MiVoice Connect

Mitel Emergency Notification Server User Guide

August 2023

Mitel®

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

1 INTRODUCTION

- This document describes how to install, configure and use the Mitel Emergency Notification Server Version 5 software. The server is packaged as a pair of Microsoft Windows services configured to run automatically whenever Windows starts. It can be installed and run on any Winders server PC running the Mitel server software including a Mitel Headquarters (HQ) server or Mitel DVS Server. The two services which comprise the server are:
- The **STPS EN service** which monitors and responds to emergency calls.
- The **STPS EN Watchdog service** which monitors the health of the main service and starts or restarts it if it is not running or becomes unresponsive.

In addition to the services, a program for configuring the server (**the Admin**) is also provided. This must be run on the same server machine as the service. It allows configuration changes to be made whether the service is running or not. If the server is running then any changes are processed as soon as they are applied unless the server is involved with an active emergency call event. In this case, the processing of any changes is internally queued until the call and related activities are all completed. The service supports several types of debug related log files, intended primarily for diagnosing possible problems. In addition, the server writes an application log file which records all user client connect and disconnect events, messages sent between users and most importantly each emergency event call and any and all responses or acknowledges related to those calls. The application log file can viewed by opening the current log file or by using the separate provided **Log Viewer** application.

As a companion to the server, there is a **client application** with its own installer and documentation. This connects to the server and provides screen pops in response to emergency or event calls, an integrated log view, messaging with other connected clients and a window to monitor the health and status of the server via a TCP/IP connection. It may be advantageous to install the client on the server machine for local testing and also to take advantage of the client's Server Status view to check the health of the server.

You must take special notice of the Testing section at the end of this document. Considering the critical role that this solution plays within an organization's emergency response strategy, Mitel recommends that customers maintain close attention to the health of the application and in particular routinely perform test calls to ensure that it operates as expected.

2 OVERVIEW

When the server is running it typically monitors for two types of calls:

- Internal calls and external calls to one of the configured emergency numbers, for example 9-911 (external) or 2345 (internal).
- Internal calls to the configured event route point extension(s). For example, 2600.

To detect external calls to configured emergency numbers, the server monitors the trunks for outbound emergency calls. To detect internal calls to configured internal numbers the server will monitor the appropriate extensions. For emergency calls, the server will not interfere with the call itself. Only the call activity is monitored. Specifically this application does not support any mechanism for users to be able to listen in on or redirect a call made to an external emergency number.

The server also monitors any configured event route points for inbound calls. When a call to an event's route point is detected the server preforms some or all of the following actions depending on the event's configuration:

- The call is answered.
- An automated voice announcement is played to inform the caller that they are generating an event. This announcement can use either a pre-recorded prompt wave file or dynamically generated speech using Text-To-Speech (TTS). See the appendix at the end for details on configuring the TTS support.
- Depending on configuration, the server can handle the event as soon as the inbound call presents to the route point or it can wait until after the calling party has heard the full announcement message. This allows the message to tell the caller to hang up if they dialed the number in error and give the caller time to respond.
- When the message completes, or, instead of a message the call can be transferred to another number, internal or external.

Regardless of whether the server is processing an emergency call event or an internal call event it can potentially respond in a number of ways:

- Logs a message to the Application Log file with the particulars of the call including the calling party's name, extension, site and location and the time when the call is detected.
- Logs a message to the Windows event log.
- Notifying any connected clients who are enabled for the event type. This includes the specific call type (emergency call and/or specific internal event call) and the caller's site. Users receive a pop-up on their screen along with an optional configured audio announcement and can respond by clicking to indicate acknowledgement of the notification. Any client acknowledgements are logged to the application log.
- Placing contact notification calls to any configured internal and/or external numbers enabled for the call type and calling site. All contacts receive voice prompts when they answer the call notifying them of details of the event. Following the announcement, the contact is prompted to press any key to acknowledge the call. If they fail to respond, the message can be repeated several times to give the called party the opportunity to respond. The overall results of the contact call are logged in the application log along with any acknowledgement. In addition, if the called party is an internal party with an IP display phone, the offering calls can optionally show in their display with a message indicating details of the call.
- Making call(s) to configured external paging devices which are enabled for the event type.
- Emailing contacts that are enabled for the event type with details of the event.
- Interfacing via the separate Mitel Enhanced Page Application in order to generate a notification page to an Enhanced Page Group if enabled for the event.

3 UPGRADING FROM MITEL E911 NOTIFICATION APPLICATION

This section describes how to upgrade a customer's existing Mitel E911 Notification Application to the newer Mitel Connect Director Emergency Notification (SEN) Application.

Follow these steps:

1. Review the current configuration of your E911 Notification Application. For this you'll want to run the E911 Notification Admin program and make note of the current contacts. You will likely want to have the same contacts notified with the new SEN system in which case you'll want to record the current contact names and numbers. In addition, you'll want to record the current route point being used by the E911 Notification Application by checking advanced settings. You'll presumably want to use the same route point for the SEN.
2. Uninstall the 911 clients if the clients need to be upgraded. Start by going to each client PC, opening the Control Panel and running Add/Remove Programs. From Add/Remove programs, locate the Mitel 911 client and remove it. Repeat this for each client PC.

   If needed, once all clients have been uninstalled for the client PCs you can then uninstall the server. On the server machine, open the Control Panel and select Add/Remove Programs. Locate the Mitel 911 Server and remove it.

Note! It is critical that you uninstall the 911 server and if needed, all of the clients before installing the new Mitel Connect Director Emergency Notification Application (SEN.)

With all of the clients and the server uninstalled you are now ready to install the new SEN Server and optionally the new clients.

4 INSTALL THE MICROSOFT TEXT TO SPEECH ENGINE AND VOICES

The Emergency Notification application support playing pre-recorded audio as well as using Text to Speech technology to play dynamically generated audio event details on notification calls. If administrators don't want to use Text to Speech for any contact call or event interactive voice then they don't need to install the Text to Speech support. However, most users will want to take advantage of Text to Speech support. To install the Text to Speech Engine and voices, see Appendix A: Configuring the Text to Speech Support. It is suggested that this step be done first, before installing the server.

5 INSTALL THE LICENSE

Along with the software, you may also have received a license for the Emergency Notification application. Installations are typically licensed for either up to 5 client users and 5 contacts OR up to 50 client users and 50 contacts.

Before you install and configure the application its best if first install the license using the Mitel Professional Services License server's web admin. If the professional services license server and associated web admin have not yet been installed then you must first install the License server and admin. The license server software can be downloaded along with installation and usage information by Mitel partners from:

http://partners.shoretel.com/support/products/applications/licensing_server.html

If you have not yet received your permanent license or you are testing the application on a trial basis then you can use the temporary license good for 45 days.

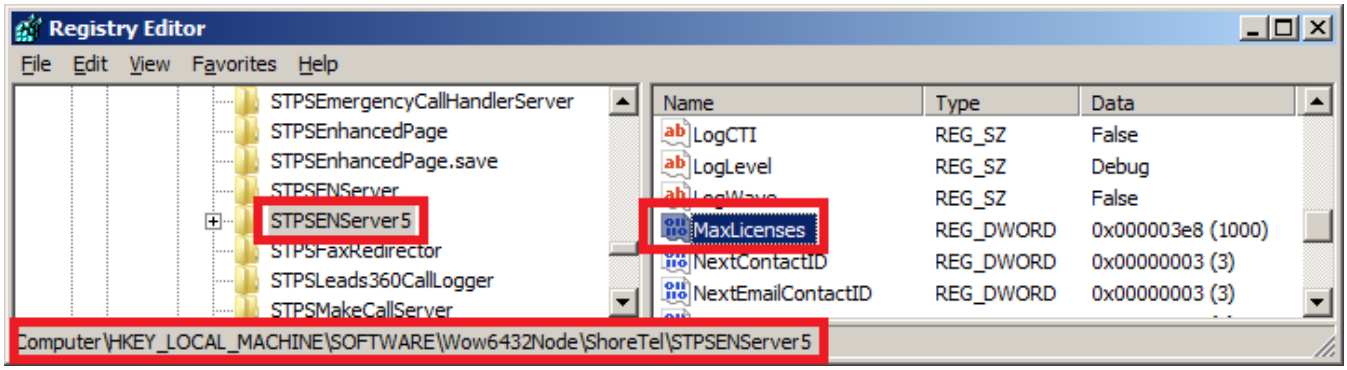
This is the trial license key that you can copy and paste into the Mitel Professional Service license application's web admin. Ensure you copy from the word "Emergency" through the two equal signs at the end of the license string. If you are inserting a permanent license then you should have received a similar string as part of your order that is your unique license key:

Emergency Notification|5|Trial License| |0|3/23/2010

20:48:35|3/23/2010|5/7/2010| |1|1440|jybUY5Olr3I4hXhA5u3I9g|1.0|gw5RpKTy51Sv41mUkq/Pjuek/ZSE

mHzKP7M7ILKcasT/q2EW6t+k5A==

Normally, customers will install a single instance of the Emergency Notification server on their network. However, in some situations, customer may benefit from installing multiple instances of the Emergency Notification Server. In this case they will want to allocate the available licenses on a server by server basis. So, for example, they might purchase 100 licenses total for two server and want each server to use up to 50 of the licenses. In this case it is necessary to set a Windows registry value to force the server to request a lesser number of licenses. If this registry value is changed while an EN service is running the service must be restarted for the change to take effect. A DWORD registry value named MaxLicenses and located at *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ \STENServer5* should be set to the integer value to use for the maximum licenses the server should request:

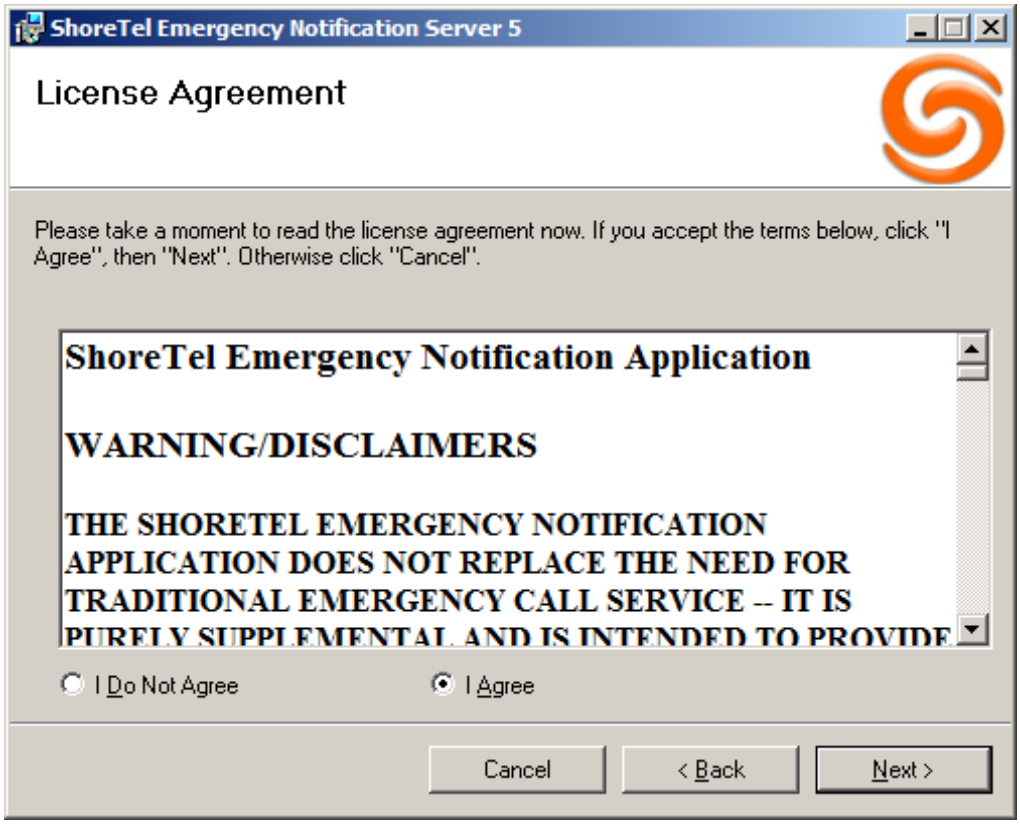


6 INSTALLING THE EMERGENCY NOTIFICATION SERVER

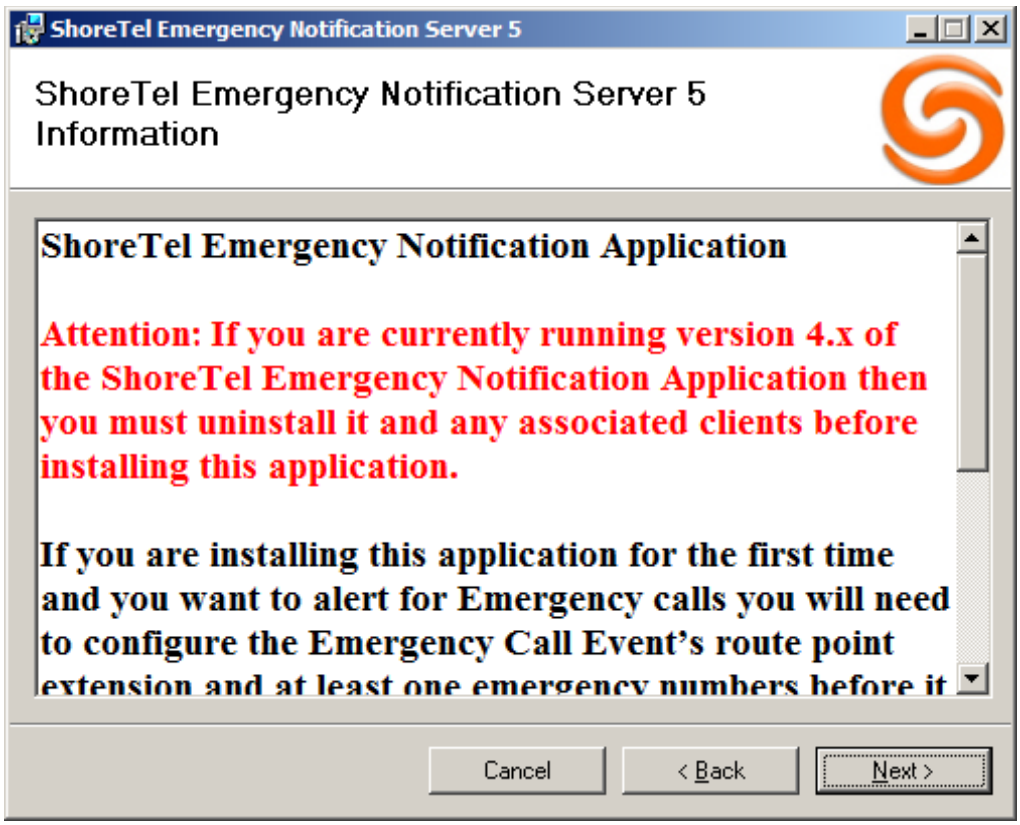
The Mitel Emergency Notification Server consists of the two Windows Services, the main service and the Watchdog service along with an associated Admin and Log viewer programs.

