strong passwords.

IAX Settings.

IAX Settings ?

UDP Port

Submit

IAX2 extension support had been enabled by default for all extensions. And IAX2 works on UDP port 4569, you may modify the port number if required.

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

9.3 Analog Settings

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

Analog Settings

Caller ID Detection ?	<input checked="" type="checkbox"/> On	Caller Name ?	<input type="checkbox"/> Off
Caller ID Signaling ?	<input type="text" value="Bell-US"/>	Caller ID Start ?	<input type="text" value="Ring"/>
Caller ID Buffer Length ?	<input type="text" value="2500"/>	Ring Debounce ?	<input type="text" value="64"/>
DTMF Hits Begin ?	<input type="text" value="2"/>	DTMF Misses End ?	<input type="text" value="3"/>
Detect Caller ID After ?	<input type="text" value="1"/>	Opermode ?	<input type="text" value="FCC"/>
Tone Zone ?	<input type="text" value="United States"/>	Send Caller ID After ?	<input type="text" value="1"/>
FXO Tune ?	<input type="checkbox"/> Off	Tone Duration ?	<input type="text"/>
FXO Ring Timeout(ms) ?	<input type="text" value="8000"/>	Relax DTMF ?	<input type="checkbox"/> Off
Denoise RX ?	<input type="checkbox"/> Off	Denoise TX ?	<input type="checkbox"/> Off
Echo Cancel When Bridged ?	<input type="checkbox"/> Off	Echo Training ?	<input type="text" value="8000"/>

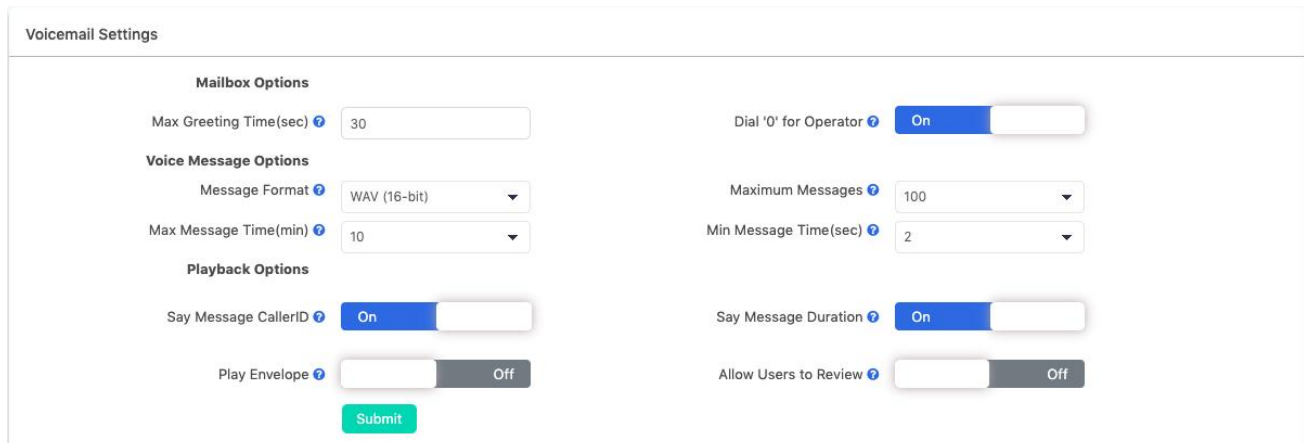
Submit

- **Caller ID Detection:** Allow\Disallow to detect caller ID.
- **Caller Name:** In some countries/regions caller name can be passed through the PSTN lines, by enabling this option the caller name will be received by the IPPBX system along with the caller ID.
- **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.
- **Caller ID Buffer Length:** The buffer length can be used to store caller ID info.
- **Ring Debounce:** Sets the minimum time in milliseconds to debounce extraneous ring events.
- **DTMF Hits Begin:** Sampling matching value of DTMF caller ID digits, you can choose 1 to 5 digits been matched then to consider it as part of the Caller ID.
- **DTMF Misses End:** Sample matching value of DTMF caller ID digits, you can choose 1 to 5 digits been mismatched then to consider it's not part of the caller ID.
- **Detect Caller ID After:** Sets the IPPBX to detect Caller ID after how many rings been detected.
- **Opermode:** Set the Opermode for FXO Ports.
- **ToneZone:** Select the tone zone of your country.
- **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).
- **FXO Tune:** FXO Tune is a utility of tuning the various settings on the FXO ports for better adaptability with the PSTN lines, e.g. impedance.
- **Tone Duration:** used to adjust caller ID detection, non-professional users please do not modify.
- **FXO Ring Timeout:** This value can be tweaked to shorten how long it takes before the analog port (FXO) consider a non-ringing line to have hungup.
- **Relax DTMF:** If you are having trouble receiving DTMF key presses, enabling this option will make the DTMF interpreter much more permissive.

- **Denoise RX/TX:** The denoise parameter will help on noise reduction of the noisy analog lines, especially when gains have been increased on the lines.
- **Echo Cancel When Bridged:** It allows echo cancellation to be enabled or disabled for calls that are bridged between two TDM devices. As most of the time, the calls between two TDM endpoints will not have any echo, so this option is not required.
- **Echo Training:** The time length setting of echo training.

9.4 Voicemail Settings

Voicemail settings can be used to configure global voicemail options for all extension users.



The Voicemail Settings form is divided into three sections: Mailbox Options, Voice Message Options, and Playback Options. Each section contains various settings that can be configured for all extension users.

Section	Setting	Value
Mailbox Options	Max Greeting Time(sec)	30
	Dial '0' for Operator	On
Voice Message Options	Message Format	WAV (16-bit)
	Maximum Messages	100
	Max Message Time(min)	10
	Min Message Time(sec)	2
Playback Options	Say Message CallerID	On
	Say Message Duration	On
	Play Envelope	Off
	Allow Users to Review	Off

A green Submit button is located at the bottom center of the form.

- **Max Greeting Time** sets the max greeting message duration the extension users can record in their mailbox to greet the callers when they entering voicemail.
- **Dial '0' for Operator** option if enabled, the callers can press 0 to call the operator extension.
- **Message Format** sets the voicemail audio file format to be saved in the IP PBX system.
- **Maximum Messages** sets the maximum number of messages can be saved in the system for each extension user.
- **Max Message Time** sets the maximum duration of a single voice message can be accepted by IP PBX system.
- **Min Message Time** sets the minimum duration of a single voice message can be accepted by the IP PBX system, message duration less than the Min Message Time will be discarded by IP PBX system.
- **Say Message Caller ID:** Announce caller ID when listening to the message on user extension.
- **Say Message Duration:** Announce message duration when listening to the message on user extension.
- **Play Envelope:** Announce date time and caller ID when listening to the message on user extension.

Allow Users to Review: Allow callers to review their message before saving.

9.5 Module Settings

Notice

Module Settings are only for configuring digital module cards (E1/T1, BRI) on PBX-C302 and PBX-C503 IPPBX systems. Ignore this part if you are using FXS/FXO/GSM modules.

Path: **Telephony -> Preferences -> Module Settings**

PBX-C302 and PBX-C503 IPPBX systems need proper module settings to load correct drivers and configure files to drive the E1 and BRI telephony modules.

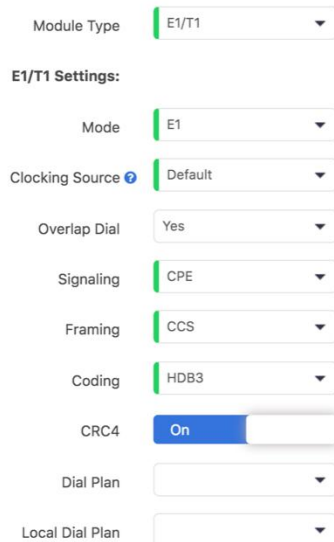
Default module settings are with module types FXS/FXO/GSM on both telephony module slots. So if you don't have E1 and BRI modules

installed then you don't have to configure module settings.

9.5.1 E1 PRI Signaling

E1 module can be installed on both Slot1 and Slot2. To ensure PBX-C302/PBX-C503 IPPBX can detect and drive E1 module in the Module Type field you should choose "E1/T1".

Slot1



- **Mode:** Sets the module to work as E1 mode.
- **Clocking Source:** Use local or remote as the E1/T1 clock source.
- **Signaling:** Sets the module to work with PRI CPE or NET, CPE is used on the client side, NET is used on the telephony provider side.
- **Framing:** By default CPE and NET use CSS (Common Channel Signaling).
- **Coding:** By default HDB3.
- **CRC4:** A method of checking for errors in transmitted data on E-1 trunk lines. Enable it only if the telephony provider implemented CRC4 on their E1 lines.
- **Dial Plan:** The ISDN-level Type Of Number (TON) or numbering plan, used for the dialed number. For most installations, leaving this as 'unknown' (the default) works in the most cases. In some very unusual circumstances, you may need to set this to 'dynamic' or 'redundant'. Note that if you set one of the others, you will be unable to dial another class of numbers. For example, if you set 'national', you will be unable to dial local or international numbers.
- **Local Dial Plan:** Only RARELY used for PRI (sets the calling number's numbering plan). In North America, the typical use is sending the 10 digit callerID number and setting the prilocaldialplan to 'national' (the default). Only VERY rarely will you need to change this.

These configuration parameters should be given by the telephony provider, please configure these parameters correctly according to what they give to match the switching equipment being used by the telephony provider.

Once the configurations had been done, save and reboot the IPPBX system. In the meantime you attach the E1 line to the E1 interface. After rebooting you should get LED indications with L1 red, L2 red, L3 off and L4 green of a successful PRI CPE connection. For more details of the LED indications please check PBX-C302 and PBX-C503 chapter in the LED Indication section.

If in the deployment you got some else connection status you should check with the telephony provider to confirm the configuration parameters. Or check with them if the line had been activated by them and ready for phone calls.

9.5.2 T1 PRI Signaling

To configure E1 telephony module to work in T1 mode, please choose **T1** in the **Mode** dropdown list. And then configure T1 related parameters given by the telephony provider.

Slot1

Module Type E1/T1

E1/T1 Settings:

Mode T1

Signaling CPE

Framing ESF

Coding B8ZS

CRC4 On

Dial Plan

Local Dial Plan

T1 runs on same signaling types as E1 mode. And T1 uses different Framing and Coding methods, configure these parameters according to the details provided by the telephony provider. In most cases CRC4 is not needed for T1 circuit, enable it only when the provider requires it.

After configurations been done, save and reboot the IPPBX system. In the meantime you attach the T1 line to the T1 interface. After rebooting you should get LED indication with L1 red, L2 red, L3 off, L4 green to indication PRI CPE signaling. For more details of the LED indications please check PBX-C302 and PBX-C503 chapter in the LED Indication section.

9.5.3 MFC/R2 Signaling

In the E1 settings section and Signaling field by selecting R2 you are able to configure E1 R2 signaling.

Slot1

Module Type E1/T1

E1/T1 Settings:

Mode E1

Signaling R2

Framing CAS

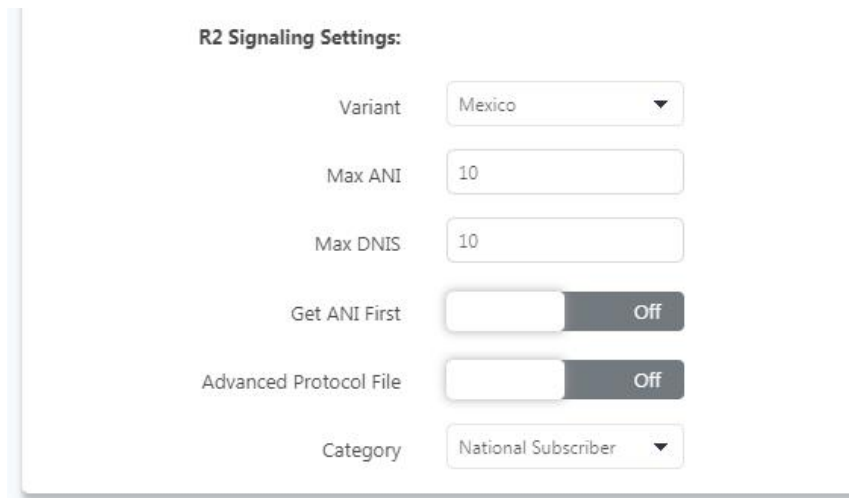
Coding HD83

CRC4 On

Dial Plan

Local Dial Plan

In **Signaling** field select R2, **Framing** and **Coding** should use default value. Below in the R2 Signaling Settings section set the R2 parameters.



R2 Signaling Settings:

Variant: Mexico

Max ANI: 10

Max DNIS: 10

Get ANI First: Off

Advanced Protocol File: Off

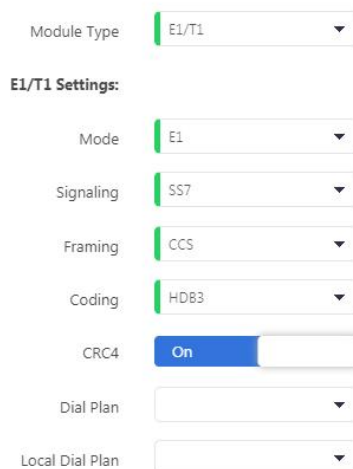
Category: National Subscriber

- **Variant:** Protocol variant setting depends on country and carries.
- **Max ANI:** The maximum expected number of ANI digits.
- **Max DNIS:** The expected number of dialed digits.
- **Get ANI First:** The usual behavior for incoming calls is to get the calling party category and the ANI as soon as possible, and to get the DNIS afterwards. This doesn't work on all systems, so the option to reverse this behavior is provided.
- **Advanced Protocol File:** Additional configurations for R2 signaling.
- **Category:** Send calling party's category. Usually National Subscriber works just fine, you can set other options if needed in real application.

9.5.4 SS7 Signaling

Signaling System No.7 (SS7) is a set of telephony protocols can be delivered via E1 and T1. In the E1 settings section and Signaling field by selecting SS7, you are able to configure E1 SS7 signaling.

Slot1



Module Type: E1/T1

E1/T1 Settings:

Mode: E1

Signaling: SS7

Framing: CCS

Coding: HDB3

CRC4: On

Dial Plan:

Local Dial Plan:

In the **Signaling** dropdown list you should select SS7, **Framing** and **Coding** should use default value. Below in the **SS7 Settings** section set the detailed SS7 parameters.

SS7 Settings:

Variant	<input type="text" value="ITU"/>
Point Code	<input type="text" value="20"/>
Point Code of Node Adjacent	<input type="text" value="20"/>
ss7 dchan	<input type="text" value="16"/>
Signaling Link Code	<input type="text" value="0"/>
Default Destination Point Code	<input type="text" value="20"/>
Network Indicator	<input type="text" value="International"/>
Called Nai	<input type="text" value="National"/>
Calling Nai	<input type="text" value="National"/>
International Prefix	<input type="text"/>
National Prefix	<input type="text"/>
Subscriber Prefix	<input type="text"/>
Unknown Prefix	<input type="text"/>

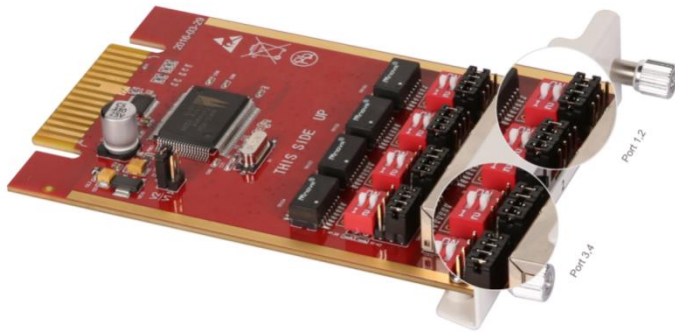
Please configure these parameters according to the instructions of the service provider or ask for advice from our support team. Otherwise please do not change these settings without professional guidance.

