TOOLVOX®

BLUE ALERT CONNECT

BLUE ALERT® MONITOR PRO

ToolVox®

XS Servier Appliance & XV Virtual Machine

Also Included: Blue Alert® Connect & Monitor Pro

Admin Guide

Installation | Configuration | Support | Maintenance | Use

Code Blue®

Table of Contents

Introduction

ToolVox is a highly versatile emergency management platform for blue light phone networks, consisting of Blue Alert Connect and Blue Alert Monitor Pro Media Gateway and administration software. The platform offers unique real-time monitoring capabilities and provides connections to PBX, public telephone (PSTN), and Internet (ISP) networks, in addition to third-party security platforms.

ToolVox is offered in three configurations. As a physical on-premises deployment, a Virtual Machine, and a Cloud Hosted option. This guide will cover the configuration and settings of the Physical and Virtual Machine Versions of the ToolVox.

Getting Started

Default IP Address for ToolVox XS

Note: ToolVox XV is left at DHCP

- Blue Alert Connect: 192.168.0.11
- Blue Alert Monitor Pro: 192.168.0.11:3000
- Webmin: 192.168.0.11:10000
- Proxmox (ToolVox XS only): 192.168.0.10:8006

Default Login Credentials

⚠ **SECURITY WARNING**: Default passwords should be changed immediately after installation.

Recommended password requirements:

- Minimum 12 characters

- Mixed case, numbers, and special characters

- Different passwords for each service

- Blue Alert CLI:
  - Username: cbadmin
  - Password: CodeBlue92

- Blue Alert Connect:
  - Username: cbadmin
  - Password: codeblue
- Blue Alert Monitor Pro:
  - Username/Email: cbadmin@codeblue.com
  - Password: codeblue

- Webmin GUI:
  - Username: cbadmin
  - Password: CodeBlue92

- Proxmox PVE (ToolVox XS only):
  - Username: cbadmin
  - Password: CodeBlue92

Ports

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_PJSIP Port 5060/UDP, standard port for SIP signaling

chan_PJSIP Port 5061/UDP, alternate SIP port

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

Blue Alert Monitor Pro

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

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

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 3000/TCP, Monitor Pro Web UI

ToolVox XS

For ToolVox XS (Physical Version) ToolVox resides on Proxmox Virtual Environment. Proxmox Virtual Environment is a complete open-source platform for enterprise virtualization. With the built-in web interface, you can easily manage VMs and containers, software-defined storage and networking, high-availability clustering, and multiple out-of-the-box tools using a single solution.

Within Proxmox (default IP: 192.168.0.10:8006) you can console into ToolVox, create backups, clones, snapshots and more. A default user with the following credentials has been pre-created.

Username: cbadmin

Password: codeblue

For more information on the functionality and capability of Proxmox Virtual Environment visit https://www.proxmox.com/en/proxmox-virtual-environment/overview or contact Technicalsupport@codeblue.com

ToolVox XS/XV Network Configuration

Users should utilize Webmin to adjust network settings for Blue Alert Connect and Blue Alert Monitor Pro.

To access the Webmin GUI for the first time, users need a workstation or laptop configured with an IP address within the 192.168.0.0/24 subnet (excluding the system IP). No gateway is necessary but can be set to 192.168.0.1.

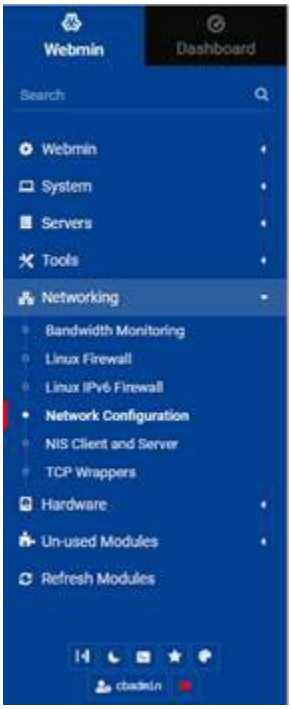
Set Static IP through Webmin GUI

Browse to the IP address of Blue Alert Monitor via port 10000 in any browser. The default IP address is https://192.168.0.11:10000. Log into Webmin interface, default credentials:

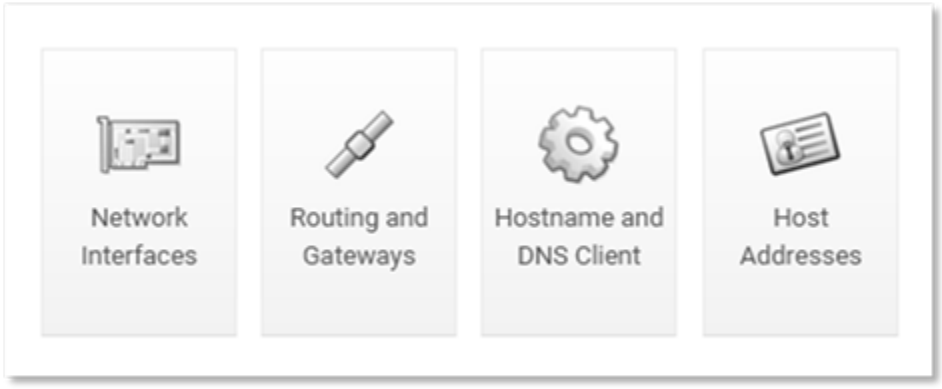
Username: cbadmin

Password: CodeBlue92

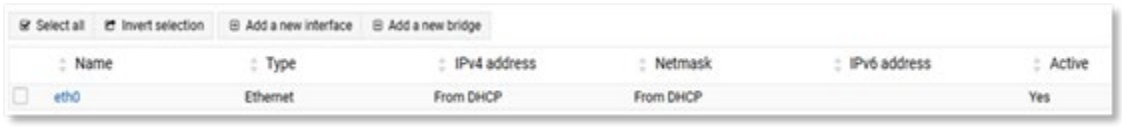
On the left-hand side browse to Networking>Network Configuration.



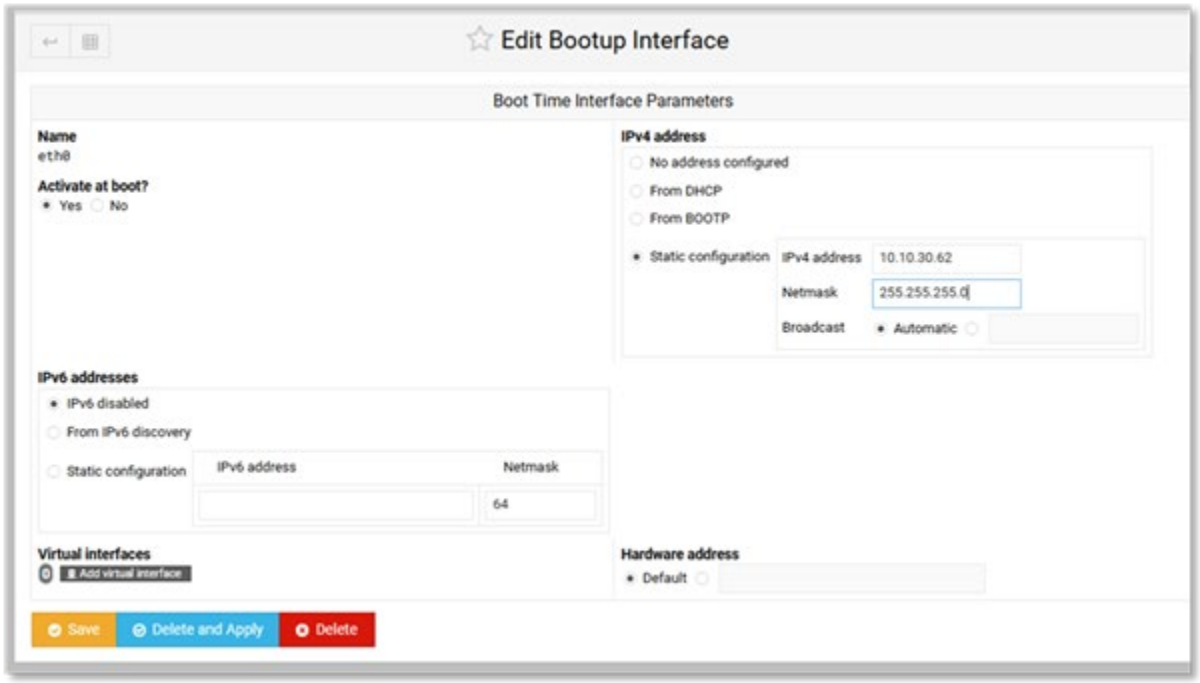
Select ‘Network Interfaces from the central menu.



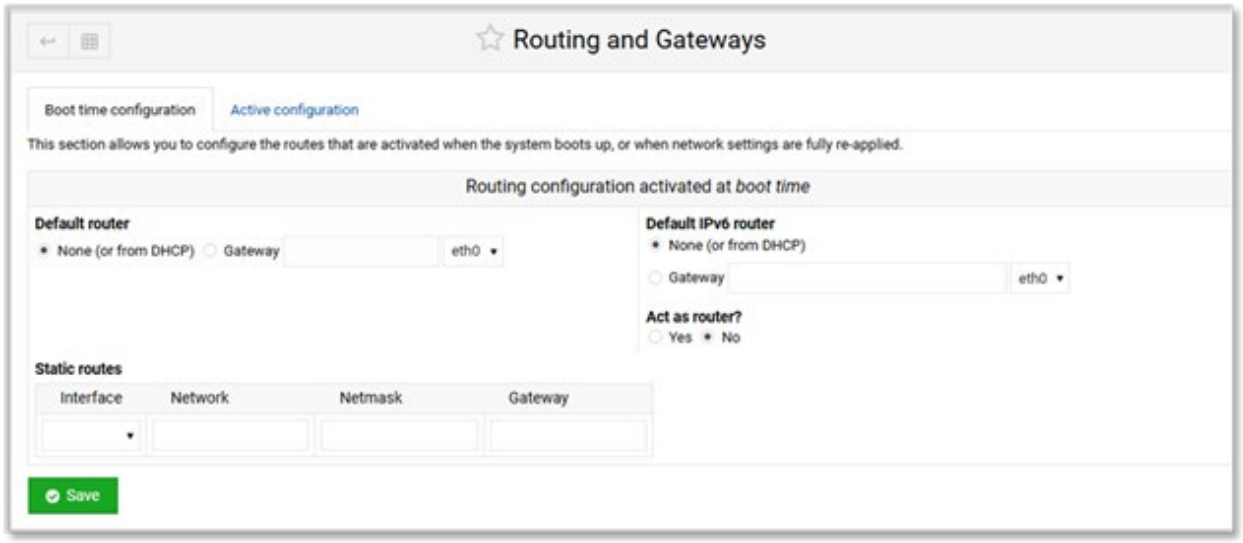
Click the name of the network port (eth0). The box does NOT need to be checked.



Here the static network information can be entered. Once complete click ‘Save’ to return to the previous screen.



To set the Gateway return to the Network Configuration menu and select ‘Routing and Gateways’.



Here the Gateway and static routing can be entered. Once complete click ‘Save’ to return to the previous screen.

Once all network information has been entered return to the Network Configuration page and click ‘Apply Configuration’.

Warning - this may make your system inaccessible via the network and cut off access to Webmin as network information will be changed.

Blue Alert Connect

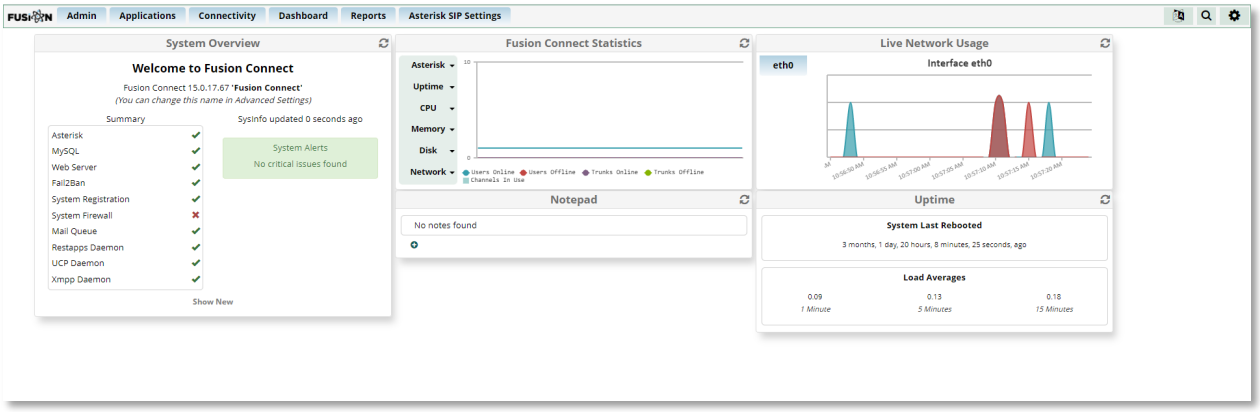
Dashboard

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.



