EasyVOIZ 5

User Manual

Contents

Contents

1. Introduction

EasyVOIZ 5 is based on a highly responsive graphic user-interface that facilitates the management of Asterisk servers, in a fast, intuitive, and secure manner.

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

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

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

laptops with a low-resolution screen, mobile devices and tablets, you will need to press on the help balloon to access the help text.

11. In some dialogs, after pressing Save or Update, you will notice the Reload icon at the top right corner of the dialog. This indicates that your update has been stored in the database, but you will need to press on the Reload icon to make the running system aware of the update.
12. Mandatory fields are indicated by an asterisk following the field name, e.g. **Name*** indicates that the Name field is mandatory.

New Concepts in EasyVOIZ 5

Class of Service

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

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

Each Class of Service comprises three groups of functionality:

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

Extensions and Devices

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

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

Host Desking

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

A Hot Desking device can be associated with an extension by dialing the hot desking feature code (*80), the extension number, and the extension password. To remove the association, you only need to key in the hot desking feature code (*80) to remove the association.

Technology Settings

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

Telephony

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

Software Maintenance

Fixed issues and improvements for the product are published on a regular basis. You can review these updates by visiting https://D-Link.com/category/EasyVOIZ-change-log/ on our website.

These updates can easily be added to your system by logging into the Linux command line interface, and running the command:

```
yum update
```

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

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

```
yum history
```

```
[root@guest99 ~]# yum history
Loaded plugins: fastestmirror
ID     | Command line             | Date and time    | Action(s)      | Altered
-------------------------------------------------------------------------------
    66 | update                   | 2017-06-05 09:12 | Update         |   10 ##
    65 | remove kernel-3.10.0-514 | 2017-06-05 09:11 | Erase          |    1
    64 | update                   | 2017-05-29 08:41 | E, I, U        |   39 EE
    63 | update                   | 2017-05-01 09:20 | Update         |    9 EE
    62 | remove kernel-3.10.0-514 | 2017-05-01 09:20 | Erase          |    1
    61 | update                   | 2017-04-24 09:26 | Update         |   14
    60 | update                   | 2017-04-19 08:29 | E, I, U        |   37 EE
    59 | update                   | 2017-04-12 11:40 | Update         |   11 EE
    58 | update                   | 2017-04-03 08:31 | Update         |    4
    57 | remove kernel kernel-3.1 | 2017-03-27 09:27 | Erase          |    1
    56 | remove kernel kernel-3.1 | 2017-03-27 09:26 | Erase          |    1
    55 | remove kernel kernel-3.1 | 2017-03-27 09:26 | Erase          |    1
    54 | remove kernel kernel-3.1 | 2017-03-27 09:25 | Erase          |    1
    53 | update                   | 2017-03-27 09:23 | Update         |   10 EE
    52 | update                   | 2017-03-21 09:09 | Update         |   12 EE
    51 | update                   | 2017-03-07 09:50 | E, I, U        |   32
    50 | update                   | 2017-02-27 08:03 | E, I, U        |   13
    49 | update                   | 2017-02-21 09:00 | Update         |   17 EE
    48 | update                   | 2017-02-14 09:39 | Update         |    2
    47 | install cpbx-upgrade     | 2017-01-31 10:35 | Install        |    1 EE
```

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

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

```
[root@guest99 ~]# yum history info 47
Loaded plugins: fastestmirror
Transaction ID : 47
Begin time     : Tue Jan 31 10:35:34 2017
Begin rpmdb    : 537:e1cc121ce37796dd0eda06876b194e09f824717f
End time       :                            (0 seconds)
End rpmdb      : 538:52318f7972c7fc9d2f5c504b71367975c02495a4
User           : root <root>
Return-Code    : Success
Command Line   : install cpbx-upgrade
Transaction performed with:
    Installed     rpm-4.11.3-21.el7.x86_64                        @base
    Installed     yum-3.4.3-150.el7.centos.noarch                 @base
    Installed     yum-plugin-fastestmirror-1.1.31-40.el7.noarch @base
Packages Altered:
    Install cpbx-upgrade-5.0.13-1.noarch @cpbx-5
Scriptlet output:
   1 SUCCESS. CompletePBX has been upgraded to v.5.0.13.
history info
```

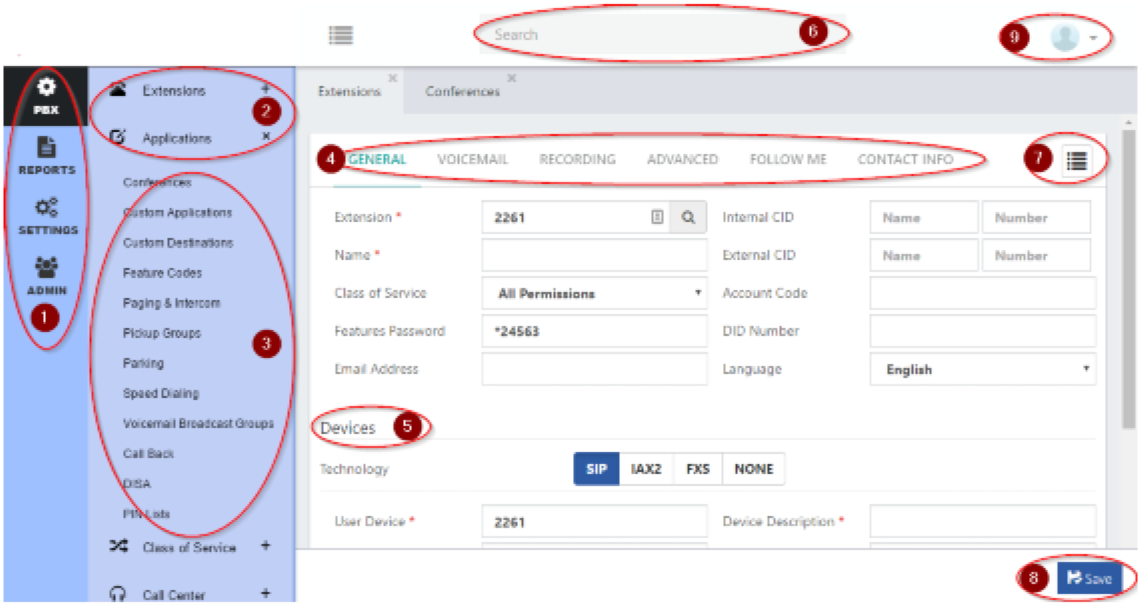
Changes and updates to the PBX system are documented in the system database, so you can review the updates by running the command:

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

```
[root@guest99 ~]# mysql ombutel -e "select * from ombu_patches"
+----------+-----------------------------------------------------+---------------------+
| patch_id | filename                                            | applied             |
+----------+-----------------------------------------------------+---------------------+
|        1 | 20160208.1.init.sql                                 | 2016-05-17 15:25:25 |
|        2 | 20160208.2.cdr.sql                                  | 2016-05-17 15:25:25 |
|        3 | 20160208.3.tables.sql                               | 2016-05-17 15:25:27 |
|        4 | 20160208.4.data.sql                                 | 2016-05-17 15:25:27 |
|        5 | 20160208.5.epm.tables.sql                           | 2016-05-17 15:25:27 |
|        6 | 20160208.6.epm.data.sql                             | 2016-05-17 15:25:31 |
|        7 | 20160209.1.queues.members_settings.sql              | 2016-05-17 15:25:32 |
|        8 | 20160210.1.destinations.table.sql                   | 2016-05-17 15:25:32 |
|        9 | 20160210.2.destinations.data.sql                    | 2016-05-17 15:25:32 |
|       10 | 20160210.ntp.sql                                    | 2016-05-17 15:25:32 |
```

Documentation Conventions

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



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

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

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

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

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

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

The User Menu ❾ at the top of the screen shows information about the current user. It can also be used to login and logout of the system, to change the language in which the user interface will be displayed, and to see the version of EasyVOIZ that is currently installed.

The following languages are currently available:

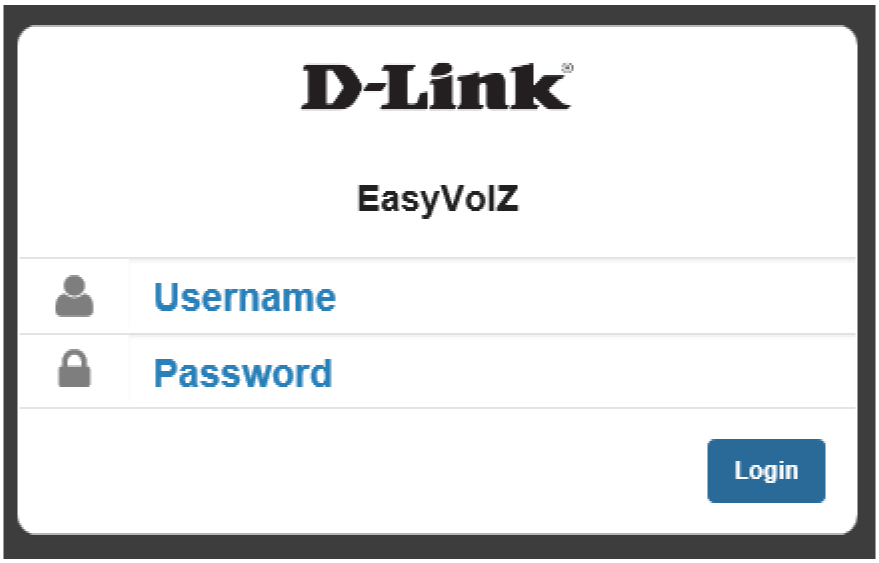
- English (en_US)
- Spanish (es_ES)
- French (fr_FR)
- Dutch (nl_NL)
- Chinese (zh_CN)

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

Accessing the User Interface

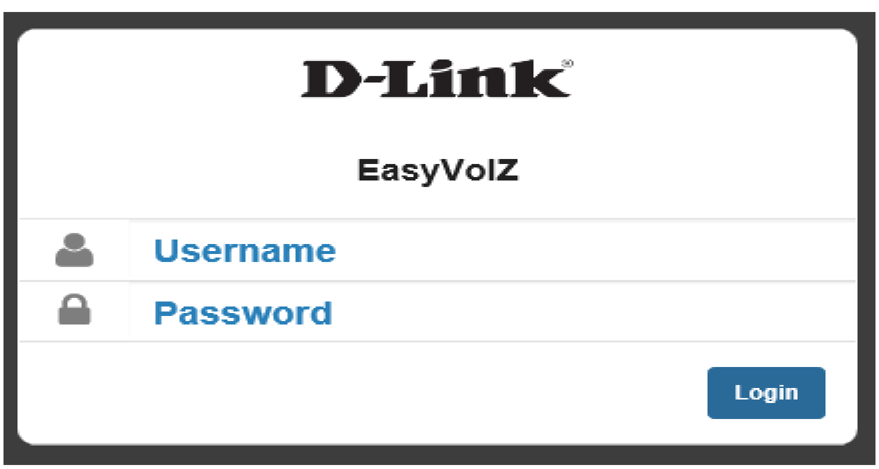
Administrator Interface

Use any internet browser to access the user interface, by entering the IP address of the server, followed by the appropriate password.



User Portal

Use any internet browser to access the Portal, by entering the IP address of the server. Enter your extension number in the Username field, and your Portal password, that has been defined in the system for your extension, in the Password field.

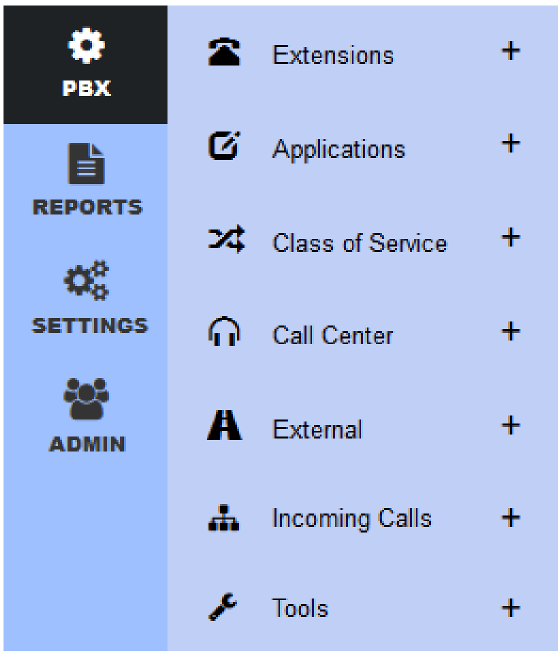


Note that you cannot simultaneously access both the User Interface and the User Portal using the same Internet browser window. If you want to access both the User Interface and the User Portal, you will need to either open another browser session, or use a different browser.

Overview of the Menu Layout

Administrator's Menu Layout

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



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

- **Extensions** menu group
  - Extensions, management of extensions and devices
  - Hot Desking, device management
  - Import Extensions, import extensions from CSV format
  - Export Extensions, export extensions into CSV format
  - Bulk Modification, bulk extension modification
  - Extension Status, status of extensions, with possibility to changing the state
- **Applications** menu group
  - Conferences, conference room management
  - Custom Applications, custom application management
  - Custom Destinations, custom destination management
  - Feature Codes, management of telephone feature codes
  - Paging & Intercom, paging & intercom management

  - **Pickup Groups**, management of pickup groups
  - **Parking**, parking management
  - **Speed Dialing**, speed dial management
  - **Import/Export Speed Dialing**,
  - **Voicemail Broadcast Group**, voicemail broadcast group management
  - **Call Back**, management of call back functionality
  - **DISA**, Direct Inward System Access (DISA) management
  - **PIN Lists**, group of pins that will be used to access outgoing routes

- **Class of Service** menu group
  - **Class of Service**, group of settings that define the dial plan which each extension can access
  - **Feature Categories**, group of feature groups that are associated with a Class of Service
  - **Dialing Restriction Rules**, dial-up restrictions that are associated with a Class of Service
  - **Customer Codes**, customer codes that can be dynamically associated to a call in order to categorize the call in the CDR
  - **Authorization Codes**, code that authorizes privileges to make a call
  - **Route Selections**, Automatic Route selection management

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

- **External** menu group
  - **Trunks**, SIP, IAX, and DAHDI trunk management
  - **Outbound Routes**, management prefixes for outgoing routes
  - **Inbound Routes**, DID management for incoming routes

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

- **Tools** menu group
  - **Asterisk CLI**, Asterisk command line management interface
  - **Blacklist**, black list management number
  - **Dashboard**, see system status in real time
  - **Log Files Viewer**, displays the contents of log files

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

- **CDR Reports** menu group

- **CDR Filters**, management of filters to apply in reports
- **CDR**, display call records (CDR)

- **PBX Reports menu group**
  - **Status**, display current status of Channels, Registrations, Peers, Hints, Voicemail, and Queues

Settings menu set, where you can find everything about the parameters of different technologies (such as SIP and IAX), voice mail settings, the PBX overall event files, configuration of analog and digital interfaces (DAHDi), auto-provisioning of phones (End Point Manager).

- **Technology Settings** menu group
  - **SIP Settings**, general SIP settings management
  - **IAX2 Settings**, general IAX2 settings management
  - **Profiles**, profile management
  - **Technology Settings**, configure default timezone for users and peers
  - **Dial Profiles**, configures Asterisk dial options to be associated with extensions
- **Voicemail Settings** menu group
  - **Voicemail Settings**, general voice mail settings management
  - **Voicemail Timezones**, time zone management for voicemail
- **PBX Settings** menu group
  - **System General**, general system settings such as directories, dial-plan settings, etc
  - **Asterisk Manager Users**, to create users of Asterisk Manager
  - **Music on Hold**, to create and upload music on hold
  - **Recordings Management**, to upload recordings
  - **Log Files**, determine format and content of log files related to Asterisk
  - **Fax Settings**, determine format of the coversheet used by outbound faxes
- **Telephony** menu group
  - **Interfaces** detects and configures new analog and digital interfaces
  - **Clock Sources**,
  - **Channel Groups**, grouping external telephony interfaces such as E1, FXO, etc
  - **Profile Assignments**,
- **End Point Manager** menu group
  - **Host Settings**, creates networks for devices search
  - **Create Template**, create templates for different devices
  - **Device Mapping**, search for devices connected to the network and configure
- **Switchboard** menu group
  - **Switchboard Manager**, allows you to configure Users, Buttons, Groups, Templates, Permissions, Plugins, and Settings for the Switchboard,

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

- **Admin** menu group
  - **Users**, management of system users
  - **User Profiles**, management of user profile
  - **Application Access**, manage access to specific applications and modules
  - **Backup & Restore**, to backup and restore telephony configuration.

- **System Settings** menu group
  - System Misc, management of system notifications and date and time settings
  - **Network Settings**, network management
  - **Email Settings**, email server configuration
  - **DHCP Settings**, DHCP server configuration
- **Security** menu group
  - **Firewall**, firewall management system
  - **Intrusion Detection**, management of fail2ban utility, which detects and block external attacks
  - **Weak Passwords**, weak password detection
- **Licenses** menu group
  - **Register Digium Products**, Digium license registration: DPMA and G729 codecs
- **TwinStar menu group**
  - **TwinStar Status**, shows the status of the TwinStar cluster

Portal Menu Layout

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

- **Configure** menu group
  - **My Extension**, enables the extension owner to manage his extension
  - **My Voicemail**, enables the extension owner to manage his voicemail settings
  - **My Time Group**, enables the extension owner to manage his time groups
  - **CDR**, enables the extension owner to view his CDR records
  - **Fax Settings**, enables the extension owner to manage his outgoing fax settings
  - **My Faxes**, enables the extension owner to view his incoming and outgoing faxes
- **Operator** menu group
  - **Switchboard**, enables the extension owner to view the Switchboard and manage call handling

Configuration Considerations

Security

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

Servers with only the most basic SSH configuration are most vulnerable to brute force attacks. Most attackers try to gain root access via SSH, so you should pay close attention to things such as disabling external SSH root logins completely, or the use of SSH key pairs for authentication, etc.

Change SSH listening port

SSH normally listens for connections on port 22 or port 443. Attackers use port scanner software to see whether hosts are running the SSH service. It's wise to change the SSH port to a number higher than 1024 because most port scanners (including nmap) by default don't scan high ports.

Open the /etc/ssh/sshd_config file and look for the line that says:

```
Port 22
```

Change the port number and restart the SSH service:

```
/etc/init.d/ssh restart
```

If you change the port for the SSH service, you will also need to update the settings of the built-in firewall. Open the PBX system user interface, go to the Admin>Security>Firewall dialog, and change the port for the SSH service in the Rules tab.

Allow only SSH protocol 2

There are two versions of the SSH protocol. Using SSH protocol 2 only is much more secure; SSH protocol 1 is subject to security issues including man-in-the-middle and insertion attacks. Edit /etc/ssh/sshd_config and look for the line that says:

```
Protocol 2,1
```

Change the line so it allows only protocol 2.

Allow only specific users to log in via SSH

You should not permit root logins via SSH, because this is a big and unnecessary security risk. If an attacker gains root login for your system, he can do more damage than if he gains normal user login. Configure SSH server so that root user is not allowed to log in. Find the line that says:

```
PermitRootLogin yes
```

Change yes to no and restart the service. You can then log in with any other defined user and switch to user root if you want to become a superuser.

You can create a dummy local user with absolutely no rights on the system and use that user to login into SSH. That way no harm can be done if the user account is compromised. When creating this user, make sure it's in the wheel group, so that you can switch to superuser. You can add a user by using the following command:

```
Useradd new_user_name
```

You can set a password for the new user with the passwd command, i.e.

```
Passwd new_user_name
```

To add a user to the wheel group, edit /etc/group, and modify the entry for wheel to look something like this:

```
Usermod –aG wheel new_user_name
```

You may also need to modify the /etc/sudoers file to grant sudo access to users belonging to the wheel group:

```
%wheel  ALL=(ALL)       ALL
```

If you would like to have a list of users who are the only ones able to log in via SSH, you can specify them in the sshd_config file. For example, let's say I want to allow users anze, dasa, and kimy to log in via SSH. At the end of sshd_config file I would add a line like this:

```
AllowUsers anze dasa kimy new_user_name
```

SIP/IAX2 extensions configuration.

- Define long and complicated passwords for SIP and IAX2 extensions that consist of digits as well as upper- and low-case letters. The minimum password length should be at least 8 characters.
- Define IP address filters for the local extensions. For example, if you know that extension 2201 will be assigned to a SIP phone that is installed in your local office, then you can define the following IP filter for this extension:

```
deny: 0.0.0.0/0.0.0.0
permit: 192.168.1.0/255.255.255.0
```

or

```
deny: 0.0.0.0/0
permit: 192.168.1.0/24
```

Global SIP configuration

- Disable inbound calls from unknown sources. Navigate to Settings>Technology Settings>SIP Settings. Go to the Security tab and make sure that the Allow Guest parameter is set to No.
- Make sure that Asterisk will reject invalid SIP requests with the same reject reason code, regardless of the real reason. This significantly hampers brute-force attackers as they receive no indication whether the extension exists, and makes it much more difficult to guess the SIP user name and secret. Navigate to Settings>Technology Settings>SIP Settings. Go to the Security tab and make sure that the Always Reject parameter is set to Yes.
- Disable requests for domains that should not serviced by the PBX system. Navigate to Settings>Technology Settings>SIP Settings. Go to the Custom tab, and define the following parameters in the Custom Options section:

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

  If the system can receive SIP calls, then it is possible that valid SIP requests will be made for the domain matches the external IP address or host name. In this case it is necessary to define this address in the 'domain' parameter. For example, if the external IP address is 1.2.3.4 and the DNS name is mycompany.com then you can define:

```
domain=1.2.3.4
domain=mycompany.com
```

Tips for improving security of external SIP extensions

- Instead of the default port (5060), use a non-default port for SIP traffic for external connections. This means that external extensions will use different (non-default) port, and your NAT router will do the translation for the incoming calls.
- If the IP address of the external SIP device is known, you can restrict the IP address of the SIP extension, by restricting the Permit field in the Devices section of the Extensions dialog. You can still use this method even if you don’t know the exact IP address of the the SIP extension, you can define an IP block, such as 203.195.84.0/24
- Use a different device name, rather than just the extension number.
- Use strong (long and complicated) passwords, including a mixture of characters (upper and lower-case), numbers, and special characters.
- You can create a special Class of Service for external SIP extensions.
- Reduce the call limit for external SIP extensions.
- Review the “Asterisk Security Threats and Best Practices” presentation located at https://files.D-Link.com/mktgdocs/presentations/protect-asterisk-pbx-webinar.pdf

Dial Plan configuration

- Do not configure uncontrolled trunk-to-trunk calls. For example, do not define context 'from-internal' for a trunk.
- DISA and Call-back must be well protected by strong passwords.

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

Change passwords

You should change any default passwords in your system that are factory-configured:

- Change MySQL, Web interface and Asterisk Management Interface passwords. You will be prompted for the new password values.
- Change the password for Linux 'root' user. You can use the following command in the Linux shell:

```
passwd
```

- You can use a Linux command, like the following example, to create strong passwords:

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

Fail2ban

Ensure that fail2ban is properly configured and running. This can be managed from the Admin > Security > Intrusion Detection dialog.

You can also use the Dashboard to verify that the fail2ban service is running.

IP protection

The PBX must be installed on a protected LAN and must not be directly connected to the public Internet. The LAN must be protected by a Firewall/NAT router. The PBX built-in firewall could be optionally used as an additional protection mean.

- Do not expose SIP (5060/udp) and IAX2 (4569/udp) ports if you don't have remote extensions.
- Use non-standard port for SSH. Thus, instead of exposing port 22/tcp define port forwarding from a not well-known port (e.g., 4223/tcp) on the external interface to port 22/tcp of the PBX.
- Enable the SSH connection from specific IP addresses only. For example, you could configure only to allow the IP address of the company that provides technical support for your PBX.
- Optionally, it is possible to disable the password authentication method in the PBX SSH server configuration and use only the private/public key authentication. Refer to your SSH client documentation for further details of the private/public key configuration.
- Do not expose either HTTP (80/tcp) or HTTPS (443/tcp) ports at all. Use SSH tunneling for access to the PBX Web interface.
- For additional protection, enable the built-in firewall.

Numbering

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

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

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

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

Dependencies

Destinations

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	Destination is Mandatory	Destination is Optional
Announcement		✓	
Authorization Codes			
Blacklist			
Call Back	✓	✓	
Class of Service		✓	
Conferences	✓		
Custom Application	✓	✓	
Custom Destination			
Customer Codes			
Dialing Restriction Rules			
DISA	✓		
Extensions	✓		✓ (Extensions only)
Extension Status			✓
Feature Categories			
Feature Codes			
Hot Desking		✓ (Devices only)	
Inbound Routes		✓	

Dialog	**Is a Destination**	**Destination is Mandatory**	**Destination is Optional**
IVR	✓	✓	
Languages	✓	✓	
Night Mode	✓	✓	
Outbound Routes			
Parking	✓	✓	
Paging & Intercom	✓	✓ (Extensions only)	
Pickup Groups	✓	✓	
PIN Lists			
Queue Priorities	✓	✓	
Queue VIP			
Queues	✓	✓	
Ring Groups	✓	✓	
Route Selections			
Speed Dialing	✓		
Terminate Call	✓		
Time Conditions	✓	✓	
Time Groups			
Trunks			
Voicemail			
Voicemail Broadcast Group	✓	✓ (Extensions only)	

Mandatory Fields and Dialog Dependencies

This table shows the dependencies between dialogs to help you optimize the flow when setting up the system, as well as highlighting which fields are mandatory. The **Need to Know** column highlights information that you may need in order to complete the definition of the object. Items that are shown in bold font in the **Need to Know** column are not optional.

Dialog	Prerequisite Dialogs	Mandatory Fields	Need to Know
Announcement	Destination	Description Custom Recording Destination	
Authorization Codes		Code Alias Description Class of Service	
Blacklist		CID Number Description	
Call Back	Destination	Description Destination	
Class of Service	Destination	Class of Service Name Last Destination Bad Destination	Feature Category Dial Restrictions Route Selection
Conferences		Extension Description	
Custom Application	Destination	Code Destination	
Custom Destination	Class of Service	Description Number to Dial Class of Service	
Customer Codes		Customer Code Description	
Dialing Restriction Rules		Description	

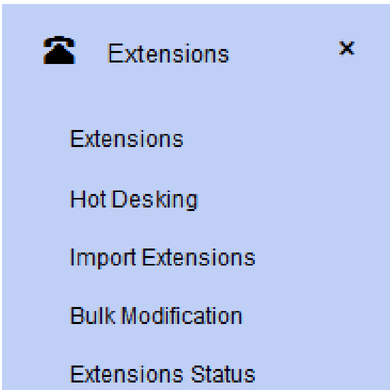
Dialog	Prerequisite Dialogs	Mandatory Fields	Need to Know
DISA		Description Password	Class of Service
Extensions	Technology Profile	Extension Name User Device Password Device Description	Class of Service Email Address Secretary Extension
Extension Status	Extension		
Feature Categories		Description	
Feature Codes			
Hot Desking	User Device	User Device Password Device Description	
Inbound Routes	Destination	Description Destination	
IVR	Destination	Description Invalid Destination Timeout Destination	Welcome Message Keys to press and destinations
Languages	Destination	Name Description Destination	
Night Mode	Destination	Toggle Code Description Destination when Disabled Destination when Enabled	
Outbound Routes	Trunk	Description Trunks Dial Patterns	

Dialog	Prerequisite Dialogs	Mandatory Fields	Need to Know
Paging & Intercom	Extension	Code Description Extensions	
Parking	Destination	Code Timeout Destination	
Pickup Groups	Extension	Description	
PIN Lists		Description	
Queue Priorities	Destination	Description Destination	
Queue VIP		Description VIP List	
Queues		Extension Description	
Ring Groups	Extension	Extension Description Extensions Ring Time Last Destination	
Route Selections		Description	Outbound Route Time Group
Speed Dialing		Speed Dial Code Destination Number	
Terminate Call			
Time Conditions	Time Group Destination	Description Time Group Destination on match Destination no match	
Time Groups		Description	

Dialog	Prerequisite Dialogs	Mandatory Fields	Need to Know
Trunks		Description	Security (for SIP) Security (for IAX) Channel Group (for DAHDi)
Voicemail			
Voicemail Broadcast Group	Extension	Code Description Extensions Password	

2. PBX Menu Set

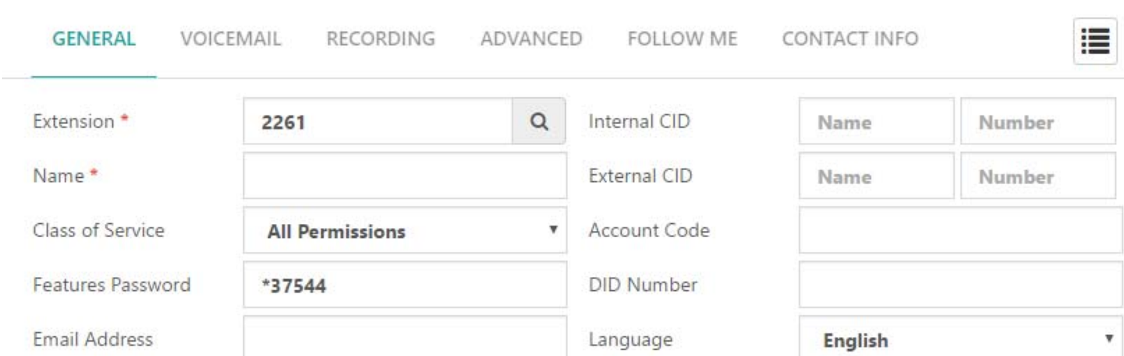
Extensions Menu Group



Extensions Dialog

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

GENERAL Tab



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

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

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

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

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

Only one address can be entered into this field.

Internal CID, internal Caller ID for the extension, consisting of two parts: the CID Name and the CID Number. These will define the caller ID text that is displayed when this user calls other (internal) users on the same PBX. This could be useful when a user is part of a department in which callbacks should be directed to the department rather than directly to the user (such as a technical support department).

This field is not mandatory. If the field is left blank, the user's extension will be used to populate the Caller ID text.

External CID, external Caller ID for the extension, consisting of two parts: the CID Name and the CID Number. This will define the Caller ID text that is displayed when this user makes calls outside of the PBX. This could be useful when a user is part of a department in which callbacks should be directed to the department rather than directly to the user (such as a technical support department). This can only be implemented if your trunk service provider supports setting the Caller ID.

This field is not mandatory, but if the field is left blank, the default Caller ID name for the trunk placing the call will be used to populate the Caller ID name text.

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

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

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

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

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

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

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

You choose from the following languages:

- English (en)
- Spanish (es)
- Spanish (Mexico) (es-MX)

- Spanish (Nicaragua) (es-NI)

Devices Section

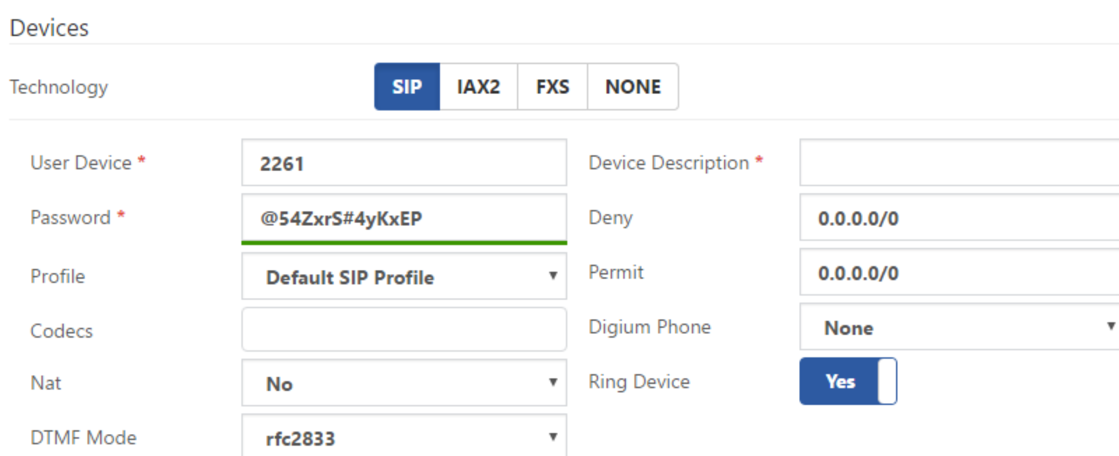
This section allows you to configure the device that is linked to the extension.

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

- **SIP**
- **IAX2**
- **FXS** (analog devices)
- **NONE** (extensions not associated with a device)

Profiles can be defined for SIP, IAX2, and FXS technology types in the Settings>Technology Settings menu group.

SIP Option



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

Password, password (secret) associated with this device. Passwords can be the weakest link of any externally accessible PBX system, as malicious users will attempt to locate extensions having weak passwords. Extensions that authenticate by using simple passwords such as **1234** stand a good chance of being compromised, allowing an attacker to place calls through your PBX. Pick strong passwords carefully, and ensure that passwords are not given to anyone who does not need to know them.

Passwords should be at least 8 characters long, and should include a random mixture of letters (both upper- and lower-case), numbers, and special characters.

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

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

NAT, (Network Address Translation) is a technology commonly used by firewalls and routers to allow multiple devices on a LAN with private IP addresses to share a single public IP address. A private IP address is an address, which can only be addressed from within the LAN, but not from the external internet. Private addresses are in the following ranges:

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

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

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

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

- **info** - SIP INFO messages (application/dtmf-relay)
- **shortinfo** - SIP INFO messages (application/dtmf)
- **inband** - Inband audio (requires 64 kbit codec -alaw, ulaw)
- **auto** - use rfc2833 if it is available, otherwise use in-band option

Device Description, a short (optional) free-text description to identify this device.

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

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

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

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

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

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

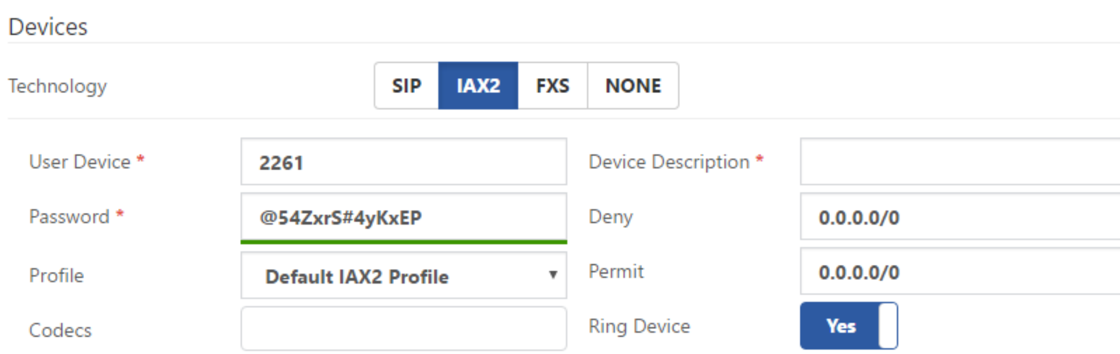
The Permit field is the opposite of the deny field. Specific IP addresses or networks can be added in this field to allow traffic to access this extension from the specified IP address or network.

This field is not mandatory. If it is left blank, traffic will be allowed from all IP addresses. Strengthen your system security by using the Deny and Permit fields. If the endpoint is static, we strongly recommend that you make proper use of the Permit and Deny fields to ensure that traffic is only allowed from the specific address. Even if the endpoint is not static, but always resides on a known subnet, you should limit the allowed range to that specific subnet.

Digium Phone, allows you to associate or create a device as line for a Digium Phone (DPMA). You will not be able to unlink this device after it has been associated to a DPMA Phone.

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

IAX2 Option



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

Password, password (secret) associated with this device. Passwords can be the weakest link of any externally accessible PBX system, as malicious users will attempt to locate extensions having weak passwords. Extensions that authenticate by using simple passwords such as **1234** stand a good chance of being compromised, allowing an attacker to place calls through your PBX.

Pick strong passwords carefully, and ensure that passwords are not given to anyone who does not need to know them. Passwords should be at least 8 characters long, and should include a random mixture of letters (both upper- and lower-case), numbers, and special characters.

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

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

Device Description, a short (optional) free-text description to identify this device.

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

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

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

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

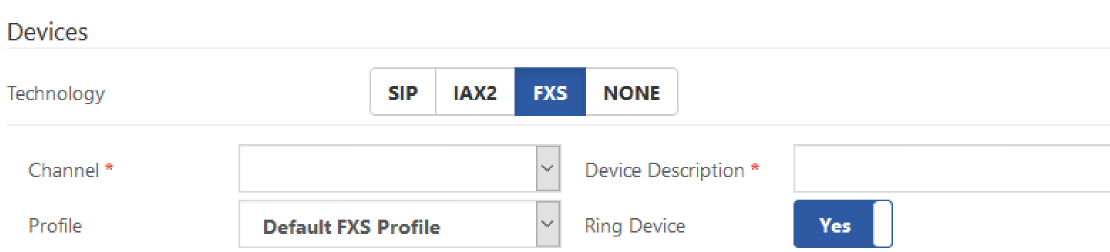
- 192.168.10.0/255.255.255.0 allows traffic from any address on the 192.168.10.x network
- 192.168.10.0/24 allows traffic from any address on the 192.168.10.x network
- 192.168.10.10/32,192.168.10.20/32 will allow traffic from either 192.168.10.10 or 192.168.10.20
  You can define multiple addresses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

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

This field is not mandatory. If it is left blank, traffic will be allowed from all IP addresses. Strengthen your system security by using the Deny and Permit fields. If the endpoint is static, we strongly recommend that you make proper use of the Permit and Deny fields to ensure that traffic is only allowed from the specific address. Even if the endpoint is not static, but always resides on a known subnet, you should limit the allowed range to that specific subnet.

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

FXS Option



Channel*, the DAHDi channel, selected from the drop-down list, that should be associated with this device.

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

Device Description, a short (optional) free-text description to identify this device.

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

NONE Option

No parameters need to be defined for a device of this type.

Digium Phone Settings Section

If you configure a device as a Digium phone, an addition Digium Phone Settings dialog will be shown which will allow you to configure additional Digium-specific information about the device.

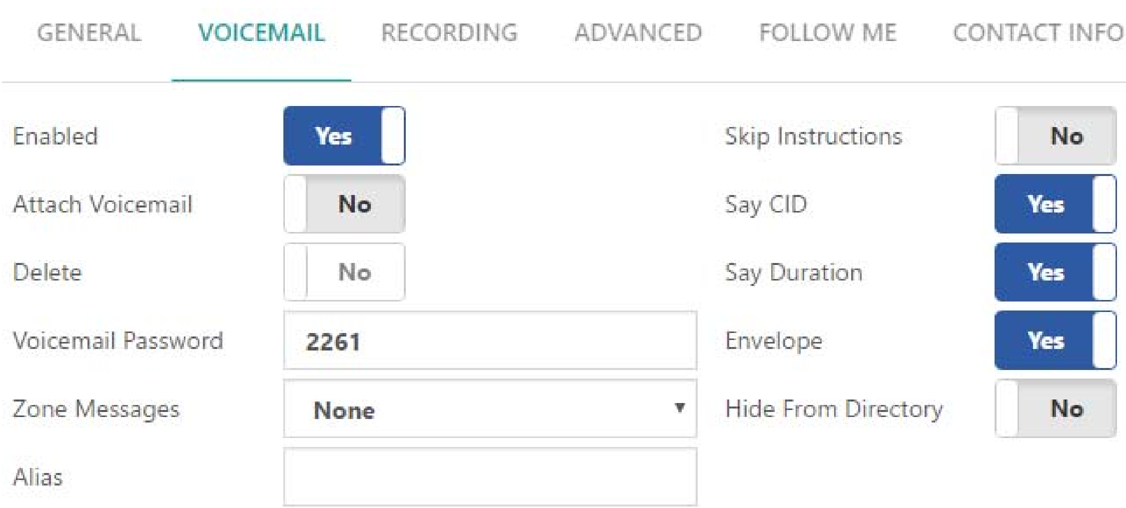
Phone Model, defines the phone model. This allows the system to know how many lines the phone can use.

Voicemail URI, if the message button on your phone should call a SIP URI (rather than opening the visual voicemail application) this option specifies what URI the message button should dial. Setting this option on a phone's primary line will disable visual voicemail.

Digit Mapping, the digit mapping to use for this line.

VOICEMAIL Tab

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



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

Attach Voicemail, determines whether the voicemail recording will be attached to emails.

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

If the password matches the user's extension number, the user will be prompted to create a new password.

This feature is very useful when configuring new extensions. The PBX administrator can set the voicemail password to match the extension number, forcing all users to personalize their password. This enhances user security, so that even the PBX administrator will not know the voicemail password of any extension.

Zone Messages, time zone that should be used for voicemail messages. If this field is configured, the time zone will be taken from the general settings section. Irrelevant if the **Envelope** field is set as **No**.

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

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

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

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

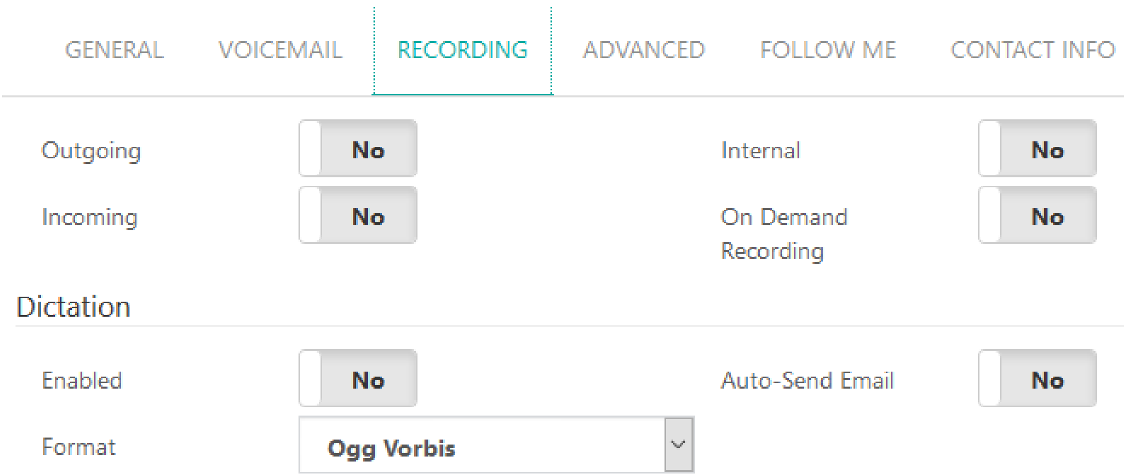
Envelope, determine whether the user will hear the date and time that the message was left prior to hearing the full voicemail message being played.

Delete, causes the voicemail to be deleted from the server after the voicemail has been delivered. Be careful with this option, because the system may delete the message without guaranteeing that a copy of it has been attached to an email notification, or that the email has been delivered successfully. This could mean that after a message is left, and the system has made an attempt to send a notification email to the user, that the actual voicemail that was left may no longer be accessible.

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

RECORDING Tab

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



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

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

Incoming, record all external incoming calls.

Internal, record all internal calls.

On Demand Recording, record only calls on demand.

Dictation Section

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

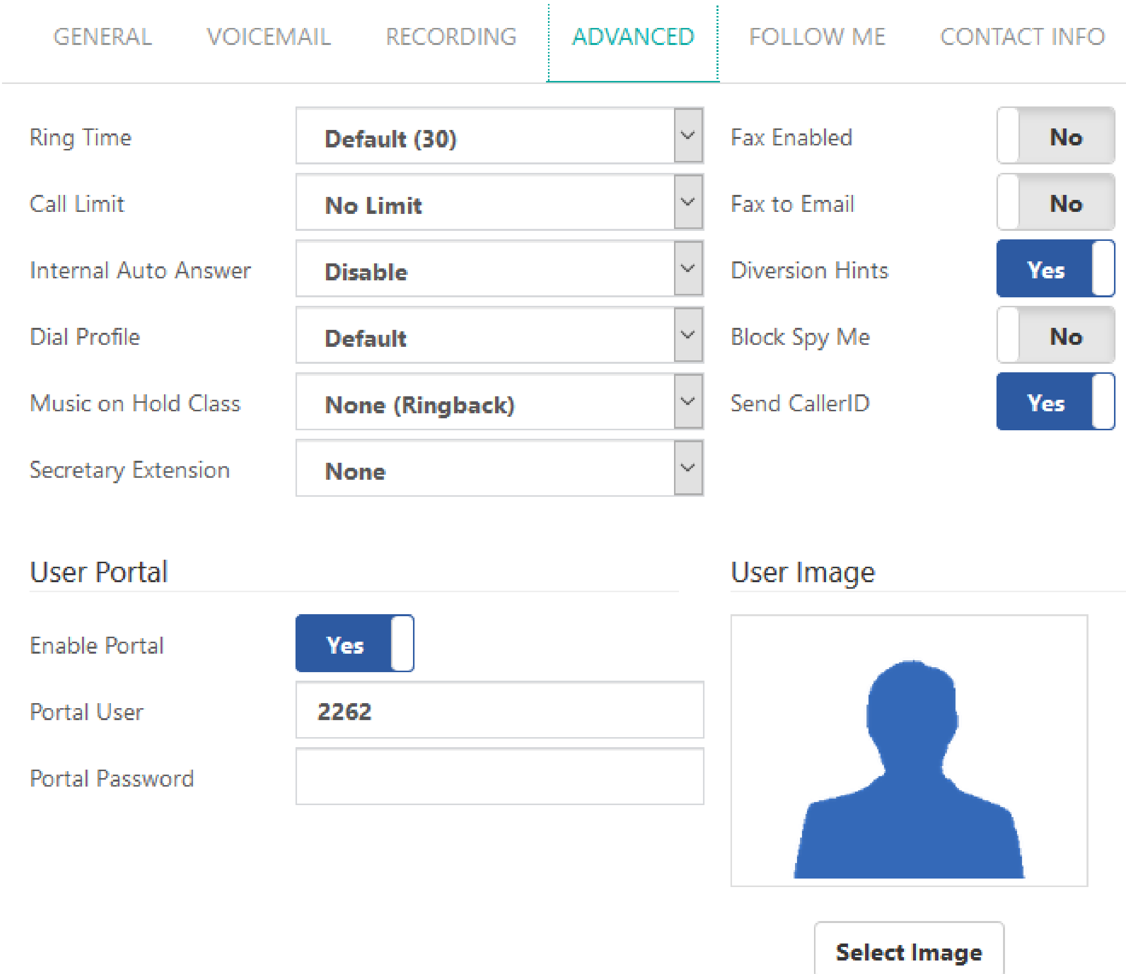
Format, records the audio in one of the formats from the drop-down list:

- Ogg Vorbis
- GSM
- WAV

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

ADVANCED Tab

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



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

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

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

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

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

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

FAX Enabled, indicates whether this extension if configured to receive faxes. If the extension is **FAX Enabled**, the extension can be used for both voice and FAX communications.

Diversion Hints, generate hints regarding diversion status of the extension. For example, hints could be generated for diversions (DND, Call Forwarding, Personal Assistant and Boss/Secretary).

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

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

User Portal Section

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

Enable Portal, determines whether the user of this extension can access the User Portal.

Portal User, contains the username for accessing the User Portal dialog.

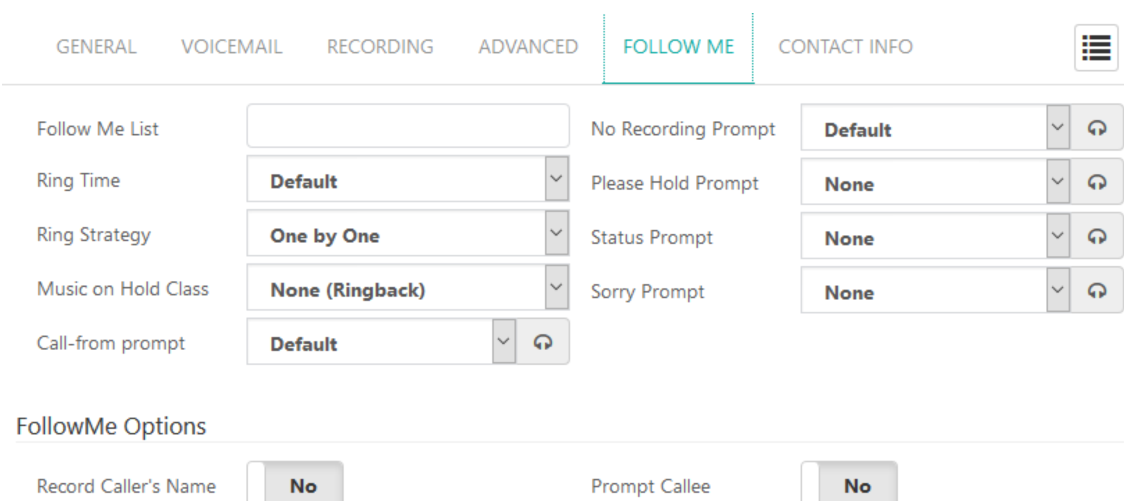
Portal Password, contains the password that is used to access the User Portal. User Portal access cannot be enabled if the password field is left blank.

User Image Section

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

FOLLOW ME Tab

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



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

After typing the digits of the Follow Me destination, you need to click on the blue box to complete the entry. Alternatively, you can press on the Enter button on your keypad. If you want to add multiple destinations, type each destination followed by a comma (“,”).

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

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

MoH Class, the class of Music on Hold that should be played to the caller while they are waiting to be connected.

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

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

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

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

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

Follow Me Options Section

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

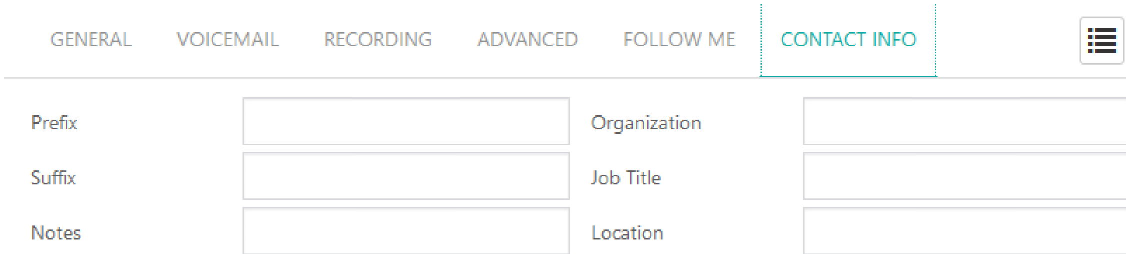
Disable Please Hold Prompt, disable the “Please hold while we try to connect your call” announcement.

Playback Unreachable Status, playback the unreachable status message if the system has run out of steps, or the callee has elected not to be reachable.

Playback Incoming Status, playback the incoming status message prior to activating the Follow Me process.

CONTACT INFO Tab

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



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

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

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

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

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

Hot Desking Dialog

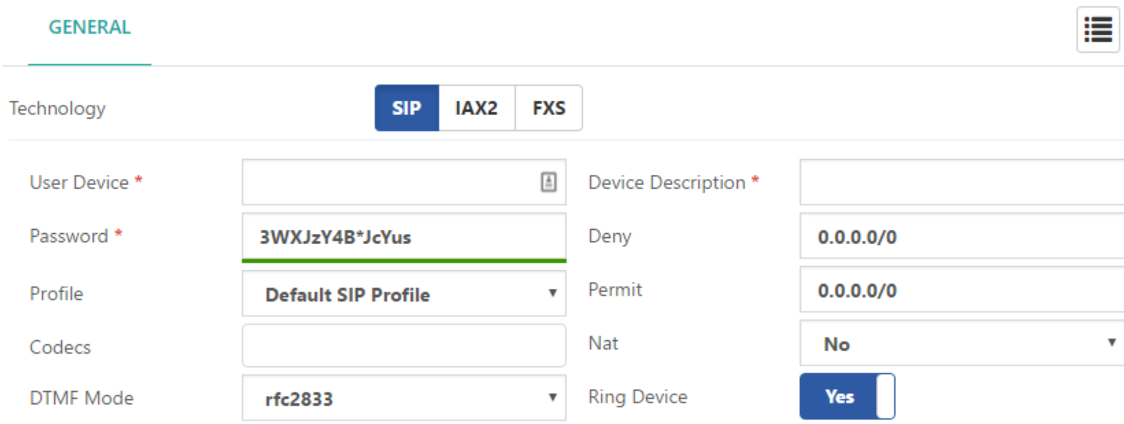
The Hot Desking dialog creates accounts for devices without the need of having an extension number. A Hot Desking device is associated with an extension that previously had to be created in the extensions dialog with technology option "None", i.e. without being associated with any device. A Hot Desking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

GENERAL Tab

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

- **SIP**
- **IAX2**
- **FXS** (analog devices)

SIP Option



User*, user to register this Hot Desk.

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

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

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

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

- **info** - SIP INFO messages (application/dtmf-relay)
- **shortinfo** - SIP INFO messages (application/dtmf)
- **inband** - Inband audio (requires 64 kbit codec -alaw, ulaw)
- **auto** - use rfc2833 if it is available, otherwise use in-band option

Device Description, a short (optional) free-text description to identify this Hot Desk.

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

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

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

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

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

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

This field is not mandatory. If it is left blank, traffic will be allowed from all IP addresses. Strengthen your system security by using the Deny and Permit fields. If the endpoint is static, we strongly recommend that you make proper use of the Permit and Deny fields to ensure that traffic is only allowed from the specific address. Even if the endpoint is not static, but always resides on a known subnet, you should limit the allowed range to that specific subnet.