A requirement of the Servers and utilities is the Microsoft .NET runtime. The install program will direct you to the Microsoft web site to download and install it if you do not already have it installed.

To install the Server, run the setup.exe application in the folder containing the server's msi file (named something like STENServerSetup5.0.8.msi). Early in the install you should be prompted with the License Agreement. Review the content and if acceptable, select "**I Agree**" and click **Next**:



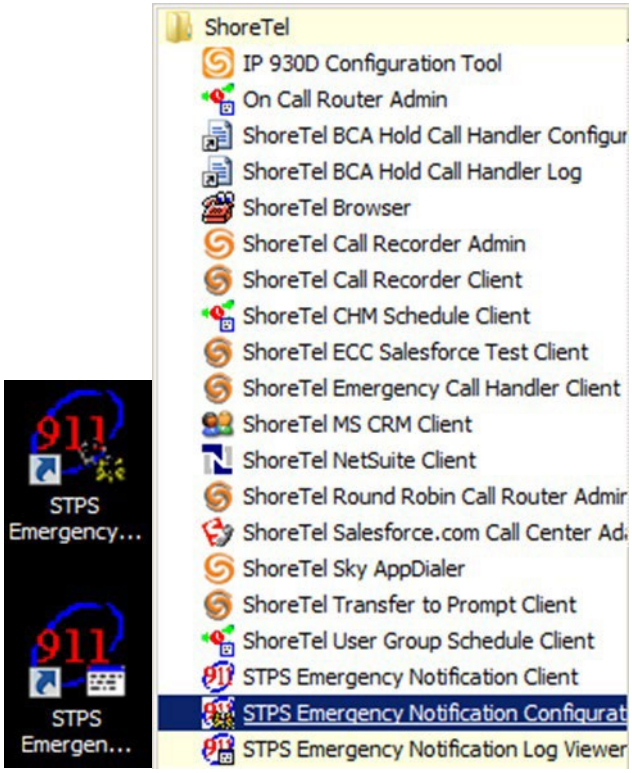
Following the License Agreement is a read me screen. Carefully review these instructions if you are upgrading from a previous version of the Mitel Emergency Notification Server:



Ensure to carefully read the text which explains the requirement to configure the route point and emergency number(s) with any required trunk access prefixes.

At the end of the server install, the Mitel Emergency Notification Server Admin application should be automatically started. This allows any additional configuration to be made. The reader is referred to the section “Configuring the Mitel Emergency Notification Server” for instructions on using the Mitel Emergency Notification Server Admin application.

When the install is complete, shortcut icons for the STPS Emergency Notification Configuration and the STPS Emergency Notification Log Viewer applications will be added to the user’s desktop as well as to the “Start | All Programs | Mitel” folder:



7 INITIAL CONFIGURATION

When initially installed, assuming it you aren't upgrading an existing compatible version, the application won't be configured to monitor for any type of calls. Some configuration must be made using the Admin utility to enable the application to function.

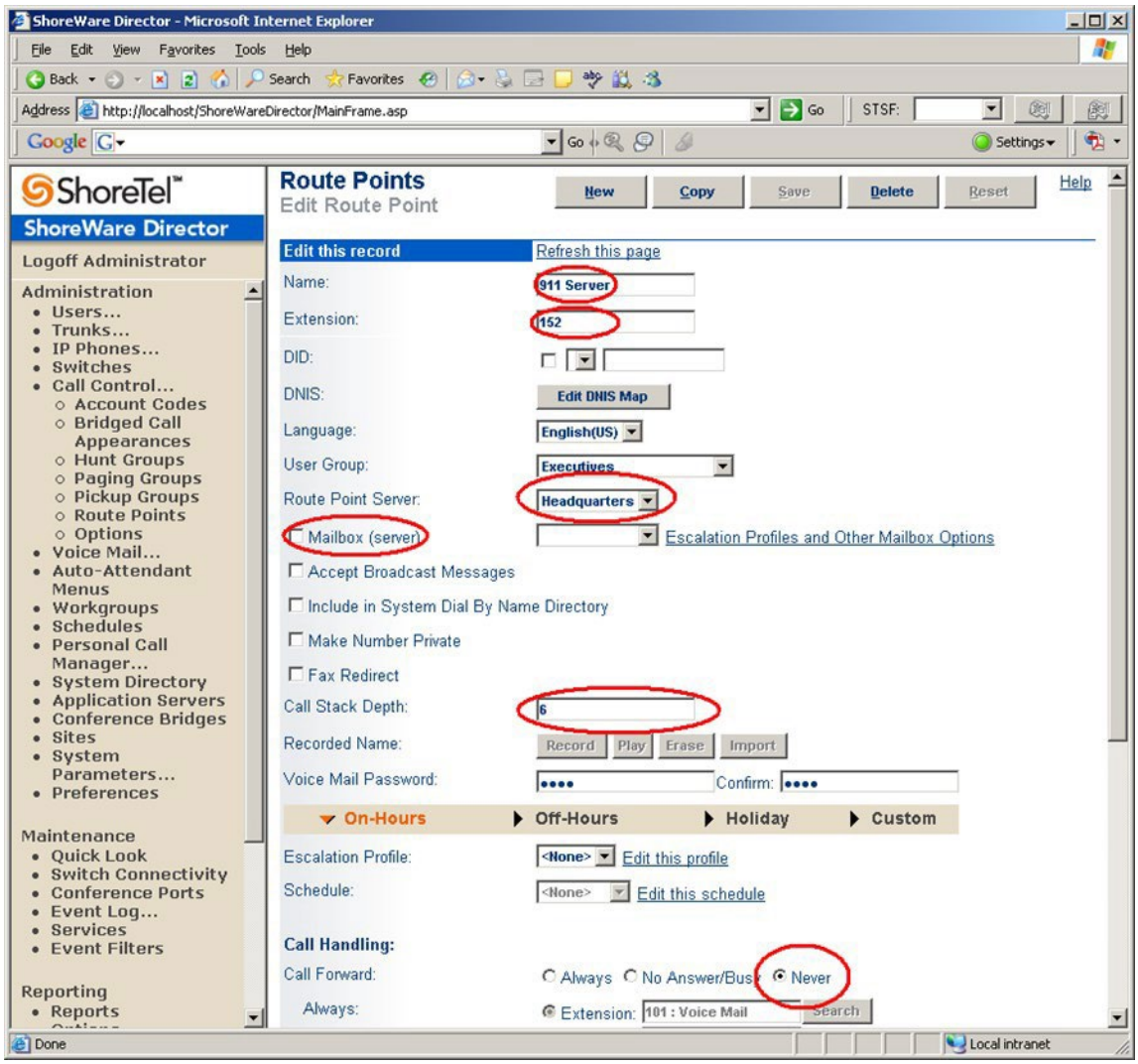
Depending on what is being configured, the user may want to create one or more route point extensions using Mitel Connect Director. Route points are used for two purposes.

1. Receiving inbound calls which trigger internal call events.
2. Placing outbound contact calls in response to a call events for all event types (emergency and internal.)

Note! For systems using On-Net Dialing (OND) prefixes, while configuring the Mitel Emergency Notification application, do not add hyphen in the route point or extensions.

The route points used should have a call stack size of at least the maximum number of contact calls the user is licensed to be able to make. In addition, for the route points used for internal call events, some additional call stack positions should be added to handle the maximum anticipated number of simultaneous inbound calls. When creating the route points you must insure that the Route Point Server setting is set to the Mitel server that the Emergency Notification server is installed on. Ensure that the User Group assigned to the route points are allowed to make external calls (assuming you want to configure external contacts.) Finally, you'll usually want to disable the mailbox and forwarding of calls.

This shows the important fields in configuring the route point in Director:



In addition to configuring the route points, for detecting external emergency calls you'll also need to configure the emergency number(s). Most North American users will want to configure x911 where x is their trunk access code.

So, for example, a site that uses 9 as a trunk access code would want to configure an emergency number of 9911. If they also used 8 as a trunk access code then they would want to also add 8911 as a second emergency number.

 **Note!** The hunt group design is updated and in the new design, the **hunt_pickup** option is set to 1 by default. Therefore, the STPS Emergency Notification no longer sends notifications for hunt group calls unless you deactivate the recent hunt group update by setting the **hunt_pickup** option to 0.

8 LOCATION AND SITE SUPPORT

The server supports a feature to provide location and site information as part of a call notification in addition to the extension and name of the calling party. Because this feature involves direct access to the Mitel Database rather than connection via the telephony link, the Connect Director Emergency Notification Server must be installed and run on a Mitel (HQ or DVS) server.

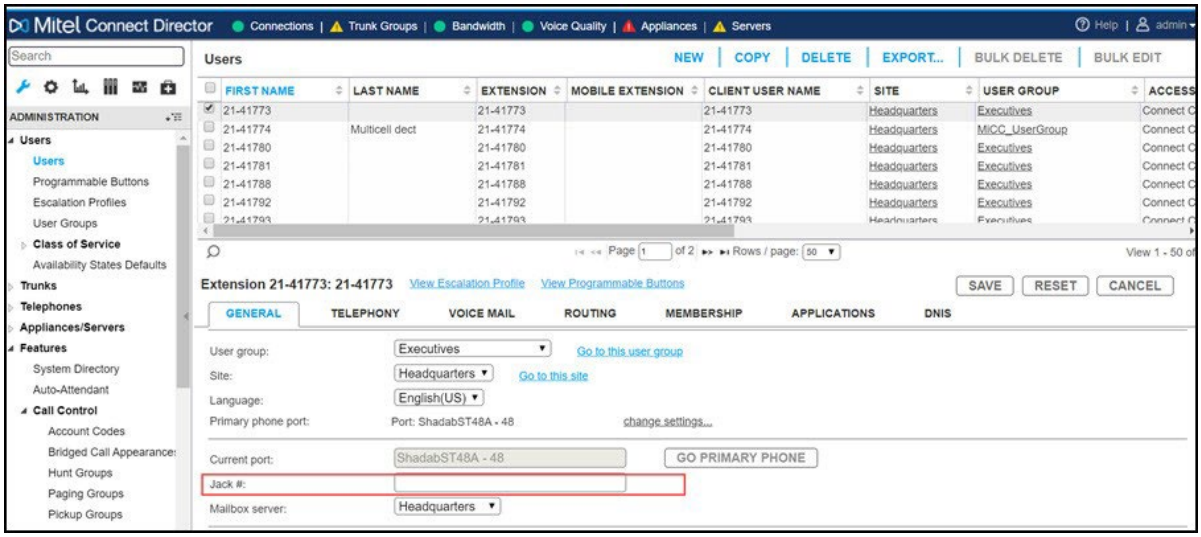
The location and site information of the caller, if available and set, are shown in the client screen pop. In addition, if the **Contact Call Setting Play Location** is enabled and the caller's location contains any digits and the dash character, then these digits are played to the contacts following the playing of the caller's extension. For example, if the location is specified as "Building 2 - Room 119" then the caller will hear, following the caller's extension: "...from location 2...dash...1...1...9...".

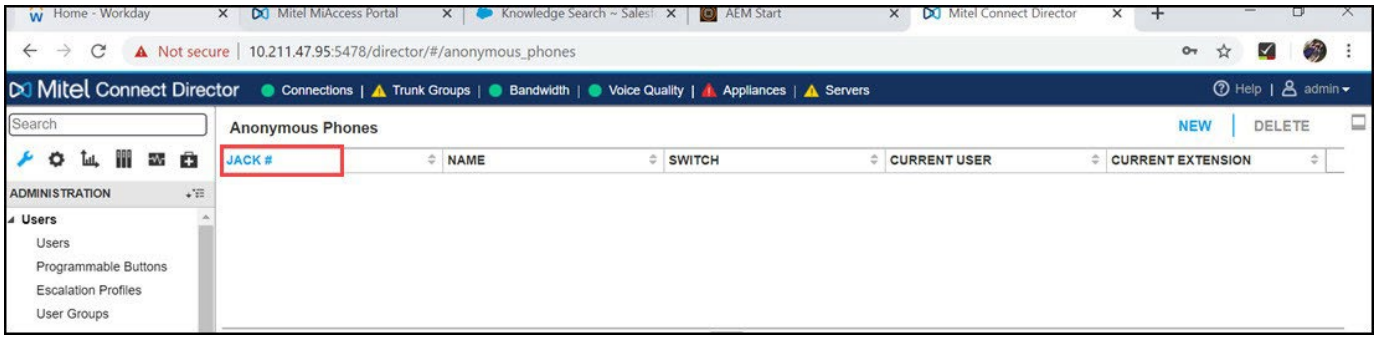
The Mitel user and anonymous telephone settings in Director do not provide a field for setting the actual location of the phone device. This solution uses the Jack # field to store location information. This is a free form text field of up to 50 characters. It is informational only and is not used by the Mitel phone system. Therefore, for location information to be effectively provided, administrators of the Mitel phone system should adopt the convention of storing location information in the **Jack #** field.