Admin Modules

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

Username: cbadmin

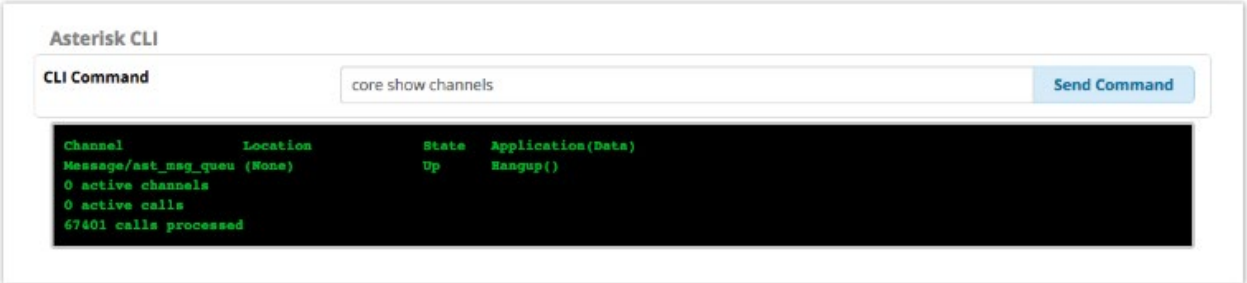
Password: codeblue

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

Asterisk CLI

The Asterisk CLI Module allows users to pass Asterisk CLI commands from the web interface and shows the resulting output.

- Enter the desired Asterisk CLI command into the text box.
- Press Send Command.



Backup and Restore

Backup Job Creation

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

Provide a name and description for the backup

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 you desire.

> 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.

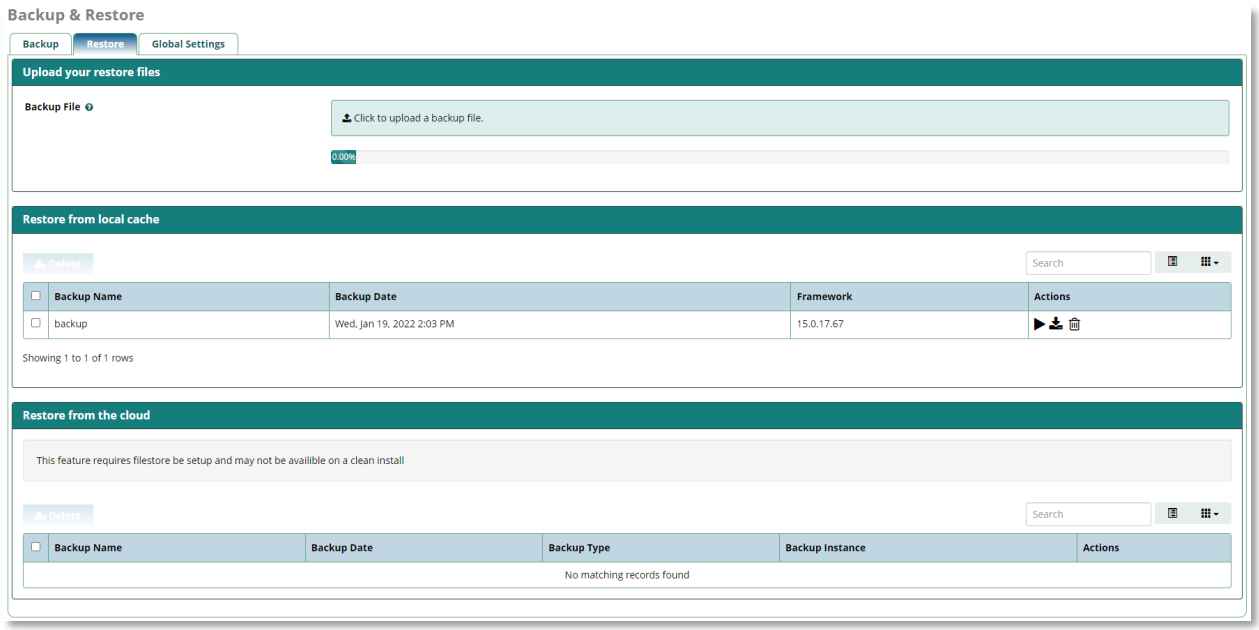
If you choose to run the backup manually, click on the 'play' button found under the 'Actions' settings of the Backup tab.

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.



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

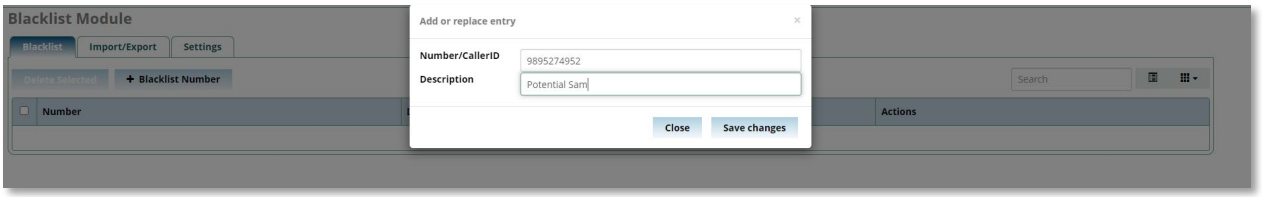
Here you will see the description of the backup job to be run including the modules backed up and decide to run the restore or go back to the restore page.

Blacklist

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 routed to a disconnect recording.

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.



Once complete click the Save Changes button. You will receive confirmation that the number was added.

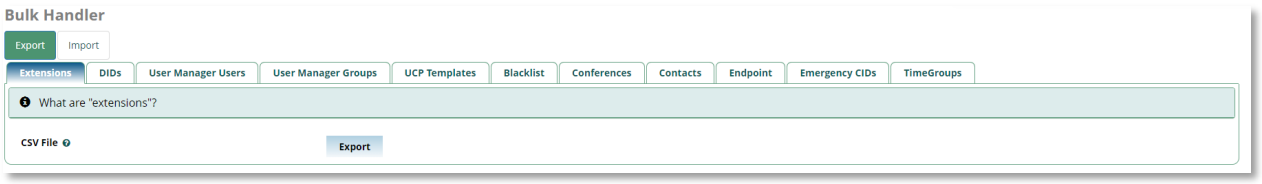
Bulk Handler

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, 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

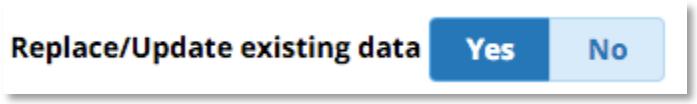
	A	B	C	D	E
1	Extension	Name	Description	Tech	Secret
2	1010	Stairway 1st Floor	Near Entrance	sip	cbUnit
3	1011	Stairway 2nd Floor		sip	cbUnit
4	1012	Stairway 3rd Floor		sip	cbUnit
5	1013	Stairway 4th Floor		sip	cbUnit
6	1014	Stairway 5th Floor		sip	cbUnit
7	1015	Stairway 6th Floor	Roof-top Parking	sip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



The contents of your CSV file will be displayed on 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 upload.

Certificate Manager

The Certificate Management module is used to manage certificates on the Blue Alert Connect

New Certificate

To add a new certificate, click this button and select from one of the three options:

Generate Let's Encrypt Certificate

Let's Encrypt Certificates are completely 100% free TLS certificates that are generated via an automated process designed to eliminate the current complex process of manual creation, validation, signing, installation, and renewal of certificates for secure websites. The Blue Alert Connect implements this same automated process.

Let's Encrypt certificate creation and validation requires unrestricted inbound http access on port 80 to the Let's Encrypt token directories. If security is managed by the PBX Firewall module, this process should be automatic. Alternate security methods and external firewalls will require manual configuration.

Upload Certificate

To upload a local, you will need to provide the following information:

- **Name:** Certificate Name. Usually the hast name
- **Description:** Certificate description
- **Passphrase:** The Passphrase of the Private Key. This will be used to decrypt the private key and the certificate. They will be stored unpassworded on the system to prevent service disruptions.
- **CSR Reference:** Certificate Signing Request to reference. If 'None' is selected, then you will be able to upload your own private key
- **Private Key:** Paste your private key here
- **Certificate:** Paste your certificate here
- **Trusted Chain:** Paste your trusted chain here

Once done click “Upload Certificate”.

Generate Self-Signed Certificate

The Blue Alert Connect generates a self-signed certificate on first boot.

To add a new Self-Signed Certificate, you will need to provide the following information:

- **Host Name:** The hostname of the system. Should be a fully qualified domain name
- **Description:** Description of this certificate
- **Organization Name:** Organization name, Used in the Certificate Authority generation process

Once all information is entered click on “Generate Certificate

Change Certificate Validity Period

You can change the value of the validity period.

Go to the Advanced Settings menu and Certificate Manager part and enter a new value (in days).

Delete Self-Signed CA

You can delete the self-signed certificate authority at any time by clicking the red button labeled "Delete Self-Signed CA".

A prompt will then come up warning you that all certificates that relied on this self-signed certificate authority will be invalidated

Once you have deleted the self-signed CA you can then generate another one by clicking "New Certificate" then "Generate Self-Signed Certificate"

Import Locally

To manually import your certificates, you need to drop the *.key and *.crt files into /etc/asterisk/keys. Then click the Import Locally button.

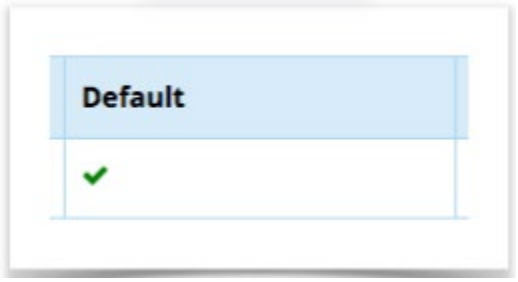
When this has finished your certificates will show up in the list of PBX certificates.

Setting a Default Certificate

Making a certificate the 'default' changes certificate settings in Advanced Settings ONLY. It will force said certificate to be the default for options in Advanced Settings that require certificates. It will also place a standard set of the certificate and its key into /etc/asterisk/keys/integration for use by other applications

To select a certificate as the default, move your mouse over the blank/empty column in the list of certificates. A grey checkmark will appear. Click that checkmark to make it the default

After checking the box, the checkmark will turn from grey to green after you move your mouse away.



Config Edit

Configuration file editor gives you the ability to edit custom Blue Alert Connect files in the browser that you would normally have to edit through the CLI.

It is not recommended to make changes to any files unless you know what you are doing.

To create or edit a file:

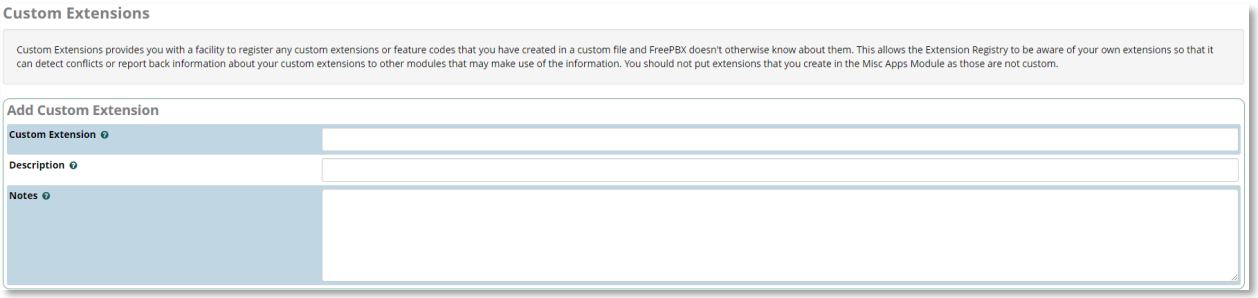
- Edit the file in the text field.
- Click the **Save** button to save your changes.
- Click the **Apply Config** button to apply the changes.

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:

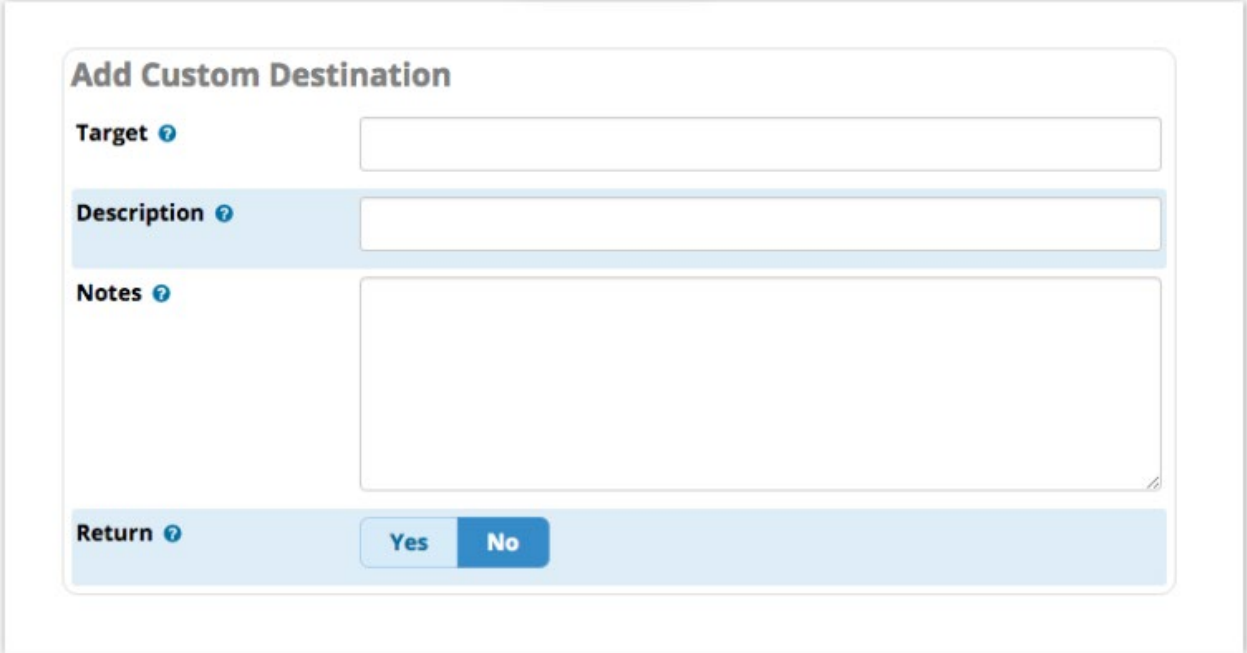


- Custom Extension: Define the custom extension number that you want the PBX to be aware of. You will not be allowed to use the number for something else.
- Description: Give this custom extension a friendly name.
- Notes: Here you can enter notes on what this custom extension is used for.

