



v3.0

v3.0

[www.vitalpbx.org](http://www.vitalpbx.org)

# INDEX

<b>1. INTRODUCTION</b> .....	<b>6</b>
<b>2. INSTALLATION</b> .....	<b>7</b>
2.1.- INSTALLATION FROM THE ISO.....	7
2.2.- VPS INSTALLATION SCRIPT.....	16
2.3.- INSTALLATION THROUGH THE DIGITAL OCEAN MARKETPLACE.....	17
<b>3. INITIAL CONFIGURATIONS</b> .....	<b>19</b>
3.1.- CREATING EXTENSIONS.....	19
3.2.- TRUNKS, DIDs, AND OUTBOUND ROUTES.....	20
3.3.- SECURITY.....	21
<b>4. MENU OVERVIEW</b> .....	<b>23</b>
<b>5. CONFIGURATION CONSIDERATIONS</b> .....	<b>28</b>
5.1.- SECURITY.....	28
5.2.- NUMBERING SYSTEM.....	28
<b>6. PBX</b> .....	<b>29</b>
6.1 EXTENSIONS.....	29
6.1.1 Extensions.....	29
6.1.2 Hot Desking.....	42
6.1.3 Import Extensions.....	46
6.1.4 Export Extensions.....	47
6.1.5 Bulk Modification.....	47
6.1.6 Bulk Extensions.....	48
6.1.7 Extensions Status.....	51
6.2 APPLICATIONS.....	53
6.2.1 Conferences.....	53
6.2.2 Custom Applications.....	56
6.2.3 Custom Destinations.....	57
6.2.4 Custom Context.....	58
6.2.5 Feature Codes.....	58
6.2.6 Paging & Intercom.....	65
6.2.7 Pickup Groups.....	69
6.2.8 Parking.....	70
6.2.9 Speed Dialing.....	71
6.2.10 Import/Export Speed Dialing.....	72
6.2.11 Voicemail Broadcast Group.....	72
6.2.12 Call Back.....	73
6.2.13 DISA.....	75
6.2.14 PIN List.....	76
6.2.15 Dynamic Destinations.....	77
6.3 CLASS OF SERVICE.....	79
6.3.1 Class of Service.....	79
6.3.2 Feature Categories.....	80
6.3.3 Dialing Restriction Rules.....	81
6.3.4 Customer Codes.....	82
6.3.5 Authorization Codes.....	83
6.3.6 Route Selections.....	84
6.4 CALL CENTER.....	85
6.4.1 Ring Groups.....	85
6.4.2 Queues.....	86

6.4.3 Queues Priorities.....	93
6.4.4 Queues VIPs.....	94
6.4.5 Queues Callback.....	95
6.5 EXTERNAL.....	98
6.5.1 Trunks.....	98
6.5.2 Outbound Routes.....	106
6.5.3 Inbound Routes (DID).....	109
6.5.4 Dynamic Routing (Auto CLIP Routes).....	111
6.6 INCOMING CALLS.....	112
6.6.1 IVR.....	112
6.6.2 Time Groups.....	115
6.6.3 Time Conditions.....	116
6.6.3 Announcements.....	117
6.6.4 Languages.....	118
6.6.5 Night Mode.....	119
6.6.6 CID Modifiers.....	120
6.6.7 CID Lookup.....	121
6.7 TOOLS.....	122
6.7.1 Asterisk CLI.....	122
6.7.2 Blacklist.....	123
6.7.3 Dashboard.....	124
6.7.4 Log File Viewer.....	125
6.7.5 Cron Profiles.....	126
6.7.6 Weak Passwords.....	127
6.7.7 Phone Books.....	128
6.7.8 Task Manager.....	130
6.8 EXTRAS.....	131
6.8.1 Video Conference.....	131
6.9 Emergency Calls.....	132
6.9.1 Emergency Numbers.....	132
6.9.2 Dispatchable Locations.....	133
6.10 PASS-THROUGH.....	134
6.10.1 PT Trunks.....	134
6.10.2 PT Extensions.....	134
6.11 END POINT MANAGER.....	136
6.11.1 Host Settings.....	136
6.11.2 Creating Template.....	138
6.11.3 Device Buttons.....	139
6.11.4 Expansion Modules.....	140
6.11.5 Advanced Settings.....	140
6.11.6 Device Mapping.....	141
6.12 COMMUNICATOR.....	143
6.12.1 Softkey Profiles.....	143
6.12.2 Pause Profiles.....	145
6.12.3 Campaigns Result Profiles.....	146
6.12.4 Campaigns.....	147
6.13 VIRTUAL FAXES.....	148
6.13.1 Fax Devices.....	148
6.13.2 Global Fax Settings.....	149
6.13.3 Fax Sending.....	149
6.13.4 Fax Viewer.....	150
<b>7. REPORTS.....</b>	<b>151</b>
7.1 CDR REPORTS.....	151
7.1.1 CDR Filters.....	151
7.1.2 View CDR Reports.....	152

7.2 PBX REPORTS.....	153
7.2.1 Active Calls .....	153
7.2.2 PJSIP Devices.....	154
7.2.3 SIP Devices .....	154
7.2.4 IAX2 Devices .....	155
7.3 IVR STATS.....	157
7.3.1 IVR Stats.....	157
7.4 CALL CENTER REPORTS.....	158
7.4.1 Queues Call Back Reports .....	158
<b>8. SETTINGS.....</b>	<b>159</b>
8.1 TECHNOLOGY SETTINGS.....	159
8.1.1 PJSIP Settings .....	159
8.1.2 SIP Settings.....	160
8.1.3 IAX2 Settings.....	168
Codecs.....	170
8.1.4 Device Profiles .....	172
8.1.5 Telephony Settings .....	177
8.1.6 Dial Profiles.....	178
8.2 VOICEMAIL SETTINGS.....	180
8.2.1 Voicemail Settings .....	180
8.2.2 Voicemail Time Zones.....	182
8.3 PBX SETTINGS .....	183
8.3.1 System General.....	183
8.3.2 Asterisk Manager Users.....	186
8.3.3 Log File.....	187
8.3.4 RTP Settings.....	188
8.3.5 CEL Settings.....	189
8.3.6 Mini HTTP Server .....	190
8.4 VOICE PROMPTS.....	191
8.4.1 Asterisk Sounds.....	191
8.4.2 Music on Hold .....	192
8.4.3 Recording Managements .....	193
8.5 TELEPHONY.....	194
8.5.1 Interface.....	194
8.5.2 Clock Sources.....	195
8.5.3 Channel Group.....	195
8.5.4 Profile Assignments.....	196
<b>9. ADMIN .....</b>	<b>197</b>
9.1 ADMIN.....	197
9.1.1 Users.....	197
9.1.2 Users Profiles.....	199
9.1.3 Application Keys.....	200
9.1.4 Tenants.....	201
9.2. SYSTEM SETTINGS.....	205
9.2.1 System Miscellaneous.....	205
9.2.2 Email Settings.....	207
9.2.3 Email Templates.....	208
9.2.4 Certificates.....	209
9.2.5 HTTP Server.....	210
9.3 FIREWALL.....	211
9.3.1 Settings.....	211
9.3.2 Firewall Services.....	213
9.3.3 Firewall Rules.....	216
9.4 NETWORK.....	217

9.4.1 Network Settings .....	217
9.4.2 DHCP Settings.....	219
9.4.3 OpenVPN Server.....	221
9.4.4 OpenVPN Client.....	233
9.4.5 GEO Firewall .....	234
9.5 ADD-ONS .....	235
9.5.1 Add-ons .....	235
9.6 TOOLS .....	238
9.6.1 Backup & Restore .....	238
9.6.2 Maintenance.....	239
9.6.3 Branding.....	240
<b>10. APPENDIX .....</b>	<b>243</b>
10.1 VITALPBX HIGH AVAILABILITY .....	243
10.2 FEATURE CODES.....	248
10.3 BLF (HINTS).....	256
10.3.1 Grandstream Phone Management .....	258
10.3.2 Yealink Management .....	259
10.3.3 Xorcom Management .....	259
10.4 VitalPBX Voice Prompts .....	260
10.5 RECOMMENDATIONS.....	267
10.6 ADDITIONAL MODULES.....	268
10.6.1 Domotic Module.....	268
10.6.2 Sonata Suite (Recording Management).....	274
10.6.3 Sonata Suite (Billing System).....	275
10.6.4 Sonata Suite (Switchboard).....	276
10.6.5 Sonata Suite (Stats).....	277
10.7 COMMAND TOOL.....	280
10.8 CREDITS.....	280
10.8.1 Sources of Information.....	280

# 1. Introduction

VitalPBX is a Graphic User Interface highly responsive that eases the management of Asterisk Servers in a quick, intuitive, and safe way.

VitalPBX provides an intuitive 3-level menu that makes it easy to locate the module you wish to configure.

Some of the usage features from VitalPBX which you must know about are:

- 1) You can use VitalPBX from any device and any web browser. VitalPBX adapts in a transparent way to every device, be it a smartphone, tablet, PC, Mac, or Linux.
- 2) On the top of every screen you will find a spyglass icon (🔍). When you click on it, you can perform a global search throughout the whole system. Which lets you easily search for extensions, call queues, conferences, DISA, trunks, modules, and much more.
- 3) When navigating through the different modules, you may notice that most of them got a list icon (☰) on the top right-hand corner. When you click on this icon, it will show you the list of all the objects that have been created in that module. On the top part of the list, you will also see a spyglass (🔍) that you can use as a filter. Write down any part of the name of the object that you are looking for, and you will see all of the objects that coincide with your filter.
- 4) VitalPBX has been designed so that all of the information is in one screen always, without the need to scroll down and lose track of the rest of the configurations. This is why you will see that most of the modules are divided in various tabs that will allow you to see all of the information for current object.
- 5) VitalPBX has a Multi-Tab system, which means that you can move to any module you have worked on, from any module. This allows you to work on any module without having to close the prior module you've been working on. There is no need to save all changes when moving between tabs, meaning that you can work on multiple tabs at the same time. For example, if you are creating a Ring Group and need to verify the extensions, you can quickly go to the extensions module and come back to the Ring Group module to finish up.
- 6) The Save and Delete buttons will always be visible on the lower right-hand corner of the screen, no matter the size of the screen you are using.
- 7) You can get more screen real estate by hiding the navigation menu on the left. You can do this by clicking on the (☰) icon on the top left-hand corner of the screen.
- 8) All of the fields have a tooltip available if you hover your mouse over their name. In the case of mobile devices, you will have to tap on the text to access the tooltip.
- 9) Obligatory fields are indicated by an asterisk next to the field name. For example, Name\* indicates that the 'Name' field is obligatory.

## 2. Installation

Coming up, we will explain step by step the installation process for VitalPBX. It is important to notice that there are three (3) ways you can install.

**From the ISO (DVD, Flash Drive, Virtual Machine)**, this method is used usually when we want to install on Hardware or a local Virtual Machine. This process will install Linux CentOS 7.x along with VitalPBX and all of its dependencies. You can download the ISO from the downloads section on our website <https://vitalpbx.org>.

**From the VPS Installation Script**, this is a process usually used when installing on the cloud with a VPS Service Provider. It is also used in the case that you already have installed a Linux CentOS 7.x on your server. For an updated step by step guide on how to use this script, you can find it on the downloads section of our website <https://vitalpbx.org>.

**VPS Provider Marketplace**, we constantly have VitalPBX updated on the Digital Ocean Marketplace, and you can also find us on the SYSTM marketplace ready to install. You can use the following link to learn on how to get US\$100.00 for a 2-month trial of the Digital Ocean Services and use VitalPBX on their systems. <https://vitalpbx.org/en/vitalpbx-cloud-pbx-digital-ocean/>. Similarly, you can contact us at [sales@vitalpbx.org](mailto:sales@vitalpbx.org) on how to get a trial period with SYSTM.

On this manual we will cover the first two methods of installing VitalPBX.

### 2.1.- Installation from the ISO

To install from the ISO, we will need to download the latest version of VitalPBX, by going to our website <https://vitalpbx.org> and then going to the downloads section. There, we proceed to click on download and get the ISO. The ISO's file size is approximately 1.2GB.

Once we have the ISO downloaded, we can proceed in one of three (3) ways:

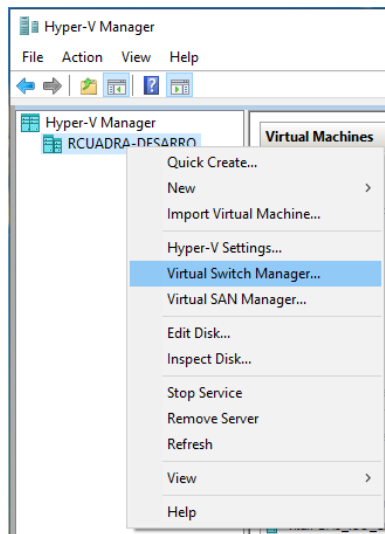
**Burn the ISO on a DVD**, for this we can use a burning program like Nero Burning  
**Flash the image on a USB Flash Drive.** For this process we recommend the use of the Balena Etcher software (<https://www.balena.io/etcher/>).

**Use the ISO directly**, in the case we are installing on a Virtual Machine, for example Hyper-V.

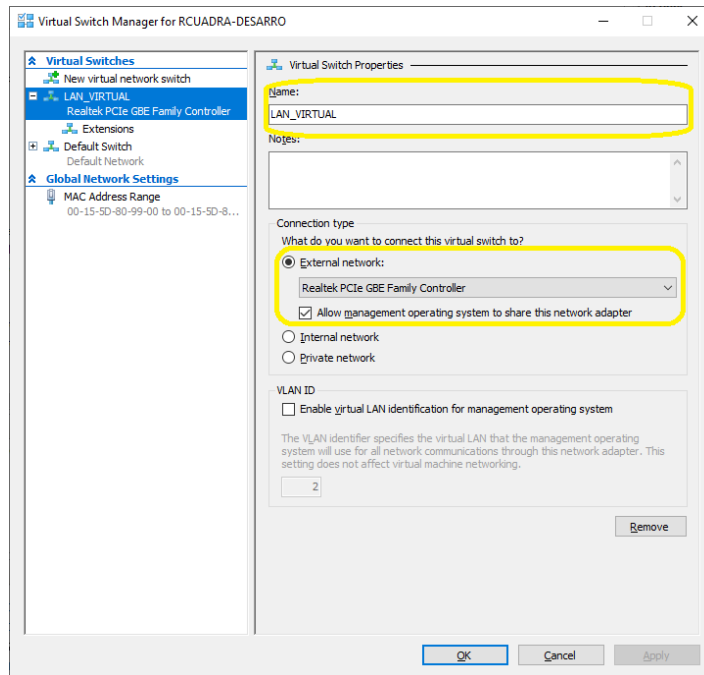
Now, we will proceed to install from the ISO. For the example on this manual, we are going to be using Hyper-V as the virtualization program. You can use any other virtualization program such as VMWare or Oracle VM VirtualBox.

We now start up Hyper-V, which would already be installed. If it is not installed, you can install it from Control Panel > Program and Features > Turn Windows features on or off and select Hyper-V. You must have the Pro Version of Windows to access this tool.

If it is the first time you are installing Hyper-V, you must create a virtual network interface, so your machine gets an IP address assigned from the DHCP on your network. When you start up Hyper-V, go to Hyper-V Manager and right click on the item shown below, and select Virtual Switch Manager from the menu.

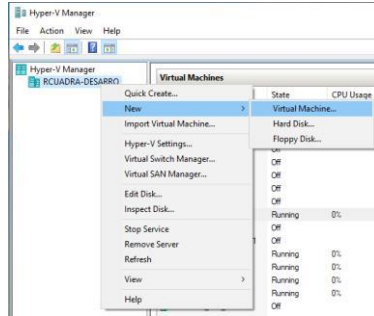


Now, we will see the following dialog so we can give our interface a name and associate it with a physical interface. We will use this interface when we are creating our virtual machine.

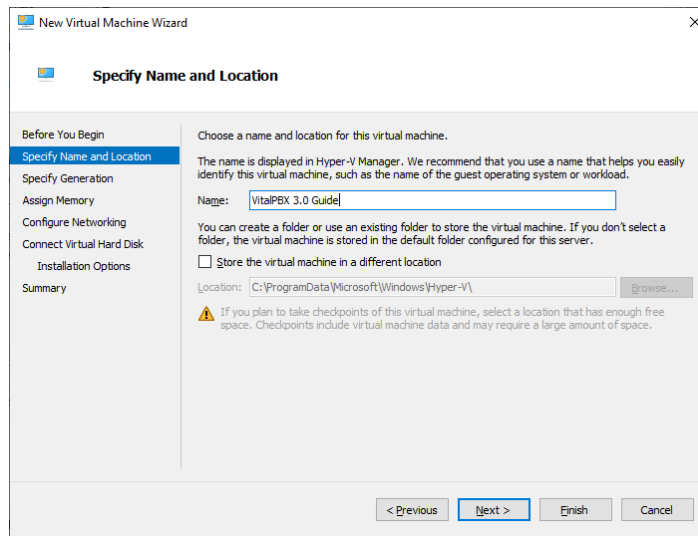




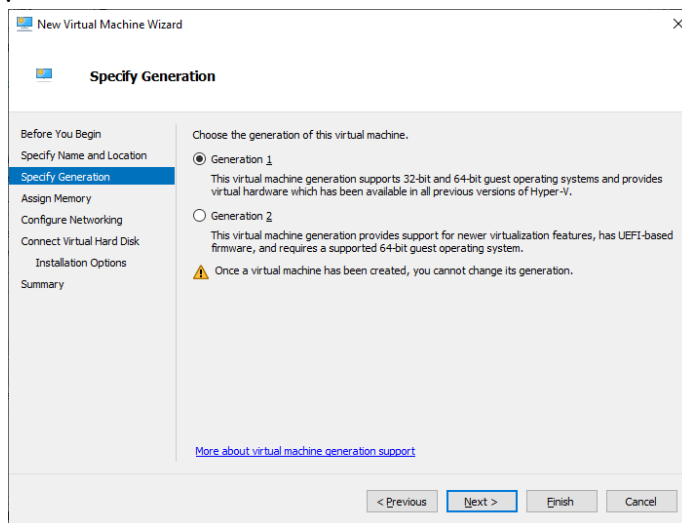
Next, we will create the new Virtual Machine to install VitalPBX on. So, we select from the menu, New > Virtual Machine.



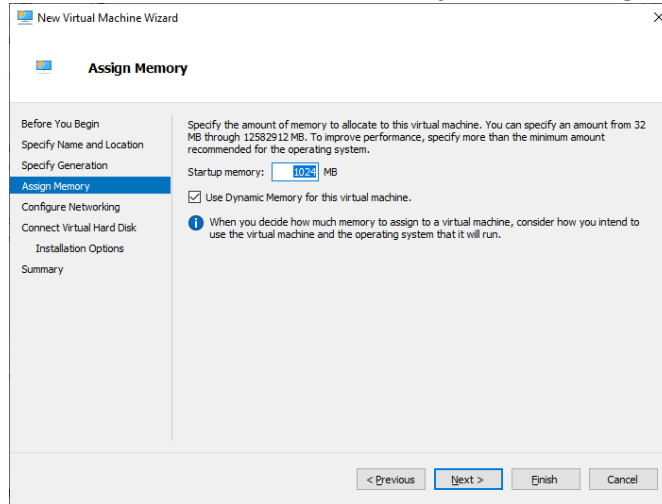
We give our Virtual Machine a name.



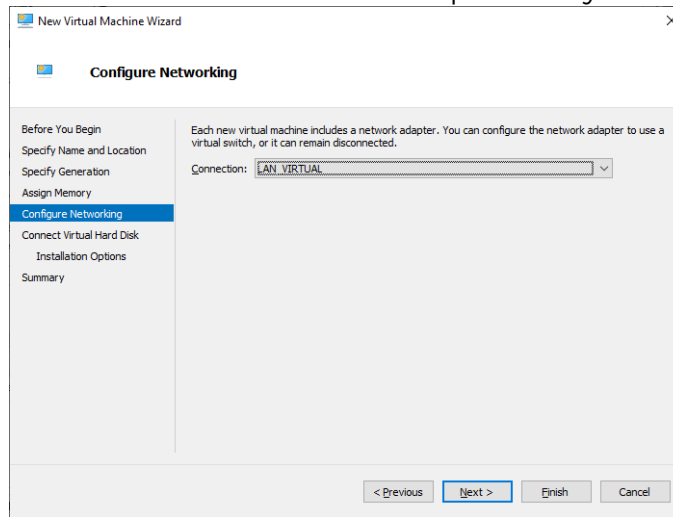
We then select Generation 1 for the generation type for the Virtual Machine. This is specific to Hyper-V.



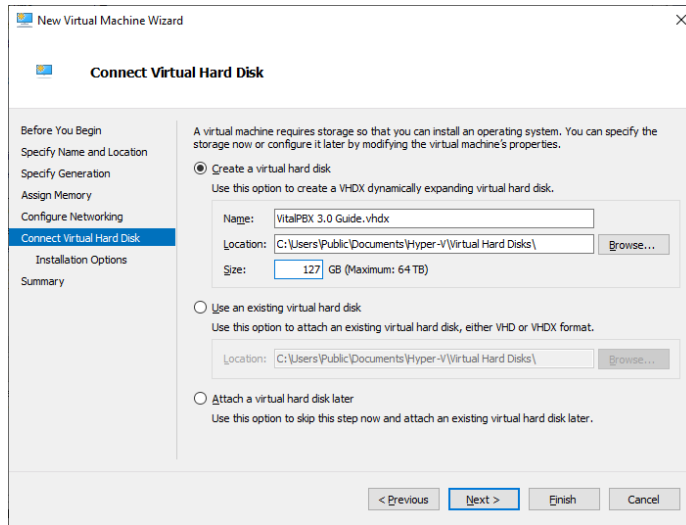
Afterwards, we specify the Memory Size that we will assign to this machine. For this example, we will be leaving this in 1GB, and we select the option “Use Dynamic Memory for this virtual machine”. This means that the minimum amount of memory will be 1GB, and if we need more additional memory will be assigned.



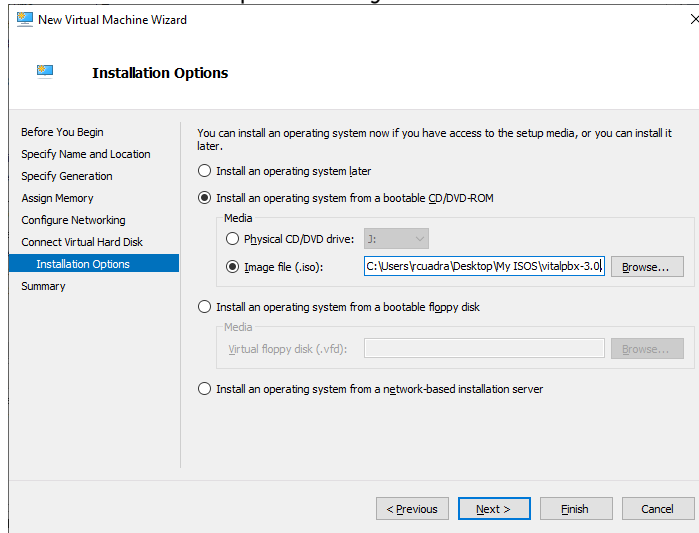
Now, we Select the virtual interface we created previously.



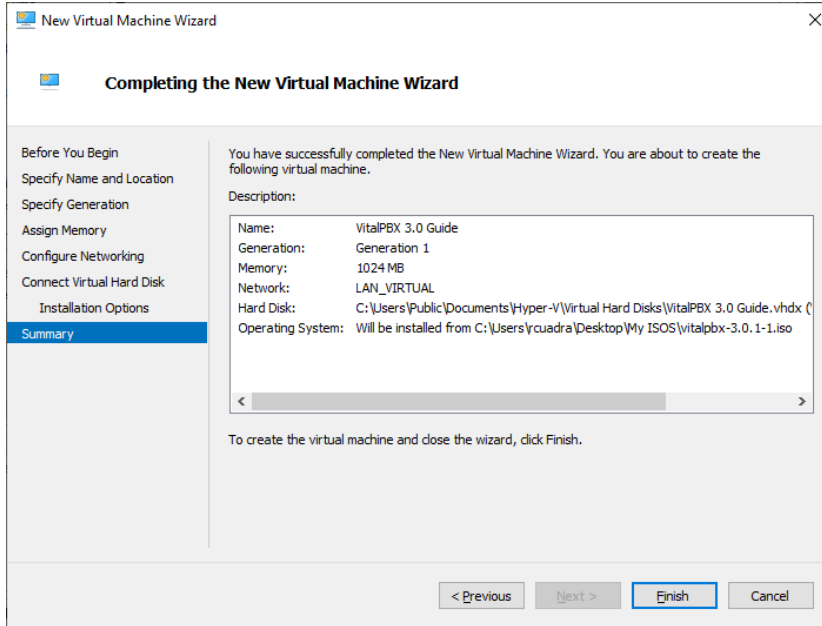
Then, we are asked for the storage size to assign to our machine. We can leave this in 127GB, which is dynamically allocated as well. Meaning that it will use real disk space as it gets filled up, not immediately.



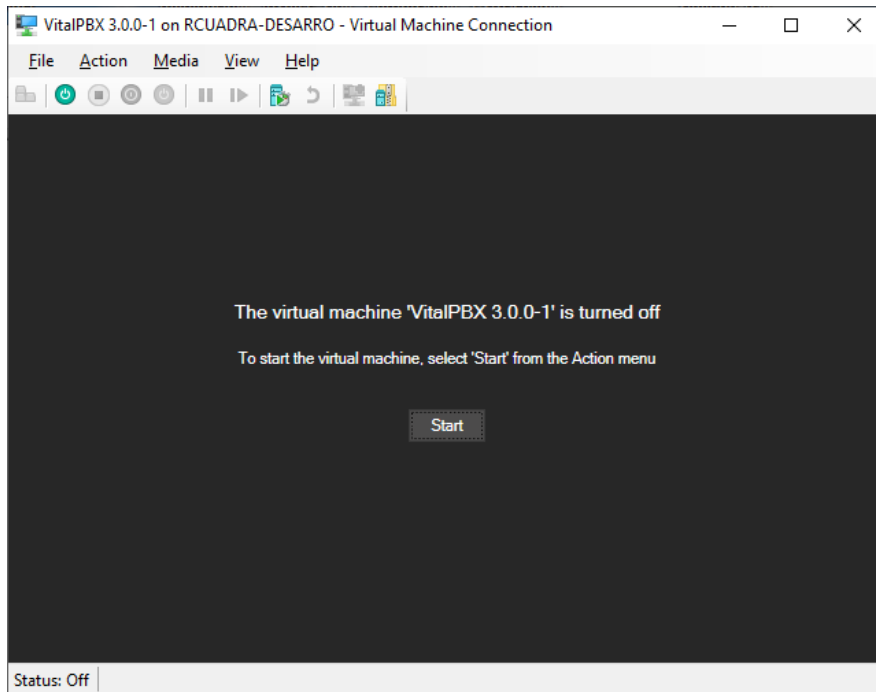
Now, we select the ISO we have previously downloaded.



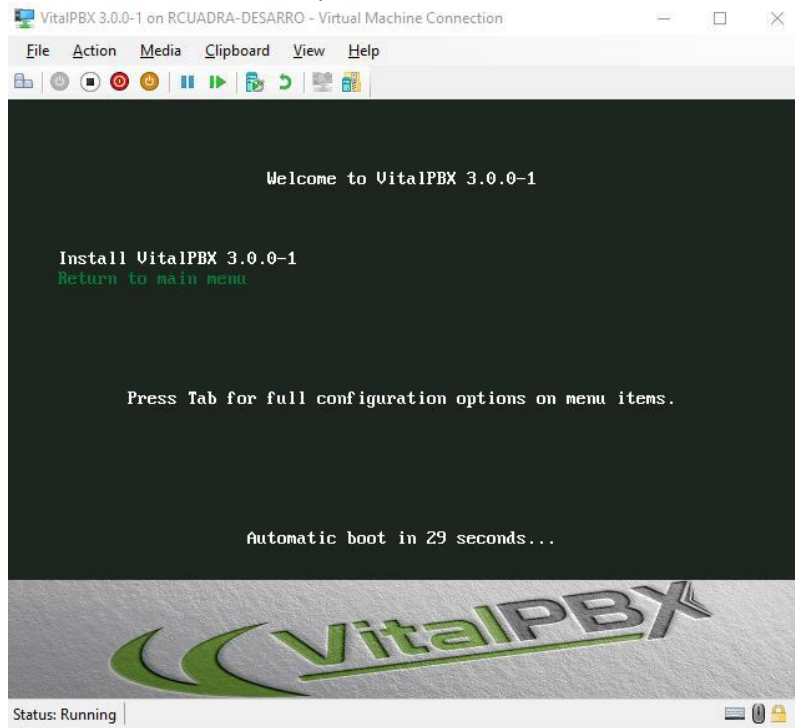
Finally, we can see a summary for our new machine, and we are going to click on Finish. Once this process is done, we can go back to the main panel and double click on our new machine to start it.



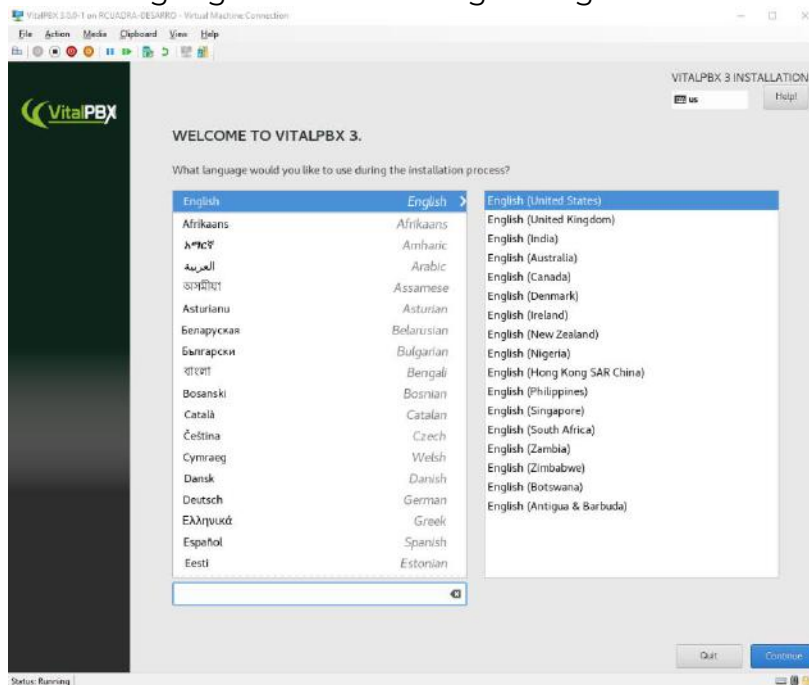
From here, we press Start, and moving on the following installation will be similar to installing a CentOS machine.



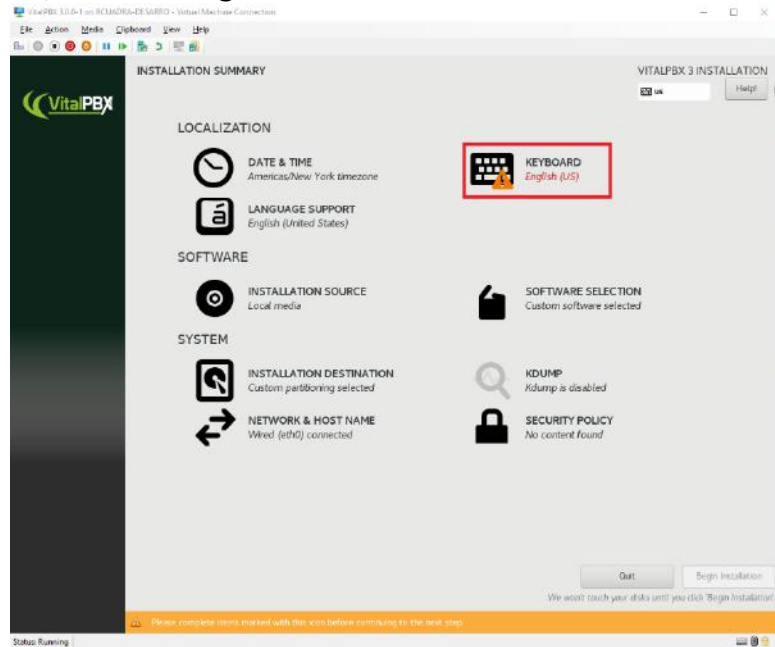
Select “Install VitalPBX 3.0.1-1” and press ‘Enter.’



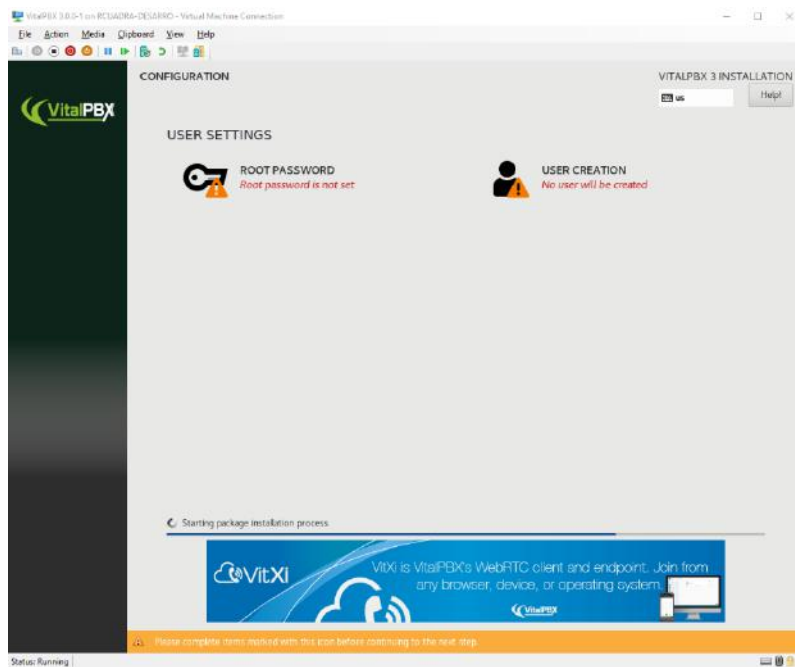
Next, we select the language we will be using during the installation.



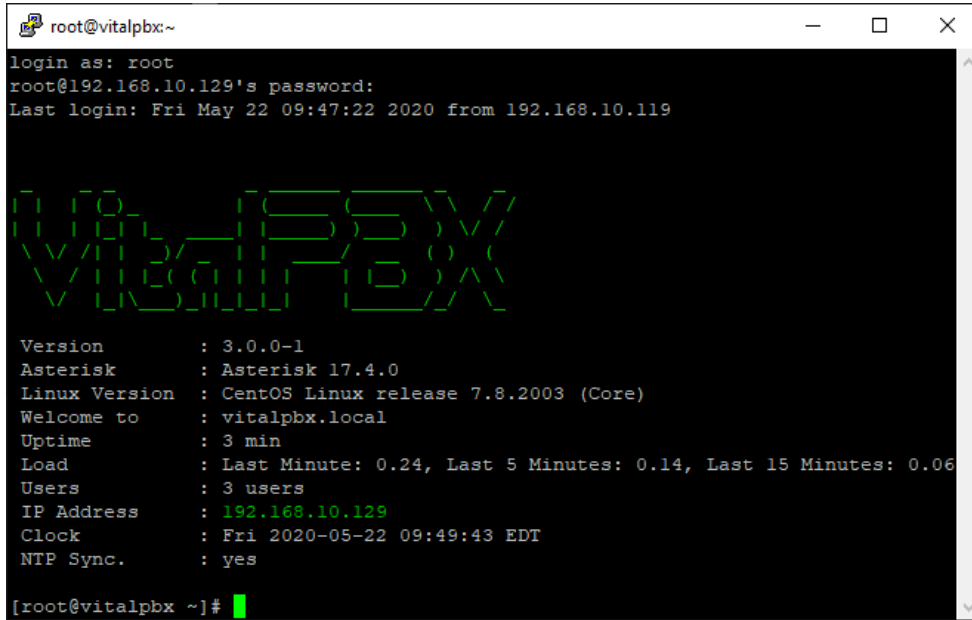
Afterwards, we will see various pre-selected options. Here, you can make any customizations if you want, for example, change the partitioning for the Storage Media (By Default, VitalPBX will use the Storage's Full Size.) Or if you like, you leave everything by default. The only mandatory option to select is the keyboard language. Once this is selected, we can 'Begin Installation.'



On the next screen, we will need to configure a password for the root user. There is no need to create additional users from here.

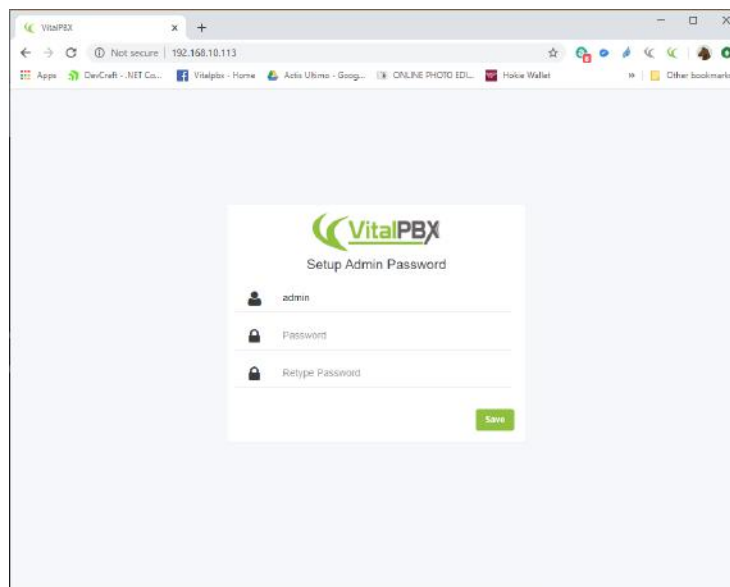


After a couple of minutes, depending on the server's hardware specifications, the machine will finish installing and will reboot. When this is done, for any further CLI usage we can move from the console screen to connecting via SSH using a terminal application like PuTTY for Windows, and Terminal or Termius for the Mac. You just need to enter the IP Address that is shown to you on your screen. You will Log In using the user root, and the password you set up during installation.

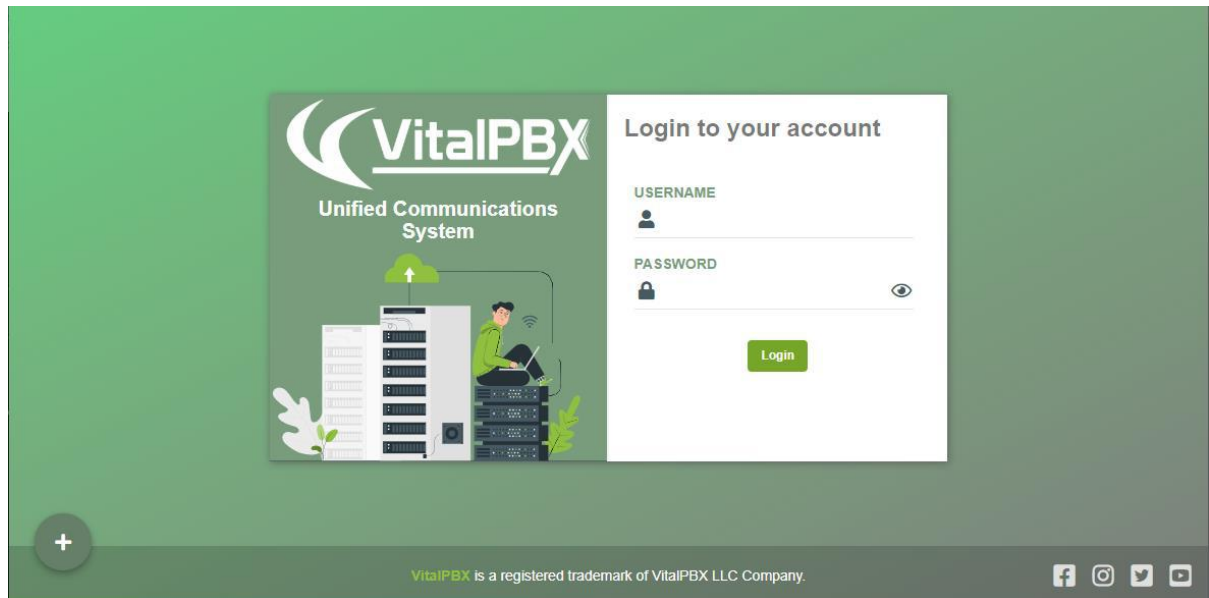


```
root@vitalpbx:~  
login as: root  
root@192.168.10.129's password:  
Last login: Fri May 22 09:47:22 2020 from 192.168.10.119  
  
VitalPBX  
  
Version      : 3.0.0-1  
Asterisk    : Asterisk 17.4.0  
Linux Version : CentOS Linux release 7.8.2003 (Core)  
Welcome to   : vitalpbx.local  
Uptime      : 3 min  
Load        : Last Minute: 0.24, Last 5 Minutes: 0.14, Last 15 Minutes: 0.06  
Users       : 3 users  
IP Address   : 192.168.10.129  
Clock       : Fri 2020-05-22 09:49:43 EDT  
NTP Sync.   : yes  
[root@vitalpbx ~]#
```

Then, you can enter the IP Address on your browser, and you will access the VitalPBX Web Interface. The first step you will be asked is to enter the admin password. This password can be different to the root user password you set up earlier.



Any other time you go to the IP Address, you will be able to log in using the user admin, and the password you set up on the previous step.



## 2.2.- VPS Installation Script

Now, we are going to install VitalPBX from the VPS installation script. To use this method, it is necessary that you have previously installed a CentOS 7.x minimal machine. This we can download from the CentOS website or install directly from a VPS Service Provider. In this case we are using a VPS service on the cloud.

Once we have our Linux CentOS 7.x installed, we will connect via SSH to our machine to access the CLI. And then, log in using the user root and the password or SSH Key provided from your CentOS 7.x installation.

We install 'wget' so we can download the script:

```
[root@guest ~]# yum install wget -y
```

Next, we will download the script and give it execution permissions, and finally, we run the script.

```
[root@guest ~]# wget https://raw.githubusercontent.com/VitalPBX/VPS/master/vps.sh
[root@guest ~]# chmod +x vps.sh
[root@guest ~]# ./vps.sh
```

Now, we wait a couple of minutes, so the installation script finishes. And once it is done, the machine will automatically reboot. Once it has rebooted, you can go to its IP Address from your browser, enter the admin password which can be different to the root password. And just like that you will then access the VitalPBX Web UI.



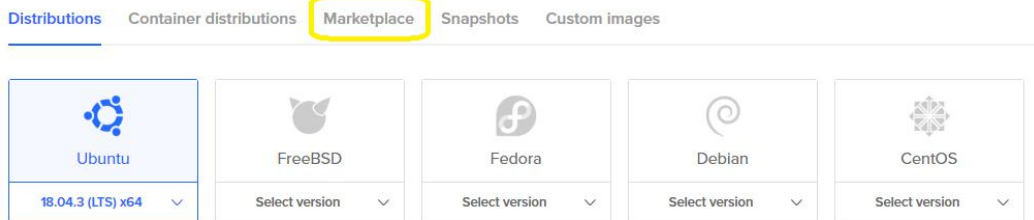
## 2.3.- Installation through the Digital Ocean marketplace.

This is one of the fastest ways to install VitalPBX on the Cloud. If you would like to get a US\$ 100.00 credit, which you can use for two months in Digital Ocean, you can use the following link: <https://m.do.co/c/550374a08708>.

Once you have registered, we can proceed to create a new Droplet, and we select 'Marketplace'.

### Create Droplets

Choose an image ?



On the search, type 'VitalPBX.'

### Create Droplets

Choose an image ?



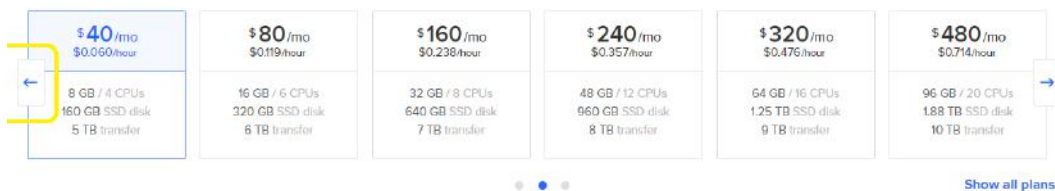
Select the Standard Plan and choose your Droplet's capacity. Here it is important to notice that Digital Ocean shows options from US\$ 40.00. If you want to see cheaper options, press the arrow to the left.

Choose a plan

[Help me choose](#)



Standard virtual machines with a mix of memory and compute resources. Best for small projects that can handle variable levels of CPU performance, like blogs, web apps and dev/test environments.

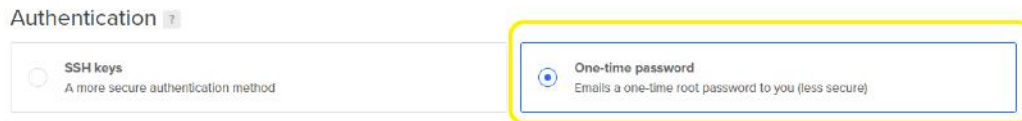


Then, you can select the Droplet location that is the most convenient to you.

Choose a datacenter region



The next step is very important. If you do not know how to create SSH keys, so you can log into your droplet, you can choose to create a password. With this option you can enter your desired root password.



Then, optionally, you can change the hostname for your droplet.

Finalize and create

How many Droplets?

Deploy multiple Droplets with the same configuration.

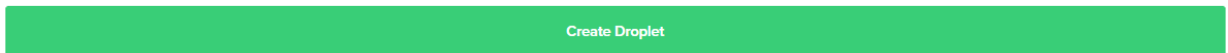
1 Droplet

Choose a hostname

Give your Droplets an identifying name you will remember them by. Your Droplet name can only contain alphanumeric characters, dashes, and periods.

vitalpbx-centos-s-1vcpu-1gb-sfo2-01

To finish up, we can click on the “Create Droplet” button.



We now wait for a couple of minutes to finish the installation, and once it is done, you can enter to the machine’s IP Address on your browser to setup the admin password. Once that is done, you can enter to VitalPBX’s Web Interface.

## 3. Initial Configurations

Up next, we will explain the steps you can take to have a basic VitalPBX with some extensions, trunks, and some security measures. For any further explanation of each field and option, the rest of the manual will cover them thoroughly.

### 3.1.- Creating Extensions

To create an extension, you can go to PBX > Extensions > Extensions, and the most important fields are:

**Extension**, the extension number.

**Name**, name of the user associated to this extension.

**User Device**, even though this is filled automatically, you can customize this field and remember it as this is the user, we will use to register our devices.

**Password**, this field is auto generated, but you can customize it to anything you like. This will be the password used for the device registration.

Always remember that after you create an object, save and afterwards 'Apply Changes' by pressing the red arrows button.



Knowing this, you can create a couple of extensions and we can connect them with any hardware device or softphone, using the following information:

**SIP Server**, the IP address for our VitalPBX.

**Username**, this is the User Device.

**Password**, the password created on the extension's device.

Once you have the two phones registered you would be able to call between them. Here are a couple of things you can troubleshoot if this is not the case.

**The phones are not registering.** Verify that the registration port 5060 is enabled on your firewall and that you have entered the correct information.

**There is no audio.** In this case, it is possible that your server is behind NAT, for which we recommend you find out the Public IP address for your server and if available the Local IP address. With this information, we can go to Settings > Technology Settings > SIP > Networking, and on the NAT section, enter your External address, and on Local Network enter your IP Address. Also, set the NAT option to Force, Comedia. Save and Apply Changes.

NAT

NAT: Force, Comedia

External Address: 186.125.35.45

External Host: [Empty]

External Refresh: [Empty]

Local Networks

IP Address: 10.10.0.5

Network Mask: 16

Add

## 3.2.- Trunks, DIDs, and Outbound Routes

So, we can communicate with the outside world, it is necessary to connect VitalPBX with any VoIP trunk provider. There are various providers out there, but we will explain the basic concepts on this example.

**Technology**, we recommend creating a PJSIP trunk. Almost all serious VoIP providers have this technology type. Though the popular one would be SIP Trunks.

**Description**, a brief description to identify the trunk.

**Class of Service**, here we select "Trunk Default".

**Local Username**, the username to identify this trunk.

**Host**, IP address or hostname for the VoIP Provider.

**Remote Username**, username provided/used by the VoIP provider to connect with them.

**Remote Secret**, password used to connect with the VoIP provider.

**Contacts**, in the case the VoIP provider is providing a PJSIP trunk, here we add the contacts or hosts that they provide. There can be more than one.

**From Domain**, the domain used on the FROM header.

**Qualify**, we set this to yes to keep the connection alive.

**Contacts**, this is a list of IP Addresses or hostnames separated by comma. The IP Addresses can use a subnet mask. The subnet mask can be written in CIDR or Octets separated by period. Separate the IP Address from the netmask with a forward slash **"/"**.

We got various articles that go into detail on how to connect with various providers:

- <https://vitalpbx.org/en/twilio-elastic-sip-trunking/>
- <https://vitalpbx.org/en/idt-express-sip-trunking-on-vitalpbx/>
- <https://vitalpbx.org/en/skytel-sip-trunk-with-vitalpbx/>
- <https://vitalpbx.org/en/voip-ms-sip-trunk-on-vitalpbx/>
- <https://vitalpbx.org/en/telnyx-sip-trunk-with-vitalpbx/>

Once we have the trunk connected to our PBX, we can configure our DID so we can receive calls through the trunk we just created. To configure this, we would need to know the DID that we purchased from the Provider, and the format they send it to our VitalPBX. (For example, 13055605776)

We will now go to PBX > External > Inbound Routes:

**Description**, a brief description to identify the inbound route.

**DID**, here we input the DID we have purchased from the VoIP Provider.

**Destination**, here we can select the destination where we will direct the call to.

Now, we will configure the way we can place outgoing calls from our VitalPBX. To do this, we go to PBX > External > Outbound Routes, and we configure the following:

**Description**, a brief description to identify the outbound route.

**Trunk**, we select the Trunk we wish to use to call outbound. In this case we select the trunk previously created.

**Prefix**, here we can enter a prefix to select this outbound route whenever we place a call. This prefix will be dropped from the phone number when a call is placed.

**Pattern**, here we configure the pattern for the numbers we wish to dial. There are a set of variables you can use, and you can see them by hovering over the word 'Pattern'. If you want to use a ten-digit phone number, you can easily enter ten X's, for example XXXXXXXXXX.

### 3.3.- Security

It is necessary that we make sure that our VitalPBX is secure against any possible external attack, for which we make the following recommendations:

Use complex passwords for the extensions you create. (We recommend the auto-generated ones.)

Use complex passwords for the root and admin users.

If you are using a firewall to forward the ports towards your PBX the needed ports are the following:

- **SIP**, ports 5062-5063 UDP/TCP (If you are not going to use the SIP protocol, then there is no need to forward it.)
- **PJSIP**, ports 5060-5061 UDP/TCP If you are not going to use the PJSIP protocol, then there is no need to forward it.)
- **IAX2**, ports 4569 UDP (If you are not going to use the IAX2 protocol, then there is no need to forward it.))
- **RTP**, ports 10000-20000 UDP
- **SSH**, port 22 (This is not necessary if you are not doing remote configurations, so there is no need to publish it.)
- **HTTP**, port 80 TCP (If you don't need to access the Web UI remotely, there is no need to publish it.)
- **HTTPS**, port 443 TCP, this is only needed if you have a valid certificate on your PBX. (If you don't need to access the Web UI remotely, there is no need to publish it.)
- **Asterisk HTTP Daemon**, ports 8088-8089 UDP/TCP, Only necessary if you are using WebRTC. (If you are not using WebRTC, there is no need to publish it.)
- **VitXi**, ports 6001-6003 TCP, these are necessary for VitXi to work properly. (If you are not using VitXi, there is no need to publish it.)
- **OpenVPN**, port 1194 UDP, if you are using the OpenVPN Server add-on, you will need to forward this port. For better security, you can close every other port on your firewall and only forward this port. You can use the OpenVPN certificates generated by this add-on to access

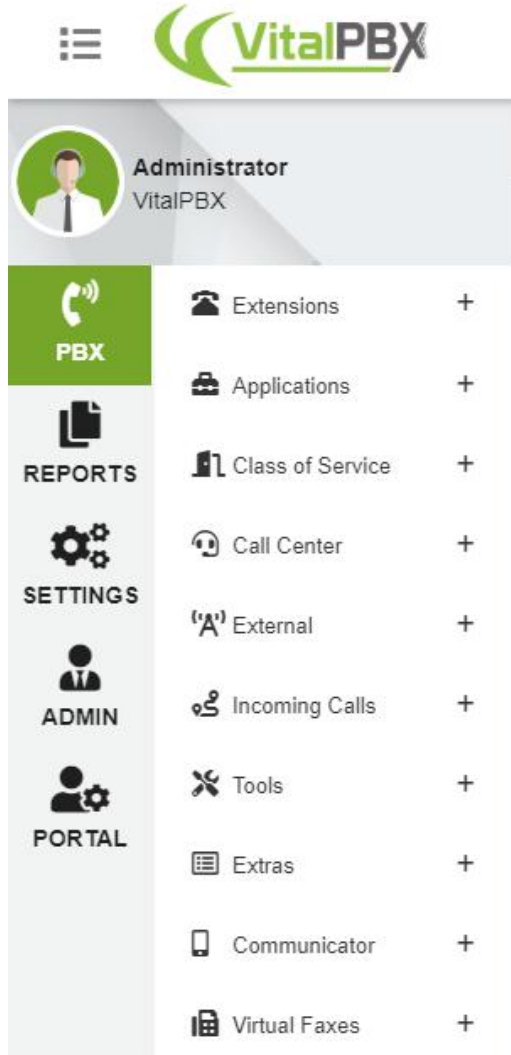
the PBX directly, and many phones nowadays have OpenVPN capabilities.

We recommend the use of the Geo Firewall add-on, which will allow you to limit the access to your PBX in the case it is published. This will prevent people from specific countries to access your PBX.

To increment the security, you can block ICMP requests by going to Admin > Firewall > Settings and disabling the “ICMP requests” option. This will disallow the ‘Ping’ requests to your PBX.

## 4. Menu Overview

The VitalPBX navigation menu is divided into four main sections, PBX, Reports, Settings, and Admin as outlined below.



**PBX**, where you can find all about the PBX settings:

- Extensions
  - **Extensions**, management of extensions and devices
  - **Hot Desking**, device management
  - **Import Extensions**, import extensions from CSV format
  - **Export Extensions**, export extensions in CSV format
  - **Bulk Modification**, bulk extension modification
  - **Bulk Extensions**, create a range of extensions in a single action
  - **Extension Status**, status of extensions, with possibility to changing the state

- Applications
  - **Conferences**, conference room management
  - **Custom Applications**, custom application management
  - **Custom Destinations**, custom destination management
  - **Custom Context**, custom context management
  - **Feature Codes**, management of telephone feature codes
  - **Paging & Intercom**, paging & intercom management
  - **Pickup Groups**, management of pickup groups
  - **Parking**, parking management
  - **Speed Dialing**, speed dial management
  - **Import/Export Speed Dialing**, Import/Export speed Dialing from/to CSV format
  - **Voicemail Broadcast Group**, voicemail broadcast group management
  - **Call Back**, management of call back functionality
  - **DISA**, Direct Inward System Access (DISA) management
  - **PIN List**, group of pins that will be used to access outgoing routes
  - **Dynamic Destination**, route calls based on the CID number.
- Class of Service
  - **Class of Service**, group of settings that define the dial plan to which each extension has access
  - **Features Category**, telephone feature groups that are associated with a Class of Service
  - **Dialing Restriction Rules**, dial-up restrictions that are associated with a Class of Service
  - **Customer Codes**, customer account codes that can be dynamically associated to a call in order to categorize the call in the CDR
  - **Authorization Code**, code that authorizes privileges to make a call
  - **Route Selections**, Automatic Route selection management
- Call Center
  - **Ring Groups**, groups of extensions that do not handle statistics. Ring Groups allow you to create a single extension number (the Ring Group number) that will ring on multiple extensions.
  - **Queues**, call queues that handle statistics through a log file
  - **Queues Priorities**, it gives priority to a queue call on another, very useful when an agent serves multiple queues simultaneously



- **Queues VIPs**, list of phones that will give priority in the call queue.
- **Queue Call Back**, with the Queues Call Back module, you can reduce customer frustration by minimizing time spent waiting.
- External
  - **Trunks**, SIP, IAX, DAHDI trunks management
  - **Outbound Routes**, management prefixes for outgoing routes
  - **Emergency Numbers**, create groups of emergency numbers to give them priority
  - **Inbound Routes**, DID management for incoming routes
  - **Dynamic Routing**, AutoCLIP Routes
- Incoming Calls
  - **IVR**, IVR and Automatic Attendant management
  - **Time Groups**, time group management
  - **Time Conditions**, time conditions management
  - **Announcement**, pre-announcement management
  - **Languages**, languages management
  - **Night Mode**, night mode management
  - **CID Modifiers**, Modifies the CID in incoming calls
  - **CID Lookup**, Search caller information in a database or URL
- Tools
  - **Asterisk CLI**, Asterisk command line management interface
  - **Blacklist**, blacklist management number
  - **Dashboard**, see system status in real time
  - **Log File Viewer**, displays the contents of log files
  - **Cron Profiles**, create profiles for periodic execution of certain routines
  - **Weak Password**, weak password detection
  - **Phonebooks**, create Phonebook to be accessed from phones
  - **Task Manager**, the task manager add-on is a powerful and fully free tool that allows you to schedule any script created by the user as a task from the GUI.
- Extras
  - **Video Conference**, create video conferences using WebRTC
- Emergency Calls
  - **Emergency Number**, this module defines the external numbers that cannot be restricted
  - **Dispatchable Locations**, this module allows you to create detailed locations which will be used when an Emergency Call is placed

**Reports**, where you can find everything about the CDR generated by phone calls

- CDR Reports
  - **CDR Filters**, management of filters to apply in reports
  - **CDR**, display call records (CDR)
- PBX Reports
  - **Active Calls**, displays calls in progress in real time.
  - **PJSIP Devices**, shows PJSIP terminals and trunks and if they are registered.
  - **SIP Devices**, shows SIP trunks and devices and if they are registered.
  - **IAX2 Devices**, shows the devices, Trunks and FAX IAX2 and if they are registered.
- **IVR Reports**, create reports of IVR use
- **Settings**, where you can find everything about the parameters of different technologies (such as SIP and IAX), voice mail settings, the PBX overall event files, configuration of analog and digital interfaces (DAHDi), auto-provisioning of phones (End Point Manager).
- Technology Settings
  - **PJSIP Settings**, general PJSIP settings management.
  - **SIP Settings**, general SIP settings management.
  - **IAX2 Settings**, general IAX settings management.
  - **Profiles**, profile management.
  - **Telephony Settings**, select Tone Zone. It is shown only if the Telephony module is installed.
  - **Dial Profiles**, dial profile management.
- Voicemail Settings
  - **Voicemail Settings**, general voice mail settings management
  - **Voicemail Timezones**, time zone management for voicemail
- PBX Settings
  - **System General**, general system settings such as directories, dial-plan settings, etc.
  - **Asterisk Manager Users**, to create users of Asterisk Manager.
  - **Log File**, create log files related to Asterisk.
  - **RTP Settings**, general RTP settings management.
  - **CEL Settings**, configure the applications to show in the detailed CDR.
  - **Mini HTTP Server**, Asterisk provides a basic HTTP/HTTPS server.
- Voice Prompts
  - **Asterisk Sounds**, manages the voice guides of the system in different languages.
  - **Music on Hold**, to create and upload music on hold.
  - **Recordings Management**, to upload recordings.

