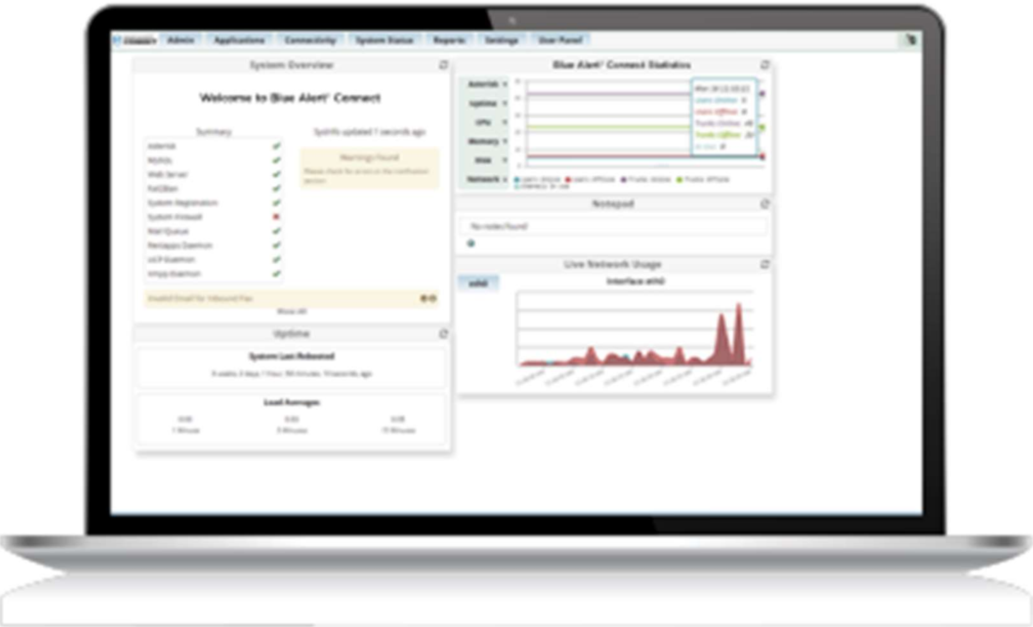
BLUE ALERT®
CONNECT



Administrator Guide

Code Blue®
800.205.7186 • www.codeblue.com

Administrator Guide

Table of Contents

IP Network Resources

Please note the below IP Network Ports are specified if you restrict Ports in your network and need to be allowed for the appropriate products listed

Blue Alert Connect

SSH Console Port 22/TCP, used to allow SSH to the PBX

HTTP/HTTPS Port 80/443/TCP, used to access the PBX Admin GUI

SMTP Port 25/TCP, Simple Mail Transfer Protocol

chan_SIP Port 5060/UDP, standard port for SIP signaling

chan_SIP Port 5061/UDP, alternate SIP port

chan_PJSIP Port 5160/UDP, standard port for SIP signaling

chan_PJSIP Port 5161/UDP, alternate port for SIP signaling

RTP for SIP Ports 10000-20000/UDP (customizable), used for voice portion of SIP call

Blue Alert Monitor

SSH Console Port 22/TCP, used to allow SSH access to the server

HTTP/HTTPS Port 80/443/TCP, used for service monitoring

SNMP Port 161/UDP, used for data collection

SNMP Trap Port 162/UDP, traps are unsolicited messages from an agent to a manager

SMTP Port 25/TCP, used for e-mail delivery of notifications, normally via a smart SMTP relay

HTTP Port 8980/TCP, The OpenNMS web UI is served on this port by default

Configuring Server Network Settings

Please note the applications of both Connect and Monitor have default static IP addresses of 192.168.0.11 and 192.168.0.12 respectively. To access the GUI and CLI for the first time a Workstation or laptop configured with the IP of 192.168.0.1 connected to the server via Network port 1 or on a local switch is required. If this is not an option, please contact Code Blue Technical Support.

Changing Static IP Address

Browse to the IP address of Blue Alert Connect in any browser. The default IP address is 192.168.0.11. Log into Blue Alert Connect, default credentials:

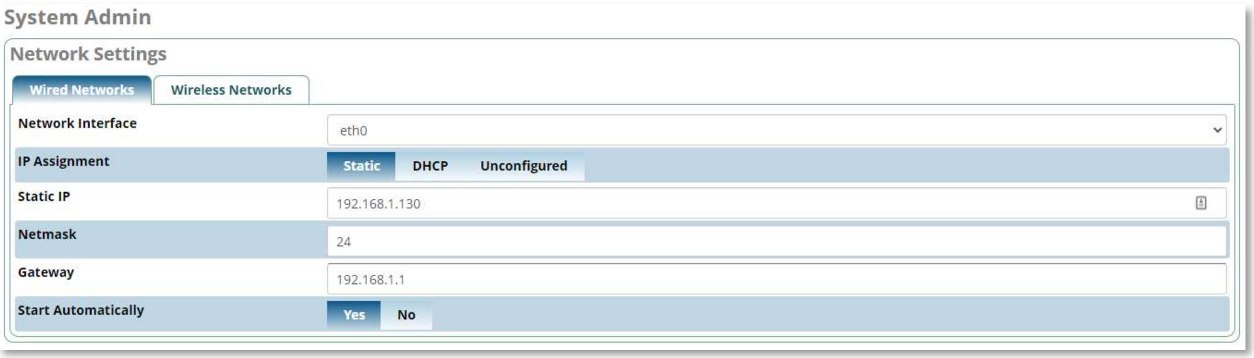
Username: cbadmin

Password: codeblue

On the top menu click Admin > System Admin. Then on the right side select Network Settings. For the VM version of Connect server this option will not appear until activated. Please contact Code Blue Technical Support to activate the server if needed.

Here you can assign a Static/DHCP address.

*** The Network Interface must be named eth0 ***


System Admin

Network Settings

Network Interface	eth0
IP Assignment	[✓ Static] DHCP Unconfigured
Static IP	192.168.1.130
Netmask	24
Gateway	192.168.1.1
Start Automatically	[✓ Yes] No

Once changes are made click “Save Interface” on the bottom right of the page. You may be prompted that the connection may be lost during this process. Click “yes” to continue.

Set Static IP through the CLI

From an SSH Client you can establish a connection to the Blue Alert Connect Server. The default IP is 192.168.0.11 and default credentials are:

Username: cbadmin

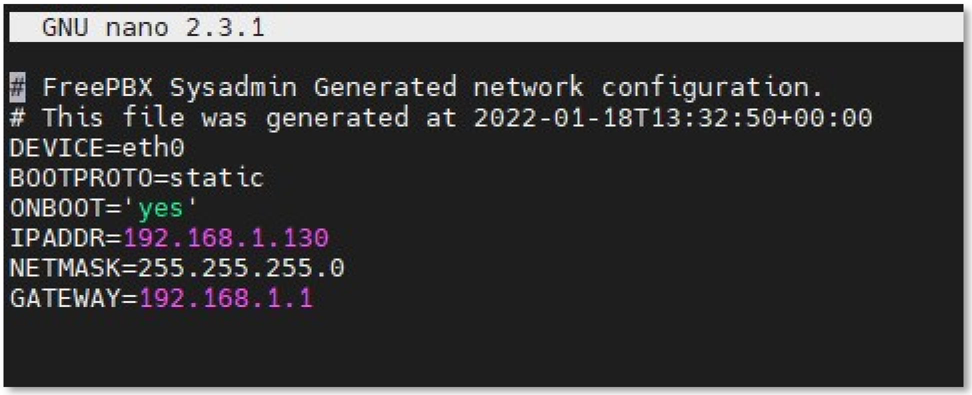
Password: CodeBlue92

Now connected to the Blue Alert Connect instance run the command:

sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0

Enter cbadmin password if prompted.

Simply change the IPADDR, NETMASK, and GATEWAY fields. Take care to not change indentation or change the device name away from eth0 as pictured below.



```
  GNU nano 2.3.1

# FreePBX Sysadmin Generated network configuration.
# This file was generated at 2022-01-18T13:32:50+00:00
DEVICE=eth0
BOOTPROTO=static
ONBOOT='yes'
IPADDR=192.168.1.130
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
```

Once the changes are made press ‘ctrl+X’ to save and exit. You will have to press ‘y’ to confirm the file name then ‘enter’ to fully save your changes.

Back at the command line run the following command for the changes to apply:

sudo service network restart

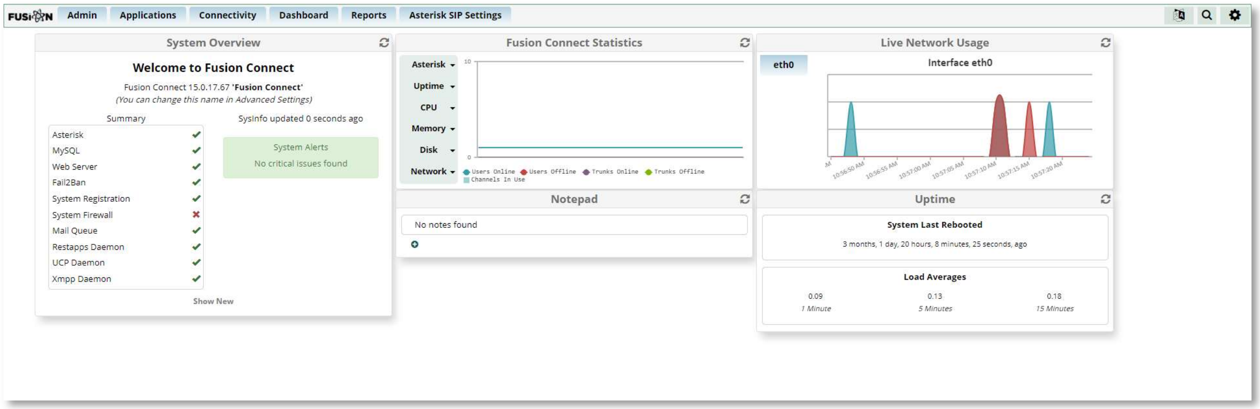
Dashboard

Browse to the IP address of Blue Alert Connect in any browser. Log into Blue Alert Connect using the credentials:

Username: cbadmin

Password: codeblue

The Dashboard, or Home Page, will show live feedback including Blue Alert Statistics, live usage, and system overview.



Welcome to Fusion Connect

Fusion Connect 15.0.17.67 **'Fusion Connect'**

(You can change this name in Advanced Settings)

Summary

Asterisk	✓
MySQL	✓
Web Server	✓
Fail2Ban	✓
System Registration	✓
System Firewall	✗
Mail Queue	✓
Restapps Daemon	✓
UCP Daemon	✓
Xmpp Daemon	✓

SysInfo updated 0 seconds ago

System Alerts

No critical issues found

No notes found

System Last Rebooted

3 months, 1 day, 20 hours, 8 minutes, 25 seconds, ago

Load Averages

0.09	0.13	0.18
1 Minute	*5 Minutes*	*15 Minutes*

Admin Modules

Browse to the IP address of Blue Alert Connect in any browser. Log into Blue Alert Connect using the credentials:

Username: cbadmin

Password: codeblue

On the top menu hover your mouse over 'Admin' to see the available modules.

Backup and Restore

On the top menu hover your mouse over 'Admin' and click on 'Backup & Restore'

Backup Job Creation

If this is a new install, your first step is to create a Filestore location. For more information see the Filestore section of the "Settings Modules" portion of this guide.

Click on the "Add Backup" button.

Give your backup a name and description.

Click the "Modules" button

Choose the modules to backup. You can click the box in the header to select all. Some modules will have their own settings which will be available by clicking the plus symbol.

Click "Save Changes"

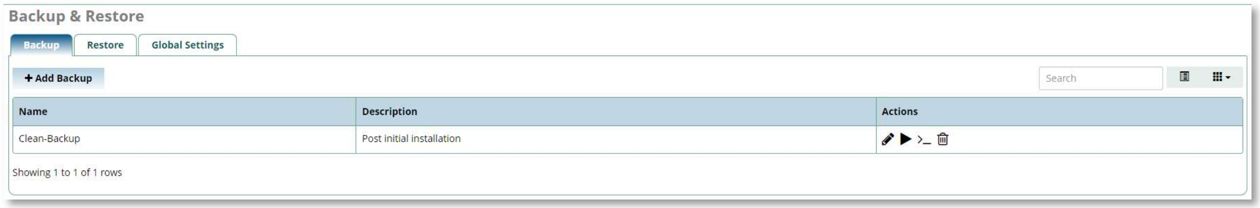
Select your notification preferences. If there is no email address, notifications will be disabled. Note notifications emails may be filtered as spam by your ISP. If this happens you can typically whitelist the sender email address.

Choose where to store the backup. You can select as many locations as desired.

> If you would like to save the backup jobs like <filestore-path>/<backup-job-name>/<backup-file> then enable "Append BackupJobName Directory into Storage path " option. By default, this option is NO which means backup file will always store to "filestore" defined path i.e. "<filestore-path>/<backup-file>"
>
> For more information and how to set up the "Filestore" path see "Filestore" under the "Settings Modules" section of this guide.

Decide if you want to run this backup automatically. To do so, set enabled to "Yes" and select the schedule. Only the options available to the selection type will be enabled. By default, these are all set randomly.

If you choose to run the backup manually, you simple have to click on the 'play' button found on the under the 'Actions' settings of the Backup tab.



Name	Description	Actions
Clean-Backup	Post initial installation	✎ ▶ >_ 🗑

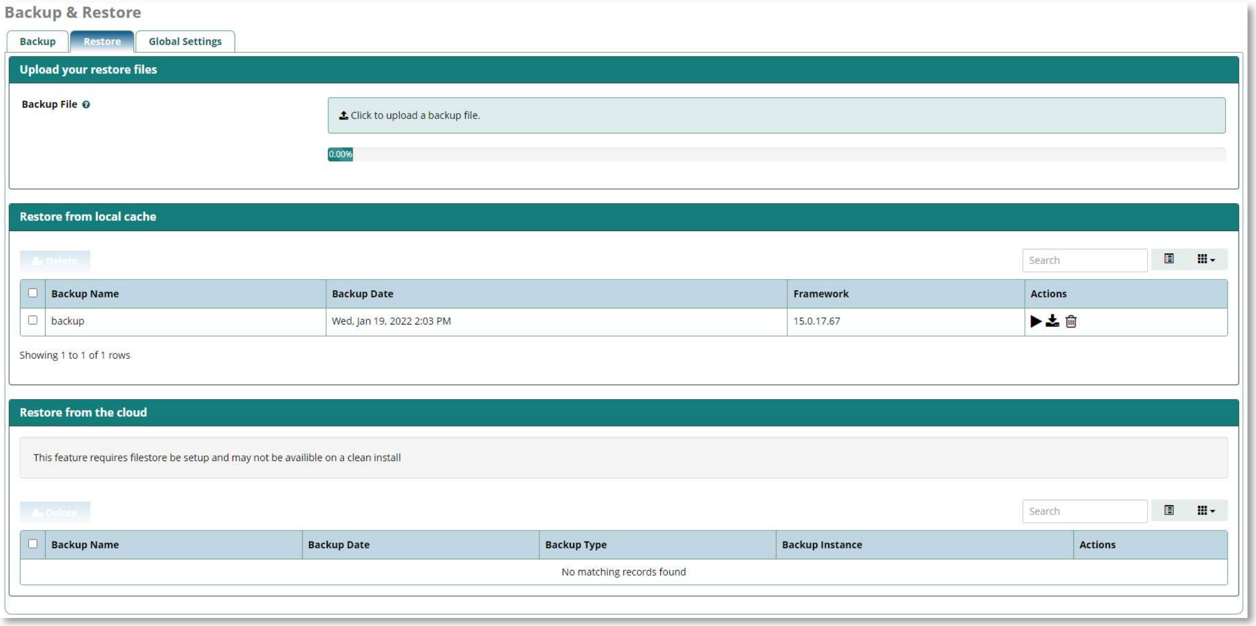
Showing 1 to 1 of 1 rows

Decide if you want the module to do housekeeping. Backups can be limited by number of runs only keeping the last X backups. They can also be kept until they reach a certain age. For "Delete After Runs" 0 is unlimited.

Save your backup.

Restore From Backup

From this window you can also download and delete stored backups.



Upload your restore files

Backup File

Restore from local cache

☐	Backup Name	Backup Date	Framework	Actions
☐	backup	Wed, Jan 19, 2022 2:03 PM	15.0.17.67	▶ ⬇ 🗑

Showing 1 to 1 of 1 rows

Restore from the cloud

This feature requires filestore be setup and may not be availible on a clean install

☐	Backup Name	Backup Date	Backup Type	Backup Instance	Actions
No matching records found					

After running or uploading a backup from the 'Actions' section of the restore tab you will go to a confirmation screen.

Here you will see the description of the backup job to be run including the modules backed up and decide to run the restore or go back to the restore page.

