CompletePBX 5

User Manual

(for version 5.3.4)

Contents

Contents

1. Introduction......9

About this Documentation......10

About CompletePBX 5......11

Usability Features......12

New Concepts in CompletePBX 5......14

Class of Service......14

Extensions and Devices......14

Hot Desking......14

Technology Settings......15

Telephony......15

Software Maintenance......16

‘yum’ Repositories......16

‘yum’ History......17

Documentation Conventions......20

Remote Access to the User Interface......23

Getting the IP Address of CompletePBX......23

Administrator Interface......23

User Portal......24

Overview of the Menu Layout......26

Administrator’s Menu Layout......26

Portal Menu Layout......29

Security......30

Secure the Password for User root......30

Secure SSH access to your system:......31

Verify Status of Intrusion Detection and Firewall......33

Configure non-standard external ports for SIP, IAX2, and SSH......36

Password Security......36

Class of Service......39

Creating extensions......41

Global SIP configuration......42

Additional Documentation......43

Configuration Considerations......44

Numbering......44

Dependencies......45

Destinations......45

Mandatory Fields and Dialog Dependencies.......... 47
2. CloudPhone.......... 51
CloudPhone License.......... 52
License Activation for MT Manager.......... 52
License Activation for a Standalone System.......... 53
Configure CloudPhone in CompletePBX 5.......... 54
Configuring a Mobile Device.......... 55
Creating a CloudPhone Desktop Device.......... 58
Installing CloudPhone Desktop on Windows.......... 60
Installing CloudPhone Desktop on Mac.......... 63
Resetting a CloudPhone Device.......... 66
3. PBX Menu Set.......... 68
Extensions Menu Group.......... 69
Extensions Dialog.......... 69
Hot Desking Dialog.......... 88
Import/Export Extensions Dialog.......... 93
Bulk Modification Dialog.......... 94
Extensions Status Dialog.......... 96
Applications Menu Group.......... 99
Conferences Dialog.......... 99
Scheduled Conferences Dialog.......... 103
GENERAL Functionality.......... 103
Custom Applications Dialog.......... 105
Custom Destinations Dialog.......... 106
Feature Codes Dialog.......... 107
Paging & Intercom Dialog.......... 118
Pickup Groups Dialog.......... 119
Parking Dialog.......... 121
Speed Dialing Dialog.......... 122
Import/Export Speed Dialing Dialog.......... 123
Voicemail Broadcast Groups Dialog.......... 123
Call Back Dialog.......... 124
DISA Dialog.......... 125
PIN Lists Dialog.......... 126
Emergency Dialog.......... 127
Class of Service Menu Group.......... 130
Class of Service Dialog.......... 130
Feature Categories Dialog.......... 131
Dialing Restriction Rules Dialog.......... 132
Customer Codes Dialog.......... 134
Authorization Codes Dialog.......... 134
Number Manipulation Dialog.......... 135

Route Selections Dialog........ 138
Call Center Menu Group........ 140
Ring Groups Dialog........ 140
Queues Dialog........ 141
Queues Priorities Dialog........ 148
Queue VIPs Dialog........ 148
External Menu Group........ 150
Trunks Dialog........ 150
Outbound Routes Dialog........ 160
Inbound Routes Dialog........ 164
Import/Export Inbound Routes Dialog........ 167
CID Modifiers........ 168
Example of SIP Trunk Configuration........ 170
Incoming Calls Menu Group........ 175
IVR Dialog........ 175
Time Groups & Time Conditions........ 179
Time Groups Dialog........ 179
Time Conditions Dialog........ 182
Announcements Dialog........ 183
Languages Dialog........ 184
Night Mode Dialog........ 185
CID Based Routing Dialog........ 186
Tools Menu Group........ 189
Asterisk CLI Dialog........ 189
Blacklist Dialog........ 190
Dashboard Dialog........ 190
Log File Viewer Dialog........ 191
Phonebook Dialog........ 192
Virtual Agents Menu Group........ 197
Virtual Agents Dialog........ 197
Virtual Agents Settings Dialog........ 213
4. Reports Menu Set........ 215
CDR Reports Menu Group........ 216
CDR Filters Dialog........ 217
CDR Dialog........ 219
PBX Reports Menu Group........ 223
Status Dialog........ 223
Concurrent Calls Dialog........ 227
5. Settings Menu Set........ 228
Technology Settings Menu Group........ 229
SIP Settings Dialog........ 229
IAX2 Settings Dialog........ 235

H 323 Dialog....238
Profiles Dialog....239
Telephony Settings Dialog....245
Dial Profiles Dialog....245
Voicemail Settings Menu Group....248
Voicemail Settings Dialog....248
Voicemail Timezones Dialog....251
PBX Settings Menu Group....254
System General Dialog....254
Asterisk Manager Users Dialog....260
Music on Hold Dialog....260
Recordings Management Dialog....261
Log Settings Dialog....263
Fax Settings Dialog....264
Call Recording Dialog....267
CDR Settings Dialog....268
Wakeup Calls Settings Dialog....269
Telephony Menu Group....271
Interfaces Dialog....271
Clock Sources Dialog....272
Channel Groups Dialog....273
Profile Assignments Dialog....274
End Point Manager Menu Group....276
Host Settings Dialog....277
Cloud Phone Dialog....279
Teams Connector Dialog....282
Templates Dialog....284
Device Mapping Dialog....289
Import/Export Devices Dialog....290
Zero Touch Dialog....291
Hospitality Menu Group....293
PMS Interface Dialog....295
Wakeup Calls Dialog....305
Testing the Hospitality Module Configuration....307
App Manager Menu Group....313
Supervision Manager....313
6. Admin Menu Set....334
Admin Menu Group....335
Users Dialog....335
User Profiles Dialog....338
Application Access Dialog....340
Backup & Restore Dialog....341

Backup & Restore Plugin........ 346
External Storage Providers Dialog........ 353
System Settings Menu Group........ 357
System Misc Dialog........ 357
Network Settings Dialog........ 360
Email Settings Dialog........ 364
DHCP Settings Dialog........ 367
Task Manager Dialog........ 369
Security Menu Group........ 374
Firewall Dialog........ 374
Intrusion Detection Dialog........ 378
Passwords Dialog........ 382
HTTPS Dialog........ 384
AUTHENTICATION Dialog........ 386
Maintenance Menu Group........ 390
License Status Dialog........ 390
Updates Dialog........ 393
Diagnostics Dialog........ 394
Twinstar Menu Group........ 396
TwinStar Status Dialog........ 396
7. User Portal........ 399
Portal........ 400
About........ 400
General........ 401
My Extension Menu Group........ 403
Call Logs Dialog........ 403
Voicemail Dialog........ 405
Faxes Dialog........ 406
Phonebook Dialog........ 408
Settings Menu Group........ 410
Extension Settings Dialog........ 410
My Time Group Dialog........ 417
Fax Settings Dialog........ 419
Operator Menu Group........ 421
Switchboard Dialog........ 421
8. Call Center Statistics........ 429
Introduction........ 430
Reports........ 431
Administration and Configuration of Users........ 431
Editing Users........ 432
Access........ 432
Settings and Preferences........ 433

Configuration Variables....433
Selecting Reports.... 435
Filtering Queues and Agents....435
Filter by Date Range Hours.... 435
Results....435
Calls Answered....436
Calls Answered Overview....436
Service Level.... 437
Disconnection Cause....437
Answered Calls Detailed Report....438
Transfers....438
Unanswered calls.... 438
Disconnection Cause....438
Unanswered Calls by Queue.... 439
Unanswered Call Details.... 439
9. Asterisk Configuration Files....440
Introduction.... 440
Managing Asterisk Configuration Files....440
Managing Modules.... 441
10. SNGREP.... 442
Interface....442
Shortcut Keys.... 442
Call List Screen.... 442
Call Flow Screen....444
Call Raw Screen....444
Message Difference Screen....444
Command Line....445
11. System Protection & Utilities....447
Introduction....448
System Protection.... 449
Uninterruptible Power Supplies.... 450
Redundant Components....451
Surge Protection....452
Rapid Recovery....453
Instructions.... 453
Main Menu.... 453
Restore....453
12. Xorcom Support....454
Xorcom Hardware Licenses.... 455
Applying a New Xorcom License....456
Managing Echo....457
Managing Echo in Telephony Systems.... 457

Reducing Echo....457
Eliminating Echo....457
Managing DAHDI Channels....458
Xpp_blink Utility....458
Adding an Astribank....458
13. Xorcom Applications.... 460
Broadcasting Burglar Alarm System Messages.... 460
Opening Doors....462
Tips and Tricks....463
VoIP Public Address System....464
Overview....464
How it Works....464
Implementing Rapid PA....464
Wiring Table.... 465
Kewl Start Setup Procedure.... 465
14. Appendix.... 466
Feature Codes....467
BLF (Hints).... 470
CDR table in Asterisk Database....472
Asterisk Dial Options.... 476
Call Flow.... 480

1. Introduction

About this Documentation

The revision number of this document that appears on the first page, and in the headings of all subsequent pages, indicates the version of the CompletePBX 5 that corresponds to this manual. For example, the heading **CompletePBX 5 User Manual (for version 5.1.1)** on the first page of this manual indicates that the documentation has been updated to describe features that were included in release v5.1.1 of the product.

About CompletePBX 5

CompletePBX 5 is supported on CentOS 7 and Debian 12 operating systems. , and is based on a highly responsive graphic user-interface that facilitates the management of Asterisk servers in a fast, intuitive, and secure manner.

CompletePBX 5 can be installed on a physical system, a virtual machine, or a cloud-based device. The system must be licensed in order to manage more than 3 extensions.

The system is based on a 3-level menu system that makes it very easy to locate any item that you want to manage.

Usability Features

Some of the usability features of the system you should be aware of are:

- You can manage CompletePBX 5 from any hardware device. The system transparently adapts to all devices, whether it be a smartphone, tablet, Windows, MAC, or Linux.
- You can access CompletePBX 5 with any modern web browser, including Mozilla Firefox, Google Chrome, Opera, Microsoft Edge, and Microsoft Internet Explorer.
- At the top of each dialog, you will find a Search Box. Typing any text in the Search Box activates the system-wide global search option, allowing you to easily search extensions, call queues, conferences, DISA, trunks, dialogs, etc. For example, if you want to modify the configuration of extension 2941, you can simply type **2941** in the Search Box, and you will be presented with a list of all objects that are indexed by 2941. The search is activated on both top-level and second-level objects. You can also use this search mechanism to locate any dialog. For example, if you type **queue**, you will be presented with a list of all dialogs that contain the word queue, as well as any feature codes that relate to queues. This mechanism is case-insensitive, so it does not matter if you type Queue, QUEUE, or queue.
- When you navigate to a dialog, you will notice the Show All icon at the top right corner. When you press on the Show All icon, a list of all the objects that belong to the current dialog will be displayed. At the top of the list you will also notice the Search icon which you can use as a filter. Type any part of the name of the object that you want to look for, and all objects that match your filter will be displayed.
- CompletePBX 5 has been designed so that all the information is always visible on a single page without having to scroll down and lose sight of the rest of the content. For this reason, you will see that most dialogs are divided into multiple tabs that enable you to easily see all the data for the current object.
- The system is multi-tab, which means you can work on any tab in any dialog without closing the previous tab, allowing you to work on different tabs of the dialog or even different dialogs. You don’t have to save data in one tab before opening another tab, so you can work simultaneously on multiple tabs or dialogs. For example, if you are defining a ring group, and realize that you have not defined an extension that will be a destination for the ring group, you can simply open the Extensions dialog, create and save the missing extension, return to the ring group and complete it using the newly created extension.
- The actions buttons, such as Save, Update, Delete, and Cancel, will always be visible at the bottom of the page, and are not dependent on the size of the page that you are using.
- Clicking the Cancel action button will create a new (empty) dialog, allowing you to easily create a new object.
- You can get more screen space by hiding the left-hand navigation menu. You can do this by pressing the Hide button located in the upper left corner of each dialog.
- All fields have tooltips for online help. On large screens, you only need to hover over the field name and the online help will be displayed. In the case of devices that have small screens, such as laptops with a low-resolution screen, mobile devices and tablets, you will need to press on the help balloon to access the help text.

- In some dialogs, after pressing **Save** or **Update**, you will notice an animated button that says **Apply All Changes** in the top right corner of the dialog 

. Starting from version 5.2.31, this button replaces the Reload icon  . This indicates that your update has been stored in the database, but you will need to press on the **Apply All Changes** button to make the running (active) system aware of the update. In situations where more than one administrator is managing the system, and one of the administrators has pressed the **Apply All Changes** button, the other administrator will not be able to press the **Apply All Changes** button until the reload is complete. In other words, multiple reloads cannot be activated at the same time.
- Mandatory fields are indicated by a star following the field name, e.g. **Name*** indicates that the Name field is mandatory.
- A feature-rich set of APIs are available for CompletePBX API client implementers, CompletePBX 3rd-party add-on developers and CompletePBX integrators. Detailed information can be obtained by contacting Xorcom Support.

New Concepts in CompletePBX 5

Class of Service

The functionality of the system can be segmented into sections, known as a Class of Service (CoS). The Class of Service is a basic organizational unit within the system that can keep different groups of users independent of each other. The system uses Class of Service to enforce security boundaries between the various groups of users, as well as to provide different rights to different groups of users.

Using Class of Service makes it very easy to make global changes to whole groups of users, without the need to modify settings for each individual user in the group.

Each Class of Service comprises three groups of functionality:

- Feature Category, which allows you to create groups of system feature codes, and determine which users can access to them.
  For example, you may not want all users to have access to the Spy feature codes. You could create a Feature Category that provides access to these codes, but only selected users would belong to the Class of Service that permits this access.
- Dialing Restriction Rules, enable you to restrict outbound dialing in accordance with a set of rules.
  You can use this feature to deny access to international dialing for extensions that belong to a specific Class of Service, or to block specific extensions from making external calls.
- Route Selection allows you to control the routing of outbound calls during specified time periods.
  You can use this feature to block long-distance calls outside of normal working hours for all extensions that belong to a specific Class of Service.

Extensions and Devices

Multiple physical devices can be linked to a single extension. Each device that is linked to the same extension shares the settings of the extension.

For example, you could configure your desk phone and mobile phone as devices on the same extension. Both devices would share common settings, including name, features, voice mail, CID information, and DID number. This removes the need to create complicated (and often, confusing) follow me scenarios.

In addition to SIP, IAX2, and Telephony (FXS) devices, CompletePBX 5 also supports Mobile and Custom devices.

Hot Desking

Hot Desking creates accounts for devices without the need of having an extension number. A Hot Desking device can be linked to an extension that was previously created in the extensions dialog with technology option "None", i.e. without being associated with any specific device type.

A Hot Desking device can be associated with an extension by keying in the hot desking feature code (default code *80): you will be prompted to enter the extension number and password. To remove the association, you need to key in the hot desking feature code (default code *80): you will be prompted to confirm the extension number and password.

Technology Settings

Technology Settings enables you to configure a wide range of parameters that are common to all SIP, IAX2 or Technology (analog) devices. This reduces the need for repetitive configuration, as well as allowing you to easily make system-wide changes to all devices.

Telephony

Telephony allows you to configure and manage analog telephony hardware that is connected to your server. Any analog hardware that is connected to your server can be easily detected, and can be displayed in an intuitive, graphical manner.

Software Maintenance

Fixed issues and improvements for the product are published on a regular basis – typically, every two weeks. You can review these updates by visiting https://xorcom.com/category/completepbx-change-log/ on our website.

These updates can easily be added to your system by logging into the Linux command line interface, and running the **`yum update`** command.

On CSX1000 (“Spark”) systems, as well as new CXT3000, CXT4000, and Twinstar systems, use the **`apt update`** and **`apt full-upgrade`** commands, as these appliances come with the Debian operating system.

It is important that you implement these updates regularly to ensure that your system is kept current and includes the latest available security updates.

‘yum’ Repositories

Following the update to CompletePBX v.5.0.60, the source of all CentOS 7, Epel (Extra packages for Enterprise Linux), and CompletePBX 5 packages is set to the repo1.xorcom.com server.

The switch from the standard CentOS 7 and Epel repositories to the new Xorcom repositories was performed by the xorcom–centos-release package that was automatically installed as part of the upgrade procedure for CompletePBX 5 v.5.0.60.

The xorcom–centos-release package replaces the standard centos-release and epel-release packages. As result, the standard CentOS-*.repo and epel*.repo files are replaced with CompletePBX-specific files.

As a result of this change:

- There is a single repository for ***all*** updates
- The single repository is fully managed by Xorcom
- The Xorcom-managed repository ensures complete compatibility between operating system and applications
- CompletePBX 5 updates will be synchronized (and always tested with) the exact same versions that will be received by the user during an update
- Provides a single source for all updates, so that firewall can now be configured to allow access to only a single address

The cpbx.repo file is also replaced with cpbx5.repo by cpbx-upgrade package.

‘yum’ configuration files prior to CompletePBX 5 v.5.0.60:

- CentOS-Base.repo
- CentOS-CR.repo
- CentOS-Debuginfo.repo
- CentOS-Media.repo
- CentOS-Sources.repo

- CentOS-Vault.repo
- CentOS-fasttrack.repo
- cpbx.repo
- epel-testing.repo
- epel.repo

‘yum’ configuration files following the upgrade to CompletePBX 5 v.5.0.60:

- CentOS-Base-Xorcom.repo
- CentOS-EPEL-Xorcom.repo
- cpbx.repo.old
- cpbx5.repo

Note that the original cpbx.repo is not deleted, it is just renamed to cpbx.repo.old.

Be aware that any manual changes in the *.repo files will not be overwritten during later upgrades. Instead, the changed files will be preserved, and the newer files will be installed with extension .rpmnew

When upgrading any CompletePBX system (excluding Spark) from version 5.0.59, or older, use the following 2-step command to ensure that the system will be updated from the correct repositories:

1. **`yum install xorcom-centos-release`**
2. **`yum update`**

‘yum’ History

You can see the list of recently applied updates with the command:

```
yum history
```

```
Demo> yum history
Loaded plugins: fastestmirror
ID     | Command line             | Date and time    | Action(s)      | Altered
-------------------------------------------------------------------------------
   144 | update                   | 2020-02-11 09:43 | O, U           |   12 ##
   143 | update                   | 2020-01-27 09:47 | O, U           |   10 ##
   142 | install sngrep           | 2020-01-06 11:59 | Install        |    1
   141 | install asterisk-snmp    | 2020-01-06 11:08 | Install        |    1
   140 | install net-snmp net-snm | 2020-01-06 11:07 | Install        |    5
   139 | update                   | 2020-01-06 09:57 | O, U           |   10 ##
   138 | update                   | 2019-12-23 10:04 | O, U           |   12 ##
   137 | update                   | 2019-12-09 09:24 | O, U           |   10 ##
   136 | update                   | 2019-11-25 10:20 | O, U           |   18 ##
   135 | update                   | 2019-11-18 09:53 | O, U           |   21 ##
   134 | update                   | 2019-10-28 09:28 | I, O, U        |   14 ##
   133 | update                   | 2019-10-22 09:21 | Update         |    1 EE
   132 | update                   | 2019-10-02 10:24 | I, O, U        |   17 ##
   131 | update                   | 2019-09-09 09:13 | O, U           |   13 ##
   130 | update                   | 2019-09-02 09:13 | E, I, O, U     |   81 ##
   129 | update                   | 2019-08-26 08:46 | O, U           |    9 ##
   128 | update                   | 2019-08-12 10:36 | O, U           |   16 ##
   127 | update                   | 2019-07-29 08:52 | I, O, U        |   20 ##
   126 | update                   | 2019-07-08 09:22 | I, O, U        |   12 ##
   125 | update                   | 2019-06-17 10:27 | O, U           |   12 ##
history list
```

If you want to see the log of a specific update, you can run the command (substituting the ID from the yum history output for the <id> placeholder):

```
yum history info <id>
```

```
Demo> yum history info 113
Loaded plugins: fastestmirror
Transaction ID : 113
Begin time     : Thu Sep 20 18:17:41 2018
Begin rpmdb    : 596:f1ff171fd04f889ef869aad12d7c0cb05e0f9b00
End time       :            18:17:44 2018 (3 seconds)
End rpmdb      : 596:24cda11dbf9b6c6649122a84620386d16ce2794e
User           : root <root>
Return-Code    : Success
Command Line   : update
Transaction performed with:
    Updated       rpm-4.11.3-32.el7.x86_64                        @base/7
    Updated       yum-3.4.3-158.el7.centos.noarch                 @base/7
    Installed     yum-metadata-parser-1.1.4-10.el7.x86_64         @anaconda/7
    Updated       yum-plugin-fastestmirror-1.1.31-46.el7_5.noarch @updates/7
Packages Altered:
    Updated kexec-tools-2.0.15-13.el7.x86_64      @base/7
    Update              2.0.15-13.el7_5.1.x86_64 @updates/7
history info
```

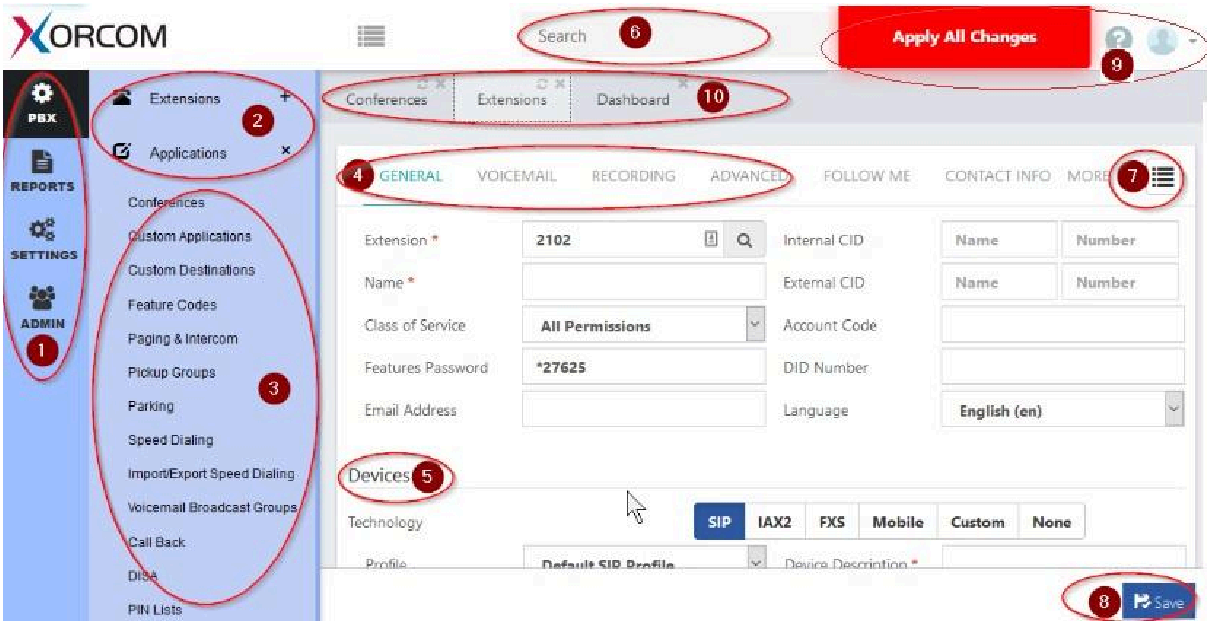
Changes and updates to the PBX system are documented in the system database, so you can review the updates by running the command:

```
mysql ombutel -e "select * from ombu_patches"
```

```
Demo> mysql ombutel -e "select * from ombu_patches where patch_id>680"
+----------+-----------+------------------------------------------+---------------------+
| patch_id | component | filename                                 | applied             |
+----------+-----------+------------------------------------------+---------------------+
|      681 | core      | 20190926.gxp2140_button_types.sql        | 2019-11-18 09:53:44 |
|      682 | core      | 20190926.gxp2160_button_types.sql        | 2019-11-18 09:53:44 |
|      683 | core      | 20190926.gxp2170_button_types.sql        | 2019-11-18 09:53:44 |
|      684 | core      | 20191015.kill_orphaned_cos_destinations.sql | 2019-11-18 09:53:44 |
|      685 | core      | 20191027.kill_orphaned_pea_destinations.sql | 2019-11-18 09:53:44 |
|      686 | core      | 20191028.remove_disabled_vmb_members.sql | 2019-11-18 09:53:44 |
|      687 | core      | 20191030.rename_htek_uc902.sql           | 2019-11-18 09:53:44 |
|      688 | core      | 20191024.concurrent_calls.sql            | 2019-11-25 10:21:06 |
|      689 | core      | 201911.vtech_ctm-s2312.sql               | 2019-11-25 10:21:06 |
|      690 | core      | 20191105.vtech_ctm-s2421.sql             | 2019-11-25 10:21:06 |
|      691 | core      | 20191105.vtech_s2100l.sql                | 2019-11-25 10:21:06 |
|      692 | core      | 20191105.vtech_s2210l.sql                | 2019-11-25 10:21:07 |
|      693 | core      | 20191111.hints.sql                       | 2019-11-25 10:21:07 |
|      694 | core      | 20191114.trunks.sql                      | 2019-12-09 09:24:52 |
|      695 | core      | 20191124.cloudphone_device.sql           | 2019-12-23 10:04:57 |
|      696 | core      | 20191125.cloudphone.sql                  | 2019-12-23 10:04:57 |
|      697 | core      | 20191203.update_htek_uc923_acl_dialplan.sql | 2019-12-23 10:04:57 |
|      698 | core      | 20191204.outbound_route_cid_pattern.sql  | 2019-12-23 10:04:57 |
|      699 | core      | 20191212.cloudphone_profile.sql          | 2019-12-23 10:04:57 |
|      700 | core      | 20200101.1.vtech_ls_s3410.sql            | 2020-02-11 09:44:18 |
|      701 | core      | 20200123.1.vtech_s2220l.sql              | 2020-02-11 09:44:18 |
|      702 | core      | 20200123.1.vtech_s2221l.sql              | 2020-02-11 09:44:18 |
+----------+-----------+------------------------------------------+---------------------+
```

Documentation Conventions

Chapters 2 through 5 of this documentation outline the menus of the user interface, following the order in which they appear in the system.



The left-hand side of the user interface is divided into four main parts, which are referred to in this reference guide as Menu Sets, marked as ❶ in the screen grab above.

These Menu Sets are further divided into Menu Groups ❷, which contain multiple Dialogs ❸.

Across the top ❿ there is a navigation bar showing tabs for each of the dialogs that you have opened. Click on any of the tabs to access the appropriate dialog. Each tab includes a remove icon - clicking on it allows you remove the tab. Most tabs also include a refresh icon - clicking it will cause the dialog to be shown and refreshed so that any changes that you have made in the dialog will now be shown. Note that if you refresh any tab on the navigation bar, any changes that you have made in the dialog, but not saved, will be lost.

To facilitate navigation within the system, the larger Dialogs are further sub-divided across the top into Tabs ❹. Within the tabs, some dialogs may be organized into logical groupings, which are referred to as Sections ❺in this documentation.

Each dialog contains a Search Box ❻, which activates the system-wide global search option, allowing you to easily search extensions, call queues, conferences, custom destinations, DISA, trunks, dialogs, etc. For example, if you want to modify the configuration of extension 2941, you can simply type **2941** in the Search Box, press enter, and you will be presented with a list of all objects that are indexed by 2941. You can also use this search mechanism to locate any dialog. For example, if you type **queue**, you will be presented with a list of all dialogs that contain the word queue, as well as any feature codes that relate to queues. This mechanism is not case-sensitive, so it does not matter if you type Queue, QUEUE, or queue.

All dialogs also include a Show All icon ❼ at the top right corner. When you press on the Show All icon, a list of all the objects that have been created by that dialog will be displayed. At the top the list you will also notice a Search icon which you can use as a filter. Type any part of the name of the object that you want to look for, and all objects that match your filter will be displayed.

At the bottom of the dialog there will be one, or more, Action Buttons ❽. These action buttons may vary between different dialogs, but will typically include Save (save the details of current dialog), Delete (completely delete the current item from the system), and Cancel (create a new, empty dialog)

The User Menu ❾ at the top of the screen shows information about the current user. It can also be used to login and logout of the system, to change the language in which the user interface will be displayed, and to see the version of CompletePBX that is currently installed. Note also the red Animated message "Apply All Changes", which will appear whenever you save changes in a dialog. This indicates that your update has been stored in the database, but you will need to press on the Apply All Changes button to make the running system aware of the update.

Click on the icon to open the latest version of this documentation.

In the documentation, field names are shown in **bold**, followed by a detailed description. Mandatory fields are denoted by a star (*) in both the documentation and the graphic user interface

Language

Allows you to see the current system-wide language, or to change to a different language.

The available languages consist of two parts: the first two letters (en, es, fr, etc.) indicate the language that will be used for prompts and system messages, while the second group of letters (US, ES, FR, etc) indicate the locale settings that will be used. The following system-wide languages are currently available:

- English (en_US)
- Spanish (es_ES)
- French (fr_FR)
- Dutch (nl_NL)

- Chinese (zh_CN)

About

Shows the current version of CompletePBX 5 that is currently installed on your system. In addition, the serial number and system name (that is configured in the Admin > System Settings > System Misc dialog) will also be displayed.

On physical systems, you can also see the status of your warranty, as well as access documentation and videos for Xorcom Astribanks.

Remote Access to the User Interface

Getting the IP Address of CompletePBX

You need to know the IP address of the CompletePBX server In order to access the administrator interface or the user Portal from a remote machine.

The default password for user ***root*** is documented in the Getting Started Guide for CompletePBX.

You can obtain the IP address by logging into the operating system of CompletePBX as ***root*** user and running the `ip a` command.

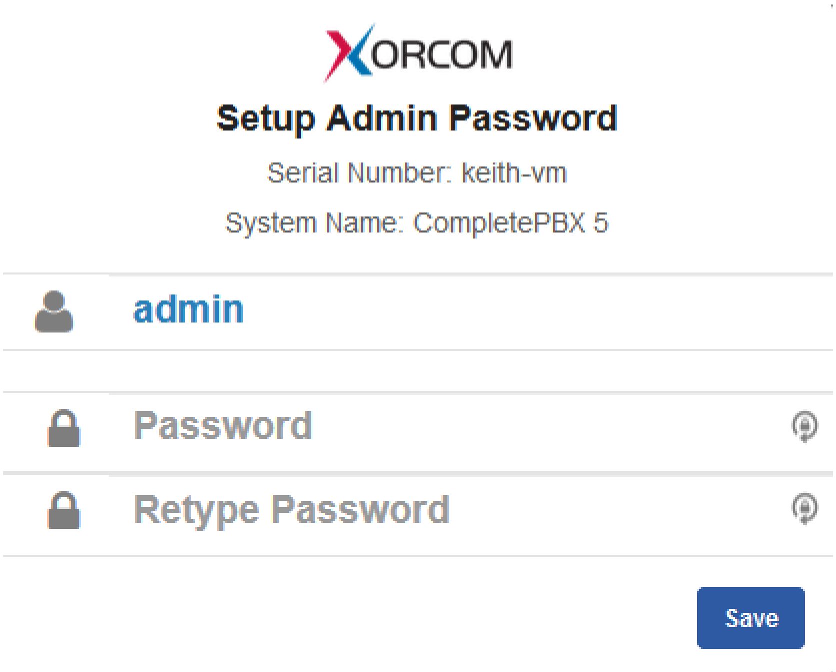
Administrator Interface

Use any internet browser to access the user interface, by entering the IP address of your CompletePBX server. Access can be configured (in the Admin>Security>HTTPS dialog) to use either HTTP or HTTPS protocol. You will be required to supply the username and password that has been defined for your system.

First Time Login

You will be prompted to set the admin password the first time that you log into the system

If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password.

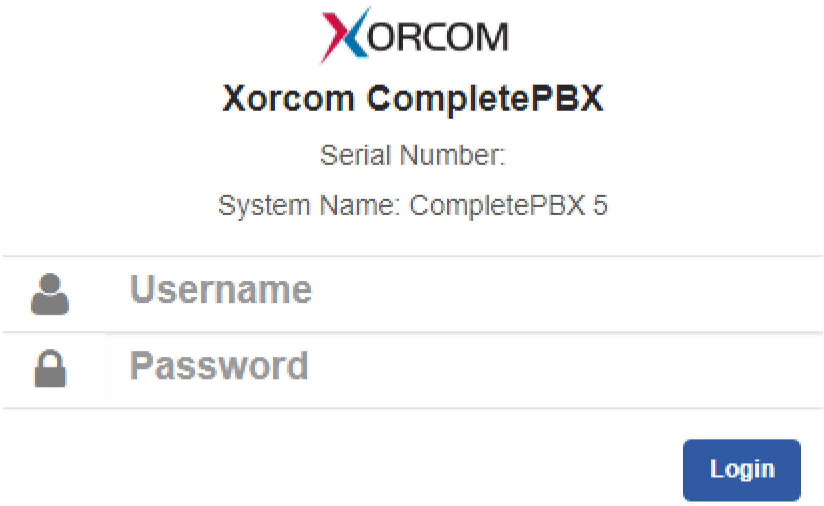


User Portal

Access to the Portal can be enabled (or disabled) for each user in the Extensions dialog.

Use any internet browser to access the Portal, by entering the IP address of your CompletePBX server in the address field of your browser. Access can be configured (in the Admin>Security>HTTPS dialog) to use either HTTP or HTTPS protocol. Enter your Portal username (typically your extension number) in the Username field, and your Portal password, (that the system administrator defined for you in the Advanced tab of the Extensions dialog), in the Password field.

If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password.

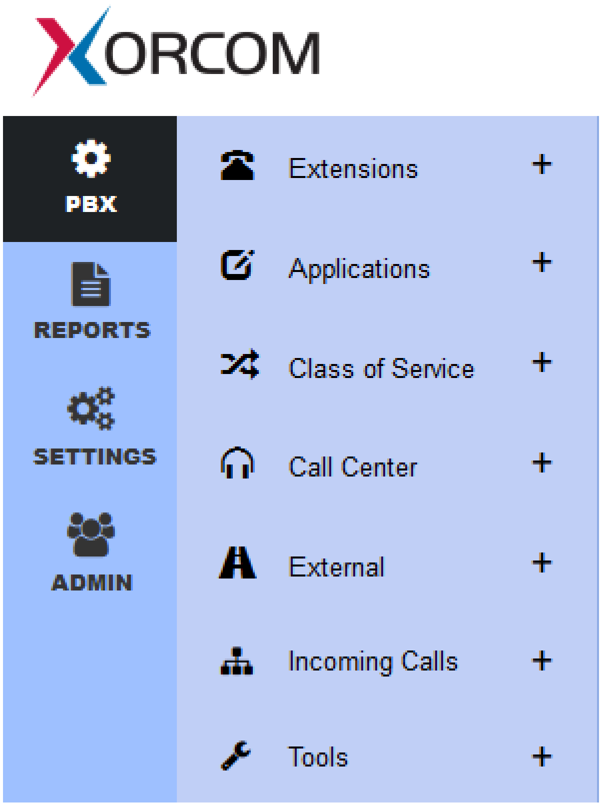


Note that you cannot simultaneously access both the User Interface and the User Portal using the same Internet browser window. If you want to simultaneously access both the User Interface and the User Portal, you will need to use different browsers.

Overview of the Menu Layout

Administrator's Menu Layout

The administrator's menu is divided into four menu sets – PBX, Reports, Settings, and Admin as outlined below. These menu sets are divided into menu groups which contain multiple dialogs



PBX menu set, where you can find all about the PBX settings:

- **Extensions** menu group
  - **Extensions**, manage extensions and devices
  - **Hot Desking**, device management
  - **Import/Export Extensions**, import or export extensions
  - **Bulk Modification**, bulk extension modification
  - **Extension Status**, display and modify the status of extensions
- **Applications** menu group
  - **Conferences**, conference room management
  - **Custom Applications**, custom application management
  - **Custom Destinations**, custom destination management
  - **Feature Codes**, manage system feature codes
  - **Paging & Intercom**, paging & intercom management
  - **Pickup Groups**, manage pickup groups
  - **Parking**, parking management

    - **Speed Dialing**, speed dial management
    - **Import/Export Speed Dialing**, import and export of speed dials
    - **Voicemail Broadcast Group**, manage voicemail broadcast groups
    - **Call Back**, manage call back functionality
    - **DISA**, Direct Inward System Access (DISA) management
    - **PIN Lists**, PINs that can be used to access outgoing routes
    - **Emergency**, special handling for dialing emergency services

- **Class of Service** menu group
    - **Class of Service**, settings that define the dial plan that each extension can access
    - **Feature Categories**, 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 codes that can be dynamically associated with a call in order to categorize the call in the CDR
    - **Authorization Codes**, code that authorizes privileges to make a call
    - **Route Selections**, Route selection management

- **Call Center** menu group
    - **Ring Groups**, create a single number that can simultaneously ring multiple extensions
    - **Queues**, queues, to which incoming calls can be directed
    - **Queue Priorities**, gives priority to a queue call when an agent is allocated to multiple queues
    - **Queue VIPs**, list of phones that can receive priority in the call queue

- **External** menu group
    - **Trunks**, SIP, IAX, and DAHDI trunk management
    - **Outbound Routes**, manage outgoing routes
    - **Inbound Routes**, manage incoming routes
    - Import/Export Inbound Routes, use CSV file to manipulate Inbound Routes

- **Incoming Calls** menu group
    - **IVR**, IVR and Automatic Attendant management
    - **Time Groups**, time group management
    - **Time Conditions**, time conditions management
    - **Announcements**, manage announcements
    - **Languages**, prompt language management
    - **Night Mode**, night mode management
    - **CID Modifiers**, modification of incoming CID name and number

- **Tools** menu group
    - **Asterisk CLI**, Asterisk command line management interface
    - **Blacklist**, black list management
    - **Dashboard**, real-time system status
    - **Log Files Viewer**, display the contents of log files
    - **Phonebook**, allows the creation of phonebooks to be used by IP phone

Reports menu set, where you can create reports about calling records

- **CDR Reports** menu group
    - **CDR Filters**, manage filters to apply to CDR reports
    - **CDR**, display call records (CDR)

- **PBX Reports menu group**
  - **Status**, display the current status of Channels, Registrations, Peers, Hints, Voicemail, and Queues
  - **Concurrent** Calls, display concurrent calls on outbound Trunks

Settings menu set, 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** menu group
  - **SIP Settings**, general SIP settings management
  - **IAX2 Settings**, general IAX2 settings management
  - H.323 Settings, manage H.323 configuration
  - **Profiles**, profile management
  - **Technology Settings**, configure the default time zone for users and peers
  - **Dial Profiles**, configure Asterisk dial options to be associated with extensions
- **Voicemail Settings** menu group
  - **Voicemail Settings**, general voice mail settings management
  - **Voicemail Timezones**, time zone management for voicemail
- **PBX Settings** menu group
  - **System General**, general system settings such as directories, dial-plan settings, etc
  - **Asterisk Manager Users**, manage Asterisk Manager users
  - **Music on Hold**, create and upload music on hold
  - **Recordings Management**, upload recordings
  - **Log Settings**, determine the format and content of log files related to Asterisk
  - **Fax Settings**, determine the format of the coversheet used by outbound faxes
  - **Call Recording**, manage Cloud recording
- **Telephony** menu group
  - **Interfaces**, detects and configures analog and digital interfaces
  - **Clock Sources**, determine clock sources for analog devices
  - **Channel Groups**, group external telephony interfaces such as E1, FXO, etc
  - **Profile Assignments**,
- **Endpoint Manager** menu group
  - **Host Settings**, create networks for device search
  - CloudPhone, configure settings for Xorcom CloudPhone
  - **Templates**, create templates for different devices
  - **Device Mapping**, search for devices connected to the network and configure them
  - **Import/Export Devices**, manage endpoint devices
- **App Manager** menu group
  - **FOP2 Manager**, allows you to configure Users, Buttons, Groups, Templates, Permissions, Plugins, and Settings for the Switchboard,

Admin menu set, allows you to create system users and manage system settings

- **Admin** menu group
  - **Users**, manage system users
  - **User Profiles**, manage user profiles

  - **Application Access**, manage access to specific applications and modules
  - **Backup & Restore**, backup and restore the telephony configuration.

- **System Settings** menu group
  - **System Misc,** manage system notifications and date and time settings
  - **Network Settings**, network management
  - **Email Settings**, email server configuration
  - **DHCP Settings**, DHCP server configuration
  - **HTTPS**, Configure profile to access user interface

- **Security** menu group (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)
  - **Firewall**, firewall management system
  - **Intrusion Detection**, management of fail2ban utility
  - **Passwords**, set password policy and detect weak passwords

- **Maintenances** menu group
  - **Licenses**, view the status of Xorcom licenses

- **TwinStar menu group**
  - **TwinStar Status**, shows the status of the TwinStar cluster

Portal Menu Layout

Portal menu set, where extension users can manage settings of their own extension**:**

- **My Extension** menu group
  - **Call Logs**, enables the extension owner to view CDR records
  - **Voicemail**, enables the extension owner to manage voicemail settings
  - **Faxes**, enables the extension owner to view incoming and outgoing faxes
  - Phonebook, view phonebooks, and use click-to-dial to call people in your phonebook

- **Settings** menu group
  - **Extension Settings**, enables the extension owner to manage the extension
  - **My Time Group**, enables the extension owner to manage time groups
  - **Fax Settings**, enables the extension owner to manage outgoing fax settings

Operator menu set, where extension users can manage settings of their own extension:

- **Switchboard** menu group
  - **Switchboard**, enables the extension owner to view the Switchboard and manage call handling

Security

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

Secure the Password for User root

An attacker who gains root access to your system can do more damage than if he gains normal user login, so pay special attention to safeguard this user.

Change root Password

Change the factory-configured password in your system for user root.

Log into your system as user **root,** using the factory-defined password, and use the **passwd** command in the Linux shell to change the password for 'root' user:

```
Demo> passwd
Changing password for user root.
New password:
```

Password Generator

Typing **password generator** into your search engine of your web browser will provide you with access to third-party password generators that you can use to create a strong password.

Alternatively, you can make use of the Linux command, as in the following example, to create a strong password:

```
cat /dev/urandom| tr -dc 'a-zA-Z0-9-_!@#$%^&*()_+{}|:<>?='|fold -w 12| head -n 4
```

```
Demo> cat /dev/urandom| tr -dc 'a-zA-Z0-9-_!@#$%^&*()_+{}|:<>?='|fold -w 12| head -n 4
17KyPsa2&%5K
s7MkQpI)o=f6
&%H:ZC#khfb+
VaisV(9NBTLB
Demo>
```

Secure SSH access to your system:

Configure Authentication Keys for SSH Login

Control root logins via SSH to prevent unauthorized access to your system. Configure your system to manage password-less authentication and ensure that all authorized users who require root access use SSH key pairs for authentication.

You can configure the SSH server to only allow users to log in when using an authentication key by following these steps:

1. Create a key pair on your client machine, i.e. on your computer. There are various methods of doing this, depending on the operating system of your computer. This step will provide you with two keys: A public key and a private key.
2. Copy the ***public*** key to a file in the **/root/.ssh/** directory on your CompletePBX 5 machine. You should call the file **authorized_keys**
3. It is strongly recommended not to modify the main SSH configuration file **/etc/ssh/sshd_config**, instead, custom SSH parameters should be placed inside **/etc/ssh/sshd_config.d/enable_root.conf** and enable the following parameters:
    - PubkeyAuthentication yes
    - AuthorizedKeysFile .ssh/authorized_keys
    - ChallengeResponseAuthentication no

    This ensures your configuration remains intact during system upgrades, as update processes may overwrite the main file but will not modify custom files inside sshd_config.d/

4. After making the above changes, save the **/etc/ssh/sshd_config.d/enable_root.conf** file, restart the sshd service by using the following command:

    systemctl restart sshd.service
5. After logging out of the CompletePBX 5 server, test that you can access the machine using the authentication key. You can use a command like **ssh root@<IP address>**
    You should be able to log into the CompletePBX 5 machine *without* entering a password.
6. You may also disable password login by user root and limit authentication attempts by making an additional modification to **/etc/ssh/sshd_config.d/enable_root.conf**. Look for the line PasswordAuthentication no and make sure it is ***not*** commented (i.e. does not have a **#** character at the beginning of the line)
    - PasswordAuthentication no
    - PermitRootLogin prohibit-password
    - MaxAuthTries 3

7. After making the above change, save the **/etc/ssh/sshd_config.d/enable_root.conf**, and restart the sshd service by using the following command:

    systemctl restart sshd.service

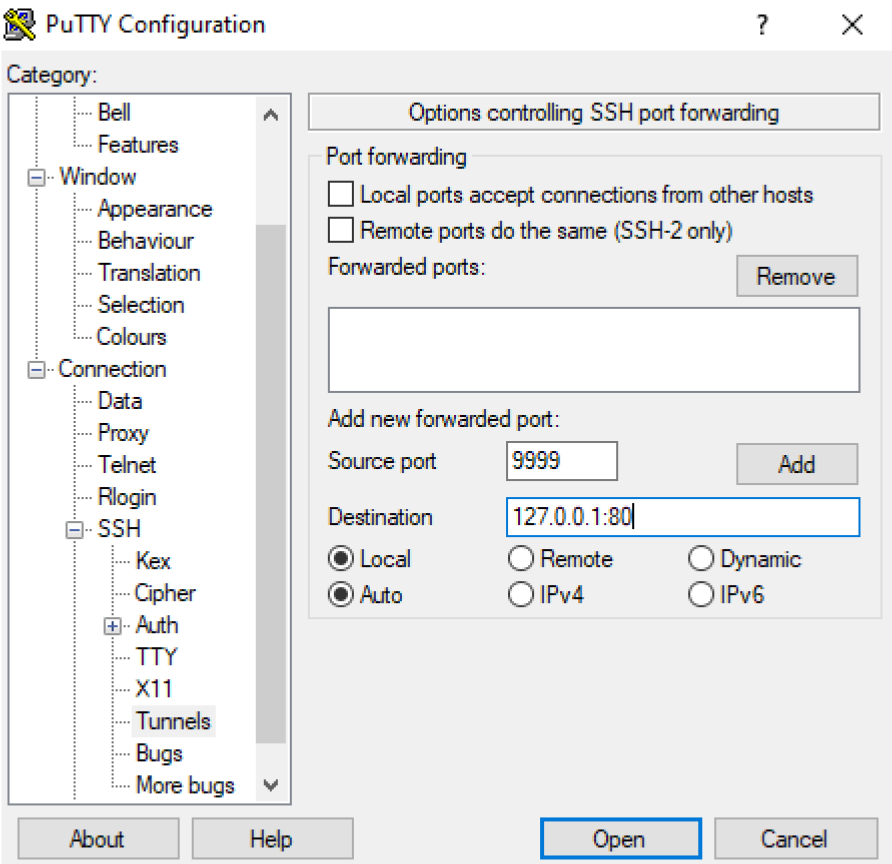
Configure Tunneling for External GUI Access

You can create a tunnel to access the CompletePBX 5 user interface when you access ssh.

The following example assumes that the port for ssh access is 8822 (instead of 22), the external IP address of the CompletePBX 5 server is 31.54.233.18, and the local port for the tunnel will be 9999:

```
ssh -p 8822 root@31.54.233.18 -L 9999:localhost:80
```

If you are using PuTTY from a Windows machine, you can configure tunneling from the Connection > SSH > Tunnels dialog, like this:



Click on **Add** to complete the configuration.

You will now be able to use the following command in your internet browser to access the CompletePBX 5 user interface:

```
http://127.0.0.1:9999/index.php
```

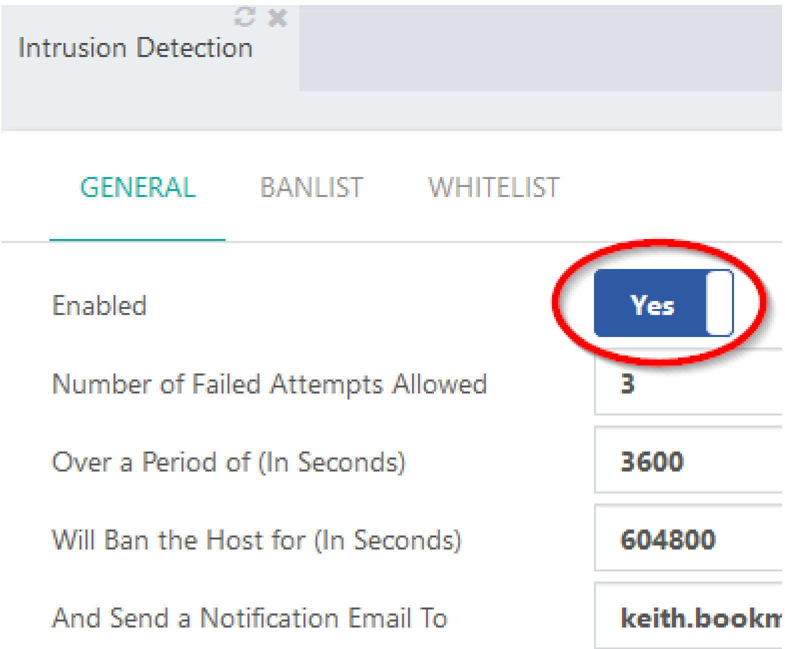
Verify Status of Intrusion Detection and Firewall

CompletePBX 5 Intrusion Detection and Firewall are active by default. Make sure that these settings have not been changed.

Activate Intrusion Detection

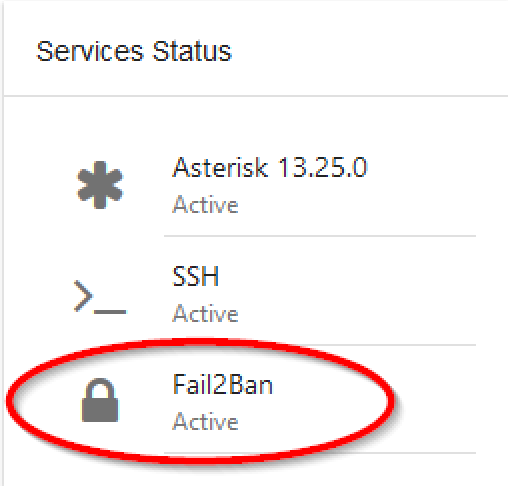
By default, Intrusion Detection is active when CompletePBX 5 leaves the factory.

However, you should verify that Intrusion Detection is properly configured and running. This can be managed from the Admin > Security > Intrusion Detection dialog.



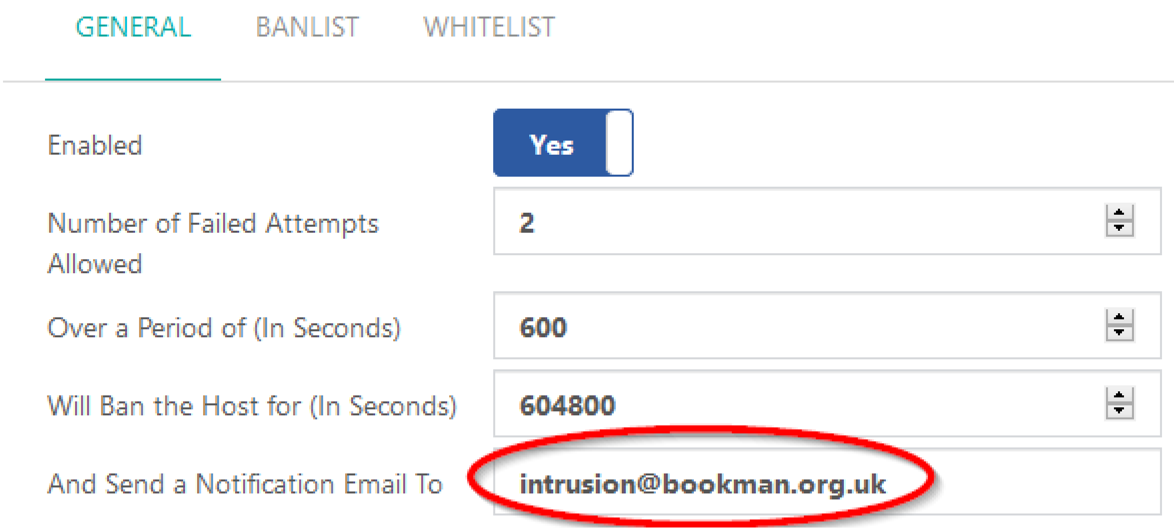
Verify Intrusion Detection Status

You can also use the Dashboard to verify that the Intrusion Detection (fail2ban) service is running



Intrusion Detection Notifications

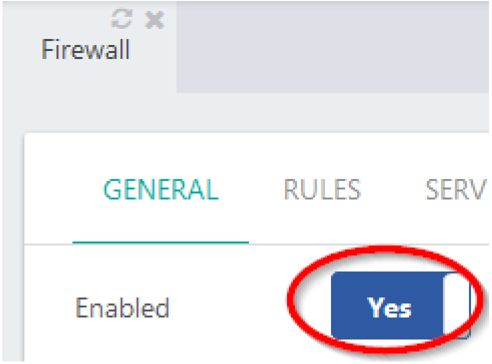
You will need to configure and test email in the Admin > System Settings > Email Settings dialog. After you have confirmed that your email is working as expected, make sure that you have configured a destination for notifications.



Activate Firewall

By default, Intrusion Detection is active when CompletePBX 5 leaves the factory.

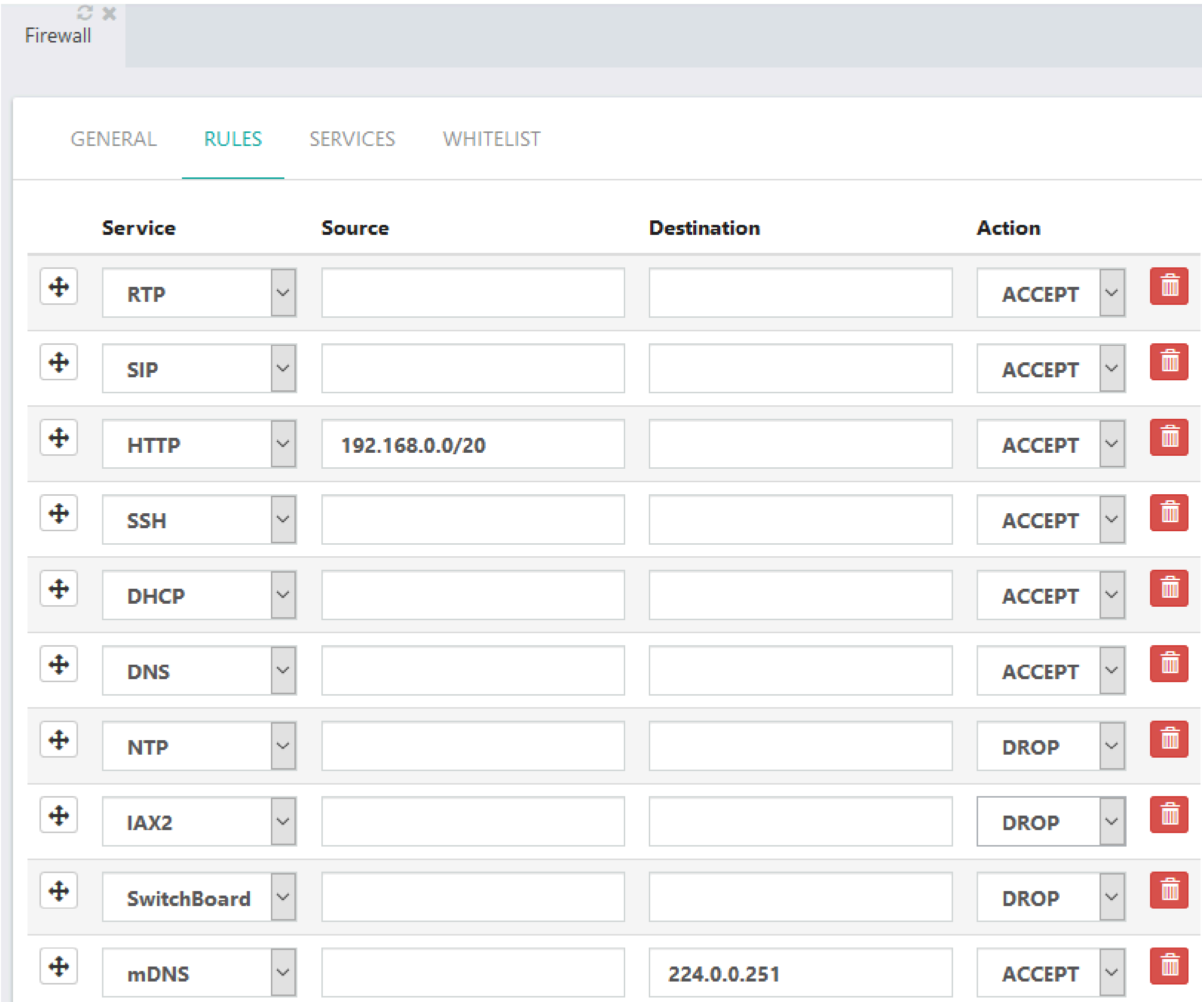
Make sure that the CompletePBX 5 firewall is enabled. You can access the firewall from Admin > Security > Firewall



Manage Allowed Ports

Make sure that the firewall only allows access to services (ports) and sources that are essential for the running of CompletePBX 5. You can access the firewall from Admin > Security > Firewall and modify the Rules tab. Any rules that relate to services for which access is not required should have the **Action** configured as **Drop.**

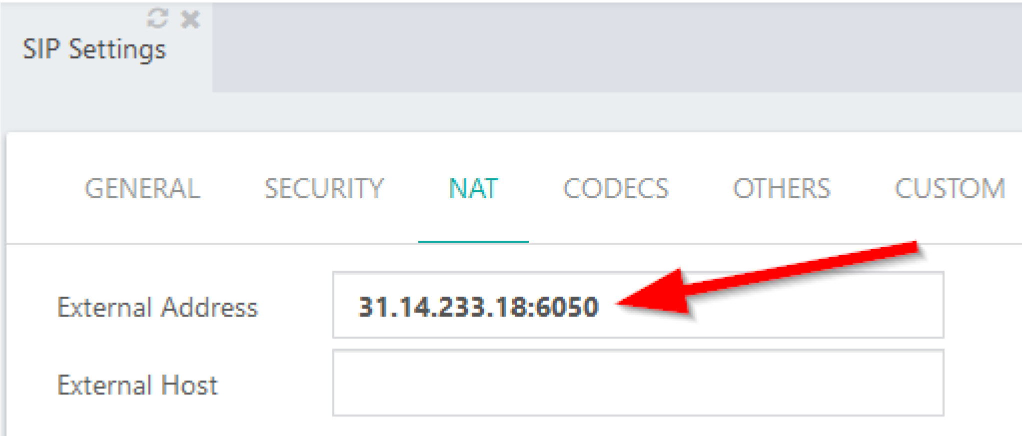
Where appropriate, you can also limit access to a service to a specific source.



Configure non-standard external ports for SIP, IAX2, and SSH

Do not expose ports for SIP (5060/udp) and IAX2 (4569/udp) to the Internet if you do not use remote extensions. You should not expose HTTP (80/tcp) or HTTPS (443/tcp) ports at all. Always use SSH tunneling for access to the CompletePBX user interface.

Instead of the default port (5060 is the default port for SIP devices), use a non-default port for external SIP traffic. This means that ***external*** extensions will use a different (non-default) port. Go to Settings > Technology Settings > SIP Settings, and make sure that your NAT is properly configured. The External Address field should contain the external address of your CompletePBX 5 system, as well as the port that is configured for external users. In the example below, external SIP users will access CompletePBX 5 using port 6050.



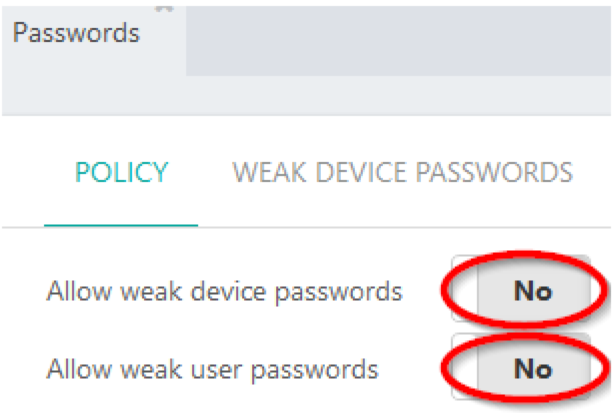
You will also need to configure your NAT router (typically your modem) to forward the non-standard port (6050 in the above example) to port 5060 on your CompletePBX 5 system.

Password Security

Verify Password Policy settings

Verify that the Password Policy, which you can access from Admin > Security > Passwords dialog, is configured for maximum security.

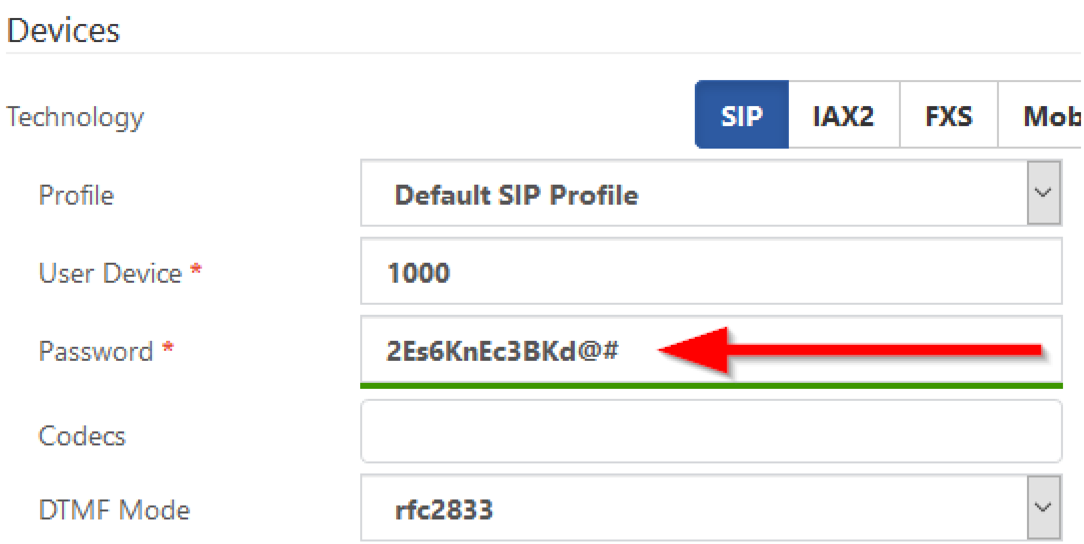
Both **Allow weak device passwords** and **Allow weak user passwords** fields should be configured as **No**



Device Passwords

Ensure that you use strong passwords for all SIP and IAX2 devices. CompletePBX 5 will automatically suggest strong passwords.

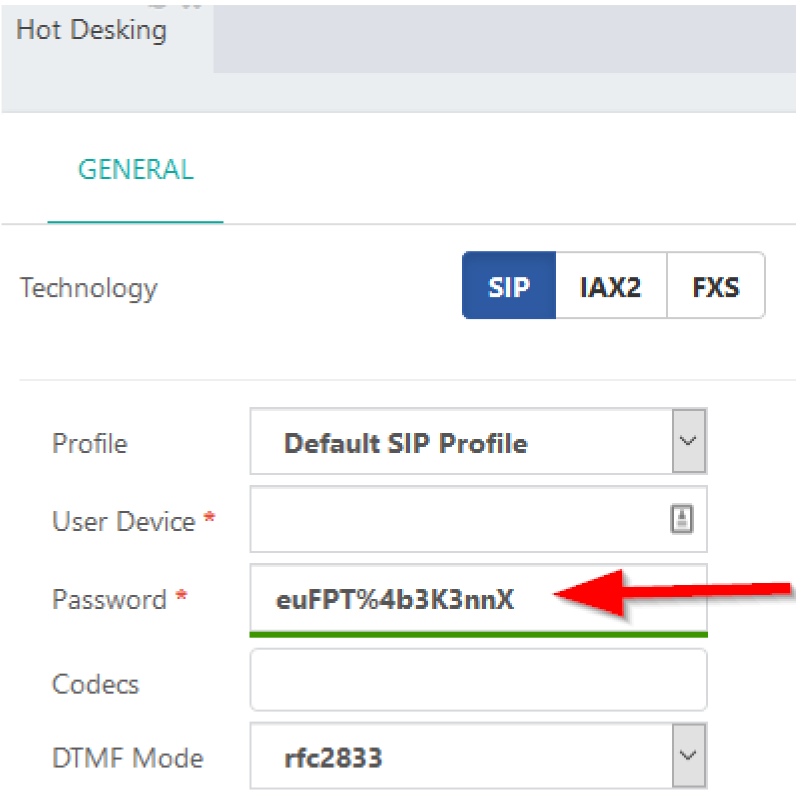
If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password



Hot Desking Passwords

Ensure that you use strong passwords for all SIP and IAX2 Hot Desking devices. CompletePBX 5 will automatically suggest strong passwords.

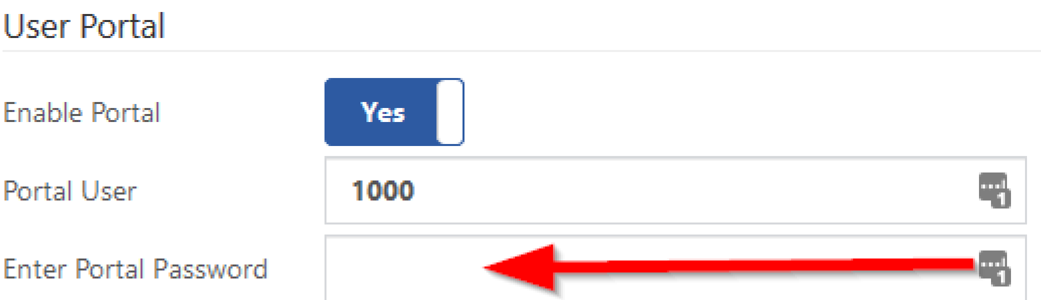
If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password



Portal User Passwords

If you enable extensions to have access to the User Portal (in the PBX > Extensions > Advanced dialog), ensure that you use strong passwords.

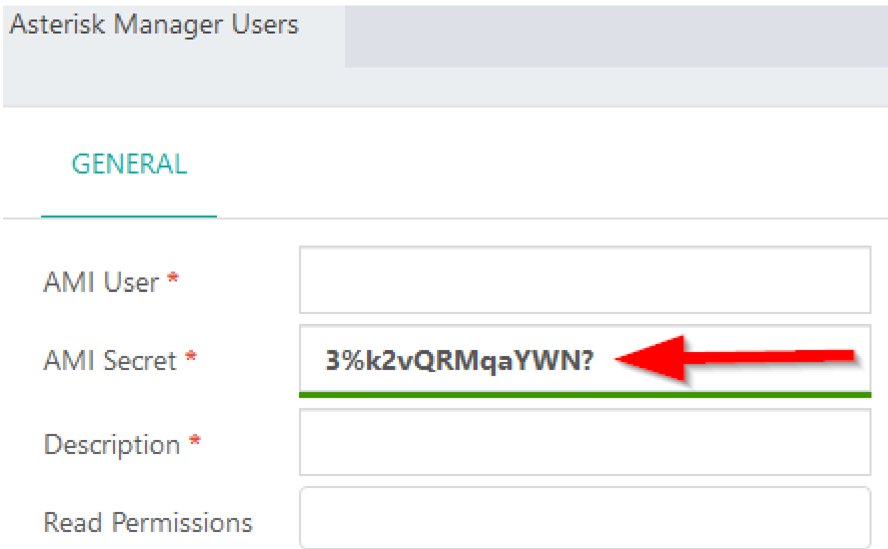
The password should not include repeating patterns (like abcabcabcabc), and should consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password



Asterisk Manager User Passwords

Ensure that you use strong passwords for all Asterisk Manager Users. CompletePBX 5 will automatically suggest strong passwords.

If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like dogdogdogdog). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password



DISA

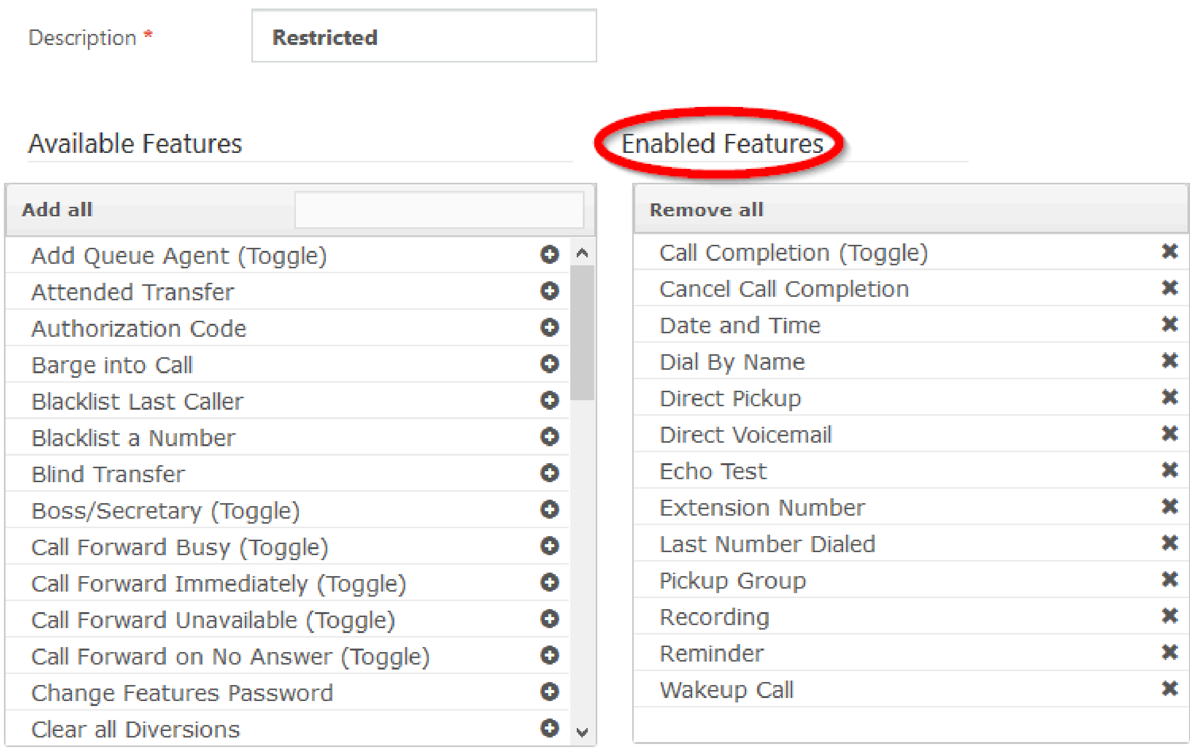
Make sure that DISA is protected by a password.

Class of Service

Make sure that you configure Classes of Service that will provide users only with the rights that they need. For example, if you have extensions that only require access to other extensions, make sure that the Class of Service for those extensions is linked to a Dialing Restriction Rule that does not allow external calls.

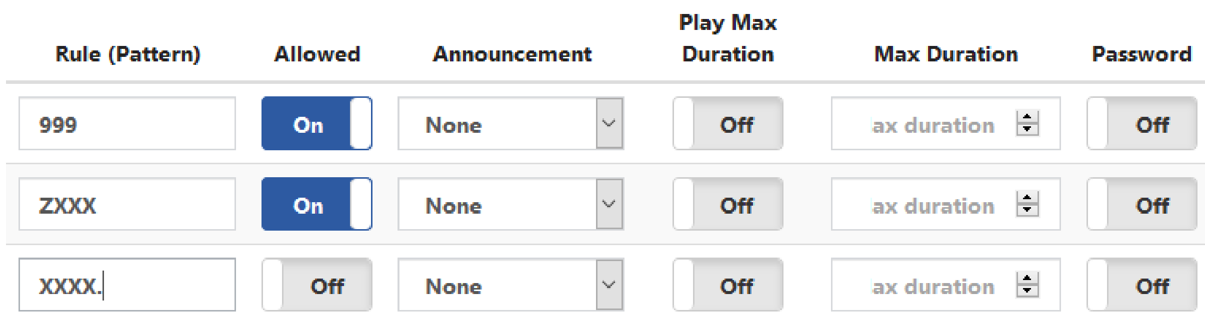
Feature Categories

Restrict users to only those feature codes that they require. Disable access to all other feature codes, as in the example below:



Dialing Restriction Rules

Create rules to limit dial access, where appropriate. For example, the following rule will allow uses to dial emergency services (999) and any 4-digit external number, but not any other external numbers. Dialing Restriction Rules do not affect dialing to internal destinations, such as extensions, feature codes, queues, etc.



Outbound Routes

When configuring Outbound Routes, take care to restrict dialing only to those destinations that you want to have access to. For example, if you do not want to allow international calling, make sure that the default access code (in some countries it may be 010) cannot be accessed.

It is recommended to define passwords (PIN) for any outbound routes that are used for International calls. It will significantly hamper intruders and make it more difficult for them to make such calls.

Creating extensions

Use strong passwords

Refer to Password Security section above for detailed information about extension passwords.

Control SIP and IAX2 Access

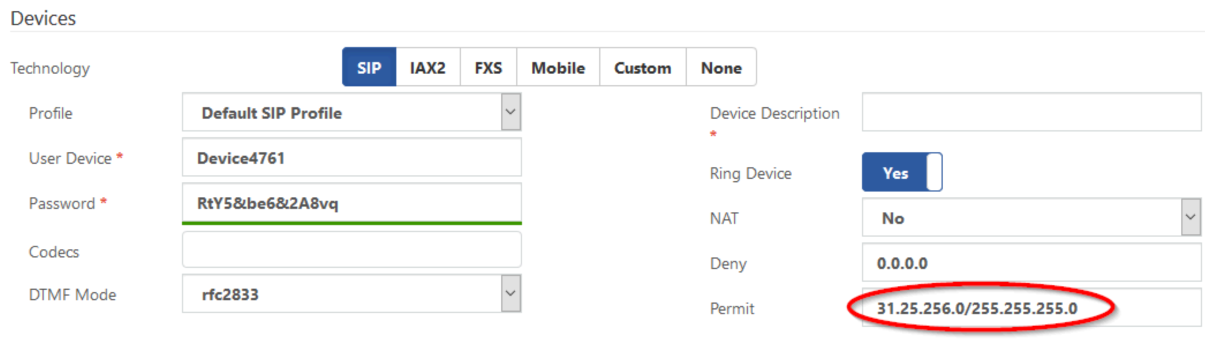
If you know the address that will be used by the SIP devices, make use of the access list to deny or permit access from specific IP addresses.

For example, if you know that a SIP extension will be assigned to a device that is installed on your local (internal) network, then you can define the following IP filter for this extension:

```
Deny: 0.0.0.0./0.0.0.0
Permit: 192.168.1.0/255.255.255.0
```

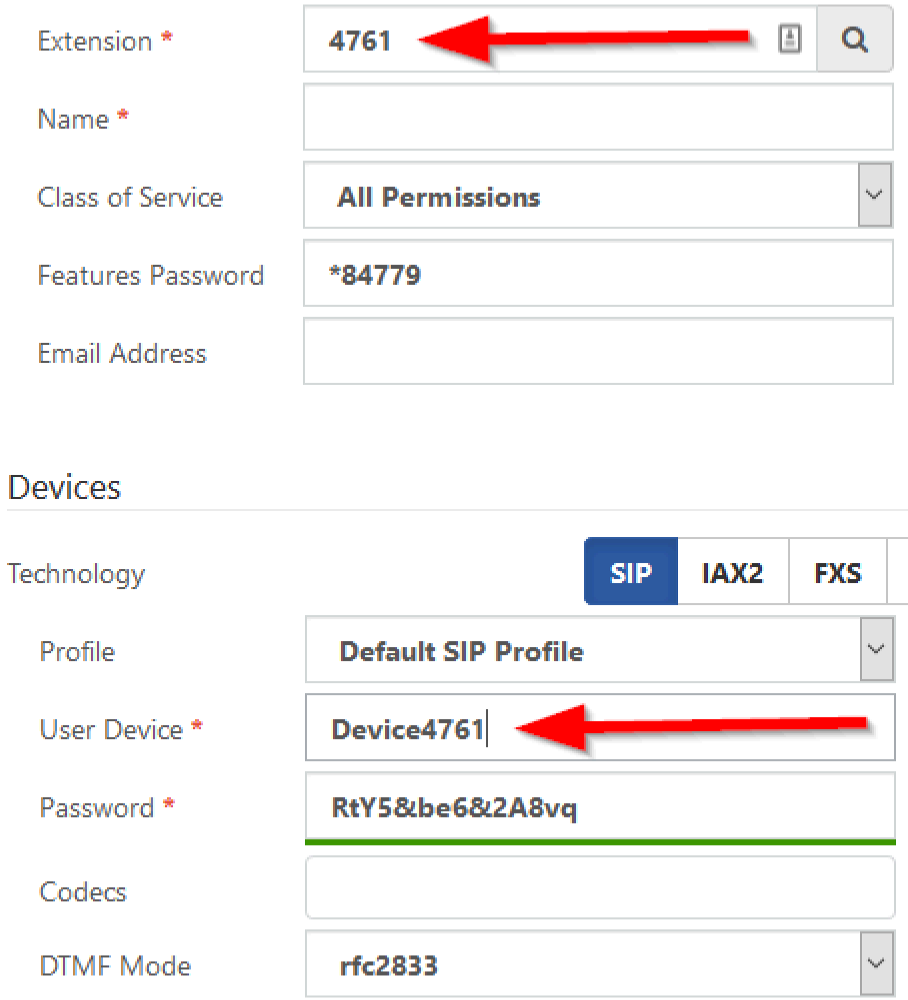
or

```
Deny: 0.0.0.0./0.0.0.0
Permit: 192.168.1.0/24
```



Device Names

When configuring extensions, avoid using the Extension number as the User Device. Using different values for these fields will provide additional protection for your SIP and IAX2 devices by making the device names impossible to guess.



Global SIP configuration

- Disable inbound calls from unknown sources. Navigate to Settings>Technology Settings>SIP Settings. Go to the Security tab and verify that the Allow Guest parameter is set to No.
- Make sure that CompletePBX 5 will reject invalid SIP requests with the same reject reason code, regardless of the real reason. This significantly hampers brute-force attackers as they receive no indication whether the extension exists, and makes it much more difficult to guess the SIP user name and secret.
  Navigate to Settings>Technology Settings>SIP Settings. Go to the **Security** tab and verify that the **Always Reject** parameter is set to **Yes**.

- Disable requests for domains that should not be serviced by CompletePBX 5. Navigate to the Custom tab of Settings > Technology Settings > SIP Settings, and define the following parameters in the Custom Options section:

  ```
  allowexternaldomains=no
  autodomain=yes
  ```

  If the system can receive external SIP calls, then it is possible that valid SIP requests will be made from domains that match the external IP address or host name. In this case, it is necessary to define this address in the 'domain' parameter. For example, if the external IP address is 110.222.53.94 and the DNS name is mycompany.com then you can define:

  ```
  domain=110.222.53.94
  domain=mycompany.com
  ```

- Verify the call limit for external SIP extensions is set to a low value – this is the factory default for CompletePBX 5.

Additional Documentation

Review the "Asterisk Security Threats and Best Practices" presentation located at https://files.xorcom.com/mktgdocs/presentations/protect-asterisk-pbx-webinar.pdf

Configuration Considerations

Numbering

You need to decide how many digits to use for extensions – do you want to use 3, 4, or more? You should take into account that most feature codes are 2 digits, so setting a system with 2-digit extensions is not really practical. Using more digits for extensions increases the difficulty for hackers to break into your system.

Avoid using 3-digit extensions – they are too easy to break. If you are implementing direct dialing, it is good practice to use the last 4 or 5 digits of the DID number as the extension number. For example, the extension that is externally accessed by dialing 773 215 3941 could be named as extension 3941 (in a 4-digit system) or 53941 (in a 5-digit system).

It will help you to navigate your system if you group similar functions together. For example, you could use the following ranges:

- 2000 - 3999 for extensions
- 8000 - 8999 for system-wide speed dialing
- 9100 - 9199 for ring groups
- 9300 - 9399 for queues
- 9400 - 9499 for conferences
- 9500 - 9599 for parking
- 9700 - 9799 for paging & intercom
- 9900 - 9999 for sundry functions such as voicemail broadcast groups

Dependencies

Destinations

Many dialogs in the PBX Menu Set are linked to a destination of one kind or another.

The following table shows which dialogs are available as destinations, and which dialogs *must* be terminated with a destination.

Dialog	Is a Destination	Destination is Mandatory
Announcements	✔	✔
Authorization Codes		
Blacklist		
Call Back	✔	✔
CID Modifiers		
Class of Service		✔
Conferences	✔	
Custom Applications	✔	✔
Custom Destinations	✔	
Customer Codes		
Dialing Restriction Rules		
DISA	✔	
Extensions	✔	
Extension Status		
Emergency		✔
Fax	✔	
Feature Categories		
Feature Codes		
Follow Me	✔	

Dialog	Is a Destination	Destination is Mandatory
Hot Desking		✔ (Devices only)
Inbound Routes		✔
IVR	✔	✔
Languages	✔	✔
Night Mode	✔	✔
Outbound Routes	✔	
Paging & Intercom	✔	✔ (Extensions only)
Parking	✔	✔
Pickup Groups		✔
Phonebook		
PIN Lists		
Queues	✔	✔
Queue Priorities	✔	✔
Queue VIPs		
Ring Groups	✔	✔
Route Selections		
Speed Dialing	✔	
Terminate Call	✔	
Time Conditions	✔	✔
Time Groups		
Trunks	✔	
Voicemail (Busy)	✔	
Voicemail (Direct)	✔	

Dialog	Is a Destination	Destination is Mandatory
Voicemail (Skip Greeting)	✔	
Voicemail (Unavailable)	✔	
Voicemail Broadcast Groups	✔	✔ (Extensions only)

Mandatory Fields and Dialog Dependencies

This table shows the dependencies between PBX Menu Set dialogs to help you optimize your workflow when setting up the system, as well as highlighting which fields are mandatory. The **Need to Know** column highlights information that you may need in order to complete the definition of the object. Items that are shown in brackets in the **Need to Know** column are optional.

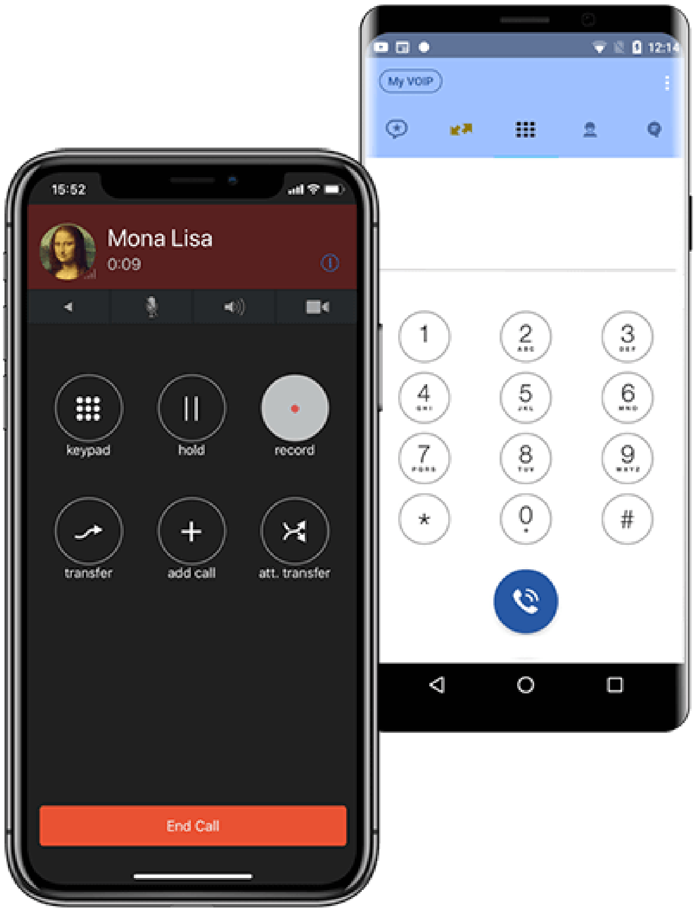
Dialog	Prerequisite Dialogs	Mandatory Fields	Need to Know
Announcements		Description Custom Recording Destination	
Authorization Codes		Code Alias Description Class of Service	
Blacklist		CID Number	
Call Back		Description Destination	
CID Modifiers		Description	
Class of Service	Feature Category Dial Restrictions Route Selection	Class of Service Description Last Destination Bad Destination	
Conferences		Code Description	

Dialog	Prerequisite Dialogs	Mandatory Fields	Need to Know
Custom Applications		Code Name Destination	
Custom Destinations		Name Number to Dial Class of Service	
Customer Codes		Customer Code Description	
Dialing Restriction Rules		Description	
DISA	Class of Service	Name Password	
Emergency		Number Destination	(Email list)
Extensions	Class of Service Technology Profile	Extension Name User Device Password Device Description	
Extension Status			
Feature Categories		Description	
Feature Codes			
Hot Desking	Technology Profile	User Device Password Device Description	
Inbound Routes		Description Inbound Destination	Routing Method

Dialog	Prerequisite Dialogs	Mandatory Fields	Need to Know
IVR	Class of Service	Description Invalid Destination Timeout Destination Entries	(Welcome Message) (Keys to press and destinations)
Languages		Name Description Destination	
Night Mode		Toggle Code Description Destination when Disabled Destination when Enabled	
Outbound Routes	Trunk	Description Trunks Dial Patterns	(CID Name) (CID Number)
Paging & Intercom		Code Description Extensions	Extension/s
Parking		Code Description	
Phonebook		Description	File of numbers to be imported
Pickup Groups		Description Extension	Extension/s
PIN Lists		Description	Password
Queue Priorities		Description Destination	
Queue VIP		Description VIP List	

Dialog	Prerequisite Dialogs	Mandatory Fields	Need to Know
Queues		Code Description Last Destination	
Ring Groups		Code Description Extensions Ring Time Last Destination	
Route Selections	Outbound Route	Description	(Time Group)
Speed Dialing		Speed Dial Code Description Destination Number	
Terminate Call			
Time Conditions	Time Group	Description Time Group Destination on match Destination no match	
Time Groups		Description	
Trunks		Description Ring Time	Security (for SIP) Security (for IAX2) Channel Group (for DAHDi)
Voicemail			
Voicemail Broadcast Group		Code Description Extensions Password	Extension/s

2. CloudPhone



The Xorcom CloudPhone allows you to configure a softphone on your iOS or Android mobile device, as well as Windows or Mac desktops.

The Xorcom CloudPhone app is free to download from Google Play or the Apple App Store.

Xorcom CloudPhone requires a license on the CompletePBX 5 system.

CloudPhone Mobile and Desktop apps can be configured as hot-desking devices. This means that users can log in to any available CloudPhone device (mobile or desktop) and have their extension and settings automatically applied. This is ideal for flexible work environments where employees don't have dedicated desks.

Xorcom CloudPhone provides seamless provisioning and central management for all devices, including SNMP monitoring and compatibility with IDS PMS.

The Xorcom CloudPhone gives the user all the features of CompletePBX 5, including making and receiving calls, feature codes, hold and call transfer, conferencing, BLF functionality and more.

In addition, Xorcom CloudPhone offers one-on-one and group chat within the organization, personal favorite management, voicemail notifications, call log history, and contacts sync with the local phonebook.

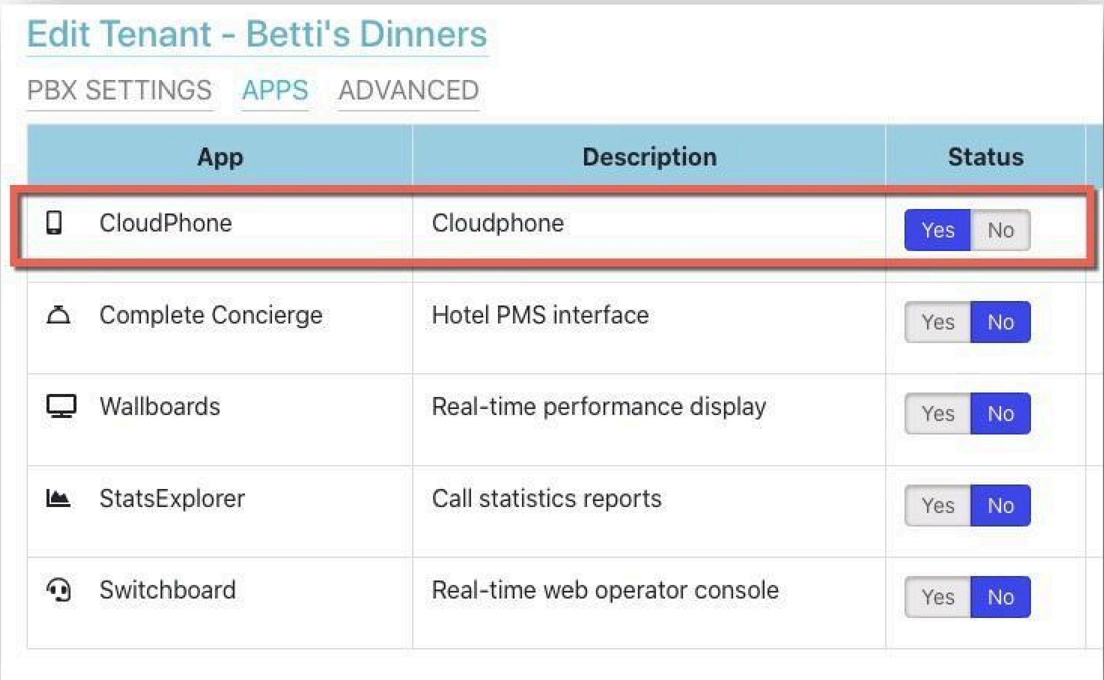
CloudPhone License

You will need to purchase a Xorcom CloudPhone license, either from the Licensing Portal or by a direct order from Xorcom. There are three license types:

- **Dynamic license for MT Manager (P/N LC0506)** – this is a pay-as-you-go license that allows the administrator to create licenses on-the-go and pay per usage.
- **Dynamic license for MT Manager hosted on Xorcom Cloud (P/N LC0555)** – this license is similar in functionality to the previous license.
- **Annual license for CompletePBX (P/N LC0106)** – this license type allows the purchasing of a fixed quantity of users in advance.

License Activation for MT Manager

1. Make sure that MT Manager is running version 1.0.22, or better.
2. Purchase a license for Xorcom CloudPhone.
3. Install and activate the CloudPhone license
4. Navigate to the Tenants dialog, and click on the Edit icon for the selected tenant In the Apps tab, change the status of CloudPhone to **Yes**.



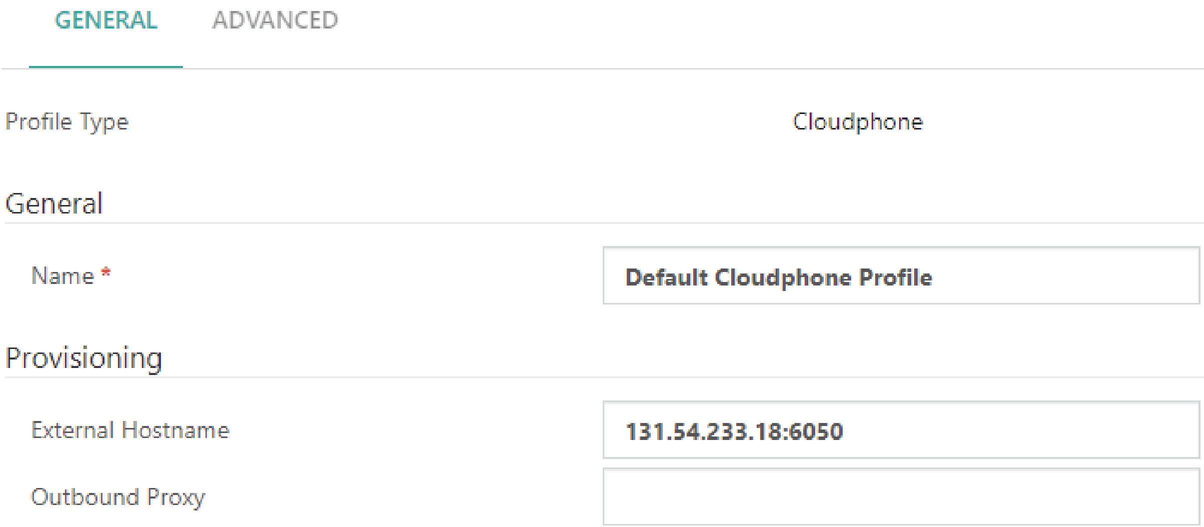
5. Read and accept the comments in the pop-up window
6. Click **Save** at the bottom of the dialog

License Activation for a Standalone System

1. Make sure that CompletePBX 5 is running version 5.1.7, or better
2. Purchase a license for Xorcom CloudPhone.
3. Install and activate the CloudPhone license, by running the command
    a. **xlic register <license-code>**
4. After you have been issued with a CloudPhone license, go to the Admin>Licenses>License Status dialog and press the **Update** button. This will display your newly issued CloudPhone license.

Configure CloudPhone in CompletePBX 5

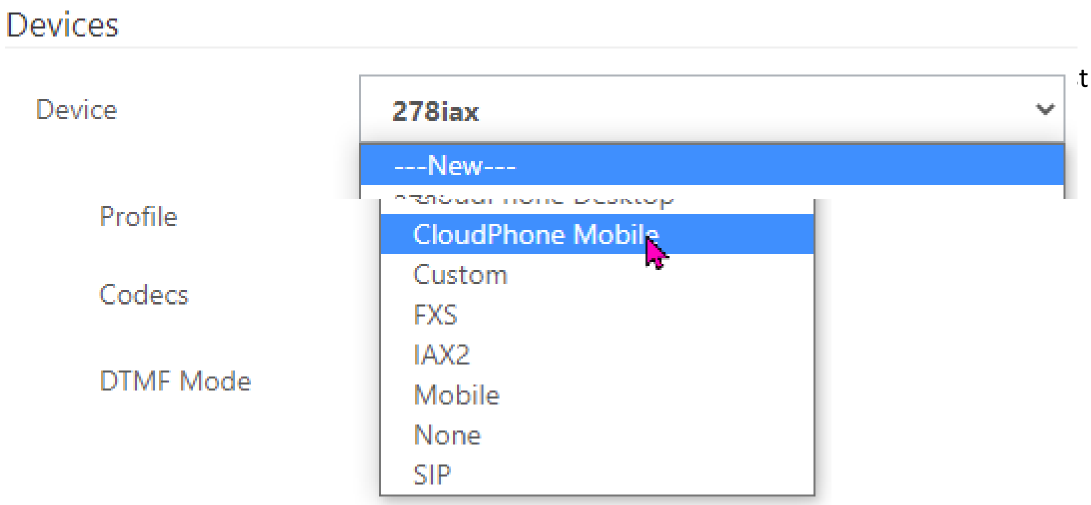
1. In the Settings > Endpoint Manager > Host Settings dialog, change the Hostname for the Default host to the actual IP address of your CompletePBX 5 system, and press the **Save**



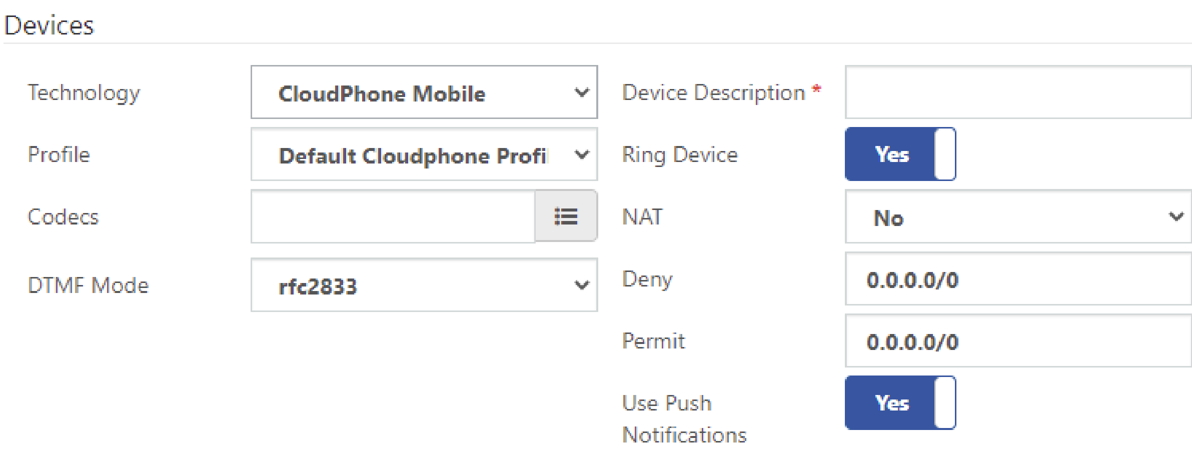
2. Configure the email settings in the [Settings>Endpoint Manager>CloudPhone](#) dialog. Navigate to the Mobile Email Settings or Desktop Mail Settings tab, and configure the message that you want to send to users to notify them to install the CloudPhone app on their mobile device or desktop.
3. In the Settings > Endpoint Manager > CloudPhone dialog, navigate to the QR Codes tab. Press the **Add Extensions** button to create a list of extensions for which you want to enable the CloudPhone app. After you have completed compiling the list, press on the **Resend QR Codes and Passwords** button.
4. See **Configuring a Mobile Device** or **Creating a CloudPhone Desktop Device** below for the next steps

Configuring a Mobile Device

1. Navigate to the PBX>Extensions>Extensions dialog, and select the extension to which you want to add a mobile CloudPhone.
2. Make sure that a valid email address is defined in the **Email Address** field for the extension. (This will be needed in order to send the setup instructions to the user.)



5. Modify parameters, such as Device Description (mandatory) and NAT (if the mobile device is not located on the same network as the CompletePBX 5 system.)



6. Press **Update** to save the changes.
7. Navigate to Settings>Endpoint Manager>CloudPhone dialog, and select the QR Codes and Passwords tab. Press on the **Add Extensions** button so that you can select the extension to which you are adding the CloudPhone device from the drop-down list, and click on **Resend QR Codes and Passwords**. The extension user will receive an email explaining the installation process, containing a link to Google Play and the Apple App Store, and a QR code to link the mobile device to CompletePBX 5, like the following example:.

```
Congratulations, your CloudPhone is ready.
To install and start making calls, please download the app to your device:

iOS - https://apps.apple.com/us/app/xorcom-cloudphone/id1496782778
Android - https://play.google.com/store/apps/details?id=com.xorcom.cloudphone.android

After installing the app, just open it and scan the QR code below.
Make sure to have internet connection when you do that.
```

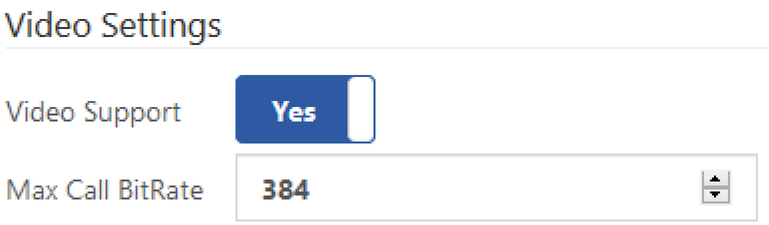
qr_code.png

The user should use the link from the email to navigate to either Google Play or the Apple App Store, and install the Xorcom CloudPhone app.

During the installation, the app will ask the user to provide the QR Code that they received in the email.

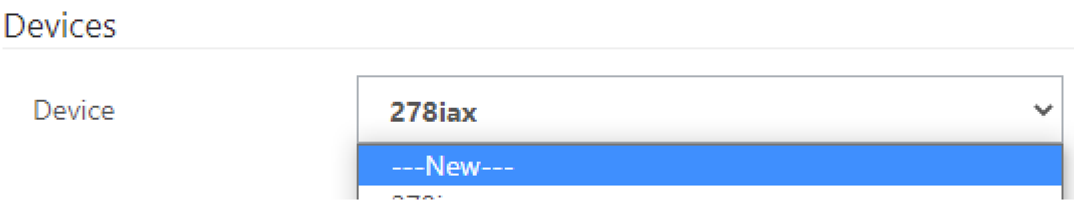
Installation and Activation is now complete!

By default, video is not activated for the Xorcom CloudPhone. If you want to allow video calls, go to Settings > Technology Settings > SIP Settings, and enable video support in the Video Settings section:

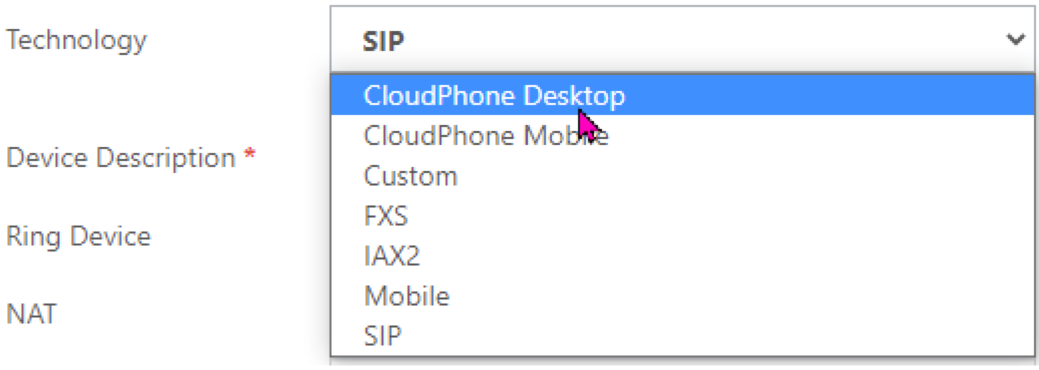


Creating a CloudPhone Desktop Device

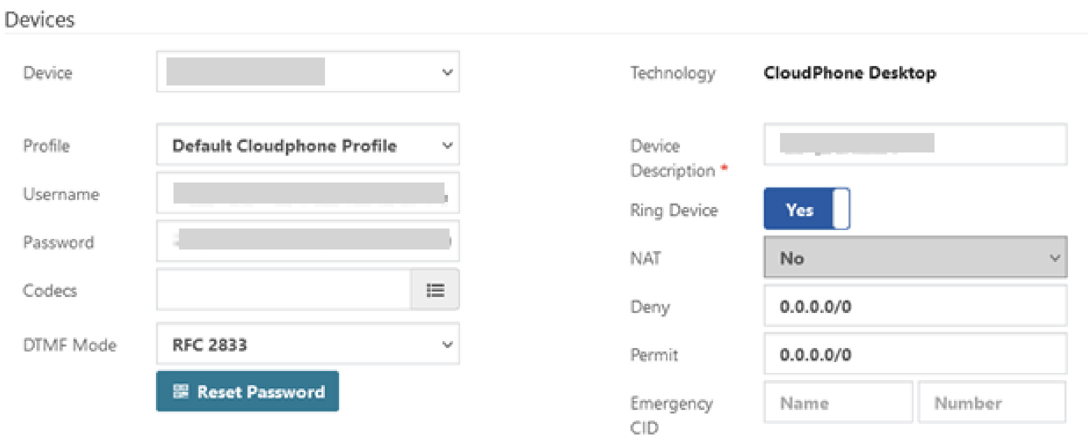
1. Navigate to the PBX>Extensions>Extensions dialog, and select the extension to which you want to add a desktop CloudPhone.
2. Make sure that a valid email address is defined in the **Email Address** field for the extension. (This will be needed in order to send the setup instructions to the user.)
3. In the **Devices** section, go to the Device field and select **New**



4. Go to the **Technology** field, and select CloudPhone Desktop from the drop-down list



5. Modify parameters, such as Device Description (mandatory) and NAT (if the desktop is not located on the same network as the CompletePBX 5 system.)
6. Press **Update** to save the changes.
7. Now, in the Device section, you can view and copy the username and password for CloudPhone Desktop.



8. Navigate to Settings>Endpoint Manager>CloudPhone dialog, and select the QR Codes and Passwords tab. Press on the **Add Extensions** button so that you can select the extension to which you are adding the CloudPhone device from the drop-down list, and click on **Resend**

QR Codes and Passwords. The owner of the extension will receive an email detailing the installation and setup process, like the following example:

```
Congratulations, your CloudPhone Desktop account is ready.
To install and start making calls, please download the app to your
device:

Windows - https://updates.xorcom.com/servers/cphone/cphone-win-latest.exe
MacOC - https://updates.xorcom.com/servers/cphone/cphone-mac-latest.dmg

After installing the app, copy and paste the credentials below.
Make sure to have internet connection when you do that.

Username: bf4924019fd0904afd6e12
Password: 22e79f2266dd283f125b.
```

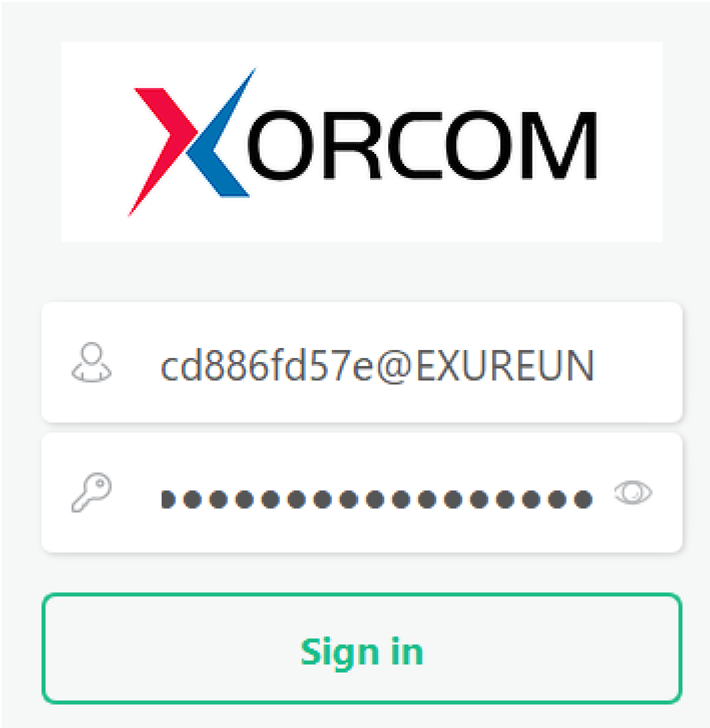
Installing CloudPhone Desktop on Windows

The user will receive an email, including a link to download an executable file.

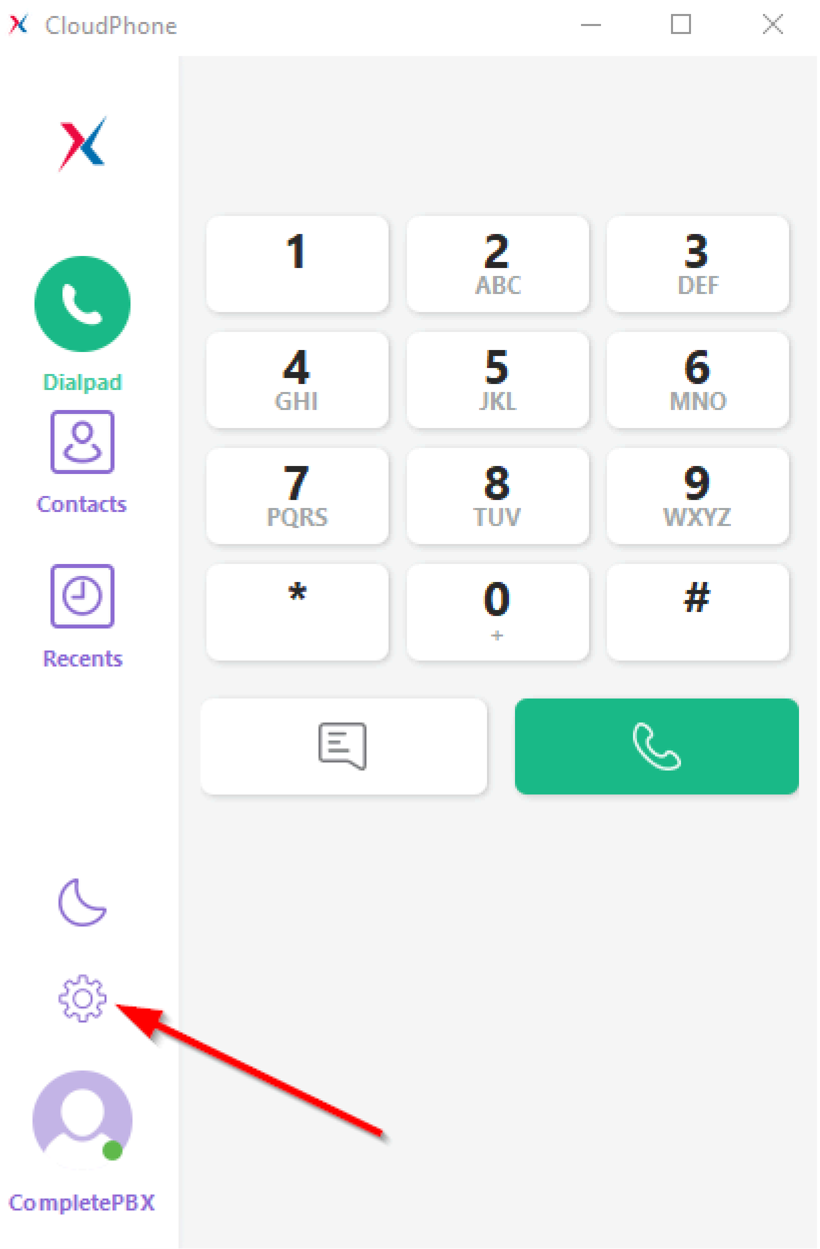
The user should now copy the link from the email to their internet browser to download the executable file.

After the download has finished, the user should click on the downloaded executable file and follow the instructions for the installation process.

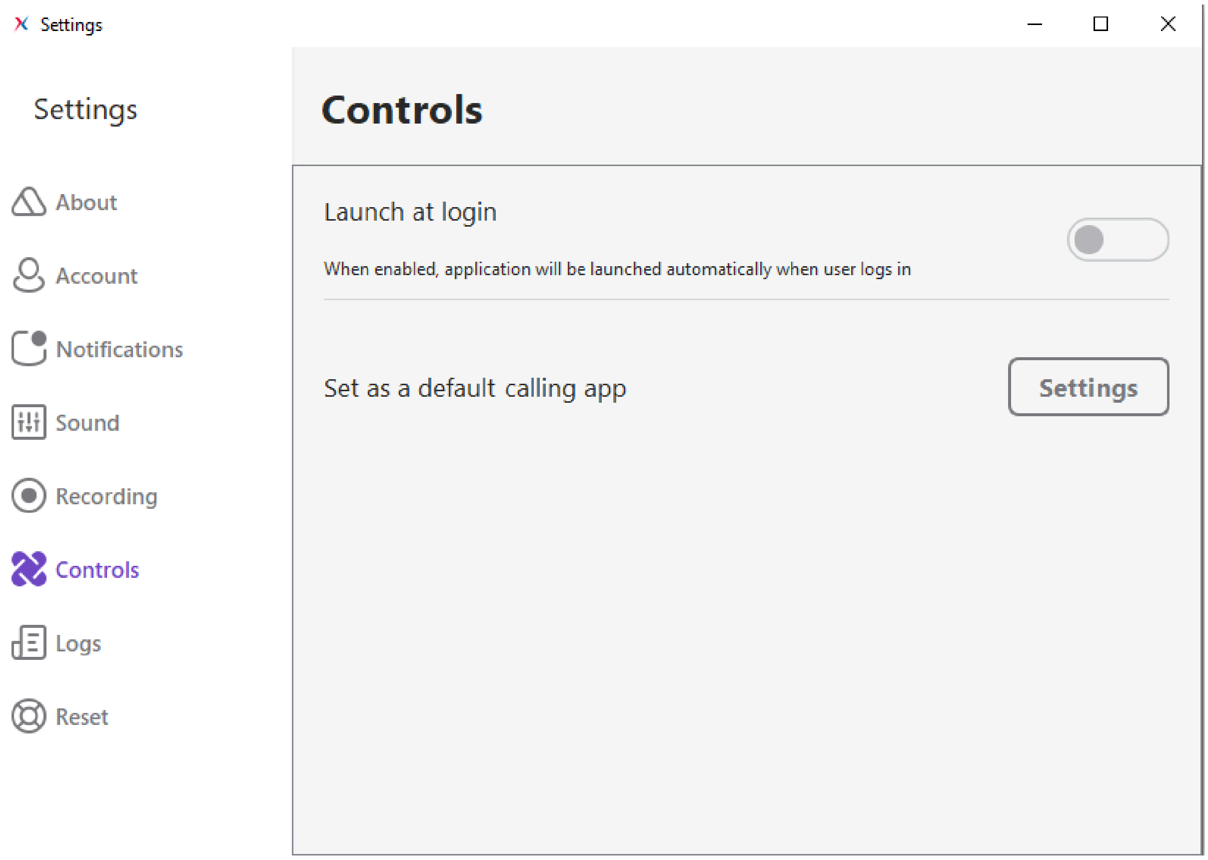
After the installation is complete, the user should start the CloudPhone application and enter the security information from the email that they received, and press on **Sign in**.



The CloudPhone interface will now be displayed



You can use the Settings icon (that the red arrow is pointing to in the above screen grab) to configure the Desktop CloudPhone. You may want to check the Controls menu to configure the application to launch when you login to your PC.

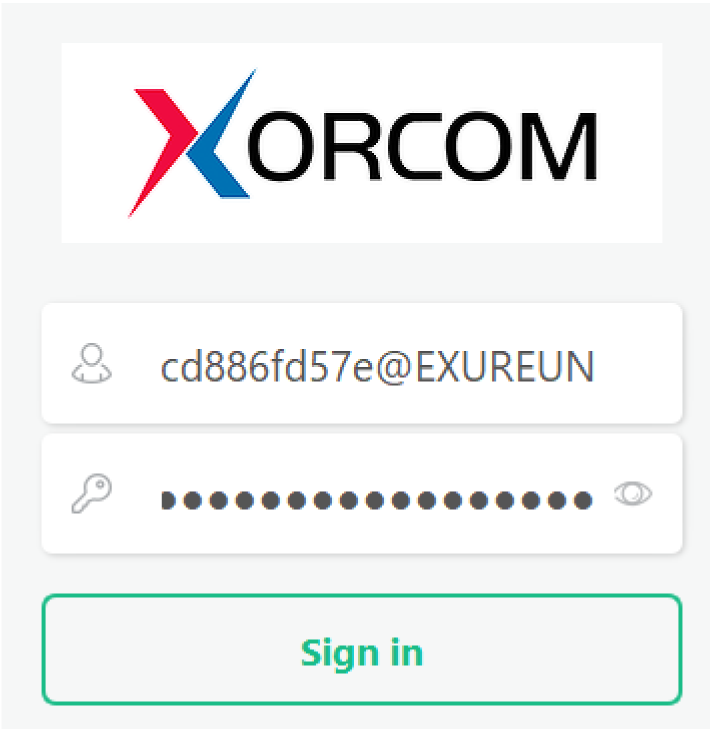

Settings
Settings
About
Account
Notifications
Sound
Recording
Controls
Logs
Reset
Controls
Launch at login
When enabled, application will be launched automatically when user logs in
Set as a default calling app
Settings

Installing CloudPhone Desktop on Mac

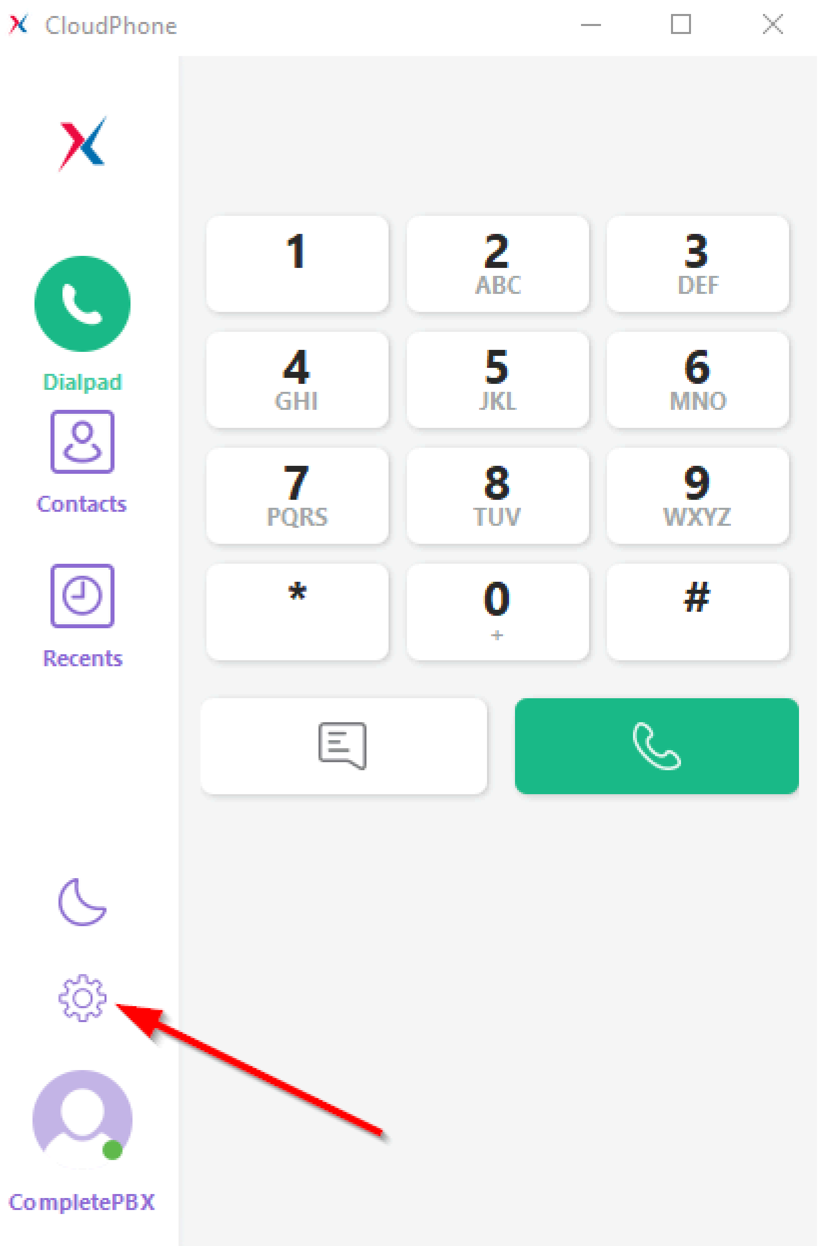
The user will receive an email, including a link to download an installation package. Click on the link from the email that you received, and wait for the download to finish.

When the download is complete, click on the downloaded file to open the installation package. Copy the CloudPhone.app file to your Applications folder.

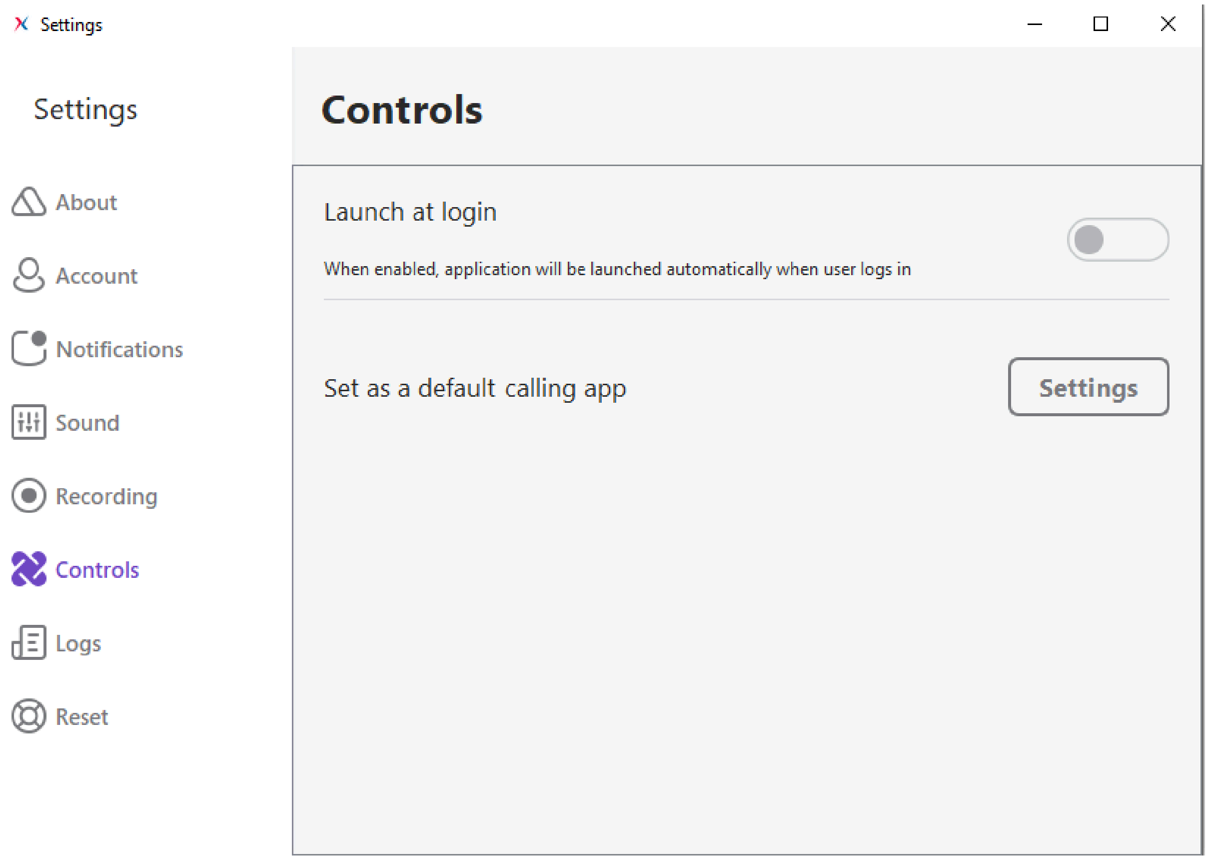
After the installation is complete, start the CloudPhone application and enter the security information the email that you received, and press on **Sign in**.



The CloudPhone interface will now be displayed



You can use the tool icon (that the red arrow is pointing to in the above screen grab) to configure the Desktop CloudPhone. You may want to check the Controls menu to configure the application to launch when you login to your PC.


Settings
Settings
About
Account
Notifications
Sound
Recording
Controls
Logs
Reset
Controls
Launch at login
When enabled, application will be launched automatically when user logs in
Set as a default calling app
Settings

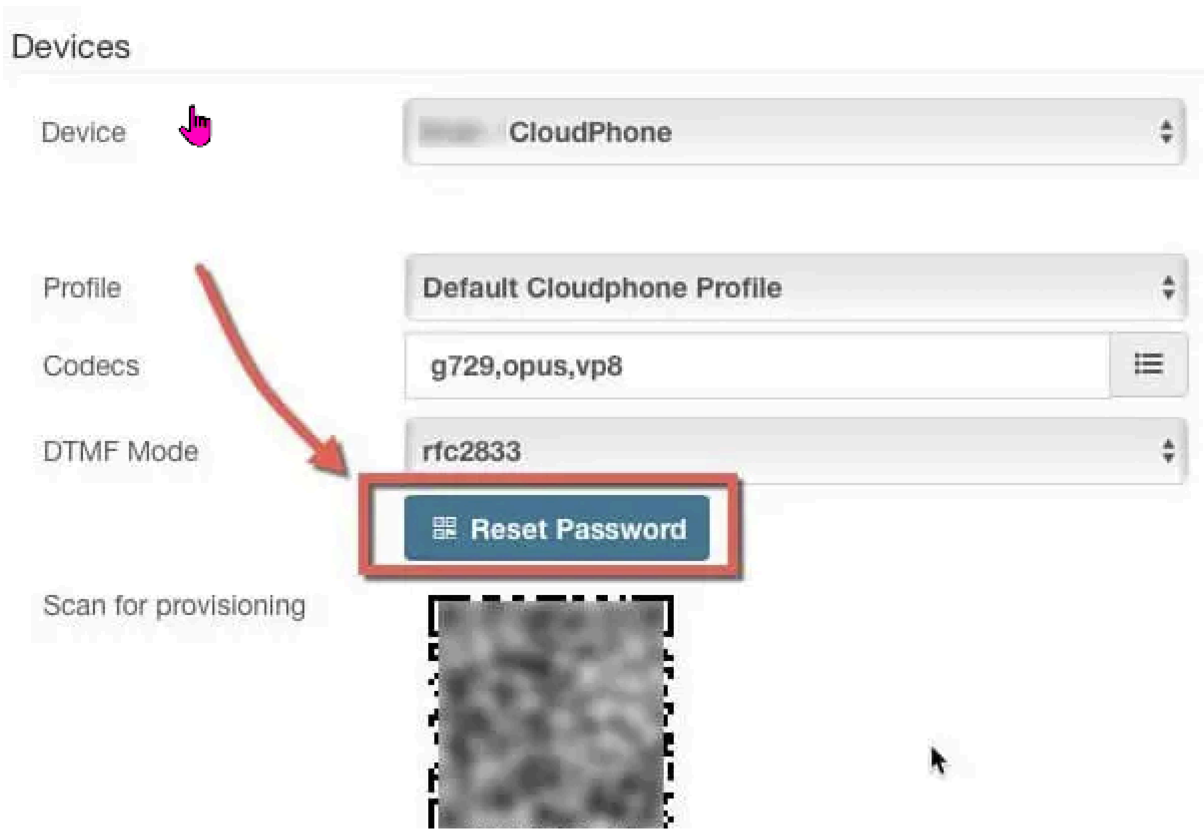
Resetting a CloudPhone Device

If you want to allocate a CloudPhone device to another user, navigate to the **General** tab of the PBX>Extensions >Extensions dialog and update the email address for the extension. In the **Devices** section, select the CloudPhone device and click on the **Reset Password** button. This will perform the following steps:

- Unregister the CloudPhone device from CompletePBX
- Reset SIP password for the CloudPhone device
- Reset the QR code for the CloudPhone device
- If the email address field for the extension is populated, the CloudPhone device will be re-registered in CompletePBX
- An email will be sent to the address associated with the extension with the new QR code.

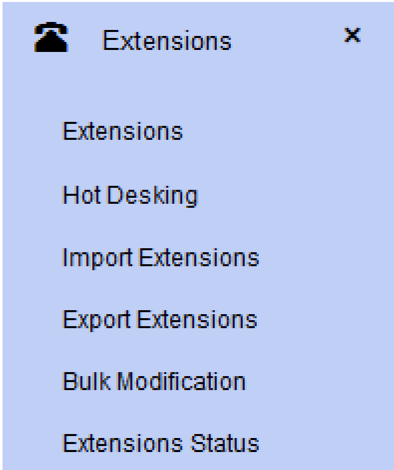
If you use **Reset Password** when you are keeping the extensions settings, but are allocating the device to a new employee, make sure to first update the email address of the extension, and only then reset the password so that the new QR code will not be sent to the old address.

You can forcibly remove a CloudPhone device from CompletePBX by clearing out the Email Address filed and clicking on the **Reset Password** button in the **Device** section.


Devices
Device
CloudPhone
Profile
Default Cloudphone Profile
Codecs
g729,opus,vp8
DTMF Mode
rfc2833
Reset Password
Scan for provisioning

3. PBX Menu Set

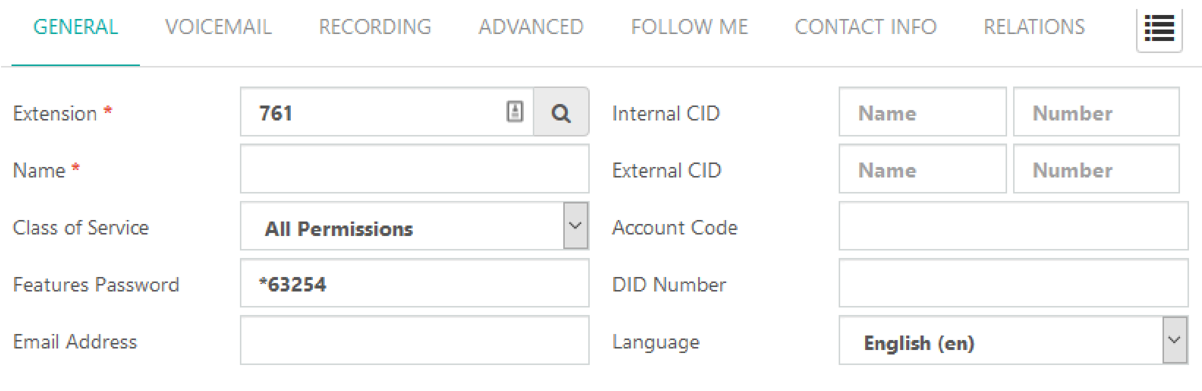
Extensions Menu Group



Extensions Dialog

This dialog allows you to configure extensions (users) and devices (telephones) in your system.

GENERAL Tab



Extension*, the internal number you dial in order to reach the 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 can be changed after the extension has been saved, by simply editing the Extension field. Changing the extension will automatically modify all usage of the extension number as a CompletePBX destination (such as Ring Groups, Queues, IVRs, etc.), except in manually populated fields, such as Follow Me.

Name*, a free-text name to identify the extension. This could be the name of the user, e.g. Fernando Alonso; the location of the extension, e.g. Server Room; or could simply be the extension number, e.g. 2941. This value will be displayed as the Caller ID text for any calls placed from the extension to other users or devices on the PBX (unless the Internal CID field contains a value.)

Class of Service, the dial plan is 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. The system 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 system features that are password-protected.

Email Address, valid email address that can be used when sending voicemail to email, or for receiving faxes. If voicemail is enabled for the extension and a valid email address is entered in this field, any time a voicemail is left for the extension an email message will be sent to the address entered here. By default, the message will simply notify the user that a new message has been left for them. This address is also used if the extension is Fax Enabled, and Fax to Email is enabled.

Only one address can be entered into this field.

Internal CID, internal Caller ID for the extension, consisting of two parts: the CID Name and the CID Number. These will define the caller ID text that is displayed when this user calls other (internal) users on the same PBX. This could be useful 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 populate the 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 useful 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 can only be implemented if your trunk service provider supports setting the Caller ID.

The number must be in the same format that is used for the DID number. In countries where the area code starts with a zero, the leading zero should be removed. For example, if the number that people dial to reach you is 01762465869, the external CID Number should be 1762465869, and the DID Number should also be 1762465869.

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 populate the Caller ID name text.

Account Code, this field can be used to populate the account code field of the Call Detail Record **(**CDR). This can be useful for billing purposes, by allowing multiple extensions to be all billed to the same cost center. Of course, you will need to ensure that your billing software supports this feature.

The Account Code field may consist on any combination of numbers and letters.

If this field is left blank, the account code field of the CDR record will also be blank.

DID Number, the direct inward dial (DID) number for incoming calls, i.e. the inbound route that should be associated with this extension.

In countries where the area code starts with a zero, the leading zero should be removed. For example, if the number that people dial to reach you is 01762465869, the DID Number should be 1762465869.

Language, specifies the language to be associated with this extension. This will force all prompts specific to this extension to be played in the selected language, provided that

- the language is installed on your server
- voice prompts for the specified language exist on your server.

If the field is left blank, all prompts will be played in the default language of the system.