9.5.5 BRI Settings

BRI module can only be installed on Slot2 of the PBX-C302 and PBX-C503 IPPBX systems. The BRI modules you have received the jumpers on the module should be set on "V2" position by default, please refer to following picture to check the jumpers before installing.



The jumpers shown in the picture below are for crossover cables and straight cables to connect a BRI connection.



The jumpers for Port 1, 2 and Port 3, 4 are on different position. Attach the BRI lines to these ports and then configure BRI parameters.

Slot2

Module Type

ISDN BRI

BRI Settings:

Type of Port 1

TE_PTP

PRI Dial Plan

National

PRI Local Dial Plan

National

International Prefix

National Prefix

Local Prefix

Private Prefix

Type of Port could be set to **TE_PTP**, **TE_PTMP**, **NT_PTP** and **NT_PTMP**.

- **TE_PTP:** BRI PTP Point to Point signaling (CPE side)
- **TE_PTMP:** BRI PTMP Point to Multi-Point signaling (CPE side)
- **NT_PTP:** BRI PTP Point to Point signaling (Network side)
- **NT_PTMP:** BRI PTMP Point to Multi-Point signaling (Network side)

For other parameters please configure them according to the instructions of the service provider or ask for advice from our support team. Otherwise please do not change these settings without professional guidance.

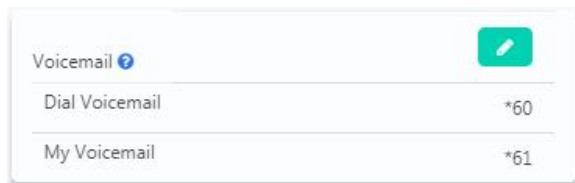
10 Feature Codes

Path: **Telephony** -> **Feature Codes**

Feature codes can be dialed from user extensions to enable and disable certain features or to achieve some call features. For example, enable and disable call forward, transfer incoming calls, check voice messages, etc.

Feature codes could be modified if necessary but please ensure all feature codes you wish to change will not conflict with other existing ones.

10.1 Voicemail feature codes

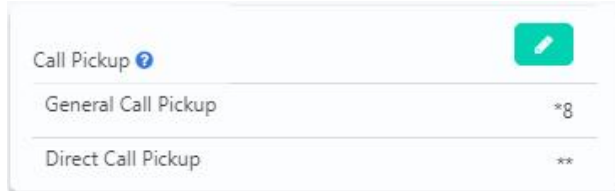


Dial *60 and you will enter the main menu of voicemail feature, by specifying the extension number and voicemail password of the required extension then you can check its voicemail and you can do this for any extension by following the system voice guidance.

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.

10.2 Call Pickup feature codes

Call pickup feature codes allow users to pick up calls that are not directed to them by dialing a feature code *8 or **.

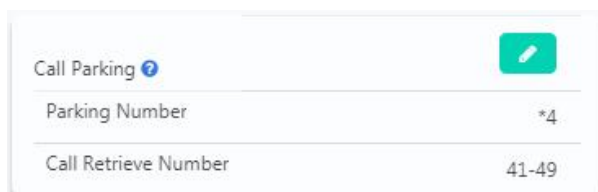


If there's an incoming call ringing on an extension that belongs to your department, you may dial the general call pickup feature code *8 (end with #) to pick up the call. While if there are 2 ringing extensions in your department, by dialing *8 will pick up the first incoming call. If you need to pick up the second incoming call or if you don't know which call came first, you may use direct call pickup feature code.

Direct call pickup feature code could be used to pick up an incoming call on a specific extension, no matter the extension is from the same department or from another department. Just dial ** following by the extension number (end with #) you'll be able to pick up the incoming call on that specific extension.

10.3 Call Parking feature codes

Call parking feature allows anyone who has received a call to park the call on an extension, allowing any other user to access the parked call.



To park a call, extension user could dial *4 during a live call, and then listen as the system tells you where you can retrieve the call (usually extension 41). The second call will be parked on 42, and it continues to park on orderly.

To retrieve the parked calls, user should dial the retrieve number given by the IPPBX system. And this could be done by any extension.

A call could be parked for maximally 120 seconds before it goes back to the extension which parked it. And the parking lot (call retrieve numbers) could be monitored by BLF. It's helpful if the operator wants to know if there are calls parked on the IPPBX system.

10.4 Call Transfer feature codes

Call Transfer is used to transfer a call in progress to some other destinations. 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 "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).



In a live call, you 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 hang up. If the transferred number doesn't answer this call then it will go to voicemail.

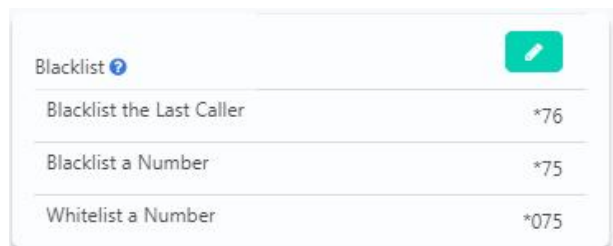
If blind transfer sometimes seems inappropriate, you may use attended transfer feature. In a live call, you can press *2 and the IPPBX system prompts "Transfer", you then enter the number to transfer to, after someone answers your call, you can introduce this call and hang up at which point the call is transferred.

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. You may also manually abort the transfer by pressing * when the third party is still ringing.

10.5 Blacklist feature codes

Black list feature codes allow the extension users to add external phone numbers to IPPBX system blacklist from their phones, consequently the numbers added will not be able to dial in to the IPPBX system.

Adding blacklist numbers from phone by using feature codes is the same as adding blacklist numbers from admin and operator UI.



Blacklist the last caller allows you to dial *76 to directly add the last caller's number to the IPPBX blacklist.


You may also dial *75 (end with #) and follow the voice prompts to specify the number you wish to blacklist to add numbers to the IPPBX system blacklist.

To remove numbers from black list (whitelist a number), you can dial *075 (end with #) and follow the voice prompts to specify the number you wish to whitelist.

10.6 Call Spy feature codes

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



Call Spy ?	
Normal	*90
Whisper	*91
Barge	*92

- **Normal Spy:** For example, extension 410 is talking to someone on the phone, you can dial *90410 (end with #) 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 following by the employee's extension number (end with #) 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 following by their extension number (end with #) to talk to both of the speakers.

Notice

Before you can spy on an extension, please enable "Call Spy" option on the extension edit popup window.

10.7 Call Queue feature codes

Call queue feature codes are for call queue agent extensions only. They are meaningless to the non-agent extensions.



Call Queue ?	
Agent Login	*62
Agent Logout	*062
Agent Pause	*95
Agent Unpause	*095

Agent Login and **Agent Logout** are for dynamic agents to login or out of the call queue. And for both static agents and dynamic agents, they can dial *95 to suspend their extensions temporarily, new calls will not be distributed to their extensions, until they dial *095 to resume.

10.8 Conference feature codes

Conference feature codes are used by conference admin for inviting participants to join in a conference or for creating a conference during a normal phone call.



When in a conference room, if the conference admin user presses 0 they will get a dial tone for inviting others to participate in this conference.

If the invited party agrees to join in the conference, conference admin user can dial ** to return to the conference with invited party.

If the invited party doesn't want to join in the conference, conference admin user can press *# to return to the conference without the invited party.

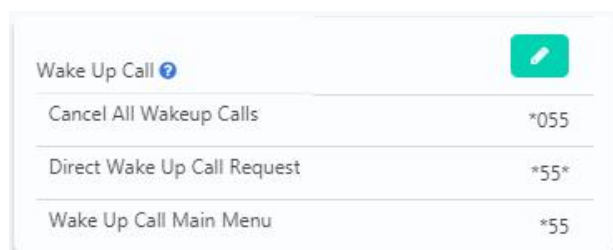
During a live call the extension user can press *0 to create a dynamic conference room. The other side will automatically enter the conference as an ordinary participant while the extension user who created this conference will be requested to enter the conference password to enter. Usually the user needs to enter the conference admin user password as the user needs to invite others to join in the conference.

Notice

After a dynamic conference is created, in reality you have entered a static conference room (by default 90 is the first available conference room). You are able to use conference admin menu to invite others to the conference and also others can dial 90 to enter this conference.

10.9 Wakeup call feature codes

Except configuring Wakeup Calls from admin and operator web user interface, extension users could request wakeup calls from their phones directly by feature codes.



- **Cancel All Wakeup Calls:** By dialing this code to cancel all requested wakeup calls.
- **Direct Wakeup Call Request:** Add a wakeup call directly by dialing this feature code followed by a specific date and time in 8-digit number format, for example, feature code is *55*, you can dial *55*08010730 to add a wakeup call of 7:30am on August 1st.
- **Wakeup Call Main Menu:** Advanced wakeup call menu for adding, viewing and canceling wakeup calls.

10.10 Call Forward feature codes

Call forward could be configured from admin and operator web user interface. With the following feature codes, extension users can activate or deactivate call forward directly from their phones without configuration on the Web GUI.

Call Forward ⓘ		
Forward All Activate	*71	
Deactivate All	*071	
Activate Forward on Busy	*72	
Deactivate Forward on Busy	*072	
Activate Forward on No Answer	*73	
Deactivate Forward on No Answer	*073	

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

- **Forward All Activate:** Dial *71985337096, press 1 to confirm.
- **Deactivate Forward All:** Dial *071.
- **Activate Forward on Busy:** Dial *72985337096, press 1 to confirm.
- **Deactivate Forward on Busy:** Dial *072.
- **Activate Forward on No Answer:** Dial *73985337096, press 1 to confirm.
- **Deactivate Forward on No Answer:** Dial *073.

10.11 DND feature codes

DND (Do Not Disturb) could be set on the IP phones from the phone level, if the phone doesn't have DND feature you may use the DND feature code to set DND from IPPBX system level. Any phone connected to the IPPBX system can use the DND feature code, no matter it's IP phone, analog phone or softphone.


DND ⓘ		
DND Activate	*74	
DND Deactivate	*074	

Simply dial *74 to enable DND, if you hear a beep sound that means DND is on. Once DND enabled, the extension will only be able to make calls, and inbound calls will be rejected.

Make sure when you are ready to receive inbound calls, dial *074 to deactivate DND.











10.12 Office Closed feature codes

Office Closed could be set on the IP phones from the phone level. Any phone connected to the IPPBX system can use the Office Closed feature code, no matter it's an IP phone, analog phone or softphone.

Office Closed ⓘ		
Office Closed On	*81	
Office Closed Off	*081	

By dialing the Office Closed On feature code you may disable all inbound control settings, all inbound calls will be forwarded to a specific destination. By dialing the Office Closed Off feature code to resume all inbound control settings.

10.13 Other feature codes

Others 	
Announce WAN Port IP 	**11
Announce LAN Port IP 	**12
Announce Extension Number 	**13
One Touch Recording 	*1
Intercom 	*50
Paging 	*51
Speed dial 	*99
Meet Me Page 	*52
Switch Phone 	*3
Audio Console	*911

- **Announce WAN Port IP:** By dialing this code you'll hear the system announce the IP address of the IPPBX WAN interface.
- **Announce LAN Port IP:** By dialing this code you'll hear the system announce the IP address of the IPPBX LAN interface.
- **Announce Extension Number:** By dialing this code you can check the extension number of your phone, either it's an IP phone or analog phone.
- **One Touch Recording:** One Touch Recording is also known as Record on Demand. It allows users to record phone calls selectively. 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.
- **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.
- **Speed Dial:** Use speed dial feature code with contact speed dial number to call a contact instead of dial the contact's actual number.
- **Meet Me Page:** Meet Me Page can be used to page someone over the phones/speakers. The paged person can use this feature code to terminate the paging and establish an intercom call with the initiator.
- **Switch Phone:** When the extension is registered on several different endpoints, you may dial *3 from an idle endpoint to switch the call to the idle endpoint.
- **Audio Console:** By dialing *911 to make live announcements to the speakers connected to the Audio Out interface.

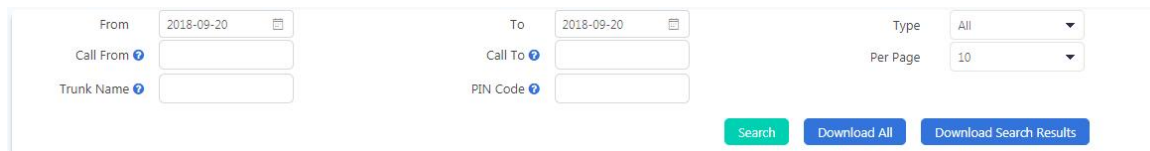
11 Reports

11.1 Call Logs

Path: **Reports -> Call Log**

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.

To query call logs, you need to first specify the searching criteria.



The search form includes fields for 'From' (date: 2018-09-20), 'To' (date: 2018-09-20), 'Type' (dropdown: All), 'Call From' (text), 'Call To' (text), 'Trunk Name' (text), and 'PIN Code' (text). It also has a 'Per Page' dropdown set to 10. Action buttons include 'Search', 'Download All', and 'Download Search Results'.

- In the **Type** drop-down list choose Outbound, Inbound or Internal to search outbound calls, inbound call or internal calls only.
- In **From** and **To** fields set the start and end date to search call logs within this period of time.
- By specifying the name of a trunk in the **Trunk Name** field to search the inbound or outbound calls came in or sent out through this specific trunk only.
- In the **PIN Code** field specify a PIN code of a [PIN Set](#) to search outbound calls made by using this PIN code.

The searching results might look like below.

Start Time	Call From	Call To	Final Callee	Duration	Trunk Name	PIN Code	Type	Status	Call Recordings
2018-02-11 15:17:46	John Doe["John Doe" <10...	965302387	965302387	00:00:30	FXO-1	9031	Outbound	Answered	Yes
2018-02-11 15:15:14	65302387	IVR(biz-en)	100	00:00:47	FXO-1		Inbound	Answered	Yes

- The time when this call took place will be listed in the **Start Time** column.
- In the **Call From** column lists the original caller of the calls.
- In the **Call To** column lists the first callee but might not be the last.
- The **Final Callee** column lists the extension/destination where the call finally ends.
- In the **Duration** column lists the call duration of each phone calls, this might not be the exact talk time, as when calling though the FXO ports, IPPBX system will auto answer the inbound calls so IVR works, and it will auto answer the outbound calls, so the IPPBX could send the numbers out through the PSTN lines.
- In the **Trunk Name** column lists the trunks used by those phone calls. Internal call will not take any trunk so this blank will be blank for internal calls.
- In the **PIN Code** column, only those outbound calls made out with a PIN code will list the PIN code used here. This is a good idea to tell which user/users made the call, as the PIN codes are not shared by every extension user. Every extension may have a PIN different than others or several extension users share a PIN code that is different than others.
- In the **Type** column it indicates the type of each phone call, inbound, outbound or internal.
- In the **Status** column you could tell if the calls are successfully made or failed for any reason.
- The **Call Recording** column indicates which calls are recorded and which ones are not.