NAT, (Network Address Translation) is a technology commonly used by firewalls and routers to allow multiple devices on a LAN with private IP addresses to share a single public IP address. A private IP address is an address, which can only be addressed from within the LAN, but not from the external internet. Private addresses are in the following ranges:

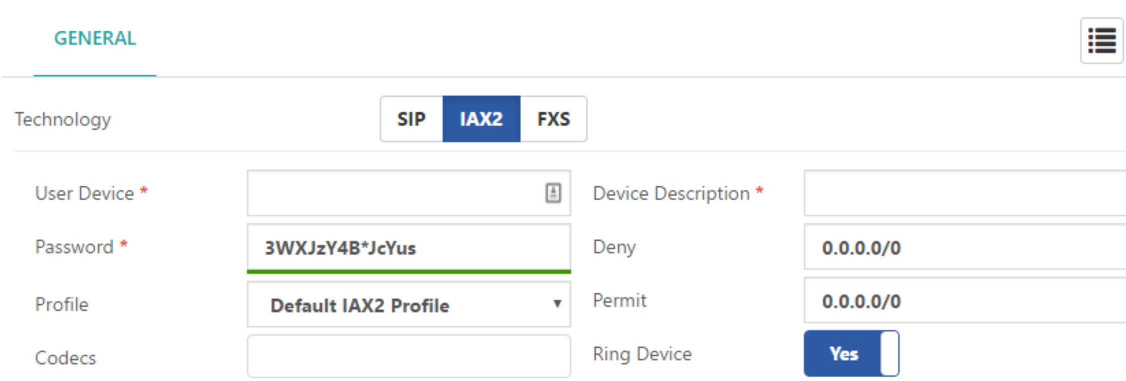
- 10.0.0.1 - 10.255.255.254 – which can also be written as 10.0.0.0/8
- 172.16.0.1 - 172.31.255.254 – which can also be written as 172.16.0.0/12
- 192.168.0.1 - 192.168.255.254 – which can also be written as 192.168.0.0/16

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

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

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

IAX2 Option



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

Password, password (secret) associated with this Hot Desk. Passwords can be the weakest link of any externally accessible PBX system, as malicious users will attempt to locate extensions having weak passwords. Extensions that authenticate by using simple passwords such as **1234** stand a good chance of being compromised, allowing an attacker to place calls through your PBX.

Pick strong passwords carefully, and ensure that passwords are not given to anyone who does not need to know them. Passwords should be at least 8 characters long, and should include a random mixture of letters (both upper- and lower-case), numbers, and special characters.

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

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

Device Description, a short (optional) free-text description to identify this Hot Desk.

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

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

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

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

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

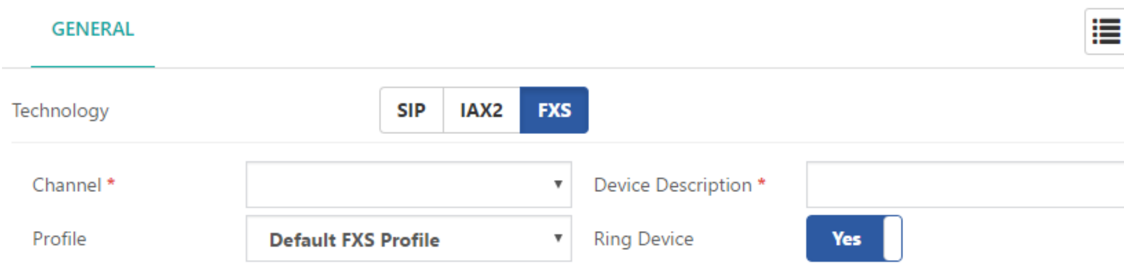
The Permit field is the opposite of the deny field. Specific IP addresses or networks can be added in this field to allow traffic to access this extension from the specified IP address or network.

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

If the endpoint is static, we strongly recommend that you make proper use of the Permit and Deny fields to ensure that traffic is only allowed from the specific address. Even if the endpoint is not static, but always resides on a known subnet, you should limit the allowed range to that specific subnet.

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

FXS Option



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

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

Device Description, a short (optional) free-text description to identify this Hot Desk.

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

Import Extensions Dialog

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

GENERAL Tab

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

An example of the file format can be downloaded by pressing the **Download Import Format** button at the bottom of the screen.

This download will also contain an explanation of each field in the first row of the spreadsheet.

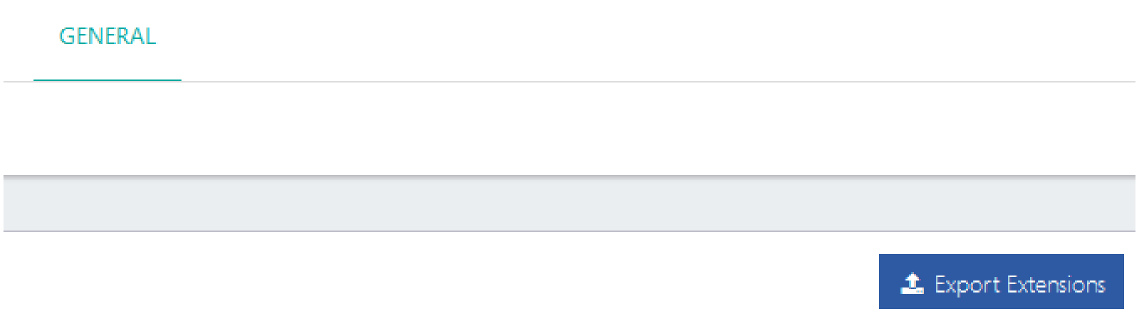
The "Add" action can be used either to add a new extension to the system, or to modify the configuration of an existing extension in the system

Any text fields that include spaces should be enclosed with quotations marks, e.g. "D-Link Sales"

Export Extensions Dialog

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

GENERAL Tab

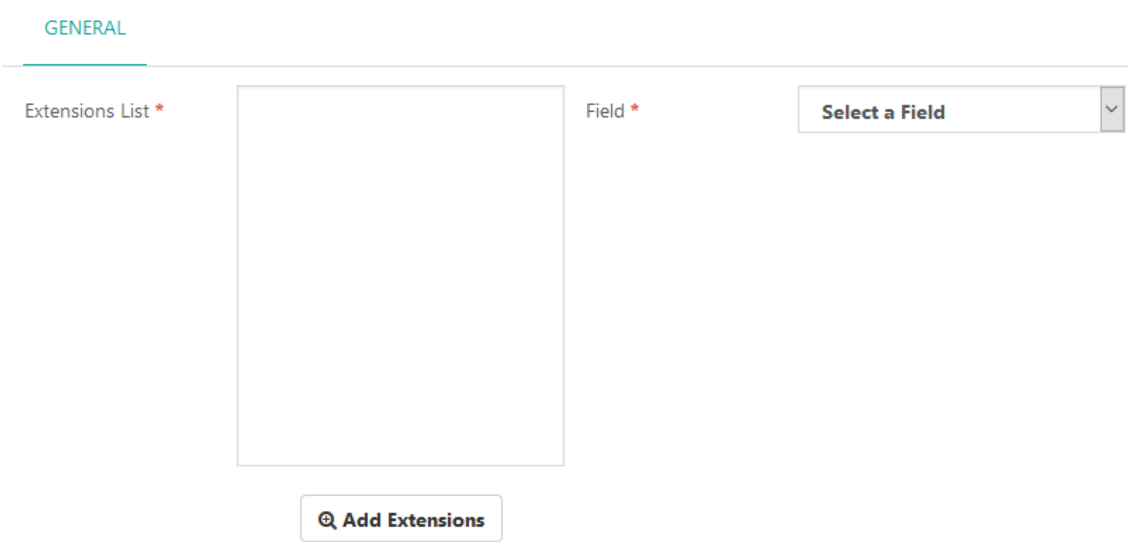


You can use this file in the Import Extensions dialog of another PBX system to create extensions, or (by changing the value in the **mode** column from **add** to **edit**), you could use this file in the Import Extensions dialog of the same PBX system to make modifications to your existing extensions.

Bulk Modification Dialog

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

GENERAL Tab



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

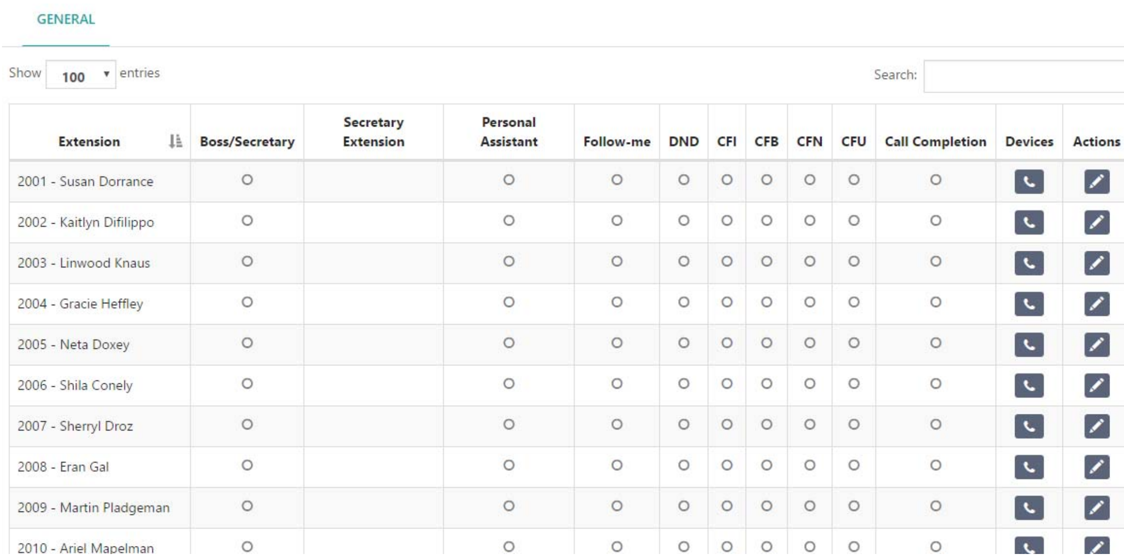
This dialog can manage the following fields:

- Class of Service
- Ring Time
- Account Code
- Dial Options
- MoH Class
- Call Recordings

Extensions Status Dialog

This dialog shows the current status of all extensions.

GENERAL Tab


GENERAL

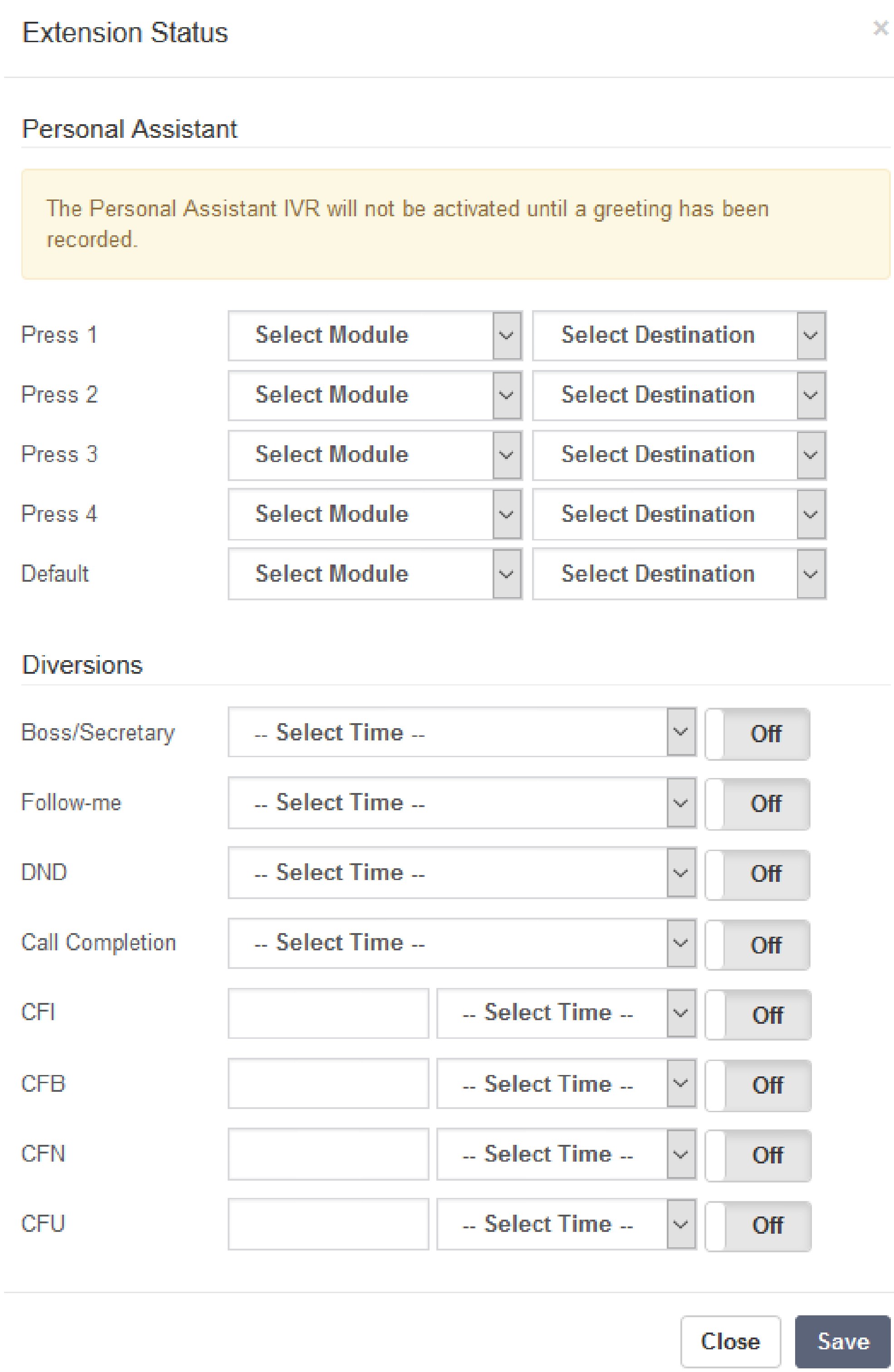
Show 100 entries Search:

Extension	Boss/Secretary	Secretary Extension	Personal Assistant	Follow-me	DND	CFI	CFB	CFN	CFU	Call Completion	Devices	Actions
2001 - Susan Dorrance	○		○	○	○	○	○	○	○	○		
2002 - Kaitlyn Difilippo	○		○	○	○	○	○	○	○	○		
2003 - Linwood Knaus	○		○	○	○	○	○	○	○	○		
2004 - Gracie Heffley	○		○	○	○	○	○	○	○	○		
2005 - Neta Doxey	○		○	○	○	○	○	○	○	○		
2006 - Shila Conely	○		○	○	○	○	○	○	○	○		
2007 - Sherryl Droz	○		○	○	○	○	○	○	○	○		
2008 - Eran Gal	○		○	○	○	○	○	○	○	○		
2009 - Martin Pladgeman	○		○	○	○	○	○	○	○	○		
2010 - Ariel Mapelman	○		○	○	○	○	○	○	○	○		

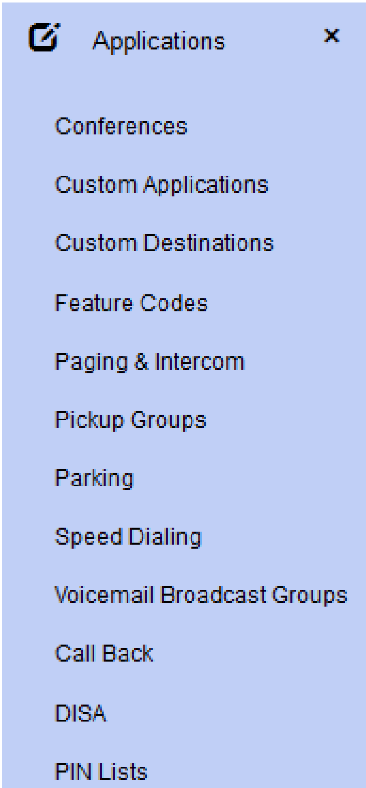
The dialog displays the following fields:

- Extension number
- Boss/Secretary status
- Secretary extension
- Personal Assistant status
- Follow Me status
- Do Not Disturb (DND) status
- Carry Forward Immediately (CFI) status
- Carry Forward Busy (CFB) status
- Carry Forward N (CFN) status
- Carry Forward Unconditionally (CFU) status
- Call Completion status
- Devices
- Actions

You can change any status by simply pressing the Actions ( )button that is located at the end of each line and making the appropriate modification. You can modify the Personal Assistant and Diversion settings of the Extension. The status can be in effect either unconditionally (by NOT selecting a Time Group from the Time drop-down), or during a specific time period as defined by the Time Group that you select from the drop-down list.


Extension Status
Personal Assistant
The Personal Assistant IVR will not be activated until a greeting has been recorded.
Press 1
Select Module
Select Destination
Press 2
Select Module
Select Destination
Press 3
Select Module
Select Destination
Press 4
Select Module
Select Destination
Default
Select Module
Select Destination
Diversions
Boss/Secretary
-- Select Time --
Off
Follow-me
-- Select Time --
Off
DND
-- Select Time --
Off
Call Completion
-- Select Time --
Off
CFI
-- Select Time --
Off
CFB
-- Select Time --
Off
CFN
-- Select Time --
Off
CFU
-- Select Time --
Off
Close
Save

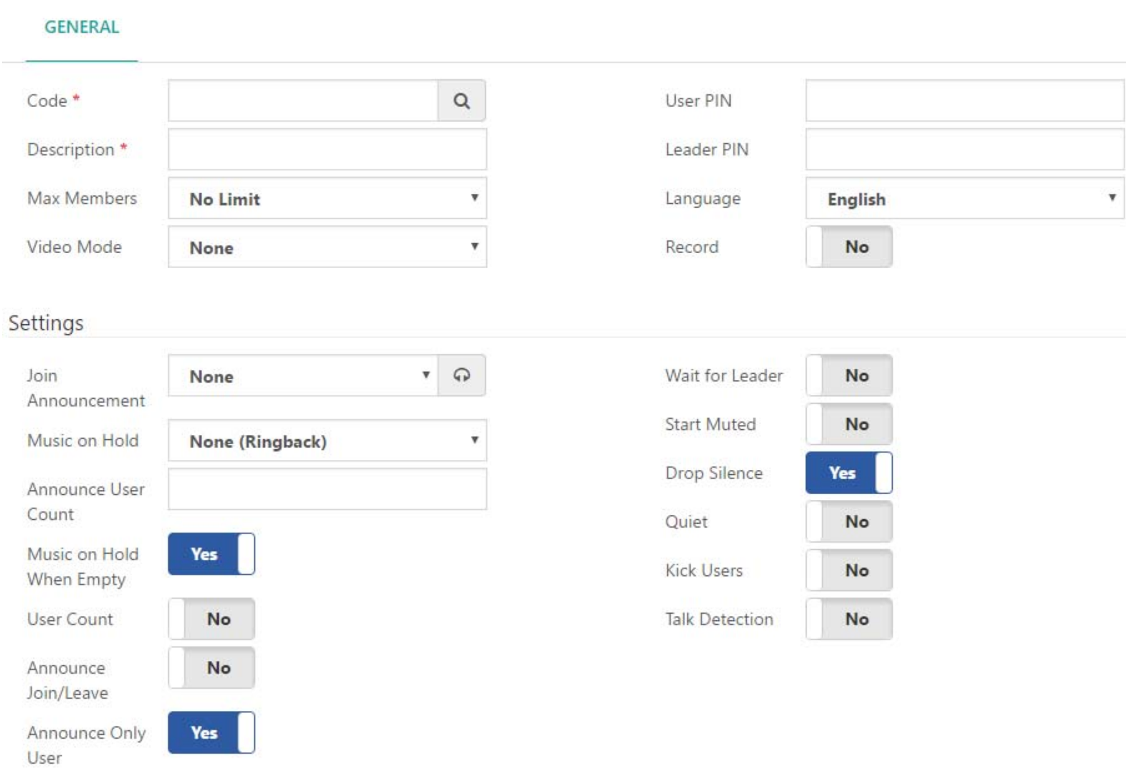
Applications Menu Group



Conferences Dialog

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

GENERAL Tab



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

Description*, short description for identify the conference.

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

Video Mode, determines how video will be displayed. The drop-down list contains the following options:

- **None** - no video sources are set by default in the conference. It is still possible for a user to be set as a video source via AMI or DTMF action at any time.
- **Follow Talker** - the video feed will follow whoever is talking and providing audio.
- **Admin** - the first administrator who joins the conference with video capability is the only source of video distribution to all participants. If the administrator leaves, the next administrator to join becomes the source.

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

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

Language, set the language used for announcements for the conference.

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

Settings Section

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

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

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

- Yes
- No (default)
- A whole number

Music on Hold When Empty, when this field is set to Yes, Music on Hold will be played if there is only one caller in the conference room, or if the conference has not started yet (because the Leader has not arrived). If this field is set to No, no sound will be played.

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

Announce Join/Leave, when this field is set to **Yes,** the conference will prompt each user to identify himself with a name when entering the conference. After the name is recorded, it will be played when the user enters or exits the conference.

Announce Only User, determines whether the **Only User Announcement** should be played when the first user enters a empty conference.

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

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

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

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

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

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

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

- ***1** – toggles Mute setting for the user. When Mute is enabled, anything the user says is not transmitted to the rest of conference members. If the conference is being recorded, anything said by the muted user is not included in the recording.
- ***4** - decreases receive volume. The user can key in this option to decrease the volume that they are hearing. This does not affect what any other conference members hear. If a user is finding other conference members too loud, they can key in *4 a few times to make the Conference quieter for themselves.
- ***5** - increases receive volume. The user can key in this option to increase the volume that they are hearing. This does not affect what any other conference members hear. If a user is having trouble hearing other members of the Conference, they can key in *5 a few times to make the Conference louder for themselves.
- ***6** - decreases transmit volume. The user can key in this option to decrease the volume that they are transmitting to the rest of the conference members. When this option is used, the user will sound quieter to all other conference members. If a user is much louder than the other members of a conference room, they can key in *6 few times to make their transmit volume quieter.
- ***7** - increases transmit volume. The user can tap this option to increase the volume that they are transmitting to the rest of the conference members. When this option is used, the user will sound louder to all other conference members. If the conference members are having trouble hearing a particular user, that user can key in *7 a few times to make their transmit volume louder.
- ***8** – user can key in this code to leave the Conference.

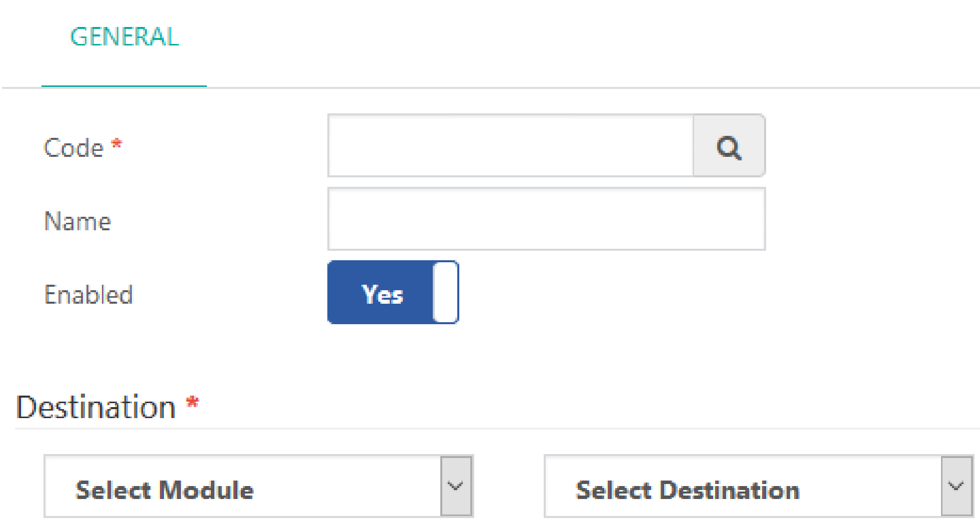
In addition, the admin has access to additional codes:

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

Custom Applications Dialog

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

GENERAL Tab



Code*, the number to call to reach this service.

Name, a free-text name to identify this Custom Application.

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

Destination Section*

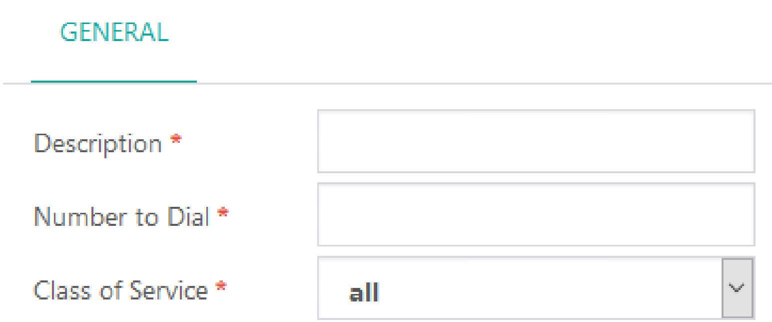
Select Module, allows you to choose from a drop-down list of available dialogs**,** which dialog should be activated.

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

Custom Destinations Dialog

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

GENERAL Tab



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

Code*, is the extension, telephone number, or feature code that the system should call when a caller is routed to this destination. Anything that can be dialed from a user extension can be entered into this field.

Class of Service*, Class of Service in which to search to find the target number.

Feature Codes Dialog

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

Blacklist Section

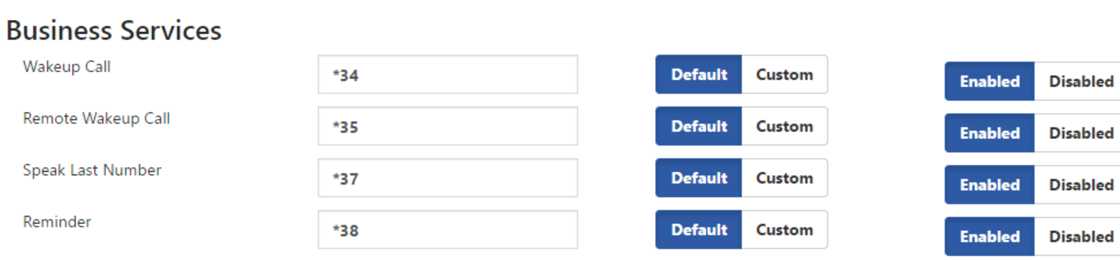
The blacklist feature codes allow users to manage their personal list of blacklisted numbers.

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

- ***30 Blacklist a Number,** prompts the user to enter a telephone number**,** which is then added to the blacklist for the extension. Inbound calls will not ring an extension if they are on the blacklist of the extension. Blacklisted callers will be told that the number they called is no longer in service.
  Key in the feature code. You will be prompted to key in the number to be blacklisted, followed by #. Make sure that you key in the number exactly as it appears in the system, i.e. include appropriate area code. Key in 1 to accept the entry, or hangup to discard it.
- ***31 Remove Number from Blacklist,** prompts the user to enter a telephone number. The entered number will be removed from the extension's blacklist.
  Key in the feature code. You will be prompted to confirm the number to be removed from the blacklist. Key in 1 to remove the blacklisted number, or hangup if you do not want to remove it from the blacklist list.
- ***32 Blacklist Last Caller,** adds the last number that called your extension to the blacklist.
  Key in the feature code. You will be prompted to key in the number to be blacklisted, followed by #. Make sure that you key in the number exactly as it appears in the system, i.e. include appropriate area code. Key in 1 to accept the entry, or hangup to discard it.

Business Services Section

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



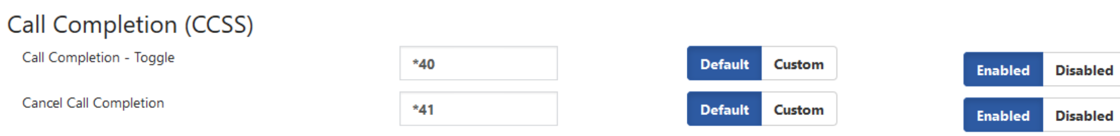
- ***34 Wakeup Call,** set up a reminder or wakeup call for the current extension. Key in the feature code**,** and follow the prompts. Press 1 for a one-time reminder**,** or press 2 for a recurring daily reminder. The time should be entered in 24-hour format using 4 digits. For example**,** key in 0930 for 9:30 am (i.e. 9:30 in the morning)**,** or 2130 for 9:30 pm (i.e. 9:30 in the evening)
  If you already have already set up a reminder call**,** you can key in 1 to cancel it.
- ***35 Remote Wakeup Call,** set up a reminder or wakeup call for another extension. Key in the feature code**,** and follow the prompts. Firstly**,** you will be prompted to enter the number of the extension for which the reminder is intended. Next**,** press 1 for a one-time reminder**,** or press 2 for a recurring daily reminder. The time should be entered in 24-hour format using 4 digits. For example**,** press 0930 for 9:30 am (i.e. 9:30 in the morning)**,** or 2130 for 9:30 pm (i.e. 9:30 in the evening.)
  For improved security, this feature code is disabled by default.

- ***37 Speak Last Number,** speaks the last number that called the current extension. Key in the feature code to hear that last number that dialed the current extension. After listening to the number, you can key in 1 to call the original caller.
- ***38 Reminder,** records a message. You can configure in how many minutes you want to hear the recording. When the set time expires, you will receive a call on the current extension and the recording will be played.

Call Completion Section

Call Completion Supplementary Services (often abbreviated to "CCSS" or simply "CC") allows a caller to let the system automatically alert him when a called party becomes available, after a previous call to that party failed for some reason. The two services offered are Call Completion on Busy Subscriber (CCBS) and Call Completion on No Response (CCNR). To illustrate, let's say that Alice attempts to call Bob, but Bob is currently on a phone call with Carol. Alice hears a busy signal, but she could activate the call completion feature code. Once Bob has finished his phone call, Alice will be alerted, and can attempt to call Bob again.

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

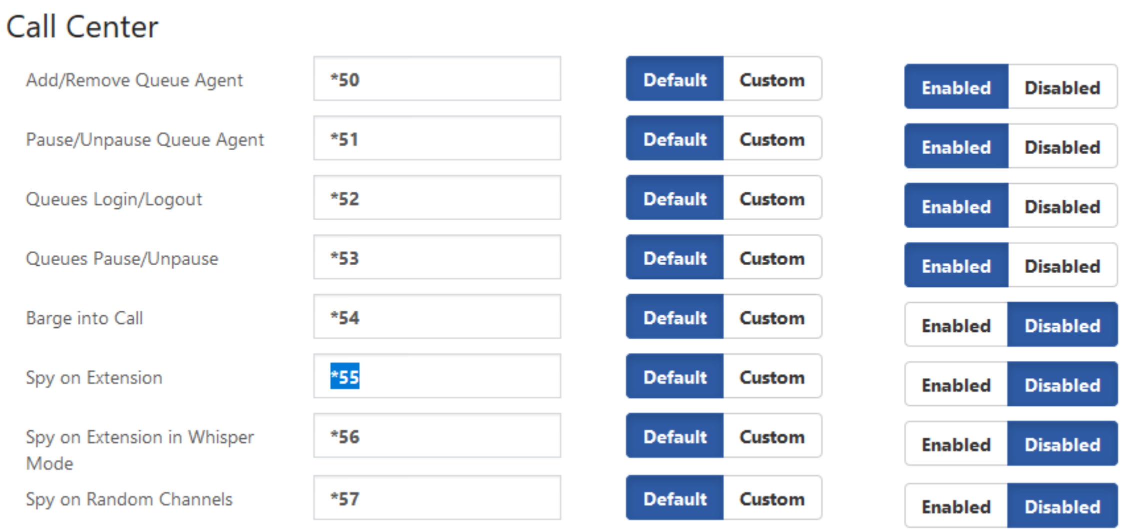


- ***40 Enable/Disable Call Completion,** toggle to activate a call to a previously unresponsive extension when that extension becomes available.
  ***41 Cancel Call Completion,** disables any previously-activated Call Completion.

Call Center Section

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

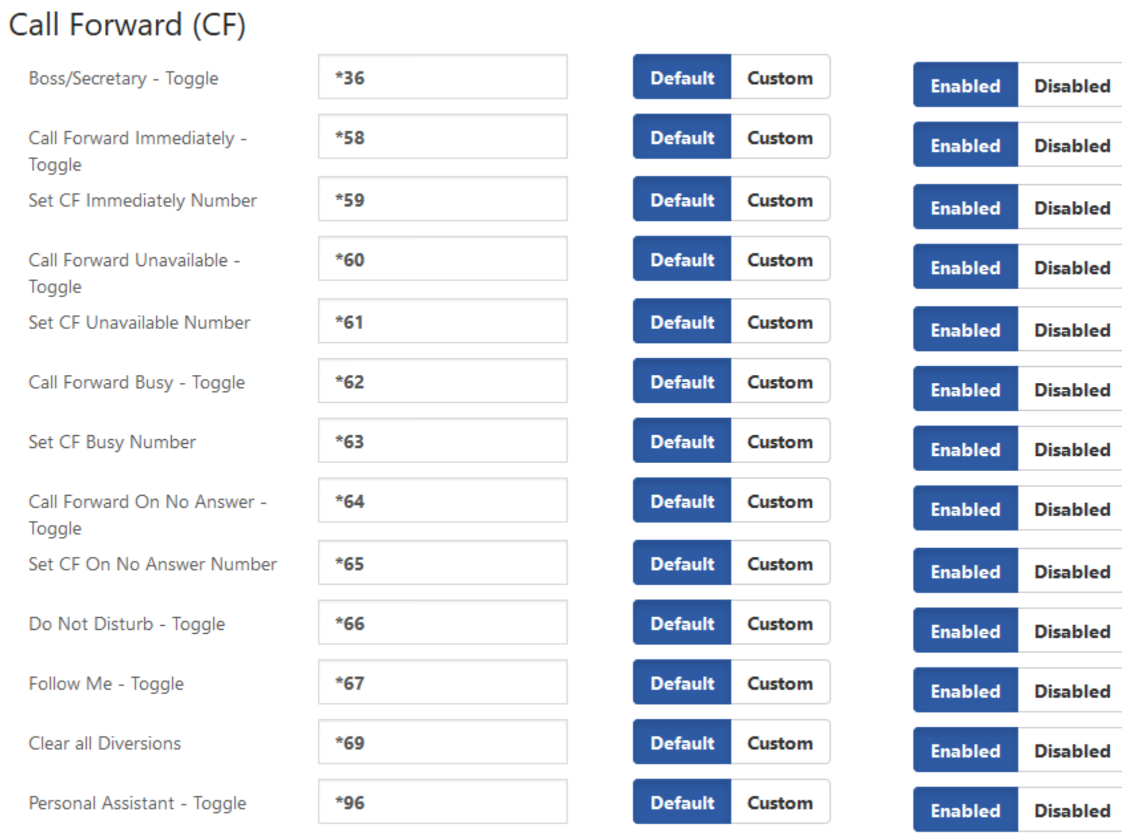
Each of these feature codes are only available to extensions where the specific feature is enabled in the Feature Category that belongs to the Class of Service that is associated with the extension.



- ***50 Add/Remove Queue Agent,** toggle to add an agent to all queue**,** or remove the agent from all queues. You can either key in the feature code and follow the prompts, or (in expert mode) key in the feature code followed by * (asterisk), immediately followed by the number of the agent.
- ***51 Pause/Unpause Queue Agent,** toggle to pause**,** or unpause**,** specific queues for an agent. You can either key in the feature code and follow the prompts, or (in expert mode) key in the feature code followed by * (asterisk), immediately followed by the number of the agent and the queue number.
- ***52 Queues Login/Logout,** allows you to login to (or logout from) a specific queue. Key in the feature code and follow the prompt.
- ***53 Queues Pause/Unpause,** allows you pause (or unpause) all queues.
- ***54 Barge into Call,** allows user to barge into an existing call.
  For improved security, this feature code is disabled by default.
- ***55 Spy on Extension,** spy on a specific extension. Key in the feature code and follow the prompt.
  For improved security, this feature code is disabled by default.
- ***56 Spy on Extension in Whisper Mode,** spy on a specific extension in whisper mode. Key in the feature code and follow the prompt.
  For improved security, this feature code is disabled by default.
- ***57 Spy Random Channels,** spy on random channels.
  For improved security, this feature code is disabled by default.

Call Forward Section

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



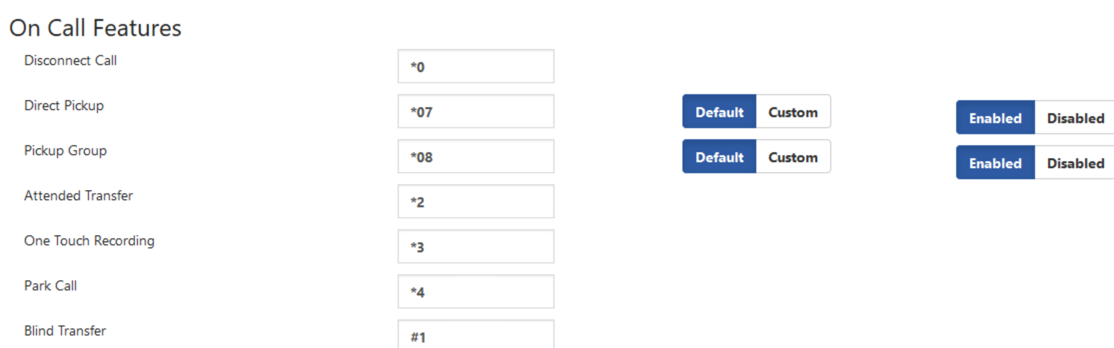
The group of call forwarding provides the following options:

- ***36 Boss/Secretary,** toggle that enables or disables the routing all incoming calls for the current extension to the extension that is defined as the “secretary” phone. Once this function has been enabled**,** only the “secretary” phone will be able to make direct calls to the “boss” phone – all other calls will be routed directly to the “secretary” phone.
  The “boss” extension can enable or disable this function by dialing this feature code.
  The “secretary” extension can also call this feature code to stop receiving calls that are directed to the “boss” extension – all calls will go directly to the “boss” extension.
  This feature code is only available after a “secretary” extension has been defined for the “boss” extension.
- ***58 Call Forward Immediately,** toggles immediate call forwarding.
- ***59 Set CF Immediately Number,** sets the number to which calls should be sent when immediate call forwarding is activated. You can either key in the feature code and follow the prompts, or (in expert mode) key in the feature code followed by * (asterisk), immediately followed by the number to which calls should be forwarded.
- ***60 Call Forward Unavailable,** toggle to enable or disable call forwarding. Calls will be forwarded to the extension defined by the default feature code ***61**.
- ***61 Set CF Unavailable Number,** set the number to which calls should be sent when unconditional call forwarding is activated. Key in the feature code and follow the prompt.
- ***62 Call Forward Busy,** toggle to enable or disable call forwarding when your extension is busy. Calls will be forwarded to the extension defined by the default feature code ***63**.
- ***63 Set CF Busy Number,** set the number to which calls should be sent when call forward busy is activated and your extension is busy. Key in the feature code and follow the prompt.

- ***64 Call Forward on No Answer,** toggle to enable or disable call forwarding when your extension is unable to answer incoming calls. Calls will be forwarded to the extension defined by the default feature code ***65**.
- ***65 Set CF on No Answer Number,** set the number to which calls should be forwarded when your extension is unable to answer. Key in the feature code and follow the prompt.
- ***66 Do Not Disturb,** toggle to enable or disable the Do Not Disturb feature.
- ***67 Follow Me,** toggle to enable or disable the Follow Me feature.
- ***69 Clear all Diversions,** dialing this code this will disable all call diversions**,** including the Do Not Disturb feature.
- ***96 Personal Assistant,** toggle to enable/disable the personal assistant for your extension. This option is only available for extensions where Has Personal Assistant has been enabled in the Advanced tab.

On Call Features Section

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



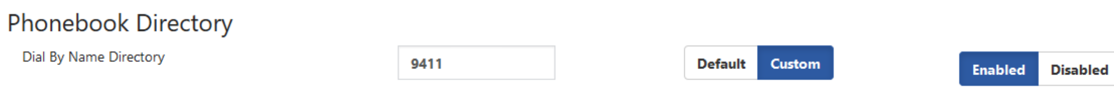
These facilities are used when you are on a call:

- ***0 Disconnect Call,** disconnect the current call.
- ***07 Direct Pickup,** capture a call that is ringing at another extension in your pickup group. You will need to key in the feature code followed by the extension number that you want to answer, i.e. key in*072490 to answer a call ringing on extension 2490 (provided that you both belong to same pickup group.)
- ***08 Pickup Group,** capture a call that is ringing at any other extension in your pickup group. To use this facility is necessary to create call group and pickup group in the extensions dialog.
- ***2 Attended Transfer,** transfer the current call to the operator.
- ***3 One Touch Recording,** force the current call to be recorded.
  This feature code is only available if the Feature Category belonging to the Class of Service that is associated with the extension enables this feature.

- ***4 Park Call,** place the current call in the call park. Key in the feature code and follow the prompt.
- **#1 Blind Transfer,** transfer the current call without notifying the extension to which the call is transferred. This function must be allowed by both the Feature Category and the Dial Profile associated with the extension. Key in the feature code and follow the prompt.

Phonebook Directory Section

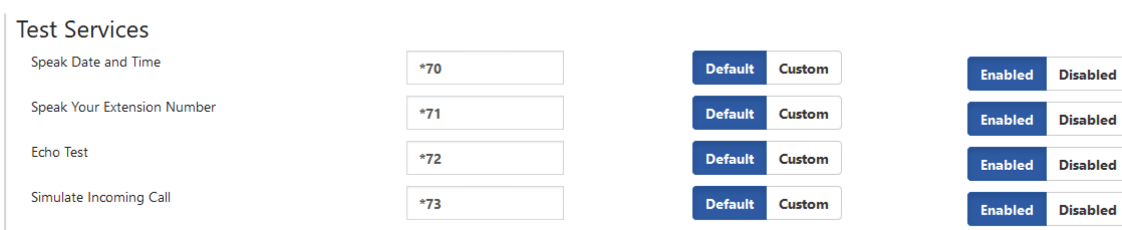
This directory is linked to names of extensions: the user will key in the first few letters of the name and will be presented with a list of extension names that match.



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

Test Services Section

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



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

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

Special Features Section

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

This is a group of features which are described below:

- ***75 Lock/Unlock Phone,** toggle to lock or unlock the current extension. No outbound calls can be made from a phone that has been locked. In order to unlock the phone**,** you will be prompted to enter the Features Password for the extension.
- ***76 Change Features Password,** change the password for the current extension in order to access password-protect telephone features. Key in the feature code and follow the prompt.
- ***77 Remote Substitution,** makes it possible for the current phone to make calls as if you are calling from different phone extension.
- ***78 Customer Code,** creates a customer code to be used by the CDR system - very useful for call accounting. Key in the feature code and follow the prompt.
- ***79 Authorization Code,** allows you to make a call from any phone by using an authorization code that is associated with a unrestricted dial plan. Key in the feature code and follow the prompt.
- ***80 Hot Desking,** toggle to enable or disable Hot Desking.
- ***81 Night Mode All,** toggle to enable/disable all defined night modes.

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

NM-1 would change from activated to deactivated

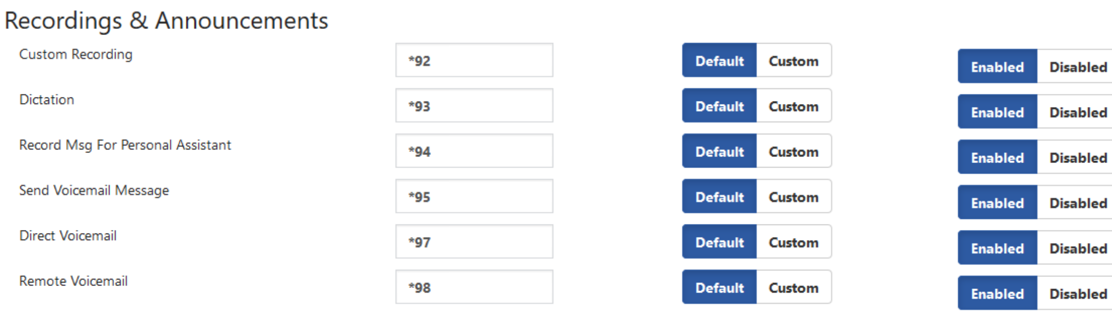
NM-2 would change from deactivated to activated

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

Recordings & Announcements Section

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

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

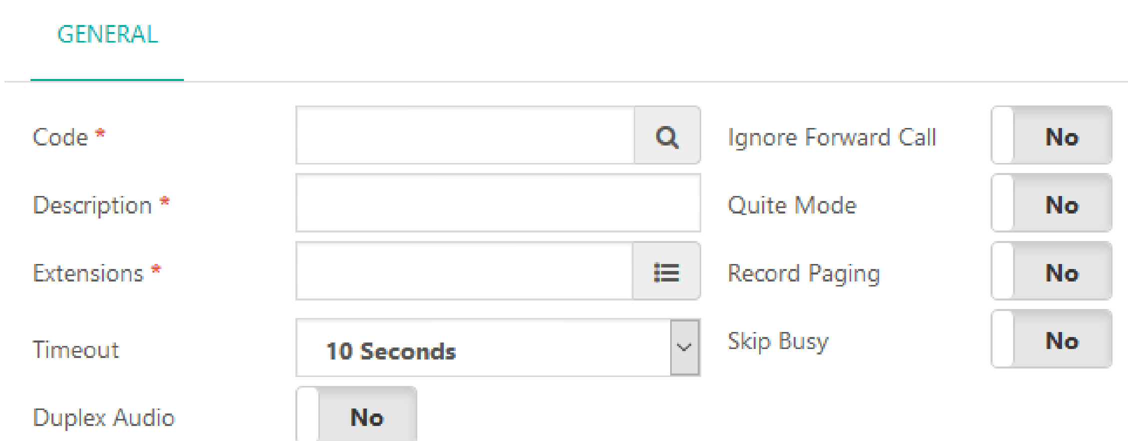


- ***92 Custom Recording,** can be used to record a message. Key in the feature code and follow the prompt.
- ***93 Dictation Services,** can be used to record a message with the option of sending it by email. Key in the feature code and follow the prompt.
  This option is only available for extensions where Dictation has been enabled in the Recording tab.
- ***94 Record Msg for Personal Assistant,** record a message that callers will hear when they are served by your personal assistant. Key in the feature code and follow the prompt.
  This option is only available for extensions where Has Personal Assistant has been enabled in the Advanced tab.
- ***95 Send Voicemail Message,** allows you to call any extension and leave a voicemail message. For example, keying in ***95*2492** will allow you to leave a voicemail message for extension 2492. Note the * that is keyed in between the feature code and the extension number.
- ***97 Direct Voicemail,** direct entry to the voicemail system to listen to voicemail for the current extension – only requires the user to input the voicemail password.
  This option is only available for extensions where voicemail has been enabled in the Voicemail tab.
- ***98 Remote Voicemail,** remote entry to the voicemail system to listen to voicemail for any extension. Requires the user to input both an extension number and the voicemail password for that extension.

Paging & Intercom Dialog

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

GENERAL Tab



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

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

Extensions*, list of the extension(s) that should belong to the page or intercom group.

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

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

Ignore Forward Call, ignore attempts to forward the call. In other words, how to behave when paging an extension that has call forwarding enabled.

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

Record Paging, record the page message in a file.

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

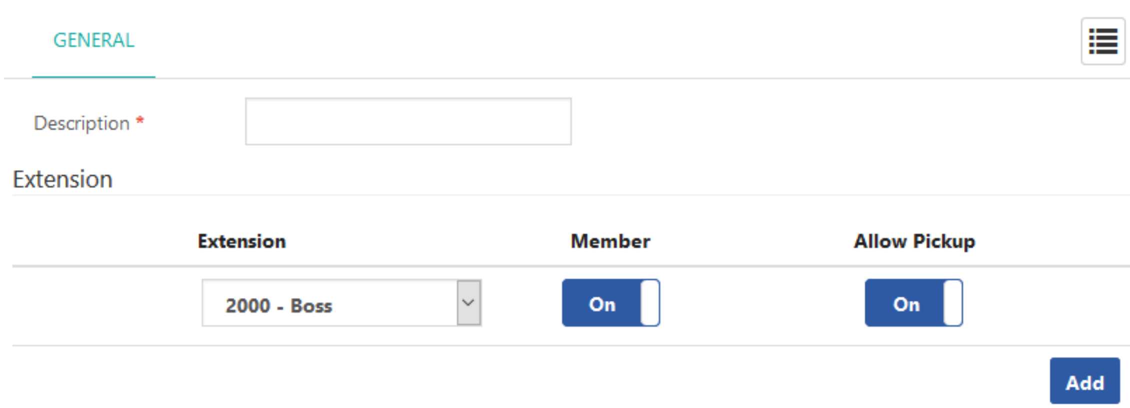
Pickup Groups Dialog

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

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

Note that a user can be part of a pickup group without being a member of the associated call group. For example**,** a senior staff member may be able to pick up calls directed to any member of his department**,** but members of the department should not be able to pick up calls directed to the senior staff member.

GENERAL Tab



Description*, a description to identify the pickup group: this is free text and can consist of numbers and names.

Extension Section

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

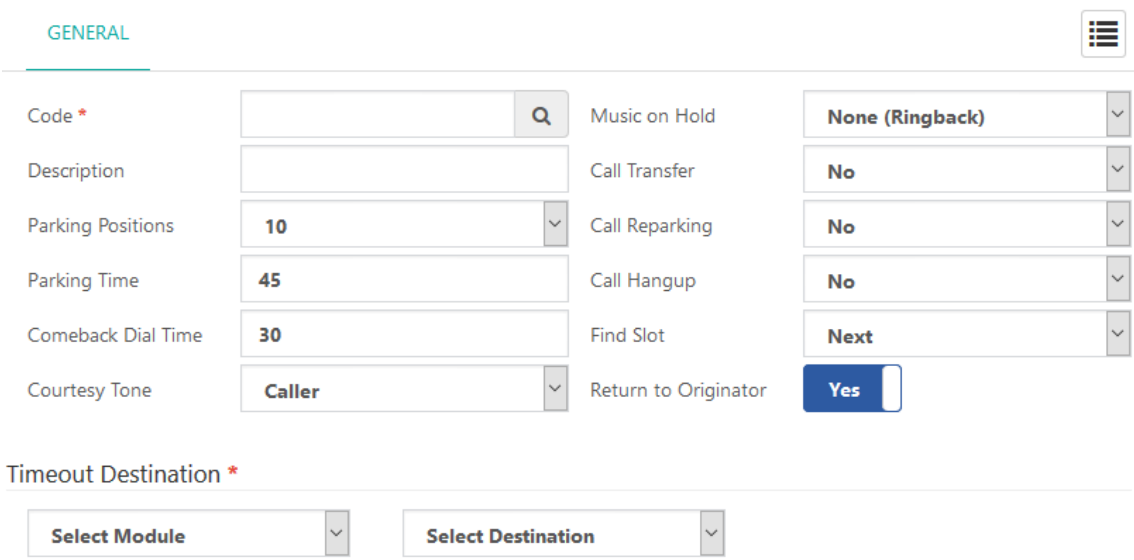
Member, when **On,** indicates that the extension is a member of the pickup group. You can temporarily remove members from the group by changing this status to **Off**

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

Parking Dialog

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

GENERAL Tab



Code*, number to call in order to reach this service.

Name, a short Dfree-text name to identify this park.

Parking Positions, number of parking spaces to allocate in this park.

TimeOut*, length of time (in seconds) that a call can be parked before being returned to the person who originally parked the call.

Return Timeout, when a parked call times out, this is of the length of time (in seconds) to call the person who originally parked the call.

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

- No one
- Caller
- Callee
- Both

MoH Class, this is the Music on Hold (MoH) class to use for music on the parked channel.

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

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

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

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

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

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

Timeout Destination Section

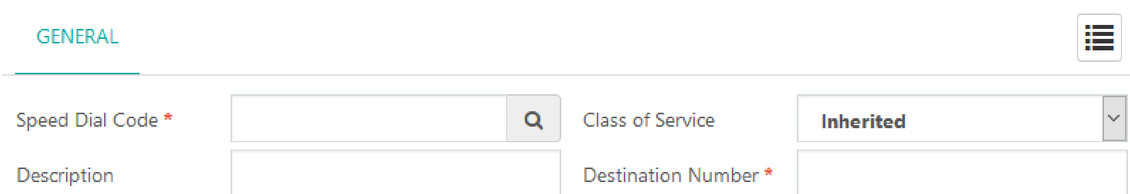
Select Module, select the dialog to used when a parked call times out.

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

Speed Dialing Dialog

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

GENERAL Tab



Speed Dial Code*, number to call in order access the Speed Dial. This must be a unique number.

Name*, short text to identify this Speed Dial.

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

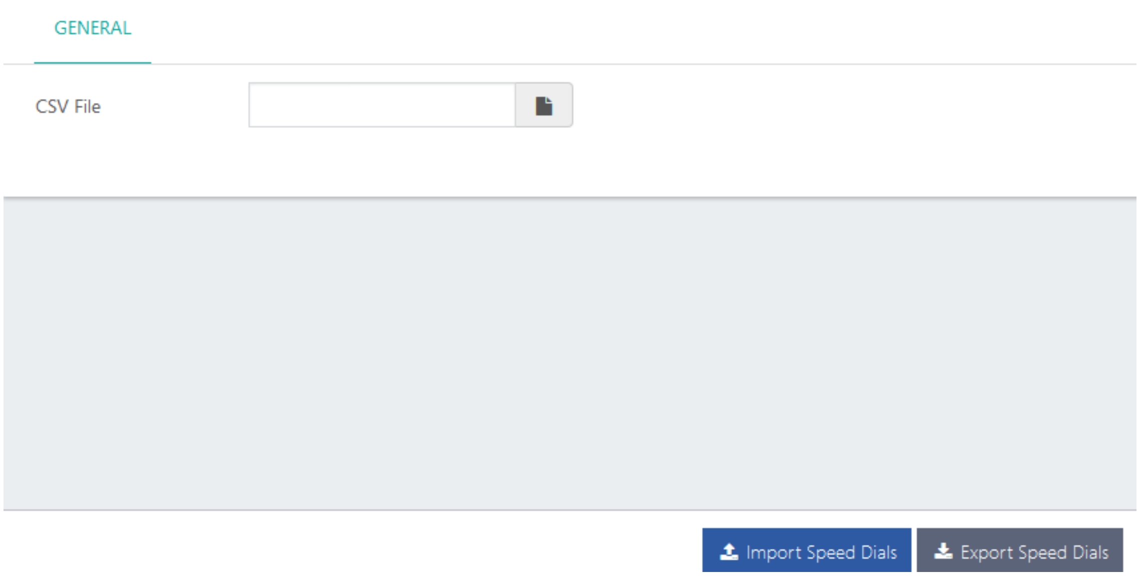
Number to Dial*, the number that will be dialed by this Speed Dial. If the target is an external number**,** this number should include any necessary digits required to access an outbound route.