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.

Custom Destinations

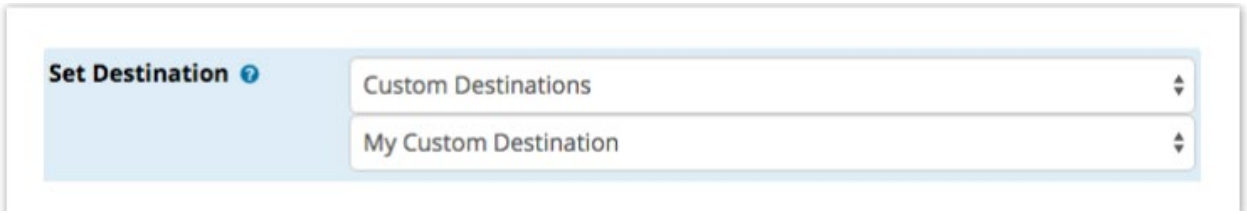
The Custom Destinations module allows you to register or publish destinations to custom dialplans, inbound routes, announcements, IVRs and others.



For each custom dial plan destination, you can define the following:

- Target: This is your custom destination. Define the custom dial plan that you want to route the caller to in the format [context],[exten],[priority]. Example: “afterhours-pin,501599,1,” which is the start of the custom “After Hours Pin” dialplan we have on this box.
- Description: Give this custom destination a friendly name.
- Notes: Here you can define notes on what this custom dialplan or script is used for.
- Return: Does your custom destination end with 'Return'? If so, you can then select a custom destination after this call flow is complete.
    - If you select Return: Yes, then you will see a new dropdown menu where you can select the appropriate return destination.

Once a Custom Destination is created modules that support destinations can utilize the custom Destination.



Module Admin

The Module Admin module allows you to enable, disable, update, and install modules. This does not include Asterisk or the underlying OS.

Checking for Available Upgrades

Click the Check Online button to check for available updates.

Once the results are in, you can check the Show only upgradeable box. This will hide all modules that don't have upgrades available.

Toward the right side of the screen, you will see a set of buttons: Download all, Upgrade all, Reset, and Process.

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

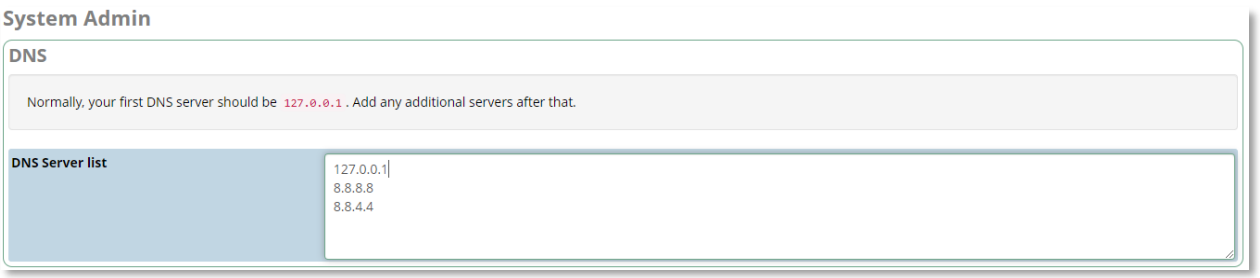
For the Physical Version of Blue Alert Connect the system will arrive pre-activated by Code Blue before being shipped.

For Virtual instances Blue Alert Connect will generate a UUID upon installation 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.

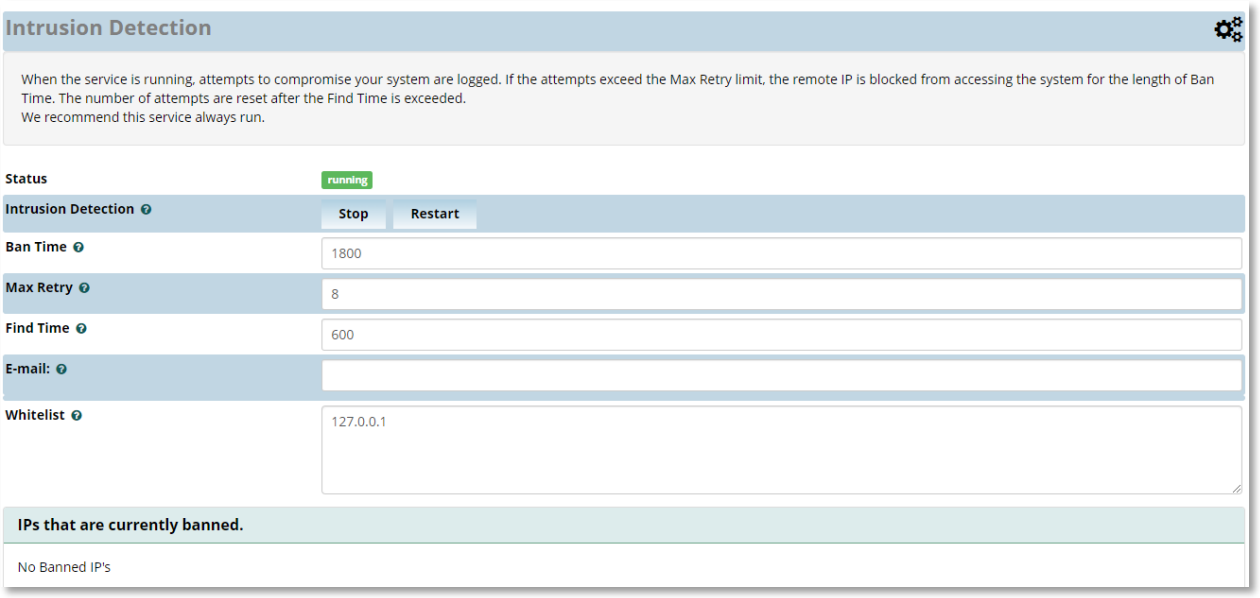
Enter the DNS Servers, one per line. Normally, your first DNS server should be 127.0.0.1. Add any additional servers after that.



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 is reset after the Find Time is exceeded. We recommend this service to always run.



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

It is NOT recommended to make network changes through System Admin; This may cause issues with Blue Alert Monitor and the Debian OS. To make Network Configuration changes please utilize Webmin or the OS CLI as outlined earlier in this guide.

Hostname

It is NOT recommended to change the Hostname through System Admin. This may cause issues with Blue Alert Monitor and the Debian OS. To make Hostname changes please utilize Webmin or the OS CLI as outlined earlier in this guide.

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.

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

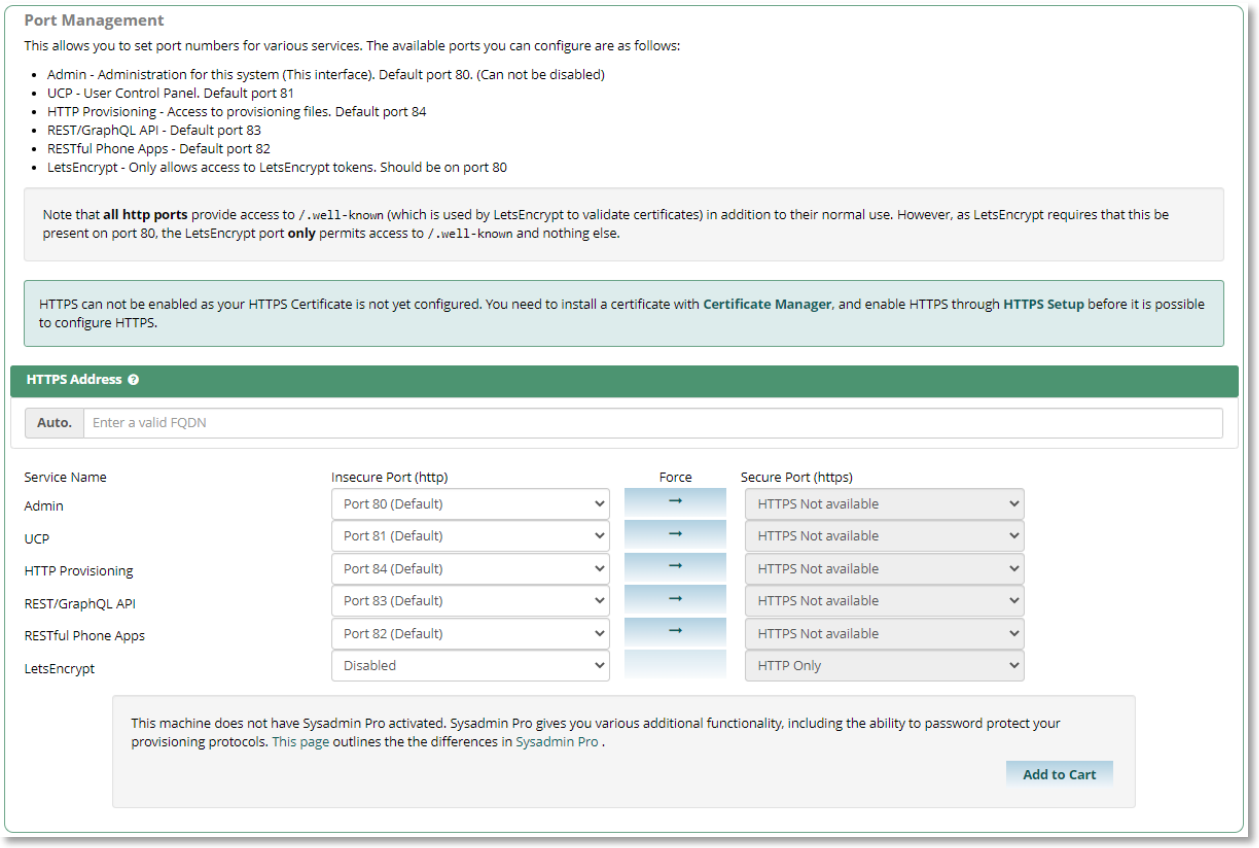
The Power Options page allows you to power down or reboot your server.

Power 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.



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.

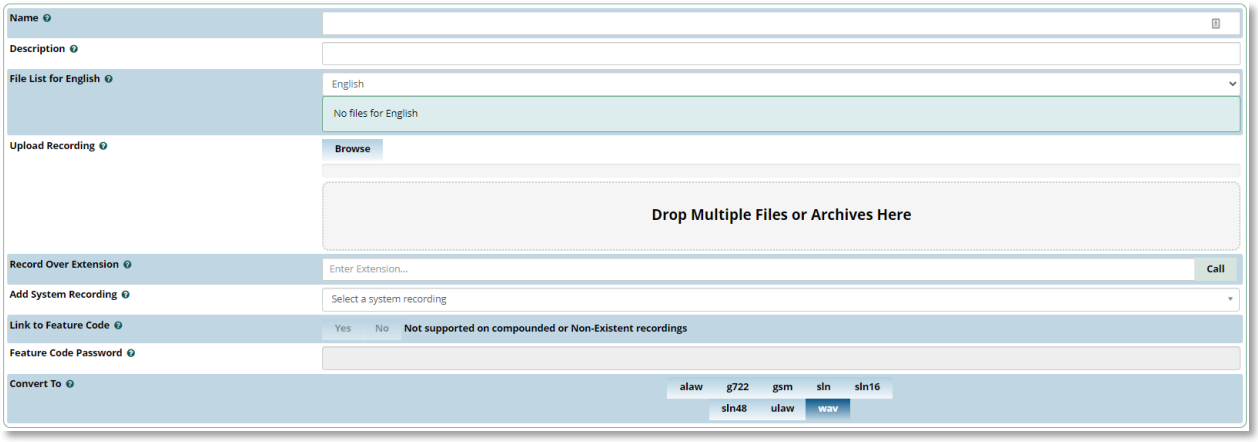
Port	Default Port #	Function
Admin	80	Web port controlling the system
UCP	81	User Control Panel
HTTP Provisioning	84	Access to provisioning files
REST/GraphQL API	83	Access to RESTful API and GraphQL API
RESTful Phone Apps	82	Access to RESTful Phone Apps
LetsEncrypt	80	Only provides access to LetsEncrypt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

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: 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 hanging up, you will be able to name the file, and it will be placed on 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.