You may download the search results as a CSV file by clicking on the [Download Search Results](#) button, or you may download all the call logs by clicking on [Download All](#).

11.2 Call Recordings

11.2.1 Call Recordings

Path: **Reports -> Call Recordings -> Call Recordings**

Call recordings to be checked here are for those extensions which had enabled call recording from the extension edit page.

Search criteria can be used to search call recordings are as follows.

From	2018-01-11	To	2018-02-11	Type	All
Call From		Call To		Per Page	10
Trunk Name		PIN Code		Search	

- **Type** could be used to search the call recording according to outbound, inbound and internal calls.
- **Call From** could be used to search according to a specific caller's number (optional).
- **Call To** could be used to search according to a specific callee's number (optional).
- **Trunk Name** could be used to search according to the inbound/outbound trunk's name (optional).
- **PIN Code** could be used only for those calls which are dialed out with PIN codes define in [PIN Set](#) (optional).

The searched recordings will be displayed in a list with some detailed information.

Start Time	Call From	Call To	Final Callee	Duration(Call/Record)	Trunk Name	PIN Code	Type	Options
2018-02-09 16:33:08	8005	8000	8000	00:25:19/00:25:15			Internal	▶ ↓ 🗑
2018-02-09 16:09:18	8005	8000	8000	00:12:32/00:12:30			Internal	▶ ↓ 🗑

You may playback the recording by built-in web player by clicking on the [▶](#) button.



Or you may click on the [↓](#) button to download or click [🗑](#) to delete.

Call recordings can be managed only by the admin user from admin web UI. Operator user can only query and review the recordings but cannot delete them.

11.2.2 Conference Recordings

Path: **Reports -> Call Recordings -> Conference Recordings**

If the [conferences](#) had call recording enabled, the conference held will be recorded and conference recordings could be found for review here.

From	2018-09-20	To	2018-09-20
Conference Number		Per Page	10
Search			

In the **Conference Number** drop-down list you may specify the conference number and search for recordings of the specific conference number only.

The searched recordings will be listed with detailed information of when the conference calls were started, the conference number and the call/record duration. There are also the same options to playback, download and delete the recording files.

Start Time	Conference Number	Duration(Call/Record)	Options
2018-02-11 14:24:14	CONFERENCE(90)	00:06:35/00:06:33	▶ ↓ 🗑
1 Total			

11.2.3 One Touch Recordings

Path: **Reports -> Call Recordings -> One Touch Recordings**

One touch recording is for those extensions that are not enabled call recording, when the user wants to record the call, by pressing *1 will start recording.



The recordings of once touch recording could be found here. Search criteria and recording list options are the same as "normal" call recordings, except one touch recording could not be found on the **Call Recording** page.

11.3 System Logs

11.3.1 Fax Logs

Path: **Reports -> System Logs -> Fax Logs**

Fax logs stores all your inbound faxes and the outbound faxes sent from the extension user portal.

Start Date:  End Date:  Search

From	To	Time	Type	Info	File
816		2018-01-15 11:08:00	Received	Success	fax000000004.tif
816		2018-01-15 11:01:00	Received	Success	fax000000003.tif
816		2018-01-15 10:37:00	Received	Success	fax000000002.tif
816		2018-01-15 09:50:00	Received	Success	fax000000001.tif

4 Total

By downloading the .tif file to your operating system you may view the fax details.

11.3.2 Web Access Logs

Path: **Reports -> System Logs -> Web Access Logs**

On Web Access Logging page you may check all the logs of the web access records, including admin user, operator user and extension users.

From	2018-09-20	To	2018-09-20	Per Page	10
User	All	IP Address		Search	Download All
				Download Search Results	

In the **From** and **To** fields set the start and end date, in User dropdown list select the user role if you want to search per the type of users, optionally if you want to search according to the user's IP address you may also specify the IP address in the **IP Address** field then finally click on **Search** button.

The searching results are as below.

Log Time	User	IP Address	Options
2018-09-20 09:08:19	admin	192.168.17.104	login
2018-09-20 09:04:45	admin	192.168.17.106	delete wake up call,ids [34]
2018-09-20 09:04:01	admin	192.168.17.106	add wake up call {dateTime:2018-09-20 11:03, extents:[005]}
2018-09-20 09:03:45	admin	192.168.17.106	add wake up call {dateTime:2018-09-20 09:03, extents:[005]}
2018-09-20 08:54:14	admin	192.168.17.106	login
5 Total			

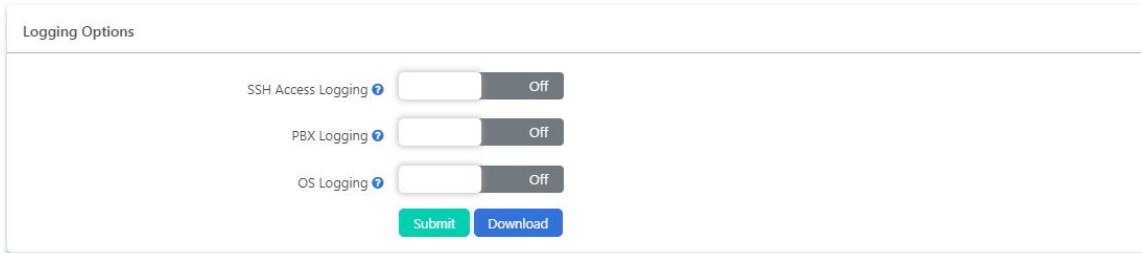
The time of when the login action took place, by which user, the source IP address and the actions taken will all be listed.

You may click on [Download Search Results](#) button to download the search results in CSV format, or click on [Download All](#) to download all web UI access logs in CSV format.

11.3.3 Advanced Logs

Path: **Reports -> System Logs -> Advanced Logs**

Advanced logging can be used for higher level of the IPPBX system troubleshooting.



Logging Options

SSH Access Logging [?](#) ☐ Off

PBX Logging [?](#) ☐ Off

OS Logging [?](#) ☐ Off

[Submit](#) [Download](#)

- **SSH Access Logging** can be used to trace the SSH login records.
- **PBX Logging** can be used to analyze the phone services related issues.
- **The OS Logging** can be used to analyze the IPPBX system OS level issues.

Enable the desired type of logging if you are qualified to analyze such kind of logs or if our support team asked for these kinds of logs for troubleshooting, otherwise please keep them disabled.

12 System

12.1 Storage

Data storage allows you to upload your recording files, log files and voicemail messages to an FTP server through the Ethernet. Or you may attach an external USB drive to the IPPBX USB interface for saving the above mentioned files.


12.1.1 USB Storage

Path: **System -> Storage -> USB Storage**

On PBX-C302 there's only 1 USB interface, on PBX-C302 and PBX-C503 there are 2 on the back panel. USB drives could be attached to the USB interface for data backup, only 1 USB drive supported on the PBX-C302 and PBX-C503.

Supported USB file system formats are: FAT16, FAT32, exFAT, NTFS, EXT3 and EXT4. If it's a portable USB hard drive, please make sure it uses external power supply. And please make sure the USB drive only has a single partition otherwise it won't be detected by the IPPBX system.

Before attaching the USB drive and configuring data storage settings please make sure no one else is signed in the IPPBX web UI and there's no phone call going on in the system. Because during the configuration process of USB data storage, the recordings, logs and voicemails generated would be lost.

Once a USB drive is detected, you'll see the **USB Mount Status** changed to **Connected**. Refresh the status by clicking on the  button if nothing happens when you have attached the USB drive.



USB Storage Status (Must Unmount USB before unplugging)

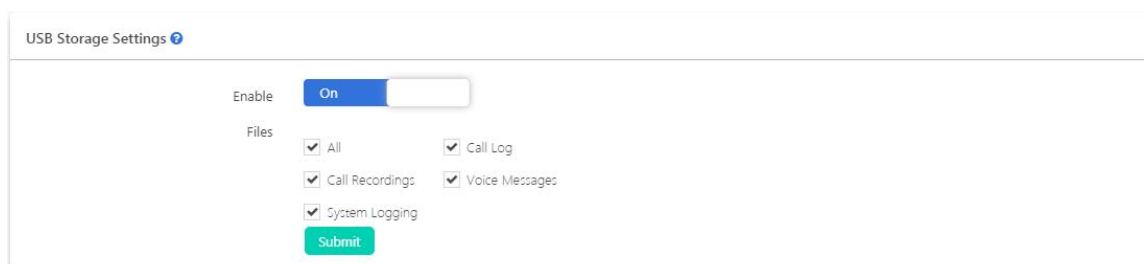
USB Mount Status: Connected  Unmount

USB Backup Status: Not Backup 

USB Storage Settings ?

Enable ☐ Off Submit

Now you may enable USB storage and configure which kind of files to be saved in the USB drive.



USB Storage Settings ?

Enable ☒ On Submit

Files

☒ All ☒ Call Log

☒ Call Recordings ☒ Voice Messages

☒ System Logging Submit


Once done click on Submit button and it will start to create folders on the USB drive and upload the existing files to the USB drive too.



USB Storage Status (Must Unmount USB before unplugging)

USB Mount Status: Connected 

USB Backup Status: Backup in progress, please wait... 

The whole process will take a few seconds to few minutes depending on the amount and size of the files. You may click on the  button to check the backup status, when done the **USB Backup Status** will change to **Backup End**.



From now on the type of files you've selected will all be written directly to the USB drive. And can be browsed on the web GUI just the same as they are saved in the internal system storage.

The volume info of the USB drive could be checked every time when you first signed in to the IPPBX system web GUI (Admin and Operator user).



Please do remember that, DO NOT remove the USB drive from the IPPBX system unless you have disabled USB storage and unmounted the USB drive by clicking on the **Unmount** button from System -> Storage -> USB Storage page.

Notice

If your USB drive could not be detected by the IPPBX system, please use USB disk format tool to delete all partitions on the USB drive and create a single new partition and try again. Before doing this please backup the data in your USB drive as doing this will erase all data on the drive.

12.1.2 FTP Storage

Path: **System -> Storage -> FTP Storage**

Utilizing your existing FTP server, you can configure the IPPBX system 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.

FTP storage should not be configured to work at the same time with USB data storage. Otherwise the data on the USB will all be migrated to your FTP server.

To configure FTP storage, enable it and configure the FTP server credentials and the file uploading options.

FTP Storage Settings

FTP Uploading

On

FTP Server Address

192.168.17.225

FTP Server Path

/

User Name

CoolVox

Password

Frequency

7

Upload Time

01 : 00

Files

☒ All
☒ Call Log
☒ Call Recordings
☒ Voice Messages
☒ System Logging

Submit

- In the **FTP Server Path** field you may specify the directory of where to store the uploading files.
- In the **Frequency** dropdown list select the number of days of each uploading.
- In the **Upload Time** field specify the exact time of the uploading.

Once configurations done, click on **Submit** button to connect the IPPBX system with the FTP server. Once connected, you'll see the **FTP Connect Status** changed to **Connected**.

FTP Connect Status

Status

Connected

Each time after uploading, the call recordings, voicemails and system logs will be removed from the IPPBX internal storage, call logs will be kept on the IPPBX system and also will make a duplicate on the FTP server.

12.1.3 System Storage

Path: **System -> Storage -> System Storage**

Storage management of recording files and voice data in the system.

USB Storage

FTP Storage

System Storage

Delete All Voicemail

This operation will delete ALL voicemail files

Delete all Voicemail files

Delete All Call Recording

This operation will delete ALL call recording files

Delete all call recording files

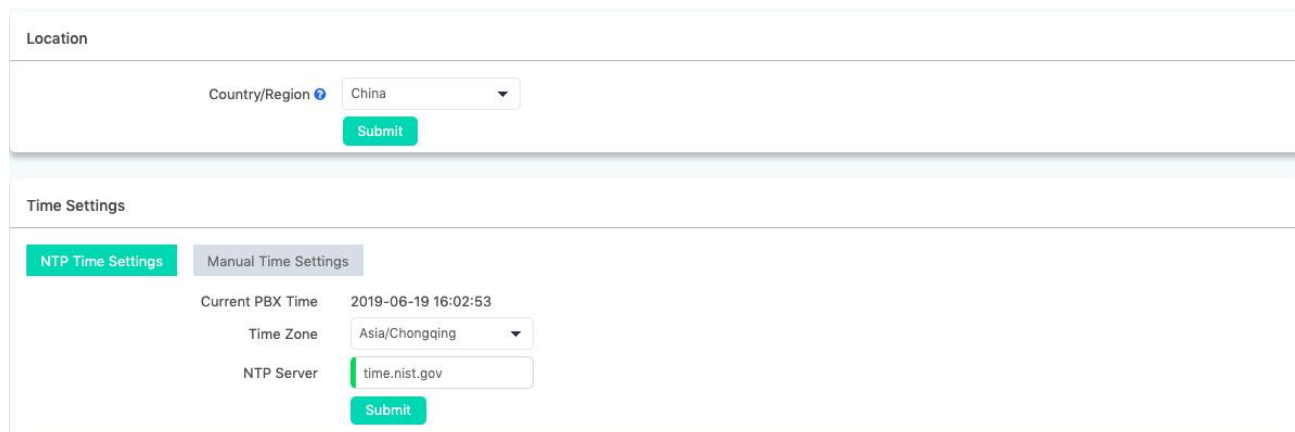
When the system storage is full, you can clear the recording files and voice data files in the system storage.

12.2 Region and Time

Path: **System -> Region and Time**

System time is very important for the IPPBX system, especially when the IPPBX system handles inbound phone calls according to time conditions, then only if the system time is correct will calls be handled properly. Also, call logs and call recordings files are named with system time. If time's not correct on the system, the phone system will not work properly.

At the initial setup while you going through the quick setup wizard your location would be set. If you had skipped the quick setup wizard or you want to change the time zone, you may do it here.



The screenshot shows two sections: 'Location' and 'Time Settings'.

Location: A dropdown menu for 'Country/Region' is set to 'China'. A green 'Submit' button is below it.

Time Settings: Two tabs are visible: 'NTP Time Settings' (active) and 'Manual Time Settings'.

NTP Time Settings:

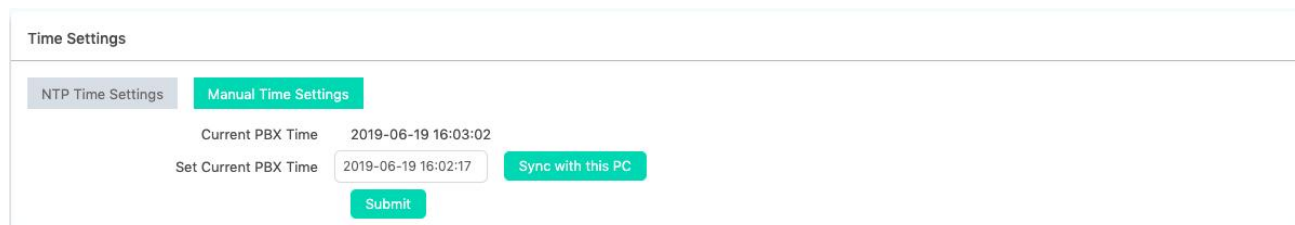
- 'Current PBX Time' is displayed as 2019-06-19 16:02:53.
- 'Time Zone' dropdown is set to 'Asia/Chongqing'.
- 'NTP Server' text input is 'time.nist.gov'.
- A green 'Submit' button is at the bottom.