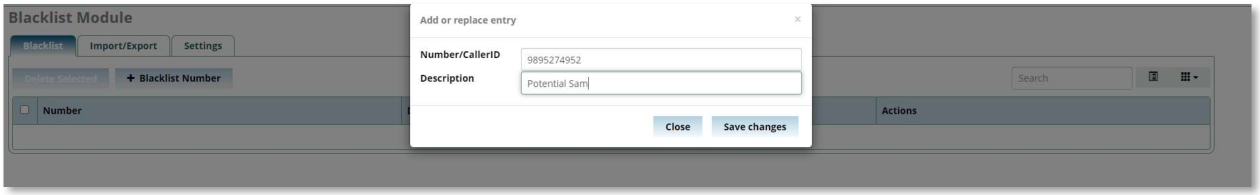
Blacklist

On the top menu hover your mouse over 'Admin' and click on 'Blacklist'

The Blacklist module allows you to have a list of numbers that will be blacklisted by the PBX. If a caller calls from one of those phone numbers, they will be sent to a destination you choose. If you do not choose a destination, they will hear the message "The number you have dialed is not in service. Please check the number and try again."

Blacklisting a Number

In the blacklist tab, click the blacklist number button. A window will pop up where you can enter a number and description.



Number/CallerID: 9895274952
Description: Potential Sam

Once complete click the Save Changes button. You'll receive confirmation that the number was added. Then, you can click the Close button.

Bulk Handler

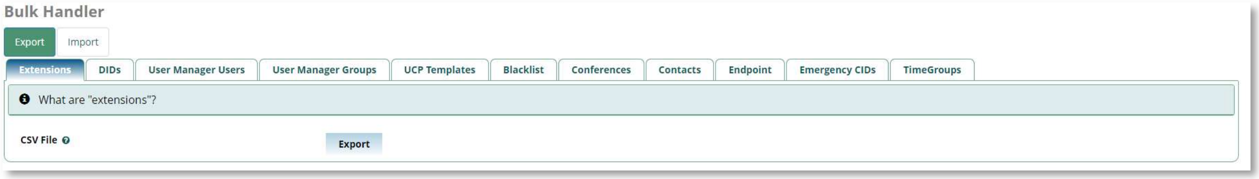
On the top menu hover your mouse over ‘Admin’ and click on ‘Bulk Handler’

Bulk Handler manages the bulk export or import of extensions. You can export this information as a CSV file. You can also upload a CSV file to save time versus having to enter each item individually. The module provides examples of required/recommended headers for your CSV files.

Exporting a CSV File

The Export section allows you to export a CSV file of Extensions, DIDs, User Manager Users, User Manager Groups, or Contacts. You can then make additions, removals, and changes to the file and import it if desired.

Exporting is also a way to create a "template" to ensure you are using all the available headers if you plan to import data.



Click the Export button at the top (selected by default).

Click the tab for the information you want to export.

Click Export near the bottom of the screen to download the CSV file through your browser.

Import a CSV File

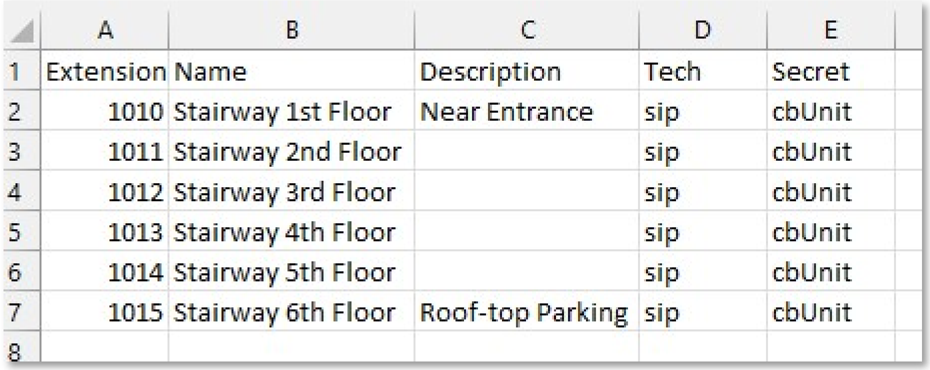
Click the Import button at the top if it is not already selected

Click the tab for the type of information you want to import. The process will be the same regardless of the type of data.

If you are creating a CSV file from scratch, note the Required/Recommended Headers listed in the middle of the page.

For importing Code blue devices as Extensions, the headers would be:

Extension; Name; Description; Tech; Secret



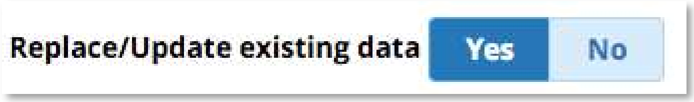
	A	B	C	D	E
1	Extension	Name	Description	Tech	Secret
2	1010	Stairway 1st Floor	Near Entrance	sip	cbUnit
3	1011	Stairway 2nd Floor		sip	cbUnit
4	1012	Stairway 3rd Floor		sip	cbUnit
5	1013	Stairway 4th Floor		sip	cbUnit
6	1014	Stairway 5th Floor		sip	cbUnit
7	1015	Stairway 6th Floor	Roof-top Parking	sip	cbUnit
8					

Click the Browse button.

Select the .csv file from your computer.

Click the Submit button at the bottom.

At the top of the screen, you will be asked whether you want to replace and update all your existing data with the contents from the CSV file.



Replace/Update existing data ● Yes ○ No

The contents of your CSV file will be displayed in a table, information can be edited by clicking the edit button ✎ . With changes made the finished button at the bottom of the page.

Click on Apply config at the top of the page to complete to upload.

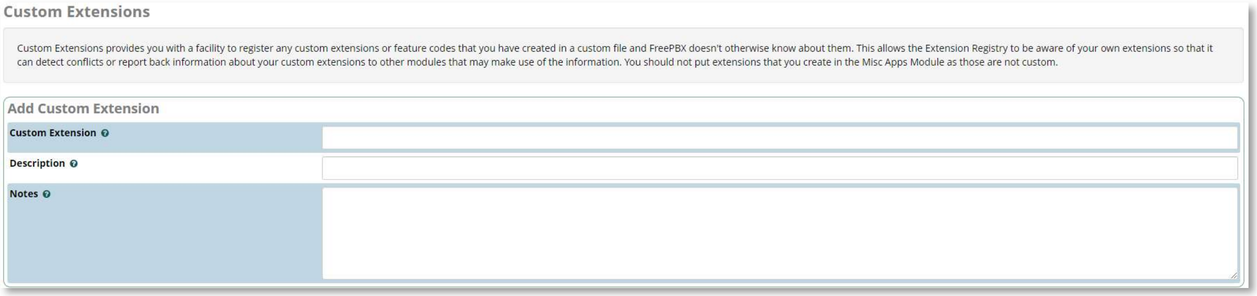
Custom Extensions

On the top menu hover your mouse over 'Admin' and click on 'Custom Extensions'

The Custom Extensions module provides you with a facility to register any custom extensions or feature codes that you have created in a custom script or dialplan when the PBX doesn't otherwise know about them.

Creating a Custom Extension

For each custom extension, you can define the following:



Custom Extensions

Custom Extensions provides you with a facility to register any custom extensions or feature codes that you have created in a custom file and FreePBX doesn't otherwise know about them. This allows the Extension Registry to be aware of your own extensions so that it can detect conflicts or report back information about your custom extensions to other modules that may make use of the information. You should not put extensions that you create in the Misc Apps Module as those are not custom.

Add Custom Extension

Custom Extension ❓	
Description ❓	
Notes ❓	

Custom Extension: Define the custom extension number that you want the PBX to be aware of. You will not be allowed to use the number for something else.

Description: Give this custom extension a friendly name.

Notes: Here you can enter notes on what this custom extension is used for.

When done click on the Submit button near the bottom of the page and Apply Config button near the top of the page to complete the process.

System Admin

On the top menu hover your mouse over ‘Admin’ and click on ‘System Admin’

The System Admin Module allows you to make changes to your Network Settings, DNS, Intrusion Detection System, Notification Settings, and Time Zone. It also allows you to power off or reboot your system and see the usage of your hard drives.

Activation

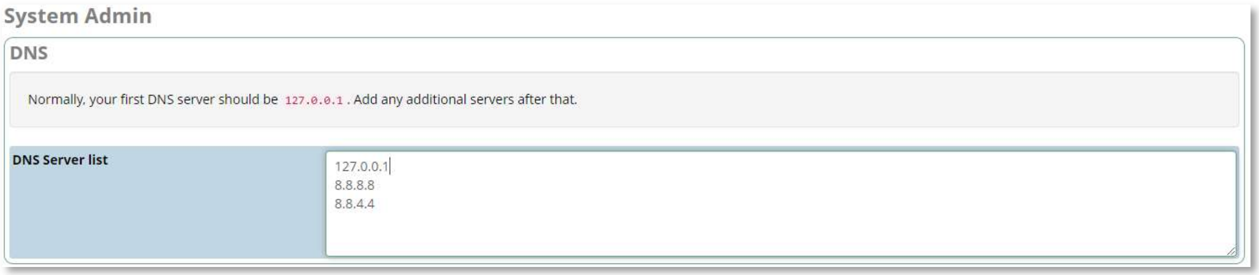
For Physical Version of Blue Alert Connect the system will come pre-activated by Code Blue before being shipped.

For Virtual instances Blue Alert Connect will generate a UUID which will then need to be activated by Code Blue’s Technical Support Team. Once the VM is installed please contact Technical Support at technicalsupport@codeblue.com

DNS

This component allows you to set the DNS servers used by your PBX.

Enter the DNS Servers, one per line. Normally, your first DNS server should be 127.0.0.1. Add any additional servers after that.



System Admin

DNS

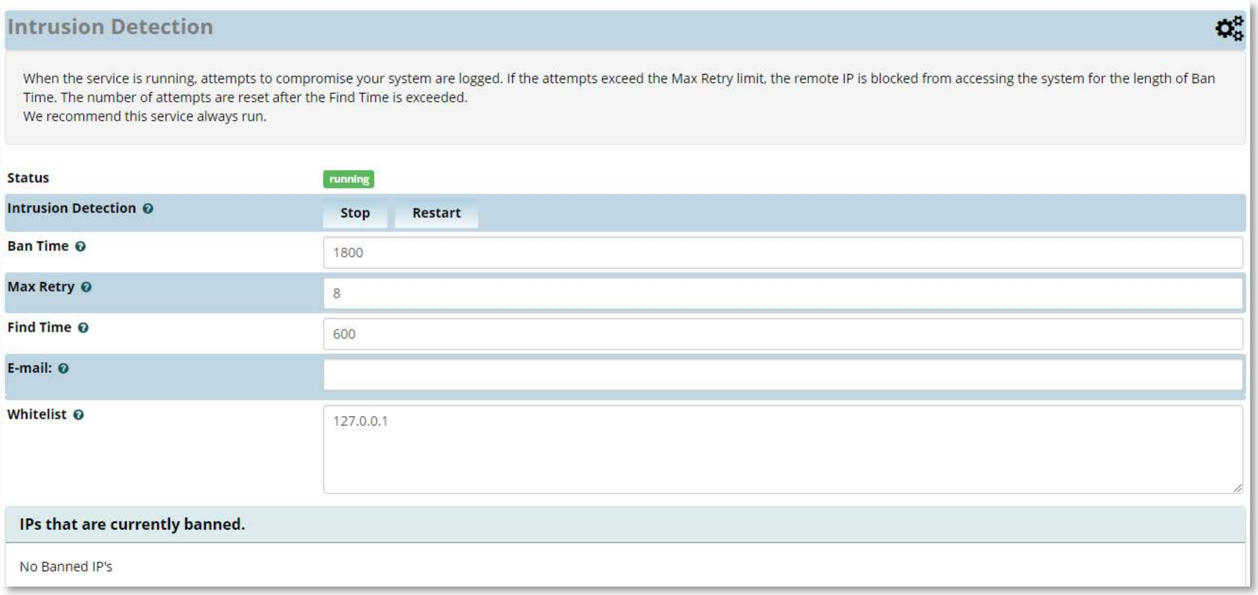
Normally, your first DNS server should be 127.0.0.1 . Add any additional servers after that.

DNS Server list	127.0.0.1 8.8.8.8 8.8.4.4

When you have the information as you want it, click the Submit button to save.

Intrusion Detection

When the service is running, attempts to compromise your system are logged. If the attempts exceed the Max Retry limit, the remote IP is blocked from accessing the system for the length of Ban Time. The number of attempts are reset after the Find Time is exceeded. We recommend this service always run.



Intrusion Detection

When the service is running, attempts to compromise your system are logged. If the attempts exceed the Max Retry limit, the remote IP is blocked from accessing the system for the length of Ban Time. The number of attempts are reset after the Find Time is exceeded.
We recommend this service always run.

Status	running
Intrusion Detection	Stop Restart
Ban Time	1800
Max Retry	8
Find Time	600
E-mail:	
Whitelist	127.0.0.1

IPs that are currently banned.

No Banned IP's

Ban Time: Amount of time, in seconds, to ban the remote IP of the potential intruder before being reset. Default = 1800 seconds (30 minutes)

Max Retry: How many times a remote IP can try to connect during the find time. This is the number of attempts a potential intruder has within the find time before they are banned. This should never be too low, as it could lock you out for a simple mistake. You should use passwords that are complex enough not to be guessed by an intruder within the max retry count.

Find Time: The window of time before resetting failed attempts to 0. Default = 600 seconds (10 minutes). For example, with the Max Retry set to 8, the system will ban any IP that fails 8 times in a 10-minute period. Most scanners will burn out the attempts in seconds.

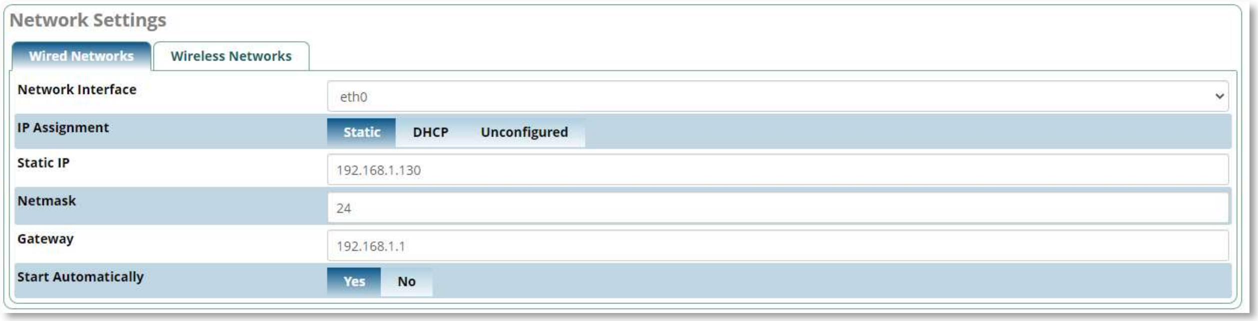
E-mail: The e-mail address to send intrusion detection notifications to.

Whitelist: This is a list of addresses/networks that can bypass the above restrictions. These IPs will not be banned. Individual address can be added or an entire subnet, for example 192.168.1.0/24.

Once changes are made, click the Submit button found at the bottom of the page.

Network Settings

This page allows you to set your network interface settings.



Network Settings

Network Interface	eth0
IP Assignment	Static DHCP Unconfigured
Static IP	192.168.1.130
Netmask	24
Gateway	192.168.1.1
Start Automatically	Yes No

Network Interface: The network interface must remain labeled as eth0 for the physical deployment of Blue Alert Connect. It can be adjusted in VM environment.

IP assignment: Choose between Static/DHCP/Unconfigured. If you choose Static, the next three fields will become available (Static IP, Netmask, and Gateway). Otherwise, those fields are grayed-out.

Static IP: The network IP address you want to assign. Example: 10.0.0.1

Netmask: The subnet mask. Example 255.255.255.0

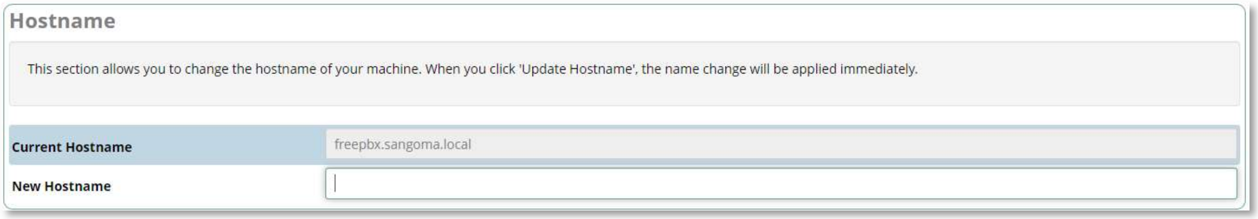
Gateway: Default Gateway. Example 10.0.0.254

Start Automatically: This allows you to choose whether this interface should load on system boot.

Once changes are made click Save Interface at the bottom of the page.

Hostname

This page allows you to configure the hostname of your PBX. This hostname will show up in network scans and when you SSH into your PBX the hostname will be shown.