Import/Export Speed Dialing

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

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

GENERAL Tab



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

Action Buttons

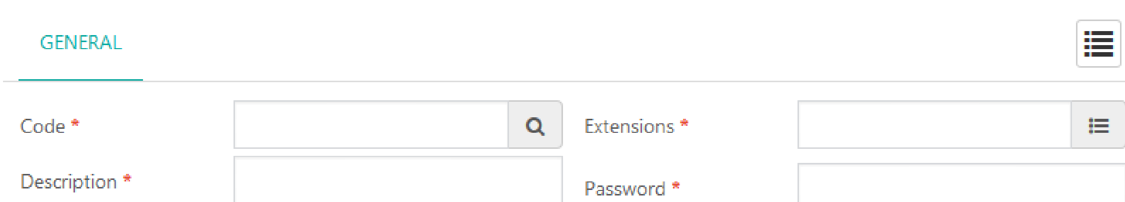
Import Speed Dials, action button to import speed dial information from the named csv file

Export Speed Dials, action button to export speed dial information to a csv file. After pressing this button, you will be asked for details of the csv file.

Voicemail Broadcast Group Dialog

Group of extensions to which voicemail can be sent.

GENERAL Tab



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

Description*, description to identify this Voicemail Broadcast Group

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

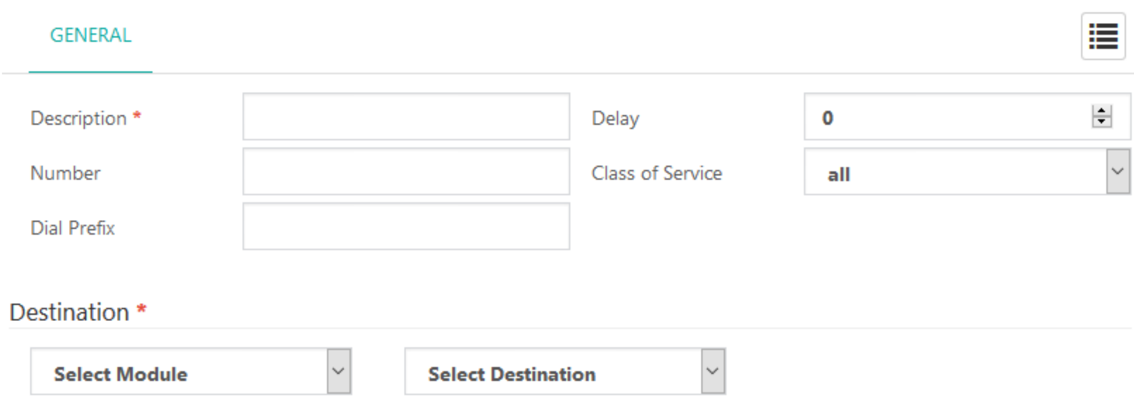
Password*, password to protect this Voicemail Broadcast Group

Call Back Dialog

Callback is a call target that will immediately hang up on a caller, call them back, and then redirect the call to another call target. This is most often used to avoid long-distance charges for remote agents who do not have direct access to all the facilities of the system. This is especially relevant in the case of mobile phones where incoming calls are usually significantly cheaper than outgoing calls.

The callback target may connect the caller with any resource on the system, such as an extension, the voicemail messaging center, or a queue; or it may be used in conjunction with DISA to give the caller a system dial tone from which they can call any telephone number they wish.

GENERAL Tab



Description*, short text description to identify this callback.

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

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

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

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

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

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

Destination Section*

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

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

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

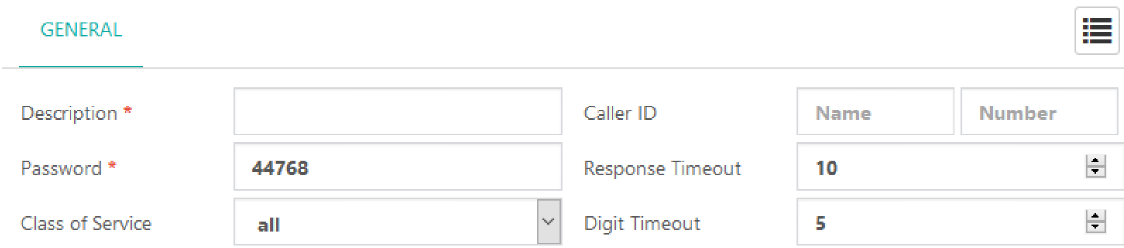
- A company where employees need the ability to check their voicemail from anywhere. Calling the toll-free company phone number costs the company too much money. A callback target could be set up to call back the incoming caller ID, and be directed to the miscellaneous destination of *98. Callers would receive a call on the number they called from, would be prompted for their extension and their password, and would then have access to their voicemail messages.
- A company receives better per-minute rates on calls made through its VoIP trunks than calls made through employees' mobile phones. Employees' mobile phones have free incoming calls. A callback target could be set up for each employee with a mobile phone to call back the employee's mobile number. The callback would be directed to a DISA destination to give the employee a dial tone on the PBX (allowing them to call out using the company's VoIP trunks without using any outgoing mobile minutes).
- A company that receives collect calls from anywhere in the world (such as a credit card company that needs to receive calls if a customer's card is lost or stolen). The company reduces their costs if they use a VoIP trunk local to the country that the customer is in, rather than paying for the entire collect call at hefty international rates. A callback target could be set up to call back the incoming caller ID of the customer and be directed to a queue. The customer would receive a call to the number they called from and would be connected with a company representative as soon as one is available.

DISA Dialog

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

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

GENERAL Tab



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

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

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

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

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

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

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

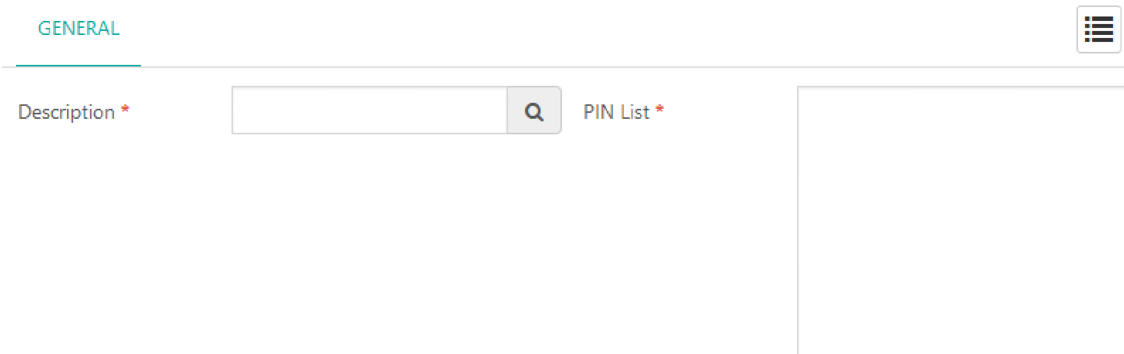
- caller has not entered any digit
- caller has partially entered a number to call without finishing the entry.

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

PIN Lists Dialog

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

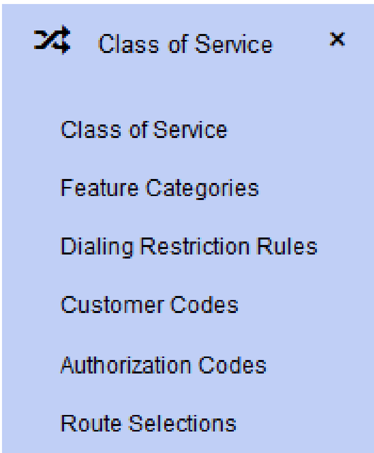
GENERAL Tab



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

Pin List*, list of PINs that can be used. A PIN may consist of any combination of numbers and the "*" (asterisk) symbol. If you want add multiple PINs, you can do so by starting a new line.

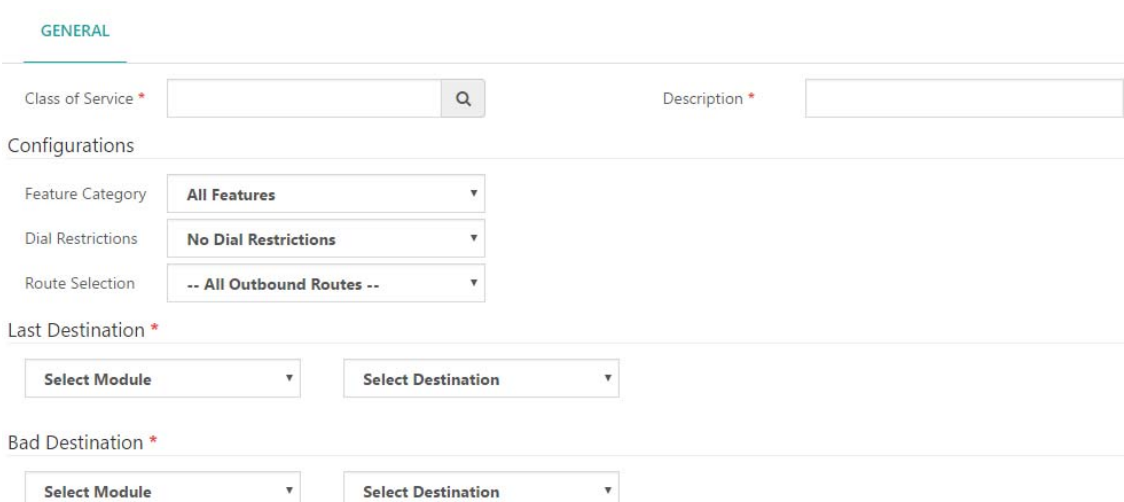
Class of Service Menu Group



Class of Service Dialog

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

GENERAL Tab



Class of Servicew*, Class of Service Name (must be unique).

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

Configurations Section

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

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

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

Last Destination Section

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

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

Bad Destination Section

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

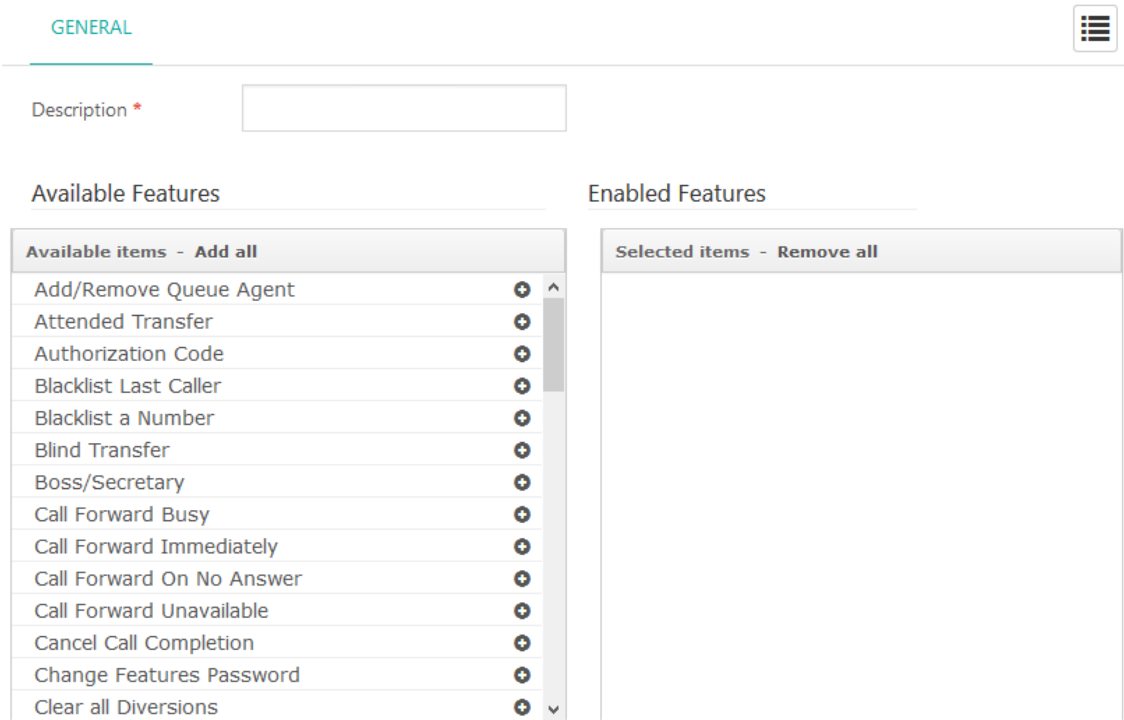
Select Destination, is the call target to which the call should be routed.

Feature Categories Dialog

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

GENERAL Tab

In this tab you will find the information about each Feature Category.



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

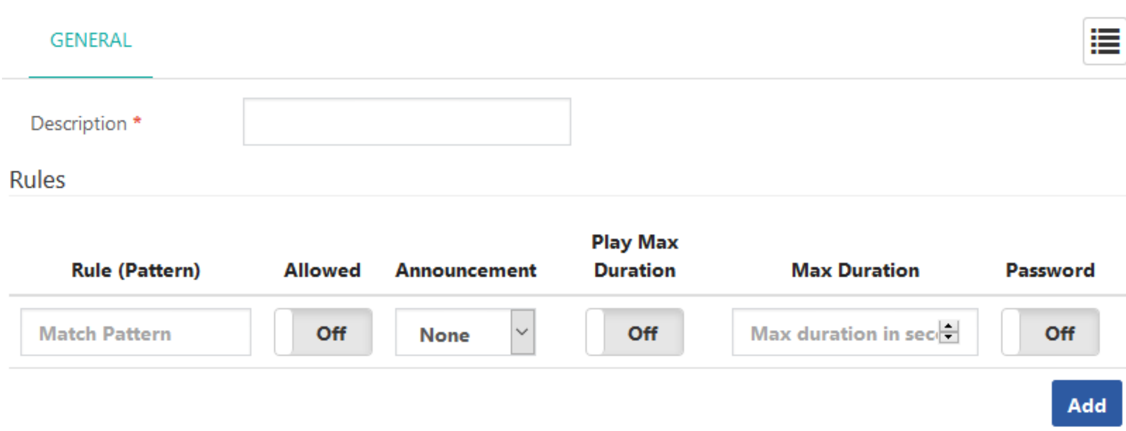
Available Features, list of available feature codes.

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

Dialing Restriction Rules Dialog

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

GENERAL Tab



Description*, short free-text title to identify this "Dialing Restriction" - must be unique.

Rules Section

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

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

Allowed, allow/disallow this pattern.

Announcement, choose an announcement associated with this pattern.

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

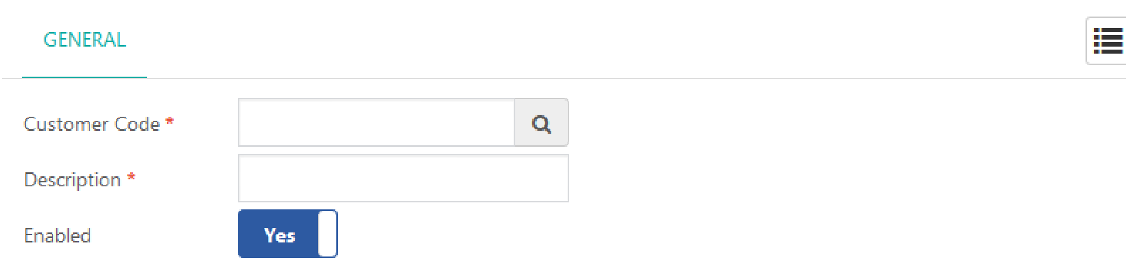
Max Duration, maximum call duration**,** in seconds**,** associated with this rule.

Password, determine whether a password is required when using this rule.

Customer Codes Dialog

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

GENERAL Tab



Customer Code*, customer code number.

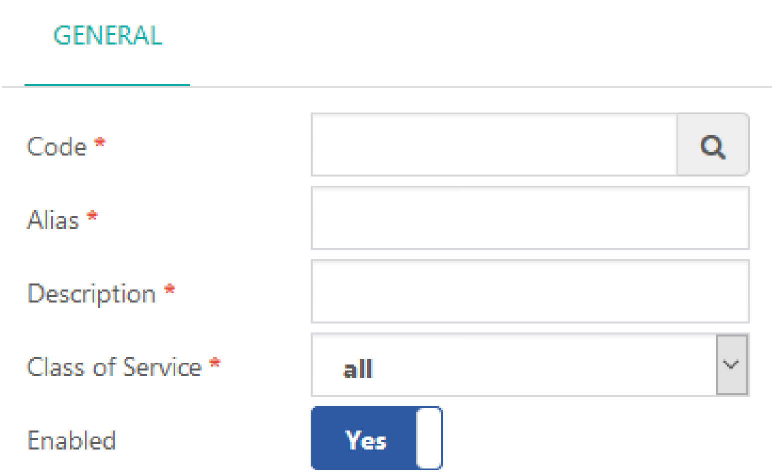
Description*, short free-text description to identify this customer code.

Enabled, enable/disable this customer code.

Authorization Codes Dialog

Code that grants privilege to make a call from any extension.

GENERAL Tab



Code*, authorization code number.

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

Description*, Short free-text description to identify this Authorization Code.

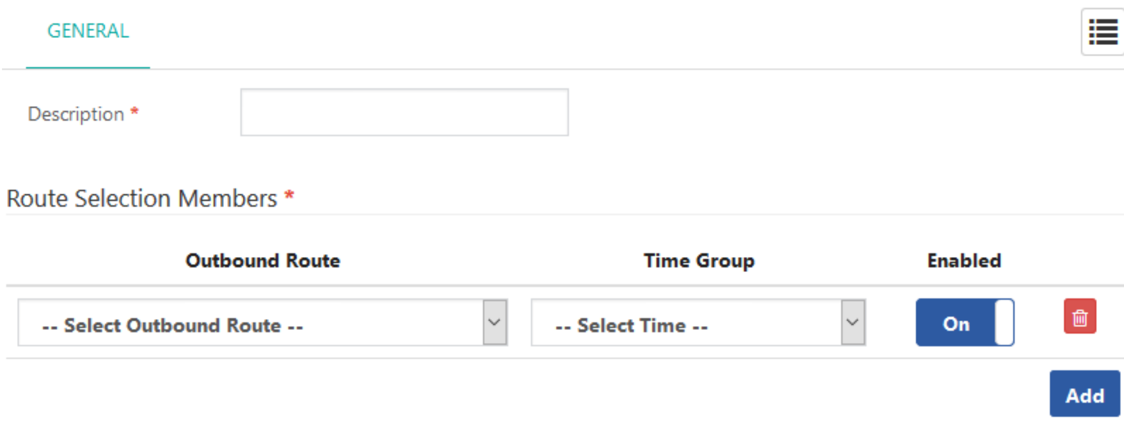
Class of Service, Class of service that is used to route the call.

Enabled, toggle to enable/disable this Authorization Code.

Route Selections Dialog

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

GENERAL Tab



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

Route Selection Members Section

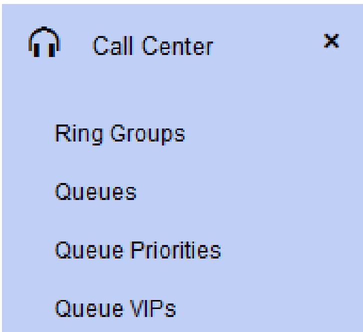
You can use the **Add** button at the bottom of the dialog to add addition route selection members.

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

Time Group, select a time group that should be applied to this route selection.

Enabled, toggle to enable or disable this route.

Call Center Menu Group



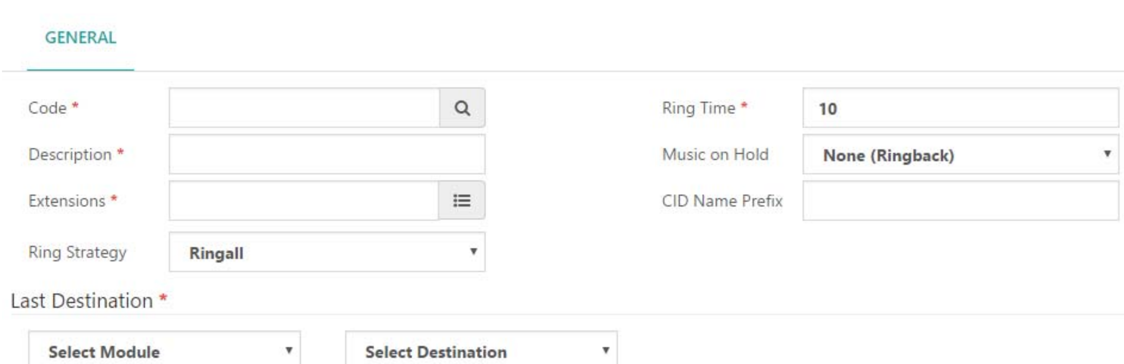
Ring Groups Dialog

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

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

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

GENERAL Tab



Code*, number to reach this service.

Description*, short free-text description to identify this ring group.

Extensions, list of extension for this ring group.

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

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

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

Music on Hold, music on hold to play.

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

Destination Section

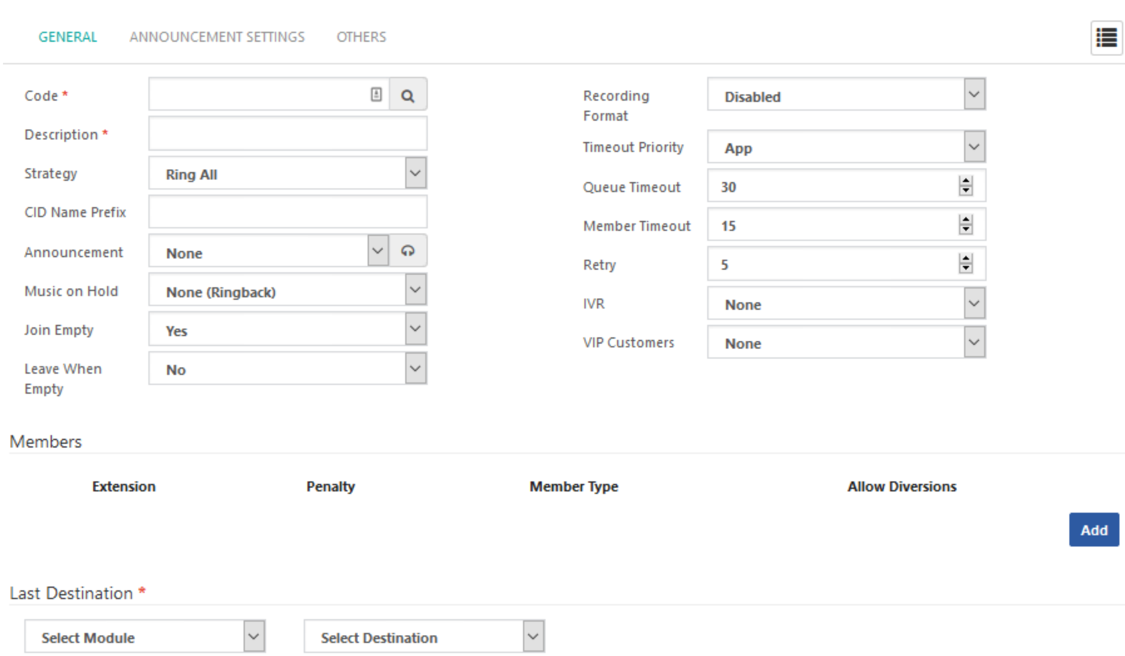
Select Module, allows the user to choose from a drop-down list of available dialogs**,** which dialog should be activated.

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

Queues Dialog

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

GENERAL Tab



Code*, number to reach this service.

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

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

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

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

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

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

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

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

Timeout Priority, controls which timeout value to use if there is a conflict between the timeout values. The Queue application has a timeout value that is used to specify the absolute time that a caller can be in the queue, while the timeout value in queues.conf determines how long to ring a member,

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

Member Timeout, determines for how long to ring a member’s device.

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

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

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

Members Section

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

Extension, extensions that can be members of this queue.

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

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

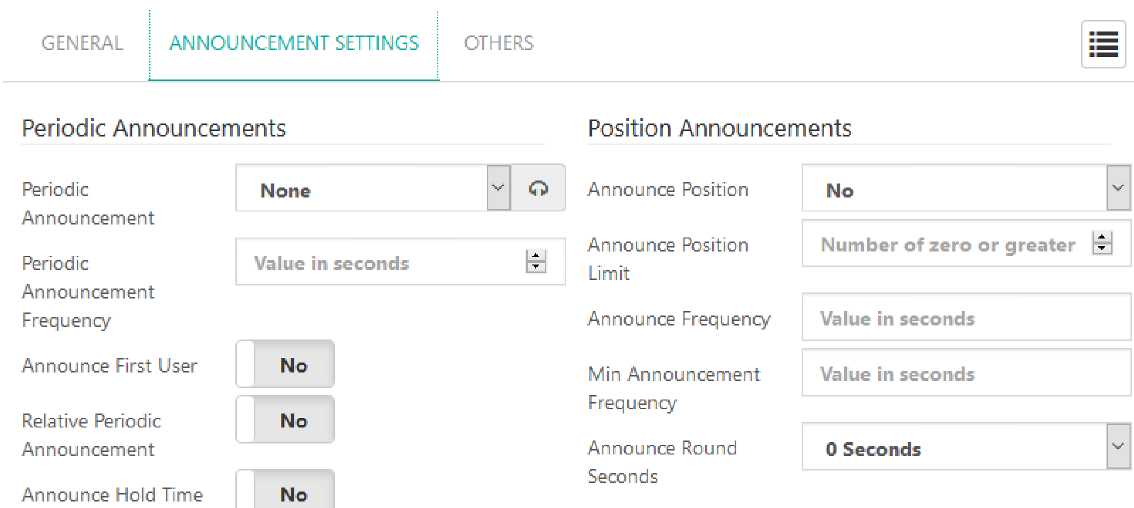
Allow Diversions, if this field is set to **No,** diversions, such as Follow Me, will be ignored.

Final Destination Section*

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

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

ANNOUNCEMENT SETTINGS Tab



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

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

- keeping this message short
- not playing it too frequently.

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

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

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

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

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

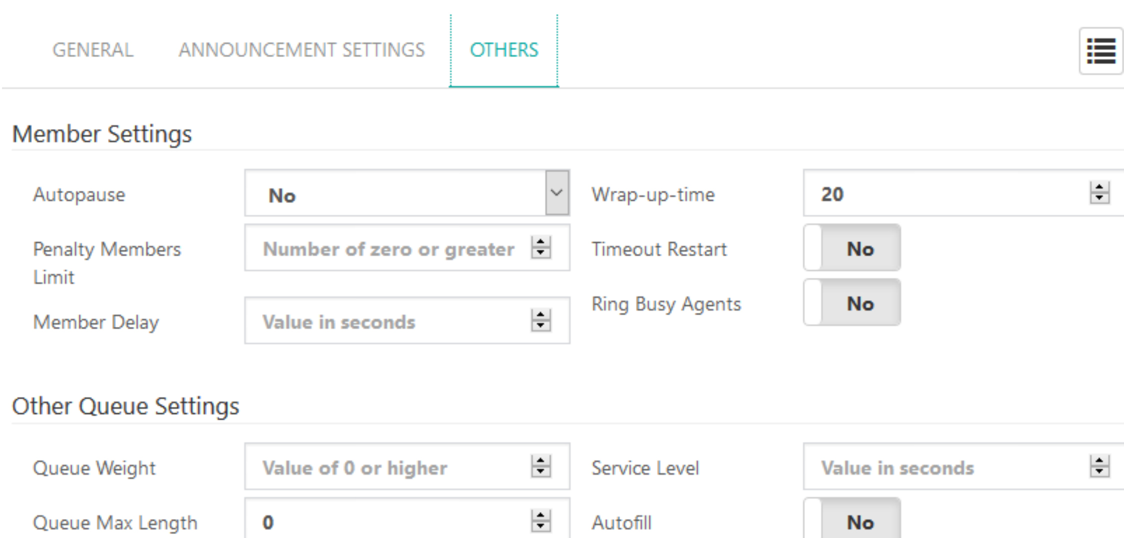
Announce Position Limit, used if you've defined Announce Position as either limit or more

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

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

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

OTHERS Tab



Members Settings Section

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

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

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

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

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

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

Other Queue Settings Section

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

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

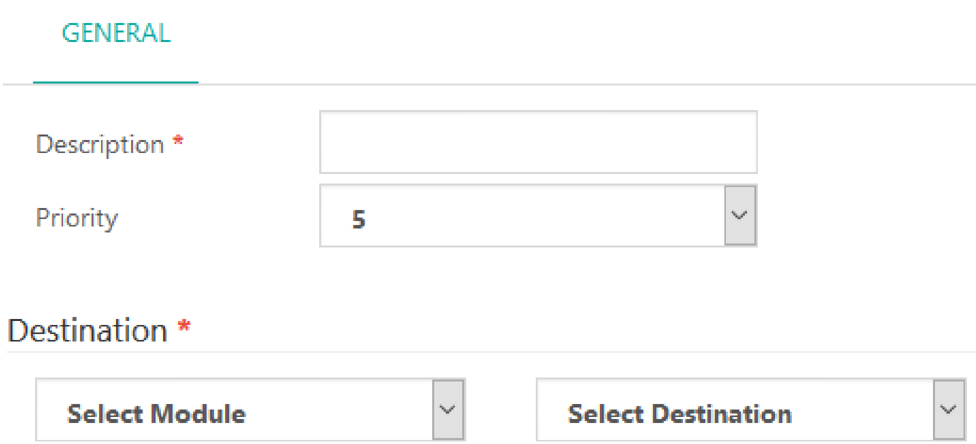
Service Level, this setting is not as useful as it should be. The idea is to define the maximum acceptable time for a caller to wait before being answered. You then note how many calls are answered within that threshold, and they go toward your service level. So, for example, if your service level is 60 seconds, and 4 out of 5 calls are answered in 60 seconds or less, your service level is 80%.

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

Queues Priorities Dialog

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

GENERAL Tab



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

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

Destination Section

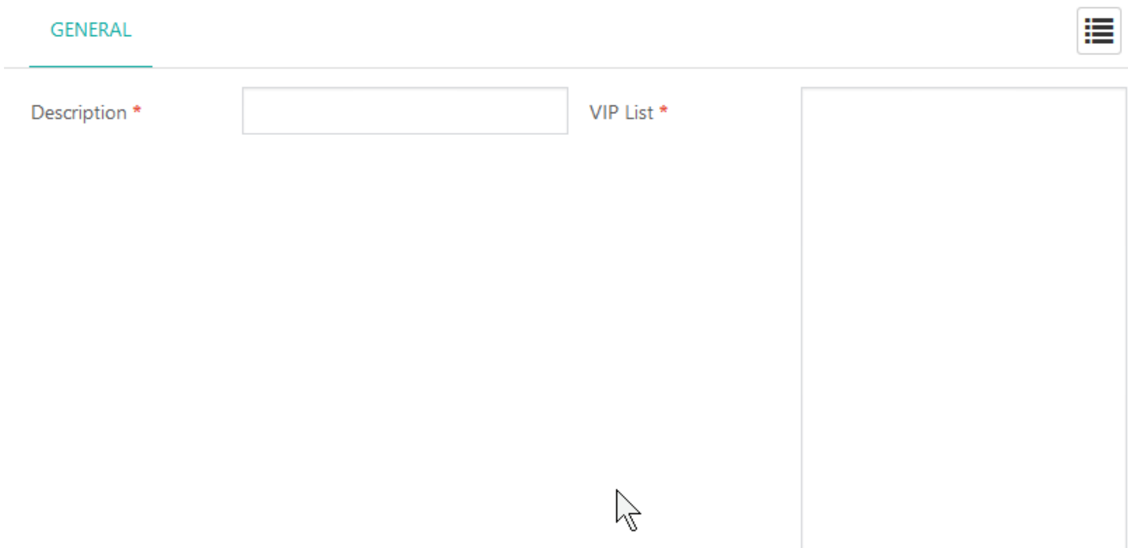
Select Module, allows the user to choose from a drop-down list of available dialogs**,** which dialog should be activated.

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

Queue VIPs Dialog

Allows you to configure customers who have priority when calling into a queue.

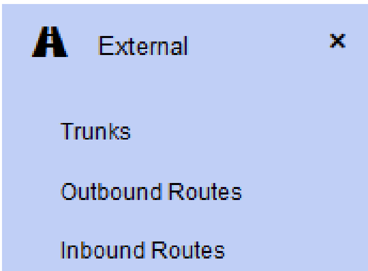
GENERAL Tab



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

VIP List*, insert the list of caller numbers (CID) separated by a carriage return.

External Menu Group



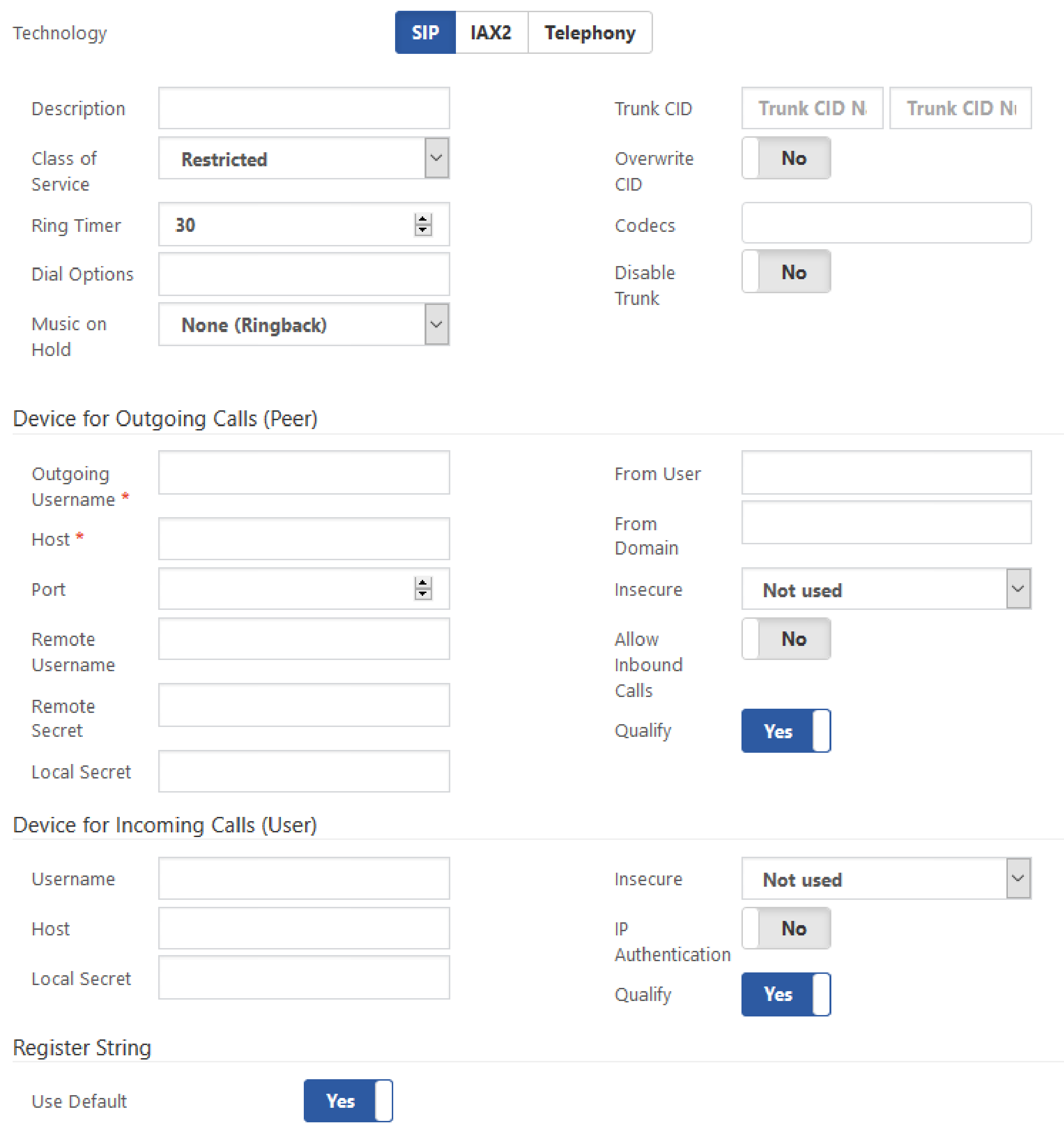
Trunks Dialog

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

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

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

GENERAL Tab



Technology Section

- SIP
- IAX2
- Telephony

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

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

Description*, a unique, free-text description to help identify this trunk

Class of service, choose a class of service for this trunk.

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

Dial Options, dial options parameters, except for Custom trunks. Examples of some common dial options:

- D(called:calling) - send the specified digits after the called party has answered, but before the call gets bridged. The 'called' digits are sent to the called party, and the 'calling' digits are sent to the calling party. Both arguments can be used alone.
- H - allow the called party to hang up by using the In-Call Asterisk Disconnect code (default value is **)
- H - allow the calling party to hang up by using the In-Call Asterisk Disconnect code (default value is **)
- i - any forwarding requests that may be received on this dial attempt will be ignored.
- I - any connected line update requests or any redirecting party update requests that may be received on this dial attempt will be ignored.
- r - generate ringing to the calling party, even if the called party is not actually ringing. Pass no audio to the calling party until the called channel has answered.
- S(x) - hang up the call x seconds after the called party has answered the call.
- t - allow the called party to transfer the calling party by using the In-Call Asterisk Blind Transfer code (default value is ##)
- T - allow the calling party to transfer the called party by using the In-Call Asterisk Blind Transfer code (default value is ##)
- w - allow the called party to enable recording of the call by using the In-Call Asterisk Toggle Call Recording code (default value is *1)
- W - allow the calling party to enable recording of the call by using the In-Call Asterisk Toggle Call Recording code (default value is *1)

See the full list of available options in Dial Options section in the appendix.

MoH Class, default music on hold for this trunk

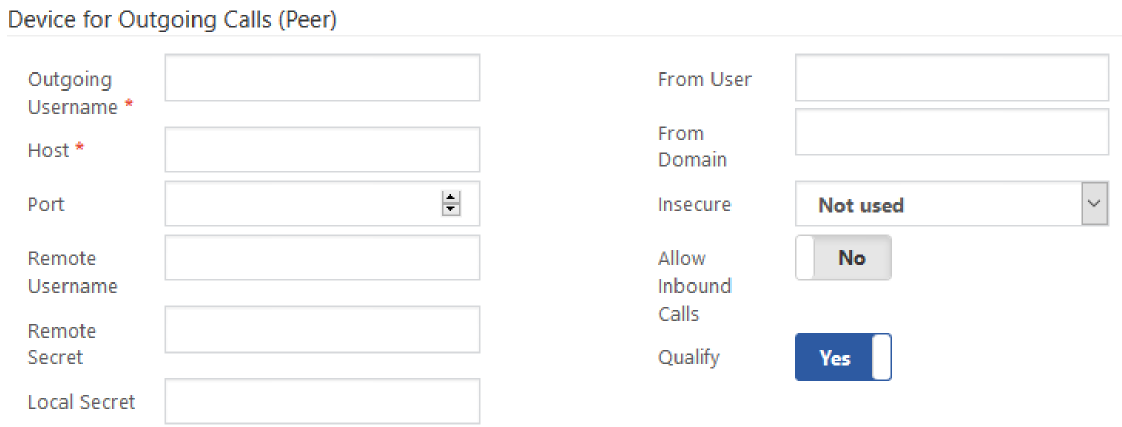
Trunk CID, sets the default caller ID name and number that will be displayed to the called party. The Trunk CID will only be used if **Overwrite CID** field is set to **Yes.** Note that setting the outbound caller ID only works on digital lines (T1/E1/J1/PRI/BRI/SIP/IAX2), not POTS lines. The ability to set outbound caller ID must also be supported by your provider.

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

Overwrite CID, determines whether to overwrite the caller number (CID) with the ID associated with the trunk.

SIP Option

Device for Outgoing Settings (Peer) Section



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

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

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

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

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

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

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

From Domain, as your provider knows your domain

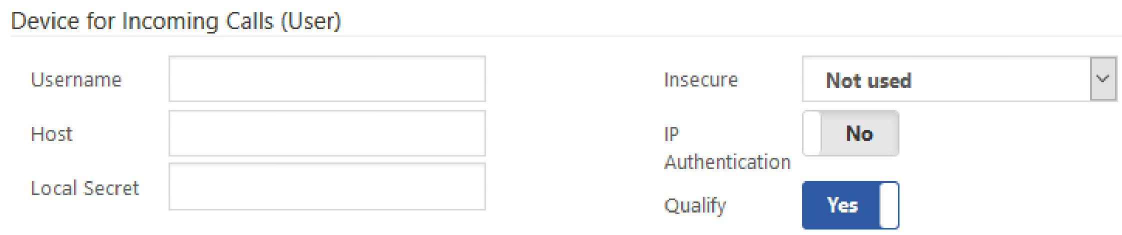
Insecure, Sets the level of authentication and verification established between machines when performing communication. Options are:

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

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

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

Device for Incoming Calls (User) Section



Username, the username credential used to contact this trunk

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

Local Secret, the password credential uses to contact this trunk

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

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

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

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

Register String Section

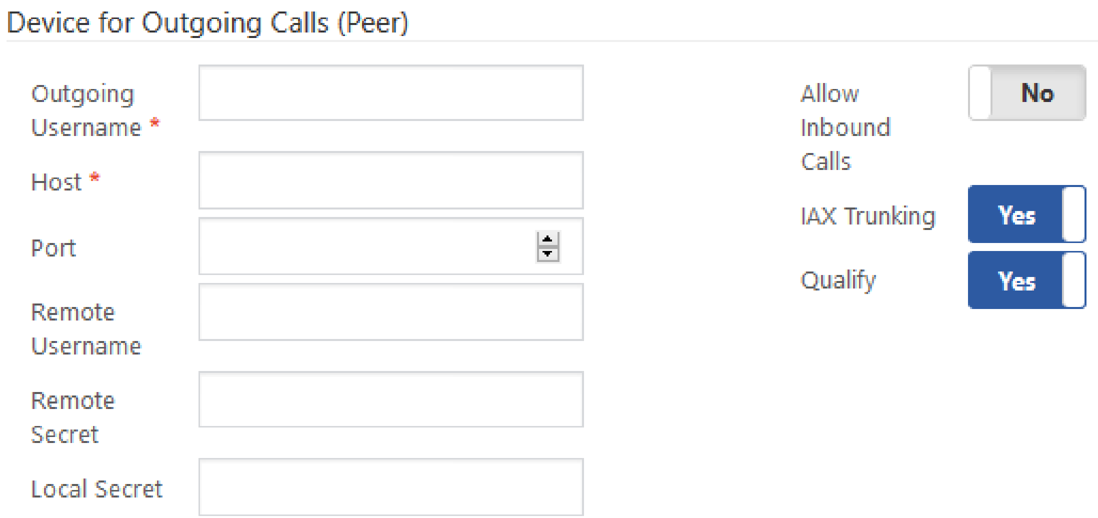
Register String, the register line includes a host name (mydomain.com) which tells Asterisk where to send the registration request; the account number and password.

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

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

IAX2 Option

Device for Outgoing Calls (Peer) Section



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

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

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

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

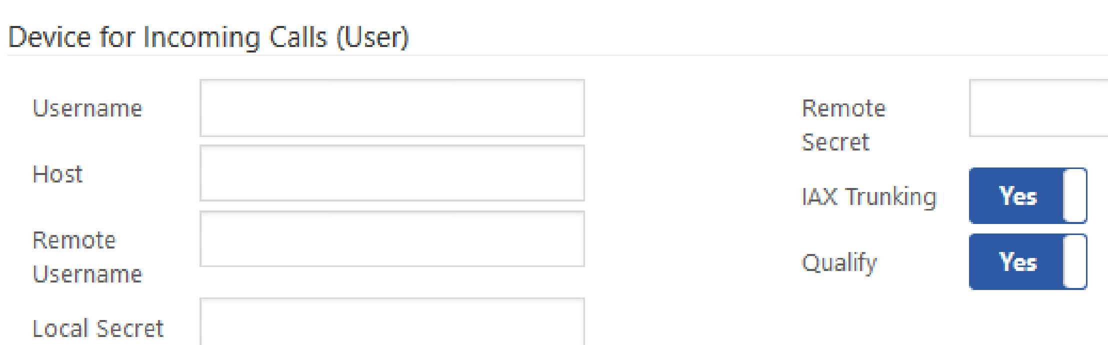
Remote Secret, the password credential used to authenticate this trunk against the provider.

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

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

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

Device for Incoming Calls (User) Section



Username, the username credential used to contact this trunk

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

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

Local Secret, the password credential uses to contact this trunk

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

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

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

Register String Section

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

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

Telephony Option

DAHDi Trunk Parameters

Channel Group, choose the channel or span for this trunk.

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

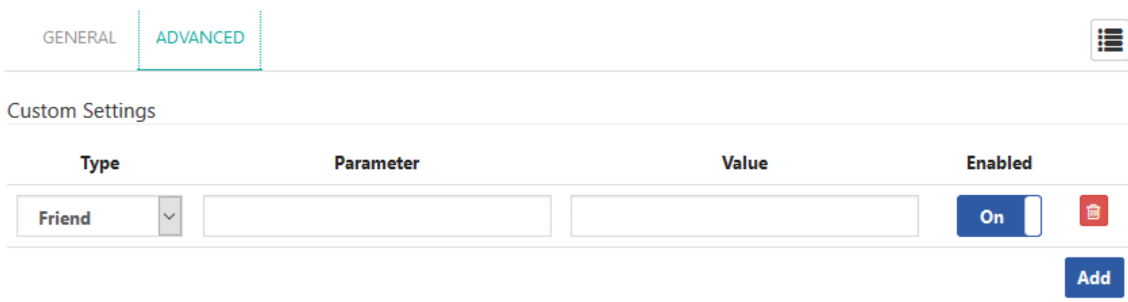
- **Linear in Ascending Order** - selects the lowest-numbered available channel. Can be referred to as ascending sequential hunt group
- **Linear in Descending Order** - selects the highest-numbered available channel. Can be referred to as descending sequential hunt group
- **Round-Robin in Ascending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

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

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,

ADVANCED Tab



Custom Settings Section

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

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

Type, Friend, User or Peer.

Parameter, any valid variable of Asterisk.

Value, any value for the Asterisk variable.

Enabled, enable or disable the custom settings.

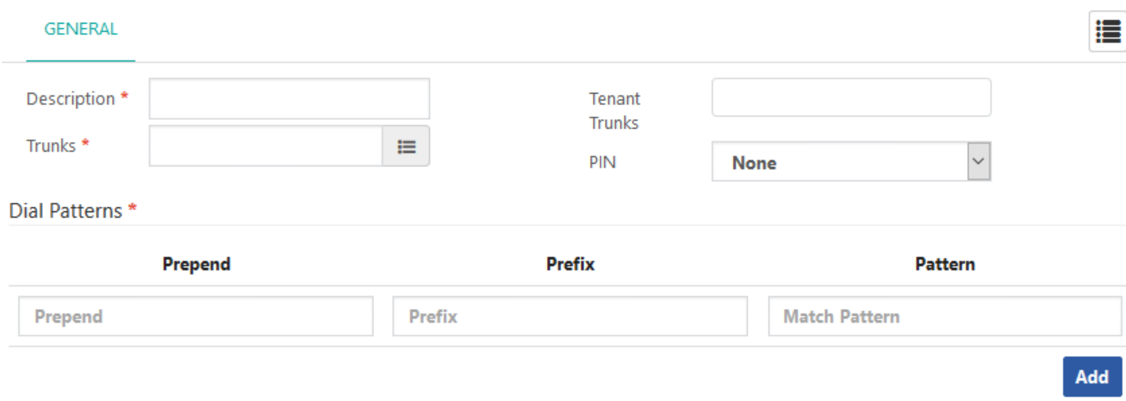
Outbound Routes Dialog

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

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

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

GENERAL Tab



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

Trunks*, list of trunks that can be used by the route.

Tenant Trunks, list of tenants that this tenant can call as trunk.

PIN, list of PINs, using previously created password sets (if any), to authenticate access to this route. Lists of PINs can be configured in the **PIN** dialog.

Dial Patterns Section

Prepend, digits to add to a successful match.

Prefix, prefix to remove from a successful match.

Pattern, Pattern matching allows us to create patterns in the dial plan that match more than one possible dialed number. Pattern matching options are:

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

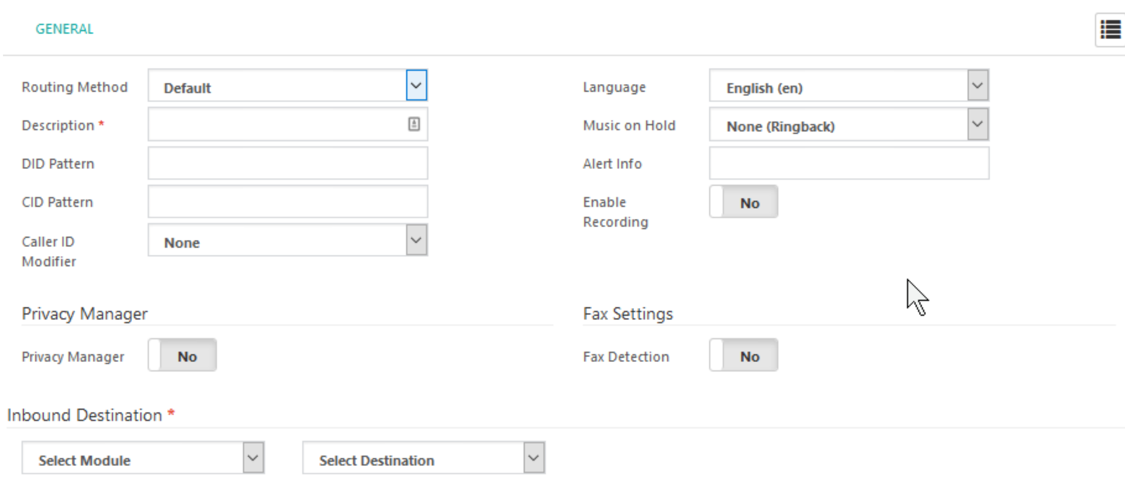
Be sure that the outbound routes you create allow you to call the following types of calls:

- **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.

Inbound Routes Dialog

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

GENERAL Tab



Routing Method, can either be the DAHDI channel for an analog port (FXO), or default for all other inbound routes.

Description*, short description to identify this DID. This field is used to hold a description to help you remember what this particular inbound route is for. This field is not parsed by the system.

DID Pattern, expected number or pattern. This field is used when DID-based routing is desired. The phone number of the DID to be matched should be entered in this field. The DID number *must* match the format in which the provider is sending the DID. Many providers will send the DID information with the call as +15555555555, while others will leave out the country code information and simply send 5555555555. If the DID entered in this field does not exactly match the number sent by the provider, then the inbound route will not be used. This field can be left blank to match calls from all DIDs (this will also match calls that have no DID information).

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

CID Pattern, CID number or CID pattern to match. This can be used when CID-based routing is preferred. As with the DID Number field, the CID entered in this field must exactly match the format in which the provider is sending the CID. Providers may send 7, 10, or 11 digits; they may include a country code and the plus symbol. Check with your provider to see the format in which the CID is sent, in order to ensure that this field is entered correctly.

The Caller ID Number field can be left blank to match with 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.

Caller ID Modifier, allows you to use a rule (that can be defined in the CID Modifiers dialog) that will be used to modify incoming CID numbers and names. Leave this field blank if you do not want to modify incoming CID data.

CID Number, CID number or CID pattern to match. This can be used when CID-based routing is preferred. As with the DID Number field, the CID entered in this field must exactly match the format in which the provider is sending the CID. Providers may send 7, 10, or 11 digits; they may include a country code and the plus symbol. Check with your provider to see the format in which the CID is sent, in order to ensure that this field is entered correctly.

The Caller ID Number field can be left blank to match with 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.

CID name prefix, can be used to add a prefix to CallerID name. This allows user-defined text to be prepended to the caller ID name information from the call. This is often used to identify where a call comes from. For example, calls to a number dedicated for technical support might be prefixed with "Support".

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

Music On Hold, this drop-down menu allows you to select the music-on-hold class for this route. Whenever a caller accessing this route is placed on hold, they will hear the music on hold defined in the class selected here. This is often used for companies that use their music on hold to advertise services, or that accept calls in multiple different languages. Calls to a French DID might play a music-on-hold class with French advertisements, while an English DID would play a class with English advertisements.

Alert Info, to set a distinctive ring for this inbound route. There does not yet seem to be a standard for how to tell a SIP phone that you want it to ring with a distinctive ring. On SIP handsets that do support distinctive ringing, the exact method of specifying distinctive ring varies from one model to another. In many cases this is done by sending a SIP_ALERT_INFO header, but the usage of this header is not consistent. This is often used for SIP endpoints that can ring differently, or auto-answer calls based on the SIP_ALERT_INFO text that is received. Any inbound call that matches this route will send the text in this field to any SIP device that receives the call.

Enable Recording, enable call recording on this route.

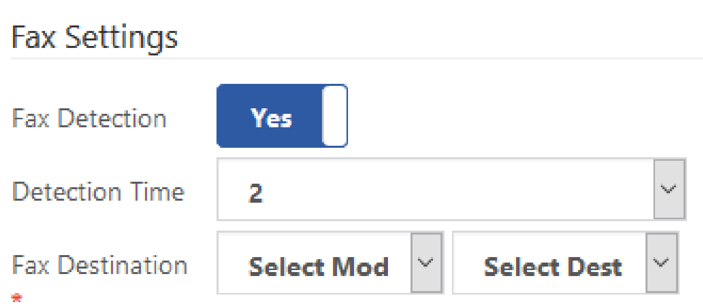
Privacy Manager Section

Privacy Manager, this drop-down menu is used to enable or disable the the system privacy manager functionality. When enabled, incoming calls that arrive without an associated caller ID number will be prompted to enter their telephone number. Callers will be given a number of attempts (as defined in the Max attempts field, below) to enter this information before their call is disconnected.