Location and time may be configured separately. Both modifying location and time settings requires rebooting the IPPBX system.

The location settings will determine the type of tone (Dial tone, Busy, Congestion tone, etc.) you heard on the phones, the time zone and also the opermode on the **Analog Settings** page. So you may not change the location settings here but adjust the time settings only.

You may set the Time Zone and NTP Server to let the IPPBX system synchronize time from the NTP server. This is by default how the system time works.

Or you may manually configure the system time.



The screenshot shows the 'Time Settings' page with the 'Manual Time Settings' tab active.

Manual Time Settings:

- 'Current PBX Time' is displayed as 2019-06-19 16:03:02.
- 'Set Current PBX Time' text input is 2019-06-19 16:02:17.
- A green 'Sync with this PC' button is next to the 'Set Current PBX Time' input.
- A green 'Submit' button is at the bottom.

In the Set Current PBX Time blank, you may manually input the date and time to set it as the current PBX time or you may click on **Sync with this PC** to synchronize the current time of your operating system. Then click on **Submit** button to save the manually set time to the IPPBX hardware.

12.3 Network Settings

12.3.1 Network Profiles

Path: **System -> Network Settings -> Network Profiles**

Network profiles could be configured through the quick setup wizard at the initial setup of the IPPBX system. When modification of the network profiles required, it could be done here.

WAN

Network Mode ⓘ

Static IP ▼

IP Address

192.168.11.146

Netmask

255.255.255.0

Gateway

192.168.11.1

Primary DNS

8.8.8.8

Alternative DNS

114.114.114.114

Enable Virtual IP ⓘ

Off

Save

The WAN network interface of IPPBXs could be configured to work in Static IP, DHCP or PPPoE mode. In most cases assign a static IP would be the best practice. As all the IP phones will communicate with the IPPBX through this IP address.

On WAN port, gateway and DNS could be configured so the IPPBX could have Internet access, as a result, SIP trunking and remote extensions could work.

As for LAN, it's only used when you don't want the IPPBX system to have Internet access.

LAN

IP Address

192.168.10.100

Netmask

255.255.255.0

Enable Virtual IP ⓘ

Off

Save

Default IP on LAN port is 192.168.10.100, you may change this IP but LAN IP should NOT be in the same network segment as WAN port.

12.3.2 IPv6

Path: **System -> Network Settings -> IPv6**

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 IPPBX system with IPv6 addresses to be able to deploy it in your IPv6 network infrastructure.

Enable IPv6

Enable	<input checked="" type="checkbox"/>
IPv6 Address	<input type="text" value="2001:db8:4005:80a::200e"/>
Subnet Prefix Length	<input type="text" value="64"/>
Gateway	<input type="text" value="2001:db8:4005:80a::1"/>
Primary DNS	<input type="text" value="2001:da8:8000:1:202:120:2:1"/>
Alternative DNS	<input type="text"/>
<input type="button" value="Save"/>	

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

12.3.3 Local Domain Name Service

Path: **System -> Network Settings -> Local Domain Name Service**

Local domain name service can be used by the IPPBX system to resolve domain name locally without using the public DNS services, especially when there are problems of domain name resolution of the IMS server using the public DNS servers.

To add a local domain name resolution record, please click on the Add button. Then please specify the domain name of the IMS server and its IP address.

Add

Domain Name

IP Address

Cancel

Submit

12.3.4 VLAN

Path: **System -> Network Settings -> VLAN**

With a layer-3 switch you can configure VLAN on 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.

VLAN Settings

WAN Port VLAN1	
Enable	<input checked="" type="checkbox"/> On
VLAN ID	<input type="text" value="1"/>
IP Address	<input type="text" value="172.16.10.3"/>
Netmask	<input type="text" value="255.255.255.0"/>
WAN Port VLAN2	
Enable	<input checked="" type="checkbox"/> On
VLAN ID	<input type="text" value="2"/>
IP Address	<input type="text" value="172.16.20.3"/>
Netmask	<input type="text" value="255.255.255.0"/>
LAN Port VLAN1	
Enable	<input checked="" type="checkbox"/> On
VLAN ID	<input type="text" value="3"/>
IP Address	<input type="text" value="172.16.30.3"/>
Netmask	<input type="text" value="255.255.255.0"/>
LAN Port VLAN2	
Enable	<input checked="" type="checkbox"/> On
VLAN ID	<input type="text" value="4"/>
IP Address	<input type="text" value="172.16.40.3"/>
Netmask	<input type="text" value="255.255.255.0"/>
<input type="button" value="Save"/>	

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

12.3.5 VPN

Path: **System -> Network Settings -> VPN**

VPN (Virtual Private Network) is mainly used for setting up long-distance and/or secured network connections. When used on the IPPBX system, all phone calls made and received are encrypted so it secures your remote offices/extensions' phone services. Built-in VPN Server on the IPPBX system is an easy way to set up a secured connection between other 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.

IPPBX supports 4 VPN varieties, PPTP VPN, OpenVPN, IPsec and L2TP. On a IPPBX system you can only configure one VPN variety to work in one role. In other words, on a IPPBX system you cannot configure OpenVPN, PPTP VPN, IPsec and L2TP to work at the same time or to configure VPN server and client at the same time.

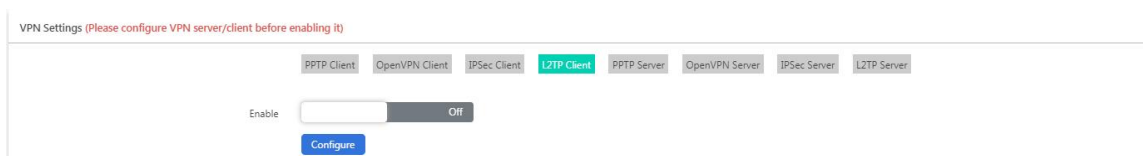
OpenVPN Server

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.

To configure OpenVPN server, please click on the **OpenVPN Server** button to show the configurations.



VPN Settings (Please configure VPN server/client before enabling it)

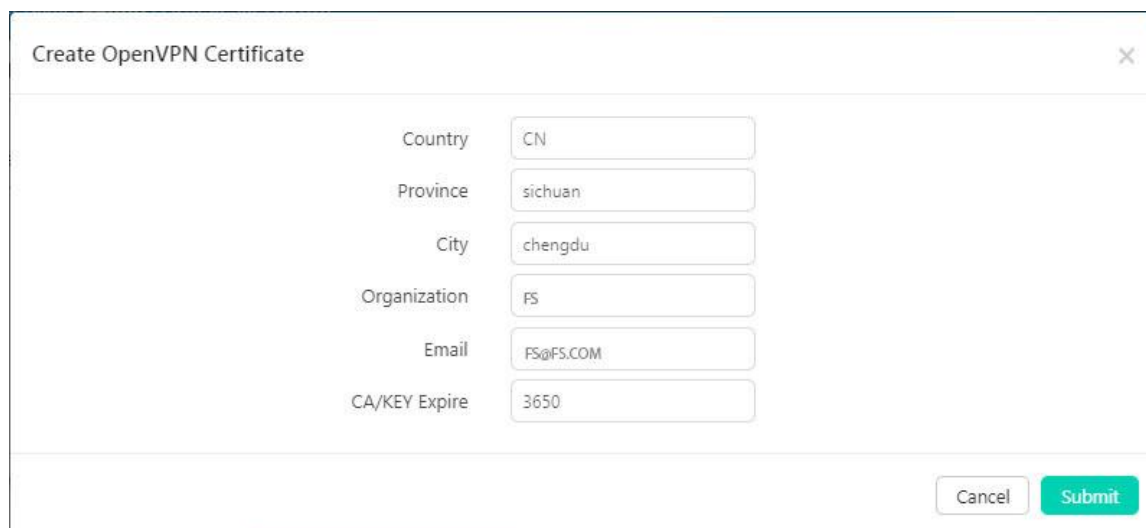
Buttons: PPTP Client, OpenVPN Client, IPsec Client, **L2TP Client**, PPTP Server, OpenVPN Server, IPsec Server, L2TP Server

Enable: ☐ Off

Configure

Configure the VPN server before turning it on.

In the **Certificate** field click on **Create** button to create the OpenVPN certificate.



Create OpenVPN Certificate

Country: CN

Province: sichuan

City: chengdu

Organization: FS

Email: FS@FS.COM

CA/KEY Expire: 3650

Cancel **Submit**

Specify your customized information and click on **Submit** button to continue.

Click on **Configure** button to setup the OpenVPN server.

OpenVPN Server Settings
✕

Stealth ☒ On
Port
Stealth Port
Protocol
Device Node
Cipher
Compress LZO ☒ On
TLS Server ☒ On
Remote Network /
Route /
Client to Client ☒ On

Cancel Submit

- **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.
- **Port:** OpenVPN service port, the default port is 1194. You will need to forward this port on your router for the clients being able to connect to the server.
- **Stealth Port:** OpenVPN service port, the default is 1194.
- **Protocol:** You can choose either UDP or TCP. But the port forwarding (1194) on your router should be using the same protocol.
- **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:** The OpenVPN client network, VPN server uses the first available IP of the client 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.

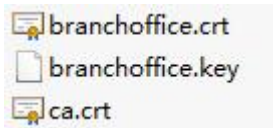
Once configurations done, click on Submit button to save the configurations and you may create certificates for the OpenVPN clients now. Each VPN client needs a certificate to be able to connect to the server. OpenVPN server on IPPBX system can connect up to 20 clients.

VPN Client Certificate Download ?
Create New VPN Certificate

User Name	Options
brachoffice	↓ 🗑

1 Total

Each certificate entry created here is for an OpenVPN client. Download the certificate and extract files inside the package, 3 files you'll get and they should be uploaded on a client to be able to connect to this server.



Finally turn on the enable switch to enable OpenVPN server.

OpenVPN Client

To configure OpenVPN client, please click on the **OpenVPN Client** button to show the configurations.

VPN Settings (Please configure VPN server/client before enabling it)

[PPTP Client](#)
[OpenVPN Client](#)
[IPSec Client](#)
[L2TP Client](#)
[PPTP Server](#)
[OpenVPN Server](#)
[IPSec Server](#)
[L2TP Server](#)

Enable ☐ Off

CA Certificate ?	None	Upload	Delete
Client Certificate ?	None	Upload	Delete
Client Key ?	None	Upload	Delete

[Configure](#)

The certificate files downloaded from the OpenVPN server should be uploaded here.

In the **CA Certificate** field upload the ca.crt file.

In the **Client Certificate** field upload the xxxx.crt file.

In the **Client Key** field upload the xxxx.key file.

When done, click on the [Configure](#) button to configure the OpenVPN client to connect to the server.

OpenVPN Client Config

Server Address ?

192.168.11.18

Stealth

Off

Port ?

1194

Protocol ?

UDP

Device Node ?

TUN

Cipher ?

Default

Compress LZO ?

On

Default Gateway ?

On

Cancel

Submit

- In the **Server Address** field you should specify the OpenVPN server address, which can be a public IP or a domain name.
- Enable **Stealth** if the OpenVPN server has enabled it.
- The **Port** number should be exactly the same as on the OpenVPN server. By default it's 1194.
- Please use the same **Stealth Port** as the OpenVPN server.
- The transport **Protocol** should be exactly the same as on the OpenVPN server. By default UDP is used.
- **Device Node** could be set to TUN or TAP, a TAP device is a virtual Ethernet adapter, while a TUN device is a virtual point-to-point IP link.
- **Cipher** (or Cypher) is an algorithm for performing encryption or decryption.

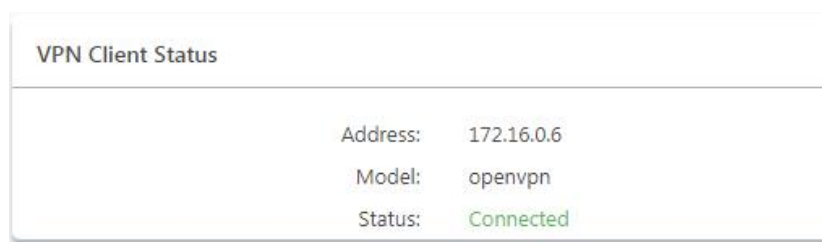
- Either to enable **Compress LZO** or not, depends on if you have enabled it on the server.
- If **Default Gateway** enabled, it will use VPN connection as default gateway, data which should be sent to the default gateway will now be sent though VPN connection.

Once done, click on submit to save the configurations. Finally click on Enable switch to switch on the VPN client connection.

VPN Settings (Please configure VPN server/client before enabling it)



And you may check the VPN connection status in the **VPN Client Status** section.



In the VPN client status section the VPN client IP, the VPN type and the connection status will be displayed.

PPTP VPN Server

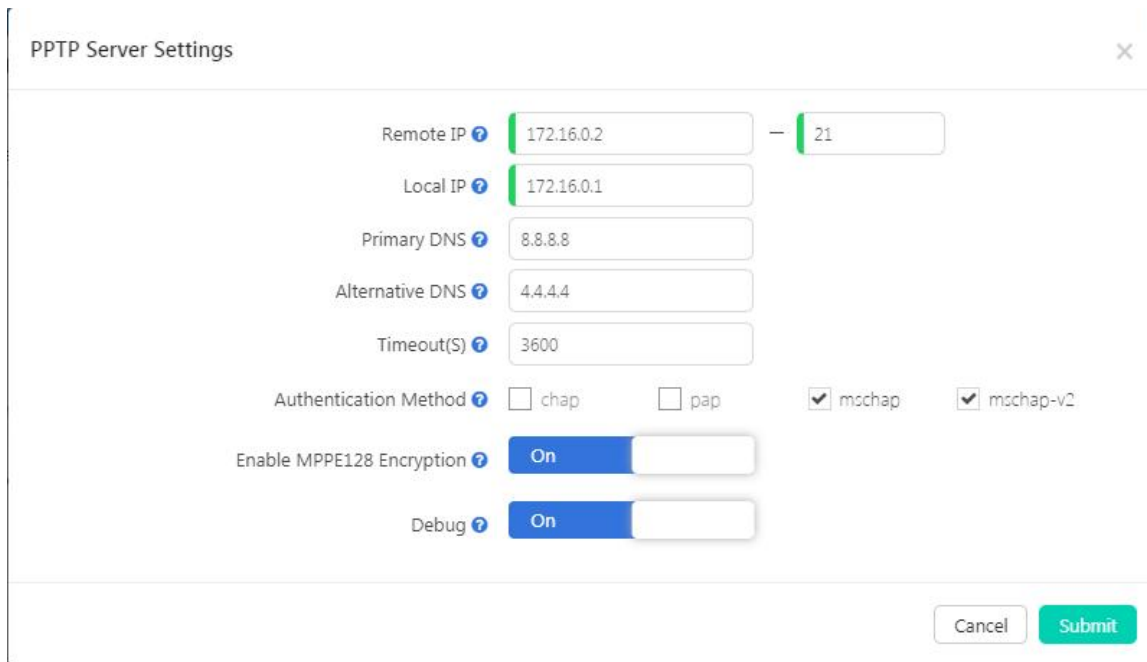
PPTP (The Point-to-Point Tunneling Protocol) uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The intended use of this protocol is to provide security levels and remote access levels comparable with typical VPN products.

Click on **PPTP Server** button to show the configurations.