Hostname

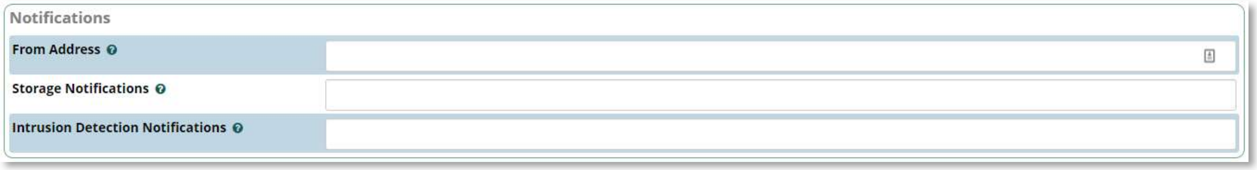
This section allows you to change the hostname of your machine. When you click 'Update Hostname', the name change will be applied immediately.

Current Hostname	freepbx.sangoma.local
New Hostname	

After entering the new hostname click on the Update Hostname button in the lower right corner. After reloading the page, the new hostname will appear as the current hostname.

Notifications Settings

This page allows you to set destination addresses for various emails that are sent out by the system, as well as the "from" address.



Notifications

From Address	
Storage Notifications	
Intrusion Detection Notifications	

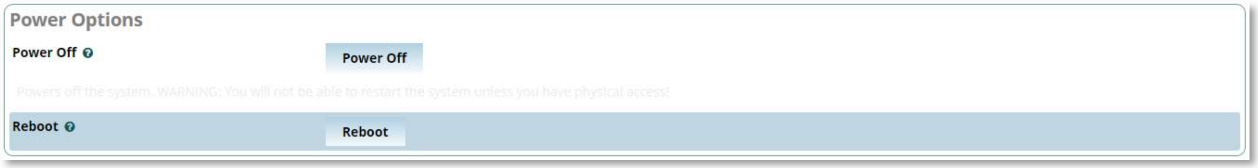
From Address: The address entered here will be set as the "From:" address. All emails sent from this machine (unless overridden elsewhere) will come from this email address.

Storage Notifications: Any storage events, such as low disk space or RAID failures, will be sent to this address.

Intrusion Detection Notifications: If a machine IP has been blocked and banned from the system by intrusion detection, an alert will be sent to this email address.

Power Options

The Power Options page allows you to power down or reboot your server.



Power Options

Power Off

Powers off the system. WARNING: You will not be able to restart the system unless you have physical access!

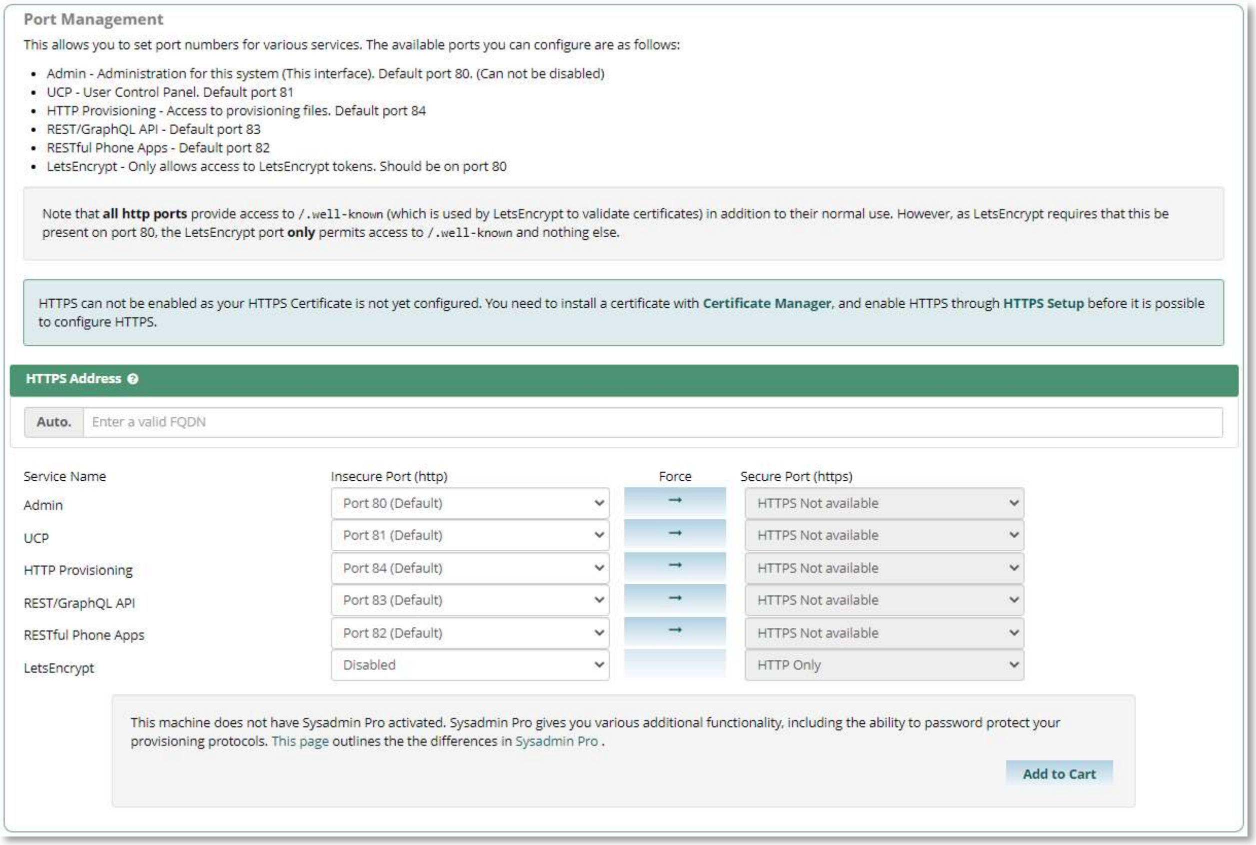
Reboot

Power Off: Powers off the system. If you click this button, a warning message will ask you to confirm. Click OK to continue.

Reboot: Reboots the server. If you click this button, a warning message will ask you to confirm. Click OK to continue.

Port Management

This page allows you to set port numbers for increased security.



Port Management

This allows you to set port numbers for various services. The available ports you can configure are as follows:

- Admin - Administration for this system (This interface). Default port 80. (Can not be disabled)
- UCP - User Control Panel. Default port 81
- HTTP Provisioning - Access to provisioning files. Default port 84
- REST/GraphQL API - Default port 83
- RESTful Phone Apps - Default port 82
- LetsEncrypt - Only allows access to LetsEncrypt tokens. Should be on port 80

Note that **all http ports** provide access to `/.well-known` (which is used by LetsEncrypt to validate certificates) in addition to their normal use. However, as LetsEncrypt requires that this be present on port 80, the LetsEncrypt port **only** permits access to `/.well-known` and nothing else.

HTTPS can not be enabled as your HTTPS Certificate is not yet configured. You need to install a certificate with **Certificate Manager**, and enable HTTPS through **HTTPS Setup** before it is possible to configure HTTPS.

HTTPS Address

Auto. Enter a valid FQDN

Service Name	Insecure Port (http)	Force	Secure Port (https)
Admin	Port 80 (Default)	→	HTTPS Not available
UCP	Port 81 (Default)	→	HTTPS Not available
HTTP Provisioning	Port 84 (Default)	→	HTTPS Not available
REST/GraphQL API	Port 83 (Default)	→	HTTPS Not available
RESTful Phone Apps	Port 82 (Default)	→	HTTPS Not available
LetsEncrypt	Disabled		HTTP Only

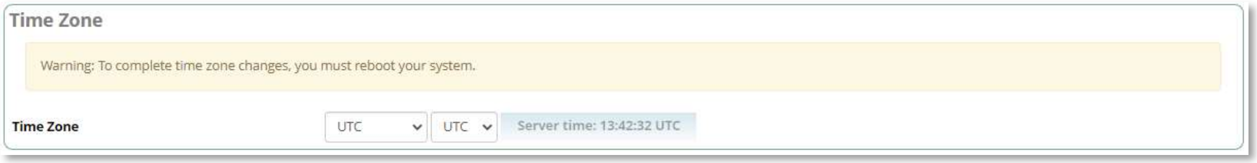
This machine does not have Sysadmin Pro activated. Sysadmin Pro gives you various additional functionality, including the ability to password protect your provisioning protocols. This page outlines the the differences in Sysadmin Pro .

To change any of the ports, you can use the dropdown to select a port number, or pick 'Custom Port' to select your own. When complete, click the Update Now button. Your changes will take effect immediately. Default ports and functions listed below.

Port	Default Port #	Function
Admin	80	Web port controlling the system
UCP	81	User Control Panel
HTTP Provisioning	84	Access to provisioning files
REST/GraphQL API	83	Access to RESTful API and GraphQL API
RESTful Phone Apps	82	Access to RESTful Phone Apps
LetsEncrypt	80	Only provides access to LetsEncrypt required files

Time Zone

The Time Zone page in System Admin allows you to set the system time zone.



Time Zone

Warning: To complete time zone changes, you must reboot your system.

Time Zone: UTC, UTC — Server time: 13:42:32 UTC

To change the time zone select you region; Select your closest locale; Click the Submit button; Reboot the system to apply the changes.

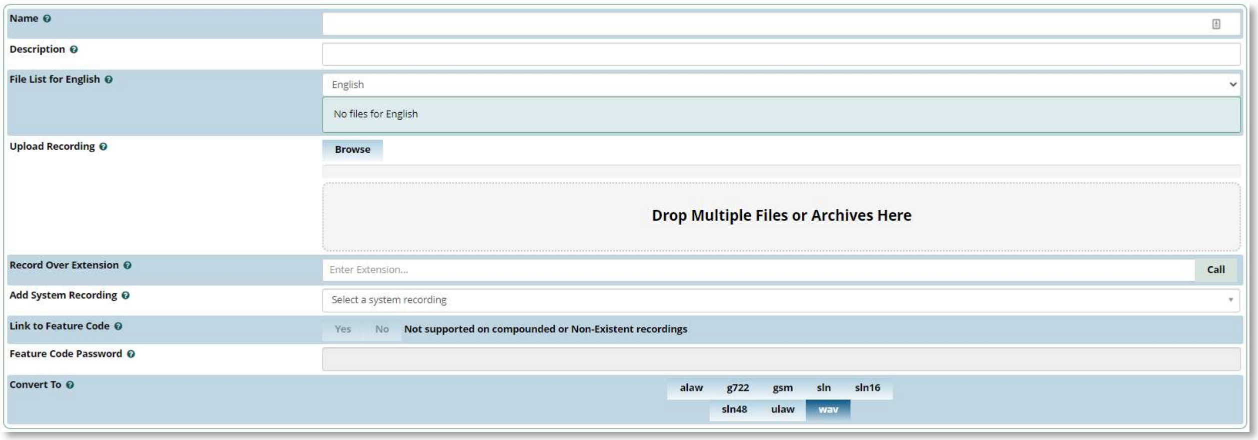
System Recordings

On the top menu hover your mouse over 'Admin' and click on 'System Recordings'

The System Recordings module is used to record or upload messages that can then be played back to callers in other modules. It can also be used to make pre-installed Asterisk recordings available for use in other modules.

Adding a System Recording

Click the Add Recording button.



Name:

Description:

File List for English: English — No files for English

Upload Recording: Browse — Drop Multiple Files or Archives Here

Record Over Extension: Enter Extension... — Call

Add System Recording: Select a system recording

Link to Feature Code: Yes No — Not supported on compounded or Non-Existent recordings

Feature Code Password:

Convert To: alaw g722 gsm sln sln16 sln48 ulaw wav

Name: The name of the system recording on the file system. If it conflicts with another file, then this will overwrite it.

Description: A description of this recording to help you identify it.

File List for English: A sortable File List / play order. Here, you can string multiple files together into one recording. The playback will be done starting from the top to the bottom.

Upload Recording: Allows upload of files from your local system. Supported upload formats are: alaw, g722, gsm, sln, sln16, sln48, ulaw and wav. This includes multiple files, and archives that contain multiple files.

Click the Browse button to select a file from your computer. Or drag and drop files from your desktop onto the Drop Multiple Files or Archives Here box.

Record Over Extension: The system will call the extension you specify. Upon hangup, you will be able to name the file and it will be placed in the list.

Convert To: The file formats you would like this system recording to be encoded into. Options include alaw, g719, g722, gsm, sln, ulaw and wav. Select one or more file formats.

When finished, click the Submit button and then click the Apply Config button.

Applications Modules

Browse to the IP address of Blue Alert Connect in any browser. Log into Blue Alert Connect using the credentials:

Username: cbadmin

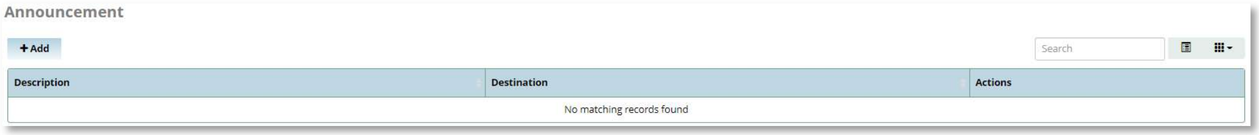
Password: codeblue

On the top menu hover your mouse over 'Applications' to see the available modules.

Announcements

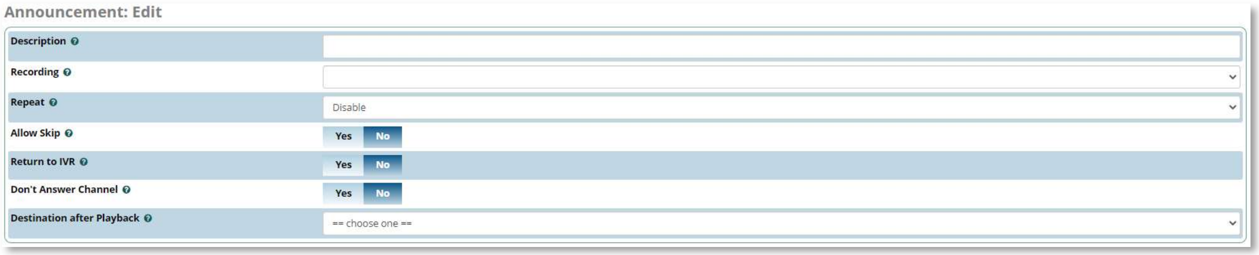
On the top menu hover your mouse over 'Applications' and click on 'Announcements'

The Announcements module is used to play a recording to callers and then send them to a different destination once the announcement has been played. The System Recording module is where you create the actual system recordings used here in Announcements.


Announcement

Description	Destination	Actions
No matching records found		

To begin creating an announcement click on the "+Add" button.


Announcement: Edit

Description	
Recording	
Repeat	Disable
Allow Skip	Yes [✓ No]
Return to IVR	Yes [✓ No]
Don't Answer Channel	Yes [✓ No]
Destination after Playback	== choose one ==

Description: Give the announcement a descriptive name to identify it.

Recording: Select the recording to be played. This is the recording that you have created using the System Recording module.

Repeat: You may optionally pick a keypress value from 0-9 or * and # that a caller can press to repeat the announcement.

Allow Skip: You can optionally enable the Allow Skip option, which will let the caller press any key on their phone to skip to the end of the recording

Return to IVR: If set to Yes, a caller who came from an IVR will be sent back to the IVR after the announcement, instead of being sent to the destination set below.

Don’t Answer Channel: The normal and recommend setting is No, which means the behavior is to answer the call and play this message. This feature is rarely supported by phone carriers.

Destination after Playback: Here you define where to route the caller after they have listened to the message. This is ignored if Return to IVR is selected.

When finished, click the Submit button and then click the Apply Config button.