Updates

The Updates section of the System Admin module allows you to update your Blue Alert Connect manually or schedule automatic updates. This update method is a user-friendly alternative to updating your system via the CLI commands.

By default, updates are scheduled to run every Saturday between 1am and 4am.

User Management

The User Management module controls and manages users and administrators for the Blue Alert Connect.

Users: The first view you will see when going to the User Management module is the listing of all of your users on the system.

Adding a User

- **Login Name:** This is the login username that the user will use to log into the Admin GUI
- **Description:** A friendly name or brief description for this user.
- **Password:** Password for the user.
- **Groups:** A list of groups the user belongs to, if any. To select a group, begin typing the group name into the field, and when the system finds it, click on the name. You can add multiple groups. An Admin Group of “Code Blue admin” has been pre-built. Most users will be added to this group and inherit its settings.

User Details

All of the fields in this tab are optional. This information is stored for use in other apps. Most fields are self-explanatory

Deleting a User

To delete a user simply click the trash can icon next to the user.

Groups: User Manager groups can be used to control permissions for the Administration Panel

An Admin Group of “Code Blue admin” has been pre-built. Most users will be added to this group and inherit its settings.

User Management Directories

Am internal directory for “Code Blue Admin” users has already been created and is associated with the “Code Blue Admin Group”

It is possible to add an external directory including:

- Microsoft Active Directory
- (Legacy) Microsoft Active Directory
- OpenLDAP

Applications Modules

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

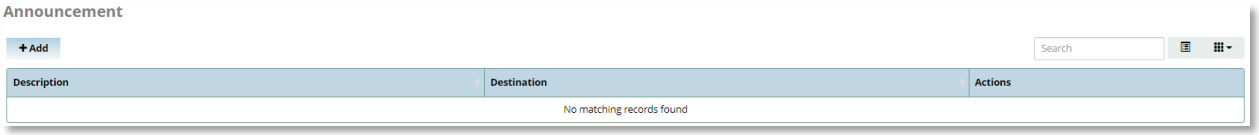
Username: cbadmin

Password: codeblue

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

Announcements

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.



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

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.

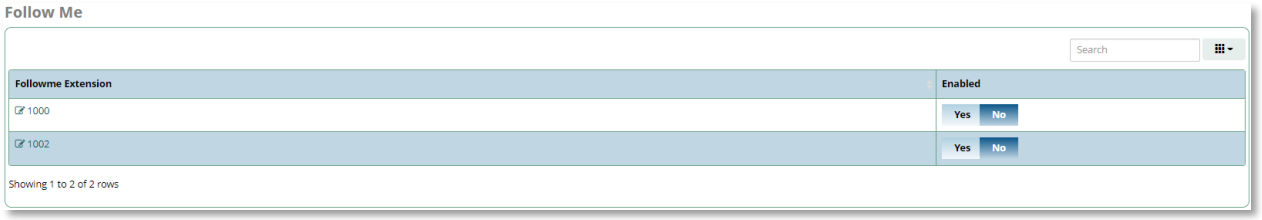
Don't Answer Channel: The recommended setting is No, which means the behavior is to answer the call and play this message. This feature is rarely supported by phone carriers.

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.

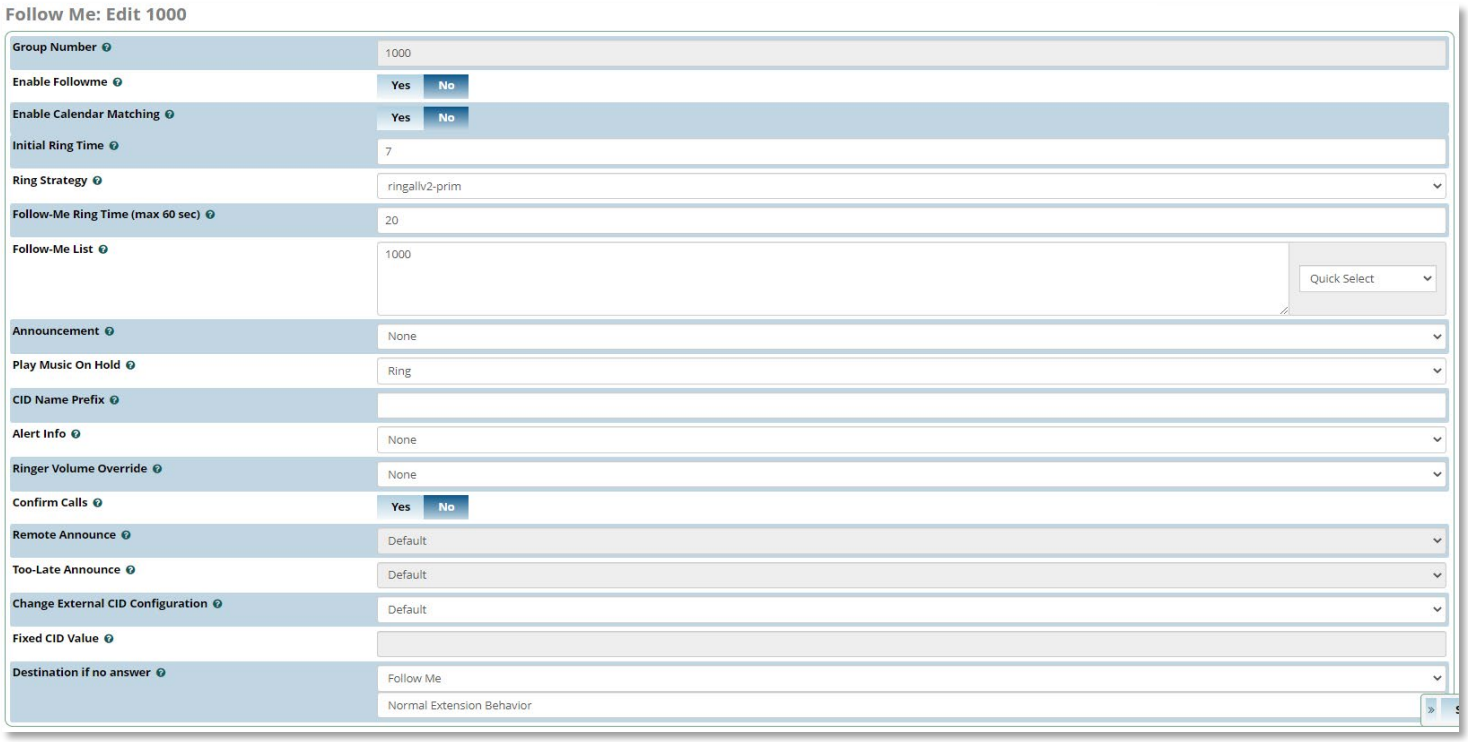
Follow Me

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.



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.



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 will not 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(which 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 - e.g., 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.

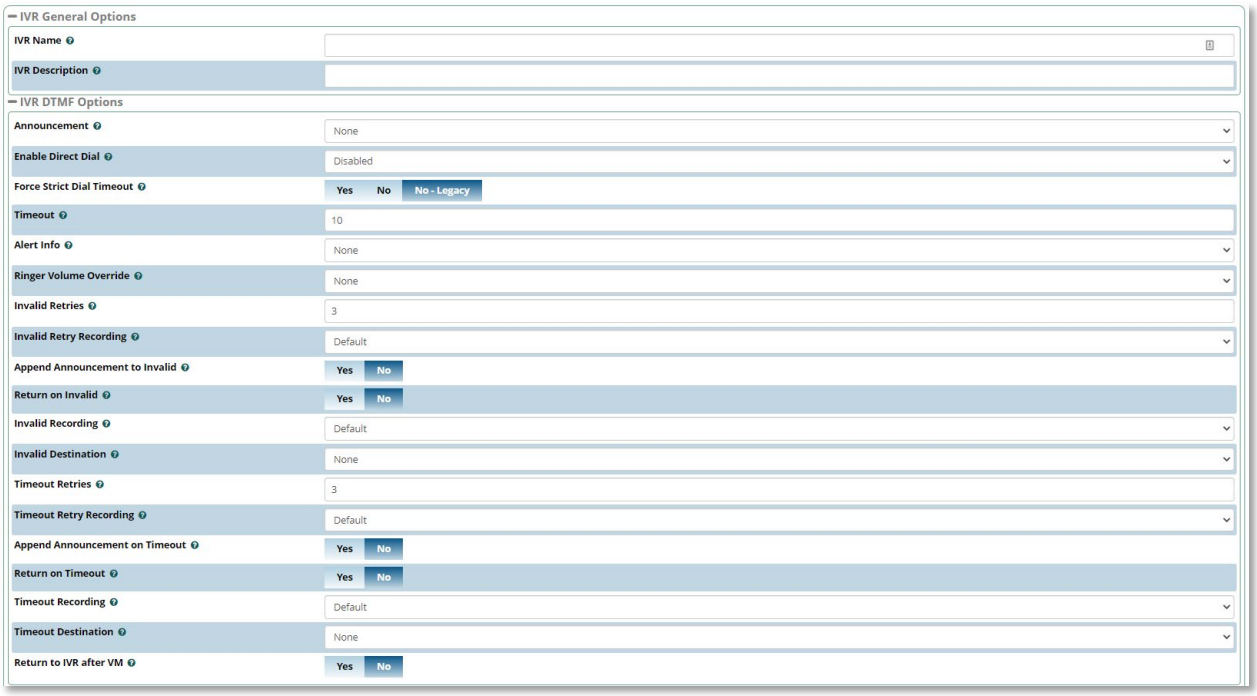
IVR

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 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: 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 number 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: 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

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: 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

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: 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

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: 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.

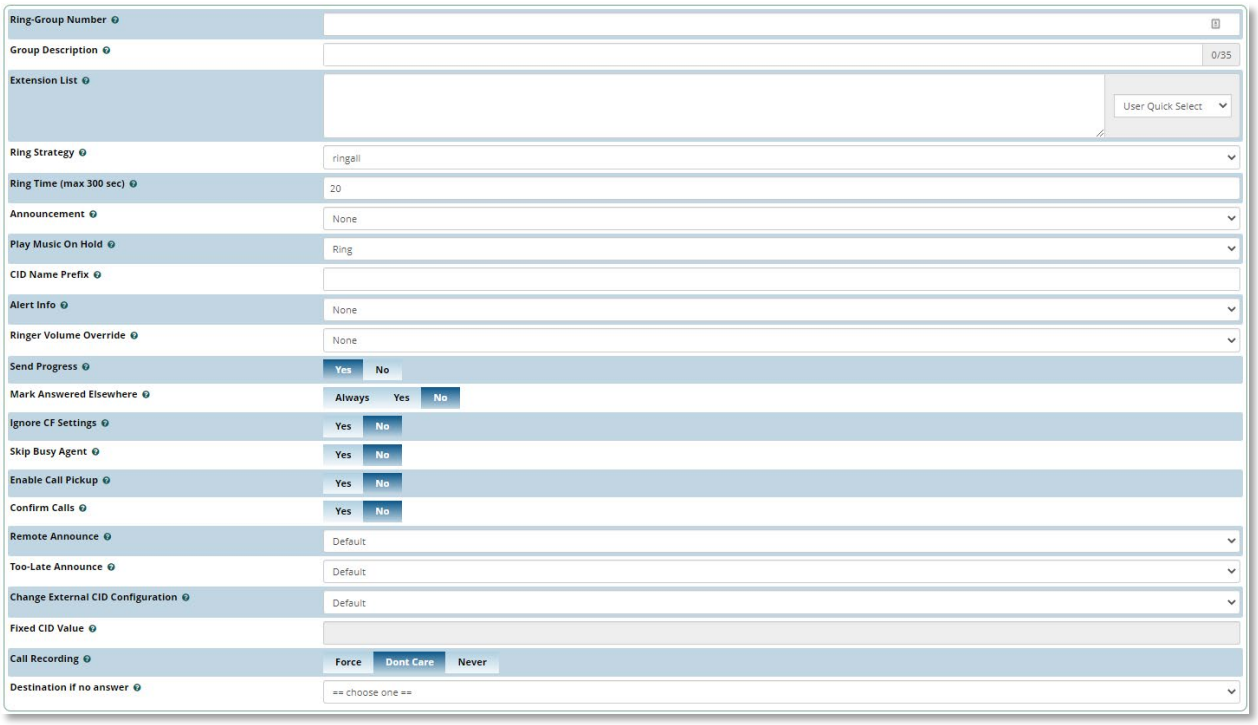
When finished building the paging group, click the Submit button and then click the Apply Config button.

Ring Groups

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: 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 will not 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.

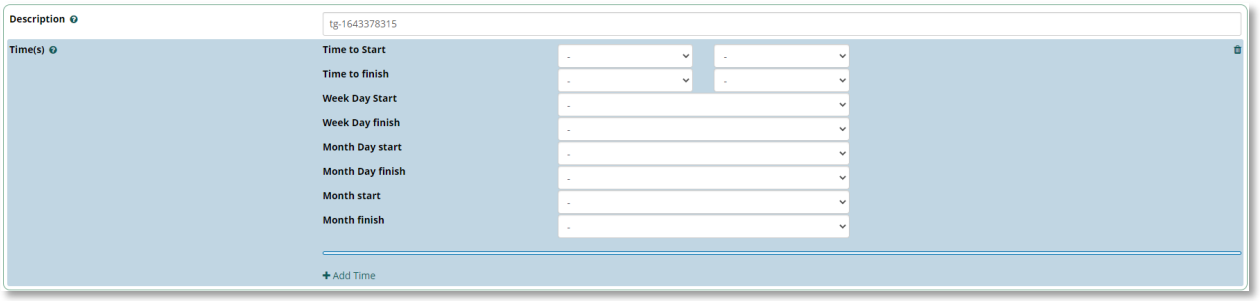
When finished click the Submit button, then click the Apply Config button.