VPN Settings (Please configure VPN server/client before enabling it)



Configure the PPTP VPN server before enabling it.



PPTP Server Settings

Remote IP —

Local IP

Primary DNS

Alternative DNS

Timeout(S)

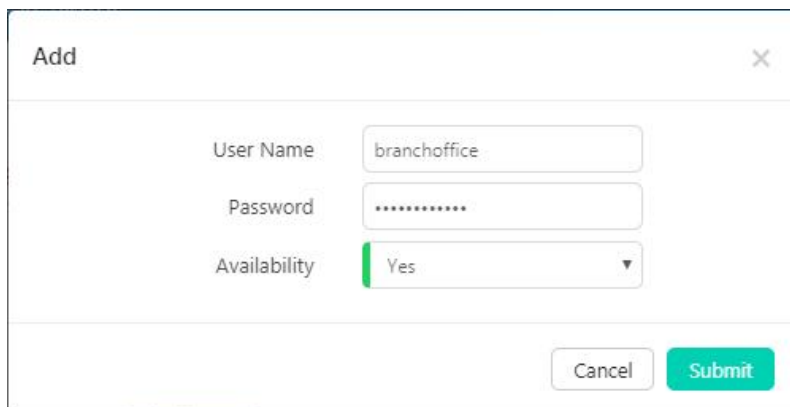
Authentication Method ☐ chap ☐ pap ☒ mschap ☒ mschap-v2

Enable MPPE128 Encryption ☐ On

Debug ☐ On

- **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(S):** 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 Encryption:** 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:** Enable debug for PPTP VPN connection, debug information will be written into system logs.

Once server configurations done, you may create PPTP client users, each user created is for a VPN client to connect. PPTP VPN server on IPPBX can connect up to 20 PPTP VPN clients.





Add

User Name

Password

Availability

Remember to set the Availability to Yes, when you don't want this user to connect, just set Availability to No or you may remove the user from the VPN user list.

List of VPN Users Add		
User Name	Availability	Options
branchoffice	true	 
1 Total		

Finally click on the Enable switch to turn the PPTP VPN server on.

VPN Settings (Please configure VPN server/client before enabling it)

PPTP Client
OpenVPN Client
IPSec Client
L2TP Client
PPTP Server
OpenVPN Server
IPSec Server
L2TP Server

Enable On 


Configure

PPTP VPN Client

To configure PPTP VPN client, please click on the PPTP Client button to show the configurations.

VPN Settings (Please configure VPN server/client before enabling it)

PPTP Client
OpenVPN Client
IPSec Client
L2TP Client
PPTP Server
OpenVPN Server
IPSec Server
L2TP Server

Enable Off 

Configure

Configure PPTP VPN client settings before enabling it.

PPTP Client Config

Enable 40/128-bit Encryption for MPPE

On

Server Address

1.1.1.1

User Name

branchoffice

Password

Default Gateway

Off

Cancel

Submit

- **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:** If enabled, all network traffic will go through the PPTP VPN connection.

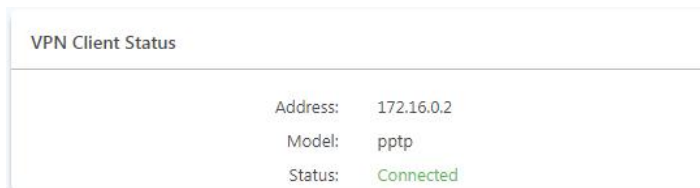
Once done, click on Submit button to continue, and now you may click on Enable switch to turn on PPTP VPN client.

VPN Settings (Please configure VPN server/client before enabling it)



The interface shows a row of tabs: PPTP Client, OpenVPN Client, IPSec Client, L2TP Client, PPTP Server, OpenVPN Server, IPSec Server, and L2TP Server. The 'PPTP Client' tab is active. Below the tabs, there is an 'Enable' section with a toggle switch set to 'On' and a 'Configure' button below it. A red rectangle highlights the 'Enable' section.

Later it should be connected to the PPTP VPN server, and the connection status will be displayed in the **VPN Client Status** section.



The 'VPN Client Status' section displays the following information:

Address:	172.16.0.2
Model:	pptp
Status:	Connected

In the VPN client status section the VPN client IP, the VPN type and the connection status will be displayed.

IPSec VPN Server

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 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 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.

Click on **IPSec Server** button to show the configurations.



The interface shows the same row of tabs as before, but now the 'IPSec Server' tab is active. The 'Enable' section shows a toggle switch set to 'Off' and a 'Configure' button below it.

Configure the IPSec Server before enabling it.

IPSec Server Settings

Type ?

Tunnel

IPSec Local IP ?

117.176.159.163

Password

IPSec Remote IP 1 ?

192.168.1.252

IPSec Remote Network 1 ?

192.168.200.0 / 255.255.255.0

IPSec Remote IP 2 ?

192.168.1.148

IPSec Remote Network 2 ?

192.168.10.0 / 255.255.255.0

IPSec Remote IP 3 ?

IPSec Remote Network 3 ?

Cancel

Submit

- **Type:** Defaults to Tunnel mode. IPSec Tunnel mode is used to encrypt all traffic between secure IPSec Gateways.
- **IPSec Local IP:** IPPBX WAN IP, which can be used to connect to the client network.
- **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 IPPBX is behind NAT, port 500 and 4500 must be open on the router/firewall.
2. If the 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 Client (Tunnel mode)

To configure IPSec VPN Client, please click on the **IPSec Client** button to show the configurations.

VPN Settings (Please configure VPN server/client before enabling it)

PPTP Client

OpenVPN Client

IPSec Client

L2TP Client

PPTP Server

OpenVPN Server

IPSec Server

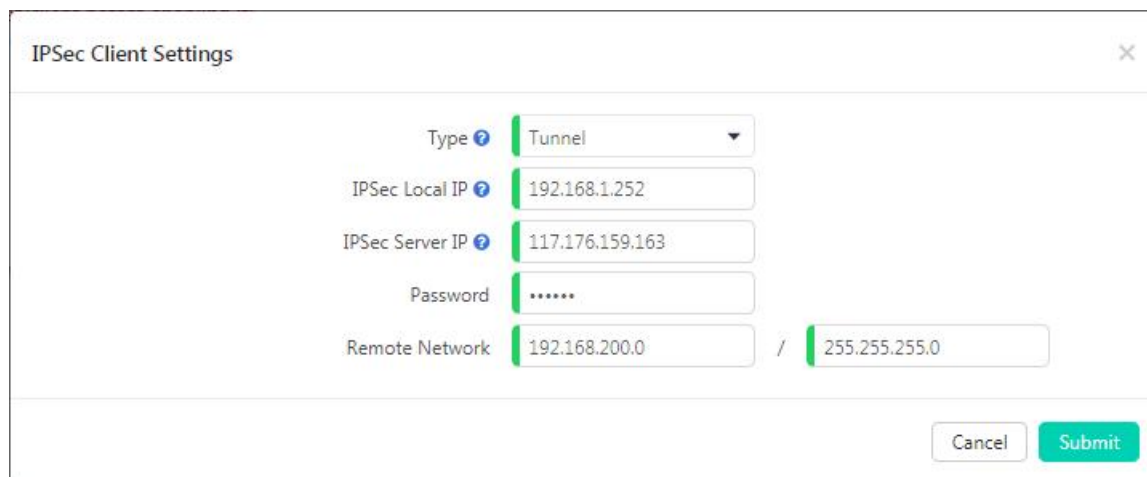
L2TP Server

Enable

Off

Configure

Configure IPSec VPN client settings before enabling it.




The dialog box titled "IPSec Client Settings" contains the following fields:

- Type: Tunnel (dropdown menu)
- IPSec Local IP: 192.168.1.252
- IPSec Server IP: 117.176.159.163
- Password: *****
- Remote Network: 192.168.200.0 / 255.255.255.0

Buttons: Cancel, Submit

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

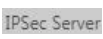
Once done, click on  button to continue, and now you may click on Enable switch to turn on IPSec VPN client.

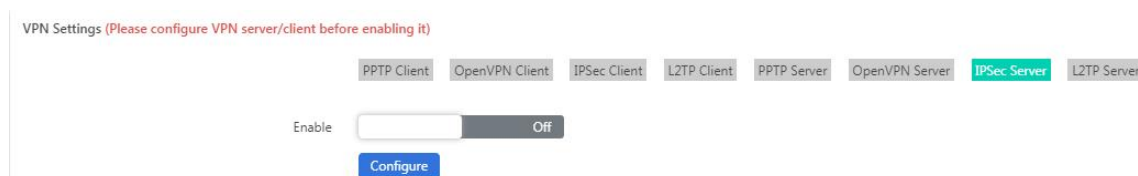
Notice

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 IPPBX's are connected via IPSec transport mode, IPSec only encrypts the communication service ports, unlike Tunnel mode which encrypts the whole LAN subnet.


Click on  button to show the configurations.



VPN Settings (Please configure VPN server/client before enabling it)

Navigation tabs: PPTP Client, OpenVPN Client, IPSec Client, L2TP Client, PPTP Server, OpenVPN Server, **IPSec Server**, L2TP Server

Enable: ☐ Off



Configure the IPSec Server before enabling it.

IPSec Server Settings

Type ? Transport

IPSec Local IP ? 117.176.159.163

Password *****

Cancel

Submit

- **Type:** Select Transport mode.
- **IPSec Local IP:** IPPBX WAN IP.(This is the same as configuring in Tunnel mode)
- **Password:** Define a password for authentication of the IPSec client.

IPSec VPN Client (Transport mode)

To configure IPSec VPN Client, please click on the **IPSec Client** button to show the configurations.

VPN Settings (Please configure VPN server/client before enabling it)

PPTP Client

OpenVPN Client

IPSec Client

L2TP Client

PPTP Server

OpenVPN Server

IPSec Server

L2TP Server

Enable

Off

Configure

Configure IPSec VPN client settings before enabling it.

IPSec Client Settings

Type ? Transport

IPSec Local IP ? 192.168.1.252

IPSec Server IP ? 117.176.159.163

Password *****

Cancel

Submit

- **Type:** Ensure this is the same as the IPSec VPN server.
- **IPSec Local IP:** IPPBX WAN IP which can connect to the IPSec server.
- **IPSec Server IP:** IPSec VPN server IP
- **Password:** Specify the IPSec VPN password defined previously on the server.

Once done, click on **Submit** button to continue, and now you may click on Enable switch to turn on IPSec VPN client.

Notice

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

L2TP 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 IPPBX system we use IPSec to do the encryption.

To configure L2TP server, please click on the **L2TP Server** button to show the configurations.

VPN Settings (Please configure VPN server/client before enabling it)

Enable ☐ Off ☐

Configure the L2TP Server before enabling it. Click on button to setup the OpenVPN server.

L2TP Server Settings
×

Client Network Start IP ?

Client Network End IP ?

Server Local IP ?

Primary DNS

Alternative DNS

Authentication Method ?

☒ chap ☒ pap

Debug ?

☐ On ☐

Enable IPSec ?

☐ On ☐

IPSec Local IP ?

IPSec Password

- **Client Network Start IP, Client Network End IP:** L2TP VPN remote network IP range, between start IP and end IP there must be less than 10 available IP addresses.
- **Server 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.
- **Enable IPSec:** Enable IPSec encryption for L2TP VPN server.
- **IPSec Local IP:** WAN IP which can access Internet.
- **IPSec Password:** Define a password for IPSec VPN client to authenticate.

Notice

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

Once configurations done, click on **Submit** button to save the configurations and you may create L2TP client users, each user created is for a VPN client to connect.

Add
×

User Name

Password

Availability

Yes



▼

Cancel

Submit

Remember to set the Availability to Yes, when you don't want this user to connect, just set Availability to No or you may remove the user from the VPN user list.

List of VPN Users **Add**

User Name	Availability	Options
branchoffice	Yes	 
1 Total		

Finally click on the Enable switch to turn the L2TP server on.

VPN Settings (Please configure VPN server/client before enabling it)

PPTP Client

OpenVPN Client

IPSec Client

L2TP Client

PPTP Server

OpenVPN Server

IPSec Server

L2TP Server

Enable

On



Configure

L2TP Client

To configure L2TP client, please click on the **L2TP Client** button to show the configurations.

VPN Settings (Please configure VPN server/client before enabling it)

PPTP Client

OpenVPN Client

IPSec Client

L2TP Client

PPTP Server

OpenVPN Server

IPSec Server

L2TP Server

Enable



Off

Configure

Click on the **Configure** button to configure the L2TP client to connect to the server.

L2TP Client Settings
✕

Server IP ?

Username ?

Password

Enable IPSec ?

On

IPSec Local IP ?

IPSec Password

Default Gateway ?

On

Cancel

Submit

- **Server IP:** L2TP server public IP.
- **Username:** L2TP VPN user name given by the VPN server.
- **Password:** L2TP VPN user password given by the VPN server.
- **Enable IPSec:** Enable IPSec support.
- **IPSec Local IP:** 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.

Once done, click on submit to save the configurations. Finally click on Enable switch to switch on the L2TP client connection.

VPN Settings (Please configure VPN server/client before enabling it)

PPTP Client

OpenVPN Client

IPSec Client

L2TP Client

PPTP Server

OpenVPN Server

IPSec Server

L2TP Server

Enable

On

Configure

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)

12.3.6 Static Routing

Path: **System -> Network Settings -> 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.

When needed you may click on the Add button to add a manual static route.

Add Static Route

Destination ? 222.209.4.1
Netmask ? 255.255.255.255
Gateway ? 192.168.10.1

Cancel Submit

- **Destination** is the IP address of the destination host or network address.
- If the packets are to be sent to the **Destination** specified above then send them to the **Gateway** address.

After the new record has been manually created you will see it listed in the route table.

12.3.7 DHCP Server

Path: **System -> Network Settings -> 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 IPPBXs WAN/LAN port which saves administrators a lot of time when compared with having to configure these settings manually.

Before activating DHCP services, please ensure there's no other DHCP server running in your LAN, otherwise there will be collision between servers.

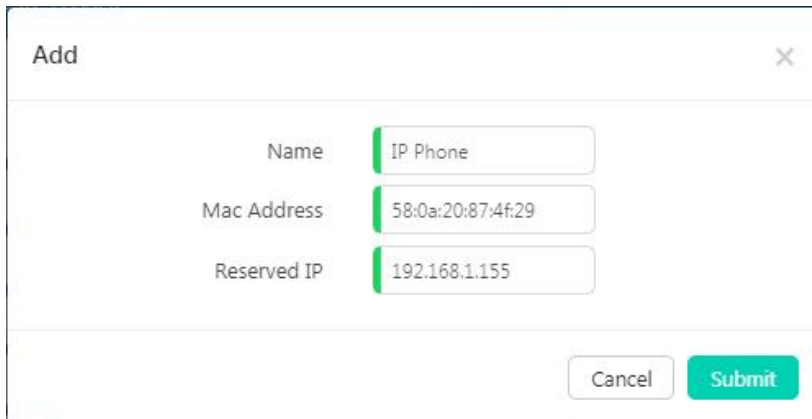
Set the DHCP server network parameters and turn it on.

DHCP Services

Enable ? On
Port ? LAN
Start IP Address ? 192.168.10.150
End IP Address ? 192.168.10.199
Netmask ? 255.255.255.0
Default Gateway ? 192.168.10.1
DNS ? 192.168.10.1
TFTP ?
Address Lease Time(Sec) ? 86400
Submit

The DHCP clients which obtained IP addresses from the IPPBX system DHCP server will be listed on the right side of the page, in the **DHCP Clients** section.