Max attempts, defines the number of attempts the caller has to enter a valid CallerID. This field is only required if Privacy Manager is enabled.

Min Length, minimum number of digits that the caller must provide when entering their CallerID number. This field is only required if Privacy Manager is enabled.

Fax Settings Section



Fax Detection, determines whether faxes should be detected on this route. If fax detection is enabled, additional parameters can be configured and a drop-down will appear which is used to select the extension to which the inbound faxes will be directed. Typically, this extension is a DAHDI extension that has a physical fax machine plugged into it. However, it may also be a virtual extension that will be answered by the system. The program will accept faxes and turn them into digital documents for review.

If fax detection is disabled, fax detection will not be used for calls on this route. Any fax calls will be handled just like voice calls.

Detection Time, determines how many seconds to wait before ringing the extension. This time enables the inbound route to listen for fax tones and determine whether the incoming call is a fax, 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 5 seconds.

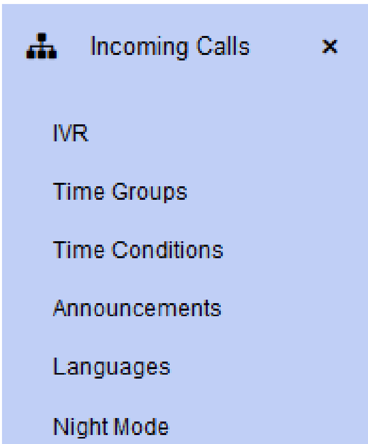
Fax Destination, determines where incoming faxes will be sent. This can be any user extension that has been configured with an email address.

Destination Section*

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

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

Incoming Calls Menu Group



IVR Dialog

IVR (Interactive Voice Response) allows you configure an auto attendant to answer calls and redirect the call in response to input from the caller. An IVR system is often referred to as a digital receptionist. An IVR plays a pre-recorded message to the caller that asks them to press various buttons on their telephone depending on which department or person they would like to speak with. The IVR system will then route the call accordingly.

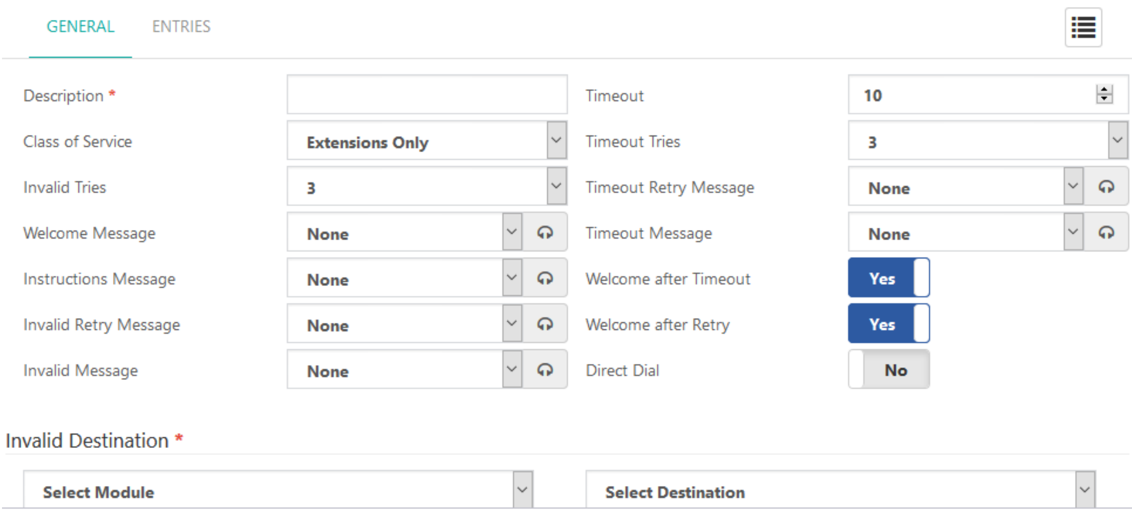
The system's IVR allows any digits to be defined for routing purposes. For example, pressing "1" could route the caller to the sales ring group. Destinations can be defined to receive the call if the IVR times out, or does not receive valid input.

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

- Handling the timeout when there is no input from the caller
- Controlling the action to take if caller provides invalid user input
- Allowing the caller to backtrack if s/he has made a mistake or gets lost
- Allowing the caller to return to the IVR if voicemail is encountered
- Provide an option that allows the caller to reach a human operator
- Whether or not to take advantage of time-based branching, by defining Time Groups, for normal office hours, that include start and end times, start and end days of the week, and much more
- Defining a Time Condition, and setting one destination if the time matches and a different destination if the time does not match
- You can avoid the use of the word **dial** when you record announcements. People today use phones with either push-buttons or touch screens, so it is preferable to say **press**.
- You can improve the usability of the IVR announcements by telling the user about the service or destination before you tell them which number to press.

- You should not more that about 4 or 5 entries in any level of the IVR, otherwise it makes it too complicated for the caller

GENERAL Tab



Description*, short description to identify this IVR. This field is not parsed by the system.

CoS Name, choose a Class of Service for this IVR.

Invalid Tries, number of invalid attempts allowed.

Language, this option specifies the language of the prompts to be used for this IVR.

Welcome Message, welcome message, selected from a drop-down menu of pre-recorded messages, that will be played to the caller when they enter the IVR. The welcome message will only be played when the caller first enters the IVR: it will always be followed by the instructions message.

Instructions Message, instruction message, selected from a drop-down menu of pre-recorded messages, that will be played to the caller each time that they return to the IVR menu. The welcome message will not be repeated when the callers returns to the IVR menu.

Invalid Retry Message, message, selected from a drop-down menu of pre-recorded messages, to be played when the IVR receives an invalid option.

Invalid Message, message, selected from a drop-down menu of pre-recorded messages, to be played when user exceeds the maximum number of attempts.

Timeout, is the maximum time, in seconds, that the system will wait for input from the caller. If this time passes without input, the call will fail over to the Timeout Destination that the user has defined.

Timeout Tries, is used to determine the number of times the IVR will repeat itself when no valid input is received. After the specified number of tries, the caller will be send to the Timeout Destination. The maximum number of loops allowed is five.

Timeout Retry Message, message, selected from a drop-down menu of pre-recorded messages, to be played when input has not been received within the period defined by Timeout. If the number of Timeout Tries has not yet been reached, then the user will be prompted to try again.

Timeout Message, message selected from a drop-down menu of pre-recorded messages, to be played when reaching the timeout.

Message on Timeout, when enabled, will return the user to the main IVR Welcome Message after playing the Timeout Retry Message.

Message on Invalid, when enabled, will return the user to the main IVR Welcome Message after playing the Invalid Retry Message.

Direct Dial, enables the caller to call an extension directly from the IVR. If this option is not enabled, the caller will receive a message that they have provided invalid input when they enter an extension, *even if the extension is valid*.

Invalid Destination Section*

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

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

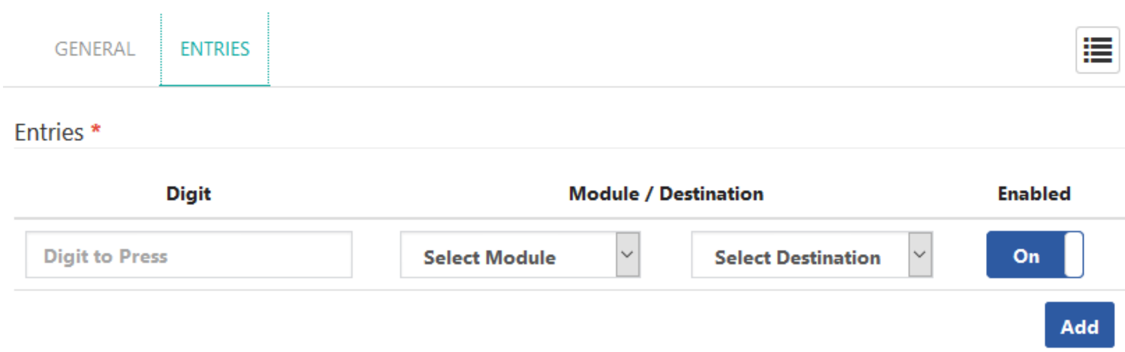
Timeout Destination Section*

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

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

IVR ENTRIES Tab

This tab defines how to handle the user's input.



Entries Section*

Digit, digit to press.

Module, dialog to activate when the caller presses the appropriate digit.

Destination, destination to call when the caller presses the appropriate digit.

Enabled, enabled or disable this option.

It is good practice to ensure that the user has an easy way of getting back to the previous menu. One simple way to do this would be to allow the user to press "*" and link that keypress to the parent IVR.

Time Groups & Time Conditions

Time conditions are a set of rules for hours, dates, or days of the week. A condition has two call targets each time. Calls sent to a time condition will be sent to one target if the time of the call matches one of the conditions, or to the other target if none of the conditions match.

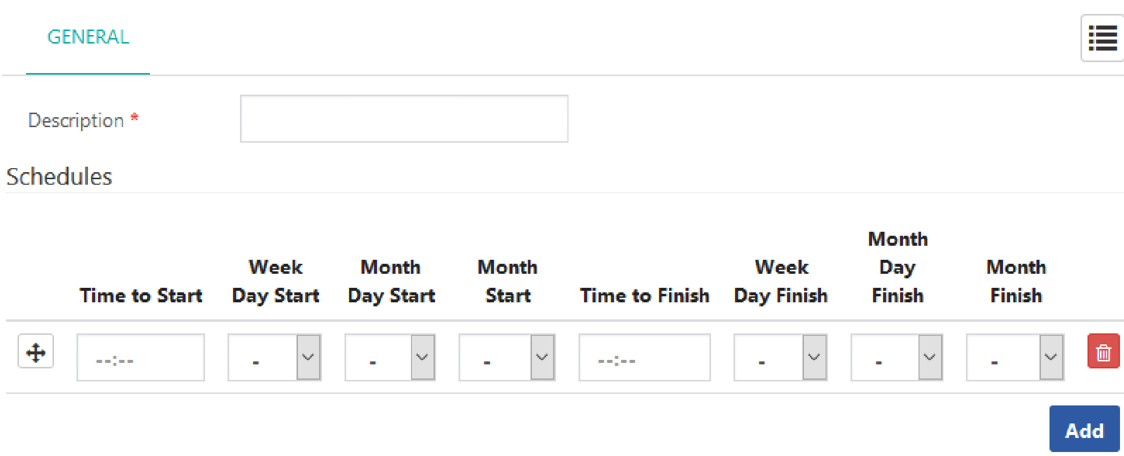
Each time condition can use multiple time definitions (known as time groups). Time conditions are often used to control how a phone system responds to callers inside and outside of business hours, and during holidays.

Before we can set up a time condition call target, we need to define a set of time groups. Time groups are a list of rules against which incoming calls are checked. The rules specify a specific date or time, and a call can be routed differently if the time it comes in matches with one of the rules in a time group.

Each time group can have an unlimited number of rules defined. It is useful to group similar sets of time rules together. For example, there may be one time group for business hours in which the time that the business will be open will be defined. Another popular time group is for holidays, in which each holiday that falls on a business day is defined.

Time Groups Dialog

GENERAL Tab



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

Schedules Section

Time to Start, time, in hours and minutes, that the time group should start.

Time to finish, time, in hours and minutes, that the time group should end.

Week Day Start, day of the week that the time group should start.

Week Day Finish, day of the week that the time group should end.

Month Day Start, day of the month that the time group should start.

Month Day Finish, day of the month that the time group should end.

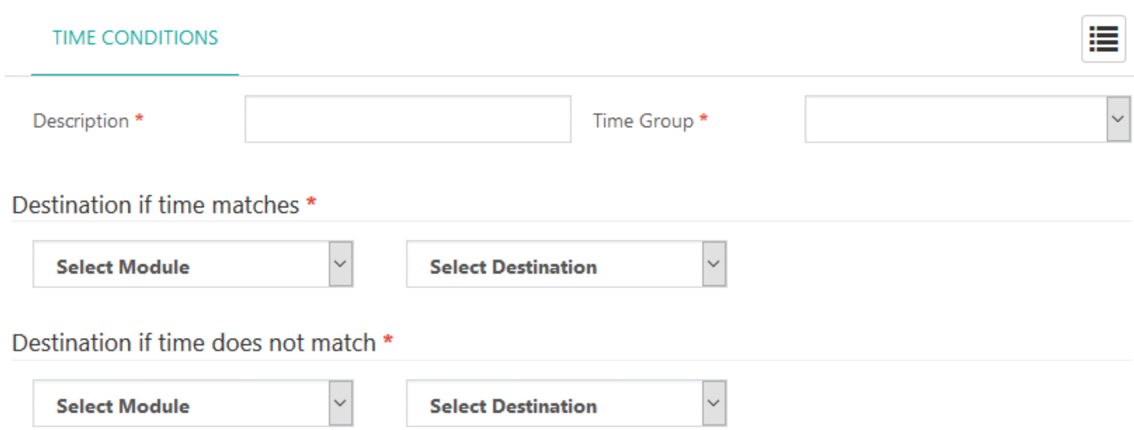
Month Start, month of the year that the time group should start.

Month Finish, month of the year that the time group should end.

Time Conditions Dialog

Once a time group has been defined, a time condition can be set up as a call target.

GENERAL Tab



Description*, short Description to identify this Time Condition.

Time Group*, select a Time Group, from the drop-down list, that was created in the Time Groups dialog.

Destination if Time Matches Section

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

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

Destination if Time does not Match Section

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

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

Announcements Dialog

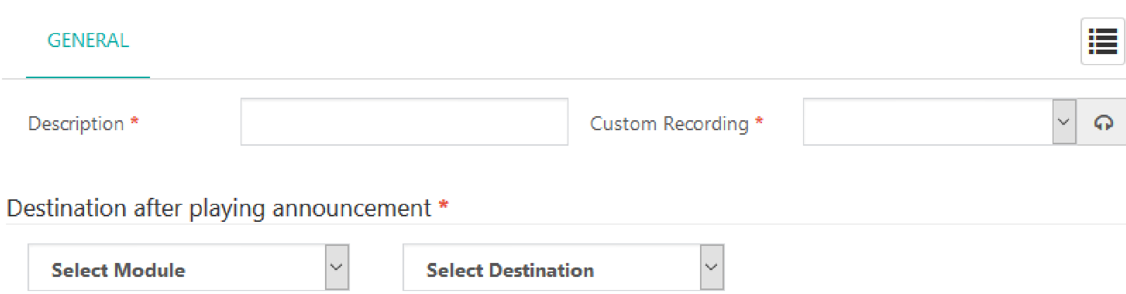
This dialog is used for when you want the caller to hear a message**,** before being automatically transferred to a fixed destination.

There are two steps that you should follow before using this dialog.

1. You need to make a recording that contains the message that you want callers to hear. This is done by dialing feature code *92 (Custom Recording) from any phone on the system. After dialing *92, follow the verbal instructions to record your message.
2. After successfully making a custom recording, navigate to the Recordings Management dialog (Settings>PBX Settings>Recordings Management). The recording that you have just made will appear with a name that is based on the timestamp when the recording was made. The format starts with a representation of the date when the recording was made, formatted as YYYYMMDD followed by the number of the extension from which the recording was made. You can click on the edit icon for the recording, and give it a more meaningful name.

Now you are ready to use the Announcements dialog.

GENERAL Tab



Description*, short description to identify this Announcement.

Custom Recording, select a recording, from the drop-down list**,** to play in this Announcement.

Destination after playing announcement Section*

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

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

Languages Dialog

This dialog is used for when you want to change the language of the prompts that are used in the course of a call, such as when an IVR is used and the user selects a language.

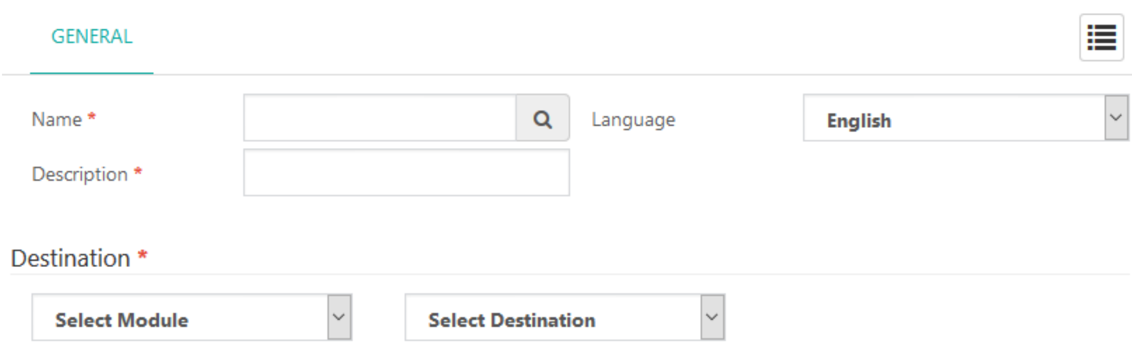
Provided that a rpm of prompts is available, you can install additional languages. You can also change the default for English, to another variant of English, such as en_US, en_UK, en_AU, etc.

For example, if you want to use Australian as your default language, you could run the command **yum install asterisk-sounds-core-en-au-ulaw**. This will create appropriate symbolic links, using the Linux ‘alternative’ system, which allows you to configure the default command in the system. For example, if you have several versions of English prompts installed, then the 'alternatives' allows you to define which version of English should be treated as the default.

In case of EasyVOIZ, 'alternatives' allows you to install several variants of a language and select which one of them should be the default. For example, it is possible to install en_US, en_UK, en_AU etc. Then one of them can be defined as the default English version.

You can use the 'man update-alternatives' command in the Linux command line interface for further information.

GENERAL Tab



Name*, short name**,** must be unique.

Description, short description to identify this language.

Language, channel language to use from drop-down list.

Destination Section

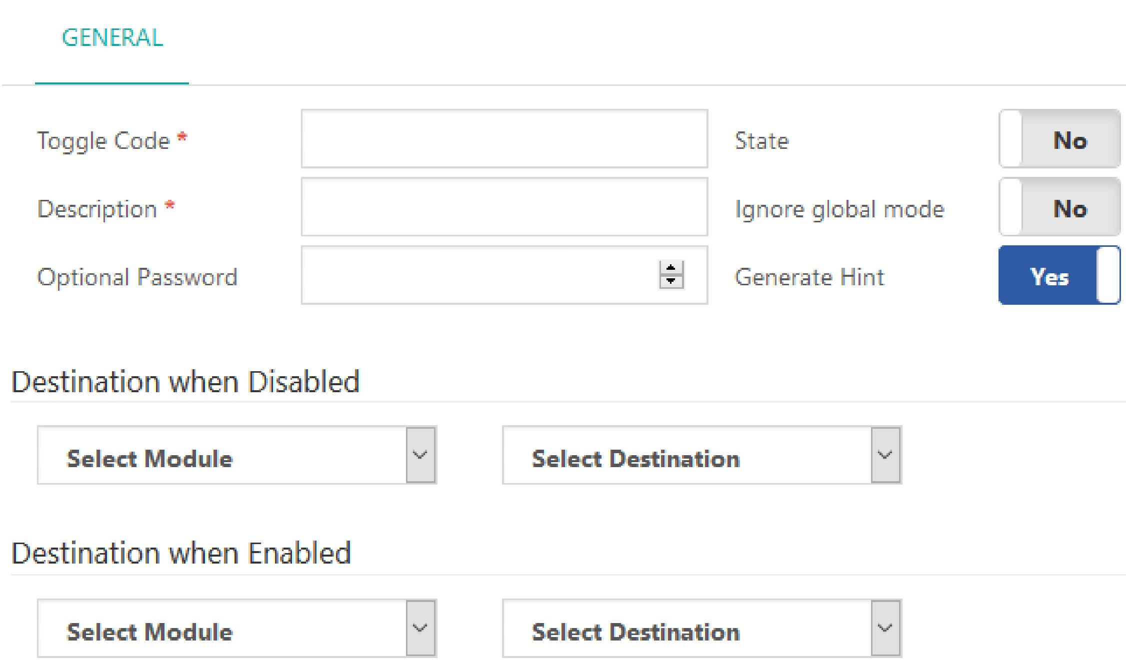
Select Module, allows the user to choose from a drop-down list of available dialogs**,** which dialog should be activated.

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

Night Mode Dialog

Night mode is used to change the conditions of an incoming route depending on whether he is active or not.

GENERAL Tab



Toggle Code*, code index to determine the order of multiple night modes

Description, short description to identify this Night Mode

Ignore global mode,

Optional Password, optional password to protect this Night Mode

State, indicates whether this Night Mode is currently active.

Destination when Disabled Section*

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

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

Destination when Enabled Section*

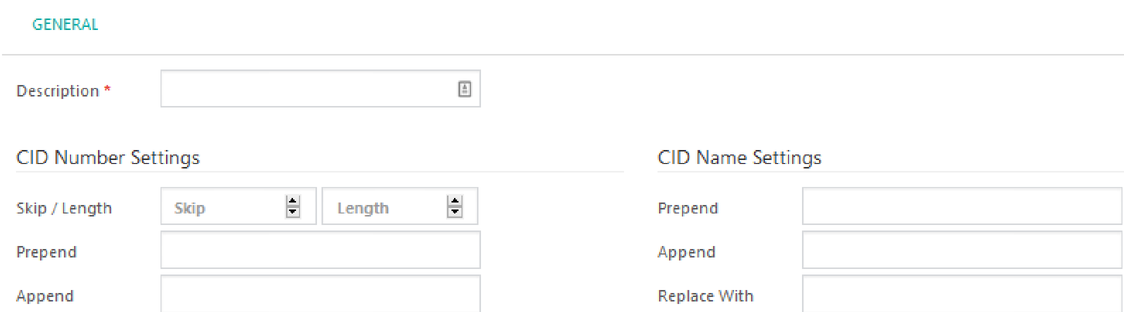
Select Module, allows the user to choose from a drop-down list of available dialogs**,** which dialog should be activated.

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

CID Modifiers

Allows you to manipulate the digits of Caller ID for incoming calls.

GENERAL Tab



Description

CID Number Settings Section

Skip / Length, allows you to modify an incoming CID number by starting the manipulation some number of digits either from the beginning or end of the CID number, while retaining any number of the remaining digits.

This definition consists of two parts:

- **Skip** defines where to start modifying the incoming CID number. If the skip value has a positive value of x, the leading x digits will be skipped, and the modified CID number will start after x digits. If the skip value has a negative value of x, the modified CID number will start x digits before the end of incoming CID number.
- **Length** determines how many digits the modified CID number will consist of. If the length is zero, all the digits after the start position will be used. You can define a negative length of x in order to discard the x trailing digits.

Examples of manipulation on an incoming CID number of 123456789:

- Skip value of 3, length value of 5, creates a modified CID number of 45678
- Skip value of 3, length value of 0, creates a modified CID number of 456789
- Skip value of -6, length value of 3, creates a modified CID number of 456
- Skip value of -6, length value of -2, creates a modified CID number of 4567

Prepend, allows you define digits that will always be added in front of the incoming CID number.

Append, allows you define digits that will always be added at the end of the incoming CID number.

CID Name Settings Section

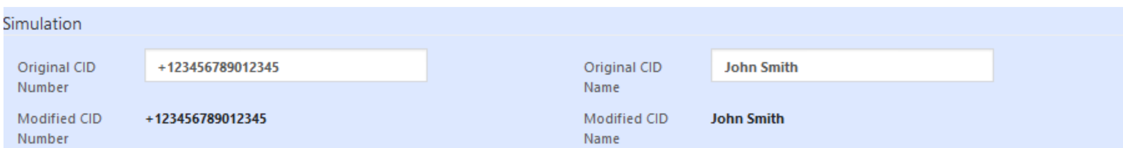
Prepend, allows you define text that will always be added in front of the incoming CID name.

Append, allows you define text that will always be added at the end of the incoming CID name.

Replace With, allows you to completely replace the incoming CID name with fixed text.

Simulation Section

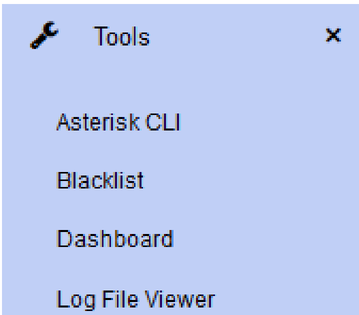
This section allows you to see how your settings will affect incoming CID number and names.



The **Modified CID Number** field will display how the digits that you enter in the **Original CID Number** field will be displayed based on the rules that you define in CID Number Settings section.

In a similar manner, the **Modified CID Name** field will display how the name that you enter in the **Original CID Name** field will be displayed based on the rules that you define in CID Name Settings section.

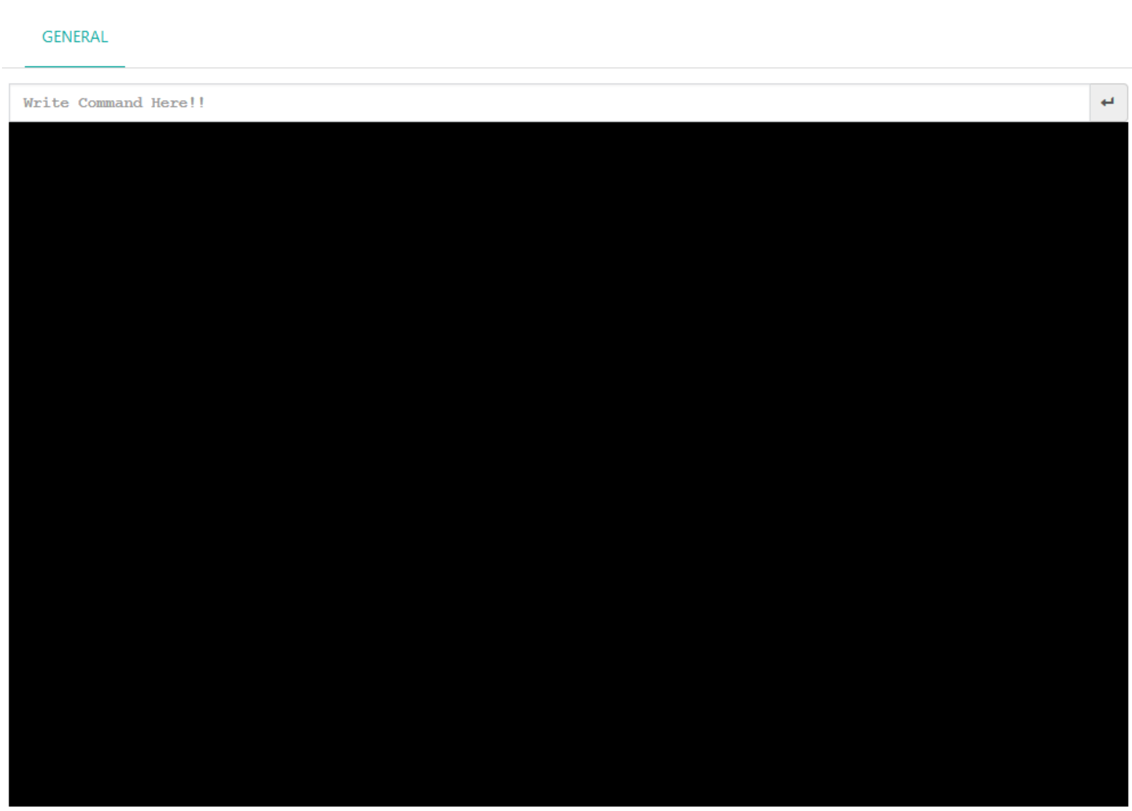
Tools Menu Group



Asterisk CLI Dialog

GENERAL Tab

From this tab you are able to access the CLI Interface.



In this dialog, you can type any valid Asterisk command. As soon as you start typing, a drop-down list of available Asterisk commands will be displayed.

Black List Dialog

Creates a list of external CID 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.

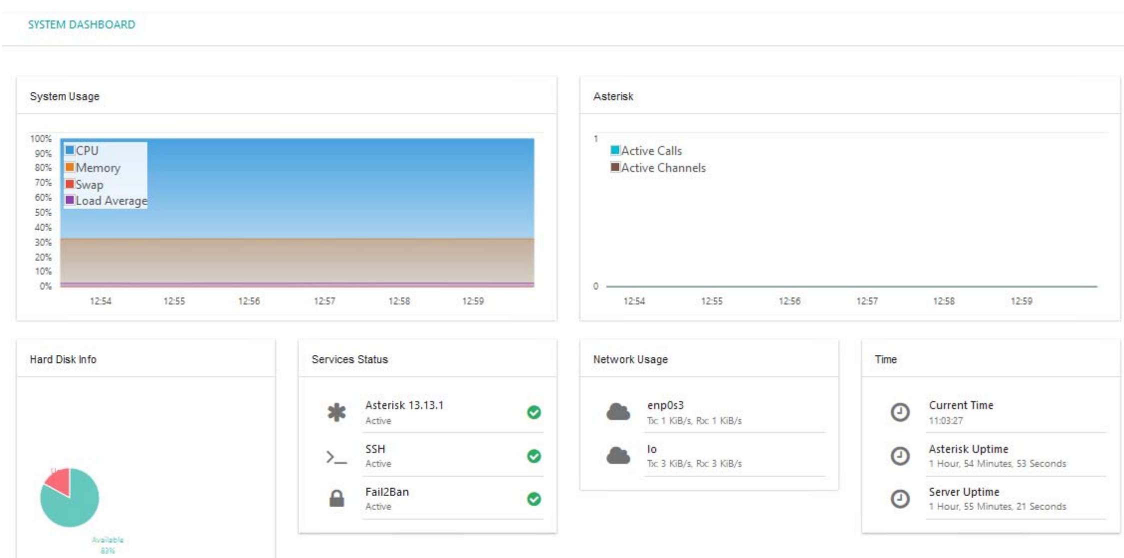
GENERAL Tab

CID Number, the number that you want to blacklist.

Description, a free-text description of the number that you want to blacklist.

Dashboard Dialog

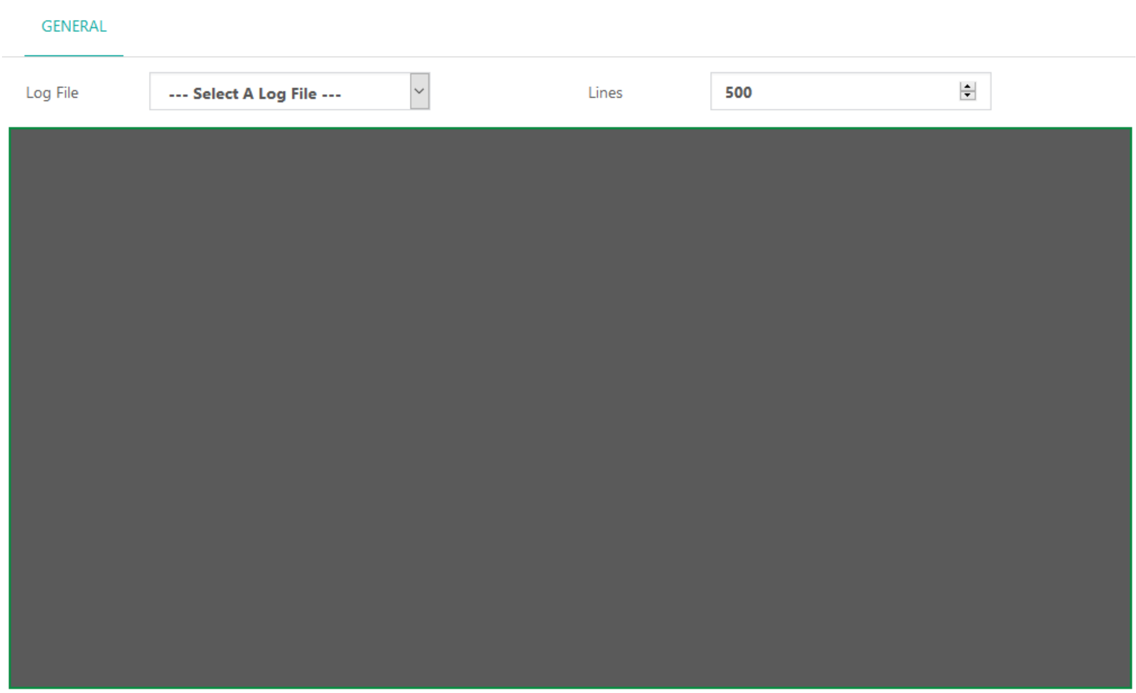
In the System Dashboard dialog you will find the Dashboard.



Log File Viewer Dialog

GENERAL Tab

In this tab you will find a tool to view log files.



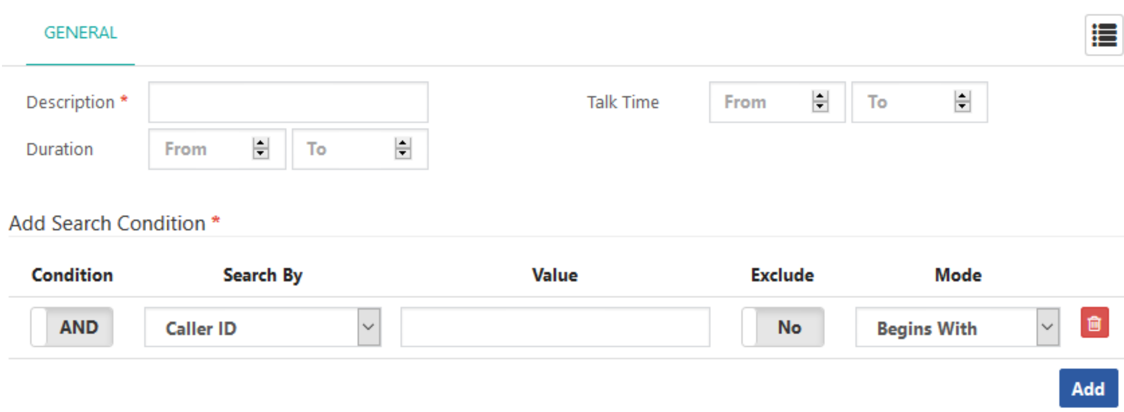
Log File, select the log file that you want to see.
Lines, how many lines to read from the tail of the log file.

3. Reports Menu Set

CDR Reports Menu Group

CDR Filters Dialog

GENERAL Tab



Description*, short description for this filter.

Duration, total duration of calls.

Talk Time, talk time of calls.

Add Search Condition Section

Pressing on the Add button allows you add additional search conditions.

Condition, determines whether the condition is enabled or not.

Search By, search for the selected field using one of the items selected from the drop-down list:

- Caller ID
- Source

- Destination
- Account Code
- Customer Code
- Status

Value, value of the selected field.

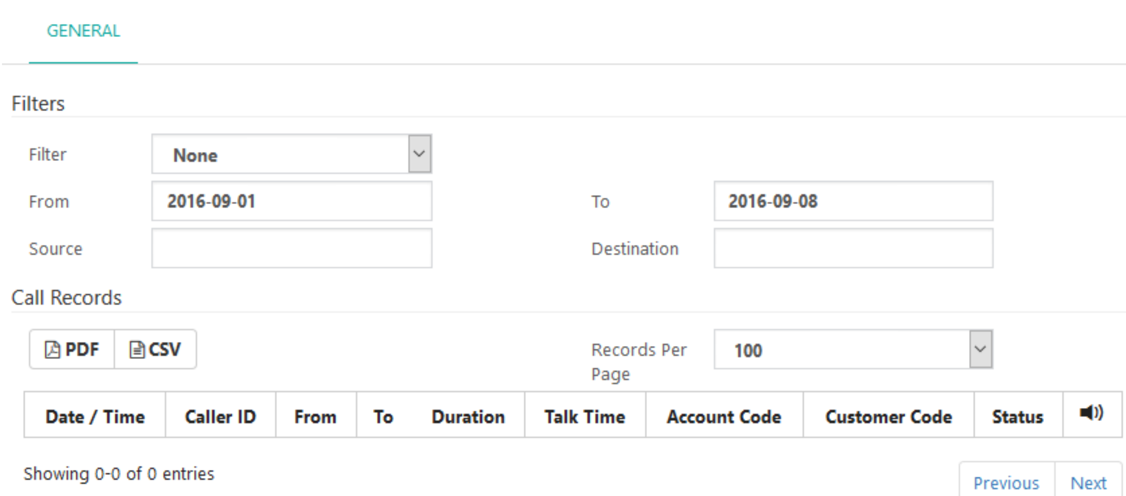
Exclude, include or exclude the selected value in the search.

Mode, search condition can be filtered in a number of methods, which can be selected from the drop-down list:

- Begins With
- Contains
- Ends With
- Exactly

CDR Dialog

GENERAL Tab



Filters Section

Filter, name of a previously-defined filter to use in this report.

From, include records starting from this date.

Source, source of calls

To, include records ending by this date.

Destination, destination of calls.

Call Records Section

PDF / CSV, click either one of these icons to export the CDR report in either PDF of CSV format.

Records Per Page, set the number of records that should be displayed on each page.

PBX Reports Menu Group

Status Dialog

Use this dialog to see the status of the system

Channels Tab

Displays a detailed list of calls in progress, together with a summary of active calls and active channels.

You can click on the **Refresh** button to update the displayed data with current real-time data.

CHANNELS REGISTRATIONS PEERS HINTS VOICEMAIL QUEUES

Channel	Caller ID	Called Number	State	Duration
SIP/3989-00000504	"Ariel" <2989>	2970	Up	00:00:32
SIP/2970-00000505	"Eran" <2970>		Up	00:00:31
SIP/2941-00000506	"Keith" <2941>	s	Up	00:00:02

Summary

Active Calls	Active Channels
1	3

Registrations Tab

Displays a detailed list of both SIP and IAX registrations.

You can click on the **Refresh** button to update the displayed data with current real-time data.

CHANNELS REGISTRATIONS PEERS HINTS VOICEMAIL QUEUES

SIP Registrations

Host	Username	State	Registration Time
127.0.0.1	loopback	No Authentication	0

IAX Registrations

Host	Username	State

Peers Tab

Displays a detailed list of SIP and IAX2 peers.

You can click on the **Refresh** button to update the displayed data with current real-time data.

CHANNELS REGISTRATIONS PEERS HINTS VOICEMAIL QUEUES

SIP Peers

Type	Username	Host	Port	Dynamic	RPORT	Comedia	ACL	Status	Description
peer	3098		0	1	no	no	1	UNKNOWN	Hot Device User 3098
peer	SIP100		0	1	no	no	1	UNKNOWN	SIP Phone 100
peer	SIP101		0	1	no	no	1	UNKNOWN	SIP Phone 101
peer	SIP102		0	1	no	no	1	UNKNOWN	SIP Phone 102
peer	SIP103		0	1	no	no	1	UNKNOWN	SIP Phone 103

Hints Tab

Displays a detailed list of hints active in the system.

You can click on the **Refresh** button to update the displayed data with current real-time data.

CHANNELS REGISTRATIONS PEERS HINTS VOICEMAIL QUEUES

Extension	Context	Hint	Status
QAP_2244_9399	cos-all-queue-hint	Custom:QAP_2244_9399	0
2238	cos-all-hint	SIP/SIP285&Custom:DND_2238	4
2239	cos-all-hint	SIP/SIP286&Custom:DND_2239	4
2199	cos-all-hint	SIP/SIP246&Custom:DND_2199	4
2198	cos-all-hint	SIP/SIP245&Custom:DND_2198	4

Voicemail Tab

Displays a detailed list of voicemail mailboxes in the system, and their current status.

You can click on the **Refresh** button to update the displayed data with current real-time data.

CHANNELS REGISTRATIONS PEERS HINTS VOICEMAIL QUEUES

Context	Mailbox	User	New Messages
ombutel-voicemail	2001	Susan Dorrance	0
ombutel-voicemail	2002	Kaitlyn Difilippo	0
ombutel-voicemail	2003	Linwood Knaus	0
ombutel-voicemail	2004	Gracie Heffley	0
ombutel-voicemail	2005	Neta Doxey	0

Queues Tab

Displays a list of calls to available queues in the system, as well as members of the queues.

You can click on the **Refresh** button to update the displayed data with current real-time data.

CHANNELS REGISTRATIONS PEERS HINTS VOICEMAIL QUEUES

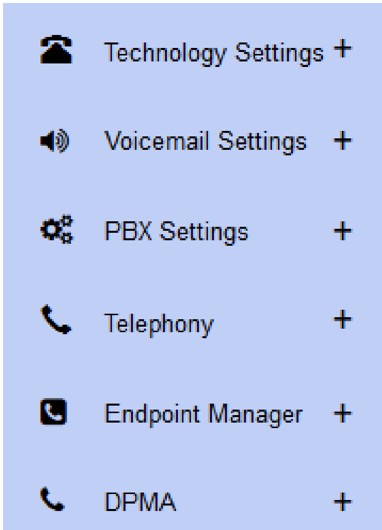
Queue: Q8010

Calls	Max	Strategy	Holdtime	Talktime	Weight	Completed	Abandoned
0	Unlimited	ringall	0	12	0	2	1

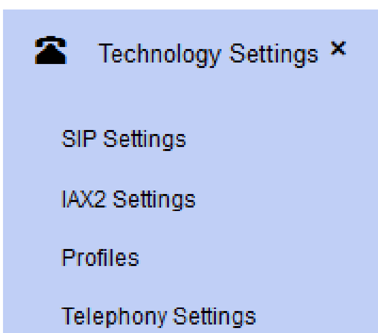
Members

Name	Location	Membership	Incall	Paused
2911	Local/2911@cos-all	static	0	0
2974	Local/2974@cos-all	static	0	0

4. Settings Menu Set



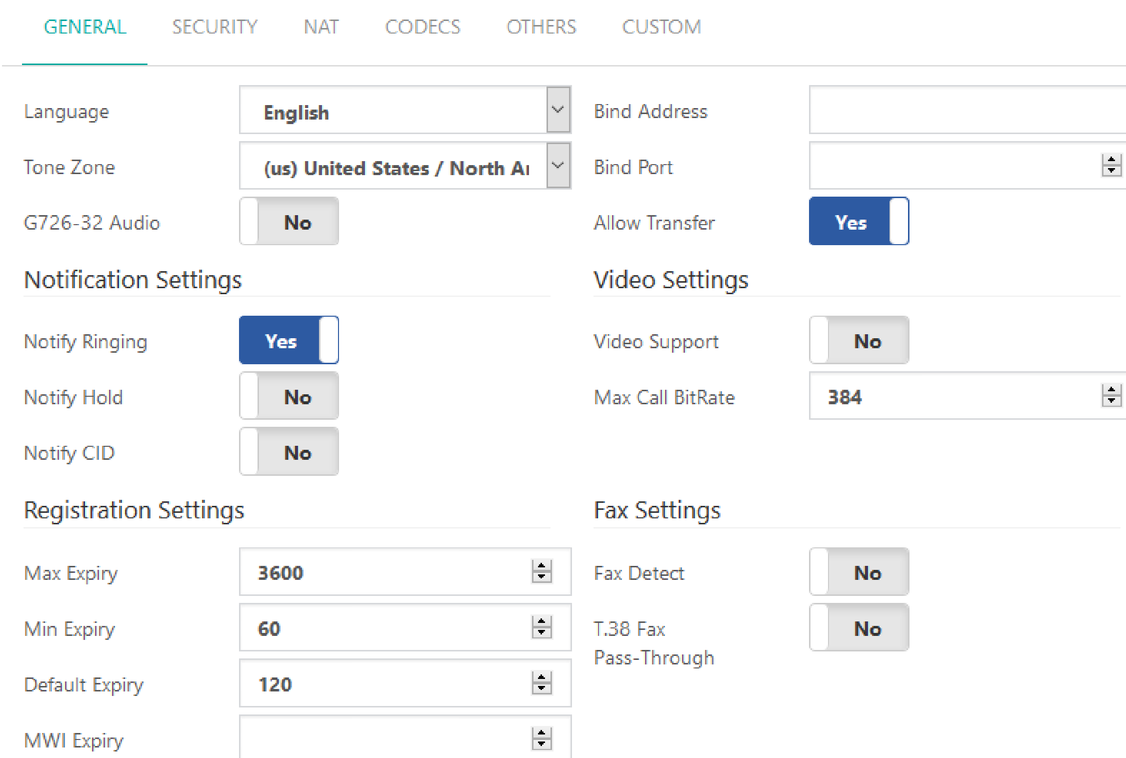
Technology Settings Menu Group



SIP Settings Dialog

The SIP Settings is used to configure the default value to be used for SIP calls.

GENERAL Tab



Language, default language setting for all users/peers. This may also be set for individual users/peers.

Tone Zone, default tone zone for all users/peers.

Call Counter, enable call counters on devices.

Bind Address, IP address to which the device should bind. Note that 0.0.0.0 binds to all IPv4 addresses, or :: for all IPv6 addresses.

Bind Port, port to which the device should bind. The standard SIP port is 5060.

Allow Transfer, disables all transfers (unless specifically enabled in peers or users). Default setting is enabled. Note that the dial options 't' and 'T' are not related as to whether SIP transfers are allowed or not.

G726-32 Audio, if the peer negotiates G726-32 audio, use AAL2 packing order instead of RFC3551 packing order (this is required for Sipura and Grandstream ATAs, among others).

Notification Settings Section

Notify Ringing, controls whether busy subscribers get sent a RINGING message when another call is sent.

Notify Hold, notify subscribers that are in HOLD state.

Notify CID, controls whether caller ID information is sent together with dialog-info+xml notifications (supported by Snom phones).

Video Section

Video Support, turns on or off support for SIP video. You need to turn this on to get any video support at all.

Max Call Bitrate, maximum bitrate for video calls (default 384 kb/s)

Registration Settings Section

Max Expiry, maximum allowed time, in seconds, for incoming registrations.

Min Expiry, minimum time, in seconds, for registrations.

Default Expiry, default length of incoming/outgoing registration.

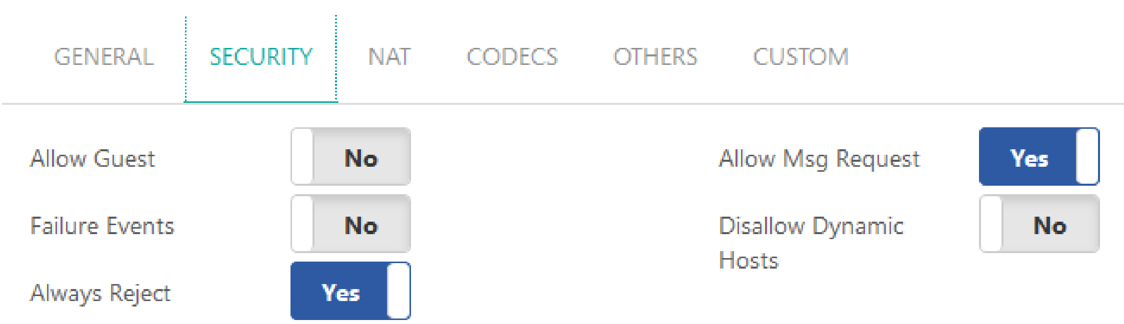
MWI Expiry, expiry time for outgoing MWI subscriptions.

Fax Settings Section

Fax Detect, When active, enables (both CNG and T.38) detection of inbound faxes.

T.38 Fax Pass-Through, enables T.38 with FEC error correction. Overrides the other values provided for the endpoint, so we can send 400 byte T.38 FAX packets to it.

SECURITY Tab



Allow Guest, allow or reject guest calls.

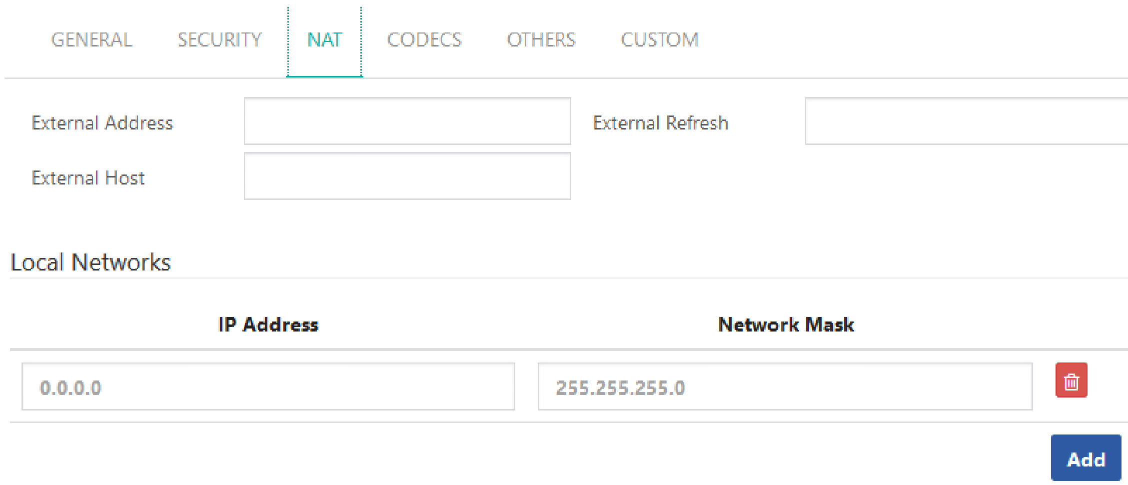
Failure Events, generate manager peer-status events when peer cannot authenticate with Asterisk. Peer-status will be rejected.

Always Reject, when rejecting an incoming INVITE or REGISTER call, for any reason, always reject with an identical response. This reduces the ability of an attacker to scan for valid SIP usernames.

Allow Msg Request, disable this option to reject all MESSAGE requests outside of a call. By default, this option is enabled, enabling MESSAGE requests to be passed to the dial-plan.

Disallow Dynamic Hosts, disallow all dynamic hosts from registering with any IP address used for statically defined hosts. This helps avoid the configuration error of allowing users to register with the same address as a SIP provider.

NAT Tab



External Address, specifies a static address, or address[:port] combination, to be used in SIP and SDP messages.

External Host, alternatively you can specify an external host, and Asterisk will perform DNS queries periodically. Not recommended for production environments, Use "External Address" instead.

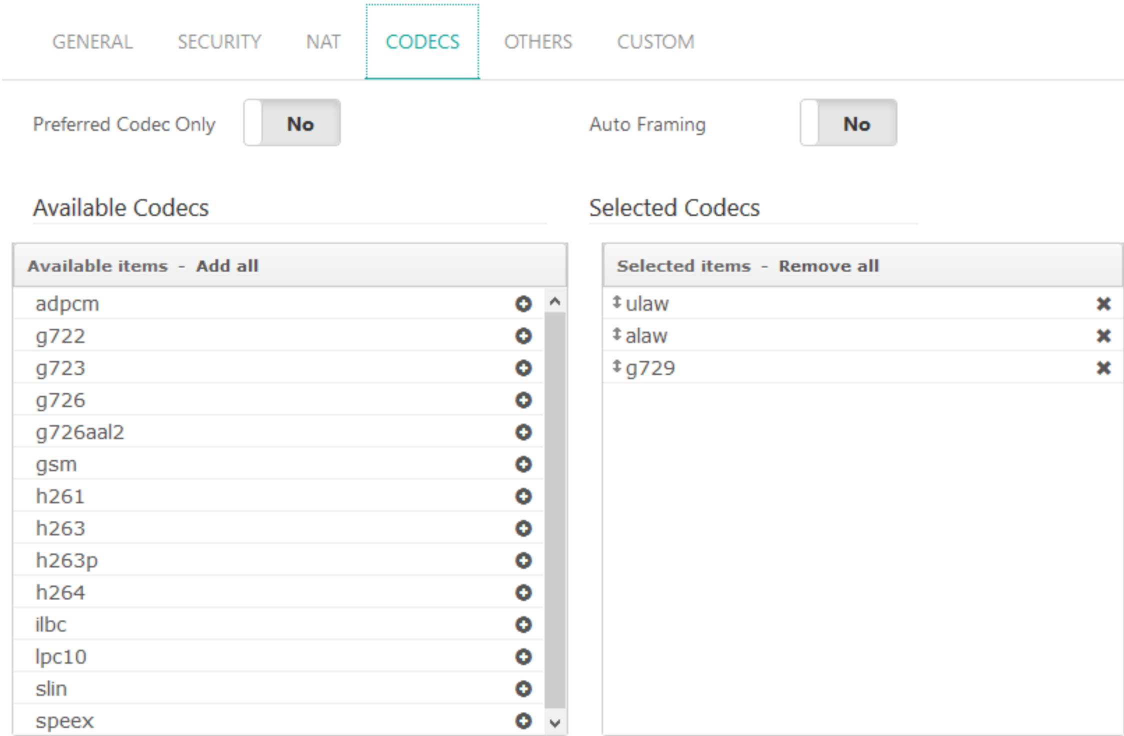
External Refresh, how often, in seconds, to refresh the "External Host," if used.

Local Networks Section

IP Address, valid IP address to be used.

Network Mask, network mask to use.

CODECS Tab



Preferred Codec Only, respond to a SIP invite with the single most preferred codec rather than advertising all codec capabilities. This limits the choice of codec by the remote side to exactly the codec that we prefer.

Auto Framing, set packetization based on the remote endpoint's (ptime) preferences.