Time Groups

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: 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
- Weekday start
- Weekday finish
- Month Day start
- Month Day finish
- Month start
- Month finish

Unset (blank) weekday, 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.

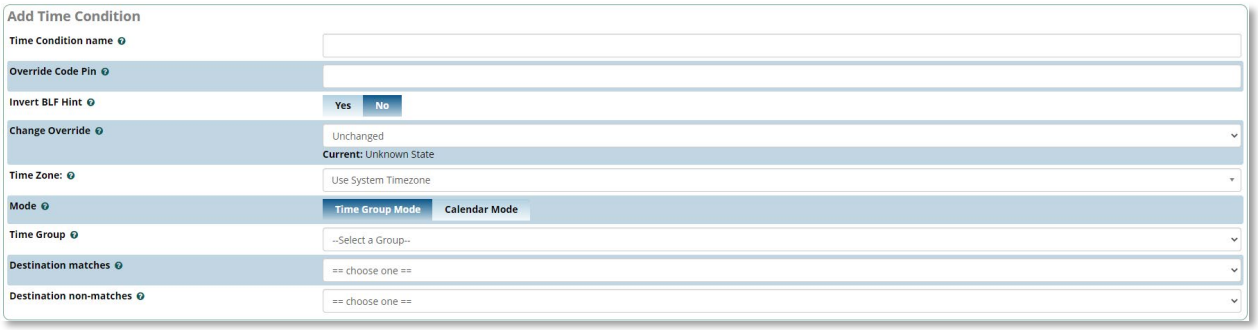
After you create a time group, it will become available for selection in the Time Conditions module.

Time Conditions

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



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

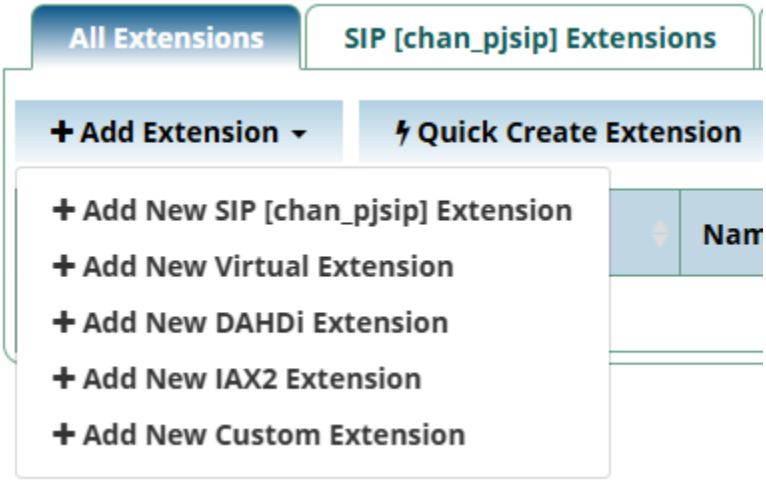
On the top menu hover your mouse over ‘Connectivity’ to see the available modules.

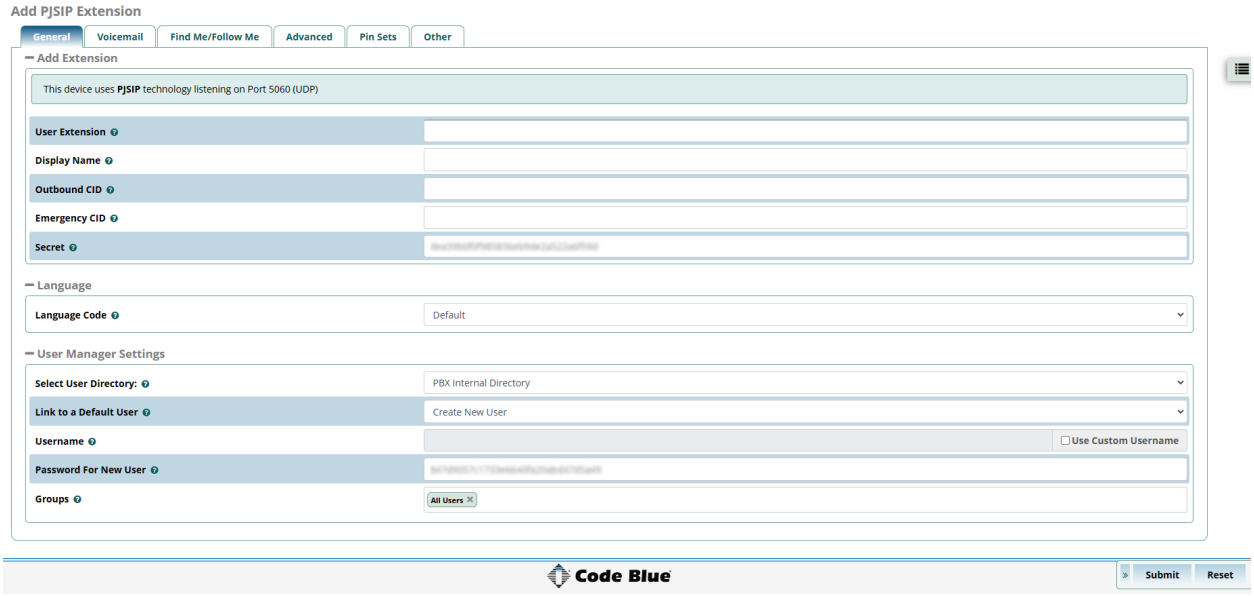
Extensions

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 SIP [chan_pjsip] Extension. This will also be the choice for the majority of Third-party Phones.





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 an Emergency. The Emergency CID overrides all other CallerID settings.

Secret: Password (secret) configured for the device. It 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

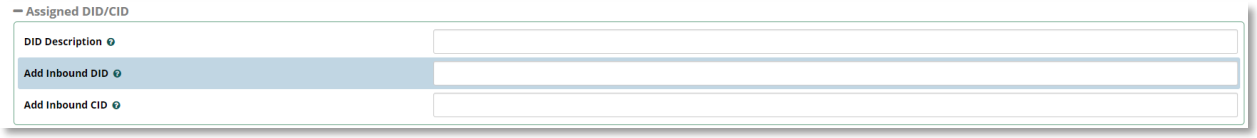
Having voicemail enabled will cause issues with Code Blue devices. It is recommended to leave this feature off.

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



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: 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.

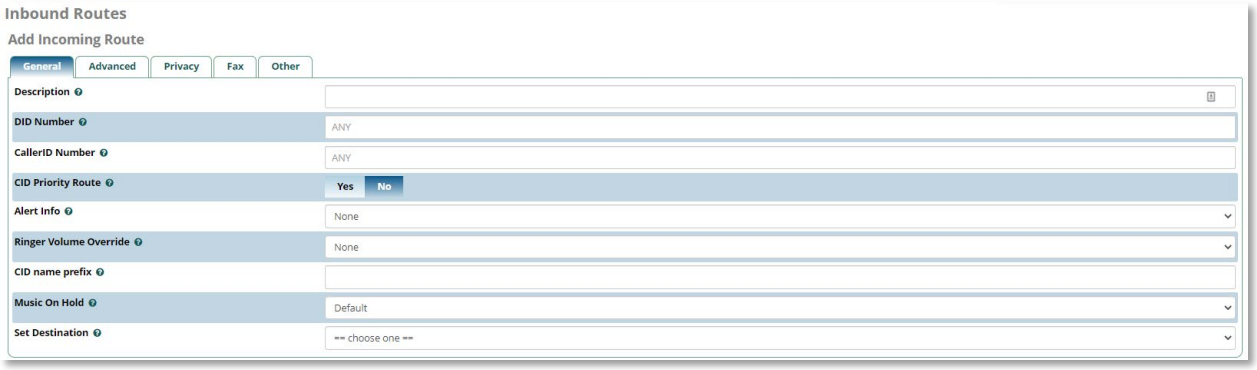
Inbound Routes

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



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 their 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.

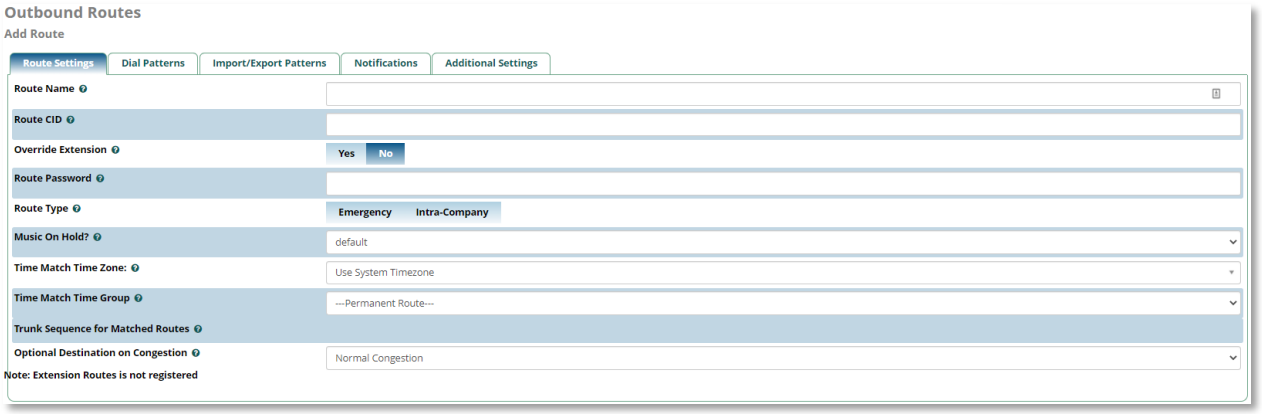
Outbound Routes

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 on a particular route.

Adding an Outbound Route

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

Route Settings Tab



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

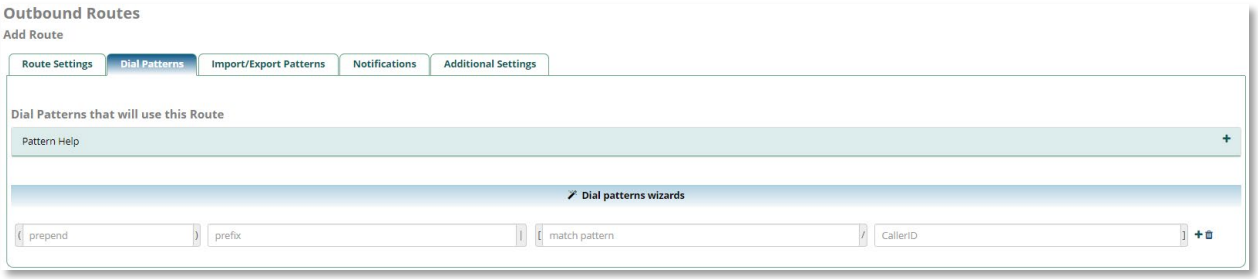
Route CID: Optional route Caller ID to be used for this route. If set, this will override all specified CIDs unless Trunk CID is set to force override or Override Extension option is set to no.

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



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 like 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.