If you want some host or client to always get the same IP address, **IP Address Reservation** will help.



The 'Add' dialog box for IP Address Reservation contains the following fields and buttons:

Field	Value
Name	IP Phone
Mac Address	58:0a:20:87:4f:29
Reserved IP	192.168.1.155

Buttons: Cancel, Submit

Just simply specify the MAC address of the client device and associate an IP address with it, and this IP will always be reserved for this specific client device.

12.3.8 DDNS

Path: **System -> Network Settings -> 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.

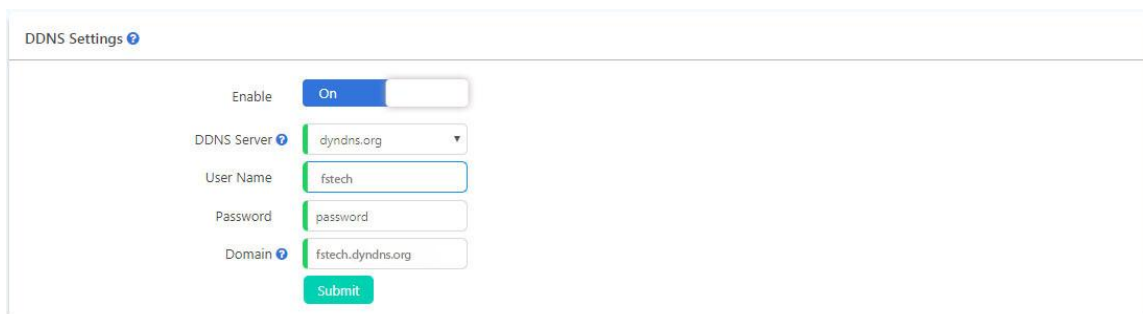
Built-in DDNS feature on IPPBX system only requires you to sign up with a Dynamic DNS provider, then with the domain name they provide which maps your IP address on the Internet, you can access IPPBX and also other services within your LAN via the domain name without needing to know your Dynamic public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

After setting DDNS, 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.

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, register it here and you DDNS domain will work with the IPPBX system.



The 'DDNS Settings' page includes the following configuration options:

Option	Value
Enable	On
DDNS Server	dyndns.org
User Name	fstech
Password	password
Domain	fstech.dyndns.org

Buttons: Submit

After completing the above, please configure port forwarding on your router/firewall, then you'll be able to remote access IPPBX services from the internet using this dynamic domain. For example, you can port forward port number 443 and then you can access the IPPBX web interface by using the URL: <http://tech.dyndns.org>.

12.3.9 SNMP

Path: **System -> Network Settings -> SNMP**

SNMP Config

Read Only	
Enable	<input checked="" type="checkbox"/> On
Community	<input type="text" value="public"/>
Network	<input type="text" value="192.168.13.0"/> / <input type="text" value="24"/>
Read Write	
Enable	<input type="checkbox"/> Off
Community	<input type="text" value="private"/>
Network	<input type="text" value="192.168.10.0"/> / <input type="text" value="24"/>
<input type="button" value="Save"/>	

- **Enable:** Turn On/OFF SNMP
- **Community:** Community tag
- **Network:** The working network of SNMP

12.4 Security Center




IPPBX system has been preconfigured with a built-in firewall which prevents your IP phone system from unauthorized access, malicious users and some other attackers.

You may not need to specifically configure the firewall settings but for security precautions please always keep it on.

12.4.1 Firewall

Path: **System -> Security -> Firewall**

IPPBX system uses Fail2Ban to perform intrusion detection and uses iptables to block any attack attempts.

Firewall 	<input checked="" type="checkbox"/> On	Drop Ping 	<input type="checkbox"/> Off
Drop All 	<input type="checkbox"/> Off	Geo IP 	<input type="checkbox"/> Off

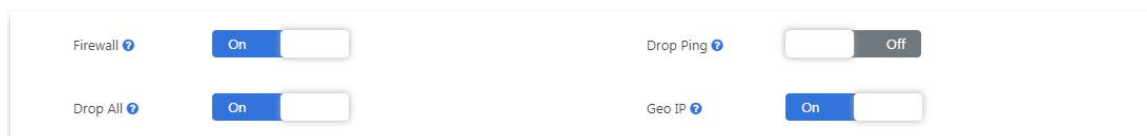
- First of all make sure the **Firewall** option is enabled. Only consider disabling your firewall if your IPPBX is behind a router/firewall without any port forwarding from the Internet.
- **Drop Ping** will cause the system to ignore ping request. If enabled, you cannot ping the IPPBX system.
- **Drop All** will cause all packets sent to the IPPBX system being dropped, this will cause IPPBX system to block all communication

with the outside world. Except web UI still works in local network, other services will all be terminated.

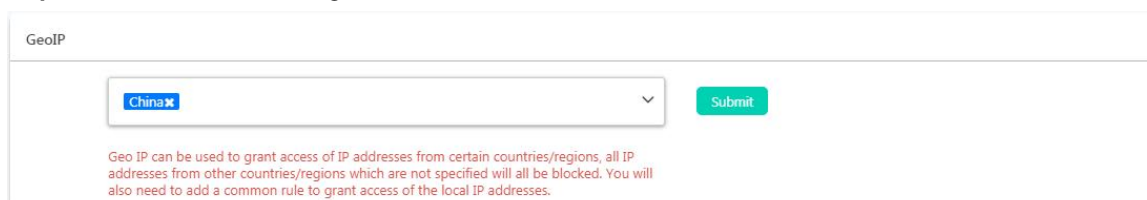
- **Geo IP** is a security policy which can be used to grant access of IP addresses from certain countries/regions, all IP addresses from other countries/regions which are not specified will all be blocked. By default, web UI will still be accessible. Enabling **Geo IP** requires **Drop All** to be enabled too.

To implement Geo IP please follow the steps below.

Step 1: Enable Geo IP and Drop All

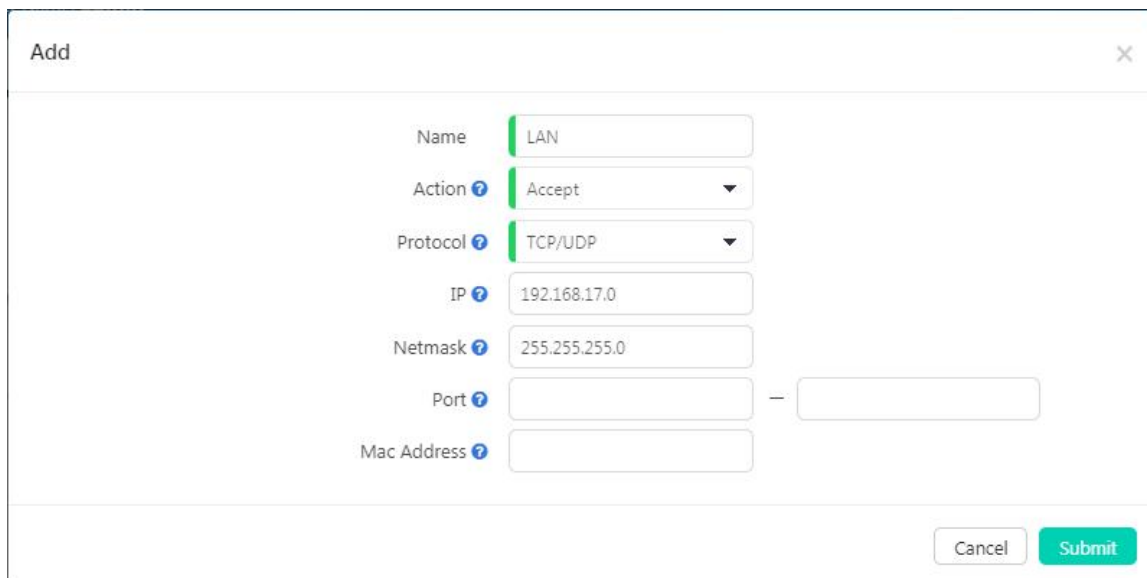


Step 2: Select trusted countries/regions



Besides selecting the trusted IP addresses from certain countries/regions, you'll still need to add a common rule in the **Common Rules** section to grant access or the local network hosts/devices.

Step 3: Add a common rule to grant access of your local LAN.











- The **Action** of this rule needs to be set as **Accept**.
- **Protocol** should be set as **TCP/UDP**.
- **IP** should be the local network address instead of a single IP address.
- **Netmask** should be the subnet mask of the network address.
- The **Port** range determines which kind of services to be granted. In this case you may leave it blank to grant local network all access to the IPPBX system.
- **Mac Address** determines the action to be taken according to the Mac address of a device instead of its IP address, it only works with devices within the same local network because Mac addresses are not routable. In this case you are going to grant access of all the local network hosts/devices, so you may leave it blank.

By now, Geo IP security policy should work. The private IP addresses from your local network and the public IP addresses from the countries/regions you've selected should be able to access your IPPBX system. Other IP addresses will all be blocked.

Common Rules can be used to 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. The priority from high to low of the firewall rules is from the top of the list to the bottom.

If you are going to grant access of some kind of services to specific IP address or network, add the grant rule/rules first then add the deny rules. If the order of the rules is not correct you may use the arrows in the **Priority** column to adjust the order of the rules.

Common Rules Add							
Priority	Name	Action	Protocol	IP	Port	Mac Address	Options
 	AcceptAMI	Drop	TCP/UDP	192.168.17.0/255.255.255.0	5038		 
 	BlockAMI	Drop	TCP/UDP		5038		 
2 Total							

In the above given example, the 2 rules "AcceptAMI" and "BlockAMI" limited that only the IP addresses from network 192.168.17.0 can have AMI access. Except IP from this network others will all be denied to access. In this case, if the "AcceptAMI" rule is moved beneath the "BlockAMI" rule, then the AMI port will be totally lockdown, no one can access it.

Notice

If you are going to add rules to block some IP addresses from accessing some kind of services on the IPPBX system, be sure you add the correct IP/network address (if not defined, the firewall will consider as ALL), and the correct service port number (if not define, the firewall will consider as ALL), otherwise misconfiguration of a deny rule might cause the IPPBX system total lockdown, only way would be using Console (PBX-C301) or HDMI (PBX-C302M and PBX-C503) to unlock the IPPBX from command lines.

Auto Defense will help with the prevention of DDOS attacks.

Add ×

Name

AMI

Port

5038

Protocol

TCP

Packet

20

Interval

60

Cancel

Submit

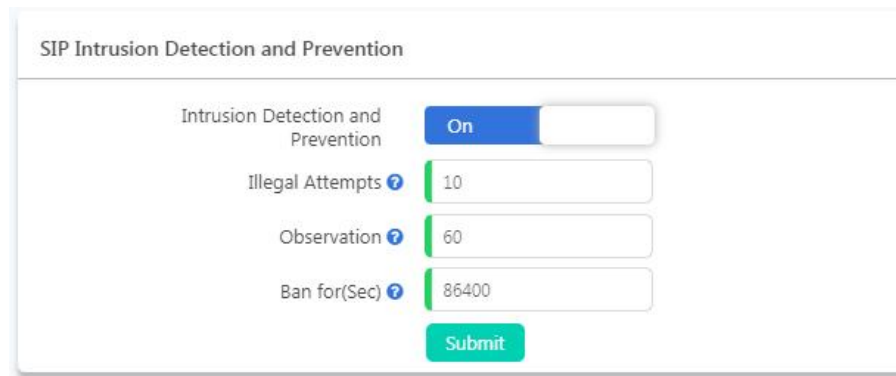
You may specify the service port number and the maximum packets to be accepted on this port number in a certain time interval. Except the specified number of packets, more packets sent within the time interval will be dropped by the IPPBX system.

12.4.2 Intrusion Detection and Prevention

Path: **System -> Security Center -> Intrusion Prevention**

IPPBX system uses Fail2Ban to perform intrusion detection. 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.

There are 4 default intrusion detection and prevention rules to secure SIP, IAX2, Web and SSH services on your IPPBX system. And by default all of them are activated to keep your IPPBX system safe.



SIP Intrusion Detection and Prevention

Intrusion Detection and Prevention ☒ On

Illegal Attempts

Observation

Ban for(Sec)

Each of the intrusion detection and prevention rule is configured with a maximum **Illegal Attempts** and the **Observation** time duration, once the **Illegal Attempts** reached the given value in the given **Observation** time duration, the source IP address of where the illegal attempts coming from will be banned by the firewall for the given time duration specified in Ban for field. Banned IP will be listed on the **IP Blacklist** page.


Besides the 4 default rules, if you want to add more rules you can do it on the **Firewall** page **Auto Defense** section.

12.4.3 IP Blacklist

Path: **System -> Security Center -> IP Blacklist**

IP Blacklist will list all suspected intruders/attackers' IP addresses. The list is automatically generated by the system firewall if possible intrusion/attacking had been detected. And the list will show the IP address of the banned hosts, as well as what kind of service intrusion was detected.

Type	IP	Options
HTTPS	117.136.70.48	
1 Total		

If an IP address appears incorrectly in the list of rejected IP, you can click on the  button to remove it from the IP blacklist.

12.4.4 IP Whitelist

Path: **System -> Security Center -> IP Whitelist**

IP Whitelist allows you to add IP addresses and network addresses to the IPPBX system as a trusted. The IP addresses in the whitelist will always be treated as trusted IP and will not be regulated by the firewall rules.

Add
×

Name

Protocol ☒ SIP ☒ IAX ☒ HTTPS ☐ SSH

IP Address

Netmask

Enable ☒ On

Cancel Submit

Adding a trusted IP to the IP whitelist, you may also define which kind of services it could access.

- **SIP** allows the IP to be able to register SIP extensions.
- **IAX** (IAX2) allows the IP to be able to register IAX extensions.
- **HTTPS** allows the IP to access the web UI of the IPPBX system.
- **SSH** allows the IP to access the IPPBX system command lines through SSH.

Notice

You'll only need to add trusted IP addresses to the IP Whitelist when you have configured Drop All or Geo IP security policies. And in the policies these IP addresses are not included as trusted IP addresses. Otherwise you don't have to add them to the IP whitelist.

12.5 Email Services

12.5.1 Mail Server Settings

Path: **System -> Email Services -> Mail Server Settings**

Various kinds of Emails could be sent from the IPPBX system. The Emails could be automatically sent by the IPPBX system in certain circumstances or manually sent by admin and operator users.

To configure the IPPBX system being able to send out emails, mail (SMTP) server needs to be configured at first priority. At the initial system setup stage while you were going through the quick installation wizard, mail server could be configured, if you've not done it from the wizard, it still can be configured from here.

We have built-in some popular Email service providers' SMTP configuration templates for users to quickly deploy their mail server.

Mail Server Settings

Mail Service Provider

SMTP Server

Port

SSL ☒ On

Email

Password

Submit Test

- In the **Mail Service Provider** dropdown list select your Email service provider. If it's not included here, please choose **Other**.

- Once you have selected the mail service provider the **SMTP Server** field will be auto filled. Otherwise you'll have to manually input the SMTP Server address.
- Default SMTP service **Port** is 25, but with SSL/TLS it would be 465. Otherwise you'll have to input the actual port number your mail service provider uses.
- **SSL** encrypts a communication channel between the IPPBX system and the SMTP server. Most of the mail service providers have implemented SSL support.
- In the **Email** field input the Email account to be used by the IPPBX system, all mails from the IPPBX system will be sent out by this mail account.
- In **Password** field input the password of the Email account you have specified.