Note!

- The location information will correctly change to reflect current Office Anywhere assignments. For example, if the "Jack #" for a user at their home phone is "Room 123" and they place an emergency call, their location will be reported as "Room 123". However, if they reassign their extension to another user's phone and that phone has a "Jack # of "Room 987" and they then place an emergency call, their location will be reported as "Room 987".
- Connect Director will only allow a Jack # to be set for Users who have a home port of "IP Phones" or "Ports". Users with a home port of SoftSwitch cannot be assigned a Jack #. By definition, if these users place an emergency call they must be assigned to user's phone or to an anonymous phone. In either case, the location reported will be from the Jack # of the relevant user or phone record.
- Jack-based location information is not transmitted to the Emergency Notification server when the user switches from deskphone mode to softphone mode and makes an emergency call.
- Jack-based location information is not supported in softphones.

The graphic below shows the relevant screens from Director for setting the Jack # (location):




Home - Workday
Mitel MiAccess Portal
Knowledge Search ~ Salesf
AEM Start
Mitel Connect Director
Not secure
10.211.47.95:5478/director/#/anonymous_phones
Mitel Connect Director
Connections
Trunk Groups
Bandwidth
Voice Quality
Appliances
Servers
Help
admin
Search
Anonymous Phones
NEW
DELETE
JACK #
NAME
SWITCH
CURRENT USER
CURRENT EXTENSION
ADMINISTRATION
Users
Users
Programmable Buttons
Escalation Profiles
User Groups

9 EXTERNAL CALLER'S SITE AND LOCATION SUPPORT

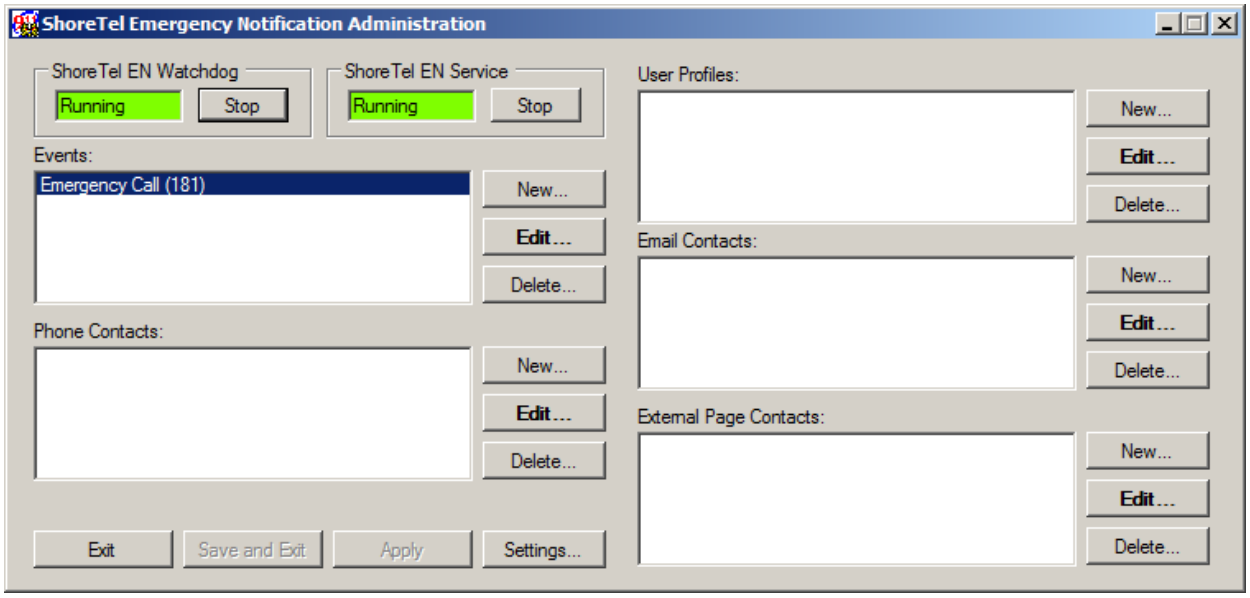
Calls received externally have a site of "External" and a location of "Unknown". If a code event to an internal event is received from an external source and assuming the event is not configured to "Ignore and disconnect external calls" then the server will respond by calling those parties that are configured to respond to the event when the calling site is "External".

10 EMERGENCY NOTIFICATION SERVER CONFIGURATION

The Configuration program is automatically run at the end of the server install. It can be run from the desktop shortcut or “Start | All Programs | Mitel | STPS Emergency Notification Configuration” shortcut.

11 SERVER CONFIGURATION MAIN SCREEN

The graphic below shows the main window of the configuration application following initial installation:



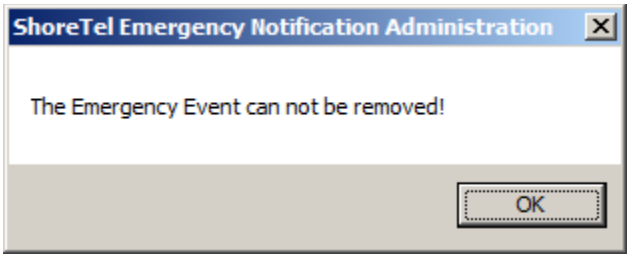
The main form consists of several areas or panes along with a number buttons associated with each pane:

- The top left **Mitel EN Watchdog** pane shows the **Status** of the **Mitel Emergency Notification Watchdog** service. It is typically running but can show starting, stopping or stopped. The service is automatically started by the install program and is configured to start automatically whenever Windows is started. As soon as it starts it should automatically start the Emergency Notification service itself. The user can use the **Start/Stop** buttons to control the running status of the watchdog server. The service can also be started and stopped from the Windows Services administrative tool. The service's name is: "STPS Emergency Notification Server Watchdog."

  Note! To stop the main service, you should first stop the watchdog otherwise it will periodically attempt to restart the main server.

- The top middle **Mitel EN Service** pane shows the **Status** of the **Mitel Emergency Call Notification** service. It is typically running but can show starting, stopping or stopped. The service is automatically started by the watchdog service which is configured to start automatically whenever Windows is started. The user can use the **Start/Stop** buttons to control the running status of the service. However, if the watchdog is running it will automatically restart the service if it is stopped. Therefore, to stop the main service you should first stop the watchdog service. The service can also be started and stopped from the Windows Services administrative tool. The service's name is: "STPS Emergency Notification Server."
- The **Events** pane lists the configured events. To edit an event's settings, select it and click **Edit** or double click on the event. To add a new event, click the **Add** button and to delete an existing event, select the event and click the **Delete** button.

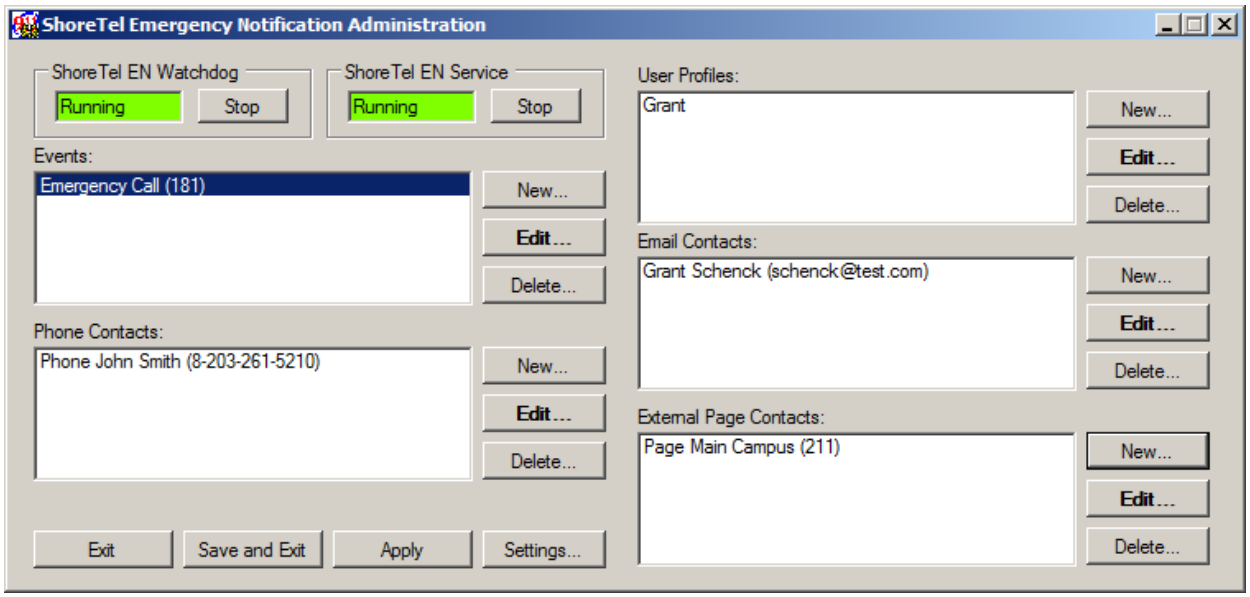
  Note! The Emergency Event can't be removed. Attempting to do so will result in this message:



See the Configuring Events section below on configuring events for details on adding or editing events.

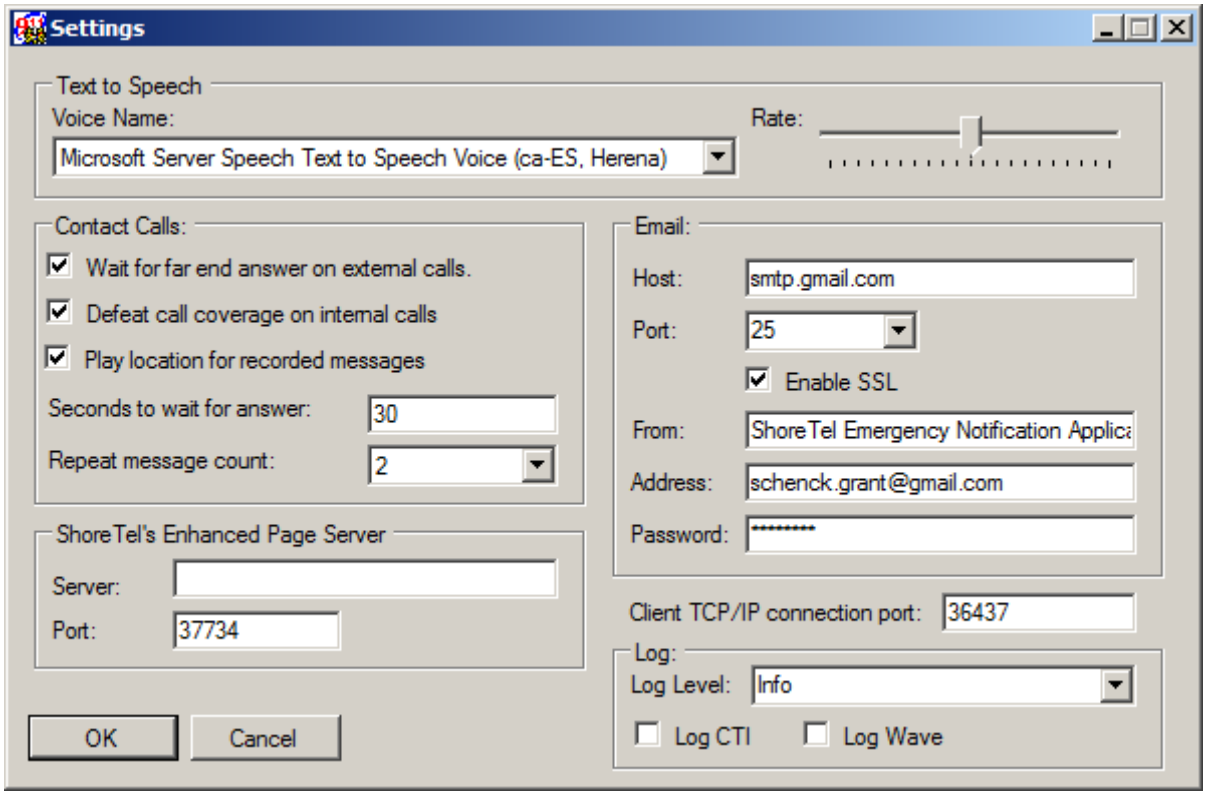
- The **Phone Contacts** pane lists the phone contacts that can be called for events. A phone contact is a name and phone number (internal or external) who can be called in response to call event(s) at specific site(s). To edit a phone contact's settings, select it and click **Edit** or double click on the contact. To add a new contact, click the **Add** button and to delete an existing contact, select the contact and click the **Delete** button. See the Configuring Phone Contacts section below on configuring phone contacts for details on adding or editing phone contacts.
- The **User Profiles** pane lists the user profiles. When you configure a client a key setting is the user profile that client is assigned to. A User profile defines which call event(s) at specific site(s) a client user should be alerted for. To edit a user profile's settings, select it and click **Edit** or double click on the user profile. To add a new user profile, click the **Add** button and to delete an existing user profile, select the user profile and click the **Delete** button. See the Configuring User Profiles section below on configuring user profiles for details on adding or editing user profiles.
- The **Email Contacts** pane lists the email contacts that will be sent an email in response to an event. You'll need to configure an SMTP email provider in the server settings dialog (see below) in order for the email contact feature to work. An email contact is a name and email address which can be emailed in response to call event(s) at specific site(s). To edit an email contact's settings, select it and click **Edit** or double click on the contact. To add a new contact, click the **Add** button and to delete an existing contact, select the contact and click the **Delete** button. See the Configuring Email Contacts section below on configuring email contacts for details on adding or editing email contacts.
- The **External Page Contacts** pane lists the external contacts that will be called and played a pre-recorded message in response to an event. An external contact is a name and phone number along with a number of settings which control and guide the Emergency Notification Application server's interaction with external page contacts. To edit an external page contact's settings, select it and click **Edit** or double click on the contact. To add a new contact, click the **Add** button and to delete an existing contact, select the contact and click the **Delete** button. See the Configuring External Page Contacts section below on configuring external page contacts for details on adding or editing external page contacts.
- The **Settings** button displays the settings dialog. The settings dialog controls the server wide settings, specifically the contact call settings, the enhanced page server location, the email server settings, the client connection port and the server log settings. See the Settings section below on configuring the settings for additional details.
- If/when you make changes, the **Save and Exit** and the **Apply** buttons will become enabled. Clicking either will update the server settings and if the server is currently running, the changes will be processed immediately or, if any emergency calls are active, as soon as the server is done handling the emergency calls.