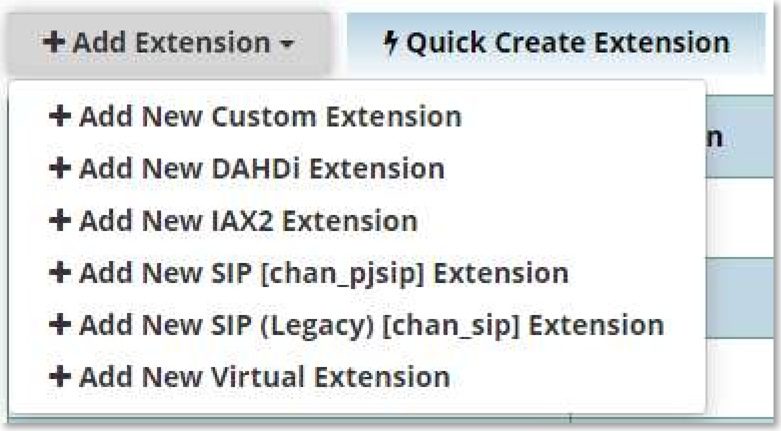
Extensions

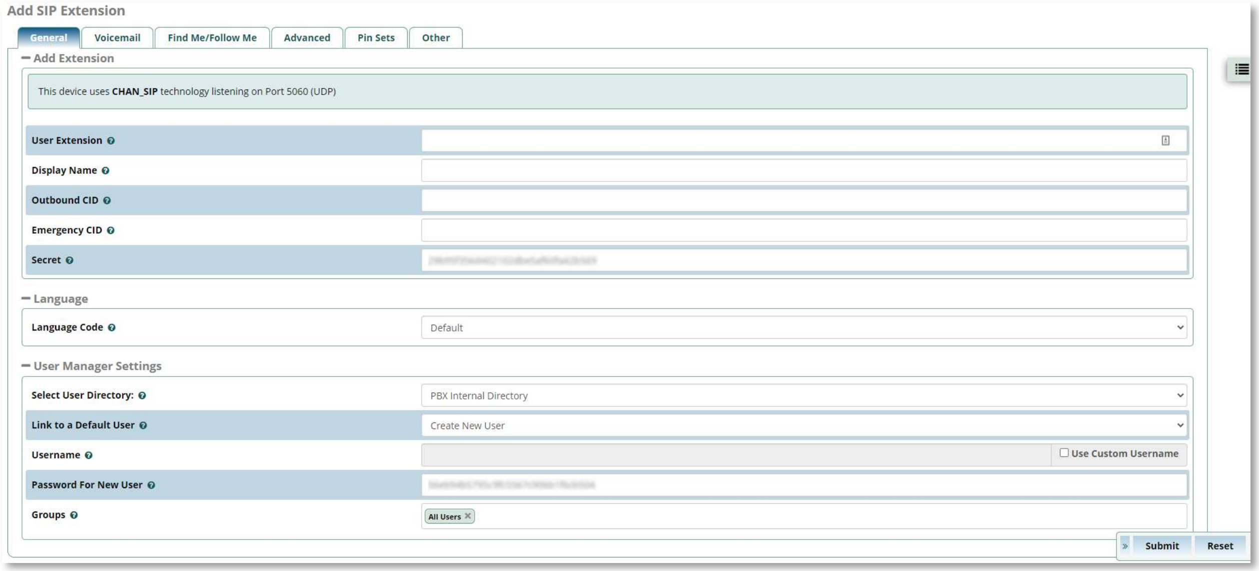
On the top menu hover your mouse over ‘Applications’ and click on ‘Extensions’

The Extensions Module is used to set up each extension on your system. This includes Code Blue devices and third-party phones. In the Extensions module, you will set up the extension number, the name of the extension, the password, and other options.

Adding a New Extension

When building an extension for a Code Blue SIP unit (IP5000/2500/1500, Centry, LS1000 or LS2000) begin by clicking +Add Extension then selecting +Add New (Legacy) SIP [chan_sip] Extension. This will also be the selection for the majority of Third-party Phones.


+ Add Extension
Quick Create Extension
+ Add New Custom Extension
+ Add New DAHDi Extension
+ Add New IAX2 Extension
+ Add New SIP [chan_pjsip] Extension
+ Add New SIP (Legacy) [chan_sip] Extension
+ Add New Virtual Extension



Add SIP Extension

− Add Extension

This device uses **CHAN_SIP** technology listening on Port 5060 (UDP)

User Extension	
Display Name	
Outbound CID	
Emergency CID	
Secret	[redacted]

− Language

Language Code	Default

− User Manager Settings

Select User Directory:	PBX Internal Directory
Link to a Default User	Create New User
Username	□ Use Custom Username
Password For New User	[redacted]
Groups	All Users ×

General Tab

User Extension: This will be the extension number associated with the device and cannot be changed once saved. This extension number will be matched in the Code Blue device account settings as its username/number.

Display Name: This is the name associated with this extension and can be edited any time. This will become the Caller ID Name. It is recommended to enter a name and not a number.

Outbound CID: Overrides the CallerID when dialing out a trunk. If you leave it blank, the system will use the route or trunk Caller ID, if set.

Emergency CID: This CallerID will always be set when dialing out an Outbound Route flagged as Emergency. The Emergency CID overrides all other CallerID settings.

Secret: Password (secret) configured for the device. Should be alphanumeric with at least 2 letters and numbers to keep secure. A secret is auto generated but you may edit it. This secret will be matched in the Code Blue device account settings as Secret/Password.

Language Code: This will cause all messages and voice prompts to use the selected language if installed. The Default is set to English.

User Management Settings: It is recommended to leave the User Manager Settings at their defaults. This is an advanced setting that is not commonly used with Code Blue products.

Voicemail Tab

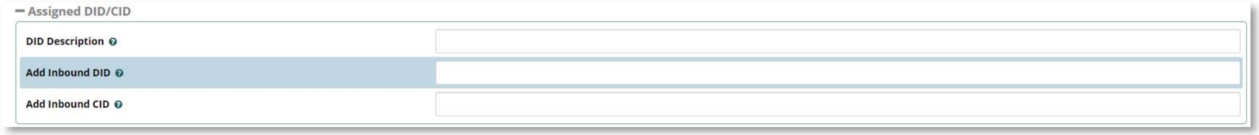
Having voicemail enabled will cause issues with Code Blue devices. It is recommended to leave this feature off.

Find Me/Follow Me Tab

This feature allows you to redirect a call that is placed to one of your extensions to another location. For more detail, please see the section “Follow Me” found later in this guide.

Advanced Tab

The advanced tab contains options are not compatible with Code Blue products. This guide will only cover the options that do pertain to Code Blue.



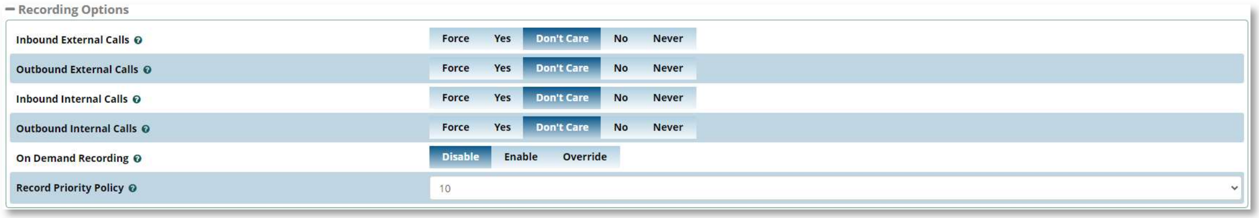
− Assigned DID/CID

DID Description	
Add Inbound DID	
Add Inbound CID	

DID Description: A description for this DID.

Add Inbound DID: A DID that is directly associated with this extension. The DID should be in the same format as provided by the provider, in a XXXXXXXXXX format.

Add Inbound CID: Add a CID for more specific DID + CID routing. An Inbound DID must be specified in the previous field.



− Recording Options

Inbound External Calls	Force Yes [✓ Don't Care] No Never
Outbound External Calls	Force Yes [✓ Don't Care] No Never
Inbound Internal Calls	Force Yes [✓ Don't Care] No Never
Outbound Internal Calls	Force Yes [✓ Don't Care] No Never
On Demand Recording	[✓ Disable] Enable Override
Record Priority Policy	10

Recording Options

Inbound External Calls: Set recording option of inbound calls from external sources.

Outbound External Calls: Set recording option of outbound calls to external sources.

Inbound Internal Calls: Set recording option of calls received from other extensions on the system.

Outbound Internal Calls: Set recording option of calls placed to other extensions on the system.

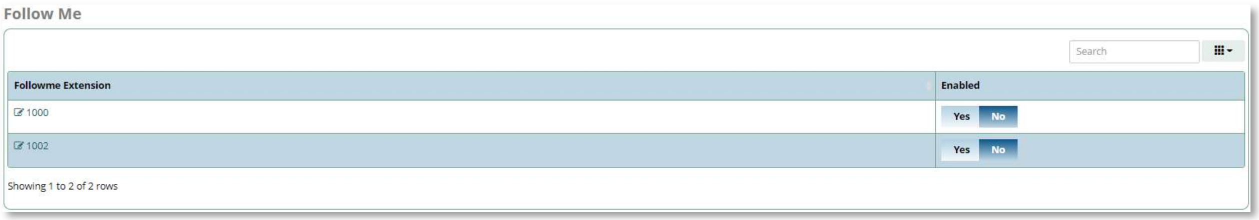
On Demand Recording: Enable or disable the ability to do on demand (one-touch) recording. The overall calling policy rules still apply, and if calls are already being recorded by "Force" or "Never," they cannot be paused unless "Override" is selected.

Record Priority Policy: This is the call recording policy priority relative to other extensions when there is a conflict (i.e. one extension wants to record and the other extension does not). The higher of the two priorities determines the policy. If the two priorities are equal, the global policy (caller or callee) determines the policy.

Follow Me

On the top menu hover your mouse over ‘Applications’ and click on ‘Follow Me’

Follow Me (also known as Find Me / Follow Me or FMFM) allows you to redirect a call that is placed to one of your extensions to another location. This is typically used in conjunction of a Virtual Extension to redirect calls to physical extensions.



Follow Me

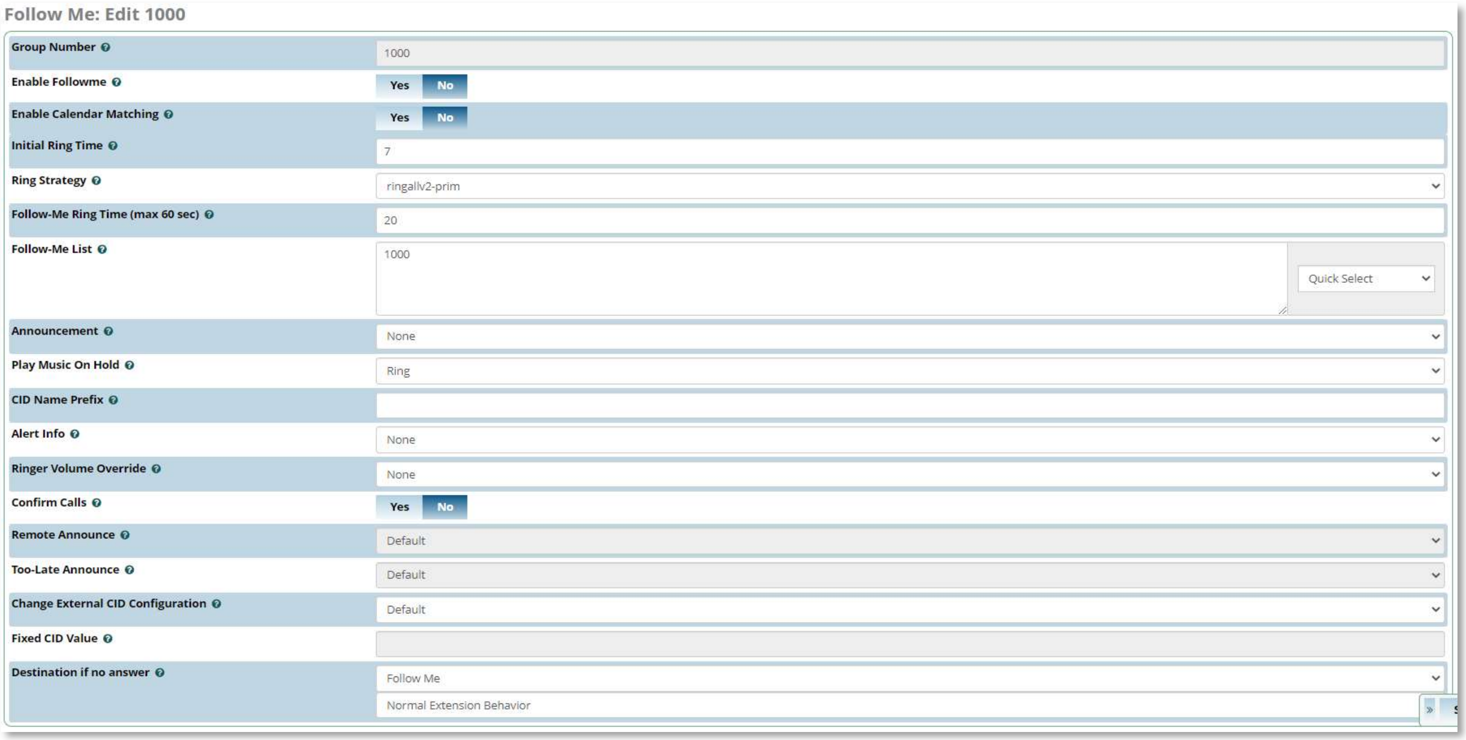
Search

Followme Extension	Enabled
1000	Yes No
1002	Yes No

Showing 1 to 2 of 2 rows

When you enter the module, you will see a list of your built extensions. You will have the ability to enable or disable the follow me settings and to edit the follow me settings per extension.

To edit the extension simply click the extension number or edit symbol on the left-hand side.



Follow Me: Edit 1000

Group Number	1000
Enable Followme	Yes No
Enable Calendar Matching	Yes No
Initial Ring Time	7
Ring Strategy	ringallv2-prim
Follow-Me Ring Time (max 60 sec)	20
Follow-Me List	1000 Quick Select
Announcement	None
Play Music On Hold	Ring
CID Name Prefix	
Alert Info	None
Ringer Volume Override	None
Confirm Calls	Yes No
Remote Announce	Default
Too-Late Announce	Default
Change External CID Configuration	Default
Fixed CID Value	
Destination if no answer	Follow Me Normal Extension Behavior

Group Number: The number of the extension users will dial to ring extensions in this Follow Me list.

Enable Follow Me: When enabled any calls to this extension will follow the settings of this page.

Initial Ring Time: This is the number of seconds to ring the primary extension prior to proceeding to the follow-me list. The extension can also be included in the follow-me list. A 0 setting will bypass this and is suggested in the case of using Virtual Extensions.

Ring Strategy: The Ring Strategy allows you to set how the extensions listed in the Follow Me list are dialed. These options include:

- **ringallv2:** ring Extension for duration set in Initial Ring Time, and then, while continuing call to extension, ring Follow-Me List for duration set in Ring Time.

- **ringall:** ring Extension for duration set in Initial Ring Time, and then terminate call to Extension and ring Follow-Me List for duration set in Ring Time.
- **hunt:** take turns ringing each available extension
- **memoryhunt:** ring first extension in the list, then ring the 1st and 2nd extension, then ring 1st 2nd and 3rd extension in the list.... etc.
- ***-prim:** these modes act as described above. However, if the primary extension (first in list) is occupied, the other extensions will not be rung. If the primary is in do-not-disturb (DND) mode, it won't be rung. If the primary is in call forward (CF) unconditional mode, then all will be rung.
- **firstavailable:** ring only the first available channel
- **firstnotonphone:** ring only the first channel which is not off hook - ignore CW

Follow Me Ring Time: Time in seconds that each extension will ring. For all hunt style ring strategies, this is the time for each iteration of extension(s) that are rung. This is in addition to the Initial Ring Time

Follow Me List: List extensions to ring, one per line, or use the Extension Quick Pick to the right. You can include an extension on a remote system(requires outbound route and trunk), or an external number by suffixing a number with a pound (#). ex: 2448089# would dial 2448089 on the appropriate trunk (see Outbound Routing).

Announcement: Message to be played to the caller before dialing this group

Play Music on Hold: If you select a Music on Hold class to play, instead of 'Ring', they will hear that instead of Ringing while they are waiting for someone to pick up.

CID Name Prefix: You can optionally prefix the CallerID name when ringing extensions in this group. For Example, if you prefix with "Code Blue:", a call from 1st Floor Stairwell would display as "Code Blue: 1st Floor Stairwell" on the extensions that ring.

Alert Info: ALERT_INFO can be used for distinctive ring with SIP devices. Not available with all SIP devices.

Confirm Calls: Enable this if you're calling external numbers that need confirmation - eg, a mobile phone may go to voicemail which will pick up the call. Enabling this requires the remote/receiving side push 1 on their phone before the call is put through. This feature only works with the ringall ring strategy. This does require a keypad to be present so if calling Code blue PAS speakers or Emergency call boxes it is recommended to leave this feature off.

Remote Announce: Message to be played to the person RECEIVING the call, if 'Confirm Calls' is enabled.

Too-Late Announce: Message to be played to the person RECEIVING the call, if the call has already been accepted before they push 1.

Destination if no answer: Where the caller will be sent if the call is not answered.

When finished, click the Submit button and then click the Apply Config button.