**Admin**, allows you to create system users and manage system settings.

- Admin
  - **Users**, management of system users.
  - **User Profiles**, management of user profiles.
  - **Application Access**, create APIs to give access to third party applications.
  - **Tenants**, Tenants settings and creation.
- System Settings
  - **System Misc.**, management of system notifications and date and time settings.
  - **Email Settings**, email server configuration
  - **Certificates**, create certificates of type Self Signed and Let's Encrypt
  - **HTTP Server**, assign ports to access the interface and enable the HTTPS server
- Firewall
  - **Settings**, here we configure all the firewall settings as well as intrusion detection (fail2ban).
  - **Services**, we add the services to be applied to the rules later.
  - **Rules**, we apply the firewall rules.
- Network
  - **Network Settings**, network management
  - **DHCP Settings**, DHCP server configuration
  - **OpenVPN Server**, manages OpenVPN server and client.
  - **OpenVPN Client**, connection settings to an OpenVPN Server.
- Add-ons
  - **Add-ons**, management add-ons modules and software.
- Tools
  - **Backup & Restore**, Backup and Restore the entire PBX configuration.
  - **Maintenance**, module to automatically maintain VitalPBX, convert **recordings**, delete old recordings, etc.
  - **Branding**, module to configure VitalPBX in a personalized way.

# 5. Configuration Considerations

## 5.1.- Security

Just like any other computer on your network that is connected to the Internet, VitalPBX can be targeted by hackers for the purpose of making cheap telephone calls. During the entire process of setting up VitalPBX, you should be constantly aware of the potential security implications of each step and make sure that your system is well protected.

## 5.2.- Numbering System

You need to decide how many digits to use for extensions – do you want to use 3, 4, or more? You should consider that most feature codes are 2 digits, so setting a system with 2-digit extensions is not really practical. It will help you to navigate your system if you group similar functions together, for example, by using the following ranges:

2000 - 2999 for extensions

500 - 599 for ring groups

600 - 699 for queues

700 - 799 for conferences

# 6. PBX

## 6.1 Extensions

### 6.1.1 Extensions

Extensions allow you to configure extensions (users) and devices (telephones) in your system.

#### General

The screenshot displays the 'Extensions' configuration page in the VitalPBX web interface. The page is titled 'Extensions' and has a navigation bar with tabs: GENERAL, VOICEMAIL, RECORDING, ADVANCED, FOLLOW ME, and INCOMING ROUTES. The main content area is divided into two sections: 'Extension' and 'Devices'.

**Extension Section:**

- Extension #: 8702
- Name: Frank Smith
- Class of Service: All Permissions
- Features Password: 129549
- Email Addresses: fsmith@vitalpbx.com
- Internal CID: Frank Smith, 8702
- External CID: Name, Number
- Emergency CID: Name, Number
- Account Code:
- Language: English (en)

**Devices Section:**

- Technology: PJSIP
- Device: 8702 - Frank Smith
- User Device: 8702
- Password:
- Device Description: Frank Smith
- Profile: Default PJSIP Profile
- Max Contacts: 1
- Codecs:
- DTMF Mode: rfc4733
- Emergency CID: Name, Number
- Dispatchable Location: Default
- Deny: 0.0.0.0/0
- Permit: 0.0.0.0/0
- Ring Device: Yes
- Send Push: No
- Vibri Client: No

At the bottom of the page, there are three buttons: 'Unlink Device' (orange), 'Update' (green), 'Delete' (red), and 'Cancel' (grey).

**Extension\***, number to dial in order to reach this extension. The extension number must be unique, and should not conflict with an existing extension number, or any other number that is assigned to any other entity within the system, such as a conference, queue, ring group, feature code, etc. The value of this field cannot be changed after the extension has been saved.

**Name\***, name to identify this extension. This is generally the end user's name or the location of the extension, e.g. Fernando Alonso or Server Room. This value will be displayed as the caller ID text for any calls placed from this extension to other users or devices on the PBX unless the Internal CID field contains a value.

**CoS Name**, the dial plan can be segmented into sections, called Classes of Service (CoS). CoS are the basic organizational unit within the dial plan, and as such, they keep different sections of the dial plan independent of each other. VitalPBX uses CoS to

enforce security boundaries between the various parts of the dial plan, as well as to provide different classes of service to different groups of users.

**Features Password**, password to access certain system features and the control panel of the phone.

**Email Address**, email address to where the services messages will be sent.

**Internal CID**, internal Caller ID for the extension, consisting of two parts: the CID Name and the CID Number. This will define the caller ID text that is displayed when this user calls other (internal) users on the same PBX. This could be used when a user is part of a department in which callbacks should be directed to the department rather than directly to the user (such as a technical support department). This field is not mandatory. If the field is left blank, the user's extension will be used to set the Outbound Caller ID text.

**External CID**, external Caller ID for the extension, consisting of two parts: the CID Name and the CID Number. This will define the caller ID text that is displayed when this user makes calls outside of the PBX. This could be used when a user is part of a department in which callbacks should be directed to the department rather than directly to the user (such as a technical support department). Setting the caller ID must be supported by the trunk service provider. This field is not mandatory, but if the field is left blank, the default caller ID name for the trunk placing the call will be used to set the caller ID name text.

**Emergency CID**, it allows to define the caller id that will be used in case of calling an emergency number.

**Account Code**, this field is used to populate the Account Code field of the Call Detail Record (CDR). If the field is left blank, the Account Code field of the CDR record will also be blank.

**Language**, specifies the language setting to be used for this extension. This will force all prompts specific to the user to be played in the selected language, provided that the language is installed, and voice prompts for the specified language exist on your server. This field is not required. If left blank, prompts will be played in the default language of the VitalPBX server.

## Devices section

This section allows you to configure the device that is linked to the extension. Technology, type of technology used by this device. The technology options are:

**PJSIP**, PJSIP device

**SIP**, SIP device

**IAX2**, IAX device

**FXS**, analog device

**NONE**, extension without device.

### PJSIP

**User Device\***, username to be used when registering this device.

**Password**, password (secret) associated with this device. Passwords can be the weakest link on any externally accessible PBX system, as malicious users will attempt to locate extensions having weak passwords. Extensions that authenticate by using simple passwords such as "1234" stand a good chance of being compromised, allowing an attacker to place calls through your PBX. Pick strong passwords carefully and ensure that passwords are not given to anyone who does not need to know them. Passwords should be at least 8 characters long and should include a random mixture of letters (both upper- and lower-case), numbers, and special characters.

**Profile**, group of settings for this device. Each technology (PJSIP, SIP, IAX2, DAHDi, or None) must have at least one (default) profile that defines attributes for the technology. You can configure these profiles in the Settings->Technology Settings->Profiles menu.

**Max Contacts**, maximum number of contacts that can bind to an AoR.

**Codecs**, list of allowed codecs. The order in which the codecs are listed determines their order of preference. If you select at least one codec, the DISALLOW=ALL parameter will be added. This will ensure that the device will only use only the codecs that you specifically define for the device.

**DTMF Mode**, sets default dtmf-mode for sending Dual Tone Multi-Frequency (DTMF). The DTMF mode for a SIP device specifies how touchtone will be transmitted to the other side of the call. The default value is rfc4733. Available options are:

- Rfc4733
- info: SIP INFO messages (application/dtmf-relay)
- shortinfo: SIP INFO messages (application/dtmf)
- inband: Inband audio (requires 64 kbit codec -alaw, ulaw)
- auto: Use rfc4733 if offered, in-band otherwise

**Device Description**, a short (optional) description to identify this device.

**Emergency CID**, this is the CID to be used when an Emergency Call is placed with this device.

**Dispatchable Location**, this is the location to be used whenever an Emergency Call is placed from this device.

**Deny**, in a user/peer definition, allows you to limit SIP traffic to and from this peer to a certain IP or network. This option should be in the format of an IP address and subnet, such as 192.168.25.10/255.255.255.255 (denies traffic from this specific IP address), or 192.168.1.0/255.255.255.0 (to disallow traffic for this extension from the IP range of 192.168.1.1 to 192.168.1.254). It is possible to enter a value of 0.0.0.0/0.0.0.0 to deny all the networks by default, and, to enter specific networks from which traffic can be accepted in the permit option. This option is commonly used to restrict endpoint usage to a particular network, so that if the endpoint is stolen or otherwise removed from the network, it cannot be used to place calls and will be essentially useless. This field is not required. If it is left blank, VitalPBX will not block traffic for this peer from any IP address.

**Permit**, in a user/peer definition, allows you to limit SIP traffic to and from this peer to a certain IP or network. For example, 192.168.10.0/255.255.255.0 allows traffic from any address on the 192.168.10.x network. The permit option is the opposite of the deny option. Specific IP addresses or networks can be added in this option to allow traffic for this extension from the entered IP/network. This field is not required. If it is left blank, traffic will be allowed from all IP addresses. Strengthen your system security by use of the deny and allow options, where possible. If the endpoint is static, we strongly recommend that you make proper use of the permit and deny options to ensure that traffic is only allowed from the specific address. Even if the endpoint is not static, but always resides on a known subnet, you should limit the allowed range to that specific subnet.

**Ring Device**, this determines whether incoming calls should cause the device to ring.

**Send Push**, if this is enabled, the PBX will attempt to send push notifications to mobile devices using **VitXi Mobile**.

**VitXi Client**, if this is enabled, this device can be used for VitXi Applications, be it WebRTC or Mobile Apps. When devices with this option enabled are use on VitXi Mobile, all of the premium features will be enabled on the softphone.

## SIP

**User Device\***, username to be used when registering this device.

**Password**, password (secret) associated with this device. Passwords can be the weakest link on any externally accessible PBX system, as malicious users will attempt to locate extensions having weak passwords. Extensions that authenticate by using simple passwords such as "1234" stand a good chance of being compromised, allowing an attacker to place calls through your PBX. Pick strong passwords carefully and ensure that passwords are not given to anyone who does not need to know them. Passwords should be at least 8 characters long and should include a random mixture of letters (both upper- and lower-case), numbers, and special characters.

**Profile**, group of settings for this device. Each technology (SIP, IAX2, DAHDi) must have at least one (default) profile that defines attributes for the technology. You can configure these profiles in the Settings->Technology Settings->Profiles menu.



**Codecs**, list of allowed codecs. The order in which the codecs are listed determines their order of preference. If you select at least one codec, the `DISALLOW=ALL` parameter will be added. This will ensure that the device will only use only the codecs that you specifically define for the device.

**NAT**, (Network Address Translation) is a technology commonly used by firewalls and routers to allow multiple devices on a LAN with 'private' IP addresses to share a single public IP address. A private IP address is an address, which can only be addressed from within the LAN, but not from the Internet outside the LAN Options:

- **Default:** will use the default NAT settings set on the SIP Settings.
- **No:** No special NAT handling other than RFC3581
- **Force:** Pretend there was a `rport` parameter even if there wasn't
- **Comedia:** Send media to the `rport` Asterisk received it from regardless of where the SDP says to send it.
- **Auto Force:** Set the force `rport` option if Asterisk detects NAT
- **Auto Comedia:** Set the comedia option if Asterisk detects NAT

**DTMF Mode**, sets default dtmf-mode for sending Dual Tone Multi-Frequency (DTMF). The DTMF mode for a SIP device specifies how touchtone will be transmitted to the other side of the call. The default value is `rfc2833`. Available options are:

- **info:** SIP INFO messages (`application/dtmf-relay`)
- **shortinfo:** SIP INFO messages (`application/dtmf`)
- **inband:** Inband audio (requires 64 kbit codec `-alaw, ulaw`)
- **auto:** Use `rfc2833` if offered, in-band otherwise

**Device Description**, a short (optional) description to identify this device.

**Deny**, in a user/peer definition, allows you to limit SIP traffic to and from this peer to a certain IP or network. This option should be in the format of an IP address and subnet, such as `192.168.25.10/255.255.255.255` (denies traffic from this specific IP address), or `192.168.1.0/255.255.255.0` (to disallow traffic for this extension from the IP range of 192.168.1.1 to 192.168.1.254). It is possible to enter a value of `0.0.0.0/0.0.0.0` to deny all of the networks by default, and, to enter specific networks from which traffic can be accepted in the permit option. This option is commonly used to restrict endpoint usage to a particular network, so that if the endpoint is stolen or otherwise removed from the network, it cannot be used to place calls and will be essentially useless. This field is not required. If it is left blank, VitalPBX will not block traffic for this peer from any IP address.

**Permit**, in a user/peer definition, allows you to limit SIP traffic to and from this peer to a certain IP or network. For example, `192.168.10.0/255.255.255.0` allows traffic from any address on the 192.168.10.x network. The permit option is the opposite of the deny option. Specific IP addresses or networks can be added in this option to allow traffic for this extension from the entered IP/network. This field is not required. If it is left blank, traffic will be allowed from all IP addresses. Strengthen your system security by use of the deny and allow options, where possible. If the endpoint is static, we strongly recommend that you make proper use of the permit and deny options to ensure that

traffic is only allowed from the specific address. Even if the endpoint is not static, but always resides on a known subnet, you should limit the allowed range to that specific subnet.

**Ring Device**, this determines whether incoming calls should cause the device to ring.

### IAX2

**User Device\***, username to be used when registering this device.

**Password**, password (secret) associated with this device. Passwords can be the weakest link on any externally accessible PBX system, as malicious users will attempt to locate extensions having weak passwords. Extensions that authenticate by using simple passwords such as "1234" stand a good chance of being compromised, allowing an attacker to place calls through your PBX. Pick strong passwords carefully and ensure that passwords are not given to anyone who does not need to know them. Passwords should be at least 8 characters long and should include a random mixture of letters (both upper- and lower-case), numbers, and special characters.

**Profile**, group of settings for this device. Each technology (SIP, IAX2, Telephony, or None) must have at least one (default) profile that defines attributes for the technology. You can configure these profiles in the Settings->Technology Settings->Profiles menu.

**Codecs**, list of allowed codecs. The order in which the codecs are listed determines their order of preference. If you select at least one codec, the DISALLOW=ALL parameter will be added. This will ensure that the device will only use only the codecs that you specifically define for the device.

**Device Description**, a short (optional) description to identify this device.

**Deny**, in a user/peer definition, allows you to limit SIP traffic to and from this peer to a certain IP or network. This option should be in the format of an IP address and subnet, such as 192.168.25.10/255.255.255.255 (denies traffic from this specific IP address), or 192.168.1.0/255.255.255.0 (to disallow traffic for this extension from the IP range of 192.168.1.1 to 192.168.1.254). It is possible to enter a value of 0.0.0.0/0.0.0.0 to deny all of the networks by default, and, to enter specific networks from which traffic can be accepted in the permit option. This option is commonly used to restrict endpoint usage to a particular network, so that if the endpoint is stolen or otherwise removed from the network, it cannot be used to place calls and will be essentially useless. This field is not required. If it is left blank, VitalPBX will not block traffic for this peer from any IP address.

**Permit**, in a user/peer definition, allows you to limit SIP traffic to and from this peer to a certain IP or network. For example, 192.168.10.0/255.255.255.0 allows traffic from any address on the 192.168.10.x network. The permit option is the opposite of the deny option. Specific IP addresses or networks can be added in this option to allow traffic for this extension from the entered IP/network. This field is not required. If it is left blank, traffic will be allowed from all IP addresses. Strengthen your system security by use of the deny and allow options, where possible. If the endpoint is static, we strongly recommend that you make proper use of the permit and deny options to ensure that

traffic is only allowed from the specific address. Even if the endpoint is not static, but always resides on a known subnet, you should limit the allowed range to that specific subnet.

**Ring Device**, this determines whether incoming calls should cause the device to ring.

### FXS – (Only available if the DAHDI add-on is installed)

**Channel\***, the Telephony (DAHDI) channel, selected from the drop-down list, that should be associated with this device.

**Profile**, group of settings for this device. Each technology (SIP, IAX2, Telephony, or None) must have at least one (default) profile that defines attributes for the technology. You can configure these profiles in the Settings->Technology Settings->Profiles menu.

**Device Description**, a short (optional) description to identify this device.

**Ring Device**, this determines whether incoming calls should cause the device to ring.

### NONE

- Extensions that do not have a device, used for virtual voicemail or Hot Desking.

## Voicemail

Setting	Value
Enabled	Yes
Voicemail Password	8890
Zone Messages	None
Alias	
Attach Voicemail	Yes
Delete	No
Allow to Call Back	No
Ask Password	Yes
Skip Instructions	No
Say CID	Yes
Say Duration	Yes
Envelope	Yes
Hide From Directory	No
Allow to Dial Out	No
Generate Hint	No

Save

**Enabled**, enable or disable voicemail. If voicemail is not enabled, voicemail messages cannot be left for the user.

**Attach Voicemail**, Attach voicemail to email.

**Delete**, the voicemail is deleted from the server after the voicemail has been delivered. Be careful with this option, because VitalPBX will allow you to delete the message without guaranteeing that a copy of it has been attached to the email notification, or that the email has been delivered successfully. This could mean that after a message

is left and a notification email is sent to the user, the actual voicemail that was left may no longer be accessible.

**Voicemail Password**, the numeric password to access the voicemail. The voicemail system will compare the password entered by the user against this value.

**Zone Messages**, time zone for messages. If not set, the time zone will be taken from the general settings section. Irrelevant if envelope is no.

**Alias**, an alternative name that can be used in the system-created phonebook, or for dialing using the Phonebook Directory feature code (411)

**Allow to Call Back**, if checked, users will be available to call back to the sender of a message. The specified Class of Service will need to be able to handle dialing of numbers in the format in which they are received (for example, the country code may not be received with the caller ID but might be required for the outgoing call).

**Ask Password**, it allows to define if the users who dials \*97 to access to their own voicemail will be prompted to enter its voicemail password or not. This doesn't apply for the "Remote Voicemail (\*98)" feature.

**Skip Instructions**, if set to yes, it will skip the playback of instructions for leaving a message to the calling party.

**Say CID**, system will play back the caller ID number of the person who left the message prior to the message being played.

**Say Duration**, turn on/off the duration information before playing the voicemail message.

**Envelope**, this determines whether the user will hear the date and time that the message was left prior to hearing the voicemail message being played.

**Hide from Directory**, hide If set to yes, this name of this user will not be visible to the system-created phonebook, and you cannot dial to this user using the Phonebook Directory feature code (411).

**Allow to Dial Out**, if allowed, users can dial out from their mailboxes (option 4 from mailbox's advanced menu). **This is considered a very dangerous practice in a phone system (mainly because many voicemail users like to use 1234 as their password) and is therefore not recommended.**

**Generate Hint**, if enabled, it will be possible to remotely monitor the voicemail status of this extension through a BLF key. To configure the BLF, you must to use the following format: vm\_1234, where 1234 is the extension that will be monitored.

## Recording

The screenshot shows the 'Recording' configuration page for an extension. The page has tabs for GENERAL, VOICEMAIL, RECORDING (selected), ADVANCED, FOLLOW ME, and INCOMING ROUTES. The RECORDING section contains several toggle switches and a dropdown menu. Outgoing, Incoming, Internal, and On Demand Recording are all set to 'No'. The Dictation section has 'Enabled' set to 'No' and 'Format' set to 'Ogg Vorbis'. The 'Auto-Send Email' toggle is also set to 'No'. A 'Save' button is located at the bottom right.

In this tab you will find the information about the recording telephone calls and dictation recording.

This group of fields allows a user to control the recording of incoming or outgoing calls. The user can either dial a feature code (\*3) to selectively enable recording for the current call, never record calls, or always record calls.

**Outgoing**, record external outgoing calls.

**Incoming**, record external incoming calls.

**Internal**, record internal calls.

**On Demand Recording**, record calls on demand.

### Dictation section

- **Enabled**, activates the dictation service when set to Yes.
- **Format**, recording audio format:
  - OGG Vorbis
  - GSM
  - WAV

**Auto-Send Email**, recording will be sent automatically once completed.

## Advanced

The screenshot shows the 'Advanced' configuration page for an extension in VitalPBX. The page is divided into several sections:

- General Settings:** Ring Time (Default 30), Call Limit (No Limit), Internal Auto Answer (Disable), Dial Profile (Default), Music on Hold Class (Default), Secretary Extension (None), CallerID On Diversions (Caller).
- Advanced Settings:** Diversion Hints (No), Block Spy Me (No), Send CallerID (Yes), Call Waiting (Yes), Pinless (No), Dynamic Routing (No).
- Call Center Settings:** Dynamic Queues and Static Queues (empty).
- User Portal:** Enable Portal (Yes), Portal User (8890), Portal Password (empty), Fax Device (-- Select a Fax Device --).
- User Image:** A green logo image is displayed with a 'Select Image' button below it.

A 'Save' button is located at the bottom right of the configuration area.

**Ring Time**, the number of seconds to ring the device before giving up and moving on to the next priority for the extension.

**Call Limit**, maximum number of simultaneous calls that can be received by this device.

**Dial Profile**, there are many options that you can set on the outbound call, including call screening, distinctive ringing, and more. Goto Settings/Technology/Dial Profile for more information.

**Internal Auto Answer**, automatic call answering can be requested from within the incoming call by using the SIP Alert-Info header. This can only be utilized when automatic call answering is allowed on the phone.

**Music on Hold Class**, this option specifies which music on hold class to suggest to the peer channel when this channel places the peer on hold.

**Secretary Extension**, functionality is used to re-route all incoming calls for this extension to the secretary's extension. Only the secretary is allowed to make direct calls to this extension.

**Caller ID on Diversions**, this allows you to define which CID will be sent when the call is forwarded.

- **Caller**, this will send the CID of the person calling.
- **Called**, this will send the CID of the person receiving the call and has the diversion activated.

**Fax Enabled**, Enable/Disable fax.

**Diversions Hints**, this generates hints regarding status of the extension. For example, hints could be generated for diversions (DND, Call Forwarding, Personal Assistant and Boss/Secretary). **Do not activate this option unless your phone has a console or keys for Hints. Activating this option can slow down the “Apply Changes” in the PBX and overload.**

**Block Spy Me**, do not let other users to spy on this extension.

**Send Caller ID**, send, or hide, the Caller ID for this extension.

**Call Waiting**, if you uncheck this option, only one incoming call will be allowed to this extension.

**Pin less**, if enabled, the user of this extension will not be prompted to enter pin on outbound routes that have assigned a pin set.

**Dynamic Routing**, this allows you to enable or disable the dynamic routing towards this extension. If enabled, when an external party (that was previously called by this extension) calls back, the call will be routed directly to this extension.

### Call Center Settings

This section contains two fields (Dynamic Queues, Static Queues) that allows you to assign or remove massively an extension to any queue or group of queues

**Dynamic Queues**, these are the agents who will be allowed to log in the call queue.

**Static Queues**, are agents that will always be in the queue, these agents do not need to log in.

### User Portal

**Enable Portal**, allow users to login to Portal to configure their own extension.

**Portal User**, user for login as portal user.

**Portal Password**, password for access to portal area.

**Fax Device**, this option assigns a fax device to this extension, so they can send and receive faxes from the user interface using the Virtual Faxes add-on.

### User Image section

Allows the user to select any image and associate it with the extension. It may be the photo of the owner of the extension, an avatar, or any other graphic; in PNG, JPG, or JPEG format. The size of the file must be less than 20 MB.

## Follow Me

**Follow Me List**, list of extensions and/or external numbers to be accessed by follow me.

**Initial Ring Time**, time in seconds to ring the primary extension before calling to the members on the follow-me list.

**Ring Time**, this is the time that the phone will be allowed to ring, without being answered, before continuing to an alternative destination.

**Ring Strategy**, here you define the strategy to ring this list.

**One by One**: ring all available number in the Follow List One by One.

**Ring All**: ring all available number in the Follow List at the same time.

**Music on Hold**, the Music on Hold class that should be used for the caller while they are waiting to be connected.

**Call-from Prompt**, you can select the default option to use the “Incoming call from” message prompt or use your own custom prompt.

**No Recording Prompt**, you can select to use the standard “You have an incoming call” message prompt when the caller elects not to leave their name or the option isn't set for them to do so or use your own custom prompt.

**Please Hold Prompt**, you can select to use the standard “Please hold while we try and connect your call” message prompt or use your own custom prompt.

**Status Prompt**, you can select to use the standard “The party you're calling isn't at their desk” message prompt or use your own custom prompt.

**Sorry Prompt**, you can select to use the standard “I'm sorry, but we were unable to locate your party” message prompt or use your own custom prompt.

**Enabled**, it allows you to enable/disable the follow-me feature on this extension.

### FollowMe Options

**Record Caller's Name**, here you can record the caller's name so it can be announced to the callee at each step.



**Prompt Called**, called party will be asked whether they wish to accept the incoming call.

## Incoming Routes

The DID number for incoming calls, i.e. the inbound route that should be associated with this extension.

The screenshot shows the 'Extensions' configuration interface. At the top, there are tabs for 'GENERAL', 'VOICEMAIL', 'RECORDING', 'ADVANCED', 'FOLLOW ME', and 'INCOMING ROUTES'. The 'INCOMING ROUTES' tab is selected. Below the tabs, there are three input fields: 'Description', 'DID Pattern', and 'CID Pattern'. A green 'Save' button is located at the bottom right of the form.

**Description**, a short description to identify the route.

**DID Pattern**, the DID number for incoming calls, i.e. the inbound route that should be associated with this extension.

**CID Pattern**, optional CID number to make route more specific.

**Actions**, go to Inbound Route module.

## Welcome Email

Starting from Version 3 of VitalPBX, it is now possible to send a welcome email with various information about the new user extension. For this to work, we need to have the following configured.

Under Settings > PBX Settings > System General, enable the option “Send Welcome Email”.

Configure the email client with the account to send emails with, under Admin > System Settings > E-Mail Settings.

Make sure that the extension you created has an email assigned on the General Tab.

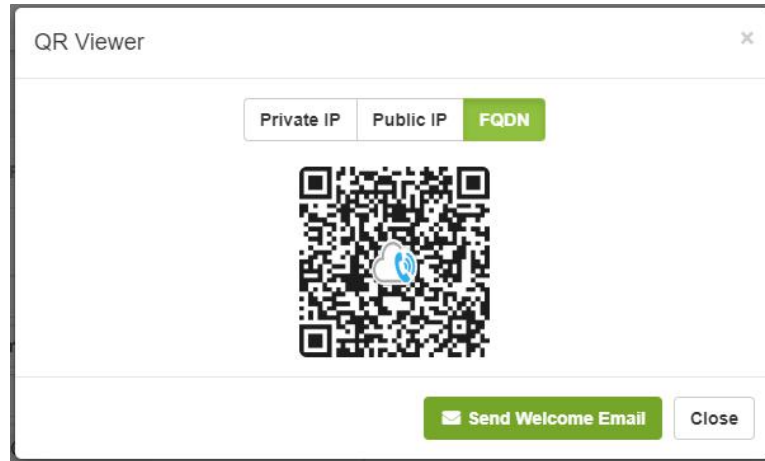
Note: If you wish to modify the contents of this email, you can do so under Admin > System Settings > Email Templates.

You can also see the QR code or send the Welcome Email Manually by pressing the QR button next to the Device Field.

Device

8702 - Frank Smith





## 6.1.2 Hot Desking

The Hot Desking module is where the accounts are created for devices without the need of having an extension number. A Hot Desking device is associated with an extension that previously had to be created in the module extensions with technology option "None", i.e. without being associated with any device. A Hot Desking device can be associated with an extension by dialing the hot desking feature code (\*80), the extension number, and the extension password. To remove the association, you only need to dial the hot desking feature code (\*80).

### General

**Technology**, type of technology for this device. There are four options:

- **PJSIP**, PJSIP device
- **SIP**, sip device
- **IAX2**, iax device
- **FXS**, analog/digital device. This is displayed if you got the DAHDI module installed.

Emergency CID, this is the Emergency CID to use when placing an Emergency Call from this device.

Dispatchable Location, Location to use whenever an Emergency Call is places.

### PJSIP

**User Device\***, username to be used when registering this device.

**Password**, password (secret) associated with this device. Passwords can be the weakest link on any externally accessible PBX system, as malicious users will attempt to locate extensions having weak passwords. Extensions that authenticate by using simple passwords such as "1234" stand a good chance of being compromised, allowing an attacker to place calls through your PBX. Pick strong passwords carefully and ensure that passwords are not given to anyone who does not need to know them. Passwords should be at least 8 characters long and should include a random mixture of letters (both upper- and lower-case), numbers, and special characters.

**Profile**, group of settings for this device. Each technology (PJSIP, SIP, IAX2, DAHDi, or None) must have at least one (default) profile that defines attributes for the technology. You can configure these profiles in the Settings->Technology Settings->Profiles menu.

**Max Contacts**, maximum number of contacts that can bind to an AoR.

Codecs, list of allowed codecs. The order in which the codecs are listed determines their order of preference. If you select at least one codec, the DISALLOW=ALL parameter will be added. This will ensure that the device will only use only the codecs that you specifically define for the device.

**DTMF Mode**, sets default dtmf-mode for sending Dual Tone Multi-Frequency (DTMF). The DTMF mode for a SIP device specifies how touchtone will be transmitted to the other side of the call. The default value is rfc4733. Available options are:

- Rfc4733
- info: SIP INFO messages (application/dtmf-relay)
- shortinfo: SIP INFO messages (application/dtmf)
- inband: Inband audio (requires 64 kbit codec -alaw, ulaw)
- auto: Use rfc4733 if offered, in-band otherwise

**Device Description**, a short (optional) description to identify this device.

**Deny**, in a user/peer definition, allows you to limit SIP traffic to and from this peer to a certain IP or network. This option should be in the format of an IP address and subnet, such as 192.168.25.10/255.255.255.255 (denies traffic from this specific IP address), or 192.168.1.0/255.255.255.0 (to disallow traffic for this extension from the IP range of 192.168.1.1 to 192.168.1.254). It is possible to enter a value of 0.0.0.0/0.0.0.0 to deny all of the networks by default, and, to enter specific networks from which traffic can be accepted in the permit option. This option is commonly used to restrict endpoint usage to a particular network, so that if the endpoint is stolen or otherwise removed from the network, it cannot be used to place calls and will be essentially useless. This field is not required. If it is left blank, VitalPBX will not block traffic for this peer from any IP address.

**Permit**, in a user/peer definition, allows you to limit SIP traffic to and from this peer to a certain IP or network. For example, 192.168.10.0/255.255.255.0 allows traffic from any address on the 192.168.10.x network. The permit option is the opposite of the deny option. Specific IP addresses or networks can be added in this option to allow traffic for this extension from the entered IP/network. This field is not required. If it is left blank, traffic will be allowed from all IP addresses. Strengthen your system security by use of the deny and allow options, where possible. If the endpoint is static, we strongly recommend that you make proper use of the permit and deny options to ensure that traffic is only allowed from the specific address. Even if the endpoint is not static, but always resides on a known subnet, you should limit the allowed range to that specific subnet.

**Ring Device**, this determines whether incoming calls should cause the device to ring.

### SIP

**User\***, user to register this device.

**Password**, password (secret) associated with this device.

**Profile**, technology profile to be associated with this device.

**Codecs**, list of allowed codecs. The order in which the codecs are listed determines their order of preference. If you do not select at least one codec, DISALLOW=ALL will be used.

**DTMF Mode**, sets default dtmf-mode for sending Dual Tone Multi-Frequency (DTMF). The DTMF mode for a SIP device specifies how touchtones will be transmitted to the other side of the call. The default value is rfc2833. Available options are:

- info: SIP INFO messages (application/dtmf-relay)
- shortinfo: SIP INFO messages (application/dtmf)
- inband: Inband audio (requires 64 kbit codec -alaw, ulaw)
- auto: Use rfc2833 if offered, in-band otherwise

**Device Description\***, a short description to identify this device.

**Deny**, in a user/peer definition, allows you to limit SIP traffic to and from this peer to a certain IP or network. This option should be in the format of an IP address and subnet, such as 192.168.25.10/255.255.255.255 (denies traffic from this specific IP address), or 192.168.1.0/255.255.255.0 (to disallow traffic for this extension from the IP range of 192.168.1.1 to 192.168.1.254). It is possible to enter a value of 0.0.0.0/0.0.0.0 to deny all of the networks by default, and, to enter specific networks from which traffic can be accepted in the permit option. This option is commonly used to restrict endpoint usage to a particular network, so that if the endpoint is stolen or otherwise removed from the network, it cannot be used to place calls and will be essentially useless. This field is not required. If it is left blank, VitalPBX will not block traffic for this peer from any IP address.

**Permit**, in a user/peer definition, allows you to limit SIP traffic to and from this peer to a certain IP or network. For example, 192.168.10.0/255.255.255.0 allows traffic from any address on the 192.168.10.x network. The permit option is the opposite of the deny option. Specific IP addresses or networks can be added in this option to allow traffic

for this extension from the entered IP/network. This field is not required. If it is left blank, traffic will be allowed from all IP addresses. Strengthen your system security by use of the deny and allow options, where possible. If the endpoint is static, we strongly recommend that you make proper use of the permit and deny options to ensure that traffic is only allowed from the specific address. Even if the endpoint is not static, but always resides on a known subnet, you should limit the allowed range to that specific subnet.

**NAT**, (Network Address Translation) is a technology commonly used by firewalls and routers to allow multiple devices on a LAN with 'private' IP addresses to share a single public IP address. A private IP address is an address, which can only be addressed from within the LAN, but not from the Internet outside the LAN Options:

- No: No special NAT handling other than RFC3581
- Force: Pretend there was an rport parameter even if there wasn't
- Comedia: Send media to the port Asterisk received it from regardless of where the SDP says to send it.
- Auto Force: Set the force\_rport option if Asterisk detects NAT
- Auto Comedia: Set the comedia option if Asterisk detects NAT

**Ring Device**, this determines whether incoming calls should cause this device to ring.

## IAX2

**User\***, user to register this device.

**Password**, password (secret) associated with this device.

**Profile**, technology profile to be associated with this device.

**Codecs**, list of allowed codecs. The order in which the codecs are listed determines their order of preference. If you do not select at least one codec, DISALLOW=ALL will be used.

**Device Description\***, a short description to identify this device.

**Deny**, in a user/peer definition, allows you to limit SIP traffic to and from this peer to a certain IP or network. This option should be in the format of an IP address and subnet, such as 192.168.25.10/255.255.255.255 (denies traffic from this specific IP address), or 192.168.1.0/255.255.255.0 (to disallow traffic for this extension from the IP range of 192.168.1.1 to 192.168.1.254). It is possible to enter a value of 0.0.0.0/0.0.0.0 to deny all of the networks by default, and, to enter specific networks from which traffic can be accepted in the permit option. This option is commonly used to restrict endpoint usage to a particular network, so that if the endpoint is stolen or otherwise removed from the network, it cannot be used to place calls and will be essentially useless. This field is not required. If it is left blank, VitalPBX will not block traffic for this peer from any IP address.

**Permit**, in a user/peer definition, allows you to limit SIP traffic to and from this peer to a certain IP or network. For example, 192.168.10.0/255.255.255.0 allows traffic from any address on the 192.168.10.x network. The permit option is the opposite of the deny option. Specific IP addresses or networks can be added in this option to allow traffic for this extension from the entered IP/network. This field is not required. If it is left blank, traffic will be allowed from all IP addresses.

Strengthen your system security by use of the deny and allow options, where possible. If the endpoint is static, we strongly recommend that you make proper use of the permit and deny options to ensure that traffic is only allowed from the specific address. Even if the endpoint is not static, but always resides on a known subnet, you should limit the allowed range to that specific subnet.

**Ring Device**, this determines whether incoming calls should cause this device to ring.

**FXS** – (Only appears when the DAHDI add-on is installed.)

**Channel\***, the Telephony (DAHDI) channels, selected from the drop-down list, to be associated with this device.

**Profile**, technology profile to be associated with this device.

**Device Description\***, a short description to identify this device.

**Ring Device**, this determines whether incoming calls should cause this device to ring.

## 6.1.3 Import Extensions

Import Extensions is an easy way to create extensions in a large system. You can create a csv file from a template that can be downloaded from this same module. This template can be edited in Excel and then imported into VitalPBX.

The screenshot shows a web interface for 'Import Extensions'. The page has a title 'General' and a sub-header 'Import Extensions'. The main content area is titled 'GENERAL' and contains a 'CSV File' input field with a file upload icon. At the bottom right, there are two buttons: 'Import Extensions' (green) and 'Download Import Format' (blue).

**CSV File**, CSV File with details of the extension/s to process.

An example of the file format can be download by press the “Download Import Format” button at the bottom of the screen. In the first line of this file there is a complete description of each field.

## 6.1.4 Export Extensions

Export all Extensions in CSV format.

### CSV Format

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Operation	Extension nu	Display nam	Language se	Class of Serv	Device techn	Profile for de	Device user	Device passv	Device descr	Caller ID nam	Caller ID num	FXS channel	Ring device c	Password for	Email address
2	mode	extension	ext_name	language	class_of_ser	technology	profile_nam	device_user	device_pass	device_descr	devices_eme	devices_eme	channel	ring_device	features_pas	email
3	add	2000	Boss	en	all	pjsip	Default PJSIF	2000	hn7Qx8Gbbn	Boss			yes	*26382		
4	add	2001	Secretary	en	all	sip	Default SIP P	2001	pSWJHj55B2	Secretary			yes	*88832		
5	add	2002	IT Admin	en	all	iax	Default IAX2	2002	WuQVYbJ5aj	IT Admin			yes	*93775		

## 6.1.5 Bulk Modification

In this module, you can make changes to a group of extensions very easily and quickly. For example, you could change the language of all the extensions at once.

### General

Click on the Add Extensions button to select the extensions that you wish to modify.

**Field,** manage the following fields:

Class of Service  
 Ring Time  
 Language  
 Account Code  
 Dial Options  
 Music on Hold  
 Call Recordings  
 Diversion Hints

## 6.1.6 Bulk Extensions

In this module it is possible to create extensions in a range defined by the user.

### General

**Extension Range**, this defines the range of extensions that you want to create, eg.: from 1000 to 1400. If any of the extensions in the range already exists will be skipped.

**Name prefix**, this allows you to define a prefix to use as part of the extension name, eg.: if you set the prefix value to Agent and the extension is 200, the extension name will be Agent 200. If blank, the word Extension will be used as prefix.

**Class of Service**, the dial plan can be segmented into sections, called Classes of Service (CoS). CoS are the basic organizational unit within the dial plan, and as such, they keep different sections of the dial plan independent of each other. VitalPBX uses CoS to enforce security boundaries between the various parts of the dial plan, as well as to provide different classes of service to different groups of users.



**Language**, this specifies the language setting to be used for this extension. This will force all prompts specific to the user to be played in the selected language, provided that the language is installed and voice prompts for the specified language exist on your server. This field is not required. If left blank, prompts will be played in the default language of the VitalPBX server.

**Devices Technology**, type of technology used by this device. The technology options are:

- PJSIP, PJSIP device
- SIP, SIP device
- IAX2, IAX device
- FXS, analog device

NONE, extension without device.

**Devices Password**, password (secret) associated with this device. Passwords can be the weakest link on any externally accessible PBX system, as malicious users will attempt to locate extensions having weak passwords. Extensions that authenticate by using simple passwords such as "1234" stand a good chance of being compromised, allowing an attacker to place calls through your PBX. Pick strong passwords carefully and ensure that passwords are not given to anyone who does not need to know them. Passwords should be at least 8 characters long and should include a random mixture of letters (both upper- and lower-case), numbers, and special characters.

**Dial Profile**, there are many options that you can set on the outbound call, including call screening, distinctive ringing, and more. Goto Settings/Technology/Dial Profile for more information.

**Codecs**, list of allowed codecs. The order in which the codecs are listed determines their order of preference. If you select at least one codec, the DISALLOW=ALL parameter will be added. This will ensure that the device will only use only the codecs that you specifically define for the device.

**Music on Hold Class**, this option specifies which music on hold class to suggest to the peer channel when this channel places the peer on hold.

**Recording calls**, this group of fields allows a user to control the recording of incoming or outgoing calls. The user can either dial a feature code (\*3) to selectively enable recording for the current call, never record calls, or always record calls.

- **Outgoing**, record external outgoing calls.
- **Incoming**, record external incoming calls.
- **Internal**, record internal calls.

**On Demand Recording**, record calls on demand.

**Voicemail Enabled**, enables or disables voicemail. If voicemail is not enabled, voicemail messages cannot be left for the user.

**Voicemail Password**, the numeric password to access the voicemail. The voicemail system will compare the password entered by the user against this value. Allows you to define the voicemail password for each extension, if left blank, the password will be

the extension number. You may use the reserved word {RANDOM} to generate a random password.

**Account Code**, this field is used to populate the Account Code field of the Call Detail Record (CDR). If the field is left blank, the Account Code field of the CDR record will also be blank. Allows you to define the account code for each extension. You may use the reserved word {EXTENSION} to use the extension as account code.

**Features Password**, password to access certain system features and the control panel of the phone. Allows you to define the features password for each extension, if left blank, a random password will be generated. You may use the reserved word {EXTENSION} to use the extension as features password.

**Ring Time**, the number of seconds to ring the device before giving up and moving on to the next priority for the extension.

**NAT**, (Network Address Translation) is a technology commonly used by firewalls and routers to allow multiple devices on a LAN with 'private' IP addresses to share a single public IP address. A private IP address is an address, which can only be addressed from within the LAN, but not from the Internet outside the LAN Options:

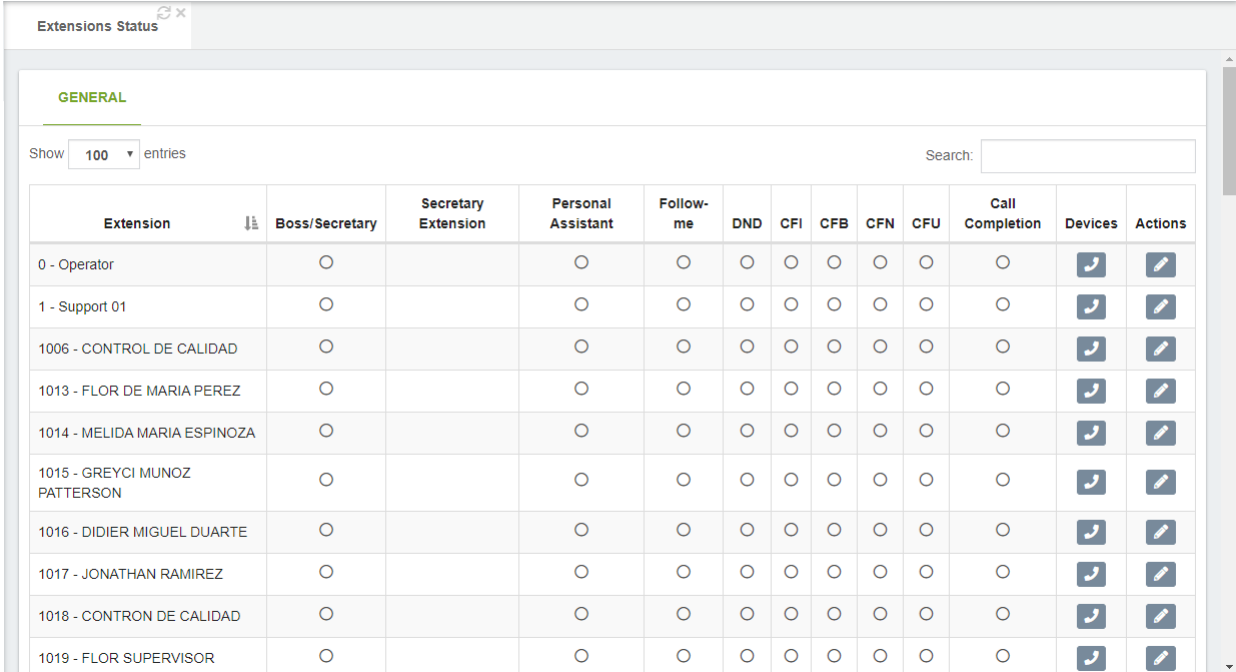
- No: No special NAT handling other than RFC3581
- Force: Pretend there was an rport parameter even if there wasn't
- Comedia: Send media to the port Asterisk received it from regardless of where the SDP says to send it.
- Auto Force: Set the force rport option if Asterisk detects NAT
- Auto Comedia: Set the comedia option if Asterisk detects NAT

**Call Waiting**, if you uncheck this option, only one incoming call will be allowed to this extension.

## 6.1.7 Extensions Status

This module shows the status of all extensions with the option to change any status by simply pressing the (✎) button that is located at the end of each line.

### General



The screenshot shows a web interface titled 'Extensions Status'. It features a 'GENERAL' tab, a 'Show 100 entries' dropdown, and a search box. Below is a table with columns for Extension, Boss/Secretary, Secretary Extension, Personal Assistant, Follow-me, DND, CFI, CFB, CFN, CFU, Call Completion, Devices, and Actions. Each row represents an extension with radio buttons for status selection and a pencil icon for editing.

Extension	Boss/Secretary	Secretary Extension	Personal Assistant	Follow-me	DND	CFI	CFB	CFN	CFU	Call Completion	Devices	Actions
0 - Operator	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
1 - Support 01	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
1006 - CONTROL DE CALIDAD	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
1013 - FLOR DE MARIA PEREZ	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
1014 - MELIDA MARIA ESPINOZA	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
1015 - GREYCI MUNOZ PATTERSON	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
1016 - DIDIER MIGUEL DUARTE	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
1017 - JONATHAN RAMIREZ	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
1018 - CONTRON DE CALIDAD	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
1019 - FLOR SUPERVISOR	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		

The dialog displays the following fields:

- Extension (number)
- Boss/Secretary (status)
- Secretary Extension (number)
- Personal Assistant (status)
- Follow-me (status)
- DND (Do Not Disturb status)
- Call Forward Immediately (CFI status)
- Call Forward Busy (CFB status)
- Call Forward No Answer (CFN status)
- Call Forward Unavailable (CFU status)
- Call Completion (status).

Use the (✎) button that is located at the end of each line to modify the status of an extension. You can modify the Personal Assistant and Diversion settings of the extension. The status can be in effect either unconditionally (by NOT selecting a time group from the time dropdown), or for a specific during the time period as defined by the time group that you select from the dropdown list, or can be effect unconditionally if no time group is selected. In addition, you can change the status by click the circle in each option.

Extension Status
✕

---

Personal Assistant

The Personal Assistant IVR will not be activated until a greeting has been recorded.

Press 1	Select Module ▾	Select Destination ▾	
Press 2	Select Module ▾	Select Destination ▾	
Press 3	Select Module ▾	Select Destination ▾	
Press 4	Select Module ▾	Select Destination ▾	
Default	Select Module ▾	Select Destination ▾	
Boss/Secretary	-- Select Time -- ▾	<input type="checkbox"/>	No
Follow-me	-- Select Time -- ▾	<input type="checkbox"/>	No
DND	-- Select Time -- ▾	<input type="checkbox"/>	No
Call Completion	-- Select Time -- ▾	<input type="checkbox"/>	No
CFI	Custom Number ▾	<input type="text" value="0558270"/>	-- Select Time - ▾ <input type="checkbox"/> No
CFB	Custom Number ▾	<input type="text" value="1"/>	-- Select Time - ▾ <input type="checkbox"/> No
CFN	Custom Number ▾	<input type="text" value="2"/>	-- Select Time - ▾ <input type="checkbox"/> No
CFU	Custom Number ▾	<input type="text" value="0"/>	-- Select Time - ▾ <input type="checkbox"/> No

Close Save

Use the ( ) button see the status of the devices associate at the extension.

Devices Info
✕

Username / Channel	Host	Port	Status	User Agent	Description
SIP/8255	10.8.2.22	5060	OK (101 ms)	Yealink SIP-T58 58.85.0.5	Rodrigo Cuadra
SIP/8255_2	(Unspecified)	0	UNKNOWN		Desktop
SIP/8255_1	(Unspecified)	0	UNKNOWN		Rodrigo Cuadra

close

## 6.2 Applications

### 6.2.1 Conferences

A conference room allows a group of people to participate in phone call. The most common form of bridge allows participants dial into a virtual meeting room from their own phone. Meeting rooms can hold dozens or even hundreds of participants. This contrasts with three-way calling, a standard feature of most phone systems which only allows a total of three participants. For most phone systems, conference bridging is an add-on feature that costs thousands of dollars.

#### General

The screenshot shows the 'Conferences' configuration page with the following settings:

- Code \***: [Empty text field]
- Description \***: [Empty text field]
- Max Members**: No Limit (dropdown)
- Video Mode**: None (dropdown)
- User PIN**: [Empty text field]
- Leader PIN**: [Empty text field]
- Language**: English (en) (dropdown)
- Record**: No (toggle)
- Settings**:
  - Join Announcement**: Default (dropdown)
  - Music on Hold**: Default (dropdown)
  - Announce User Count**: [Empty text field]
  - Class of Service**: All Permissions (dropdown)
  - Music on Hold When Empty**: Yes (toggle)
  - User Count**: No (toggle)
  - Announce Join/Leave**: No (toggle)
  - Announce Only User**: Yes (toggle)
  - Wait for Leader**: No (toggle)
  - Start Muted**: No (toggle)
  - Drop Silence**: Yes (toggle)
  - Quiet**: No (toggle)
  - Kick Users**: No (toggle)
  - Talk Detection**: No (toggle)
  - Allow to Invite**: No (toggle)

A 'Save' button is located at the bottom right of the form.

**Extension\***, number to dial to reach this service. This is a number that internal endpoints can dial to reach this conference. Like the ring groups, this can be thought of as the extension number of the conference.

**Description\***, short description for identify this conference.

**Max Members**, this option limits the number of participants for a single conference to a specific number. After the limit is reached, the conference will be locked until someone leaves. Note however that an Admin user will always be allowed to join the conference regardless if this limit is reached or not.

**Video Mode**, Options:

- None: No video sources are set by default in the conference. It is still possible for a user to be set as a video source via AMI or DTMF action at any time.

- Follow Talker: The video feed will follow whoever is talking and providing video.
- Admin: The first administrator who joins the conference with video capability is the only source of video distribution to all participants. If the administrator leaves, the next administrator to join after them becomes the source.

**User PIN\***, this is a numeric passcode that is used to enter the conference room. If a PIN is entered in this field, no one is able to join the conference room without entering the PIN.

**Admin PIN**, functions in the same way as the User PIN. The Admin PIN and User PIN should not be set to the same value. The Admin PIN is used in conjunction with the Wait Admin option explained further in this chapter, in order to identify the administrator or leader of the conference.

**Language**, here you can set the language used for voice prompts to the conference.

**Record Conference**, when set to yes, records the conference call starting when the first user enters the room, and ending when the last user exits the room.

#### Conference Settings section

**Music on Hold**, the music on hold class to use for this conference.

**Announce User Count**, used for announcing the participant count to all members of the conference. If set to a number, then the announcement is only played when the number of participants is above the set number. Available options are yes, no, or a whole number. Default is no.

**Music on Hold When Empty**, when this option is enabled on-hold music will be played if there is only one caller in the conference room or if the conference has not started yet (because the leader has not arrived). If this option is disabled, no sound will be played during these situations.

**User Count**, when this option is enabled, the number of users currently in the conference room will be announced to each caller before they are bridged into the conference.

**Announce Join/Leave**, when enabled, this option will prompt the user for a name when entering the conference. After the name is recorded, it will be played when the user enters or exits the conference.

**Announce Only User**, sets if the only user announcement should be played when a user enters an empty conference.

**Wait for Leader**, if this option is enabled, the conference will not begin until the conference administrator joins the conference room. The administrator is identified by the Admin PIN. If other callers join the conference room before the leader does, they will hear on-hold music or silence until the conference begins (what they hear depends on the MoH When Empty setting explained earlier in this section). If this option is set to "No", the callers will be bridged into the conference as soon as they call the conference room number.

**Start Muted**, when this option is enabled, all users joining the conference are initially muted.

**Drop Silence**, this option drops what Asterisk detects as silence from entering into the bridge. Enabling this option will drastically improve performance and help remove the buildup of background noise from the conference. Highly recommended for large conferences due to its performance enhancements.

**Quiet**, when this option is enabled, user introductions, enter prompts, and exit prompts are not played. There are some prompts, such as the prompt to enter a PIN number that will still be played regardless of how this option is set.

**Kick Users**, enabling this option will kick out all remaining users of the conference, after the last admin user leaves the conference.

**Talk Detection**, this option sets whether or not notifications of when a user begins and ends talking should be sent out as events over AMI.

**Allow to Invite**, if enabled, all the participants could press “\*\*” or “0” to invite other people to this conference.

The following codes can be entered by all conference participants:

**\*1** – toggles mute for the user. When enabled, anything the user says is not transmitted to the rest of conference members. If the conference is being recorded, anything said by a muted user is not part of the recording.

**\*4** - decreases receive volume. The user can tap this option to decrease the volume of what they are hearing. This does not affect what any other conference member hears. If a user is finding other conference members too loud, they can press \*4 a few times to make the conference quieter for themselves.

**\*5** - increases receive volume. The user can tap this option to increase the volume of what they are hearing. This does not affect what any other conference member hears. If a user is having trouble hearing other members of the conference, they can press \*5 a few times to make the conference louder for themselves.

**\*6** - decreases transmit volume. The user can tap this option to decrease the volume of what they are transmitting to the rest of the conference members. When this option is used, the user will sound quieter to all other conference members. If a user is much louder than the other members of a conference room, they can tap \*6 few times to make their transmit volume quieter.

**\*7** - increases transmit volume. The user can tap this option to increase the volume of what they are transmitting to the rest of the conference members. When this option is used, the user will sound louder to all other conference members. If the conference members are having trouble hearing a particular user, that user can tap \*7 a few times to make their transmit volume louder.

**\*8** – user can tap this code to leave the conference.

In addition, the admin has access to additional codes:

**\*2** - toggles the conference lock. When a conference is locked, no more callers may join. A locked conference must be unlocked for any new users to join. This option is

only available to a conference administrator. If the conference does not have an admin PIN configured or the user has joined the conference as a user instead of an admin, this option is not available.

**\*3** - Kicks the last user who joined the conference from the conference room. The user will hear a message informing them that they have been kicked from the conference and that their call will be terminated. Note that if a conference is unlocked, the user may rejoin. The best way to remove an abusive conference user is to eject them and then immediately lock the conference. This option is only available to a conference administrator. If the conference does not have an admin PIN configured, or the user has joined the conference as a user.

## 6.2.2 Custom Applications

This module allows you to call modules that have no extension number, such as pre-announcement, Time Condition, IVR, etc. A custom application is a custom feature code. A custom application allows a custom extension or star code to be defined, which will direct the caller to any call target when dialed. For example, if we have a ring group that calls the cell phones of all staff members, we might create a custom application that calls that ring group when \*CELL (\*2355) is dialed.

**General**

Custom Applications

**GENERAL**

Code \*

Name \*

Enabled  Yes

Destination \*

Select Module  Select Destination

**Code \***, number to dial to reach this service.

**Name\***, short description to identify this custom application.

**Enabled**, enable or disable this custom application. If disabled, then users will be informed that the extension they dialed is not valid if they attempt to use the custom application. This field allows a custom application to be quickly disabled without having to remove the application entirely.



### Destination\* section


**Select Module**, allows to choose from a drop-down list of available modules, which module should be activated.


**Select Destination**, this is the call target to which the module should be routed. Any call target that has been previously configured is a valid destination for a custom application.

## 6.2.3 Custom Destinations

A custom destination is used to add a custom call target that can be used by VitalPBX dialogs. Anything that can be dialed from a user's extension can be turned into a custom destination. For example, by default, there is no way to send an inbound caller directly to the messaging center so that the caller could log in and check their voicemail messages. For example, A custom destination could be set up to dial \*98 and then an inbound route could point directly to that custom destination. A caller who was routed through that inbound route would immediately hear the prompts to log into their voicemail box, just as if they were a user on the PBX and had dialed \*98.

General


Custom Destinations 

**GENERAL** 

Description \*

Number to Dial \*

Class of Service \* All Permissions ▼

 Save

**Description\***, is used to identify this destination when it is being selected as a call target in other dialogs.

**Number to Dial\***, is the extension, telephone number, or feature code that the system should dial when a caller is routed to this destination. Anything that can be dialed from a user's extension can be entered into this field.

**Class of Service\***, Class of Service to search the number to dial.

## 6.2.4 Custom Context

Allows the integration of personalized contexts, especially useful for advanced users.

**Description\***, a short description to identify this custom context.

**Context\***, name of the custom context created by yourself.

**Extension**, the extension defined in your custom context.

**Priority**, the priority defined in your custom context.

**Destination**, destination after having executed the custom context.

## 6.2.5 Feature Codes

VitalPBX includes all the telephony features currently available in all Asterisk distributions plus features that until now were only available in expensive, commercial PBX systems.

### Blacklist Section

Prompts the user to enter a telephone number. The entered number is then added to the user's blacklist. Inbound calls will not ring an extension if they are on that extension's blacklist. Blacklisted callers will be told that the number they dialed is no longer in service. This option is very popular as it allows users to block unwanted numbers.

#### Blacklist

Blacklist a Number	<input type="text" value="*30"/>	<input checked="" type="radio"/> Default <input type="radio"/> Custom	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Remove Number From Blacklist	<input type="text" value="*31"/>	<input checked="" type="radio"/> Default <input type="radio"/> Custom	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Blacklist Last Caller	<input type="text" value="*32"/>	<input checked="" type="radio"/> Default <input type="radio"/> Custom	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

**\*30 - Add Number to Blacklist**, prompts the user to enter a telephone number. The entered number is then added to the user's blacklist. Inbound calls will not ring an extension if they are on that extension's blacklist. Blacklisted callers will be told that the number they dialed is no longer in service.

**\*31 - Remove Number from Blacklist**, prompts the user to enter a telephone number. The entered number is removed from the user's blacklist.

**\*32 - Add Last Caller to Blacklist**, adds the last number that called the user to the blacklist.

## Business Services section

Here we can find the following feature codes:

### Business Services

Wakeup Call	*34	Default	Custom	Enabled	Disabled
Remote Wakeup Call	*35	Default	Custom	Enabled	Disabled
Speak Last Number	*37	Default	Custom	Enabled	Disabled
Reminder	*38	Default	Custom	Enabled	Disabled

**\*34 - Wakeup Call**, set up a reminder or wakeup call for the current extension.

**\*35 - Remote Wakeup Call**, create a reminder or wakeup call for another extension.

**\*36 - Boss/Secretary**, this functionality is used to re-route all incoming calls for the boss phone to the secretary phone. Only the secretary is allowed to call the boss phone directly.

**\*37 - Speak Last Number**, says the last number that called the current extension, with the possibility to press a button to call back to the original caller.

**\*38 - Reminder**, records a message. You can configure in how many minutes you want to hear the recording. When the set time expires, you will receive a call to your extension and the recording will be played.

## Call Completion Section

Call Completion Supplementary Services (often abbreviated "CCSS" or simply "CC") allows a caller to let VitalPBX automatically alert him when a called party has become available, given that a previous call to that party failed for some reason. The two services offered are Call Completion on Busy Subscriber (CCBS) and Call Completion on No Response (CCNR). To illustrate, let's say that Alice attempts to call Bob. Bob is currently on a phone call with Carol, though, so Alice hears a busy signal. In this situation, assuming that Asterisk has been configured to allow for such activity, Alice would be able to request CCBS. Once Bob has finished his phone call, Alice will be alerted. Alice can then attempt to call Bob again.

## Call Completion (CCSS)

Call Completion - Toggle	*40	Default	Custom	Enabled	Disabled
Cancel Call Completion	*41	Default	Custom	Enabled	Disabled

**\*40 - Call Completion**, to activate a call to a previously unresponsive extension when that extension become reachable.