Once done the above settings, click on **Submit** button to make configurations effective. And you may click on **Test** button and input an Email address to send a test email to verify if the mail server is successfully deployed.

Notice

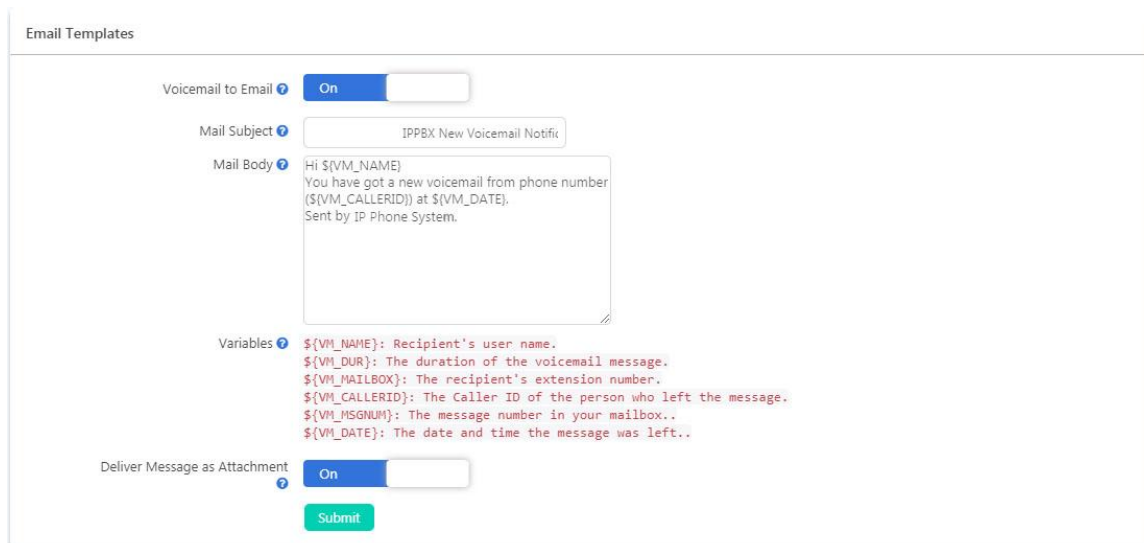
You may need to activate SMTP service from your Email web portal before you can successfully configure SMTP server on the IPPBX system.

12.5.2 Voicemail to Email Settings

Path: **System -> Email Services -> Voicemail to Email Settings**

Voicemail to Email is a very useful feature for the extension users, as the IPPBX system has the ability to send received new voicemail messages of their extensions to their Email box.

It could be an Email notification or administrator could set the IPPBX system to send Email with voice messages attached in the Email notifications.



The screenshot shows the 'Email Templates' configuration page. At the top, there's a toggle for 'Voicemail to Email' set to 'On'. Below it, the 'Mail Subject' field is set to 'IPPBX New Voicemail Notifik'. The 'Mail Body' field contains a template: 'Hi \${VM_NAME} You have got a new voicemail from phone number (\${VM_CALLERID}) at \${VM_DATE}. Sent by IP Phone System.' Below the mail body, there's a 'Variables' section listing:

- `${VM_NAME}`: Recipient's user name.
- `${VM_DUR}`: The duration of the voicemail message.
- `${VM_MAILBOX}`: The recipient's extension number.
- `${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..

 At the bottom, there's a toggle for 'Deliver Message as Attachment' set to 'On', and a 'Submit' button.

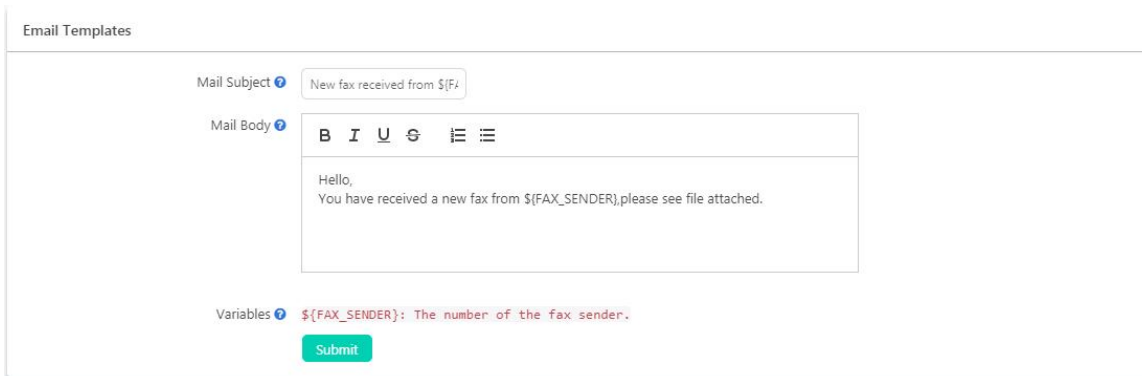
- The **Mail Subject** field you can set customized Email subject which will be received by the extension users when they have new messages.
- The **Mail Body** is also customizable, you may use variables in the mail body to describe the new voice messages they got. The format of the variables must be the same as listed in the **Variables** section.
- **Variables** could be used in the mail body to indicate the extension users about their new voice message details.
- With **Deliver Message as Attachment** option enabled the voice message will be attached to the notify Email, users may playback the voice messages when they got the notify Email.

With Voicemail to Email enabled and Mail Server configured, the extension users will get Email notifications when new voice message received on their extensions, just make sure the extensions have their Email addresses specified.

12.5.3 Fax to Email Settings

Path: **System -> Email Services -> Fax to Email Settings**

If you have configured the IPPBX system to send the inbound fax as Email, here on this page is where you configure the Email templates.

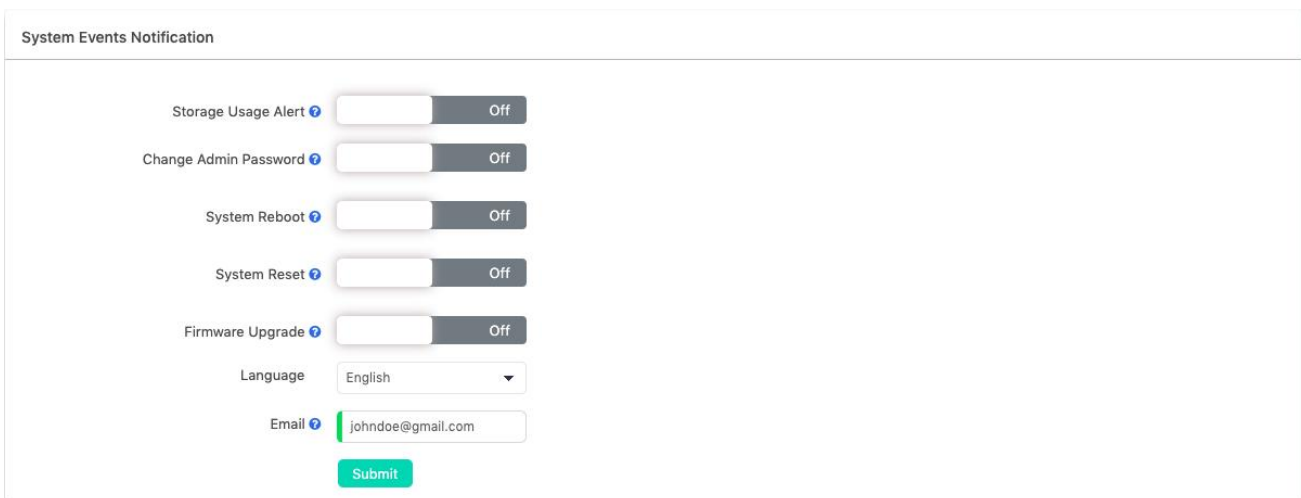


You may customize the fax notification mail subject and mail body. The variable `${FAX_SENDER}` could be used in mail subject or mail body to describe who sent the fax.

12.5.4 Email Notifications

Path: **System -> Email Services -> Email Notifications**

You may configure the IPPBX system to send Email notifications to the administrator on some system events.



- **Storage Usage Alert** can be used to notify the administrator about the system internal storage usage when reached the threshold.
- **Change Admin Password** can be used to notify the administrator about the admin password changing.
- **System Reboot** can be used to notify the administrator after a system reboot. No matter after a manual reboot or a power failure.
- **System Reset** can be used to notify the administrator before resetting the IPPBX system to factory defaults.
- **Firmware Upgrade** can be used to notify the administrator before upgrading the IPPBX system firmware.
- **Language** sets the email body language to be sent to the system administrator.
- In the **Email** field you should specify the Email address of who's responsible to respond to these system events.

13 Maintenance

13.1 Users

There are 4 user roles could be used to manage the IP PBXes.

- **Admin**

Admin user is mainly used for IPPBX system administrations from the IPPBX web interface, including all system advanced configurations and management.

- **Operator**

Operator user is mainly used by the company receptionist, secretary or some other employee who's responsible for managing the departments, extensions, call logs, recordings, faxes, some common call features, etc.

- **API User**

API user is used for secondary development, for the IPPBX system being able to integrated with third party systems.

- **Conference Manager**

Conference manager can be used to start and manage a conference from the Web interface.

- **Root**

Root user is used by highly experienced technicians for advanced managing and troubleshooting the IPPBX system from command line level.

13.1.1 Admin User

Path: **Maintenance -> Users -> Admin User**

Admin user password should be changed regularly on this page. And the password should be at least 6 characters long and contain a combination of letters, digits and symbols.

13.1.2 Operator User

Path: **Maintenance -> Users -> Operator User**

Admin user could change the operator password here on this page when needed. And can turn AMI (Asterisk Management Interface, port 5038) access with operator credentials on or off.

AMI access using operator credentials can be used to achieve some CTI (Computer Telephony Integration) implementations.

13.1.3 API User

Path: **Maintenance -> Users -> API User**

Please create API user only when third party integration is required. Admin user could change the API password here on this page when needed.

13.1.4 Conference Manager

Path: **Maintenance -> Users -> Conference Manager**

By default there's no conference manager account, you have to create one.



Click on Create User button to create a conference manager user account.

User Info ?

User Name:

conference-8yw

Password:

ZMbqQ!2fv0

Delete User

Change Password

New Password (Strong) ?

ZMbqQ!2fv0

Submit

Conference Manager Extension

Extension Number ?

Please Select

Submit

The user name is generated in “conference-xxx” format, and a random password will be generated for this user account. The password could be changed but please use strong password for security reasons. An extension need to be assigned to the conference manager, the conference manager will use this extension number to join and manage the conferences.

After creating the user please give the credentials to the conference manager user. By using these credentials the user can login to the IP PBX Web interface to start and manage conferences. For more details please refer to the [Web conference manager user guide](#).

13.1.5 Root User

Path: **Maintenance -> Users -> Root User**

Root user password could be managed by admin user as well. When admin user modifies the root password for the first time, admin needs to provide the old (default) root password which is the last 8 characters of the IPPBX WAN port MAC address.

By default, SSH access to the IPPBX system is disabled. When enabled, user may access the IPPBX system Linux command line interface via SSH on port 22.

If you are not a highly experienced Linux user with Asterisk command line troubleshooting skills, for security precautions please DO NOT enable SSH.

13.2 Upgrade

The downloaded firmware package should be in .rar or .zip format, please extract the package first and upgrade with the ulmage-md5.xxx file to upgrade your IPPBX system.

Path: **Maintenance -> Upgrade**

The current firmware version and the last time when the firmware was upgraded will be displayed on the firmware upgrade screen.

Firmware Version


Current Firmware Version


v3.0.2

Last Upgrade ?

2018-09-18/14:54:09

Before upgrading, you may refer to the information and consider if a new firmware upgrading is necessary.

To upgrade the firmware please click on the  button to locate the ulmage-md5.xxx file, the file extension “xxx” should match your IPPBX model, otherwise the upgrade will fail.

After the file is located, click on  button to upgrade. For PBX-C301, the whole process will take 4 to 5 minutes, for PBX-C302 and PBX-C503, the whole process will take 2 to 3 minutes, when done please refresh the web page to re-login.

Notice

Firmware upgrade will cause the IPPBX system restart and as a result all the phone calls going through the system will be terminated. So please make sure there're no phone calls going on before you upgrade.

13.3 Diagnostic

13.3.1 PING

Path: **Maintenance -> Diagnostic -> 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.

Specify the domain or IP of the host you want to contact, then click on **Start** button, and then the command begins to process. You will receive results output from the system indicating the reachability of the destination.

Ping

IP Address/Domain Name

8.8.8.8

Start

Results

```

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=52 time=200 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=195 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=52 time=195 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=52 time=196 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 195.341/196.969/200.236/1.992 ms

```

13.3.2 Traceroute

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

Path: **Maintenance -> Diagnostic -> Traceroute**

In the IP Address/Domain Name field specify the IP or domain name that you want to lookup and click on **Start** button to begin tracing.

Traceroute

IP Address/Domain Name

8.8.8.8

Start

Results

```

0  * * * * *
1  221.183.19.41 (221.183.19.41) 1.824 ms 221.183.19.45 (221.183.19.45) 1.824 ms 221.183.19.45 (221.183.19.45) 1.824 ms
2  221.176.18.13 (221.176.18.13) 82.164 ms 221.176.20.137 (221.176.20.137) 82.164 ms 221.176.20.137 (221.176.20.137) 82.164 ms
3  221.176.22.106 (221.176.22.106) 43.240 ms 221.176.24.6 (221.176.24.6) 43.240 ms 221.176.24.6 (221.176.24.6) 43.240 ms
4  221.183.25.121 (221.183.25.121) 42.864 ms 221.176.19.242 (221.176.19.242) 42.864 ms 221.176.19.242 (221.176.19.242) 42.864 ms
5  221.183.55.81 (221.183.55.81) 44.436 ms 44.845 ms 221.183.55.53 (221.183.55.53) 44.436 ms 44.845 ms 221.183.55.53 (221.183.55.53) 44.436 ms 44.845 ms
6  223.120.13.165 (223.120.13.165) 200.596 ms 223.120.12.9 (223.120.12.9) 200.596 ms 223.120.12.9 (223.120.12.9) 200.596 ms
7  223.120.6.70 (223.120.6.70) 191.617 ms 193.600 ms 193.559 ms
8  72.14.217.10 (72.14.217.10) 189.590 ms 223.121.6.2 (223.121.6.2) 189.590 ms 223.121.6.2 (223.121.6.2) 189.590 ms
9  * * 108.170.247.161 (108.170.247.161) 196.599 ms
10 108.170.235.27 (108.170.235.27) 194.641 ms 198.379 ms 209.85.143.5 (209.85.143.5) 194.641 ms 198.379 ms 209.85.143.5 (209.85.143.5) 194.641 ms 198.379 ms
11 google-public-dns-a.google.com (8.8.8.8) 198.432 ms 197.168 ms 200.236 ms

```


During the whole process each step will output in the Results field, you can view which routes the packets have taken before reaching their final destination.

13.3.3 Ethernet Capture

Ethernet capture uses TCPDUMP which is a common packet analyzer allows users to capture TCP/IP and other packets being transmitted or received over a network to which the Vox IPPBX is attached. The captured packets can be downloaded from the IPPBX system and been analyzed on your Windows PC to display the SIP traffic details. It can be used to debug a VoIP call problem.