This shows the dialog with two events and one configured contact for each of the types of supported contacts:


ShoreTel Emergency Notification Administration
ShoreTel EN Watchdog
Running
Stop
ShoreTel EN Service
Running
Stop
Events:
Emergency Call (181)
New...
Edit...
Delete...
Phone Contacts:
Phone John Smith (8-203-261-5210)
New...
Edit...
Delete...
Exit
Save and Exit
Apply
Settings...
User Profiles:
Grant
New...
Edit...
Delete...
Email Contacts:
Grant Schenck (schenck@test.com)
New...
Edit...
Delete...
External Page Contacts:
Page Main Campus (211)
New...
Edit...
Delete...

12 SETTINGS

The settings dialog provides some system wide settings used by the server. Clicking **Settings…** from the main window displays this dialog:



The top section contains the **Text to Speech Settings**. These settings allow a specific TTS Voice Name to be selected and the playback **Rate** (from -10 to 10 with zero being normal) to be selected. See Appendix A: Configuring the Text to Speech Support regarding configuring the Windows Server Text to Speech Engine which covers downloading and installing the service as well as downloading and selecting TTS voices.

The middle left section contains the **Contact Call Settings**. These settings control how the server handles the outbound contact calls it makes:

- **Wait for far end answer on external calls**

  When calling external contacts on most trunks, the server is able to detect when the called party actually answered the call. However, certain trunk types such as analog trunks may lack this detection. In this case this option needs to be un-checked so the outbound IVR will not wait to start playing for the far end answered event that will never come.

- **Override CHM on internal calls**

  Normally, the contact calls made to internal extensions will just follow any forwarding set at the user's phone. However, if customers want contact calls to "punch through" and always alert the users phone then they should clear this option.

- **Play location for recorded messages**

  If the contact call feature is using Recorded Messages to support the outbound IVR then this setting controls whether the IVR will attempt to play any location details. Note that this rendering is quite limited vs. text to speech. Specifically only digits and the dash character that are part of the location are played. See the Configuring Phone Contacts section on the Event's Contact Call IVR below for more details.

- **Seconds to wait for answer**

  When making contact calls, if we don't see the call connect within this timeout we give up and log the contact as not answering.

- **Repeat message count**

  This controls how many times the outbound message is automatically repeated before the call hangs up.

The bottom left section contains the **Mitel Enhanced Page Server Settings**. These settings provide the server name or IP address and the port where the Emergency Notfication Server expects to connect to the Mitel Enhanced Page Server:

- **Server:**

  This is the server name or IP address where the Mitel Enhanced Page server is running. If left blank the Emergency Notification server will try to connect to the Enhanced Page server running on the same PC.

- **Port:**

  By default, the Enhanced Page Server listen for connections on port 37734. If you for some reason you configured the Enhanced Page server to listen on a different port then you'll need to change the port setting to match.

The middle right section contains the **Email Settings**. These settings provide the detailed needed for the Emergency Notification server to send emails in response to events. These settings provide the SMTP Host, port, SSL settings as well as the sending account's name, address and password:

- **Host:**

  This is the email server. You'll need to contact your mail provider for the host that should be configured.

- **Port:**

  This is the email server's port. Most providers use port 25 or port 587 but your provider may use another value. Like the host setting your email provider can provide the port value you should use.

- **Enable SSL:**

  If your email provider uses Secure Sockets, then you'll need to check Enable SSL.

- **From:**

  This is the name of the sending party that email recipients will see in the message header.

- **Address:**

  This is the sending email address and must be a valid email address for the configured host you are using.

- **Password:**

  This is the password associated with the sending email address.

Towards the bottom right, the **Client TCP/IP connection port** sets the port that the server expects the clients to connect on. Since the default value is (36437) is the same value that the clients expect to connect on it is best to leave this unchanged unless there is a specific conflict in the customer's network.

Lastly in the bottom right, the Log Settings control the several debug related log features. The two debug logs are:

- **Log Level**

  This controls the internal log of the service. It is the primary log that is used to diagnose field issues. Log Level ranges from Off through Debug.

- **Log CTI with optional Log Wave details**

  These settings control a lower level log that provides details of the underlying computer telephony interface and an extra level of detail regarding wave related events.

Typically these log settings would only be changed if requested by Mitel Advanced Applications group. For most issues, setting the Log Level to debug while not enabling Log CTI or Log Wave should be sufficient.

13 DEBUG LOG FILE LOCATIONS

The server potentially creates three sets of debug log files. The main Debug log, the one controlled by the above Log Settings: Log Level, is named STPSENDebug.log and stored in the Debug Logs folder of the application's install folder. For example:

C:\Program Files (x86)\Mitel\Mitel Emergency Notification Server 5\Debug Logs

Each day that the server runs, a new file is written and previous files are renamed to conating the year, month and day as part of the file name, for example:

STPSENDebug.log20130829

If the Settings: Log CTI is enabled then a second set of CTI (Computer Telephony Integration) log files are written to the Debug Logs folder of the application's install folder. At most, seven of these logs are written and after one week are overritten assuming the server is running at midnight and CTI logging is enabled. These log files have the format:

STPSEN_CTI_<day of the week>.Log

So, for example, STPSEN_CTI_WEDNESDAY.Log would contain the CTI log details from Wednesday.

If the Settings: **Log Wave** is enabled and Log CTI is also enabled than additional details related to the wave playback activities of the underlying CTI interface will also be logged. This logging is should almost never be requested and should not be enabled normally due to the large log files that can result.

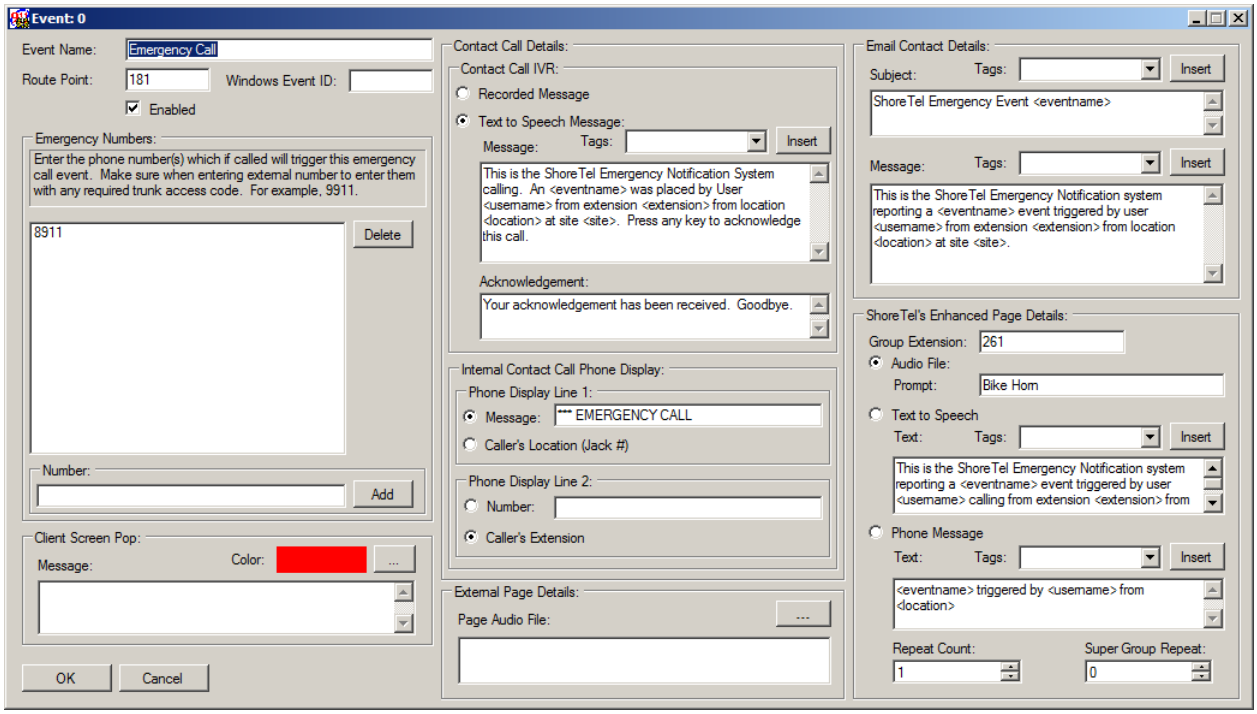
14 CONFIGURING EVENTS

There are two types of events that the server can be configured to respond to:

- Calls to external and internal emergency numbers.
- Calls to internal emergency event route points.

The Add/Edit dialog displays somewhat different details for the Emergency Call event vs. other events. Specifically, the Emergency Call event provides configuration of the actual external emergency number (such as 9-911) that should be considered emergency calls and other events provide configuration of what the calling party will hear when calling the event's route point (the inbound interactive voice response treatment or inbound IVR.)

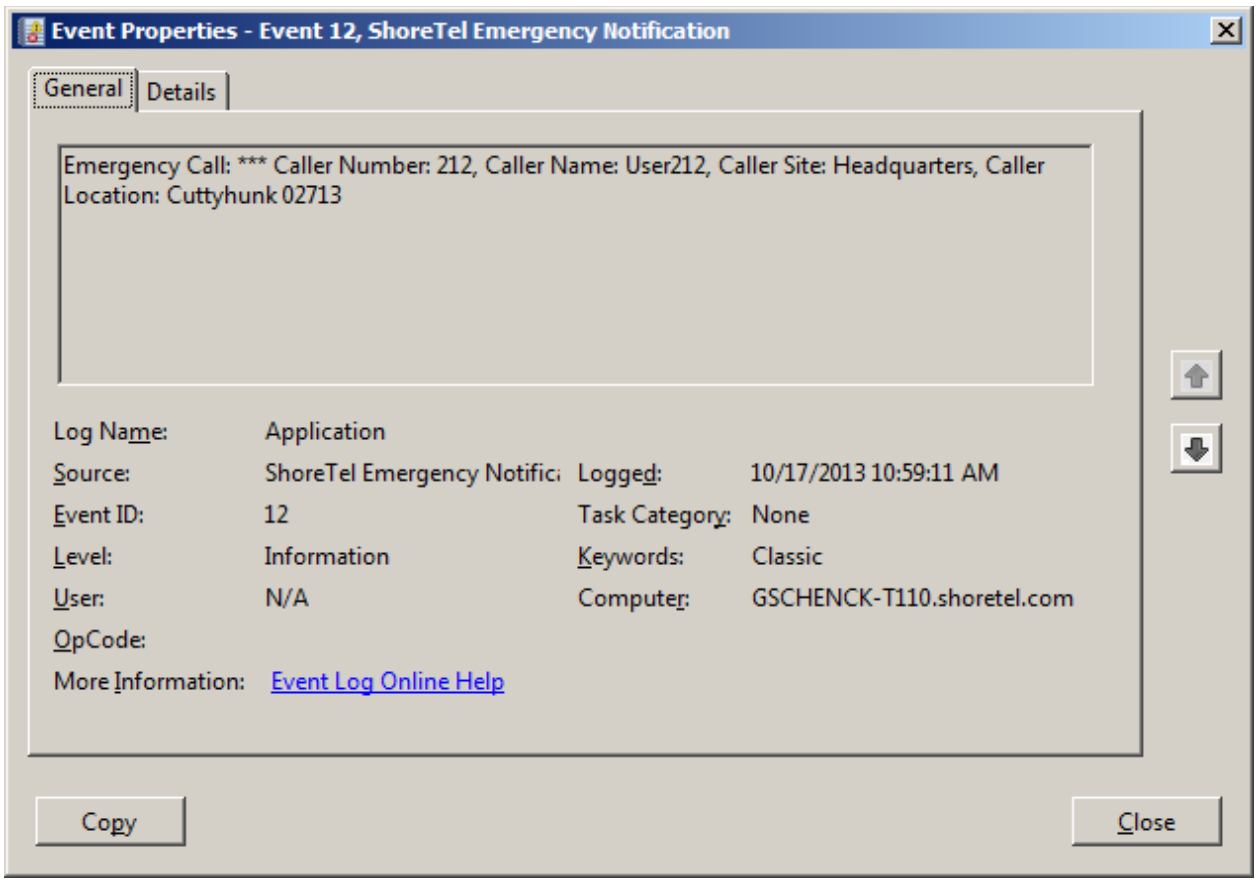
This shows the initial configuration of the Emergency event:



In the upper left is the **Event Name**, the **Route Point** assigned to the event, the optional **Event ID** to be logged in the Windows event log and the event **Enabled** setting. For the emergency event, the route point is used to call any contacts for the event. The route point for the Emergency event is optional if the customer doesn't intend to assign any Phone or External Paging System contacts to be notified of the event. For all other event types, the route point must be set to a valid route point extension for the event to function.