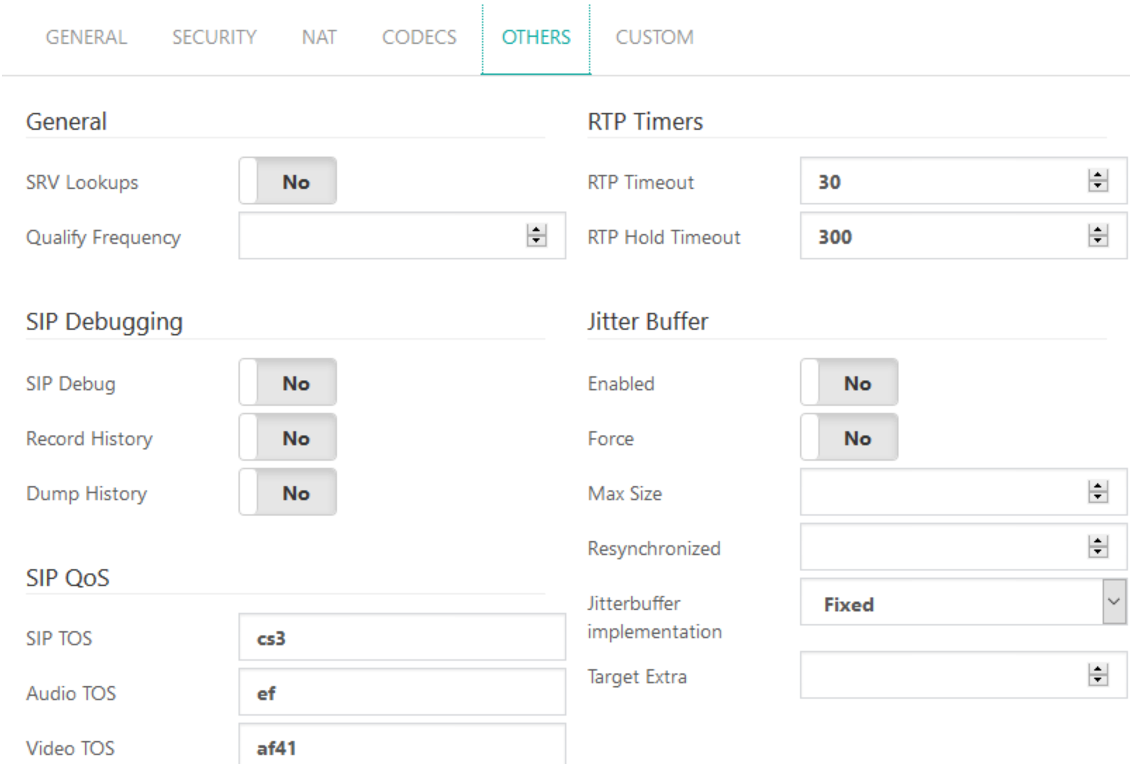
Codecs Selection Section

Press on + or – minus icons to move available codecs to list of selected codecs. Press on the x icon to remove codecs from the list of selected codecs. You can also select or remove all codecs by pressing on either the Add All or Remove All buttons.

Available Codecs, list of available codecs.

Selected Codecs, list of selected codecs.

OTHERS Tab



General Section

SRV Lookups, enables or disables DNS SRV lookups on outbound calls

Qualify Frequency, determines how often, in seconds, to check that the host is alive, as reported, in milliseconds, with sip show settings command.

RPT Timers Section

RPT Timeout, sets the time, in seconds, to terminate the call if there is no RTP or RTCP activity on the audio channel.

RPT Hold Timeout, sets the time, in seconds, to terminate the call if there is no RTP or RTCP activity on the audio channel.

SIP Debugging Section

SIP Debug, toggle SIP debugging, from the moment the channel loads this configuration.

Record History, toggles recording of SIP history.

Dump History, toggles dump SIP history at end of a SIP dialogue. SIP history is output to the DEBUG logging channel.

Jitter Buffer Section

Enabled, enables or disables the use of a jitter-buffer on the receiving side of a SIP channel.

Force, forces the use of a jitter-buffer on the receiving side of a SIP channel.

Max Size, maximum length, in milliseconds, of the jitter-buffer.

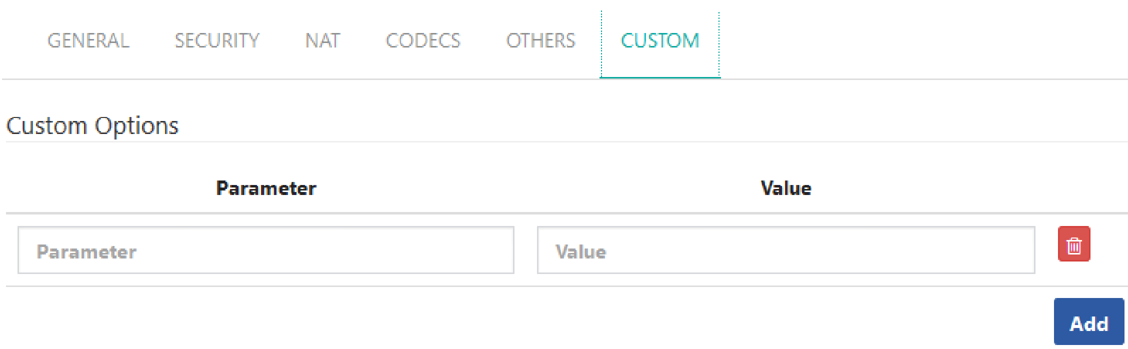
Resynchronized, gap in the frame timestamps, in milliseconds, beyond which the jitter-buffer will be resynchronized.

Implementation, used on the receiving side of a SIP channel. There is a choice of two options:

- Fixed: size always equals to jb-max-size
- Adaptive: variable size, actually the new jb of IAX2.

Target Extra, sets the time, in milliseconds , the new jitter buffer will pad its size. This option only affects the jb when 'jbimpl = adaptive' is set.

CUSTOM Tab



Custom Options Section

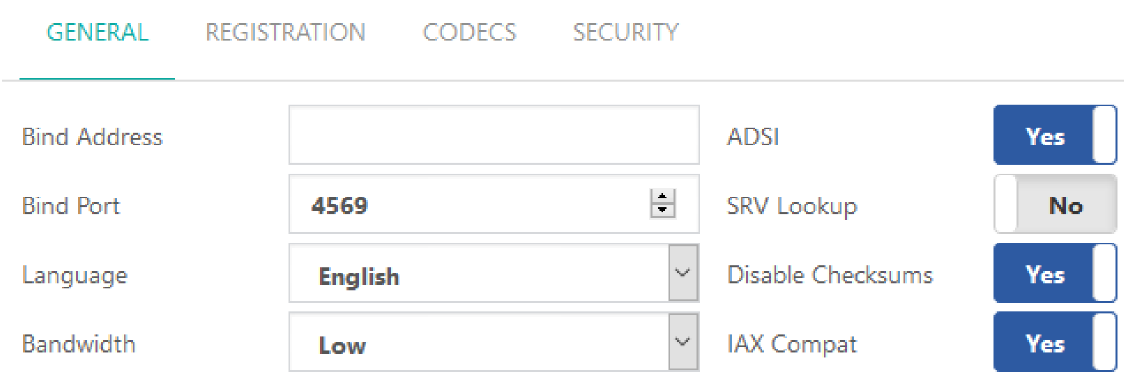
Parameter, The SIP parameter to be included in the [general] section.

Value, value of the SIP parameter to be used.

IAX2 Settings Dialog

The IAX2 Settings is used to configure the default value to be used for SIP calls.

GENERAL Tab



Bind Address, IP address to which to bind. Note that 0.0.0.0 binds to all IP addresses.

Bind Port, port to which IAX2 should bind. The default port is 4570.

Language, allows you to specify a global default language of prompts for all users who use this profile. This can be specified also on a per-user basis.

Bandwidth, specify bandwidth (low**,** medium**,** or high) to control which codecs should be used.

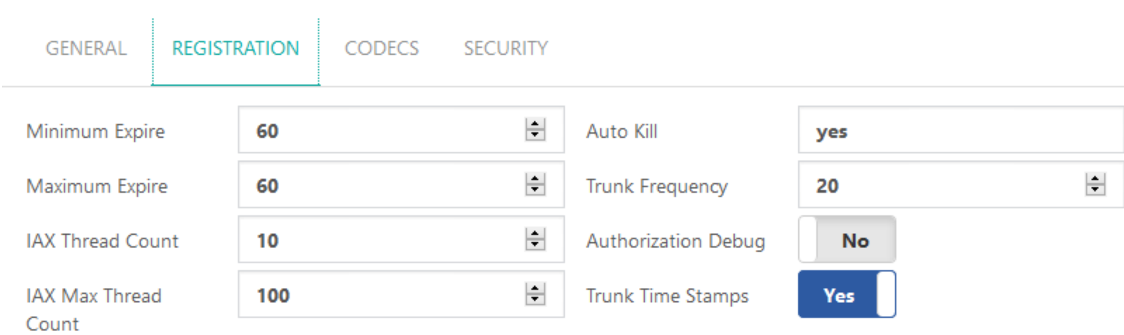
ADSI, Analog Display Services Interface(ADSI) can be enabled if you have ADSI-compatible CPE equipment.

SRV Lookup, whether or not to perform SRV lookup on outbound calls.

Disable Checksums, disable use of UDP checksums. If no checksum is set**,** then checksum will not be calculated or checked on systems supporting this feature.

IAX Compat, set to yes if you plan to use layered switches or some other scenario which may cause a delay when performing a lookup in the dial-plan. This option causes Asterisk to spawn a separate thread when it receives an IAX2 DPREQ (Dial-plan Request) instead of blocking while it waits for a response.

REGISTRATION Tab



Minimum Expire, minimum time**,** in seconds**,** that IAX2 peers can request registration.

Maximum Expire, maximum time, in seconds, that IAX2 peers can request registration.

IAX Thread Count, establishes the number of IAX helper threads to handle I/O.

IAX Max Thread Count, establishes the maximum number of IAX helper threads that can be used to handle I/O. The Asterisk Manager Interface (AMI), establishes the number of extra dynamic threads that may be spawned to handle I/O.

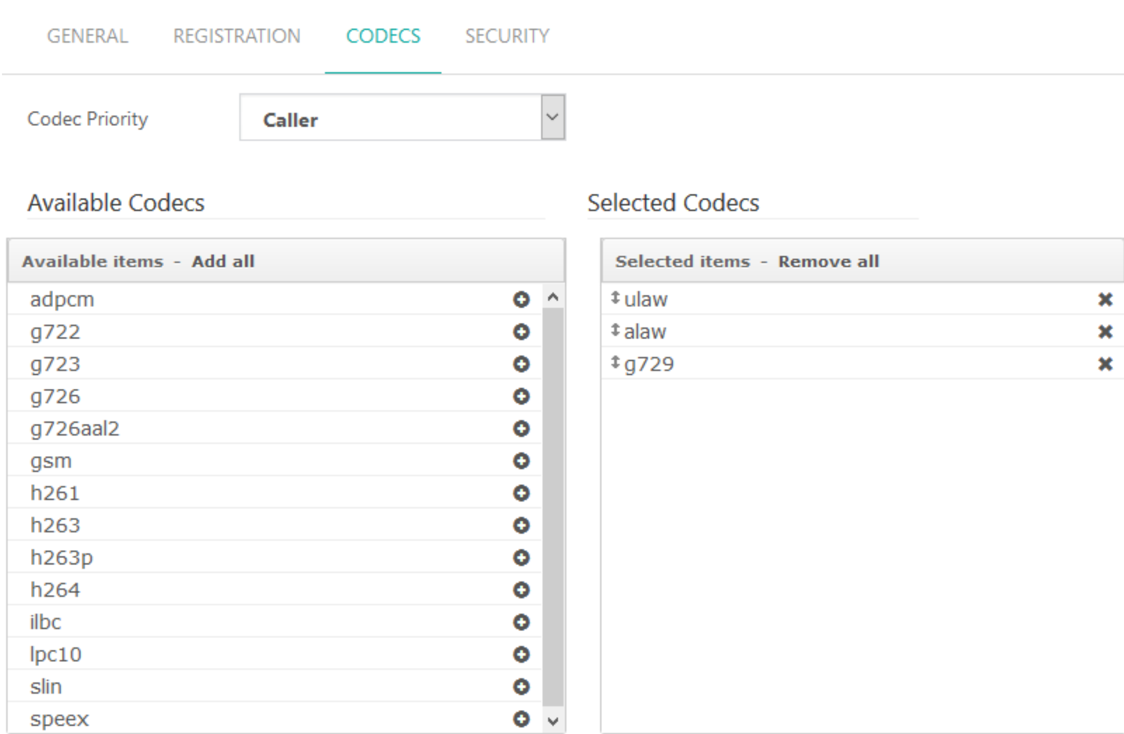
Auto Kill, this is used to keep the system from stalling when a host is not available. In addition to 'yes' or 'no' you can also specify a number of milliseconds.

Trunk Frequency, sets how frequently, in milliseconds, trunk messages are sent. This means the trunk will send all the data queued to it in the past period. By increasing the time between sending trunk messages, the trunk's payload size will increase as well.

Authorization Debug, enables authentication debugging, but will increase the amount of debug traffic.

Trunk Time Stamps, should we send timestamps for the individual sub-frames within trunk frames? There is a small bandwidth use for these (less than 1kbps/call), but they ensure that frame timestamps get sent end-to-end properly.

CODECS Tab



Codec Priority, controls the codec negotiation of an inbound IAX2 call. There are a number of options:

- Caller: consider the preferred order of the caller before considering the preferred order of the host.

- Host: consider the preferred order of the host before considering the preferred order of the caller.
- Disabled: disable the consideration of codec preference altogether.
- Reqonly: Behaves in a similar manner as the disabled option. The call will only be accepted if the requested format is available.

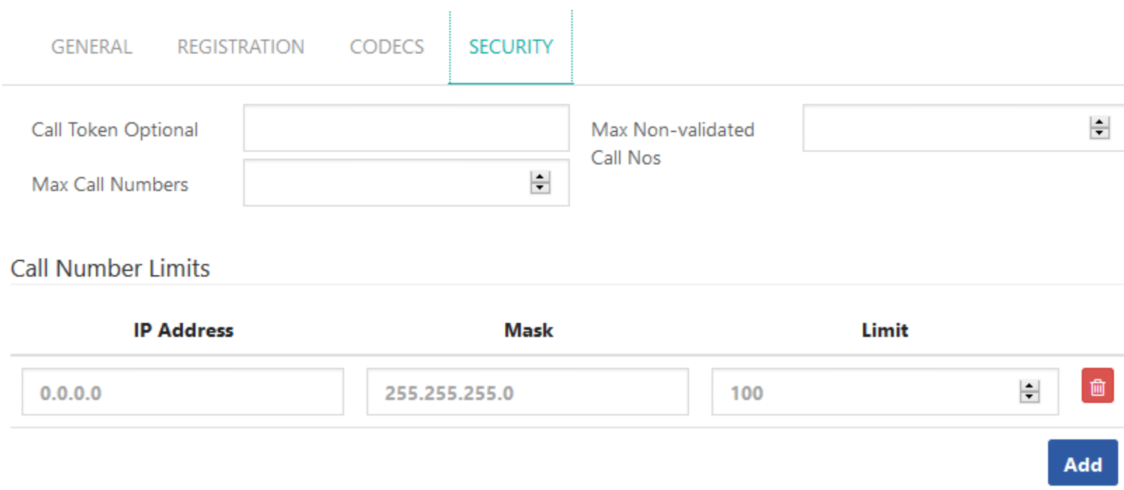
Codecs Selection Section

Press on + or – minus icons to move available codecs to list of selected codecs. Press on the x icon to remove codecs from the list of selected codecs. You can also select or remove all codecs by pressing on either the Add All or Remove All buttons.

Available Codecs, list of available codecs.

Selected Codecs, list of selected codecs.

SECURITY Tab



Call Token Optional, call token validation can be set as optional for a single IP address or a IP address range by enabling this option. This is a global option.

Max Call Numbers, this option limits the number of call numbers allowed for each individual remote IP address. Once an IP address reaches its call number limit, no more new connections are allowed until an existing connection is closed. This option can be used in a peer definition as well, but only takes effect for the IP of a dynamic peer after it completes registration

Max Non-validated Call Nos., thei parameter is used to set the combined number of call numbers that can be allocated for connections where call token validation has been disabled. Unlike the Max Call Numbers option, this limit is not separate for each individual IP address. Any connection resulting in a non-call token validated call number being allocated contributes to this limit.

Call Number Limits Section

- **IP Address,** valid IP address to be used.
- **Mask,** network mask to use.
- **Limit,** limits the number of call numbers allowed for this group of IP addresses. Once an IP address group reaches its call number limit**,** no more new connections are allowed until an existing connection is closed.

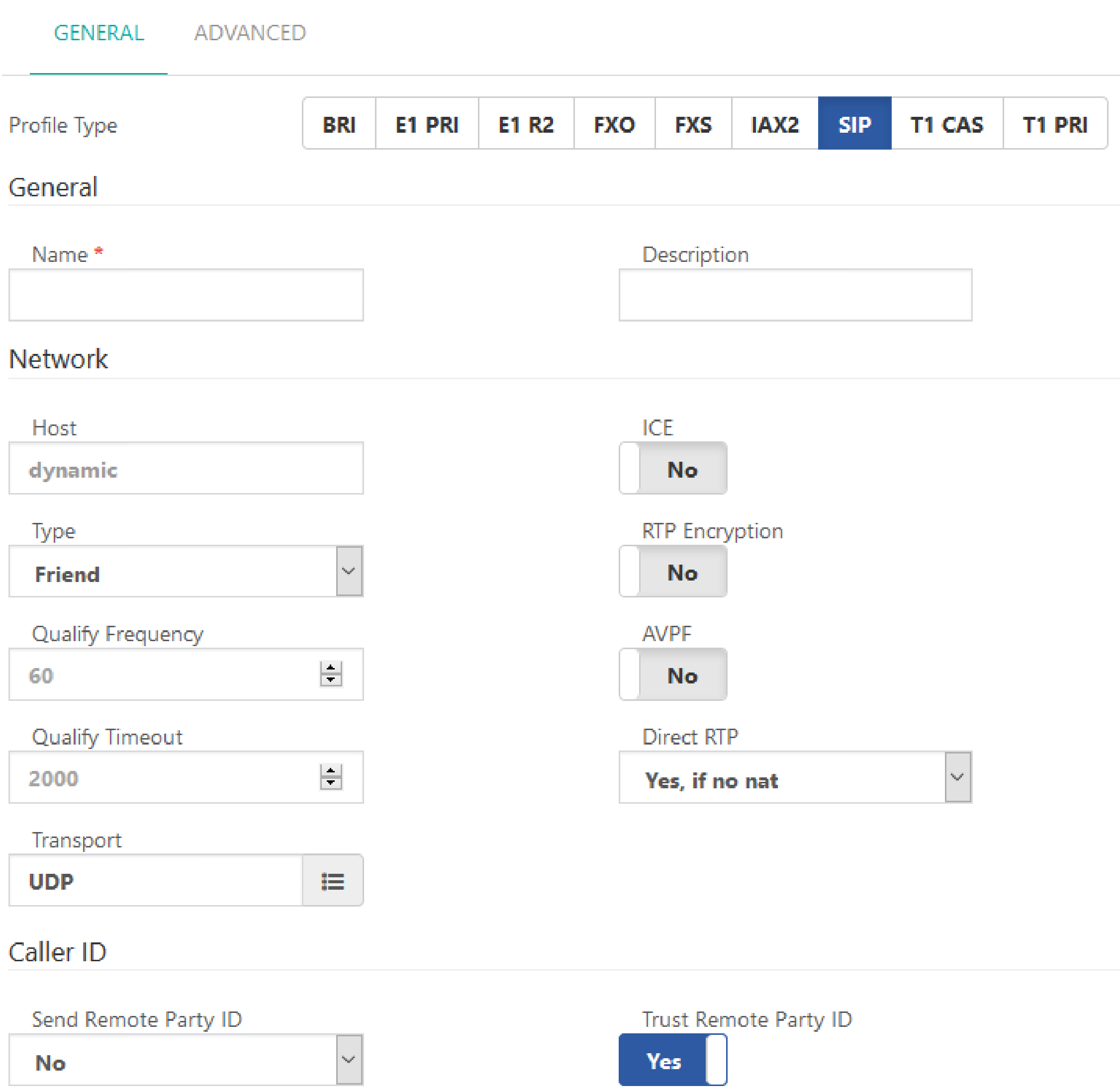
Profiles Dialog

Profiles are sets of characteristics that are generally repeated when creating extensions and / or devices. Instead of repeating in the forms and dial-plan these data we create profiles that group this data.

GENERAL Tab

There are many profile type options, including:

- BRI
- E1 PRI
- E1 R2
- FXO
- FXS
- IAX2
- SIP
- T1 CAS
- T1 PRI



Name*, user-defined name for the profile.

Description, short description to identify this profile.

Network Section

Host, the host parameter specifies the hostname or IP address of a SIP peer or user. It is used to make both outbound calls and to find the peer when an inbound call is received. Host can take the following formats:

- Domain Name / Hostname e.g. sip.zxv.com
- IP Address e.g. 234.23.42.103
- Dynamic**,** which means the phones must register.

Type, determines their roles within Asterisk. The type options are:

- Peer : Peers handle both inbound and outbound calls and are matched by IP/port. When there are incoming calls from the peer, the IP address must match in order for the invitation to be accepted.
- User : Asterisk users handle inbound calls only, which means that that they can call Asterisk, but Asterisk can't call them. The callers must be authenticated by their authorization information (username and secret).
- Friend : Asterisk will create the entity as both a friend and a peer. Asterisk will accept calls from friends just as it would for users, requiring only that the authorization matches, rather than the IP address.

Qualifyfreq, how often to check for the host to be up in seconds and reported in milliseconds with sip show settings.

Qualify Timeout, setting to yes (equivalent to 2000 msec) will send an OPTIONS packet to the endpoint periodically (default every minute). Used to monitor the health of the endpoint. If delays are longer then the qualify time, the endpoint will be taken offline and considered unreachable. Can be set to a value which is the threshold in milli-seconds. Setting this value to **No** will turn this off. Can also be helpful to keep NAT pinholes open.

Transport, set the default transports. The order determines the primary default transport.

ICE, whether to Enable ICE Support. Defaults to no. ICE (Interactive Connectivity Establishment) is a protocol for Network Address Translator (NAT) traversal for UDP-based multimedia sessions established with the offer/answer model. This option is commonly enabled in WebRTC setups.

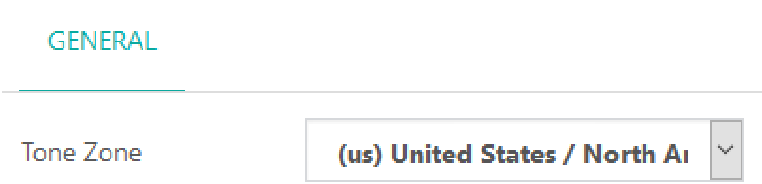
RTP Encryption, whether to offer SRTP encrypted media (and only SRTP encrypted media) on outgoing calls to a peer.

AVPF, enable inter-operability with media streams using the AVPF RTP profile.

Telephony Settings Dialog

Use this dialog to configure the default time zone to use applied to all users.

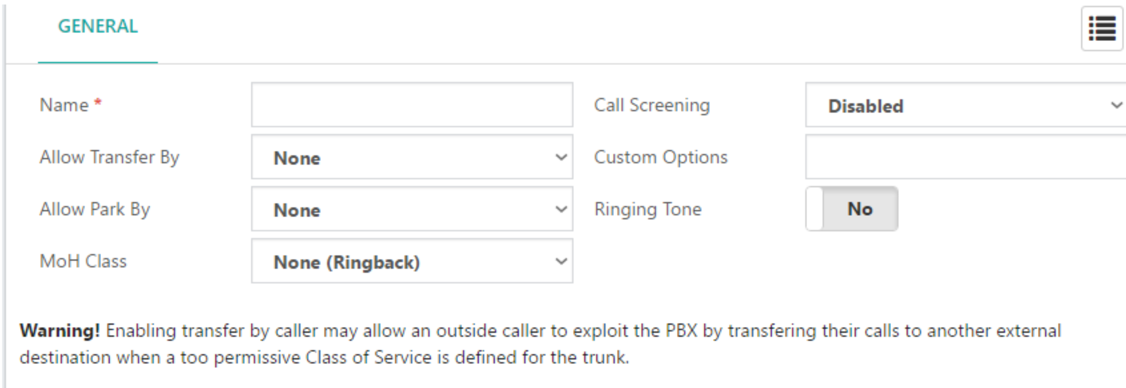
GENERAL Tab



Dial Profiles Dialog

Use this dialog to create a profile that can be used to control the functionality of extensions. EasyVOIZ will use this information to configure commonly-used Asterisk dial options. You can use the Advanced tab of the Extensions dialog to define which Dial Profile to associate with an extension.

GENERAL Tab



Name*, a free-text name to identify this profile.

Allow Transfer By, configure who is allowed to transfer calls. Sets the **t** and **T** Asterisk dial options.

- **None** – calls cannot be transferred
- **Caller** – calls can only be transferred by the caller
- **Recipient** – call can only be transferred by the recipient of the call
- **Both** – call can be transferred by both the caller and the recipient of the call

Enabling transfer by the caller may allow an external caller to exploit the PBX by transferring a call to an external destination, unless this is blocked by the Class of Service associated with the Trunk.

Allow Park By, configure who is allowed to park calls. Sets the **k** and **K** Asterisk dial options.

- **None** – calls cannot be parked
- **Caller** – calls can only be parked by the caller
- **Recipient** – call can only be parked by the recipient of the call
- **Both** – call can be parked by both the caller and the recipient of the call

MoH Class, sets the Music on Hold to be played to the calling party until the call is answered. Select any existing MoH Class from the dropdown list. Sets the **m** Asterisk dial option.

Call Screening, when enabled, requires the caller to identify themselves. This sets the **p** and **P** Asterisk dial options.

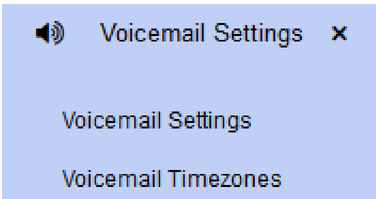
- **Disabled** – callers are not required to be identified
- **Ask Once** – ask callers to identify themselves the first time that they call the extension, and remember this for future calls.
- **Always Ask** – always ask callers to identify themselves, i.e. ask them for identification every time that they ring the extension.

Custom Options, allows you define custom dial option. There are many options that you can set on the outbound call, including call screening, distinctive ringing, and more. Type **core show application**

dial in the Asterisk CLI for a complete list of all available options. If you want to specify multiple options, simply concatenate them together. For example, if you want to use both the **m** and **H** options, you would set **mH** as the options parameter. See the full list of available dial options in Dial Options section in the appendix, or refer to Asterisk online documentation for full list of dial options.

Ringing Tone, when set to Yes, will cause the ringing tone to be played to the caller, even if the device of the called party is not ringing. Sets the **r** Asterisk dial option.

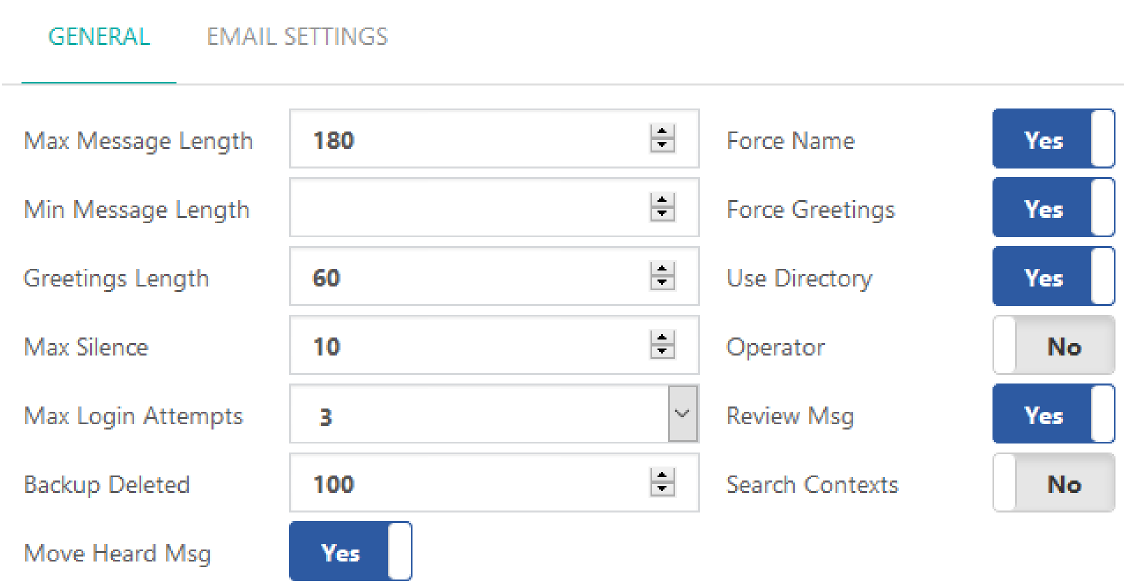
Voicemail Settings Menu Group



Voicemail Settings Dialog

GENERAL Tab

In this tab you will find the information about Voicemail Settings.



Max Message Length, maximum length of a voicemail message in seconds. Leave empty for No Limit.

Min Message Length, minimum length of a voicemail message in seconds for the message to be kept. Leave empty for No Minimum.

Greetings Length, maximum length of greetings in seconds.

Max Silence, how many seconds of silence before we end the recording.

Max Login Attempts, max number of failed login attempts.

Move Heard Msg, move heard messages to the Old folder automagically.

Backup Deleted, maximum number of messages allowed in the Deleted folder.

Force Name, forces a new user to record their name. A new user is determined by the password being the same as the mailbox number.

Force Greetings, forces a new user to record their greeting message. A new user is determined by the password being the same as the mailbox number.

Use Directory, permit finding entries for forward/compose from the directory.

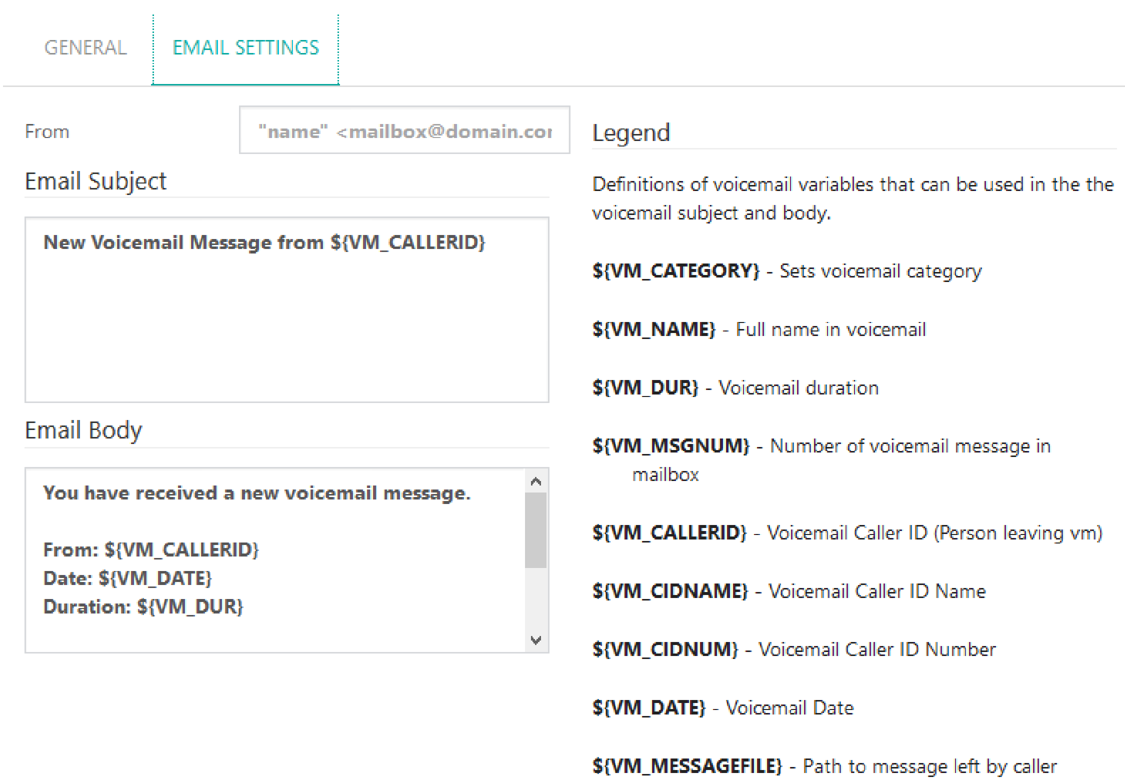
Operator, allow sender to hit 0 before/after/during leaving a voicemail to reach an operator. This option REQUIRES an o extension in the same context (or in exit context, if set), as that is where the 0 key will send you.

Review Msg, allow sender to review/rerecord their message before saving it

Search Context, current default behavior is to search only the default context if one is not specified. The older behavior was to search all contexts.

EMAIL SETTINGS Tab

In this tab you will find the information about email settings for send voicemail.



From, the sender of the e-mail notification.

Email Subject, the text that will be written in the subject line of the email. You can also include system-defined placeholders within the text:

- $(VM_CALLERID) inserts the caller ID (name and number) of the caller who left the message

- $(VM_CIDNAME) inserts the name of the caller who left the message
- ${VM_CIDNUM} inserts the number of the caller who left the message
- $(VM_DATE) inserts the timestamp of the voicemail
- $(VM_DUR) inserts the duration of the voicemail
- $(VM_NAME) inserts the name of the extension receiving the voicemail
- $(VM_MSGNUM) inserts the sequential number of the message that is allocated by the phone system
- $(VM_MAILBOX) inserts the number of the mailbox receiving the voicemail

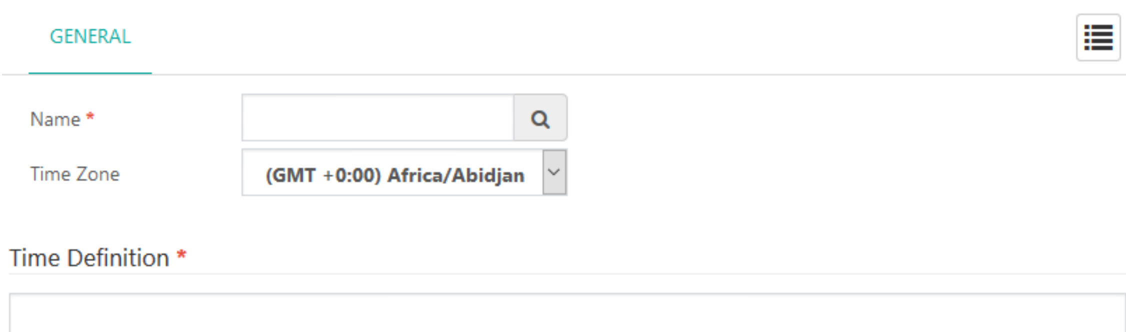
Email Body, the text that will be written in the body of the email. You can also include system-defined placeholders within the text:

- $(VM_CALLERID) inserts the caller ID (name and number) of the caller who left the message
- $(VM_CIDNAME) inserts the name of the caller who left the message
- ${VM_CIDNUM} inserts the number of the caller who left the message
- $(VM_DATE) inserts the timestamp of the voicemail
- $(VM_DUR) inserts the duration of the voicemail
- $(VM_NAME) inserts the name of the extension receiving the voicemail
- $(VM_MSGNUM) inserts the sequential number of the message that is allocated by the phone system
- $(VM_MAILBOX) inserts the number of the mailbox receiving the voicemail

Voicemail Timezones Dialog

GENERAL Tab

Configures information about Timezone Settings for voicemail.



Name*, short name of time zone.

Time Zone, country for time zone.

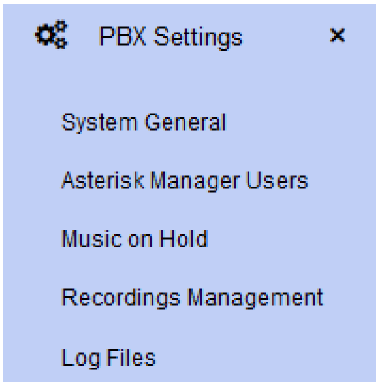
Time Definition*, enables you to configure the format of the timestamp, for example, the following example sets up two different voicemail zones, one for the Central time zone in 12-hour format, and a second in the Mountain time zone, in 24-hour format:

- central=America/Chicago|'vm-received' Q 'digits/at' IMp
- mountain24=America/Denver|'vm-received' q 'digits/at' H 'digits/hundred' M 'hours'

There are a number of formatting symbols that are available:

- A or a indicates the day of the week (Saturday, Sunday, etc.)
- B or b or h indicates the name of the month (January, February, etc.)
- d or e indicates the numeric day of the month (first, second... thirty-first)
- Y indicates the year
- I or l indicates the hour, in 12-hour format
- H indicates the hour, in 24-hour format - single-digit hours are preceded by "oh"
- K indicates the hour, in 24-hour format - single-digit hours are not preceded by "oh"
- M indicates the minute
- P or p indicates to use A.M. or .P.M.
- Q indicates "today", "yesterday," or ABdY (note: not standard strftime value)
- q indicates "" (for today), "yesterday", weekday, or ABdY (note: not standard strftime value)
- R indicates the 24-hour time, including minutes

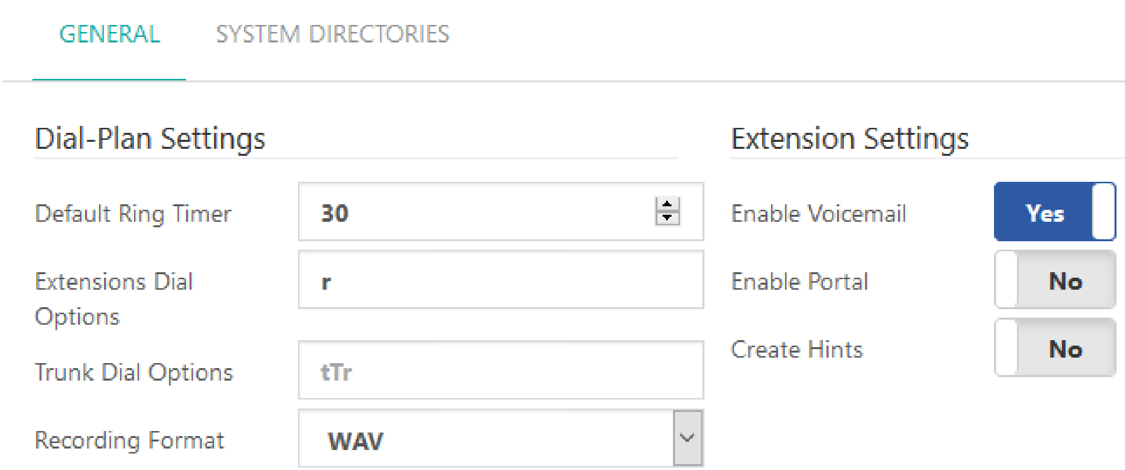
PBX Settings Menu Group



System General Dialog

GENERAL Tab

In this tab you will find the information about PBX Settings.



Dial-Plan Settings Section

Default Ring Timer, time extensions by default ringing.

Extension Dial Options, options for extension dial application. See the full list of available dial options in Dial Options section in the appendix.

Trunk Dial Options, options for trunks dial application. See the full list of available dial options in Dial Options section in the appendix.

Recording Format, file format for calls recording.

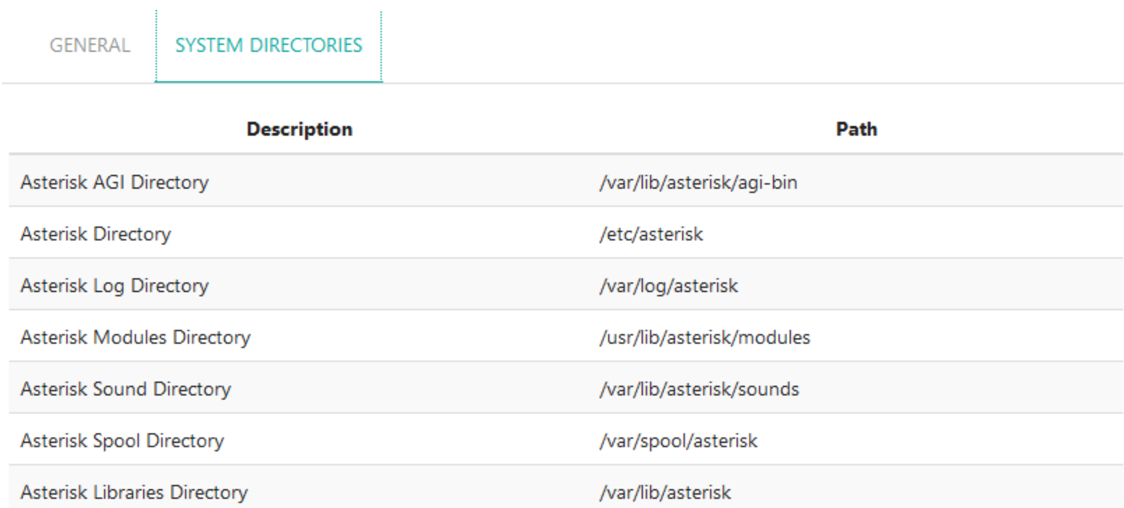
Extension Settings Section

Enable Voicemail, determines whether voicemail will be automatically enabled for all new extensions.

Enable Portal, determines whether Portal will be automatically enabled for all new extensions.

Create Hints, determines whether hints will be automatically created for all new extensions.

SYSTEM DIRECTORIES Tab



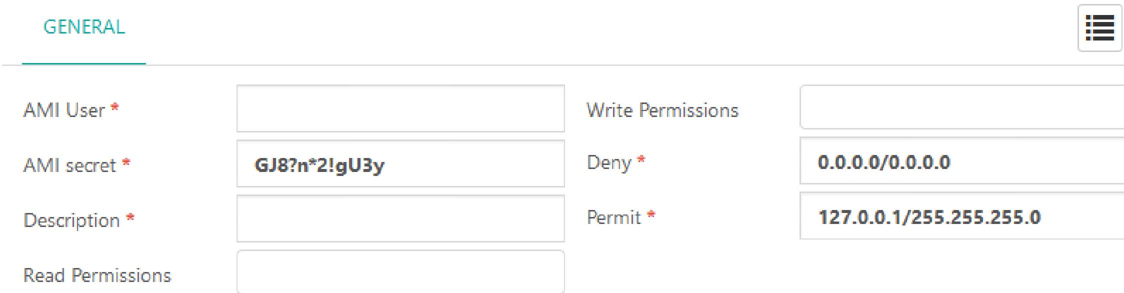
Description	Path
Asterisk AGI Directory	/var/lib/asterisk/agi-bin
Asterisk Directory	/etc/asterisk
Asterisk Log Directory	/var/log/asterisk
Asterisk Modules Directory	/usr/lib/asterisk/modules
Asterisk Sound Directory	/var/lib/asterisk/sounds
Asterisk Spool Directory	/var/spool/asterisk
Asterisk Libraries Directory	/var/lib/asterisk

- Asterisk Directory**,** home Asterisk directory.
- Asterisk Modules Directory**,** Asterisk dialogs directory.
- Asterisk Libraries Directory**,** Asterisk libraries directory.
- Asterisk Log Directory**,** Asterisk log directory.
- Asterisk Sound Directory**,** Asterisk sound directory.
- Asterisk AGI Directory**,** Asterisk AGI directory.
- Asterisk Spool Directory**,** Asterisk spool (recording) directory

Asterisk Manager Users Dialog

GENERAL Tab

In this tab you will find the information about Asterisk Manager Users.



AMI User*, user name for connect to Asterisk Management Interface (AMI) - must be unique

AMI Secret*, secret for login to Asterisk Management Interface (AMI)

Description*, free-text description

Read Permissions, Asterisk Management Interface (AMI) read permissions - select one (or more) from the list of available options

Write Permissions, Asterisk Management Interface (AMI) write permissions - select one (or more) from the list of available options

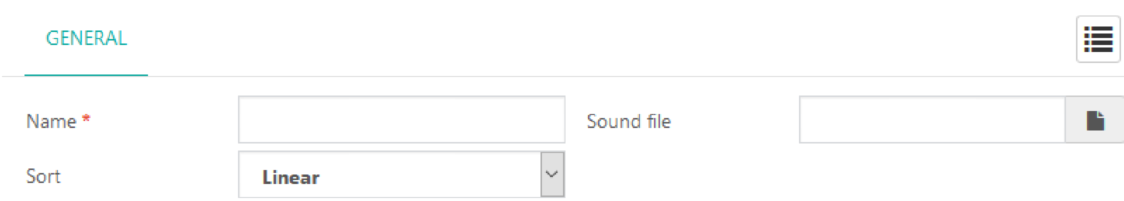
Deny, to deny multiple hosts or networks**,** use & char as separator, for example: 192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0

Permit, to permit multiple hosts or networks**,** use & char as separator, for example: 192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0

Music on Hold Dialog

GENERAL Tab

In this tab you will find the information about Music on Hold.



Name*, short description for identify this MoH Category.

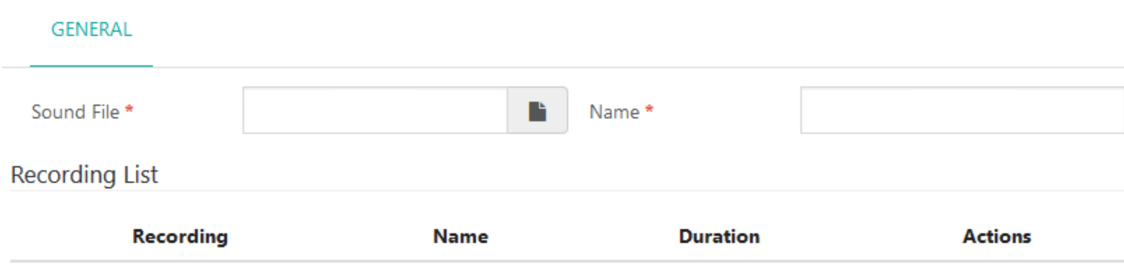
Sort, Sort the files to play Options:

Sound File, upload a wav or mp3 file.

Recordings Management Dialog

GENERAL Tab

In this tab you will find the information about Recordings Management.



Sound File*, upload a wav or mp3 file.

Name*, short description for identify this recording.

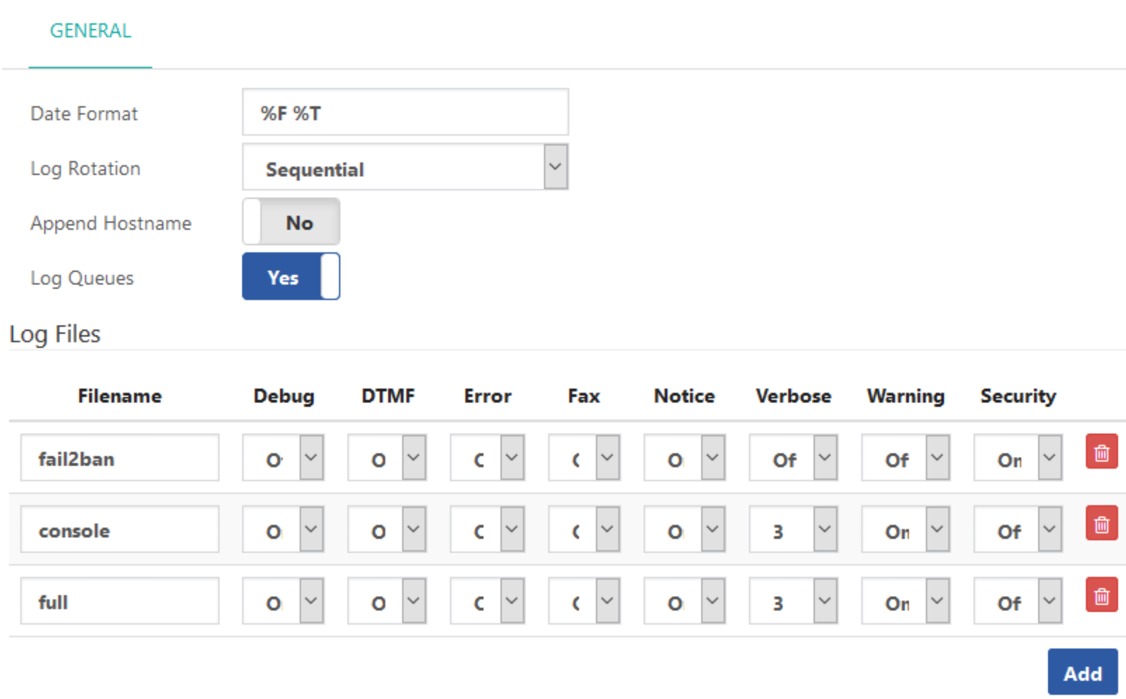
Recording List

- **Recording,** name of the sound file.
- **Name,** description of the sound file.
- **Duration**, length (in seconds) of the recording
- **Action**
    - , edit description.
    - , listen recording.
    - , delete recording.

Log Files Dialog

GENERAL Tab

In this tab you will find the information about create new log file.



Date Format, customize the display of debug message time stamps. See strftime(3) Linux manual for format specifiers. Note that there is also a fractional second parameter which may be used in this field. Use %1q for tenths, %2q for hundredths, etc. Leave blank for default: ISO 8601 date format yyyy-mm-dd HH:MM:SS (%F %T).

Log Rotation

- Sequential: Rename archived logs in order, such that the newest has the highest sequence number.
- Rotate: Rotate all the old files, such that the oldest has the highest sequence number (expected behavior for Unix administrators).
- Timestamp: Rename the log files using a timestamp instead of a sequence number when "logger rotate" is executed.
- Append Hostname, appends the hostname to the name of the log files.

Append Hostname, appends the hostname to the name of the log file

Log Queues, log queue events to a file.

Log Files Section

- **Filename,** name of log file.
- **Debug,** debugging is only useful if you are troubleshooting a problem with the Asterisk code itself. You would not use debug to troubleshoot your dial-plan, but you would use it if the Asterisk developers asked you to provide logs for a problem you were reporting. Do not use debug in production, as the amount of detail stored can fill up a hard drive in a matter of days.
- **DTMF,** logging DTMF can be helpful if you are getting complaints that calls are not routing from the auto attendant correctly.

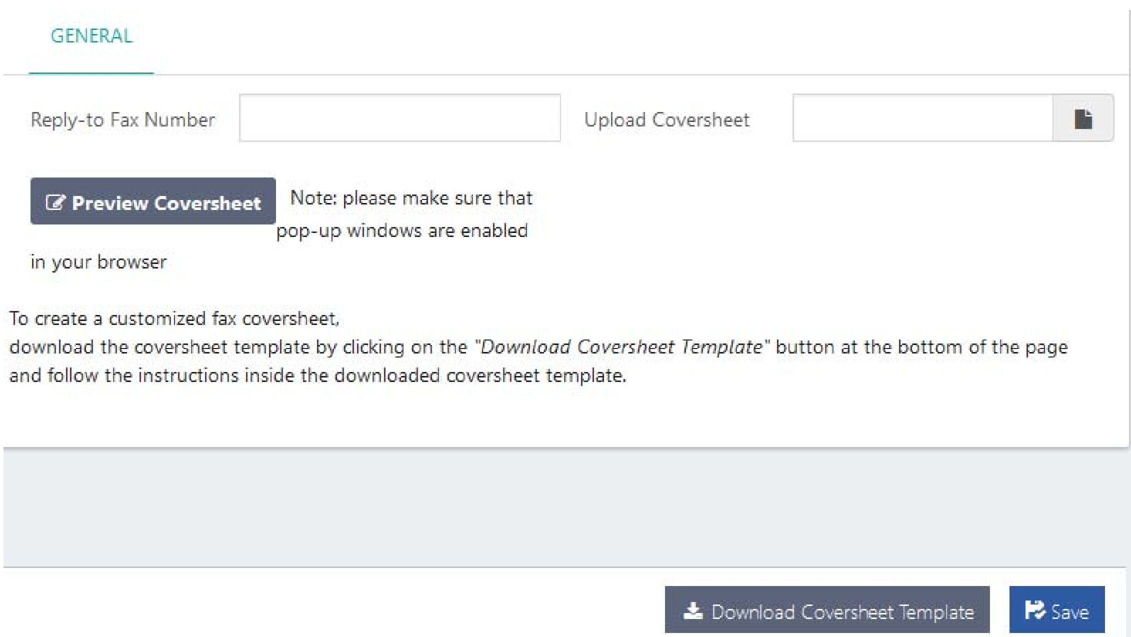
- **Error,** errors represent significant problems in the system that must be addressed immediately.
- **Fax,** this type of logging causes fax-related messages from the fax technology backend (res_fax_spandsp or res_fax_digium) to be logged to the fax logger.
- **Notice,** you will see a lot of these during a reload, but they will also happen during normal call flow. A notice is simply any event that Asterisk wishes to inform you of.
- **Verbose,** this is one of the most useful of the logging types, but it is also one of the more risky to leave unattended, due to the possibility of the output filling your hard drive.
- **Warning,** a warning represents a problem that could be severe enough to affect a call (including disconnecting a call because call flow cannot continue). Warnings need to be addressed.
- **Security,** output security messages.

Fax Settings Dialog

Fax Master is a commercial module that is licenced by D-Link. This dialog will not be active unless a valid licence is linked to the system.

This dialog allows you to configure the system-wide cover sheet that will be used for outbound faxes.