Path: **Maintenance -> Diagnostic -> Ethernet Capture**

To capture the network traffic, you need to select the network interface according to on which the IPPBX system is working on. Then click on **Start** button to start capturing the network traffic.



Once the process begins, the Start button will change to Stop. At this moment, you should make a call to recur the phone call problem or ensure some other problem had recurred, so the captured network traffic could content errors that are helpful for troubleshooting. Once done click on **Stop** button, and the captured network traffic will be automatically downloaded.

The downloaded file could be analyzed by Wireshark or you could send the file to support team for help.

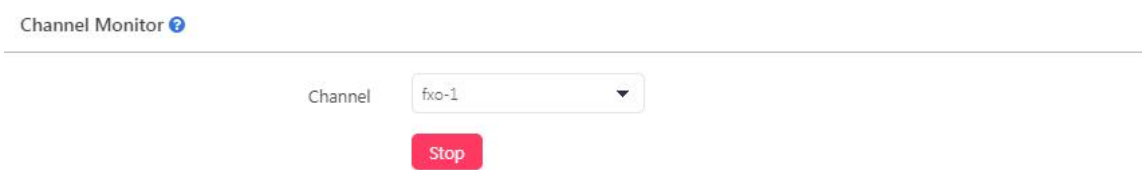
13.3.4 Channel Monitor

Channel Monitor, technically DAHDI Monitor allows you to monitor signal level on analog channel and record the output to a file. Recorded audio files are by default raw signed linear PCM. You can play it to the speaker to listen to the phone call signaling on the analog channel. Or you can use a sounds editor to visual display the audio level at both the Rx (audio Received by Asterisk) and Tx (audio Transmitted by Asterisk).

Usually Channel Monitor can be used to capture the caller ID signaling of an FXO channel. If you are experiencing caller ID problem you can perform channel monitor on the FXO port and then analyze the captured packets. If needed, you can send this file to support for help.

Path: **Maintenance -> Diagnostic -> Channel Monitor**

Before starting channel monitor, you need to select an FXO interface. Then click on **Start** button to capture signaling on the selected interface.

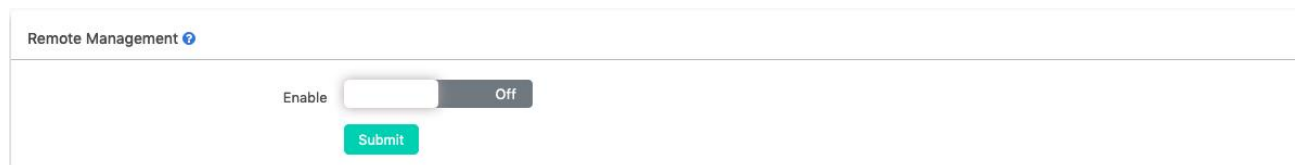


Once the process started the button will change to Stop. Now you should recur the problem by making a call in through the selected interface. When the extension started to ring the third time you may hangup and stop channel monitor by clicking on **Stop** button. As soon as the channel monitor stopped, the captured signaling will be automatically downloaded.

If you have knowledge of how to analyze the files you may open them with some sound editors like Wavepad, or you may send the file to support team for help.

13.3.5 Remote Management

Remote management can be turned on to support remote access your device when troubleshooting is needed. With remote management, remote access can be done without any third-party remote desktop tool.



Remote Management [?](#)

Enable ☐ Off

[Submit](#)

When remote troubleshooting is needed, users can enable remote management from **Maintenance** -> **Diagnostic** -> **Remote Management** page.

You don't have to worry about your system security, as no one can access your system when remote management is disabled, even if when it's enabled only authorized support engineers can access your system via our remote management platform. No one can access your system by any other means, if they don't have access to our remote management platform.

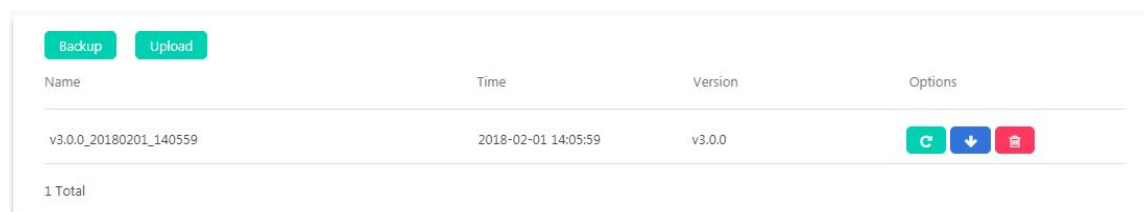
13.4 Backup

Taking a backup on IPPBX system is the same as when you create a recovery point on your Windows system. By restoring the backup you can recover the 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.

Path: **Maintenance** -> **Backup**

You may click on [Backup](#) button to take a backup of your system when necessary. A backup file will be generated.



Name	Time	Version	Options
v3.0.0_20180201_140559	2018-02-01 14:05:59	v3.0.0	C ↓ ✖

1 Total

File name is generated according to the software version, date and exact time when the backup is performed. You may click on [↓](#) button to download the backup to you operating system. Or click on [✖](#) button to delete it from the IPPBX system.

When you want to restore the backup, you may click on the [C](#) button. Restoring a backup will cause the system reboot, so please make sure there are no phone calls going on in the IPPBX system before you doing this.

If you are going to restore an offline backup (backup downloaded to your operating system) please click on the [Upload](#) button.

Notice

Backups will not be cleared after a system reset. So you may not need to download the backup to your operating system. And after a system reset, you may skip the quick setup wizard and go to the backup page to restore a backup directly to recover your previous configurations.

13.5 Reboot and Reset

13.5.1 Reboot

Path: **Maintenance** -> **Reboot and Reset**

By clicking on the [Reboot](#) button you may restart your IPPBX from the web UI. Restart the IPPBX system will terminate all active phone

calls, please make sure there're no phone calls going on before restarting the IPPBX system.

With v3.0.2 software, the time it takes to reboot each of the IPPBX model is listed below.

	PBX-C301	PBX-C302	PBX-C503
Phone call	2mins	1.5mins	1.5mins
Web UI	4mins	2mins	2mins

13.5.2 Reset


Path: **Maintenance -> Reboot and Reset**

To reset PBX-C301 please refer to below 3 reset methods (**Method 1**, **Method 2** and **Method 3**).

To reset PBX-C302 and PBX-C503 there's only 1 way, please refer to **Method 1**.

Method 1: Reset from web UI

Resetting the IPPBX system

Click on  button and confirm with the popup window, reset process will begin. During the reset process the IPPBX system will restart and the whole process will take around 4 to 5mins for PBX-C301, 2 to 3mins for PBX-C302 and PBX-C503.

Before resetting you may enable options "I'd like to keep the network profiles" and "I'd like to keep the call logs and recordings", so after resetting you may still access the IPPBX system web UI from the same IP with all your call logs and recordings remain untouched. If network profiles had been reset too, you'll need to access the IPPBX system via the default IP address.

WAN default IP: 192.168.1.100 / LAN Default IP: 192.168.10.100

After resetting when you access the web UI you'll first see the quick setup wizard. If you choose to use backup file to restore the system configurations, you may skip the quick setup wizard. If you wish to configure a fresh new phone system, you may follow the wizard to complete the configurations.

Notice

Reset from web UI will clear all system configurations, except if you have enabled "I'd like to keep the network profiles" and "I'd like to keep the call logs and recordings" options which will keep the network configurations and the call logs and call recordings.

By default backups will be kept, so after resetting from web UI you may restore backup directly from the IPPBX system.

Method 2: Reset by RST button at system running stage (PBX-C301 only)

When the PBX-C301 IPPBX system is running, the SYS LED indicator winks once every 2 seconds. Now you may press and hold the RST button on the back panel of the IPPBX for about 7 seconds, then the SYS LED will go off, the IPPBX system will reboot and start the reset process.

Reset PBX-C301 IPPBX this way is the same as resetting from the web UI. Only difference would be you cannot choose to keep the network profiles, call logs and recordings, and you will need to access the IPPBX system via the default IP.

Method 3: Reset by RST button at system booting stage (PBX-C301 only)

Reset the PBX-C301 IPPBX system by RST button at system booting stage will erase everything on the IPPBX system, including backups will be erased as well. Resetting this way will fully recover the IPPBX system to factory defaults.

So if you wish to restore the IPPBX configurations with a previous backup, please download it to you operating system first before resetting.

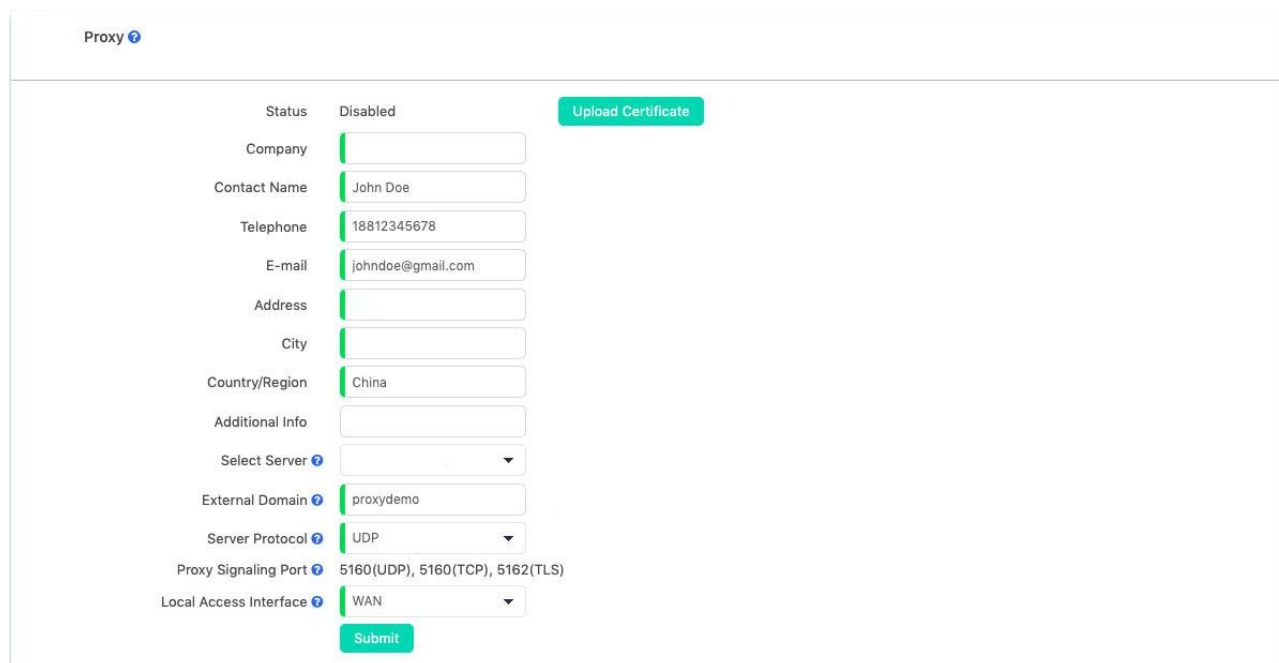
To reset the PBX-C301 IPPBX system at system booting stage, you need to first cut off the power supply. Press and hold the RST button then power it on. 4 to 5 seconds later when SYS LED goes on release the RST button.

Around 5mins later access the IPPBX system via the default IP address. You'll first be directed to the quick setup wizard page, you may start configuring a fresh new phone system or you may skip and upload offline backup to restore previous configurations.

14 Addons

14.1 Proxy

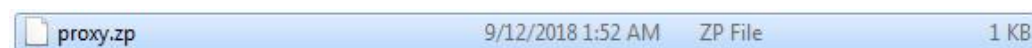
Proxy server is dedicated for NAT traversal of remote SIP registers. When enabled, you may register remote extensions directly without any other additional settings on the IPPBX or your router.



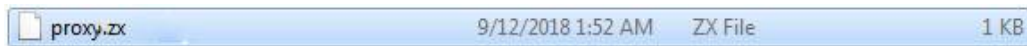
- You need to complete the form with your real contact info, we may have to contact you with the contact info you have provided, and the certificate will be sent to the email address given by you.
- In the **Select Server** field, please select a preferred country which we had deployed our proxy services. If the your country is not listed here please consult your sales team or support team for advice.
- In the **External Domain** field, you may define a customized prefix for the domain name you wish to be assigned to your IPPBX. Once the SIP proxy service is activated, the domain name can be used to register remote SIP extensions directly without any other additional settings.
- **Server Protocol** defines the signaling protocol that the IP PBX communicates with the SIP proxy server, it can be different than the protocol the SIP endpoints communicate with the IP PBX system.
- **Proxy Signaling Ports** listed the port number of protocols the SIP proxy server supports. SIP Proxy supports SIP over UDP, TCP and TLS transport protocols, so you may set the extensions on the IP PBX system to use one of these 3 protocols. As per the protocol chosen on the IP PBX system, the SIP endpoints need to use the same protocol and the corresponding given port number so remote register will work.
- In the **Local Access Interface** field, by default it uses WAN interface, modify it only when you use LAN to contact to your local network.

Once completed this form, please click on the “Submit” button to save these info and then click on the “Download Source File” button, please send the downloaded file to our distributor or our sales representative, we will issue the certificate for activating the proxy server within 3 work days.

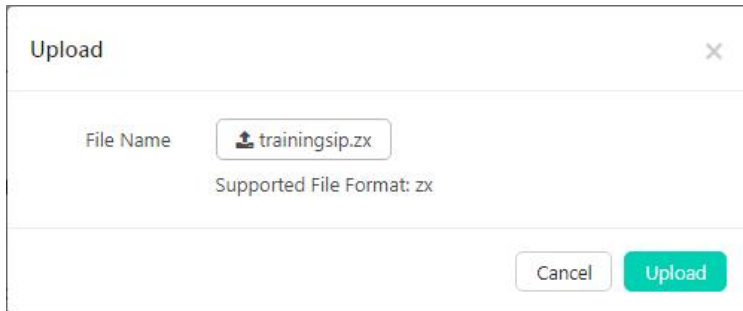
The downloaded source file is as shown below.



The certificate file issued by us is as shown below.



Please upload the certificate from the "Addons"->"Proxy Server" page by clicking on the "Upload Certificate" button.

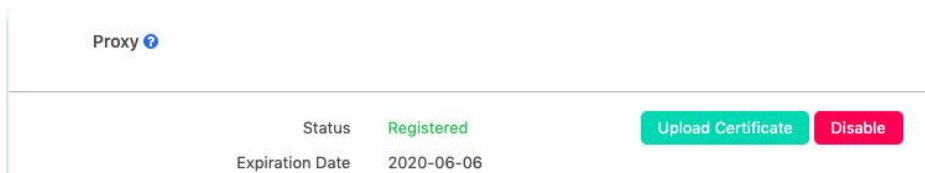


Upload

File Name

Supported File Format: zx

Once uploaded, the SIP proxy server will be activated. The activated SIP proxy service status and the license expiration is as shown below.



Proxy ?

Status	Registered	<input type="button" value="Upload Certificate"/>	<input type="button" value="Disable"/>
Expiration Date	2020-06-06		

By now, SIP proxy services should be working, and the external domain name could be used to register remote SIP extensions.



 <https://www.fs.com>



The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.