**\*41 - Cancel Call Completion**

## Call Center section

Call centers are special offices that are purpose-built to handle a large volume of phone calls. Call centers typically handle customer service, support, telemarketing, billing and collection functions. The employees who staff call centers are referred to as “agents” or “customer service representatives”. Call centers range from very small informal operations to quite large, highly optimized sites with hundreds of agents. This group of feature codes allows us to interact with various features directly from the phone:

### Call Center

Add/Remove Queue Agent	*50	Default	Custom	Enabled	Disabled
Pause/Unpause Queue Agent	*51	Default	Custom	Enabled	Disabled
Queues Login/Logout	*52	Default	Custom	Enabled	Disabled
Queues Pause/Unpause	*53	Default	Custom	Enabled	Disabled
Spy on Extension In Barge Mode	*54	Default	Custom	Enabled	Disabled
Spy on Extension	*55	Default	Custom	Enabled	Disabled
Spy on Extension In Whisper Mode	*56	Default	Custom	Enabled	Disabled
Spy Random Channels	*57	Default	Custom	Enabled	Disabled

**\*50 - Add/Remove Queue Agent**, Add/Remove an Agent to a specific queue.

**\*51 - Pause/Unpause Queue Agent**, Pause/Unpause an Agent to a specific queue.

**\*52 - Queues Login/Logout**, Add/Remove an Agent to all queue that agent belong to.

**\*53 - Queues Pause/Unpause**, Pause/Unpause an Agent to all queue that agent belong to.

**\*54 - Spy on Extension in Barge Mode**, this will create a three-way conference between the client, the agent, and the user barging in.

**\*55 - Spy on Extension**, spy on a specified extension.

**\*56 - Spy on Extension in Whisper Mode (Coaching)**, spy on a specified extension in whisper mode.

**\*57 - Spy Random Channels**, spy on random channels.

## Call Forward section

### Call Forward (CF)

Boss/Secretary - Toggle	*36	Default Custom	Enabled Disabled
Call Forward Immediately - Toggle	*58	Default Custom	Enabled Disabled
Set CF Immediately Number	*59	Default Custom	Enabled Disabled
Call Forward Unavailable - Toggle	*60	Default Custom	Enabled Disabled
Set CF Unavailable Number	*61	Default Custom	Enabled Disabled
Call Forward Busy - Toggle	*62	Default Custom	Enabled Disabled
Set CF Busy Number	*63	Default Custom	Enabled Disabled
Call Forward On No Answer - Toggle	*64	Default Custom	Enabled Disabled
Set CF On No Answer Number	*65	Default Custom	Enabled Disabled
Do Not Disturb - Toggle	*66	Default Custom	Enabled Disabled
Follow Me - Toggle	*67	Default Custom	Enabled Disabled
Clear all Diversions	*69	Default Custom	Enabled Disabled
Personal Assistant - Toggle	*96	Default Custom	Enabled Disabled

The group of call forwarding provides the following options:

- \*36 - Boss/Secretary – Toggle**, enable or disable call forwarding from the boss to the secretary.
- \*58 - Call Forward Immediately**, enable or disable call forwarding.
- \*59 - Set CF Immediately Number**, set the number to which diverted calls should be sent.
- \*60 - Call Forward Unavailable**, enable or disable call forwarding.
- \*61 - Set CF Unavailable Number**, set the number to which diverted calls should be sent.
- \*62 - Call Forward Busy**, enable or disable call forwarding when your extension is busy.
- \*63 - Set CF Busy Number**, set the number to which diverted calls should be sent.
- \*64 - Call Forward on No Answer**, enable or disable call forwarding when your extension does not answer incoming calls.
- \*65 - Set CF On No Answer Number**, set the number to which diverted calls should be sent.
- \*66 - Do Not Disturb**, enable or disable Do Not Disturb.
- \*67 - Follow Me**, enable or disable Follow Me.
- \*69 - Clear all Diversions**, disable all diversions.
- \*96 - Personal Assistant – Toggle**, enable or disables the Personal Assistant for the extension.

## On Call Features section

### On Call Features

Disconnect Call	<input type="text" value="*0"/>	<input checked="" type="radio"/> Default <input type="radio"/> Custom	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Direct Pickup	<input type="text" value="*07"/>	<input checked="" type="radio"/> Default <input type="radio"/> Custom	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Pickup Group	<input type="text" value="*08"/>	<input checked="" type="radio"/> Default <input type="radio"/> Custom	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Attended Transfer	<input type="text" value="*2"/>		
One Touch Recording	<input type="text" value="*3"/>		
Park Call	<input type="text" value="*4"/>		
Blind Transfer	<input type="text" value="#1"/>		

These facilities are used when you are on a call:

- \*0 - Disconnect Call**, disconnect the current call.
- \*07 - Direct Pickup**, remotely capture a call that is ringing at another extension.
- \*08 - Pickup Group**, captures any call that is ringing the group that belongs to the extension if it has the right permission. To use this facility is necessary to create a pickup.
- \*2 - Attended Transfer**, transfer the current call with notifying the extension to which the call will be transferred.
- \*3 - One Touch Recording**, forces the call to be recorded.
- \*4 - Park Call**, call parking.
- #1 - Blind Transfer**, transfer the current call without notifying the extension to which the call will be transferred.

## Phonebook Directory Section

This directory is completely linked to extensions that have voice mail, with which they create a name and the full name of the person is recorded to listen when there is a match when the user will type the first few letters of the name or last name.

### Phonebook Directory

Dial By Name Directory	<input type="text" value="411"/>	<input checked="" type="radio"/> Default <input type="radio"/> Custom	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
------------------------	----------------------------------	---	---

**411 - Dial by Name Directory**

## Test Services section

### Test Services

Speak Date and Time	*70	Default	Custom	Enabled	Disabled
Speak Your Extension Number	*71	Default	Custom	Enabled	Disabled
Echo Test	*72	Default	Custom	Enabled	Disabled
Simulate Incoming Call	*73	Default	Custom	Enabled	Disabled

These are a group of features in order to test the system.

- \*70 - Speak Date and Time**, Listen to the current date and time.
- \*71 - Speak Your Extension Number**, you can hear your extension number.
- \*72 - Echo Test**, an echo test system to measure the response time.
- \*73 - Simulate Incoming Call**, simulation of an incoming call to test ringing of the phone.

## Special Features Section

### Special Features

Lock/Unlock Phone	*75	Default	Custom	Enabled	Disabled
Change Features Password	*76	Default	Custom	Enabled	Disabled
Remote Substitution	*77	Default	Custom	Enabled	Disabled
Customer Code	*78	Default	Custom	Enabled	Disabled
Authorization Code	*79	Default	Custom	Enabled	Disabled
Hot Desking	*80	Default	Custom	Enabled	Disabled
Night Mode All	*81	Default	Custom	Enabled	Disabled
Paging	*82	Default	Custom	Enabled	Disabled

This is a group of features which are described below:

- \*75 - Lock/Unlock Phone**, lock and unlock the current extension.
- \*76 - Change Features Password**, change the password to access to certain telephone facilities.
- \*77 - Remote Substitution**, makes it possible for a remote phone to make calls as if you are on your own phone.
- \*78 - Account Code**, CDR assigned to an account code, very useful for call accounting.
- \*79 - Authorization Code**, from any phone you can make a call using a code that is associated with unrestricted dial plan.
- \*80 - Hot Desking**, assign an extension number to a hot desking device type.
- \*81 - Night Mode All**, change the state of all-night mode.

**\*82 - Paging**, places an outgoing call from the given extension, and returns the call on conference as a muted participant, e.g. 827000. The feature must be enabled in the Feature Category associated with the extension.

## Recording & Announcements Section

This group of feature codes allows you to interact with your voice mail and other similar applications.

### Recordings & Announcements

Custom Recording	*92	Default	Custom	Enabled	Disabled
Dictation	*93	Default	Custom	Enabled	Disabled
Record Msg For Personal Assistant	*94	Default	Custom	Enabled	Disabled
Send Voicemail Message	*95	Default	Custom	Enabled	Disabled
Direct Voicemail	*97	Default	Custom	Enabled	Disabled
Remote Voicemail	*98	Default	Custom	Enabled	Disabled

\*92 - Custom Recording, records a message.

\*93 - Dictation Services, records a message with the option of sending it by email.

\*94 - Record Msg for Personal Assistant, records a message that callers will hear when they are served by the personal assistant.

\*95 - Send Voicemail Message, allows you to dial any extension and leave a voicemail. For example, when dialing \*95\*2492, you can leave a voicemail message to extension 2492. The feature must be enabled on the Feature Category associated to the extension.

\*97 - Direct Voicemail, direct entry to the voicemail system – requires password.

\*98 - Remote Voicemail, remote entry to the voicemail – requires both extension number and password.



## 6.2.6 Paging & Intercom

This module creates hunt groups to which they were able to send a message marked a number. It can also be used to create an intercom between 2 extensions.

### General

The screenshot shows the 'Paging & Intercom' configuration page. The 'GENERAL' tab is selected. The form includes the following fields and controls:

- Code\***: Text input field.
- Description\***: Text input field.
- Extensions**: Text input field with a list icon.
- Announcement**: Dropdown menu set to 'None' with a speaker icon.
- Timeout**: Dropdown menu set to '15 Seconds'.
- Mode**: Dropdown menu set to 'Default'.
- Duplex Audio**: Toggle switch set to 'No'.
- Ignore Forward Call**: Toggle switch set to 'Yes'.
- Quiet Mode**: Toggle switch set to 'Yes'.
- Record Paging**: Toggle switch set to 'No'.
- Skip Busy**: Toggle switch set to 'No'.
- MulticastRTP** section:
  - IP Address**: Text input field containing '224.0.1.120'.
  - Port**: Text input field containing '1234'.
  - Add**: Green button to add the MulticastRTP entry.
- Save**: Green button at the bottom right.

**Code\***, number to reach this service.

**Description\***, short description to identify this paging group.

**Extensions\***, list of the extension(s) to dial.

**Announcement\***, announcement to be played to all paged participants.

**Timeout**, this specifies the length of time that the system will attempt to connect a call. After this duration, any intercom calls that have not been answered will be hung up by the system.

**Mode**, it allows you to define the paging behavior, Options:

- Default: Default behavior. Plays the announcement if defined and then allows to the caller continue speaking
- Announcement Only: Plays the announcement and then hang up.

**Duplex Audio**, sometimes referred to as "talkback paging." The use of this option implies that the equipment that receives the page has the ability to transmit audio back at the same time as it is receiving audio. Generally, you would not want to use this unless you had a specific need for it.

**Ignore Forward Call**, ignore attempts to forward the call.

**Quiet Mode**, it does not play a beep to caller.

**Record Paging**, this allows you to record the page message into a file.

**Skip Busy**, dials a channel only if the device state is NOT\_INUSE. This option is likely only useful (and reliable) on SIP-bound channels, and even so may not work if a single line is allowed multiple calls on it.

## Schedule

It is possible to schedule paging actions and play an announcement. This is quite useful for schools (bell system), automation announcements on the office, airports, train stations, etc.

The capability to schedule paging items has been added. This new feature comes as an add-on.

The options to configure are the following:

**Enabled**, enable or disable the execution of the scheduled payment

**Time**, time to execute paging

**Start Day**, initial day to execute the paging

**End Day**, final day to execute the paging

**Excluded Dates**, the dates listed are excluded from the paging execution schedule

**Month**, month to exclude

**Day of Month**, day of the month to exclude

**Description**, brief description to remember why that date is being excluded.

## MulticastRTP

Multicast Paging allows you to send pages to groups of phones directly, without the PBX being involved in the page. With multicast paging, phones are programmed to listen to a broadcast address. The advantage to this method is that the multicast

page is a single SIP call instead of a multiple-party conference call. This greatly reduces the workload placed on the PBX, especially when a large number of devices are involved.

All phones that you want to include in the multicast paging group need to be on the same network, since a network broadcast protocol is used.

**IP Address**, the multicast IP address that the station shall listen to, e.g. 224.0.1.120. Multicast IP addresses are in the range from 224.0.0.0 to 239.255.255.255.

**Port**, the multicast Port number that the station shall listen to.

## Multicast RTP Phone Configuration

## Examples

### Yealink

**Multicast Listening**

Paging Barge: 10

Ignore DND: Disabled

Paging Priority Active: Enabled

IP Address	Listening Address	Label	Channel	Priority
1 IP Address	224.0.1.116:60000	Sales	0	1
2 IP Address			0	2
3 IP Address			0	3
4 IP Address			0	4
5 IP Address			0	5
6 IP Address			0	6
7 IP Address			0	7
8 IP Address			0	8
9 IP Address			0	9
10 IP Address			0	10

**NOTE**  
**Multicast Paging**  
 Multicast paging allows IP phones to send/receive Real-time Transport Protocol (RTP) streams to/from the pre-configured multicast address(es) without SIP signaling. Up to 10 listening multicast addresses can be specified on the IP phone.  
 Click here to get more product documents.

## Grandstream

The screenshot shows the Grandstream GXP2140 web interface. At the top, there is a navigation bar with 'Admin Logout | Reboot | Provision | Factory Reset' and a language dropdown set to 'English'. Below this is the Grandstream logo and a menu with 'STATUS', 'ACCOUNTS', 'SETTINGS', 'NETWORK', 'MAINTENANCE', and 'PHONEBOOK'. A version indicator 'Version 1.0.5.23' is on the right. The left sidebar contains a 'Settings' menu with options like 'General Settings', 'Call Features', 'Multicast Paging', 'Ring Tone', 'Audio Control', 'LCD Display', 'LED Control', 'Date and Time', 'Web Service', 'XML Applications', 'Programmable Keys', 'Extension Boards', 'EXT 1-4', 'Broadsoft', 'Broadsoft XSI', and 'Broadsoft IM&P'. The main content area is titled 'Multicast Paging' and includes the following settings:

- Paging Barge: Disabled
- Paging Priority Active:  Disabled  Enabled
- Multicast Paging Codec: PCMA

Below these settings is the 'Multicast Listening' section, which contains a table with 10 rows. The first row is populated with the following data:

Priority	Listening Address	Label
1	224.0.1.118:60000	Sales
2		
3		
4		
5		
6		
7		
8		
9		
10		

At the bottom of the configuration area are three buttons: 'Save', 'Save and Apply', and 'Reset'. A footer at the very bottom of the page reads 'Copyright © Grandstream Networks, Inc. 2018. All Rights Reserved.'

## 6.2.7 Pickup Groups

Pickup Group specifies to which pickup groups an extension belongs. An extension can belong to multiple pickup groups. The call group and pickup group options allow users to pick up calls that are not directed to them by dialing a feature code (\*08). Calls directed to any phone in a particular call group can be answered by any user who is a member of the corresponding pickup group. For example, a user in pickup group Support will be able to pick up any call directed to any phone in the Support call group. This can be useful for small office or home setups, where it is easier to simply pick up a call from another phone rather than forward that call to another extension. Note that a user can be part of a pickup group without being a member of the associated call group. For example, a senior staff member may be able to pick up any call directed to anyone in his department, but his department should not be able to pick up calls directed to the senior staff member.

### General

**Pickup Groups**

**GENERAL**

Description \*

Extension \*

Extension	Member	Allow Pickup	
<input type="text" value="7500 - Jose Rivera"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="text" value="3801 - Antonio Desk"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="text" value="3807 - BRIA Marcia"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

**Description\***, a description to identify the pickup group, can consist of numbers and names.

#### Extension Section

**Extension**, any extension that you want to add to this group.

**Member**, when enabled, indicates that the extension is a member of the pickup group.

**Allow Pickup**, when enabled, indicates that this extension can pick up calls that are directed to this group.

## 6.2.8 Parking

The Call Parking feature allows you to place a caller on hold and then retrieve them from any phone, anywhere on the system.

### General

The screenshot shows the 'Parking' configuration page in VitalPBX. The 'GENERAL' tab is active. The form contains the following fields and values:

- Code \*: 700
- Parking Positions: 701-710
- Description \*: Default Parking
- Parking Positions: 10
- Parking Time: 45
- Comeback Dial Time: 20
- Courtesy Tone: Caller
- Music on Hold: None (Ringback)
- Call Transfer: No
- Call Reparking: No
- Call Hangup: No
- Find Slot: First
- Return to Originator: Yes
- Announce Space Number: Yes
- Timeout Destination \*: Terminate Call, Hangup

At the bottom right, there are three buttons: Update (green), Delete (red), and Cancel (blue).

**Code\***, number to reach this service.

**Description\***, short Description to identify this parking.

**Parking Positions**, number of parking spaces to use.

**Parking TimeOut\***, number of seconds a call can be parked before being returned.

**Comeback DialTime\***, when a parked call times out, this is the number of seconds to dial the device that originally parked the call.

**Courtesy Tone**, to whom to play the courtesy tone while waiting for someone to pick up the parked call. Options are:

- No one
- Caller
- Callee
- Both

**Music on Hold**, this is the MoH class to use for the parked channel.

**Call Transfer**, enables or disables DTMF based transfers when picking up a parked call.

**Call Re-Parking**, enables or disables DTMF based parking when picking up a parked call.

**Call Hang up**, enables or disables DTMF based hang up when picking up a parked call.

**Find Slot**, sets the method for selecting parking spaces when a call is parked. Options are:

- First: use the lowest numbered parking space available
- Next: use the next parking space from the most recently used one.

**Return to Origin**, setting this option configures the behavior of call parking when the parked call times out

**Announce Space Number**, if set to no, the announcement of the parking space number will be silenced.

### Timeout Destination section

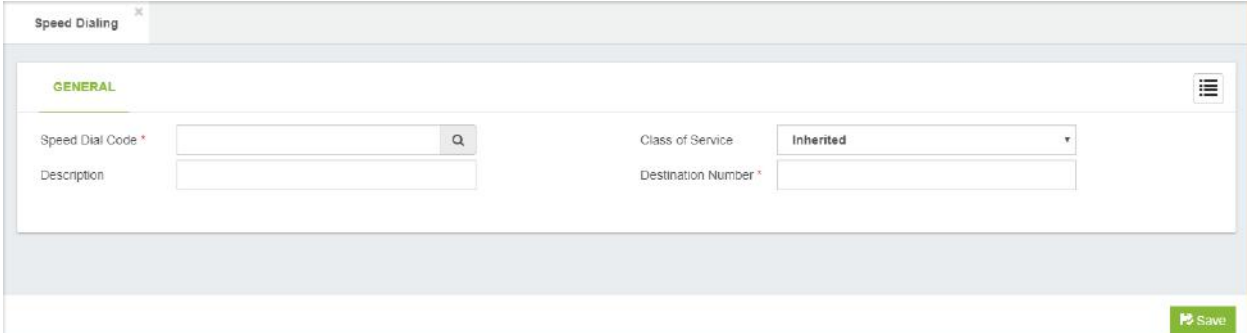
**Select Module**, select the module to used when a parked call timed out.

**Select Destination**, destination for a parked called that has timed out.

## 6.2.9 Speed Dialing

This feature which permits fast dialing of frequently used numbers. Sometimes there are long numbers we want to abbreviate a short dialing.

### General



The screenshot shows a web-based configuration form for Speed Dialing. The form is titled "Speed Dialing" and has a "GENERAL" section. It contains the following fields:

Speed Dial Code *	<input type="text"/>	Class of Service	Inherited
Description	<input type="text"/>	Destination Number *	<input type="text"/>

At the bottom right of the form is a green "Save" button.

**Speed Dial Code\***, number to access the speed dial. This number must be unique.

**Description\***, short Description to identify this Speed Dial.

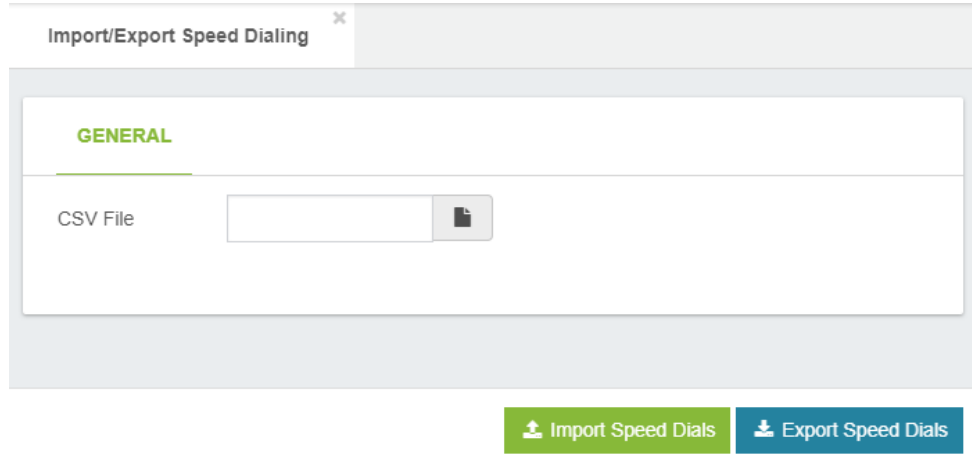
**Class of Service**, class of service to use for dialling this speed dial.

**Dial Number\***, the number that will be dialed by this speed dial.

## 6.2.10 Import/Export Speed Dialing

Import/Export Speed Dialing to/from CSV file.

### General



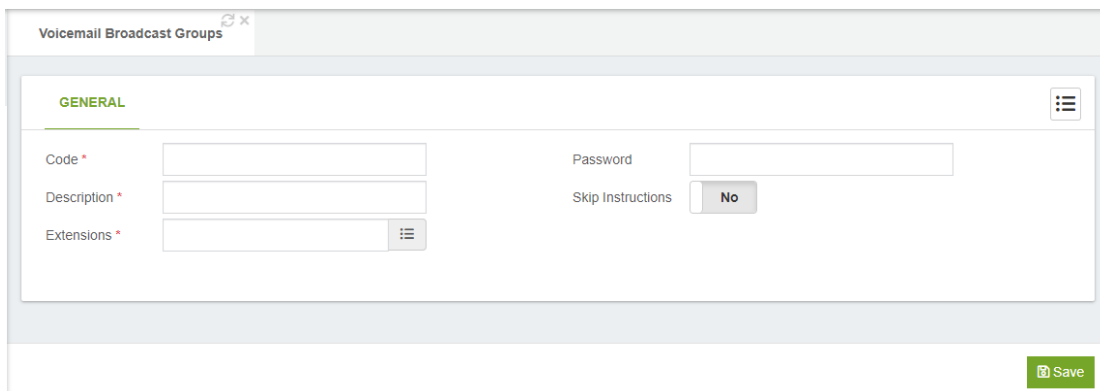
An example of the file format can be download by press the “Download Import Format” button at the bottom of the screen. The first row is for the header.

	A	B	C	D	E
1	mode	speeddial	dest_number	description	class_of_service
2	add	*6969	8264	test	
3					

## 6.2.11 Voicemail Broadcast Group

Extension Group to which voicemail can be sent.

### General



**Code\***, number to dial to send broadcast voicemail



**Description\***, short Description to identify this Voicemail Broadcast Group

**Extensions\***, list of extensions for mass-mailing voicemail. Note that you can only see the extensions that have active voicemail.

**Password\***, password to protect this Voicemail Broadcast Group

**Skip Instructions**, if enabled, skips the playback of instructions for leaving a message to the listed extensions on this VM group.

## 6.2.12 Call Back

Callback is a call target that will immediately hang up on a caller, call them back, and then redirect the call to another call target. This is most often used to avoid long-distance charges for remote agents who do not have access to a VoIP endpoint. This is especially relevant in the case of mobile phones where incoming calls are usually significantly cheaper than outgoing calls. The callback target may connect the caller with any resource on VitalPBX (such as an extension, the voicemail messaging center, or a queue), or it may be used in conjunction with DISA to give the caller a dial tone on the system from which they can call any telephone number they wish.

### General

The screenshot shows the 'Call Back' configuration page in the VitalPBX interface. The 'GENERAL' tab is selected. The form contains the following fields:

- Description \***: A text input field.
- Number**: A text input field.
- Dial Prefix**: A text input field.
- Delay**: A text input field with the value '5'.
- Class of Service**: A dropdown menu with 'All Permissions' selected.
- Destination \***: A section containing two dropdown menus: 'Select Module' and 'Select Destination'.

A green 'Save' button is located at the bottom right of the form.

**Description\***, short Description to identify this callback.

**Number**, this is the phone number that VitalPBX will dial to reconnect with the caller after the call that initiated the callback is terminated. The number must be in a format that one of the outbound routes configured in the Outbound Routes section of VitalPBX can be matched with (for example, if there is no outbound route defined to match a 10-digit dialing pattern, entering 5551234567 for this field would render the callback configuration useless, as the outbound callback would never be completed). If the field is left blank, then VitalPBX will attempt to call back the caller ID number that initiated the callback.

**Dial Prefix**, this prepends the prefix to the number to dial.

**Delay**, delay before return call.

**Class of Service**, Class of Service for making the call.

### Destination\* Section

**Select Module**, to choose which module should be activated.

**Select Destination**, to configure the call target that the caller will be connected to, once the callback dialog reconnects the caller to VitalPBX. Any existing call target can be used.

A few common examples of when a callback target might be used are as follows:

A company where employees need the ability to check their voicemail from anywhere. Calling the toll-free company phone number costs the company too much money. A callback target could be set up to call back the incoming caller ID and be directed to the miscellaneous destination of \*98. Callers would receive a call on the number they called from, would be prompted for their extension and their password, and would then have access to their voicemail messages.

A company receives better per-minute rates on calls made through its VoIP trunks than calls made through employees' mobile phones. Employees' mobile phones have free incoming calls. A callback target could be set up for each employee with a mobile phone to call back the employee's mobile number. The callback would be directed to a DISA destination to give the employee a dial tone on the PBX (allowing them to dial out using the company's VoIP trunks without using any outgoing mobile minutes).

A company that receives collect calls from anywhere in the world (such as a credit card company that needs to receive calls if a customer's card is lost or stolen). The company reduces their costs if they use a VoIP trunk local to the country that the customer is in, rather than paying for the entire collect call at hefty international rates. A callback target could be set up to call back the incoming caller ID of the customer and be directed to a queue. The customer would receive a call to the number they called from and would be connected with a company representative as soon as one is available.

## 6.2.13 DISA

DISA allows you to create a destination that allows people to call in to from an outside line and reach the system dial tone. This is useful if you want people to be able to take advantage of the low rate for international calls that you have available on your system, or to allow outside callers to be able to use the paging or intercom features of the system. Always protect this feature with a strong password.

A DISA call target will provide a caller with a dial tone on VitalPBX. Once the caller has a dial tone, they can utilize the same set of functions that are utilized by a user with VoIP endpoint attached to VitalPBX. This means that a person who is remotely located could be given access to dial any extension directly, check their voicemail messages, or even place calls to external telephone numbers through VitalPBX.

### General

The screenshot shows the 'DISA' configuration page with the 'GENERAL' tab selected. The form contains the following fields:

- Description \***: An empty text input field.
- Password \***: A text input field containing the value '72732'.
- Class of Service**: A dropdown menu currently set to 'All Permissions'.
- Caller ID**: A section with two sub-fields: 'Name' (empty) and 'Number' (empty).
- Response Timeout**: A text input field containing the value '10'.
- Digit Timeout**: A text input field containing the value '5'.

A green 'Save' button is located at the bottom right of the form.

**Description\***, short description for identify this DISA when it is being selected as a call target in other parts of the VitalPBX interface.

**Password**, this is used to authenticate a caller when they want to activate DISA feature. If the password field contains a value, then the caller will be prompted to enter the password. The password that the user enters must match the value of the password field, otherwise the call will be disconnected, and the caller will not be able to access the DISA feature.

**Class of Service**, this specifies the dial plan context in which the user-entered extension will be matched.

**Caller ID**, this is used to set the outbound caller ID, consisting of two parts: the CID Name and the CID Number. This will define the caller ID text that is displayed when this user calls other. This is an optional field. If this field is left blank, then the caller ID of the person placing the call will be used.

**Response Timeout**, this specifies how long VitalPBX will wait for valid input before disconnecting the call. This not only applies when a caller has not entered any digit yet, but also if a caller has partially entered a number to call without finishing the entry. The default value for this field is 10 seconds.

**Digit Timeout**, this specifies how long VitalPBX will wait between digits before dialing the call. If a caller begins entering digits and then stops, VitalPBX will wait for

the number of seconds specified in this field, before sending the entered digits to VitalPBX for dialing. The default value for this field is five seconds. This is usually sufficient as most people do not take more than five seconds between button pushes on their phone once they have started dialing.

## 6.2.14 PIN List

List of PIN that is associated with an outgoing trunk. Any extension that want to make a call you will be asked for a PIN number.

General

PIN Lists ✕

GENERAL
☰

Description \*

Q

PIN List

Save

**Description\***, this is a short description for this PIN List.

**Pin List\***, here you set the PIN List for this record (If you want to add more than one pin do it in a new line). You can only introduce numbers and the characters \* and #.

## 6.2.15 Dynamic Destinations

With this add-on, you are able to dynamically route the calls based on the DID. You are able to perform a query to a database or API, and depending on the response, route the number to a specific destination.

Here are the different options that can be configured.

### For MySQL Source Type

**Description**, a brief description for this Dynamic Destination.

**Database**, MySQL database to query.

**Query**, Query to perform. The special token [CIDNUM] will be replaced by the CID number of the calling party, for example, `SELECT 'VIP_CUSTOMER'; as `response` FROM `customers` WHERE `number` = '[CIDNUM]'`

**Default Destination**, destination to use in case we receive an un-defined answer, or not taken into consideration for the destinations configured.

**Host**, IP address or hostname for the server where the MySQL database is located at.

**Username**, database username used to perform the query.

**Password**, database user password used to perform the query.

### For URL Source Type

**Description**, a brief description for this Dynamic Destination.

**Host**, IP address or hostname for the server where the script is located at.

**Path**, name of the script to execute.

**Query String**, Series of parameters that will be sent as part of the script. The special argument [CIDNUM] will be replaced with the CID number of the calling party. For example, “*caller\_num=[CIDNUM]&ctype=vip*”

**Default Destination**, destination to use in case we receive an un-defined answer, or not taken into consideration for the destinations configured.

**Port**, port used to perform the request. Normally 80 for HTTP, and 443 for HTTPS.

**Auth User**, user to authenticate the HTTP/HTTPS request.

**Auth Password**, Password used to authenticate the HTTP/HTTPS request.

**Secure**, if enabled, the request will be sent through HTTPS, else it will be sent through HTTP.

### Destinations

**Response**, the expected response from the query.

**Destination**, the destination to which we route the call to.

**Enabled**, enable or disable the routing based on the response.

## 6.3 Class of Service

### 6.3.1 Class of Service

Class of Service is a Group of settings that define the dial plan that has access to the extension.

#### General

The screenshot shows the 'Class of Service' configuration page with the 'GENERAL' tab selected. The form contains the following fields and options:

- Class of Service \***: A text input field.
- Description \***: A text input field.
- Feature Category**: A dropdown menu with 'All Features' selected.
- Dial Restrictions**: A dropdown menu with 'No Dial Restrictions' selected.
- Route Selection**: A dropdown menu with '-- All Outbound Routes --' selected.
- Allowed Calls By**: A dropdown menu with a list icon.
- Private**: A radio button with the label 'No' selected.

A green 'Save' button is located at the bottom right of the form.

**Class of Service \***, Class of Service Name (Must be Unique). Alphanumeric values with dash and underscore are allowed.

**Description \***, this is a short Description for identify this Class of Service.

**Feature Category**, features allowed for this Class of Service.

**Dial Restrictions**, dial restriction rules set for this Class of Service.

**Route Selection**, routes to use for this Class of Service.

**Allowed Calls By**, it defines the list of CoS to be allowed to call to this CoS when Private field is checked.

**Private**, it defines if extensions with this CoS may be called by others with different CoS. If is checked only calls with the same CoS or calls coming from CoS selected on Allowed Calls By field will be allowed. It applies for internal calls only.

## 6.3.2 Feature Categories

In this module you can create groups of feature codes. This allows you to prevent some users from having access to some of the more sensitive feature codes.

### General

The screenshot shows the 'Feature Categories' configuration page in the 'GENERAL' tab. At the top, there is a 'Description \*' field. Below it, the page is divided into two main sections: 'Available Features' and 'Enabled Features'. The 'Available Features' section has an 'Add all' button and a list of feature codes with plus signs next to them. The 'Enabled Features' section has a 'Remove all' button and is currently empty. A 'Save' button is located at the bottom right of the form.

Available Features	Enabled Features
<input type="button" value="Add all"/>	<input type="button" value="Remove all"/>
# 1 - Blind Transfer	
*0 - Disconnect Call	
*07 - Direct Pickup	
*08 - Pickup Group	
*2 - Attended Transfer	
*3 - One Touch Recording	
*4 - Park Call	
*30 - Blacklist a Number	
*31 - Remove Number From Blacklist	
*32 - Blacklist Last Caller	
*34 - Wakeup Call	
*35 - Remote Wakeup Call	
*36 - Boss/Secretary - Toggle	
*37 - Speak Last Number	

**Description\***, this is a short description to identify this feature category - must be unique.

**Available Features**, list of available feature codes.

**Enabled Features**, list of feature codes that have been included.



## 6.3.3 Dialing Restriction Rules

Here you can create dial restrictions rules. These can be associated with a class of services.

### General

The screenshot shows the 'Dialing Restriction Rules' configuration interface. It includes a 'GENERAL' tab, a 'Description \*' field, a 'Custom Rules Context' field, and a table for defining rules. The table columns are 'Rule (Pattern)', 'Allowed', 'Announcement', 'Play Max Duration', 'Max Duration', and 'Password'. A sample rule is shown with 'Match Pattern', 'No', 'None', 'No', 'Max duration in seconds', and 'No'. There are 'Add' and 'Save' buttons.

**Description\***, short description to identify this "Dialing Restriction" - must be unique.  
**Custom Rules Context**, this allows you to include a custom context with your own advanced rules.

### Rules section

**Rules (Pattern)**, allows you to create extension patterns in your dial plan that match one or more possible dialed numbers. The pattern options are:

- The letter X or x represents a single digit from 0 to 9.
- The letter Z or z represents a single digit from 1 to 9.
- The letter N or n represents a single digit from 2 to 9.
- The period (.) character is a wildcard that matches one or more characters.
- The exclamation mark (!) is a wildcard that matches zero or more characters.
- [1237-9] matches any digit or letter in the brackets (in this example, 1,2,3,7,8,9)
- [a-z] matches any lower-case letter
- [A-Z] matches any UPPER-case letter

**Allowed**, allow/disallow this pattern.

**Announcement**, you can choose an announcement associated with this pattern.

**Play Max Duration**, play max duration only if max duration is greater than 0 or not in blank.

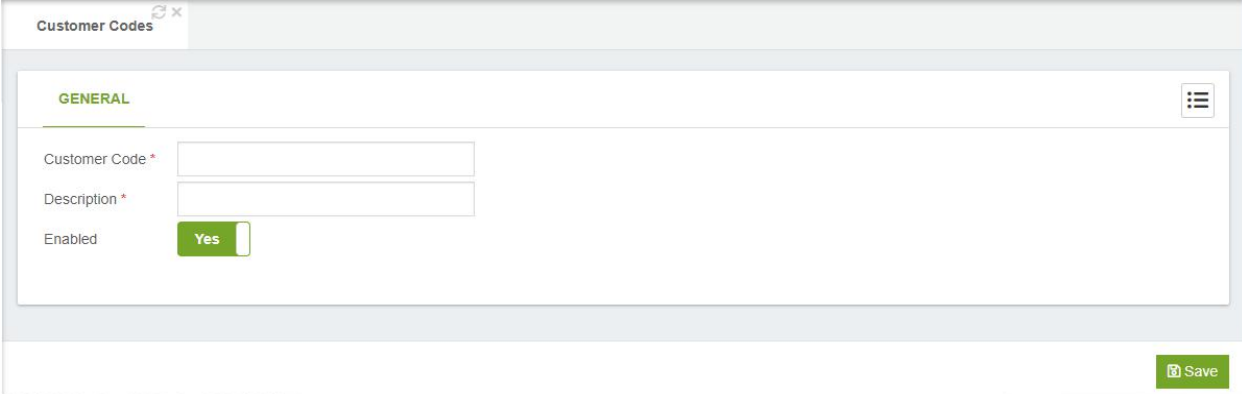
**Max Duration**, maximum call duration associated with this pattern.

**Password**, this determines if a password is required when using this pattern.

## 6.3.4 Customer Codes

Customer codes associated dynamically to a call-in order to register this code in the CDR.

General



Customer Codes

GENERAL

Customer Code \*

Description \*

Enabled  Yes

Save

**Customer Code\***, customer code number.

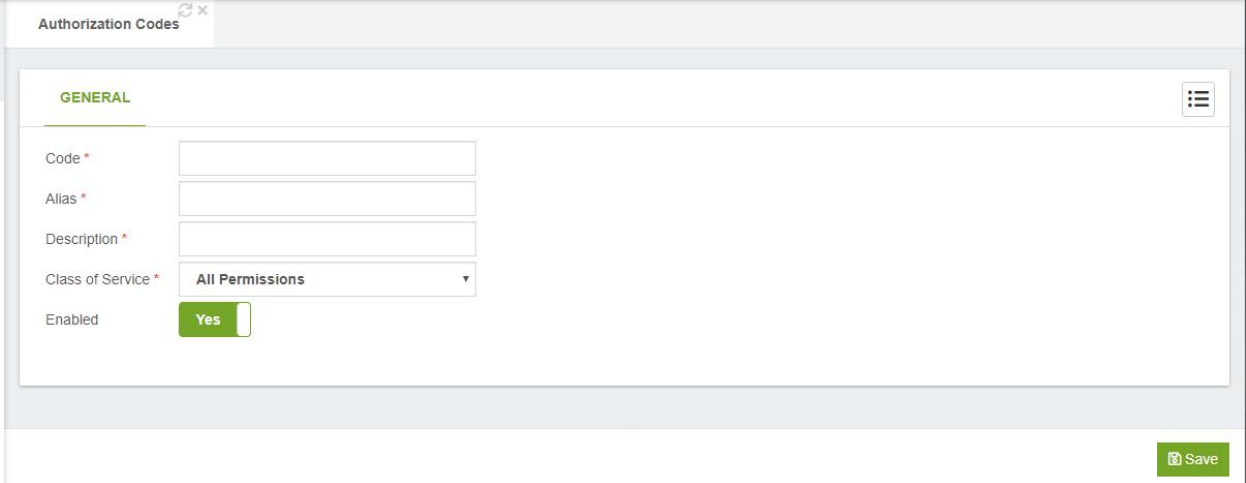
**Description\***, short description to identify this Customer code.

**Enabled**, enable/disable this Customer Code.

## 6.3.5 Authorization Codes

Code that grants privileges to make a call from any extension, based on its Class of Service.

### General



The screenshot shows a web interface for configuring 'Authorization Codes'. The page title is 'Authorization Codes' with a refresh icon. The main content area is titled 'GENERAL' and contains the following fields:

- Code \***: A text input field.
- Alias \***: A text input field.
- Description \***: A text input field.
- Class of Service \***: A dropdown menu currently set to 'All Permissions'.
- Enabled**: A toggle switch currently set to 'Yes'.

A 'Save' button is located at the bottom right of the form.

**Authorization Code\***, authorization code number.

**Authorization Alias\***, Alias to identify this authorization code. For security reasons this will appear on CDR reports instead of the authorization code.

**Description\***, Short description to identify this "Authorization Code".

**Class of Service**, Class of Service is used to route the call.

**Enabled**, enable/disable this Authorization Code.

## 6.3.6 Route Selections

Route selection is a private branch exchange (PBX) feature that allows a system to route a telephone call over the most appropriate carrier and service offering based on factors such as the type of call (i.e., local, local long distance, etc.), the user's class of service (CoS), the time of day, and the day of the week (e.g., workday, weekend, or holiday).

### General

The screenshot shows the 'Route Selections' configuration interface. At the top, there's a tab labeled 'Route Selections'. Below it, the 'GENERAL' section is active. A 'Description \*' field is present. The 'Route Selection Members' section contains a table with the following structure:

	Outbound Route	Time Group	Enabled	
+	-- Select Outbound Route --	-- Select Time --	On	🗑️
				Add

At the bottom right of the form is a 'Save' button.

**Description\***, a short description for identify this Route Selection

### Route Selection Members section

**Outbound Route**, here you can select outbound route.

**Time Group**, here you can select time group.

**Enabled**, enable or disable this route.

## 6.4 Call Center

### 6.4.1 Ring Groups

Ring Groups offer the possibility that a call to be received by more than one internal extension. The option is used most often for picking up calls received on a certain line (Inbound Routes) and sending them to a certain destination (Welcome prompt, IVR and ring groups). Also, the group can be accessed internally, calling the code assigned to it.

#### General

The screenshot shows the 'Ring Groups' configuration page in the VitalPBX interface. The 'GENERAL' tab is active. The form includes the following fields and controls:

- Code \***: Text input field.
- Description \***: Text input field.
- Extensions**: Text input field with a list icon.
- External Numbers**: Text input field.
- Ring Strategy**: Dropdown menu with 'Ringall' selected.
- Ring Time**: Dropdown menu with 'Default (30)' selected.
- Class of Service**: Dropdown menu with 'All Permissions' selected.
- Ringback Tone**: Dropdown menu with 'None (Ringback)' selected.
- CID Name Prefix**: Text input field.
- Allow Diversions**: Toggle button set to 'No'.
- Mark Cancelled Calls as Answered**: Toggle button set to 'No'.
- Last Destination \***: Section containing two dropdown menus: 'Select Module' and 'Select Destination'.
- Save**: Green button with a save icon.

**Code\***, number to dial to reach this service.

**Description\***, short description to identify this ring group.

**Extensions**, list of extension for this ring group.

**External Numbers**, list of external number for this ring group.

**Ring Strategy**, ring strategy of extension group.

**Ring Time**, ring time in seconds, MAX 160 seconds.

**Class of Service**, Class of Service to use for dial the external numbers listed in this ring group.

**Music on Hold**, music on hold to play.

**CID Name Prefix**, prefix to append to this ring group.

**Allow Diversions**, allows you to define if the diversions defined for the different extension members will be applied or not.

**Mark Cancelled Calls as Answered**, with this option enabled prevents the other phones to record a missed call when the call has been answered by another member

listed on this ring group. This is a very useful setting when the ring strategy is set to “Ring All”

### Last Destination Section

**Select Module**, allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination**, this is the call target to which the module should be routed.

## 6.4.2 Queues

ACD (Automatic Call Distributor) is what distributes incoming calls in the order of arrival to the first available agent. The system answers each call immediately and, if necessary, holds it in a queue until it can be directed to the next available call center agent. Balancing the workload among agents ensures that each caller receives prompt and professional service.

### General

The screenshot shows the 'Queues' configuration interface. The 'GENERAL' tab is active. Fields include:

- Code \***: Text input
- Description \***: Text input
- Strategy**: Dropdown menu (set to Ring All)
- CID Name Prefix**: Text input
- Join Announcement**: Dropdown menu (set to None) with a speaker icon
- Agent Announcement**: Dropdown menu (set to None) with a speaker icon
- Service Level**: Text input (Value in seconds)
- Join Empty**: Dropdown menu (set to Yes)
- Leave When Empty**: Dropdown menu (set to No)
- Timeout Priority**: Dropdown menu (set to App)
- Queue Timeout**: Text input (set to 30)
- Member Timeout**: Text input (set to 15)
- Retry**: Text input (set to 5)
- Wrap-up-time**: Text input (set to 0)
- Queue Callback**: Dropdown menu (set to Disabled)
- Music on Hold**: Dropdown menu (set to Default)
- Ring Busy Agents**: Radio button (set to No)
- Record**: Radio button (set to No)

**Members** section:

Extension	Penalty	Member Type	Allow Diversions
<a href="#">Add</a>			

**Final Destination \*** and **After Agent Hangup Destination** sections:

- Final Destination \***: Two dropdown menus (Select Module, Select Destination)
- After Agent Hangup Destination**: Two dropdown menus (Select Module, Select Destination)

A **Save** button is located at the bottom right of the form.

**Code\***, number to reach this service.

**Description\***, short Description to identify this queue.

**Strategy**, this defines the strategy to ring this queue. Options are:

- **Ring All**: Ring all available channels until one of the members answers the phone.

- **Least Recent:** Ring interface which was least recently hung up by this queue.
- **Fewest Calls:** Ring the one with fewest completed calls from this queue.
- **Random:** Ring random interface.
- **Round Robin Memory:** Round robin with memory, remember where we left off last ring pass.
- **Round Robin Ordered:** Same as Round Robin Memory, except the queue member order from config file is preserved.
- **Linear:** Rings interfaces in the order specified in this queue. If you use dynamic members, the members will be rung in the order in which they were added.
- **Weight Random:** Rings random interface but uses the member's penalty as a weight when calculating their metric.

**CID Name Prefix,** prefix to append to this queue, typically indicate to the agents from which queue the call comes.

**Join Announcement,** allowing you to define an announcement to be played to the caller immediately as they reach the queue.

**Agent Announcement,** an announcement may be specified which is played for the member as soon as they answer a call, typically to indicate to them which queue this call should be answered as, so that agents or members who are listening to more than one queue can differentiated how they should engage the customer.

**Service Level,** the idea is to define the maximum acceptable time for a caller to wait before being answered. You then note how many calls are answered within that threshold, and they go toward your service level. So, for example, if your service level is 60 seconds, and 4 out of 5 calls are answered in 60 seconds or less, your service level is 80%.

**Join Empty,** If there are calls queued, and the last agent logs out, the remaining incoming callers will immediately be removed from the queue, and the Queue() call will return, If leavewhenempty” is set to “strict”.

“joinempty” set to “strict” will keep incoming callers from being placed in queues where there are no agents to take calls. The Queue() application will return, and the dial plan can determine what to do next.

This setting controls whether callers can join a queue with no members.

There are four choices:

- **yes** – callers can join a queue with no members or only unavailable members
- **no** – callers cannot join a queue with no members
- **strict** – callers cannot join a queue with no members or only unavailable members
- **loose** – same as strict, but paused queue members do not count as unavailable (new in 1.6)

**Leave When Empty**, used to control whether callers are kicked out of the queue when members are no longer available to take calls.

**Timeout Priority**, this is used to control the priority of the two possible timeout options specified for a queue. The Queue (App) application has a timeout value that can be specified to control the absolute time a caller can be in the queue. The timeout value controls the amount of time (along with retry) to ring a member for. Sometime these values conflict, so you can control which value takes precedence.

**Queue Timeout**, this will cause the queue to fail out after a specified number of seconds.

**Member Timeout**, this specifies the number of seconds to ring a member's device.

**Retry**, specifies the number of seconds to wait before attempting the next member in the queue if the timeout value is exhausted while attempting to ring a member of the queue.

**Wrap-up time**, the number of seconds to keep a member unavailable in a queue after completing a call. This time allows an agent to finish any post call processing they may need to handle before they are presented with the next call.

**Queue Callback**, when you have the Queues Callback add-on installed, here you can select the Queue Callback for this Queue.

**Music on Hold**, this option sets the class of music for this queue.

**Ring Busy Agent**, this is used to avoid sending calls to members whose status is In Use.

**Record**, record the calls in this queue.

### Members section

**Extension**, extension number for the Queue Member.

**Penalty**, within a queue, we can penalize members in order to lower their preference for being called when there are people waiting in a particular queue. For example, we may penalize queue members when we want them to be a member of a queue, but to be used only when the queue gets full enough that all our preferred agents are unavailable. This means we can have three queues (say, Support, Sales, and Billing), each containing the same three queue members: James Shaw, Kay Madsen, and Danielle Roberts. Suppose, however, that we want James Shaw to be the preferred contact in the Support Queue, Kay Madsen preferred in Sales, and Danielle Roberts preferred in Billing. By penalizing Kay Madsen and Danielle Roberts in Support, we ensure that James Shaw will be the preferred queue member called. Similarly, we can penalize James Shaw and Danielle Roberts in the Sales Queue, so Kay Madsen is preferred, and penalize James Shaw and Kay Madsen in the Billing Queue so Danielle Roberts is preferred.

**Member Type**, this decides if the member will be **Dynamic** or **Static**.

**Allow Diversion**, decide if the member executed or not the diversions when called.



## Final Destination\*

The destination if the call is not answered after the “Queue Timeout”

**Select Module**, allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination**, this is the call target to which the module should be routed.

## After Agent Hang-up Destination

This option is generally used when performing quality surveys for customer service. Once the call is hung up by the agent, we can send this call to someone to survey the customer or to an IVR tree with all the options. Afterwards, in the case of the IVR tree, we can use the IVR stats add-on to export the information based on the options selected by the customers.

**Select Module**, allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination**, this is the call target to which the module should be routed.

## Announcement Settings

**Periodic Announcement**, periodic announcement to provide to the caller. The system default message is "All representatives are currently busy assisting other callers. Please wait for the next available representative."

**Periodic Announcement Frequency**, this indicates how often we should make periodic announcements to the caller. Bear in mind that playing a message to callers on a regular basis will tend to upset them. Pleasant music will keep your callers far happier than endlessly repeated apologies or advertising, so give some thought to:

- keeping this message short
- Don't play it too frequently.

**Announce First User**, if enabled, play announcements to the first user waiting in the Queue. This may mean that announcements are played when an agent attempts to connect to the waiting user, which may delay the time before the agent and the user can communicate.

**Relative Periodic Announcement**, if set to yes, the Periodic Announce Frequency timer will start from when the end of the file being played back is reached, instead of from the beginning.

**Announce Hold Time**, defines whether the estimated hold time should be played along with the periodic announcements.

**Announce Position**, defines whether the caller's position in the queue should be announced. If you have any logic in your system that can promote callers in rank (i.e., high-priority calls get moved to the front of the queue), it is best not to use this option. Very few things upset a caller more than hearing that they've been moved toward the back of the line. Options are:

- **No:** The position will never be announced
- **Yes:** The caller's position will always be announced
- **Limit:** The caller will hear her position in the queue only if it is within the limit defined by Announce Position Limit.
- **More:** The caller will hear her position if it is beyond the number defined by Announce Position Limit.

**Announce Position Limit**, used if you've defined Announce Position as either limit or more

**Announce Frequency**, defines how often we should announce the caller's position and/or estimated hold time in the queue. Set this value to zero to disable. In a small call center, it is unlikely that the system will be able to make accurate estimates, and thus callers are more likely to find this information frustrating.

**Min Announce Frequency**, this specifies the minimum amount of time that must pass before we announce the caller's position in the queue again. This is used when the caller's position may change frequently, to prevent the caller hearing multiple updates in a short period of time.

**Announce Round Seconds**, if this value is nonzero, the number of seconds is announced and rounded to the value defined.

## Others

The screenshot shows the 'Others' settings page for a queue in VitalPBX. The page is divided into two main sections: 'Member Settings' and 'Other Queue Settings'. The 'Member Settings' section includes 'Autopause' (set to 'No'), 'Penalty Members Limit' (set to 'Number of zero or greater'), 'Member Delay' (set to 'Value in seconds'), 'Timeout Restart' (set to 'No'), and 'Mark Cancelled Calls as Answered' (set to 'No'). The 'Other Queue Settings' section includes 'Queue Weight' (set to 'Value of 0 or higher'), 'Queue Max Length' (set to '0'), 'Reset Stats' (set to 'Disabled'), 'IVR' (set to 'None'), 'VIP Customers' (set to 'None'), and 'Autofill' (set to 'Yes'). A 'Save' button is located at the bottom right of the form.

### Members Settings

**Auto Pause**, this enables/disables the automatic pausing of agents who fail to answer a call. A value of All causes this agent to be paused in all queues that they are a member of. This parameter can be tricky in a live environment, because if the agent doesn't know they've been paused, you could end up with agents waiting for calls, not knowing they've been paused. Never use this unless you have a way to indicate to the members that they've been paused or have a supervisor who is watching the status of the queue in real time.

**Penalty Members Limit**, a limit can be set to disregard penalty settings when the queue has too few members. No penalty will be weighed in if there are only X or fewer queue members.

**Member Delay**, this is used if you want a delay prior to the caller and queue member being connected to each other.

**Timeout Restart**, if set to yes, resets the timeout for an agent to answer if either a BUSY or CONGESTION status is received from the channel. This can be useful if the agent is allowed to reject or cancel a call.

### Other Queue Settings section

**Queue Weight**, this option defines the weight of a queue. A queue with a higher weight defined will get first priority when members are associated with multiple queues. Keep in mind that if you have a very busy queue with a high weight, callers in a lower-weight queue might never get answered (or have to wait for a long time).

**Queue Max Length**, this value specifies the maximum number of callers allowed to be waiting in a queue. A value of zero means an unlimited number of callers are allowed in the queue.

**Reset Stats**, it allows you to select a Cron Profile to reset the queue stats periodically.

**IVR**, an IVR may be specified, in which if the user types a SINGLE digit extension while they are in the queue, they will be taken out of the queue and sent to that extension in this IVR.

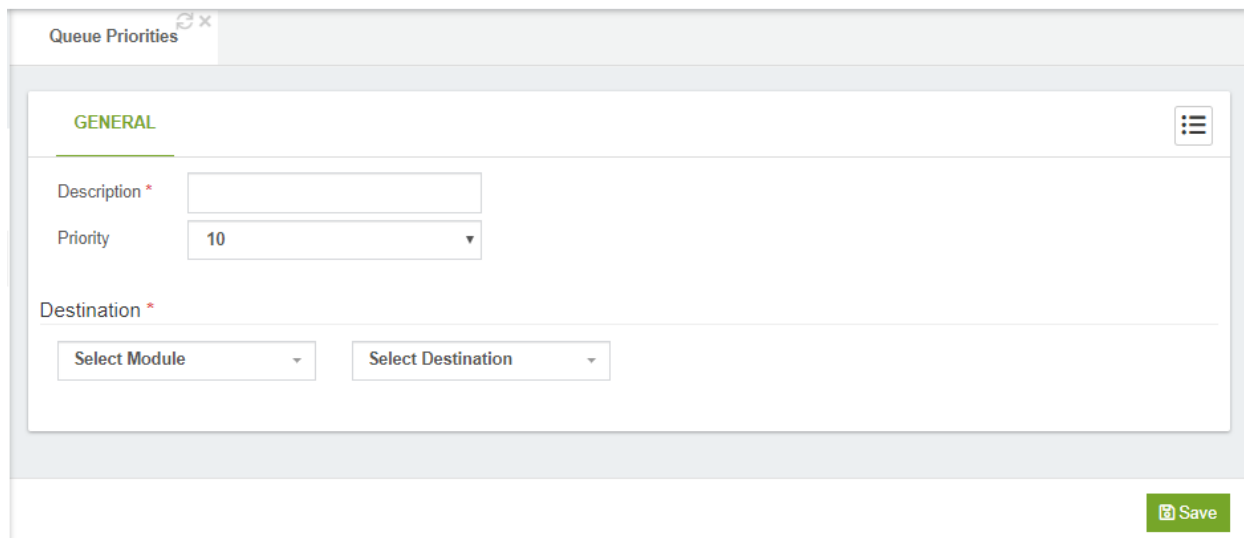
**VIP Customer**, List of VIP Customers, these customers have more priority in this queue.

**Autofill**, the old behavior of the queue (autofill=no) is to have a serial type behavior in that the queue will make all waiting callers wait in the queue even if there is more than one available member ready to take calls until the head caller is connected with the member they were trying to get to.

## 6.4.3 Queues Priorities

Here, you can change the weight of a queue dynamically, in order to prioritize calls that incoming for this way. Usually the destination is a queue.

### General



The screenshot shows a web interface for configuring 'Queue Priorities'. The main heading is 'GENERAL'. There are three main sections: 'Description \*' with a text input field; 'Priority' with a dropdown menu currently showing '10'; and 'Destination \*' which contains two dropdown menus labeled 'Select Module' and 'Select Destination'. A green 'Save' button is located at the bottom right of the form area.

**Description\***, short Description to identify this queue priority

**Priority**, the Queue Priority to set.

#### Destination section

**Select Module**, allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination**, this is the call target to which the module should be routed.

## 6.4.4 Queues VIPs

These are the customers who will have a higher priority when calling.

### General

The screenshot shows a web interface for configuring 'Queue VIPs'. At the top, there's a tab labeled 'Queue VIPs'. Below it, the 'GENERAL' tab is active. The form contains two fields: 'Description \*' with a text input box, and 'VIP List \*' with a larger text area. A green 'Save' button is positioned at the bottom right of the form area.

**Description\***, short description to identify this.

**VIP List\***, here you can insert the list of numbers separated by line.

## 6.4.5 Queues Callback

With the Queues Callback module, you can reduce customer frustration by minimizing the time spent on hold. This feature provides callers with the option to request a callback from the next available agent instead of waiting on hold, allowing them to disconnect from the call and tend to other things.

### How it Works?

When someone calls your company and there are no available agents, after the customers have waited for a predefined length of time, an automated message can offer to call them back. If the customer decides to request the callback service, their number will be saved and queued. When an agent becomes available, VitalPBX will then automatically call the person who left the callback request. If that person answers the call, they will be connected to the agent.

### Why Use It?

There are many reasons this module can be effective for you, but between those reasons you can find:

Increased customer satisfaction and retention: providing this feature to your customer, you let them know that you value their time. It is a courtesy that boosts the customers' impression of your service and results in higher satisfaction with the customer experience.

Reduce call abandonment rate: When your customers have the option to request a callback, they will no longer be tempted to hang up and move on from your services. Instead, they can request a callback and go about their day while they wait for an agent to return their call.

Manage high volumes: Whether you regularly experience peak periods at your call center or occasionally have spikes in call volume, callbacks can defer calls until volumes are more manageable. "Smoothing out" peak periods make more efficient use of agents, improving call center productivity and reducing the need to hire additional resources.

Lowering Telco costs: When you keep a caller in a queue, a PSTN line is occupied the whole time. Often, a toll-free DID at a premium per-minute rate. The callback feature eliminates the need to keep lines open, removing the telco costs associated with the queue waiting time.

Boost employee morale: Your customers don't like waiting in queues, and your agents don't like dealing with customers who have been kept waiting. When your customers haven't had to wait on hold for a long time to reach an agent, they are more likely to

be in a better mood when speaking with your agents. That reduces stress on your agents and helps them improve their productivity.

In the Queues Callback module, you need to configure the following options:

**Description**, brief description

**Callback Queue**, it allows you to define the queue where callers who request a callback will be sent.

**Class of Service**, it allows you to define what Class of Service will be used to perform the callback. Remember that the class of service contains the permissions to allow outgoing calls through specific trunks or outbound routes.

**Dial Prefix**, if defined, it will be prepended to the requested callback number.

**Time Group**, it allows you to configure a time group to define the allowed times to perform callbacks.

**Maximum Tries**, number of allowed tries to perform before marking the call back as failed.

**Caller ID**, Caller ID info to use during the callback. This information could be modified during the call process by the trunks or outbound routes settings.

**Instructions Message**, message to be played with the instructions for requesting a callback.

- **Default Message:** "All of our representatives are currently busy. Please stay on the line and your call will be answered by the next available representative, or press one to be called back when a representative is available"



**Invalid Message**, message to be played when the provided number by caller doesn't match with the defined number rules.

- **Default Message:** "I'm sorry, that is not a recognized phone number"

**Number Prompt Message**, instructions message for asking to enter the callback number.

- **Default Message:** "Please enter your telephone number"

**Ring Time**, it allows you to define the time that the callback numbers will ring before marking the call as not answered.

**Ask Callback Number**, if enabled, the caller will be prompted to enter its callback number. If set to no, the caller id number it will be used as callback number, as long as the number match with the allowed number rules.