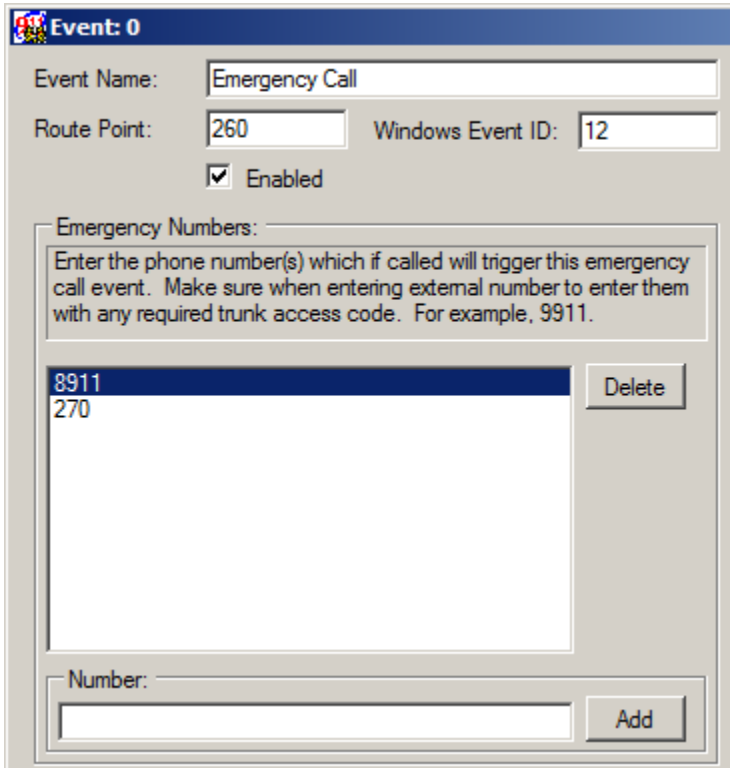
Note! All route points must be unique. You cannot share a single route point across events! In addition, you should never configure a code event route point as an emergency number. Events can be enabled or disabled using the **Enabled** checkbox.

If set, the Event ID will be used to log an event to the Windows event log with details about the event. For example, this shows an Emergency Call event:

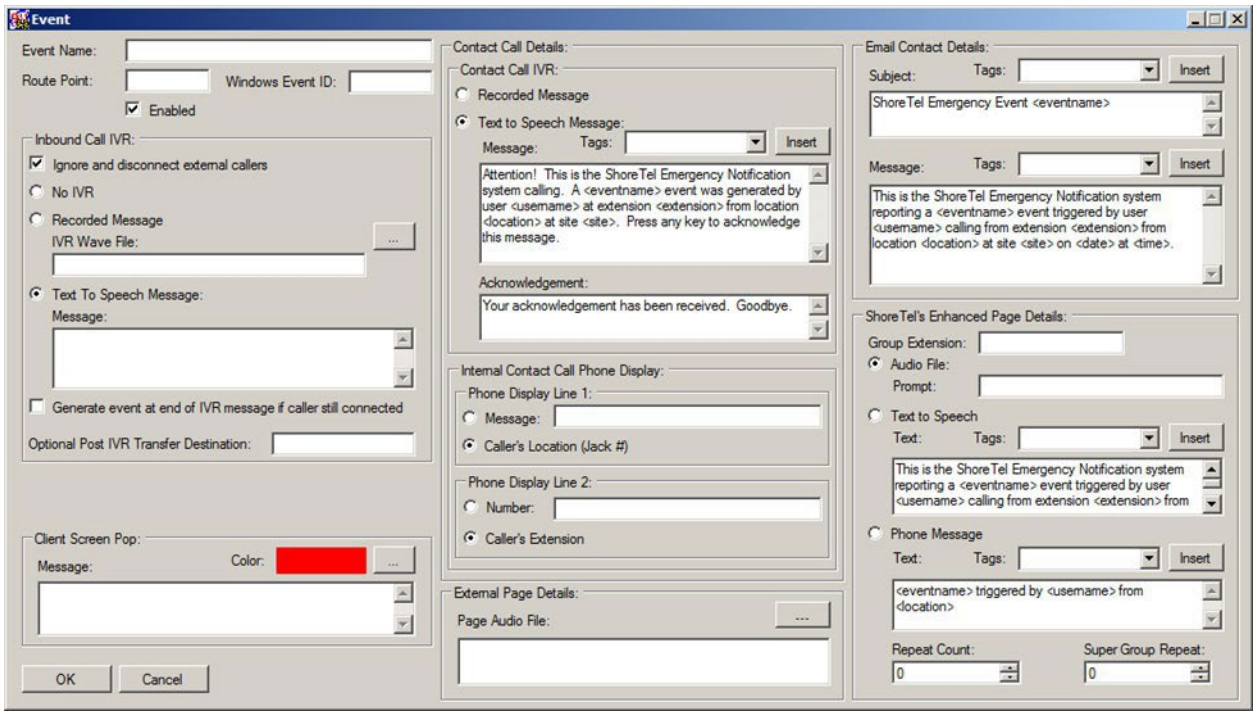


For the Emergency Event only, the next section is where the **Emergency Numbers** are configured. This is the list of internal and external numbers. Make sure that you include any required trunk access codes when configuring external numbers. For example, to handle a call to 911you would enter it along with the trunk access code(s) that the system would use when making the call. For example, if 8 is the trunk access code then you would want to configure 8911 as an emergency number. If both 8 and 9 are used then you'd configure both numbers, 8911 and 9911. To add a number, enter it in the **Number** field and click **Add**. To delete an existing number, select it and click **Delete**.

This shows the Emergency Call event set up to use route point "260" and trigger on both calls external number 8911 and internal extension 270:



To contrast with the non-Emergency Event types, from the main Admin screen we click **New…** in the Events section this shows the event dialog for the internal events:



Note! The Emergency Numbers section is replaced with an Inbound Call IVR section. You must provide a name and a route point for the event. Since the non-Emergency events are triggered by placing a call to their route point, the event will not function until a valid route point is set, even if there are contacts configured for theevent.

The **Inbound Call IVR** section controls the message heard by the party calling the route point to trigger the event.

The first checkbox, **Ignore and disconnect external callers**, controls whether or not the event can be triggered by external callers as well as internal callers. It default to checked, that is external callers can not trigger the code event. To allow external callers to be able to trigger the event you would want to uncheck this option. If the event does not allow external callers then you won't be able to configure any parties to be notified for the event for callers from the "External" site.

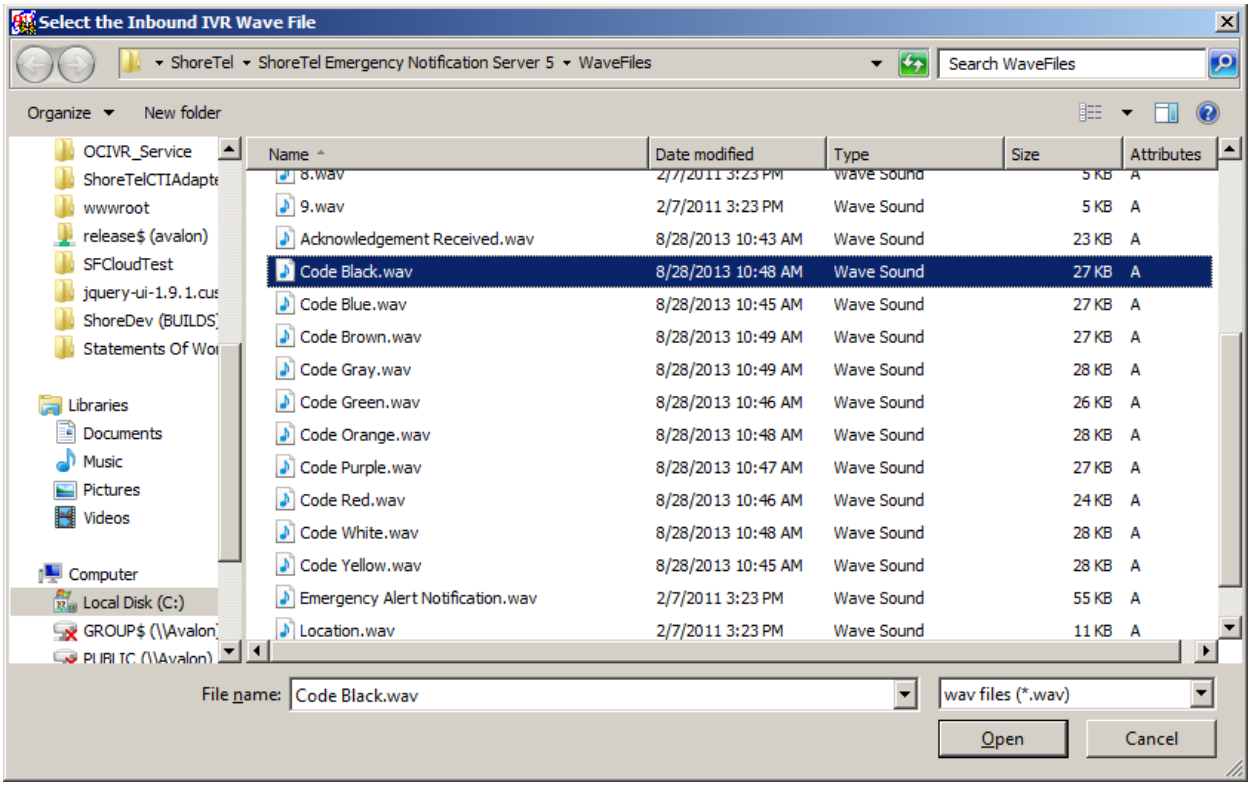
There are three choices which control what the caller hears:

- **No IVR**

  The caller hears no message. If the Optional Post IVR Transfer Destination is set (see below) then the caller would be immediately transferred on but if not the call is immediately disconnected (but the event is still triggered.)

- **Recorded Message**

  The caller hears a prerecorded message. For example, you could have a pre-recorded message that said "Your call has triggered a Code Blue event, goodbye." The system comes with several examples. Clicking the **browse button ("…")** next to the **IVR Wave File** field should drill down to a folder in the "WaveFiles" folder of the server's install folder where there are several examples named "Code " and a color name:



The format of these files should be:

CCITT u-Law 8.000 KHz, 8 Bit, Mono format

Note! This is not the same format as the client uses for the 911 alert files.

- **Text to Speech Message**

  The caller hears a message generated from the entered text. For example:

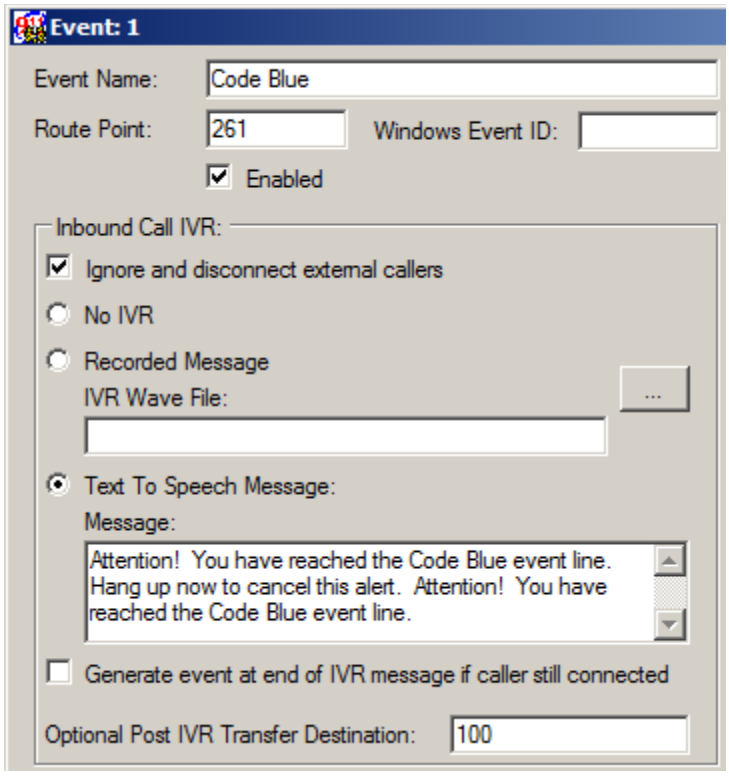
  “Attention. You have reached the Code Blue event line. A code blue event has been generated. Goodbye.”

The **Generate Event at end of IVR message if caller is still connected** setting is useful if you want to give calling parties the opportunity to hang up and not generate the event. For example, with this option enabled you could use a longer message to give the calling party time to hang up:

“Attention. You have reached the Code Blue event line. Hang up now to cancel this alert. Attention. You have reached the Code Blue event line.”

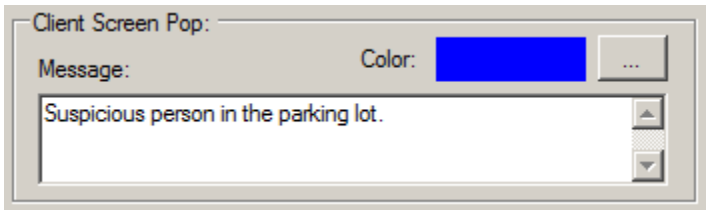
The **Optional Post IVR Transfer Destination** allows an extension or external number (entered with any required trunk access code) to be configured for the event. When the IVR message (if any) completes and the caller is still connected they will be transferred to the configured number.