IVR

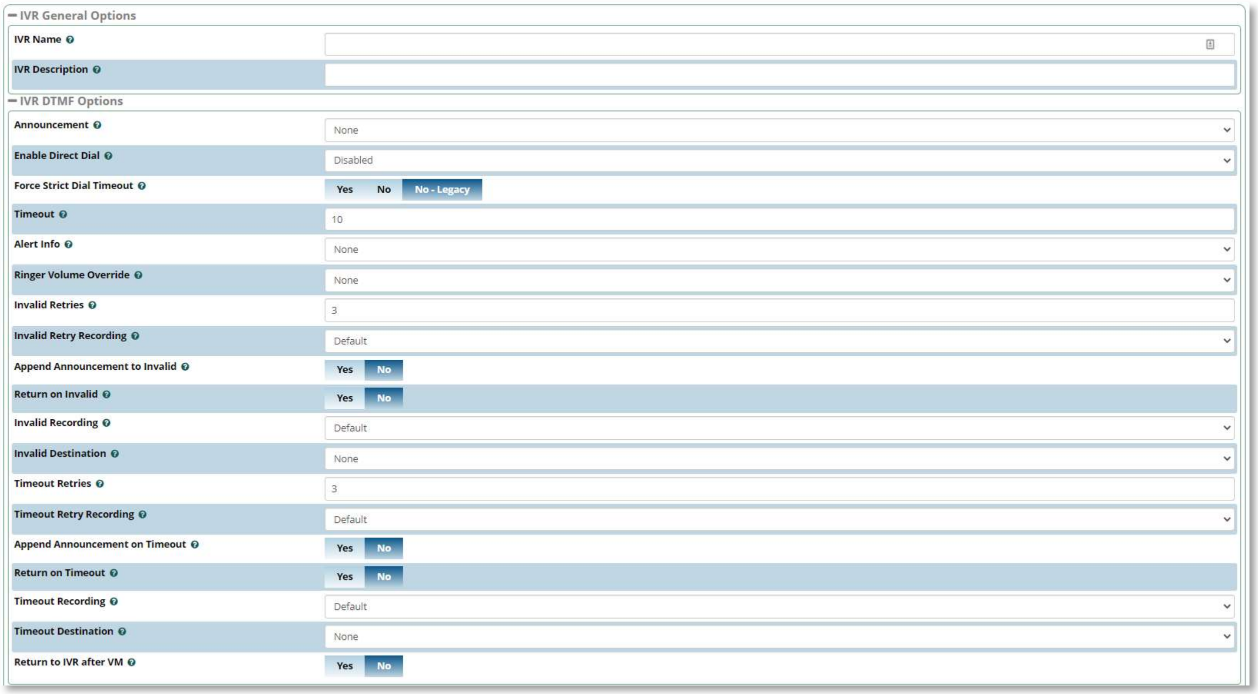
On the top menu hover your mouse over ‘Applications’ and click on ‘IVR’

The IVR module allows you to create one or more IVRs ("Interactive Voice Response" systems or Auto Attendants). You can then route calls to the IVR and play a recording prompting the caller what options to enter, such as “press 1 for security and press 2 for the front desk.”

If the call is being originated from a Code Blue Help Point a Keypad is required to utilize this feature

Creating a New IVR

To add an IVR, click the +Add IVR button.



IVR General Options

IVR Name	
IVR Description	

IVR DTMF Options

Announcement	None
Enable Direct Dial	Disabled
Force Strict Dial Timeout	Yes No [✓ No - Legacy]
Timeout	10
Alert Info	None
Ringer Volume Override	None
Invalid Retries	3
Invalid Retry Recording	Default
Append Announcement to Invalid	Yes [✓ No]
Return on Invalid	Yes [✓ No]
Invalid Recording	Default
Invalid Destination	None
Timeout Retries	3
Timeout Retry Recording	Default
Append Announcement on Timeout	Yes [✓ No]
Return on Timeout	Yes [✓ No]
Timeout Recording	Default
Timeout Destination	None
Return to IVR after VM	Yes [✓ No]

IVR General Options

IVR Name: Add a descriptive name to identify the IVR

IVR Description: Add an optional description for the IVR to help you remember what it is for.

IVR DTMF Options

Announcement: Choose which recording to be played to the caller when they enter the IVR. This can be any system recording that you have defined in the System Recording module. It will usually give them instructions, such as “press 1 for Security and 2 for the Front Desk.”

Enable Direct Dial: Allow callers to be able to enter an extension number when navigating the IVR to go directly to that user's extension

Force Strict Dial Timeout: No - Legacy is the recommended setting for this. If set to 'No' then IVR will match on the first digit(s) that match IVR entries, thus if you have entries of 1 and 123 when the caller presses 1 it will dial entry 1, when they press 123 it will match on the first entry so it will dial 1. If set to 'Yes' then IVR will wait the full timeout for the entry so that 123 will match 123.

Timeout: Enter the amount of time (in seconds) the system should wait for the caller to enter an option on their phone keypad.

Alert Info: ALERT_INFO can be used for distinctive ring with SIP devices. This is not available with all SIP phones.

Invalid Retries: Number of times to retry before ending the call when receiving an invalid/unmatched response from the caller.

Invalid Retry Recording: Prompt to be played before sending the caller to an alternate destination due to the caller pressing 0 or receiving the maximum amount of invalid/unmatched responses (as determined by Invalid Retries).

Append Announcement to Invalid: Controls whether a caller who makes an invalid entry will hear the main IVR announcement again.

Return on Invalid: Controls whether a caller who makes an invalid entry in a "sub-menu" IVR will be returned to the parent IVR.

Invalid recording: The recording to play to the caller after they have reached the invalid retry count defined above.

Invalid Destination: If callers cannot find a match after reaching the number of invalid retries defined above, they will be transferred to the invalid destination you set here.

Timeout Retries: How many times callers are allowed to timeout without pressing any options on their keypad before they are sent to the invalid destination defined above.

Timeout Retry Recordings: The recording to play to a caller who times out.

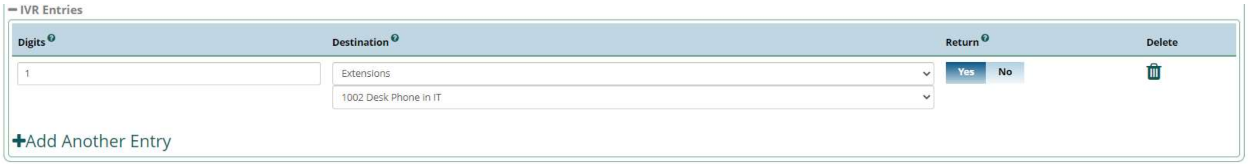
Append Announcement on Timeout: Controls whether a caller who times out will hear the main IVR announcement again.

Return on Timeout: Controls whether a caller who times out in a "sub-menu" IVR will be returned to the parent IVR.

Timeout Recording: The recording to play to a caller when they have used the number of timeouts retries defined above.

Timeout Destination: If callers do not make an entry within the maximum number of timeouts retries defined above, they will be transferred to the timeout destination.

Return to IVR after VM: Whether to offer callers who end up in a user's voicemail box the option to return to the IVR.



— IVR Entries

Digits	Destination	Return	Delete
1	Extensions 1002 Desk Phone in IT	Yes No	

+Add Another Entry

IVR Entries

Digits: The digits the caller should press to reach the destination.

Destinations: The destination to route the caller to when they press the digits in the Ext field.

Return: Whether to send callers back to the parent IVR when they press the digits in the Ext field.

When finished, click the Submit button and then click the Apply Config button.

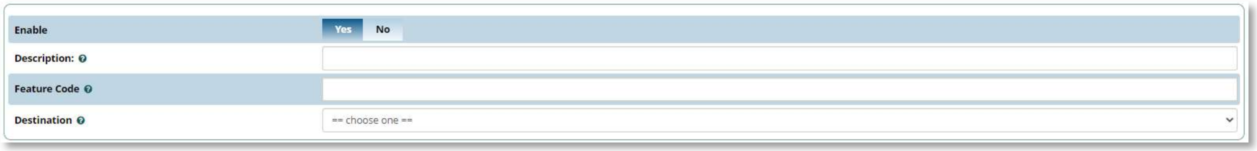
Misc Applications

On the top menu hover your mouse over ‘Applications’ and click on ‘Misc Applications’

A miscellaneous application is a custom feature code that you can dial from internal phones to go to various destinations available in the PBX.

Creating a new Misc Application

Click on +Add Misc Application



Enable	Yes No
Description:	
Feature Code	
Destination	== choose one ==

Enable: Choose to enable this miscellaneous application.

Description: Used to identify this application.

Feature Code: The custom feature code that users will dial to access this application. This can be a star code (example, *7876) or simply a normal extension (example, 7876). This value must be unique and not shared with any user, application, or star code on Blue Alert Connect. This can also be modified on the feature codes page.

Destination: Where to send callers when they dial the custom feature code.

When finished, click the Submit button and then click the Apply Config button.

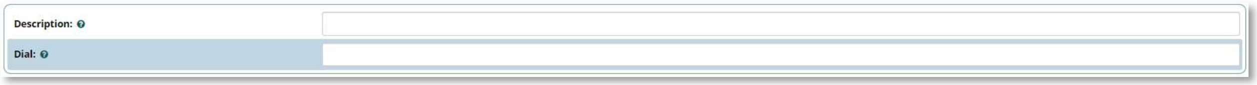
Misc Destinations

On the top menu hover your mouse over ‘Applications’ and click on ‘Misc Destinations’

A miscellaneous destination is a custom call target that can be used by another module. Anything that can be dialed from a user’s extension can be turned into a misc destination.

Creating a New Misc Destination

Click on +Add Misc Destination



Description: ❓	
Dial: ❓	

Description: Enter a description of the destination to help you identify it.

Dial: Enter the extension, telephone number, feature code, or application that the system should dial when a caller is routed to the destination.

When finished, click the Submit button and then click the Apply Config button.

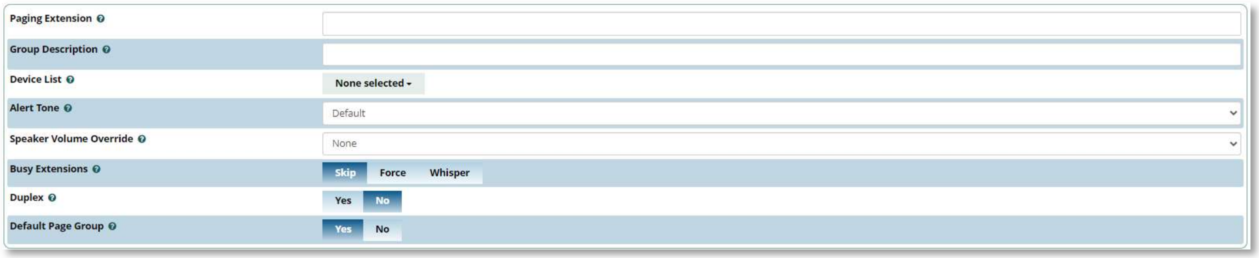
Paging and Intercom

On the top menu hover your mouse over ‘Applications’ and click on ‘Paging and Intercom’

In the Paging and Intercom module, you can configure groups of phones that will auto-answer and play the page over their speakers when called from the page group. Requires phones to be set to auto-answer.

Creating a New Page Group

Click on +Add Page Group



Paging Extension ❓	
Group Description ❓	
Device List ❓	None selected ▾
Alert Tone ❓	Default
Speaker Volume Override ❓	None
Busy Extensions ❓	[✓ Skip] Force Whisper
Duplex ❓	Yes [✓ No]
Default Page Group ❓	[✓ Yes] No

Paging Extension: The extension number for this page group. Users can dial this number to page this group. This must be unique and not match any existing extensions or groups.

Group Description: a short description to help you identify the group.

Device List: Choose which extension(s) to include in the page group by dragging the desired extensions to the Selected bin. These will be included in the page group.

Alert Tone: Announcement to be played to remote party.

Busy Extension: How to handle paging if an extension is busy (such as on a call).

Duplex: If you enable duplex, the extensions that are called in the page group will not be muted, which will allow anyone to talk in the page group. Usually this will be set to No.

Default Page Group: Whether to consider this page group a "default" page group.

When finished building the paging group, click the Submit button and then click the Apply Config button.

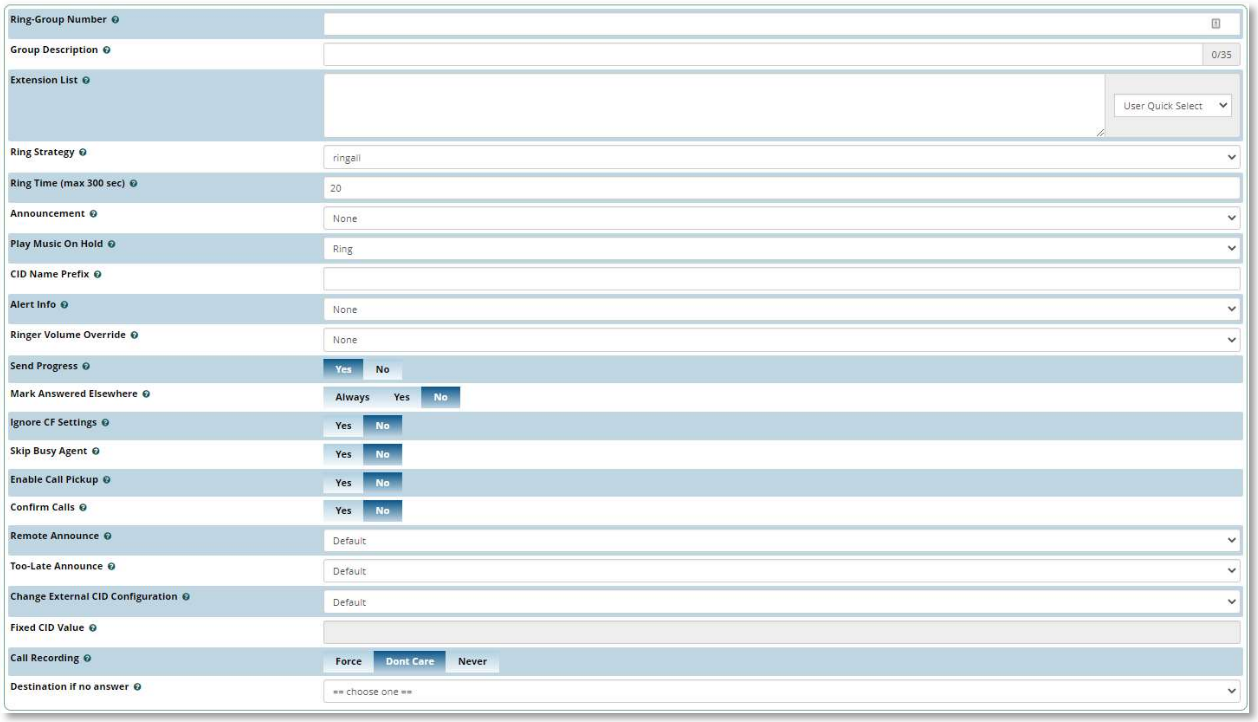
Ring Groups

On the top menu hover your mouse over 'Applications' and click on 'Ring Groups'

The Ring Groups module provides a method to ring several extensions with a variety of ring strategies.

Creating a New Ring Group

Click on +Add Ring Group



Ring-Group Number	
Group Description	0/35
Extension List	User Quick Select
Ring Strategy	ringall
Ring Time (max 300 sec)	20
Announcement	None
Play Music On Hold	Ring
CID Name Prefix	
Alert Info	None
Ringer Volume Override	None
Send Progress	[✓ Yes] No
Mark Answered Elsewhere	Always Yes [✓ No]
Ignore CF Settings	Yes [✓ No]
Skip Busy Agent	Yes [✓ No]
Enable Call Pickup	Yes [✓ No]
Confirm Calls	Yes [✓ No]
Remote Announce	Default
Too-Late Announce	Default
Change External CID Configuration	Default
Fixed CID Value	
Call Recording	Force [✓ Dont Care] Never
Destination if no answer	== choose one ==

Ring Group Number: The number to dial to reach this ring group.

Group Description: A descriptive title for the ring group to help you identify it.

Ring Strategy: The Ring Strategy allows you to set how the extensions listed in the Follow Me list are dialed. These options include:

- **ringall:** ring Extension for duration set in Initial Ring Time, and then terminate call to Extension and ring Follow-Me List for duration set in Ring Time.
- **hunt:** take turns ringing each available extension
- **memoryhunt:** ring first extension in the list, then ring the 1st and 2nd extension, then ring 1st 2nd and 3rd extension in the list.... etc.
- ***-prim:** these modes act as described above. However, if the primary extension (first in list) is occupied, the other extensions will not be rung. If the primary is in do-not-disturb (DND) mode, it won't be rung. If the primary is in call forward (CF) unconditional mode, then all will be rung.
- **firstavailable:** ring only the first available channel
- **firstnotonphone:** ring only the first channel which is not off hook - ignore CW

Ring Time: The time, in seconds, that the phones will be rung. For hunt-style strategies, this is the ring time for each iteration.

Announcement: Message to be played to the caller prior to calling the ring group.

Play Music on Hold: The default setting is to play ringing to the caller.

CID Name Prefix: You can optionally prefix the CallerID name when ringing extensions in this group. For Example, if you prefix with "Code Blue:", a call from 1st Floor Stairwell would display as "Code Blue: 1st Floor Stairwell" on the extensions that ring.

Ignore CF Settings: When set to Yes, agents who attempt to call forward will be ignored.

Remote Announce: Message to be played to the person receiving the call.

Too-Late Announce: Message to be played to the person receiving the call if the call is accepted by someone else.

Change External CID Configuration: Select from the following modes.

- Default
  - This transmits the caller's CID if allowed by the trunk.
- Fixed CID Value
  - This always transmits the ”Fixed CID Value” entered below.
- Outside Calls Fixed CID
  - This will transmit the “Fixed CID Value” value only on calls that come from the outside. Internal extension-to-extension calls will still operate in default mode.
- Use Dialed Number
  - This will transmit the number that was dialed as the CID for calls coming from the outside. Internal extension-to-extension calls will still operate in default mode. There must be a DID on the inbound route for this. This will be blocked on trunks that block foreign caller ID.
- Force Dialed Number

- This will transmit the number that was dialed as the CID for calls coming from the outside. Internal extension-to-extension calls will still operate in default mode. There must be a DID on the inbound route for this. This will be transmitted on trunks that block foreign caller ID.