Devices Section

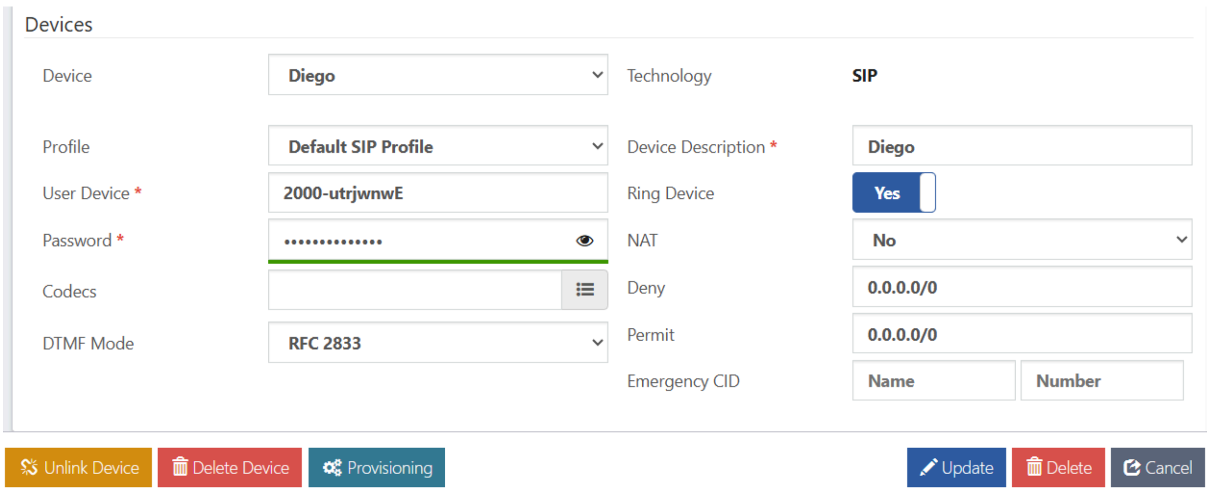
This section allows you to configure the device that is linked to the extension.

Technology, indicates the type of technology to be associated with this device. The technology options are:

- **CloudPhone Desktop**
- **CloudPhone Mobile**
- **Custom**
- **FXS** analog devices (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)
- **IAX2** (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)
- **Mobile**
- **None**
- **SIP**
- **Teams Connector (NOTE** that this option is only available with an active Teams Connector license)

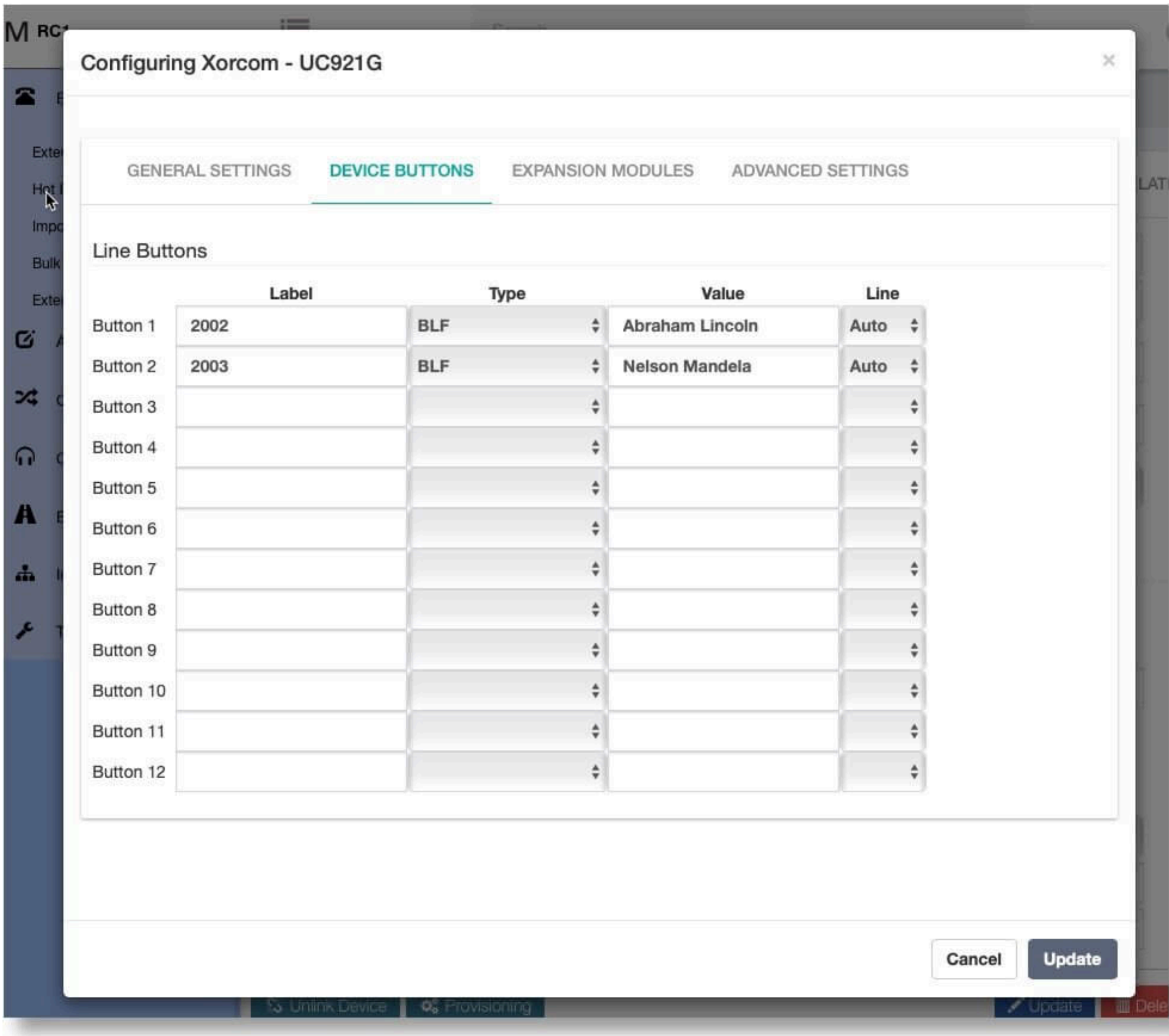
Profiles can be defined for the technology types in the Settings>Technology Settings>Profiles dialog.

IP Phone Provisioning available for IP phone devices:



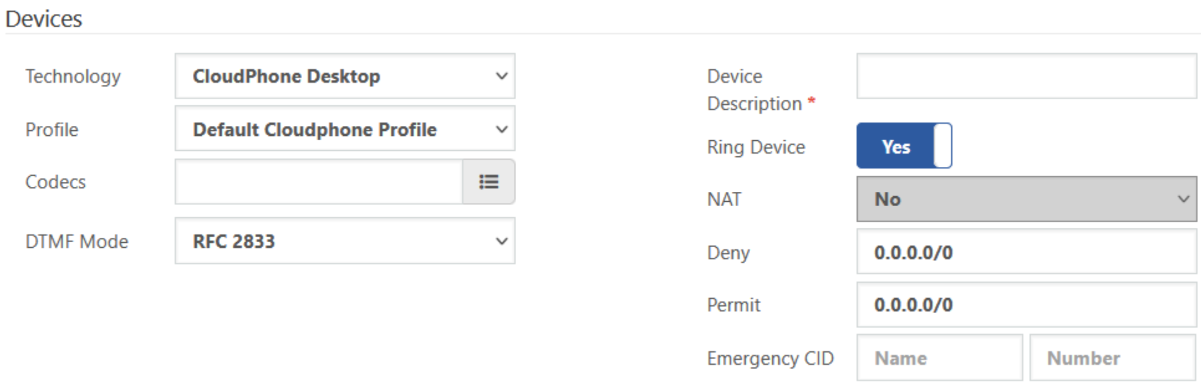
- **NOTE** that it is possible to delete a device directly from the Extension dialogue, without unlinking it first.

- The provisioning buttons will open all the provisioning options for that device, as found in Settings -> Endpoint Manager -> Templates. This allows the admin or user to edit Device Buttons, Expansion Modules, and Advanced Settings for that specific device.

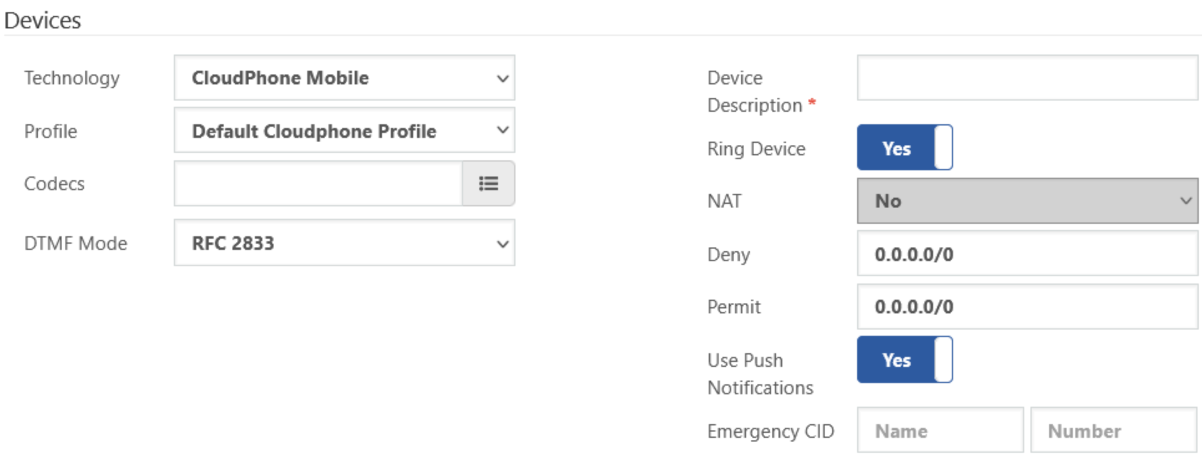


- Users do not need to have permissions to Endpoint Manager to edit these parameters.
- **NOTE** that the phone must first be associated with the extension in Endpoint Manager, and only after that it can be accessed via the Provisioning button in the Device or User Portal.

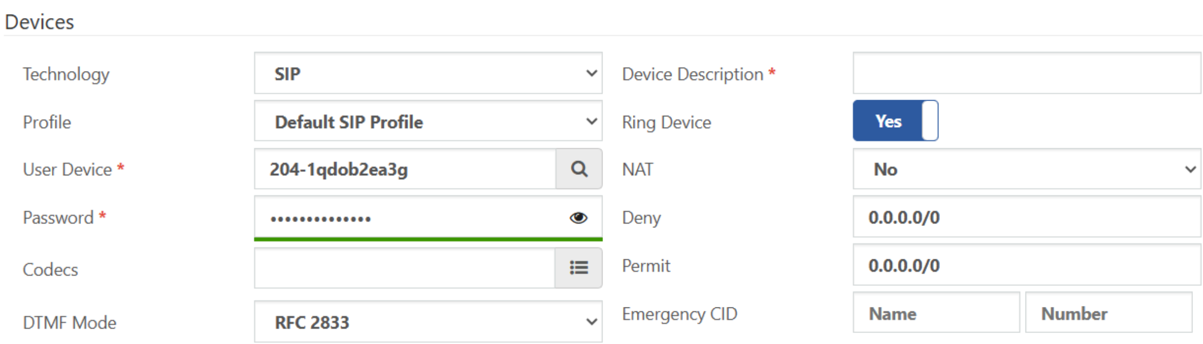
CloudPhone Desktop



CloudPhone Mobile



SIP Option



Profile, technology profile settings associated with the device. There must be at least one (default) profile that defines common attributes to be associated with the Technology. You can configure these profiles in the Settings>Technology Settings menu group.

User Device*, the username that will be used when registering the device. By default, it is populated with a randomized, hard-to-guess name when creating new extensions.

Password*, password (secret) associated with the device. Passwords can be the weakest link of 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.

If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password.

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 touchtones will be transmitted to the other side of the call. The default value is rfc2833. Other options available in the drop-down list 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 it is available, otherwise use in-band option

Device Description, a short (optional) free-text description to identify the device. It is used by to populate the description field in the Peers tab of the Reports>PBX Reports>Status dialog.

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

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 external internet. Private addresses are in the following ranges:

- 10.0.0.1 - 10.255.255.254 – which can also be written as 10.0.0.0/8
- 172.16.0.1 - 172.31.255.254 – which can also be written as 172.16.0.0/12
- 192.168.0.1 - 192.168.255.254 – which can also be written as 192.168.0.0/16

NAT options can be selected from the drop-down list:

- **No** - no special NAT handling other than RFC3581
- **Force** - pretend there is a rport parameter even if there is not
- **Comedia** - send media to the same port that Asterisk received it from, regardless of where the SDP says to send it.

- **Force,Comedia** - combines both Force and Comedia options
- **Auto Force** - set the force rport option if Asterisk detects NAT
- **Auto Comedia** - set the comedia option if Asterisk detects NAT

NAT is always set to **No** in multi-tenant systems, and no other option can be configured.

Deny, in a user/peer definition, allows you to limit SIP traffic to and from the peer to one or more specific IP addreses or networks. This option should be in the format of an IP address and subnet.

- 192.168.25.10/255.255.255.255 denies traffic for the extension from the specific IP address
- 192.168.25.10/32 denies traffic for the extension from the specific IP address
- 192.168.1.0/255.255.255.0 denies traffic for the extension from all IP addresses in the range of 192.168.1.1 to 192.168.1.254
- 0.0.0.0/0.0.0.0 denies access from all networks by default. Note that you can specify which networks can have access by specifying them in the Permit field
- You can define multiple addresses by separating each address with the "," (comma) symbol, i.e. 192.168.0.0/24,192.168.6.0/24

Deny 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, the system will not block traffic for the peer from any IP address.

Permit, in a user/peer definition, allows you to limit SIP traffic to and from the peer to one or more specific IP addresses, or networks.

- 192.168.10.0/255.255.255.0 allows traffic from any address on the 192.168.10.x network
- 192.168.10.0/24 allows traffic from any address on the 192.168.10.x network
- 192.168.10.10/32,192.168.10.20/32 will allow traffic from either 192.168.10.10 or 192.168.10.20
- You can define multiple addresses by separating each address with the "," (comma) symbol, i.e. 192.168.0.0/24,192.168.6.0/24

The Permit field is the opposite of the deny field. Specific IP addresses or networks can be added in this field to allow traffic to access this extension from the specified IP address or network.

This field is not mandatory. If it is left blank, traffic will be allowed from all IP addresses. Strengthen your system security by using the Deny and Permit fields. If the endpoint is static, we strongly recommend that you make proper use of the Permit and Deny fields 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.

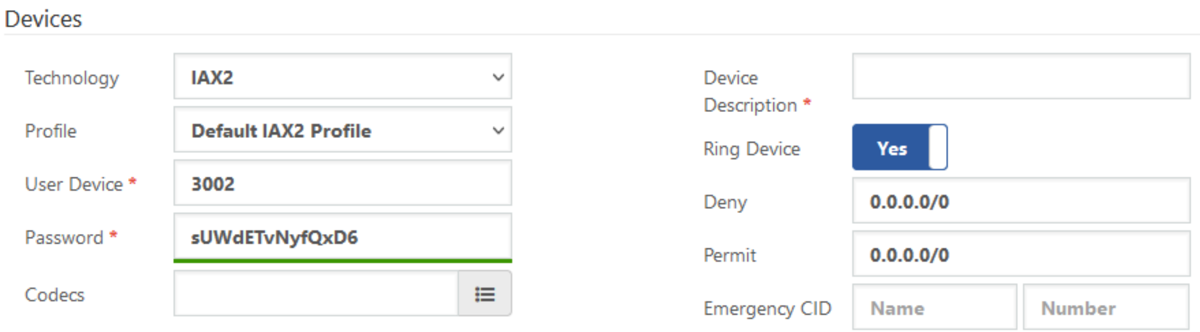
Emergency CID allows for the creation of a special emergency caller ID per device, consisting of two parts: the **Emergency CID Name** and the **Emergency CID Number**. The **Emergency CID Name** is a descriptive field used to provide crucial location information (e.g., "RM 101, Building A, Main St"), which is transmitted as the caller ID name during an emergency call. The **Emergency CID Number** is the specific phone number assigned for direct callback to that exact device.

This mechanism is essential for aiding emergency responders by allowing them to quickly identify the location of the caller and to call back directly if the call is disconnected. The Emergency CID is configured at the device level and on the extension, as a single extension may have devices in different physical locations.

When an emergency call is placed from a device with a configured Emergency CID, the specified name and number are sent to emergency services. Importantly, creating an Emergency CID automatically generates a corresponding DID number. **NOTE** that emergency responders to directly call back the Emergency CID Number and reach the physical device that originated the call, bypassing normal PBX behaviors such as extension routing, voicemail, or busy signals. This direct line capability is critical for confirming the emergency and accurately locating the caller.

IAX2 Option

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)



Profile, determines the technology profile settings for the device. There must be at least one (default) profile that defines common attributes to be associated with the technology. You can configure these profiles in the Settings->Technology Settings->Profiles menu**.**

User Device*, the username that will be used when registering the device. By default, this is set to the extension number, but you can improve security of your system by using text in this field.

Password*, password (secret) associated with the device. Passwords can be the weakest link of 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.

If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password.

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) free-text description to identify the device. It is used by to populate the description field in the Peers tab of the Reports>PBX Reports>Status dialog.

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

Deny, in a user/peer definition, allows you to limit SIP traffic to and from the peer to a specific IP address or network. This option should be in the format of an IP address and subnet.

- 192.168.25.10/255.255.255.255 denies traffic for the extension from the specific IP address
- 192.168.25.10/32 denies traffic for the extension from the specific IP address
- 192.168.1.0/255.255.255.0 disallows traffic for the extension from all IP addresses in the range of 192.168.1.1 to 192.168.1.254
- 0.0.0.0/0.0.0.0 denies access from all networks by default. Note that you can specify which networks can have access by specifying them in the Permit field
- You can define multiple addresses by separating each address with the "," (comma) symbol, i.e. 192.168.0.0/24,192.168.6.0/24

Deny 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, the system will not block traffic for the peer from any IP address.

Permit, in a user/peer definition, allows you to limit SIP traffic to and from the peer to a specific IP address, or network.

- 192.168.10.0/255.255.255.0 allows traffic from any address on the 192.168.10.x network
- 192.168.10.0/24 allows traffic from any address on the 192.168.10.x network
- 192.168.10.10/32,192.168.10.20/32 will allow traffic from either 192.168.10.10 or 192.168.10.20

You can define multiple addresses by separating each address with the "," (comma) symbol, i.e. 192.168.0.0/24,192.168.6.0/24

The Permit field is the opposite of the deny field. Specific IP addresses or networks can be added in this field to allow traffic to access the extension from the specified IP address or network.

This field is not mandatory. If it is left blank, traffic will be allowed from all IP addresses. Strengthen your system security by using the Deny and Permit fields. If the endpoint is static, we strongly recommend that you make proper use of the Permit and Deny fields 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.

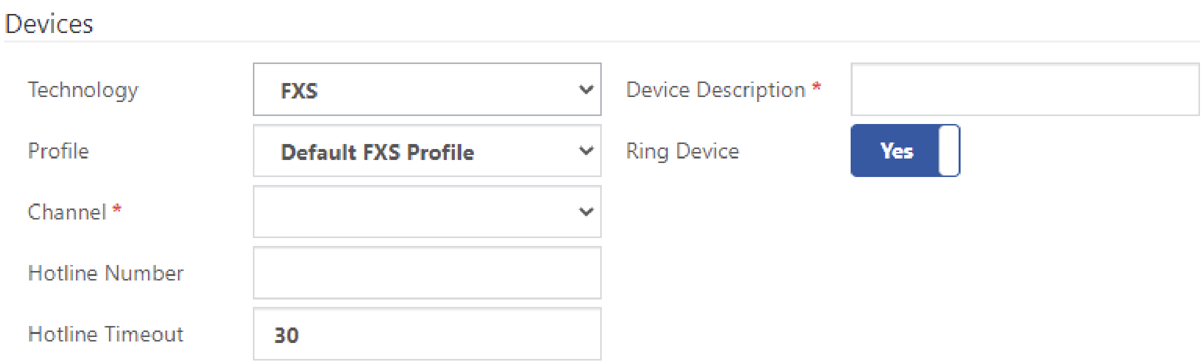
Emergency CID allows for the creation of a special emergency caller ID per device, consisting of two parts: the **Emergency CID Name** and the **Emergency CID Number**. The **Emergency CID Name** is a descriptive field used to provide crucial location information (e.g., "RM 101, Building A, Main St"), which is transmitted as the caller ID name during an emergency call. The **Emergency CID Number** is the specific phone number assigned for direct callback to that exact device.

This mechanism is essential for aiding emergency responders by allowing them to quickly identify the location of the caller and to call back directly if the call is disconnected. The Emergency CID is configured at the device level and on the extension, as a single extension may have devices in different physical locations.

When an emergency call is placed from a device with a configured Emergency CID, the specified name and number are sent to emergency services. Importantly, creating an Emergency CID automatically generates a corresponding DID number. **NOTE** that emergency responders to directly call back the Emergency CID Number and reach the physical device that originated the call, bypassing normal PBX behaviors such as extension routing, voicemail, or busy signals. This direct line capability is critical for confirming the emergency and accurately locating the caller.

FXS Option

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)



Profile, technology profile settings associated with the device. There must be at least one (default) profile that defines common attributes to be associated with the Technology. You can configure these profiles in the Settings>Technology Settings menu group.

Channel*, the telephony (DAHDi) channel, selected from the drop-down list, which should be associated with the device.

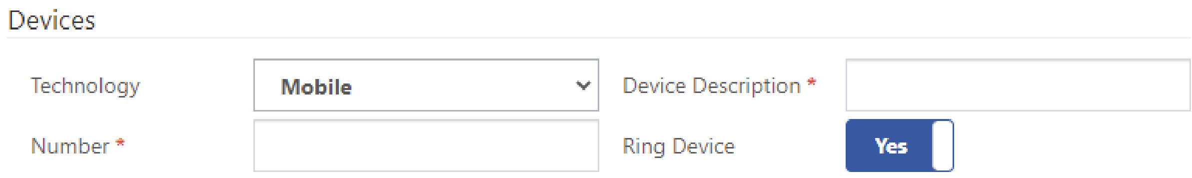
Hotline Number, the extension will automatically call this number if the phone is off the hook for the time defined in the **Hotline Timeout** field. This feature is disabled when the **Hotline Number** field is empty.

Hotline Timeout, after the phone has been off the hook for the defined number of seconds, an automatic call will be made to the preset number defined as **Hotline Number**. The call will be made immediately if this field is set to zero.

Device Description*, a free-text description to identify the device.

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

Mobile Option

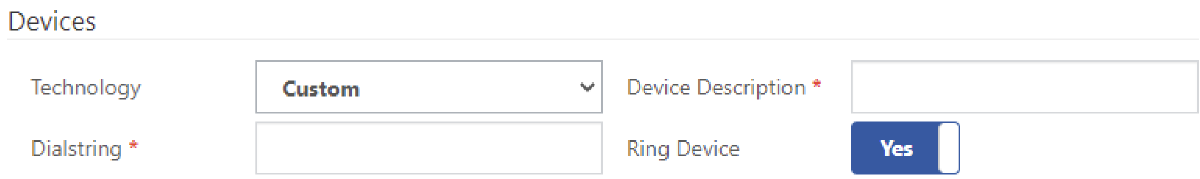


Number*, the number to dial to reach a mobile device associated with this extension. As with other devices, the mobile device will ring in parallel with all devices associated with the extension. Do not forget to take into account the dialout code, if it is required to reach the mobile device.

Device Description*, a free-text description to identify the device.

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

Custom Option

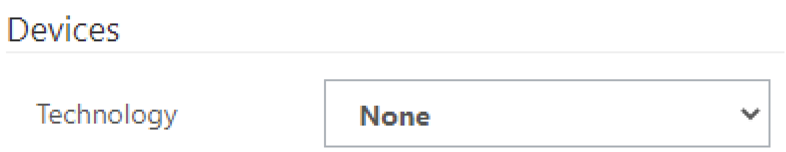


Dialstring*, the dialstring to reach a device associated with this extension. For example, the dialstring could contain something like Local/49909183@cos-all. This would dial the external number 49909183 using the cos-all Class of Service. As with other devices, this device will ring in parallel with all devices associated with the extension.

Device Description*, a free-text description to identify the device.

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

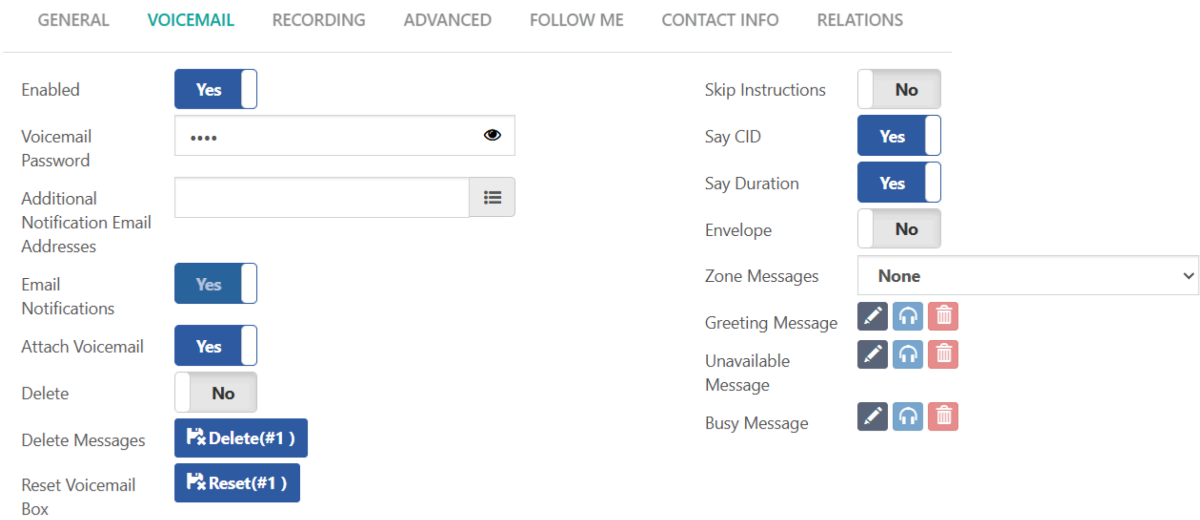
None Option



Use this option to create an extension that does not have a device associated with it. You can use this option to create an extension that will be used for Hot Desking, or to create a virtual extension.

VOICEMAIL Tab

It is not mandatory to define any fields in this tab. However, the voicemail feature will not be available unless the **Enabled** field is set to **Yes**



Enabled, enables or disables voicemail. If voicemail is not enabled, voicemail messages cannot be left for the extension. If Email Notifications field is set to **Yes** and an email address is defined in the General tab, voicemail messages can also be emailed to the user.

Voicemail Password, numeric password to access user's voicemail. Can be left blank, or can consist of any number of digits. May also include (but cannot start with) the star (*) character.

If the voicemail password matches the user's extension number, the user will be prompted to create a new password when voicemail is next accessed. This feature is very useful when configuring new extensions. The PBX administrator can set the voicemail password to match the extension number, allowing all users to personalize their own password.

Additional Notification Email Addresses, additional email addresses that will receive voicemail notifications, in addition to the extension's main email address. Separate email addresses by comma.

Email Notifications, controls whether voicemail messages will be sent to extension's email address.

Attach Voicemail, determines whether a recording of voicemail will be attached to the notification email. If an email address is defined (in the General tab of the Extensions dialog), the user will receive an email notification of any new voice messages.

Delete, causes the voicemail to be deleted from the server after the voicemail has been delivered. Be careful with this option, because the system may delete the message without guaranteeing that the email has been delivered successfully. This could mean that after a message is left, and the system has made an attempt to send a notification email to the user, that the actual voicemail that was left may no longer be accessible. You can only set **Delete** to **Yes** when **Attach Voicemail** is also set to **Yes**.

Delete Messages, press this button to delete all voicemail messages from the voicemail box. Note that this button will display the number of messages that will be deleted when taking this action (e.g., 3 messages).

Reset Voicemail Box, press this button to delete all messages and greetings from the voicemail box and reset the voicemail password. Note that this button will display the number of messages that will be deleted when taking this action (e.g., 3 messages).

Skip Instructions, skip playing voicemail instructions to the caller when set to **Yes**

Say CID, causes the system to play back the **Caller ID** (CID) number of the person who left the message, prior to playing the full message.

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

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

Zone Messages, time zone that should be used for formatting timestamps in voicemail messages. If this field is not configured, the time zone will be taken from the general settings section. Irrelevant if the **Envelope** field is set as **No**.

Greeting Message, the message that you want to play to callers when they reach your voicemail. You can use the **Edit** icon to upload a new message, the **Listen** icon to hear your current message, or the **Delete** icon to delete your current message.

Unavailable Message, the message that you want to play to callers when you are not available. You can use the **Edit** icon to upload a new message, the **Listen** icon to hear your current message, or the **Delete** icon to delete your current message.

Busy Message, the message that you want to play to callers when your line is busy. You can use the **Edit** icon to upload a new message, the **Listen** icon to hear your current message, or the **Delete** icon to delete your current message.

Icons used for Managing Messages:

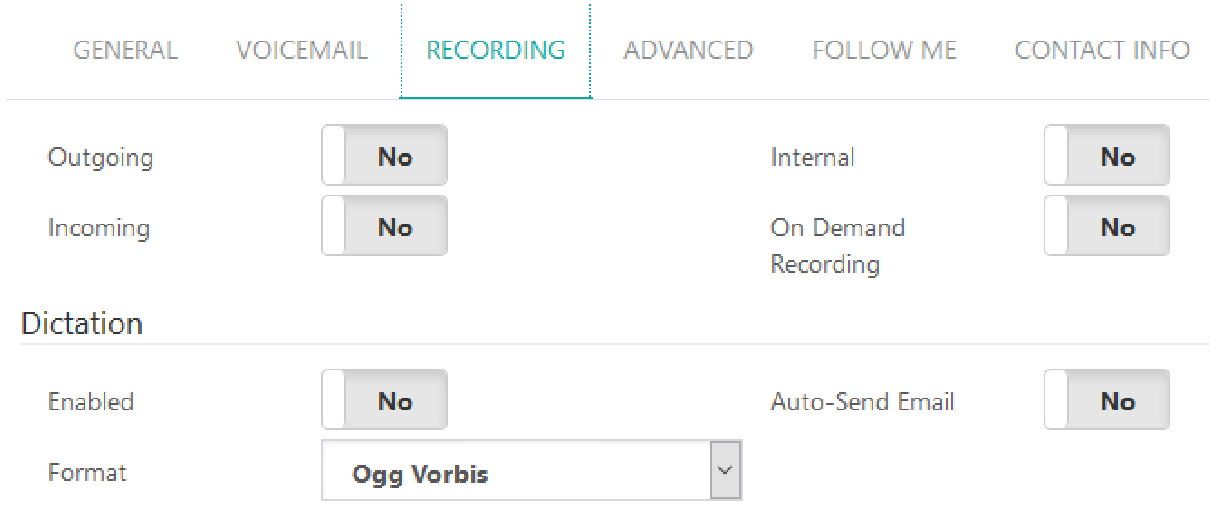
 Edit icon

 Listen Icon

 Delete icon

RECORDING Tab

It is not mandatory to define any fields in this tab.



In this tab you will find information about recording telephone calls and dictation. These fields allow a user to control the recording of incoming or outgoing calls. The user can either key a feature code (*3) to selectively enable recording for the current call, never record calls, or always record calls.

Outgoing, record all external outgoing calls**.**

Incoming, record all external incoming calls.

Internal, record all internal calls.

On Demand Recording, record only calls on demand.

Dictation Section

Enabled, activates the dictation service when set to **Yes**.

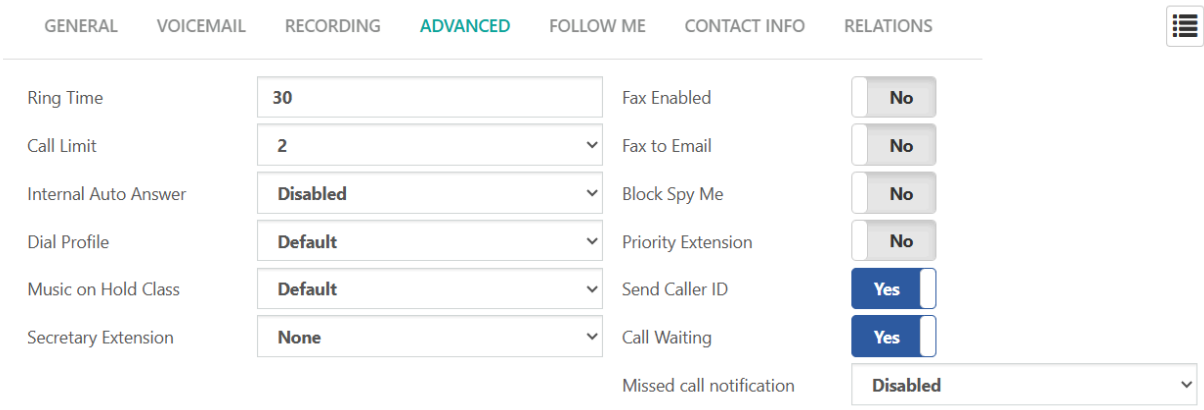
Format, records the audio in one of the formats from the drop-down list:

- Ogg Vorbis
- GSM
- WAV

Auto-Send Email, dictated recordings will be automatically sent to your email on completion.

ADVANCED Tab

It is not mandatory to define any fields in this tab.



Ring Time, the number of seconds to ring the extension before giving up and moving on to the next destination, such as voicemail, for the Extension.

Call Limit, maximum number of simultaneous calls that can be handled by each SIP device of the extension. The default value of 2 allows a SIP device to transfer a call while holding the incoming call.

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 Device.

Dial Profile, allows you to select a Dial Profile to be associated with the extension. Dial Profiles control functionality such as call transfer, parking, call screening, etc.

Music on Hold Class, the default Music on Hold class to be associated with the extension.

Secretary Extension, this is used to re-route all incoming calls for the current extension to the extension of a designated secretary. Only the designated secretary is allowed to make direct calls to the extension.

Note that after defining the Secretary Extension, you need to use the Extension Status dialog to activate the new setting.

FAX Enabled, indicates whether the extension is configured to receive faxes. This allows the extension to be used as a destination for both voice and FAX communications.

If you want to receive faxes using the inbound route associated with the extension, ensure that Fax Detect is enabled for the inbound route, and that faxes are directed to a valid fax recipient.

Fax to Email, if enabled, will send incoming faxes to the email addressed defined in the General tab of the extension.

Block Spy Me, do not let others users to spy on the extension.

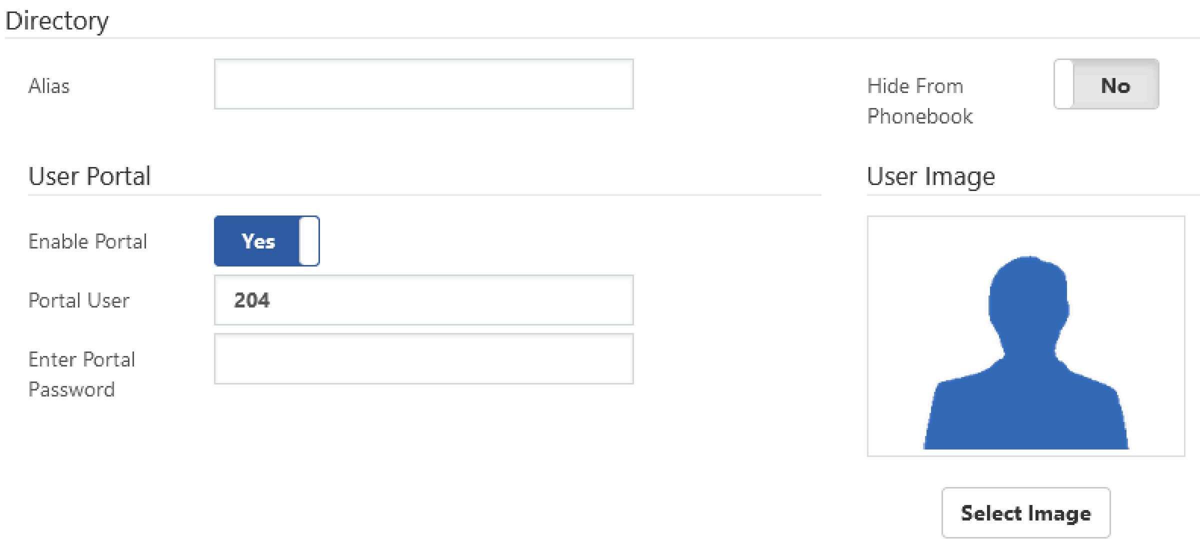
Priority Extension, allows this extension to interrupt the Do Not Disturb (DND) mode of other extensions. This ensures that urgent or high-priority calls can reach users even when DND is active.

Send CallerID, send, or hide, the Caller ID (CID) for the extension.

Call Waiting, determines whether call waiting will be enabled for the extension. If you call a busy extension where call waiting is enabled, the caller will hear a stutter tone to indicate that the person is busy with another call.

Missed call notification, enables the system to send email notifications to the user when a call to their extension is missed. You can configure the notification to include all missed calls or limit it to only those originating from external numbers. The email address used for the notifications is the one defined in the General tab of the extension. This feature ensures users stay informed of missed communication attempts even when they are away from their phone.

Directory Section

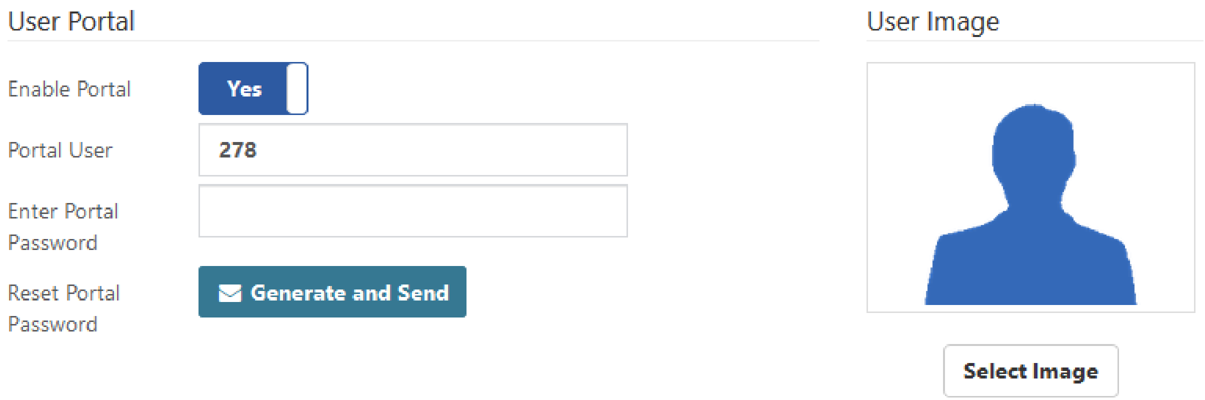


Alias, an alternative name that can be used in the system-created phonebook directory, or for dialing using the Phonebook Directory feature code (411).

Hide From Phonebook, when the field is set to **Yes**, the name of the extension will not be visible to the system-created phonebook directory, and you cannot call the user using the Phonebook Directory feature code (411).

User Portal Section

Enabling the User Portal provides the extension user with access to some of the extension parameters. Each user can only see (and configure) parameters relating to their own extension.



Enable Portal, determines whether the user associated with the extension can access the User Portal.

Portal User, contains the username for accessing the User Portal dialog. Can consist of letters and numbers, but cannot include special characters.

Portal Password, contains the password that is used to access the User Portal. User Portal access cannot be enabled if the password field is left blank.

If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password.

Reset Portal Password, click on **Generate and Send** button to send an email to the Portal user, provided that:

- A valid email address is defined for the extension
- Email for CompletePBX 5 is configured and working correctly

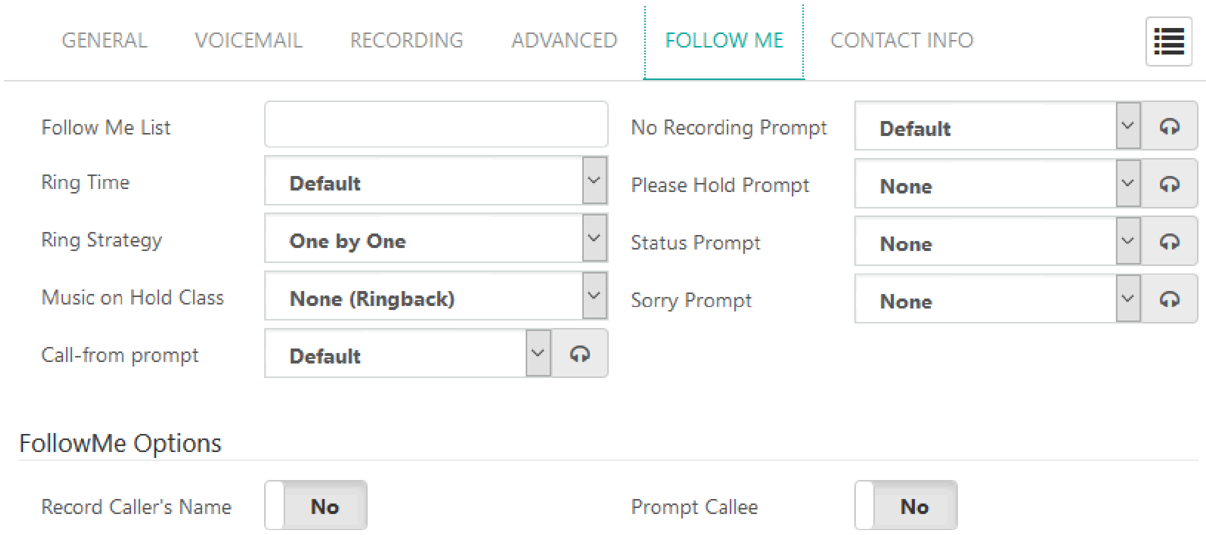
The email will also provide the Portal user with the user name to access the Portal, Portal password, and the link that should be used to access the Portal, so it is important that the administrator accesses CompletePBX 5 with the same URL that the Portal user should use.

User Image Section

Allows the user to select any image and associate it with his extension. It may be the photo of the owner of the extension, an avatar, or any other graphic. The image should be in png, jpg, or jpeg format. The size of the file must be less 20 MB

FOLLOW ME Tab

It is not mandatory to define any fields in this tab.



Follow Me List, list of extensions and/or external numbers to be accessed by Follow Me. Follow Me can consist of one or more internal extensions or external numbers. Note that if you include external numbers in the Follow Me list, you must include any access codes that would be required to make the call. For example, if external calls require an access code of "9" in order to gain trunk access, the "9" must be included in the number that is entered as a Follow Me destination.

After entering the digits of the Follow Me destination, press on the Enter button on your keypad. You can add multiple destinations by entering each destination followed by a comma (",").

Note that after defining the Follow Me destinations, you ***must*** use the Extension Status dialog to activate the Follow Me setting, or use the Feature Code (*67) to toggle Follow Me.

Ring Time, is the time that the phone will ring the numbers defined in the **Follow Me List** without being answered, before continuing to an alternative destination, such as Voicemail.

Music on Hold Class, the class of Music on Hold that should be played to the caller while they are waiting to be connected. The default setting is to play the country-specific ring sound.

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 when no option is 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 is not at their desk” message prompt, or use your own custom prompt.

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

Follow Me Options Section

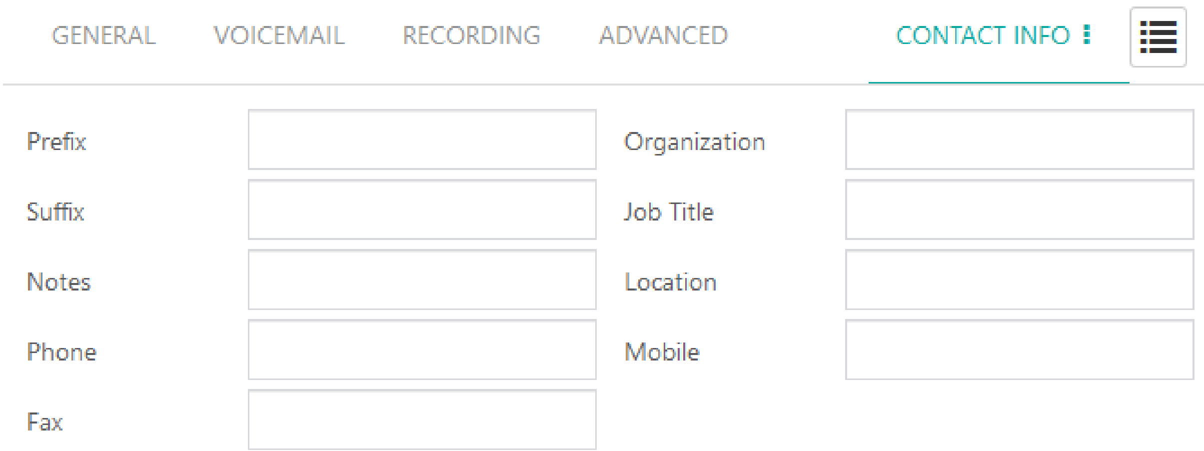
Record Caller’s Name, record the name of the caller so that it can be announced to the callee at each step.

Prompt Callee, prompts the user at follow me destination to confirm that they want to receive the call.

You should always activate **Prompt Callee** when using Follow Me option with a mobile device. This will ensure that if the call is not answered by the mobile device, the call will not reach the voicemail system of the mobile device, and will return to the voicemail of the original extension that was dialed.

CONTACT INFO Tab

It is not mandatory to define any fields in this tab.



Name, specifies the name for the Contact. This is a free-text field, so can include salutations, such as Mr, Dr, etc. as well suffixes, such Jr, etc.

Notes, any notes that you want to associate with the contact. This is a free-text field.

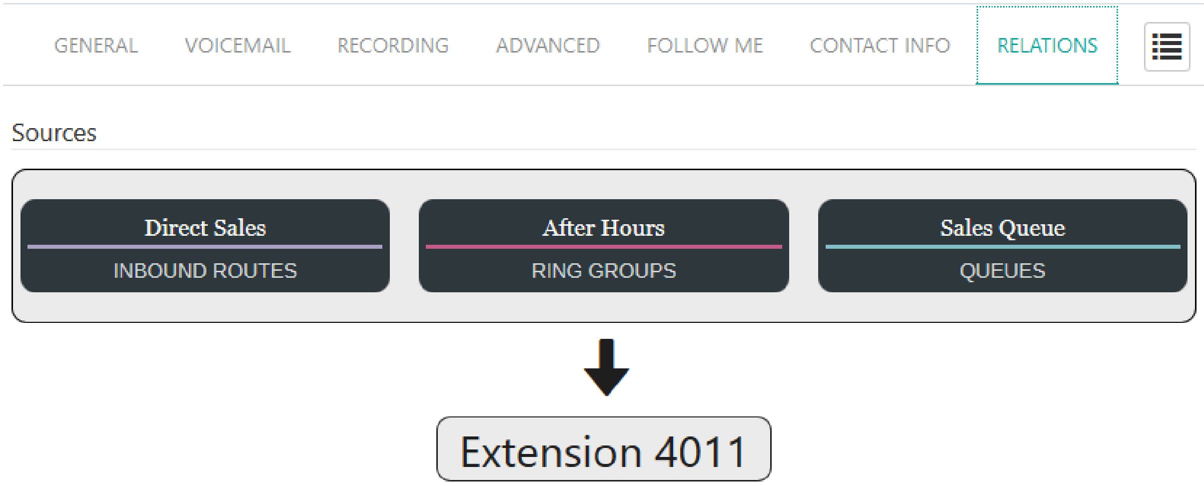
Organization, sets an organization to be associated with the contact. This is a free-text field.

Job Title, specifies a job title for the contact, e.g. “Sales Manager”. This is a free-text field.

Location, sets a location for the contact, e.g. "Las Vegas". This is a free-text field.

RELATIONS Tab

This tab provides a graphical display all the modules that are used by the extension that you are currently viewing. This allows you to see at a glance all modules that include the currently-selected extension as a destination.



You can click on any of the displayed items to jump directly to the dialog where the relationship is defined.

Hot Desking Dialog

The Hot Desking dialog creates accounts 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 extensions dialog 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 (default code *80): you will be prompted for the extension number, and the password. *You can also direct-dial into an extension by using a string dialing of the feature code, extension, and password, e.g., *80*EXT**PASS. This allows setting up BLF buttons for quick login for different users on the device. To remove the association, you need to key in the hot desking feature code (default code *80): you will be prompted to enter the extension number and password.

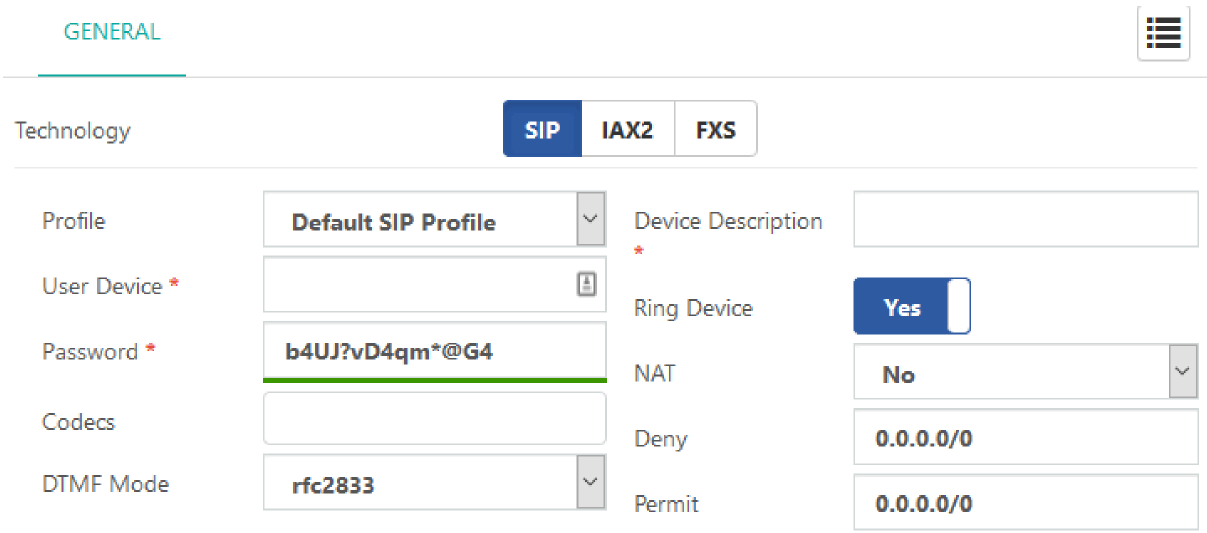
When a Hot Desk device logs in or out of the system, an entry will be created in the CDR Report, indicating the activity.

GENERAL Tab

Technology, type of technology for the device. There is a selection of three options:

- **SIP**
- **IAX2** (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)
- **FXS** analog devices (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

SIP Option



User*, user to register this Hot Desk.

Password, password (secret) associated with this Hot Desk.

If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password.

Profile, technology profile settings for the device. At least one (default) profile must be defined that defines common attributes to be associated with the Technology. You can configure these profiles in the Settings>Technology Settings 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.

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. Other options available in the drop-down list 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 it is available, otherwise use in-band option

Device Description*, a free-text description to identify the Hot Desk.

Deny, in a user/peer definition, allows you to limit SIP traffic to and from the peer to one or more specific IP addresses or networks. This option should be in the format of an IP address and subnet.

- 192.168.25.10/255.255.255.255 denies traffic for the extension from the specific IP address
- 192.168.1.0/255.255.255.0 denies traffic for the extension from all IP addresses in the range of 192.168.1.1 to 192.168.1.254
- 0.0.0.0/0.0.0.0 denies access from all networks by default. Note that you can specify which networks can have access by specifying them in the Permit field
- You can define multiple addresses by separating each address with the "," (comma) symbol, i.e. 192.168.0.0/24,192.168.6.0/24

Deny 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, the system will not block traffic for the peer from any IP address.

Permit, in a user/peer definition, allows you to limit SIP traffic to and from the peer to one or more specific IP addresses, or networks.

- 192.168.10.0/255.255.255.0 allows traffic from any address on the 192.168.10.x network

The Permit field is the opposite of the deny field. Specific IP addresses or networks can be added in this field to allow traffic to access the extension from the specified IP address or network.

This field is not mandatory. If it is left blank, traffic will be allowed from all IP addresses. Strengthen your system security by using the Deny and Permit fields. If the endpoint is static, we strongly recommend that you make proper use of the Permit and Deny fields 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 external internet. Private addresses are in the following ranges:

- 10.0.0.1 - 10.255.255.254 – which can also be written as 10.0.0.0/8
- 172.16.0.1 - 172.31.255.254 – which can also be written as 172.16.0.0/12
- 192.168.0.1 - 192.168.255.254 – which can also be written as 192.168.0.0/16

NAT options can be selected from the drop-down list:

- **No** - no special NAT handling other than RFC3581
- **Force** - pretend there is an rport parameter even if there is not

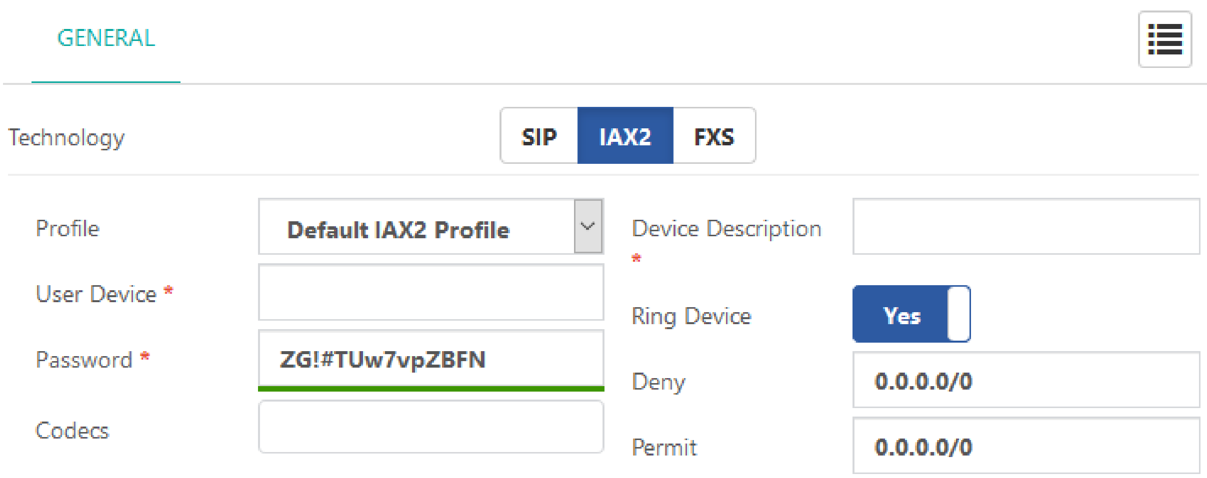
- **Comedia** - send media to the same port that Asterisk received it from, regardless of where the SDP says to send it.
- **Force, Comedia**
- **Auto Force** - set the force_rport option if Asterisk detects NAT
- **Auto Comedia** - set the comedia option if Asterisk detects NAT

NAT is always set to **No** in multi-tenant systems, and no other option can be configured.

Ring Device, determines whether incoming calls should cause the Hot Desk to ring.

IAX2 Option

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)



User*, username to be used when registering the Hot Desk.

Password, password (secret) associated with the Hot Desk. Passwords can be the weakest link of 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.

If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password.

Profile, technology profile settings for the Device. At least one (default) profile must be defined that defines common attributes to be associated with the Technology. You can configure these profiles in the Settings>Technology Settings 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 Hot Desk will only use only the codecs that you specifically define for the Hot Desk.

Device Description*, a free-text description to identify the Hot Desk device.

Deny, in a user/peer definition, allows you to limit SIP traffic to and from the peer to a specific IP address or network. This option should be in the format of an IP address and subnet.

- 192.168.25.10/255.255.255.255 denies traffic for the extension from the specific IP address
- 192.168.1.0/255.255.255.0 denies traffic for the extension from all IP addresses in the range of 192.168.1.1 to 192.168.1.254
- 0.0.0.0/0.0.0.0 denies access from all networks by default. Note that you can specify which networks can have access by specifying them in the Permit field
- You can define multiple addresses by separating each address with the "," (comma) symbol, i.e. 192.168.0.0/24,192.168.6.0/24

Deny 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, the system will not block traffic for the peer from any IP address.

Permit, in a user/peer definition, allows you to limit SIP traffic to and from the peer to a specific IP address, or network.

- 192.168.10.0/255.255.255.0 allows traffic from any address on the 192.168.10.x network.

The Permit field is the opposite of the deny field. Specific IP addresses or networks can be added in this field to allow traffic to access the extension from the specified IP address or network.

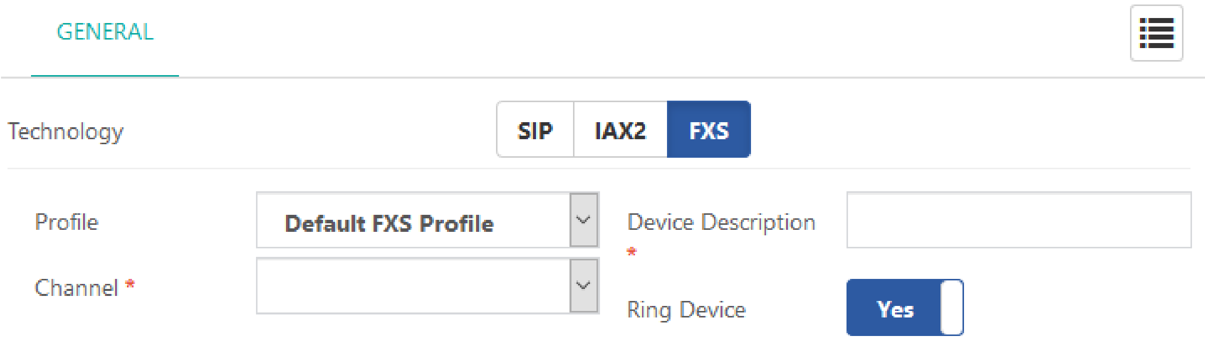
This field is not mandatory. If it is left blank, traffic will be allowed from all IP addresses. Strengthen your system security by using the Deny and Permit fields.

If the endpoint is static, we strongly recommend that you make proper use of the Permit and Deny fields 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, determines whether incoming calls should cause the Hot Desk to ring.

FXS Option

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)



Channel*, the number of the DAHDi channel**,** selected from the drop-down list**,** that should be associated with the Hot Desk.

Profile, technology profile settings for the Device. At least one (default) profile must be defined that defines common attributes to be associated with the Technology. You can configure these profiles in the Settings>Technology Settings menu.

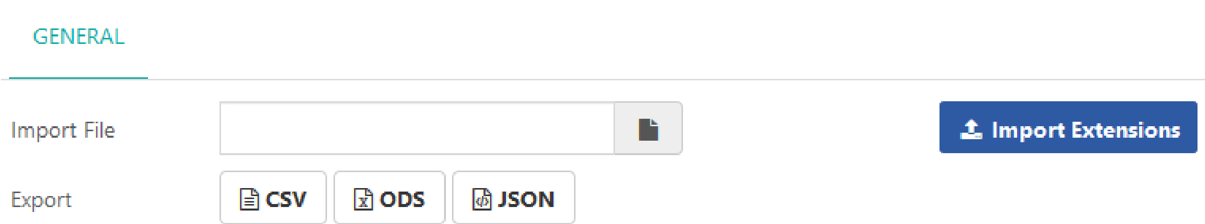
Device Description*, a free-text description to identify the Hot Desk device.

Ring Device, determines whether incoming calls should cause the Hot Desk to ring.

Import/Export Extensions Dialog

Export Extensions is an easy way to create a list of extensions, as well Host Desking devices, from a large system**.** You can use this dialog to create a file in CSV, ODS, or JSON format, listing the existing extensions and Host Desking devices in your system. This file can be edited and then imported back into a system using the same dialog

GENERAL Tab



Import File, the file containing details of the extensions that you want to add to the system, modify in the system, or delete from the system.

An example of the file format can be downloaded by pressing any of the export format buttons.

This downloaded example contains an explanation of each field in the first row of the spreadsheet.

Operation mode, which is set in the first column of each row, can have the following values:

- **Add**, to add a new extension, or modify an existing extension.
- **Delete**, to remove an existing extension from CompletePBX

Export, select any of the displayed formats (CSV, ODS, or JSON) to export details of the extensions that are configured in your system.

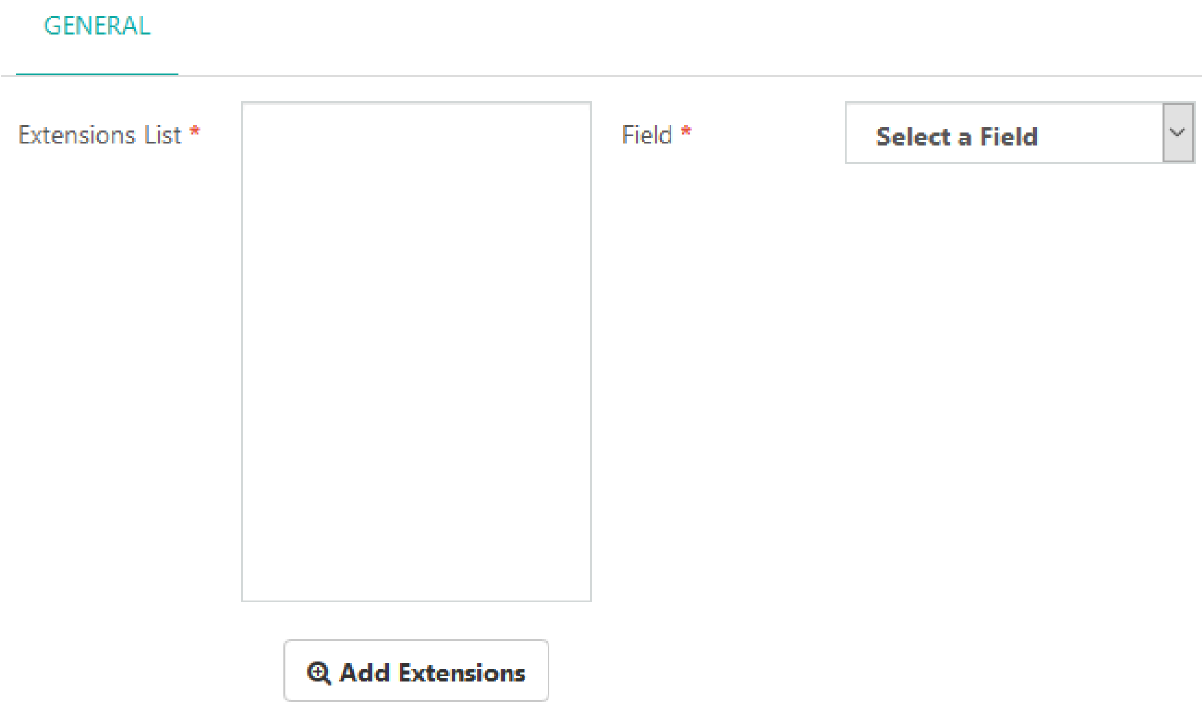
Be careful with the Delete option: deleting any device associated with an extension will cause the entire extension to be deleted.

Microsoft Excel does not always handle CSV files properly, depending on the locale settings of the computer: in such cases ODS file format should be used.

Bulk Modification Dialog

In this dialog 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 Tab



Press on the Add Extension button to select the extensions that you wish to modify.

This dialog can manage the following fields:

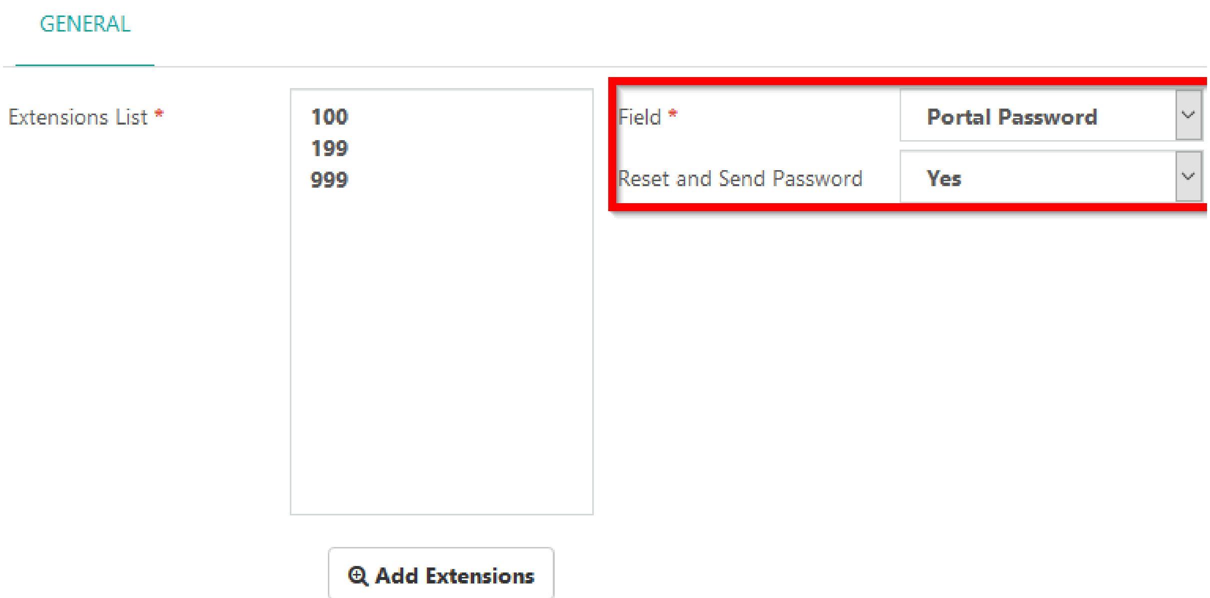
- Class of Service
- Ringtime
- Language
- Account Code

- Dial Profile
- Music on Hold
- Call Recordings
- Portal User
- Portal Password
- Call waiting
- Fax
- Voicemail
- Apply Diversions to external calls only

If you select **Portal Password,** an email will be sent to the Portal user, provided that:

- The extension is configured as a Portal user
- A valid email address is defined for the extension
- Email for CompletePBX 5 is configured and working correctly

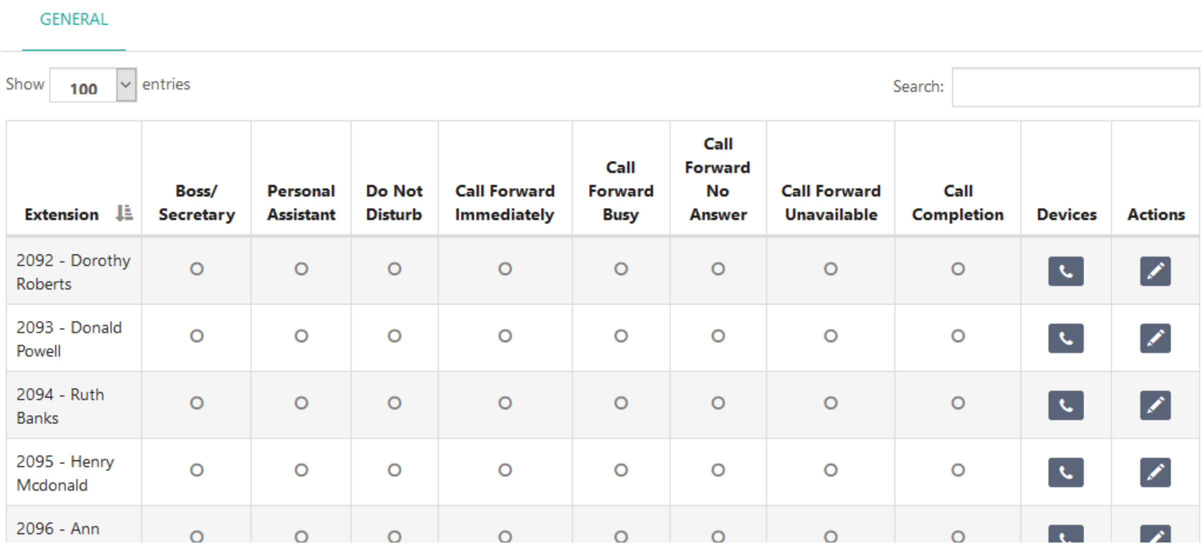
The email will also provide the Portal user with the user name to access the Portal, Portal password, and the link that should be used to access the Portal, so it is important that the administrator access CompletePBX 5 with the same URL that the Portal user should use.



Extensions Status Dialog

This dialog shows the current status of all extensions.

GENERAL Tab



The dialog displays the following fields:

- Extension number
- Boss/Secretary status
- Secretary Extension
- Personal Assistant status
- Follow Me status
- DND (Do Not Disturb) status
- CFI (Carry Forward Immediately) status
- CFB (Carry Forward Busy) status
- CFN (Carry Forward on No Answer) status
- CFU (Carry Forward Unconditionally) status
- Call Completion status
- Devices
- Actions

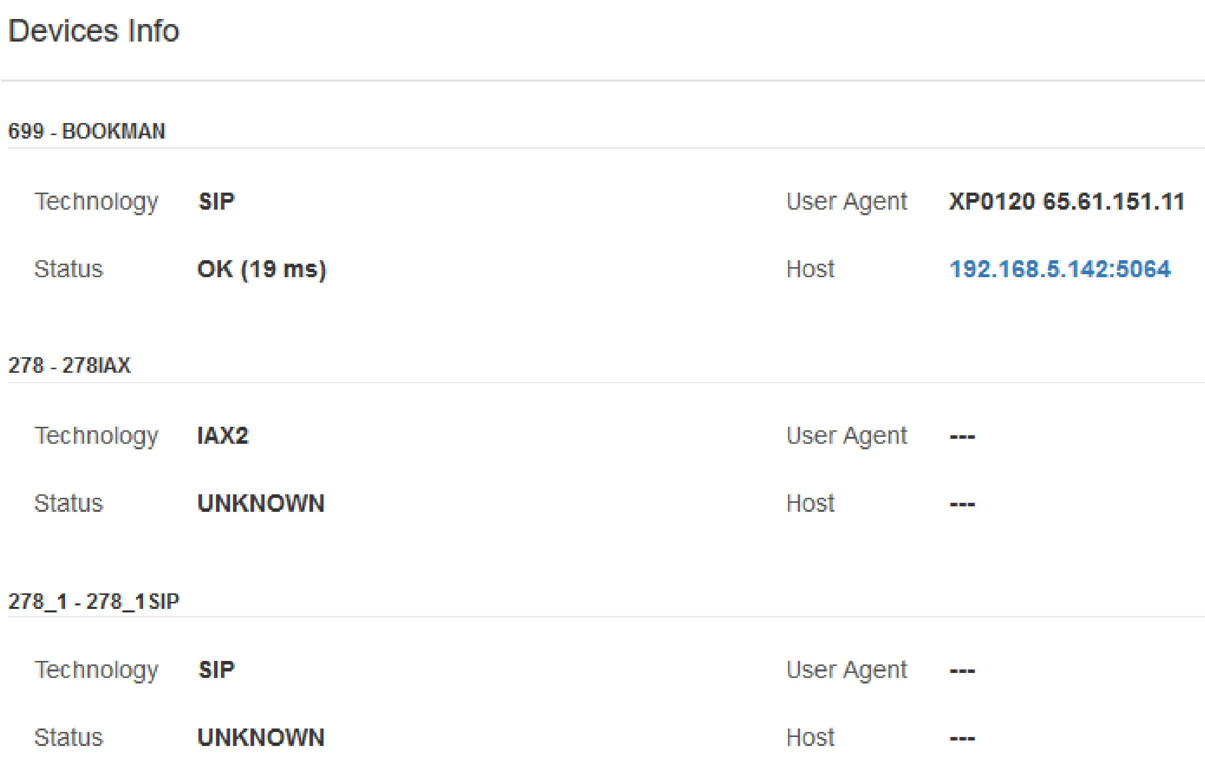
Any column can be sorted by clicking on the sort icon which is displayed in the column header for each field.

Three different icons are used to indicate the current state:

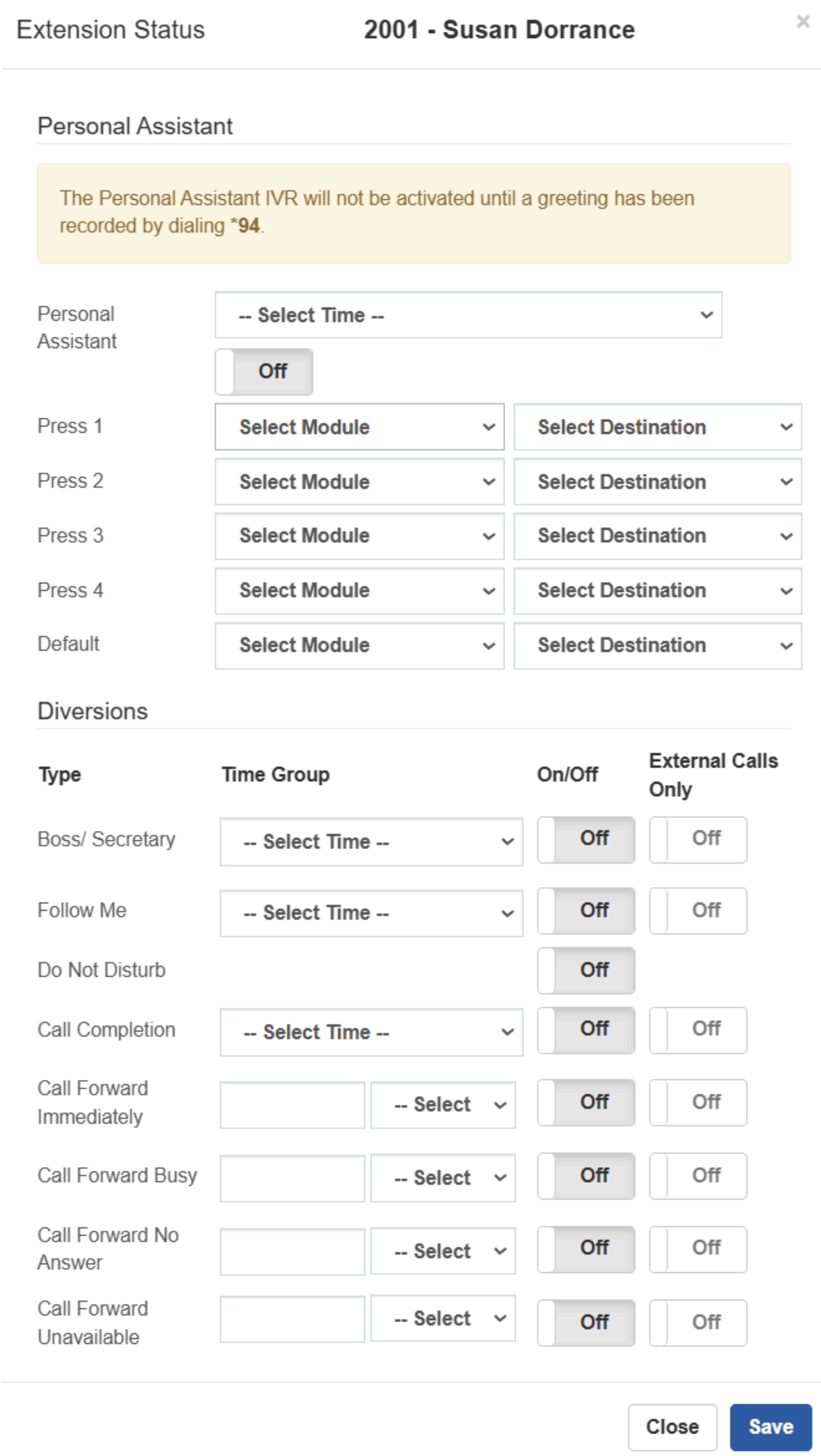
- (an empty circle) indicates that the diversion function is not enabled

- (a green checkmark) indicates that the diversion function is always enabled
- (a blue checkmark) indicates that the diversion is set only for external calls
- (a clock) indicates that the function is only active when the time matches the Time Group that is associated with the diversion

Devices, allows you to see all the devices that are associated with the extension.



Actions, allows you to change any status by simply pressing the Actions ( )button that is located at the end of each line, and making the appropriate modification. 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 drop-down)**,** or during a specific time period as defined by the Time Group that you select from the drop-down list.

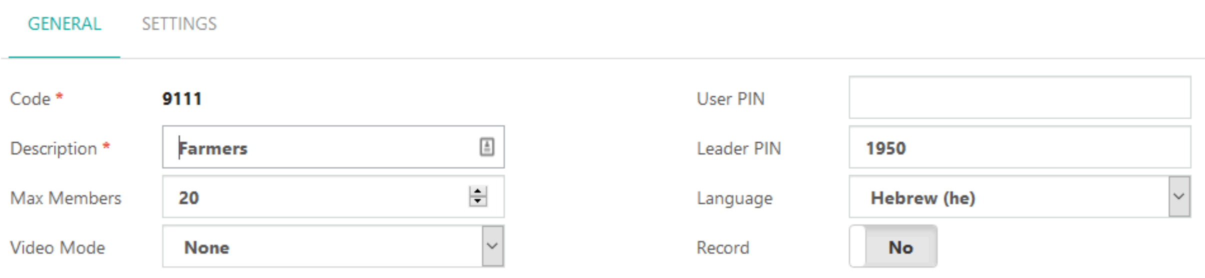

Extension Status
2001 - Susan Dorrance
Personal Assistant
The Personal Assistant IVR will not be activated until a greeting has been recorded by dialing *94.
Personal Assistant
-- Select Time --
Off
Press 1
Select Module
Select Destination
Press 2
Select Module
Select Destination
Press 3
Select Module
Select Destination
Press 4
Select Module
Select Destination
Default
Select Module
Select Destination
Diversions
Type
Time Group
On/Off
External Calls Only
Boss/ Secretary
-- Select Time --
Off
Off
Follow Me
-- Select Time --
Off
Off
Do Not Disturb
Off
Call Completion
-- Select Time --
Off
Off
Call Forward Immediately
-- Select
Off
Off
Call Forward Busy
-- Select
Off
Off
Call Forward No Answer
-- Select
Off
Off
Call Forward Unavailable
-- Select
Off
Off
Close
Save

Applications Menu Group

Conferences Dialog

A conference room allows a group of people to participate in phone calls. The most common form of conference bridge allows participants to call into a virtual meeting room from their own phone. Meeting rooms can hold dozens or even hundreds of participants. This is in contrast to three-way calling, a standard feature of most phone systems which only allows a total of three participants.

GENERAL Tab



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

Description*, a free-text description for identify the conference.

Max Members, this option limits the number of participants for a single conference to a specific number. Unlimited participants will be able to join the conference if **Max Members** is set to zero. After the user-configured 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, determines how video will be displayed. The drop-down list contains the following 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 audio.
- **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 becomes the source.

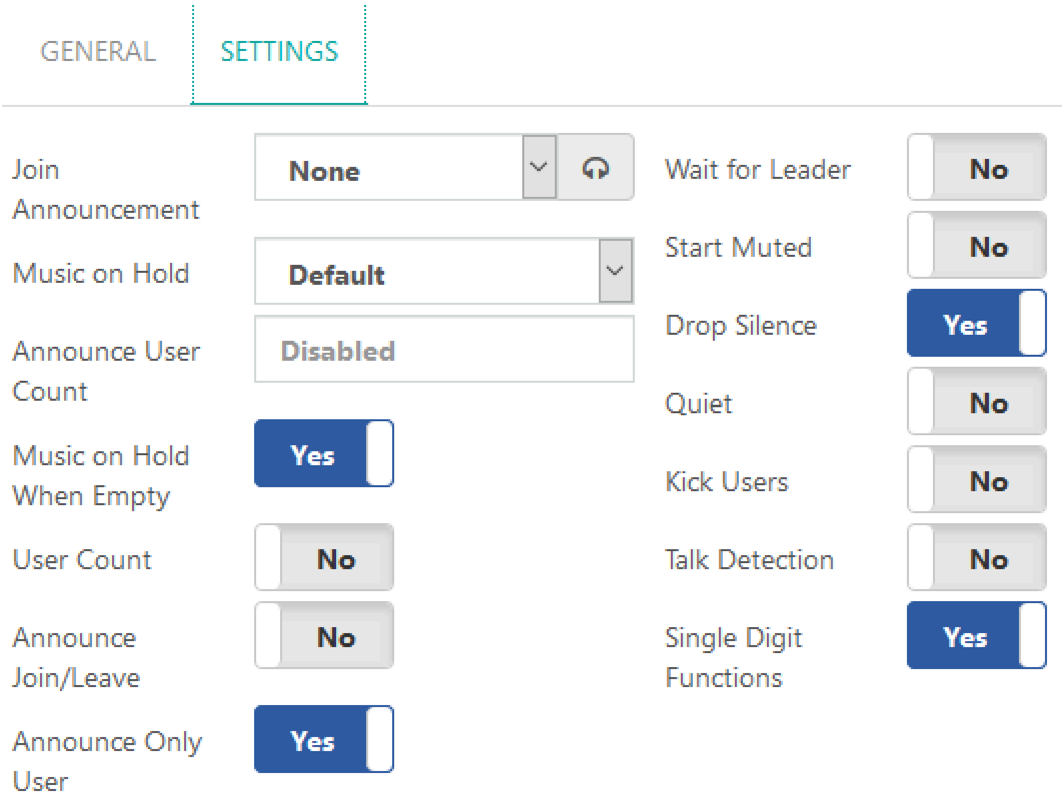
User PIN, a numeric passcode that is used to enter the conference. If a PIN is entered in this field, no one can join the conference room without entering the PIN.

Leader PIN, functions in a similar manner to the **User PIN**. The Admin PIN is used in conjunction with the **Wait Admin** option explained later in this chapter, in order to identify the administrator or leader of the conference. The Admin PIN and User PIN should not be set to the same value, otherwise the system will not be able to determine whether the participant should be treated as an Admin or as an ordinary participant.

Language, set the language which should be used for announcements in the conference.

Record, 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.

SETTINGS Tab



Join Announcement, defines a message that can be played to participants when they join the conference.

Use Xorcom voice recording services to ensure that you have high-quality, professional announcements. You can count on the continuity of our professional services so that whenever you would like to change or add a recording, you will be able to use the same professional voice for a coherent customer experience.

Music on Hold, the Music on Hold class to use for the conference.

Announce User Count, used for announcing the participant count to all members of the conference. If set to any value, then the announcement is only played when the number of participants is greater than the set number. Available options are:

- Yes
- No (default)
- A number, which will cause the user count to be announced only after the number of participants exceeds the user-defined number

Use Xorcom voice recording services to ensure that you have high-quality, professional announcements. You can count on the continuity of our professional services so that whenever you would like to change or add a recording, you will be able to use the same professional voice for a coherent customer experience.

Music on Hold When Empty, when the field is set to Yes**,** Music on Hold 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 the field is set to No**,** no sound will be played.

User Count, when the field is set to **Yes,** 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 the field is set to **Yes,** the conference will prompt each user to identify themselves with 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, determines whether the **Only User Announcement** should be played when the first user enters an empty conference.

Wait for Leader, when the field is set to **Yes,** the conference will not begin until the conference leader joins the conference room. The leader is identified by the Leader 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 the field is set to **No,** the callers will be bridged into the conference as soon as they call the conference number.

Start Muted, when the field is set to **Yes,** all users joining the conference are initially muted. This setting does not apply to the conference leader

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. This option is highly recommended for large conferences due to its performance enhancement.

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

Kick Users, when the field is set to **Yes,** all remaining users in the conference will be kicked out after the last conference leader user leaves the conference.

Talk Detection, indicates whether or not notifications of when a participant begins and ends talking should be sent out as an event to Asterisk Manager Interface (AMI).

Single Digit Functions, determines which codes can be entered by conference users to manage settings during a conference call. When set to **Yes**, users can enter either **1** or ***1** to toggle the mute setting. When set to **No**, only ***1** will toggle the mute setting. This function is useful when some of the conference participants have a bad line, which can lead to spurious DTMF signaling.

The following codes can be dialed by all participants during the course of a conference:

- **1** or***1** – toggles Mute setting for the user. When Mute is enabled**,** anything the user says is not transmitted to the rest of conference members. If the conference is being recorded**,** anything said by the muted user is not included in the recording.
- **4** or ***4** - decreases receive volume. The user can key in this option to decrease the volume that they are hearing. This does not affect what any other conference members hear. If a user is finding other conference members too loud**,** they can key in *4 a few times to make the Conference quieter for themselves.
- **5** or***5** - increases receive volume. The user can key in this option to increase the volume that they are hearing. This does not affect what any other conference members hear. If a user is having trouble hearing other members of the Conference**,** they can key in *5 a few times to make the Conference louder for themselves.

- **6** or ***6** - decreases transmit volume. The user can key in this option to decrease the volume that 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 key in *6 few times to make their transmit volume quieter.
- **7** or ***7** - increases transmit volume. The user can tap this option to increase the volume that 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 key in *7 a few times to make their transmit volume louder.
- **8** or ***8** – user can key in this code to leave the Conference.

In addition, the admin has access to additional codes:

- **2 or** *2 - toggles the conference lock. When a conference is locked, no more callers may join. A locked conference must be unlocked to all any new users to join. This option is only available to the conference leader. This option is not available if the conference does not have an admin PIN configured or the leader has joined the Conference as a user instead of an admin.
- **3** or ***3** - ejects from the conference room the last user who joined the conference. The user will hear a message informing them that they have been ejected from the conference and that their call will be terminated. Note that if a conference is subsequently 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 not available if the conference does not have an admin PIN configured or the leader has joined the conference as a user instead of an admin.

Scheduled Conferences Dialog

The **Scheduled Conferences** module provides advanced control and flexibility for setting up and managing conference calls. Unlike standard ad-hoc conferences, this feature allows administrators to schedule recurring meetings and include both internal and external participants in advance.

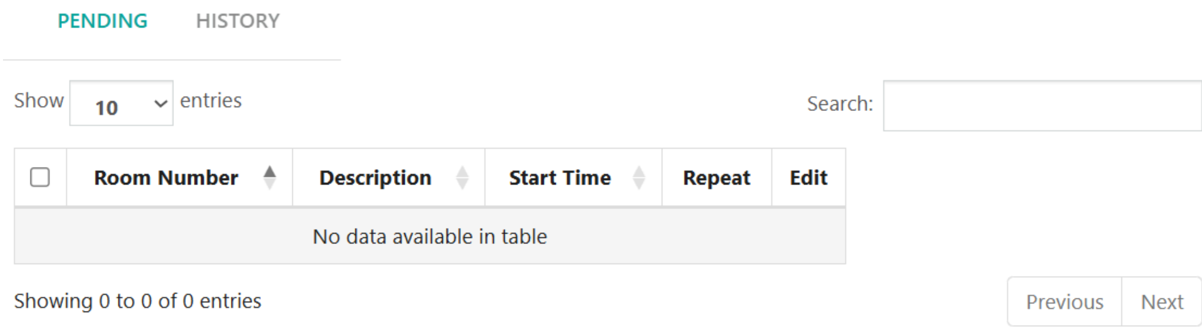
GENERAL Functionality

- **Schedule a repeatable conference**, allowing you to configure conferences to occur automatically on a recurring basis (daily, weekly, monthly).

- **Add external participants**, making it easy to invite participants from outside your organization when scheduling a conference.

This functionality ensures that scheduled conferences are organized, predictable, and inclusive of both internal extensions and external numbers.

PENDING Tab

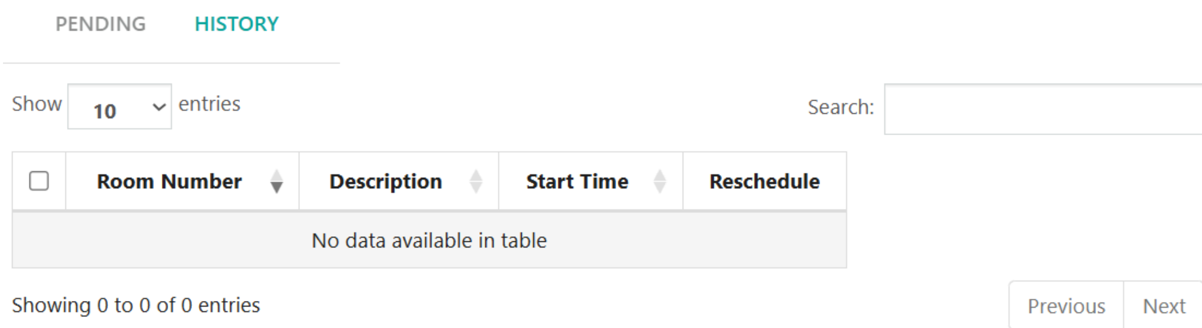


The **Pending** tab displays all upcoming scheduled conferences that have not yet occurred. Each entry includes details such as:

- **Room Number**, the extension number assigned to the conference room.
- **Description**, a free-text description to identify the scheduled conference.
- **Start Time**, the scheduled start time of the conference.
- **Repeat**, whether the conference is a one-time event or part of a recurring schedule (daily, weekly, monthly).
- **Edit,** allows you to edit the schedules conference.

Administrators may edit or cancel a scheduled conference from this tab before it begins.

HISTORY Tab



The **History** tab provides a record of all previously scheduled conferences. Each entry includes:

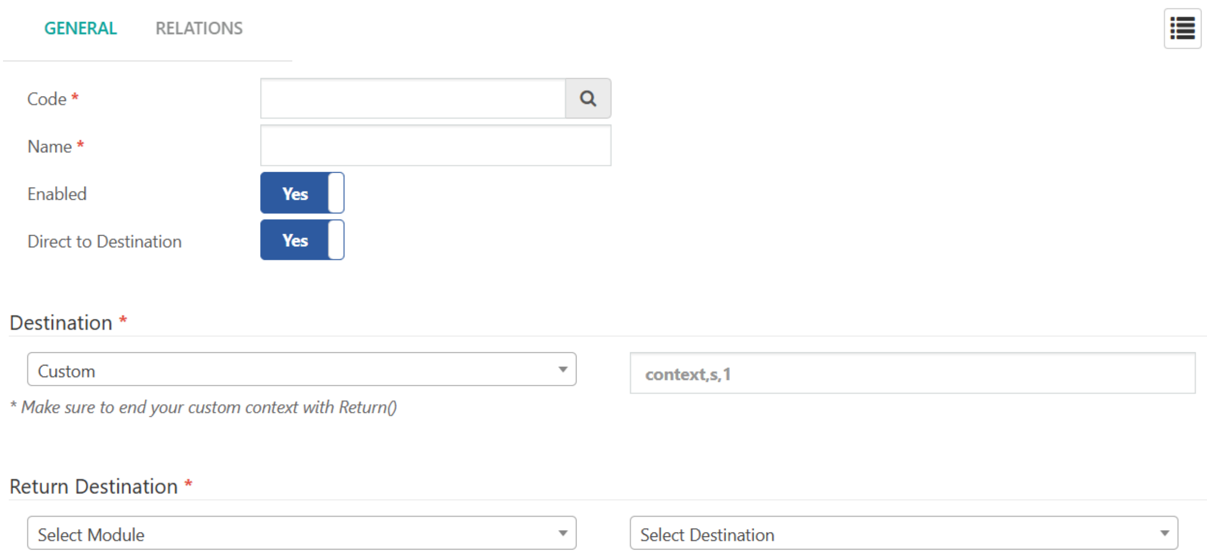
- **Room Number**, the extension number of the conference room used.
- **Description**, a free-text description to identify the scheduled conference.
- **Start Time**, the scheduled start time of the conference.
- **Reschedule**, enable to reschedule the past conference.

This historical view helps administrators track usage, verify participation, and review past scheduled meetings for auditing and reference purposes.

Custom Applications Dialog

This dialog allows you to call dialogs that do not have an extension number, such as Follow Me, Parking, IVR, etc. A Custom Application enables you to create a custom feature code, allowing a custom extension or Feature Code to be defined, which can direct the caller to any call target when dialed. For example, if you have a Ring Group that calls the cell phones of all staff members, you could create a Custom Application that calls that Ring Group when **CELL* (**2355*) is dialed.

GENERAL Tab



Code*, the number to call to reach the service. The Code can be changed at any time, provided that it does not clash with any existing destination, such as an extension, queue, etc. The change will be automatically implemented in the system in any places where the Custom Application is configured as a destination. The Code supports dialing patterns, not just a fixed number. For example, you can use a pattern like 2XXXX.

Name*, a free-text name to identify the Custom Application. The Name cannot be modified after the Custom Application has been configured in the system.

Enabled, enable or disable the 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 Custom Application entirely.

Destination Section*

Select Module, allows you to choose from a drop-down list of available dialogs, which dialog should be activated.

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

Return Destination Section*

Select Module, allows you to choose from a drop-down list of available dialogs, which dialog should be activated.
Select Destination, is the call target to which the call should be routed. When using a Custom destination, ensure that your custom dialplan context ends with a Return() statement—otherwise, the return destination will not be used.

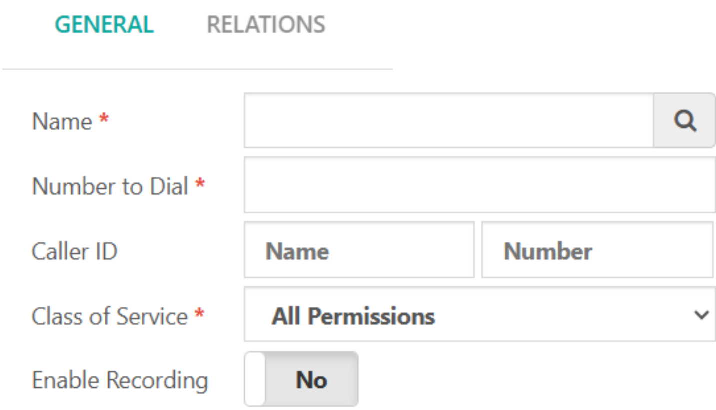
RELATIONS Tab

This tab provides a graphical display all the modules that are used by the Custom Application that you are currently viewing. This allows you to see at a glance all modules that are associated with the currently-selected Custom Application.

Custom Destinations Dialog

A Custom Destination is used to add a custom call target that can be used by system dialogs. Anything that can be dialed from a user 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. A Custom Destination could be set up to key in ***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 Tab



Name*, free-text name to identify the 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 call when a caller is routed to the destination. Any destination that can be dialed from a user extension can be entered into the field.

Caller ID, for the Custom Destination, consisting of two parts: the CID Name and the CID Number. This sets the caller ID text that is displayed while calls on the PBX.

Class of Service*, Class of Service, selected from the list shown in the drop-down, that should be associated with the custom destination.

Enable Recording, enable call recording on this Custom Destination.

RELATIONS Tab

This tab provides a graphical display all the modules that are used by the Custom Destination that you are currently viewing. This allows you to see at a glance all modules that are associated with the currently-selected Custom Destination.

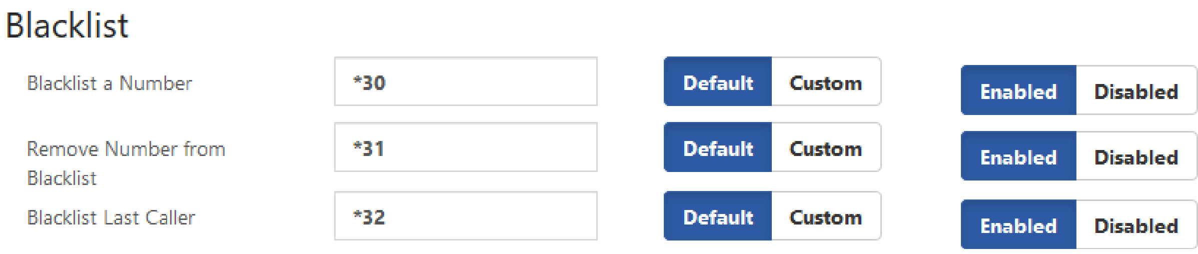
Feature Codes Dialog

The system includes all the telephony features currently available in Asterisk distributions plus features than until now were only available in expensive**,** commercial PBX systems.

Blacklist Section

The blacklist feature codes allow users to manage their personal list of blacklisted numbers.

Each of these feature codes are only available to extensions where the specific feature is enabled in the Feature Category that belongs to the Class of Service that is associated with the extension.



- ***30 Blacklist a Number,** prompts the user to enter a telephone number**,** which is then added to the system-wide blacklist. Inbound calls will not ring an extension if they are on the blacklist. Blacklisted callers will be told that the number they called is no longer in service.
Key in the feature code. You will be prompted to 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 code. Key in 1 to accept the entry, or hangup to discard it.
- ***31 Remove Number from Blacklist,** prompts the user to enter a telephone number. The entered number will be removed from the system-wide blacklist.
Key in the feature code. You will be prompted to confirm the number to be removed from the blacklist. Key in 1 to remove the blacklisted number, or hangup if you do not want to remove it from the blacklist list.
- ***32 Blacklist Last Caller,** adds the last number that called your extension to the system-wide blacklist.
Key in the feature code. You will be prompted to 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 code. Key in 1 to accept the entry, or hangup to discard it.

Business Services Section

Each of these feature codes are only available to extensions where the specific feature is enabled in the Feature Category that belongs to the Class of Service that is associated with the extension.

- ***34 Wakeup Call,** set up a reminder or wakeup call for the current extension. Key in the feature code, and follow the prompts. 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. For example, key in 0930 for 9:30 am (i.e. 9:30 in the morning), or 2130 for 9:30 pm (i.e. 9:30 in the evening).
  If you already have already set up a reminder call, you can enter 1 to cancel it.
- ***35 Remote Wakeup Call,** set up a reminder or wakeup call for another extension. Key in the feature code, and follow the prompts. Firstly, you will be prompted to enter the number of the extension for which the reminder is intended. Next, 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. For example, press 0930 for 9:30 am (i.e. 9:30 in the morning), or 2130 for 9:30 pm (i.e. 9:30 in the evening.)
  For improved security, this feature code is disabled by default.
- ***37 Last Number,** plays the last number that called the current extension. Key in the feature code to hear that last number that dialed the current extension. After listening to the number, you can key in 1 to call the caller.
- ***38 Reminder,** records a message. You can configure when you want to hear the recording, and at what extension. At the set time, you will receive a call on the designated extension and the recording will be played.
- ***33 Dynamic Conferences,** allows users to create or join a conference room on demand. By dialing the feature code, a unique 4-digit number can be entered to create a new room, join an active room, or directly transfer a call to a specific room, providing flexibility for dynamic conferencing without requiring predefined rooms.

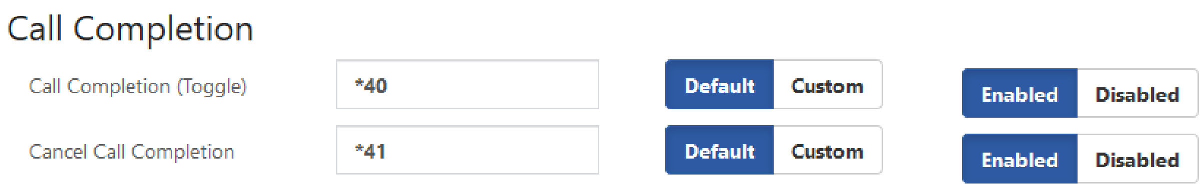
Call Completion Section

Call Completion Supplementary Services (often abbreviated to "CCSS" or simply "CC") allows a caller to let the system automatically alert him when a called party becomes available, after a previous call to that party failed for some reason. The Call Completion service can be activated when the called party is busy (CCBS), or when the called party does not respond (CCNR).

To illustrate, let's say that Alice attempts to call Bob, but Bob is currently busy on a phone call. Alice hears a busy signal: she could activate the call completion feature code. Once Bob has finished his phone call, Alice's phone will ring to alert her that Bob is now available. When Alice picks up the phone, a call will automatically be made to Bob's phone. However, if Alice ***rejects*** the alert that Bob's phone is now free, the Call Completion will be cancelled.

This feature code is only available to extensions where this feature is enabled in the Feature Category that belongs to the Class of Service that is associated with the extension.

Call Completion alerts send a special ringtone, Bellcore-dr3, to SIP phones that support this ringtone.



- ***40 Enable/Disable Call Completion,** toggle to activate a call to a previously unresponsive extension when that extension becomes available.
  ***41 Cancel Call Completion,** disables any previously-activated 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, telesales 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 options from the telephone.

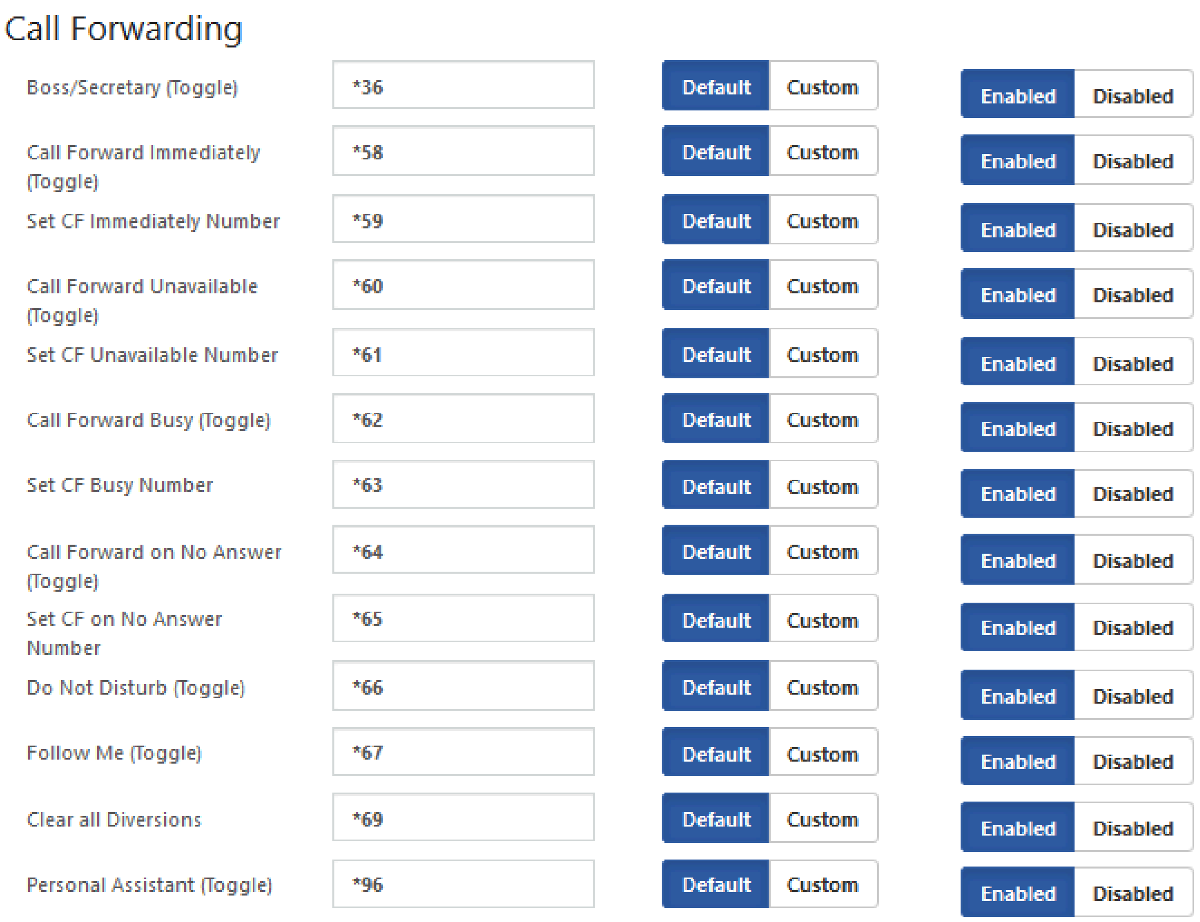
Each of these feature codes are only available to extensions where the specific feature is enabled in the Feature Category that belongs to the Class of Service that is associated with the extension.

- ***50 Add/Remove Queue Agent,** toggle to add an agent to all queue, or remove the agent from all queues. You can either key in the feature code and follow the prompts, or (in expert mode) key in the feature code followed by * (star), immediately followed by the number of the agent.
- ***51 Pause/Unpause Queue Agent,** toggle to pause, or unpause, specific queues for an agent. You can either key in the feature code and follow the prompts, or (in expert mode) key in the feature code followed by * (star), immediately followed by the number of the agent and the queue number.
- ***52 Queues Login/Logout,** allows you to login to (or logout from) a specific queue. Key in the feature code and follow the prompt.
- ***53 Queues Pause/Unpause,** allows you pause (or unpause) all queues.

- ***54 Barge into Call,** allows user to barge into an existing call.
  For improved security, this feature code is disabled by default.
- ***55 Spy on Extension,** spy on a specific extension. Key in the feature code and follow the prompt.
  For improved security, this feature code is disabled by default.
- ***56 Spy on Extension in Whisper Mode,** spy on a specific extension in whisper mode. Key in the feature code and follow the prompt.
  For improved security, this feature code is disabled by default.

Call Forward Section

Each of these feature codes are only available to extensions where the specific feature is enabled in the Feature Category that belongs to the Class of Service that is associated with the extension.



Call Forwarding

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:

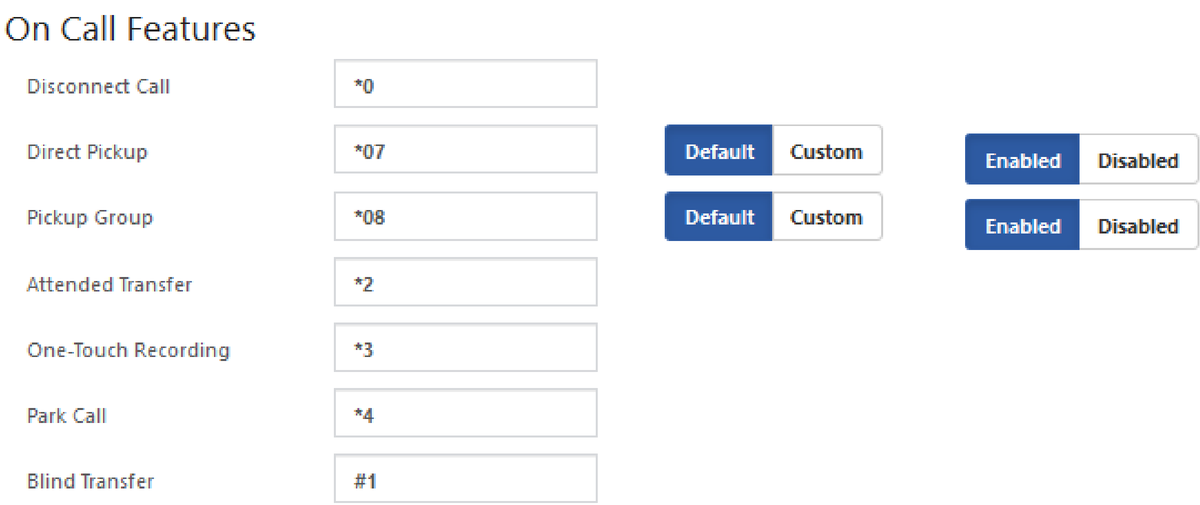
- ***36 Boss/Secretary,** toggle that enables or disables the routing all incoming calls for the current extension to the extension that is defined as the “secretary” phone. Once this function has been enabled**,** only the “secretary” phone will be able to make direct calls to the “boss” phone – all other calls will be routed directly to the “secretary” phone.
The “boss” extension can enable or disable this function by dialing this feature code.
The “secretary” extension can also call this feature code to stop receiving calls that are directed to the “boss” extension – all calls will go directly to the “boss” extension.
This feature code is only available after a “secretary” extension has been defined for the “boss” extension.
- ***58 Call Forward Immediately,** toggles immediate call forwarding.
- ***59 Set CF Immediately Number,** sets the number to which calls should be sent when immediate call forwarding is activated. You can either key in the feature code and follow the prompts, or (in expert mode) key in the feature code followed by * (star), immediately followed by the number to which calls should be forwarded.
- ***60 Call Forward Unavailable,** toggle to enable or disable call forwarding. Calls will be forwarded to the extension defined by the default feature code ***61**.
- ***61 Set CF Unavailable Number,** set the number to which calls should be sent when unconditional call forwarding is activated. You can either key in the feature code and follow the prompts, or (in expert mode) key in the feature code followed by * (star), immediately followed by the number to which calls should be forwarded.
- ***62 Call Forward Busy,** toggle to enable or disable call forwarding when your extension is busy. Calls will be forwarded to the extension defined by the default feature code ***63**.
- ***63 Set CF Busy Number,** set the number to which calls should be sent when call forward busy (CFB) is activated and your extension is busy. You can either key in the feature code and follow the prompts, or (in expert mode) key in the feature code followed by * (star), immediately followed by the number to which calls should be forwarded.
- ***64 Call Forward on No Answer,** 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 the default feature code ***65**.
- ***65 Set CF on No Answer Number,** set the number to which calls should be forwarded when your extension is unable to answer. You can either key in the feature code and follow the prompts, or (in expert mode) key in the feature code followed by * (star), immediately followed by the number to which calls should be forwarded.
- ***66 Do Not Disturb,** toggle to enable or disable the Do Not Disturb (DND) feature.
Incoming calls will be treated as follows when DND is enabled: if Call Forward Unavailable is configured, the call will be forwarded accordingly; if Voicemail is enabled, the call will be sent to voicemail; otherwise the caller will receive the busy tone.

  Do Not Disturb can be set from another extension if Remote DND is enabled in Feature Categories for the extension that wants to make the change. Dial the DND feature code, followed by asterisk (*) and then the extension for which Do Not Disturb is to be activated. For example, dialing *66*2001 will set DND for extension 2001. Dialing the same number again will remove the DND setting from extension 2001.
- ***67 Follow Me,** toggle to enable or disable the Follow Me feature.
- ***69 Clear all Diversions,** dialing this code this will disable all call diversions**,** including the Do Not Disturb feature.

- ***96 Personal Assistant,** toggle to enable/disable the personal assistant for your extension. This option is only available for extensions where **Has Personal Assistant** has been enabled in the **Advanced** tab.

On Call Features Section

Each of these feature codes are only available to extensions where the specific feature is enabled in the Feature Category that belongs to the Class of Service that is associated with the extension.



These facilities are used when you are on a call:

- ***0 Disconnect Call,** disconnect the current call.
  The availability of this feature depends on settings of the dial option parameter in the Custom tab of the Settings>Technology Settings dialogs.
- ***07 Direct Pickup,** capture a call that is ringing at a ***specific*** extension in your pickup group. You will need to key in the feature code followed by the extension number that you want to answer, i.e. key in*072490 to answer a call ringing on extension 2490 (provided that you both belong to same pickup group.)
- ***08 Pickup Group,** capture a call that is ringing at ***any*** extension in your pickup group. To use this facility is necessary to create call group and pickup group in the extensions dialog.
- ***2 Attended Transfer,** transfer the current call to the operator.
  The availability of this feature depends on settings of the dial option parameter in the Custom tab of the Settings>Technology Settings dialogs.
- ***3 One-Touch Recording,** force the current call to be recorded. A single “beep” sound will be played when initiating a recording. If you press the feature code again, two “beeps” will be played indicating that the recording has been paused. You may press the feature code again

to restart the recording – single “beep” will be heard.
The recording for the call will be saved to a single file, even if the recording is paused and restarted.
The availability of this feature depends on settings of the dial option parameter in the Custom tab of the Settings>Technology Settings dialogs.

- ***4 Park Call,** place the current call in the call park. Key in the feature code and follow the prompt.
  The availability of this feature depends on settings of the dial option parameter in the Custom tab of the Settings>Technology Settings dialogs.
- **#1 Blind Transfer,** transfer the current call without notifying the extension to which the call is transferred.
  The availability of this feature depends on settings of the dial option parameter in the Custom tab of the Settings>Technology Settings dialogs.

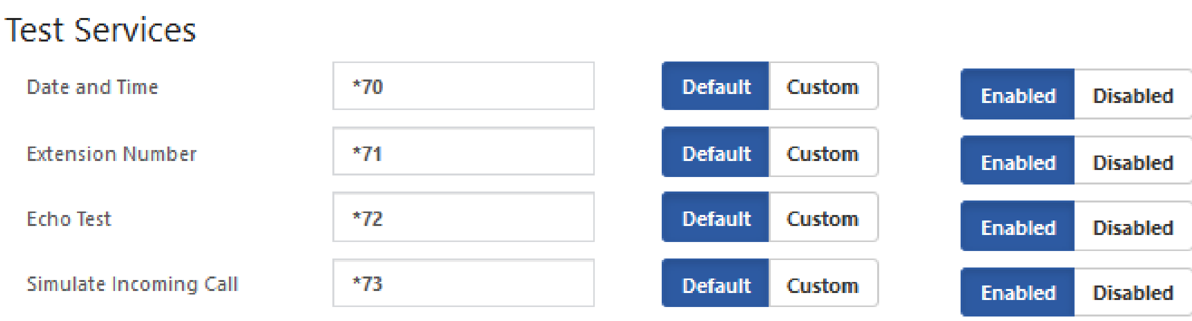
Phonebook Directory Section

This directory is linked to names of extensions: the user will key in the first few letters of the name and will be presented with a list of extension names that match.

- **411 Dial by Name Directory,** key in this feature code and use your numerical keypad to input a user name. For example, the extension for internal support may be called HELP**,** so you can key in **411** (to activate this feature) and then **4357** to reach support

Test Services Section

This feature code is only available to extensions where the specific feature is enabled in the Feature Category that belongs to the Class of Service that is associated with the extension.

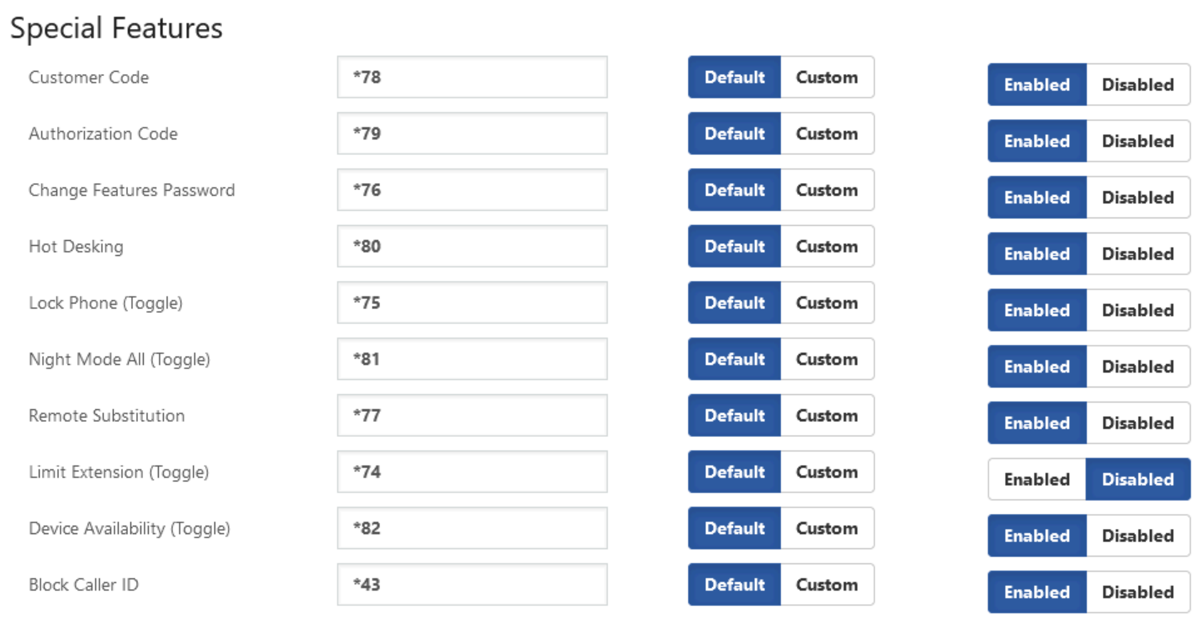


These are a group of features in order to test the system.

- ***70 Speak Date and Time,** will speak the current system date and time.
- ***71 Speak Your Extension Number,** will speak the extension number that you are calling from.
- ***72 Echo Test,** a system echo test to measure the response time.
- ***73 Simulate Incoming Call,** simulate an incoming call to test ringing of the phone.

Special Features Section

Each of these feature codes are only available to extensions where the specific feature is enabled in the Feature Category that belongs to the Class of Service that is associated with the extension.



This is a group of features which are described below:

- ***43 Block Caller ID,** allows the user to block caller ID for a specific call. The user should dial *43nnnnnnnn to block the caller ID for that specific call.

Blocking caller ID must be supported by the trunk provider. Make sure your trunk provider supports this option before using this feature.

- ***74 Limit Extension (Toggle),** allows the user to toggle between the Class of Service normally associated with the user’s extension, and the Limited CoS (defined in the **Limit Extension CoS** field in the Settings>PBX Settings>System General dialog). This can be useful, for example, when the user is out of the offices, and does not want to make available all the features normally associated with the extension.

- ***75 Lock/Unlock Phone,** 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.
- ***76 Change Features Password,** change the password for the current extension in order to access password-protect telephone features. Key in the feature code and follow the prompt.
- ***77 Remote Substitution,** makes it possible for the current phone to make calls as if you are calling from different phone extension.
- ***78 Customer Code,** creates a customer code to be used by the CDR system - very useful for call accounting. Key in the feature code and follow the prompt.
- ***79 Authorization Code,** allows you to make a call from any phone by using an authorization code that is associated with an unrestricted dial plan. Key in the feature code and follow the prompt.
- ***80 Hot Desking,** toggle to enable or disable Hot Desking.

When a Hot Desk devices logs in or out of the system, and entry will be created in the CDR Report, indicating the activity.

- ***81 Night Mode All,** toggle to enable/disable all defined night modes.

If you have 3 night modes defined (as in the example below), and you key in the default feature code *81, it will have the following effect:

NM-1 would change from activated to deactivated

NM-2 would change from deactivated to activated

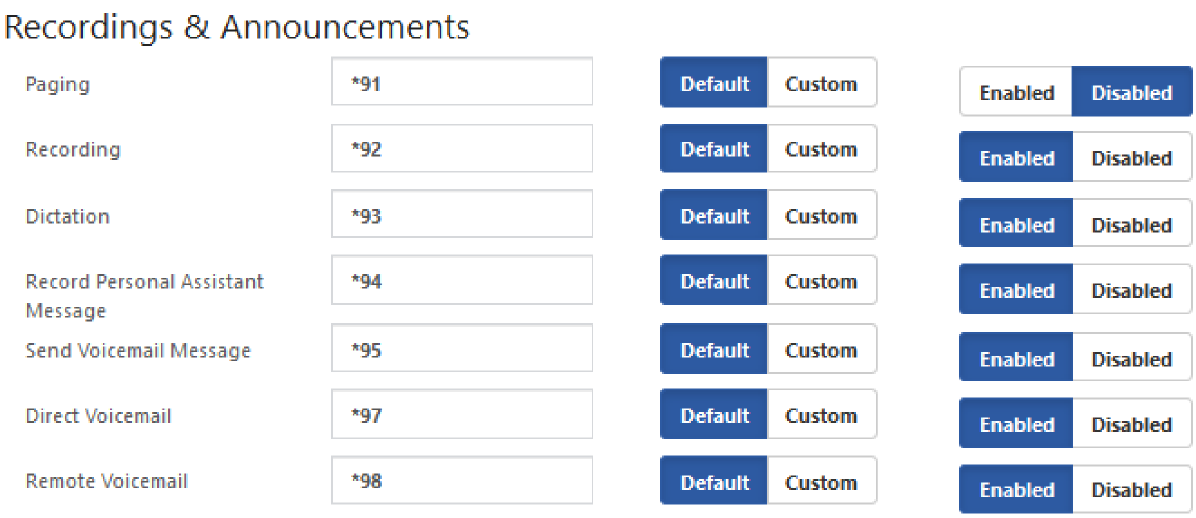
NM-3 defined with **Ignore Global Mode** set to **Yes** would not be changed.

- ***82 Device Availability,** toggle to enable/disable the status of the device used to make the call (e.g. for changing status of the CloudPhone Mobile app, dial *82 from the app)

Recordings & Announcements Section

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

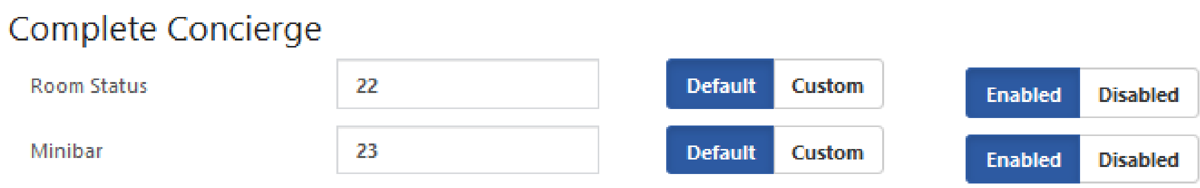
Each of these feature codes are only available to extensions where the specific feature is enabled in the Feature Category that belongs to the Class of Service that is associated with the extension.



- ***91 Paging,** allows you to dial any extension in paging mode. This feature will only work if the device being called supports paging. Key in the feature code and follow the prompts.
- ***92 Custom Recording,** can be used to record a message. Key in the feature code and follow the prompts.
- ***93 Dictation Services,** can be used to record a message with the option of sending it by email. Key in the feature code and follow the prompts.
  This option is only available for extensions where Dictation has been enabled in the Recording tab.
- ***94 Record Msg for Personal Assistant,** record a message that callers will hear when they are served by your personal assistant. Key in the feature code and follow the prompts.
  This option is only available for extensions where **Has Personal Assistant** has been enabled in the **Advanced** tab.
- ***95 Send Voicemail Message,** allows you to call any extension and leave a voicemail message. For example, keying in ***95*2492** will allow you to leave a voicemail message for extension 2492. Note the * that is keyed in between the feature code and the extension number.
- ***97 Direct Voicemail,** 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.
- ***98 Remote Voicemail,** 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. Can also be used as a BLF to monitor and access a shared mailbox. To create a BLF to monitor the shared mailbox 2001, you should create a BLF containing ***982001**

Hospitality Section

This group of feature codes allows you to manage Xorcom Complete Concierge application.

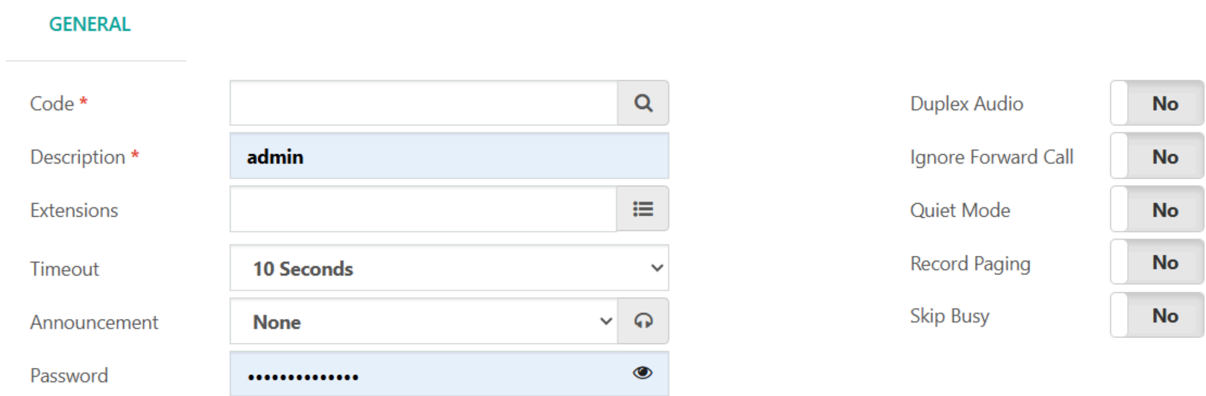


- **22 Room Status,** allows user to enter the status of the room
- **23 Minibar,** allows the user to report on items missing from the minibar

Paging & Intercom Dialog

This dialog creates groups to which users can send a message by dialing a single number. It can also be used to create an intercom between extensions. In both cases, the endpoint (telephone) must be capable of supporting this functionality.

GENERAL Tab



Code*, number to input in order to reach the page or intercom group.

Description*, short description to identify the page or intercom group.

Extensions*, list of the extensions that belong to the page or intercom group.

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

Announcement, an announcement that will be played to recipients when they answer. For example, this can be used for an emergency paging message, such as “Attention all employees, evacuate the facility immediately.”

Password, to protect the Paging Group.

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. In other words**,** how to behave when paging an extension that has call forwarding enabled.

Quiet Mode, just broadcast to the extension**,** without playing a beep to caller at the beginning of the page call.

Record Paging, record the page message in a file.

Skip Busy, dials a channel only if the device state is **NOT_INUSE**. This option may not behave as expected on an endpoint (telephone) that supports multiple lines.

MulticastRTP Section

In this section, you can configure multicast pagin. This feature is particularly useful when you need to use multiple devices for paging while minimizing resource usage.

Multicast IP Address, enter the multicast IP address to be used for paging.

Port, specify the port number for the multicast paging.

Enable, toggle to enable or disable multicast paging.

NOTE that for multicast to work properly, both the phones and the PBX must be on the same network. This functionality cannot be used with MT Manager tenants.

Pickup Groups Dialog

Pickup Groups allow you to group a number of extensions into a single group. The call group and pickup group options allow users to pick up calls that are not directed to them by dialing a system-defined feature code (***08**).

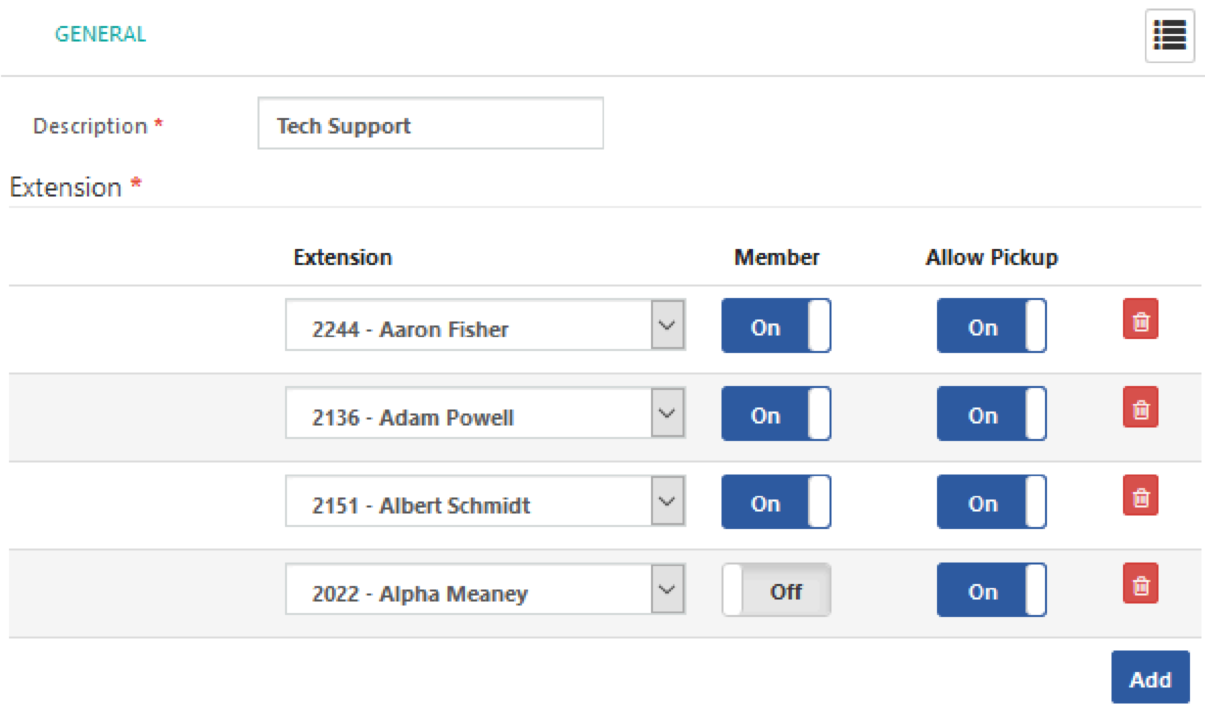
A maximum of 64 pickup groups is allowed.

Calls directed to any phone in a particular call group can be answered by any user who is a member of the same 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 by dialing ***08**. This can be useful for small office or home setups, where it is easier to simply pick up a call from your current phone rather than forward that call to another extension. You should note that an extension can belong to multiple pickup groups.

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 calls directed to any member of his department**,** but members of the department should not be able to pick up calls directed to the senior staff member.

In the example below, Alpha Meaney can pickup calls to Aaron Fisher, Adam Powell, and Albert Schmidt, but nobody can pickup calls directed to Alpha Meaney.

GENERAL Tab



Description*, a free-text description to identify the pickup group.

Extension Section

Extension, any extension that you want to make a member of the group.

Member, when **On,** indicates that the extension is a member of the pickup group. You can temporarily remove members from the group by changing this status to **Off**.

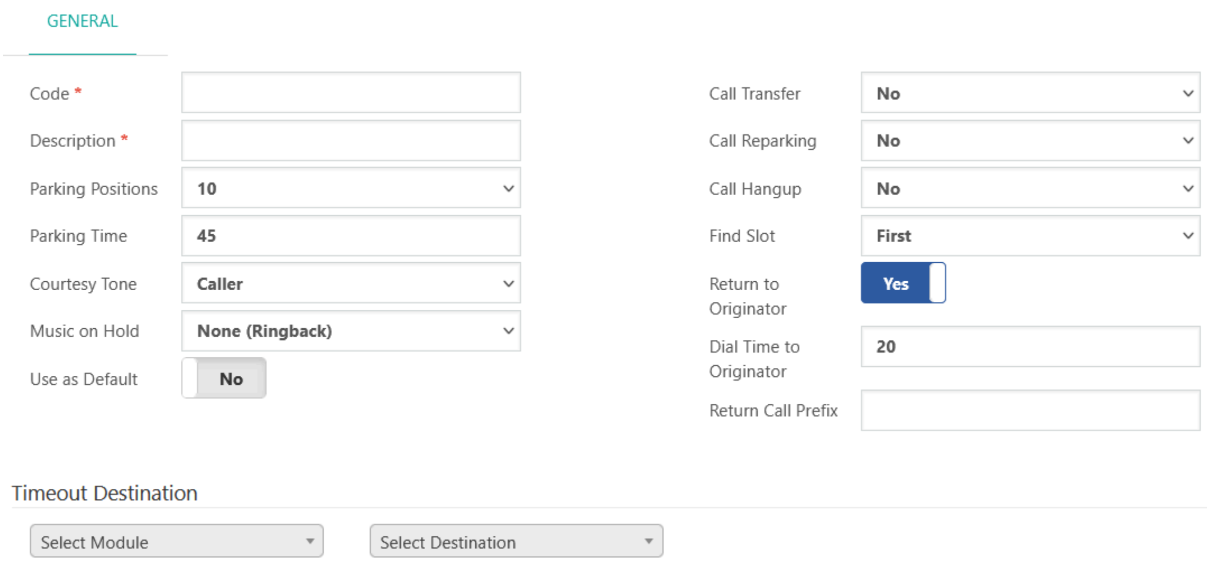
In the example above, Amy Cole can pickup calls to Aaron Fisher and Albert Schmidt, but nobody can pickup calls directed to Amy Cole.

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

Parking Dialog

The Call Parking feature allows you to place a caller on hold. The call can then be retrieved from any phone, anywhere on the system.

GENERAL Tab



Code*, number to call in order to reach the parking service.

Description*, a free-text name to identify the park**.**

Parking Positions, controls the range of parking slots to be allocated.

Parking Time, length of time (in seconds) that a call can be parked before being returned to the person who 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 Music on Hold to use for music on the parked channel.

Use as Default, when set to **Yes**, indicates that this parking lot should be the system-wide default parking lot.

Call Transfer, this is a toggle to enable or disable DTMF-based transfers when picking up a parked call.

Call Reparking, this is a toggle to enable or disable DTMF-based parking when picking up a parked call.

Call Hangup, this is a toggle to enable or disable DTMF-based hang up when picking up a parked call.

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

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

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

Dial Time to Originator, when a parked call times out**,** this is of the length of time (in seconds) to call the person who originally parked the call.

Return Call Prefix, prefix to prepend to CID Name. Can be used to indicate to the originator which parking lot the call comes from.

Timeout Destination Section

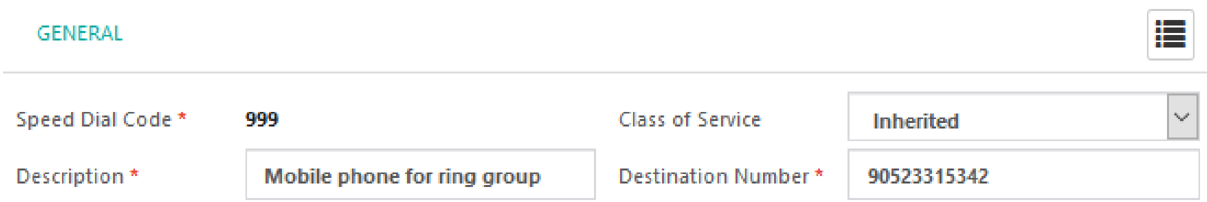
Select Module, select the dialog to be used when a parked call times out.