This shows an event and it’s **Inbound Call IVR** configured to use a Text to Speech Message, generate the event at the end of the message if the caller is still connected and then transfer the caller to extension 100:



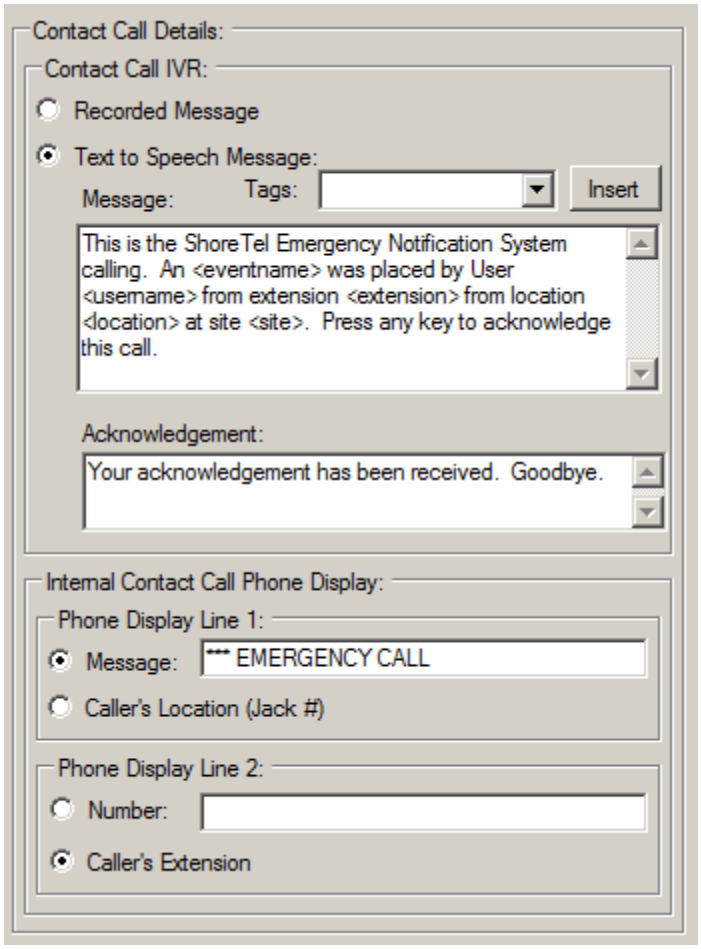
The remaining Event settings apply to both the Emergency Call event and other events.

In the lower left corner is the **Client Screen Pop** settings which control the client popup's border **Color** and a custom **Message** to be shown in the popup. For example, this shows the Color set to show a blue border, selected by clicking the **browse button ("…"),** and a Message of "Suspicious person in the parking lot.":



This is the popup that might result at a client user assigned to a User Profile enabled for this event. See the Configuring User Profiles section and also the separate client documentation:

The **Contact Call Details** at the top of the middle of the dialog control the various aspects of the outbound contact calls made by the server in response to an event.



At the top of the details are the controls for configuring the outbound Contact Call IVR details. There are two choices:

- **Recorded Message**

  This uses prerecorded prompts located in the install folder's WaveFiles folder to render basic information about the event. The only flexibility allowed is whether the message should include location details (based on the Contact Call setting in the Settings dialog described above.) See the Contact Calls section below that explains the contact calls.

- **Text to Speech Message**

  This plays a custom **Message** replacing any of the specific tags with the corresponding information from the call. As shown, the default for the Emergency Event and new events is to play this message:

  This is the ShoreTel Emergency Notification System calling. An <eventname> was placed by User <username> from extension <extension> from location <location> at site <site>. Press any key to acknowledge this call.

  Note the "tags" of the format <name>. For example <eventname>. When the tags are replaced, this could result in an actual message played to the contacts as follows:

  This is the ShoreTel Emergency Notification System calling. An Emergency Call was placed by User Smith from extension 212 from location Graduate Residence Hall, Third Floor, Room 2212 at site Campus. Press any key to acknowledge this call.

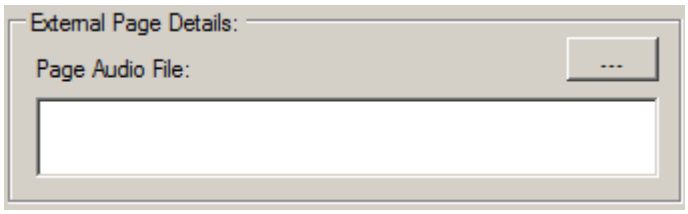
The available tags are inserted into the text by selecting them from the **Tags** dropdown and clicking the **Insert** button to place the tag into the text. You can manually enter the tags but you must exactly match the valid values shown in the list.

In addition to the Message, there is also an **Acknowledgement** message. Note that this is a static message and does not support the message tags.

At the bottom are the settings which control the Internal Contact Call Phone Display. These two panes control what information will show up in the top two lines of an internal contacts IP Phone display when receiving a contact call as a result of the event:

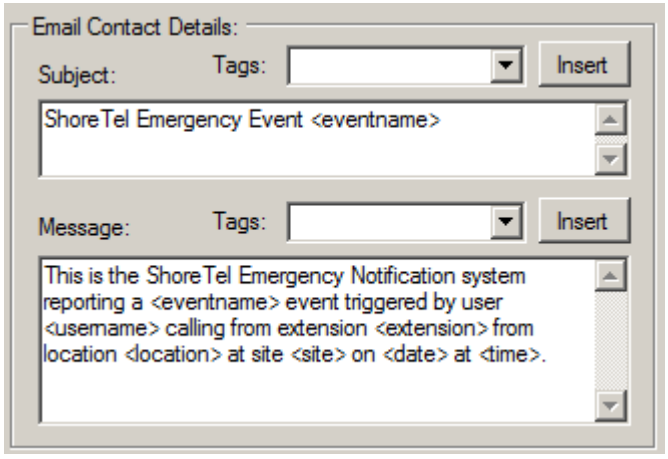
- **Phone Display Line 1:** Checking Message will display the associated text on the first line of IP phone display. Checking Caller's Location (Jack #) will display the caller's location on the IP phone display.
- **Phone Display Line 2:** Checking Number will display the associated number on the second line of the IP phone display. Checking Caller's Extension will display the caller's extension on the IP phone display.

The **External Page Details** at the bottom of the middle section of the dialog allows selection of a pre-recorded audio file that will be played to configured external contacts.



You can directly enter the full server path into the Page Audio File field or click the **browse button ("…")** to locate the file.

The **Email Contact Details** at the top right of the dialog controls the message subject and message body that is dynamically generated in response to an event and sent to any configured email contacts.



- **Subject:**

  The **Subject** of the email is generated using the text while replacing any of the specific tags with the corresponding information from the call. As shown, the default for the Emergency Event and new events is to email a message with this subject:

  ShoreTel Emergency Event <eventname>.

  Note the "tags" of the format <name>. For example <eventname>. When the tags are replaced, this could result in an actual email subject as follows:

  ShoreTel Emergency Event Emergency Call.

  The available tags are inserted into the text by selecting them from the **Tags** dropdown and clicking the **Insert** button to place the tag into the text. You can manually enter the tags but you must exactly match the valid values shown in the list.

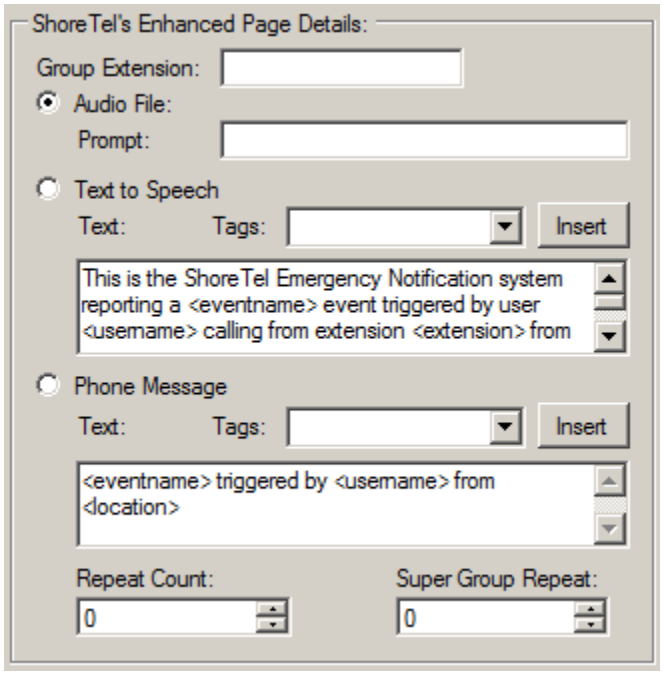
- **Message:**

  The **Message** of the email is generated using similar logic as the Subject. As shown, the default for the Emergency Event and new events is to email a message with this body:

  This is the ShoreTel Emergency Notification system reporting a <eventname> event triggered by user <username> calling from extension <extension> from location <location> at site <site> on <date> at <time>.

15 INTEGRATION WITH THE MITEL ENHANCED PAGING APPLICATION

Lastly the **Mitel Enhanced Page Details** at the lower right of the dialog controls the type of page generated in response to this event. Unlike other notification mechanisms, the Enhanced Page interface only allows a single page event to be generated and is not filterable by where the event is generated. If configured, then a page will be sent using the Enhanced Page server.



- **Group Extension**

  The Enhanced Page server group's extension is configured here. If left blank, then no EnhancedPage activity will occur for this event.

- **Audio File**
- **Text to Speech**
- **Phone Message**

  These three radio buttons select which of the three types of pages supported by the Enhanced Page system will be generated in response to this event. Each page type has some additional configuration.

- **Audio File | Prompt**

  This sets the path of a pre-recorded audio file that should be played to the Enhanced Page group. Unlike other wave file configured for use by the Emergency Notification server, this file must be located on the Enhanced Page server in the application's Pages folder. See the *Enhanced Page Applications* documentation for additional details.

- **Text to Speech | Text**

  The **Text** converted to an audio file by the Enhanced Page server is generated using the text while replacing any of the specific tags with the corresponding information from the call. The available tags are inserted into the text by selecting them from the **Tags** dropdown and clicking the Insert button to place the tag into the text. You can manually enter the tags, but you must exactly match the valid values shown in the list.

- **Phone Message | Text**

  The **Text** shown on the phone displays of the paging group members is generated using the text while replacing any of the specific tags with the corresponding information from the call. The available tags are inserted into the text by selecting them from the **Tags** dropdown and clicking the Insert button to place the tag into the text. You can manually enter the tags, but you must exactly match the valid values shown in the list.

- **Repeat Count**

The repeat count is only used for the Text to Speech and Phone Message page types. If set to a value greater than zero, then the audio message will repeat the specified number of times.

- **Super Group Repeat**

  The super group repeat is only used for the Text to Speech and Phone Message page types. If set to a value greater than zero and the paging group is a super group, then the page will repeat the specified number of times to each subgroup

Important considerations when using the Enhanced Paging application with the Emergency Notification application:

The **Enhanced Paging** application can deliver an alert page to hundreds of IP phones in an environment that does not otherwise have an overhead paging system in those locations. However, the application does have operational limits to keep in mind:

- **Multiple instances of the Enhanced Paging application are separate**

  The Enhanced Paging application can be installed (with the required licensing) on multiple servers. Note however that each instance is separate and do not share server resources or paging groups. The main motive for adding additional instances of Enhanced Paging is to support simultaneous pages to separate groups of phones (for example, building A users making announcements to phones in building A using one server while building B users are making different announcements to phones in building B using a second server).

- **Each server has finite number of media paths**

  An HQ or DVS server provides 254 media paths. These paths are used for multiple functions including voice mail, auto attendants, workgroup queues and various advanced applications. The Enhanced Paging application uses 1 media path for each phone within a paging group as it is receiving the page. So a paging group of 100 phones uses 100 media paths to deliver a page. If you configure a super group with multiple paging groups, the application still only uses 100 media paths since it delivers the page to one group within the super group at a time. If two separate pages to two groups/super groups are launched at the same time, the Enhanced Paging application will use 200 media paths, 100 for each page. Three separate concurrent pages would need 300 media paths, but since there are only 254 media paths available and some may already be in use by other system functions, this third page would be delayed until the other pages have completed and the server has sufficient resources available. The repeat count is only used for the **Text to Speech** and **Phone Message** page types. If set to a value greater than zero, then the audio message will repeat the specified number of times.

- **SIP and Analog phones must answer within the configured timeout to hear the page**

  If SIP and/or analog extensions are included in an Enhanced Paging group or if the user has used the Extension Assignment feature to assign their extension to their cell phone for example, the page will cause their phone to ring like a regular phone call and they will hear the page if they answer within the timeout defined for the page group.

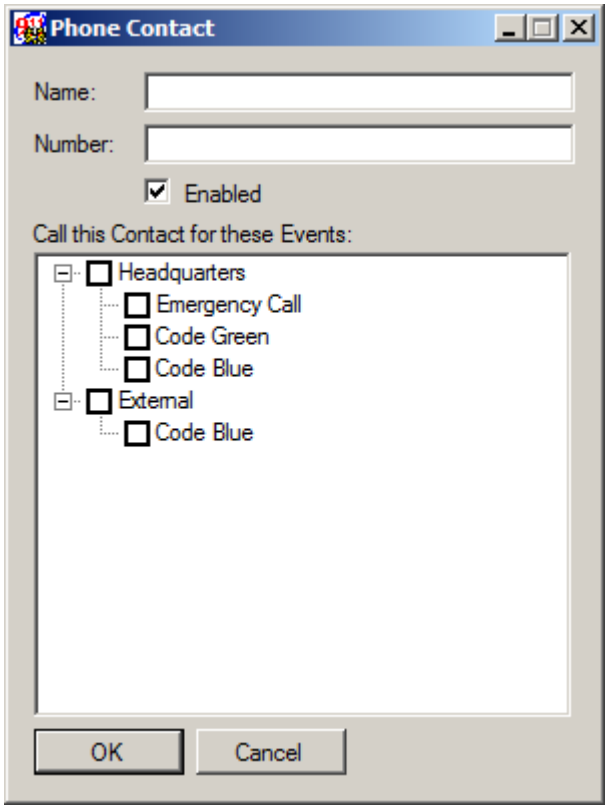
- **An alert in Emergency Notification can only be linked to a single Enhanced Paging group or super group, not one per site**

  In the current version of the Emergency Notification application, an alert can only trigger a page to a single group or super group. As such, it currently does not support the site-specific configuration of the other alert notification types (phone, workstation, email and overhead paging). To make an alert for each site with the appropriate Enhanced Paging group, you must define a separate alert extension (route point) for each site.

