

TOOLVOX Admin | CDR Reports | EM3 Records | IP Info | Help

Setup Tools

ToolVox System Status

ToolVox Notices
No new notifications
[Show all](#)

ToolVox Statistics

Tool active calls	3
Internal calls	3
External calls	3
Tool active channels	3

ToolVox Connections
[IP Trunks Overview](#)

Uptime

System Uptime: 1 day, 1 hour, 31 minutes
PBX Engine Uptime: 1 day, 1 hour, 30 minutes
Last Reload: 1 day, 58 minutes

System Statistics

Processor
Load Average: 0.10
CPU: 0%

Memory
RAM Memory: 91%

Disks
/: 0%
/usr: 8%

Networks
eth0: 3.45 Kbps
eth1: 0.72 Kbps
eth2: 0.00 Kbps
eth3: 0.00 Kbps

Server Status

PBX Engine	<div style="width: 100%;"></div>
MySQL	<div style="width: 100%;"></div>
Web Server	<div style="width: 100%;"></div>
SIP Server	<div style="width: 100%;"></div>

TOOLVOX
Version: 3.2.10 (2014.02.10) © 2014 Code Blue Corporation
ToolVox is a registered trademark of Code Blue Corporation

TOOLVOX³

Administrator Guide



Code Blue

800.205.7186 • www.codeblue.com



Table of Contents

Section	Page
2 IP Network Resources.....	3
3 Configuring Server Settings.....	5
4 ToolVox® Software Update Procedure.....	11
5 Configuring Digital & Analog (DAHDI) Hardware.....	13
6 Configuring Trunks.....	18
7 Configuring Outbound Routes.....	28
8 Configuring Code Blue Devices.....	30
9 Configuring Business Phones.....	55
10 Configuring Digital Receptionist (IVR).....	58
11 Configuring Inbound Routes.....	62
12 Configuring System Recordings.....	65
13 Configuring License Key Administration.....	66
14 Configuring Backup & Restore.....	67
15 Unit Programming and Diagnostics (UPD) Configuration and Operation.....	69
16 Integrations.....	85
16.1 Milestone XProtect.....	85
16.2 Lenel OnGuard®.....	102
16.3 SIP Trunk Configuration with Cisco CM.....	134
17 IP Audio Interface Wiring Diagram.....	139
18 Lightning Protection.....	140
19 ToolVox DHCP Server Configuration.....	143
20 Email - Postfix Setup for ToolVox X3.....	145
21 Virtual Instance Setup Guide.....	172
21.1 Initial Configuration.....	172
21.2 Manual Network Configuration.....	172
21.3 Licensing.....	172
22 Download Information.....	173



2 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® EMS

TCP outgoing to port 5038 on ToolVox

RTSP outgoing to port 554 (or other locally-configured port) on cameras if video is in use

IP1500/2500/5000

HTTP/TCP, HTTPS/TCP incoming to ports 80, 443 for web-based management

NTP/UDP outgoing to port 123 on ToolVox for time service

SNMP/UDP incoming to port 161 for UPD testing

SNMPTRAP/UDP outgoing to port 162 for UPD traps

HTTPS/TCP incoming to port 443 from ToolVox for programming

IAX2/UDP outgoing to port 4569 on ToolVox

SIP/UDP outgoing to port 5060 on ToolVox

RTP/UDP incoming from ToolVox to UDP ports 23456-23556 (configurable)

TFTP outgoing to port 69 for batch programming

ToolVox

DHCP for IP5000 units if configured

SSH/TCP incoming to port 22 for secure shell management

SMTP/TCP outgoing to port 25 on configured mail server for mail alerts

DNS/UDP outgoing to port 53 if configured to use DNS servers

HTTP/TCP, HTTPS/TCP incoming to ports 80, 443 for web-based management

NTP/UDP incoming to port 123 from IP1500/2500/5000 for time service

SNMP/TCP outgoing to port 161 on IP1500/2500/5000 for UPD testing

SNMPTRAP/TCP incoming to port 162 from IP1500/2500/5000 for UPD traps

H.323/TCP incoming and outgoing to and from port 1720 for H.323 trunks

HTTPS/TCP incoming to port 2000 for Webmin management

TCP incoming to port 2840 from Blue Alert clients

IAX2/UDP incoming to port 4569 from IAX2 phones

TCP incoming to port 5038 from EMS clients

RTSP outgoing to port 554 (or other locally-configured port) on cameras if EMS video is in use

SIP/UDP incoming to port 5060 from SIP phones and trunks

RTP/UDP incoming to ports 10000-20000 from SIP and H.323 phones and trunks

TFTP incoming to port 69 from SIP phones for batch programming

ToolVox Blue Alert MNS

Core Application

HTTP/TCP and HTTPS/TCP incoming to ports 80 and 443 on ToolVox

Optional Internet access to the Google Maps API over HTTP and HTTPS for aerial imagery

4U2SEE Digital Signage

TCP outgoing to port 3001 on 4U2SEE digital signs



Desktop Alert

Multicast UDP to port 9264 on the configured IPv4 multicast address, which must be routed appropriately to destination systems

Email

SMTP/TCP outgoing to port 25 on configured mail relay

PAS

Delivered via telephony connections to Code Blue PAS units (see ToolVox and IP5000 network resources)

RSS

HTTP/TCP incoming to port 80 to read feed content
This access should be proxied instead of allowing ToolVox to directly service requests from public networks

SMS via 2SMS

HTTP/TCP to port 80 via the Internet to www.2sms.com

SMS via email

See "Email"



3 Configuring Server Settings

Warning: Advanced knowledge of the ToolVox system is required before making any changes other than network settings to the system. Changing settings other than the network settings may result in complete system failure. Hourly support packages are available and require remote access to the system via remote desktop control.

The ToolVox X3 has the IP configuration set to DHCP by default. While facing the back of the ToolVox X3 server, the NIC on the left is eth0 and the NIC on the right is eth1. NIC eth0 is the only interface that is activated at boot. NIC eth1 would need to be activated in Webmin, if it is needed. A user account was also added to run the following from the CLI for those familiar with Linux platforms:

There are multiple methods for logging into the ToolVox server. Initially you may just want a keyboard and monitor directly plugged into the server. You can then configure the network settings using CLI commands listed below. Once you know the IP address of the server you can connect via SSH or use a web browser and enter the Webmin side of the server to edit network settings. You do not need to do both methods.

Configuration of Network Settings Via Direct Connect and SSH commands:

This is the login information for the user account on the Toolvox systems:

Login: cbadmin
Password: CodeBlue92

These are some of the common commands this user is able to run as sudo:

Ifconfig (see current network info)

The server by default is DHCP so once you have connected a network connection to the eth0 port on the rear of the server, it will pull an IP address if DHCP is running on your network.

If the network is not running DHCP, then run the below command to configure a static IP address.

sudo system-config-network (setup Dynamic/Static network settings for the ToolVox).



1. Select Edit Devices and eth0 (illus. 5 and 6).

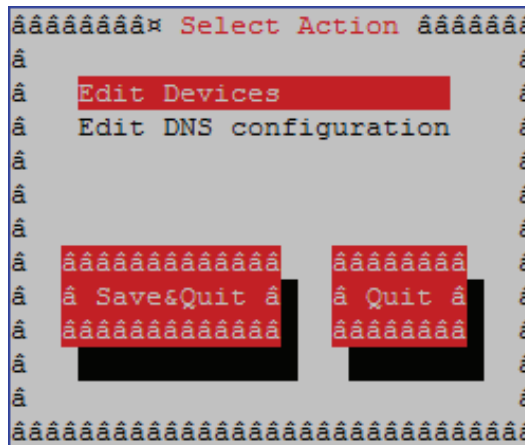


Illustration 5

2. Enter your static IP address, Netmask, and Default Gateway, then select Ok, Save, and

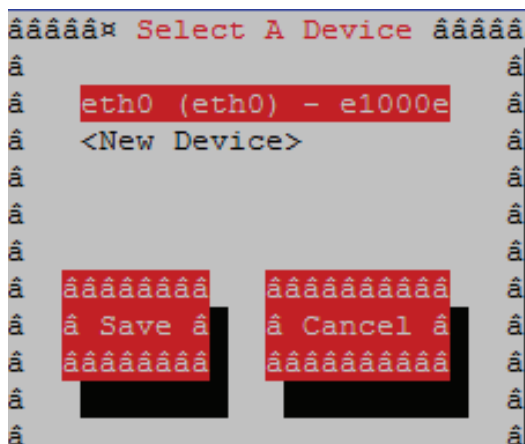


Illustration 6

Save & Quit (illus. 7).

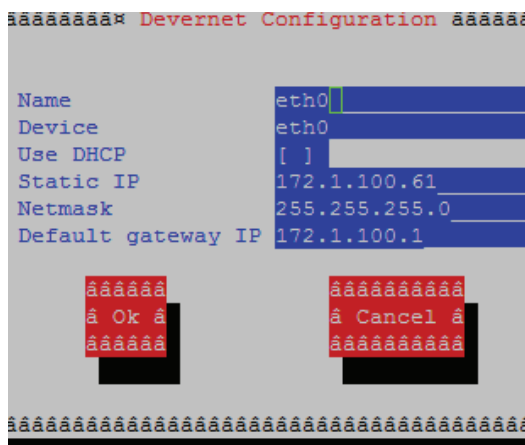


Illustration 7



NOTE: After changing the network settings, you **MUST** restart your network services using the following command:

```
sudo /etc/init.d/network restart
```

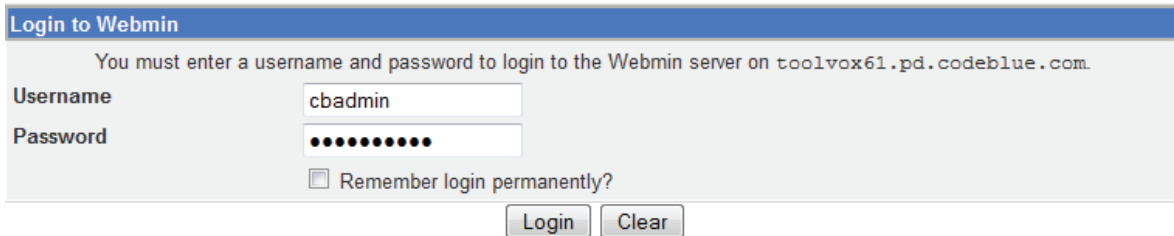
If you already know the IP address of ToolVox you can simply browse to the IP address of ToolVox you can simply browse to the IP address to directly access the system and begin setting up Code Blue Phones. The below is another side of the server if you wanted to setup the network devices and/or the Post Fix Mail Server settings.



Webmin commands:

Once you connect ToolVox to your network, you should be able to log in to the Webmin management portal with the DHCP assigned address or Static IP that you set up in the preceding steps: Using your web browser, browse to: <https://ToolVoxIP:2000>.

Enter the default username '**cbadmin**' and password '**codeblue**'.
Click Login



Login to Webmin

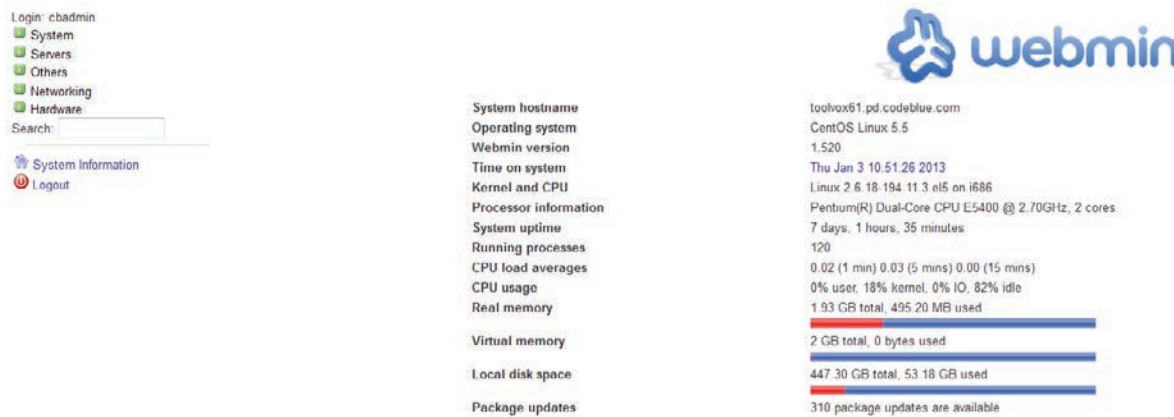
You must enter a username and password to login to the Webmin server on `toolvox61.pd.codeblue.com`.

Username:

Password:

Remember login permanently?

If you wish to change
Click Networking on the left navigation bar.



Webmin dashboard showing system information:

- System hostname: toolvox61.pd.codeblue.com
- Operating system: CentOS Linux 5.5
- Webmin version: 1.520
- Time on system: Thu Jan 3 10:51:26 2013
- Kernel and CPU: Linux 2.6.18-194.11.3.el5 on i686
- Processor information: Pentium(R) Dual-Core CPU E5400 @ 2.70GHz, 2 cores
- System uptime: 7 days, 1 hours, 35 minutes
- Running processes: 120
- CPU load averages: 0.02 (1 min) 0.03 (5 mins) 0.00 (15 mins)
- CPU usage: 0% user, 18% kernel, 0% IO, 82% idle
- Real memory: 1.93 GB total, 495.20 MB used
- Virtual memory: 2 GB total, 0 bytes used
- Local disk space: 447.30 GB total, 53.18 GB used
- Package updates: 310 package updates are available


Click on Network Configuration.



Webmin Network Configuration page with tabs: Network Interfaces, Routing and Gateways, Hostname and DNS Client, Host Addresses.

Click this button to activate the current boottime interface and routing settings, as they normally would be after a reboot. Warning - this may make your system inaccessible via the network, and cut off access to Webmin.

Click on Network Interfaces.



Webmin Network Interfaces page showing active interfaces:

Name	Type	IP Address	Netmask	Status
<input type="checkbox"/> eth0	Ethernet	172.1.100.61	255.255.255.0	Up
<input type="checkbox"/> lo	Ethernet	fe80::21c:c0ff:feb0:950f	64	Up
<input type="checkbox"/> lo	Loopback	127.0.0.1	255.0.0.0	Up
<input type="checkbox"/> lo	Loopback	:::1	128	Up



Click on Activated at Boot then click on `eth0`.

Module Index

Edit Bootup Interface

Boot Time Interface Parameters

Name: `eth0` Activate at boot? Yes No

Address source: From DHCP From BOOTP Static configuration

IP Address: 172.1.100.61
 Netmask: 255.255.255.0
 Broadcast: Automatic 172.1.100.255

MTU: Default
 Hardware address: Default

Virtual interfaces: 0 (Add virtual interface)

[Return to network interfaces](#)

Enter the IP Address and Netmask then click

Click [Return to network configuration](#)

Click on [Routing and Gateways](#)

Module Index

Routing and Gateways

Boot time configuration **Active configuration**

This section allows you to configure the routes that are activated when the system boots up, or when network settings are fully re-applied.

Routing configuration activated at boot time

Interface	Gateway
eth0	172.1.100.1

Act as router? Yes No

Interface	Network	Netmask	Gateway

Interface	Network	Netmask

[Return to network configuration](#)

Enter the Gateway IP Address for eth0 and click

Click [Return to network configuration](#)

Click on [Hostname and DNS Client](#)

Module Index

Hostname and DNS Client

DNS Client Options

Hostname: toolvox61.pd.codeblue.com

Resolution order: Hosts DNS Search domains

DNS servers:

None Listed

pd.codeblue.com

[Return to network configuration](#)

Enter Hostname and DNS server IP Address information (if other than default) then click



This concludes the network configuration. You may need to reboot the system for the new settings to take effect. Below is the list of the settings you can control via Webmin on your ToolVox.

Login: cbadmin

- System
 - Bootup and Shutdown
- Servers
 - DHCP Server
 - Postfix Mail Server
- Others
 - System and Server Status
- Networking
 - Linux Firewall
 - Network Configuration
- Hardware
 - CD Burner
 - System Time

Search:

 [System Information](#)

 [Logout](#)

Under Bootup and Shutdown you can shut down or restart your ToolVox. Located at the bottom of the Bootup and Shutdown section.



4 ToolVox® Software Update Procedure

Only customers under ToolVox Annual Maintenance plans receive Full Hardware & Software Coverage and Software Upgrades/Enhancements/Bug fixes etc. Please inquire to Customer Service if not under a Plan.

ToolVox Software Update

1.1 Insert the ToolVox Update CD for your ToolVox edition (Standard or Advanced) into the ToolVox hardware’s DVD-ROM drive

1.2 Browse to the IP address of your ToolVox Communications Server

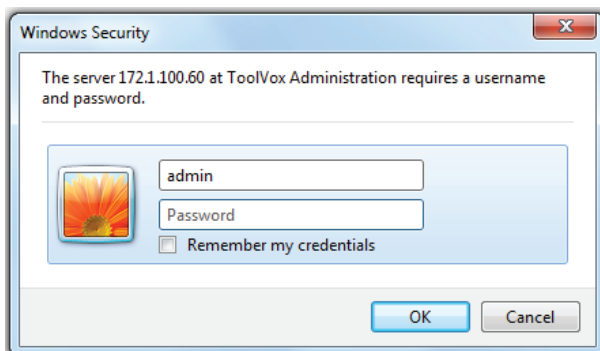
1.2.1 http://<IP address of ToolVox>

1.2.2 Click on “Administration”



1.3 Enter “Username”: admin

1.4 Enter “Password”: codeblue (default) or another password





1.5 Click on **Tools** next to Setup

1.6 WARNING – if you haven't done a backup recently please consider this a good time to start this practice. See "Configuring Backup & Restore" chapter.

1.7 Under "System Administration", click **ToolVox Update**

1.8 Click **Update System**.

1.9 Select **Apply configuration changes** (red bar) at the top of screen and Reload (red box)

The screenshot shows the ToolVox web interface. At the top left is the 'TOOLVOX' logo. To its right is a navigation bar with buttons for 'Admin', 'CDR Reports', 'EMS Records', 'IP Info', and 'Help'. Below this is a sidebar menu with two main sections: 'Setup' and 'Tools'. Under 'Tools', several items are listed, including 'Admin', 'Support', 'System Administration', and 'User Settings'. The 'ToolVox Update' item is highlighted with a red bar. The main content area on the right is titled 'ToolVox System Update'. It includes a 'System Version' section showing 'ToolVox X3' and 'Version 2.99.7+3.0beta3-1'. Below that is an 'Update' section with instructions: 'Insert your ToolVox Update CD-ROM into the system drive and press the button below to install updates'. A warning message states: 'WARNING: Make sure you have backed up your system configuration before proceeding!'. At the bottom of this section is a button labeled 'Update System'.

1.10 After updating, you may need to refresh your screen.

1.11 Log out and then log back in to ToolVox.

1.12 The update process is now complete.



5 Configuring Digital & Analog (DAHDI) Hardware

Digital Hardware

Span	Alarms	Framing/Coding	Channels Used/Total	Signalling	Action
Wildcard TE131/TE133, Card 1 - Port (span_1)	OK	ESF/B8ZS	24/24	tko_ks	Edit

Analog Hardware

Type	Ports	Action
FXO Ports	25,26	Edit
FXS Ports	27,28	Edit

Advanced Settings

Module Name: wctdm24exp
 Tone Region: United States/North America
 Opermode: USA
 A-law Override: ulaw
 FXS Honor Mode: Apply Opermode to FXO Modules
 Boosting: Normal
 Fastringer: Normal
 Lowpower: Normal
 Ring Detect: Standard
 MWI Mode: None

Buttons: Cancel, Save, Restart DAHDI

This is used to display and configure Digital and Analog Hardware that may have been installed in your ToolVox. T1 PRI, FXO, and FXS, depending on what is required in the application.

The Ports will be auto numbered during boot up of the ToolVox.

FXS Ports – FXS’s produce dial tone and should be cross connected to analog Code Blue devices or phones that need dial tone. These FXS Port numbers are used when you build your phones in Code Blue Devices.

Click the Blue “Edit” button next to the FXS Ports. They should be configured as follows. Note that your port numbering may be different and the Group Number should be 1. Do not change Kewl Start.



Analog FXS Ports

NOTE: Analog ports with group 0 will be placed

Port 27: Kewl Start ▾ Group: 1

Port 28: Kewl Start ▾ Group: 1

Hit save then



Then Continue with reload.

Apply Configuration Changes

Reloading will apply all configuration changes made in ToolVox to your PBX Engine and make them active.

Continue with reload

Cancel reload and go back to editing

If done making adjustments in DAHDI then press the Restart DAHDI button.

Press OK

Restarting DAHDI will temporarily shut down your PBX engine and may take several minutes.

Please wait for the page to return before continuing to configure ToolVox.

Are you sure you want to do this?



FXO Ports – FXO's receive dial tone, and should be cross connected to Bell POTS phone lines or to Phone lines from customer PBX. These Port numbers are used when you build trunks to transport calls into and out of the ToolVox.

Click the Blue "Edit" button next to the FXO Ports. Note that your port numbering may be different and the Group Number should be 2. Do not change Kewl Start and make sure the ports are set up as follows.

Hit save then



Then Continue with reload.

If done making adjustments in DAHDI then If done making adjustments in DAHDI then press the Restart DAHDI button.

Press OK



T1 PRI – If you are interconnecting ToolVox with a PBX via a T1 PRI configure this section provided your hardware displays.

Click the Blue “Edit” button next to the Wildcard TE122 Card.



Set the ToolVox to the opposite of the PRI Signaling then the PBX your connecting to.

Span: Wildcard TE131/TE133 Card 0

Alarms: OK

Framing/Coding: ESF/B8ZS ▾

Channels: 23/24 (T1)

Signalling: PRI - CPE ▾

Switchtype: National ISDN 2 (default) ▾

Sync/Clock Source: 0 ▾

Line Build Out: 0 db (CSU)/0-133 feet (DSX-1) ▾

Pridialplan: National ▾

Prilocaldialplan: National ▾

Group: 3

Context: from-pstn

Channels: 23 ▾ From: 1-23 Reserved: 24

Cancel Submit

Restart DAHDI

Customer PBX needs to be Net or CPE.
Hit save then

✖ Apply Configuration Changes

Then Continue with reload.

Apply Configuration Changes

Reloading will apply all configuration changes made in ToolVox to your PBX Engine and make them active.

Continue with reload

Cancel reload and go back to editing

If done making adjustments in DAHDI then If done making adjustments in DAHDI then If done making adjustments in DAHDI then press the Restart DAHDI button.

Cancel Save

Restart DAHDI

Press OK

Restarting DAHDI will temporarily shut down your PBX engine and may take several minutes.

Please wait for the page to return before continuing to configure ToolVox.

Are you sure you want to do this?

OK Cancel



6 Configuring Trunks

The screenshot shows the ToolVox X3 administrator interface. At the top left is the 'TOOLVOX' logo. To its right are navigation tabs: 'Admin', 'CDR Reports', 'EMS Records', 'IP Info', and 'Help'. Below the logo is a sidebar menu with two main sections: 'Setup' and 'Tools'. Under 'Setup', there are sub-sections: 'Admin' (containing 'ToolVox System Status'), 'Basic' (containing 'Business Phones', 'DAHDI', 'General Settings', and 'Outbound Routes'), 'Trunks' (highlighted in red), 'Administrators', and 'Code Blue Software' (containing 'License Key Administration' and 'Code Blue Devices'). The main content area is titled 'Add a Trunk' and features a list of options: 'Add Trunk' (a red button), 'SIPto61 (sip)', and five green plus icons with corresponding text: 'Add Zap Trunk (DAHDI compatibility mode)', 'Add SIP Trunk', 'Add IAX2 Trunk', 'Add ENUM Trunk', and 'Add DUNDI Trunk'. A sixth option, 'Add Custom Trunk', is also visible at the bottom of the list.

To be able to pass calls from the ToolVox to exterior phones lines or to a PBX you must configure a trunk.

Your options are Dahdi (PRI T1, FXO phone line), IAX2, or a SIP trunk. If your server has hardware installed it will display in the DAHDI screen.



Add ZAP/DAHDI Trunk



Admin CDR Reports EMS Records IP Info Help

Setup | Tools

Admin

ToolVox System Status

Basic

Business Phones

DAHDI

General Settings

Outbound Routes

Trunks

Administrators

Code Blue Software

License Key Administration

Code Blue Devices

Diagnostic Schedules

Diagnostic Reports

EMS Administration

UPD Administration

PAS Administration

Inbound Call Control

Inbound Routes

Announcements

Follow Me

IVR

Ring Groups

Time Conditions

Time Groups

Internal Options & Config

Languages

Misc Destinations

System Recordings

Third Party Addon

Custom Contexts

Add Trunk
SIPto61 (sip)

Add ZAP Trunk (DAHDI compatibility mode)

General Settings

Trunk Description:

Outbound Caller ID:

CID Options: Allow Any CID ▾

Maximum Channels:

Disable Trunk: Disable

Monitor Trunk Failures: Enable

Outgoing Dial Rules

Dial Rules:

Clean & Remove duplicates

Dial Rules Wizards: (pick one) ▾

Outbound Dial Prefix:

Outgoing Settings

Zap Identifier (trunk name):

Submit Changes

General Settings

Outbound Caller ID(Optional): This is the Caller ID that will be used for outbound calls on this trunk. The format is: "Caller Name" <#####>. You can use the string "hidden" to disable Caller ID on this trunk if it is a digital line



(PRI/BRI/E1/T1/J1/SIP/IAX).

Never Override Caller ID(Optional): Check this box to disable using the Outbound CID set up in the extensions configuration page. You must enter an Outbound Caller ID when checking this box.

Maximum Channels(Optional): The maximum number of outgoing calls that can be made simultaneously on this trunk. Incoming calls have no effect on the maximum. A default of blank specifies no maximum.

Disable Trunk(Optional): Disables the trunk for all routes configured.

Monitor Trunk Failures(Optional): If checked enter the AGI script that will be called to either log, email, or take action due to a trunk failure other than CANCEL or NOANSWER.

Outgoing Dial Rules

Dial Rules(Optional): A Dial Rule to set how calls are sent out this trunk. If your outbound call does not match anything then it will be dialed as is.

- X matches any digit from 0-9
- Z matches any digit from 1-9
- N matches any digit from 2-9
- . is a wildcard that matches one or more characters
- | removes the dialing prefix from the number dialed. Example 9|.
 - o This would send any number beginning with 9 out this route. 95551212 would send 5551212 out this trunk.
- + adds a dialing prefix to the number dialed. Example 1616+.
 - o This would add 1616 to any number sent out this trunk. 5551212 would be prepended and sent to the carrier as 16165551212.

Dial Rules Wizards(Optional): Useful in creating Dial Rules. You can use the wizard to add or delete a prefix to numbers or lookup numbers for local calling.

Outbound Dial Prefix(Optional): Enter the outbound dial prefix for Centrex or other custom type of trunks where you have to dial a 9 etc. to make a call to the PSTN.

Outgoing Settings

ZAP Identifier (trunk name): This is the group number or individual channel number of this trunk. After you have looked in the DAHDI menu screen and noted the FXO channel numbers you need to create one of these trunks for each FXO you wish to use.

For example if your FXO's are 1-4 enter 1 in the Zap Identifier (trunk name) field. Then create 3 more trunks, 2,3, and 4. Your Outbound Route will need to be created that will reference these trunks as available routes.

If using a PRI T1, use the group number you were assigned in DAHDI. Example g3

To save your settings click:

Submit Changes



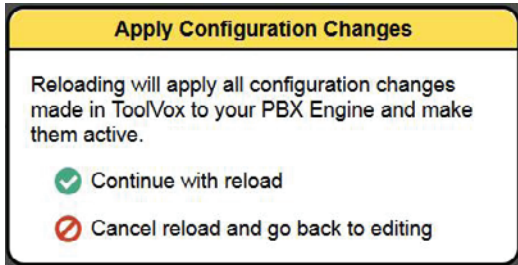
To apply the changes to the system click:



At the top of the screen.

Click - **Continue with reload** - to finish the changes otherwise click -

Cancel reload and go back to editing - to cancel the changes and continue editing the extension.





Add IAX2 Trunk

General Settings

Outbound Caller ID(Optional): This is the Caller ID that will be used for outbound calls on this trunk. The format is: "Caller Name" <#####>. You can use the string "hidden" to disable Caller ID on this trunk if it is a digital line (PRI/BRI/E1/T1/J1/SIP/IAX).

Never Override Caller ID(Optional): Check this box to disable using the Outbound CID set up in the extensions configuration page. You must enter an Outbound Caller ID when checking this box.

Maximum Channels(Optional): The maximum number of outgoing calls that can be made simultaneously on this trunk. Incoming calls have no effect on the maximum. A default of blank specifies no maximum.

Disable Trunk(Optional): Disables the trunk for all routes configured.

Monitor Trunk Failures(Optional): If checked enter the AGI script that will be called to either log, email, or take action due to a trunk failure other than CANCEL or NOANSWER.



Outgoing Dial Rules

Dial Rules(Optional): A Dial Rule to set how calls are sent out this trunk. If your outbound call does not match anything then it will be dialed as is.

- X matches any digit from 0-9
- Z matches any digit from 1-9
- N matches any digit from 2-9
- . is a wildcard that matches one or more characters
- | removes the dialing prefix from the number dialed. Example 9|.
 - o This would send any number beginning with 9 out this route. 95551212 would send 5551212 out this trunk.
- + adds a dialing prefix to the number dialed. Example 1616+.
 - o This would add 1616 to any number sent out this trunk. 5551212 would be prepended and sent to the carrier as 16165551212.

Dial Rules Wizards(Optional): Useful in creating Dial Rules. You can use the wizard to add or delete a prefix to numbers or lookup numbers for local calling.

Outbound Dial Prefix(Optional): Enter the outbound dial prefix for Centrex or other custom type of trunks where you have to dial a 9 etc. to make a call to the PSTN.

Outgoing Settings

Trunk Name: The name you wish the trunk to be identified as.

PEER Details: Enter the details of the IAX2 PEER here. The order of any allow or deny statements will be followed in order.

USER Context: The user name or account identifier the PEER is expecting.

USER Details: Enter the details of the IAX2 USER here. The order of any allow or deny statements will be followed in order.

Registration

Register String: The registration string required to authenticate with the IAX2 PEER. Example: username:password@iax.toolvox.com

To save your settings click:

Submit Changes

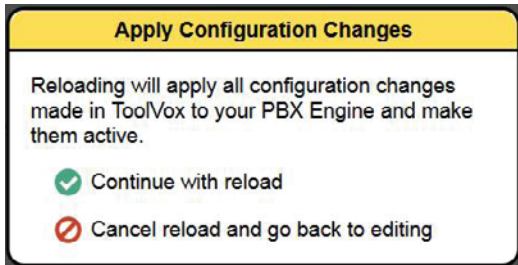
To apply the changes to the system click:

Apply Configuration Changes



At the top of the screen.

Click - **Continue with reload** - to finish the changes otherwise click - **Cancel reload and go back to editing** - to cancel the changes and continue editing the extension.





Add SIP Trunk

General Settings

Outbound Caller ID(Optional): This is the Caller ID that will be used for outbound calls on this trunk. The format is: "Caller Name" <#####>. You can use the string "hidden" to disable Caller ID on this trunk if it is a digital line (PRI/BRI/E1/T1/J1/SIP/IAX).

Never Override Caller ID(Optional): Check this box to disable using the Outbound CID set up in the extensions configuration page. You must enter an Outbound Caller ID when checking this box.

Maximum Channels(Optional): The maximum number of outgoing calls that can be made simultaneously on this trunk. Incoming calls have no effect on the maximum. A default of blank specifies no maximum.

Disable Trunk(Optional): Disables the trunk for all routes configured.

Monitor Trunk Failures(Optional): If checked enter the AGI script that will be called to either log, email, or take action due to a trunk failure other than CANCEL or NOANSWER.



Outgoing Dial Rules

Dial Rules: Dial Rules(Optional): A Dial Rule to set how calls are sent out this trunk. If your outbound call does not match anything then it will be dialed as is.

- X matches any digit from 0-9
- Z matches any digit from 1-9
- N matches any digit from 2-9
- . is a wildcard that matches one or more characters
- | removes the dialing prefix from the number dialed. Example 9|.
 - o This would send any number beginning with 9 out this route. 95551212 would send 5551212 out this trunk.
- + adds a dialing prefix to the number dialed. Example 1616+.
 - o This would add 1616 to any number sent out this trunk. 5551212 would be prepended and sent to the carrier as 16165551212.

Dial Rules Wizards(Optional): Useful in creating Dial Rules. You can use the wizard to add or delete a prefix to numbers or lookup numbers for local calling.

Outbound Dial Prefix(Optional): Enter the outbound dial prefix for Centrex or other custom type of trunks where you have to dial a 9 etc. to make a call to the PSTN.

Outgoing Settings

Trunk Name: The name you wish the trunk to be identified as.

PEER Details: Enter the details of the SIP PEER here. The order of any allow or deny statements will be followed in order.

Example:

host=X.X.X.X (Ip address of corresponding IP PBX)

type=peer

qualify=yes

context=from-internal

USER Context: The user name or account identifier the PEER is expecting. Most cases a name you make up and is not needed.

USER Details: Enter the details of the SIP USER here. The order of any allow or deny statements will be followed in order.

Example:

host=X.X.X.X (IP address of corresponding IP PBX)

type=user



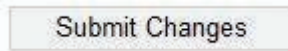
context=from-trunk

Registration

Register String(Optional): The registration string required to authenticate with the IAX2 PEER.

Example: username:password@iax.toolvox.com

To save your settings click:

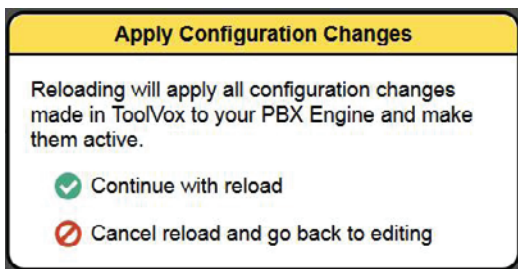


To apply the changes to the system click:



at the top of the screen.

Click - **Continue with reload** - to finish the changes otherwise click - **Cancel reload and go back to editing** - to cancel the changes and continue editing the extension.





7 Configuring Outbound Routes

Outbound Routes is the area that you configure the ToolVox to select a Trunk to transport calls out of ToolVox.

Route Name: Describe the type of route here. Examples would be: Local Calls, Long Distance and International.

The screenshot shows the 'Add Route' configuration page in the ToolVox X3 administrator interface. The page has a top navigation bar with 'Admin', 'CDR Reports', 'EMS Records', 'IP Info', and 'Help'. A left sidebar contains a menu with categories like 'Setup', 'Tools', 'Admin', 'Basic', 'Outbound Routes', and 'Inbound Call Control'. The 'Outbound Routes' category is selected. The main content area is titled 'Add Route' and includes the following fields and controls:

- Add Route** (button)
- 0 out** (button)
- Route Name:** text input field
- Route CID:** text input field with an **Override Extension CID** checkbox
- Route Password:** text input field
- PIN Set:** dropdown menu with 'None' selected
- Emergency Dialing:** checkbox
- Intra Company Route:** checkbox
- Music On Hold?:** dropdown menu with 'default' selected
- Dial Patterns:** large text area with a **Clean & Remove duplicates** button below it
- Dial patterns wizards:** dropdown menu with '(pick one)' selected
- Trunk Sequence:** dropdown menu
- Submit Changes** (button)

Route Password: (Optional)Use a route password to have the system prompt each caller to this route to enter the password in order to be able to make calls. This is useful to prevent unauthorized long distant or international calling.

Pin Set: (Optional)Enter the Pin Set group to be used for authenticating calls out on this route. If utilizing a Pin Set leave the Route Password field blank.

Emergency Dialog: (Optional)This setting will force the extensions Emergency CID to be used on an outgoing call. This setting is typically used on routes to 911 or public safety dispatch centers.

Intra Company Route: (Optional)This setting will preserve the internal Extension CID and not replace it with the Outbound CID of the extension or the trunk. This is used for dialing across connected ToolVox systems.

Music on Hold: (Optional)Select which music on hold category to use or select none.



Dial Patterns: A Dial Pattern will be used to select this trunk for outbound calls.

- X matches any digit from 0-9
- Z matches any digit from 1-9
- N matches any digit from 2-9
- . is a wildcard that matches one or more characters
- | separates the dialing prefix from the number dialed. Example 9|.ul>- o This would send any number beginning with 9 out this route. 95551212 would send 5551212 to the trunks selected by this route

Dial Patterns Wizard: (Optional) Use the wizard to select common route matching schemes.

Trunk Sequence: Select the trunks to be used for this route and which order they should be used in.

To save your settings click:

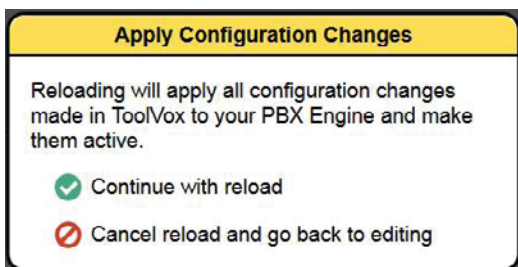


To apply the changes to the system click:



At the top of the screen.

Click - **Continue with reload** - to finish the changes otherwise click - **Cancel reload and go back to editing** - to cancel the changes and continue editing the extension.





8 Configuring Code Blue Devices

Device Info

Extension: This will be the internal number displayed on the phones Caller ID screen and EMS agent screen.

Caller ID Display Name: This will be the internal number NAME displayed on the phones Caller ID screen and EMS agent screen.

Unit Info

Model: Choose the type of Code Blue Phone you are configuring.

Subtype: This field only appears if you are selecting an IP5000 model speakerphone.

- IP5000 v1 is the legacy firmware 1.X.X phone;
- IP5000 v2 is the current production firmware 2.X.X phone.

Device Connection Type: Choose the method of connection the Code Blue phone is using to connect to ToolVox.

FXS Analog Extension – IA4100, CB3000, CB3100, IA500

SIP & IAX Extensions – IP1500/2500/5000

Off System Unit – IA4100, CB3000, CB3100, IA500

The difference between Off System and FXS is that FXS are FXS ports providing dial tone directly off of ToolVox. Off System Unit means the analog phone line is provided by an external PBX or local Bell company.



Assigned DID/CID

(Optional) If you wish to have an inbound Direct Dialed number associated to this phone and ring it when dialed you can fill this out and it will create an Inbound Route to this Extension.

Push the Next button to continue configuration

Next

Please scroll down in this manual to the appropriate Model of phone you are provisioning. They are titled in **RED** lettering.

CB3000 & CB3100 Models

Device Options - FXS Analog Extension type

This device uses zap technology.

Channel (FXS Port)	<input type="text"/>
context	from-internal
immediate	no
signalling	fxo_ks
echocancel	yes
echocancelwhenbridged	no
echotraining	100
busydetect	no
busycount	7
callprogress	no

Enter in the FXS Port number from Dahdi that you have cross connected the Analog Code Blue Phone to. Do not duplicate this number with another Code Blue Device.

Every other field in the Device Options FXS analog Extension type Section leave as default.

Device Options - Off System Unit

This device uses custom technology.

Unit Phone Number

Enter in the actual phone number ToolVox needs to dial to reach this unit.

Example: 916163928296 or 6163928296 or 4378

This may or may not be the same number you assigned it as an extension on the ToolVox system



Voicemail Playback Commands

<input type="radio"/>	Play Message 1 to Guard
<input checked="" type="radio"/>	Play Message 1 at Unit
<input type="radio"/>	Play Message 1 at Unit. Play Message 2 to Guard
<input type="radio"/>	Play Messages to Guard and at Unit
Message 1	<input type="text" value="None"/>
Message 2	<input type="text" value="None"/>
Message Repeat	<input type="text" value="1"/> times
Playback Volume	<input type="text" value="3"/>

Skip this section if not using Messages. See the System Recording on how to load Messages.

Play Message 1 to Guard – 1st single message must be less than 18 seconds and will be played only to the guard.

Play Message 1 at Unit – 1st message must be less than 18 seconds and will be played at the CB unit until the guard answers.

Play Message 1 at Unit. Play Message 2 to Guard – 1st message must be less than 9 seconds and will be played at the CB unit until the guard answers. 2nd message must be less than 9 seconds and will be played to the guard and at the CB unit until the guard answers.

Play Messages to Guard and at Unit – 1st message must be less than 9 seconds and will be played at both ends after the guard answers. 2nd message must be less than 9 seconds and will be played at both ends after the 1st message.

Message 1 & Message 2 – you can select System Recordings you have previously loaded.

Message Repeat – How many times to repeat the message.

Playback Volume – 3 is the highest

Other Options

<u>Ring Down and ANI</u>	Line Type
	<input checked="" type="radio"/> Standard Trunk <input type="text" value="Disable ANI"/>
	<input type="radio"/> Ring Down <input type="text" value="Disable ANI"/>
<u>Call Button</u>	<input checked="" type="radio"/> Auto Dial Off
	<input type="radio"/> Auto Dial On
<u>Ring Back Detection</u>	<input type="radio"/> Disabled
	<input checked="" type="radio"/> Enabled
<u>Wink Time</u>	<input type="text" value="2"/> milliseconds
<u>In Call Commands</u>	<input type="radio"/> Disabled
	<input checked="" type="radio"/> Enabled
<u>Ring Time</u>	<input type="text" value="30"/>



Ring Down and ANI – Ring down selection & Automatic Number identification (ANI). Selections 0-3 are available only for standard trunk lines, while selections 4-6 are available only for analog ring down lines. Note: this was originally for RPD/CMS. For most users you only need to select whether this CB phone is connected on a Dial up phone line or a Ring Down/Hot line.

Call Button (CB3100 only) – This command is used with the CB3100K keypad faceplate to allow for a number to be automatically dialed before using the keypad.