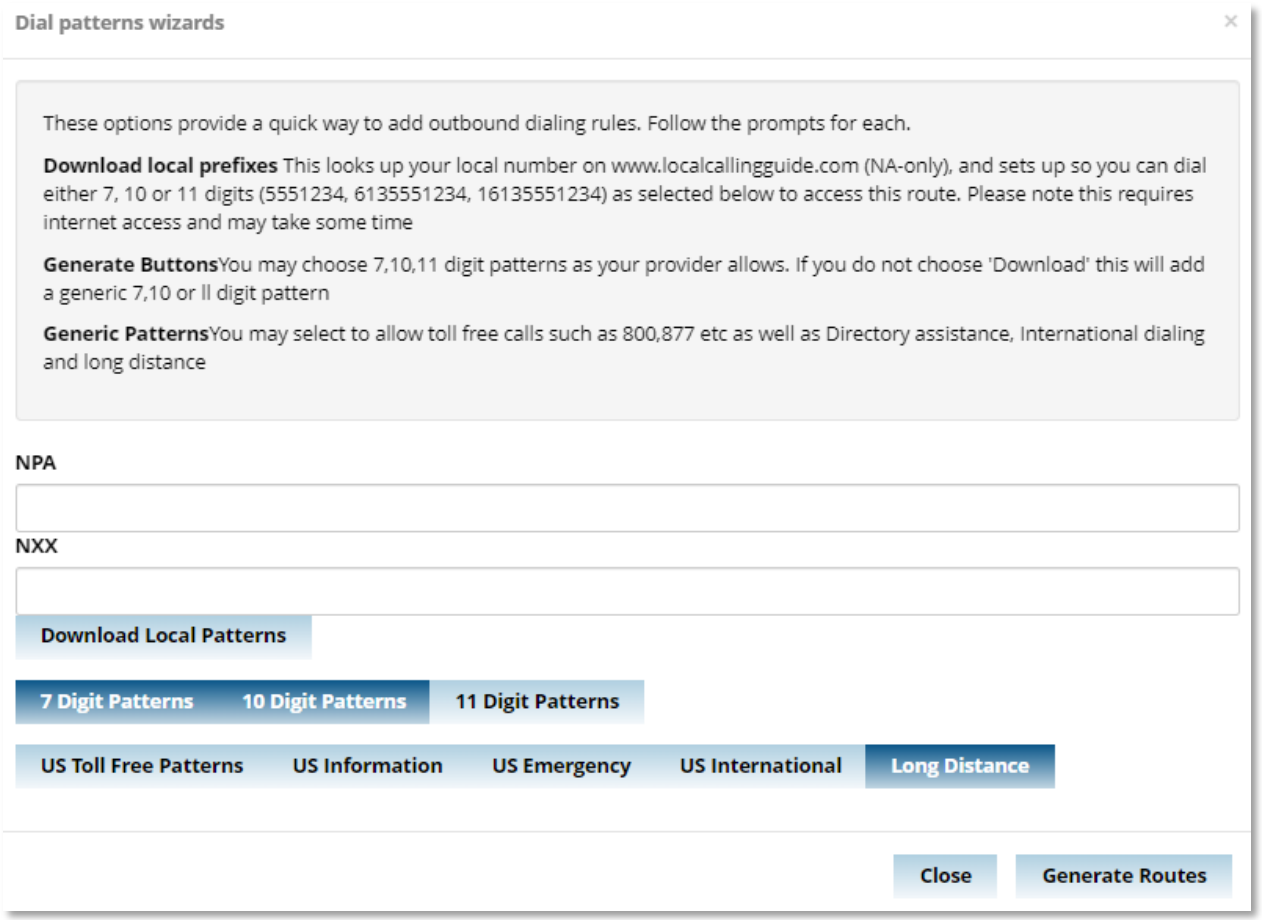
Prefix: Prefix to remove upon a successful match. The dialed number is compared to this and the subsequent columns for a match (prefix + match pattern). Upon a match, this prefix is removed (stripped) from the dialed number before sending the sequence to the trunks.

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.



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.

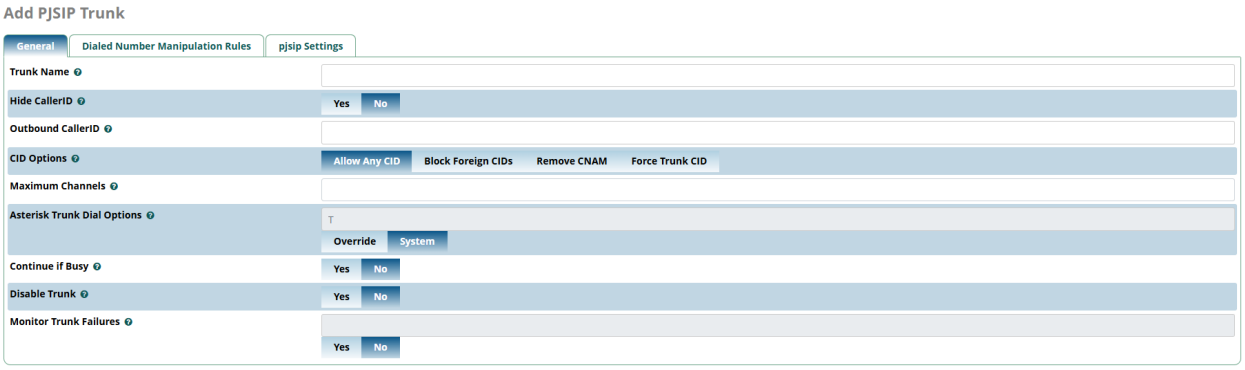
Trunks

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 PBXs. 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 PJSIP (chan_pjsip) Trunks (first choice in the drop-down menu). For other types of Trunks please contact technicalsupport@codeblue.com for assistance.

General Tab



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.

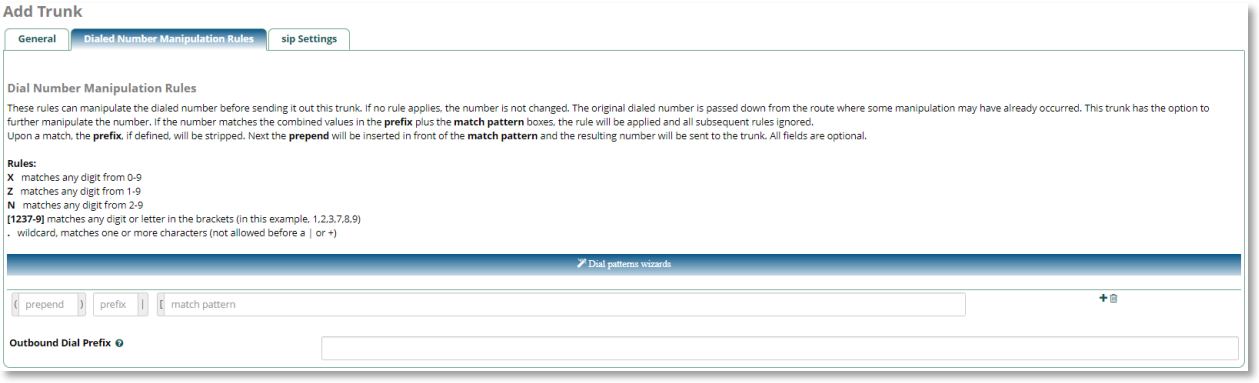
Maximum Channels: Controls the maximum number of outbound channels (simultaneous calls) that can be used on this trunk.

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



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.

PATTERN	DESCRIPTION
	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 like 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.

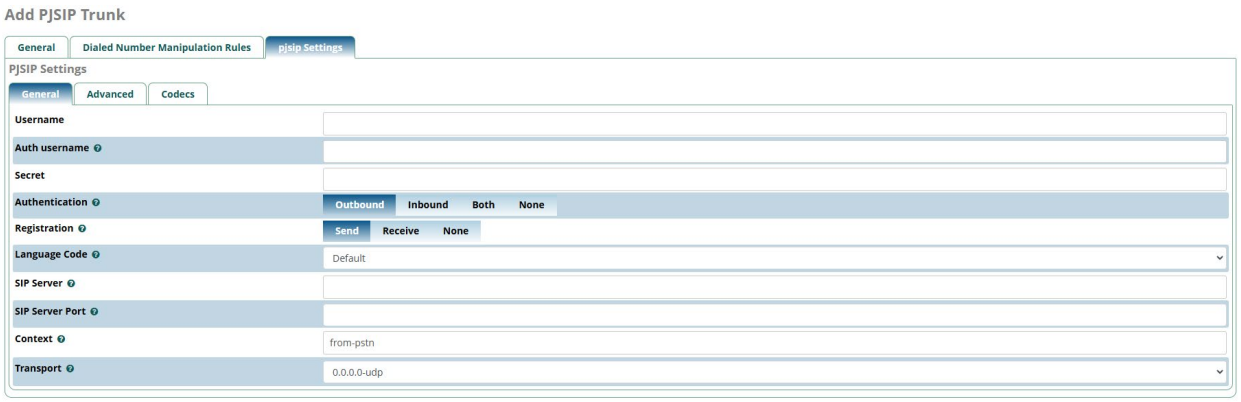
Match Pattern: The dialed number will be compared against the prefix + this match pattern. Upon a match, this portion of the number will be sent to the trunks after removing the prefix and appending the prepend digits.

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.

PJSIP Settings Tab

General



Username: SIP Username

Auth Username: Can be left blank unless the auth username is different than the username

Secret: SIP Authentication Password; Can be left blank if the Auth Username is the same as the Username

Authentication: Usually, this will be set to 'Outbound', which sends the Auth credentials from the Blue Alert Connect and allows unauthenticated calls in from the other server. If you select 'None', all calls from or to the specified SIP Server are unauthenticated. Setting this to 'None' will blank out the above fields and is only suggested if you are in control of both SIP Servers.

Registration: You normally Send registration, which tells the remote server where to send your calls. If the other server is not on a fixed address, it will need to register to this server (Receive), so this server can send calls to it. You would select None if both machines have a fixed address and do not require registration.

Warning: If you select 'None', registration attempts for the Username and Secret specified above will be rejected.

SIP Server: IP address or URL of the SIP server or service

SIP Server Port: SIP server port (default: 5060) This is ignored if the Registration is set to Receive

Context: Set the context of how to receive inbound calls; Typically set to 'from-pstn' (treat incoming calls as an outside call) or 'from-internal' (treat incoming call as an internal call)

Transport: Select the transport type (must be available in global settings to appear in list)

Advanced

Unless specified by the SIP server you are establishing a trunk with these settings are typically left at default.

Codecs

The global default audio codecs will be preselected. Adjust as needed.

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

Asterisk Info

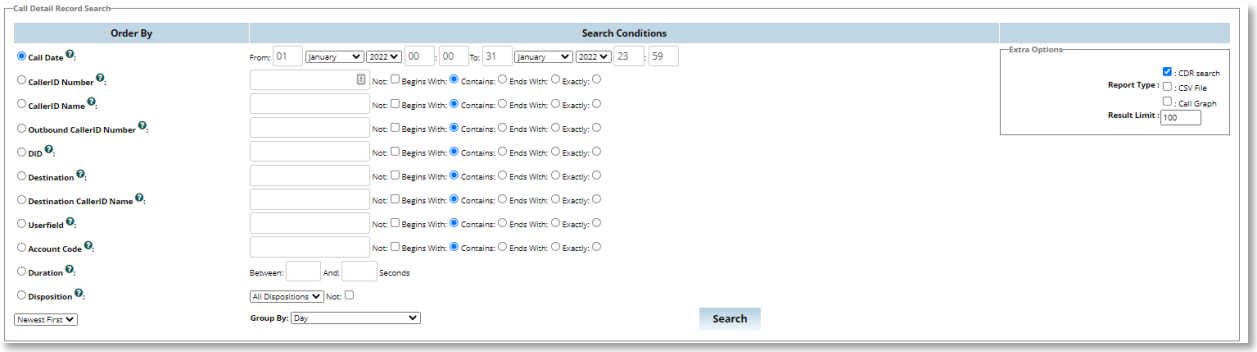
The Asterisk Info page gives you the ability to look at key things in Asterisk such as extension registration information and is typically used to troubleshoot issues.