GENERAL Tab

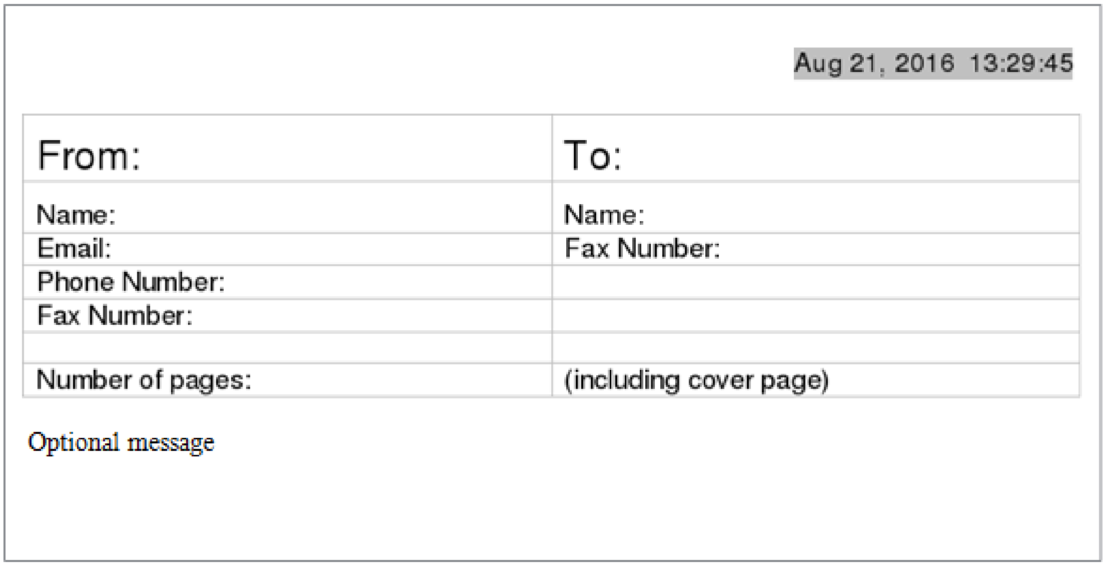


Reply-to-Fax Number, is the number that identifies your fax station. Typically, this would be the number which external users would use to send faxes to your system.

Preview Coversheet, allows you to review the coversheet that is currently stored in the system. Pop-up windows must be enabled in order to display the coversheet.

Upload Coversheet, allows you to upload a coversheet that can be used on outbound faxes. The coversheet must be in pdf format. You can download a coversheet template by clicking on the **Download Coversheet Template** button at the bottom of the screen.

Download Coversheet Template, allows you to download a template which can use to create your personalized coversheet. The template is downloaded in doc format: after completing your modifications, it must be saved in pdf format for uploading.



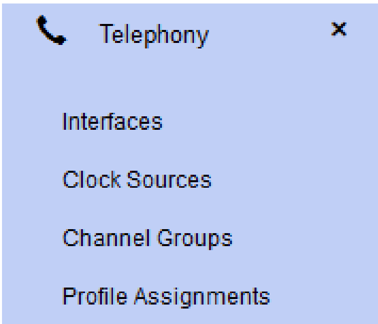
Aug 21, 2016 13:29:45

From:	To:
Name:	Name:
Email:	Fax Number:
Phone Number:	
Fax Number:	
Number of pages:	(including cover page)

Optional message

- The areas that are shaded in gray (such as the date and timestamp fields) are auto populated by the system with dynamic information, so you must not change them.
- In the blank areas you may place any static image or text, such as your company logo, slogan, policy statement etc.
- Delete the instructions box and save the file in pdf format.
- Upload the created file using this dialog.

Telephony Menu Group

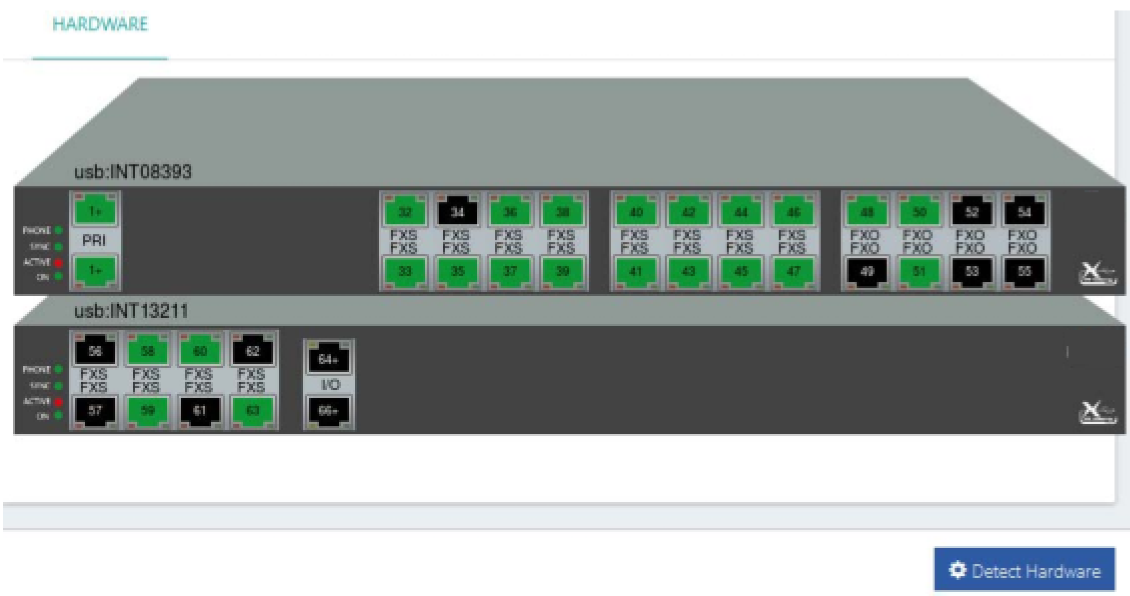


Interfaces Dialog

HARDWARE Tab

Allows you to see a visual representation of telephony hardware that is integrated into your system. The graphical display will indicate what kind of interfaces are available, and their channel numbers.

Click on **Detect Hardware** to automatically detect attached telephony hardware

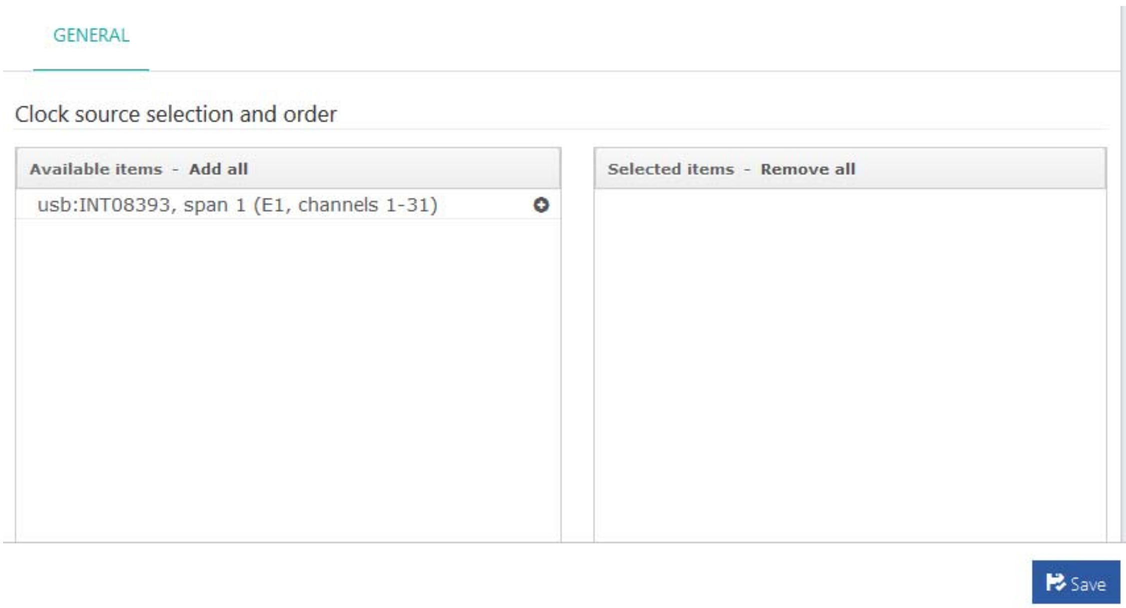


Clock Sources Dialog

General Tab

Displays list of clock sources, enabling you to configure the order in which they will be processed.

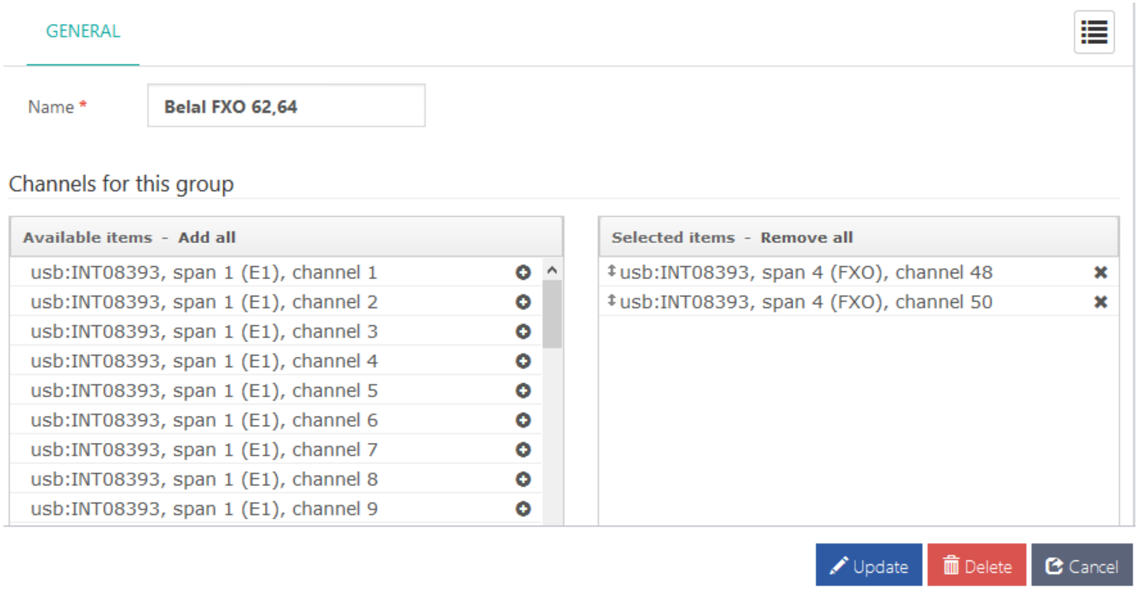
Don't forget to click on **Save** after making any changes.



Channel Groups Dialog

Allows you to create groups of channels, by selecting available channels from drop-down list. The drop-down list is automatically populated by clicking **Detect Hardware** in the Settings > Telephony > Interfaces dialog.

GENERAL Tab



Name*, is free-text description to uniquely identify a Channel Group.

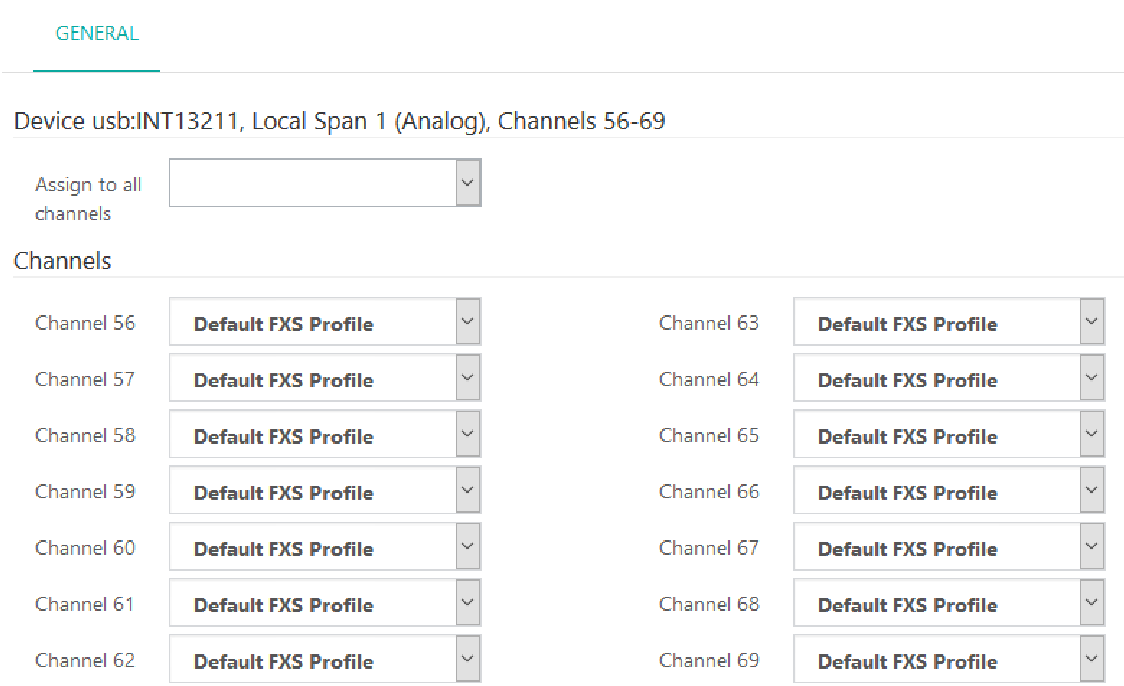
Available Items, is a list of all channels that have been discovered on the system

Selected Items, is a list of all channels that have been selected as members of the Channel Group.

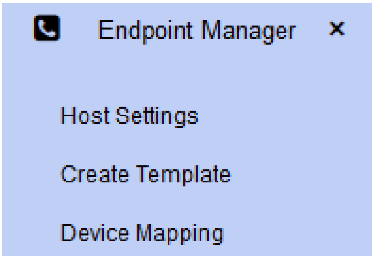
Profile Assignments Dialog

The list of profiles is automatically populated by clicking **Detect Hardware** in the Settings > Telephony > Interfaces dialog.

GENERAL Tab


GENERAL
Device usb:INT13211, Local Span 1 (Analog), Channels 56-69
Assign to all channels
Channels
Channel 56
Default FXS Profile
Channel 57
Default FXS Profile
Channel 58
Default FXS Profile
Channel 59
Default FXS Profile
Channel 60
Default FXS Profile
Channel 61
Default FXS Profile
Channel 62
Default FXS Profile
Channel 63
Default FXS Profile
Channel 64
Default FXS Profile
Channel 65
Default FXS Profile
Channel 66
Default FXS Profile
Channel 67
Default FXS Profile
Channel 68
Default FXS Profile
Channel 69
Default FXS Profile

End Point Manager Menu Group



The Endpoint Manager allows you to centrally manage the configuration settings for all IP devices that can be accessed on the network.

It is important to note that IP phones are identified in the Endpoint Manager by their MAC address. This provides you with a powerful tool to pre-provision IP phones before the phones are even connected to the network. This can be done without even opening the box containing the phone, as phone manufacturers typically print the MAC address on the outside of the packaging.

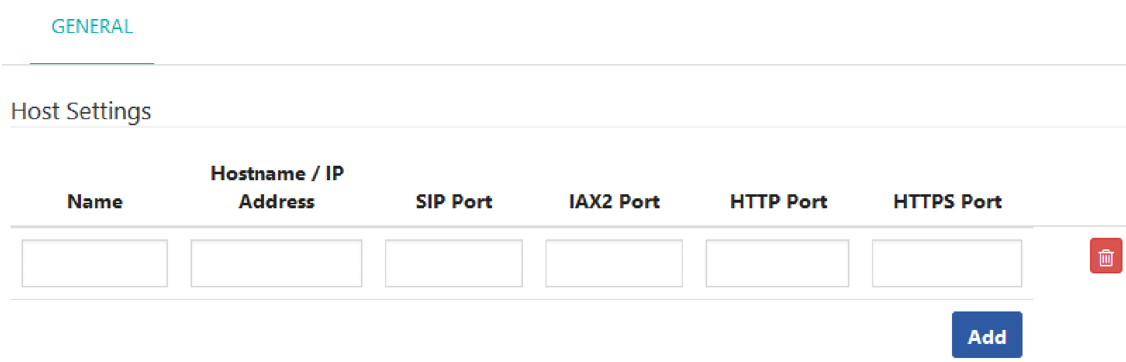
Note that EasyVOIZ uses http (and not tftp) protocol to manage the configuration of endpoint devices.

There are a small number of simple tasks that you will need to complete in order to make the Endpoint Manager fully operational:

1. Ensure that your DHCP server is correctly configured to support Option 66, and that the format of Option 66 address is compatible with the Endpoint Manager.
2. Create an entry in the Host Settings dialog to define:
    - Host address of your PBX server
    - Ports used by SIP, IAX2, HTTP, and HTTPS protocols
    - 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 D-Link phones, you would need to create two templates – one for each model.
4. Use the Device Mapping dialog to scan your network for available phone devices. You can also manually add devices that the network discovery cannot find.
5. Link each device that you want to manage to a template and to one (or more) PBX extensions

Host Settings Dialog

The Host Settings dialog allows you to configure one or more sets of parameters that can be used when configuring phones. This provides Endpoint Manager with information about the environment to which the phones belong. For example, you may have one template for IP phones that reside on the same network segment as your PBX server, and another template for phones that are located on a different segment. Why would you want to do this? For example, you may use port forwarding for external SIP connections so that external SIP phones can be forwarded from port 6050 to port 5060, whereas internal phones (that reside on the same network as the PBX server) directly access port 5060.



Host Settings Section

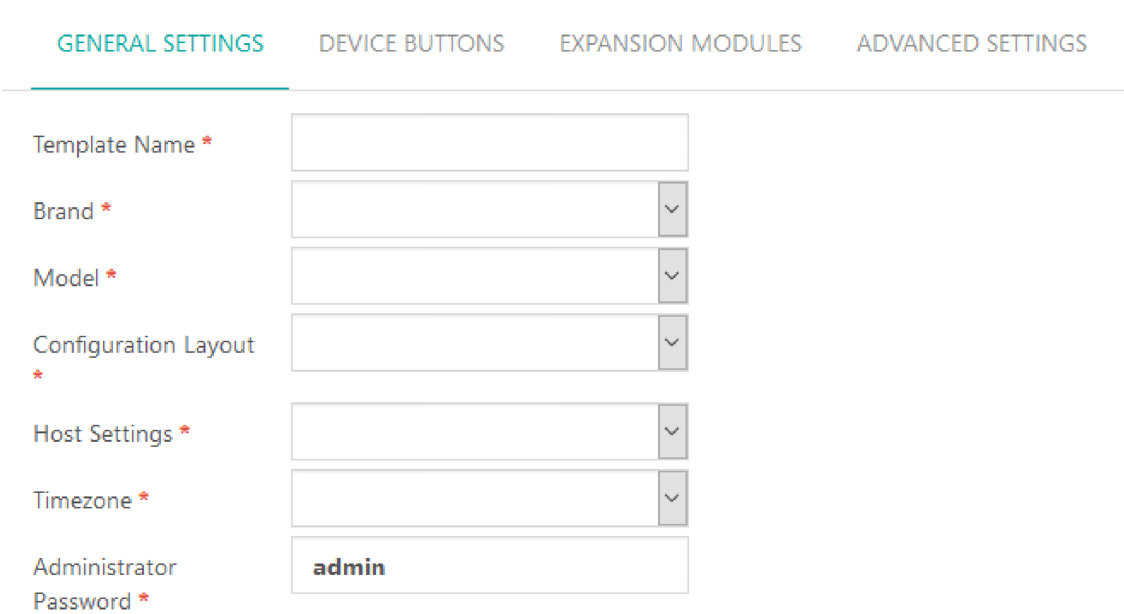
- **Name,** helps to simplify maintenance: each host setting should be identified with a unique label.
- **Hostname / IP Address,** is the address of your PBX server. Note that the IP address used by phones that reside on the same network as PBX may be different from the address used by phones that are outside the network. Phones that are on the same network can use the physical address of PBX, even if it is a private IP address. Phones that are outside the network will need to use a publicly-accessible IP address or hostname.
- **SIP Port,** typically 5060, is the port that IP phones will access when using SIP protocol. Phones that are on the same network as your PBX typically use the default port, while phones that are outside the local network may utilize port-forwarding to use a different port. There is no default value if this field is left blank: if you do not type a value for this field, SIP phones will not work.
- **IAX2 Port,** typically 4569, is the port that IP phones will access when using IAX2 protocol. Phones that are on the same network as your PBX typically use the default port, while phones that are outside the local network may utilize port-forwarding to use a different port. There is no default value if this field is left blank: if you do not type a value for this field, IAX2 phones will not work.
- **HTTP Port,** typically 80, is the port that IP phones will use for HTTP access. Phones that are on the same network as your PBX typically use the default port, while phones that are outside the local network may utilize port-forwarding to use a different port. There is no default value if this field is left blank.
- **HTTPS Port,** typically 443, is the port that IP phones will use for HTTPS access. Phones that are on the same network as your PBX typically use the default port, while phones that are outside the local network may utilize port-forwarding to use a different port. There is no default value if this field is left blank.

Create Template Dialog

You need to create at least one template for every model of IP phone that you want to manage. If you have phone models that use different host settings, you will need to create a template for each combination of phone model/host settings.

GENERAL SETTINGS Tab

You will need to create multiple templates, for example, when you want to use a different set of host settings (for the same model phone), or when you have phone models in different time zones.



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

Brand, select a Brand from the drop-down list of brands that are supported by Endpoint Manager. If you require a brand that does appear in the drop-down list, you can contact support, by pressing on the Add new model support menu (on the right-hand side of the dialog).

Various models from the following brands are supported:

- Aastra
- D-Link
- Escene
- Fanvil
- GrandStream
- Hanlong
- Polycom
- Snom
- Vtech
- D-Link

- Yealink

Model, select a Model from the drop-down list of models that are supported by Endpoint Manager. If you require a model that does appear in the drop-down list, you can contact support, by pressing on the Add new model support menu (on the right-hand side of the dialog).

Configuration Layout, indicates what layout of configuration file you want to use. A very small number of phones may use more than one style of configuration file, depending on the firmware version that is installed.

Host Settings, allows you to select the name of the Host Settings (described above) that you want to use in this template.

Time zone, allows you to select the time zone offset to be used by all phones that use this template.

Administrator Password, is the password that can be used by users to manually access the configuration interface of IP phones based on this template. You should be aware of the limitation imposed by your IP Phone. For example, some IP phones will only accept the password as numeric digits. The Endpoint Manager does not validate whether the password will be acceptable by the phone: you must refer to the documentation for your specific phone.

DEVICE BUTTONS Tab

Allows you to configure the DSS (direct station select) buttons for IP phones that use this template.

The button types, which depend on the brand and model of IP phone that you are using, can include such types as:

- ACD
- BLF
- Call Park
- Call Pickup
- Call Return
- Conference
- DND
- DTMF
- Forward
- Hold
- Intercom
- Line
- Local Directory
- N/A
- Record
- Redial
- Remote Directory
- Speed Dial
- Transfer
- Voice Mail

Some phones do not support device buttons at all. In such cases, a suitable message will be displayed.

For some phones, such as Fanvil, the type has no significance (and will be ignored), as the type is included as a parameter in the Value field

EXPANSION MODULES Tab

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

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

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

For some phones, such as Fanvil, the type has no significance (and will be ignored), as the type is included as a parameter in the Value field.

ADVANCED SETTINGS Tab

Advanced Settings allows you to manage the configuration file for phones that belong to this template.

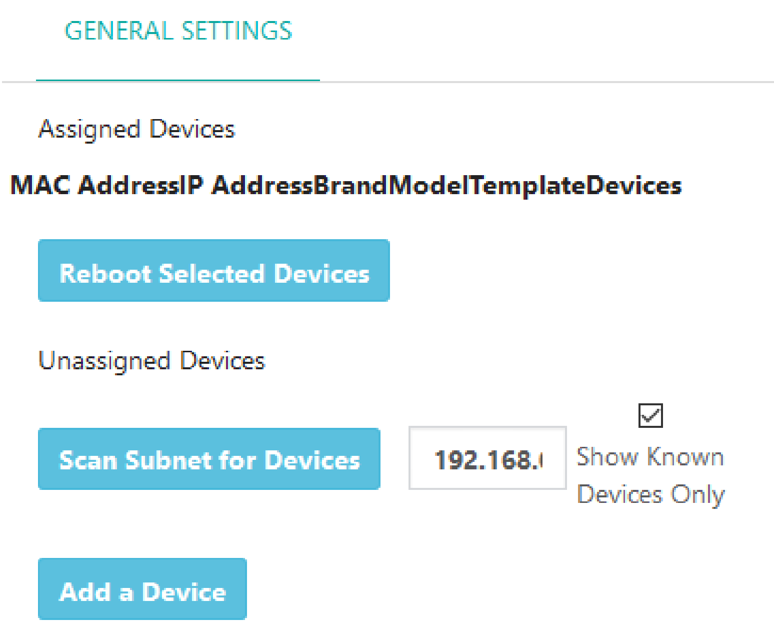
Advanced Settings provides access to parameters that are not directly managed by the Endpoint Manager. Codec settings would be an example of such a parameter. Manufacturers' default values, where applicable, are already defined in the file. You would only need to modify values in the configuration file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

Device Mapping Dialog

This dialog manages your devices. The devices that you want to manage can be automatically discovered. Type in a target network segment and mask, such as 192.168.25.0./24, and press on Scan subnet for devices.

The auto discovery will take some time, depending on the number of addresses that can potentially exist on the subnet. Be careful not to use a mask that is too big, as this will impact the time required to complete the discovery process. If devices cannot be discovered by scanning the network, you can manually enter the MAC address of any phones that you want to manage.

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.


GENERAL SETTINGS
Assigned Devices
MAC AddressIP AddressBrandModelTemplateDevices
Reboot Selected Devices
Unassigned Devices
Scan Subnet for Devices
192.168.(
Show Known Devices Only
Add a Device

Switchboard Menu Group

Switchboard Manager Dialog

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 EasyVOIZ.

Dashboard Tab

Users Tab

This dialog enables you to manage Switchboard users and permissions, and also select which groups each user can view.

In order to have access to the Switchboard, users must be suitably defined. Only users that are defined as Switchboard Users can login to the Switchboard. Default security uses the extension number and voicemail password, although a different password can be defined in the Switchboard Users dialog. Switchboard Users who are not defined in the Users dialog cannot access the Switchboard.

Click on the **Submit Changes** button to save all changes or modifications.

Extension, extension allocated to the user.

Secret, 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, 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 **Permissions** dropdown list.

Permissions, allows you to see a list of all available permissions.

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.

Plugins, allows you to add additional plugins which will loaded for this Switchboard user.

Buttons Tab

The buttons dialog allows you to define the behavior of each button.

For example, you can change button labels (overriding the existing EasyVOIZ 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 EasyVOIZ.

Label, defines the name that will be displayed on the button in the Switchboard.
Email, allows you to send emails to the user from 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
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.
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.
Tags, can be defined for buttons, which can used to filter the buttons that will be displayed, as described in the **Filter Box** section.
Custom ASTDB, is the ASTDB key to search for custom states. By default, this set to Call Forward Unconditional state.
Enabled, determines whether this button should be enabled or not

Do not forget to click on the **Submit Changes** button to save all your changes and modifications.

Groups Tab

Name, allows you to create a free-text name to reference the group.

Included Buttons, displays all available buttons: allows you to select (by checking the checkbox to the right of the item) which buttons that should be included in this group.

Do not forget to click on the **Submit Changes** button to save all your changes and modifications.

Templates Tab

This dialog simplifies user management by allowing you create and manage templates, which you can then assign to users.

Name, allows you to create a free-text name to reference the template. By checking the appropriate checkbox, you can make this the default template for all ***new*** users.

Permissions, allows you to see a list of all available permissions and to specify what actions the user will be able to perform

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.

Plugins, allows you to add additional plugins which will loaded for this Switchboard group.

Permissions Tab

Name, allows you to create a free-text name to reference this group of permissions.

Permissions, allows you to see a list of all available permissions and to specify what permissions will belong to this permissions group

Groups, enables you to select (by selecting the appropriate checkbox) to which groups this permission group should be applied. If no groups are selected the permission will be permitted on all buttons.

Do not forget to click on the **Submit Changes** button to save all your changes and modifications.

Permissions Dialog

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

Name, allows you to create a free-text name to reference this group of permissions.

Permissions, allows you to see a list of all available permissions and to specify what permissions will belong to this permissions group

Groups, enables you to select (by selecting the appropriate checkbox) to which groups this permission group should be applied. If no groups are selected the permission will be permitted on all buttons.

Do not forget to click on the **Submit Changes** button to save all your changes and modifications.

Plugins Tab

Lists all plugins that are available for the Switchboard. Allows you to install, buy, or deinstall plugins.

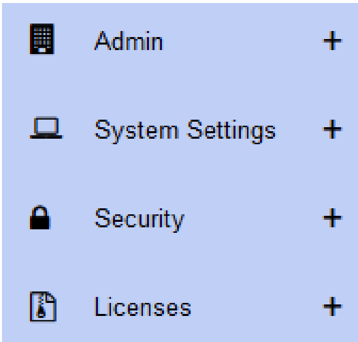
You can also modify settings of plugins that are already integrated into the system.

Additionally, you can use this tab to upload tar or gzip files from your local machine.

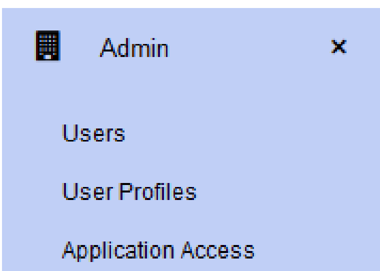
Settings Tab

Displays various parameters that can be managed by the Switchboard administrator.

5. Admin Menu Set



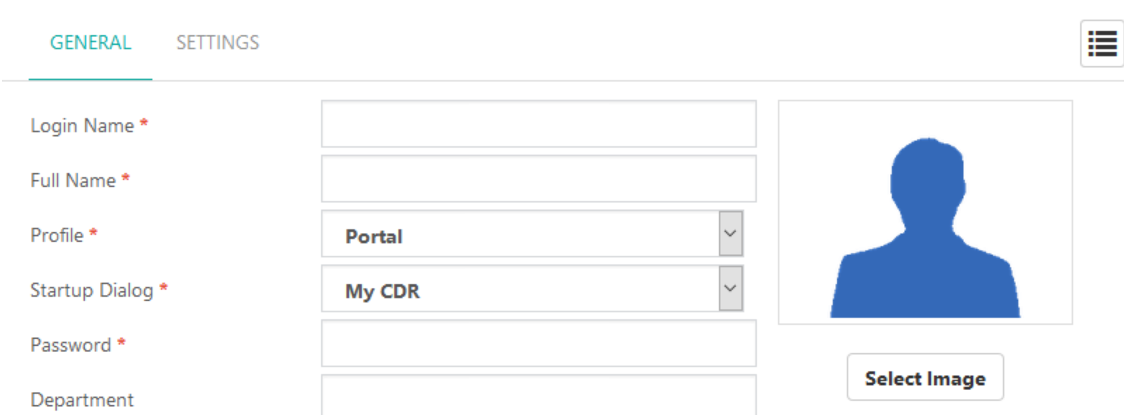
Admin Menu Group



Users Dialog

GENERAL Tab

In this tab you will find the information about management users.



Login Name*, user name that you will use to login to the system.

Full Name, full**,** real name**,** of the user.

Profile*, user profile to be associated with this user. This determines the security rights of the user within the system. You can use the User Profiles dialog to manage the rights that are associated with each profile.

Note that with the exception of the built-in Administrator user, all other users are not able to modify their Profile. Only the user who created the user has access to the Profile dropdown.

Startup Dialog*, set the dialog that will shown when the user logs into the system.

Password*, the password that this user will use to login to the system.

Department, user department (Example: System Admininstrators)

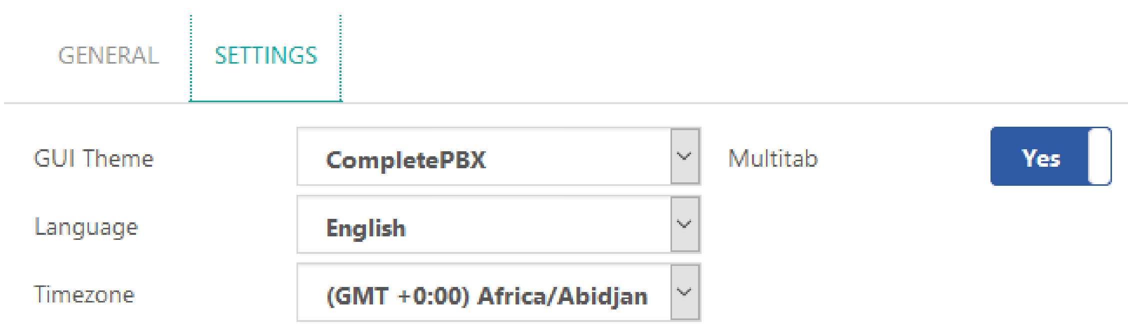
Select Image, image which will be associated with the user. Can be an avatar**,** graphic**,** or a photo of the user.

If you have lost the password for the **admin** user, you can login to the linux system and run the command ***./usr/share/ombutel/scripts/reset_ombu_password***

After doing this, you will be asked to create a new **admin** password next time you access the web login dialog.

SETTINGS Tab

In this tab you will be able to manage the user's themes and settings.



GUI Theme, choose a theme from the drop-down list – this determines the theme that will be used for displaying the user interface. This change will only take effect after your next login to the system.

Language, choose a language from the drop-down list – this determines the language that will be used in the user interface. This change will only take effect after your next login to the system.

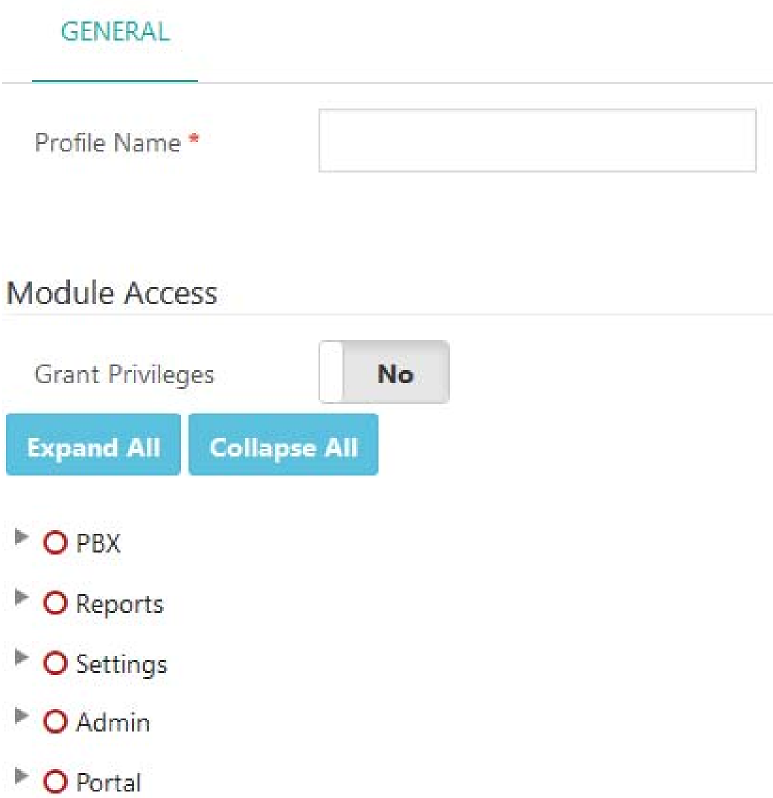
Timezone, the timezone that should be associated with this user. This change will only take effect after your next login to the system.

Multi-tab, enable if you want multiple tabs to be displayed in the user interface. This change will only take effect after your next login to the system.

User Profiles Dialog

GENERAL Tab

In this tab you will find the information about management user's profiles.



Profile Name*, name for this profile.

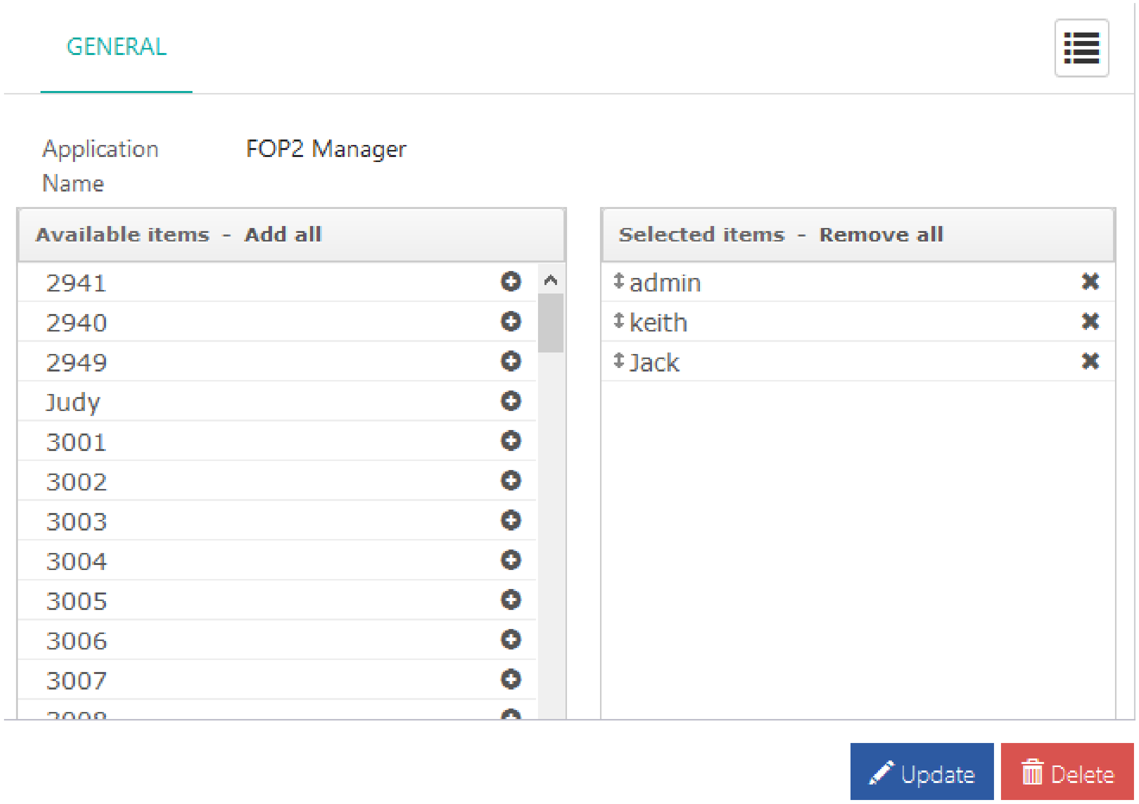
Module Access

- **Grand Privileges,** allow access to all dialogs.

Application Access Dialog

Allows system administrator to control user access to specific applications or modules.

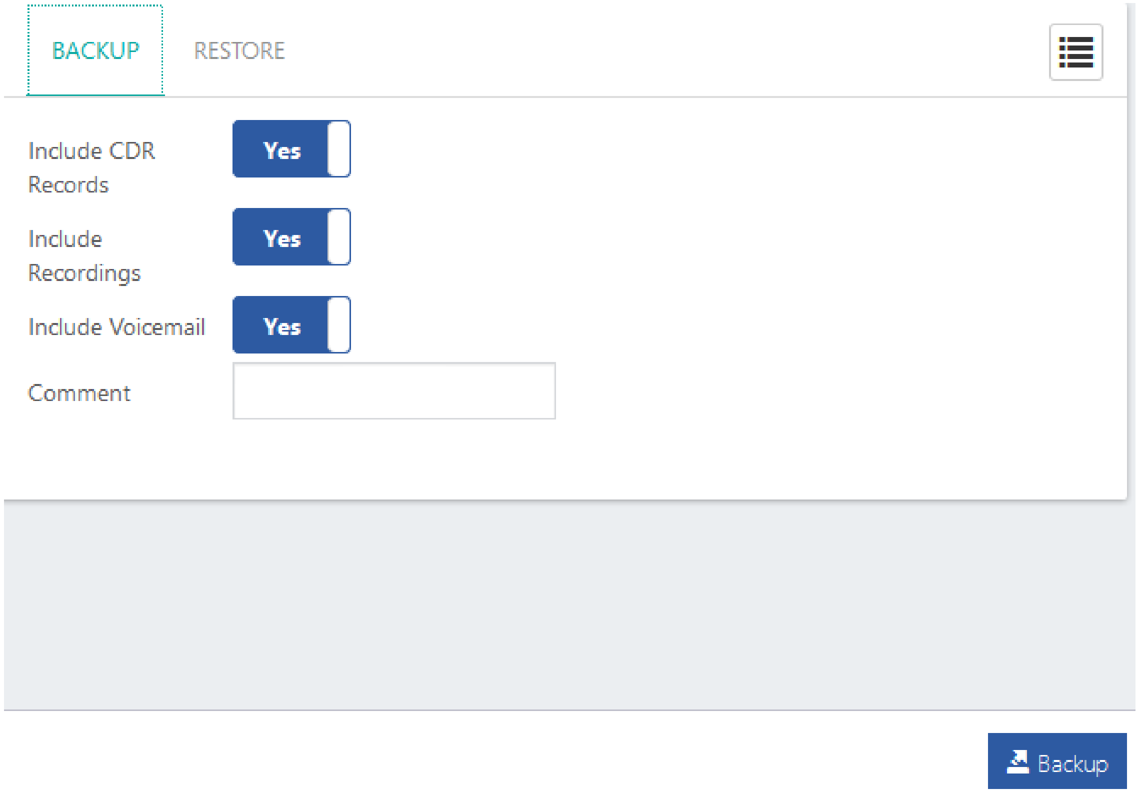
Use the Show All button the right-hand side of the dialog to see the list of available applications



Backup & Restore Dialog

Allows the system administrator to create a backup of the current system, or to restore a previously-create backup. The backup will save the configuration information required in order to restore the PBX configurations and settings. The backup does not include the operating system, or configuration information for any third-party applications that may be integrated into the system. You can use Rapid Recovery to create a full system backup, that includes the entire operating system – see details in Rapid Recovery.

Backup Tab



Include CDR Records, allows you to save backup space by determining whether the backup set should include CDR records. Backing up CDR data will back up all the call detail records stored on the system. Without this backup all CDR records will be lost if the system needs to be rebuilt. There is no way to recover CDR records without this backup.

Include Recordings, allows you to save backup space by determining whether the backup set should include recordings. Backing up recordings will back up all the voice prompts and custom Music on Hold recordings. Without this backup, prompts for IVRs, follow-me, queues, and Music on Hold recordings will all have to be re-recorded or re-uploaded after a system failure.

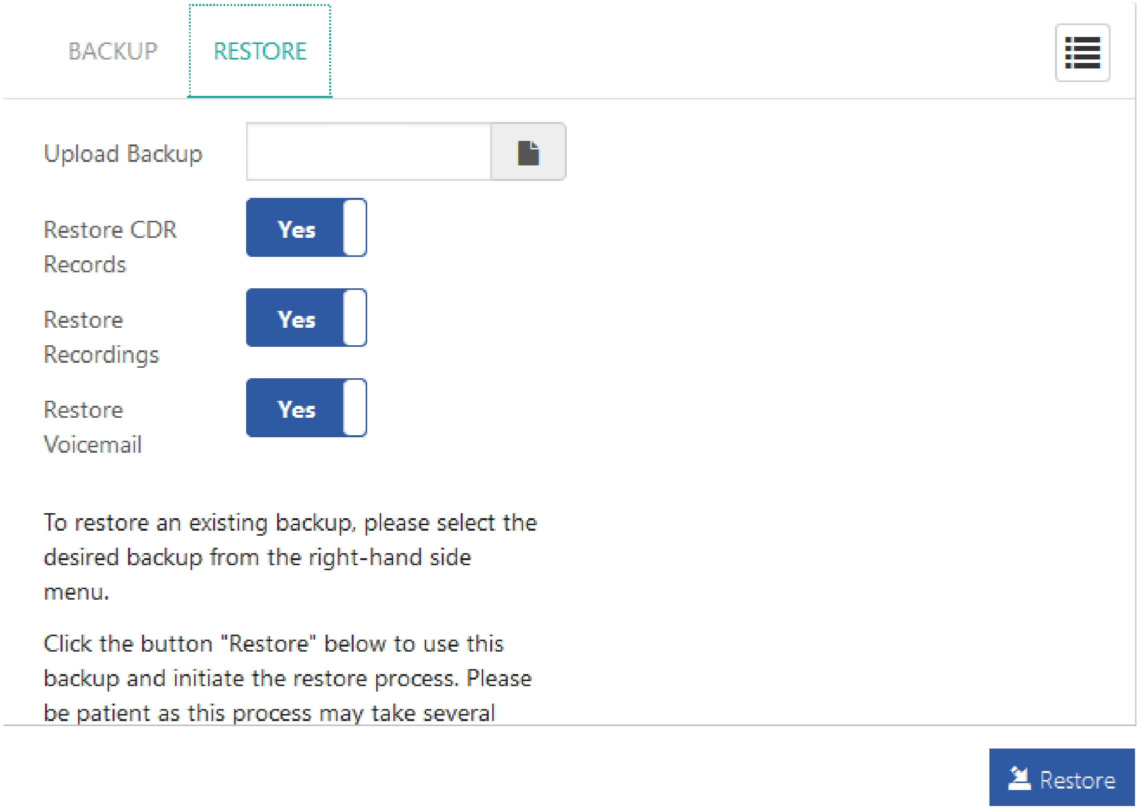
Include Voicemail, allows you to save backup space by determining whether the backup set should include voicemail recordings. Backing up voicemail will back up all the voicemail messages stored in the system.

Comment, allows you to add free-text to help identify the purpose of the backup.

Click the **Backup** button at the bottom of the dialog in order to create a backup. The backup set, by default, will be stored in the `/var/lib/ombutel/static/backup` directory.

Click on the Show All icon at the right-hand side of the menu to see all backups that are currently stored on the server.

Restore Tab



Upload Backup, allows you select the backup set from which you want to restore your system.

If you want to use a backup set that resides on the server, click on the Show All icon on the right-hand side of the dialog to see a list of all backup sets currently stored on the system

Restore CDR Records, use this option if your backup set includes CDR Records, but you do not want to restore them.

Restore Recordings, use this option if your backup set includes recordings, but you do not want to restore them.

Restore Voicemail, use this option if your backup set includes voicemail message, but you do not want to restore them.

Click the **Restore** button at the bottom of the dialog in order to restore the selected backup.

Maintaining and Protecting Backups

The way in which the system provides backups is simple and effective, but requires consideration of two factors: storage and protection. The backup data must be properly maintained or the system will eventually run out of space and cease to function. Make sure that your backup procedures include periodic deletion of old backup sets, to prevent your system from running out of disk space.

Once the problem of backup maintenance is taken care of, the problem of backup protection still exists. The backups taken by the system reside on the server itself. If the hard disk crashes or the local backup becomes corrupted, there will be no way to restore a failed system. Make sure that you periodically move sets of backup data from your server to another location. It is good practice to maintain copies of your backup at a different location, so ensure that are protected in case of some catastrophe such as fire or flooding.

Protecting Backups

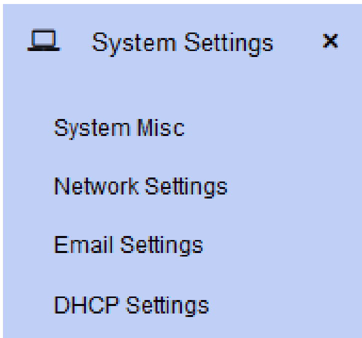
There are a number of ways to protect backups. Each one may protect a particular deployment scenario better than the other. While the specifics of each protection scenario are outside the scope of this document, it is worth keeping them in mind when setting up backups to make sure that a backup is always close at hand. The most common methods for protecting backups are as follows:

Redundant hardware (specifically, hard disks in a RAID configuration)

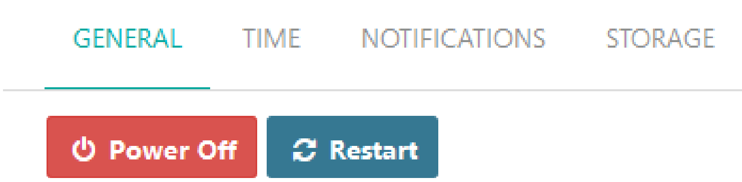
Automating the copy of backups to an external hard disk or network location

Automating the copy of backups to an off-site backup server

System Settings Menu Group



System Misc Dialog

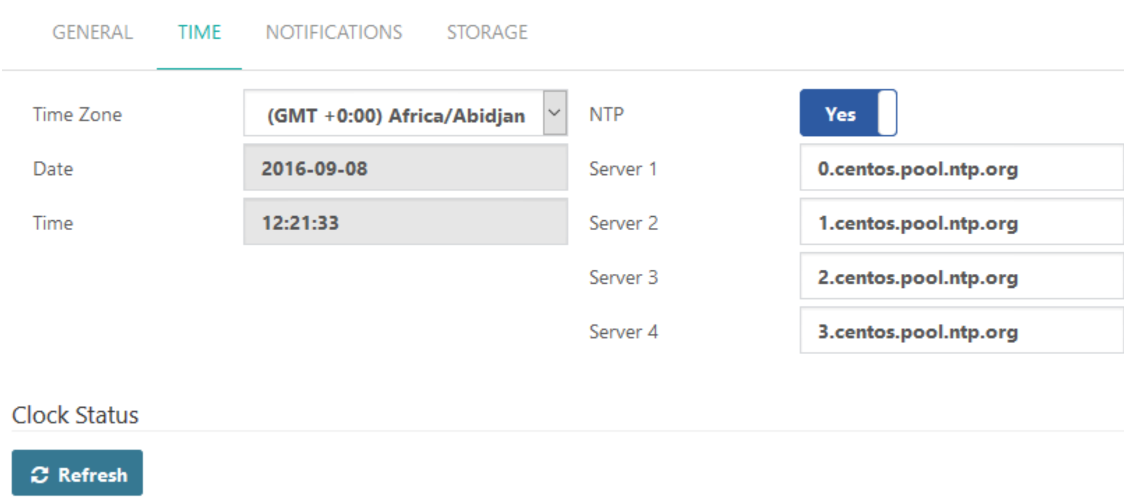


clicking on the Power Off button will completely shut down the PBX server

clicking on the Restart button will cause the PBX server to shutdown, before performing a restart.

TIME Tab

In this tab you will find the information about System Miscellaneous Settings. You can also use the buttons at the bottom of the dialog to shutdown or restart the system.



Time Zone, shows the actual time zone on server. You can change this setting and click on Update to update the system.

Date, shows the current date of the system. You can change this setting and click on Update to update the system.

Time, shows the current time of the system. You can change this setting and click on Update to update the system.

NTP, indicates whether to activate the NTP (Network Time Protocol) service for synchronizing the system clock.

Server 1, is the first IP address to be used by the NTP service

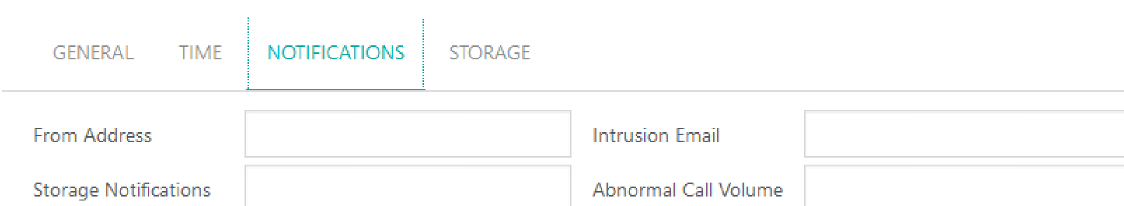
Server2, is the second IP address to be used by the NTP service

Server 3, is the third IP address to be used by the NTP service

Server 4, is the fourth IP address to be used by the NTP service

Clock Status, shows the current date and time settings for the PBX server

NOTIFICATIONS Tab



From Address, the email address entered here will be used as the "From:" address for emails sent by the system

Storage Notifications, notifications will be sent to the email address entered here if your hard drive is low on space or the RAID has been broken.

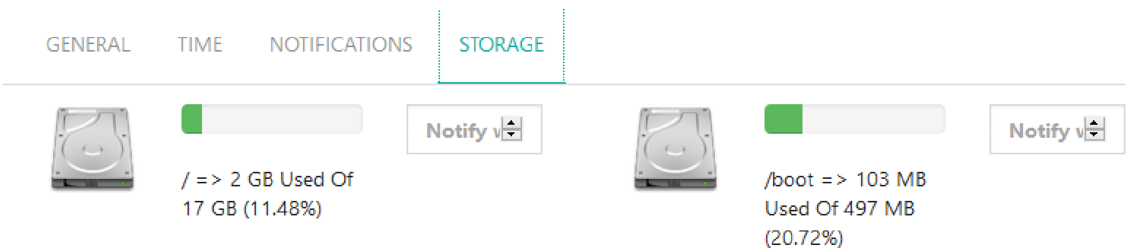
Intrusion Email, notifications will be sent to this email address when the Intrusion Detection services are activated, or when an intruder is detected.

Abnormal Call Volume, notifications will be sent to this email address to notify you about abnormal call volumes.

STORAGE Tab

Provides visual information about the capacity and utilization of the storage devices on your system.

For each device, you can configure the utilization threshold for notifications. You will receive an email notification when the utilization is greater than the configured value.



Network Settings Dialog

The Network Settings dialog allows you to configure the network environment of the PBX server.

What is a Private IP Address?

When you send a letter from your house to a friend, you have to know the address to send it to so that the postman knows which street and which house to take it to. Computer networks such as the Internet are no different, except instead of sending your Web traffic to a street address, your computer's "location" is known by its IP address.

In theory, your individual computer has to have its own unique IP address so that it will only receive the information that is meant for you. You don't want your emails and the responses to your Google searches going anywhere else.

However, there is a major exception to this: That would be those network computers that are linked to a router and share the same IP address. Included in that number are home/office networks. All routers have an IP address built in.

In this instance, the router—once it has established its Internet connection through an Internet Service Provider—sends data to each individual device on that network based on something called Network Address Translator (NAT).

The organization that doles out IP addresses to the world reserves a range of IP addresses for private networks. Private networks can use IP addresses anywhere in the following ranges:

- 192.168.0.1 - 192.168.255.254 (65,536 IP addresses)
- 172.16.0.1 - 172.31.255.254 (1,048,576 IP addresses)

- 10.0.0.1 - 10.255.255.254 (16,777,216 IP addresses)

The assumption is that these private address ranges are not directly connected to the Internet, so the addresses don't have to be unique. In today's world, these private address ranges are often used for the protected network behind network translation devices.

Because the private address ranges in a network don't have to be synchronized with the rest of the world, the complete address range is available from any network. A network administrator using these private addresses has more room for *subnetting*, and many more assignable addresses.

These blocks of addresses can be used by anyone, anywhere. Even if your neighbor is using the exact same addresses, it won't cause a problem. This is possible because these addresses are known as non-routable addresses. The network devices on the Internet are programmed to recognize these addresses. These devices (known as routers) will recognize that these are private addresses belonging to your network and will never forward your traffic onto the Internet.

You do need to obtain one real address from the general pool so that your home router can perform what is known as Network Address Translation (NAT). NAT is a process in which your router changes your private IP Address into a public one so that it can send your traffic over the Internet, keeping track of the changes in the process. When the information comes back to your router, it reverses the change—from a real IP address into a private one—and forwards the traffic back to your computer.

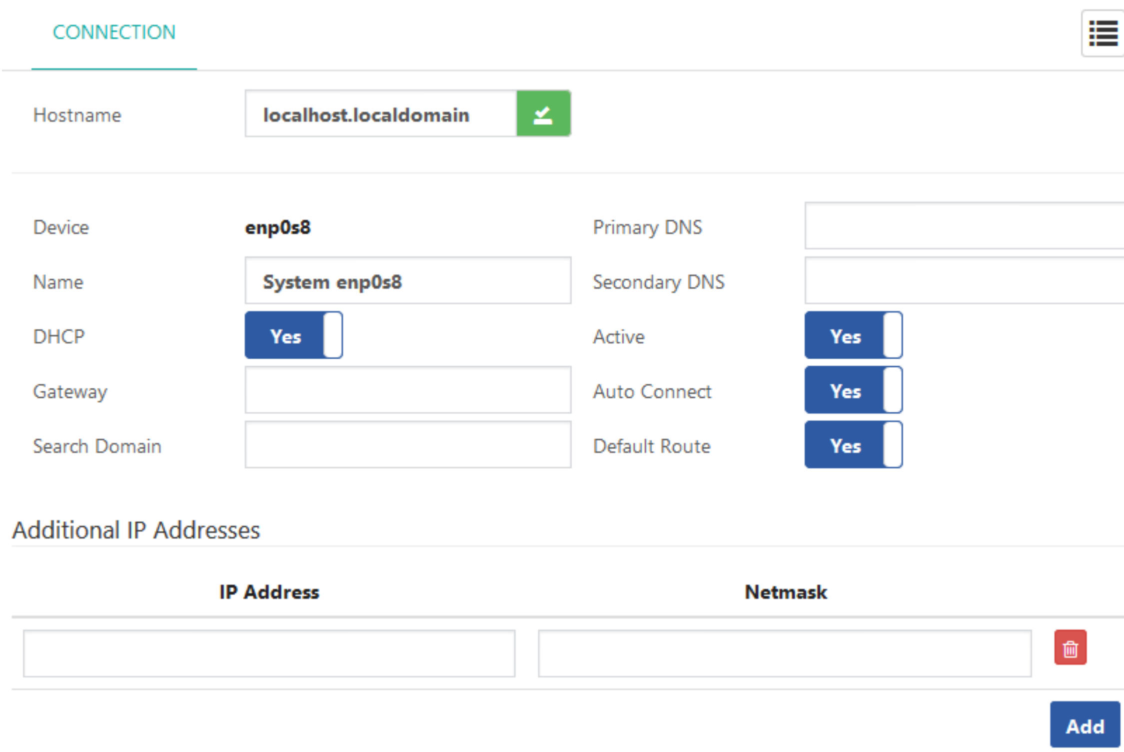
A typical home network router keeps two IP addresses: one for local devices to connect to across the local area network (LAN), and one for the external or wide area network (WAN) Internet connection.

The internal LAN-IP address is normally set to a default, private number. Linksys brand routers, for example, use 192.168.1.1 for their internal IP address. No matter the brand of router, its default internal IP address is listed in the manufacturer's documentation. Administrators have the option to change this IP address during router setup or at any time later. Unless someone manually changes it, however, this private LAN-IP address remains fixed.

The external WAN-IP address of the router is set when the router connects to the Internet service provider. This address can also be viewed on the router's administrative console. Alternatively, the WAN-IP address can be found by visiting a Web-based IP address lookup service—such as WhatIsMyIPAddress.com—from any computer on your network.

CONNECTION Tab

In this tab you will find the information about Network Settings of your system.



Hostname, hostname of the system.

Device, name of the connection, such as eth0, eth1, etc.

DHCP, whether to use DHCP on this connection for obtaining network configuration.

IP Address, IP address to assign to this connection.

Netmask, network mask or prefix.

Gateway, gateway IP address to use.

Search Domain, restrict DNS searches to the specified domain.

Primary DNS, primary DNS IP address.

Secondary DNS, secondary DNS IP address.

Active, whether this connection is currently active**.**

Auto Connect, whether to automatically connect on startup.

Default Route, whether to use this gateway as the default route.

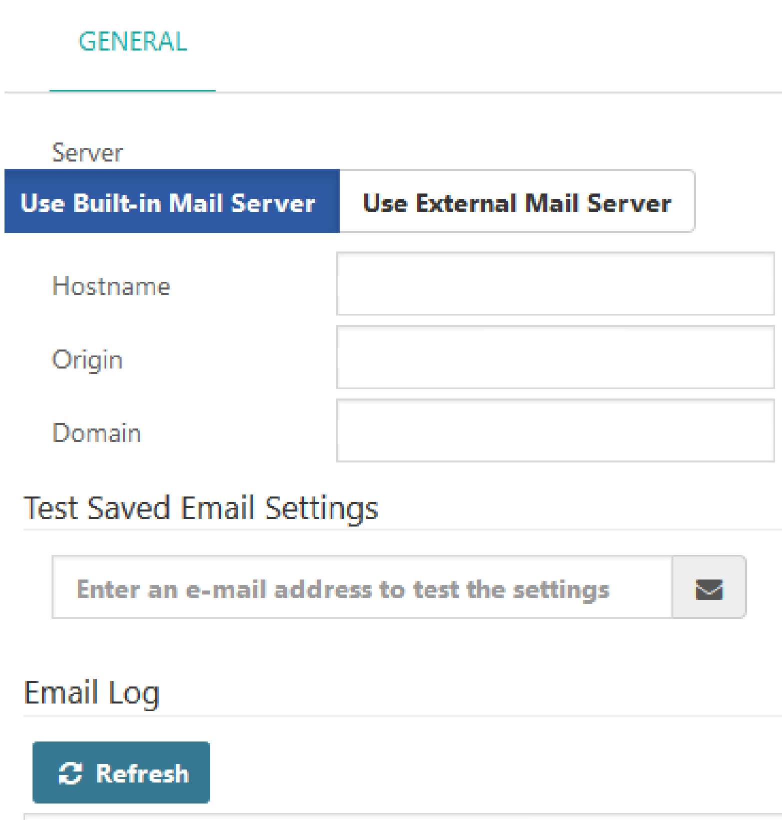
VLAND ID, VLAN ID for this connection**,** leave blank if you do not wish to use a VLAN.

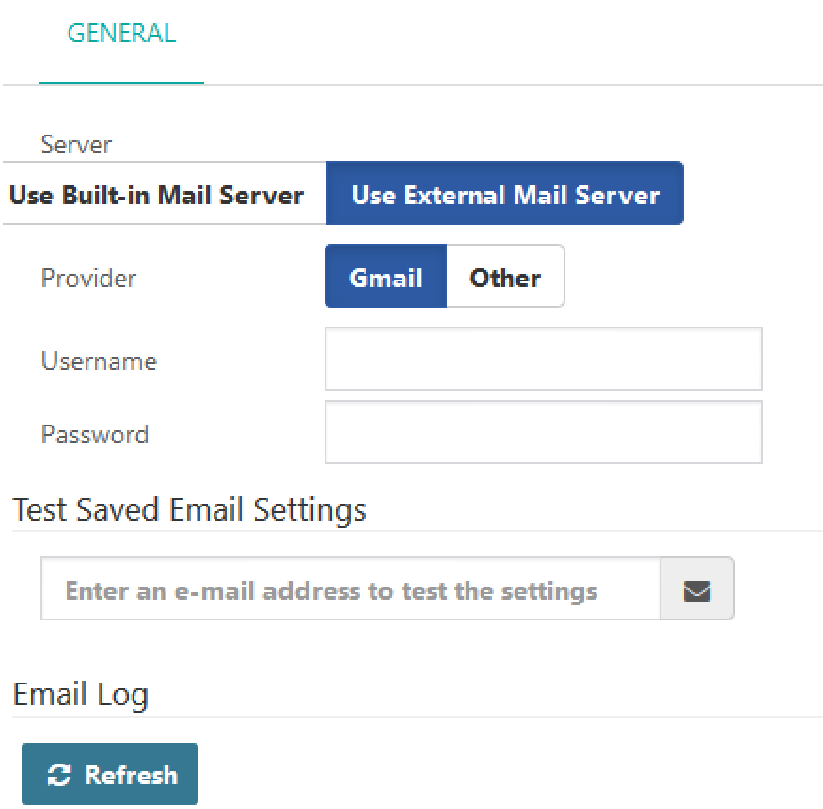
Email Settings Dialog

Email settings allows you the option to send outbound email messages either by using the built-in mail server (such as Postfix) that is active on the PBX server**,** or by using a network-accessible relay server that is hosted on another machine. Press on Use Built-in Mail Server to use the built-in mail server that is active on PBX, or Use External Mail Server to use a network-accessible relay server.

GENERAL Tab

In this tab you will find the information about email settings.





Server, you can relay outbound email messages either by using a built-in mail server (such as Postfix) that is active on the the system server**,** or by using a network-accessible relay server that is hosted on another machine.

Provider, provider can be Gmail**,** or any other provider. The only additional information required for Gmail is Username and Password.

SMTP Server, the address that your provider has given you to enable you to send outgoing emails.

Port, SMTP server IP port number. By default**,** port 25 is used.

Origin, specifies the origin domain for for all outgoing email. By default, origin is configured as your server hostname, e.g. pbx.mycompany,com. Some mail servers do a reverse lookup to authenticate email client, so you need to make sure that **origin** is externally accessible.

TLS, Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate**,** TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

Authentication, select the Use Authentication button if your email provider requires authentication (Username and Password) to send outgoing email.

User Name, username that your email service provider has given you to allow you to access your email account. Typically**,** this would be something like user@my-mail-server.com.

Password, the password that you use to log into your email account.

Test Saved Email Settings, testing the email settings. Note that this test will use ***saved*** email settings to send a test email to the address that you provide.

If you have updated the email configuration, you must save the settings before testing the configuration.

Email Log, display email event log.

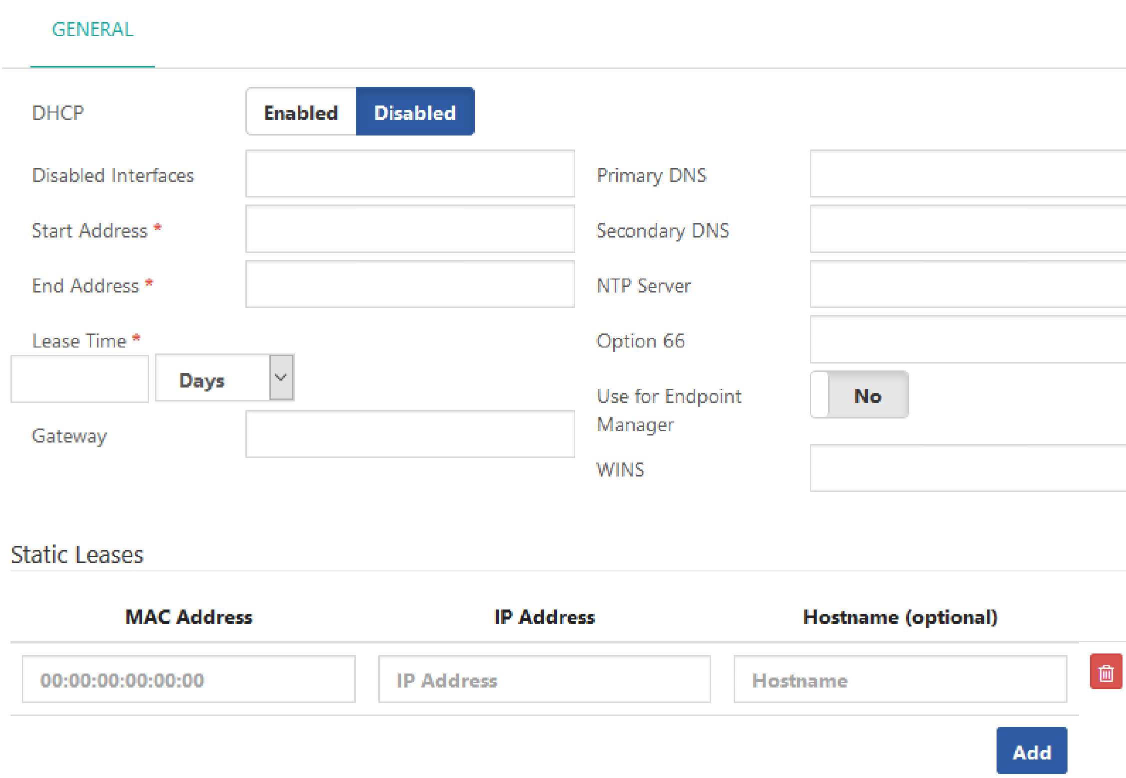
DHCP Settings Dialog

Dynamic Host Configuration Protocol (DHCP) is the mechanism that dynamically allocates physical IP addresses to machines and devices on the network. You can choose to use an existing DHCP server on your network, or to use PBX as your DHCP server. If you want to use PBX as your DHCP server, check on the Enable button.

Be careful – you can only have one DHCP server active on your network.

GENERAL Tab

In this tab you will find the information about DHCP settings.



DHCP, set to enable if you want the system to act as a DHCP server for this network, or Disable if you already have a DHCP server on this network.

Disables Interface, you can disable DHCP on one or more interfaces. If you wish to specify multiple interfaces, separate them with commas. For example: eth0,eth0.201

Start Address*, the first address on your network that can be allocated as a dynamic IP address.

End Address*, the last address on your network that can be allocated as a dynamic IP address.

Lease Time*, period that the DHCP server grants an IP address to a device. The device must renew its IP address before the end of the period.

Gateway, the default IP gateway address.

Primary DNS, domain Name System (DNS) translates Internet domain and host names to physical IP addresses in numerical notation, i.e. from mypbx.mydomain.com to 67.67.222.220.

Secondary DNS, define a Secondary DNS to be used if your primary DNS fails to respond.

NTP Server, network Time Protocol (NTP) is a networking protocol to synchronize clocks between computer systems over the Internet.

Option 66, option 66 provides IP phones with an URL for configuration provisioning. The system Endpoint Manager provides the IP phones with configuration information in response to a HTTP request. The format of the request URL in this case looks like http://[pbx-ip-address]/xepm-provision/. If you define the PBX IP address or host name in the Option 66 field and check the 'Use for Endpoint Manager' check-box then the correct format of the URL will be built automatically. If you have already-prepared IP phone configuration files located in the /tftpboot directory then you should put the PBX IP address or host name in the Option 66 field and uncheck the 'Use for Endpoint Manager' check-box.

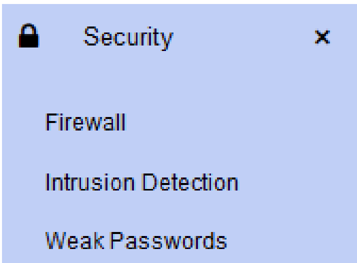
Use for End Point Manager, automatically format the Option 66 address for Endpoint Manager based on the address provided for Option 66 above. This will be done by prefixing http:// to the Option 66 address above and appending /xepm-provision/. In order for this to work correctly**,** the IP address provided above for Option 66 should only consist of the IP address or hostname of the server.

WINS, windows Internet Name Service (WINS) is a name resolution service that maps NetBIOS names to an IP address on the network that uses NetBIOS over TCP/IP (NetBT). The primary purpose of WINS is to support clients that run older versions of Windows and applications that use NetBIOS.

Statics Leases

- **MAC Address,** device MAC address.
- **IP Address,** device IP address.
- **Host Name (optional),** host name.

Security Menu Group

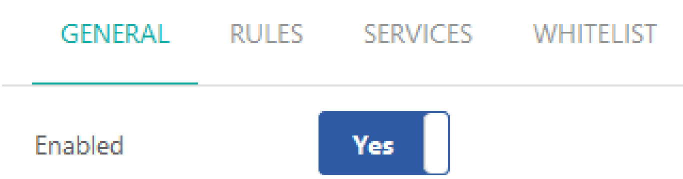


Firewall Dialog

The system is preconfigured with a built-in firewall. You can choose to disable this built-in firewall by setting Enabled to No, followed by the Save button.

GENERAL Tab

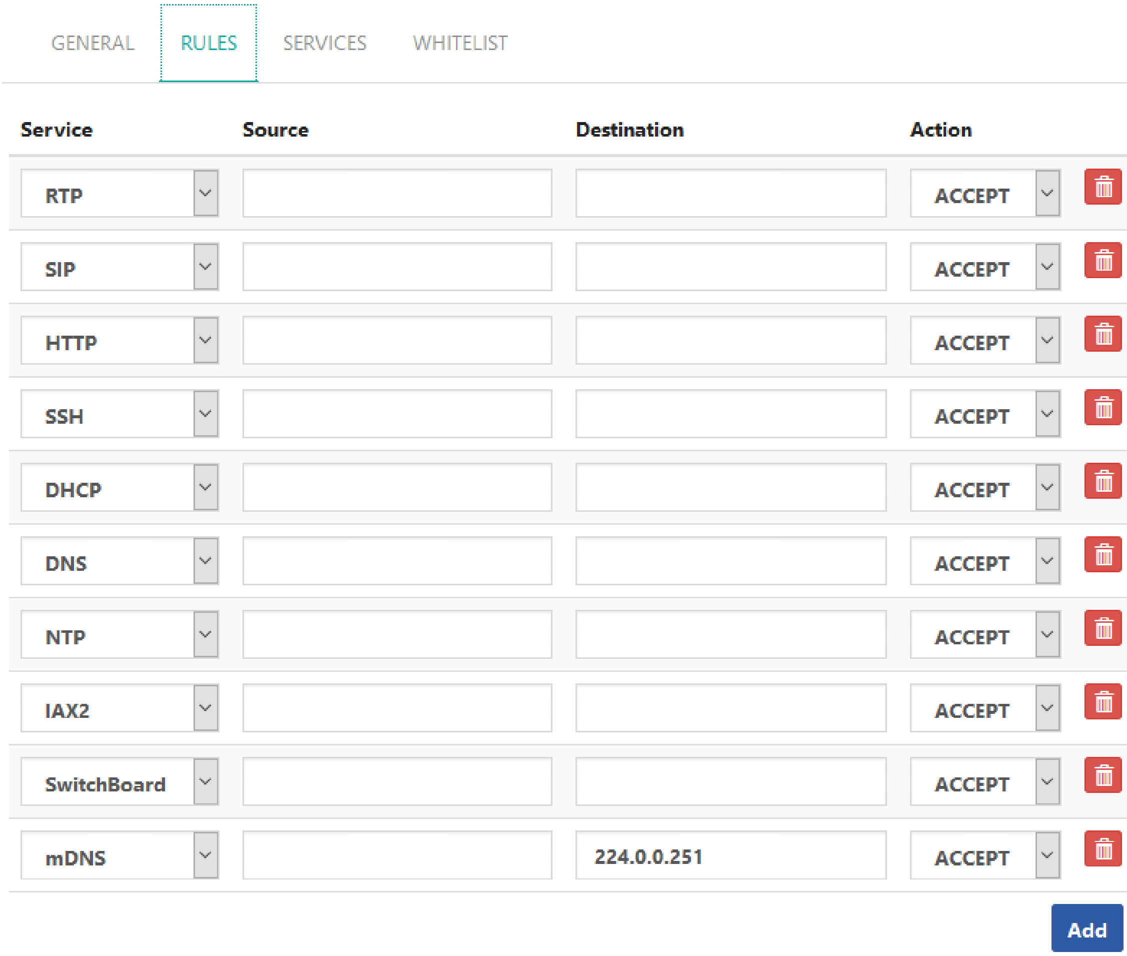
In this tab you will find the information about Firewall status.



Enabled, toggle to enable or disable the firewall.

RULES Tab

If the firewall is enabled, you can define multiple Services, on which you can base Rules. The system is preconfigured with a number of standard Services and Rules. You may want to add additional Rules that are specific to your installation. To add a Rule, press on the Add button at the end of the list of Rules that have already been configured in the system.



Service, is selected from a drop-down box. The drop-down box is populated with the Services that have been defined in the Services tab.

Source, is used if you want the rule to be restricted to access attempts from a specific IP address or subnet only.

You can leave this field blank, or use Any, to make the rule apply all IP addresses.

To restrict the rule to a specific IP address type in the IP address.

You can define a range of IP addresses by adding a subnet mask, i.e. 10.0.0.0/24 to restrict the rule to IP addresses in the range from 10.0.0.1 to 10.0.0.254

In most cases you will probably want to define IP address as Any.

Destination, is used if you want the rule to be restricted to access attempts to a specific IP address or subnet only.

You can leave this field blank, or use Any, to make the rule apply all IP addresses.

To restrict the rule to a specific IP address type in the IP address.

You can define a range of IP addresses by adding a subnet mask, i.e. 10.0.0.0/24 to restrict the rule to IP addresses in the range from 10.0.0.1 to 10.0.0.254

In most cases you will probably want to define IP address as Any.

Action, configures whether this rule should Allow, Deny, or Reject access.

- Accept will unconditionally accept all packets that match the definition of the Rule.
- Drop means that the packet is discarded, but no response will be given to the originator of the request. Dropping packets increases the cost (to the originator of the packet) of doing probes as it takes longer to probe a machine. On the other hand, Reject is more "friendly" to legitimate connection requests, as a detailed error message is provided.
- Reject means that the packet is discarded, and a response will be given to the originator of the request. Reject is more "friendly" to legitimate connection requests, as a detailed error message is provided.

SERVICES Tab

Enables you define Services, by defining the protocol used by the Service (i.e. TCP, UDP, or Both), and the port/s on which the Service operates.

GENERAL RULES SERVICES WHITELIST

Name	Protocol	Port
SIP	Both	5060
DNS	Both	53
NTP	UDP	123
DHCP	UDP	67-68
HTTP	TCP	80
SSH	TCP	22
RTP	UDP	10000-20000
IAX2	UDP	4569
SwitchBoard	TCP	4445
mDNS	UDP	5353

Add

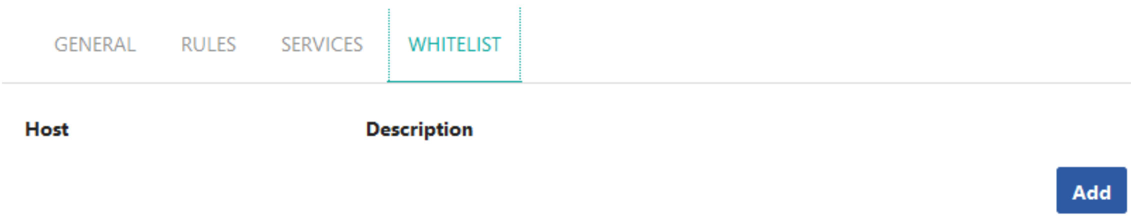
Name, give the Service a meaningful name to help you to easily recognize it. This name will be used to refer to the Service in the Rules table.

Protocol, determines the protocol that will be used by the application. The protocol options are TCP, UDP, or Both.

Port, the IP ports that are used by the Service. This can be defined as a single port (e.g. 80), a range of ports separated by a dash (e.g. 10000-20000), or a list of ports separated by commas (e.g. 80, 10000-20000, 5060).

WHITELIST Tab

This enables you to create a list of IP addresses that should always be ignored by the firewall.



Host, IP or Subnet.

Description, a short description to help you identify the whitelisted host.

Intrusion Detection Dialog

Intrusion Detection configures the fail2ban application, which detects, and blocks, unauthorized attempts to access the system. Fail2ban is a highly versatile tool to help prevent brute-force attacks as they occur. Rather than alerting an administrator after the damage may already be done, fail2ban can take proactive steps to deny access to the system from the attacking IP address.

After a potential intruder has been detected, the intruder's IP address will be blocked from further access to the system for the ban period (defined in minutes).

Apart from the financial damage that can be caused by someone actually breaking into your system, there is also a performance 'cost' to be considered. Even if an attacker is unable to find valid extensions or guess passwords, the activity created in the process of trying to break into your system can cause a high load on your server.

Fail2ban can drastically reduce the potential for damage from such attacks by limiting the number of invalid login attempts to a small number, and then by blocking the attacking IP address for a period of time.

This is done by adding rules to iptables. By default, fail2ban inserts rules at the top of the iptables chain, so they will override any rules you have configured in iptables. This is good because you may allow all sip traffic, but fail2Ban will be able to block individual hosts after they have been detected trying to make an attack.

Although iptables is an integral part of the installation, you must ensure that it activated, by making sure that the internal firewall is enabled.

Asterisk does not have built-in tools to prevent these attacks. However, it does a very effective job of logging these potential attacks, enabling fail2ban to detect them, and take appropriate action.

Fail2ban provides a way to automatically protect the server from unwanted activity. Fail2ban is an open source intrusion detection framework that works by scanning log files and reacting to unwanted actions such as repeated login failures, and bans failure-prone addresses. Fail2ban updates firewall rules to reject the IP address or can execute user defined commands.

Fail2ban is configured to monitor various logs, including:

- /var/log/asterisk/full (Asterisk)
- /var/log/secure (ssh)
- /var/log/httpd/error_log (apache)
- /var/log/httpd/*access_log (apache)
- /var/log/vsftpd.log (vsftpd)

Fail2ban is preconfigured with files that contain known error strings, and searches the logs for occurrences of those messages. For example, the Asterisk logs are scanned for messages that contain the following texts:

- Registration from '.*' failed for <HOST>
- No registration for peer
- Host <HOST> failed MD5 authentication

This would detect events that could be the result of:

- Incorrect password
- Mismatch between username and security No
- matching peer found in system database Peer
- is not supposed to register on the system
- Device does not match ACL
- MD5 authentication failure - Digest Authentication is a feature of the SIP protocol enabling password not to be sent in clear text.
- Device attempting to login that is not configured to use the specific transport type

The default fail2ban configuration file is located in /etc/fail2ban/. All configuration changes are managed from the user interface, which updates the local copy of the jail file (jail.local). Manual changes should not be done to jail.conf, as they will be overwritten by the user interface.

A potential intrusion is defined as a user-defined number of unsuccessful attempts to access the system within a user-defined period of time (defined in seconds).

An email alert will be emailed to the defined email address after a potential intruder is detected.

You can create a whitelist of addresses that will be ignored by this dialog. Typically, you should include the PBX itself in the whitelist, by adding 127.0.0.1 to the whitelist.

GENERAL Tab

Enabled, indicates the current status of the service,

Number of Failed Attempts Allowed, number of attempts that will trigger a ban. It is the number of incorrect login that a host is allowed to attempt during the **Find Time** before being considered to be an intruder, and getting banned for the length of time defined by **Ban Time**.

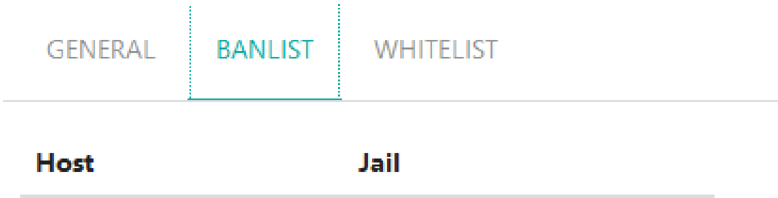
Over a Period of (in seconds), time period over which the number of attempts will trigger a ban. This parameter sets the length of time that a host is monitored for, before the clock is reset. The default setting is 600 seconds (10 minutes).

Will Ban the Host for (in seconds), is the number of seconds that a host is blocked from accessing the server if the host is found to be in violation of any of the rules. This is especially useful in the case of bots, as once they are banned, they will simply move on to the next target. The default is set to 1800 seconds (30 minutes) – you can increase this to one hour (or higher), if you like..

And Send a Notification Email to, address to which notifications will be sent each time that a host address is banned. Multiple email addresses can be used – separate each email address with a , (comma).

BANLIST Tab

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 press on the Unban button to remove it from the list.



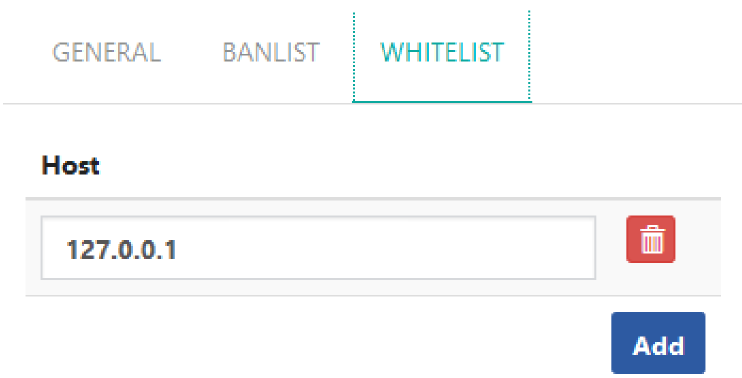
Host, list of banned IP addresses.

Jail, fail2ban rule that detected the instrusion.

, unban button. This allows you to select a banned IP address, and remove it from the list of banned IP addresses. You should only do this after you have found the cause for the ban, and you are sure that it is safe to unban the IP address.

WHITELIST Tab

List of IPs that will not be blocked by the instruction detection under any circumstances.



Host, IP address. This enables you to configure addresses that will be never be locked out by fail2ban, such as your personal IP address. Including your own IP address will guarantee that you do not accidentally ban yourself from your own server. By default, the Whitelist will always include your local host, i.e. 127.0.0.1. Enter each address on a new line.

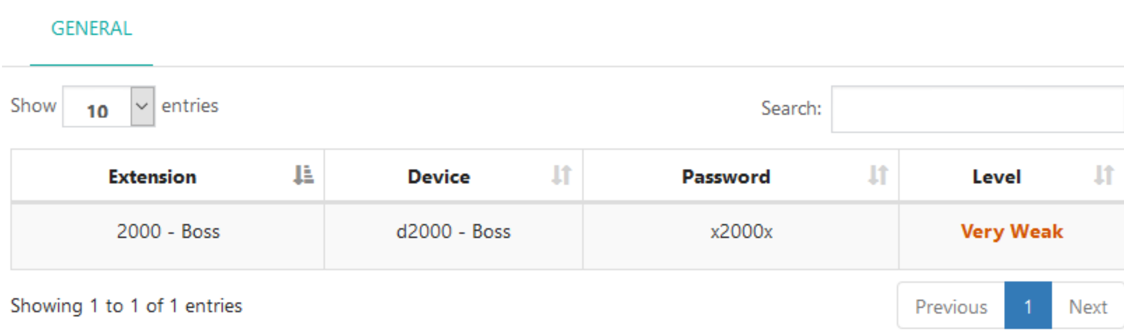
Weak Passwords Dialog

This dialog creates a visual report of any extensions, user accounts, or trunks that use weak registration passwords.

Accounts with weak passwords represent a potential security hole and should be updated as soon as possible.

GENERAL Tab

In this tab you will find a list of all extensions**,** user accounts**,** or trunks where the password does not match a minimum level of difficulty.



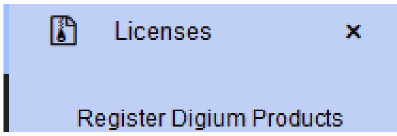
Extension, shows the Extension and Extension Name

Device, shows the User and Device Description

Password, displays the current password

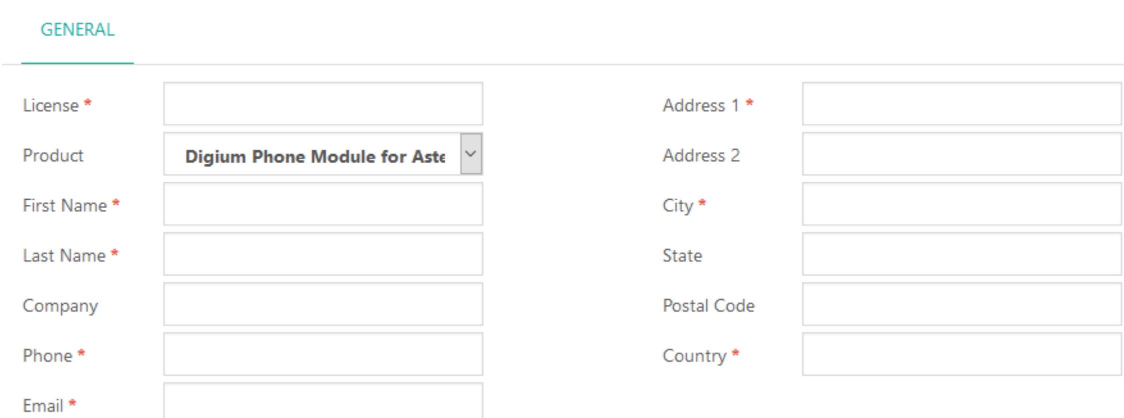
Level, indicates the security level of the current password

Licenses Menu Group



Register Digium Products Dialog

GENERAL Tab



License*, product license key that was provided by Digium.

Product, product for which you want to activate the license.

First Name*, your first name.

Last Name*, your last name.

Company, your company name.

Phone*, your phone number.

Email*, your email address.

Address 1*, first line of your office address.

Address 2, additional line of your office address.

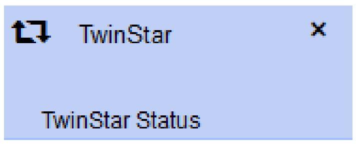
City*, city where your office is located.

State, state where your office is located.

Postal Code, postal code for your office address.

Country *, (2-letter) country code) for your office address.

Twinstar Menu Group

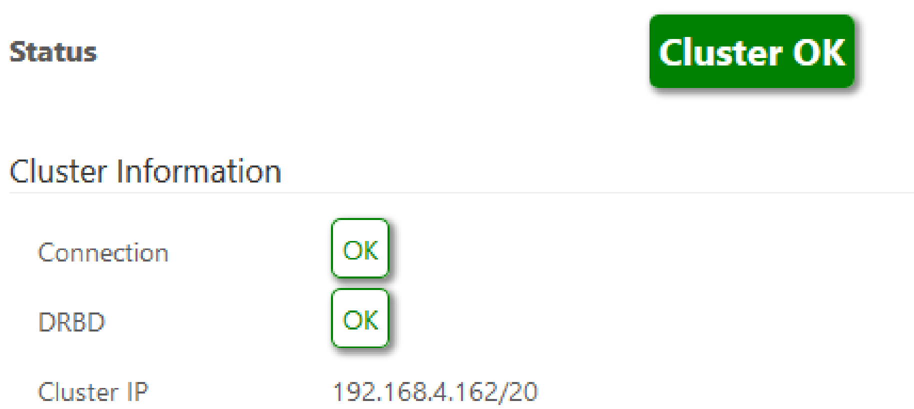


TwinStar Status Dialog

This dialog will only be shown in the Admin menu when you are managing a TwinStar cluster.

GENERAL Tab

Cluster Information Section



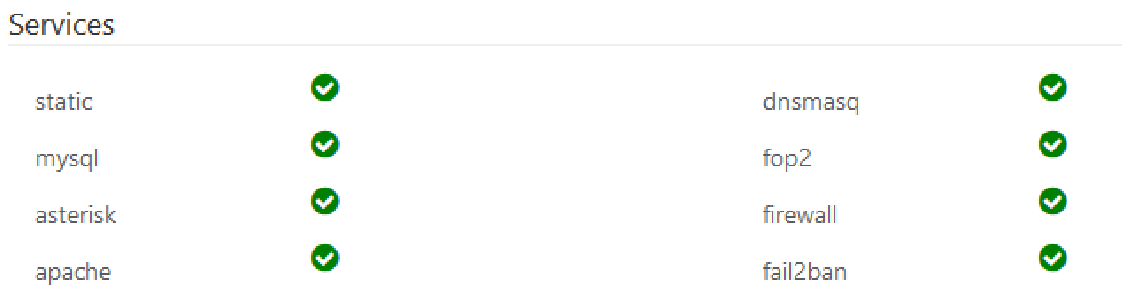
This section indicates the current status of the TwinStar cluster. If the TwinStar cluster does not have any problems, a green **Cluster OK** message will be displayed. However, if there are problems with the cluster, a red **Cluster Error** message will be displayed.

Connection indicates the current state of the connection to the TwinStar cluster.

DRBD indicates the status of the DRBD.

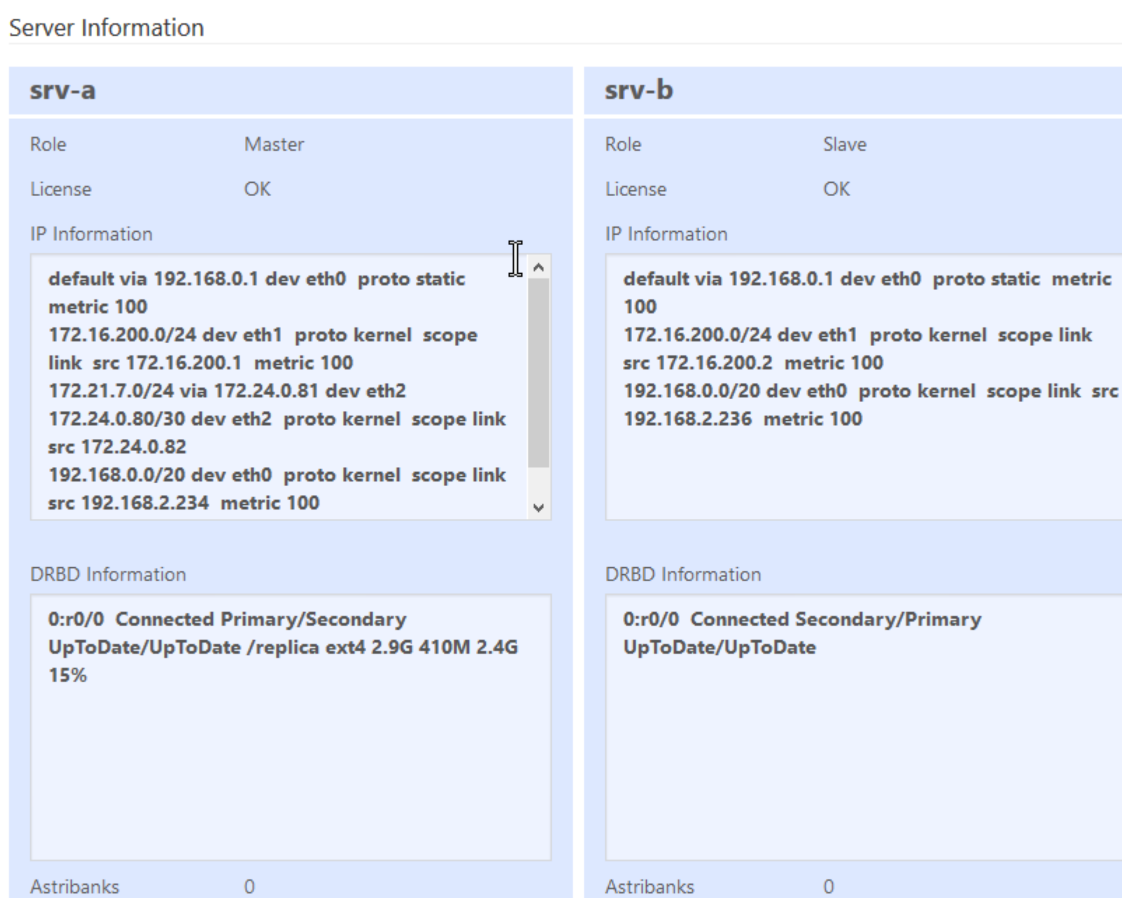
Cluster IP shows the IP address for the TwinStar cluster.

Services Section



This section displays the current status of all the services associated with the TwinStar cluster. All services that are behaving correctly will be shown with a green ✓ symbol. Any service that is not behaving in the correct manner will be shown with a red × symbol.

Server Information Section



This section displays information about each server in the TwinStar cluster.

Role indicates whether the server is acting as the Master or Slave within the TwinStar cluster.

License indicates the current state of the TwinStar license for each server

IP Information details the IP information associated with each server in the TwinStar cluster **DRBD Information** shows the current status of the DRDB (Distributed Replicated Block Device)

Astribanks shows the status of any D-Link Astribanks that are connected to the TwinStar cluster.

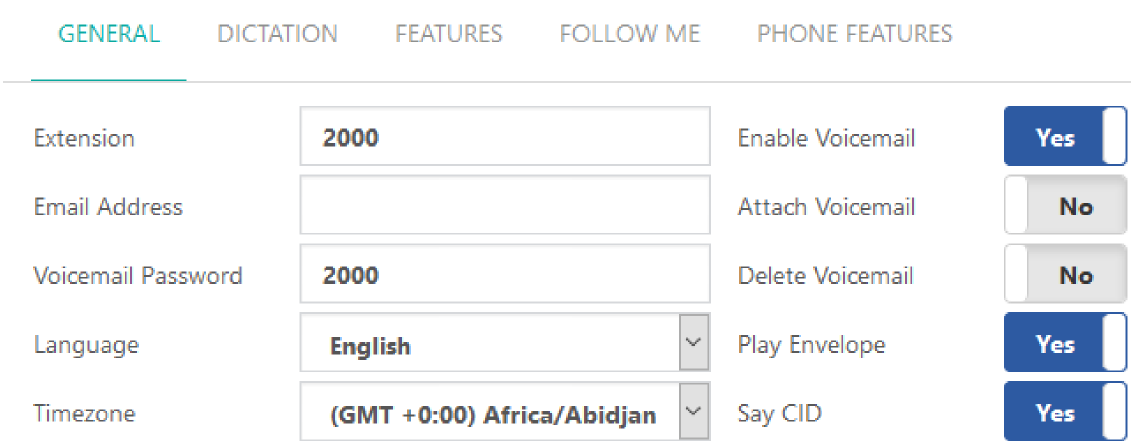
6. User Portal

Portal

Portal provides every extension user access to a number of dialogs to give them better control of the behavior of their extension. Each user is only able to see and modify settings that relate to their own extension, and cannot see or modify settings relating to extensions belonging to other users. The Portal also provides each user with access to lists of their emails, call history, and faxes.

My Extension Dialog

GENERAL Tab



Extension, displays the number of the current extension. This field cannot be modified.

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

Only one address can be entered into this field.

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

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

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

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

Timezone, timezone that should be associated with this user. This will affect timestamps displayed in the CDR Report, Dictation, and Voicemail.

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

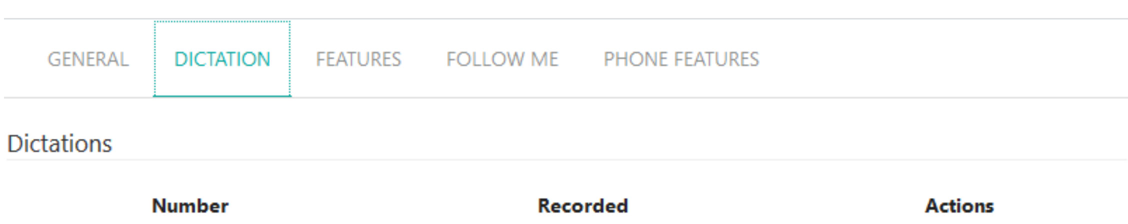
Attach Voicemail, determines whether the voicemail recording will be attached to emails.

Delete Voicemail, causes the voicemail to be deleted from the server after the voicemail has been delivered. Be careful with this option, because the system may delete the message without guaranteeing that a copy of it has been attached to an email notification, or that the email has been delivered successfully. This could mean that after a message is left, and the system has made an attempt to send a notification email to the user, that the actual voicemail that was left may no longer be accessible.

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

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

DICTATION Tab



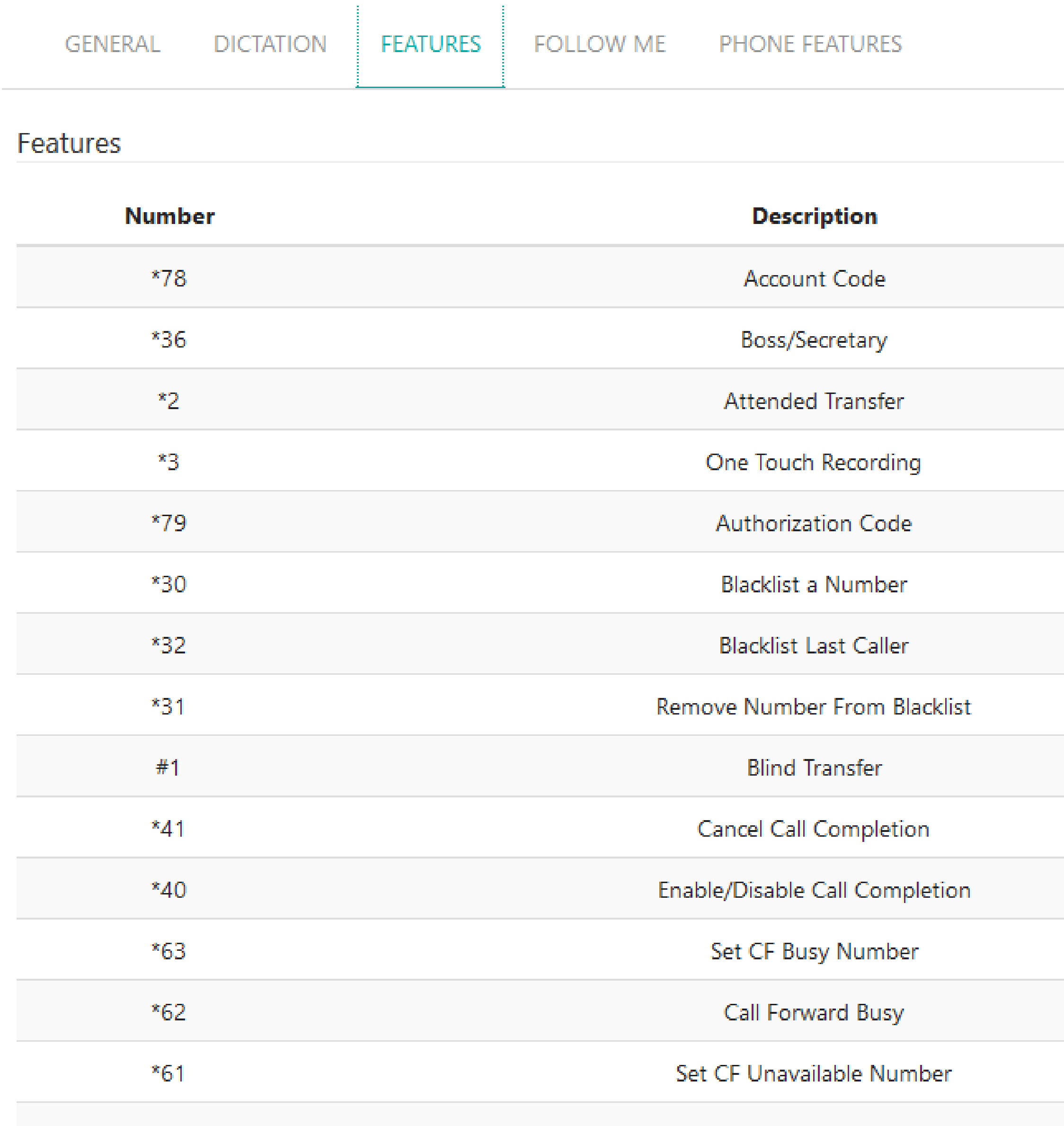
Dictations Section

Number, a system-allocated number used to uniquely identify each dictation.

Recorded, timestamp to indicate when the dictation was recorded.

Actions, action that can be performed on each dictation.

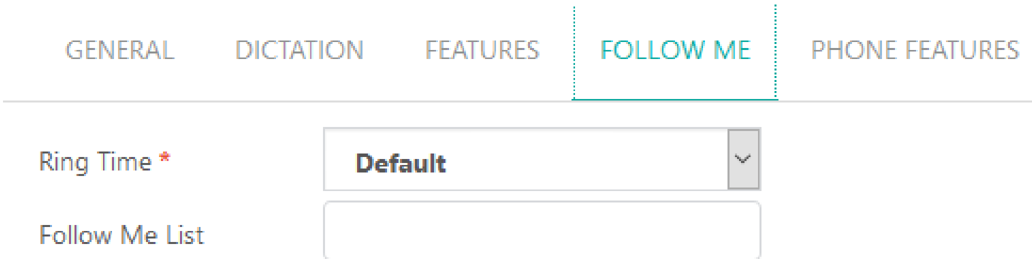
FEATURES Tab



Number	Description
*78	Account Code
*36	Boss/Secretary
*2	Attended Transfer
*3	One Touch Recording
*79	Authorization Code
*30	Blacklist a Number
*32	Blacklist Last Caller
*31	Remove Number From Blacklist
#1	Blind Transfer
*41	Cancel Call Completion
*40	Enable/Disable Call Completion
*63	Set CF Busy Number
*62	Call Forward Busy
*61	Set CF Unavailable Number
*60	Call Forward Unavailable

Lists all the feature codes that are available for this extension.

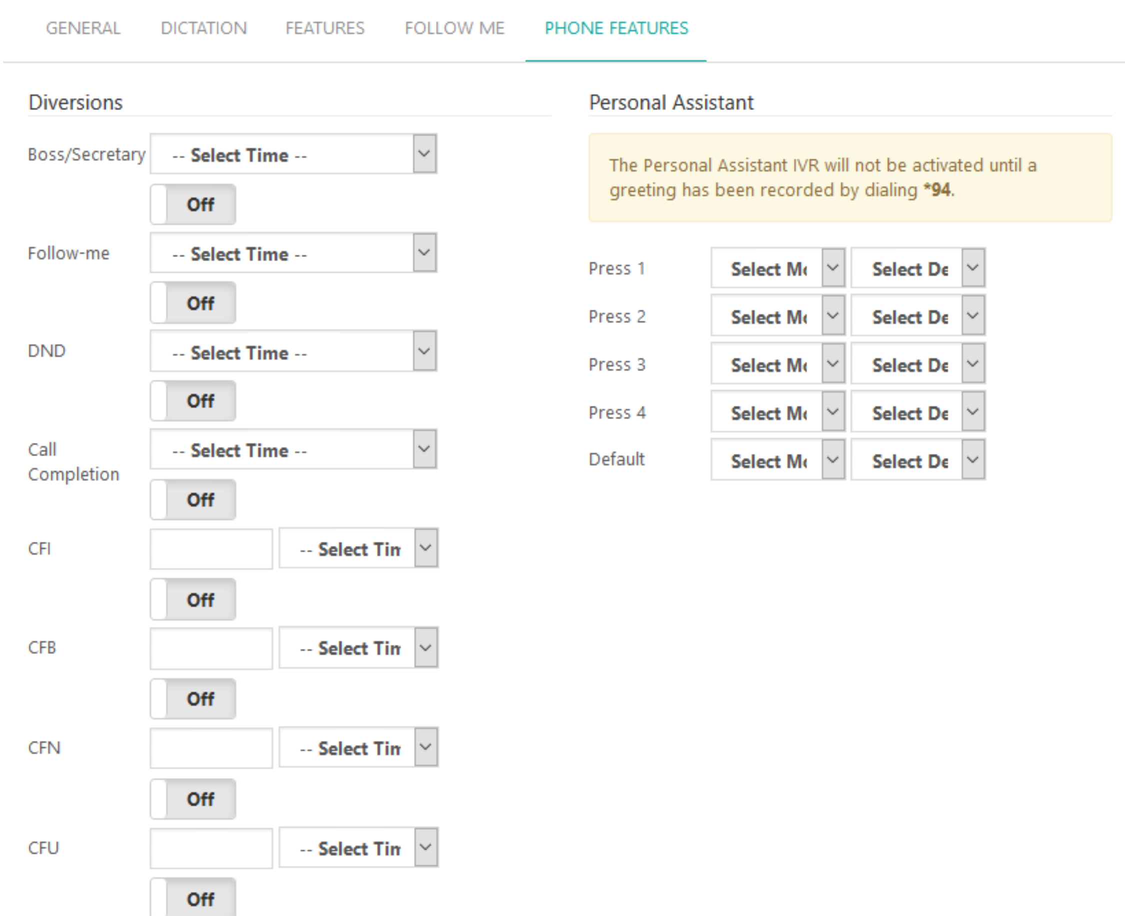
FOLLOW ME Tab



Ring Time*, determines how long to ring the numbers listed for follow me, before continuing to an alternative destination, such as voicemail or hangup.

Follow Me List, list of numbers to which the call be sent. Can be an internal extension, any other internal destination (such as a ring group, queue, etc.) or and external number. When defining an external number, take care to include any codes that may be necessary to call out to an external number.

PHONE FEATURES Tab



Diversions Section

There are two settings that you can configure for each type of diversion.

- If you wish, you can restrict the activation of a diversion setting to a specific span of time, by using a time group (which you can create in the My Time Group dialog)
- Each diversion setting can be activated (**On**) or disabled (**Off**)

Boss/Secretary, sends calls to the Secretary extension if the system administrator has defined a Boss/Secretary relationship for this extension. (This is similar to using the standard system feature code ***36**)

Follow Me, diverts incoming calls to the list defined in the Follow Me dialog.

Do Not Disturb, prevents incoming calls from ringing your phone. Incoming calls will be treated as if you are not available.

Call Completion, call completion allows a caller to let the system automatically alert him when a called party becomes available**,** after a previous call to that party failed for some reason. You can use the On/Off switch (together with a time group) to determine whether to receive such notifications.

CFI, (Call Forwarding Immediately) determines whether to activate call forwarding immediately. In other words, call forward will always be activated.

CFB, (Call Forwarding when Busy) determines whether to activate call forwarding when your extension is busy.

CFN, (Call Forwarding when No Answer) determines whether to activate call forwarding when you do not answer your extension.