Ring Back Detection (CB3100 only) – Call progress monitor for hang up.

Wink Time (CB3100 only) – This is the minimum amount of time that talk battery is removed or reversal of polarity for the CB phone to hang up. 2=200 milliseconds etc. 0-9

In Call Commands (CB3100 only) – The operators ability to send commands during a call.

Ring Time – The amount of time the phone will try a number before resetting and dialing the next number 00-60.

Dial Type (CB3000 only) – Phone line uses Pulse or DTMP encoding

Other Options (cont.)

- Auxiliary #2
 - Unslave from Aux #1
 - Slave to Aux #1
- Auto Connection
 - Disabled
 - Enabled
- Auxiliary #2 Active Time

Auxiliary #2 – Determines whether Auxiliary output #2 (pins 7&8) activate the same as Auxiliary output #1 (pins 5&6 Slaved) or by pressing the 6 key during a call (Unslaved).

Auto Connection – If Auxiliary output #2 is unslaved from Auxiliary output #1, Disabling allows the use of the In Call Command (DTMF 6) to activate Auxiliary output #2. If enabled Auxiliary output #2 will activate on an incoming call.

Auxiliary #2 Active Time – The amount of time Auxiliary output #2 will stay active. 00=Active for the duration of the call. 01-89=Active for 1-89 minutes. 90-99=5-50 seconds in 5 second increments (90=5 seconds, 91=10 seconds, etc.)



Phone Numbers

1 st Emergency Number	<input type="text"/> Ringback Cadence 1 ▾
2 nd Emergency Number	<input type="text"/> Ringback Cadence 1 ▾
3 rd Emergency Number	<input type="text"/> Ringback Cadence 1 ▾
1 st Information Number	<input type="text"/> Ringback Cadence 1 ▾
2 nd Information Number	<input type="text"/> Ringback Cadence 1 ▾
3 rd Information Number	<input type="text"/> Ringback Cadence 1 ▾
Power loss Phone Number	<input type="text"/> Ringback Cadence 1 ▾

Progress Tone Table

Cadence #	Ring Back(seconds)	Busy Tones(seconds)	Recorder Tone
1	2 ON, 4 OFF	1/2 ON, 1/2 OFF	1/4 ON, 1/4 OFF
2	1/2 ON, 1/4 OFF, 1/2 ON, 4 OFF	1/2 ON, 1/2 OFF	1/4 ON, 1/4 OFF
3	1/2 ON, 1/2 OFF, 1/2 ON, 2 1/2 OFF	1/2 ON, 1/2 OFF	1/4 ON, 1/4 OFF
4	1 ON, 3 OFF	1/2 ON, 1/2 OFF	1/4 ON, 1/4 OFF

Cycle Count ▾

Enter in the Phone Number you wish the CB phone to call. If you have a double button phone enter in the Number you wish for the Information Number. A Cadence table is provided if you desire custom tone intervals.

Cycle Count – Number

of cycles the CB phone will cycle through the above Numbers if a busy tone is encountered

Command Passwords

Programming Password	<input type="text" value="2258"/>
Monitoring Password	<input type="text" value="2258"/>

Programming Password – The password used to access programming mode(2) on initial calls into the unit.

Monitoring Password – The password used to access 2-way monitoring mode(1) on initial call in to the unit.



Commands

Off Hook Time	<input type="text" value="10"/> minutes
Silent Timeout & Alt Hangup	<input type="text" value="00"/> seconds
Auxiliary Input #1	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Speaker Operation	<input type="radio"/> Speaker disabled for entire call <input type="radio"/> Speaker disabled while placing call <input checked="" type="radio"/> Speaker enabled for entire call
Wait for Dial Tone	<input type="text" value="5"/> seconds
Wait for Call Progress Tone	<input type="text" value="20"/> seconds

Off Hook Time – Maximum conversation time in minutes before CB phone hangs up.

Silent Timeout Alternate Hang-up Method – If this command is enabled the CB phone will hang-up after hearing silence for the set number of seconds. 00-disabled 05-99 seconds.

Auxiliary Input #1 – Enables Auxiliary Input #1 (pins 9&10). When activated it will activate a red button call.

Speaker Operation – Select the type of speaker operation here

Wait for Dial tone – This is the maximum time that the CB phone will wait for a dial tone 0-99 seconds.

Wait for progress tone – This is the maximum time that the CB phone will wait for a call progress tone after the last digit has been dialed.

In-Call Commands

#	Command Text	DTMF Tone
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>

This is used to display the In-Call Commands in the Pop-Up window on the Agents Computer if using the Event Management Software



EMS Unit Location Information



Enter in the most accurate Long and Lat of this specific CB unit. This will pop up a Bing Satellite map on the Agents Computer if using the Event Management Software. Then set your pin location for the unit. You can also enter a location in the “Find” box or use the satellite map to navigate and set your pin location for this unit.

Detailed Unit Location – you can select a custom map to place the CB unit onto, that will Pop-Up a window on the Agents Computer if using the Event Management Software.

Location Description / Notes – Custom Detailed CB Unit location info that will Pop-Up a window on the Agents Computer if using the Event Management Software.

Device Camera URL's

Camera 1 & Camera 2 – You can enter up to 2 camera streams to tap into, that will display in the Pop-Up a window on the Agents Computer if using the Event Management Software

Unit Address Info

Address Info that will appear in the Pop-Up window on the Agents Computer if using the Event Management Software

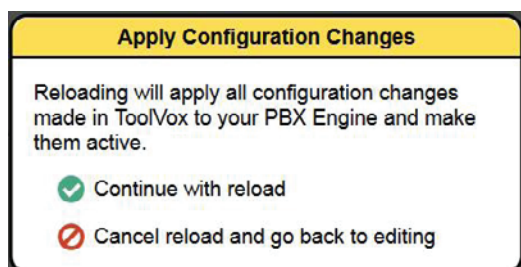
Push “Finish” when done

Finish

Push “Apply Configuration Changes”

Apply Configuration Changes

Push “Continue with reload”





If you have UPD (Unit Programming and Diagnostics) then you can click “Program Extension” to have ToolVox call out to the Unit and program it, provided the ToolVox and Phone lines are all built.



You may also now copy the Code Blue extension you just built to save time. If an analog unit you will have to either change the FXS port or the Unit number it calls out to, if off system. If you have EMS you will also need to change that info.

IA500 Model

Device Options - FXS Analog Extension type

This device uses zap technology.

Channel (FXS Port)	<input type="text"/>
context	from-internal
immediate	no
signalling	fxo_ks
echocancel	yes
echocancelwhenbridged	no
echotraining	100
busydetect	no
busycount	7
callprogress	no

Enter in the FXS Port number from Dahdi that you have cross connected the Analog Code Blue Phone to. Do not duplicate this number with another Code Blue Device.

Every other field in the Device Options Section for an FXS analog unit leave as default.

Device Options - Off System Unit

This device uses custom technology.

Unit Phone Number

Enter in the actual phone number ToolVox needs to dial to reach this unit.

Example: 916163928296 or 6163928296 or 4378

This may or may not be the same number you assigned it as an extension on the ToolVox system.



General Options

Programming Password	<input type="text" value="2258"/>
Off Hook Time	<input type="text" value="10"/> minutes
Ring Time	<input type="text" value="30"/> seconds
Cycle Count	<input type="text" value="2"/> ▾
Auxiliary Output Closure Time	<input type="text" value="00"/>

Programming Password – The password used to access programming mode(2) on initial calls into the unit.

Off Hook Time – Maximum conversation time in minutes before CB phone hangs up.

Ring Time – The amount of time the phone will try a number before resetting and dialing the next number 00-60.

Cycle Count – Number of cycles the CB phone will cycle through the above Numbers if a busy tone is encountered

Auxiliary Output Closure Time – The default is for the duration of the call. Enter 01-99 seconds to allow activation during a call by pressing the 6 key on the called party's keypad

Phone Numbers

Phone Number 1	Red "Help" Button ▾	<input type="text"/>
Phone Number 2	Red "Help" Button ▾	<input type="text"/>
Phone Number 3	Red "Help" Button ▾	<input type="text"/>
Phone Number 4	Red "Help" Button ▾	<input type="text"/>
Phone Number 5	Red "Help" Button ▾	<input type="text"/>
Phone Number 6	Red "Help" Button ▾	<input type="text"/>

Enter in however many phone numbers you wish the CB phone to call. If upon encountering a busy line it will roll to the 2nd number automatically. By Default the CB phone is set to roll through the numbers twice. This can be controlled with the Call Cycle count option above. You can program up to 6 numbers for the Red Help button or a combination of 6 numbers for the Red Help and Black Info button if you have a double button phone.

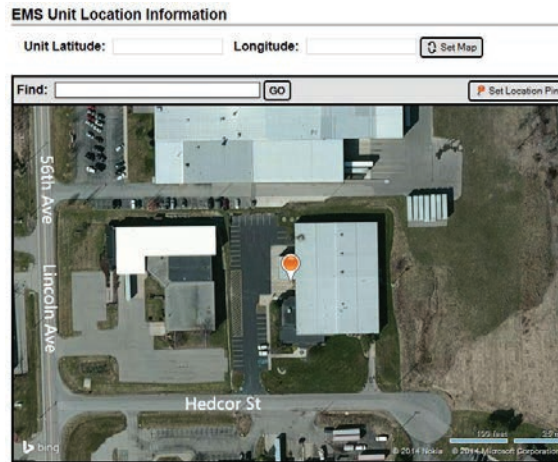
In-Call Commands

#	Command Text	DTMF Tone
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>

This is used to display the In-Call Commands in the Pop-Up window on the Agents Computer if using the Event Management Software.



EMS Unit Location Information



Enter in the most accurate Long and Lat of this specific CB unit. This will pop up a Bing Satellite map on the Agents Computer if using the Event Management Software. Then set your pin location for the unit. You can also enter a location in the “Find” box or use the satellite map to navigate and set your pin location for this unit.

Detailed Unit Location – you can select a custom map to place the CB unit onto, that will Pop-Up a window on the Agents Computer if using the Event Management Software.

Location Description / Notes – Custom Detailed CB Unit location info that will Pop-Up a window on the Agents Computer if using the Event Management Software.

Device Camera URL's

Camera 1 & Camera 2 – You can enter up to 2 camera streams to tap into, that will display in the Pop-Up a window on the Agents Computer if using the Event Management Software

Unit Address Info

Address Info that will appear in the Pop-Up window on the Agents Computer if using the Event Management Software

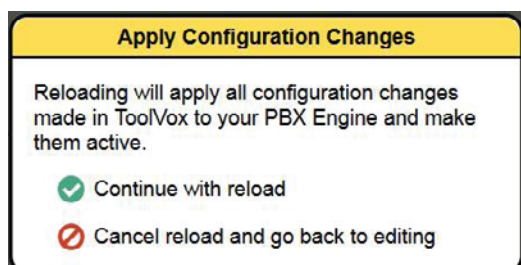
Push “Finish” when done

Finish

Push “Apply Configuration Changes”

Apply Configuration Changes

Push “Continue with reload”





If you have UPD (Unit Programming and Diagnostics) then you can click “Program Extension” to have ToolVox call out to the Unit and program it, provided the ToolVox and Phone lines are all built.



You may also now copy the Code Blue extension you just built to save time. If an analog unit you will have to either change the FXS port or the Unit number it calls out to, if off system. If you have EMS you will also need to change that info.

IA4100 Model

Device Options - FXS Analog Extension type

This device uses zap technology.

Channel (FXS Port)	<input type="text"/>
context	<input type="text" value="from-internal"/>
immediate	<input type="text" value="no"/>
signalling	<input type="text" value="fxo_ks"/>
echocancel	<input type="text" value="yes"/>
echocancelwhenbridged	<input type="text" value="no"/>
echotraining	<input type="text" value="100"/>
busydetect	<input type="text" value="no"/>
busycount	<input type="text" value="7"/>
callprogress	<input type="text" value="no"/>

Enter in the FXS Port number from Dahdi that you have cross connected the Analog Code Blue Phone to. Do not duplicate this number with another Code Blue Device.

Every other field in the Device Options FXS analog Extension type Section leave as default.

Device Options - Off System Unit

This device uses custom technology.

Unit Phone Number

Enter in the actual phone number ToolVox needs to dial to reach this unit.

Example: 916163928296 or 6163928296 or 4378

This may or may not be the same number you assigned it as an extension on the ToolVox system

Firmware	
Revision Level	2

After running a test to the phone, the ToolVox will sense whether it is revision level 1 or 2. This makes certain fields available or not.



Phone Numbers

Phone #1	<input type="text"/>
Phone #2	<input type="text"/>
Phone #3	<input type="text"/>
Phone #4	<input type="text"/>
Phone #5	<input type="text"/>
Phone #6	<input type="text"/>
Phone #7	<input type="text"/>
Phone #8	<input type="text"/>
Phone #9	<input type="text"/>

You can enter in up to 9 Phone numbers into these memory slots. They will be referenced further down in the configuration.

Outputs

Output #1 Active Time	<input type="text" value="91"/>
Output #2 Active Time	<input type="text" value="01"/>
Output #3 Active Time	<input type="text" value="01"/>

Output #1 Active Time – 00=Disabled, 01-60=1-60 seconds, 61-90=1-30 minutes, 91=till end of call, 92=trigger on input 2.

Output #2 Active Time – 00=Disabled, 01-60=1-60 seconds, 61-90=1-30 minutes, 91=till end of call, 92=trigger on input 2.

Output #3 Active Time – 00=Disabled, 01-60=1-60 seconds, 61-90=1-30 minutes, 91=till end of call, 92=trigger on input 2.

Recordings

Recording #1	<input type="text" value="None"/>
Recording #2	<input type="text" value="None"/>
Recording #3	<input type="text" value="None"/>
Recording #4	<input type="text" value="None"/>
Recording #5	<input type="text" value="None"/>
Recording #6	<input type="text" value="None"/>
Recording #7	<input type="text" value="None"/>
Recording #8	<input type="text" value="None"/>
Recording #9	<input type="text" value="None"/>

If you wish to use messages you can record them in System Recordings and reference them here. You have 9 memory slots and these will be called upon further down in the configuration.



Buttons and Inputs

Button 1 – this is the Red button on your CB phone. By default it will try numbers in memory slots 1,2, and 3 from above. It will also play recording 1 from above and activate Outputs 1 and 3 which are normally open contacts. The Call Cycle count is set for 2 by default, so for example if you set Phone Numbers as 11 it would call Phone Number in memory slot 1 Four times if it encountered a busy signal.

Button 2 – this is the Black button on your CB phone. Choose 0 as the phone number if your CB phone has a key pad. This will provide dial tone when the black button is pushed so the keypad can be used. If there is no key pad present then you can enter a Phone Number slot to have Button 2 place a call.

Button 3,4 – If you have a CB phone with a 3rd and 4th button you can program them here.

Input #1,#2 – select which button you want the input to mimic

Loss of AC Power – Enter the phone number memory slot 1-9 and outputs that you want the unit to dial should there be a loss of AC power. Enter the recordings 1-9 that the unit should play when the call is answered.

Low Battery - Enter the phone number memory slot 1-9 and outputs that you want the unit to dial should there be a low battery condition (less than 11.7 VDC). Enter the recordings 1-9 that the unit should play when the call is answered.

AMP SPKR Fault - Enter the phone number memory slot 1-9 and outputs that you want the unit to dial should there be an AMP/PAS fault. Enter the recordings 1-9 that the unit should play when the call is answered.

Call Properties

<u>Wait For Dial Tone</u>	<input type="text" value="05"/>
<u>Call Progress Detection Delay</u>	<input type="text" value="20"/>
<u>Wait For Answer</u>	<input type="text" value="30"/>
<u>Call Connected</u>	<input type="text" value="0"/>
<u>Call Loop Cycles</u>	<input type="text" value="2"/>
<u>Duplex Operation</u>	<input type="radio"/> Full <input checked="" type="radio"/> Half
<u>Full Duplex Noise Cancellation</u>	<input type="text" value="Low"/>
<u>Answer Message Repeat</u>	<input checked="" type="radio"/> No <input type="radio"/> Yes
<u>Acknowledge Beep Delay</u>	<input type="text" value="15"/>
<u>Call In Answer Mode</u>	<input type="text" value="Two Way Audio"/>

Wait For Dial Tone – 00=ring down/Hot line, 01 to 99 =1-99 seconds. If dial tone is not detected in this time the phone will hang up.

Call Progress Detection Delay – 1 to 99 is 1-99 seconds. The time that the phone will wait to hear progress tones after dialing.



Wait for Answer -

The amount of time the phone will try a number before resetting and dialing the next number 00-99. Timer begins at button press.

Call Connected –

0 or 1, 0=when voice or DTMF is detected by the CB phone. 1=call is assumed connected immediately and will not retry. (Non-ADA)

Call Loop Cycles –

Number of cycles the CB phone will cycle through the above Numbers if a busy tone is encountered.

Duplex Operation –

Audio operation of the CB phone. Half or Full. Half is generally much better in most situations. In very load environments Full may be necessary so the mic and speaker are both on at the same time.

Full Duplex Noise Cancellation –

If you use Full Duplex then you can increase Noise cancellation but may suffer some audio degradation.

Answer Message Repeat –

Enabling will force messages after the guard answers to repeat until the in-call command 33 is sent to the unit.

Acknowledge Beep Delay – The amount of time the phone will wait to play acknowledgment tones. Designated value * 20 = time in milliseconds. Example Value 15=300ms.

Call In Answer Mode – In two way Audio the unit will answer and immediately go into 2 way talk mode. In 2 way Audio – Password required, the unit will prompt the caller for a password before entering 2 way talk mode.

Miscellaneous

Miscellaneous	
DTMF On Time	<input type="text" value="7"/>
DTMF Off Time	<input type="text" value="7"/>
DTMF Dialing Volume	<input type="text" value="5"/>
Recording Playback Level	<input type="text" value="5"/>
Answer Ring Count	<input type="text" value="0"/>
Ring-In Unit Speaker	<input checked="" type="radio"/> No <input type="radio"/> Yes
Enable Mass Notification System	<input checked="" type="radio"/> No <input type="radio"/> Yes
Mass Notification Outputs:	Mass Notification Recordings:
<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3	<input type="text"/>
Disable Battery Check	<input checked="" type="radio"/> No <input type="radio"/> Yes

DTMF On Time – DTMF tone duration: 1 to 3 = 100 to 200ms, 4 to 9 = 40ms to 90ms.

DTMF Off Time – Silence between DTMF tone duration: 1 to 3 = 100 to 200ms, 4 to 9 = 40ms to 90ms.



DTMF Dialing Volume – Sets the volume of the DTMF tones during the dialing sequence

Recording Playback level – Sets the volume level of the recordings played back out of the unit and to the guard.

Answer Ring count – Number of Rings before the unit will answer

Ring-In Unit Speaker – Enable to hear incoming call ring out of the unit speaker

Enable Mass Notification System – Enabling will force the IA4100 to answer incoming calls and pass the audio to the amp/speaker array.

Mass Notification Outputs - If desired select 1 of the Auxiliary Outputs and a recording to play from one of the recording memory slots above.

Disable Battery Check - Yes - Do not check the battery. No - Check battery and call number set above in “Low Battery” Section.

Hang up Methods

Hangup Methods/Ring Detection	
Wink Timing	2
Revert To Dial Tone	00 seconds
Silent Time Out	0
Reorder/Repeating Tones	00 cycles
Call Time Out	10 minutes
Wink Voltage Minimum	0
Minimum Ring Voltage Detection Threshold	0
Maximum Ring Frequency	0

Wink Timing – 0=disabled, 1-9 = 100ms to 900ms. Length of the wink signal coming from the connected phone line.

Revert to dial tone – 00=disabled, 01-99 1 to 99 seconds. Continuous sound for this period of time will cause the unit to hang up.

Silent Time Out – 0 to 3, 0=disabled, 1=30 sec, 2=60 sec, 3=90 sec. Silence for this period of time will cause the unit to hang up.

Reorder/Repeating Tones – 00=disabled, 01 to 99= 1 to 99 cycles. This is the number of repeating cycles that will cause the unit to hang up.

Call Time Out – 00=disabled, 01-99 = 1 to 99 minutes. DTMF tones BBBBBB will play to both parties during a call notifying them 30 seconds prior to call disconnect. At this time the call can be extended by entering the IN call command 31. Once the timer has expired, if command 31 is not entered, the unit will hang up.

Wink Voltage Minimum – Minimum voltage change to interpret as a WINK. 0=5V thru 9=14V.

Minimum Ring Voltage Detection – Threshold - 0=13 Vrms, 1=19 Vrms, 2=40 Vrms.

Maximum Ring Frequency – 0=75 Hz, 1=50 Hz, 2=35 Hz.



Advanced Programming Passcode

Audio Passcode

Pass Codes

Advanced Programming Passcode – 2583 is the default for entering into programming mode. You can change it.

Audio Passcode – default is blank. You can add it if necessary.

In-Call Commands

#	Command Text	DTMF Tone
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>

This is used to display the In-Call Commands in the Pop-Up window on the Agents Computer if using the Event Management Software

EMS Unit Location Information

EMS Unit Location Information

Unit Latitude: Longitude:

Find:



Enter in the most accurate Long and Lat of this specific CB unit. This will pop up a Bing Satellite map on the Agents Computer if using the Event Management Software. Then set your pin location for the unit. You can also enter a location in the “Find” box or use the satellite map to navigate and set your pin location for this unit.

Detailed Unit Location – you can select a custom map to place the CB unit onto, that will Pop-Up a window on the Agents Computer if using the Event Management Software.

Location Description / Notes – Custom Detailed CB Unit location info that will Pop-Up a window on the Agents Computer if using the Event Management Software.

Device Camera URL's

Camera 1 & Camera 2 – You can enter up to 2 camera streams to tap into, that will display in the

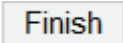


Pop-Up a window on the Agents Computer if using the Event Management Software

Unit Address Info

Address Info that will appear in the Pop-Up window on the Agents Computer if using the Event Management Software

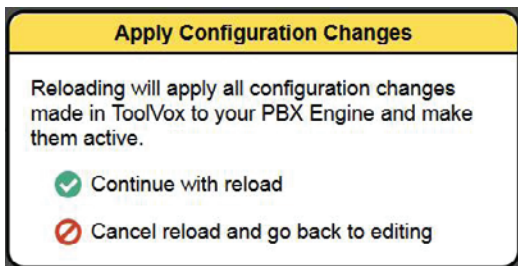
Push “Finish” when done



Push “Apply Configuration Changes”



Push “Continue with reload”



If you have UPD (Unit Programming and Diagnostics) then you can click “Program Extension” to have ToolVox call out to the Unit and program it, provided the ToolVox and Phone lines are all built.



You may also now copy the Code Blue extension you just built to save time. If an analog unit you will have to either change the FXS port or the Unit number it calls out to, if off system. If you have EMS you will also need to change that info.

IP1500/2500 or IP5000 Models

Device Options

This device uses sip technology.

secret	cbUnit
dtmfmode	inband
canreinvite	no
context	from-internal
host	dynamic
type	friend
nat	yes
port	5060
qualify	yes

Other than the secret please do not change any of these settings. The secret listed is the default and is set in the IP1500/2500/5000 phone to match by default. You can change it if necessary.



Administration

Current Username	<input type="text" value="admin"/>
Current Password	<input type="text" value="admin"/>
New Username	<input type="text"/>
New Password	<input type="text"/>

You can change the default username & password of the IP1500/2500/5000 phone if desired. This is the same username and password for both web and telnet.

Network - Dynamic IP Default Setting

Host	<input type="text"/>
Domain	<input type="text"/>
Connection Type	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP
MAC Address	<input type="text"/>
IP Address	<i>Unit IP address is unknown, run IP Unit Scan from UPD Administration</i>

Network - Static IP

Host	<input type="text"/>
Domain	<input type="text"/>
Connection Type	<input type="radio"/> Dynamic IP <input checked="" type="radio"/> Static IP
<hr/>	
Static IP Address	
Address	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
Mask	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
Default Router	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
DNS Primary	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
DNS Secondary	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
DNS Tertiary	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
MAC Address	<input type="text"/>
IP Address	<i>Unit IP address is unknown; run IP Unit Scan from UPD Administration</i>

Host – DNS Host Name (Optional)

Domain – DNS Domain Name (Optional)

Connection Type – Dynamic or Static. The IP1500/2500/5000 phone by default is set for Dynamic.

Address – Static IP Address to assign to the CB Phone

Mask – Network Mask defining the network scope

Default Router – IP address of Default Router if routing traffic off the subnet

DNS Primary, Secondary, Tertiary – IP Address of DNS Servers if desired but not necessary

MAC Address – Required – Mac Address of IP1500/2500/5000 Phone can be found on rear of the phone or by browsing to the phone and looking under Administration.

IP Address – If you have the UPD software package, after you provision the phone in ToolVox you can run Unit Scan from UPD Administration. After 2-3 minutes you can Program the Phone from ToolVox.



VLAN – Enable or Disable VLAN Support

ID - VLAN Identifier 1-4094, 0 indicates this frame does not belong to any VLAN

User Priority – Priority level (PCP). Higher numbers will tag frames will tag frames with higher priority.

Account 1

Registration Lifetime

Keep-Alive

STUN Disabled Enabled

DTMF threshold dB

VLAN User Priorities

SIP

RTP Audio

Registration Lifetime – in seconds. If IP1500/2500/5000 phone is losing registration to ToolVox but is still accessible on the network consider lowering down to 60 seconds.

Keep-Alive – Keep Alive method to use. Whether or not to send SIP Keep Alive.

STUN – Enable or disable STUN for NAT traversal. Set the STUN server in advanced settings.

DTMF Threshold – Level to recognize DTMF tones. Adjust to resolve issues with inadvertent in-call command activation.

SIP – VLAN priority for SIP traffic. Default is 0

RTP Audio - VLAN priority for RTP audio traffic. Default is 6

Account 2

You can configure a 2nd Account on the same phone.



Media

RTP Configuration

Port Range to

Codec Selection

<p>Available</p> <ul style="list-style-type: none"> G.711 uLaw G.711 aLaw G.726 (16kbps) G.726 (24kbps) G.726 fixed payload G.726 (40kbps) G.722 HD DVI4 Narrowband DVI4 HD Linear PCM 	<input type="button" value="➤"/> <input type="button" value="➤"/>	<p>Preferred</p> <ul style="list-style-type: none"> G.711 uLaw G.711 aLaw G.726 fixed payload G.726 (16kbps) G.726 (40kbps)
---	--	---

Codec – this is the preferred codecs ToolVox will communicate with to the IP5000 phones.

Advanced Settings

STUN

Server

Port

Server – STUN server address for NAT traversal. STUN must be enabled on each account that uses it.

Port – STUN Server port for NAT traversal. This is an advanced setting; it should typically be left at the default of 3478

Date & Time

Daylight Savings Disabled Enabled

Time Zone

NTP Server

Enabled Disabled Enabled

Server Address

Daylight Savings – enable or disable

Time Zone – Choose your time zone

Enabled (NTP) – enable or disable NTP service

Server Address – by default your IP1500/2500/5000 will pull NTP from ToolVox and you can set the ToolVox to pull NTP time from your server or from an external source.



Numbers

Number	Description
<input type="text" value="Account 1"/>	<input type="text"/>

Enter in the Phone Numbers you wish the IP1500/2500/5000 phone to call upon button press.

Enter Number and Description then press the green + icon. You may enter in multiple numbers to have the phone roll to more numbers.

Recordings

Recording	Description
<input type="text" value="CB8LocMsg.wav"/>	<input type="text"/>

Enter in Recordings and descriptions here then press the green + icon to submit it. You can enter multiple entries.

Hardware Configuration

Interface	
Button Count	<input checked="" type="radio"/> 1 Button <input type="radio"/> 2 Buttons <input type="radio"/> 3 Buttons <input type="radio"/> 4 Buttons
Keypad	<input type="radio"/> Available <input checked="" type="radio"/> Unavailable
Public Address	<input type="radio"/> Available <input checked="" type="radio"/> Unavailable
Public Address Gain	<input type="text" value="0"/>
Power Sources	
A/C	<input type="radio"/> Available <input checked="" type="radio"/> Unavailable
D/C	<input type="radio"/> Available <input checked="" type="radio"/> Unavailable
PoE	<input type="radio"/> Available <input checked="" type="radio"/> Unavailable
Auxiliary I/O	
Aux Input 1	<input checked="" type="radio"/> Available <input type="radio"/> Unavailable
Aux Output 1	<input checked="" type="radio"/> Available <input type="radio"/> Unavailable
Aux Output 2	<input checked="" type="radio"/> Available <input type="radio"/> Unavailable

Button Count – The number of buttons on the face of the IP5000

Keypad – Does the IP5000 have a keypad on the faceplate

Public Address – Whether the phone has a public address system connected to it - only applies to the IP5000 model.

Public Address Gain – gain in dB for the public address output - only applies to the IP5000 model.

A/C – specify if available or not - only applies to the IP5000 model.

D/C – specify if available or not - only applies to the IP5000 model.

PoE – specify if available or not.

Aux Input 1 – specify if available or not. - only applies to the IP5000 model.

Aux Output 1 – specify if available or not.

Aux Output 2 – specify if available or not . - only applies to the IP5000 model.



General Settings

Incoming Calls	
Answer In	Immediately ▾
Public Address	<input checked="" type="radio"/> Disabled <input type="radio"/> Always route incoming calls to public address
Aux Output 1	<input checked="" type="radio"/> Disabled <input type="radio"/> Enable while incoming calls are active
Aux Output 2	<input checked="" type="radio"/> Disabled <input type="radio"/> Enable while incoming calls are active
Location Message	
Location Recording	None Selected ▾

Answer In – Specify how many rings the IP1500/2500/5000 should receive before answering an incoming call.

Public Address – Route all incoming calls to the Public Address output - only applies to the IP5000 model.

Aux Output 1 – Enable auxiliary output 1 when incoming calls are active.

Aux Output 2 – Enable auxiliary output 2 when incoming calls are active. - only applies to the IP5000 model.

Location Recording – Specify a location recording that will be played for in-call command 1.

Action Scripts

Script for:	Button #1 Pressed ▾
<input type="radio"/> Do Nothing	
<input type="button" value="Add Action"/>	<input type="button" value="Save Script"/>

This is the section to specify the action the IP5000 phone does upon button press. Here is a sample of a typical setup for Button 1.

Script for:	Button #1 Pressed ▾
<input checked="" type="radio"/> Control AUX Output + - ✖	
<input type="radio"/> Output Number:	1 : AUX One ▾
<input type="radio"/> Set to:	Enabled ▾
<input type="radio"/> Duration:	Until Disabled ▾
<input checked="" type="radio"/> Place Call + - ✖	
<input type="radio"/> Call	6163928296 : Code Blue ▾
<input type="radio"/> If not answered, then	Go to next step ▾
<input type="radio"/> Dialing/Answer timeout:	60 seconds
<input type="radio"/> Maximum call duration:	600 seconds
<input type="radio"/> While Dialing:	Standard Ringback ▾
<input type="radio"/> When Answered:	Normal Two-Way Conversation ▾
<input type="radio"/> In Call Commands:	Enabled ▾
<input checked="" type="radio"/> Control AUX Output + - ✖	
<input type="radio"/> Output Number:	1 : AUX One ▾
<input type="radio"/> Set to:	Disabled ▾
<input type="button" value="Add Action"/>	<input type="button" value="Save Script"/>



The above action takes place in order from top to bottom upon a Button 1 press. The above will activate Aux Output 1 turning a strobe light on, then place a call. It will try calling the first phone number for 60 seconds if no answer. The max call duration is set at 600 seconds. During dialing the person at the CB phone will hear standard ring back. Upon the call being answered Normal 2-way conversation will be set up. In Call commands (specified in the IP1500/2500/5000 Manual) will be allowed to be in use. Upon hang-up Aux Output 1 will be disabled stopping the combo/beacon light from strobing.

There are many options you can use in the Actions Script area. Actions Scripts are covered in more detail in the IP1500/2500 or IP5000 Administrators Guides.

Diagnostic Settings

SNMP	
SNMP Traps	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
SNMP Server	ToolVox IP Address
SNMP Server Port	162
Power Supply Failure Timeout	
12-24 Volt A/C or D/C	900
12 Volt D/C Battery	900
PoE Failure Timeout	900
Others	
Microphone Test	Disabled
Microphone Test Hour	12 AM
Microphone Test Days	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat
Microphone Test Max Beeps	5
Microphone Test Volume	Soft

SNMP Traps – enabled by default to send traps for UPD monitoring of the IP5000 phone by ToolVox

SNMP Server – by default the ToolVox IP Address

SNMP Server Port – 62 default port

12-24 Volt A/C or D/C - timeout in seconds to notify before a power failure on the main line is reported - only applies to IP5000 model.

12 Volt D/C Battery – imeout in seconds before a power failure on the battery line is reported - only applies to IP5000 model.

PoE Failure Timeout – timeout in seconds before a PoE failure is reported.

Microphone Test – frequency to test the IP1500/2500/5000 Microphone

Microphone Test Hour – What Hour to test the microphone at. Only applies to Daily and Weekly.

Microphone Test Days – Which days of the week to test the microphone on. Only applies to Weekly.

Microphone Test Max Beeps – Maximum number of beeps used for the microphone test.

Microphone Test Volume - Microphone setting for the microphone test



In-Call Commands

#	Command Text	DTMF Tone
1		
2		
3		
4		
5		
6		
7		
8		

This is used to display the In-Call Commands in the Pop-Up window on the Agents Computer if using the Event Management Software.

EMS Unit Location Information

Unit Latitude: Longitude:

Find:

Enter in the most accurate Long and Lat of this specific CB unit. This will pop up a Bing Satellite map on the Agents Computer if using the Event Management Software. Then set your pin location for the unit. You can also enter a location in the "Find" box.

Detailed Unit Location – you can select a custom map to place the CB unit onto, that will Pop-Up a window on the Agents Computer if using the Event Management Software.

Location Description / Notes – Custom Detailed CB Unit location info that will Pop-Up a window on the Agents Computer if using the Event Management Software.

Device Camera URL's

Camera 1 & Camera 2 – You can enter up to 2 camera streams to tap into, that will display in the Pop-Up a window on the Agents Computer if using the Event Management Software

Unit Address Info

Address Info that will appear in the Pop-Up window on the Agents Computer if using the Event Management Software

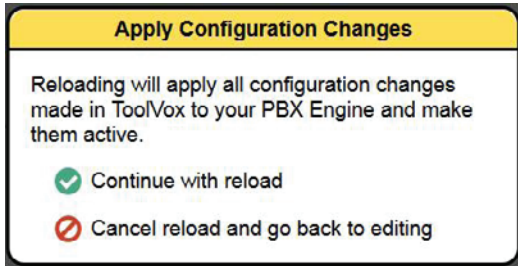
Push "Finish" when done



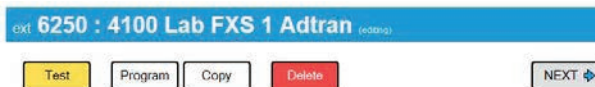
Push "Apply Configuration Changes"



Push "Continue with reload"



If you have UPD (Unit Programming and Diagnostics) then you can click "Program Extension" to have ToolVox communicate out to the Unit and program it, provided the ToolVox is provisioned. Make sure UPD administration is configured and Unit scan has been run since building your Code Blue Devices.



You may also now copy the Code Blue extension you just built to save time. You will have to enter in a unique Mac Address and Extension number as well. If you have EMS you will also need to change that info.



9 Configuring Business Phones

The screenshot shows the ToolVox X3 web interface. At the top left is the 'TOOLVOX' logo. To its right are navigation tabs: 'Admin', 'CDR Reports', 'EMS Records', 'IP Info', and 'Help'. Below the logo is a sidebar menu with 'Setup' and 'Tools' tabs. Under 'Tools', 'Business Phones' is selected. The main content area has a sub-header 'Add Extension' and a form with a 'Device' dropdown menu set to 'SIP Device' and a 'Submit' button.

Business Phones is the area you would build **non-Code Blue** devices into. For example: SIP, IAX2, Analog (FXS) or Virtual Extension. Note that the screens when adding a Business Phone look different then when editing an existing one.

Add Extension

User Extension: Number you wish to give this Phone that will be dialed.

Display Name: The Caller ID name for calls from this user will be set to this name. Only enter the name, not the number.

CID Num Alias: (Optional) The CID Number to use for internal calls, if different from the extension number. This is used to appear as a different user. A common example is a team of support people who would like their internal Caller ID to display the general support number (a ring group or queue). There will be no effect on external calls.

SIP Alias: (Optional) If you want to support direct sip dialing of users internally or through anonymous sip calls you can supply a friendly name that can be used in addition to the user's extension to call them.

Extension Options

Outbound CID: (Optional) Overrides the caller id when dialing out a trunk. Any setting here will override the common outbound caller id set in the Trunks admin. The format is "caller name" <#####>. Leave this field blank to disable the outbound Caller ID feature for this user.

Ring Time: (Optional) Number of seconds to ring the extension prior to going to voicemail. Default will use the value set in the General Setting. If no voicemail is configured this will be ignored.
Call Waiting: (Optional) Allows/Disallows call waiting on the extension.

Call Screening: (Optional) Call Screening requires external callers to say their name, which will be played back to the user and allow the user to accept or reject the call. Screening with memory only



verifies a caller for their caller-id once. Screening without memory always requires a caller to say their name. Either mode will always announce the caller based on the last introduction saved with that Caller ID. If any user on the system uses the memory option, when that user is called, the caller will be required to re-introduce themselves and all users on the system will have that new introduction associated with the caller's Caller Id.

Pinless Dialing: (Optional) enabling will allow the extension to bypass any pin codes normally required on outbound calls.

Emergency CID: (Optional) This Caller ID will always be set when dialing out an Outbound Route flagged as Emergency. The Emergency CID overrides all other Caller ID settings.

Assigned DID/CID (Optional)

DID Description: (Optional) A description for this DID, such as "Sales"

Add Inbound DID: (Optional) This is where you enter the Direct Inward Dial (DID) you'd like to reach this extension. The format should be: XXXXXXXXXX or XXXX or whatever Number you route into this Gateway if you want it to ring this Extension. If you do not enter a value here all calls to that DID will route to the inbound route setting for the trunk the call comes in on. Putting a value here automatically creates an Inbound Route. This can also be done in Inbound Routes.

Add Inbound CID: (Optional) Add a CID for more specific DID + CID routing. A DID must be specified in the above Add Inbound DID box. In addition to standard dial sequences, you can also put Private, Blocked, Unknown, Restricted, Anonymous and Unavailable in order to catch these special cases if the provider transmits them.

Device Options - FXS Extension

Enter the DAHDi channel that this extension will use. Go into DAHDi to see available FXS channels. Do not duplicate.

Device Options -SIP Extension

Secret: alpha numeric secret password you create. This must match what you provision in your SIP Device. This is the value used to authenticate the device to the system. This should not be the same as the device name or extension number.

Device Options -Custom Extension

This device uses custom technology.

dial

Utilized to dial out to a Custom Extension which is not directly attached to the ToolVox system. An example would be an offsite phone attached to a GSM cellular unit or analog line.



Language(Optional)

Language Code

This setting will cause all messages and voice mail prompts to utilize the language of choice if installed on the system.

Recording Options

Record Incoming
 Record Outgoing

This will allow the recording of incoming and outgoing calls. Values are: Never, On Demand, Always. **Always is Mandatory if using EMS ToolVox Software**

To save your settings click:

To apply the changes to the system click:

At the top of the screen.

Click - **Continue with reload** - to finish the changes otherwise click - **Cancel reload and go back to editing** - to cancel the changes and continue editing the extension.

Apply Configuration Changes

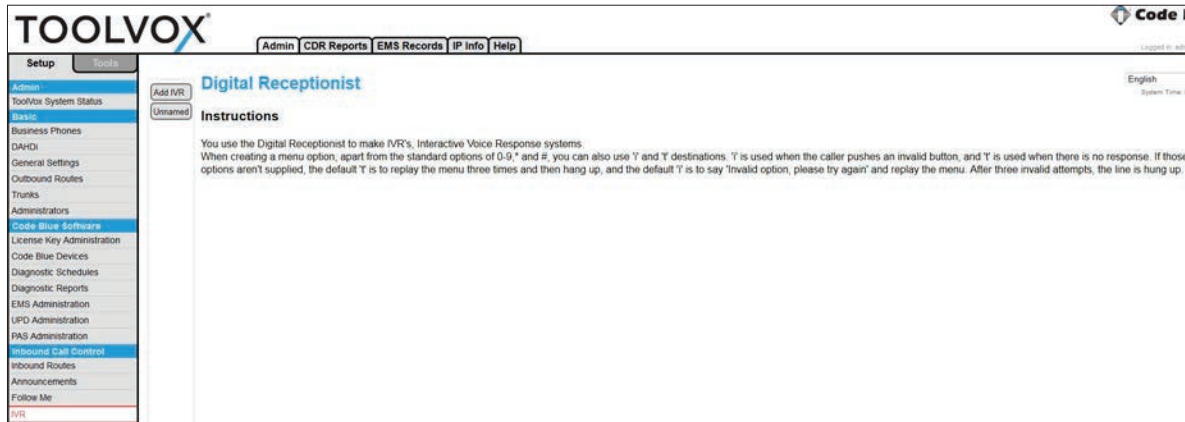
Reloading will apply all configuration changes made in ToolVox to your PBX Engine and make them active.

Continue with reload

Cancel reload and go back to editing



10 Configuring Digital Receptionist (IVR)



Much can be customized and configured with the IVR options. If you have your Inbound Route set up to point to the IVR your creating you simply just need to make sure “Enable Direct Dial” is checked. No announcements needed, recordings or any other settings. You will then be able to call into the ToolVox and be able to enter in the Extension Number of the Business Phone or Code Blue device you’re trying to reach. If using Blue Alert and want to route inbound calls select Misc Destinations below.