Fixed CID Value: When needed, enter your "Fixed CID Value" here.

Call Recording: You can always record calls that come into this ring group (Force), never record them (Never), or allow the extension that answers to do on-demand recording (Don't Care).

Destination if no answer: Choose where to send the call after the ring time has been exceeded or after a -prim mode prevents ringing the group. Most often, this is set to an extension or group.

When finished click the Submit button, then click the Apply Config button.

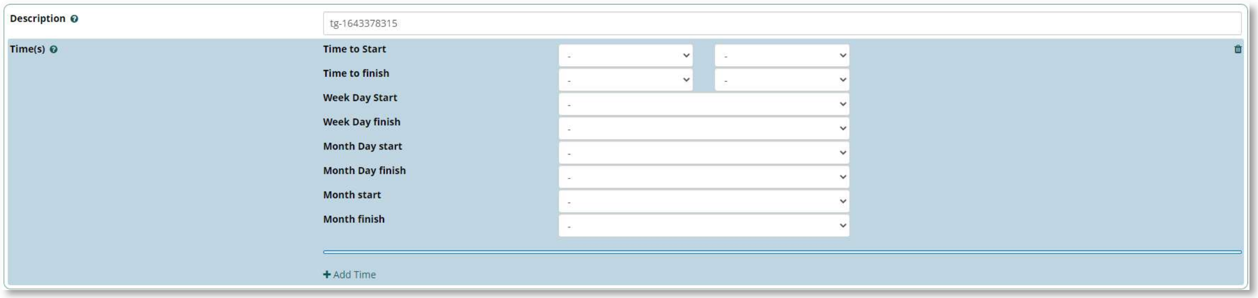
Time Groups

On the top menu hover your mouse over 'Applications' and click on 'Time Groups'

A Time Group is a list of times against which incoming or outgoing external calls are checked. These rules do not apply to internal calls. The rules specify a time range, by the time, day of the week, day of the month, and month of the year. Time groups are associated with time conditions, which control the destination of a call based on the time

Creating a Time Group

Click on +Add Time Group



Description		tg-1643378315	
Time(s)	Time to Start	-	-
	Time to finish	-	-
	Week Day Start	-	
	Week Day finish	-	
	Month Day start	-	
	Month Day finish	-	
	Month start	-	
	Month finish	-	

Description: Enter a description to identify this time group.

Times: This is where you will define a time range. By default, there is one range available. You can define multiple ranges in the same time group by clicking the Add Time button.

Available parameters are:

- Time to start
- Time to finish

- Week day start
- Week day finish
- Month Day start
- Month Day finish
- Month start
- Month finish

Unset (blank) week day, month day, and month parameters will default to "all." For example, setting a start time of 09:00 and an end time of 17:00, and nothing else (no day, month, etc.), will make the condition true from 9AM to 5PM every day of the week, every day of the month, every month of the year.

When done building the Time Group Click the Submit button, then click the Apply Config button.

After you create a time group, it will become available for selection in the Time Conditions module.

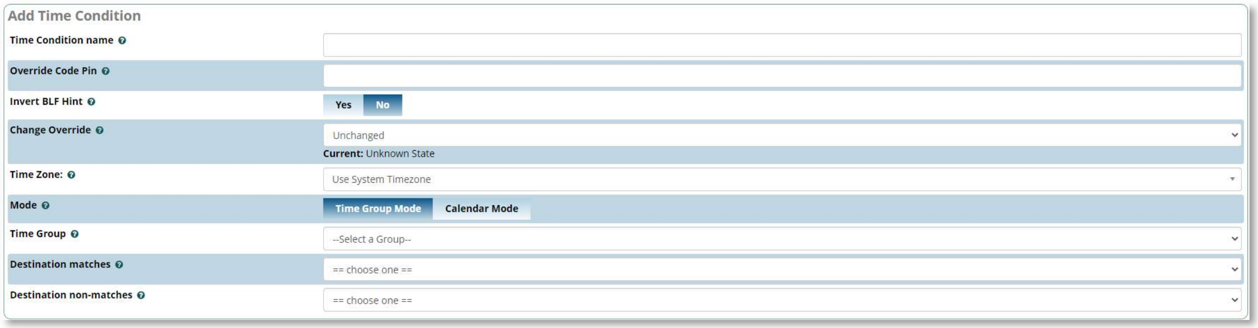
Time Conditions

On the top menu hover your mouse over ‘Applications’ and click on ‘Time Conditions’

The Time Conditions module defines a set of rules based on time groups. A time condition has two call destinations, one if the time of the call matches the time group assigned, and another if there is no match.

Creating a Time Condition

Click on +Add Time Condition



Add Time Condition

Time Condition name	
Override Code Pin	
Invert BLF Hint	Yes [✓ No]
Change Override	Unchanged Current: Unknown State
Time Zone:	Use System Timezone
Mode	[✓ Time Group Mode] Calendar Mode
Time Group	--Select a Group--
Destination matches	== choose one ==
Destination non-matches	== choose one ==

Time condition Name: Enter a description to identify this time condition.

Override Code Pin: If a PIN is entered here, users will be prompted to enter the PIN after dialing the override feature code.

Time Zone: Specify the time zone by name if the destinations are in a different time zone than the server.

Mode: Select the Mode for checking time conditions

Time Group: Select a Time Group created under Time Groups.

Destination Matches: Choose Destination route for calls that match the time group.

Destination non-Matches: Choose Destination route for calls that do not match the time group.

When done building the Time Group Click the Submit button, then click the Apply Config button.

Connectivity Modules

Browse to the IP address of Blue Alert Connect in any browser. Log into Blue Alert Connect using the credentials:

Username: cbadmin

Password: codeblue

On the top menu hover your mouse over ‘Connectivity’ to see the available modules.

Inbound Routes

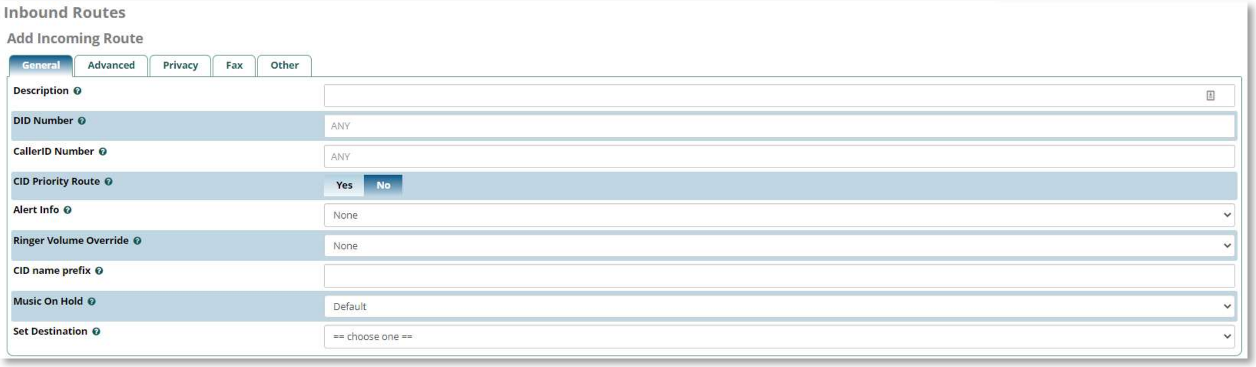
On the top menu hover your mouse over ‘Connectivity’ and click on ‘Inbound Routes’

The Inbound Routes module is the mechanism used to tell Blue Alert Connect where to route inbound calls based on the phone number or DID dialed. This module is used to handle SIP, PRI, and analog inbound routing.

Adding an Inbound Route

Blue Alert Connect allows two specific types of inbound routing: DID & CID Routing. These two routing methods can be used on their own or in conjunction with one another. Leaving both fields blank will create a route that matches all calls.

Near the top left of the page click on Add Inbound Route



Inbound Routes

Add Incoming Route

Description	
DID Number	ANY
CallerID Number	ANY
CID Priority Route	Yes [✓ No]
Alert Info	None
Ringer Volume Override	None
CID name prefix	
Music On Hold	Default
Set Destination	== choose one ==

Description: Enter a unique description to identify the route.

DID Number: In the DID field, you will define the expected “DID Number”. Leave this blank to match calls with any or no DID info. The DID number entered must match the format of the provider sending the DID. You can also use a pattern match to match a range of numbers. Patterns must begin with an underscore (_) to signify they are patterns. Within patterns, X will match the numbers 0-9 and N will match number 2-9 and specific numbers can be matched if they are placed between square parentheses. For example, “_212NXXXXXX” (without the quotes) will match any DID with a 212-area code. This field can also be left blank to match calls from all DIDs. This will also match calls that have no DID information.

CallerID Number: Routing calls based on the caller ID number of the person that is calling. Define the caller ID number to be matched on incoming calls. Leave this field blank to match any or no CID info. In addition to standard dial sequences, you can also put “Private,” “Blocked,” “Unknown,” “Restricted,” “Anonymous” or “Unavailable” to catch these special cases if the telco transmits them. Caller ID can be specified as a dial pattern when prefixed with an underscore, so for example to intercept all calls from area code 902, CID can be specified as "_902NXXXXXX" (without the quotes).

CID Priority Routes: This will only affect routes that do not have an entry in the DID field. If set to Yes, calls with this CID will be routed to this route, even if there is a route to the DID that was called.

Priority levels are matched in the following way.

With CID Priority Route disabled:

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

With CID Priority Route enabled:

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

Set Destination: Blue Alert Connect provides multiple ways to route a call, from extensions, trunks, IVRs and more. This is the place where the desired call target is selected.

When done click Submit in the bottom right of the page a Apply Config at the top of the page.

Outbound Routes

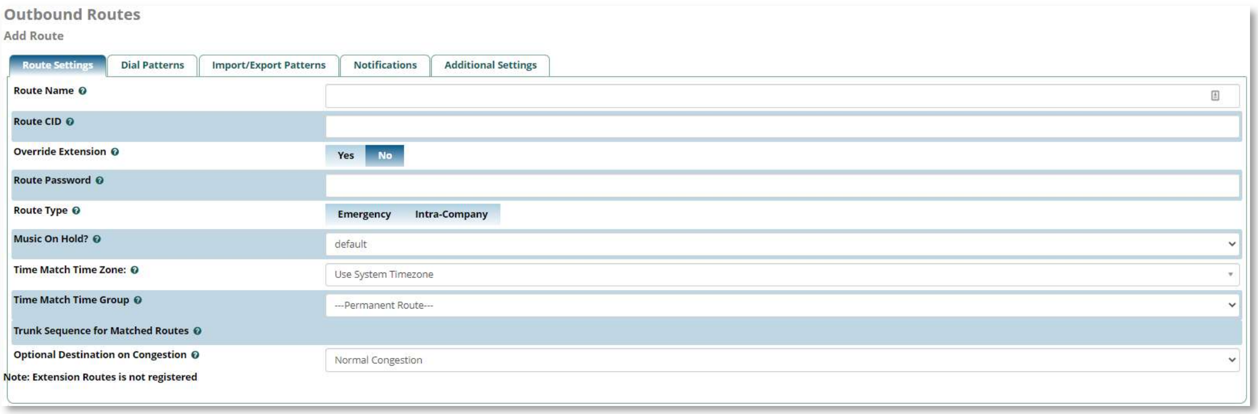
On the top menu hover your mouse over ‘Connectivity’ and click on ‘Outbound Routes’

Outbound routing is a set of rules that Blue Alert Connect uses to decide which trunk to use for an outbound call. Outbound routes are used to specify what numbers are allowed to go out a particular route.

Adding an Outbound Route

Near the top left of the page click on Add Outbound Route

Route Settings Tab



Outbound Routes
Add Route

Route Settings | Dial Patterns | Import/Export Patterns | Notifications | Additional Settings

Route Name	
Route CID	
Override Extension	Yes [✓ No]
Route Password	
Route Type	Emergency Intra-Company
Music On Hold?	default
Time Match Time Zone:	Use System Timezone
Time Match Time Group	---Permanent Route---
Trunk Sequence for Matched Routes	
Optional Destination on Congestion	Normal Congestion

Note: Extension Routes is not registered

Route Name: Name of this route. Usually used to describe what type of calls this route matches (for example, "local" or "longdistance"). Cannot contain spaces.

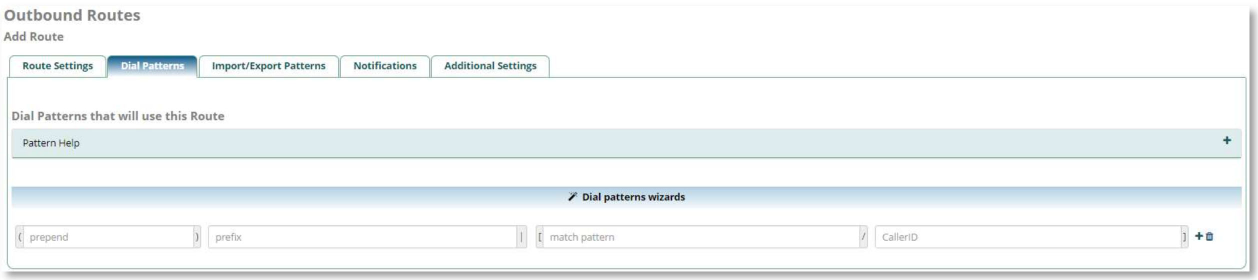
Route CID: Optional route Caller ID to be used for this route. If set, this will override all CIDs specified unless Trunk CID is set to force override or Override Extension option is set to no.

Override Extension: If set to Yes, the extension's Outbound CID will be ignored in favor of the route CID set above.

Route Type: Optional settings to determine whether the route is considered an emergency or intra-company route.

Time Group: If this route should only be available during certain times, then select a time group created under the Time Groups module.

Dial Patterns Tab



Outbound Routes
Add Route

Route Settings | Dial Patterns | Import/Export Patterns | Notifications | Additional Settings

Dial Patterns that will use this Route

Pattern Help +

Dial patterns wizards

(prepend) prefix | [match pattern / CallerID]

You can enter any combination of numbers and the following special patterns:

PATTERN	DESCRIPTION
X	Any whole number from 0-9
Z	Any whole number from 1-9
N	Any whole number from 2-9
[###]	Any whole number in the brackets, example [123] is 1 OR 2 OR 3. Note that multiple numbers can be separated by commas and ranges of numbers can be specified with a dash ([1.3.6-8]) would match the numbers 1,3,6,7 and 8.
.	It matches one or more characters and (acts as a wildcard)

Prepend: The prepend will be added to the beginning of a successful match. If the dialed number matches the patterns specified by the subsequent columns, then this will be prepended to the sequence before sending it to the trunks.

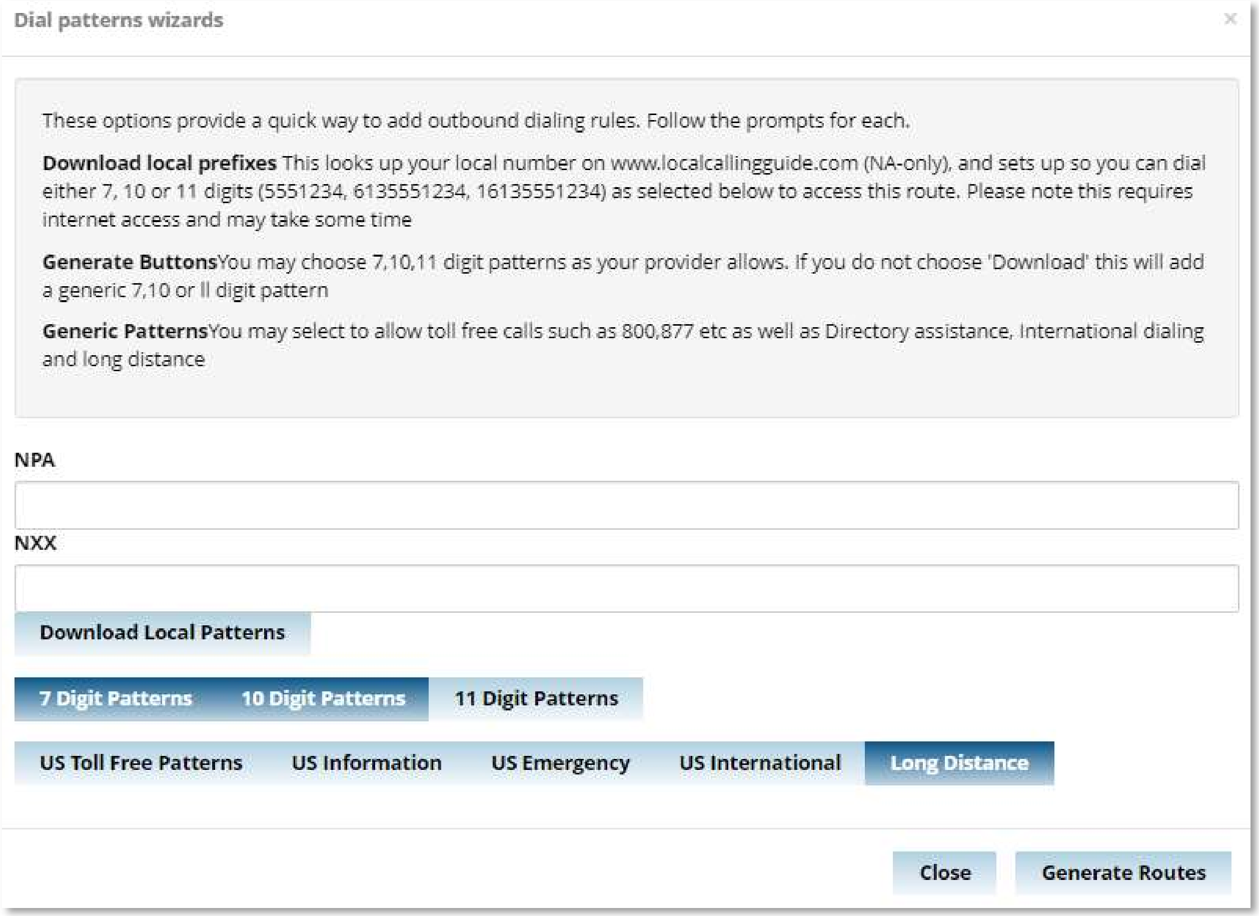
Prefix: Prefix to remove upon a successful match. The dialed number is compared to this and the subsequent columns for a match (prefix + match pattern). Upon a match, this prefix is removed (stripped) from the dialed number before sending the sequence to the trunks.

Match Pattern: The dialed number will be compared against the prefix + this match pattern. Upon a match, the match pattern portion of the dialed number will be sent to the trunks.

CallerID: If caller ID is supplied, the dialed number will only match the prefix + match pattern if the caller ID being transmitted matches this. When extensions make outbound calls, the caller ID will be their extension number and NOT their outbound CID. The above special matching sequences can used for caller ID matching similar to other number matches.

Dial Pattern Wizard: These are pre-constructed dial patterns. Selecting a pre-made pattern will automatically populate the Dial Pattern fields.

To use a wizard, click the “Dial patterns wizards” button.



Dial patterns wizards

These options provide a quick way to add outbound dialing rules. Follow the prompts for each.

Download local prefixes This looks up your local number on www.localcallingguide.com (NA-only), and sets up so you can dial either 7, 10 or 11 digits (5551234, 6135551234, 16135551234) as selected below to access this route. Please note this requires internet access and may take some time

Generate Buttons You may choose 7,10,11 digit patterns as your provider allows. If you do not choose 'Download' this will add a generic 7,10 or ll digit pattern

Generic Patterns You may select to allow toll free calls such as 800,877 etc as well as Directory assistance, International dialing and long distance

Select one or more pattern options in the next line of buttons.

Once you have selected your options click the Generate Routes button on the bottom right.

Once you have built your Dial Patterns click the Submit button at the bottom right of the page and the Apply Config button at the top of the page.

Trunks

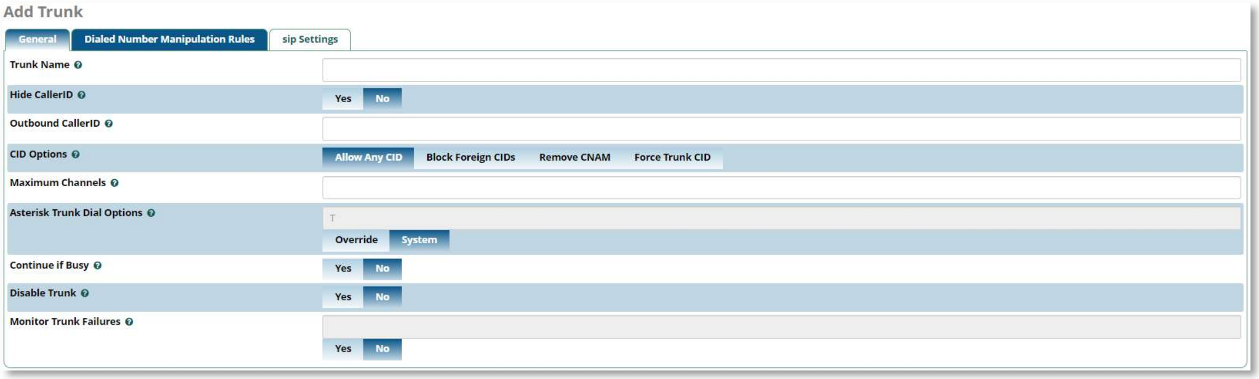
On the top menu hover your mouse over ‘Connectivity’ and click on ‘Trunks’

The Trunks module is where you control connectivity to the PSTN and your VoIP provider(s). This is where you also control connections to other PBX’s. The most common trunk is SIP and examples will be covered in this guide. Other than the Extensions module, the Trunks module is one of the most critical modules on the system and allows for a great deal of flexibility.

Adding a Trunk

Click on the “+Add Trunk” button near the top of the page. In this guide we will be covering SIP (chan_sip) Trunks (second option in the drop-down menu). For other types of Trunks please contact technicalsupport@codeblue.com for assistance.

General Tab



Add Trunk

Trunk Name	
Hide CallerID	Yes [✓ No]
Outbound CallerID	
CID Options	[✓ Allow Any CID] Block Foreign CIDs Remove CNAM Force Trunk CID
Maximum Channels	
Asterisk Trunk Dial Options	T Override [✓ System]
Continue if Busy	Yes [✓ No]
Disable Trunk	Yes [✓ No]
Monitor Trunk Failures	Yes [✓ No]

For most instances, a Trunk name will be added, and the rest of the settings will be left as default.

Trunk Name: Set a descriptive name to identify the trunk.

Hide CallerID: Set the options to hide the caller ID sent out over digital lines

Outbound CallerID: Use this field to specify caller ID for calls placed out of this trunk with the <NXXNXXXXXX> format.

CID Options: This setting determines what CIDs will be allowed out of this trunk.

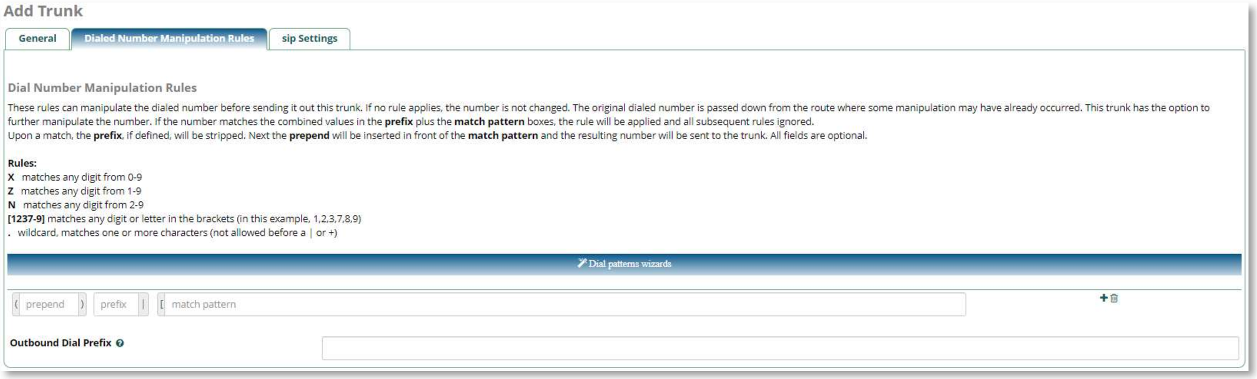
Maximum Channels: Controls the maximum number of outbound channels (simultaneous calls) that can be used on this trunk.

Asterisk Trunk Dial Options: Asterisk Dial command options to be used when calling out this trunk. To override the Advanced Settings default, check the box and then provide the required options for this trunk. The Default of “T” is almost never changed and will work with the vast majority of systems.

Continue if Busy: Normally the next trunk is only tried upon a trunk being 'Congested' in some form, or unavailable. Checking this box will force a failed call to always continue to the next configured trunk or destination even when the channel reports BUSY or INVALID NUMBER. This should normally be unchecked

Disable Trunk: Check this to disable this trunk in all routes where it is used.

Dialed Number Manipulation Rules Tab



Add Trunk

Dial Number Manipulation Rules

These rules can manipulate the dialed number before sending it out this trunk. If no rule applies, the number is not changed. The original dialed number is passed down from the route where some manipulation may have already occurred. This trunk has the option to further manipulate the number. If the number matches the combined values in the **prefix** plus the **match pattern** boxes, the rule will be applied and all subsequent rules ignored.
Upon a match, the **prefix**, if defined, will be stripped. Next the **prepend** will be inserted in front of the **match pattern** and the resulting number will be sent to the trunk. All fields are optional.

Rules:
X matches any digit from 0-9
Z matches any digit from 1-9
N matches any digit from 2-9
[1237-9] matches any digit or letter in the brackets (in this example, 1,2,3,7,8,9)
. wildcard, matches one or more characters (not allowed before a | or +)

Outbound Dial Prefix

This tab allows you to manipulate the dialed number before sending it out this trunk. If no rule applies, the number is not changed. The original dialed number is passed down from the route where some manipulation may have already occurred, most commonly in the Outbound routes settings.

You can enter any combination of numbers and the following special patterns:

PATTERN	DESCRIPTION
X	Any whole number from 0-9
Z	Any whole number from 1-9
N	Any whole number from 2-9
[###]	Any whole number in the brackets, example [123] is 1 OR 2 OR 3. Note that multiple numbers can be separated by commas and ranges of numbers can be specified with a dash ([1.3.6-8]) would match the numbers 1,3,6,7 and 8.
.	It matches one or more characters and (acts as a wildcard)

Prepend: The prepend will be added to the beginning of a successful match. If the dialed number matches the patterns specified by the subsequent columns, then this will be prepended to the sequence before sending it to the trunks.

Prefix: Prefix to remove upon a successful match. The dialed number is compared to this and the subsequent columns for a match (prefix + match pattern). Upon a match, this prefix is removed (stripped) from the dialed number and any prepend added before sending the sequence through the trunk.

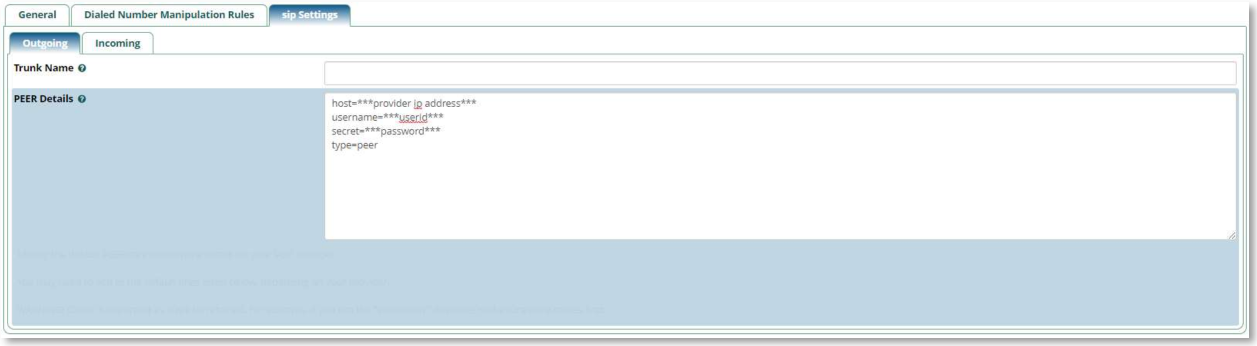
Match Pattern: The dialed number will be compared against the prefix + this match pattern. Upon a match, this portion of the number will be sent to the trunks after removing the prefix and appending the prepend digits.

Dial Pattern Wizard: These are pre-constructed dial patterns. Selecting a pre-made pattern will automatically populate the Dial Pattern fields.

To use a wizard, click the “Dial patterns wizards” button.

SIP Settings Tab

Outgoing Tab



Trunk Name

PEER Details

```
host=***provider ip address***
username=***userid***
secret=***password***
type=peer
```

Trunk Name: Give the trunk a descriptive name to identify the Trunk

PEER Details: Here you give the PEER connection parameters. This information could be provided by your VoIP provider. You may need to add to the provided default settings and in some cases remove default settings depending on your provider or application.

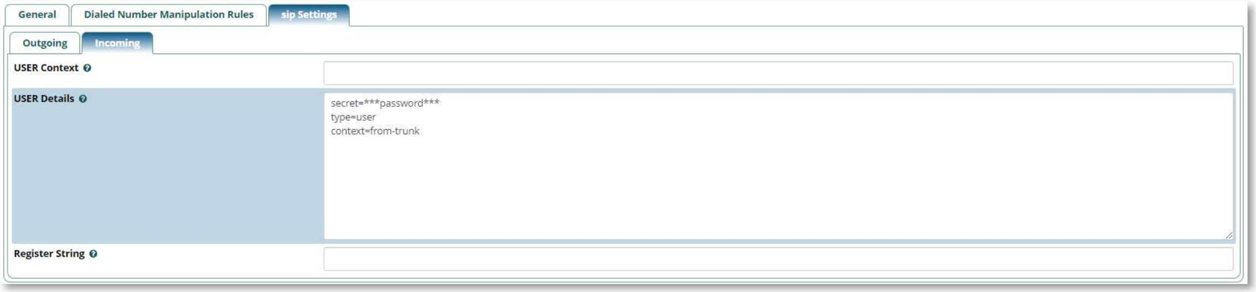
Here are some examples of common configurations:

```
host=10.0.0.100
type=peer
qualify=yes
context=from-internal
```

or

```
host=192.168.159.154
type=peer
username=Blue Alertconect
secret=c0d$B1u&
context=from-pstn
```

Incoming Tab



USER Context

USER Details

```
secret=***password***
type=user
context=from-trunk
```

Register String

USER Context: Normally a descriptive name to identify the USER of the trunk This is sometimes the account name or number supplied by your VoIP provider.

USER Details: Here you supply the USER connection parameters. Sometimes supplied by your VoIP provider. You may need to add to the provided default settings and in some cases remove default settings depending on your provider or application.

Here is an example of a common configuration:

```
host=10.0.0.100
type=user
context=from-trunk
```

Once you are done building the Trunk click the Submit button at the bottom right of the page and the Apply Config button at the top of the page.

Cisco Unified Call Manager Trunk Setup

1. Login to Cisco Unified Communication Manager.
2. Create a Trunk between CUCM and Connect. To do this follow the below shared steps.
   - Go to Device -> Trunk -> Add a New Trunk -> Trunk Type = SIP Trunk
   - Device Protocol -> SIP Trunk
   - Trunk Service Type -> None (Default)
   - Click on Next
   - Device Name – Trunk-to-Connect
   - Description – Trunk configured for Connect
   - Device Pool – Select appropriate Device Pool
   - MRGL – Select appropriate MRGL
   - Location – Select appropriate Location
   - Check Mark – Media Termination Point Required
   - Check Mark – Retry Video Call as Audio
   - Inbound Calls – Select appropriate Calling Search Space
   - Check Mark – Redirecting Diversion Header Delivery – Inbound
   - SIP Information – Enter Connect IP Address under Destination Address X.X.X.X
   - Enter the Port as 5060

- Select SIP Trunk Security Profile – Non-Secure SIP Trunk Security Profile
- SIP Profile – Standard SIP Profile
- Click on Save
- Click on Apply

3. Create Route Pattern which points to Connect. To do this follow the below shared steps.

- Go to Call Routing -> Route/Hunt -> Route Pattern
- Click on Add New
- Route Pattern -> Enter appropriate Route Pattern which will be routed to Connect
- Route Partition -> Enter appropriate Route Partition which a caller can call
- Gateway/Route List -> Select the trunk which was created in Point 2.