CFU, (Call Forwarding when Unavailable) determines whether to activate call forwarding when your extension when your extension is not available. You could be "not available" because you have activated Do Not Disturb, or because your phone is not currently logged into the phone system.

Personal Assistant Section

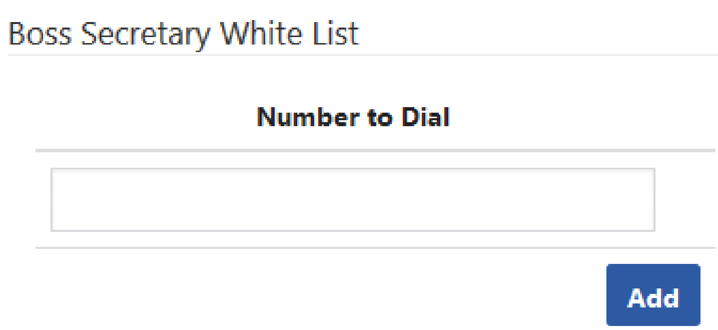
This enables you to create a personal IVR (Interactive Voice Response) menu that allows you redirect your callers in response to input from them. Before you can create a personal IVR, you must use the ***94** feature code to create a recording that will describe the available options to your callers.

It is important that you carefully plan the call flow and branching options for IVRs, while considering the user experience.

If you wish, you can restrict the activation of the Personal Assistant to a specific span of time, by using a time group (which you can create in the My Time Group dialog)

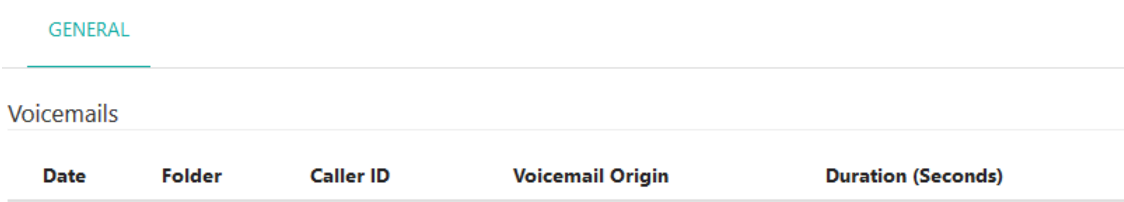
You can define how the system will behave when the caller presses any digit between 1 and 4. Additionally, you can define default behavior should be used if the caller enters an invalid option, or fails to respond.

Boss Secretary White List Section



My Voicemail Dialog

GENERAL Tab



Voicemails Section

Lists voicemail messages that have been left for you. You can use this dialog to listen to voicemail recordings by clicking on the icon to the right of each voicemail message.

Date, timestamp of the voicemail message.

Folder, current location of the voicemail message. Voicemail messages that have not been moved to another folder will initially be located in the INBOX location.

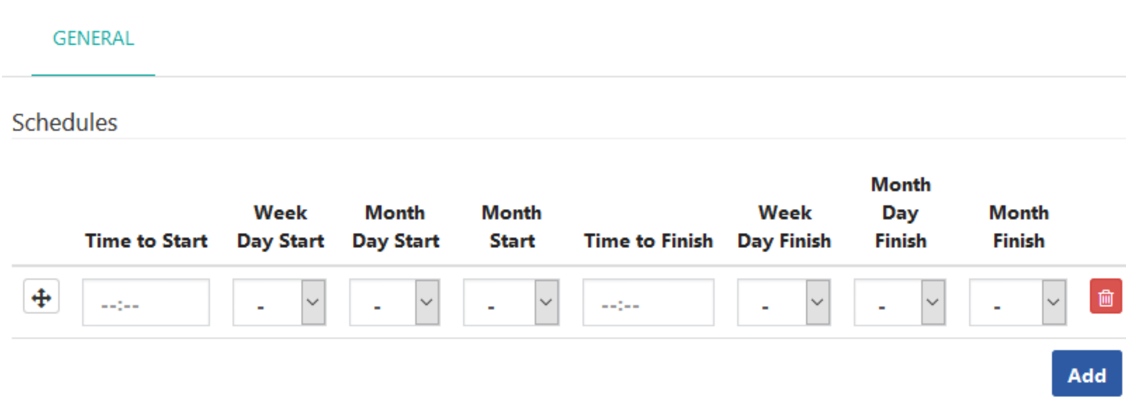
Caller ID, the full caller ID of the person who left the voicemail message.

Voicemail Origin, the phone number from which the voicemail message originated.

Duration (Seconds), the duration, in seconds, of the voicemail message.

My Time Group Dialog

GENERAL Tab



Schedules Section

Allows you to specify a period of time that can be used when configuring call diversions.

Time to Start, the time when the schedule should begin.

Week Day Start, the day of the week (i.e. Monday, Tuesday, Wednesday, etc.) when the schedule should begin.

Month Day Start, the day of the month (i.e. 1, 2, 3, etc.) when the schedule should begin.

Month Start, the month (i.e. January, February, March, etc.) when the schedule should begin.

Time to Finish, time when the schedule should end.

Week Day Finish, the day of the week (i.e. Monday, Tuesday, Wednesday, etc.) when the schedule should end.

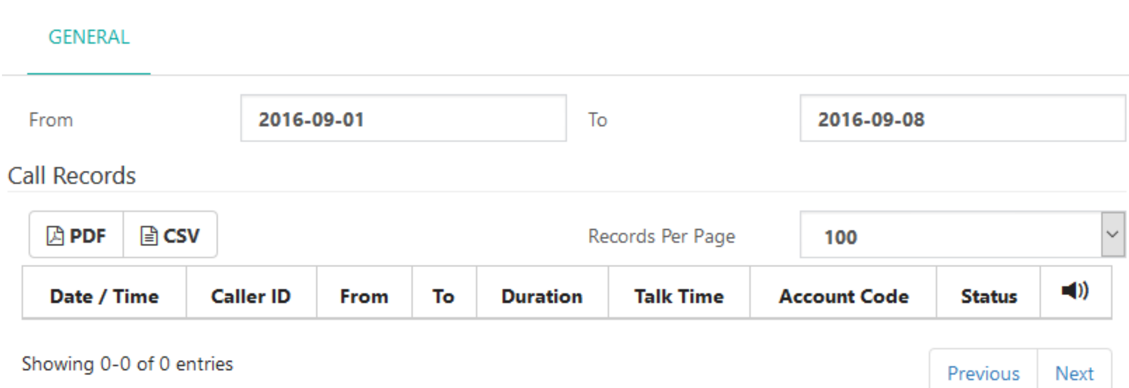
Month Day Finish, the day of the month (i.e. 1, 2, 3, etc.) when the schedule should end.

Month Finish, the month (i.e. January, February, March, etc.) when the schedule should end.

If any of the fields are left blank, the system will assume that the field is not relevant. For example, if you define Time to Start, but leave Week Day Start empty, the schedule will start at the start time ***every*** day of the week.

CDR Dialog

CDR Tab



From, sets the start date for the CDR records that you want to view.

To, sets the end date for the CDR records that you want to view.

After changing one (or both) of these parameters, you will need to click on the **Search** button at the bottom of the screen in order to refresh the data that is displayed.

Call Records Section

Clicking on either the PDF or CSV will output the data (that is currently displayed on your screen) into a file of the chosen format. The file will be saved in your download directory, with the name of either CDR Records.pdf or CDR Records.csv

Fax Settings Dialog

Fax Master is a commercial module that is licenced by D-Link. This dialog will not be active unless a valid licence is linked to the system.

GENERAL Tab

Fax Notifications Section

Outgoing Notification, when set to **Yes**, sends a notification to the email associated with the extension when an outbound fax has been sent.

Incoming Notification, when set to **Yes**, sends a notification to the email associated with the extension when an inbound fax has been received.

Coversheet Settings Section

Name, the sender's name that will be displayed on the coversheet of outgoing faxes

Phone Number, the phone number that will be displayed on the coversheet of outgoing faxes. This is the phone number that the recipient of the fax should call if he wants to contact the sender of the fax.

Email, the email address that will be displayed on the coversheet of outgoing faxes. This the email address to which the recipient of the fax should send an email to if he wants to contact the sender of the fax.

Reply-to Fax Number, is the fax number which will be displayed on the coversheet from which outbound faxes will appear to be sent, to enable the recipient to reply by fax

Preview Coversheet, pressing this button allows the user to see a preview of their own personalized coversheet

My Faxes Dialog

Fax Master is a commercial module that is licenced by D-Link. This dialog will not be active unless a valid licence is linked to the system.

GENERAL Tab

Send Fax Section

Destination*, is the full fax number of the person to whom you are sending the fax. Do not forget any code that may be required by your phone system to access external lines or to access international service providers.

Include Coversheet, indicates whether you want to add your standard coversheet to this fax

File to Send*, allows you to browse to the file that you want to send as a fax. The file must be in pdf format. Click on the (+) icon to include additional pdf documents in the fax, or click on the trash icon to remove a document that you have previously added.

Note the **Add** button that allows you add additional documents to the fax.

Filter Faxes Section

Use this filter option to display just the faxes that you are interested in. If you leave any value empty, then all values will be displayed

From Date, limit the display to only display faxes sent (or received) after the **from** date

To Date, limit the display to only display faxes sent (or received) before the **to** date

Source, insert a single value to display faxes sent from a specific source

Destination, insert a single value to display faxes sent to a specific destination

Stored Faxes Section

Records Per Page, limit the numbers of faxes to be displayed on each screen

Direction, 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.

Date/Time, displays the timestamp when the fax was received (in the case of an inbound fax), or sent (in the case of an outbound fax.)

Preview, clicking on the icon allows you to view the complete fax that was sent, including the coversheet (if requested) and all documents, in pdf format.

Resend/Forward, clicking on the icon allows you to resend the fax, or forward it to a new recipient

Delete, allows you to completely remove the stored fax from the system by clicking on the trash icon

Switchboard

Switchboard Dialog

After a successful login, you will be presented with the panel window. There is a toolbar that is always visible at the top, and four sections in the content area: one for each kind of button.

General Tab

The button corresponding to your extension (the one you used to login), is always at the top left of the Extension block. Its label will be highlighted with a bold font.

Each block has a title bar with a plus/minus button to the right. Clicking on the button will collapse or expand the view of the section. The collapse state is remembered across all future sessions. Suppose that you are not interested in trunks: you can collapse the section and it will remain minimized until you click the plus sign again.

Anatomy of the Toolbar

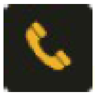
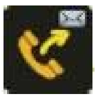
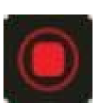
At the top of the panel there is a toolbar. From here you will perform most of the actions that can be done with the Switchboard. There are some distinctive sections as follows:

Action bar

The action bar consists of a row of buttons that represent actions that can be taken for active calls. The buttons will be displayed only is the user has been given permission for the action. To activate an action, you need to first select the destination or target button with a click of the mouse. After you have done that, the borders of the target button will turn to red.

After selecting a target extension, you can perform your command by clicking on the appropriate action button. The following actions are available:

Button	**Action**
 Dial	Required permission: **dial** Will originate a call to the button previously selected from the list of available extensions. Your phone will ring and after you pick it up, it will call the requested destination extension

Button	**Action**
 Transfer	Required permission: **transfer** Will initiate a call transfer to the button previously selected from the list of extensions
 Transfer to voicemail	Required permission: **transfer** Will initiate a transfer to the voicemail of the selected extension
 Pickup	Required permission: **pickup** Will pick up the ringing extension that was selected.
 Listen	Required permission: **spy** Will start a call-spying session. It will first ring your phone**,** and after you pick it up**,** it will start listening to the previously selected extension.
 Whisper	Required permission: **whisper** Will start a call-spying session with whisper enabled. It will first ring your phone and when you pick it up**,** it will start spying on the previously selected extension. You can then talk to the target extension without the other party hearing you.
 Hangup	Required permission: **hangup** Will hang up the first active call on the selected extension.
 Record	Required permission: **record** Will initiate or stop recording on the selected extension. A call that is being recorded will be marked with a cassette icon.

Filter Box

Type text in this input box to filter out any button having a label that does not match your filter. If you have a panel with a hundred buttons and you only want to see the state for “Bob”, just type “Bob” into the input box, and all buttons except those containing “Bob” will be hidden.

Dial Box

The dial box is powerful option, with multiple actions:

Option	Action
Dial to a phone number	When your phone is idle, just type in a number and press ENTER: your phone will ring and will originate a call to that number
Transfer to any number	When you are on an active call you can type in a number (either an internal extension or an external number) and press ENTER. This will transfer your current call to that number.
Invite any number to a conference	If you select a conference button, type a number in the dial box, and hit enter, the Switchboard will originate a call to the number typed, and will send the call to the selected conference.
Direct VoIP dial	Type a sip address with the format: SIP/$(ext)@$(domain) and the Switchboard will originate a direct sip call to that extension @ server.
Phonebook search	Anything you type here will be searched in the visual phonebook as you type, and results will appear as a selection list at the bottom of the box. You can use the arrow keys to select the proper result, and then click on ENTER to originate a call to the selected number.
.tel domain lookup	If you type a .tel domain, the system will perform a DNS domain lookup and display any matching results that are found. You can find voice numbers, direct VoIP dial, and Web sites. If you select a result and press enter, a call will be originated to the phone number, direct VoIP call, or the target Web page will be opened in a new window.

Presence Select Box

You can use this to set your presence information. The information is stored in the EasyVOIZ 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 EasyVOIZ to indicate that the device is in adhoc mode. This is an example button that is ringing:

The button has a number of elements:

Element	Explanation
1 - Presence icon	Indicates the presence state for the extension. Green circle means that the extension is not in a call. Red circle indicates that the extension is busy or in a call. Little card icon indicates a special presence that was set by the user. The color of the custom presence is configurable. If you mouse over the icon, a tooltip with the custom presence text will appear. Tape icon indicates that someone initiated a call recording from within the Switchboard, and that the call is now being recorded. Clicking on the presence icon will display an action menu: if you have the appropriate permission, you will be able to add, remove, or pause the member in a queue, or send an email to that user (if the email setting is defined in the button configuration).
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.

Element	Explanation
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 on envelope, indicates if there is voicemail waiting or stored for the extension. The number of messages is displayed in the tooltip when you mouse over it.
5 - Line activity icon	Indicates whether the line is ringing, is engaged in an outgoing call (right arrow), engaged with an incoming call (left arrow), or on hold (hourglass).
6 - Line callerid	Shows the callerid name and number, if available
7 - Line timer	Shows the timer for the current call.

Performing Actions

Buttons can be clicked to select or deselect them. When a button is selected, the border of the button will become red. Once a button is selected it will become the target button for any action that you choose.

Every button in the toolbar requires that a destination button also be selected. Clicking an action button with no extension selected will not trigger any action. Some actions will work only on the active line for that extension. For example, if an extension has two calls, and one of them is on hold, if you click the record button it will start recording only the active line and not the line on hold. The same happens with the hangup button: if you have two calls on your phone and one is on hold, clicking the transfer button will redirect your **active** call, and not the call on hold.

To transfer a call, when talking to someone, click on the target extension (which will be highlighted in red) and then click the transfer button on the toolbar.

To record a conversation to disk, click on the extension button that you want to monitor and then click on the record button on the toolbar.

Action Submenu

The presence icon for any type of button can be clicked to perform additional actions. A single click on the icon will cause a popup menu to appear, listing the available actions for the selected button. In this manner, you can add, remove or pause 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 cam 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.

7. Call Center Statistics

Introduction

EasyVOIZ Call Center Stats is a reporting system for monitoring call centers based on Asterisk. The system allows you to run reports on call center activity, divided by and filtered by agent and time, which shows a detail of what happened in your call center.

The default username used to access this dialog is ***admin***, and the default password is also ***admin***.

We recommend that you change the admin password the first time you log in: click on the Users tab and then click on admin user.

Reports

With EasyVOIZ Call Center Stats you can see:

- Calls answered
- Call abandoned
- Incoming Call Statistics
- By Agent
- By Queue
- Distribution of calls by week and day
- Distribution of calls per hour
- Easy retrieval of call recordings

Reports can be executed while the call center is in operation, so that you can see information in real time, without delay.

You can also listen to calls that have been recorded right through your computer using your browser. You can also export data to comma separated files (csv) or to PDF format.

Call Center Stats is a web based application, which means you do not need any software on the client machine, except a web browser. To view the interactive graphic, you must have the Flash Player.

Administration and Configuration of Users

As soon as you connect to the reporting system through your web browser, you must set access credentials. Call Center Stats has a powerful system of permissions to control resources, which are fully configurable by the administrative user.

Username	Key	Notes
user	user	Basic level of access Cannot create users or perform system configurations
admin	admin	Administrator Can perform all operations, including the creation of users

To create users and assign permissions, to need to log in as admin user, so that you have administrator privileges. Once logged in, you must choose the **Users** tab so that you can modify and create new accounts and their permissions.

We recommend that you change the admin password the first time you log in: click on the Users tab and then click on admin user.

To add a user, simply select the option from the menu. To delete a user, check the checkbox to the list of users or to delete and select Delete Users menu marked. To modify a user, click on the line for the user, which will open the edit screen users

Editing Users

In the edit screen, users can enter the access data such as account name and password, as well as assign access keys to select the queues and agents that may be accessed by this account. You can select all columns or choose an individual or agent in the selection box.

Access

In the system there are 3 defined access keys:

- admin
- user
- agent

These keys can be assigned individually or in combination to user accounts that you define. Depending on the keys that are assigned an account, it can access the various reports and reports as they are defined in the Edit screen in the Access Control tab Users. For example, it is possible to restrict the reporting of service level to accounts that hold the key agent only. This way, if an account is not allocated this key, the report will not be shown.

The **Access Control** menu option allows users to define the access keys that are required to access each of the reports and options in EasyVOIZ Call Center Stats. In normal use, there is no need for modifications. However it is possible to limit the reports to different levels of users by assigning each of the three keys of access available to them.

To change the table of access controls, simply click on the resource you want to change, view the display for editing access control. From here you can define what access keys are needed to view or select the remedy chosen.

To assign keys to make them click on the selection list. Using ctrl-click you can check more than one.

Settings and Preferences

The Setup tab lets you set preferences and general settings for the program, such as time intervals in different reports, language, time of abandonment by default, etc.

Configuration Variables

Variable	Explanation
alarm_hold_duration	Alarm in seconds for wait time in queue in real-time view. Can be set per queue
alarm_last_call	Alarm in seconds for last call taken by agent, also for the real-time view. Can be set per queue
alarm_wait_count	Alarm (in number of calls) for calls waiting in a queue
alarm_wait_threshold	Threshold (in percentage) from which to start coloring in alarm calls.
default_end_hour	Default end hour in HH:SS format for the date/time selection
default_start_hour	Default start hour in HH:SS format for the date/time selection
dict_agent	Dictionary entry for Agents. It will replace the agent set as the parameter to the value you specify (So you can use names instead of interfaces).
dict_queue	Dictionary entry for Queues. Same as the agent dictionary, but for replacing queue names.
distribution_interval	Time interval in minutes to split the distribution table

Variable	Explanation
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
spycontext	Asterisk context where to send spy calls, it must be similar to this one: [spy] exten => _X.,1,ChanSpy(SIP/${EXTEN},w) exten => _X.,2,Hangup

Selecting Reports

On the Home tab is a section where we will have to specify the minimum data to generate a report. These include the selection of the queue or, if having more than one, the agents and the range of dates and times.

Filtering Queues and Agents

By default the reporting system will report on all Queues and all Agents. You can filter this reporting by only selecting the specific queue(s) and specific agent(s) you wish to report on. You can then filter by Data and Time as well.

Filter by Date Range Hours

Select the date range for the reports. Some shortcuts are provided for date selection, including:

- Today: Selects the current day
- This week: Selects week beginning the Monday before
- This month: Selects from the 1st day of the month until the last day of the month
- Last 3 months: Selects the last 3 months, on the last day of the last month.

Once you have selected all the parameters to generate a report which are:

- Queues
- Agents
- Date Range
- Time Frame

Now you can click on Display Report to generate your reports.

Results

Once the report is displayed you will have a set of tabs across the top of the page. The first tab is Distribution. Quantity of calls distributed as follows:

- By Queues
- Per Month
- Per Week
- Per Day
- Per Hour
- Per Day of Week

You can scroll down the page to view each report section or click on the underlined sub-tabs in blue and jump right to that section.

In the report, whenever you see numbers or names in orange, scroll over that text with your mouse and click on the link and it will display the call details for this queue or agent. This is a common feature throughout all the reports.

Once the call detail is open and you are recording telephone calls, there is a column on the right hands side that states “Pl ay”. Scroll your mouse of the “Play” icon and a flash player will automatically begin to buffer the recorded call and begin playing it back to you. If you would like to download that specific recording to your computer, click on the green down arrow to the right of the play button and select where you would like to save the file.

It is also possible to automatically save recordings to an external server or HDD, and convert all recordings to MP3 file format.

Each report also has the option to be exported to CSV or PDF, and there is a link to each format at the end of each subsection. This is a common feature throughout all the reports.

Calls Answered

The second tab is labeled Answered. Reports on quantity of calls Answered as follows:

- By Queues
- Per Agent Service
- Level Disconnection
- Cause Answered Calls
- Detail Transfers
-

You can scroll down the page to view each report section or click on the underlined sub-tabs in blue and jump right to that section.

Calls Answered Overview

The sub-reports show the time per agent and number of calls answered by each agent.

The columns are:

- **Agent**: The name of the channel / agent can display the details of each call handled. Calls: Number of calls answered by this agent
- **Call%**: Percentage of calls answered within the current selection
- **Duration**: Time in minutes cumulative total of all calls answered.
- **% Of time**: Similar to the number of calls
- **Average**: The average duration of calls to the agent
- **Waiting time**: Waiting time accrued for all calls handled by the Agent
- **% Period**: average waiting time (% Time-out calls)

There are also interactive bar graphs showing the cumulative duration of calls per agent, the number of calls, etc. Pointing the mouse you can see in detail the values that are represented in each column.

Note that the percentages (such as the percentage of length) are calculated based on 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.

Transfers

This report shows how many calls were transferred to each extension in the time interval selected for the report. Note: When a call is transferred, the system does not record the duration of the calls within the queue.

Unanswered calls

The third tab is labeled Unanswered, which reports on:

- Abandon Rate
- Disconnection Cause
- Unanswered Calls by Queue
- Disconnection Cause
- Unanswered Calls Detail

Unanswered calls are those that have been lost (the caller could not connect with an agent). This can occur when the caller decides to disconnect by not wanting in queue or the queue decides to disconnect the caller after the end of the maximum waiting time and transfers the caller to voicemail or to another queue.

Disconnection Cause

This report shows the reason for disconnection of calls that were not completed.

The possible reasons are:

- Hangup by the caller
- Call time reached the maximum waiting time configured in EasyVOIZ for the queue
- Caller activated option of leaving the queue

Unanswered Calls by Queue

This report provides a breakdown of the calls by Queue that could not be completed.

If the report shows more than one queue, there will be a number and percentage of calls with regard for each queue accompanied by a graphic illustration.

Unanswered Call Details

This report details calls that could not be answered.

By clicking on the orange date and time link on the left, you can display the granular detail of the abandon call that entered the queue and when they hung up.

8. System Protection

Introduction

At this stage, we have a fully-functional system configured precisely the way we need. Now, we need to make sure it stays that way. Even with the best hardware, the failure of a system component is a danger that is always present. Without proper protection and backups, we could wind up without a working PBX and have no way to restore it. In this chapter, we will discuss the following:

- System protection using UPS devices, redundant components, and surge protection
- Making one-time backups
- Configuring recurring backups
- Restoring a backup
- Maintaining backup sets

System Protection

There are many ways to protect the components of a server from failure or damage. As the system controls voice communications for a company, these protection methods are even more important since any downtime means lost income and angry employees.

While the installation and setup of the equipment listed here is beyond the scope of this documentation, it is worth keeping them in mind during installation.

Uninterruptible Power Supplies

An **Uninterruptible Power Supply** (**UPS**) is essential to every VoIP system. A UPS acts as a battery backup in the event of a power failure. If the power supply is cut, anything plugged into the UPS will continue to run until the battery runs out. Most UPS units will also be able to send a shutdown signal to the server when the battery is nearly empty, allowing a clean shutdown.

Some UPS units will also provide a power conditioning service, sending a stable level of power to any attached device. This protects any attached equipment from surges or dips on the power line that can be very damaging. Note that power conditioning is not included in all the makes and models of UPS, so be sure to check before purchasing.

Also note that for a VoIP PBX to continue to be truly effective during a power outage, it must be able to maintain an Internet connection for any VoIP trunk. It is generally a good idea to ensure that the UPS will power not only the PBX but also any modems, routers, and switches required for connectivity.

Redundant Components

D-Link provide options for various types of redundant components. The most common redundant component is the hard drive, usually set up in a RAID configuration. This means that even if a hard drive fails, the system can continue to run without any downtime. Power supplies are another common redundant component. Redundant power supllies allow the server to continue to operate even after the failure of a unit.

Surge Protection

The most common type of surge protection is for power lines, but surges can affect other components of the system that will impact functionality. If analog lines are in use with analog ports, a power surge down the phone lines can ruin equipment. A power surge down a cable or DSL line can take a modem out of operation, or any other routing equipment attached to it. It is important to install surge protection on these types of entry points to the system.

Rapid Recovery

The D-Link Rapid Recovery (XRR) is a unique accessory that can back up the system (including the operating system) to a USB Disk-on-Key (DOK). It enables simple, safe and speedy recovery of your system. Note, however, that by default, logs, voicemail, and call recording files are not backed up. They can be marked for inclusion in the backup, if desired. For more information about customizing the backup, contact support@D-Link.com

Instructions

- Connect a monitor and keyboard to your system
- Connect your D-Link Rapid Recovery (XRR) to a USB port of the system
- Power on the system while pressing the F11 key, which will cause the system to boot from the disk-on-key
- The following option screen will appear
- Choose the first option (Backup/Restore), or just wait for 5 seconds, when the system will automatically begin to load the XRR software).
- The next option menu will now be displayed.

Main Menu

To create a backup, choose the “Backup” menu option, and define a descriptive name for the backup file:

Choose the target for the backup, and backup your system (depending on the configuration you have selected, the backup will take up about 1 GB and will take a few minutes.

Restore

- Choose the “Restore” menu option.
- Choose the appropriate backup file that you want to restore from, and restore your system.

Note that it is possible to keep several backups on the same disk-on-key. Each backup is saved as a separate folder under the disk-on-key 'backup' folder. You can delete the folder if you don't need a particular backup anymore.

9. D-Link Support

D-Link Hardware Licenses

Access the server via SSH protocol and type the following command to see which USB devices are connected:

```
# lsusb
```

Your output should look similar to this:

Note the bus number and the device number for the USB device that has an ID beginning with "e4e4". In the above example, the first Astribank bus number is 001 and the device number is 023. You can use the following command to receive a listing of the current license of the unit, using information that you collected from the *lsusb* command above:

```
astribank_allow –D /proc/bus/usb/[Bus #]/[Device #]
```

Based on the information returned from the *lsusb* command above, the command line would look something like this:

```
astribank_allow –D /proc/bus/usb/001/002
```

Copy the text from the screen to the clipboard. The relevant text begins with

---------BEGIN TELEPHONY DEVICE LICENSE BLOCK----

and ends with

---------END TELEPHONY DEVICE LICENSE BLOCK----

Applying a New D-Link Licence

Access the server via SSH protocol, stop both Asterisk and DAHDI, and type the following command to see which USB devices are connected:

```
# lsusb
```

Your output should look similar to this:

Note the bus number and the device number for the USB device that has an ID beginning with “e4e4”. In the above example, the first Astribank bus number is 001 and the device number is 023. You can use the following command to apply the updated license to the unit, using information that you collected from the *lsusb* command above:

```
astribank_allow –D /proc/bus/usb/[Bus #]/[Device #] -w
```

Based on the information returned from the *lsusb* command above, the command line would look something like this:

```
astribank_allow –D /proc/bus/usb/001/002 -w
```

Copy the text of the updated licence that you received from D-Link to the clipboard, and paste it into the command line by typing Ctrl-D

Restart the Astribank and check that all of the required ports are available, using the following commands:

```
/usr/share/dahdi/xpp_fxloader reset

dahdi_hardware –v
```

Managing Echo

Managing Echo in Telephony Systems

Echo in telephony systems is a phenomenon in which one caller hears the echo of his own voice after a short (or long) delay, together with the remote party's voice. There are two sources of echo in telephony systems:

- Network echo, which is produced by the interface between the two-wire local subscriber loop (a telephone set, for example) and the four-wire transmission system of telecommunications trunk lines (PBXs, PSTN, etc.).
- Acoustic echo, which is caused by feedback at the terminal device level, such as phone speaker acoustic feedback to its microphone.

Both types of echo can occur simultaneously in any single connection, compounding the negative effects. Although echo can be generated on both sides of the line (as a matter of fact, at each point that the four-wire system interfaces with the two-wire system), the echo that degrades phone call quality is typically generated on the other party's equipment (the remote side).

The reason that the local echo does not affect the call is simple: when a portion of the voice energy is fed back into the earpiece with a very small delay (milliseconds), we hear it as the positive feedback of a working telephone line.

Telephone sets are designed to feed our voice back from the microphone to the earpiece, and the local echo is just additional volume that is perceived as acceptable.

Reducing Echo

The main reason for line echo generation is impedance mismatch. Impedance is the circuit resistance to AC signals, and it changes with frequency. The first step to reduce echo is to match impedances.

This is done in two steps:

- Set the country (in /etc/zaptel.conf loadzone = [your country]) and adjust the impedance of the FXO ports to match those of the PSTN lines.
- Fine-tune the impedance matching by running the “FXO Tune” program (execute the “fxotune” command as root user). This program sends a tone to the telephone line and listens to the echo level. It checks the echo with different parameters, and chooses the parameter set that produces the least amount of echo.

Eliminating Echo

The procedure described above will decrease the echo, but will not eliminate it. Echo cancellation is done by a signal processing code that compares the digital voice that is sent to the circuit with the digital voice that is received by the circuit. When a pattern is identified, the signal processing program subtracts it from the outgoing signal, producing an echo-free signal for transmission.

You can find more detailed information about echo in VoIP telephony systems by navigating to: http://www.linuxjournal.com/article/8424 and http://www.gipscorp.com

Managing DAHDI Channels

Xpp_blink Utility

You can use the xpp_blink utility to determine the physical location of a dahdi channel on an Astribank. The syntax of the utility is as follows:

```
xpp_blink {on|off|bzzt} {span <number>} | chan <number> | xpd
<bus number> [xpd number>] | label <label>}
```

Some common examples:

xpp_blink on xpd 00 will cause the LEDs of the Astribanks to blink

xpp_blink on label usb:X000150 will cause the LEDs on the appropriate Astribank to blink

xpp_blink on span 4 will activate the LEDs of the XBUS-00/XPD-00 module *xpp_blink*

on chan 42 will blink the LED corresponding to DAHDI channel 42 *xpp_blink off chan*

42 will stop blinking the LED corresponding to DAHDI channel 42

Adding an Astribank

Initially, when a EasyVOIZ is manufactured, a utility is activated that populates all the available DAHDI (analog) channels in the Extensions dialog. These channels will be designated with extension numbers like 20xx, where xx indicates the channel number on the Astribank. However, if you run this utility after you have configured parameters for DAHDI channels, the information will initialized, and any changes will be over-written, and lost.

If you need to add an Astribank to an existing configuration, you need to ensure that the new Astribank is logically located after the existing Astribanks. As a result, the channel numbers of the new Astribank will continue from the last channel of the last existing Astribank. You can use the *lsdahdi* command to determine the sequence of the Astribanks. The output will look something like this:

Span 1: XBUS-00/XPD-00 “D-Link 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 "D-Link 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)

10.D-Link Applications

Burglar Alarms

Broadcasting Burglar Alarm System Messages

Every member of the D-Link line of products has an FXS module at the leftmost position that includes two auxiliary output ports and four auxiliary input ports. These features open up a whole world of exciting applications for the system. These notes will demonstrate how to broadcast burglar alarm system voice messages to designated phone numbers by using one of the Astribank input ports and modifying the Asterisk dialing plan.

An input port can be activated by connecting two wires in the input RJ-45 connector ("dry contact"). An input activation is translated as an "off hook" state of an extension. The default mapping of the input ports (when using the D-Link Rapid™ auto-configuration) starts with the number of the 8th FXS port plus 3. For example, if the Astribank-8 extensions are 401 to 408, the input ports will be extensions 411, 412, 413 and 414 (extensions 409 and 410 are the output ports).

Following is a step-by-step explanation of how to wire and set up your Astribank to send voice messages (as a response to any external event) to designated phone numbers.

- Prepare a cable: you can use a simple CAT-5 network cable. Cut it on one end, and strip the housing off the 8 internal wires
- The following table shows the wiring diagram of the output RJ-45 connector. An input event is generated by connecting the input pin to the associated ground pin.

RJ45 PIN	Functionality
1	IN 1
2	Common (GND)
3	IN 3
4	Common (GND)
5	IN 2
6	Common (GND)

7	IN 4
8	Common (GND)

- To emulate the "off-hook" status for a specific input, you should connect the pair that is associated with the required input. The input pairs are RJ-45 pins 1-2, 3-4, 5-6 and 7-8
- Connect the wiring to an isolated switch, such as a relay with "dry contact"

The input ports are not fused and are not designed to accept any external voltage. Driving external voltage will damage the input ports, and may damage the entire Astribank unit and void your warranty!

- Update the EasyVOIZ 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. EasyVOIZ will generate the calls as per your dialing plan and play the associated voice files.

Opening Doors

Every member of the D-Link line of products has an FXS module at the leftmost position that includes two auxiliary output ports and four auxiliary input ports. These features open up a whole world of exciting applications for the system. These notes will demonstrate how to control access of pre-approved personnel to restricted areas by using the Astribank output ports, and modifying the Asterisk dialing plan.

By using internally isolated relay, each one of the two output ports can switch up to 220 volts, 2 amperes. A relay can be activated by dialing in to its extension. Following is a step-by-step explanation of how to wire and set up your Astribank to control doors, or any other equipment of your choice.

Call in to the relay and listen to it: if your system is configured to support extensions 401 to 408, call extension 409 with your ear close to the Astribank. You'll hear a "click" from the Astribank. Hang up your phone; you will soon hear another "click". The first "click" is the sound that the relay makes when it is activated. This works exactly like a light switch, or pressing a push-button to activate a doorbell. Dialing to the second relay (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)

The output relays are not fused. Driving more than 2 amperes may damage the relay and void your warranty!

If you are switching voltages that are more than 24 volts, use licensed electrician services to wire the system.

Make sure that you use the Ground Tab of the Astribank unit to ground the Astribank box.

- Test the installation: call to the relay (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 D-Link XPP™ Technology

Overview

Rapid PA is an add-on for D-Link IP-PBX and Astribank channel banks that interfaces with any D-Link 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 D-Link 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 D-Link's default setting. If for any reason the setup is different, see the "Kewl Start Setup Procedure" below for proper settings. This is important in order to enable automatic disconnection from the PA system when the call terminates.

Rapid PA should be located close to the PA amplifiers

Wiring Table

RJ11 Connector/Pin	Description	Notes
PBX 1	Not connected	
PBX 2	FXS port TIP or RING	Crossing Pin2 and 3 is OK
PBX 3	FXS port TIP or RING	Crossing Pin2 and 3 is OK
PBX 4	Not connected	
PA 1	Not connected	
PA 2	PA Audio In	Crossing Pin2 and 3 is OK
PA 3	PA Audio In	Crossing Pin2 and 3 is OK
PA 4	Not connected	

Kewl Start Setup Procedure

In the */etc/dahdi/system.conf* file the channel must be defined as "fxoks". For example:

```
fxoks=1
```

In the */etc/asterisk/chan_dahdi_additional.conf* file the channel must be defined as fxo_ks. For example:

```
signalling=fxo_ks
```

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 system and go into the feature codes section
- 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 call the number that you have given him to access the voicemail system from outside the office. The process would work something like this.

- Call 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 key in 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.

11.Appendix

Feature Codes

Code	Description
Blacklist	
*30	Add a number to blacklist
*31	Remove a number from blacklist
*32	Blacklist the last caller
Business Services	
*34	Wakeup Call
*35	Remote Wakeup Call
*37	Speak Last Number
*38	Remind Me
Call Completion (CCSS)	
*40	Toggles Requests for Call Completion
*41	Cancel Pending Call Completion
Call Center	
*50	Toggles Add/Remove an agent to/from a specific queue
*51	Toggles Pause/Unpause an agent on a specific queue
*52	Login/logout queues
*53	Pause/Unpause queues
*54	Barge into Call
*55	Spy on an extension
*56	Spy on an extension in whisper mode
*57	Spy on random channels

Call Forward	
*36	Toggle Boss/Secretary
*58	Toggles Call Forward Immediately
*59	Set number for Call Forward Immediately
*60	Toggles Call Forward Unavailable
*61	Set Number For Call Forward Unavailable
*62	Toggles Call Forward Busy
*63	Set Number For Call Forward Busy
*64	Toggles Call Forward on No Answer
*65	Set Number For Call Forward on No Answer
*66	Toggles Do Not Disturb
*67	Toggles Follow Me
*69	Clear all Diversions
*96	Toggles Personal Assistant
On Call Features	
*0	Disconnect Call
*07	Direct Pickup
*08	Pickup Group
*2	Attended Transfer
*3	One Touch Recording
*4	Park Call
#1	Blind transfer
Phonebook Directory	
411	Dial By Name Directory
Test Services	
*70	Speak the date and Time

*71	Speak number of current Extension
*72	Perform Echo Test
*73	Simulate Incoming Call
Special Features	
*75	Toggles Phone lock
*76	Change password for current Extension
*77	Remote Substitution
*78	Customer Code
*79	Authorization Code
*80	Hot Desking
*81	Night Mode All
Voicemail	
*92	Custom Recording
*93	Dictation Services
*94	Record a message for Personnel Assistant
*95	Send Voicemail message
*97	Direct Voicemail
*98	Remote Voicemail

BLF (Hints)

Name	Dial	Description
DND_EXT	*66	Do Not Disturb
LOK_EXT	*75	Lock Phone
CFU_EXT	*64	Call Forwarding on No Answer
CFI_EXT	*60	Call Forwarding Unavailable
CFB_EXT	*62	Call Forward Busy
FWM_EXT	*67	Follow Me
PEA_EXT	*96	Personal Assistant
BOS_EXT	*36	Boss/Secretary
QAL_EXT	*50	Add/Remove Agent
QAP_EXT	*51	Pause/Unpause Agent
	*69	Clear all Diversions
NM_1	*81	Night Mode

Dial Options

- A (**x**) - Play an announcement to the called party, where *x* is the prompt (file)to be played
- a - Immediately answer the calling channel when the called channel answers in all cases. Normally, the calling channel is answered when the called channel answers, but when options such as A() and M() are used, the calling channel is not answered until all actions on the called channel (such as playing an announcement) are completed. This option can be used to answer the calling channel before doing anything on the called channel. You will rarely need to use this option, the default behavior is adequate in most cases.
- B (context^exten^**priority**) - Before initiating an outgoing call, Gosub to the specified location using the newly created channel. The Gosub will be executed for each destination channel.
- B (context^exten^**priority**) - Before initiating the outgoing call(s), Gosub to the specified location using the current channel.
- C - Reset the call detail record (CDR) for this call.
- c - If the Dial() application cancels this call, always set HANGUPCAUSE to 'answered elsewhere'
- d - Allow the calling user to call a 1-digit extension while waiting for a call to be answered. Exit to that extension if it exists in the current context, or the context defined in the EXITCONTEXT variable, if it exists.
- D (called:calling:progress) - Send the specified DTMF strings after the called party has answered, but before the call gets bridged. The called DTMF string is sent to the called party, and the calling DTMF string is sent to the calling party. Both arguments can be used alone. If progress is specified, its DTMF is sent to the called party immediately after receiving a PROGRESS message. See SendDTMF for valid digits.
- e - Execute the h extension for peer after the call ends
- f (x) - If *x* is not provided, force the CallerID sent on a call-forward or deflection to the dialplan extension of this Dial() using a dialplan hint. For example, some PSTNs do not allow CallerID to be set to anything other than the numbers assigned to you. If *x* is provided, force the CallerID sent to *x*.
- F (context^exten^**priority**) - When the caller hangs up, transfer the **called** party to the specified destination and **start** execution at that location.
- F - When the caller hangs up, transfer the **called** party to the next priority of the current extension and **start** execution at that location.
- g - Proceed with dialplan execution at the next priority in the current extension if the destination channel hangs up.
- G (context^exten^**priority**) - If the call is answered, transfer the calling party to the specified *priority* and the called party to the specified *priority* plus one.
- h - Allow the called party to hang up by sending the DTMF sequence defined for disconnect in features.conf.
- H - Allow the calling party to hang up by sending the DTMF sequence defined for disconnect in features.conf.
- i - Asterisk will ignore any forwarding requests it may receive on this call attempt.

- I - Asterisk will ignore any connected line update requests or any redirecting party update requests it may receive on this call attempt.
- k - Allow the called party to enable parking of the call by sending the DTMF sequence defined for call parking in features.conf.
- K - Allow the calling party to enable parking of the call by sending the DTMF sequence defined for call parking in features.conf.
- L (**x**:y:z) - Limit the call to *x* milliseconds. Play a warning when *y* milliseconds are left. Repeat the warning every *z* milliseconds until time expires. This option is affected by the following variables:
  - LIMIT_PLAYAUDIO_CALLER - If set, this variable causes Asterisk to play the prompts to the caller. Default is YES.
  - LIMIT_PLAYAUDIO_CALLEE - If set, this variable causes Asterisk to play the prompts to the callee. Default is NO.
  - LIMIT_TIMEOUT_FILE - If specified, *filename* specifies the sound prompt to play when the timeout is reached. If not set, the time remaining will be announced.
  - LIMIT_CONNECT_FILE - If specified, *filename* specifies the sound prompt to play when the call begins. If not set, the time remaining will be announced.
  - LIMIT_WARNING_FILE - If specified, *filename* specifies the sound prompt to play as a warning when time *x* is reached. If not set, the time remaining will be announced.
  - **x** - Maximum call time, in milliseconds
  - y - Warning time, in milliseconds
  - z - Repeat time, in milliseconds
- m (class) - Provide hold music to the calling party until a requested channel answers. A specific music on hold *class* (as defined in musiconhold.conf) can be specified.
- M (**macro**^arg) - Execute the specified *macro* for the **called** channel before connecting to the calling channel. Arguments can be specified to the Macro using ^ as a delimiter. The macro can set the variable MACRO_RESULT to specify the following actions after the macro is finished executing:
  - MACRO_RESULT - If set, this action will be taken after the macro finished executing.
    - ABORT - Hangup both legs of the call
    - CONGESTION - Behave as if line congestion was encountered
    - BUSY - Behave as if a busy signal was encountered
    - CONTINUE - Hangup the called party and allow the calling party to continue dialplan execution at the next priority
    - GOTO:[[<CONTEXT>^]<EXTEN>^]<PRIORITY> - Transfer the call to the specified destination.
  - **macro** - Name of the macro that should be executed.
  - arg[^arg...] - Macro arguments
- n (delete) - This option is a modifier for the call screening/privacy mode. (See the p and P options.) It specifies that no introductions are to be saved in the priv-callerintros directory.

  - delete - With *delete* either not specified or set to 0, the recorded introduction will not be deleted if the caller hangs up while the remote party has not yet answered. With *delete* set to 1, the introduction will always be deleted.

- N - This option is a modifier for the call screening/privacy mode. It specifies that if CallerID is present, do not screen the call.
- o (x) - If *x* is not provided, specify that the CallerID that was present on the **calling** channel be stored as the CallerID on the **called** channel. This was the behavior of Asterisk 1.0 and earlier. If *x* is provided, specify the CallerID stored on the **called** channel. Note that o(${CALLERID(all)}) is similar to option o without the parameter.
  - O (mode) - Enables **operator services** mode. This option only works when bridging a DAHDI channel to another DAHDI channel only. if specified on non-DAHDI interfaces, it will be ignored. When the destination answers (presumably an operator services station), the originator no longer has control of their line. They may hang up, but the switch will not release their line until the destination party (the operator) hangs up. - With *mode* either not specified or set to 1, the originator hanging up will cause the phone to ring back immediately. With *mode* set to 2, when the operator flashes the trunk, it will ring their phone back.
- p - This option enables screening mode. This is basically Privacy mode without memory.
- P (x) - Enable privacy mode. Use *x* as the family/key in the AstDB database if it is provided. The current extension is used if a database family/key is not specified.
- Q (**cause**) - Specify the Q.850/Q.931 *cause* to send on unanswered channels when another channel answers the call. As with Hangup(), *cause* can be a numeric cause code or a name such as NO_ANSWER, USER_BUSY, CALL_REJECTED or ANSWERED_ELSEWHERE (the default if Q isn't specified). You can also specify 0 or NONE to send no cause. See the causes.h file for the full list of valid causes and names.
- R (tone) - Default: Indicate ringing to the calling party, even if the called party isn't actually ringing. Send audio 'tone' from the indications.conf tonezone currently in use. Pass no audio to the calling party until the called channel has answered.
- R - Default: Indicate ringing to the calling party, even if the called party isn't actually ringing. Allow interruption of the ringback if early media is received on the channel.
- S (**x**) - Hang up the call *x* seconds **after** the called party has answered the call.
- s (**x**) - Force the outgoing CallerID tag parameter to be set to the string *x*. Works with the f option.
- t - Allow the called party to transfer the calling party by sending the DTMF sequence defined in features.conf. This setting does not perform policy enforcement on transfers initiated by other methods.
- T - Allow the calling party to transfer the called party by sending the DTMF sequence defined in features.conf. This setting does not perform policy enforcement on transfers initiated by other methods.
- U (**x**^arg) - Execute via Gosub the routine *x* for the **called** channel before connecting to the calling channel. Arguments can be specified to the Gosub using ^ as a delimiter. The Gosub routine can set the variable GOSUB_RESULT to specify the following actions after the Gosub returns.
  - GOSUB_RESULT
    - ABORT - Hangup both legs of the call.

        - CONGESTION - Behave as if line congestion was encountered.
        - BUSY - Behave as if a busy signal was encountered.
        - CONTINUE - Hangup the called party and allow the calling party to continue dialplan execution at the next priority.
        - GOTO:[[<CONTEXT>^]<EXTEN>^]<PRIORITY> - Transfer the call to the specified destination.
    - **x** - Name of the subroutine to execute via Gosub
    - arg[^arg...] - Arguments for the Gosub routine
    - u (**x**) - Works with the f option, where **x f**orces the outgoing callerid presentation indicator parameter to be set to one of the values passed in *x*:
        - allowed_not_screened
        - allowed_passed_screen
        - allowed_failed_screen
        - allowed
        - prohib_not_screened
        - prohib_passed_screen
        - prohib_failed_screen
        - prohib unavailable
- w - Allow the called party to enable recording of the call by sending the DTMF sequence defined for one-touch recording in features.conf.
- W - Allow the calling party to enable recording of the call by sending the DTMF sequence defined for one-touch recording in features.conf.
- x - Allow the called party to enable recording of the call by sending the DTMF sequence defined for one-touch automixmonitor in features.conf.
- X - Allow the calling party to enable recording of the call by sending the DTMF sequence defined for one-touch automixmonitor in features.conf.
- z - On a call forward, cancel any timeout which has been set for this call.

Voicemail.conf Options

When setting up an extension (Extensions mode) or a user (DeviceAndUser mode), EasyVOIZ 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	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. Note that this option can be configured within the EasyVOIZ interface using the Email Attachment field and should not be manually configured. Manually configuring this option could result in conflicting configurations and unpredictable result.
attachfmt	gsm, wav, wav49	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.

Option	Valid Values	Purpose
callback	[any valid context]	The EasyVOIZ 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 EasyVOIZ will use for placing the outbound call. By default, users created under EasyVOIZ use the from-internal context to place their calls, and this option can be safely set to this value. 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. If this option is not configured, no default value will be used and the callback feature of the voicemail application will be disabled.
delete	yes, no	If voicemail to email notifications are enabled, the delete option provides the ability to delete voicemail messages from the EasyVOIZ 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 EasyVOIZ. Note that this option can be configured within the EasyVOIZ interface using the Delete Voicemail field and should not be manually configured. Manually configuring this option could result in conflicting configurations and unpredictable result.
envelope	yes, no	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.

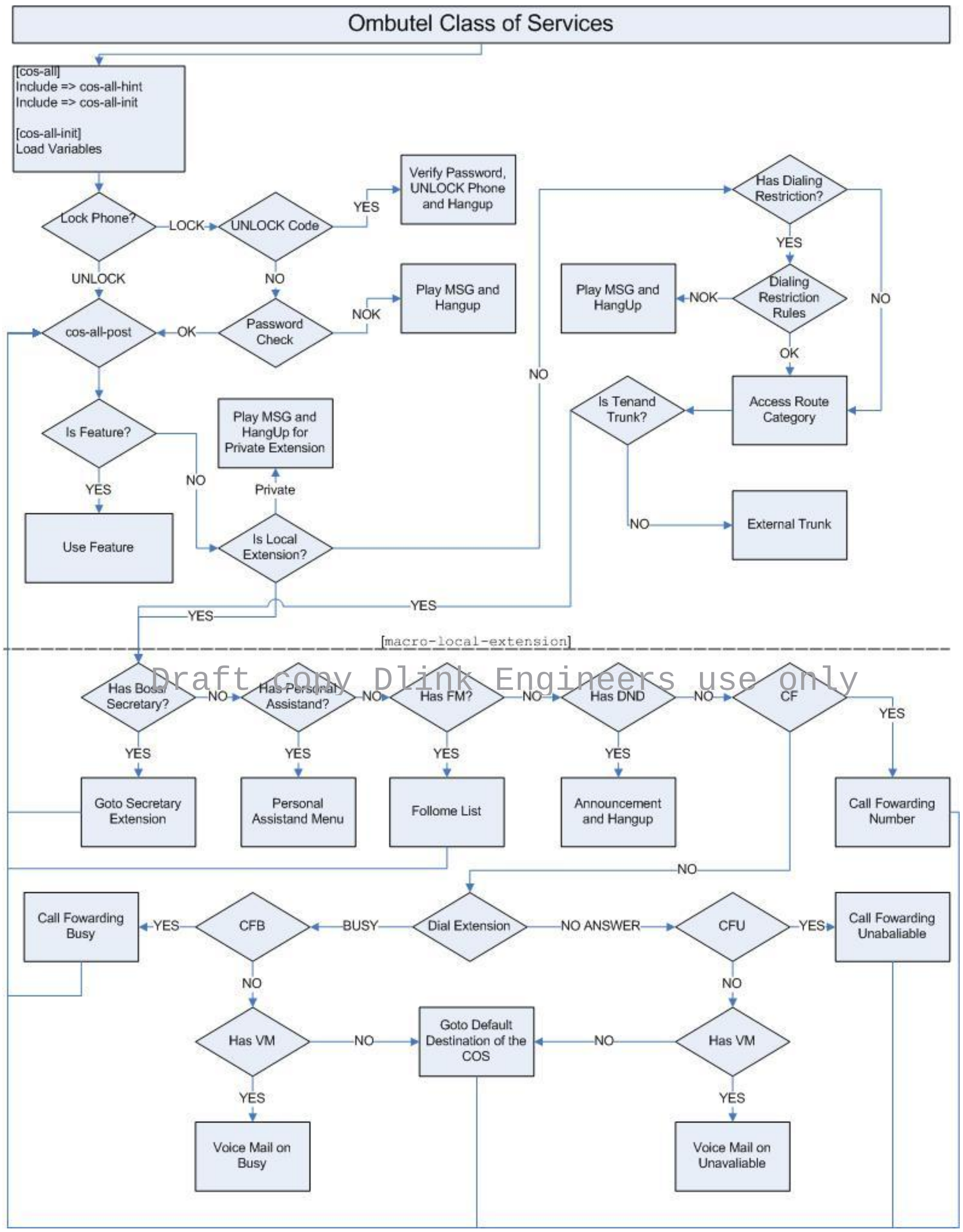
Option	Valid Values	Purpose
forcegreetings	yes, no	If set to "yes", new users will be prompted to record their busy and unavailable outgoing messages the first time they log into their mailbox. The voicemail application determines that a user is new if their voicemail password is the same as their extension. 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 */etc/asterisk/vm_general.inc* must be edited in order to include a line that reads imapserver=servername (where servername is replaced with the actual hostname of the IMAP server being used). Once the imapserver configuration option is defined in the vm_general.inc file, the imapuser and imappassword 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 EasyVOIZ **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	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. Note that this option can be configured within the EasyVOIZ interface using the **Play CID** field and should not be manually configured. Manually configuring this option could result in conflicting configurations and unpredictable results.
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 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]	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 EasyVOIZ server, check the contents of the /usr/share/zoneinfo folder. 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 EasyVOIZ server.

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.

Call Flow


Ombutel Class of Services
[cos-all]
Include => cos-all-hint
Include => cos-all-init
[cos-all-init]
Load Variables
Lock Phone?
LOCK
UNLOCK Code
YES
Verify Password, UNLOCK Phone and Hangup
NO
UNLOCK
cos-all-post
OK
Password Check
NOK
Play MSG and Hangup
Is Feature?
YES
Use Feature
NO
Play MSG and HangUp for Private Extension
Private
Is Local Extension?
YES
Has Dialing Restriction?
Dialing Restriction Rules
Play MSG and HangUp
Access Route Category
Is Tenand Trunk?
External Trunk
[macro-local-extension]
Has Boss/Secretary?
Has Personal Assistand?
Has FM?
Has DND
CF
Goto Secretary Extension
Personal Assistand Menu
Followe List
Announcement and Hangup
Call Fowarding Number
Dial Extension
BUSY
NO ANSWER
CFB
CFU
Call Fowarding Busy
Call Fowarding Unabaliable
Has VM
Goto Default Destination of the COS
Voice Mail on Busy
Voice Mail on Unavaliable