Edit Menu Unnamed

Save Delete Digital Receptionist Unnamed

Change Name	<input type="text" value="Unnamed"/>
Announcement	<input type="text" value="None"/>
Timeout	<input type="text" value="10"/>
Enable Directory	<input checked="" type="checkbox"/>
VM Return to IVR	<input type="checkbox"/>
Directory Context	<input type="text" value=""/>
Enable Direct Dial	<input checked="" type="checkbox"/>
Loop Before t-dest	<input type="checkbox"/>
Timeout Message	<input type="text" value="None"/>
Loop Before i-dest	<input type="checkbox"/>
Invalid Message	<input type="text" value="None"/>
Repeat Loops:	<input type="text" value="2"/>

Edit Menu

Change Name: This is the name of the IVR.

Announcement(Optional): Message to be played to the caller. To add additional recordings please use the “System Recordings” Menu

Timeout: The amount of time (in seconds) before the “t” option if specified is used.

Enable Directory(Optional): Let callers into the IVR dial # to access the directory

VM Return to IVR(Optional): If checked upon exiting voicemail a caller will be returned to this IVR if they got a user’s voicemail.

Directory Context(Optional): When # is selected, this is the voicemail directory context that is used

Enable Direct Dial: Let callers into the IVR dial an extension directly

Loop Before t-dest(Optional): If checked, and there is a “t” timeout destination defined below, the IVR will loop back to the beginning if no input is provided for the designated loop counts prior to going to the timeout “t” destination.

Timeout Message(Optional): If a timeout occurs and a message is selected, it will be played in place of the announcement message when looping back to the top of the IVR. It will not be played if the “t” destination is the next target.

Loop Before i-dest(Optional): If checked, and there is an “i” (invalid extension) destination defined below, the IVR will play invalid option and then loop back to the beginning for the designated loop counts prior to going to the invalid “i” destination.

Invalid Message(Optional): If an invalid extension is pressed and a message is selected it will be played in place of the announcement message.

Repeat Loops(Optional): The number of times we should loop when invalid input or no input has



been entered before going to the defined or default generated “i” or “t” options. If the “i” or “t” boxes are defined the above check boxes must be checked in order to loop.

Phonebook Directory: Phonebook Directory ▾
 Terminate Call: Hangup ▾
 Return to IVR Extensions: <6100> Test Lab Polycom ▾
 Ring Groups: rg EMS <6198> ▾
 Custom Contexts: Full Internal Access ▾
 Misc Destinations: Test Page ▾
 IVR: IVR ▾

Phonebook Directory: Phonebook Directory ▾
 Terminate Call: Hangup ▾
 Return to IVR Extensions: <6100> Test Lab Polycom ▾
 Ring Groups: rg EMS <6198> ▾
 Custom Contexts: Full Internal Access ▾
 Misc Destinations: Test Page ▾
 IVR: IVR ▾

Phonebook Directory: Phonebook Directory ▾
 Terminate Call: Hangup ▾
 Return to IVR Extensions: <6100> Test Lab Polycom ▾
 Ring Groups: rg EMS <6198> ▾
 Custom Contexts: Full Internal Access ▾
 Misc Destinations: Test Page ▾
 IVR: IVR ▾

These Destinations represent what to do if a particular key is pushed from the calling party’s keypad once into the IVR. If you’re just using the Direct Dial then nothing need be entered in this section since you can just enter in the extension number and will be transferred immediately. If using Blue Alert and are trying to reach a specific Misc Destination choose it here. This is useful if wanting a special pin code used to access certain page groups.

To save your settings click:



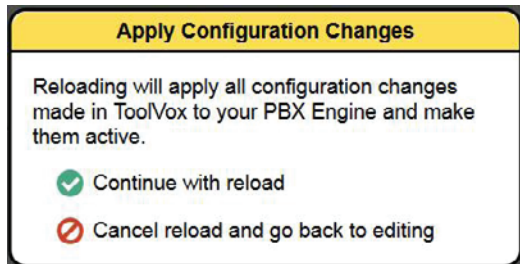
To apply the changes to the system click:





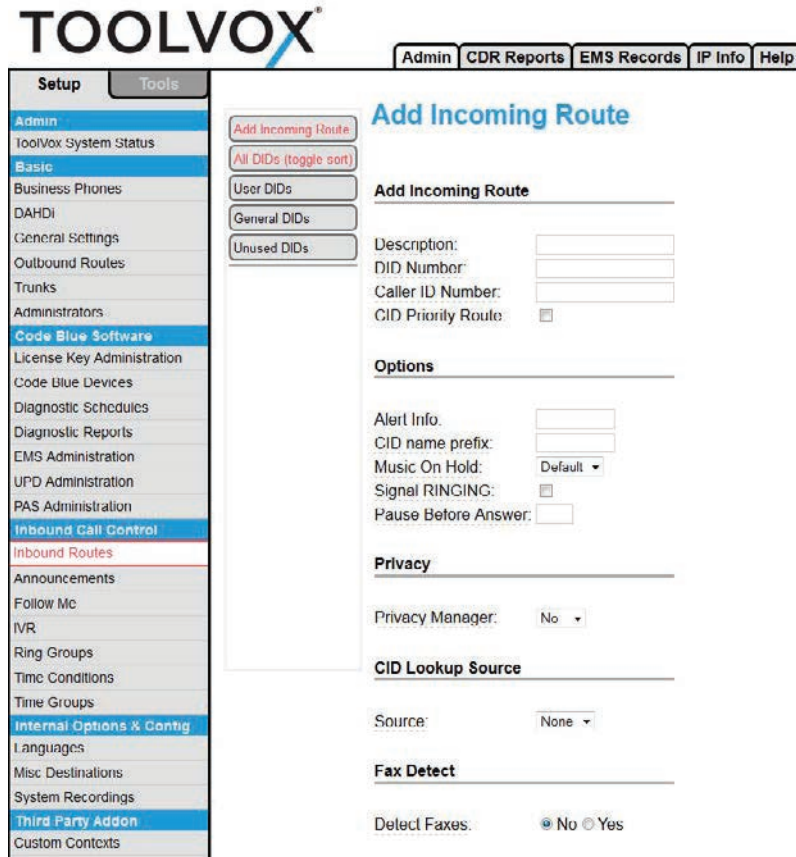
At the top of the screen.

Click - **Continue with reload** - to finish the changes otherwise click - **Cancel reload and go back to editing** - to cancel the changes and continue editing the extension.





11 Configuring Inbound Routes



If you need to call into ToolVox or Phones connected to the ToolVox you will need Inbound Routes configured to control call Routing. Reasons for needing this can include Manual programming of Analog phones through an IVR, Adjusting In-Call phone settings on phones like speaker and mic gain, or allowing only specific DID and CLID combinations into the system for making Blue Alert Pages. There is a lot of flexibility.

Add Incoming Route

Description: Provide a description name for this route to be refined by

DID Number(Optional): Define the expected DID Number if your trunk passes DID on incoming calls. Leave blank if you want to allow ALL DID's access. A pattern can also be entered (see Dial Patterns in the Trunks section to understand how to create a Dial Pattern).

Caller ID Number(Optional): Define the Caller ID Number to be matched on incoming calls. Leave this field blank to match a specific CLID Number to allow it or leave blank to allow ALL. You can also enter in a Dial Pattern (see trunks for instructions) or put in Private, Blocked, Unknown, Restricted, Anonymous, and Unavailable to match on, if the Telco transmits them.

CID Priority Route(Optional): This effects CID ONLY routes where no DID is specified. If checked calls with this CID will be routed to this route, even if there is a route to the DID that was called. Normal behavior is for the DID route to take the calls. If there is a specific DID/CID route for this CID, that route will still take the call when that DID is called.



Options

Alert Info(Optional): Alert_INFO can be used for distinctive ring with SIP devices.

CID name prefix(Optional): You can optionally prefix the Caller ID name i.e.: IF you prefix with “Sales” a call from John Doe would display as “Sales :John Doe” on the extensions that ring.

Music on Hold(Optional): Set the MoH class that will be used for calls that come in on this route. For example, choose a type appropriate for routes coming in from a country which may have announcements in their language.

Signal RINGING(Optional): Some devices or providers require RINGING to be sent before ANSWER. You’ll notice this happening if you can send calls directly to a phone, but if you send it to an IVR, it won’t connect the call.

Pause before Answer(Optional): An optional delay to wait before processing this route. Setting this value will delay the channel from answering the call. This may be handy if external fax equipment or security systems are installed in parallel and you would like them to be able to seize the line.

Privacy

Privacy Manager:

Privacy

Privacy Manager(Optional): If no Caller ID has been received, Privacy Manager will ask the caller to enter their phone number. If a user/extension has Call Screening enabled, the incoming caller will be prompted to say their name when the call reaches the user/extension.

Language

Language:

Language

Language(Optional): Allows you to set the language for this DID

Fax Detect

Detect Faxes: No Yes

Fax Detect

Detect Faxes(Optional): if set to yes it TV will try to determine if this is a fax call and route to the selected destination below.



CID Lookup Source

Source:

CID Lookup Source

Source(Optional): Sources can be added in Caller Name Lookup Sources Section

Set Destination

- Phonebook Directory:
- Terminate Call:
- Extensions:
- Ring Groups:
- Custom Contexts:
- Misc Destinations:
- IVR:

Set Destination

(Required)

Upon Match of DID and/or CLID, select in the ToolVox system where to have the call routed to.

To save your settings click:

To apply the changes to the system click:

At the top of the screen.

Click - **Continue with reload** - to finish the changes otherwise click - **Cancel reload and go back to editing** - to cancel the changes and continue editing the extension.

Apply Configuration Changes

Reloading will apply all configuration changes made in ToolVox to your PBX Engine and make them active.

- Continue with reload
- Cancel reload and go back to editing



12 Configuring System Recordings

TOOLVOX Admin CDR Reports EMS Records IP Info Help

System Recordings

Add Recording

Step 1: Record or upload

If you wish to make and verify recordings from your phone, please enter your extension number here:

Alternatively, upload a recording in any supported asterisk format. Note that if you're using wav, (eg, recorded with Microsoft Recorder) the file **must** be PCM Encoded, 16 Bits, at 8000Hz.

No file selected.

Step 2: Name

Name this Recording:

Click "SAVE" when you are satisfied with your recording

Recordings can be useful for pushing messages to your Phones. They can be created and can be done in 2 different ways. You can use a phone connected directly to ToolVox or by making the recording off system and loading it into ToolVox. Note that the format must be compatible though; PCM Encoded, 16 Bits at 8 MHz.

Add Recording

If using a phone to make the recording, enter in your extension number and hit "Go" Dial *77 on that phone and the system will prompt you on what to do.

After you hang up, name the recording and save it. It will appear on the right side of the screen and will be available throughout the ToolVox system for use.

If uploading a recording from your PC, browse to it and upload. Name the recording and save it. It will appear on the right side of the screen and will be available throughout the ToolVox system for use.



13 Configuring License Key Administration

TOOLVOX Admin CDR Reports EMS Records IP Info Help

Setup Tools

Software Licensing

Max Code Blue Units:	50
Max allowed EMS Users:	5
EMS Type:	EMS Advanced
UPD Enabled:	Yes
Blue Alert PAS Enabled:	Yes
Cepstral Voice:	Enabled
Blue Alert MNS Features:	core, desktop, email, feed, pas, signage, sms

System UUID: 7FF072EF-5045-5A3F-915A-5ADE6570529B

ToolVox ID: CADF-5AF2-6383

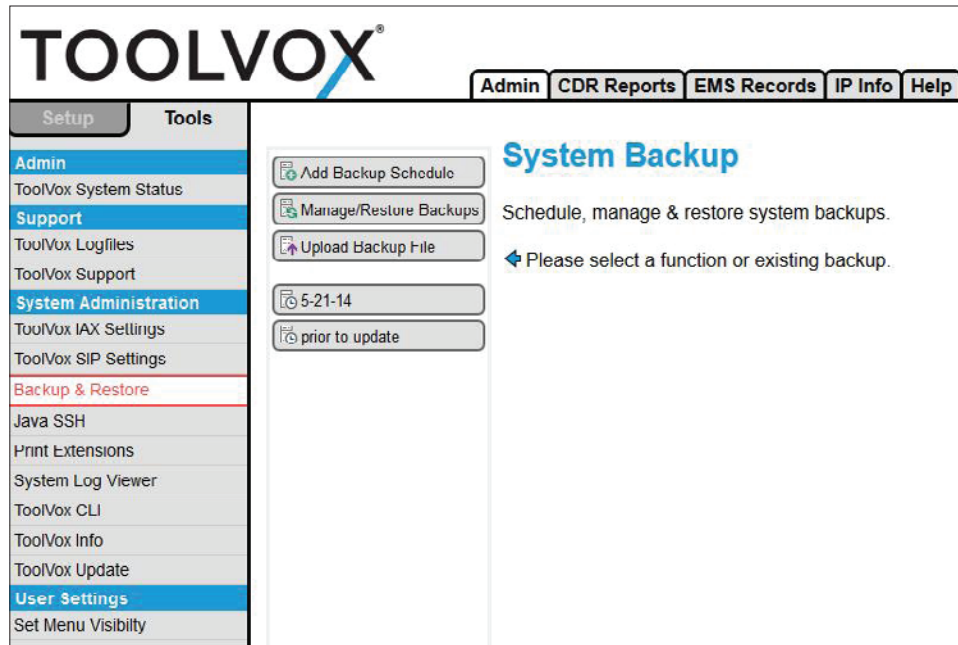
License (paste new license code here)

Software Licensing

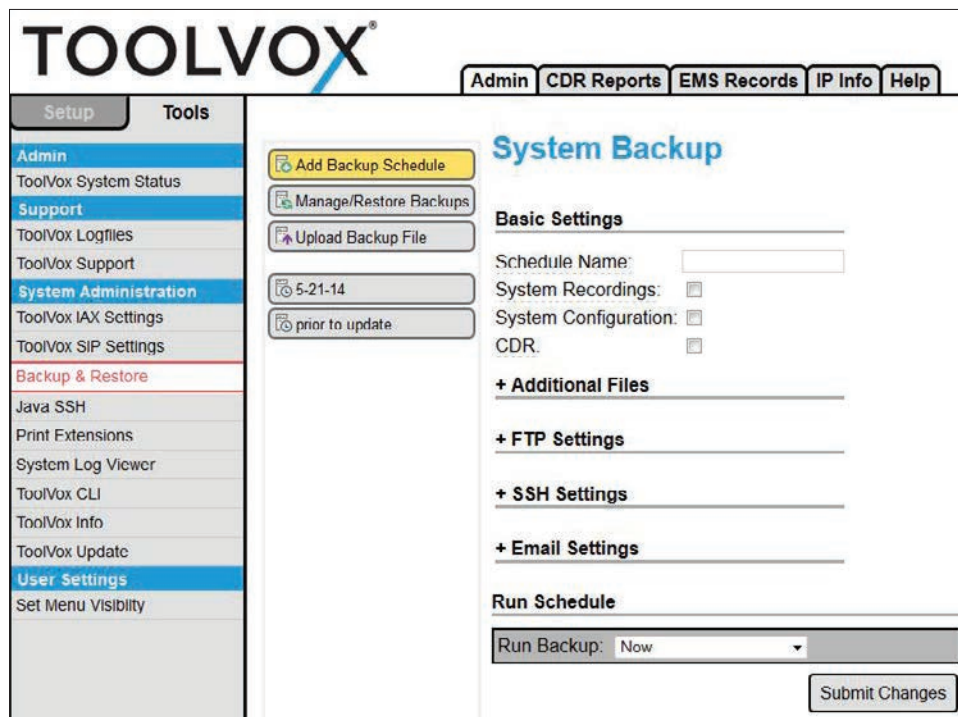
This screen lists what Your ToolVox is licensed for. If you notice any discrepancies with what you ordered please notify Code Blue Technical Services. Make note of your System UUID and ToolVox ID.



14 Configuring Backup & Restore



You can configure a regular backup schedule to ensure that you have a copy of your ToolVox configuration settings and CDR's. You can also restore a previous backup, in case of data loss or a major configuration fault. Backups are stored on the file system at /var/lib/asterisk/backups. You should make a point of making an offline copy of important backups.





Add Backup Schedule

Basic Settings

Create the Backup Set

At a minimum check the System Configuration box. If you utilize recordings in your ToolVox then also choose System Recordings. The other items are completely optional.

FTP & SSH Settings

If you have an FTP or SSH server on your network you can enter in it's settings here to have it automatically FTP or SSH the backup file off the ToolVox.

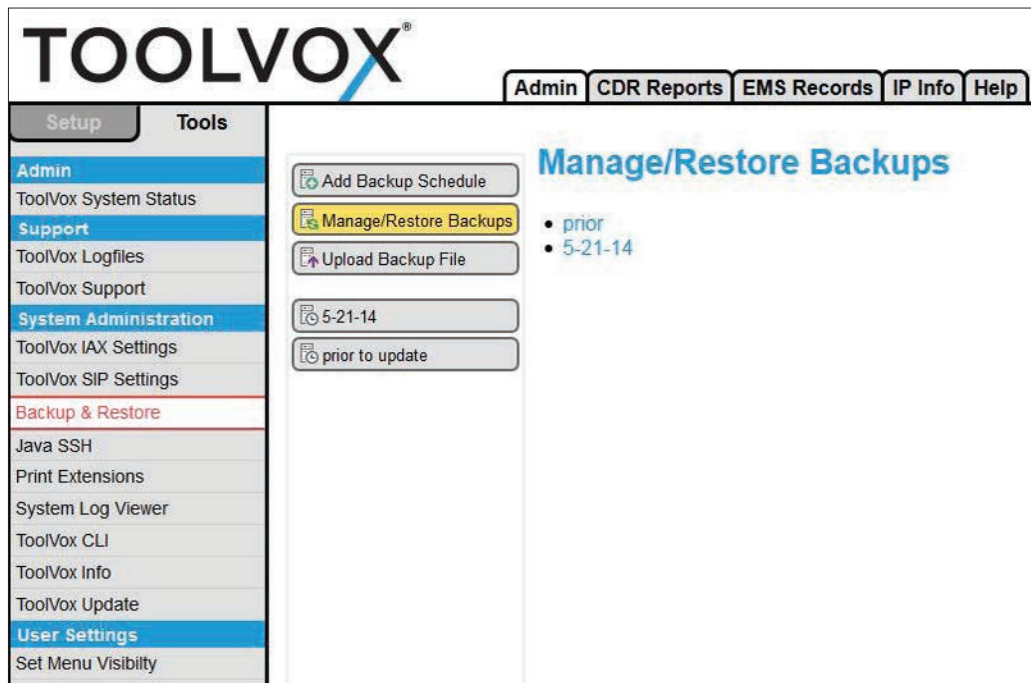
Email Settings

If email is configured on your ToolVox server you can choose to have the backup set emailed to the designated address.

Run Schedule

You can have it run "NOW" or set up a schedule using these options.

Manage/Restore Backups



When selecting Manage/Restore Backups you can see your backup set and restore from it. You will have the option of only restoring parts of your backup set or all. Click on your backup set while in this screen. You can click on "Download File Set" via your web browser to your computer. It's important to get your backup off the ToolVox in case it's needed.



15 Unit Programming and Diagnostics (UPD) Configuration and Operation

The screenshot displays the ToolVox X3 administrator interface. The top navigation bar includes 'Admin', 'CDR Reports', 'EMS Records', 'IP Info', and 'Help'. The left sidebar contains a menu with categories like 'Setup', 'Admin', 'Basic', 'Code Blue Software', and 'Inbound Call Control'. The main content area is titled 'Code Blue Devices' and features a search bar, a list of units, and a detailed view for extension 202: IP2501. The detailed view includes fields for 'Extension', 'Caller ID Display Name', 'Unit Info', and 'Assigned DID/CID'.

Unit Search:	
2009 : 4100 Guard Shack	202 : IP2501
203 : IP1500	300 : IP5000

Unit Last Edited:	
2009 : 4100 Guard Shack	202 : IP2501
203 : IP1500	300 : IP5000

Device Info	
Extension	202
Caller ID Display Name	IP2501

Unit Info	
Model	IP1500/2500
Device Connection Type	SIP Extension

Assigned DID/CID	
DID Description	
Add Inbound DID	
Outbound CID	

NOTE: The ToolVox® Media Gateway must be installed and configured before the UPD software can be configured. Onsite installation and remote support packages are available from your authorized Code Blue dealer.



UPD End User License Agreement

IMPORTANT – READ CAREFULLY. This is a legal agreement between you (either an individual or an entity), the end user, and Code Blue Corporation of Holland, Michigan. By opening the sealed CD-ROM packet(s) and installing or otherwise using the software, you agree to be bound by the terms of this End User License Agreement (EULA). If you do not agree to the terms of this Agreement, promptly return the disk package and accompanying items (including written materials, binders or other containers) to the place you obtained them.

1. **GRANT OF LICENSE.** This EULA permits you to use one copy of the Code Blue software product (“Software”) on any single computer, provided the software is in use on only one computer at any time. If you have multiple licenses for the software, then at any time you may have as many copies of the software in use as you have Licenses. The software is “in use” in a computer when it is loaded into the temporary memory (i.e., RAM) or is installed into the permanent memory (e.g. hard disk, CD-ROM or other storage device) of that computer. However, a copy installed on a network server for the sole purpose of distribution to other computers is not “in use.” If the anticipated number of users of the software will exceed the number of applicable Licenses, you must have a reasonable mechanism or process in place to assure that the number of persons using the software concurrently does not exceed the number of Licenses. If the software is permanently installed on the hard disk or other storage device of a computer (other than a network server), then the person authorized to use such computer also may use the software on a portable computer, laptop and home computer. If such person’s authorization to use such computer ceases for any reason (e.g. termination of employment), then such person’s authority to use the software on a portable computer, laptop and home computer shall cease.

2. **COPYRIGHT.** The software is owned by Code Blue Corporation or its suppliers and is protected by United States copyright laws and international treaty provisions. Therefore, you must treat the software like any other copyrighted material (e.g., books or musical recordings), except that you may either: a) make one copy of the software solely for backup or archival purposes, or b) transfer the software to a single hard disk provided you keep the original solely for backup or archival purposes.

3. **OTHER RESTRICTIONS.** The License is your proof of license to exercise the rights granted herein and must be retained by you. You may not rent or lease the software, but you may transfer your rights under this License on a permanent basis provided that you transfer this License, the software and all accompanying written materials, you retain no copies and the recipient agrees to the terms of this License. You may not decompile or disassemble the software. If the software is an update, any transfer must include the update and all prior versions.

4. **MULTIPLE MEDIA SOFTWARE.** If the software package contains compact discs or other media, then you may use only the media appropriate for your single designated computer or network server. You may not use the other media on another computer or computer network, or loan, rent, lease or transfer them to another user except as part of a transfer or other use expressly permitted by this License.

5. **LIMITED WARRANTY.** Code Blue warrants that the software will perform substantially in accordance with the accompanying written materials and will be free from defects in materials and workmanship under normal use and service for a period of 90 days from the date of receipt. Any implied warranties on the software are limited to 90 days. Some states do not allow limitations on the duration of an implied warranty, so the above limitations may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

6. **CUSTOMER REMEDIES.** Code Blue’s entire liability and your exclusive remedy shall be, at Code Blue’s option, either (a) return of the price paid or (b) repair or replacement of the software that does not meet Code Blue’s Limited Warranty and that is returned to Code Blue with a copy of your receipt. This Limited Warranty is void if failure of the software has resulted from accident, abuse or misapplication. Any replacement software will be warranted for the remainder of the original warranty period or 30 days, whichever is longer. Neither these remedies, nor any product support services offered by Code Blue, are available for this USA version product outside the United States of America.

7. **NO OTHER WARRANTIES.** Code Blue disclaims all other warranties, either expressed or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to the software, the accompanying written materials and any accompanying hardware.

8. **NO LIABILITY FOR CONSEQUENTIAL DAMAGES.** In no event shall Code Blue or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information or other pecuniary loss) arising out of the use of or inability to use the software, even if Code Blue has been advised of the possibility of such damages. Because some states do not allow the exclusion or limitations of consequential or incidental damages, the above limitations may not apply to you.

U. S. **GOVERNMENT RESTRICTED RIGHTS.** The software and documentation are provided with restricted rights. Use duplication, or disclosure by the government, is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause as DFARS 252.227-7013 or subparagraphs (c) (1), (2) and (3) of the Commercial Computer Software – Restricted Rights at 48 CFR 52.227-19, as applicable, and any amendments thereto. Contractor/manufacturer is Code Blue Corporation, 259 Hedcor Street, Holland, Michigan 49423 USA. This Agreement is governed by the laws of the State of Michigan.

For more information about Code Blue’s licensing policies, please call Code Blue at 800.205.7186.



UPD Activation

1. Open your web browser and enter the IP address of your ToolVox.
Example: `http://172.1.100.65`
2. Click **TOOLVOX ADMINISTRATION** button (Ill. 3A).



Illustration 3A

3. Enter your administrator User Name and Password (**admin** and **codeblue**) at popup menu (Ill. 3B).

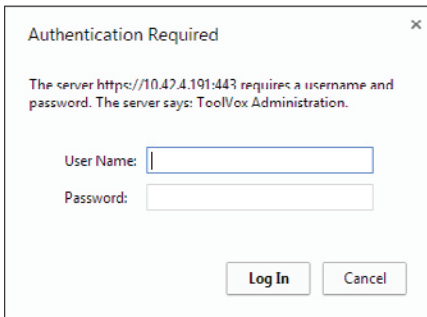


Illustration 3B

4. Click the **OK** button.



5. A new menu ToolVox System Status will initiate (Ill. 3C).

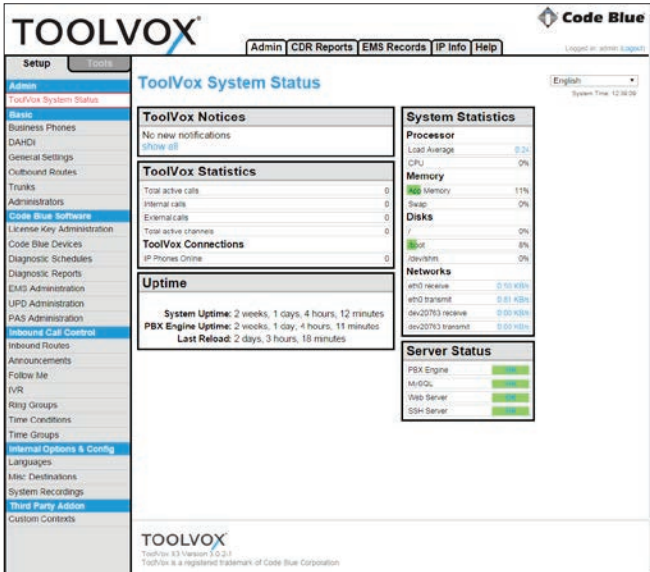


Illustration 3C

6. Under the **SETUP** tab, go to Code Blue Software > License Key Administration.

7. Software Licensing screen will open (Ill. 3D).



Illustration 3D

8. Enter the License Key provided from Code Blue (only needed after original purchase).

9. Select **SUBMIT** button to apply.



UPD Page Navigation

NOTE: At the top of the web page you will see this message: To navigate this form, please do not use the browser Back, Forward or Reload buttons (Ill. 4A).

To navigate through this form, please do not use the browser Back, Forward, or Reload buttons

Illustration 4A

1. Utilize the **NEXT**, **BACK** and **FINISH** buttons located at the top and bottom of each page to navigate through the unit forms.
2. All of the field titles on these pages have a dashed line below them. Place the mouse pointer over these fields to receive a description of its use.

Example: Description (orange box) displays upon user's mouse rollover on **MUSIC ON HOLD** text (Ill. 4B).

The screenshot shows a form with the following fields: "Alert Info:" with a text input, "CID name prefix:" with a text input, "Music On Hold:" with a dropdown menu set to "Default", a checkbox, and another text input. A yellow tooltip box is overlaid on the "Music On Hold:" label, containing the text: "Set the MoH class that will be used for calls that come in on this route. For example, choose a type appropriate for routes coming in from a country which may have announcements in their language." Below the form is a "Privacy" link.

Illustration 4B

3. EMS/UPD Administration

- Update Unit Failure Address
 - Enter email address and click **UPDATE UNIT FAILURE EMAIL ADDRESS** (Ill. 4C).

The screenshot shows a form titled "UPD Administration" with a sub-section "Update Unit Failure Email Addresses". It features a large text input field for email addresses. Below the input field is a note: "You may enter multiple email addresses. Separate email addresses with a semicolon(;) or a comma(,)." At the bottom of the form is a button labeled "Update Unit Failure Email Addresses".

Illustration 4C



- 3. • IP Unit Information Monitor
 - Check the boxes you wish to monitor.
 - Click on **UPDATE IP MONITORING** (Ill. 4D).

IP Unit information to Monitor

- Script Triggered
- Auxillary Out Toggled
- Call Incoming
- Call Outgoing
- Incoming DTMF Commands
- Account Registration
- Call Failed
- Audio Playback Failed
- Script Failure
- Button Failure
- Power Failure
- Public Address Failure
- High Temperature
- Mic/Speaker Failure

Illustration 4D

- IP Unit Address Range (only needed if using SIP or IAX)
 - Enter **IP UNIT NETWORK/MESH**.
 - Click **UPDATE IP SUBNET** (Ill. 4E).

IP Unit Address Range

IP Unit Network/ Mask:

Example: 192.168.1.1/24 for complete subnet range 192.168.1.1 through 192.168.1.255
Contact your Network Administrator for more information.

Illustration 4E

- Max Analog or Pri Trunks for Testing Analog Phones
 - Enter **MAX TRUNKS USED**
 - Click **UPDATE TRUNK AMOUNT** (Ill. 4F).

Maximum Analog or PRI Trunks for Testing Analog Phones

Maximum amount of analog or PRI trunks to be used simultaneously during scheduled tests. If left blank analog phones will not be tested.

Max trunks:

Illustration 4F

- Update Access Information for EMS Software
 - Enter Authorization Code
 - Enter Authorization IP Subnet/Mask
 - Click **UPDATE INFORMATION** (Ill. 4G).

Update Access Information for EMS Software

Authorization Code:

Authorized IP Subnet / Mask:

Example: 192.168.1.0/255.255.255.0 for complete subnet or for individual IP: 192.168.1.10/255.255.255.255
Contact your Network Administrator for more information.

Illustration 4G



UPD - Recording Custom Messages

1. Some Code Blue models have the capability to store messages that are played in various manners when the unit is activated. You may want to record these messages prior to configuring your units. ToolVox allows you to select the recording from the dropdown menu on the model configuration page (Ill. 5A).

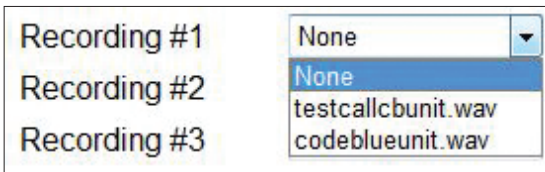


Illustration 5A

2. To record your message(s) from the **SETUP** tab, go to Internal Options & Configuration > System Recordings.
3. The System Recordings page will initiate (Ill. 5B).

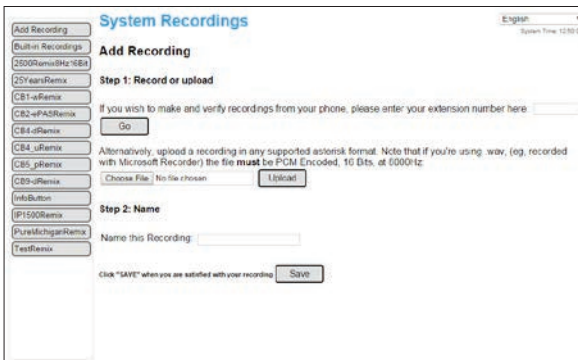


Illustration 5B

4. Follow the instructions on this page. You can either use your phone to record the message(s) or upload them from your PC.

NOTE: Recordings uploaded from your PC must be PCM Encoded, 16 bits at 8 kHz.



Adding a Code Blue Unit

1. From the **SETUP** tab go to Code Blue Software > Code Blue Devices.
2. Follow the section below that pertains to your Code Blue installation scenario:
 “7: Creating a New Unit”
 “8: Copy a Unit”

Creating a New Unit

1. From the **SETUP** tab go to **Code Blue Software > Code Blue Devices**.
2. When creating a new unit, you will be prompted to enter the following information on the first page (Ill. 7A).



Illustration 7A

3. Device Information
 - **EXTENSION:** *Required field.* This is the number given to each unit for system identification. A carefully thought out dial plan should be devised before configuring your ToolVox and UPD system.
 - **CALLER ID DISPLAY NAME:** *Required field.* This is the location or name you wish to label the unit.
4. Unit Information
 - **MODEL:** *Required field.* UPD will configure all Code Blue unit types. Select your model here.
NOTE: If OTHER is selected in the Model field, then no unit type will be used. Only the extension and EMS information will be configured. This is for EMS database entries of people or non-Code Blue devices to be managed by the Code Blue Emergency Communications System.
 - **DEVICE CONNECTION TYPE:** *Required field.* Selection informs ToolVox unit’s connection type:
 - FXS Analog Extension
 - SIP Extension
 - IAX Extension
 - GSM Offsite Unit
5. Hit the **NEXT** button to continue unit configuration on the next page.



6. The following are the required parameters that will be presented, based on the Device Type previously selected:

- FXS Analog Extension
 - **CHANNEL: *Required field.*** This is the FXS port number the unit is connected to. This information may be different for each system. Refer to the ToolVox documentation received with the system for a list of available FXS ports (ill. 7B) Do not change the other fields unless instructed by Code Blue technical support personnel.

Channel (FXS Port)	25
context	from-internal
immediate	no
signalling	fxo_ks
echocancel	yes
echocancelwhenbridged	
echotraining	100
busydetect	no
busycount	7
callprogress	no

Illustration 7B

- SIP Extension

NOTE: After the IP phone is connected to the network, click on 1) EMS/UPD ADMINISTRATION and 2) RUN IP UNIT SCAN below IP Unit Address Range before creating a unit. Run again after creating a unit.

- **SIP SECRET: *Required field.*** Used for SIP phones or analog terminal adapters (see Ill. 7C).
- This is used to authenticate the SIP phone to the ToolVox system.

secret	cbUnit201
dtmfmode	inband
canreinvite	no
context	from-internal
host	dynamic
type	friend
nat	yes
port	5060
qualify	yes

Illustration 7C

NOTE: Strong password methodologies are recommended.

- IAX Extension



- **IAX SECRET:** *Required field.* Used for IAX phones or analog terminal adapters (see Ill. 7D).
- Off System Unit

secret	cbUnit
nottransfer	yes
context	from-internal
host	dynamic
type	friend
port	4569
qualify	yes

Illustration 7D

NOTE: After IP phone is connected to the network, click on 1) EMS/UPD ADMINISTRATION and 2) RUN IP UNIT SCAN below IP Unit Address Range before creating a unit. Run again after creating a unit.

- **UNIT PHONE NUMBER:** *Required field.* For GSM/Offsite units. This number will frequently include an outside line access number, such as 9, in front of the phone number (Ill. 7E).

This device uses custom technology.
Unit Phone Number

Illustration 7E

7. The commands at this point will be configured for your particular model of Code Blue phone. Each command will give you an explanation when you roll the mouse over the command (ill.7F).

Cycle Count

Number of cycles for the programmed numbers to repeat

Illustration 7F

8. On the last page of each unit you will be presented with the following categories:

- **IN CALL COMMANDS:** These commands will be utilized on the EMS Agent screen to control the unit (Ill. 7G).

In-Call Commands		
#	Command Text	DTMF Tone
1	Volume Up	22
2	Volume Down	23
3	MIC Volume Up	20
4	MIC Volume Down	21
5	Open Gate	11
6	Enable PAS	**#9
7	Play Message	01
8		

Illustration 7G



- EMS Unit Location Information consists of selecting the Latitude/Longitude on a MS Bing™ map (Ill. 7H).

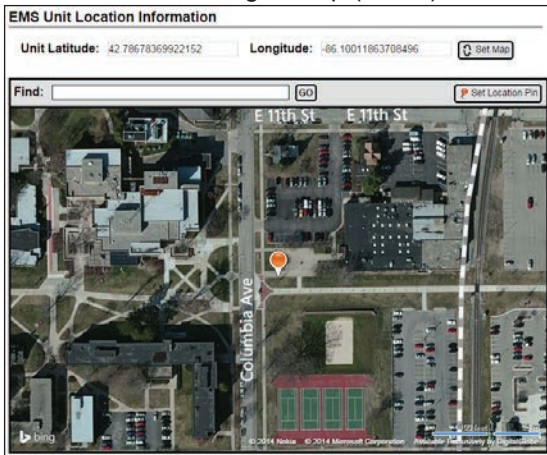


Illustration 7H

- Detailed Unit Location allows you to select the uploaded map (configured in EMS/UPD Administration) and place a Code Blue unit on the map in the desired location (Ill. 7I).

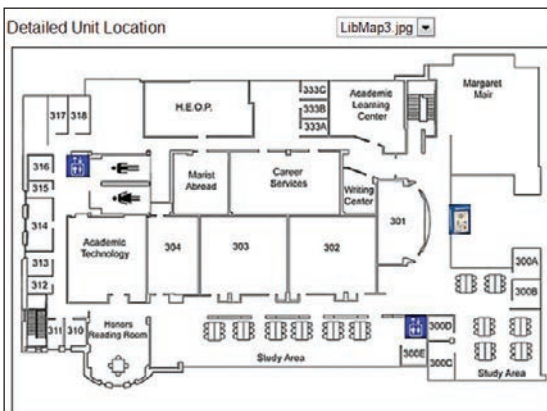


Illustration 7I

- Location Description/Notes allows you to enter specific location/unit information to be displayed on the EMS Agent screen (Ill. 7J).

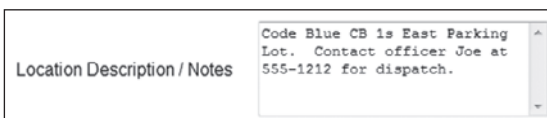


Illustration 7J

- Device Camera URL's allows for the entries of two IP camera streams, which will be displayed on the EMS Agent screen (Ill. 7K).



Illustration 7K



- Unit Address Info allows for the physical address to be documented for display on the EMS Agent screen (Ill. 7L).

Unit Address Info	
Address	92 East 64th St.
City	Holland
State/Province/Region	MI
Postal Code	49423
Country	United States

Illustration 7L

- After configuring your Code Blue unit, click the **FINISH** button on the last page.
- Click **APPLY CONFIGURATION CHANGES** button at the top of the screen (Ill. 7M).



Illustration 7M

- Click **CONTINUE WITH RELOAD** radio button to finish the changes (Ill. 7N).
- Cancel the changes and continue editing the extension by selecting **CANCEL RELOAD AND GO BACK TO EDITING** (Ill. 7N).

Apply Configuration Changes

Reloading will apply all configuration changes made in ToolVox to your PBX Engine and make them active.

Continue with reload

Cancel reload and go back to editing

Illustration 7N

- There are two ways to send the configuration to the Code Blue units:
 - Select the unit by clicking on the extension and click **PROGRAM EXTENSION** at the top of the page.
 - Click **PROGRAM ALL UNITS**.



UPD - Copying a Unit

1. From the **SETUP** tab, go to **Code Blue Software > Code Blue Devices**.
2. Select a unit to copy.
3. Click **COPY EXTENSION** button.
4. When copying a unit you will be prompted to enter the following information (Ill. 8A):



Illustration 8A

- **EXTENSION:** *Required field.* This is the number given to each unit for system identification. A carefully thought out dial plan should be devised before configuring your ToolVox and UPD system.
 - **CALLER ID DISPLAY NAME:** *Required field.* This is the location or name you wish to label the unit.
 - **CHANNEL:** *Required field.* This is the FXS port number the unit is connected to. This information may be different for each system and is configured at the factory. Refer to the ToolVox documentation received with the system for a channel list.
 - **IAX SECRET:** *Required field.* Used for IAX phones or analog terminal adapters.
NOTE: Strong password methodologies are recommended.
 - **UNIT PHONE NUMBER:** *Required field.* This is the phone number of GSM or Offsite units. This number will frequently include an outside line access number, such as 9, in front of the phone number.
5. All other values will remain the same unless changed by the user.
 6. After configuring your Code Blue unit, click the **FINISH** button on the last page.
 7. Click **APPLY CONFIGURATION CHANGES** button at the top of the screen (Ill. 7M).
 8. Click **CONTINUE WITH RELOAD** radio button to finish the changes (Ill. 7N).
 9. Cancel the changes and continue editing the extension by selecting **CANCEL RELOAD AND GO BACK TO EDITING** (Ill. 7N).
 10. There are two ways to send the configuration to Code Blue units:
 - Select the unit by clicking on the extension and click **PROGRAM EXTENSION** at the top of the page.
 - Click **PROGRAM ALL UNITS**.



UPD Diagnostic Schedules

1. UPD Diagnostics can run as many schedules as you configure. Keep in mind that each phone is tested every 2 seconds, beginning at the scheduled time. If you put the same phones in multiple testing schedules, ensure that the time period will not overlap or you may cause erroneous fault reports.
2. From the **SETUP** tab go to **Code Blue Software > Diagnostic Schedules** (see III. 9A)

The screenshot shows the 'Test Schedule' configuration page. It is divided into three main sections: 'Currently Scheduled Unit Tests', 'Schedule New Analog Unit Test', and 'Daily Log Emails'.
 - The 'Schedule New Analog Unit Test' section is active, showing 'For Extensions' set to 7503 through 7503. It offers three radio button options: 'Test Weekly Every Sunday At 12 AM Plus 0 Minutes', 'Test Daily At 12 AM Plus 0 Minutes', and 'Test Hourly At 0 Minutes'. An 'Add' button is visible.
 - The 'Schedule New IP Unit Test' section is inactive, showing 'For Extensions' set to 7501 through 7501 and 'Test Every 1 Minutes'. An 'Add' button is visible.
 - The 'Daily Log Emails' section is also inactive, showing 'For Extensions' set to 7501 through 7501 and 'Email logs Daily at 12 AM Plus 0 Minutes'. A 'To' field is present with a dropdown arrow, and an 'Add' button is at the bottom.