4. Change Outgoing Transport Type as UDP. To do this follow the below shared steps.

- Go to System -> Security -> Non-Secure SIP Trunk Security Profile
- Select Outgoing Transport Type as UDP
- Click on Save
- Click on Apply

Reports Modules

Browse to the IP address of Blue Alert Connect in any browser. Log into Blue Alert Connect using the credentials:

Username: cbadmin

Password: codeblue

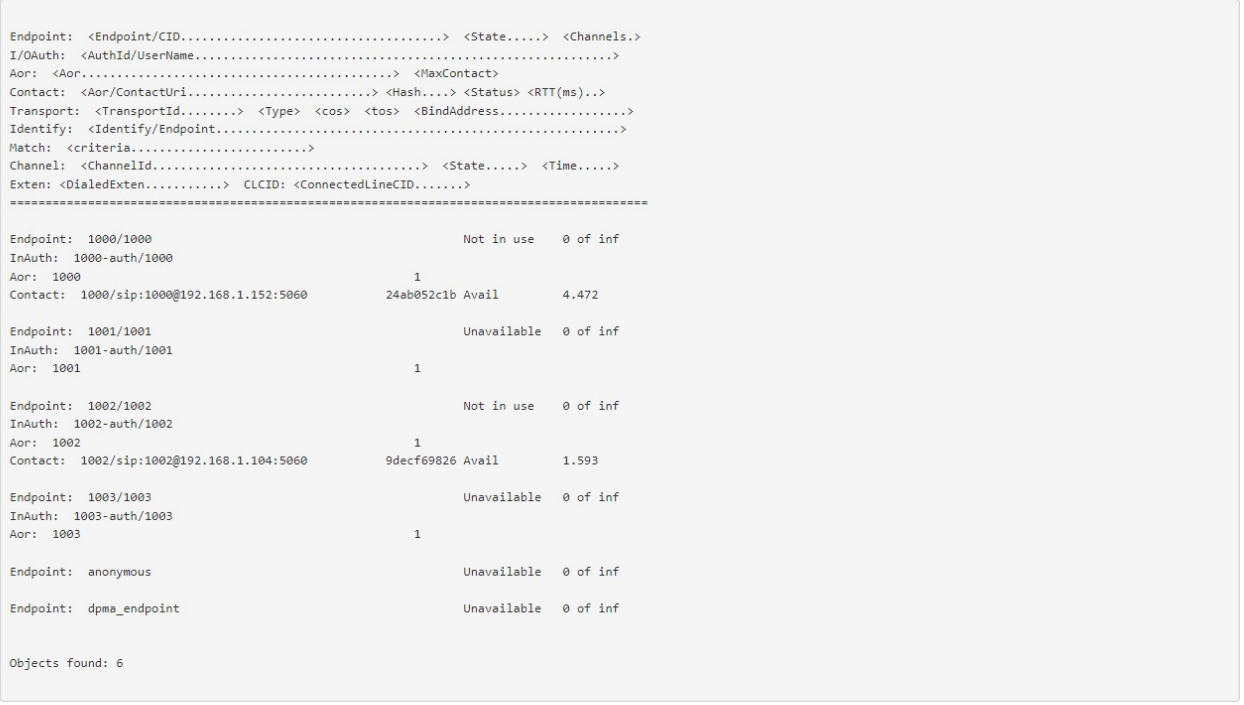
On the top menu hover your mouse over ‘Reports’ to see the available modules.

Asterisk Info

On the top menu hover your mouse over ‘Reports’ and click on ‘Asterisk Info’

The Asterisk Info page gives you the ability to look at key things in Asterisk such as extension registration information and is typically used to troubleshoot issues.

As seen in the example below looking at the “Peers” section of the report will show which extensions or online and which are offline.



```
Endpoint:  <Endpoint/CID.....................................>  <State.....>  <Channels.>
I/OAuth:  <AuthId/UserName...........................................................>
Aor:  <Aor............................................>  <MaxContact>
Contact:  <Aor/ContactUri..........................> <Hash....> <Status> <RTT(ms)..>
Transport:  <TransportId........>  <Type>  <cos>  <tos>  <BindAddress..................>
Identify:  <Identify/Endpoint.........................................................>
Match:  <criteria.........................>
Channel:  <ChannelId......................................>  <State.....>  <Time.....>
Exten: <DialedExten...........>  CLCID: <ConnectedLineCID.......>
==========================================================================================

Endpoint:  1000/1000                                            Not in use    0 of inf
InAuth:  1000-auth/1000
Aor:  1000                                                1
Contact:  1000/sip:1000@192.168.1.152:5060           24ab052c1b Avail         4.472

Endpoint:  1001/1001                                            Unavailable   0 of inf
InAuth:  1001-auth/1001
Aor:  1001                                                1

Endpoint:  1002/1002                                            Not in use    0 of inf
InAuth:  1002-auth/1002
Aor:  1002                                                1
Contact:  1002/sip:1002@192.168.1.104:5060           9decf69826 Avail         1.593

Endpoint:  1003/1003                                            Unavailable   0 of inf
InAuth:  1003-auth/1003
Aor:  1003                                                1

Endpoint:  anonymous                                            Unavailable   0 of inf

Endpoint:  dpma_endpoint                                        Unavailable   0 of inf


Objects found: 6
```

Asterisk Logfiles

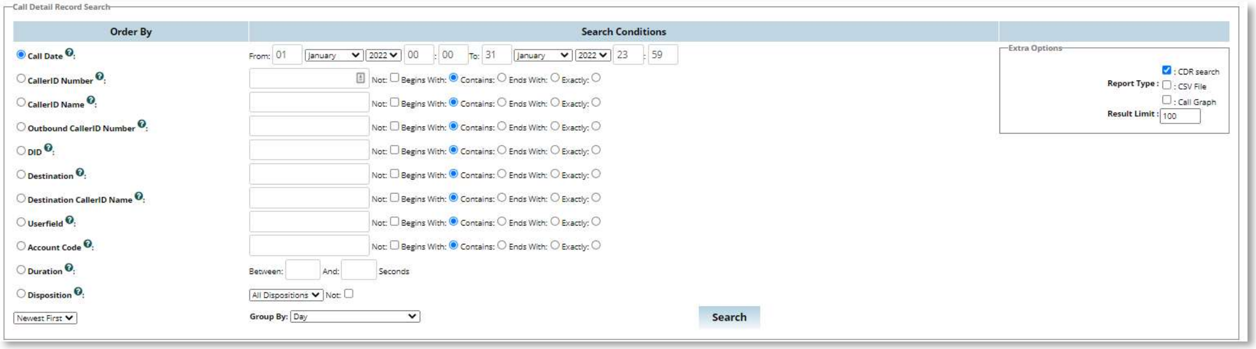
On the top menu hover your mouse over ‘Reports’ and click on ‘Asterisk Log Files’

The Asterisk logfiles allows you to view a live feed of log files automatically generated. This can be a very useful debug and troubleshooting tool to get information of current operations.

CDR Reports

On the top menu hover your mouse over ‘Reports’ and click on ‘CDR Reports’

Call Reports is designed to be the raw data of all call activity on your phone system.



Call Detail Record Search

Order By	Search Conditions	
● Call Date:	From: 01 January 2022 00 : 00 To: 31 January 2022 23 : 59	Extra Options Report Type : ☑ : CDR search □ : CSV File □ : Call Graph Result Limit : 100
○ CallerID Number:	Not: □ Begins With: ● Contains: ○ Ends With: ○ Exactly: ○	
○ CallerID Name:	Not: □ Begins With: ● Contains: ○ Ends With: ○ Exactly: ○	
○ Outbound CallerID Number:	Not: □ Begins With: ● Contains: ○ Ends With: ○ Exactly: ○	
○ DID:	Not: □ Begins With: ● Contains: ○ Ends With: ○ Exactly: ○	
○ Destination:	Not: □ Begins With: ● Contains: ○ Ends With: ○ Exactly: ○	
○ Destination CallerID Name:	Not: □ Begins With: ● Contains: ○ Ends With: ○ Exactly: ○	
○ Userfield:	Not: □ Begins With: ● Contains: ○ Ends With: ○ Exactly: ○	
○ Account Code:	Not: □ Begins With: ● Contains: ○ Ends With: ○ Exactly: ○	
○ Duration:	Between: And: Seconds	
○ Disposition:	All Dispositions Not: □	
Newest First	Group By: Day	

CDR Reports can be filtered by:

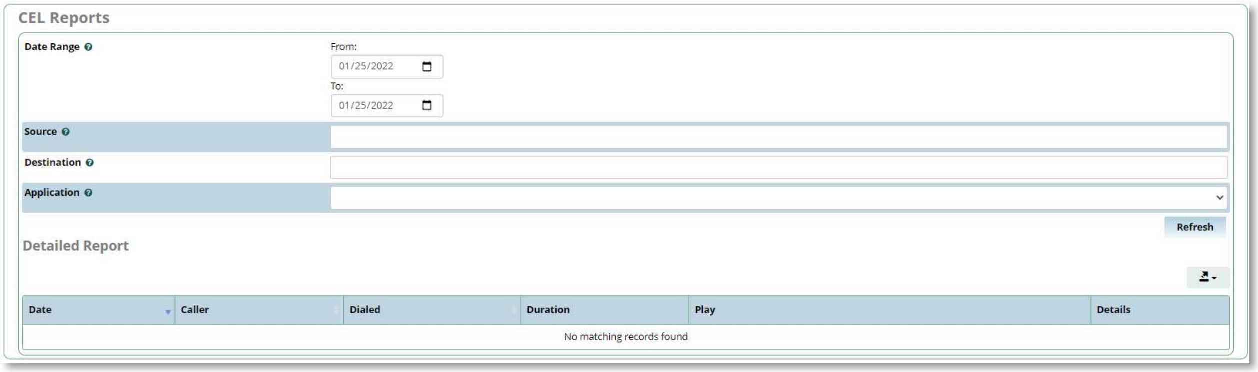
- Call Date
- CallerID Number
- CallerID Name
- Outbound CallerID Number
- DID
- Destination
- Destination CallerID Name
- Userfield
- Account Code
- Duration
- Disposition

Once a filter has been selected and modified click the Search button at the bottom of the page. The CDR will then populate a table with any call information matching the filter and display all Call Detail Records.

Call Event Logging

On the top menu hover your mouse over 'Reports' and click on 'Call Event Logging'

The Call Event Logging module allows you to see all inbound and outbound calls and listen to any call recordings that are associated with that call.



CEL Reports

Date Range: From: 01/25/2022 To: 01/25/2022

Source:

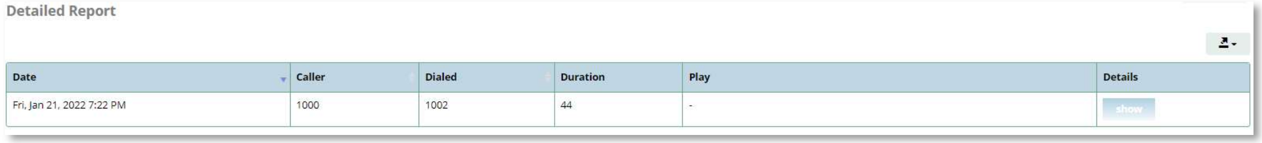
Destination:

Application:

Detailed Report

Date	Caller	Dialed	Duration	Play	Details
No matching records found					

The Call Event Logs can be filtered based on the Date, Source, Destination, or Application. Once the field is entered click the refresh button on the bottom right to show any and all calls that match the filter.



Detailed Report

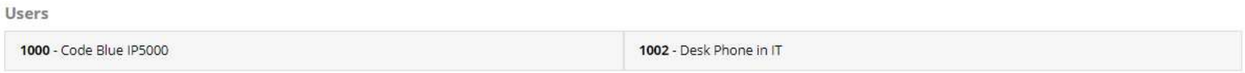
Date	Caller	Dialed	Duration	Play	Details
Fri, Jan 21, 2022 7:22 PM	1000	1002	44	-	show

Clicking on Show button, a window displays the channel events in detail for the call. This is a very helpful troubleshooting tool when calls are not completing.

Print Extensions

On the top menu hover your mouse over ‘Reports’ and click on ‘Print Extensions’

The Print Extensions Module is a useful tool that allows you to print a list of all numbers that can be dialed from or to your system.



Users

1000 - Code Blue IP5000	**1002** - Desk Phone in IT

This would include extensions and inbound routes, which are numbers that an outside caller will be routed to if dialed.

Settings Modules

Browse to the IP address of Blue Alert Connect in any browser. Log into Blue Alert Connect using the credentials:

Username: cbadmin

Password: codeblue

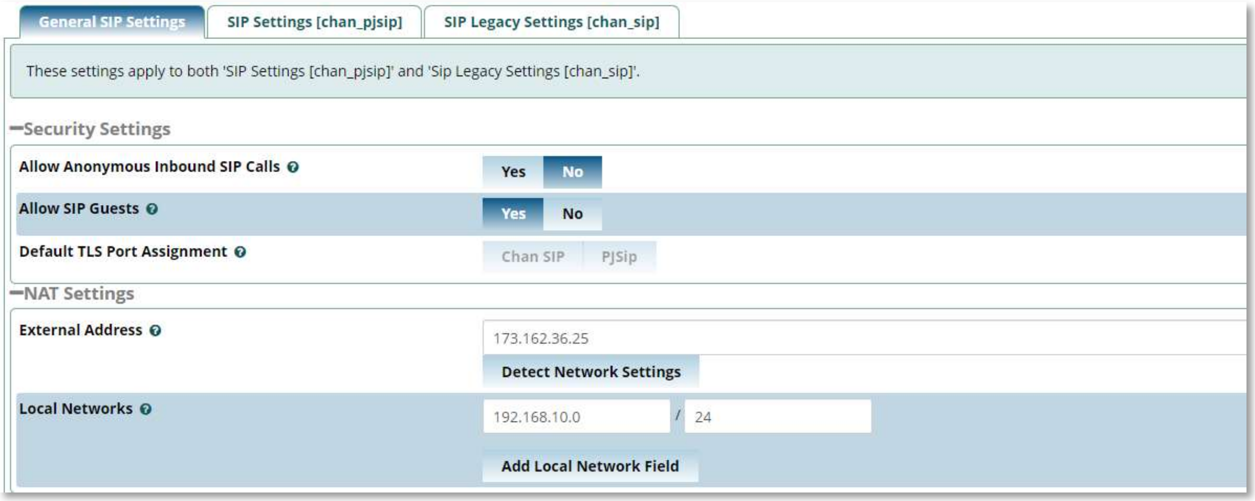
On the top menu hover your mouse over ‘Settings’ to see the available modules.

Asterisk SIP Settings

On the top menu hover your mouse over ‘Settings’ and click on ‘Asterisk SIP Settings’

The Asterisk SIP Settings Module is used to configure the default settings used for SIP calls. This module allows you to modify the default port settings of SIP based calls as well as allow/disallow certain features.

***Please Note; If experiencing Audio Issues (One-way audio or no audio) click the “Detect Network Settings” and add any subnets that will contain End Points under General SIP settings and then reboot the server. ***



These settings apply to both 'SIP Settings [chan_pjsip]' and 'Sip Legacy Settings [chan_sip]'.

−Security Settings

Allow Anonymous Inbound SIP Calls	Yes [✓ No]
Allow SIP Guests	[✓ Yes] No
Default TLS Port Assignment	Chan SIP PJSip

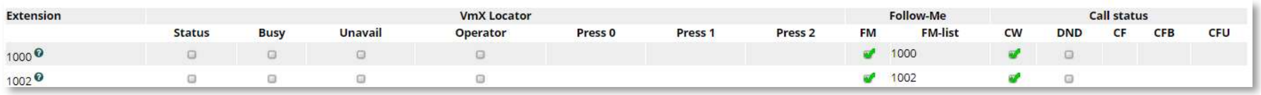
−NAT Settings

External Address	173.162.36.25
Local Networks	192.168.10.0 / 24

Extension Settings

On the top menu hover your mouse over ‘Settings’ and click on ‘Extension Settings’

The Extension Settings page will show you each extension on your system and whether that extension has Call Waiting, Do Not Disturb, Call Forwarding, VMX Locator, Follow-Me, and other features enabled or disabled.

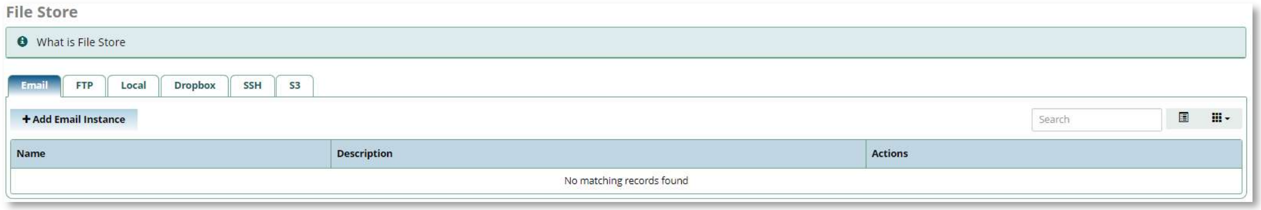


Extension	VmX Locator							Follow-Me		Call status				
	Status	Busy	Unavail	Operator	Press 0	Press 1	Press 2	FM	FM-list	CW	DND	CF	CFB	CFU
1000 ?	□	□	□	□				✓	1000	✓	□			
1002 ?	□	□	□	□				✓	1002	✓	□			

Filestore

On the top menu hover your mouse over ‘Settings’ and click on ‘Filestore’

The Filestore module provides a simple interface to various storage options to transfer and store backups from the Backup & Restore module.



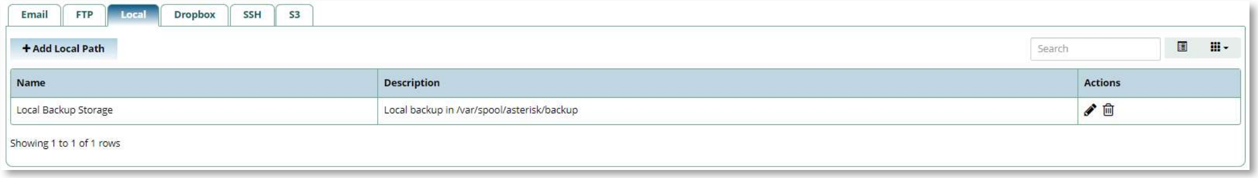
File Store

What is File Store

Name	Description	Actions
No matching records found		

Storage options include E-mail, FTP, Local, SSH, S3 and Dropbox.

If stored locally the backup file will by default be stored at /var/spool/asterisk/backup as shown below.



Name	Description	Actions
Local Backup Storage	Local backup in /var/spool/asterisk/backup	✎ 🗑

Showing 1 to 1 of 1 rows