**Allowed Number Rules**, they are the numbers allowed to return the call, Patterns can be used.

**Pattern**, it allows to define rules of what type of numbers can be used when requesting a call back options:

- X: The letter X or x represents a single digit from 0 to 9.
- Z: The letter Z or z represents any digit from 1 to 9.
- N: The letter N or n represents a single digit from 2 to 9.
- .: wildcard, this matches one or more characters.
- !: wildcard, matches zero or more characters immediately.
- [1237-9]: matches any digit or letter in the brackets (in this example, 1,2,3,7,8,9)
- [a-z]: matches any lower-case letter
- [A-Z]: matches any Upper-case letter
- Enabled, it allows you to Enable/Disable pattern rules.

# 6.5 External

## 6.5.1 Trunks

In the simplest of terms, a trunk is a pathway into or out of a telephone system. A trunk connects VitalPBX to outside resources, such as PSTN telephone lines or additional PBX systems to perform inter-system transfers. Trunks can be physical, such as a PRI or PSTN line, or they can be virtual by routing calls to another endpoint using Internet Protocol (IP) links.

Trunks are the PBX equivalent of an external phone line. They are the links that allow your system to make calls to the outside world, and to receive calls from the outside world. Without a trunk, you cannot call anyone, and no one can call you. You can configure a trunk to connect with:

- Any VoIP service provider
- Any PSTN/Media Gateway, which allows you to make and receive calls over standard telephone lines from your local telephone company
- Connect directly to another PBX.

### General

The screenshot shows the 'Trunks' configuration page in VitalPBX. The 'GENERAL' tab is active. The 'Technology' dropdown is set to 'PJSIP'. The 'Description' field is empty. The 'Class of Service' is set to 'Trunk Default'. The 'Ring Time' is set to '90'. The 'Dial Profile' is set to 'Default'. The 'Profile' is set to '-- None --'. The 'Music on Hold' is set to 'Default'. The 'Codecs' field is empty. The 'Simultaneous Calls' is set to 'Unlimited'. The 'Call DID From' and 'Get CID From' are both set to 'Default'. The 'Trunk CID' is set to 'rfo4733'. The 'DTMF Mode' is set to 'rfo4733'. The 'Overwrite CID' is set to 'No'. The 'Disable Trunk' and 'Continue on Busy' are both set to 'No'. The 'General Configurations' section includes fields for 'Local Username', 'Remote Host', 'Remote Port', 'Local Secret', 'Transport' (set to 'UDP'), 'Remote Username', 'Remote Secret', 'From User', 'From Domain', and 'Match'. The 'Outbound Registration Settings' section includes 'Require Registration' (set to 'Yes'), 'Permanent Auth Rejection' (set to 'Yes'), 'Client URI', 'Server URI', 'Contact User', 'Max Retries' (set to '10'), 'Expiration' (set to '3600'), 'Retry Interval' (set to '60'), and 'Forbidden Retry Interval' (set to '10'). A 'Save' button is located at the bottom right.

**Technology**, the type of trunk that you want to create.

- PJSIP

- SIP
- IAX2
- TELEPHONY (Shown if the DAHDI add-on is installed)
- TENANT (Shown if a Tenant is created)
- CUSTOM

SIP, PJSIP and IAX2 trunks utilize the technologies of their namesakes. These trunks have the same highlights and pitfalls that extensions and devices using the same technology do. Telephony trunks require physical hardware cards for incoming lines to plug into. SIP trunks are the most widely adopted and compatible, but have difficulties traversing firewalls. IAX2 trunks are able to traverse most firewalls easily but are limited to Asterisk-based systems.

Setting up a trunk is very similar to setting up an extension. All of the trunks share common setup fields, followed by fields that are specific to the technology of the trunk.

**Description**, a description to help identify this trunk

**Class of Service**, class of service to be used by this trunk.

**Ring Timer**, time to ring the trunk before determining that the call cannot be completed.

**Dial Profile**, there are many options that you can set on the outbound call, including call screening, distinctive ringing, and more. Go to Settings > Technology > Dial Profile for more information.

**Profile**, profile with common parameters for the technology selected.

**Music on Hold**, default music on hold for this trunk.

**Codecs**, list of allowed codecs for SIP trunks, in order of preference. Codecs that are not listed will not be allowed for this trunk. **Port**, the port number we want to connect to on the remote side.

**NAT**, (Network Address Translation) is a technology most commonly used by firewalls and routers to allow multiple devices on a LAN with “private” IP addresses to share a single public IP address. A private IP address is an address, which can only be addressed from within the LAN, but not from the Internet outside the LAN. The Options are:

- **No**: Do no special NAT handling other than RFC3581
- **Force**: Pretend there was a rport parameter even if there was
- **Comedia**: Send media to the port Asterisk received it from regardless of where the SDP says to send it.
- **Auto Force**: Set the force\_rport option if Asterisk detects NAT.
- **Auto Comedia**: Set the comedia option if Asterisk detects NAT.

**Get DID From**, it allows you to define from which SIP header will be extracted the DID number.

**Get CID From**, it allows you to define from which SIP header will be extracted the caller ID info.

**Trunk CID**, this sets the default caller ID name and number that will be displayed to the called party. The Trunk CID will only be used if **Overwrite CID** field is set to **Yes**.

Note that setting the outbound caller ID only works on digital lines (T1/E1/J1/PRI/BRI/SIP/IAX2), not POTS lines. The ability to set outbound caller ID must also be supported by your provider.

**Name**, a string that can be used to identify calls on this trunk. If this field is left blank, only the Trunk CID number will be sent.

**Number**, the telephone number that will be displayed by calls on this trunk.

**DTMF Mode**, set default dtmf-mode for sending DTMF. Default rfc2833|rfc4733, Options:

- **info**: SIP INFO messages (application/dtmf-relay)
- **shortinfo**: SIP INFO messages (application/dtmf)
- **inband**: Inband audio (requires 64 kbit codec -alaw, ulaw)
- **auto**: Use rfc2833|rfc4733 if offered, in-band otherwise

**Overwrite CID**, Overwrites the CID sent by the Extension or module. You got the following options:

No, no overwrite will take place and the CID number is preserved.

Yes, will overwrite any CID number sent through this route.

If not Provided, will overwrite the CID information if no External CID is provided.

**Disable Trunk**, this allows you to disable this trunk to be inaccessible.

**Continue on Busy**, it forces to continue the call to the next configured trunk when this trunk being busy. **Note**: The call will also continue to the next trunk if any error happens, even if this checkbox is not checked.

## SIP/PJSIP/IAX settings

### Device for Outgoing Calls (Peer)

**Outgoing Username**, Username the remote server should use to contact this PBX. It is also the device name that will be created.

**Host**, this is the IP address or DNS hostname of the SIP provider. This is the destination server or network that VitalPBX will send calls to when using this trunk.

**Port**, this value sets the default port to be accessed on the remote endpoint device. Only required for SIP trunks.

**Local Secret**, secret to be used for authentication requests from remote server.

- **Insecure**: Allows relaxing authentication of incoming SIP requests. Options:
  - **Port**: Allow matching of peer by IP address without matching port number
  - **Invite**: Do not require authentication of incoming INVITES'
  - **Port, Invite**: The combination is the minimum security since no checking or port check or authentication to the INVITE message type.

**Allow Inbound Calls**, if checked, this device will be allowed also to accept calls.

**Remote Username**, authentication username for remote server

**Remote Secret**, the password credential used to authenticate this trunk against the provider

**From User**, the user credential used to authenticate this trunk against the provider

**From Domain**, as your provider knows your domain

**Qualify**, causes VitalPBX to regularly send a SIP OPTIONS command to check that the peer is still online. If the peer does not answer within the configured period, VitalPBX will consider the device to be off-line and not available for future calls.

**IAX Trunking**, allows sending voice of several calls in one IAX packet. It can significantly reduce the required network bandwidth.

### Device for Incoming Calls (User)

**Username**, the username credential used to contact this trunk

**Host**, the host they use to contact us (We could specify the "dynamic" option and leave open the possibility that any device connected to your machine without an IP in particular.)

**Local Secret**, secret to be used for authentication requests from remote server.

**Insecure**, Sets the level of authentication and verification established between machines when performing communication. Options are:

- **Port**: Allow matching of peer by IP address without matching port number
- **Invite**: Do not require authentication of incoming INVITEs
- **Port, Invite**: The combination is the minimum security since no checking or port check or authentication to the INVITE message type.

**IP Authentication**, if checked, allows the incoming requests authentication by IP address in addition to the username authentication.

**Qualify**, make periodic checks to make sure that the user is alive.

**IAX Trunking**, allows sending voice of several calls in one IAX packet. It can significantly reduce the required network bandwidth.

### General Configurations (PJSIP)

**Transport**, explicit transport configuration to use.

**Match**, the value is a comma-delimited list of IP addresses or hostnames. IP addresses may have a subnet mask appended. The subnet mask may be written in either CIDR or dotted-decimal notation. Separate the IP address and subnet mask with a slash ("/").

**Contacts**, Permanent contacts assigned to an AoR. You can define multiple contact addresses in SIP URI format. e.g.: sip:198.51.100.1:5060.

### Outbound Registration Settings (PJSIP)

**Require Registration**, it defines, if is required to register against the remote server or VoIP provider.

**Permanent Auth Rejection**, if this option is enabled and an authentication challenge fails, registration will not be attempted again until the configuration is reloaded.

**Client URI**, this is the address-of-record for the outbound registration (i.e. the URI in the to header of the REGISTER). For registration with an ITSP, the client SIP URI may need to consist of an account name or number and the provider hostname for their registrar, e.g. 1234567890@example.com. This may differ between providers.

**Server URI**, this is the URI at which to find the registrar to send the outbound REGISTER. This URI is used as the request URI of the outbound REGISTER request from Asterisk.

**Contact User**, this establishes the user portion from the SIP contact header of the SIP URI. This will affect the reached extension on the Dial Plan when the far end calls you at this registration.

**Max Retries**, maximum number of registration attempts.

**Expiration**, expiration time for registrations in seconds.

**Retry Interval**, interval in seconds between retries if outbound registration is unsuccessful.

**Forbidden Retry Interval**, it defines the time to wait before attempting registration again, after receiving a 403 Forbidden response. If 0 is specified, no retry will be made after receiving a 403 Forbidden response.

- For registration to generic registrars, the client SIP URI will depend on networking specifics and configuration of the registrar.
- For registration with an ITSP, the setting may often be just the domain of the registrar, e.g. sip:sip.example.com.

### Register String

**Register String**, the register line includes a host name (mydomain.com) which tells Asterisk where to send the registration request; the account number and password, for example: account:password@mydomain.com:5060

## Telephony Settings

### General

The screenshot shows the 'Trunks' configuration page with the 'GENERAL' tab selected. The 'TELEPHONY' radio button is chosen under the Technology section. Other settings include: Description (empty), Class of Service (Trunk Default), Ring Time (90), Dial Profile (Default), Music on Hold (Default), Simultaneous Calls (Unlimited), Trunk CID (Trunk CID Name and Trunk CID Number), Overwrite CID (No), Disable Trunk (No), Continue on Busy (No), DAHDI Trunk Parameters (Channel Group: E1 Fix Test, Mode: Linear in Ascending Order), and a Save button at the bottom right.

### DAHDI Trunk Parameters

**Channel Group**, the channel group used by this trunk.  
**Mode**, selection mode for available channels.

### Advanced

In Advanced Settings, you can add any valid value in the account settings of the trunk.

The screenshot shows the 'Trunks' configuration page with the 'ADVANCED' tab selected. It displays a 'Custom Settings' table with columns for Type, Parameter, Value, and Enabled. A 'Friend' type is added with a 'Yes' status and a trash icon. An 'Add' button is at the bottom right of the table. A 'Switch to Text Mode' button is at the bottom left, and a 'Save' button is at the bottom right.

Type	Parameter	Value	Enabled
Friend			Yes

**Type**, Friend, User or Peer.

**Parameter**, any valid variable from Asterisk.

**Value**, any value for the Asterisk variable.  
**Enabled**, enable or disable the custom setting.

## Dial Manipulation Rules

The screenshot shows the 'Dial Manipulation Rules' configuration page. At the top, there are tabs for 'GENERAL', 'ADVANCED', and 'DIAL MANIPULATION RULES'. Below the tabs is a table with the following columns: 'Prepend', 'Prefix', 'Pattern', and 'Enabled'. The 'Enabled' column contains a green 'Yes' button and a red trash icon. Below the table is an 'Add' button. At the bottom left, there is a 'Switch to Text Mode' button, and at the bottom right, there is a 'Save' button.

Dialing Manipulation Rules, that allows you to manipulate the dialed number depending of the trunk. e.g.: Suppose you have two providers, both have emergency calls service, but the number to dial is different for each one, for the first provider you must to dial 933 and for the second one you must to dial 944. So, you can configure in your outbound route the 911 and replace this number depending on the trunk on which the call is dialed through.



## Switch to Text Mode

Due to many requests about configuring trunks in text mode like in other Asterisk distros, we have decided to allow you to create trunks just by writing or pasting the configuration of your provider in a text box. This is to help the customers who come from other distros to have a very easy transition. This option is only available for SIP and IAX2 Trunks.

The screenshot shows the 'Trunks' configuration page in VitalPBX. The 'GENERAL' tab is active. The 'Technology' dropdown is set to 'IAX2'. The 'Description' field is empty. The 'Class of Service' is set to 'Trunk Default'. The 'Ring Time' is set to '80'. The 'Dial Profile' is set to 'Default'. The 'Profile' is set to '-- None --'. The 'Music on Hold' is set to 'Default'. The 'Simultaneous Calls' is set to 'Unlimited'. The 'Get DID From' is set to 'Default'. The 'Trunk CID' is set to 'Default'. The 'DTMF Mode' is set to 'rft2333'. The 'Overwrite CID' is set to 'No'. The 'Disable Trunk' is set to 'No'. The 'Continue on Busy' is set to 'No'. There are two sections for device configuration: 'Device for Outgoing Calls (Peer)' and 'Device for Incoming Calls (User)'. Each section has a 'Local Username' field and a 'Peer Parameters' or 'User Parameters' text area. A 'Register String' field is at the bottom. A 'Switch to Visual Mode' button is in the bottom left, and a 'Save' button is in the bottom right.

## Tenant - Technology

If it is configured in the main tenant it is to be used as a gateway for the other Tenant, if it is configured in the secondary Tenants it is to allow calls between Tenants. This option will only appear if you have installed the Multi-Tenant add-on module.

## Custom - Technology

They are used to support protocols type H323 or any other protocol that is not defined.

## 6.5.2 Outbound Routes

Outbound Routes enable you to choose which Trunks (phone lines) to use when users dial external telephone numbers. A simple installation will direct the PBX to send all calls to a single trunk. However, a complex setup could have an outbound route for emergency calls, another outbound route for local calls, another for long distance calls, and perhaps even another for international calls.

You can even create a "dead trunk" and route prohibited calls (such as international and premium calls) to it.

Outbound Routes are a set of rules that VitalPBX uses to determine which trunk to use for an outbound call. Many VoIP systems have access multiple trunks, as it can be unnecessarily expensive to route all calls over a single trunk. Outbound routing also allows dialed numbers to be rewritten on the fly (to remove or prepend dialed numbers with specific outside access codes or area codes). Routes are defined using patterns, against which the dialed numbers are matched.

Outbound routes have a priority. If a dialed number matches the pattern in two outbound routes, the route with the lower priority rating will be used to place the call. The priority is determined when you define an outbound route: The Route Position list in the Route Settings section determines the sequence in which outbound routes are tested, until a match is found.

### General

The screenshot shows the 'Outbound Routes' configuration page in VitalPBX. The 'GENERAL' tab is active. The form includes the following fields and sections:

- Description \***: A text input field.
- Trunks \***: A dropdown menu with a list icon.
- PIN**: A dropdown menu with 'None' selected.
- Outbound CID**: Two input fields for 'CID Name' and 'CID Number'.
- Overwrite CID**: A dropdown menu with 'No' selected.
- Intra-Company**: A checkbox with 'No' selected.
- Dial Patterns \***: A table with four columns: 'Prepend', 'Prefix', 'Pattern', and 'CID Pattern'. Each column has a corresponding input field. Below the table is a green 'Add' button.
- Failover Destination**: Two dropdown menus labeled 'Select Module' and 'Select Destination'.
- A green 'Save' button is located at the bottom right of the form.

**Description\***, short description to identify this outbound route. The name is usually descriptive of the purpose of the route (for example, "local" or "international").

**Trunks**, list of trunks to use. The order of these matter, the top one will have a higher priority over the others below.

**PIN**, from PIN Lists, using the previously created password sets (if any), to authenticate access to this route. PIN sets can be configured in the VitalPBX PIN dialog.

**Outbound CID**, it allows you to define a specific Caller ID Number/Name that will be using on this outbound route when the “Overwrite CID” setting is enabled.

**Overwrite CID**, Overwrites the CID sent by the Extension or module. You got the following options.

- **No**, no overwrite will take place and the CID number is preserved.
- **Yes**, will overwrite any CID number sent through this route.
- **If not Provided**, will overwrite the CID information if no External CID is provided.

**Intra-Company**, if checked, the internal caller id will be sent through this outbound route, instead of the external caller id of the calling extension.

#### **Dial Patterns:**

- **Prepend**, digits to add to a successful match.
- **Prefix**, prefix to remove to a successful match.
- **Pattern**, pattern matching allows us to create extension patterns in our dial plan that match more than one possible dialed number

Options:

- X: The letter X or x represents a single digit from 0 to 9.
- Z: The letter Z or z represents any digit from 1 to 9.
- N: The letter N or n represents a single digit from 2 to 9.
- .: wildcard, this matches one or more characters.
- !: wildcard, matches zero or more characters immediately.
- [1237-9]: matches any digit or letter in the brackets (in this example, 1,2,3,7,8,9)
- [a-z]: matches any lower-case letter
- [A-Z]: matches any Upper-case letter

**CID Pattern**, if defined, calls that match with the Dial Pattern, will also need to have a matching CID number to place a call through this route. The CID number to take into consideration is the Internal CID not the External CID. You got the following options.

- X: The letter X or x represents a single digit from 0 to 9.
- Z: The letter Z or z represents any digit from 1 to 9.
- N: The letter N or n represents a single digit from 2 to 9.
- .: wildcard, this matches one or more characters.
- !: wildcard, matches zero or more characters immediately.
- [1237-9]: matches any digit or letter in the brackets (in this example, 1,2,3,7,8,9)
- [a-z]: matches any lower-case letter
- [A-Z]: matches any Upper-case letter

Be sure that the outbound routes you create allow you to dial the following types of calls:

**Emergency:** Dedicate a route just for this purpose. Calls for emergency services should never be mangled by another dial pattern.

**Local:** Calls to local numbers (usually NXXXXXXXXX).

**Toll-free:** Calls to toll-free numbers (such as 1-888 or 1-800 numbers)

**Mobiles:** Ensure that your outbound routes have been configured to handle calls to all mobile phone providers.

**International:** Calls outside of the country, if permitted (usually 011)

**Special:** Calls that do not fit any other category. This includes calls such as calls to the operator (0) and directory assistance (411)

**Long distance:** Calls outside of the local calling area, if permitted (usually 1NXXXXXXXXX). Make sure that your outbound routes are designed to properly handle calls if you are using a dedicated provider for international calls.

## 6.5.3 Inbound Routes (DID)

The Inbound Routes module is where you define how the PBX 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.

### General

The screenshot shows the 'Inbound Routes' configuration interface. The 'GENERAL' tab is active. The form contains the following fields and controls:

- Routing Method:** A dropdown menu set to 'Default'.
- Description \*:** A text input field.
- DID Pattern:** A text input field.
- CID Pattern:** A text input field.
- Caller ID Modifier:** A dropdown menu set to 'None'.
- CID Lookup:** A dropdown menu set to 'None'.
- Language:** A dropdown menu set to 'English (en)'.
- Music on Hold:** A dropdown menu set to 'None (Ringback)'.
- Alert Info:** A text input field.
- Enable Recording:** A toggle switch set to 'No'.
- Privacy Manager:** A section containing a 'Privacy Manager' toggle switch set to 'No'.
- Fax Settings:** A section containing a 'Fax Detection' toggle switch set to 'No'.
- Inbound Destination \*:** Two dropdown menus labeled 'Select Module' and 'Select Destination'.

A green 'Save' button is located at the bottom right of the form.

**Routing Method**, here you can either be the Telephony channel for an analog port (FXO), or default for all other inbound routes like E1, T2, Sip or IAX trunk. From version 2.3.8 onward it is possible to route a DID range to an extension number. For example, if I have the DID range from 1 (305) 6724 7100 to 1 (305) 6724 7200, it is possible to get the last four digits of the DID and route it to the corresponding extension.

**Description\***, short description to identify this DID. This field is used to hold a description to help you remember what this particular inbound route is for. This field is not parsed by VitalPBX.

**DID Pattern\***, expected number or pattern. This field is used when DID-based routing is desired. The phone number of the DID to be matched should be entered in this field. The DID number must match the format in which the provider is sending the DID. Many providers will send the DID information with the call as +15555555555, while others will leave out the country code information and simply send 5555555555. If the DID entered in this field does not exactly match the number sent by the provider, then the inbound route will not be used. This field can be left blank to match calls from any DIDs (this will also match calls that have no DID information).

- This field also allows patterns to match a range of numbers. Patterns must begin with an underscore (\_) to signify that they are patterns. Within patterns, X will match the numbers 0 through 9, and specific numbers can be matched if they are placed between square parentheses. For example, to match both 555-555-1234 and 555-555-1235, the pattern would be `_555555123[45]`.

**CID Pattern**, CID number or CID pattern to match. This can be used when CID-based routing is preferred. As with the DID Number field, the CID entered in this field must exactly match the format in which the provider is sending the CID. Providers may send 7, 10, or 11 digits; they may include a country code and the plus symbol. Check with your provider to see the format in which the CID is sent, in order to ensure that this field is entered correctly.

- The Caller ID Number field can be left blank to match with any CIDs (this will also match calls that have no CID information sent with them). The field allows Private, Blocked, Unknown, Restricted, Anonymous, and Unavailable values to be entered, as many providers will send these in the CID number data.

Leaving both the DID Number and Caller ID Number fields blank will create a route that matches all calls.

**Caller ID Modifier**, this allows you to modify the caller id name/number.

**CID Lookup**, it allows you to select a CID Lookup item to search the incoming caller number into a directory of a CRM or a cloud directory, or other and set the correct CID Name.

**Language**, this option specifies the language setting to be used for this route. This will force all prompts specific to the route to be played in the selected language, provided that the language is installed and voice prompts for the specified language exist on your server. This field is not required. If left blank, prompts will be played in the default language of the VitalPBX server.

**Music on Hold**, this drop-down menu allows you to select the music-on-hold class for this route. Whenever a caller accessing this route is placed on hold, they will hear the music on hold defined in the class selected here. This is often used for companies that use their music on hold to advertise services, or that accept calls in multiple different languages. Calls to a French DID might play a music-on-hold class with French advertisements, while an English DID would play a class with English advertisements.

**Alert Info**, to set a distinctive ring for this inbound route. There does not yet seem to be a standard for how to tell a SIP phone that you want it to ring with a distinctive ring. On SIP handsets that do support distinctive ringing, the exact method of specifying distinctive ring varies from one model to another. In many cases this is done by sending a SIP\_ALERT\_INFO header, but the usage of this header is not consistent. This is often used for SIP endpoints that can ring differently, or auto-answer calls based on the SIP\_ALERT\_INFO text that is received. Any inbound call that matches this route will send the text in this field to any SIP device that receives the call.

**Enable Recording**, enable call recording on this route.

#### Privacy Manager section

**Privacy Manager**, this drop-down menu is used to enable or disable the VitalPBX privacy manager functionality. When enabled, incoming calls that arrive without an associated caller ID number will be prompted to enter their telephone number. Callers will be given a number of attempts (as defined in the Max attempts field, below) to enter this information before their call is disconnected.

#### Fax Settings

**Fax Detection**, this determines whether faxes should be detected on this route. If fax detection is enabled, additional parameters can be configured, and a dropdown will appear which is used to select the extension to which the inbound faxes will be directed. Typically, this extension is a DAHDI extension that has a physical fax machine plugged into it. However, it may also be a virtual extension that will be answered by VitalPBX. The program will accept faxes and turn them into digital documents for review.

If fax detection is disabled, fax detection will not be used for calls on this route. Any fax calls will be handled just like voice calls.

#### Destination\* Section

**Select Module**, allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination**, this is the call target to which the module should be routed.

## 6.5.4 Dynamic Routing (Auto CLIP Routes)

This feature allows you to route missed or not completed outgoing calls to the original caller. When extension user makes an outgoing call, the called party can call back extension user directly, no pass through the Inbound route setting.

### General

The screenshot shows the 'Dynamic Routing' configuration window with the 'GENERAL' tab selected. The interface includes the following elements:

- Dynamic Routing** (window title)
- GENERAL** (tab) and **LIST** (tab)
- Expiration Time**: A dropdown menu set to **8 Hours**.
- Digits Match**: An empty text input field.
- Delete Used Records**: A checkbox with a green **Yes** button.
- Only Keep Missed Calls**: A checkbox with a green **Yes** button.
- Save**: A green button with a floppy disk icon in the bottom right corner.

**Expiration Time**, it allows to define how long the records of the dynamic routing list will be conserved, before they are automatically deleted.

**Digits Match**, it allows to define the number of digits to be extracted from the caller's number (from right to left), to later search for matches in the dynamic routing list. If left blank, the entire caller's number will be used to search for matches.

**Delete Used Records**, if checked, the record will be deleted from the dynamic routing list when the callback is answered.

**Only Keep Missed Calls**, if checked, only calls (outgoing) that are missed by the called party will be saved in the dynamic routing list.

## List

Call Date & Time	Extension Number	Called Number	Trunk	Completed	Actions

Displays the complete list of calls that are pending completion of the Dynamic Route action. The action could be canceled through the options of the Actions button.

**Note:** In order for the Dynamic Route to work, the option in the Extension configuration in the Advanced TAB must be activated.

## 6.6 Incoming Calls

### 6.6.1 IVR

IVR (Interactive Voice Response) allows you configure an auto attendant to answer calls and redirect the call-in response to input from the caller. An IVR system is often referred to as a digital receptionist. An IVR plays a pre-recorded message to the caller that asks them to press various buttons on their telephone depending on which department or person they would like to speak with. The IVR system will then route the call accordingly.

VitalPBX's IVR allows any digits to be defined for routing purposes. For example, pressing "1" could route the caller to the sales ring group. Destinations can be defined to receive the call if the IVR times out or does not receive valid input.

It is important that you carefully plan the call flow and branching options for IVRs, while considering the user experience. IVRs use customized Announcements, so you will need to make sure that they are clear and meaningful, and configured to optimize the caller experience. Factors that you should consider include:

Handling the timeout when there is no input from the caller



Controlling the action to take if caller provides invalid user input  
 Allowing the caller to backtrack if s/he has made a mistake or gets lost  
 Allowing the caller to return to the IVR if voicemail is encountered  
 Whether or not to take advantage of time-based branching, by defining Time Groups, for normal office hours, that include start and end times, start and end days of the week, and much more  
 Defining a Time Condition, and setting one destination if the time matches and a different destination if the time does not match

## General

**Description\***, short description to identify this IVR. This field is not parsed by VitalPBX.

**Class of Service**, here you can choose a Class of Service for this IVR.

**Invalid Tries**, number of invalid attempts allowed.

**Welcome Message**, welcome message, selected from a drop-down menu of pre-recorded messages that will be played to the caller when they enter the IVR.

**Instructions Message**, Message to be played after the welcome message. This message is useful for avoid repeating the welcome message on invalid/timeout event.

**Invalid Retry Message**, message, selected from a drop-down menu of pre-recorded messages, to be played when the IVR receives an invalid option.

**Invalid Message**, message, selected from a drop-down menu of pre-recorded messages, to be played when user exceeds the maximum number of attempts.

**Timeout**, this value is the maximum time, in seconds, that the system will wait for input from the caller. If this time passes without input, the call will fail over to the Timeout Destination that the user has defined.

**Timeout Tries**, is used to determine the number of times the IVR will repeat itself when no valid input is received. After the specified number of tries, the caller will be send to the Timeout Destination. The maximum number of loops allowed is five.

**Timeout Retry Message**, message, selected from a drop-down menu of pre-recorded messages, to be played when input has not been received within the period defined by Timeout. If the number of Timeout Tries has not yet been reached, then the user will be prompted to try again.

**Timeout Message**, message selected from a drop-down menu of pre-recorded messages, to be played when reaching the timeout.

**Welcome after Timeout**, when enabled, will return the user to the main IVR Welcome Message after playing the Timeout Retry Message.

**Welcome after Retry**, when enabled, will return the user to the main IVR Welcome Message after playing the Invalid Retry Message.

**Direct Dial**, this enables the caller to dial an extension directly from the IVR. If this option is not enabled, the caller will receive a message that they have provided invalid input when they enter an extension, even if the extension is valid.

**Generate Stats**, if is set on yes, it will be saved stats for each option marked. These statistics can be consulted in the IVR Stats module.

### Invalid Destination\* Section

**Select Module**, allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination**, this is the call target to which the module should be routed.

### Timeout Destination\* Section

**Select Module**, allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination**, this is the call target to which the module should be routed.

### IVR Entries

This tab defines how to handle the user's input.

Digit	Module / Destination	Enabled
<input type="text" value="Digit to Press"/>	<input type="text" value="Select Module"/>	<input type="text" value="Select Destination"/>
		<input type="checkbox"/> Yes <input type="button" value="Delete"/>

**Digit**, digit to press.

**Module**, module to activate when the caller presses the appropriate digit.

**Destination**, destination to call when the caller presses the appropriate digit.

**Enabled**, enabled or disable this option.

It is good practice to ensure that the user has an easy way of getting back to the previous menu. One simple way to do this would be to allow the user to press “\*” and link that keypress to the parent IVR.

## 6.6.2 Time Groups

Time conditions are a set of rules for hours, dates, or days of the week. A condition has two call targets each time. Calls sent to a time condition will be sent to one target if the time of the call matches one of the conditions, or to the other target if none of the conditions match. Each time condition can have multiple time definitions (known as time groups). Time conditions are often used to control how a phone system responds to callers inside and outside of business hours, and during holidays.

Before we can set up a time condition call target, we need to define a set of time groups. Time groups are a list of rules against which incoming calls are checked. The rules specify a specific date or time, and a call can be routed differently if the time it comes in matches with one of the rules in a time group. Each time group can have an unlimited number of rules defined. It is useful to group similar sets of time rules together. For example, there may be one-time group for business hours in which the time that the business will be open will be defined. Another popular time group is for holidays, in which each holiday that falls on a business day is defined.

### General

The screenshot shows the 'Time Groups' configuration page. The 'GENERAL' tab is selected. There is a 'Description' field with an asterisk indicating it is required. Below it is a 'Schedules' section with a table for defining time rules. The table has the following columns: Time to Start, Week Day Start, Month Day Start, Month Start, Time to Finish, Week Day Finish, Month Day Finish, and Month Finish. Each column has a corresponding input field or dropdown menu. There is a plus icon to add a new row and a trash icon to delete a row. At the bottom right of the table is an 'Add' button, and at the bottom right of the form is a 'Save' button.

**Description\***, used to identify the time group, when selecting it during the setup of a time condition. This value is not parsed by VitalPBX.

### Schedules Section

**Time to Start**, time, in hours and minutes, that the time group should start.

**Weekday Start**, day of the week that the time group should start.

**Month Day Start**, day of the month that the time group should start.

**Month Start**, month of the year that the time group should start.

**Time to finish**, time, in hours and minutes, that the time group should end.

**Weekday Finish**, day of the week that the time group should end.

**Month Day Finish**, day of the month that the time group should end.

**Month Finish**, month of the year that the time group should end.

## 6.6.3 Time Conditions

Once a time group has been defined, a time condition can be set up as a call target.

### General

The screenshot shows the 'TIME CONDITIONS' configuration interface. It features a header with the title 'TIME CONDITIONS' and a menu icon. The form is organized into several sections:

- Basic Information:** Includes 'Toggle Code \*' (text input), 'Description \*' (text input), 'Time Group \*' (dropdown menu showing '-- Select Time --'), and 'Time Zone' (dropdown menu showing 'System').
- Security and Status:** Includes 'Authorization Pin' (text input), 'Status' (dropdown menu showing 'Default'), and 'BLF Inverted' (checkbox button showing 'No').
- Destination Settings:** Two sections for 'Destination if time matches \*' and 'Destination if time does not match \*'. Each section contains two dropdown menus: 'Select Module' and 'Select Destination'.

**Toggle Code\***, dial code to toggle the time condition state through the phone.

**Description\***, short Description to identify this Time Condition.

**Time Group\***, select a Time Group, from the drop-down list, that was created in the Time Groups dialog.

**Time Zone**, as an extended feature, you can set at which Time Zone the Time Condition will be running at.

**Authorization Pin**, optional password to protect from unauthorized people of modifying this time condition.

**Status**, allows you to override the default behavior of a time condition, Options:

- **Default:** Default behavior
- **Temporary Matched/Unmatched:** Overrides temporary the time condition and sends the calls to the matched/unmatched

destination until the current time span has elapsed. After that, the behavior will return to default

- o **Permanently Matched/Unmatched:** Overrides permanently the time condition and sends the calls to the matched/unmatched destination until the override is removed.

**BLF Inverted,** by default the BLF light color is green when the time condition is matching and red when is not matching. Setting up this to “yes” will make that the behavior be the inverse of what is described above.

### Destination if Time Matches Section

**Select Module,** allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination,** this is the call target to which the module should be routed.

### Destination if Time does not Match Section

**Select Module,** allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination,** this is the call target to which the module should be routed.

## 6.6.3 Announcements

This module is used for when you want the caller to hear a message, before being automatically transferred to a fixed destination.

### General

**Description\*,** short description to identify this Announcement.

**Custom Recording,** here you can select a recording, from the drop-down list, to play in this Announcement.

### Destination after playing announcement\* Section

**Select Module,** allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination**, this is the call target to which the module should be routed.

## 6.6.4 Languages

This module is used for when you want to change the language of the voice guide in the course of a call, such as when an IVR is used and the user selects a language.

### General

The screenshot shows a web interface for configuring languages. The main heading is 'Languages'. Underneath, there's a 'GENERAL' section. It includes a 'Name \*' field, a 'Description \*' field, and a 'Language' dropdown menu currently set to 'English (en)'. Below these, there's a 'Destination \*' section with two dropdown menus: 'Select Module' and 'Select Destination'. A green 'Save' button is positioned at the bottom right of the form.

**Name\***, short name, must be unique.

**Description**, short description to identify this language.

**Language**, channel language to use from drop-down list.

#### Destination section

**Select Module**, allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination**, this is the call target to which the module should be routed.

## 6.6.5 Night Mode

Night mode is used to change the conditions of an incoming route depending on whether it is active or not.

### General

**Toggle Code\***, code to dial to change the night mode state via phone.

**Description**, short description to identify this Night Mode

**Optional Password**, optional password to protect this Night Mode

**State**, this indicates whether this Night Mode is currently active.

**Ignore global mode**, this means that it will not be affected by the state of global night mode.

**Generate Hint (indicator)**, generates hint for this night mode to be seen from a console or monitoring key.

### Destination on Destination when Disabled\* Section

**Select Module**, allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination**, this is the call target to which the module should be routed.

### Destination on Destination when Enabled\* Section

**Select Module**, allows the user to choose from a drop-down list of available modules, which module should be activated.

**Select Destination**, this is the call target to which the module should be routed.

## 6.6.6 CID Modifiers

CID Modifiers allow you to modify the incoming CID name and number:

You can append or prepend anything to the CID name/number

You can replace completely the CID name

You can cut or delete certain part of the code number

Description, short description to identify this CID Modifiers.

### CID Number Settings

**Skip/Length**, this allows you to modify incoming CID number by starting the manipulation a number of digits either from the beginning or end of the CID number, while retaining any number of the original digits. Options:

- **Skip:** Specify where to start modifying the CID number. A positive skip value of x will ignore the leading x digits. A negative value of x will start x digits before the end of incoming CID number.
- **Length:** determines the length of the modified CID number. If length is zero, all digits after the start position will be used. Define a negative length of x in order to discard the x trailing digits.

**Prepend**, prefix to be added at the beginning of the original Caller ID number.

**Append**, suffix to be added after the original Caller ID number.

### CID Name Settings

**Prepend**, Text that can be added in front of the original Caller ID name.

**Append**, Text that can be added at the end of the original Caller ID name.



**Replace With**, completely replace the CID name with this text. Leave this field blank to keep the original CID name.

## 6.6.7 CID Lookup

With this module it is possible to consult a database or a URL with a telephone number in order to document the call with the name of the telephone number owner.

### General

The screenshot shows the 'CID Lookup' configuration window with the 'GENERAL' tab selected. The fields are arranged in two columns:

- Left Column:**
  - Description \*
  - Source \* (Dropdown menu showing 'HTTP/HTTPS')
  - Host \*
  - Port
  - Auth User
  - Auth Password
- Right Column:**
  - Path
  - Query String
  - Timeout
  - Secure (Radio button, currently set to 'No')

A 'Save' button is located at the bottom right of the form.

**Description**, short description to identify this CID Lookup.

**Source**, it defines the method to get the CID name of an incoming caller.

**Host**, it defines the API host to make the request.

**Port**, it defines the port to make the request. By default, 80 for HTTP request and 443 for HTTPS request.

**Auth User**, it defines the user to authenticate the HTTP/HTTPS request.

**Auth Password**, it defines the password to authenticate the HTTP/HTTPS request

**Path**, it defines the script file name to execute on request. Example: cid\_lookup.php

**Query String**, it defines the arguments needed for execute the script. The special argument value [CIDNUM] it will be replaced by caller cid number. Example: caller\_num=[CIDNUM]&ctype=vip.

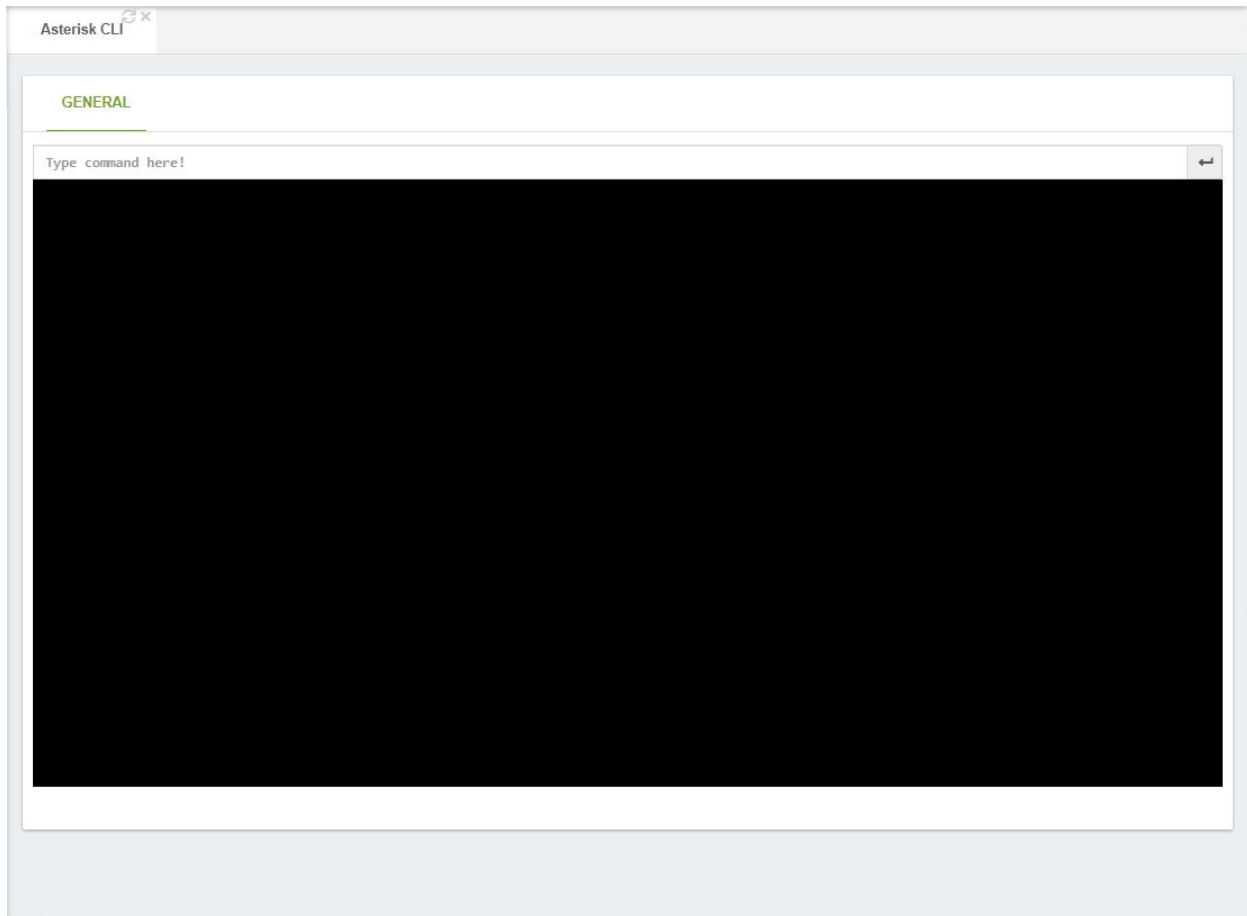
**Secure**, if it is checked, the request will be through HTTPS, in other way it will be through HTTP.

## 6.7 Tools

### 6.7.1 Asterisk CLI

From this tab you are able to access the CLI Interface.

#### General



In this dialog, you can type any valid Asterisk command. As soon as you start typing, a drop-down list of available Asterisk commands will be displayed.

## 6.7.2 Blacklist

It is possible to define a blacklist number with a pattern and define a destination for it. Also, it is possible to disable/enable a blacklist item through the GUI. If no destination is defined for the blacklisted item a message will be played to the caller.

### General

The screenshot shows the 'Blacklist' configuration window with the 'GENERAL' tab selected. The window has a title bar with 'Blacklist' and a close button. The 'GENERAL' section contains the following fields:

- CID Number \***: A text input field.
- Description \***: A text input field.
- Enabled**: A toggle switch currently set to 'Yes'.
- Destination**: Two dropdown menus labeled 'Select Module' and 'Select Destination'.

A green 'Save' button is located at the bottom right of the configuration area.

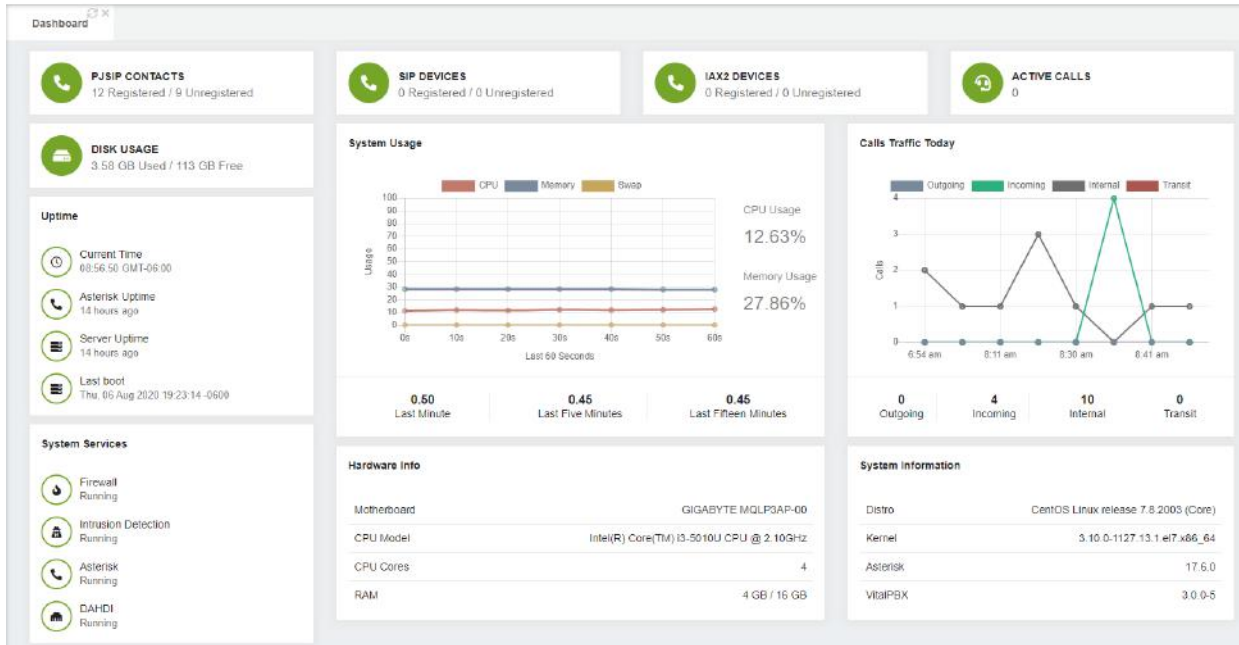
**CID Number**, the number that you want to blacklist.

**Description**, a description of the number that you want to blacklist.

**Enabled**, Enable/Disable this CID number from the blacklist.

**Destination**, optional destination. If set, the caller with a CID Number that match with the configured above, will be redirected to the configured destination. If not set, a message will be played instead.

## 6.7.3 Dashboard



From the Dashboard it is possible to monitor various aspects from your PBX. The Dashboard itself is composed of multiple widgets with this information.

**Monitor Devices,** you can see how many devices are registered for PJSIP, SIP, and IAX2.

**Active Calls,** here you can view the number of active calls at that moment.

**Disk Usage,** with this widget you can monitor the usage you have for your storage.

**System Usage,** this allows you to monitor your CPU, Memory, and SWAP activity.

**Call Traffic Today,** this widget, available from Version 3 and onward, allows you to track the number of calls you have had for this day. You can monitor the following types of calls.

- **Outgoing,** calls flowing outbound from the PBX.
- **Incoming,** calls flowing inbound from the PBX.
- **Internal,** calls between internal extensions and modules.
- **Transit,** Passthrough calls going through the PBX.

**Uptime,** this will show the uptime for Asterisk and the Server. It will also show the current time, and when the server was last booted on.

**System Services,** on this widget you will see the status of the Firewall, Intrusion Detection (Fail2ban), Asterisk, and DAHDI. DAHDI only being available if you have installed the DAHDI add-on module.

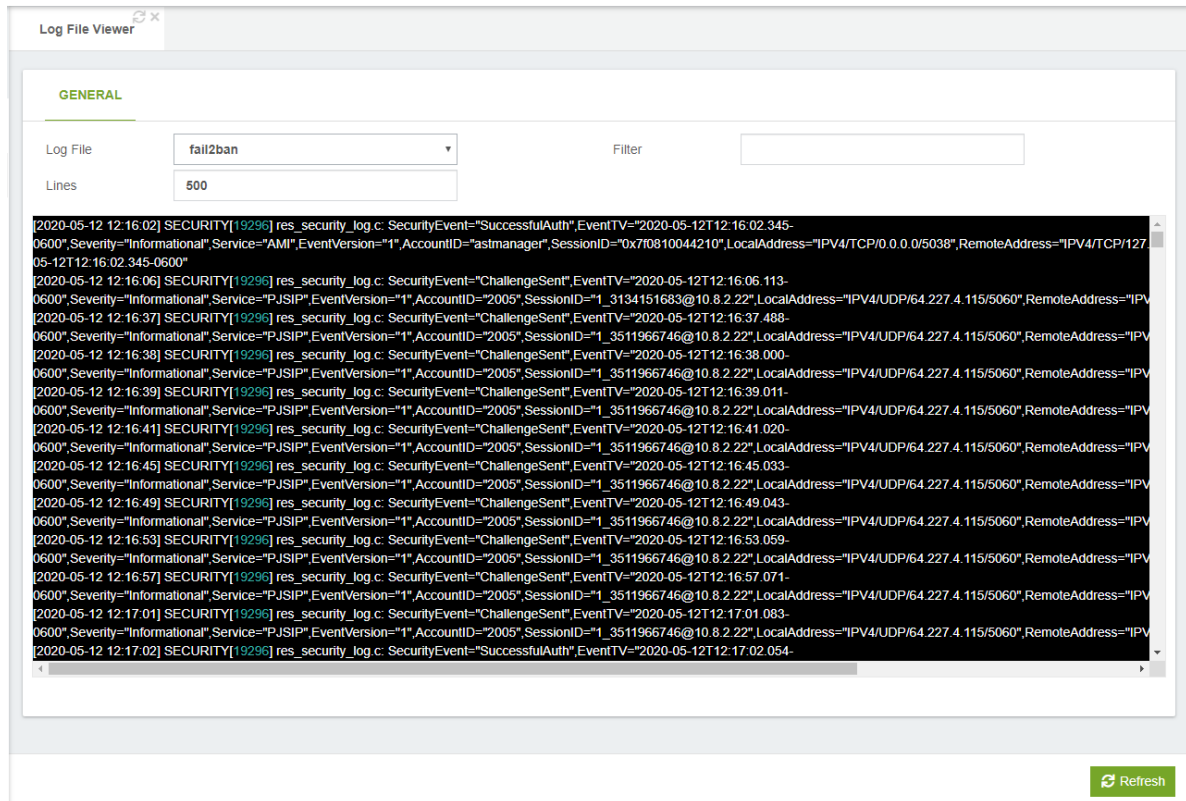
**Hardware Info,** this will list the hardware where you have VitalPBX installed on. This will be the Motherboard or Virtualization software, CPU Model and frequency, CPU Cores, and RAM amount.

**System Information**, here you will see the information about the current version of various layers of the software. This would be the Distro version, Kernel version, Asterisk version, and VitalPBX version.

## 6.7.4 Log File Viewer

In this tab you will find a tool to view log files.

### General



**Log File**, here you can select the log file to see.

**Lines**, last lines to read from the log file.

**Filter**, Filter the Log for specific information.

## 6.7.5 Cron Profiles

In this module the profiles of the tasks to be executed are created.

### General

The screenshot shows the 'Cron Profiles' configuration window. The 'GENERAL' tab is active. It features a 'Description' text input field and a 'Template' dropdown menu currently set to '-- Quick Settings Template --'. Below this is a 'Settings' section with five rows, each containing a label, a text input field, and a dropdown menu:

Label	Input Field	Dropdown Menu
Minute	<input type="text"/>	-- Quick Template --
Hour	<input type="text"/>	-- Quick Template --
Day of Month	<input type="text"/>	-- Quick Template --
Month	<input type="text"/>	-- Quick Template --
Day of Week	<input type="text"/>	-- Quick Template --

A green 'Save' button is located at the bottom right of the form.

**Description**, a brief description to identify this profile of Cron.

**Template**, predefined templates to configure your CRON profile settings easy and faster.

#### Settings

**Minute**, this controls what minute of the hour the command will run on and is between 0 and 59.

**Hour**, this controls what hour the command will run on, and is specified in the 24-hour clock, values must be between 0 and 23 (0 is midnight).

**Day of Month**, this is the Day of Month, that you want the command run on, e.g. to run a command on the 19th of each month, the day would be 19.

**Month**, this is the month a specified command will run on, it may be specified numerically (0-12), or as the name of the month (e.g. May).

**Day of Week**, this is the Day of Week that you want a command to be run on, it can also be numeric (0-7) or as the name of the day (e.g. sun).

## 6.7.6 Weak Passwords

Creates a report of any user accounts, extensions, or trunks that have weak registration passwords.

Accounts with weak passwords represent a security hole and should be updated as soon as possible.

In this tab you will find a list of all weak password in your system

### General

GENERAL			
Show <b>10</b> entries	Search: <input type="text"/>		
Extension	Device	Password	Level
111 - YealinkDev	111 - YealinkDev	1234	Weak
2000 - Boss	2000 - Boss	password	Weak
2001 - Secretary	2001 - Secretary	toor	Weak
2002 - IT Admin	2002 - IT Admin	pa\$\$w0rd	Weak

Showing 1 to 4 of 4 entries

Previous **1** Next

## 6.7.7 Phone Books

This module allows you to create Phone Books that can be viewed from any device that supports URLs for external directories.

### General

The screenshot shows the 'GENERAL' configuration page for a Phone Book. It includes several input fields and dropdown menus:

- Description \***: My Extensions
- Extensions**: 2000 - Boss, 2001 - Secreta... (with a list icon)
- Speed Dials**: (with a list icon)
- Feature Codes**: (with a list icon)
- Ring Groups**: (with a list icon)
- Conferences**: (with a list icon)
- Queues**: (with a list icon)
- Phonebook URL**: http://192.168.0.85/phonebook.php?pb=cJinsNudN
- A QR code is displayed next to the URL.
- A green button labeled "Send by E-mail" is located below the QR code.

**Description**, brief description to identify this phone book configuration.

**Extensions**, it allows you to select which extensions will be available on this Phone Book.

**Features Codes**, it allows you to select which feature codes will be available on this Phone Book.

**Ring Groups**, it allows you to select which ring groups will be available on this Phone Book.

**Conferences**, it allows you to select which conferences will be available on this Phone Book.

**Queues**, it allows you to select which queues will be available on this Phone Book.

**Phone Book URL**, copy and paste this URL into your device.

**Send by E-mail**, allows you to send a QR code with the Phonebook URL data for use with a VitXi mobile device.

Below we will show a couple of examples of how to configure the Phone Book on your device.

1. Grandstream
  - a. Go to PHONEBOOK
  - b. In Phonebook Management
  - c. Enable Phonebook XML Download, Enable, use HTTP or HTTPS.
  - d. Phonebook XML Path, here you will input the URL.
2. Yealink
  - a. Go to Contacts
  - b. In Remote Phone Book



- **Phone Book URL**, here you will input the URL.
- **Name**, descriptive name of this phonebook.

It is also possible to create external Telephone Guides for which when creating it, you must choose **Type** > *External*. We can download the format to import the External Guide by pressing the *Download CSV format* button.

As an extended feature, you can add, remove, and edit external contacts from the interface directly.

**GENERAL** ☰

Description \*  CSV File

Prefix


Contacts

Search:

First Name	Last Name	Phone	Organization	Job Title	E-mail	Actions
Joseph	Montes	1 (305) 560 5776	VitalPBX LLC	Channel Manager	joseph@vitalpbx.com	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Lincoln	Hyland	(159) 935 - 4798	Swordfish and Grill	Owner	lincoln@swordfishgrill.com	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Patrick	Smith	1 (555) 468 7122	Luigi's Auto Systems	Technician	PatSmith@luigiautosys.com	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

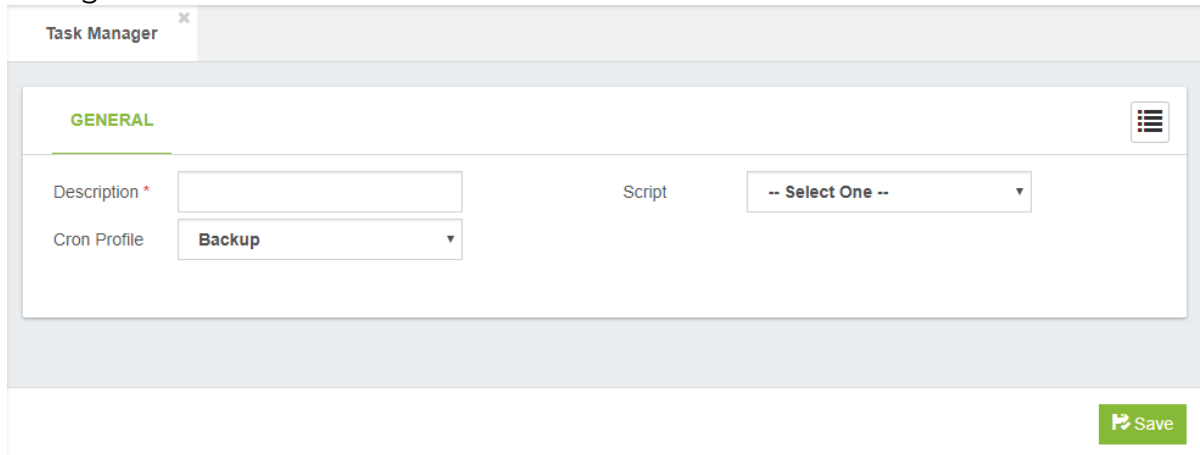
Showing 1 to 3 of 3 entries Previous **1** Next

Phonebook URL



## 6.7.8 Task Manager

The task manager add-on is a powerful and fully free tool that allows you to schedule any script created by the user as a task from the GUI. The user must first place the scripts under the following path `/var/lib/vitalpbx/scripts/` and give to its scripts the right permissions, those scripts will be listed automatically in task manager module, allowing to the user associated a Cron Profile to schedule the execution of its scripts. After save the task the user must to apply changes to make effective its configurations.



The screenshot shows a web interface for the Task Manager. At the top, there is a tab labeled "Task Manager" with a close button (x). Below the tab is a section titled "GENERAL" in green, with a menu icon on the right. The form contains three fields: "Description \*" with an empty text input, "Script" with a dropdown menu showing "-- Select One --", and "Cron Profile" with a dropdown menu showing "Backup". A green "Save" button with a floppy disk icon is located at the bottom right of the form.

## 6.8 Extras

### 6.8.1 Video Conference

Through WebRTC technology, VitalPBX includes a module which can make your video conferences using our powerful meetings server in the cloud, which have the following options:

**Simple to use**, no downloads required. VitXi Meet works directly within your browser. Simply share your conference URL with others to get started.

**Low Bandwidth**, multi-party video conferences work with as little as 128Kbps. Screen-sharing and audio-only conferences are possible with far less.

**Unlimited Users**, there are no artificial restrictions on the number of users or conference participants. Server power and bandwidth are the only limiting factors.

**Screen Sharing**, it's easy to share your screen with others. VitXi Meet is ideal for on-line presentations, lectures, and tech support sessions.

**Secure Rooms**, need some privacy? VitXi Meet conference rooms can be secured with a password in order to exclude unwanted guests and prevent interruptions.

**Share Notes**, with VitXi Meet features Etherpad, a real-time collaborative text editor that's great for meeting minutes, writing articles, and more.

The screenshot shows a web interface for a video conference. At the top, there's a tab labeled 'Video Conference'. Below it, a 'GENERAL' section is highlighted. It contains three fields: 'Server' with a dropdown menu set to 'VitalPBX', 'Room Name' with a text input containing 'MaroonOctopusGaffer' and a refresh icon, and 'URL' with the text 'https://meet.vitalpbx.org/MaroonOctopusGaffer'. A green 'Join / Create' button is located at the bottom right of the form.

**Server**, here you can select the server where conference will be hosted.

**Room Name**, a room name to join or start a new conference.

**URL**, you can share this URL with the other participants of the video conference.

**Note:** Remember to download our plugins in the Chrome web store, look for them with the word VitXi Meet.

## 6.9 Emergency Calls

With the introduction of Kari's Law in the United States, from version 3 and onward, the Emergency module was created. With it, we have two modules, Emergency Numbers and Dispatchable Locations. These two come into play whenever an Emergency Call is placed into action from any extension or device within the PBX.

### 6.9.1 Emergency Numbers

This module defines the external numbers that cannot be restricted, these numbers can be dialed from any extension, either a Hotdesking that is not registered or any extension that has completely restricted outgoing calls.

#### General

The screenshot shows the 'Emergency Numbers' configuration interface. At the top, there's a tab labeled 'GENERAL'. Below it, there are four input fields: 'Description', 'Trunks' (with a dropdown menu icon), 'Email Addresses', and a table for 'List of Emergency Numbers'. The table has two columns: 'Number' and 'Service Name'. Below the table, there are two input fields with placeholder text: 'eg.: 911' and 'eg.: Police, Firefighters, Ambulance, Etc.'. There is a trash icon to the right of the second input field and an 'Add' button at the bottom right.

**Description**, a short description to easy recognize this list of emergency numbers.

**Trunks**, list of trunks than can be used in case of an emergency call.

**Email Addresses**, these are the email addresses that are used for the emergency contacts. These emails will have a notification sent to when

**List of Emergency Numbers**, telephone number to contact local emergency services for assistance and name of the service that represents this telephone number. eg.: Police, Firefighters, Ambulance, etc.

## 6.9.2 Dispatchable Locations

Complying as well with Kari's Law, when have now included this module from Version 3 and onward. This module allows you to create detailed locations which will be used when an Emergency Call is placed. This is the location that is sent to the Emergency Contacts.

### General

**Name**, a brief description to recognize this Dispatchable Location.

**Country**, the country for this Dispatchable Location.

**Street Address**, this is the street for this Dispatchable Location.

**Address type**, the type of address for this location.

**City**, the city for the location.

**State**, State, Province or Region.

**Postal/ZIP Code**, ZIP Code to be used for the location.

**Caller ID**, Caller ID to be used for this location. In case the Emergency CID for the device or extension is not used, this is the CID used.

**Default**, if enabled set the location as the default Dispatchable Location for new extensions.

## 6.10 Pass-Through

With the Passthrough add-on module, you can connect traffic between two trunks together. This allows you to monitor this traffic on the CDR, and even allow you to use VitalPBX as a man in the middle, and record calls for a third-party PBX system.

### 6.10.1 PT Trunks

#### General

The screenshot shows the 'PT Trunks' configuration form. The 'GENERAL' tab is active. It contains the following fields:

- Description \***: A text input field.
- Private Trunk**: A dropdown menu with 'Lns Enitsl' selected.
- Public Trunk**: A dropdown menu with 'Lns Enitsl' selected.
- Save**: A green button with a floppy disk icon.

**Description**, this is a brief description to recognize the Passthrough Trunks.

**Private Trunk**, this is the trunk that goes towards a private trunk, being another PBX, for example.

**Public Trunk**, this is a trunk that generally goes towards a PSTN.

### 6.10.2 PT Extensions

#### General

The screenshot shows the 'PT Extensions' configuration form. The 'GENERAL' tab is active. It contains the following fields:

- Extension Owner**: A text input field.
- Extension**: A text input field.
- Incoming DID**: A text input field.
- Record Incoming**: A toggle switch set to 'Yes'.
- Record Outgoing**: A toggle switch set to 'Yes'.
- Save**: A green button with a floppy disk icon.

**Extension Owner**, name of the extension you wish to monitor.

**Extension**, the number of the extension to monitor.

**Incoming DID**, the incoming DID that is related to the Extension monitored.

**Record Incoming**, if this is enabled, then calls incoming from the declared DID towards the Extension Number will be recorded.

**Record Outgoing**, if this is enabled, you can record outgoing calls from the extension declared.

## 6.11 End Point Manager

The Endpoint Manager allows you to centrally manage the configuration settings for all IP devices that can be accessed on the network.

This provisioning system from Version 3 and onward is an add-on that you need to install post-installation.

It is important to note that IP phones are identified in the Endpoint Manager by their MAC address. This provides you with a powerful tool to pre-provision IP phones before the phones are even connected to the network. This can be done without even opening the box containing the phone, as phone manufacturers typically print the MAC address on the outside of the packaging.

There are a small number of simple tasks that you will need to complete in order to make the Endpoint Manager fully operational:

Ensure that your DHCP server is correctly configured to support Option 66, and that the format of Option 66 address is compatible with the Endpoint Manager.

Create an entry in the Host Settings dialog to define:

Host address of your PBX server

Ports used by SIP, IAX2, HTTP, and HTTPS protocols

Addresses of DNS and NTP server/s

Create a Template for each group of phone models that you want to manage and link it to a set of Host Settings. (You do not need to create a template for every IP phone in the system, only for groups of phones. For example, if you are supporting two different models of Xorcom phones, you would need to create two templates – one for each model.

Use the Device Mapping dialog to scan your network for available phone devices. You can also manually add devices that the network discovery cannot find.

Link each device that you want to manage to a template and to one (or more) PBX extensions

### 6.11.1 Host Settings

The Host Settings dialog allows you to configure one or more sets of parameters that can be used when configuring phones. This provides Endpoint Manager with information about the environment to which the phones belong. For example, you may have one template for IP phones that reside on the same network segment as your PBX server, and another template for phones that are located on a different segment. Why would you want to do this? For example, you may use port forwarding for external SIP connections so that external SIP phones can be forwarded from port 6050 to port 5060, whereas internal phones (that reside on the same network as the PBX server) directly access port 5060.



Host Settings

GENERAL

Host Settings

Name	Hostname / IP Address	SIP Port	IAX2 Port	HTTP Port	HTTPS Port
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Add

Save

**Name**, this helps to simplify maintenance: each host setting should be identified with a unique label.

**Hostname/IP Address**, this is the address of your PBX server. Note that the IP address used by phones that reside on the same network as PBX may be different from the address used by phones that are outside the network. Phones that are on the same network can use the physical address of PBX, even if it is a private IP address. Phones that are outside the network will need to use a publicly accessible IP address or hostname.

**SIP Port**, typically 5060, is the port that IP phones will access when using SIP protocol. Phones that are on the same network as your PBX typically use the default port, while phones that are outside the local network may utilize port-forwarding to use a different port. There is no default value if this field is left blank: if you do not type a value for this field, SIP phones will not work.

**IAX2 Port**, typically 4569, is the port that IP phones will access when using IAX2 protocol. Phones that are on the same network as your PBX typically use the default port, while phones that are outside the local network may utilize port-forwarding to use a different port. There is no default value if this field is left blank: if you do not type a value for this field, IAX2 phones will not work.

**HTTP Port**, typically 80, is the port that IP phones will use for HTTP access. Phones that are on the same network as your PBX typically use the default port, while phones that are outside the local network may utilize port-forwarding to use a different port. There is no default value if this field is left blank.

**HTTPS Port**, typically 443, is the port that IP phones will use for HTTPS access. Phones that are on the same network as your PBX typically use the default port, while phones

that are outside the local network may utilize port-forwarding to use a different port. There is no default value if this field is left blank.

## 6.11.2 Creating Template

You need to create at least one template for every model of IP phone that you want to manage. If you have phone models that use different host settings, you will need to create a template for each combination of phone model/host settings. You will need to create multiple templates, for example, when you want to use a different set of host settings (for the same model phone), or when you have phone models in different time zones.

**Template Name\***, this helps to simplify maintenance: each template should be identified with a unique name.

**Brand\***, select a Brand from the dropdown list of brands that are supported by Endpoint Manager. If you require a brand that does not appear in the dropdown list, you can contact support, by clicking on the Add new model support menu (on the right-hand side of the dialog).

**Model\***, select a Model from the dropdown list of models that are supported by Endpoint Manager. If you require a model that does not appear in the dropdown list, you can contact support, by clicking on the Add new model support menu (on the right-hand side of the dialog).

**Configuration Layout\***, this indicates what layout of configuration file you want to use. A very small number of phones may use more than one style of configuration file, depending on the firmware version that is installed.

**Host Settings\***, this allows you to select the name of the Host Settings (described above) that you want to use in this template.

**Time zone\***, this allows you to select the time zone offset to be used by all phones that use this template.

**Administrator Password\***, this is the password that can be used by users to manually access the configuration interface of IP phones based on this template. You should be aware of the limitation imposed by your IP Phone. For example, some IP phones will only accept the password as numeric digits. The Endpoint Manager does not validate whether the password will be acceptable by the phone: you must refer to the documentation for your specific phone.

## 6.11.3 Device Buttons

Allows you to configure the DSS (direct station select) buttons for IP phones that use this template.

The screenshot shows the 'Create Template' interface with the 'DEVICE BUTTONS' tab selected. It features two main sections: 'DSS Buttons' and 'Line Buttons'. Each section contains a table with columns for 'Label', 'Type', 'Value', and 'Line'. The 'DSS Buttons' section has 8 rows, and the 'Line Buttons' section has 3 rows. A 'Save' button is located at the bottom right of the interface.

The button types, which depend on the brand and model of IP phone that you are using, can include such types as:

- ACD
- BLF
- Call Park
- Call Pickup
- Call Return
- Conference
- DND
- DTMF
- Forward
- Hold

Intercom  
 Line  
 Local Directory  
 N/A  
 Record  
 Redial  
 Remote Directory  
 Speed Dial  
 Transfer  
 Voice Mail

Some phones do not support device buttons at all. In such cases, a suitable message will be displayed.

For some phones, such as Fanvil, the type has no significance (and will be ignored), as the type is included as a parameter in the Value field

## 6.11.4 Expansion Modules

Allows you to configure the DSS (direct station select) buttons on the expansion module for IP phones that have this hardware and use this template.

Note that each user can use My Extensions to define settings and overwrite the template definitions. This is a useful feature to allow users to personalize some buttons on their phone.

The number of buttons that are displayed are specific to each expansion module.

The screenshot shows a web interface titled "Create Template" with a close button (X). It features four tabs: "GENERAL SETTINGS", "DEVICE BUTTONS", "EXPANSION MODULES" (which is active and highlighted in green), and "ADVANCED SETTINGS". A hamburger menu icon is in the top right. Under the "EXPANSION MODULES" tab, there is a label "Select module to attach" next to a dropdown menu showing "GXP2200EXT". To the right of the dropdown is a green "Add Module" button. Below this is a section labeled "Attached Modules" which is currently empty. At the bottom right of the interface is a green "Save" button with a floppy disk icon.

For some phones, such as Fanvil, the type has no significance (and will be ignored), as the type is included as a parameter in the Value field.

## 6.11.5 Advanced Settings

Advanced Settings allows you to manage the configuration file for phones that belong to this template. Advanced Settings provides access to parameters that are not directly managed by the Endpoint Manager. Codec settings would be an example

of such a parameter. Manufacturers' default values, where applicable, are already defined in the file. You would only need to modify values in the configuration file if you want to define some non-standard behavior.

Parameter	Value
P2	admin
P3	
P8	0
P9	192
P10	168
P11	0
P12	100
P13	255
P14	255
P15	0

## 6.11.6 Device Mapping

This dialog manages your devices. The devices that you want to manage can be automatically discovered. Type in a target network segment and mask, such as 192.168.25.0/24, and click on Scan subnet for devices. The discovery will take some time, depending on the number of addresses that can potentially exist on the subnet. Be careful not to use a mask that is too big, as this will impact the time required to complete the discovery process. If devices cannot be discovered by scanning the network, you can manually enter the MAC address of any phones that you want to manage.

Checking on Only show recognized devices will filter out any devices having a MAC address that is not defined in the Endpoint Manager database as an endpoint device.

x
Device Mapping

**GENERAL SETTINGS**

Search Devices  Q

Assigned Devices

**MAC Address Brand Model Template Devices**

Reboot Selected Devices

Unassigned Devices

Scan Subnet for Devices

Show Known Devices Only

MAC Address	IP Address	Brand	Model	Template	Devices
00:0b:82:48:f4:7b	192.168.31.28	GrandStream ▾	▾	▾	
00:0b:82:55:ef:3a	192.168.31.2	GrandStream ▾	▾	▾	
00:0b:82:5e:4e:ca	192.168.25.162	GrandStream ▾	▾	▾	
00:0b:82:5e:4e:cb	192.168.24.250	GrandStream ▾	▾	▾	
00:0b:82:5e:4f:b4	192.168.26.100	GrandStream ▾	▾	▾	
00:0b:82:66:3f:2f	192.168.31.4	GrandStream ▾	▾	▾	
00:0b:82:72:b2:59	192.168.25.190	GrandStream ▾	▾	▾	
00:0b:82:77:22:7a	192.168.31.27	GrandStream ▾	▾	▾	
00:0b:82:78:df:83	192.168.31.14	GrandStream ▾	▾	▾	
00:0b:82:7b:b0:37	192.168.25.102	GrandStream ▾	▾	▾	

Save

## 6.12 Communicator

This add-on named “Communicator” that allows creating simple outbound campaigns in conjunction with the VitalPBX Communicator Softphone.

### 6.12.1 Softkey Profiles

In combination with VitalPBX Communicator (Desktop Softphone) centralized profiles are created in the dynamic key PBX and when modified in VitalPBX they affect the Softphone.

Softkey Profiles

GENERAL

Description \*

Softkey	Status	Actions
1	Unconfigured	
2	Unconfigured	
3	Unconfigured	
4	Unconfigured	
5	Unconfigured	

Save

The different types of keys it has are:

**BLF**, it supervises an extension or service that has the capacity of BLF in the PBX.

**Speed Dialing**, it is used to enter numbers that we want to dial by pressing the key

**Auto Answer**, it has two states, activate the auto answer function or deactivate it

**Record Call**, key to record call on the same phone

**Queues-Agent Login**, key to log in to the queues that the extension belongs to, the same key is also used to log out.

**Queues-Agent Pause**, key to pause the queues belonging to the extension, the same key is also used to remove the pause.

**Redial**, it is used to call the last number dialed.

**Account**, it is used to change the softphone registration account, very useful for sharing the same computer with several agents.

**Dialer**, it is used to activate / deactivate the Dialer campaign.

**Description**, main key description.

**Idle Value**, value that is executed when the key is pressed for the first time. If it were a BLF, for example for the do not disturb action, this value would be DND\_EXT (EXT -> Extension). In the cases of Account, Redial, Dialer Record Call and Auto Answer it is left blank

**Active value**, value that is executed when the key has already been pressed. If it were a BLF, for example for the do not disturb action, this value would be DND\_EXT (EXT -> Extension). In the cases of Account, Redial, Dialer Record Call and Auto Answer it is left blank

**Idle Label**, short text to show in normal state. Maximum 7 characters.

**Active Label**, short text to show in active state. Maximum 7 characters.

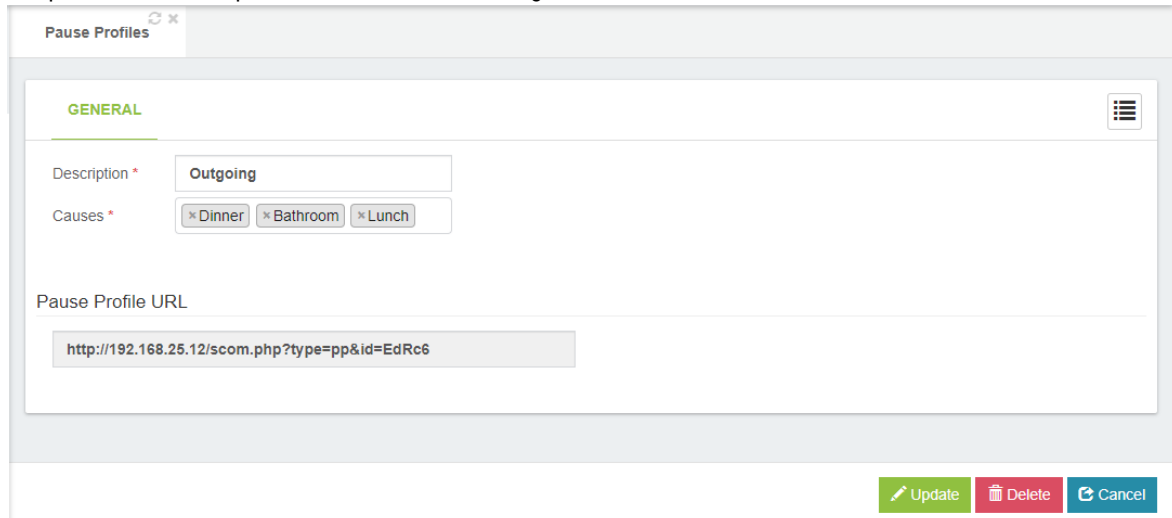
**Idle Title**, description to show in normal state.

**Active Title**, description to show in active state.



## 6.12.2 Pause Profiles

For statistics, the cause of pause of the agents is often necessary, so it is necessary to create pause cause profiles that can be synchronized with VitalPBX Communicator.



The screenshot shows a web interface for configuring a pause profile. The title bar reads "Pause Profiles" with a refresh icon and a close button. The main content area is titled "GENERAL" and contains three fields: "Description \*" with the value "Outgoing", "Causes \*" with three tags: "Dinner", "Bathroom", and "Lunch", and "Pause Profile URL" with the value "http://192.168.25.12/scom.php?type=pp&id=EdRc6". At the bottom right, there are three buttons: "Update" (green), "Delete" (red), and "Cancel" (blue).

The options to consider are the following,

**Description**, brief profile description.

**Causes**, allows you to setup different cause of pauses separated by comma.

**Pause Profile URL**, URL to retrieve the pause profile settings, this URL is configured in VitalPBX Communicator.

## 6.12.3 Campaigns Result Profiles

To be able to quantify the result of the campaign it is necessary that each call be assigned a result of it, this is where the results profiles are created.

Campaigns Result Profiles

**GENERAL**

Description \*

Results

Result	Type
<input type="text" value="Answered"/>	<input type="text" value="Positive End"/>
<input type="text" value="Dropped"/>	<input type="text" value="Negative End"/>
<input type="text" value="Call Later"/>	<input type="text" value="Rescheduled"/>

The options to configure are the following:

**Description\***, brief description to identify this profile.

### Results

**Result**, brief description of the result of the call.

**Type**, the result type. You have the following options

- Positive End, it means that the management was successful and that the desired person was contacted.
- Negative End, it means that the management was not successful and that the desired person could not be reached.
- Rescheduled, the call is scheduled to call later or another day.

## 6.12.4 Campaigns

Now we are going to create the marketing campaign for which it is necessary to fill in the following information.

The screenshot shows the 'Campaigns' configuration page. The 'GENERAL' tab is active. It contains the following fields and controls:

- Description \***: A text input field.
- Result Profile**: A dropdown menu with 'Default' selected.
- Contacts List \***: A text input field with a file upload icon.
- Wrap-up Time**: A dropdown menu with '0 Seconds' selected.
- Enabled**: A toggle switch set to 'Yes'.

At the bottom of the form, there are two buttons: 'Download CSV Format' (blue) and 'Save' (green).

**Description**, Short campaign description.

**Result Profile**, it allows you to select a profile with the available results during a campaign.

**Contacts List**, a CSV file with the list of contacts to be added on this campaign.

**Wrap-up Time**, this represents the time spent by an agent doing After Call Work (ACW) once they have concluded an interaction.

**Enable**, if set to no, this campaign will be not listed on communicator softphones.

**Download CSV Format**, if we want to have a sample of the format of the list to upload in Contacts List press this button.

	A	B	C	D	E	F	G	H
1	Phone	First Name	Last Name	Company	Address	Job Title		
2								
3								
4								
5								

## 6.13 Virtual Faxes

With this module it is possible to send faxes from the VitalPBX interface, as well as to receive faxes in our PBX so that they can be read in the VitalPBX interface.

### 6.13.1 Fax Devices

In this screen where fax devices are created which can be associated with an extension.

The screenshot shows a web form for creating a fax device. The form is titled "Fax Devices" and has a "GENERAL" tab selected. The form contains the following fields:

- Description \* (text input)
- Associated Email \* (text input)
- Class of Service (dropdown menu, currently set to "All Permissions")
- CID Name \* (text input)
- CID Number \* (text input)
- Country Code (text input, currently set to "1")
- Area Code (text input, currently set to "754")

A "Save" button is located at the bottom right of the form.

**Description**, Short description to identify this fax device.

**Associated Email**, Email to receive notifications and faxes.

**Class of Service**, Class of service to use for routing outbound faxes.

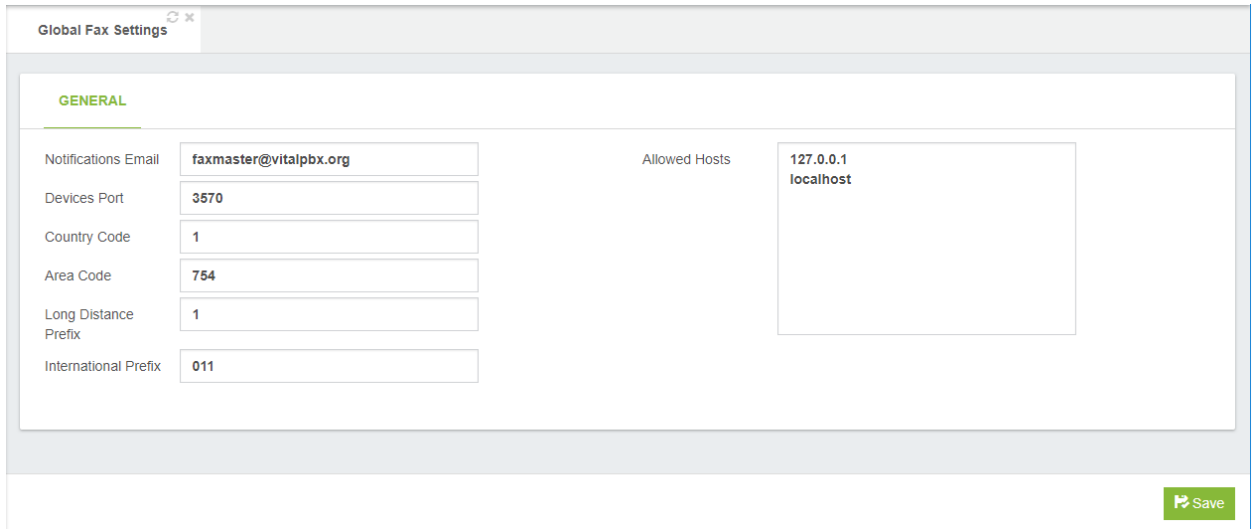
**CID Name**, CID Name to use when a fax is sent.

**CID Number**, CID Number to use when a fax is sent.

**Country Code**, country code.

**Area Code**, area code.

## 6.13.2 Global Fax Settings



The screenshot shows a web browser window titled "Global Fax Settings". The form is divided into a "GENERAL" section. On the left, there are input fields for "Notifications Email" (filled with "faxmaster@vitalpbx.org"), "Devices Port" (filled with "3570"), "Country Code" (filled with "1"), "Area Code" (filled with "754"), "Long Distance Prefix" (filled with "1"), and "International Prefix" (filled with "011"). On the right, there is a text area for "Allowed Hosts" containing "127.0.0.1" and "localhost". A green "Save" button is located at the bottom right of the form.

**Notifications Email**, Email address who will receive notifications of received messages, errors and activity summary of the Fax Server.

**Device Port**, the port that fax devices listen.

**Country Code**, country code.

**Area Code**, area code.

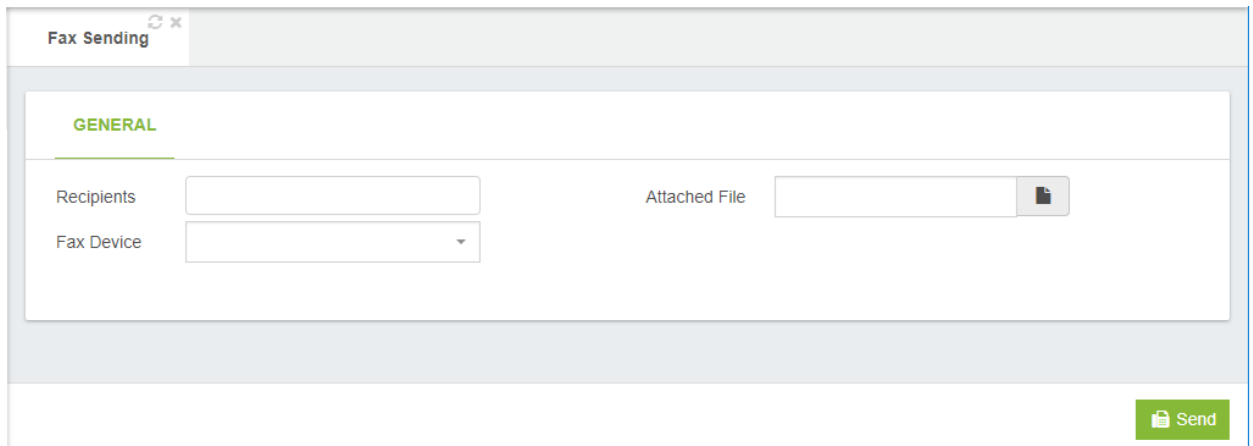
**Long Distance Prefix**, long distance dialing prefix (1 in US).

**International Prefix**, international dialing prefix (011 in US).

**Allow Hosts**, specifies the hosts that are allowed to send faxes.

## 6.13.3 Fax Sending

From this form it is possible to send a fax to a telephone or extension, either on the same PBX or outside it to a fax machine or virtual fax.



The screenshot shows a web browser window titled "Fax Sending". The form is divided into a "GENERAL" section. On the left, there are input fields for "Recipients" and "Fax Device" (a dropdown menu). On the right, there is an "Attached File" field with a file upload icon. A green "Send" button is located at the bottom right of the form.

**Recipients**, numbers to which the fax will be sent.

**Fax Device**, fax device to use for sending the fax.

**Attached File**, file to send through the fax device. The supported formats are: PDF, TIFF, TXT.

## 6.13.4 Fax Viewer

In this screen we can see the list of faxes received by a specific device with a specific date range.

The screenshot shows the 'Fax Viewer' interface. At the top, there is a 'GENERAL' section with filter options: 'Fax Device' (dropdown menu set to '-- All Devices --'), 'Type' (dropdown menu set to '-- All Types --'), 'Start Date' (text input field with '2019-02-01 00:00:00'), and 'End Date' (text input field with '2019-02-18 23:59:59'). Below these filters is a 'Faxes List' section. It includes a 'Show 10 entries' dropdown, a search box, and a table with columns: 'Date / Time', 'Fax Device', 'Type', 'Sender', 'Recipient', 'Fax File', and 'Actions'. The table is currently empty, displaying 'No data available in table'. At the bottom of the list, it says 'Showing 0 to 0 of 0 entries' and has 'Previous' and 'Next' buttons. A green 'Search' button is located at the bottom right of the interface.

**Fax Device**, this allows you to filter the fax list per device.

**Type**, this allows you to filter the fax list by type.

**Start Date**, allows you to filter the fax list by date.

**End date**, this allows you to filter the fax list by date.

# 7. Reports

## 7.1 CDR Reports

### 7.1.1 CDR Filters

#### General

CDR Filters

**GENERAL**

Description \*  Talk Time From  To

Duration From  To

Add Search Condition \*

Condition	Search By	Value	Exclude	Mode
<input type="checkbox"/> AND	Caller ID	<input type="text"/>	<input type="checkbox"/> No	Begins With

Add

Save

**Description\***, short description for this filter.

**Duration**, call duration range in seconds.

**Talk Time**, talk time range in seconds.

#### Add Search Condition Section

Clicking on the Add button allows you add additional search conditions.

**Condition**, this determines whether the condition is enabled or not. AND → it means that this value has to be met in conjunction with the previous one and so on, OR → means that this value or the previous one must be met.

**Search By**, search for the selected field using one of the items selected from the drop-down list:

- Caller ID
- Source
- Destination
- Account Code

- Status
- Customer Code

**Value**, value of the selected field.

**Exclude**, include or exclude the selected value in the search.

**Mode**, search condition can be filtered in a number of methods, which can be selected from the drop-down list:

- Begins With
- Contains
- Ends With
- Exactly

## 7.1.2 View CDR Reports

### General

The screenshot shows the 'CDR' report interface. At the top, there's a 'GENERAL' section with filter options. The 'Filter' dropdown is set to 'None'. The 'From' date is '2020-01-01 00:00:00' and the 'To' date is '2020-05-13 23:59:59'. Below the filters, there are 'Call Records' with options to export to 'CSV' or 'PDF'. A table displays the call records with columns: Date / Time, Caller ID, From, To, Call Type, Duration, Talk Time, Account Code, Customer Code, Status, and CEL Events. The table shows several records, including internal calls and one with a warning status. A 'Refresh' button is located at the bottom right of the table area.

Date / Time	Caller ID	From	To	Call Type	Duration	Talk Time	Account Code	Customer Code	Status	CEL Events
2020-05-09 20:11:08	"Maynor Peralta" <2000>	2000	2005	Internal	00:00:35	00:00:35			📞	🔊
2020-05-09 20:11:08	"Rodrigo Cuadra" <2004>	2004	2000	Internal	00:01:15	00:01:05			📞	🔊
2020-05-09 19:58:40	"Rodrigo Cuadra" <2004>	2004	+50578961838	Internal	00:00:00	00:00:00			⚠️	🔊
2020-05-09 19:53:11	"Maynor Peralta" <2000>	2000	*72	Internal	00:00:40	00:00:40			📞	🔊
2020-05-09 19:52:24	"Maynor Peralta" <2000>	2000	2004	Internal	00:01:53	00:01:47			📞	🔊
2020-05-09 19:42:10	"Rodrigo Cuadra" <2004>	2004	2000	Internal	00:02:35	00:02:20			📞	🔊
2020-05-09 19:15:34	"Rodrigo Cuadra" <2004>	2004	2000	Internal	00:02:27	00:02:17			📞	🔊
2020-05-01 11:54:41	"PBX Operator" <100>	0	3021	Internal	00:00:00	00:00:00			⚠️	🔊

### Filters section

**Filter**, filter, defined in Report Filters dialog, to be used in the report.

**From**, include records starting from this date and time.

**To**, include records ending by this date and time.

**Source**, call source.

**Destination**, dialed number.



## Reports section

**Record Per Page**, set the number of records that should be displayed on each page.  
**PDF, CSV**, export the report in PDF or CSV.

## CEL Event

CEL Events allow you trace the call's steps from the moment it entered the PBX, to when the call was tended to.

Event Time	Event Type	CID Name	CID Number	Dialed Number	Extension	Context	Application
2020-05-09 20:11:08	CHAN_START	Rodrigo Cuadra	2004		2000	cos-all	
2020-05-09 20:11:08	APP_START	Rodrigo Cuadra	2004	2000	2000	sub-local-dialing	Dial
2020-05-09 20:11:08	CHAN_START	Maynor Peralta	2000		s	cos-all	
2020-05-09 20:11:19	ANSWER	Maynor Peralta	2000		2000	cos-all	AppDial
2020-05-09 20:11:19	ANSWER	Rodrigo Cuadra	2004	2000	2000	sub-local-dialing	Dial
2020-05-09 20:11:19	BRIDGE_ENTER	Maynor Peralta	2000			cos-all	AppDial
2020-05-09 20:11:19	BRIDGE_ENTER	Rodrigo Cuadra	2004	2000	2000	sub-local-dialing	Dial
2020-05-09 20:12:24	BLINDTRANSFER	Rodrigo Cuadra	2004	2000	2000	sub-local-dialing	Dial
2020-05-09 20:12:24	BRIDGE_EXIT	Rodrigo Cuadra	2004	2000	2000	sub-local-dialing	Dial
2020-05-09 20:12:24	HANGUP	Rodrigo Cuadra	2004	2000	h	sub-local-dialing	
2020-05-09 20:12:24	CHAN_END	Rodrigo Cuadra	2004	2000	h	sub-local-dialing	
2020-05-09 20:12:24	BRIDGE_EXIT	Maynor Peralta	2000		2005	cos-all	AppDial
2020-05-09 20:12:24	APP_START	Maynor Peralta	2000		2005	sub-local-dialing	Dial
2020-05-09 20:12:24	APP_START	Maynor Peralta	2000		s	sub-vm	VoiceMail
2020-05-09 20:13:00	HANGUP	Maynor Peralta	2000		h	sub-local-dialing	AppDial
2020-05-09 20:13:00	CHAN_END	Maynor Peralta	2000		h	sub-local-dialing	AppDial

## 7.2 PBX Reports

### 7.2.1 Active Calls

Shows the ongoing calls in real-time with the following details:

Channel	Caller ID	Called Number	State	Duration	LinkedID
PJSIP/2000-00000000	"Boss" <2000>	*71	Up	00:04	1598030479.0

**Channel**, channel through which the call is taking place.

**Caller ID**, CID of the person that placed the call.

**Called Number**, Number of the person being called.

**State**, current state of the call.

**Duration**, running duration for the call.

**Linked ID**, Unique ID that links two channels to the same call

## 7.2.2 PJSIP Devices

Shows the status of the endpoints with the following information:

Extension	Endpoint	Contacts	Max Contacts
2000 - Boss	2000	sip:2000@192.168.0.224:5070	1

**Extension,** Extension number and name.

**Endpoint,** Endpoint user.

**Contacts,** Registered contact with its origin and port.

**Max Contacts,** Max number of contacts for this user.

We can also see the PJSIP Trunks with the following information:

**Trunk Description,** description for the PJSIP Trunk to monitor.

**Endpoint,** endpoint user.

**Contacts,** the different remote contacts that are connected to this trunk.

**Match,** this value is a list of IP addresses or Hostnames separated by commas. The IP Addresses can have a subnet mask attached. The subnet mask can be written in CIDR or octets.

We can then see the Outbound Registrations with the following information:

**Trunk Name,** description of the PJSIP trunk to monitor.

**Endpoint,** endpoint user.

**Client URI,** this is the registration address for the outbound registration, meaning, the URI on the REGISTER header. To register with an ITSP, the SIP Client URI can be formed by an account name or number and the hostname for the provider, for example, 1234567890@example.com. This may vary between providers.

**Server URI,** this is the URI to find the registrar and send the outgoing REGISTER request. This URI is used as the request URI for the outgoing REGISTER request from Asterisk. For the registration of the ITSP, the configuration can be the registrar's domain, for example, sip:sip.example.com.

**Status,** current status for the connection.

## 7.2.3 SIP Devices

Shows the status for the SIP Devices with the following information:

Extension	Device	Host	Port	Status	User Agent
2001 - Secretary	2001		0	UNREGISTERED	

**Extension,** Extension number and name.

**Device,** user device for the extension.

**Host**, from where the user is registered from.

**Port**, port used to register the user device.

**Status**, user status.

**User Agent**, User agent sent by the user. With this information we can know the make and model from the phone the user is registered from.

Then, we can see the Available SIP Trunks with the following information:

**Trunk Description**, brief description of the trunk to monitor.

**Device**, device connected to this account.

**Host**, IP Address from where the the registration comes from.

**Port**, port used for the registration.

**Status**, device status. This indicates the response time.

Finally, we can see the different registrations with the following information:

**Device**, device connected to this account.

**Host**, IP Address from where the registration is coming from.

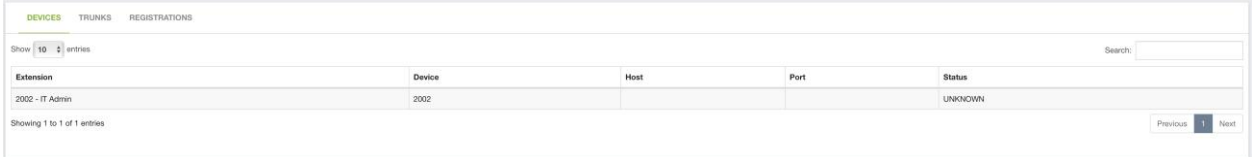
**Port**, port used for the registration.

**Refresh**, how often there is a registration request.

**Status**, device status. Indicated the response time.

## 7.2.4 IAX2 Devices

Shows the status of the different IAX2 Devices with the following information:



Extension	Device	Host	Port	Status
2002 - IT Admin	2002			UNKNOWN

**Extension**, Extension number and name.

**Device**, user device for the extension.

**Host**, from where the user is registered from.

**Port**, port used to register the user device.

**Status**, user status.

Then, we can see the Available IAX2 Trunks with the following information:

**Trunk Description**, brief description of the trunk to monitor.

**Device**, device connected to this account.

**Host**, IP Address from where the registration comes from.

**Port**, port used for the registration.

**Status**, device status. This indicates the response time.

Afterwards, we can see the different registrations with the following information:

**Device**, device connected to this account.

**Host**, IP Address from where the registration is coming from.

**Port**, port used for the registration.

**Refresh**, how often there is a registration request.

**Status**, device status. Indicated the response time.

Finally, we can see the status of Faxes using IAX2. This will only be available when using the Virtual Faxes add-on:

**Description**, brief description of the Device to monitor.

**Device**, device connected to this account.

**Host**, IP Address from where the registration comes from.

**Port**, port used for the registration.

**Status**, device status. This indicates the response time.

## 7.3 IVR Stats

### 7.3.1 IVR Stats

When we install the IVR statistics module, this option will appear in the Reports menu.

With this module it is possible to obtain statistics of how many times each option is pressed in the IVR, this is very useful to determine which options are not being used in the IVR.

Another application is that of surveys, since this module in combination with the call queue allows us to carry out satisfaction surveys in our Call Center:

The screenshot shows the IVR Stats interface with the following components:

- Filters:** IVR dropdown set to 'IVR\_LABORAL', End Date '2020-05-13', and Start Date '2020-05-01'.
- Summary Table:**

Option	Pressed Times
1	5
260	2
3	3
8072	1
- Detailed Table:**

Call Date	Option	Caller	Callee	Call Duration	Call Status
2020-05-13 09:10:49	8072	--	--	--	ivr_stats.no_cdr
2020-05-13 08:38:58	1	--	--	--	ivr_stats.no_cdr
2020-05-12 13:58:17	1	--	--	--	ivr_stats.no_cdr
2020-05-12 10:39:16	1	--	--	--	ivr_stats.no_cdr
2020-05-11 13:54:46	260	--	--	--	ivr_stats.no_cdr
2020-05-08 12:08:54	1	--	--	--	ivr_stats.no_cdr
2020-05-08 12:08:00	3	--	8253	00:00:44	NO ANSWER
2020-05-08 11:39:09	3	--	8253	00:00:38	ANSWERED
2020-05-06 16:29:11	3	--	8253	00:00:43	NO ANSWER
2020-05-04 15:54:13	260	--	--	--	ivr_stats.no_cdr
- Navigation:** 'Showing 1 to 10 of 11 entries' and pagination buttons (Previous, 1, 2, Next).
- Export:** 'CSV' buttons for both summary and detailed views.
- Search:** A search bar at the bottom right.

It also gives us the facility of being able to export the data to CSV

## 7.4 Call Center Reports

### 7.4.1 Queues Call Back Reports

When we install the Queues Call Back add-on module, we will now have this option on the Reports Menu.

On this report we will see the calls that are queued to be called back. These calls opted for this feature while waiting in Queue on our Call Center.

Queues CallBack Report

**REPORT**

Queue CallBack: All

Status:  Queued  In Progress  Successful  Failed

Start Date: 2020-09-01 00:00:00

End Date: 2020-09-02 23:59:59

Scheduled Queue Callbacks

Search:

Date & Time	CallBack Queue	CallBack Requester Name	CallBack Number	Tries	Status	Actions
No data available in table						

Showing 0 to 0 of 0 entries

Previous Next

Refresh

Here you can see the following information:

**Queue Callback**, here you can select the Queue Callback you wish to monitor.

**Status**, here you select the status you want to filter from.

**Start Date**, from when you wish to see the report.

**End Date**, when you want the report to end.

#### Scheduled Queue Callbacks Section

These are all of the Callbacks scheduled based on the filters input above.

**Date & Time**, this is the date and time the Callback was Scheduled.

**Callback Queue**, the queue where the callback will be sent to.

**Callback Requester Name**, the CID name for the Callback requester.

**Callback Number**, the number to which the callback will be made to.

**Tries**, the number of tries the PBX has made to reach the callback number.

**Status**, the current status for the callback.

**Actions**, actions you can do to this callback. In this case, delete it.

# 8. Settings

## 8.1 Technology Settings

### 8.1.1 PJSIP Settings

The PJSIP Settings is used to configure the default value to be used for PJSIP calls.

#### General

The screenshot shows the 'PJSIP Settings' interface with the 'GENERAL' tab active. The configuration is as follows:

Field	Value
Debug	No
Bind	0.0.0.0, 5060
TLS Bind	0.0.0.0, 5061
Certificate	itexpo2020.vitalpbx.org
SSL Method	tlsv1
Timer T1	500
Timer B	32000
Disable TCP Switch	Yes
Verify Client	No
Verify Server	No
Local Net	
External Media Address	
External Signal Address	

**Debug**, Enable/Disable SIP debug logging.

**Bind**, IP Address and optional port to bind to for this transport.

**TLS Bind**, IP Address and optional port over TLS protocol to bind to for this transport.

**Certificate**, path to certificate file to present to peer.

SSL Method, method of SSL transport (TLS ONLY).

**Timer T1**, timer T1 is the base for determining how long to wait before retransmitting requests that receive no response when using an unreliable transport (e.g. UDP). Note: Because this value is system, it will only be applied when the Asterisk service is restarted.

**Timer B**, timer B determines the maximum amount of time to wait after sending an INVITE request before terminating the transaction. Note: Because this value is a system value, it will only be applied when the Asterisk service is restarted.

**Disable TCP Switch**, disable automatic switching from UDP to TCP transports if outgoing request is too large. Note: Because this value is a system value, it will only be applied when the Asterisk service is restarted.

**Verify Client**, require verification of client certificate (TLS ONLY).

**Verify Server**, require verification of server certificate (TLS ONLY).

## Nat Settings Section

**Local Net**, network to consider local (used for NAT purposes).

**External Media Address**, external IP address to use in RTP handling.

**External Signal Address**, external address for SIP signaling.

## 8.1.2 SIP Settings

The SIP Settings is used to configure the default value to be used for SIP calls.

### General

The screenshot shows the 'SIP Settings' web interface with the 'GENERAL' tab selected. The interface is organized into several sections:

- Language:** English (en)
- Tone Zone:** (us) United States / North America
- G726-32 Audio:** No
- Notification Settings:**
  - Notify Ringing: Yes
  - Notify Hold: No
  - Notify CID: No
- Registration Settings:**
  - Max Expiry: 3600
  - Min Expiry: 60
  - Default Expiry: 120
  - MWI Expiry: (empty)
- Bind Address:** 0.0.0.0 (IP) and 5062 (Port)
- Allow Transfer:** Yes
- Enable Websocket:** No
- Video Settings:**
  - Video Support: Yes
  - Max Call BitRate: 384
- Fax Settings:**
  - Fax Detect: No
  - T.38 Fax Pass-Through: No

A 'Save' button is located at the bottom right of the form.

**Language**, default language setting for all users/peers. This may also be set for individual users/peers.

**Tone Zone**, default tone zone for all users/peers.

**G726-32 Audio**, if the peer negotiates G726-32 audio, use AAL2 packing order instead of RFC3551 packing order (this is required for Grandstream ATAs, among others).



**Bind Address**, IP address to which the device should bind. Note that 0.0.0.0 binds to all IP addresses.

**Bind Port**, port to which the device should bind. The standard SIP port is 5060.

**Allow Transfer**, disables all transfers (unless specifically enabled in peers or users). Default setting is enabled. Note that the dial options 't' and 'T' are not related as to whether SIP transfers are allowed or not.

**Enable Websocket**, set to “No” by default, so SIP Channels do not listen for a WebSocket. This is necessary when SIP and PJSIP WebSockets are used on the same system.

## Notification Settings Section

**Notify Ringing**, controls whether busy subscribers get sent a RINGING message when another call is sent.

**Notify Hold**, notify subscribers that are in HOLD state.

**Notify CID**, controls whether caller ID information is sent together with dialog-info+xml notifications (supported by Snom phones).

## Video Section

**Video Support**, this turns on or off support for SIP video. You need to turn this on to get any video support at all.

**Max Call Bitrate**, maximum bitrate for video calls (default 384 kb/s)

## Registration Settings Section

**Max Expiry**, maximum allowed time, in seconds, for incoming registrations.

**Min Expiry**, minimum time, in seconds, for registrations.

**Default Expiry**, default length of incoming/outgoing registration.

**MWI Expiry**, expiry time for outgoing MWI subscriptions.

## Fax Settings Section

**Fax Detect**, when active, enables (both CNG and T.38) detection of inbound faxes.

**T.38 Fax Pass-Through**, enables T.38 with FEC error correction. Overrides the other values provided for the endpoint, so we can send 400-byte T.38 FAX packets to it.

## Security

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

Setting	Value
Allow Guest	No
Failure Events	No
Always Reject	Yes
Auto-Domain	No
Allow Msg Request	Yes
Disallow Dynamic Hosts	No
Allow External Domains	Yes

The 'SIP Domains' section contains a table with the following entry:

Domain
myasterisk.dom

Buttons for 'Add' and 'Save' are visible at the bottom right of the settings area.

**Allow Guest**, allow or reject guest calls. Do not activate this option unless you are sure what you are doing. By activating this option, you are allowing anyone to make a call to your PBX without having to register in it

**Failure Events**, these generate manager peer-status events when peer cannot authenticate with Asterisk. Peer-status will be rejected.

**Always Reject**, when rejecting an incoming INVITE or REGISTER call, for any reason, always reject with an identical response. This reduces the ability of an attacker to scan for valid SIP usernames.

**Allow Msg Request**, disable this option to reject all MESSAGE requests outside of a call. By default, this option is enabled, enabling MESSAGE requests to be passed to the dial-plan.

**Disallow Dynamic Hosts**, disallow all dynamic hosts from registering with any IP address used for statically defined hosts. This helps avoid the configuration error of allowing users to register with the same address as a SIP provider.

**Auto Domain**, this is an important setting with respect to SIP domains. When it is set to "no", Asterisk will only recognize domains that were explicitly defined or will simply not support SIP domains at all (if there were no explicitly defined domains). If you set it to "yes" please be aware that Asterisk will create a domain based on the external IP address of your firewall as specified in the "externip" parameter. This might represent a compromise on your SIP security. If you don't want a domain to be created based on "externip", then set to "no" and explicitly add domains for your local (internal) IP address and for any other domains you require.

**Allow External Domains**, tells Asterisk whether or not to allow SIP-to-SIP calls to non-local domains.

**SIP Domains**, when used, they provide enhanced security because registrations will only be accepted when they come from an IP phone (or other SIP client) that is using one of the recognized domains. When Asterisk knows the identity of all its local SIP domains, this allows a higher level of security in the routing of SIP-to-SIP calls too.

## Network

The screenshot displays the 'SIP Settings' window with the 'NETWORK' tab selected. The settings are organized into several sections:

- GENERAL:** Includes 'TCP Enable' (No), 'TCP Bind Address' (0.0.0.0, 5062), 'Enable TLS' (No), and 'TLS Bind Address' (0.0.0.0, 5063).
- SECURITY:** Includes 'TLS Do Not Verify' (No) and 'TLS Certificate' (PBX Certificate).
- NAT:** Includes 'NAT' (No), 'External Host', 'External Address', and 'External Refresh'.
- Local Networks:** A table with columns for 'IP Address' and 'Network Mask'. One entry is shown: IP Address: 0.0.0.0, Network Mask: 255.255.255.0. An 'Add' button is present to the right of the table.

At the bottom right of the window, there is a 'Save' button.

## General Section

TCP Enable, use TCP.

TCP Bind Address, IP address and optional port to bind for this transport.

Enabled TLS, enable TLS

TLS Bind Address, IP address and optional port to bind for this transport.

TLS Do Not Verify, if set to yes, don't verify the server's certificate when acting as a client.

TLS Certificate, the server's certificate file.

## NAT Section

**NAT**, NAT (Network Address Translation) is a technology most commonly used by firewalls and routers to allow multiple devices on a LAN with "private" IP addresses to share a single public IP address. A private IP address is an address, which can only be addressed from within the LAN, but not from the Internet outside the LAN.

Options:

- **No:** Do no special NAT handling other than RFC3581
- **Force:** Pretend there was an rport parameter even if there wasn't.
- **Comedia:** Send media to the port Asterisk received it from regardless of where the SDP says to send it.
- **Auto Force:** Set the force\_rport option if Asterisk detects NAT.
- **Auto Comedia:** Set the comedia option if Asterisk detects NAT.

**External Address**, specifies a static address, or address[:port] combination, to be used in SIP and SDP messages.

**External Host**, alternatively you can specify an external host, and Asterisk will perform DNS queries periodically. Not recommended for production environments, Use "External Address" instead.

**External Refresh**, how often, in seconds, to refresh the "External Host," if used.

## Local Networks Section

**IP Address**, valid IP address to be used.

**Network Mask**, network mask to use.

## Codecs

SIP Settings

GENERAL SECURITY NETWORK **CODECS** OTHERS CUSTOM

Preferred Codec Only  No Auto Framing  No

Available Codecs Selected Codecs

Add all	Remove all
slin	ulaw
g726	alaw
gsm	g729
ilbc	h264
g723	opus
g726aal2	vp8
adpcm	h263p
lpc10	g722
speex	
h263	
h261	
vp9	
codec2	

Save

**Preferred Codec Only**, respond to a SIP invite with the single most preferred codec rather than advertising all codec capabilities. This limits the choice of codec by the remote side to exactly the codec that we prefer.

**Auto Framing**, this sets packetization based on the remote endpoint's (ptime) preferences.

**Available Codecs**, list of available codecs.

**Selected Codecs**, list of selected codecs.

**Note:** Click on + icons to move available codecs to list of selected codecs. Click on the x icon to remove codecs from the list of selected codecs. You can also select or remove all codecs by clicking on either the Add All or Remove All buttons.

## Others

The screenshot shows the 'SIP Settings' window with the 'OTHERS' tab selected. The tabs at the top are GENERAL, SECURITY, NETWORK, CODECS, OTHERS, and CUSTOM. The 'OTHERS' tab is highlighted in green.

**General**

- SRV Lookups:
- Qualify Frequency:

**SIP Debugging**

- SIP Debug:
- Record History:
- Dump History:

**SIP QoS**

- SIP TOS:
- Audio TOS:
- Video TOS:

**RTP Timers**

- RTP Timeout:
- RTP Hold Timeout:

**Jitter Buffer**

- Enabled:
- Force:
- Max Size:
- Resynchronized:
- Jitterbuffer implementation:
- Target Extra:

A green 'Save' button is located at the bottom right of the settings window.

### General Section

**SRV Lookups**, enables or disables DNS SRV lookups on outbound calls

**Qualify Frequency**, determines how often, in seconds, to check that the host is alive, as reported, in milliseconds, with sip show settings command.

### RPT Timers Section

**RPT Timeout**, sets the time, in seconds, to terminate the call if there is no RTP or RTCP activity on the audio channel.

**RPT Hold Timeout**, sets the time, in seconds, to terminate the call if there is no RTP or RTCP activity on the audio channel.

### SIP Debugging Section

**SIP Debug**, toggle SIP debugging, from the moment the channel loads this configuration.

**Record History**, toggles recording of SIP history.

**Dump History**, toggles dump SIP history at end of a SIP dialogue. SIP history is output to the DEBUG logging channel.

### Jitter Buffer Section

**Enabled**, enables or disables the use of a jitter-buffer on the receiving side of a SIP channel.

**Force**, this forces the use of a jitter-buffer on the receiving side of a SIP channel.

**Max Size**, maximum length, in milliseconds, of the jitter-buffer.

**Resynchronized**, gap in the frame timestamps, in milliseconds, beyond which the jitter-buffer will be resynchronized.

**Jitter-buffer Implementation**, this is used on the receiving side of a SIP channel.

There is a choice of two options:

**Fixed:** size always equals to jb-max-size

**Adaptive:** variable size, actually the new jb of IAX2.

**Target Extra**, this sets the time, in milliseconds, the new jitter buffer will pad its size.

This option only affects the jb when 'jbimpl = adaptive' is set.

## SIP QoS Section

**SIP TOS**, this sets the TOS for SIP packets.

**Audio TOS**, this sets the TOS for RTP audio packets.

**Video TOS**, this Sets the TOS for RTP video packets.

## Custom

The screenshot shows a web interface for SIP Settings. At the top, there is a tab labeled 'SIP Settings' with a refresh icon. Below the tab, there are several menu items: GENERAL, SECURITY, NETWORK, CODECS, OTHERS, and CUSTOM. The CUSTOM menu item is highlighted with a green underline. Below the menu items, there is a section titled 'Custom Options'. This section contains a table with two columns: 'Parameter' and 'Value'. Below the table, there is an 'Add' button. At the bottom right of the interface, there is a 'Save' button.

## Custom Options Section

**Parameter**, the SIP parameter to be included in the [general] section.

**Value**, value of the SIP parameter to be used.

## 8.1.3 IAX2 Settings

The IAX Settings is used to configure the default value to be used for IAX calls.

### General

The screenshot shows the 'IAX2 Settings' window with the 'GENERAL' tab selected. The settings are as follows:

Field	Value	Field	Value
Bind Address		ADSI	Yes
Bind Port	4569	SRV Lookup	No
Language	English (en)	Disable Checksums	Yes
Bandwidth	Low	IAX Compat	Yes

A 'Save' button is located at the bottom right of the settings panel.

**Bind Address**, IP address to which to bind. Note that 0.0.0.0 binds to all IP addresses.

**Bind Port**, port to which IAX2 should bind. The default port is 4570.

**Language**, this allows you to specify a global default language for all users who use this profile. This can be specified also on a per-user basis.

**Bandwidth**, here you can specify bandwidth (low, medium, or high) to control which codecs should be used.

**ADSI**, Analog Display Services Interface (ADSI) can be enabled if you have ADSI-compatible CPE equipment.

**SRV Lookup**, whether or not to perform SRV lookup on outbound calls.

**Disable Checksums**, disable use of UDP checksums. If no checksum is set, then checksum will not be calculated or checked on systems supporting this feature.

**IAX Compact**, set to yes if you plan to use layered switches or some other scenario which may cause a delay when performing a lookup in the dial-plan. This option causes Asterisk to spawn a separate thread when it receives an IAX2 DPREQ (Dial-plan Request) instead of blocking while it waits for a response.



## Registration

IAX2 Settings	
REGISTRATION	
Minimum Expire	60
Maximum Expire	60
IAX Thread Count	10
IAX Max Thread Count	100
Auto Kill	yes
Trunk Frequency	20
Authorization Debug	No
Trunk Time Stamps	Yes

Save

**Minimum Expire**, minimum time, in seconds, that IAX2 peers can request registration.  
**Maximum expire**, maximum time, in seconds, that IAX2 peers can request registration.

**IAX Thread Count**, establishes the number of IAX helper threads to handle I/O.

**IAX Max Thread Count**, establishes the maximum number of IAX helper threads that can be used to handle I/O. The Asterisk Manager Interface (AMI), establishes the number of extra dynamic threads that may be spawned to handle I/O.

**Auto Kill**, this is used to keep the system from stalling when a host is not available. In addition to 'yes' or 'no' you can also specify a number of milliseconds.

**Trunk Frequency**, sets how frequently, in milliseconds, trunk messages are sent. This means the trunk will send all the data queued to it in the past period. By increasing the time between sending trunk messages, the trunk's payload size will increase as well.

**Authorization Debug**, this enables authentication debugging, but will increase the amount of debug traffic.

**Trunk Time Stamps**, should we send timestamps for the individual sub-frames within trunk frames? There is a small bandwidth use for these (less than 1kbps/call), but they ensure that frame timestamps get sent end-to-end properly.

## Codecs

IAX2 Settings

GENERAL REGISTRATION **CODECS** SECURITY

Codec Priority:

Available Codecs

Add all	
adpcm	+
codec2	+
g722	+
g723	+
g726	+
g726aal2	+
gsm	+
h261	+
h263	+
h263p	+
lpc10	+
slin	+
speex	+

Selected Codecs

Remove all	
ulaw	×
alaw	×
g729	×
h264	×
ilbc	×
opus	×
vp8	×
vp9	×

**Codec Priority**, this controls the codec negotiation of an inbound IAX2 call. There are a number of options:

- **Caller:** consider the preferred order of the caller before considering the preferred order of the host.
- **Host:** consider the preferred order of the host before considering the preferred order of the caller.
- **Disabled:** disable the consideration of codec preference altogether.
- **Reqonly:** Behaves in a similar manner as the disabled option. The call will only be accepted if the requested format is available.

## Codecs Selection Section

**Available Codecs**, list of available codecs.

**Selected Codecs**, list of selected codecs.

**Note:** Click on + icons to move available codecs to list of selected codecs. Click on the x icon to remove codecs from the list of selected codecs. You can also select or remove all codecs by clicking on either the Add All or Remove All buttons.

## Security

The screenshot shows the 'IAX2 Settings' window with the 'SECURITY' tab selected. The 'GENERAL' tab is also visible. The 'SECURITY' section contains the following fields:

- Call Token Optional:
- Max Call Numbers:
- Max Non-validated Call Nos:

Below these is the 'Call Number Limits' section, which is a table with the following structure:

IP Address	Mask	Limit
0.0.0.0	255.255.255.0	100

There are 'Add' and 'Save' buttons at the bottom right of the form.

**Call Token Optional**, call token validation can be set as optional for a single IP address or a IP address range by enabling this option. This is a global option.

**Max Call Numbers**, this option limits the number of call numbers allowed for each individual remote IP address. Once an IP address reaches its call number limit, no more new connections are allowed until an existing connection is closed. This option can be used in a peer definition as well, but only takes effect for the IP of a dynamic peer after it completes registration

**Max Non-validated Call Nos**, they parameter is used to set the combined number of call numbers that can be allocated for connections where call token validation has been disabled. Unlike the Max Call Numbers option, this limit is not separate for each individual IP address. Any connection resulting in a non-call token validated call number being allocated contributes to this limit.

## Call Number Limits Section

**IP Address**, valid IP address to be used.

**Mask**, network mask to use.

**Limit**, this limits the number of call numbers allowed for this group of IP addresses. Once an IP address group reaches its call number limit, no more new connections are allowed until an existing connection is closed.

## 8.1.4 Device Profiles

Profiles are sets of characteristics that are generally repeated when creating extensions and /or devices. Instead of repeating in the forms and dial-plan these data we create profiles that group this data.

There are four profile type options:

PJSIP

SIP

IAX2

Telephony (BRI, E1 PRI, E1 R2, FXO, FXS, T1 CAS, T1 PRI). These options will only appear if the DAHDI add-on is installed.

### 8.1.4.1 PJSIP Profile

#### General

The screenshot shows the 'Device Profiles' configuration interface. At the top, there are tabs for 'GENERAL' and 'ADVANCED'. Below the tabs, the 'Profile Type' is set to 'PJSIP'. The 'General' section contains a 'Name' field and a 'Description' field. The 'Network' section includes settings for Transport (UDP), Qualify Frequency (0), Qualify Timeout (3), Force rport (Yes), ICE Support (No), Rewrite Contact (No), Remove Existing (No), and Use AVPF (No). The 'Media' section includes Media Encryption (No), Direct Media (Yes), and Media Transport Received (No). The 'DTLS' section includes DTLS Certificate (-- None --), DTLS Fingerprint Hash (SHA-256), DTLS Setup (Actpass), and DTLS Rekey Interval (0). A 'Save' button is located at the bottom right of the form.

**Name**, this is the user-defined name for the profile.

**Description**, a brief description to identify the profile.

#### Network

**Transport**, desired transport configuration.

**Qualify Frequency**, interval between attempts to rate the contact to reach it. If 0 never qualify. Time in seconds.

**Qualify Timeout**, If the contact does not respond to the OPTIONS request before the time out, the contact is marked as unavailable. If the value is 0 there is no timeout.

**Force rport**, force use of the return port.

**ICE support**, enable the ICE mechanism to help traverse NAT.

**Rewrite Contact**, this allows the contact header to be rewritten with source IP address port.

**Remove Existing**, this allows a registration to succeed by displacing any existing contacts that now exceed the "Max Contacts" count. Any removed contacts are the next to expire. The behavior is beneficial when "Rewrite Contact" is enabled and "Max Contacts" is greater than one. The removed contact is likely the old contact created by "Rewrite Contact" that the device is refreshing.

**Use AVPF**, determine if res\_pjsip will use and enforce the use of AVPF for this endpoint.

**RTP Symmetric**, enforce that RTP must be symmetric.

**RTCP Mux**, with this option enabled, Asterisk will try to negotiate the use of the "rtcp-mux" attribute on all media streams. This will result in RTP and RTCP being sent and received on the same port. This switches the demultiplexing logic to the application rather than the transport layer. This option is useful when interoperating with WebRTC endpoints as they enforce the use of this option.

**Asymmetric RTP Codec**, allow the send and receive RTP codec to differ.

**Send Diversion Header**, send the forward header, transmitting the forwarding information to the called user agent.

**Send P-Asserted Identity**, send the Header P-Asserted Identity.

**Send Remote-Party-ID**, send the Header Remote-Party-ID.

**WebRTC**, when set to "Yes", this also enables the following settings required for basic WebRTC support to work: `rtcp_mux`, `use_avpf`, `ice_support`, and `use_received_transport`.

## Media

**Media Encryption**, this determines if res\_pjsip will use and enforce the use of media encryption for this endpoint.

**Direct Media**, this determines if media can flow directly between endpoints.

**Received Media Transport**, this determines if res\_pjsip will use the media transport received in the offer SDP in the corresponding response SDP.

**Optimistic Media Encryption**, this determines whether encryption should be used if possible, but does not terminate the session if not achieved.

**Disable NAT Direct Media**, direct media session disable is updated when NAT obstructs media session.

## DTLS

**DTLS certificate**, certificate to use with DTLS connections.

**DTLS Setup**, if we are willing to accept connections, connect with the other party, or both. Valid options are:

- **Active**, we want to connect with the other party.
- **Passive**, we only want to accept connections.
- **Actpass**, we will do both. This value will be used in outbound SDP when offered and for inbound SDP offers when remote party sends actpass.

**DTLS Verify**, verify that the provided peer certificate is valid.

**DTLS Fingerprint Hash**, the hash to use for the fingerprint in SDP.

**DTLS Rekey interval**, interval in which to renegotiate the TLS session and reactivate the SRTP session. If this is not configured or the provided value is 0, reordering will be disabled.

## Advanced

Here we can add any PJSIP parameter that is not included in the VitalPBX interface. And the options are as follows:

**Parameter**, the PJSIP parameter to be included in the PJSIP profile.

**Value**, value of the PJSIP parameter to be used.

### 8.1.4.2 SIP Profile

The screenshot shows the 'Device Profiles' configuration page for a SIP profile. The 'GENERAL' tab is active, and the 'SIP' profile type is selected. The configuration is organized into several sections:

- General:** Fields for 'Name \*' and 'Description'.
- Network:** Fields for 'Host' (dynamic), 'Type' (Friend), 'Qualify Frequency' (60), 'Qualify Timeout' (2000), and 'Transport' (UDP). There are also checkboxes for 'RTP Encryption' (No), 'AVPF' (No), 'Direct Media' (Yes, if no nat), 'Force AVP' (No), and 'RTCP MUX' (No).
- ICE:** A checkbox for 'ICE' (No).
- DTLS:** Fields for 'Enable' (No), 'DTLS Certificate' (-- None --), 'DTLS Setup' (Actpass), 'DTLS Verify' (No), 'DTLS Fingerprint Hash' (SHA-256), and 'DTLS Rekey Interval' (0).
- Caller ID:** Fields for 'Send Remote Party ID' (No) and 'Trust Remote Party ID' (Yes).

A 'Save' button is located at the bottom right of the form.

**Name**, user-defined name for the profile.

**Description**, short description to identify this profile.

## Network

**Host**, the host parameter specifies the host name or IP address of a SIP peer or user. It is used to make outgoing calls and to find the pair when an incoming call is received. The host can take the following formats:

- Domain name / host name, eg.: sip.zxv.com
- IP address, eg. 234.23.42.103
- Dynamic, which means that phones must be registered.

**Type**, this determines their roles within Asterisk. The type options are:

- **Peer**: they handle incoming and outgoing calls and correspond with IP / Port. When there are incoming calls from the peer, the IP address must match for the invitation to be accepted.
- **User**: They only handle incoming calls, which means they can call Asterisk, but Asterisk can't call them. Callers must be authenticated by their authorization information (username and secret).
- **Friend**: will accept friend calls as it would for users, requiring only that the authorization match, rather than the IP address.

**Qualify Frequency**, how often the host should be verified to be in seconds and reported in milliseconds with the sip show setting.

**Timeout for Qualifier**, if this is set to yes (equivalent to 2000 ms), it will send an OPTIONS packet to the endpoint periodically (by default every minute). It is used to control the state of the endpoint. If the delays are longer than the qualify time, the endpoint will be disconnected and considered unreachable. It can be set to a value that is the threshold of msec. Setting to 'no' will not disable it. It may also be useful to keep NAT pinholes open.

**Transport**, this sets the default transports. The order determines the main default transport.

**ICE**, whether to enable ICE support. The default value is no. ICE (Interactive Connectivity Establishment) is a Network Address Translator (NAT) handover protocol for UDP-based multimedia sessions established with the offer / response model. This option is commonly enabled in WebRTC configurations.

**RTP Encryption**, enables RTP voice encryption.

**AVPF**, enable interoperability with media streams using the AVPF RTP profile.

**Direct RTP**, allows the direct sending of RTP between the call participants.

## DTLS

**Enable**, enable, or disable DTLS-SRTP support.

**DTLS Certificate**, certified for use with DTLS connections.

**DTLS Setup**, if we are willing to accept connections, connect with the other party, or both. Valid options are:

- **Active**, we want to connect with the other party.
- **Passive**, we only want to accept connections.
- **Actpass**, we will do both. This value will be used in outbound SDP when offered and for inbound SDP offers when remote party sends actpass.

**DTLS Verify**, verify that the provided peer certificate is valid.

**DTLS Fingerprint Hash**, the hash to use for the fingerprint in SDP.

**DTLS Rekey Interval**, interval in which to renegotiate the TLS session and reactivate the SRTP session. If this is not configured or the provided value is 0, reordering will be disabled.

## Caller ID (CID)

**Send ID to Remote Location**, add remote party ID header to SIP INVITATIONS.

**Trust Remote Location ID**, with this we assume the remote party ID header is correct.

## Advanced

Here we can add any SIP parameter that is not included in the VitalPBX interface. And the options are as follows:

**Parameter**, the SIP parameter to be included in the SIP profile.

**Value**, value of the SIP parameter to be used.

### 8.1.4.3 IAX2 Profile

The screenshot shows the 'Device Profiles' configuration page in VitalPBX. The 'GENERAL' tab is selected, and the 'Profile Type' is set to 'IAX2'. The form includes the following fields:

- Name \***: A text input field.
- Description**: A text input field.
- Host**: A dropdown menu with 'dynamic' selected.
- Quality Frequency**: A text input field with '60'.
- Type**: A dropdown menu with 'Friend' selected.
- Quality Timeout**: A text input field with '2000'.
- Call Token**: A dropdown menu with 'No' selected.
- Transfer**: A dropdown menu with 'Yes' selected.

A 'Save' button is located at the bottom right of the form.

**Name**, user-defined name for the profile.

**Description**, short description to identify this profile.



## Network

**Host**, hostname, or device address.

**Type**, this defines the type of device.

- **User**, this option is a device that makes calls, requires authentication.
- **Peer**, this option is a trunk device, accompanied by the Host.
- **Friend**, this option is a combination of "User" and "Peer".

**Test call**, this uses requirecalltoken for authentication.

**Qualifier Frequency**, this defines the interval of qualifying in seconds. A value of zero will disable this feature.

**Qualifier Timeout**, this defines the maximum response time in milliseconds before a device is considered unreachable. A value of zero will disable this feature.

**Transfer**, allow transfers from this device

## Advanced

Here we can add any IAX2 parameter that is not included in the VitalPBX interface. And the options are as follows:

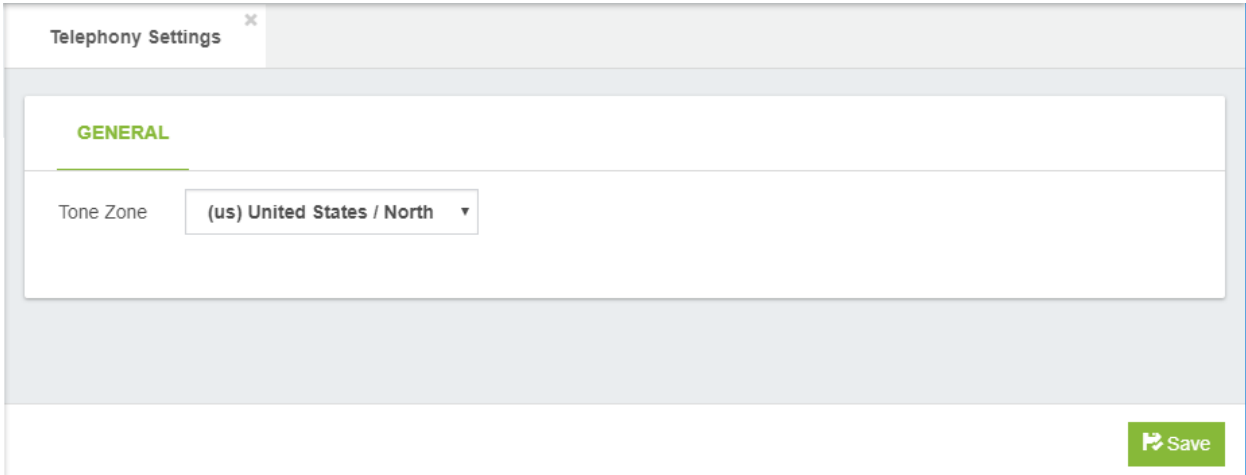
**Parameter**, the IAX parameter to be included in the profile.

**Value**, value of the IAX parameter to be used.

## 8.1.5 Telephony Settings

This option will only appear if the DAHDI add-on module is installed.

### General



The screenshot shows a web interface for 'Telephony Settings'. The 'GENERAL' section is highlighted. Under 'Tone Zone', a dropdown menu is open, showing '(us) United States / North'. A green 'Save' button is located in the bottom right corner of the settings area.

**Tone Zone**, default tone zone for all users/peers.

## 8.1.6 Dial Profiles

All dialing options are grouped in a Dial Profile.

### General

The screenshot shows the 'Dial Profiles' configuration page in the VitalPBX interface. The 'GENERAL' tab is active. The form includes the following fields:

- Name \***: A text input field.
- Allow Transfer By**: A dropdown menu set to 'Recipient'.
- Allow Park By**: A dropdown menu set to 'Recipient'.
- Ringback Tone**: A dropdown menu set to 'None (Ringback)'.
- Call Screening**: A dropdown menu set to 'Disabled'.
- Custom Options**: A text input field.
- Ringling Tone**: A toggle switch set to 'Yes'.

A yellow warning banner is displayed below the form:

**Warning!** Enabling transfer by caller may allow an outside caller to exploit the PBX by transferring their calls to another external destination when a too permissive Class of Service is defined for the trunk.

A 'Save' button is located at the bottom right of the form.

**Name**, name to identify this profile.

**Allow Transfer By**, allow the called/calling party to transfer the calling party by sending the DTMF sequence defined in feature codes.

**Allow Park By**, allow the called/calling party to enable parking of the call by sending the DTMF sequence defined for "Park Call" in feature codes.

**MoH Class**, provide hold music to the calling party until a requested channel answers.

**Call Screening**, before ringing your extension, the caller is asked to supply an introduction. The application asks them: "After the tone, say your name". They are allowed 4 seconds of introduction.

**Custom Options**, this allows you to define custom dial parameters that have not been included. Examples of some common dial options:

- D (called:calling) - send the specified digits after the called party has answered, but before the call gets bridged. The 'called' digits are sent to the called party, and the 'calling' digits are sent to the calling party. Both arguments can be used alone.
- H - allow the called party to hang up by using the In-Call Asterisk Disconnect code (default value is \*\*)
- i - any forwarding requests that may be received on this dial attempt will be ignored.
- l - any connected line update requests or any redirecting party update requests that may be received on this dial attempt will be ignored.

- r - generate ringing to the calling party, even if the called party is not actually ringing. Pass no audio to the calling party until the called channel has answered.
- S(x) - hang up the call x seconds after the called party has answered the call.
- t - allow the called party to transfer the calling party by using the In-Call Asterisk Blind Transfer code (default value is ##)
- T - allow the calling party to transfer the called party by using the In-Call Asterisk Blind Transfer code (default value is ##)
- w - allow the called party to enable recording of the call by using the In-Call Asterisk Toggle Call Recording code (default value is \*1)
- W - allow the calling party to enable recording of the call by using the In-Call Asterisk Toggle Call Recording code (default value is \*1)

**Ringing Tone**, this indicates a ringing tone to the calling party, even if the called party is not yet ringing. Do not pass audio to the calling party until the called channel is answered.

**Warning!** Enabling transfer by caller may allow an outside caller to exploit the PBX by transferring their calls to another external destination when a too permissive Class of Service is defined for the trunk.

## 8.2 Voicemail Settings

### 8.2.1 Voicemail Settings

In this tab you will find the information about Voicemail Settings

#### General

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

Setting	Value	Toggle
Max Message Length	180	Move Heard Msg: Yes
Min Message Length		Force Name: Yes
Greetings Length	60	Force Greetings: Yes
Max Silence	10	Use Directory: Yes
Max Login Attempts	3	Operator: No
Backup Deleted	100	Review Msg: Yes
Max Messages	100	Search Contexts: No

Operator Destination: Select Module, Select Destination

Save

**Max Message Length**, maximum length of a voicemail message in seconds. Leave empty for No Limit.

**Min Message Length**, minimum length of a voicemail message in seconds for the message to be kept. Leave empty for No Minimum.

**Greetings Length**, maximum length of greetings in seconds.

**Max Silence**, how many seconds of silence before we end the recording.

**Max Login Attempts**, max number of failed login attempts.

**Backup Deleted**, maximum number of messages allowed in the Deleted folder.

**Max Messages**, maximum number of messages per folder. If set to 0, a mailbox will be greetings-only.

**Operator Number**, Extension to dial on pressing 0 while listening a voicemail.

**Move Heard Msg**, move heard messages to the Old folder automatically.

**Force Name**, forces a new user to record their name. A new user is determined by the password being the same as the mailbox number.

**Force Greetings**, this is the same as "Force Name", except for recording.

**Use Directory**, permit finding entries for forward/compose from the directory.

**Operator**, this will allow the sender to hit 0 before/after/during leaving a voicemail to reach an operator. This option **REQUIRES** an o extension in the same context (or in exit context, if set), as that is where the 0 key will send you.

**Review Msg**, allow sender to review/rerecord their message before saving it

**Search Context**, current default behavior is to search only the default context if one is not specified. The older behavior was to search all contexts.

**Operator Destination**, the extension to call when pressing 0 while listening to the voicemail box.

## Email Settings

In this tab you will find the information about Email Settings for send the Voicemail.

The screenshot shows the 'Voicemail Settings' interface with the 'EMAIL SETTINGS' tab selected. The 'From Email' field is set to 'mailbox@domain.com' and 'From Name' is 'Asterisk PBX'. The 'Email Subject' is 'New Voicemail Message from \${VM\_CALLERID}'. The 'Email Body' contains a preview of an email notification: 'You have received a new voicemail message. From: \${VM\_CALLERID}, Date: \${VM\_DATE}, Duration: \${VM\_DUR}'. A legend on the right lists variables like \${VM\_CATEGORY}, \${VM\_NAME}, \${VM\_DUR}, \${VM\_MSGNUM}, \${VM\_CALLERID}, \${VM\_CIDNAME}, \${VM\_CIDNUM}, \${VM\_DATE}, and \${VM\_MESSAGEFILE} with their respective definitions. A 'Save' button is at the bottom right.

**From Email**, Who the e-mail notification should appear to come from. Example: mailbox@domain.com.

**From Name**, name that will appear in emails from your PBX.

**Email Subject**, email subject.

**Email Body**, email body.

## 8.2.2 Voicemail Time Zones

In this tab you will find the information about Time Zones Settings for Voicemail

### General

**Name**, short name of time zone.

**Time Zone**, continent/country time zone to be selected.

**Time Definition\***, users may be located in different time zones, or may have different message announcements for their introductory message when they enter the voicemail system. Set the message and the time zone each user hears here. Set the user into one of these zones with the tz= attribute in the options field of the mailbox. Of course, language substitution still applies here so you may have several directory trees that have alternate language choices. Look in /usr/share/zoneinfo/ for names of time zones.

Supported values:

- 'filename', filename of a sound file (single ticks around the filename required)
- \${VAR}, variable substitution
- A or a, Day of week (Saturday, Sunday, ...)
- B or b or h, Month name (January, February, ...)
- d or e, numeric day of month (first, second, ..., thirty-first)
- Y, Year
- l or l, Hour, 12 hour clock
- H, Hour, 24 hour clock (single digit hours preceded by "oh")
- K, Hour, 24 hour clock (single digit hours NOT preceded by "oh")
- M, Minute, with 00 pronounced as "o'clock"
- N, Minute, with 00 pronounced as "hundred" (US military time)
- P or p, AM or PM
- Q, "today", "yesterday" or ABdY (\*note: not standard strftime value)

- Q, "" (for today), "yesterday", weekday, or ABdY (\*note: not standard strftime value)
- R, 24 hour time, including minute

### Examples:

eastern=America/New\_York|'vm-received' Q 'digits/at' IMp  
 central=America/Chicago|'vm-received' Q 'digits/at' IMp  
 central24=America/Chicago|'vm-received' q 'digits/at' H N 'hours'  
 military=Zulu|'vm-received' q 'digits/at' H N 'hours' 'phonetic/z\_p'  
 european=Europe/Copenhagen|'vm-received' a d b 'digits/at' HM

## 8.3 PBX Settings

### 8.3.1 System General

In this tab you will find the information about PBX Settings

#### General

#### Extension Settings

**Default Language**, language to select by default when a new extension is being created.

**Device Prefix**, prefix to append by default to devices name.

**Enable Voicemail**, if enabled, the voicemail will be enabled automatically each time you create an extension.

**Enable Portal**, if enabled, the portal will be enabled automatically each time you create an extension.

**Create Hints**, if enabled, the hints will be enabled automatically each time you create an extension.

## Dial-Plan Settings

**Default Ring Timer**, time extensions by default ringing.

**Transfer Digit Timeout**, number of seconds to wait between digits when transferring a call (default is 3 seconds).

**Features Digit Timeout**, max time (ms) between digits for feature activation (default is 1000 ms).

**Recording Format**, file format for calls recording.

**Recording Script**, Script to be executed when the recording is over. The script parameters can be defined as space separated sequence of strings like `^ {name}`, where name can be any channel or MixMonitor variable. For example, `^ {UNIQUEID}` - channel ID, `^ {MIXMONITOR_FILENAME}` - recording file name.

## GUI Settings

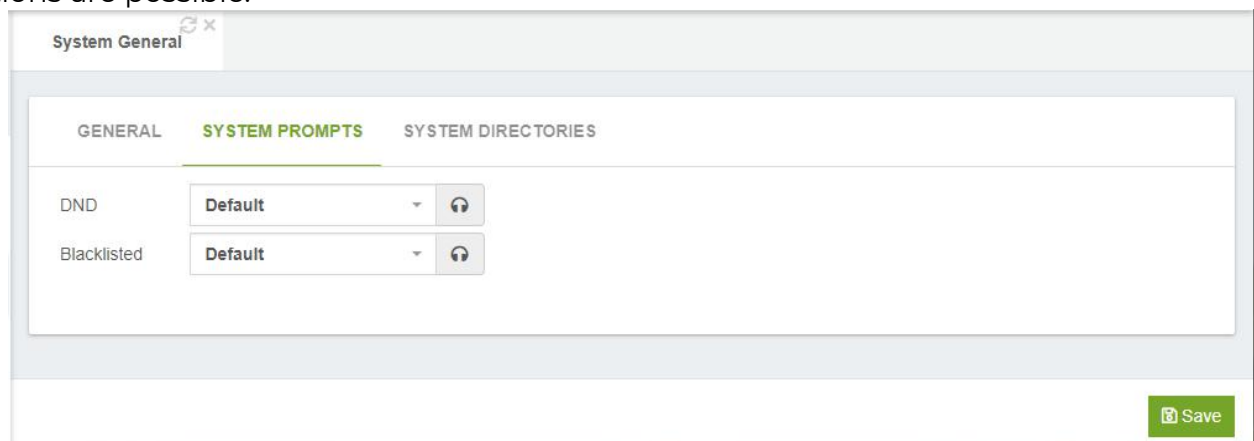
**Show Login Panel**, if set to yes, it shows a panel with the sonata add-ons when these are installed.

## Queues Callback

**Search Frequency**, this value defines the frequency in which the Queues Callback service will search for calls.

## System Prompts

It allows to customize certain voice guides of the system, now only a couple of options are possible.



**DND**, allows you to define a custom prompt that will be reproduced when an extension has active the DND.



**Blacklisted**, allows you to define a custom prompt that will be reproduced to callers who are blacklisted.

## System Directories Tab

Description	Path
Asterisk AGI Directory	/var/lib/asterisk/agi-bin
Asterisk Directory	/etc/asterisk
Asterisk Log Directory	/var/log/asterisk
Asterisk Modules Directory	/usr/lib/asterisk/modules
Asterisk Sound Directory	/var/lib/asterisk/sounds
Asterisk Spool Directory	/var/spool/asterisk
Asterisk Libraries Directory	/var/lib/asterisk

### Asterisk Directories

Asterisk AGI Directory, Asterisk AGI directory.

Asterisk Directory, home Asterisk directory.

Asterisk Modules Directory, Asterisk modules directory.

Asterisk Libraries Directory, Asterisk libraries directory.

Asterisk Log Directory, Asterisk log directory.

Asterisk Sound Directory, Asterisk sound directory.

Asterisk Spool Directory, Asterisk spool (recording) directory

## 8.3.2 Asterisk Manager Users

In this tab you will find the information about Asterisk Manager Users

### General

The screenshot shows the 'Asterisk Manager Users' configuration page. The 'GENERAL' tab is active, displaying several input fields for user configuration. The fields are arranged in two columns. The left column contains 'AMI User \*', 'AMI Secret \*', 'Description \*', and 'Read Permissions'. The right column contains 'Deny \*', 'Permit \*', and 'Write Permissions'. The 'AMI Secret' field contains the value 'K5bmzztfQN8gAc'. The 'Deny' field contains '0.0.0.0/0.0.0.0'. The 'Permit' field contains '127.0.0.1/255.255.255.0'. There are menu icons (three horizontal lines) next to the 'Read Permissions' and 'Write Permissions' fields. A green 'Save' button is located at the bottom right of the form.

**AMI User\***, username for connect to AMI (must be unique)

**AMI Secret**, secret for login to Asterisk Management Interface (AMI)

**Description**, short description.

**Read Permissions**, AMI read permissions.

**Write Permissions**, AMI write permissions.

**Deny**, if you want to deny many hosts or networks, use & char as separator. Example:  
192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0

**Permit**, if you want to permit many hosts or networks, use & char as separator.

## 8.3.3 Log File

In this tab you will find the information about create new log file.

### General

The screenshot shows the 'Log Files' configuration page with the 'GENERAL' tab selected. The configuration options are as follows:

- Date Format: %F %T
- Log Rotation: Sequential
- Append Hostname: No
- Log Queues: Yes

Below these options is a table for configuring individual log files:

Filename	Debug	DTMF	Error	Fax	Notice	Verbose	Warning	Security
fail2ban	Off	Off	Off	Off	On	Off	Off	On
console	On	Off	On	Off	On	3	On	Off
full	On	Off	On	Off	On	3	On	Off

Buttons for 'Add' and 'Save' are visible at the bottom right of the configuration area.

**Date Format**, here you can customize the display of debug message time stamps. See `strftime(3)` Linux manual for format specifiers. Note that there is also a fractional second parameter which may be used in this field. Use `%1q` for tenths, `%2q` for hundredths, etc. Leave blank for default: ISO 8601 date format `yyyy-mm-dd HH:MM:SS` (`%F %T`).

**Log Rotation**, how to write down the logs.

- **Sequential:** Rename archived logs in order, such that the newest has the highest sequence number.
- **Rotate:** Rotate all the old files, such that the oldest has the highest sequence number (expected behavior for Unix administrators).
- **Timestamp:** Rename the log files using a timestamp instead of a sequence number when "logger rotate" is executed.

**Append Hostname**, appends the hostname to the name of the log files.

**Log Queues**, log queue events to a file.

#### Log Files

**File Name**, name of log file.

**Debug**, debugging is only useful if you are troubleshooting a problem with the Asterisk code itself. You would not use debug to troubleshoot your dial-plan, but you would use it if the Asterisk developers asked you to provide logs for a problem you

were reporting. Do not use debug in production, as the amount of detail stored can fill up a hard drive in a matter of days.

**DTMF**, logging DTMF can be helpful if you are getting complaints that calls are not routing from the auto attendant correctly.

**Error**, errors represent significant problems in the system that must be addressed immediately.

**Fax**, this type of logging causes fax-related messages from the fax technology backend (res\_fax\_spandsp or res\_fax\_digium) to be logged to the fax logger.

**Notice**, you will see a lot of these during a reload, but they will also happen during normal call flow. A notice is simply any event that Asterisk wishes to inform you of.

**Verbose**, this is one of the most useful of the logging types, but it is also one of the riskier to leave unattended, due to the possibility of the output filling your hard drive.

**Warning**, a warning represents a problem that could be severe enough to affect a call (including disconnecting a call because call flow cannot continue). Warnings need to be addressed.

**Security**, output security messages.

## 8.3.4 RTP Settings

In this tab you will find the information about RTP Settings

### General

GENERAL	
RTP Start	10000
RTP End	20000
Strict RTP	No
RTP Checksums	Yes
ICE Support	Yes
Stun Server	stun4.l.google.com:19302
Turn Server	
Turn Server Name	
Turn Server Password	

**RTP Start**, indicates where the port start.

**RTP End**, indicates the end of the port.

**Strict RTP**, enable strict RTP protection. This will drop RTP packets that do not come from the source of the RTP stream, whether to enable or disable UDP checksums on RTP traffic.

**RTP Checksums**, whether to enable or disable UDP checksums on RTP traffic.

**ICE Support**, whether to enable or disable ICE support. This option is disabled by default.

**Stun Server**, hostname or address for the STUN server used when determining the external IP address and port an RTP session can be reached at. The port number is optional.

**Turn Server**, hostname or address for the TURN server to be used as a relay. The port number is optional.

**Turn Server Name**, username used to authenticate with TURN relay server.

**Turn Server Password**, password used to authenticate with TURN relay server.

## 8.3.5 CEL Settings

The Channel Event Logs for Asterisk provides a mechanism to track various events related to a call. CEL es quite granular and a fine grain at that. It has been designed having billing information in mind. It admits various backend for storage and is a great alternative for the Call Detail Recordings for administrators that require event registries that are extremely detailed. The immense amount of detail will allow for the construction of precise data for billing and callflow.

### General

The screenshot shows the 'CEL Settings' window with the 'GENERAL' tab selected. The 'Enable' checkbox is checked and labeled 'Yes'. The 'APPS' field contains 'Dial, Park, Queue, ConfBrid...' with a list icon. The 'Events' field contains 'APP\_START, CHAN\_START...' with a list icon. The 'Date Format' field contains '%F %T'. A 'Save' button is visible at the bottom right.

**Enable**, enable or disable the Channel Event Logs for Asterisk.

**APPS**, this allows you to specify the list of applications from which you want to receive the CEL events from.

**Events**, this allows you to specify a list of events that you wish to generate when they occur.

**Date Format**, this allows you to specify the date format used when generating CEL Events.

## 8.3.6 Mini HTTP Server

The core of Asterisk provides a basic HTTP/HTTPS server.

Certain Asterisk modules may make use of the HTTP service, such as the Asterisk Manager Interface over HTTP, the Asterisk Restful Interface or WebSocket transports for modules that support that, like chan\_sip or chan\_pjsip.

In this tab you will find the information about Mini HTTP Server.

### General

GENERAL			
HTTP Bind Address	0.0.0.0 8088	Enable HTTP	Yes
TLS Bind Address	0.0.0.0 8089	TLS Enable	Yes
Certificate	itexpo2020.vitalpbx.org		

Save

**HTTP Bind Address**, address and optional port to bind to, both for HTTP and HTTPS.

**TLS Bind Address**, address and port to bind to this transport.

**Certificate**, certificate for TLS connections.

**Enable HTTP**, whether HTTP/HTTPS interface is enabled or not.

**TLS Enable**, HTTPS support. In addition to enabled, you need to explicitly enable TLS, define the port to use, and have a certificate somewhere.

## 8.4 Voice Prompts

### 8.4.1 Asterisk Sounds

This module allows end users to install additional Asterisk sounds according to their needs.

✕
Asterisk Sounds

**GENERAL**

---

Sound Package	Installed Version	Available Version	Actions
English (Australia) - CORE_ULAW		2.0.0-2	
Japanese - CORE_ULAW		2.0.0-2	
Russian - CORE_ULAW		2.0.0-2	
German - ULAW		2.0.0-2	
English (United Kingdom) - ULAW		2.0.0-2	
French - ULAW		2.0.0-2	
Hebrew - GSM		2.0.0-2	
Italian - ULAW		2.0.0-2	
Portuguese (Brazil) - ULAW		2.0.0-2	

Clean Cache
Check Online

## 8.4.2 Music on Hold

In this tab you will find the information about Music on Hold. As an extended feature, you will be able to use an application to playback the MoH. This can be used to stream music from a streaming server.

### General

The screenshot shows a web interface for configuring Music on Hold. The title bar reads "Music on Hold" with a refresh icon and a close button. Below the title bar, the "GENERAL" tab is selected. The form contains the following fields:

Name *	<input type="text" value="Radio"/>	Streaming URL	<input type="text"/>
Mode	<input type="text" value="Custom"/>	Format	<input type="text"/>
Application	<input type="text" value="/usr/bin/mpg123 -q -r 8000 -f 8192"/>	Default	<input type="checkbox" value="No"/>

A "Save" button is located at the bottom right of the form.

**Name**, short description for identify this MoH Category.

**Mode**, this defines the mode to play or retrieve music on hold.

- **Options:**

- **Files:** plays files from a directory in any media format supported by Asterisk.
- **Custom:** run a custom application. For example, an online radio.

**Sort**, sort the files to listen to.

**Sound file**, you can use this to upload a wav or mp3 file.

**Default**, if checked, the sounds from this music group will be used for the default music class on hold. Only one music group can be marked as default.

**Application**, application that will be used to reproduce a broadcast. If the application is not provided, the mpg123 application will be used in the following format: `mpg123 -q -r 8000 -f 8192 --mono -s`.

**Transmission URL**, URL that will be transmitted by the defined application.

**Format**, the format option specifies the audio format that the application will provide to Asterisk.



## 8.4.3 Recording Managements

In this tab you will find the information about Record Management.

### General

The screenshot shows a web interface for 'Recordings Management'. At the top, there's a tab labeled 'Recordings Management'. Below it, the 'GENERAL' tab is selected. There are two input fields: 'Name \*' and 'Sound File \*'. The 'Sound File \*' field has a file upload icon. Below these is a 'Recording List' section with a table. The table has four columns: 'Recording', 'Name', 'Duration', and 'Actions'. At the bottom right, there are two buttons: 'Upload Recording' (green) and 'Refresh' (blue).

**Name**, short description for identify this recording.

**Sound File**, here you can upload a wav or mp3 file.





### Recording List

**Recording**, name of the sound file.

**Name**, description of the sound file.

**Duration**, duration of the recording.

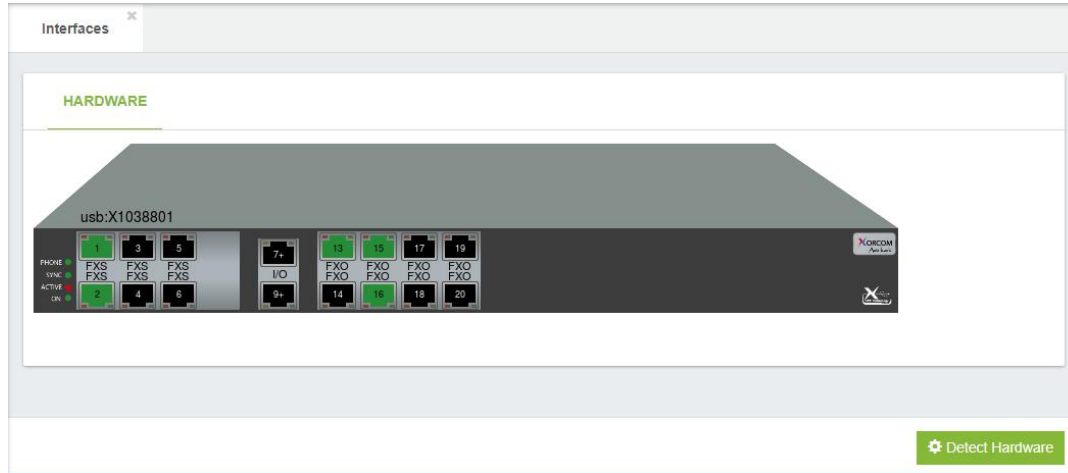
Action

- , edit description.
- , listen recording.
- , record by phone.
- , delete recording.

## 8.5 Telephony

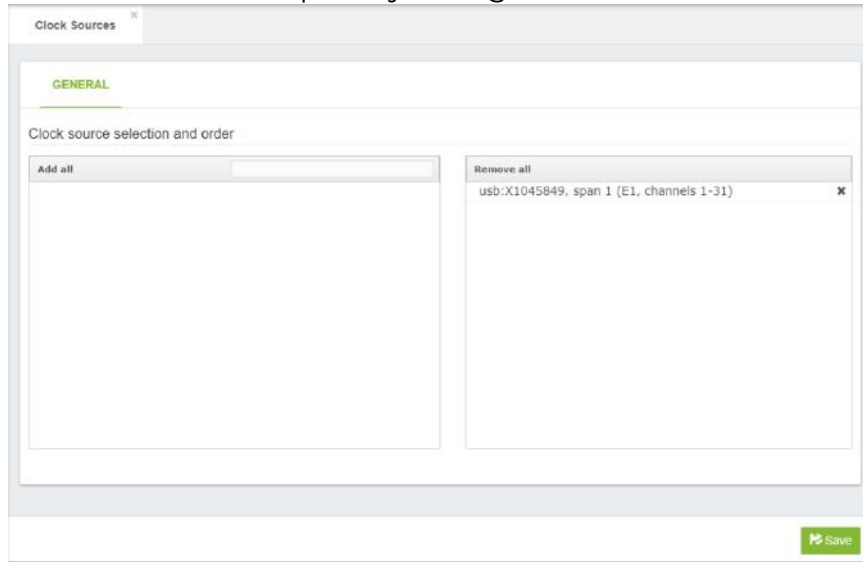
### 8.5.1 Interface

Telephony Interface detect any new hardware that is connected to our system, either a Hardware connected by USB or directly to a PCI port of our PC or server. Do not worry about pressing the button Detect Hardware you will not lose any previous settings related to the existing hardware.



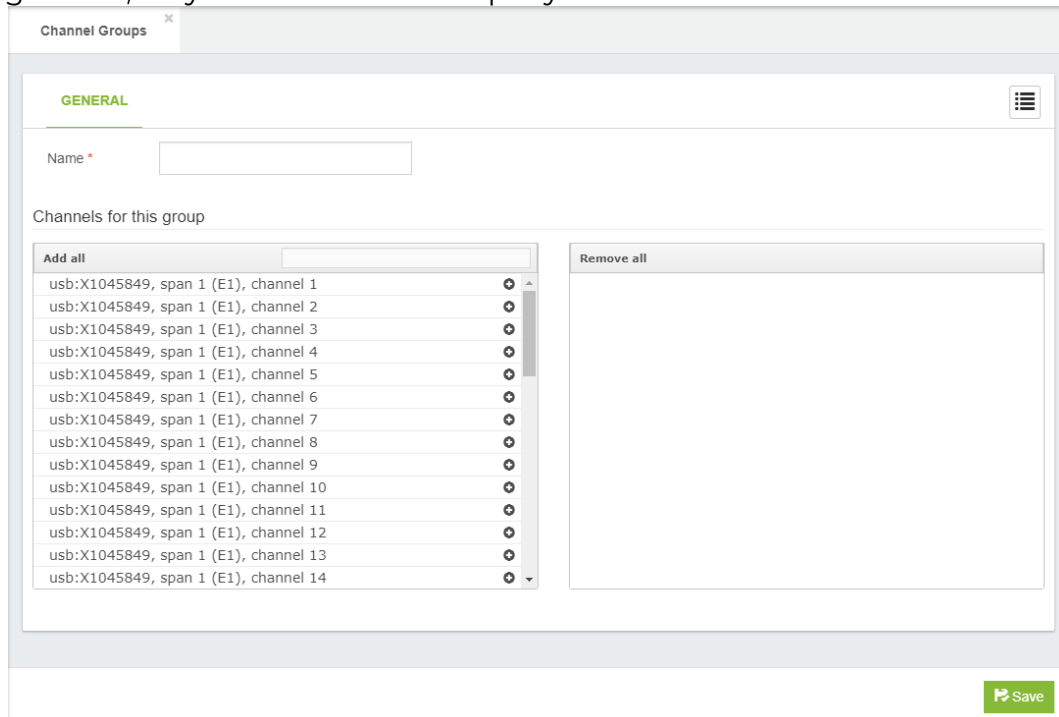
## 8.5.2 Clock Sources

Select the clock source and its priority for digital interfaces.



## 8.5.3 Channel Group

Grouped the analog and digital interfaces into groups to be used separately on outgoing routes, very useful when a company share external trunks.



**Name\***, name of the channel group

## 8.5.4 Profile Assignments

Assign to each channel a profile previously created in Settings > Technology > Profile.

**Profile Assignments** x

**GENERAL**

Device usb:X1045849, Local Span 2 (Analog), Channels 32-39

Assign to all channels

**Channels**

Channel 32	<input type="text" value="Default FXS Profile"/>	Channel 36	<input type="text" value="Default FXS Profile"/>
Channel 33	<input type="text" value="Default FXS Profile"/>	Channel 37	<input type="text" value="Default FXS Profile"/>
Channel 34	<input type="text" value="Default FXS Profile"/>	Channel 38	<input type="text" value="Default FXS Profile"/>
Channel 35	<input type="text" value="Default FXS Profile"/>	Channel 39	<input type="text" value="Default FXS Profile"/>

# 9. Admin

## 9.1 Admin

### 9.1.1 Users

In this tab you will find the information about management users.

#### General

The screenshot shows the 'Users' management interface. The 'GENERAL' tab is selected, and the form contains the following fields and options:

- Username \***: Text input field.
- E-mail**: Text input field.
- Password \***: Text input field with a visibility toggle (eye icon).
- Profile \***: Dropdown menu with 'Super Administrator' selected.
- Startup Dialog \***: Dropdown menu with 'Active Calls' selected.
- Full Name**: Text input field.
- Department**: Text input field.
- Tenants \***: Dropdown menu with 'VitalPBX' selected.
- Select Image**: Button to upload a user profile picture.
- Save**: Button to save the user configuration.

**Username \***, user as you will be login (Nick name).

**E-Mail**, this is the email address for the user.

**Password \***, your secure password for login

**Profile \***, profile for this user.

**Startup Menu \***, set the module for startup.

**Full Name**, full real name user.

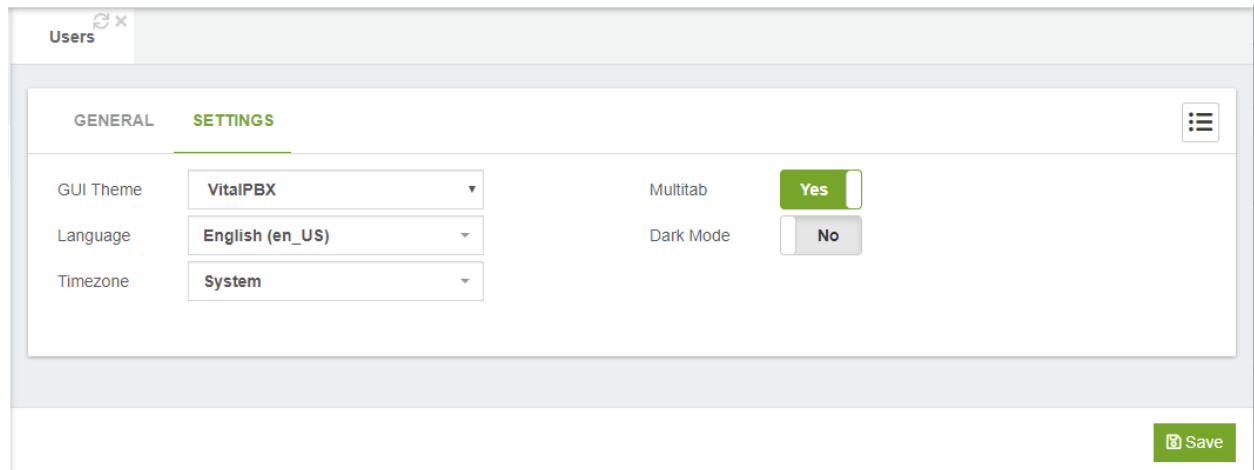
**Department**, user department (Example: Admin)

**Tenants \***, this option allows you to select which tenants a user will have access to.

**Select Image**, image with which the user is associated, it can be a photo of the user.

**Note:** The main user, “admin”, can only have its privileges modified given they are always total. If you want to create a user with administrator privileges, select the “Super Administrator” profile.

## Settings



The screenshot shows the 'Users' settings page in light theme. The 'SETTINGS' tab is active. On the left, there are three dropdown menus: 'GUI Theme' set to 'VitalPBX', 'Language' set to 'English (en\_US)', and 'Timezone' set to 'System'. On the right, there are two toggle switches: 'Multitab' set to 'Yes' and 'Dark Mode' set to 'No'. A green 'Save' button is located at the bottom right.

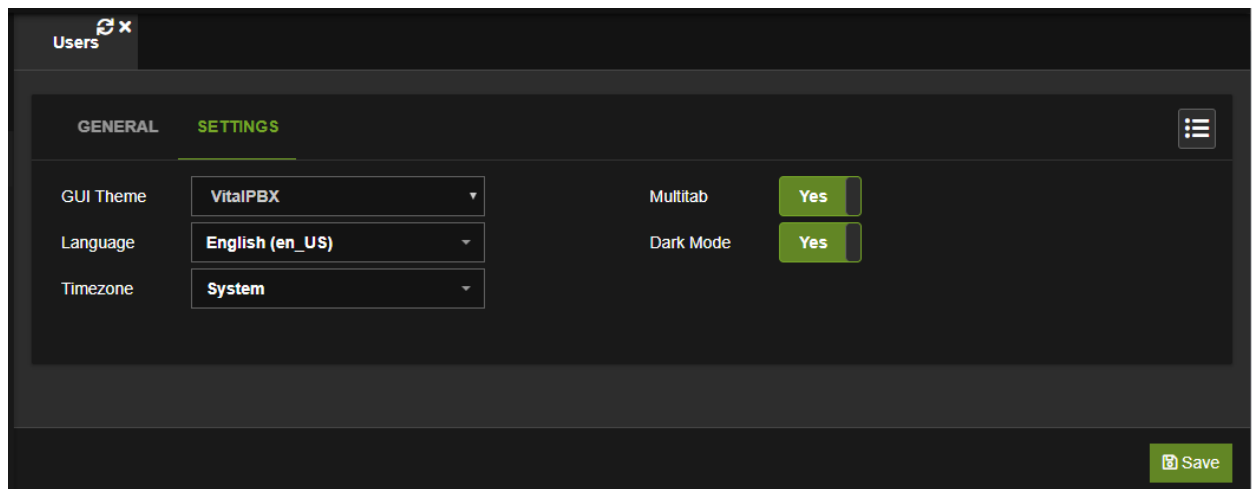
**GUI Theme**, appearance of the interface.

**Language**, interface language.

**Time Zone**, local Time Zone for this user.

**Multi-tab**, you can enable this if you want multiple tabs in the interface with modules you previously visited.

**Dark Mode**, when this option is enabled VitalPBX's interface will turn into a dark theme. Great for working in the dark and saving a mobile device's battery life.



The screenshot shows the 'Users' settings page in dark theme. The 'SETTINGS' tab is active. On the left, there are three dropdown menus: 'GUI Theme' set to 'VitalPBX', 'Language' set to 'English (en\_US)', and 'Timezone' set to 'System'. On the right, there are two toggle switches: 'Multitab' set to 'Yes' and 'Dark Mode' set to 'Yes'. A green 'Save' button is located at the bottom right.

## 9.1.2 Users Profiles

In this tab you will find the information about management user's profiles.

### General

The screenshot shows the 'User Profiles' form with the 'GENERAL' tab selected. The 'Profile Name' field is filled with 'Super Administrator'. Under the 'Module Access' section, the 'Grant Privileges' toggle is set to 'Yes'. Below this, there are 'Expand All' and 'Collapse All' buttons. A list of modules is displayed, each with a green checkmark and a right-pointing arrow: PBX, Reports, Settings, Admin, and Portal. At the bottom right of the form are three buttons: 'Update' (green), 'Delete' (red), and 'Cancel' (blue).

**Profile Name**, name for this profile.

### Modules Access

**Grant Privileges**, this option allows access to all modules.

### Permissions

By its due nature, some permissions are not linked to the main menu. On this form you can configure these types of permissions.

The screenshot shows the 'User Profiles' form with the 'PERMISSIONS' tab selected. There are three permission toggles, all set to 'Yes': 'Update Profile', 'Get Updates', and 'Change Language'. At the bottom right of the form are three buttons: 'Update' (green), 'Delete' (red), and 'Cancel' (blue).

**Update Profile**, this determines if a user with this profile can update their profile information, with the only limitation being to change the User Profile.

**Get Updates**, if a user with this profile has this option, they will be able to update VitalPBX from the GUI.

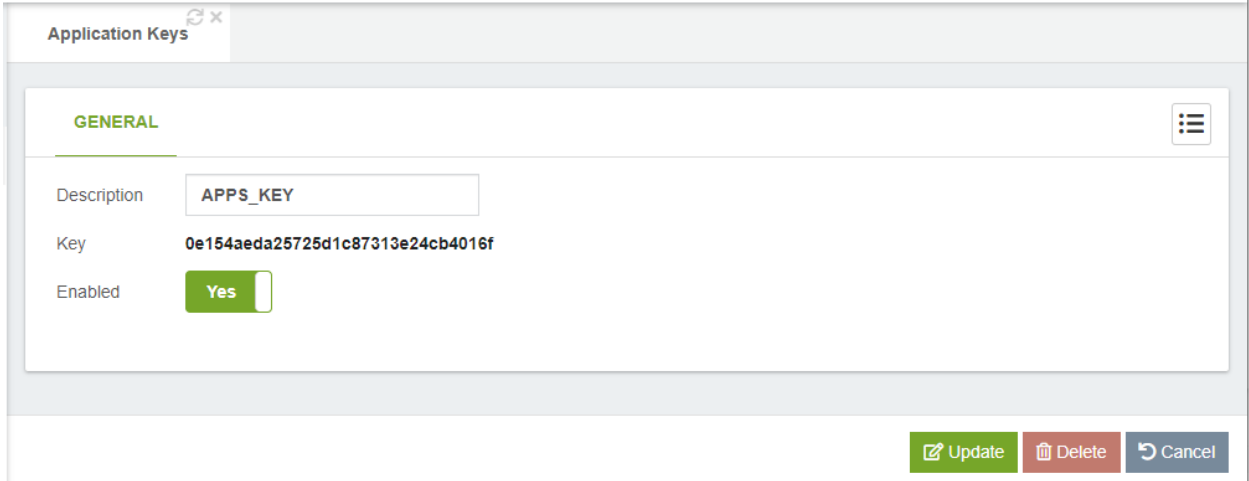
**Change Language**, this determines if a user with this profile can change the language from the GUI.

## 9.1.3 Application Keys

Here, we can create the API Key to grant permissions to third-party applications to use the VitalPBX API.

For updated information about our API, please visit the following link:  
<https://documenter.getpostman.com/view/5481262/S17rvTgc?version=latest>

### General



The screenshot shows a web interface for managing Application Keys. The title bar reads "Application Keys" with a close button. The main content area is titled "GENERAL" and contains the following fields:

- Description: APPS\_KEY
- Key: 0e154aeda25725d1c87313e24cb4016f
- Enabled: Yes (checked)

At the bottom right, there are three buttons: "Update" (green), "Delete" (red), and "Cancel" (blue).



## 9.1.4 Tenants

The term "software multitenancy" refers to a software architecture in which a single instance of software runs on a server and serves multiple tenants. A tenant is a group of users who share a common access with specific privileges to the software instance. With a multitenant architecture, a software application is designed to provide every tenant a dedicated share of the instance - including its data, configuration, user management, tenant individual functionality and non-functional properties.

As of version 2.2 of VitalPBX, the Multitenant module is added with which, for free, you can have the main Tenant plus an additional one to test all the functions.

### General

The screenshot shows the 'Tenants' configuration page in VitalPBX. The 'GENERAL' tab is active, with sub-tabs for 'CALLS ROUTING' and 'SETTINGS'. The interface includes the following fields and controls:

- Name \***: Text input field.
- Description \***: Text input field.
- Prefix**: Text input field with the value 'Generate Automatically'.
- Enabled**: Toggle switch set to 'Yes'.
- Tenant Administrator** section:
  - Assign to Existing User**: Toggle switch set to 'No'.
  - Admin Email \***: Text input field.
  - Admin Password \***: Password input field with a visibility toggle.
  - Full Name**: Text input field.
  - Profile \***: Dropdown menu set to 'Tenant Administrator'.
  - Startup Dialog \***: Dropdown menu set to 'Dashboard'.
  - Send Welcome Email**: Toggle switch set to 'Yes'.
- Privileges** section:
  - Extensions**: Dropdown menu set to 'Unlimited'.
  - Trunks**: Dropdown menu set to 'Unlimited'.
  - Queues**: Dropdown menu set to 'Unlimited'.
  - IVRs**: Dropdown menu set to 'Unlimited'.
  - Conferences**: Dropdown menu set to 'Unlimited'.
  - Parking Lots**: Dropdown menu set to 'Unlimited'.
  - Allow Recordings**: Toggle switch set to 'No'.

A green 'Save' button is located at the bottom right of the form.

**Name**, a unique name for this tenant. This name will be used to create folders, linking CDR info, etc.

**Description**, this is a short Description to identify this tenant.

**Prefix**, this allows you to define a prefix to be used for extensions devices and others. If left blank an automatic prefix will be used.

**Enabled**, it allows you to enable/disable a tenant. If the tenant is disabled, the users who belongs to it will not be able to login to it nor perform any action.

### Tenant Administrator

**Assign to Existing User**, if checked, instead of creating a new user for the tenant, you may assign it an existing one.

**Admin Email**, the email address of the user who will manage this Tenant.

**Admin Password**, password to authenticate the default admin user of this tenant.

**Full Name**, administrator's full name, if not defined, the tenant description will be used instead.

**Profile**, role profile for the administrator of this tenant. **Be careful not to assign a too permissive role, which may affect other tenants.**

**Startup Dialog**, which dialog to be displayed when logging into the system.

### Limitations

**Extension**, it allows you to define the maximum number of extensions for this tenant.

**Trunks**, it allows you to define the maximum number of trunks for this tenant.

**Queues**, it allows you to define the maximum number of queues for this tenant.

**IVRs**, it allows you to define the maximum number of ivrs for this tenant.

**Conferences**, it allows you to define the maximum number of conferences for this tenant.

**Parking Lots**, it allows you to define the maximum number of parking lots for this tenant.

**Softphone Devices**, it allows you to define how many Sonata Communicator/VitalPBX Communicator Devices could be activated on this tenant.

**Allow Recordings**, it allows you to define if this tenant will be able to record or not calls.

### Recordings Maintenance Settings

**Clear Oldest Recordings**, this allows you to defined the maximum number of days that recordings should be retained. The recordings with more age than the days defined here will be deleted.

**Schedule**, it allows you to define the schedule in which the maintenance of the PBX will be executed (Conversion of Recordings, cleaning of Recordings and CDR, etc). If no schedule is selected, all the maintenance options will be disabled.

**Convert Recordings**, Enabled/Disable call recordings conversion to MP3.

## Call Routing

It is possible to share the route selections items as outbound profiles for other tenants, this way you will not need to create tenant trunks for using main tenant as a gateway, and not need to re-define outbound routes per tenant.

The screenshot shows the 'Tenants' configuration page with the 'CALLS ROUTING' tab selected. The interface includes several configuration fields:

- Allowed Tenant Trunks:** A dropdown menu with a list icon.
- Outbound Profiles:** A dropdown menu with a list icon.
- Allowed Outbound Routes:** A dropdown menu with a list icon.
- Emergency Trunks:** A dropdown menu with a list icon.
- Inbound DIDs:** A section with a table header 'DID Pattern' and a single row containing the pattern '1NXXNXXXXXX' in a text input field, a delete icon, and an 'Add' button.

A 'Save' button is located at the bottom right of the configuration area.

**Allow Tenant Trunks,** it allows you to define which tenants could be used as tenant trunks.

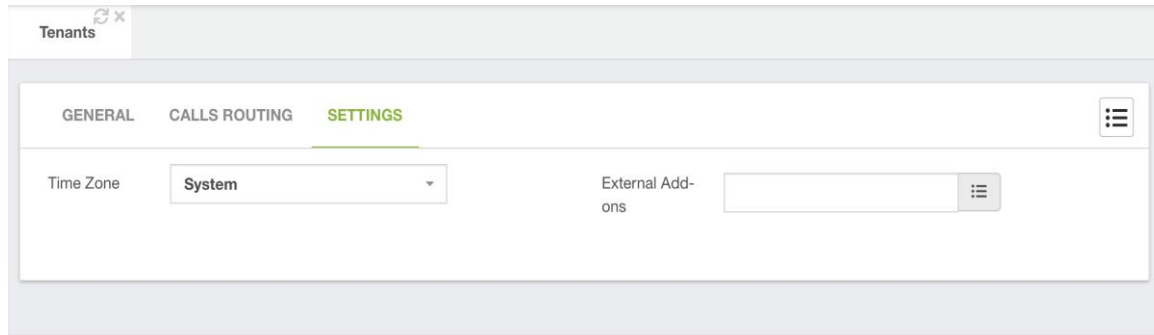
**Allow Outbound Routes,** routes that will be used when this tenant make calls through a tenant trunk pointing to the main tenant. Calls made to any other tenant than the main tenant will be sent through Inbound Routes definitions.

**Outbound Profiles,** this allows you to define what route selection items can be used as an outbound profile on this tenant. From version 3 and onward, when you assign an Outbound Route it is automatically applied to the All Permissions Class of Service for the Tenant. To create an Outbound Route, you must create a Route Selection under PBX > Class of Service > Route Selection.

**Emergency Trunks,** this option allows you to share emergency trunks with the tenant for the Emergency Numbers module.

**Inbound DIDs,** list of numbers/patterns belonging to this tenant. Calls that match with these numbers will be forward automatically to these tenant inbound routes. The configuration of these numbers takes precedence over the inbound routes' definitions on the main tenant. From version 3 and onward, when you assign a DID for the Inbound DID's section on the tenant, this will automatically create an Inbound Route on the tenant, where the Destination will be "Verify DID" which allows you to hear the DID number back when dialed.

## Settings

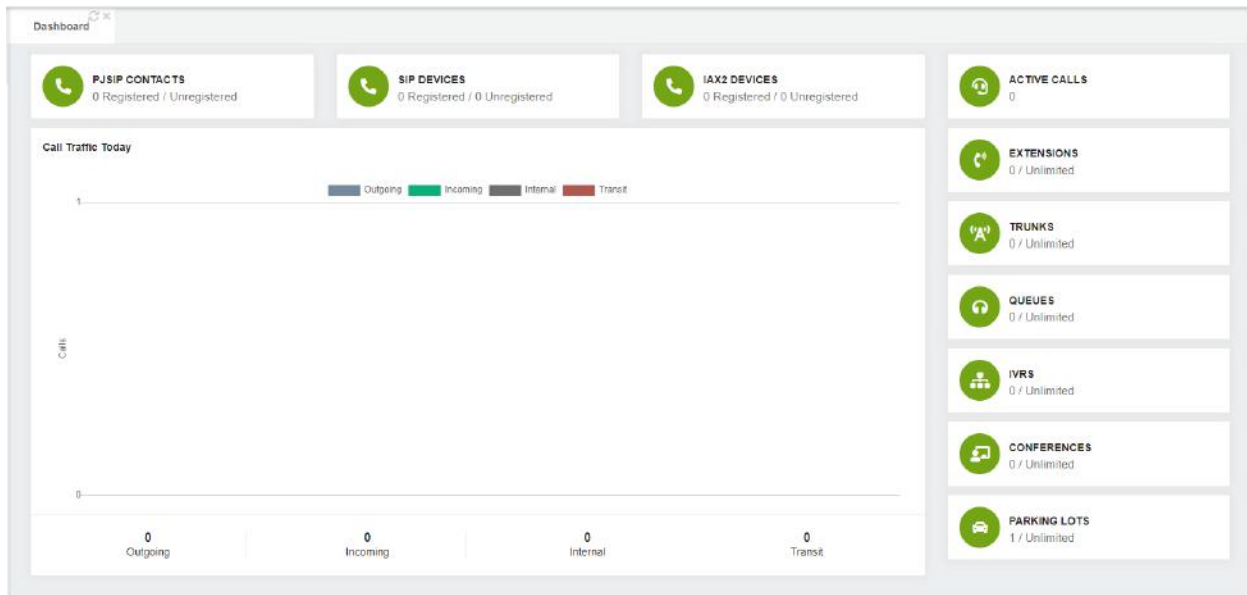


It is possible from version 3 of VitalPBX and onward to further customize the Tenant experience. Here you are able to do the following.

**Time Zone**, select the time zone that this tenant will operate in. This will affect every time-based configuration for the tenant.

**External Add-ons**, here you can select which external add-ons you want to give the tenant access to. External add-ons would be the Sonata Suite of Applications and VitXi.

Next, we show the Panel that will be shown to the Tenant administrator.

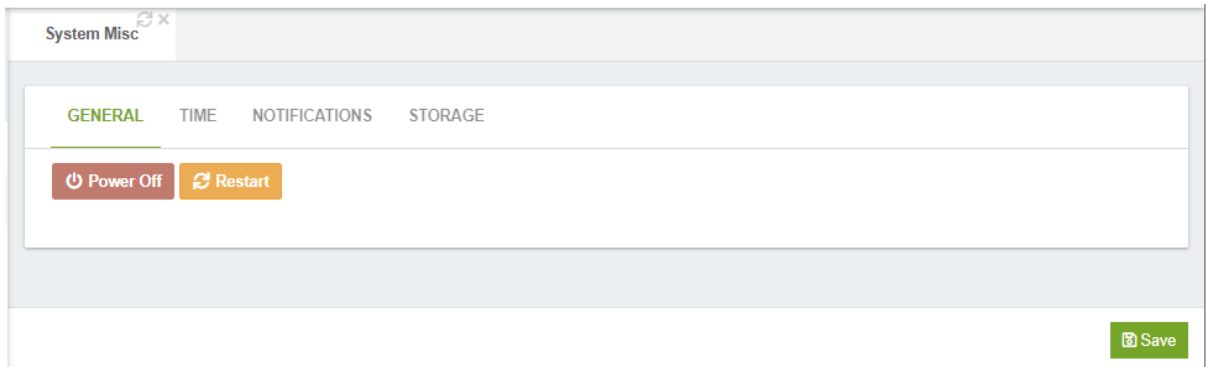


## 9.2. System Settings

### 9.2.1 System Miscellaneous

In this tab you will find the information about System Miscellaneous Settings.

#### General

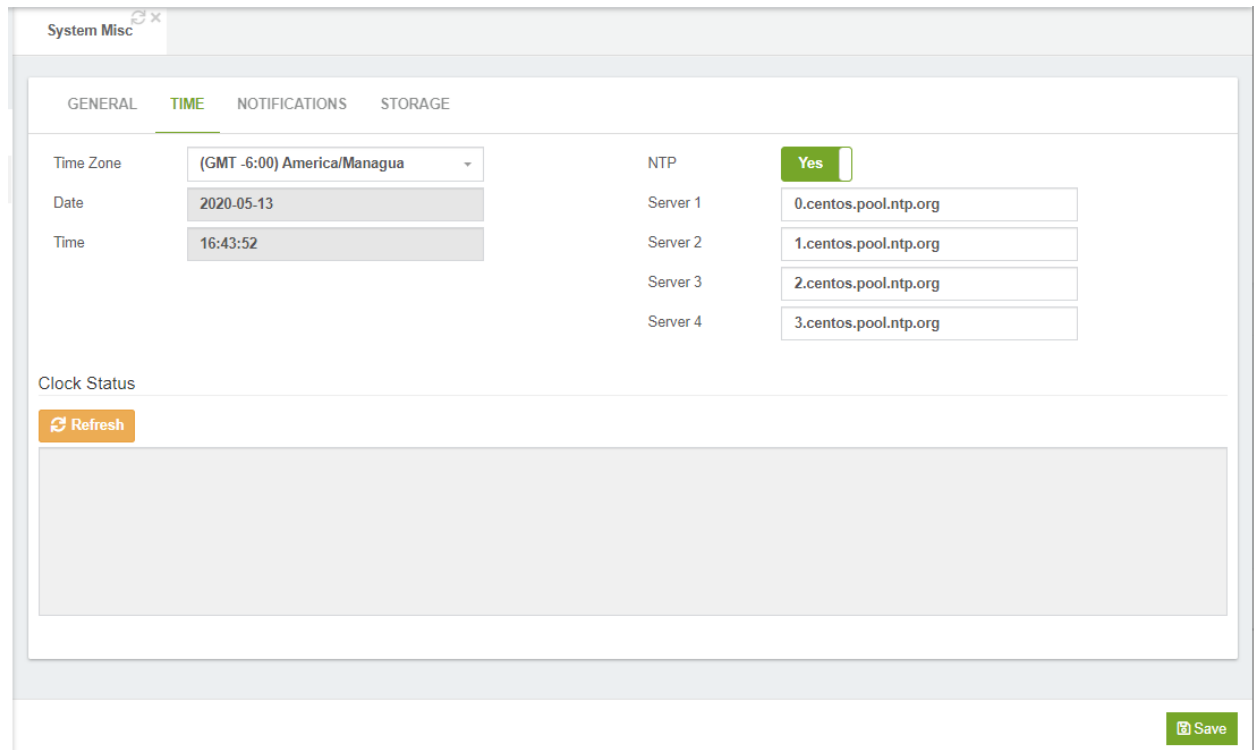


The screenshot shows the 'System Misc' window with the 'GENERAL' tab selected. At the top, there are four tabs: 'GENERAL', 'TIME', 'NOTIFICATIONS', and 'STORAGE'. Below the tabs, there are two buttons: 'Power Off' (with a power icon) and 'Restart' (with a refresh icon). At the bottom right of the window, there is a 'Save' button (with a floppy disk icon).

 , server power off (be careful).

 , restart Asterisk.

#### Time



The screenshot shows the 'System Misc' window with the 'TIME' tab selected. The 'GENERAL' tab is also visible. The 'TIME' tab contains the following settings:

Setting	Value
Time Zone	(GMT -6:00) America/Managua
Date	2020-05-13
Time	16:43:52
NTP	Yes
Server 1	0.centos.pool.ntp.org
Server 2	1.centos.pool.ntp.org
Server 3	2.centos.pool.ntp.org
Server 4	3.centos.pool.ntp.org

Below the settings, there is a 'Clock Status' section with a 'Refresh' button. At the bottom right of the window, there is a 'Save' button.

**Time Zone**, this sets the server time zone.

- Date**, here you can set date of the system.
- Time**, here you can set time of the system.
- NTP**, Enable/Disable NTP.
- Server1**, NTP server.
- Server2**, NTP server.
- Server3**, NTP server.
- Server4**, NTP server.

## Notifications

The screenshot shows the 'System Misc' configuration page with the 'NOTIFICATIONS' tab selected. The page contains four input fields: 'From Address', 'Storage Notifications', 'Intrusion Email', and 'Abnormal Call Volume'. A green 'Save' button is located at the bottom right.

- From Address**, the address entered here will be set as the "From:" address
- Storage Notifications**, this will send notifications if your hard drive become low on space or the raid has been broken.
- Intrusion Detection**, this will send notifications if a remote ip has been banned from your system.
- Abnormal call Volume**, this will send notifications to notify you of abnormal call volumes.

## Storage

The screenshot shows the 'System Misc' configuration page with the 'STORAGE' tab selected. It features a storage icon, a progress bar showing 7 GB used of 50 GB (13.76%), a text input field with the value '70', and 'Enabled' and 'Disabled' radio buttons. A green 'Save' button is at the bottom right.

## 9.2.2 Email Settings

Server allows you the option to send outbound email messages either by using the built-in mail server (such as Postfix) that is active on the PBX server, or by using a network-accessible relay server that is hosted on another machine. Click on Use Built-in Mail Server to use the built-in mail server that is active on PBX or Use External Mail Server to use a network-accessible relay server.

In this tab you will find the information about email settings.

### General

The screenshot shows the 'Email Settings' window with the 'GENERAL' tab selected. It features two radio buttons: 'Use Built-in Mail Server' (which is selected) and 'Use External Mail Server'. Below these are four input fields for 'From Address', 'Hostname', 'Origin', and 'Domain'. A 'Test Saved Email Settings' section contains a text input field with 'admin' and an email icon. An 'Email Log' section has a 'Refresh' button and a large empty area. A 'Save' button is located at the bottom right.

**Server**, you can relay outbound email messages either by using a built-in mail server (such as Postfix) that is active on the VitalPBX server, or by using a network-accessible relay server that is hosted on another machine.

**From Address**, the address entered here will be set as the “From:” address.

**Provider**, provider can be Gmail, or any other provider. The only additional information required for Gmail is Username and Password.

**SMTP Server**, the address that your provider has given you to enable you to send outgoing emails.

**Port**, SMTP server IP port number. By default, port 25 is used.

**Origin**, this specifies the origin domain for all mail posted by the PBX. By default, origin is configured to use your server hostname (e.g.,pbx.mycompany.com)

**TLS**, Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client

communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

**Authentication**, here you can select the Use Authentication button if your email provider requires authentication (Username and Password) to send outgoing email.

**Username**, username that your email service provider has given you to allow you to access your email account. Typically, this would be something like user@my-mail-server.com.

**Password**, the password that you use to log into your email account.

**Testing Email Settings**, testing the email settings.

**Email Log**, display email event log.

## 9.2.3 Email Templates

### General

Notification Type	Actions
New Voicemail Email	
Extension Welcome Email	
Emergency Notification Email	
Tenant Welcome Email	
Phonebooks QR Email	

From Version 3 and onward, you can send various email notifications, and on this module, you can customize the email templates. You can customize the following types of email notifications.

**New Voicemail Email**, here you can customize the email notification sent when using the voicemail to email feature.

**Extension Welcome Email**, here you can customize the email notification sent to new extensions. This is the same email sent when you select “Send Welcome Email” on the Extensions Module.

**Emergency Notification Email**, this is the email to be sent to the Emergency Contacts under the Emergency Numbers Module.

**Tenant Welcome Email**, this is an email sent to the tenant administrator whenever a new tenant is created and assigned to them.

**Phonebooks QR Email**, this is the email sent when you press the “Email QR code” option on the Phonebooks module.



You can then perform a couple of actions. These would be to edit the email templates and to send a test email, so you can verify the email's design.

## 9.2.4 Certificates

In this tab you will find the information about Certificates.

### General

The screenshot shows a web interface for configuring certificates. The 'GENERAL' tab is active. The form contains the following fields:

- Type:** A dropdown menu currently set to 'Let's Encrypt'.
- Description \*:** A text input field.
- Hostname \*:** A text input field.
- Owners Email:** A text input field.
- Country:** A dropdown menu currently set to 'United States'.
- State:** A dropdown menu currently set to 'Alabama'.

A green 'Save' button is located at the bottom right of the form.

**Type,** certificate type, Self Signed, Let's Encrypt or Custom

**Description,** short description to identify this certificate.

**Hostname,** name of hostname

**Owner Email,** Owners Email (Let's Encrypt only).

**Country,** Country (Let's Encrypt only).

**State,** State (Let's Encrypt only).

**Certificate,** this should be the content of certificate file (e.g.: certificate.crt) (Custom only).

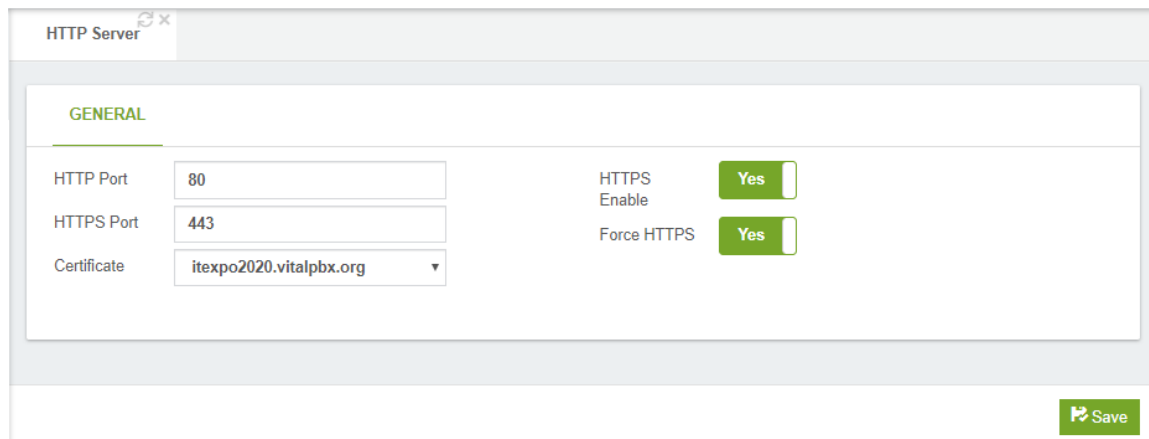
**Key,** this should be the content of key file (e.g.: private.key) (Custom only).

**Chain,** this should be the content intermediate certificate file (e.g.: ca\_bundle.crt) (Custom only).

## 9.2.5 HTTP Server

In this tab you will find the information about HTTP Server settings.

### General



The screenshot shows the 'HTTP Server' configuration window with the 'GENERAL' tab selected. The settings are as follows:

Field	Value	Field	Value
HTTP Port	80	HTTPS Enable	Yes
HTTPS Port	443	Force HTTPS	Yes
Certificate	itexpo2020.vitalpbx.org		

A 'Save' button is located at the bottom right of the configuration window.

**HTTP Port**, it defines from which port will be accessible the GUI through HTTP protocol.

**HTTPS Port**, it defines from which port will be accessible the GUI through HTTPS protocol.

**Certificate**, it defines the certificate to use when the GUI be accessed through HTTPS. By default, the pre-build certificate is used, if you want to use another go to Certificates module to generate one.

**HTTPS Enable**, if checked the GUI will be accessible through HTTPS. Enable by default.

**Force HTTPS**, if checked all the traffic to HTTP protocol it will be redirected to HTTPS protocol.

## 9.3 Firewall

### 9.3.1 Settings

VitalPBX comes with a pre-configured firewall built in. You can choose to enable or disable the Firewall from here.

Intrusion Detection configures the Fail2ban application, which detects unauthorized attempts to access the system. After detecting the possible intruder, the IP Address from the intruder will be banned to prevent any further access attempts for a period of time.

A possible intrusion is defined by a specified quantity of failed attempts within a specific time frame defined in seconds. An alert can be sent to a defined email address to alert about the possible intrusion once it is detected.

You can create a whitelist of the IP Addresses that must be ignored by this application. Usually, you must include the PBX on the White List, by adding the localhost 127.0.0.1 to the White List Section.

In this module you will find information about the status of the firewall.

#### General

The screenshot shows the 'Firewall Settings' web interface. It features three tabs: 'GENERAL', 'WHITELIST', and 'BANLIST'. The 'GENERAL' tab is selected. The settings are as follows:

- Enable Firewall:** Yes (checked)
- Enable Intrusion Detection:** Yes (checked)
- Block ICMP Requests:** No
- Intrusion Detection Settings:**
  - Failed Attempts Allowed:** 3
  - Find Time:** 600
  - Ban Time:** 86400
  - Notifications E-mail:** (empty field)

A 'Save' button is located at the bottom right of the form.

**Enable Firewall,** enable or disable the Firewall

**Enable Intrusion Detection,** enable or disable the intrusion detection.

**Block ICMP Requests,** when this is enabled, the system will ignore any ping requests sent to it.

#### Intrusion Detection Settings Section

**Failed Attempts Allowed,** this is the number of attempts allowed before banning the IP address.

**Find Time (seconds),** this is the period of time that the number of failed attempts are placed in before getting banned.

**Ban time (seconds)**, this is amount of time in which the possible intruder will be banned for. Set to -1 for permanent banning.

**Send Notification**, here you can define the email address to send an email notification to when an intrusion is detected

## Whitelist


The screenshot shows the 'Whitelist' tab in the Firewall Settings interface. It contains a table with two columns: 'Host' and 'Description'. Each row represents a whitelisted IP address and its corresponding description. There are also 'Add' and 'Save' buttons at the bottom right of the table.

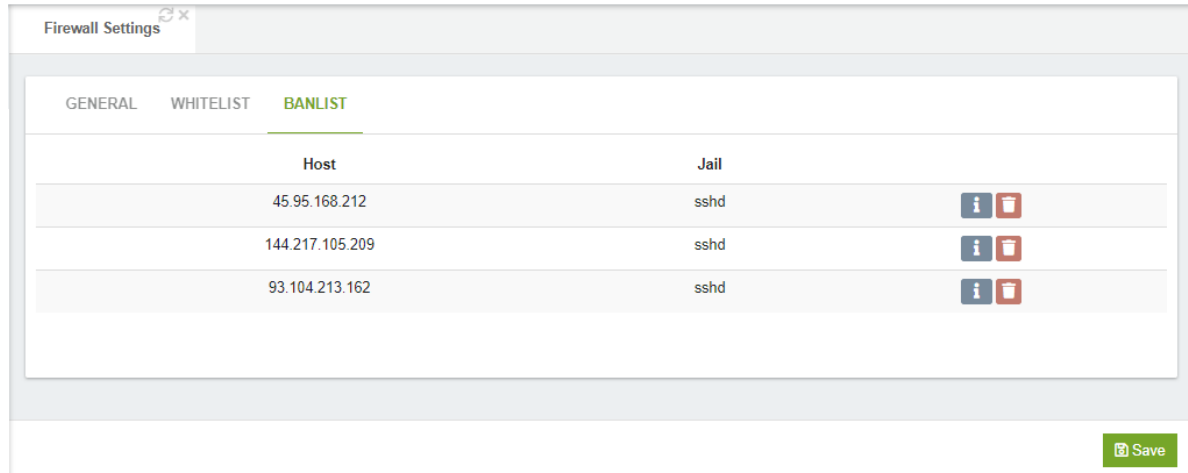
Host	Description
192.168.31.0/24	DHCP Addresses
192.168.25.0/24	eBD Addresses
192.168.26.0/24	Telesoft Addresses
192.168.24.0/24	Gateway Addresses
192.168.24.0/24	Gateway Addresses
10.8.2.0/24	Public VPN
186.77.196.68/32	Rodrigo Cuadra

**Host**, IP Address or hostname.

**Description**, a brief description to identify the IP address.


## Banlist

Here, you will find any IP address that has been banned. It will be shown on the table below. This table shows the IP Address that has been banned, as well as the Jail for the reason it was banned. If a host appears incorrectly on this list, you click on the  button to remove them from the list.



**Host**, Banned IP Address.

**Jail**, the type of action that was tried to be executed before the banning.

 , additional information about the banned IP address.

 , by pressing this option you can unban the IP Address.

## 9.3.2 Firewall Services







































On this module you can create and modify the different firewall rules services.

If the Firewall is enabled, you can define various applications here. It is possible to add additional applications specific to your installation. To add an application, click on the “Add” button at the bottom of the module.

Firewall Services

GENERAL

Show 25 entries Search:

Service Name	Port	Protocol	Actions
SIP	5060	Both	 
DNS	53	Both	 
NTP	123	UDP	 
DHCP	67-68	UDP	 
HTTP	80	TCP	 
SSH	22	TCP	 
RTP	10000-20000	UDP	 
IAX2	4569	UDP	 
mDNS	5353	UDP	 
Sonata Switchboard	3001	TCP	 
HTTPS	443	TCP	 
Asterisk HTTP Daemon	8088-8089	Both	 
PJSIP	5062-5063	Both	 
VPBX Dashboard	3000	TCP	 
VPBX Dashboard (HTTPS)	3005	TCP	 
Sonata Switchboard(HTTPS)	3008	TCP	 
VDI WebSocket	6001,6003	TCP	 
MySQL	3306	TCP	 
OpenVPN	1194	UDP	 

Showing 1 to 19 of 19 entries Previous 1 Next

[Add Service](#)

**Name**, here you can give the application a meaningful name to help you to easily recognize it. This name will be used to refer to the application in the Rules table.

**Protocol**, this determines the protocol that will be used by the application. Can be any one of TCP, UDP, or Both.

**Port**, the IP ports that are used by the application. This can be defined as a single port (e.g. 80), a range of ports (e.g. 10000:20000), or a list of ports separated by commas (e.g. 80, 10000:20000, 5060).

## List of important ports

<b>Service</b>	<b>Protocol</b>	<b>Port</b>
SIP	UDP/TCP	5060
DNS	UDP/TCP	53
NTP	UDP	123
DHCP	UDP	67-68
HTTP	TCP	80
SSH	TCP	22
RTP	UDP	10000-20000
IAX2	UDP	4569
Sonata SwitchBoard	TCP	3001
Sonata SwitchBoard (HTTPS)	TCP	3008
mDNS	UDP	5353
HTTPS	TCP	443
Asterisk HTTP Daemon	UDP/TCP	8088-8089
PJSIP	UDP/TCP	5062-5063
VPBX Dashboard	TCP	3000
VPBX Dashboard (HTTPS)	TCP	3005
MySql	TCP	3306
AMI	TCP	5038
OpenVPN	UDP	1194

## 9.3.3 Firewall Rules

### General

Seq.	Service	Source	Destination	Action	
0	RTP			ACCEPT	
1	SIP			ACCEPT	
2	HTTP			ACCEPT	
3	HTTPS			ACCEPT	
4	SSH			ACCEPT	
5	DHCP			ACCEPT	
6	DNS			ACCEPT	
7	NTP			ACCEPT	
8	IAX2			ACCEPT	
9	mDNS		224.0.0.251	ACCEPT	
10	Sonata Switchboard			ACCEPT	
11	PJSIP			ACCEPT	
12	VPBX Dashboard			ACCEPT	
13	VPBX Dashboard (HTTPS)			ACCEPT	
14	Sonata Switchboard(HTTPS)			ACCEPT	
15	VIXI WebSocket			ACCEPT	
16	MySQL	192.168.26.0/24		ACCEPT	
16	OpenVPN			ACCEPT	

Showing 1 to 18 of 18 entries

Previous 1 Next

Add Rule

**Service**, name of the services to use.

**Source**, this is used if you want the rule to be restricted to messages that are sent from a specific IP address or subnet only. Use any to allow all IP addresses. If you want to restrict the rule to a specific IP address, then you have to define the IP address with 32 as the subnet mask. If you use IPv6 then the subnet mask must be 128. In most cases you will define IP address as any.

**Destination**, here you can follow the same conventions as for Source above.

**Action**, configures whether this rule should Allow, Deny, or Reject access.

- **ACCEPT**, allow will pass all messages regardless of any rules that may be defined.
- **REJECT**, reject means that the packet is not allowed to pass, and a response is given to the originator of the request.
- **DROP**, drop means that the packet is discarded, but no response is given to the originator of the request.



## 9.4 Network

### 9.4.1 Network Settings

The Network Settings dialog allows you to configure the network environment of the PBX server.

In this tab you will find the information about Network Settings.

#### General

**Hostname**, hostname of the system.

**Device**, the physical device to use for this connection.

**Name**, name of the connection.

**DHCP**, whether to use DHCP on this connection for obtaining network configuration automatically.

**IP Address**, IP address to assign to this connection.

**Netmask**, network mask or prefix.

**Gateway**, gateway IP address to use.

**Search Domain**, this restricts DNS searches to the specified domain.

**Primary DNS**, primary DNS IP address.

**Secondary DNS**, secondary DNS IP address.

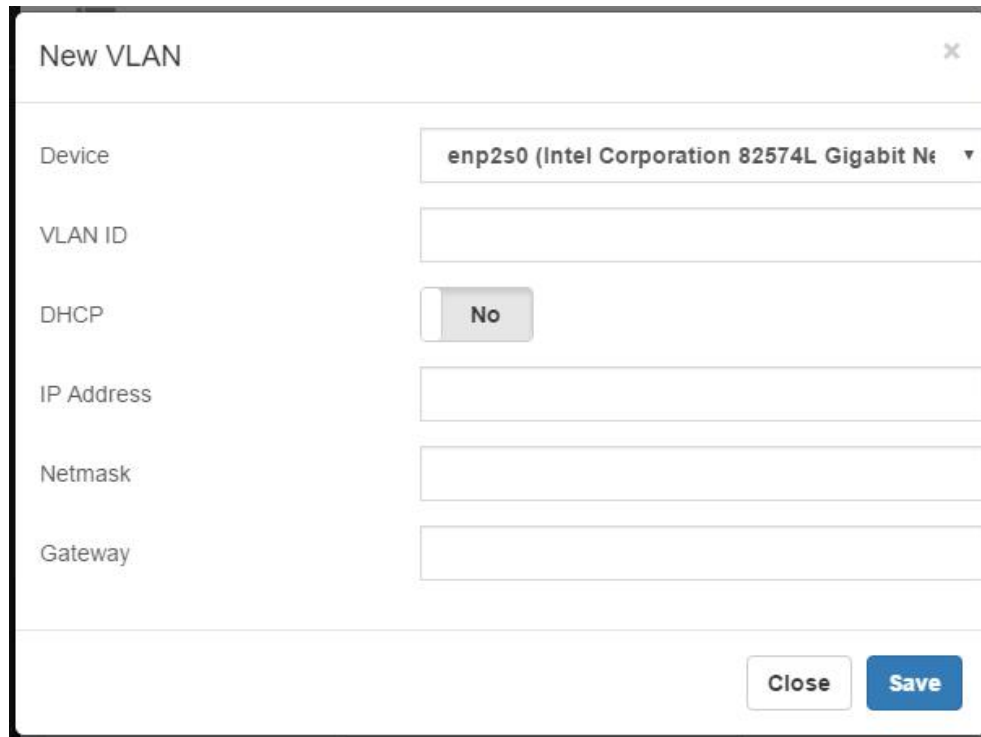
**Active**, whether this connection is currently active.

**Auto connect**, whether this connection should be enabled on startup.

**Default Router**, whether to use this gateway as the default route.

**Additional IP Addresses**, add additional IP addresses to this interface.

### Add VLAN



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

- Device:** A dropdown menu showing 'enp2s0 (Intel Corporation 82574L Gigabit Net'.
- VLAN ID:** An empty text input field.
- DHCP:** A toggle switch currently set to 'No'.
- IP Address:** An empty text input field.
- Netmask:** An empty text input field.
- Gateway:** An empty text input field.
- Buttons:** 'Close' and 'Save' buttons at the bottom right.

**Device**, the physical device to use for this connection.

**VLAN ID**, VLAN ID for this connection, leave blank if you do not wish to use a VLAN.

**DHCP**, whether to use DHCP on this connection for obtaining network configuration automatically.

**IP Address**, IP address to assign to this connection.

**Netmask**, network mask or prefix.

**Gateway**, gateway IP address to use.

## 9.4.2 DHCP Settings

Dynamic Host Configuration Protocol (DHCP) is the mechanism that dynamically allocates physical IP addresses to machines and devices on the network. You can choose to use an existing DHCP server on your network, or to use PBX as your DHCP server. If you want to use PBX as your DHCP server, check on the Enable button.



**Be careful!**

You can only have one active DHCP server on your network.

In this tab you will find the information about DHCP settings.

### General

**DHCP Server**

**GENERAL**

DHCP:  Enabled  Disabled

Disabled Interfaces:

Start Address \*:

End Address \*:

Lease Time \*:  Days

Gateway:

Primary DNS:

Secondary DNS:

NTP Server:

Option 66:

Use for Endpoint Manager:  No

WINS:

Static Leases

MAC Address	IP Address	Hostname (optional)
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="IP Address"/>	<input type="text" value="Hostname"/>

**DHCP**, set this to enable if you want VitalPBX to act as a DHCP server for this network, or Disable if you already have a DHCP server on this network.

**Disables Interface**, you can disable DHCP on one or more interfaces. If you wish to specify multiple interfaces, separate them with commas. For example: eth0, eth0.201

**Start Address\***, the first address on your network that can be allocated as a dynamic IP address.

**End Address\***, the last address on your network that can be allocated as a dynamic IP address.

**Lease Time\***, period that the DHCP server grants an IP address to a device. The device must renew its IP address before the end of the period.

**Gateway**, the default IP gateway address.

**Primary DNS**, domain Name System (DNS) translates Internet domain and host names to physical IP addresses in numerical notation, i.e. from mypbx.mydomain.com to 67.67.222.220.

**Secondary DNS**, here you can define a Secondary DNS to be used if your primary DNS fails to respond.

**NTP Server**, network Time Protocol (NTP) is a networking protocol to synchronize clocks between computer systems over the Internet.

**Option 66**, option 66 provides IP phones with an URL for configuration provisioning. VitalPBX Endpoint Manager provides the IP phones with configuration information in response to a HTTP request. The format of the request URL in this case looks like `http://[pbx-ip-address]/xepm-provision/`. If you define the PBX IP address or host name in the Option 66 field and check the 'Use for Endpoint Manager' checkbox then the correct format of the URL will be built automatically. If you have already-prepared IP phone configuration files located in the /tftpboot directory, then you should put the PBX IP address or host name in the Option 66 field and uncheck the 'Use for Endpoint Manager' checkbox.

**Use for End Point Manager**, automatically format the Option 66 address for Endpoint Manager based on the address provided for Option 66 above. This will be done by prefixing `http://` to the Option 66 address above and appending `/xepm-provision/`. In order for this to work correctly, the IP address provided above for Option 66 should only consist of the IP address or hostname of the server.

**WINS**, windows Internet Name Service (WINS) is a name resolution service that maps NetBIOS names to an IP address on the network that uses NetBIOS over TCP/IP (NetBT). The primary purpose of WINS is to support clients that run older versions of Windows and applications that use NetBIOS.

### Static Leases Section

**MAC Address**, device MAC address.

**IP Address**, device IP address.

**Host Name (optional)**, host name.

## 9.4.3 OpenVPN Server

OpenVPN Access Server is a full featured secure network tunneling VPN software solution that integrates OpenVPN server capabilities, enterprise management capabilities, simplified OpenVPN Connect UI, and OpenVPN Client software packages that accommodate Windows, MAC, Linux, Android, and iOS environments. OpenVPN Access Server supports a wide range of configurations, including secure and granular remote access to internal network and/ or private cloud network resources and applications with fine-grained access control.

To install the OpenVPN module you must go to Admin > Add-ons > Add-ons. Press Check-Online and install VitalPBX OpenVPN. The free version is limited only to the creation of two VPN Clients.

In this tab you will find the information about OpenVPN Server.

### Server

SERVER		CLIENTS	
Enabled	<input checked="" type="checkbox"/>	Redirect Gateway	<input checked="" type="checkbox"/>
Port	1194	Primary DNS	8.8.8.8
Server Range	10.8.0.0 - 255.255.255.0	Secondary DNS	8.8.4.4
Public Host		Max Clients	100
Keep-Alive	10 - 120	Compression	comp-lzo
Cipher Method	Blowfish		

**Enabled**, it shows the current status of the OpenVPN Server service.

**Port**, the port that OpenVPN should listen on.

**Server Range**, this defines the virtual IP range to be used in the VPN tunnel network. e.g.: if you use as range the IP address 10.8.0.0, the server IP will be 10.8.0.1 and the first client will be assigned the IP 10.8.0.2.

**Public Host**, remote host or IP address on the client, which specifies the OpenVPN server.

**Keep-Alive**, the keepalive directive causes ping-like messages to be sent back and forth over the link so that each side knows when the other side has gone down. All values in seconds.

**Redirect Gateway**, if enabled, this directive will configure all clients to redirect their default network gateway through the VPN, causing all IP traffic such as web browsing and DNS lookups to go through the VPN (The OpenVPN server machine may need to NAT or bridge the TUN/TAP interface to the internet in order for this to work properly).

**Primary DNS**, Primary DNS to use when the “Redirect Gateway” option is enabled.

**Secondary DNS**, Secondary DNS to use when the “Redirect Gateway” option is enabled.

**Max Clients**, the maximum number of concurrently connected clients we want to allow.

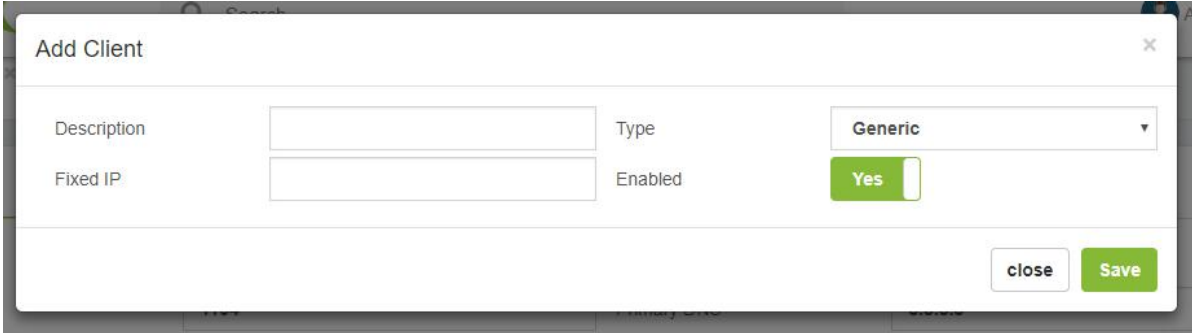
**Cipher method**, encrypt data channel packets with cipher algorithm alg. You have the following options.

- Blowfish
- AES-128
- AES-256
- Triple-DES

**Compression**, this allows you to define the type of compression to use between server & clients traffic. You have the following options.

- None
- comp-lzo
- lz4-v2

## Add Client



Description	<input type="text"/>	Type	Generic
Fixed IP	<input type="text"/>	Enabled	Yes

close Save

**Description**, a short description to identify this OpenVPN client.

**Fixed IP**, this allows you to assign a specific IP address to this client.

**Type**, it allows to define the type of client, depending on it, the configuration that is downloaded will vary. You can choose between:

- Generic
- Yealink
- Grandstream
- VitalPBX
- Fanvil

**Enabled**, it allows you to enable or disable this user.

## Clients

In this tab you will find the information about OpenVPN Clients.

Description	Assigned IP	Real Address	Connected	Packets Rx / Tx	Connected Since	Type	Enabled	Actions
Grandstream 1625			No			Grandstream	Yes	
Iphone Rodrigo Cuadra			No			Generic	Yes	

**Description**, a short description to identify this OpenVPN client.

**Assigned IP**, IP assigned at the time of the VPN connection.

**Real Address**, the IP from where the VPN request comes.

**Connected**, connection status.

**Packets Rx/Tx**, Packages received and transmitted.

**Connected Since**, it shows how long the connection has been established.

**Type**, it allows to define the type of client, depending on it, the configuration that is downloaded will vary.

**Enabled**, it allows you to enable or disable this user.

Actions

**Edit**, modify the client

**Download**, download the config file to be installed on the client.

**Delete**, delete the client.

Notes:

When you create the SIP extension to connect remember that to have audio it is necessary in the configuration NAT must be Force, Comedy.

If for some reason an IP range was configured for security in Settings > Technology > SIP Settings > Network tab, Local Network section, remember to add the new IP range that was configured in OpenVPN Server. By default, VitalPBX does not bring any restriction.

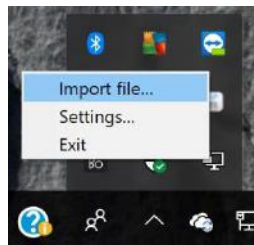
The screenshot shows the 'SIP Settings' window with the 'NETWORK' tab selected. The settings are organized into several sections:

- GENERAL:** TCP Enable (Yes), Enable TLS (Yes).
- TCP Bind Address:** Address and Port fields.
- TLS Bind Address:** 0.0.0.0 and 5061.
- TLS Do Not Verify:** Yes.
- TLS Certificate:** My Local.
- NAT:** External Address, External Host, and External Refresh fields.
- Local Networks:** A table with columns for IP Address and Network Mask. One entry is shown: IP Address: 0.0.0.0, Network Mask: 255.255.255.0. An 'Add' button is present.

A 'Save' button is located at the bottom right of the window.

## OpenVPN Desktop Client Setup [ Windows ]

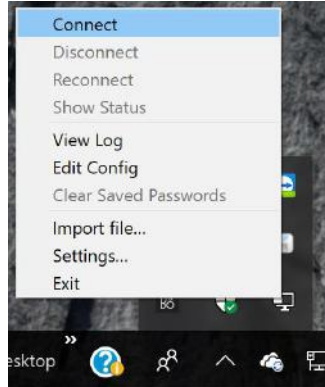
- **Step 1:** Download and Install the OpenVPN Desktop Client
- <https://openvpn.net/index.php/open-source/downloads.html>
- **Step 2:** Create OpenVPN Client and Download Config File
- Download the OpenVPN Config file from your VitalPBX Server.
- **Step 3:** Add OpenVPN Configuration File to the Desktop Client
- Run the OpenVPN Client. Go to Tray Bar, select OpenVPN Icon + Right-Click. Then Import File.



Locate and unzip your OpenVPN configuration file (client\_full.ovpn) and import it.

- **Step 4:** Connect to OpenVPN





**Step 5:** It was assigned an IP corresponding to the range programmed in the Server section. Remember that the IP to reach VitalPBX is the first in that range, that is, if we have the range 10.8.0.0, the IP of the PBX is 10.8.0.1.

## OpenVPN Grandstream Client Setup

VitalPBX includes a new OpenVPN module that together with the current Grandstream firmware includes support (server/client mode) which allows you to tunnel the whole SIP/RTP traffic over an encrypted channel. This is also the best solution to avoid any kind of NAT/routing issues because all devices are directly accessible within the virtual ip subnet.

Next we will show how to configure a Grandstream phone.

- 1.- First make sure that the compression is of the “comp-lzo” type in the Server configuration.
- 2.- We create a client as Grandstream Type and download the configuration.



- 3.- In the compressed file that we download there are 3 files:

ca.crt  
clientX.crt  
clientX.key

4.- Now we go to the phone and in Network/OpenVPN® Settings

### OpenVPN® Settings

OpenVPN® Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
OpenVPN® Server Address	<input type="text"/>
OpenVPN® Port	<input type="text" value="1194"/>
OpenVPN® Transport	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
OpenVPN® CA	<input type="button" value="Upload"/> <input type="button" value="Delete"/>
OpenVPN® Certificate	<input type="button" value="Upload"/> <input type="button" value="Delete"/>
OpenVPN® Client Key	<input type="button" value="Upload"/> <input type="button" value="Delete"/>
OpenVPN® Cipher Method	<input checked="" type="radio"/> Blowfish <input type="radio"/> AES-128 <input type="radio"/> AES-256 <input type="radio"/> Triple-DES
OpenVPN® Username	<input type="text" value="admin"/>
OpenVPN® Password	<input type="password" value="*****"/>
<input type="button" value="Save"/> <input type="button" value="Save and Apply"/> <input type="button" value="Reset"/>	

OpenVPN® Server Address, we configure the IP/Domain of our server.

OpenVPN® Port, here we configure the port to access the server.

OpenVPN® CA, we load ca.crt file.

OpenVPN® Certificate, we load clientX.crt file.

OpenVPN® Client key, we load clientX.key file.

After establishing the tunnel, it is necessary to configure the SIP account of the telephone. Remember that the IP to reach VitalPBX is the first in that range, that is, if we have the range 10.8.0.0, the IP of the PBX is 10.8.0.1.

### OpenVPN Yealink Client Setup

VitalPBX includes a new OpenVPN module that together with the current Yealink firmware includes support (server/client mode) which allows you to tunnel the whole SIP/RTP traffic over an encrypted channel. This is also the best solution to avoid any kind of NAT/routing issues because all devices are directly accessible within the virtual ip subnet.

Next we will show how to configure a Yealink phone.

1.- First make sure that the compression is of the “comp-lzo” type in the Server configuration.

2.- We create a client as Yealink Type and download the configuration.



Now we are going to configure a Yealink phone, uploading the tar file in Network/Advanced VPN Section.

**VPN**

Active

Upload VPN Config

Copyright © 1998-2018 \*\*Inc. All Rights Reserved

**Active**, enable the VPN option.

**Upload VPN Config**, here you can upload the previously downloaded tar file.

After establishing the tunnel, it is necessary to configure the SIP account of the telephone. Remember that the IP to reach VitalPBX is the first in that range, that is, if we have the range 10.8.0.0, the IP of the PBX is 10.8.0.1.

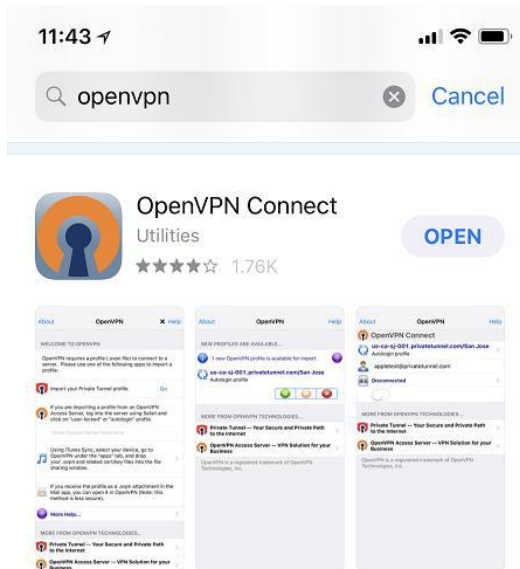
## iPhone (mobile) VoIP over OpenVPN in VitalPBX

The OpenVPN protocol is not one that is built into the Apple iOS operating system for iPhones, iPads, and iPods. Therefore, a client program is required that can handle capturing the traffic you wish to send through the OpenVPN tunnel and encrypting it and passing it to the OpenVPN server. And of course, the reverse, to decrypt the return traffic. So, a client program is required, and there is only one client available that works on standard Apple iOS devices.

### Official OpenVPN Connect app

On the official Apple App Store, the client you can download and install for free there is called OpenVPN Connect. This program supports only one active VPN tunnel at a time. Trying to connect to two different servers at the same time is a function that is not build into the official application OpenVPN Connect app, and it is also not possible because the underlying operating system does not allow this. The OpenVPN Connect app is able to remember multiple different servers, but only one can be active at a time.

To obtain the OpenVPN Connect app, go to the Apple App Store on your Apple iOS device. Look for the words "openvpn connect" and the application will show up in the search results. You can install it from there. Once installed an icon will be placed on your home screen where you can find the app.

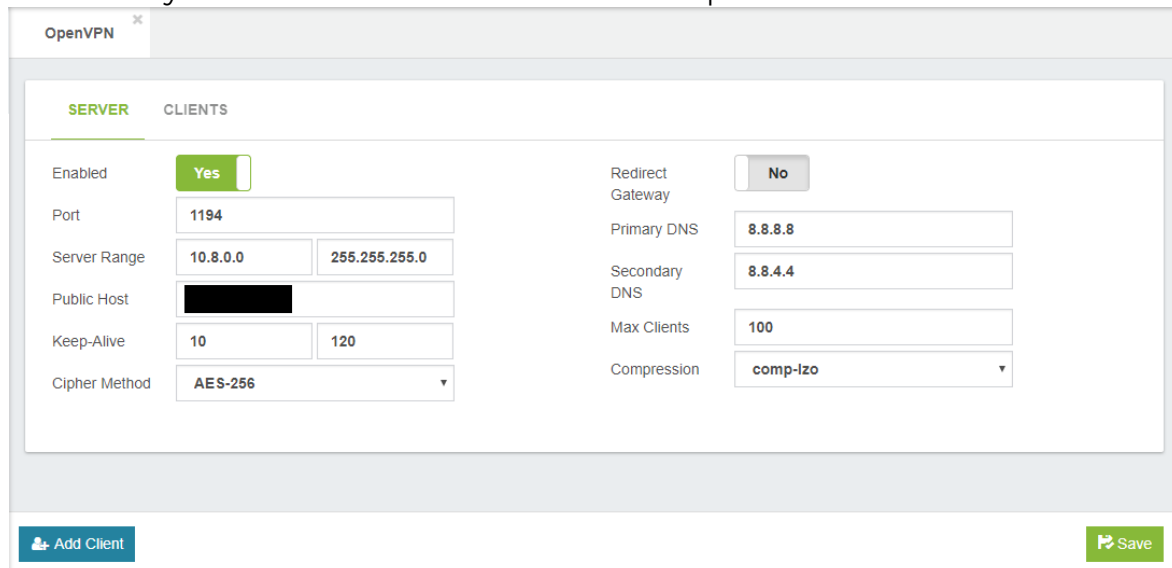


Next, we will show how to configure a Iphone OpenVPN phone.

1.- First make sure that the Server Configuration is complete.

### Server

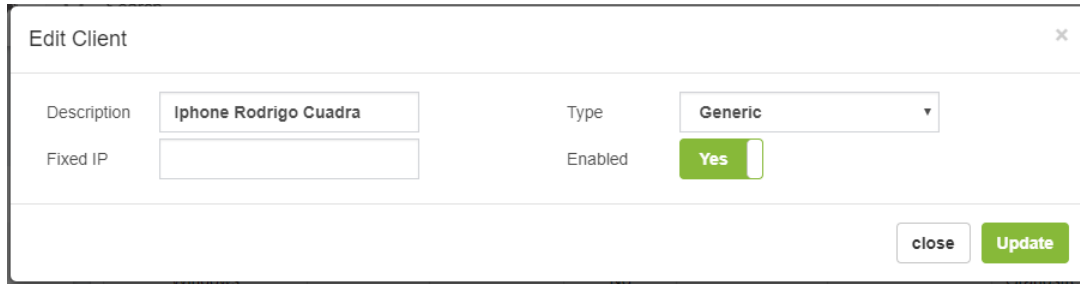
In this tab you will find the information about OpenVPN Server.



Add OpenVPN client by pressing the button on the bottom left



## Add Client



Description	<input type="text" value="Iphone Rodrigo Cuadra"/>	Type	<input type="text" value="Generic"/>
Fixed IP	<input type="text"/>	Enabled	<input type="button" value="Yes"/>

We create a client and download the configuration.



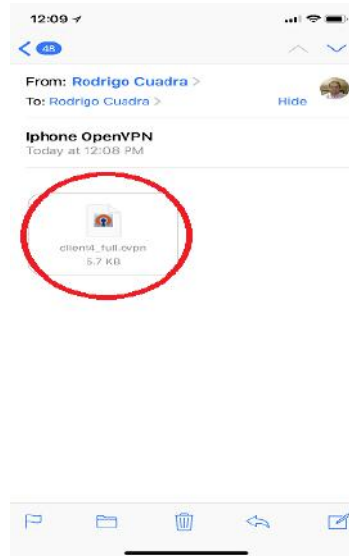
In the compressed file that we download there are 5 files:

- ca.crt
- clientX.crt
- clientX.key
- clientX.ovpn
- clientX\_full.ovpn

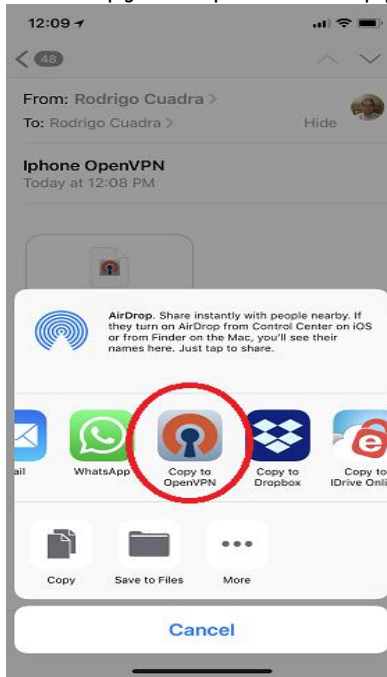
We are going to use only the number five named clientX\_full.ovpn.

Now we send an email to our account with the attachment to be read on our Iphone. When receiving the e-mail, we press on the attachment and in this way our OpneVPN will be configured. Please follow the next steps:

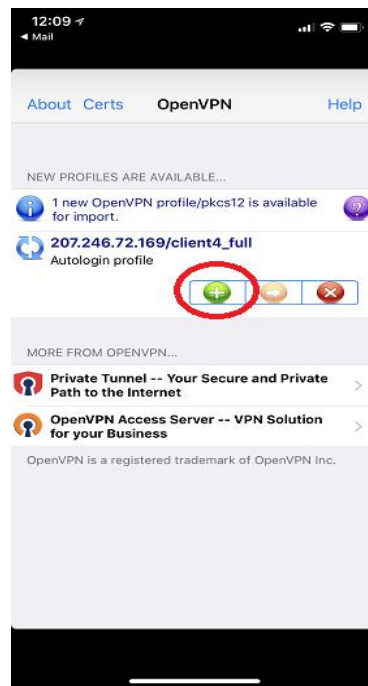
a.- Open the email



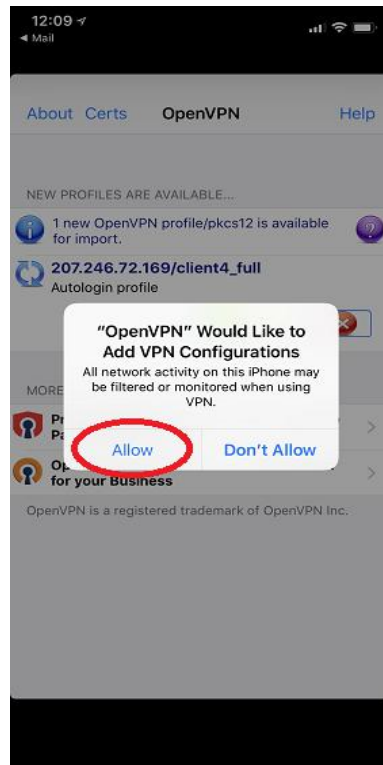
b.- Click the attach file and use Copy to OpenVPN App.



c.- Now add the profile.



d.- Then Allow the profile.



e.- Now that everything is configured just press the connect button



f.- If everything is OK, the connect button will turn green and you will see activity in the sending/receiving of packages.



After establishing the tunnel, it is necessary to configure the account of the SIP or IAX Mobile App. Remember that the IP to reach VitalPBX is the first in that range, that is, if we have the range 10.8.0.0, the IP of the PBX is 10.8.0.1.



## 9.4.4 OpenVPN Client

It is also possible for VitalPBX to connect as an OpenVPN Client to another PBX, this facilitates the interconnection between two VitalPBX.

First, create a Client for VitalPBX as you created it in the previous step.

Then, upload the certificate in this form and your two VitalPBX will be interconnected.

The screenshot shows the 'OpenVPN Client' configuration page. The 'GENERAL' tab is active. The 'VPN Configuration' field is empty with a file upload icon. The 'Connection Info' section contains the following data:

Service Status	Stopped	Assigned IP	0.0.0.0
Connection Status	Disconnected	Network Mask	0.0.0.0
Server IP	0.0.0.0		

The 'Connection Log' section displays '-- No entries --'. At the bottom right, there are two buttons: 'Enable' and 'Update Configuration'.

**VPN configuration**, allows to load the configuration of the OpenVPN client in TAR format, this was generated in OpenVPN / Add Client selecting VitalPBX type.

### Connection Information

**Service Status**, shows the status of the service. Do not confuse this status with the status of the connection, the service may be running, but not necessarily connected to the server.

**Connection Status**, shows the current connection status of the OpenVPN client.

**Server IP**, shows the OpenVPN Server IP.

**Assigned IP**, shows the IP address assigned by the OpenVPN server to this client.

**Network Mask**, network mask.

**Connection Record**, shows list of records.

## 9.4.5 GEO Firewall

### Increased security

With today's accessibility to the internet, the world has become even smaller and we are able to communicate with anyone around the globe. We now have voice over IP connections established through the internet, and that makes our connections to our business and homes more reachable. But sometimes, people from places we do not intend to give access to our means of communication, in this case, our PBX systems, try to connect and use it for their own benefit.

At VitalPBX we want to make it easier to control who can connect or not to our PBX system. That is why we have created this brand-new commercial module called "Geo Firewall". With the Geo Firewall add-on, you can choose specific countries that can and cannot connect to your PBX system. And we have made it as easy as it gets.



### How does it work?

To use the Geo Firewall add-on, you simply select the countries you wish to block access to your PBX, and then click "Save". It is as simple as that. The add-on will make sure to block any requests incoming from the blocked countries selected, and only allow from those that are allowed.

## 9.5 Add-ons

### 9.5.1 Add-ons

#### General

Addon	Installed Version	Available Version	Status	Actions
Branding	1.0.1-1	-		
Bulk Extensions	2.2.0-1	-		
Communicator	2.0.3-2	-		
Custom Contexts	2.3.0-1	-		
Dahdi	-	1.0.0-1		
Domotic	-	2.2.1-1		
Dynamic Destinations	1.0.0-1	-		
Epm	1.0.0-1	-		
Geo Firewall	2.0.1-2	-		
High Availability	-	1.0.1-1		
IVR Stats	2.2.0-5	-		
Maintenance	2.2.0-2	-		
Multi Tenant	2.0.3-8	-		
OpenVPN	2.0.0-4	-		

**Addon**, Name of the Module or Application.

**Installed Version**, Currently installed version.

**Available Update**, Currently available version.

**Status**, state of the Module or Application.

**Buy License** Activate/Buy the license, for this it is necessary to have bought a license in the VitalPBX store (<https://vitalpbx.org/en/vitalpbx-store/>),

See license with the possibility of revoke to be able to transfer it to another server.

**Actions**, there are three types of actions displayed depending on whether the plugin is installed or not:

Brief description of the plugin.

Install add-ons.

Uninstall the add-ons.

**Clean Cache**, if you have any problems with the installations or updates maybe you need to clean the cache, please use this button.

**Check Online**, please use this button to check the latest updates.

Next, we list the available add-ons with a brief description of them:

- **Rebranding**, the rebranding add-ons is a simple but powerful module that allows you to customize the VitalPBX GUI according to your preferences (colors, logo, title, application name, etc.).
- **Bulk Extensions**, the Bulk Extensions add-ons is totally free and allows you to create massive extension ranges with common settings. It's a powerful time-saving tool when creating a large number of extensions.
- **Communicator**, the Communicator add-ons allows you to centralize VitalPBX Communicator settings such as pauses and programmable keys. In addition, it allows you to create campaigns that can be used in the Communicator for automatic dialing (Outbound Campaigns).
- **Custom Context**, expand the power of VitalPBX with your own dial plan.
- **Dahdi**, this add-ons installs the DAHDI drivers and all the necessary settings to be able to manage telephony devices on your PBX.
- **Domotic**, automate your environment with home automation and Asterisk technologies.
- **Dynamic Destination**, allows you to make MySQL queries and API requests (HTTP / HTTPS), and depending on the response, the call will be routed to a specific destination according to the conditions defined in this module.
- **EPM**, this add-on installs all the necessary configurations to be able to provision various brands of telephones from the central.
- **Geo Firewall**, the Geo Firewall add-ons is very essential to prevent brute force attacks to your PBX from certain countries, therefore, installing this plugin will improve your security, decrease the likelihood of a hacker compromising your PBX and also you will prevent VoIP fraud.
- **High Availability**, allows you to monitor and manage HA nodes from the GUI.
- **IVR Stats**, the IVR Stats add-ons allows you to get reports on your customers' interaction with your IVRs, allowing you to know which options are used the most or which departments are requested the most, and more.
- **Maintenance**, with the "Maintenance" add-ons you can easily clean your PBX and save a lot of storage: by deleting old recordings or converting recordings from wav format to mp3, you can also delete recordings with short durations and old CDRs.
- **Multi Tenant**, the multi-tenant add-ons allows you to manage multiple clients (tenants) with a single instance of VitalPBX, allowing you to significantly reduce operating costs.
- **Open VPN**, the OpenVPN add-ons is a commercial module and allows you to configure an OpenVPN server and its clients directly from the GUI. The free version comes with all the features, but you can only set up two clients at most.
- **Paging PRO**, this add-ons expands the paging functionalities, allowing you to schedule ads to page to the list of defined members. This is useful for scheduling school bells or announcements at companies, airlines, train stations, etc.

- **Phone Books**, the phone book add-ons is completely free and allows you to generate unlimited internal and external phone books on the fly and use those phone books in the different supported brands (Yealink, Grandstream, Alcatel, Fanvil, Xorcom, Htek).
- **Queues CallBack**, Queued Callback allows you to optimize your customer experience by offering callers the ability to request a callback based on your call center conditions. When your call center experiences unexpected spikes in call volumes, the queued callback function steps in to offer your customer to call you back when an agent is available.
- **Task Manager**, the Task Manager add-ons is completely free and allows you to schedule tasks with custom user scripts through the GUI. The user must previously load the scripts to the path `/var/lib/vitalpbx/ scripts` and grant all the necessary permissions.
- **Trunk Passthrough**, this module allows you to send calls between trunks, thus turning your PBX into a recording server.
- **Virtual Faxes**, the virtual fax add-ons allows you to configure multiple fax modems to send and receive faxes from the VitalPBX graphical user interface.
- **Sonata Switchboard**, advanced monitoring software for your PBX, take control of your PBX with this powerful tool. You can monitor queues, trunks, outgoing/incoming calls, perform actions on calls and many other functionalities. All information is in real time.
- **Sonata Recordings**, a recording management system for your PBX that allows you to label, qualify calls and everything related to call center supervision.
- **Sonata Billing**, is a powerful software to rate and manage your PBX calls, it provides a collection of reports to have total control of your calls.
- **Sonata Stats**, a system through which you can obtain detailed and summarized reports of all the activity in your call center. Among the most important reports we have the SLA, Unanswered Calls, etc.

## 9.6 Tools

### 9.6.1 Backup & Restore

In this tab you will find the information about Backup & Restore.

#### General

The screenshot shows the 'Backup & Restore' configuration page. The 'GENERAL' section includes the following fields and options:

- Name:** Full Backup
- Run Automatically:** Daily Backup
- Comment:** Full PBX Backup
- Limit:** 2
- Include CDR Records:** Yes
- Include Call Recordings:** Yes
- Include Voicemail:** Yes
- Include Faxes:** Yes

The 'Backups List' table contains the following data:

Date & Time	Backup	VitalPBX Version	Actions
2018-01-30 14:27:31	vitalpbx-1517344051.tar (34.30 MB)	2.0.0-2b	[Download] [Restore] [Delete]
2018-01-30 11:24:07	vitalpbx-1517339047.tar (34.30 MB)	2.0.0-2b	[Download] [Restore] [Delete]

At the bottom of the interface, there are buttons for 'Run Backup Now!', 'Update', 'Delete', and 'New'.

**Name**, Descriptive name for this backup.

**Run Automatically**, it allows you to use a Cron previously created at PBX/Tools/Cron Profiles to automatically create a backup with your selected settings.

**Comment**, a user-defined comment that will be added to the backup.

**Limit**, it allows you to define the number of backup copies that will be stored. When the limit is reached, the oldest copy will be deleted.

**Include CRD Records**, enabling this will add CDR records to the backup.

**Include Call Recordings**, enabling this will add call recordings to the backup.

**Include Voicemail**, enabling this will add voicemail boxes to the backup.

**Include Faxes**, enabling this will add faxes to the backup.




#### Backup List

**Date & Time**, date and time the backup was made

**Backup**, name of the file that contains the backup.

**VitalPBX Version**, VitalPBX version of the backup.

**Actions**, possible actions that can be performed with the backup are:

-  Download
-  Restore
-  Delete

## 9.6.2 Maintenance

This is a simple add-on with powerful settings that allows you to save space in your PBX. This is a commercial add-on and you may buy it through the following link: [store.vitalpbx.org](https://store.vitalpbx.org)

### How it works.

The maintenance add-on has various settings, between them, the possibility to assign a Cron Profile item to schedule the execution of the configured options. These are the most powerful settings:

**Tenant**, allows you to select the tenant on which the maintenance configurations will be applied.

**Clear Oldest CDR**, allows you to define the maximum number of days that CDR should be retained. The CDR with more days than defined here will be deleted.

**Clear Oldest Recordings**, this option allows you to define the maximum number of days that recordings should be retained, allowing you to keep only the most recent recordings.

**Clear Short Recordings**, allows you to define the minimum duration in seconds for a recording to be considered as too short, and delete it.

**Schedule**, it allows you to define the schedule in which the maintenance of the PBX will be executed (Conversion of Recordings, Cleaning of Recordings and CDR, etc). If no schedule is selected, all the maintenance options will be disabled.

**Convert Recordings**, this option allows you to enable the conversion of CDR recordings from WAV to MP3.

**Enabled**, it allows you to enable or disable the PBX maintenance.

## 9.6.3 Branding

This simple but very useful add-on allows you to customize the VitalPBX colors, logos (Mobile and Desktop Version), browser title and others.

**Base Color**, main color used for active menu items, active form tabs and selected text.

**APP Title**, allows you to customize the header title that appears in the browser tab.

**APP Name**, it allows you to modify the main Tenant name.

**Slogan**, it allows you to customize the Slogan that appears in the login screen.

**Facebook Page**, it allows you to customize the Facebook Page link that appears in the login footer.

**Instagram Page**, it allows you to customize the **Instagram Page** link that appears in the login footer.

**Twitter Page**, it allows you to customize the Twitter Page link that appears in the login footer.

**YouTube Channel**, it allows you to customize the YouTube Channel link that appears in the login footer.

**Log In Footer**, it allows you to customize the footer content in the login screen.

**Meet URL**, URL to be used by default for conferences generated through the video conferences module.

**Desktop Logo**, logo to show when accessed from a desktop computer.



**Mobile Logo**, logo to show when it is accessed from a mobile.

## Login Design

The screenshot shows the 'Branding' configuration window with the 'LOGIN DESIGN' tab selected. The configuration options are as follows:

Field	Value
Login Background	[Blank]
Font Color	#769c7b
Form Background	#769c7b
Submit Button Color	#71a97b
Add-ons Menu	#647f67

Buttons for 'Reset' and 'Save' are visible at the bottom of the window.

**Login Background**, background color for the login page. If left in blank, the default background will be used.

**Font Color**, font color for the login page. If left in blank, the default color will be used.

**Form Background**, background color for left panel in the login form.

**Submit Button Color**, background color for the login button.

**Add-ons Menu**, background color for the add-ons menu button.

If you wish to also change the Welcome message when you access SSH, you must follow the following procedure

```

root@vitalpbx:~
login as: root
root@192.168.10.129's password:
Last login: Fri May 22 09:47:22 2020 from 192.168.10.119

VitalPBX

Version      : 3.0.0-1
Asterisk    : Asterisk 17.4.0
Linux Version : CentOS Linux release 7.8.2003 (Core)
Welcome to   : vitalpbx.local
Uptime      : 3 min
Load        : Last Minute: 0.24, Last 5 Minutes: 0.14, Last 15 Minutes: 0.06
Users       : 3 users
IP Address   : 192.168.10.129
Clock       : Fri 2020-05-22 09:49:43 EDT
NTP Sync.   : yes

[root@vitalpbx ~]#

```

Go to the `/etc/profile.d` folder and modify the `vitalwelcome.sh` file

Replaces the Text that is between `{green}` and `{txtrst}`, line 23

To create your new ASCII text we recommend the following web page.

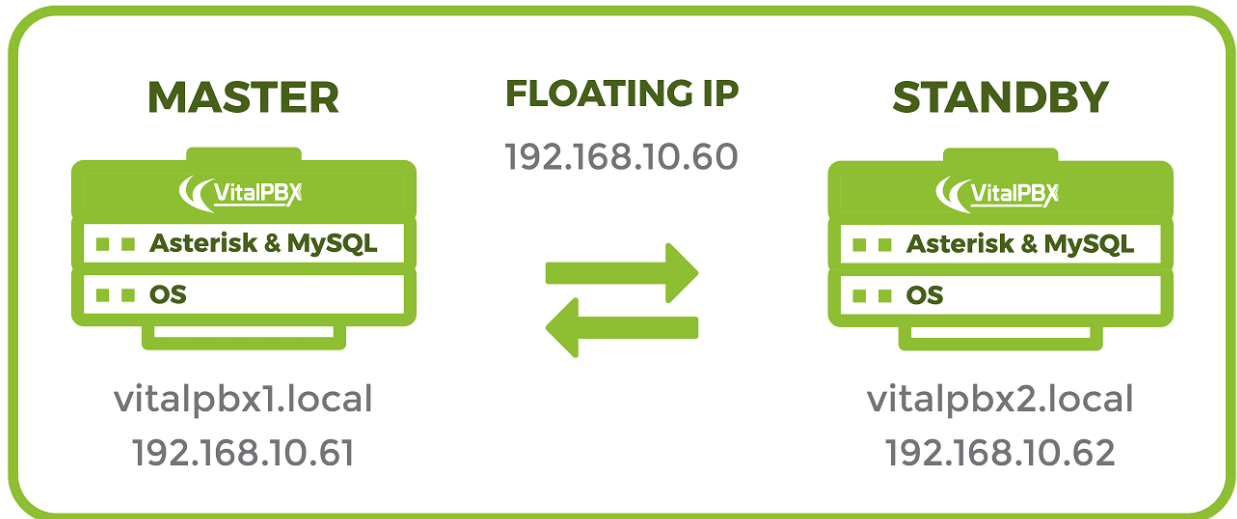
<http://patorjk.com/software/taag>

# 10. Appendix

## 10.1 VitalPBX High Availability

High availability is a characteristic of a system which aims to ensure an agreed level of operational performance, usually uptime, for a higher than normal period.

Make a high-availability cluster out of any pair of VitalPBX servers. VitalPBX can detect a range of failures on one VitalPBX server and automatically transfer control to the other server, resulting in a telephony environment with minimal down time.



### Prerequisites

In order to install VitalPBX in high availability you need the following:

- a.- 3 IP addresses.
- b.- Clean installation of VitalPBX Version 3.0 in two servers with similar characteristics.
- c.- MariaDB 10 (include in VitalPBX 3)
- d.- Corosync, Pacemaker, PCS and Isyncd.


## 10.1.1.- IP Configuration and Hostname

We will configure in each server the IP address and the host name.

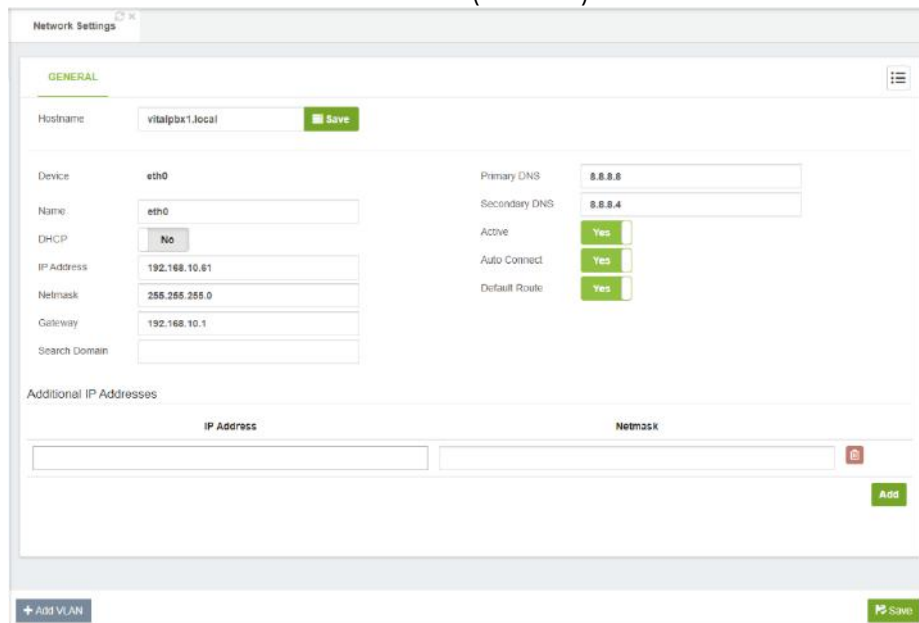
First, we will go to the web interface under:  
**Admin>System Settings>Network Settings**

Disable DHCP and configure the selected IP and hostname. In our example we will use the following values.

Name	Master	Standby
Hostname	vitalpbx1.local	vitalpbx2.local
IP Address	192.168.10.61	192.168.10.62
Netmask	255.255.255.0	255.255.255.0
Gateway	192.168.10.1	192.168.10.1
Primary DNS	8.8.8.8	8.8.8.8
Secondary DNS	8.8.4.4	8.8.4.4

First change the Hostname, remember press the **Save button** (  ) next to it to apply the new hostname.

Server 1 (Master)



The screenshot shows the 'Network Settings' web interface for 'Server 1 (Master)'. The 'GENERAL' tab is active. The 'Hostname' field is set to 'vitalpbx1.local' with a green 'Save' button next to it. Below this, the 'Device' is 'eth0', 'Name' is 'eth0', 'DHCP' is set to 'No', 'IP Address' is '192.168.10.61', 'Netmask' is '255.255.255.0', and 'Gateway' is '192.168.10.1'. There is a 'Search Domain' field. On the right side, 'Primary DNS' is '8.8.8.8', 'Secondary DNS' is '8.8.8.4', 'Active' is 'Yes', 'Auto Connect' is 'Yes', and 'Default Route' is 'Yes'. At the bottom, there is an 'Additional IP Addresses' section with 'IP Address' and 'Netmask' input fields and an 'Add' button. A '+ Add VLAN' button is at the bottom left, and a 'Save' button is at the bottom right.

Server 2 (Standby)

You can also change the hostname from the console using the following command:

Server 1

```
[root@ vitalpbx ~]# hostnamectl set-hostname vitalpbx1.local
```

Server 2

```
[root@ vitalpbx ~]# hostnamectl set-hostname vitalpbx2.local
```

### 10.1.2.- Installing the necessary software dependencies

For High Availability services we need to install in both servers **Corosync** and **Pacemaker**.

```
[root@ vitalpbx1-2 ~]# yum -y install corosync pacemaker pcs
```

We are going to synchronize some directories in both servers. For this we need to install lsync in both Server.

```
[root@ vitalpbx1-2 ~]# yum install lsyncd -y
```

### 10.1.3.- Create authorization

Create authorization key for the Access between the two servers without credentials.

Create key in Server 1

```
[root@ vitalpbx1 ~]# ssh-keygen -f /root/.ssh/id_rsa -t rsa -N "" >/dev/null
[root@ vitalpbx1 ~]# ssh-copy-id root@192.168.10.62
Are you sure you want to continue connecting (yes/no)? yes
root@192.168.10.62's password: (remote server root's password)
```

```
Number of key(s) added: 1
```

Now try logging into the machine, with: "ssh 'root@192.168.10.62'"  
and check to make sure that only the key(s) you wanted were added.

```
[root@vitalpbx1 ~]#
```

### Create key in Server 2

```
[root@ vitalpbx2 ~]# ssh-keygen -f /root/.ssh/id_rsa -t rsa -N "" >/dev/null
[root@ vitalpbx2 ~]# ssh-copy-id root@192.168.10.61
Are you sure you want to continue connecting (yes/no)? yes
root@192.168.10.61's password: (remote server root's password)
```

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'root@192.168.10.61'"  
and check to make sure that only the key(s) you wanted were added.

```
[root@vitalpbx2 ~]#
```

## 10.1.4.- Installing from Scripts

If you want to continue step by step go to step 2.5, but if you want to create the configuration automatically, run the following script in Server 1:

```
[root@ vitalpbx1 ~]# mkdir /usr/share/vitalpbx/ha
[root@ vitalpbx1 ~]# cd /usr/share/vitalpbx/ha
[root@ vitalpbx1 ~]# wget https://raw.githubusercontent.com/VitalPBX/vitalpbx_ha/master/vpbxha.sh
[root@ vitalpbx1 ~]# chmod +x vpbxha.sh
[root@ vitalpbx1 ~]# ./vpbxha.sh

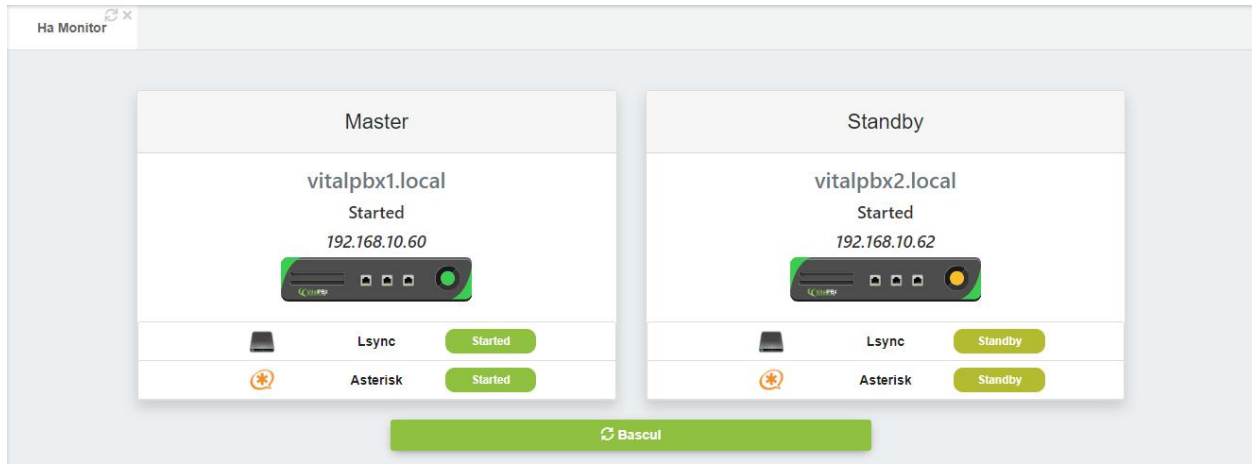
*****
*   Welcome to the VitalPBX high availability installation   *
*                   All options are mandatory                *
*****
IP Master..... > 192.168.10.61
IP Standby..... > 192.168.10.62
Floating IP..... > 192.168.10.60
Floating IP Mask (SIDR).. > 24
hacluster password..... > MyPassword (any password)
*****
*                   Check Information                          *
*   Make sure you have internet on both servers              *
*****
Are you sure to continue with this settings? (yes, no) > yes
```

This process may take a couple of minutes, and once it is done, VitalPBX High Availability will be ready to use.

Always remember to use floating ip to manage your VitalPBX. In this example it is 192.168.10.60.

## 10.1.5.- Install High Availability Module

Now we go to VitalPBX GUI and in Admin/Add-Ons/Add-Ons we install the High Availability module.



## 10.2 Feature Codes

Name	Dial	Description
Blacklist		
Blacklist a Number	*30	Enter a telephone number, which is then added to the blacklist for the extension. Inbound calls will not ring an extension if they are on the blacklist of the extension. Blacklisted callers will be told that the number they dialed is no longer in service. Feature must be enabled in the Feature Category associated with the extension.
Remove Number From Blacklist	*31	Enter a blacklisted telephone number - the blacklisted number will be removed from the extension's blacklist. Feature must be enabled in the Feature Category associated with the extension.
Blacklist Last Caller	*32	Adds the last number that called your extension to your extension blacklist. Key in the number to be blacklisted, followed by #. Make sure that you key in the number exactly as it appears in the system, i.e. include appropriate area codes, etc. Key in 1 to accept the entry, or hangup to discard it. Feature must be enabled in the Feature Category associated with the extension.
<b>Business Services</b>		
Wakeup Call	*34	Set a reminder or wakeup call for the current extension. Press 1 for a one-time reminder, or press 2 for a recurring daily reminder. Time should be entered in 24-hour format using 4 digits. If you have already set up a reminder call, you can press 1 to cancel it. Feature must be enabled in the Feature Category associated with the extension.
Remote Wakeup Call	*35	Set a reminder or wakeup call for another extension. Enter the number of the extension for which the reminder is intended. Press 1 for



			a one-time reminder, or press 2 for a recurring daily reminder. The time should be entered in 24-hour format using 4 digits. Feature must be enabled in the Feature Category associated with the extension.
Speak Last Number		*37	Speaks the last number that called the current extension. You can press 1 to call the original caller. Feature must be enabled in the Feature Category associated with the extension.  
Reminder		*38	Records a message. You can configure in how many minutes you want to hear the recording. When the set time expires, you will receive a call on the current extension and the recording will be played. Feature must be enabled in the Feature Category associated with the extension.
<b>Call Completion (CCSS)</b>			
Enable/Disable Call Completion	Call	*40	When enabled, callers will be allowed to request a call completion for your extension, this means that when you finish to talk asterisk automatically will generate a call from who requested the call completion to your extension.
Cancel Call Completion	Call	*41	It allows you to cancel any call completion request made from your extension.
<b>Call Center</b>			
Add/Remove Agent	Queue	*50	Toggle to add an agent to a specific queue, or remove the agent from the queue. You can either follow the prompts, or (in expert mode) enter the feature code immediately followed by * (asterisk) and the number of the queue. Feature must be enabled in the Feature Category associated with the extension.
Pause/Unpause Agent	Queue	*51	Toggle to pause, or unpause, an agent for a specific queue. You can either follow the prompts, or (in

		expert mode) enter the feature code immediately followed by * (asterisk) and the number of the queue. Feature must be enabled in the Feature Category associated with the extension.
Queues Login/Logout	*52	Add/Remove an Agent to all queue that agent belong to
Queues Pause/Unpause	*53	Pause/Unpause an Agent to all queue that agent belong to.
Spy on Extension in Barge Mode	*54	Instead of whispering on a single channel barge in on both channels involved in the call.
Spy on Extension	*55	Spy on a specific extension. Feature must be enabled in the Feature Category associated with the extension.
Spy on Extension In Whisper Mode	*56	Spy on a specific extension in whisper mode. Feature must be enabled in the Feature Category associated with the extension.
Spy Random Channels	*57	Spy on random channels. Feature must be enabled in the Feature Category associated with the extension.
<b>Call Forward</b>		
Boss/Secretary	*36	Toggle that enables or disables the routing all incoming calls for the current extension to the extension that is defined as the “secretary” phone. Once this function has been enabled, only the “secretary” phone will be able to make direct calls to the “boss” phone – all other calls will be routed directly to the “secretary” phone. Feature must be enabled in the Feature Category associated with the extension, and is only available after a “secretary” extension has been defined for the “boss” extension. The “secretary” extension can dial this feature code to stop receiving calls.
Call Forward Immediately	*58	Toggles immediate call forwarding. Feature must be enabled in the Feature Category associated with the extension.

Set CF Immediately Number	*59	Sets the number to which calls should be sent when immediate call forwarding is activated. You can either follow the prompts, or (in expert mode) enter the feature code immediately followed by * (asterisk) and the number to which calls should be forwarded. Feature must be enabled in the Feature Category associated with the extension.
Call Forward Unavailable	*60	Toggle to enable or disable call forwarding. Calls will be forwarded to the extension defined by default feature code *61. Feature must be enabled in the Feature Category associated with the extension.
Set CF Unavailable Number	*61	Set the number to which calls should be sent when unconditional call forwarding is activated. Feature must be enabled in the Feature Category associated with the extension.
Call Forward Busy	*62	Toggle to enable or disable call forwarding when your extension is busy. Calls will be forwarded to the extension defined by default feature code *63. Feature must be enabled in the Feature Category associated with the extension.
Set CF Busy Number	*63	Sets the number to which calls should be sent when call forward busy is activated and your extension is busy. Feature must be enabled in the Feature Category associated with the extension.
Call Forward On No Answer	*64	Toggle to enable or disable call forwarding when your extension is unable to answer incoming calls. Calls will be forwarded to the extension defined by default feature code *65. Feature must be enabled in the Feature Category associated with the extension.
Set CF On No Answer Number	*65	Sets the number to which calls should be forwarded when your extension is unable to answer. Feature must be enabled in the

		Feature Category associated with the extension.
Do Not Disturb	*66	Toggle to enable or disable the Do Not Disturb feature. Feature must be enabled in the Feature Category associated with the extension.
Follow Me	*67	Toggle to enable or disable the Follow Me feature. Feature must be enabled in the Feature Category associated with the extension.
Clear all Diversions	*69	Disables all call diversions, including the Do Not Disturb feature. Feature must be enabled in the Feature Category associated with the extension.
Personal Assistant - Toggle	*96	Toggle to enable/disable the personal assistant for your extension.
<b>On Call Features</b>		
Disconnect Call	*0	When you are on a call, disconnect the current call. Feature must be enabled in the Feature Category associated with the extension.
Direct Pickup	*07	When you are on a call, capture a call that is ringing at another extension in your pickup group. You will need to dial the feature code followed by the extension number that you want to answer. Feature must be enabled in the Feature Category associated with the extension.
Pickup Group	*08	When you are on a call, capture a call that is ringing at any other extension in your pickup group. To use this facility is necessary to create call group and pickup group in the extensions dialog. Feature must be enabled in the Feature Category associated with the extension.
Attended Transfer	*2	When you are on a call, transfer the current call to the operator. Feature must be enabled in the Feature Category associated with the extension.

One Touch Recording	*3	When you are on a call, force the current call to be recorded. Feature must be enabled in the Feature Category associated with the extension.
Park Call	*4	When you are on a call, place the current call in the call park. Feature must be enabled in the Feature Category associated with the extension.
Blind Transfer	#1	When you are on a call, transfer the current call without notifying the extension to which the call is transferred. This feature must be allowed by both the Feature Category and the Dial Profile associated with the extension.
<b>Phonebook Directory</b>		
Dial By Name Directory	411	Use your numerical keypad to dial a user name. For example, the extension for internal support may be called HELP, so you dial 411 (to activate this feature) and then 4357 to reach support. Feature must be enabled in the Feature Category associated with the extension.
<b>Test Services</b>		
Speak Date and Time	*70	Speak the current system date and time. Feature must be enabled in the Feature Category associated with the extension.
Speak Your Extension Number	*71	Speak the extension number that you are calling from. Feature must be enabled in the Feature Category associated with the extension.
Echo Test	*72	Echo test to measure the response time. Feature must be enabled in the Feature Category associated with the extension.
Simulate Incoming Call	*73	Simulate an incoming call to test ringing of the phone. Feature must be enabled in the Feature Category associated with the extension.
<b>Special Features</b>		
Lock/Unlock Phone	*75	Toggle to lock or unlock the current extension. No outbound

		calls can be made from a phone that has been locked. In order to unlock the phone, you will be prompted to enter the Features Password for the extension. Feature must be enabled in the Feature Category associated with the extension.
Change Password	Features *r76	Change the password for the current extension in order to access password-protect telephone features. Feature must be enabled in the Feature Category associated with the extension.
Remote Substitution	*r77	Makes it possible for the current phone to make calls as if you are calling from different phone extension. Feature must be enabled in the Feature Category associated with the extension.
Customer Code	*r78	Creates a customer code to be used by the CDR system - very useful for call accounting. Feature must be enabled in the Feature Category associated with the extension.  
Autorization Code	*r79	Allows you to make a call from any phone by using an authorization code that is associated with an unrestricted dial plan. Feature must be enabled in the Feature Category associated with the extension.
Hot Desking	*80	This feature enables the ability to possess multiple extensions using one device, depending on who is using it. Very useful for Call Centers. To use this option you need to create several extensions without device PBX/Extensions/Extension (Technology: None). Then you must create a Hot Desking device PBX/Extensions/Hot Desking
Night Mode All	*81	Toggle to enable/disable all defined night modes. Feature must be enabled in the Feature Category associated with the extension.
<b>Recordings &amp; Announcements</b>		

Custom Recording	*92	Used to record a message. Feature must be enabled in the Feature Category associated with the extension.
Dictation	*93	Used to record a message with the option of sending it by email. Only available for extensions where Dictation has been enabled in the Recording tab.
Record Msg For Personal Assistant	*94	Record a message that callers will hear when they are served by your personal assistant. Only available for extensions where Has Personal Assistant has been enabled in the Advanced tab.
Send Voicemail Message	*95	Allows you to dial any extension and leave a voicemail message. For example, dialing *95*2492 will allow you to leave a voicemail message for extension 2492. Feature must be enabled in the Feature Category associated with the extension.
Direct Voicemail	*97	Direct entry to the voicemail system to listen to voicemail for the current extension – only requires the user to input the voicemail password. This option is only available for extensions where voicemail has been enabled in the Voicemail tab.
Remote Voicemail	*98	Remote entry to the voicemail system to listen to voicemail for any extension – requires the user to input both an extension number and the voicemail password for that extension. Feature must be enabled in the Feature Category associated with the extension.

## 10.3 BLF (Hints)

Name	Dial	Description
DND_EXT	*66	DND
LOK_EXT	*75	Lock Phone
CFN_EXT	*64	Call Forwarding No Answer
CFU_EXT	*60	Call Forwarding Unavailable
CFI_EXT	*58	Call Forwarding Immediately
CFB_EXT	*62	Call Forwarding Busy
FWM_EXT	*67	Call Follow me
PEA_EXT	*96	Personal Assistance
BOSS_EXT	*36	Boss/Secretary
QAL_EXT	*50	Login/Logout Agent (All dynamic queues to which it belongs)
QAP_EXT	*51	Pause/Unpause Agent (All dynamic queues to which it belongs)
QAL_EXT_QUEUE	*52	Login/Logout Agent in a specific queue
QAP_EXT_QUEUE	*53	Pause/Unpause Agent in a specific queue
vm_EXT		Voice Mail
TC-#		It monitors the status of the Time Conditions, whether it is reversed temporarily or permanently, however, it will only allow us to change the status of the Time Condition from the phone if said status is temporary and not permanent. # -> ID
NM-#		Monitors night mode, # -> ID, pressing forces the state to change permanently until pressed again.
	*69	Clear all
701-710		Default Parking
		Notes: EXT → Extension, QUEUE → Queue Number

In VitalPBX activate in each extension Generate Hints. Settings > PBX Settings > System



## General

The screenshot shows the 'System General' configuration page. It has a tabbed interface with 'GENERAL', 'SYSTEM PROMPTS', and 'SYSTEM DIRECTORIES'. The 'GENERAL' tab is active. Under 'Extension Settings', there are fields for 'Default Language' (set to 'English (en)'), 'Devices Prefix', and three checkboxes: 'Enable Voicemail' (Yes), 'Enable Portal' (Yes), and 'Create Hints' (Yes). The 'Create Hints' checkbox is circled in red. Under 'Dial-Plan Settings', there are fields for 'Default Ring Time' (30), 'Recording Format' (WAV), and 'Recording Script' (/var/lib/my\_script). A 'Save' button is located at the bottom right.

Section	Field	Value
Extension Settings	Default Language	English (en)
	Devices Prefix	
	Enable Voicemail	Yes
	Enable Portal	Yes
	Create Hints	Yes
Dial-Plan Settings	Default Ring Time	30
	Recording Format	WAV
	Recording Script	/var/lib/my_script

## 10.3.1 Grandstream Phone Management

Go to Settings > Extension Boards

### EXT 1

	Mode	Account	Description	Value
EXT 1	Busy Lamp Field (BLF) ▼	Account 1 ▼	Nigh Mode	NM_1
EXT 2	Busy Lamp Field (BLF) ▼	Account 1 ▼	DND	DND_8000
EXT 3	None ▼	Account 1 ▼	<i>Description</i>	<i>Value</i>
EXT 4	Busy Lamp Field (BLF) ▼	Account 1 ▼	CF Immediately	CFI_8000
EXT 5	None ▼	Account 1 ▼	<i>Description</i>	<i>Value</i>
EXT 6	Busy Lamp Field (BLF) ▼	Account 1 ▼	CF Busy	CFB_8000
EXT 7	None ▼	Account 1 ▼	<i>Description</i>	<i>Value</i>
EXT 8	Busy Lamp Field (BLF) ▼	Account 1 ▼	CF No Answer	CFN_8000
EXT 9	None ▼	Account 1 ▼	<i>Description</i>	<i>Value</i>
EXT 10	Busy Lamp Field (BLF) ▼	Account 1 ▼	CF Unavailable	CFU_8000
EXT 11	None ▼	Account 1 ▼	<i>Description</i>	<i>Value</i>
EXT 12	Busy Lamp Field (BLF) ▼	Account 1 ▼	Personal Assistance	PEA_8000
EXT 13	None ▼	Account 1 ▼	<i>Description</i>	<i>Value</i>
EXT 14	Busy Lamp Field (BLF) ▼	Account 1 ▼	Boos/Secretary	BOSS_8000
EXT 15	None ▼	Account 1 ▼	<i>Description</i>	<i>Value</i>
EXT 16	Busy Lamp Field (BLF) ▼	Account 1 ▼	Lock/Unlock Phone	LOK_8000
EXT 17	Speed Dial ▼	Account 1 ▼	<i>Description</i>	<i>Value</i>
EXT 18	Busy Lamp Field (BLF) ▼	Account 1 ▼	LogIn/Logout 501	QAL_8000_501
EXT 19	Speed Dial ▼	Account 1 ▼	<i>Description</i>	<i>Value</i>
EXT 20	Busy Lamp Field (BLF) ▼	Account 1 ▼	Pause/Unpause 501	QAP_8000_501

## 10.3.2 Yealink Management

Go to DSS Key

Key	Type	Value	Account	Extension
DSS Key1	BLF ▼	DND_8000	Account 1 ▼	*66
DSS Key2	BLF ▼	LOK_8000	Account 1 ▼	*75
DSS Key3	BLF ▼	CFI_8000	Account 1 ▼	*58
DSS Key4	BLF ▼	CFU_8000	Account 1 ▼	*64
DSS Key5	BLF ▼	CFB_8000	Account 1 ▼	*62
DSS Key6	BLF ▼	FWM_8000	Account 1 ▼	*67
DSS Key7	BLF ▼	BOSS_8000	Account 1 ▼	*36
DSS Key8	BLF ▼	PEA_8000	Account 1 ▼	*96
DSS Key9	Speed Dial ▼	*69	Auto ▼	
DSS Key10	N/A ▼		Auto ▼	

## 10.3.3 Xorcom Management

Go to DSS Key

Key	Type	Value	Line	Extension
DSS Key1	BLF ▼	DND_8000	Line 1 ▼	*66
DSS Key2	BLF ▼	LOK_8000	Line 2 ▼	*75
DSS Key3	BLF ▼	CFI_8000	Line 1 ▼	*58
DSS Key4	BLF ▼	BOSS_8000	Line 1 ▼	*36
DSS Key5	BLF ▼	PEA_8000	Line 1 ▼	*96
DSS Key6	Speed Dial ▼	*69	Auto ▼	

## 10.4 VitalPBX Voice Prompts

There is a list of the VitalPBX specific voice prompts.

Description	Prompt Name	Message (En)	Mensaje (Es)
Simulate Incoming Call(Read DID)	vital-sim-incoming-call-did	Enter the DID number to simulate an incoming call, followed by the pound key.	Por favor digite el D-I-D para simular la llamada entrante, seguido de la tecla numeral
Wake up Call(Welcome Message)	vital-welcome-wake-up-call	Welcome to the wake-up call service!	Bienvenido al servicio de despertador
Wake up Call Remote(Ask for remote extension)	vital-remote-wake-up-call-number	Enter the extension number of the person who should receive this wake-up call.	Por favor digite el número de extensión de la persona que recibirá el servicio de despertador
Voicemail Direct/Remote(Voicemail Disable)	vital-vm-no-avaliable	Voicemail service is disabled for this extension.	El servicio de correo de voz está deshabilitado para esta extensión
Add/Remove Queue Agent(not member)	vital-queue-no-dyn-member	You are not a dynamic member of this queue.	Usted no es un miembro dinámico de esta cola.
Spy Extension	vital-spy-extension-number	Enter the extension number to be monitored.	Por favor digite el número de extensión a ser monitoreada
Announcement about follow-me activation/de activation	vital-follow-me	Follow-me is ...	Sigueme está.....
Announcement that	vital-agent-already-login	Agent is already logged in.	Este agente está actualmente logueado

agent is already log on			
Announcement that agent is in pause	vital-agent-pause	Agent is now paused.	Agente está ahora en pausa
Announcement that queue number	vital-agent-queue-number	Queue number ...	Número de cola
Announcement that agent is unpause	vital-agent-unpause	Agent is now available.	Agente está ahora disponible
Announcement about Call completion activated/de activated	vital-call-completion	Call-completion is ...	Completado de llamada está ...
Ask if you have to request the call completion for the current call	vital-call-completion-request	For call-completion, please dial ...	Para completar la llamada marque ....
Announcement about Personal assistant activated/de activated	vital-personal-assistant	Personal assistant is ...	Asistente personal está...
Announcement personal assistant destination number	vital-pls-enter-pa-dest-number	Enter the number you wish to call.	Por favor, introduzca el número al que desea llamar

Announcement personal assistant recording message	vital-pls-rcrd-personal-assistant	Record your personal assistant message. When done, press the pound key.	Por favor grabe su mensaje del asistente personal, cuando termine presione la Tecla numeral.
Announcement the extension number	vital-your-extension-number-is	Your extension number is ...	Su número de extensión es....
Announcement snooze for wake-up call	vital-snooze-for	Snooze for ...	Posponer por .....
Announcement about diversions activated/de activated	vital-all-diversions-are	Call diversions are .....	Todos los Desvíos están .....
Announcement Caller ID	vital-callerid	Caller ID	Identificador de Llamada
Announcement Inbound Number	vital-inbound-number <to be deleted>	Inbound number	Numero Entrante
Announcement about night mode activated/de activated	vital-night-mode	Night-mode is .....	Modo nocturno esta .....
Announcement about night mode all activated/de activated	vital-night-mode-all	all night-modes are .....	Modo nocturno general esta .....

Ask about the Customer Account Number	vital-customer-account-number	Enter customer account number, followed by the pound key	Por favor ingrese el número de cuenta del cliente seguido de la tecla numeral
Custom recording greeting message (*92)	vital-custom-recording	Say your message, and then press the pound key.	Diga su mensaje y luego presiona la tecla numeral.
Ask for authorization code (*79)	vital-authorization-code	Enter your authorization code, followed by the pound key	Ingrese su código de autorización, seguido de la Tecla numeral
Login/Logout hot desking device (*80)	vital-hotdesking-login	Please enter the extension number followed by the pound key	por favor ingrese el número de extensión seguido de la tecla numeral
	vital-hotdesking-login-confirm	The extension was successfully added	La extensión fue agregada satisfactoriamente
	vital-hotdesking-logout	Your extension is added, to remove press 1, to cancel press 2	su extensión está agregada, para eliminar presione 1, para cancelar presione 2
	vital-hotdesking-logout-remove	the extension was successfully removed	la extensión fue eliminada con éxito
	vital-hotdesking-logout-cancel	extension remains associated with this device	la extensión sigue asociado a este dispositivo
Phone Unlock	vital-phone-unlock	your extension has been unlocked	Su extensión ha sido desbloqueada
Phone Lock	vital-phone-lock	your extension has been locked	Su extensión ha sido bloqueada
Not a dynamic member of any Queue (*52)	vital-no-dyn-member	you are not a dynamic member of any Queue	Usted no es un miembro dinámico de ninguna Cola

	vital-agent-login-logout	Press 1 for agent login or press 2 for agent logoff	Presione 1 para iniciar sesión como agente o presione 2 para cerrar sesión como agente
	vital-agent-login	Agent logged in	Agente agregado a las colas
	vital-agent-logoff	Agent logged off	Agente removido de las colas
Private Class Of Service	vital-cos-private	You are not allowed to call this extension	Usted no tiene permisos para llamar a esta extensión
Hot Desking extension (*80)	vital-no-hotdesking-extension	Sorry, but the provided extension is not hot-desking	Lo siento, pero la extensión proporcionada no es hot-desking
Hot Desking device (*80)	vital-no-hotdesking-device	Sorry, but your device is not hot-desking	Lo siento, pero su dispositivo no es hot-desking
	vital-max-tries	You have reached the maximum number of attempts	Ha alcanzado el máximo número de intentos
Authorization Code (*79)	vital-auth-code-invalid	You have provided an invalid authorization code	Ha proveído un código de autorización inválido.
Authorization Code (*79)	vital-auth-code-disabled	The authorization code you have provided is disabled	El código de autorización que ha proveído está deshabilitado
Customer Code (*78)	vital-customer-account-number-invalid	You have provided an invalid customer account number	Ha proveído un número de cuenta de cliente inválido
Customer Code (*78)	vital-customer-account-number-disabled	The customer account number you have provided is disabled	El número de cuenta de cliente que ha proveído está deshabilitado.
Record Msg For Personal Assistant (*94)	vital-personal-assistant-no-recording	You have not recorded the personal assistant message, please record it and try again	No ha grabado el mensaje del asistente personal, por favor, grábelo e intente de nuevo



Record Msg For Personal Assistant (*94)	vital-personal-assistant-rec-message	After the tone, please record your personal assistant message	Después del tono grabe el mensaje de su asistente personal
	vital-invalid-option	You have dialed an invalid option	Ha marcado una opción invalida
Cancel Call Completion (*41)	vital-call-completion-cancelled	The call completion service has been canceled	El servicio de completado de llamada ha sido cancelado
Reminder (*38)	vital-reminder	Please enter the extension number to which you wish to send the message	Por favor introduzca el número de extensión a la cual desea enviar el mensaje
	vital-feature-disabled	The feature you have dialed is disabled for this extension	La opción que ha marcado esta deshabilitada para esta extensión
Simulate Incoming Call (*73)	vital-sim-incoming-cid	Please dial the C.I.D. number to simulate an incoming call, followed by the pound key.	Por favor digite el C-I-D para simular la llamada entrante, seguido de la tecla numeral
Queues Pause/Unpause (*53)	vital-queues-pause	To pause all queues...	Para ponerse en pausa en todas las colas...
Queues Pause/Unpause (*53)	vital-queues-unpause	To un-pause all queues...	Para ponerse disponible en todas las colas...
Boss/Secretary - Toggle (*36)	vital-boss-secretary	Secretary mode...	Modo secretaria...
	vital-no-queues	There are no available queues	No hay colas disponibles
	vital-timeout-reached	You have depleted the waiting time	Ha agotado el tiempo de espera
	trunk-out-service	The trunk through which you are trying to dial is disconnected or out of service.	La troncal a través de la cual está intentando marcar está

			desconectada o fuera de servicio.
For Incoming Calls	tenant-in-disable	The service for the number you have dialed is disconnected.	El servicio para el número que ha marcado está desconectado.
For Out/Local Calls	tenant-disable	The call service has been disconnected for this tenant.	El servicio de llamadas se ha desconectado para este Tenant.
	qc-instructions	All of our representatives are currently busy. Please stay on the line and your call will be answered by the next available representative or press one to be called back when a representative is available.	Todos nuestros representantes están ocupados actualmente. Permanezca en la línea y su llamada será respondida por el próximo representante disponible o presione uno para que le devuelvan la llamada cuando haya un representante disponible.
	qc-number-prompt	Please enter your telephone number	Por favor introduzca su número de teléfono
	qc-thanks-prompt	Thanks, you will be callback soon	Gracias, le devolveremos la llamada pronto
	qc-invalid-number	We are sorry, you have provided an invalid phone number	Lo sentimos, proporcionaste un número de teléfono no válido.

## 10.5 Recommendations

Servers often fail due to lack of space on your hard disk. If you want to keep your server in optimum conditions, we recommend the following:

Remove unnecessary and old recording periodically. If you want to make this automatically, we recommend that you include this cron in cron.daily

```
#!/bin/sh
cd /var/spool/asterisk/monitor/
/usr/bin/find . -type f -name "*.mp3" -mtime +180 | /usr/bin/xargs /bin/rm -f >/dev/null 2>&1
/usr/bin/find . -type f -name "*.wav" -mtime +180 | /usr/bin/xargs /bin/rm -f >/dev/null 2>&1
exit 0
```

Where +180 means the number of days of recording. You can change.

Remember to change the permission to 755.

Convert the recording from .wav to .mp3 periodically. If you want to make this automatically, we recommend that you include this cron in cron.daily

```
#!/bin/sh
cd /var/spool/asterisk/monitor/
/usr/bin/find . -type f -name "*.wav" -size -200k | /usr/bin/xargs /bin/rm -f >/dev/null 2>&1
/usr/bin/find . -type f -name "*.wav" | /usr/bin/xargs -i lame -r {}
/usr/bin/find . -type f -name "*.wav" | /usr/bin/xargs /bin/rm -f >/dev/null 2>&1
exit 0
```

The third line deleted unnecessary recordings of less than 200k, the four line converts from .wav to .mp3 and the five line deleted all .wav file that was converted to mp3.

Remember to change the permission to 755.

Remember to remove periodically the log files, this file is located in:

```
/var/log/
/var/log/asterisk
```

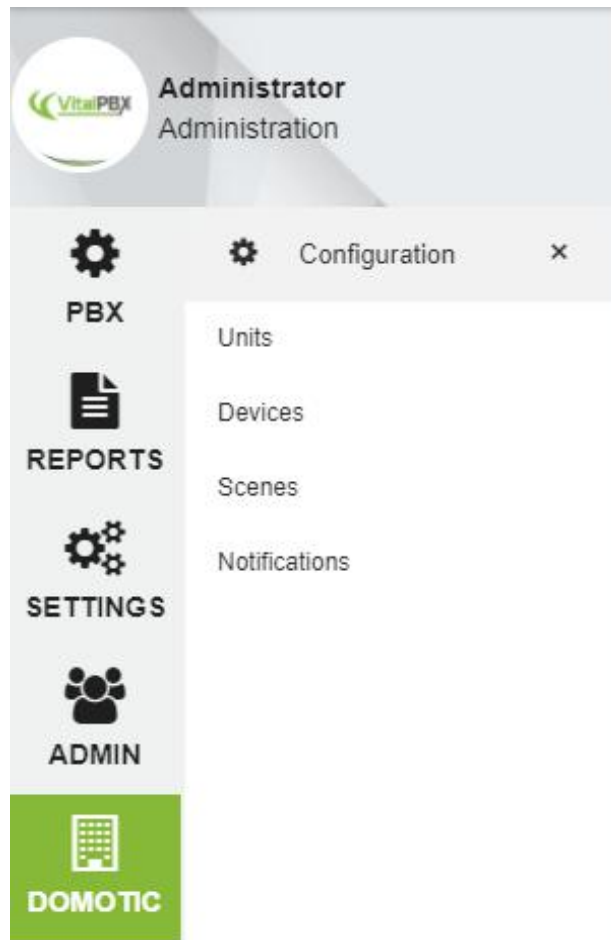
You can remove the log file that finished in .0, .1, etc.

## 10.6 Additional Modules

### 10.6.1 Domotic Module

The Domotic module facilitates the integration of VitalPBX with home or office automation systems.

For now, this module is compatible with the Vera Gateway, in the future we plan to integrate more Gateway.



This module has 4 configuration forms, Units, Device, Scenes and Notifications

**Units**, the gateways are configured, it is possible to connect more than one gateway to VitalPBX.

**Device**, the devices that are connected to the Gateway are configured, these are automatically detected when the Gateway is configured.

**Scenes**, these Scenes are obtained from the Gateway. A Scenes is a group of devices that execute an action in conjunction with just running the Scene

**Notifications**, these notify when a Devices executes an action, in the case of Devices that possess this characteristic, these can be the movements or magnetic sensors.

### 10.6.1.1 Units

The gateways are configured, it is possible to connect more than one gateway to VitalPBX.

The screenshot shows a web interface for configuring a unit. The title bar says 'Units'. Below it is a 'GENERAL' tab. The configuration fields are as follows:

Field	Value
Model	Vera Smarter Home Control
Description	Vera Oficina
IP Address	192.168.25.11
Port	3480

At the bottom of the form, there are four buttons: 'Synchronize' (orange), 'Update' (green), 'Delete' (red), and 'Cancel' (blue).

**Model**, this is the brand and model of the gateway to be configured.

**Description**, a brief description to identify the Gateway.

**IP Address**, Gateway IP address.

**Port**, Gateway IP port

**Synchronize**, use this if you make any changes in the Gateway it is necessary to Synchronize again, with this button you can do it.

## 10.6.1.2 Devices

The devices that are connected to the Gateway are configured; these are automatically detected when the Gateway is configured

The screenshot shows the 'Domotic Devices' configuration window. The 'GENERAL' tab is active. The settings are as follows:

Number to Dial	232	Class of Service	All Permissions
Description	Cerradura	PIN List	None
Unit	Vera Oficina EBD	White List	
Device	Schlage Deadbolt	Toggle Mode	Yes
Welcome Message	None	Generate Hint	Yes
BLF Hint	domotic_dev_16		

At the bottom right, there are three buttons: Update (green), Delete (red), and Cancel (blue).

**Number to Dial,** Is the number to dial to change the status of the Device.

**Description,** A brief description to identify the Device.

**Unit,** Select the Gateway that we want to configure the Device.

**Device,** us this to select the Device to be configured.

**Welcome Message,** Message to listen when the Device is called (optional).

**Class of Services,** Class of Service to which the Device is associated.

**PIN List,** Pin List associated with the Device, the person must know at least one PIN to change the status of the Device.

**White List,** List of Telephone Numbers or extensions. All that are in this list can change the status of the Device without having to enter PIN. If a number is added to this list automatically the remaining extensions and numbers are blocked.

**Toggle Mode,** if this option is in Yes, the Device status will be changed automatically without asking any questions.

**Generate Hint,** Generates Hint to be accessed from the console of an IP phone.

**BLF Hint,** this is the Hint that must be configured in the console of the IP phone.

### 10.6.1.3 Scenes

Scenes are obtained from the Gateway. A Scenes is a group of devices that execute an action in conjunction with just running the Scene

The screenshot shows a web interface for configuring Domotic Scenes. The 'GENERAL' tab is selected. The configuration fields are as follows:

Number to Dial	220	Class of Service	All Permissions
Description	Oficina Abierta	PIN List	None
Unit	Vera Oficina EBD	White List	
Scene	Office Open	Skip Instructions	Yes
Welcome Message	None		

At the bottom of the form, there are three buttons: Update (green), Delete (red), and Cancel (blue).

**Number to Dial,** Is the number to dial to execute the Scene.

**Description,** A brief description to identify the Scene.

**Unit,** Select the Gateway that we want to configure the Scene.

**Scene,** use this to select the scene to execute.

**Welcome Message,** Message to listen when the Scene is called (optional).

**Class of Services,** Class of Service to which the Scene is associated.

**PIN List,** Pin List associated with the Scene, the person must know at least one PIN to execute the Scene.

**White List,** List of Telephone Numbers or extensions. All that are in this list can execute the Scene without having to enter PIN. If a number is added to this list automatically the remaining extensions and numbers are blocked.

**Skip Instructions,** if this option is in Yes, instructions are ignored and only the scene is executed.

### 10.6.1.4 Notifications

Notify when a Devices executes an action, in the case of Devices that possess this characteristic, these can be the movements or magnetic sensors.

The screenshot shows a configuration window titled "Domotic Notifications". It has a "GENERAL" tab selected. The configuration includes:

- Unit:** A dropdown menu with "Vera Oficina EBD" selected.
- Device:** A dropdown menu with "Door/Window Sensor" selected.
- Welcome Message:** A dropdown menu with "None" selected and a refresh icon.
- Enabled:** A toggle switch set to "Yes".
- Destination:** Two dropdown menus, the first with "Extensions" and the second with "8255 - Rodrigo Cuadra".

A green "Save" button is located at the bottom right of the form.

**Unit,** Select the Gateway that we want to configure the Notification.

**Device,** with this you can select the Device to be configured.

**Welcome Message,** Message to listen when the Scene is called (optional).

**Enabled,** enable or disable the notification.

**Destination,** the action to take when the device changes state



## 10.6.1.5 Some Console Pictures

### Touch Phone



### Traditional Console



## 10.6.2 Sonata Suite (Recording Management)

Sonata Recording Management is one of the applications of Sonata Suite that will help you manage the recordings in your VitalPBX Server. This is completely integrated with VitalPBX.

This application can be installed from Add-ons in VitalPBX.

The screenshot shows the Sonata Suite Recordings web interface. The browser address bar displays '192.168.25.12/sonata/recordings/'. The interface includes a sidebar with navigation options: PANEL, REPORTS, and SETTINGS. The main content area is titled 'GENERAL' and contains a table of call recordings. The table has columns for Date, Time, Team, Extension, Calltype, Number, Duration, and Actions. Below the table, it indicates 'Showing 1 to 10 of 32 entries' and includes a pagination control with 'Previous', '1', '2', '3', '4', and 'Next' buttons.

Date	Time	Team	Extension	Calltype	Number	Duration	Actions
2017-10-17	10:49:38	ADMINISTRACION	8250	←	8253	00:00:21	[Icons]
2017-10-17	10:49:38	ADMINISTRACION	8253	→	8250	00:00:21	[Icons]
2017-10-17	10:48:34	ADMINISTRACION	8255	→	254	00:00:01	[Icons]
2017-10-17	10:48:34	ADMINISTRACION	8255	→	254	00:00:01	[Icons]
2017-10-17	10:38:03	SOPORTE	8263	←	8253	00:01:25	[Icons]
2017-10-17	10:38:03	ADMINISTRACION	8253	→	8263	00:01:25	[Icons]
2017-10-17	10:33:26	ADMINISTRACION	8255	←	7500	00:00:06	[Icons]
2017-10-17	10:26:01	ADMINISTRACION	8303	→	922528920	00:00:34	[Icons]
2017-10-17	09:54:44	ADMINISTRACION	8303	→	922528920	00:00:38	[Icons]
2017-10-17	09:40:53	ADMINISTRACION	8255	→	8270	00:00:39	[Icons]

## 10.6.3 Sonata Suite (Billing System)

Sonata Billing System is one of the applications of Sonata Suite that will help you manage the CDR in your VitalPBX Server. This applications is completely integrated with VitalPBX.

This application can be installed from Add-ons in VitalPBX.

Date	Hour	Extension	Cell Type	Callee	Duration	Cost
2017/10/18	16:12:18	8250 - Recepcion	Internal	8253	00:00:06	0.00
2017/10/18	15:46:43	8250 - Recepcion	Internal	8253	00:00:09	0.00
2017/10/18	15:46:34	8252 - Juan Romero	Internal	8250	00:00:20	0.00
2017/10/18	15:43:49	8251 - Felix Gallo	Internal	8250	00:00:06	0.00
2017/10/18	15:43:20	8251 - Felix Gallo	Internal	8250	00:00:19	0.00
2017/10/18	15:43:20	8250 - Recepcion	Internal	8253	00:00:25	0.00
2017/10/18	15:43:01	8251 - Felix Gallo	Internal	8250	00:00:36	0.00
2017/10/18	15:41:55	8251 - Felix Gallo	Internal	8250	00:00:12	0.00
2017/10/18	14:25:15	8264 - Rummer Moraga	Internal	8251	00:01:41	0.00
2017/10/18	13:59:23	8263 - Mauro Jiron	Internal	8251	00:02:11	0.00
2017/10/18	13:52:33	8251 - Felix Gallo	Outgoing	922668002	00:00:55	0.23
2017/10/18	13:44:11	8253 - Contabilidad	Internal	8253	00:00:19	0.00

## 10.6.4 Sonata Suite (Switchboard)

Sonata Switch Board is one of the applications of Sonata Suite that will help you to visualize in a clear and simple way what is happening with your VitalPBX Server in real time.

This application can be installed from Add-ons in VitalPBX.

The screenshot displays the Sonata Suite Switchboard interface. It features a top navigation bar with the 'Sonata Suite Switchboard' logo, a 'Dial' button, and a user profile for 'Rodrigo Cuadra #255'. The main dashboard is divided into several sections:

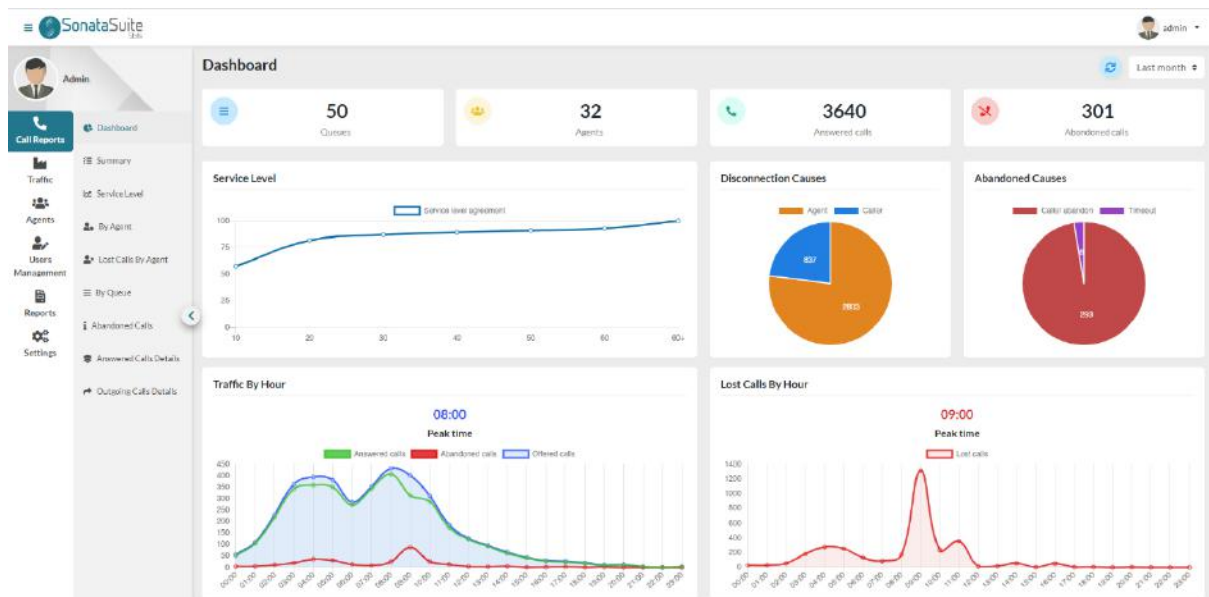
- MY EXTENSION:** Shows the user's current extension as 8355 - Rodrigo Cu... with a status of 0011 and a numeric keypad below.
- EXTENSIONS:** A grid of extension cards, each with a status indicator (red for busy, green for available) and a name. Examples include:
  - 8255 - RODRIGO CUADRA (0011) - Status: Busy
  - 8250 - RECEPCION - Status: Available
  - 8258 - CONTABILIDAD - Status: Available
  - 8260 - OSCAR ROMERO - Status: Available
  - 8264 - HUMMER MORAGA - Status: Available
  - 8267 - CABINA TELEFONICA - Status: Available
  - 8271 - MAYNOR PERALTA - Status: Available
  - 8274 - ROGER - Status: Available
  - 8299 - ALARMA - Status: Available
  - 8601 - YASSIER BONILLA - Status: Available
  - 8604 - EMANUEL LYONS DESKTOP - Status: Available
  - 8903 - VIOLETA MERCADO - Status: Available
  - 8555 - RODRIGO CUADRA WIFI (0011) - Status: Busy
  - 8608 - EMANUEL LYONS-EL VALLE - Status: Available
- TRUNK:** Shows trunk lines like 'Line Enthal' and '850 Honduras'.
- PARKING:** Shows a parking area '700 - Default Parking'.
- QUEUES SUMMARY:** A table with columns for Queue, Strategy, Logged in Members, Available Members, Queued Calls, Completed Calls, Abandoned Calls, Service Level, Longest Hold Time, Hold Time, and Talk Time.
 

Queue	Strategy	Logged in Members	Available Members	Queued Calls	Completed Calls	Abandoned Calls	Service Level	Longest Hold Time	Hold Time	Talk Time
300 - Soporte	Ring All	2	2	0	2	1	0.9	0	9	36
301 - Verdad	Ring All	4	4	0	1	0	0.9	0	3	89
302 - Contabilidad	Ring All	0	0	0	0	0	0.9	0	0	0
500 - Tesoro	Ring All	2	2	0	0	0	0.9	0	0	0
- SUPPORT:** A summary card for support metrics, showing 0% SLA, 2 Completed Calls, 1 Abandoned Calls, 0 SLA Target, 0 Working Calls, 00:00 Longest Hold Call, 2 Logged in Members, and 2 Available Members.
- SALES:** A summary card for sales metrics, showing 0% SLA, 1 Completed Calls, 0 Abandoned Calls, 0 SLA Target, 0 Working Calls, 00:00 Longest Hold Call, 4 Logged in Members, and 4 Available Members.

## 10.6.5 Sonata Suite (Stats)

Sonata Suite Stats is a fully featured Call Center Queues and Agent Statistics program. Use Sonata Suite Stats to create detailed reports to measure your different Queues and Agents, so you can take your Call Center to the next level.

This application can be installed from the Add-ons module in VitalPBX.



**Call Reports**, here we will find the summarized and detailed reports by calls taking into account the queues (Queues) and the agents (Agents). The types of reports are:

**Summary**, a summarized report where the total number of answered and abandoned calls, as well as the level of service, is shown on the same screen.

**Service Level**, detailed report of the service level.

**By Agent**, summary and detailed report of calls answered and missed by Agent.

**Lost Calls By Agents**, detailed report of lost calls by Agent, with the possibility of inspecting if at the end the call was answered by another agent.

**By Queue**, summary and detailed report by call queue.

**Abandoned Calls**, detailed report of abandoned calls in queues and their respective cause.

**Answered Calls Details**, detailed report of incoming calls to each queue, with the possibility of seeing all the events related to the call.

**Outgoing Calls Details**, detailed report of outgoing calls by Agent.

**Distribution**, here we get reports summarized by day, hour and day of the week.

**Traffic By Hour**, graphically shows what time there is the highest call traffic, this report can be obtained every hour or every half hour. It also shows abandoned and missed calls per hour.

**Traffic By Day**, graphical summary report of calls per day.

**Traffic By Day of Week**, graphical summary report of calls by day of the week.

**Traffic By Month**, summary graphical report of calls per month.

**Agents**, in reports by agents we can observe the following information:

**Session Details**, summary and detailed report of the sessions of each agent.

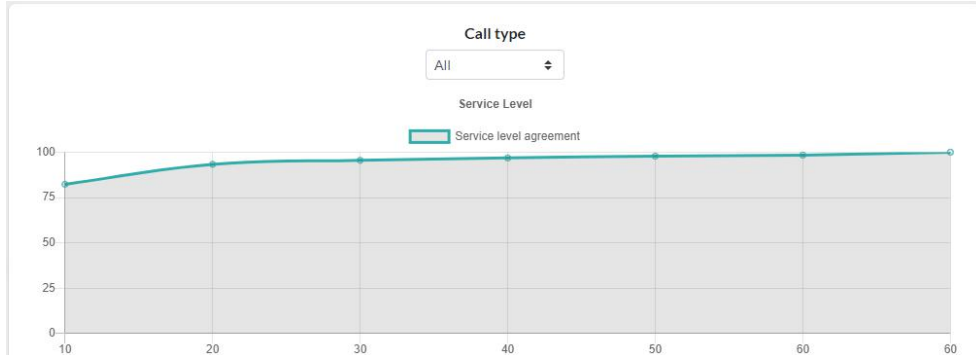
**Availability**, detailed report of the availability of agents.

**Session By Hour**, here we can see the total duration of the session of the agents per hour.

**By Hour**, in this report we can see how many agents had registered on an exact date and time and the list of them.

Here is a small sample of the reports:

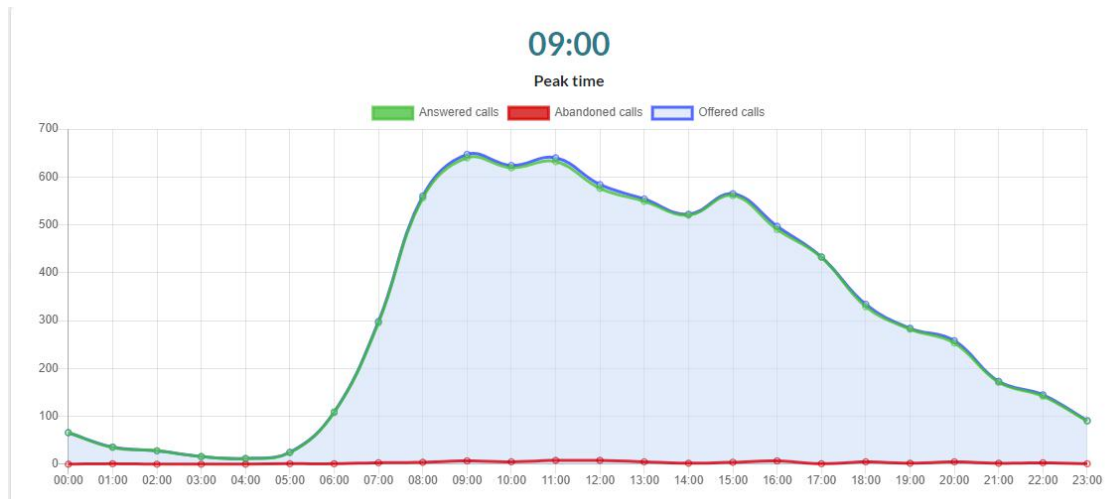
Graph where the behavior of the service level (SLA) can be observed.



And the data reflected in a table.

Hangup	Number calls	Delta	Percent
Within 10 seconds	6180	0	82.39%
Within 20 seconds	7003	+ 823	93.36%
Within 30 seconds	7170	+ 167	95.59%
Within 40 seconds	7263	+ 93	96.83%
Within 50 seconds	7336	+ 73	97.80%
Within 60 seconds	7388	+ 52	98.49%
Within 60+ seconds	7501	+ 113	100.00%

In this report we are going to graphically observe the hours of highest call traffic in our Call Center, this information is very useful as it helps us make decisions to know how many agents we need depending on the time. It is also possible to obtain this report every half hour.



And many more reports. We recommend viewing the complete manual already available on our website <https://www.vitalpbx.org>

## 10.7 Command Tool

This tool contains a series of commands to easily give maintenance to the VitalPBX installation. To invoke this tool you must use the following syntax: "vitalpbx COMMAND [command-options]". In the future, we expect to add new functionalities, by now, the available commands are:

**vitalpbx reset-pwd [username]:** Reset password for any user. If not, user is specified, it resets the password for admin user (Main Tenant Only)

**vitalpbx build-db:** Execute a series of scripts to build VitalPBX database (apply\_patches)

**vitalpbx dump-conf:** Dump Asterisk Configurations and re-build Asterisk DB (Main Tenant Only)

**vitalpbx fully-dump-conf:** Dump Asterisk Configurations and re-build Asterisk DB (All Tenants)

**vitalpbx check-integrity:** The command to check the environment integrity now verifies the integrity of each tenant and set the right permissions and owner/group for the folders

## 10.8 Credits

### 10.8.1 Sources of Information

VitalPBX Tooltips

Digium web page & wiki

Asterisk files

Google Search (Various)

Voip-info.org

dictionary.com

openvpn.net

<http://www.asteriskdocs.org>