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
```

CDR Reports

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



CDR Reports can be filtered by:

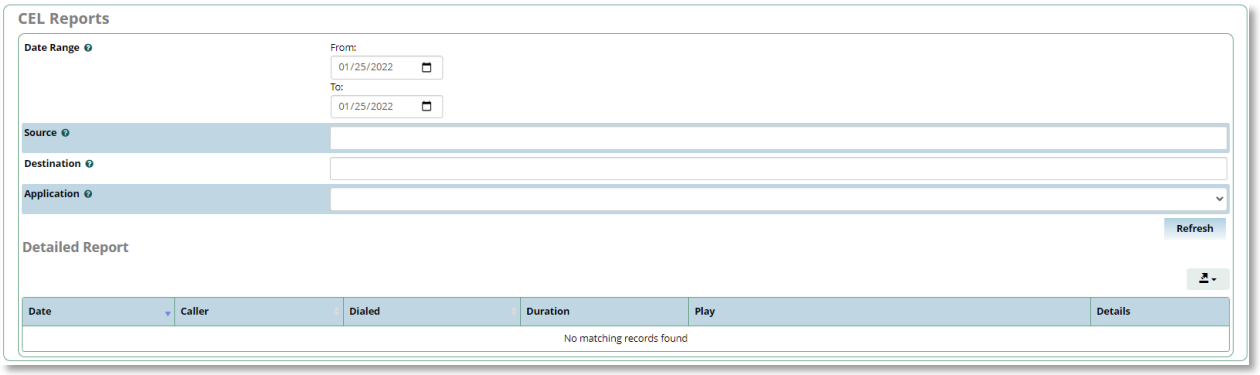
- Call Date
- CallerID Number
- CallerID Name
- Outbound CallerID Number
- DID
- Destination
- Destination CallerID Name

- Userfield
- Account Code
- Duration
- Disposition

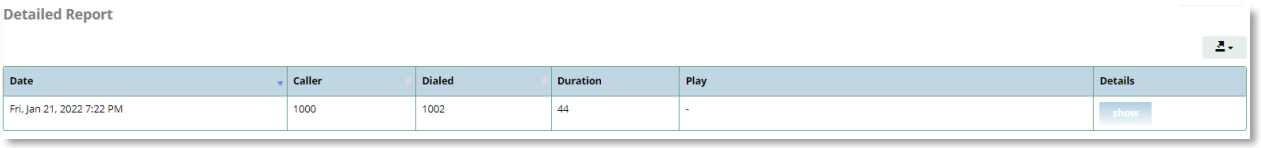
Once a filter has been selected and modified click the Search button at the bottom of the page. The CDR will then populate a table with any call information matching the filter and display all Call Detail Records.

Call Event Logging

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.



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.



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

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.

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

System Logfiles

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

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.

Advanced Settings

Some of these settings can render your system inoperable. It is recommended to not make changes to this page unless you know what you are doing.

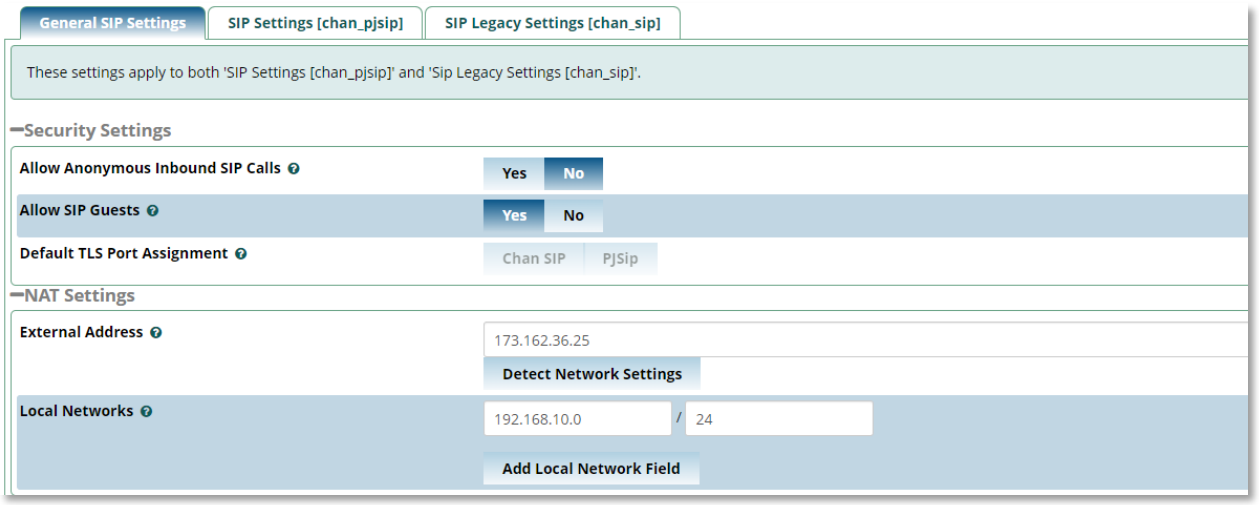
You are urged to backup before making any changes.

Read-only settings are usually more volatile, they can be changed by changing 'Override Read-only Settings' to Yes.

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. ***

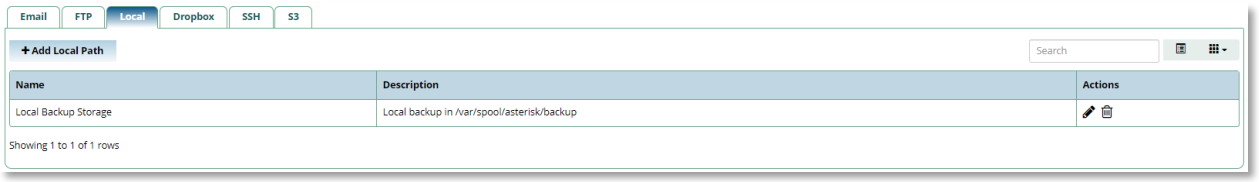


Filestore

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

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.



Blue Alert Monitor Pro

Blue Alert Monitor Pro is a comprehensive diagnostics application designed to ensure the reliability of Code Blue and third-party emergency stations through automated presence testing of both analog and SIP-based stations. The application monitors network-based stations by collecting SNMP traps and performing scheduled presence tests to verify system availability. When failures are detected, the system automatically generates detailed reports and sends email notifications to designated personnel, enabling rapid response to potential issues.

Requirements

Monitor Pro utilizes the Connect PBX for Presence Testing. An ARI user must be configured within the Connect PBX for full functionality. An ARI user has been created by default for this reason.

Logging into Blue Alert Monitor Pro

To access Blue Alert Monitor Pro web interface, browse to **http://<IP of ToolVox Server>:3000**

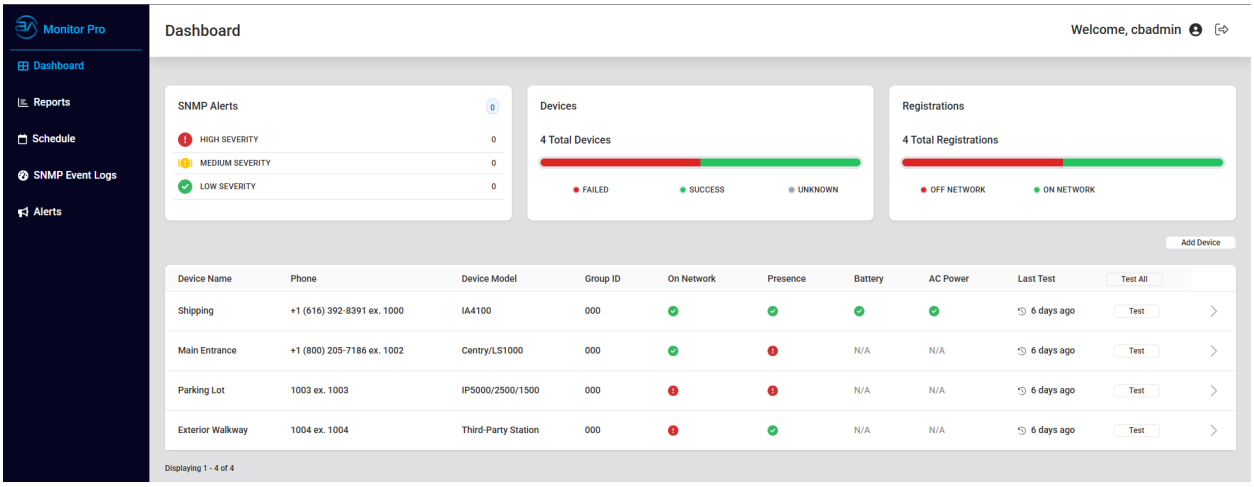
The default login is:

Username/Email: cbadmin@codeblue.com

Password: codeblue

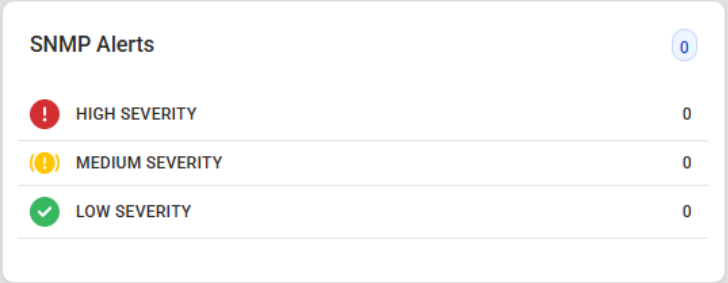
Dashboard

The Dashboard of Blue Alert Monitor Pro shows the current status of stations as well as the latest results of any performed presence test. Users can add new devices and manually initiate presence testing for individual stations or all stations simultaneously.



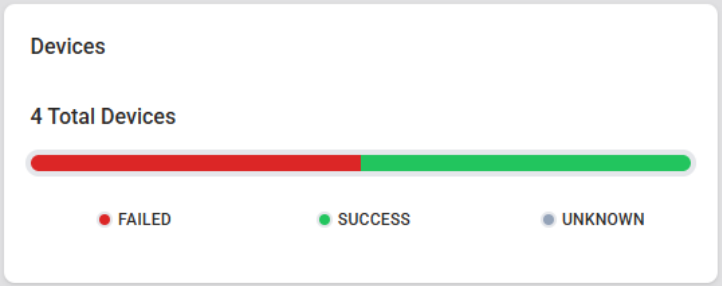
SNMP Alerts

SNMP Alerts table will show the number of current SNMP Traps received and their severity.



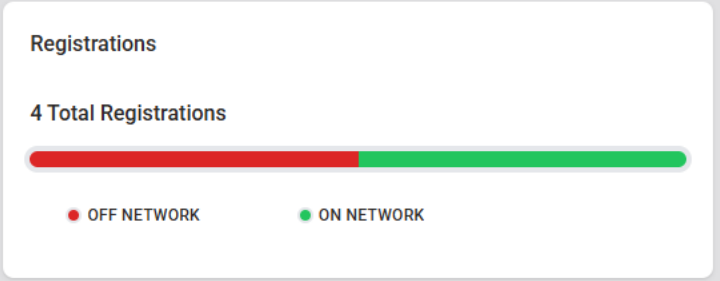
Devices

Devices table shows the status of the latest presence tests.



Registration

Registrations Table shows the current number of devices registered to the ToolVox.



Device Table

The Device table shows the detailed information of the individual stations, live On Network status (registration), the result of the last presence test, and the time since the last test.

Clicking on the row of an individual unit will provide more detailed information and allow for editing or removal of the device.

Presence Test Results

Presence testing verifies station availability by having the ToolVox PBX place a test call to each station and determine whether the call is answered successfully.

Monitor Pro reports four possible test outcomes

On Network	Presence	Battery	AC Power
✓	✓	✓	✓
✓	!	N/A	N/A
!	!	N/A	N/A
!	✓	N/A	N/A

Test Result Categories

On-Network with Successful Presence Test:

The station maintains proper registration with the system and successfully answered the incoming test call.

On-Network with Failed Presence Test:

The station shows good registration status but failed to answer the incoming test call. For analog devices connected through an ATA or FXS gateway, this indicates the gateway is communicating properly, but the connected analog phone is not responding.

Off-Network with Failed Presence Test:

The station shows no registration with the system and cannot answer incoming calls.

Off-Network with Successful Presence Test:

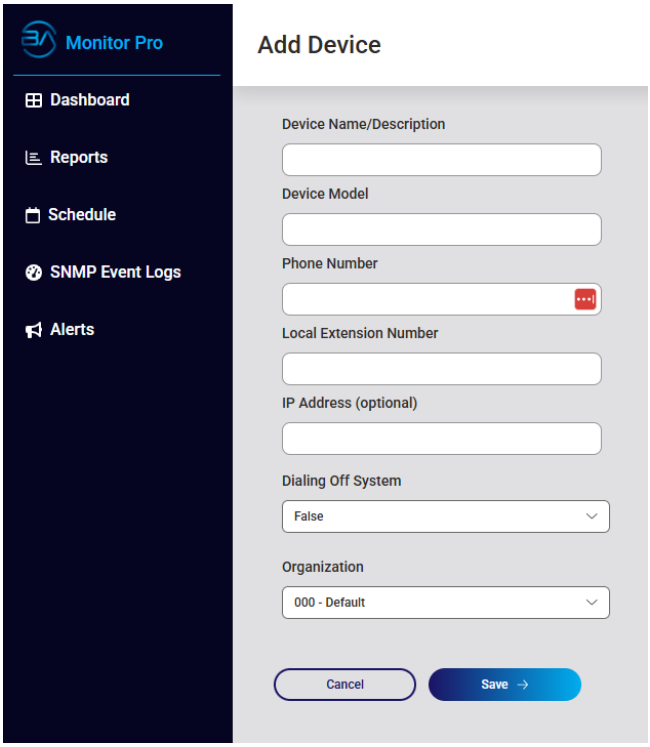
The station is not registered to the ToolVox system but successfully answered the test call. This typically occurs when the station is registered to a different PBX or service provider that can still provide dial tone functionality.

Additional Diagnostics:

The Code Blue IA4100 provides enhanced diagnostic capabilities, including monitoring of battery status, AC power status, and button fault detection.

Add Device

To add new stations to be monitored click the “Add Device” button .



Device Name/Description: This will appear on the Dashboard, configuration of scheduled events, as well as email notifications.

Device Model: Make/Model of station; This may alter how a presence test is performed.

Phone Number: If the device being monitored is an off-system unit (no registration to ToolVox) this is the number that will be tested during a presence test. This requires SIP trunk to dial off-system. If not dialing off system the local extension number can be entered here.

Local Extension Number: If the station being monitored is on-system (registered to the ToolVox) this is the number that will be tested during a presence test. If no local extension is being used the 'Phone Number' can be entered here.

IP Address: Required for receiving SNMP Traps from SIP based stations

Dialing Off System: By default, is set to False to dial the local extension for presence testing. If the 'Phone Number' needs to be tested set to True.

Organization: (Future release) Station can be added to separate organizations for viewing and filtering.

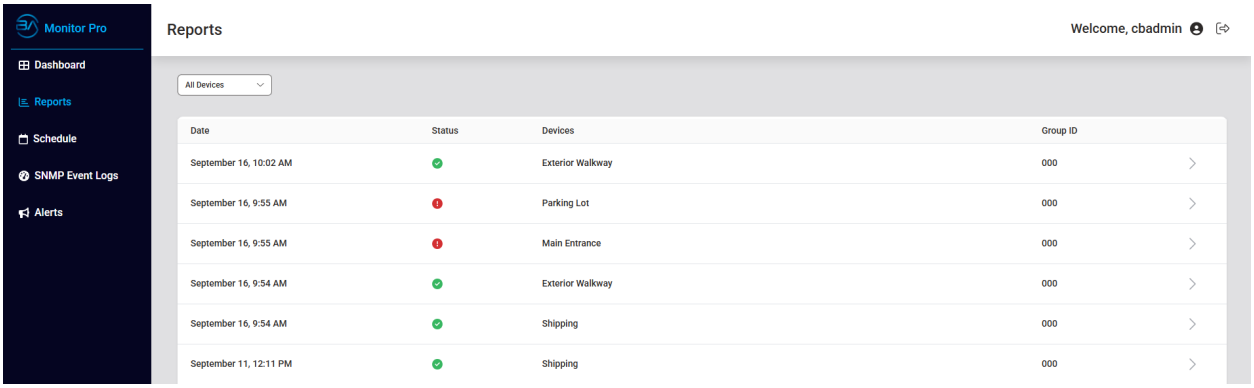
Manual Presence Test

On the right-hand side of the device table, you can click “Test” or Test All” this will initiate a presence test for the individual unit or all units in sequence.

Reports

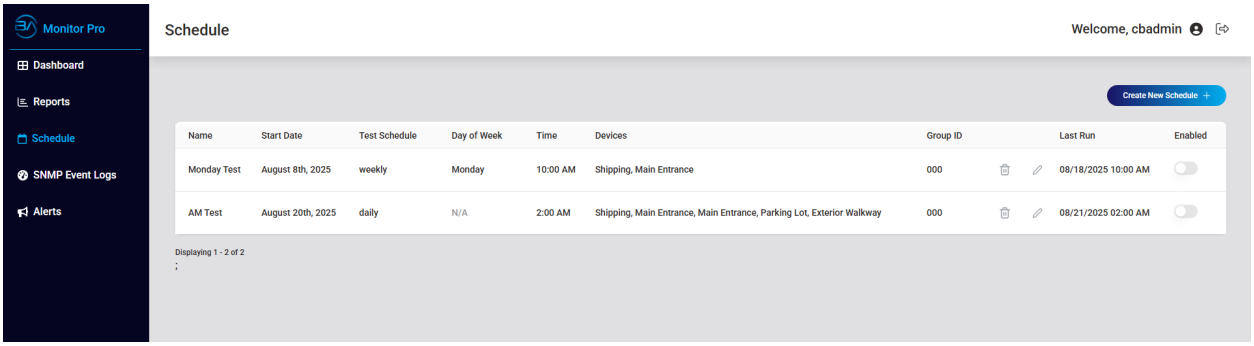
The Reports section provides a table of all previous presence tests. The Dropdown menu in the top left allows you to filter by the name of the devices.

Each row can be selected to show more detail of the device that was tested.



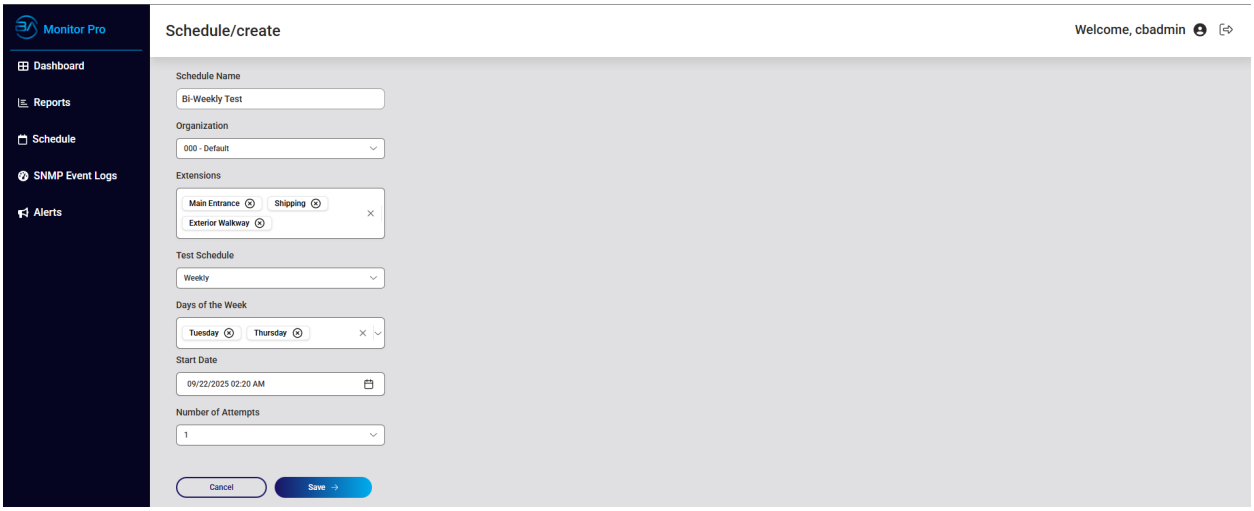
Schedule

Create scheduled presence test events for one or many devices.



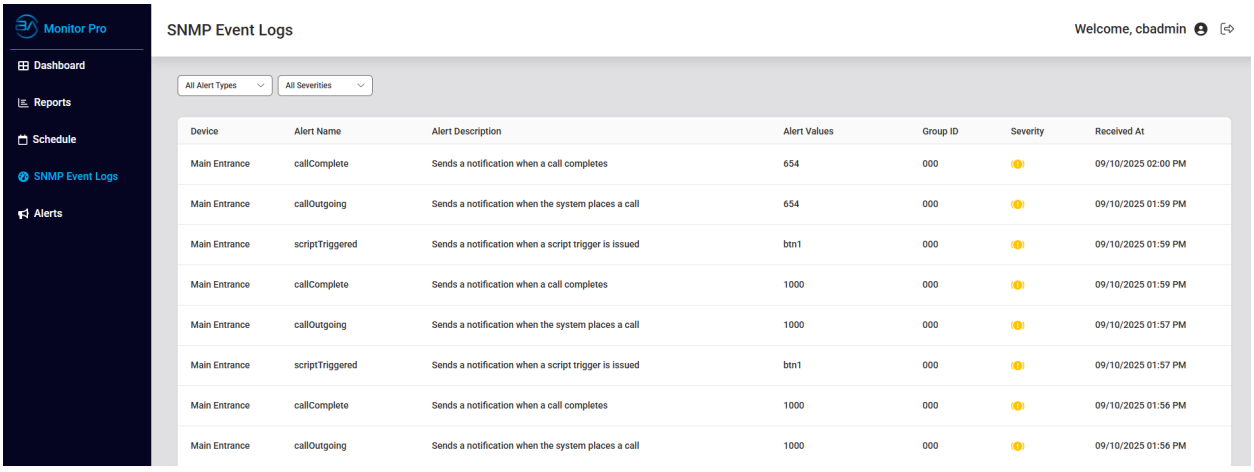
Create New Schedule +

Build a new schedule event to run automatically at pre-determined times. Results of the scheduled tests can be emailed or viewed in the Reports section.



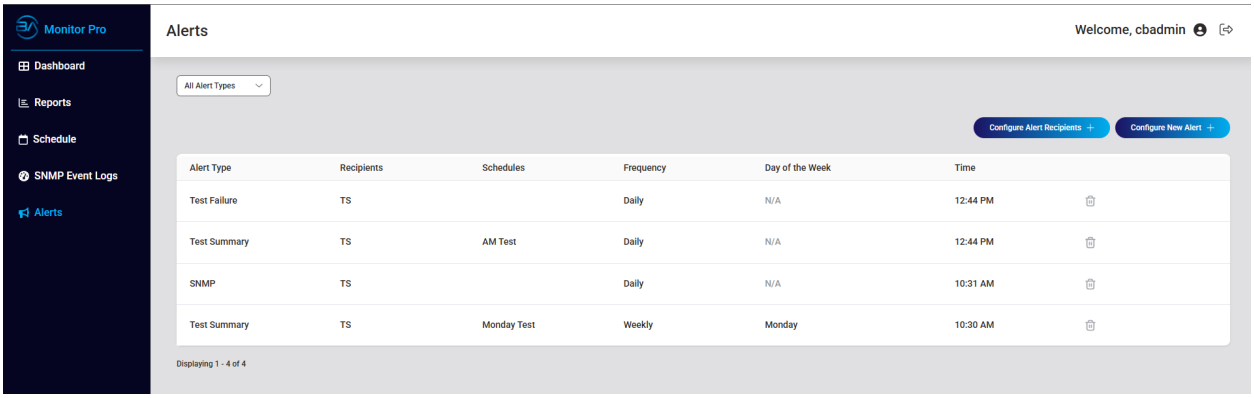
SNMP Event Logs

The SNMP Events log shows all received SNMP Traps from monitored stations. The dropdown menus can be used to filter the table by device of severity.



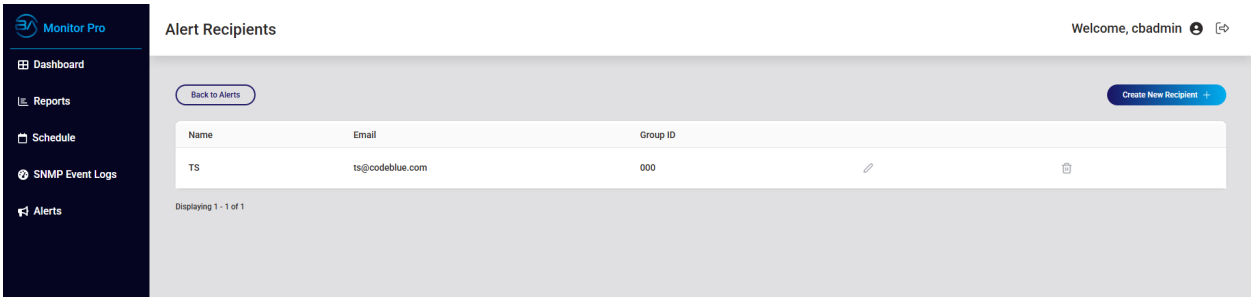
Alerts

Configure and schedule Email alerts for individual tests and scheduled test events.



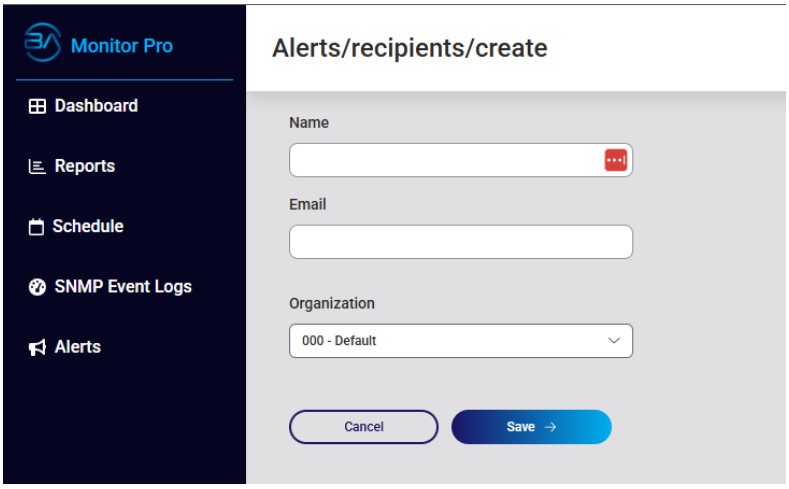
Configure Alert Recipient

Add email addresses to receive notifications.



Add New Recipient +

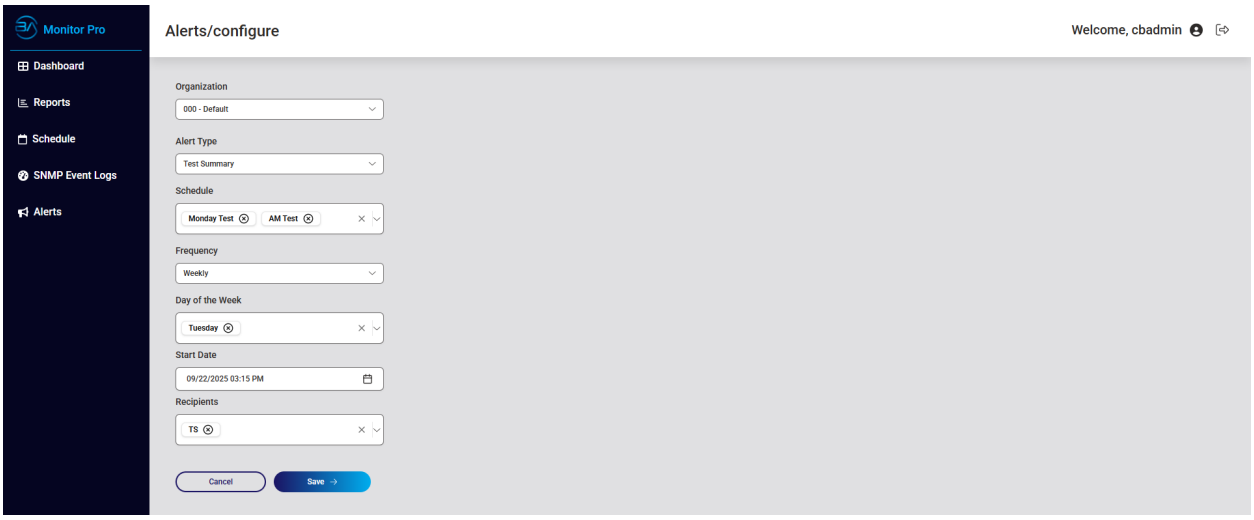
Enter name and email address of new recipient



Configure New Alert

Alerts can be created for individual SNMP Traps, individual station presence test failure, or scheduled presence test summaries.

For the scheduled tests summary alerts, you can select one or multiple scheduled tests and frequency of the reports.



Users

To add, remove, update password or change role of users.

“Admin” role has full access to all features.

“User” Role has access to all features except the Users section.