Illustration 9A

3. Schedule New Analog Unit Test
 - Select the range you wish to include in the schedule.
 - Select the appropriate schedule for your needs.
 - Click on **Add** to create the schedule (III. 9B).

The screenshot shows the 'Set Schedule' configuration page. It is divided into two main sections: 'Currently Scheduled Unit Tests' and 'Add New Unit Tests'.
 - The 'Add New Unit Tests' section is active, showing 'For Extensions' set to 200 through 200. It offers three radio button options: 'Test Weekly Every Tuesday At 12 AM Plus 27 Minutes', 'Test Daily At 7 AM Plus 29 Minutes', and 'Test Hourly At 0 Minutes'. The 'Test Daily' option is selected. An 'Add' button is visible at the bottom right.

Illustration 9B

4. Schedule New IP Unit Test
 - Select the range you wish to include in the schedule.
 - Select **TEST EVERY 1-59 MINUTES**.
 - Click on **Add** to create the schedule.



5. Repeat steps 7.3 through 7.4 to create additional schedules.
6. Diagnostic Reports
 - Click on **Code Blue Software > Diagnostic Reports** (Ill. 9C).

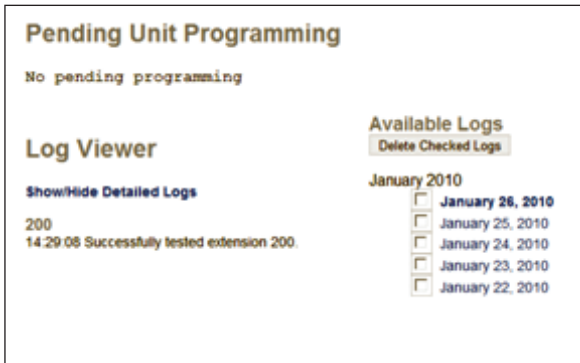


Illustration 9C

- Information pertaining to unit programming and logs from test schedules will be displayed. Click on the log you wish to view under Available Logs. Click on the **Show/Hide Detailed Logs** to view detailed information of the testing/programming of the units (ill. 9D).



Illustration 9D

- Select the check box beside each log and click on **Delete Checked Logs** to delete old log files.



UPD Test Options

IA500/IA3000/IA3100 and Non-Code Blue Analog Model Phones that respond with a tone when called

- RFA tone (presence)

IA4100 Analog Model Phone

- RFA tone (presence)
- Low Battery
- AC/DC Power Fault
- PAS Fault

IP1500/2500/5000 Model Phones

- Action Script Triggered
- Auxiliary Out Toggled (with specific one, status)
- Call Incoming (with Number)
- Call Outgoing (with Number)
- Incoming DTMF Commands
- Account Registration (SIP/IAX2)
- Call Failed (with reason)
- Audio Playback failure (with reason and channel)
- Action Script Failure (with error)
- Button failure (with button #)
- Power Failure (with power source that failed)
- Public Address Failure
- High Temperature
- Mic/Speaker Failure



16 Integrations

16.1 Milestone XProtect



This section contains detailed instructions regarding the Code Blue ToolVox®/ Milestone XProtect software integration so please read it in its entirety before beginning installation.

System Requirements

System requirements for Milestone products can be found on the Milestone website:

www.milestonesys.com/Support/Technical-Support/Product-System-Requirements

The Code Blue integration software was created with the MIP SDK 3.0 and tested with version 2013 R2 and 2016 R2 of the XProtect software.

The integration can be used with these editions of XProtect:

- Corporate
- Expert
- Enterprise
- Professional
- Express

Contents

The integration software consists of two plug-ins. The plug-ins add functionality to XProtect. Each plug-in consists of a DLL file and a “plugin.def” files. These files must be placed in XProtect installation folders to take effect. Note that the two “plugin.def” files are different.

- Event Server plugin
 - CBEventServerPlugin.dll
 - plugin.def
- Management Client plug-in
 - CBManagementClientPlugin.dll
 - plugin.def



Installation

Copy Plug-in Files into XProtect Directories

The installation process involves copying the integration software files to the XProtect installation directories.

There are two plug-ins to install:

- Management Client plug-in
- Event Server plug-in

Use the Windows paths below as a guide. The examples here are based on default installations of XProtect version 2013 R2 and 2016 R2, Corporate Edition and Enterprise Edition. The XProtect installation location may be different for other versions or other editions of XProtect. For other versions and editions, contact Milestone support or refer to www.milestonesys.com/support.

Install the Event Server plug-in on the computer running the Event Server.

Install the Management Client plug-in on computers with Management Client installed.

XProtect 2013 R2 and 2016 R2 Corporate Edition on Windows 7:

C:\Program Files\Milestone\MIPPlugins\CBManagementClientPlugin\CBManagementClientPlugin.dll
C:\Program Files\Milestone\MIPPlugins\CBManagementClientPlugin\plugin.def
C:\Program Files\Milestone\MIPPlugins\CBEEventServerPlugin\CBEEventServerPlugin.dll
C:\Program Files\Milestone\MIPPlugins\CBEEventServerPlugin\plugin.def

XProtect 2013 R2 and 2016 R2 Enterprise Edition on Windows 7:

C:\Program Files (x86)\Milestone\MIPPlugins\CBManagementClientPlugin\CBManagementClient.dll
C:\Program Files (x86)\Milestone\MIPPlugins\CBManagementClientPlugin\plugin.def
C:\Program Files (x86)\Milestone\MIPPlugins\CBEEventServerPlugin\CBEEventServerPlugin.dll
C:\Program Files (x86)\Milestone\MIPPlugins\CBEEventServerPlugin\plugin.def

You will need to create the folders “CBEEventServerPlugin” and “CBManagementClientPlugin”.

Each plug-in has a file called “plugin.def”. If you lose track of the .def files, open them in a text editor such as Notepad to confirm which DLL they go with.



Verifying the Installation

Once you have configured telephones and Code Blue devices in ToolVox, verify that XProtect is recognizing the plug-ins.

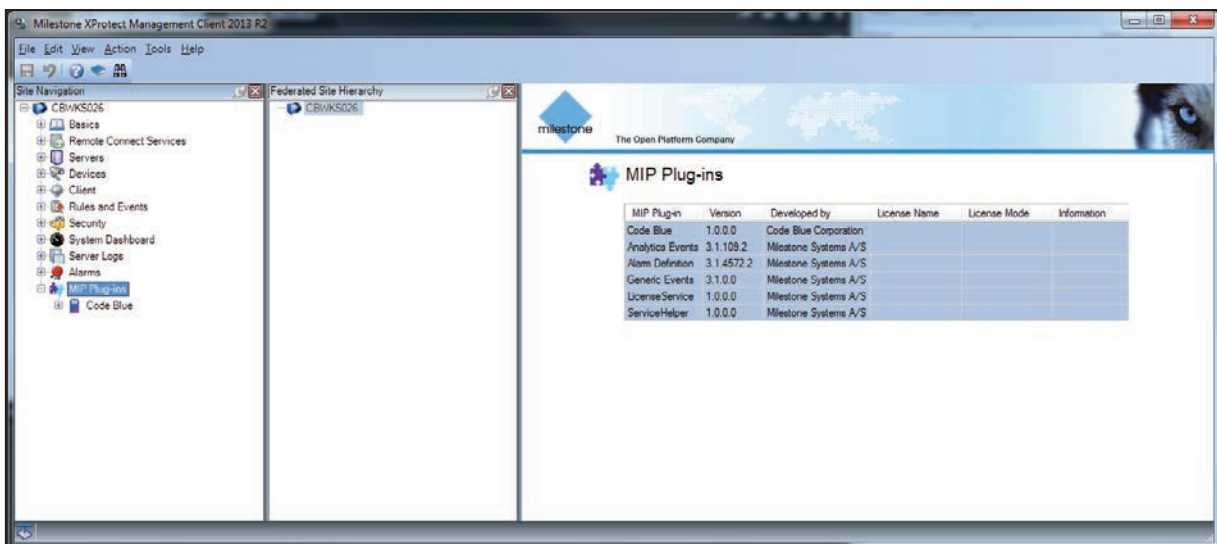
Open the Management Client application, which is called the Management Application in some editions of XProtect. Here it will be referred to as Management Client.

Log in to Management Client.



ED-10041-A

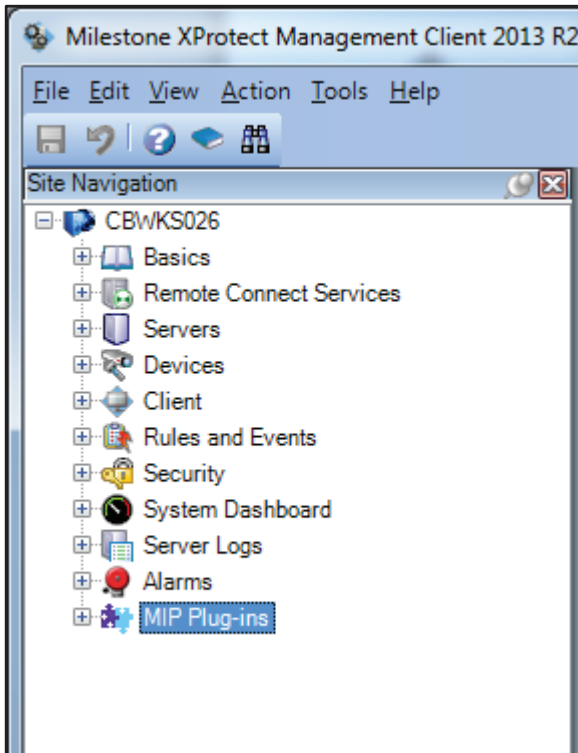
Once logged in, you will see the Site Navigation Tree on the left side of the window:



ED-10042-A



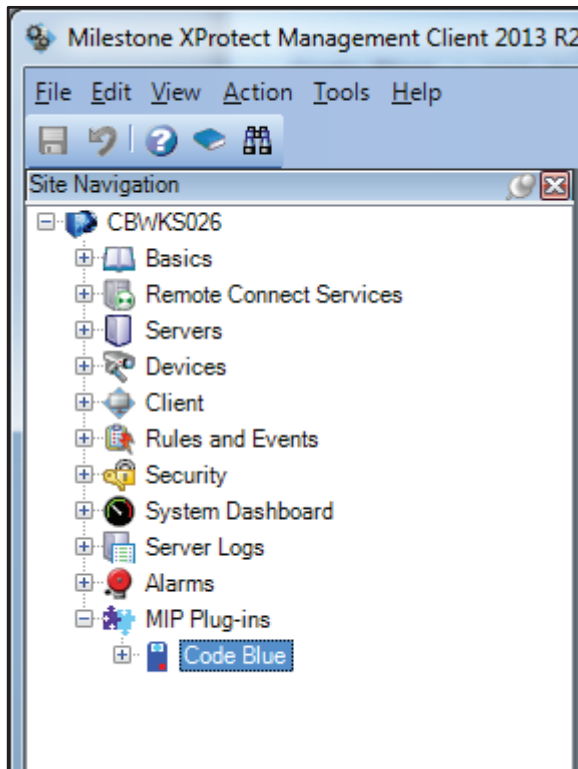
Find the “MIP Plug-ins” node in the System Status Tree:



ED-10043-A



If the System Connector plugin files have been placed correctly, you should be able to expand the MIP Plug-ins node and you will see a Code Blue node listed under it.



ED-10044-A

If you don't see the Code Blue node listed in the MIP Plug-ins node, the plugin files are probably not being found by the Management Client application. Verify that the plugin files are in the correct locations. Refer to the Installation chapter of this document for instructions on installing the plugins.

Setting up ToolVox

Telephones and Devices

Telephones and Code Blue devices must be configured in ToolVox Media Gateway before using the software integration.

Refer to Section 8 for step-by-step instructions on setting up telephones and Code Blue devices in ToolVox.

EMS Administration

ToolVox Administration -> EMS Administration -> ToolVox API section

Fill in the following fields located at the bottom of the EMS Administration page:

Destination URL: Web URL pointing to XProtect Host with port.

e.g.: `http://192.168.1.50:3333`



Keep alive Interval – Time interval (in seconds) to ping a heartbeat to XProtect Event server host.

e.g.: 60

Data Type – Must be set to XML

ToolVox API

Specify a destination URI that the ToolVox API will post event messages to. You can specify either a URI in the format `http://hostname/path` for HTTP POST or `tcp://hostname:port` to send the contents of the event message directly to a TCP socket.

Destination URL:

Keep Alive Interval: seconds (0 = disable ping)

Data Type: JSON XML CSV

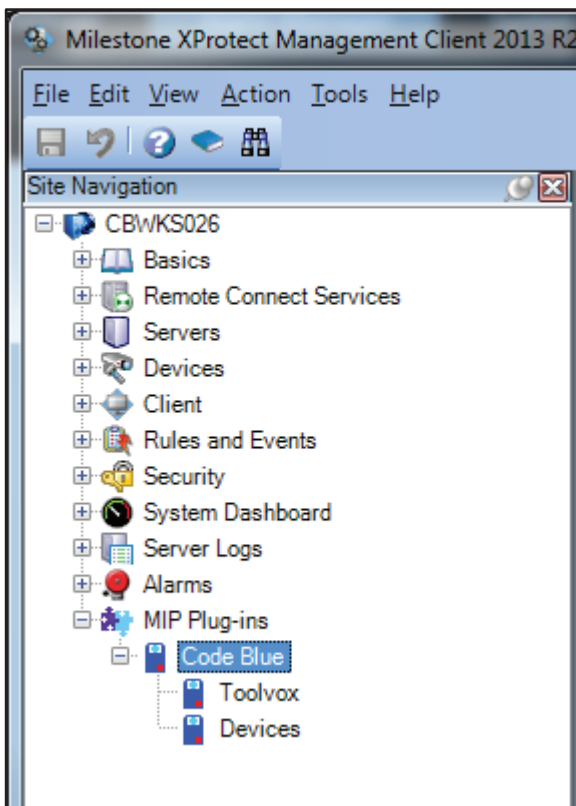
Setting up XProtect

Adding ToolVox Media Gateway units to XProtect

This section will explain how to add a Toolvox Media Gateway to the XProtect system. Screenshots are from the Corporate Edition and may look different if you are using a different edition of XProtect.

Open Management Client (known as Management Application in some editions of XProtect).

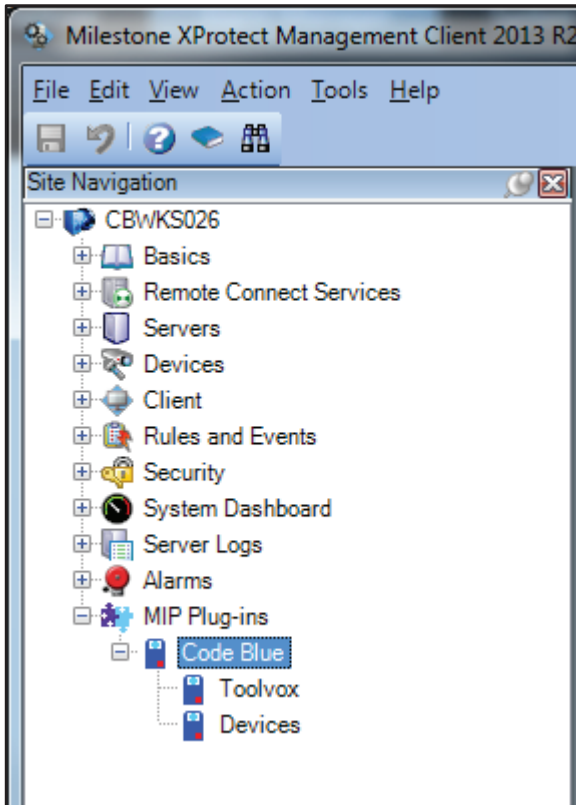
Expand the MIP Plug-ins node in the Site Navigation tree. Expand the Code Blue node. There are two nodes inside: Toolvox and Devices.



ED-10045-A

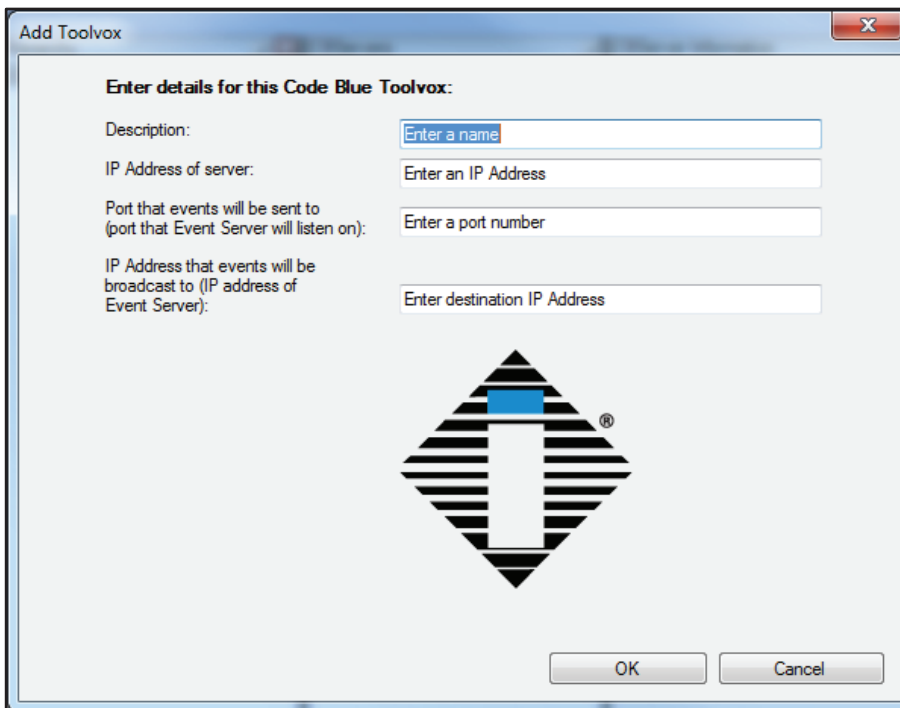


Open the Management Client (or Management Application in some editions of XProtect). Right-click the Toolvox node, then select “Add New...”.



ED-10046-A

The Add Toolvox form will appear.



ED-10047-A

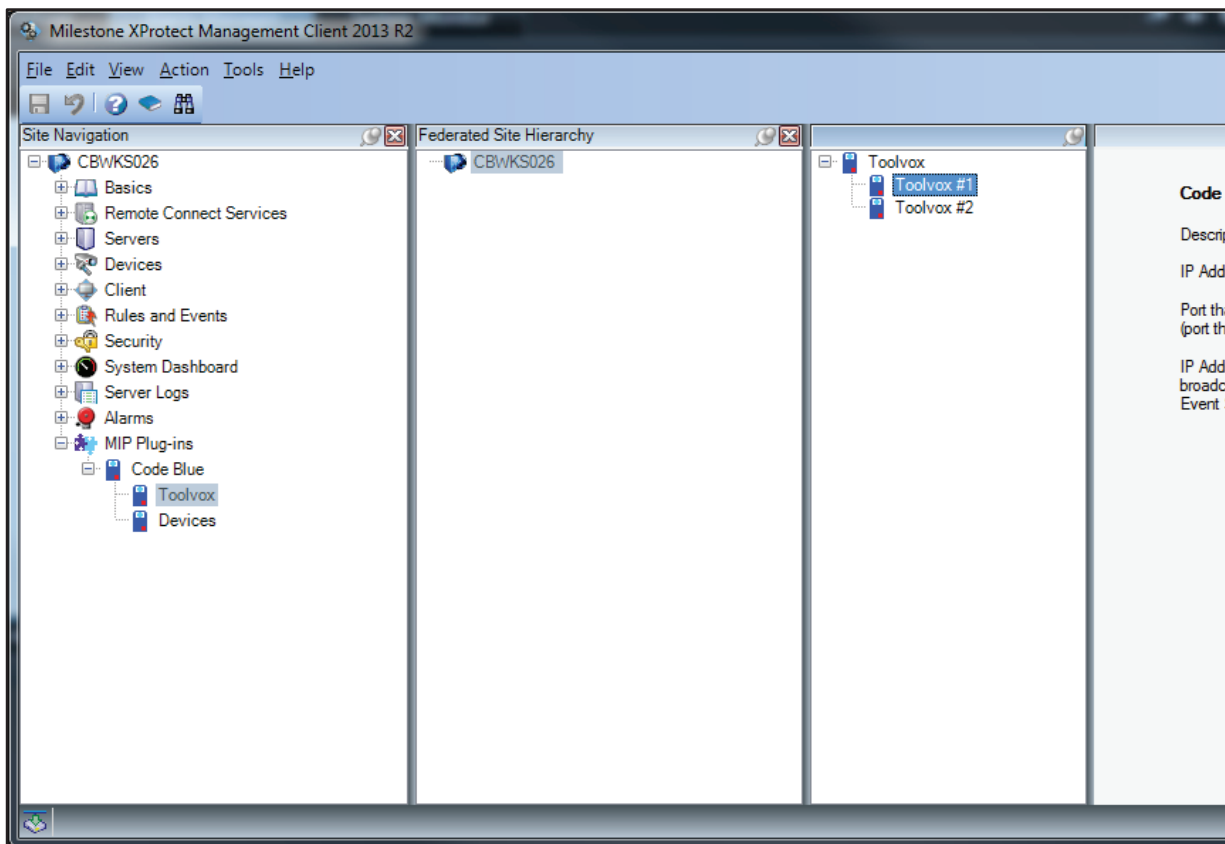


Fill out the fields:

- **Description** – Description of this particular Toolvox Media Gateway. If you have multiple Toolvox Media Gateway units, enter something that will help you identify which is which.
- **IP Address of server** – The IP Address of the Toolvox Media Gateway is displayed in alerts, and is used for call event transmission.
- **Port that events will be sent to (port that Event Server will listen on)** – Specify the port on the computer running Milestone XProtect Event Server to which events should be sent to. If you not sure what to enter, contact the Server Administrator and request an available port. You will need a port that can be used in conjunction with the Event Server's IP address you are using.
- **IP Address that events will be broadcast to (IP address of Event Server)** – Enter the IP address of the Milestone XProtect Event Server. If you are not sure what the IP address of the Event Server is, contact the Server Administrator to request an IP address that can be used in conjunction with the port entered in the Port field.

Press the OK button to save.

ToolVox units that you have configured show up in a list in a separate panel. In the following screenshot, you can see there are two ToolVox units configured: ToolVox #1 and ToolVox #2.



ED-10048-A



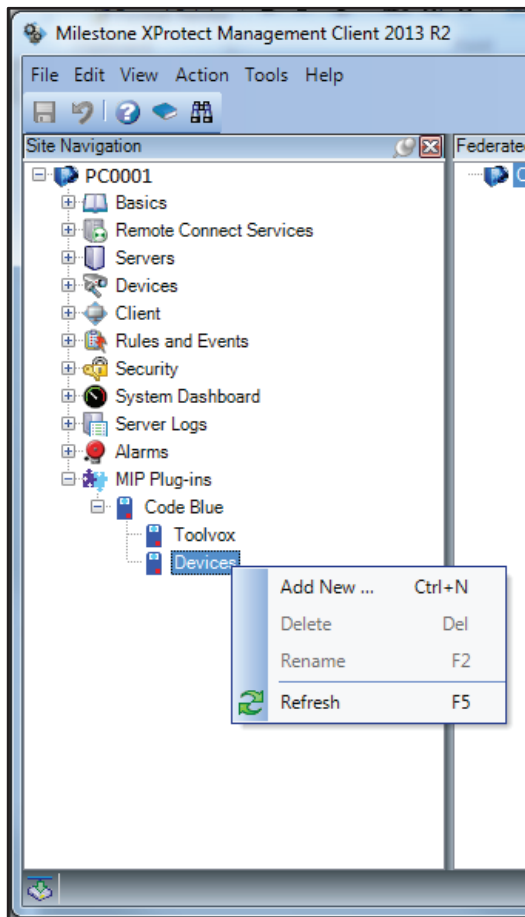
Adding Devices to XProtect

This section will explain how to add devices to the XProtect system. Screenshots are from the Corporate Edition and may look different if you are using a different edition.

Devices can be any physical device that communicates through a ToolVox Media Gateway. Examples of devices include, but are not limited to:

- Telephone that security personnel use to respond to calls from Code Blue products
- Code Blue wall mounted unit
- Code Blue pole mounted unit
- Code Blue speakerphone

Open the Management Client (or Management Application in some editions of XProtect). Right-click the Devices node in the Site Navigation tree, and select “Add New...”.



LD-10049-A



The Add Device form will appear.

Enter details for this Code Blue Device/Phone:

Description:

Extension:

Toolvox:

OK Cancel

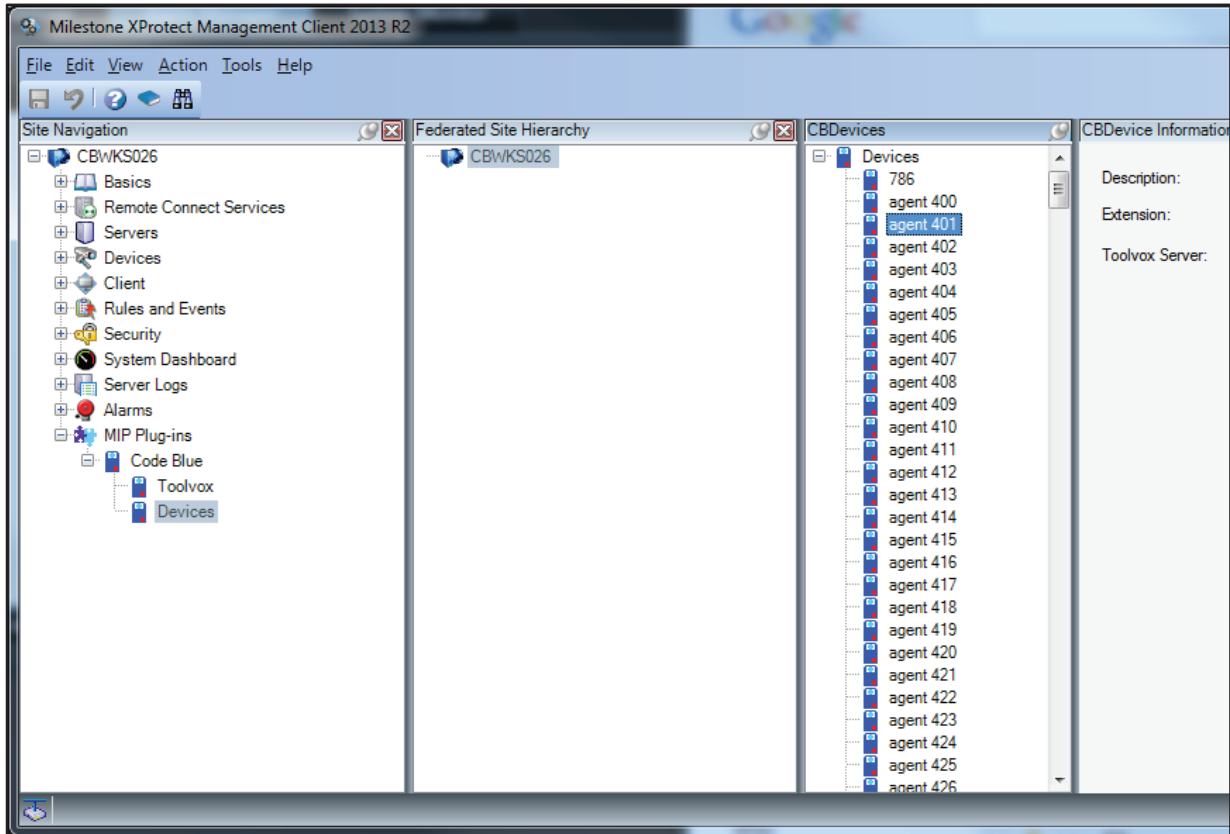
ED-10050-A

Fill out the fields and press the OK button to save:

- **Description** – Description of this particular device. You can enter whatever you like, but it is recommended that you enter something that will help you identify this device, such as the extension or a verbal description of its geographic location.
- **Extension** – The extension number of this device.
- **Toolvox** – This dropdown menu will list the Toolvox Media Gateway units that have been added in Management Client. Toolvox Media Gateway units must be configured first before they will be in this list. Select the Toolvox that this device will communicate through.



A list of devices that have been configured is shown in a separate panel. In the following screenshot, you can see that many devices have been added:



ED-10051-A

Test every device before “going live”.



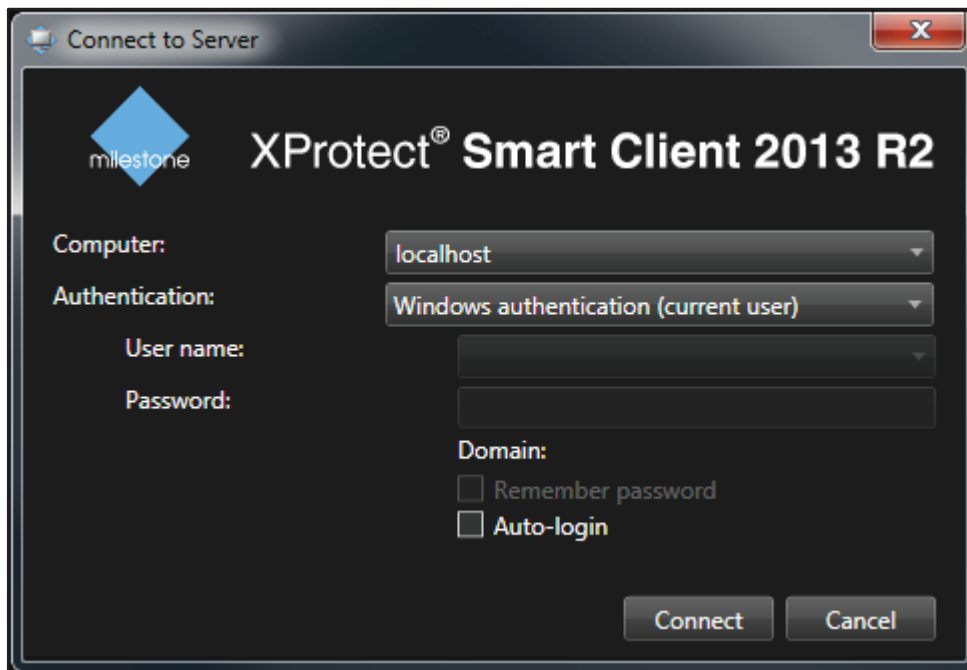
Using the Integration Software

Introduction

When a call is made using a Code Blue emergency communication device, an alarm will be generated in Smart Client. This documentation shows examples of alarms generated by the Code Blue System Connector. For general guidance using the Smart Client application, refer to Milestone documentation.

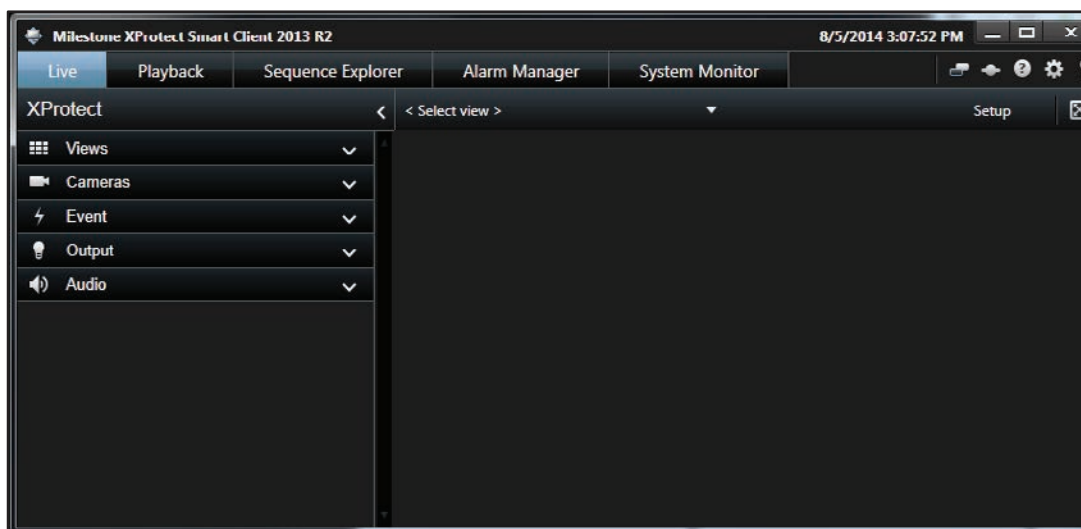
Making a Call

Open the XProtect Smart Client and log in.



ED-10052-A

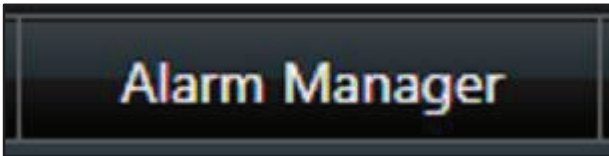
You will see the Smart Client screen.



ED-10053-A

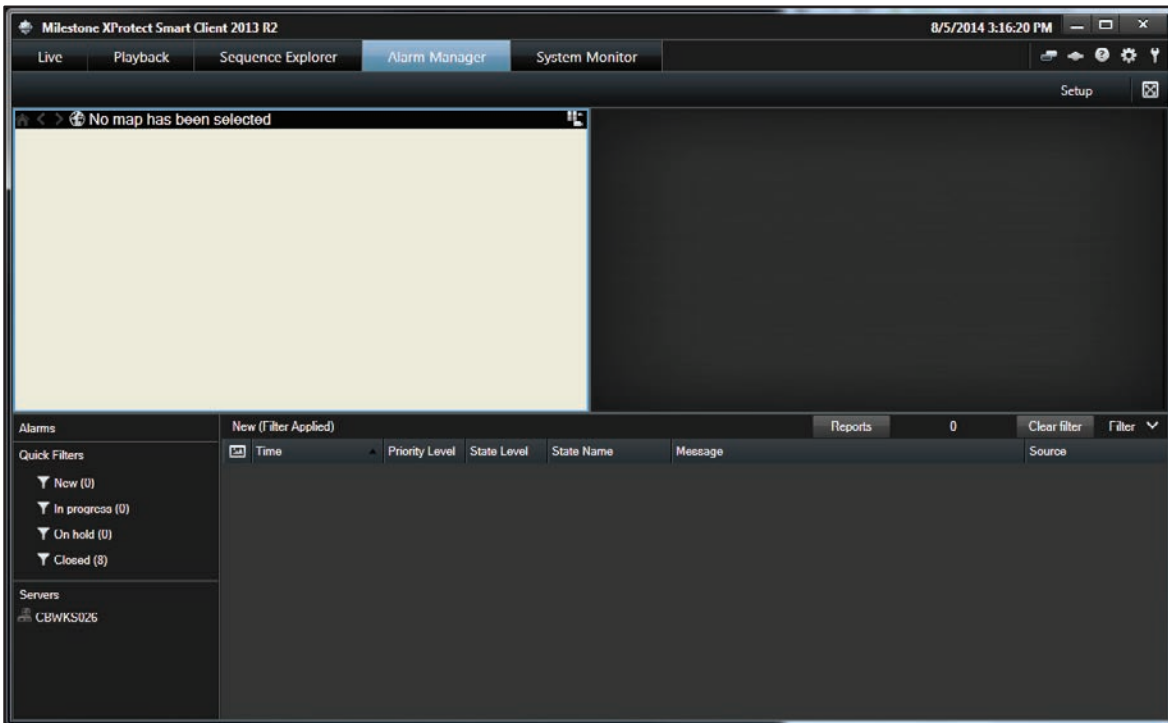


Click the Alarm Manager tab to monitor alarms.



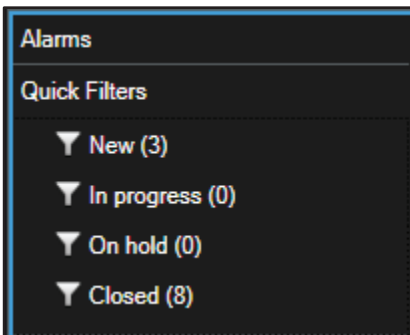
ED-10054-A

The Alarm Manager will appear:



ED-10055-A

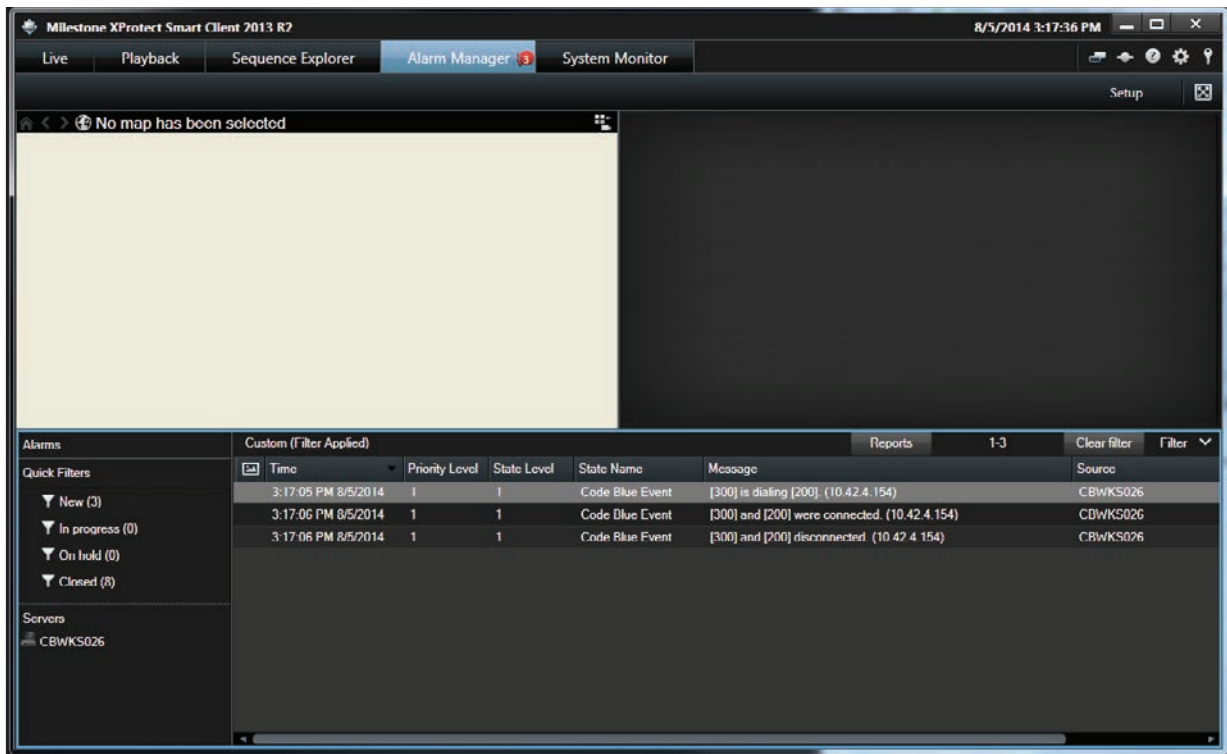
Alarms generated by Code Blue devices appear as “New” alarms. To view the New alarms, click the “New” Quick Filter:



ED-10056-A



Alarms that are generated during a call show up in the lower-right portion of the screen:



ED-10057-A

The most important part of an alarm is the message:



ED-10058-A

You can view more information about the alarm by double-clicking it. This will open a new window.



Alarms Generated by the Integration Software

Overview

There are several types of alarms that can be generated by Code Blue devices. Most alarms will be triggered when someone makes a call using a Code Blue speakerphone device. Other alarms alert security personnel to changes in the status of a ToolVox unit.

Call Alarms

A call in ToolVox can be divided into separate events.

1. When someone presses a button on a Code Blue device to initiate a call, that is the “dial” event. The Code Blue device is dialing a telephone that security personnel will answer.
2. When security personnel answer a telephone, a connection is established between the Code Blue speakerphone device and the telephone. When this happens, ToolVox begins transmitting audio. This is the “connect” event.
3. When the two people talking are finished, the security personnel hangs up their telephone. ToolVox recognizes this and stops transmitting audio. This is the “hangup” event. The “hangup” event occurs once for the speakerphone device, and once for the telephone, for a total of two hangup events.
4. The “disconnect” happens automatically after the hangup events. The speakerphone device and telephone return to their original state, before the “dial” event.

The alarms generated in Smart Client correspond to these events. Alarms are not displayed for the hangup event. So for a typical call, there are three alarms: Dialing, Connected, and Disconnected.

ToolVox Status Alarms

An alarm will be generated if communication is lost between the XProtect Event Server and a ToolVox unit for more than 60 seconds. When communication is restored, another alarm will appear.



Troubleshooting

Log Files

Overview

The Event Server plug-in writes messages to a log file when certain events happen. The log file is a normal part of XProtect and is not part of the Code Blue integration software. You can view the log files to diagnose problems or verify that the System Connector is configured properly.

Log messages generated by the Code Blue Event Server Plugin are marked with the text “CBEventServerPlugin”.

File Locations

In XProtect 2013 R2 and 2016 R2, the log files that the Code Blue Event Server Plugin can be found here:

C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs\

For other versions of XProtect and other operating systems, contact Milestone support.

Sample log messages and what they mean

These examples are intended to demonstrate typical log entries. This is not a complete list of possible log entries.

```
CBEventServerPlugin      Attempt to create socket failed for: CBTV16.  
(IP=192.168.10.21) (Port=8000)
```

First, we know this log entry was generated by the Code Blue Event Server Plugin because it starts with “CBEventServerPlugin”. The rest of the message indicates that the plugin was unable to open a communication channel on the IP address and port specified. Check that the IP address matches that of the Event Server, and that the port is not in use by another program on the Event Server. If you need to change the settings of that Toolvox, you can see here that the unit that needs to be reconfigured is the unit called CBTV16.

```
CBEventServerPlugin      Configuration changed. 3 Toolvox Media Gateways are now  
configured.
```

A change was made to a Toolvox Media Gateway unit in Management Client/Management Application. Maybe one was added, removed, or edited; the number tells you how many Toolvox Media Gateway units are now present in the configuration. You can compare this to past numbers. This message also appears when the Event Server first starts up.

The following example log entries just repeat what the Code Blue System Connector alarms in Smart Client say:

```
CBEventServerPlugin      [300] is dialing [200]. (Toolvox IP=192.168.10.2)
```

```
CBEventServerPlugin      [300] and [200] were connected. (Toolvox  
IP=192.168.10.3)
```

```
CBEventServerPlugin      [300] hung up. (Toolvox IP=192.168.10.4)
```




CBEventServerPlugin Toolvox with IP Address=(192.168.10.5) is inactive.

CBEventServerPlugin Toolvox with IP Address=(192.168.10.5) came back on-line.

Symptoms and resolutions

Alarms are not being generated when calls are made

Data from the device(s) is not making it to the Smart Client. There are many possible causes for a lapse in communication, including but not limited to hardware issues, network connectivity issues, and incorrect configuration settings . Some possibilities:

- Is the Toolvox Media Gateway hardware configured and running?
- Has it been added to the Management Client (called Management Application in some editions of XProtect)?
- Are the configuration details of the Toolvox correct (IP address, port, etc.)?
- Is the device connected to the Toolvox Media Gateway?
- Has it been added to the Management Client (called Management Application in some editions of XProtect)?
- Are the configuration details of the device correct (IP Address, port, etc.)?
- Check the log files for any relevant information.

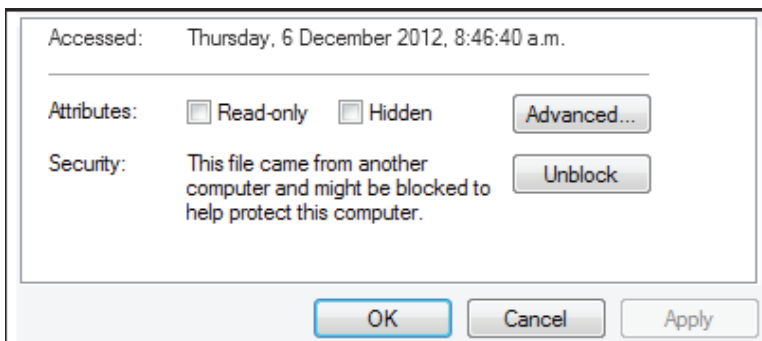
“ToolVox offline” alarm shows up even though the ToolVox is running and connected to the network

- Is Event Server running? If not, start the service. If it is already running, try restarting it.
- Check the log files for any relevant information.

Management Client fails to start with the following error: Could not load file or assembly 'file:///C:\Program Files\Milestone\MIPPlugins\CBManagementClientPlugin\CBManagementClient Plugin.dll' or one of its dependencies. Operation is not supported.

This sometimes occurs on hosts running The .NET Framework versions 4 and above. The reason this occurs is Microsoft Windows has flagged the CBManagementClient Plugin.dll as originating from a foreign host (ie from a remote host / the internet).

To resolve this error, try opening the file properties and clicking 'Unblock':





16.2 Lenel OnGuard®



Technical Specifications

Minimum System Hardware Requirements

The following requirements apply to OnGuard® 2013. The Accessory Add-On is certified by Lenel to work with OnGuard® 2013. If you can run OnGuard® 2013 on your hardware, you can also run the Accessory Add-On.

- Pentium IV 1 GHz Processor
- 2 GB RAM
- DVD-ROM
- USB Port
- 1024x768 color display
- 6 GB of available space



Lenel - Operating System Compatibility Chart

Last Updated: 9/27/2013

Please review the OnGuard Product Release Notes for additional information and known limitations pertaining to supported operating systems.

Tested with OnGuard Version along with the latest Cumulative Hot Fix:

OnGuard Version	OnGuard 2013	OnGuard 2012	OnGuard 2010 Technology Update
Operating Systems	6.6.287	6.5.624	6.4.500 TU
Windows 7 Enterprise, Professional, and Ultimate (32 bit, 64-bit) ¹	SP1	SP1	✓
Windows 8 Enterprise and Professional (32 bit, 64-bit) ¹	Not Supported	✓ ⁴	Not Supported
Windows Server 2012 Standard (64-bit)	Not Supported	✓ ⁴	Not Supported
Windows Server 2008 R2 Standard and Enterprise (64-bit)	SP1	SP1	SP1, ✓
Windows Server 2008 Standard and Enterprise (32 & 64-bit)	SP2	SP2	SP2
Windows XP (32-bit) ¹	SP3	SP3	SP3
Windows Vista Business and Enterprise Editions (32-bit) ³	EOL	EOL	SP2
Windows Server 2003 Standard and Enterprise (32-bit only) ²	SP2, R2 SP2	SP2, R2 SP2	SP2,R2 SP2

Key Notes:

EOL = End of Life ✓ = Base Version (no Service Pack)

1 Not recommended for use as the Web Application Server for all OnGuard supported versions. Please refer to the Release Notes for additional information.

2 Windows Server 2003 64-bit is not supported.

3 Windows Vista (For 6.4.500 TU and prior)

A. Not recommended for use as the Web Application Server for all OnGuard supported versions. Please refer to Release Notes for additional information.

B. Windows Vista is not supported for LDVR and OnGuard Go! products.

4 Starting with HF 1.0



Supported Operating Systems

The following products have been approved with the listed operating systems and system service packs. All new systems shipped from Lenel will include at least these service pack versions. Operating system requirements are now enforced. Installations attempted on other operating systems will not run.

Note: OnGuard® is a 32-bit application that can be run on some 64-bit systems. 64-bit systems are only supported as listed in this section.

For an up-to-date list of tested operating systems and service packs, refer to the compatibility charts on the Lenel Web site:

<http://www.lenel.com/support/downloads/onguard#compatibility-charts>. (You will need your Lenel login to gain access to this site.)

Windows XP Professional with Service Pack 3

- Windows XP Professional SP3 32-bit is approved for OnGuard® server and client operations.
- Windows XP is not supported for use as the Web Application Server (LS Application Server service) because the number of client connections to IIS is limited in this operating system.
- Windows XP Professional is approved for use as any Lenel Digital Video product host operating system.
- Windows XP 64-bit is not supported.
- Windows XP SP3 is supported for communication with HID Edge Devices.
- Windows XP SP3 will be called Windows XP, from this point forward, in the OnGuard® 2013 Release Notes.

Windows Server 2003 with Service Pack 2

- Windows Server 2003 SP2 32-bit Standard and Enterprise are approved for all OnGuard® server and client operations.
- Windows Server 2003 64-bit is not supported.
- Windows Server 2003 SP2 Standard and Enterprise are approved for use as any Lenel Digital Video product host operating system, not including the OnGuard® GO! product.
- Windows Server 2003 SP2 Standard and Enterprise can be utilized as the separate OnGuard® server with Lenel Digital Video products.
- Windows Server 2003 Standard and Enterprise SP2 will be called Windows Server 2003, from this point forward, in the OnGuard® 2013 Release Notes.

Windows Server 2003 R2 with Service Pack 2

- Windows Server 2003 R2 SP2 32-bit Standard and Enterprise are approved for all OnGuard® server and client operations.
- Windows Server 2003 R2 64-bit is not supported.
- Windows Server 2003 R2 SP2 Standard and Enterprise are approved for use as any Lenel Digital Video product host operating system, not including the OnGuard® GO! product.



- Windows Server 2003 R2 SP2 Standard and Enterprise can be utilized as the separate OnGuard® server with Lenel Digital Video products.
- Windows Server 2003 R2 SP2 Standard is supported for communication with HID Edge Devices.
- Windows Server 2003 Standard and Enterprise R2 SP2 will be called Windows Server 2003 R2, from this point forward, in the OnGuard® 2013 Release Notes.

Windows Server 2008 with Service Pack 2

- Windows Server 2008 Standard and Enterprise SP2 32-bit and 64-bit are approved for OnGuard® server and client operations.
- Windows Server 2008 SP2 32-bit and 64-bit is approved for use as a Lenel NVR product host operating system. Note: Windows Server 2008 is not approved for use as any Lenel Digital Video product host operating system when using OnGuard® 201 O and prior.
- Windows Server 2008 SP2 is not supported with Visitor Management Front Desk Application.
- Windows Server 2008 SP2 Standard Edition 32-bit is supported for communication with HID Edge Devices.
- Windows Server 2008 Standard and Enterprise SP2 will be called Windows Server 2008, from this point forward, in the OnGuard® 2013 Release Notes.

Windows Server 2008 R2 with Service Pack 1

- Windows Server 2008 Standard and Enterprise R2 SP1 64-bit are approved for all OnGuard® server and client operations.
- Windows Server 2008 Standard and Enterprise R2 SP1 are approved for use as a Lenel NVR product host operating system.
- Windows Server 2008 Standard and Enterprise R2 SP1 can be utilized as the separate OnGuard® server with Lenel Digital Video products. Note: Windows Server 2008 is not approved for use as any Lenel Digital Video product host operating system when using OnGuard® 2010 and prior.
- Windows Server 2008 R2 SP1 Enterprise 64-bit is not supported for communication with HID Edge Devices.
- Windows Server 2008 Standard and Enterprise R2 SP1 will be called Windows Server 2008 R2, from this point forward, in the OnGuard® 2013 Release Notes.

Windows 7 with Service Pack 1

- Windows 7 SP1 Enterprise, Professional, and Ultimate 32-bit and 64-bit are approved for all OnGuard® server and client operations.
- Windows 7 is not recommended for use as the Web Application Server (LS Application Server service) because the number of client connections to 11S is limited in this operating system.
- Windows 7 Enterprise 32-bit is supported for communication with HID Edge Devices.
- Windows 7 Enterprise 64-bit is not supported for communication with HID Edge Devices.
- Lenel NVR is supported on Windows 7 SP1 32-bit and 64-bit.



- Windows 7 SP1 Enterprise, Professional, and Ultimate will be called Windows 7, from this point forward, in the OnGuard® 2013 Release Notes Supported Operating Systems

Contents of Accessory Add-On

The Accessory Add-On for Code Blue Intercom Support is provided to the customer as an installation file. This will likely be provided inside a compressed ZIP file. The customer runs this file as if they were installing any other program. A graphical installation program will walk the customer through the installation process.

For more information on the installation process, see the Installation section of this document. Lenel calls these installation files “Accessory Add-Ons”, so this is how Code Blue will refer to them when working with customers. The full name for the Accessory Add-On that Code Blue created to integrate speakerphone devices with Lenel OnGuard® is:

6.6 Accessory Add-On for Code Blue Intercom Support.msi

- “6.6” refers to the version of OnGuard® this Accessory Add-On has been certified with.
- The “.msi” extension designates the file as a “Microsoft Installer” or “Windows Installer”.
- Note that the “.msi” extension may not be visible on a customer’s computer. This depends on their settings, and it should not be assumed that they can see that part of the file name.

Distribution of the Accessory Add-On to Customers

Lenel will provide the actual Accessory Add-On file(s) to customers.



Installation

Installing OnGuard®

For assistance installing the OnGuard® security system, contact Lenel. This section only documents installation of the Accessory Add-On.

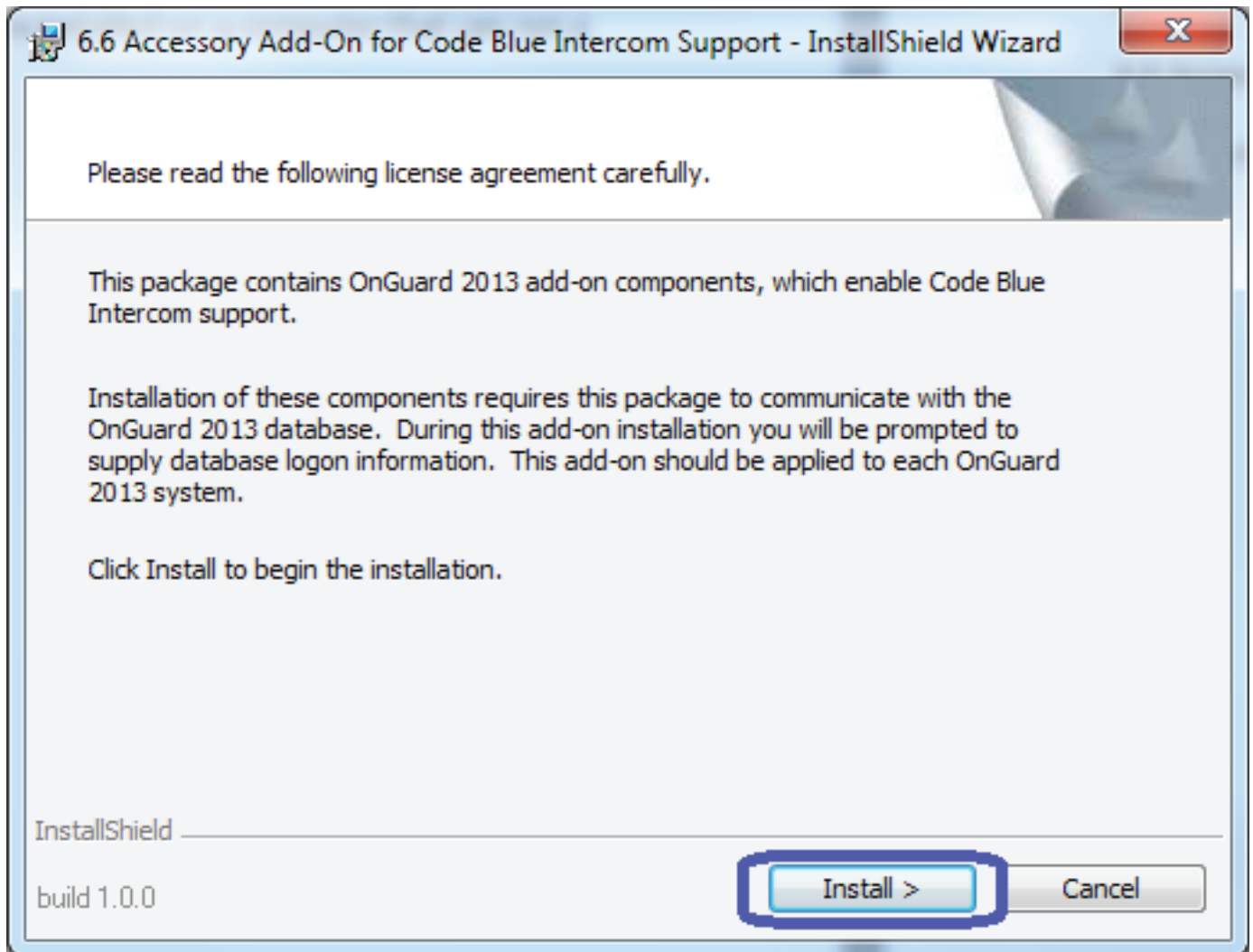
Prerequisites

- Lenel OnGuard® 2013 6.6 must be installed.
- ToolVox® hardware should be installed and operational. Testing of the Accessory Add-On will not be possible until ToolVox® is operational.
- Code Blue speakerphone hardware should be installed and operational for the same reason.

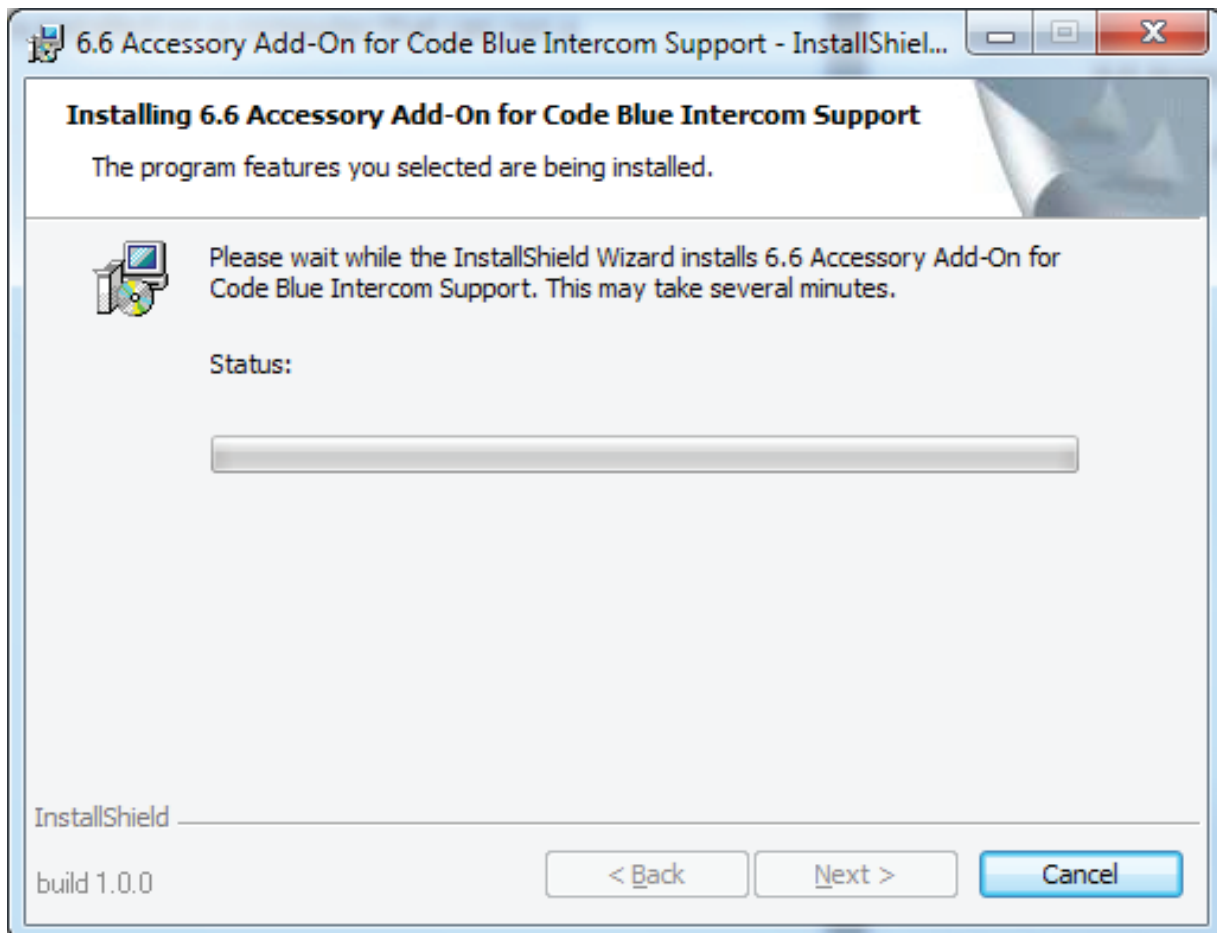
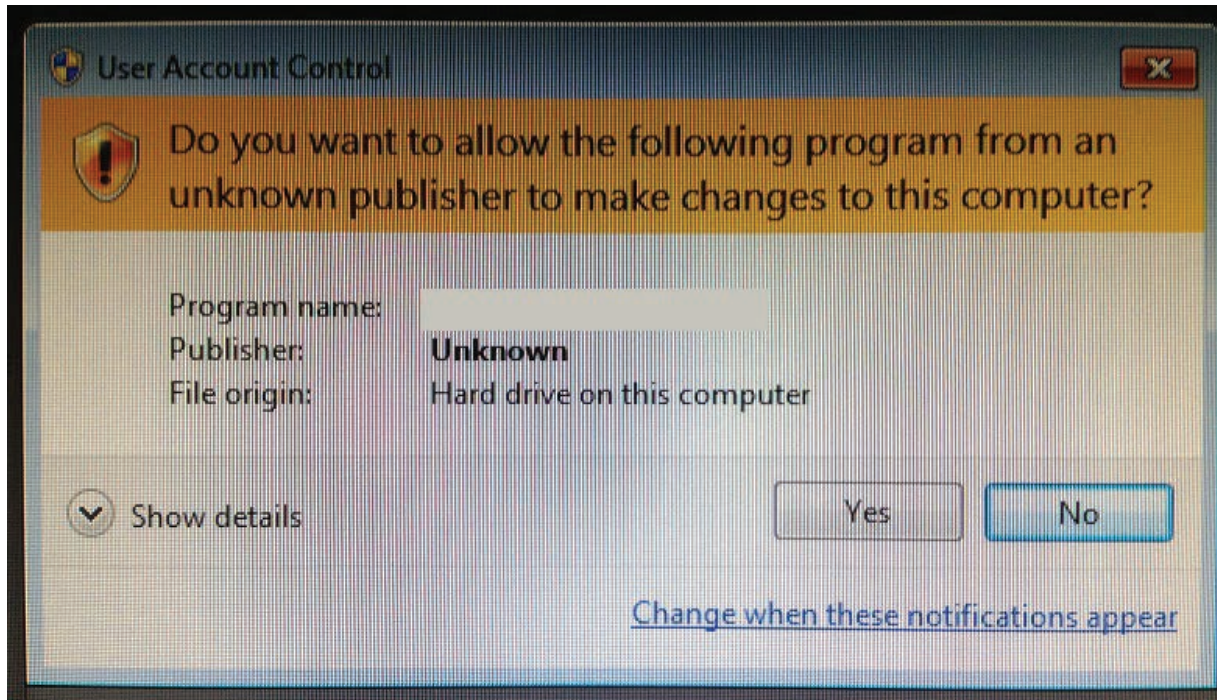
Step-by-Step Installation

The Accessory Add-On should be installed wherever the OnGuard® Communication Server is installed. This may be only one computer at the customer's site. Only one installation is needed because the Accessory Add-On adds functionality to the Communication Server, which then distributes alarms to all computers running the OnGuard® Alarm Monitoring application. The customer should execute the Accessory Add-On installer file by double-clicking on it. It will run the installer on-screen. If the installer file is still in a ZIP file, the customer will need to unzip it first.

When the installation window appears, press the "Install" button to continue.

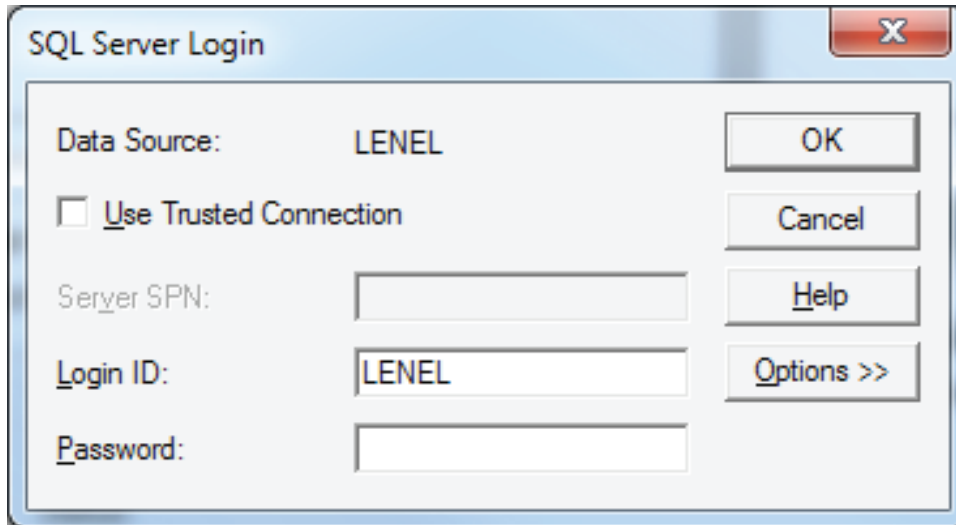


The installer will be installing the Accessory Add-On to the computer. A window may appear asking if the customer wants to allow the installer to make changes to the computer. Click “Yes” to allow.

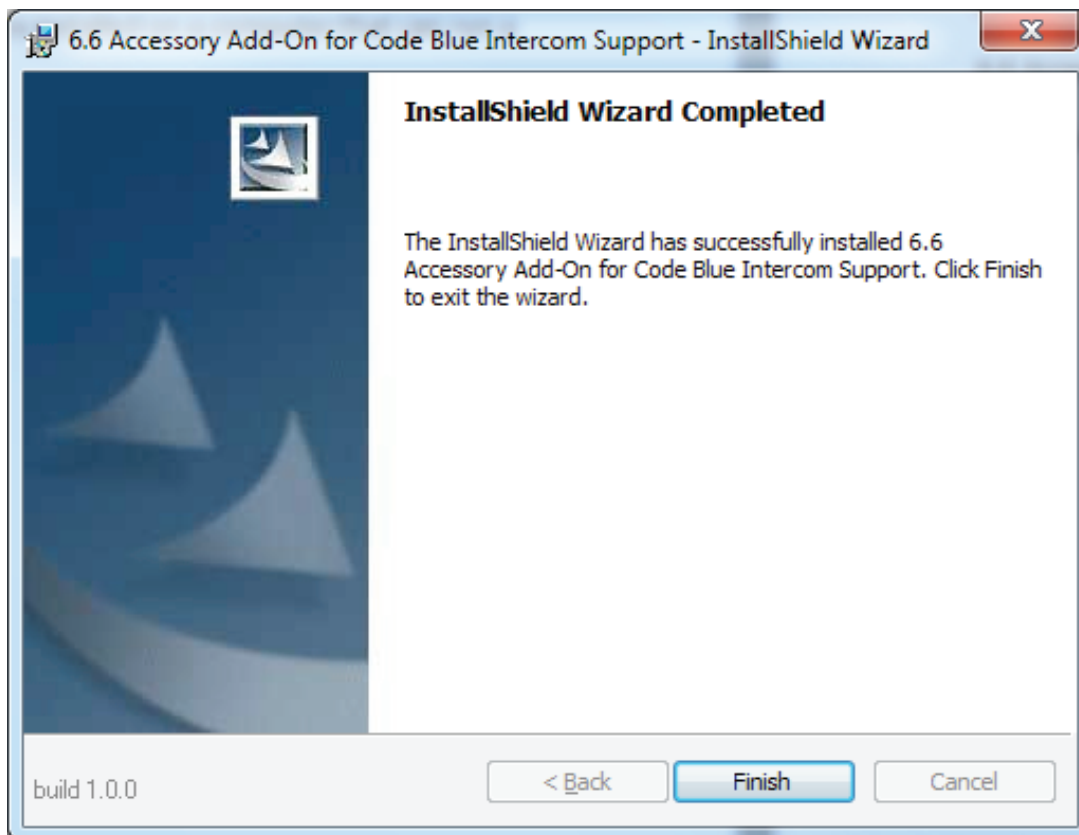




Next, the SQL Server Login window will appear. In the “Password” field, the customer should enter the password for the database that is part of OnGuard®. This password was likely set by the customer when OnGuard® was installed. Code Blue will not know this password.



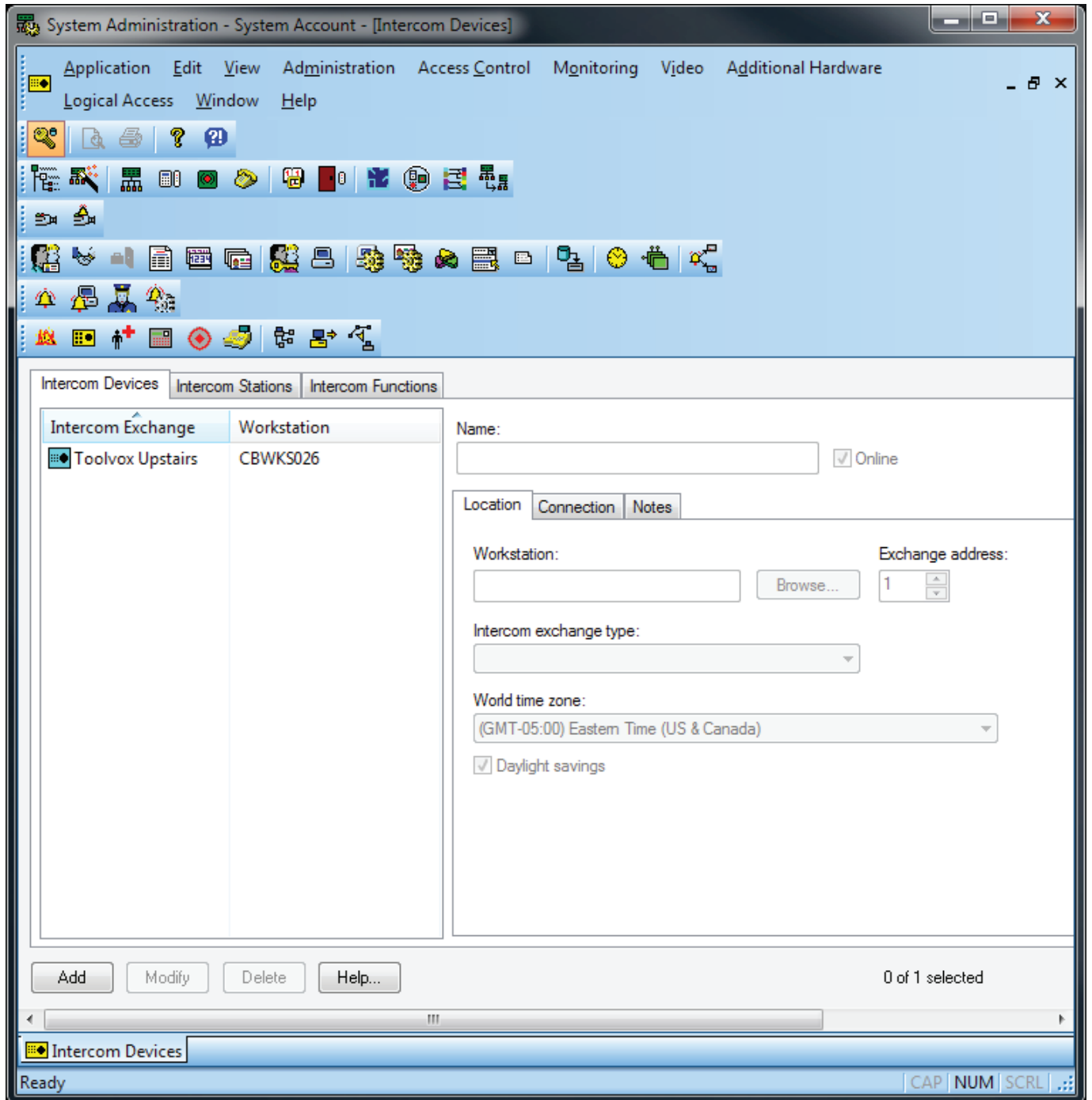
On the next screen, press “Finish” to complete the installation process.





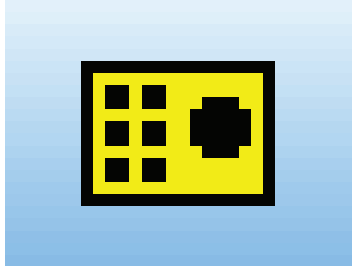
Verify that the Accessory Add-On has been installed

Open the OnGuard® System Administration application.

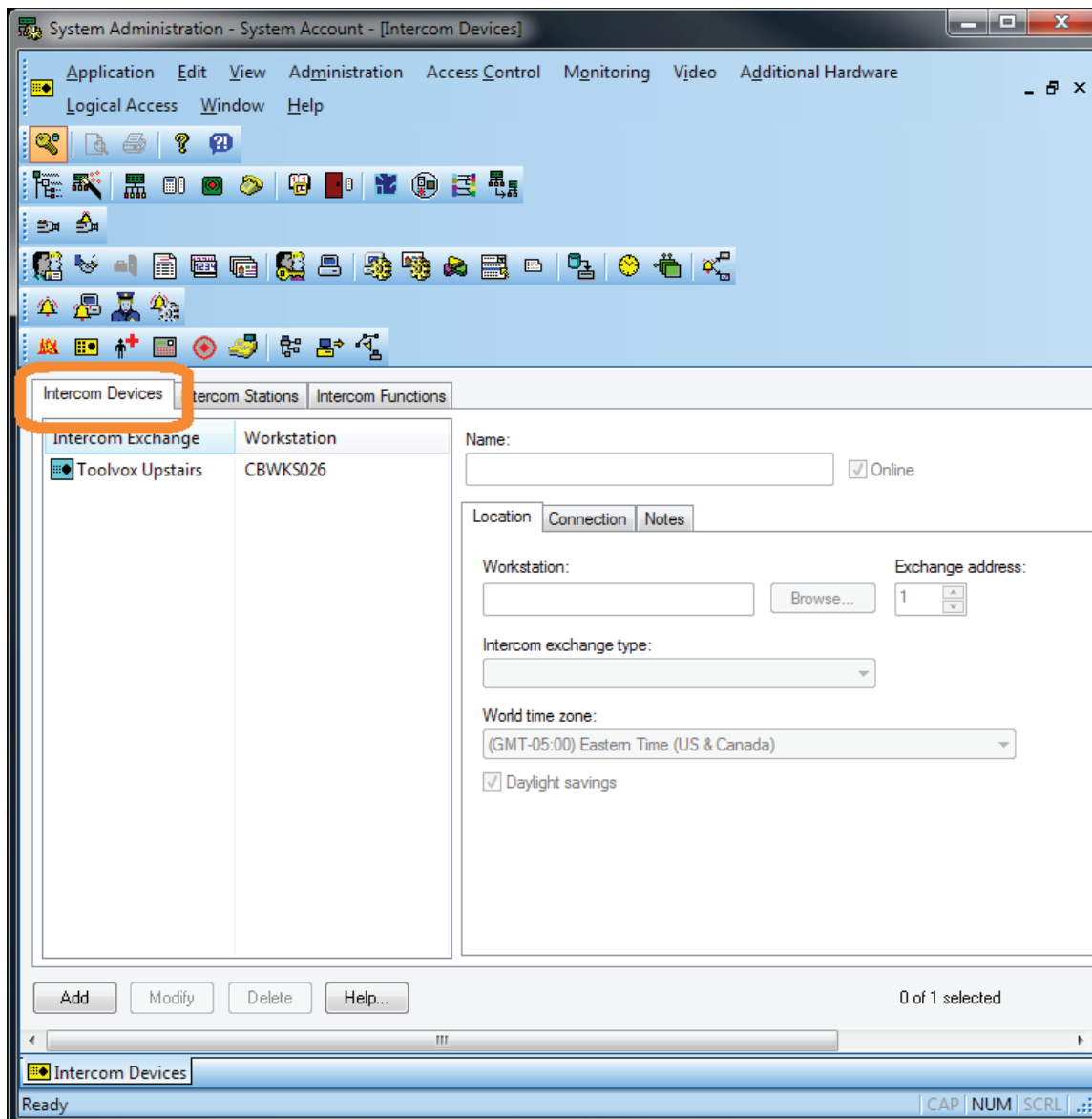




Open the Intercoms configuration screen by clicking on the yellow rectangle icon with black dots



There are three tabs: Intercom Devices, Intercom Station and Intercom Functions. Click on Intercom Devices.

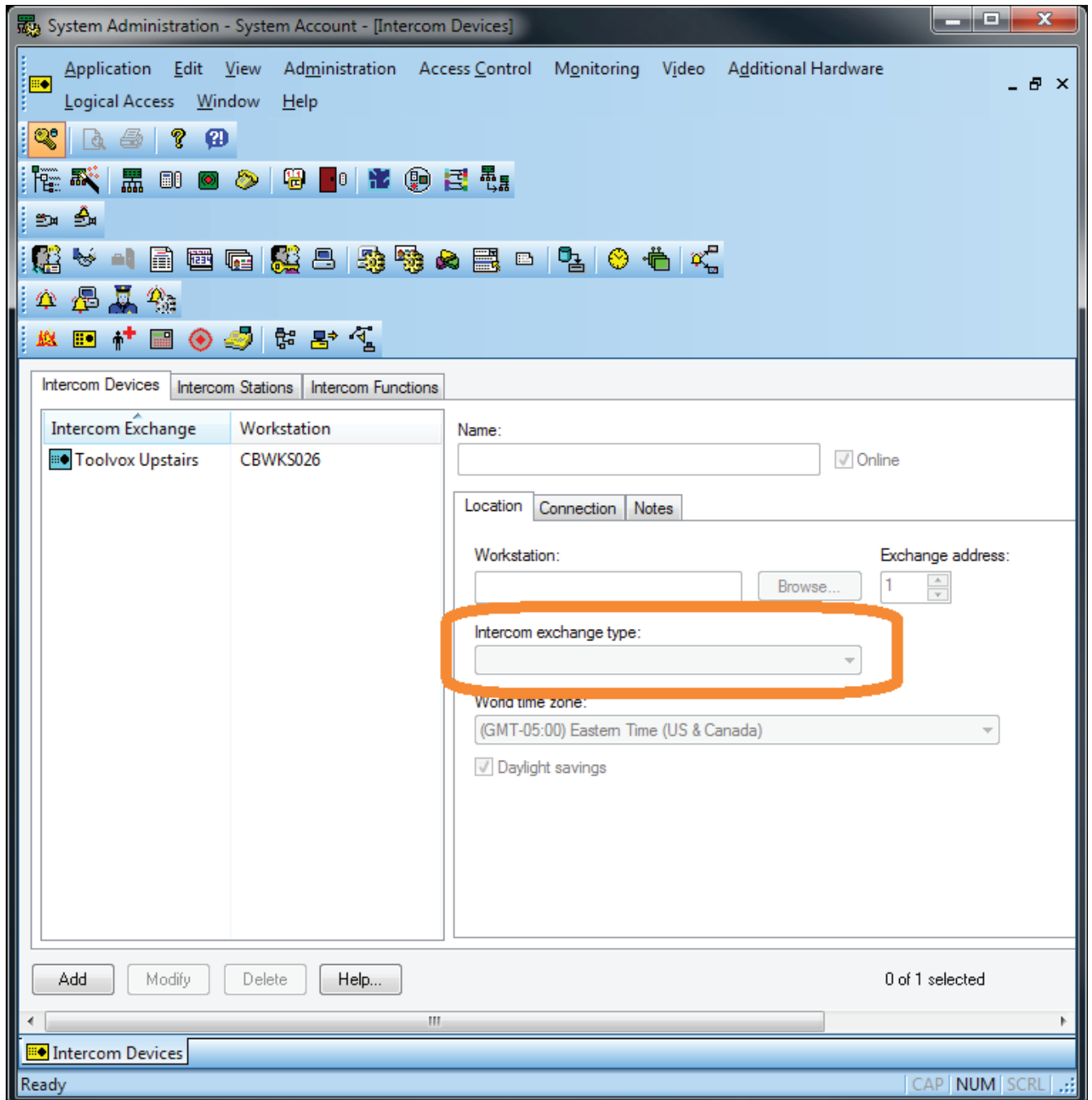




On the left is a list of Intercom Exchanges. This is where ToolVox® units will be listed.

On the right are configurable settings.

In the dropdown menu labeled “Intercom exchange type”, you should see “Code Blue Intercom” listed. If you see it, the Add-On was successfully installed.





Configuration

Configuration of Code Blue hardware must be performed before using the Accessory Add-On. This chapter is divided into four sections:

- Configuring Code Blue speakerphone devices within ToolVox®
- Configuring telephones within ToolVox®
- Configuring ToolVox® units within OnGuard®
- Configuring speakerphones and telephones within OnGuard®

Configuring ToolVox® units within OnGuard®

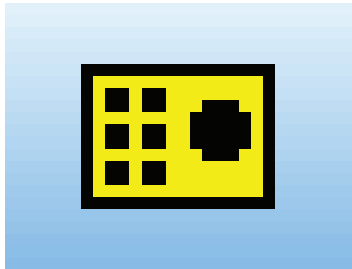
Overview

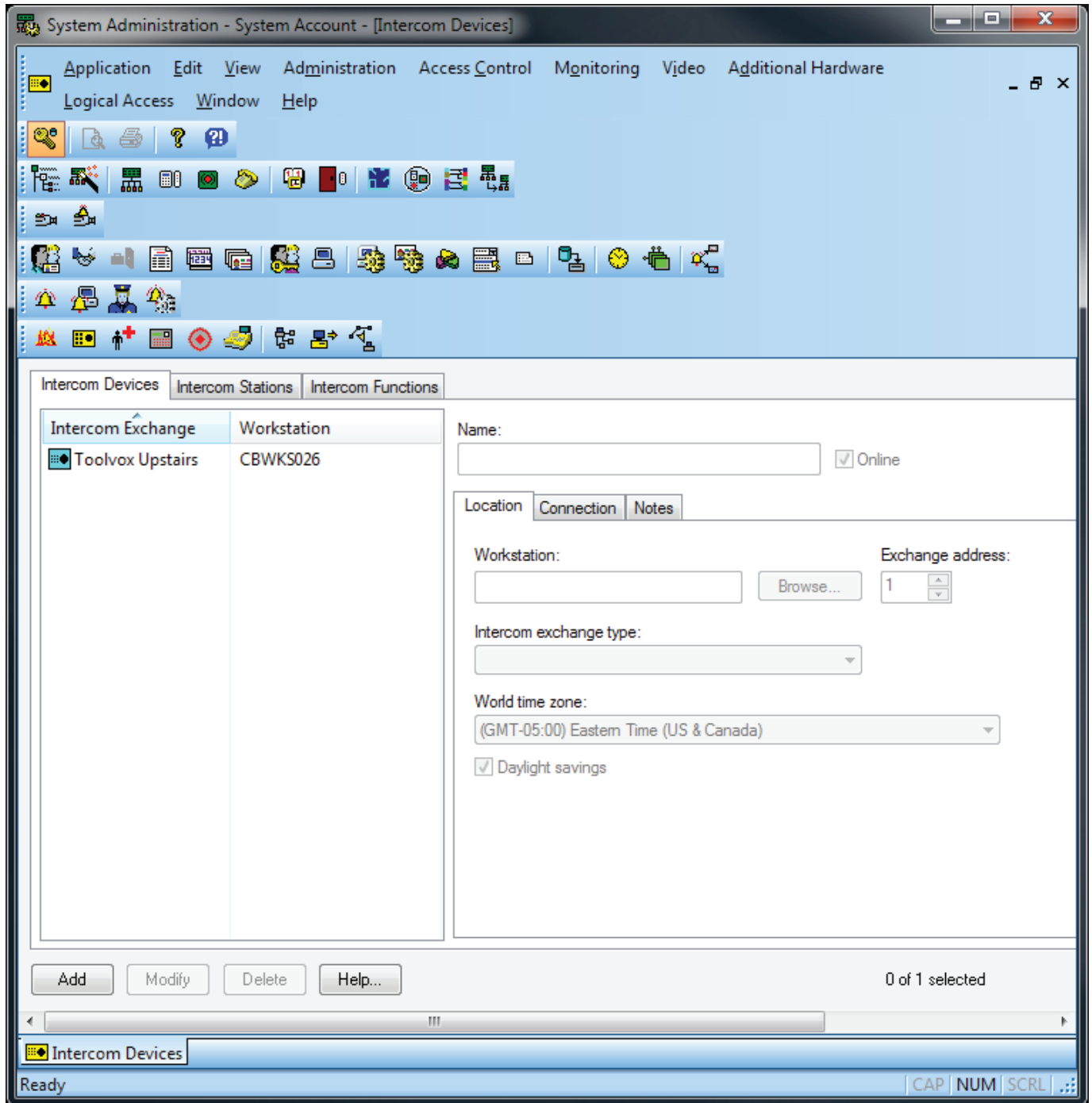
Before you can use OnGuard® to monitor calls made with Code Blue devices, you must enter the ToolVox® units into the OnGuard® software. This is done in the OnGuard® System Administration application.

Step-by-Step Instructions

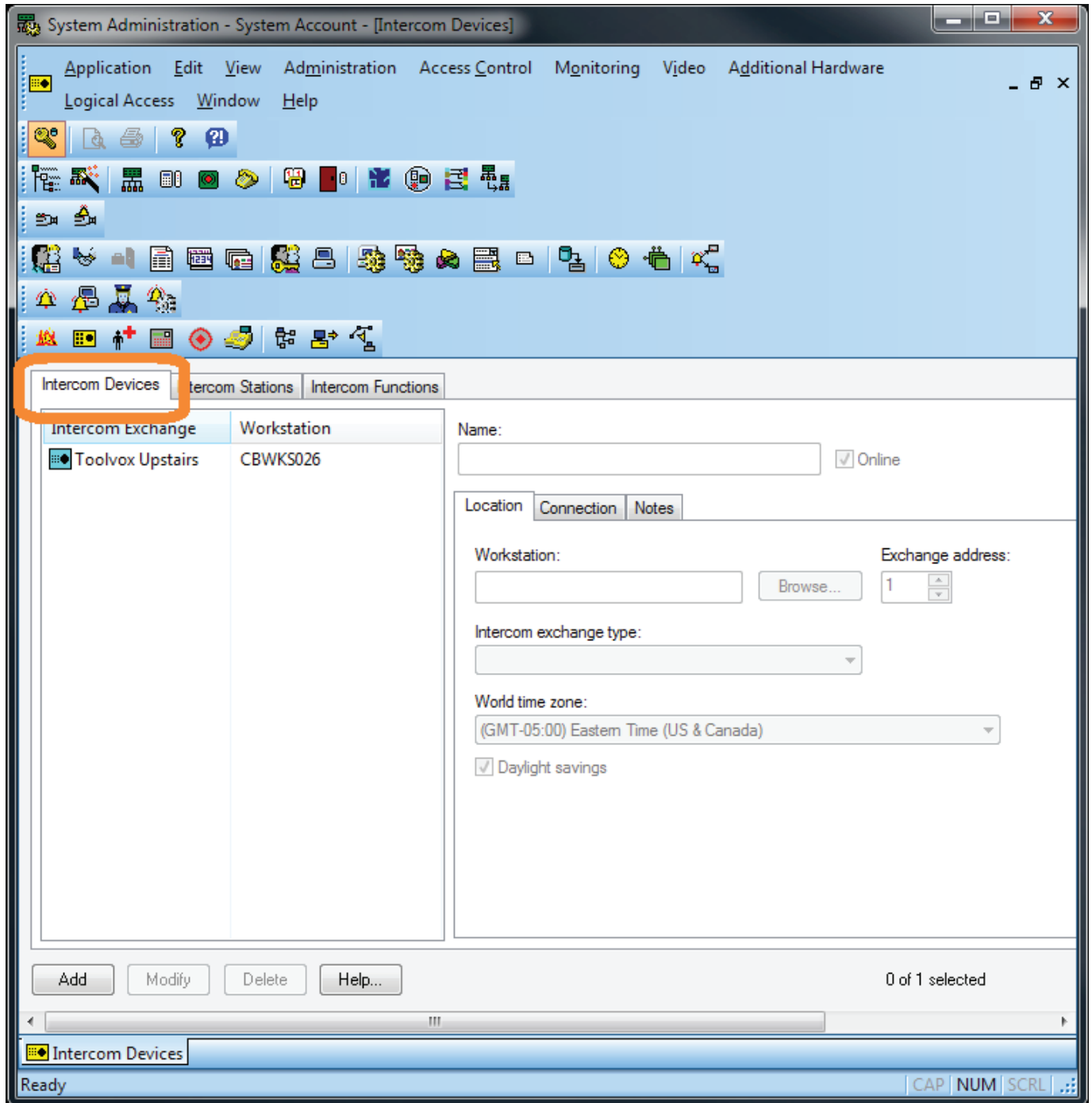
Open the OnGuard® System Administration application and log in. The customer will have the username and password to log into the OnGuard® system. Code Blue will not know this information.

Open the Intercoms configuration screen by clicking the yellow rectangular icon with black dots .



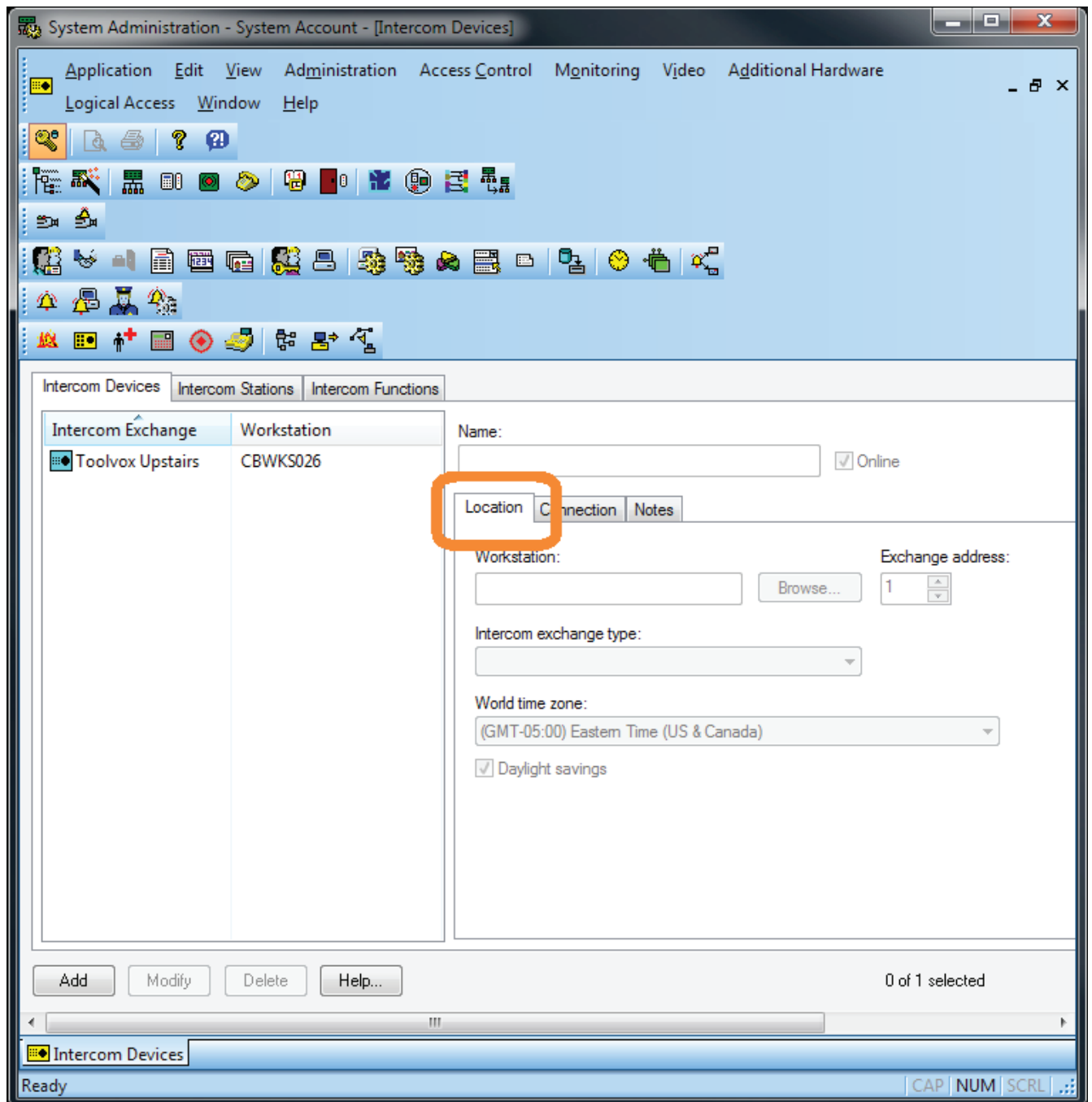


There are three tabs: Intercom Devices, Intercom Stations and Intercom Functions. Click “Intercom Devices”.



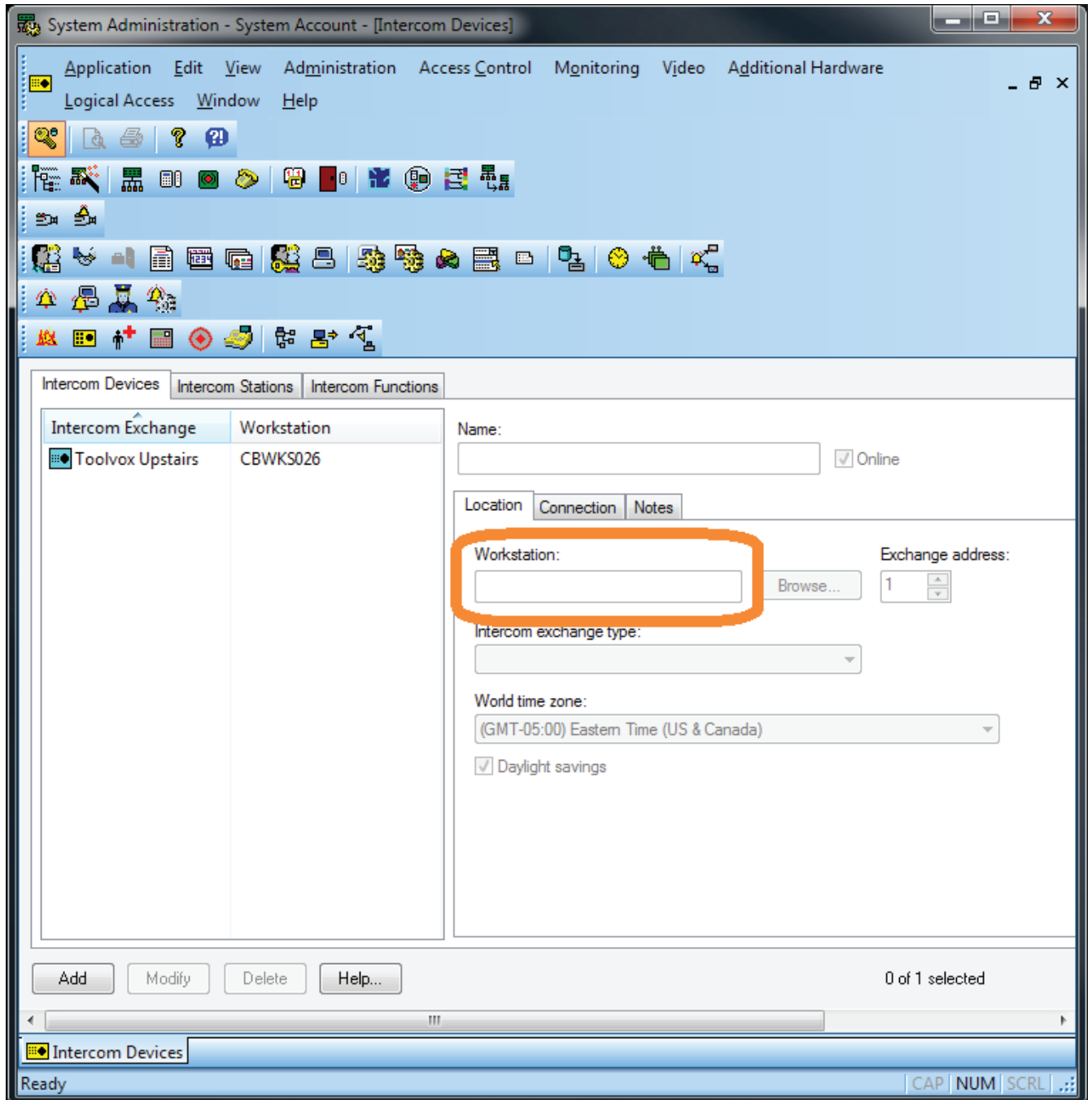


On the right side of the screen, you should see three tabs: Location, Connection and Notes. Click "Location".



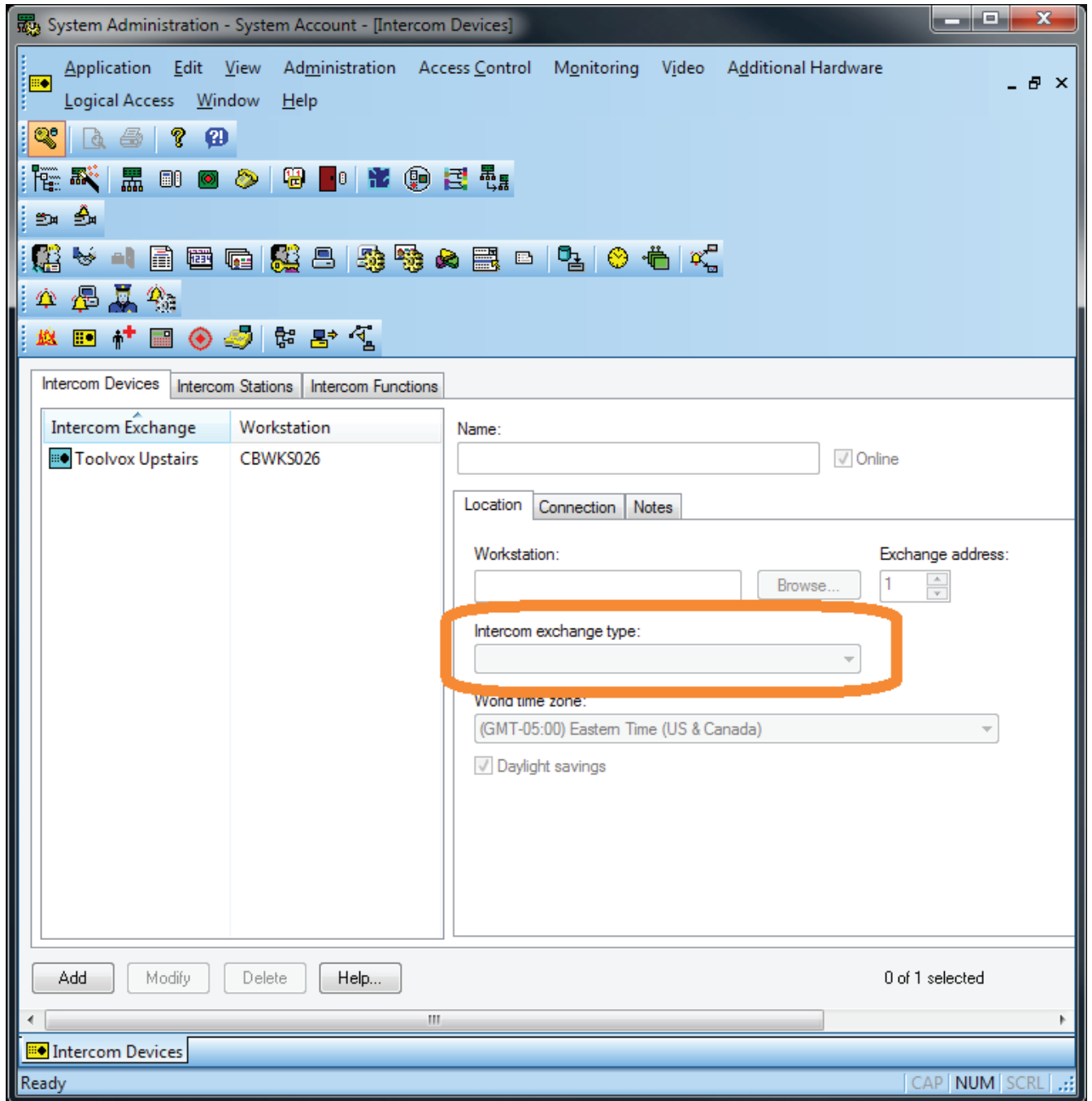


In the field labeled 'Workstation,' enter the name of the computer running Level Communication Server.





Using the dropdown menu labeled “Intercom exchange type”, select “Code Blue Intercom”.





Click the Connection tab.

The screenshot shows a configuration window for a device. At the top, there is a 'Name:' field and an 'Online' checkbox. Below this is a tabbed interface with three tabs: 'Location', 'Connection', and 'Notes'. The 'Connection' tab is highlighted with an orange rectangle. Under the 'Connection' tab, there are two radio button options: 'Direct' and 'LAN'. The 'Direct' option is selected. For 'Direct', there is a 'COM port:' dropdown menu showing '1' and a 'Baud rate:' dropdown menu. For the 'LAN' option, there is an 'IP address:' field and a 'Port:' field showing '3001'. At the bottom of the window, it says '0 of 2 selected' and there is a 'Close' button.



Select the “LAN” radio button and enter the IP address of the ToolVox® server you are creating a panel for.

The screenshot shows a configuration window for a ToolVox unit. At the top, there is a "Name:" field and an "Online" checkbox. Below this are three tabs: "Location", "Connection", and "Notes". The "Connection" tab is active and contains two radio button options: "Direct" and "LAN". The "Direct" option is currently selected. To the right of "Direct" are fields for "COM port:" (set to 1) and "Baud rate:". The "LAN" option is highlighted with an orange oval. To the right of "LAN" are fields for "IP address:" (containing three dots) and "Port:" (set to 3001). At the bottom of the window, it says "0 of 2 selected" and has a "Close" button.

In the field to the right, enter the port number that was configured in the ToolVox® APL

Repeat for any other ToolVox® units.



Configuring speakerphones and telephones within OnGuard®

Overview

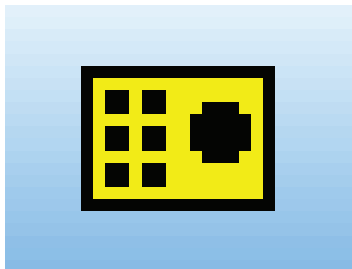
Before calls can be monitored in OnGuard®, devices and telephones must be added. This is done using the System Administration application.

The System Administration application refers to both Code Blue speakerphone devices and telephones as “stations”. If a customer asks about “stations”, it is any hardware device that users interact with. In this case, “users” includes both the people who press the speakerphone buttons and the security personnel who answer the phone. All of these “stations” must be entered in the “Intercom Stations” form.

Step-by-Step Instructions

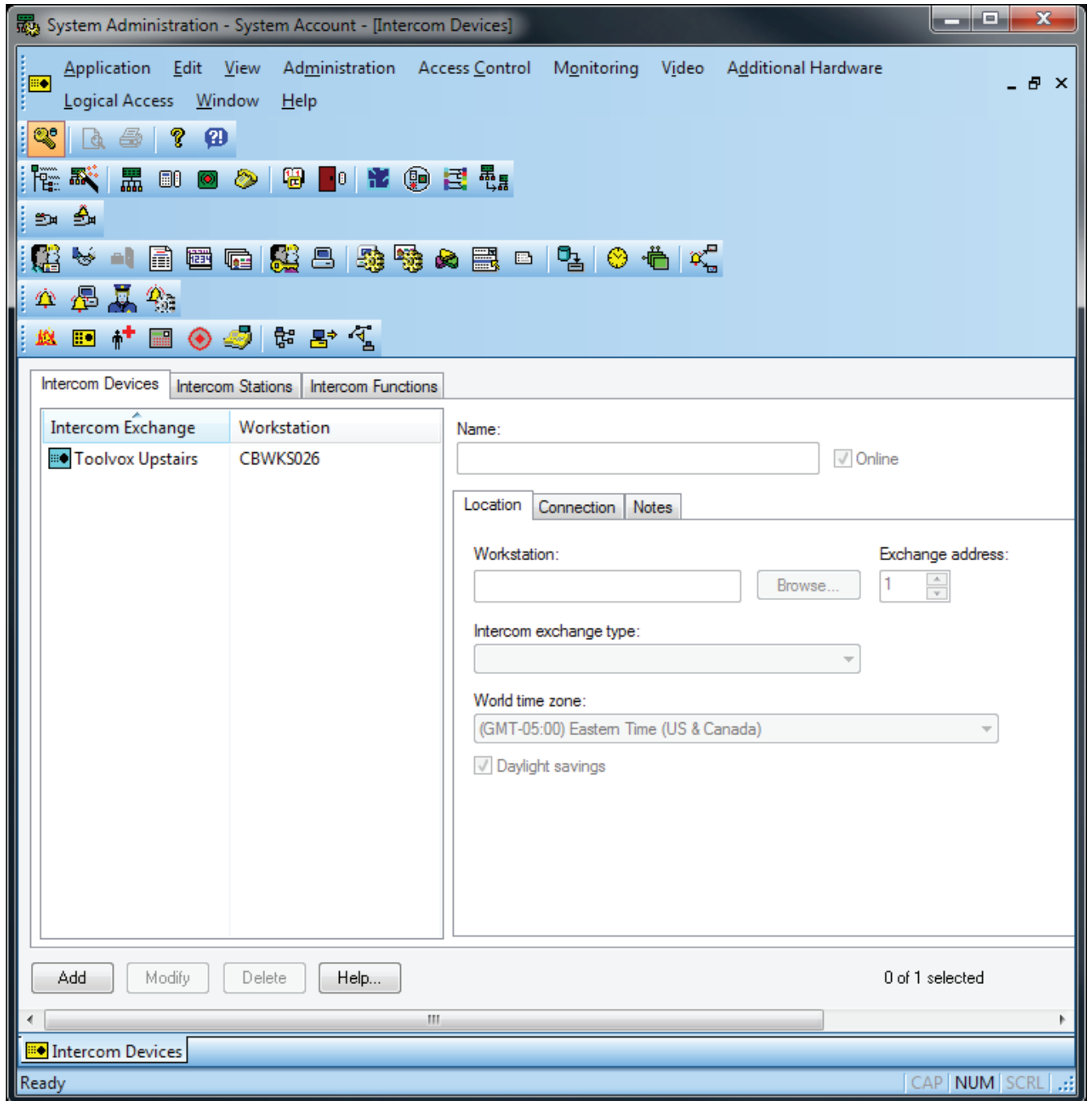
Open the OnGuard® System Administration application and log in. The customer will have the username and password to log into the OnGuard® system. Code Blue will not know this information.

Open the Intercoms screen by clicking the yellow rectangular icon with black dots.



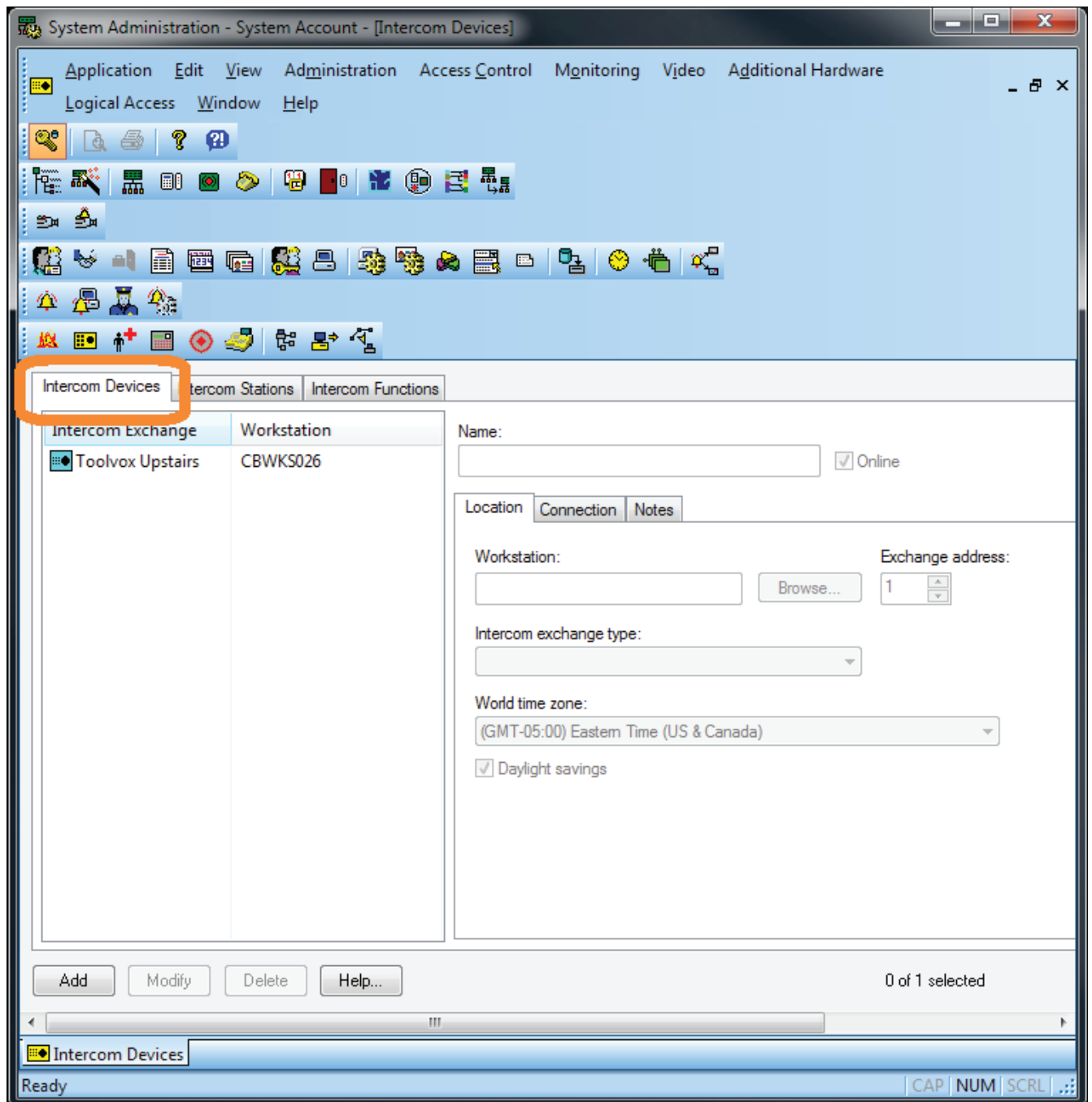


This screen will appear:



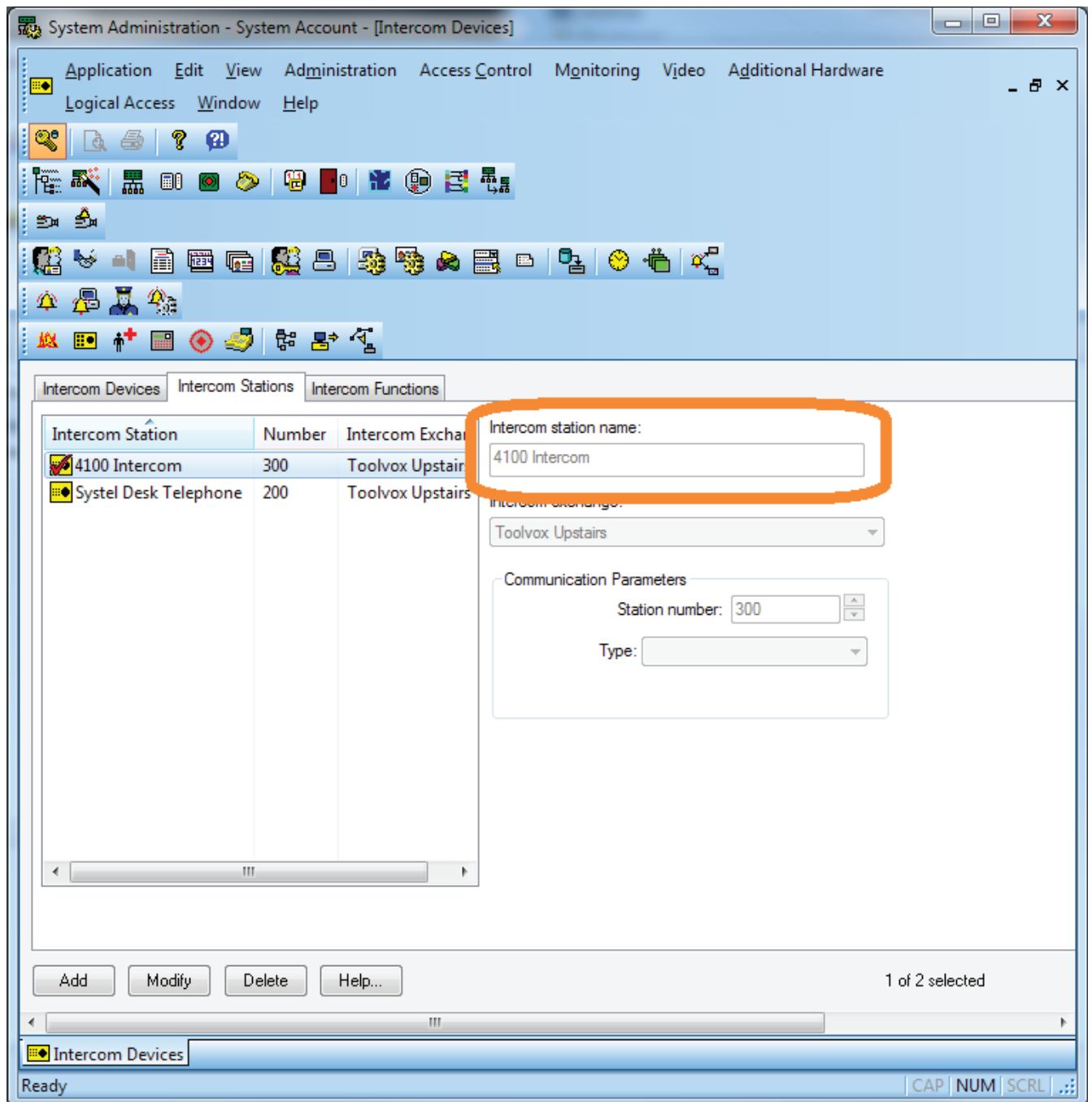


There are three tabs: Intercom Devices, Intercom Stations and Intercom Functions. Click “Intercom Stations”.



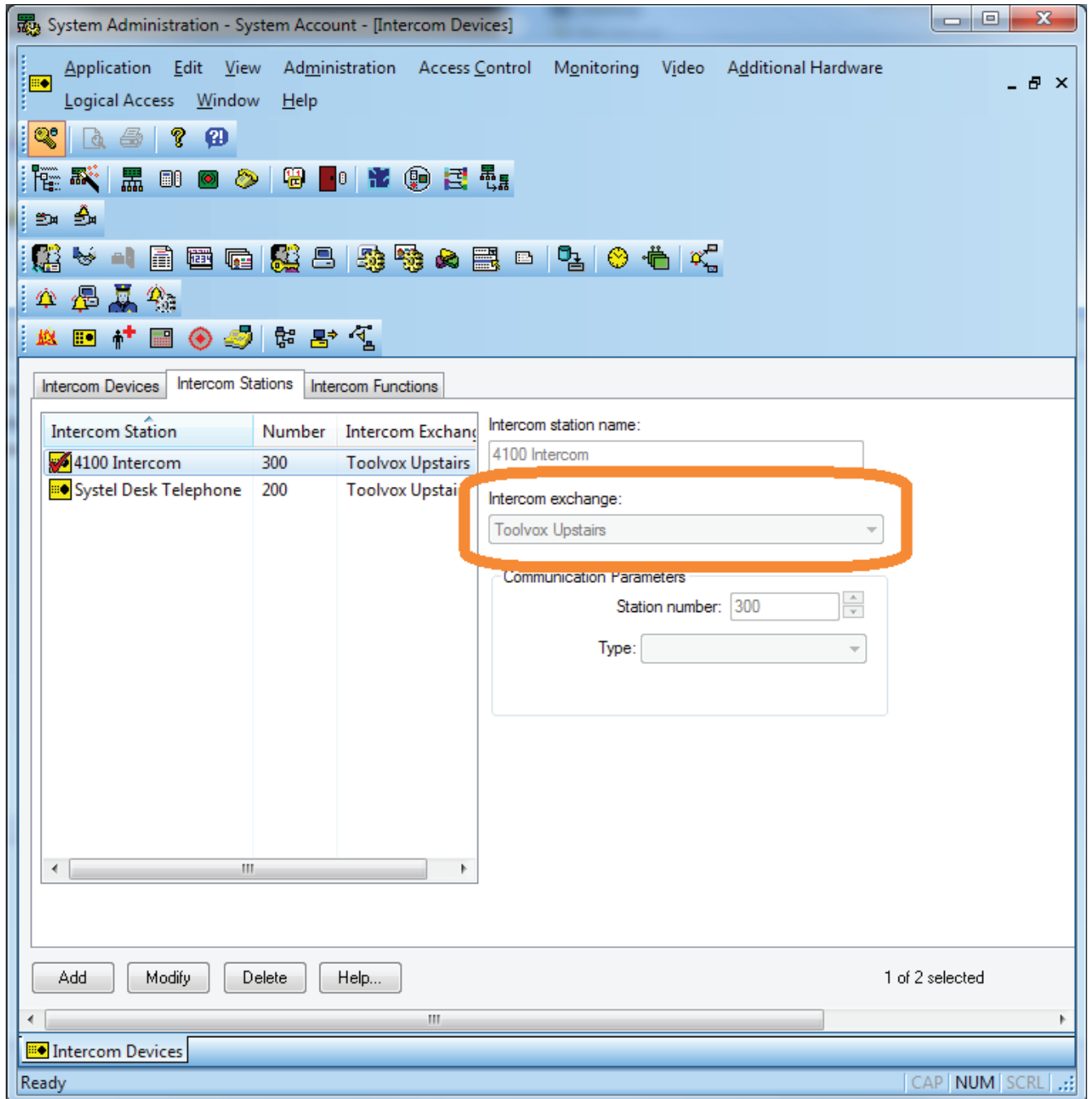


Enter a descriptive name for the device/telephone into the “Intercom station name” text field. Whatever you enter here will show up in alarms.



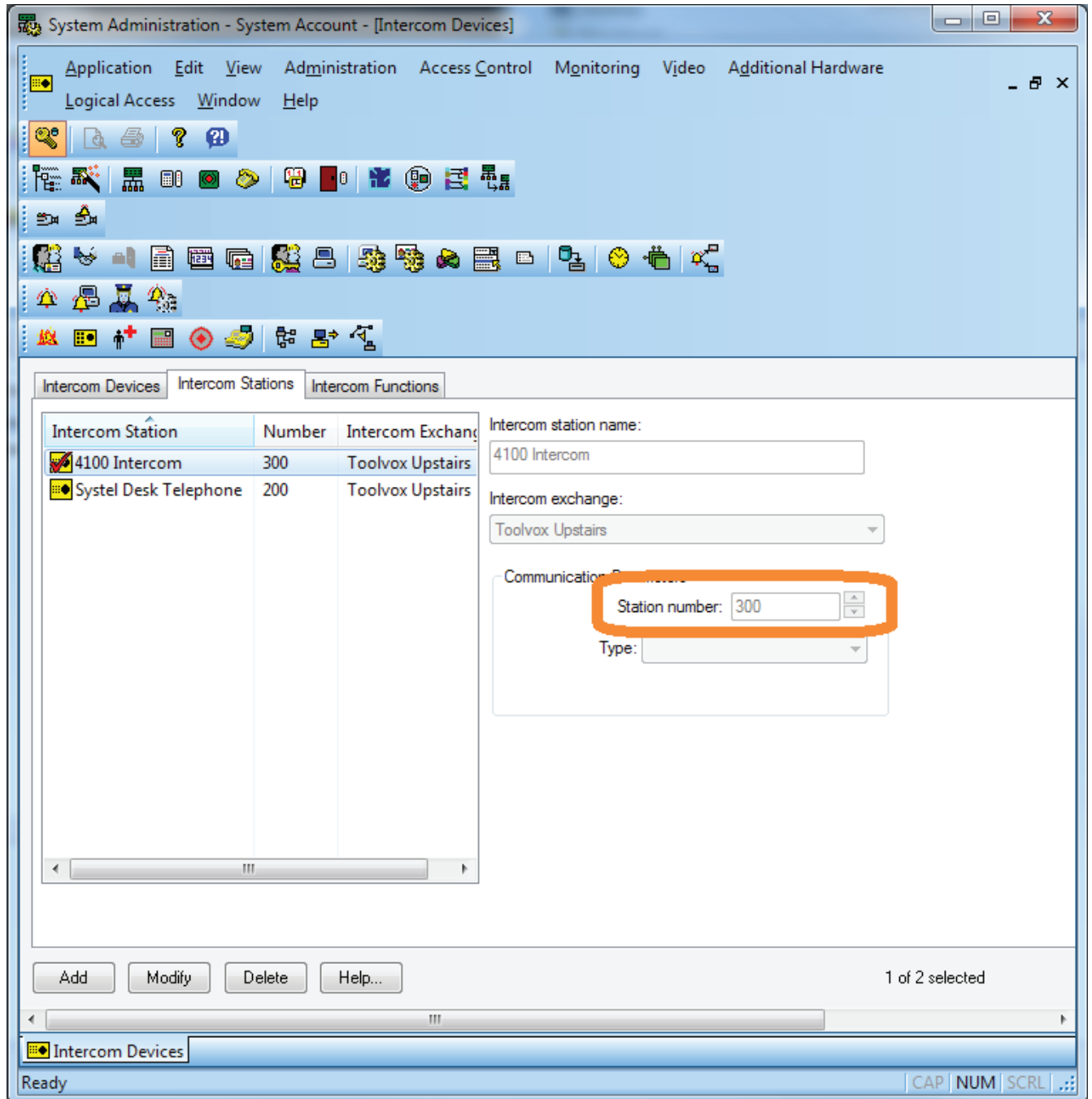


Use the “Intercom exchange” dropdown menu to select the ToolVox® unit that this speakerphone or telephone will connect through. ToolVox® units will not show up in the dropdown menu until they have been entered in the “Intercom Devices” tab.





Under the “Intercom exchange” dropdown menu, there is a field labeled “Station number”. Enter the extension number of the device/telephone.



Repeat for the rest of the speakerphone devices and telephones.



Monitoring Alarms in OnGuard®

Introduction

The central purpose of the Accessory Add-On for Code Blue Intercom Support is to notify security personnel when someone is using a Code Blue speakerphone device. This section describes how to interpret the alarms that are generated by the Accessory Add-On. The customer should already have an understanding of how to use the OnGuard® Alarm Monitoring application.

Anatomy of a Call

A call, in the context of ToolVox®, involves two devices, typically one Code Blue speakerphone and one telephone.

ToolVox® defines four phases to each call:

- DIAL - A device is dialing another device
- LINK - Two devices are connected and audio is being transmitted between them
- UNLINK - Two devices are disconnected and audio stops transmitting
- HANGUP - A device is hung up and is not able to be linked or start dialing

An alarm is sent to the Alarm Monitoring application for each of the four call phases. Since the HANGUP event happens for both devices, five alarms are generated when someone initiates a call with a Code Blue speakerphone device:

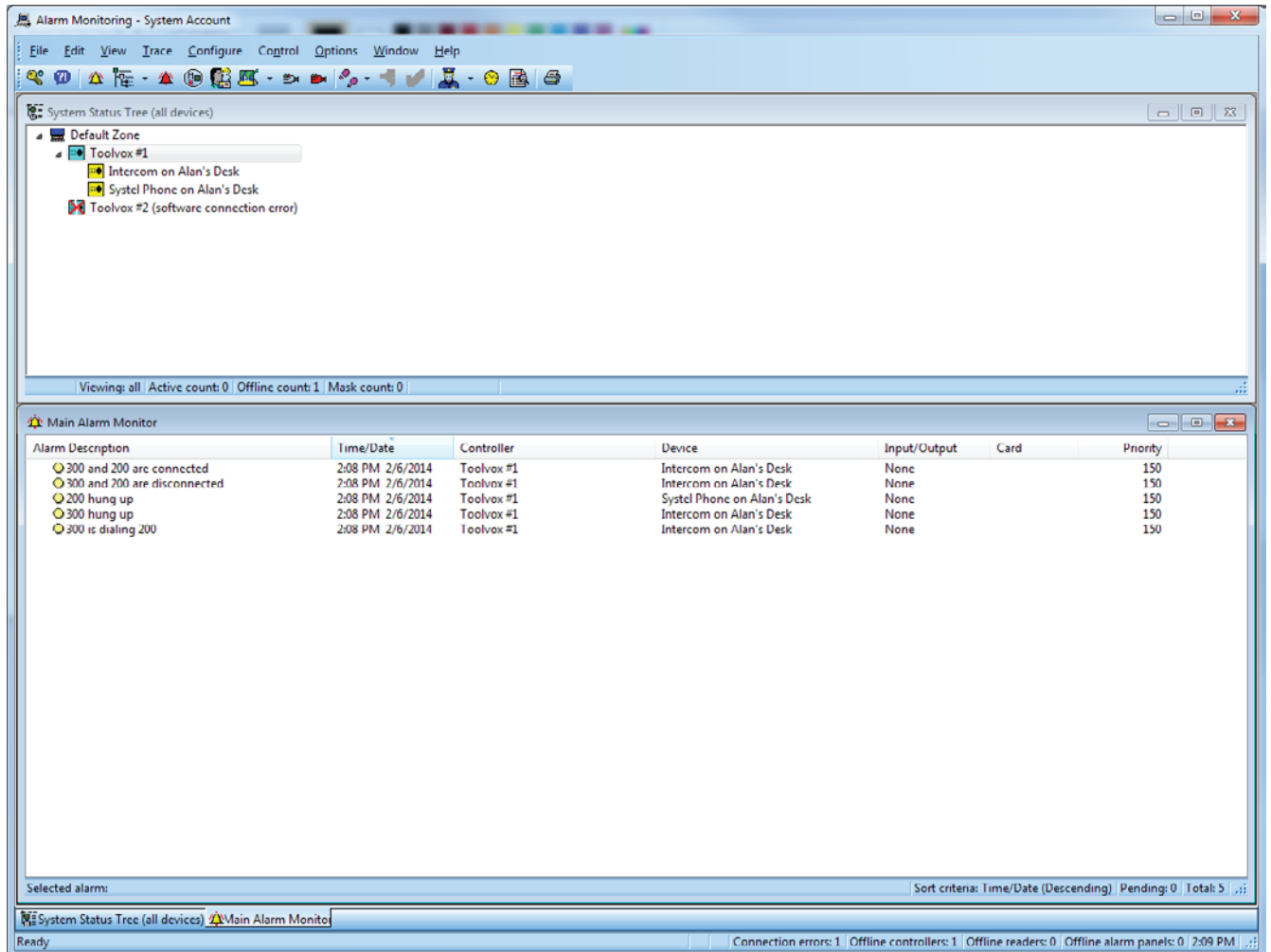
- DIAL - Speakerphone is dialing telephone
- LINK - Speakerphone is linked to telephone
- UNLINK - Speakerphone and telephone are unlinked
- HANGUP - Speakerphone is hung up (happens automatically)
- HANGUP - Telephone hangs up (hung up by user)

Brief Overview of the Alarm Monitoring Interface

This section only describes the parts of the Graphical User Interface (GUI) that are relevant to this Accessory Add-On.



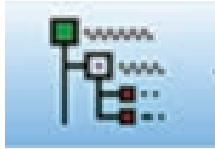
This is what the main interface of the OnGuard® Alarm Monitoring application looks like:



You can see that in this screenshot, two windows are open, one in the upper half and the other in the lower. The System Status Tree is open in the lower half. It lists all ToolVox® units, Code Blue devices and telephones. These appear once they are configured in the System Administration application. You may need to restart the Alarm Monitoring application for configuration changes to appear.



You can open the System Status Tree by clicking this icon in the top menu:



The System Status Tree lists ToolVox® units, speakerphone devices and telephones. Devices will only show up if they have been configured in the System Administration application.

Alarm Monitoring - System Account

System Status Tree (all devices)

- Default Zone
 - Toolvox #1
 - Intercom on Alan's Desk
 - System Phone on Alan's Desk
 - Toolvox #2 (software connection error)

Viewing: all | Active count: 0 | Offline count: 1 | Mask count: 0

Main Alarm Monitor

Alarm Description	Time/Date	Controller	Device	Input/Output	Card	Priority
300 and 200 are connected	2:08 PM 2/6/2014	Toolvox #1	Intercom on Alan's Desk	None		150
300 and 200 are disconnected	2:08 PM 2/6/2014	Toolvox #1	Intercom on Alan's Desk	None		150
200 hung up	2:08 PM 2/6/2014	Toolvox #1	System Phone on Alan's Desk	None		150
300 hung up	2:08 PM 2/6/2014	Toolvox #1	Intercom on Alan's Desk	None		150
300 is dialing 200	2:08 PM 2/6/2014	Toolvox #1	Intercom on Alan's Desk	None		150

Selected alarm: Sort criteria: Time/Date (Descending) | Pending: 0 | Total: 5

System Status Tree (all devices) | Main Alarm Monitor

Ready | Connection errors: 1 | Offline controllers: 1 | Offline readers: 0 | Offline alarm panels: 0 | 2:09 PM



The Main Alarm Monitor lists alarms.

The screenshot shows the 'Alarm Monitoring - System Account' application window. The 'Main Alarm Monitor' window is highlighted with an orange border and contains the following table:

Alarm Description	Time/Date	Controller	Device	Input/Output	Card	Priority
300 and 200 are connected	2:08 PM 2/6/2014	Toolvox #1	Intercom on Alan's Desk	None		150
300 and 200 are disconnected	2:08 PM 2/6/2014	Toolvox #1	Intercom on Alan's Desk	None		150
200 hung up	2:08 PM 2/6/2014	Toolvox #1	Systel Phone on Alan's Desk	None		150
300 hung up	2:08 PM 2/6/2014	Toolvox #1	Intercom on Alan's Desk	None		150
300 is dialing 200	2:08 PM 2/6/2014	Toolvox #1	Intercom on Alan's Desk	None		150

Below the table, the status bar shows: Selected alarm: [empty] Sort criteria: Time/Date (Descending) Pending: 0 Total: 5

The bottom status bar of the application shows: Ready Connection errors: 1 Offline controllers: 1 Offline readers: 0 Offline alarm panels: 0 2:09 PM



List of Possible Alarms

There are several alarms that can be generated by ToolVox®. This is a brief description of each:

- Dialing - A speakerphone device has been activated and is dialing a telephone.
- Connected - A speakerphone has dialed a telephone and the two are now connected.
- Disconnected - Happens when one device hangs up. Audio is no longer being transmitted between the devices.
- Hang up - A speakerphone was automatically hung up or a telephone was hung up.
- ToolVox® offline - Communication appears to have ceased from the ToolVox® unit.
- ToolVox® back online - The ToolVox® unit appears to be back online after having been offline.



Troubleshooting

Calls are made, but no events show up in Alarm Monitoring

Verify that devices and telephones have been added and configured properly in both ToolVox® and OnGuard® System Administration.

Device extensions entered in System Administration must match extensions configured in ToolVox®. Verify that all IP Addresses are accurate.

ToolVox® may be down. It may take up to 65 seconds for the panel to be marked as offline.

Red X appears over panel icon in Alarm Monitoring

ToolVox® may be down. If it was recently turned on, it may take up to 65 seconds for communication to be restored. When communication is restored, the red X will disappear.

Device/Panel/Intercom Exchange/Intercom Station icon doesn't show up in Alarm Monitoring

Verify that the missing item has been added to OnGuard® System Administration. Log out of Alarm Monitoring, then log back in.

If the item exists in System Administration but continues to not show up in Alarm Monitoring, you may need to contact Lenel.

The "Device" column in Alarm Monitoring/Main Alarm Monitor says <Unknown> or is not showing the device name.

Device names are pulled from OnGuard® System Administration. Make sure that the devices have been added to System Administration.

The Station Number configured in System Administration must match the extension number configured in ToolVox®. If the extensions do not match, the device name will not show up in Alarm Monitoring.

Unable to place call, call intercom or cancel call

Right-clicking on a panel or device in Alarm Monitoring will bring up a menu which may include options, such as:

- Place Call
- Cancel Intercom
- Cancel Call

These currently do nothing and it is not possible to place or cancel calls using the Graphical User Interface (GUI). This functionality may be added in future versions.



16.3 Cisco Call Manager



Configure the Cisco Unified Call Manager

- Open a browser window and type in the IP address of your Cisco Unified Call Manager (CUCM).
- Log on to Cisco Unified CM Administration with the proper Username and Password provided by your CUCM Administrator.
- Execute the following configuration: (Parameters not mentioned should be left untouched to their default setting)

Configure a Date/Time Group

System -> Date/Time Group -> Add New

- Group Name: Code Blue
- Time Zone: Choose your time zone
- Separator: -(dash)
- Date Format: Choose your date format
- Time Format. Choose your time format
- Press Save
- Press Reset/Restart

Configure a Region

System -> Region -> Add New

- Name: Code Blue
- Press Save
- Press Reset/Restart



Configure a SIP Trunk Security Profile

System -> Security -> SIP Trunk Security Profile -> Add New

- Name: ToolVox
- Description: ToolVox SIP Secure Profile
- Device Security Mode: Non Secure
- Incoming Transport Type: TCP+UDP
- Outgoing Transport Type: UDP
- Enable:
 - Accept Presence Subscription
 - Accept Out-of-Dialog REFER
 - Accept Unsolicited Notification
 - Accept Replaces Header
- Press Save
- Press Reset/Restart

Configure a Route Partition

Call Routing -> Class of Control -> Partition -> Add New

- Name: AllLines
- Press Save
- Press Reset/Restart

Configure a Calling Search Space

Call Routing -> Class of Control -> Calling Search Space -> Add New

- Name: DefaultUser
- Description: DefaultUser
- Select AllLines in the "Available Partitions" window and use the "Move Down" arrow to move it to the "Selected Partitions" window.
- Press Save



Configure a Media Resource Group

Media Resources -> Media Resource Group -> Add New

- Name: ToolVox
- Description: ToolVox_MRG
- Select MTP_2 in the "Available Media Resources" window and use the "Move Down" arrow to move it to the "Selected Media Resources" window.
- Press Save
- Press Reset/Restart

Configure a Media Resource Group List

Media Resources -> Media Resource Group List -> Add New

- Name: ToolVox_MRGL
- Select ToolVox_MRG in the "Available Media Resource Groups" window and use the "Move Down" arrow to move it to the "Selected Media Resource Groups" window.
- Press Save
- Press Reset/Restart

Configure a Device Pool

System -> Device Pool -> Add New

- Device Pool Name: Code Blue
- Cisco Unified Communications Manager Group: Default
- Calling Search Space for Auto-registration: DefaultUser
- Reverted Call Focus Priority: Default
- Date/Time Group: Code Blue
- Region: Code Blue
- Media Resource Group List: ToolVox_MRGL
- Location: Hub_None
- SRST Reference: Use Default Gateway
- Press Save
- Press Reset/Restart



Configure a Media Termination Point

Media Resources -> Media Termination Point -> Find, then select: MTP_2

- Set Device Pool: Code Blue
- Press Save
- Press Reset/Restart

Configure a SIP Trunk

Device -> Trunk -> Add New

- Trunk Type: SIP Trunk
- Device Protocol: SIP
- Press Next
- Device Name: ToolVox
- Description: ToolVox
- Device Pool: Code Blue
- Media Resource Group List: ToolVox_MRGL
- Enable: 'Media Termination Point Required'
- Calling Search Space: DefaultUser
- Destination Address: Your ToolVox IP address
- SIP Trunk Security Profile: ToolVox
- SIP Profile: Standard SIP Profile
- Press Save
- Press Reset/Restart

Configure a Route Group

Call Routing -> Route/Hunt -> Route Group -> Add New

- Name: ToolVox_RG
- Select ToolVox from "Available Devices" and press "Add to Route Group"
- Press Save



Configure a Route List

Call Routing -> Route/Hunt -> Route List -> Add New

- Name: ToolVox_RL
- Cisco Unified Communications Manager Group: Default
- Press Save
- Press Add Route Group
- Route Group: ToolVox_RG [NON-QSIG]
- Press Save
- Press Save
- Press Reset/Restart

Configure a Route Pattern

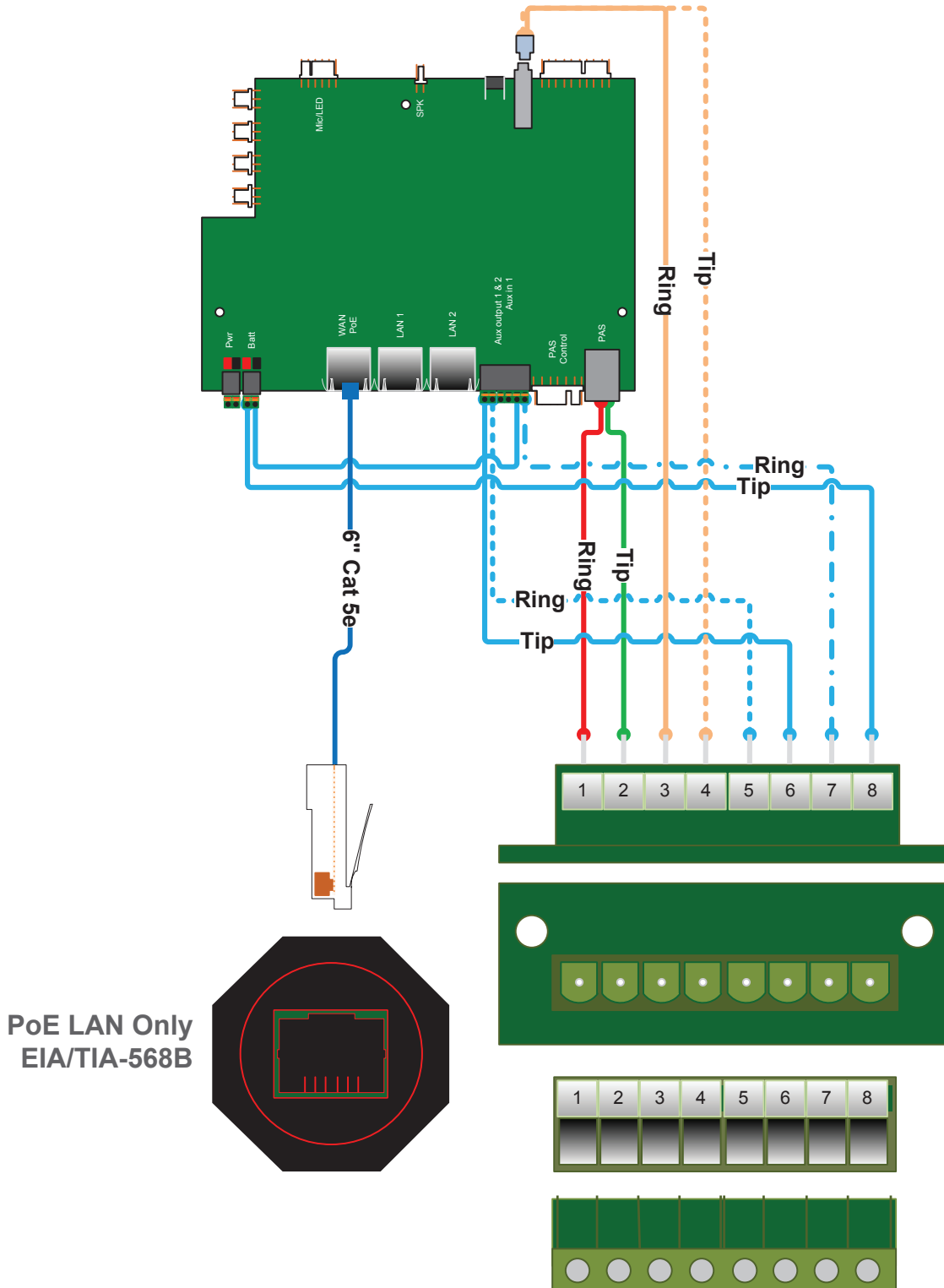
Call Routing -> Route/Hunt -> Route Pattern -> Add New

- Route Pattern: 2xxx (This allows calls to all numbers beginning with 2 in the ToolVox)
- Route Partition: AllLines
- Description: ToolVox_RP
- Gateway/Route List: ToolVox_RL
- Press Save

For ToolVox SIP Trunk Configuration, see Chapter 6 - Configuring Trunks.



17 IP Audio Interface Wiring Diagram



Product wiring diagram shown reasonably represents current offering and is intended to assist in component identification and service. Earlier product production may have different components and wiring connections. Reference the model and serial number from the unit ID tag and contact manufacturer to confirm replacement part version and availability.



18 Lightning Protection

Installation procedure for the recommended ToolVox Lightning Protection

ITW SurgeGate CO/25 Module

SurgeGate CO/25 modules are used to protect the ToolVox Analog FXO/FXS telephony card(s) and Adtran 624 units.

Installation

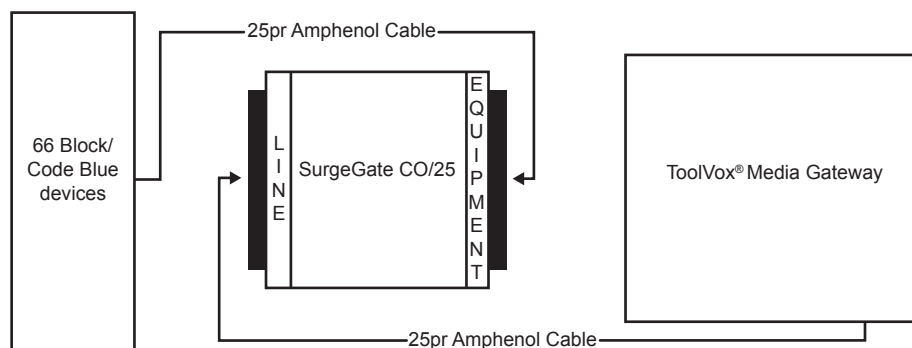
1. Install the Velcro clamps provided with the protector.



2. Securely mount the SurgeGate between the 66 block and the ToolVox Media Gateway.
3. Connect an Amphenol cable from the ToolVox to the “Line” side of the SurgeGate.

***Do not connect the SurgeGate directly to the back of the ToolVox. This will not provide adequate protection and will void the warranty.**

4. Connect an Amphenol cable from the 66 block to the “Equipment side of the SurgeGate. This will be the side the Code Blue devices.



5. Secure both Amphenol ends with the Velcro mounted on the clamps of the SurgeGate.



Important Safety Points

ITW Linx surge protectors and the connected equipment must be indoors in a dry location and in the same building. Although your protector is durable, its internal components are not isolated from the environment. Do not install any product near any heat-emitting appliances, such as a radiator or heat register. Do not install this product where excessive moisture is present.

ATTENTION

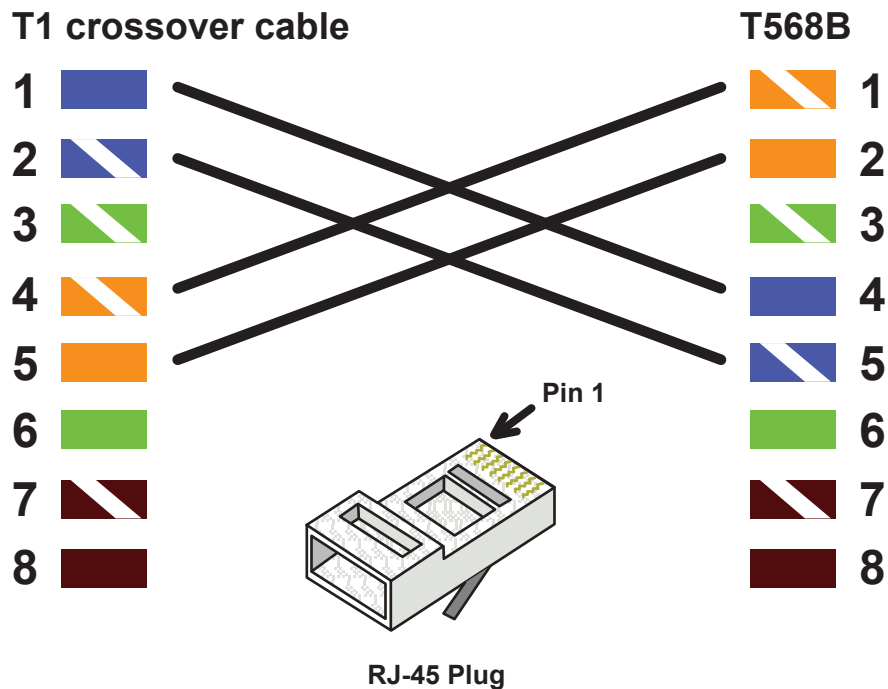
To ensure proper protection, the SurgeGate module **MUST BE CONNECTED TO EARTH GROUND**. There cannot be any exceptions. A minimum #14 green insulated copper wire, with a ring terminal at each end, should be used. Route the wire as directly as possible. Do not make any other connections to the ground terminal of the module.



T1 Crossover Cable Wiring

For customers utilizing an AdTran 624 or 850 with ToolVox®, a T1 pinout is required to establish a T1 connection from the ToolVox to the AdTran. A crossover cable must be used or the T1 will not synch with the opposite end.

To create a crossover cable, use the following pinout:



Once complete, connect your T1 crossover cable from the T1 port on the T1 card on the back of your ToolVox to the NTKW port on the AdTran 624 or 850.

If you have any questions, please call Code Blue Customer Service at [800-205-7186](tel:800-205-7186), opt. 2 or email customerservice@codeblue.com.



19 ToolVox DHCP Server Configuration

Considerations

This DHCP configuration is basic and will only work on the same subnet the ToolVox is on. Advanced configurations are possible, but advanced network administration is required.

This procedure will clear out existing ToolVox DHCP server configuration.

Do not start DHCP servers on networks that already have them. If done improperly, you may have consequences on your ethernet network with devices requesting DHCP.

Prerequisites

You will need the following information:

- ToolVox IP address
- Network address (e.g. 172.1.100.0)
- Subnet mask (e.g. 255.255.255.0)
- Default router or gateway address (e.g. 172.1.100.1)
- DNS server addresses, if any

Procedure

1. Sign in to the ToolVox server's Webmin interface, e.g. <https://IPofToolVox:2000/>
2. User Name = cbadmin; Password = codeblue
3. Navigate to Servers > DHCP Server.
4. Click the Configfile button.
5. Clear out the contents of the Edit window and replace it with the following, using the ToolVox server's IP address for the value of the tftp-server-name option (this is required for an IP5000 to pull its configuration from UPD on boot):

```
ddns-update-style ad-hoc;  
option tftp-server-name "IPofToolVox";
```

6. Click Save.
7. If you wish to have DHCP configure DNS servers, click Edit Client Options.
 - a. DNS servers: click the radio button next to the text box, and enter the DNS server address(es) separated by spaces, e.g. **DNSIP1 DNSIP2**
8. Click Save.
9. Under Subnets and Shared Networks, add a new subnet for the network the ToolVox server will be serving DHCP for:
 - a. Subnet description: a free-form descriptive name for the subnet
 - b. Network address: the network address of the subnet, e.g. 172.1.100.0
 - c. Netmask: subnet mask for the subnet, e.g. 255.255.255.0
 - d. Address ranges: IP addresses the DHCP server has the authority to hand out



10. Click Create.
11. Click on your newly created subnet and click Edit Client Options to edit the options that will be sent to this subnet:
 - a. Default routers, if any (required only if the devices will be communicating with other subnets): click the radio button next to the text box and enter the default router, e.g. 172.1.100.1
 - b. Subnet mask: click the radio button next to the text box and enter the subnet mask, e.g. 255.255.255.0
12. Click Save.
13. Navigate to System > Bootup and Shutdown.
14. Click dhcpd.
15. For Start at boot time?, click Yes.
16. Click Save.
17. Click dhcpd again.
18. Click Start Now.



20 Email - Postfix Setup for ToolVox X3

Logging into Postfix

10. Sign in to the ToolVox server's Webmin interface, e.g. <https://IPofToolVox:2000/>
11. User Name = cbadmin; Password = codeblue
12. Navigate to Servers > Postfix

General Options

The **General Options** page configures a number of options regarding the general behavior of Postfix. Specifically, most of the configuration options that impact all users and all messages are configured here. Postfix, keeping with its philosophy of simplicity, usually requires only a few configuration file changes to get a mail server running efficiently and securely.

The **General Options** page is divided into two parts. The upper section is labeled **Most Useful General Options** and the lower **Other General Options**. In many standard installations, it may be possible to start a Postfix installation with just the configuration of one or more of the three directives in the upper section. Unless otherwise stated, all of the options on this page correspond to directives in the main.cf file in the Postfix configuration directory.

Most Useful General Options

In some installations, these are the only three options that need to be altered to get Postfix running for both sending and receiving email.

Send outgoing mail via

This option configures whether outgoing mail should be delivered directly to the recipient's mail server or if a parent mail gateway should be used as an intermediary. If the server is behind a firewall, behind a network address translating router/gateway, or something similar, it may be necessary to use an intermediary server to achieve reliable service. Many mail servers on the Internet will not accept mail from a server that does not have a working DNS entry and routable IP address to help prevent spam from forged addresses. Also, local network use policy may require the use of an intermediary for logging, virus scanning or other purposes that require aggregation of outgoing mail traffic onto a central server. This option corresponds to the relayhost directive and defaults to sending mail directly.

What domain to use in outbound mail

Here you may specify the domain or host name to identify the source on outgoing mail. Postfix defaults to the host name of the server, but you likely will want it to identify mail as coming from your domain name instead. If your mail server will be accepting mail for a large number of users under a single domain name, you will likely configure a domain name here and create a domain-wide alias database to map user names to their respective local mail servers. This option correlates to the myorigin Postfix directive.

What domain to receive mail for

This option accepts a list of domains and addresses to receive mail as its final destination. In other words, when mail reaches the server destined for addresses in this field, it will deliver the mail to a



local user rather than forward it to another mail server. By default, this is all configured addresses on the machine, as well as localhost within the local domain. You may specify any number of domains or host names separated by commas, or you may provide a full path to a file containing similar entries. The variables `$myhostname` and `$mydomain` may be used to represent those concepts to Postfix automatically. The ability of Postfix to use such variables throughout its configuration files makes it easier to maintain a number of Postfix servers with similar configurations. This option correlates to the `mydestination` directive.

What trouble to report to the postmaster

Postfix provides the ability to select what types of error messages will be mailed to the designated postmaster of the mail server. Assuming you have set up a postmaster alias that directs mail to a real person, Postfix will send reports of all trouble designated here. The available classes are:

`bounce`

When this option is selected, whenever a message is undeliverable, a bounce message (called a single bounce message) will be sent to the message sender and the local postmaster. For the sake of privacy, only the headers will be sent to the postmaster. If the first bounce is returned as undeliverable, a double bounce message will be sent to the postmaster with the entire contents of the first single bounce message.

`2bounce`

Causes double bounce messages to be sent to the postmaster.

`delay`

If the delivery of a message is delayed, the postmaster will receive a notice, along with the headers of the delayed message.

`policy`

Notifies the postmaster of messages that were rejected due to an unsolicited commercial email policy restriction. The complete transcript of the SMTP session is sent.

`protocol`

Notifies the postmaster of protocol errors or client requests that contained unimplemented commands. The complete transcript of the SMTP session is included in the message.

`resource`

Informs the postmaster of undelivered mail due to resource problems, such as a queue file write error.

`software`

Notifies the postmaster of mail not delivered due to software failures.

This option correlates to the `notify_classes` directive, and defaults to reporting only problems that usually indicate a misconfiguration or serious problem (specifically `resource` and `software`). In some



high load environments, altering this to include bounce notifications could lead to a large number of notices.

Other General Options

The lower section of this page is devoted to global options that are less likely to need alteration. In many installations, these options will remain at their defaults.

Address that receives bcc of each message

With this option, an optional email address may be specified to receive a copy of every message that enters the Postfix system, excluding locally generated bounce messages. This can represent a breach of privacy in many circumstances and may be illegal in some countries. It is advisable to be cautious about utilizing this option. It can be useful in some environments where email archives are valuable for legal or technical reasons. This option correlates to the `always_bcc` directive and defaults to none.

Timeout on handling requests

This option determines how long a Postfix daemon will wait on a request to complete before it assumes the daemon has locked up, at which time the daemon will be killed. This option corresponds to the `daemon_timeout` and defaults to 18,000 seconds.

Default database type

This option determines the type of database to use in the `postalias` and `postmap` commands, and corresponds to the `default_database_type` directive. The default depends on the OS and installed system libraries at the time of building Postfix. Ordinarily this will be `hash` or `dbm` on UNIX systems.

Default message delivery transport

The term *delivery transport* refers to the protocol, or language, used to deliver the message from one mail server to another. The transport on modern systems is nearly always `smtp`, and this is the default in Postfix, but there are still a few legacy `uucp` systems in use. This option is merely the default choice when no transport is explicitly selected for the destination in the optional transport table. This option corresponds to the `default_transport` directive.

Sender address for bounce mail

In the event a message double-bounces, or first bounces from the recipient and then bounces from the sender after the first bounce notice is sent, it will be sent to this address. All messages will be silently discarded. In this way, bounce-loops can be avoided. This option correlates to the `double_bounce_sender` and defaults to `double-bounce`. The name may be any arbitrary name, but it must be unique.

Number of subdir levels below the queue dir

This option configures the number of subdirectory levels below the configured queue directories that will be used by Postfix for mail storage. Because of the design of the traditional UNIX filesystem, which includes UFS used by all modern BSD systems and the Linux `ext2` and `ext3` filesystems, performance becomes measurably slower when an extremely large number of files are stored in a single directory. Thus, programs that generate a large number of files often provide the ability to



split files out to a number of subdirectories to keep lookups fast. This option correlates to the `hash_queue_depth` directive and defaults to 2, which is suitable for most moderate and even relatively large installations. Because the number of directories in use increases the search time for object seeks, using too high a value here can be harmful to performance.

Name of queue dirs split across subdirs

Postfix uses a number of queues to organize messages with varying states and destinations. Each of these queues can be configured to use hashed subdirectories. If a queue is selected here, it will be stored in a hashed subdirectory. In some cases, a queue must not be listed here as performance will be severely impacted, specifically the world-writable mail drop directory. The defer log file directory, on the other hand, must be stored in hashed directories or performance will suffer. This option corresponds to the `hash_queue_names` directive and defaults to `incoming,active,deferred,bounce,defer,flush` and is rarely necessary or beneficial to alter this configuration.

Max number of Received: headers

A message that contains more Received: headers than this will bounce. An extremely large number may indicate a mail loop or a misconfigured mail server somewhere in the path of this message. This option correlates to the `hopcount_limit` directive and defaults to 50. This value rarely needs to be altered from its default.

Time in hours before sending a warning for no delivery

If a message cannot be delivered immediately, it will be queued for later delivery. After this number of hours, if the message still cannot be delivered, a warning will be sent to the sender notifying them that the server has been unable to send the message for a specified time. This correlates to the `delay_warning_time` directive and defaults to not sending a warning.

Network interfaces for receiving mail

This option configures the network addresses on which Postfix will accept mail deliveries. By default, Postfix will accept mail on every active interface. Here, Postfix will accept the variables discussed earlier. This option configures the `inet_interfaces` directive.

Idle time after internal IPC client disconnects

This option sets the time in seconds when an internal IPC client will disconnect. This allows servers to terminate voluntarily. This feature is used by the address resolution and rewriting clients. This option correlates to the `idle_time` directive and defaults to 100 seconds. This option should never need to be altered under normal circumstances.

Timeout for I/O on internal comm channels

This option determines the amount of time in seconds the server will wait for I/O on internal communication channels before breaking. If the timeout is exceeded, the server aborts with a fatal error. This directive corresponds to the `ipc_timeout` directive and defaults to 3,600 second (60 minutes).



Mail system name

This option identifies the mail server system in use to connecting users. It will be used in the `smtpd_banner`, which is sent in Received: headers, the SMTP greeting banner and in bounced mail. Security experts who promote security through obscurity suggest anonymizing all server software to prevent potential crackers from identifying the software on the server. It is probably not the best use of an administrator's time or effort in most environments, however, and many other security tactics are more effective and won't negatively impact the ability to track software problems. This option correlates to the `mail_name` directive and defaults to Postfix.

Mail owner

This option specifies the owner of the Postfix mail queue and most of the Postfix daemon processes. This user should be unique on the system and share no groups with other accounts or own any other files or processes on the system. After binding to the SMTP port (25), Postfix can drop root privileges and become the user specified here for all new daemon processes. If the Postfix daemon is ever compromised, the exploiter will only have access to mail and a few other files. Obviously it is good to avoid this as well, but it is certainly better than a root exploit, which would allow the exploiter to access and alter anything on the system. This option correlates to the `mail_owner` directive and defaults to `postfix`.

Official mail system version

This parameter configures the version number that will be reported by Postfix in the SMTP greeting banner, among other things. This correlates to the `mail_version` directive and defaults to the version of Postfix that is installed. Once again, security-by-obscurity promoters may encourage obfuscation of this value.

Time to wait for next service request

A Postfix daemon process will exit after the time specified here if it does not receive a new request for service during that time. This option corresponds to the `max_idle` directive and defaults to 100 seconds. This directive does not impact the queue manager daemon process.

Max service requests handled before exiting

This option configures the maximum number of requests that a single Postfix daemon process will answer before exiting. This option configures the `max_use` directive and defaults to 100.

Internet hostname of this mail system

This option specifies the Internet host name of the mail server. By default, this value will be set to the fully qualified host name of the server, as determined by a call to `gethostname()`. This option sets the `$myhostname` variable, which is used in the defaults to many other options. This option correlates to the `myhostname` directive.

Local Internet domain name

This option corresponds to the `mydomain` directive and defaults to the contents of the `$myhostname` variable minus the first component. This option defines the `$mydomain` variable and is used in a number of other configuration option defaults.



Local networks

Postfix provides a flexible set of options to help prevent UCE or other unauthorized uses of the mail server. This option defines what networks will be considered to be local by Postfix. The value is used to determine whether a client is local or remote. Policies can be more relaxed for local clients. This option configures the mynetworks directive and defaults to a list of all networks attached to the server. For example, if the server has an IP of 192.168.1.48 and a netmask of 255.255.255.0, all of the 192.168.1.0 network will be considered local. If you would like stricter control or the ability to treat other network blocks as local clients, you can specify them here in the form of network/mask pairs (i.e., 172.16.0.0/16). Network/mask pairs may be inserted from a separate file by specifying the absolute path to the file here.

Send postmaster notice on bounce to...

This option configures the user name or email address where bounce notices will be sent. This option correlates to the bounce_notice_recipient and is set to postmaster by default.

Send postmaster notice on 2bounce to...

This option configures the user name or email address where second bounce messages will be sent. This allows an administrator to watch for second bounce warnings more closely than first bounce messages, because first bounces are far more common and less likely to indicate serious problems. The option configures the 2bounce_notice_recipient directive and defaults to postmaster.

Send postmaster notice on delay to...

This option configures where delay warnings will be sent. This option correlates to the delay_notice_recipient directive and defaults to postmaster.

Send postmaster notice on error to...

Specifies where error warnings will be sent. This option correlates to the error_notice_recipient directive and defaults to postmaster.

Mail queue directory

This specifies the directory where Postfix will store queued mail. This will also be the root directory for Postfix daemons that run in a chroot environment. The queue is where messages awaiting delivery are stored, providing enough space to accommodate your user mail load in this directory. This option correlates to the queue_directory directive and usually defaults to a sensible location for your OS. Many Linux systems will have the mail queue in /var/spool/mail or /var/spool/postfix.

Lock file dir, relative to queue dir

This option configures the location of the Postfix lock directory. It should be specified relative to the queue directory and generally will simply be a subdirectory of the queue directory. This option configures the process_id_directory directive and defaults to pid.

Separator between user names and address extensions

This option specifies the separator character between user names and address extensions. This option correlates to the recipient_delimiter directive and defaults to using no delimiter. This option



impacts Canonical Mapping, Relocated Mapping and Virtual Domains.

Postfix support programs and daemons dir

This option specifies the directory where Postfix will look for its various support programs and daemons. The directory should be owned by root. This option correlates to the `program_directory` directive and defaults vary depending on installation method and OS variant. On many Linux systems this will be `/usr/libexec/postfix`.

Relocated mapping lookup tables

Postfix can provide a relocation notice in response to messages sent to users who no longer receive mail from this server. If enabled, this option specifies the location of the file containing a table of contact information for users who no longer exist on this system. By default, this feature is disabled. This option correlates to the `relocated_maps` directive. If enabled, a reasonable choice for this option might be `/etc/postfix/relocated`.

Disable kernel file lock on mailboxes

On Sun workstations, kernel file locks can cause problems because the mailtool program holds an exclusive lock whenever its window is open. Users of other OS variants, or Sun systems where no Sun mail software is in use, may ignore this option. This option correlates to the `sun_mailtool_compatibility` directive and defaults to No.

Max time to send a trigger to a daemon

This option specifies the maximum amount of time allowed to send a trigger to a Postfix daemon. This limit helps prevent programs from getting hung up when the mail system is under an extremely heavy load. This option correlates to the `opts_trigger_timeout` directive and defaults to 10 seconds.

Address Rewriting and Masquerading

Postfix offers a relatively easy to use and flexible address rewriting system, allowing it to act as a mail gateway for a large network or as a gateway between legacy mail systems and the Internet at large.

Note

The options on this page are also discussed on the [Postfix Configuration - Address Manipulation](#) page at the Postfix homepage. It is worth reading if advanced address rewriting is required in your mail system.

Rewrite “user%domain” to “user@domain”

This option is useful for some legacy systems that used strange address trickery, such as `user%domain@otherdomain`. It is not generally useful in modern environments, but it is not harmful so it usually defaults to Yes. This option correlates to the `allow_percent_hack` directive.

Rewrite “user” to “user@\$mydomain”

This option configures how Postfix will handle an address that has no domain name in the destination. If enabled, it will append the value of `$mydomain` to the address. This option correlates



to the `append_at_myorigin` directive and defaults to Yes. Because most Postfix components expect addresses to be in the form of `user@domain`, it is probably not appropriate to disable this feature.

Rewrite “user@host” to “user@host.\$mydomain”

This option configures simple host addresses that have the value of `$mydomain` appended to them. This option correlates to the `append_dot_mydomain` directive and defaults to Yes. Some administrators may find that this explicit rewrite has unexpected consequences, but it is rarely a problem.

Rewrite “site!user” to “user@site”

Legacy UUCP networks use a different addressing format than modern SMTP systems. This option enables Postfix to convert the old-style address to a modern address for delivery via the standard SMTP protocol. This option configures the `swap_bangpath` directive and defaults to Yes.

Send mail with empty recipient to...

This specifies the destination of mail that is undeliverable. Typically, this will be bounce notifications and other error messages. This option correlates to the `empty_address_recipient` directive and defaults to `MAILER-DAEMON`, which by default is simply an alias to `postmaster`.

Address masquerading

Address masquerading is a method where hosts behind the gateway mail server may be hidden, and all mail will appear to have originated from the gateway server. If enabled, the host and/or subdomain portion of an address will be stripped off and only the domain specified will be included in the address. For example, if `$mydomain` is specified an outgoing mail from `joe@joesmachine.swelltech.com` would become `joe@swelltech.com`, assuming the `$mydomain` variable contains `swelltech.com`. This option correlates to the `masquerade_domains` directive and is disabled by default.

Masquerade exceptions

It is possible to skip over the masquerade rules defined above for some user names. The names to be excepted from those rules can be entered here. This option corresponds to the `masquerade_exceptions` directive and no exceptions are made by default.

Mail Aliases

Mail aliases provide a means to redirect mail to local recipients. Specifically, it allows mail destined for a number of different addresses to be delivered to a single mailbox. A common use is to direct mail for users like a `postmaster` to a real person. This page is divided into two sections. The upper section labeled `Aliases Options` contains the location and format of the alias files that Postfix should use to construct its alias databases and specifies the type of database to use. The lower section provides a list of all configured aliases on the system and what the alias maps to.

Aliases Options

Alias databases used by the local delivery agent

This option sets the filenames that Postfix will use for local delivery alias translation. The filename



will have a suffix appended to it based on the file type. This option correlates to the `alias_maps` directive and the default is system dependent. Common defaults include `hash:/etc/aliases` or `hash:/etc/postfix/aliases`. The first part of the entry preceding the colon is the type of database to use, which will be one of `hash` for systems with a modern Berkeley DB implementation, `dbm` for older style systems that only have `dbm` available, or `nis` for systems that run NIS. The after-colon portion of the entry is the path to the filename where the database name is derived. The databases will be built from the contents of the flat files by Postfix on startup or when running the `newaliases` command.

Alias databases built by Postfix

This option, which is closely related to the previous `Alias` option, specifies the alias database file(s) that are built when the `newaliases` or `sendmail -bi` commands are run. These commands generate the alias database from the flat file in the previous `Alias` option in order to speed alias lookups performed by Postfix. Because there may be thousands of aliases on a large mail server, importing them into a database is necessary to maintain efficiency. This option correlates to the `alias_database` directive. Defaults are system dependent, but will commonly be the same as the previous `Alias` option, with the appropriate database file suffix appended.

Aliases

This section of the page provides a list of all configured aliases. To edit an alias, click on the name. To create an alias, click on the `Create a new alias` button and fill in the `Name` and `Alias to...` fields. Whenever aliases files have been modified, it is necessary to recreate the aliases database files in order for changes to take effect. When using Webmin, this is performed automatically and no additional steps are required.

Note

If adding aliases from the command line, it is possible to regenerate the aliases database using the command `postalias`. The main page for this command is a useful resource for understanding how aliases databases are handled in Postfix.