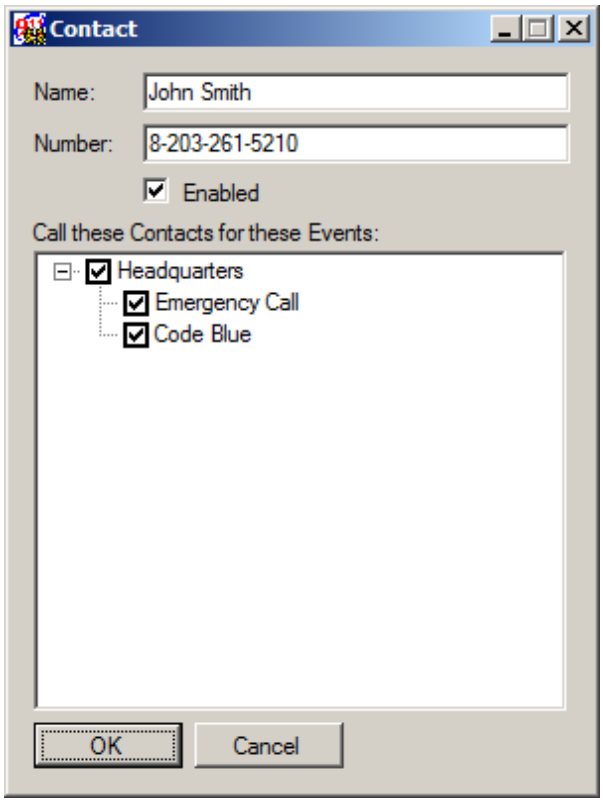
16 CONFIGURING PHONE CONTACTS

Phone contacts are parties called to be notified of an event. Contact calls have a feature that expects the called party to respond with a button press on their phone to acknowledge the calls. Based on the configuration of the event, contact calls either play a stock message using pre-recorded prompt or a more dynamic message using text to speech.

Before an event can alert a contact, the contact has to be configured using the Admin and enabled to be notified for that event at one or more of the available sites. To add a new contact, click the **Contact** Pane's **New…** button in the middle of the main **Admin** window. To edit an existing contact, select it and click Edit… or double click it. To delete a contact, select it and click the **Delete…** button. This shows the new Contact dialog:



Enter a **Name** for the contact and a **Phone Number**. If the contact is an external party, make sure to include any required trunk access code to be used when calling the contact. You can disable a contact by un-checking the **Enabled** checkbox. At the bottom of the dialog is a tree view showing each site and under each site all the configured event types. You can include all event types for a site by clicking on the Site name such as Headquarters in the above dialog. You can selectively enable events by clicking on the individual event names such as Emergency Call or Code Blue in the above dialog. This shows an external contact (note the 8-trunk access code) to be called for all event types:

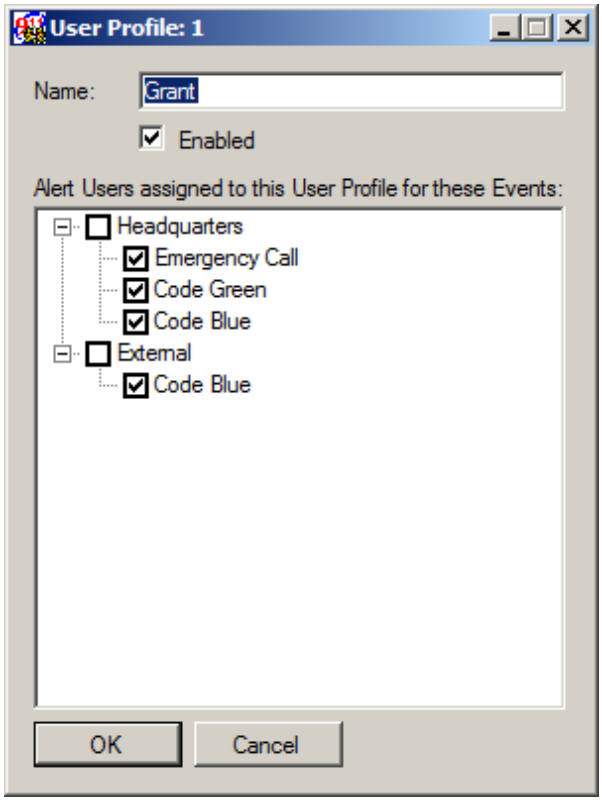

Contact
Name:
John Smith
Number:
8-203-261-5210
Enabled
Call these Contacts for these Events:
Headquarters
Emergency Call
Code Blue
OK
Cancel

17 CONFIGURING USER PROFILES

The server supports a client that can provide event alerts and other features to Windows desktop PC users. See the separate documentation that describes the installation and usage of the client. A key setting that is made as part of configuring the client is the User Profile the client should use. The supplied value must match the name of a User Profile configured on the server using the server's admin program. The user profile configuration defines the sites and events that client users assigned to that profile should alert for. User Profiles can be defined for each client user or can define a class of users where more than one user is assigned to that profile.

To add a new user profile, click the **User Profiles** Pane's **New…** button near the bottom of the main Admin window. To edit an existing user profile, select it and click **Edit…** or double click it. To delete a user profile, select it and click the **Delete…** button.

Enter a **Name** for the user profile. You can disable a user profile by un-checking the **Enabled** checkbox. At the bottom of the dialog is a tree view showing each site and under each site all the configured event types. You can include all event types for a site by clicking on the Site name such as Headquarters in the above dialog. You can selectively enable events by clicking on the individual event names such as Emergency Call or Code Blue. This shows a user to be called for all event types:

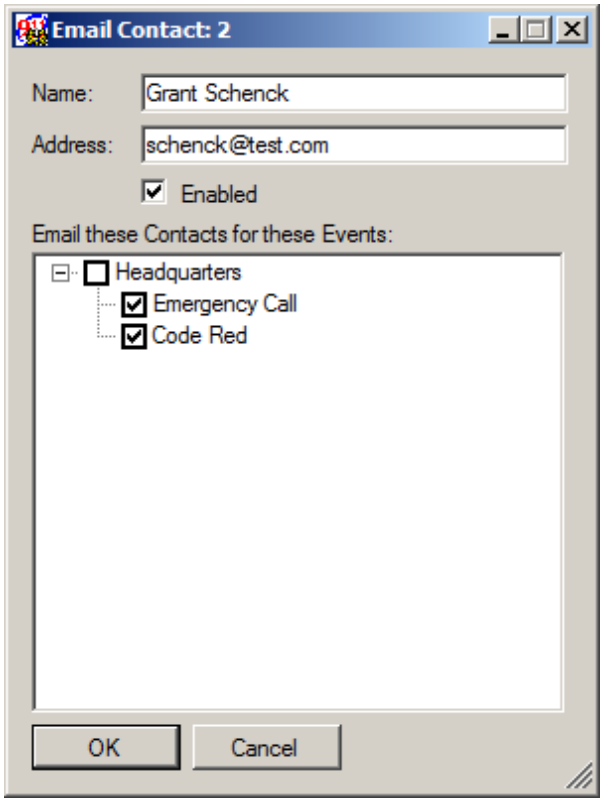


18 CONFIGURING EMAIL CONTACTS

The server supports email notification to configured email contacts. The email contact configuration defines the name and email address of a contact along with the sites and events that the contact should be sent an email for.

To add a new email contact, click the **Email Contact** Pane's **New…** button in the middle right side of the main Admin window. To edit an existing email contact, select it and click **Edit…** or double click it. To delete an email contact, select it and click the **Delete…** button.

Enter an email user's **Name** and **email Address** for the email contact. You can disable a contact by un-checking the **Enabled** checkbox. At the bottom of the dialog is a tree view showing each site and under each site all the configured event types. You can include all event types for a site by clicking on the Site name such as Headquarters in the above dialog. You can selectively enable events by clicking on the individual event names such as Emergency Call or Code Blue. This shows a user to be called for all event types:

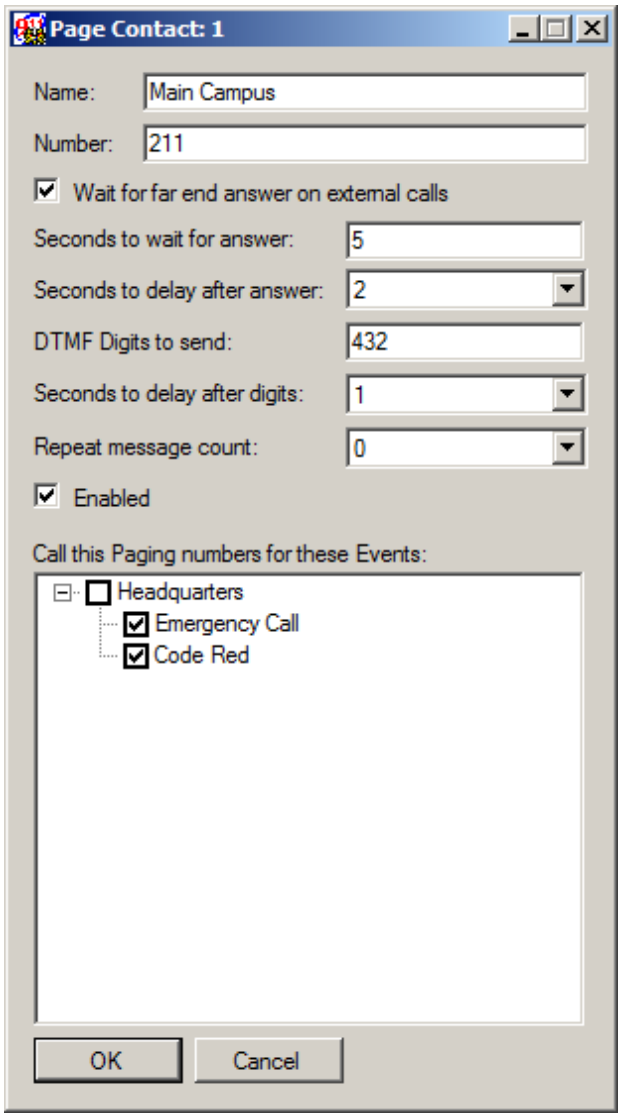


19 CONFIGURING EXTERNAL PAGE CONTACTS

The server supports automated notification voice calls made to external paging systems. These are similar to the Phone Contacts feature except only a single pre-recorded message is supported in the Event settings (no Text to Speech message) and there is no request for an acknowledgement of the call since obviously, an external paging system can't acknowledge a voice message. Through the contact settings, the External Page Contact feature supports a fair degree of flexibility with regards to synchronizing and interfacing with External Page systems. While there is no guarantee that a given page system is supported, most basic paging systems should be. The external page contact configuration defines the name and phone number of a paging system along with details to help guide the Emergency Notification System when interfacing to the paging system as well as the sites and events that the contact should be sent a page for.

To add a new external page contact, click the **External Page Contacts** Pane's **New…** button in the lower right side of the main Admin window. To edit an existing external page contact, select it and click **Edit…** or double click it. To delete an external page contact, select it and click the **Delete…** button.

Enter the **Name** and **Number** of the external paging system. **Wait for far end answered on external calls** is only used when an external phone number is configured for the Page Contact. If enabled the system will wait for the far end to answer before continuing. If unchecked then the system will attempt to interface as soon as the call connects to a trunk. **Seconds to wait for answer** is similar to the contact call system level setting of the same name. That is, it controls how long the system waits for the called party to answer before giving up due to no answer. If the Seconds to wait after answer is set to a non-zero value then the server will wait that number of seconds following the connection. This is to give the external paging system time to possibly play an outgoing message or wait for the paging system to be ready to accept a paging zone. **DTMF Digits to send** allows the sending of digits to the external paging system, typically to provide a paging zone or security code. **Seconds to delay after digits** allows a secondary delay after any digits are sent to allow the paging system to be ready to start capturing the audio page. This might be to allow time for a prompt or beep tone. If set to a value greater than zero, repeat message count will result in the message being repeated one or more additional times. You can disable notification by un-checking the **Enabled** checkbox. At the bottom of the dialog is a tree view showing each site and under each site all the configured event types. You can include all event types for a site by clicking on the Site name such as Headquarters in the above dialog. You can selectively enable events by clicking on the individual event names such as Emergency Call or Code Blue. This shows a user to be called for all event types:


Page Contact: 1
Name:
Main Campus
Number:
211
Wait for far end answer on external calls
Seconds to wait for answer:
5
Seconds to delay after answer:
2
DTMF Digits to send:
432
Seconds to delay after digits:
1
Repeat message count:
0
Enabled
Call this Paging numbers for these Events:
Headquarters
Emergency Call
Code Red
OK
Cancel

20 CONTACT CALLS

When an event is triggered in the system the server will go through the current list of enabled contacts as configured in the Admin application. Depending on the type of call (Emergency or Internal) and the contact settings (enabled and matching site monitored) it will potentially place a call to the contact. The call is placed in such a way that if the contact is an internal party with a display phone then the caller ID information associated with the call will reflect the Internal Contact Call Phone Display settings for the event. The server will wait the configured amount of time as configured in the Settings from the point where the call is made for the call to connect. If the call doesn't connect in time, then it is automatically disconnected. If the call does connect then the server starts the outbound IVR notification. This can be either a pre-recorded message based on a series of audio files or it can be generated using text to speech to better include details such as the username and location.