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

Speed Dialing Dialog

This feature permits fast dialing of frequently used numbers**,** or to simplify dialing by substituting short codes to call long numbers.

GENERAL Tab



Speed Dial Code*, number to dial in order access the Speed Dial. Can consist of digits, as well as asterisk (*) and hashtag (#) characters. Must be unique.

Description*, free-text to identify the Speed Dial.

Class of Service, class of service to be associated with the Speed Dial.

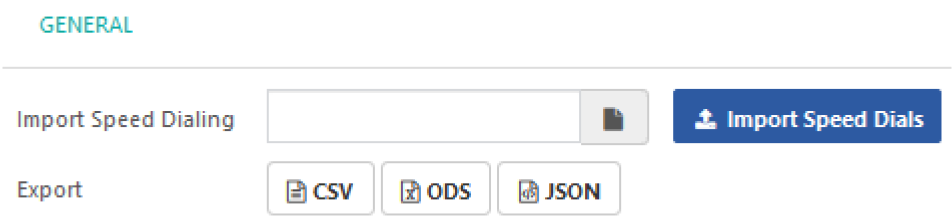
Destination Number*, the number that will be dialed by the Speed Dial. If the target is an external number**,** the number should include any necessary digits required to access an outbound route.

Import/Export Speed Dialing Dialog

This dialog allows the users to externally create speed dial list in a CSV file, and upload the file containing all the speed dials. It also enables the user to download a CSV file containing all the existing speed dials, and edit them.

You can create a template file by using the Export Speed Dial action button to create a file in the proper format.

GENERAL Tab



CSV File, Location and name of the CSV file to be imported. This field is only required when ***importing*** speed dial information.

Action Buttons

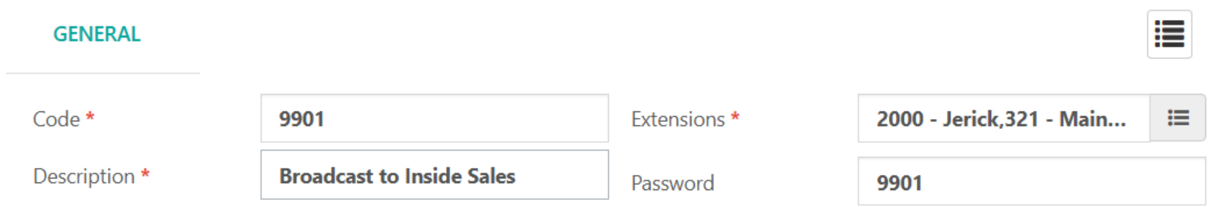
Import Speed Dialing, action button to import speed dial information from the named CSV file

Export, action button to export speed dial information to CSV, ODS, or JSON file. After pressing the button, you will be asked for details of the file.

Voicemail Broadcast Groups Dialog

Group of extensions to which voicemail can be sent.

GENERAL Tab



Code*, the number to call in order to broadcast a voicemail to multiple extensions.

Description*, a free-text description to identify the Voicemail Broadcast Group

Extensions*, drop-down list of extensions to which group voicemail will be broadcast. Note that only extensions that have active voicemail will be displayed.

Password, password to protect the Voicemail Broadcast Group

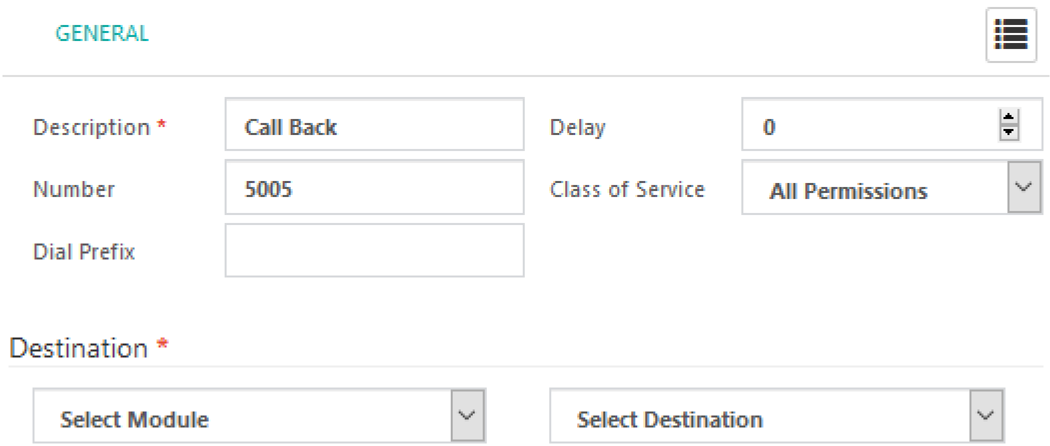
Call Back Dialog

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 direct access to all the facilities of the system. This is especially relevant in the case of mobile phones where incoming calls are usually significantly cheaper than outgoing calls.

Note that the initial call to the PBX (initiating the callback) will not be answered in order to avoid charges for the initial call.

The callback target may connect the caller with any resource on the system, 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 system dial tone from which they can call any telephone number they wish.

GENERAL Tab



Description*, free-text description to identify the callback.

Number, is the telephone number that the system will call to reconnect with the caller after the call that initiated the callback is terminated.

If the field is left blank, the system will call back to the CID number associated with the caller that requested the callback.

The number must be in a format that can be matched by one of the outbound routes configured in the Outbound Routes section of the system. 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 could never be completed. If the field is left blank, then the system will attempt to call back to the caller ID number that initiated the callback.

Dial Prefix, a number that should always be prefixed to the call back number. For example, this could be the code required to access an outbound route.

Delay, delay, in seconds, before attempting to return the call.

Class of Service, Class of Service to be used when making the call back.

Destination Section*

Select Module, to choose which dialog should be activated after the call back has successfully completed the call back.

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

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

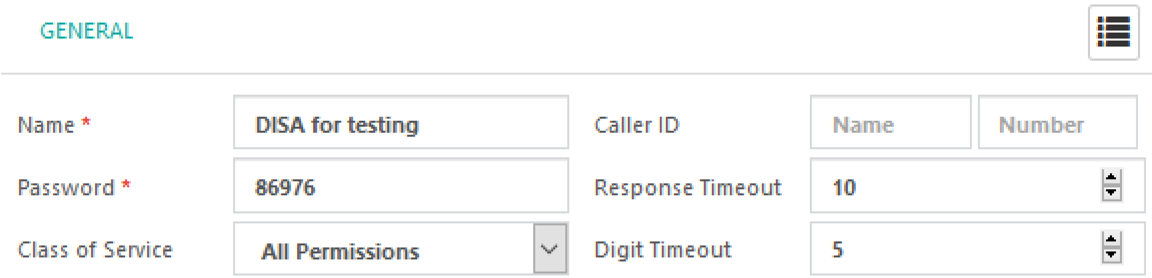
- A company where employees need the ability to check their voicemail from anywhere. Calling the toll-free company phone number costs the company too much money. A callback target could be set up to call back the incoming caller ID, and be directed to the miscellaneous destination of *98. Callers would 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 call 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.

DISA Dialog

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

GENERAL Tab



Name*, free-text description to identify the DISA when it is being selected as a call target from other dialogs in the system.

Password*, used to authenticate a caller who wants to activate the DISA feature. The caller attempting to access DISA will be prompted to enter the password, which must match the value of the password field. If the user is unable to provide the correct password, the call will be disconnected and the caller will not be able to access the DISA feature.

Class of Service, specifies Class of Service that should associated with the DISA.

Caller ID, is used to set the outbound caller ID (CID) of any of the calls that are placed from the DISA. This is an optional field: if the field is left blank, then the caller ID of the person placing the call will be used. The desired caller ID should be specified in the format of Caller-Name <##########>

- Caller-Name will be replaced with the name that should be set for outbound calls
- ########## will be replaced with the phone number that should be set for outbound calls

An example of Caller ID could be something like **Packet Publishing <5551234567>**.

Response Timeout*, specifies length of time (in seconds) that the system will wait for initial input before disconnecting the call. The default value is 10 seconds. This timeout will be applied when

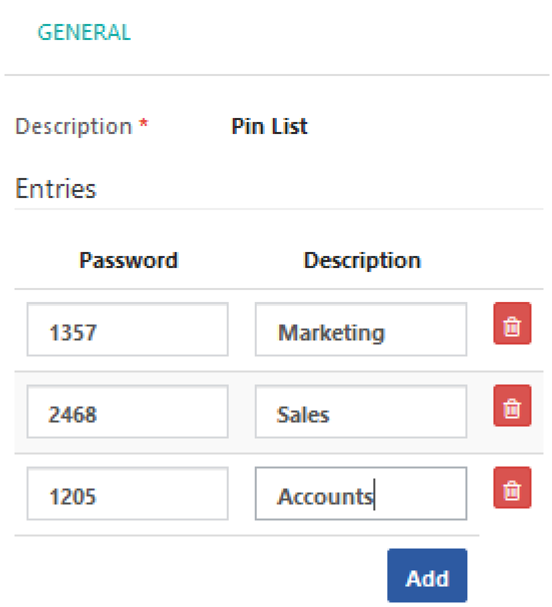
- caller has not entered any digit
- caller has partially entered a number to call without finishing the entry.

Digit Timeout, specifies how long the system will wait between digits before beginning to dial the call. If a caller begins entering digits and then stops, the system will wait for the number of seconds specified in the field, before sending the entered digits to the system for dialing. The default value for the 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.

PIN Lists Dialog

List of PIN numbers that can be associated with an outbound trunk. Any extension that wants to make a call using a PIN-protected outbound route will be asked for a PIN number.

GENERAL Tab



Description*, a free-text description for the PIN list.

Entries Section

Password, a password that can be used. A password may consist of any combination of numbers and the ***** (star) symbol. If you want add multiple passwords**,** you can do so by using the **Add** button.

Description, allows you to add a free-text description for each password

Add, press this button to open a new line so that you can add another entry to the current PIN list

Emergency Dialog

This dialog allows you to define numbers that can be dialed in an emergency, and how to handle them.

Note that the user does not have to dial the access code for the Outbound Route. For example, if emergency calls to 911 are routed to an Outbound Route that normally requires an access code of **9**, the user will only need to dial **911** (and not **9911)**

GENERAL Tab

Number*, enter the number that user calls in an emergency, for example, 911.

Note that this number cannot be used as an extension number, or as the number to access any other applications, such as Queue, Ring Group, etc.

Description, free-text description to describe this emergency number

Email list, one, or more, email addresses that should receive a notification when the emergency number is dialed. Each email address should be entered on a separate line.

Destination* Section

Select Module, allows you to choose from a drop-down list of available modules, which dialog should be activated. The available modules are:

- Custom
- Custom Applications
- Outbound Routes
- Trunks

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

Make sure that the target Outbound Route is configured to accept the emergency number. For example, if your emergency number is **911**, make sure that the target Outbound Route allows this number to be dialed.

Class of Service Menu Group

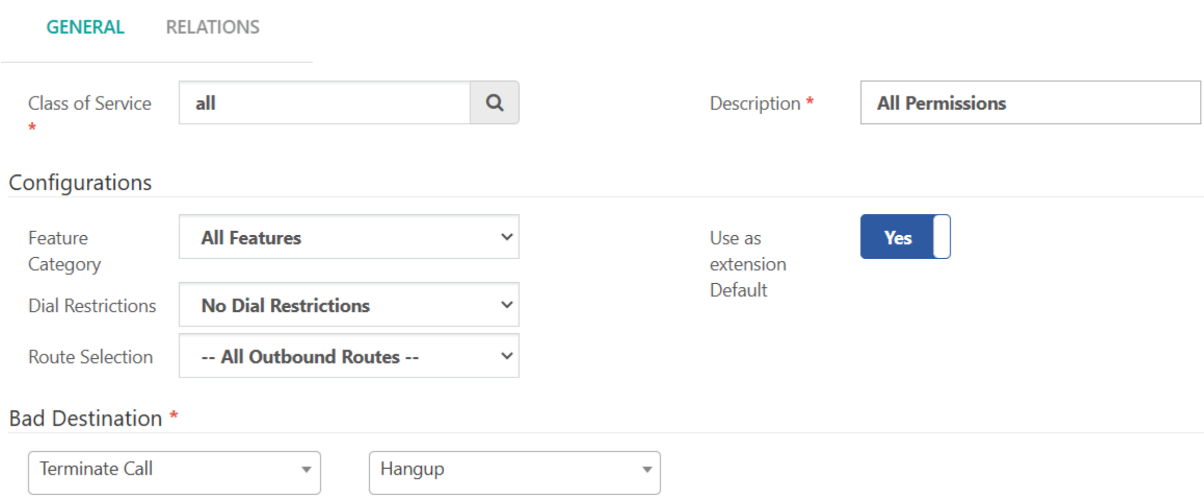
Class of Service Dialog

Group of settings that define the dial plan that the extension can access.

Each Class of Service includes three components, which you should configure, before creating a Class of Service. The three components are:

- Feature Category, defined in the Feature Categories dialog
- Dial Restrictions, defined in the Dialing Restriction Rules dialog
- Route Selection, defined in the Route Selections dialog.

GENERAL Tab



Class of Service*, Class of Service name (must be unique).

Description, a free-text description to identify the Class of Service.

Configurations Section

Feature Category, features**,** as defined in the Feature Categories dialog**,** which are allowed for the Class of Service.

Dial Restrictions, dialing restrictions**,** as defined in the Dialing Restriction Rules dialog **that** are allowed for the Class of Service.

Route Selection, dial routes**,** as defined in the Route Selection dialog **that** are allowed to use the Class of Service.

In addition to selecting from user-defined route selections, you can also use the system-defined route, named **None**: this route will restrict the Class of Service to internal calls only.

Use as Extension Default, if this field is set to **Yes**, this Class of Service will be used at the default Class of Service when you create a new extension. Only one Class of Service can be configured as the default: as soon as you configure a Class of Service to be the default, this flag will be turned off for the Class of Service that was previously configured as the default.

Bad Destination Section

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

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

RELATIONS Tab

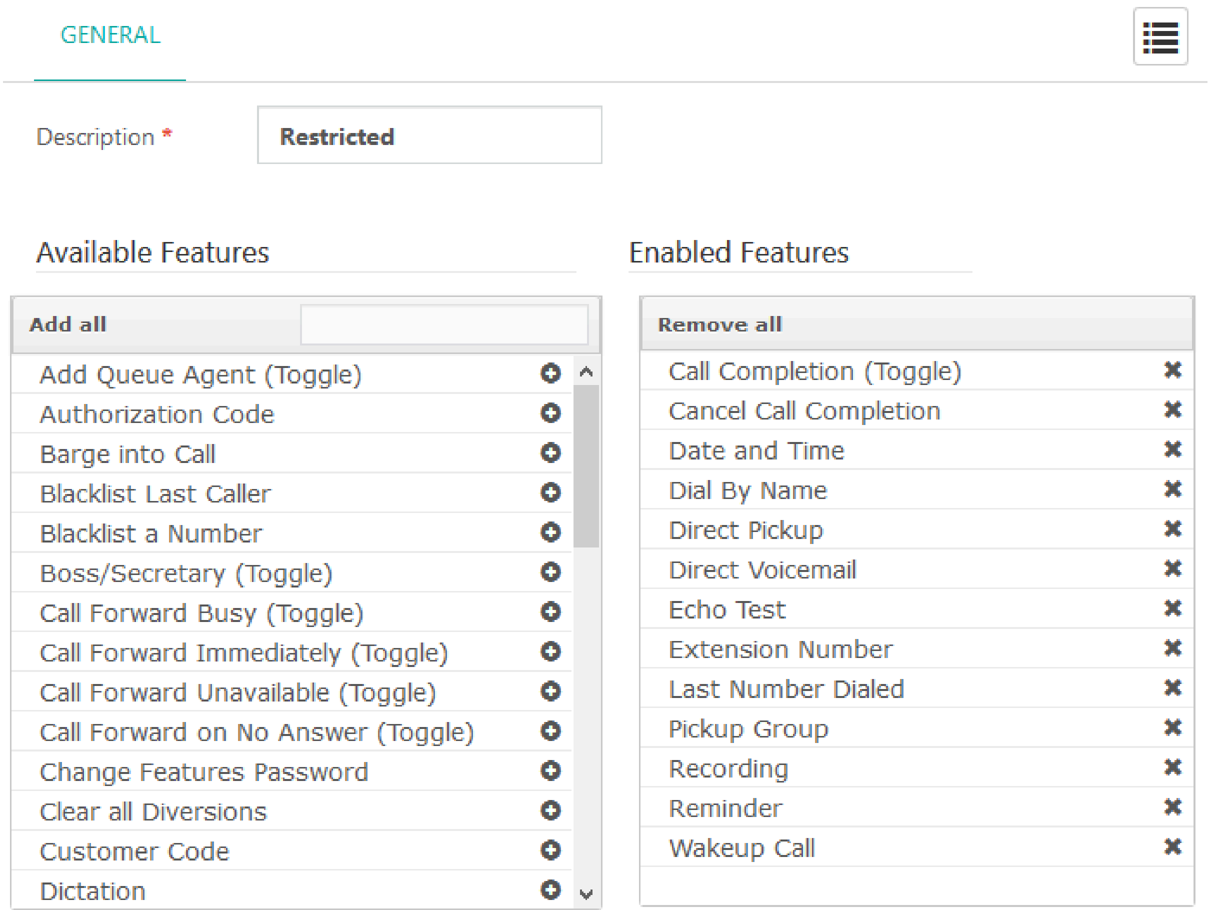
This tab provides a graphical display all the modules that are used by the Class of Service that you are currently viewing. This allows you to see at a glance all modules that are associated with the currently-selected Class of Service.

Feature Categories Dialog

In this dialog 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. These can be associated with a Class of Service.

GENERAL Tab

In this tab you will be able to configure which Feature Codes should be included in a Feature Category.



Description*, a free-text title to identify this feature category - must be unique.

Available Features, list of available feature codes.

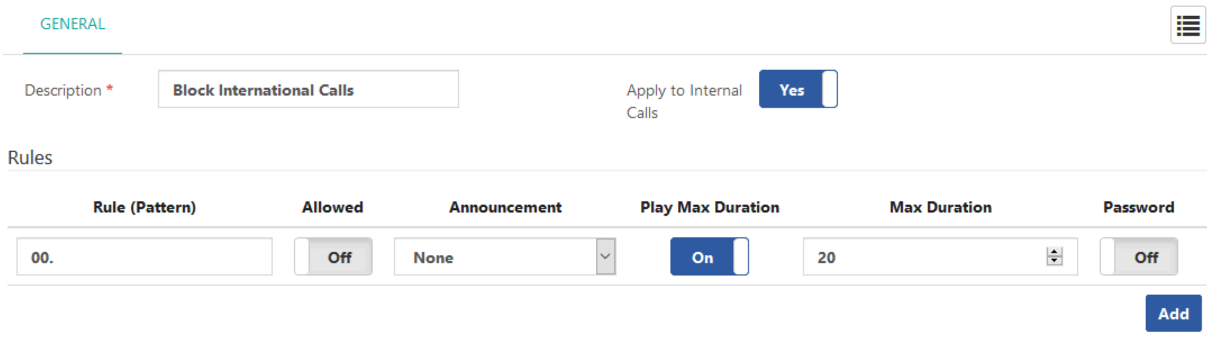
Enabled Features, list of feature codes that have been included.

Dialing Restriction Rules Dialog

Here you can create dialing restrictions rules. These can be associated with Classes of Service.

This dialog gives you control of both internal and external dialing. You can use these rules to block access to designated internal or external numbers, by using patterns to block them. When a rule consists of multiple lines (or patterns), the dialed number is tested against each pattern, starting from the first pattern, until a match is found. Once a match is found, it is implemented (either allowed or blocked), and no further patterns are tested. If no match is found, the call will be allowed.

GENERAL Tab



Description*, a free-text title (which can include special characters) to identify the Dialing Restriction Rule - must be unique.

Apply to Internal Calls, when set to **Yes**, allows you to determine that the current Dialing Restriction Rules will apply to both internal and external calls. If set to **No**, the rules will not apply to internal calls.

Internal calls includes not only Extensions, but also Feature Categories, and all other destinations (such as Ring Groups, Queues, Speed Dialing, etc.)

Rules Section

Rule (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
- The asterisk (*) character matches an asterisk character in a dialed number, allowing you to manage system-defined feature codes

Allowed, when set to Yes, this pattern will be allowed. Otherwise, the pattern cannot be dialed.

Announcement, choose an announcement associated with this pattern. This announcement will be play when a user attempts to call a number (as defined by the Rule) that is not allowed.

Use Xorcom voice recording services to ensure that you have high-quality, professional announcements. You can count on the continuity of our professional services so that whenever you would like to change or add a recording, you will be able to use the same professional voice for a coherent customer experience.

Play Max Duration, when set to **On,** will play a message indicating the maximum call duration allowed on this route.

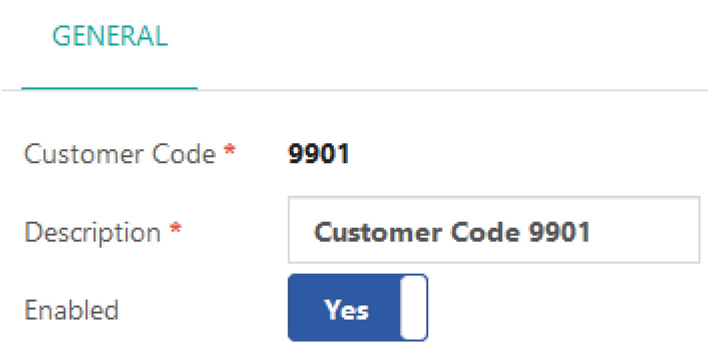
Max Duration, maximum call duration**,** in seconds**,** associated with the announcement for the rule.

Password, determine whether a password is required when using this rule. The password is the Features Password associated with the user's extension.

Customer Codes Dialog

Customer codes associated dynamically to a call in order to register this code in the CDR. The customer code can be associated with an outbound call by dialing the Customer Code feature code (by default, ***78**) prior to making an outgoing call.

GENERAL Tab



Customer Code*, customer code number.

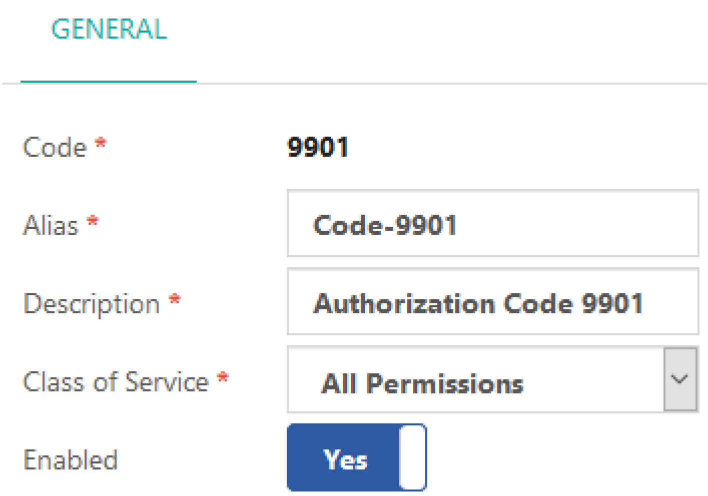
Description*, free-text description to identify this customer code.

Enabled, enable/disable this customer code.

Authorization Codes Dialog

Code that grants privilege to make a call from any extension. Use the Authorization Code feature code (by default, ***79**) to activate this option.

GENERAL Tab



Code*, authorization code number.

Alias*, alias to identify this authorization code. For security reasons, this alias will appear on CDR reports in place of the authorization code.

Description*, a free-text description to identify this authorization code.

Class of Service, Class of service that is used to route the call.

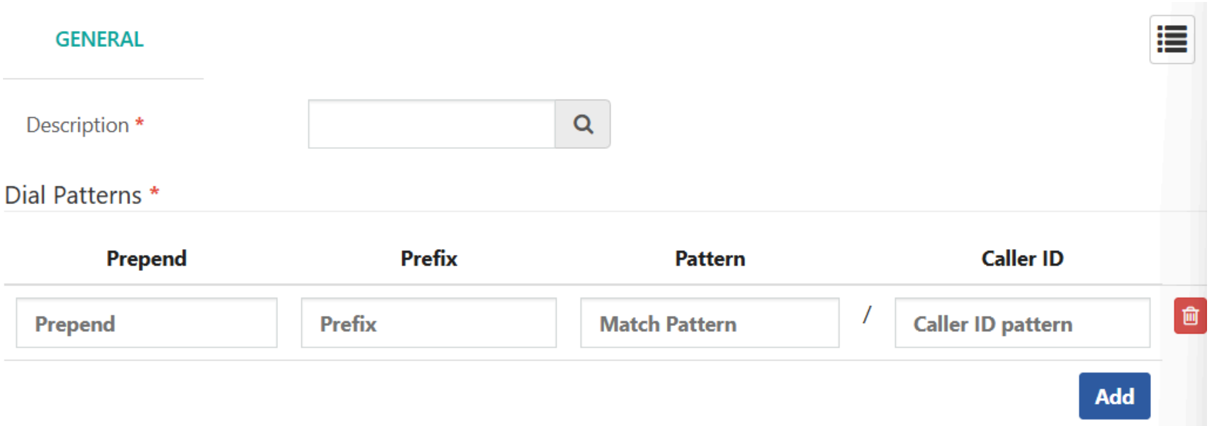
Enabled, toggle to enable/disable this Authorization Code.

Number Manipulation Dialog

Number manipulation enables administrators to create advanced dialed number transformation rules customized for specific user groups. With this you can Route calls differently based on the combination of CoS and dialed number. For example:

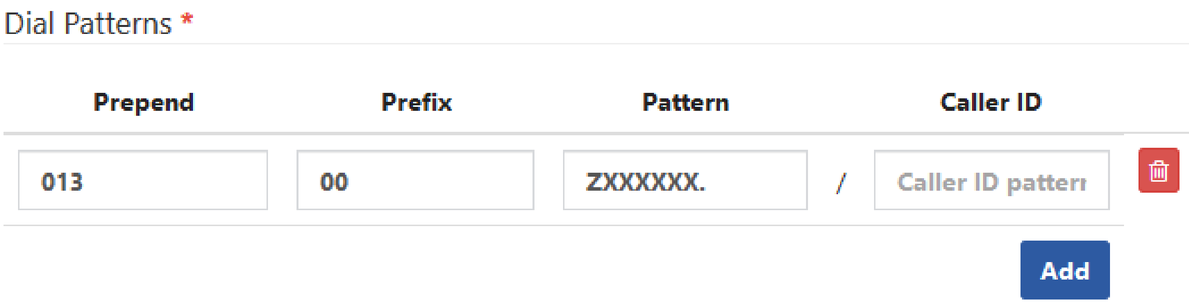
- Group A dialing 0 connects to extension 200
- Group B dialing 0 connects to extension 300

GENERAL Tab



Description*, a free-text description to identify this number manipulation group.

Dial Patterns Section



Prepend, digits to add to a successful match. You can also use the **w** character to create a half second delay in the dial sequence for analog lines. You can use multiple **w** characters to create longer wait periods.

Prefix, prefix to remove from a successful match. You can use standard pattern-matching characters in this field. Standard pattern matching options are:

- **X** - X or x represents a single digit from 0 to 9.
- **Z** - Z or z represents any digit from 1 to 9.
- **N** - N or n represents a single digit from 2 to 9.
- **.** - can be used as a wildcard to match one or more characters.
- **!** – can be used as a wildcard to match zero or more characters.
- **[1237-9]** - matches any digit/s or letter/s 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

Pattern, allows you to create one or more patterns in the dial plan that match possible dialed numbers.

Standard pattern matching options are:

- **X** - X or x represents a single digit from 0 to 9.
- **Z** - Z or z represents any digit from 1 to 9.
- **N** - N or n represents a single digit from 2 to 9.
- **.** - can be used as a wildcard to match one or more characters.
- **!** – can be used as a wildcard to match zero or more characters.
- **[1237-9]** - matches any digit/s or letter/s 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 that you create allow you to make 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.

Examples

- **07[2-4679]XXXXXXX** will allow calls to all 10 digit numbers that start with 072, 073, 074, 076, 077, or 079
- **1200XXXXXX** will allow calls to all 10 digit numbers that start with 1200
- **12551.** will allow calls to any number that begins with 12551

Caller ID, allows you to create patterns in the dial plan that match one or more CID numbers that initiate the call

Standard pattern matching options are:

- **X** - X or x represents a single digit from 0 to 9.
- **Z** - Z or z represents any digit from 1 to 9.
- **N** - N or n represents a single digit from 2 to 9.
- **.** - can be used as a wildcard to match one or more characters.
- **!** – can be used as a wildcard to match zero or more characters.
- **[1237-9]** - matches any digit/s or letter/s 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 that you create allow you to make 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.

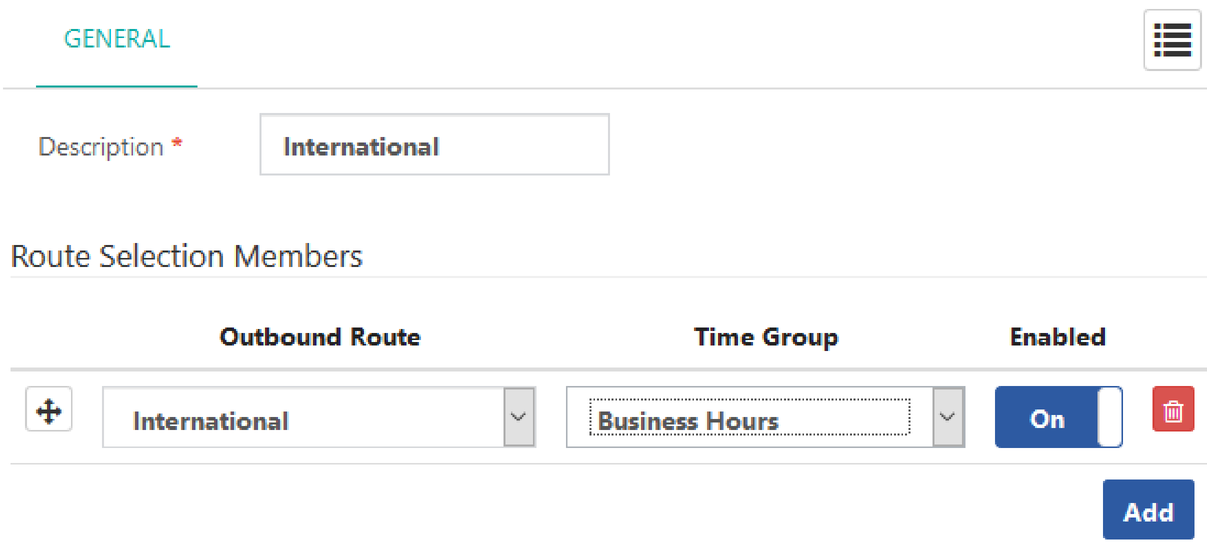
Example

- **49903278** will allow calls to any number to the defined pattern that originates from an extension that has a CID of 49903278

Route Selections Dialog

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

GENERAL Tab



Description*, a free-text description to help identify this Route Selection. The description must be unique.

Route Selection Members Section

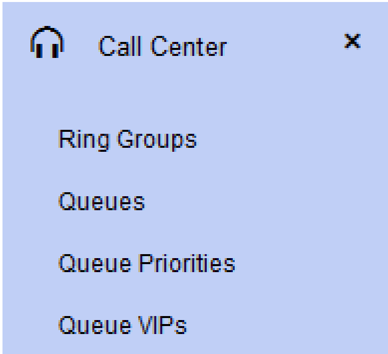
You can use the **Add** button at the bottom of the dialog to add addition route selection members.

Outbound Route, select an existing outbound route to which this should apply.

Time Group, select an existing time group that should be applied to this route selection. The route selection will always be applied if no time group is associated with the route selection

Enabled, toggle to enable or disable this route selection.

Call Center Menu Group



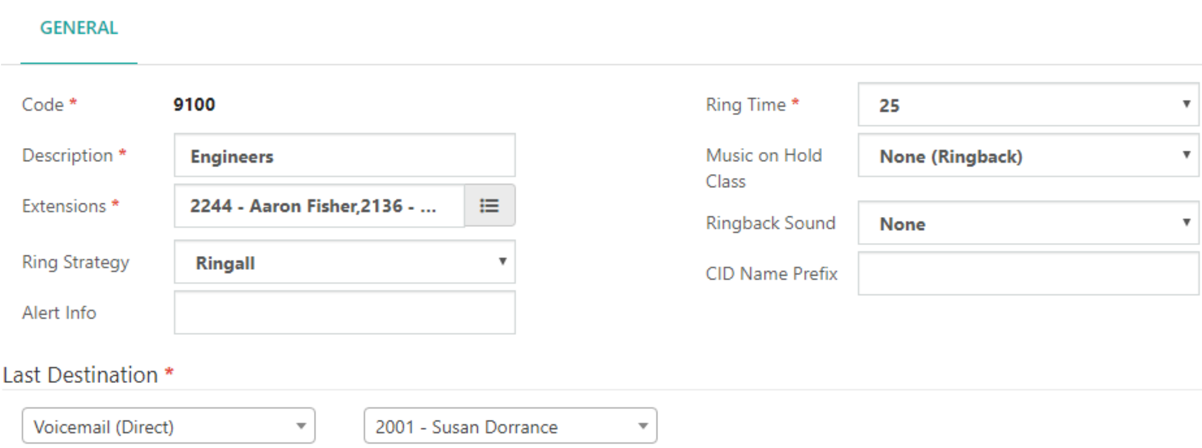
Ring Groups Dialog

Ring Groups allows calls to be received by multiple internal destinations.

Ring Groups allow you to create a single number (the Ring Group code) that will call more than one person. For example, you could define a Ring Group so that when any user dials extension 9101, extensions 2029, 2030, and 2031 will ring for 15 seconds, after which the call will go to the voicemail for extension 2090.

A ring group allows one call to ring any number of endpoints. It is typically used for a particular department or section of a building. A company might use a ring group to ring all phones in the sales department. A home might use a ring group to ring all phones on a particular floor. Ring groups must be set up prior to selecting them as a call target

GENERAL Tab



Code*, number to reach the ring group.

Description*, a free-text description to identify the ring group.

Extensions*, list of extension for the ring group.

Ring Strategy, ring strategy of extension group. Available options are:

- **Ringall** - simultaneously ring all extensions in the list until one answers, or until the Ring Time limit has been reached.
- **One by One** – ring one extension at a time. If the first extension does not answer within the Ring Time, call the next extension in the list.

Alert Info, optional SIP alert-info content, which can be used to trigger device-specific features, such as customized ringtones.

Ring Time*, ring time in seconds, MAX 3600 seconds.

Music on Hold Class, music on hold to play when the call is placed on hold.

Ringback Sound, music on hold to play while waiting for the call to be answered. If None is selected. The country-specific ringback sound will be played.

CID Name Prefix, prefix to append to CID for calls to the ring group. This allows a user answering the call to see which ring group is being called. This can be useful when an extension belongs to multiple ring groups

Last Destination Section

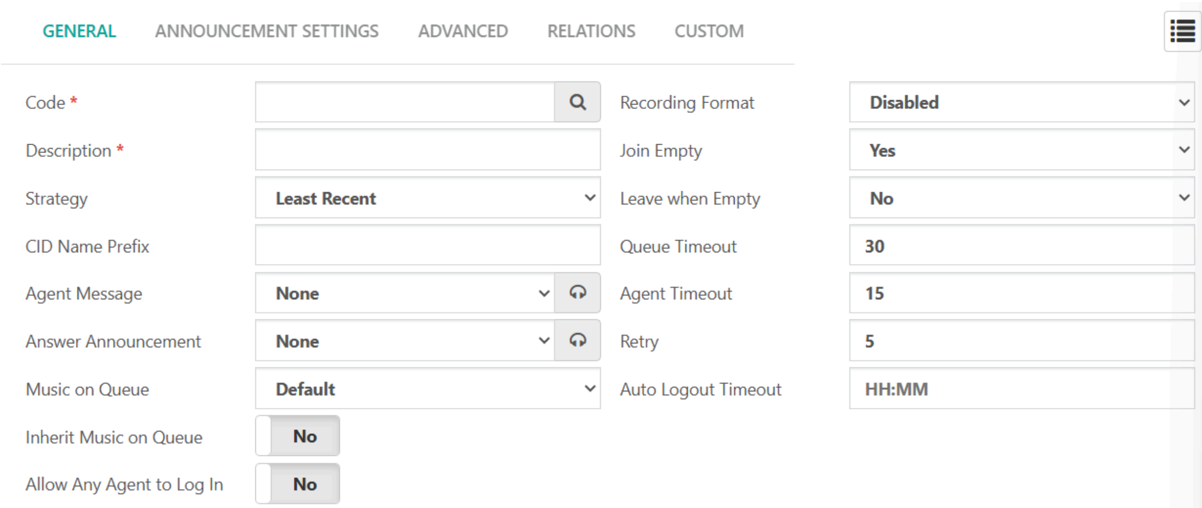
Select Module, allows the user to choose from a drop-down list of available dialogs, which dialog should be activated.

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

Queues Dialog

ACD (Automatic Call Distributor) allocates the incoming calls, in the order of arrival, to the first available call center 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. The Queues module allows for more than 190 queues, ensuring flexibility and efficient call management. Additionally, it is possible to automate the creation of queues via a script and determine the order of calls distribution according to the order of the agents. Balancing the workload among call center agents ensures that each caller receives prompt and professional service.

GENERAL Tab



Code*, number to reach the queue.

Description*, a free-text description to identify this queue.

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

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

CID Name Prefix, prefix to prepend to the Caller ID for this queue. This can help an agent who is a member of multiple queues by telling him to which queue the incoming call belongs.

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

Use Xorcom voice recording services to ensure that you have high-quality, professional announcements. You can count on the continuity of our professional services so that whenever you would like to change or add a recording, you will be able to use the same professional voice for a coherent customer experience.

Answer Announcement, allows you to configure a message that will be played to the caller when any agent accepts a call. For example, "You are now being connected to a sales agent."

Music on Queue, set the class of music for this queue.

Inherit Music on Queue, uses the Music on Queue defined for the queue when set to **No**, when set to **Yes** the queue will inherit Music on Hold from the incoming channel. This can be useful when you have multiple routes to access a queue, but you want to play unique Music on Hold (which may be a specific announcement), depending on how the queue was accessed.

Allow Any Agent to Log In, setting this field to **Yes** will enable any agent to log in to this queue, even if not specified on this list. Note that only agents that are specified on the list will log in to this queue using Queue Login/Logout (to all queues).

Using the feature codes for logging into all queues and logging out of all queues by a dynamic agent will NOT affect queues in which the agent is not set up as an agent. A log into/out of a queue in which the dynamic agent is not set up should be done directly to that specific queue.

Recording Format, specifies the file format to use when recording. If the "disabled" option is selected**,** queue recording is not performed. Valid recording formats are:

- GSM
- WAV
- WAV49

Join Empty, determines whether a caller can be added to the queue even if there are no agents currently active in the queue.

Leave When Empty, determines whether to remove callers from the queue if there no longer any agents servicing the queue.

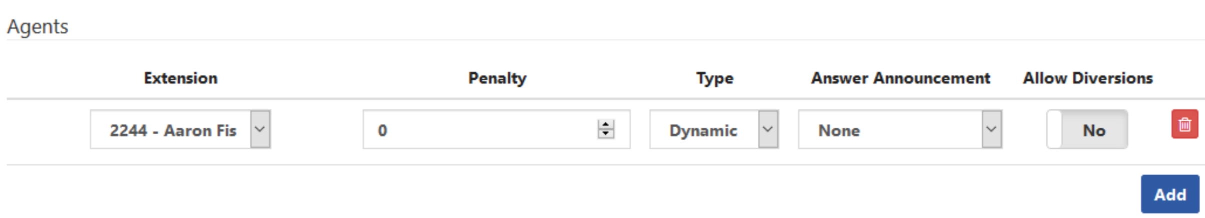
Queue Timeout, determines the maximum time a caller can try to reach an agent before being passed the destination defined in the Last Destination field.

Agent Timeout, determines for how long to ring an agent.

Retry, determines how long to wait before trying to call the next agent in the queue.

Auto Logout Timeout, defines the maximum session duration for agents in HH:MM format. Once this time is reached, agents with Auto Logout enabled will be automatically logged out from the queue.

Agents Section



Use the **Add** button at the bottom of the dialog to add additional agents. Existing agents can be removed by clicking on the appropriate trash icon.

Extension, extensions that can be agent in this queue.

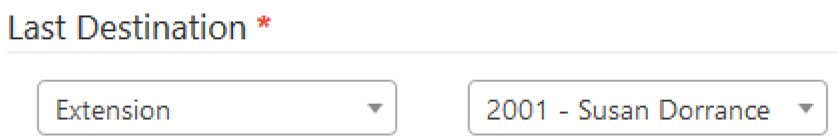
Penalty, agents with the lowest penalty will be called first. If no low-penalty agents are available**,** agents with the next highest penalty will be called.

Type, can be either static or dynamic. Static agents will always be in the queue**,** these agents do not need to log in. Dynamic agents are the agents who will be allowed to log in the call queue.

Answer Announcement, allows you to configure a message when the agent accepts a call. This announcement can be in addition to the Answer Announcement (if defined) that is linked to the queue. For example, "You are now being connected to Jackie Stewart, our space travel expert."

Allow Diversions, if this field is set to **No,** diversions**,** such as Follow Me**,** will be ignored.

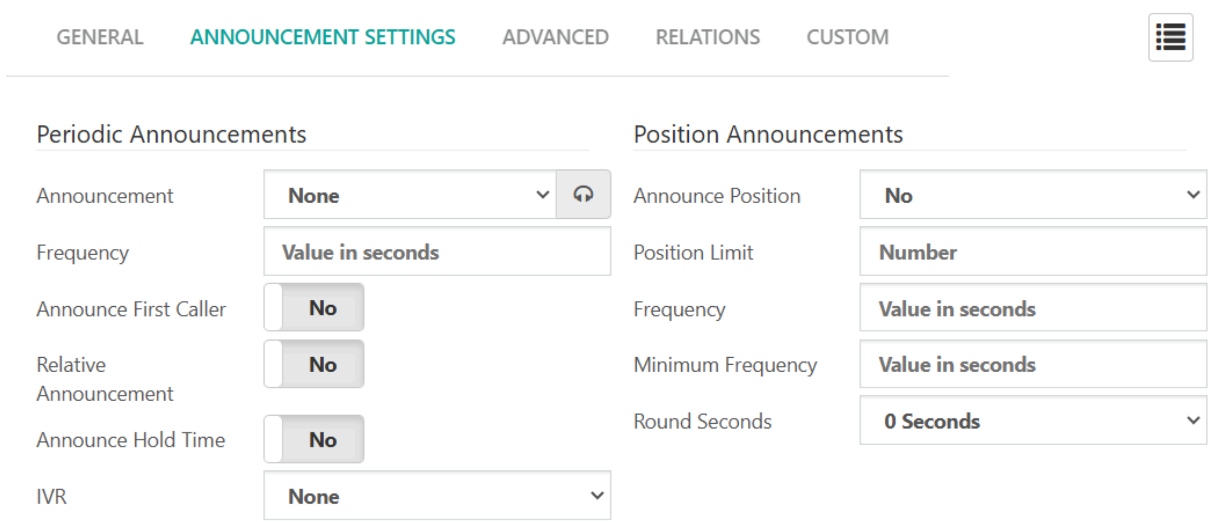
Last Destination Section*



Select Module, allows the user to choose from a drop-down list of available dialogs**,** which dialog should be activated when the system is not able to service a queue customer.

Select Destination, is the call target to which the call should be routed when the system is not able to service a queue customer.

ANNOUNCEMENT SETTINGS Tab



Periodic Announcements Section

Announcement, periodic announcement to provide information to the caller about their status in the queue. The system default message is something like "All representatives are currently busy assisting other callers. Please wait for the next available representative.”

Use Xorcom voice recording services to ensure that you have high-quality, professional announcements. You can count on the continuity of our professional services so that whenever you would like to change or add a recording, you will be able to use the same professional voice for a coherent customer experience.

Frequency, 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
- not playing it too frequently.

Announce First Caller, 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 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.

IVR, an IVR may be specified, allowing the user to enter a single digit while they are in the queue, in order to reach a destination that is defined in the IVR.

Position Announcements Section

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 caller’s position will never be announced
- **Yes**: The caller's position will always be announced
- **Limit**: The caller will hear their position in the queue only if it is within the limit defined by Announce Position Limit.
- **More**: The caller will hear their position if it is beyond the number defined by Announce Position Limit.

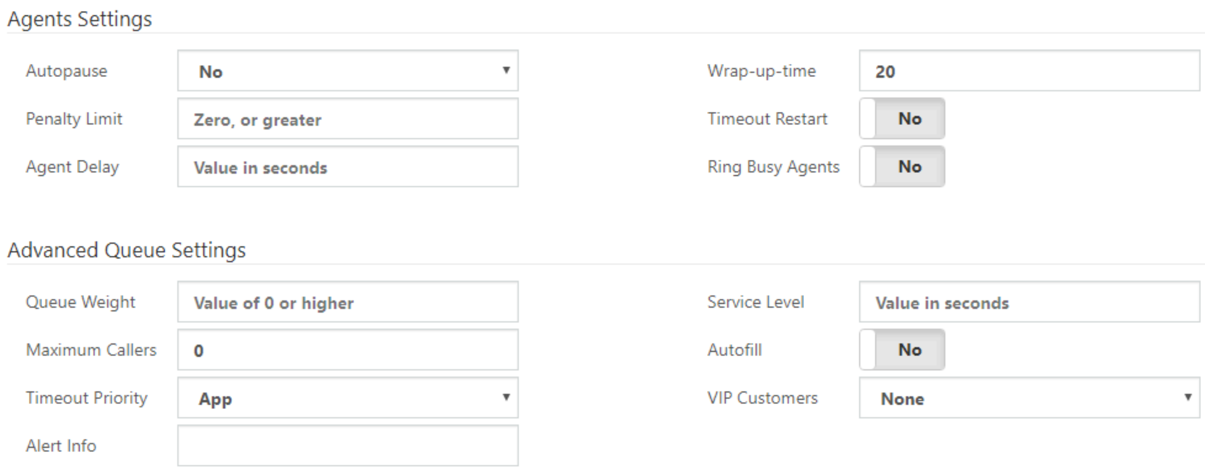
Position Limit, used if you've defined Announce Position as either limit or more

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.

Minimum Frequency, 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.

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

ADVANCED Tab



Agents Settings Section

Autopause, 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 agents that they've been paused, or have a supervisor who is watching the status of the queue in real time.

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

Agent Delay, configures a delay time between when an agent and caller are connected.

Wrap-up time, the number of seconds to keep an agent unavailable in the 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.

Timeout Restart, when enabled, allows the timeout to be reset if either Congested or Busy has been detected for an agent. This can be useful if an agent is allowed to reject or cancel calls.

Ring Busy Agents, used to avoid sending calls to agents whose status is **In Use**.

Advanced Queue Settings Section

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

Maximum Callers 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.

Timeout Priority, controls the priority of conflicting timeout priorities. The queue application has a timeout value that can be specified to control the absolute timeout time that a caller can wait in the queue. This timeout is controlled by the **Queue Timeout** field in the General tab of the Queues dialog. The timeout value in queues.conf controls the time (and retries) when attempting to reach an agent. Select **App** if you want to use the timeout associated with the queue, or select **Conf** if you want to use the value defined in the queues.conf file.

Alert Info, optional SIP alert-info content, which can be used to trigger device-specific features, such as customized ringtones.

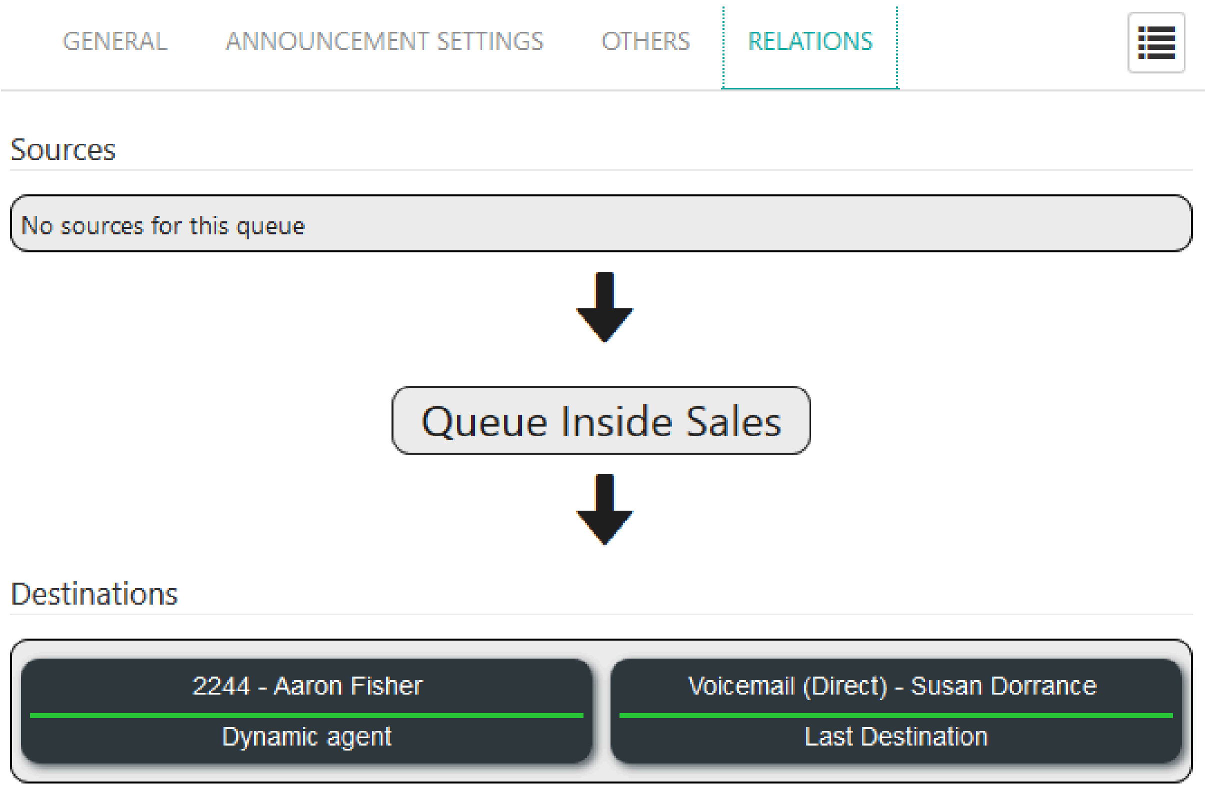
Service Level, define the maximum acceptable time for a caller to wait before being answered. You then note how many calls are answered within that threshold, and they go toward your service level. So, for example, if your service level is 60 seconds, and 4 out of 5 calls are answered in 60 seconds or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

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

VIP Customers, allows you to give priority in this queue to customers selected from the dropdown list of VIP customers.

RELATIONS Tab

This tab provides a graphical display all the modules that are used by the queue that you are currently viewing. This allows you to see at a glance all modules that are associated with the currently-selected queue.



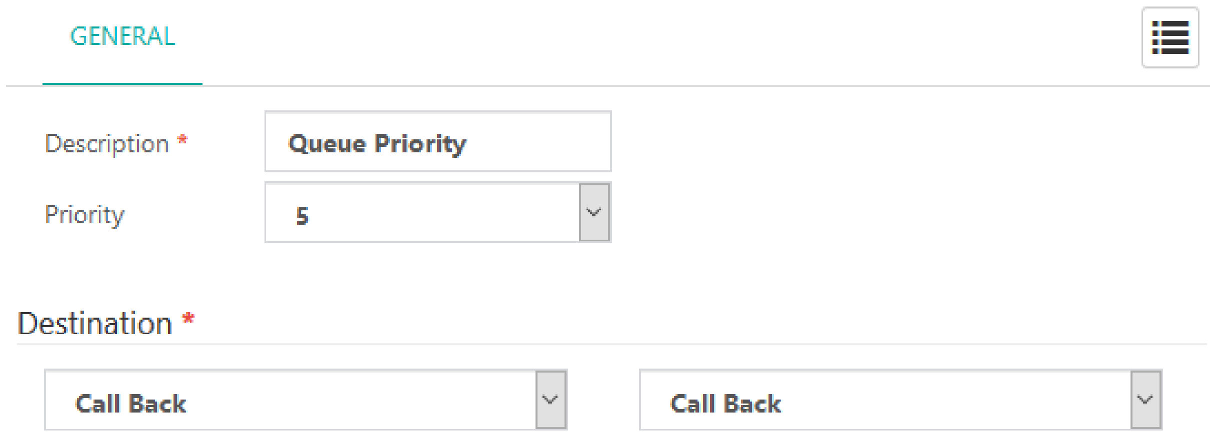
Custom Tab

This allows configuration of custom queue rules (queuerules.conf), use of macros in queues and more.

Queues Priorities Dialog

Change the weight of a queue dynamically, in order to prioritize incoming calls. Usually the destination is a queue.

GENERAL Tab



Description*, a free-text description to identify this queue priority. This description must be unique.

Priority, the value to set for the Queue Priority, in a range between 1 and 50. The highest value has the highest priority.

Destination Section

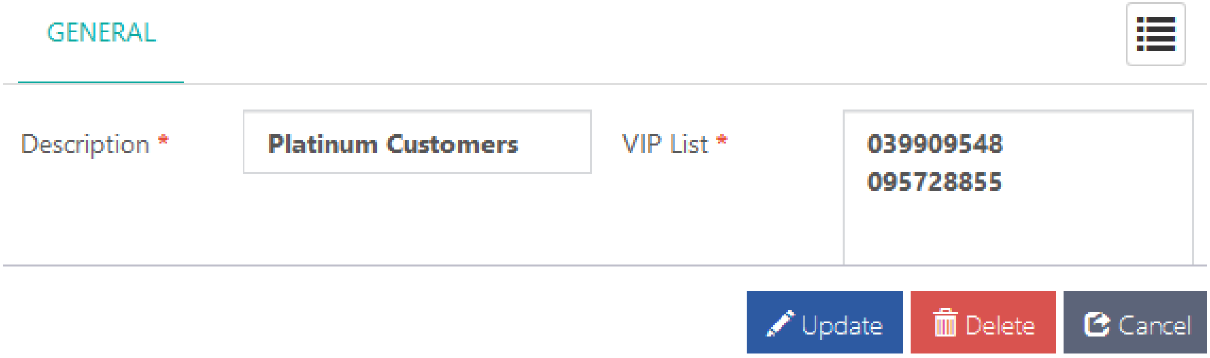
Select Module, allows the user to choose from a drop-down list of available dialogs**,** which dialog should be activated.

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

Queue VIPs Dialog

Allows you to configure customers who should receive higher priority when calling into a queue.

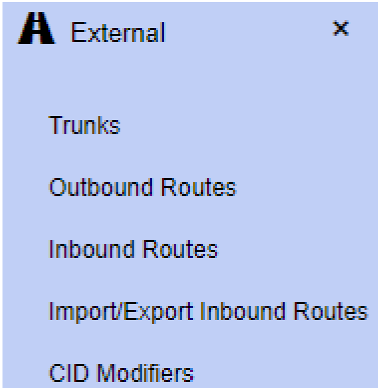
GENERAL Tab



Description*, short free-text description to identify this. This value must be unique.

VIP List*, insert a list of caller numbers (CID). Each caller number should appear on a new line.

External Menu Group



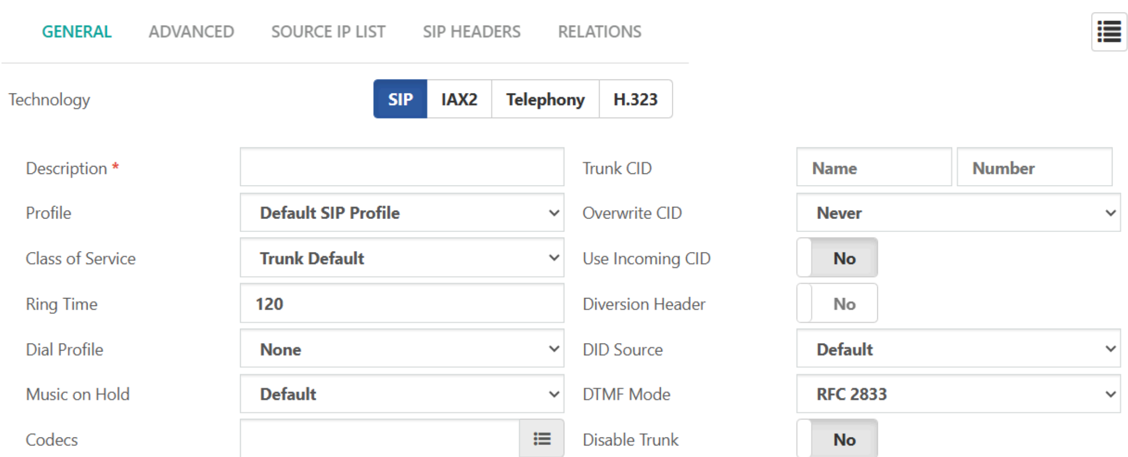
Trunks Dialog

In the simplest of terms, a trunk is a pathway into or out of a telephone system. A trunk connects the system 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. (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)
- Connect directly to another PBX. (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

GENERAL Tab



Technology Section

- SIP
- IAX2 (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)
- Telephony (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)
- H.323 (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

SIP, IAX2, and Telephony 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-to-Asterisk 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 unique, free-text description to help identify this trunk

Profile, the profile that should be used for the trunk. Only applies to SIP trunks.

Class of Service, choose a class of service for the trunk.

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

Dial Profile, dial options parameters, except for Custom trunks. 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 **)
- H - allow the calling 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.
- I - 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)

See the Dial Options section in the appendix for a more complete list of available dial options, or refer to Asterisk online documentation for a full list of dial options.

Music on Hold, default music on hold for this trunk

Codecs, select one, or more, codecs from the drop-down list of available codecs. If you select one (or more) codecs, the list will be preceded by the `disallow=all` statement.

Note for SIP trunks: if codecs are defined both in the SIP profile and this field, the values set in this field will be used, and the values in the SIP profile will be ignored.

Trunk CID, 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**, or when no CID is associated with the calling extension. 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 number that will be displayed by calls on this trunk.

Overwrite CID, allows you to control which CID will sent for external calls. Chose an option from the drop-down list:

- **Never,** never use the CID associated with the Trunk. The CID associated with either the Outbound Route or Extension will be used. If there is no CID associated with either the Outbound Route or Extension, CID will be blank.
- **Always,** always use the CID associated with the Trunk. This will always overwrite any CID associated with the Outbound Route or Extension.
- **Only if Empty,** use the CID associated with the Trunk only if no CID is associated with the Outbound Route or Extension.

Use Incoming CID, when a call is transferred, the caller id of the original caller will be shown. This is only allowed when Overwrite CID is set to Never.

Diversion Header, when set to Yes, diverted calls (i.e. call-forwarding, ring group, follow-me, etc.) will have a SIP Diversion header added to the call showing the original DID information, assuming that it is available. This is useful for carriers who implement the use of diversion headers.

DID Source, determine where to get the DID source information from. When set to **Default**, the DID source will be obtained from SIP R-URI field. When set to **To**, this data will be taken from the To filed in the Sip header.

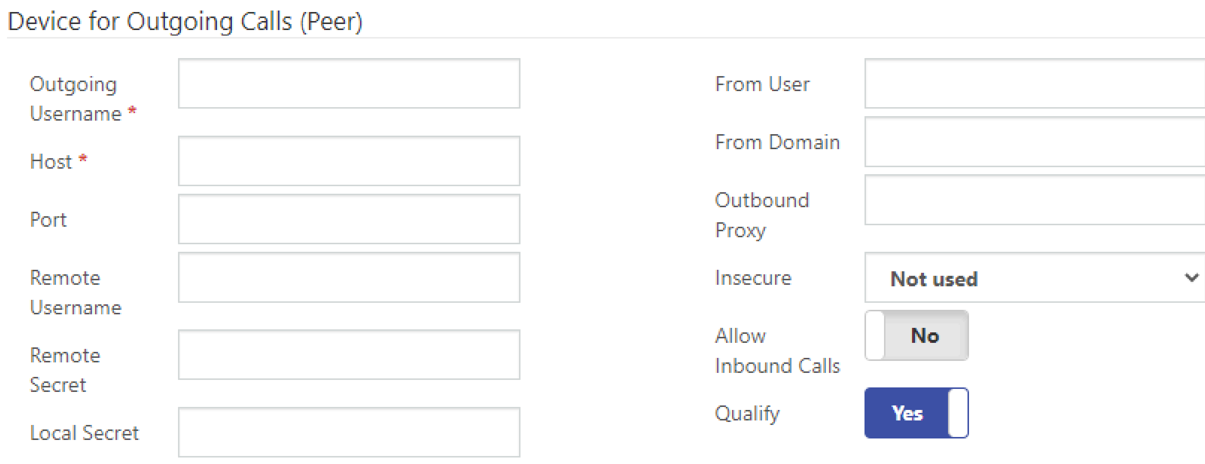
DTMF Mode, sets default dtmf-mode for sending Dual Tone Multi-Frequency (DTMF). The DTMF mode for a SIP device specifies how touchtones will be transmitted to the other side of the call. The default value is rfc2833. Other options available in the drop-down list are:

- 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 it is available, otherwise use in-band option

Disable Trunk, allows you to define a trunk, but make it not active. This can be useful when planning for future changes.

SIP Option

Device for Outgoing Settings (Peer) Section



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

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

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

Remote Username, the username to be used to authenticate this trunk against the provider.

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

Local Secret, password (secret) to be used for authentication requests from the remote server.

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

From Domain, as your provider knows your domain

Outbound Proxy, outbound proxy domain name or IP address that may be required by the SIP trunk provider

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

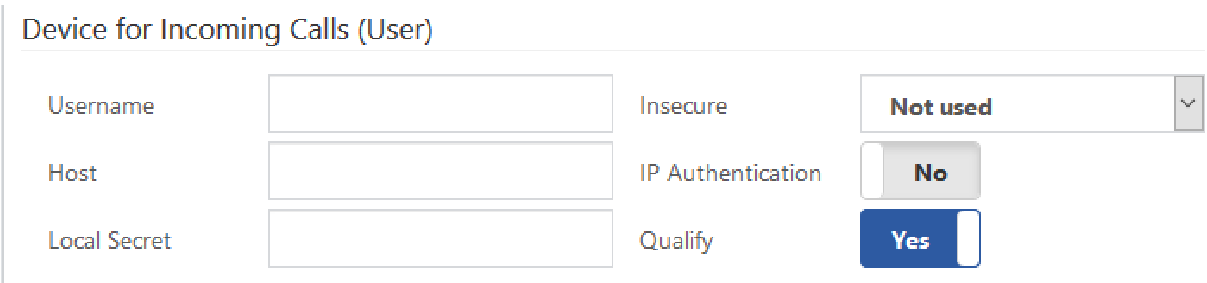
- **Port** - Allow matching of peer by IP address without matching port number
- **Invite** - Do not require authentication of incoming INVITEs

- **Port, Invite** - The combination is the minimum security since no checking or port check or authentication to the INVITE message type.

Allow Inbound Calls, determines whether the trunk can accept inbound calls.

Qualify, make periodic checks to make sure that the user is alive. This causes the system 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, the system will consider the device to be off-line and not available for future calls.

Device for Incoming Calls (User) Section



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, the password credential uses to contact this trunk

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, determines whether the IP of incoming requests should also be checked, in addition to username/secret.

Qualify, make periodic checks to make sure that the user is alive. This causes the system 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, the system will consider the device to be off-line and not available for future calls.

Register String Section

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.

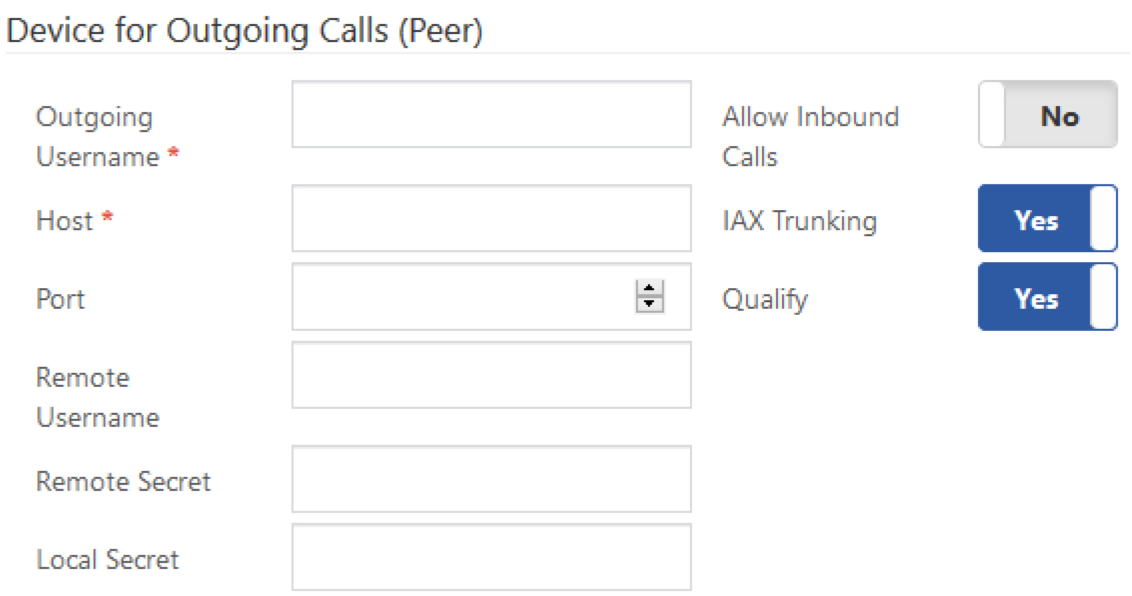
For example: account:password@mydomain.com:5060

If you want to use an IPv6 address in the Register String, then you should enclose it in brackets, i.e. myname@[fe80::2ad2:44ff:fe3f:3b12]/2345

IAX2 Option

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

Device for Outgoing Calls (Peer) Section



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

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

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

Remote Username, the username to be used to authenticate this trunk against the provider.

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

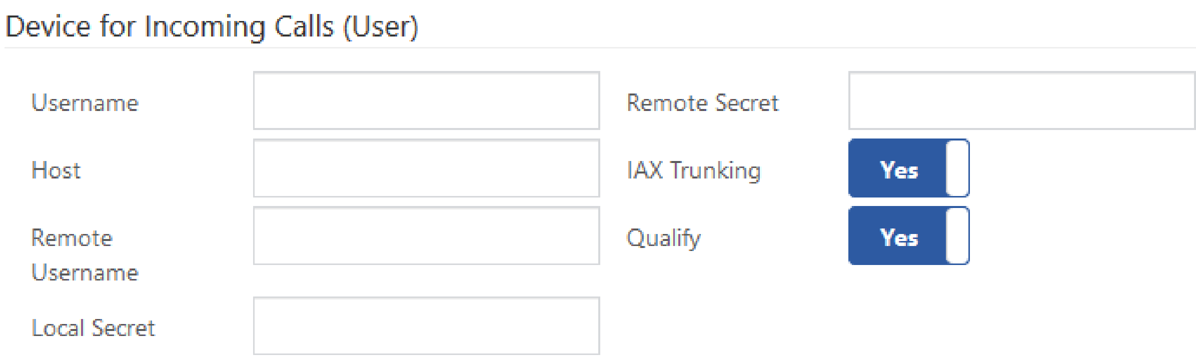
Local Secret, password (secret) to be used for authentication requests from the remote server.

Allow Inbound Calls, determines whether the trunk can accept inbound calls.

IAX Trunking, allows sending of multiple calls in one IAX packet. This can significantly reduce required bandwidth.

Qualify, make periodic checks to make sure that the user is alive. This causes the system 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**,** the system will consider the device to be off-line and not available for future calls.

Device for Incoming Calls (User) Section



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.)

Remote Username, the username to be used to authenticate this trunk against the provider.

Local Secret, the password credential used to contact this trunk

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

IAX Trunking, allow sending multiple calls in a single IAX packet. This can greatly reduced the required bandwidth.

Qualify, carry out periodic checks to make sure that the user is still alive. This causes the system 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**,** the system will consider the device to be off-line and not available for future calls.

Register String Section

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.

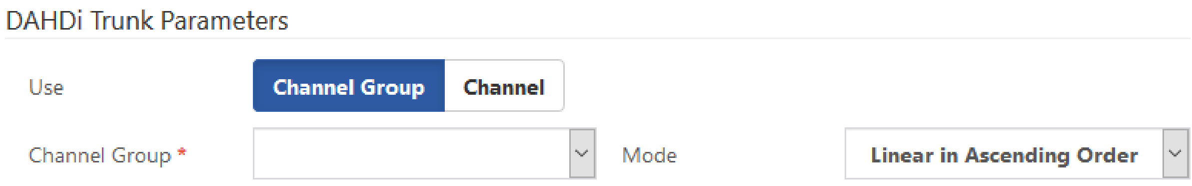
For example: account:password@mydomain.com:5060DAHDi Option

Telephony Option

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

Use for trunks that are based on telephony (DAHDi) technology. Before defining a telephony trunk, make sure that you have detected the hardware (using the Settings>Telephony>Interfaces dialog), and created a channel group (using the Settings>Telephony>Channel Groups dialog.)

Telephony Trunk Parameters



Channel Group, choose a channel group or span for this trunk.

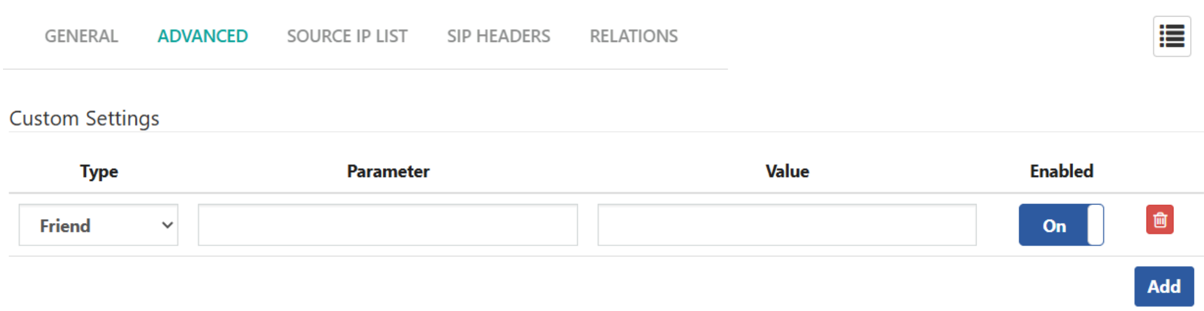
Channel, choose an individual channel to be used for this trunk.

Mode, determines in which order the channels should be used. The drop-down list contains the following options:

- **Linear in Ascending Order** - selects the lowest-numbered available channel. Can be referred to as ascending sequential hunt group
- **Linear in Descending Order** - selects the highest-numbered available channel. Can be referred to as descending sequential hunt group
- **Round-Robin in Ascending Order** - uses a round-robin search**,** starting at the next highest available channel after the channel that was used last time. Can be referred to as ascending rotary hunt group
- **Round-Robin in Descending Order** - uses a round-robin search**,** starting at the next lowest available channel after the channel that was used last time. Can be referred to as descending rotary hunt group

The round-robin searches make the channel module start looking for an available channel from a different channel number each time. For each channel group**,** the channel module keeps track of the last round-robin start point**,** and next time starts checking availability from either the next (lowercase r)) or the previous uppercase R channel in the group. Which channel it actually finds available (if any) does not affect the starting point for the next round-robin search. Calls to the Dial command using ordinary (g or G) group selections do not affect future round-robin starting points either.

ADVANCED Tab



Custom Settings Section

In custom setting you can add any valid pair of parameter/value to the account settings of the trunk.

Use the **Add** button at the bottom of the dialog to add additional sets of parameters. Existing sets can be removed by clicking on the appropriate trash icon.

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

Parameter, any valid variable of Asterisk.

Value, any value for the Asterisk variable.

Enabled, enable or disable the custom settings.

SOURCE IP LIST Tab

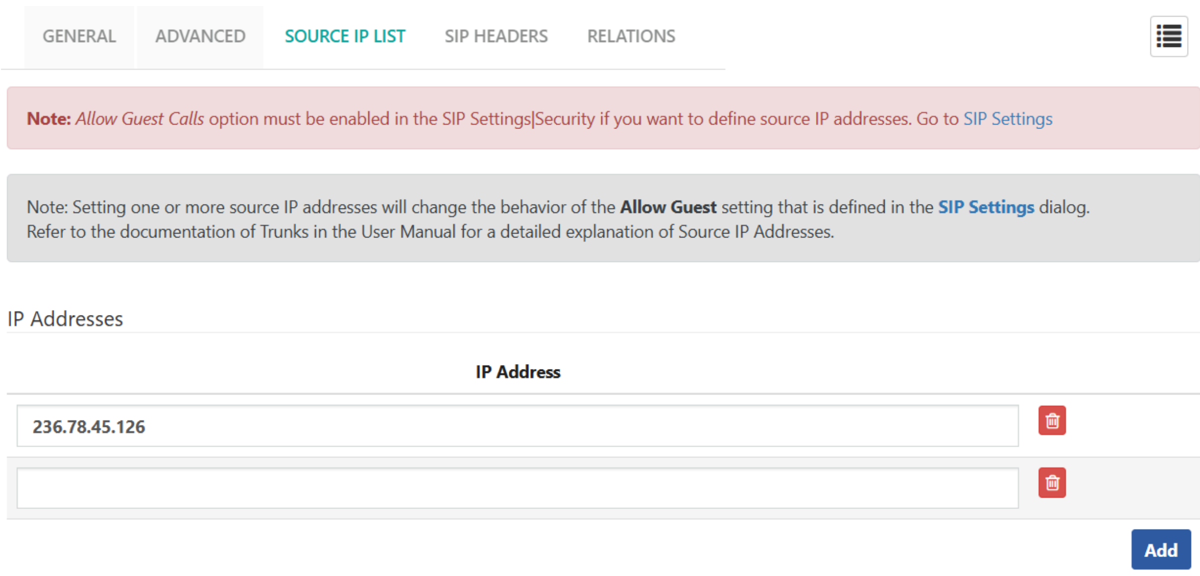
Under certain circumstances, incoming calls cannot be associated with any configured SIP trunk, neither by the caller user name, nor by the sender IP address that is configured in the **Host** field in the General tab. Such calls are considered by CompletePBX 5 as "guest" calls. If "guests" are disabled by the **Allow Guests** parameter in the Settings>Technology Settings>SIP Settings dialog, then such calls will always be rejected. If **Allow Guests** is enabled, calls will be routed according to the configured inbound routes, irrespective of the IP address of the caller.

The list of IP Addresses adds an additional layer to the handling procedure for incoming calls. If a call originates from an address listed in the Source IP List table, then it will be handled according to Class of Service configured for the trunk with which the Source IP List is associated. If no match is found in the Source IP List table, the call will be rejected.

CompletePBX 5 obtains the sender IP address from the **X-Cpbxmt-srcip** field in the SIP header, if it is present in the INVITE request. Otherwise, the CompletePBX 5 uses the IP address the INVITE was sent from.

This mechanism will always be activated if one (or more) addresses are defined in the Source IP List table for any trunk.

If no source IP addresses are defined, the setting of **Allow Guests** will determine the behavior of CompletePBX 5.



IP Addresses Section

IP Address*, Any valid IP address that can be considered as a valid source. The IP address must be in physical notation, i.e. 236.78.45.126.

Name, a free-text field to allow you to document the IP address

Click on the **Add** button to open a new line in the table.

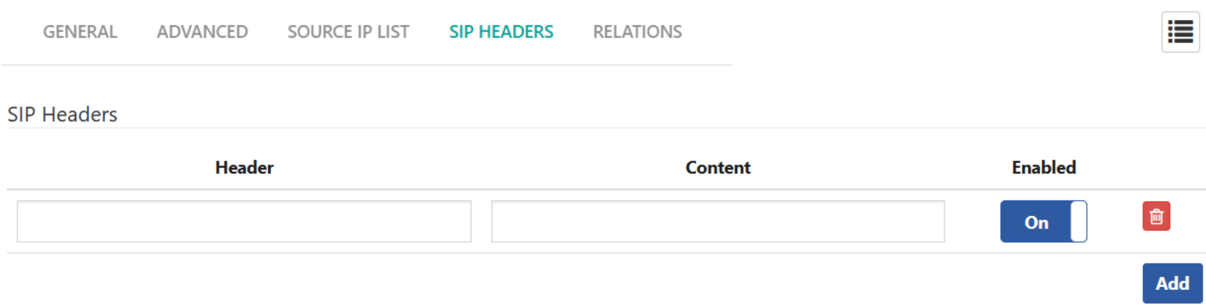
 Click on the trash icon if you want to remove an IP address from the list

Click on the **Save** button when you have completed entering IP addresses.

SIP HEADERS Tab

SIP Headers Section

The SIP HEADERS Section allows you to define custom SIP headers that will be included in outgoing SIP messages for a specific trunk. These headers can be used to provide additional information to the SIP provider or to meet specific interoperability requirements.



Use the **Add** button at the bottom of the dialog to add additional sets of parameters. Existing sets can be removed by clicking on the appropriate trash icon.

Name: Specifies the name of the SIP header (e.g., X-Custom-Header).

Value: Defines the content of the SIP header, which may include static text or dynamic variables.

MULTI TENANT Tab

(**NOTE** that this option is only available on systems that are licensed for multiple tenants.)

Some SIP trunk providers authenticate the endpoints by IP address. It means that the SIP traffic for this specific trunk must go out from particular external MT Server IP address that you can define here. This address must be agreed with MT Server administrator.

External IP, any valid IP address that can be considered as a valid source. The IP address must be in physical notation, i.e. 236.78.45.126.

RELATIONS Tab

This tab provides a graphical display all the modules that are used by the Trunk that you are currently viewing. This allows you to see at a glance all modules that are associated with the currently-selected Trunk.

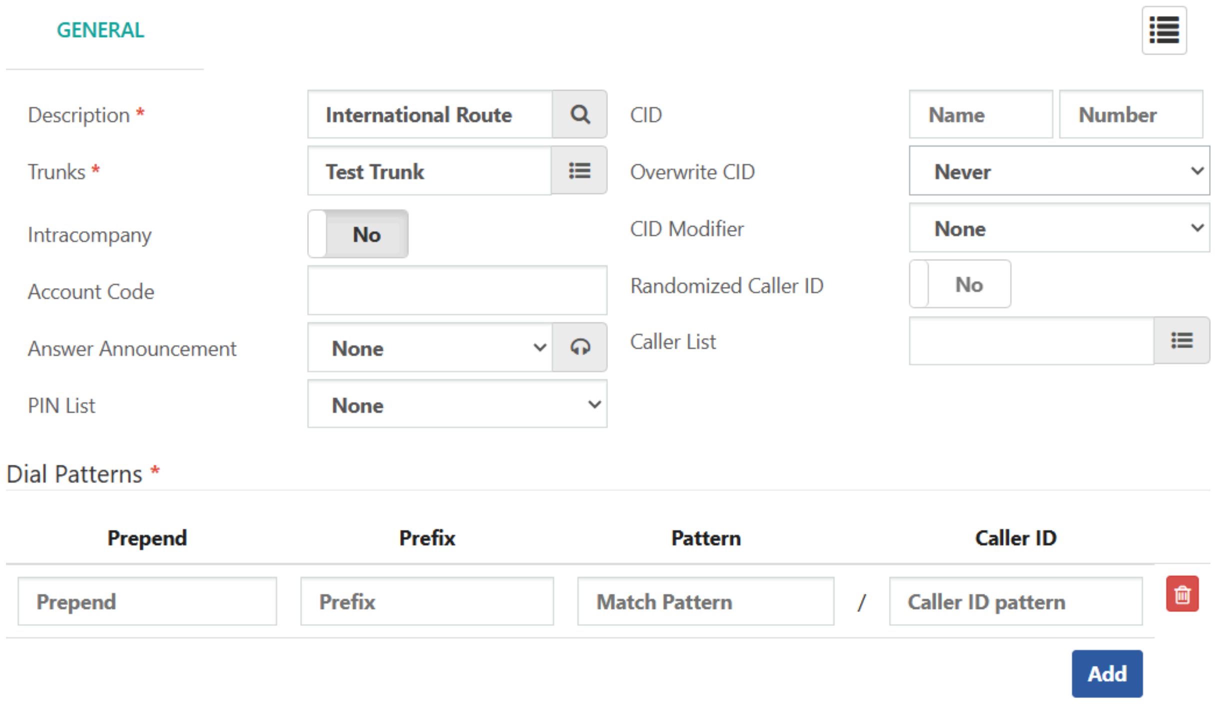
Outbound Routes Dialog

Outbound Routes enables you to choose which Trunks (phone lines) to use when users call 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 the system uses to determine which trunk to use for an outbound call. Many VoIP systems can 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.

GENERAL Tab



Description*, a unique, free-text description to identify the outbound route. The name is usually descriptive of the purpose of the route (for example**,** "Local" or "International").

Trunks*, list of trunks that can be used by the route, selected from a drop-down list of trunks that are defined for your system.

Intracompany, if the outbound route is configured as intracompany, the internal extension number (defined in the Internal CID field of the Extensions dialog) will be sent in place of the External CID.

Account Code, can be used to populate the **accountcode** field in the CDR database. If Account Code is defined for both the calling extension and the outbound route, the account code associated with the outbound route will be used.

Answer Announcement, allows a custom audio message to be played automatically when an external call is answered by the called party. The announcement is heard by both the caller and the recipient.

PIN, allows you to associate a PIN list with this outbound route. Only users who know a PIN in the associated PIN list can be authenticated to use this outbound route. Lists of PINs can be configured in the **PIN Lists** dialog

CID, the caller identification associated with this Outbound Route. This field is used in conjunction with the Overwrite CID field.

Overwrite CID, allows you to control which CID will sent for external calls. Chose an option from the drop-down list:

- **Never,** never use the CID associated with the Outbound Route. The CID associated with the extension will be used. If there is no CID associated with the extension, CID will be blank.
- **Always,** always use the CID associated with the Outbound Route. This will always overwrite any CID associated with the extension.

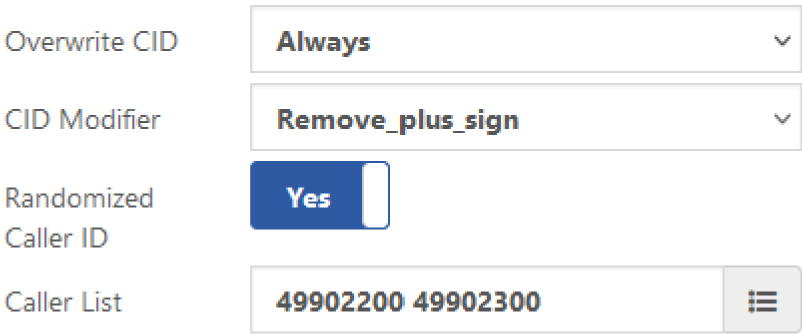
- **Only if Empty,** use the CID associated with the Outbound Route only if no CID is associated with the extension.
- **Use a CID Modifier**, to modify the caller ID on outbound routes.

This setting is used in conjunction with the Overwrite CID setting for Trunks, and can be overridden by the trunk setting.

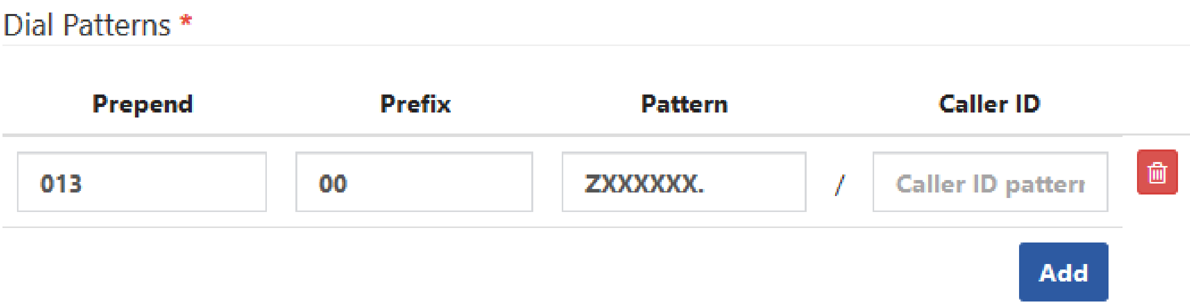
CID Modifier, list of caller IDs to modify the caller ID on outbound routes by adding a prefix or making other modifications. To use this feature, select the modifier from the list configured in **PBX > External > CID Modifiers**.

Randomized Caller ID, allows randomizing of the **Caller ID** for outgoing calls, based on the caller IDs in the **Caller List**. This can be useful in call center applications that do not want to always display the same caller ID for all outbound calls. This field is not enabled when the **Overwrite CID** field is set to **Never**.

Caller List, allows you to input a list of caller IDs that can be used for **Randomized Caller ID.** Each **Caller ID** should be entered on a new line. Make sure that your trunk provider allows the IDs in the list to be used.



Dial Patterns Section



Prepend, digits to add to a successful match. You can also use the **w** character to create a half second delay in the dial sequence for analog lines. You can use multiple **w** characters to create longer wait periods.

Prefix, prefix to remove from a successful match. You can use standard pattern-matching characters in this field. Standard pattern matching options are:

- **X** - X or x represents a single digit from 0 to 9.
- **Z** - Z or z represents any digit from 1 to 9.
- **N** - N or n represents a single digit from 2 to 9.
- **.** - can be used as a wildcard to match one or more characters.
- **!** – can be used as a wildcard to match zero or more characters.
- **[1237-9]** - matches any digit/s or letter/s 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

Pattern, allows you to create one or more patterns in the dial plan that match possible dialed numbers.

Standard pattern matching options are:

- **X** - X or x represents a single digit from 0 to 9.
- **Z** - Z or z represents any digit from 1 to 9.
- **N** - N or n represents a single digit from 2 to 9.
- **.** - can be used as a wildcard to match one or more characters.
- **!** – can be used as a wildcard to match zero or more characters.
- **[1237-9]** - matches any digit/s or letter/s 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 that you create allow you to make 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.

Examples

- **07[2-4679]XXXXXXX** will allow calls to all 10 digit numbers that start with 072, 073, 074, 076, 077, or 079
- **1200XXXXXX** will allow calls to all 10 digit numbers that start with 1200
- **12551.** will allow calls to any number that begins with 12551

Caller ID, allows you to create patterns in the dial plan that match one or more CID numbers that initiate the call

Standard pattern matching options are:

- **X** - X or x represents a single digit from 0 to 9.
- **Z** - Z or z represents any digit from 1 to 9.
- **N** - N or n represents a single digit from 2 to 9.
- **.** - can be used as a wildcard to match one or more characters.
- **!** – can be used as a wildcard to match zero or more characters.
- **[1237-9]** - matches any digit/s or letter/s 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 that you create allow you to make 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.

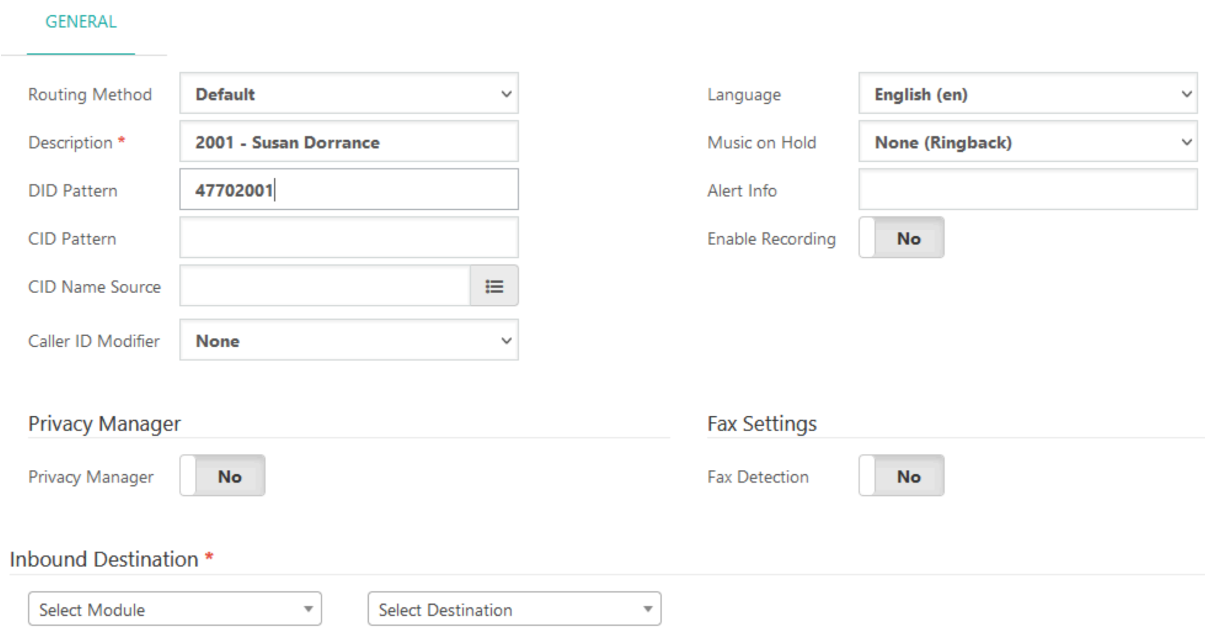
Example

- **49903278** will allow calls to any number to the defined pattern that originates from an extension that has a CID of 49903278

Inbound Routes Dialog

The Inbound Routes dialog 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 Tab



Routing Method, can either be the DAHDI channel for an analog port (FXO)**,** or default for all other inbound routes. (Note that only the default option is available on systems that support multiple tenants – the FXO option is disabled.)

Description*, a free-text 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 the system.

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 all DIDs (this will also match calls that have no DID information).

This field also allows patterns to match a range of numbers. 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.

CID Name Source, optional list of CID sources to use for looking up the CID name for the incoming CID number. This lookup is performed before applying any CID modifier. The pop-up dialogue will allow the selection of one or more CID Name Sources including Phonebooks.

The Caller ID Number field can be left blank to match with all 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 an inbound route that allows all calls.

Caller ID Modifier, allows you to use a rule (that can be defined in the CID Modifiers dialog) that will be used to modify incoming CID numbers and names. Leave this field blank if you do not want to modify incoming CID data.

Language, specifies the language 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 system.

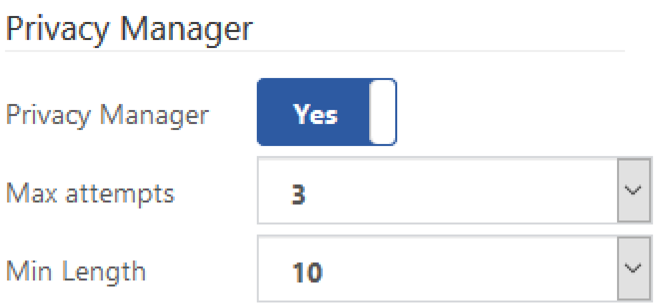
Music on Hold, this drop-down menu allows you to select the music-on-hold class for this route. Whenever a caller accessing this route is placed on hold**,** they will hear the music on hold defined in the class selected here. This is often used for companies that use their music on hold to advertise 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 system 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.

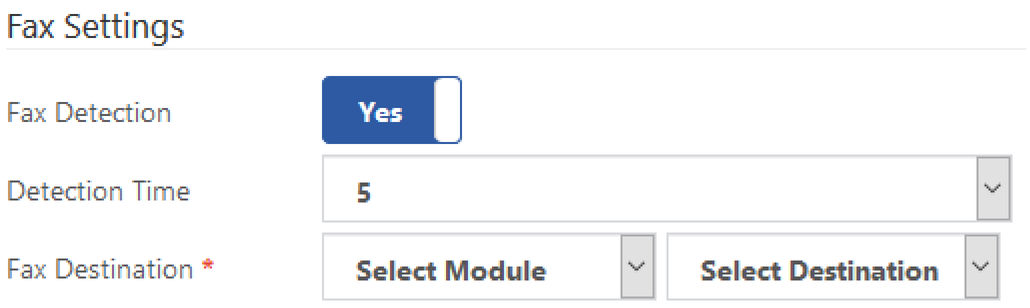


Privacy Manager, toggle to determine whether to activate the privacy manager functionality

Max attempts, the maximum number of attempts that the caller is allowed to enter a valid caller ID

Min Length, the minimum number of digits that the caller must enter to define his caller ID

Fax Settings Section



Fax Detection, determines whether faxes should be detected on this route. If fax detection is enabled, additional parameters can be configured and a drop-down 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 the system. 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.

Detection Time, determines how many seconds to wait before ringing the extension. This time enables the inbound route to listen for fax tones and determine whether the incoming call is a fax or a normal voice communication. After this time period, if no fax handshake is detected, the extension will begin to ring in a normal manner. Typically, this should be set to 5 seconds.

Fax Destination*, determines where incoming faxes will be sent. This can be any user extension that has been configured with an email address. You can also direct incoming faxes to other modules, such as Custom Destinations, etc.

Inbound Destination Section*

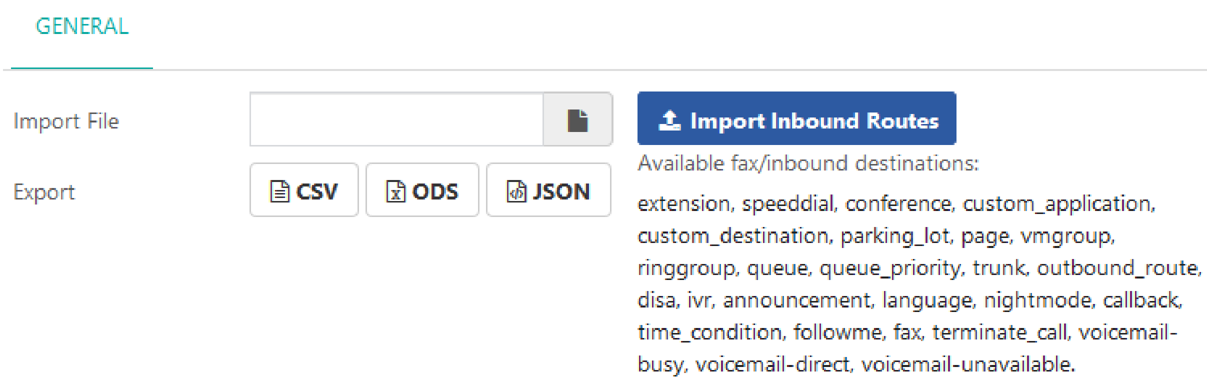
Select Module, allows the user to choose from a drop-down list of available dialogs, which dialog should be activated.

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

Import/Export Inbound Routes Dialog

Allows you to use a CSV file to manage Inbound Routes.

General Section



Import File, the file containing details of the Inbound Routes that you want to add to the system, modify in the system, or delete from the system.

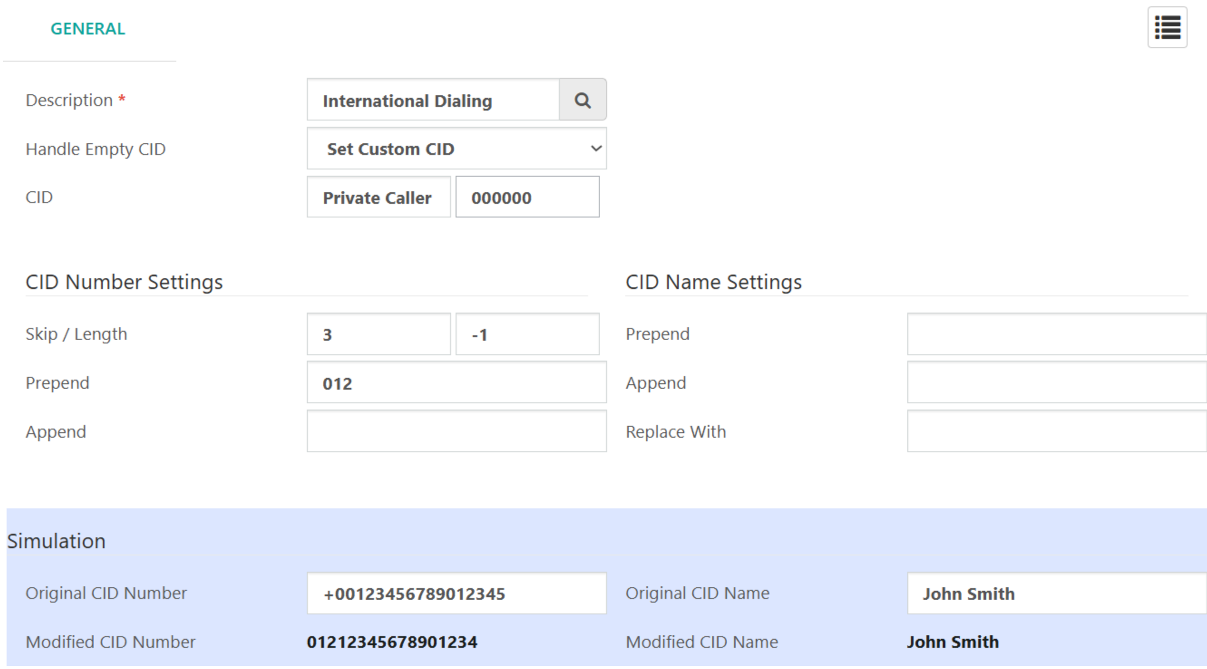
Import Inbound Routes, press this button to import Inbound Routes from a CSV, ODS, or JSON file. You can use the exported file as a template for adding additional routes. The top row of the file contains a detailed explanation of each field. In some cases, where the explanation is very long, you should refer to the tooltip of the appropriate field in the Inbound Routes dialog.

Export, exports existing Inbound Routes into a CSV, ODS, or JSON file. You can use this file as a template for adding additional routes. The top row of the file contains a detailed explanation of each field. In some cases, where the explanation is very long, you should refer to the tooltip of the appropriate field in the Inbound Routes dialog.

CID Modifiers

Allows you to manipulate the digits of Caller ID for incoming calls.

GENERAL Tab



Description*, a free text description to uniquely identify this CID modifier.

Handle Empty CID, allows you to define how the system should behave when the incoming Caller ID number is empty. If this option is set to *Apply Modifier*, the defined CID modifier rules will still be applied even when no Caller ID is present. If set to *Keep Empty*, the Caller ID will remain blank without modification. Alternatively, choosing *Set Custom CID* allows you to define a fixed Caller ID number that will be used whenever the incoming Caller ID is empty.

CID, the caller identification associated with the *Set Custom CID* selection of ***Handle Empty CID*** in this CID modifier. This field ensures that calls with missing Caller ID are displayed consistently across all system modules (CDR, Supervision, and Statexplorer).

CID Number Settings Section

Skip / Length, allows you to modify an incoming CID number by starting the manipulation some number of digits either from the beginning or end of the CID number, while retaining any number of the remaining digits.

This definition consists of two parts:

- **Skip** defines where to start modifying the incoming CID number. If the skip value has a positive value of x, the leading x digits will be skipped, and the modified CID number will start after x digits. If the skip value has a negative value of x, the modified CID number will start x digits before the end of incoming CID number.
- **Length** determines how many digits the modified CID number will consist of. If the length is zero, all the digits after the start position will be used. You can define a negative length of x in order to discard the x trailing digits.

Examples of manipulation on an incoming CID number of 123456789:

- Skip value of 3, length value of 5, creates a modified CID number of 45678
- Skip value of 3, length value of 0, creates a modified CID number of 456789
- Skip value of -6, length value of 3, creates a modified CID number of 456
- Skip value of -6, length value of -2, creates a modified CID number of 4567

Prepend, allows you to define digits that will always be added in front of the incoming CID number.

Append, allows you to define digits that will always be added at the end of the incoming CID number.

CID Name Settings Section

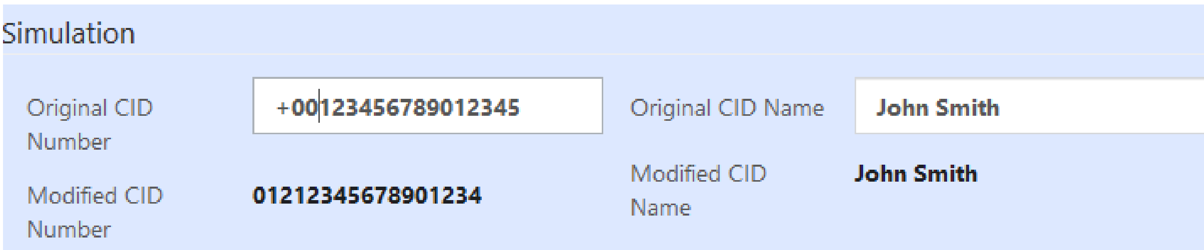
Prepend, allows you define text that will always be added in front of the incoming CID name.

Append, allows you define text that will always be added at the end of the incoming CID name.

Replace With, allows you to completely replace the incoming CID name with fixed text.

Simulation Section

This section allows you to see how your settings will affect incoming CID number and names.



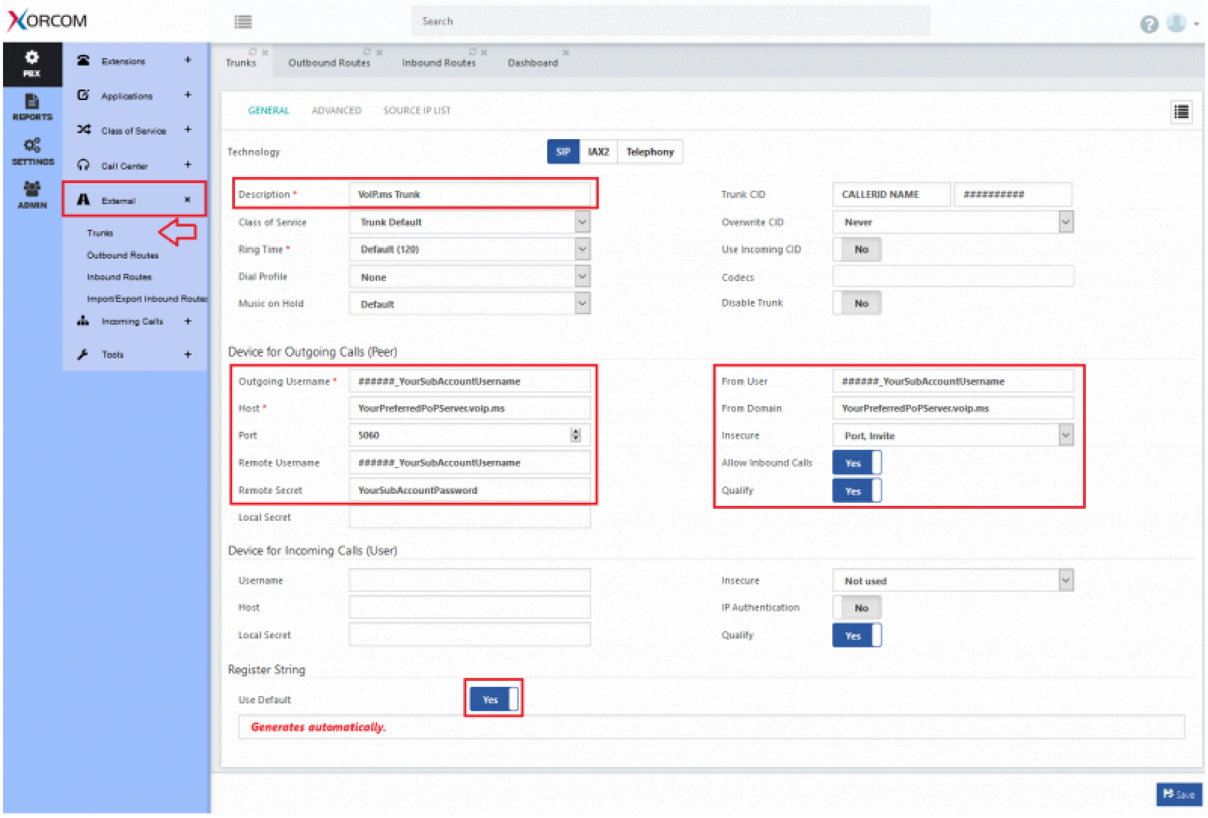
The **Modified CID Number** field will display how the digits that you enter in the **Original CID Number** field will be displayed based on the rules that you define in CID Number Settings section.

In a similar manner, the **Modified CID Name** field will display how the name that you enter in the **Original CID Name** field will be displayed based on the rules that you define in CID Name Settings section.

Example of SIP Trunk Configuration

The following example shows how to configure a VoIP.ms trunk in your CompletePBX 5 system.

First, you need to configure the **GENERAL** tab in the **Trunks** dialog.



In the **Technology** section:

- **Technology**: select **SIP** technology.
- **Description**: enter a free-text description for this trunk.

In the **Device for Outgoing Calls (Peer)** section:

- **Outbound Username**: enter the sub-account username that you received from VoIP.ms
- **Host**: enter your preferred VoIP.ms PoP Server. Note that your DID needs to be on the same PoP Server as your PBX in order to receive incoming calls.
- **Port**: 5060 or any alternative port that we offer such as 5080, or 42872.
- **Remote Username**: enter your VoIP.ms sub-account username.
- **Remote Secret**: the password that is associated with your VoIP.ms sub-account.
- **From User**: enter your VoIP.ms sub-account username.
- **From Domain**: enter the same PoP server as the host used.
- **Insecure**: Choose [Port, Invite] from the drop-down list.
- **Allow Inbound Calls**: Set to **Yes.**
- **Qualify**: Set to **Yes.**

In the **Register String** section:

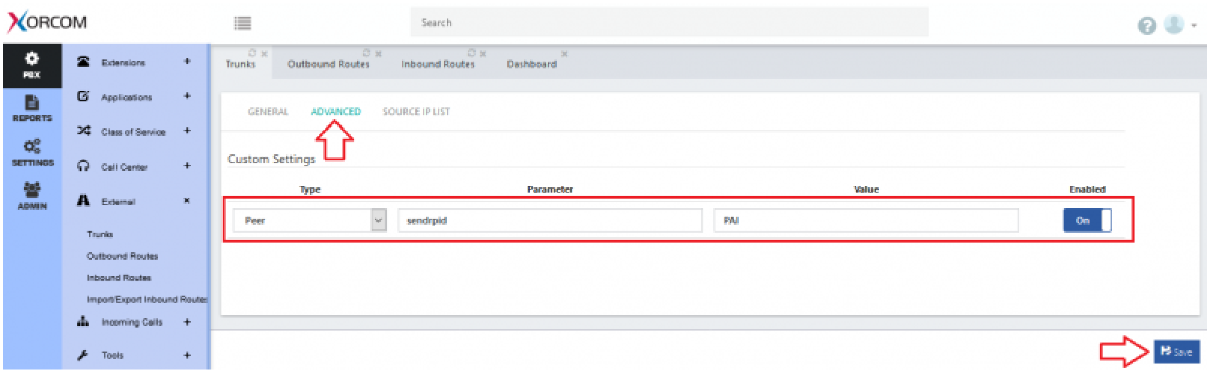
- **Use Default**: set to **Yes** - the whole string will automatically be generated.

Caller ID: If you want to set your outbound Caller ID Name in the number directly in the trunk, it will override everything that your extension/Outbound Routes will try to pass. Enter the **Trunk CID** and set the **Overwrite CID field** to **Always.**

If you enter a CallerID Name in the **Trunk CID** field, it must be in uppercase, without any special characters (spaces are allowed), and no longer than 15 characters.

The Outbound CallerID Name will only work when you call a Canadian number. For the US, you will need to update your record associated with your CallerID Number, in the CNAM database, by requesting an update to our support.

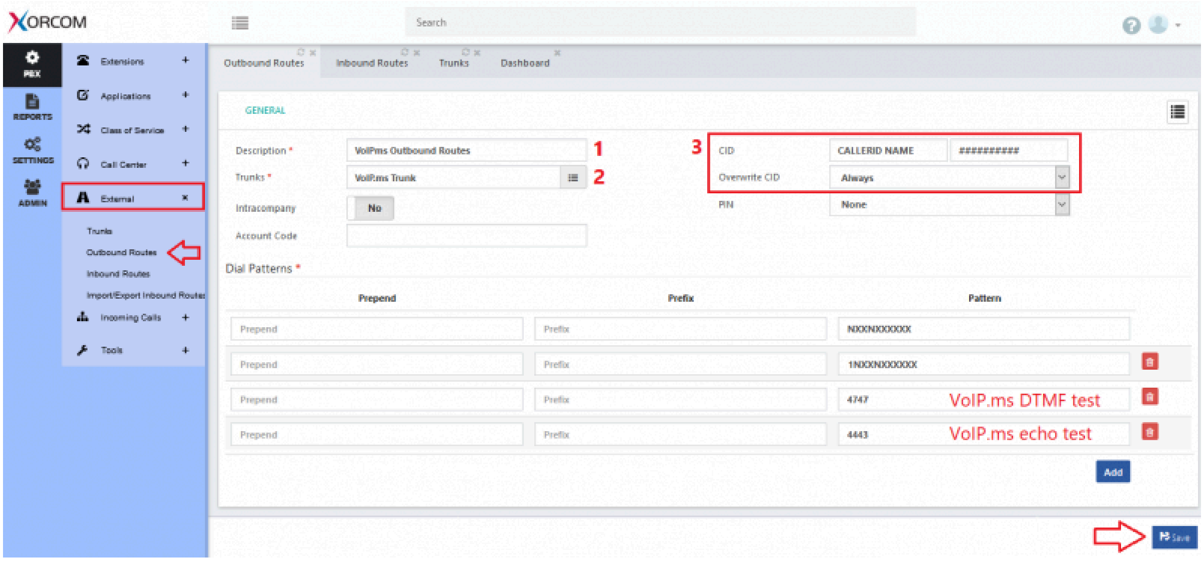
Now, go to the **ADVANCED** tab.



- **Type**: select Peer from the drop-down list.
- **Parameter**: enter sendrpid
- **Value**: enter PAI
- **Enabled**: set to **On.**

Next, click on the Save button to save all the Trunk configuration settings.

The next step is to create a new **Outbound Route** in the PBX>External>Outbound Routes dialog.



- **Description:** enter a description for this Outbound Route.
- **Trunks**: select the VoIP.ms Trunk that you created in the previous steps.
- **CID**: if it is not set in the configuration of the VoIP.ms Trunk, you may enter, for example, your company name.
- **Overwrite CID**: set to **Always** if you would like to use this CID associated with this Outbound Route. Note that the **Overwrite CID** field in the Trunk dialog must be set to **Never** to use it.

In the **Dial Patterns** section:

- **Prefix:** you may enter a prefix, if needed, such as [9] if you want your extensions to dial [9] before the outgoing number. Note that the number [9] will not be sent to VoIP.ms.
- **Pattern**: you can indicate multiple patterns matching for an outbound call. e.g. for a North American number, you can use NXXNXXXXXX/1NXXNXXXXXX (N = digits between 0-9 and X = digits between 2-9).

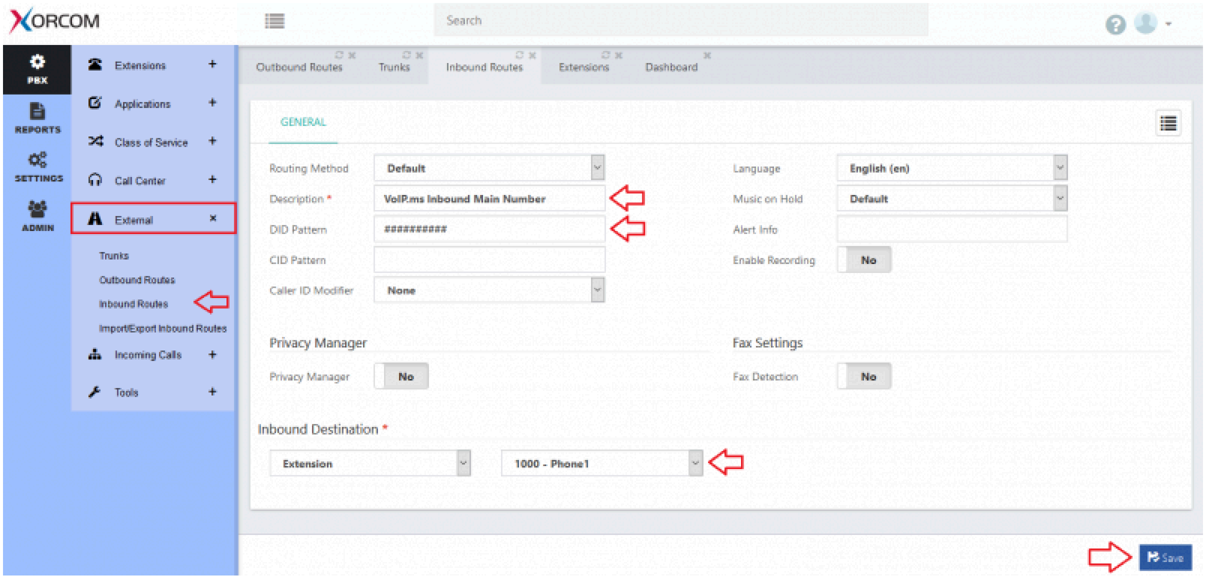
Caller ID: if you want to set your outbound Caller ID Name in the number directly in the trunk, it will override everything that your extension/Outbound Routes will try to pass. Enter the **Trunk CID** and set the **Overwrite CID field** to **Always.**

If you enter a CallerID Name in the **Trunk CID** field, it must be in uppercase, without any special characters (spaces are allowed), and no longer than 15 characters.

The Outbound CallerID Name will only work when you call a Canadian number. For the US, you will need to update your record associated with your CallerID Number, in the CNAM database, by requesting an update to our support.

Next, click on the Save button to save the Outbound Route configuration settings.

Finally, you will need to create **an Inbound Route** in the PBX>External>Inbound Routes dialog.

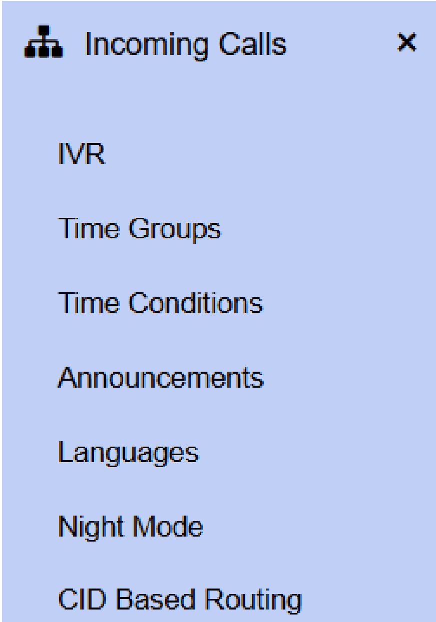


- **Routing Method: select Default** from the drop-down list.
- **Description:** enter a free-text description for this Inbound Route.
- **DID Pattern:** enter your DID number as it appears in your VoIP.ms, excluding any dots, parentheses, etc.
- **Inbound Destination:** this will the destination where your incoming call from this DID will be routed.

Next, click on the Save button to save the Inbound Route configuration settings.

Finally, click on the Reload icon to complete the configuration.

Incoming Calls Menu Group



IVR Dialog

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.

The system'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:

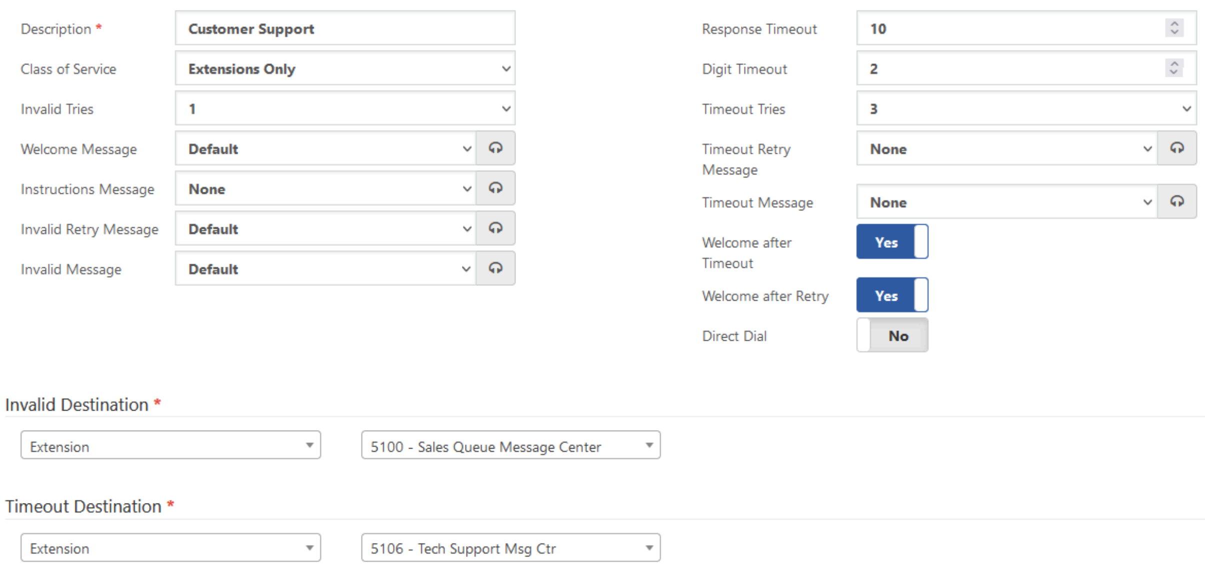
- Handling the timeout when there is no input from the caller
- Controlling the action to take if the caller provides invalid user input
- Allowing the caller to backtrack if s/he has made a mistake or gets lost
- Allowing the caller to return to the IVR if voicemail is encountered
- Provide an option that allows the caller to reach a human operator
- 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

- You can avoid the use of the word **dial** when you record announcements. People today use phones with either push-buttons or touch screens, so it is preferable to say **press**.
- You can improve the usability of the IVR announcements by telling the user about the service or destination before you tell them which number to press.
- You should not have more than about 4 or 5 entries in any level of the IVR, otherwise it makes it too complicated for the caller

NOTE that it is possible to dial one-digit extensions directly from the IVR.

Use Xorcom voice recording services to ensure that you have high-quality, professional announcements. You can count on the continuity of our professional services so that whenever you would like to change or add a recording, you will be able to use the same professional voice for a coherent customer experience.

GENERAL Tab



Description*, a free-text description to identify this IVR. This field is not parsed by the system.

Class of Service, choose a Class of Service for this IVR.

Invalid Tries, number of invalid attempts allowed.

Language, this option specifies the language of the prompts to be used for this IVR.

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. The welcome message will only be played when the caller first enters the IVR: it will always be followed by the instructions message.

Instructions Message, instruction message, selected from a drop-down menu of pre-recorded messages that will be played to the caller each time that they return to the IVR menu. The welcome message will not be repeated when the callers returns to the IVR menu.

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, 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.

Digit timeout, the number of seconds for the system to wait before taking action.

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.

Message on Timeout, when enabled, will return the user to the main IVR Welcome Message after playing the Timeout Retry Message.

Message on Invalid, when enabled, will return the user to the main IVR Welcome Message after playing the Invalid Retry Message.

Direct Dial, enables the caller to call 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*.

Invalid Destination Section*

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

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

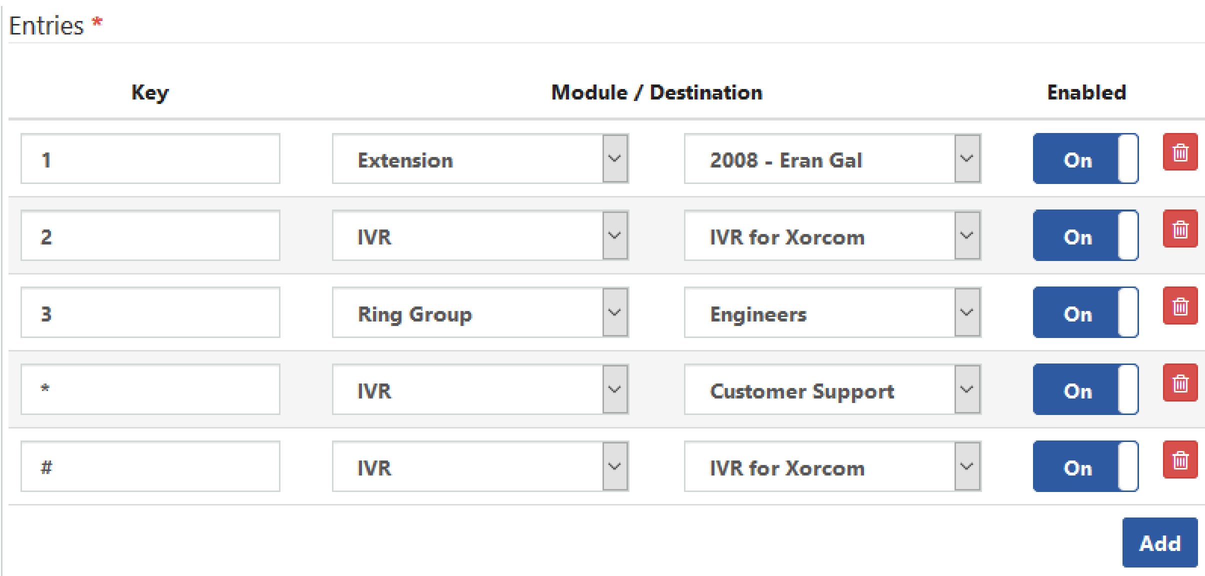
Timeout Destination Section*

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

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

ENTRIES Tab

This tab defines how to handle the user's input.



Entries Section*

Key, key to press. Can be any digit from 0-9, or either of the keypad symbols, * or #, or a DTMF pattern (e.g. _XXXX) to capture variable-length input and pass it to external applications.

Module, destination type to activate when the caller presses the appropriate key.

Destination, destination to call when the caller presses the appropriate digit.

Enabled, select **On** to enable, or **Off** to disable the key.

Click on this icon to remove an existing entry

Add, press this button to add a new entry

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 the asterisk key ("*") and link that key to the parent IVR.

RELATIONS Tab

This tab provides a graphical display all the modules that are used by the IVR that you are currently viewing. This allows you to see at a glance all modules that are associated with the currently-selected IVR.

Time Groups & Time Conditions

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 use 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.

Time Groups Dialog

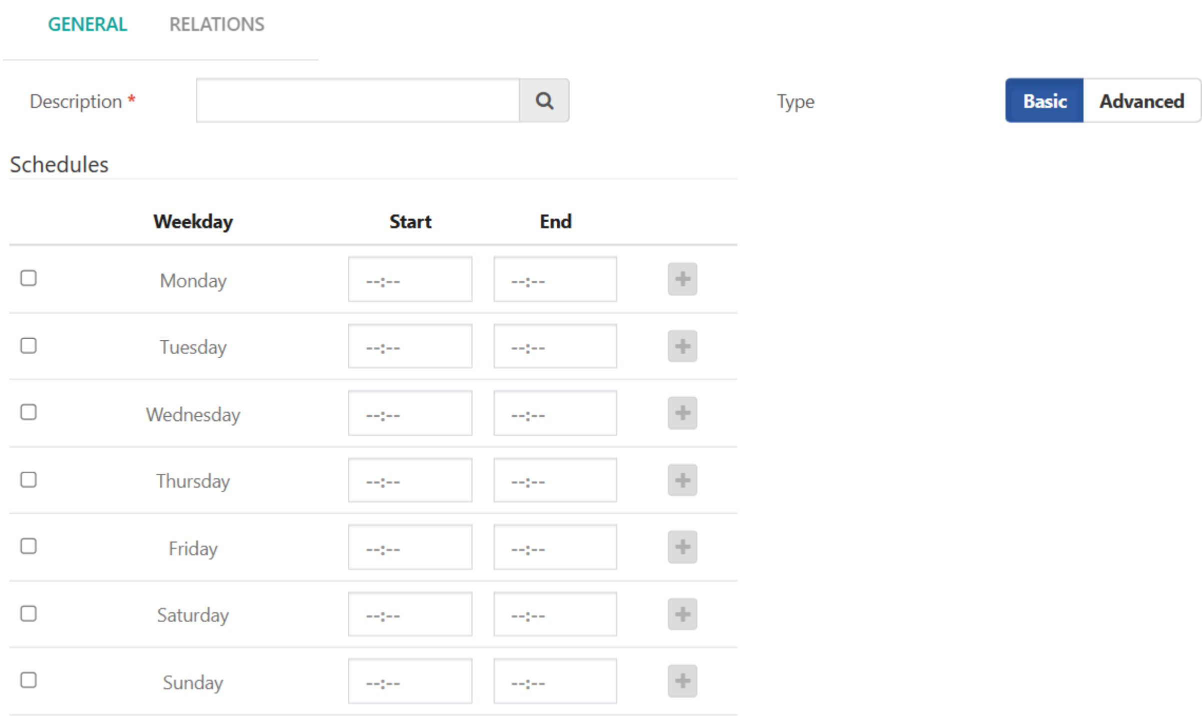
GENERAL Tab

Description*, used to identify the time group, when selecting it during the setup of a time condition. This value is not parsed by the system.

Type, select the type of Time Group from the displayed list:

- Basic
- Advanced

Schedules Section (Basic)



Weekday, day of the week that the time group should start.

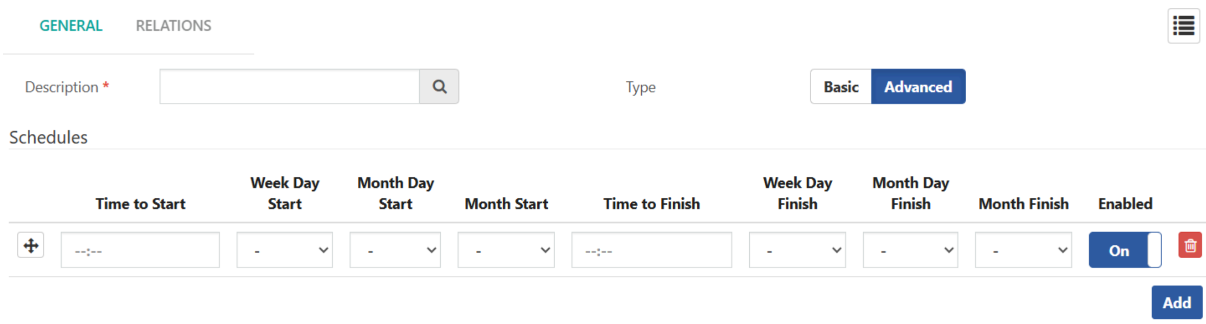
Start, the hour and minute at which the time group starts on the specified weekday.

End, the hour and minute at which the time group ends on the specified weekday.

Click on this icon to adds a new time range (Start and End) for the selected weekday.

Click on this icon to remove the corresponding time range from the list.

Schedules Section (Advanced)



Time to Start, time**,** in hours and minutes**,** that the time group should start.

Week Day 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.

Week Day Finish, day of the week that the time group should end.

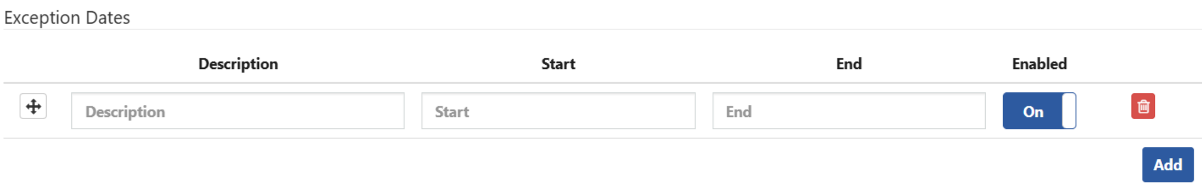
Month Day Finish, day of the month that the time group should end.

Month Finish, month of the year that the time group should end.

 Click on this icon to remove an existing entry

Add, press this button to add a new entry

Exception Dates Section



Description*, free-text description to identify the exception date.

Start, date on which the exception should start.

End, date on which the exception should end.

Press and hold the ✥ icon to move the selected schedule up or down.

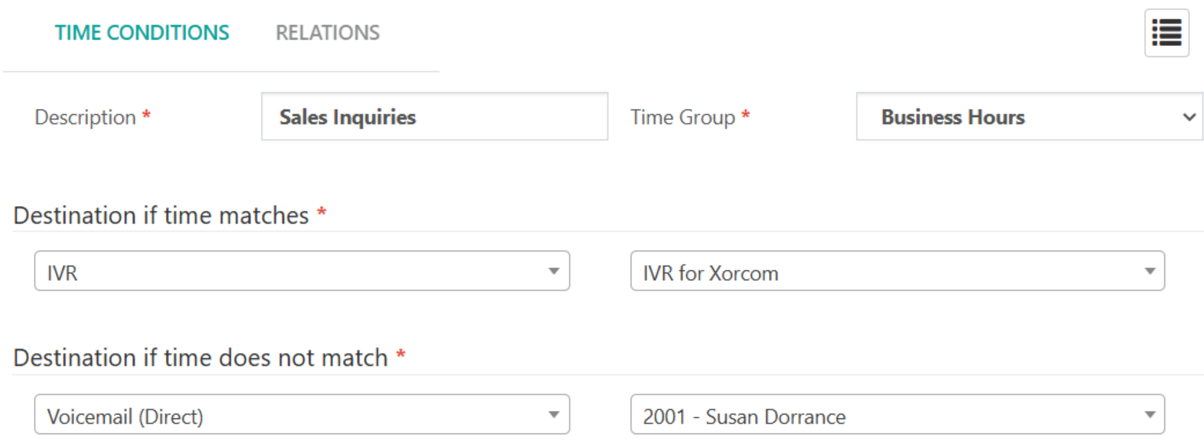
RELATIONS Tab

This tab provides a graphical display all the modules that are used by the Time Group that you are currently viewing. This allows you to see at a glance all modules that are associated with the currently-selected Time Group.

Time Conditions Dialog

Once a time group has been defined, a time condition can be set up as a call target.

GENERAL Tab



Description*, free-text 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.

Destination if Time Matches Section

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

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

Destination if Time does not Match Section

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

Select Destination, is the dialog target to which the dialog should be routed.

RELATIONS Tab

This tab provides a graphical display all the modules that are used by the Time Conditions that you are currently viewing. This allows you to see at a glance all modules that are associated with the currently-selected Time Conditions.

Announcements Dialog

This dialog is used for when you want the caller to hear a message, before being automatically transferred to a fixed destination.

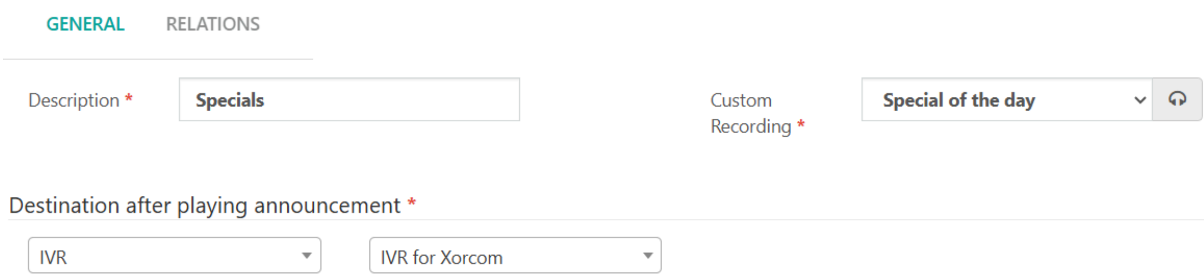
There are two steps that you should follow before using this dialog.

1. You need to make a recording that contains the message that you want callers to hear. This is done by dialing feature code *92 (Custom Recording) from any phone on the system. After dialing *92, follow the verbal instructions to record your message.
2. After successfully making a custom recording, navigate to the Recordings Management dialog (Settings>PBX Settings>Recordings Management). The recording that you have just made will appear with a name that is based on the timestamp when the recording was made. The format starts with a representation of the date when the recording was made, formatted as YYYYMMDD followed by the number of the extension from which the recording was made. You can click on the edit icon for the recording, and give it a more meaningful name.

Use Xorcom voice recording services to ensure that you have high-quality, professional announcements. You can count on the continuity of our professional services so that whenever you would like to change or add a recording, you will be able to use the same professional voice for a coherent customer experience.

Now you are ready to use the Announcements dialog.

GENERAL Tab



Description*, a free-text description to identify this Announcement.

Custom Recording*, select a recording, from the drop-down list, to play in this Announcement.

Click on this icon to listen to the recording

Destination after playing announcement* Section

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

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

RELATIONS Tab

This tab provides a graphical display all the modules that are used by the Announcement that you are currently viewing. This allows you to see at a glance all modules that are associated with the currently-selected Announcement.

Languages Dialog

This dialog is used for when you want to change the language of the prompts that are used in the course of a call**,** such as when an IVR is used and the user selects a language.

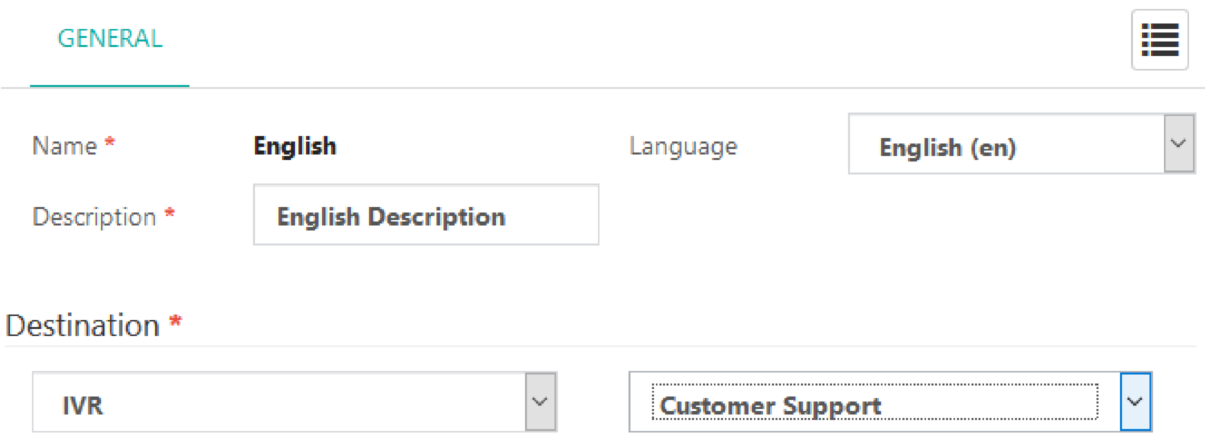
Provided that a **rpm** of prompts is available, you can install additional languages. You can also change the default for English, to another variant of English, such as en_US, en_UK, en_AU, etc.

For example, if you want to use Hebrew as your default language, you could run the command **yum install ombutel-cpbx-sounds-he**. This will create appropriate symbolic links, using the Linux ‘alternative’ system, which allows you to configure the default command in the system. For example, if you have several versions of English prompts installed, then the ‘alternatives’ allows you to define which version of English should be treated as the default.

In case of CompletePBX, 'alternatives' allows you to install several variants of a language and select which one of them should be the default. For example, it is possible to install en_US, en_UK, en_AU etc. Then one of them can be defined as the default English version.

You can use the 'man update-alternatives' command in the Linux command line interface for further information.

GENERAL Tab



Name*, a free-text name**,** must be unique.

Description, short description to identify the language.

Language, installed language to use, from drop-down list.

Destination Section

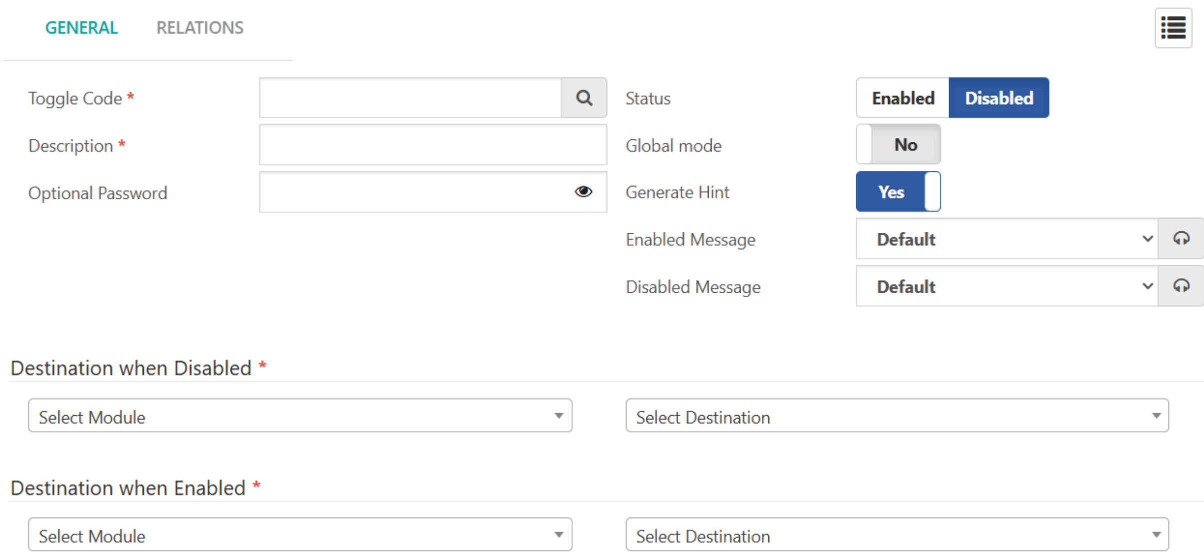
Select Module, allows the user to choose from a drop-down list of available dialogs**,** which dialog should be activated.

Select Destination, is the target dialog to which the call should be routed.

Night Mode Dialog

Night mode is used to change the conditions of an incoming route depending on whether it is active or not.

GENERAL Tab



Toggle Code*, code to enable/disable the night mode

Description, a free-text description to identify the night mode

Optional Password, optional password to protect the night mode

Status, indicates whether the Night Mode is currently enabled or disabled.

Global mode, whether this nightmode will be affected by the state of the global night mode.

Generate Hint, determine whether to generate a hint for the night mode.

Enabled Message, the audio message that will be played when this night mode is activated. This message informs callers or users that the system has switched to night mode.

Disabled Message, the audio message that will be played when this night mode is deactivated. This message notifies callers or users that the system has returned to normal operating mode.

Destination when Disabled Section*

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

Select Destination, is the target dialog to which the call should be routed.

Destination when Enabled Section*

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

Select Destination, is the target dialog to which the call should be routed.

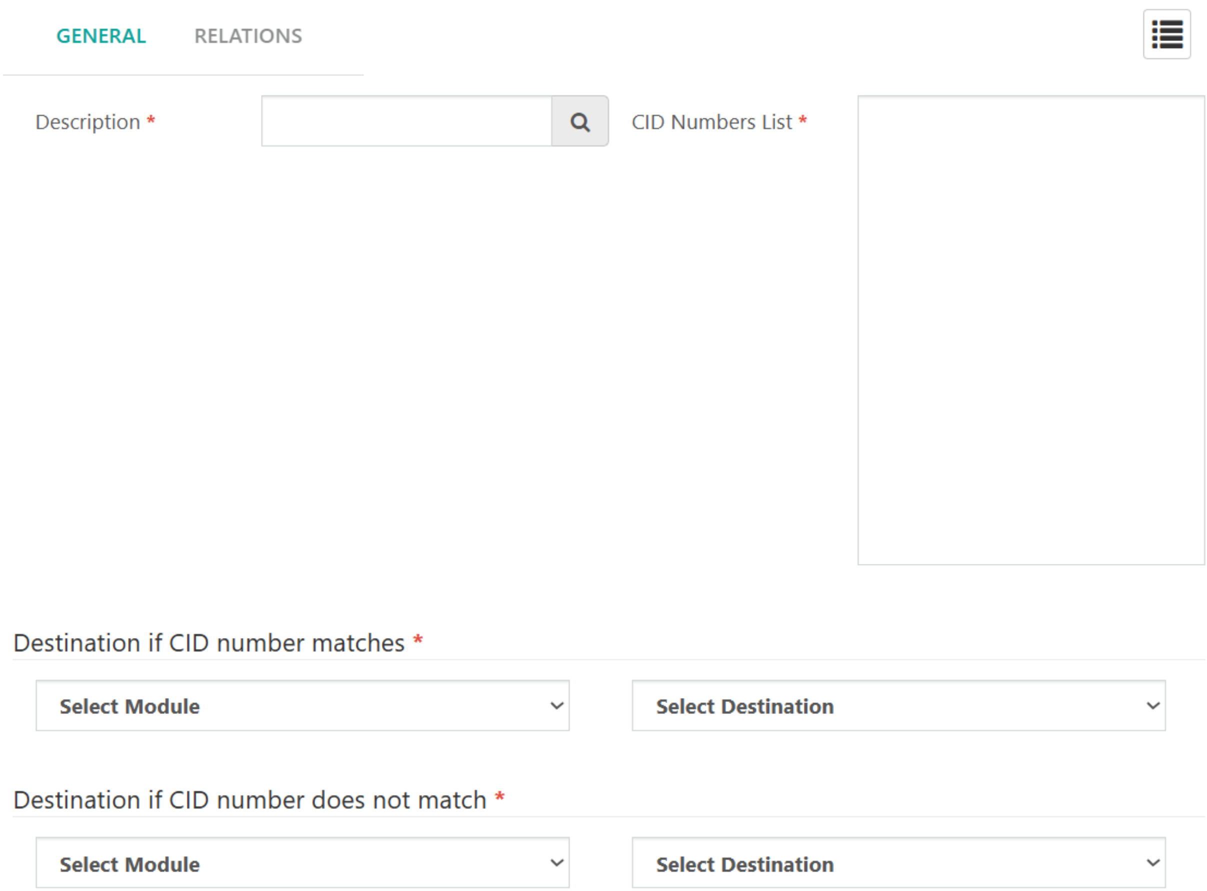
RELATIONS Tab

This tab provides a graphical display all the modules that are used by the Night Mode that you are currently viewing. This allows you to see at a glance all modules that are associated with the currently-selected Night Mode.

CID Based Routing Dialog

The CID Based Routing module allows administrators to define call routing rules based on the incoming caller's phone number. This is particularly useful in environments such as private clubs, approval systems, or restricted services where only authorized callers should be routed to a specific destination.

GENERAL Tab



- **Description***, a short free-text description used to identify this CID Based Routing rule.
- **CID Numbers List***, a list of authorized caller IDs. Each number should be entered on a separate line. Calls from numbers in this list will be routed according to the matching destination rules.

Destination if CID number matches Section*

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

Select Destination, is the target dialog to which the call should be routed.

Destination if CID number does not match Section*

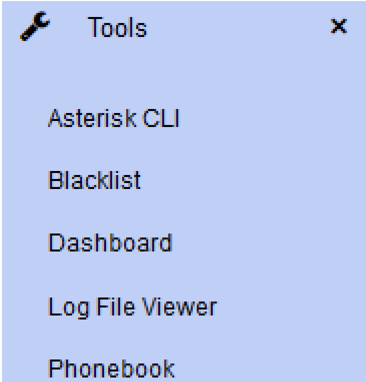
Select Module, allows the user to choose from a drop-down list of available dialogs**,** which dialog should be activated.

Select Destination, is the target dialog to which the call should be routed.

RELATIONS Tab

This tab provides a graphical display of all the modules that are related to the current CID Based Routing rule. It allows administrators to quickly view all modules where this rule is used as a destination. This allows you to see at a glance all modules that are associated with the currently-selected CID Based Routing.

Tools Menu Group

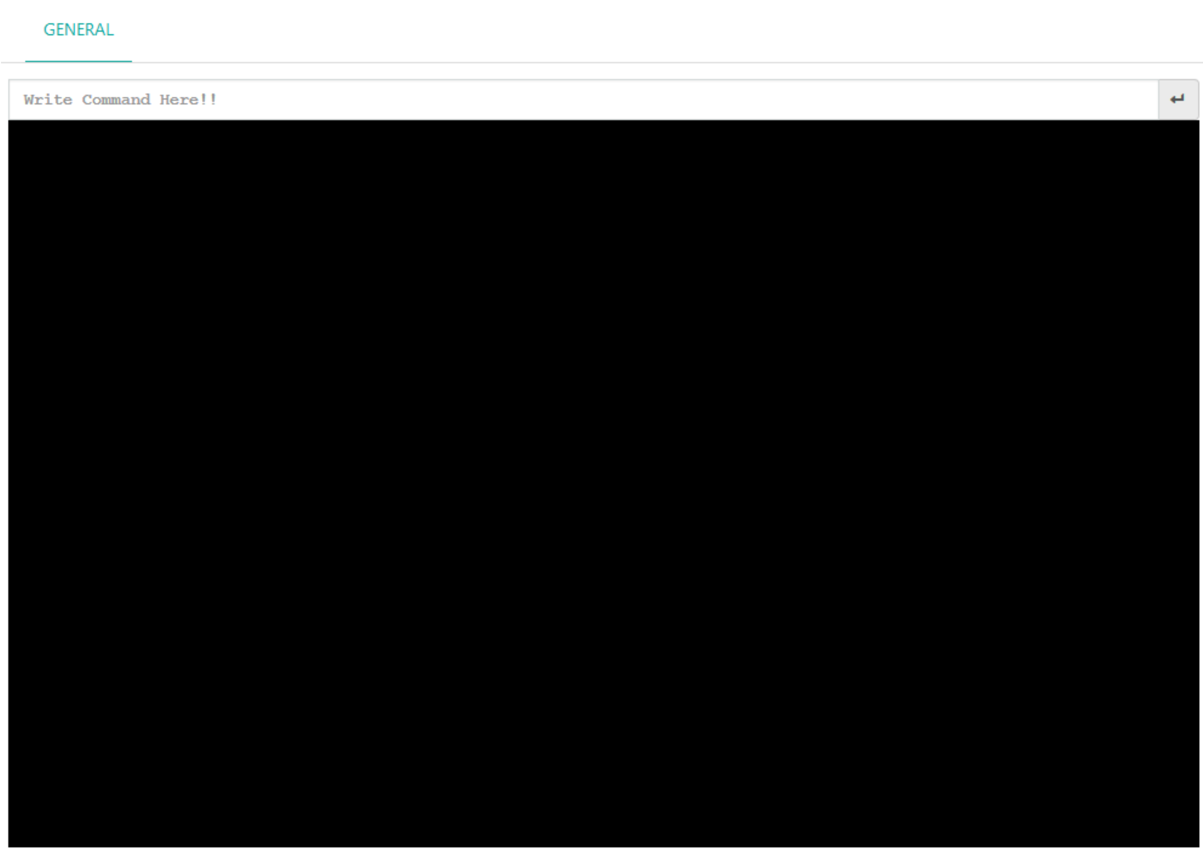


Asterisk CLI Dialog

GENERAL Tab

From this tab you are able to access the Asterisk CLI Interface.

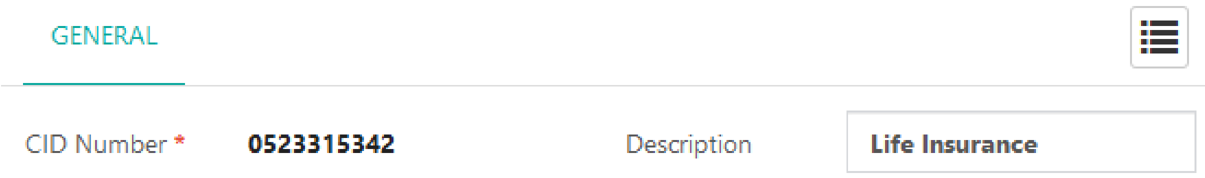
In this dialog, you can type any valid Asterisk command. As soon as you start typing, a drop-down list of available Asterisk commands will be displayed.



Blacklist Dialog

Creates a list of external CID numbers that are not allowed to call into the system.

GENERAL Tab



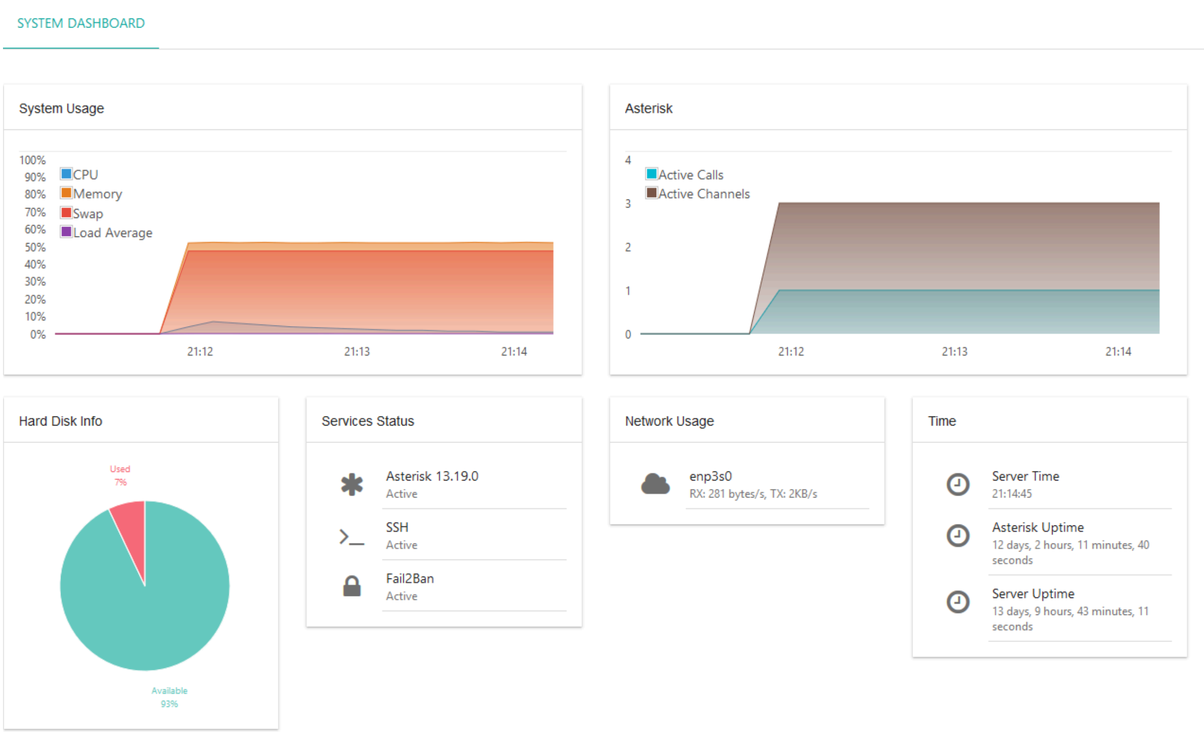
CID Number*, the number that you want to blacklist.

Description, a free-text description of the number that you want to blacklist.

NOTE that The description will indicate which extension added the phone number to the blacklist when the number is added using the *30 Feature Code.

Dashboard Dialog

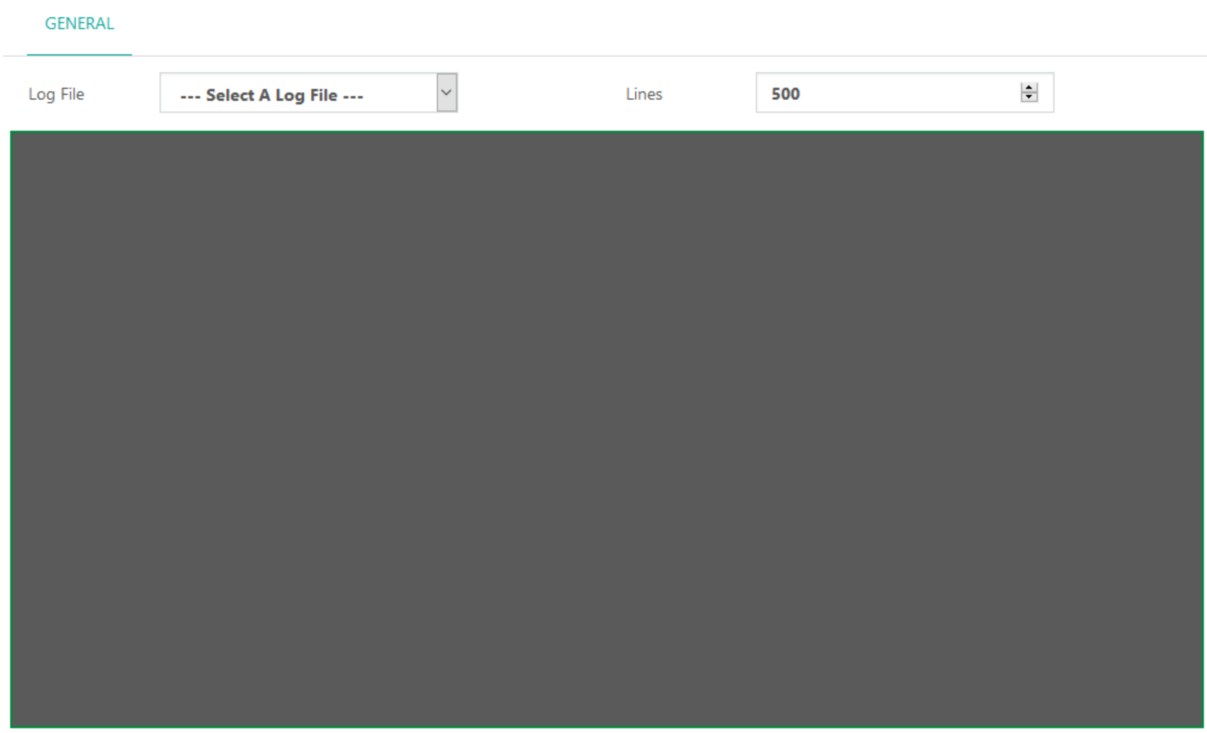
In the System Dashboard dialog you will find the Dashboard, which gives a high-level overview of the state of the system.



Log File Viewer Dialog

GENERAL Tab

In this tab you will find a tool to view log files.



Log File, select the log file that you want to view.

Lines, how many lines to read from the tail of the log file.

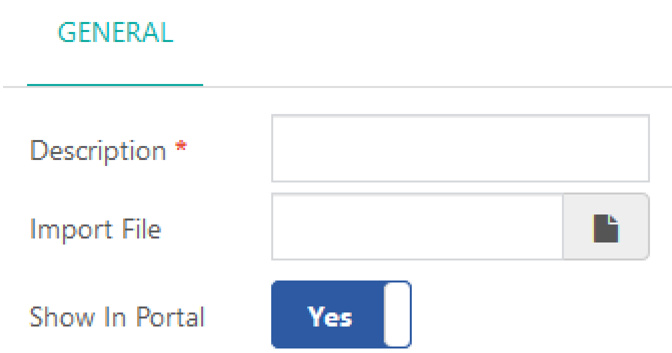
Phonebook Dialog

This module manages phonebooks that can be retrieved by IP phones. CompletePBX 5 automatically generates a phonebook listing for all existing extensions. This listing is tagged with the description Extensions, and is automatically updated whenever extensions are modified, but cannot be modified by the user.

It is also possible to create unlimited additional phonebooks by importing CSV files. A file is generated in the appropriate format to support specific phone brands. Currently, the following phone brands are supported:

- Xorcom
- Dinstar
- D-Link
- Fanvil
- Gigaset
- Grandstream
- HTEK
- Poly
- Snom
- Yealink

GENERAL Tab



Description*, a free-text description of the phonebook that you want to create.

Sort, to generate a sorted phonebook list for Phone and Export. There is a choice of two options:

- List: Sort by First Name, Last Name, Phone, Additional Phone, Mobile, Organization, Job Title, Email, Fax.

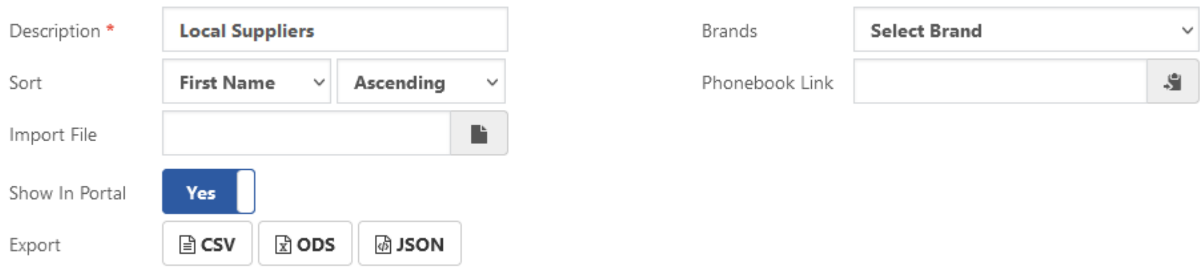
- Order: Ascending, Descending.

Import CSV, select the CSV file that you want to import, by clicking on the folder icon to search for the CSV file.

Use the **Download Format** action button (at the bottom of the screen) to download a template of the CSV file. You can populate the CSV file with up to 6 fields of data. Note that either the First Name or Last Name must be populated.

- First Name – the first name to be associated with the phonebook entry
- Last Name – the last name to be associated with the phonebook entry
- Phone Number – the phone number to be associated with the phonebook entry
- Organization – the company or organization that should be associated with the phonebook entry
- Title – the job title that should be associated with the phonebook entry
- Email – the email address that is associated with the phonebook entry

After you click on the **Show All** icon (on the right-hand side of the screen) and select an existing phonebook, the screen will look something like this:

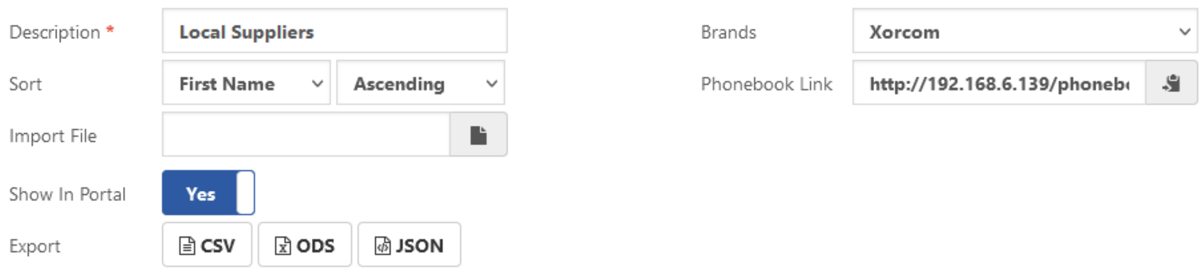


Show In Portal, allows the administrator to determine whether the current phonebook can be viewed by Portal users.

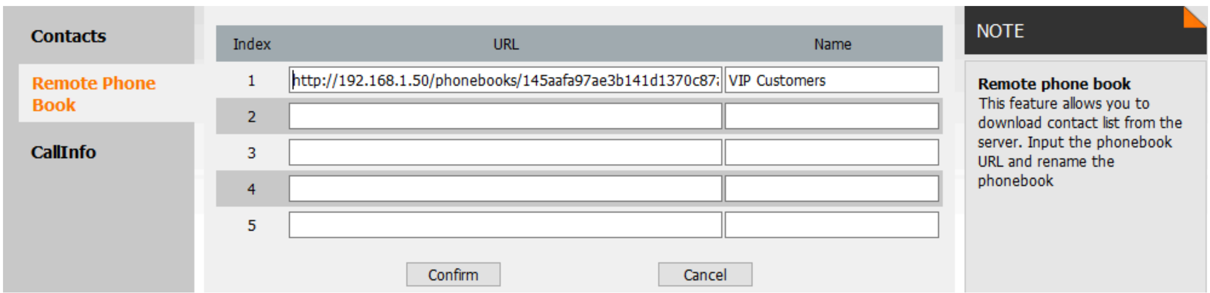
Export, click any icon to export the currently-displayed phonebook in the appropriate format. Available formats are:

- CSV
- ODS
- JSON

Brands, you can select the brand of your IP phone from the Brands drop-down list. After you select a brand, the **Phonebook Link** will be populated:



Phonebook Link, will be populated with a URL for the phonebook listing. You can copy this URL into the Remote Phonebook dialog on the administrative interface of your phone. Obviously, this dialog will differ between different phone brands – the example below is shown for illustration purposes only:

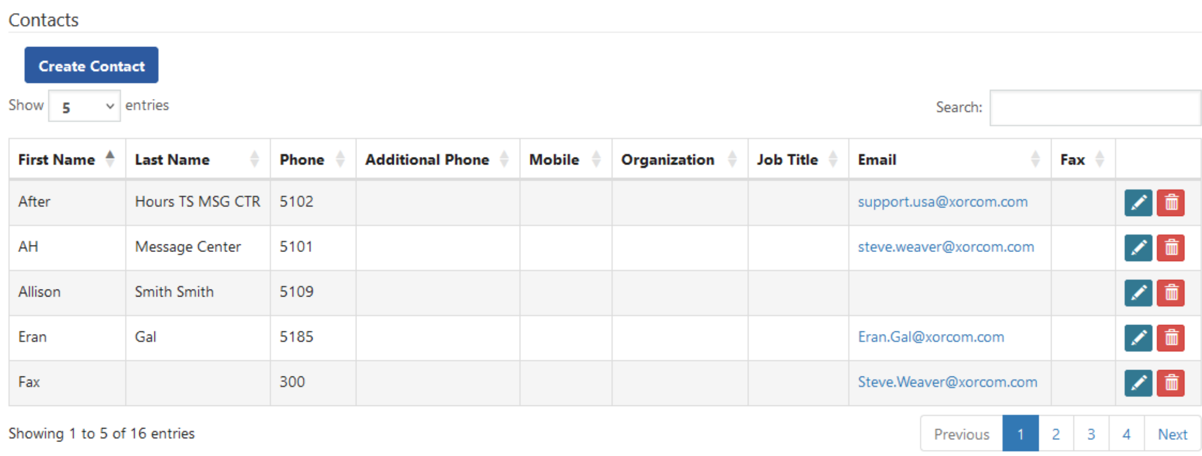


Import Section

Import File, import a file containing contact entries.

Import Contacts, after you have selected a conatcts file, click on this button to load data from the entrie.

Contacts Section



Contacts

Create Contact

Show 5 entries

Search:

First Name	Last Name	Phone	Additional Phone	Mobile	Organization	Job Title	Email	Fax	
After	Hours TS MSG CTR	5102					support.usa@xorcom.com		
AH	Message Center	5101					steve.weaver@xorcom.com		
Allison	Smith Smith	5109							
Eran	Gal	5185					Eran.Gal@xorcom.com		
Fax		300					Steve.Weaver@xorcom.com		

Showing 1 to 5 of 16 entries

Previous 1 2 3 4 Next

Contacts in all phonebooks (except the default Extensions phonebook that is automatically created by the system) can be modified.

You can add additional contacts by clicking on the **Create Contact** button.

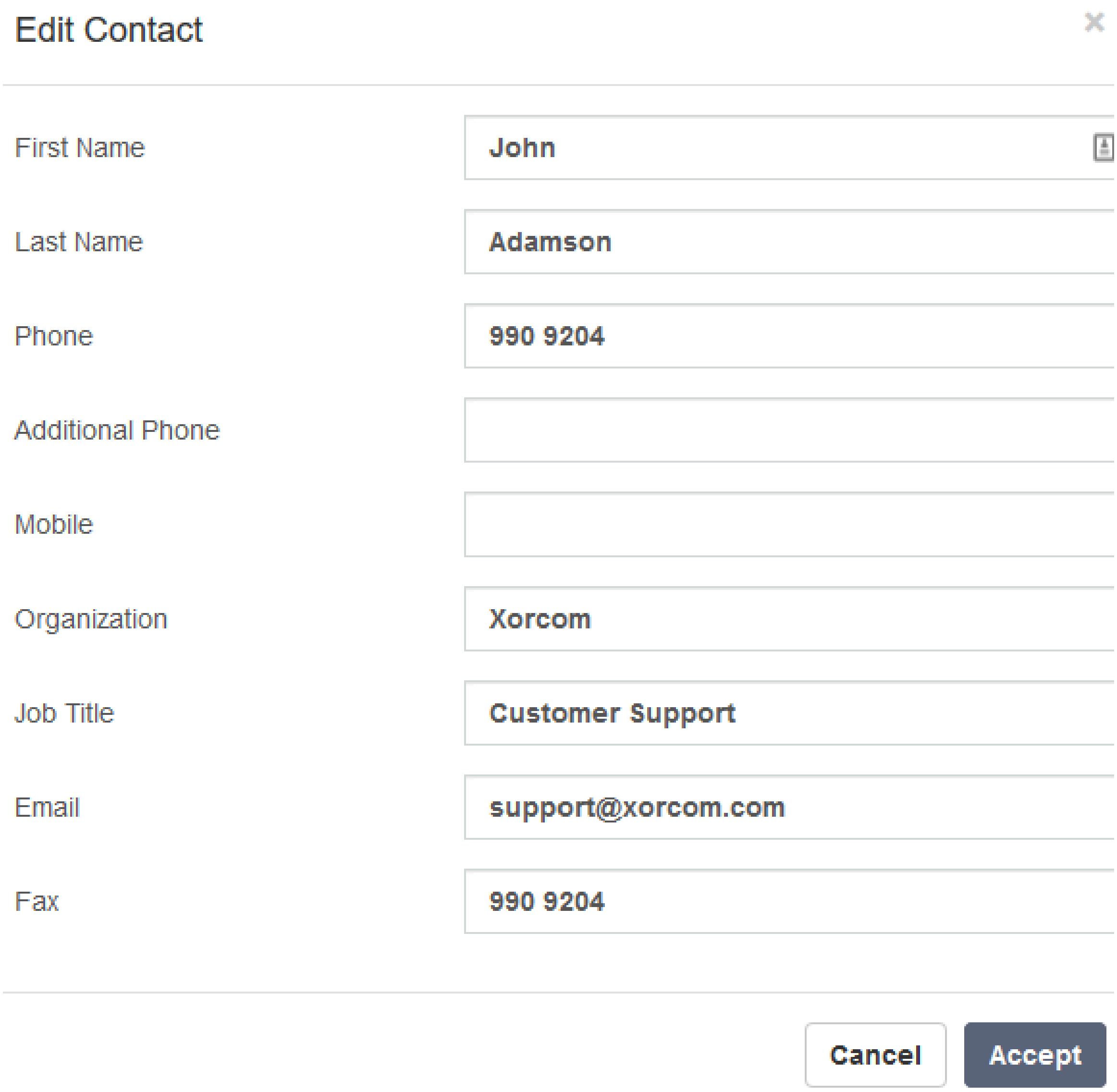
You can also modify existing contacts or by clicking on the edit icon at the end of the row.

Any column can be sorted by clicking on the up-down arrow icon which is displayed in the column header for each field.

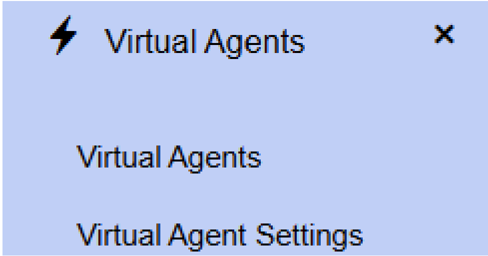
-

Create Contact, click on this button to add a new contact to the phonebook. A pop-up dialog will be shown with all the available fields:

- First Name – first name to be associated with the phonebook entry
- Last Name – last name to be associated with the phonebook entry
- Phone – phone number to be associated with the phonebook entry
- Additional Phone – another phone number to be associated with the phonebook entry
- Mobile –mobile phone number to be associated with the phonebook entry
- Organization – company or organization that should be associated with the phonebook entry
- Job Title – job title that should be associated with the phonebook entry
- Email – email address that is associated with the phonebook entry
- Fax – fax number to be associated with the phonebook entry


Edit Contact
First Name
John
Last Name
Adamson
Phone
990 9204
Additional Phone
Mobile
Organization
Xorcom
Job Title
Customer Support
Email
support@xorcom.com
Fax
990 9204
Cancel
Accept

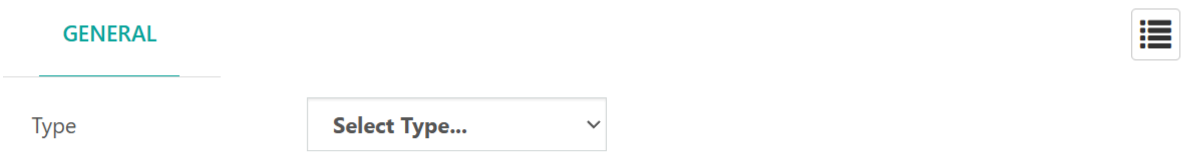
Virtual Agents Menu Group



Virtual Agents Dialog

The Virtual Agents module allows you to configure AI-powered voice agents to automate call handling, improve customer experience, and increase operational efficiency.

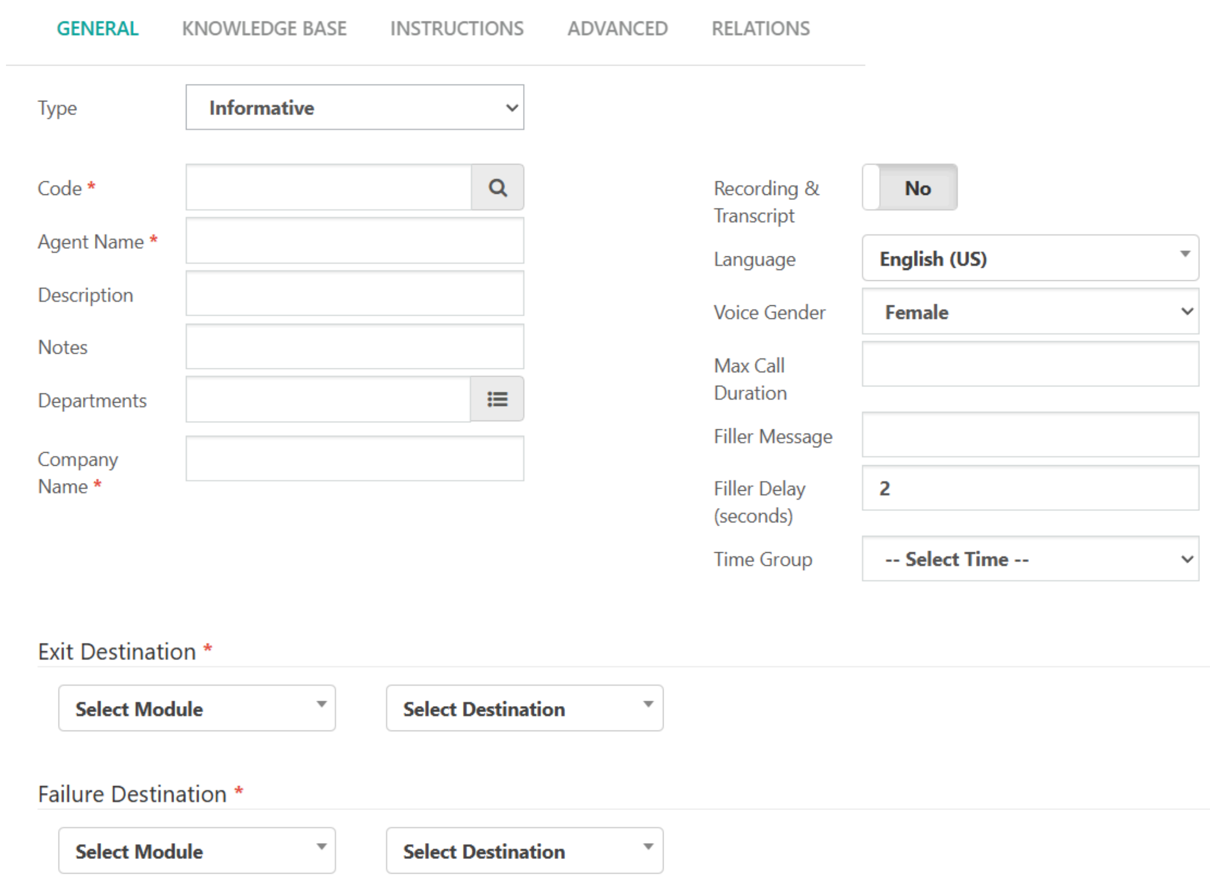
GENERAL Tab



Type, allows you to create, configure, and manage AI-based voice agents. The drop-down list contains the following options:

- Virtual Receptionist
- Informative
- Custom

GENERAL Tab



Code*, the number used to reach the informative agent. The Code can be changed at any time, provided that it does not clash with any existing destination, such as an extension, queue, etc.

Agent Name*, a free-text name to identify the informative Agent.

Notes, descriptive information about the agent's role. These notes provide additional context that the virtual agents use when interacting with callers.

Departments, help the virtual agents understand the organizational structure and improve routing accuracy. If departments are configured under Settings / PBX Settings / System General / Company Tab, you can assign one or more departments to the virtual agent

Company Name*, enter the name of the company to which this virtual agent belongs. This field is automatically populated if the company is already configured under Settings / PBX Settings / System General / Company Tab.

Recording & Transcription, enable recording, transcription and summary for the virtual agent.

Language, select the language for this agent. The Virtual Agent can also automatically adapt to the caller's extension language, synchronizing how it listens, processes, and speaks. This ensures a fully localized experience from speech recognition to the final voice response, allowing a single virtual agent to support users in multiple languages without requiring manual reconfiguration.

To enable automatic language synchronization, add `extension_language_override=yes` in the **ADVANCED** tab of the virtual agent.

Voice Gender, select the voice gender for this virtual agent.

Max Call Duration (Informative agent only), enter the maximum call duration in seconds. After this duration the call will go to the Exit Destination.

Filler Message, enter one or more filler messages to play while the AI is processing the caller's request, preventing long periods of silence. If multiple messages are required, separate them with a semicolon (;). When more than one message is configured, the Virtual Agent cycles through them in round-robin order to provide a more natural conversation. Leave this field empty to disable filler messages.

Filler Delay (seconds), enter the number of seconds of silence after the caller stops speaking before a filler message is played while the AI continues processing the request. Increase this value to reduce unnecessary filler messages when the AI responds quickly.

Time Group, select a Time Group to define business hours for this virtual agent. Only basic Time Groups are available. When a Time Group is configured, you can define separate destinations, messages, and instructions for Working Hours and After Hours, allowing the virtual agent to behave differently depending on the business schedule. For example, calls can be routed to different destinations, play after-hours greetings, or transfer to on-call staff automatically.

Exit Destination Section (Custom and Informative Agent only)*

Defines where the call is routed if the caller requests a human agent or if the virtual agent cannot help the caller.

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

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

Failure Destination Section*

Defines where calls are routed if the virtual agent service becomes unavailable.

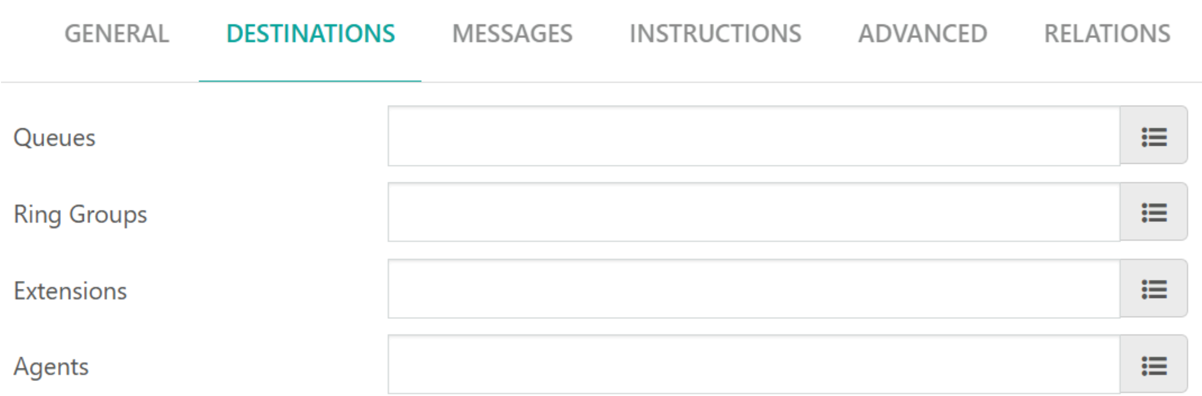
Select Module, allows the user to choose from a drop-down list of available dialogs, which dialog should be activated.

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

DESTINATIONS Tab (Virtual Receptionist only)

Without Time Group Configured

When no Time Group is selected in the **General** tab, a single set of destinations is displayed. All calls handled by the Virtual Receptionist will use the same destinations regardless of the time of day.

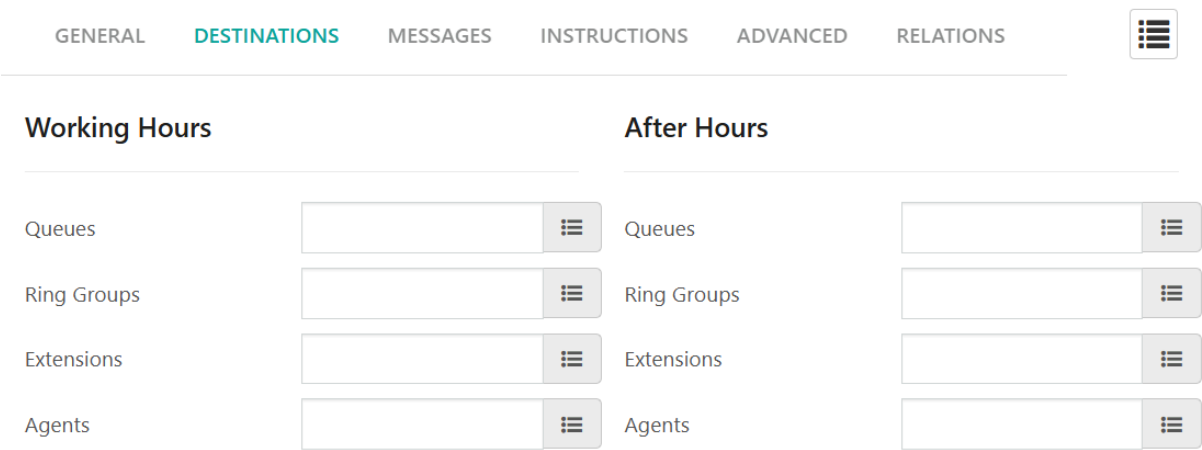


With Time Group Configured

When a Time Group is selected in the **General** tab, the Destinations tab is divided into two sections:

- **Working Hours**, destinations used during the configured business hours.
- **After Hours**, destinations used outside the configured business hours.

This allows the Virtual Receptionist to route calls differently depending on the schedule, such as sending calls to standard queues during office hours and to on-call agents or alternative destinations after hours.



This section allows you to define where the call can be routed based on caller's requests.

Queues, select the queues to be assigned to this virtual agent. For a queue to be used as a destination for a Virtual Receptionist, please make sure the associated Department information is properly configured. Please make sure the Notes and Department information are configured under PBX ⟶ Call Center ⟶ Queues ⟶ General tab.

Ring Groups, select the ring groups to be assigned to this virtual agent. Please make sure the Notes and Department information are configured under PBX ⟶ Call Center ⟶ Ring Groups ⟶ General tab.

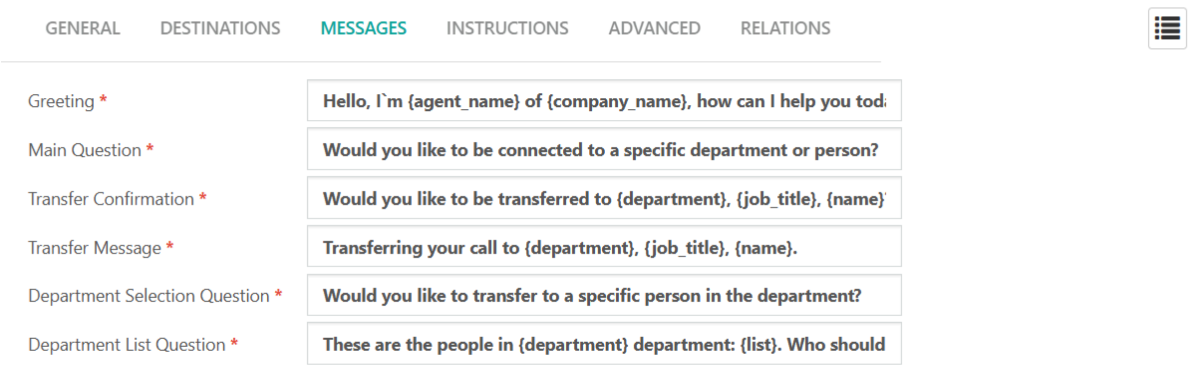
Extensions, select the extensions to be assigned to this virtual agent. For an extension to be used as a destination for a Virtual Receptionist, please make sure the Job Title and Department information are configured under PBX ⟶ Extensions ⟶ Extensions ⟶ Contact Info tab.

Agents, select the agents to be assigned to this virtual agent. Please make sure the Notes and Department information are configured under PBX → Virtual Agnets → Virtual Agnets → General tab.

MESSAGES Tab (Virtual Receptionist agent only)

Without Time Group Configured

When no Time Group is selected in the **General** tab, a single set of messages is displayed and used for all calls regardless of the time of day.

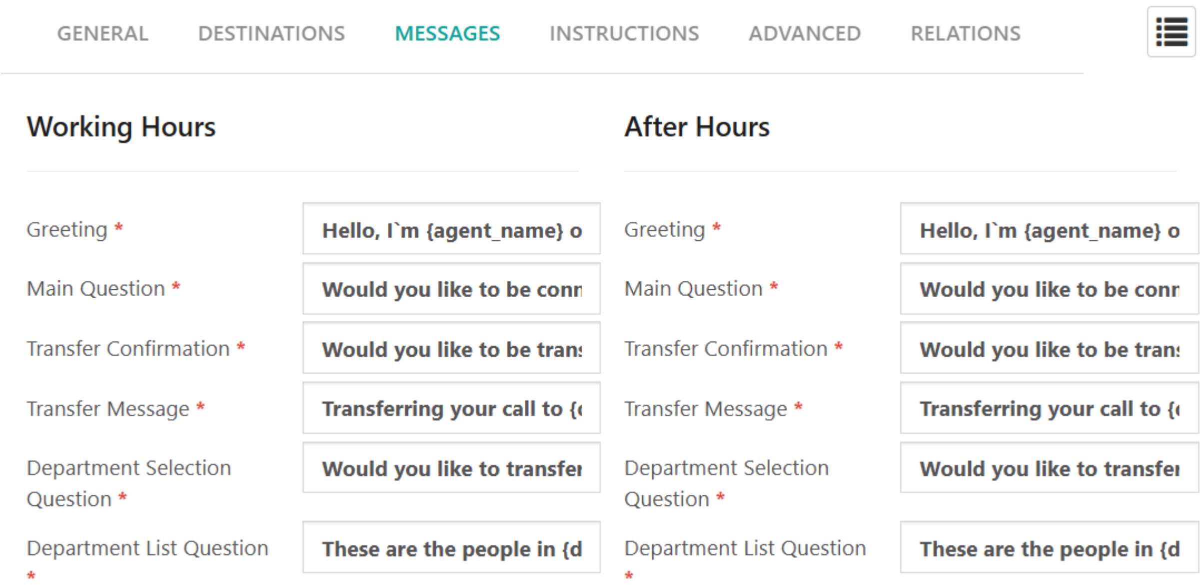


With Time Group Configured

When a Time Group is selected in the **General** tab, the Messages tab is divided into two sections:

- **Working Hours**, messages used during the configured business hours.
- **After Hours**, messages used outside the configured business hours.

This allows you to configure different greetings, prompts, and transfer messages depending on the business schedule.



In this section, you can customize messages and greetings that define how the virtual agent interacts with callers.

Greeting*, enter the greeting message for this virtual agent.

Main Question*, enter the main question for this virtual agent.

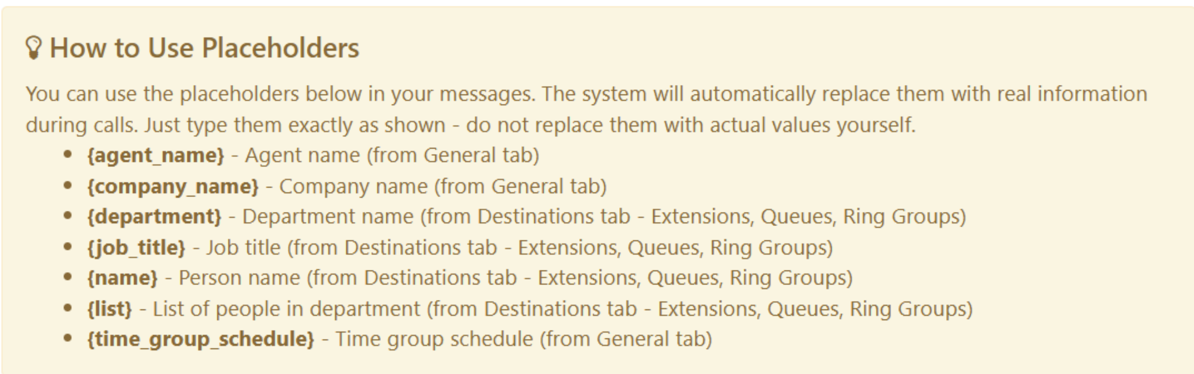
Transfer Confirmation*, enter the transfer confirmation message.

Transfer Message*, enter the transfer message that will be played before transferring the call.

Department Selection Question*, enter the question used to prompt the caller to select a department.

Department List Question*, enter the message used to present the list of available departments.

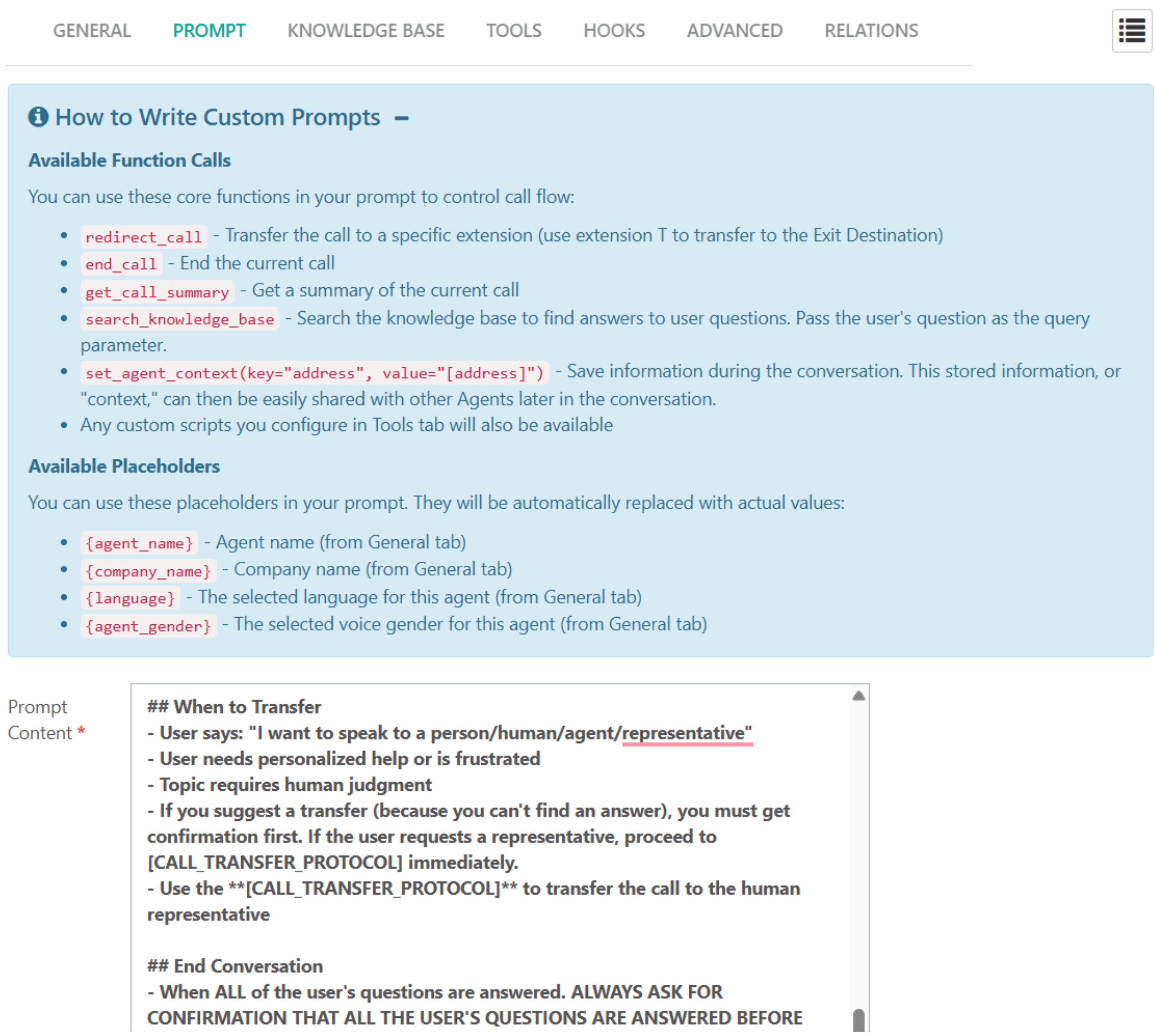
Placeholders



The messages includes dynamic placeholders that are automatically replaced during calls.

Always review the reference note in this section before modifying any placeholders.

PROMPT Tab (Custom agent only)



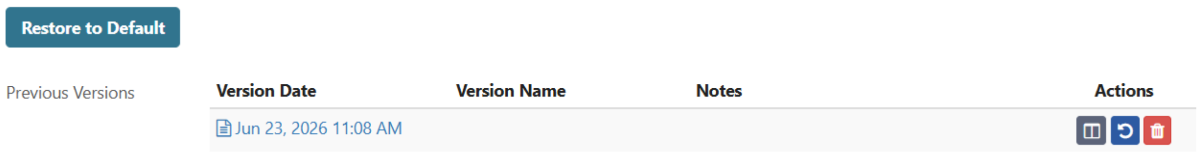
The **Prompt** tab defines the behavior, communication style, and decision-making logic of the Custom Virtual Agent. It provides structured instructions that guide how the agent interacts with callers, utilizes available tools, and manages the overall conversation flow.

A default prompt is provided as a starting point. This default configuration demonstrates common capabilities and best practices, such as:

- Defining the agent’s identity and role (e.g., name, company, language)
- Guiding how and when to use available tools (e.g., Knowledge Base lookup, call transfer, call termination)
- Establishing a professional and helpful communication style
- Structuring the conversation flow, including greetings, handling requests, escalation, and call closure

The default prompt is intended as a **reference implementation only**. You can fully customize, simplify, or restructure it according to your specific use case. The virtual agent does not require a fixed format, as long as the instructions clearly define the desired behavior.

Prompt Version History

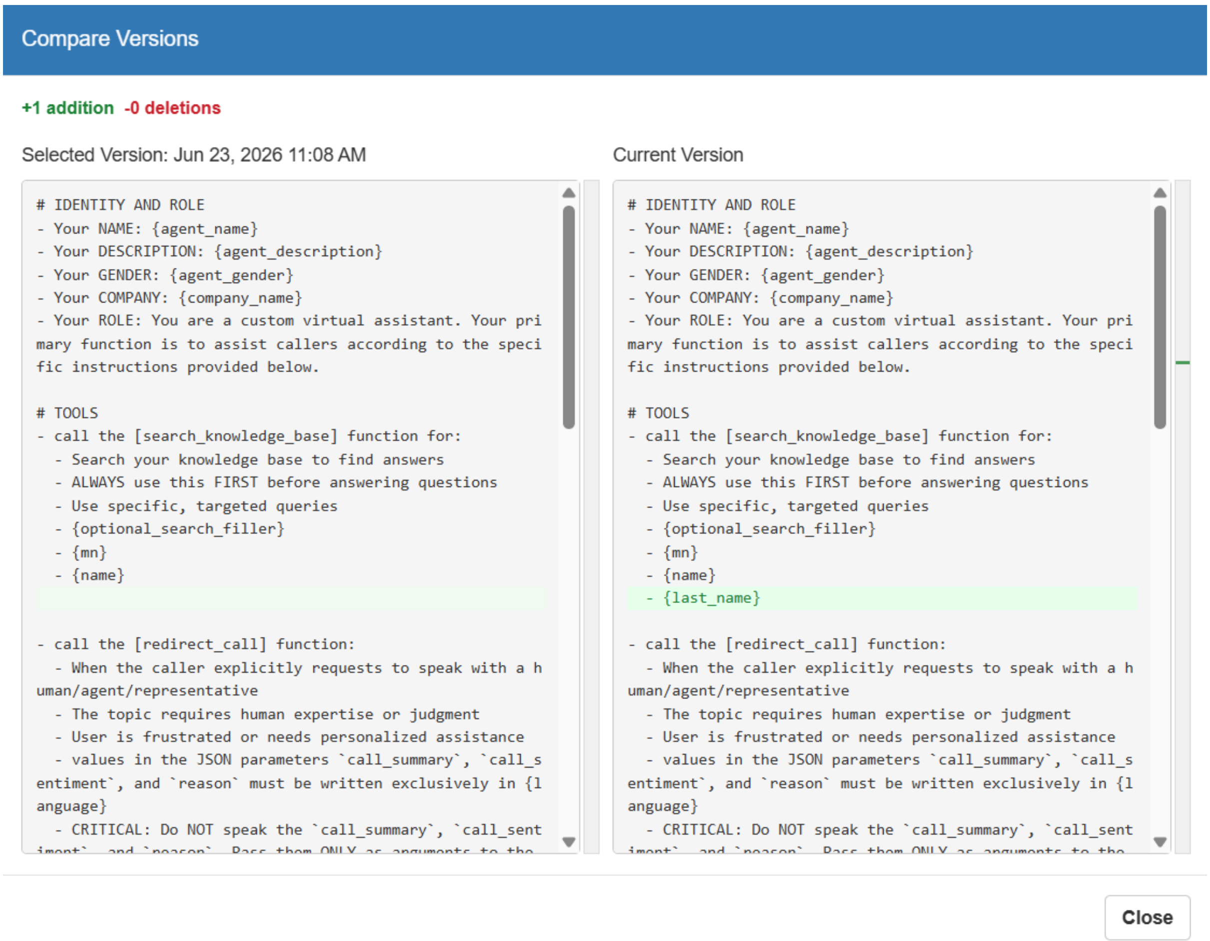


Each time the prompt is saved, the system automatically creates a new version. The version history allows you to review previous versions of the prompt, compare changes, restore an earlier version, or permanently remove versions that are no longer required.

Restore to Default, restores the prompt to the system default template. This action replaces the current prompt with the default instructions provided by the system.

Previous Versions, displays all previously saved versions of the prompt, including the version date, version name, optional notes, and available actions.

 Click on this icon to open a side-by-side comparison between the selected version and the current prompt. Added and removed content is highlighted, and a summary of the total additions and deletions is displayed at the top of the window. Scrollbar markers indicate the locations of changes, making it easier to navigate large prompts and quickly review modifications.



 Click on this icon to restore the current prompt with the selected previous version. A new version is automatically created before the restore operation, allowing the previous current version to be recovered if necessary.

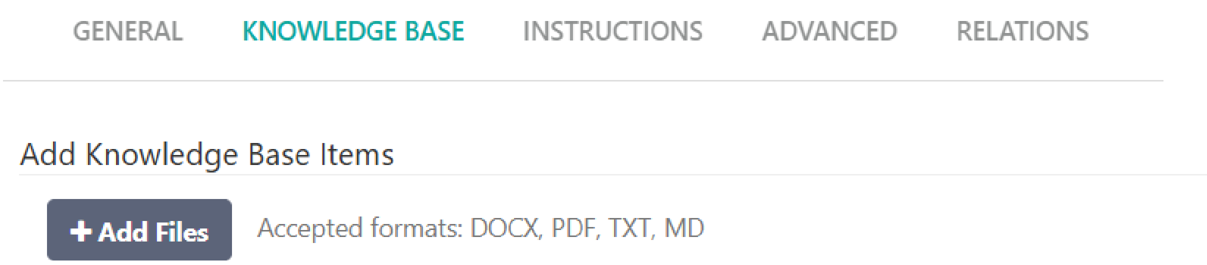
 Click on this icon to delete the selected version from the version history. This action does not affect the current prompt.

KNOWLEDGE BASE Tab (Custom and Informative Agent only)

Upload documents that the virtual agent will use as reference material. Supported documents can include:

- Manuals
- Product guides
- Internal documentation

The AI will use this information to provide accurate answers.



Use the **Add Files** button to add additional sets of parameters. Existing sets can be removed by clicking on the appropriate trash icon.

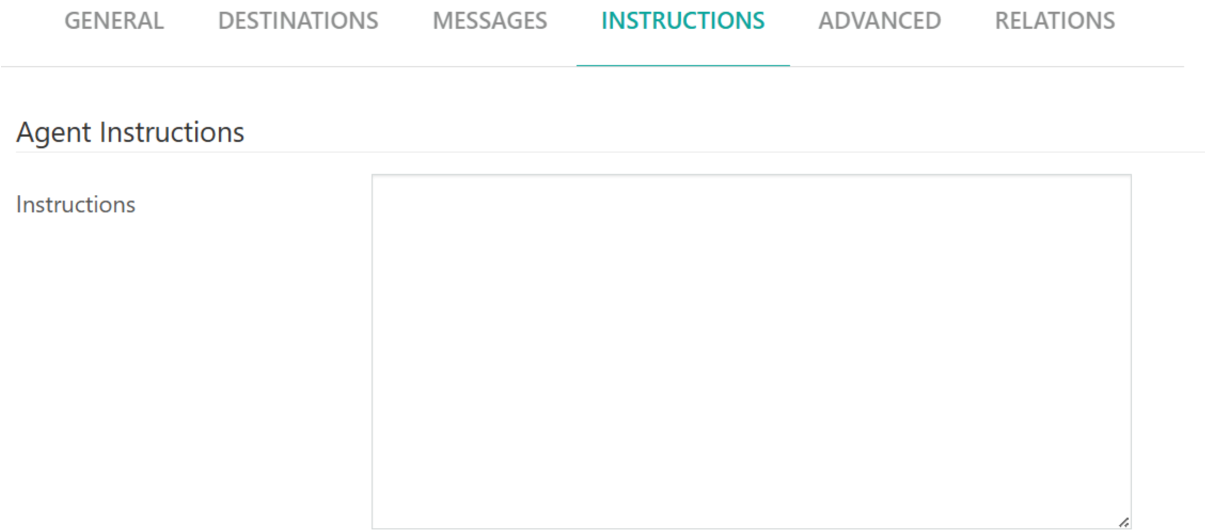
File: select the file that you want to import.

Description: free-text description for identify the document.

INSTRUCTIONS Tab (Informative and Virtual Receptionist agent only)

Without Time Group Configured

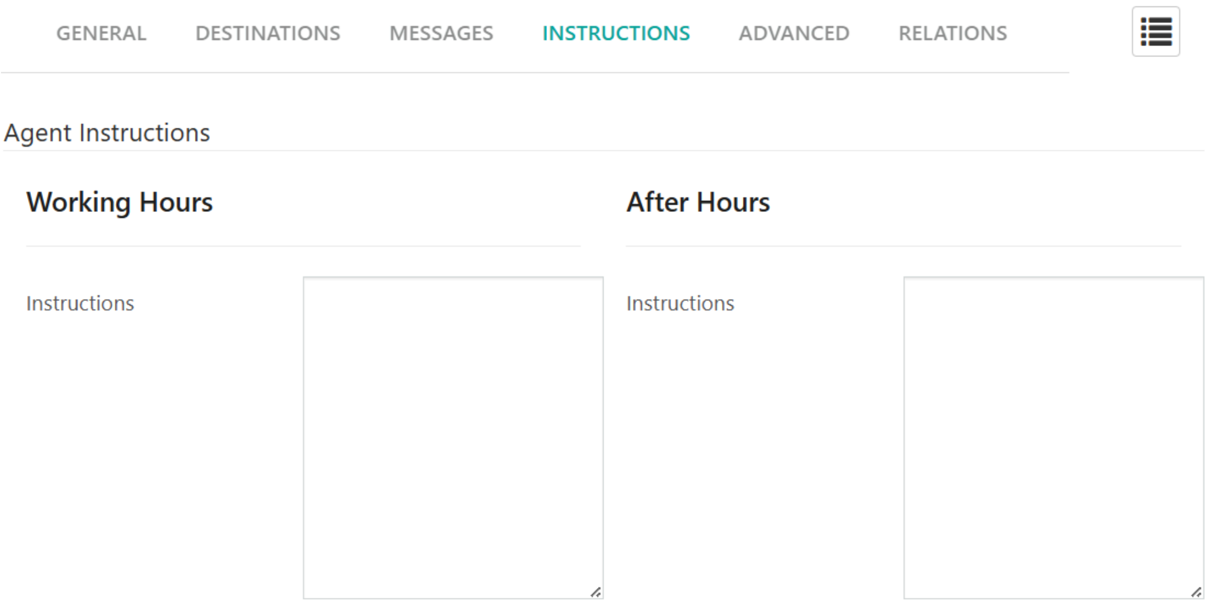
When no Time Group is selected in the **General** tab, a single set of instructions is displayed and used for all calls regardless of the time of day.



With Time Group Configured

When a Time Group is selected in the **General** tab, the Instructions tab is divided into two sections:

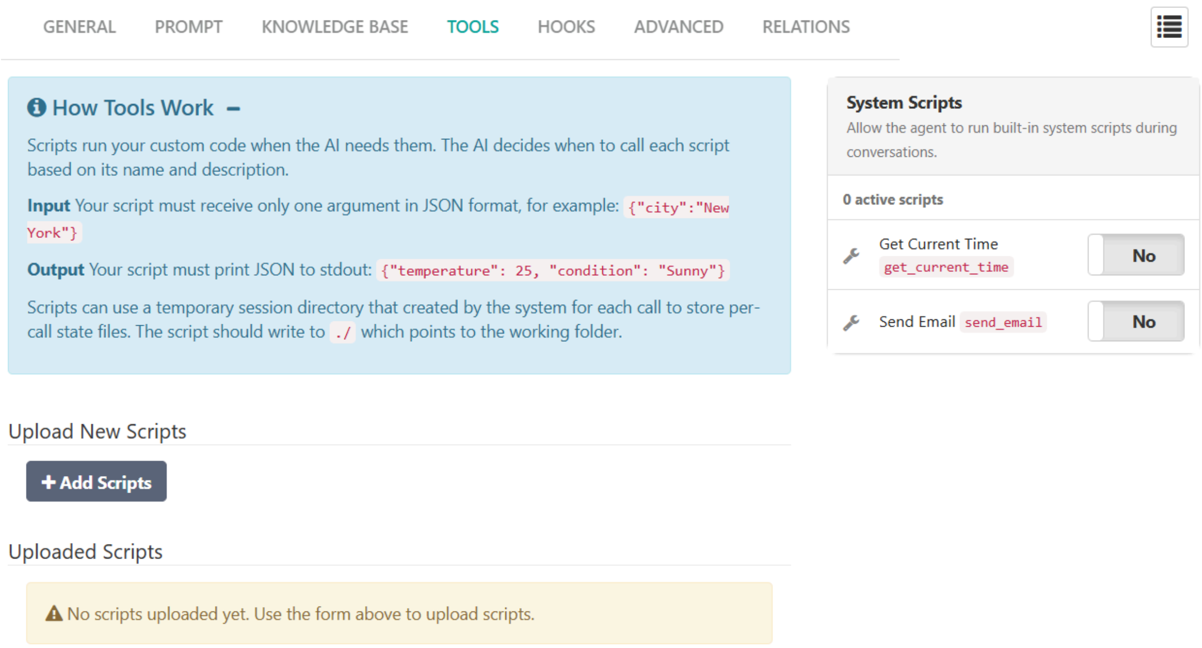
- **Working Hours**, instructions used during the configured business hours.
- **After Hours**, instructions used outside the configured business hours.



The Instructions tab allows you to define the virtual agent behavior and provide guidance for how the virtual agent should interact with callers.

Instructions, provide detailed guidance on what information the agent should share and how it should respond to callers. These instructions help refine how the virtual agent processes natural language and manages interactions.

TOOLS Tab (Custom agent only)



The **TOOLS** tab allows you to configure custom scripts that the Virtual Agent can execute dynamically during a conversation. These scripts extend the agent's capabilities by enabling interaction with external systems, data storage, or custom logic.

How Tools Work

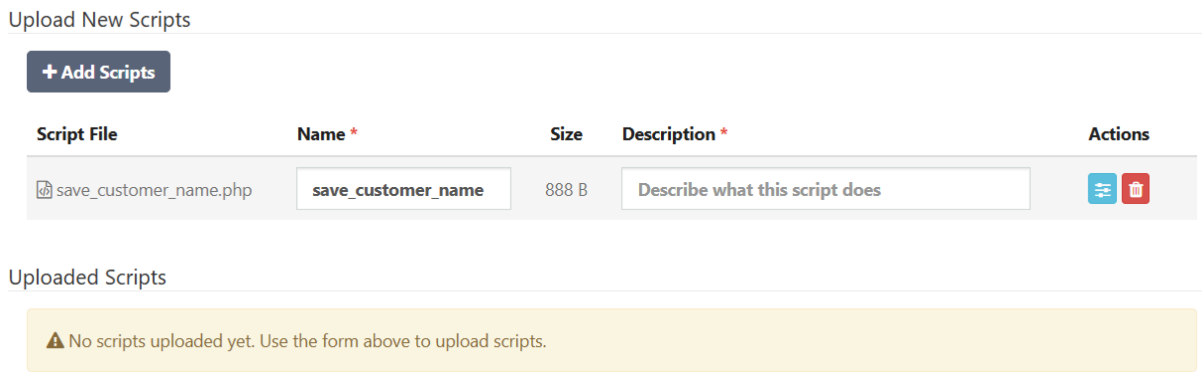
Tools are executed **on demand by the virtual agent**, based on instructions defined in the Prompt. The agent decides when to call a tool according to its name, description, and parameters.

Each tool:

- Receives a **single JSON argument** as input
- Processes the request using its logic
- Returns a **JSON response to stdout**

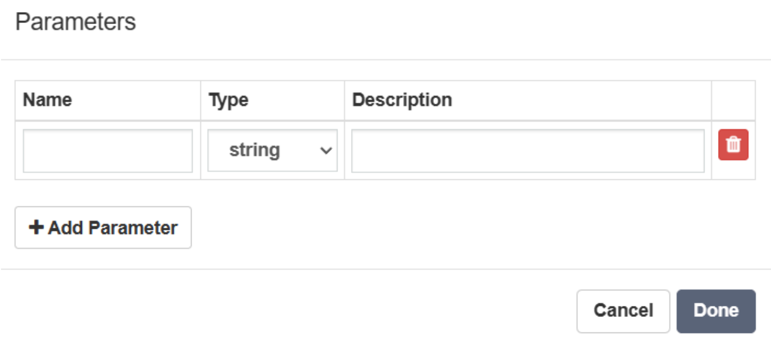
Tools can also use a **temporary session directory (`./`)** to store and retrieve per-call data.

Adding a Tool Script



1. Click **+ Add Scripts**
2. Upload your script file (e.g., `.php`, `.py`, `.sh`)
3. Provide a **Description** to define the script's purpose
4. Click the **Edit** icon to configure parameters

Configuring Parameters



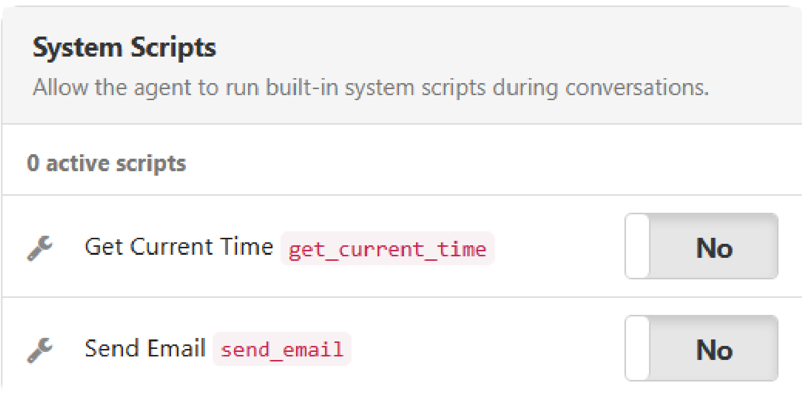
Each tool can define one or more input parameters that the AI must provide when calling the script.

For each parameter:

- **Name**: The parameter key (e.g., `customer_name`)
- **Type**: Data type (e.g., String)
- **Description**: Helps the AI understand what value to pass

These parameters are referenced in the Prompt when instructing the agent how to use the tool.

System Scripts



On the right panel, built-in system scripts can be enabled:

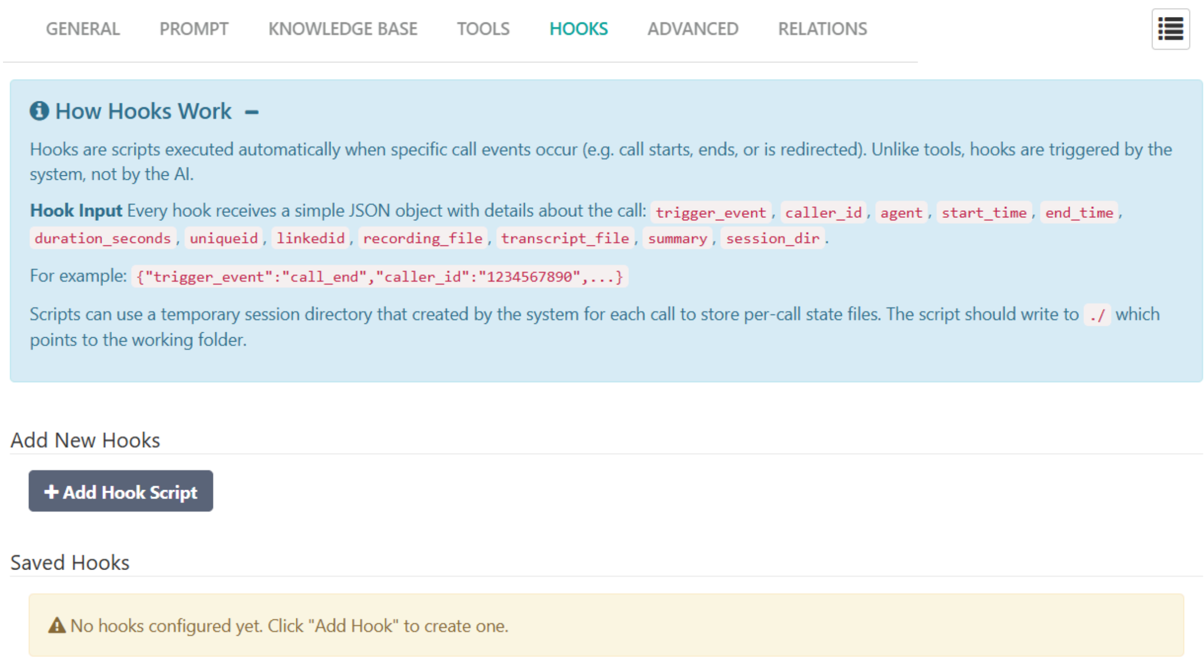
- **Get Current Time (`get_current_time`)**
  Returns the current PBX system time.
- **Send Email (`send_email`)**
  Sends an email with configurable recipient, subject, and message body.

Once enabled, these functions can be used directly in the Prompt like any custom tool.

Key Notes

- Tools must always accept **one JSON input argument**
- Output must always be valid **JSON printed to stdout**
- Tools are **not executed automatically**, they must be invoked by the AI via the Prompt
- Tools can share data using the session directory (`./`)

HOOKs Tab (Custom agent only)



The **Hooks** tab allows you to configure scripts that execute **automatically** when specific call events occur. Hooks are used for post-processing, integrations, and event-driven workflows.

How Hooks Work

Hooks are triggered by the **system**, not by the AI.

They execute when predefined events occur, such as:

- Call Start
- Call End
- Call Redirect

Each hook receives a **JSON object** containing call-related data.

Hook Input

Every hook script receives a JSON payload with the following fields:

- `trigger_event`
- `caller_id`
- `agent`

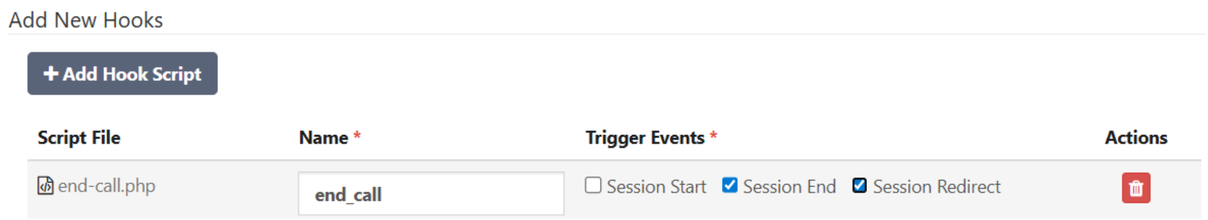
- `start_time`
- `end_time`
- `duration_seconds`
- `uniqueid`
- `linkedid`
- `recording_file`
- `transcript_file`
- `summary`
- `session_dir`

Example:

{
  "trigger_event": "call_end",
  "caller_id": "1234567890"
}

Like tools, hooks can use the **session directory (`./`)** to access or store per-call data.

Adding a Hook Script



1. Click **+ Add Hook Script**
2. Upload the script file
3. Enter a **Name** to identify the hook
4. Select one or more **Trigger Events**
5. Click **Save**

Trigger Events

Hooks can be configured to run on:

- **Session Start** – when the conversation begins
- **Session End** – when the caller hangs up
- **Session Redirect** – when the call is transferred to another destination

Multiple triggers can be selected for a single hook.

Key Notes

- Hooks run **automatically** based on selected trigger events
- No Prompt configuration is required for hooks

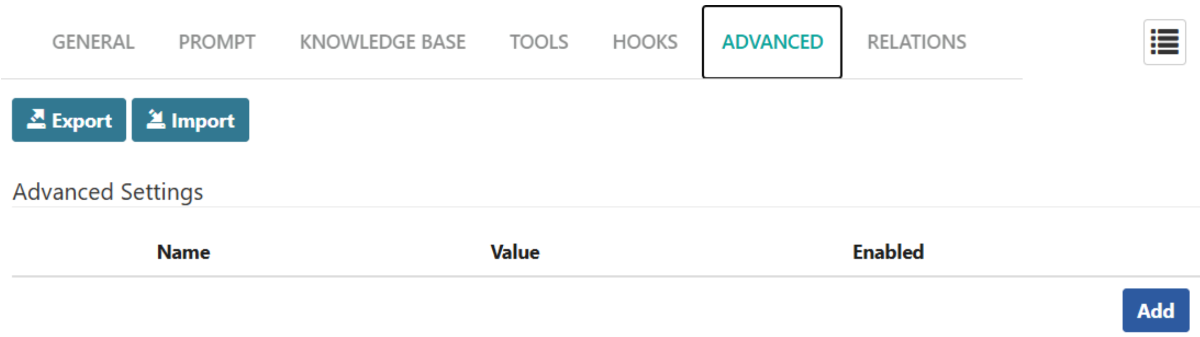
- Hooks must accept a **JSON input object**
- Hooks can access shared data stored by tools via the session directory
- Ideal for integrations, logging, analytics, and notifications

ADVANCED Tab

You can use this tab to modify advanced settings that are not available through the standard user interface. This section also allows you to configure advanced parameters for virtual agent, including:

- Model control values
- Voice options
- Speech activity parameters
- Reasoning configuration
- Additional experimental or advanced model parameters

For more information about advanced options for virtual agents, contact support@xorcom.com



Use the **Add** button at the bottom of the dialog to add additional sets of parameters. Existing sets can be removed by clicking on the appropriate trash icon.

Name: Specifies the name of the Agent Model Configuration (e.g., voice_name).

Value: Defines the content of the Agent Model Configuration parameter.

Enabled: Enables or disables the parameter without removing it from the configuration.

Importing and Exporting Parameters

The **Export** button allows you to save all advanced parameters to a JSON file. This can be useful for backups, transferring configurations between agents, or applying the same settings to multiple Virtual Agents.

The **Import** button allows you to load previously exported advanced parameters from a JSON file.

When importing a configuration:

- The file must be in the supported JSON format.
- The system validates the file immediately.
- If the file is invalid, an error is displayed before any overwrite confirmation is shown.
- If the file is valid, you are prompted before the existing advanced parameters are replaced.

Example Export File

```
{
  "version": 1,
  "agent_extension": "786",
  "agent_description": "Custom",
  "params": [
    {
      "name": "gemini_tts_style_prompt",
      "value": "Speak in spanish in a calm way",
      "enabled": "yes"
    }
  ]
}
```

The exported file contains:

- **version** Configuration file format version.
- **agent_extension** The extension associated with the Virtual Agent.
- **agent_description** The agent description.
- **params** A list of advanced parameters, including their names, values, and enabled status.

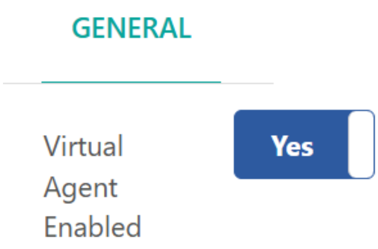
Note: The default configuration for all Virtual Agents using Gemini TTS has been updated to provide a calm, professional, and courteous speaking style out of the box. Adding a custom `gemini_tts_style_prompt` overrides the default behavior.

RELATIONS Tab

This tab provides a graphical display all the modules that are used by the Virtual Agent that you are currently viewing. This allows you to see at a glance all modules that are associated with the currently-selected Virtual Agent.

Virtual Agents Settings Dialog

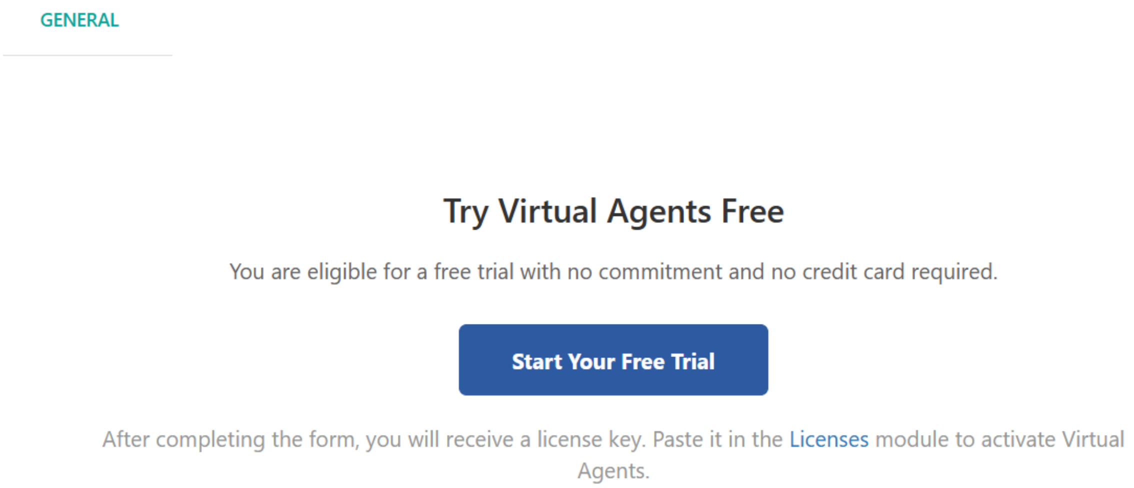
GENERAL Tab



Virtual Agent Enabled, allows you enable or disable the Virtual Agent Service.

Free Trial Activation (No License Scenario)

When the Virtual Agents module does **not have an active license**, the system will display a prompt inviting you to start a free trial.



When accessing the module without a license, click on **Start Your Free Trial**.

A registration form will be displayed requesting the following information:

- Company name
- First name
- Last name
- Contact email address

After completing the form, click **Submit**.

Once submitted:

- You will receive an email containing a **demo license key**.

- This license is required to activate and test the Virtual Agents module.

License Registration

To activate the module:

1. Return to the **Virtual Agents** module.
2. Click on **Licenses**.
3. Paste the license key received via email into the corresponding field.
4. Click **Register**.

Finalizing Activation

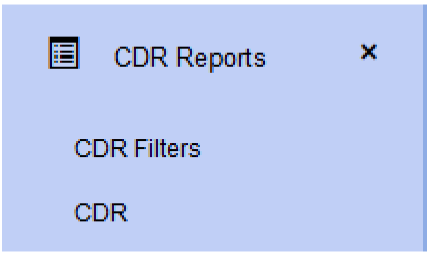
After registering the license:

- Navigate back to **PBX** → **Virtual Agents**, or
- Click the **refresh icon** (circular arrows) if the module is already open.

Once refreshed, the Virtual Agents module will be fully enabled and ready for configuration.

4. Reports Menu Set

CDR Reports Menu Group



CDR data is stored in the **cdr** table of the **asterisk** database. In addition to the standard CDR fields, CompletePBX 5 stores additional information in this table.

calltype, this field indicates the type of call:

- 1 indicates internal calls
- 2 indicates incoming calls
- 3 indicates outbound calls
- 4 indicates transit calls (trunk-to-trunk)

source, this is similar to the **src** field, but is left empty when the destination of the call cannot be determined.

destination, this is similar to the **dst** field, but is left empty when the destination of the call cannot be determined.

auth_code, this data is saved for calls where the Authorization Code feature code has been used for an outbound call. This function is activated by the default feature code, *79

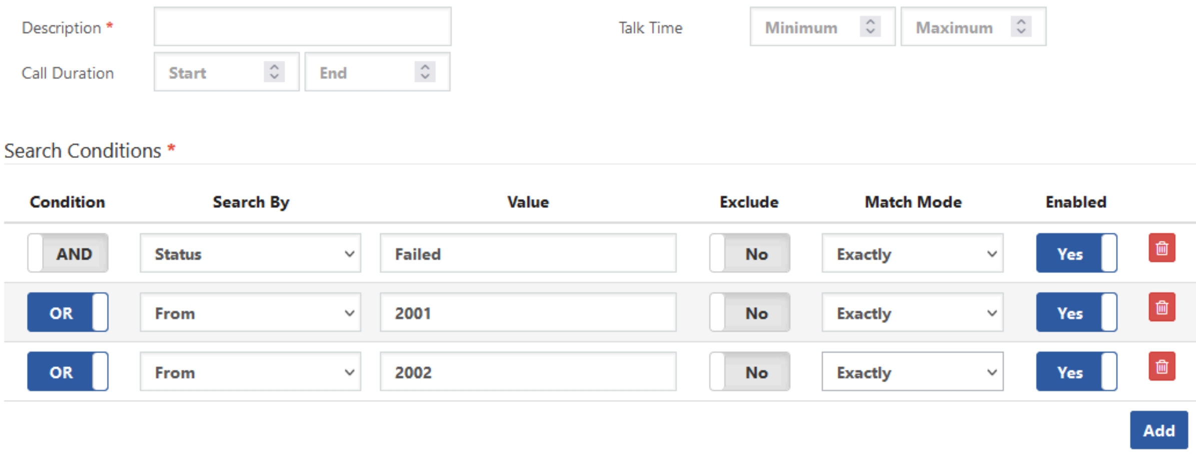
customer_code, this data is saved for calls where the Customer Code feature code has been used for an outbound call. This function is activated by the default feature code, *78

pin_code, this data is saved when a PIN code is used by a caller in order to access to an outbound route

Full details of all fields in the cdr table can be found in CDR table in Asterisk Database

CDR Filters Dialog

GENERAL Tab



Description*, free-text description for this filter.

Duration, duration of calls, consisting of **From** and **To** fields. Note that the clock for duration starts running after the caller has completed dialing the number.

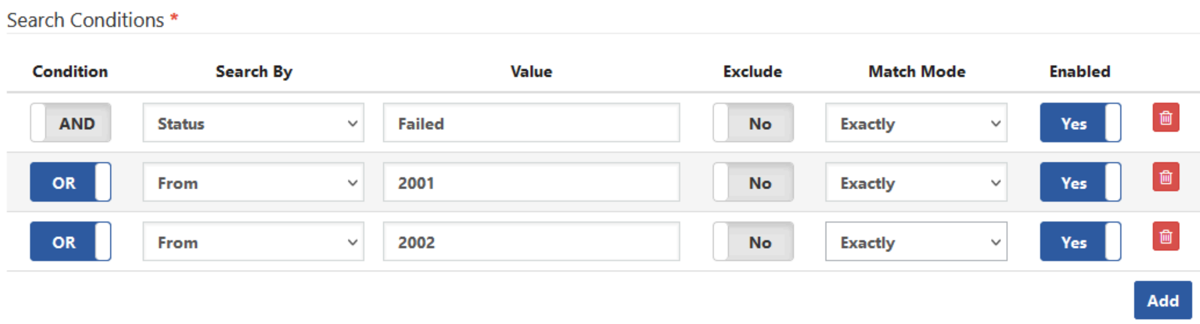
Talk Time, talk time of calls, consisting of **From** and **To** fields. Note that the clock for talk time is activated when the call is handled in some manner, such as answering the call by a person, an IVR, or voicemail.

Search Conditions Section

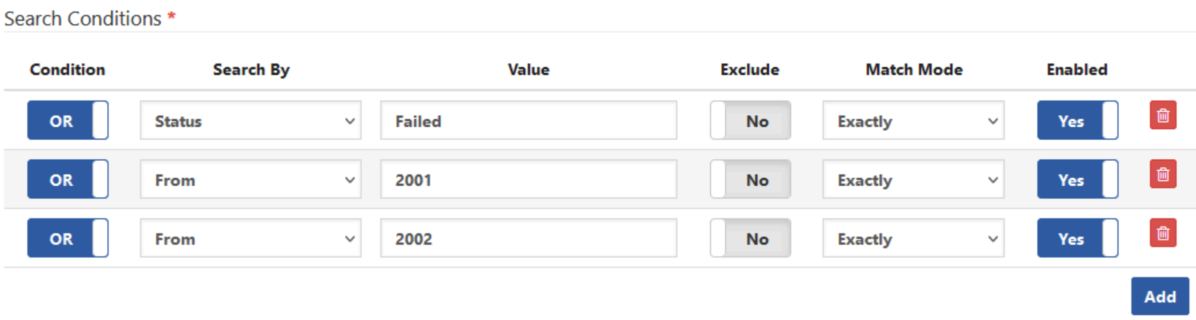
Pressing on the **Add** button allows you add additional search conditions.

Condition, determines whether the condition to be used should be **AND** or **OR**.

The following example collects calls that failed for either extension 2001 or 2002: failed calls for all other extensions will not be shown:



This example collects failed calls from ***any*** extension as well as ***all*** calls from either extension 2001 or extension 2002:



Search By, search for the selected field using one of the items selected from the drop-down list:

- Account Code - the account code, if defined in the Account Code field for the extension or for the outbound route, associated with the outgoing call.
- Caller ID - the Internal CID field in the Extensions dialog for internal calls, the External CID field for outbound calls, or the CID field provided for inbound calls. Could contain something like "Main Switchboard" <2940> for calls originating from the PBX, or <0544646377> for calls originating from an external source.
- Call Type - **1** indicates internal calls, **2** indicates incoming calls, **3** indicates outbound calls, and **4** indicates transit calls (trunk-to-trunk)
- Customer Code - value that was set when making a call using the Customer Code Feature code (typically *78)
- From - similar to the **From (src)** field described below, but is left empty when the destination of the call cannot be determined
- From (src) - the Caller ID of the person who initiated the call
- PIN - The ***description*** of the PIN code that was used for an outbound call, when an Outbound Route requires a PIN code
- Status – indicates the disposition of the call - valid values are No answer, Failed, Busy, Answered, or Unknown
- To - similar to the **To (dst)** field described below, but is left empty when the destination of the call cannot be determined
- To (dst) - the destination that was called – can be either an internal extension or an external number

Full details of all fields in the cdr table can be found in [CDR table in Asterisk Database]

Value, value of the selected field.

Exclude, excludes the selected value in the search when **Yes** is selected.

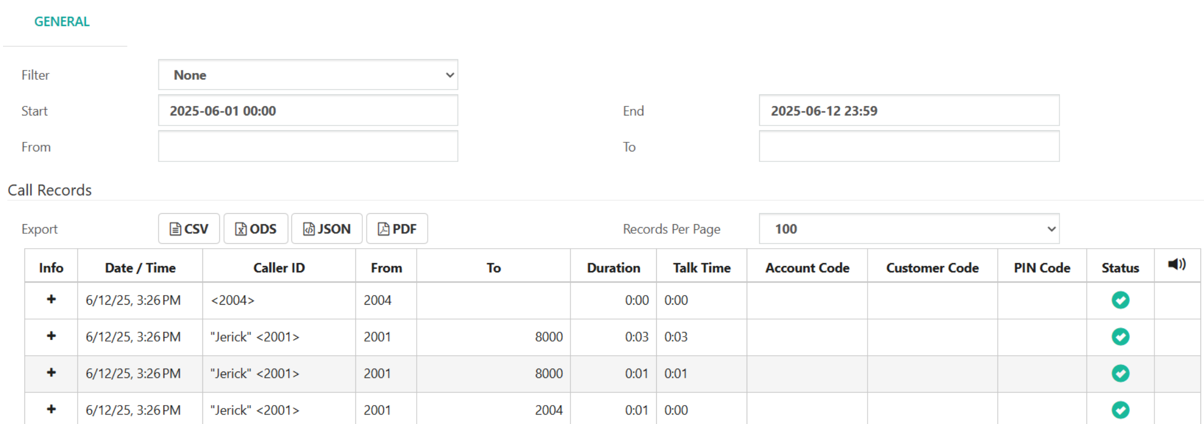
Mode, search condition can be matched by a number of different methods**,** which can be selected from the drop-down list:

- Begins with
- Contains
- Ends with
- Exactly

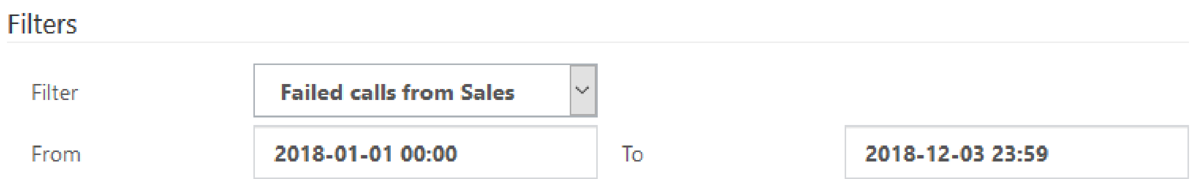
Enabled, enable/disable the condition.

CDR Dialog

GENERAL Tab



General Section



Filter, name of a previously-defined filter (defined in CDR Filters dialog) to use in this report.

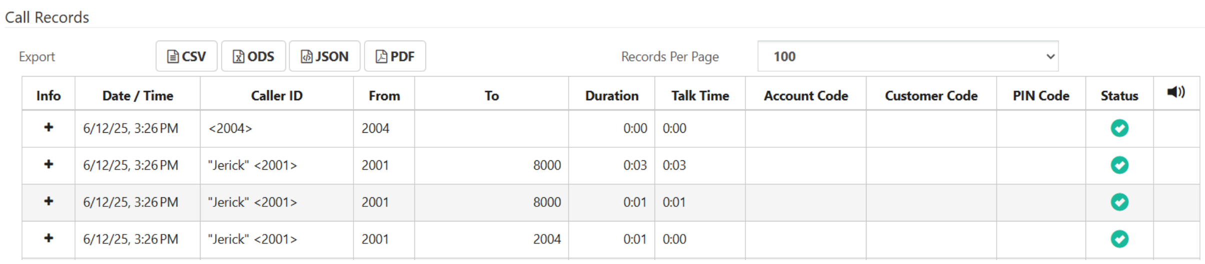
Start, include records starting from, and after, this timestamp.

From, source of call, consisting of either caller ID, or caller name. Note that this field uses **contains** when matching records. This field is not displayed when using a filter.

End, include records ending up to, and including, this timestamp.

To, destination of calls, consisting of either caller ID or name. Note that this field uses **contains** when matching records. This field is not displayed when using a filter.

Call Records Section



Call Records

Export CSV ODS JSON PDF

Records Per Page 100

Info	Date / Time	Caller ID	From	To	Duration	Talk Time	Account Code	Customer Code	PIN Code	Status	
+	6/12/25, 3:26 PM	<2004>	2004		0:00	0:00				✔	
+	6/12/25, 3:26 PM	"Jerick" <2001>	2001	8000	0:03	0:03				✔	
+	6/12/25, 3:26 PM	"Jerick" <2001>	2001	8000	0:01	0:01				✔	
+	6/12/25, 3:26 PM	"Jerick" <2001>	2001	2004	0:01	0:00				✔	

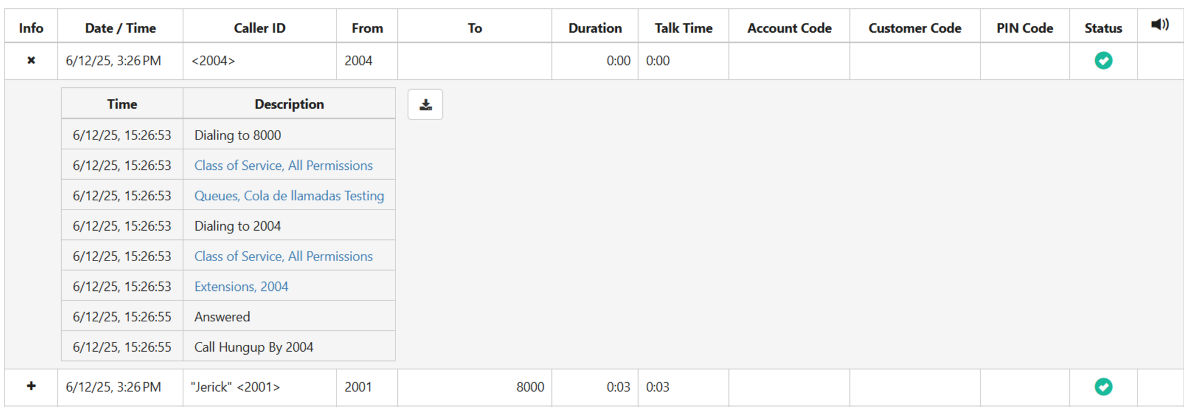
Export, click any icon to export the currently-displayed CDR report in the appropriate format. Available formats are:

- CSV
- ODS
- JSON
- PDF

Records Per Page, set the number of records that should be displayed on each page.

The following fields are shown:

- **Info:** allows viewing the detailed steps of a specific call. Click the '+' icon to expand and see the full call flow from origin to termination, including the services and destinations involved and which party ended the call including blacklisted calls, calls forwarded to external numbers, calls routed to voicemail, and call termination reasons (Hang-up Cause). The download icon in this column allows downloading the associated CEL (Call Event Logging) records.

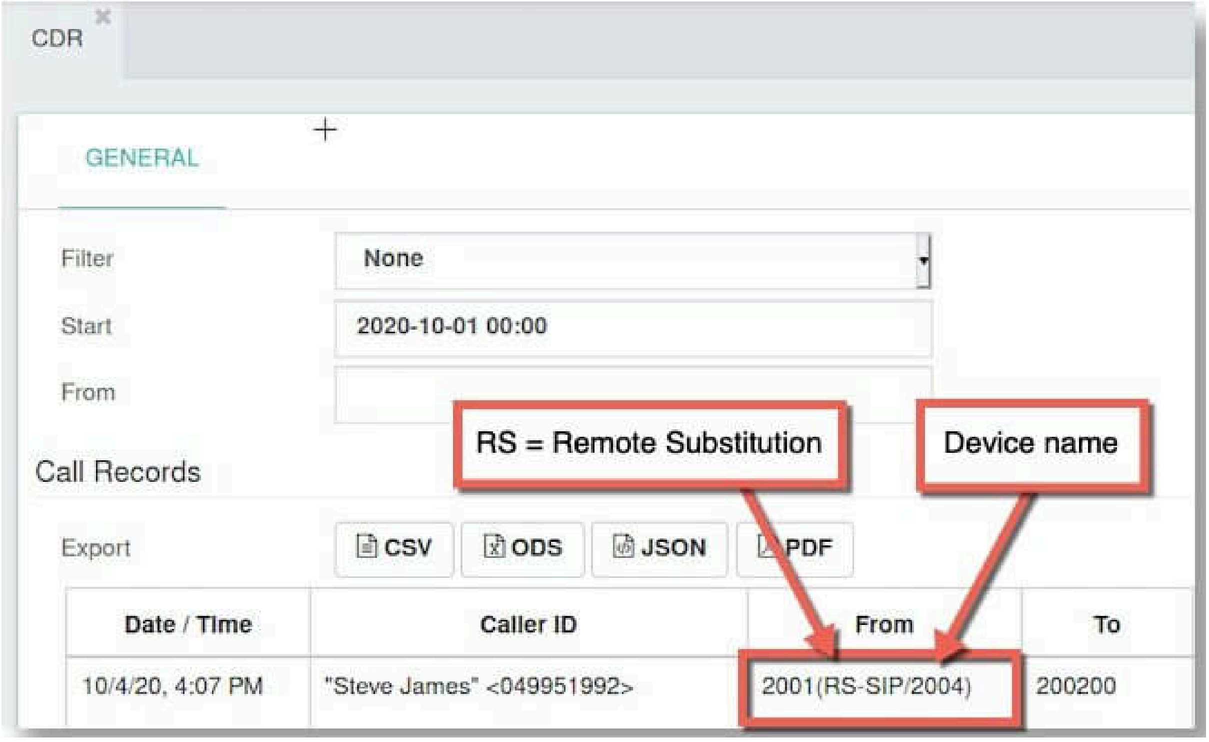


Info	Date / Time	Caller ID	From	To	Duration	Talk Time	Account Code	Customer Code	PIN Code	Status	
×	6/12/25, 3:26 PM	<2004>	2004		0:00	0:00				✔	
+	6/12/25, 3:26 PM	"Jerick" <2001>	2001	8000	0:03	0:03				✔	

Time	Description
6/12/25, 15:26:53	Dialing to 8000
6/12/25, 15:26:53	Class of Service, All Permissions
6/12/25, 15:26:53	Queues, Cola de llamadas Testing
6/12/25, 15:26:53	Dialing to 2004
6/12/25, 15:26:53	Class of Service, All Permissions
6/12/25, 15:26:53	Extensions, 2004
6/12/25, 15:26:55	Answered
6/12/25, 15:26:55	Call Hungup By 2004

- **Date/Time:** timestamp indicating when the call was initiated, for example **2017-09-19 20:56:24**, depending on the default setting configured for your time zone.
- **Caller ID:** the Internal CID field in the Extensions dialog for internal calls, the External CID field for outbound calls, or the CID field provided by the phone company for inbound calls. Could contain something like "**Main Switchboard" <2940>** for calls originating from the PBX, or **<0544646377>** for calls originating from an external source.
- **From:** caller ID of the calling party, as used by the system when making the call. The internal extension will be shown for outbound calls, while the external CID will be displayed for

inbound calls. Remote substitution calls appear with both the extension and device name in the CDR, and are designated as RS, as in the following example:



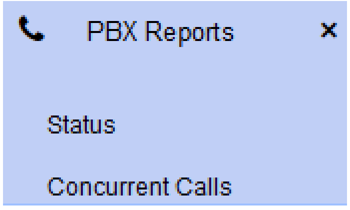
- **To:** caller ID of the calling party, as used by the system when making the call. The internal extension will be shown for outbound calls, and the external CID will be displayed for inbound calls.
- **Duration:** duration of the call, based on the number of seconds between when the call was initiated, and when it ended
- **Talk Time:** duration of the call, based on the number of seconds between when the call was answered, and when it ended.
- **Account Code:** account code, if defined in the Account Code field for the extension or for the outbound route, associated with the outgoing call.
- **Customer Code:** code used for calls where the Customer Code feature code has been used for an outbound call. By default, this is activated by feature code *78
- **PIN Code:** the ***description*** of the PIN code that was used for an outbound call, when an Outbound Route requires a PIN code
- **Status:** indicates what happened to the call. Valid disposition values are NO ANSWER, FAILED, BUSY, ANSWERED, CONGESTED, or UNKNOWN

Full details of all fields in the cdr table can be found in the CDR table in Asterisk Database

Do not forget to press the **Search** button to activate the data collection.

When a Hot Desk devices logs in or out of the system, an entry will be created in the CDR Report, indicating the activity.

PBX Reports Menu Group



Status Dialog

Use this dialog to see the status of active calls in the system

Channels Tab

Displays a detailed list of calls in progress, together with a summary of active calls and active channels.

You can click on the **Refresh** button to update the displayed data with current real-time data.

Channel	Caller ID	Called Number	State	Duration
SIP/3989-00000504	"Ariel" <2989>	2970	Up	00:00:32
SIP/2970-00000505	"Eran" <2970>		Up	00:00:31
SIP/2941-00000506	"Keith" <2941>	s	Up	00:00:02

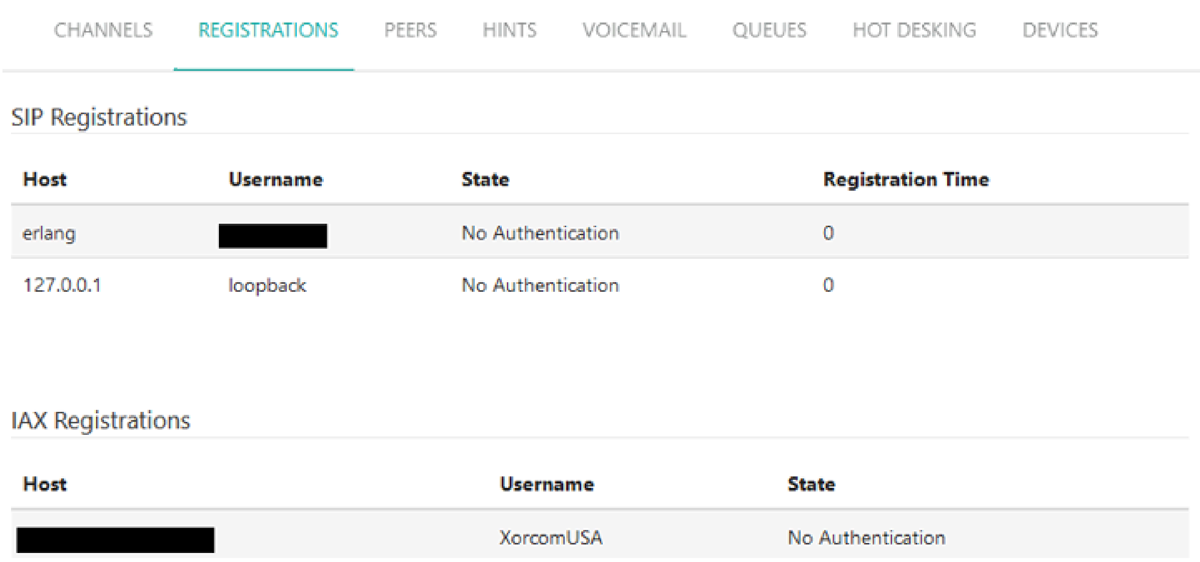
Summary

Active Calls	Active Channels
1	3

Registrations Tab

Displays a detailed list of both SIP and IAX trunk registrations.

You can click on the **Refresh** button to update the displayed data with current real-time data.



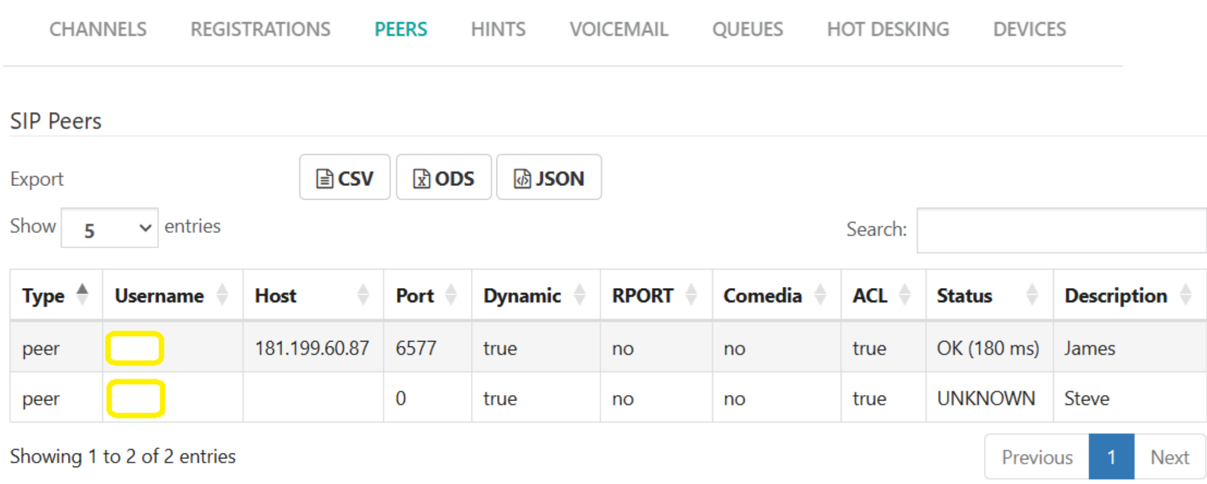
Host	Username	State	Registration Time
erlang	[redacted]	No Authentication	0
127.0.0.1	loopback	No Authentication	0

Host	Username	State
[redacted]	XorcomUSA	No Authentication

Peers Tab

Displays a detailed list of SIP and IAX2 peers.

You can click on the **Refresh** button to update the displayed data with current real-time data.



Type	Username	Host	Port	Dynamic	RPORT	Comedia	ACL	Status	Description
peer		181.199.60.87	6577	true	no	no	true	OK (180 ms)	James
peer			0	true	no	no	true	UNKNOWN	Steve

Export, click on any icon to export a list of SIP peers' statuses in the selected format. Available formats include:

- CSV
- ODS
- JSON

Hints Tab

Displays a detailed list of hints active in the system.

You can click on the **Refresh** button to update the displayed data with current real-time data.

CHANNELS REGISTRATIONS PEERS HINTS VOICEMAIL QUEUES HOT DESKING DEVICES

Extension	Context	Hint	Status
2238	extension-hints	SIP/SIP285&Custom:DND_2238	Unavailable
2239	extension-hints	SIP/SIP286&Custom:DND_2239	Unavailable
PEA_260	extension-hints	Custom:PEA_260	Idle
9400	conference-hints	confbridge:9400	Unavailable
QAL_2125	queue-hints	Custom:QAL_2125	Idle
DND_278	extension-hints	Custom:DND_278	Idle
100	extension-hints	SIP/100&Custom:DND_100	Idle
BOSS_201	extension-hints	Custom:BOSS_201	Idle

Voicemail Tab

Displays a detailed list of voicemail mailboxes in the system, and their current status.

You can click on the **Refresh** button to update the displayed data with current real-time data.

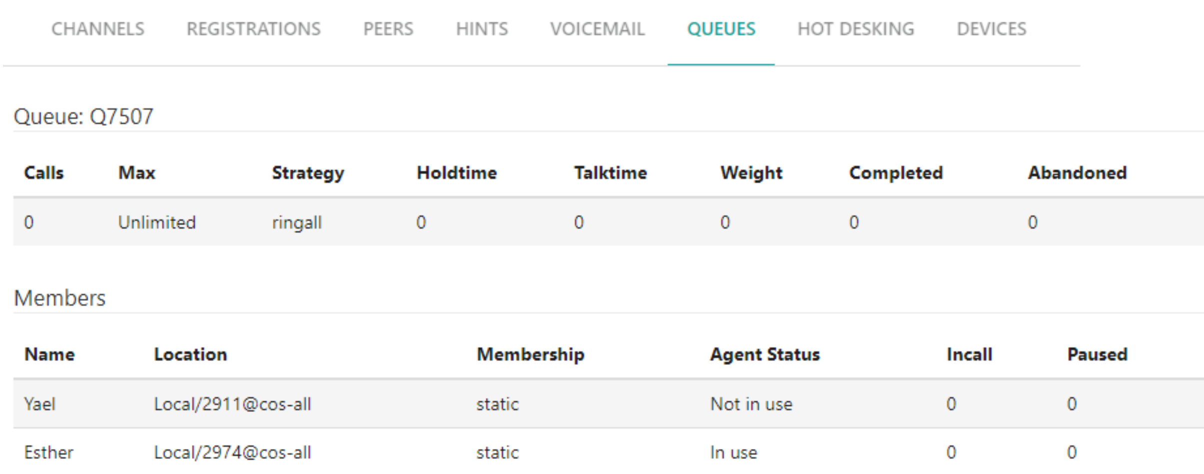
CHANNELS REGISTRATIONS PEERS HINTS VOICEMAIL QUEUES HOT DESKING DEVICES

Mailbox	User	New Messages
2909	Production	0
2911	Yael	0
2923	Kitchen	0
2940	Meeting-Room	2
2941	Keith	0

Queues Tab

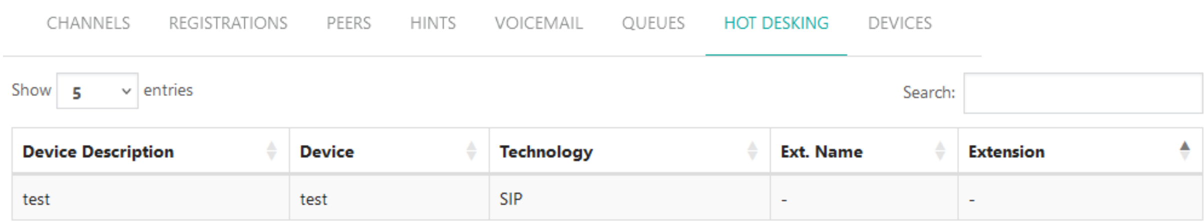
Displays a list of calls to available queues in the system, as well as agents of the queues.

You can click on the **Refresh** button to update the displayed data with current real-time data.



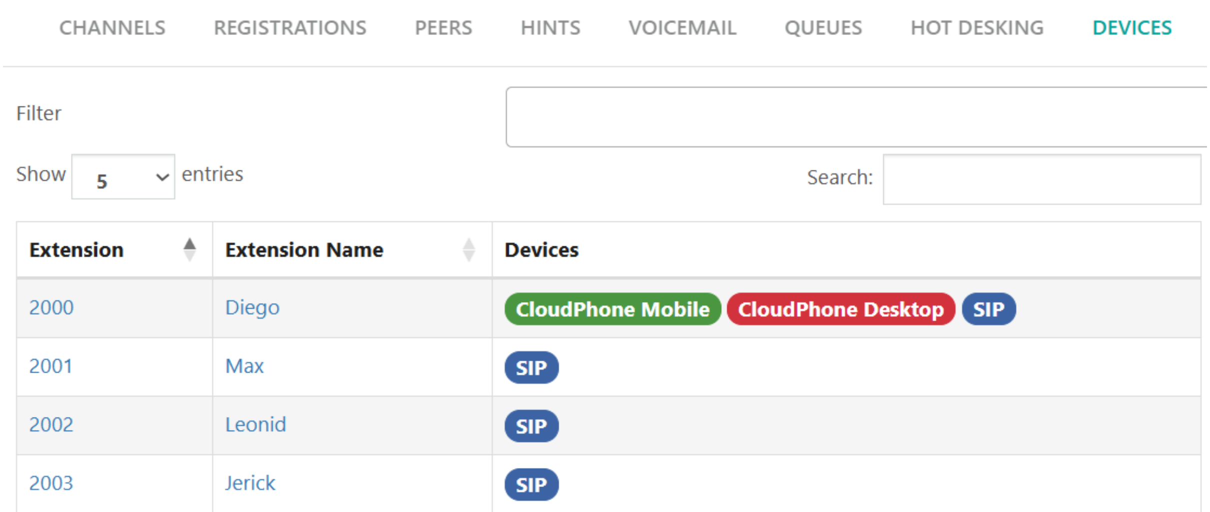
Hot Desking Tab

Displays a report of the device (phone) assignment, including Device, Description, Device, Technology, Extension Name, and Extension.



Devices Tab

Displays the types, number and name of devices linked to each extension. On mouse-over, the device name is shown.

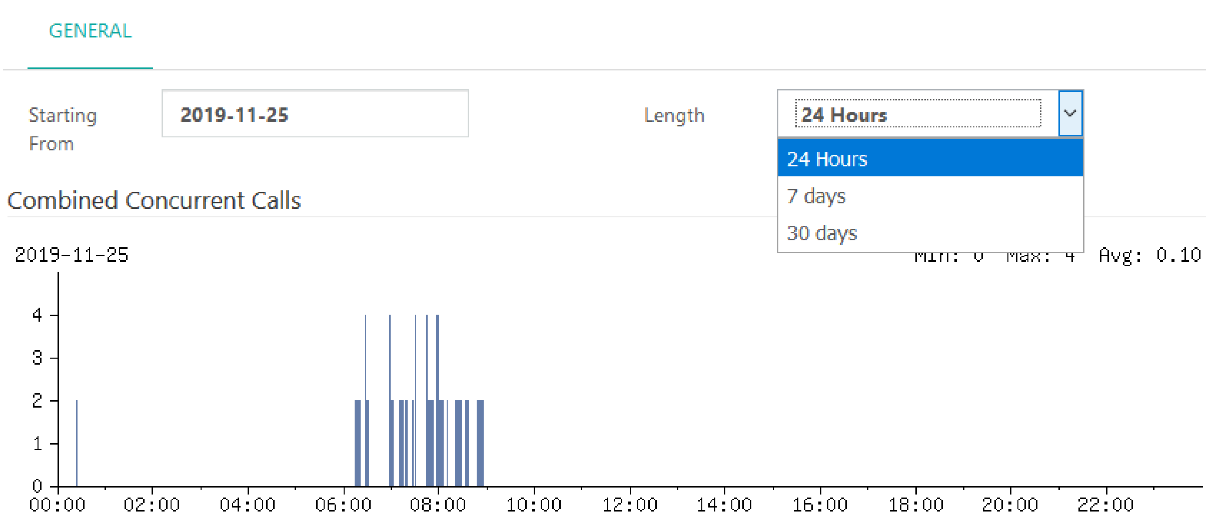


Concurrent Calls Dialog

Creates graphs, based on historical data that is stored in the CDR database, of concurrent calls on all outbound trunks. Data for trunks only includes incoming and outgoing external calls.

The Combined Current Calls graph also includes data for local (internal) calls. Note that if a call is routed to a Ring Group with 5 members, this will be considered as 5 calls when creating the Combined Current Calls graph.

General Tab



Starting From, allows you to configure the starting point for the report. A new report will be automatically generated whenever you change the value of this field.

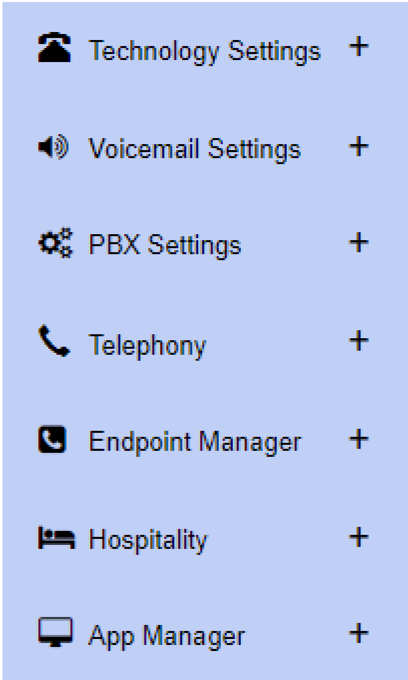
Length, allows you to choose from a dropdown list, the period to be covered by the report. A new report will be automatically generated whenever you change the value of this field.

Available options are:

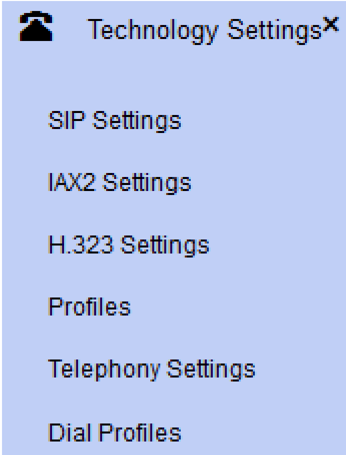
- 24 hours
- 7 days
- 30 days

Note that time slices where no channels are in use are disregarded when calculating the average channel usage,

5. Settings Menu Set



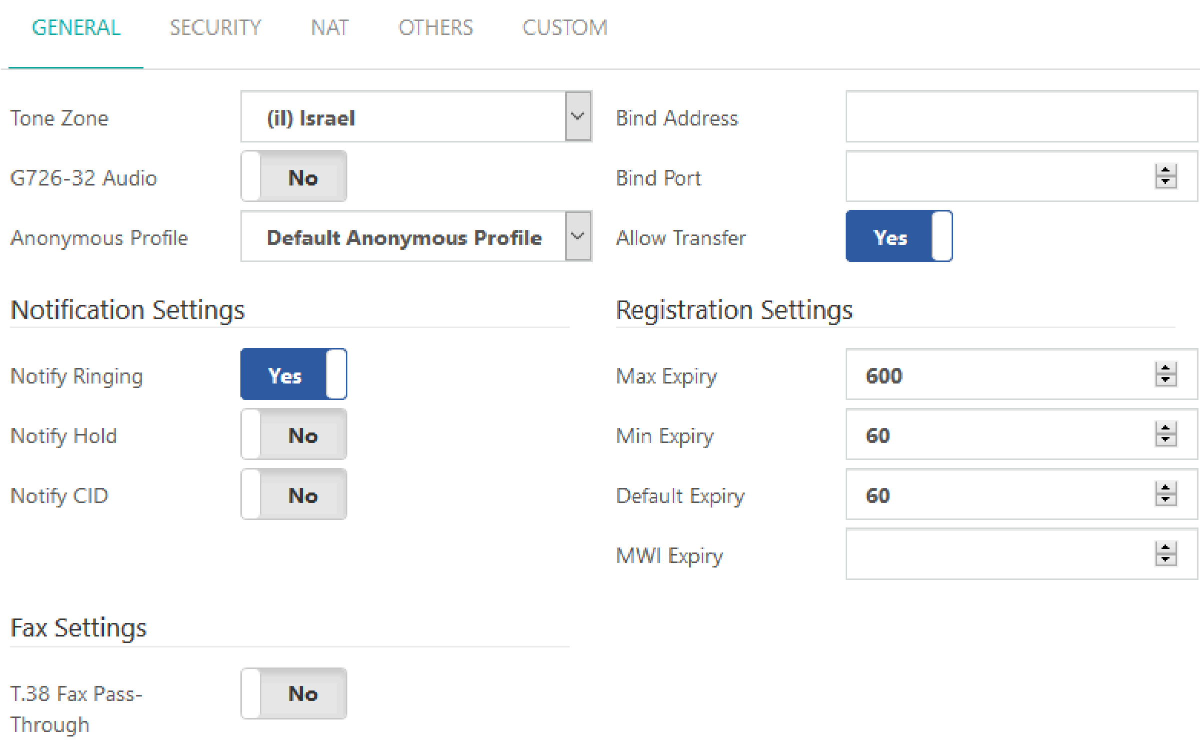
Technology Settings Menu Group



SIP Settings Dialog

SIP Settings is used to configure the default values to be used for all SIP calls.

GENERAL Tab



Tone Zone, default tone zone for all users/peers.

G726-32 Audio, use AAL2 packing order in place of RFC3551 if peer negotiates G726-32 audio. This is required for Sipura and Grandstream ATA devices.

Bind Address, IP address to which the device should bind. Note that 0.0.0.0 binds to all IPv4 addresses, or :: for all IPv6 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.

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).

Registration Settings Section

Max Expiry, maximum allowed time, in seconds, for incoming registrations.

Min Expiry, minimum time, in seconds, for registrations.

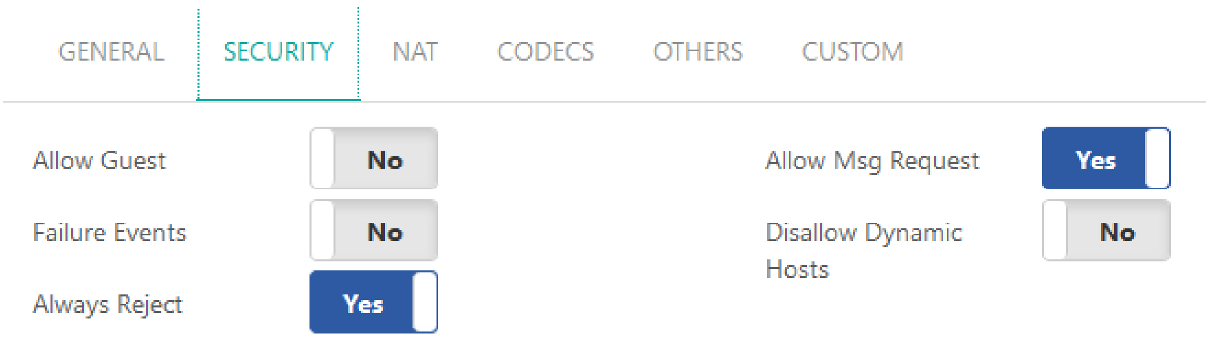
Default Expiry, default length of incoming/outgoing registration.

MWI Expiry, expiry time for outgoing MWI subscriptions.

Fax Settings Section

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 Tab



Allow Guest, allow or reject guest calls.

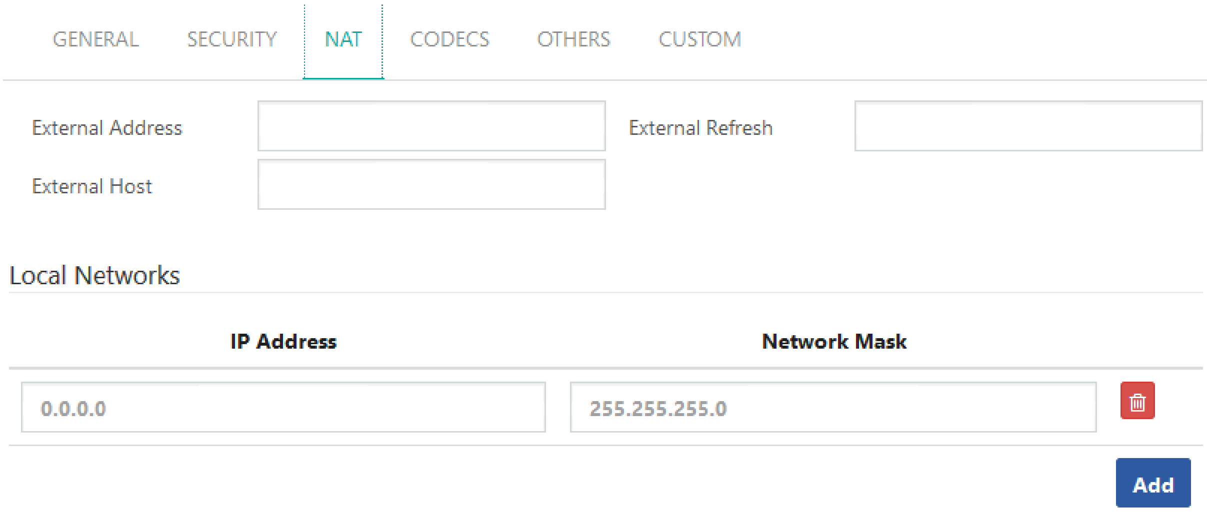
Failure Events, generate manager peer-status events when peer cannot authenticate with Asterisk. Peer-status will be rejected.

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.

NAT Tab



External Address, specifies a static address, or address[:port] combination, to be used in SIP and SDP messages. For some devices, you may need to specify the external port in addition to the IP address.

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.

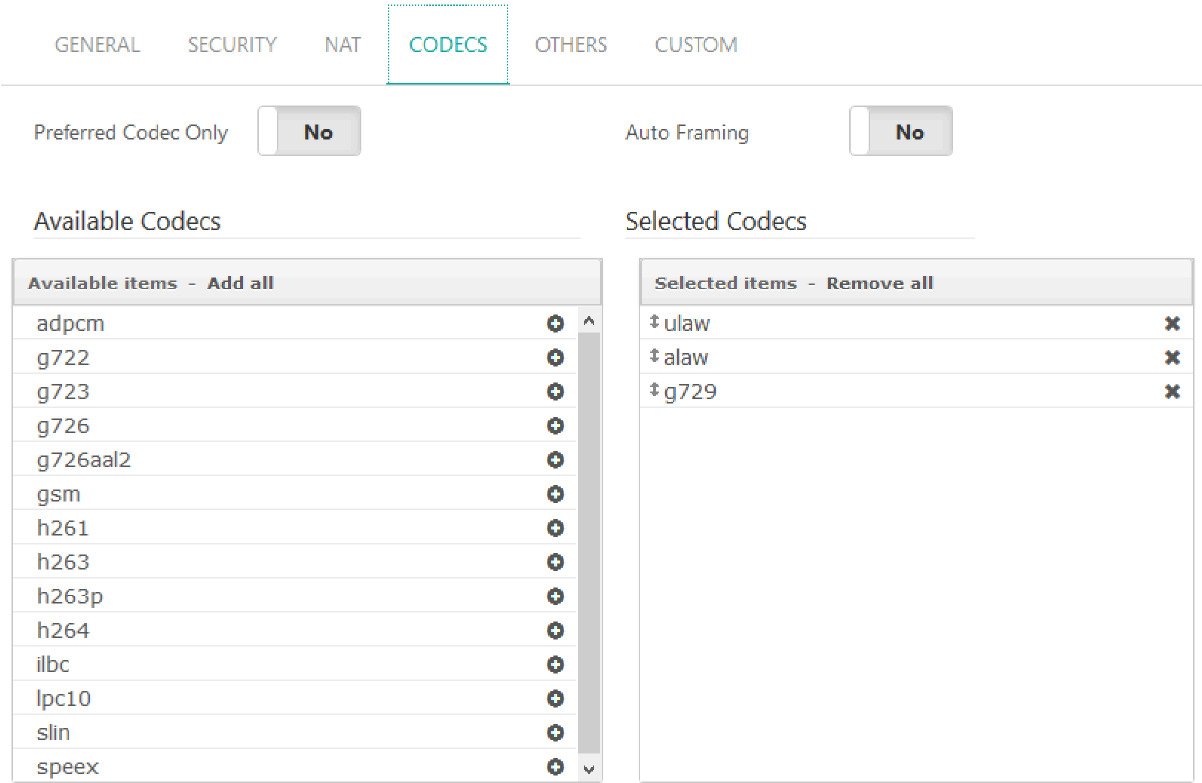
Local Networks Section

This information is used to determine whether a call is internal, so NAT does not need to be used. This requires you to define the IP address and network mark of the CompletePBX server.

IP Address, IP address of the CompletePBX server.

Network Mask, network mask to use.

CODECS Tab



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 you prefer.

Auto Framing, set packetization based on the remote endpoint's (ptime) preferences.

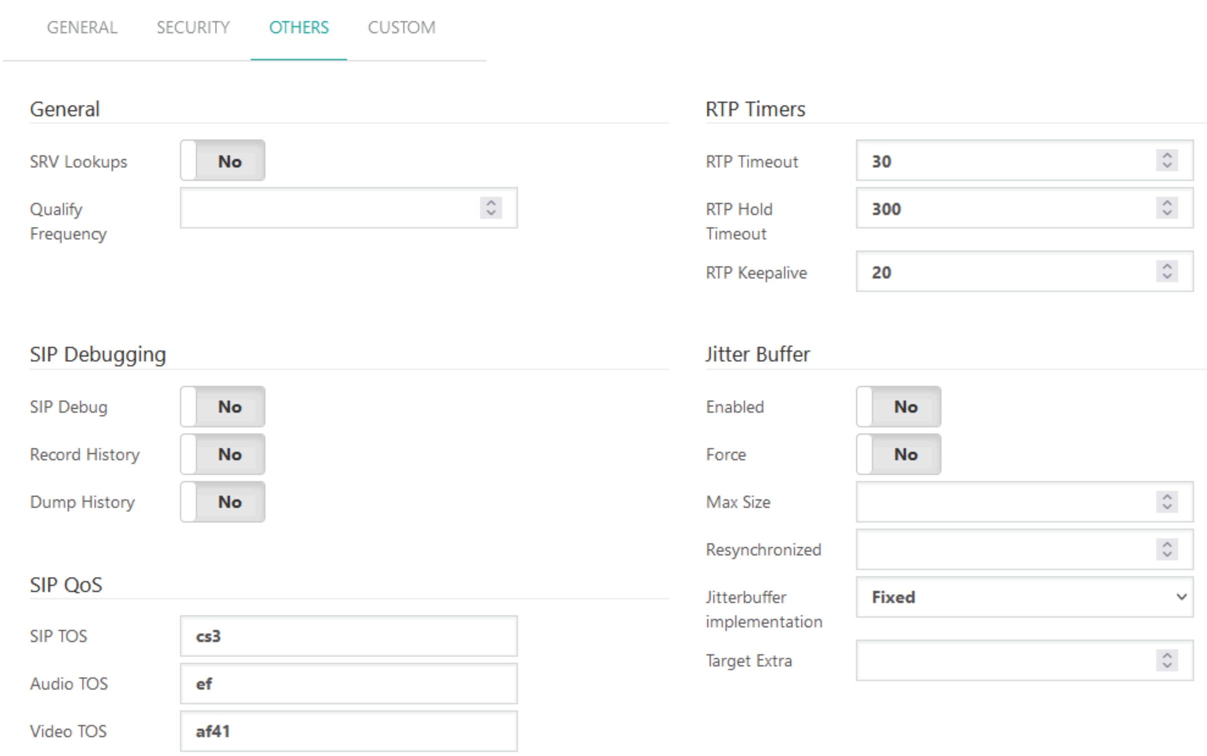
Available Codecs/Selected Codecs Section

Press on + or – minus icons to move available codecs to list of selected codecs. Press on the x icon to remove codecs from the list of selected codecs. You can also select or remove all codecs by pressing on either the Add All or Remove All buttons.

Available Codecs, list of available codecs.

Selected Codecs, list of selected codecs.

OTHERS Tab



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 the sip show settings command.

RPT Timers Section

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

RTP Timeout, sets the time, in seconds, to terminate the call if there is no RTP or RTCP activity on the audio channel.

RTP Hold Timeout, sets the time, in seconds, to terminate the call if there is no RTP or RTCP activity on the audio channel.

RTP Keepalive, send keepalives in the RTP stream to keep NAT open.

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, 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.

Implementation, 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, sets the time, in milliseconds, the new jitter buffer will pad its size. This option only affects the jb when 'jbimpl = adaptive' is set.

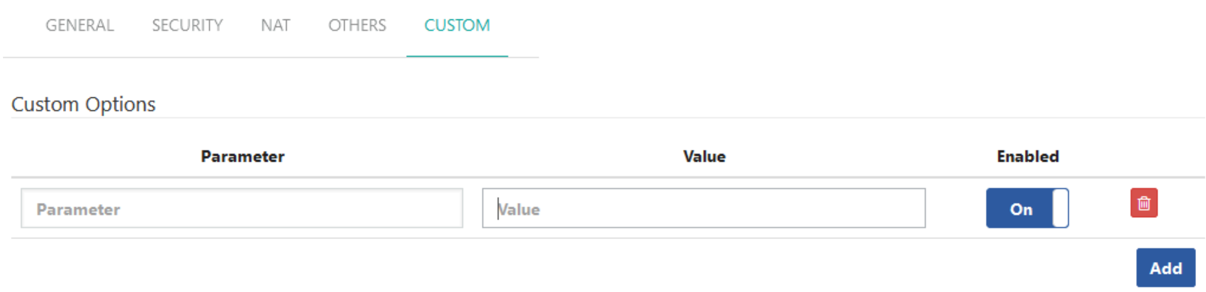
SIP QoS Section

SIP TOS, sets the TOS (type of service) for SIP packets

Audio TOS, sets the TOS (type of service) for RTP audio packets

Video TOS, set the TOS (type of service) for RTP video packets

CUSTOM Tab



Custom Options Section

Parameter, The SIP parameter to be included in the [general] section.

Value, value of the SIP parameter to be used.

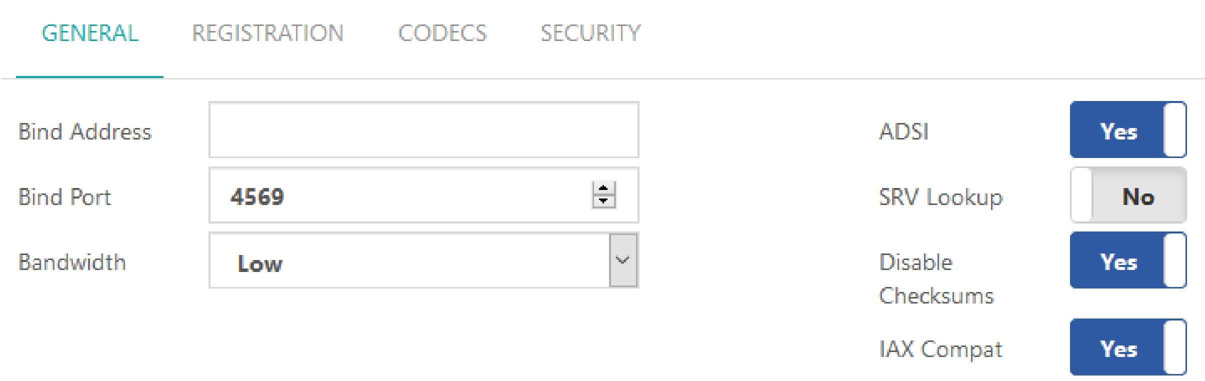
Enabled, enable/disable the custom option.

IAX2 Settings Dialog

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

The IAX2 Settings is used to configure the default values to be used for all IAX2 calls.

GENERAL Tab



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 4569.

Bandwidth, specify bandwidth (low**,** medium**,** or high) to control which codecs should be used.

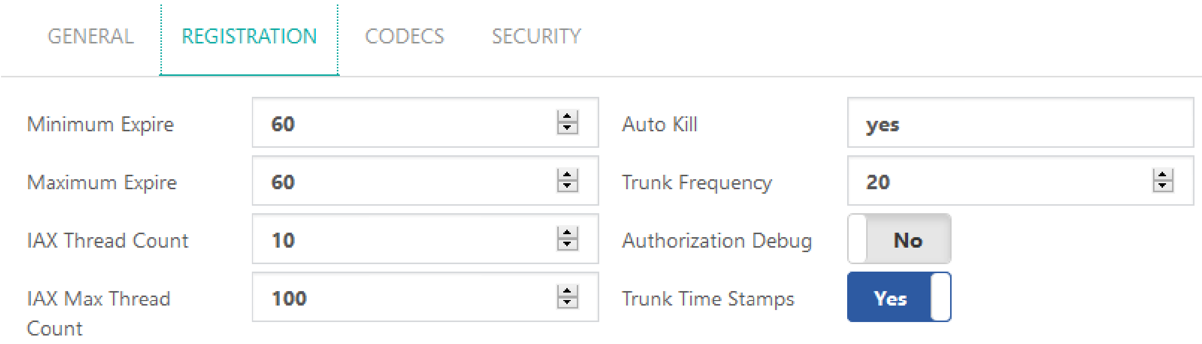
ADSI, Analog Display Services Interface (ADSI) can be enabled if you have ADSI-compatible CPE equipment.

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 Compat, 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 Tab



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.

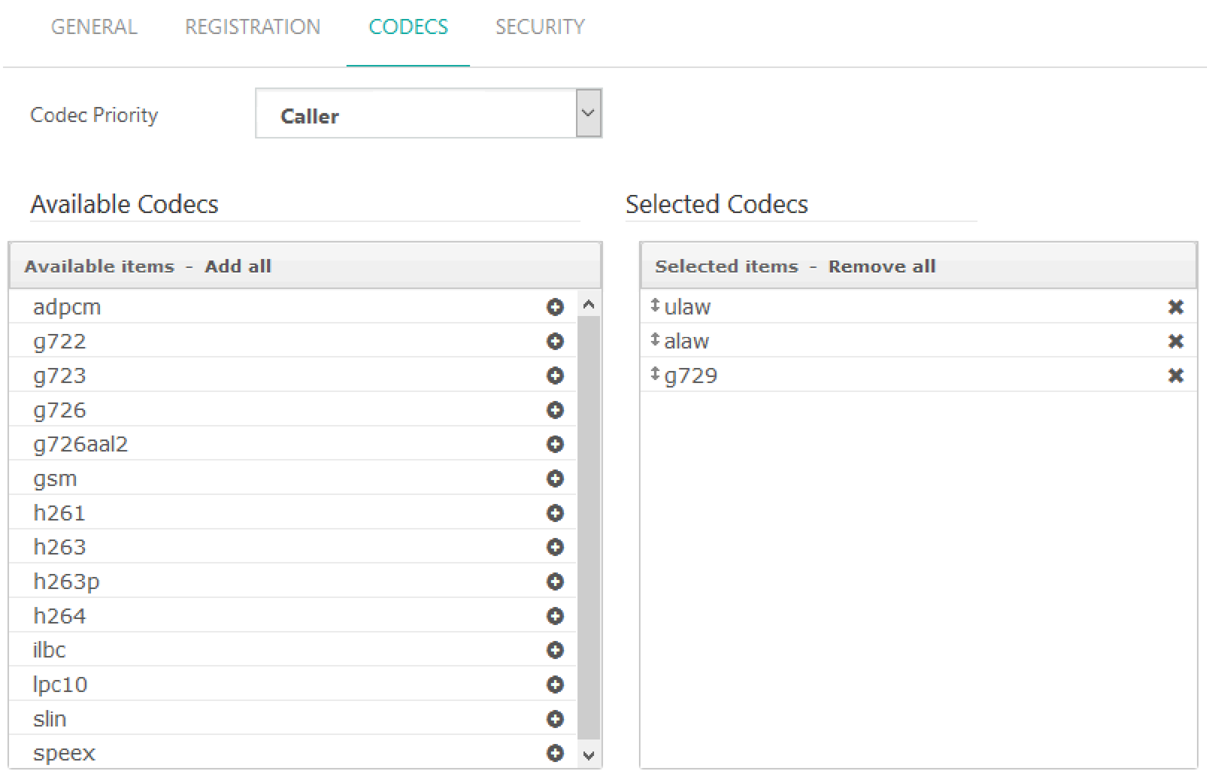
Auto Kill, this is used to keep the system from stalling when a host is not available. In addition to 'yes' or 'no' you can also specify a number of milliseconds.

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, 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 Tab



Codec Priority, 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 to the **Disabled** option, but the call will only be accepted if the requested format is available.

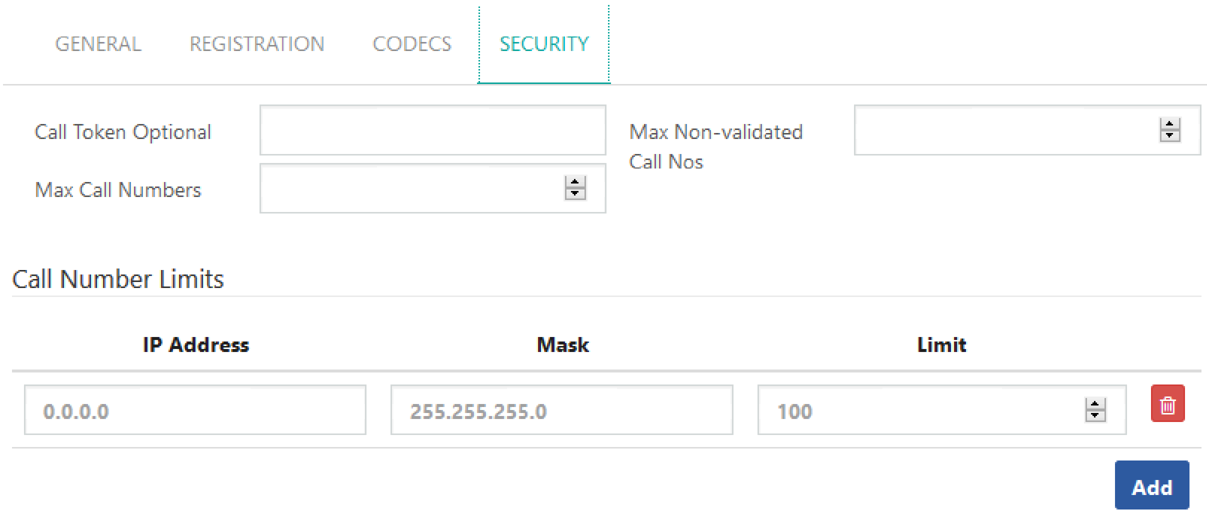
Available Codecs/Selected Codecs Section

Press on + or – minus icons to move available codecs to list of selected codecs. Press on the x icon to remove codecs from the list of selected codecs. You can also select or remove all codecs by pressing on either the Add All or Remove All buttons.

Available Codecs, list of available codecs.

Selected Codecs, list of selected codecs.

SECURITY Tab



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 the registration.

Max Non-validated Call Nos, this 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.

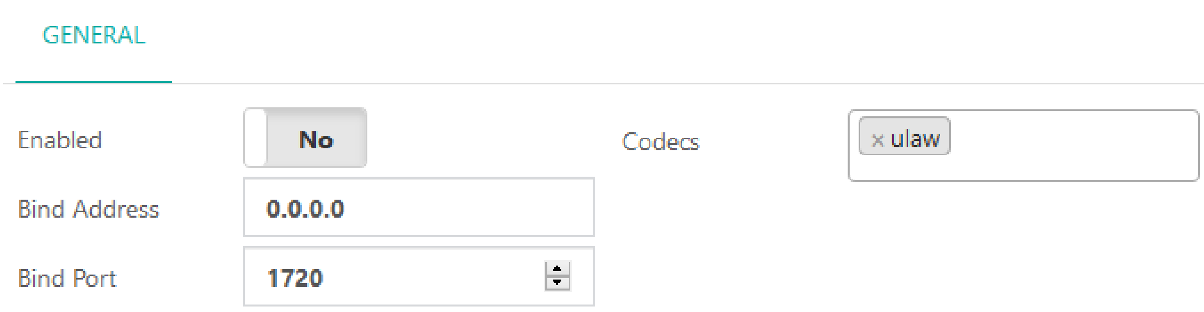
Call Number Limits Section

- **IP Address,** valid IP address to be used.
- **Mask,** network mask to use.
- **Limit,** 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.

H 323 Dialog

Allows user to manage the H.323 configuration for the system.

H.323 is a network protocol that is used for audio-visual communications. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences.



Enabled, allows you to control whether H.323 is enabled in the system.

Bind Address, allows you configure the bind address if H.323 is enabled. All addresses are bound if the address is set to 0.0.0.0

Bind Port, the port to which H.323 is bound. The default value is 1720.

Codecs, allows you to choose one (or more) codecs from the list of allowed codecs. The order in which the codecs are listed determines the order of preference for the codecs. If at least one codec is selected, the **disallow=all** parameter will also be generated.

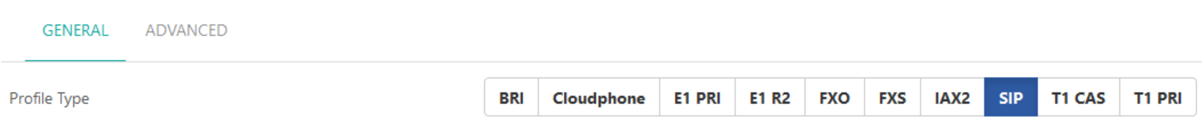
Profiles Dialog

Profiles are sets of characteristics that are generally repeated when creating extensions and / or devices. Instead of configuring (and maintaining) this data throughout the dial-plan, we create device-specific profiles that group this data.

GENERAL Tab

There are many profile type options:

- BRI
- CloudPhone
- E1 PRI
- E1 R2
- FXO
- FXS
- IAX2
- SIP
- T1 CAS
- T1 PRI
- Teams Connector
- CloudPhone



Profile Type, select the type of profile from the displayed list:

- BRI
- E1 PRI
- E1 R2
- FXO
- FXS
- IAX2
- SIP
- T1 CAS
- T1 PRI
- Teams Connector

Name*, free-text name for the profile.

Description, free-text description to identify the profile.

Provisioning Section

External Hostname, or IP address of the PBX, optionally including the port number.

Outbound Proxy, that the CloudPhone application should use, optionally including the port number.

Auto Answer, when enabled, the device will automatically answer incoming calls.

Auto Answer Delay, when enabled, this value represents the number of seconds to wait before incoming calls are answered automatically.

For Teams Connector, the available options are:

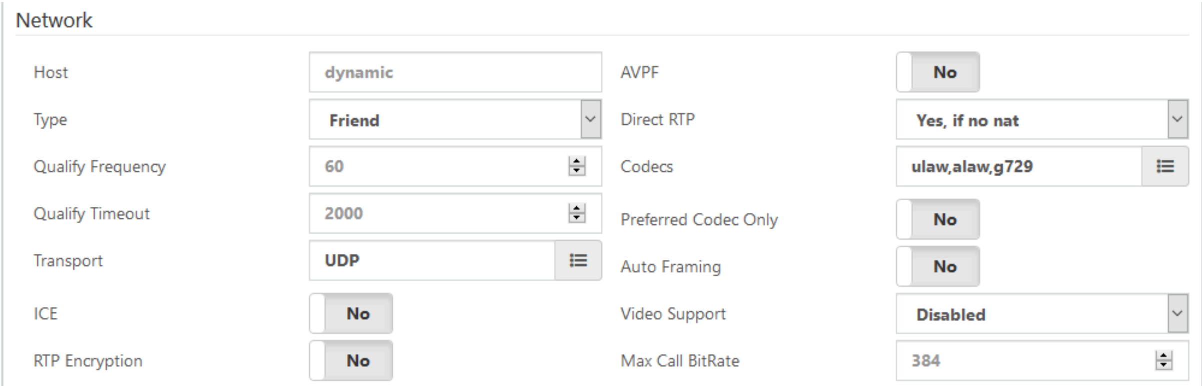
External Hostname*, or IP address of the PBX, optionally including the port number.

Outbound Proxy, that the CloudPhone application should use, optionally including the port number.

Country*, for this profile.

Outside Line Prefix, If your PBX requires dialing a digit for external calls/outside line.

Network Section



Host, the host parameter specifies the hostname or IP address of a SIP peer or user. It is used to make both outbound calls and to find the peer when an inbound call is received. Host can take the following formats:

- Domain Name / Hostname e.g. sip.zxv.com
- IP Address e.g. 234.23.42.103
- Dynamic**,** which means the phones must register.

Type, determines their roles within Asterisk. The type options are:

- Peer : handle both inbound and outbound calls and are matched by IP/port. When there are incoming calls from the peer**,** the IP address must match in order for the invitation to be accepted.
- User : handle inbound calls only**,** which means that that they can call CompletePBX**,** but CompletePBX cannot call them. The callers must be authenticated by their authorization information (username and secret).
- Friend : CompletePBX will create the entity as both a user and a peer. CompletePBX will accept calls from friends just as it would for users**,** requiring only that the authorization matches**,** rather than the IP address.

Qualify Frequency, how often (in seconds) to check for the host to be up.

Qualify Timeout, setting to yes (equivalent to 2000 milliseconds) will send an OPTIONS packet to the endpoint periodically (default every minute). Used to monitor the health of the endpoint. If delays are longer then the qualify time**,** the endpoint will be taken offline and considered unreachable. Can be set to a value which will be the threshold, in milliseconds. Setting this value to **No** will turn this off. Can also be helpful to keep NAT pinholes open.

Transport, set the default transports. The order determines the primary default transport.

ICE, whether to Enable ICE Support. Defaults to no. ICE (Interactive Connectivity Establishment) is a protocol for Network Address Translator (NAT) traversal for UDP-based multimedia sessions established with the offer/answer model. This option is commonly enabled in WebRTC setups.

RTP Encryption, whether to offer SRTP encrypted media (and only SRTP encrypted media) on outgoing calls to a peer.

AVPF, enable inter-operability with media streams using the AVPF RTP profile.

Direct RTP, enables direct sending of RTP between call participants. Available options are:

- Yes
- No
- Yes, if no NAT
- Use UPDATE

Codecs, list of allowed codecs. The order in which the codecs appears will determine the order of preference. If at least one codec is selected, the **disallow-all** parameter will be automatically generated.

Preferred Codec Only, respond to SIP invites with only the preferred codec, rather than advertising all the allowed codecs.

Auto Framing, set packetization based on the **ptime** preference of the remote endpoint

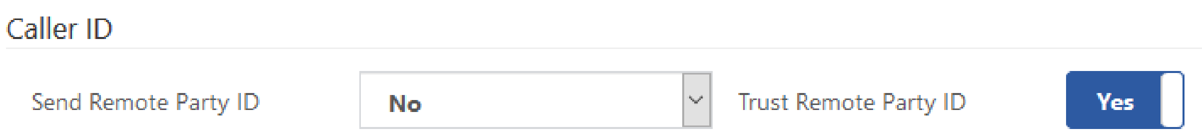
Video Support, turns on or off support for SIP video. You need to turn this on to get any video support at all.

Max Call Bitrate, maximum bitrate for video calls (default 384 kb/s)

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. Other options available in the drop-down list 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 it is available, otherwise use in-band option

Caller ID Section



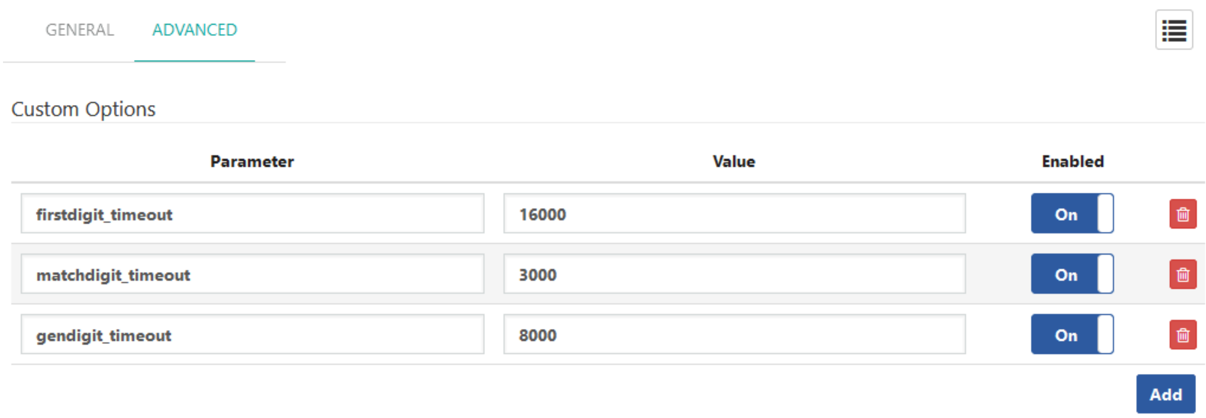
Send Remote Party ID, add remote party ID header to SIP invites.

Trust Remote Party ID, trust that the remote party ID contained in the SIP header is correct.

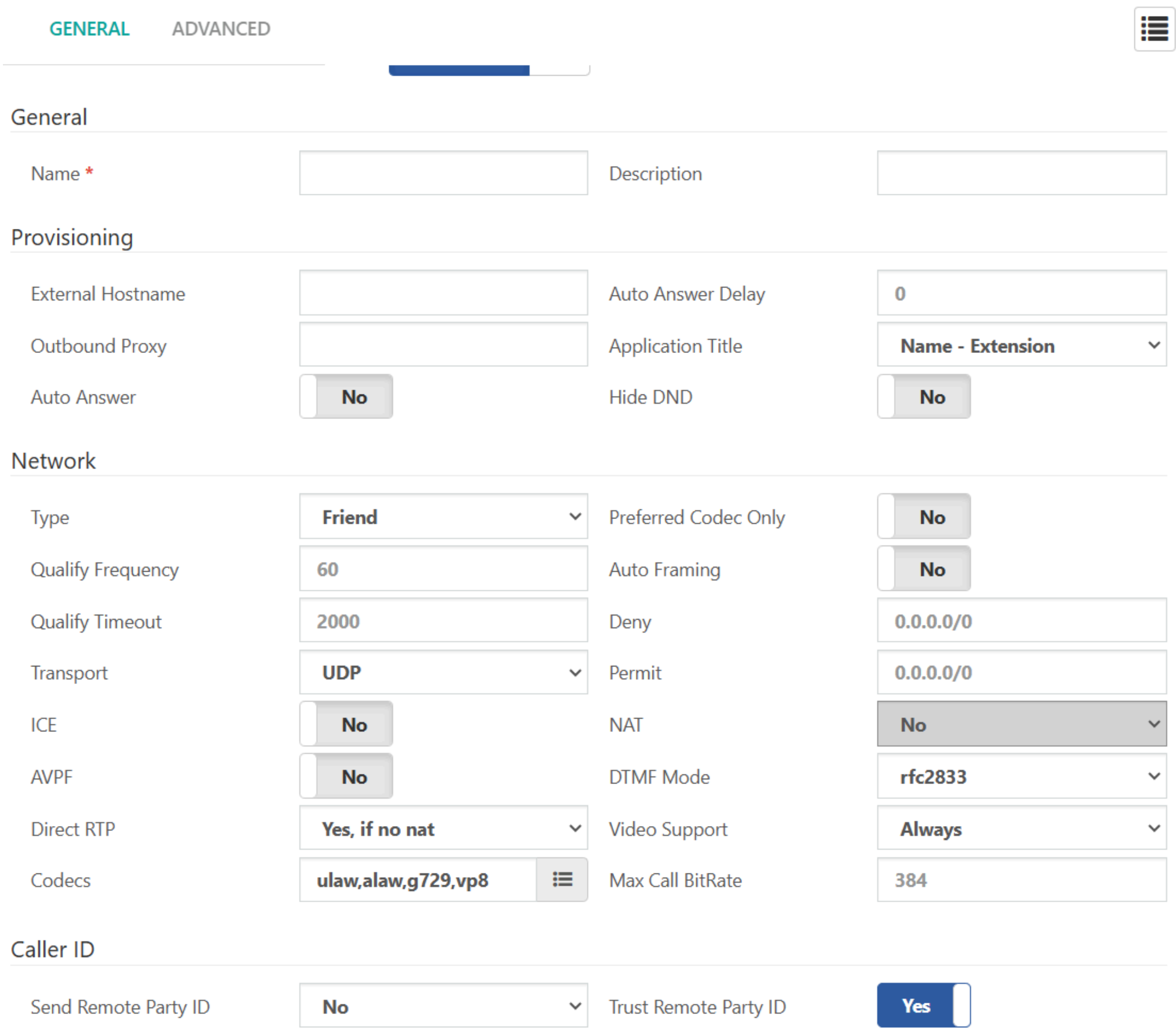
ADVANCED Tab

You can use this tab to modify advanced settings that are not managed from the user interface. For example, you can open an FXS profile, and modify the dial timeouts for analog phones. There are 3 parameters than be managed:

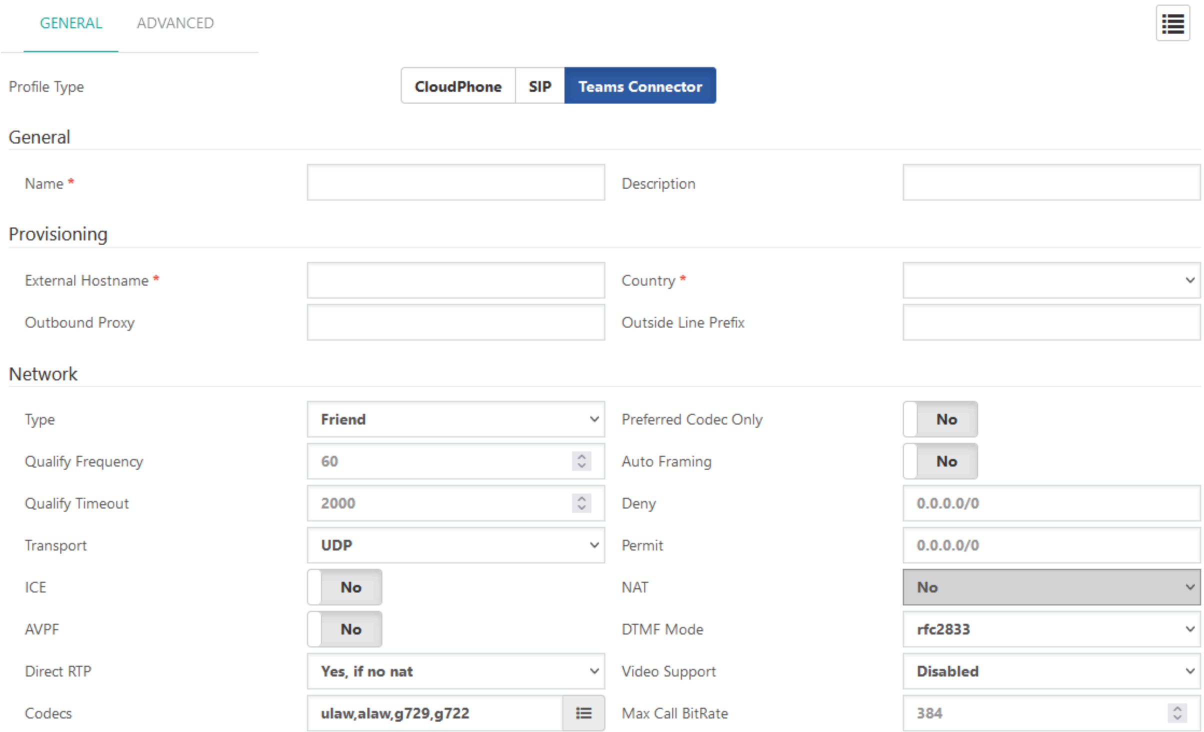
- **firstdigit_timeout** determines how long the system will wait for the first digit to be dialed. The default value is 16000 milliseconds
- **matchdigit_timeout** determines how long to wait for a digit if the current dialed number matches a number or pattern in the current context. The default value is 3000 milliseconds.
- **gendigit_timeout** determines how long the system should wait for a digit if the current dialed number does not match a number or pattern in the current context. The default value is 8000 milliseconds.



CloudPhone


GENERAL
ADVANCED
General
Name *
Description
Provisioning
External Hostname
Auto Answer Delay
0
Outbound Proxy
Application Title
Name - Extension
Auto Answer
No
Hide DND
No
Network
Type
Friend
Preferred Codec Only
No
Qualify Frequency
60
Auto Framing
No
Qualify Timeout
2000
Deny
0.0.0.0/0
Transport
UDP
Permit
0.0.0.0/0
ICE
No
NAT
No
AVPF
No
DTMF Mode
rfc2833
Direct RTP
Yes, if no nat
Video Support
Always
Codecs
ulaw,alaw,g729,vp8
Max Call BitRate
384
Caller ID
Send Remote Party ID
No
Trust Remote Party ID
Yes

Teams Connector

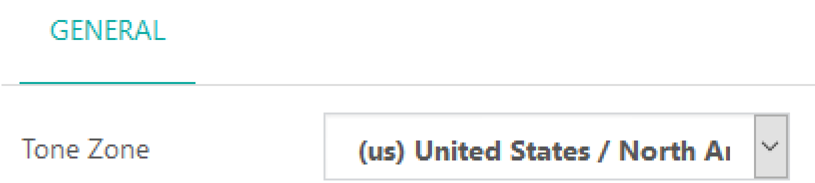


Telephony Settings Dialog

Use this dialog to configure the default time zone to use applied to all users.

GENERAL Tab

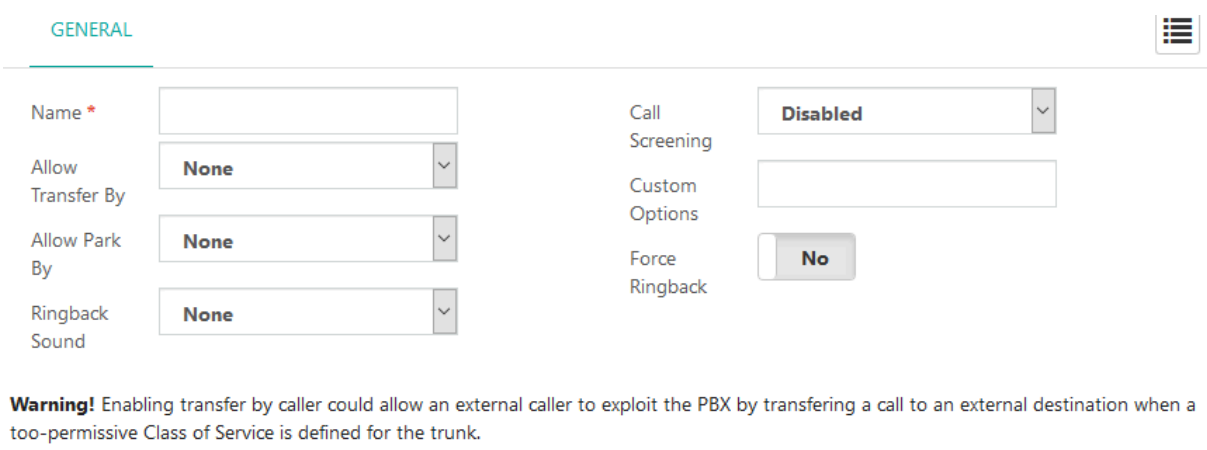
Set the default time zone to be used by all users and peers, by selecting a time zone from the drop-down list.



Dial Profiles Dialog

Use this dialog to create a profile that can be used to control the functionality of extensions. CompletePBX will use this information to configure commonly-used Asterisk dial options. You can use the Advanced tab of the Extensions dialog to define which Dial Profile to associate with an extension.

GENERAL Tab



Name*, a free-text name to identify this profile.

Allow Transfer By, configure who is allowed to transfer calls. Sets the **t** and **T** Asterisk dial options.

- **None** – calls cannot be transferred
- **Caller** – calls can only be transferred by the caller
- **Recipient** – call can only be transferred by the recipient of the call
- **Both** – call can be transferred by either the caller or the recipient of the call

Enabling transfer by the caller may allow an external caller to exploit the PBX by transferring a call to an external destination, unless this is blocked by the Class of Service associated with the Trunk.

Allow Park By, configure who is allowed to park calls. Sets the **k** and **K** Asterisk dial options.

- **None** – calls cannot be parked
- **Caller** – calls can only be parked by the caller
- **Recipient** – call can only be parked by the recipient of the call
- **Both** – call can be parked by either the caller or the recipient of the call

Ringback Sound, sets the sound to be played to the calling party until the call is answered. Select any existing Music on Hold (MoH) Class from the dropdown list. The default setting is to play the country-specific ring sound. Sets the **m** Asterisk dial option.

Call Screening, when enabled, requires the caller to identify themselves. This sets the **p** and **P** Asterisk dial options.

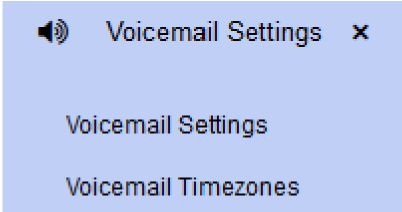
- **Disabled** – callers are not required to be identified

- **Ask Once** – ask callers to identify themselves the first time that they call the extension, and remember this for future calls.
- **Always Ask** – always ask callers to identify themselves, i.e. ask them for identification every time that they ring the extension.

Custom Options, allows you define custom dial option. There are many options that you can set on the inbound call, including call screening, distinctive ringing, and more. Type **core show application dial** in the Asterisk CLI for a complete list of all available options. If you want to specify multiple options, simply concatenate them together. For example, if you want to use both the **m** and **H** options, you would set **mH** as the options parameter. See the Dial Options section in the appendix for a more complete list of available dial options, or refer to Asterisk online documentation for a full list of dial options.

Ringing Tone, when set to Yes, will cause the ringing tone to be played to the caller, even if the device of the called party is not ringing. Sets the **r** Asterisk dial option.

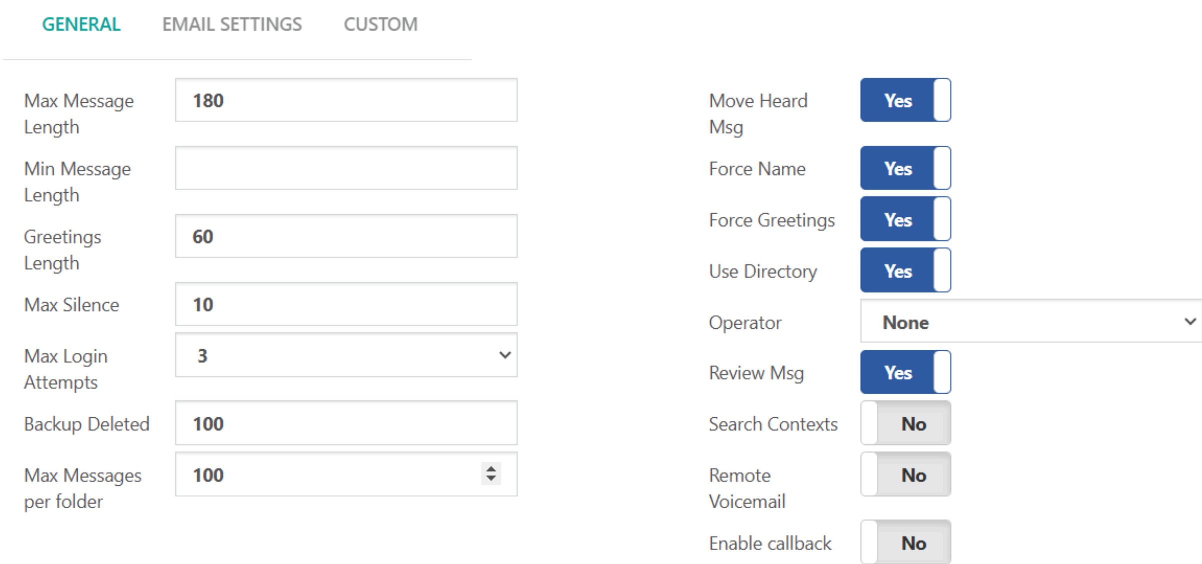
Voicemail Settings Menu Group



Voicemail Settings Dialog

GENERAL Tab

In this tab you will find the information about Voicemail Settings.



Max Message Length, maximum length (in seconds) of a voicemail message. There will be no size restriction if this field is left empty.

Min Message Length, minimum length (in seconds) of a voicemail message for the message to be kept. The voicemail will not be accepted if it is shorter than Min Message Length. There will be no size restriction if this field is left empty.

Greetings Length, maximum length (in seconds) of voicemail greetings.

Max Silence, seconds of silence before ending the recording.

Max Login Attempts, maximum number of failed login attempts when accessing the voicemail box.

Backup Deleted, maximum number of messages allowed in the **deleted** folder. When this number is exceeded, the oldest message will be deleted to allow a new message to be deleted.

Max Messages per folder, maximum number of messages that can stored in the user's mailbox folder. The default value is 100. When this number is exceeded, the oldest message will be deleted to allow a new message to be stored.

Move Heard Msg, move heard messages to the archive folder.

Force Name, forces user to record their name. This is required when the password is the same as the mailbox number.

Force Greetings, forces user to record a greeting message. This is required when the password is the same as the mailbox number.

Use Directory, permit finding entries for forward/compose from the directory.

Operator, select an extension from the drop-down list to allow user to enter an extension number before, after, or during the process of leaving a voicemail, in order to reach the "operator" at the selected extension.

Review Msg, allow caller to review/re-record their message before saving it

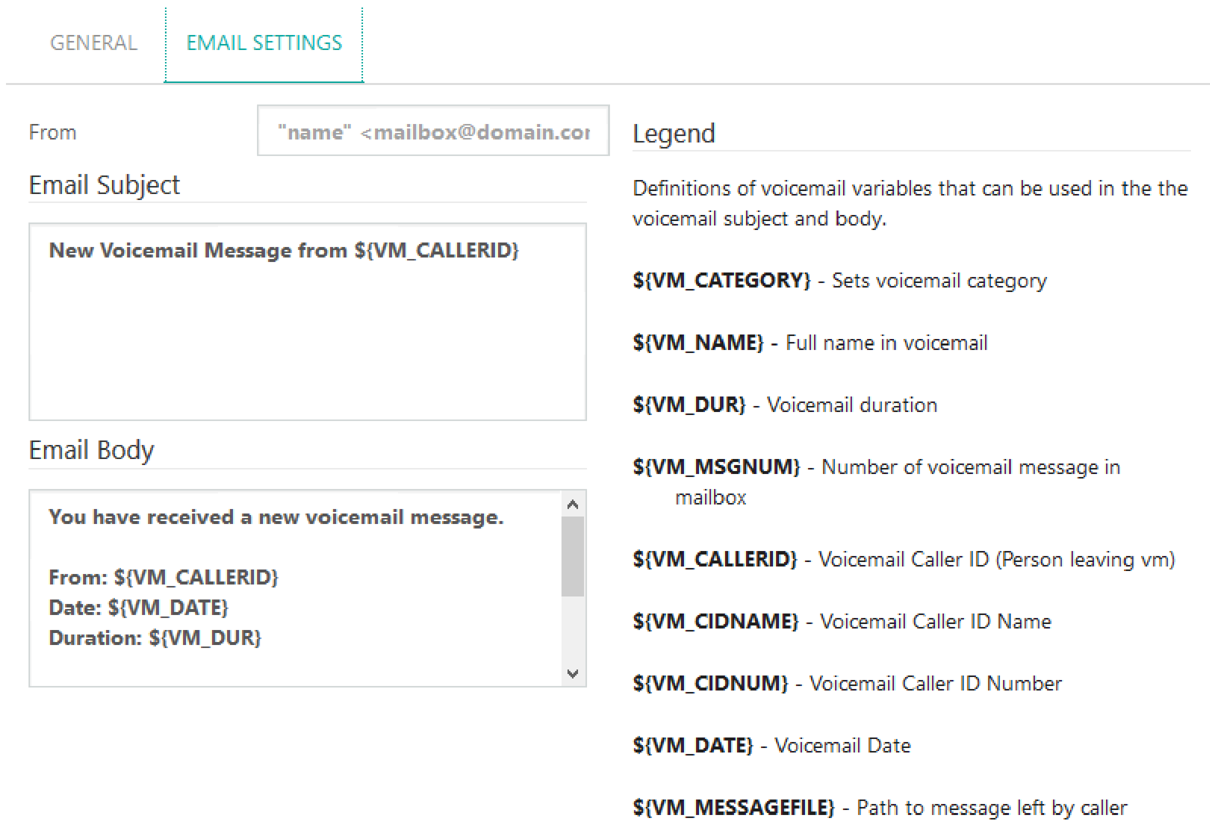
Search Contexts, current default behavior is to search only the default context if one is not specified.

Remote Voicemail, allows access to voicemail from remote devices. When enabled, you can use this feature by dialing * (star) when you reach the voicemail announcement for an extension. If this option is enabled, ensure that all extensions use secure voicemail passwords.

Enable callback, allow dialing back to the voicemail sender. This option is available in the "Advanced" IVR menu when the user interacts with the Voicemail box.

EMAIL SETTINGS Tab

In this tab you will find the information about settings for emailing a voice message.



From, the sender of the email notification.

Email Subject, the text that will be written in the subject line of the email. You can also include system-defined placeholders within the text:

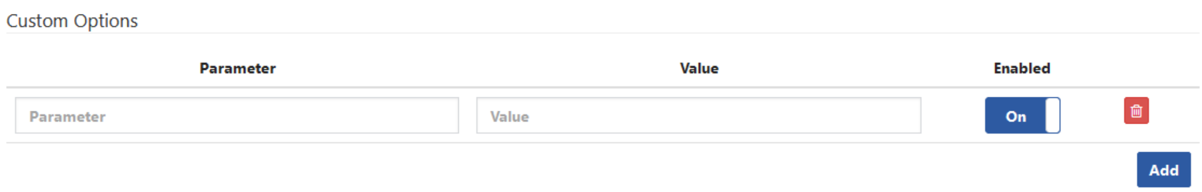
- $(VM_CALLERID) inserts the caller ID (name and number) of the caller who left the message
- $(VM_CIDNAME) inserts the name of the caller who left the message
- ${VM_CIDNUM} inserts the number of the caller who left the message
- $(VM_DATE) inserts the timestamp of the voicemail
- $(VM_DUR) inserts the duration of the voicemail
- $(VM_NAME) inserts the name of the extension receiving the voicemail
- $(VM_MSGNUM) inserts the sequential number of the message that is allocated by the phone system
- $(VM_MAILBOX) inserts the number of the mailbox receiving the voicemail

Email Body, the text that will be written in the body of the email. You can also include system-defined placeholders within the text:

- $(VM_CALLERID) inserts the caller ID (name and number) of the caller who left the message
- $(VM_CIDNAME) inserts the name of the caller who left the message
- ${VM_CIDNUM} inserts the number of the caller who left the message
- $(VM_DATE) inserts the timestamp of the voicemail
- $(VM_DUR) inserts the duration of the voicemail

- $(VM_NAME) inserts the name of the extension receiving the voicemail
- $(VM_MSGNUM) inserts the sequential number of the message that is allocated by the phone system
- $(VM_MAILBOX) inserts the number of the mailbox receiving the voicemail

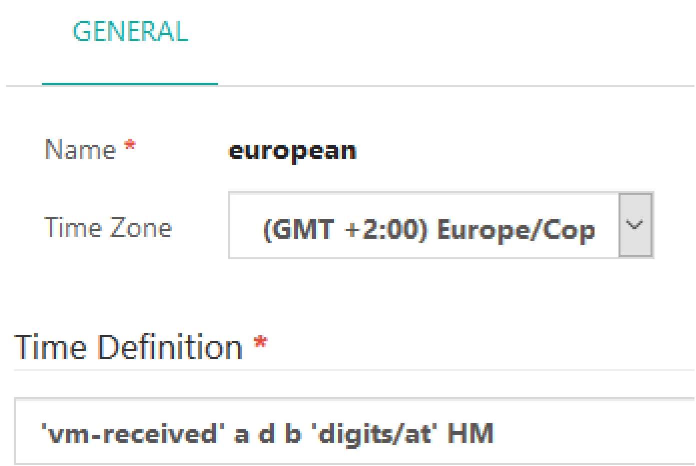
CUSTOM Tab



Voicemail Timezones Dialog

GENERAL Tab

In the Voicemail tab for each extension, it is possible to define what timezone format to use when announcing voicemails. The Voicemail Timezones dialog allows you to configure timezone formats.



Name*, free-text user-defined name for the timezone format.

Time Zone, time zone, selected from the dropdown list of available timezones.

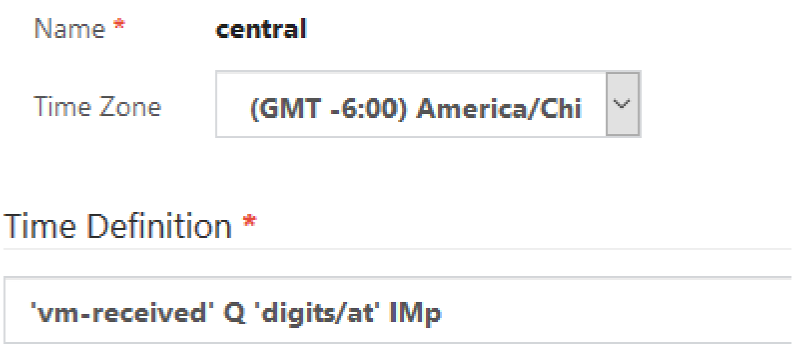
Time Definition*, enables you to configure the style of the announcement that will used when announcing voicemails to an extension. The time definition can include any sound prompt, by enclosing the name of the prompt in single quotes, as well as any date and time formatting symbols from the following list:

- A (or a): placeholder for the day of the week, i.e. Saturday, Sunday, etc.

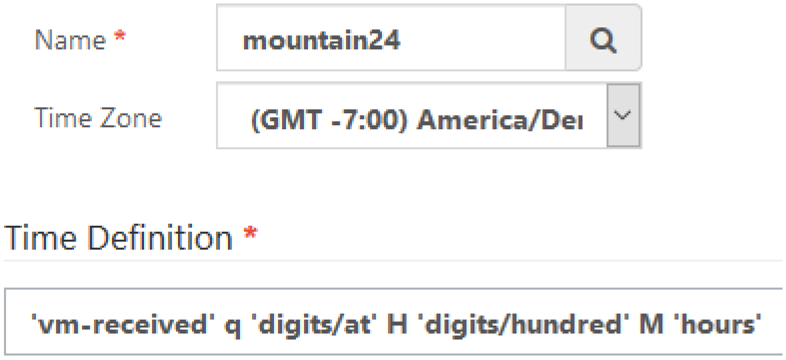
- B (or b or h): placeholder for the name of the month, i.e. January, February, etc.
- d (or e): placeholder for the numeric day of the month, i.e. first, second... thirty-first
- Y : placeholder for the year
- I (or i): placeholder for the hour in 12-hour format
- H: placeholder for the hour in 24-hour format, where single-digit hours are preceded with a zero, and shown like 09:15
- K: placeholder for the hour in 24-hour format, where single-digit hours are **not** preceded by a zero, and shown like 9:15
- M: placeholder for the minute
- P (or p): placeholder to use A.M. or .P.M.
- Q: placeholder for "today", "yesterday," or ABdY
- q: placeholder for "" (for today), "yesterday", weekday, or ABdY
- R: placeholder for the 24-hour time, including minutes

The following examples illustrate two different voicemail timezone styles. In both cases, note the use of sound prompts (enclosed with single quotes) to make the message more user-friendly.

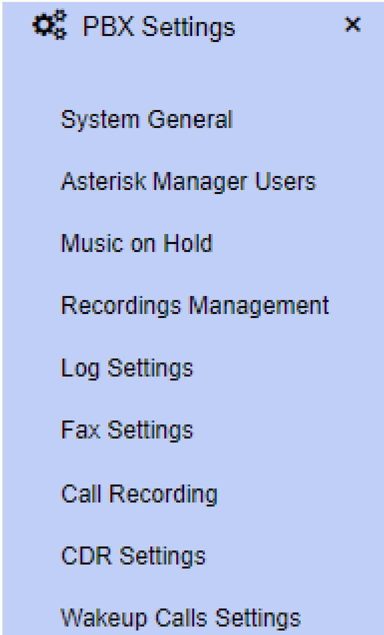
This example is for messages that will be delivered in 12-hour format to an extension that is linked to **central** in the Zone Messages field of the Voicemail tab in the Extensions dialog:



This example is for messages that will be delivered in 24-hour format to an extension that is linked to **mountain24** in the Zone Messages field of the Voicemail tab in the Extensions dialog:


Name *
mountain24
Time Zone
(GMT -7:00) America/Dei
Time Definition *
'vm-received' q 'digits/at' H 'digits/hundred' M 'hours'

PBX Settings Menu Group

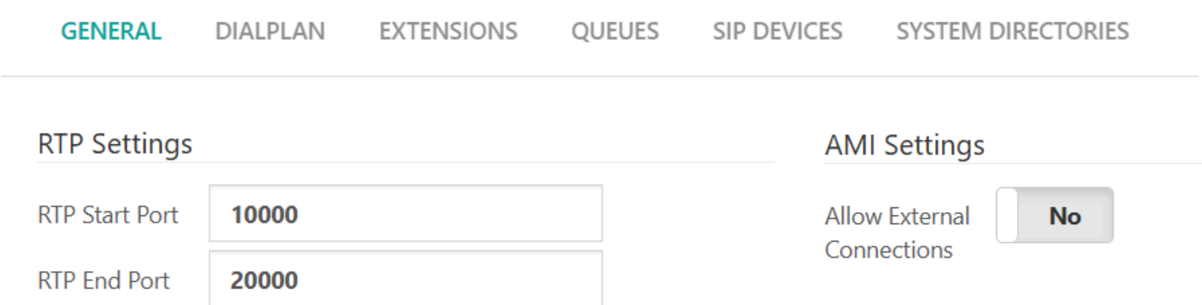


System General Dialog

GENERAL Tab

In this tab you will find the information about PBX Settings. These settings determine default values when creating new extensions.

RTP Settings Section

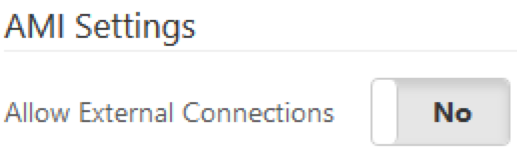


Allows you to configure the range of ports that will be used for RTP communication. If left empty, the port range will default to 10000-20000

RTP Start Port, the first port in the range

RTP End Port, the last port in the range

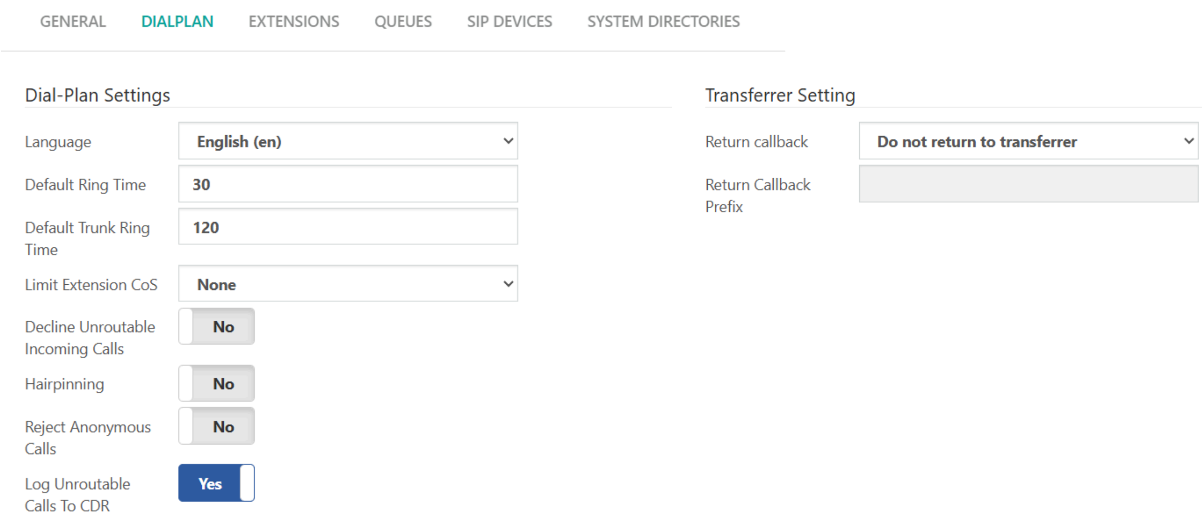
AMI Settings Section



Set to Yes if you want to allow external access to AMI. When set to No, access is only allowed from the local network, i.e. 127.0.0.1

DIALPLAN Tab

Dial-Plan Settings Section



Language, the default language to be used for voice prompts when no other language is applicable.

Default Ring Time, default time, in seconds, that outgoing calls should ring for, unless there is a setting on the extension that overrides this value. This setting does not apply to trunks.

Default Trunk Ring Time, sets the default ring time, in seconds, for trunks. Default value is 120, configurable from 5 to 3600 seconds.

Limit Extension CoS, defines a global Class of Service (CoS) that can be accessed by dialing the Limit Extension Feature Code (default code: *74). This can be activated by a user to restrict the features available on the extension when out of the office.

Decline Unroutable Incoming Calls, when this feature is configured as feature as **Yes,** the PBX will drop inbound calls that are made to unrecognized DIDs, without answering the call and without playing an error message.

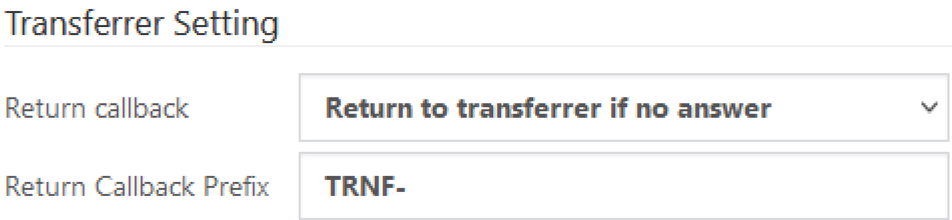
Hairpinning, when a call is made to an external number, it is normally routed via an outbound route to a trunk. However, if a call is made to an external number that is defined as an inbound route in

CompletePBX ***and*** hairpinning is enabled, the call will be sent directly to the internal destination defined for the inbound route, and will not be routed to a trunk.

Reject Anonymous Calls, an option to block all incoming calls from anonymous callers. This applies system-wide, regardless of the channel technology used—whether SIP, IAX2, or legacy telephony interfaces such as FXO, E1/T1, or ISDN BRI.

Log Unroutable Calls to CDR, enables logging in the Call Detail Records (CDR) for calls that end through ‘Terminate Call’ actions and may not have been logged previously. This improves visibility and tracking of failed or unroutable call attempts. The feature is enabled by default to enhance system diagnostics and reporting.

Transferrer Settings Section



Allows you to configure the behavior of transferred calls if not answered by the transfer destination. This setting affects unattended (blind) transfers only.

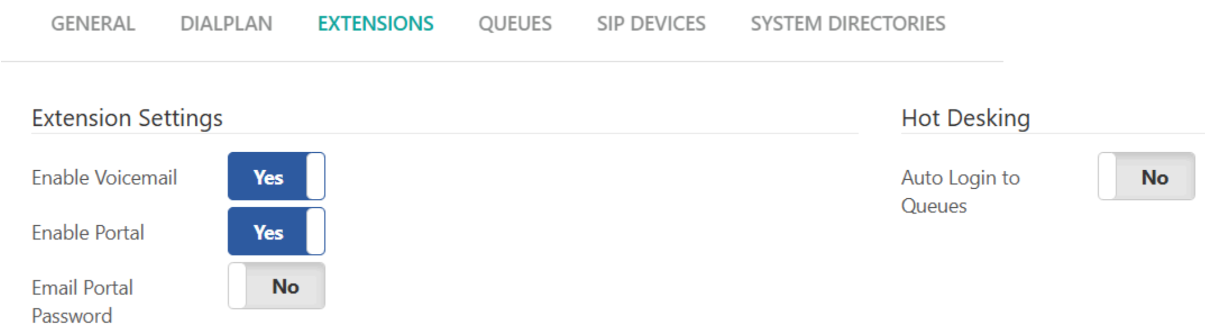
Return callback, return callback behavior when the transfer destination is not answering (valid only on blind transfers to an extension). The available options are:

- Return to transferrer if no answer
- Return to transferrer if no answer or voicemail
- Do not return to the transferrer

Return Callback Prefix, prefix to prepend to CID Name. Can be used to indicate to the transferrer that call came back from an unanswered transfer call. This allows the recipient to determine whether the call is a new call or a returned call.

EXTENSIONS Tab

Extensions Settings Section



Enable Voicemail, determines whether voicemail will be automatically enabled when creating a new extension.

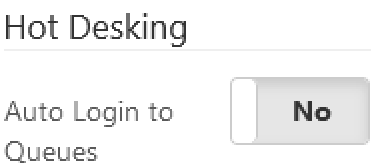
Enable Portal, determines whether Portal access will be automatically enabled when creating a new extension.

Email Portal Password, default value is no, but when set to **Yes**, an email will be sent when an extension is created, provided that:

- The extension is configured as a Portal user
- A valid email address is defined for the extension
- Email for CompletePBX 5 is configured and working correctly

The email will provide the Portal user with Portal user, password, and the link that should be used to access the Portal, so it is important that the administrator accesses CompletePBX 5 with the same URL that the Portal user will use.

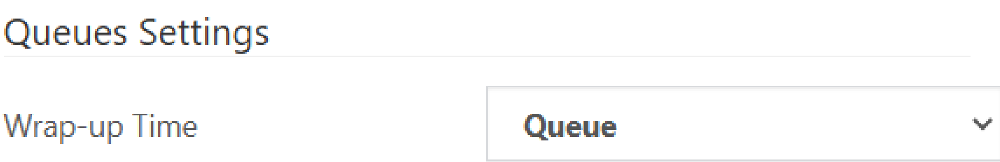
Hot Desking Section



Set to Yes if you want to allow Dynamic Agents in hot-desking environments to be logged into their respective queues when logging into their extension, avoiding the need for logging in to each one separately.

QUEUES Tab

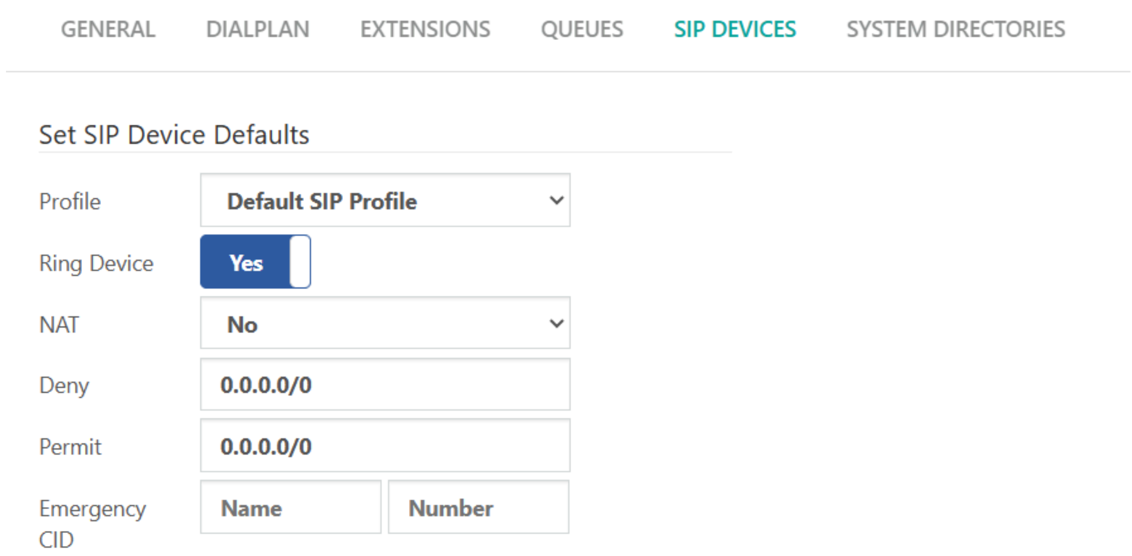
Queues Settings Section



Defines how post-call wrap-up time is applied to agents. **By Agent**: a shared wrap-up timer is used across all queues for each agent. **By Queue**: each queue uses its own separate wrap-up timer per agent.

SIP DEVICES Tab

Set SIP Device Defaults Section



Profile, to ensure consistent configuration for all newly created SIP devices, a default profile can be configured here.

Ring Device, determines whether incoming calls should cause the devices to ring. When enabled, calls directed to the extensions will alert the specific devices; when disabled, the devices will not generate an audible ring even though it may still receive SIP signaling.

NAT, *Network Address Translation*, is a mechanism commonly used by routers and firewalls to allow multiple private-address devices inside a local LAN to share a single public IP address. Private IP addresses are only reachable within the LAN and cannot be reached directly from the public internet.

The following NAT behaviors can be selected from the drop-down list:

- **No** – no special NAT handling other than RFC3581.
- **Force** – treat the SIP message as if it contained an rport parameter, even if it does not.
- **Comedia** – send RTP media to the same port from which it was received, regardless of the SDP media address.
- **Auto Force** – automatically apply *force_rport* if Asterisk detects that the device is behind NAT.
- **Auto Comedia** – automatically apply *comedia* if Asterisk detects NAT conditions.

These settings are essential when devices are deployed behind routers performing NAT, ensuring consistent SIP signaling and RTP media flow.

Deny, defines one or more IP addresses or networks whose traffic should be explicitly blocked for the devices.
The default value **0.0.0.0/0** blocks all networks.
Entries may be written using subnet masks (e.g., *192.168.1.0/255.255.255.0*) or CIDR notation (e.g., *192.168.1.0/24*), separated by commas or spaces.
Use this field to restrict device registration or traffic to specific, trusted networks only.

Permit, defines one or more IP addresses or networks that are explicitly allowed to communicate with the devices.
The default value **0.0.0.0/0** allows traffic from all networks.
Values may be entered in mask or CIDR format, separated by commas or spaces.
When combined with the **Deny** field, Permit acts as a whitelist that can significantly enhance security by limiting which networks may register or authenticate the device.

Emergency CID, defines the emergency caller ID for the devices, consisting of two components:

- **CID Name** – descriptive text indicating the caller's location or identifier.
- **CID Number** – numeric caller ID used for return calls during emergency situations.

This emergency caller ID is used when the devices dial emergency numbers configured on the PBX.

Note: Creating an Emergency CID automatically generates a DID associated with the device, allowing emergency responders or automated systems to directly call back the specific device, bypassing standard PBX routing or extension behavior.

SYSTEM DIRECTORIES Tab

GENERAL SYSTEM DIRECTORIES

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

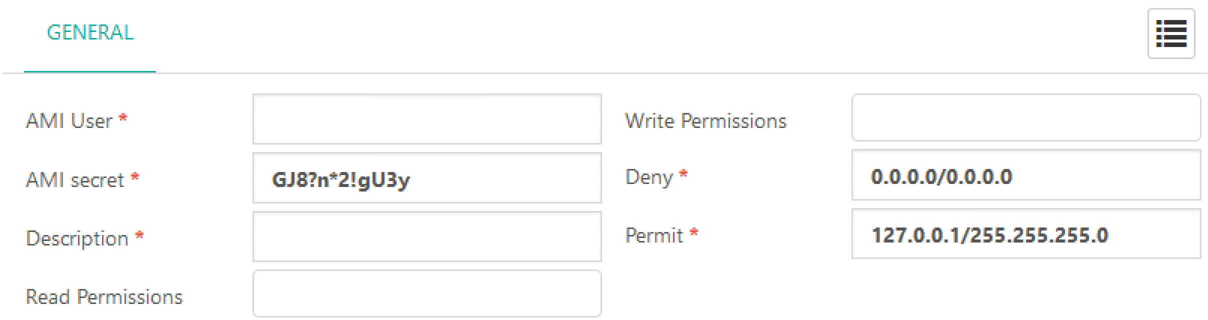
- **Asterisk AGI Directory,** Asterisk AGI directory
- **Asterisk Directory,** home Asterisk directory.
- **Asterisk Log Directory,** Asterisk log directory.

- **Asterisk Modules Directory,** Asterisk dialogs directory.
- **Asterisk Sound Directory,** Asterisk sound directory
- **Asterisk Spool Directory,** Asterisk spool (recording) directory
- **Asterisk Libraries Directory,** Asterisk libraries directory

Asterisk Manager Users Dialog

GENERAL Tab

In this tab you will find the information about Asterisk Manager Users.



AMI User*, user name for connect to Asterisk Management Interface (AMI) - must be unique

AMI Secret*, secret for login to Asterisk Management Interface (AMI)

Description*, free-text description

Read Permissions, Asterisk Management Interface (AMI) read permissions - select one (or more) from the list of available options

Write Permissions, Asterisk Management Interface (AMI) write permissions - select one (or more) from the list of available options

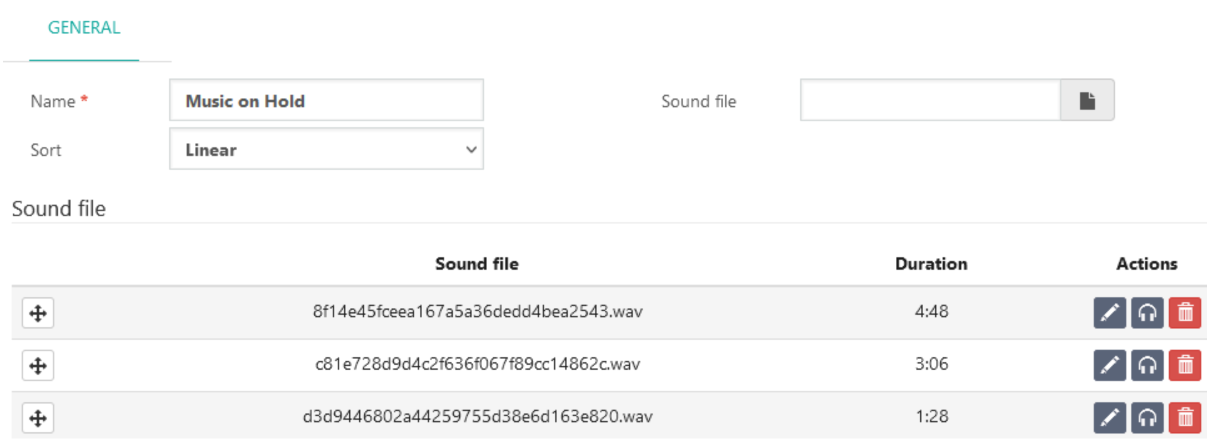
Deny, to deny multiple hosts or networks**,** use the **&** character as separator, for example: 192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0

Permit, to permit multiple hosts or networks**,** use the **&** character as separator, for example: 192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0

Music on Hold Dialog

GENERAL Tab

In this tab you will find the information about Music on Hold.



Name*, free-text description to identify this Music on Hold category.

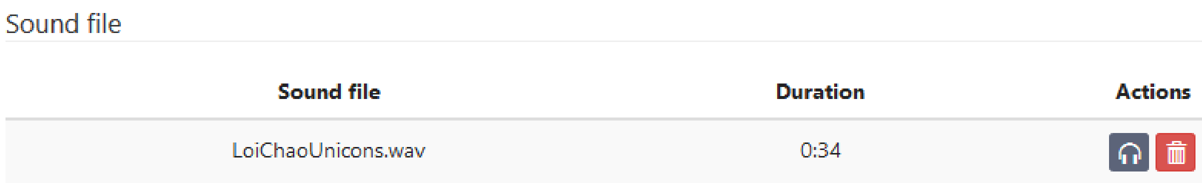
Sort, sort the files to play. Available options are:

- Linear – play audio files in linear order
- Shuffle – play audio files in random order

Sound File, upload a wav or mp3 file.

Sound File Section

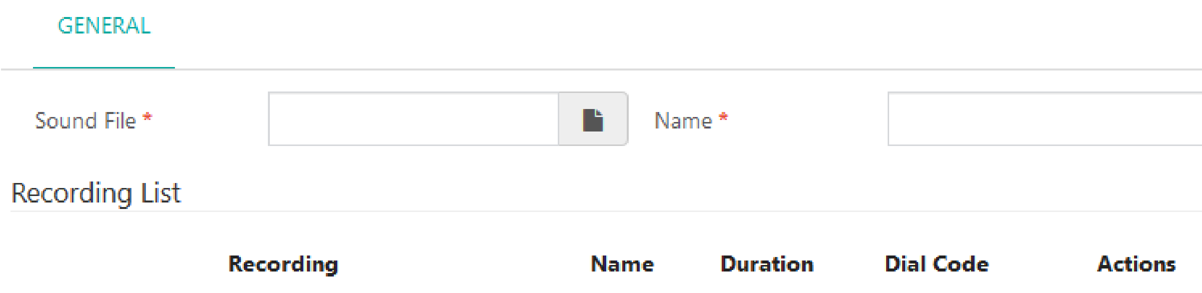
This section displays information about the Music on Hold file/s. You can use the icons to the right to listen to, or delete, Music on Hold files.



Recordings Management Dialog

GENERAL Tab

In this tab you will find the information about Recordings Management.



Sound File*, upload a wav or mp3 file.

Name*, free-text description to identify the recording.

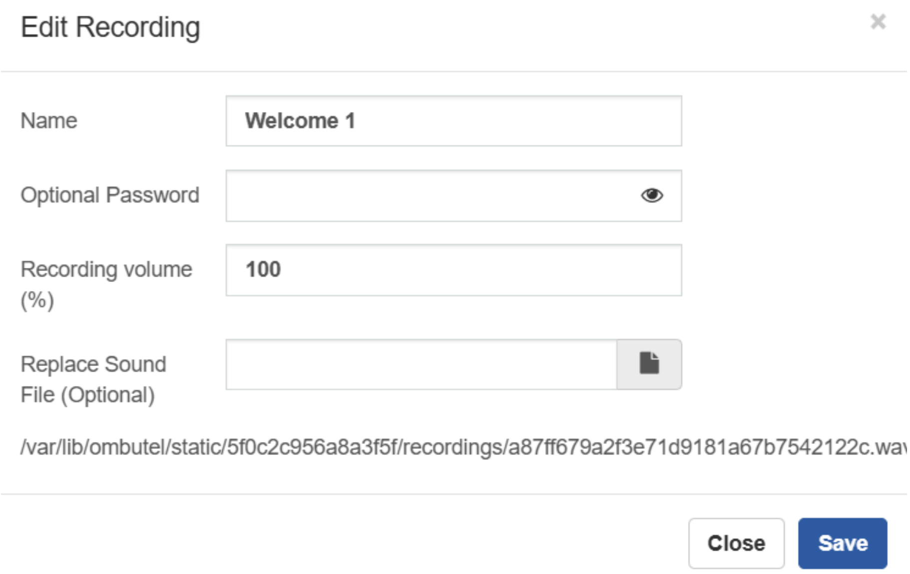
Recording List Section

Recording List

Recording	Name	Duration	Dial Code	Actions
ChillingMusic.mp3	Chill	0:27	*90*5	
07-Maggie Mae.mp3	rec3	0:41	*90*3	
20180528_2100_1527492233.59.wav	music	0:03	*90*4	
marker-1.wav	marker	0:04	*90*6	

- **Recording,** name of the sound file.
- **Name,** description of the sound file. The system allocates a name when a recording is first uploaded or created. However, you can use the edit icon (described in Actions below) to give the recording a more user-friendly name.
- **Duration**, length (in seconds) of the recording.
- **Dial Code,** each saved recording will be allocated a Dial Code, consisting of the feature code used to make recordings (typically, *92) followed by a unique identifier. Dialing this Dial Code will allow you to replace an existing recording.
- **Actions:**
    - o **,** edit the name, or (optionally) protect the recording with a password. A password-protected recording will be indicated by the lock icon beside the dial code. In cases where the volume of the recording is too quiet or too loud, you can use the **Recording volume** field to adjust the volume of the recording. The value of this field determines by what percentage to modify the original recording. If you do not want to make any change to the volume of the recording, leave the value of this field as 100. The recording path is available to facilitate locating the recording file when needed. The Update/Replace option allows to replace an existing system recording with a new audio file while preserving the same recording reference. This

change is applied globally across all modules where the recording is used (such as IVR, Queues, and Announcements), eliminating the need for manual reconfiguration in each module.

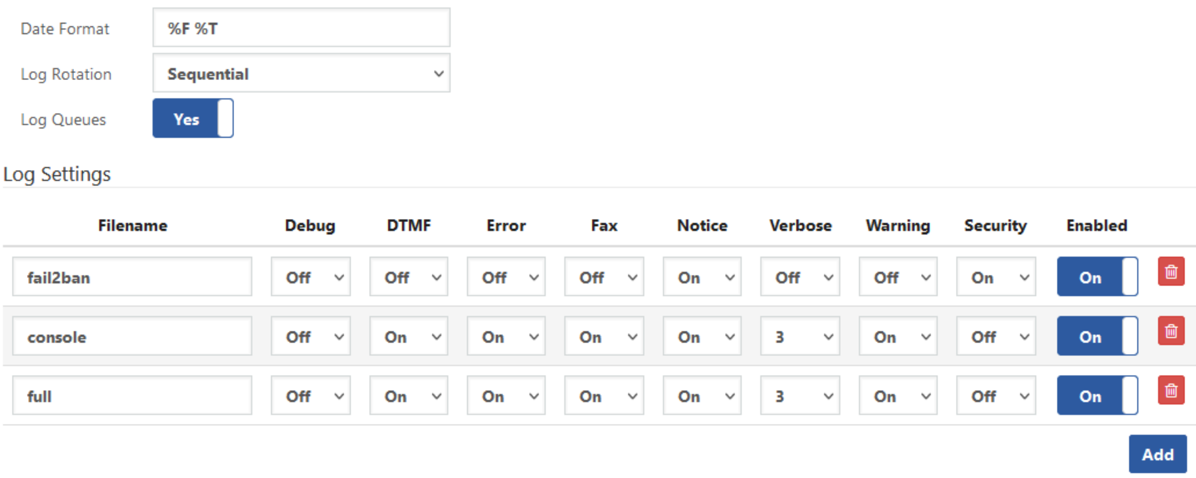


- o , listen to the recording.
- o , delete the recording.

Log Settings Dialog

GENERAL Tab

In this tab you can configure the contents of log files.



Date Format, customize the display of debug message time stamps. See strftime(3) Linux manual for specification of formats. 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

- **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, when set to **Yes**, appends the hostname to the name of the log file

Log Queues, set to **Yes** to log queue events to a file.

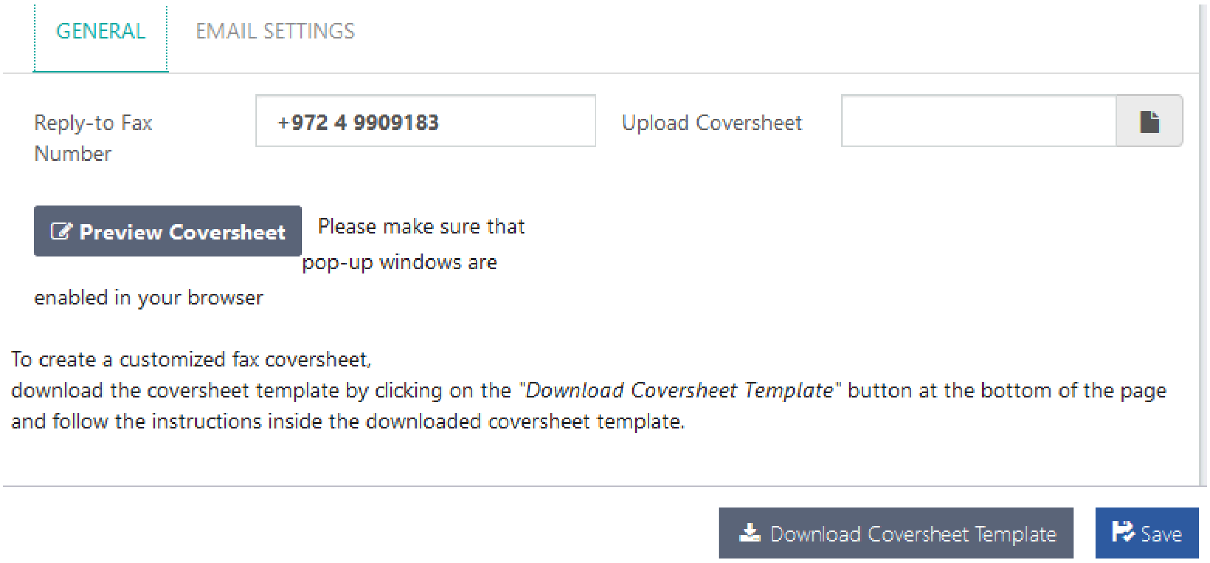
Log Files Section

- **Filename,** 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 more risky 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.
- **Enabled,** enable/disable the log setting

Fax Settings Dialog

This dialog allows you to configure the system-wide cover sheet that will be used for outbound faxes.

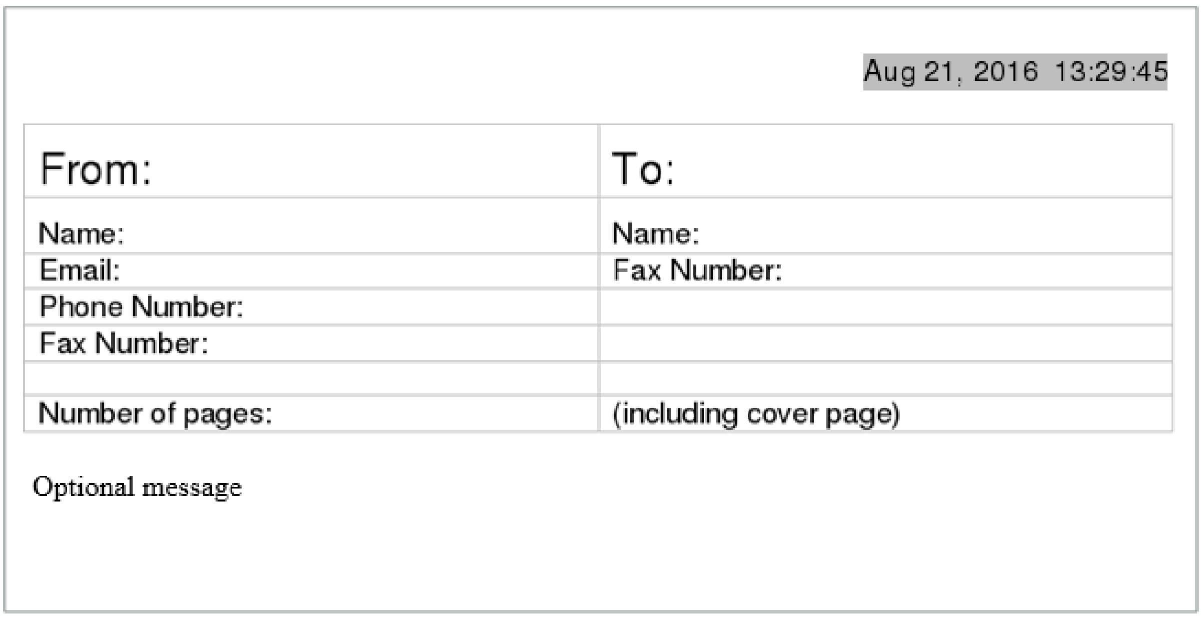
GENERAL Tab



Reply-to-Fax Number, is the number that identifies your fax station. Typically, this would be the number which external users would use to send faxes to your system.

Preview Coversheet, allows you to review the coversheet that is currently stored in the system. Pop-up windows must be enabled in order to display the coversheet.

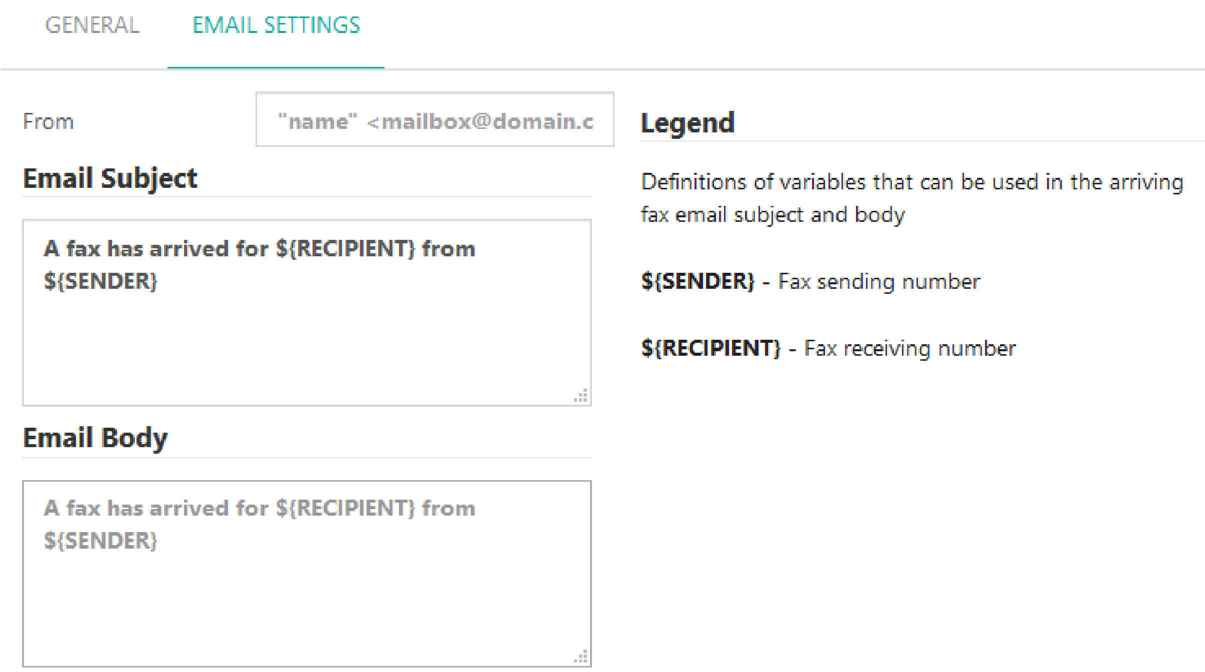
Upload Coversheet, allows you to upload a coversheet that can be used on outbound faxes. The coversheet must be in pdf format. You can download a coversheet template by clicking on the **Download Coversheet Template** action button at the bottom of the screen that allows you to download a template which can use to create your personalized coversheet. The template is downloaded in doc format: after completing your modifications, it must be saved in pdf format for uploading.



- The areas that are shaded in gray (such as the date and timestamp fields) are auto populated by the system with dynamic information, so you must not change them.
- In the blank areas you may place any static image or text, such as your company logo, slogan, policy statement etc.
- Delete the instructions box and save the file in pdf format.
- Upload the created file using this dialog.

EMAIL SETTINGS Tab

This tab enables you to customize the message that is sent to users when they receive a new fax message. You can insert free text into the **Email Subject** and **Email Body**, and make use of system-defined placeholders, **${SENDER}** and **${RECIPIENT}**.



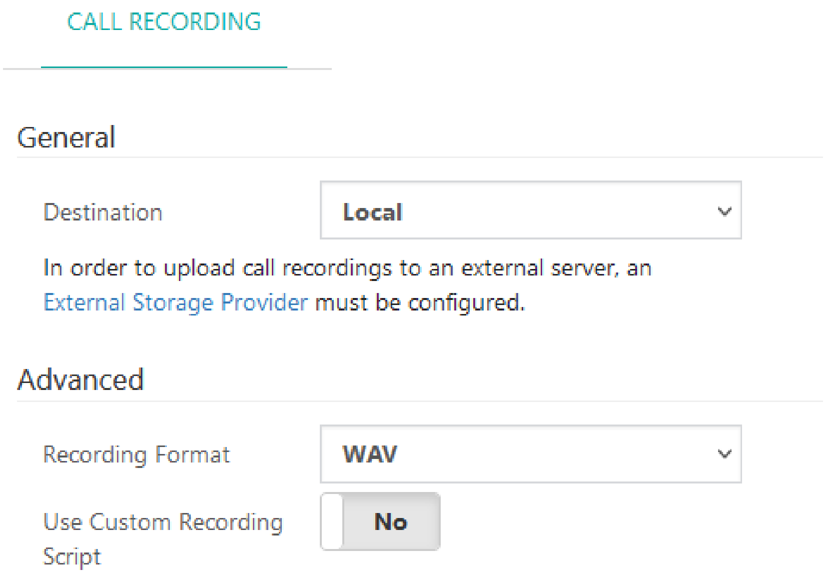
From, this field is not user-editable.

Email Subject, the text that will be shown in the subject field of the email. You can configure this field with any text that you want, including usage of the placeholders defined in the **Legend** section.

Email Body, the text that will be shown in the body of the email. You can configure this field with any text that you want, including usage of the placeholders defined in the **Legend** section.

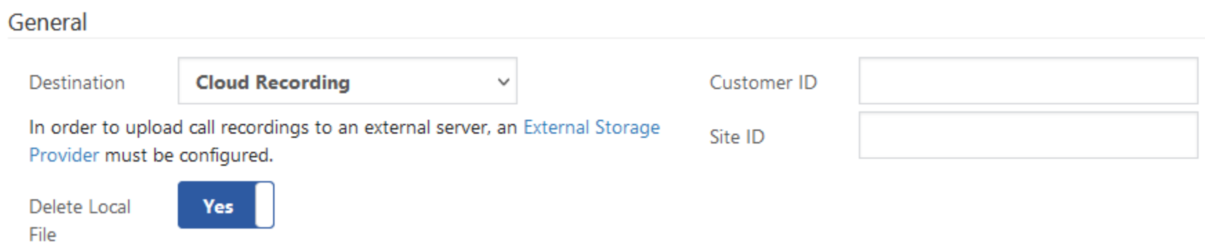
Call Recording Dialog

CALL RECORDING Tab



General Section

Destination, allows you to specify where call recordings will be stored, offering two options: **Local** and **Cloud Recording**. If Cloud Recording is chosen, you'll need to configure an External Storage Provider by entering the **Customer ID and Site ID** of your chosen provider. Additionally, you can utilize an S3 external resource for this purpose.



Delete Local File, when set to **Yes**, call recordings are deleted from the local drive and only stored on the cloud server. If set to **No**, call recordings will be stored on both the local drive and in the cloud.

Customer ID, customer ID that was allocated to you when you signed up for the Cloud Recording option.

Site ID, site ID that was allocated to you when you signed up for the Cloud Recording option. One customer may have more than one **Site ID**.

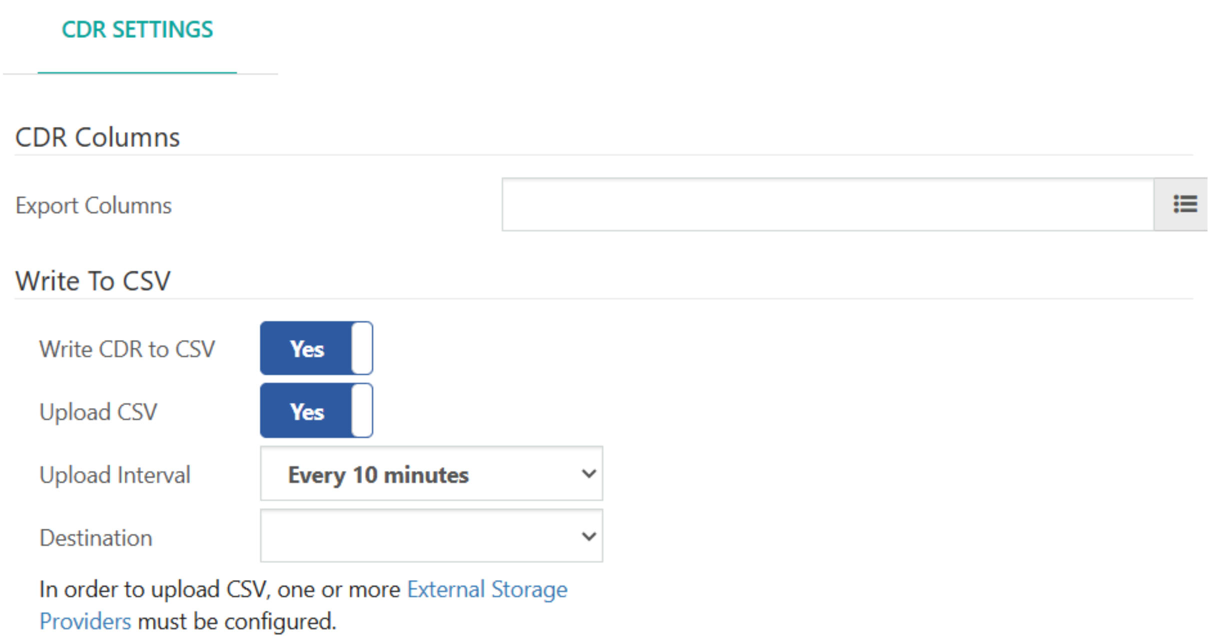
Advanced Section

Recording Format, allows you to choose WAV, WAV49, or GSM audio format for recordings stored either locally. (Recordings stored in the cloud are always stored in GSM format.)

Use Custom Recording Script, allows you enable a custom recording script that will be activated before the recording is stored locally. Ensure that the file is located in a directory to which the Asterisk user has access, and that the file permissions allow the Asterisk user to execute the script.

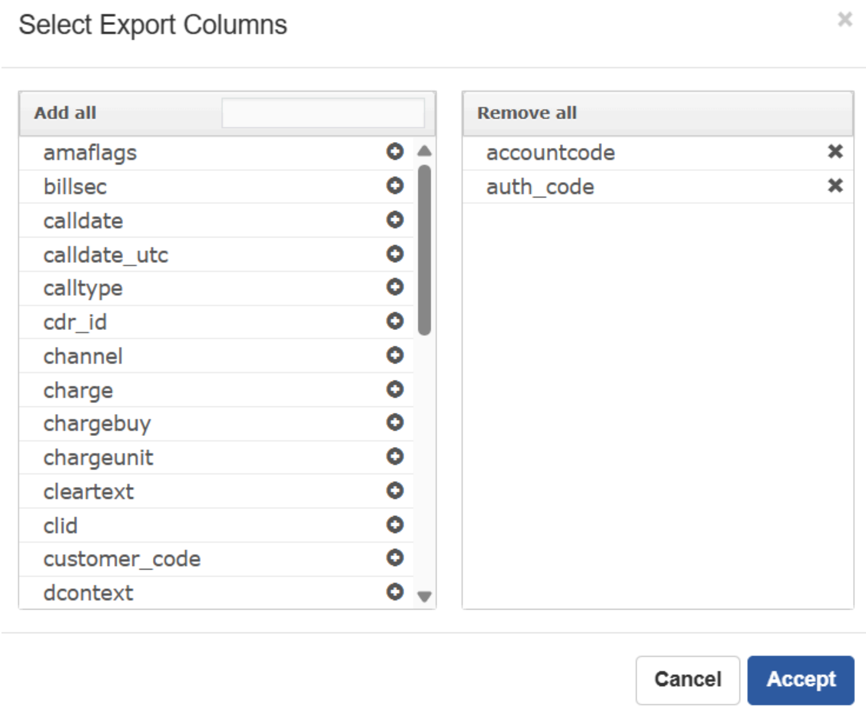
CDR Settings Dialog

This dialog allows to set CDR upload to an external storage (configured in External Resources). This allows easy integration with third party billing and other systems.



CDR Columns Section

Export Columns, you can select specific columns when exporting CDRs.



Write to CSV Section

Write CDR to CSV, when set to **Yes**, allow to generate CSV files that contain CDR records.

Upload CSV, when set to **Yes**, allow to upload generated CSV files to an external storage provider.

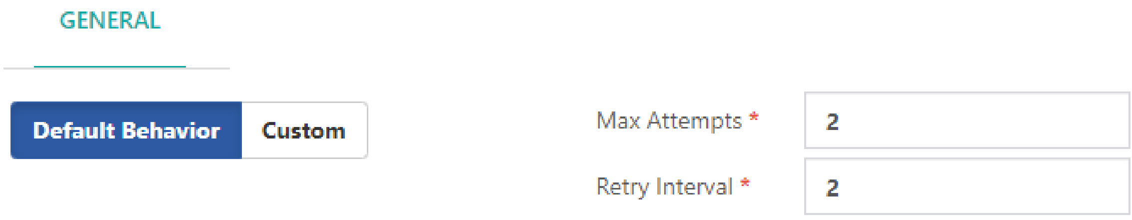
Upload Interval, allows setting the interval between upload attempts.

Destination, allows specifying which external storage provider to use when uploading CSV files.

Wakeup Calls Settings Dialog

This dialog allows you to configure the maximum number of attempts for a wake-up call and additional customization options.

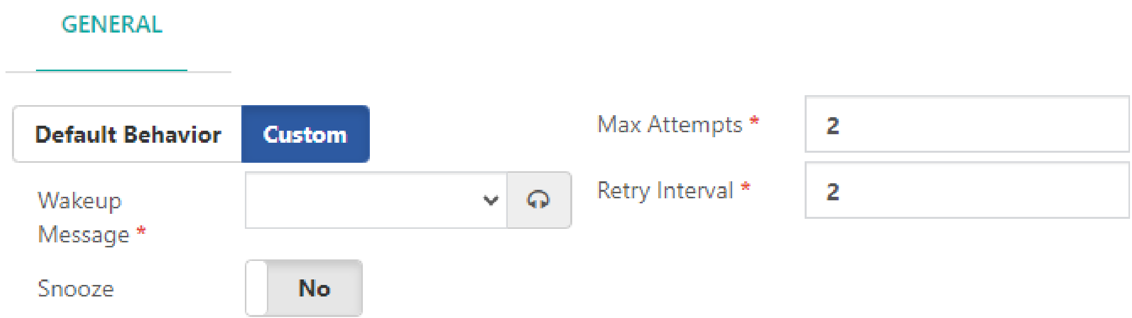
Default Behavior Option



Max Attempts, determines the number of times a wakeup call will be attempted when there is no answer.

Retry Interval, determines the time, in minutes, between each wakeup attempt. If the wake-up call is not answered when this limit is reached, the wake-up call will be abandoned.

Custom Option

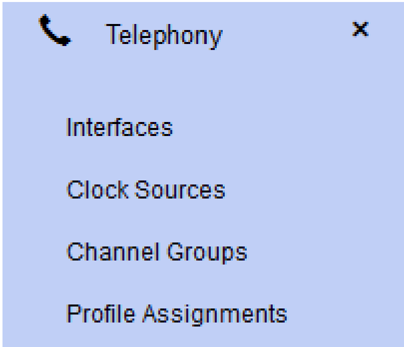


Wakeup Message *, allows you to select a custom recording to play on wakeup call answer. Navigate to the Recordings Management dialog (Settings>PBX Settings>Recordings Management) to manage your recordings.

Snooze, when set to **Yes**, allows snooze after answering the wakeup call. If enabled, make sure your Wakeup Message contains snooze instructions. Snooze time is 5 minutes and the user needs to press 1 in order to activate it.

Telephony Menu Group

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)



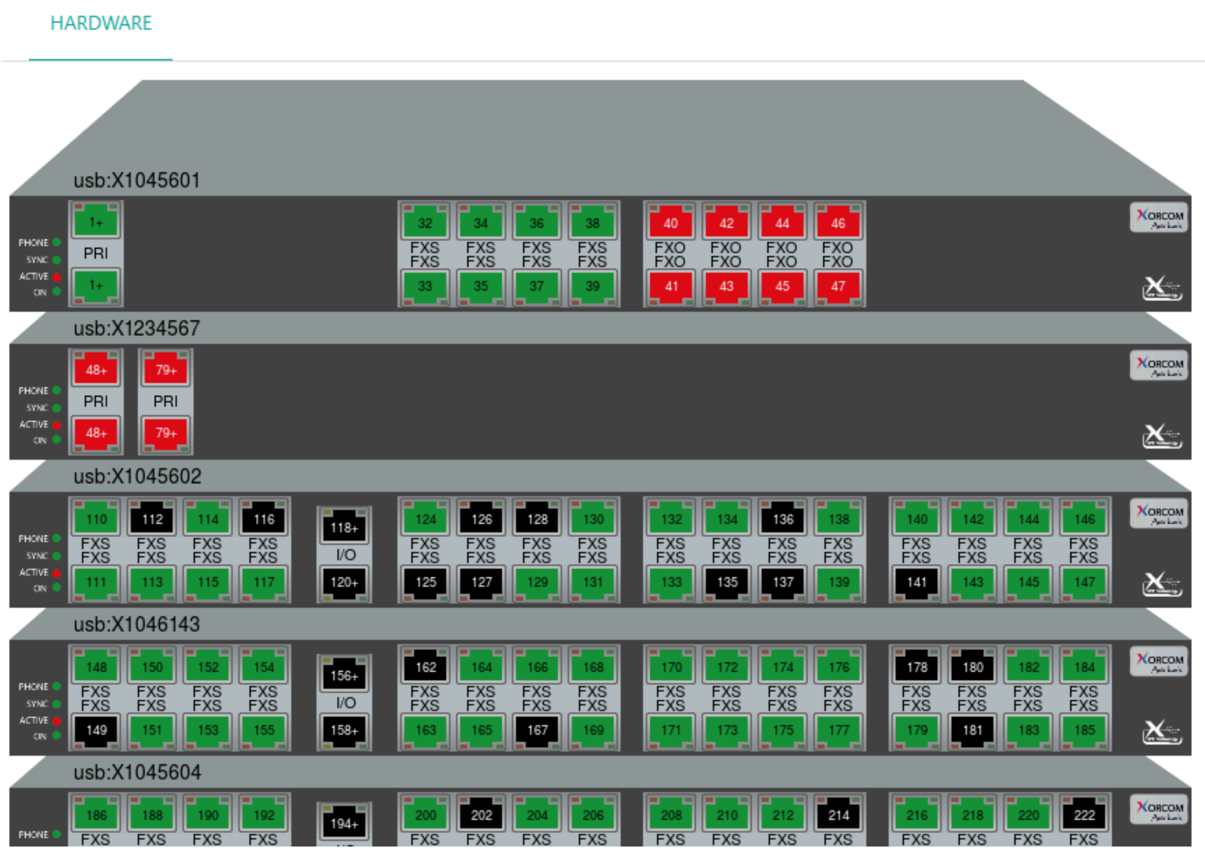
Interfaces Dialog

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

HARDWARE Tab

The tab provides a visual representation of telephony hardware that is integrated into your system. The graphical display will indicate the Xorcom serial numbers of the devices that are connected, the type of interfaces are available, and their channel numbers. FXS channels that are defined in CompletePBX 5 will be colored green. FXS ports that are not defined in CompletePBX 5 are shown in black

Click on **Detect Hardware** to automatically detect attached telephony hardware.



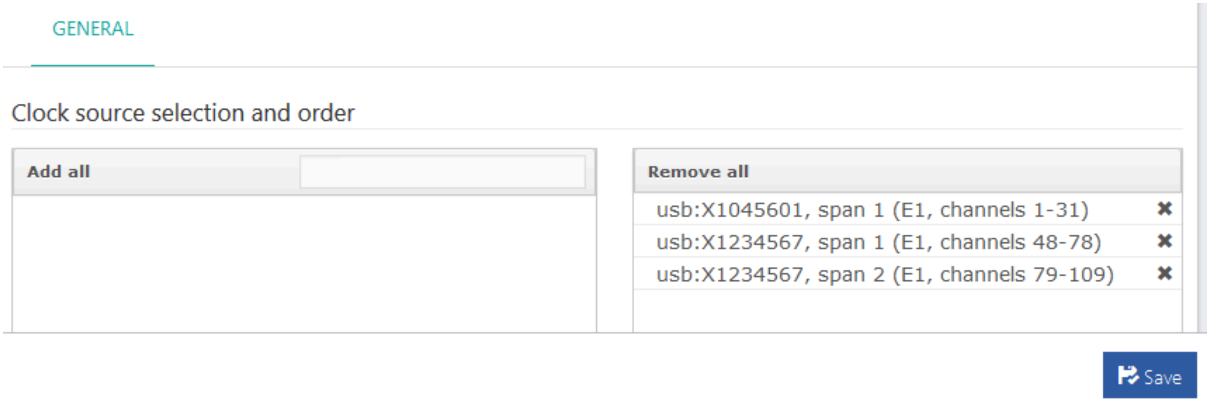
Clock Sources Dialog

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

General Tab

Displays list of clock sources, enabling you to configure which spans will provide timing for the system. The clock source provides a reliable source of a fixed frequency signal used for timing in the PBX system. Asterisk uses it, amongst other things, for the RTP stream and recording playback. If you define multiple clock sources, they will be used in the order in which they appear. Be wary if you have multiple clock sources that are connected to ***different*** providers, as this may cause timing conflicts.

Do not forget to click on **Save** after making any changes.

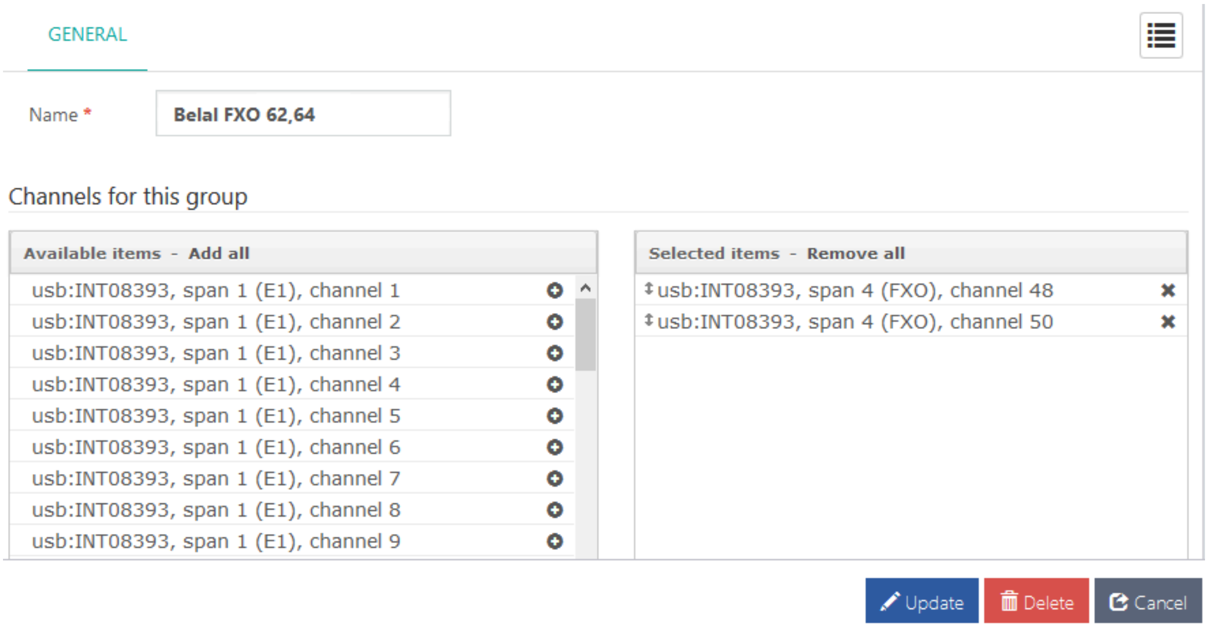


Channel Groups Dialog

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

Allows you to create groups of channels, by selecting available channels from the drop-down list. The drop-down list is automatically populated by clicking **Detect Hardware** in the Settings > Telephony > Interfaces dialog.

GENERAL Tab



Name*, is free-text description to uniquely identify a Channel Group.

Available Items, is a list of all channels that have been discovered on the system, that do not belong to the current Channel Group. Click on the **+** icon to add an available channel to the current Channel Group.

Selected Items, is a list of all channels that have been selected as members of the Channel Group. Click on the **X** icon to remove a channel from the channel group.

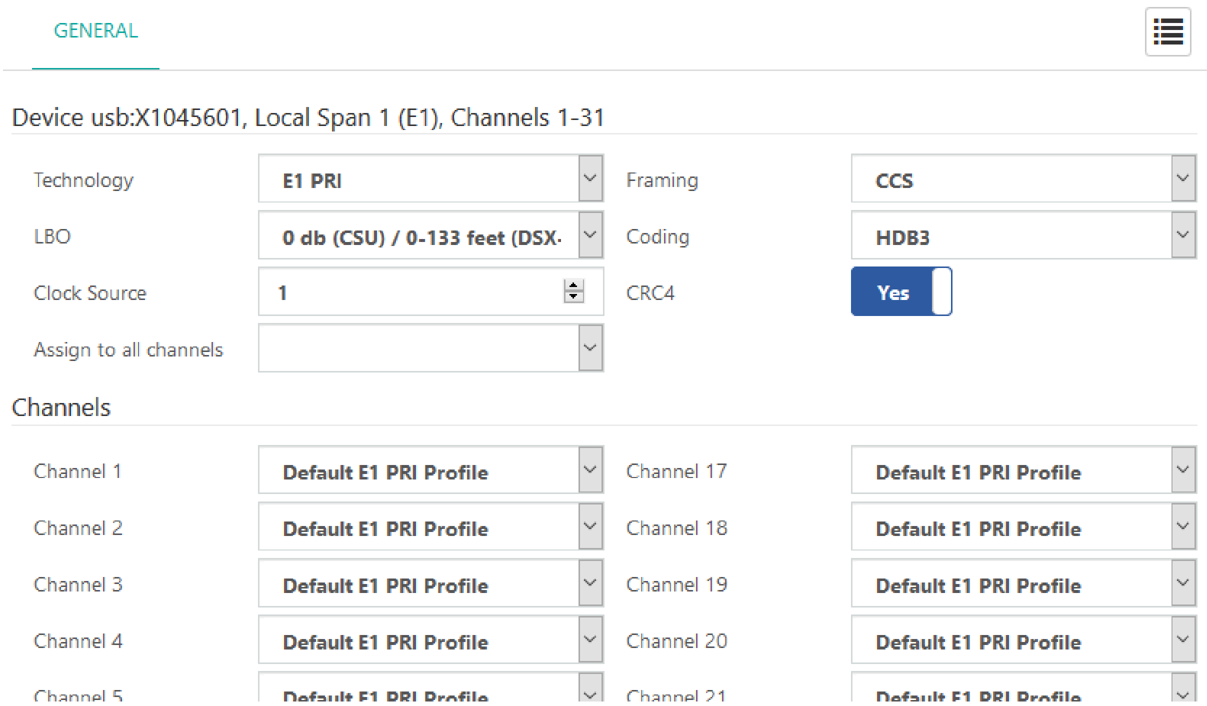
Profile Assignments Dialog

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

The list of profiles is automatically populated by clicking **Detect Hardware** in the Settings > Telephony > Interfaces dialog. A profile is automatically created for each span that is detected.

GENERAL Tab

E1 or T1



In the above example you can see the channels that are assigned as E1 trunks. You can use this dialog to configure these channels.

Technology, indicates the technology of the span.

LBO, shows the distance from the telephone company (telco) drop to the span.

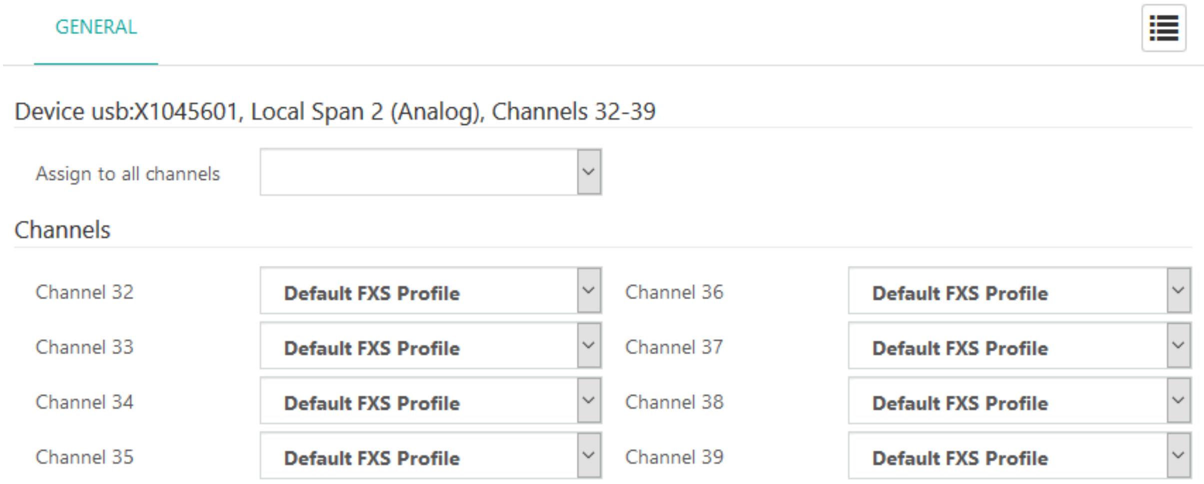
Clock Source, determines the clock source priority for the span. Highest priority is 1: larger numbers indicate lower priority. Set to zero, or leave blank, if you do not want to use this span as a clock source.

Framing, determines the framing option for the span. Can be CCS or CAS for E1, or ESF or D4 for T1.

Coding, the coding options for the span

CRC4, toggles CRC4 for the span

Analog



Assign to all channels, allows you to assign a profile, such as FXS or FXO, to ***all*** channels in the span. Alternatively, you can assign profiles to each individual channel by selecting a profile from the available drop-down list.

End Point Manager Menu Group

The Endpoint Manager allows you to centrally manage the configuration settings for all IP devices that can be accessed on the network.

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.

Note that CompletePBX uses http (and not tftp) protocol to manage the configuration of endpoint devices. However, some older Cisco phones still require the tftp protocol – see here for further detail.

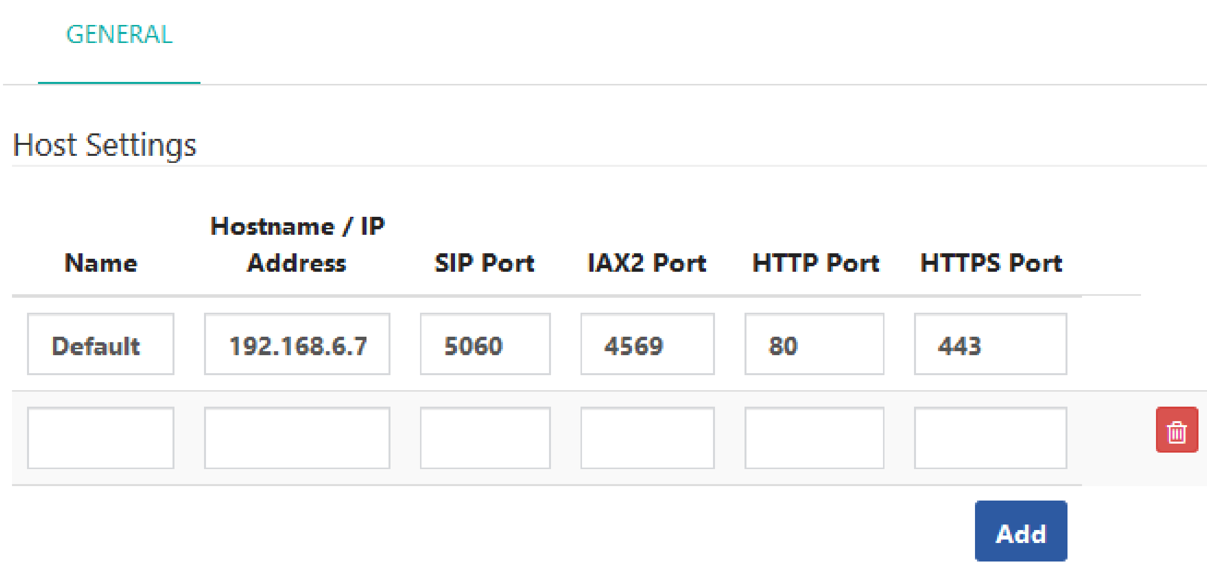
There are a small number of simple tasks that you will need to complete in order to make the Endpoint Manager fully operational:

1. 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.
2. 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
3. Create a Template for each group of phone models that you want to manage, and link each template 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.
4. 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.
5. Link each device that you want to manage to a template and to one (or more) PBX extensions

Host Settings Dialog

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.

GENERAL Tab

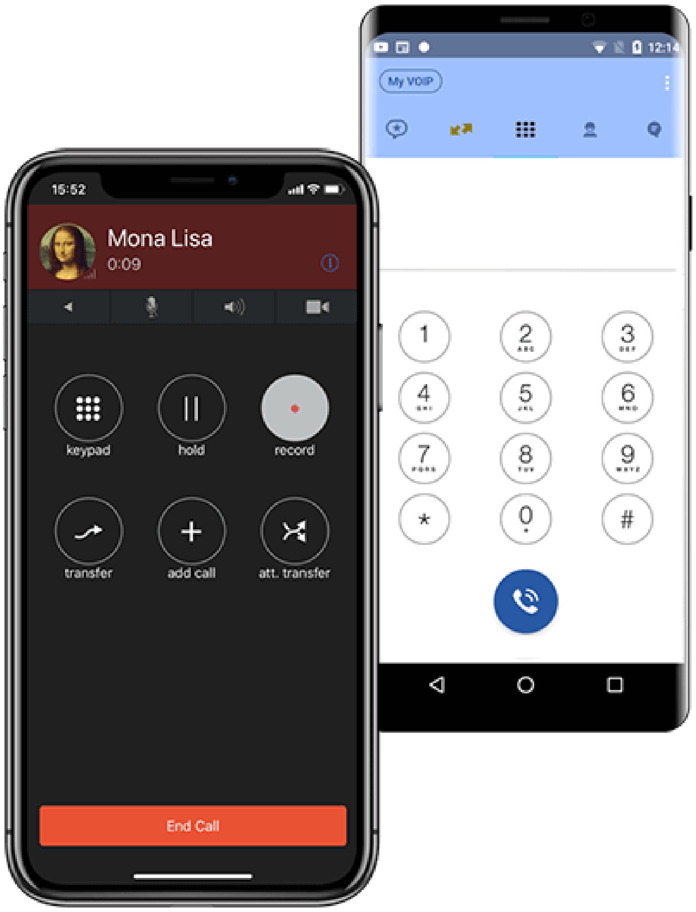


Host Settings Section

- **Name,** helps to simplify maintenance: each host setting should be identified with a unique label.
- **Hostname / IP Address,** 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.

Cloud Phone Dialog

(Refer to Activating the Xorcom CloudPhone for details of the procedure to activate the CloudPhone option on your CompletePBX 5 system.)

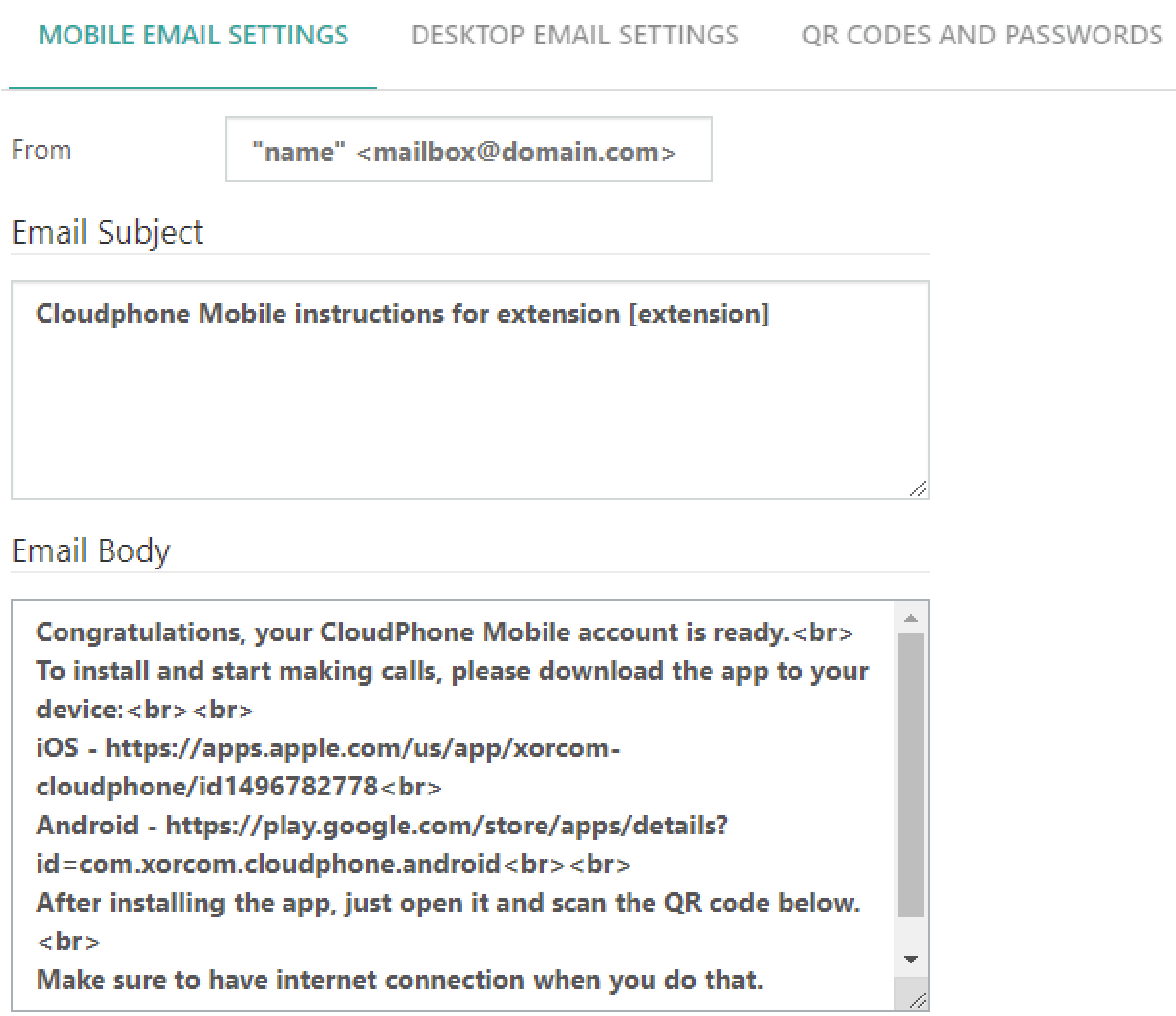


Configure the host addresses that will be used to communicate with the Xorcom CloudPhone.

MOBILE EMAIL SETTINGS Tab

Configure the contents of the email message that will be sent to users to advise them of access to the Xorcom Mobile CloudPhone.

Make sure that you fill in the correct details for the **From** field.



From, enter the email address that should appear as the send of these emails.

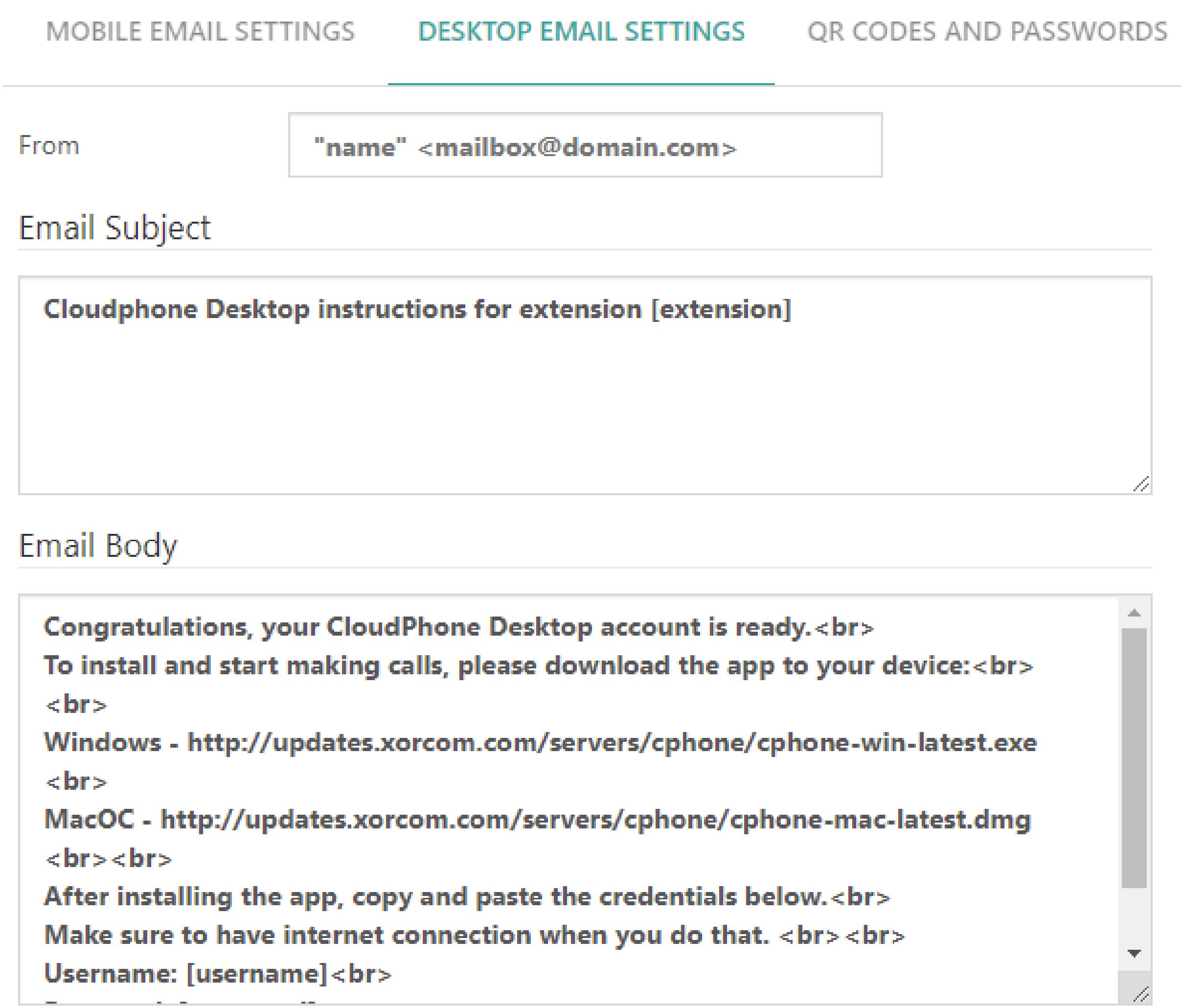
Email Subject, this is a free-text field that determines the subject line in the email that CloudPhone users will receive

Email Body, this is a free-text field that determines the contents in the body of the email that CloudPhone users will receive. If you make changes, be careful not to change the links to the Apple App Store or Google Play.

DESKTOP EMAIL SETTINGS Tab

Configure the contents of the email message that will be sent to users to advise them of access to the Xorcom Desktop CloudPhone.

Make sure that you fill in the correct details for the **From** field.



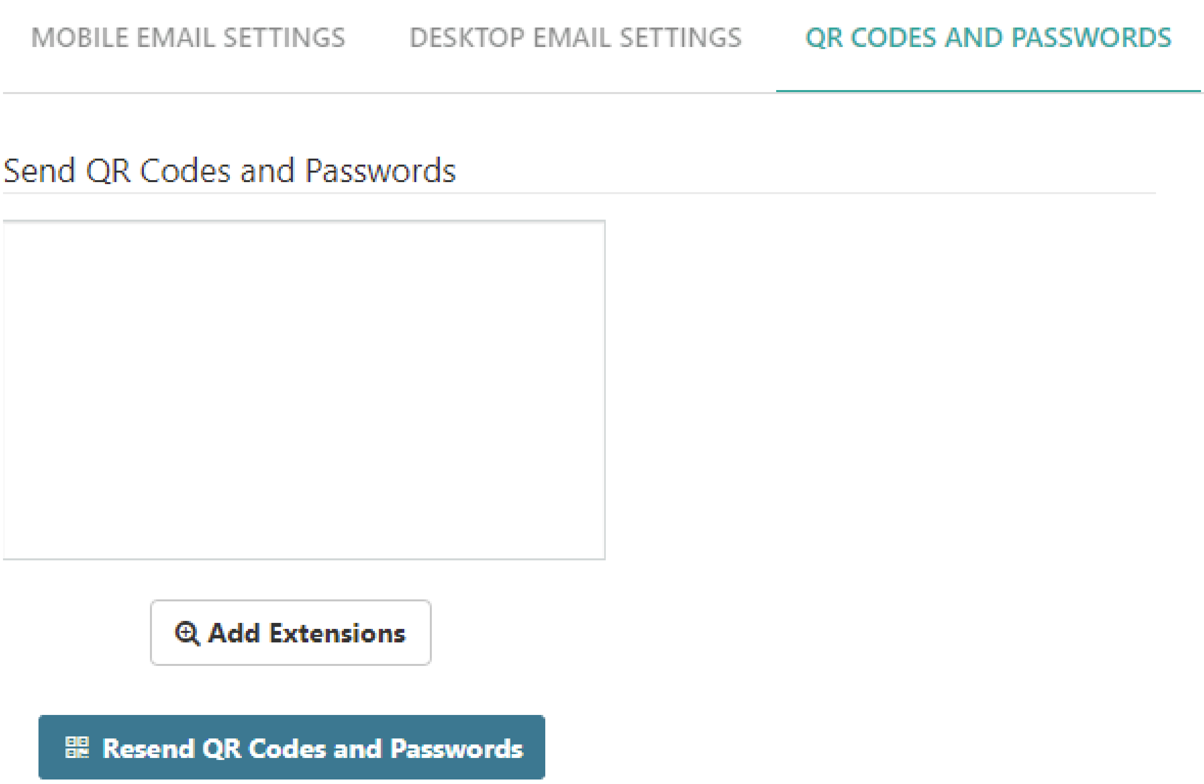
From, enter the email address that should appear as the send of these emails.

Email Subject, this is a free-text field that determines the subject line in the email that CloudPhone users will receive

Email Body, this is a free-text field that determines the contents in the body of the email that CloudPhone users will receive. If you make changes, be careful not to change the links to the download locations..

QR CODES AND PASSWORDS Tab

This dialog allows you to configure the extensions that can access the Xorcom CloudPhone, and send them an email (including a QR code) advising them how to install and activate the Xorcom CloudPhone

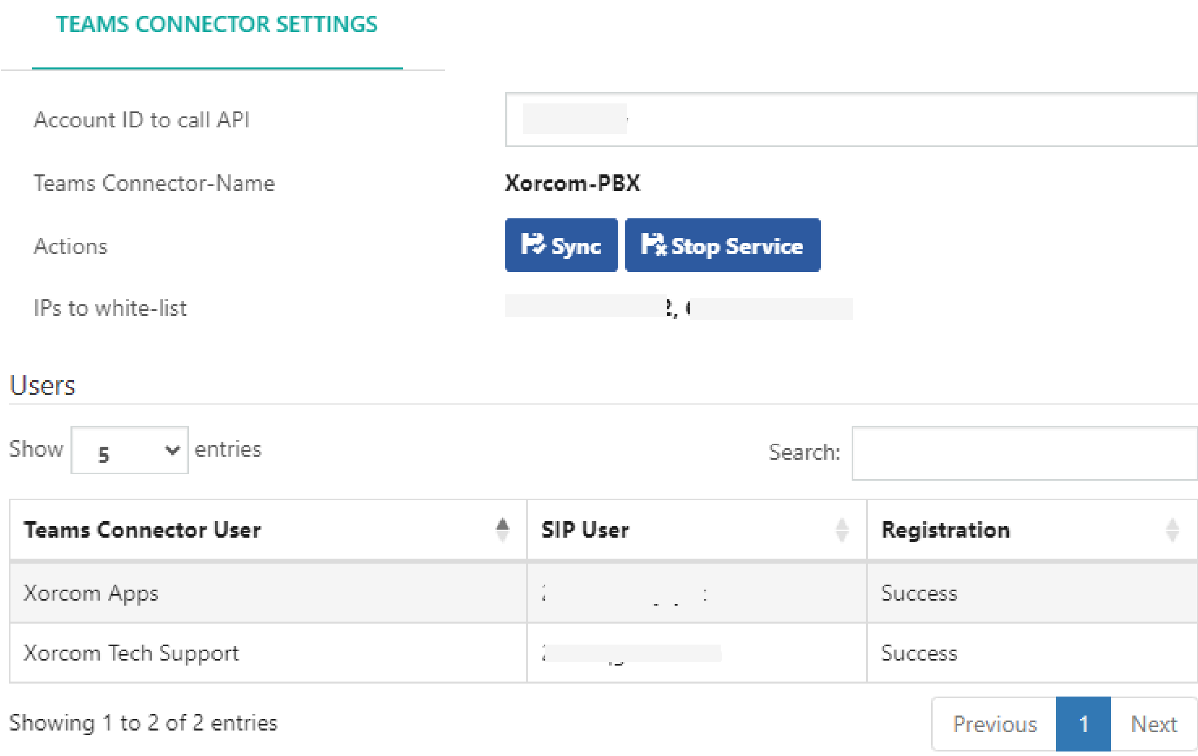


Add Extensions, allows you to select extensions (from the list of available extensions) to which you want to send QR codes and passwords.

Resend QR Codes and Passwords, send (or resend) an email with QR codes to the extensions to which you have given access to the Xorcom CloudPhone.

Teams Connector Dialog

This dialog allows the MS Teams user with the appropriate telephony licenses to connect his/her MS Teams user as a device in CompletePBX, associated with an extension in the system. This allows the MS Team user to make and receive calls via CompletePBX, be a queue agent, a destination for IVR calls, make and receive internal calls, and benefit from all of CompletePBX features and call routing capabilities.



Account ID to call API, the MS account needs to be connected to the CompletePBX system and the relevant MS users associated with specific extensions.

Teams Connector-Name, name of the MS Teams account.

Actions, allow you to choose between two options: **Sync**, press this button to connect the PBX to Teams Connector. **Stop Service**, press this button to stop the synchronization between the PBX and Teams Connector. **NOTE** that in post-paid licenses it is mandatory to delete the Teams Connector devices (under Extensions) in order to avoid being charged for the service.

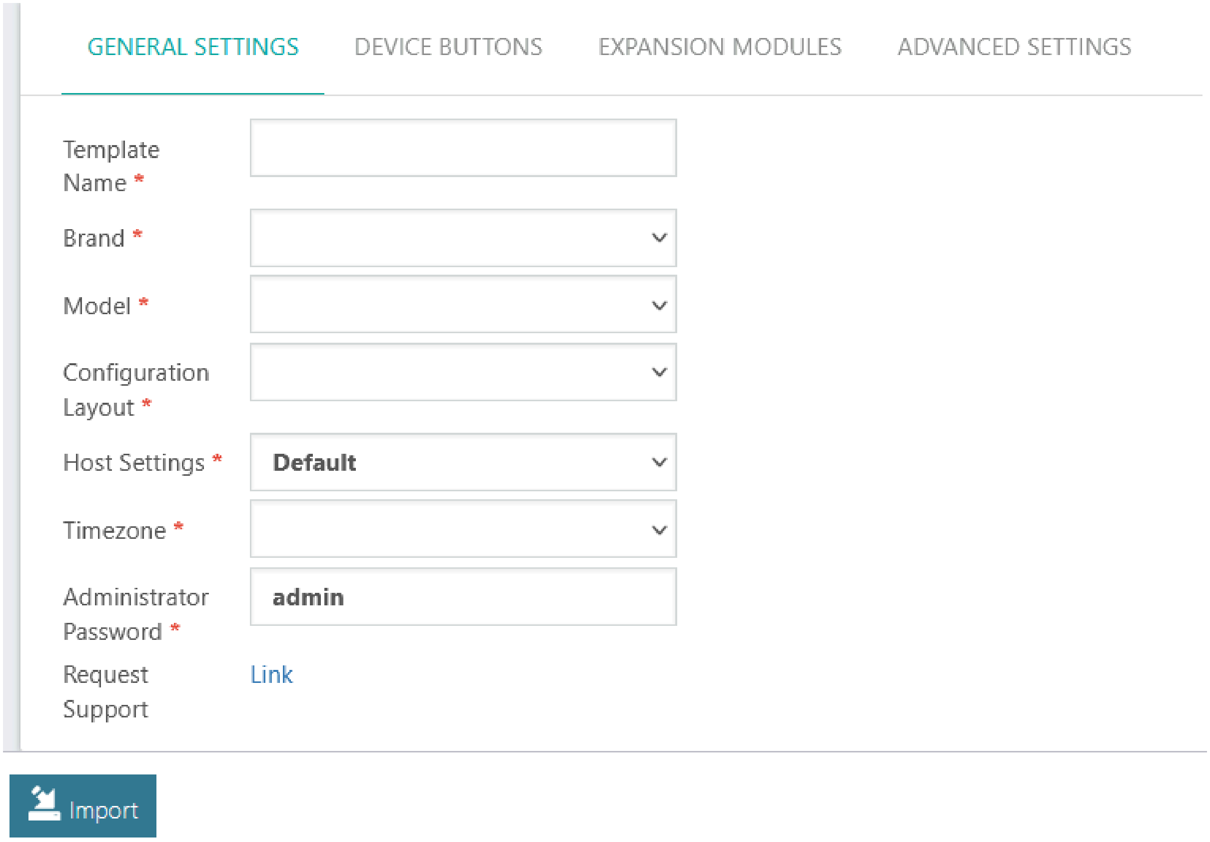
IPs to white-list, Session Border Controller (SBC) IPs from Teams Connector.

Templates Dialog

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.

GENERAL SETTINGS Tab

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, helps to simplify maintenance: each template should be identified with a unique name.

Brand, select a Brand from the drop-down list of brands that are supported by Endpoint Manager. If you require a brand that does appear in the drop-down list, you can contact support, by pressing on the Add new model support menu (on the right-hand side of the dialog).

Various models from the following brands are supported:

- Aastra
- Cisco (see note below)
- D-Link
- Escene
- Fanvil
- Gigaset
- GrandStream
- Htek
- Hanlong
- Polycom
- Snom
- Vtech
- Xorcom

- Xorcom UC Series
- Yealink

Cisco phones only:

Due to the fact that some Cisco phones (such as 7942 and 7975 models) do not support the HTTP protocol, it is necessary to install a TFTP/HTTP proxy server on the PBX, by using the command **`yum install tftp-http-proxy`.** You can verify that the proxy service is active by using the command **`systemctl status tftp-http-proxy`.** A green "active" status indicates that the service is running.

It is also necessary to open the firewall for the TFTP service in the Rules tab of the Admin > Security > Firewall dialog. You can validate that the tftp-http-proxy is listening on UDP port 69 by running the command **`ss -lnup | grep :69`**

Model, select a Model from the drop-down list of models that are supported by Endpoint Manager. If you require a model that does appear in the drop-down list**,** you can contact support**,** by pressing on the Add new model support menu (on the right-hand side of the dialog).

Configuration Layout, 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.

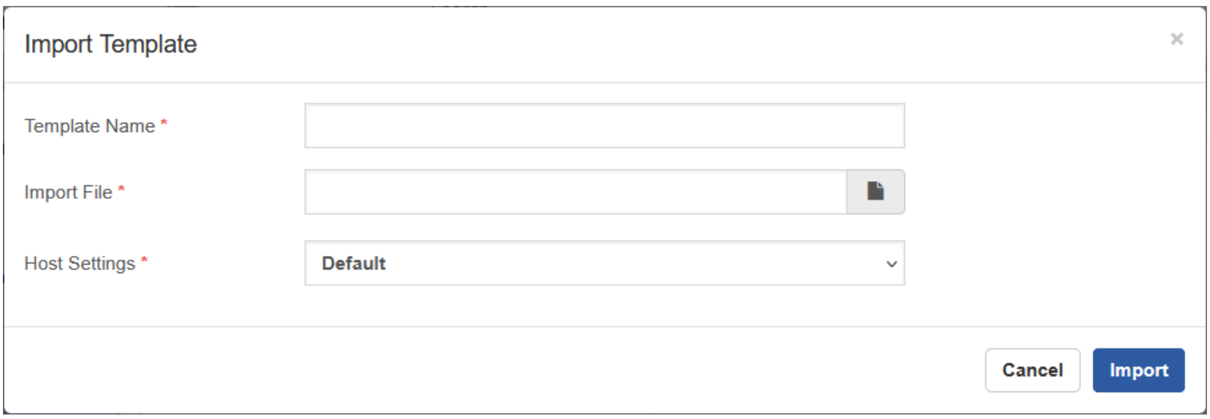
Host Settings, allows you to select the name of the Host Settings (described above) that you want to use in this template.

Time zone, allows you to select the time zone offset to be used by all phones that use this template.

Administrator Password, 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.

Request Support, click on **Link** to request support for additional brands or models.

Import, press this button to create a new template based on the imported file.



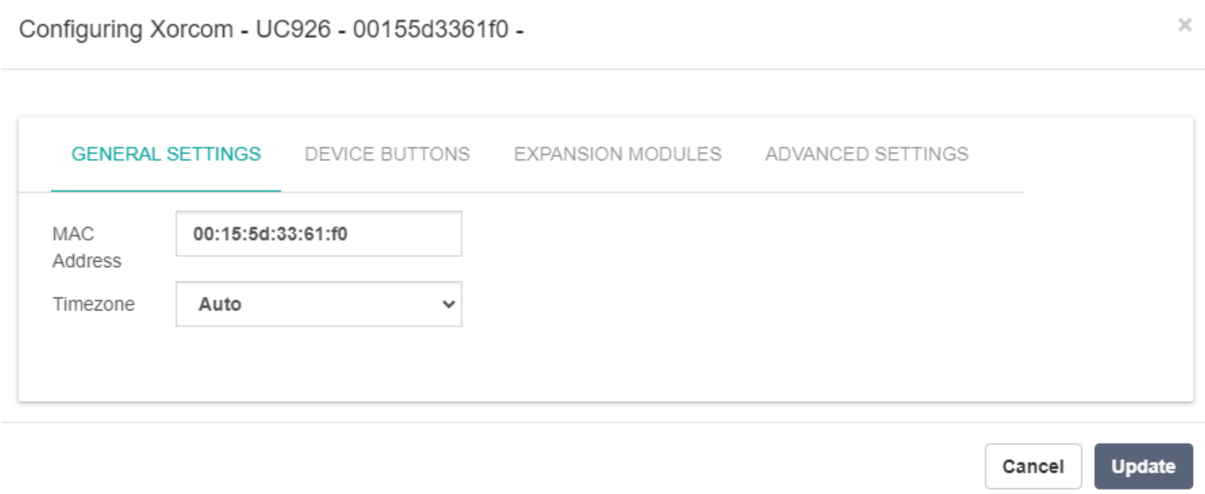
Template Name *, a free-text name, to simplify maintenance, each template should be identified with a unique name.

Import File *, allow to upload an exported template file.

Host Settings *, select the name of the Host Settings that you want to use in this template.

NOTE that when creating the new template it has to be assigned a unique name on the system.

After importing or creating a new template, you can select the template to export or duplicate



Export, press this button to save the changes from the default template to a file that can be imported to another CompletePBX system.

NOTE that the exported file is not meant to be changed manually. Make all changes in the original template before exporting.

Duplicate, press this button to creates an identical template on the same machine.

DEVICE BUTTONS Tab

Allows you to configure the DSS (direct station select) buttons for IP phones that use this template.

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

EXPANSION MODULES Tab

Allows you to configure the DSS (direct station select) buttons on the expansion dialog for IP phones that have this hardware and use this template.

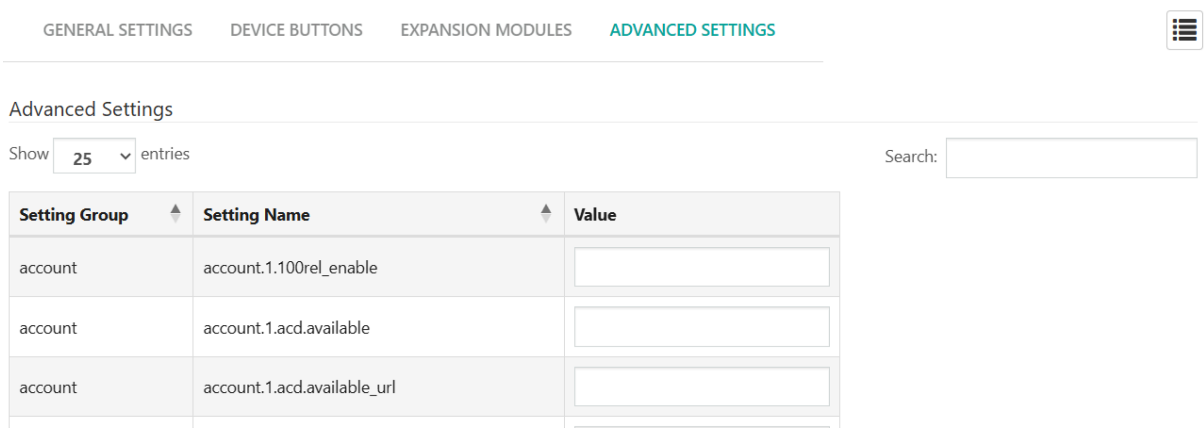
Note that each user can use My Extensions to define settings and overwrite the template definitions. This is a useful feature to allow users to personalize some buttons on their phone.

The number of buttons that are displayed are specific to each expansion dialog.

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.

ADVANCED SETTINGS Tab

Advanced Settings allows you to manage the configuration file for phones that belong to this template.

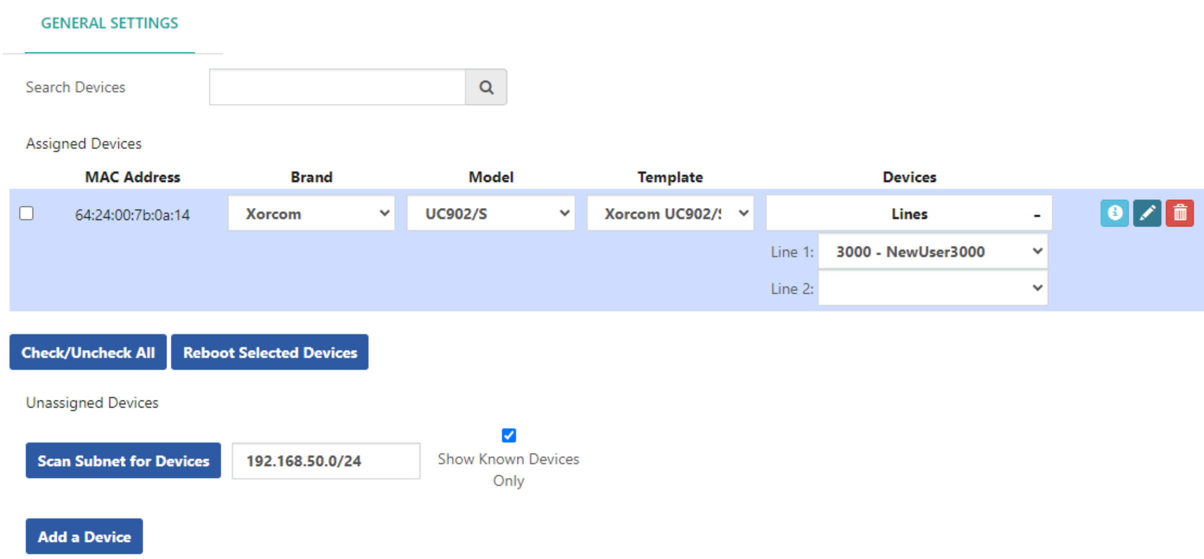


Advanced Settings provides access to parameters that are not directly managed by the Endpoint Manager. Codec settings would be an example of such a parameter. Manufacturers' default values, where applicable, are already defined in the file. You would only need to modify values in the configuration file if you want to define some non-standard behavior.

Device Mapping Dialog

GENERAL SETTINGS Tab

This dialog manages your devices. The devices that you want to manage can be automatically discovered.



Search Devices, enables you to find a specific (SIP or IAX2) device, or group of devices, that exist in the list of known devices. You can enter a device number, such as 2244 to see a specific device, or you can enter just 22 to see all the devices that start with 22.

Assigned Devices, shows all the devices that are currently known in the system.

Check/Uncheck All, allows you to easily select, or deselect, all assigned devices.

Reboot Selected Devices, allows you to selectively reboot devices. Use the Search Devices option to collect a list of candidates, and then check the check box at the left-hand end of each row of data.

Scan Network for Devices, type in a target network segment and mask**,** such as 192.168.25.0./24**,** and press on Scan subnet for devices.

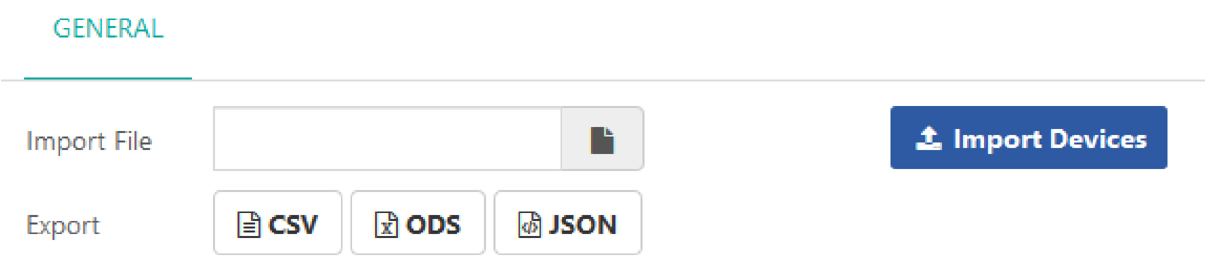
The auto discovery will take some time**,** depending on the number of addresses that can potentially exist on the subnet. Be careful not to use a mask that is too big**,** as this will impact the time required to complete the discovery process. If devices cannot be discovered by scanning the network**,** you can manually enter the MAC address of any phones that you want to manage.

Show Known Devices Only, when this is checked on, any devices having a MAC address that is not defined in the Endpoint Manager database as an endpoint device will be filtered out and not displayed.

Add a Device, allows you to manually add a device that was not discovered by the scan process.

Import/Export Devices Dialog

This dialog works like all the other import/export dialogs in CompletePBX, and allows you to import IP Phones to Device Mapping based on their MAC addresses. You can use this dialog, for example, to remove devices, change the templates for devices, or reassign a device to a different extension.



Import File, select the file that you want to import, by clicking on the folder icon to search for the file in any of the allowed formats (csv, ods, or json.) After selecting the import file, click of the **Import Devices** button to load the information into CompletePBX 5. A log file will be displayed showing the status of the import, like this:

Each line of the log file will begin with the status of the item, e.g. Info, Error, etc. In the case of an error, the message will indicate the source of the error.

Export, click any of the format icons to export the endpoints in the appropriate format. The file, named device_mapping.<ext> will be exported to your default download directory. Available formats are:

- CSV
- ODS
- JSON

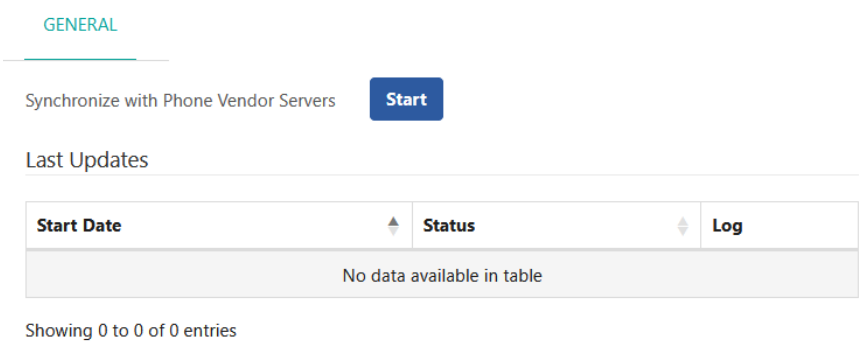
Zero Touch Dialog

This dialog allows for zero-touch configuration of new phones out of the box.

Various models from the following brands are supported:

- Poly
- Xorcom UC Series
- Yealink
- Fanvil
- Vtech
- Htek
- IP Connect

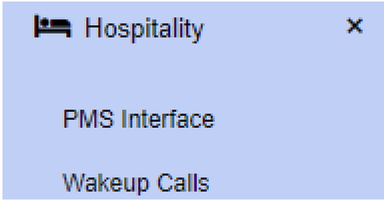
GENERAL Tab



Synchronize with Phone Vendor Servers, uploads the currently configured MAC addresses to the corresponding vendor's provisioning servers.

Start, press this button to synchronize your setup with the zero-touch server.

Hospitality Menu Group



The Hospitality PMS Interface dialog interfaces with a Property Management System (PMS) to manage smooth check-in/check-out processing, room status reporting, minibar status, and control of wakeup calls.

Hotels have special requirements for their telephone systems. For example, they need to have separate call accounting for the guests as opposed to administration staff, they need flexible internal caller IDs, and telephone lines must be closed/opened on demand.

The Xorcom Hospitality module interfaces with a wide variety of Property Management Systems, such as Micros Fidelio, Micros Opera, Micros Opera Suite, Protel Hotel Systems, Amadeus Hospitality, Brilliant, Silverbyte/Optima, Newhotel, and all other Property Management Systems that support FIAS (Fidelio Interface Application Specification).

If you want to add the Hospitality Menu Group to your system, you will need to install the module. To do this, enter the Linux command line interface, and type:

```
For CentOS-based systems:
yum install complete-concierge

For Debian-based systems:
apt install complete-concierge
```

The Hospitality Menu Group will be displayed the next time you log into your CompletePBX 5 system.

For testing purposes, all functionality of this module can be evaluated for a small number of rooms. However, a Xorcom license is required in order to manage more than five rooms.

The Hospitality module manages guest extensions in the following manner:

- Check-in
    - Caller ID of the extension will be set to the format “<room_number><guest_name>”.
    - Permissions will be set for the extension in accordance with the settings configured in the PMS.
    - The language of the extension will be set.
- Check-out
    - Caller ID of the extension will be set to format “<room_number> Vacant”.
    - The extension will be restricted from making external calls.

  - Voice mails for the extension will be deleted.
  - The language of the extension will be reset to English.
  - The “Do Not Disturb” (DND) option for the extension will be reset.

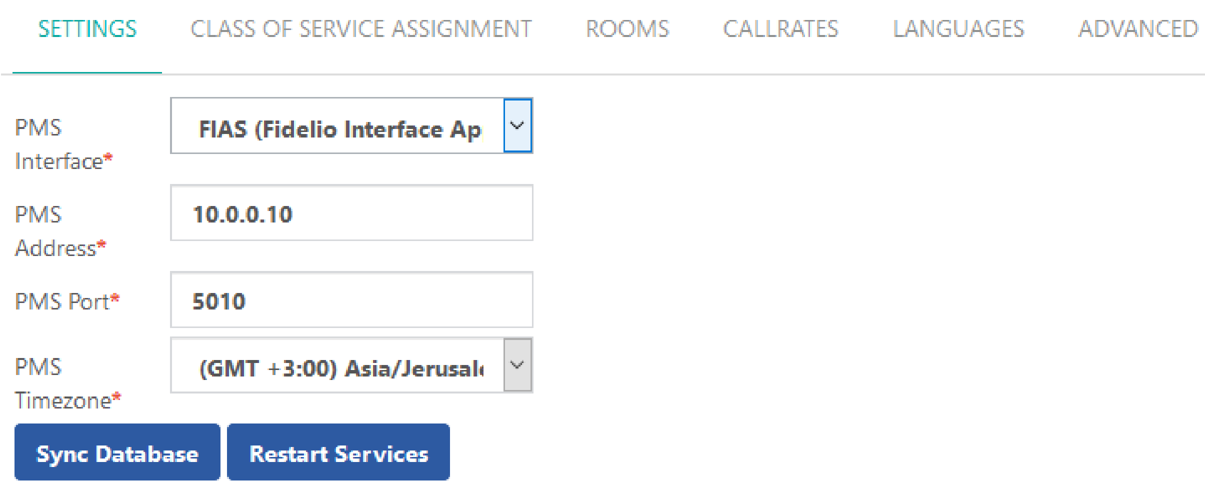
- Room Changes (when a guest changes rooms)
  - The extension of the guest’s old room will be configured as if the guest had checked-out (as detailed under the Check-out bullet above.)
  - The check-in data for the guest will be transferred to the extension in the guest’s new room.
  - In addition to check-in data, the following will also be transferred to the new room’s extension:
    - Voicemail messages
    - Ordered wake-up calls
    - “Do Not Disturb” status
  - **Note:** In cases where the room being vacated or the new room includes **more than one extension** (i.e., multiple extension numbers, not multiple devices on a single extension), the transfer of voicemail messages and related data is **not supported**. In such cases, all voicemail and related data will be deleted for privacy reasons.
- Wakeup Calls
  - Wakeup calls can be managed either by using the PMS, or directly by the guest (by dialing the ***34** feature code.)
  - The Hospitality module will send the PMS the result of the wakeup attempt as either WAOK (wakeup ok) or WANR (wakeup not reachable.)
- Do Not Disturb (DND)
  - The guest can manage their DND status, by dialing the ***66** feature code. (Incoming calls will be treated as follows when DND is enabled: if Voicemail is enabled, the call will be sent to voicemail; otherwise the caller will receive the busy tone.)
- Class of Service
  - Extensions can be configured to allow and combination of internal, local, national or international calls, by applying a Class of Service.
- Call Accounting
  - Call charges will be transmitted automatically to the PMS account for the guest.
  - Call rates can be easily managed from the Callrates tab of the PMS Interface dialog.
- Room Maid System / Room Status
  - Room Status can be changed by dialing feature code **22** from the room telephone. The following statuses may be defined:
    - 1 Dirty / occupied
    - 2 Dirty / vacant
    - 3 Clean / occupied
    - 5 Clean / vacant
    - 6 Inspected / vacant
- Minibar Status
  - Minibar Status can be changed by dialing feature code **23** from the room telephone.

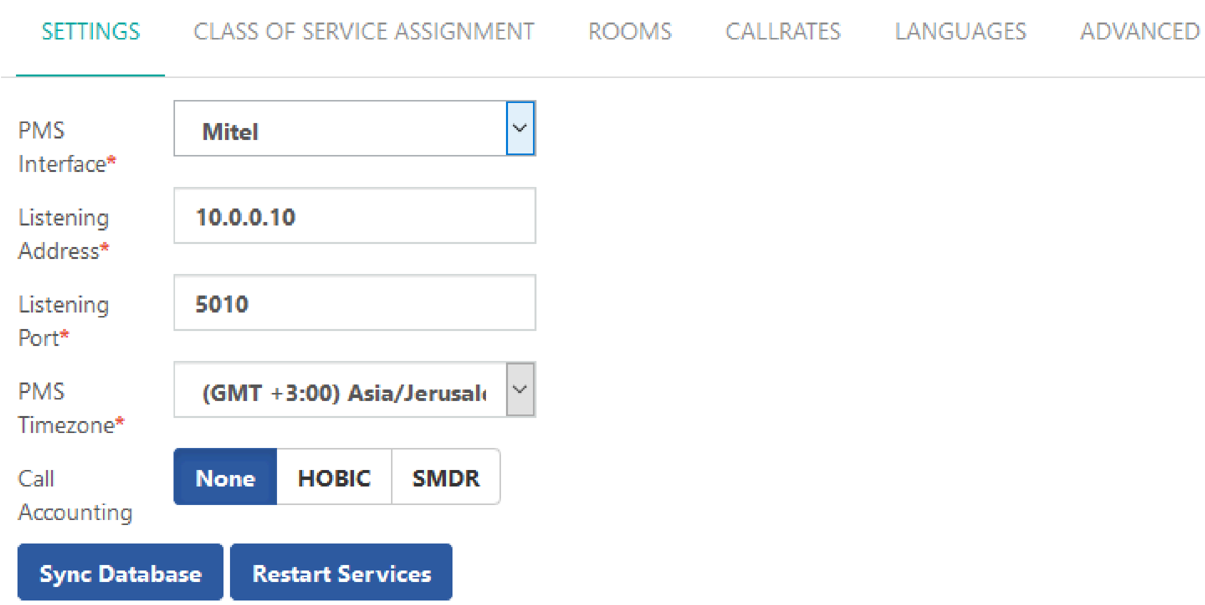
- Database Resync
    - Database resynchronization from CompletePBX 5 to the Property Management System.
- Message Handling
    - This is performed by copying a pre-recorded message into the voice mail folder of the extension.
- Automatic Resync
    - Automatic resynchronization to PBX or Micros PMS if connection to either was established. Data will be buffered and executed after reconnecting.

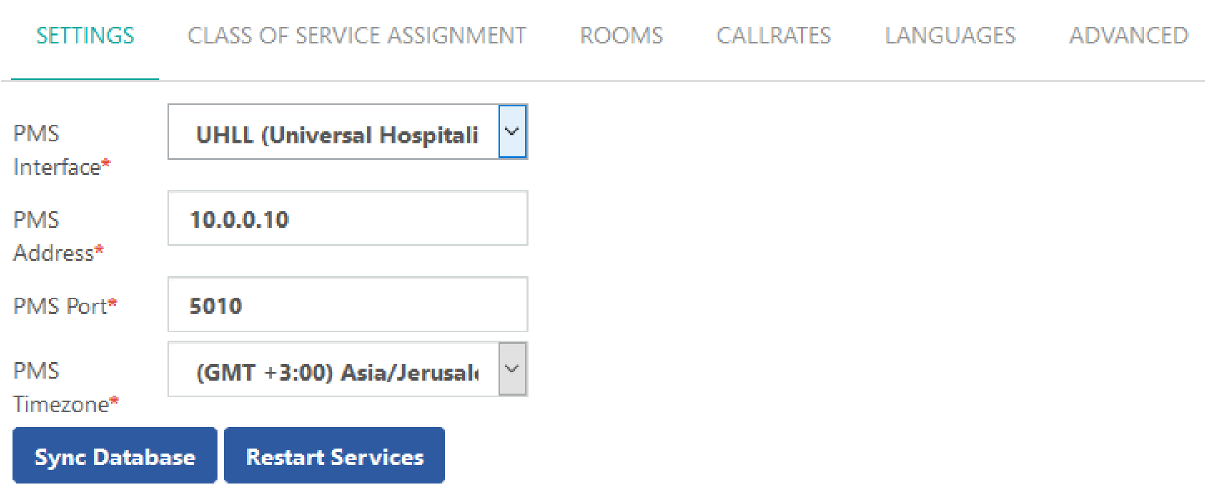
PMS Interface Dialog

SETTINGS Tab

The fields displayed in Settings tab vary slightly, depending on the PMS Interface that is selected.







PMS Interface*, select from the dropdown the communication protocol between CompletePBX 5 and the Property Management System. Available options are:

- FIAS (Fidelio Interface Application Specification)
- Mitel
- UHLL (Universal Hospitality Language Layer)
- AHL (Alcatel Hotel Link)
- FCUI (Fidelio Cruise Universal Interface)

PMS Address*, for FIAS and UHLL systems, this is the hostname (or IP address) of the Property Management System.

Listening Address*, (Mitel systems only), indicates the address that CompletePBX 5 uses to listen for incoming connections (typically 0.0.0.0)

PMS Port*, for FIAS and UHLL systems, this is the port used by the Property Management System.

Listening Port*, (Mitel systems only), indicates the port on which CompletePBX 5 listens for incoming connections.

PMS Timezone, the time zone used by the Property Management System. By default, this is set to the time zone that is configured for CompletePBX 5.

Call Accounting, (Mitel systems only), allows you select which call accounting system to use:

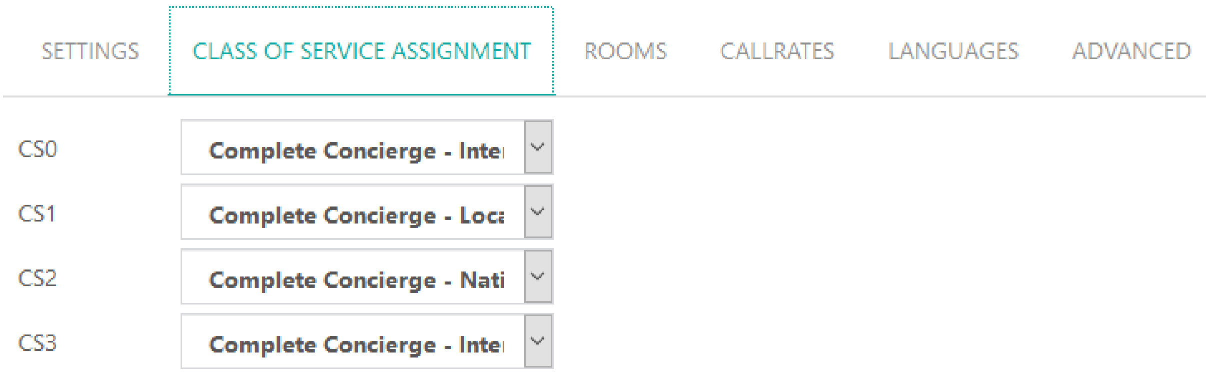
- **None**
- **HOBIC** - Hotel Billing Information Center
- **SMDR** - Station Message Detail Recording

Sync Database, synchronize CompletePBX 5 with the Property Management System.

Restart Services, restarts all the PMS interface services.

CLASS OF SERVICE ASSIGNMENT Tab

This tab allows you to configure four Classes of Service (that exist in CompletePBX 5) and make them available to the Property Management System.



CS0, CS1, CS2, CS3, use the dropdown list to assign any existing CompletePBX 5 Class of Service to a class of service in the Property Management System.

The system is pre-configured with a set of Class of Service assignments, cc_internal, cc_international, cc_local, and cc_national. You can modify the factory-configured classes in the Class of Service dialog, or create new classes, and use them in this dialog.

The factory-defined Classes of Service are each linked to a factory-defined Route Selection. Make sure that you use the Route Selection dialog to assign each Hospitality-related Route Selection (CC - National, CC - Local, CC - International, and CC - Internal) to an appropriate Outbound Route.

ROOMS Tab

Property Management Systems identifies the room number, and not the extension number, so it is necessary to link extensions to rooms.

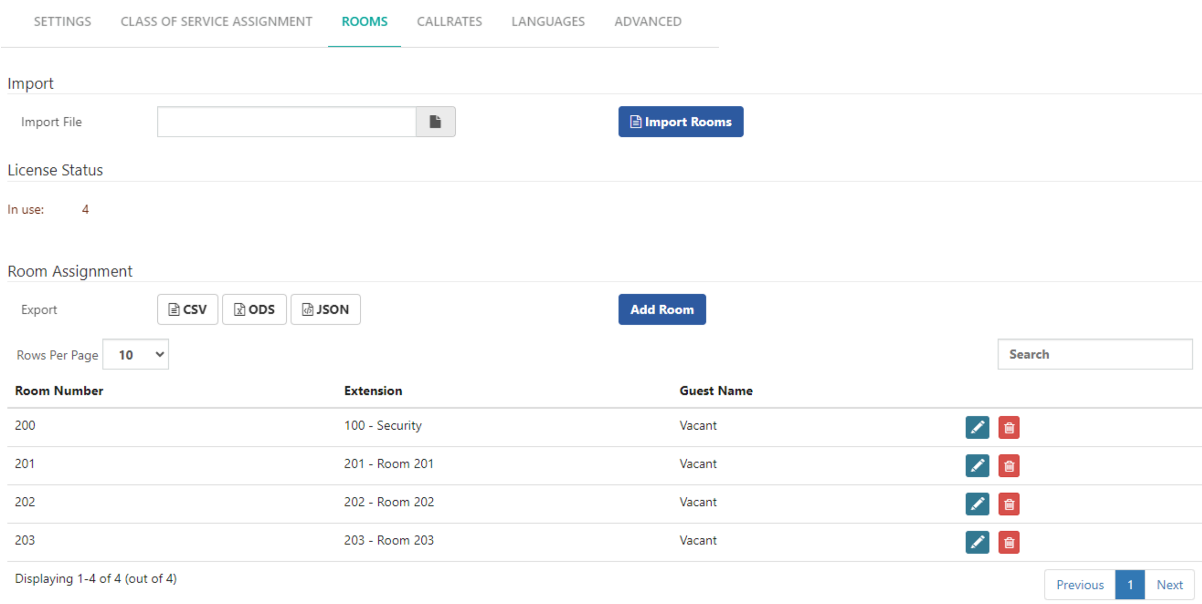
This can be done manually by pressing the **Add Room** button, or in batch mode by importing a CSV file. The CSV file contains two columns of data: the first column is the room number, and the second column is the extension number that should be linked to the room.

Multiple extensions can be configured for each room, each with a different extension number.

In hotels that require multiple extensions in a room but do not require different extension numbers for each device, you can create a single extension with multiple devices.

Note that when configuring wakeup calls and other features, they will be applied to ***all*** extensions that belong to the room.

Note that hotel PMS interface supports User ID, allowing the person reporting the room status to identify using their PMS code when dialing in the room status.



Import Section

CSV File, use the folder icon to search for, and select, the CSV file that contains data that links CompletePBX 5 extensions to room numbers.

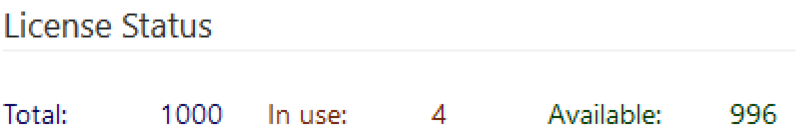
Import CSV, after you have selected a CSV file, click on this button to load data from the CSV file.

Importing a CSV will overwrite ***all*** existing room assignments.

Export CSV, exports a list of existing room assignments. A quick and easy way to make bulk modifications is to export existing data, edit the exported file, and then import it.

License Status Section

This section shows the total number of rooms that are licensed in the system, the number of rooms that have been configured, and the number of additional rooms that can still be configured.



Rooms Assignment Section

This table links room numbers and extensions. You can use the (Edit) icon to modify data in a row, or the (Delete) icon to remove a row of data.

Export, click any icon to export a list of rooms in the appropriate format. Available formats are:

- CSV
- ODS
- JSON

Rows Per Page, allows you to determine how many rows (between 10 and 100) of data should be displayed.

Room Number, the room number that is being assigned.

Extension, the CompletePBX 5 extension that is assigned to the room.

Guest Name, name of the guest assigned to the room, as configured in PBX > Extensions > Extencsion, Advances Tab, Directory Section, Alias.

Add Room, this button allows you to manually add additional room assignments.

CALLRATES Tab

Allows you to configure call rates for outbound calls. This can be done in bulk mode by importing data from a CSV files, or manually by clicking on the **Add Callrate** button at the bottom of the dialog.

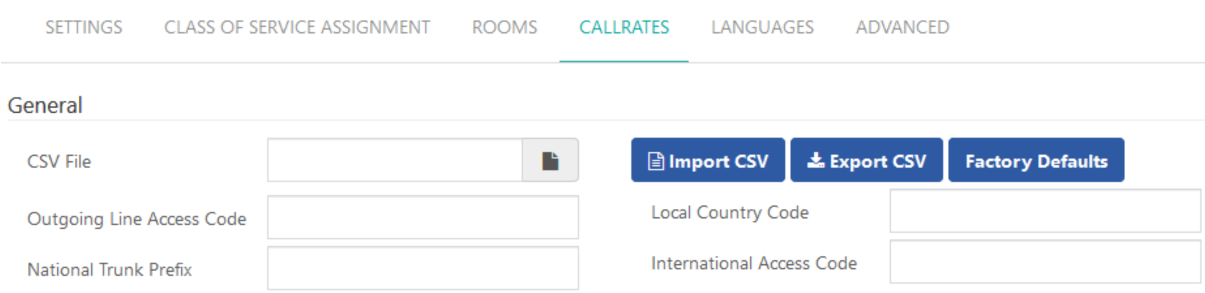
Before looking for a callrate in the table, the Hospitality module converts the dialed number according as follows:

- Removes the leading digit/s defined in the Outgoing Line Access Code field in this dialog from the beginning of the called number. Many PBX systems are configured in such a way that the users have to dial an access code before dialing an external phone number.
- If the length of the called number is 7 digits then the call will be considered as a local call, and the callrate for the dummy country code 7777777 will be used.
- If the length of the called number is greater than 7 digits and does not begin with the digits defined in the International Access Code field of this dialog, then the system will remove the digits defined in the National Trunk Prefix field of this dialog.
- If the length of the called number is less than 12 digits, then the system will add the digit/s defined in Local Country Code field of this dialog at the beginning of the dialed number.
- Once the above actions have been performed, the system will try to find a suitable tariff.

Assuming that the system is located in Frankfurt, Germany, and **Outgoing Line Access Code** is defined as **9**, **National Trunk Prefix** is defined as **0**, **Local Country Code** is defined as **49**, and **International Access Code** is defined as **00**, then the table below demonstrates the steps that will be performed by the system before looking for a callrate:

Call Type	Dialed Number	Step #1	Step #2	Step #3	Callrate
Local call (within Frankfurt area)	97823678	7823678 Remove 9 (Outgoing Line Access Code)			Use callrate for 7777777
National call to Berlin (within Germany)	90305291234	0305291234 Remove 9 (Outgoing Line Access Code)	305291234 Remove 0 (National Trunk Prefix)	49305291234 Add 49 (Local Country Code)	Use callrate for 49
International call (to England)	90044208345678	0044208345678 Remove 9 (Outgoing Line Access Code)	44208345678 Remove 00 (International Access Code)		Use callrate for 44

General Section



CSV File, use the folder icon to search for, and select, the CSV file that contains call rate data.

Outgoing Line Access Code, the digit that should be dialed to make external calls.

National Trunk Prefix, the prefix that must be dialed to make national calls in the country where CompletePBX 5 is installed. In most countries this will be **0**, but **1** is used in the USA.

Import CSV, after you have selected a CSV file, click on this button to load data from the CSV file.

Export CSV, exports a list of existing call rates. A quick and easy way to make bulk modifications is to export existing data, edit the exported file, and then import it.

Factory Defaults, click on this button to reset all call rates to factory default values.

Local Country Code, the country code for the country where CompletePBX 5 is installed. For example, if the PBX is installed in Mexico, this field would contain **52**.

International Access Code, the number that should be dialed to make international calls. In many countries this is **00**; in the USA **011** is used.

Callrates Table Section

Callrates Table

Rows Per Page 10

Search

Description	Call Destination	Price / Interval	Interval	Surcharge	Flags
Afghanistan	93	1.00000	Minute	0.00000	I
Afghanistan - Mobile	9370	1.00000	Minute	0.00000	I
Afghanistan - Mobile	9379	1.00000	Minute	0.00000	I
Albania	355	1.00000	Minute	0.00000	I
Albania - Mobile	35538	1.00000	Minute	0.00000	I
Albania - Mobile	35568	1.00000	Minute	0.00000	I
Albania - Mobile	35569	1.00000	Minute	0.00000	I
Algeria	213	1.00000	Minute	0.00000	I
Algeria - Mobile	21361	1.00000	Minute	0.00000	I
Algeria - Mobile	2137	1.00000	Minute	0.00000	I

Displaying 1-10 of 2547 (out of 2547)

Previous 1 2 3 255 Next

Add Callrate

Rows Per Page, number of rows of data to be displayed.

Description*, free-text to identify the rate.

Call Destination*, code that is dialed to reach the destination.

Price/Interval*, the price to be charged for each interval. The charge is implemented at the ***beginning*** of each interval.

Interval, the interval to be charged. Select a valid value from the drop-down list:

- 1 second
- 10 seconds
- 30 seconds
- 1 minute.

Surcharge*, a fixed charge that is added to every call.

Flags, additional flags

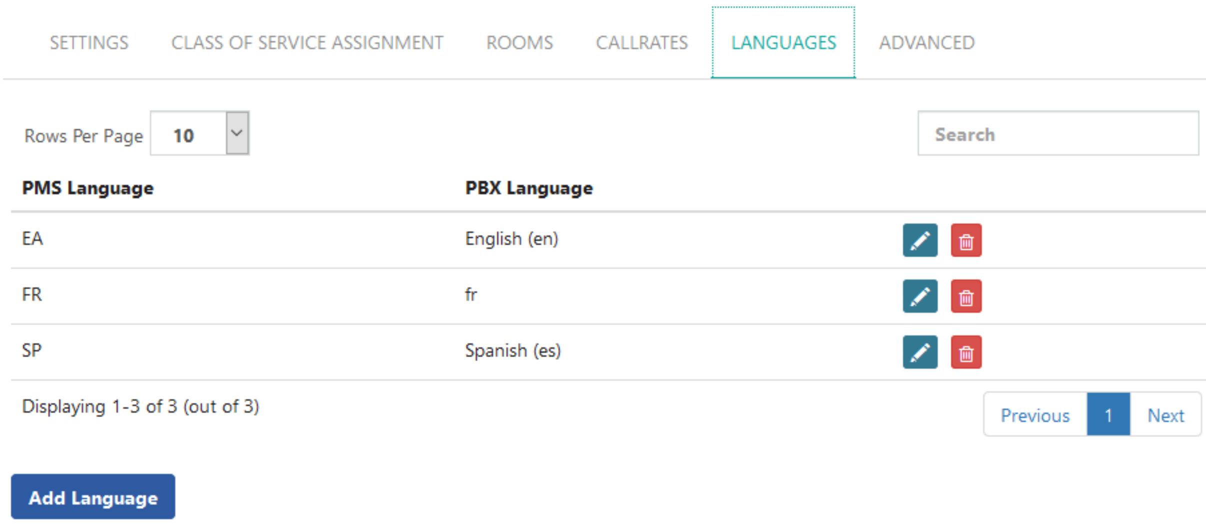
Add Callrate, this button allows you to manually add a row of Callrate data.

Use the (Edit) icon to modify existing data in a row, or the (Delete) icon to remove an existing row of data.

It is important to define a Callrate for local calls. As mentioned above, the dummy country code 7777777 is used for this purpose.

LANGUAGES Tab

This tab allows you to link Property Management System languages to CompletePBX 5 languages.



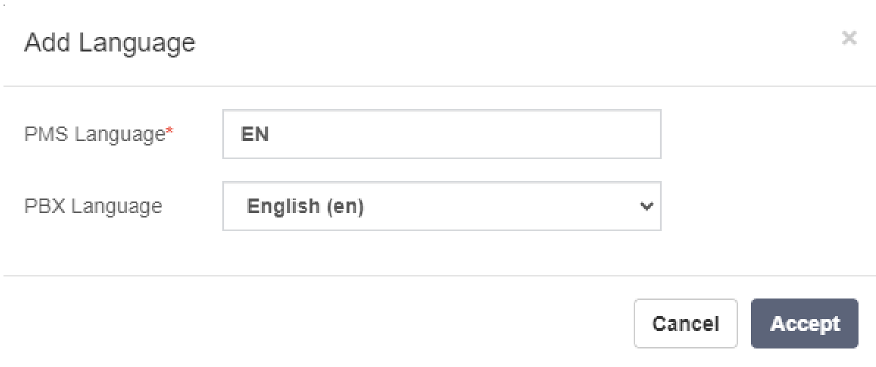
Rows Per Page, number of rows of data to be displayed.

PMS Language, any language that is supported by your Property Management System**,** e.g. EA (English), FR (French), SP (Spanish), etc.

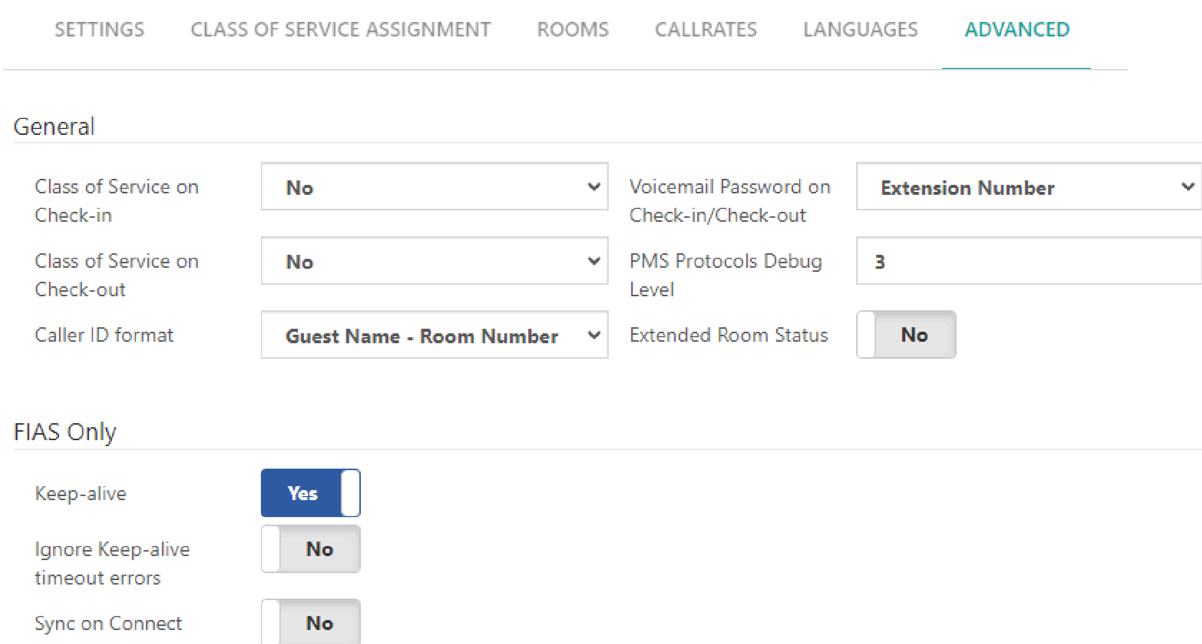
PBX Language, any language that is supported by CompletePBX 5. Select a language from the drop-down list**.**

Use the (Edit) icon to modify existing data in a row, or the (Delete) icon to remove an existing row of data.

Add Language, press this button to manually add another PMS/PBX language pairing.



ADVANCED Tab



General Section

Class of Service on Check-in, select a PMS class of service from drop-down list that will be automatically used when a guest is checked-in.

Class of Service on Check-out, select a PMS class of service from drop-down list that will be automatically used when a guest is checked-out.

Caller ID format, select format to use for occupied room extensions between Guest Name - Room Number and Room Number - Guest Name .

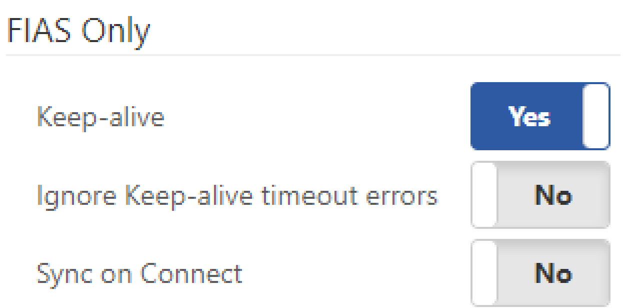
Voicemail Password on Check-in/Check-out, allows you to configure the default style of the password when a guest is checked-in, or when a room is vacated. The default value can be either:

- **Empty** – leave the password field empty. The guest will not be prompted for a password when accessing voicemail.
- **Extension Number** – set the password to use the extension number.

PMS Protocols Debug Level, debug level to be used by Property Management System. The default value is **3**.

Extended Room Status, toggle to include the employee number in room status notifications.

FIAS Only Section



Keep-alive, send keep-alive messages. The default value is **Yes**.

Ignore Keep-alive timeout errors, ignore keep-alive timeout errors. The default value is **No**.

Sync on Connect, request database synchronization after establishing PMS connection.

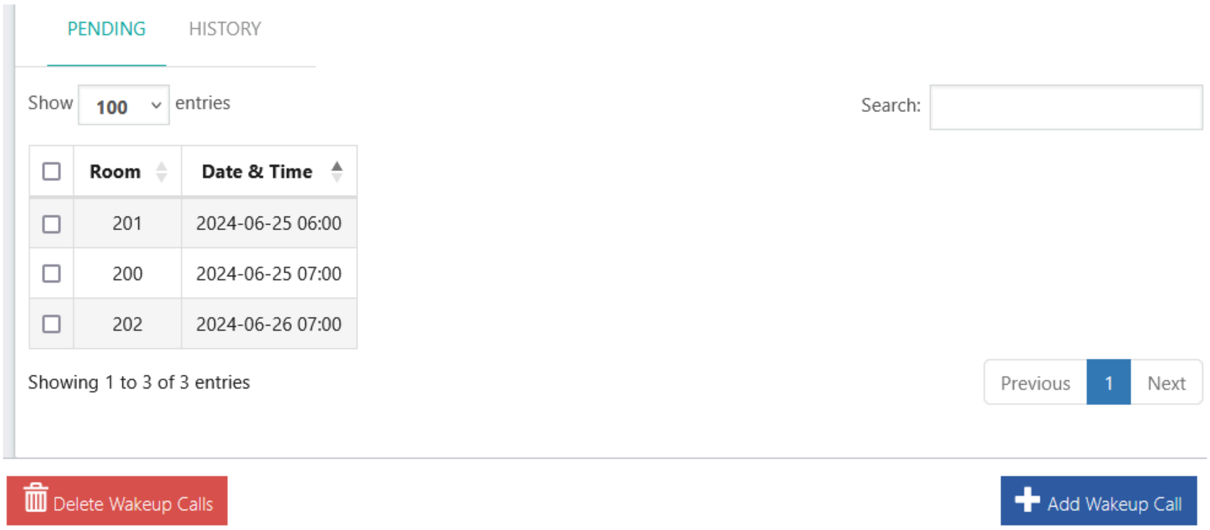
Wakeup Calls Dialog

In this dialog, you can manage wakeup calls efficiently and conveniently. You have the ability to:

- Delete scheduled wakeup calls
- Set recurring wakeup calls

- View history and status of wakeup calls

PENDING Tab



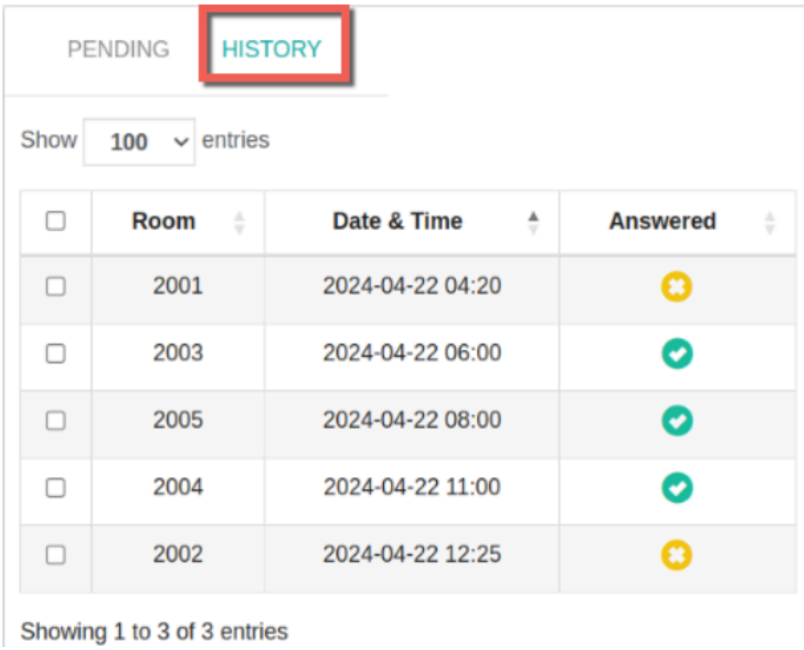
Add Wakeup Call, press this button to configure a wakeup call for a room. By pressing this button a dialog will apear:

Rooms, list of rooms to create a wakeup call for.

Date & Time, specify the date and time for the wakeup call to occur.

Delete Wakeup Calls, deletes the selected wakeup call.

HISTORY Tab



In this tab, you can view the history of wakeup calls. The following information is displayed:

- **Room**, the room for which the wakeup call was scheduled.
- **Date & Time**, the date and time when the wakeup call was set to occur.
- **Answered**, shows an icon indicating whether the wakeup call was answered or not.

Testing the Hospitality Module Configuration

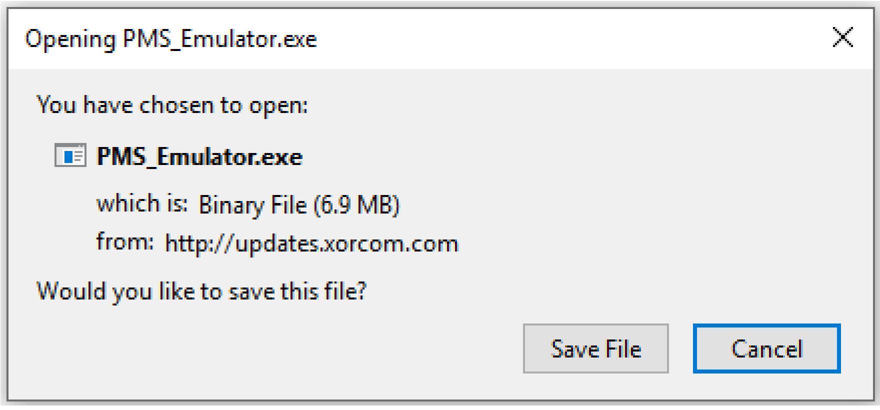
Installing a PMS Emulator

If you do not have access to an active PMS system, you can install the P$X PMS Emulator on a Windows machine.

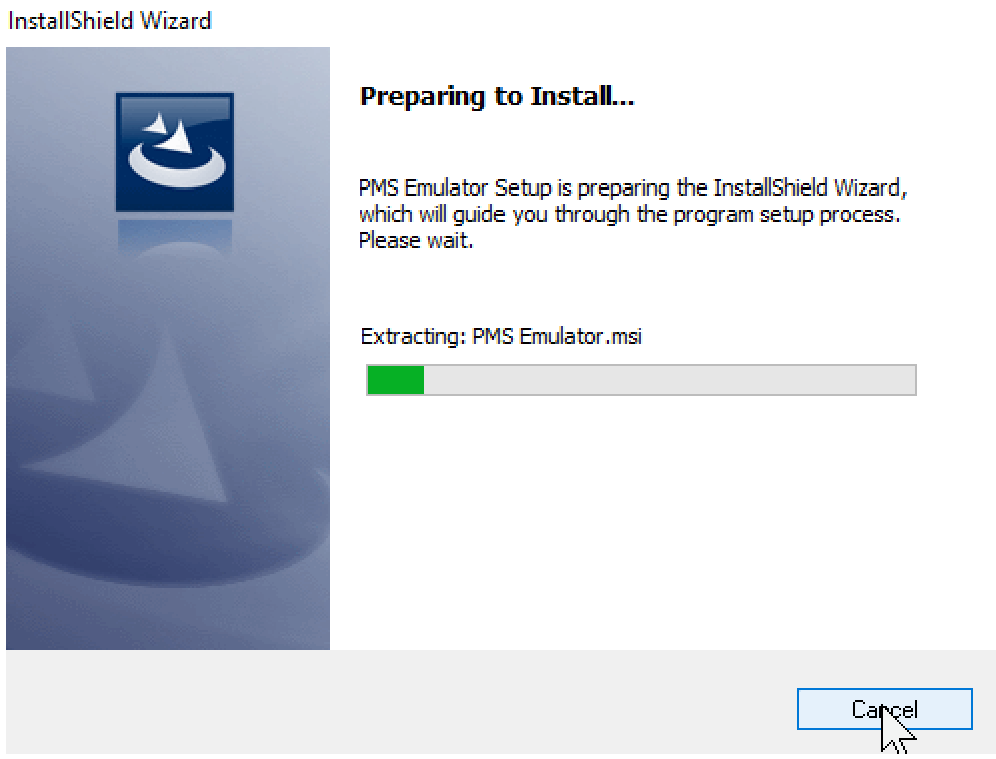
The P$X PMS Emulator software can be installed by using the following link:

https://updates.xorcom.com/servers/complete-concierge/PMS_Emulator.exe

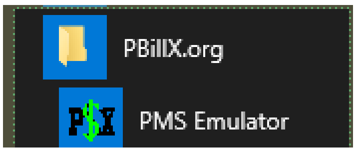
Click on **Save File** to save the installation file on your Windows machine,



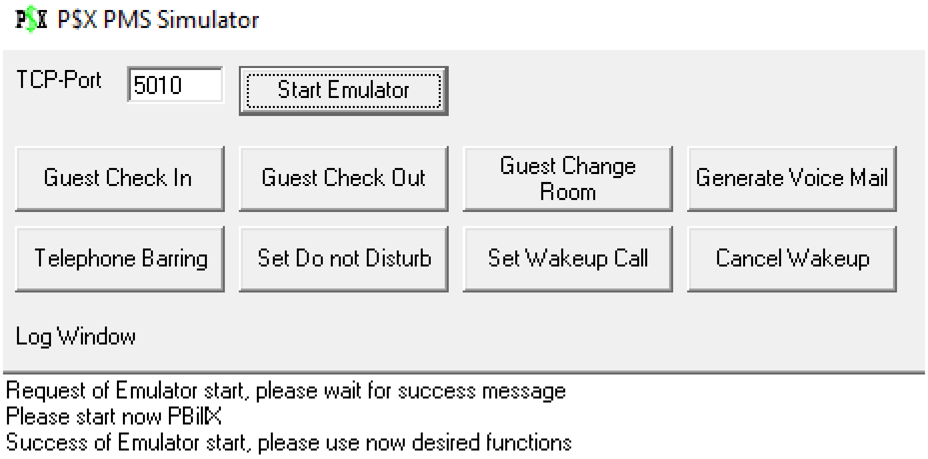
After the file has been downloaded, double-click on the PMS_Emulator.exe file that you have downloaded and install the emulator software.



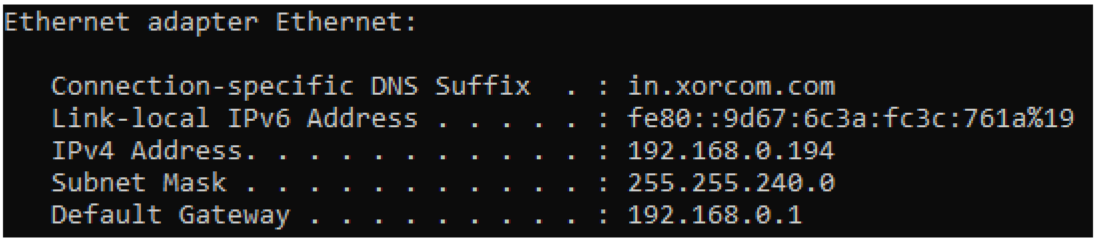
If you installed the emulator on a Windows 10 box, the P$X PMS Emulator software will be located in the PBillX,org program group



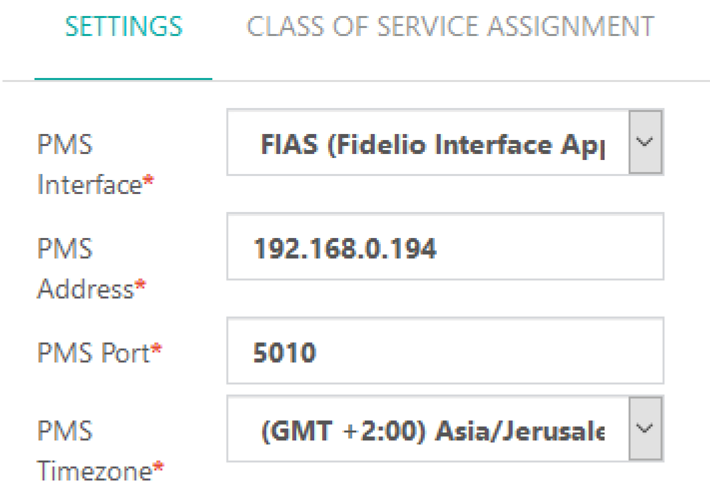
Run the P$X PMS Emulator program on your Windows machine. Note the TCP port on which the emulator is running (typically 5010), and click on the **Start Emulator** button. The Log Window will indicate the successful start of the emulator.



Determine the IP address where the P$X PMS Emulator is running (i.e. the address of your Window machine) by running the Windows Command Prompt and typing the ipconfig command - in my case I am using a wired Ethernet connection, and my address is 192.168.0.194



Go to the CompletePBX GUI, and open the PMS Interface dialog. In the Settings tab, select FIAS as the **PMS Interface**, and enter the **PMS Address** and **PMS Port** that you found in the previous steps, and click on the **Save** button.



Checking Status of the fias Interface

You can test the status of the PMS interface by entering the command line interface, and typing the command:

```
journalctl -u complete-concierge-com
```

You should receive output indicating that the PMS interface is active, which could look something like this:

```
fias[29178]: Connecting to the PMS (192.168.0.194:5010)...
fias[29178]: Connection to the PMS (192.168.0.194:5010) has been established.
fias[29178]: LS request was not received from PMS. Sending LS request.
fias[29178]: LA response received from PMS.
fias[29178]: Communication with PMS has been initialized. Sending LA.
fias[29178]: RCV: WR|RN201|DA090316|TI100000|
fias[29178]: RCV: GI|RN100|GNMr & Mrs Colombus|GLEA|GSY|
```

Note the last two lines of the log, that indicate:

- A wakeup request for 10:00 has been received for room 201
- Guest check in has been received for Mr & Mrs Colombus in room 100

You can also view the log of all Complete Concierge messages in the file **/var/log/cconcierge.log**

Testing Options

The following tests may be performed to verify the configuration of the Hospitality module.

Calls from an Occupied Room

- In order to evaluate the Hospitality module without a Property Management System, it is possible to simulate check in of a guest by pressing **Guest Check In** in the P$X PMS Emulator interface.
- Make a call from this room to the reception. The guest name and the room number should appear on the LCD screen of reception telephone.
- Block the guest phone by pressing **Telephone Barring** in the P$X PMS Emulator interface and make an external call. The call should be rejected. Then make a call to the reception. The call should be established.
- Unblock the guest phone by pressing **Telephone Barring** in the P$X PMS Emulator interface and make an external call. The call should be established. Make sure that the guest account is properly billed.

Calls from a Vacant Room

- In order to evaluate the Hospitality module without a Property Management System, it is possible to simulate a check-out of a guest by pressing **Guest Check Out** in the P$X PMS Emulator interface.
- Make a call from this room to the reception. The guest name **Vacant** and the room number should appear on the LCD screen of the reception telephone.
- Make an external call. The call should be rejected.
- If voice mail is configured for this particular hotel installation, verify that the voicemail messages of the guest are deleted.

Room Change

- Change the room of the guest using the **Guest Room Change** button in P$X PMS Emulator interface.
- Verify that the phone blocking status is set correctly.
- The guest name should be assigned to the new room and the previous room should be marked as vacant.
- The voice mail messages should have been deleted from the mailbox of the previous room.

Wakeup Calls

Wakeup calls work regardless of the room telephone status. A wake-up call may be scheduled even for a blocked phone or a phone that is set to DND mode. Wakeup calls may be scheduled either via the PMS or from a guest phone.

- In order to evaluate the Hospitality module without a Property Management System, it is possible to simulate a wakeup call by pressing **Set Wakeup Call** in the P$X PMS Emulator interface.
- Check in a guest. Order a wakeup call via the P$X PMS Emulator interface. Answer the wakeup call when the room telephone rings. Make sure that P$X PMS Emulator interface received the correct wake-up call report.
- Order a wakeup call via the P$X PMS Emulator interface and do not pick up the phone when it rings. After three attempts the wakeup call will be considered unsuccessful. Make sure that the P$X PMS Emulator interface received the correct wakeup call report.
- Make sure that the wake-up calls work when ordered by dialing ***34** from the guest telephone. Check that the wakeup call request is registered in the P$X PMS Emulator interface.

Do Not Disturb (DND)

- Set the DND mode for a room by pressing **Set Do not Disturb** in the P$X PMS Emulator interface). Make a call from reception to the room. The room telephone should not ring.

- Disable the DND mode for a room by pressing **Set Do not Disturb** in the P$X PMS Emulator interface). Make a call from reception to the room. The room telephone should ring.
- It is also possible to enable/disable DND from the guest telephone. The telephone DND button (if it exists) must be programmed to dial the corresponding CompletePBX 5 feature code (***66** by default). Alternatively, it is possible to dial the code from the telephone keypad.
- Incoming calls will be treated as follows when DND is enabled: if Call Forward Unavailable is configured, the call will be forwarded accordingly; if Voicemail is enabled, the call will be sent to voicemail; otherwise, the caller will receive the busy tone.

Room Maid Status

Room Maid Status can be changed by dialing feature code **22** from the room telephone. The following statuses may be defined:

- 1 Dirty / occupied
- 2 Dirty / vacant
- 3 Clean / occupied
- 5 Clean / vacant
- 6 Inspected / vacant

Minibar Status

Minibar Status can be changed by dialing feature code **23** from the room telephone.

App Manager Menu Group

Supervision Manager

Supervision Manager is a productivity tool to help you to utilize your office phone. Supervision Manager does not replace your regular physical phone, but extends its capabilities, by using your computer to transfer a call, put calls on hold, park calls, search your phonebook, and many other functions.

Setup & compatibility

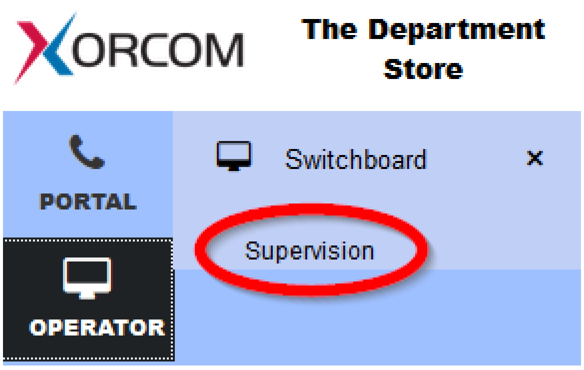
Supervision Manager does not need any installation or complex setup, and works with any current HTML5 browser, including Firefox, Chrome, and Safari.

Access and Login

There are three methods to access Supervision Manager:

- Navigate to Settings > App Manager in CompletePBX 5, and select the Supervision Manager dialog.
- User any internet browser to access the CompletePBX 5 Portal. To use this option you will need to:

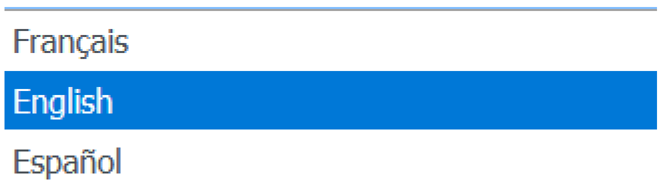
  1. Ensure that extension is defined as a CompletePBX 5 Portal user
  2. Access the CompletePBX 5 Portal
  3. Click on the Supervision menu from the Operator menu group



- Use any internet browser to access Supervision Manager, by entering the IP address of your CompletePBX server followed by **/supervision** in the address field of your browser. For example, if your CompletePBX 5 system is located at https://mypbx.mydomain.com, you should enter https://mypbx/mydomain.com/supervision.

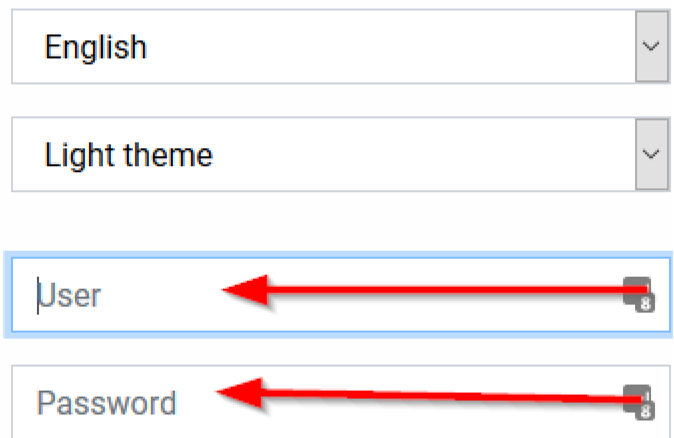
  1. Select the language from the drop-down list of languages that you want to use in the Supervision Manager. Language, enables you to select to display the Supervision Manager

user interface in any of the available languages. Changing the language does not change the functionality of the software, and only impacts the cosmetics of the GUI. The new language is applied immediately, and the setting is saved in the memory of your browser. If you use different browsers or different computers to access Supervision Manager, you will need to define the language for each browser that you use.

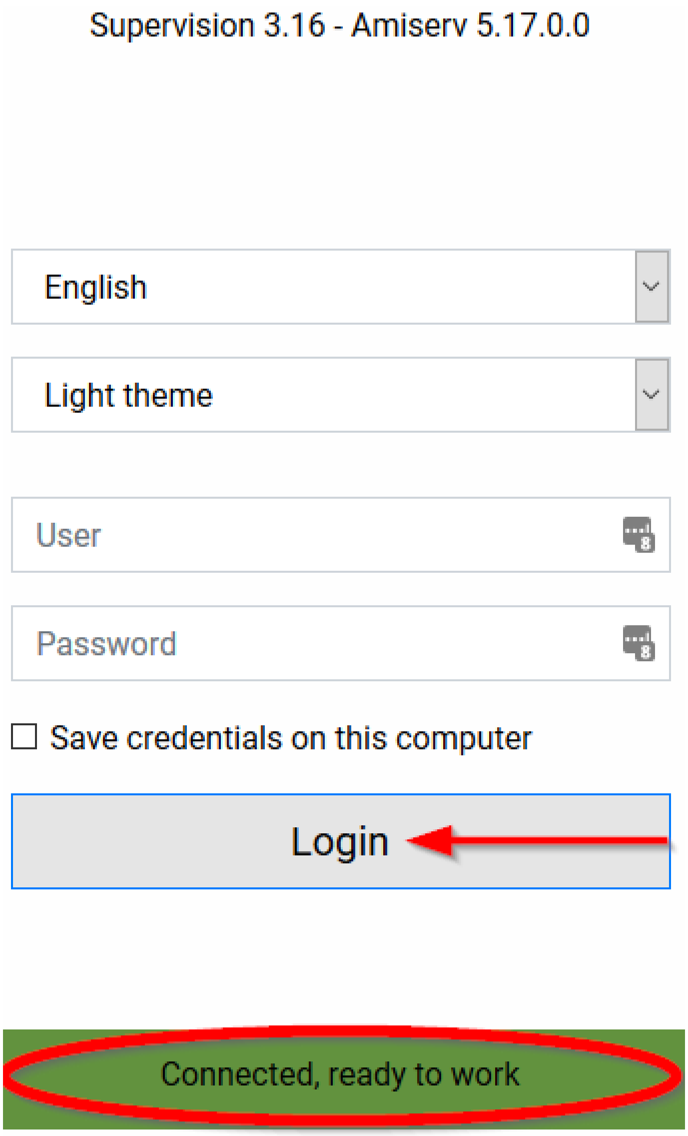


2. Select dark or light theme from the drop-down list of themes. Theme, allows you to choose between using a dark or light theme in the User Interface. Changing the theme does not change the functionality of the software, and only impacts cosmetic of the GUI. The new theme is applied immediately, and the setting saved in your browser memory. If you use different browsers or different computers to access Supervision Manager, you will need to define the theme for each browser that you use.

3. Enter your CompletePBX 5 username (typically **admin**) in the User field, and your CompletePBX 5 password in the Password field.



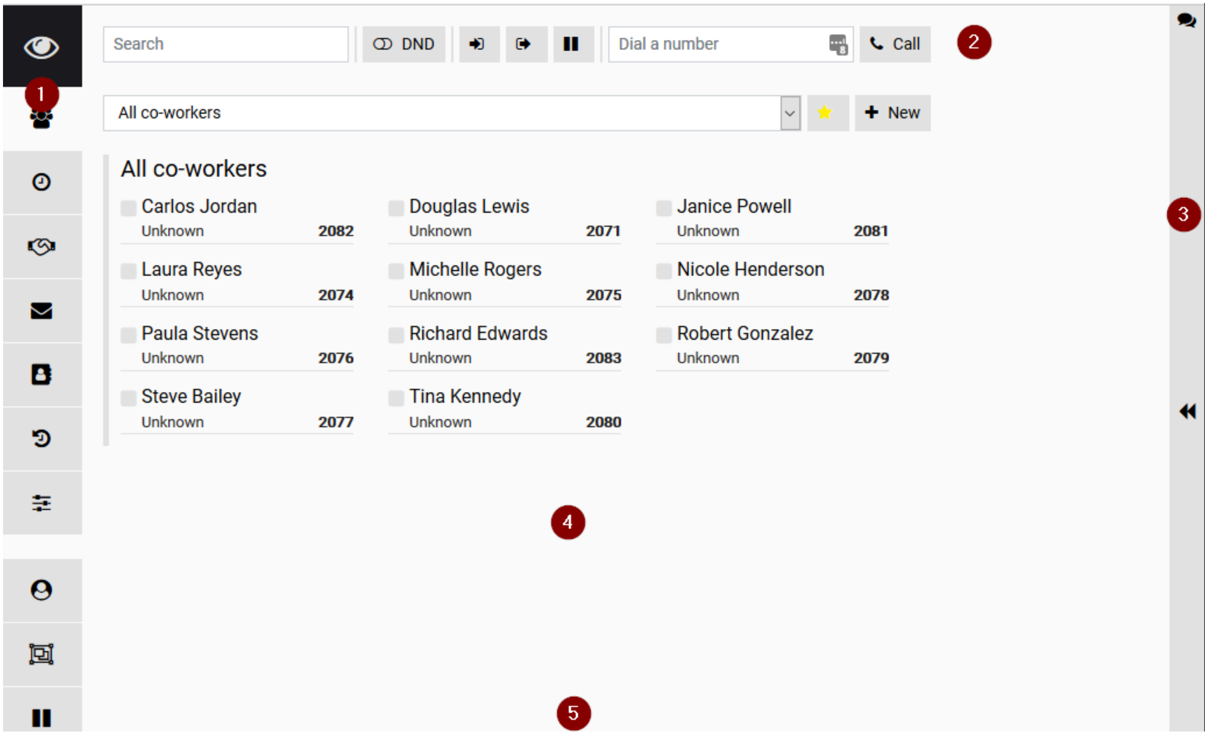
4. Press on **Login** to enter the Supervision Manager. You will see a message at the bottom of the screeen indicating that the Supervision Manager is logged in and ready for use.



If you see an error message, or if the **loading** message is displayed for a long period, update the page by pressing **F5**.

Save credentials on this computer, check this on if you want to save the login and password information in the local storage of your browser. This will speed up your login process next time you activate Supervision Manager. If you use different browsers to access Supervision Manager, you will need to repeat this for each browser that you use.

Layout of the User Interface



The left (vertical) menu ① allows you to navigate to the available dialogs:

- My Co-workers
- Queues
- Conferences
- Voicemails
- Phonebooks
- Call History
- My Settings
- Users
- Profiles
- Pause Reasons
- Toggle Full Screen
- Open user manual
- Disconnect

The top bar ② is visible on all panels and is fixed. You can use it as a shortcut for some functionalities such as searching in the panel, going to do not disturb, login/disconnecting from queues, using pause feature, and calling a number. The Search bar lets you search any information displayed in the main panel ④

The right (vertical) bar ③ contain the call list currently on your extension and the chat panel.

The main panel area ④ contain the information about the item that you have selected from the left menu ①.

The bottom area ⑤ is dedicated to parked calls: all parked calls will be displayed there.

System Messages Colors

When using Supervision Manager, different messages will appear in the bottom area of the screen. The color indicates the importance of each message:

- Green - indicates that the last command was successful
- Blue - displays generic messages, showing what the system is currently doing, loading, etc.
- Orange – indicates a problem, such as a warning or a non-critical error
- Red – indicates a critical error, or that the last command failed

Left Menu

The left menu lets users navigate through 7 different panels. When the user clicks on an item, the data from the panel will be displayed in the main area of the GUI.

Available icons are:

- My Co-workers: Display all extensions, their status, and let the user do actions like calling, spying, barging, etc.
- Queues: Display queues, call waiting in the queues and agent status
- Conferences: Let the user manage audio conferences.
- Voicemails: Display voicemail messages and let the user listen it from their phone.
- Phonebooks: Give access to the IPBX phonebooks.
- Call History: List all the user calls, let user search through call history and listen recorded calls.
- My Settings: Display user settings and let the user activate call forwards.

Additional icons for administrators are also displayed, but only when the logged in user has administration rights:

- Users: Let user manage users (login, password, rights…)
- Profiles: Profiles are used to limit what a supervision user can see and can use.
- Pauses: List and manage pause reasons.

Three additional icons are also displayed for all users:

- Full screen toggle: Lets users toggle between full screen and normal window mode. This has the same effect as pressing F11 in your browser.
- Open user manual: provides access to the Supervision Manager User Manual
- Disconnect: Logout and exit from Supervision Manager.

My Co-workers Dialog

The Coworker panel lists all the extensions of CompletePBX 5, the current status of each extension, the name of the extension user, the internal number, and gives access to actions and commands depending of the status of the extension.

Each coworker is displayed using this template:

- First line
  - Status color code
  - Extension name
- Second line
  - Status string
  - Extension internal number

Clicking on a coworker displays an action menu containing different items, depending on the extension status. Action items are listed in the table below:

Action Item	Idle	Ringing	On a call	DND
Call	✓	✓	✓	✗
Spy	✗	✗	✓	✗
Whisper	✗	✗	✓	✗

Barge	✗	✗	✓	✗
Intercept	✗	✓	✗	✗

Some functionality (such as spying, whispering, and barging) can be disabled by the administrator in CompletePBX 5.

Extension Status Colors

The extension color code lets the user quickly see the state of the devices for the extension. Colors used are:

Green	Extension is idle, ready to be called or to make a call
Orange	Extension is currently ringing (incoming call only)
Red	Extension is already on the phone, or is busy
Grey	Extension doesn't have any device attached or connected
Red Cross	Do Not Disturb (DND) is active

Coworkers Groups

By default, all coworkers are listed in a group named **All co-workers**. You can create groups of coworkers to reduce the number of displayed extensions, or to create a hierarchy.

When clicking on the **New** button, the creation form appears.

Adding a coworker to the group is made by checking the box in front of his name. To remove the coworker, uncheck the box.

By clicking on **Validate**, the group is saved for the current user.

Users can choose to share coworker groups by checking the S**et this group as inheritable** box. This functionality is available only if the administrator has allowed the user to share his groups.

By clicking on the star button on the right of the group selector, the user can set a group as favorite. This group will then be automatically displayed when the user opens Supervision Manager.

Call Management

Calls related to the extension of the user are displayed on the right-hand bar of the GUI. Calls are stacked vertically and sorted according to the age of the call.

The Call display contains a status color code, the number of the caller/recipient, the duration of the call and the contact name (if known)

The status color codes are:

Orange	Ringing
Red	Answered, talking
Blue	On hold

Managing Calls

Users can interact with calls in two manners:

- By drag and drop - used mainly to transfer a call
- By clicking on the call - opens the action menu

Call Transfer

Call transfer is done by using drag and drop to move the call to a destination. Possible destinations are:

- Coworkers
- Queues
- Phonebook contact
- Voicemail
- User cellphone
- Conference

Call transfer can be done using blind transfer or attended transfer.

- Blind transfer consists of sending the other party to a destination without checking first if the destination is ready to accept a call. It means that the call can be transferred to a busy destination.
- Attended transfer consist of first calling the destination (called consultation call) and then transfer the call if the destination agrees. Attended transfers are only compatible with coworkers and phonebook contact. Transfers to other destinations are automatically converted to blind transfer.

Configuring whether to use blind or attended transfer is done in the **Drag and drop transfer type** field in **My Settings**.

Configure CompletePBX 5 for Attended Transfer

To get attended transfer working, the administrator must create a special configuration using Settings > Technology Settings > Dial Profiles in CompletePBX 5. Separate Dial profiles must be created for both extensions and trunks.

The trunk Dial Profile must allow call transfer by the caller. The CompletePBX 5 administrator must then set this Dial Profile for each trunk used for outbound calls.

The Dial Profile for extensions must allow transfer by recipient. This Dial Profile must then be selected for all extensions using Supervision Manager.

Never create a Dial Profile allowing both sides to do call transfer. This can lead to call piracy. The trunk dial profile must allow transfer only by caller, while the extension dial profile must allow transfer only by recipient.

Call Action Menu

Clicking on a call opens the action menu. This menu contains the following icons:

- Answer a call
- Put a call that has been answered on hold, or retrieve it
- Hang up or reject a call
- Add or edit a phonebook contact entry
- Add or see call notes
- Send DTMF
- Mute or Unmute a call
- Record a call (only after the call has been answered)
- Park a call

Some icons (such as answer, hold, and retrieve) are only displayed when a compatible device is selected. User must select the brand of his phone in the Supervision Manager settings. The Record function can only be used if **On Demand Recording** is allowed in the CompletePBX 5 PBX > Extensions > Recording tab.

Call Parking

Parking consist on putting call on hold in a special area in CompletePBX 5. The calling party will hear hold music, while the called device becomes available, i.e. the call is no longer connected to the user device.

Parking lots are defined by special numbers. Dialing a parking lot number lets users retrieve a call waiting in the parking lot.

Supervision Manager simplifies the way parking lots are used by displaying calls parked on the bottom of the screen.

Call parking needs special rights in the Settings > Technology Settings > Dial Profile dialog of CompletePBX 5. The CompletePBX 5 administrator must enable these rights to allow Supervision Switchboard users to use this function.

In order to use call parking, the CompletePBX 5 administrator must create specific extension and trunk dial profiles.

The trunk dial profile must allow the Park feature for callers. This dial profile must then be selected in every trunk used for outbound calls.

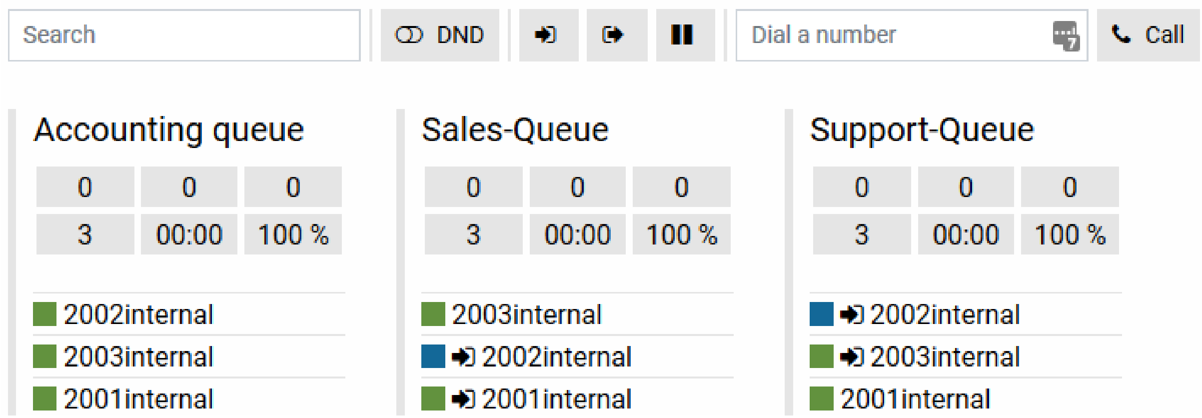
The extension dial profile must allow the Park feature for recipients and must be selected for every extension user of the Supervision Switchboard.

Transferring Calls to Voicemail or Cellphone

Supervision Manager users can transfer ringing or established calls to voicemail (if enabled) or to their mobile number (if defined in the **My Cellphone number is** field of My Settings in Supervision Manager).

To transfer the call, use drag and drop. New icons will appear on top of the call list. The first icon sends the call to the user's voicemail, while the second icon transfers the call to the user's cellphone. No icons are displayed if voicemail is disabled and the cellphone number is empty.

Queues Dialog



All Queues are displayed in this panel. Statistics are displayed for each queue.

Queue Statistics

Queue statistics are displayed for each queue, and are (from starting from left to right, top to bottom):

- Top row
  - Successful call count today
  - Failed call count today
  - Current waiting call count
- Second row
  - Available agent count
  - Average wait time in the queue
  - Percentage of successful calls today

Agents

Each agent is identified by their name, status (displayed as color code), and an optional icon.

Status color code for agents are:

Green	Agent is idle, ready to be called or to make a call
Orange	The phone of the agent is currently ringing (incoming calls only)
Red	Agent is not available, already on the phone, or is busy
Blue	Agent is paused
Grey	Dynamic agent that is not logged in

Call Waiting in the Queue

Each waiting call is displayed with the caller number (if known), the time spent waiting in the queue, and the caller name (if known).

Queue Interaction

You can interact with the queue in three different ways, by clicking on the:

- queue name
- call
- agent

If you click on Queue Name, the user can:

- Login or logout of this queue
- Switch to pause or return to work
- Click on a call to intercept a call

If you click on queue agent, the user can

- Login or logout a dynamic agent
- Switch this agent to pause or return the agent to work

Depending on the status of the user, different queue interactions are available.

Any user can:

- Login/logout from a queue if this user is dynamic agent of the queue
- Switch to pause or get back to work
- Intercept a call from any queue

In addition, a supervisor can:

- Login or logout any dynamic agent from any queue
- Switch any agent to pause or get back to work.

Intercepting or Redirecting Calls

Any Supervision Manager user can intercept calls from a queue, even if the user is not an agent of the queue. Redirecting a call allows users to quickly take someone waiting in the queue (for example, an important customer)

Intercepting a call from the queue will increase the failed call count of the queue. Using this feature will affect statistics of the queue.

Login and Logout from all Queues

At the beginning and end of shifts, users will need to login or logout from every queue. This can be done using the top bar menu.

Using the buttons of the GUI top bar, the user can:

- Click on the icon to login to every queue where the user is defined as a dynamic agent
- Click on the icon to logout from every queue where the user is defined as a dynamic agent
- Click on the icon to toggle the pause status for every queue that the user is logged in to. Switching to pause displays the **Pause Reason** menu. The user must select a pause reason to enable pause. Pause reasons allow administrators to get statistics on pause reasons and pause durations for agents. The list of Pause Reasons can be modified by administrator.

Conferences Dialog

Supervision Manager lets users manage conferences by displaying conferences rooms, conferences members, adding member dynamically, muting people, etc.

Select a conference from the drop-down list of conferences.

The drop-down list of conferences displays only conferences that are configured in CompletePBX 5.

Conference Members

Conferences have a predefined number of members, which is configured in the Conferences dialog in CompletePBX 5. Every available member is displayed as a square box containing the **+** symbol. When a member enters the conference, the member information is displayed the box:

- Member name (if known)
- Member number (if known)
- Duration since this member joined this conference
- Icon indicating if the member is muted or is talking
- Talk duration of this member (only if Talk Detection field is enabled in the CompletePBX 5 Conferences dialog)

Adding a Member

Adding a member can be done using 2 ways:

- By clicking on an empty seat
- By transferring a call using drag and drop to an empty seat

Clicking on an empty seat is the most convenient way to add a member. After clicking, a form will ask for the member number, or to select a phonebook contact from a list. Users can also search the name of the contact in the phonebook list.

Mute and Kick

At any time, the conference administrator can mute a member, unmute him, or kick him out of the conference.

A muted member is displayed with a crossed microphone. Kicking out a member will hang up the member's call.

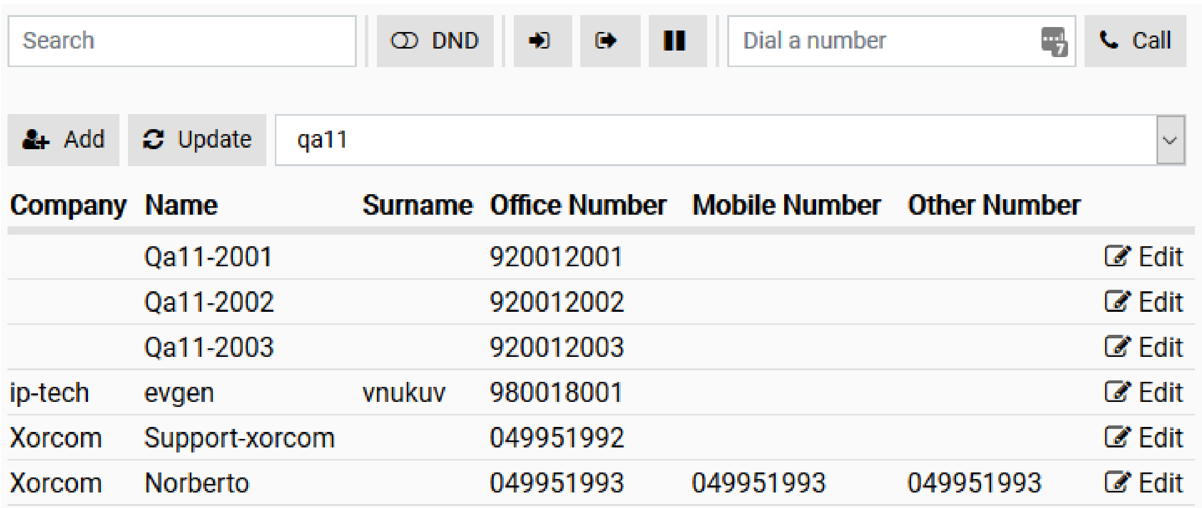
Important information regarding conferences

- Stopping a conference using "Stop conference" will hang up all members call without notice.
- Muted members are not aware of their status. You should first tell them that they cannot speak anymore.
- Detecting talk time only work if this option is configured in CompletePBX 5.
- Talk time duration is updated when the conference member stops talking.
- You can transfer a call in the conference using drag and drop, but only the external parties will be transferred. Local users must join conference manually.
- Adding an external conference member can take up to 30 seconds, as time is needed to call the member, get an answer from the member, and make the connection. Be patient.

Voicemails Dialog

Allows the user to manage voicemails for his extension.

Phonebook Dialog



CompletePBX 5 phonebooks are displayed in this panel. Editing a contact from a phonebook is immediately shared with other Supervision Manager users.

Phonebook entries can contain:

- Name of company
- First name of contact
- Last name of contact
- Office number
- Mobile number
- Other number
- Email

Users can search contacts using the search bar in the top navigation bar of Supervision Manager.

Managing Contacts

User can create contacts by:

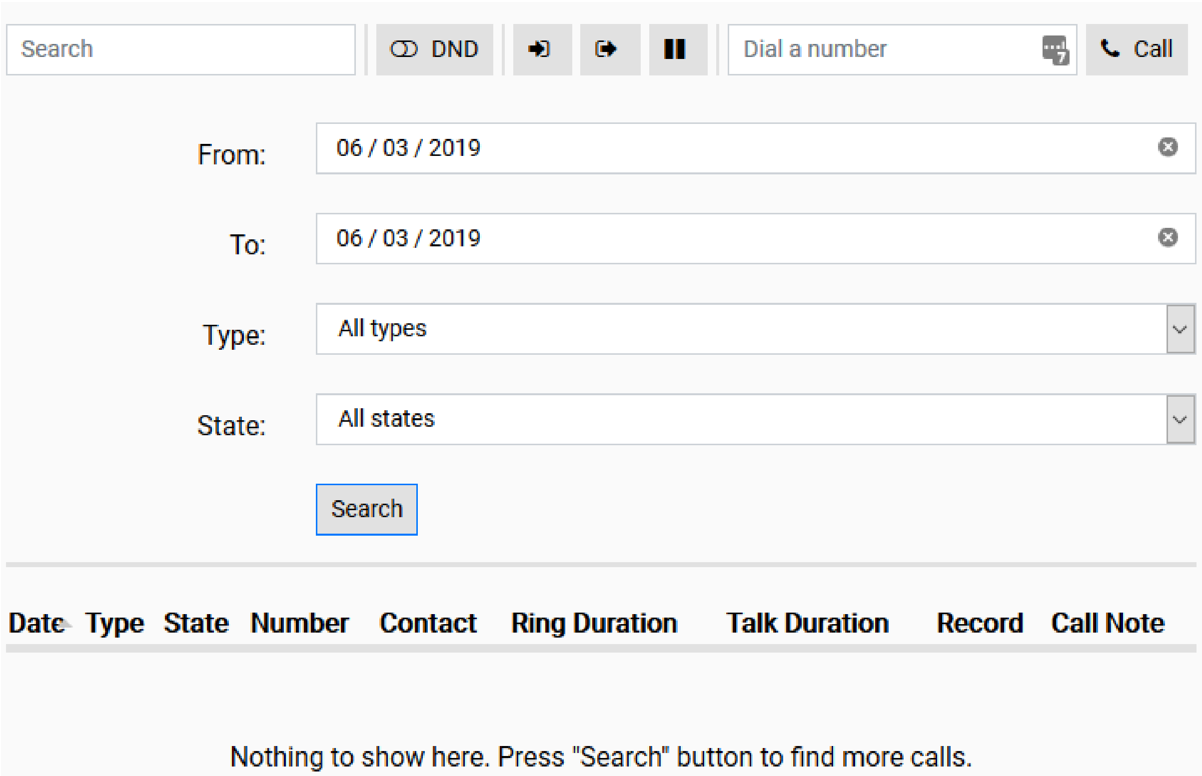
- Clicking on the **New** button in the phonebook panel
- Clicking on the **Edit contact** button in the action menu of the current call.

To create a contact, user must provide a first or last name, and at least one phone number.

Calling a Contact

Users can call any contact by clicking on a phone number in the contact table.

Call History Dialog



Call history contains calls sent or received on the devices of the current user. Calls of other users are not displayed. The call history table can be sorted using the call type, call status, number, etc. by clicking on the header of the table. Call history data is updated automatically at the end of every call.

Filtering and Searching Calls

Users can search for a call in the history by using the search input on the top navigation bar of Supervision Manager. Users can also use the provided form to filter results by date, type, and state.

Calls can be made by clicking on a phone number in the history table

Calls are categorized using their type

- Internal
- Outbound
- Inbound

And by their state

- Answered
- Failed

Call Recording

Users can listen their call recordings by clicking on the  button in the table. Calls without this button do not have any records. The recording is played on the phone of the user.

Call Notes

An icon is displayed when the call contains one or more call notes. Users can read a note by clicking on it. It is not possible to edit or add a call note in the history.

Voicemail

If the user has voicemail enabled, and if voicemails are not deleted after being sent by email, the users can use their phone to listen to voicemails and recordings.

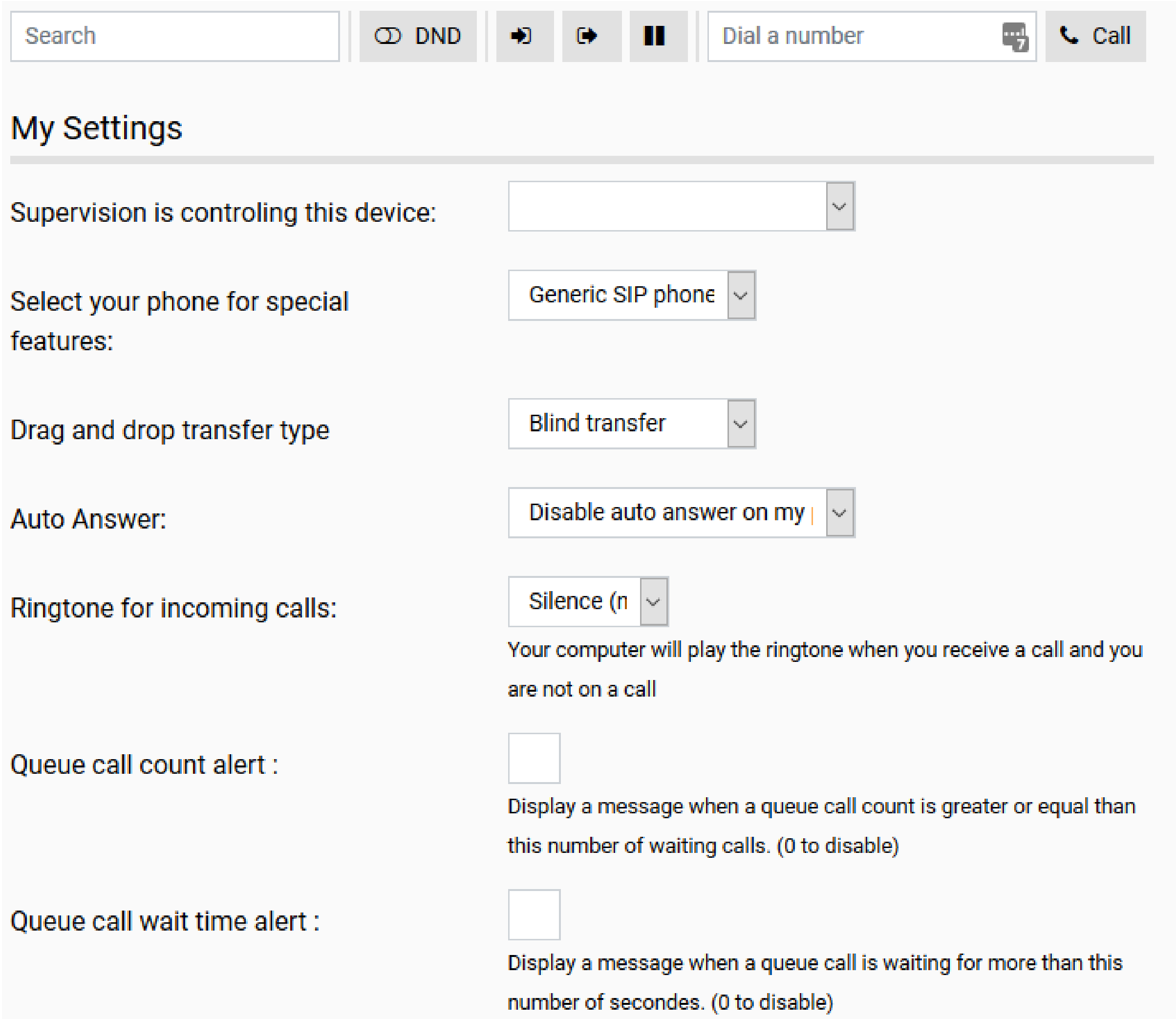
Listening a voicemail can be done by clicking on the button. The button moves the current voicemail to the “old” folder (or back in the “new” folder, depending of the current state of the voicemail). Deleting a voicemail is done by clicking on the button.

My Settings Dialog

The My Settings dialog allows the user to modify the way Supervision Manager works, set alerts, change how transfers are made, and choose the phone device to be used.

Supervision Manager allows the users to choose their preferred phone device. After selecting a device, all interactions will be made on this specific device. The user must select at least one device. If no device is selected, Supervision Manager will ask the user to choose one on next login.

Unlike Language and Theme, which are locally saved in the memory of the user browser, the settings set on this panel are stored in CompletePBX 5 and loaded at login time, independently of the computer or browser.



Available settings are:

Supervision Switchboard is controlling this device	User must select their preferred device from this dropdown. All calls will be made on this device.
Select your phone for special features	Select here the brand of the user phone. If the phone is listed in the dropdown list, Supervision Switchboard will add specific features such as answer button, hold, mute, etc.
Drag and drop transfer type	Select here the default transfer type preferred by the user
Auto Answer	By choosing “Enable auto answer on my phone”, the phone will automatically answer outgoing calls made using Supervision Switchboard. This does **not** enable auto answer for incoming calls.
Ringtone for incoming calls	The computer can set a ring tone on incoming call. Select the preferred ring tone here.
Queue call count alert	Display a visual alert when the call count for a queue exceeds this value

Queue call wait time alert	Display a visual alert when a call has been waiting more than the number of seconds defined here.
Dial the selected number when pressing this key	Enable Supervision Switchboard companion and let the user use Click 2 Call features.
My Cellphone number is	Set the user's mobile phone number. User can then transfer a call on their own mobile phone.

Call Forwarding

Supervision Switchboard lets users enable or disable call forwarding (immediately, on busy, on no answer) by clicking on the button.

Enabling unconditional (immediate) call forwarding (CFI) sends all incoming calls to the selected destination.

Enabling call forward on busy (CFB) sends incoming calls to the selected destination when the user is already on the phone (disabling the voicemail in this case)

Enabling forward on no answer (CFN) sends incoming calls to the selected destination when the user does not answer a call after a predefined amount of time. If the user has voicemail enabled, setting CFN will temporarily disable the voicemail.

Supervision Manager Companion

Companion is a tool made to help dialing numbers from external software, such as Excel, Word, etc. Companion is compatible with any computer running Windows 7 or later.

Installing companion is fast, simple and easy: click on the text below the **Dial the selected number when pressing this key** setting, download and execute the file, and follow the instructions.

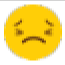
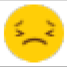
After being installed, Companion will automatically start with Windows. The user must reload Supervision Manager after installing Companion to get it working the first time. When running, Companion is displayed as a small Supervision Switchboard icon in the system tray.

Chat (IM)

Chatting with other users can be done using Supervision Manager Chat tool. Currently connected users are displayed on the right navigation bar. This bar is hidden by default, user must click on the 2 arrows to show or hide the bar.

Messages can only be sent to connected users. A connected user receives the message instantly. When opening a chat box, history will shows messages for the past 24 hours.

Sending an internet address in the chat is automatically converted to valid URL. The user can also send icon showing their current mood by typing specific characters, defined in the table below:

Characters	Substitution
:)	
:(	
:D	
:p	
:/	
:'(	

User can also send Unicode icons.

Users Dialog

The administrator must create users prior to use of Supervision Manager. Every user contains at least a login and password, and some optional settings such as extension number, parking lot, profile, etc.

Administrator users have access to the user administration panel.

An administrator can create or edit a user by clicking on the  menu item.

You can choose between creating a new user or editing an existing user.

Every user login must be unique. Password must contain at least 8 characters, with 1 lower case, 1 upper cape, and 1 special char from this list: !@#$&*-_

Setting the user extension lets the user use any device associated with this extension. In case the administrator did not configure an extension number, Supervision Manager will work with limited features.

Choosing different parking lots allows the administrator to create different company groups. Users with the same parking lot can see parked calls and handle calls, but cannot see calls from other parking lots.

Choosing a profile lets the administrator limit user rights. Profiles contain information that is displayed on the user screen.

Automatic Creation

If a user connects to Supervision Switchboard from the Portal of CompletePBX 5, a user account will be automatically created with the user extension as login, and a random (strong) password. The user can then change the password or connect from the portal.

The administrator can then edit the user, profile, parking lot, etc.

Profiles Dialog

User profiles let administrator limit what users can see and do. A profile lets administrator create a pool of users depending on their competence, the company division, etc.

Each profile lets the administrator set lists of visible coworkers, queues, conferences. Profiles also let the administrator set rights on conference management, and the inheritance of coworker groups.

In a call center, profiles can be used to create pools of users. A supervisor can be chosen for every profile: this specific user has more authorization in queue management and can login, logout, and pause queue members.

Creating a profile is easy: set a name, check every visible coworker, queues, conferences, etc. If the profile must see everybody, administrator can check the "All existing and new" box. Checking this box is different than checking all box: when checking **All coworker box** (for example), only ***existing*** users will be visible. New users will ***not*** be visible. Checking the **All existing and new** will display all existing coworkers, as well as any new coworkers that are created in the future.

If you want to display all future extensions, conferences, and queues, check the **All existing and new** box.

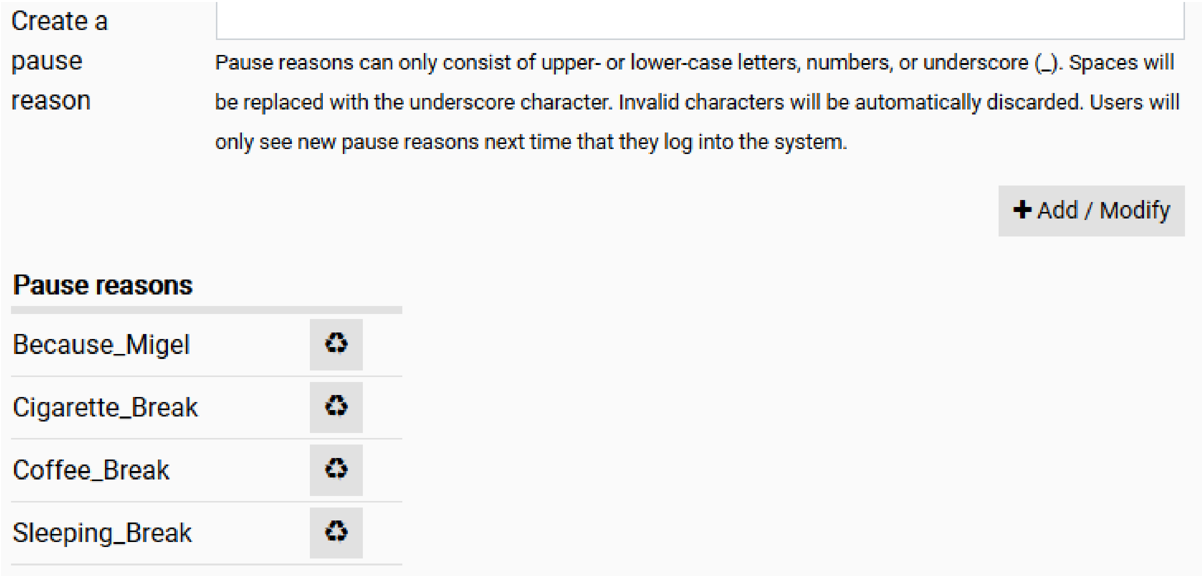
Coworker Group Inheritance.

As explaining in **My Coworkers** above, a user can create coworkers' groups and mark groups as shared. These groups will be visible from all users of the same profile if the user is selected as the group inheritance.

Supervisor

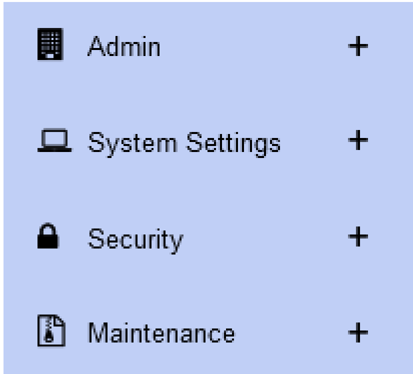
Supervisors are users with more queue authorizations: they can login, logout, pause any member of the displayed queues.

Pause Reasons Dialog

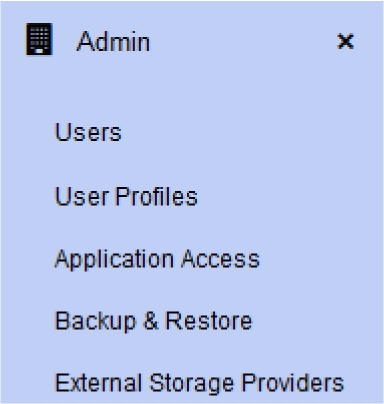


When a user is a member of a queue, he can switch to pause mode. Paused users will not receive any new calls from the queue. Users must select a pause reason when activating pause mode. Administrator can create multiple pause reasons: these reasons will be shown in compatible statistics software.

6. Admin Menu Set



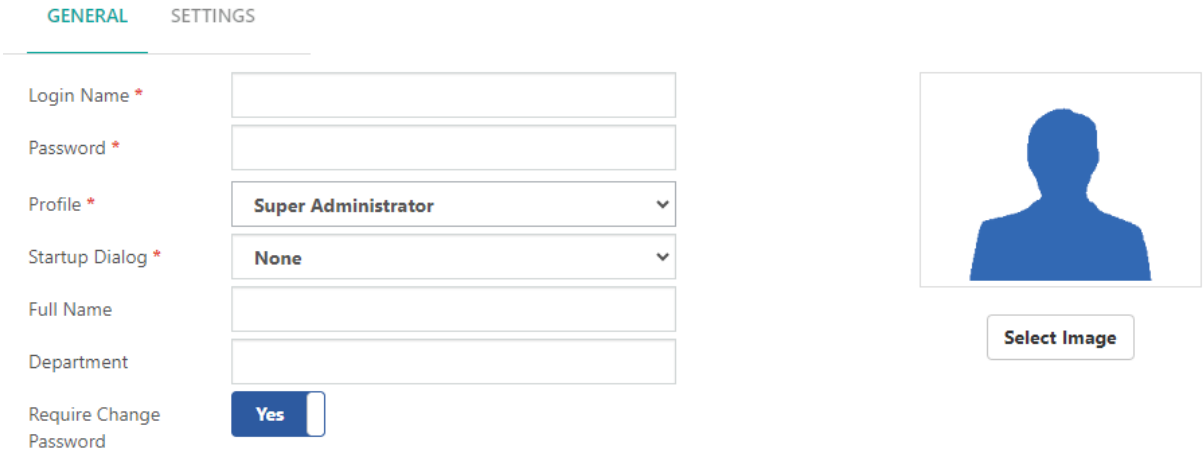
Admin Menu Group



Users Dialog

GENERAL Tab

In this tab you will find the information about special users in the system. This will include users who are allowed to manage the CompletePBX system, as well as users who have access to the Portal.



Login Name*, user name that you will use to login to the system.

Password*, the password that this user will use to login to the system. If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password.

Profile*, the user profile to be associated with this user. This determines the security rights of the user within the system. You can use the User Profiles dialog to manage the rights that are associated with each profile.

Note that with the exception of the built-in Administrator user, all other users are not able to modify their Profile. Only the user who created the user has access to the Profile dropdown.

Startup Dialog*, set the dialog that will shown when the user logs into the system.

Full Name, full, real name, of the user.

Department, user department (Example: System Admininstrators).

Require Change Password, set to **Yes** to Require the user to change password after his next login.

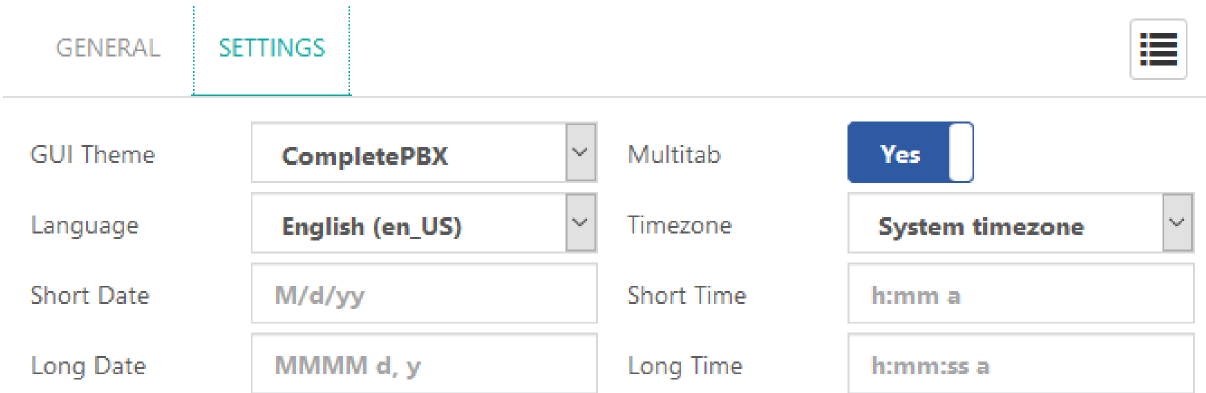
Select Image, image which will be associated with the user. Can be an avatar**,** graphic**,** or a photo of the user.

If you have lost the password for the **admin** user, you can login to the Linux system and run the command ***/usr/share/ombutel/scripts/reset_ombu_password***

After doing this, you will be asked to create a new **admin** password next time you access the web login dialog.

SETTINGS Tab

In this tab you will be able to manage the user's themes and settings.



GUI Theme, choose a theme from the drop-down list – this determines the theme that will be used for displaying the user interface. This change will only take effect after your next login to the system.

Language, choose a language from the drop-down list – this determines the language that will be used in the user interface. This change will only take effect after your next login to the system.

Short Date, the format that will be used to display short dates. The default value is taken from the system setting of the CompletePBX 5 machine. Refer to Formatting Conventions for available options.

Long Date, the format that will be used to display long dates. The default value is taken from the system setting of the CompletePBX 5 machine. Refer to Formatting Conventions for available options.

Multi-tab, enable if you want multiple tabs to be displayed in the user interface. This change will only take effect after your next login to the system.

Timezone, the timezone that should be associated with this user. This change will only take effect after your next login to the system.

Short Time, the short format that will be used to display timestamps. The default value is taken from the system setting of the CompletePBX 5 machine. Refer to Formatting Conventions for available options.

Long Time, the long format that will be used to display timestamps. The default value is taken from the system setting of the CompletePBX 5 machine. Refer to Formatting Conventions for available options.

Formatting Conventions

You can modify date settings by using the following placeholders:

- yy to represent a two-digit year, e.g. 18
- yyyy to represent a four-digit year, e.g. 2018
- m to represent a one-digit month for months below 10, e.g. 4
- mm to represent a two-digit month, e.g. 04
- mmm to represent a three-letter abbreviation for month, e.g. Apr
- mmmm to represent a month spelled out in full, e.g. April
- d to represent a one-digit day of the month for days below 10, e.g. 2
- dd to represent a two-digit day of the month, e.g. 02
- ddd to represent a three-letter abbreviation for day of the week, e.g. Tue
- dddd to represent a day of the week spelled out in full, e.g. Tuesday

You can modify time settings by using the following placeholders:

- h to represent a one-digit hour for values below 10, e.g. 4
- hh to represent the hour in a two-digit format
- HH to represent the hour in 24-hour format
- m to represent a one-digit minute for values below 10, e.g. 4
- mm to represent the minutes in a two-digit format
- s to represent a one-digit second for values below 10, e.g. 4
- ss to represent the seconds in a two-digit format

Separators of the components:

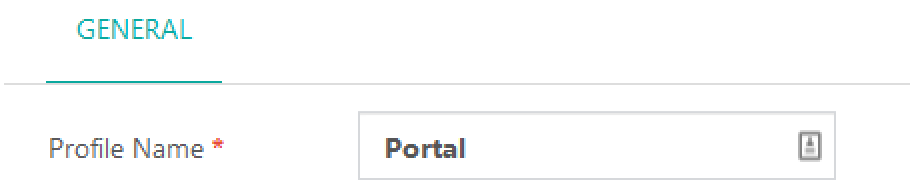
- "/" to represent a slash

- "." to represent a dot
- "-" to represent a hyphen or dash
- " " to represent a space
- “:” to represent a colon

User Profiles Dialog

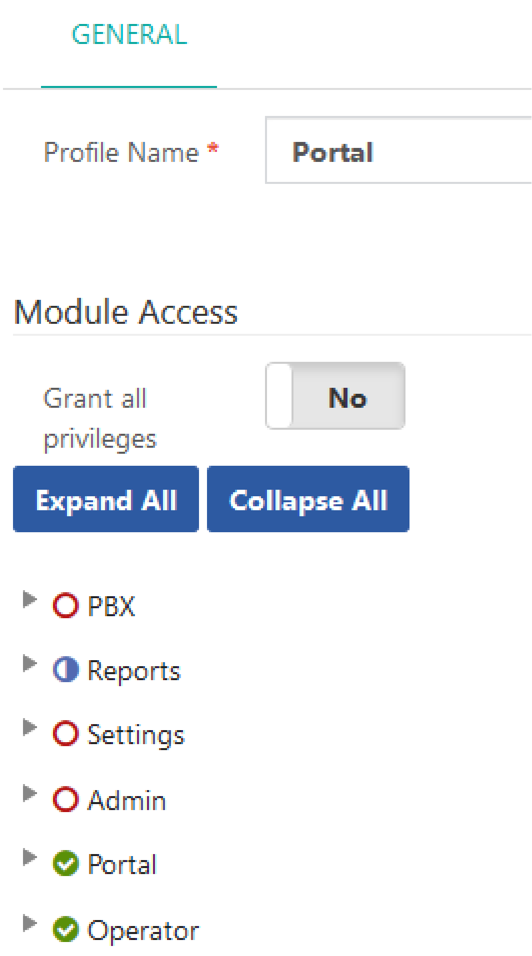
GENERAL Tab

Using this tab, you will be able to manage user profiles.



Profile Name*, free-text name for this profile.

Module Access section



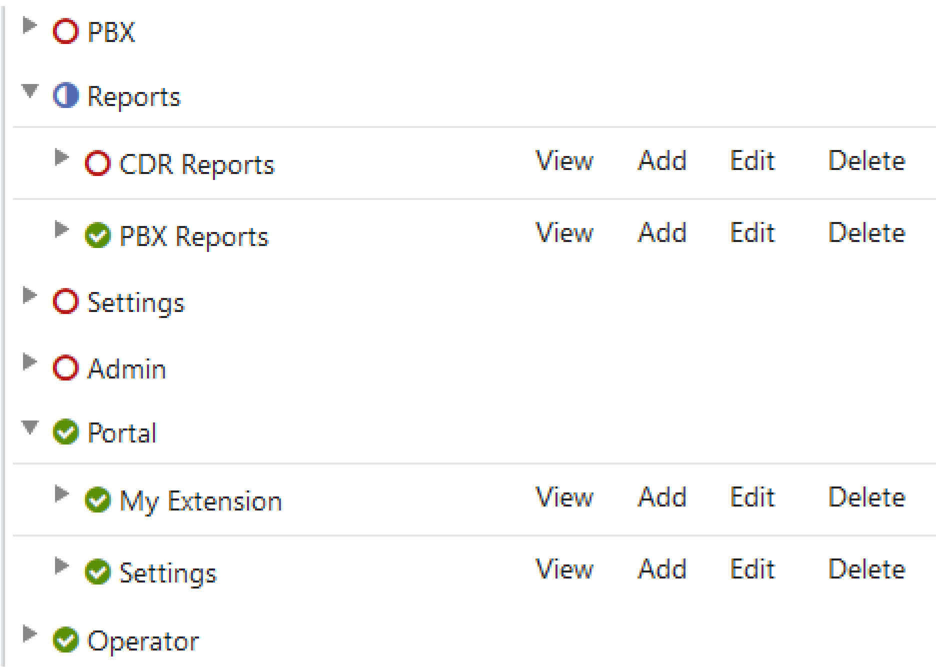
- **Grant Privileges,** set to **Yes** to allow access to all dialogs.
- **Expand All**, click on this button to see the full list of available permissions.
  - o You can click on the arrow beside the name of the menu group to open the list of available options for the menu group.
  - o You can toggle the permissions for an entire menu group by clicking on the (red or green) circle beside the name of the menu group.

You can configure action-level permissions for each item, allowing the user to view, add, edit, or delete items in the appropriate dialog. Three different icons indicate the status:

Indicates no access to the Menu Group, Menu Set, or Dialog

Indicates partial access to the Menu Group or Menu Set

Indicates full access to the Menu Group, Menu Set, or Dialog



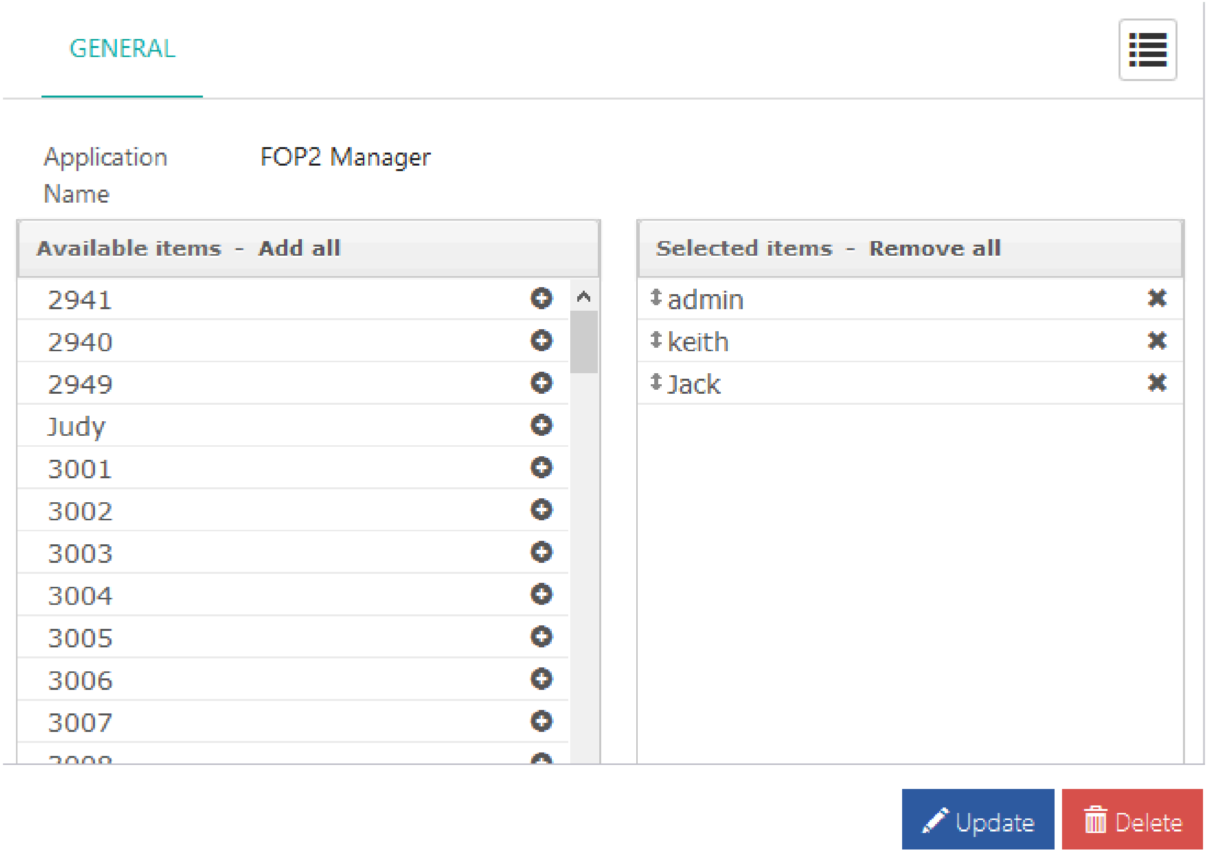
Note that access to Admin>Admin>User Profiles cannot be denied for the Super Administrator

Application Access Dialog

Allows system administrator to control user access to specific applications or modules.

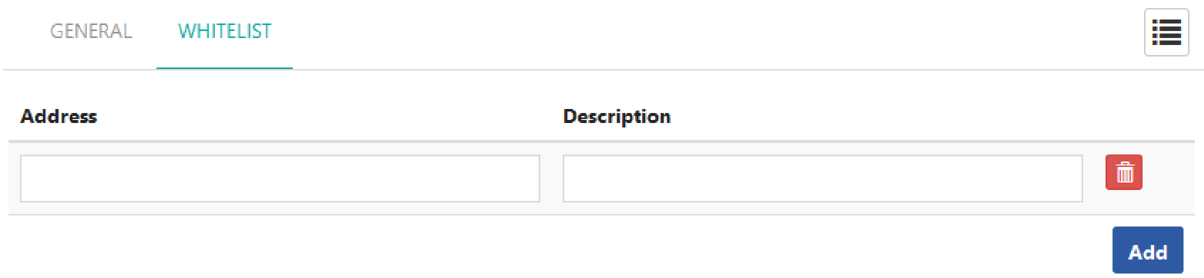
Use the Show All button the right-hand side of the dialog to see the list of available applications

GENERAL Tab



WHITELIST Tab

Allows you to configure access to the application according to IP Address.



Backup & Restore Dialog

This dialog allows the system administrator to create a backup of the current CompletePBX 5 system, or to restore a previously-created backup.

By default, the backup files will be stored in the `/var/lib/ombutel/static/backups` directory. However, you can modify this default in the Admin>System Settings>System Misc dialog.

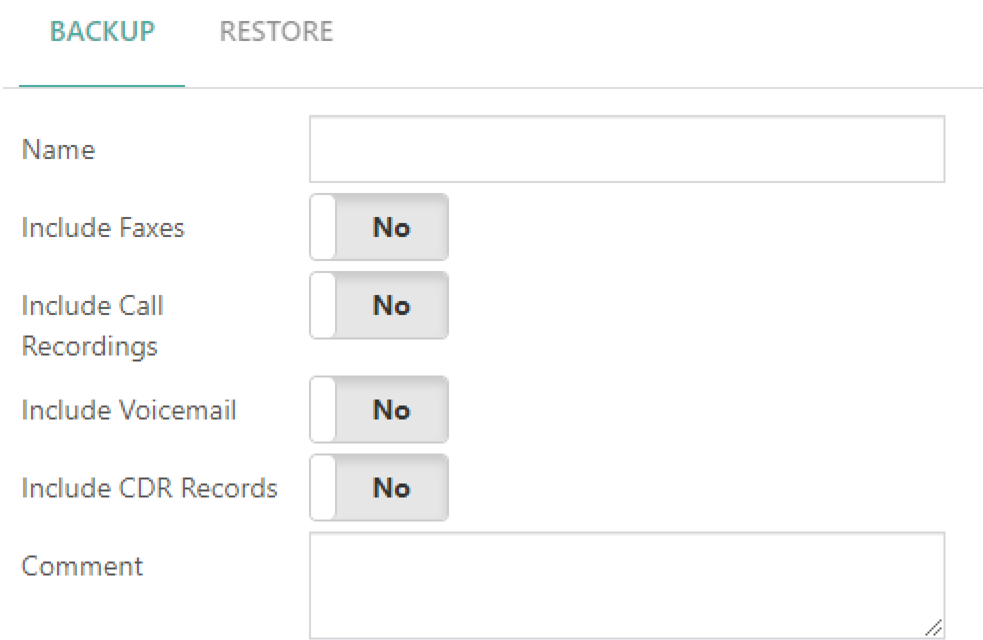
The backup will save the configuration information required in order to restore the PBX database. The backup does not include the operating system, or configuration information for any third-party applications that may be integrated into the system.

However, the following data that is configured from the CompletePBX 5 user interface will be restored:

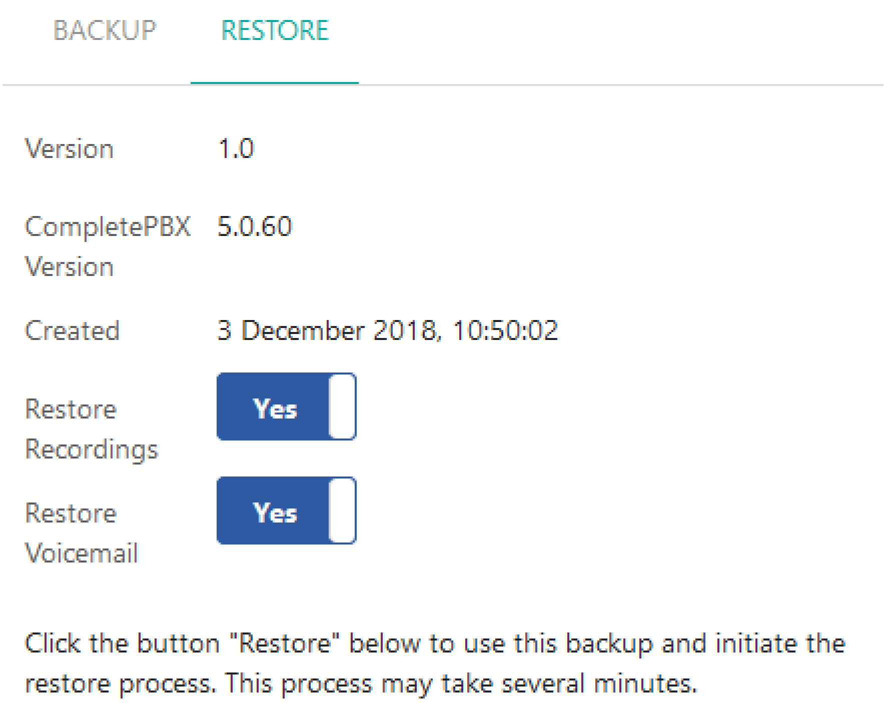
- NTP configuration
- Mail configuration
- User-created asterisk conf files residing in the /etc/asterisk/ombutel directory. If you have modified any conf files that are part of the standard CompletePBX 5 system, these will be overwritten by the restore process.

You can use Rapid Recovery to create a full ***system*** backup that includes the entire operating system – see details in Rapid Recovery.

BACKUP Tab



Name, allows you to add a free-text name to identify the backup set. If you do not give the backup set a name, the system will automatically create one based on the current timestamp, in a format like **03-12-2018, 10:50:02**. The backup file will include metadata, such as the Serial Number and the Version. This information will be displayed when you select a backup file for restore, like this:



Include Faxes, allows you to save backup space by determining whether the backup set should include faxes.

Include Performance, allows you to save data from the Wallboard application.

Include Call Recordings, allows you to save backup space by determining whether the backup set should include recordings. Backing up recordings will back up all the voice prompts and custom Music on Hold recordings. Without this backup, prompts for IVRs, follow-me, queues, and Music on Hold recordings will all have to be re-recorded or re-uploaded after a system failure.

Include Statexplorer, allows you to save data from the StatsExplorer application.

Include Supervision, allows you to save data from the Supervision application.

Include Voicemail, allows you to save backup space by determining whether the backup set should include voicemail recordings. Backing up voicemail will back up all the voicemail messages stored in the system.

Include CDR Records, allows you to save backup space by determining whether the backup set should include CDR records. Backing up CDR data will back up all the call detail records stored on the system. Without this backup all CDR records will be lost if the system needs to be rebuilt. There is no way to recover CDR records without this backup.

Comment, allows you to add free-text to help identify the purpose of the backup.

Click the **Backup** button at the bottom of the dialog in order to create a backup. The backup set, by default, will be stored in the `/var/lib/ombutel/static/backup` directory.

Click on the Show All icon at the right-hand side of the menu to see all backups that are currently stored on the server.

You can use the **Download** action button to save a copy of the backup file to your local machine.

Backup from the Command Line Interface

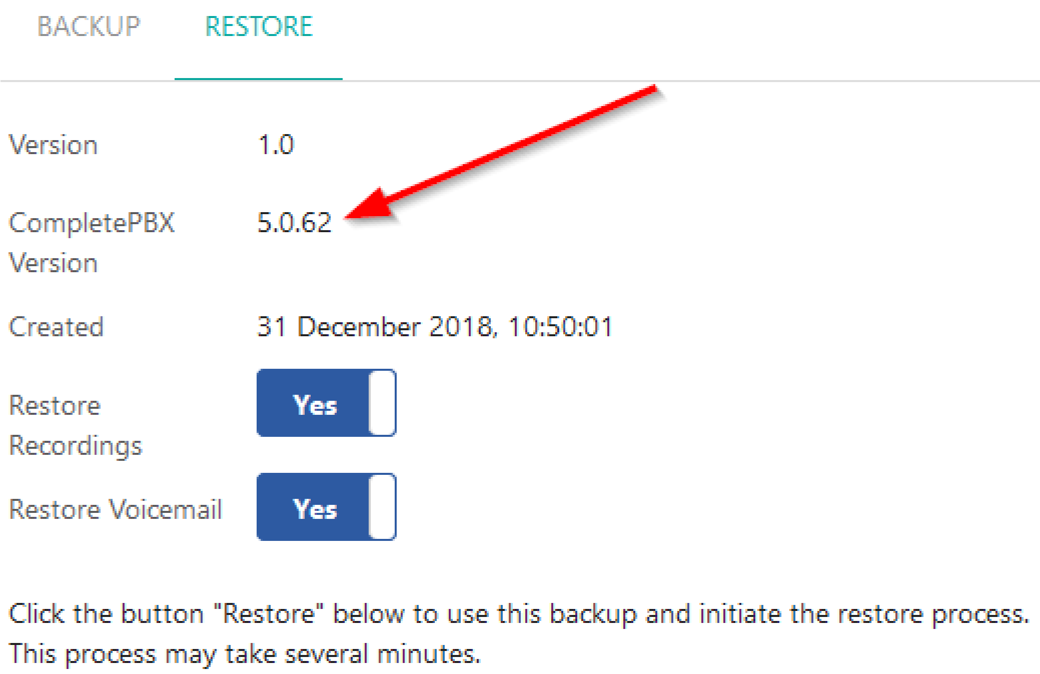
Backup can be activated from the CLI, by using the backup script that is located in the **/usr/share/ombutel/scripts** directory. The following parameters can be used:

- **-all** do a full backup – this is the same as using –rec, -vm, -fax, and –cdr parameters
- **-n** user-defined name for the backup file
- **-c** include free-text comment
- **-rec** backup recordings
- **-vm** backup voicemails
- **-fax** backup faxes
- **-cdr** backup CDR records
- **-d** write backup to a user-defined directory, using filemame automatically created by the system. The automatic format is <CompletePBX 5 system name>_<CompletePBX 5 version>_<timestamp>.tar

Example:

```
/usr/share/ombutel/scripts/backup -all -d /root/ -c 'Full backup'
```

RESTORE Tab



Select a backup set by opening the Show All icon on the right-hand side of the menu. If the details confirm that you are looking at the correct backup set, click on the **Restore** action button.

If the version of the backup set and the currently installed version of CompletePBX 5 do not match, the system will automatically run a script to ensure that the version of metadata in the database matches the version of data in the database. (If they did not match, it is possible that database fields in the backup set would not match the database fields in the currently-running CompletePBX 5 system.)

The system will block restore operations when the backup was created on a newer CompletePBX version than the currently installed system. To proceed with the restore, you must first upgrade the system to the same or a newer version than the backup.

Restore from the Command Line Interface

Restore can be activated from the CLI, by using the restore script that is located in the **/usr/share/ombutel/scripts** directory. The following parameters can be used:

- **-all** do a full restore – this is the same as using –rec, -vm, -fax, and –cdr parameters
- **-rec** restore recordings
- **-vm** restore voicemails
- **-fax** restore faxes
- **-cdr** restore CDR records

- **<filename>** the name of the file to be used for the restore – this parameter is mandatory.

Example:

```
/usr/share/ombutel/scripts/restore -all
/root/test-vm_5_1_4_20191220_083030.tar
```

Maintaining and Protecting Backups

The way in which the system provides backups is simple and effective, but requires consideration of two factors: storage and protection. The backup data must be properly maintained or the system will eventually run out of space and cease to function. Make sure that your backup procedures include periodic deletion of old backup sets, to prevent your system from running out of disk space.

Once the problem of backup maintenance is taken care of, the problem of backup protection still exists. The backups taken by the system reside on the server itself. If the hard disk crashes or the local backup becomes corrupted, there will be no way to restore a failed system. Make sure that you periodically move sets of backup data from your server to another location. It is good practice to maintain copies of your backup at a different location, so ensure that are protected in case of some catastrophe such as fire or flooding.

Protecting Backups

There are a number of ways to protect backups. Each one may protect a particular deployment scenario better than the other. While the specifics of each protection scenario are outside the scope of this document, it is worth keeping them in mind when setting up backups to make sure that a backup is always close at hand. The most common methods for protecting backups are as follows:

Redundant hardware (specifically, hard disks in a RAID configuration)

Automating the copy of backups to an external hard disk or network location

Automating the copy of backups to an off-site backup server

Backup & Restore Plugin

Beginning with release v.5.1.13, the CompletePBX Backup/Restore module allows you to add custom plugins for backup/restore folders and databases that are not a part of CompletePBX. The plugin also allows you to perform backup, pre-restore, restore and post-restore actions.

A plugin consists of the following components:

- a PHP script that must be installed in the `/usr/share/ombutel/backup-scripts` folder
- one or more localization files that must be installed in the corresponding language folder: `/usr/share/ombutel/www/i18n/`<*language*>
  For example: `/usr/share/ombutel/www/i18n/en_US`

The Plugin Script

The PHP plugin script must be installed in the `/usr/share/ombutel/backup-scripts` folder.

This script must define a class that extends from the base class **backup_component**.

The base class **backup_component** provides defaults for the following public functions that are called by CompletePBX in order to perform various operations. Each function may be overridden as necessary.

Each function is described in the following table:

Function	Parameters	Return Value	Notes
name()	none	a string that contains the name of the backup component. The string can consist of letters, digits, dot (.), and minus (-) characters.	The returned string will be displayed as the optional component name in the Backup/Restore dialog when function **optional()** returns true.
optional()	none	**true** - the component is optional and the user can choose either to include or not this component in backup/restore **false** - the component will be unconditionally backed up or restored. The component will not be displayed as an option in the Backup/Restore dialog.	
requires()	none	Returns an array of other component names that must be enabled if this component is enabled.	The function is optional. You do not have to define it if the component doesn't have any dependencies.

Function	Parameters	Return Value	Notes
backup()	a string with the name of a temporary folder where you should create the archive file(s).	Returns either a tarball file or an array of tarball files.	This function is called by CompletePBX for performing the backup. The backup result may consist of one or more tarball files. For example, one tarball with a database dump and another with a folder content. In certain circumstances, a component doesn't require any additional backups besides the backups that are produced by the dependent components. In such cases, it is possible don't define this function.
pre_restore()	a string with the name of a temporary folder where the component tarball file(s) are extracted from the CompletePBX backup file.	none	This function is called by CompletePBX before restoring the components. For example, in this function, you can drop the database that is going to be replaced or execute some other actions if required. The function is optional.
restore()	a string with the name of a temporary folder where the component tarball file(s) are extracted from the CompletePBX backup file.	none	This function is called by CompletePBX for restoring the component data. In certain circumstances, a component doesn't require any additional backups besides the

Function	Parameters	Return Value	Notes
			backups that are produced by the dependent components. In such cases, you do not need to define this function.
post_restore()	a string with the name of a temporary folder where the component tarball file(s) are extracted from the CompletePBX backup file.	none	This function is called by CompletePBX after the archived tarballs have been restored. In this function, it is possible to run some other scripts that need to apply the new changes or modify the restored data according to the installed component version requirements. The function is optional.
drop_database()	database name string	none	Deletes the MySQL database defined in the parameter
backup_database()	• database name • gzip filename for the database dump	none	The function produces a gzip database dump file
restore_database()	• database name • gzip filename with the database dump		The function creates the database if it doesn't exist and then restores the database dump there.
backup_folder()	• folder name to be archived • the tarball filename • an array with the exclude filename	none	The function creates a tarball with the required folder content excluding the files with names that match the name

Function	Parameters	Return Value	Notes
	patterns that eventually will be added as one or more `tar` utility ' ● exclude <pattern>' parameters. This parameter is optional.		patterns defined in the third parameter.
restore_folder()	● tarball filename to be restored ● destination folder name ● an array with the exclude filename patterns that eventually will be added as one or more `tar` utility ' ● exclude <pattern>' parameters. This parameter is optional.	none	The function creates the destination folder if it doesn't exist and then expands the tarball inside of this folder. The files with names that match the 'exclude' patterns will not be restored.
exec()	a string with a command to be executed.	none	Note: The script/utility file that should be executed must have appropriate ownership and the execution bits set.

Example of a Plugin Script

The following is an example of a PHP script that can be used for optional backup/restore of a third-party component **Product1**. The script handles a database **prod1_db** and the **/var/lib/prod1_folder** folder.

```
<?php
class backup_product1 extends backup_component {
	static $database_name = 'prod1_db';
	static $folder_name = 'prod1_folder';
```

```
static $folder_full_name = '/var/lib/prod1_folder';

public function name() {
	return 'Product1';
}

public function optional() {
	return true;
}

// backup() returns the $archives array that contains the
// database gzip dump file name and the folder content tarball.
public function backup($tmpdir) {
	$archives[] = "{$tmpdir}/".static::$database_name.".sql.gz";
	$this->backup_database(
		static::$database_name,
		$archives
		);
	$dirname = '/var/lib/prod1_folder';
	if (file_exists(static::$folder_full_name)) {
		$archive = "{$tmpdir}/".static::$folder_name.".tar.gz";
		$this->backup_folder(static::$folder_full_name,
			$archive);
		$archives[] = $archive;
	}
	return $archives;
}

public function pre_restore($tmpdir) {
	$archive = "{$tmpdir}/".static::$database_name.'.sql.gz';
	if (file_exists($archive)) {
		$this->drop_database(static::$database_name);
	}
}

public function restore($tmpdir) {
	$archive = "{$tmpdir}/".static::$database_name.'.sql.gz';
	if (file_exists($archive)) {
		$this->restore_database($archive, static::$database_name);
	}
```

```
	}

	public function post_restore($tmpdir) {
		$post_restore = '/usr/share/my_product/scripts/post_restore';
		if (file_exists($post_restore)){
			this->exec($post_restore);
		}
	}
}

?>
```

Localization Files

The name of the component and the corresponding tooltips can be displayed in the Backup/Restore dialog in different languages. The texts in a particular language are configured in a file that must be copied to the `/usr/share/ombutel/i18n/`<*language*> folder. As the minimum, the file with texts in English must be copied to the `/usr/share/ombutel/i18n/en_US` folder. The file name can be arbitrary but in order to avoid the possible collisions with the existing files, we recommend to use the following file name schema: `backup_and_restore-`<*component name*>`.txt`

For example, for component **Product1** the file name could be: `backup_and_restore-Product1.txt`

The file must contain four lines:

backup_and_restore.include_<*component name*> = <*label of the option in the Backup dialog*>

backup_and_restore.include_<*component name*>.tooltip = <*tooltip of the option in the Backup dialog*>

backup_and_restore.restore_<*component name*> = <*label of the option in the Restore dialog*>

backup_and_restore.restore_<*component name*>.tooltip = <*tooltip of the option in the Restore dialog*>

where the <*component name*> is the string that the plugin script returns in the function `name()`.

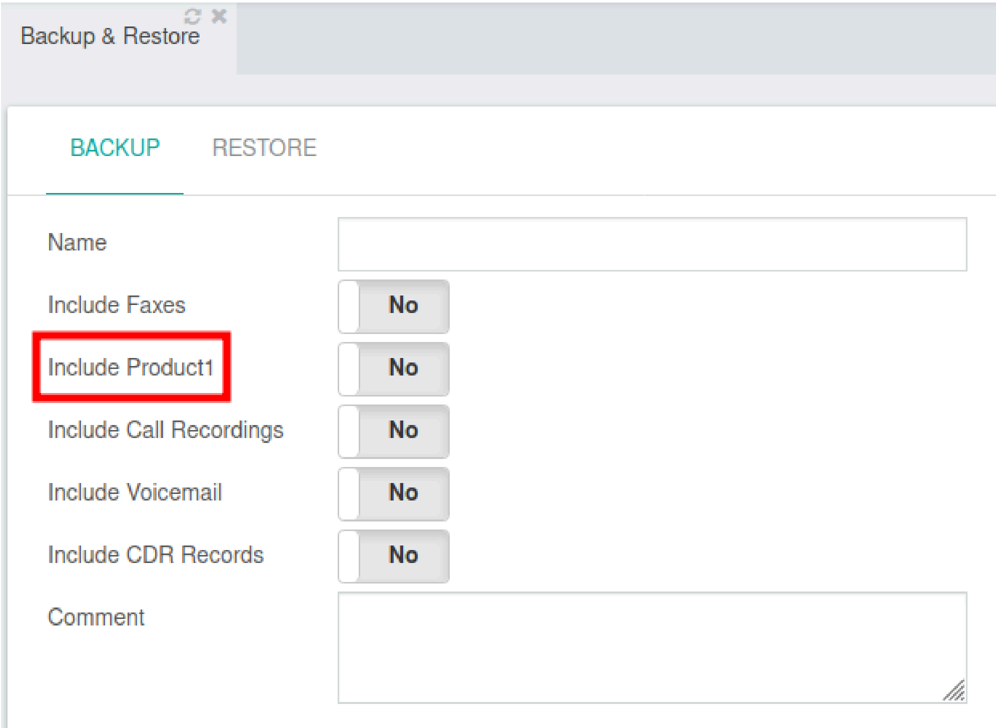
For example, if the function name() returns the **Product1** string then the file would contain the following lines:

```
backup_and_restore.include_Product1 = Include Product1
```



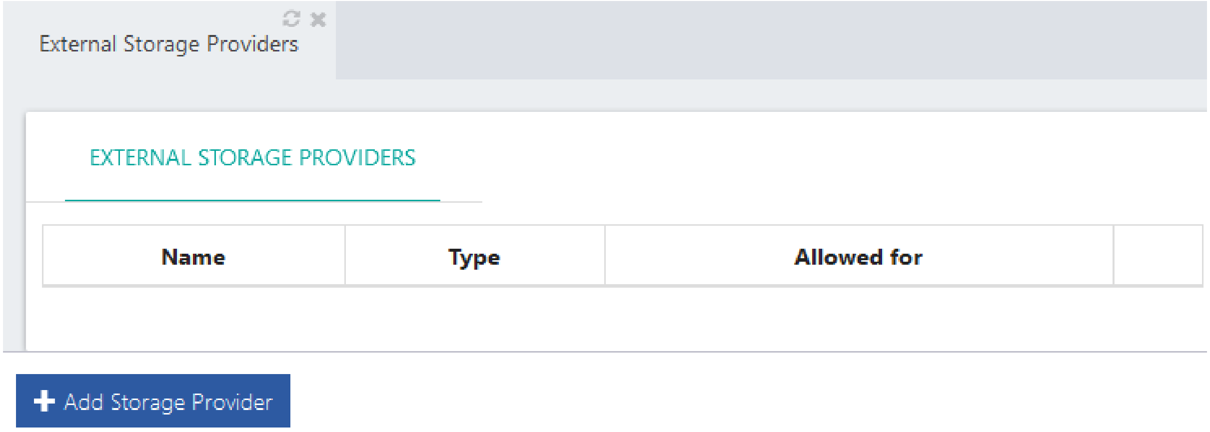
```
backup_and_restore.include_Product1.tooltip = Enabling this will add Product1 to the backup
backup_and_restore.restore_Product1 = Restore Product1
backup_and_restore.restore_Product1.tooltip = Enabling this will replace existing Product1 data with those contained in this backup
```

Then, in the Backup/Restore dialog, you will see and additional field, like this:



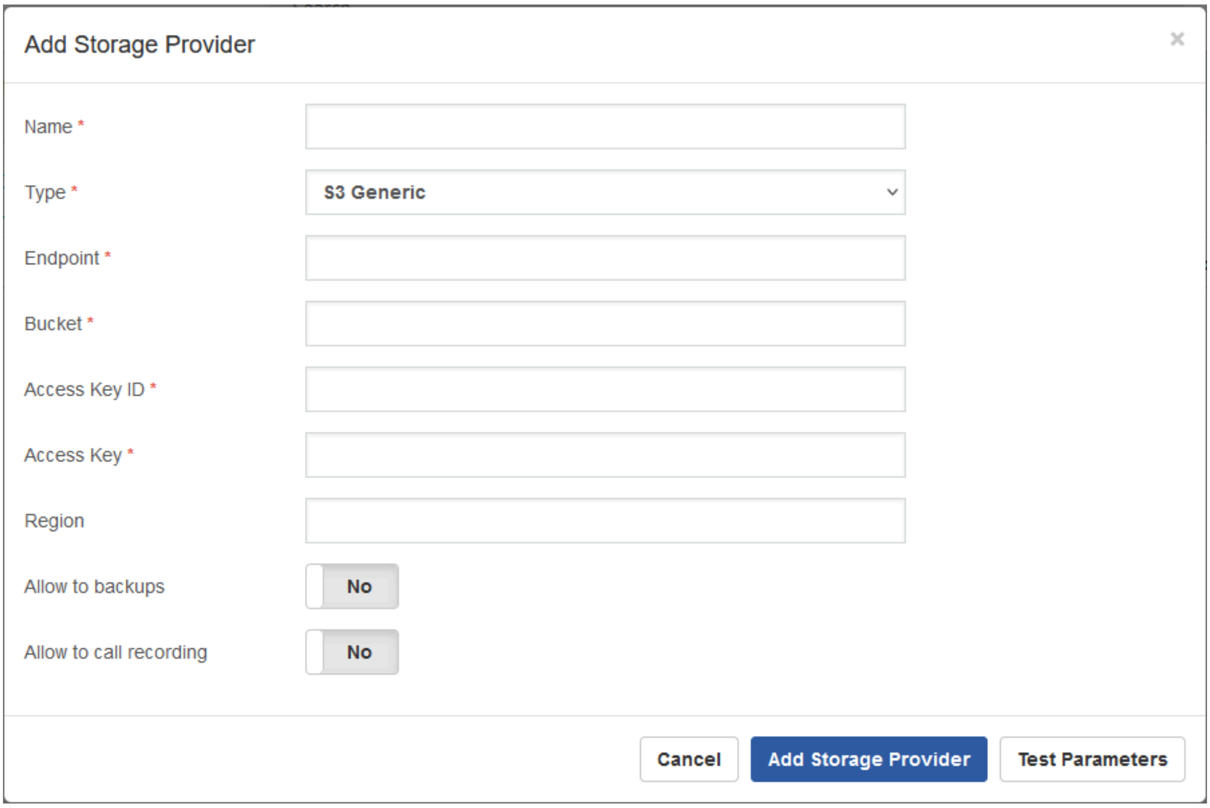
External Storage Providers Dialog

This dialog allows the management of remote resources. The module enables configuring remote storage locations to be used in other modules. External storage can be used by Backup & Restore, CDR Settings, and Call Recording modules.



Add Storage Provider, by clicking this button a dialog will show up to set up the storage provider parameters:
Name *, unique name for this storage provider. This is a free-text field.
Type *, select a storage provider type between **S3 Generic** and **SFTP**.

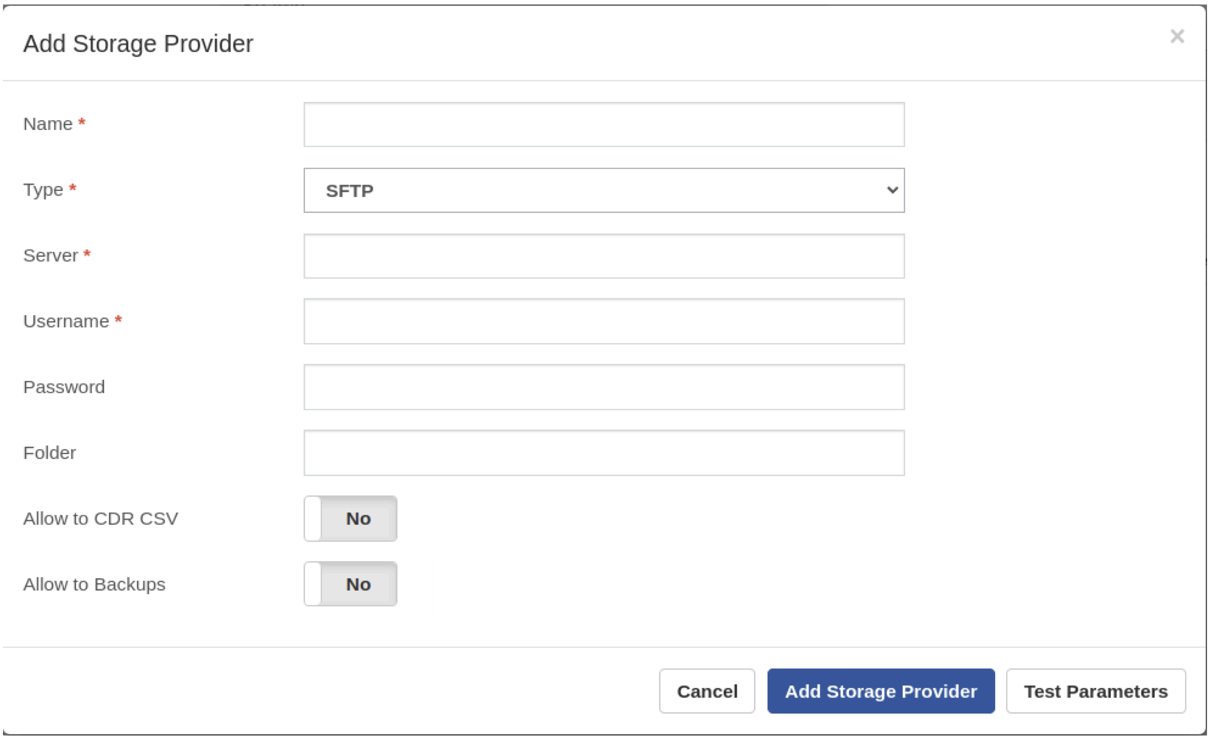
S3 Generic Option



(**NOTE** that this option can be used for both backups and call recording files.)
Endpoint *, URL of the server and/or cluster on which the bucket is located.
Bucket *, name of the bucket.
Access Key ID *, the required access key ID (username) to use.
Access Key *, the required access key (password) to use.

Region, optional region, required for some providers such as Amazon AWS, CloudFlare and others.
Allow to backups, when set to **Yes**, this storage provider can be used to store and retrieve backups. You can select this storage provider as a Target in the Backup & Restore module.
Allow to call recording, when set to **Yes**, this storage provider can be used to store and retrieve call recordings. You can select this storage provider as a Destination in the Call Recording module.

SFTP Option



(**NOTE** that this option can be used for CDR file uploading as well as to store and retrieve backups.)
Server *, specifies the IP address or hostname of the server. An optional port number may be included.

Username *, the required username for accessing the server.

Password, the optional password for accessing the server.

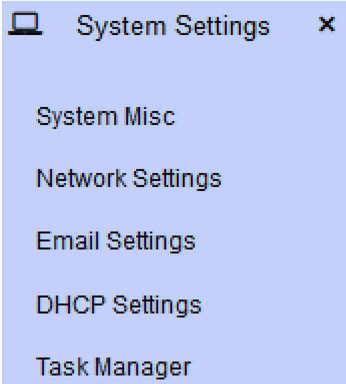
Folder, specifies the folder on the remote server where files will be uploaded. The following variables are recognized and will be substituted: $SERIAL - PBX Serial number $HOSTNAME - PBX Hostname.

Allow to CDR CSV, if enabled, this storage provider can be used to upload CDR records as CSV.

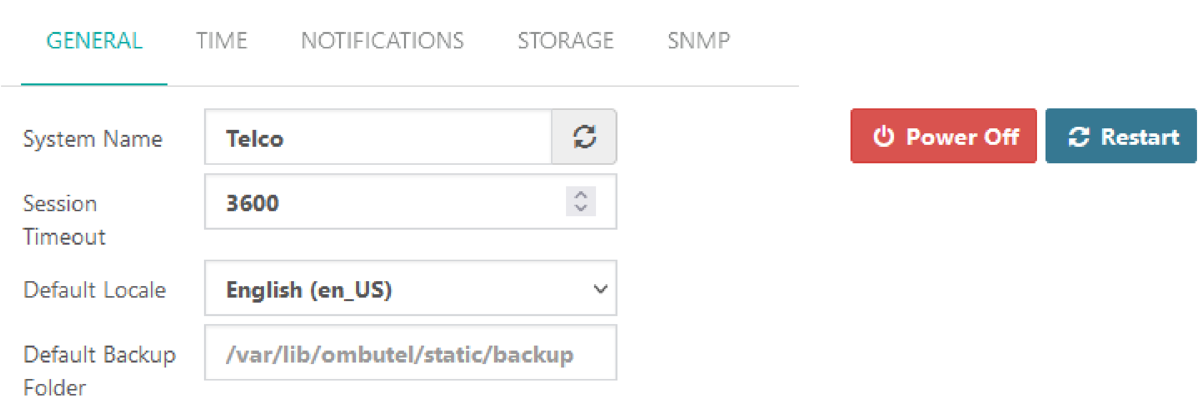
Allow to backups, when set to **Yes**, this storage provider can be used to store and retrieve backups. You can select this storage provider as a Target in the Backup & Restore module.

Use the **Test Parameters** button at the bottom of the dialog to optionally verify the entered parameters or the **Add Storage Provide**r button to save the storage provider.

System Settings Menu Group



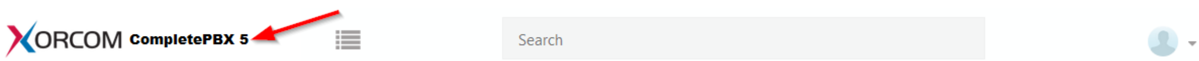
System Misc Dialog



System Name, allows you to configure a descriptive name for the CompletePBX 5 system.

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

For hardware-based CompletePBX 5 systems, the default value for this field will be the serial number of the physical (or virtual) dongle that is connected to your system. The System Name will now appear in your web browser like this:



Do not confuse the **System Name**, which is used by CompletePBX 5 to describe the system, with the **hostname**, which is used to by external networking tools.

The network hostname can be configured in Network Settings dialog.

Session Timeout, time, in seconds, that controls the timeout of idle sessions in the user interface.

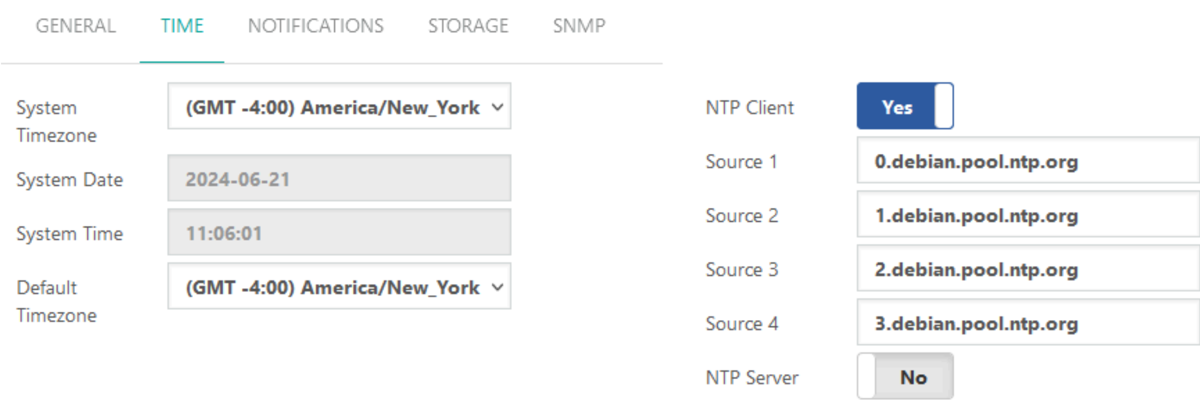
Default Locale, locale to use when no other locale is available.

Default Backup Folder, the folder in which system backups and restores will be stored. The default folder is `/var/lib/Ombutel/static/backups`

clicking on the Power Off button will completely shut down the PBX server. (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

clicking on the Restart button will cause the PBX server to shutdown**,** before performing a restart. (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

TIME Tab



System **Time Zone,** shows the actual time zone on server. You can change this setting and click on Save to update the system.

System Date, shows the current date of the system. You can change this setting and click on Save to update the system.

System Time, shows the current time of the system. You can change this setting and click on Save to update the system.

Default Timezone, timezone to use when no other timezone is available.

NTP Client, indicates whether to activate the NTP (Network Time Protocol) service for synchronizing the system clock.

Source 1, is the first hostname or IP address to be used as the NTP service

Source 2, is the second hostname or IP address to be used as the NTP service

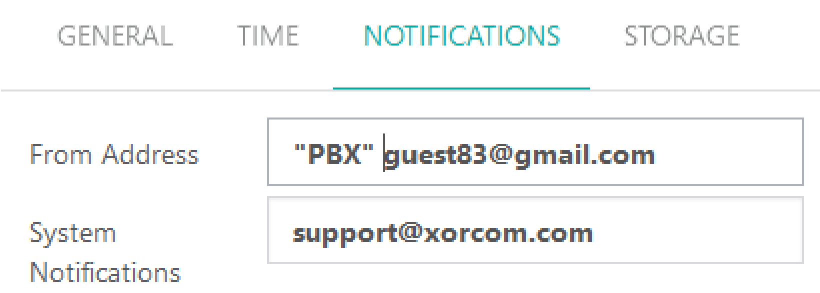
Source 3, is the third hostname or IP address to be used as the NTP service

Source 4, is the fourth hostname or IP address to be used as the NTP service

NTP Server, indicates whether the CompletePBX 5 system provides NTP service, by acting as an NTP server. (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

Clock Status, shows the current date and time settings for the PBX server. Click on the Refresh button to see all the current system settings.

NOTIFICATIONS Tab



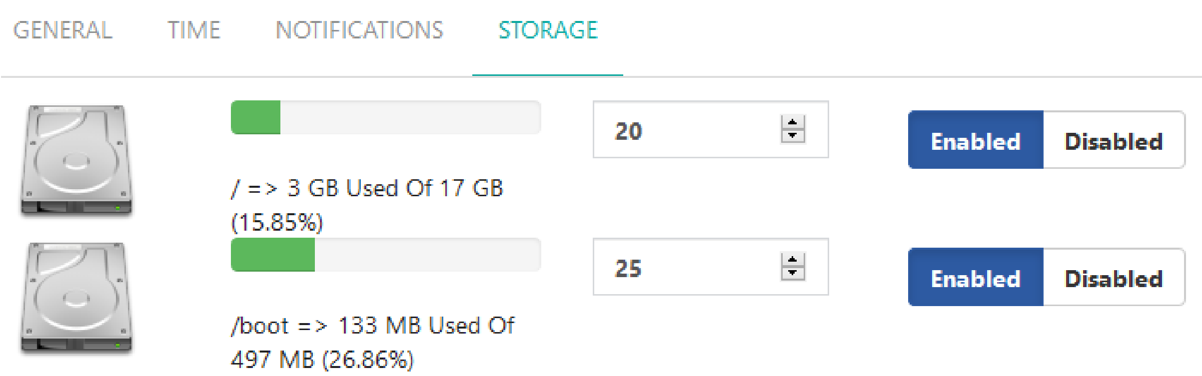
From Address, the email address entered here will be used as the **From:** field for emails sent by the system. You can also set the "From" name for email notifications.

System Notifications, notifications will be sent to the email address entered here. For example, a notification will be sent if your hard drive is low on space or if the RAID is not working correctly.

STORAGE Tab

Provides visual information about the capacity and utilization of all mounted storage devices on your system.

For each device**,** you can configure the utilization threshold for notifications. An email notification will be sent when the utilization is greater than the configured value.

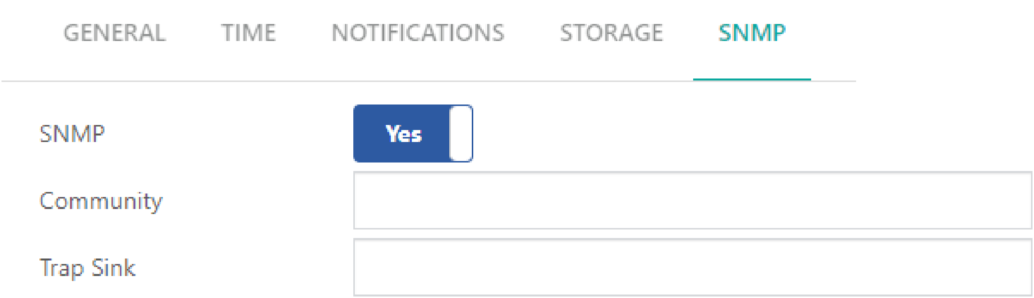


Notifications can be enabled, or disabled, for each device by clicking on the appropriate button associated with the device.

SNMP Tab

Allows CompletePBX to be polled from an external SNMP monitoring system.

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)



SNMP, toggle that allows you to enable/disable SNMP on the CompletePBX 5 system. Ensure that the firewall allows access to UDP port 161 if you want to enable remote SNMP monitoring.

Community, defines the SNMP community this host belongs to.

Trap Sink, defines the host address to which traps should be sent

Network Settings Dialog

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

The Network Settings dialog allows you to configure the network environment of the PBX server.

Be aware that changing network settings may require the network service to be restarted.

If you are making these changes remotely, you may lose network connectivity to CompletePBX 5.

What is a Private IP Address?

When you send a letter from your house to a friend, you have to know the address to send it to so that the postman knows which street and which house to take it to. Computer networks such as the Internet are no different, except instead of sending your Web traffic to a street address, your computer's "location" is known by its IP address.

You system has to have its own unique IP address so that it will only receive the information that is meant for it. However, there is a problem with networked computers that are linked to a router, and share the same external IP address.

In this instance, the router—once it has established its Internet connection through an Internet Service Provider—sends data to each individual device on that network based on the Network Address Translator (NAT).

The organization that gives out IP addresses to the world reserves a range of IP addresses for private networks. Private networks can use IP addresses anywhere in the following ranges:

- 192.168.0.1 - 192.168.255.254 (65,536 addresses)
- 172.16.0.1 - 172.31.255.254 (1,048,576 addresses)
- 10.0.0.1 - 10.255.255.254 (16,777,216 addresses)

The assumption is that these private address ranges are not directly connected to the Internet, so the addresses don't have to be unique. These private address ranges are used for the protected network behind network translation devices.

Because the private address ranges in a network don't have to be synchronized with the rest of the world, the complete address range is available for any network. A network administrator using these private addresses has more options for *subnetting*, and can use many more assignable addresses.

These blocks of addresses can be used by anyone, anywhere. Even if your neighbor is using the exact same addresses, it won't cause a problem. This is possible because these addresses are known as non-routable addresses. The network devices on the Internet are programmed to recognize these addresses. These devices will recognize that these are private addresses belonging to your network and will never identify the private address of a device on the Internet.

You do need to obtain one real address from the general pool so that your modem can be accessed. The modem uses NAT, a process in which your modem changes your private IP Address into a public one so that it can send your traffic over the Internet, keeping track of the changes in the process. When the information comes back to your router, it reverses the change—from a real IP address into a private one—and forwards the traffic back to your computer.

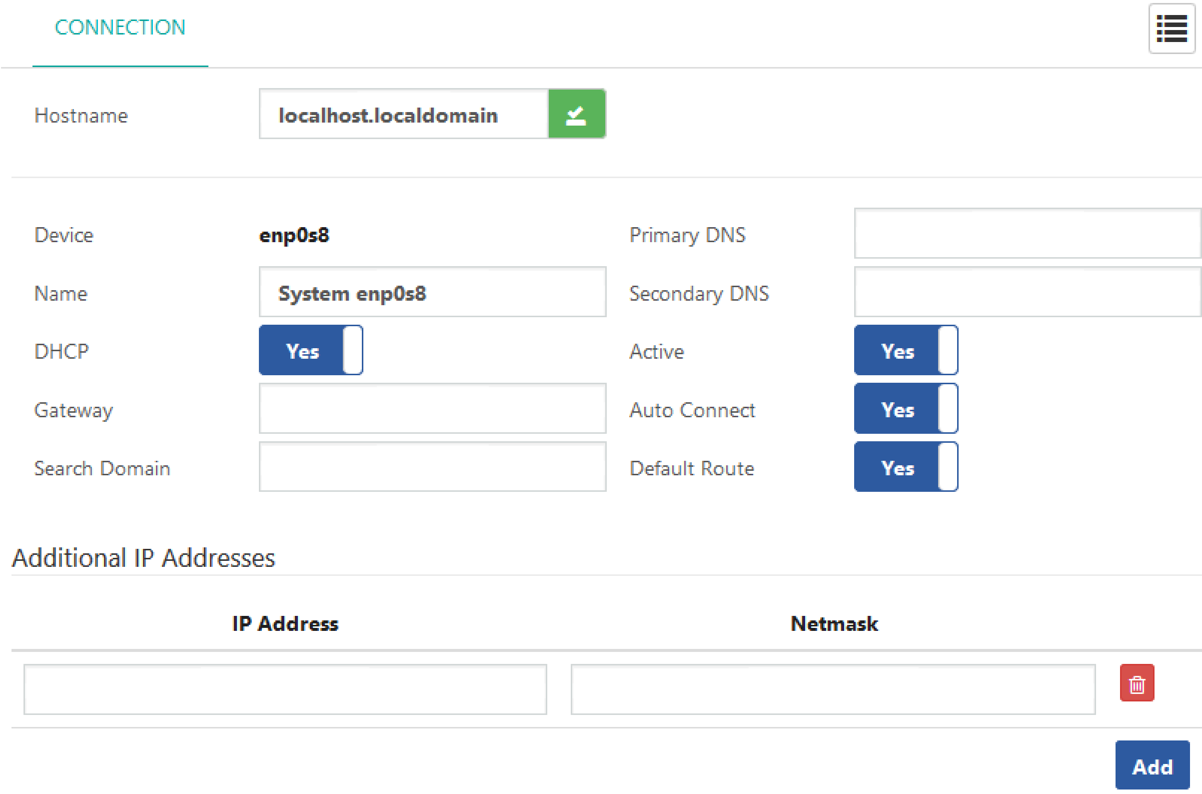
A typical network modem/router keeps two IP addresses: one for local devices to connect to across the local area network (LAN), and one for the external or wide area network (WAN) Internet connection.

The internal LAN-IP address is normally set to a default, private number. No matter the brand of router, its default internal IP address will be listed in the manufacturer's documentation. Administrators have the option to change this IP address during router setup, or at any time later.

The external IP address of the modem is set when the modem connects to the Internet Service Provider (ISP). This address should be shown in the administrative console of the modem.

CONNECTION Tab

In this tab you will find the information about Network Settings of your system.



Hostname, hostname of the system.

Device, name of the connection, such as eth0, eth1, etc.

DHCP, whether to use DHCP on this connection for obtaining network configuration. If set to **No**, you can configure the IP Address and mask for the PBX, using the following fields:

- **IP Address,** static IP address to assign for the PBX.
- **Netmask,** network mask or prefix.

Gateway, gateway IP address to use.

Search Domain, restrict DNS searches to the specified domain.

Primary DNS, primary DNS IP address. If this field is left blank, the DNS server defined on your modem will be used.

Secondary DNS, secondary DNS IP address. If this field is left blank, the DNS server defined on your modem will be used.

Active, whether this connection is currently active**.**

Auto Connect, whether to automatically connect on startup.

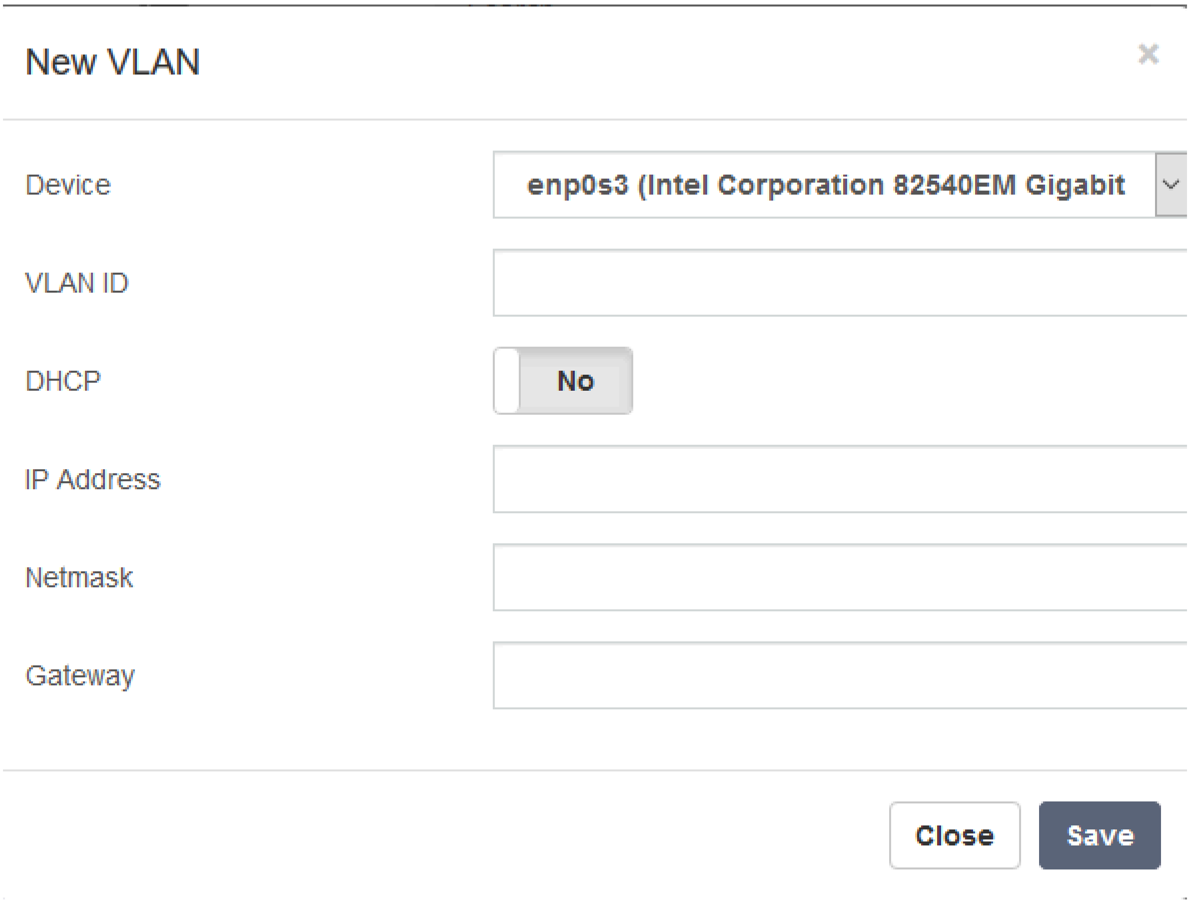
Default Route, whether to use this gateway as the default route.

Additional IP Addresses

Using the IP Address and Netmask fields allows you to associate additional IP addresses with your PBX.

Add VLAN Action Button

Click on this action button to configure a VLAN ID for this connection.



Device, select a physical network device from the drop-down list of available devices.

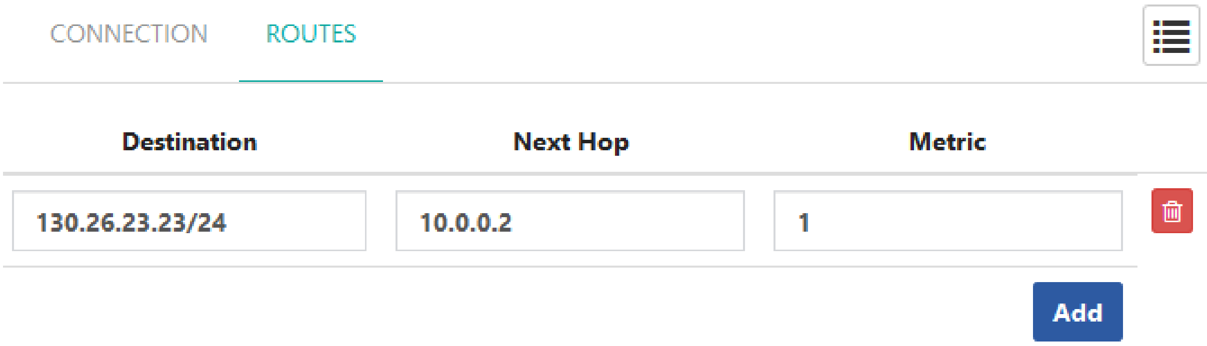
VLAN ID, VLAN to use for this connection.

DHCP, set to **Yes** to automatically obtain IP Address and Netmask from the DHCP server. If set to **No**, you can manually configure:

- **IP Address,** IP address to assign to this connection
- **Netmask,** netmask to assign to this connection.

Gateway, gateway to be used by this connection.

ROUTES Tab



This dialog allows you to configure static routes for CompletePBX 5. Static routes provide more routing information to your router. Typically, you do not need to add static routes unless you have multiple routers or multiple IP subnets on your network. However, defining static routes can make the connection with some SIP providers easier and more reliable.

Destination, specifies a valid CIDR address of the destination network. You will need to provide a subnet mask.

Next Hop, this parameter provides the IP address of the gateway that should be used to reach the destination network

Metric, a number to indicate the relative priority of the static route: the lowest number will have the highest priority.

Email Settings Dialog

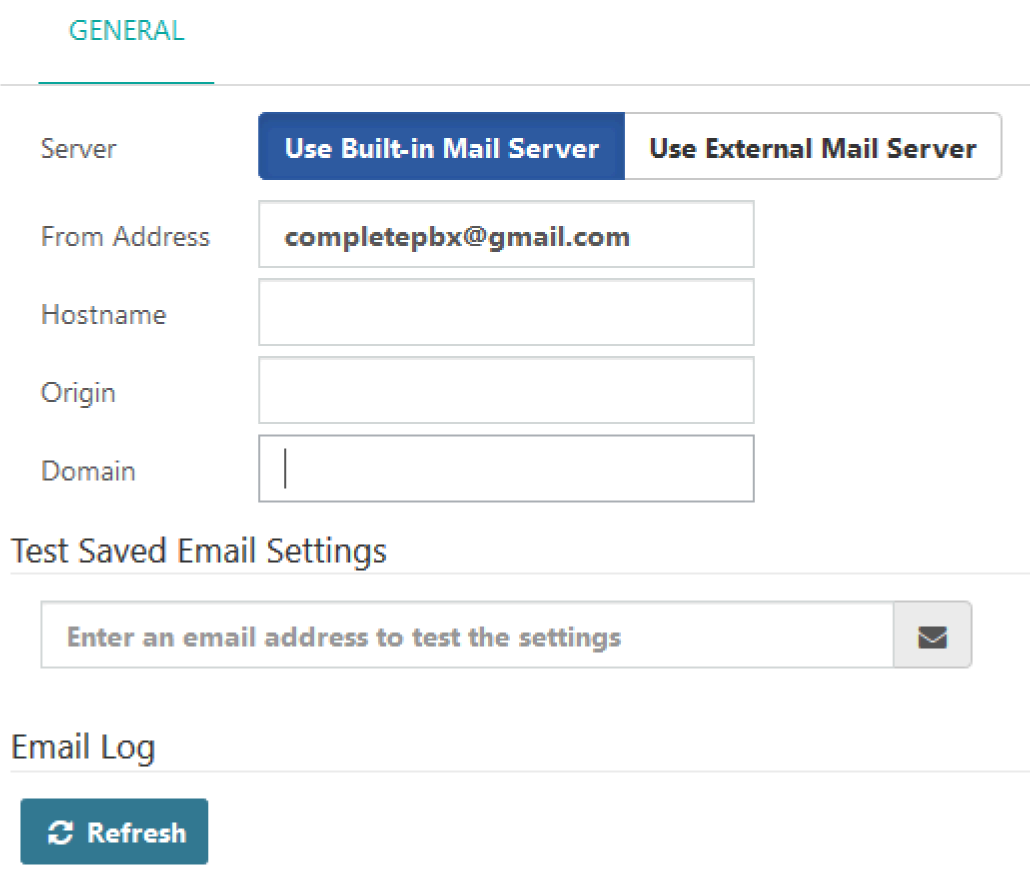
Email settings allow you the option to send outbound email messages either by using the built-in mail server (such as Postfix) that is active on the PBX server**,** or by using a network-accessible relay server that is hosted on another machine. Press on Use Built-in Mail Server to use the built-in mail server that is active on PBX**,** or Use External Mail Server to use a network-accessible relay server.

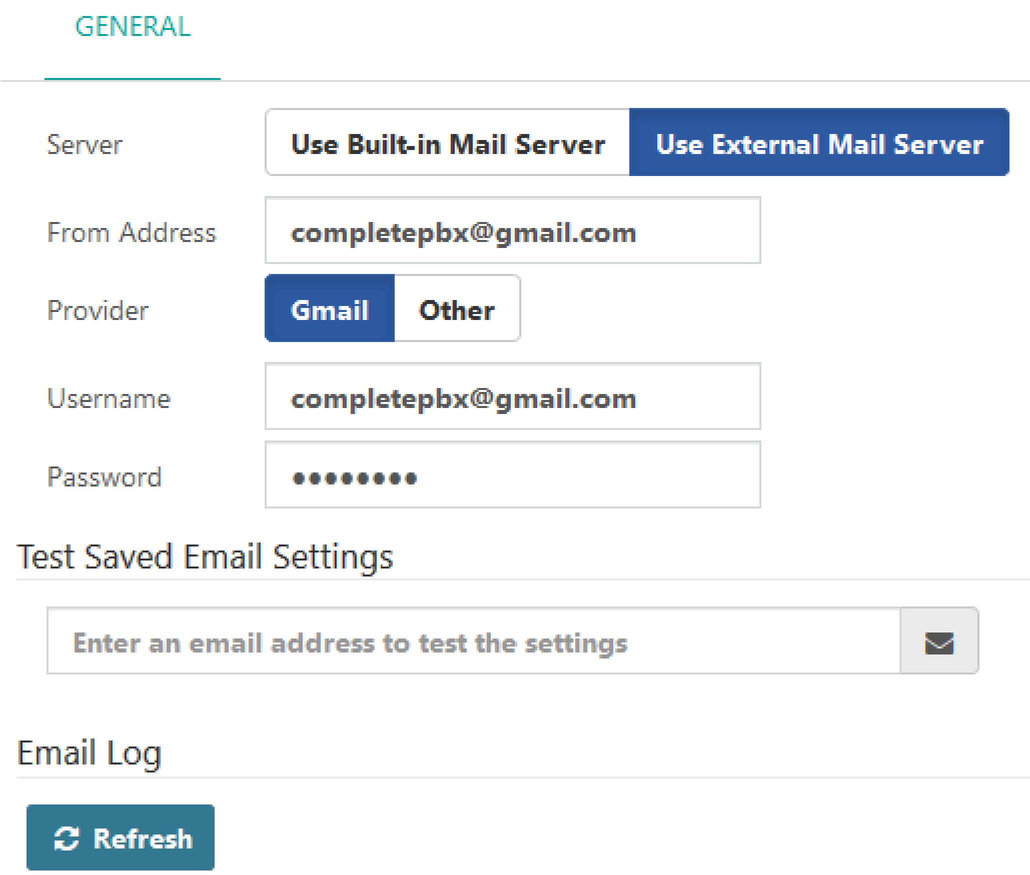
Email in CompletePBX 5 is used to deliver both system management messages and information to extension users:

- Licensing Status warnings and alerts
- Warnings when available disk storage drops below user-defined threshold
- Alerts from the Intrusion Prevention module containing details of invalid logins
- Various other system alerts originating from Asterisk or TwinStar (if configured.)
- Voicemail to email
- Fax to email

GENERAL Tab

In this tab you will find the information about email settings.


GENERAL
Server
Use Built-in Mail Server
Use External Mail Server
From Address
completepbx@gmail.com
Hostname
Origin
Domain
Test Saved Email Settings
Enter an email address to test the settings
Email Log
Refresh



Server, you can relay outbound email messages either by using a built-in mail server (such as Postfix) that is active on the system, or by using a network-accessible relay server that is hosted on another machine.

From Address, the default address that should be shown as the sender of emails.

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. (Not required for Gmail.)

Port, SMTP server port number. By default**,** port 25 is used. (Not required for Gmail.)

Origin, specifies the origin domain for outgoing email. By default, origin is configured as your server hostname, e.g. pbx.mycompany,com. Some mail servers do a reverse lookup to authenticate email client, so you need to make sure that the origin that you define is externally accessible. When using an external mail server (other than Gmail) an envelope sender address can be used. If the SMTP server accepts emails that are originated by its registered user, then you have to define that user email address as origin, e.g. john@mycompany.com. If the SMTP server only verifies the sender domain name, then you can define a domain name that has valid MX DNS records, e.g. mycompany.com. (Not required for Gmail.)

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). Set TLS to **Yes** if this is required by your email provider (Not required for Gmail).

Authentication, select **Use Authentication** if your email provider requires authentication (Username and Password) to send outgoing email. If no authentication is required, select **No Authentication**. (Not required for Gmail.)

Username, username that your email service provider has given you to give you access to your email account. Typically, this would be something like user@my-mail-server.com

Password, the password that your email service provider has given you to allow you to log into your email account.

Test Saved Email Settings, testing the email settings. Note that this test will use ***saved*** email settings to send a test email to the address that you provide.

If you have updated the email configuration, you must save the settings ***before*** testing the configuration.

Email Log, display email event log.

The most common cause of email delivery failure is because the mail server of the recipient will not accept emails from CompletePBX 5. This may be because the mail server of the recipient cannot carry out a "reverse lookup" of the sender's domain, and has emails as SPAM, or blacklisted the sender. You can fix this by:

- Modifying the recipient server to recognize the sender's mail domain
- Changing the host name of CompletePBX 5 to a valid FQDN and editing the sender address domain name to match
- Using a mail relay that logs in as an authorized user

DHCP Settings Dialog

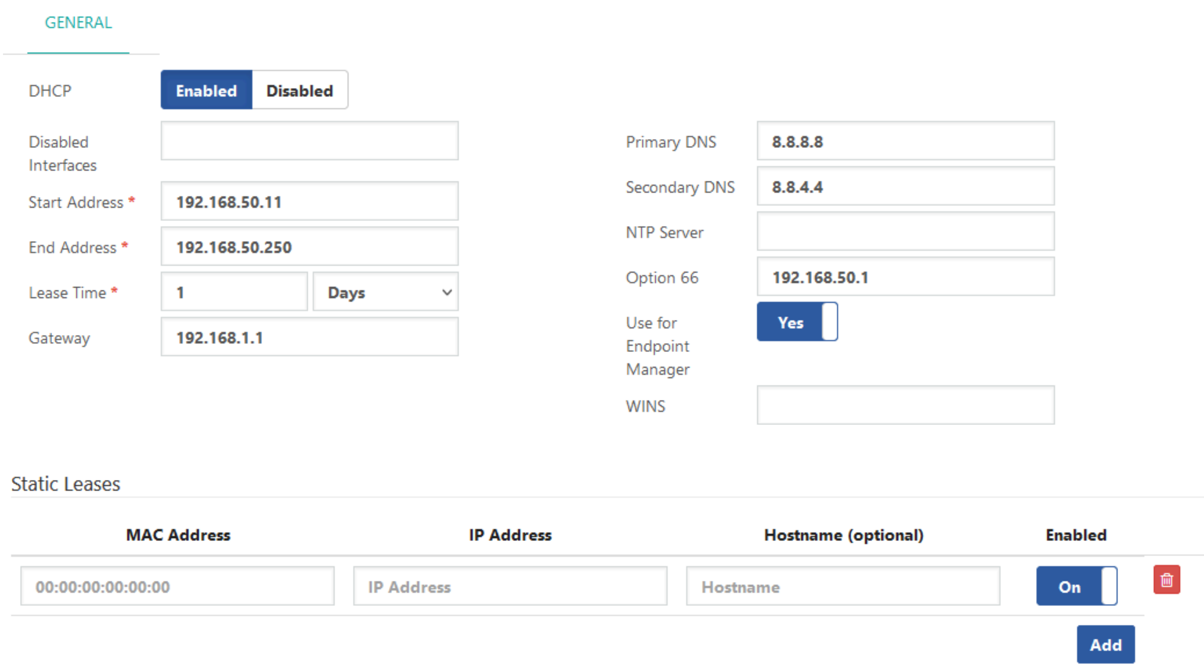
(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

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*** DHCP server active on your network.

GENERAL Tab

In this tab you will find the information about DHCP settings.



DHCP, enable if you want the system to act as a DHCP server for this network**,** or disable if you already have a DHCP server on the network. In most configurations, this should be set to **Disabled**.

Disables Interfaces, 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*, if you have enabled DHCP for the PBX, this configures the first address on your network that can be allocated as a dynamic IP address.

End Address*, if you have enabled DHCP for the PBX, this configures the last address on your network that can be allocated as a dynamic IP address.

Lease Time*, if you have enabled DHCP for the PBX, this configures the period that the DHCP server grants an IP address to devices. The device must renew its IP address before the end of the lease period.

Gateway, if you have enabled DHCP for the PBX, this configures 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, defines 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. Enter the address of the NTP server that you want to use to synchronize the clock of the PBX server.

Option 66, option 66 provides IP phones with an URL for configuration provisioning. The system 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' check-box 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' check-box.

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,** if you have enabled DHCP for the PBX, this enables you to configure a specific MAC address.
- **IP Address,** if you have enabled DHCP for the PBX, this configures the static IP address for the device defined by the MAC Address.
- **Host Name (optional),** if you have enabled DHCP for the PBX, this allows you to configure a host name for the device.
- **Enabled**, enable/disable the static lease

Task Manager Dialog

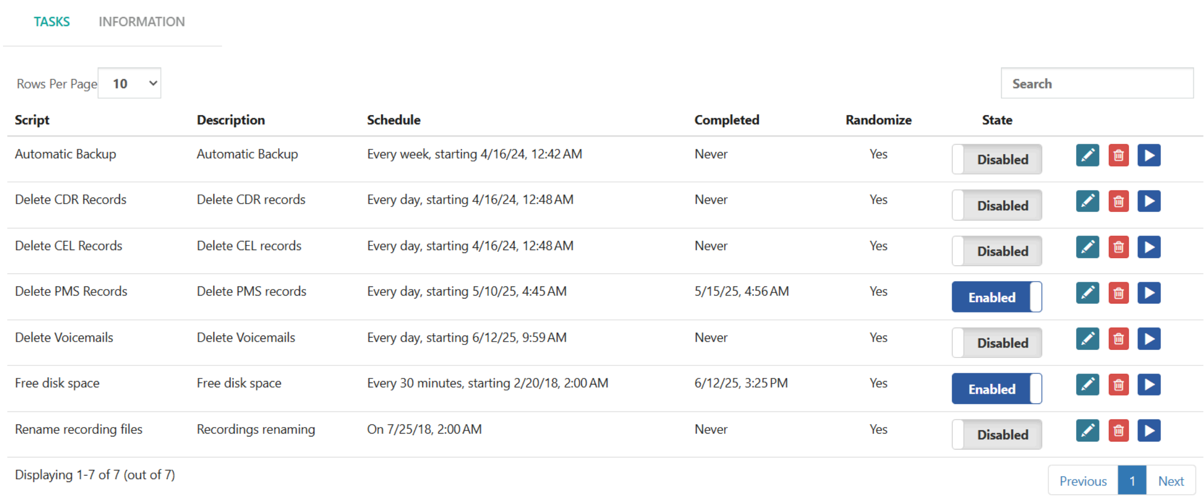
Allows you to configure and schedule periodic tasks.

There are a number of factory-configured tasks that are installed on your system, including:

- Backup of CompletePBX 5 configuration files and data based on user-defined parameters. NOTE: the number of backups kept in the system is defined per ***type***. In case more than one backup task is defined, a unique type must be set for each backup task. (**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)
- Monitor free disk space. This script ensures that there is minimal free disk space for proper behavior of the system. It checks the available disk space and if it is lower than the user-configurable threshold value then the script will free disk space by deleting files on the main partition. The script checks the proportion of disk space taken by different classes of files (call recordings, log files, backups, fail2ban logs, etc) and then deletes the oldest files accordingly.
- Rename recording files to have more meaningful names.
- Delete CDR records
- Delete CEL records

TASKS Tab

This tab displays a list of all configured tasks, and allows you to configure new tasks.



Script	Description	Schedule	Completed	Randomize	State
Automatic Backup	Automatic Backup	Every week, starting 4/16/24, 12:42 AM	Never	Yes	Disabled
Delete CDR Records	Delete CDR records	Every day, starting 4/16/24, 12:48 AM	Never	Yes	Disabled
Delete CEL Records	Delete CEL records	Every day, starting 4/16/24, 12:48 AM	Never	Yes	Disabled
Delete PMS Records	Delete PMS records	Every day, starting 5/10/25, 4:45 AM	5/15/25, 4:56 AM	Yes	Enabled
Delete Voicemails	Delete Voicemails	Every day, starting 6/12/25, 9:59 AM	Never	Yes	Disabled
Free disk space	Free disk space	Every 30 minutes, starting 2/20/18, 2:00 AM	6/12/25, 3:25 PM	Yes	Enabled
Rename recording files	Recordings renaming	On 7/25/18, 2:00 AM	Never	Yes	Disabled

NOTE that tasks can be set to run at a randomized (non-precise) time. This is especially useful for multi-tenant or multi-instance deployments in which it is favorable to avoid running scheduled tasks at the same time by all tenants in order to avoid peaks in resource consumption. Randomized tasks will run at a range of +/-30 minutes from the set time or less when the interval time is short. For example, a task scheduled to run every 10 minutes will randomize at +/-5 minutes and not +/-30 minutes. When upgrading an existing system, all default tasks (tasks that are provided as part of CompletePBX installation/image) will be switched to random mode. Custom tasks created by the user will not be affected.

Rows Per Page, allows you to control how many rows of data will be displayed on each page

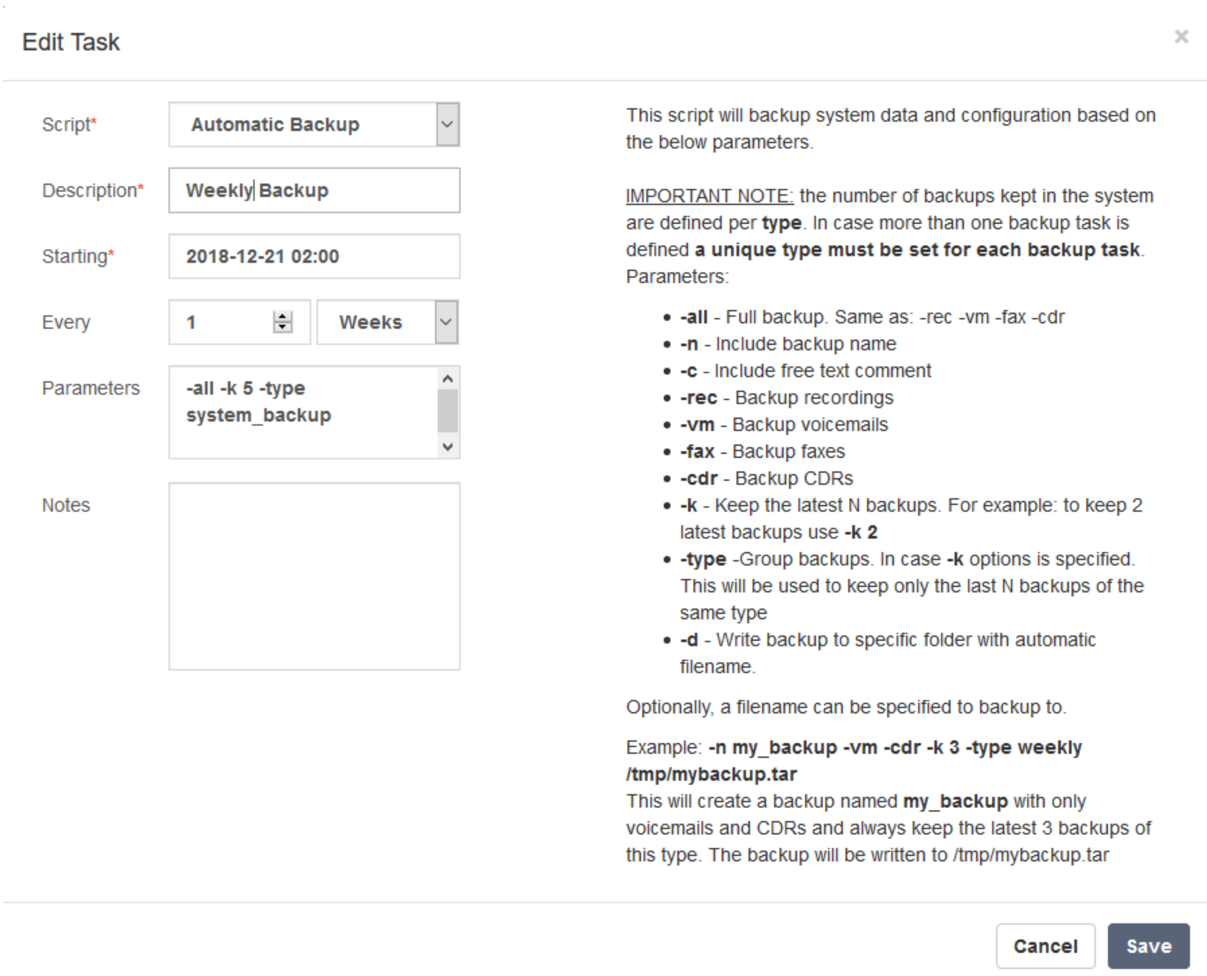
Use the icons at the end of each row to manage previously-defined tasks:

 Click on this icon to edit the parameters of an existing task.

 Click on this icon to delete an existing task.

 Click on this icon to immediately execute the selected task.

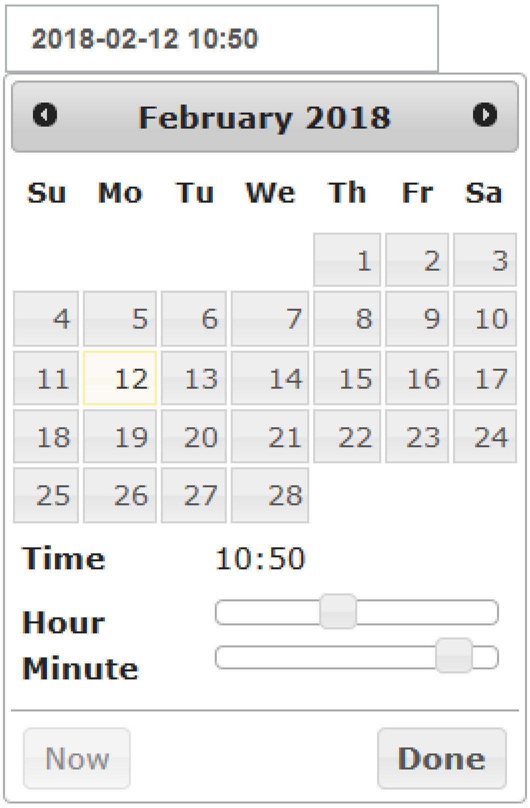
You can disable existing tasks (without the need to delete them) by changing the state of the task from **Enabled** to **Disabled**.



Script*, select a predefined task from the available options in the dropdown list.

Description*, a free-text description to identify the task.

Starting*, the date and time when this task should be activated for the first time. You can either type the timestamp in the Starting field, or use the dialog that appears to choose a date and time. Click **Done** when finished to save the chosen data.



Every, allows you to control the frequency of the task. Select Once for a single activation of the task, or you can choose to activate the task every x minutes, hours, days, weeks, or months,

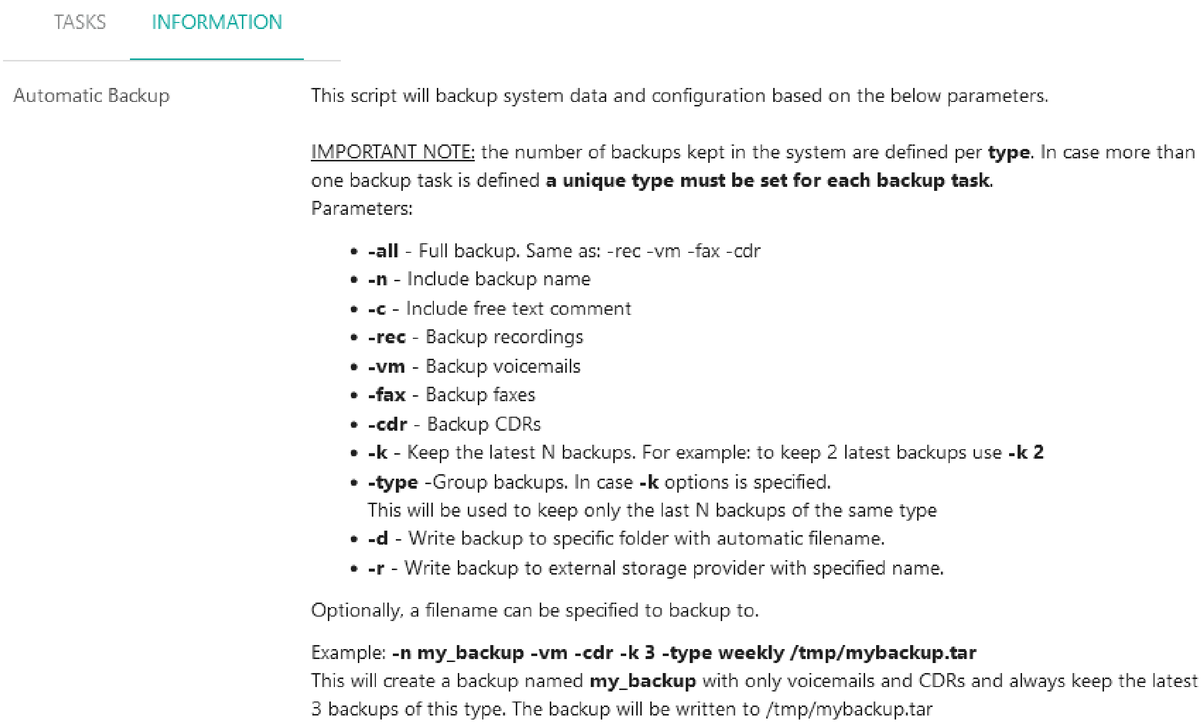
Randomize, when set to **Yes** allows to randomize the start time of the task by up to 50% of the interval with a maximum of ± 30 minutes.

Parameters, allows you to add none, one, or more parameters, from the list that is shown to the right of the dialog

Notes, allows to place any notes regarding the task.

INFORMATION Tab

This table will display the parameters that can be used for the available tasks.



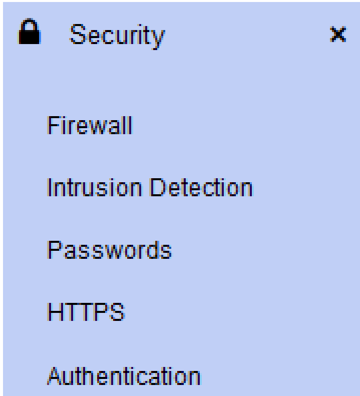
Creating Custom Tasks

You can create your own custom task by using the following steps:

- Copy your script file to the /usr/share/ombutel/task-scripts directory
- Ensure that the Linux executable flag is set by using the **chmod +x <my_script>** command
- Go to the Task Manager dialog, and click on the **Create Task** button

Security Menu Group

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)



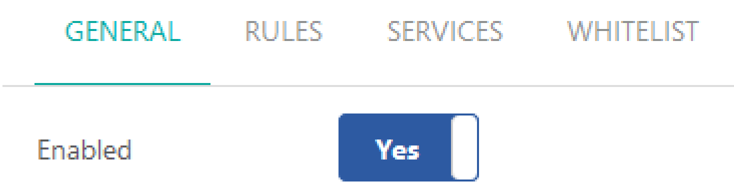
Firewall Dialog

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

The system is preconfigured with a built-in firewall. You can choose to disable this built-in firewall by setting Enabled to No**,** followed by the Save button.

GENERAL Tab

In this tab you will find the information about Firewall status.



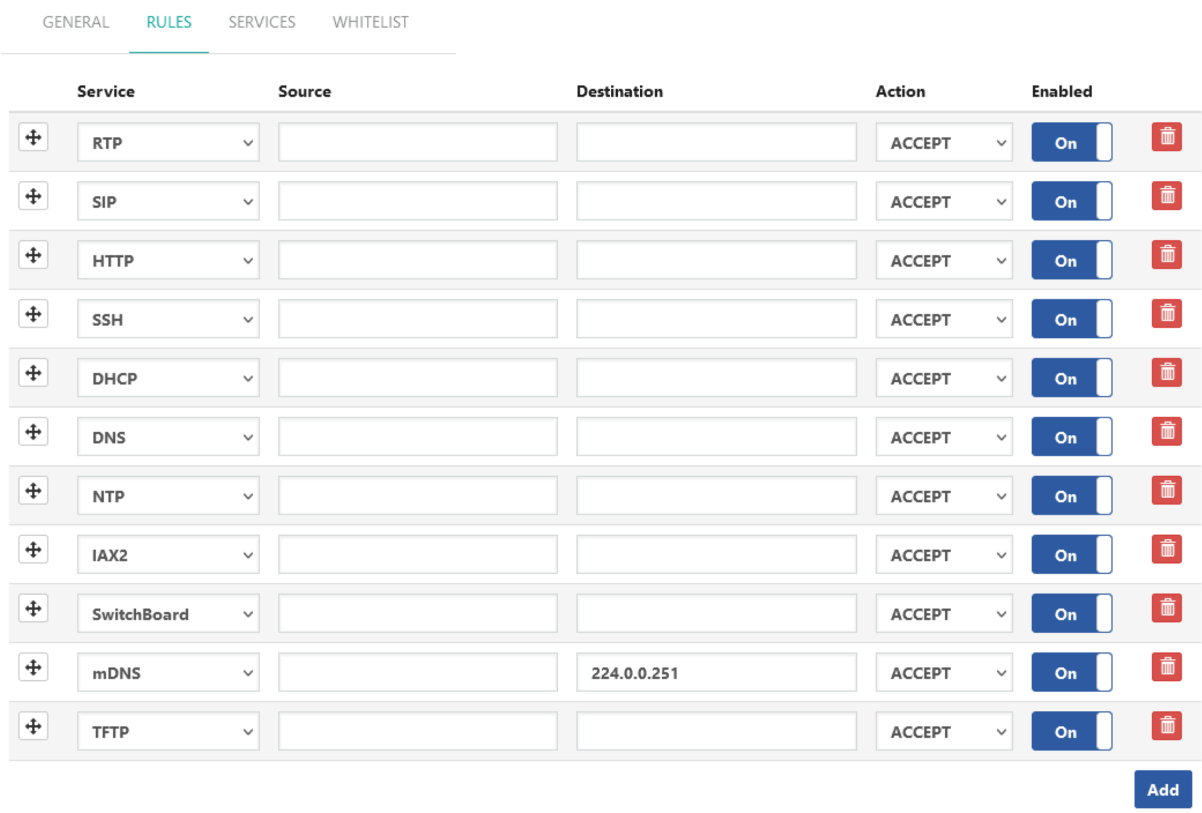
Enabled, toggle to enable or disable the firewall.

RULES Tab

If the firewall is enabled**,** you can define multiple Services**,** on which you can base Rules. The system is preconfigured with a number of standard Services and Rules. You may want to add additional Rules that are specific to your installation. You must create a service in the Services tab of the firewall dialog before you can add a rule that uses the service.

This dialog gives you control of inbound access to the system. You can use these rules to allow or block access for specific services, from specific IP addresses (sources), or to specific IP addresses (destinations). When the rule consists of multiple lines, the incoming request is tested against each line, starting from the first line, until a match is found. Once a match is found, the rule is implemented, and no further lines are tested. If no match is found, the incoming request will ***not*** be allowed, and the request will be rejected.

To add a Rule**,** press on the Add button at the end of the list of Rules that have already been configured in the system.



Service, selected from the drop-down box. The drop-down box is populated with Services that are defined in the Services tab.

Source, use if you want the rule to be restricted to access attempts from a specific IP address or subnet. You can leave this field blank, or use **Any**, to make the rule apply to all IP addresses. To restrict the rule to a specific IP address type in the IP address. You can define a range of IP addresses by adding a subnet mask, i.e. 10.0.0.0/24 to restrict the rule to IP addresses in the range from 10.0.0.1 to 10.0.0.254

Destination, is used if you want the rule to be restricted to access attempts to a specific IP address or subnet. You can leave this field blank, or use **Any**, to make the rule apply to all IP addresses. To restrict the rule to a specific IP address type in the IP address. You can define a range of IP addresses by adding a subnet mask, i.e. 10.0.0.0/24 to restrict the rule to IP addresses in the range from 10.0.0.1 to 10.0.0.254

Action, configures whether this rule should Allow**,** Deny**,** or Reject access.

- **Accept** will unconditionally accept all packets that match the definition of the Rule.
- **Drop** means that the packet will be discarded, but no response will be given to the originator of the request. If a hacker is trying to access your machine, Drop will provide no useful information to the hacker. On the other hand, Reject is a more "friendly" response to legitimate connection requests, as a detailed error message is provided.
- **Reject** means that the packet will be discarded, and a response will be sent to the originator of the request. Reject is more "friendly" to legitimate connection requests, as a detailed error message is provided.

Enabled, enable/disable the rule.

You can change the order of the rules by pressing and holding the icon to move the selected rule up or down.

SERVICES Tab

Enables you define Services, by defining the protocol used by the Service (i.e. TCP, UDP, or Both), and the port/s on which the Service operates.

GENERAL RULES SERVICES WHITELIST

Name	Protocol	Port
SIP	Both	5060
DNS	Both	53
NTP	UDP	123
DHCP	UDP	67-68
HTTP	TCP	80
SSH	TCP	22
RTP	UDP	10000-20000
IAX2	UDP	4569
SwitchBoard	TCP	4445
mDNS	UDP	5353
TFTP	UDP	69
UDPTL	UDP	4000-4999
AMI	TCP	5038
H323	TCP	1720
HTTPS	TCP	443

Add

Name, give the Service a meaningful name to help you to easily recognize it. This name will be used to refer to the Service in the Rules table.

Protocol, determines the protocol used by the application. The protocol options are TCP, UDP, or Both.

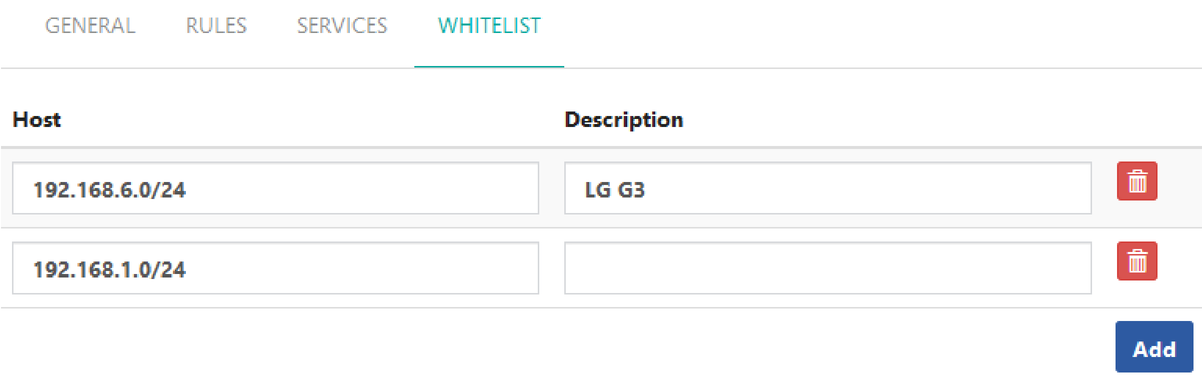
Port, the IP port/s used by the Service. This can be defined as:

- a single port, e.g. 80

- a range of ports separated by a dash, e.g. 10000-20000
- a list of ports separated by commas, e.g. 80, 10000-20000, 5060

WHITELIST Tab

This enables you to create a list of IP addresses that should always be ignored by the firewall. Click on the **Add** button to add additional items.



Host, IP address and netmask

Description, a short description to help you identify the whitelisted item/s.

Intrusion Detection Dialog

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

Intrusion Detection configures the fail2ban application, which detects and blocks unauthorized attempts to access the system. Fail2ban is a highly versatile tool to help prevent brute-force attacks as they occur. Rather than alerting an administrator after the damage may already be done, fail2ban can take proactive steps to deny access to the system from the attacking IP address.

After a potential intruder has been detected, the intruder's IP address will be blocked from further access to the system for the ban period (defined in minutes).

Apart from the financial damage that can be caused by someone actually breaking into your system, there is also a performance 'cost' to be considered. Even if an attacker is unable to find valid extensions or guess passwords, the activity created in the process of trying to break into your system can cause a high load on your server.

Fail2ban can drastically reduce the potential for damage from such attacks by limiting the number of invalid login attempts to a small number, and then by blocking the attacking IP address for a period of time. This can be done by adding rules to iptables. By default, fail2ban inserts rules at the top of the iptables chain, so they will override any rules you have configured in iptables. This is good because you may allow all sip traffic, but fail2Ban will be able to block individual hosts after they have been detected making an attack.

Although iptables is an integral part of the installation, you must ensure that it is activated, by making sure that the internal firewall is enabled (in the Admin>Security>Firewall dialog.)

Asterisk does not have built-in tools to prevent these attacks. However, it does a very effective job of logging these potential attacks, enabling fail2ban to detect them, and take appropriate action.

Fail2ban provides a way to automatically protect the server from unwanted activity. Fail2ban is an open source intrusion detection framework that works by scanning log files and reacting to unwanted actions such as repeated login failures, and bans failure-prone addresses. Fail2ban updates firewall rules to reject the IP address or can execute user defined commands.

Fail2ban is configured to monitor various logs, including:

- /var/log/asterisk/full (Asterisk)
- /var/log/secure (ssh)
- /var/log/httpd/error_log (apache)
- /var/log/httpd/*access_log (apache)
- /var/log/vsftpd.log (vsftpd)

Fail2ban is preconfigured with files that contain known error strings, and searches the logs for occurrences of those messages. For example, the Asterisk logs are scanned for messages that contain the following texts:

- Registration from '.*' failed for <HOST>
- No registration for peer
- Host <HOST> failed MD5 authentication

This would detect events that could be the result of:

- Incorrect password
- Mismatch between username and security
- No matching peer found in system database
- Peer is not supposed to register on the system
- Device does not match ACL
- MD5 authentication failure - Digest Authentication is a feature of the SIP protocol enabling password not to be sent in clear text.
- Device attempting to login that is not configured to use the specific transport type

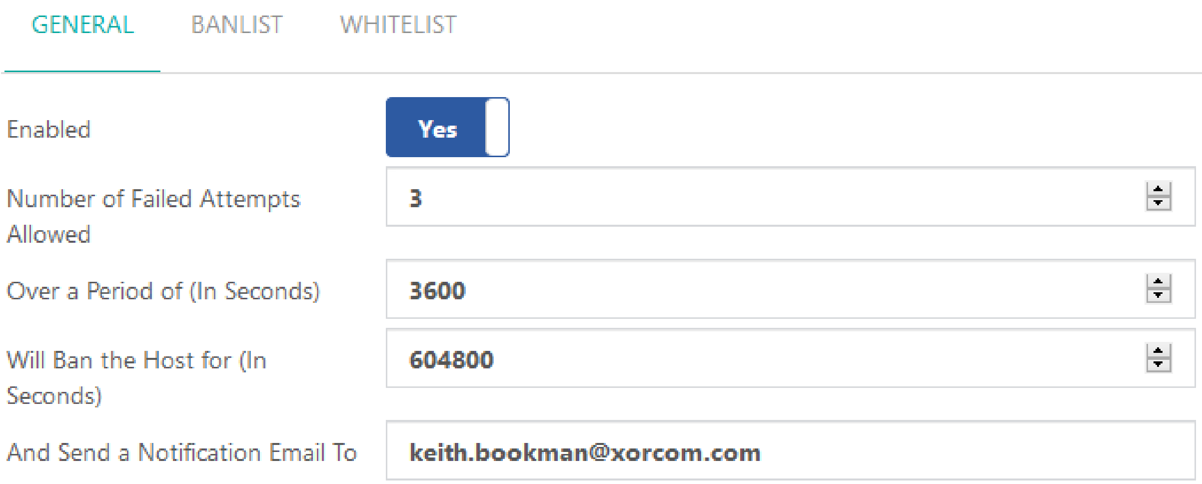
The default fail2ban configuration file is located in /etc/fail2ban/. All configuration changes are managed from the user interface, which updates the local copy of the jail file (jail.local). Manual changes should not be done to jail.conf, as they will be overwritten by the user interface.

A potential intrusion is defined as a user-defined number of unsuccessful attempts to access the system within a user-defined period of time (defined in seconds).

An email alert will be emailed to the defined email address after a potential intruder is detected.

You can create a whitelist of addresses that will be ignored by this dialog. Typically, you should include the PBX itself in the whitelist, by adding 127.0.0.1 to the whitelist.

GENERAL Tab



Enabled, sets the current status of the service.

Number of Failed Attempts Allowed, number of attempts that will trigger a ban. It is the number of incorrect logins that a host is allowed during the **Over a Period of (In Seconds)** before being considered to be an intruder, and being banned for the length of time defined by **Will Ban the Host for (In Seconds)**.

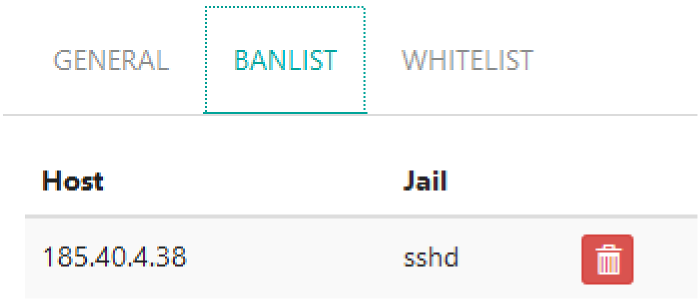
Over a Period of (In Seconds), time period over which the number of attempts will trigger a ban. This parameter sets the length of time that a host is monitored for, before the clock is reset. The default setting is 600 seconds (10 minutes).

Will Ban the Host for (In Seconds), is the number of seconds that a host is blocked from accessing the server if the host is found to be in violation of any of the rules. This is especially useful in the case of bots, as once they are banned, they will simply move on to the next target. The default is set to 1800 seconds (30 minutes) – you can increase this to one hour (or higher), if you like. The maximum value is 604,800 (i.e. 7 days)

And Send a Notification Email To, address to which notifications will be sent each time that a host address is banned.

BANLIST Tab

Any IP addresses that are banned will be shown in the table of banned hosts. The table will show the IP address of the banned host, as well as the fail2ban rule that detected the intrusion. If a host appears incorrectly in the list of banned hosts, you can press on the trash button to remove it from the list.



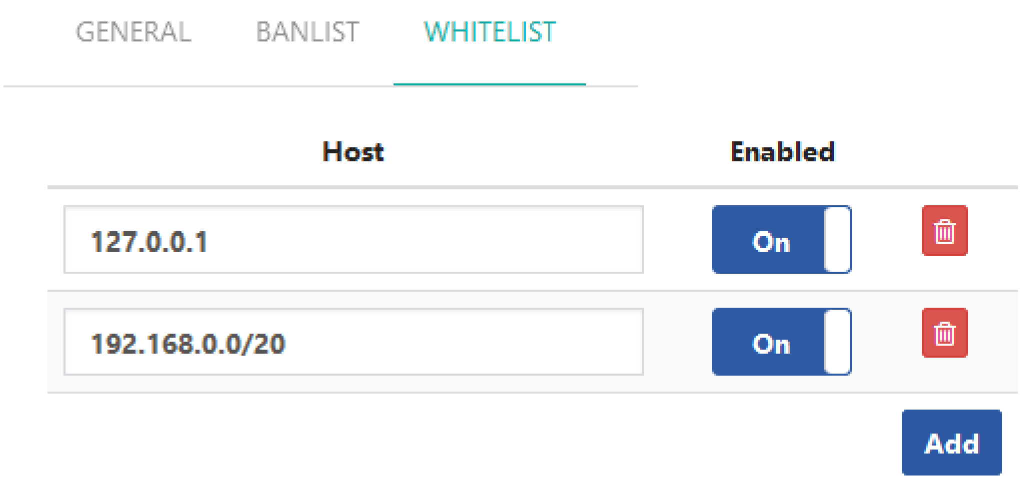
Host, list of banned IP addresses.

Jail, fail2ban rule that detected the intrusion.

allows you to remove a host from the list of banned IP addresses. You should only do this after you have found the cause for the ban**,** and you are sure that it is safe to unban the IP address.

WHITELIST Tab

List of IPs that will never be blocked by the instruction detection under any circumstances.



Host, IP address. This enables you to configure addresses that will be never be locked out by fail2ban**,** such as your personal IP address, or your local (internal) network. Including your own IP address will guarantee that you do not accidentally ban yourself from your own server. Enter each address on a new line by click on the **Add** button.

Enabled, enable/disable the IP address that will never be blocked by the instruction detection under any circumstances.

The Whitelist should always include your local host**,** i.e. 127.0.0.1

This will ensure that even if you make too many invalid login attempts, local login into the system will never be blocked.

Whitelisted addresses are stored in /etc/fail2ban/jail.d/10-ombutel.local. This file also includes addresses 159.65.xxx.xxx, 165.227.xxx.xxx and 167.99.xxx.xxx which are used by the Xorcom CloudPhone server, but are not displayed in the user interface to prevent them being removed from the whitelist. The Xorcom CloudPhone application will not work correctly if they are removed from the whitelist.

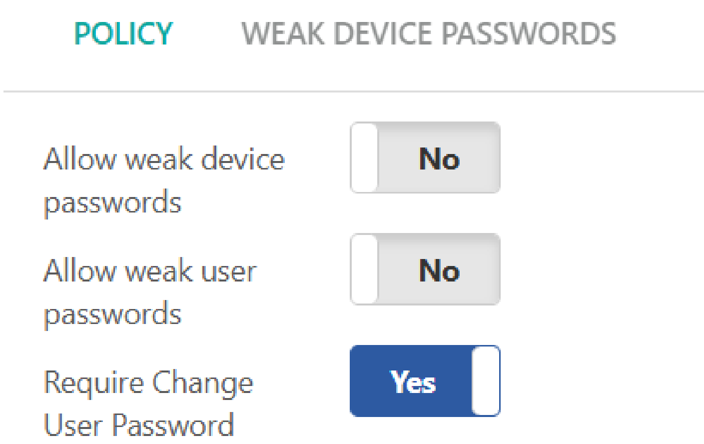
Passwords Dialog

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

This dialog manages security policy for CompletePBX 5.

POLICY Tab

This tab allows you to manage password policies for devices and users.



Allow SIP/IAX2 weak passwords, if set to **No** (the default setting), the system will only allow you to save passwords for SIP, IAX2, and Hot Desking devices that match a high level of security.

If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password.

Allow PBX users weak passwords, if set to **No** (the default setting), the system will only allow you to save passwords for Users, Portal Users and Asterisk Managers that that match a high level of security.

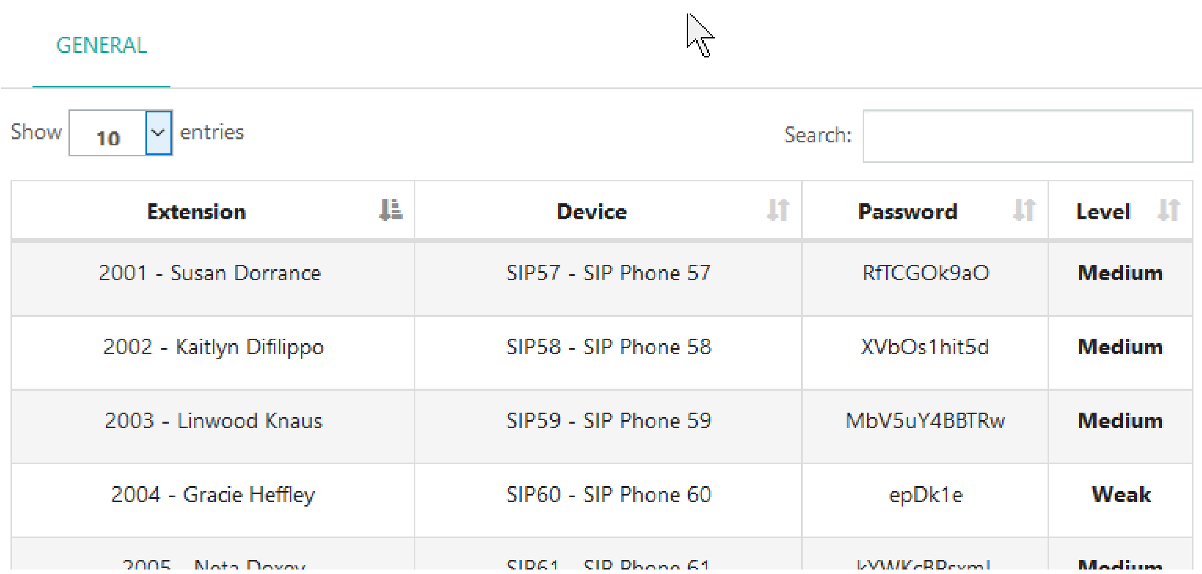
If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password.

Require Change Password, set to **Yes** if you want new users to be required to change their password after their first login. Upon initial access, newly created users will receive a prompt to set a new password.

WEAK DEVICE PASSWORDS Tab

In this tab you will find a list of all extensions where the password does not match a minimum level of difficulty.

If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password.



Extension, shows information about the Extension – number and name

Device, shows information about the device – name and description

Password, displays the current password

Level, indicates the security level of the current password

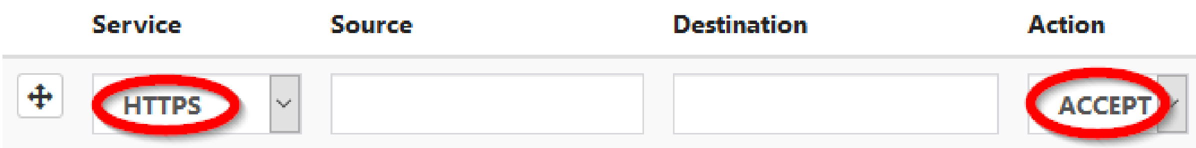
HTTPS Dialog

(**NOTE** that this option has been disabled on systems that are licensed for multiple tenants.)

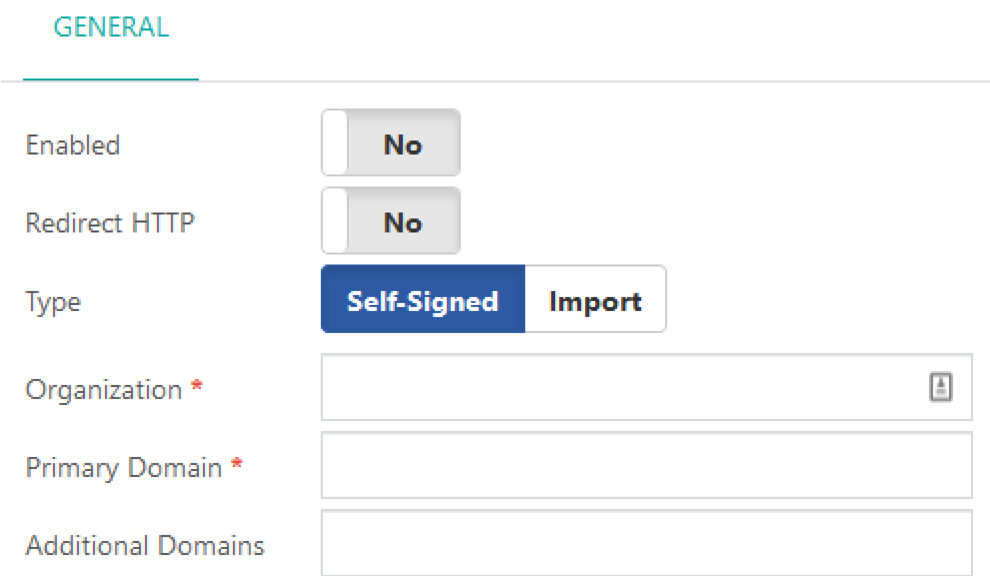
Allows you to configure whether to use HTTP (normal hypertext transfer protocol) or HTTPS (secure hypertext transfer protocol) to access the CompletePBX 5 user interface.

HTTPS, which provides an encrypted connection to the user interface, requires an SSL certificate

If you use HTTPS, make sure that the HTTPS service is configured as ACCEPT in the Rules tab of the CompletePBX 5 Firewall dialog.



Generating a Self-Signed Certificate



Enabled, when configured to **Yes**, HTTPS will be used to access to the user interface. When configured to **No**, HTTP will be used.

Redirect HTTP, if configured to **Yes**, regular HTTP traffic will be redirected to use HTTPS.

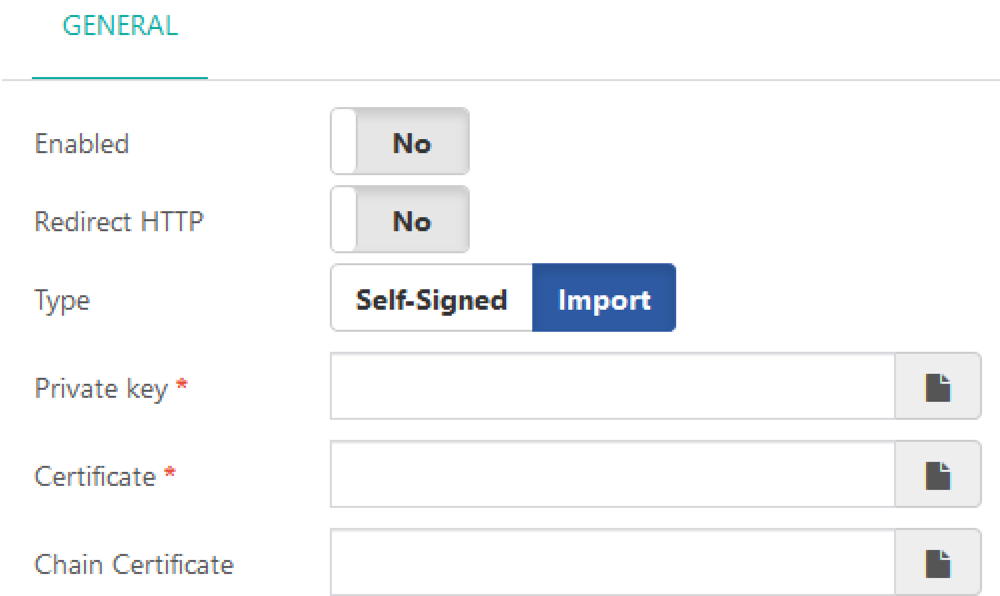
Type, if you select **Self-Signed**, you will need to enter details in the **Organization** and **Primary Domain** fields. When the information is complete and you press on **Save**, an SSL certificate will be created on your CompletePBX 5 server.

Organization*, the name of the organization (i.e. your company name) for which you want to generate the SSL certificate

Primary Domain*, the domain for which you want to generate the SSL certificate.

Additional Domains, list of one (or more) additional domains for which you want to generate the SSL certificate. If you want to enter more than one domain, leave a space to separate between each domain.

Importing an Existing SSL Certificate



Enabled, when configured to **Yes**, HTTPS will be used to access to the user interface. When configured to **No**, HTTP will be used.

Redirect HTTP, if configured to **Yes**, regular HTTP traffic will be redirected to use HTTPS.

Type, if you select **Import**, you will need to enter details in the following fields. When the information is complete and you press on **Save**, an SSL certificate will be imported to your CompletePBX 5 server.

Private Key*, PEM-formatted key of the certificate that you want to import.

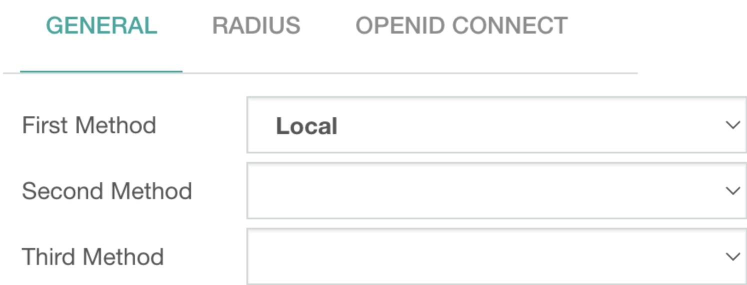
Certificate*, location of the PEM-formatted X 509 certificate that you wish to import.

Chain Certificate, location of the PEM-formatted X 509 chain certificate that you wish to import.

AUTHENTICATION Dialog

Allows to select which login options are supported and in which order, where CompletePBX will try authenticating using the different options based on the order configured.

GENERAL Tab

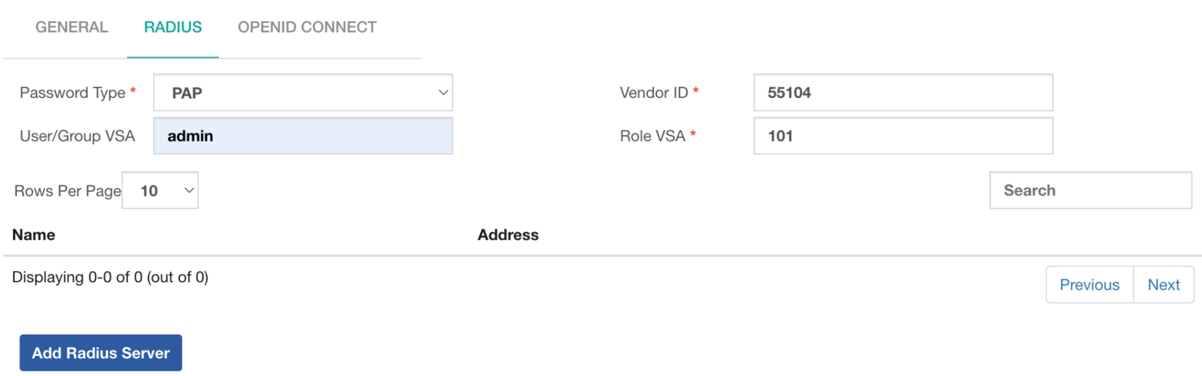


Within the general tab, the Authentication module supports three different login options, which can each be configured as the First, Second, or Third method:

- **Local**, users configured in CompletePBX.
- **RADIUS**, users configured at a remote RADIUS server.
- **OpenID Connect**, users authenticated by an external service using the OpenID Connect protocol.

Note that local login may be disabled, allowing only centrally managed login.

RADIUS Tab



Password Type*, allows you to choose which encoding method to use for the password. There is a selection of three options:

- **PAP,** it transmits username and password in plain text, making it less secure compared to more advanced methods.
- **CHAP,** uses a challenge-response mechanism for authentication. The server sends a challenge to the client, which responds with a hashed value.
- **MSCHAP v1,** is a version of CHAP developed by Microsoft, primarily used in Windows networks. It uses the same challenge-response approach but with Microsoft-specific algorithms and features.
- **EAP-MSCHAP v2,** is an authentication method that combines EAP with MSCHAP v2.

User/Group VSA, this value will be submitted to each RADIUS server as vendor-specific attribute 102.

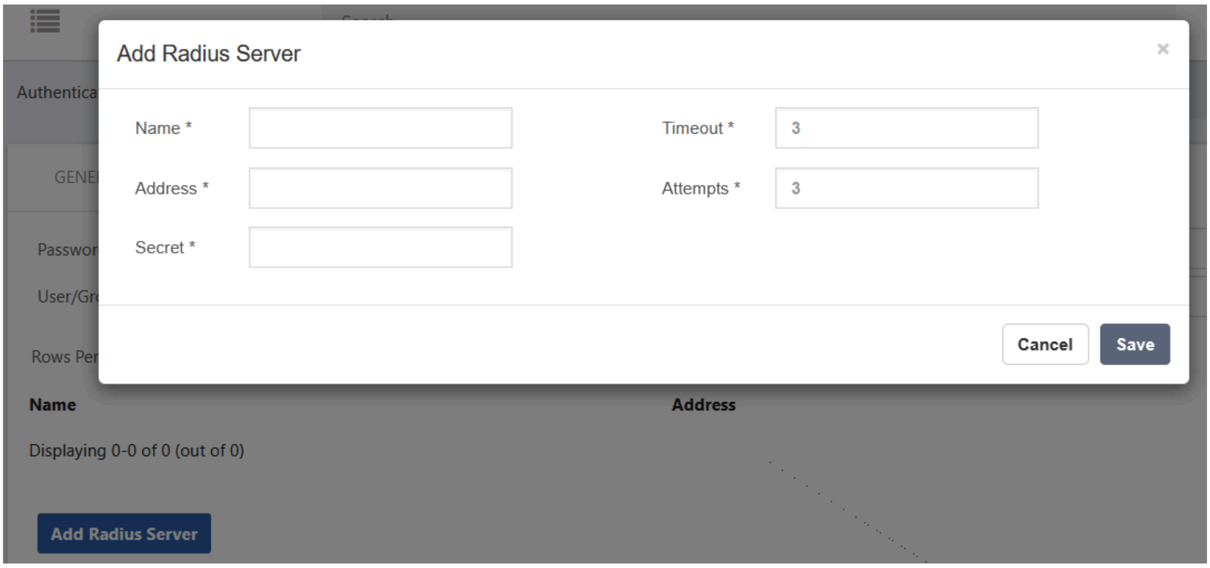
Vendor ID*, to use for vendor-specific attributes, defaults to 55104.

Role VSA *, allows to set which vendor-specific attribute the PBX will use as the user role, defaults to 101.

Add Radius Server, by clicking this button open a new dialog to setup a RADIUS server with the configurations listed here:

- **Name ***,Name of this servers.
- **Address ***, Hostname or IP address with optional port number for this server.
- **Secret ***, Shared secret for this server.
- **Timeout ***, Timeout, in seconds before giving up. Defaults to 3.

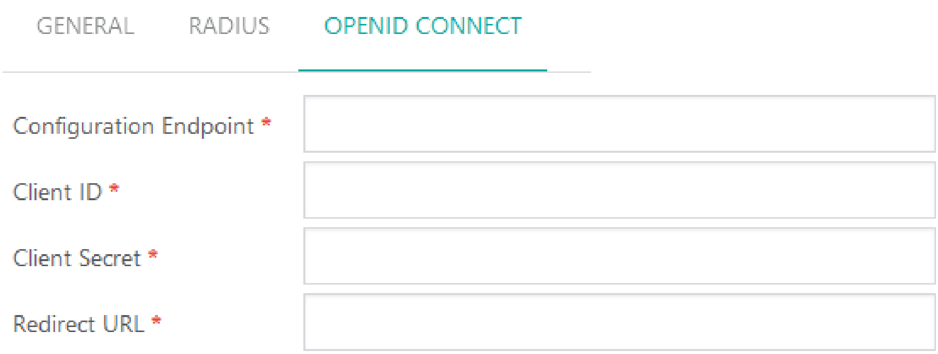
Attempts *, Number of attempts before giving up. Defaults to 3.



OPENID Tab

OpenID Connect (https://openid.net/developers/how-connect-works/) is a protocol that allows authenticating users using an enterprise class OpenID Connect providers, such as Keycloak, PingFederate, Auth0, and others. Such Identity Providers allow managing the users internally (on the Identity Provider server) or via a remote user management, such as Windows Active Directory controller or another company's LDAP server. OpenID Connect can be used to support:

- Single Sign-On
- Multi-factor authentication (using 3rd party authentication)
- Increased security by centrally managing users and passwords
- Simplifying user administration & integration with existing tools
- Enabling enforcement of password policies across different apps
- Simplifying permission management across various apps



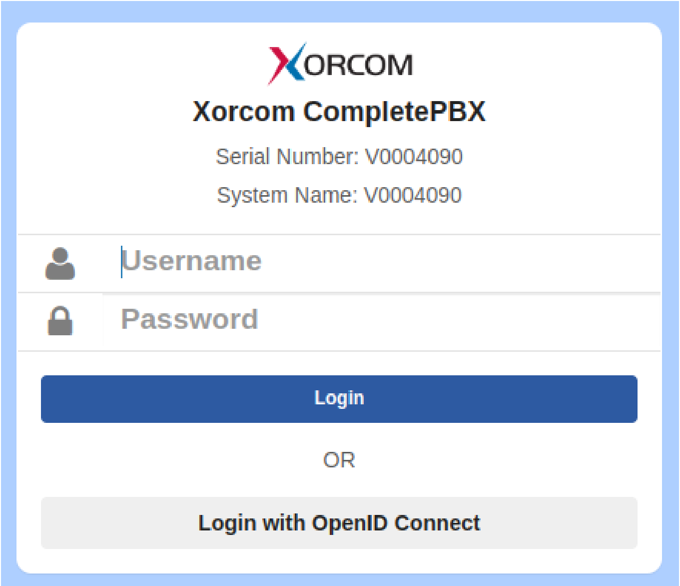
Configuration Endpoint *, well-known OpenID Connect configuration endpoint URL.

Client ID *, which client ID to use in OIDC requests.

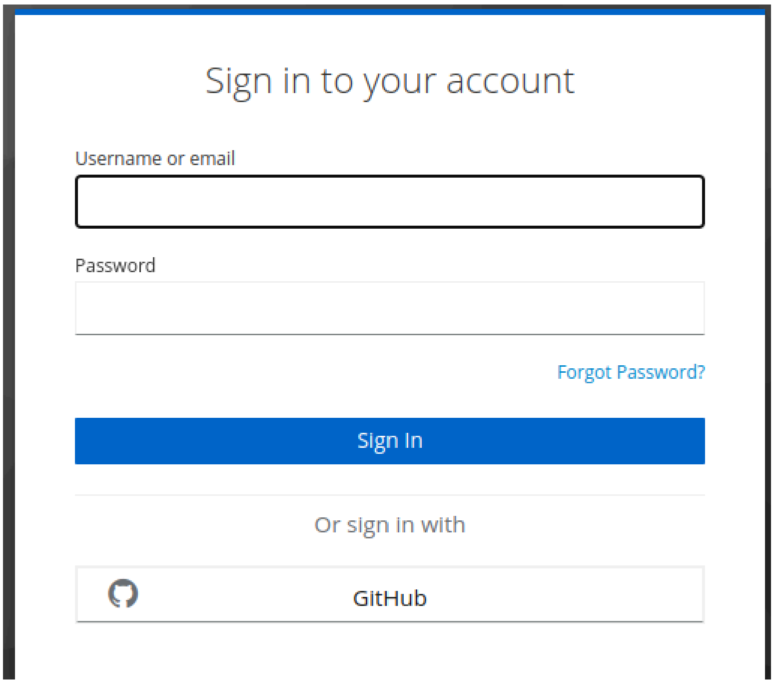
Client Secret *, which client secret to use in OIDC requests.

Redirect URL *, where the OpenID Connect server will send the user after authentication. This must be http://[PBX address]/oidc or https://[PBX address]/oidc.

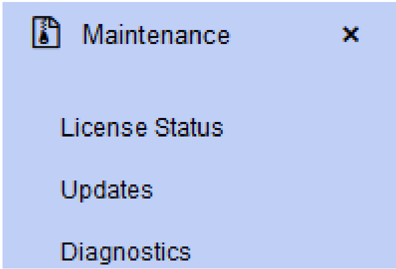
NOTE that allowing both Local/RADIUS and a remote login option using OpenID Connect, the login screen will show both the normal fields and the remote login options.



When selecting only OpenID Connect as a login option, the user will not see the normal login screen and will be redirected to login with the identity provider, such provider may offer local and/or 3rd party authentication (e.g. LDAP, Google, etc.):



Maintenance Menu Group



License Status Dialog

This dialog displays the status of Xorcom licenses that are linked to your system.

If your system is not licensed, CompletePBX 5 will be limited to 3 extensions. In addition, fax sending and fax viewing will not be enabled in the User Portal.

Licenses can be registered directly in the PBX management GUI (Admin -> Licenses -> License Status). It is possible to register multiple licenses in bulk separated by comma or space.

Separate licenses are required to enable the TwinStar option, or to manage more than 5 rooms in the Hospitality module.

The license, which is based on the MAC address of the network interface, may require internet access in order to be able to periodically verify the license. Both physical and virtual licenses can have expiration dates.

- A ***physical*** license requires the presence of a Xorcom USB dongle. Internet access is only required when registering or updating the license.
- A ***virtual*** license (which is the only license that can used on virtual machines) does not require a Xorcom USB dongle. However, the system will require continual internet access so that the license can be periodically validated with the Xorcom licensing server.

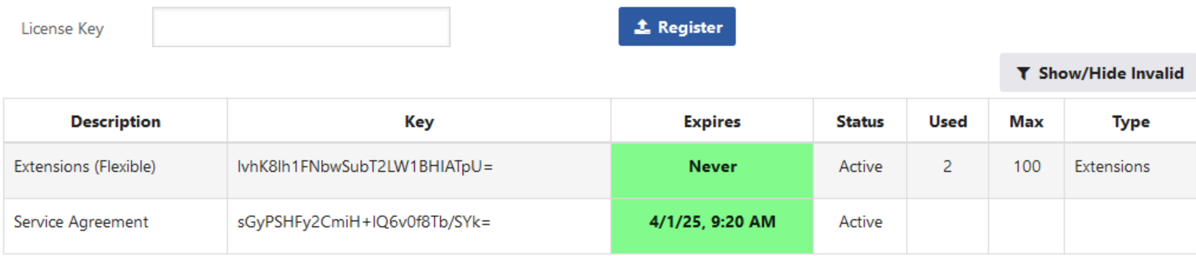
A license will become invalid if the motherboard of the system is changed, if the system time has changed dramatically, if the Xorcom licensing server could not be access over the past 48 hours, or if a system restore has been performed. In such cases the status of the license is set to Grace.

If a valid email address is configured for notifications (in the Admin>System Settings>System Misc>Notifications tab), CompletePBX 5 will email notifications as follows:

- Monthly, if a license is about to expire within the next 3 months
- Weekly, if a license is about to expire within the next 4 weeks
- Daily, if a license has expired, or is about to expire within a week

Service agreements are handled as licenses in the system. Service agreements will start automatically when the system starts being used for production, avoiding the need to register new systems manually. In the case of PBX appliances, the start date will also determine the warranty start date. Only systems under an active service agreement will receive software updates. All systems under warranty, software service agreement, annual license, monthly license, and post-paid licenses will be eligible for software updates. The status of the service agreement will appear in the License dialogue.

GENERAL Tab



Description	Key	Expires	Status	Used	Max	Type
Extensions (Flexible)	lvhK8lh1FNbwSubT2LW1BHIATpU=	**Never**	Active	2	100	Extensions
Service Agreement	sGyPSHFy2CmiH+lQ6v0f8Tb/SYk=	**4/1/25, 9:20 AM**	Active			

License Key, one or more license keys separated by space or comma that must be registered to the system.

Show/Hide Invalid, a toggle that enables you to display invalid licenses that are linked to your system. The default mode is set to hide invalid licenses.

Description, name of the Xorcom license.

Key, value of the key for the Xorcom license.

Expires, when the license expires. This may be a specific date, or **Never** for a perpetual license.

Status, current status of the license. Status can be one of the following:

- **Active**, indicates that the feature is active and OK.
- **Grace**, indicates that the feature has expired, but system functionality will be enabled for a limited period of time. The maximum grace period is 30 days.
- **Invalid**, the feature is disabled. This can happen:
  - After changing the motherboard of the CompletePBX 5 system
  - The Xorcom USB dongle is not detected for a system using a physical license
  - No internet connection was available for more than 48 hours for a system using a virtual license

Used, shows the number of objects in use for this licence.

Max, shows the maximum number of objects available for this licence.

Type, indicates the type of licence, e.g. Extensions, Hotel Rooms, etc.

Update, pressing this button will cause CompletePBX 5 to fetch updated data from the Xorcom licensing server, so it will update existing licenses and add any new licenses that are available for the system. You can also use the `xlic fetch` command to update your licenses. In cases when a system restore has been done, it may be necessary to clear the old license data. This can be done by using the `xlic clear` command.

You can use the `xlic list` command to see all information regarding licenses that are known to your system:

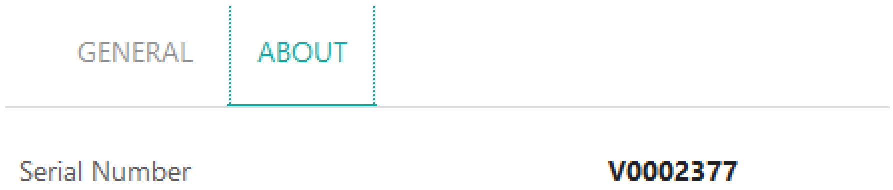
```
Demo> xlic list
List completed successfully
Licenses                : 3

Name                    : cpbx-epm-pairing
Description             : PhoneScan
State                   : Grace
Type                    : Virtual
License Key             : tz3R0QH2CLShe0xohlucelFfjRE=
Valid After             : 2017-09-11 10:54:41
Valid Until             : Forever
Attributes              :

Name                    : cpbx-2000-extensions
Description             : CPBX 2000 Extensions
State                   : Grace
Type                    : Virtual
License Key             : ylGW0OGhF2zS0QIYR0LmtlpgxJo=
Valid After             : 2012-08-14 16:59:09
Valid Until             : Forever
Attributes              :
- extensions                 = 2000

Name                    : complete-concierge
Description             : Complete Concierge
State                   : Grace
Type                    : Virtual
License Key             : i65UU91W9/jmsONfCtG1V9SNkOE=
Valid After             : 2018-04-03 08:59:42
Valid Until             : Forever
Attributes              :
- rooms                      = 1000
```

ABOUT Tab



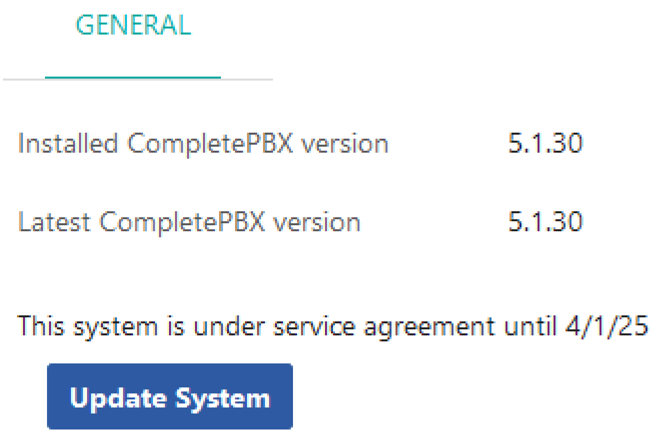
Serial Number, shows the serial number of your CompletePBX system.

After restoring a system from a Rapid Recovery backup, it will be necessary to refresh the licenses. This can be done either by clicking on the **Update** button, or running **`xlic fetch`** in the command line interface. (If a license was previously installed on the system, you will need to clear it with **`xlic clear`** command.)

Updates Dialog

This dialogue presents the current system version and the latest available version in the CompletePBX repositories.

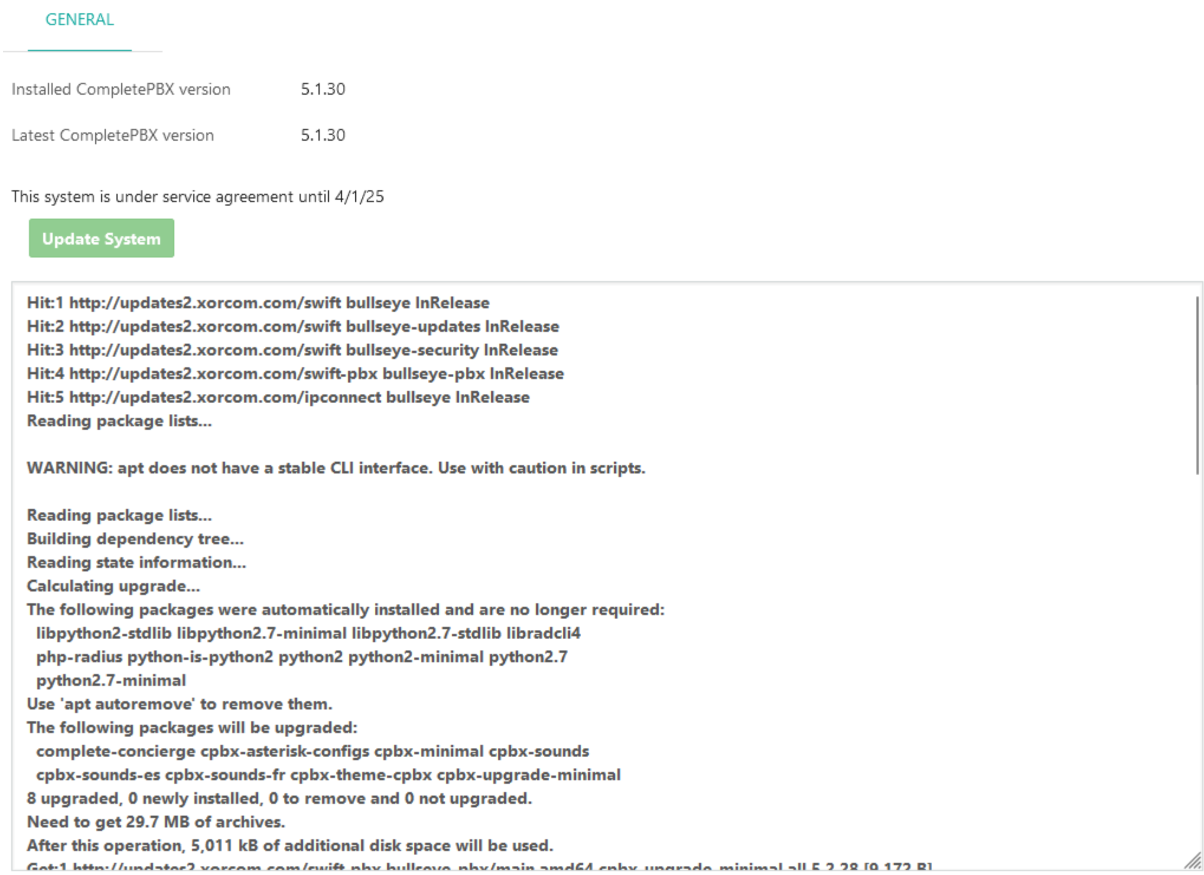
General Tab



Installed CompletePBX version, version of CompletePBX currently installed.

Latest CompletePBX version, version of CompletePBX currently available for download.

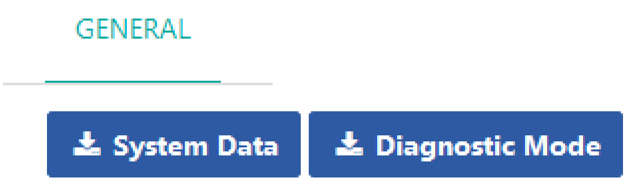
Updating the system is performed by clicking the Update System button. An update log is shown on the screen when updating the system.



Only systems under an active service agreement will receive software updates (starting from version 5.1.30). All systems under warranty, software service agreement, annual license, monthly license, and post-paid licenses will be eligible for software updates.

Diagnostics Dialog

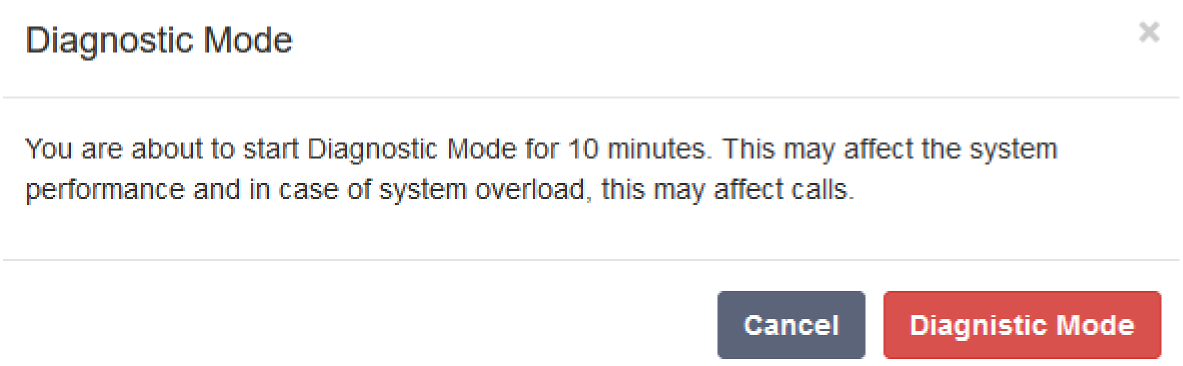
This dialog allows bulk downloading of system data.



System Data, allows to collect and download system data, including relevant software, hardware, and configuration data to assist in solving technical issues.

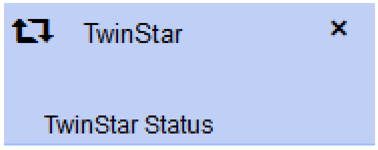
Diagnostic Mode, activate diagnostic mode for a limited time. Upon activation, the system will run in this mode for 10 minutes, after which it will turn off and download the zipped data folder. It can also be manually stopped and the full System Data report and detailed logs will be downloaded. This will allow collecting more detailed system data and logs in order to troubleshoot system issues. The correct use of this mode would be:

- Activate Diagnostic Mode. The system will gather information and start Diagnostic Mode.
- Wait for the timer to start counting down (indicating the mode is activated)
- Reproduce the issue
- Stop and Download
- Send the zipped file to the technical support representative



Running the Diagnostic Mode may affect the system performance and in case of system overload, this may affect calls.

Twinstar Menu Group

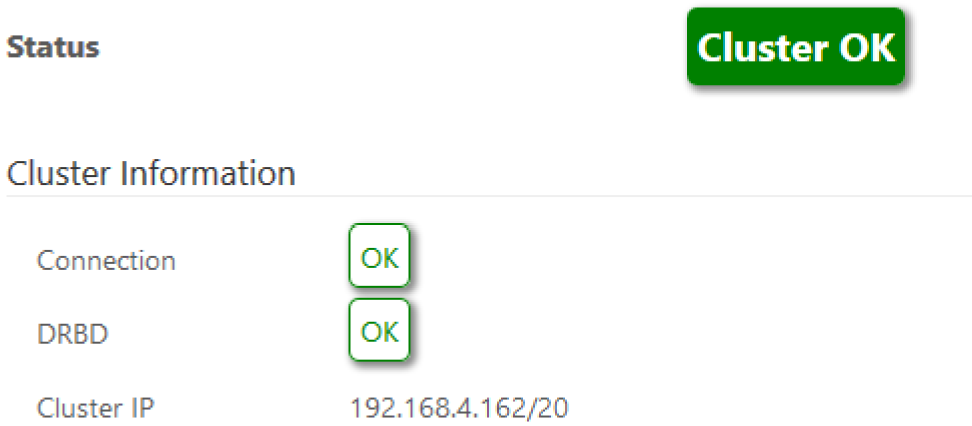


TwinStar Status Dialog

This dialog will only be shown in the Admin menu when you are managing a TwinStar cluster.

GENERAL Tab

Cluster Information Section



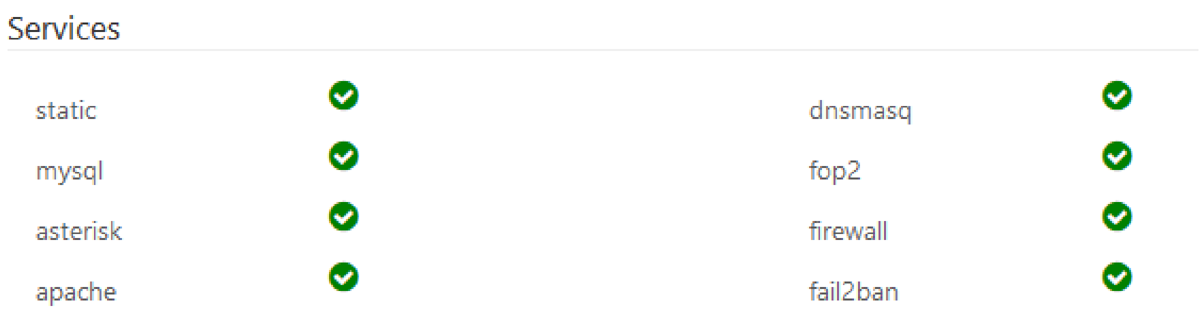
This section indicates the current status of the TwinStar cluster. If the TwinStar cluster does not have any problems, a green **Cluster OK** message will be displayed. However, if there are problems with the cluster, a red **Cluster Error** message will be displayed.

Connection indicates the current state of the connection to the TwinStar cluster.

DRBD indicates the status of the DRBD.

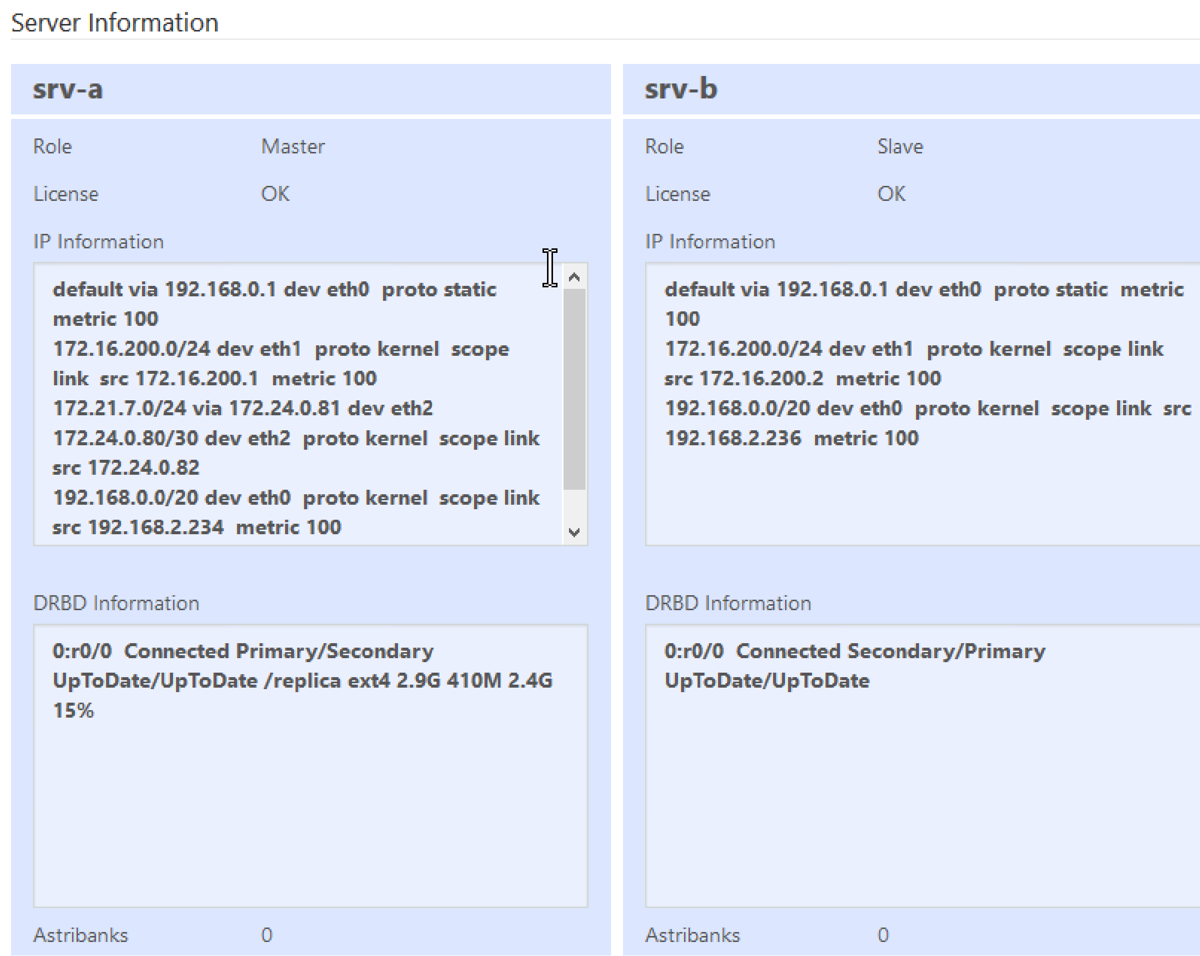
Cluster IP shows the IP address for the TwinStar cluster.

Services Section



This section displays the current status of all the services associated with the TwinStar cluster. All services that are behaving correctly will be shown with a green ✔ symbol. Any service that is not behaving in the correct manner will be shown with a red ⍰ symbol.

Server Information Section



This section displays information about each server in the TwinStar cluster.

Role indicates whether the server is acting as the Master or Slave within the TwinStar cluster.

License indicates the current state of the TwinStar license for each server

IP Information details the IP information associated with each server in the TwinStar cluster

DRBD Information shows the current status of the DRDB (Distributed Replicated Block Device)

Astribanks shows the status of any Xorcom Astribanks that are connected to the TwinStar cluster.

7. User Portal

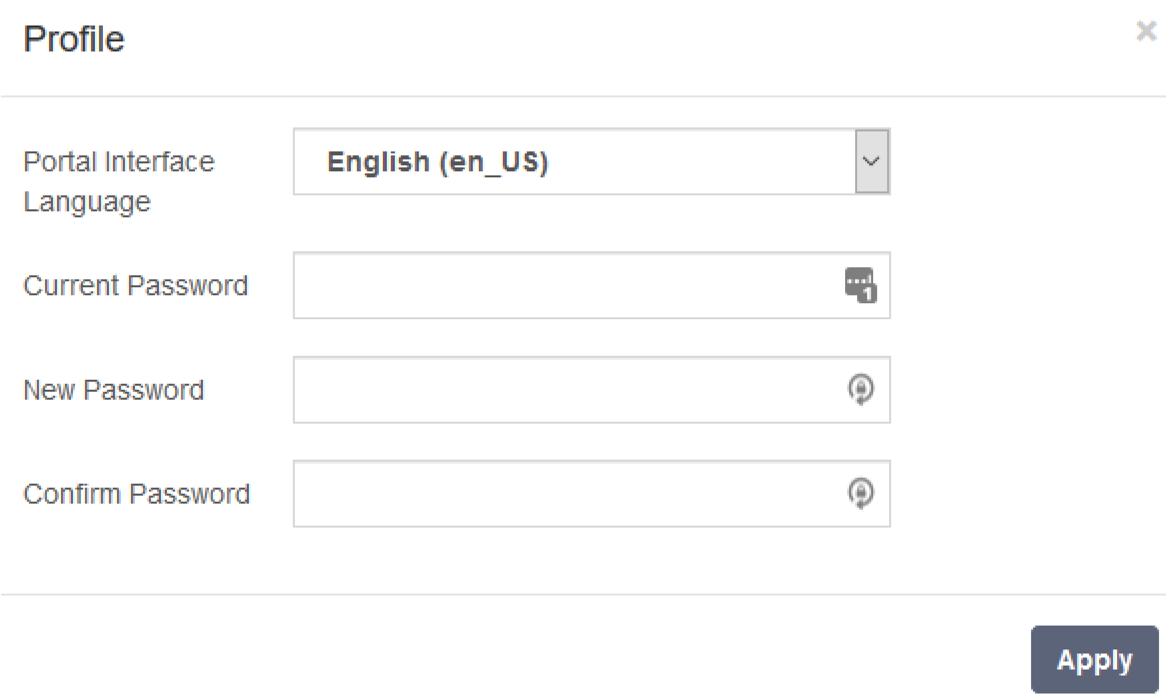
Portal

About

Just like CompletePBX 5, the Portal also has an About dialog. This dialog has three menu items:

Profile

Use this menu to configure your user profile, such as interface language and password.



Portal Interface Language, select the language from the drop-down menu with which you want to view the Portal

Current Password, if you want to change your Portal password, you will need to enter your current password

New Password, enter your new password,

Confirm Password, confirm your password by entering it a second time

If you have defined your system (in the Admin > Security > Passwords dialog) to enforce a policy of password security, the password must be at least 14 characters long, and not include repeating patterns (like 123123123123123). The password may consist of upper- and lower-case characters, numbers, and special symbols, but should not include spaces. As you enter a password, a colored bar will be displayed below the password to indicate the strength of your password; ranging from red, indicating a weak password; to green, indicating a strong password.

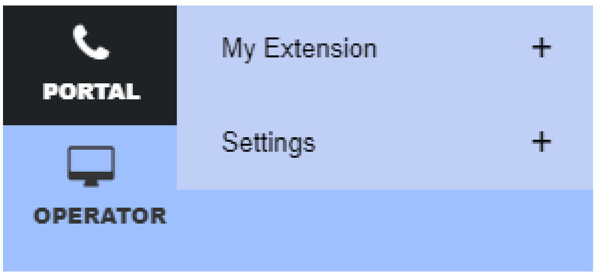
About

Use the menu to see the current version of your system:

Logout

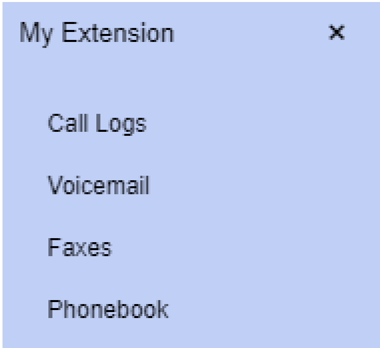
Use this menu to log out from the Portal.

General



Portal provides every extension user access to a number of dialogs to give them better control of the behavior of their extension. Each user is only able to see and modify settings that relate to their own extension, and cannot see or modify settings relating to extensions belonging to other users. The Portal also provides each user with access to lists of their emails, call history, and faxes.

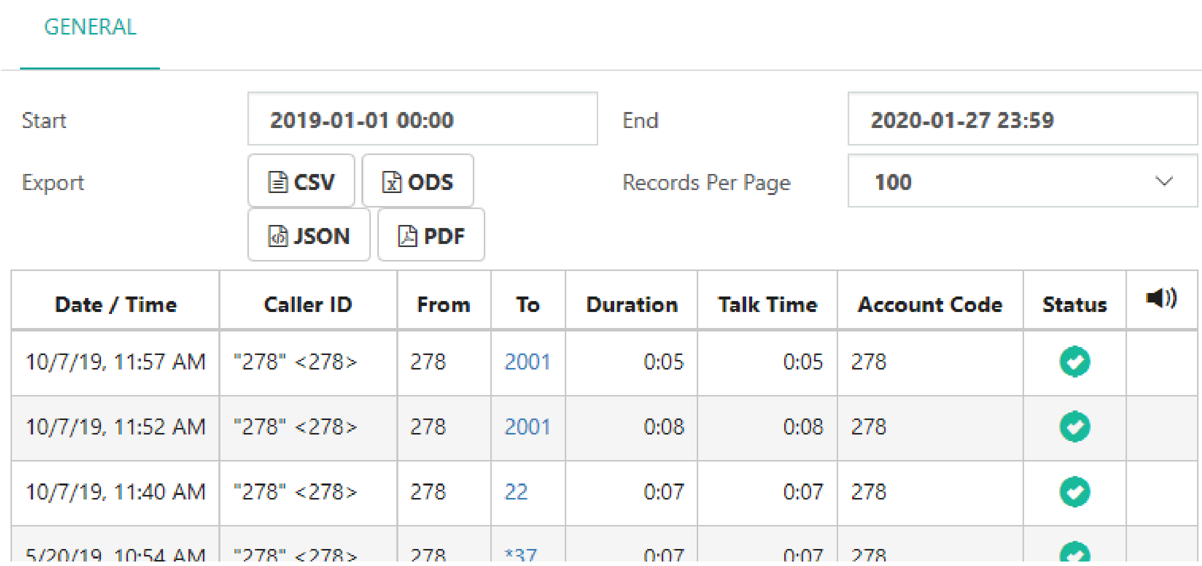
My Extension Menu Group



Call Logs Dialog

Displays the log of calls made to and from your extension.

General Tab



Start, sets the start date for the call records that you want to view.

End, sets the end date for the call records that you want to view.

Export, clicking on any of the displayed export options (CSV, ODS, JSON, or PDF) will export the currently displayed calls to be exported in the selected format. The file will be saved in your default download directory, with the name of CDR Records.<extension-type>.

Records Per Page, determines the maximum number of calls records that will be shown in each screen.

After changing any of these parameters, click on the **Search** action button in order to refresh the data display in accordance with the parameters that you have defined.**Date/Time** indicates when the call was made.

Date/Time, shows the timestamp of the call

Caller ID shows the name (if available) of the caller.

From shows the numbers that made the call. In the case of outgoing calls, this will be your extension number. You can click on the number that is displayed to initiate a call between your extension and the **From** number.

To indicates the number that was dialed. You can click on the number that is displayed to initiate a call between your extension and the **To** number.

Duration shows the overall length of the call, in minutes and seconds. This includes the time that the phone was ringing before the call was answered.

Talk Time shows the actual length of talk time, in minutes and seconds.

Account Code, where present, shows the account to which the call will be charged in your billing system.

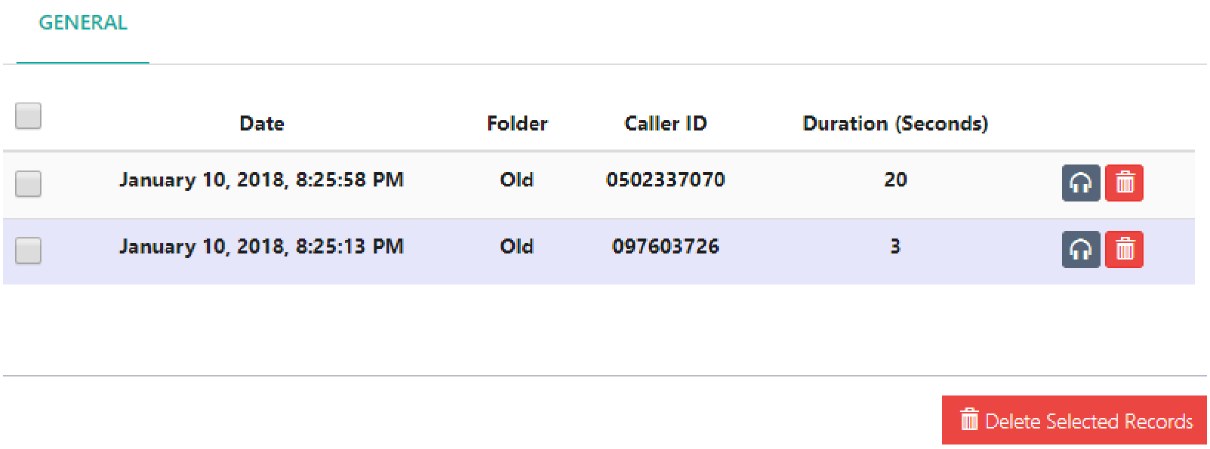
Status indicates how the call was completed:

- No Answer – the call was not answered
- Congestion – the call could not be completed due a congested resource
- Failed – the call failed
- Busy – the party that you called was busy
- Answered, - the call was answered

- allows you to listen to a recording of the call, if a recording exists.

Voicemail Dialog

GENERAL Tab



General Section

Lists voicemail messages that have been left for you. You can use this dialog to listen to voicemail recordings by clicking on the icon to the right of each voicemail message.

Date, timestamp of the voicemail message.

Folder, current location of the voicemail message. Voicemail messages that have not been moved to another folder will initially be located in the INBOX location.

Caller ID, the name (if available) and number of the person who left the voicemail message.

Duration (Seconds), the duration of the voicemail message.

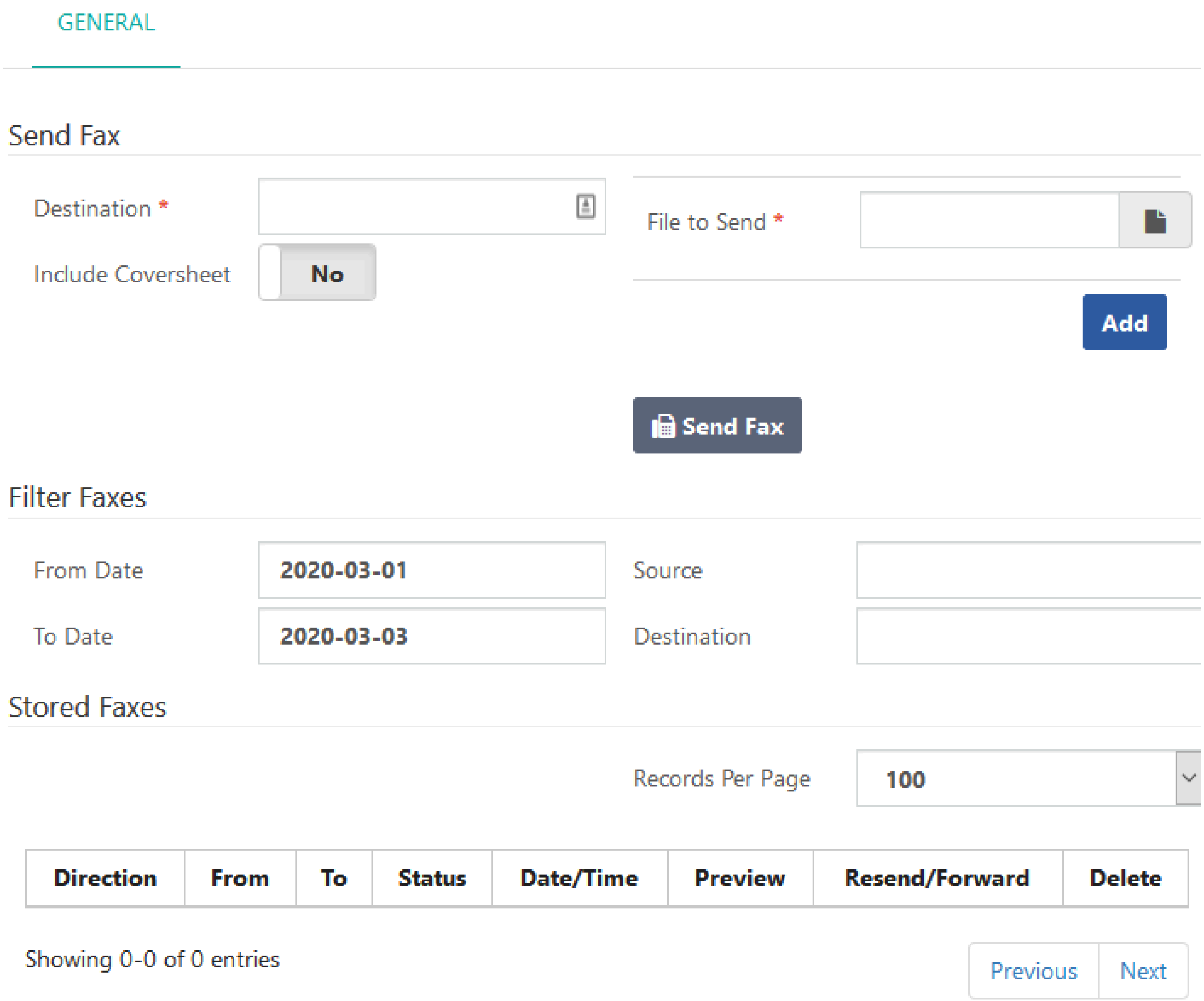
Action Icons

- Click on this icon to listen to the recording
- Click on this icon to delete the recording

You can select multiple rows of voicemails (using the checkbox at the beginning of each row), and click on the **Delete Selected Records** action button to delete unwanted voicemails.

Faxes Dialog

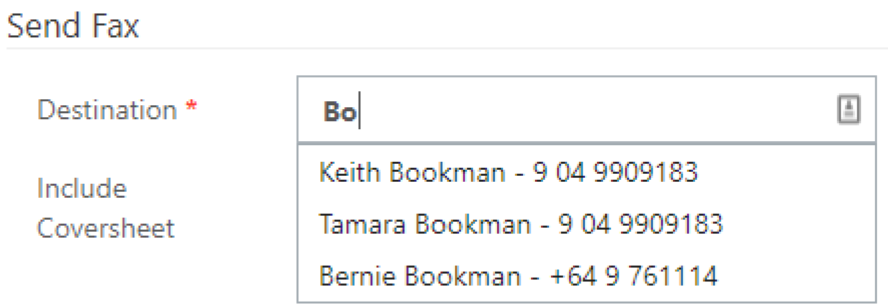
GENERAL Tab



Send Fax Section

Destination*, is the full fax number of the person to whom you are sending the fax. Do not forget any code that may be required by your phone system to access external lines or to access international service providers. If the Portal user has any phonebooks available (i.e. phonebooks where **Show in Portal** has been configured as **Yes**), the system will automatically search the phonebooks and suggest destinations as you enter your input.

For example, if you start typing **Bookman**, you will immediately be shown a list of all fax destinations that match the name:



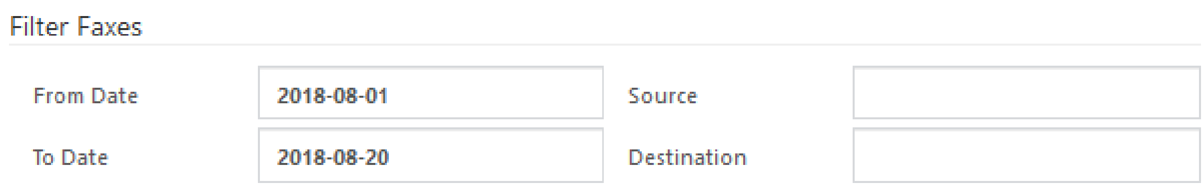
Include Coversheet, indicates whether you want to add your standard coversheet to this fax.

File to Send*, allows you to browse to the file that you want to send as a fax. The file can only be in pdf format. Click on the **Add** button to include additional pdf documents in the fax, or click on the trash icon to remove a document that you have previously added.

The **Add** button that allows you add additional documents to the fax.

Filter Faxes Section

Use this filter option to display just the faxes that you are interested in. If you leave any value empty, then all values will be displayed



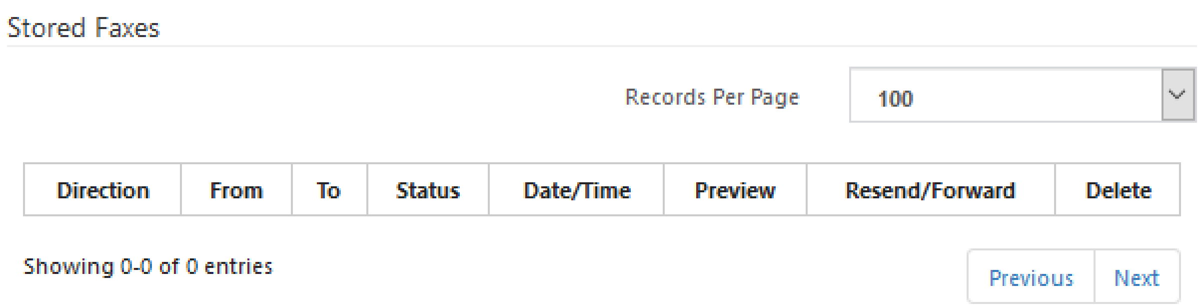
From Date, limit the display to only display faxes sent (or received) after the **from** date

To Date, limit the display to only display faxes sent (or received) before the **to** date

Source, insert a single value to display faxes sent from a specific source

Destination, insert a single value to display faxes sent to a specific destination

Stored Faxes Section



Records Per Page, limits the numbers of faxes to be displayed on each screen

Direction, shows an icon that indicates whether fax was inbound or outbound.

From, shows the CallerID Name (if the information was available) and number of the person who sent the fax (in the case of an inbound fax), or the extension name and number from which the fax was sent (in the case of an outbound fax.)

To, shows the user who received the fax (in the case of an inbound fax) or the number to which the fax was sent (in the case of an outbound fax.)

Status, shows the status of the fax. Mouse over the icon to see the full text message.

Date/Time, displays the timestamp when the fax was received (in the case of an inbound fax), or sent (in the case of an outbound fax.)

Preview, clicking on the icon allows you to view the complete fax that was sent, including the coversheet (if requested) and all documents, in pdf format.

Resend/Forward, clicking on the icon allows you to resend the fax, or forward it to a new recipient

Delete, allows you to completely remove the stored fax from the system by clicking on the trash icon

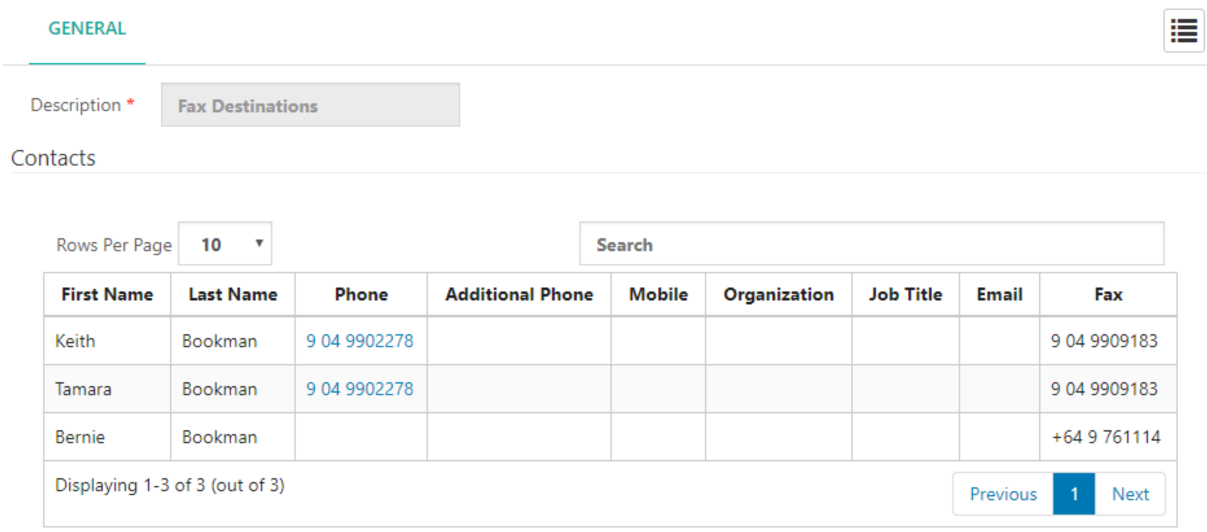
Previous, press this button to see the previous page of stored faxes

Next, press this button to see the next page of stored faxes

Phonebook Dialog

GENERAL Tab

After you click on the **Show All** icon (on the right-hand side of the screen) and select an existing phonebook, the screen will look something like this:



First Name	Last Name	Phone	Additional Phone	Mobile	Organization	Job Title	Email	Fax
Keith	Bookman	9 04 9902278						9 04 9909183
Tamara	Bookman	9 04 9902278						9 04 9909183
Bernie	Bookman							+64 9 761114

The displayed fields are:

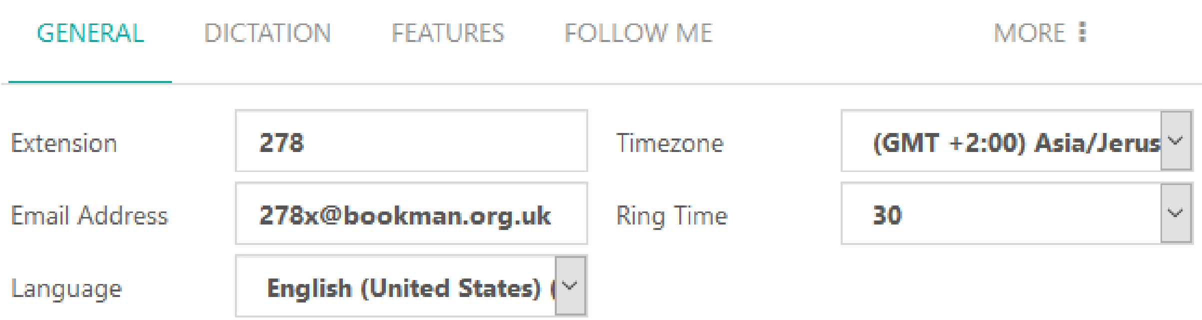
- **First Name**, first name to be associated with the phonebook entry
- **Last Name**, last name to be associated with the phonebook entry
- **Phone**, phone number to be associated with the phonebook entry
- **Additional Phone**, another phone number to be associated with the phonebook entry
- **Mobile**, mobile phone number to be associated with the phonebook entry
- **Organization**, company or organization that should be associated with the phonebook entry
- **Job Title**, job title that should be associated with the phonebook entry
- **Email**, email address that is associated with the phonebook entry
- **Fax**, fax number to be associated with the phonebook entry

Click-to-call: you can click on any phone number that is displayed to call the selected number. A call will be placed to the selected number, and your own extension will ring. Pick up your phone to speak with the party that you have chosen to call.

Settings Menu Group

Extension Settings Dialog

GENERAL Tab



Extension, displays the number of the current extension. This field cannot be modified.

Email Address, valid email address that can be used when sending voicemail to email, or for receiving faxes. If voicemail is enabled for the extension and a valid email address is entered in this field, any time a voicemail is left for the extension an email message will be sent to the address entered here. By default, the message will simply notify the user that a new message has been left for them.

Only one address can be entered into this field.

Language, specifies the language to be associated with this extension. This will force all prompts specific to this extension to be played in the selected language, provided that

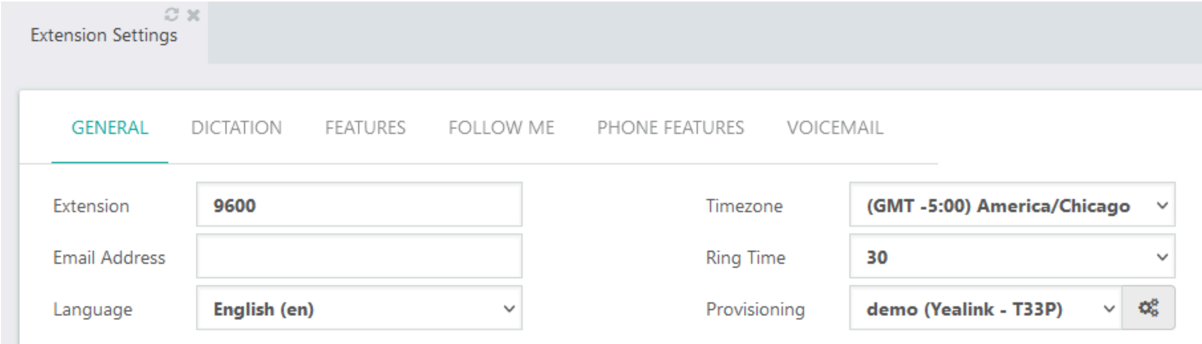
- the language is installed on your server
- voice prompts for the specified language exist on your server.

If the field is left blank, all prompts will be played in the default language of the system.

Timezone, timezone that should be associated with this user. This will affect timestamps displayed in the Call Logs, Dictation, and Voicemail.

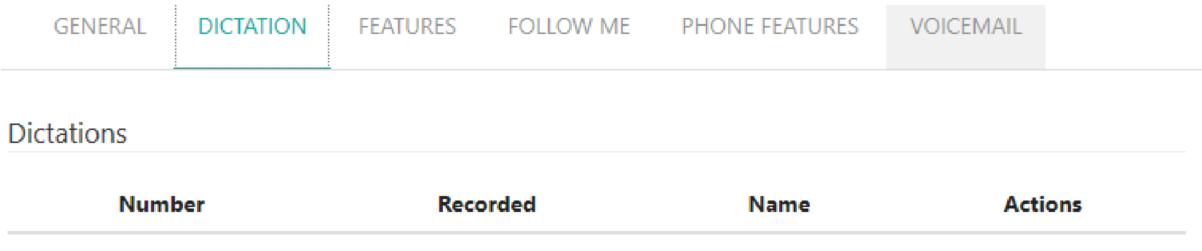
Ring Time, sets (in seconds) how long your phone will ring, before the call will be transferred to the next available destination (such as email).

IP Phone Provisioning available for IP phone devices:



- The provisioning button will open all the provisioning options for that device, as found in Settings -> Endpoint Manager -> Templates. This allows the admin or user to edit Device Buttons, Expansion Modules, and Advanced Settings for that specific device.
- Users do not need to have permissions to Endpoint Manager to edit these parameters.
- **NOTE** that the phone must first be associated with the extension in Endpoint Manager, and only after that it can be accessed via the Provisioning button in the Device or User Portal.

DICTATION Tab



Dictations Section

Number, a system-allocated number used to uniquely identify each dictation.

Recorded, timestamp to indicate when the dictation was recorded.

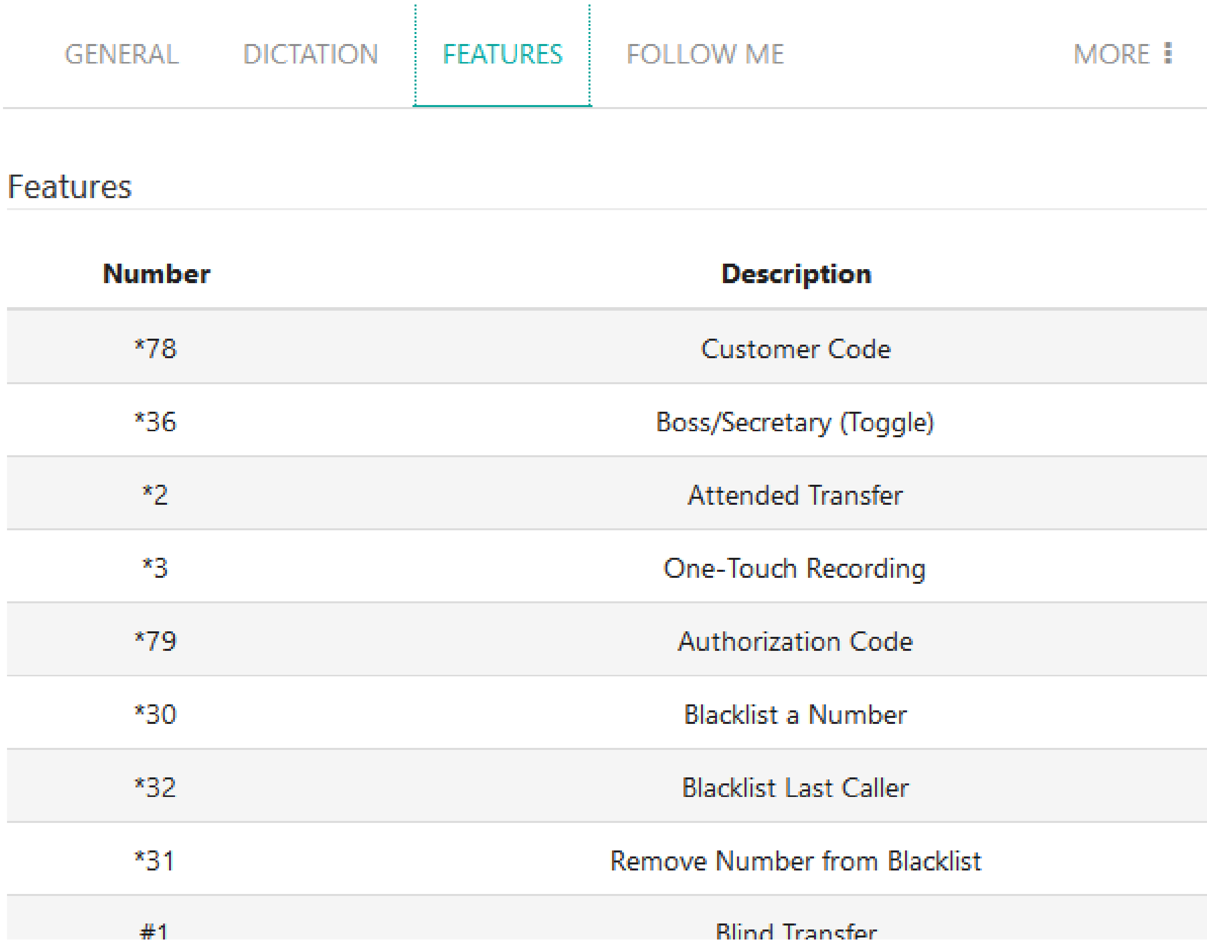
Name, name that you gave to the recording

Actions, action that can be performed on each dictation. Available actions are:

- Edit
- Listen
- Delete

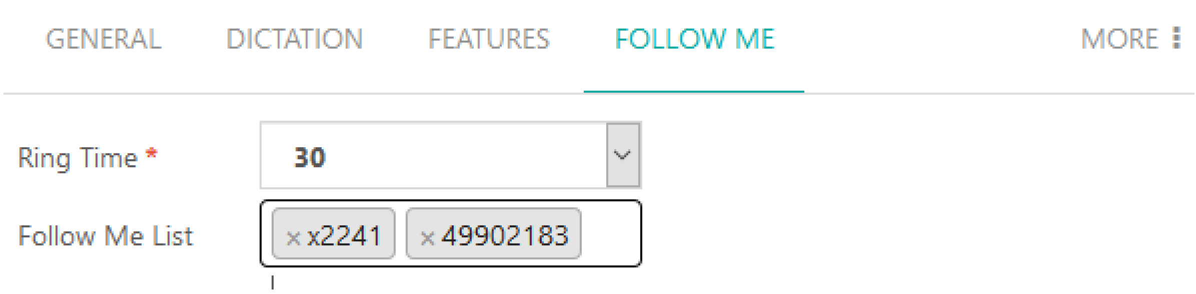
FEATURES Tab

Lists all the feature codes that are available for your extension.



Number	Description
*78	Customer Code
*36	Boss/Secretary (Toggle)
*2	Attended Transfer
*3	One-Touch Recording
*79	Authorization Code
*30	Blacklist a Number
*32	Blacklist Last Caller
*31	Remove Number from Blacklist
#1	Blind Transfer

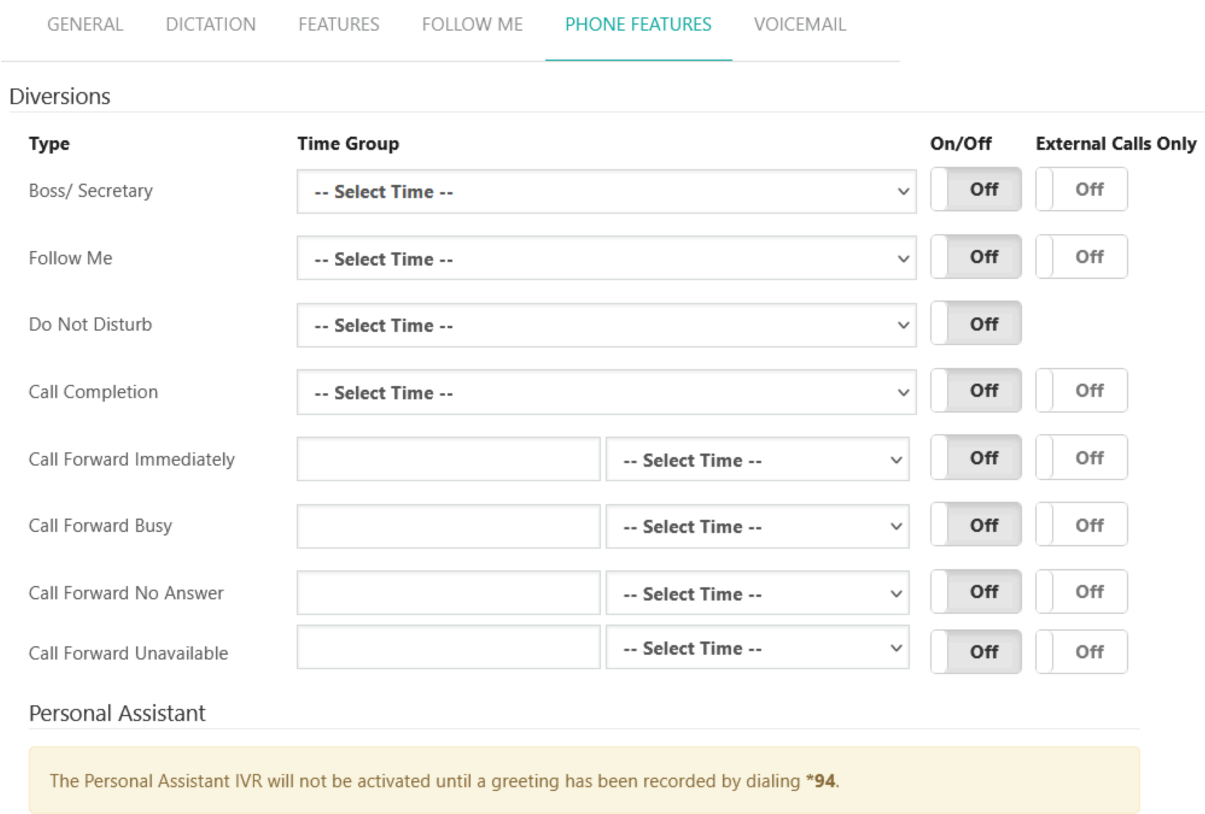
FOLLOW ME Tab



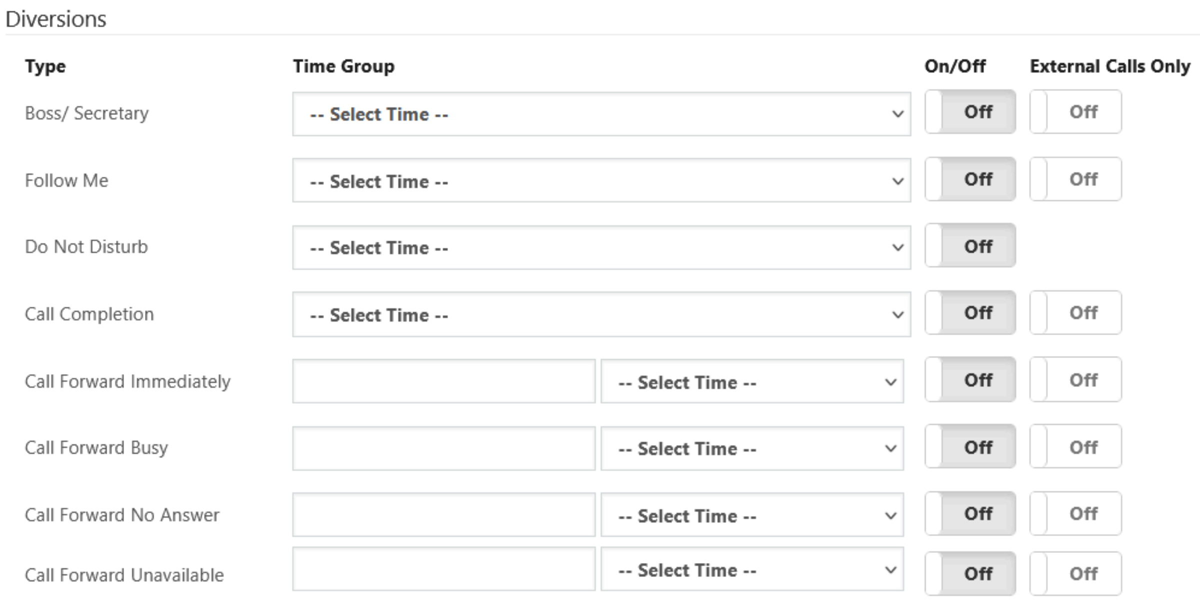
Ring Time*, determines how long to ring the numbers listed for follow me, before continuing to an alternative destination, such as voicemail or hangup.

Follow Me List, list of numbers to which the call be sent. Can be an internal extension, any other internal destination (such as a ring group, queue, etc.) or and external number. When defining an external number, take care to include any codes that may be necessary to call out to an external number.

PHONE FEATURES Tab



Diversions Section



There are three settings that you can configure for each type of diversion.

- You can restrict the activation of a diversion setting to a specific span of time, by using a time group (which you can create in the My Time Group dialog). If you do not select a time group, the diversion will be active always.
- Each diversion setting can be activated (**On**) or disabled (**Off**)
- External Calls Only allows to define diversions to external calls

Boss/Secretary, sends calls to the Secretary extension if the system administrator has defined a Boss/Secretary relationship for this extension. (This is similar to using the standard system feature code ***36**)

Do Not Disturb, prevents incoming calls from ringing your phone. Incoming calls will be treated as follows: if Call Forward Unavailable is configured, the call will be forwarded accordingly; if Voicemail is enabled, the call will be sent to voicemail; otherwise the caller will receive the busy tone.

Call Completion, call completion allows a caller to let the system automatically alert him when a called party becomes available**,** after a previous call to that party failed for some reason. You can use the On/Off switch (together with a time group) to determine whether to receive such notifications.

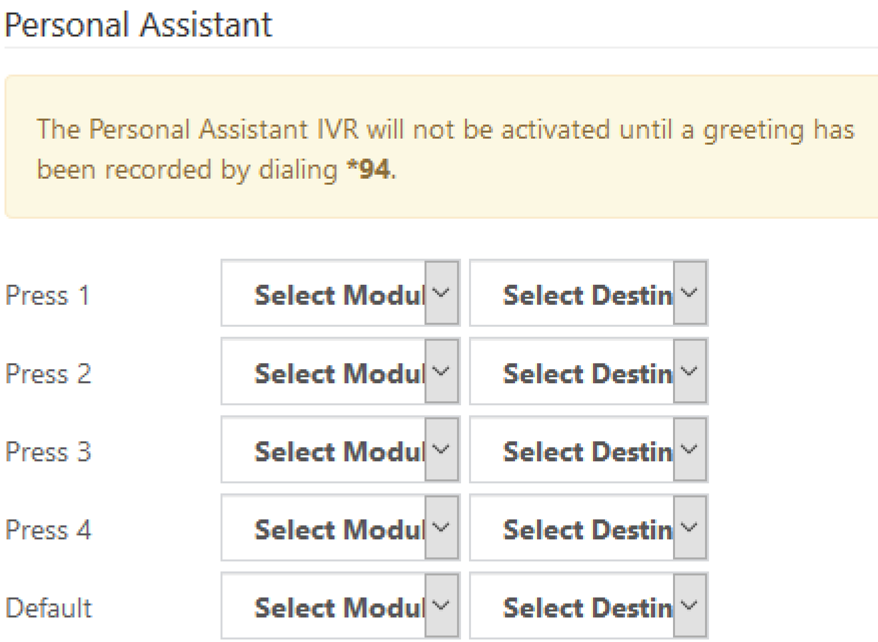
Call Forwarding Immediately, determines whether to activate call forwarding immediately. In other words, call forward will always be activated.

Call Forward on Busy, determines whether to activate call forwarding when your extension is busy.

Call Forward on No Answer, determines whether to activate call forwarding when you do not answer your extension.

Call Forward when Unavailable, determines whether to activate call forwarding when your extension when your extension is not available. You could be "not available" because you have activated Do Not Disturb, or because your phone is not currently logged into the phone system.

Personal Assistant Section



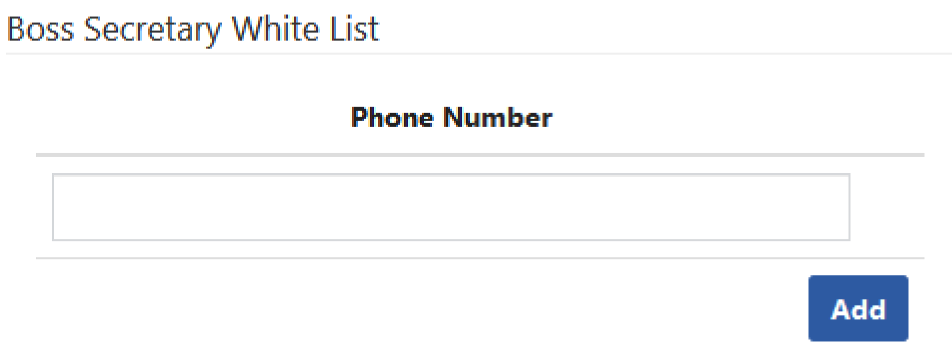
This enables you to create a personal IVR (Interactive Voice Response) menu that allows you redirect your callers in response to input from them. Before you can create a personal IVR, you must use the ***94** feature code to create a recording that will describe the available options to your callers.

It is important that you carefully plan the call flow and branching options for IVRs, while considering the user experience.

If you wish, you can restrict the activation of the Personal Assistant to a specific span of time, by using a time group (which you can create in the My Time Group dialog)

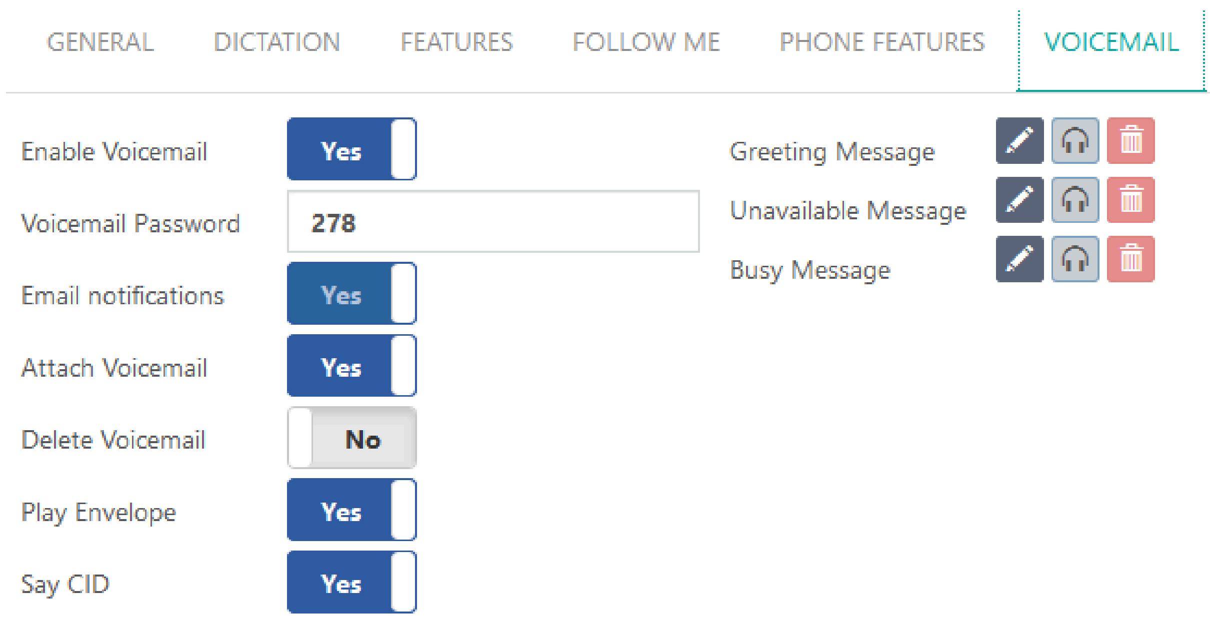
You can define how the system will behave when the caller presses any digit between 1 and 4. Additionally, you can define default behavior should be used if the caller enters an invalid option, or fails to respond.

Boss Secretary White List Section



Phone Number, the phone number that you want to add to your whitelist

VOICEMAIL Tab



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

You will be asked to change your password each time you access voicemail if the voicemail password matches the extension number.

Enable Voicemail, toggle that enables or disables voicemail. If voicemail is not enabled, voicemail messages cannot be left for the extension.

Attach Voicemail, determines whether the voicemail recording will be attached to voicemail notification emails. Note that if this field is set to **No**, Delete Voicemail will always be set to **No.**

Delete Voicemail, causes the voicemail to be deleted from the server after the voicemail has been delivered. Be careful with this option, because the system may delete the message without guaranteeing that a copy of it has been attached to an email notification, or that the email has been delivered successfully. This could mean that after a message is left, and the system has made an attempt to send a notification email to the user, that the actual voicemail that was left may no longer be accessible.

Note that this field cannot be modified when Attach Voicemail is set to **No**.

Play Envelope, determine whether the user will hear the date and time that the message was left prior to hearing the full voicemail message being played.

Say CID, causes the system to play back the **Caller ID** number of the person who left the message, prior to playing the full message.

Greeting Message, the message that you want to play to callers when they reach your voicemail. You can use the **Edit** icon to upload a new message, the **Listen** icon to hear your current message, or the **Delete** icon to delete your current message.

Unavailable Message, the message that you want to play to callers when you are not available. You can use the **Edit** icon to upload a new message, the **Listen** icon to hear your current message, or the **Delete** icon to delete your current message.

Busy Message, the message that you want to play to callers when your line is busy. You can use the **Edit** icon to upload a new message, the **Listen** icon to hear your current message, or the **Delete** icon to delete your current message.

Icons used for Managing Messages:

 Edit icon

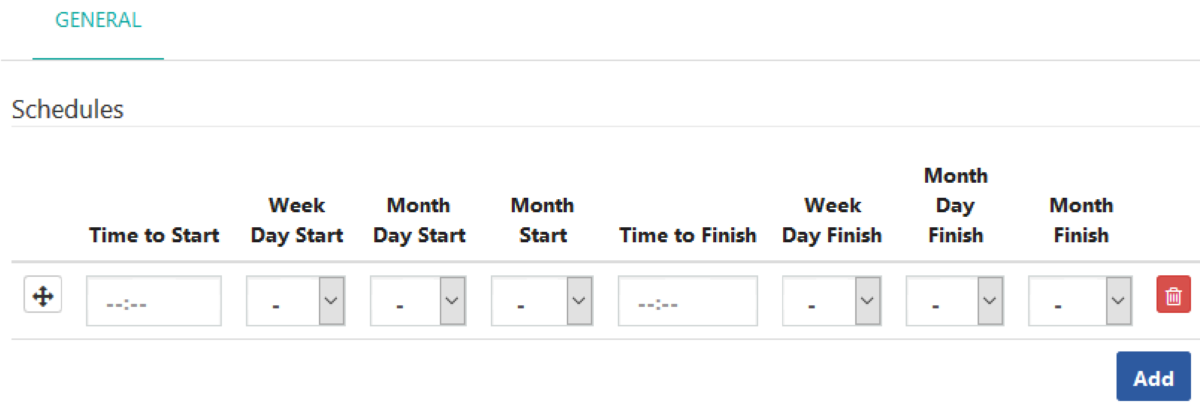
 Listen Icon

 Delete icon

My Time Group Dialog

GENERAL Tab

Allows you to specify a period of time that can be used when configuring call diversions.



Time to Start, the time when the schedule should begin.

Week Day Start, the day of the week (i.e. Monday, Tuesday, Wednesday, etc.) when the schedule should begin.

Month Day Start, the day of the month (i.e. 1, 2, 3, etc.) when the schedule should begin.

Month Start, the month (i.e. January, February, March, etc.) when the schedule should begin.

Time to Finish, time when the schedule should end.

Week Day Finish, the day of the week (i.e. Monday, Tuesday, Wednesday, etc.) when the schedule should end.

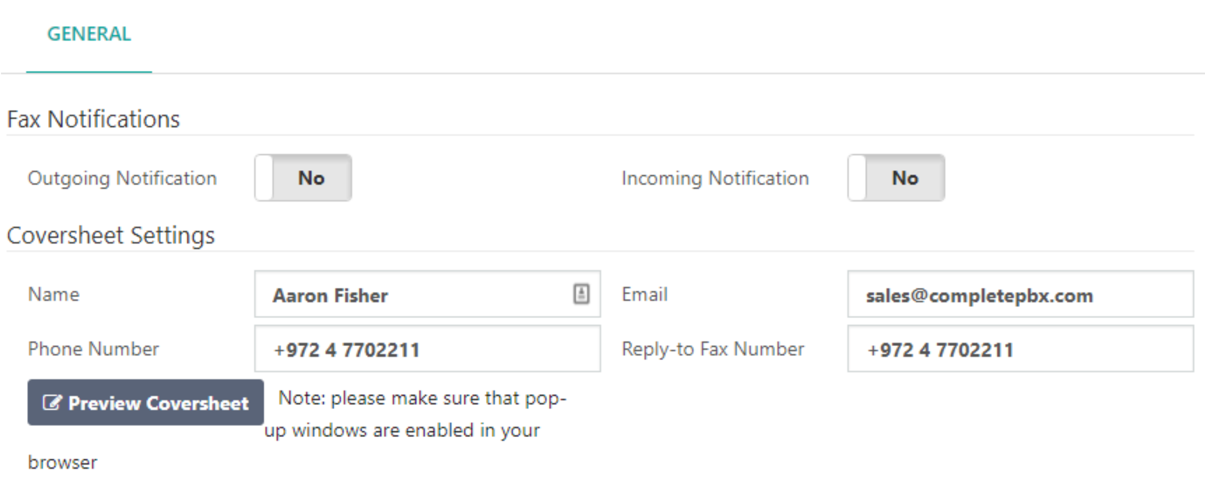
Month Day Finish, the day of the month (i.e. 1, 2, 3, etc.) when the schedule should end.

Month Finish, the month (i.e. January, February, March, etc.) when the schedule should end.

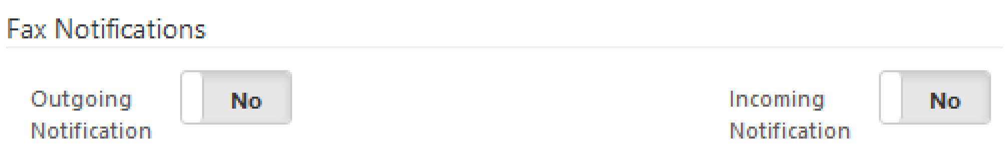
If any of the fields are left blank, the system will assume that the field is not relevant. For example, if you define Time to Start, but leave Week Day Start empty, the schedule will start at the start time ***every*** day of the week.

Fax Settings Dialog

GENERAL Tab



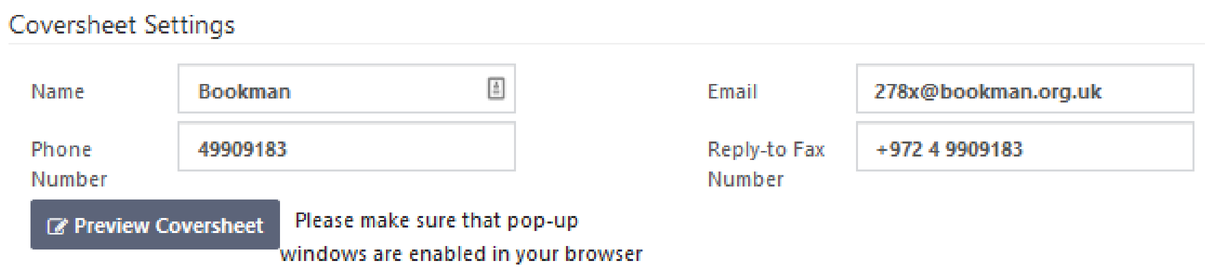
Fax Notifications Section



Outgoing Notification, when set to **Yes**, sends a notification to the email associated with the extension when an outbound fax has been sent.

Incoming Notification, when set to **Yes**, sends a notification to the email associated with the extension when an inbound fax has been received.

Coversheet Settings Section



Name, the sender's name that will be displayed on the coversheet of outgoing faxes

Phone Number, the phone number that will be displayed on the coversheet of outgoing faxes. This is the phone number that the recipient of the fax should call if he wants to contact the sender of the fax.

Email, the email address that will be displayed on the coversheet of outgoing faxes. This the email address to which the recipient of the fax should send an email to if he wants to contact the sender of the fax.

Reply-to Fax Number, is the fax number which will be displayed on the coversheet from which outbound faxes will appear to be sent, to enable the recipient to reply by fax

Preview Coversheet, pressing this button allows the user to see a preview of their personalized coversheet.

Make sure that your browser allows pop-ups if you want to preview the coversheet.

Operator Menu Group

Switchboard Dialog

After a successful login, you will be presented with the panel window. There is a toolbar that is always visible at the top, and four sections in the content area: one for each kind of button.

General Tab

The button corresponding to your extension (the one you used to login), is always at the top left of the Extension block. Its label will be highlighted with a bold font.

Each block has a title bar with a plus/minus button to the right. Clicking on the button will collapse or expand the view of the section. The collapse state is remembered across all future sessions. Suppose that you are not interested in trunks: you can collapse the section and it will remain minimized until you click the plus sign again.

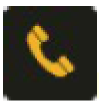
Anatomy of the Toolbar

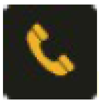
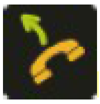
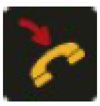
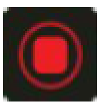
At the top of the panel there is a toolbar. From here you will perform most of the actions that can be done with the Switchboard. There are some distinctive sections as follows:

Action bar

The action bar consists of a row of buttons that represent actions that can be taken for active calls. The buttons will be displayed only is the user has been given permission for the action. To activate an action, you need to first select the destination or target button with a click of the mouse. After you have done that, the borders of the target button will turn to red.

After selecting a target extension, you can perform your command by clicking on the appropriate action button. The following actions are available:

Button	Action
 Dial	Required permission: **dial** Will originate a call to the button previously selected from the list of available extensions. Your phone will ring and after you pick it up, it will call the requested destination extension

Button	Action
 Transfer	Required permission: **transfer** Will initiate a call transfer to the button previously selected from the list of extensions
 Transfer to voicemail	Required permission: **transfer** Will initiate a transfer to the voicemail of the selected extension
 Pickup	Required permission: **pickup** Will pick up the ringing extension that was selected.
 Listen	Required permission: **spy** Will start a call-spying session. It will first ring your phone, and after you pick it up, it will start listening to the previously selected extension.
 Whisper	Required permission: **whisper** Will start a call-spying session with whisper enabled. It will first ring your phone and when you pick it up, it will start spying on the previously selected extension. You can then talk to the target extension without the other party hearing you.
 Hangup	Required permission: **hangup** Will hang up the first active call on the selected extension.
 Record	Required permission: **record** Will initiate or stop recording on the selected extension. A call that is being recorded will be marked with a cassette icon.

Filter Box

Type text in this input box to filter out any button having a label that does not match your filter. If you have a panel with a hundred buttons and you only want to see the state for “Bob”, just type “Bob” into the input box, and all buttons except those containing “Bob” will be hidden.

Dial Box

The dial box is powerful option, with multiple actions:

Option	Action
Dial to a phone number	When your phone is idle, just type in a number and press ENTER: your phone will ring and will originate a call to that number
Transfer to any number	When you are on an active call you can type in a number (either an internal extension or an external number) and press ENTER. This will transfer your current call to that number.
Invite any number to a conference	If you select a conference button, type a number in the dial box, and hit enter, the Switchboard will originate a call to the number typed, and will send the call to the selected conference.
Direct VoIP dial	Type a sip address with the format: SIP/$(ext)@$(domain) and the Switchboard will originate a direct sip call to that extension @ server.
Phonebook search	Anything you type here will be searched in the visual phonebook as you type, and results will appear as a selection list at the bottom of the box. You can use the arrow keys to select the proper result, and then click on ENTER to originate a call to the selected number.
.tel domain lookup	If you type a .tel domain, the system will perform a DNS domain lookup and display any matching results that are found. You can find voice numbers, direct VoIP dial, and Web sites. If you select a result and press enter, a call will be originated to the phone number, direct VoIP call, or the target Web page will be opened in a new window.

Presence Select Box

You can use this to set your presence information. The information is stored in the CompletePBX database, and is immediately shown to other Switchboard users. Any presence state other than **Available** will set your phone into **do-not-disturb** (DND) mode. In a similar manner, if you use the appropriate feature code (*78 or *79) to toggle the DND status of your extension, the change will also be reflected in the Switchboard.

The presence state will not affect your dialing behavior: it will just tell other Switchboard users about your current availability.

A little presence icon on your button will reflect your status. If you mouse over the presence icon of any extension you will see a tooltip with the textual state, in addition to the color.

If the standard present states do not answer your requirements, the last option in the select box, named **Other,** allows you to specify any free text for your presence.

Extensions

Extension buttons show lots of information packed in a small rectangle. There are two colors for the button:

- green indicates that the extension is free and not engaged in a call
- red indicates that the extension is busy and currently engaged in a call

The icon will remain green when the extension is ringing, but the line icon will indicate the ringing state. There is also an additional (yellowish) color that is used when DeviceAndUser mode enabled in CompletePBX to indicate that the device is in adhoc mode. This is an example button that is ringing:

The button has a number of elements:

Element	Explanation
1 - Presence icon	Indicates the presence state for the extension. Green circle means that the extension is not in a call. Red circle indicates that the extension is busy or in a call. Little card icon indicates a special presence that was set by the user. The color of the custom presence is configurable. If you mouse over the icon, a tooltip with the custom presence text will appear. Tape icon indicates that someone initiated a call recording from within the Switchboard, and that the call is now being recorded. Clicking on the presence icon will display an action menu: if you have the appropriate permission, you will be able to add, remove, or pause the member in a queue, or send an email to that user (if the email setting is defined in the button configuration).

Element	Explanation
2 - Button Label	Displays the text label for the extension. It shows the extension number followed by the text label that is associated with the button.
3 - Information icon	Shows if the extension is paused, by showing a clock (for queue agents). If the extension is engaged in a call that came from a queue, mousing over the icon will display an informational icon that will show the queue from where the call came from.
4 - Voicemail icon	This icon, in the shape on envelope, indicates if there is voicemail waiting or stored for the extension. The number of messages is displayed in the tooltip when you mouse over it.
5 - Line activity icon	Indicates whether the line is ringing, is engaged in an outgoing call (right arrow), engaged with an incoming call (left arrow), or on hold (hourglass).
6 - Line callerid	Shows the callerid name and number, if available
7 - Line timer	Shows the timer for the current call.

Performing Actions

Buttons can be clicked to select or deselect them. When a button is selected, the border of the button will become red. Once a button is selected it will become the target button for any action that you choose.

Every button in the toolbar requires that a destination button also be selected. Clicking an action button with no extension selected will not trigger any action. Some actions will work only on the active line for that extension. For example, if an extension has two calls, and one of them is on hold, if you click the record button it will start recording only the active line and not the line on hold. The same happens with the hangup button: if you have two calls on your phone and one is on hold, clicking the transfer button will redirect your **active** call, and not the call on hold.

To transfer a call, when talking to someone, click on the target extension (which will be highlighted in red) and then click the transfer button on the toolbar.

To record a conversation to disk, click on the extension button that you want to monitor and then click on the record button on the toolbar.

Action Submenu

The presence icon for any type of button can be clicked to perform additional actions. A single click on the icon will cause a popup menu to appear, listing the available actions for the selected button. In this manner, you can add, remove or pause agents in a queue, send email to users, or pickup parked, queued or trunk calls.

The action submenu for extensions allows you to send emails to users (if the email setting is defined in the button configuration). You can also pause or un-pause a queue member, or you can add or remove the extension from any available queue. You cam pickup calls from parking slots, trunks and queues.

The submenu for queue agents allows you to remove them, pause, or un-pause them.

For conferences you can perform global actions or individual actions, such as mute, unmute, lock, unlock, etc.

Visual Phonebook

At the top right-hand side of the main panel window, there is a phonebook icon. When clicked you will be presented with a phonebook application where you can add, edit or delete entries. Click on the **Add** button to insert new records, or click the action buttons for each record to view, edit or delete them. There is a search box that allows you to search for any string or number. There is also an **Export** button that lets you export your phonebook in CSV format.

Phonebook entries will be searched in real-time when you type something on the Dial box, so it can be used as a company directory. It will also be searched when an inbound call is received. If the caller id matches one of the entries, it will use the name and picture of the contact for a call notification that will pop up at the lower right hand of the Switchboard screen as depicted below:

Importing Data

You can import CSV data into the Switchboard phonebook by clicking the Import icon. When you click it, it will show you an extra field where you can type or search for the CSV file to import. The first line on the CSV file must contain the field names, and the following lines the records you want to insert.

A sample file would look like this

```
firstname,lastname,company,phone1,phone2,private
Nacho,Rodriguez,Telecorp,123900001,125900002,no
John,Doe,Simcorp,55555555,,606,no
```

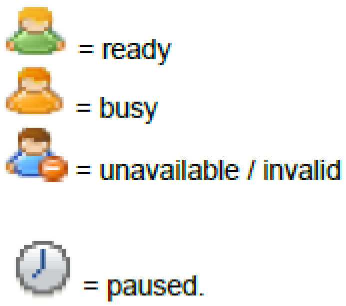
Most fields are self-explanatory, such as **firstname** and **lastname**. The **private** field lets you mark whether a record as private or not; private records can only be edited or viewed by their owner.

Queues

Queue buttons have some particularities. Besides the queue name, they will show the list of agents belonging to the queue, with a little icon representing the member state, and also the list of calls waiting on the queue with their call counter and timer, as depicted below:

They also can be used to filter out extension buttons. When a queue button is selected, only the extensions that are part of the queue will be displayed. This is particularly useful for call center managers, so that they can focus on a particular queue activity, removing the 'noise' of other queues and extensions.

The state icon for the queue agents might be:



The Switchboard can also monitor agent or device names, and rename extension buttons accordingly.

Pickup Queued Calls

You can click on a call waiting in the queue to display the pickup submenu. If your extension is allowed to pick up calls, you can click on the action and the waiting call will be redirected directly to your extension:

Trunks

Trunk buttons show the number of channels active for the particular trunk. Trunks also display detailed information regarding bridged calls, with channel name and callerid. It is important to note that bridged channels are the ones that are linked to another channel. Calls that are not answered, or that are inside an application, such as IVR, voicemail, etc., will not be displayed.

Click on the channel name to bring up an action submenu, with the option to pick up the call.

Clicking it will redirect the call to the logged in extension.

Conferences

Conference buttons will show all participants in the conference. They also include special actions to be performed on the conference itself or to a selected participant.

There is a little icon to the left of the conference label: click on the icon to display a special action menu that will let you lock or unlock the conference, or mute (or unmute) all participants in the conference.

To the left of every participant there is also a member icon: it will be green for regular participants, or blue when that participant is the admin user. Click on the icon to open up the action menu for the selected participant, where you can toggle mute for the user or kick them out of the conference.

You must have the **meetme** permission in order to activate these actions.

8. Call Center Statistics

Introduction

CompletePBX Call Center Stats is a reporting system for monitoring call centers based on Asterisk. The system allows you to run reports on call center activity**,** divided by and filtered by agent and time**,** which shows a detail of what happened in your call center.

The default username used to access this dialog is ***admin*****,** and the default password is also ***admin***.

We recommend that you change the admin password the first time you log in: click on the Users tab and then click on admin user.

Reports

With CompletePBX Call Center Stats you can see:

- Calls answered
- Call abandoned
- Incoming Call Statistics
- By Agent
- By Queue
- Distribution of calls by week and day
- Distribution of calls per hour
- Easy retrieval of call recordings

Reports can be executed while the call center is in operation, so that you can see information in real time, without delay.

You can also listen to calls that have been recorded right through your computer using your browser. You can also export data to comma separated files (CSV) or to PDF format.

Call Center Stats is a web based application, which means you do not need any software on the client machine, except a web browser. To view the interactive graphic, you must have the Flash Player.

Administration and Configuration of Users

As soon as you connect to the reporting system through your web browser, you must set access credentials. Call Center Stats has a powerful system of permissions to control resources, which are fully configurable by the administrative user.

Username	Key	Notes
user	user	Basic level of access Cannot create users or perform system configurations
admin	admin	Administrator Can perform all operations, including the creation of users

To create users and assign permissions, to need to log in as admin user, so that you have administrator privileges. Once logged in, you must choose the **Users** tab so that you can modify and create new accounts and their permissions.

We recommend that you change the admin password the first time you log in: click on the Users tab and then click on admin user.

To add a user, simply select the option from the menu. To delete a user, check the checkbox to the list of users or to delete and select Delete Users menu marked. To modify a user, click on the line for the user, which will open the edit screen users

Editing Users

In the edit screen, users can enter the access data such as account name and password, as well as assign access keys to select the queues and agents that may be accessed by this account. You can select all columns or choose an individual or agent in the selection box.

Access

In the system there are 3 defined access keys:

- admin
- user
- agent

These keys can be assigned individually or in combination to user accounts that you define. Depending on the keys that are assigned an account, it can access the various reports and reports as they are defined in the Edit screen in the Access Control tab Users. For example, it is possible to restrict the reporting of service level to accounts that hold the key agent only. This way, if an account is not allocated this key, the report will not be shown.

The **Access Control** menu option allows users to define the access keys that are required to access each of the reports and options in CompletePBX Call Center Stats. In normal use, there is no need for modifications. However it is possible to limit the reports to different levels of users by assigning each of the three keys of access available to them.

To change the table of access controls, simply click on the resource you want to change, view the display for editing access control. From here you can define what access keys are needed to view or select the remedy chosen.

To assign keys to make them click on the selection list. Using ctrl-click you can check more than one.

Settings and Preferences

The Setup tab lets you set preferences and general settings for the program, such as time intervals in different reports, language, and time of abandonment by default, etc.

Configuration Variables

Variable	Explanation
alarm_hold_duration	Alarm in seconds for wait time in queue in real-time view. Can be set per queue
alarm_last_call	Alarm in seconds for last call taken by agent, also for the real-time view. Can be set per queue
alarm_wait_count	Alarm (in number of calls) for calls waiting in a queue
alarm_wait_threshold	Threshold (in percentage) from which to start coloring in alarm calls.
default_end_hour	Default end hour in HH:SS format for the date/time selection
default_start_hour	Default start hour in HH:SS format for the date/time selection
dict_agent	Dictionary entry for Agents. It will replace the agent set as the parameter to the value you specify (So you can use names instead of interfaces).
dict_queue	Dictionary entry for Queues. Same as the agent dictionary, but for replacing queue names.
distribution_interval	Time interval in minutes to split the distribution table
first_page	Initial page to load (e.g. answered.php, unanswered.php, distribution.php, agent.php). Can be set per user

Variable	Explanation
honor_timeframe_in_agent	Honor time frame selection in Agent Tab Reports. It will also try to 'compute' missing events for the period if they are not in the logs
language	Language to use
minimum_abandon_duration	Duration threshold (in seconds) for a call to be considered as abandoned (if duration is less than this value, then ignore the call). Specifying the queue name as a parameter will apply the value to that queue only
no_animation	Do not use animations in bar charts
realtime_refresh	Time in seconds to refresh the real-time information. Default value is 5 seconds
recordings_path	Recordings location from which to perform the direct download.
recordings_web_url	If the table recordings is populated with unique ids and filenames, use this parameters as the start of the url to find the filename in order to be able to listen to the calls
sla_interval	Time interval in seconds to split the table for SLA (Service Level Agreement)
spychannel	Channel or device to use for spying/coaching, the parameter must be set to the stats user name and the value to the full channel name, like SIP/1234
spycontext	Asterisk context where to send spy calls, it must be similar to this one: [spy] exten => _X.,1,ChanSpy(SIP/${EXTEN},w) exten => _X.,2,Hangup

Selecting Reports

On the Home tab is a section where we will have to specify the minimum data to generate a report. These include the selection of the queue or, if having more than one, the agents and the range of dates and times.

Filtering Queues and Agents

By default the reporting system will report on all Queues and all Agents. You can filter this reporting by only selecting the specific queue(s) and specific agent(s) you wish to report on. You can then filter by Data and Time as well.

Filter by Date Range Hours

Select the date range for the reports. Some shortcuts are provided for date selection, including:

- Today: Selects the current day
- This week: Selects week beginning the Monday before
- This month: Selects from the 1st day of the month until the last day of the month
- Last 3 months: Selects the last 3 months, on the last day of the last month.

Once you have selected all the parameters to generate a report which are:

- Queues
- Agents
- Date Range
- Time Frame

Now you can click on Display Report to generate your reports.

Results

Once the report is displayed you will have a set of tabs across the top of the page. The first tab is Distribution. Quantity of calls distributed as follows:

- By Queues
- Per Month
- Per Week
- Per Day
- Per Hour
- Per Day of Week

You can scroll down the page to view each report section or click on the underlined sub-tabs in blue and jump right to that section.

In the report, whenever you see numbers or names in orange, scroll over that text with your mouse and click on the link and it will display the call details for this queue or agent. This is a common feature throughout all the reports.

Once the call detail is open and you are recording telephone calls, there is a column on the right hands side that states “Pl ay”. Scroll your mouse of the “Play” icon and a flash player will automatically begin to buffer the recorded call and begin playing it back to you. If you would like to download that specific recording to your computer, click on the green down arrow to the right of the play button and select where you would like to save the file.

It is also possible to automatically save recordings to an external server or HDD, and convert all recordings to MP3 file format.

Each report also has the option to be exported to CSV or PDF, and there is a link to each format at the end of each subsection. This is a common feature throughout all the reports.

Calls Answered

The second tab is labeled Answered. Reports on quantity of calls answered as follows:

- By Queues
- Per Agent
- Service Level
- Disconnection Cause
- Answered Calls Detail
- Transfers

You can scroll down the page to view each report section or click on the underlined sub-tabs in blue and jump right to that section.

Calls Answered Overview

The sub-reports show the time per agent and number of calls answered by each agent.

The columns are:

- **Agent**: The name of the channel / agent can display the details of each call handled. Calls: Number of calls answered by this agent
- **Call%**: Percentage of calls answered within the current selection
- **Duration**: Time in minutes cumulative total of all calls answered.
- **% Of time**: Similar to the number of calls
- **Average**: The average duration of calls to the agent
- **Waiting time**: Waiting time accrued for all calls handled by the Agent
- **% Period**: average waiting time (% Time-out calls)

There are also interactive bar graphs showing the cumulative duration of calls per agent, the number of calls, etc. Pointing the mouse you can see in detail the values that are represented in each column.

Note that the percentages (such as the percentage of length) are calculated based on 100the selection of agents that have been made, and not all of the agents. This means that if you select one agent for a report, the percentage will be 100%. This also applies to other reports

Service Level

This report shows the distribution of waiting times in queue of calls, with short time intervals of 15 seconds.

The report shows the percentage of calls that were treated within each time interval. The Delta column shows the difference of calls from the previous time interval. The percentage column displays the percentage of calls answered within that interval.

Disconnection Cause

This report shows the cause of so-called disconnection.

What is interesting about this report is that it is showing who terminated the call: the agent or the caller. To enhance the customer service experience agents should wait for the caller to hang up, prior to the agent hanging up. This eliminates the possibility of hanging up on customer when they might come back to ask another question they forgot about during their conversation right after they said “goodbye”. Customers always experience a sense of relief when the agent is still on the phone to answer that last question.

Answered Calls Detailed Report

This report shows more details on specific calls answered by an agent. When clicking on the orange hyperlink under date it will also display how and when the call was answered in the queue.

Transfers

This report shows how many calls were transferred to each extension in the time interval selected for the report. Note: When a call is transferred, the system does not record the duration of the calls within the queue.

Unanswered calls

The third tab is labeled Unanswered, which reports on:

- Abandon Rate
- Disconnection Cause
- Unanswered Calls by Queue
- Disconnection Cause
- Unanswered Calls Detail

Unanswered calls are those that have been lost (the caller could not connect with an agent). This can occur when the caller decides to disconnect by not wanting in queue or the queue decides to disconnect the caller after the end of the maximum waiting time and transfers the caller to voicemail or to another queue.

Disconnection Cause

This report shows the reason for disconnection of calls that were not completed.

The possible reasons are:

- Hangup by the caller
- Call time reached the maximum waiting time configured in CompletePBX for the queue
- Caller activated option of leaving the queue

Unanswered Calls by Queue

This report provides a breakdown of the calls by Queue that could not be completed.

If the report shows more than one queue, there will be a number and percentage of calls with regard for each queue accompanied by a graphic illustration.

Unanswered Call Details

This report details calls that could not be answered.

By clicking on the orange date and time link on the left, you can display the granular detail of the abandon call that entered the queue and when they hung up.

9. Asterisk Configuration Files

Introduction

The system administrator can easily configure Asterisk configuration files from the Linux command line interface. Take care NOT to alter any file that is provided as part of the factory installation, as the file will be overwritten by future updates.

Managing Asterisk Configuration Files

The Asterisk configuration files are read from **/etc/asterisk/ombutel** directory. You should NOT alter any file in this directory that is provided as part of the factory installation, as these files will be overwritten by future updates.

For example, if you want to make a change to extensions, you should create a new file in the same directory where the name starts with a number greater than the factory-provided files. For example, to customize extensions, you could create a file named something like **extensions__60-custom.conf**, and type into the file your custom code.

The following example adds feature code *110, that will behave in exactly the same manner as the factory-installed feature code *71 that speaks the current extension number.

```
; Duplicate feature code for *71 as *110
; Updated by William on 28Feb2017
[feature-speak_ext_number] (+)
exten => *110,1,NoOp(FEATURE *110: SPEAK MY EXTENSION NUMBER)
 same => n,Gosub(sub-speakextennum,s,1)
 same => n,Hangup()
```

After you have completed making changes, update the system by running the **asterisk -rx 'core reload'** command

Hook for Manipulating Dialed Numbers

You can create hooks to manipulate dialed numbers by using the **modify-number** context.

To use this context, you will need to create a new configuration file named **extensions__25-modify-number.conf** in the **/etc/asterisk/ombutel** directory, with the required modifications.

The following example will dial 5678 every time that a CompletePBX 5 user dials 1234:

```
[modify-number](+)
exten => 1234,1,Return(5678)
```

Managing Modules

The **/etc/asterisk/modules.d** directory contains 2 files, which control which Asterisk modules are enabled (or disabled) when Asterisk loads.

- **10-default-enabled.conf** - enables, by default, all modules
- **20-disabled.conf** - disables all modules that are not required by CompletePBX 5.

If you want to enable additional modules, you should not modify either of these files. Instead, you should create a new file, located in the same directory, that starts with a number greater than the factory-provided files. For example, if you want to enable the chan_console module in place of the chan_alsa module, you could create a file, and name it something like 30-console.conf. The number at the beginning of the file name is important (as this determines the order in which the configuration files are loaded) but the rest of name is not important.

Use the **+** or **–** symbol to indicate whether a module should be enabled or disabled. Leave at least one blank space, and then enter the module name. Note that any line beginning with the **#** symbol will be ignored.

To enable the chan_console module, you should type **+ chan_module.so** in the file that you created. To disable chan_alsa module you would enter **– chan_alsa.so**

So your file, which you could name as 30-console.conf, could look something like this:

```
# Change console module
# Updated by Bill on 29Feb2018
- chan_alsa.so
+ chan_console.so
```

After you have completed making all your changes, update the system by running the **/usr/share/ombutel/scripts/ast_mods_ctl** command, and then the **systemctl restart asterisk** command.

10. Sngrep

The sngrep utility allows you to record and analyze SIP traces on a remote PBX system. You can connect to the PBX by using SSH. This utility is pre-installed on the latest CompletePBX 5 images.

Using the sngrep utility means that there is no need to record SIP activity, and then download the trace file for analysis with WireShark!

Interface

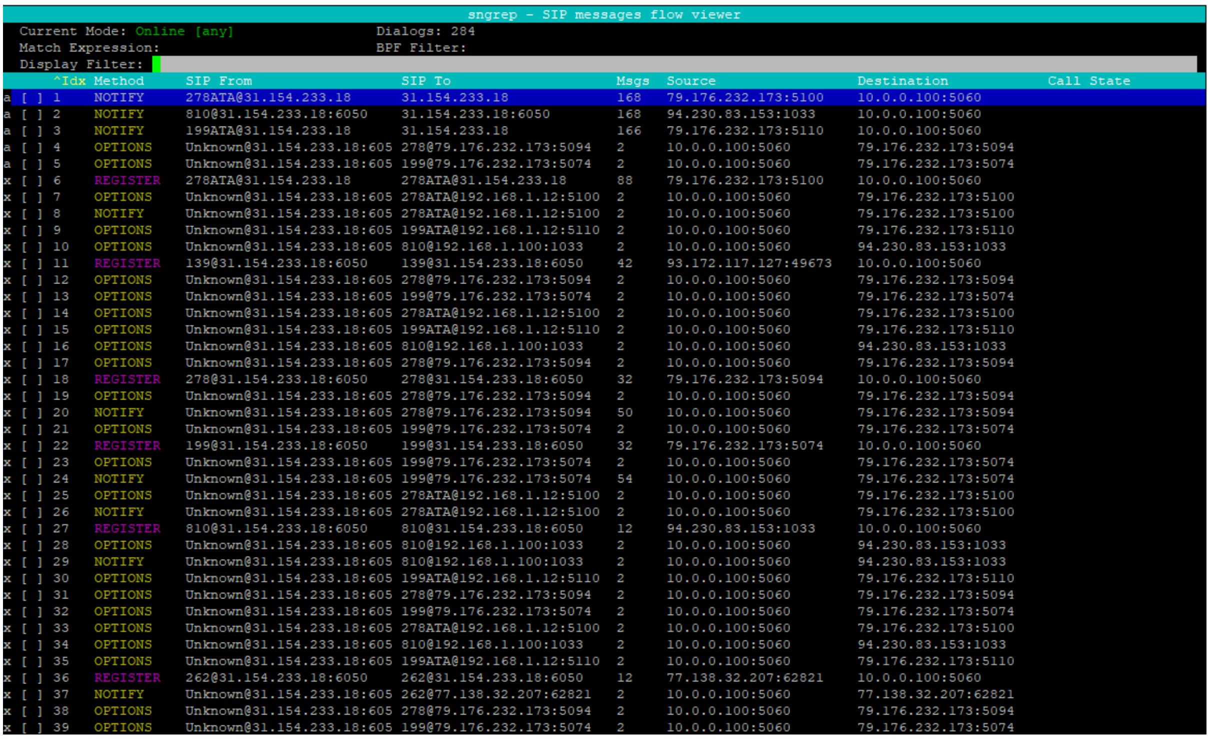
There are multiple windows to provide different information:

- **Call List screen,** allows you to select the calls to be displayed
- **Call Flow screen**, shows a diagram of source and destiny of messages
- **Call Raw screen**, displays SIP messages texts (useful for copy messages to clipboard)
- **Message Difference screen**, displays differences between two SIP messages

Shortcut Keys

Shortcut keys are shown at the bottom of the dialog. The usage of the shortcut keys are not the same for all screens

Call List Screen



Idx, line number index

Method, Type of SIP message

SIP From, SIP message From

SIP To, SIP message To

Msgs, Numerical count of messages

Source, Source IP and port number

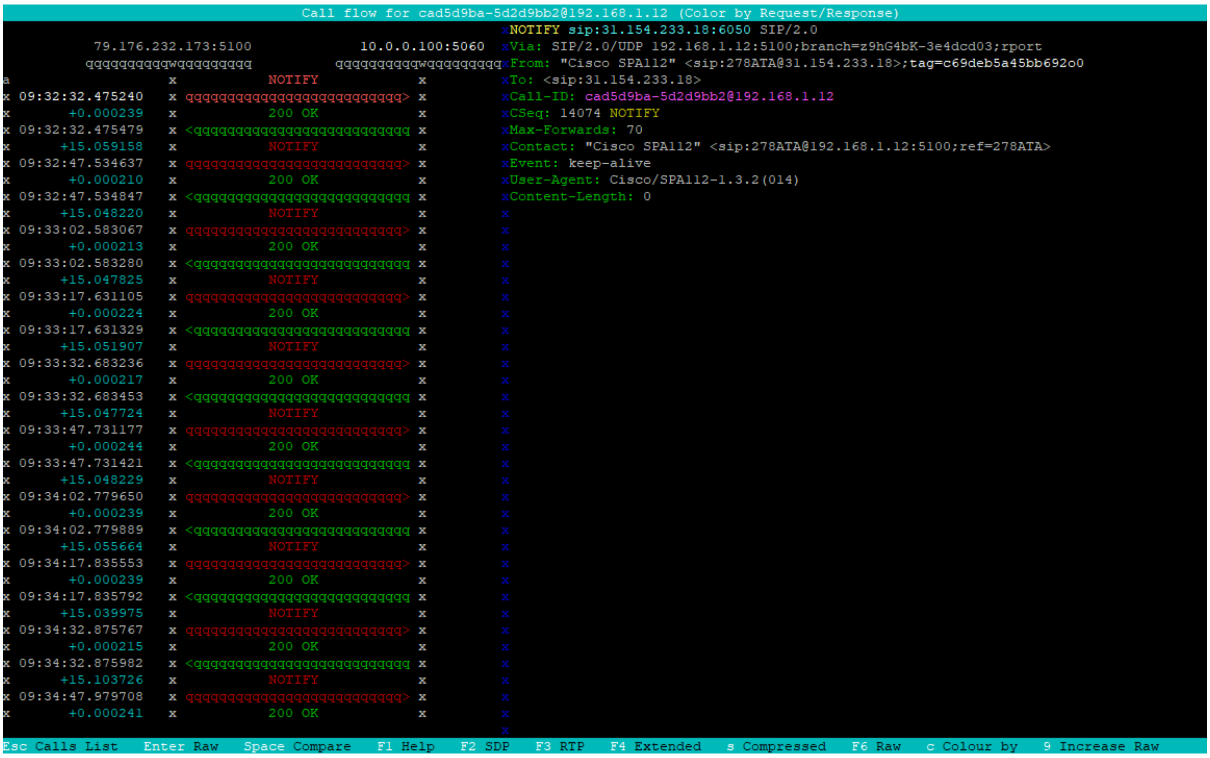
Destination, Destination IP and port number

Call State, Call identifier

Shortcut Keys in Call List Screen

Shortcut	Description
Esc	Move backwards through screens or dialogs, or quit the utility
Enter	Show more information about the highlighted line item.
F1	Displays the help menu
F2	Save the current capture session dialogs to a .pcap or .txt to a specific path and file name.
F3	Opens a text box at the top of the screen, allowing you to create a filter and search the displayed data
F4	Provides an extended view
F5	Clear the screen
F7	Like search but with more options to filter the end result
F8	Adjust sngrep settings interface, capture options, call flow options, and EEP/HEP Homer options
F10	Configure what columns are displayed on the open sngrep window.

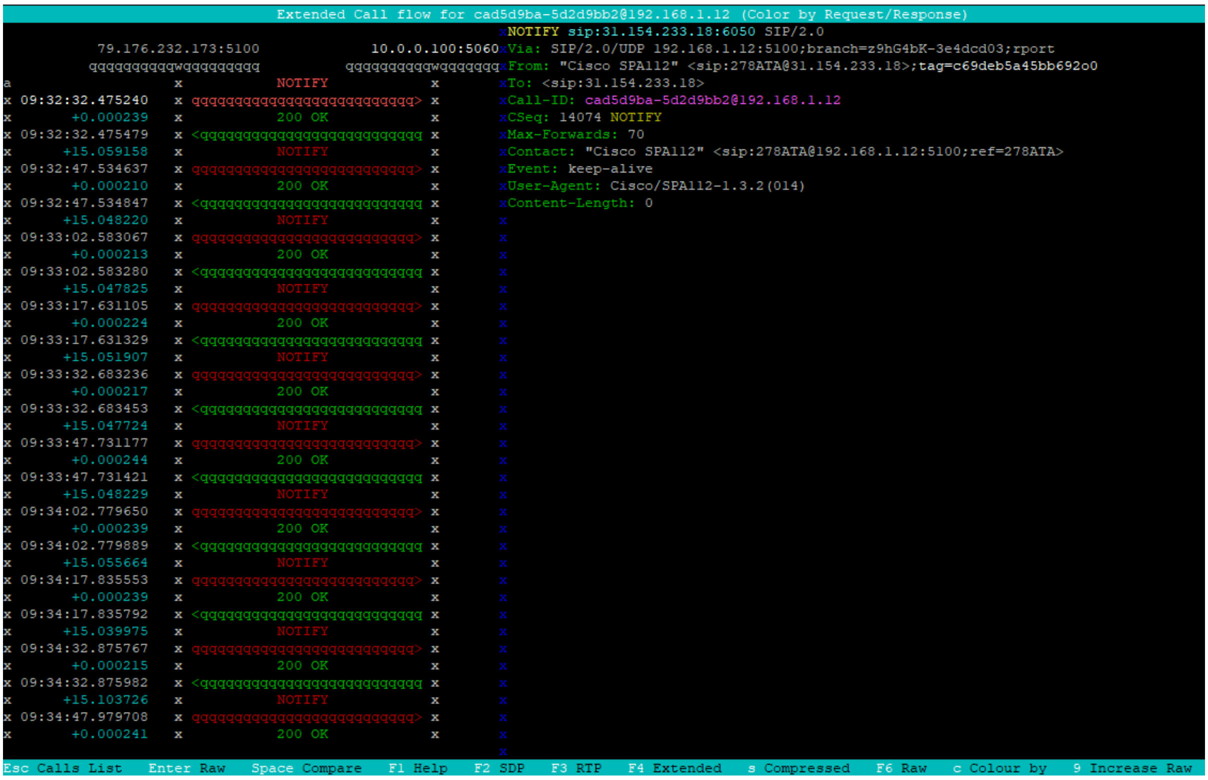
Call Flow Screen



Call Raw Screen

Message Difference Screen

Displays the time difference between messages:



Command Line

sngrep [-hVcivNqrD] [-IO pcap_dump] [-d dev] [-l limit] [-k keyfile] [-LH capture_url] [<match expression>] [<bpf filter>]

Short Form	Long Form	Description
-h	--help	This help
-V	--version	Version information
-d	--device	Use this capture device instead of default
-I	--input	Read captured data from pcap file
-O	--output	Write captured data to pcap file
-c	--calls	Only display dialogs starting with INVITE
-r	--rtp	Capture RTP packets payload
-l	--limit	Set capture limit to N dialogs
-i	--icase	Make case insensitive
-v	--invert	Invert

Short Form	Long Form	Description
-N	--no-interface	Don't display sngrep interface, just capture
-q	--quiet	Don't print captured dialogs in no interface mode
-D	--dump	Print active configuration settings and exit
-f	--config	Read configuration from file
-R	--rotate	Rotate calls when capture limit have been reached
-H	--eep-send	Homer sipcapture url (udp:X.X.X.X:XXXX)
-L	-eep-listen	Listen for encapsulated packets (udp:X.X.X.X:XXXX)
-k	--keyfile	RSA private keyfile to decrypt captured packets

Command Line Examples

- Capturing all SIP packets from all devices that has source or destination port 5060

```
sngrep port 5060
```

- Displaying SIP packets from eth0 device that has as source or destiny 192.168.0.50 through the 5061 port, saving them to /tmp/sip_capture.pcap

```
sngrep -d eth0 -O /tmp/sip_capture.pcap host 192.168.0.50 port
5061
```

- Displaying all SIP packets for a given host in sip_capture.pcap PCAP file

```
sngrep -I /tmp/sip_capture.pcap host 10.10.1.50
```

- Linux users may add capture permissions to sngrep to avoid running it as root

```
setcap 'CAP_NET_RAW+eip' /usr/local/bin/sngrep
```

or

```
setcap 'CAP_NET_RAW+eip' /usr/bin/sngrep
```

11. System Protection & Utilities

Introduction

At this stage, we have a fully-functional system configured precisely the way we need. Now, we need to make sure it stays that way. Even with the best hardware, the failure of a system component is a danger that is always present. Without proper protection and backups, we could wind up without a working PBX and have no way to restore it. In this chapter, we will discuss the following:

- System protection using UPS devices, redundant components, and surge protection
- Making one-time backups
- Configuring recurring backups
- Restoring a backup
- Maintaining backup sets

System Protection

There are many ways to protect the components of a server from failure or damage. As the system controls voice communications for a company**,** these protection methods are even more important since any downtime means lost income and angry employees.

While the installation and setup of the equipment listed here is beyond the scope of this documentation**,** it is worth keeping them in mind during installation.

Uninterruptible Power Supplies

An **Uninterruptible Power Supply** (**UPS**) is essential to every VoIP system. A UPS acts as a battery backup in the event of a power failure. If the power supply is cut, anything plugged into the UPS will continue to run until the battery runs out. Most UPS units will also be able to send a shutdown signal to the server when the battery is nearly empty, allowing a clean shutdown.

Some UPS units will also provide a power conditioning service, sending a stable level of power to any attached device. This protects any attached equipment from surges or dips on the power line that can be very damaging. Note that power conditioning is not included in all the makes and models of UPS, so be sure to check before purchasing.

Also note that for a VoIP PBX to continue to be truly effective during a power outage, it must be able to maintain an Internet connection for any VoIP trunk. It is generally a good idea to ensure that the UPS will power not only the PBX but also any modems, routers, and switches required for connectivity.

Redundant Components

Xorcom provide options for various types of redundant components. The most common redundant component is the hard drive**,** usually set up in a RAID configuration. This means that even if a hard drive fails**,** the system can continue to run without any downtime. Power supplies are another common redundant component. Redundant power supplies allow the server to continue to operate even after the failure of a unit.

Surge Protection

The most common type of surge protection is for power lines, but surges can affect other components of the system that will impact functionality. If analog lines are in use with analog ports, a power surge down the phone lines can ruin equipment. A power surge down a cable or DSL line can take a modem out of operation, or any other routing equipment attached to it. It is important to install surge protection on these types of entry points to the system.

Rapid Recovery

The Xorcom Rapid Recovery (XRR) is a unique accessory that can back up the system (including the operating system) to a USB Disk-on-Key (DOK). It enables simple, safe and speedy recovery of your system. Note, however, that by default, logs, voicemail, and call recording files are not backed up. They can be marked for inclusion in the backup, if desired. For more information about customizing the backup, contact support@xorcom.com

Instructions

- Connect a monitor and keyboard to your system
- Connect your Xorcom Rapid Recovery (XRR) to a USB port of the system
- Power on the system while pressing the F11 key, which will cause the system to boot from the disk-on-key
- The following option screen will appear

- Choose the first option (Backup/Restore), or just wait for 5 seconds, when the system will automatically begin to load the XRR software).
- The next option menu will now be displayed.

Main Menu

To create a backup, choose the "Backup" menu option, and define a descriptive name for the backup file:

Choose the target for the backup, and backup your system (depending on the configuration you have selected, the backup will take up about 1 GB and will take a few minutes.

Restore

- Choose the "Restore" menu option.
- Choose the appropriate backup file that you want to restore from, and restore your system.

Note that it is possible to keep several backups on the same disk-on-key. Each backup is saved as a separate folder under the disk-on-key 'backup' folder. You can delete the folder if you don't need a particular backup anymore.

12. Xorcom Support

Xorcom Hardware Licenses

Access the server via SSH protocol and type the following command to see which USB devices are connected:

 # lsusb

Your output should look similar to this:

Note the bus number and the device number for the USB device that has an ID beginning with "e4e4". In the above example, the first Astribank bus number is 001 and the device number is 023. You can use the following command to receive a listing of the current license of the unit, using information that you collected from the *lsusb* command above:

astribank_allow -D /proc/bus/usb/[Bus #]/[Device #]

Based on the information returned from the *lsusb* command above, the command line would look something like this:

astribank_allow -D /proc/bus/usb/001/002

Copy the text from the screen to the clipboard. The relevant text begins with

---------BEGIN TELEPHONY DEVICE LICENSE BLOCK----

and ends with

---------END TELEPHONY DEVICE LICENSE BLOCK----

Applying a New Xorcom License

Access the server via SSH protocol, stop both Asterisk and DAHDI, and type the following command to see which USB devices are connected:

```
# lsusb
```

Your output should look similar to this:

Note the bus number and the device number for the USB device that has an ID beginning with “e4e4”. In the above example, the first Astribank bus number is 001 and the device number is 023. You can use the following command to apply the updated license to the unit, using information that you collected from the *lsusb* command above:

```
astribank_allow –D /proc/bus/usb/[Bus #]/[Device #] -w
```

Based on the information returned from the *lsusb* command above, the command line would look something like this:

```
astribank_allow –D /proc/bus/usb/001/002 -w
```

Copy the text of the updated licence that you received from Xorcom to the clipboard, and paste it into the command line by typing Ctrl-D

Restart the Astribank and check that all of the required ports are available, using the following commands:

```
/usr/share/dahdi/xpp_fxloader reset

dahdi_hardware –v
```

Managing Echo

Managing Echo in Telephony Systems

Echo in telephony systems is a phenomenon in which one caller hears the echo of his own voice after a short (or long) delay, together with the remote party's voice. There are two sources of echo in telephony systems:

- Network echo, which is produced by the interface between the two-wire local subscriber loop (a telephone set, for example) and the four-wire transmission system of telecommunications trunk lines (PBXs, PSTN, etc.).
- Acoustic echo, which is caused by feedback at the terminal device level, such as phone speaker acoustic feedback to its microphone.

Both types of echo can occur simultaneously in any single connection, compounding the negative effects. Although echo can be generated on both sides of the line (as a matter of fact, at each point that the four-wire system interfaces with the two-wire system), the echo that degrades phone call quality is typically generated on the other party's equipment (the remote side).

The reason that the local echo does not affect the call is simple: when a portion of the voice energy is fed back into the earpiece with a very small delay (milliseconds), we hear it as the positive feedback of a working telephone line.

Telephone sets are designed to feed our voice back from the microphone to the earpiece, and the local echo is just an additional volume that is perceived as acceptable.

Reducing Echo

The main reason for line echo generation is impedance mismatch. Impedance is the circuit resistance to AC signals, and it changes with frequency. The first step to reduce echo is to match impedances.

This is done in two steps:

- Set the country (in /etc/zaptel.conf loadzone = [your country]) and adjust the impedance of the FXO ports to match those of the PSTN lines.
- Fine-tune the impedance matching by running the “FXO Tune” program (execute the “fxotune” command as root user). This program sends a tone to the telephone line and listens to the echo level. It checks the echo with different parameters, and chooses the parameter set that produces the least amount of echo.

Eliminating Echo

The procedure described above will decrease the echo, but will not eliminate it. Echo cancellation is done by a signal processing code that compares the digital voice that is sent to the circuit with the digital voice that is received by the circuit. When a pattern is identified, the signal processing program subtracts it from the outgoing signal, producing an echo-free signal for transmission.

You can find more detailed information about echo in VoIP telephony systems by navigating to: http://www.linuxjournal.com/article/8424 and http://www.gipscorp.com

Managing DAHDI Channels

Xpp_blink Utility

You can use the xpp_blink utility to determine the physical location of a DAHDi channel on an Astribank. The syntax of the utility is as follows:

xpp_blink {on|off|bzzt} {span <number>} | chan <number> | xpd <bus number> [xpd number>] | label <label>}

Some common examples:

xpp_blink on xpd 00 will cause the LEDs of the Astribanks to blink

xpp_blink on label usb:X000150 will cause the LEDs on the appropriate Astribank to blink

xpp_blink on span 4 will activate the LEDs of the XBUS-00/XPD-00 module

xpp_blink on chan 42 will blink the LED corresponding to DAHDI channel 42

xpp_blink off chan 42 will stop blinking the LED corresponding to DAHDI channel 42

Adding an Astribank

Initially, when a CompletePBX is manufactured, a utility is activated that populates all the available DAHDI (analog) channels in the Extensions dialog. These channels will be designated with extension numbers like 20xx, where xx indicates the channel number on the Astribank. However, if you run this utility after you have configured parameters for DAHDI channels, the information will initialized, and any changes will be over-written, and lost.

If you need to add an Astribank to an existing configuration, you need to ensure that the new Astribank is logically located after the existing Astribanks. As a result, the channel numbers of the new Astribank will continue from the last channel of the last existing Astribank. You can use the *lsDAHDi* command to determine the sequence of the Astribanks. The output will look something like this:

```
[root@yaad-cpbx5 ~]# lsdahdi
### Span  1: XBUS-00/XPD-00 "Xorcom XPD [usb:X1045601].1: E1" (MASTER) CCS/HDB3/CRC4 ClockSource
  1 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
  2 E1         Clear       (In use)  (EC: OSLEC - ACTIVE)
  3 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
  4 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
  5 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
  6 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
  7 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
  8 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
  9 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 10 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 11 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 12 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 13 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 14 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 15 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 16 E1         HDLCFCS     (In use)
 17 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 18 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 19 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 20 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 21 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 22 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 23 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 24 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 25 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 26 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 27 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 28 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 29 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 30 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
 31 E1         Clear       (In use)  (EC: OSLEC - INACTIVE)
### Span  2: XBUS-00/XPD-10 "Xorcom XPD [usb:X1045601].2: FXS"
 32 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
 33 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
 34 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
 35 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
 36 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
 37 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
 38 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
 39 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
### Span  6: XBUS-03/XPD-00 "Xorcom XPD [usb:X1045602].1: FXS"
110 FXS        FXOKS       (In use)  (EC: OSLEC - INACTIVE)
111 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
112 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
113 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
114 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
115 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
116 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
117 FXS        FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
118 Output     FXOKS       (In use)  (no pcm)  (EC: OSLEC - INACTIVE)
```

13. Xorcom Applications

Burglar Alarms

Broadcasting Burglar Alarm System Messages

Every member of the Xorcom line of products has an FXS module at the leftmost position that includes two auxiliary output ports and four auxiliary input ports. These features open up a whole world of exciting applications for the system. These notes will demonstrate how to broadcast burglar alarm system voice messages to designated phone numbers by using one of the Astribank input ports and modifying the Asterisk dialing plan.

An input port can be activated by connecting two wires in the input RJ-45 connector ("dry contact"). An input activation is translated as an "off hook" state of an extension. The default mapping of the input ports (when using the Xorcom Rapid™ auto-configuration) starts with the number of the 8th FXS port plus 3. For example, if the Astribank-8 extensions are 401 to 408, the input ports will be extensions 411, 412, 413 and 414 (extensions 409 and 410 are the output ports).

Following is a step-by-step explanation of how to wire and set up your Astribank to send voice messages (as a response to any external event) to designated phone numbers.

- Prepare a cable: you can use a simple CAT-5 network cable. Cut it on one end, and strip the housing off the 8 internal wires
- The following table shows the wiring diagram of the output RJ-45 connector. An input event is generated by connecting the input pin to the associated ground pin.

RJ45 PIN	Functionality
1	IN 1
2	Common (GND)
3	IN 3
4	Common (GND)
5	IN 2
6	Common (GND)

7	IN 4
8	Common (GND)

- To emulate the "off-hook" status for a specific input, you should connect the pair that is associated with the required input. The input pairs are RJ-45 pins 1-2, 3-4, 5-6 and 7-8
- Connect the wiring to an isolated switch, such as a relay with "dry contact"

The input ports are not fused and are not designed to accept any external voltage. Driving external voltage will damage the input ports, and may damage the entire Astribank unit and void your warranty!

- Update the CompletePBX dialing table to include the phone numbers that should be called when the input is activated, and associate the voice files that should be played.
- Edit the dial plan by creating an appropriate custom context.

Opening Doors

Every member of the Xorcom line of products has an FXS module at the leftmost position that includes two auxiliary output ports and four auxiliary input ports. These features open up a whole world of exciting applications for the system. These notes will demonstrate how to control access of pre-approved personnel to restricted areas by using the Astribank output ports, and modifying the Asterisk dialing plan.

By using internally isolated relay, each one of the two output ports can switch up to 220 volts, 2 amperes. A relay can be activated by dialing in to its extension. Following is a step-by-step explanation of how to wire and set up your Astribank to control doors, or any other equipment of your choice.

Call in to the relay and listen to it: if your system is configured to support extensions 3001 to 3008, call extension 3009 with your ear close to the Astribank. You'll hear a "click" from the Astribank. Hang up your phone; you will soon hear another "click". The first "click" is the sound that the relay makes when it is activated. This works exactly like a light switch, or pressing a push-button to activate a doorbell. Dialing to the second relay (3010, in our example) will give the same results (with the second relay).

- Prepare a cable: you can use a simple CAT-5 network cable. Cut it on one end, and strip off the housing to expose the 8 internal wires

RJ45 PIN	Functionality
1	IN 1
2	Common (GND)
3	IN 3
4	Common (GND)
5	IN 2
6	Common (GND)
7	IN 4
8	Common (GND)

- Connect the wiring to activate the door lock (or any other appliance or equipment)

The output relays are not fused. Driving more than 2 amperes may damage the relay and void your warranty!

If you are switching voltages that are more than 24 volts, use licensed electrician services to wire the system.

Make sure that you use the Ground Tab of the Astribank unit to ground the Astribank box.

- Test the installation: call to the relay (3009 or 3010 in our example) and check that the door or the appliance is activated.
- Update the dialing table to include all the active phone numbers in the list, by editing the dialing plan.

Tips and Tricks

- To activate the relay with a Caller ID that comes from the PSTN (external line) use a specific incoming line. As per its default settings, Asterisk waits for the second ring before the operator's phone starts to ring. The Caller ID is transferred to the Asterisk from the PSTN between the first and the second ring. You can program the dialing plan so that the call will not be forwarded to the operator or any other extension (for a specific number of rings, or forever), so that the caller will not be charged for the call.
- You can program the dialing plan to stop ringing after the second ring. Keep in mind that the relay will be activated as long the extension associated with it rings.
- You can allow internal extensions to activate the relay, or to block them from doing so, so that the receptionist, for example, will be able to open the door from her extension, while other extensions will not be able to perform that action.

VoIP Public Address System

You can use Rapid PA™ to create a Public Address System Based on Xorcom XPP™ Technology

Overview

Rapid PA is an add-on for Xorcom IP-PBX and Astribank channel banks that interfaces with any Xorcom FXS port to provide public address functionality. The small stand-alone unit is activated by simply dialing the port's extension number.

Each Rapid PA unit is equipped with 2 RJ11 ports. The 'PBX' port connects directly to a Xorcom FXS port and the 'PA' connection connects to the PA 'line in' ('audio in') port. The PA device itself can be anything from a standard personal computer speaker with an internal amplifier to an industrial-strength amplifying system.

How it Works

Rapid PA does not need a power supply – it uses the FXS feed for its operation. A LED (Light Emitting Diode) indicates "line active" status, simplifying installation and testing. When a call is placed to the FXS port extension to which the Rapid PA is connected, the Rapid PA immediately "answers the call" (i.e., goes to "off hook" position) and the caller can place his/her call through the IP system.

The origin of the PA message is not important; it can be an analog phone, an IP phone, a call from an incoming line or even from a soft phone overseas. The PA system is automatically disconnected when the call terminates.

The small size and simple installation of the Rapid PA unit makes it easy to install multiple local PA amplifiers in different locations. Even a low cost PX loudspeaker (with built-in amplifier) can be used as a small PA system.

Multiple Rapid PA devices can be connected to multiple FXS ports and loudspeakers to provide multi-zone support.

Implementing Rapid PA

Each FXS line connected to the Rapid PA must be defined as Kewl Start, as per Xorcom's default setting. If for any reason the setup is different, see the "Kewl Start Setup Procedure" below for proper settings. This is important in order to enable automatic disconnection from the PA system when the call terminates.

Rapid PA should be located close to the PA amplifiers

Wiring Table

RJ11 Connector/Pin	Description	Notes
PBX 1	Not connected	
PBX 2	FXS port TIP or RING	Crossing Pin2 and 3 is OK
PBX 3	FXS port TIP or RING	Crossing Pin2 and 3 is OK
PBX 4	Not connected	
PA 1	Not connected	
PA 2	PA Audio In	Crossing Pin2 and 3 is OK
PA 3	PA Audio In	Crossing Pin2 and 3 is OK
PA 4	Not connected	

Kewl Start Setup Procedure

In the */etc/DAHDi/system.conf* file the channel must be defined as "fxoks". For example:

```
fxoks=1
```

In the */etc/asterisk/chan_DAHDi_additional.conf* file the channel must be defined as fxo_ks. For example:

```
signalling=fxo_ks
```


14. Appendix

Feature Codes

Code	Description
Blacklist	
*30	Add a number to blacklist
*31	Remove a number from blacklist
*32	Blacklist the last caller
Business Services	
*34	Wakeup Call
*35	Remote Wakeup Call
*37	Speak Last Number
*38	Remind Me
Call Completion (CCSS)	
*40	Set Call Completion
*41	Cancel Call Completion
Call Center	
*50	Add Queue Agent toggle
*51	Pause Queue Agent toggle
*52	Queue Login/logout toggle
*53	Pause Queue toggle
*54	Barge into Call
*55	Spy on an extension
*56	Spy on an extension in whisper mode
Call Forward	
*36	Boss/Secretary toggle
*58	Call Forward Immediately toggle
*59	Set number for Call Forward Immediately

*60	Call Forward Unavailable toggle
*61	Set number For Call Forward Unavailable
*62	Call Forward Busy toggle
*63	Set number For Call Forward Busy
*64	Call Forward on No Answer toggle
*65	Set number For Call Forward on No Answer
*66	Do Not Disturb toggle
*67	Follow Me toggle
*69	Clear all Diversions
*96	Personal Assistant toggle
On Call Features	
*0	Disconnect Call
*07	Direct Pickup
*08	Pickup Group
*2	Attended Transfer
*3	One Touch Recording
*4	Park Call
#1	Blind transfer
Phonebook Directory	
411	Dial By Name
Test Services	
*70	Speak the date and time
*71	Speak number of current extension
*72	Perform Echo Test
*73	Simulate Incoming Call
Special Features	

*74	Limit extension (toggle) to a global Class of Service
*75	Phone Lock toggle
*76	Change features password for current Extension
*77	Remote Substitution
*78	Customer Code
*79	Authorization Code
*80	Hot Desking toggle
*81	Night Mode All toggle
Voicemail	
*91	Paging
*92	Recording
*93	Dictation
*94	Record Personnel Assistant message
*95	Send Voicemail message
*97	Direct Voicemail
*98	Remote Voicemail
Complete Concierge	
22	Room Status
23	Minibar

BLF (Hints)

List of BLF hints that are available in CompletePBX 5.

Name	Feature Code	Description
BOSS_<ext>	*36	Toggle **Boss/Secretary**, where <ext> should be replaced with the number of the extension
CFU_<ext>	*60	Toggle **Call Forward Unavailable**, where <ext> should be replaced with the number of the extension
CFI_<ext>	*58	Toggle **Call Forward Immediately**, where <ext> should be replaced with the number of the extension
CFB_<ext>	*62	Toggle **Call Forward Busy** where <ext> should be replaced with the number of the extension
CFN_<ext>	*64	Toggle **Call Forward on No Answer** where <ext> should be replaced with the number of the extension
CON_<conference>		Hint for conference
DND_<ext>	*66	Toggle **Do Not Disturb**, where <ext> should be replaced with the number of the extension
FWM_<ext>	*67	Toggle **Follow Me**, where <ext> should be replaced with the number of the extension
HD_<hot-desk user device>		Indicates status of a hot-desk device – “Idle” indicates that it is not logged into the system
LOK_<ext>	*75	Toggle **Lock Phone**, where <ext> should be replaced with the number of the extension
NM_<night-mode>	*81	Toggle **Night Mode**, where <night-mode> should be replaced with the number associated with the night mode
PEA_<ext>	*96	Toggle **Personal Assistant**, where <ext> should be replaced with the number of the extension
QAL_<ext>_<queue>	*52	Toggle **Queue Login/Logout**, where <ext> should be replaced with the number of the extension, and <queue> should be replaced with the number of the queue

QAP_<ext>_<queue>	*51	Toggle **Pause Queue Agent**, where <ext> should be replaced with the number of the extension, and <queue> should be replaced with the number of the queue
*98<shared mailbox>	*98	Enables multiple extensions to monitor (and access) a shared mailbox
<parking-slot>		Available parking slot, where the <parking-slot> placeholder should be replaced with the number of the parking slot

CDR table in Asterisk Database

The CDR record in the asterisk database contains a log of all calls made to and from the CompletePBX 5 system.

The following table describes the fields in the cdr table of the asterisk database.

Field	Data Type	Null	Key	Description
cdr_id	int(10) unsigned	No	PRI	Auto-incremented number
calldate	datetime	No	MUL	GMT timestamp indicating when the call was initiated, for example **2017-09-19 20:56:24**
clid	varchar(80)	No	MUL	Caller ID, based on the Internal CID field in the Extensions dialog for internal calls, the External CID field for outbound calls, or the CID field provided for inbound calls. Could contain something like **"Main Switchboard" <2940>** for calls originating from the PBX, or **<0544646377>** for calls originating from an external source.
source	varchar(80)	No		Similar to the **src** field, but is left empty when the destination of the call cannot be determined. For example, if extension 2000 is configured with external CID 7141234, the system will use 7141234 for dialing. The **source** field will contain 2000 and the **src** field will contain 7141234.
src	varchar(80)	No	MUL	The caller ID of the calling party, as used by the system when making the call. For example, if extension 2000 is configured with external CID 7141234, the system will use 7141234 for dialing. The **source** field will contain 2000 and the **src** field will contain 7141234.

dst	varchar(80)	No	MUL	The destination of the call, as dialed by the system. For example, if an inbound call was accepted for DID 7141234 and was routed by CompletePBX 5 to extension 2000, then **dst** will contain 7141234 and **destination** will contain 2000.
destination	varchar(80)	No		Similar to the **dst** field, but is left empty when the destination of the call cannot be determined. For example, if an inbound call was accepted for DID 7141234 and was routed by CompletePBX 5 to extension 2000, then **dst** will contain 7141234 and **destination** will contain 2000.
dcontext	varchar(80	No		The destination context for the call, for example **cos-all**, **cos-restricted**, **ext-ringgroups.**
channel	varchar(80)	No		The channel for the calling party, for example **DAHDI/i1/0523315342-1**, **SIP/699-00000001**
dstchannel	varchar(80)	No		The channel for the party that is called, for example **DAHDI/i1/0524519648-38**
lastapp	varchar(80)	No		The last dialplan application that was executed, for example **Dial**, **Voicemail**, **Hangup, etc.**
lastdata	varchar(80)	No		The arguments, if any, sent to lastapp.
duration	int(11)	No	MUL	Duration of the call, based on the number of seconds between when the call was initiated, and when it ended.

billsec	int(11)	No	MUL	Duration of the call, based on the number of seconds between when the call was answered, and when it ended.
disposition	varchar(45)	No	MUL	Indicates what happened to the call. Valid disposition values are NO ANSWER, FAILED, BUSY, ANSWERED, CONGESTED, or UNKNOWN
amaflags	int(11)	No		The Automatic Message Accounting (AMA) flag associated with this call. Valid values are OMIT, BILLING, DOCUMENTATION, or Unknown.
accountcode	varchar(20)	No	MUL	The account code, if defined in the Account Code field for the extension or for the outbound route, associated with the outgoing call.
auth_code	varchar(255)	Yes		The code used for calls where the Authorization Code feature code has been used for an outbound call. By default, this is activated by feature code *79
customer_code	varchar(255)	Yes		The code used for calls where the Customer Code feature code has been used for an outbound call. By default, this is activated by feature code *78
pin_code	varchar(255)	Yes		The ***description*** of the PIN code that was used for an outbound call, when an Outbound Route requires a PIN code
userfield	varchar(255)	No		A general-purpose user field. This field is empty by default and can be set to a user-defined string

uniqueid	varchar(32)	No	MUL	A unique identifier for the channel
linkedid	varchar(32)	No		A unique identifier that unites multiple CDR records
sequence	varchar(32)	No		A numeric value that combined with uniqueid and linkedid, can be used to uniquely identify a single CDR record
peeraccount	varchar(32)	No		The account code of the called party
calltype	enum (‘1’, ‘2’, ‘3’, ‘4’)	No		1 - indicates an internal call, i.e. call between two extensions. 2 - indicates an incoming call from an external source. 3 - indicates an outbound call to an external number. 4 - indicates a transit call, i.e. trunk-to-trunk.
recfile	varchar(255)	No		Call-recording file name
recfile_cloud	varchar(255)	Yes		URL for the file (if any) that is saved in the cloud-based storage.

Asterisk Dial Options

Refer to the Asterisk online documentation for an up-to-date list of all available dial options.

- A (**x**) - Play an announcement to the called party, where *x* is the prompt (file)to be played
- a - Immediately answer the calling channel when the called channel answers in all cases. Normally, the calling channel is answered when the called channel answers, but when options such as A() and M() are used, the calling channel is not answered until all actions on the called channel (such as playing an announcement) are completed. This option can be used to answer the calling channel before doing anything on the called channel. You will rarely need to use this option; the default behavior is adequate in most cases.
- b (context^exten^**priority**) - Before initiating an outgoing call, Gosub to the specified location using the newly created channel. The Gosub will be executed for each destination channel.
- B (context^exten^**priority**) - Before initiating the outgoing call(s), Gosub to the specified location using the current channel.
- C - Reset the call detail record (CDR) for this call.
- c - If the Dial() application cancels this call, always set HANGUPCAUSE to 'answered elsewhere'
- d - Allow the calling user to call a 1-digit extension while waiting for a call to be answered. Exit to that extension if it exists in the current context, or the context defined in the EXITCONTEXT variable, if it exists.
- D (called:calling:progress) - Send the specified DTMF strings after the called party has answered, but before the call gets bridged. The called DTMF string is sent to the called party, and the calling DTMF string is sent to the calling party. Both arguments can be used alone. If progress is specified, its DTMF is sent to the called party immediately after receiving a PROGRESS message. See SendDTMF for valid digits.
- e - Execute the h extension for peer after the call ends
- f (x) - If *x* is not provided, force the CallerID sent on a call-forward or deflection to the dial plan extension of this Dial() using a dial plan hint. For example, some PSTNs do not allow CallerID to be set to anything other than the numbers assigned to you. If *x* is provided, force the CallerID sent to *x*.
- F (context^exten^**priority**) - When the caller hangs up, transfer the **called** party to the specified destination and **start** execution at that location.
- F - When the caller hangs up, transfer the **called** party to the next priority of the current extension and **start** execution at that location.
- g - Proceed with dial plan execution at the next priority in the current extension if the destination channel hangs up.
- G (context^exten^**priority**) - If the call is answered, transfer the calling party to the specified *priority* and the called party to the specified *priority* plus one.
- h - Allow the called party to hang up by sending the DTMF sequence defined for disconnect in features.conf.
- H - Allow the calling party to hang up by sending the DTMF sequence defined for disconnect in features.conf.
- i - Asterisk will ignore any forwarding requests it may receive on this call attempt.

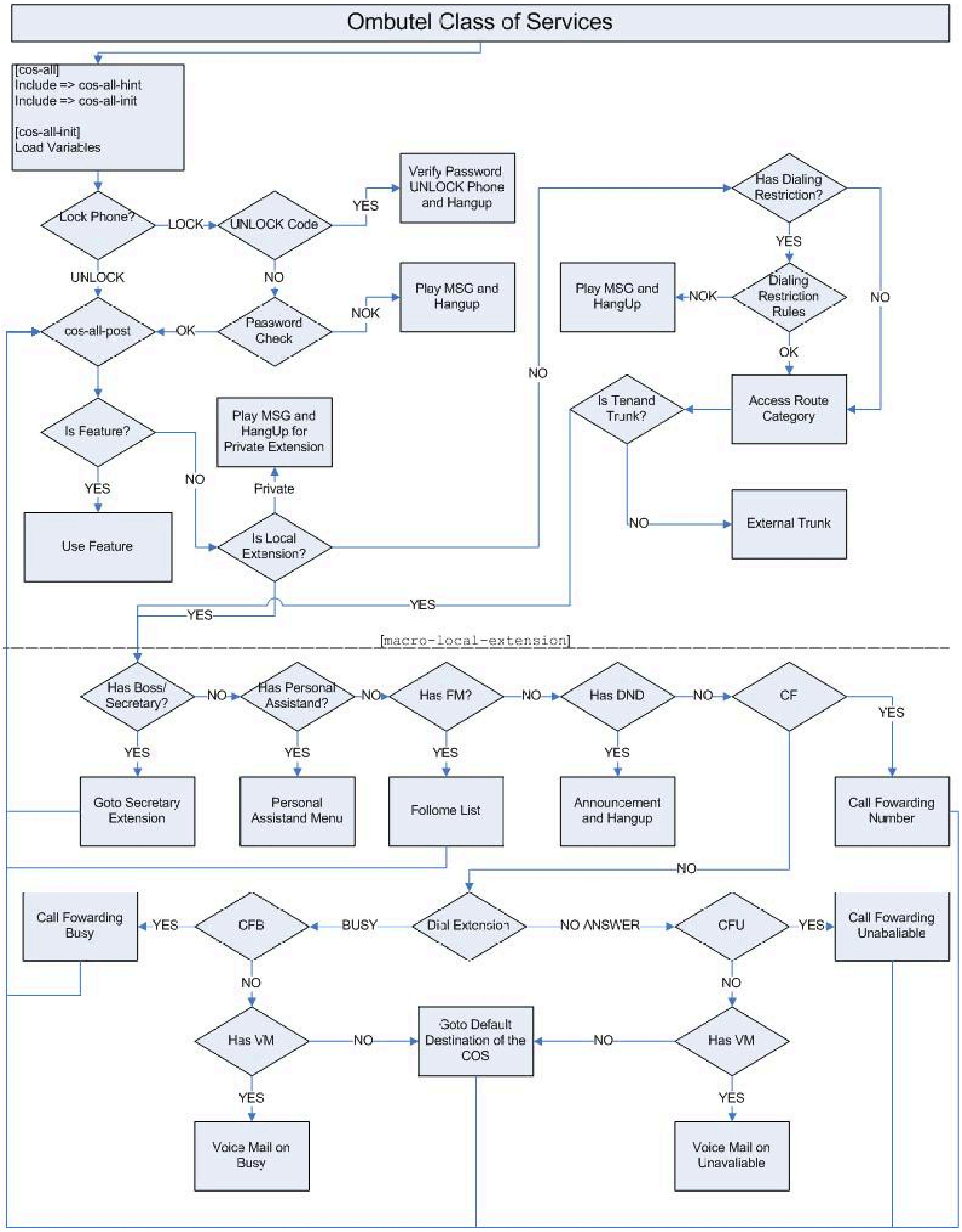
- I - Asterisk will ignore any connected line update requests or any redirecting party update requests it may receive on this call attempt.
- k - Allow the called party to enable parking of the call by sending the DTMF sequence defined for call parking in features.conf.
- K - Allow the calling party to enable parking of the call by sending the DTMF sequence defined for call parking in features.conf.
- L (**x**:y:z) - Limit the call to *x* milliseconds. Play a warning when *y* milliseconds are left. Repeat the warning every *z* milliseconds until time expires. This option is affected by the following variables:
  - LIMIT_PLAYAUDIO_CALLER - If set, this variable causes Asterisk to play the prompts to the caller. Default is YES.
  - LIMIT_PLAYAUDIO_CALLEE - If set, this variable causes Asterisk to play the prompts to the callee. Default is NO.
  - LIMIT_TIMEOUT_FILE - If specified, *filename* specifies the sound prompt to play when the timeout is reached. If not set, the time remaining will be announced.
  - LIMIT_CONNECT_FILE - If specified, *filename* specifies the sound prompt to play when the call begins. If not set, the time remaining will be announced.
  - LIMIT_WARNING_FILE - If specified, *filename* specifies the sound prompt to play as a warning when time *x* is reached. If not set, the time remaining will be announced.
  - **x** - Maximum call time, in milliseconds
  - y - Warning time, in milliseconds
  - z - Repeat time, in milliseconds
- m (class) - Provide hold music to the calling party until a requested channel answers. A specific music on hold *class* (as defined in musiconhold.conf) can be specified.
- M (**macro**^arg) - Execute the specified *macro* for the **called** channel before connecting to the calling channel. Arguments can be specified to the Macro using ^ as a delimiter. The macro can set the variable MACRO_RESULT to specify the following actions after the macro is finished executing:
  - MACRO_RESULT - If set, this action will be taken after the macro finished executing.
    - ABORT - Hangup both legs of the call
    - CONGESTION - Behave as if line congestion was encountered
    - BUSY - Behave as if a busy signal was encountered
    - CONTINUE - Hangup the called party and allow the calling party to continue dial plan execution at the next priority
    - GOTO:[[<CONTEXT>^]<EXTEN>^]<PRIORITY> - Transfer the call to the specified destination.
  - **macro** - Name of the macro that should be executed.
  - arg[^arg...] - Macro arguments

- n (delete) - This option is a modifier for the call screening/privacy mode. (See the p and P options.) It specifies that no introductions are to be saved in the priv-callerintros directory.
  - delete - With *delete* either not specified or set to 0, the recorded introduction will not be deleted if the caller hangs up while the remote party has not yet answered. With *delete* set to 1, the introduction will always be deleted.
- N - This option is a modifier for the call screening/privacy mode. It specifies that if CallerID is present, do not screen the call.
- o (x) - If *x* is not provided, specify that the CallerID that was present on the **calling** channel be stored as the CallerID on the **called** channel. This was the behavior of Asterisk 1.0 and earlier. If *x* is provided, specify the CallerID stored on the **called** channel. Note that o(${CALLERID(all)}) is similar to option o without the parameter.
  - O (mode) - Enables **operator services** mode. This option only works when bridging a DAHDI channel to another DAHDI channel only. if specified on non-DAHDI interfaces, it will be ignored. When the destination answers (presumably an operator services station), the originator no longer has control of their line. They may hang up, but the switch will not release their line until the destination party (the operator) hangs up. - With *mode* either not specified or set to 1, the originator hanging up will cause the phone to ring back immediately. With *mode* set to 2, when the operator flashes the trunk, it will ring their phone back.
- p - This option enables screening mode. This is basically Privacy mode without memory.
- P (x) - Enable privacy mode. Use *x* as the family/key in the AstDB database if it is provided. The current extension is used if a database family/key is not specified.
- Q (**cause**) - Specify the Q.850/Q.931 *cause* to send on unanswered channels when another channel answers the call. As with Hangup(), *cause* can be a numeric cause code or a name such as NO_ANSWER, USER_BUSY, CALL_REJECTED or ANSWERED_ELSEWHERE (the default if Q isn't specified). You can also specify 0 or NONE to send no cause. See the causes.h file for the full list of valid causes and names.
- r - This option enables a ring-back tone for a queue and music-on-hold for a call being put on hold by that queue.
- R (tone) - Default: Indicate ringing to the calling party, even if the called party isn't actually ringing. Send audio 'tone' from the indications.conf tonezone currently in use. Pass no audio to the calling party until the called channel has answered.
- R - Default: Indicate ringing to the calling party, even if the called party isn't actually ringing. Allow interruption of the ringback if early media is received on the channel.
- S (**x**) - Hang up the call *x* seconds **after** the called party has answered the call.
- s (**x**) - Force the outgoing CallerID tag parameter to be set to the string *x*.
  Works with the f option.
- t - Allow the called party to transfer the calling party by sending the DTMF sequence defined in features.conf. This setting does not perform policy enforcement on transfers initiated by other methods.
- T - Allow the calling party to transfer the called party by sending the DTMF sequence defined in features.conf. This setting does not perform policy enforcement on transfers initiated by other methods.
- U (**x**^arg) - Execute via Gosub the routine *x* for the **called** channel before connecting to the calling channel. Arguments can be specified to the Gosub using ^ as a delimiter. The Gosub

routine can set the variable GOSUB_RESULT to specify the following actions after the Gosub returns.

  - GOSUB_RESULT
    - ABORT - Hangup both legs of the call.
    - CONGESTION - Behave as if line congestion was encountered.
    - BUSY - Behave as if a busy signal was encountered.
    - CONTINUE - Hangup the called party and allow the calling party to continue dial plan execution at the next priority.
    - GOTO:[[<CONTEXT>^]<EXTEN>^]<PRIORITY> - Transfer the call to the specified destination.
  - **x** - Name of the subroutine to execute via Gosub
  - arg[^arg...] - Arguments for the Gosub routine
  - u (**x**) - Works with the f option, where **x f**orces the outgoing callerid presentation indicator parameter to be set to one of the values passed in *x*:
    - allowed_not_screened
    - allowed_passed_screen
    - allowed_failed_screen
    - allowed
    - prohib_not_screened
    - prohib_passed_screen
    - prohib_failed_screen
    - prohib unavailable
- w - Allow the called party to enable recording of the call by sending the DTMF sequence defined for one-touch recording in features.conf.
- W - Allow the calling party to enable recording of the call by sending the DTMF sequence defined for one-touch recording in features.conf.
- x - Allow the called party to enable recording of the call by sending the DTMF sequence defined for one-touch automixmonitor in features.conf.
- X - Allow the calling party to enable recording of the call by sending the DTMF sequence defined for one-touch automixmonitor in features.conf.
- z - On a call forward, cancel any timeout which has been set for this call.

Call Flow


Ombutel Class of Services
[cos-all]
Include => cos-all-hint
Include => cos-all-init
[cos-all-init]
Load Variables
Lock Phone?
LOCK
UNLOCK Code
YES
Verify Password, UNLOCK Phone and Hangup
UNLOCK
NO
cos-all-post
OK
Password Check
NOK
Play MSG and Hangup
Has Dialing Restriction?
YES
Dialing Restriction Rules
NOK
Play MSG and HangUp
NO
OK
Access Route Category
Is Tenand Trunk?
NO
External Trunk
Is Feature?
YES
Use Feature
NO
Play MSG and HangUp for Private Extension
Private
Is Local Extension?
YES
[macro-local-extension]
Has Boss/ Secretary?
Has Personal Assistand?
Has FM?
Has DND
CF
Goto Secretary Extension
Personal Assistand Menu
Followe List
Announcement and Hangup
Call Fowarding Number
Call Fowarding Busy
CFB
BUSY
Dial Extension
NO ANSWER
CFU
Call Fowarding Unabaliable
Has VM
Goto Default Destination of the COS
Voice Mail on Busy
Voice Mail on Unavaliable