Canonical Mapping

Canonical mapping in Postfix is used for modifying mail in the incoming queue. It alters both the message headers and the message envelope information for local or remote mail. This mapping can be useful to replace login names with `Firstname.Lastname` style addresses, or to clean up odd addresses produced by legacy mail systems.

Canonical Mapping Tables

If you use any canonical mapping tables, they must be specified in the first section of the **Canonical Mapping** module. After defining them, you can edit them from the second section of the module.

Address mapping lookup tables

This option specifies the location of the optional canonical address mapping table file. This mapping is applied to both sender and recipient addresses, in both envelopes and headers. This option configures the `canonical_maps` directive and is disabled by default. Like the aliases files discussed in the last section, canonical mapping files are specified by a database type and a file name. The accepted database types depend on your operating system and installed components. Usually `hash`



and dbm are used as the database type. A common choice for this value might be hash:/etc/postfix/canonical.

Tables for RECIPIENT addresses

This parameter configures address mapping only on recipient addresses and not sender addresses. Mapping is performed on both envelopes and headers. These lookups are performed before the configured **Address mapping lookup tables**. This option correlates to the recipient_canonical_maps directive and is disabled by default.

Tables for SENDER addresses

This configures mapping for sender addresses only and not recipient addresses. Both envelope and header information is modified. This option correlates to the sender_canonical_maps directive and is disabled by default.

Editing Canonical Mappings

Once a file name is selected for any of the canonical mapping tables, it may be edited by clicking the appropriate **Edit...** buttons. A new page will open, listing any existing mappings and allowing the creation of new mappings. The format of mappings in all files is the same.

Canonical mappings may seem, on the surface, to be similar to aliases or virtual domains. However, they are quite distinct and are useful for other purposes. While aliases merely make a decision about which user will receive an email and virtual domains only impact the envelope address, the canonical mapping alters both the envelope address and the SMTP header address. This change can be used to make mail appear to come from a different user or domain, or direct mail to a different user or domain by changing the address on the message.

For example, if I have a number of local subdomains, but would like all mail to appear to originate from a single domain, it is possible to create a canonical mapping to make the translations. In the **Edit a Map** page, the Name will be a subdomain that is mapped to the domain, such as @lab.swelltech.com. The Maps to... value will simply be the domain I'd like this subdomain converted to, @swelltech.com. After saving the mapping and applying changes, all outgoing mail from lab.swelltech.com will appear to originate from swelltech.com.

Virtual Domains

This functionality in Postfix provides a means to redirect messages to different locations by altering the message envelope address. The header address is not altered by a virtual domain mapping. While some functionality of virtual domains overlaps with features available in aliases, it can be used for local or non-local addresses, while aliases can only be used for local address.

Domain mapping lookup tables

Much like aliases tables and canonical mapping tables, this is simply the path to a file containing the mapping tables for virtual domains. This is usually something along the lines of hash:/etc/postfix/virtual, and must be converted to a database format in Postfix. Webmin will perform the database generation step for you.



Transport Mapping

The term transport refers to the mechanism used to deliver a piece of email. Specifically, SMTP and UUCP are mail transports supported by Postfix. Transport mapping can be used for a number of purposes, including SMTP to UUCP gatewaying, operating Postfix on a firewall with forwarding to an internal mail server, etc.

Transport mapping lookup tables

This option configures the path to a file containing one or more transport mappings. These tables are like mapping tables, and are converted to a database and used by Postfix in the same way. This option correlates to the `transport_maps` directive. This feature is disabled by default. A common value for this option is `/etc/postfix/transport`.

To create a new mapping, first define the mapping file. Then click **Add a mapping**. If your goal is to redirect mail to a protected internal host from Postfix running on a firewall, you could enter the outside domain name into the **Name** field, `swelltech.com`, and then enter into the **Maps to...** field the address of the internal machine, `smtp:privatehost.swelltech.com`. To improve upon this, local delivery on this machine could be disabled, and increased controls over where and to whom mail should be accepted. There are more examples in the tutorial section of this chapter.

Relocated Mapping

Using this option, it is possible to notify senders if a local user has moved to another address. For example, if a user leaves an organization but still receives occasional mail at her local address, it may be convenient to notify anyone sending mail to the user of the move and new contact information for that user. Usage is just like the previous types of mappings and won't be documented specifically here, although an example of a relocated mapping will be given to display the types of information that can be provided by this feature.

Let's say I move from my current company to the far more relaxed atmosphere of the Oval Office. To make sure all of my friends and clients can keep in touch with me, I could provide a relocated mapping with a **Name** of `joe@swelltech.com` with a **Maps to...** of `president@whitehouse.gov`. While this won't redirect mail to me at my new home, it will notify the people trying to contact me that I've changed email addresses. Hopefully they will update their address books and resend their mail to the new address.

Local delivery

Local delivery is what Postfix does when it reaches the end of its list of mappings and access controls and still finds that the message is allowed and destined for a user on the local machine (i.e., a mapping could potentially send the message elsewhere for final delivery, so all mappings, as well as various access checks, are performed before reaching this stage). This page configures a number of options relating to how Postfix handles the delivery of mail for local users.

Name of the transport for local deliveries

This configures the name of the transport that will be used for delivery to a destination that will match the `$mydestination` or `$inet_interfaces` variables. This can be a simple mailbox drop handled by the Postfix local delivery agent, or any appropriate delivery command. This option correlates to the `local_transport` directive and defaults to the defined transport type named `local`.



Shell to use for delivery to external command

If a command shell is required to communicate properly with your chosen local delivery transport, this option selects the one that will be used. By default, no shell is used and the transport command will be executed directly. However, if the command contains shell meta-characters or shell built-in commands, they will be passed to `/bin/sh` or whatever shell you configure here. A popular choice for this is `smrsh`, or Sendmail's Restricted Shell, which is included in recent Sendmail distributions. `smrsh` allows more precise control over what commands users can execute from their `.forward` files. This option corresponds to the `local_command_shell` and defaults to `/bin/sh`.

Search list for forward

This is a comma-separated list of possible locations for user forward files. Postfix will try each entry in the list until a forward file is found, or until all have been checked and no match is found. The forward file allows users to configure delivery options for themselves, including delivery-time processing by a program like `procmail`, as well as the forwarding of messages to a different server. A number of variable expansions are performed on the entries. The expansions:

Forward search path variable expansions

`$user`

The user name of the recipient.

`$shell`

The shell of the recipient.

`$home`

Recipient's home directory.

`$recipient`

The full recipient address.

`$extensions`

Recipient address extensions. This is a separate part of the email address, separated by the **Separator between user names and address extensions** defined on the **General Options** page.

`$domain`

The recipient's domain name.

`$local`

The entire local part of the recipient address.

`$recipient_delimiter`

The separation delimiter for the recipient.



Valid mail delivery to external commands

This parameter restricts mail delivery to only those commands specified here. The default is to disallow delivery to commands specified in `:include:` files, and allow execution of commands in alias and forward files. This option correlates to the `allow_mail_to_command` directive.

Valid mail delivery to external files

This option restricts mail delivery to external files. The default is to disallow delivery to files specified in `:include:` but to allow delivery to files specified in aliases and forward files. This option correlates to the `allow_mail_to_files` directive.

Default rights of the local delivery agent

This option configures the privileges that the delivery agent will have for delivery to a file or a command. This option should never be a privileged user or the Postfix owner. This option corresponds to the `default_privs` directive and defaults to `nobody`.

Pathname of user mailbox file

When delivering mail locally, Postfix will drop mail in the directory configured here or in its default mail spool directory. If you wish to use the maildir format for mail storage, this value can be appended with a trailing slash. For example, to store mail in the user's home directory in the Maildir subdirectory, the value would be `Maildir/`. This option correlates to the `home_mailbox` directive and usually defaults to some location under `/var/spool/mail` or `/var/spool/postfix`.

Destination address for unknown recipients

If a message is received for a recipient that does not exist, the message is normally bounced. However, it is possible to instead have the message delivered to an alternate address. This option corresponds to the `user_relay` directive. Variable expansions matching those discussed for the **Search list for forward** are also valid for this directive.

Spool directory

This option specifies the directory where UNIX-style mailboxes are stored. Defaults vary depending on OS variant and version, but a common choice is `/var/spool/mail`. This option correlates to the `mail_spool_directory` option.

External command to use instead of mailbox delivery

This option defines a command to use for delivery instead of delivering straight to the user's mailbox. The command will be run as the recipient of the message with appropriate `HOME`, `SHELL` and `LOGNAME` environment variables set. This option is commonly used to set up system-wide usage of procmail. If you use a command to deliver mail to all users, you must configure an alias for root, as the command will be executed with the permissions of the `$default_user`. This option correlates to the `mailbox_command` directive and is disabled by default.

Optional actual transport to use

This option configures the message transport to use for all local users, whether they are in the UNIX



passwd database or not. If provided, the value will override all other forms of local delivery, including **Destination address for unknown recipients**. This option corresponds to the `mailbox_transport` directive and is disabled by default. This option may be useful in some environments, for example, to delegate all deliveries to an agent like the cyrus IMAPD.

Optional transport for unknown recipients

If a user cannot be found in the UNIX passwd database and no alias matches the name, the message will ordinarily be bounced or handled via the **Destination address for unknown recipients** option. However, if you would like unknown users to be handled by a separate transport method, this option overrides the **Destination address for unknown recipients** option. This option correlates to the `fallback_transport` directive and is disabled by default.

Max number of parallel deliveries to the same local recipient

This option limits the number of simultaneous deliveries to a single local recipient. If `.forward` files are allowed for users, a user may run a time-consuming command or shell script, leading to overload caused by several processes being started up at once. This option correlates to the `local_destination_concurrency_limit` directive and the default is 2. A low value is recommended for this option, unless it is certain that no complex `.forward` files will be in use.

Max number of recipients per local message delivery

This option configures the maximum number of recipients per local message delivery. This option correlates to the `local_destination_recipient_limit` and is set to the value of Max number of recipients per message delivery by default.

Prepend a Delivered-To: when...

This parameter determines when Postfix should insert a `Delivered-to:` message header. By default, Postfix inserts this header when forwarding mail and when delivering to a file. The defaults are recommended, and it is generally preferable not to disable insertion into forwarded mail. This option corresponds to the `prepend_delivered_header` directive.

General resource control

This page provides access to the various memory and process limits for the Postfix processes. It is rarely necessary to alter the values on this page, except for highly loaded servers or very low resource machines.

Max size of bounced message

This option limits the amount of original message content in bytes that will be sent in a bounce notification. This option correlates to `bounce_size_limit` and defaults to 50000 bytes.

Max time for delivery to external commands

When delivering mail to an external command rather than via direct mailbox delivery, Postfix will wait this amount of time for the delivery to complete. If this value is to be set to a high limit (3,600 seconds or more), the value of **Timeout for I/O on internal comm channels** in **General Options** must also be increased. This option correlates to the `command_time_limit` directive and defaults to 1000 seconds.



Max number of Postfix child processes

This option limits the number of child processes that Postfix will spawn. On high load servers, the default may be too low and need to be raised to as much as 500 or more. For most environments, 50 is more than adequate and may even be overkill. For example, on dial-up or consumer broadband serving one to 10 users, a more appropriate limit might be 10. If in doubt, leave its default unless it causes problems. This option correlates to the `default_process_limit` directive and defaults to 50.

Max number of addresses remembered by the duplicate filter

While expanding aliases and `.forward` files, Postfix will remember addresses that are being delivered to and attempt to prevent duplicate deliveries to the same address. This option limits the number of recipient addresses that will be remembered. It corresponds to the `duplicate_filter_limit` directive and defaults to 1000. There is no compelling reason to increase this value.

Max attempts to acquire file lock

This option limits the number of attempts Postfix will make when attempting to obtain an exclusive lock on a mailbox or other file requiring exclusive access. It corresponds to the `deliver_lock_attempts` directive and defaults to 20.

Time in seconds between file lock attempts

Postfix will wait a specified time between attempts to lock a given file after a failed lock attempt. This option configures the `deliver_lock_delay` directive and defaults to 1 second.

Max attempts to fork a process

If Postfix attempts to fork a new process and fails, due to errors or a lack of available resources, it will try again a specified number of times. This option correlates to the `fork_attempts` directive and defaults to 5.

Time in seconds between fork attempts

Postfix will try to spawn a new process a specified time after a failed attempt. This option correlates to the `fork_delay` directive and defaults to 1 second.

Max memory used for processing headers

This option limits the amount of memory in bytes that Postfix will use to process message headers. If a message header is too large to fit into the memory specified, the headers will be treated as part of the message body. This option correlates to the `header_size_limit` directive and defaults to 102,400.

Max memory used for handling input lines

This option limits the amount of memory in bytes that Postfix will use to handle input lines. An input line is any line read from an `:include:` or `.forward` file. In order to prevent the mail server from using excessive amounts of memory, it will break up files into chunks of this length. This option correlates to the `line_length_limit` directive and defaults to 2048.



Max size of a message

This option limits the size in bytes of a message that will be delivered, including the message envelope information. This limit should be set high enough to support any email messages your users will need to be able to send or receive. This option correlates to the `message_size_limit` directive and defaults to 10,240,000.

Max number of messages in the active queue

This option limits the number of messages that can exist in the message queue at any given time. It correlates to the `qmgr_message_active_limit` directive and defaults to 10,000.

Max number of in-memory recipients

This parameter limits the number of in-memory recipient data structures. This memory contains the short-term *dead list*, which indicates a destination was unavailable when last contacted, among other things. This option correlates to the `qmgr_message_recipient_limit` directive and defaults to 1000.

Min free space in the queue file system

Postfix will refuse mail if the filesystem on which the queue is located has less available space in bytes than the value set in this option. This option correlates to the `queue_minfree` directive and defaults to 0.

Max time after which stale lock is released

This option configures how old an external lock file may be before it is forcibly removed. This option correlates to the `stale_lock_time` and defaults to 500 seconds.

Time in seconds between attempts to contact a broken MDT

This option configures the time in seconds between the queue manager attempts to contact an unresponsive mail delivery transport. This option correlates to the `transport_retry_time` and defaults to 60 seconds.

SMTP server options

This page configures the majority of options that directly affect the behavior of the SMTP server portion of Postfix, specifically the portions that impact how the server behaves towards an SMTP client that connects to the server.

SMTP greeting banner

When a client connects to an SMTP server, a *greeting banner* will be sent to the client (note the term *client* in this context is not the end user, but rather the email software program used to make the connection). This option configures the text that will follow the status code in the banner. It is possible to use a number of variable expansions, for example, to display the specific version of the server software, though Postfix does not include the version by default. If configuring this option to be other than the default, you must include `$myhostname` at the start of this line, as it allows Postfix to report and respond to a mailer loop rather than overload the system with multiple deliveries. This



option correlates to the smtpd_banner directive and contains \$myhostname ESMTP \$mail_name by default.

Note

A proposed federal law in the U.S. would make it illegal to send unsolicited commercial email through a mail server if the server included in its SMTP greeting the words NO UCE.

Max number of recipients accepted for delivery

This option limits the number of recipients that may be specified in a single message header. It is usually rare for legitimate messages to have an extremely large number of recipients specified in a single message header, but it is often done in UCE messages. The legitimate exception is messages to a mailing list, possibly sent by mailing list software like majordomo or mailman. This option correlates to the smtpd_recipient_limit and defaults to 1000.

Disable SMTP VRFY command

Normally, the SMTP VRFY command is used to verify the existence of a particular user. However, it is also illegitimately used by spammers to harvest live email addresses. Thus, it is sometimes useful to disable this command. This option correlates to disable_vrfy_command and defaults to No.

Timeout in seconds for SMTP transactions

This option sets the timeout for a client to respond to the SMTP servers response with an SMTP request. The connection process involves the client opening a connection to the server, the server replying with a greeting and the client making its request. If the client request does not come within the time specified here, the connection will be closed. This option correlates to the opts_smtpd_timeout directive and defaults to 300 seconds.

Timeout before sending 4xx/5xx error response

When sending an error response to a client, the server will sleep for a specified time. The purpose of this feature is to prevent certain buggy clients from hitting the server with repeated requests in rapid succession. This option correlates to the smtpd_error_sleep_time directive and defaults to 5 seconds.

Error count for temporarily ignore a client

This option configures the number of errors that a client may generate before Postfix will stop responding to requests for a specified time. Some buggy mail clients may send a large number of requests, while ignoring or responding incorrectly to the error messages that result. Postfix attempts to minimize the impact of these buggy clients on normal service. This option correlates to the smtpd_soft_error_limit and defaults to 10.

Error count for closing connection

If the number exceeds this limit, the connection will be closed. This option correlates to the smtpd_hard_error_limit and defaults to 100.



HELO is required

Enabling this option causes Postfix to require clients to introduce themselves with a HELO header at the beginning of an SMTP session. This may prevent some UCE software packages from connecting, although it may also impact other legitimate clients. This option correlates to the `smtpd_helo_required` and defaults to No.

Allow untrusted routing

This option configures whether Postfix will forward messages with *sender-specified routing* from untrusted clients to destinations within the accepted relay domains. This feature closes a potential loophole in access controls that would normally prevent the server from being an open relay for spammers. If this behavior is allowed, a malicious user could exploit a backup MX mail host into forwarding junk mail to a primary MX server that believes the mail has originated from a local address. This option correlates to the `allow_untrusted_routing` and is disabled by default. Enabling this option should be done with extreme caution to prevent turning your Postfix installation into an open relay.

Restrict ETRN command upon...

The SMTP ETRN command is a clumsy means for clients that are not always connected to the Internet to retrieve mail from the server. The usage of this command is rather outdated and rarely used, as POP3 and IMAP are better suited to solve this problem. This option correlates to the `smtpd_etrn_restrictions` directive and the default is to allow ETRN from any host. This option accepts the following directives: `check_etrn_access` `maptype:mapname`, `permit_naked_ip_address`, `reject_invalid_hostname`, `check_helo_access` `maptype:mapname`, `reject_maps_rbl`, `reject_unknown_client`, `permit_mynetworks`, `check_client_access`, `permit`, `reject`, `warn_if_reject`, and `reject_unauth_pipelining`.

This option, as well as the following three **Restrictions...** options, accept one or all of the following values in the text field. Each is described only once here and the specific entry will include the list of accepted directives for the option. The impact of some of these choices depends on configuration performed elsewhere, and could potentially open security holes if not configured carefully.

`permit_mynetworks`

Permit the message if the relevant address (sender or recipient, depending on the restriction) is within the local network.

`reject_unknown_client`

The request will be refused if the client IP has no PTR record in the DNS. This means a client with an IP address that cannot be resolved to a host name cannot send mail to this host.

`check_client_access` `maptype:mapname`

This option requires the inclusion of an already configured map. This will restrict, based on the contents of the map, allowing only clients that are allowed by the map. The map may contain networks, parent domains or client addresses, and Postfix will strip off unnecessary information to match the client to the level of specificity needed.

`check_sender_access` `maptype:mapname`



This will restrict, based on the contents of the map, allowing only senders that are allowed by the map. The map may contain networks, parent domains, or localpart@.

reject_maps_rbl

reject_invalid_hostname

If the client host name is invalid due to bad syntax, the request will be rejected.

permit_naked_ip_address

If the client HELO or EHLO command contains a naked IP address without the enclosing [] brackets as required by the mail RFC, the message will be rejected. Beware that some popular mail clients send a HELO greeting that is broken this way.

reject_unknown_hostname

Reject the request if the host name in the client HELO command has no A or MX record in the DNS.

reject_non_fqdn_hostname

If the client host name is not in the form of a fully-qualified domain name, as required by the RFC, the message will be rejected.

check_helo_access maptype:mapname

The server will search the named access database map for the HELO host name or parent domains. If the result from the database search is REJECT or a 4xx text or 5xx text error code, the message will be refused. A response of OK or RELAY or an all numerical response will permit the message.

permit

This simply permits anything. Generally, this will be at the end of a set of restrictions in order to allow anything that has not been explicitly prohibited.

reject

Rejects everything. This can be used at the end of a chain of restrictions to prohibit anything that has not be explicitly permitted.

warn_if_reject

This is a special option that changes the meaning of the following restriction, so that a message that would have been rejected will be logged but still accepted. This can be used for testing new rules on production mail servers without the risk of denying mail due to a problem with the rules.

reject_unauth_pipelining

If the client sends commands ahead of time without first confirming the server support SMTP command pipelining, the message will be rejected. This will prevent mail from poorly written bulk email software that uses pipelining to speed up mass deliveries.



Restrictions on client hostnames/addresses

This restriction applies to the client host name and/or address. By default, Postfix will allow connections from any host, but you may add additional restrictions using the following: `reject_unknown_client`, `permit_mynetworks`, `check_client_access maptype:mapname`, `reject_maps_rbl`, `maps_rbl_reject_code`, `permit`, `reject`, `warn_if_reject`, `reject_unauth_pipelining`.

Restrictions on sends in HELO commands

This option specifies additional restrictions on information that can be sent by client in the HELO and EHLO commands. This option correlates to the `smtpd_helo_restrictions` directive. By default Postfix accepts anything, and the following restrictions may be added: `reject_invalid_hostname`, `permit_naked_ip_address`, `reject_unknown_hostname`, `reject_non_fqdn_hostname`, `check_helo_access maptype:mapname`, `reject_maps_rbl`, `reject_unknown_client`, `check_client_access maptype:mapname`, `permit`, `reject`, `warn_if_reject`, `reject_unauth_pipelining`.

Restrictions on sender addresses

This option restricts what can be contained in the MAIL FROM command in a message. It may be used to prevent specific email addresses from sending mail, reject clients without a resolvable host name, etc. This option correlates to the `smtpd_sender_restrictions` directive and may contain any of the following restrictions: `permit_mynetworks`, `reject_unknown_client`, `reject_maps_rbl`, `reject_invalid_hostname`, `reject_unknown_hostname`, `reject_unknown_sender_domain`, `check_sender_access maptype:mapname`, `check_client_access maptype:mapname`, `check_helo_access maptype:mapname`, `reject_non_fqdn_hostname`, `reject_non_fqdn_sender`, `reject`, `permit`.

Restrictions on recipient addresses

This parameter places restrictions on the recipients that can be contained in the RCPT TO command of a sent message. It can be used to dictate where email may be sent. This option correlates to the `smtpd_recipient_restrictions`, and may contain any of the following restrictions: `permit_mynetworks`, `reject_unknown_client`, `reject_maps_rbl`, `reject_invalid_hostname`, `reject_unknown_hostname`, `reject_unknown_sender_domain`, `check_relay_domains`, `permit_auth_destination`, `reject_unauth_pipelining`, `permit_mx_backup`, `reject_unknown_recipient`, `check_recipient_access`, `check_client_access`, `check_helo_access`, `check_sender_access`, `reject_non_fqdn_hostname`, `reject_non_fqdn_sender`, `reject_non_fqdn_recipient`, `reject`, `permit`.

DNS domains for blacklist lookups

This option configures the optional blacklist DNS servers that will be used for all RBL checks that have been specified in all access restrictions. It may contain any number of servers in a whitespace separated list. These services can be used to help prevent spam, as discussed earlier in this section, with the **Restrict ETRN command upon...** parameter. This option configures the `maps_rbl_domains` directive and is empty by default.

Restrict mail relaying

This option specifies which hosts, networks, domains, etc., Postfix will relay email for. This option correlates to the `relay_domains` directive and defaults to `$mydestination`.

SMTP server response on access map violation, SMTP server response on RBL domains violation, SMTP server response on forbidden relaying, SMTP server response on unknown client reject,



SMTP server response on invalid hostname reject, SMTP server response on unknown domain reject, SMTP server response on unknown hostname reject

These options configure the error result code that will be sent to the client when any of the specified restrictions are applied. These errors have sensible default values and generally should not need to be changed. Consult with RFC 822 if you wish to understand more about the SMTP error codes or have a reason to change any of these values.

SMTP Client Options

The SMTP client options configures how Postfix will behave when dealing with other mail servers as a client, i.e., when sending mail on behalf of a user. This portion of the configuration primarily dictates how the server will respond to certain error conditions.

Action when listed as best MX server

As discussed in the BIND chapter, a mail server performs a name server query to find the MX, or mail server, record for the destination domain. If this record indicates that the local server is the server to which mail should be sent, it can respond in a couple of ways. The default is to bounce the message with an error indicating a mail loop. If the field is selected and local is entered, the mail will be directed to the local delivery agent instead of bouncing. This option correlates to the `best_mx_transport` directive.

Hosts/domains to hand off mail to on invalid destination

By default, mail that cannot be delivered because the destination is invalid will be bounced with an appropriate error message. However, it is possible to configure Postfix to hand off email to another server instead. This option correlates to the `fallback_relay` directive.

Ignore MX lookup error

If a name server query fails to provide an MX record, the server defaults to deferring the mail and trying again later. If Yes is selected, an A record query will be done and an attempt to deliver to the resulting address will be made. This option correlates to the `ignore_mx_lookup_error` directive.

Skip 4xx greeting

If a remote server responds to a connection with a 4XX status code, Postfix will, by default, select the next available mail exchanger specified by the MX records. If set to No, mail delivery will be deferred after the first mail delivery attempt and another attempt will be made later. This option correlates to the `smtp_skip_4xx_greeting` directive.

Skip wait for the QUIT command

This option configures whether Postfix will wait for the receiving mail server to respond to the QUIT command. This option correlates to the `smtp_skip_quit_response` directive and defaults to no.

Max number of parallel deliveries to the same destination

This option specifies the maximum number of deliveries that Postfix will perform to the same destination simultaneously. This option correlates to the `smtp_destination_concurrency_limit` directive and defaults to the system-wide limit for parallel deliveries configured in the **Delivery**



Rates page.

Max number of recipients per delivery

Limits the number of recipients per delivery. This option correlates to the `smtp_destination_recipient_limit` directive and defaults to the system-wide limit for recipients per delivery.

Timeout for completing TCP connections

Specifies the time in seconds that the Postfix delivery agent will wait before timing out a TCP connection. This option correlates to the `smtp_connect_timeout` directive and defaults to 0, which disables connection timeouts.

Timeout on waiting for the greeting banner

Limits how long Postfix will wait for a greeting banner to be received from the destination server. This option corresponds to the `smtp_helo_timeout` directive and defaults to 300 seconds.

Timeout on waiting for answer to MAIL FROM

Sets the timeout in seconds for sending the SMTP MAIL FROM command and receiving the destination server's response. This option correlates to the `smtp_mail_timeout` and defaults to 300 seconds.

Timeout on waiting for answer to RCPT TO

Sets the timeout in seconds for sending the SMTP RCPT TO command and receiving the destination server's response. This option correlates to the `smtp_rcpt_timeout` directive and defaults to 300 seconds.

Timeout on waiting for answer to DATA

Sets the timeout in seconds for sending the SMTP DATA command and receiving the destination server's response. This option correlates to the `smtp_data_init_timeout` and defaults to 120 seconds.

Timeout on waiting for answer to transmit of message content

Specifies the SMTP client timeout in seconds for sending the contents of the message. If the connection stalls for longer than this timeout, the delivery agent will terminate to transfer. This option corresponds to the `smtp_data_xfer_timeout` directive and defaults to 180 seconds.

Timeout on waiting for answer to ending "."

Specifies the SMTP client timeout in seconds for sending the closing SMTP "." and receiving the destination server's reply. This option correlates to the `smtp_data_done_timeout` directive and defaults to 600 seconds.

Timeout on waiting for answer to QUIT

Sets the timeout in seconds for sending the SMTP QUIT command and receiving the destination server's response. This option correlates to the `smtp_quit_timeout` and defaults to 300 seconds



Delivery Rates

This page contains the options for setting the default rate and concurrency limits for all Postfix components. These rates can usually be overridden within their respective configuration sections.

Max number of parallel deliveries to the same destination

This option specifies the maximum number of deliveries that Postfix will perform to the same destination simultaneously. This option correlates to the `default_destination_concurrency_limit` directive and defaults to 10.

Max number of recipients per message delivery

Limits the number of recipients per delivery. This option correlates to the `default_destination_recipient_limit` directive and defaults to 50.

Initial concurrency level for delivery to the same destination

Specifies the initial number of simultaneous deliveries to the same destination. This limit applies to all SMTP, local and pipe mailer deliveries. A concurrency of less than two could lead to a single problem email backing up delivery of other mail to the same destination. This option configures the `initial_destination_concurrency` directive and defaults to 5.

Max time (days) in queue before message is undeliverable

Defines the number of days a message will remain queued for delivery in the event of delivery problems before the message is sent back as undeliverable. This option configures the `maximal_queue_lifetime` directive and defaults to 5 days.

Min time (secs) between attempts to deliver a deferred message

In the event of a delivery deferral, Postfix will wait a specified amount of time before reattempting delivery. This value also specifies the time an unreachable destination will remain in the destination status cache. This option correlates to the `minimal_backoff_time` directive and defaults to 1000 seconds.

Max time (secs) between attempts to deliver a deferred message

Specifies the maximum amount of time between delivery attempts in the event of a deferred delivery. This option configures the `maximal_backoff_time` directive and defaults to 4000 seconds.

Time (secs) between scanning the deferred queue

Specifies the time in seconds between queue scans by the queue management task. This option correlates to the `queue_run_delay` and defaults to 1000 seconds.

Transports that should not be delivered

This field specifies which delivery transports, if any, defined in the **Transport Mapping** section will not have their messages sent automatically. Instead, the messages will be queued and delivered manually using the `sendmail -q` command. This option correlates to the `defer_transports` directive and contains nothing by default.



Debugging features

Postfix has two levels of logging. The first level is the normal maillog, which reports on all normal mail activities, such as received and sent mail, server errors, shutdowns and startups. The second level is more verbose and can be tuned to log activity relating to specific SMTP clients, host names or addresses. This page contains the configuration for the second level of logging.

List of domain/network patterns for which verbose log is enabled

This is a list of patterns or addresses that match the clients, hosts or addresses whose activity you would like to have more verbose logging for. Values could be an IP address like 192.168.1.1 or a domain name like swelltech.com. This option correlates to the `debug_peer_list` directive and is empty by default.

Verbose logging level when matching the above list

Specifies the level of verbosity of the logging for the activity that matches the above patterns. This option correlates to the `debug_peer_level` directive and defaults to 2. The above field must have at least one value for this debug level to have any impact.

Postfix, Unsolicited Commercial Email and Access Controls

Postfix offers an extremely flexible set of access controls, primarily targeted at preventing unsolicited commercial email from being delivered through the server. In order to construct a suitable set of controls, it is necessary to understand the order rules are checked and how they interact. By default, Postfix will accept mail for delivery from or to any client on your local network and any domains that are hosted by Postfix. So, by default, Postfix is not an open relay. This is a good beginning and all that is needed in many environments. However, because UCE is such a nuisance for users and network administrators, it may be worthwhile to implement more advanced filtering. This section will address the basics of the Postfix UCE control features.

Access Control List Order

Every message that enters the `smtpd` delivery daemon will be processed by access control lists and checked against rules to ensure that the message is one that the administrator actually wants delivered. The goal for most administrators is to prevent unsolicited commercial email from passing through these rules, yet allow legitimate emails to be delivered. This is a lofty goal, and a delicate balance. No perfect solution exists as long as people are willing to steal resources for their own commercial gain and go to great lengths to overcome the protections in place to prevent such abuse. However, in most environments it is possible to develop a reasonable set of rules that prevents most spam and allows most or all legitimate mail through unharmed.

It is important to understand the order of processing if complex sets or rules are to be used, as attempting to use a rule too early in the chain can lead to subtle errors or strange mail client behavior. Because not all clients react correctly to some types of refusals, and not all clients create correctly formed SMTP requests, it is not unlikely that a misplaced rule will lock out some or all of your clients from sending legitimate mail. It could also lead to opening a hole in your spam protections early in the rule set, which would allow illicit mail to pass.

The Postfix UCE controls begin with a couple of simple yes or no checks, called `smtpd_helo_required` and `strict_rfc821_envelopes`, both configured in the **SMTP Server Options** page. The first, if enabled, requires a connecting mail client to introduce itself fully by sending a HELO command.



This can stop some poorly designed bulk email programs. The second option requires the envelope to fit the SMTP specification precisely, enforcing complete headers. Though the envelope and HELO can be forged by a bulk mailer, it may stop the more hastily implemented variants.

The next stage includes the four SMTP restrictions also found on the **SMTP Server Options** page. These limit from where and to where mail will be delivered. The order of traversal for these four lists of rules:

6. **Restrictions on client hostnames/addresses** or `smtpd_client_restrictions`
7. **Restrictions on sends in HELO commands** or `smtpd_helo_restrictions`
8. **Restrictions on sender addresses** or `smtpd_sender_restrictions`
9. **Restrictions on recipient addresses** or `smtpd_recipient_restrictions`

Each of these checks can return REJECT, OK or DUNNO. If REJECT, the message will be refused and no further rules will be checked. If OK, no further rules in the given restriction will be checked and the next restriction list will be checked. If DUNNO, the list will continue to process the current restriction until it gets another result (OK or REJECT), or until the list end is reached, which is an implicit OK. If all lists return OK, the message will be passed to the regular expressions checks, otherwise it will be rejected.

Next are the regular expression-based `header_checks` and `body_checks`. These options, if enabled, provide a means to test the actual contents of the headers and the body of the email, respectively. Both operate in the same way, but they should be used somewhat differently. Header checks can be used to prevent well-known spamming domains from sending you email, or for stopping some well-known bulk-mailer software. By entering some signatures of the offender, like the domain name or the X-mailer field identifying the software, the mail can be rejected before the body is even sent. Body checks, though they use the same regular expressions and file format as header checks, should be used more sparingly, as the mail must be accepted before it can be checked. Thus bandwidth is wasted on receipt of the mail, and worse, the server will be occupied for a potentially long time processing the entire contents of every email. In short, use header checks whenever it is convenient and use body checks only when an effective header check cannot be devised. Only REJECT or OK are permitted for the returned values.

Note

Webmin, as of this writing (version 1.020), does not provide access to the regular expressions based checks, `header_checks` and `body_checks`. It is likely that a near future version will support these features, however.

Tutorial: Setting up a basic Postfix mail server

As with most of the server software documented here, Postfix has an intimidatingly large number of options and features. But, as we've already seen with BIND and Apache, even complex software can be easy and quick to set up if you know what to do to get started. Postfix is no different. At the end of this short section, you'll have a fully functioning mail server capable of sending and receiving mail on behalf of one or more domains.

In most environments, only three configuration details are needed to begin providing mail service with Postfix. First, browse the the **General Options** page of the module. The top two options, **What domain to use in outbound mail** and **What domains to receive mail for**, need to be configured to suit your environment.



For the first option, you will likely want to select Use domainname in order to select the domain name of your server as the source of email sent from it. For example, if my mail server is named mail.swelltech.com and I selected this option, mail will appear to originate from swelltech.com.

The second option specifies the domains for which you will receive email. The default is probably too restrictive in that it will only permit receipt of mail to \$mydomainname and localhost.\$mydomain, or the server itself. While this depends on your environment and needs, it is likely you will want to add the \$mydomain variable to the list of accepted domains.

The last step to making Postfix fully functional for sending and receiving mail is to ensure the **Local networks** parameter is set appropriately. If you only have one network block, this will already be set appropriately, as the default is to accept mail for delivery from all attached networks (i.e., all configured and active network addresses). However, if you have a public and private network interface, you'll likely want to remove to the public interface to prevent other clients of your ISP from being able to relay mail through your server.

Click the **Save and Apply** button to make your changes take effect. It is a good idea to test your changes to make sure things are working as intended. Assuming an appropriate DNS MX record has already been configured, as discussed in the BIND tutorials, you can send yourself an email at the new domain. Watch the maillog in the **System Logs** module for errors and to see if the message is delivered. Next, configure your mail client to send through your new mail server to ensure it is working for sending mail. The maillog will likely give clues about what is wrong in the event of problems.

Tutorial: Virtual Hosting email with Postfix

If you've performed the configuration in the previous tutorial, you'll be able to accept mail for any number of domains. However, this is not the same as providing independent virtual hosting support with Postfix. You can only have one user of a given name and mail sent to that user name at any of the domains for which you accept mail will be delivered. For example, if you hosted swelltech.com, penguinfeet.org and nostarch.com on the same server, and mail was sent to user joe at each of those domains, all three would end up in the same mailbox. Therefore, you have to introduce another layer to solve this problem.

Postfix has two commonly used methods. The first is the native Postfix method, using a virtual table to direct mail to the correct destination. The second method is modeled after the way Sendmail handles the problem and is a lot more complex. Because simplicity is better than complexity, you'll learn the native Postfix mechanism exclusively. The Postfix virtual man page covers both methods in moderate detail. If you have an older Sendmail installation that is being converted to Postfix, you may wish to use the second method and maintain your current virtual mail configuration. If you will be running an extremely large number of virtual domains, it is likely preferable to use the second method, as well.

The first step for setting up virtual domain delivery is to create a virtual map table using the **Virtual Domains** page. Enter the map type (hash, dbm, etc.), followed by the file name of the flat file that will contain the table information. For example, you could use /etc/postfix/virtual for this purpose. This is a pretty common location for this file.

Save and apply the change, and return to the **Virtual Domains** page. Click the **New mapping** button. You first have to create a generic map for the new domain. For the **Name** field, enter your virtual domain name. In the **Maps to...** field, you can technically enter anything you like (as long as we enter something). The custom seems to be to enter "virtual" in this field, as that is its purpose.



Click Save mapping to add it to the virtual table.

Next, add a postmaster alias, as all mail servers must have a functioning postmaster address to be compliant with the relevant RFC. Click New mapping again. This time, enter postmaster@virtual.domain into the **Name** field, where virtual.domain is the name of your domain. Enter postmaster into the **Maps to...** field so that mail to this address will be mapped to the local postmaster address for normal delivery.

You're ready to start adding your virtual domain users to the table. Once again, create a new mapping. Fill in your new virtual domain mail address in the Name field. For example, you might fill in joe@virtual.domain. In the Maps to... section, enter the name of a local user that you would like to receive mail for this address. In this case, you would use virtual-joe or perhaps virtual.domain.joe. This new local user must exist for mail to be delivered, therefore you'll need to add the new user to the system.

Now, **Save and Apply** your changes, and test it out: The virtual maps can be handled by various database types, or exported to an LDAP database. There is no reasonable limit to the number of virtual users and domains you can have.



21 Virtual Instance Setup Guide

21.1 Initial Configuration

ToolVox Virtual Machine Specifications: 500 GB Hard Drive, 2 Processor and 1 GB or RAM

After importing the appliance but before starting it, you will need to take a few steps to configure your new virtual machine.

1. Connect the machine's network port to your network. Since you will be connecting SIP phones to the instance, you must not configure the network port as NAT or another network type that obstructs communication. Bridged mode or similar is a good choice.
2. Ensure that DHCP service is available on the network that is connected to the virtual machine. ToolVox® will request a DHCP-provided IPv4 address by default. If you do not have DHCP service, you may manually configure networking after powerup.

Once these steps are complete, you may power up the virtual machine. You may determine the IP address it has obtained either via your DHCP lease table or by logging in via the virtual machine console. Sign in with your username (cbadmin) and password (CodeBlue92), and issue the command: `ifconfig eth0`.

The IP address, if configured, will appear after internet address.

21.2 Manual Network Configuration

Manual network configuration can be accomplished via the virtual machine console once the machine is powered up. Sign in with your username (cbadmin) and password (CodeBlue92), and issue `sudo system-config-network` at the prompt. From here, you can configure eth0 with static IPv4 information, as well as provide system DNS configuration. Once you've entered your configuration, issue `sudo /etc/init.d/network restart` to apply changes.

21.3 Licensing

The virtual appliance is shipped unlicensed. ToolVox® license keys are system-locked. Because we cannot predict your virtualization environment, you will need to provide us with an identifier that lets us provide you with a software license.

1. Navigate to the IP address with your web browser.
2. Click ToolVox® Administration.
3. Sign in with username (admin) and password (codeblue).
4. In the left-hand navigation bar, under Code Blue Software, click License Key Administration.
5. Copy and paste the values for System UUID and ToolVox® ID and provide it to Code Blue support. We will provide you with a license key that you can then paste into the license key field.

At this point, contact Solutions or Technical Support to schedule a remote ToolVox® Configuration and training Session.

technicalsupport@codeblue.com

solutions@codeblue.com

22 Download Information

Code Blue now has a centralized location where you can find installation, setup, information, configuration and operation instructions.

1. Centry[®] Administrator Guide: www.codeblue.com/resources/guides
2. CB 1 Series Administrator Guide: www.codeblue.com/resources/guides
3. CB 2 Series Administrator Guide: www.codeblue.com/resources/guides
4. CB 4 Series Administrator Guide: www.codeblue.com/resources/guides
5. CB 5 Series Administrator Guide: www.codeblue.com/resources/guides
6. CB 9 Series Administrator Guide: www.codeblue.com/resources/guides
7. CB RT Administrator Guide: www.codeblue.com/resources/guides
8. Phone Enclosures Administrator Guide: www.codeblue.com/resources/guides
9. Stainless Steel Maintenance Guide: www.codeblue.com/support
10. IA4100 Administrator Guide: www.codeblue.com/resources/guides
11. IP5000 Administrator Guide: www.codeblue.com/resources/guides
12. IP1500/2500 Administrator Guide: www.codeblue.com/resources/guides
13. ToolVox[®] X3 Administrator Guide: www.codeblue.com/resources/guides
14. Public Address Administrator Guide: www.codeblue.com/resources/guides
15. Blue Alert[®] MNS User Guide: www.codeblue.com/resources/guides
16. Blue Alert[®] EMS User Guide: www.codeblue.com/resources/guides
17. IP1500/IP2500 Firmware: www.codeblue.com/support/firmware
18. IP5000 Versions 1.X & 2.X Firmware: www.codeblue.com/support/firmware

For Legacy Product Information:

www.codeblue.com/legacy-products

These guides should contain all the information needed for your application. If further information is required, please contact **customerservice@codeblue.com**.