



CompletePBX v4.6

Reference Guide

(rev. 4.6.2)

Contents

1. OVERVIEW	9
WIKI	9
DESIGNING COMPLETEPBX	9
Security	9
Extensions (or Devices and Users)	9
Numbering System	9
Flow Chart	9
Trunks	9
Outbound Routes	10
Routing Groups	10
Inbound Routes	10
Follow Me	10
Ring Groups	11
Faxing	11
Parking Lot	11
Paging and Intercom	11
Conferences	12
IVR	12
Queues	12
Feature Codes	13
Voicemail Settings	13
System Recordings and Announcements	13
Direct Inward System Access (DISA)	13
Backup and Restore	14
Endpoint Manager	14
DEPENDENCIES	14
Destinations	14
Mandatory Fields and Dependencies between Dialogs	15
ACCESSING COMPLETEPBX	18
Login to the User Interface	18
CompletePBX Launch Pad	18
MODULE MAINTENANCE	20
UPDATING FROM THE ONLINE REPOSITORY	21
2. DEVICES AND EXTENSIONS	22
WHAT ARE THEY?	22
OPERATIONAL MODES FOR EXTENSIONS	22
ENDPOINT TYPES	24
SIP Endpoints	24
IAX2 Endpoints	25
DAHDI Endpoints	25
Custom Endpoints	25
Virtual Endpoints	25
ENDPOINT FIELDS	25
Common Extension/User Fields	25
Common Endpoint Fields	29
Common SIP/IAX2 Fields	30
Additional SIP Fields	30
Additional IAX2 Fields	34
Common DAHDI Fields	35
Additional DAHDI Fields	35
Common Custom Fields	37

CONFIGURING EXTENSIONS IN EXTENSIONS MODE.....	37
<i>Configuring Extensions Mode</i>	37
<i>Configuring Extensions</i>	37
CONFIGURING EXTENSIONS IN DEVICEANDUSER MODE.....	39
<i>Configuring DeviceAndUser Mode</i>	39
<i>Configuring Users</i>	40
<i>Configuring Devices</i>	42
FAXING.....	43
VOICEMAIL SETUP.....	44
<i>Voicemail Delivery Options</i>	44
<i>Managing Voicemail Messages</i>	46
ENDPOINT MANAGER.....	47
<i>Overview</i>	48
<i>Option 66 on DHCP Server</i>	48
<i>Configuration Files</i>	49
<i>Multi-layer Definitions</i>	49
<i>Brands and Models</i>	50
<i>Host Settings</i>	50
<i>Create a Template</i>	52
<i>Device Mapping</i>	56
SUMMARY.....	58
3. TRUNKS.....	59
TRUNK TYPES.....	59
CONFIGURING A TRUNK.....	60
<i>Common Trunk Fields</i>	61
<i>DAHDI Trunks</i>	64
<i>SIP Trunks</i>	65
<i>IAX2 Trunks</i>	68
<i>ENUM Trunks</i>	70
<i>Custom Trunks</i>	71
COMMON TRUNK CONFIGURATION SETTINGS.....	71
SUMMARY.....	72
4. BASIC CALL TARGETS.....	73
TERMINATING CALLS.....	73
EXTENSIONS AND VOICEMAIL.....	74
RING GROUPS.....	75
CONFERENCES.....	79
SUMMARY.....	83
5. ADVANCED CALL TARGETS.....	84
QUEUE.....	84
<i>Queue Priorities</i>	84
<i>Queues</i>	86
<i>Add Queue</i>	86
<i>Queue Options</i>	88
<i>Caller Position Announcements</i>	92
<i>Periodic Announcements</i>	92
TIME-BASED RULES.....	94
TIME GROUPS.....	94
TIME CONDITIONS.....	96
IVR (DIGITAL RECEPTIONIST).....	98
PAGING & INTERCOM.....	100
PARKING.....	102
<i>Parking Lot Options</i>	104

<i>Returned Call Behavior</i>	104
<i>Alternate Destination</i>	104
SUMMARY	105
6. CALL ROUTING	106
INBOUND ROUTING	106
<i>Inbound Routing Priorities</i>	107
FOLLOW ME AND VMX LOCATER	111
<i>Default Follow Me</i>	111
<i>VmX Locater</i>	114
OUTBOUND ROUTES	116
ROUTING GROUPS	119
<i>Creating a Routing Group</i>	120
SUMMARY	121
7. RECORDING AND LISTENING TO CALLS	122
RECORDING FORMATS	122
<i>Transcoding During Recording</i>	123
GENERAL CALL RECORDING OPTIONS	124
RECORDING CALLS	124
<i>Recording Calls for Extensions</i>	124
<i>Recording Calls for Queues</i>	125
<i>Recording Calls for Conferences</i>	126
MAINTAINING CALL RECORDINGS	127
G.729 IMPLEMENTATION GUIDELINES	127
<i>Conversion Times Based on Compression Method</i>	127
<i>Methods for Obtaining the G.729 Codec</i>	127
<i>Installing the Open Source G.729 Codec</i>	127
<i>Estimating Number of G.729 Channels Required</i>	128
<i>Typical Translation Time between Formats: XR3000</i>	128
<i>Typical Translation Time between Formats: XR2000</i>	128
LISTENING TO VOICE RECORDINGS	129
<i>Prerequisites</i>	129
<i>Accessing Voice Recordings</i>	129
SUMMARY	130
8. PERSONALIZING YOUR PBX	132
MUSIC ON HOLD	132
<i>Customization</i>	132
<i>Using Audio Files</i>	132
<i>Using Audio Streams</i>	134
VOICE PROMPTS	136
<i>Recording Voice Prompts</i>	136
<i>Merging Existing Voice Prompts</i>	137
FEATURE CODES	139
CALLBACK	141
DIRECT INWARD SYSTEM ACCESS (DISA)	143
PIN SETS	145
MISC APPLICATIONS	147
MISC DESTINATIONS	148
FAXING	149
<i>Inbound Fax</i>	149
<i>Outbound Fax</i>	151
<i>Presentation Options</i>	151
<i>Fax Feature Code Option</i>	151
<i>Fax Transport Options</i>	151

<i>Fax Module Options</i>	152
<i>Cover Page</i>	152
SUMMARY	153
9. MY EXTENSION	155
ACCESS.....	155
CALL MONITOR.....	155
<i>Actions</i>	155
<i>Fields Displayed</i>	156
VOICEMAIL.....	156
<i>Actions</i>	156
<i>Fields Displayed</i>	157
FEATURE CODES.....	157
PHONE FEATURES.....	158
FAXES	159
<i>Send Fax</i>	159
<i>Stored Faxes</i>	160
SETTINGS.....	160
LOGOUT	162
10. MANAGING CALL FLOW	163
CONFIGURING MY SWITCHBOARD	163
<i>Templates</i>	164
<i>Users</i>	166
<i>Buttons</i>	168
<i>Groups</i>	168
USING MY SWITCHBOARD.....	169
<i>Queue Events</i>	169
<i>Login</i>	169
<i>Passing Credentials via URL</i>	170
<i>Main Panel View</i>	170
<i>Anatomy of the Toolbar</i>	171
<i>Action bar</i>	171
<i>Filter Box</i>	172
<i>Dial Box</i>	173
<i>Presence Select Box</i>	173
<i>Extensions</i>	174
<i>Performing Actions</i>	175
<i>Action Submenu</i>	176
<i>Visual Phonebook</i>	176
<i>Importing Data</i>	177
<i>Queues</i>	177
<i>Pickup Queued Calls</i>	178
<i>Trunks</i>	178
<i>Conferences</i>	178
CALL CENTER STATS	178
<i>Introduction</i>	178
<i>Reports</i>	179
<i>Administration and Configuration of Users</i>	179
<i>Editing Users</i>	180
<i>Access</i>	181
<i>Settings and Preferences</i>	182
<i>Configuration Variables</i>	182
<i>Selecting Reports</i>	184
<i>Filtering Queues and Agents</i>	184
<i>Filter by Date Range Hours</i>	184

<i>Results</i>	185
<i>Calls Answered</i>	186
<i>Calls Answered Overview</i>	186
<i>Service Level</i>	187
<i>Disconnection Cause</i>	188
<i>Answered Calls Detailed Report</i>	188
<i>Transfers</i>	189
<i>Unanswered calls</i>	189
<i>Disconnection Cause</i>	189
<i>Unanswered Calls by Queue</i>	190
<i>Unanswered Call Details</i>	190
11. SYSTEM PROTECTION	192
INTRODUCTION	192
SYSTEM PROTECTION.....	192
UNINTERRUPTIBLE POWER SUPPLIES	192
REDUNDANT COMPONENTS.....	192
SURGE PROTECTION.....	192
BACKUPS	193
<i>Configuring Backup</i>	193
<i>Backup Templates</i>	195
<i>Storage Servers</i>	197
<i>Maintaining and Protecting Backups</i>	197
<i>Maintaining Backups</i>	198
<i>Protecting Backups</i>	198
<i>Restore</i>	198
RAPID RECOVERY.....	202
<i>Instructions</i>	202
<i>Main Menu</i>	202
<i>Restore</i>	203
SUMMARY	203
12. SECURITY AND ACCESS CONTROL	204
COMPLETE SBC	204
<i>CompleteSBC Configuration Tasks</i>	204
<i>Enabling the CompleteSBC Web Interface</i>	205
<i>Configuring IP Addresses for Signaling and Media Interfaces</i>	205
<i>Enable Communications with CompleteSBC</i>	206
<i>NAT Router Configuration</i>	207
<i>CompletePBX Firewall Configuration</i>	208
<i>CompletePBX Configuration</i>	208
<i>Remote SIP Server Configuration</i>	209
<i>Licensing</i>	211
<i>Instructions for Disabling CompleteSBC</i>	211
SIP/IAX2 EXTENSIONS.....	213
GENERAL SIP SETTINGS	214
<i>Codecs (Transcoding)</i>	214
<i>Advanced General Settings</i>	215
DIALPLAN CONFIGURATION	216
REMOTE ACCESS AND LOCK DOWN	216
<i>VPN or SSH Tunnels</i>	216
<i>SSH Tunneling on Linux</i>	216
<i>SSH Tunneling on Windows</i>	217
ADMINISTRATOR ACCOUNTS.....	220
<i>Administrator Accounts and Permissions</i>	220
PORT USAGE	226

SUMMARY	227
13. MANAGING THE SYSTEM	228
SYSTEM SETTINGS.....	228
<i>About</i>	228
<i>DHCP</i>	228
<i>Email Settings</i>	230
<i>Firewall</i>	233
<i>Firewall Applications</i>	233
<i>Firewall Rules</i>	234
<i>Configuring Firewall with CompleteSBC Disabled</i>	236
<i>Intrusion Prevention</i>	238
<i>Network Settings</i>	239
<i>Notification Settings</i>	243
<i>Power Options</i>	244
<i>Storage Information</i>	244
<i>Time Settings</i>	245
14. SUPPORT	247
XORCOM HARDWARE LICENSES.....	247
APPLYING A NEW XORCOM LICENCE	248
MANAGING ECHO	249
<i>Introduction to Managing Echo in Telephony Systems</i>	249
<i>Reducing Echo</i>	249
<i>Eliminating Echo</i>	249
MANAGING DAHDI CHANNELS	250
<i>Xpp_blink Utility</i>	250
<i>Adding an Astribank</i>	250
15. APPLICATIONS	251
BURGLAR ALARMS.....	251
OPENING DOORS	252
<i>Tips and Tricks</i>	254
VOIP PUBLIC ADDRESS SYSTEM.....	254
<i>Overview</i>	254
<i>How it Works</i>	255
<i>Implementing Rapid PA</i>	255
<i>Wiring Table</i>	255
<i>Kewl Start Setup Procedure</i>	256
EXTERNALLY CONTROLLING FOLLOW ME	256
16. TWINSTAR	258
AN EXAMPLE OF AN ASTERISK HIGH AVAILABILITY CLUSTER	258
TWINSTAR IMPLEMENTATION DETAILS	261
EVENTS THAT ARE MONITORED	263
CONTROLLING THE TWINSTAR STATUS.....	263
<i>Check Status:</i>	264
<i>Enforce Switching to Another USB Interface:</i>	264
<i>Start USB Voltage Monitoring and Exchange of Watchdog Messages:</i>	264
<i>Stop USB Voltage Monitoring and Exchange of Watchdog Messages:</i>	264
TWINSTAR INSTALLATION.....	264
17. FEATURE CODES.....	265
BLACKLIST	265
CALL FORWARDING.....	265
CALL WAITING.....	266
CORE	267

DICTATION	268
DO-NOT-DISTURB (DND)	269
FOLLOW ME.....	269
INFO SERVICES	269
PAGING AND INTERCOM	270
PHONEBOOK DIRECTORY.....	270
RECORDINGS	271
SPEED DIAL	271
VOICEMAIL.....	271
18. MENU OVERVIEW	273
19. APPENDIX	283
VOICEMAIL.CONF OPTIONS	283

1. Overview

Wiki

Additional useful information can be obtained via the Internet by visiting the CompletePBX section of the [Xorcom wiki](#).

Designing CompletePBX

Security

Just like any other computer on your network that is connected to the Internet, CompletePBX can be targeted by hackers for the purpose of making cheap telephone calls. During the entire process of setting up CompletePBX, you should be constantly aware of the potential security implications of each step and make sure that your system is well protected. CompleteSBC, a session border controller, is integrated into CompletePBX. Refer to [Security and Access Control](#) in Chapter 12 for more detailed notes and considerations regarding security of CompletePBX. You can also use this link to download the [CompleteSBC Handbook](#)

Extensions (or Devices and Users)

Connectivity → Extensions

Extensions are where you configure devices (telephones) and users (extensions) on your system. Review [Devices and Extensions](#) in Chapter 2 to get a better understanding of the differences between Extensions and DeviceAndUser modes, and how to choose the correct mode for your system.

More detailed information can be found in Chapter 2, [Devices and Extensions](#).

Numbering System

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. It will help you to navigate your system if you group similar functions together, for example, by using the following ranges:

- 2000 - 2999 for extensions
- 7000 - 7100 for ring groups
- 8000 - 8100 for queues
- 9000 - 9100 for conferences

Flow Chart

It will help you to plan and visualize your CompletePBX configuration if you create a flowchart of everything that you want to setup in the system.

Trunks

Connectivity → Trunks

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

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

Before you start to configure CompletePBX, it is important that you decide what kind of trunks you will be using – SIP, DAHDI, etc.

Most reputable VoIP providers will give instructions on how to configure a trunk with their service.

The Dialed Number Manipulation Rules lets you redirect calls to other numbers. For example, if someone dials **411**, CompletePBX can be configured to change that to **1-800-FREE-411**. Or you could configure **511** to call your grandmother.

More detailed information can be found in Chapter 3, [Trunks](#).

Outbound Routes

Connectivity → Outbound Routes

Outbound Routes enables you to tell CompletePBX which Trunks (phone lines) to use when people dial external telephone numbers. A simple installation will direct CompletePBX 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.

More detailed information can be found in the [Outbound Routes](#) section of Chapter 6.

Routing Groups

Connectivity → Routing Groups

The Routing Groups module enables you to restrict certain extensions from making outbound calls. Only extensions that are members of a Routing Group can access outbound routes that are linked to that Routing Group. If an extension belongs to a Routing Group which has does not have access to any outbound routes, then the extension will not be able to make any external calls.

Inbound Routes

Connectivity → Inbound Routes

The Inbound Routes module is where you define how CompletePBX 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.

More detailed information can be found in the [Call Routing](#) section of Chapter 6.

Follow Me

Connectivity → Follow Me

The Follow Me module allows you to create a more specialized method of routing calls that are sent to a specific extension. Using this module, you can cause a call to an extension to ring several other extensions, or even external phone numbers. You can also make calls to an extension terminate in the voicemail of another extension.

For example, using Follow Me, you could cause a call to extension 2009 to:

- Initially ring extensions 2009, 2010, and 2011
- If none of the above extensions answer the call, ring a cellular phone for 15 seconds
- If the cellular phone also does not answer the call, send the call to the voice mailbox for extension 2003

More detailed information can be found in the [Follow Me and the VmX Locator](#) section of Chapter 6.

Ring Groups

Applications → Ring Groups

Ring Groups allow you to create a single extension number (the Ring Group number) that will call more than one person. For example, you could define a Ring Group so that when any user dials extension 6001, extensions 2009, 2010, and 2011 ring for 15 seconds, after which the call will go to the voicemail for extension 2000.

More detailed information can be found in the [Ring Groups](#) section of Chapter 4.

Faxing

Settings → Fax Configuration

Connectivity → Inbound Routes

Connectivity → Extensions

CompletePBX provides the complete answer to your fax needs. You can create multiple inbound fax routes, as well as enable all users to create and send outbound faxes.

Enterprise-wide setup for outbound faxes can be done using the Fax Configuration dialog, which is found in the Settings menu. See the [Faxing](#) section in Chapter 8.

Any extension can be designated as a Fax Recipient by modifying the Fax section in the Extension dialog, and making the extension fax-enabled. See the [Outbound Fax](#) section in Chapter 2.

Any inbound route can be configured to receive incoming faxes after it has been configured to detect faxes. For more information, refer to [Call Routing](#) in Chapter 6.

Parking Lot

Settings → Parking Lot

A Parking Lot allows anyone who has received a call to park the call on an extension, allowing any other user to access the parked call. Typically, you receive the call, transfer it to extension 70, and then listen as the system tells you where you can pick up the call (usually extension 71). Anyone else on your CompletePBX can now dial 71 to pick-up the parked call.

More detailed information can be found in the [Parking](#) section of Chapter 5.

Paging and Intercom

Applications → Paging & Intercom

The Paging and Intercom feature allows you to use your phone system as an intercom system, provided that your endpoints (phone devices) support this functionality. The Paging and Intercom dialog allows you to define a number (just like an extension or Ring Group number) that will simultaneously page a group of devices. For example, in a small office, you might define a paging group that allows any user to dial 6999, allowing them to page the entire office. You can also use the

*80 feature code to page a single extension, by dialing *80 followed by the extension number.

More detailed information can be found in the [Paging & Intercom](#) section of Chapter 5.

Conferences

Applications → Conferences

The **Conferences** function allows you to create an extension number that people can dial into in order to participate in a conference call. For example, a number of users could dial extension 9000 and join a conference call. A conference can also be accessed by external users by setting a Conference as the destination of an inbound route or an IVR system.

More detailed information can be found in the [Conferences](#) section of Chapter 4.

IVR

Applications → IVR

IVR allows you configure an auto attendant to answer calls and redirect the call in response to input from the caller.

It is important that you carefully plan the call flow and branching options for IVRs, while considering the user experience. IVRs use customized Announcements, so you will need to make sure that they are clear and meaningful, and configured to optimize the caller experience. Factors that you should consider include:

- Handling the timeout when there is no input from the caller
- Controlling the action to take if caller provides invalid user input
- Allowing the caller to backtrack if s/he has made a mistake or gets lost
- Allowing the caller to return to the IVR if voicemail is encountered
- Whether or not to take advantage of time-based branching, by defining Time Groups, for normal office hours, that include start and end times, start and end days of the week, and much more
- Defining a Time Condition, and setting one destination if the time matches and a different destination if the time does not match

More detailed information can be found in the [IVR \(Digital Receptionist\)](#) section of Chapter 5.

Queues

Applications → Queues

A queue manages incoming calls that need to be answered in an organized manner. Queues allow you to create rules to help you effectively manage the flow of incoming calls.

Call queues are especially useful for scenarios in which the volume of callers is expected to exceed the number of people or agents that are available to answer calls. Scenarios such as a technical support line or a sales line are good examples.

There are many parameters that can be configured to customize queue-handling to meet your specific needs, including:

- Sensitive queues can be password-protected
- Users can be given feedback of their position in the queue and their estimated hold time
- Queues can have both static and dynamic agents
- Multiple ring strategy options are available
- Calls can be redirected to any destination if no agent is available to answer the call



Important Note

If you want the Switchboard to track the status of queues and to create statistics for call center reporting, make sure that both **Event When Called** and **Member Status Event** (in the **Events, Stats and Advanced** section of the Queue dialog) are set to **Yes** when defining a new queue.

More detailed information can be found in the [Queue](#) section of Chapter 5.

Feature Codes

Admin → Feature Codes

This dialog allows you to set the special codes that users can dial to access various features. You can also disable features if you don't want users to be able to access them.

More detailed information can be found in the [Customizing Feature Codes](#) section of Chapter 8. A detailed list of all feature codes can be found in [Chapter 17](#).

Voicemail Settings

Settings → Voicemail → Dialplan Behavior

This dialog has several important features you may want to consider changing:

Voicemail Recording Gain allows you to control the volume level of voicemail messages. If you find that the voicemail messages you receive are quiet compared to the system recordings, you might want to change this from the default of 0 to 5.

Use **Operator Extension** to specify the extension number or ring group number to which callers will be transferred when they dial 0 while leaving a voicemail. If you leave this blank, the caller will return to the Ring Group from which they came before reaching voicemail.

System Recordings and Announcements

Admin → System Recordings

Applications → Announcements

System Recordings allows you record system-wide messages. Before these recordings can be used for use on your auto-attendant (IVR), Queue, etc., they must be customized as an Announcement. A single System Recording can be used in multiple Announcements.

More detailed information can be found in the [Custom Voice Prompts](#) section of Chapter 8.

Direct Inward System Access (DISA)

Applications → DISA

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

More detailed information can be found in the [Direct Inward System Access \(DISA\)](#) section of Chapter 8.

Backup and Restore

Admin → Backup and Restore

Backup and Restore allows you to backup and restore the CompletePBX settings as well as recordings made by CompletePBX. After you have created a backup, you can find it by typing the following at the command prompt:

```
cd /var/spool/asterisk/backup
ls -l
```

More detailed information can be found in the [Backups](#) section of Chapter 9.

Endpoint Manager

Settings → Endpoint Manager

Endpoint Manager provides you with a central tool for managing and updating the configuration settings of IP phones. For more detailed information, refer to the [Endpoint Manager](#) section of Chapter 2.

Dependencies

Destinations

Almost all dialogs are linked to a destination of one kind or another. The following table shows which dialogs are available as destinations, which dialogs must be terminated with a destination, and which modules can *optionally* be terminated with a destination.

Dialog	Is a Destination	Must Have Destination	Can Have a Destination
Announcements	✓	✓	
Blacklist			
Call Flow Control	✓	✓	
Call Recording		✓	
Callback	✓	✓	
Conferences	✓		
Custom Destination	✓		
DAHDI Channel DIDs			
DISA	✓		
Directory			
Extensions	✓		✓
FAX Recipient (Extension)	✓	Defined in Extensions	

Dialog	Is a Destination	Must Have Destination	Can Have a Destination
Feature Code	✓		
Follow Me			✓
Inbound Routes		✓	
Endpoint Manager			
IVR	✓	✓	
Languages		✓	
Misc Applications		✓	
Misc Destinations	✓		
Music on Hold			
Outbound Routes		Trunk Only	
PIN Sets			
Paging & Intercom	✓	Extensions Only	
Queues	✓		✓
Ring Groups	✓	✓	
Routing Groups			
Set CallerID		✓	
Terminate Call (System)	✓		
Time Conditions	✓	✓	
Time Groups			
Trunks	✓		
Voicemail	✓	Defined in Extensions	
Voicemail Blasting	✓	Extensions Only	
Wake Up Calls		Extensions Only	

Mandatory Fields and Dependencies between Dialogs

This table shows the dependencies between dialogs to help you optimize the flow when setting up

CompletePBX, as well as highlighting which fields are mandatory. The **Need to Know** column highlights information that you may need to complete the definition of the object. Items that are shown in bold font in the **Need to Know** column are not optional.

Dialog	Other Dialogs Required	Mandatory Fields	Need to Know
Extensions	Other Destinations (Optional)	User Extension Display Name Secret (SIP, IAX2) Channel (DAHDI only)	Outbound CID Inbound DID Secret, for IAX2 & SIP FAX enabled? Email address for FAX Password for voicemail Email address for voicemail
Outbound Routes	Trunks (Mandatory) Time Groups (Optional) PIN Sets (Optional)	Route Name	Dial Patterns
Callback	Destinations (Mandatory) DISA (Optional) Extensions (Optional) Other Destinations (Optional)	Description	
Directory	Extensions (Mandatory) Announcements (Optional) which may require System Recordings	Directory Name	
Endpoint Manager	Extensions	Host Settings Templates	
Follow Me	Destinations (Mandatory) Extensions (Mandatory) Announcements (Optional) which may require System Recordings Music on Hold (Optional) Other Destinations (Optional)	Extension	Ring strategy

Dialog	Other Dialogs Required	Mandatory Fields	Need to Know
Queues	Extensions Announcements (Optional) which may require System Recordings Music on Hold) (Optional) IVR (Optional) which may require Announcements and System Recordings Destinations (Optional) which may require Extensions or Other Destinations	Queue Number Queue Name	Ring strategy
Misc Applications	Destinations (Optional)	Description	
Parking Lot	Destinations (Optional) Announcements (Optional) which may require System Recordings Music on Hold (Optional)		
Inbound Routes	Music on Hold (Optional) Destinations (Optional), which may require Extensions or Other Destinations	Description DID Number Destination	DID number FAX enabled?
IVR	Announcements (Optional) which may require System Recordings Destinations (Optional) which may require Extensions or Other Destinations	IVR Name Invalid Destination Timeout Destination	
Ring Groups	Announcements (Optional) which may require System Recordings Music on Hold (Optional) Destinations (Optional) which may require Extensions or Other Destinations	Ring Group Number Group Description Extension/s Destination	Ring strategy
Routing Groups	Outbound Routes	Name	

Dialog	Other Dialogs Required	Mandatory Fields	Need to Know
Call Flow Control	Announcements (Optional) which may require System Recordings Destinations (Optional)		

Accessing CompletePBX

Login to the User Interface

Using any browser-enabled computer on your network, open a Web browser and enter the IP address of your CompletePBX server. If you don't know the IP address of your CompletePBX, go to the Linux console/command prompt.



Security to access Linux console

You can login to the Linux console/command prompt using the username **root** and the root password. The initial root password is documented in the Getting Started Guide, which was packed with your CompletePBX hardware.

After you login, type **ifconfig** at the command line and determine the IP address of your machine:

```
-----
[root@erlang ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:22:4D:A3:56:D3
          inet addr:192.168.0.127  Bcast:192.168.15.255  Mask:255.255.240.0
          inet6 addr: fe80::222:4dff:fea3:56d3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:309860363 errors:0 dropped:0 overruns:0 frame:0
          TX packets:116996463 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3435831734 (3.1 GiB)  TX bytes:1546974731 (1.4 GiB)
          Interrupt:16 Memory:80120000-80140000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:19688038 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19688038 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4257520274 (3.9 GiB)  TX bytes:4257520274 (3.9 GiB)
```

CompletePBX Launch Pad

The Launch Pad (the main CompletePBX screen) offers you five options:

- **Administration** will allow you to configure and manage CompletePBX.



Security to access Administration

The default username is **superadmin** and the initial password is documented in the Getting Started Guide, which was packed with your CompletePBX hardware. The password for this user should reset during the installation.

- **CompleteSBC**, added in release v4.6, is a proprietary session border controller that is integrated into CompletePBX. Sessions Border Controllers are usually deployed in a similar manner to firewalls, with the goal of establishing a clear separation between two VoIP networks. Full documentation for the [Xorcom CompleteSBC](#) can be downloaded from the Xorcom website.
- **My Extension** allows users to manage the properties of their own extension. For example, they can listen to voicemail messages and change certain features of their extension, such as call forwarding. Users can only modify features of their own extension. Users cannot listen to recordings or modify the setup for any extension other than their own.



Security to access My Extension

Users can login using their extension number and their voicemail password. Users who do not have a valid voicemail password cannot login to My Extension.

- **My Switchboard** is a screen that allows designated users, such as service agents, call center managers, or an office manager, to view and manage calls, queues, and many other functions.

Security to access My Switchboard



In order to have access to My Switchboard, users must be suitably defined. Use the Administration dialog (accessed from the CompletePBX Launch Pad) to access the Switchboard menu and select the Users dialog. Only users that are defined as Switchboard Users can login to My Switchboard. Default security uses the extension number and voicemail password, although a different password can be defined in the Users dialog. Users who are not defined in the Users dialog cannot access My Switchboard.

- **Call Center Statistics** displays call center statistics, either on the user's screen, or in pdf format. The default username used to access this dialog is **admin**, and the default password is also **admin**.



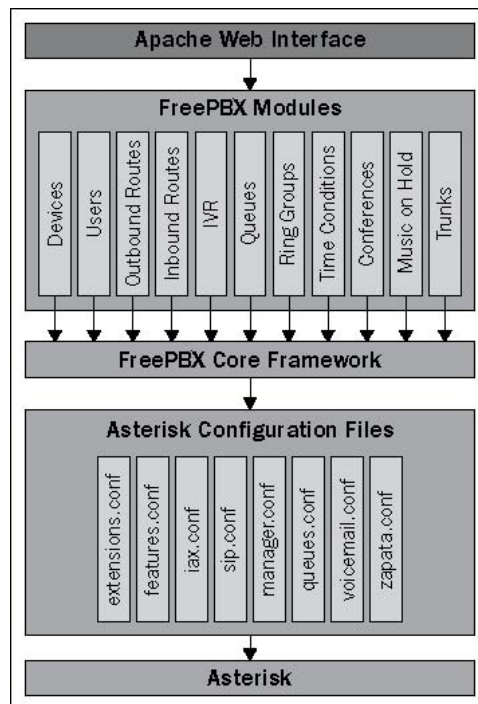
Module Maintenance

Admin → Module Admin

CompletePBX is a complete framework (or wrapper) which provides a simple graphic user interface, adding functionality, features, bug fixes, and stability to open-source PBX software, such as Asterisk. From inbound routing to voicemail, this architecture provides a pluggable module framework that allows expansion of CompletePBX, while maintaining supportability.

Xorcom has tested the integration of more than fifty modules, each providing a specific set of functions. When administering a CompletePBX system, Apache serves as a Web interface for each module. The modules store their configuration in a database, which the framework processes, and writes out to the CompletePBX configuration files. The configuration files are read by the system when you login.

This process is illustrated in the following figure:



CompletePBX is a collection of modules, including the base components provided by the Core Framework, in addition to the many other components that enhance the functionality of CompletePBX. This modularized structure enables us to add new features to the product easily, as well as simplify the process of applying updates.

Splitting functionality into modules also allows each installation of CompletePBX to be built specifically for its deployment requirements. If a PBX simply needs to store voicemail for users, all it will require is the inbound routing and voicemail modules. A PBX that answers calls and then routes them to another PBX may just require the inbound routing and outbound routing modules. Installing just the required modules simplifies administration and improves startup and reload times.

Modules can specify dependencies, allowing each module to be as small and efficient as possible, by building upon previously created modules. All of the modules will generally have at least one dependency.

Updating from the Online Repository

As part of our commitment to provide periodic updates to CompletePBX, Xorcom creates and publishes update scripts on the [Xorcom wiki](#). These scripts are only published after the updates have been completely tested. In order to ensure the integrity of your system, and to make sure that only fully-tested updates are applied, you should **not** update the software by any other method, from other sources, or by using the Module Admin dialog.

The next chapter will discuss configuring extensions and user voicemail.

2. Devices and Extensions

What are they?

Much like traditional PBX systems, CompletePBX uses extensions to route calls to individual users. Each person utilizing CompletePBX will typically be assigned a single extension. Users can dial an extension to directly access other extensions, or users. Extensions can have voicemail boxes associated with them. They can be members of ring groups, call queues, and can be targets for direct inbound calls.

Rather than having an extension associated with a particular telephone, CompletePBX separates the actual telephones into a concept called *devices*. An extension may be mapped directly to a device in the traditional style, or a device may be independent of an extension and the extension that rings the phone may change based on who is using it. CompletePBX supports both of these methodologies. In this chapter, we will discuss:

- Operational modes for extensions
- Endpoint types
- Common fields
- Setting up a new extension in Extensions mode
- Setting up a new extension in DeviceAndUser mode
- Voicemail setup

Operational Modes for Extensions

CompletePBX has the following two different modes that can be used in order to configure extensions:

- Extensions
- DeviceAndUser

In the **Extensions** mode, each numerical extension that is configured within CompletePBX corresponds to a dedicated physical telephony endpoint. An endpoint can be a physical telephone, a softphone, an Analog Telephony Adapter (ATA), or anything else that communicates with CompletePBX. In this mode, each endpoint is statically assigned to a particular device. This device is fixed, and never changes.

An example of this would be a typical cubical-office environment. Each cubical has a phone, and the number (or extension) that rings that phone will never change. Even if the employee who works in a particular cubical is replaced, the extension that rings their phone will remain the same. Most end users find this setup intuitive, as it allows them to dial one number, and their call will ring one phone. This mode is the easiest to set up, but offers less flexibility than the DeviceAndUser mode.

In the **DeviceAndUser** mode, the endpoints (devices) and extensions (users) are separate, allowing one numerical extension to correspond to an unlimited number of endpoints. The DeviceAndUser mode also allows a user to roam from endpoint to endpoint, logging in or out of a phone as their location changes.

An example of this might be a warehouse in which a manager needs to receive calls even while he is on the floor. The manager can select a cordless phone, log into it, and begin his rounds. Any calls to his extension will ring the cordless phone. When he has finished, he logs out of the phone and it no longer rings when his extension is called. This mode can be unintuitive to end users as dialing a person's direct extension number can result in several different phones ringing. This mode is very

powerful, but it is more complicated to set up.


Each operational mode has its own strengths and drawbacks. As with most complex systems, there are multiple ways to accomplish almost any telephony task with CompletePBX, so ultimately the mode that you choose should be the one that seems to best suit your environment.

Operational modes can be changed any time, but doing so may mean that a significant amount of reconfiguration is required before the system is fully functional again. It is recommended that an operational mode be chosen prior to configuring any extensions in CompletePBX.

The following table lists some common scenarios that may assist in deciding upon the two operational modes for extensions:

Scenario	Operational mode to use
A large business where new employees assume the extension of a person who has left the company. Employees always work at the same telephone	Extensions
A small business where employees generally work at the same desk, but may opt to work from home. Employees should be able to make and receive calls from home	DeviceAndUser
A hotel where each room has a static extension associated with it. Regardless of who occupies the room, calling the room's extension will always ring the phone in the room	Extension
An executive office where users sit down at a desk on a first come, first serve basis. The phone on their desk needs to ring the extension that is assigned to the person	DeviceAndUser
A technical support call center where the phone at each station is only used for inbound calls. Employees are not assigned to a particular station, but selected randomly when they report to work	Extension
A marketing company where the call center is staffed 24 hours per day. Calls are outbound only, but it needs to track who made which calls. Employees are assigned an extension, and they log into their phone when they start their shift	DeviceAndUser

You can configure the operational mode of CompletePBX by selecting the Settings menu, selecting the Advanced dialog, navigating to the System Setup section, and setting User & Devices Mode to either **extensions** or **deviceanduser**

User & Devices Mode 

extensions ▼

Choose extension numbers wisely



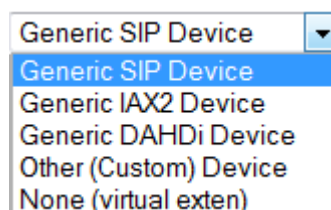
No matter which operational mode you choose, you must choose a numbering system for your extensions. It is important to choose carefully. Several extension numbers are pre-configured in CompletePBX. Other extensions are very common and are targeted by malicious users attempting to gain access to your PBX. We recommend that you use (at least) four-digit extension numbers. Avoid extensions between 201 and 299 which is a common range, and therefore are often targeted by malicious users. A common practice is to assign the last four digits of a DID as a user's extension number, so for example, DID of 555-555-5432 would ring to extension 5432.

Endpoint Types

Connectivity → Extensions

CompletePBX allows different types of endpoints to be configured:

- SIP (Session Initiation Protocol)
- IAX2 (Inter-Asterisk eXchange 2)
- DAHDI
- Other (custom)
- None (virtual extension)



CompletePBX does not require a single type to be chosen for *all* of the endpoints: types can be mixed. As long as the endpoint can communicate with CompletePBX using one of these protocols, CompletePBX will bridge calls between the devices.

SIP Endpoints

SIP endpoints are the most common type of endpoints. Most VoIP phones are SIP-based devices. Nearly all of the softphone endpoints support SIP. Choosing to utilize SIP endpoints provides the widest endpoint selection.

However, due to the large range of ports required for the **Real-time Transport Protocol (RTP)** audio stream, SIP can be problematic when traversing firewalls and other NAT devices. Common SIP configurations require a large range of open ports to function correctly. Configuration can be particularly troublesome if both the endpoint and the CompletePBX system are behind their own firewalls. The default port used to initiate SIP communications is 5060, but you can improve the security of SIP connectivity by assigning a different external port number on the firewall, and using NAT to transfer that port to the correct internal port

IAX2 Endpoints

The IAX2 protocol was designed with the shortcomings of SIP in mind and is most commonly used to link CompletePBX systems together. Several endpoints that support IAX2 are on the market, including several softphones and a few hardphones.

IAX2 uses a single port for call signaling and transmission of a VoIP audio stream. The choice of IAX2 endpoints can be very limiting, but additional firewall configuration is very simple and often not required at all.

DAHDI Endpoints

DAHDI devices are adapters for traditional two-wire **Plain Old Telephone Service (POTS)** handsets - the same handsets that are found in a home using the traditional telephone service. DAHDI endpoints are provided by Astribank FXS ports.

Custom Endpoints

Custom endpoints can be based on any protocol supported by CompletePBX. Custom endpoints are commonly based on the **Media Gateway Control Protocol (MGCP)** and the H.323 protocol. As long as CompletePBX can communicate with the endpoint using the *Dial* command, CompletePBX will allow it to be used within its interface.

Virtual Endpoints

Virtual endpoints can also be created. A virtual extension can be used, for example, as the destination for voicemail for a team of support engineers, or as the company-wide fax destination. You could configure the mailbox for all the support engineers by accessing the *Connectivity* → *Extensions* menu, and configuring the **mailbox** parameter in the **Device Options** section, so that each support engineer uses the same default mailbox. All the support engineers would receive notification that voicemail is waiting, provided that voicemail alerts are activated. Any available support engineer could access the voicemail on the virtual extension, and action it accordingly.

Endpoint Fields

Connectivity → *Extensions*

Several common configuration fields exist under both Extensions and DeviceAndUser modes. Regardless of the operational mode that is chosen for CompletePBX to operate in, these fields function in the same way. Use this section as a reference when setting up either operational mode. All of the common configuration fields and their purposes are listed here.

Common Extension/User Fields

User Extension should be a unique numerical value. If an extension that is already in use is entered, CompletePBX will display a warning when you attempt to save the extension, and the new extension will not be saved. The User Extension number can be dialed from other endpoints attached to the PBX to call this user. This field can only be edited when creating a new extension: this value of this field cannot be changed after it has been defined. This field is mandatory.

Display Name is generally the end user's name or the location of the device, e.g. Fernando Alonso or Server Room. This value will be displayed as the caller ID text for any calls placed from this user or device to other users or devices on the PBX. This field is mandatory.

CID Num Alias will change the caller ID text displayed when this user calls other users on the PBX. This is commonly used when a user is part of a department in which callbacks should be directed to

the department rather than directly to the user (such as a technical support department). This field is not required. If it is left blank, the user's extension will be used to set the Outbound Caller ID text.

SIP Alias is used to provide a friendly name for direct SIP calls made to this user. SIP aliases are most often used to distribute an address for contacting a particular user, similar to how email addresses are distributed to allow a user to be sent a message directly. A SIP alias will allow external callers to dial *alias@example.com* to call this particular user directly, without knowing the user's extension number. Note that the SIP Alias field is shown for all types of extensions (SIP, IAX2, DAHDI, and Custom). Calls to a SIP alias must come from a SIP device, but CompletePBX will bridge the call to any type of endpoint that it is able of communicating with. This field is not required. If it is left blank, the only way to place a direct SIP call to the user will be the SIP URL *<extension>@example.com*, where the extension field is replaced by the user's numerical extension.

- Edit Extension

Display Name [?]	<input type="text" value="VP Marketing"/>
CID Num Alias [?]	<input type="text"/>
SIP Alias [?]	<input type="text"/>

Outbound CID is used to set the caller ID text for calls to devices outside of the PBX. This option always requires a digital trunk (PRI/BRI, or VoIP) and setting the caller ID must be supported by the trunk service provider. This field is not required. If it is left blank, the default caller ID name for the trunk placing the call will be used to set the caller ID name text.

Asterisk Dial Options allows you to define dial options that are specific to an extension. If the **Override** checkbox is checked, this value will override the global setting that is defined in the Dialplan and Operational section of the Settings → Advanced dialog.

Ring Time is the number of seconds to ring the endpoint before sending the caller to voicemail. CompletePBX allows an endpoint to ring between 1 and 120 seconds. If no voicemail is configured for the user, this option will be ignored and the endpoint will ring until the caller hangs up. This field is a dropdown. If it is left at the default value, the extension will ring for the number of seconds configured in the **Ringtime Default** field of the Advanced Settings dialog.

Call Forwarding Ring Time determine how long (in seconds) to ring another phone, when any mode of call forwarding is active, before continuing to voicemail or some other failover destination.

Outbound Concurrency Limit limits the number of concurrent outbound calls that can be made an extension. This is a useful security feature as will limit the number of simultaneous calls that can be made on a compromised extension.

Call Waiting toggles the call waiting option on an extension. With call waiting enabled, if a user is called while the endpoint is already in use, the user will be notified of the new incoming call and will be given the option to answer it. Disabling call waiting will send incoming calls to voicemail if the endpoint is already in use. Users can manipulate call waiting from My Extension, or by dialing a feature code (*70 to activate, *71 to deactivate). This option is simply the initial setting for call waiting on an extension. If the call waiting state is toggled from the user's endpoint, then it will stay that way. It will not be overwritten by CompletePBX when it reloads. This field is a drop-down menu.

Internal Auto Answer enables automatic answering of internal calls provided that the endpoint

technology allows it. You could use a Paging & Intercom group (or a Ring group) for all the extensions that all have Internal Auto Answer enabled to enable internal users to page the phones in the group. Calls originating from external callers will not be answered automatically, and will be handled in the normal manner.

Call Screening allows users to hear who is calling before picking up a call. With this option enabled, callers will be prompted to say their name before ringing the user's endpoint. Upon answering the call, the user will hear the caller's name being played back to them and will be given the option to accept or reject the call. Rejected calls are sent to the user's voicemail, if configured, or disconnected otherwise. Call screening can either be enabled with memory (caller ID text is remembered, and callers who have identified themselves in the past will never be prompted to do so again, or without memory (callers are prompted to identify themselves every time they call in). This field is a dropdown.

Pinless Dialing allows the extension to bypass any pin codes normally required on outbound calls. Be aware that enabling this option will bypass the security on a trunk that has PIN protection.

- Extension Options

Outbound CID	<input type="text"/>	
Asterisk Dial Options	Ttr	<input type="checkbox"/> Override
Ring Time	Default	▼
Call Forward Ring Time	Default	▼
Outbound Concurrency Limit	3	▼
Call Waiting	Enable	▼
Internal Auto Answer	Disable	▼
Call Screening	Disable	▼
Pinless Dialing	Disable	▼
Emergency CID	<input type="text"/>	
Queue State Detection	Use State	▼

Assigned DID/CID group of options allow specific external telephone numbers to be assigned directly to a user's extension. Multiple DIDs can be assigned to a single extension.

None of the fields in the Assigned DID/CID group of options are required. If they are left blank, the extension will function as normal, and will only receive calls when an inbound route directs calls to it or another extension calls it directly.

DID Description is a description of the number associated with the extension.

Add Inbound DID is the actual number associated with the extension. The number must be in the format that the trunk provider sends it in (often 11 digits or full international dialing standard).

Inbound CID allows only specific caller IDs on the inbound DID to be routed to the user's extension. Caller ID text can be a specific phone number, as well as any text that may be delivered by the

telephone company, such as "Private", "Blocked", "Unknown", "Restricted", "Anonymous", or "Unavailable".

- Assigned DID/CID

DID Description [?]

Add Inbound DID [?]

Add Inbound CID [?]

 7337332001

Routing Groups section allows you control which Outbound Routes are accessible to the extension. You can grant an extension access to all available routes by selecting All Routes from the drop-down list, by selecting some other Routing Group from the drop-down list, if you want to limit access to a list of outbound or . You can use the Routing Group dialog to create a Routing Groups.

- Routing Groups

Routing Groups [?]

The **Language Code** field will force all prompts specific to the user to be played in the selected language, provided that the language is installed and voice prompts for the specified language exist on your CompletePBX server. This field is not required. If left blank, prompts will be played back in the default language of the CompletePBX server.

Some of the standard ISO 639-1 language codes that you can use include:

Language	Code
Dutch	nl
English	en

Language	Code
French	fr
German	de
Italian	it
Portuguese	pt
Russian	ru
Spanish	es
Turkish	tr

The **Recording Options** group of fields allows a user to control the recording of incoming or outgoing calls. The user can either dial a feature code (*1) to selectively enable recording for the current call, never record calls, or always record calls.

Record Priority Policy determines what will happen when there is a conflict between extensions. The recording options defined for the extension with the highest value (between 0 and 20) will be used.

- Recording Options

Inbound External Calls [?]	Always	Don't Care	Never
Outbound External Calls [?]	Always	Don't Care	Never
Inbound Internal Calls [?]	Always	Don't Care	Never
Outbound Internal Calls [?]	Always	Don't Care	Never
On Demand Recording [?]	Disable	Enable	
Record Priority Policy [?]	0	▼	

Voicemail & Directory options are discussed in a dedicated section later in this chapter.

Common Endpoint Fields

Regardless of the endpoint technology selected, the Emergency CID will always be present. The value entered here will override any other caller ID text set for the extension when the user places a call through a route configured for emergency calls in CompletePBX. This option is useful for allowing outbound calls to send accurate caller ID text to emergency service dispatch centers, where

caller ID text would otherwise provide different information (call centers often provide corporate call back numbers in caller ID text that are assigned to buildings in different physical locations from the call centers themselves). This is especially important for VoIP trunks, as calls over VoIP can originate from anywhere in the world, and the trunks do not carry the information related to location that T1 or PSTN lines do. The Emergency CID field is not required. If it is left blank, the default caller ID settings on a trunk will be used to set the caller ID when an emergency call is placed.

Common SIP/IAX2 Fields

SIP and IAX2 endpoints will have a **secret** field. This field defines the password that the endpoint will use to authenticate with CompletePBX. This field is mandatory.

Choose endpoint passwords carefully



Endpoint passwords can be the weakest link on any externally accessible PBX system, as malicious users will attempt to locate extensions having weak passwords. Endpoints 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 endpoint passwords are not distributed 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.

SIP endpoints will also have a `dtmfmode` field. The DTMF mode for a SIP device specifies how touch tones will be transmitted to the other side of the call. Possible values for this field are `rfc2833`, `inband`, `info`, and `auto`. The default value of `rfc2833` is typically fine and should not be changed unless a trunk provider specifically requires it.

It is important to set the DTMF mode correctly, based on the trunk. DTMF tones that are transmitted inband on a compressed stream (anything that is not using the ULAW or ALAW codec) will be garbled and will not be recognized on the receiving side. The value `rfc2833` will send the tones as data within the RTP payload, and `info` will send the tones as data in the SIP info headers. Both data methods are more reliable at transmitting understandable tones than inband, but must be supported by the device generating the tones. The **auto** option will attempt to use `rfc2833`, but will fail over to inband if the receiving host does not indicate support for the data-based tones. The `dtmfmode` field is required.

Additional SIP Fields

Once saved, clicking on a SIP device will show additional options that were not available during the initial setup:

The **canreinvite** option specifies whether a SIP endpoint can issue re-invites to other endpoints. By default, the media stream for a SIP call will pass through the CompletePBX server before reaching the other endpoint, even if both endpoints are on the same network. Re-invites allow two SIP endpoints to take CompletePBX out of the media path and speak directly with one another. This can improve latency in certain situations, but for most setups, this will cause dropped calls or unusable call quality. Valid values for `canreinvite` are **yes** and **no**. This field is not required. If it is left blank, the default value of **no** will be used.

The **context** option allows the device to be placed into a specific context within CompletePBX. A

context should have been manually created in *the /etc/asterisk/extensions_custom.conf* file for this to work properly. The CompletePBX **from-internal** context includes everything needed to provide access to all the standard extension features, such as voicemail, outbound routes, and feature codes, and should be used as the default context. Specifying a custom context may cause certain CompletePBX features to function incorrectly. This field is required.

The **host** option is used to define where calls for an extension should be sent. Valid values are "dynamic", or a specific IP address. Dynamic extensions will register with CompletePBX and CompletePBX will keep track of where they registered from, hence it knows where to send the call. Endpoints that have dynamic IP addresses should leave this set as "dynamic". Endpoints with static IP addresses can have their IP address entered in this field. These devices are not required to register with CompletePBX because when CompletePBX receives a call for them, it will forward the call to the configured IP. This field is not required. If it is left blank, the default value of "dynamic" will be used.

The **type** option is used to configure what types of calls will be expected from this extension. Valid options for the type field are **peer**, **user**, and **friend**. From the perspective of the CompletePBX server, calls are sent to peer endpoints, they are received from user endpoints, and can be either sent to or received from "friend" endpoints. A normal office telephone handset will be configured as a "friend" endpoint. A call center that does not allow its agents to make outbound calls may configure all of its endpoints as peer endpoints. A hotel lobby may have a phone that is for outbound calls only (to other hotel guests), which would be configured as a user endpoint. This field is not required. If it is left blank, the default value of "friend" will be used.

The **NAT** option specifies whether this endpoint is expected to be placed behind a device performing **Network Address Translation (NAT)**. This option should only be disabled if a specific setup requires internal IP addresses to be sent to a remote CompletePBX server (for example, a phone that connects to CompletePBX over a VPN and the VPN passes through a NAT device). Valid nat values can only either **yes** or **no**. This field is not required. If it is left blank, the default value of "yes" will be used. Setting nat to "no", CompletePBX will use rport if the remote side says to use it; setting nat to "yes" forces rport to always be on.

The **port** option allows a custom port to be set for the endpoint, SIP control data is sent on this custom port. Note that this port is only used for SIP signaling and not for the actual media stream. The default port is **5060**, and most SIP servers will be listening on this port. This option is commonly changed where endpoints are using a connection on which port 5060 is blocked. Note that if the port value is changed, the CompletePBX server must also be listening for SIP signaling connections on the custom port specified. Valid values for **port** are numeric entries between 1 and 65,000. This field is not required. If it is left blank, the default value of 5060 will be used.

Port for external SIP devices



Note that the default setting in the firewall only allows access to ports 5060/5061 from internal networks (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) so you will need to configure the firewall to allow access from whatever ports you choose to use for external SIP devices. You should also be aware that CompleteSBC (with default settings) uses ports 6075/6076: access via these ports is allowed in the default firewall configuration.

The **qualify** option will keep track of an endpoint causing CompletePBX to ensure that the endpoint is still online. If qualification for an endpoint is enabled, CompletePBX will also track its response

time relative to the PBX. This option can be useful for tracking latency between the PBX and its endpoints. Running the command *sip show peers* from the **CompletePBX command line interface (CompletePBX CLI)** will show a list of all SIP endpoints along with the number of milliseconds it has been since the endpoint responded to a qualify request. Valid values for the **qualify** option are **no**, **yes**, or a numerical time value in milliseconds. Setting this option as **yes** will qualify an endpoint every 200 milliseconds. This field is not required. If it is left blank, the default value of **no** will be used.

The **callgroup** and **pickupgroup** options allow users to pick up calls that are not directed to them by dialing a feature code (*8). Both values are numeric and range between 0 and 63.

Extensions can be placed into multiple groups by separating numerical values by commas. Calls directed to any phone in a particular call group can be answered by any user who is a member of the corresponding pickup group (for example, a user in *pickupgroup 1* will be able to pick up any call directed to any phone in *callgroup 1*). This can be useful for small office or home setups, where it is easier to simply pick up a call from another phone rather than forward that call to another extension.

Note that a user can be part of a *pickupgroup* without being a member of the associated *callgroup* (for example, a senior staff member may be able to pick up any call directed to anyone in his department, but his department should not be able to pick up calls directed to the senior staff member).

Neither the *callgroup* field nor the *pickupgroup* field is required. If they are left blank, the endpoint will simply not be a member of a *callgroup* or *pickupgroup*, and will not be able to use the call pickup functionality.

The **disallow** option should contain a list of codecs, which the endpoint should not use to communicate with CompletePBX. Multiple codecs can be specified separated by spaces. Valid **codec** values are "all", "g723", "gsm", "ulaw", "alaw", "g726", "adpcm", "slin", "lpc10", "g729", "speex", and "libc".

It is common practice to first disallow all codecs in this line, and then, specifically allow a select few using the **allow** option. This field is not required. If it is left blank, no codecs will be disallowed, and CompletePBX may attempt any codec available to it when establishing a call to the endpoint.

The **allow** option is the opposite of the **disallow** option, and is used to specify which codecs should be used for communication with the endpoint. Codecs are used with preference to the order in which they are specified.

The **allow** option has the same valid values as the **disallow** option. This field is not required. If it is left blank, no codec will be preferred by the endpoint, and CompletePBX may use any codec available to it when establishing a call to the endpoint. CompletePBX will give preference to codecs that do not require transcoding.

This device uses sip technology.

secret [?]	<input type="text" value="RD2XJlb8T"/>
dtmfmode [?]	<input type="text" value="RFC 2833"/>
canreinvite [?]	<input type="text" value="No"/>
context [?]	<input type="text" value="from-internal"/>
host [?]	<input type="text" value="dynamic"/>
trustpid [?]	<input type="text" value="Yes"/>
sendrpid [?]	<input type="text" value="No"/>
type [?]	<input type="text" value="friend"/>
nat [?]	<input type="text" value="No - RFC3581"/>
port [?]	<input type="text" value="5060"/>
qualify [?]	<input type="text" value="yes"/>
qualifyfreq [?]	<input type="text" value="60"/>
transport [?]	<input type="text" value="UDP Only"/>
encryption [?]	<input type="text" value="No"/>
callgroup [?]	<input type="text"/>
pickupgroup [?]	<input type="text"/>
disallow [?]	<input type="text"/>
allow [?]	<input type="text"/>
dial [?]	<input type="text" value="SIP/2941"/>
accountcode [?]	<input type="text" value="2941"/>
mailbox [?]	<input type="text" value="2941@default"/>
vmexten [?]	<input type="text"/>
deny [?]	<input type="text" value="0.0.0.0/0.0.0.0"/>
permit [?]	<input type="text" value="192.168.0.0/255.255.240.0"/>

The **dial** option is the dial string CompletePBX will use to call the endpoint. Any valid CompletePBX dial string is admissible for this option. This field is required.

The **accountcode** option is typically used for billing purposes. A string value of length up to 20 characters may be used for the account code. The value entered here will show up in the CompletePBX CDR for every call placed by this extension. This field is not required. If it is left blank, the CDR will log the extension that placed a call, but will not log any account code associated with the call.

The **mailbox** option is used to specify the voicemail box that the device will be checking. The SIP protocol will return the number of waiting messages in the specified mailbox when this device queries CompletePBX for waiting messages. Most endpoints will provide some kind of indication when their mailboxes have messages in them (such as a flashing light or a stuttering dial tone). Valid values are any mailboxes that have been created using CompletePBX or entered manually into the */etc/asterisk/voicemail.conf* file. This field is not required. If left blank, the endpoint will not check to see if any voicemail messages are waiting.

The **deny** option specifies network addresses from which CompletePBX should not accept traffic for this peer. This option should be in the format of an IP address and subnet, such as 192.168.1.0/255.255.255.0 (to disallow traffic for this extension from the IP range of 192.168.1.1 to 192.168.1.254). It is possible to enter a value of 0.0.0.0/0.0.0.0 to deny all of the networks by default, and, to enter specific networks from which traffic can be accepted in the **permit** option.

This option is commonly used to restrict endpoint usage to a particular network, so that if the endpoint is stolen or otherwise removed from the network, it cannot be used to place calls and will be essentially useless. This field is not required. If it is left blank, CompletePBX will not block traffic for this peer from any IP address.

The **permit** option is the opposite of the **deny** option. Specific IP addresses or networks can be added in this option to allow traffic for this extension from the entered IP/network. This field is not required. If it is left blank, traffic will be allowed from all IP addresses.

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

Additional IAX2 Fields

Once saved, clicking on an IAX2 device will show additional options that were not available during initial setup:

This device uses iax2 technology.

secret [?]	<input type="text" value="226"/>
transfer [?]	<input type="text" value="Yes"/>
context [?]	<input type="text" value="from-internal"/>
host [?]	<input type="text" value="dynamic"/>
type [?]	<input type="text" value="friend"/>
port [?]	<input type="text"/>
qualify [?]	<input type="text"/>
disallow [?]	<input type="text" value="all"/>
allow [?]	<input type="text" value="gsm"/>
dial [?]	<input type="text" value="IAX2/5972"/>
accountcode [?]	<input type="text" value="2972"/>
mailbox [?]	<input type="text" value="2972@default"/>
deny [?]	<input type="text" value="0.0.0.0/0.0.0.0"/>
permit [?]	<input type="text" value="0.0.0.0/0.0.0.0"/>
requirecalltoken [?]	<input type="text" value="Yes"/>

The additional options shown for IAX2 endpoints are very similar to the additional options shown for SIP endpoints. The only additional option available to IAX2 endpoints is the **nottransfer** option.

The IAX2 **nottransfer** option is the equivalent of the SIP **canreinvite** option (although the values are reversed). Setting the **nottransfer** option to **yes** prohibits the media path from being transferred away from CompletePBX, keeping CompletePBX in the media path at all times. If **nottransfer** is set to **no**, IAX2 endpoints will be able to communicate directly with one another, removing CompletePBX from the media path entirely.

All other additional IAX2 options are equivalent in functionality to their SIP option counterparts.

Common DAHDI Fields

DAHDI endpoints must have a **channel** field. It refers to the DAHDI channel that the CompletePBX DAHDI driver will use to communicate with the DAHDI endpoint. The channel is specific to each FXS port of the Astribank. Running the *lsdahdi* command from the Linux command line will output a list of all (DAHDI) devices on the system and a list of the channels for each device. The value that is entered into the channel field must be present in the list that the *lsdahdi* command returns.

Additional DAHDI Fields

Once saved, clicking on a DAHDI device will show additional options seen in the following screenshot, which were not available during initial setup:

This device uses dahdi technology.

channel [?]	<input type="text" value="73"/>
context [?]	<input type="text" value="from-internal"/>
immediate [?]	<input type="text" value="No"/>
signalling [?]	<input type="text" value="fxo_ks"/>
echocancel [?]	<input type="text" value="yes"/>
echocancelwhenbridged [?]	<input type="text" value="No"/>
echotraining [?]	<input type="text" value="no"/>
busydetect [?]	<input type="text" value="No"/>
busycount [?]	<input type="text" value="no"/>
callprogress [?]	<input type="text" value="No"/>
dial	<input type="text" value="DAHDI/73"/>
accountcode [?]	<input type="text"/>
callgroup [?]	<input type="text" value="1"/>
pickupgroup [?]	<input type="text" value="1"/>
mailbox [?]	<input type="text" value="1011@device"/>

Several additional DAHDI configuration options are equivalent to their SIP or IAX2 configuration option counterparts.

immediate will cause CompletePBX to start executing its dialplan for this extension as soon as the handset goes "off hook", without the caller ever having to dial anything. This option is commonly used for emergency phones, such as phones in an elevator, so that the emergency personnel are contacted as soon as someone picks up the phone.

This option is useful only if a custom context has been built to support it, and that context is specified in the context option. Custom contexts must be manually written into the `/etc/asterisk/extensions_custom.conf` file.

signalling is used to specify the type of signaling used by the channel. Signaling is specified using a string, and must correspond to the DAHDI settings for the channel. For example, Xorcom Astribank FXS channels are defined in the DAHDI configuration file (`/etc/dahdi/system.conf`) as `'fxoks=1'` so the 'signaling' parameter must be defined as `fxo_ks`

echocancel enables *software* echo cancellation for the endpoint. This is not to be confused with hardware echo cancellation that some devices have as an option. Hardware echo cancellation must be configured on the device itself. The **echocancel** option can be set to one of these values—**no**, **yes**, **16**, **32**, **64**, **128**, or **256**.

Setting the option to **no** disables echo cancellation. Setting the option to **yes** enables echo cancellation with a value of 128. The numerical value specified in the **echocancel** option is the number of taps that CompletePBX will use to sample the media stream to determine the best way to cancel an echo on the call. One tap is one sample from the data stream.

Note that if this option is set to anything other than one of the valid values specified, CompletePBX will default the option to yes (128 taps) without warning.

echocancelwhenbridged allows echo cancellation to be enabled or disabled for calls that are bridged between two DAHDI channels. As most of the time the calls between two DAHDI endpoints will not have any echo, this option is not required. It is best practice to begin adjusting for echo only after the echo is experienced, rather than trying to adjust the echo cancellation properties based on echoes that might occur. Valid values for the **echocancelwhenbridged** field are **yes** or **no**.

echotraining allows a DAHDI channel to train itself for the proper echo cancellation requirements for the call, before the call begins. Valid values for echo training are **yes**, or they may be numbers between 10 and 4,000. When enabled, CompletePBX will mute the channel at the beginning of any call made to or from this device for the number of milliseconds entered as a value. During this time, a pulse will be sent to the other side of the call, and the information gathered from whatever echo of this pulse is returned, which will be used to fine tune the echo cancellers on the channel. This can often result in echo-free calls from the very beginning of the conversation, instead of forcing the echo trainer to begin training after the call has already started. As with the **echowhenbridged** field, it is a good idea to start adjusting the **echotraining** field only after the echo is experienced. Note that **echotraining** is not required for OSLEC software echo canceller or for the Hardware Echo Canceller

busydetect is used to detect if a called DAHDI channel returns a busy tone. As DAHDI endpoints are typically analog devices and can therefore not return their status to CompletePBX, enabling the **busydetect** option allows CompletePBX to know that the called endpoint is in use and enables calls to be routed appropriately based on that information. Valid values for this option are **yes** and **no**.

busycount works in conjunction with the **busydetect** option. If the **busydetect** option is set to **yes**, the value set in the **busycount** option is used as the number of busy tones for which CompletePBX will wait before it determines that a channel is busy.

Valid values are whole numbers greater than 1. The higher this value is, the longer a busy channel will take to disconnect. However, lower values may cause repetitive sounds in a conversation to be treated as busy/disconnect tones, and that call will be terminated. The default value of **7** is recommended.

When enabled, the **callprogress** option will force CompletePBX to try to recognize various analog tones, which are types of **Special Information Tones (SIT)**, in order to determine how a call is progressing. CompletePBX will attempt to recognize ringing tones, busy tones, disconnection tones, or sounds indicating that a call has been answered. Although this option typically provides few

benefits, it will usually result in quicker termination of disconnected channels.

Common Custom Fields

Custom endpoints must have a **dial** field. This field is for specifying a custom *Dial* command that CompletePBX will use to communicate with the endpoint (using a protocol that is not SIP, IAX2, or DAHDI).

Common custom dial strings are *H323/`\${EXTEN}@(IPADDRESS)* for an H.323 device, and *MGCP/`\${EXTEN}@(IPADDRESS)* for an MGCP device. The *IPADDRESS* token should be replaced with the IP address of the device being added.

Configuring Extensions in Extensions Mode

Connectivity → *Extensions*

In Extensions mode, each user who is defined in CompletePBX has a single endpoint associated with them. Extensions mode is a good choice for simple setups where each person configured on the PBX is always expected to be using the same phone. If your CompletePBX system is configured in the *DeviceAndUser* mode, you can skip this section.

Configuring Extensions Mode

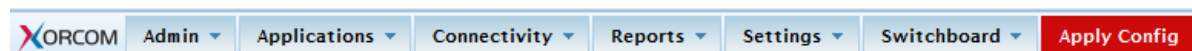
Settings → *Advanced*

Switching CompletePBX between operational modes is done from the Administration GUI by entering the **Advanced Settings** dialog.



If CompletePBX was configured to use Extensions mode during initial installation, no additional configuration is required to begin creating extensions. These instructions only need to be followed if CompletePBX was set up to use the *DeviceAndUser* mode during the initial installation

Log in to the Administration interface, navigate to the Settings menu, and select the Advanced dialog. Navigate down to the System Setup section, and modify the **User & Devices Mode** parameter to the default value of **extensions**, and click on the arrow within the green circle to the right. The configuration changes must be applied to CompletePBX by clicking on the red-colored **Apply Config** bar at the top of the screen.

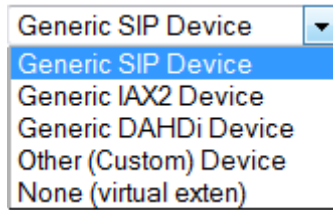


CompletePBX will now be running in **extensions** mode.

Configuring Extensions

Connectivity → *Extensions*

Now that CompletePBX is running in Extensions mode, we can begin creating extensions. Each endpoint used will require a unique extension. To configure extensions, navigate to the CompletePBX Administration interface and click on the Connectivity menu on the navigation bar, and select the Extensions dialog. The **Add an Extension** dialog will be displayed:



From the **Device** drop-down menu, select the type of endpoint that is being configured (SIP, IAX2, DAHDI, or other). Click on the **Submit** button. Additional form fields will be displayed like those in the following screenshot:

Add SIP Extension

- Add Extension

User Extension [?]	<input type="text"/>
Display Name [?]	<input type="text"/>
CID Num Alias [?]	<input type="text"/>
SIP Alias [?]	<input type="text"/>

- Extension Options

Outbound CID [?]	<input type="text"/>
Ring Time [?]	Default ▾
Call Forward Ring Time [?]	Default ▾
Outbound Concurrency Limit [?]	No Limit ▾
Call Waiting [?]	Enable ▾
Internal Auto Answer [?]	Disable ▾
Call Screening [?]	Disable ▾
Pinless Dialing [?]	Disable ▾
Emergency CID [?]	<input type="text"/>
Queue State Detection [?]	Use State ▾

- Assigned DID/CID

DID Description [?]	<input type="text"/>
Add Inbound DID [?]	<input type="text"/>
Add Inbound CID [?]	<input type="text"/>

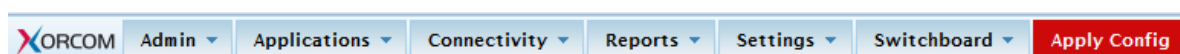
Fill out the form fields with the appropriate information. Information on most fields can be found in the *Common fields* section covered earlier in this chapter. Information regarding the **Voicemail & Directory** group of fields can be found in the [Voicemail setup](#) section of this chapter. Information

regarding **VmX Locator** fields can be found in the [Follow Me and VmX Locator](#) section of Chapter 6.

Note that only **User Extension**, **Display Name**, and if present, **secret** are required fields. All other fields can be left at their default values and the extension will still be created successfully. In addition, all fields except for the User Extension field can be altered after the extension has been saved.

Note that a list of all of the user extensions that already exist is present on the right side of the screen. This list can be used to easily determine the next available unique extension number.

Once all fields have been filled out, click on the **Submit** button at the bottom of the page to save the extension. The extension that was just saved will be in the extension list on the right side of the screen. Before the extension can be used, the configuration changes must be applied to CompletePBX. Click on the red-colored **Apply Config** bar at the top of the screen:



Once a device is saved, clicking on the device name in the active extensions list will provide additional options that were not accessible during the extensions initial setup for SIP, IAX2, and DAHDI devices. (Note that custom devices do not have any additional options.) CompletePBX assigns the most common values to these additional options. Typical setups will not require any changes.

Configuring Extensions in DeviceAndUser Mode

In the DeviceAndUser mode, each user defined in CompletePBX can have multiple endpoints associated with them. DeviceAndUser mode is a good choice for more complex setups, where each person configured on the PBX is expected to work from multiple, different phones or multiple locations. If your CompletePBX system is configured in the Extensions mode, this section can be skipped.

Configuring DeviceAndUser Mode

Settings → Advanced

Switching CompletePBX between operational modes is done from the Administration interface in the Advanced Settings dialog.



If CompletePBX was configured to use **DeviceAndUser** mode during initial installation, no additional configuration is required to begin creating devices and users. These instructions only need to be followed if CompletePBX was set up to use the Extensions mode during initial installation

Log in to the Administration interface, navigate to the **Settings** menu, and select the **Advanced** dialog. Navigate down to the **System Setup** section, and modify the **User & Devices Mode** parameter from the default value of **extensions** to **deviceanduser**, and click on the arrow within the green circle to the right of the parameter.

You should also modify the value of **Dynamically Generate Hints** (in the **Dialplan and Operational** section) to **True**, so that the dial plan can be dynamically modified whenever a User logs in. Again, do not forget to click on the arrow within the green circle to the right of the parameter.

The configuration changes must be applied to CompletePBX by clicking on the red-colored **Apply Config** bar at the top of the screen.



CompletePBX will now be running in **deviceanduser** mode.

Configuring Users

Connectivity → Users

Now that CompletePBX is running in DeviceAndUser mode, we can begin creating users on the system. Each user will require a unique numerical extension. To configure users, navigate to the **Connectivity** menu and select the **Users** dialog. Click on the **Add Users**: the **Add User/Extension** screen will be displayed:

Add User/Extension

- Add User

User Extension [?]	<input type="text"/>
User Password [?]	<input type="password"/>
Display Name [?]	<input type="text"/>
CID Num Alias [?]	<input type="text"/>
SIP Alias [?]	<input type="text"/>

- Extension Options

Outbound CID [?]	<input type="text"/>
Ring Time [?]	Default ▾
Call Forward Ring Time [?]	Default ▾
Outbound Concurrency Limit [?]	2 ▾
Call Waiting [?]	Enable ▾
Internal Auto Answer [?]	Disable ▾
Call Screening [?]	Disable ▾
Pinless Dialing [?]	Disable ▾
Queue State Detection [?]	Use State ▾

- Assigned DID/CID

DID Description [?]	<input type="text"/>
Add Inbound DID [?]	<input type="text"/>
Add Inbound CID [?]	<input type="text"/>

Fill out the form fields with the appropriate information. Besides the common configuration fields, there will be a **User Password** field. This field is a numerical password that this user can use to log into any endpoint attached to CompletePBX.

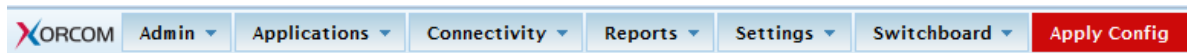
Information on most fields can be found in the *Common fields* section earlier in this chapter. Information regarding **Voicemail & Directory** fields can be found in the [Voicemail Setup](#) section later in this chapter. Information regarding the VmX Locator fields can be found in the [Follow Me and VmX Locator](#) section of Chapter 6.

Note that only **User Extension**, **User Password**, and **Display Name** are required fields. All of the other fields can be left at default values and the extension will still be created successfully. In addition, all fields except for the User Extension field can be altered after the extension has been

saved.

Once all of the fields have been filled out, click on the **Submit** button at the bottom of the page to save the extension. The user that was just saved will now be shown in the active user list on the right side of the screen.

Before the extension can be used, the configuration changes must be applied to CompletePBX. Click on the red-colored **Apply Config** bar at the top of the screen as shown in the following screenshot:



Once a user is saved, clicking on the user name in the active users list will load the user settings to be edited. Certain dialogs such as **Follow Me** will add additional options that were not accessible during the initial setup of the user.

Follow Me Settings are discussed in more detail in Chapter 6. Once a user is configured, we can proceed with configuring devices.

Configuring Devices

Connectivity → *Devices*

With a user configured, it is now possible to configure devices. To configure devices, navigate to the CompletePBX Administration interface, click on the **Connectivity** menu on the navigation bar and select **Devices** dialog:

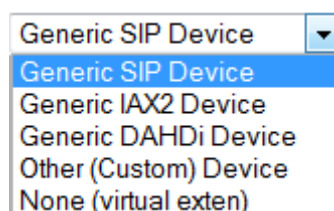
Add Device

Please select your Device below then click Submit

- Device

Device

From the Devices drop-down menu, select the type of endpoint that is being configured (SIP, IAX2, DAHDI, or other). Click on the **Submit** button.



Fill in the appropriate fields in the dialog. The fields in the dialog will vary depending on the type of

endpoint that will be in use. All endpoint types will have fields for **Device ID**, **Description**, **Emergency CID**, **Device Type**, and **Default User**.

The **Device ID** field is a unique numerical value that is used by CompletePBX to dial the device. SIP and IAX2 devices will require this value when the devices themselves are being configured.

Description is a text description of the purpose of the device. It is common to use this field to describe the location of the device or its MAC address.

The **Device Type** field can be either "fixed" or "adhoc". A **fixed** device will always have the same user logged into it (it will not be possible for the user to log out of the device). An **adhoc** device allows users to log in and out of itself at will. When a user is logged into an ad-hoc endpoint, any calls to their extension will ring that endpoint. Users can be simultaneously logged into as many endpoints as they wish.

The user selected in the Default User dropdown is the user that will be logged into the device by default. Fixed devices require this value to be set. Adhoc devices can have this value set to "none" so that no user is logged into the device by default.

Once all of the required fields are filled in, click on the **Submit** button at the bottom of the page to save the device configuration.

Once a device is saved, clicking on the device name in the active devices list will load additional device configuration options that were not available during the initial setup for SIP, IAX2, and DAHDI devices.

CompletePBX assigns the most common values to these additional options. Typical setups will not require any changes.

Faxing

Connectivity → *Extensions* or *Connectivity* → *Users*

Any extension can also be used as a fax recipient in order to receive inbound faxes. Navigate to the Fax section towards the bottom of the Extensions dialog. If you check on Enabled, the extension will become a Fax Recipient and can be used as a destination for inbound faxes. You must also enter an email address to be associated with the extension to enable the system to activate the fax-to-email capability of the CompletePBX. You can also configure the format that will be used when attaching incoming faxes to email. The format options that you can select are: pdf, tif, or both.

- Fax

Enabled [?]

Fax Email [?]

Attachment Format [?]

The user of any extension can also send outbound faxes. Use the Fax Master section, also towards the bottom of the Extensions dialog, to personalize settings for outbound faxes

Local Station Identifier is the fax number from which outbound faxes will appear to be sent, to enable the recipient to reply by fax.

Name for Cover Sheet is the sender's name that will be shown on outgoing faxes.

Phone Number for Cover Sheet is the sender's phone number that will be shown on outgoing faxes, to enable the fax recipient to call the sender.

Email for Cover Sheet is the sender's email address that will be shown on outgoing faxes, to enable the fax recipient to respond by email.

- Fax Master

Local Station Identifier	7337331001
Name for Cover sheet	VP Marketing
Phone Number for Cover sheet	+9727337332001
Email for Cover sheet	completepbx@gmail.com

Voicemail Setup

Connectivity → *Extensions* or *Connectivity* → *Users*

The voicemail capabilities built into CompletePBX compare well against enterprise-level voicemail solutions. CompletePBX makes voicemail boxes a breeze to set up.

Voicemail Delivery Options

Voicemail options are located either on the **Extensions** page (if CompletePBX is operating in Extensions mode), or on the **Users** page (if CompletePBX is operating in DeviceAndUser mode). From the CompletePBX **Connectivity** menu, either click on **Extensions** or on **Users**, click on the name of the user for whom you want to configure voicemail settings in the active users list, and scroll to the bottom of the page to view voicemail settings:

- Voicemail

Status	Enabled ▾
Voicemail Password [?]	2001
Email Address [?]	2001@mymailbox.com
Pager Email Address [?]	
Email Attachment [?]	yes no
Play CID [?]	yes no
Play Envelope [?]	yes no
Delete Voicemail [?]	yes no
VM Options [?]	
VM Context [?]	default

The **Status** field can be set to either "Enabled" or "Disabled". If voicemail is disabled, messages cannot be left for the user and calls directed to them will continue to ring until the caller hangs up.

All other voicemail options are disabled, unless this field is set to "Enabled".

The **Voicemail Password** field should be set to a numerical password that the user will enter to access their message center. This setting can also be changed by the user from their VoIP endpoint.

If a valid email address is entered in the **Email Address** field, any time a voicemail is left for the user 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.

The **Pager Email Address** field can be used to have CompletePBX send a short message to a mobile device (or to a secondary email address) whenever a new message is left in the user's voicemail. The message will be under 140 characters, and is typically used in conjunction with SMS or pager mobile services. Note that this field is *not* for a mobile phone number, but rather an email address that will reach a mobile device. Most mobile carriers provide an email-to-SMS gateway service that can be used to send emails to mobile telephones. Only one address can be entered into this field.

If the **Email Attachment** field is set to **yes**, the email message sent to the address in the Email Address field will have a copy of the voicemail attached to it. This message can then be played through the speakers of the computer on which it was received. Messages are not attached to email notifications sent to the address in the Pager Email Address field.

If the **Play CID** field is set to **yes**, the system will play back the caller ID number of the person who left the message prior to the message being played.

If the **Play Envelope** field is set to **yes**, the user will hear the date and time that the message was left prior to hearing the message being played.

If **Delete Voicemail** field is set to **yes**, new messages will be deleted from the user's messaging center as soon as the notification email is delivered to the address specified in the Email Address field.

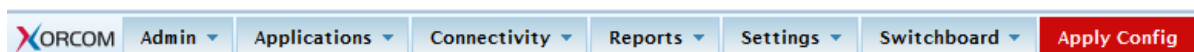


Be very careful with the **Delete Voicemail** option, because CompletePBX will allow you to delete the message without guaranteeing that a copy of it attached to the email notification. This could mean that after a message is left and a notification email is sent to the user, the actual voicemail that was left may not be accessible at all.

The **VM Options** field can contain any option that would normally be specified in the */etc/asterisk/voicemail.conf* file. These options can enable other options such as forcing a user to record their name and greeting before listening to messages, increasing the volume on voicemail messages as they are recorded, or enabling a warning for the user if they are using a temporary greeting as their outgoing message. Details on these options can be found in Appendix C, *Voicemail.conf Options*, or in the CompletePBX documentation for the *voicemail.conf* file. Multiple options can be entered into this field by separating the options with commas.

The **Voicemail Context** field is a string value that can be set to any valid context configured within the */etc/asterisk/voicemail.conf* file. Voicemail contexts can be used to apply one collection of settings to a particular group of mailboxes. If you have not manually edited the */etc/asterisk/voicemail.conf* file to create your own voicemail contexts, leave it as "default".

When configuring voicemail settings is complete, click on the **Submit** button at the bottom of the page followed by the red-colored **Apply Config** bar at the top of the page.



Managing Voicemail Messages

There are two primary ways for a user to manage their voicemail messages:

- Dialing into the CompletePBX messaging center using a feature code
- Viewing CompletePBX **My Extension** web site

Users can dial *97 to access their own mailbox when dialing from their own extension (Extensions mode), or from the device where their extension is logged in. They will be prompted for a password only. If the user is calling from someone else's phone on the PBX, they can dial *98. They will be prompted for their extension and their password. Once a valid password has been entered, the user will hear voice prompts that direct which buttons to press on their touch tone telephone or softphone in order to listen to and manage their voicemail messages.

Once logged into the messaging center, the following options are valid:

1: Plays the oldest unheard message (if any), or plays the oldest message that is still stored. When listening to a message, the following options are valid:

3: Advanced options, allows user to send a voice reply, call the caller who left the message, and hear date and time information about the voicemail

4: Play the previous message

5: Repeat the current message from the beginning

6: Play the next message

7: Delete the current message

8: Forward the message to another user on the PBX

9: Save the message to another folder

*****: Rewind the message five seconds

#: Fast forward the message five seconds

2: Change folders

3: Advanced mailbox options

0: Mailbox options. Once in mailbox options, the following options are valid:

1: Record unavailable message

2: Record busy message



3: Record name

4: Change voicemail password

*****: Return to the main menu

If the user would like to have a visual overview of their messages, voicemail messages can be viewed and administered from **My Extension** Web page that is accessible from the CompletePBX Launch Pad. To access **My Extension**, visit the IP address of your CompletePBX server in the recordings directory (for example, <http://192.168.0.64/recordings>). The **My Extension** login screen will be shown:

Login

Login: 
Password: 

 Remember Password

Use your **Voicemail Mailbox and Password**
 This is the same password used for the phone

For password maintenance or assistance, contact your Phone System Administrator.

Users can log into **My Extension** using their extension number for the **Login** field and their voicemail password for the **Password** field. Once logged in, users will see a visual representation of their voicemail messages:

Call Monitor
Voicemail

Fax

Feature Codes
Follow Me
Phone Features

VmX™ Locator
Settings

Logout




Folders:
INBOX (1)

Voicemail for Sales 5 (2008)

delete move_to Folder forward_to Results 1

email_to

select: all none

	Date	Time	Caller ID	Priority	Orig Mailbox	Duration	Playback	Download
<input type="checkbox"/>	2013-04-09	9:33:41	"Support 1" <2009>	2	2008	2 sec	 	

From **My Extension**, users will be able to play messages by clicking on the **play** link in the **Playback** column.

A message can be deleted by clicking on the checkbox next to the message date and clicking on the **delete** button.

A message can be moved into another folder by clicking on the checkbox next to the message date, selecting a new folder in the **Folder** dropdown, and then clicking on the **move_to** button.

A message can be forwarded to another user by clicking on the checkbox next to the message date, selecting a user in the empty second-row dropdown, and then clicking on the **forward_to** button.

Endpoint Manager

Settings → Endpoint Manager

Overview

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.

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 CompletePBX server
 - Ports used by SIP, IAX2, HTTP, and HTTPS protocols
 - Addresses of DNS and NTP server/s
3. Create a Template for each group of phone models that you want to manage, and link it to a set of Host Settings. (You do not need to create a template for every IP phone in the system, only for groups of phones. For example, if you are supporting two different models of Xorcom phones, you would need to create two templates – one for each model.
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) CompletePBX extensions

Option 66 on DHCP Server

Configuring Option 66 on your DHCP server will tell the DHCP server to provide IP phones with the URL that they should use for configuration provisioning.

Endpoint Manager provides the IP phones with configuration information in response to a HTTP request. The format of the request URL must be in the format **http://[pbx-ip-address]/xepm-provision**.

If you choose to use the DHCP server that is built-in to CompletePBX, configuring the Option 66 settings is quite simple.

Type the IP address of the server that will be hosting the configuration file in the **Option 66** field. A physical address has been used in the example below, but you could also use a logical address, provided that your DNS server is able to translate the logical address to a physical address.

If you check on the **Use for Endpoint Manager** check box, the DHCP server will automatically prefix the Option 66 address with **http://**, and will automatically add **/xepm-provision** at the end of the address.

If you are using a non-standard directory, you will need to write the complete location, for example **http://212.199.17.117/EPM** in the Option 66 field, and **NOT** check on the **Use for Endpoint Manager** check box

If you are not using the DHCP server that is built-in to CompletePBX, you will need to define the complete URL for option 66 on your DHCP server in the format **http://212.199.17.117/xepm-provision**.

DHCP Configuration

Settings

DHCP [?]	<input type="button" value="Enable"/> <input type="button" value="Disable"/>
Disabled Interfaces [?]	<input type="text"/>
Start Address [?]	<input type="text"/>
End Address [?]	<input type="text"/>
Lease Time [?]	<input type="text"/> Hours <input type="button" value="v"/>
Gateway [?]	<input type="text"/>
Primary DNS [?]	<input type="text"/>
Secondary DNS [?]	<input type="text"/>
NTP Server [?]	<input type="text"/>
Option 66 [?]	<input type="text" value="212.199.17.114"/>
Use for Endpoint Manager [?]	<input checked="" type="checkbox"/>
WINS [?]	<input type="text"/>

Configuration Files

Previous versions of Endpoint Manager created static configuration files which were stored in the /tftpboot directory. When a device required provisioning, it would “pull” the file from this directory. However, this approach could potentially impact the integrity of the system. The Endpoint Manager introduced in CompletePBX v4.5 creates these files dynamically. When an IP phone requires provisioning, it makes a request to the Endpoint Manager for a new configuration file, which is generated “on-the-fly”, and is sent to the phone. Clicking **Apply** after making modifications makes these changes immediately available to any phone requesting an update.

Multi-layer Definitions

When you create a template, you can also define General Settings, Device Buttons, Expansion Modules and Advanced Settings.

However, after a device is designated as an Assigned Device in the Device Mapping dialog, you can modify any of those settings. Any settings that are changed in the Device Mapping dialog will now override the base definitions that were stored in the template.

Alternatively, extension users can enter My Extensions, and personalize some (but not all) of their phone settings, such as Device Buttons, Expansion Modules, and Timezone. Any setting that is modified by users from My Extension will also modify settings stored by the Device Mapping dialog. Any setting that has been modified from either the Device Mapping dialog or My Switchboard will take precedence over any setting that was defined in the Template dialogs.



Note that if you update any configuration settings in the Template dialog, the changes will be applied to all phones using the template, except for any fields that you may have specifically modified in either the Device Mapping dialog, or from My Extension.

Brands and Models

CompletePBX is factory-configured to support a number of IP phone brands and models. If you cannot find the brand or model that you require in the appropriate drop-down lists, you can contact Xorcom and request that we add support for the missing brand and model. Clicking on the **Request support for new model** button in the right-hand menu of the Endpoint Manager will initiate a feature request to add support for a missing device. We cannot guarantee that every request will be implemented, but we will provide a timely response to indicate how your request will be handled.

Host Settings

Settings → Endpoint Manager → Host Settings

The Host Settings dialog allows you to configure one or more sets of parameters that can be used when configuring phones. This provides Endpoint Manager with information about the environment to which the phones belong. For example, you may have one template for IP phones that reside on the same network segment as your CompletePBX 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 CompletePBX server) directly access port 5060.

Name helps to simplify maintenance: each host setting should be identified with a unique label.

Hostname/IP Address is the address of your CompletePBX server. Note that the IP address used by phones that reside on the same network as CompletePBX 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 CompletePBX, 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.



Logical Addresses

While this field can contain either a logical or physical address, you need to be careful, as some phone manufacturers only partially support the use of logical addresses. To be on the safe side, you should use full-qualified host names, such as `pbx.mydomain.com..`

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 CompletePBX 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 CompletePBX 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 CompletePBX 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 CompletePBX 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.

Press the **DNS/NTP Servers** button to open a small dialog where you can enter the addresses of DNS and NTP servers.

DNS Servers define the servers that IP phones will use for DNS resolution. The server must be written in physical notation, i.e. 192.168.0.100. Phones that are on the same network may use the DNS settings of the corporate gateway, while phones that are outside the network may use an external DNS server.

NTP Servers define the servers that IP phones will use for NTP updates.





The **Delete** icon (it looks like a trash can) allows you to delete an item from the list. Note that you must define at least one item.

Endpoint Manager

Host Settings

Host Settings allows you to define settings that can be used in templates. For example, the settings for phones that are connected to the internal company network may be different from the settings for phones that are outside the corporate firewall.

Host Addresses

Label	Hostname / IP Address	SIP Port	IAX2 Port	HTTP Port	HTTPS Port	Server Settings
External Devices 	<input type="text" value="pbx.mycompany.com"/>	<input type="text" value="6050"/>	<input type="text" value="6945"/>	<input type="text" value="8888"/>	<input type="text" value="2323"/>	<input type="button" value="DNS/NTP Servers"/> 
Internal Devices	<input type="text" value="192.168.0.138"/>	<input type="text" value="5060"/>	<input type="text" value="4569"/>	<input type="text" value="80"/>	<input type="text" value="443"/>	<input type="button" value="DNS/NTP Servers"/> 
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="DNS/NTP Servers"/> 



Note!

Do not forget to press on **Apply** button after making any changes.

Create a Template

General Settings

Settings → Endpoint Manager → Create New Template → General Settings

You need to create at least one template for every **model** of IP phone that you want to manage. If you have phone models that use different host settings, you will need to create a template for each combination of phone model/host settings. You will need to create multiple templates, for example, when you want to use a different set of host settings (for the same model phone), or when you have phone models in different timezones.

Template Name helps to simplify maintenance: each template should be identified with a unique name.

Select a **Brand** from the dropdown list of brands that are supported by Endpoint Manager. If you require a brand that does not appear in the dropdown list, you can contact support, by clicking on the **Add new model support** menu (on the right-hand side of the dialog).

Select a **Model** from the dropdown list of models that are supported by Endpoint Manager. If you require a model that does not appear in the dropdown list, you can contact support, by clicking on the **Add new model support** menu (on the right-hand side of the dialog).

Configuration Layout 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.

Timezone allows you to select the timezone 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.

Endpoint Manager - Template

General Settings	Device Buttons	Expansion Modules	Advanced Settings
Template Name	<input type="text" value="Telemarketing"/>		
Brand	<input type="text" value="Xorcom"/>		
Model	<input type="text" value="XP0120P"/>		
Configuration Layout	<input type="text" value="Generic"/>		
Host Setting	<input type="text" value="Internal Devices"/>		
Timezone	<input type="text" value="-5:00 Bahamas(Nassau)"/>		
Administrator Password	<input type="text" value="admin"/>		
<input type="button" value="Apply"/>			

**Note!**

Do not forget to press on **Apply** after making any changes.

Device Buttons

Settings → Endpoint Manager → Create New Template → Device Buttons

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

Device Buttons & Type



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

Endpoint Manager - Template

General Settings

Device Buttons

Expansion Modules

Advanced Settings

Note: Some of the options listed below may not be relevant for certain devices.

DSS Buttons

	Label	Type	Value	Line
Button 1	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text" value="v"/>
Button 2	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text" value="v"/>
Button 3	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text" value="v"/>
Button 4	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text" value="v"/>
Button 5	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text" value="v"/>
Button 6	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text" value="v"/>

Apply



Note!

Do not forget to press on **Apply** after making any changes.

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.

Expansion Modules

Settings → Endpoint Manager → Create New Template → Expansion Modules

Allows you to configure the DSS (direct station select) buttons on the expansion module for IP phones that have this hardware and use this template.

Note that each user can use My Extensions to define settings and overwrite the template definitions. This is a useful feature to allow users to personalize some buttons on their phone.

The number of buttons that are displayed are specific to each expansion module.



Note!

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

Endpoint Manager - Template

General Settings
Device Buttons
Expansion Modules
Advanced Settings

Select module to attach

Attached modules:

XP0020

Note: Some of the options listed below may not be relevant for certain devices.

	Label	Type	Value	Line
Button 1	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text" value="v"/>
Button 2	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text" value="v"/>
Button 3	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text" value="v"/>
Button 4	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text" value="v"/>
Button 5	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text" value="v"/>



Note!

Do not forget to press on **Apply** after making any changes.

Advanced Settings

Settings → Endpoint Manager → Create New Template → Advanced Settings

Advanced Settings allows you to manage the configuration file for phones that belong to this template. Advanced Settings provides access to parameters that are not directly managed by the Endpoint Manager. Codec settings would be an example of such a parameter. Manufacturers' default values, where applicable, are already defined in the file. You would only need to modify values in the configuration file if you want to define some non-standard behavior.

Device Mapping

Settings → Endpoint Manager → Device Mapping

This dialog manages your devices. The devices that you want to manage can be automatically discovered. Type in a target network segment and mask, such as 192.168.0.0/24, and click on **Scan subnet for devices**. The discovery will take some time, depending on the number of addresses that can potentially exist on the subnet. Be careful not to use a mask that is too big, as this will impact the time required to complete the discovery process. If devices cannot be discovered by scanning the network, you can manually enter the MAC address of any phones that you want to manage.

Checking on **Only show recognized devices** will filter out any devices having a MAC address that is not defined in the Endpoint Manager database as an endpoint device.

Deleting an Assigned Device



If you delete an assigned device (by clicking on the trash button at the right-hand end of the line), the device will be removed from the list of assigned devices. Of course, it can be rediscovered next time you scan the subnet for devices. If you delete a device, all the settings on the phone will remain on the phone from the last time that the phone was provisioned, but the phone settings will no longer be updated.

Unassigned Devices

Scan subnet for devices:

192.168.0.0/20

 Only show recognized devices

Note: This operation may take a long time.

MAC Address	IP Address	Brand	Model	Template	Extensions
00:15:65:11:ac:8e	192.168.0.185	Yealink			
00:15:65:1b:3a:0f	192.168.0.244	Yealink			
00:15:65:1b:3a:1b	192.168.0.250	Yealink			
00:15:65:1b:3b:1f	192.168.0.222	Yealink			
00:15:65:3c:f3:ee	192.168.6.3	Yealink			
64:24:00:00:02:6b	192.168.5.172	Xorcom			
64:24:00:00:02:8b	192.168.5.171	Xorcom			
64:24:00:00:03:55	192.168.5.173	Xorcom			
64:24:00:00:03:f9	192.168.5.170	Xorcom			
64:24:00:00:04:11	192.168.5.174	Xorcom			

After completing a scan, or manually adding a device, you will need to define additional parameters for each phone:

Brand from the drop-down list of known brands

Model from the drop-down list of models that are factory-defined

Template that this phone should use

Extension, or extensions, that should be linked to this phone. A phone can host one, or more, extensions.

Assigned Devices

MAC Address	IP Address	Brand	Model	Template	Extensions
<input type="checkbox"/> 64:24:00:00:02:8b-		Xorcom	XP0120P	Telemark	2012 - Sal 2013 - Sal 2002 - VP

Reboot Selected Devices



Selecting Brand and Model

Make sure that you make the correct choices when you chose the brand and model. If the brand and/or model are not correct, the configuration information sent to the phone will not be correct and the phone may not work as expected.



Note!

Do not forget to press on **Apply** after making any changes.

Summary

In this chapter, we learned how to create users and endpoints in either Extensions or DeviceAndUser mode. We also discussed the distinctions between devices and users when CompletePBX is run in the DeviceAndUser mode, as well as use of the Endpoint Manager.

After this chapter, we should have a CompletePBX system configured with user accounts and device options that are appropriate for our network. We also learned how to create a voicemail box for each user, and how to manage voicemail boxes using both the CompletePBX messaging center and **My Extension**. Each user account on our PBX should now have a voicemail box and be listed in the directory.

In the next chapter, we will learn how to connect our PBX with the outside world or other PBX servers using trunks.

3. Trunks

Connectivity → Trunks

In the simplest of terms, a trunk is a pathway into or out of a telephone system. A trunk connects CompletePBX 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. In this chapter, we will discuss:

- Various types of trunks allowed by CompletePBX
- Methods for setting up each type of trunk
- Checking the status of any configured trunk

Trunk Types

Connectivity → Trunks

CompletePBX allows the creation of six different types of trunks as follows:

- DAHDI
- IAX2
- SIP
- ENUM
- DUNDi
- Custom

DAHDI, IAX2, and SIP trunks utilize the technologies of their namesakes. These trunks have the same highlights and pitfalls that extensions and devices using the same technology do. DAHDI 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 adoption mainly to Asterisk-based systems.

In terms of VoIP, **ENUM (E.164 NUmber Mapping)** is a method for unifying E.164 (the international telecommunication numbering plan) with VoIP routing. The ENUM system can be considered very similar to the way that the Internet DNS system works. In the DNS system, when a domain name is looked up an IP address is returned. The IP address allows a PC to traverse the Internet and find the server that belongs to that IP address. The ENUM system provides VoIP routes back when queried for a phone number. The route that is returned is usually a SIP or IAX2 route.

An ENUM trunk allows CompletePBX to send the dialed phone number to the public *e164.org* ENUM server. If the called party has listed their phone number in the *e164.org* directory, a VoIP route will be returned and the call will be connected using that route. A VoIP route contains the VoIP protocol, the server name or IP address, the port, and the extension to use in order to contact the dialed phone number.

For example, a SIP route for dialing the number 555-555-1234 might appear as SIP:1234@pbx.example.com:5060. This is advantageous in several ways. It is important to note that indirect routes to another telephony system are often costly. Calling a PSTN telephone number typically requires that call to route through a third-party provider's phone lines and switching equipment (a service they will happily charge for). If a number is listed in the ENUM directory, the returned route will bridge the call directly to the called party (or their provider), bypassing the cost of routing through a third party.

ENUM also benefits the called party, allowing them to redirect inbound calls to wherever they would like. Service disruptions that would otherwise render a particular phone number useless can be bypassed by directing the phone number to a different VoIP route in the ENUM system.

More information on ENUM can be found at the following Web sites:

- The ENUM home page: <http://www.enum.org/>
- The e164.org home page: <http://www.e164.org/>
- The Internet Engineering Task Force ENUM charter:
- <http://www.ietf.org/html.charters/enum-charter.html>

DUNDi (Distributed Universal Number Discovery) is a routing protocol technology similar to ENUM. In order to query another CompletePBX or CompletePBX system using DUNDi, that system must be "peered" with your own CompletePBX system. Peering requires generating and exchanging key files with the other peer.

DUNDi is a decentralized way of accomplishing ENUM-style lookups. By peering with one system you are effectively peering with any other system that your peer is connected to. If system A peers with system B, and system B peers with system C, then system C will be able to see the routes provided by system A. In peer-to-peer fashion, system B will simply pass the request along to system A, even though system C has no direct connection to system A.

DUNDi is not limited to E.164 numbering schemes like ENUM and it allows a PBX to advertise individual extensions, or route patterns, instead of whole phone numbers. Therefore, it is a good candidate for distributed office setups, where a central PBX can be peered with several satellite PBX systems. The extensions on each system will be able to call one another directly without having to statically set up routes on each individual PBX.

More information on DUNDi can be found at the following Web sites:

- DUNDi home page: <http://www.dundi.com/>
- Example of DUNDi SIP configuration can be found at:
<http://www.voip-info.org/wiki/view/DUNDi+Enterprise+Configuration+SIP>
- Example of DUNDi IAX2 configuration can be found at:
<http://dundiglobal.org/documentation/tying-two-pbxes-together-using-dundi-and-iax2>

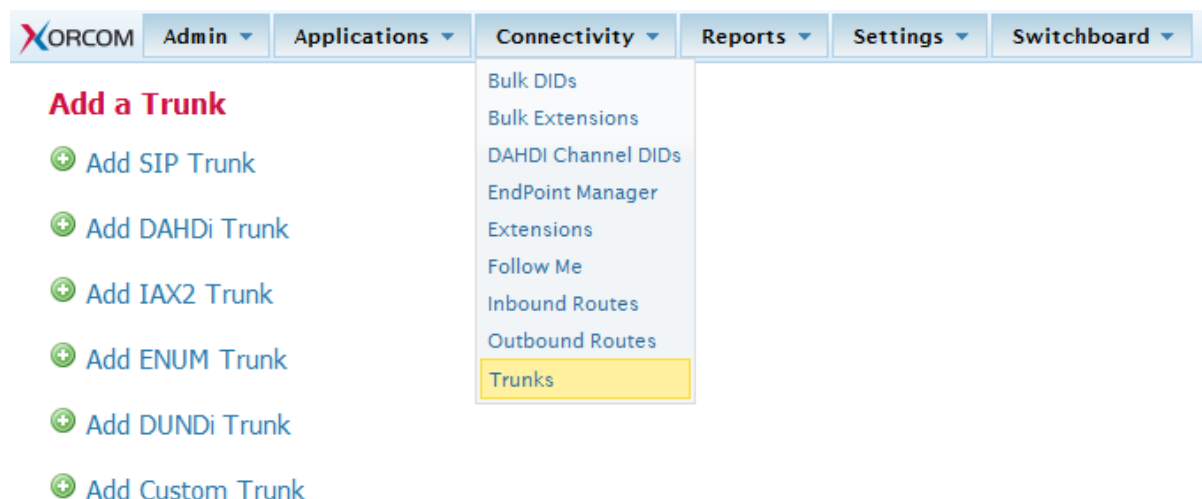
Custom trunks work in the same fashion as custom extensions do. Any valid CompletePBX *Dial* command can be used as a custom trunk by CompletePBX. Custom trunks typically use additional VoIP protocols such as H.323 and MGCP.

Configuring a Trunk

Connectivity → Trunks

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

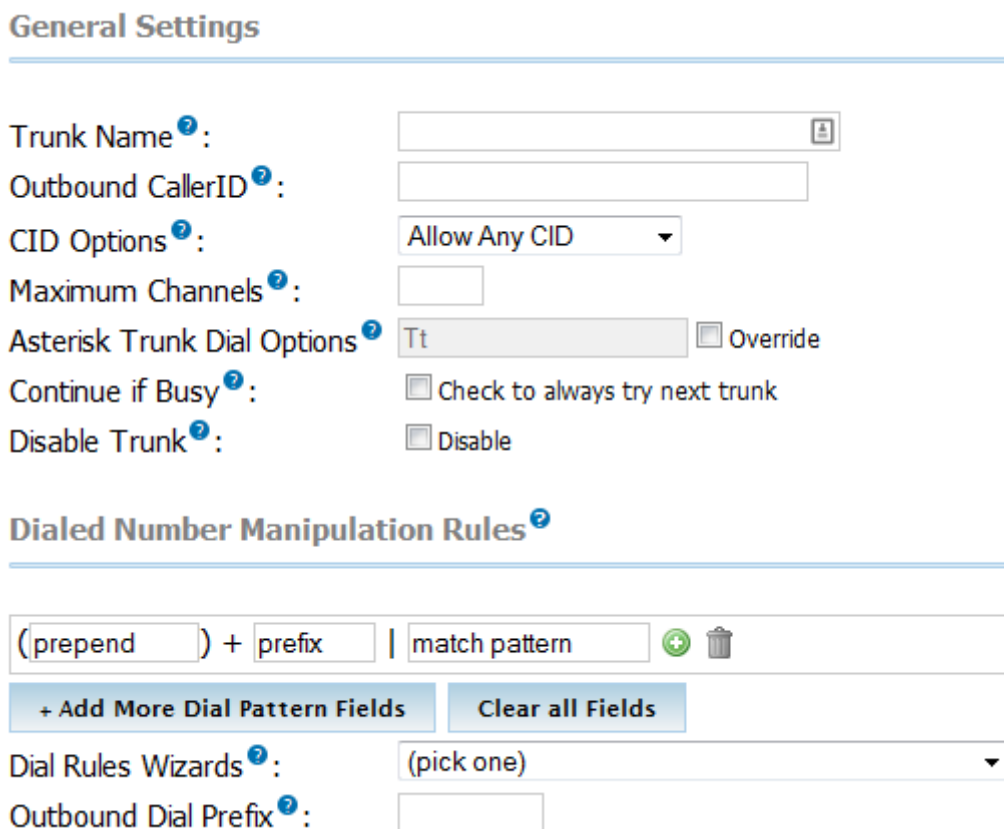
In order to begin setting up a trunk, navigate to the **Connectivity** menu and select the **Trunks** dialog:



From the **Add a Trunk** screen, click on the name of the technology that the trunk will be using (for example, if a SIP trunk will be used, click on **Add SIP Trunk**).

Common Trunk Fields

No matter which technology a trunk will be used, the same common fields will appear first on the configuration page as shown in the following screenshot:



Outbound Caller ID sets the caller ID name and number that will be displayed to the called party. Caller ID should be in the format of "Name" <#####>, where "Name" is the name that will be displayed, and <#####> will be the telephone number displayed. Be sure to include the quotes and angle brackets to send both name and number information. In order to send just a telephone number without a name, simply put the telephone number in the **Outbound Caller ID** field without quotes or angle brackets. Note that setting 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.

Outbound Caller ID



CompletePBX will ignore the Outbound Caller ID field if it is not in the proper format. Be sure that a caller ID with a name and number contains a name in quotes and a telephone number in angle brackets. A caller ID with just a telephone number must only contain the number and nothing else. CompletePBX will not set the caller ID on outbound calls that do not match one of these two formats

Maximum Channels is the maximum number of *outbound* calls that this trunk can support. Note that CompletePBX does not count inbound calls against the channel limit. Whole numbers greater than one are the only valid values for this field. Leave this field blank if you do not want to set a limit.

The **Disable Trunk** checkbox allows a trunk to be temporarily disabled in any outbound route where the trunk is in use. If a trunk is experiencing difficulties, it can be disabled here in order to have outbound calls skip the trunk entirely in their routing sequence. Under normal circumstances, a downed trunk will simply refuse a call, but in scenarios in which a trunk accepts a call but fails to connect it properly, this option is especially useful. Without disabling the trunk in this scenario, all of the calls will be dropped. Disabling the trunk allows outbound calls to bypass the problematic trunk while it is repaired, instead of having to remove the trunk entirely and recreate it when the problem is resolved.

The **Monitor Trunk Failures** field allows an AGI script to be called when a trunk fails. CompletePBX determines that a trunk has failed when calls cannot be completed and the returned status from CompletePBX is *not* *BUSY*, *NOANSWER*, or *CANCEL*. Scripts specified in this field can perform any action that can be scripted, including reloading CompletePBX configuration to force trunk re-registration, or notifying a system administrator of the failure through email. Failure scripts must be located in the `/var/lib/asterisk/agi-bin` directory. The full name of the failure script should be specified.

Dialed Number Manipulation Rules allow dialed numbers to be manipulated before they are passed to the trunk. Dialed numbers are altered based on the patterns entered into this field. There should only be one pattern per line. Only the first matched rule will be acted upon (other patterns will be ignored, even if they match). Patterns are matched based upon the order they are listed in, that is, from top to bottom. Patterns can consist of the following items:

Pattern	Description
X	Any whole number from 0-9

Pattern	Description
Z	Any whole number from 1-9
N	Any whole number from 2-9
[#]	Any whole number or letter in brackets. Note that multiple numbers can be separated by commas, and a range of numbers can be specified with a dash, so [1,3,6-8] would match the numbers 1, 3, 6, 7, and 8
.	Matches one or more characters (acts as a wildcard)
	Removes a prefix from the dialed number (555 1234567 would take 5551234567 and pass 1234567 to the trunk)
+	Add a prefix to the dialed number (555+1234567 would take 1234567 and pass 5551234567 to the trunk)

Note that wildcards are not valid before a "+" or "/". Also, "+" and "|" can be used in the same pattern (0|01+15551234567 would take 015551234567 and pass 0115551234567 to the trunk). Dial rules are very useful for allowing users to continue dialing numbers the way they are accustomed to, even if the provider is expecting them to be delivered in a different way.

A few real-world examples of dial pattern usage are given below:

Scenario	Dial Pattern(s)
Users are used to dialing 9 to access an outside line. A CompletePBX system replaces their existing PBX, but should accommodate this dialing pattern instead of forcing users to learn a new one. The provider is expecting all of the numbers to be sent in standard North American 10 digit format	9 1+NXXNXXXXXX 9 1NXXNXXXXXX
The provider requires an account code to be sent in front of all of the dialed calls (in this example, the account code is 654321). Calls must be sent in standard North American 10 digit format	5432101+NXXNXXXXXX 543210+1NXXNXXXXXX
The provider requires all of the numbers to be sent in standard North American 10 digit format except for toll free calls. Toll free calls should never send the leading 1. In this example, note the order that items are listed in. If the last item were listed first and a user were to dial 800-555-1234, a 1 would be appended and sent to the provider, and the call would fail.	1 888NXXXXXX 1 866 NXXXXXX 1 877 NXXXXXX 1 800 NXXXXXX 1+NXXNXXXXXX

Dial Rules Wizards are pre-constructed dial patterns for use in the **Dial Rules** field. Selecting the name of one of the pre-made patterns will populate the **Dialed Number Manipulation Rules** box with the appropriate pattern.

Outbound Dial Prefix can be used in order to add a prefix to every call dialed through this trunk. This option can be useful if accessing an outside line requires dialing an extra number (usually 9). This option can also be useful for certain DAHDI cards that are slow to pick up the line and therefore, start dialing before the line is listening for the digits. Adding a "w" as the outbound dial prefix will cause the system to wait for 50 milliseconds before dialing (multiple "w" characters can be strung together to create a longer wait). Anything that is valid in a CompletePBX dial string command can be entered into this field.

DAHDI Trunks

Beyond the common trunk fields, DAHDI trunks only have one additional field to fill in as shown in the following screenshot:

Outgoing Settings

DAHDI Identifier [?]:

Submit Changes

Duplicate Trunk

DAHDI Identifier should match the group or the channel number that is set up for this DAHDI trunk in the `/etc/asterisk/dahdi-channels.conf` file. `dahdi-channels.conf` will have a section like the ones below for each DAHDI channel that is present in the system:

```
context=from-zaptel
group=0
signalling=fxs_ks
channel => 1
context=from-zaptel
group=0
signalling = fxs_ks
channel => 2
```

Entering a value of **1** in the **DAHDI Identifier** field will use channel 1 for this trunk.

There are various ways to define the channel groups for trunks: gN, GN, rN, RN where N is a channel group number. The group number prefix (g, G, r, or R) has the following meaning:

Identifier	Usage
g	Select the lowest-numbered available channel. Can be referred to as ascending sequential hunt group
G	Select the highest-numbered available channel. Can be referred to as descending sequential hunt group

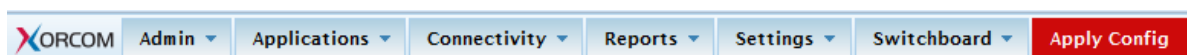
Identifier	Usage
r	Use a round-robin search, starting at the next highest available channel after the channel that was used last time. Can be referred to as ascending rotary hunt group
R	Use a round-robin search, starting at the next lowest available channel after the channel that was used last time. 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 this 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.

For example, if you have defined channel group 2 as containing channels 1, 2, 5 and 8, and the last round-robin search for this group (group 2) began searching from channel 5, this is the order of searching that the Zap channel module will use for the four possible selection methods:

- g2 will search in order 1, 2, 3, 4, 5, 3
- G2 will search in order 24,23, 22, 21, 20, 22
- r2 will search in order 1, 2, 3, 4, 5, 6, 7, 8
- R2 will search in order 24, 23, 22, 21, 20, 19, 18,

When all of the required values have been entered, click on the **Submit** button to write the changes to the database. As with all of the changes, click the red-colored **Apply Config** bar to load the new configuration changes into memory.



SIP Trunks

An example of a SIP trunk is shown in the screenshot below.

Trunk Name [?] :	MyITSP
PEER Details [?] :	<pre>host=myitsp.cc defaultuser=4003 remotesecret=x4003x type=friend outboundproxy=127.0.0.1:6075,force trustpid=yes qualify=no context=from-trunk insecure=invite</pre>

Registration	
Register String [?] :	MyITSP?4003:x4003x@myitsp.cc/4003

The above screenshot is applicable when CompleteSBC has been enabled. You must add a line to the Peer Details of the Outgoing Settings, **outboundproxy=127.0.0.1:6075,force**, since all outbound calls must be relayed to the CompleteSBC. This line is not required when CompleteSBC is not enabled.

Trunk Name that appears in the Outgoing Settings is important. Be careful not to include any special characters for this field: use only normal printing characters (a-z), number characters, or underscore.

PEER Details are the outbound configuration details that CompletePBX will insert into *sip_additional.conf*. These details will vary widely from trunk to trunk, and should be supplied by the trunk provider. By default, CompletePBX populates this field with the most commonly required values.

In the **PEER Details**, **host** is the IP address or DNS hostname of the provider. This is the destination server or network that CompleteSBC (or CompletePBX) will send calls to when using this trunk. The **defaultuser** and **remotesecret** lines are for the credentials used to authenticate this trunk against the provider. You should use **remotesecret** for outbound authentication, and **secret** for authenticating inbound requests. Note that if no **remotesecret** is supplied for an outbound registration or call, the secret will be used.

SIP entities have one of three types which determines their roles within CompletePBX. Make sure that you understand how CompletePBX matches incoming calls.

1. CompletePBX checks the SIP header and matches against names of devices with **type=user**. The name is the text between square brackets [name]
2. CompletePBX checks the From: address and matches the list of devices with a **type=peer**
3. CompletePBX checks the IP address (and port number) from which the INVITE was sent, and matches against any devices with **type=peer**

- **Peer**
Peers handle both inbound and outbound calls and are matched by IP address/port, so for incoming calls from the peer, the IP address must match in order for the invitation to work. This means calls made from either direction won't work if the peer is not registered while host=dynamic or if the host is otherwise not set to the correct IP of the sender.
- **User**
CompletePBX users handle *inbound* calls only, meaning that they can call CompletePBX but CompletePBX cannot call them, and are matched by their authorization information (authname and secret). CompletePBX does not rely on their IP address and will accept calls regardless of the host setting as long as the incoming SIP invite authorizes successfully.
- **Friend**
CompletePBX will create the entity as both a **friend** and a **peer**. CompletePBX will accept calls from friends as it would for users, requiring only that the **authorization** matches rather than the **IP address**. Since it is also a peer, a friend can also be called as long as its IP address is known to CompletePBX. In the case of host=dynamic, this means it is necessary for the entity to register before CompletePBX can call it.

Note that in most cases It is not necessary to configure Incoming Settings.

The **USER Context** field is the telephone number, account number, or account name that your provider is sending inbound calls to. Some providers will simply send a call to the registered IP address, in which case this field is not required.

The **USER Details** field is for the inbound configuration details. As with the **PEER Details** field, these details can vary widely, but should be supplied by the trunk provider.

In the **USER Details** field, the **secret** line is the **password** that the provider will use to authenticate incoming calls against. The **type** line should almost always be set to **user**, as this designates that this set of details is for a peer that CompletePBX is receiving calls from (not sending calls to). The **context** line indicates the context that inbound calls from this trunk should be sent to. Unless you have defined custom contexts, leave this field set to **from-trunk** to allow CompletePBX to process the calls.

Order is important



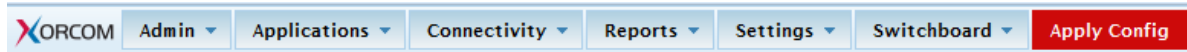
The order in which the codec handling is specified for **PEER Details** and **USER Details** fields is important. Details are read from top to bottom. If a parameter appears twice or if conflicting parameters are defined, the second instance will be used and the first will be ignored.

For example, If **allow=ulaw** is followed by **disallow=all**, all of the codecs will be denied and the **allow=ulaw** statement will be ignored. Pay close attention to how these parameters are ordered. It can often save hours of troubleshooting later on when a trunk seems to be refusing calls for no reason at all

The value in the **Register String** field will determine how CompletePBX to attempt to register with the trunk provider. Registration lets the provider know where to send calls when they arrive for your telephone number. The register string should be constructed in the format of [trunkname]?[username]:[password]@[voipserver]/[user]. You should be aware that when using CompleteSBC, you will need to prefix the registration string with the trunk name to ensure that the session border controller passes the registration string to your trunk provider. The trunk name should be followed by the ? separator as shown in the screen grab above. If a registration string is not provided, then the trunk provider must be configured to send calls to a specific IP address, and the IP address of your trunk provider server must be fixed.

If you have one-way audio, you probably have NAT problems. If your CompleteSBC (or CompletePBX) is on a public IP, and the phone is inside of a NAT device then you will need to configure NAT option for those phones, as well as turning on qualify=yes to keep the NAT session open

Once the changes have been saved, click on the red-colored **Apply Config** bar at the top of the screen.



IAX2 Trunks

An example of a IAX trunk is shown in the screenshot below.

Outgoing Settings

Trunk Name [?]:

PEER Details [?]:

```
type=friend
host=68.198.17.52
context=extens-and-ringgroups
disallow=all
allow=gsm
```

Incoming Settings

USER Context [?]:

USER Details [?]:

Registration

Register String [?]:

Trunk Name is a "friendly" name. This value is not parsed by CompletePBX in any way; it is simply used to refer to the trunk in other parts of the CompletePBX interface. Be careful not to include any special characters for this field: use only normal printing characters (a-z), number characters, or underscore.

PEER Details are the outbound configuration details that would normally be placed into *iax_additional.conf*. These details will vary widely from trunk to trunk, and should be supplied by the

trunk provider. By default, CompletePBX populates this field with the most commonly required values.

In the **PEER Details** field, **host** is the IP address or DNS hostname of the provider. This is the destination server or network that CompletePBX will send calls to when they use this trunk. The **username** and **secret** lines are for the credentials used to authenticate this trunk against the provider. The **type** line should almost always be set to **peer**, as this designates that this set of details is for a destination that CompletePBX is sending calls to (not receiving calls from).

The **USER Context** field is the telephone number, account number, or account name that your provider is sending inbound calls to. Some providers will simply send a call to the registered IP address, in which case this field is not required.

The **USER Details** field is for the inbound configuration details. As with the **PEER Details** field, these details can vary widely, but should be supplied by your trunk provider.

In the **USER Details** field, the **secret** line is the **password** that the provider will use to authenticate incoming calls against. The **type** line should almost always be set to **user**, as this designates that this set of details is for a peer that CompletePBX is receiving calls from (not sending calls to). The **context** line indicates the context that inbound calls from this trunk should be sent to. Unless you have defined custom contexts, leave this field set to **from-trunk** to allow CompletePBX to process the calls.

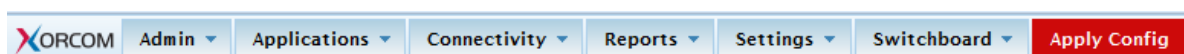
Order is important



The order in which the parameters are specified for the **PEER Details** and **USER Details** fields is important. Details are read from top to bottom. If a parameter appears twice or if conflicting parameters are defined, the second instance will be used and the first will be ignored.

For example, If **allow=ulaw** is followed by **disallow=all**, all of the codecs will be denied and the **allow=ulaw** statement will be ignored. Pay close attention to how these parameters are ordered. It can often save hours of troubleshooting later on when a trunk seems to be refusing calls for no reason at all

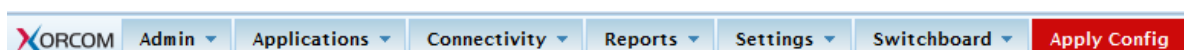
Once the changes have been saved, click on the red-colored **Apply Config** bar at the top of the screen.



ENUM Trunks

ENUM trunks require no additional configuration beyond the common configuration fields. The only item worth noting for ENUM trunks is that all of the calls are queried against the *e164.org* database. *e164.org* expects calls to be in the format of [CountryCode][PhoneNumber], so adjust dial patterns appropriately for your location.

Once the changes have been saved, click on the red-colored **Apply Config** bar at the top of the screen.



Custom Trunks

Custom trunks are very similar to custom extensions and devices. There is only one additional field for setting up custom trunks as shown in the following screenshot:

Outgoing Settings

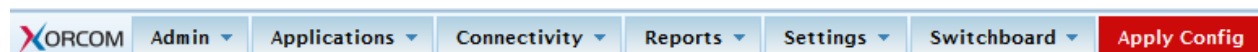
Custom Dial String [?]:

Submit Changes

Duplicate Trunk

The **Custom Dial String** can be any valid dial command that would normally be used in the CompletePBX dialplan, with one notable exception: the called number is inserted into the dial string using the `$OUTNUM$` variable. For example, the string to call an H.323 device at IP address 192.168.1.2 might be `H323/192.168.1.2/$OUTNUM$`.

As with any changes made to CompletePBX, make sure to click on the **Submit Changes** button, followed by the red-colored **Apply Config** bar at the top of the screen to save and reload all of the settings.



Common Trunk Configuration Settings

The trunk configuration settings for common VoIP providers are as follows. Simply replace the required information tokens in the following configurations with their appropriate values to configure a fully working trunk.

Required information tokens that may be used are listed as follows:

Token	Replace with
(Name)	The name of the owner of the trunk. This might be a company's name or a person's name. Letters, numbers, and spaces are allowed. No other special characters may be used.
(TelNumber)	The telephone number associated with the trunk that is being configured. For PSTN trunks, this will be a number in the format of the local calling area (for example, nine digits for North America). Trunks to other VoIP providers may have different formats. For example, the Free World Dialup (FWD) network uses six-digit telephone numbers.

Token	Replace with
(Username)	The username or user ID assigned by the VoIP provider. This is usually a numeric user ID.
(Password)	The password or "secret" assigned by the VoIP provider.
(MaxChannels)	The maximum number of active channels that the provider can support. Some providers have a set limit (in which case that limit will be listed). Some providers allow the purchase of additional channels for which a monthly fee is charged (in this case, the (MaxChannels) token is used).
(FailureScript)	The script that is used to monitor trunk failures, if one exists.
(VoIPHost)	The SIP or IAX2 server supplied by the provider. This might be referred to as the "registration server" or simply the "host" by the provider.

Summary

By now we should have a CompletePBX system with some fully-functional trunks configured. We should be able to configure a new trunk of any type, and be able to check the status of our trunks using the CompletePBX command line interface (CompletePBX CLI), if necessary. We should also have a good idea about how to monitor the health of each trunk, and how to alert an administrator on failure.

Now that we have operational trunks, the next chapter will walk through setting up various call targets so that incoming calls coming in through our brand new trunks have somewhere to go.

4. Basic Call Targets

A call target in CompletePBX is any kind of destination for a phone call that enters the system. A target might be a voice-response menu that prompts the caller to press various digits to route their call, a ring group to call a number of endpoints, or virtually any other type of processor to route the call in whatever way is desired. A call may have several targets throughout its lifespan.

The following list shows some of the types of call targets that are available in CompletePBX:

- Terminate Call
- Extension
- Voicemail
- Ring Groups
- Conferences
- Phonebook Directory
- Queues
- Time Conditions
- IVR (Digital Receptionist)
- Custom Destinations
- Fax Recipient
- Follow Me
- Misc Destinations
- Paging & Intercom
- Queue Priorities
- Trunks
- Announcements
- Call Flow Control
- Call Recording
- Callback
- DISA
- Language
- Misc Destinations
- Queue Priorities
- Voicemail Blasting

This chapter will cover the first five targets (the "basic" call targets) of the above list. The more advanced call targets will be covered in the next chapter. Basic call targets generally have a single, easy-to-configure function, whereas advanced call targets tend to have several functions and are more complicated to configure.

Chapters 4 and 5 deal with understanding and configuring the different types of call targets. These call targets are put to use through the configuration of inbound routes and users' follow-me settings. Once all the required call targets have been configured, please see Chapter 6, **Call Routing** for information on routing inbound calls to the new call targets.

Terminating Calls

CompletePBX provides several clever ways to terminate calls. We may wish to terminate a call because the calling number is a known telemarketer, or perhaps the caller has attempted to reach an invalid extension too many times. Whichever the case, the following options are available for the **Terminate Call** target:

- **Hangup:** Terminates the call immediately without any further call processing or signaling.
- **Congestion:** Sends a signal indicating that there are no channels available to complete the call before terminating it. This is used only for digital channels (such as SIP, IAX, or PRI). Some providers will use this signal to locate an alternate route or process the call in another way.
- **Busy:** Relays a busy tone to the caller. The call terminates when the calling party hangs up (CompletePBX will play a busy tone indefinitely).
- **Play SIT Tone:** Plays a SIT (**S**pecial **I**nformational **T**one) to the calling party. A special informational tone consists of two short tones and one long tone. It is designed to indicate that the called number is not in service. SIT tones are recognized by a large portion of automated dialing equipment, so this tone is often useful for playback to known telemarketing numbers. Automated dialers who understand this tone will usually remove the called number from their dialing lists. Once the intercept tone is played, the call will be terminated immediately.
- **Put caller on hold forever:** Places the calling party on hold until they terminate the call themselves.
- **Play ringtones to caller until they hangup:** Continually plays back a ringing tone to the calling party until they terminate the call themselves.

Be aware of indefinite termination options!

The **Busy**, **Put caller on hold forever**, and **Play ringtones to caller until they hangup** options open up the possibility of a call never terminating until the PBX or the calling party loses connectivity and the call is dropped.



This could possibly mean a call that lasts for weeks. With VoIP providers charging by the minute, such calls can get expensive! The latter two options are typically used to annoy unwanted callers.

Indefinite ringtones or hold music are relatively safe for these kinds of calls as the caller will terminate the call themselves when they do not receive a human on the other end of the line.

Nevertheless, be aware of the activity on your PBX to avoid being billed for a week-long session of hold music. When in doubt, terminate the call rather than opting to leave it on hold indefinitely.

Extensions and Voicemail

Connectivity → *Extensions* or *Connectivity* → *Users*

The **Extension** target will route calls directly to a particular extension. The only option available for the Extension target is to which extension to send a call.

If CompletePBX is in Extensions mode, an extension must have been previously created for this target to be available. If CompletePBX is in DeviceAndUser mode, a user must have been previously created for this target to be available.







The **Voicemail** target will route calls directly to an extension's voicemail box without ringing the extension first. The Voicemail target provides options of selection such as **busy**, **unavail**, or **no-msg**. These options control the outgoing message that will be played prior to playing the standard instructional message asking the caller to leave a message. If the selected message does not exist, a standard message stating that the person at the called extension is either on the phone or unavailable will be played. For the voicemail target to be available, the **Voicemail & Directory** option must be enabled when setting up an extension or user.

Ring Groups


Applications → Ring Groups

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. To set up a ring group, navigate to the **Applications** menu and select the **Ring Groups** dialog. The **Add Ring Group** screen will be displayed as shown in the next screenshot:

Add Ring Group

Ring-Group Number: [?]
 Group Description: [?]
 Ring Strategy: [?] 
 Ring Time (max 300 sec) [?]
 Extension List: [?]
 Extension Quick Pick [?] 
 Announcement: [?] 
 Play Music On Hold? [?] 
 CID Name Prefix: [?]
 Alert Info [?]:
 Ignore CF Settings [?]:
 Skip Busy Agent [?]:
 Enable Call Pickup [?]:
 Confirm Calls [?]:
 Remote Announce: [?] 
 Too-Late Announce: [?] 


Change External CID Configuration

Mode: [?] 
 Fixed CID Value: [?]

Call Recording

Record Calls [?]

Destination if no answer:



Each field or dropdown should be configured to ensure the ring group behaves in the desired manner.

The **Ring-Group Number** is a number that can be dialed from internal endpoints to access this ring

group. Users can either dial this number directly, or transfer a caller they have on the line to this number. The Ring-Group Number can be thought of as the extension number of the ring group.

The **Group Description** field is just used to identify this ring group when selecting it as a call target. The contents of this field are not visible to callers in any way.

The **Ring Strategy** dropdown defines the way in which the endpoints in this ring group will be rung. Endpoints can be rung using the following methods:

- **ringall**: Ring all group members listed in the Extension List field at the same time.
- **ringall-prim**: If the first extension listed in the Extension List is not in use, all group members will be rung at the same time. If the first extension is in use or is in the do-not- disturb mode, none of the extensions will be rung and the call will immediately fail over to the target selected in the **Destination if no answer** section.
- **hunt**: Ring each group member one at a time in the order that they are listed in the Extension List field.
- **hunt-prim**: Functions similar to the ringall-prim method. If the first extension is in use, no group members will be rung. Otherwise, each extension is rung in the same fashion as in the hunt method.
- **memoryhunt**: Rings the first extension listed in the Extension List field, then rings the first and second extensions listed in the Extension List field, then rings the first, second, and third extensions listed in the Extension List field (and so on until all extensions are ringing or a timeout is reached).
- **memoryhunt-prim**: If the first extension is in use no group members will be rung. Otherwise, each extension is rung in the same fashion as in the **memoryhunt** method.
- **firstavailable**: Rings the first extension in the Extension List that is available to ring. If an extension has call waiting enabled, it will be considered "available", even if it is already on a call.
- **firstnotonphone**: Rings the first extension in the Extension List that is completely unoccupied. Call waiting settings are not taken into account. If an extension is already on a call, it will not be rung whether or not call waiting is enabled.

The **Ring Time (max 300 sec)** field is for defining the number of seconds that the ring group will be rung before failing over to the **Destination if no answer** field. For the hunt type of strategies, the ring time is applied to each stage of the hunt sequence.

For example, if the Ring Time (max 300 sec) field is set to "30" and the Ring Strategy field is set to "memoryhunt", the first extension in the Extension List will be rung for 30 seconds. Following this, the first and second extensions will be rung for 30 seconds, then the first, second, and third extensions will be rung for 30 seconds, and so on until the end of the Extension List is reached.

Extension List contains a list of all extensions to ring. Extensions should be listed one per line. Available internal extensions can also be selected from the **Extension Quick Pick** dropdown to insert them into the Extension List. Any extension listed here will be rung directly and Follow Me Settings will not apply. To force the ring group to respect Follow Me Settings, append the pound (#) symbol to the extension number (for example, 5001#).

External phone numbers or extensions can be added to a ring group by suffixing them with a pound symbol as well (for example, 11234567890# would dial 1-123-456-7890 whenever the ring group is called). As long as a trunk exists to route the number, it will be dialed as part of the ring group. Note that external numbers will take longer to connect, so ring groups that include them are likely to have longer ring times.

The pound symbol is also used to include internal resources that are not extensions to the group. In this fashion, it is possible to ring other ring groups or queues simply by adding their number to the Extension List and suffixing it with a pound.

The message selected in the **Announcement** dropdown will be played to the caller entering the ring group prior to any extensions being rung.

The music on hold category selected in the **Play Music On Hold?** dropdown will be played to the caller while the ring group members are being rung. Selecting the **Ring** option will cause the caller to hear the ringing instead.

The **CID Name Prefix** field will prefix the caller ID of all calls to this ring group with the value specified here. This is useful for the person receiving the call as they can determine if a caller is attempting to call them directly or is calling a larger group.

The **Alert Info** field is used to transmit some information in the *ALERT_INFO* SIP headers to a SIP endpoint. Some SIP endpoints can be set up to play alternate ringtones depending on the *ALERT_INFO* data they receive. If the endpoint being rung does not use SIP technology, this field is ignored for that endpoint.

When the **Ignore CF Settings** option is checked, any extension in the Extension List that has call forwarding enabled will not be rung.

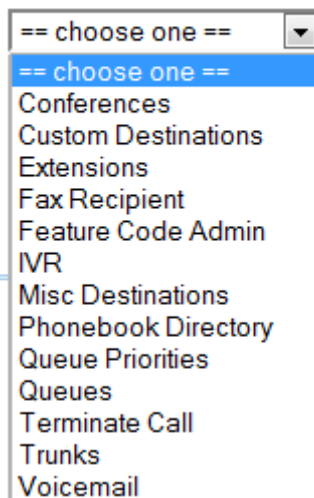
When the **Skip Busy Agent** option is checked, any extension in the Extension List that is in use will not be rung. This option will ignore call waiting settings, so multi-line or single-line phones with call waiting enabled will not be rung if they are in use at all.

The **Confirm Calls** option will prompt the person who answers the call to press *1* on their phone before the call is actually bridged to their extension. This is often useful for ring groups that contain external phone numbers in the Extension List. If one of the external phone numbers goes to voicemail, the PBX will see that the call has been "answered" and will bridge the caller to the external number even though a real person did not answer the call. If the call is not confirmed by the external party, the call will continue ringing the rest of the Extension List as normal. The Confirm Calls option will only work with the ringall ring strategy.

The **Remote Announce** and **Too-Late Announce** dropdowns are only applicable if the Confirm Calls option is enabled. The message in the Remote Announce field is played to the person who picks up the call (this should be a message asking them to press *1* to confirm the call). The message in the Too-Late Announce field is played to the person who picks up the call if someone else in the ring group picked up the call before they were able to confirm it. Default messages for these two fields do not exist and must be recorded. More information on recording custom voice prompts can be found in the [Voice Prompts](#) section of Chapter 8.

Personalizing your PBX

The **Destination if no answer** section is used when nobody in a ring group picks up the call within the designated ring time – see some of the available options in the following screenshot:

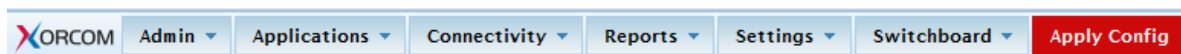
Destination if no answer:

== choose one ==

- == choose one ==
- Conferences
- Custom Destinations
- Extensions
- Fax Recipient
- Feature Code Admin
- IVR
- Misc Destinations
- Phonebook Directory
- Queue Priorities
- Queues
- Terminate Call
- Trunks
- Voicemail

The destination chosen is a normal call target. The options available in this section will vary depending on which types of targets have already been configured in CompletePBX.

Once all options have been configured, click on the **Submit Changes** button, followed by the red-colored **Apply Config** bar.



Conferences

Applications → Conferences

Conferences allow two or more calls to be joined together so that all parties on the call can hear one another. Conferences are also referred as Conference Bridges or Conference Rooms. At least one conference room must be configured before this target option is available. To configure a conference room, navigate to the **Applications** menu and select the **Conferences** dialog. A conference can be used as a destination, for example, for an inbound route or IVR.

The first section of the Add Conference screen requires a number and description for the conference room that is being created:

Add Conference

Add Conference

Conference Number: [?]	<input type="text"/>
Conference Name: [?]	<input type="text"/>
User PIN: [?]	<input type="text"/>
Admin PIN: [?]	<input type="text"/>

Conference Number is a number that internal endpoints can dial to reach this conference. Like the ring groups, this can be thought of as the extension number of the conference.

Conference Name can be used to identify the purpose of the conference room. The name is used only when selecting the room as a call target, and is not visible by the caller in any way.

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

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

The second section of the Add Conference page sets up general conference options that determine how the conference room behaves when in use:

Edit Conference

Conference Number:	<input type="text" value="9001"/>
Conference Name:	<input type="text" value="Technical Support"/>
User PIN:	<input type="text"/>
Admin PIN:	<input type="text" value="120546"/>

Conference Options

Join Message:	<input type="text" value="None"/>
Leader Wait:	<input type="text" value="Yes"/>
Talker Optimization:	<input type="text" value="No"/>
Talker Detection:	<input type="text" value="No"/>
Quiet Mode:	<input type="text" value="No"/>
User Count:	<input type="text" value="Yes"/>
User join/leave:	<input type="text" value="Yes"/>
Music on Hold:	<input type="text" value="No"/>
Music on Hold Class:	<input type="text" value="inherit"/>
Allow Menu:	<input type="text" value="Yes"/>
Record Conference:	<input type="text" value="Yes"/>
Maximum Participants:	<input type="text" value="5"/>
Mute on Join:	<input type="text" value="No"/>

Join Message is a message that will be played to anyone attempting to join the conference. The caller will hear this message before their channel is bridged into the conference room.

If the **Leader Wait** option is set to "Yes", the conference will not begin until the conference administrator joins the conference room. The administrator is identified by the Admin PIN option. 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 **Music on Hold** option explained later in this section). If this option is set to "No", the callers will be bridged into the conference as soon as they call the conference room number.

If the **Quiet Mode** option is set to "No", a tone will be played whenever a caller enters or exits the conference room.

If **User Count** option 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.

If **User join/leave** option is set to "Yes", the caller will be prompted to say their name and press the

pound (#) key before joining the conference. The existing conference room participants will hear the name of the new caller being played back before the caller is bridged into the conference room.

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

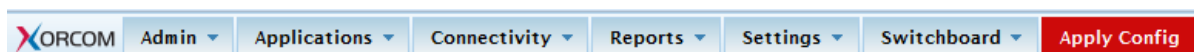
If **Allow Menu** is set to "Yes", conference participants are able to press the CompletePBX (*) key on their phones to be presented with an audio menu that only they can hear. The menu gives them the ability to mute/unmute their channel, increase/decrease their transmit volume, and increase/decrease their receive volume. If this option is set to **No**, pressing the CompletePBX key will do nothing. The available menu options and their functions are listed in the following table:

Menu Option	Action
*1	Toggles mute for the user. When enabled, anything the user says is not transmitted to the rest of conference members. If the conference is being recorded, anything said by a muted user is not part of the recording
*2	Toggles the conference lock. When a conference is locked, no more callers may join. A locked conference must be unlocked for any new users to join. This option is only available to a conference administrator. If the conference does not have an admin PIN configured or the user has joined the conference as a user instead of an admin, this option is not available
*3	Ejects the last user who joined the conference from the conference room. 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 unlocked, the user may rejoin. The best way to remove an abusive conference user is to eject them and then immediately lock the conference. This option is only available to a conference administrator. If the conference does not have an admin PIN configured, or the user has joined the conference as a user instead of as an admin, this option is not available
*4	Decreases receive volume. The user can tap this option to decrease the volume of what they are hearing. This does not affect what any other conference member hears. If a user is finding other conference members too loud, they can press 4 a few times while in the conference menu to make the conference quieter for themselves
*5	Increases receive volume. The user can tap this option to increase the volume of what they are hearing. This does not affect what any other conference member hears. If a user is having trouble hearing other members of the conference, they can press 6 a few times while in the conference menu to make the conference louder for themselves
*6	Decreases transmit volume. The user can tap this option to decrease the volume of what they are transmitting to the rest of the conference members. When this option is used, the user will sound quieter to all other conference members. If a user is much louder than the other members of a conference room, they can tap 7 a few times while in the conference menu to make their transmit volume quieter.

Menu Option	Action
*7	Increases transmit volume. The user can tap this option to increase the volume of what they are transmitting to the rest of the conference members. When this option is used, the user will sound louder to all other conference members. If the conference members are having trouble hearing a particular user, that user can tap 9 a few times while in the conference menu to make their transmit volume louder.

If the **Record Conference** option is set to **Yes**, all the channels that are bridged together for the conference will be recorded into a single WAV file. The file will be stored in the */var/spool/asterisk/monitor* folder, and the filename will have a time and date stamp of when the conference ended.

When all of the conference options are configured for the desired behavior, click on the **Save** button to save the conference, and then click on the red-colored **Apply Config** bar to load the conference into the running CompletePBX configuration.



Summary

By this point, we should have a good understanding of each of the different types of basic call targets, and should likely have several targets set up and ready to accept calls. We should be able to create call targets in order to do the following:

- Terminate calls
- Ring an extension directly
- Drop a call directly to voicemail (without ringing an extension first)
- Ring a group of phones using various ring strategies
- Conference multiple users together

In the next chapter, we will cover the advanced call targets of queues, time conditions, and IVRs.

5. Advanced Call Targets

Advanced call targets in CompletePBX require a bit of additional set up before they can be used. They often generate complicated call flows. However, for the most part, CompletePBX developers have encapsulated this complexity into a straightforward interface. Advanced call targets allow callers to be directed to queues (so that a caller hears music until all of the calls in front of them have been cleared and someone is available to take their call), or to digital receptionists routing calls based on input from the caller. Advanced call targets also allow calls to take different paths depending on the date, day of the week, or time of the day.

In this chapter, we will be discussing advanced call targets in CompletePBX, which are as follows:

- Queues
- Time Conditions
- IVR (Digital Receptionist)

Queue

Applications → Queues

A queue is a "line up" or "stack" of calls that need to be answered. By default, CompletePBX queues work in a First In, First Out (FIFO) fashion (the first caller who enters the queue is the first caller to be picked up out of the queue). Call queues are useful for scenarios in which the volume of callers is expected to exceed the number of people available to answer calls. Scenarios such as a technical support line or a sales line are good examples. Callers who are placed into a queue will hear music while on hold until someone is available to answer their call.

It is often helpful to think of queues in terms of a physical store, wherein, there are a small number of employees to serve a large number of people. Imagine you are in a line at the bank with ten other people and there are only three tellers. The three tellers are unable to serve all of the ten people at once, and it would be rude for them to help someone from the middle of the line before the person who is next in the line.

Each person is called up to an available teller in the order that they entered the line. In North America, this is generally called "waiting in line", but in some countries this is actually referred to as a queue. Such is the case with a telephone queue. If you are the fifth caller to enter a queue, then you will be the fifth caller to be picked up by an available user.

Queue Priorities

Connectivity → Queue Priorities

By default, any queue created in CompletePBX will treat callers with a FIFO methodology. However, there may be situations, when certain callers should be prioritized in order to enable shorter wait times. Going back to the analogy of a physical bank, those ten customers waiting in line may see a new customer enter the bank and walk straight past the line to be serviced by an available teller. The customer may be a business customer instead of a personal banking customer, or they may simply be paying for a higher level of service. Whatever the case may be, they are allowed to bypass all of the other customers in order to receive faster service. Queue priorities allow particular callers to be weighted differently than others, in order to enable this kind of prioritization.

The default setting for all of the callers is to have a priority of zero. Callers with a priority above zero will be placed in front of priority zero callers. The highest priority call will be placed first when ordering calls in the queue, and the order will be decided by descending priority. Queue priorities

are often used when **service level agreements (SLAs)** are present, which stipulate that certain callers must have their call answered within a certain timeframe. Setting those callers up with a higher priority will ensure they are placed at the front of the queue and that their call will be answered more quickly than calls from those without SLAs. CompletePBX allows call priorities to be set between zero and twenty.

Queue priorities act as their own call target. A caller is directed to a queue priority target and is then immediately redirected to another call target. Once passing through a queue priority target, a call will hold its newly assigned priority for any queue that it enters (a caller only needs to be prioritized once, after which they can enter as many queues as they need to, without fear of losing their priority number).

In order to set up a new queue priority target, navigate to the **Connectivity** menu and select the **Queue Priorities** dialog. The queue priorities edit screen will be displayed as follows:

Add Queue Priority Instance

Description:

Priority:

Destination:

Submit Changes

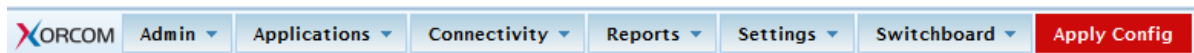
The edit screen has two main sections as follows:

- Edit Queue Priority Instance
- Destination

The first section allows for a description (used when selecting this priority as a target) and the actual priority itself. In this example, the queue priority is being set up in order to prioritize bronze level callers. Callers are given a priority of **5**, placing them above callers with no priority, but leaving plenty of room for callers with a higher-level SLA.

The **Destination** section is for selecting the call target that the caller will be sent to, now that they are prioritized. Queue priorities that do not have a queue as their eventual destination are essentially useless. So, be sure that the caller will eventually wind up in a queue if they are sent through a queue priority target. This usually means sending the caller directly to a queue or an IVR where a queue is a possible option.

When the **Description**, **Priority**, and **Destination** fields have been set, click on the **Submit Changes** button in order to save the priority, and then click on the red-colored **Apply Config** bar in order to have the changes take effect.



Queue priorities are usually set up as the first call target for inbound calls. Inbound routes can be set up in order to recognize a particular caller's caller ID and then route them to the appropriate call priority. Alternatively, if customers are given different phone numbers to call based upon their service level, then an inbound route can send calls to those numbers to specific queue priorities.

Queues

Applications → Queues

Queues can be very simple to set up for basic functionality, but advanced options and behaviors come with a bit of a learning curve. Queues have over thirty options, making them the most complicated call target available in CompletePBX. In order to set up a new queue, navigate to the **Applications** menu and select the **Queues** dialog.



Important Note

If you want the Switchboard to track the status of queues and to create statistics for call center reporting, make sure that both **Event When Called** and **Member Status Event** (in the **Events, Stats and Advanced** section of the Queue dialog) are set to **Yes** when defining a new queue.

Add Queue

Applications → Queues

The **Add Queue** section has several options and an **Extension Quick Pick** drop-down menu as shown in the following screenshot:

Add Queue

Add Queue

Queue Number: [?]	<input type="text"/>
Queue Name: [?]	<input type="text"/>
Queue Password: [?]	<input type="text"/>
Generate Device Hints: [?]	<input type="checkbox"/>
Call Confirm: [?]	<input type="checkbox"/>
Call Confirm Announce: [?]	Default <input type="text"/>
CID Name Prefix: [?]	<input type="text"/>
Wait Time Prefix: [?]	No <input type="text"/>
Alert Info [?] :	<input type="text"/>
Static Agents: [?]	<div style="border: 1px solid #ccc; height: 80px; width: 100%;"></div>
Extension Quick Pick [?]	(pick extension) <input type="text"/>
Dynamic Members: [?]	<div style="border: 1px solid #ccc; height: 80px; width: 100%;"></div>
Extension Quick Pick [?]	(pick extension) <input type="text"/>
Restrict Dynamic Agents [?]	Yes No <input type="text"/>
Agent Restrictions [?]	Call as Dialed <input type="text"/>

Keep it simple!



There are so many options and flags that can be set to improve queue management that you may find it to be rather confusing.

You can create a basic queue by defining only **Queue Number**, **Queue Name**, and **Fail Over Destination** fields. All other fields are optional, but will give you greater control over the behavior of the queue.

Queue Number can be thought of as the "extension" assigned to the queue. If a caller is calling into the queue from an endpoint on this system, or someone is transferring a call to the queue, then this is the number they will use. The **Queue Number** is also used to sign in and out of the queue. If an

employee is not permanently a member of the queue, they can dial this **Queue Number** plus * to log into the queue, and this **Queue Number** plus ** to log out (for example, a Queue Number of 5000 would have agents dial 5000* to log in and 5000** to log out).

Queue Name is used to identify the queue when selecting it as a call target. This name is not parsed by CompletePBX.

If **Queue Password** is not left blank then queue agents will be required to enter this password before they are able to join the queue. This option is used in conjunction with the **Queue Number** (agents will be prompted for the password after dialing the **Queue Number** plus *). This setting is optional.

The **CID Name Prefix** is used to prefix the caller ID of callers in the queue with the value entered in this field. This is often used when agents are members of multiple queues so that they know which department a person has called (for example, a CID may be prefixed with "Sales" or "Tech Support").

Wait Time Prefix is used to prefix the caller ID of callers in the queue with the number of minutes the caller has been waiting in the queue. The time will be rounded off to the nearest minute, and will be prefixed with the letter "M". If the call is subsequently transferred to another queue with this feature set, the time count will reset.

Alert Info is used to send specific *ALERT_INFO* SIP headers to SIP endpoints that support them. Many SIP endpoints can be set up to ring differently, or automatically answer calls when specific *ALERT_INFO* values are received. For *ALERT_INFO* headers to trigger an action on an endpoint, the *ALERT_INFO* header that the phone is configured to look for must match the *ALERT_INFO* header that CompletePBX is sending. Some endpoints will allow the information headers to be configured on the device, while others have these header values statically configured so they cannot be changed. The documentation that accompanies a SIP endpoint should list whether or not the device supports *ALERT_INFO* headers, as well as if the headers can be configured, or are predefined.

Static Agents are extensions that are always members of the queue. Static agents do not need to log into the queue, and cannot log out of the queue. As long as an agent listed in this field is available, their endpoint will be rung when a caller is in this queue. Extensions should be listed one per line. Remote telephone numbers or extensions can also be added to this field. Note that unlike ring groups, external numbers can be added as they would be dialed from a normal endpoint on the system, and do not require a pound symbol at the end.

Advanced users can add agents from their */etc/asterisk/agents.conf* file to the **Static Agents** field by prefixing their agent number with the letter "A" (for example, agent number 2223 would be listed as A2223). For the time being, this functionality is considered experimental and may cause various issues with terminating and transferring calls that are received by these agents.

Any agent listed in the Static Agents field can have a penalty value appended to their extension after a comma (for example, agent 2223 with a penalty value of 1 would be listed as "2223,1"). Listing an agent without a penalty value assigns the agent a penalty of zero. Penalties affect when certain agents are called. The higher the penalty an agent has, the less likely they are to receive a call from the queue. An agent with a penalty of one will only be rung if nobody with a penalty of zero is available. Likewise, an agent with a penalty of two will only be rung if nobody with a penalty of zero or one is available. Penalties are useful for adding agents to the queue who would not normally be taking these type of calls, but should be available to handle overflow of calls if the need arises.

The **Extension Quick Pick** list allows any configured extension to be selected from the drop-down menu. The selected extension will be copied into the **Static Agents** field with a penalty of zero.

Queue Options

Applications → Queues

The **Queue Options** section has just under twenty options available for configuring the queue as shown in the following screenshot:

General Queue Options

Ring Strategy: [?]	ringall ▾
Autofill: [?]	<input type="checkbox"/>
Skip Busy Agents: [?]	No ▾
Queue Weight: [?]	0 ▾
Music on Hold Class: [?]	inherit ▾
Ringing Instead of MoH: [?]	<input type="checkbox"/>
Join Announcement: [?]	None ▾
Call Recording: [?]	No ▾
Recording Mode: [?]	Include Hold Time ▾
Caller Volume Adjustment: [?]	No Adjustment ▾
Agent Volume Adjustment: [?]	No Adjustment ▾
Mark calls answered elsewhere: [?]	<input type="checkbox"/>

The **Agent Announcement** drop-down menu is used to select a sound file to be played back to the agent who answers the call before the call is bridged to them. This file must be pre-recorded or uploaded to the system by using the **System Recordings** dialog. More information on creating custom recordings for the Agent Announcement field can be found in the [Voice Prompts](#) section in Chapter 8. This announcement is optional, but may serve the purpose of telling the agent which queue the call came from (if CID is not available to provide this information).

The **Join Announcement** drop-down menu is used to select a sound file to be played back to the caller before they are dropped into the queue. This file must be pre-recorded or uploaded to the system through the **System Recordings** section of CompletePBX. This announcement is optional, but will usually state that the caller is being placed into a queue, and that their call will be answered in priority sequence.

The **Music on Hold Class** drop-down menu is used to configure the music that is played to the caller while they wait in the queue. The **inherit** option can be selected in order to have the queue use the same music on hold class already assigned to the call (usually this is set through an inbound route). Music on hold classes can be configured by using the **Music on Hold** dialog. Further information on creating custom recordings for the **Agent Announcement** field can be found in the [Music on Hold](#) section in Chapter 9.

If the **Ringing Instead of MoH** box is checked then callers will hear ringing instead of Music on Hold while they wait in a queue. Use this option carefully; a long wait time can mean dozens of ring tones and often a caller who hangs up (thinking their call is never going to be answered). If this option is enabled, the option selected in the **Music on Hold Class** drop-down menu is ignored.

Max Wait Time is the amount of time, in seconds, that a caller is able to wait in the queue before the call is considered failed and routed to the failover destination. Set it to **Unlimited** in order to

configure the queue to use an unlimited wait time. This field has a maximum value of one hour otherwise.

Max Callers is the maximum number of callers allowed to enter the queue at any time. Callers over this limit will immediately be sent to the failover destination. Enter **0** to configure the queue for an unlimited number of callers. This field has a maximum value of 50 otherwise.

If **Join Empty** is set to **Yes**, then callers are able to join the queue and wait even if no agents are signed into the queue. The **Strict** option will not allow callers to join the queue if either no agents are signed in or all of the signed in agents are unavailable. The **No** option will not let callers join the queue if no agents are signed in, but it *will* allow callers to join if all of the signed in agents are unavailable. Callers that are not allowed to join the queue because of Strict or No settings are immediately sent to the failover destination.

Leave When Empty drop-down menu carries the same settings as the **Join Empty** drop-down menu. Leave When Empty is employed when there are suddenly no more agents signed into the queue *after* a caller has already joined the queue.

Ring Strategy drop-down menu determines the way that agents will be called when a caller enters the queue. It has the following options:

- **ringall**: All of the agents are rung until one answers.
- **roundrobin**: Agents are rung one at a time in the order they are listed in the **Ring Strategy** textbox until one of them picks up.
- **leastrecent**: It is similar to **roundrobin**, but starts with the agent who was least recently called by this queue. Note that CompletePBX does not account for call length, so the timer that counts how long ago an agent was rung starts counting from when an agent picks up a call, not from when the call is completed. An agent who is on a call for an hour is still considered to have been rung an hour ago.
- **fewestcalls**: Rings the agent who has answered the fewest calls from this queue.
- **random**: Rings a random agent.
- **memory**: It is similar to roundrobin, but remembers the last agent who was rung in the last round robin and starts by calling them first.

Agent Timeout is the number of seconds an agent's phone can ring before the call is considered failed for that agent. Set this to **Unlimited** in order to ring the agents continuously until somebody answers the call. This field has a maximum value of 60 seconds otherwise. Note that this field will be overridden if either the general ring time setting or an extension's own follow-me ring time setting is lower than the specified timeout. For example, if the CompletePBX general ring time setting is set to 30 seconds, and **Agent Timeout** is set to 45 seconds, then the maximum amount of time that an agent's phone will ring is 30 seconds. Also, setting this field to **Unlimited** will only work for the **ringall** ring strategy. Other strategies will ring extensions for 60 seconds (or the value of the general ring time setting or the extension's follow-me ring time, whichever is shorter) before carrying on to ring the next agent.

Retry value is the number of seconds the system will wait before calling an agent after the last attempt timed out. Selecting **No Retry** will send the caller to the failover destination as soon as the first attempted agent times out (additional agents will not be rung). This field has a maximum value of 20 seconds.

Wrap-Up-Time is the number of seconds an agent is considered unavailable after they have completed a call from this queue. Setting this option to **0 seconds** means no delay. This field has a maximum value of 60 seconds.

If **Call Recording** is set to any value except **No** then calls to this queue will be recorded in the selected format and saved to the `/var/spool/asterisk/monitor` directory. Calls to a queue that are

recorded will be named using the format: *q(QueueNumber)-(Date)-(Time)-(CallID).(Format)*. The tokens will be replaced with the following values to locate the file:

Token	Will be replaced with
(QueueNumber)	The number or extension of the queue. The number of the queue is configured in the Queue Number field
(Date)	The date that the call was answered on. The date is in the format of YYYYMMDD
(Time)	The time that the call was answered. The time is in the format of HHMMSS, and is in 24 hour format
(CallID)	A unique ID assigned to the call by CompletePBX. The ID is not referenced anywhere in the CompletePBX interface. Hence, if two calls come into the same queue at the exact same time, they will have to be heard in order to determine which call is which.
(Format)	The appropriate file extension for the format of the call. WAV and WAV49 formats will have an extension of .wav; the GSM format has an extension of .gsm

For example, a call that came into queue number 8001 on July 19, 2009 at 7:05:45 p.m. would have a filename like *q8001-20090715-190545-1247699145.4355.wav*.

If **Event When Called** is set to **Yes**, the events generated during the progress of a call to this queue include AgentCalled, AgentDump, AgentConnect, and AgentComplete. These events can be used by third-party software programs, such as **My Switchboard**, in order to track call progress and generate call metrics.

Similar to **Event When Called**, when **Member Status** is set to **Yes** the QueueMemberStatus event will be generated during call progress.

If **Skip Busy Agents** is set to **Yes**, then agents who are on a call will not be rung when there is a caller in the queue. This option applies to extensions with call waiting active, or multi-line endpoints. Even though these endpoints have the ability to receive multiple calls at the same time, if they are in use they will not be rung.

Queue Weight gives all of the callers in the queue a particular priority. This weighting is used by CompletePBX to determine which call to deliver to agents signed into multiple queues. If an agent is signed into multiple queues and both queues have callers waiting in them, the queue with the higher Queue Weight will ring through to the agent first.

The **Autofill** option is only applicable to CompletePBX version 1.4 and later versions. This option allows multiple callers to be sent to multiple agents at the same time. For example, if three callers are in the queue, and three agents are available, enabling this option will send each caller to one of the agents. If this option is disabled then only one call is processed at a time, and every caller must wait to be first in line before any agent is rung for their call. This option has no effect in CompletePBX version 1.2. This option is not affected by the selected ring strategy (agents are still rung in the order defined by the ring strategy).

Agent Regex Filter can be used to restrict the extensions of agents who are allowed to sign into the queue. If this field is left blank then it is possible for any agent who knows the queue number and

password to sign into the queue. Entering a regular expression in this field can restrict the agents who can log into the queue to specific extensions or ranges of extensions.

Regular Expressions



Regular expressions can be very complicated. It is a good idea to have a thorough understanding of how to craft regular expressions before attempting to use the Agent Regex Filter field. An invalid regular expression in this field could make the queue entirely inaccessible to all of the agents. More information on regular expressions can be found at http://en.wikipedia.org/wiki/Regular_expression

Caller Position Announcements

Applications → Queues

The **Caller Position Announcements** section has three configurable options as shown in the following screenshot:

Caller Position Announcements

Frequency: ?	0 seconds ▼
Announce Position: ?	No ▼
Announce Hold Time: ?	No ▼

This section is used to control how often a message is played to each caller in the queue detailing their position in the queue and how long it is estimated that they will be on hold.

Frequency drop-down menu controls how often this type of announcement is made. Setting this to **0 seconds** disables the announcements entirely. This field has a maximum value of 20 minutes otherwise.

If **Announce Position** is set to **Yes** then the caller will be told their place in the queue each time the position announcement is played.

If **Announce Hold Time** is set to **Yes**, then the caller will be told their estimated hold time each time this message is played. If this field is set to **Only Once**, then the estimated hold time will be played to the caller when they first join the queue, but never again. When estimated hold times are less than one minute, hold times are not announced.

If both **Announce Position** and **Announce Hold Time** are set to **No**, neither announcement will ever be played no matter to what the **Frequency** field is set.

Periodic Announcements

Applications → Queues

Periodic announcements can be played to each caller in order to give them the option to perform another task. Usually this means that an IVR is presented to the caller, and the caller is given the option to leave a voicemail or to reach a different department. The **Periodic Announcements** section has two configurable options as shown in the following screenshot:

Periodic Announcements

IVR Break Out Menu: [?]

Repeat Frequency: [?]

IVR Break Out Menu is the IVR that should be presented to the caller each time the announcement is played. The recording set for the selected IVR is what will be played to the caller. The selected IVR must only contain single-digit options.

Repeat Frequency is how often the IVR should be presented to the caller. Setting this to **0 seconds** disables the periodic announcements. This field has a maximum value of 20 minutes otherwise.

The user can only select one **Fail Over Destination** as shown in the following screenshot:

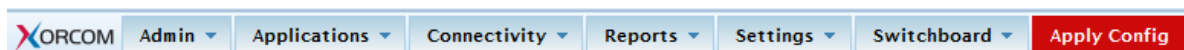
Fail Over Destination

== choose one ==

- == choose one ==
- Conferences
- Custom Destinations
- Extensions
- Fax Recipient
- Feature Code Admin
- IVR
- Misc Destinations
- Phonebook Directory
- Queue Priorities
- Queues
- Terminate Call
- Trunks
- Voicemail

Select the call target where callers should be directed if their call to this queue fails for any reason. A call could be considered failed because no agents were signed into the queue, the caller waited in the queue for too long, or no signed in agents were available to answer the call (depending on the configured options).

When all of the options have been configured for the desired queue behavior, click on the **Submit Changes** button in order to save the queue, and then click on the red-colored **Apply Config** bar in order to load the queue into the running CompletePBX configuration.



Time-based Rules

Time conditions are a set of rules for hours, dates, or days of the week. A condition has two call targets each time. Calls sent to a time condition will be sent to one target if the time of the call matches one of the conditions, or to the other target if none of the conditions match. Each time condition can have multiple time definitions (known as time groups). Time conditions are often used to control how a phone system responds to callers inside and outside of business hours, and during holidays.

Time Groups

Applications → Time Groups

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.

In order to create a new time group, navigate to the **Applications** menu and select the **Time Groups** dialog. The **Add Time Group** screen will be displayed as shown in the following screenshot:

Add Time Group

- Time Group

Description [?]

- New Time

Time to start: :

Time to finish: :

Week Day start:

Week Day finish:

Month Day start:

Month Day finish:

Month start:

Month finish:

The **Description** field is used to identify this time group, when selecting it during the setup of a time condition. This value is not parsed by CompletePBX.

The **New Time** section is used to define a time rule that a call will be matched against. Leaving a field as the default dash (-) will match all of the values (for example, **Week Day Start** to **Week Day Finish** will match on every day of the week). Keep in mind that all of the conditions must be true for the rule to match, so it is possible to create rules that never match (setting **Month Day start** and **Month Day finish** to 31 and **Month start** and **Month finish** to September will never match as there is no 31st of September).

Once the appropriate rule has been defined, click on the **Submit** button in order to save the rule. Additional time rules can be added to a time group by clicking on the group's name in the time group list on the right and selecting additional rule parameters in the **New Time** section at the bottom of the page. An example of a time group with multiple rules might be a group defining business hours as shown in the following screenshot:

- Time GroupDescription  **- 08:30-17:30|mon-fri|*|***

Time to start: :

Time to finish: :

Week Day start:

Week Day finish:

Month Day start:

Month Day finish:

Month start:

Month finish:

- New Time

Time to start: :

Time to finish: :

Week Day start:

Week Day finish:

Month Day start:

Month Day finish:

Month start:

Month finish:

In this example, the condition will match Monday through Friday, 8:30 a.m. through 5:30 p.m. and on Saturday from 9:30 a.m. through 3:30 p.m.

Time Conditions

Applications → Time Conditions

Once a time group has been defined, a time condition can be set up as a call target. In order to create a new time condition, navigate to the **Applications** menu and select the **Time Conditions** dialog. The **Add Time Condition** screen will be displayed along with four configuration sections. The first section is the **Add Time Condition** section as shown in the following screenshot:

Add Time Condition

Add Time Condition

Time Condition name: [?]

Generate BLF Hint [?]

Enable Override Code [?]

Time Group: [?]

Destination if time matches:

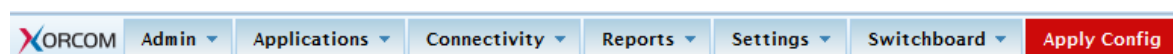
Destination if time does not match:

Submit

The **Time Condition name** field is used for identifying the time condition when selecting it as a call target. This value is not parsed by CompletePBX.

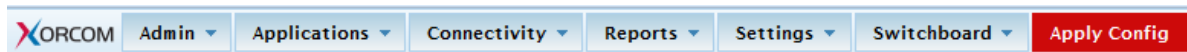
The **Time Group** drop-down menu is used to select the time group that this time condition should be referencing for time rules. When a call reaches this time condition, the rules in the selected Time Group will be parsed in order to determine where to send the call next.

Click on the **Submit Changes** button in order to save the queue, and then click on the red-colored **Apply Config** bar to load the queue into the running CompletePBX configuration.



The last two sections, **Destination if time matches** and **Destination if time does not match** are for setting up the call targets for calls that match the rules set up in the selected time group and for calls that do not.

Select the desired call destinations, click on the **Submit Changes** button in order to save the destination, and then click on the red-colored **Apply Config** bar in order to load the destination into the running CompletePBX configuration.



IVR (Digital Receptionist)

Applications → IVR

An **Interactive Voice Response (IVR)** system is often referred to as a digital receptionist. An IVR plays back 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.

CompletePBX IVRs allow any digits to be defined as destinations (for example, pressing one might route to the sales ring group). A destination of **t** can also be defined to route the call if the IVR times out without receiving any input. A destination of **i** can be defined to route the call if the IVR receives invalid input.

In order to create an IVR, navigate to the **Applications** menu and select the **IVR** dialog. The **Digital Receptionist** screen will appear with two configuration sections: **IVR options** and **IVR destinations**. The **IVR options** section has configurable options as shown in the following screenshot:

Add IVR

- IVR General Options

IVR Name [?]	<input type="text"/>
IVR Description [?]	<input type="text"/>

- IVR Options (DTMF)

Announcement [?]	<input type="text" value="None"/>
Direct Dial [?]	<input type="text" value="Disabled"/>
Timeout [?]	<input type="text" value="10"/>
Invalid Retries [?]	<input type="text" value="3"/>
Invalid Retry Recording [?]	<input type="text" value="Default"/>
Append Original Announcement [?]	<input type="checkbox"/>
Invalid Recording [?]	<input type="text" value="Default"/>
Invalid Destination [?]	<input type="text" value="== choose one =="/>
Timeout Retries [?]	<input type="text" value="3"/>
Timeout Retry Recording [?]	<input type="text" value="Default"/>
Append Original Announcement [?]	<input type="checkbox"/>
Timeout Recording [?]	<input type="text" value="Default"/>
Timeout Destination [?]	<input type="text" value="== choose one =="/>
Return to IVR after VM [?]	<input type="checkbox"/>

- IVR Entries

Ext	Destination	Return [?]	Delete
<input type="text" value="digits pressed"/>	<input type="text" value="== choose one =="/>	<input type="checkbox"/>	

Submit

Change Name is used as a name for identifying the IVR. This field is not parsed by CompletePBX.

The **Announcement** drop-down menu is used to select a pre-recorded message that will be played to the caller as they enter the IVR. Recordings must be pre-recorded or updated in the **System Recordings** CompletePBX section.

Timeout is the number of seconds that the system will wait for input from the caller. If this number of seconds passes without input, the call will fail over to the **t** destination (if defined), or the call will be disconnected.

If **Enable Directory** is checked then callers can press the pound (#) key to enter a directory system that will allow them to search for a person by first name or last name. Otherwise, pressing the pound key will play back a message stating that the caller has provided invalid input.

If **VM Return to IVR** is checked then a caller who transfers from the IVR to a voicemail box will be transferred back to the IVR when they are done leaving a message. If this option is not selected then the caller will be disconnected after leaving a voicemail.

If multiple directory contexts are defined, the directory that should be accessible to the caller when the pound key is pressed can be selected from the **Directory Context** drop-down menu.

Enable Direct Dial enables the callers to dial an extension directly from the IVR. If this option is disabled then the callers will receive a message stating that they have provided invalid input when they enter an extension, *even if the extension is valid*.

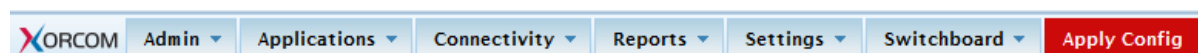
Timeout Message is the message that will be played to the caller if they fail to enter any input before the number of seconds specified in the **Timeout** box. This message will only be played if the **t** destination is not defined.

Invalid Message is the message that will be played to the caller if they enter invalid options while in the IVR. This message will only be played if the **i** destination is not defined.

Repeat Loops is used to select the number of times the IVR will repeat itself when no valid input is received. After the specified number of loops, the caller will be disconnected. The maximum number of loops allowed is nine.

IVR destinations section allows multiple key presses to be mapped to specific destinations:

When all of the IVR options are configured for the desired behavior, click on the **Save** button to save the IVR, and then click on the red-colored **Apply Config** bar to load the IVR into the running CompletePBX configuration.



Paging & Intercom

Applications → Paging & Intercom

Paging allows you to page a number of extensions, provided that you have phones that support this. You dial a number, and all the phones in the paging group pick up automatically, go into hands-free mode, and play what the caller is saying through the speaker. This can be useful in an office environment to announce that a call has been sent to the Parking Lot, and is waiting for someone to handle it.

To add a paging group, simply put in the Paging group number - this is the number that people will dial to page the group, and the list of devices, one per line, that are to be paged. This dialog is for specific phones that are capable of Paging or Intercom.

Intercom must be enabled on a handset before it will allow incoming calls. It is possible to restrict incoming intercom calls to specific extensions only, or to allow intercom calls from all extensions but explicitly deny from specific extensions.

This dialog should work with Xorcom IP phones as well as most other SIP phones (not ATAs). Any

phone that is always set to auto-answer should also work.

Navigate to the **Applications** menu and selecting the **Paging & Intercom** dialog.

Paging Extension is the number you will dial to talk to a paging group.

Group Description is a descriptive name to help you identify a paging group.

Busy Extensions enables you to determine how to handle paged extensions that are busy, with options to **Skip**, **Force**, or **Whisper** to the extension. Each option affects busy extensions only – other extensions will be paged in the normal manner.

- **Skip** will not page any busy extension. All other extensions will be paged as normal
- **Force** will not check if the device is in use before paging it. This means conversations can be interrupted by a paging call, depending on how the device handles it. This is useful for emergency paging groups.
- **Whisper** will attempt to use the ChanSpy capability on SIP channels, resulting in the paging call being sent to the device's earpiece, and being "whispered" to the user, but not heard by the remote party. If ChanSpy is not supported on the device or otherwise fails, no page will get through. It probably does not make much sense to choose duplex if using Whisper mode.

Paging is typically one way for announcements only. Checking on **Duplex** will make the paging call duplex, allowing all phones in the paging group to be able to talk and to be heard by all. This makes it like an instant conference.

Modify Paging Group

Paging Extension [?]

Group Description [?]

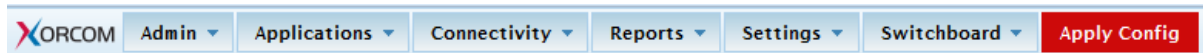
Selected	Not Selected
<input checked="" type="checkbox"/> 2001 - VP Marketing	<input type="checkbox"/> 1001 - DAHDI channel 1
<input checked="" type="checkbox"/> 2002 - VP Sales	<input type="checkbox"/> 1002 - DAHDI channel 2
<input checked="" type="checkbox"/> 2003 - VP Support	<input type="checkbox"/> 1003 - DAHDI channel 3
<input checked="" type="checkbox"/> 2020 - CEO	<input type="checkbox"/> 1004 - DAHDI channel 4
	<input type="checkbox"/> 1005 - DAHDI channel 5

Busy Extensions [?] Skip Force Whisper

Duplex [?]

Default Page Group

When all of the paging options are configured for the desired behavior, click on the **Save** button to save the paging group, and then click on the red-colored **Apply Config** bar to load it into the running CompletePBX configuration.



Parking

Settings → Parking Lot

This dialog allows you to configure the settings for the parking lot functionality of CompletePBX. Navigate to the **Settings** menu and select the **Parking Lot** dialog.

Parking Lot Options

Parking Lot Extension:

Parking Lot Name:

Parking Lot Starting Position:

Number of Slots: (71-78)

Parking Timeout (seconds):

Parked Music Class:

BLF Capabilities:

Find Slot:

Returned Call Behavior

Pickup Courtesy Tone:

Transfer Capability:

Re-Parking Capability:

Parking Alert-Info:

CallerID Prepend:

Auto CallerID Prepend:

Announcement:

Alternate Destination

Come Back to Origin:

Destination:

An especially useful part of this dialog is the ability to specify a destination for parked calls that get orphaned. This can occur if the call is not picked up and for some reason the original parker cannot be reached (e.g. the original parker is on the phone and does not have call waiting or ignores it). In this case, the call is diverted to the chosen destination which is any of the standard destinations. Prior to sending the call to that destination, you can configure options to further identify the orphaned call:

- Parking Alert-Info, to provide a unique ring for the returned call
- CallerID Prepend (to identify the call with additional CID information)
- Announcement (to be played to the orphaned caller to reassure them that call is still active)

Parking Lot Options

Settings → Parking Lot

Parking Lot Extension defines the extension number where you will transfer a call to, in order to park it.

Parking Lot Name allows you to provide a name for the parking lot.

Parking Slot Starting Position allows you to determine the first number that will be available in the parking lot.

Number of Slots defines the total number of parking lot spaces to configure. For example, if 70 is the extension and 8 slots are configured, the parking slots will be 71-78.

Parking Timeout is the period that a parked call will attempt to ring back to the original parker if the call is not answered.

Parked Music Class is the music class that will be played to a parked call while in the parking lot UNLESS the call flow prior to parking the call explicitly set a different music class, such as if the call came in through a queue or ring group.

BLF Capabilities should be checked on to have 'hints' generated to use with BLF buttons.

Find Slot determines the behavior when you want the parking lot to seek the next sequential parking slot relative to the last parked call instead of seeking the first available slot.

Returned Call Behavior

Settings → Parking Lot

Pickup Courtesy Tone defines to whom to play the courtesy tone to when a parked call is retrieved. This can be the caller, the parker, or both.

Transfer Capability toggles DTMF based transfers when picking up a parked call.

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

Parking Alert-Info to be added to the call prior to sending back to the Originator or to the Alternate Destination.

Auto Caller ID Prepend is the string to prepend to the current Caller ID associated with the parked call prior to sending back to the Originator or the Alternate Destination.

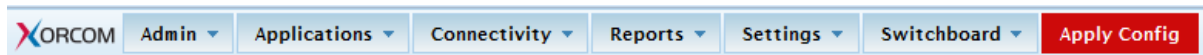
Announcement is an optional message to be played to the call prior to sending back to the Originator or the Alternate Destination.

Alternate Destination

Settings → Parking Lot

Come Back to Origin determines where to send a parked call that has timed out. The call can be sent back to the original device that parked the call, or it can be sent back to the alternate destination. In both cases, any configured Alert-Info, Caller ID prepend, or announcement will be applied to the call. If configured to send back to the Originator and they are not available (phone is offline), the alternate destination will be used.

When all of the parking options are configured for the desired behavior, click on the **Save** button to save the configuration, and then click on the red-colored **Apply Config** bar to load it into the running CompletePBX configuration.



Summary

By this point, we should have a good understanding of advanced call targets. We should be able to route calls using complicated time conditions into an IVR system that eventually routes the caller into a call queue, if we desire to do so.

The next chapter will put our call targets into action with inbound call routes. We will also discuss setting up outbound routes (in order to utilize the trunks we set up a few chapters ago), in addition to setting up least cost routing in order to properly route calls over the cheapest available trunk.

6. Call Routing

Up until this point, we have discussed various call targets and what will happen to calls when they reach those targets. In this chapter, we will discuss the following:

- Inbound routing
- Follow Me and the VmX Locator
- Outbound routing
- Least Cost Routing (the ability to pick the cheapest route for a call, based on the dialed destination)

Inbound Routing

Connectivity → *Inbound Routes*

Inbound routing is one of the key pieces to a functional CompletePBX phone system. Inbound routes in CompletePBX are where we finally get to put to use the call targets discussed in Chapters 4, **Basic Call Targets** and Chapter 5, **Advanced Call Targets**.

CompletePBX allows two specific types of inbound routing:

1. **DID-based routing:** DID-based routing routes calls based on the trunk on which the call is coming in. CID-based routing routes calls based on the caller ID number of the person who is calling. Within those two routing methods, CompletePBX allows the detection of inbound faxes. **DID (Direct Inward Dialing)**, in VoIP telephony, refers to a trunk and the telephone number associated with that trunk. As it is possible for a phone system to have several trunks, CompletePBX allows different routing rules to be set up for each trunk. This is commonly used when a company has a dedicated technical support phone number (which routes directly to their support department), while other calls to the company come in to a different phone number and are routed to an IVR or a receptionist.
2. **CID-based routing:** **CID (caller ID)** refers to the name and number of the person calling. CompletePBX allows inbound calls to be routed based on the number someone is calling from. This is commonly used to immediately disconnect calls from known telemarketers, but can also be used to route calls from specific people in a different way than routing calls from the general public.

These two routing methods can be used on their own or in conjunction with one another.

To set up inbound routing, navigate to the **Connectivity** menu and select the **Inbound Routes** dialog. A number of sections are present on the **Add Incoming Route** page:

- Add Incoming Route
- Options
- Privacy
- Call Recording
- Language
- Fax Detect
- CID Lookup Source
- Set Destination

The **Add Incoming Route** section has the following four options:

1. Description
2. DID Number

3. Caller ID Number
4. CID Priority Route

Add Incoming Route

Description [?] :	<input type="text"/>
DID Number [?] :	<input type="text"/>
CallerID Number [?] :	<input type="text"/>
CID Priority Route [?] :	<input type="checkbox"/>

Description is used to hold a description to help you remember what this particular inbound route is for. This field is not parsed by CompletePBX.

DID Number 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 with 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. Patterns must begin with an underscore (`_`) to signify that they are patterns. Within patterns, `X` will match the numbers 0 through 9, and specific numbers can be matched if they are placed between square parentheses. For example, to match both 555-555-1234 and 555-555-1235, the pattern would be `_555555123[45]`.

Caller ID Number is used when CID-based routing is desired. 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 the field is entered correctly.

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 a route that matches all calls.

Inbound Routing Priorities

Connectivity → Inbound Routes

It is possible to run into a situation in which a call matches several of the defined inbound routes. In this scenario, CompletePBX will give a route priority in the following sequence:

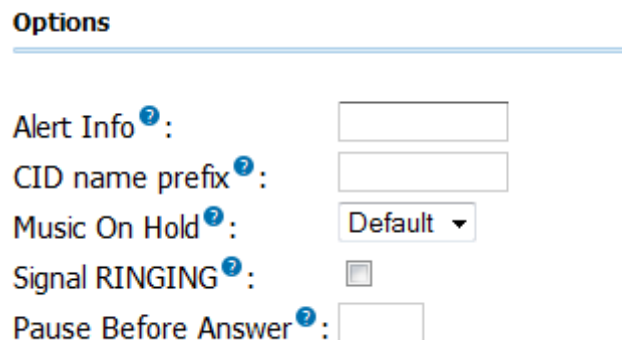
- Routes with a specific DID and CID will always be first in priority.
- Routes with a specific DID but no CID will be second in priority.
- Routes with no DID, but with a specific CID will be third in priority.
- Routes with no specific DID or CID will be last in priority.

It is important to note that by default, setting up a route for a specific DID will take preference over

setting up a route for a specific CID.

The **CID Priority Route** toggle affects the inbound routing priority behavior. If this checkbox is selected, all calls from the number specified in the **Caller ID Number** field will be routed using the route even if there is a route for the DID on which the call came in. If there is a specific route that specifies both DID and CID, then that route will still take precedence. Checking the CID Priority Route toggle simply swaps the second and third routing priorities for this particular route.

The **Options** section has five fields as shown in the following screenshot:



Options

Alert Info [?]:

CID name prefix [?]:

Music On Hold [?]:

Signal RINGING [?]:

Pause Before Answer [?]:

Alert Info is used to send a string of text in the SIP *ALERT_INFO* headers. This is often used for SIP endpoints that ring differently, or auto-answer calls based on the *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.

CID name prefix allows text to be prepended to the caller ID name information from the call. This is often used to identify where a call came from (calls to a number dedicated for technical support might be prefixed with "Tech").

Music On Hold drop-down menu allows the music-on-hold class for this call to be selected. Whenever a caller who passes through 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 advertise in their music on hold and 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.

Signal RINGING toggle will send "ringing" in the call progress data, before CompletePBX lets the other side know that the call has been answered. Some providers require this, while this can break functionality with others. Check with your provider to see if they require "ringing" to be sent as a call progress before the call is answered.

Pause Before Answer contains the number of seconds that CompletePBX should pause before answering the call. This is not useful for digital channels, but analog DAHDI channels may have security systems or fax machines installed in parallel with the VoIP system. In such cases, a tone is usually played within a few seconds of the call being picked up to identify that the call is not a voice call. Setting a delay of a few seconds allows this tone to be played and the other piece of equipment to seize the line for communications. If the line has not been picked up by the end of this delay, CompletePBX will answer the call.

The **Privacy** section only has one configurable field:

Privacy

Privacy Manager[?]:

The **Privacy Manager** drop-down menu is used to enable or disable the CompletePBX privacy manager functionality. When enabled, calls that come in without an associated caller ID number will be prompted to enter their 10-digit telephone number. Callers will be given three attempts to enter this information before their call is disconnected.

The **Fax Detect** section has one configurable field:

Fax Detect

Detect Faxes[?]:

The **Fax Detect** toggle determines whether faxes should be detected on this route. If fax detection is activated, additional parameters can be configured and a dropdown will appear which is used to select the extension that the inbound faxes will be directed to. 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 CompletePBX. The program will accept faxes and turn them into digital documents for review.

Fax Detect

Detect Faxes[?]:

Fax Detection type[?]:

Fax Detection Time[?]:

Fax Destination[?]:

If **disabled** is selected, fax detection will not be used for calls that match this route. Any fax calls will be routed just like voice calls.

The **Fax Detection Type** drop-down menu determines which type of detection mechanism CompletePBX will use to detect the fax:

- **DAHDI** should be used when the fax is coming from a DAHDI trunk
- **SIP** should be used when the fax is coming from a SIP trunk

Fax 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, and not 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 4 or 5 seconds.

Fax Destination determines where incoming faxes will be sent. This can be any user extension that has been configured as a fax recipient, by checking on Fax Enabled, or a virtual extension that has been configured as a fax recipient.

**Take Care!**

If you are configuring behaviors such as Follow Me, you **must** ensure that the initial ring time is at least as long as the Fax Detection Time that is set here. Otherwise the fax module will not have sufficient time to detect an incoming fax.

The **CID Lookup Source** section only has one configurable field as shown in the following screenshot:

CID Lookup Source

Source [?]:

Source drop-down menu allows any predefined lookup source to be selected. Any calls that match this route will be checked against the source specified here, and will have their caller ID name changed if they match an entry in the source. Caller ID lookup sources are specified by using the **CallerID Lookup Sources** dialog.

Lastly, the **Set Destination** section has one option to configure:

== choose one ==

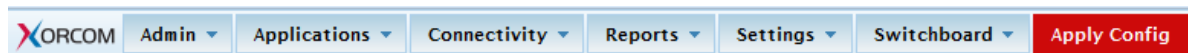
- Conferences
- Custom Destinations
- Extensions
- Fax Recipient
- Feature Code Admin
- IVR
- Misc Destinations
- Phonebook Directory
- Queue Priorities
- Queues
- Terminate Call
- Trunks
- Voicemail

== choose one ==

This is the place where the desired call target is selected. Any previously set up call target can be selected including extensions, IVRs, time conditions, conference rooms, and queues.

When all options have been selected, click on the **Submit** button to save the route. Clicking on the **Clear Destination & Submit** button will save the route without any associated destination. This is generally used for fax-only routes, where a fax must be detected or the call will be terminated. Once the route has been saved, be sure to click on the red-colored **Apply Config** bar at the top of the

screen to make the route active.



Follow Me and VmX Locater

Connectivity → Follow Me

Follow Me will force CompletePBX to try and track a user down when their extension is called instead of simply ringing their assigned endpoint. This is often used to call a cell phone before dropping the caller to voicemail. With this enabled, the user never needs to give out their cell number because the system will always try to reach them there when their main endpoint is not answered. Likewise, if the cell number changes it simply has to be updated in one place and no calls are missed.

CompletePBX has two implementations of the "follow-me" system—the default Follow Me and the VmX Locater.

The default follow-me system is controlled by the CompletePBX administrator, and allows for varying ring strategies, ring times, music-on-hold selections, and various other complex settings. The VmX Locater is controlled by the end user, but is a much simpler implementation that consists of prompting the caller to press 0, 1, or 2 and directing calls to different numbers based on what was selected.

Default Follow Me

Connectivity → Follow Me

The default follow-me routing will ring a set number of extensions in a pre-selected ring pattern (similar to a ring group) before failing over to another call target. This could mean that several VoIP phones and a cell phone are rung at the same time, or they might be rung in order, until one of them picks up. If there is no answer, the call could fail over to voicemail, or be redirected to another person at the company.

To set up default follow-me routing in CompletePBX, navigate to the **Connectivity** menu and select the **Follow Me** dialog. Click on the user that requires Follow Me settings in the list on the right and the **Follow Me** screen is displayed as shown in the following screenshot:

Follow Me: 2001

 Edit Extension 2001

Delete Entries

Edit Follow Me

Disable [?] :	<input type="checkbox"/>
Initial Ring Time: [?]	0 ▾
Ring Strategy: [?]	ringallv2 ▾
Ring Time (max 60 sec) [?]	20
Follow-Me List: [?]	2001
Extension Quick Pick [?]	(pick extension) ▾
Announcement: [?]	None ▾
Play Music On Hold? [?]	Ring ▾
CID Name Prefix: [?]	
Alert Info: [?]	

Call Confirmation Configuration

Confirm Calls [?] :	<input type="checkbox"/>
Remote Announce: [?]	Default ▾
Too-Late Announce: [?]	Default ▾

Change External CID Configuration

Mode: [?]	Default ▾
Fixed CID Value: [?]	

Destination if no answer:

Follow Me ▾	Normal Extension Behavior ▾
-------------	-----------------------------

The **Disable** checkbox will temporarily disable the follow-me setup while retaining the follow-me configuration. Any calls that are direct dial calls or calls that come from an IVR or a directory search

will ring the extension directly instead of using the follow-me routing. Note that if follow me is specifically selected as a call target, the follow-me route will be respected for that call, regardless of whether this checkbox is selected.

The **Initial Ring Time** field is used to configure the number of seconds that the primary extension is rung before any extensions in the follow-me list are rung. This can be a value between 0 and 60. Setting this to 0 will cause CompletePBX to immediately start ringing the members of the follow-me list instead of trying to ring the primary extension first. As the primary extension can be included as a member of the follow-me list, this is often the desired behavior.



Take Care!

If the extension is defined as a fax recipient, you **must** ensure that the initial ring time defined here is at least as long as the Fax Detection Time. Otherwise the fax module will not have sufficient time to detect an incoming fax.

Ring Strategy drop-down menu allows the order in which the follow-me list members will be rung to be configured. There are 10 available ring strategies. The ring strategies in a follow-me route are identical to those used in a ring group. Please refer to the [Ring Groups](#) section of Chapter 4, for ring strategy definitions.

Ring Time (max 60 sec) configures the maximum number of seconds for which a phone will be rung before the call is considered failed. For hunt ring strategies, this is the number of seconds that each round of the hunt sequence will ring the appropriate phone.

Follow-Me List is the list of extensions that should be rung for this follow-me route. Extensions should be listed one per line. As with ring groups and queues, external numbers and extensions can be listed as long as they are suffixed with a pound (#) symbol, e.g.95551234567#

Extension Quick Pick drop-down menu lists all previously configured extensions on the system. Selecting an extension from this menu will place that extension into the **Follow-Me List**.

Announcement is the pre-recorded message that will be played to the caller before any of the Follow-Me List members are rung. This message can serve to inform the caller that several phones are being rung, or to ask them to be patient during the process (for example, "Please wait while the person you are trying to reach is located."). Recordings can be added in the CompletePBX **System Recordings** screen. (More information on System Recordings can be found in the [Voice Prompts](#) section of Chapter 8).

Play Music On Hold? dropdown menu allows a selection of the music-on-hold class to be played for the caller while they are waiting for all follow-me list members to be rung. Selecting **None** will play nothing while extensions are tried. Selecting **Ring** will play ringing instead of music on hold. Music classes can be defined in the **Music on Hold** screen. (More information on Music on Hold can be found in the [Music on Hold](#) section of Chapter 08).

CID Name Prefix allows text to be prepended to the caller ID name of all of the callers who pass through this follow-me route.

Alert Info allows custom text to be sent in the SIP *ALERT_INFO* headers for all calls that pass through this follow-me route. *ALERT_INFO* headers are often used to force a distinctive ring, or auto-answer on compatible SIP endpoints.

When **Confirm Calls** is enabled, then the person who answers a call from this follow-me route will be prompted to press **1** before the call will be bridged to their endpoint. Requiring the user to confirm

the call avoids scenarios in which mobile phones send the call to voicemail, CompletePBX counts the call as "answered", and bridges the caller to the mobile voicemail (when the call should be sent to the failover destination instead).

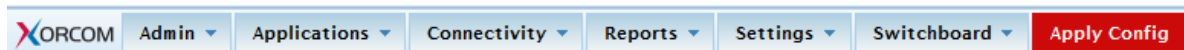
Remote Announce is used to select the message that will be played to the person who picks up a call from this follow-me route if **Confirm Calls** is enabled. This message should inform the person receiving the call that they have an inbound follow-me call and need to press *1* to accept it.

Too-Late Announce is the message played to the person receiving the call if they try to confirm a call (by pressing *1*), but someone else has already answered the call. This message should inform them that the call they were trying to accept has been answered by someone else.

Once the follow-me settings have been configured, select a call target for the call to failover to in the event that none of the listed extensions pick up:

In many cases, the failover destination will be the voicemail for the user account that this follow-me belongs to (but the destination can be any valid call target on the system).

Once all options are configured, click on the **Submit Changes** button and then click on the red-colored **Apply Config** button at the top of the screen.



VmX Locater

Connectivity → *Extensions*

The VmX Locater is a very simplified version of the default CompletePBX follow-me setup. These settings can be set and edited by the CompletePBX administrator, but if the locater is enabled for a user, then they will be able to change these settings themselves using **My Extensions**.

Note that the VmX Locater can work in conjunction with the CompletePBX follow-me routing, instead of replacing it entirely. The VmX Locater prompts are played when a caller would normally reach voicemail. At that point, the caller can be directed to press *0* for the operator, *1* to run through follow-me routing, and *2* for an optional additional extension.

To set up the VmX Locater in CompletePBX, navigate to the **Connectivity** menu and select either the **Users** or **Extensions** dialog. The dialog that is present will depend on the operational mode that CompletePBX is running in (DeviceAndUser or Extensions):

Click on the name of the user that requires VmX Locater configuration and scroll down to the bottom of the page to find the VmX Locater settings:

- VmX Locator

VmX Locator™ [?] Enabled ▾

Use When: [?] unavailable busy

Voicemail Instructions: [?] Standard Voicemail prompts.

Press 0: [?] Go To Operator

Press 1: [?] Send to Follow-Me

Press 2: [?]

To enable the **VmX Locator**, select **Enabled** in the first drop-down menu.

The **Use When** checkboxes allow the locator to be engaged when the called user is **unavailable**, **busy**, or both. Note that if neither checkbox is selected, the locator will never be engaged.

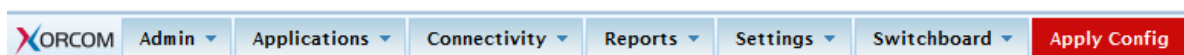
The **Voicemail Instructions** checkbox configures whether or not to play the standard CompletePBX voicemail prompts after the user's pre-recorded outgoing voicemail message. If this box is not selected, the user's message will be played and will be immediately followed by a beep. Otherwise, the standard prompts asking the caller to "please leave their message after the tone" will be played.

The **Press 0**, **Press 1**, and **Press 2** fields can be used to configure specific extensions, ring groups, queues, or external phones to be rung when the appropriate digit is pressed during playback of the outgoing voicemail message. When the VmX Locator is enabled, the associated user should re-record their voicemail prompts to ask the user to press one of these three digits, in order to route the call appropriately. External phone numbers used in these fields *do not* require pound symbols at the end of them.

The **Press 0** field can optionally be configured to redirect the caller to the PBX operator (defined in the **Voicemail** section of the **Settings/General** dialog) instead of a specific extension or phone number.

The **Press 1** field can optionally be configured to redirect the caller to the default CompletePBX follow-me settings for the user (if they have also been configured).

When all settings have been configured, click on the **Submit** button followed by the red-colored **Apply Config** bar to save the changes and make them live.



When the user is logged into **My Extension**, they can view and edit these settings by clicking on the **VmX Locator Settings** link in the navigation menu:

[Call Monitor](#)
[Voicemail](#)

[Fax](#)

[Feature Codes](#)
[Follow Me](#)
[Phone Features](#)

VmX™ Locator Settings

[Logout](#)

VmX Locator™ Settings for CEO (2020)

Use When: [?](#) unavailable busy

Voicemail Instructions: [?](#) Standard voicemail prompts.

Press 0: [?](#) Go To Operator

Press 1: [?](#) Send to Follow-Me

Press 2: [?](#)

Outbound Routes

Connectivity → Outbound Routes

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

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

To start setting up an outbound route, navigate to the **Connectivity** menu and select the **Outbound Routes** dialog. The **Add Route** page consists of configurable options and one "quick pick" drop-down menu used to populate certain fields as shown in the following screenshot:

Add Route

Route Settings

Route Name [?] :	<input type="text"/>	<input type="checkbox"/>
Route CID: [?]	<input type="text"/>	<input type="checkbox"/> Override Extension [?]
Route Password: [?]	<input type="text"/>	
Route Type: [?]	<input type="checkbox"/> Emergency <input type="checkbox"/> Intra-Company	
Music On Hold? [?]	default ▼	
Time Group: [?]	---Permanent Route--- ▼	
Route Position [?]	Last after Emergency ▼	

Additional Settings

Call Recording [?] :	Allow ▼
PIN Set [?] :	None ▼

Dial Patterns that will use this Route [?]

(prepend) + prefix | [match pattern / CallerID]

+ Add More Dial Pattern Fields

Dial patterns wizards [?]: (pick one) ▼

Trunk Sequence for Matched Routes [?]

0	<input type="text"/>
1	<input type="text"/>

Optional Destination on Congestion [?]

Normal Congestion ▼

Submit Changes

Duplicate Route

Route Name is just used to identify this route. This value cannot contain any spaces. The name is usually descriptive of the purpose of the route (for example, "local" or "international").

The **Route Password** field can be used to secure a route against unauthorized dialing. For example, a company may wish to restrict all long distance calls, or calls to 1-900 numbers. A numerical password can be placed in this field, or a direct path to a file containing a list of valid passwords (one password per line). When this field is not blank, all calls that pass through this outbound route will not be placed through any provider until the caller successfully enters a valid password.

The **PIN Set** field performs the same function as the **Route Password** field but uses previously created password sets. PIN sets can be configured in the CompletePBX **PIN Sets** screen (more

information on PIN Sets can be found in the [PIN sets](#) section of Chapter 8). If PIN sets are to be used, the **Route Password** field must be left blank. If both the **Route Password** field is left blank and the **PIN Set** field is set to **None**, callers will be able to use this route without authentication.

The **Emergency Dialing** checkbox is used to specify that the route will *only* be used for emergency calls. When this option is set, any calls that pass through this route will set their caller ID to the emergency CID setting of the device the call originated from (if set). Do not select this option if the route may sometimes route emergency calls. Only select this option if the route will *always* be used to route emergency calls.

If the **Intra Company** option is checked, then the caller ID of the device that initiated the call will be preserved instead of having the caller ID rewritten to whatever is specified by the trunk. This option should be used when an outbound route is directing calls to another VoIP system from the same company, and the call is not passing over public telephony routes.

The **Music On Hold?** dropdown menu allows a specific music-on-hold class to be selected for calls that pass through this outbound route. Once a call is placed through this route, the music that is heard anytime the call is placed on hold will be defined by the class selected in this field.

The **Dial Patterns** field is the heart of every outbound route. Specific numbers can be matched here (for example, 911 or 999). Otherwise, patterns can be specified using the characters in the following table:

Pattern	Description
X	Any whole number from 0-9
Z	Any whole number from 1-9
N	Any whole number from 2-9
[###]	Any whole number in the brackets. Note that multiple numbers can be separate by commas, and ranges of numbers can be specified with a dash ([1, 3, 6-8] would match the numbers 1, 3, 6, 7, and 8.
.	Matches one or more characters (acts as a wildcard). Note that this character is counted as part of the length of the pattern, so a pattern defined as XZZ. would match a pattern of numbers containing 4, or more, digits.

The **Trunk Sequence** drop-down menus are for configuring the order in which the trunks will be used when calls match the pattern specified in the **Dial Patterns** field. If the first trunk in the list is unavailable or congested, the call will fail over to the second trunk. This behavior will repeat until all listed trunks have been exhausted.

The **Dial patterns wizards** and **Trunk Sequence** fields are where the concept of **Least Cost Routing (LCR)** comes into play. LCR involves configuring each outbound route to send calls to the cheapest trunk first. This often involves setting up multiple outbound routes for similar styles of calls. For example, say that a CompletePBX system is configured with two SIP trunks—one from a provider that allows unlimited flat-rate calling to the state of New York and one from a provider that allows unlimited flat-rate calls to the state of California. It seems logical that calls to the New York area codes should be routed via the New York trunk and calls to the California area codes should be

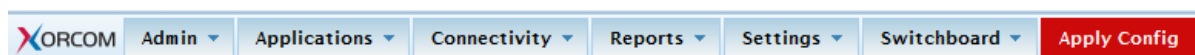
routed via the California trunk. However, with a single route to match US-format calls, all calls will prefer a single trunk first and charges will apply when calls could be free. In this case, it would make sense to create two outbound routes.

The first route would have a pattern that would match all calls for New York state area codes (dialed in both local and long-distance formats). The **Trunk Sequence** set of fields would list the New York trunk first and the California trunk second.

The second route would have a pattern that matches all calls for California state area codes (again, in both local and long distance formats). The **Trunk Sequence** set of fields would be reversed to have the California provider first and the New York provider second:

In this manner, when CompletePBX routes a call to either New York or California, it will attempt to use the cheapest route first. The end goal is that all users on the system should be able to dial a number just as they normally would, without having to worry about manually picking the cheapest line or dialing the call in a special way. Whenever they dial a number, the PBX is smart enough to dial it properly, using the most economical trunk.

Once trunk options have been configured, click on the **Submit Changes** button followed by the red-colored **Apply Config** bar at the top of the screen to make the new outbound route live.



A note about routes



It is extremely easy to forget about a particular type of call and not associate it with an outbound route.

Doing so can leave users stranded when they need to make an important call!

After you finish defining your outbound routes, test a sample of real destinations, and verify that you have configured your system to handle all of them.

Be sure to include methods to dial the following types of calls:

- **Emergency:** Dedicate a route just for this purpose. Calls for emergency services should never be mangled by another dial pattern.
- **Local:** Calls to local numbers (usually NXXXXXXXXX).
- **Toll-free:** Calls to toll-free numbers (such as 1-888 or 1-800 numbers)
- **Mobiles:** Ensure that your outbound routes have been configured to handle calls to all mobile phone providers.
- **International:** Calls outside of the country, if permitted (usually 011)
- **Special: Calls** that do not fit any other category. This includes calls such as calls to the operator (0) and directory assistance (411)
- **Long distance:** Calls outside of the local calling area, if permitted (usually 1NXXXXXXXXX). Make sure that your outbound routes are designed to properly handle calls if you are using a dedicated provider for international calls.

Routing Groups

Connectivity → *Routing Groups*

Routing Groups enable you to create groups of outbound routes so that only extensions that are members of the Routing Group can access outbound routes that are linked to the Routing Group.

If you create a Routing Group which does not have access to any outbound routes, then extensions that belong to that Routing Group will not have access to any outbound route, and will not be able to make external calls. Even though you may want to block an extension from making external calls, you may still want to allow the extension to make emergency calls. You should create a dedicated outbound route only for emergency calls, and ensure that all Routing Groups include the emergency outbound route.

Available Outbound Routes lists all the outbound routes that are currently defined in your CompletePBX system that have not yet been enabled for the current Routing Group.

Enabled Outbound Routes shows the outbound routes that you want to allow members of the Routing Group to use.

Routing Groups

Only for Visitors

Delete Only for Visitors

Enabled Outbound Routes

Emergency

Available Outbound Routes

Local
International
National
Cellular



Submit

Creating a Routing Group

Click on the **Add Route** button to create a new Routing Group, or select an existing Routing Group if you want to make modifications.

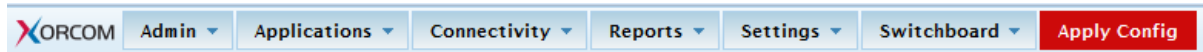
Give a meaningful name to the new Routing Group. To improve readability, the name can include spaces.

To link outbound routes to a Routing Group, simply select one or more items from the list of available outbound routes, and click on the arrow pointing to the list of enabled outbound routes.

The order in which the outbound routes appear in the list of enabled outbound routes determines the order in which routes will be used. To change the order in which the outbound routes will be

used, select an item from the table of enabled outbound routes that you want to move, and use the up/down arrows below the table to change to position of the selected item.

Once Routing Groups have been configured, click on the **Submit Changes** button followed by the red-colored **Apply Config** bar at the top of the screen.



Summary

By this point, our CompletePBX system should be routing calls! This chapter discussed setting up inbound routes to match against the number that was dialed and the number that the caller is dialing from. Inbound calls can also be run against a follow-me route or a VmX Locator route in order to attempt to find a user who is not at their desk phone. Our CompletePBX system should also be able to detect and route inbound faxes, should any fax come through our trunks. In addition, outbound calls will now be routed properly using the most economical routes.

The next chapter will discuss taking all those calls that are now running through our system and recording them for playback later.

7. Recording and Listening to Calls

CompletePBX has a wonderful, built-in ability to record calls. No additional software is required to make this happen. When CompletePBX records a call, both sides of the call are recorded and written out to a file for playback on a computer. Call recording is often performed in call centers to ensure call quality, or to keep calls for later review, should the need arise. CompletePBX provides the ability to record all of the calls, or to selectively record calls.

Refer to the [Managing Call Recordings in CompletePBX](#) article on the Xorcom wiki for some suggestions for managing the space used to store recordings.

In this chapter, we will discuss the following:

- General recording options
- Recording calls to extensions
- Recording calls to queues
- Recording calls to conferences
- Maintaining call recordings

Know the law!



Before enabling call recording, make sure that you are aware of the legalities surrounding call recordings and privacy laws.

Call recordings are prohibited in certain places, unless the caller is told that the call will be recorded. For example, in the state of California all of the parties on the call must consent to the call being recorded before it begins.

Recording Formats

CompletePBX allows calls to be recorded in the following formats:

- WAV
- WAV49
- ULAW
- ALAW
- SLN
- GSM

Each format has its own ratio of file size to recording quality, and certain formats will not play on all of the computers. A comparison between all of the available formats is as follows:

Format	Description
WAV	<p>Uncompressed WAV format recording.</p> <p>Sound quality will be very good, but the file will be very large in size (roughly 1 megabyte per minute of the recording).</p> <p>WAV format recordings are natively playable on nearly all of the computers without additional software</p>

Format	Description
WAV49	<p>WAV format recorded using the GSM codec. As GSM is a compressed codec, the sound quality is compromised.</p> <p>Sound quality on a GSM recording is usually equivalent to the quality that is achieved during mobile telephone calls.</p> <p>File size is much smaller than a standard WAV (roughly 100 kilobytes per minute of the recording)</p> <p>WAV49 files are often difficult to play on computers without additional software that understands the GSM codec</p>
ULAW or ALAW	<p>G.711 codec recording.</p> <p>The recording quality is excellent, and should sound exactly like the call did to all of the parties who were on the original call.</p> <p>File size is very large (similar to the WAV format at about 1 megabyte per minute).</p> <p>ULAW and ALAW recordings are very difficult to play on most computers. There are very few computers that will play the recording without additional software that understands the G.711 codec</p>
SLN	<p>CompletePBX native SLINEAR format.</p> <p>Recordings that are in SLN format will have the same quality and file size as WAV recordings. SLN recordings are raw WAV, little endian 16-bit signed linear (PCM) format recordings.</p> <p>Most computers will play these files, although some software packages refuse to play them unless the extension is renamed to .wav from .sln</p>
GSM	<p>GSM codec recording.</p> <p>As with WAV49 calls, the quality of GSM recordings is less than that of ULAW/ALAW or WAV calls, but is generally acceptable for most purposes.</p> <p>GSM recordings weigh in at around 100 kilobytes per minute</p>

Transcoding During Recording

One very important aspect of call recording to keep in mind is that if the recording uses a different codec than the original call, transcoding must occur. For example, a call that uses the G.711 ULAW codec that is being recorded using the WAV49 format will need to be transcoded into the GSM codec before being saved. Transcoding recordings place additional load on a server's disk I/O and processor resources. On high traffic systems, it is possible to max out all of the available resources if the transcoding recordings are not accounted for.

In general, the rule of thumb for recording will be the same as it is for selecting the codec that a trunk or extension will use: try to make everything match. If all of the calls are using the GSM codec, then it would be safe to record those calls in the GSM format. A system that has all of the calls in G.711 ULAW format would be put under an unnecessary amount of stress to record in GSM format. If transcoding is required (for example, limited disk space dictates the use of GSM recordings), be

sure to size the resources of the system accordingly in order to allow the additional load.

General Call Recording Options

Settings → Advanced

CompletePBX has several settings that govern the global operation of call recording. These settings determine if call recording should be globally enabled or disabled, which format to record calls in, and a command to run after a call has been recorded (if desired).

In order to access the global options, navigate to the **Settings** menu and select the **Advanced** dialog.

The **Call recording format field** in the **System Setup** section allows us to change the format of the call in which it will be stored. The default value is **wav**, but can be changed to **WAV** (WAV49—a GSM file stored as a **wav**), **ulaw**, **alaw**, **sln**, **gsm**, and **g729**. More information on recording formats can be found earlier in this chapter in the [Recording Formats](#) section.

Recording Calls

CompletePBX can be configured in order to record calls to a particular extension, queue, or conference. If a call encounters a request to initiate recording twice (for example, a caller enters a queue that is being recorded and the agent who picks up has set up their extension to record all of the calls), the call will only be recorded once. The call will be recorded by the target that first answered the call. In the previous example, the queue would record the call as the queue answered the call before the extension did.

If a call encounters conflicting recording instructions (for example, a caller enters a queue that is being recorded, but the agent who picks up has set up their extension to never record calls), the call will still be recorded. The target that has recording enabled will record the call. It is important to note that there is no way to stop a call from being recorded if it utilizes a call target that is set up to always record calls.

Recording Calls for Extensions

Connectivity → Extensions or Connectivity → Users

CompletePBX allows all of the calls to a particular user to be recorded, or for calls to be selectively recorded. CompletePBX allows the choice between recording only incoming calls, only outgoing calls, or both.

In order to set up call recording for a particular user, navigate to the **Connectivity** menu and select **Users** or **Extensions** dialog (this depends on the operational mode in which CompletePBX is running. More information on setting up users/extensions can be found in Chapter 2, **Devices and Extensions**).

Click on the name of the user you wish to edit and scroll down to the **Recording Options** section:

- Recording Options

Inbound External Calls [?]	Always	Don't Care	Never
Outbound External Calls [?]	Always	Don't Care	Never
Inbound Internal Calls [?]	Always	Don't Care	Never
Outbound Internal Calls [?]	Always	Don't Care	Never
On Demand Recording [?]	Disable	Enable	
Record Priority Policy [?]	0 ▾		

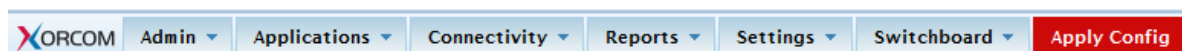
The Record Incoming and Record Outgoing settings can be configured as Always, Don't Care, or Never.

When the **Don't Care** option is selected, the user can dial *1 during a call to start recording the call. *1 can be dialed again to stop recording the call. The on demand toggle only lasts for the current call. In order to record the next call, the user would have to dial *1 again.

If these options are set to **Always**, then all of the calls in the selected direction will be recorded. When **Always** is selected, pressing *1 will *not* stop call recording.

If these options are set to **Never**, then no calls in the selected direction will be recorded. When **Never** is selected, pressing *1 will *not* start recording.

Be sure to click on the **Submit** button, followed by the red-colored **Apply Config** bar at the top of the screen in order to save any changes made to the recording settings.



Recording Calls for Queues

Applications → *Queues*

All the calls to a particular queue can be recorded. This is often used on larger call queues for later call review by management, or to resolve disputes about what was said on a particular call. In order to record all of the calls that are picked up out of a particular queue, navigate to the **Applications** menu and select the **Queues** dialog.

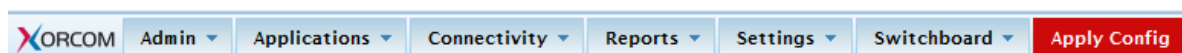
Click on the name of the queue in the menu on the right, which needs call recording enabled:

Under the **General Queue Options** section, the **Call Recording** drop-down menu can be changed from **No** to **wav49**, **wav**, or **gsm**.

General Queue Options

Ring Strategy: [?]	ringall
Autofill: [?]	<input type="checkbox"/>
Skip Busy Agents: [?]	No
Queue Weight: [?]	0
Music on Hold Class: [?]	inherit
Ringing Instead of MoH: [?]	<input type="checkbox"/>
Join Announcement: [?]	None
Call Recording: [?]	No
Recording Mode: [?]	wav49
Caller Volume Adjustment: [?]	wav
Agent Volume Adjustment: [?]	gsm
Mark calls answered elsewhere: [?]	No
	<input type="checkbox"/>

Select the desired recording format, click on the **Submit Changes** button, and click on the red-colored **Apply Config** bar in order to enable recording on the queue.



Note that queues tend to have a high volume of calls. It is important to select an appropriate call recording format, and to ensure that recordings are maintained and cleaned up periodically. More information on recording formats can be found earlier in the [Recording Formats](#) section of this chapter. Recording maintenance is discussed later in this chapter in the [Monitoring Call Recordings](#) section.

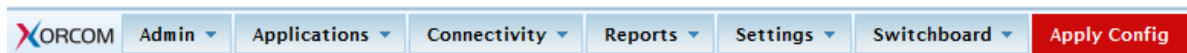
Recording Calls for Conferences

Applications → Conferences

All of the calls to a particular conference room can be recorded. All of the members of the conference will be recorded and merged into a single file. In order to enable call recordings for a particular conference, navigate to the **Applications** menu and select the **Conferences** dialog.

Select the conference room that should have recording enabled from the menu on the right. Under **Conference Options**, the **Record Conference** drop-down menu will turn recording on or off:

Selecting **Yes** will record the entire conference (from the time the first member joins) in WAV format (more information on the WAV format can be found earlier in this chapter in the [Recording Formats](#) section). Selecting a different format to record the conference in is not currently supported. Once **Yes** has been selected from the **Record Conference** drop-down menu, click on the **Submit Changes** button followed by the red-colored **Apply Config** button in order to enable call recordings for the conference.



Maintaining Call Recordings

It is worth noting that call recordings can be quite large. If left unattended, a PBX that automatically records all of the calls could fill up the entire available hard disk space and prevent CompletePBX from processing calls. It is important to have a maintenance strategy for dealing with call recordings in order to avoid this.

G.729 Implementation Guidelines

[G.729](#) is one of the most popular voice compression protocols used in IP telephony. This is due to the fact that G.729 reduces the bandwidth usage for a standard telephone call from 80 kilobits per second (kbps) to 24 kbps, with minimal voice quality degradation¹.

While in the past the G.729 algorithm ran on dedicated Digital Signal Processors ([DSP](#)), today's processors can easily run the G.729 algorithm effectively while addressing other tasks as well.

This section describes how to add the open G.729 codec to Xorcom's IP-PBX appliances:

Conversion Times Based on Compression Method

G.729 requires CPU resources. The [tables at the end of this document](#) show the conversion time (using different compression methods) that can be achieved by each member of Xorcom's IP-PBX family.

Methods for Obtaining the G.729 Codec

There are two ways to obtain the G.729 codec for an Asterisk-based IP-PBX:

- [Buy the licenses from Digium](#)
- Install the Open Source version

Both codec versions provide the same performance, but in case of the Open Source version you undertake the responsibility for payment of the license fee. The legal aspects of using the Open Source version of the G.729 codec are discussed in the following article: <http://voip-info.org/wiki/view/Asterisk+G.729+Licensing>

Installing the Open Source G.729 Codec

To install the Open Source implementation of G.729 codec on CompletePBX, perform the following actions:

- Download the codec binary file from http://asterisk.hosting.lv/bin/codec_g729-ast14-gcc4-glibc-pentium4.so
- Copy it to the `/usr/lib/asterisk/modules` folder.
- Restart the Asterisk with either `/etc/init.d/asterisk restart` or `amportal restart` command

Estimating Number of G.729 Channels Required

If you choose to purchase the G.729 license from Digium you will need to compute the number of G.729 channels required by your configuration.

You can estimate the required value by using the following information:

- A call between two SIP extensions usually requires two G.729 channels, unless the pass-thru mode is used (<http://voip-info.org/wiki/view/Asterisk+G.729+pass-thru>), in which case it doesn't require a G.729 channel.
- A call between a SIP extension and a Zaptel/DAHDI extension/trunk requires one G.729 channel.
- A call to Voice Mail or another Asterisk service where IVR messages must be played requires one G.729 channel.

Typical Translation Time between Formats: XR3000

The following table contains the values of typical translation time between formats (in milliseconds) for one second of data source format (rows) to destination format (columns) in the Xorcom XR3000 IP-PBX appliance:

Source Format	Destination Format												
	G723	GSM	μ -law	a-law	G726-aal2	ADPCM	SLIN	LPC10	G729	Speex	iLBC	G726	G722
G723	-	-	-	-	-	-	-	-	-	-	-	-	-
GSM	-	-	2	2	2	2	1	3	5	13	-	2	-
μ -law	-	5	-	1	2	2	1	3	5	13	-	2	-
a-law	-	5	1	-	2	2	1	3	5	13	-	2	-
G726-aal2	-	5	2	2	-	2	1	3	5	13	-	1	-
ADPCM	-	5	2	2	2	-	1	3	5	13	-	2	-
SLIN	-	4	1	1	1	1	-	2	4	13	-	1	-
LPC10	-	5	2	2	2	2	1	-	5	13	-	2	-
G729	-	5	2	2	2	2	1	3	-	13	-	2	-
Speex	-	6	3	3	3	3	2	4	6	-	-	3	-
iLBC	-	-	-	-	-	-	-	-	-	-	-	-	-
G726	-	5	2	2	2	2	1	3	5	13	-	-	-
G722	-	-	-	-	-	-	-	-	-	-	-	-	-

Typical Translation Time between Formats: XR2000

The following table contains the values of typical translation time between formats (in milliseconds) for one second of data source format (rows) to destination format (columns) in the Xorcom XR2000 IP-PBX appliance:

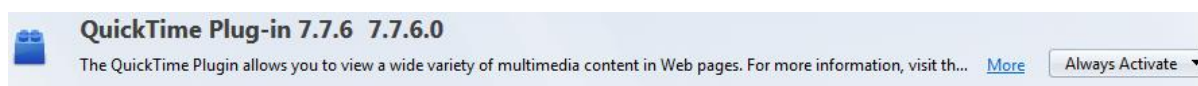
Source Format ⬇	Destination Format												
	G723	GSM	μ -law	a-law	G726-aal2	ADPCM	SLIN	LPC10	G729	Speex	iLBC	G726	G722
G723	-	-	-	-	-	-	-	-	-	-	-	-	-
GSM	-	-	3	3	4	3	2	6	11	25	-	4	-
μ -law	-	6	-	1	3	2	1	5	10	24	-	3	-
a-law	-	6	1	-	3	2	1	5	10	24	-	3	-
G726-aal2	-	7	3	3	-	3	2	6	11	25	-	1	-
ADPCM	-	6	2	2	3	-	1	5	10	24	-	3	-
SLIN	-	5	1	1	2	1	-	4	9	23	-	2	-
LPC10	-	8	4	4	5	4	3	-	12	26	-	5	-
G729	-	7	3	3	4	3	2	6	-	25	-	4	-
Speex	-	8	4	4	5	4	3	7	12	-	-	5	-
iLBC	-	-	-	-	-	-	-	-	-	-	-	-	-
G726	-	7	3	3	1	3	2	6	11	25	-	-	-
G722	-	-	-	-	-	-	-	-	-	-	-	-	-

Listening to Voice Recordings

Prerequisites

You have to ensure that your web browser (whether it be Firefox, Chrome, or something else) can play your voice recordings. The default format for voice recordings is .wav, so you need to ensure that your browser has a suitable addon to play voice recordings in this format. Quicktime provide a plugin that is compatible with Firefox (Quicktime Plug-in), or an extension for Chrome (Quicktime for Chrome).

In both cases, ensure that the addon is configured to always allow activation. You can configure this In Firefox by changing the default setting from “Ask to Activate” to “Always Activate”





Accessing Voice Recordings

Voice recordings can be accessed from two different locations in CompletePBX.

The CompletePBX administrator can access voice recordings in the Administration GUI from the **CDR Reports – Basic** sub-menu in the **Reports** menu. Use the Call Detail Record Search to find calls. Any call that is recorded will display an icon in the Recording column. Clicking on this icon will play the selected voice recording to your default speakers.

Call Detail Record - Search Returned 12 Calls

Call Date	Recording	System	CallerID	Outbound CallerID	DID	App	Destination	Disposition	Duration	Userfield	Account
2014-12-10 11:24:17		1418203457.5	"Keith - Demo" <2941>			VoiceMail	vmu2002	ANSWERED	00:21		2941
2014-12-10 11:24:02		1418203447.4	"Keith - Demo" <2941>			Wait	*65	ANSWERED	00:09		2941
2014-11-23 18:08:53		exten-2001-2941-20141210-112417-1418203457.5.wav	"Keith - Demo" <2941>			Wait	*97	ANSWERED	00:01		2941
2014-09-16 16:13:31		1410873211.29	"Keith - Demo" <2941>			VoiceMailMain	*97	ANSWERED	00:32		
2014-09-16 15:40:02		1410871202.28	"Keith - Demo" <2941>			VoiceMailMain	*97	ANSWERED	00:13		
2014-09-16 14:30:01		1410867001.27	"Keith - Demo" <2941>			Hangup	*97	ANSWERED	00:28		
2014-08-13 14:57:36		1407931056.25	"Keith - Demo" <2941>			Dial	1011	NO ANSWER	00:12		
2014-08-13 14:55:59		1407931012.22	"Keith - Demo" <2941>			Dial	1011	NO ANSWER	00:10		

Extension users can access their own voice recordings (and only their own recordings) from **My Extension**. Login to **My Extension** by using your extension number in the **Login** field and your voicemail password in the **Password** field, and then clicking **Submit**.

Login

Login: *
 Password: *



Once you have access, click on **Call Monitor** from the left-hand menu. A table of all your calls will be displayed. Any calls that were recorded will display two icons in the Monitor column.

Clicking on the first icon (which looks like a loudspeaker) will play the selected voice recording to your default speakers. Clicking on the second icon will allow you to download the voice recording to your machine, so that you can use it on your machine. For example, you could attach it to an email and send it to the person with whom you were talking as record of your conversation or meeting.

Call Monitor for Keith - Demo (2941)

Results 12

select: all none

	Date ▼	Time	Caller ID	Source	Destination	Duration	Monitor
<input type="checkbox"/>	2014-12-10	11:24:17	"Keith - Demo" <2941>	2941	vmu2002	21 sec	 
	2014-12-10	11:24:02	"Keith - Demo" <2941>	2941	*65	9 sec	
	2014-11-23	18:08:53	"Keith - Demo" <2941>	2941	*97	1 sec	
	2014-09-16	16:13:31	"Keith - Demo" <2941>	2941	*97	32 sec	

Summary

By now, we have learned how to record any call that enters our PBX, if we choose to do so. We now know of the importance of maintaining our recordings so that they do not fill up the hard disk on our

PBX, and we are able to create some basic scripts to accomplish recording maintenance (with a little help from cron).

The next chapter will focus on personalizing our PBX by changing the default music on hold, recording custom voice prompts, and customizing feature codes/star codes.

8. Personalizing your PBX

By now, we have a working PBX. It's time to make the PBX our own. CompletePBX allows for several options to customize the way our call structures sound. In this chapter, we will discuss how to:

- Upload our own custom music that will be played when callers are placed on hold
- Record custom voice prompts to answer incoming calls automatically
- Customize star codes that users will dial to activate various features
- Set up automated callback systems
- Configure Direct Inward System Access (DISA) to give remote agents a dial tone
- Configure customer caller ID lookup sources to properly identify incoming callers
- Configure PIN sets for increased security
- Configure custom applications
- Configure custom destinations

Music on Hold

Customization

Applications → Music On Hold

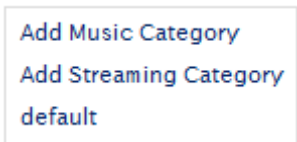
CompletePBX allows two styles of music-on-hold customization—static files and streaming. Static files are audio files (such as WAV or MP3 files) that are uploaded to the CompletePBX server and played back when a caller is placed on hold. Streaming audio is used to connect to a live audio feed from a particular source. Typically, this would be an Internet stream (many radio stations broadcast over the Internet), but it could also be a stream from a sound card or some other audio device.

CompletePBX separates different groups of music on hold into categories. Different static file categories can contain different sets of files. Each streaming category can only contain one audio stream. Music-on-hold categories can be applied to inbound routes (so that all calls that match the route will hear that category) as well as to queues and ring groups. Categories assigned at the call target level will override the music-on-hold category for that particular target only. Once a call leaves that target it will fall back into the music-on-hold category specified in the inbound route, which it was matched against.

Using Audio Files

Applications → Music On Hold

In order to create a music-on-hold category using static audio files, navigate to the **Applications** menu and select the **Music On Hold** dialog. Click on the **Add Music Category** link in the menu on the right:



Add Music Category
Add Streaming Category
default

The initial setup screen for a static file category has one only field as shown in the following screenshot:

On Hold Music

Add Music Category

Category Name:

Submit Changes

Type a name for the category in the textbox and click on the **Submit Changes** button. On the resulting screen, click on the **Browse** button to find an MP3 or WAV file for upload, and then click on the **Upload** button. The quality of the files is not terribly important, as CompletePBX will downsample everything it gets to mono 8 kHz, 8 bits-per-sample, ULAW format.

On Hold Music

Category: default

Upload a .wav or .mp3 file:

Browse... **Upload**

Volume 100% ▾ Volume Adjustment [?]

Enable Random Play

After clicking on the **Upload** button, CompletePBX will display a warning as shown in the following screenshot:

Please wait until the page loads. Your file is being processed.

OK



Warning!

After you click on the OK button, the page will still be loading. With larger files or slower connections, it can take several minutes for the page to load. Navigating to a new page before the page has finished loading will result in an incomplete upload and a corrupted music-on-hold file that will not function correctly.

Once the page has finished loading, the music file that was uploaded will be present as shown in the following screenshot:


On Hold Music

Category: default

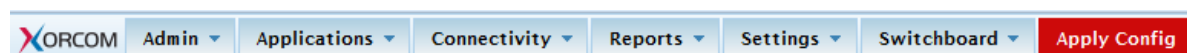
Upload a .wav or .mp3 file:

Volume 100% ▾ Volume Adjustment [?]

Completed processing Kalimba.mp3!

wav_Kalimba.wav 

Click on the **Submit Changes** button followed by the red-colored **Apply Config** button in order to save your configuration:



The music category is now ready for use (although it will only have one music file in it that will be played over and over again). Repeat the upload process for as many additional files as you would want to add. Music files will be played in the order in which they are uploaded unless random play is enabled. By clicking on the **Enable Random Play** button, the songs are played to the caller in a random order.

Using Audio Streams

Applications → Music On Hold

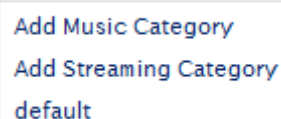
Using an audio stream for music on hold is a bit more complicated than using static audio files, and the results can be somewhat unpredictable depending on the source and type of the stream. Nonetheless, it is definitely possible to set up a live stream as a music-on-hold category. The only restriction CompletePBX imposes on the music stream is that it must be a mono 8 kHz, 8 bits-per-sample, ULAW audio stream. Most streaming audio programs support converting their streams to a new output format on the fly.

A streaming music-on-hold class can negatively affect the performance of a PBX due to bandwidth usage or transcoding issues. Each streaming class should be streamed only once at any given time (if multiple callers are placed on hold, all of them will be connected to the same stream). However, if multiple streaming classes are created, it is possible for multiple streams to be active at the same time. Each active stream can take up a significant amount of bandwidth (standard online broadcasts usually run at the speed of 96 kbps or 128 kbps). It is important to take bandwidth usage into account

when planning a system.

In addition to bandwidth issues, a streaming music-on-hold class may require transcoding to be played to a caller. CompletePBX requires that the a stream be in ULAW format, so calls already using the G.711 ULAW codec will be able to listen to the stream without any transcoding. A call that is using a compressed codec such as G.729 would force the stream to be transcoded for the caller to hear it. Not only does this place additional processing load on CompletePBX, but it also requires an additional G.729 license for the concurrent caller that the stream has to be transcoded for. If there are few processor resources available or the available codec licensing will be a problem, it may be beneficial to avoid streaming music on hold all together.

In order to create a streaming music-on-hold category, navigate to the **Applications** menu and select the **Music On Hold** dialog. Click on the **Add Streaming Category** link in the menu on the right:

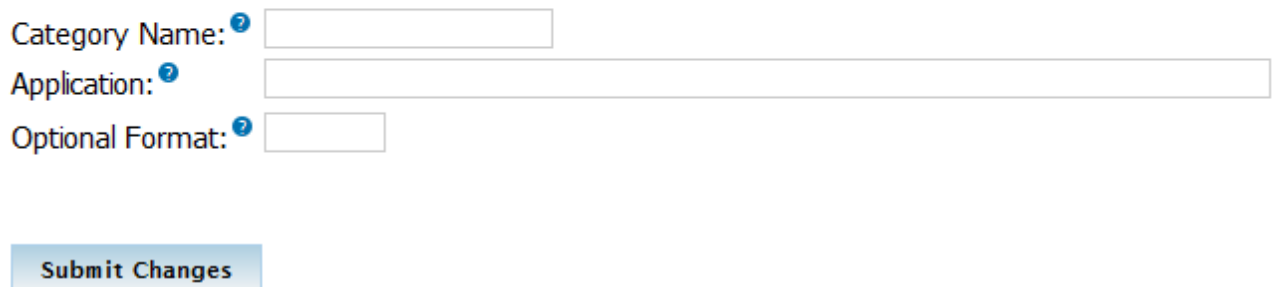


A screenshot of a menu with three items: "Add Music Category", "Add Streaming Category", and "default". The "Add Streaming Category" item is highlighted with a blue background.

The streaming category setup screen has three fields as shown in the following screenshot:

On Hold Music

Add Streaming Category



A screenshot of a web form titled "Add Streaming Category". It contains three input fields: "Category Name:" with a small question mark icon, "Application:" with a small question mark icon, and "Optional Format:" with a small question mark icon. Below the fields is a blue button labeled "Submit Changes".

The **Category Name** is a name for the streaming class, which will be used as a reference to the stream when selecting it wherever it is used in your call trees.

The **Application** field is likely to be the most complicated one that CompletePBX asks for. The value in this field is the program or script that CompletePBX will invoke in order to start "listening" to the stream. For RAW TCP streams, the built-in streamplayer application can be used in the format of `/usr/sbin/streamplayer server port`. However, this will only work for RAW TCP streams, and will not play icecast or shoutcast streams.

In order to play icecast or shoutcast streams, a shell script is typically written, which is invoked by CompletePBX. The shell script will use a combination of various audio programs to start the stream, convert it to an acceptable format, and then feed it to CompletePBX. For example, the following script called `streamicecast.sh` uses `ogg123` to start a stream from `icecastserver.net` and uses `sox` to

convert the stream to the required format:

```
#!/bin/bash
# /usr/bin/streamicecast.sh
# Streams icecast feed from icecastserver.net for use
# with CompletePBX
/usr/bin/ogg123 -q -b 128 -p 32 -d wav -f - http://icecastserver.net/ sox -r 16000 -t wav - -r
8000 -c 1 -t raw - vol 0.25
```

Then, we would just simply have to put `/usr/bin/streamicecast.sh` in the **Application** field.

The **Optional Format** field is used to tell CompletePBX the format of the stream. This must be a format that CompletePBX understands (such as ULAW or GSM). For the most part, it is safest to leave this field blank and force the stream to the proper ULAW format.

Click on the **Submit Changes** button followed by the red-colored **Apply Config** button in order to save your configuration:



Voice Prompts

Admin → System Recordings

Voice prompts are played to a caller when the caller enters an IVR, a follow-me, a ring group, or anywhere else they might be prompted for input. The purpose of a prompt is to instruct the user what to do. This is usually something as simple as, "Thank you for calling Packet Publishing. Press 1 for sales, 2 for publishing, or an extension at any time."

Recording Voice Prompts

CompletePBX provides a simple method for recording new voice prompts right from a telephone handset.

To record a new script, navigate to the **Admin** menu and select the **System Recordings** dialog, and click on the **Add Recording** link in the menu on the right.

The **Add Recording** screen provides two methods to add system recordings to CompletePBX:

- Uploading existing audio files
- Recording new audio files via a VoIP endpoint

System Recordings

Add Recording

Step 1: Record or upload

If you wish to make and verify recordings from your phone, please enter your extension number here:

Alternatively, upload a recording in any supported asterisk format. Note that if you're using .wav, (eg, recorded with Microsoft Recorder) the file **must** be PCM Encoded, 16 Bits, at 8000Hz:

Step 2: Name

Name this Recording:

Click "SAVE" when you are satisfied with your recording

Add Recording
Built-in Recordings
followme_announcem
ent
StandardBusinessHo
ursGreeting

To record a new prompt, enter the extension of the endpoint from which you will be recording into the extension number box and click on the **Go** button. The screen will change to reflect that an extension has been entered:

Uploading an existing recording is done in the same way in which a static music file is uploaded to a music-on-hold category (click on the **Browse** button, select the desired file, and click on the **Upload** button).

In order to record a new prompt, dial *77 on the extension that was entered and begin speaking after the beep. Hang up when recording is complete. To review the recording, dial *99 from the extension that was entered. Repeat this process until you are satisfied with the recording.

Enter a name for the recording in the **Name this Recording** box. Note that the name can only contain letters and numbers, not spaces and special characters (for example, the characters that may not be used include " , - , + , = , * , & , ^ , % , \$, # , @ , !).

Click on the **Save** button when you have finished recording. The recording will show up in the menu on the right.

Merging Existing Voice Prompts

Admin → System Recordings

CompletePBX also allows existing voice prompts to be merged together. A merged prompt will be played as a single, continuous file. To merge prompts, navigate to the **Admin** menu and select the **System Recordings** dialog, and click on the **Built-in Recordings** link in the menu on the right.

The **Built-in Recordings** screen has a single drop-down menu. Select the recording you wish to start with as the base recording from this menu, and click on the **Go** button as shown in the following screenshot:

System Recordings


Built-in Recordings

Select System Recording:

The **Edit Recording** screen will be shown as follows:

System Recordings

Edit Recording




 **Remove Recording** *(Note, does not delete file from computer)*




Change Name [?]

Descriptive Name [?]

Direct Access Feature Code Not Available [?]:

Files:


The **Change Name** changes the name of the recording. The name should be changed to distinguish the merged recording with the original recording.

The value of the **Descriptive Name** field is displayed as a hint to what the recording contains when it is being selected in places such as queues and IVRs.

The **Files** drop-down menus are where individual recordings are selected to be merged. Select a recording from the second drop-down menu and click on the **Save** button to add it to the merged recording. This can be done many times to include several recordings as shown in the following screenshot:

System Recordings

Edit Recording







 **Remove Recording** *(Note, does not delete file from computer)*

Change Name [?]

Descriptive Name [?]

Direct Access Feature Code Not Available [?]:

Files:

<input type="text" value=".asterisk-core-sounds-en-gsm-1.4.21"/>			
<input type="text" value=".asterisk-extra-sounds-en-gsm-1.4.9"/>			

Clicking on the arrow buttons will move a recording up or down, changing the order in which it will be played; clicking on the garbage buttons will remove a recording from the merged recording.

You must make sure to click on the **Save** button after making any of the changes.

Feature Codes

Admin → *Feature Codes*

Feature codes are “extensions” that users can dial to enable or disable certain features for themselves. Feature codes are typically prefixed with an asterisk (*) sign followed by two numbers. The feature codes on a CompletePBX system can be altered to use a different extension or disabled.

To customize feature codes, navigate to the **Admin** menu and select the **Feature Codes** dialog:

All the available features codes will be displayed, ordered by sections, as shown in the following screenshot:

Feature Code Admin

		Use Default?	Feature Status
Blacklist			
Blacklist a number	*30	<input checked="" type="checkbox"/>	Enabled ▾
Blacklist the last caller	*32	<input checked="" type="checkbox"/>	Enabled ▾
Remove a number from the blacklist	*31	<input checked="" type="checkbox"/>	Enabled ▾
Call Forward			
Call Forward All Activate	*72	<input checked="" type="checkbox"/>	Enabled ▾
Call Forward All Deactivate	*73	<input checked="" type="checkbox"/>	Enabled ▾
Call Forward All Prompting Deactivate	*74	<input checked="" type="checkbox"/>	Enabled ▾
Call Forward Busy Activate	*90	<input checked="" type="checkbox"/>	Enabled ▾
Call Forward Busy Deactivate	*91	<input checked="" type="checkbox"/>	Enabled ▾
Call Forward Busy Prompting Deactivate	*92	<input checked="" type="checkbox"/>	Enabled ▾
Call Forward No Answer/Unavailable Activate	*52	<input checked="" type="checkbox"/>	Enabled ▾
Call Forward No Answer/Unavailable Deactivate	*53	<input checked="" type="checkbox"/>	Enabled ▾
Call Forward Toggle	*740	<input checked="" type="checkbox"/>	Enabled ▾
Call Waiting			
Call Waiting - Activate	*70	<input checked="" type="checkbox"/>	Enabled ▾
Call Waiting - Deactivate	*71	<input checked="" type="checkbox"/>	Enabled ▾

To change the “extension” that a feature code uses, uncheck the **Use Default?** and type in the new “extension” that should be used as shown in the following screenshot:

Blacklist			
Blacklist a number	*29	<input type="checkbox"/>	Enabled ▾
Blacklist the last caller	*32	<input checked="" type="checkbox"/>	Enabled ▾
Remove a number from the blacklist	*31	<input checked="" type="checkbox"/>	Enabled ▾

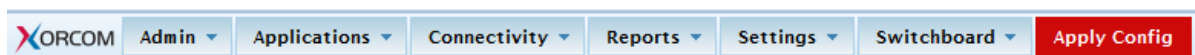
To disable a feature code entirely, change the drop-down value from **Enabled** to **Disabled** as shown

in the following screenshot:

Blacklist

Blacklist a number	<input type="text" value="*29"/>	<input type="checkbox"/>	Disabled ▾
Blacklist the last caller	<input type="text" value="*32"/>	<input checked="" type="checkbox"/>	Enabled ▾
Remove a number from the blacklist	<input type="text" value="*31"/>	<input checked="" type="checkbox"/>	Enabled ▾

Click on the **Submit Changes** button followed by the red-colored **Apply Config** button in order to save your configuration:



Callback

Applications → Callback

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

In order to set up a callback target, navigate to the **Applications** menu and select the **Callback** dialog.

Callback targets have only four configuration options:

- Callback Description
- Callback Number
- Delay Before Callback
- Destination after Callback

Add Callback

Add Callback

A callback will hang up on the caller and then call them back, directing them to the selected destination. This is useful for reducing mobile phone charges as well as other applications. Outbound calls will proceed according to the dial patterns in Outbound Routes.

Add Callback

Callback Description:

Callback Number:

Delay Before Callback:

Destination after Callback:

== choose one ==

Submit Changes

The **Callback Description** field is used to set a name to refer to this callback configuration whenever call targets are being selected in our call trees.

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

Test thoroughly

Test the callback dialog thoroughly if the Callback Number field is left blank.



Many mobile phones have their caller ID show up as "unknown" or "unavailable" when calls are placed to landline telephone services. If a caller with an unknown caller ID number initiates a callback, the callback will silently fail without any notification to the caller.

If there is no way for a caller to send caller ID information, then a callback target will only be useful to that person if it calls them back at a specific predefined telephone number.

Entering a number into the **Delay Before Callback** field will delay the start of the callback process for the number of seconds specified in the field once a callback is initiated. This field is optional and may be left blank if no delay is desired. Certain phone services can take several seconds to be available again after a call is terminated. It is often useful to configure a delay of a few seconds in order to mitigate the risk of the callback dialog receiving a busy signal while the original caller's service resets itself to accept incoming calls again.

The **Destination after Callback** field is used to configure the call target that the caller will be connected to, once the callback dialog reconnects the caller to the PBX. Any existing call target is available.

Once all options have been configured, click on the **Submit Changes** button followed by the red-

colored **Apply Config** bar to save the callback target and make it active.



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 (more information on **Misc Destinations** can be found later in this chapter in the [Misc Destinations](#) section). Callers would receive a call on the number they called from, would be prompted for their extension and their password, and would then have access to their voicemail messages.

A company receives better per-minute rates on calls made through its VoIP trunks than calls made through employees' mobile phones. Employees' mobile phones have free incoming calls. A callback target could be set up for each employee with a mobile phone to call back the employee's mobile number. The callback would be directed to a DISA destination to give the employee a dial tone on the PBX (allowing them to dial out using the company's VoIP trunks without using any outgoing mobile minutes). More information on DISA is available later in this chapter in the [Direct Inward System Access \(DISA\)](#) section.

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.

Direct Inward System Access (DISA)

Applications → *DISA*

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

In order to set up a DISA call target, navigate to the **Applications** menu and select the **DISA** dialog.

DISA call targets have following eight configuration options:

- DISA name
- PIN
- Response Timeout
- Digit Timeout
- Require Confirmation
- Caller ID
- Context
- Allow Hangup

Add DISA[Add DISA](#)

DISA is used to allow people from the outside world to call into your PBX and then be able to dial out of the PBX so it appears that their call is coming from the office which can be handy when traveling. You can set a destination in an IVR that points to the DISA or set a DID. Make sure you password protect this to keep people from dialing in and using your PBX to make calls out.

Add DISA

DISA name: [?]	<input type="text"/>
PIN [?]	<input type="text"/>
Response Timeout [?]	<input type="text" value="10"/>
Digit Timeout [?]	<input type="text" value="5"/>
Require Confirmation [?]	<input type="checkbox"/>
Caller ID [?]	<input type="text"/>
Context [?]	<input type="text" value="from-internal"/>
Allow Hangup [?]	<input type="checkbox"/>

[Submit Changes](#)

The **DISA name** field is used to identify the DISA configuration when it is being selected as a call target in other parts of the CompletePBX interface.

PIN is used to authenticate a caller when they reach the DISA call target. If the PIN field is not left blank, then the caller will be prompted to enter their authentication code. The PIN that the user enters must match with the value of the PIN field, otherwise the call will be disconnected and the caller will not be able to access the DISA call target. Multiple PIN values can be entered by separating valid PIN values by commas (for example, entering 1234, 5678, 9012 would authenticate callers if they entered any one of the numbers—1234, 5678, 9012 as their PIN when prompted).

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

The **Digit Timeout** field is used to specify how long CompletePBX will wait between digits before dialing the call. If a caller begins entering digits and then stops, CompletePBX will wait for the number of seconds specified in this field, before sending the entered digits to CompletePBX for dialing. The default value for this field is five seconds. This is usually sufficient as most people do not take more than five seconds between button pushes on their phone once they have started dialing.

If the **Require Confirmation** option is checked, then CompletePBX will prompt the caller to press 1, in order to initiate the DISA process as soon as they are transferred to the DISA call target. If the user fails to press 1, then the call is disconnected. This is useful when calls are transferred directly to a DISA call target through an inbound route that matches the caller ID. It is common for the call to be set up and answered so quickly that the caller will not hear any ring or confirmation before being placed into the DISA call target, and the caller will then time out and disconnect before they realize what happened. Requiring confirmation alerts the user that they are about to enter the DISA call target and allows them to press 1 when they are ready.

The **Caller ID** field is used to set the outbound caller ID of any of the calls that are placed from within the DISA call target. The desired caller ID should be specified in the format of "*Caller Name*" <#####>—*Caller Name* is replaced with the name that should be set on outbound calls and ##### should be replaced with the phone number that should be set on outbound calls (for example, "*Packet Publishing*" <5551234567>). This is an optional field. If this field is left blank, then the caller ID of the person placing the call will be used.

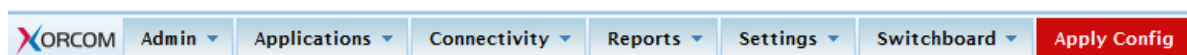


Setting a caller ID value in the Caller ID field does not guarantee that the specified value will be used. If the trunk that routes the call has the Never Override CallerID option enabled, then the caller ID will be whatever is specified in the trunk configuration. More information on trunk caller ID options can be found in Chapter 3, **Trunks**.

The **Context** field is used to specify the context in which CompletePBX will place the caller when they enter the DISA call target. The context that a user is in defines the features and trunks they have access to. CompletePBX places all users into the *from-internal* context by default. As DISA is meant to mimic the functions of an internal user, CompletePBX sets the **Context** field to *from-internal* by default as well. Changing this field will require an understanding of the CompletePBX configuration files, and will likely mean that a custom context has been manually created in the */etc/asterisk/extensions_custom.conf* file. Setting a different context in this field could render the DISA call target useless, hence be sure that the context entered here is valid.

If the **Allow Hangup** checkbox is selected, then the caller can press the hangup feature code (by default this code is **) to end their current call and be presented with a dial tone again. This prevents the caller from actually hanging up their phone, calling back into CompletePBX, and re-authenticating to gain DISA again. If desired, the feature code for hanging up a call can be changed. More information on how to change the feature codes can be found in the *Customizing Feature Codes* section of this chapter.

Once all options have been configured, click on the **Submit Changes** button followed by the red-colored **Apply Config** bar to save the DISA call target and make it active.



PIN Sets

Applications → *PIN Sets*

A **Personal Identification Number (PIN)** is a numeric password that CompletePBX can use to authenticate users when they attempt to dial specific features on the PBX such as outbound routes or DISA. Without entering a valid PIN, these features are inaccessible. A PIN set provides the ability for a group of PINs to be used to authenticate the use of a feature instead of just a single PIN. With a PIN set, each individual user can be given a unique PIN, and it is possible to revoke one user's access to a PBX feature without changing anyone else's PIN.

In addition to authenticating users, PIN sets can also be helpful in tracking which users used which features. When a PIN set is used as an authentication mechanism, CompletePBX can log which unique PIN was used to access a feature in the *accountcode* column of the call detail records. Even if a user places a call from someone else's extension, they will need to enter their own account code. When generating a report of which users used certain features, the detail records will provide an accurate report based on which PINs were used. This feature is often used by companies which implement restrictions on long-distance calling. It is possible to track which users make heavy use of the long-distance outbound routes by checking the PINs used to dial out.

In order to set up a PIN set, navigate to the Applications menu and select the **PIN Sets** dialog.

PIN sets have only three configuration options:

- PIN Set Description
- Record In CDR?
- PIN List

Add PIN Set

Add Password Set

PIN Sets are used to manage lists of PINs that can be used to access restricted features such as Outbound Routes. The PIN can also be added to the CDR record's 'accountcode' field.

New PIN Set

PIN Set Description:

Record In CDR?:

PIN List:

PIN Set Description is used to identify this PIN set when it is being selected during the configuration of an outbound route.

If the **Record In CDR?** checkbox is selected, then anytime a user authenticates themselves using this PIN set, the PIN they used will be stored in the *accountcode* field of the call detail records alongside the details of the call they made. This is a reliable method of tracking the usage of outbound routes, because even if a user calls from an extension other than their own, they still must enter their own PIN to place a call through a protected route. If this option is not enabled then the call is logged normally without any details in the *accountcode* field.

The **PIN List** is a list of one or more PIN codes. Each PIN should be on its own line. PINs can be as long as desired. However, as users are supposed to remember their PINs, it is typical to make PINs only four or five digits long.

A completed PIN set might look like the following:

Add PIN Set

Add Password Set

PIN Sets are used to manage lists of PINs that can be used to access restricted features such as Outbound Routes. The PIN can also be added to the CDR record's 'accountcode' field.

New PIN Set

PIN Set Description:

Record In CDR?:

PIN List:

In order to put our new PIN set to use we must assign it to an outbound route. Navigate to the **Connectivity** menu and select the **Outbound Routes** dialog.

Click on the name of outbound route with which the new PIN set will be associated.

From the **PIN Set** drop-down menu, select the name of the new PIN set:

Add Route

Route Settings

Route Name [?] :	<input type="text"/>	<input type="checkbox"/>
Route CID: [?]	<input type="text"/>	<input type="checkbox"/> Override Extension [?]
Route Password: [?]	<input type="text"/>	
Route Type: [?]	<input type="checkbox"/> Emergency <input type="checkbox"/> Intra-Company	
Music On Hold? [?]	default ▼	
Time Group: [?]	---Permanent Route--- ▼	
Route Position [?]	Last after Emergency ▼	

Additional Settings

Call Recording [?] :	Allow ▼
PIN Set [?] :	Long-distance Calls ▼

Click on the **Submit Changes** button followed by the red-colored **Apply Config** bar. All calls that pass through the selected outbound route will now be authenticated through one of the PINs in our new PIN set.

Misc Applications

Applications → Misc Applications

A misc application is a custom feature code. A misc application allows a custom extension or star code to be defined, which will direct the caller to any call target when dialed. For example, if we have a ring group that calls the cell phones of all staff members, we might create a misc application that calls that ring group when **CELL* (*2355) is dialed.

In order to create a misc application, navigate to the **Applications** menu and select the **Misc Applications** dialog.

Misc applications have four configuration options:

1. Description
2. Feature Code
3. Feature Status
4. Destination

Add Misc Application

Misc Applications are for adding feature codes that you can dial from internal phones that go to various destinations available CompletePBX. This is in contrast to the **Misc Destinations** module, which is for creating destinations that can be used by other CompletePBX modules to dial internal numbers or feature codes.

Add Misc Application
Dynamic Conference
Security Alert

Add Misc Application

Description:
 Feature Code:
 Feature Status:

Destination:

Submit Changes

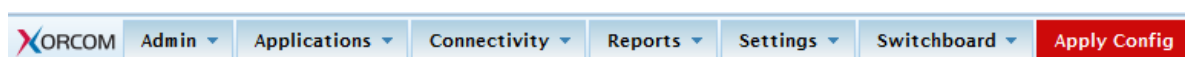
Description is used to identify this application if it needs to be edited or removed at a later time.

Feature Code is the custom feature code that users will dial in order to access this application. This can be a star code (for example, *1234) or simply a normal extension (for example, 1234). The value of this field must be unique (a misc application cannot share a feature code with any other user, application, or star code on the system).

Feature Status determines whether or not the application is active. If this field is set to **Disabled**, then users will be informed that the extension they dialed is not valid if they attempt to use the application. This field allows an application to be quickly disabled without having to remove the application entirely.

Destination is the call target that the application should route the caller to. Any call target that has been previously configured is a valid destination for a misc application.

Once all options have been configured, click on the **Submit Changes** button at the bottom of the page followed by the red-colored **Apply Config** bar at the top of the page.



The application is now active and can be accessed by dialing the selected feature code from any extension on the PBX.

Misc Destinations

Applications → Misc Destinations

A misc destination is used to add a custom call target that can be used by CompletePBX dialogs. Anything that can be dialed from a user's extension can be turned into a misc 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 misc destination could be set up to dial *98 and then an inbound route could point directly to that misc 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.

To create a misc destination, navigate to the Applications menu and select the **Misc Destinations**

dialog.

Misc destinations have two configuration options:

1. Description
2. Dial

Add Misc Destination

Add Misc Destination
Security Provider

Misc Destinations are for adding destinations that can be used by other FreePBX modules, generally used to route incoming calls. If you want to create feature codes that can be dialed by internal users and go to various destinations, please see the **Misc Applications** module. If you need access to a Feature Code, such as *98 to dial voicemail or a Time Condition toggle, these destinations are now provided as Feature Code Admin destinations. For upgrade compatibility, if you previously had configured such a destination, it will still work but the Feature Code short cuts select list is not longer provided.

Add Misc Destination

Description:

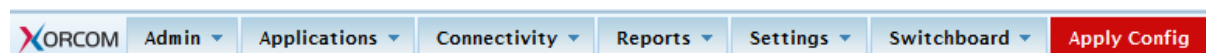
Dial:

Submit Changes

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

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

Once all options have been configured, click on the **Submit Changes** button at the bottom of the page followed by clicking on the red-colored **Apply Config** at the top of the page.



The destination we just created will now be available as a call target from any other CompletePBX dialog.

Faxing

Connectivity → Inbound Routes and Settings → Fax Configuration

Inbound Fax

Connectivity → Inbound Routes

Navigate to the **Connectivity** menu and select the **Inbound Routes** dialog. This will allow you to select the inbound route that will receive faxes

Navigate down to **Fax Detect** section, and set **Detect Faxes** to **True**. This will enable the selected inbound route to receive faxes

Define **Fax Detection Type** – typically DAHDI

Set the **Fax Detection Time** to 5 to enable CompletePBX to detect an incoming fax before the call is answered, and set **Fax Destination** to deliver the incoming fax to the required extension.

Fax Detect

Detect Faxes [?] :	<input type="radio"/> No <input checked="" type="radio"/> Yes
Fax Detection type [?] :	Dahdi ▼
Fax Detection Time [?] :	4 ▼
Fax Destination [?] :	Fax Recipient ▼ VP Marketing (2001) ▼

Now navigate to the **Connectivity** menu and select the **Extensions** dialog, and select the extension that is linked to the inbound route (configured in the above step) that will receive the faxes.

Navigate down to **Fax** section, and check on **Enabled**, and type the email address to which faxes should be delivered in the **Fax Email** field.

- Fax

Enabled [?]	<input checked="" type="checkbox"/>
Fax Email [?]	<input type="text" value="completepbx@gmail.com"/>
Attachment Format [?]	pdf ▼

The standard cover sheet has placeholders where your personal information can be displayed. Navigate to the **Fax Master** section and set the remaining coversheet details as appropriate:

Local Station Identifier should be the fax number to enable the fax recipient to contact you by fax

Name for Cover Sheet is your name to identify you to the fax recipient

Phone Number for Cover Sheet is your phone number, to enable the fax recipient to contact you by phone

Email for Cover Sheet is your email address, to enable the fax recipient to contact you by email

- Fax Master

Local Station Identifier	<input type="text" value="7337331001"/>
Name for Cover sheet	<input type="text" value="VP Marketing"/>
Phone Number for Cover sheet	<input type="text" value="+9727337332001"/>
Email for Cover sheet	<input type="text" value="completepbx@gmail.com"/>

Outbound Fax

Settings → Fax Configuration

Precondition



An extension can only send faxes if it is also defined as a fax recipient, i.e.

- the extension has been defined as a fax recipient (by checking on Enabled in the Fax section of the Extension dialog)
- the inbound route that is linked to the extension has Fax Detect set to Yes

Navigate to the **Settings** and select the **Fax Configuration** dialog. This dialog consists of five sections

- Fax Presentation Options
- Fax Feature Code Options
- Fax Transport Options
- Fax Module Options
- Fax Cover Page options

Presentation Options

Settings → Fax Configuration

Navigate down to the **Fax Presentation Options** section where you can configure information for all outbound faxes, such as:

- Default Fax header, i.e. your company name that will be shown on outgoing faxes.
- Local Station Identifier, i.e. the number that the fax recipient can respond to by fax
- Outgoing email address, i.e. an address that the fax recipient can respond to by email

Fax Presentation Options

Default Fax header: [?]	<input type="text" value="Xorcom Inc"/>
Default Local Station Identifier: [?]	<input type="text" value="7337331001"/>
Outgoing Email address: [?]	<input type="text" value="support@mymailbox.com"/>

Fax Feature Code Option

Email address that faxes are sent to when using the “Dial System Fax” feature. This is also the email address used for fax detection in legacy mode,

Fax Transport Options

The **Error Correction Mode** (ECM) setting determines whether or not to use error correction.

Maximum Transfer Rate and **Minimum Transfer Rate** determine the maximum and minimum transfer rates during fax rate negotiation.

Fax Transport Options

Error Correction Mode [?]	<input type="button" value="Yes"/> <input type="button" value="No"/>
Maximum transfer rate [?]	<input type="text" value="14400"/> ▼
Minimum transfer rate [?]	<input type="text" value="4800"/> ▼

Fax Module Options

This is a legacy feature that is no longer in use. Read the balloon tooltip for a full explanation.

Cover Page

Settings → Fax Configuration

Navigate down to the **Fax Cover Page Options** where you can define cover page details such as:

- Company logo in jpg format
- Company details
- Name
- Address
- Phone
- Website
- Footer

Fax Cover Page Options

Company Logo: [?]	<input type="button" value="Choose File"/> xorcom_logo.jpg <input type="checkbox"/> Remove Logo
Company Name: [?]	<input type="text" value="Xorcom Ltd"/>
Company Address 1: [?]	<input type="text" value="Rabin House"/>
Company Address 2: [?]	<input type="text" value="Misgav Industrial Park"/>
Company Address 3: [?]	<input type="text" value="Misgav 2017400"/>
Company Phone: [?]	<input type="text" value="+97249951999"/>
Company Web Site: [?]	<input type="text" value="www.xorcom.com"/>
Footer: [?]	<input type="text" value="The information contained in this fax is proprietary"/>

When you have completed defining your cover page, you can click on the **Preview** button to see how the cover page will look.

FAX



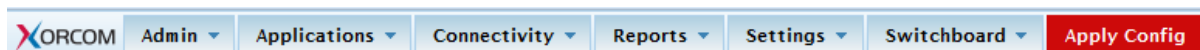
Xorcom Ltd
 +97249951999
 Rabin House
 Misgav Industrial Park
 Misgav 2017400
 www.xorcom.com

Date: Wed, Jun. 18, 2014 09:52 am
 Page: 1 of 1

To:	From:
Fax:	Name:
Recipient Name:	Fax number : 7337331001
	Phone:
	Email: noreply@mydomain.tld

The information contained in this fax is proprietary

Once all options have been configured, click on the **Submit Changes** button at the bottom of the page followed by clicking on the red-colored **Apply Config** at the top of the page.



Summary

By now our CompletePBX should truly be our own. In this chapter, we've learnt how to:

- Upload custom on-hold music
- Create on-hold music from streaming Internet sources
- Set up automated callback systems

- Configure DISA
- Configure custom caller ID lookup sources
- Configure PIN sets
- Create custom applications
- Create custom destinations

Our CompletePBX is now entirely unique and customized to our specifications.

In the next chapter, we will discuss important topics such as system protection, backup and restoration, just in case disaster strikes.

9. My Extension

My Extension provides every extension user access to a number of dialogs 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.

Access

My Extension can either be accessed from the **My Extension** icon in the CompletePBX landing page, or by creating a shortcut for the user in the format <IP Address>/recordings/

i.e. <http://192.168.0.64/recordings>



Security to access My Extension

Users login using their extension number and their voicemail password. Users who do not have a valid voicemail password cannot login to **My Extension**

To access My Extension, the user's extension number should be entered in the Login field, and the user's voicemail password should be entered in the password field. Only users that have password-protected voicemail are able to access My Extension.

Call Monitor

This dialog gives the user access to call logging, for both incoming and outgoing calls, for the user's extension, as well as access to recordings made by that extension.

Call Monitor for VP Marketing (2001)

delete
duration
ignore
Results 13

select: all none

	Date▼	Time	Caller ID	Source	Destination	Duration	Monitor
	2014-01-15	14:01:08	"VP Marketing" <2001>	2001	s	15 sec	
<input type="checkbox"/>	2014-01-15	14:00:26	"VP Marketing" <2001>	2001	2001	5 sec	
	2014-01-15	13:58:25	"VP Marketing" <2001>	2001	2020	12 sec	
	2014-01-15	13:58:11	"CEO" <2020>	2020	2001	6 sec	

Actions

Search will match the text that you type with any text in any field of the call log.

Delete will remove all recordings that are currently checked in the call log. To check a row in the call log, click on the checkbox at the left-hand end of the row. These recordings will no longer be included in the call monitor, and the logs cannot be restored. The call log information will not be deleted, only the recording will be deleted.

Duration can be used in conjunction with the **Ignore** button to ignore calls of specified duration. Only calls that are longer in duration than the value that you typed in the duration box will be displayed.

Fields Displayed

Date indicates the date when the call was made.

Time indicates the time when the call was made.

Caller ID provides information about the caller, if the information is available.

Source is the number from which the call originated.

Destination is the number that was dialed when the call was made.

Duration shows the length of the call, in seconds.

Monitor will display icons if any recordings have been made. The speaker icon allows you to listen to the recording on your machine. The download icon allows you to download the recording onto your machine.

VoiceMail

VoiceMail for VP Marketing (2001)

Search

delete
move_to
Folder
forward_to
Results 5

email_to

select: all none

	Date▼	Time	Caller ID	Priority	Orig Mailbox	Duration	Playback	Download
<input type="checkbox"/>	2014-01-15	12:28:44	"CEO" <2020>	2	2001	6 sec		
<input type="checkbox"/>	2014-01-15	12:25:25	"CEO" <2020>	2	2003	1 sec		
<input type="checkbox"/>	2014-01-15	12:01:51	"VP Support" <2003>	2	2001	146 sec		
<input type="checkbox"/>	2014-01-15	12:01:10	"CEO" <2020>	2	2001	13 sec		
<input type="checkbox"/>	2014-01-15	11:54:28	"VP Support" <2003>	2	2001	12 sec		

Actions

Search will match the text that you type with any text in any field of the voicemail log.

Delete will remove all voicemails that are currently checked from your voicemail. To check a row in the voicemail log, click on the checkbox at the left-hand end of the row. These voicemails will no

longer be included in your voicemail log, and cannot be restored.

Move To in conjunction with the associated dropdown list allows you to categorize the currently displayed voicemails and store them in one of the following folders: Family, Friends, Old, and Urgent.

Forward To in conjunction with the associated dropdown list of extensions allows you to forward the currently displayed voicemails to another extension.

Email To allows you to send, by email, the currently displayed voicemails to the email address that you type in the appropriate text box.

Fields Displayed

Date indicates the date that the voicemail was created.

Time indicates the time that the voicemail was created.

Caller ID provides information about the caller, if the information is available.

Priority indicates the priority of the voicemail.

Orig. Mailbox shows the mailbox where the voicemail originated in cases where the voicemail has been forwarded to you from another extension.

Duration shows the length of the voicemail, in seconds.

Playback will display icons if any voicemail recordings have been made. The speaker icon allows you to listen to the recording on your machine. The phone icon allows you to listen to the recording on your extension.

Download will display an icon if any recordings have been made, allowing you to download the recording onto your machine.

Feature Codes

The Feature Codes menu provides a quick-reference guide of all the feature codes that are available to the user, with a brief description of each feature code.

The first column, headed **Handset Feature Code** is the code that you should dial to activate the feature, and the **Action** column displays a brief description of the feature code.

Handset Feature Code Action

*30	Blacklist a number
*31	Remove a number from the blacklist
*32	Blacklist the last caller
*52	Call Forward No Answer/Unavailable Activate
*53	Call Forward No Answer/Unavailable Deactivate
*72	Call Forward All Activate
*73	Call Forward All Deactivate
*74	Call Forward All Prompting Deactivate
*740	Call Forward Toggle
*90	Call Forward Busy Activate

Phone Features

This menu enables the user to personalize the handling of incoming calls.

Phone Features for VP Marketing (2001)

Phone Features

Call Waiting

Do Not Disturb

Call Screening: 

Ringtimer: 

CallForward Ringtimer: 

Call Forwarding

Unconditional: Enable

Unavailable: Enable

Busy: Enable

Call Waiting enables toggling of the call waiting feature. When you are busy on the phone and another incoming call arrives, call waiting will provide you with an indication that you have another incoming call.

Do Not Disturb enables toggling of the Do Not Disturb presence. If Do Not Disturb is activated, your phone will be considered busy, and all incoming calls will be handled accordingly.

Call Screening requires incoming callers to state their name. This name identification is played to you when you answer the phone, when you have the option to either accept or reject the call.



Note

Call screening information is stored by the system, so a caller only has to go through this process once per phone number that they are calling you from.

Ringtimer determines the time, in seconds, that your phone will ring, before going to voicemail, or handling any other options that have been configured, such as Follow Me, etc.

Call Forwarding: Unconditional will forward ALL incoming calls to the designated number. If the designated number is an internal extension, then only the extension number needs to be entered. However, if the destination is an external number, the system dialout code (typically 9) will be required. All non-extension destinations (such as ring groups, queues, external numbers, etc.) must

be followed by the # character.

Call Forwarding: Unavailable will forward unanswered incoming calls to the designated number. If the designated number is an internal extension, then only the extension number is needs to be entered. However, if the destination is an external number, the system dialout code (typically 9) will be required. All non-extension destinations (such as ring groups, queues, external numbers, etc.) must be followed by the # character.

Call Forwarding: Busy when your extension is busy, will forward ALL incoming calls to the designated number. If the designated number is an internal extension, then only the extension number needs to be entered. However, if the destination is an external number, the system dialout code (typically 9) will be required. All non-extension destinations (such as ring groups, queues, external numbers, etc.) must be followed by the # character.



Tip

Do not forget to press on **Update** after making any changes.

Faxes

The Faxes menu allows users to send faxes, and to view their history of stored (inbound and outbound) faxes.

Send Fax


Destination is the full fax number of the person to whom you are sending the fax. Do not forget any dial code that may be required by your phone system to access external lines or to access international service providers.


File to send allows you to browse to the file that you want to send as a fax. The file must be in pdf, tif, or tiff format. Click on the (+) icon to include additional documents in the fax, or click on the trash icon to remove a document that you have previously added.


Include Cover Sheet? checkbox indicates whether you want to add the standard company-wide coversheet to your fax. Your system administrator should have already defined a standard company coversheet: check this option if you want to add this standard coversheet to your fax.

If you include the coversheet, you can also add the recipient's name to the coversheet, as well as brief message


Send Fax

Destination 








Include Cover Sheet 

Recipient name 

Message 

Here is the information that you requested. Good luck with your poker tournament!



Tip

Do not forget to press on the **Send fax** button to send your fax.

Stored Faxes

Fax column icon 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.

File allows you to view the complete fax that was sent, including the coversheet (if requested) and all documents, in pdf format.

Time displays the time when the fax was received (in the case of an inbound fax), or sent (in the case of an outbound fax.)

Delete allows you to completely remove the stored fax from the system by clicking on the trash icon.

Settings

Gives each user the option to manage the settings for their extension

Settings for VP Marketing (2001)

Language:

Password Settings

Passwords must be all numbers and at least 3 digits

Voicemail Password:

Enter again to confirm:

Notification Settings

Email Address: Enable

Attach voicemail to email

Delete voicemail after emailed

Pager Email Address: Enable

Web Playback Settings

Call Me Number:

Audio Format:

Phone Playback Settings

Say caller ID

Say envelope (date/time)

Language determines the language that will be used throughout **My Extension** dialog

Password Settings

Voicemail Password is the password to access the user's voicemail, as well as the password to access **My Extension**. The password must be completely numeric, and must be at least 3 digits in length.

Enter again to confirm is a security feature to verify that you have really typed the password that you intended to type.

Notification Settings

Email Address is the email address that CompletePBX will use to send voicemail alerts to

Enable allows you disable the email notification feature, while saving all settings, by unchecking this option box.

Attach voicemail to email, when checked, delivers a copy of all voicemails to your email. This is a very nice feature for listening to your office voicemails from your mobile device or from some other location.

Selecting the **Delete voicemail after emailed** checkbox causes voicemails to be deleted from the server after they have been emailed to the specified email address. Be careful with this option, as there is no way to recover voicemails after they have been deleted.

Page Email Address enables a brief notification to be sent to you alerting about a new voicemail.

Web Playback Settings

Call Me Number can be any dialable number, such as an extension, where you want to hear your voicemail messages.

Audio Format determines the format in which your voicemail messages will be stored. This allows you choose higher quality recordings, or a format that require less storage space.

Phone Playback Settings

Say caller ID will say the caller's phone number (in the voicemail) before playing the actual voicemail message.

Say Envelope will say the date and time a voicemail message was left (in the voicemail) before playing the actual voicemail message.



Tip

Do not forget to press on **Update** after making any changes.

Logout

Click on Logout to exit the My Extension module.

10. Managing Call Flow

Configuring My Switchboard



Important Note

If you want the Switchboard to track the status of queues and to create statistics for call center reporting, make sure that both Event When Called and Member Status Event (in the Events, Stats and Advanced section of the Queue dialog) are set to Yes when defining a new queue.



The Switchboard on CXR series machines can display up to 15 buttons only. Check on all the buttons that you want to hide, so that no more than 15 buttons remain unchecked

There is no limit on the number of buttons that can be displayed by the CXE and CTS series of CompletePBX.

Permissions

Switchboard → *Permissions*

This dialog allows you to create groups of permissions, which can be used either in templates or to define the permissions granted to a user

Navigate to the **Switchboard** menu and select the **Permissions** dialog.

This module will let you manage advanced FOP2 permissions.

basic

[Delete FOP2 Permission 'basic'](#)

Edit Permission

Name:

Permissions:

Permission Quick Pick

Apply to Groups

Select the groups you want to apply this permission to. You will be able to perform the actions only to the extension/buttons that are part of the selected groups. If no groups are selected, the permission will be allowed to every button on the panel.

- | | |
|-----------------|--------------------------|
| All Buttons | <input type="checkbox"/> |
| All Extensions | <input type="checkbox"/> |
| All Queues | <input type="checkbox"/> |
| All Conferences | <input type="checkbox"/> |
| All Trunks | <input type="checkbox"/> |

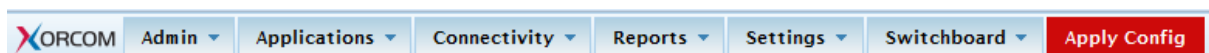
Name allows you to reference the permission group.

Permissions allow you to specify what actions can be performed by a user who is granted this permission group

Click on the **Permission Quick Pick** to see a list of all available permissions.

Apply to Groups enables you to select which groups should belong to this permission group. If no groups are selected the permission group will be granted to all buttons.

Once all options have been configured, click on the **Submit Changes** button at the bottom of the page followed by clicking on the red-colored **Apply Config** at the top of the page.



Templates

Switchboard → Templates

This dialog simplifies user management by allowing you create and manage templates, which you can then assign to users.

Navigate to the **Switchboard** menu and select the **Templates** dialog.

Add FOP2 Template

This module will let you manage FOP2 templates, that you can assign to users for easy management.

Add Template

Name:

Permissions:

Permission Quick Pick

Make Default:

Allowed Groups

Select the groups you want to add to this template. If no groups are selected, the user will be able to see all buttons.

- All Buttons
- All Extensions
- All Queues
- All Conferences
- All Trunks

- (pick permission) ▾
- (pick permission)
 - all
 - dial
 - hangup
 - hangupself
 - meetme
 - pickup
 - record
 - recordself
 - spy
 - transfer
 - transferexternal
 - whisper
 - queuemanager
 - queueagent
 - phonebook
 - chat
 - preferences
 - voicemailadmin

Name allows you to reference the template.

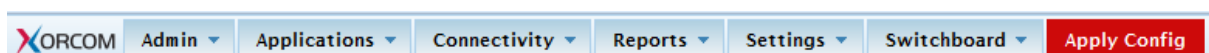
Permissions allow you to specify what actions the user will be able to perform

Click on the **Permission Quick Pick** to see a list of all available permissions.

Check on **Make Default** if you want this template to become the default template, which will be applied to all users for which another template has not been specified.

Allowed Groups enables you to select which groups should be added to this template. If no groups are selected the user will be able to see all buttons. This gives you the ability to restrict the buttons that are displayed to users of this template.

Once all options have been configured, click on the **Submit Changes** button at the bottom of the page followed by clicking on the red-colored **Apply Config** at the top of the page.



Users

Switchboard → *Users*

This dialog enables you to manage Switchboard users and permissions, and also select which groups each user can view.



Security to access My Switchboard

In order to have access to **My Switchboard**, users must be suitably defined. Use the **Administration** dialog (accessed from the CompletePBX Launch Pad) to access the **Switchboard** menu and select the **Users** dialog. Only users that are defined as Switchboard Users can login to **My Switchboard**. Default security uses the extension number and voicemail password, although a different password can be defined in the **Users** dialog. Users who are not defined in the Users dialog cannot access **My Switchboard**.

Navigate to the **Switchboard** menu and select the **Users** dialog

This module will let you manage FOP2 users and permissions, and also mark the groups the user will be able to view.

[Delete FOP2 User '2002'](#)

Edit User

Extension: [?]

Secret: [?]

Template Quick Pick [?]

Permissions

Permissions: [?]

Permission Quick Pick [?]

Allowed Groups

Select the groups you want the user to see in the panel. If no groups are selected the user will be able to see all buttons.

All Buttons	<input type="checkbox"/>
All Extensions	<input type="checkbox"/>
All Queues	<input type="checkbox"/>
All Conferences	<input type="checkbox"/>
All Trunks	<input type="checkbox"/>

Extension is the extension allocated to the user.

Secret is the password that will be used by the user to access the Switchboard. If no password is defined, the user's voicemail password will be used.

Template Quick Pick provides a dropdown list of previously defined templates that can be applied to the user.

If no template is used, you can grant the user a selected list of permission from the **Permission Quick Pick** dropdown list.

Allowed Groups enables you to select which groups should be available to the user. If no groups are selected, the user will be able to see all groups. This gives you the ability to restrict the groups of buttons that are displayed to the user.

Once all options have been configured, click on the **Submit Changes** button at the bottom of the page followed by clicking on the red-colored **Apply Config** at the top of the page.

Buttons

Switchboard → *Buttons*

The buttons dialog allows you to define the behavior of each button.

Navigate to the **Switchboard** menu and select the **Buttons** dialog

For example, you can change button labels (overriding the existing CompletePBX label) and privacy options (to prevent the button to be monitored and/or hide the CallerID) among other things. You can also sort the list by dragging the elements



The Switchboard on CXR series machines can display up to 15 buttons only. Check on all the buttons that you want to hide, so that no more than 15 buttons remain unchecked

There is no limit on the number of buttons that can be displayed by the CXE and CTS series of CompletePBX.

- **Label** defines the name that will be displayed on the button in the Switchboard.
- **Privacy** allows you to disable monitoring, or hide the CallerID for this button.
 - **clid** restricts the display of either the CallerID or dialed number
 - **monitor** prevents the device from being spied on, or from being monitored
 - **all** prevents both clid and monitor
- **Email** allows you to send emails to the user from the Switchboard.
- **External Transfer** allows you to define the **number@context** that will be used for external transfers. The default context for the extension will be used if the context is omitted.
- **Channel** can be used to add extra channels for the button. You can overflow channels into any extension, so if My Switchboard detects activity with *any* of the channels in the list, it will be displayed as activity for that extension/button. For example, if you have a local SIP channel for your internal extension, and an IAX extension for use when you are on the road, you can specify the IAX channel on the button. Calls made from either of the channels, SIP or IAX, will be displayed on the same button.
- **Group** allows you to assign an extension to a group. The Switchboard will display all extensions belonging to the same group in a separate box.
- **Custom ASTDB** is the ASTDB key to search for custom states. By default, this is set to Call Forward Unconditional state.
- **Originate Channel** allows you to define which channel to use when originating a call from the Switchboard.
- **ChanSpy** Options are passed to the ChanSpy function.
- **Tags** can be defined for buttons, which can be used to filter the buttons that will be displayed, as described in the **Filter Box** section below.

Groups

Switchboard → *Groups*

Navigate to the **Switchboard** menu and select the **Groups** dialog:

This module will let you manage FOP2 groups.

Add Group

Name: [?]

Included Buttons

Select the buttons you want to include in this group.

Extensions

1001	DAHDI channel 1
1002	DAHDI channel 2
1003	DAHDI channel 3
1004	DAHDI channel 4
1005	DAHDI channel 5
1006	DAHDI channel 6

Check All

Using My Switchboard

Queue Events



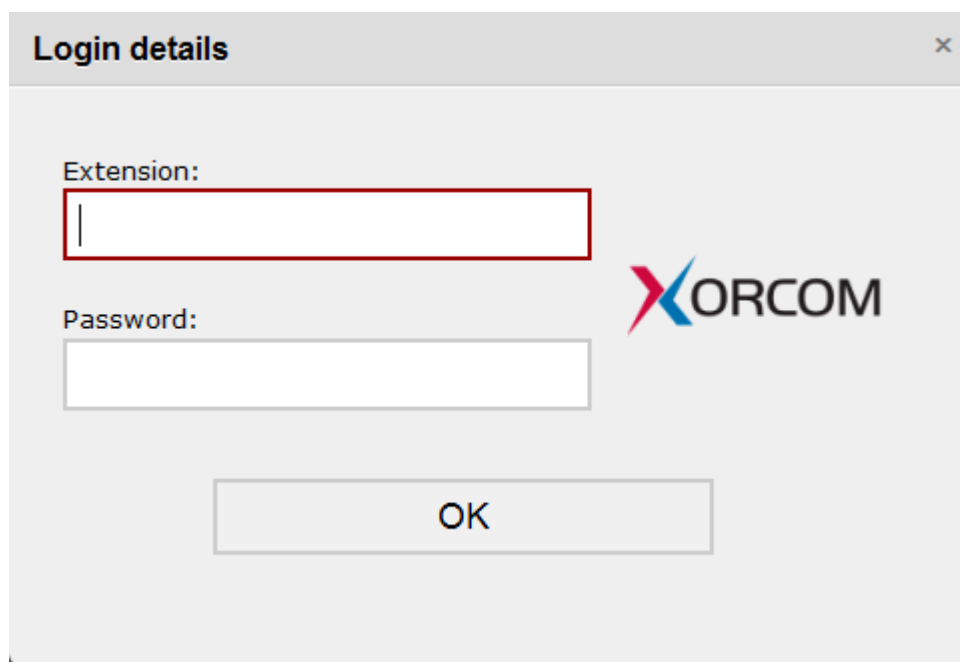
Important Note

If you want the Switchboard to track the status of queues and to create statistics for call center reporting, make sure that both **Event When Called** and **Member Status Event** (in the **Events, Stats and Advanced** section of the Queue dialog) are set to **Yes** when defining a new queue.

Login

To reach the login dialog, navigate to the CompletePBX Launch Pad, click on the **My Switchboard** icon. Alternatively, you can open an Internet browser and enter the Web address for the panel in the address panel. The address depends on the IP address of your CompletePBX machine, but it could be something like **http://192.168.0.11/fop2**

If the Switchboard server is running, you will be presented with the login box.



Use your extension number, and voicemail password to login.

In order to perform actions with the panel, you must login with an extension that has been granted permissions, as that extension will be the originator of the actions you perform.

Passing Credentials via URL

It is possible to pass the extension and password in a URL to avoid being prompted to login. You can use this feature to embed the panel into another application, or to create a bookmark. In order to do this, you must append extension and password parameters, as in this example:

```
http://192.168.0.11/fop2/?exten=2002&pass=2002
```

Main Panel View

After a successful login, you will be presented with the panel window.

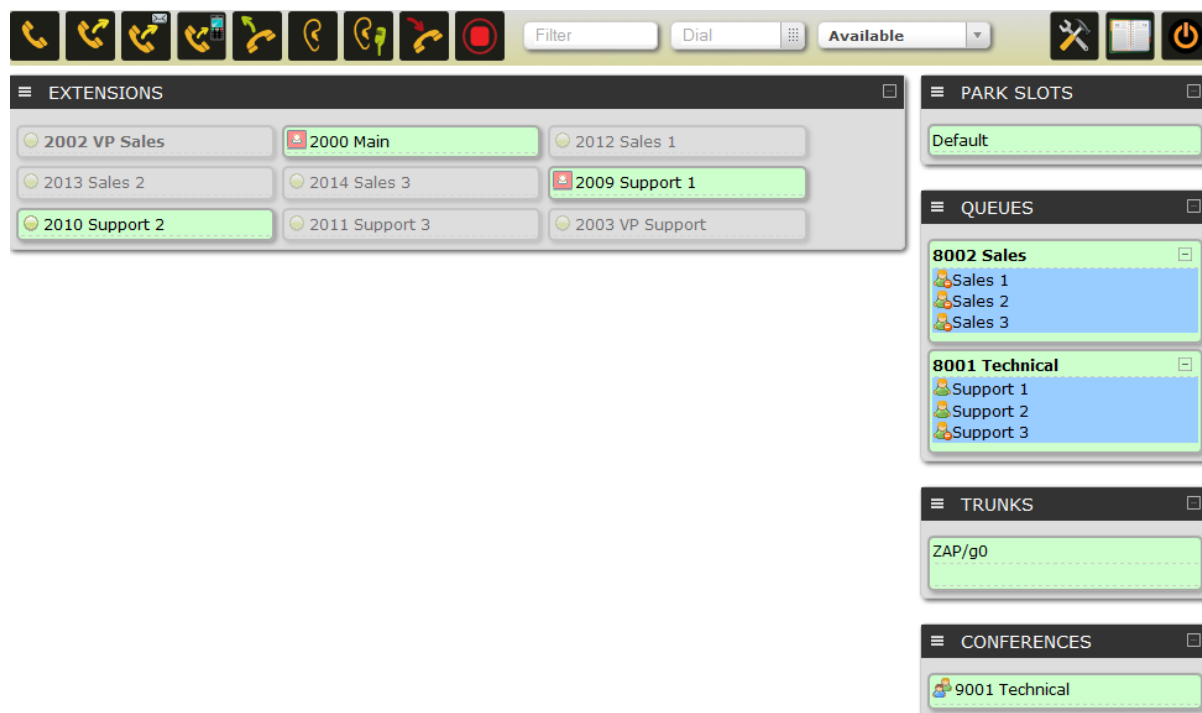


The Switchboard on CXR series machines can display up to 15 buttons only. Check on all the buttons that you want to hide, so that no more than 15 buttons remain unchecked

There is no limit on the number of buttons that can be displayed by the CXE and CTS series of CompletePBX.

There is a toolbar that is always visible at the top, and four sections in the content area: one for each kind of button.

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 if 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 dial 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.

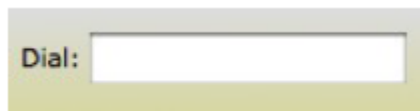
Filter Box

Filter:

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

Element	Explanation
1 - Presence icon	<p>Indicates the presence state for the extension.</p> <p>Green circle means that the extension is not in a call.</p> <p>Red circle indicates that the extension is busy or in a call.</p> <p>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.</p> <p>Tape icon indicates that someone initiated a call recording from within the Switchboard, and that the call is now being recorded.</p> <p>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).</p>
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 members). 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 of an 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

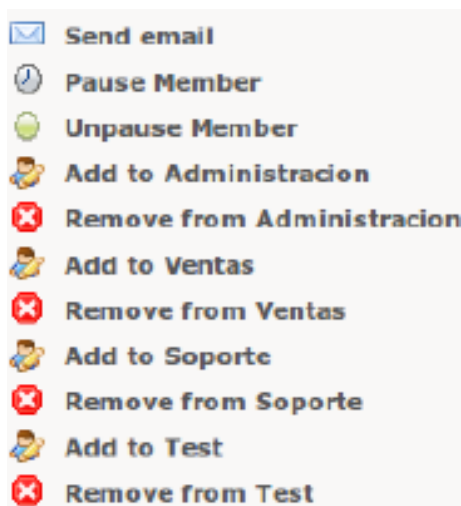
Buttons can be clicked to select or deselect them. When a button is selected, the border of the button will become red. Once a button is selected it will become the target button for any action that you choose.

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 members 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 can pickup calls from parking slots, trunks and queues.

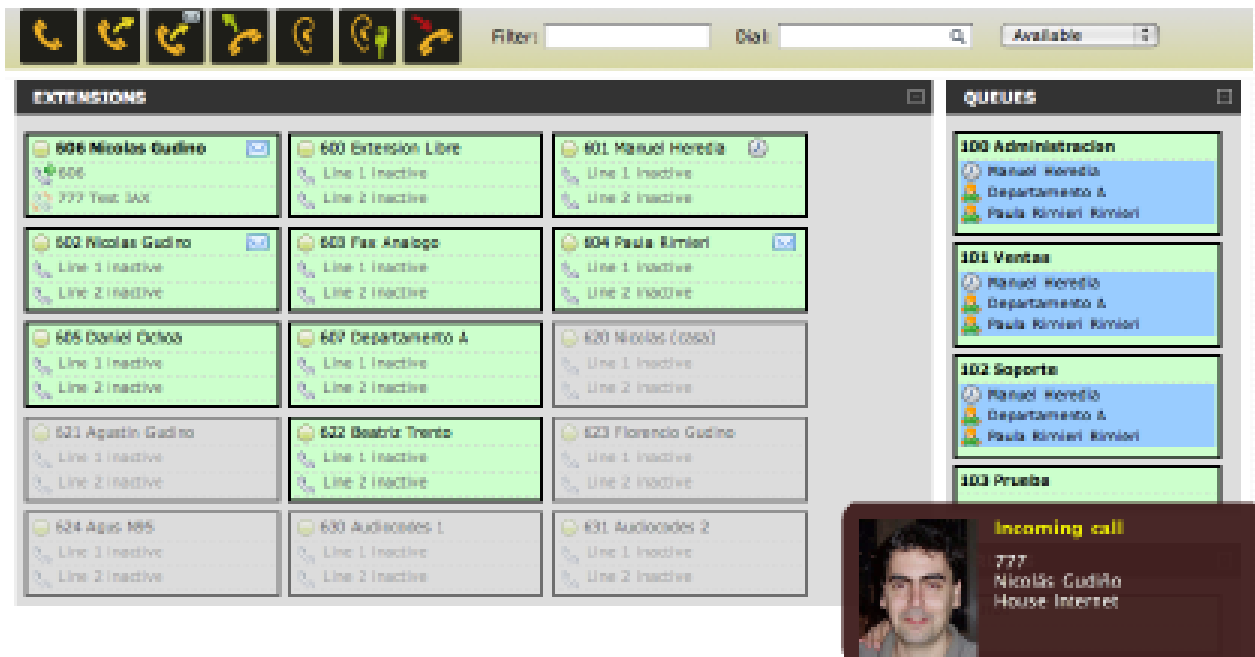
The submenu for queue members allows you to remove them, pause, or un-pause them.

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

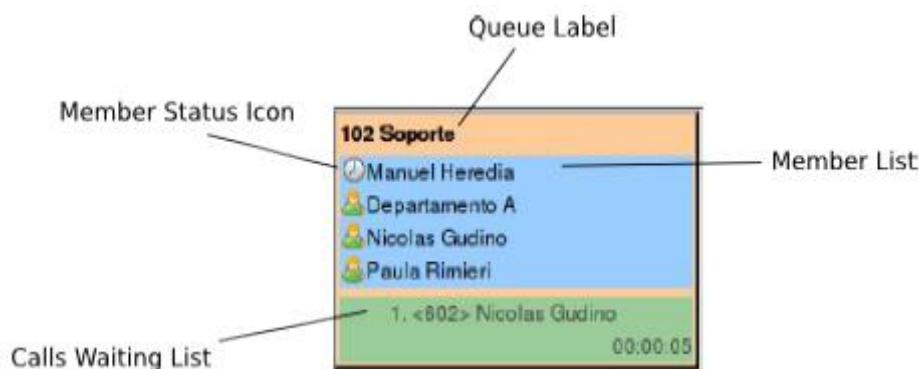
```

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 members or 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 members might be:

 = ready

 = busy

 = unavailable / invalid

 = paused.

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.

Call Center Stats

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**.



Recommendation

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.

A screenshot of a web browser showing the login page for Call Center Stats. The page has a light yellow background and a teal header bar with the word "Home" on the left. A login form is centered on the page, containing fields for "Username" and "Password", and a "Login" button. At the bottom of the page, there is a footer with the text "Page processed in 0.0149 seconds ccQstats powered by Xorcom" on the left, and "CompletePBX Call Center Stats" on the right.

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, you 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.

Username	Password	Name	Access Tokens
user			user
admin	password	Admin	user_admin_agent
user	user	User	user
xorcom	xorcom	Xorcom Login	user_admin_agent



Recommendation

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

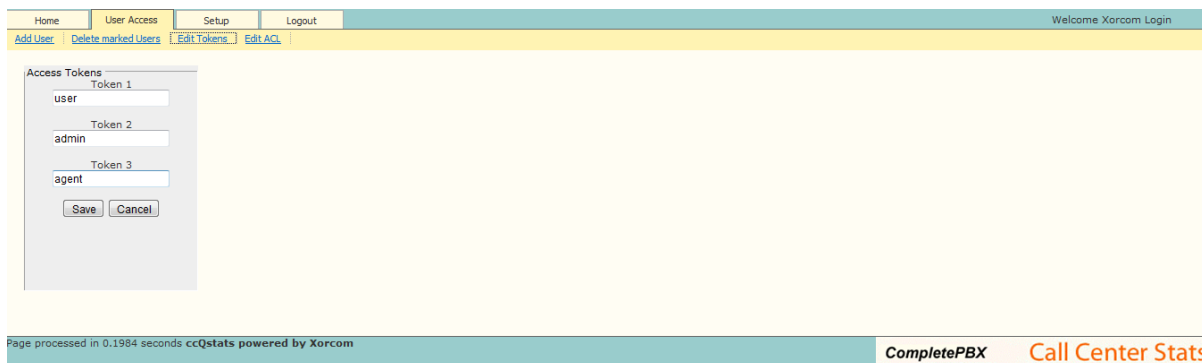
These keys can be assigned individually or in combination to user accounts that you define. Depending on the keys that are assigned an account, it can access the various reports and reports as they are defined in the Edit screen in the Access Control tab Users. For example, it is possible to restrict 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.

Access Control	
Resource	Required Tokens
Abandon Rate	user
Add Keyword	admin
Add User	admin
admin-setup.php	admin
User Access Page	admin
Agent reports	user
Agent Availability (for all queues)	user
Agent Session and Pause Durations	user
Agent Summary	user
Answered calls reports	user
Answered Calls by Agent	user
Answered Calls by Queue	user
Answered Calls Detail	user
Answered report summary	user

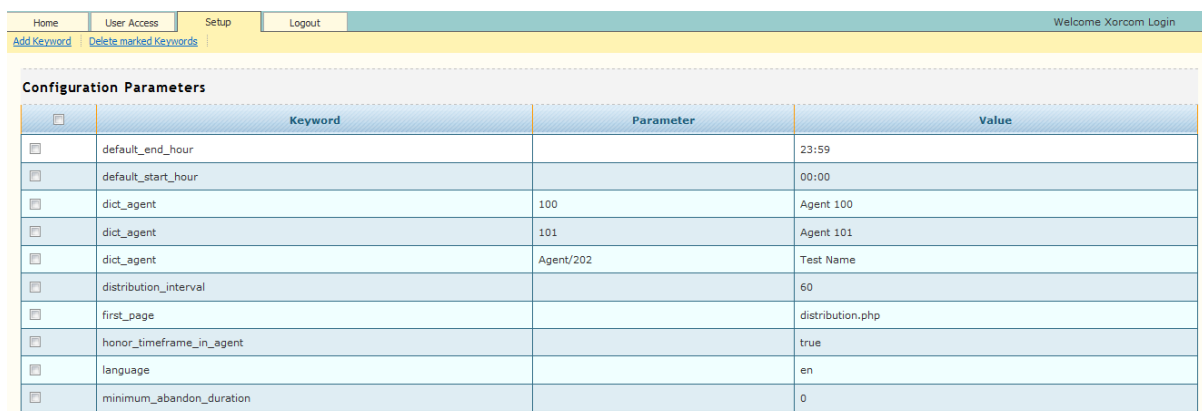
To change the table of access controls, simply click on the resource you want to change, view the display for editing access control. From here you can define what access keys are needed to view or select the remedy chosen.

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, 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

Variable	Explanation
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
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 uniqueids 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

Variable	Explanation
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.

Home Distribution Answered Unanswered Realtime Agent User Access Setup Logout Welcome Xorcom Login									
Per queue Per month Per week Per day Per hour Per day of week									
Report Info					Total Calls				
Queue:	8011,8021,9000,9021				Number of Connected Calls:	1417 calls			
Start Date:	2010-01-01				Number of Answered Calls:	1290 calls			
End Date:	2010-03-31				Number of Unanswered Calls:	127 calls			
Hour range:	00:00 - 23:59				Abandon Rate:	8.96 %			
Period:	90 days				Transferred Calls:	0 calls			
					Agent Login:	0			
					Agent Logoff:	0			
Call Distribution per queue									
Queue	Received	Answered	Unanswered	Transfers	% Answ	% Unansw	Avg Durat.	Avg Wait	
8011	938	856	82	0	91.26 %	8.74 %	6:43 min	25 secs	
8021	435	397	38	0	91.26 %	8.74 %	5:11 min	17 secs	
9000	42	37	5	0	88.10 %	11.90 %	4:52 min	6 secs	
9021	2	0	2	0	0.00 %	100.00 %	0:00 min	66 secs	
Total	1417	1290	127	0	91.04 %	8.96 %			



Note

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 hand side that states “Play”. 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.



Configuration

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.

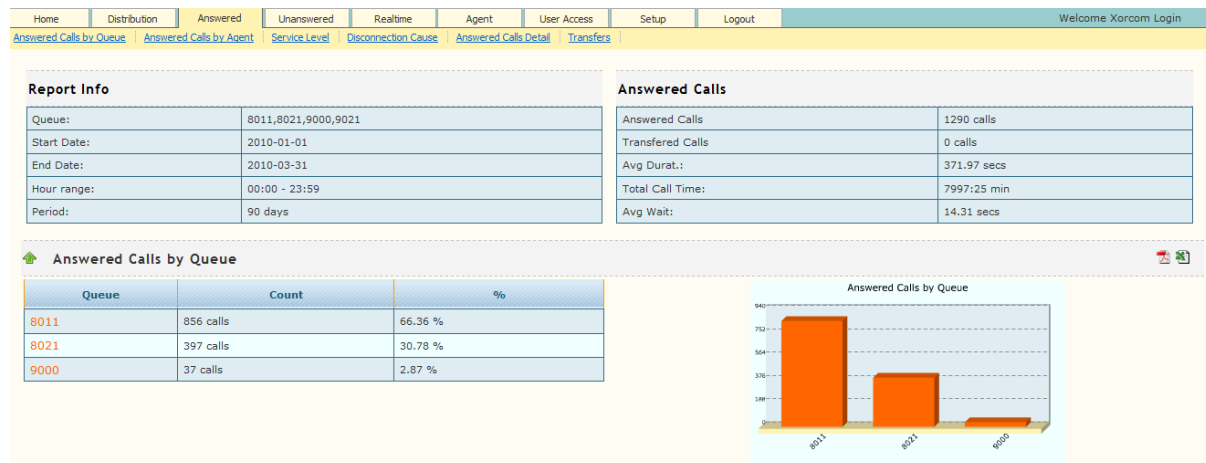
Calls Answered

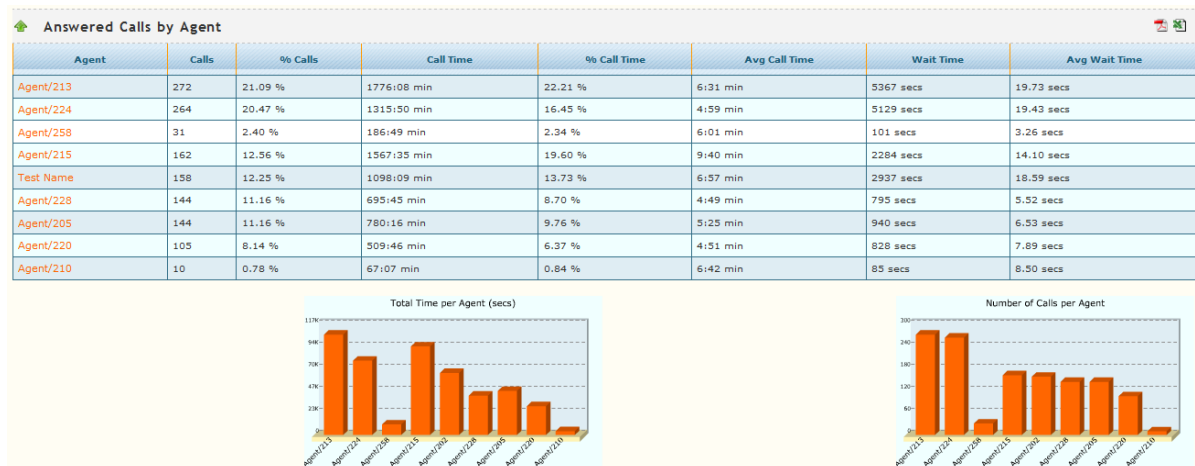
The second tab is labeled Answered. Reports on quantity of calls Answered as follows:

- 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.

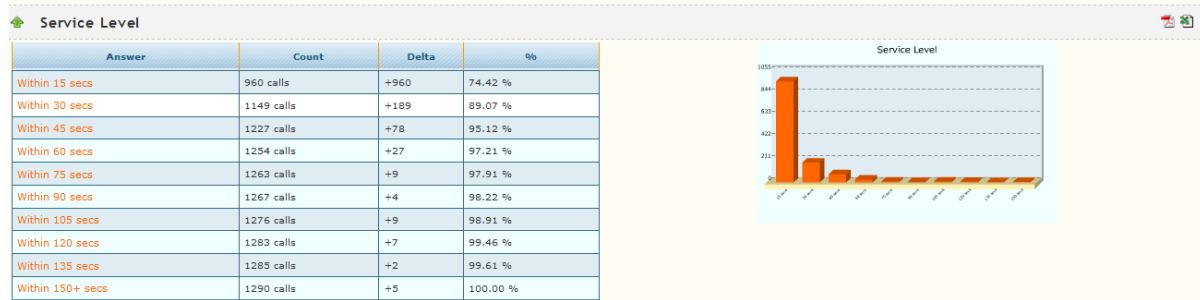


Important

Note that the percentages (such as the percentage of length) are calculated based on the 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

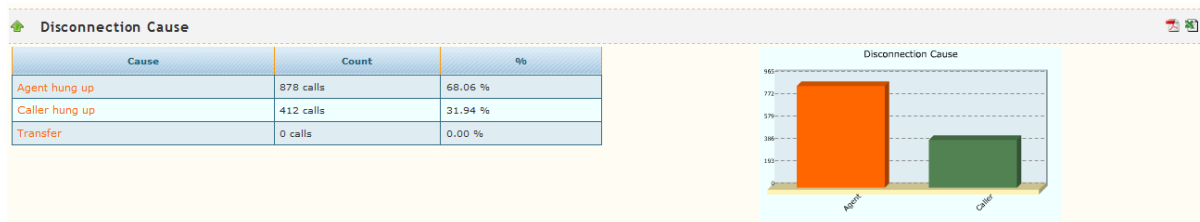
This report shows the distribution of waiting times in queue of calls, with short time intervals of 15 seconds.



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.

Date	Agent	Queue	Phone Number	Event	Wait Time	Call Time	Actions
2010-01-04 07:42:15	Agent/213	8011	7325417900	COMPLETEAGENT	5 secs	1:25 min	
2010-01-04 08:47:43	Agent/224	8011	9787581045	COMPLETEAGENT	27 secs	9:00 min	
2010-01-04 08:52:38	Agent/258	8021	9524485910	COMPLETEAGENT	3 secs	10:51 min	
2010-01-04 08:56:01	Agent/258	8021	3126637903	COMPLETEAGENT	3 secs	0:39 min	
2010-01-04 09:11:09	Agent/215	8011	7174456701	COMPLETEAGENT	5 secs	2:32 min	
2010-01-04 09:19:56	Test Name	8011	7275307700	COMPLETEAGENT	5 secs	17:05 min	
2010-01-04 09:29:58	Agent/215	8011	7013568190	COMPLETEAGENT	25 secs	1:25 min	
2010-01-04 09:36:01	Agent/228	8021	8604412430	COMPLETEAGENT	3 secs	6:33 min	
2010-01-04 09:46:48	Agent/213	8011	2706895250	COMPLETEAGENT	2 secs	1:05 min	
2010-01-04 09:50:23	Agent/205	8021	441473237600	COMPLETEAGENT	2 secs	1:06 min	
2010-01-04 09:56:11	Agent/228	8021	5036163227	COMPLETEAGENT	4 secs	3:18 min	
2010-01-04 10:01:54	Agent/220	8021	7174456701	COMPLETEAGENT	9 secs	1:43 min	

Date	Queue	Event	Agent	info1	info2	info3
2010-01-04 07:42:10	8011	ENTERQUEUE	NONE		7325417900	
2010-01-04 07:42:15	8011	CONNECT	Agent/213	5	1262616130.1557	
2010-01-04 07:43:40	8011	COMPLETEAGENT	Agent/213	5	85	1

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.

Agente	Hasta:	Nro
SIP/601	604@internos	9
SIP/601	602@internos	6
SIP/604	601@internos	134
SIP/604	9998@internos	4
SIP/604	602@internos	2
SIP/604	606@internos	12
SIP/601	fax@default	1
SIP/604	603@internos	2
SIP/601	606@internos	2
SIP/601	607@internos	1
SIP/604	607@internos	1

Figura 4.8: Sumario de transferencias

Unanswered calls

The third tab is labeled Unanswered, which reports on:

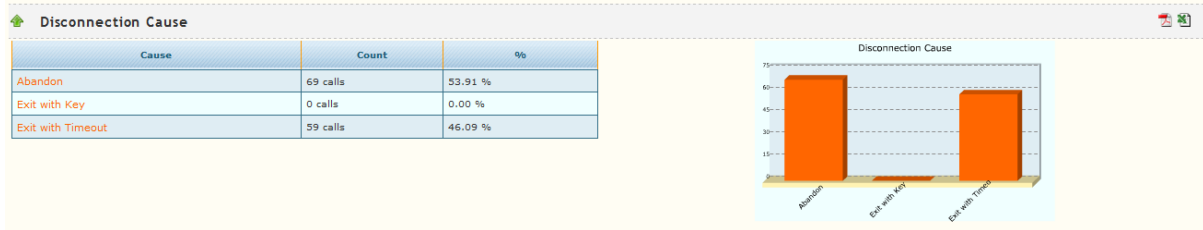
- Abandon Rate
- Disconnection Cause
- Unanswered Calls by Queue
- Disconnection Cause
- Unanswered Calls Detail

Report Info		Unanswered Calls	
Queue:	8011,8021,9000,9021	Number of Unanswered Calls:	128 calls
Start Date:	2010-01-01	Avg wait time before disconnect:	189 secs
End Date:	2010-03-31	Avg queue position at disconnection:	1
Hour range:	00:00 - 23:59	Avg start queue position:	1
Period:	90 days		

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.

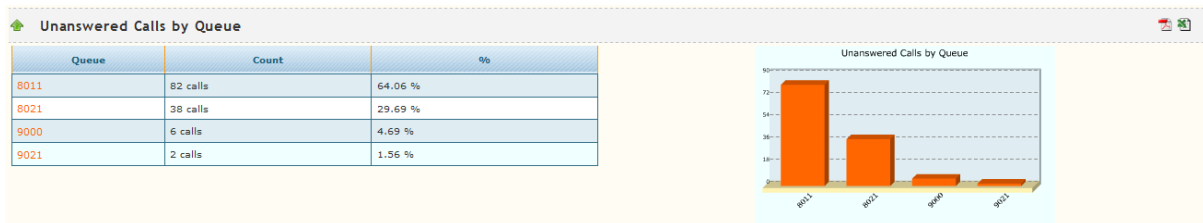


The possible reasons are:

- 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.

The screenshot displays a report titled "Unanswered Calls Detail". It is a table with seven columns: Date, Queue, Phone Number, Event, Start Position, End Position, and Wait Time. The table lists individual call events with their respective dates, times, and details.

Date	Queue	Phone Number	Event	Start Position	End Position	Wait Time
2010-01-04 13:20:03	8011	6022910304	Abandoned	1	1	0:09 min
2010-01-06 08:05:53	9000	7874552066	Timeout		1	0:16 min
2010-01-06 17:56:27	8011	9565476700	Timeout		1	3:00 min
2010-01-07 13:57:39	8011	6024372234	Abandoned	1	1	2:11 min
2010-01-07 15:27:37	9000	9318815590	Abandoned	1	1	0:00 min
2010-01-08 07:10:55	8021	2487392152	Timeout		1	3:00 min
2010-01-08 07:11:10	8011	6316916400	Timeout		1	3:00 min
2010-01-08 07:35:37	9021	9546724466	Abandoned	1	1	0:12 min
2010-01-08 07:53:21	8021	5088300088	Abandoned	1	1	2:44 min

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.

Date	Queue	Event	Agent	Info1	Info2	Info3
2010-01-07 13:57:39	8011	ENTERQUEUE	NONE		6024372234	
2010-01-07 13:57:39	8011	RINGNOANSWER	Test Name	0		
2010-01-07 13:57:49	8011	RINGNOANSWER	Agent/224	10000		
2010-01-07 13:58:02	8011	RINGNOANSWER	Test Name	0		
2010-01-07 13:58:02	8011	RINGNOANSWER	Agent/213	0		
2010-01-07 13:58:02	8011	RINGNOANSWER	Agent/215	0		
2010-01-07 13:58:12	8011	RINGNOANSWER	Agent/224	10000		
2010-01-07 13:58:28	8011	RINGNOANSWER	Agent/224	10000		
2010-01-07 13:58:33	8011	RINGNOANSWER	Agent/215	0		
2010-01-07 13:58:34	8011	RINGNOANSWER	Agent/213	1000		
2010-01-07 13:58:34	8011	RINGNOANSWER	Test Name	1000		
2010-01-07 13:58:44	8011	RINGNOANSWER	Agent/224	10000		
2010-01-07 13:58:59	8011	RINGNOANSWER	Agent/224	10000		
2010-01-07 13:59:12	8011	RINGNOANSWER	Agent/215	1000		
2010-01-07 13:59:12	8011	RINGNOANSWER	Agent/213	1000		
2010-01-07 13:59:12	8011	RINGNOANSWER	Test Name	1000		
2010-01-07 13:59:22	8011	RINGNOANSWER	Agent/224	10000		
2010-01-07 13:59:38	8011	RINGNOANSWER	Agent/224	10000		
2010-01-07 13:59:43	8011	RINGNOANSWER	Agent/215	0		
2010-01-07 13:59:43	8011	RINGNOANSWER	Agent/213	0		
2010-01-07 13:59:44	8011	RINGNOANSWER	Test Name	1000		
2010-01-07 13:59:50	8011	ABANDON	NONE	1	1	131

11. System Protection

Introduction

At this stage, we have a fully-functional CompletePBX 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. While dealing with a CompletePBX, these protection methods are even more important. As CompletePBX controls voice communications for a company, downtime often means lost income and angry employees.

While the installation and setup of the equipment listed here is beyond the scope of this book, 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 CompletePBX provides options for various types of redundant components. The most common redundant component is the hard drive, usually set up in a RAID configuration. This allows a hard drive to fail while the server keeps running. Power supplies are also a common redundant component, again allowing for one to fail without downing the server.

Surge Protection

The most common type of surge protection is for power lines, but surges can affect other

components of the CompletePBX 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 CompletePBX.

Backups

CompletePBX allows a system backup of voicemails, system recordings, system configuration, CDRs, and Operator Panel configuration to be taken. Backups can be taken on a one-off basis, or a scheduled basis.

Backing up voicemail will back up all the voicemail messages and outgoing voicemail greetings for all the users configured on the system. If this is not backed up, then all the users will have to re-record their greetings, and they will be unable to retrieve historical voicemails which were received before the failure.

Backing up system 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.

Backing up system configuration will back up all the configuration data. This includes all of the configuration data for trunks, users, devices, IVRs, queues, time conditions—pretty much all the configuration data on the system. Without this backup, the system will have to be reconfigured all over again after a failure. This will be akin to starting from scratch.

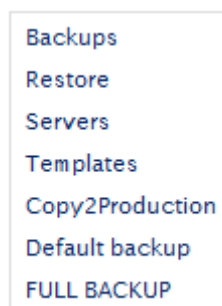
Backing up CDR data will back up all the call detail records stored on the system. Without this backup, if the system needs to be rebuilt all CDR records will be lost. There is no way to rebuild CDR records without this backup.

Backing up the Operator Panel will back up all the HTML and configuration data for the Switchboard. Without this backup, any Switchboard customizations will have to be completed again, and the Switchboard will have to be reconfigured.

Configuring Backup

Admin → Backup & Restore

In order to set up a backup, navigate to the **Admin** menu and select the **Backup & Restore** dialog, click on **Backup** in the menu on the right, and click on **New Backup**:



The **Backup** dialog will be displayed as follows:

Backup

Backup Name

Description

Status Email

Items

Backup Items

Type Path/DB Exclude Delete



Templates

- + CDR's
- + Config Backup
- + Exclude Backup Settings
- + Full Backup
- + System Audio
- + Voice Mail

Hooks

Pre-backup Hook

Post-backup Hook

Pre-restore Hook

Post-restore Hook

Backup Server

Backup Server

Storage Locations

Storage Servers



Available Servers

- + Legacy Backup (local)
- + Local Storage (local)

Backup Schedule

Run Automatically

Maintenance

Delete after Minutes

Delete after runs

Backup Name is a short text to allow you to easily identify the backup set. The name can be up to 50 characters long, including spaces.

Description allows you add useful information about the backup. This field can contain up to 255 characters.

Status Email is the email address to which a notification will be sent when the backup task is run.

In the **Backup Items** section, select items from the predefined templates that should be backed up in this backup schedule. Note that a single CompletePBX system can have multiple different backup schedules configured. It is possible to back up the **System Configuration** daily, **VoiceMail** weekly, and **System Recordings** and **CDR** monthly, if desired.

The **Hooks** section allows you configure scripts that will be activated before and after backup or restore.

The **Backup Server** section allows you to send the backup any backup server that is configured on the system. By default, the CompletePBX machine is defined as a backup server. In addition, you can use the Servers menu (on the right-hand side of the dialog) to configure servers for Email, FTP, Local, or SSH.

The **Backup Schedule** section allows you to configure the frequency of the backup. In order to set up a scheduled backup, select one of the predefined schedules from the **Run Automatically** drop-down menu, or select **Custom** and define your own schedule from the table. In order to create a one-time backup, select **Never** from the drop-down menu.

The **Maintenance** section allows you to control how long to keep backups. You can either configure for how long to keep the backups, or how many generations of backup should be stored.

Click on the **Submit Changes** button in order to save the schedule. Once saved, the backup will appear in the menu on the right:

Clicking on the name of an existing backup schedule will load the **Backup** screen, allowing the schedule and items that are being backed up to be edited.

Backup Templates

Template Name	Template includes	Template does not include
CDR's	Local call detail record database, i.e. the MySQL database named asteriskcdrdb	
Config Backup	Local call detail record database, i.e. the MySQL database named asteriskcdrdb	Configuration customizations that may have been made in /etc/asterisk/*.conf files, e.g. *_custom.conf files) – they are included in the Full Backup template

Template Name	Template includes	Template does not include
Exclude Backup Settings		Excludes the backup settings
Full Backup	<p>CDR's template</p> <p>Config Backup template</p> <p>Directory referenced by the variable <code>__ASTETCDIR__</code> (which by default points to <code>/etc/asterisk</code>), including all subdirectories</p> <p>Directory referenced by the variable <code>__AMPWEBROOT__</code> (which by default points to <code>/var/www/html</code>), including all subdirectories. (PBX web administration console modules are located in this directory tree)</p> <p>Directory referenced by the variable <code>__AMPSBIN__</code> (which by default points to <code>/usr/sbin</code>), including all subdirectories</p> <p>Directory <code>/etc/dahdi</code></p>	<p>User voicemails</p> <p>Voice mailbox greetings</p> <p>System audio greeting recordings</p>
System Audio	<p>Music on hold files referenced by the variable <code>__ASTVARLIBDIR__</code>/<code>moh</code> (which by default points to <code>/var/lib/asterisk/moh</code>) including all subdirectories</p> <p>Custom system recordings such as IVR menu recordings, referenced by the variable <code>__ASTVARLIBDIR__</code>/<code>sounds/custom</code> (which by default points to <code>/var/lib/asterisk/sounds/custom</code>) including all subdirectories</p>	

Template Name	Template includes	Template does not include
Voice Mail	Extension voice mail greetings and messages in the directory referenced by the variable <code>__ASTSPOOLDIR__</code> /voicemail (which by default points to <code>/var/spool/asterisk/voicemail</code>) including all subdirectories	

Amportal.conf



The **amportal.conf** file does not need to be specifically backed up, as it is automatically generated from the configuration database

Storage Servers

There are two default disk storage locations for backup files:

- Local Storage - this is the default option
 - The backup file is stored in `/var/spool/asterisk/backup/(backupjobname)/*.tgz` on the local machine
- Legacy Backup
 - Only used for backups made prior to CompletePBX v3

Backups can be sent to additional locations, such as an e-mail account, a remote FTP server, a remote server using SFTP, or a remote MySQL server. These options are used for sending backups to a different site.

Maintaining and Protecting Backups

The way in which CompletePBX provides backups is simple and effective, but requires consideration of two factors: storage and protection. In the same manner in which call recordings have to be managed (or they will fill up all the available storage space) CompletePBX backup schedules will continue to back up the system, and store the backup data indefinitely. 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 CompletePBX 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 CompletePBX machine 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.

Maintaining Backups

Maintaining backups is best accomplished by a script that simply looks for backups older than a certain threshold and deletes them. The following script will search for all backups older than 90 days and delete them. The script can be adjusted to suit the appropriate backup retention policy for your PBX by changing the value of the *BACKUPEXPIRY* line as follows:

The following script is called *OldBackupDeletion.sh*:

```
#!/bin/bash
# Change this path to reflect your backup storage location
# (default is /var/spool/asterisk/backup)
BACKUPS=/var/spool/asterisk/backup
# Change this number to reflect the maximum age of backups
# (in days)
BACKUPEXPIRY=90
# Change this number to reflect the maximum age of the
# deletion logs (in days) LOGEXPIRY=365
# Current date
DATE='date'
# Delete recordings older than $EXPIRY days
find $BACKUPS -mtime +$BACKUPEXPIRY -exec rm -rfv > removal-$(date +%Y-%m-%d).log\
# Delete log files older than $LOGEXPRY
find . -mtime +$LOGEXPIRY -exec rm -rf\
```

This script can be run once daily to find backup sets older than the age limit and delete them. Adding the following line to cron will execute the script from */etc/backupdeletion* daily at 5:00 a.m.:

```
0 5 * * * /etc/backupdeletion/OldBackupDeletion.sh
```

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 book, 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

Restore

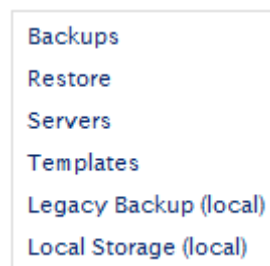
Backups taken by CompletePBX can only be restored back to a running CompletePBX system. In the event of a total failure, the operating system will have to be reinstalled along with CompletePBX and MySQL, and backup archives will have to be copied back onto the server before a backup can be restored.

- Restore to the same version of CompletePBX only
- Backups should always be restored to the same version of CompletePBX that created the backup.

- A backup may be restored to a different version without error, but there is a good chance that something will be broken and cause further headaches down the line

Every backup that is taken by CompletePBX is stored in `/var/spool/asterisk/backup`. Each backup schedule has its own subfolder in this directory. If a backup is being restored to a newly built system, the original subfolder and all contained backup archives must first be copied to `/var/spool/asterisk/backup` before the backup will be accessible from within the CompletePBX interface.

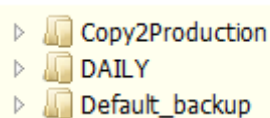
In order to restore a backup, navigate to the **Admin** menu and select the **Backup & Restore** dialog, click on **Restore** in the menu on the right. The **Restore** screen will be displayed. If you have uploaded the backup file to your CompletePBX box, you can use the Browse button to select the file from which you want to restore. Alternatively, select one of the backup locations from the right-hand menu.



Every backup schedule that has been set up and executed will be present in the restore menu, including both one-time backups and recurring backups. Click on the name of the backup set that is being restored to show a list of all available backup images from that backup schedule:

Restore

Select a file and click go






Go!

Download

Images are titled by the date and time they were taken. Click on the name of the backup image that should be restored to show all data contained within the image:

Restore

Select a file and click go

▲  Copy2Production	
20130320-162416-1363789456-346122097.tgz	
▲  DAILY	
20130410-000001-1365541201-1365475570.tgz	
20130411-000001-1365627601-1053508534.tgz	
▲  Default_backup	
20130306-155720-1362578240-222299108.tgz	
20130401-000002-1364763602-905909945.tgz	
20130501-000001-1367355601-528768693.tgz	

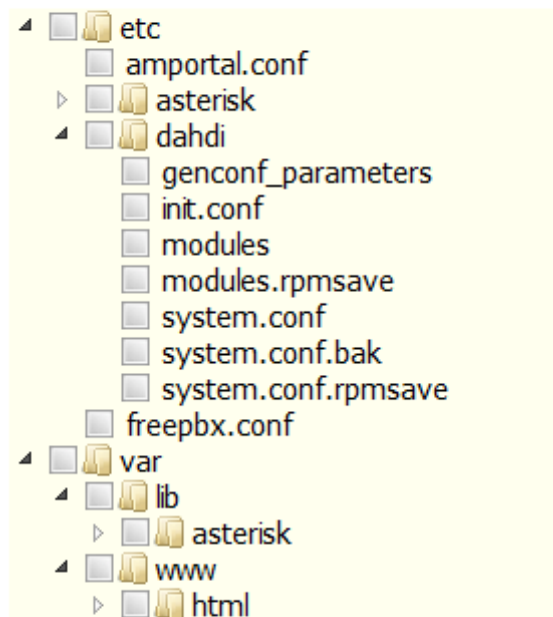
Name: Copy2Production
Created: Wed Mar 20 2013 16:24:16 GMT+0200
Time)
Files: 5073
Mysql DB's: 1
AstDB's: 1

Go! **Download**

The various links provide the ability to delete the set, restore the entire set, or selectively restore individual parts of a set. It is possible to restore multiple parts of a particular set individually.

Restore

Select files and databases to restore:



PBX Settings

Restore

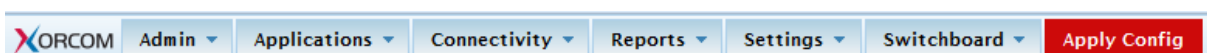
In order to start restoration, click on the item that should be restored. CompletePBX will warn about overwriting the item that is being restored. Click on **OK** to proceed or **Cancel** to stop the restore:

Precaution!



It is a good idea to take a full backup of all the CompletePBX configuration data prior to attempting a restore. The restore process will completely overwrite all the existing configurations for the component that is being restored. If the wrong backup set is accidentally restored, then it is not possible to undo the changes.

Once the restore is complete be sure to click on the red-colored **Apply Config** bar at the top of the screen in order to reload all restored changes into the live configuration being used by CompletePBX.

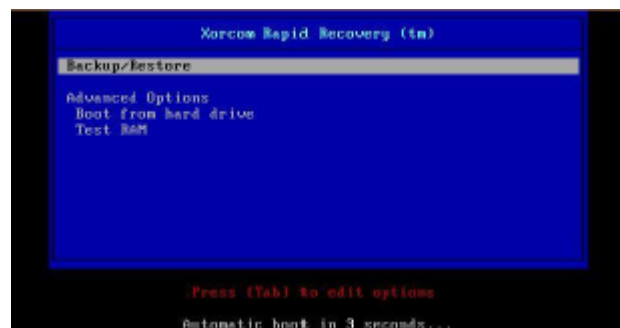


Rapid Recovery

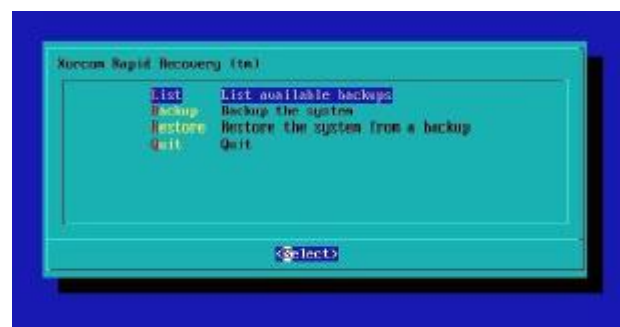
The Xorcom Rapid Recovery (XRR) is a unique accessory that can back up CompletePBX (including the operating system) to a USB Disk-on-Key (DOK). It enables simple, safe and speedy recovery of your CompletePBX system. Note, however, that by default, logs, voicemail, and call recording files are not backed 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 CompletePBX
- Connect your Xorcom Rapid Recovery (XRR) to a USB port of the CompletePBX
- Power on the CompletePBX 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.

Summary

Your CompletePBX system is prepared to handle disaster. You now know the appropriate steps to take in order to prevent the failure of CompletePBX. Your CompletePBX system is backing itself up regularly, and you are maintaining and protecting those backups. In the unfortunate event of a systems failure, you are also prepared to restore from one of those backups.

In the next chapter, we will discuss the ins and outs of securing CompletePBX.

12. Security and Access Control

A CompletePBX-based phone system, just like any other server on your network, runs on software that must be secured and maintained to ensure the system does not fall prey to hackers or malicious users. Given the nature of a PBX there is often no leeway afforded for downtime in the event that a system is compromised, so the best practice is to know how to protect the system to start with. In this chapter, we will discuss the following:

- CompleteSBC integrated session border controller
- Strong passwords for SIP and IAX2 extensions. You can use the **Weak Passwords** dialog (in the **Reports** menu) to detect potentially problematic passwords
- Secure SIP settings in the General Settings dialog
- Creating a safe dialing plan
- Securing remote access to the PBX
- Securing CompletePBX administration through administrator accounts
- Intrusion Detection and Prevention

CompleteSBC

CompleteSBC is a software-based session border controller that is integrated into CompletePBX. You can download the latest CompleteSBC Handbook from the [Xorcom Product Manuals](#) page of our website.

CompleteSBC serves as the first line of defense, fending off attacks coming over the Internet, hiding internal topology, applying rate limits and performing Call Admission Control, limiting the number of simultaneous calls and call duration, off-loading registrar and registration throttling and providing confidentiality using cryptographic TLS and SRTP protocols

CompleteSBC is initially configured to perform the following functions:

- Register caching
- Limit the number of concurrent calls that pass through the CompleteSBC public realm
- Reject SIP requests from endpoints where the user agent names are not configured in CompleteSBC
- All accepted SIP requests from the CompleteSBC public realm are routed to CompletePBX
- All accepted SIP requests from the CompleteSBC internal realm are routed to the CompleteSBC public realm according to the information contained in the SIP Request-URI (R-URI)

CompletePBX and CompleteSBC are shipped with default configuration designed to provide maximum protection. By default, all incoming communications from the CompleteSBC public signaling interface are blocked. The administrator will need to un-block them in order to enable incoming calls to pass through CompleteSBC.

CompleteSBC includes a demo license that permits generation of up to 200 simultaneous external calls, with each call limited to a maximum duration of 90 seconds.

You may choose not to enable CompleteSBC on your system. In this case, you will need to follow certain instructions to disable the CompleteSBC, which are [detailed here](#).

CompleteSBC Configuration Tasks

In order to allow calls to pass through CompleteSBC, you will need to carry out the following tasks:

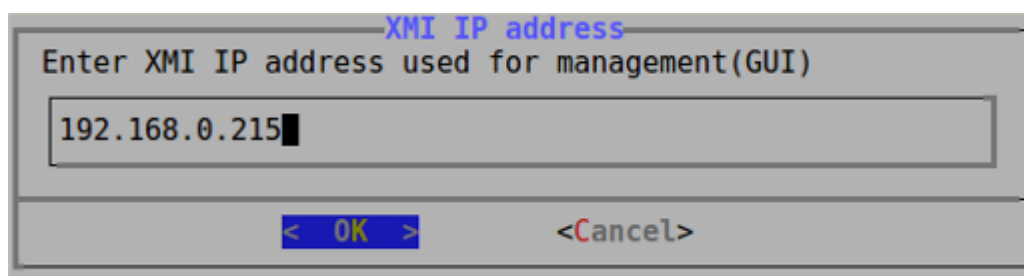
- Configure and enable the CompleteSBC web interface

- Configure the IP address for the CompleteSBC signaling and media interfaces
- Allow SIP requests on the CompleteSBC public realm
- Ensure that the SIP device agent names you use in CompletePBX appear in the list of permitted devices in CompleteSBC

Enabling the CompleteSBC Web Interface

The CompleteSBC Web interface must be bound explicitly to the IP address of the CompletePBX machine. This can be done, using the command line interface, as follows:

- Connect to CompletePBX using SSH
- Login as user **root** using the default linux password (that is documented in the Getting Started Guide that was packed with your CompletePBX hardware.)
- Run **sb-init-gui** utility, by typing sbc-init-gui, and configure an IP address:



- You can access the CompleteSBC web interface by clicking on the CompleteSBC icon that is on the CompletePBX Launch Pad. This will present you with the following login dialog

Login to CompleteSBC	
You must enter a username and password to login to the CompleteSBC on 192.168.6.98.	
Username	<input type="text"/>
Password	<input type="password"/>

- Use your standard linux credentials to login (i.e. user **root** with the default linux password that is documented in the Getting Started Guide that was packed with your CompletePBX hardware.)

Configuring IP Addresses for Signaling and Media Interfaces

System -> Interfaces

Navigate to the **System** menu and select the **Interfaces** application to access the **SBC - Interfaces** dialog as shown below:

SBC - InterfacesWed, 11 Mar 2015 11:11:02
Up since: Wed, 11 Mar 2015 06:10:35[Select all](#) | [Invert selection](#) | [Insert new Interface](#)Displaying Records 1-5 of 5 | [First](#) | [Prev](#) | [1](#) | [Next](#) | [Last](#)

	Interface name	Interface description	Interface type	System interface	IP address	Public IP address	Port(s)	Interface options
<input type="checkbox"/>	ifxmi	XMI interface	External mgmt.	eth0	192.168.6.98	-	-	edit
<input type="checkbox"/>	medint	Media internal	Media	lo	127.0.0.1	-	20002 - 20402	edit
<input type="checkbox"/>	medpub	Media public	Media	eth0	192.168.6.98	-	20002 - 20402	edit
<input type="checkbox"/>	sigint	Signaling internal	Signaling	lo	127.0.0.1	-	6075	edit
<input type="checkbox"/>	sigpub	Signaling public	Signaling	eth0	192.168.6.98	-	6075	edit

[Select all](#) | [Invert selection](#) | [Insert new Interface](#)Displaying Records 1-5 of 5 | [First](#) | [Prev](#) | [1](#) | [Next](#) | [Last](#)

You must now define IP addresses for the **medpub** and **sigpub** interfaces. Click the [edit](#) link for each item in turn, and define the correct IP address. The IP address should be the local IP address of your CompletePBX system.

Public IP Address

If you want CompleteSBC to substitute your public Internet IP address in the outbound SIP messages, then you will have to define the address in the **Public IP address** field for both **medpub** and **sigpub** interfaces, and disable this feature in the CompletePBX SIP settings.

The IP port ranges for both **medint** and **medpub** interfaces can be modified. The default range is 20002-20402, which is sufficient for 200 simultaneous calls (since RTP only uses even-numbered ports). To enable a higher number of simultaneous calls, the range can be modified by adding 2 ports for each additional call. For example, if you want to allow for an additional 100 simultaneous calls, you would need to extend the range of ports by 200. Be aware that if you change the default IP port range for the **medpub** interface (which is set to 20002-20402/UDP by default) then you must make corresponding changes in the CompletePBX firewall configuration.

Activate and Reboot!

After making changes to the IP addresses, you will need to click on **activate** (at the top of the dialog) and reboot your CompletePBX machine after making changes to the interface settings.

Enable Communications with CompleteSBC

CompletePBX and CompleteSBC are pre-configured for maximum protection, so by default all inbound traffic is blocked by the CompleteSBC **sigpub** interface.

Most of the traffic restriction-related parameters are found in the **Settings** table. Navigate to the

Tables menu and select **Table: settings** from the dropdown list in order to reach the following dialog:

SBC - Provisioned table settings

Wed, 11 Mar 2015 11:28:03
Up since: Wed, 11 Mar 2015 06:10:35

View older version of the table:

3 - (provisioning)

Select all | Invert selection | Insert new record | Activate changes Displaying Records 1-3 of 3 | First | Prev | 1 | Next | Last

uuid	key_value	value	
<input type="checkbox"/> 10a73849-2889-7068-9aad-00006af4f8f9	allowed-user-agents	VP[0-9] Akuvox\s Aastra\s Cisco\SPA[0-9] ES[0-9] Fanvil\s Grandstream\s Htek\s Polycom snom[0-9] VSP[0-9] XP01[0,2,5]0 Yealink SIP-T[0-9] IP Phone SIP-T[0-9] Z\s Zoiper\s Asterisk\s GHJ- FPBX-	edit
<input type="checkbox"/> 34d7d757-bc30-66e8-2330-000066addc44	block-public	1	edit
<input type="checkbox"/> 23d56424-8fea-bac8-0a47-000075121db2	call-limit	200	edit

Select all | Invert selection | Insert new record | Activate changes Displaying Records 1-3 of 3 | First | Prev | 1 | Next | Last

The table contains three key/value pairs:

Key Value	Description
allowed-user-agents	A regular expression for detecting permitted SIP user agent names. By default, the expression includes SIP user agent names for all supported SIP phones listed in the CompletePBX Endpoint Manager, Zoiper, standard Asterisk, FreePBX, and CompletePBX.
block-public	1 – reject incoming SIP requests received from the CompleteSBC public realm 0 – accept incoming SIP requests received from the CompleteSBC public realm
call-limit	Maximum number of concurrent calls that can pass through the CompleteSBC public realm

You can change the values in the table according to your requirements. Click on **Activate changes** to apply the new settings when you have finished,.

NAT Router Configuration

If you have remote SIP extensions, then it is necessary to configure port forwarding on your NAT router configuration:

- The CompleteSBC **sigpup** interface port (by default this is defined as 6075/UDP) must be forwarded to CompletePBX
- The CompleteSBC **mediapub** interface ports range (by default this is set to 20002-20402/UDP) must be forwarded to CompletePBX

CompletePBX Firewall Configuration

The default setting of the CompletePBX Firewall only allows access to the SIP ports (5060/UDP & TCP and 5061/TCP) for requests which originate from hosts with private IP addresses, i.e.

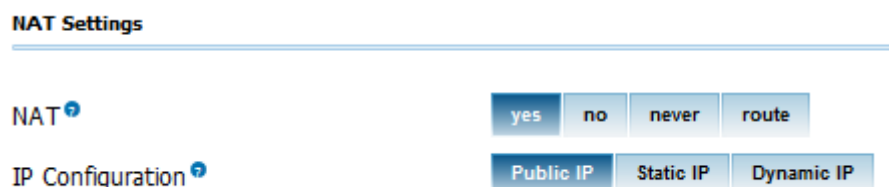
- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

As a result, CompletePBX will not be able to receive SIP calls from remote SIP endpoints. If you do not want to use CompleteSBC, you will need to modify the CompletePBX firewall configuration so that the SIP ports will be accessible from **any** source IP address.

If you change the default IP port range for the **medpup** interface (which is set to 20002-20402/UDP by default) then you must make a corresponding changes in the CompletePBX firewall configuration.

CompletePBX Configuration


You will need to disable external IP address substitution by CompletePBX in the SIP messages. Navigate to the CompletePBX **Settings** menu, select **SIP Settings** from the dropdown list, and define the **IP Configuration** parameter in the **NAT Settings** as **Public IP**.



You will also need to define a list of domains that can be used in the SIP requests. For example:

- Local SIP phones will send SIP requests to CompletePBX using 192.168.6.98:5060
- Remote SIP phones/servers will send SIP requests to CompletePBX to either 212.1.2.3:6075 or mypbx.mycompany.com:6075

Navigate to the CompletePBX **Settings** menu, select the **SIP Settings** application, and scroll down to the **Other Sip Settings** section. You will need to define the IP addresses of these three domains, as shown in the following example:

Other SIP Settings 

allowexternaldomains	=	no
autodomain	=	yes
domain	=	192.168.6.98
domain	=	212.1.2.3
domain	=	mypbx.mycompany.com

Add Field

You will also need to configure the remote extension that is used to communicate with the CompletePBX external IP address, and ports that are forwarded by the NAT router to the CompleteSBC **sigpub** interface.

Remote SIP Server Configuration

CompletePBX and CompleteSBC must be configured in a special way in order to allow communication between CompletePBX and the remote SIP server:

- CompleteSBC **sigint** interface (127.0.0.1:6075) must be defined as an outbound proxy in the SIP trunk settings.
- All SIP messages from the remote SIP server will be sent by CompleteSBC from the **sigint** interface, so CompletePBX will not be able to recognize the SIP server messages by their source IP/port. Therefore, it will be necessary to configure CompleteSBC in such a way that it will substitute the CompletePBX SIP trunk name in the user name field of the **From** header. In order to preserve the Caller ID that usually appears in that field, CompleteSBC should create the Remote-Party-ID header, and place the Caller ID value there.
- If a remote SIP server communication must be routed to the service provider's outbound proxy, then this will need to be configured in CompleteSBC

The following screenshot should help to illustrate this:

Trunk Name [?]:

PEER Details [?]:

```

host=myitsp.cc
defaultuser=4003
remotesecret=x4003x
type=friend
outboundproxy=127.0.0.1:6075,force
trustpid=yes
qualify=no
context=from-trunk
insecure=invite
    
```

Registration

Register String [?]:

As you can see, the **outboundproxy** parameter points on the internal SBC interface (**sigint**).

In the Registration string, the **MyITSP?** prefix references to the **MyITSP** peer setting. This causes CompletePBX to send REGISTER requests to the **outboundproxy** (i.e. the CompleteSBC internal interface) that is defined in MyITSP PEER Details field.

In many cases, service providers have their own session border controller and will require that your PBX send the SIP messages there (to their session border controller) rather than directly to their SIP server (e.g., **myitsp.cc**). This message-redirection must be implemented in CompleteSBC, by using the Routing menu item in the CompleteSBC Web interface.

You can see an example of such a configuration below:

SBC - Routing (B) Rules

Up since: Wed, 11 Mar 2015 06:10:35

Select all | Invert selection | Insert new Rule | Append new Rule

Displaying Records 1-3 of 3 | First | Prev | 1 | Next | Last

Conditions		Route to		Call Agent	Active	Comment				
Realm	Agent	Realm	Agent				edit	clone	up	down
<input type="checkbox"/>	Source Realm == "internal" AND R-URI Domain == "myitsp.cc"	public	MyITSP-proxy	✓	✓	An example of rule that sends PBX requests to ITSP outbound route	edit	clone	up	down
<input type="checkbox"/>	Source Realm == "internal"	public	public-users	✓	✓	Route Asterisk requests to the public domain	edit	clone	up	down
<input type="checkbox"/>	Source Realm == "public"	internal	PBX	✓	✓	Route inbound requests to the PBX.	edit	clone	up	down

Select all | Invert selection | Insert new Rule | Append new Rule

Displaying Records 1-3 of 3 | First | Prev | 1 | Next | Last

As you can see, CompleteSBC will route all SIP requests received from 'internal' realm (where CompletePBX is located) to the **MyITSP-proxy** call agent and destined to myitisp.cc (the host configured in the **MyITSP** trunk.) The **MyITSP-proxy** call agent is defined in the public realm of the CompleteSBC configuration ('Realms', 'call-agents' for the 'public' realm):

Now let us review a solution for handling SIP requests that are sent by the remote SIP server (**myitisp.cc**) to CompletePBX. Let us also assume that your server provider has his own session border controller (e.g., 1.2.3.4:5060 in our example) that actually sends the messages to the PBX.

The provider's session border controller is configured as the **MyITSP-proxy** call agent for the CompleteSBC **public** domain. Now we can define a set of inbound rules for the **MyITSP-proxy** call agent that will do the following:

- Create the Remote-Party-ID header, if it doesn't exist. Use the user name defined in the **From** header for it. Don't change the existing Remote-Party-ID header.
- Replace the user name in the **From** header with the trunk name defined in the CompletePBX configuration (**MyITSP**):



Trustpid

It is necessary to define **trustpid=yes** in the CompletePBX trunk configuration. Otherwise, CompletePBX will not accept the Caller ID that appears in the Remote-Party-ID header field.

Licensing

CompleteSBC has a demo license installed that allows generation of up to 200 simultaneous calls, each having a maximum duration of 90 seconds. In order to review the current licensing status, or apply a commercial license, navigate to the **System** menu and select **License** from the dropdown list.

In order to apply a commercial license, verify that CompletePBX has Internet access and carry out the following steps:

1. Input the activation code in the **Activation Code** field
2. Input the CompletePBX serial number in the **Serial Number** field
3. Click the **Apply** button

In a few seconds you should see details of the newly-activated license in the **Current License** field at the top of the dialog.

If it is not possible to provide Internet access for CompletePBX then you can get a license file instead of the activation code. That license file can be uploaded to the PBX and then activated. Please contact a Xorcom authorized reseller for assistance.

Instructions for Disabling CompleteSBC

Follow the instructions below to disable the CompleteSBC on your CompletePBX system.

Firstly, you will need to decide which ports to use for SIP communication. If you decide to use ports other than the default ports of 5060/5061, you will need to navigate to Admin menu, select System Settings, select Applications, and modify the ports that are defined as SIP-PBX.

Name	Ports	Protocol	
DNS	53	Both	
DRBD	7789	TCP	
NTP	123	UDP	
TFTP	69	UDP	
DHCP	67:68	UDP	
HTTP	80	TCP	
SSH	22	TCP	
SIP-PBX	5060,5061	Both	
RTP-PBX	10000:20000	UDP	
IAX2	4569	UDP	
Asterisk-AMI	5038	TCP	
Switchboard	4445	TCP	
RTP-SBC	20002:20402	UDP	
SIP-SBC	6075,6076	Both	
HTTPS	443	TCP	

Secondly, you will also need to navigate to Admin menu, select System Settings, select Rules, and modify the source IP address that are defined for the SIP-PBX application. When using CompleteSBC, only local network addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) are allowed access on the SIP ports.

Rules

[Storage Info](#)
[Time Setting](#)

	Action	Interface	Source		Destination		
			IP	Application	IP	Application	
	allow	any : in	any	any	any	TFTP	
	allow	any : in	any	any	any	NTP	
	allow	any : in	any	any	any	DNS	
	allow	any : in	any	any	any	DRBD	
	allow	any : in	any	any	any	HTTP	
	allow	any : in	any	any	any	HTTPS	
	allow	any : in	any	any	any	SSH	
	allow	any : in	any	any	any	IAX2	
	deny	any : in	any	any	any	Asterisk-AMI	
	allow	any : in	any	any	any	Switchboard	
	allow	any : in	any	any	any	DHCP	
	allow	any : in	any	any	any	SIP-SBC	
	allow	any : in	any	any	any	RTP-SBC	
	allow	any : in	10.0.0.0/8	any	any	SIP-PBX	
	allow	any : in	172.16.0.0/12	any	any	SIP-PBX	
	allow	any : in	192.168.0.0/16	any	any	SIP-PBX	



Firewall

When CompleteSBC is not enabled and you want to enable external SIP communication, you will need to open the SIP ports to allow access from any IP address.

SBC - Config License

Current License

```
sbc_serial = Demo-Version  
sbc_max_calls = 200  
sbc_max_duration = 90
```

Request New License

License Status
Activated

Activation Code

Serial Number

Activate

Upload License File

License

License file: No file selected.

SIP/IAX2 Extensions

Make sure that you define long and complicated passwords for SIP and IAX2 extensions. They should consist of a mixture of digits, upper-case, and lower-case letters. The minimum password length should be 8 characters.

Define IP address filters for the local extensions. For example, if you know that extension 2001 is assigned to a SIP phone that is installed in the local office then you can define the following IP filter in the **Device Options** section of the **Extensions** dialog:

```
deny: 0.0.0.0/0.0.0.0
permit: 192.168.1.0/255.255.255.0
```

This will ensure that only devices from within the internal network can connect to your CompletePBX as extension 2001, and prevent any other device or program from outside your network from doing that.

General SIP Settings

Settings → *SIP Settings*

Codecs (Transcoding)

The codecs that each side of a call supports play the biggest role when choosing a default codec for an endpoint or a trunk. The rule of thumb for codec selection is to try and configure an endpoint to use the same codec as the trunk it will be using for external calls.

When an endpoint uses a different codec than the trunk carrying the endpoint's call, CompletePBX must convert the audio stream of the call in real-time. This process is known as **transcoding**. Transcoding uses processor resources, so excessive use of transcoding can cause a significant load on the CompletePBX server. A system performing transcoding for every call is able to handle a significantly fewer number of concurrent calls than a system that does not.

Transcoding also incurs a latency penalty for the call's audio (that is, the time between when one party says something and the other party hears it is increased). Depending on the original quality of the call before transcoding, this could be enough to make an audible difference in the amount of lag time that each party on the call hears. In extreme cases, it may not be possible to carry on a conversation.

DAHDI trunks (PSTN lines, PRI lines, and T1 lines) will use the G.711 codec. North American and Japanese style trunks should use the G.711 ulaw codec. Trunks in other areas of the world should use G.711 alaw. VoIP trunks will typically use either G.711 or G.729 and they may support both.

Transcoding costs can be determined by running the command *core show translation* in the Asterisk CLI. Asterisk will output a matrix of all the codecs it can use and the latency penalty that a call will incur when being transcoded between each available codec.

Note that certain codecs may need to be purchased (for example, Digium sells the G.729 codec on a per-channel basis). Some codecs may be free, but will need to be installed before they can be used, such as Speex.

The other factor to consider during codec selection is the available bandwidth where the CompletePBX server resides.

The G.711 codecs (*ulaw* and *alaw*) use about 64 kbps for each side of the call (that is, 64 kbps for sending what is said, and 64 kbps for receiving what the other party says, for a total of 128 kbps). The G.729 codec knocks the required bandwidth down to 8 kbps for each side of the call. The iLBC can use about 15 kbps per side of the call, and Speex is a variable bit-rate codec, using between 4 kbps and 48 kbps for each side of the call. Using 128 kbps of bandwidth to connect a phone over a local network to CompletePBX is certainly no problem as there will be plenty of bandwidth to spare. Although, when VoIP trunks or phones outside of the local network come into play, bandwidth is significantly limited. Many broadband providers have a limited upload speed of 768 kbps or less (this is especially common for DSL connections). Factoring in normal connection overhead, this leaves us

with space for about 10 active calls if we use G.711, but dozens of calls if we use G.729.

The rule of thumb when selecting a codec is to try to use the same codec for endpoints and trunks as long as the bandwidth required for doing so does not exceed available resources. If matching the codecs is not possible, the next best method is simply to balance the requirement for lowering bandwidth against the requirement for reducing transcoding as much as possible.

Keep in mind that not all of the endpoints must use the same codec. For example, if all calls go out of G.711 trunks, it is always feasible to have all of the endpoints on the network that is local to CompletePBX use G.711, while endpoints outside of the network (that connect to CompletePBX over a broadband connection) use G.729. This method will only use transcoding for those endpoints that are outside of the office. External calls will use 16kbps of bandwidth to connect with CompletePBX.

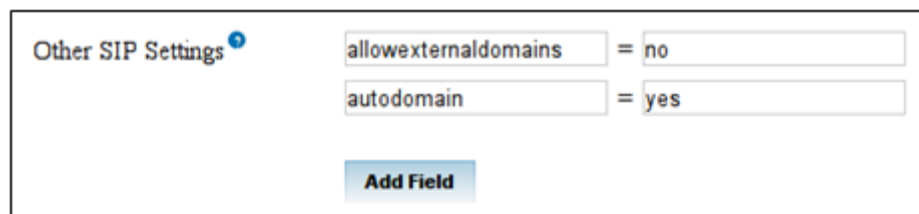
Advanced General Settings

Disable inbound calls from unknown sources. This can be done by configuring the **Allow SIP Guests** parameter as “No”. You can configure this by navigating to the **Settings** menu, selecting the **SIP Settings** dialog, and navigating down to the **Advanced General Settings** section. This value is the default setting for CompletePBX.

Disable accepting requests for domains not serviced by your CompletePBX. You can configure this by navigating to the **Settings** menu, selecting the **SIP Settings** dialog, navigating down to the **Other SIP Settings** section, and adding the following parameters:

allowexternaldomains=no disables requests from domains not defined in the CompletePBX network

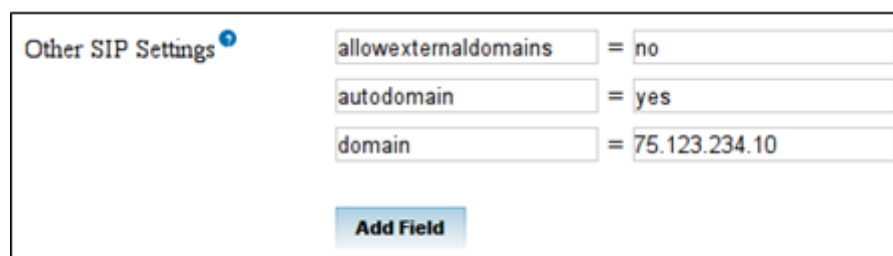
autodomain=yes implicitly adds CompletePBX IP addresses to the list of the local domains.



Other SIP Settings	allowexternaldomains	=	no
	autodomain	=	yes
Add Field			

Note that the external SIP endpoints and SIP servers of Internet Telephony Service Providers (ITSP) will send SIP request to the PBX by using the NAT router external interface IP address. By default, CompletePBX will reject such requests. In order accept inbound SIP requests, click on the **Add** button, and define one or more **domain** parameters.

For example, if the external IP address of your CompletePBX is 75.123.234.10 then you must define:



Other SIP Settings	allowexternaldomains	=	no
	autodomain	=	yes
	domain	=	75.123.234.10
Add Field			

Make sure that CompletePBX will reject unwanted SIP requests with the same reject reason code, regardless of the real reason. This significantly hampers brute-force attackers from guessing the SIP

user name and secrets. This is configured in CompletePBX by default in the */etc/asterisk/sip_general_additional.conf* file, with the parameter *alwaysauthreject=yes*

Dialplan Configuration

Do not configure uncontrolled trunk-to-trunk calls. For example, if you define a DHADI trunk, you should not associate the context **from-internal** to the trunk. If you did so, you would be allowing any traffic arriving via the trunk to have full access to functionality of CompletePBX that should only be made available to local extensions.

Make sure that DISA and Call-back are well protected by using strong passwords.

You should define passwords (PIN) for all outbound routes that are used for International calls. This will significantly hamper intruders from making malicious calls. Refer to the [PIN Sets](#) section in Chapter 8 for help configuring PIN sets.

Remote Access and Lock Down

The point at which a system is opened up so it can be remotely administered is almost always the point of compromise in an intrusion. It is a good idea to close off the system as much as possible from the outside world, in addition to locking down all network access to the server.

CompletePBX should be installed on a protected LAN, and should not be directly connected to the public Internet. The LAN should be protected by a Firewall/NAT router. The built-in firewall that is installed on CompletePBX can be used as an additional means of protection.

- Do not expose the SIP (5060/udp) or IAX2 (4569/udp) ports if you have not defined any remote extensions.
- Use a non-standard port for SSH. Instead of exposing port 22/tcp, define port forwarding from a not well-known port, for example 4223/tcp, on the external interface to port 22/tcp of CompletePBX.
- Enable the SSH connection from specific IP address only. For example it could be the IP address of the company that provides technical support for you CompletePBX.
- Optionally it is possible to disable the password authentication method in the CompletePBX SSH server configuration and use only private/public key authentication. Refer your SSH client documentation for further details of the private/public key configuration.
- Never expose the HTTP (80/tcp) port at all. Always use SSH tunneling to access the CompletePBX Web interface.

VPN or SSH Tunnels

The most secure method of remote access is the one that does not exist directly at all. If the organization where the PBX will be deployed has an existing VPN solution, then the most secure way to access their CompletePBX interface is over a VPN tunnel.

If no VPN exists, it is still possible to reduce the attack surface considerably by forcing Web access to CompletePBX through an SSH tunnel.

SSH Tunneling on Linux

In order to generate an SSH tunnel under a Linux operating system, use a command similar to the following:

```
sudo ssh -L 3000:127.0.0.1:80 root@<external PBX IP address>
```

3000 is the port on your computer that will be forwarded to port 80 on the CompletePBX. You

replace this value with any other free port on your local machine.

<**external PBX IP address**> is the externally accessible IP address of the CompletePBX to which you to connect.

For example, if CompletePBX has an external IP of 2.2.2.2, our SSH command would look like this:

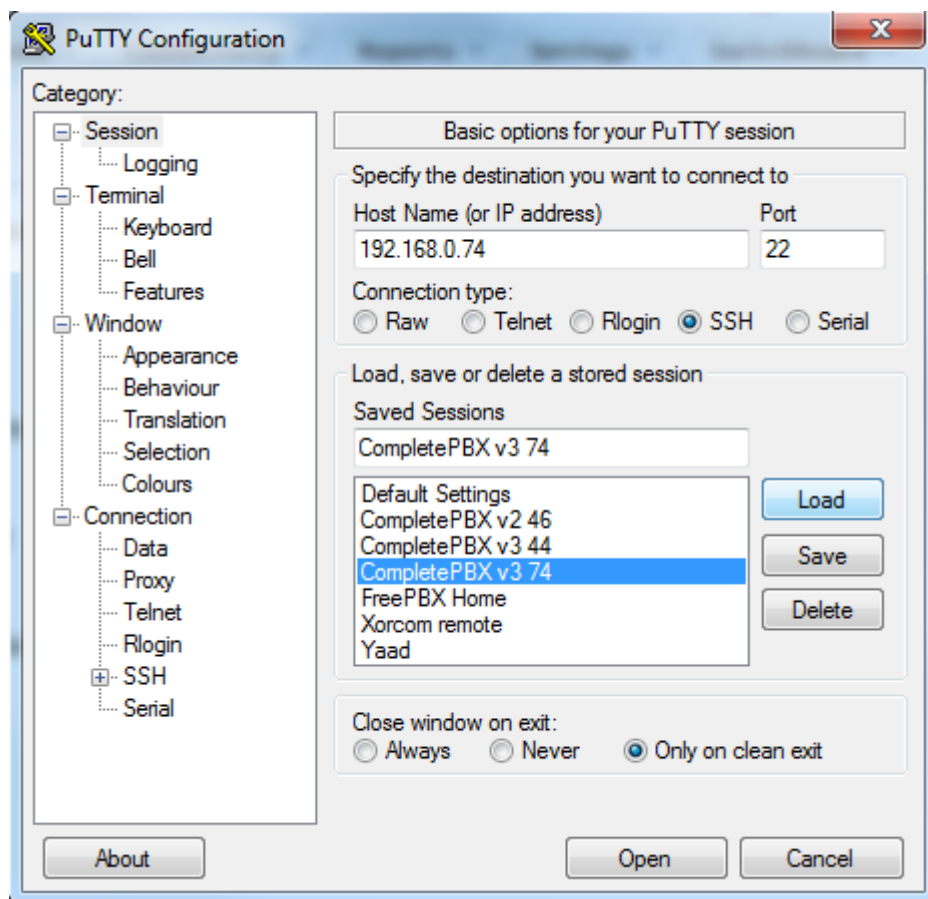
```
sudo ssh -L 3000:127.0.0.1:80 root@2.2.2.2
```

The above command will map local port 3000 to port 80 on the target machine. Once the SSH session has been established, opening up a Web browser and pointing it to <http://localhost:3000> will load the CompletePBX interface on your machine.

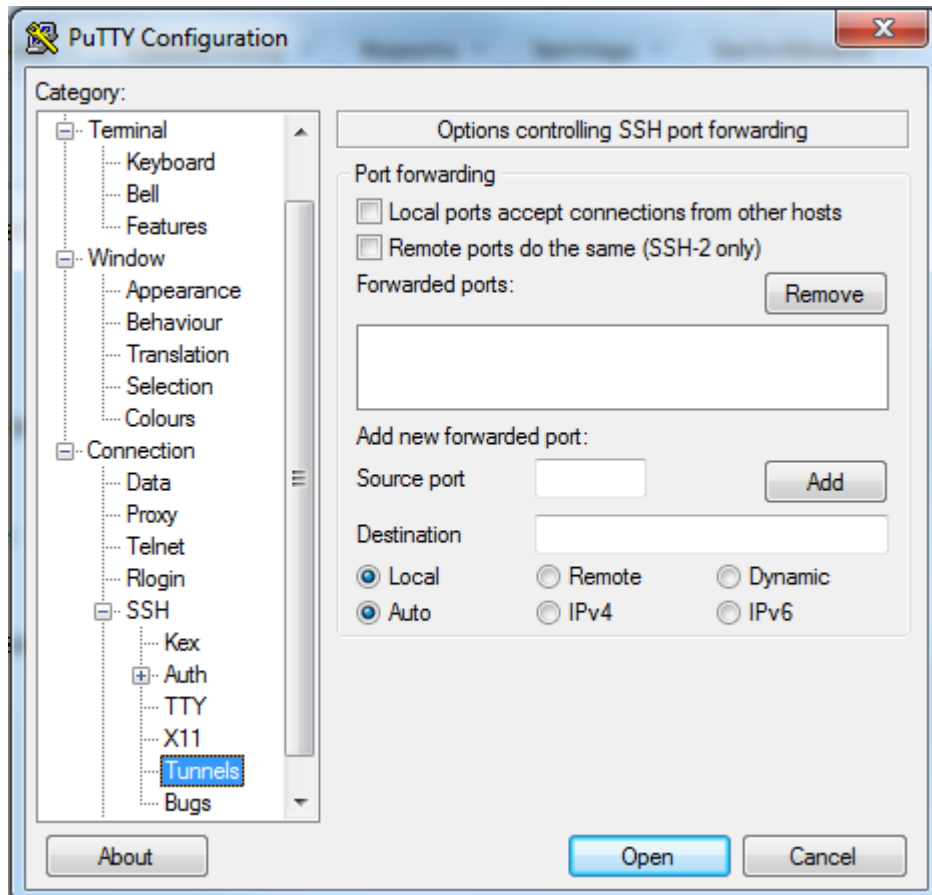
SSH Tunneling on Windows

Generating SSH tunnels under Windows can be accomplished using a simple utility called PuTTY. PuTTY can be downloaded from <http://www.chiark.greenend.org.uk/~sgtatham/putty/>.

In order to set up an SSH tunnel in PuTTY, first enter the external IP address into the **Host Name (or IP address)** field:



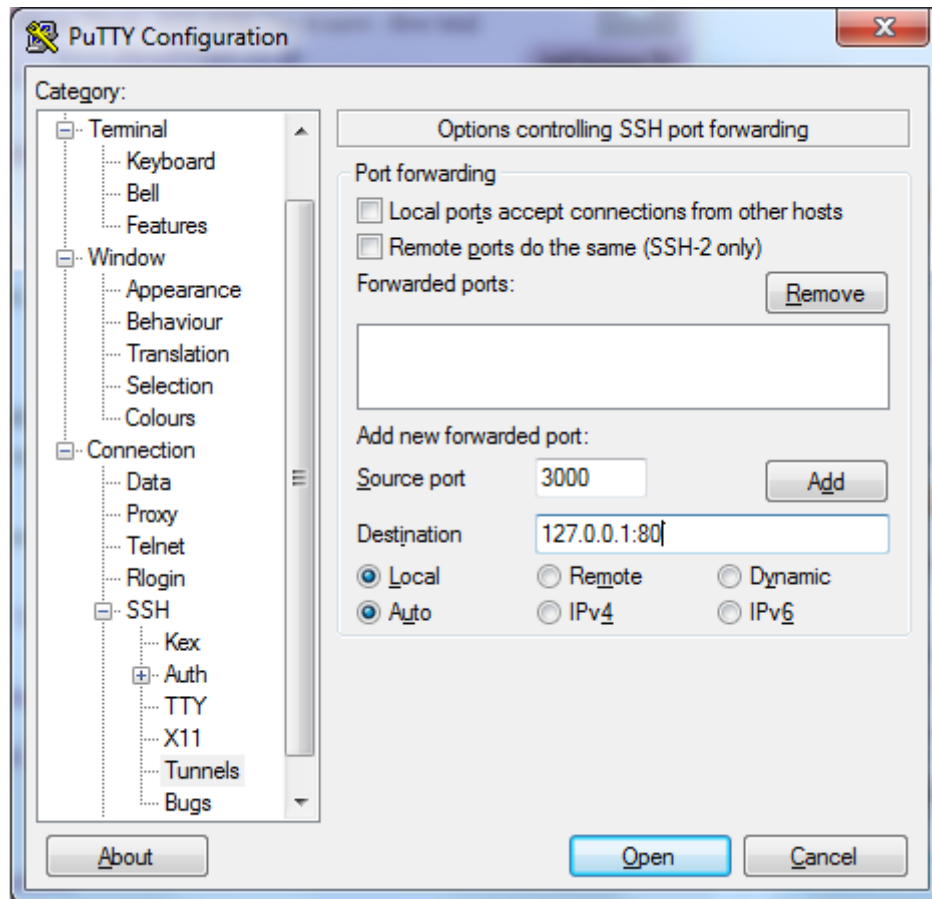
Expand **SSH** in the menu on the left (under **Connection**) and click on **Tunnels**:



In the **Source port** field, type in 3000.

In the **Destination** field, type in the loopback IP address of the PBX server followed by a colon, and the port on which the Apache server is running.

Leave all other settings at with their default value, and click on the **Add** button. Now you can click on the **Open** button to open the SSH tunnel.



Once the tunnel is authenticated, CompletePBX can be viewed by opening a Web browser and browsing to <http://localhost:3000>



Administrator Accounts

Admin → Administrators

CompletePBX incorporates the concept of different levels of administrator access. Administrator accounts can have their access restricted to a specific extension range, or a specific set of dialogs. Separate administrator accounts should always be given out to anyone who administers the CompletePBX system. Any staffing changes will then simply require a person's account to be removed to ensure they no longer have access.

Administrator Accounts and Permissions

Admin → Administrators

CompletePBX is supplied with 4 pre-defined users, each having fewer rights than the previous user, as defined in the table below:

Menu	Dialog	superadmin	admin	superuser	user
Admin	Administrators	✓			
	Backup & Restore	✓	✓		

Menu	Dialog	superadmin	admin	superuser	user
	Blacklist	✓	✓	✓	
	CallerID Lookup Service	✓	✓		
	Custom Destinations	✓			
	Custom Extensions	✓	✓	✓	
	DUNDI Lookup	✓	✓		
	Feature Codes	✓	✓	✓	
	Module Admin	✓			
	Phone Restart	✓	✓		
	System Recordings	✓	✓		
	System Settings	✓	✓		
	System Speed Dialing	✓	✓	✓	
Applications	Announcements	✓	✓	✓	
	Call Flow Control	✓	✓		
	Call Recording	✓	✓		
	Callback	✓			
	Conferences	✓	✓	✓	
	DISA	✓			
	Directory	✓	✓		
	IVR	✓	✓	✓	
	Languages	✓	✓		

Menu	Dialog	superadmin	admin	superuser	user
	Misc Applications	✓	✓		
	Misc Destinations	✓	✓		
	Music on Hold	✓	✓	✓	
	PIN Sets	✓	✓		
	Paging & Intercom	✓	✓		
	Queue Priorities	✓	✓		
	Queues	✓	✓	✓	
	Ring Groups	✓	✓		
	Set CallerID	✓	✓		
	Time Conditions	✓			
	Time Groups	✓			
	Voicemail Blasting	✓	✓		
	Wake Up Calls	✓	✓	✓	
Connectivity	Bulk DIDs	✓			
	Bulk Extensions	✓			
	DAHDI Channel DIDs	✓			
	Extensions	✓	✓	✓	✓
	Follow Me	✓	✓	✓	✓
	Inbound Routes	✓			
	Endpoint Manager	✓			
	Outbound Routes	✓			

Menu	Dialog	superadmin	admin	superuser	user
	Routing Groups	✓			
	Trunks	✓			
Reports	CDR Reports – Advanced	✓	✓	✓	
	CDR Reports - Basic	✓	✓	✓	
	Extension Settings	✓	✓	✓	
	PBX Log	✓	✓	✓	
	PBX Status	✓	✓	✓	
	Phone Book	✓	✓	✓	
	System Status	✓	✓	✓	
	Weak Passwords	✓	✓	✓	
Settings	Advanced	✓			
	Asterisk Managers	✓			
	Congestion Messages	✓			
	Fax Configuration	✓	✓	✓	
	IAX Settings	✓			
	PBX Log Settings	✓	✓	✓	
	Parking Lot	✓	✓		
	SIP Settings	✓			
	Voicemail	✓	✓		
Switchboard	Buttons	✓	✓	✓	

Menu	Dialog	superadmin	admin	superuser	user
	Groups	✓	✓	✓	
	Permissions	✓	✓		
	Templates	✓	✓		
	Users	✓	✓		

Passwords



The password for superadmin user is factory set, and is documented in the Getting Started Guide that was packed with your CompletePBX hardware. However, we strongly recommend that you change this password.

You must set the passwords for admin, superuser, and user before any of these users will be able to access the system.


You can manage the permissions granted to each user and modify passwords from the Administrators dialog. Login to CompletePBX, navigate to the **Admin** menu and select the **Administrators** dialog. The **Add User** screen is shown:


General Settings


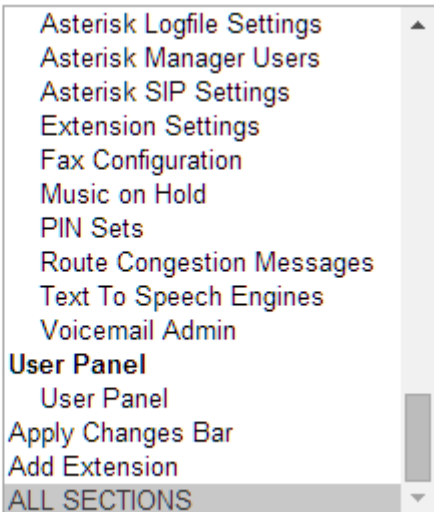
Username : 

Password : 

Access Restrictions

Department Name :

Extension Range : to

Admin Access : 

- Asterisk Logfile Settings
- Asterisk Manager Users
- Asterisk SIP Settings
- Extension Settings
- Fax Configuration
- Music on Hold
- PIN Sets
- Route Congestion Messages
- Text To Speech Engines
- Voicemail Admin
- User Panel**
- User Panel
- Apply Changes Bar
- Add Extension
- ALL SECTIONS

In the **Username** field, enter the account name for the user that is being set up. This is the name that the user will enter when prompted during the login process.

In the **Password** field, assign a password to the new user. This is the password that the user will enter when prompted during the login process.

It is best to use a mixture of upper- and lower-case letters, numbers, and special characters. Note that it is technically possible to create an administrator account that does not have a password. However, this is a dangerous practice and should be avoided.

The **Department Name** restricts this user's view of System Recordings and IVRs. The user will only be able to see System Recordings and IVRs that belong to the department that is defined in this field.

The **Extension Range** fields restrict the range of extensions that this administrator can manage. This is useful if extensions are specific to a department (for example, if the Sales department was using extensions 2150 through 2199, granting a Sales administrator access to alter only these extensions may be useful). Leaving these fields blank allows the administrator to access all extensions.

The **Admin Access** field allows the administrator to be restricted to specific dialogs. In order to select multiple rows in Windows or Linux, *Ctrl + Click* on each desired row and on Mac, *Command/Apple + Click*. Each dialog that the administrator should have access to should be selected in this field.

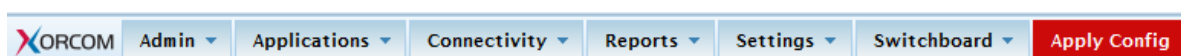


Apply Changes Bar

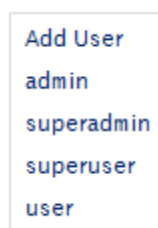
The **Apply Changes Bar** is treated as a separate access dialog, so it is possible to give an administrator access to change something without allowing them to apply those changes.

Note that **Apply Changes Bar** is a separate access dialog, so it is possible to give an administrator access to change something without giving them access to actually apply those changes.

Once all fields have been filled out appropriately click on the **Submit Changes** button followed by the red-colored **Apply Config** bar in order to make the new administrator active.



The administrator will show up in the menu on the right, and can be edited by clicking on their username:



Port Usage

Name	Port	Type	Description
SIP (PBX)	5060-5051	UDP/TCP	Ports used by CompletePBX for communicating with SIP devices that reside on the internal network. (Phones residing on external networks will communicate with CompleteSBC on port 6075.)
TFTP	69	TCP/UDP	Used for TFTP (Trivial File Transfer Protocol) configuration file loads. Remote VoIP telephones and devices that are automatically provisioned require this port to be open. Forwarding this port is required if automatic configuration is desired for re

Name	Port	Type	Description
IAX2	4569	UDP	Used for Asterisk to Asterisk IAX2 Trunking
RTP (PBX)	10000-20000	UDP	Used by CompletePBX to allow local IP phones to communicate with CompletePBX. If these ports are not open and forwarded, the phones will have one-way audio or no audio when making and receiving calls through the phone system
RTP (SBC)	20002-20402	UDP	Used by CompleteSBC to allow remote IP phones to communicate to CompleteSBC. If these ports are not open and forwarded, the remote phones will have one-way audio or no audio when making and receiving calls through the phone system
SSH	22	TCP	Used for SSH, a remote terminal configuration tool. Xorcom uses this port for remote diagnostics and custom configuration requests. Forwarding this port from the public internet to your IP PBX may be required for many support and configuration requests
HTTP	80	TCP	Used for remote administration via the GUI web interface
HTTPS	443	TCP	Used for remote administration via the GUI web interface if Secure HTTP is desired
FOP2	4445	TCP	Used for remote users who are using My Switchboard (Flash Operator Panel)
SIP (SBC)	6075	UDP	Used by external phones (or NAT) to communicate with CompleteSBC, and by the CompleteSBC to communicate with Asterisk server on the CompletePBX machine.

Summary

By now we are master of the CompletePBX realm. Your PBX should rival any of the competing closed-source solutions in terms of reliability, feature set, and security. Your system should now be locked down and secure, allowing minimal access from outside the network. Each administrator should have their own login, and should be restricted to just the dialogs that they need to change.

13. Managing the System

System Settings

About

The About dialog provides you with useful information about your CompletePBX system, including the Xorcom serial number of your hardware, and the version of CompletePBX that is currently installed.

Serial Number: X1069910

CPBX Version: 4.6.0

DHCP

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 CompletePBX as your DHCP server. If you want to use CompletePBX as your DHCP server, check on the **Enable** button.




Be careful!


You can only have one active DHCP server on your network.

Clicking on **Enable**, after clicking on **Apply**, will configure your CompletePBX machine as a DHCP server, using the settings defined in the fields below. You can configure DHCP settings even though the Disable button is active. This will allow you to preconfigure settings in preparation for enabling CompletePBX to act as a DHCP server at a later stage.

Settings

DHCP [?]	<input type="button" value="Enable"/> <input type="button" value="Disable"/>
Disabled Interfaces [?]	<input type="text"/> 
Start Address [?]	<input type="text" value="192.168.0.1"/>
End Address [?]	<input type="text" value="192.168.0.99"/>
Lease Time [?]	<input type="text" value="12"/> <input type="text" value="Hours"/> <input type="button" value="v"/>
Gateway [?]	<input type="text" value="192.168.0.100"/>
Primary DNS [?]	<input type="text" value="192.168.0.100"/>
Secondary DNS [?]	<input type="text"/>
NTP Server [?]	<input type="text" value="64.90.182.55"/>
Option 66 [?]	<input type="text" value="192.168.0.22"/>
Use for Endpoint Manager [?]	<input checked="" type="checkbox"/>
WINS [?]	<input type="text"/>

Static Leases[?]

MAC Address	IP Address	Hostname (optional)	
<input type="text" value="00:B0:D0:86:BB:F7"/>	<input type="text" value="192.168.0.101"/>	<input type="text" value="Coffee Machine"/>	
<input type="button" value="+ Add Lease"/>			
<input type="button" value="Apply"/>			

Disabled Interfaces enables you to disable DHCP on one, or more interfaces. If you want to disable multiple interfaces, create a list and separate each interface with a comma, i.e. eth0,eth2,eth3

Start Address is the first address on your network that can be allocated as a dynamic IP address.

End Address is the last address on your network that can be allocated as a dynamic IP address.

Lease Time is the period (in days, hours, minutes, or seconds) that the DHCP server grants an IP address to a device. The device must renew its IP address before the end of the period.

Gateway is the default IP gateway address.

Primary DNS – Domain Name System (DNS) translates Internet domain and host names to physical IP addresses.

Secondary DNS allows you to define a Secondary DNS to be used in case 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. You can define the IP address of the machine with which you

want to synchronize your CompletePBX server. A detailed list of available servers can be found on the Internet.

Option 66 - Trivial File Transfer Protocol (TFTP) is a technology for transferring files between network devices. The TFTP server can be used to maintain a local repository of configuration files for the SIP phones on your network. Option 66 provides IP phones with an URL for configuration provisioning. CompletePBX 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 on 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.

When **Use for Endpoint Manager** option is checked on, CompletePBX will automatically format the full 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.

You can use **Static Leases** to reserve dedicated IP addresses for specific devices. Each device will be identified by its MAC address, in a standard format, consisting of 6 groups of hexadecimal digits, separated by colons, i.e. 12:AA:34:4F:3D:00. You can use the **Hostname** field to name the device, to make it easier for you to identify the device.



Tip

You can configure DHCP settings in advance, without enabling the DHCP server, making it easier to prepare for a future change.

Email Settings

Server allows you the option to send outbound email messages either by using the built-in mail server (such as Postfix) that is active on the CompletePBX server, or by using a network-accessible relay server that is hosted on another machine. Click on **Use Built-in Mail Server** to use the built-in mail server that is active on CompletePBX, or **Use External Mail Server** to use a network-accessible relay server.

Email Settings

Server [?] Use Built-in Mail Server Use External Mail Server

Provider [?] Gmail Other

SMTP Server [?] Port [?]

TLS Enable Disable

Authentication [?] Use Authentication No Authentication

If you choose to use the built-in mail server, you will need to provide:

Server [?] Use Built-in Mail Server Use External Mail Server

Hostname [?]

Origin [?]

Domain [?]

Hostname which is the internet host name of the PBX. This should be the fully-qualified hostname, e.g. pbx.mycompany.com

Origin which specifies the origin domain for all mail posted by the PBX. By default, origin is configured to use your server hostname, e.g. pbx.mycompany.com

Domain specifies the parent domain of the hostname, e.g., mycompany.com if the hostname is pbx.mycompany.com

If you choose to use an external mail server, you will have two options: **Gmail**, or **Other**.

Email Settings

Server [?] Use Built-in Mail Server Use External Mail Server

Provider [?] Gmail Other

Username [?]

Password [?]

If you choose **Gmail**, you will need to enter the **Username** and **Password** that are associated with your Gmail account.

Other external mail servers need more detailed information.

Email Settings

Server [?] Use Built-in Mail Server Use External Mail Server

Provider [?] Gmail Other

SMTP Server [?] Port [?]

TLS Enable Disable

Authentication [?] Use Authentication No Authentication

Username [?]

Password [?]

You will need to define the location of the **SMTP Server**, which is the address that your email service provider has given you to enable you to send outgoing emails, the **Port** that your email service provider has told you to use for outbound email, and whether or not **TLS Authentication** should be activated (in accordance with the settings given to you by your email service provider).

If authentication is required, you will need to enter the **Username** that your email service provider has given you to allow you to access your email account. Typically, this would be something like

user@my-mail-server.com. You will also need to enter the **Password** associated with this email account.

**Note!**

Do not forget to press on **Apply** after making any changes.

Firewall

CompletePBX is preconfigured with a built-in firewall. You can choose to disable this built-in firewall by pressing **Disable**, followed by the **Apply** button.

















**Note!**

You should disable the built-in firewall only if your CompletePBX is behind some other (hardware or software) firewall.

Firewall Applications

If the firewall is enabled, you can define multiple Applications, on which you can base rules. CompletePBX is preconfigured with a number of standard applications. You may want to add additional applications that are specific to your installation. To add an application, click on the **Add Application** button at the bottom of the list of applications.

Applications

Name?	Ports?	Protocol?	
DNS 	53	Both ▼	
DRBD	7789	TCP ▼	
NTP	123	UDP ▼	
TFTP	69	UDP ▼	
DHCP	67:68	UDP ▼	
HTTP	80	TCP ▼	
SSH	22	TCP ▼	
SIP-PBX	5060,5061	Both ▼	
RTP-PBX	10000:20000	UDP ▼	
IAX2	4569	UDP ▼	
Asterisk-AMI	5038	TCP ▼	
Switchboard	4445	TCP ▼	
RTP-SBC	20002:20402	UDP ▼	
SIP-SBC	6075,6076	Both ▼	
HTTPS	443	TCP ▼	

[+ Add application](#)

Name - give the application a meaningful name to help you to easily recognize it. This name will be used to refer to the application in the Rules table

Ports – the IP ports that are used by the application. This can be defined as a single port (e.g. 80), a range of ports (e.g. 10000:20000), or a list of ports separated by commas (e.g. 80, 10000:20000, 5060)

Protocol determines the protocol that will be used by the application. Can be any one of TCP, UDP, or Both



Note!

Do not forget to press on **Apply** after making any modifications to the list of applications.

Firewall Rules

Rules⁹

	Action	Interface	Source		Destination		
			IP	Application	IP	Application	
	allow	any : in	any	any	any	TFTP	
	allow	any : in	any	any	any	NTP	
	allow	any : in	any	any	any	DNS	
	allow	any : in	any	any	any	DRBD	
	allow	any : in	any	any	any	HTTP	
	allow	any : in	any	any	any	HTTPS	
	allow	any : in	any	any	any	SSH	
	allow	any : in	any	any	any	IAX2	
	deny	any : in	any	any	any	Asterisk-AMI	
	allow	any : in	any	any	any	Switchboard	
	allow	any : in	any	any	any	DHCP	
	allow	any : in	any	any	any	SIP-SBC	
	allow	any : in	any	any	any	RTP-SBC	
	allow	any : in	10.0.0.0/8	any	any	SIP-PBX	
	allow	any : in	172.16.0.0/12	any	any	SIP-PBX	
	allow	any : in	192.168.0.0/16	any	any	SIP-PBX	
	allow	any : in	any	any	any	RTP-PBX	

Add Rule

Default Policy determines policy for inbound and outbound traffic, but can be overridden by a rule. Both Inbound and Outbound have three options:

Deny means that the packet is discarded, but no response is given to the originator of the request

Reject means that the packet is not allowed to pass, and a response is given to the originator of the request

Allow will pass all messages regardless of any rules that may be defined.

Firewall rules are checked in order from top to bottom. Once a match is made, no further rules will be checked. A rule can be moved up and down by clicking on the appropriate arrow at the left-hand end of each row. Rules can also be deleted, enabled, disabled, or modified by clicking on the appropriate icon at the right-hand end of each row.

Click on the **Add Rule** button at the bottom of the dialog to add rules. The following fields are available for each new rule:

Action configures whether this rule should Allow, Deny, or Reject access.

Allow will pass all messages regardless of any rules that may be defined.

Deny means that the packet is discarded, but no response is given to the originator of the request.

Reject means that the packet is not allowed to pass, and a response is given to the originator

of the request

Interface determines the interface to which the rule should be applied, e.g. eth0. If the rule should be applied to all interfaces then it must be defined as **any**. The current firewall version supports regular or VLAN interfaces, such as eth1.209; but does not support interface aliases, such as eth0:0

Direction indicates whether the rule should be applied to incoming, outgoing, or to both directions.

Source IP and **Application** is used if you want the rule to be restricted to messages that are sent from a specific IP address or subnet only. Use **any** to allow all IP addresses. If you want to restrict the rule to a specific IP address then you have to define the IP address with 32 as the subnet mask. If you use IPv6 then the subnet mask must be 128. In most cases you will define IP address as **any**.

You can also restrict the source port(s) and protocol by choosing an application from the list box.

IP 192.168.1.0/24 Application any would pass all messages from your subnet

IP any / [empty] Application HTTP would apply to messages from port 80 (using the predefined application HTTP) from any IP address

Destination IP and **Application** follow the same conventions as for **Source** above.






















Note!

Do not forget to press on **Apply** after making any modifications to the list of rules.

Configuring Firewall with CompleteSBC Disabled

















































If you choose not to enable CompleteSBC on your system, you will need to make some changes to your firewall configuration.

Firstly, you will need to decide which ports to use for SIP communication. If you decide to use ports other than the default ports of 5060/5061, you will need to navigate to Admin menu, select System Settings, select Applications, and modify the ports that are defined as SIP-PBX.

Name 	Ports 	Protocol 	
DNS 	53	Both ▾	
DRBD	7789	TCP ▾	
NTP	123	UDP ▾	
TFTP	69	UDP ▾	
DHCP	67:68	UDP ▾	
HTTP	80	TCP ▾	
SSH	22	TCP ▾	
SIP-PBX	5060,5061	Both ▾	
RTP-PBX	10000:20000	UDP ▾	
IAX2	4569	UDP ▾	
Asterisk-AMI	5038	TCP ▾	
Switchboard	4445	TCP ▾	
RTP-SBC	20002:20402	UDP ▾	
SIP-SBC	6075,6076	Both ▾	
HTTPS	443	TCP ▾	

Secondly, you will also need to navigate to Admin menu, select System Settings, select Rules, and modify the source IP address that are defined for the SIP-PBX application. When using CompleteSBC, only local network addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) are allowed access on the SIP ports.

Rules[®]Storage Info
Time Settings

	Action	Interface	Source		Destination		
			IP	Application	IP	Application	
^^	allow	any : in	any	any	any	TFTP	  
^^	allow	any : in	any	any	any	NTP	  
^^	allow	any : in	any	any	any	DNS	  
^^	allow	any : in	any	any	any	DRBD	  
^^	allow	any : in	any	any	any	HTTP	  
^^	allow	any : in	any	any	any	HTTPS	  
^^	allow	any : in	any	any	any	SSH	  
^^	allow	any : in	any	any	any	IAX2	  
^^	deny	any : in	any	any	any	Asterisk-AMI	  
^^	allow	any : in	any	any	any	Switchboard	  
^^	allow	any : in	any	any	any	DHCP	  
^^	allow	any : in	any	any	any	SIP-SBC	  
^^	allow	any : in	any	any	any	RTP-SBC	  
^^	allow	any : in	10.0.0.0/8	any	any	SIP-PBX	  
^^	allow	any : in	172.16.0.0/12	any	any	SIP-PBX	  
^^	allow	any : in	192.168.0.0/16	any	any	SIP-PBX	  

Firewall

When CompleteSBC is not enabled and you want to enable external SIP communication, you will need to open the SIP ports to allow access from any IP address.

Intrusion Prevention

Intrusion Detection configures the fail2ban application, which detects unauthorized attempts to access the system. 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).

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 CompletePBX itself in the whitelist, by adding 127.0.0.1 to the whitelist.

Intrusion Prevention

Status [?] **Enable** **Disable**

Settings

Ban an intruder for [?] minutes who tries to connect at least [?] times within [?] seconds and send an email to: [?]

Set whitelist [?]

```
127.0.0.1
192.168.0.178
```



Note!

Do not forget to press on **Apply** after making any modifications.

Any IP address that is 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 click on the Unban button to remove it from the list

Banned Hosts [?]

Host [?]	Jail Type [?]	
<input type="text" value="192.168.0.222"/>	<input type="text" value="asterisk-iptables"/>	Unban

Network Settings

The Network Settings dialog allows you to configure the network environment of the CompletePBX server.

Hostname can be used locally to access the system.

Gateway is a local node that provides access to and from the external network

DNS servers provide services to translate logical host names into IP addresses

**Note!**

DNS servers can only be defined for interfaces that use static IP addresses.



The Local DNS Settings section allows you to modify the system */etc/hosts* file, so that logical addresses (such as **localhost**) can be resolved without the need for a DNS server. This is important to ensure that the CompletePBX system will continue to work efficiently even when internet access is not available.

Network Settings

Hostname  Gateway

DNS servers 

Interface Settings

Interface	Type	IP	Mask	MAC Address	
eth0	dhcp			00:F1:F3:0E:10:E8	
eth1	dhcp				

[Add VLAN](#)

Local DNS Settings (/etc/hosts file)

IP Address	Hosts	
<input type="text" value="127.0.0.1"/>	<pre>localhost localhost.localdomain localhost4 localhost4.localdomain4</pre>	
<input "::1"="" type="text" value=""/>	<pre>localhost localhost.localdomain localhost6 localhost6.localdomain6</pre>	

[Add host](#)

Note!

Do not forget to press on **Apply** after making any modifications.

Applying the changes may take a minute or more while the system network services are reconfigured and restarted.

The Interface Settings section is initially populated with information about the devices that are physically available on the machine. In the Interface settings section, clicking on the edit icon (to the right of an existing interface will open a new dialog which will allow to you modify the configuration of an existing interface.

Interface is the name of the interface that is recognized by the operating system, such as eth0, eth1, etc.

Type provide a dropdown of two options:

Static indicates that the address for the interface is static.

DHCP indicates that the address for the interface should be obtained from a DHCP server.

If you select Static, you can enter the physical IP address and mask in the appropriate fields

MAC Address allows you to configure the MAC address that should be used by the interface.

When **On Boot** is checked on, the above settings will take affect only after the machine has been rebooted.

Interface

Interface	<input type="text" value="eth0"/>
Type	<input type="text" value="DHCP"/>
IP	<input type="text"/>
Mask	<input type="text"/>
MAC Address	<input type="text" value="00:F1:F3:0E:10:E8"/>
On Boot	<input checked="" type="checkbox"/>

Note!

Do not forget to press on **Apply** after making any modifications.

You can also click on the VLAN button to link VLANs to existing devices.

Interface is the name of an existing interface that is recognized by the operating system, such as

eth0, eth1, etc.

VLAN ID is a number that is used to identify the VLAN

Type provide a dropdown of two options:

Static indicates that the address for the interface is static.

DHCP indicates that the address for the interface should be obtained from a DHCP server.

If you select Static, you can enter the physical IP address and mask in the appropriate fields

MAC Address allows you to configure the MAC address that should be used by the interface.

When **On Boot** is checked on, the above settings will take affect only after the machine has been rebooted.

New VLAN

Interface	eth0 ▾
VLAN ID [?]	<input type="text"/>
Type	DHCP ▾
IP	<input type="text"/>
Mask	<input type="text"/>
On Boot [?]	<input checked="" type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	



Note!

Do not forget to press on **Apply** after making any modifications.

Notification Settings

This dialog allows you configure the address from which system alerts will be sent, as well as the recipients for each available alert. The recipient address can be defined by this dialog, or in the Storage Information/Intrusion Prevention dialogs. The recipient will be set to the last value that was entered, either in this dialog or in the relevant dialog.

Notification Settings

From Address	<input type="text" value="completepbx@xorcom.co"/>
Storage Notifications	<input type="text" value="bookman@xorcom.com"/>
Intrusion Notification	<input type="text" value="bookman@xorcom.com"/>



Note!

Do not forget to press on **Submit** after making any modifications.

Power Options

This dialog allows you to manage your system from the user interface. You can either completely shut down the system by clicking on **Power Off**, or click on **Reboot** to restart the system. After clicking on either of these buttons, you will be asked to confirm the chosen action.

Power Options

Power Off	<input type="button" value="Power Off"/>
Reboot	<input type="button" value="Reboot"/>

Storage Information

Storage Information provides you with information regarding storage devices that are available on your system. You can also use this dialog to send email alerts when any monitored device exceeds a predefined threshold.

Use the **Monitor** column in the **Drive Usage** section to check (or uncheck) a device: threshold alerts will only be sent for devices that have **Monitor** checked on.

Storage Information

RAID Status [?]

Disk	Status
A	Active Sync
B	Active Sync

Drive Usage

Drive	Size	Used	Available	Mounted On	% Used	Monitor [?]
/dev/md1	229G	1.7G	215G	/		<input type="checkbox"/>
/dev/md0	97M	33M	60M	/boot		<input type="checkbox"/>

Notification [?]

Threshold [?] %

Email [?]

Apply

In the Notification section you can define the threshold for email alerts, and the recipient for those alerts. When the usage on any monitored disk exceeds the threshold value, an email alert will be created.



Note!

Do not forget to press on **Apply** after making any modifications.

Time Settings

If the date of your system is not correct, you can manually repair it by clicking on the date that is currently displayed. This will provide you with an intuitive dialog which will allow you to choose the

correct date.

If the time of your system is not correct, you can manually repair it by entering the correct time in the **New Time** field, using the format hh:mm:ss

You can modify the **Timezone** of your system by selecting the correct timezone from the dropdown list.

Time Settings

Current Date: 13:26:27 11 June, 2014

New Date:

New Time:

Timezone:



Note!

Do not forget to press on **Apply** after making any changes.

14. Support

Xorcom Hardware Licenses

Access the CompletePBX server via SSH protocol and type the following command to see which USB devices are connected:

```
# lsusb
```

Your output should look similar to this:

```
Bus 003 Device 001: ID 0000:0000
Bus 004 Device 001: ID 0000:0000
Bus 005 Device 001: ID 0000:0000
Bus 001 Device 023: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 022: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 021: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 020: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 018: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 017: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 019: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 001: ID 0000:0000
Bus 001 Device 005: ID 05e3:0608 Genesys Logic, Inc. USB-2.0 4-Port HUB [Hama]
Bus 002 Device 001: ID 0000:0000
```

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----
```

```

-----BEGIN TELEPHONY DEVICE LICENSE BLOCK-----
Version: 1.0
Timestamp: 1357544664
Serial: X1055544
Capabilities.Port.FXS: 32
Capabilities.Port.FXO: 0
Capabilities.Port.BRI: 0
Capabilities.Port.PRI: 0
Capabilities.Port.ECHO: 0
Capabilities.Twinstar: 0
Data:
c0e4e460110102005831303535353434
2000000000000000d87cea508aa90f1d
3a333f773296258b02bbf520
-----END TELEPHONY DEVICE LICENSE BLOCK-----

```

Applying a New Xorcom Licence

Access the CompletePBX 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:

```

Bus 003 Device 001: ID 0000:0000
Bus 004 Device 001: ID 0000:0000
Bus 005 Device 001: ID 0000:0000
Bus 001 Device 023: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 022: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 021: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 020: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 018: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 017: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 019: ID e4e4:1162 Xorcom Ltd. Astribank 2 series
Bus 001 Device 001: ID 0000:0000
Bus 001 Device 005: ID 05e3:0608 Genesys Logic, Inc. USB-2.0 4-Port HUB [Hama]
Bus 002 Device 001: ID 0000:0000

```

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

Introduction to 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 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.

In CompletePBX, 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.

More information about echo in telephony systems can be found at: <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 be 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:

```
### Span 1: XBUS-00/XPD-00 "Xorcom XPD [usb:X1063616].2: FXS"
```

```
32 FXS          FXOKS          (In use) (no pcm) (EC: XPP - INACTIVE)
33 FXS          FXOKS          (In use) (no pcm) (EC: XPP - INACTIVE)
34 FXS          FXOKS          (In use) (no pcm) (EC: XPP - INACTIVE)
35 FXS          FXOKS          (no pcm) (EC: XPP - INACTIVE)
36 FXS          FXOKS          (In use) (no pcm) (EC: XPP - INACTIVE)
37 FXS          FXOKS          (no pcm) (EC: XPP - INACTIVE)
38 FXS          FXOKS          (no pcm) (EC: XPP - INACTIVE)
39 FXS          FXOKS          (no pcm) (EC: XPP - INACTIVE)
### Span 2: XBUS-00/XPD-20 "Xorcom XPD [usb:X1063616].3: FXS"
40 FXS          FXOKS          (no pcm) (EC: XPP - INACTIVE)
41 FXS          FXOKS          (In use) (no pcm) (EC: XPP - INACTIVE)
42 FXS          FXOKS          (In use) (no pcm) (EC: XPP - INACTIVE)
43 FXS          FXOKS          (no pcm) (EC: XPP - INACTIVE)
44 FXS          FXOKS          (no pcm) (EC: XPP - INACTIVE)
45 FXS          FXOKS          (no pcm) (EC: XPP - INACTIVE)
46 FXS          FXOKS          (In use) (no pcm) (EC: XPP - INACTIVE)
47 FXS FXOKS (In use) (no pcm) (EC: XPP - INACTIVE)
```

15. Applications

Burglar Alarms

Using the Atribank-8™ Input Ports to Broadcast

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 CompletePBX. These notes will demonstrate how to broadcast burglar alarm system voice messages to designated phone numbers by using one of the Atribank 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 Atribank-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 Atribank 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"



Warning

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 dialplan by creating a custom context:

```
[astbank-input]
; Using the default channel for this context
; The following line will call channel number 1
; And play the "alarm-message" sound file
exten => s,1,Dial(Zap/1 ,10,A(alarm-message))
; After channel 1 finishes, channel 2 will be called
exten => s,2,Dial(Zap/2 ,10,A(warning-message))
; You can add as many actions as you like using the following syntax:
exten => s,[sequence-number], [action]
```

- Update the dialplan using Asterisk Management Portal and check your setup by activating (short circuit) the relevant input port. CompletePBX will generate the calls as per your dialing plan and play the associated voice files.

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 CompletePBX. 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.

Dial in to the relay and listen to it: if your CompletePBX is configured to support extensions 401 to 408, dial extension 409 with your ear close to the Astribank. You'll hear a "click" from the CompletePBX unit. 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 (410, 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)

Warnings



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: dial to the relay (409 or 410 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:

```
; Define an extension you will call in order to activate the relay
; For this example, extension number => 456
; Goto virtual extension "ActivateRelay / valid-[CallerIdValue]" exten =>
456,1,Goto(ActivateRelay,valid-#{CALLERIDNUM},1)
; Define the context of the virtual extensions
[ActivateRelay]
```

```

; Define an extension for each legitimate CallerId
exten => valid-100,1,Noop
exten => valid-101,1,Noop
exten => valid-102,1,Noop
exten => valid-103,1,Noop
; The following items will execute for all legitimate Callers
; Open the relay using a dial command to the hardware
exten => _valid-.,2,Dial(ZAP/10/10/tr)
; Wait for 1 second exten => _valid-.,3,Wait(1)
; Play a confirmation message
exten => _valid-.,4,Playsound(goodbye)
; End the call
exten => _valid-.,5,Hangup()
; If the Caller ID is not recognized the caller will hear an error message
; and the call will terminate
exten => i,1,Playsound(invalid-callerId)
exten => i,2,Hangup()

```

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 Atribank 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.



Note

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	

RJ11 Connector/Pin	Description	Notes
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
```

Externally Controlling Follow Me

You can turn your follow me service on or off by calling into the phone system.

If your customer has a requirement to have different people "on call", and they don't want to use time conditions and time groups to manage it because they prefer to do it manually, this application note will help you.

The scenario is this: your client has a service that a customer will call in, usually after-hours, and when they call in the number should be forwarded to the on-call person. It is easy enough to point the number at a queue and that queue may have four or five extensions in it. Some of the extensions may have find-me follow-me activated to their cell phones. The trick is that not all extensions should be receiving the call at the same time. So the people who have the cell phones may want to call in and activate or deactivate their find-me follow-me service so the right person receives the call.

Here is the way to do it.

- If you already have an IVR set up with various options, one of the options should be to access your voicemail but this is not mentioned on the IVR announcement to callers. In the industry it is simply known as a, "hidden key". For example, you should be able to press 8 from the IVR as an option and it will direct you to a feature code option which would be *98, which will bring you to voicemail.
- Next, create an inbound route that is pointed at a queue which has the appropriate extensions in the queue. Obviously you could also point to a queue from an IVR.
- The extensions in the queue should all have find-me follow-me service activated with their cell phone numbers programmed in. I would highly recommend 60 seconds to search for the phone number and also enable "use confirmation".
- Login into the CompletePBX and go into the feature codes section of the PBX
- Change the default code for the find me follow me toggle from the default value of *21 to something like 9876

- Submit and apply your settings and you are done.

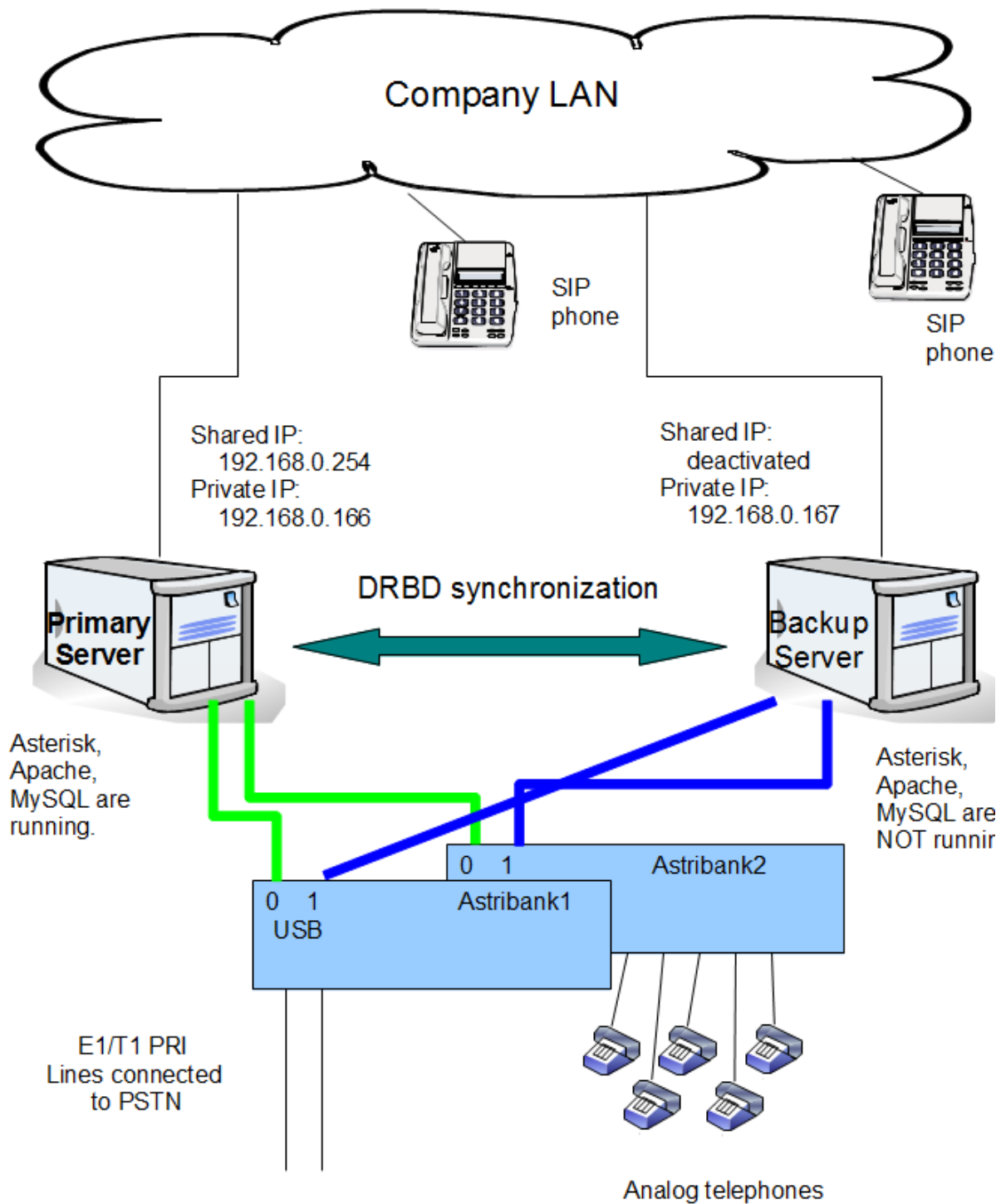
Now the user can dial the number that you have given him to access the voicemail system from outside the office. The process would work something like this.

- Dial the number for the PBX and press the appropriate key to access the voicemail system
- You will hear "welcome to the message center please enter your mailbox number"
- the user will enter the mailbox number followed by the #
- now they will hear, "welcome to the message center please enter your password"
- the user will enter their voicemail password followed by the #
- they can now press, 3 for advanced options, 4 to make an outgoing call
- they dial 999#
- then they will hear, "find me follow me activated" or "find me follow me deactivated" depending on the state it was in when they called
- the caller does not have to wait for the prompts to end. In other words, after they enter their extension number and voicemail password they can just press, 34999#, and then they will hear the find me follow me activation message.

16. TwinStar

An Example of an Asterisk High Availability Cluster

Two Asterisk servers can comprise an Asterisk cluster. One of the servers acts as the Primary server and the other server acts as the Secondary (hot-backup) server. Each server has its own private IP address. This allows server management and configuration replication to be performed between the two servers via the IP network. The VoIP PBX extensions communicate with the PBX cluster via a special public (or cluster) IP address, which is activated only on the current Primary server. When the servers swap roles, for example due to the Primary server failure, then that cluster IP address will be activated automatically on the Secondary server. As a result, the IP phones will continue to use the same PBX IP address.

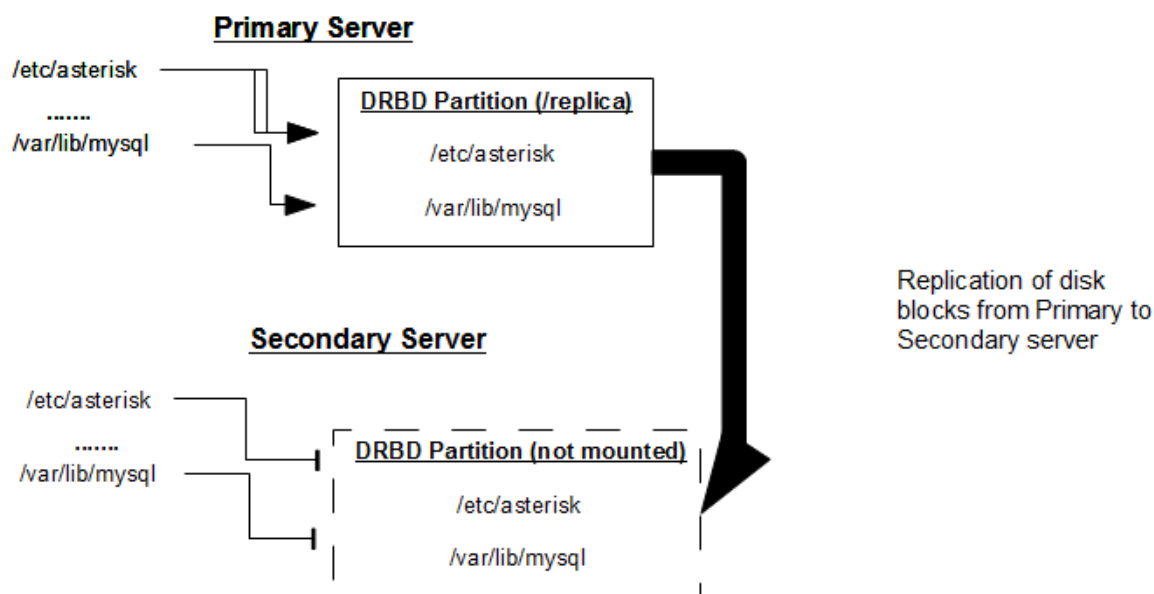


The replication of the servers' configuration files may be performed by using DRBD ("Distributed Replicated Block Device"). Visit the <http://www.drbd.org> Web site for further details. Nowadays, the DRBD is widely used for building many different high availability clusters. The DRBD concept assumes that there are special hard disk partitions that are replicated on the physical level via the IP network. Thus a changed hard disk block on the Primary server will be replicated to the Secondary server.

All files that need to be replicated must be allocated in the DRBD partition. For example, usually it is necessary to replicate the Asterisk configuration files, MySQL database files, etc. Therefore, folders such as /etc/asterisk and /var/lib/mysql must be allocated in a DRBD partition and soft links need to

be created instead of the regular file names. For example, the `/etc/asterisk` will be a link that points to `/replica/etc/asterisk`, where `/replica` is the default mount name of the DRBD partition.

Please note that the DRBD partition (`/replica`) is mounted on the Primary server only. On the Secondary server the DRBD partition is not mounted and therefore the `/etc/asterisk` files as well as other replicated files are not available. Services that depend on those files do not run (Asterisk, MySQL server etc). This ensures that the replicated files cannot be changed simultaneously on both servers.



In addition to the data replication function, a tool that detects the Primary server failure and forces the Secondary server to take over the cluster services is required. In many cases, High Availability (HA) software is used. Visit the <http://www.linux-ha.org/> Web site for further details. The HA uses its own IP watchdog protocol to detect the active server failure and activate one of the backup servers. Astribank TwinStar technology allows the implementation of similar cluster management tools.

Each Astribank device has two USB interfaces (0 and 1). Once powered up, the Astribank will always use the USB interface 0, which should be connected to the Primary server. After all of the services have started it is possible to activate the TwinStar watch dog mechanism that monitors (a) voltage availability on the USB port and (b) continuity of communication between the Astribank device and the Astribank DAHDI driver.

When at least one of the conditions is not met, the Astribank will deactivate the USB interface 0 and automatically activate the USB interface 1. As a result, the Secondary server receives a plug-and-play event that a new USB device is connected to the server. The plug-and-play system calls special scripts that check that all of the configured Astribank devices have switched to the Secondary server. After that, a special script is called and the following occurs:

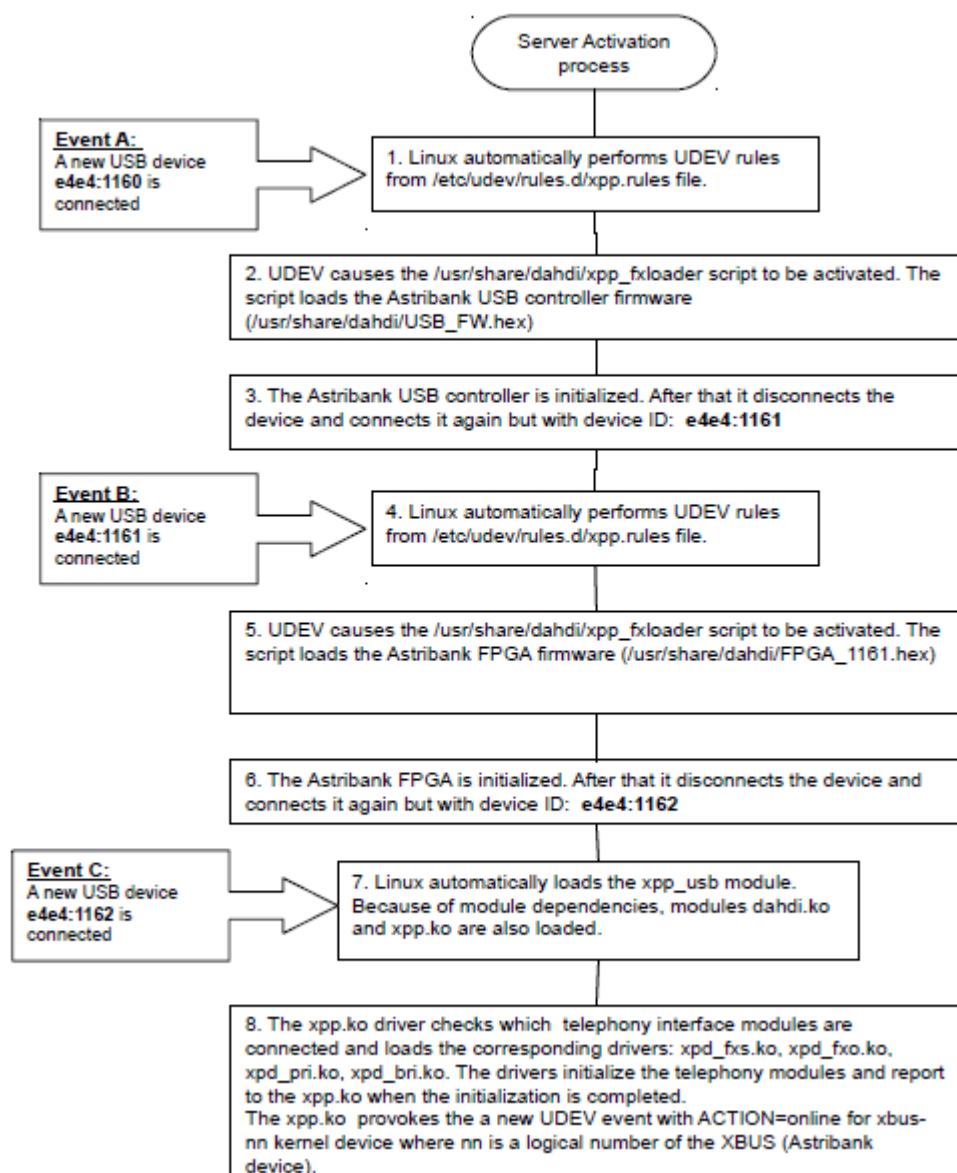
- The script registers the Astribank channels on DAHDI and configures them.
- The script mounts the DRBD partition (`/replica`). As a result, the `/etc/asterisk`, `/var/lib/mysql` etc. folders become available.
- The shared IP is activated.
- MySQL, Asterisk, and Apache services are started.

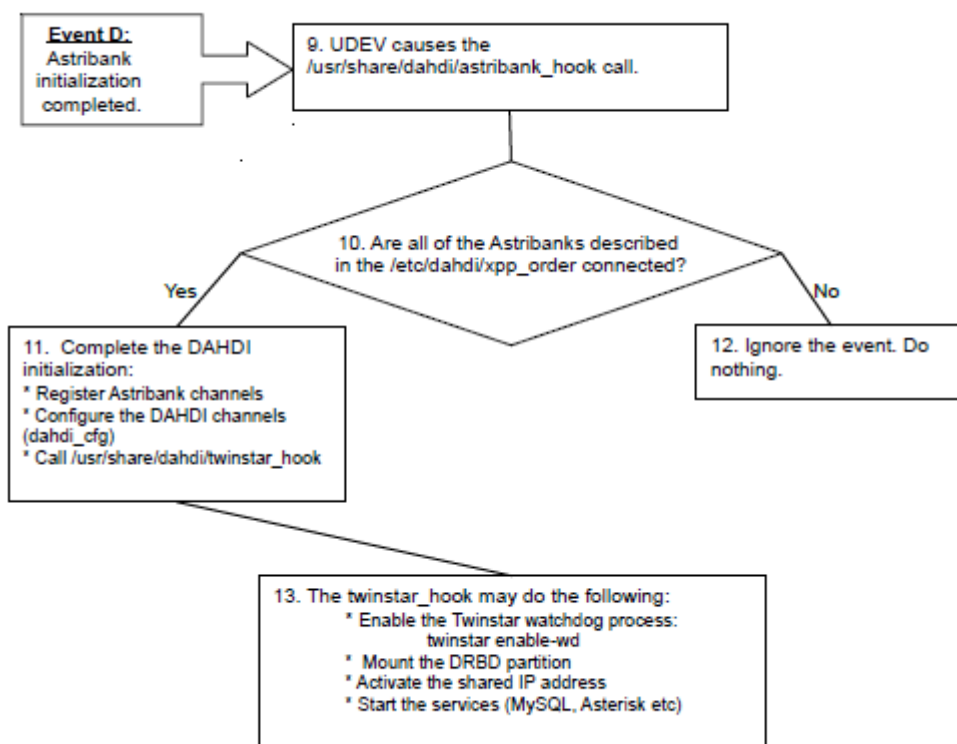
TwinStar Implementation Details

The Astribank device is plug-and-play by nature. When an Astribank device is discovered by the Linux plug-and-play system and, based on the predefined UDEV rules (`/etc/udev/rules.d/xpp`), the `/usr/share/daohdi/xpp_fxloader` script is called. This utility is responsible for loading the Astribank firmware. Once the firmware has been loaded Linux loads the Astribank drivers that initialize the device.

After that, a special UDEV event is generated and as a result, the `/usr/share/daohdi/astribank_hook` script is called. The `astribank_hook` may check if all of the required Astribank devices have been activated. In order to do so, the script inspects the `/etc/daohdi/xpp_order` file which contains a sorted list of configured Astribank devices. The script also checks the `/sys` file system for existence and status of connected Astribanks.

If all of the devices listed in the `xpp_order` file are active, then the `astribank_hook` may complete the DAHDI start-up procedure and start all of the necessary services. For example, to mount the DRBD partition, activate the shared IP, start Asterisk, etc. Those services actually may be started from a separate `twinstar_hook` script that is called by the `astribank_hook`. The flow chart below provides a detailed explanation of the process.





As you can see, the proposed solution assumes that the services such as Asterisk, MySQL, Apache, etc. -- which are usually started automatically during the Linux start-up--must be started only on the Primary server and only when DAHDI has been successfully started (when all of the Atribanks are active) and their configuration files are available (the DRBD partition is mounted

Events that are Monitored

As was mentioned above, the Atribank TwinStar monitors the voltage of the active USB port and controls the regularity of the watchdog messages exchanged between the device and the Atribank driver. Therefore, the Atribank will switch over to the second USB interface when one of the following happens:

- the server is switched off
- the Atribank driver stopped working, for any reason. For example, the Linux kernel crashed,
- the driver was unloaded, etc.
- the USB cable is disconnected

Switching of the servers can be made conditional upon other events as well. For example, another server monitoring system like Monit (<http://mmonit.com/monit>),

Runit (<http://smarden.sunsite.dk/runit>) or even the Linux Heart Beat (<http://www.linux-ha.org>) can be installed and configured in such a way that Atribank switching will take place when the monitoring system discovers a problem.

Controlling the TwinStar Status

You can use the 'twinstar' utility that is located in the /usr/sbin folder.

Check Status:

```
#twinstar status
```

DEVICE	PORT	WATCHDOG	POWER0	POWER1
usb:001/006	0	on	yes	yes
usb:001/007	0	on	yes	yes

Enforce Switching to Another USB Interface:

```
twinstar jump
```

Start USB Voltage Monitoring and Exchange of Watchdog Messages:

```
twinstar enable-wd
```

Stop USB Voltage Monitoring and Exchange of Watchdog Messages:

```
twinstar disable-wd
```

The watchdog should be disabled before stopping the DAHDI for maintenance purposes.

TwinStar Installation

Please note that some TwinStar-related utilities and scripts are not installed by default during regular DAHDI installation procedure and need to be installed manually

**Note**

Xorcom does not provide technical support for DRBD or any server monitoring software/hardware packages. Xorcom provides pre-configured DRBD/TwinStar-ready XR2000/XR3000 Asterisk appliances in its product offering.

17. Feature Codes

Admin → Feature Codes

With all dialogs installed, CompletePBX has more than 45 feature codes that users can dial to toggle features or run applications. Feature codes can be customized from the **Feature Code Admin** page (they can be located by clicking on the **Feature Codes** option under the **Basic** menu in the CompletePBX interface). The default feature codes and their actions are listed as follows:

Blacklist

Feature Code	Default	Action
Blacklist a number	*30	Prompts the user to enter a telephone number. The entered number is then added to the user's blacklist. Inbound calls will not ring an extension if they are on that extension's blacklist. Blacklisted callers will be told that the number they dialed is no longer in service.
Blacklist the last caller	*32	Adds the last number that called the user to the blacklist.
Remove a number from the blacklist	*31	Prompts the user to enter a telephone number. The entered number is removed from the user's blacklist.

Call Forwarding

Feature Code	Default	Action
Call Forward All Activate	*72	Prompts the user to enter a phone number or extension number. Any calls to the user's extension will be forwarded to the entered number until call forwarding is deactivated.
Call Forward All Deactivate	*73	Deactivates call forwarding on the extension of the user placing the call.
Call Forward All Prompting Deactivate	*74	Prompts the user to enter an extension number. Call forwarding will then be disabled on the entered extension. This feature code enables a user to remove call forwarding on their extension from another extension on the system, or from any phone if the users have DISA access.

Feature Code	Default	Action
Call Forward Busy Activate	*90	Prompts the user to enter a phone number or extension number. If the user is on the phone from that point onward, inbound calls will be forwarded to the entered number. If the user is not on the phone when an inbound call comes in, the user's extension will ring as normal.
Call Forward Busy Deactivate	*91	Disables call forward on busy service, on the extension of the user placing the call.
Call Forward Busy Prompting Deactivate	*92	Prompts the user to enter an extension number. Call forward on busy service will then be disabled on the entered extension. This feature code enables a user to remove call forward on busy service from their extension using another extension on the system, or from any phone if the users have DISA access.
Call Forward No Answer/Unavailable Activate	*52	Prompts the user to enter a telephone number or extension number. If the user does not answer an inbound call or the user's telephone is not registered with CompletePBX, inbound calls to the user will be forwarded to the entered number. If the user is on the phone when an inbound call comes in, the call will be processed normally (either by initiating call waiting or by failing over to another destination).
Call Forward No Answer/Unavailable Deactivate	*53	Disables call forward on no answer or unavailable service on the extension of the user placing the call.

Call Waiting

Feature Code	Default	Action
Call Waiting Activate	*70	Enables call waiting service on the extension of the user placing the call. If an inbound call comes into an extension that is already on the line and call waiting is enabled, then the user receiving the call will hear a beep and may see the caller ID of the new caller (depending on their telephone). The user receiving the call can then place their current call on hold and pick up the new caller. Without call waiting, the new caller would either receive a busy signal or would immediately be dropped to voicemail without the extension ringing.
Call Waiting Deactivate	*71	Deactivates call waiting on the extension of the user placing the call.

Core

Feature Code	Default	Action
General Call Pickup	*8	Allows the user to pick up a call that is ringing another phone as long as the user's pickup group matches the ringing extension's call group. For example, if extension 5000 is in call group 1 and extension 5001 is in pickup group 1, the user at extension 5001 can pick up a call that is ringing extension 5000 by dialing *8. If the user's pickup group does not match the call group of the ringing phone, dialing this feature code will have no effect.
ChanSpy	555	Allows the user to listen to an active call. After initiating the ChanSpy application, the user can dial the *key to cycle through all active channels. (User must be granted permission to use this feature).
Dial System FAX	666	Dials the extension that is defined as the default fax extension. The default fax extension is set on the General Settings page by changing the extension of the fax machine for the receiving faxes drop-down menu.
Directed Call Pickup	** (ext)	Allows the user to pick up a call directed to another extension. The (ext) token should be replaced with the extension being picked up. For example, if extension 2001 is ringing, another user could dial **2001 to pick up the call.
In-call Attended Transfer	*2	When on a call, a user can dial this feature code to initiate an attended transfer. The user will hear a dial tone and at this point, they can enter an extension or telephone number. The users will be connected with the number they dialed. When the user hangs up the phone, the person they are transferring will be connected with the person the user called. Attended transfers are used when the person transferring the call wishes to speak to the person receiving the call before the call is transferred. A common scenario for this would be a call center agent transferring a call to their manager. The agent needs to first brief the manager on the problem before the call is transferred.
In-call Blind Transfer	##	When on a call, a user can dial this feature code to initiate a blind transfer. The user will hear a dial tone and at this point, they can enter an extension or telephone number. The person the user was speaking with will be immediately transferred to the number the user entered.

Feature Code	Default	Action
In-Call Toggle Call Recording	*1	When on a call, a user can dial this feature code to start the recording of the call using the CompletePBX MixMonitor application. This feature code works if the user's Recording Options are set to On Demand on their configuration page in the CompletePBX interface. Recorded calls are saved to the <i>/var/spool/asterisk/monitor</i> directory by default.
Simulate Incoming Call	7777	Simulates an inbound call to the PBX. The call will be matched against any inbound route rules in the same way as an incoming call through a trunk would be matched.
User Logon	*11	If CompletePBX is configured in the DeviceAndUser mode, this feature code will allow a user to log in to a telephone with their extension and password. Once a user is logged in, any calls to the user's extension will ring the phone the user logged into.
User Logoff	*12	If CompletePBX is configured in DeviceAndUser mode, this feature code will allow a user to log out of a phone they are currently logged into. If a user is not logged in to any device when a call comes into their extension, the call will immediately proceed to the user's failover destination (this is normally voicemail, but it can be other extensions or telephone numbers if follow-me is configured).
ZapBarge	888	Prompts the user for a channel number. The user will then be able to listen and talk to an active call on the DAHDI channel, which they entered.

Dictation

Feature Code	Default	Action
Perform Dictation	*34	Prompts the user to enter a numeric filename followed by the pound (#) key. The user is then connected to the dictation application where whatever they say will be recorded. The dictation application allows recording to be paused at will, and can be switched to playback mode to hear the current recording.
Email completed dictation	*35	Prompts the user to enter a numeric filename followed by the pound (#) key. If a dictation recording with that filename exists, it will be emailed to the email address specified in the user's dictation options in the CompletePBX interface.

Do-Not-Disturb (DND)

Feature Code	Default	Action
DND Activate	*78	Activates the Do-Not-Disturb (DND) mode for the extension placing the call. Any calls directed to an extension with DND enabled will not ring any of the phones associated with that extension. Calls to an extension that has DND enabled will immediately continue to the extension's failover destination (this is usually voicemail, but could be other extensions or phone numbers if follow me is enabled).
DND Deactivate	*79	Deactivates the Do-Not-Disturb (DND) mode for the extension placing the call.
DND Toggle	*76	Toggles the state of Do-Not-Disturb (DND) mode for the extension placing the call.

Follow Me

Feature Code	Default	Action
Findme Follow Toggle	*21	Toggles follow-me mode on the extension placing the call. Any calls to an extension with follow me enabled will follow the call flow defined in the extension's Follow Me configuration page in the CompletePBX interface. If follow me is disabled, calls to the extension will ring any associated phones as normal, and fail over to voicemail (if enabled) or eventually disconnect the call (if voicemail is not enabled).

Info Services

Feature Code	Default	Action
Call Trace	*69	Plays back the telephone number or extension number of the last caller to the phone dialing the feature code.
Directory	#	Connects the user to the company directory. The directory is populated with all users who have voicemail boxes. The directory can be searched by first name and last name (this is a configurable option on the CompletePBX General Settings page). When a user finds the person they are looking for, they can opt to be transferred to that person.

Feature Code	Default	Action
Echo Test	*43	Plays back whatever the user is saying as they are saying it. The echo test is designed to provide a sense of the latency between the telephone dialing the feature code and the CompletePBX server.
Speak Your Extension Number	*65	Plays back the extension number of the extension placing the call.
Speaking Clock	*60	Plays back the current time on the CompletePBX server.

Paging and Intercom

Feature Code	Default	Action
Intercom Prefix	*80 (ext)	Connects the user to another extension via intercom functionality (the called phone does not ring, but immediately answers the call and places the call on speaker phone). The (ext) token should be replaced with the extension that the user is trying to connect to. For example, to start an intercom session with extension 5001, dial *805001. The extension being called must have intercom functionality enabled, and the phone must support auto-answer via SIP info headers. Most SIP phones provide this support.
User Intercom Allow	*54	Enables intercom functionality on the extension placing the call. Any user can initiate an intercom session with an extension that has this functionality enabled.
User Intercom Disallow	*55	Disables intercom functionality on the extension placing the call. If intercom functionality is disabled on an extension, any user who tries to initiate an intercom session with that extension will hear a message indicating that all circuits are busy, and hence the session will not be established.

Phonebook Directory

Feature Code	Default	Action
Phonebook dial-by-name directory	411	Works in conjunction with the CompletePBX Phonebook dialog. The user is prompted to enter three letters on their touch tone phone to make a search in the phonebook. When the desired entry is found, the user is given the option to press 1 to dial the phone number associated with the matching entry.

Recordings

Feature Code	Default	Action
Save Recording	*77	Plays a single beep after which whatever the user says is recorded to a temporary file on the PBX. This is used in conjunction with the CompletePBX System Recordings dialog. The CompletePBX interface is used to name the temporary recording and transfer it to a more permanent location.
Check Recording	*99	Plays back the most recent temporary recording that was made by the user placing the call. It is used to verify that a recording sounds the way it was meant to. If the user is not satisfied with the recording, they can dial the Save Recording feature code again to re-record it.

Speed Dial

Feature Code	Default	Action
Set user speed dial	*75	Allows the user to configure a speed dial entry. The user is prompted for a speed dial location followed by the pound (#) key. The speed dial location can be any number. The user is then prompted for the telephone number or extension number, which they wish to add to speed dial followed by the pound (#) key. For example, to add the phone number 555-555-1234 to the speed dial location 1000, dial *75, wait for the prompt, then dial 1000# and wait for the prompt, and now dial 5555551234#.
Speeddial prefix	*0 (num)	The (num) token should be replaced by the speed dial location being dialed. Dialing this feature code connects the user with the speed dial phone number associated with the speed dial location they entered. For example, to dial the telephone associated with speed dial location 1000, dial *01000.

Voicemail

Feature Code	Default	Action
Dial Voicemail	*98	Prompts the user to enter a voicemail box number and the password associated with that mailbox. If the user is authenticated successfully, they are transferred to the messaging center where they can listen to their voicemails and record their outgoing voicemail messages.

Feature Code	Default	Action
My Voicemail	*97	Assumes the user is calling to check messages in the voicemail box associated with the extension they are calling from. It prompts the user for a password. If the user is authenticated successfully, they are transferred to the messaging center where they can listen to their voicemails and record their outgoing voicemail messages.

18. Menu Overview

CompletePBX includes more than 50 modules that are periodically updated from the online repository. A listing of all of the available modules and their functions as of the time of writing is as follows:

Menu	Dialog	Function
Admin	Administrators	Defines administrators who can manage CompletePBX. Each administrator has a unique password, and has permission to access selected menus.
	Backup & Restore	Provides the administrator with the ability to set up one-time or recurring backups of CompletePBX configuration data, recordings, and voicemails, as well as to restore those backups. These backups are taken while the system is running, so they do not backup the operating system. You must use Rapid Recovery if you need to make an image backup including the operating system.
	Blacklist	Creates a list of numbers that are not allowed to call into the system. Callers that are listed in the blacklist will hear a prompt informing them that the number they called is not in service.
	CallerID Lookup Sources	Lets you specify a source for resolving numeric CallerIDs of incoming calls, allowing you to link a CID source to a specific Inbound Route. This will provide you with a more detailed CDR report, with information taken directly from your CRM. You can also install the phonebook module to have a small number-to-name association. Note that name lookup may slow down your system.
	Custom Destinations	Custom Destinations allow you to register destinations that point to custom dialplans and 'publish' these destinations as available destinations to other dialogs. This is an advanced feature and should only be used by knowledgeable users.
	Custom Extensions	Custom Extensions provide you with a facility to register any extension or feature code that you have created in a custom file that CompletePBX would not otherwise know about them.
	DUNDi Lookup	

Menu	Dialog	Function
	Feature Codes	Provides the ability to enable/disable feature codes, or change the numbers that are dialed to access certain feature codes. Feature codes are numbers (just like extensions) that can be dialed by users to access PBX features, such as call forwarding activation, voicemail, and call waiting activation.
	Module Admin	Allows you to run an online check to verify that all modules are up-to-date, and to apply any available updates. Also allows you to enable/disable individual modules.
	Phone Restart	Allows you to select and restart registered SIP phones.
	System Recordings	Allows users to record, upload, and merge audio recordings. Recordings can be used in IVRs and as confirmation clips for ring groups.

Menu	Dialog	Function
	System Settings	<p>Manages additional system settings, including:</p> <ul style="list-style-type: none"> • About – provides information about the current version of CompletePBX as well as the serial number of the hardware. • DHCP – configure CompletePBX as a DHCP server • Email Settings – configure email server to used by CompletePBX for outbound email messages, to enable delivery of voicemail to email, fax to email, alerts, etc. • Firewall – activate the built-in firewall, define applications, create rules to manage the applications, and manage order of the rules. • Intrusion Prevention – configure fail2ban to detect potential intruders, and to block access. • Network Settings – configure the network settings for each interface of CompletePBX, including gateway, DNS servers, VLANs, and configuration of /etc/hosts file. • Notification Settings – manage destination for email alerts • Power Options – to reboot or power down the system. • Storage Options – provides a visual display of status of storage devices, and to configure alert thresholds when disks are running out of space • Time Settings – configures current date, time, and timezone settings.
	System Speed Dialing	<p>Works in conjunction with the Phonebook Directory dialog.</p> <p>Entries in the phonebook can be assigned short speed dial codes that users can dial. CompletePBX will then dial the associated full number of the phonebook entry and connect the call with the dialing user.</p>
Applications	Announcements	Defines how to make use of system recordings
	Call Flow Control	<p>Defines user-activated controls that can be inserted into your call flow.</p> <p>Each Call Flow Control is automatically allocated a dedicated feature code, which can be used to toggle the control.</p>

Menu	Dialog	Function
	Call Recording	<p>Call Recording provides the ability to force a call to be recorded or not recorded based on the call flow, and override all other recording settings.</p> <p>If a call is to be recorded, it can start immediately (which will incorporate any announcements, hold music, etc.) prior to being answered, or it can start recording at the time that call is answered.</p>
	Callback	<p>Allows a trigger to be configured that calls back a specific number and provides the callee with access to a module or application.</p> <p>The callback number can be predefined, or can be the number that triggered the callback.</p> <p>Typically used to provide a user's cell phone with a dial tone on the CompletePBX system, giving them access to long distance calling that is cheaper than dialing directly from their cell phone.</p>
	Conferences	<p>Provides the ability to set up conference rooms in which two or more users can join together in a single call.</p> <p>Conference rooms can be password protected.</p>
	DISA	<p>Provides Direct Inward System Access (DISA) as a call target.</p> <p>This will give the caller a dial tone on the system allowing them to dial any of the features of the system, or initiate an outbound call through the trunks of the system.</p>
	Directory	<p>Allows you to create phone directories.</p> <p>Allows a caller to select a destination when the directory is inserted into an IVR.</p>
	Endpoint Manager	<p>Provides ability to centrally manage and update IP phones</p>
	IVR	<p>Provides digital receptionist functionality.</p> <p>The IVR module answers a call, plays back a sound clip, and waits for the caller to push digits on their phone in order to route the call.</p>

Menu	Dialog	Function
	Languages	Allows you to change the language of the call flow before continuing on to the desired destination. For example, you may have an IVR option that says "For French Press 5 now". You would then create a French language instance and point it's destination to a French IVR. The language used will now be in French. This will result in French sounds being chosen if installed.
	Misc Applications	Allows an administrator to configure arbitrary feature codes that direct the caller to a specific call target.
	Misc Destinations	Allows an administrator to configure call targets that dial any local number (such as an extension, feature code, or external phone number). These destinations can then be set up as the target for inbound routes or as the failover destination for other call targets.
	Music on Hold	Provides the ability to upload custom sound files or define streaming audio sources that will be played to callers while they are on hold.
	PIN Sets	Allows an administrator to define a set of identification codes that can be used to grant access to outbound routes or conferences.
	Paging & Intercom	Allows an administrator to define paging groups. When a paging group is called, all the phones in the group will automatically answer the call and play the caller's audio through their speakers. It also allows the creation of an intercom feature code that allows paging functionality to be directed to one phone specifically.
	Queue Priorities	Provides the ability to give a particular caller higher priority when entering a queue. Callers with higher priority will be placed at the front of the queue and have their calls answered faster.
	Queues	Allows callers to be routed in a call queue where they wait on hold until someone is available to answer their call. Callers are placed into the queue in the order they called in (unless their call order is altered by a queue priority).

Menu	Dialog	Function
	Ring Groups	Creates a call target that will ring a predefined set of extensions. Extensions can either be rung all at the same time or in various hunt sequences that ring one extension at a time.
	Set CallerID	Allows you to change the Caller ID for a call and then continue to the desired destination. For example, you may want to change the caller id form "John Doe" to "Sales: John Doe".
	Time Conditions	Provides the ability to route calls to call targets, depending on the day of the week, month, date, or time.
	Time Groups	Allows you to define periods, or groups of periods, that can be used in a Time Condition.
	Voicemail Blasting	Allows an administrator to create a group of extensions that can be "blasted" with a single voicemail message. When this functionality is invoked the caller records a message that is delivered to the voicemail box of all of the extensions that are members of the blast group.
	Wake Up Calls	Allows the creation of wakeup calls by an authorized administrator
Connectivity	Bulk DIDs	Allows administrator to download all DIDs to a CSV file, edit the file, and load the file back into the system. Useful for making bulk changes to multiple DIDs.
	Bulk Extensions	Allows you to download extension definitions to a CSV file, edit the file, and load the file back into the system. Useful for making bulk changes to many extensions.
	DAHDI Chanel DIDs	Allows you to assign a DID to specific DAHDI channel. You can supply the same DID to multiple channels. This would be a common scenario if you have multiple POTS lines that are on a hunt group from your provider.
	Extensions	Define SIP, IAX2, DAHDI, or Virtual extensions.

Menu	Dialog	Function
	Follow Me	Provides the ability to create a personalized 'ring group' for each user on the system. A set of phone numbers is configured to ring when the user's extension is rung, and a fail over destination is specified.
	Inbound Routes	Define inbound routes, and link them to the required destination, such as extension, queue, conference, etc.
	Outbound Routes	Configure pattern matching to enable routing of outbound calls.
	Routing Groups	Allows creation of groups of outbound routes to be used by extensions
	Trunks	Link outbound routes to external trunk lines.
Reports	CDR Reports - Advanced	Advanced CDR reporting.
	CDR Reports - Basic	Basic CDR reporting.
	Extension Settings	Provides a printable list of all of the configured extensions, conferences, queues, and feature codes.
	PBX Log	Allows an administrator to view the CompletePBX log files through the CompletePBX Web interface.

Menu	Dialog	Function
	PBX Status	<p>Provides the following information from CompletePBX:</p> <ul style="list-style-type: none"> • Summary • Active SIP and IAX2 channels • Number of SIP and IAX2 registrations • Number of online and offline SIP and IAX2 peers • Registries • Active SIP and IAX2 registrations (including registration host, username, refresh interval, and registration state) • Channels • Active channel summary • Active number of SIP and IAX2 channels • Peers • Shows all of the defined SIP and IAX2 extensions/peers • SIP Info • Specific SIP registry and peer information • IAX Info • Specific IAX2 registry and peer information • Conferences • Shows details on conferences that are currently active • Subscriptions • Shows registered dial plan hints • Voicemail users • Shows a list of users that have a voicemail box and the number of waiting messages for those users • Full report • Shows a full listing of all of the information contained within the other information sections
	Phone Book	<p>Provides an audio phonebook that users can search through from their telephones. The phonebook is populated from the CompletePBX Web interface.</p> <p>Users can search by name and are given the associated phone number when their search matches an entry.</p>

Menu	Dialog	Function
	System Status	The landing page that is shown whenever logging into the CompletePBX Administration. The landing page includes the following pieces of information: <ul style="list-style-type: none"> • CompletePBX Notices • CompletePBX Statistics • System Statistics
	Weak Passwords	Creates a report of any user accounts, extensions, or trunks that have weak registration passwords. Accounts with weak passwords represent a security hole and should be updated as soon as possible.
Settings	Advanced	Provides access to many global configuration parameters, without the need to open the command line interface.
	Asterisk Managers	Creates an asterisk manager, including password, allowable networks, and access rights.
	Congestion Messages	Defines messages or tone when congestion is encountered for standard, intra-company, and emergency routes as well as for trunk failures.
	Fax Configuration	Defines outbound fax options, including storage and cover page.
	IAX Settings	Provides access to global IAX configuration parameters, without the need to open the command line interface.
	PBX Settings	
	PBX Log Settings	Manage the log files that are used by Asterisk. This dialog can determine the rotation policy to be used, as well as determine which logfiles should be created.
	Parking Lot	Allows calls to be "parked". When a call is parked, the person parking the call is given a parking space number. Anyone who dials that parking space number will be connected with the parked caller.
	SIP Settings	Provides access to global IAX configuration parameters, without the need to open the command line interface.

Menu	Dialog	Function
	Voicemail	Provides access to global voicemail configuration parameters, without the need to open the command line interface. Also provides information about voicemail usage, and allows administrator to determine timezone to be used for voicemail timestamps.
Switchboard	Buttons	Manages buttons that will be displayed in My Switchboard.
	Groups	Manages groups of buttons for use in My Switchboard.
	Permissions	Manages permissions granted to My Switchboard users.
	Templates	Manages templates of permissions for use in My Switchboard.
	Users	Manages users who can access My Switchboard.

19. Appendix

Voicemail.conf Options

When setting up an extension (Extensions mode) or a user (DeviceAndUser mode), CompletePBX provides a field called **VM Options** under the **Voicemail & Directory** group of options. This field allows any option to be entered that could be included as a mailbox option in */etc/asterisk/voicemail.conf*. These options affect the behavior of a mailbox and the way the voicemail messages are received and processed. Options should be listed using the syntax *optionname=value* (where *optionname* is replaced with the name of the option being configured, and *value* is replaced with a valid value for that option). Multiple options can be specified by placing a pipe character (|) between each option (for example,

attach=yes|attachfmt=gsm).

Option	Valid values	Purpose
attach	yes, no	<p>If voicemail to email notifications are enabled, the attach option allows a copy of the voicemail to be attached to the email notification. If this option is not configured, the default value of "no" will be used.</p> <p>Note that this option can be configured within the CompletePBX interface using the Email Attachment field and should not be manually configured. Manually configuring this option could result in conflicting configurations and unpredictable result.</p>
attachfmt	gsm, wav, wav49	<p>Specifies the format that the sound file attached to the notification email should be in. GSM files are raw GSM encoded, WAV files are 16-bit linear WAV encoded, and WAV49 files are GSM encoded WAV format files. Windows PCs can play back WAV files by default, and most stock Linux desktop PCs should be able to play back GSM files. Any operating system should be able to play any of these formats, but additional software may be required. If this option is not configured, the default value of "wav" will be used.</p>

Option	Valid values	Purpose
callback	(Any valid context)	<p>The CompletePBX voicemail applications provide the ability for a user to call back the telephone number or extension number of the person who left them a voicemail. The callback option configures the context that CompletePBX will use for placing the outbound call. By default, users created under CompletePBX use the from-internal context to place their calls, and this option can be safely set to this value.</p> <p>The only time this option typically differs from the context that the user normally utilizes is when a user's outbound calling ability is restricted. If a user can typically call local telephone numbers, but not long distance, they would be unable to return a voicemail from anyone who is not within the local calling area. It is prudent for a company to allow callbacks to someone who has left a message. A company may choose to create a special context specifically for the purpose of voicemail callbacks in which calls to long distance numbers are allowed. In this case, the callback option would be set to the name of the custom context that allows long distance calling.</p> <p>If this option is not configured, no default value will be used and the callback feature of the voicemail application will be disabled.</p>
delete	yes, no	<p>If voicemail to email notifications are enabled, the delete option provides the ability to delete voicemail messages from the CompletePBX server as soon as the notification email is sent. This option is intended to be used by users who wish to receive their voicemails through email only. If this option is not configured, the default value of "no" will be used by CompletePBX.</p> <p>Note that this option can be configured within the CompletePBX interface using the Delete Voicemail field and should not be manually configured. Manually configuring this option could result in conflicting configurations and unpredictable result.</p>
envelope	yes, no	<p>If set to "yes", the user will hear the date and time a message was left prior to the message being played when they check their messages.</p>

Option	Valid values	Purpose
forcegreetings	yes, no	If set to "yes", new users will be prompted to record their busy and unavailable outgoing messages the first time they log into their mailbox. The voicemail application determines that a user is new if their voicemail password is the same as their extension. If this option is not configured, the default value of "no" will be used.
forcename	yes, no	If set to "yes", new users will be prompted to record their name the first time they log into their mailbox. The voicemail application determines that a user is new if their voicemail password is the same as their extension. If this option is not configured, the default value of "no" will be used.
hidefromdir	yes, no	If set to "yes", the user will be hidden from the company directory. If this option is not configured, the default value of "no" will be used.
imapuser/imappassword	(IMAP account credentials)	The voicemail application allows voicemail messages to be stored on an IMAP server. Storing messages on an IMAP server allows voicemail to be managed either through a phone or an email client. Changes made using one management method are reflected in the other. For IMAP storage to work, the file <i>/etc/asterisk/vm_general.inc</i> must be edited in order to include a line that reads <code>imapserver=servername</code> (where <code>servername</code> is replaced with the actual hostname of the IMAP server being used). Once the <code>imapserver</code> configuration option is defined in the <i>vm_general.inc</i> file, the <code>imapuser</code> and <code>imappassword</code> options must be configured to use valid user account credentials for the IMAP server. If these options are not configured, there are no default values used, and IMAP voicemail storage will not be used.
maxmsg	(whole number)	Defines the maximum number of messages that the user can have in each one of their voicemail folders. If this option is not configured, then there is no default value used and no limit will be placed on the amount of voicemail messages a user can store.

Option	Valid values	Purpose
operator	yes, no	If set to "yes", the person leaving the message is able to press 0 to return to the call target they came from before dialing an extension. For example, if a caller is directed to an IVR and then dials a user's extension and receives voicemail, they can press 0 to return to the IVR. If the caller did not come from a previous call target (they were routed directly to the user's extension), pressing 0 will route their call to the extension defined in the Operator Extension field on the CompletePBX General Settings page. If this option is not configured, the default value of "no" will be used.
review	yes, no	If set to "yes", the person leaving the message is able to press the pound (#) key after leaving their message in order to review the message they just recorded. They are given the option to re-record their message if they choose to. If this option is not configured, the default value of "no" will be used.
sayid	yes, no	<p>If set to "yes", the user will hear the caller ID number of the person who left the voicemail prior to the voicemail being played when they check their messages. If this option is not configured, the default value of "no" will be used.</p> <p>Note that this option can be configured within the CompletePBX interface using the Play CID field and should not be manually configured. Manually configuring this option could result in conflicting configurations and unpredictable results.</p>
sayduration	yes, no	If set to "yes", the user will hear the duration of the voicemail message prior to the voicemail being played when they check their messages. If this option is not configured, the default value of "no" will be used.

Option	Valid values	Purpose
saydurationm	(Minimum time, in whole number of minutes)	This option restricts when the voicemail application will say the duration of a message. If this value is set, then the voicemail application will only announce the duration of a message if the message is longer than the value of saydurationm. For example, if this option is set to "2", the application will only announce the duration of messages that are longer than two minutes. This option only takes effect when the sayduration option is set to "yes". If this option is not configured, no default value will be used and all message durations will be announced when the sayduration option is set to "yes".
sendvoicemail	yes, no	If set to "yes", the user is able to forward a voicemail message they have received to another user. Otherwise, this functionality is disabled. If this option is not configured, the default value of "no" will be used.
serveremail	(Email address)	This option sets the email address from which voicemail to email notification messages appear to come. For example, this might be voicemail@example.com.
tempgreetwarn	yes, no	If set to "yes" and the user has a temporary greeting enabled, they will be notified that the greeting is enabled each time they check their voicemail messages. If this option is not configured, the default value of "no" will be used.
tz	(Valid timezone)	<p>This option specifies which time zone a user is in, so that the envelope time data is played in the user's local time instead of the server's local time. This option must be a valid time zone. In order to find the valid time zones on the CompletePBX server, check the contents of the /usr/share/zoneinfo folder.</p> <p>The files in this folder are valid time zones; the subfolders contain country-specific time zones. If this option is not configured, the default time zone will be the local time zone of the CompletePBX server.</p>

Option	Valid values	Purpose
volgain	Positive or negative numbers, rounded to one decimal place)	Specifies the gain that should be used when recording messages for the user. If messages are generally too quiet, the value should be higher (for example, 1.5). If messages are too loud, the number should be lower (for example, -2.1). If this option is not configured, the default value of "0" will be used and no gain will be applied to voicemail messages.