If the outbound message uses the **Recorded Message** option, then it will announce the call and the extension of the party who placed it. If **Play Location** setting is enabled is Settings and there are any digits contained or dash characters in the caller's location information (Director's Jack # field) then the digits and dashes are played as the location of the call to the contact. The called contact is given the opportunity to respond by pressing "1" on their phone to acknowledge the call.

This is the sequence of steps for the server's contact call interactive voice response interaction:

1. Call a contact. If any failures, then log and complete.
2. Wait for contact to answer. If contact fails to answer by Seconds to wait for answer setting then log, drop the call and complete.
3. For a Recorded Message:
    a) Play notification prompt followed by the caller's extension digits.
    b) If **Play Location** is enabled and location information was retrieved for the caller and the location contains digits or dashes, then play a prompt followed by caller's location digits.
    c) Play the request acknowledgement prompt and wait for up to 3 seconds after playing for caller to respond with a '1' digit.
    d) If no '1' digit is received, then check to see if we have played the announcement **Play Message Count** times. If not, then loop back up and play the message again.
    e) If we have then log, drop the call and complete.
    f) If a '1' digit is received then log, play the **Acknowledgement Received** prompt, drop the call and complete.
4. For a Text to Speech Message:
    a) Insert the value of any valid tags in the Message text and then play it to the called contact using text to speech. Wait for up to 3 seconds after playing for the caller to respond with a button on their phone.
    b) If no button press is received, then check to see if we have played the announcement **Repeat Message Count** times. If not, then loop back up and play the message again.
    c) If we have then log, drop the call and complete.
    d) If a '1' digit is received then log, play the **Acknowledgement** text using text to speech, drop the call and complete.

Note! An important point to about the contact call feature is that the system will only attempt to call a given contact at the time that the call is first detected. This means that if the call fails then there is no notification to that user. The server itself will skip calling a contact to which it already has a call active due to a previous call. This means that if two emergency or code events occur in close proximity than the contact call message will only play for the first call. The server will also skip calling a contact if that contact is the party who placed the alert call.

21 PHONE DISPLAY FOR INTERNAL CONTACTS

This shows an example of the default display of a 530/560 phone for a contact call when the contact is an internal extension. Note that this can be changed via the event settings.

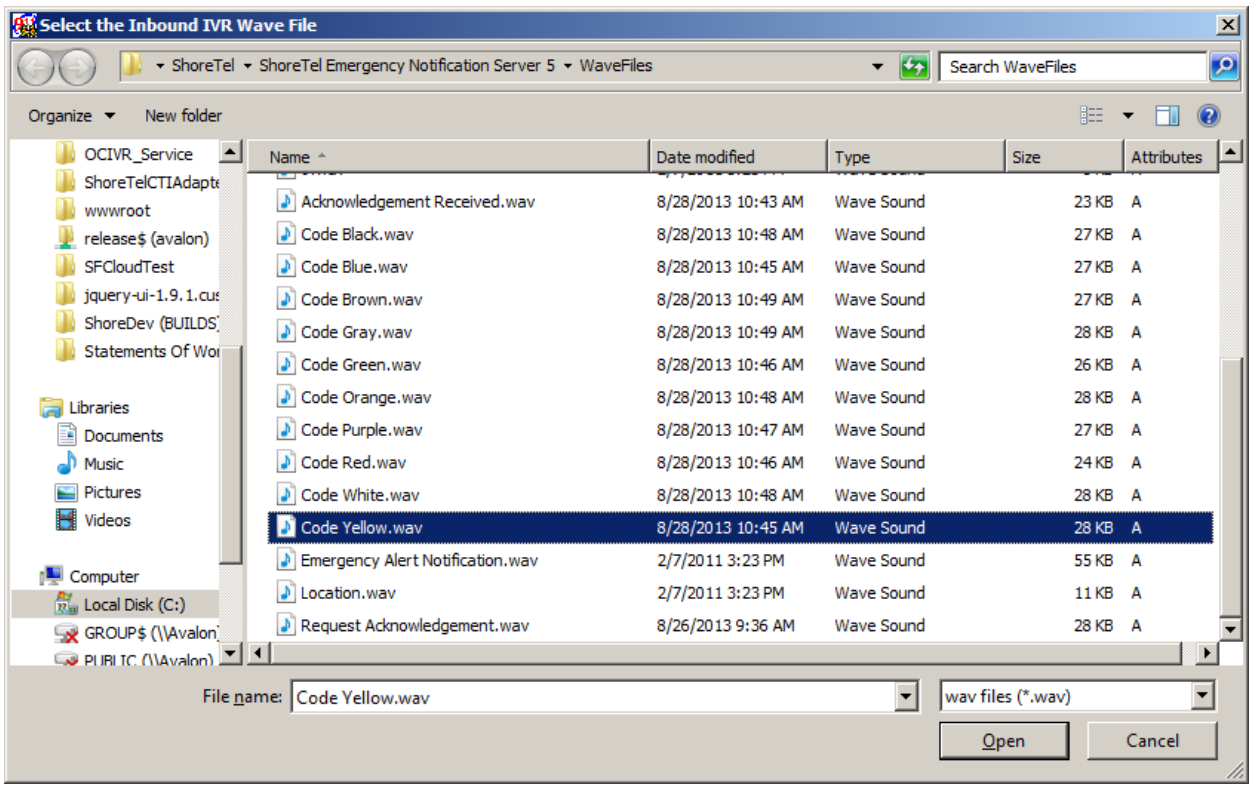
This example shows the display when extension 109 called 911:

```
+--------------------------+
| *** EMERGENCY CALL |
| 109 |
|  |
```

22 REPLACING CONTACT CALL PROMPTS

The server comes with default wave file prompts to play to contacts. These are stored in the application's folder in the WaveFiles subfolder. Typically, this will be:

C:\Program Files (x86)\ShoreTel\ShoreTel Emergency Notification Server 5\WaveFiles



The following prompts are used:

- **Emergency Alert Notification.wav:** "This is the Mitel phone system emergency call notification system calling. An Emergency call was placed from..." This is the first prompt heard by a contact when being notified of an emergency (911) call.
- **Location.wav:** "...from location..." If the **Play Location** option is enabled and location in available, then this prompt is played following the extension and proceeding the digits from the location being played.
- **Request Acknowledgement.wav:** "Please press 1 on your phone to acknowledge this call." This prompt follows the extension and any location and asks the caller to respond.
- **Acknowledgement Received.wav:** "Your acknowledgement has been received. This concludes this call." Prompt which plays at the end if the contact presses 1 to acknowledge the contact call.
- **-.wav, 0.wav, 1.wav, ...9.wav:** "Dash, Zero, One,... Nine." Dash and digit prompts use to play the calling parties extension digits and location digits.
- **Code Black.wav, Code Blue.wav… Code Yellow.wav:** "These are sample inbound IVR files that could be used to provide pre-recorded acknowledgement to caller that an event has been generated.

If a user wishes to replace any of the sound files, they will need to record replacements and place them in the WaveFiles folder with the same names as the current files. They should make backups before replacing the files and run a test after. They should also avoid replacing them if an event could happen while they are updating the files.

The format of these files should be:

CCITT u-Law 8.000 KHz, 8 Bit, Mono format

Note! This is not the same format as the client uses for the 911 alert files.

So, for example, if you use the Windows Sound Recorder applet to record your own replacement files, make sure that when you save the wave files you specify the above format.

23 THE SERVER LOG

Key to the server is the integrated logging feature. As installed, the system logs all activity to the STPSEN.log file in the Logs subfolder in the server's install folder. This would typically be located here:

C:\Program Files (x86)\ShoreTel\ShoreTel Emergency Notification Server 5\Logs

Each day that the server runs, a new file is written and previous files are renamed to concatinate the year, month and day as part of the file name, for example:

STPSEN.log20130829

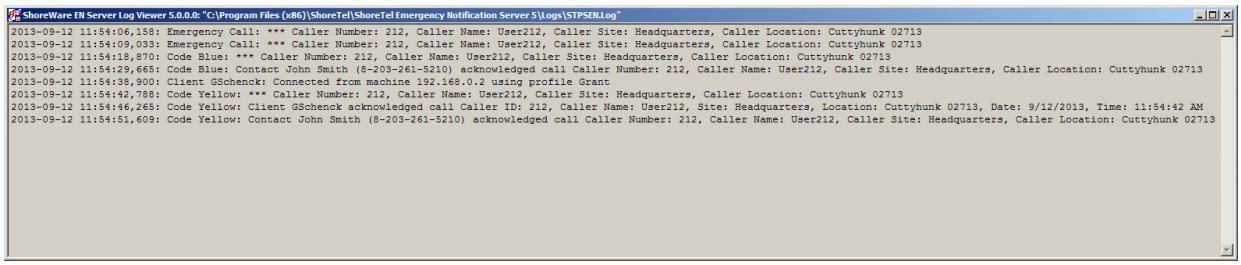
The log file can be viewed by opening the application log file in an appropriate editor or by using the Application Log Viewer utility installed on the server PC

24 THE APPLICATION LOG VIEWER

A simple log viewer utility is supplied to facilitate viewing the current log file. It provides two conveniences:

- Saves the user from finding or typing in the current log file location.
- Watches the file for changes while it is running and reloads it. This provides a semi-real-time view of the log.

The log viewer is installed as part of the server install. It can be run from the desktop shortcut or “Start | All Programs | Mitel | Mitel Emergency Notification Server Log Viewer” shortcut.



25 THE LOG CONTENTS

The server log shows various activities within the Server. Logging is generated in time order and will show intermingled activities. For example, logging of the emergency calls as well as the client contact and contact calls will be interlaced.

What follows are examples of the different types of logging generated by the server:

- *2013-09-12 11:54:06,158: Emergency Call: *** Caller Number: 212, Caller Name: User212, Caller Site: Headquarters, Caller Location: Cuttyhunk 02713*

  An event being generated for an “Emergency Call”. It shows the calling parties details and logs the date and time of the event.

- *2013-09-12 11:54:18,870: Code Blue: *** Caller Number: 212, Caller Name: User212, Caller Site: Headquarters, Caller Location: Cuttyhunk 02713*

  This shows an event being generated for “Code Blue”. It shows the calling parties details and logs the date and time of the event.

- *2013-09-12 11:54:29,665: Code Blue: Contact John Smith (8-203-261-5210) acknowledged call Caller Number: 212, Caller Name: User212, Caller Site: Headquarters, Caller Location: Cuttyhunk 02713*

  This shows the contact John Smith acknowledging the Code Blue event.

- *2013-09-12 11:54:38,900: Client GSchenck: Connected from machine 192.168.0.2 using profile Grant*

  This shows a client named GSchenck logging in and connecting to the server.

- *2013-09-12 11:54:42,788: Code Yellow: *** Caller Number: 212, Caller Name: User212, Caller Site: Headquarters, Caller Location: Cuttyhunk 02713*

  An event being generated for “Code Yellow”. It shows the calling parties details and logs the date and time of the event.

- *2013-09-12 11:54:46,265: Code Yellow: Client GSchenck acknowledged call Caller Number: 212, Caller Name: User212, Site: Headquarters, Location: Cuttyhunk 02713, Date: 9/12/2013, Time: 11:54:42 AM*

  This shows the client GSchenck acknowledging the Code Yellow event.

- *2013-09-12 11:54:51,609: Code Yellow: Contact John Smith (8-203-261-5210) acknowledged call Caller Number: 212, Caller Name: User212, Caller Site: Headquarters, Caller Location: Cuttyhunk 02713*

  This shows the contact John Smith acknowledging the Code Yellow event.

- *2013-09-12 11:57:34,102: Client GSchenck: "I called the police to check on the person."*

  This shows a message sent by client GSchenck to the other client users.

26 TESTING

Once the system is installed and configured, you will want to test the system to ensure that it is fully functional. In addition, you should plan to periodically run tests to confirm that all aspects of the system are operational. The primary mechanism for testing the system's response is to place an actual code blue and actual emergency call.

Mitel recommends the following initial and ongoing testing:

- Following initial installation and configuration, you may want to start placing test calls to event route points to confirm that all configured contacts are notified, and any connected clients configured for the caller's site and the event type show the popup.
- Assuming you'll also be configuring Emergency Calls you'll want to notify the emergency operators in your community and schedule a true emergency test call. Again, confirm that all configured contacts are notified, and any configured connected clients show the popup.
- Anytime any significant configuration changes are made, it is recommended that you run an appropriate test call and confirm correct operation.

If the system is installed and running, we recommend periodic testing to ensure normal operation, perhaps once a month.

27 APPENDIX A: CONFIGURING THE TEXT TO SPEECH SUPPORT

This application uses the Microsoft Server Text-to-Speech (TTS) engine to convert textual information into audio streams. To use TTS, customers will need to install the Microsoft Speech Platform Runtime (x86 version) and the voice file along with a voice for playback.

To configure the Test-to-Speech support, follow these steps:

1. Install the Microsoft Speech Platform x86 Runtime:
    a. The Microsoft Text-to-Speech components are now distributed in the zip package with the Advanced Application code. To install, locate the MSTextToSpeechRuntime.zip and unzip the two files to the hard drive.
    b. Run the **SpeechPlatformRuntime.msi** file and follow the prompts to complete the installation.
2. Install the voice file and select the voice:
    a. On the same computer, run the **MSSpeech_TTS_en-US_Helen.msi** file to install the voice files.
    b. There might be other voice files available from Microsoft as part of their Software Development Kits, but these are not distributed with the Mitel application. To select the voice file to use, run the admin program and after selecting the server, navigate to the **Settings** dialog, and in the **Text to Speech** pane at the top right corner, select the **Voice Name** drop-down list and then select a voice as shown in the following screen capture: