



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring the Genesis GenAlert Solution with Avaya IP Office - Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required to integrate the Genesis GenAlert Solution with Avaya IP Office. The Genesis GenAlert Solution is a web or client based solution that provides on-site notification when an emergency call has been placed.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the configuration steps required to integrate the Genesis GenAlert Solution (hereafter, also referred to as “GenAlert”) with Avaya IP Office. GenAlert offers a web or client based solution for on-site notification when an emergency call has been placed. GenAlert provides screen pops, sounding alarms, emails and SMS text messaging options to notify about the emergency.

The GenAlert server connects to the IP Office Simple Network Management Protocol (SNMP) port and collects SNMP traps that are generated when an emergency call is placed and provides the notification using screen pops, emails, SMS text messages or sounding an alarm.

## 2. General Test Approach and Test Results

The compliance test focused on the ability for the GenAlert application to accurately report all the information gathered from SNMP traps generated by IP Office.

When an emergency call is placed, an On Site Notification (OSN) message is generated by IP Office and provided as an SNMP trap. GenAlert collects this SNMP trap, compiles all information present in the trap and presents it in user friendly form of screen pop, email, SMS text message or sounding an alarm.

The solution contains of two modules under GenStart. One module named GCOM collects the raw SNMP data and the other module named GENALERT processes this data and outputs it in the required format for screen pops, emails or SMS text messages.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

### 2.1. Interoperability Compliance Testing

The general test approach was to verify the integration of GenAlert with Avaya IP Office. Various emergency calls were placed from Avaya IP Office telephones to verify SNMP traps were properly logged and displayed (via pop-up alerts) by GenAlert. GenAlert’s email and text message notification of the alert was also tested.

Additionally, basic serviceability testing examined the handling of and recovery from error conditions (such as network disconnects and power failures).

## 2.2. Test Results

The Genesis GenAlert Solution successfully passed compliance testing with the following observation:

- Emergency alert notification using email and text can be delayed since these are dependent on the email servers and local Telco providers. During compliance testing, alerts notified using email was almost instantaneous however there were delays in receiving alerts via the text messages.
- In a setup where there is only one PSTN line from the Primary Server and if an emergency call is made from a phone registered to the Expansion system, GenAlert captures the SNMP traps generated by both Primary and Expansion however only the SNMP trap from the Expansion has all the required details. Similar behavior will be displayed if there is only one PSTN line from the Expansion system.

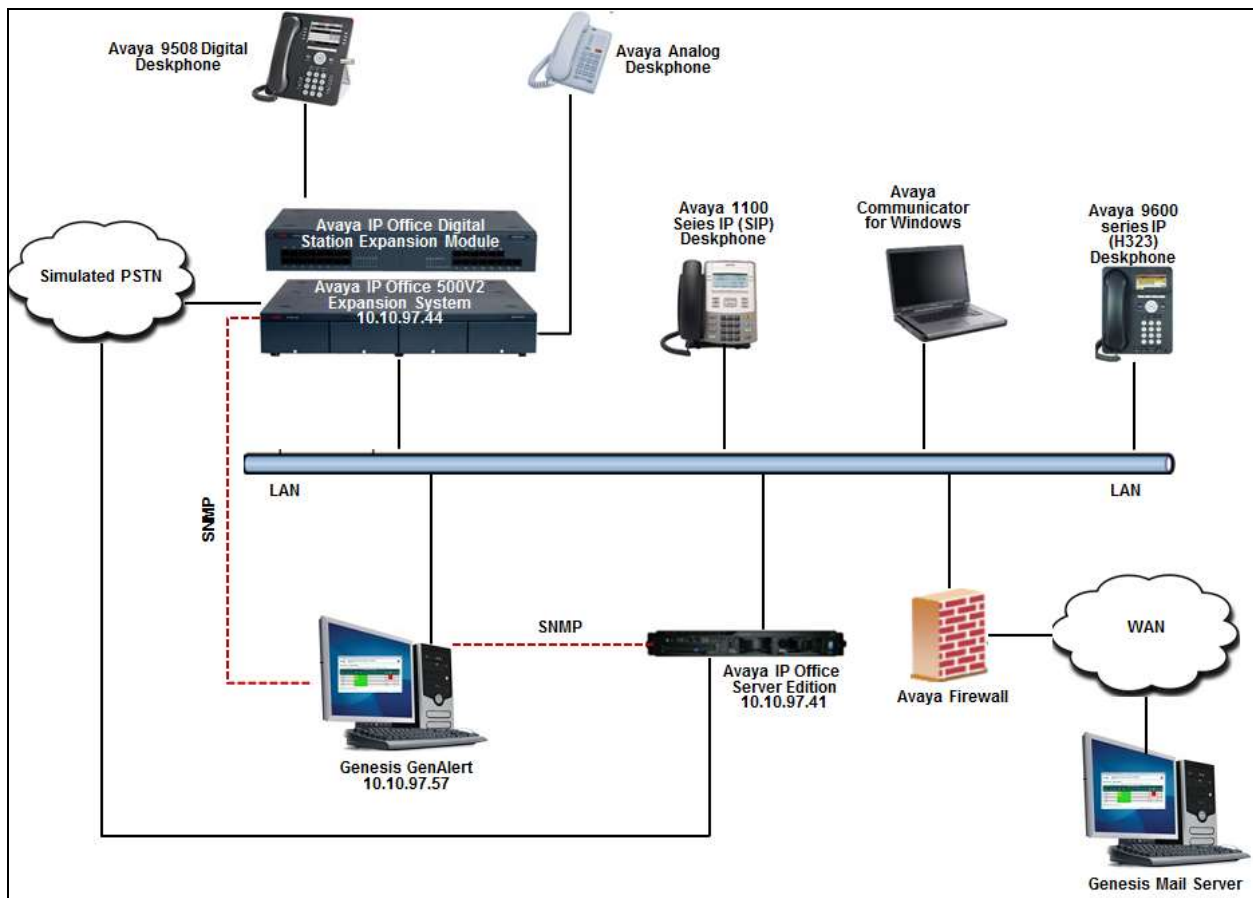
## 2.3. Support

Information, Documentation and Technical support for Genesis products can be obtained at:

- Phone: 1 (888) 993-2288 or 1 (604) 530-9348
- Web: <http://www.buygenesis.com>
- Email: [support@buygenesis.com](mailto:support@buygenesis.com)

### 3. Reference Configuration

**Figure 1** below illustrates the configuration used to compliance test the Genesis GenAlert solution with Avaya IP Office Server Edition with a 500V2 box as expansion. The Genesis GenAlert Solution and the screen pop client were installed on a Windows 7 Professional SP1 OS. For email verification, a Genesis mail server was used and for SMS texting a local Telco provider was used.



**Figure 1: Genesis GenAlert Solution with Avaya IP Office**

## 4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

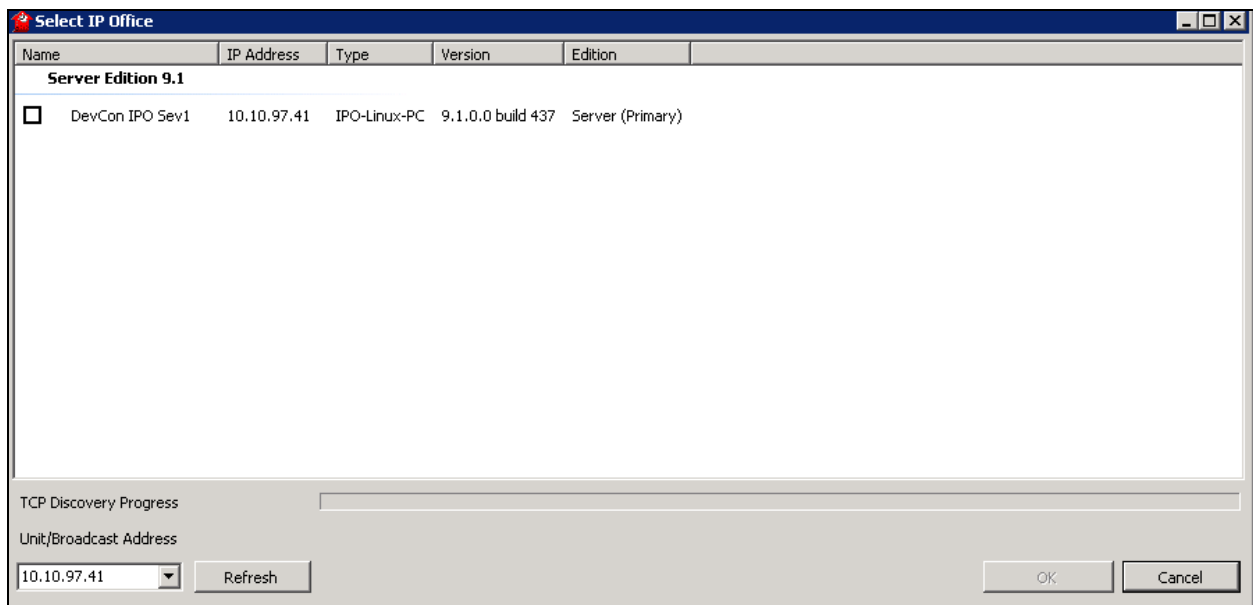
Equipment/Software	Release/Version
Avaya IP Office Server Edition server (Linux)	9.1.0.437
Avaya IP Office 500 V2 Expansion Module	9.1.0.437
Avaya Telephones: <ul style="list-style-type: none"><li>• 1140 IP (SIP) Deskphone</li><li>• 9621G IP (H323) Deskphone</li><li>• Communicator for Windows</li><li>• 9508 Digital Deskphone</li><li>• Analog Deskphone</li></ul>	<ul style="list-style-type: none"><li>• 4.04.18</li><li>• 6.4014</li><li>• 2.0.3.30</li><li>• 0.55</li><li>• N/A</li></ul>
Genesis: GenAlert installed on MS Windows 7 Professional SP1 OS	3.3.3
GenStart Module	4.15

**Note:** Testing was performed with IP Office Server Edition R9.1 and an Expansion IP Office 500 v2 R9.1. Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with IP Office Server Edition in all configurations.

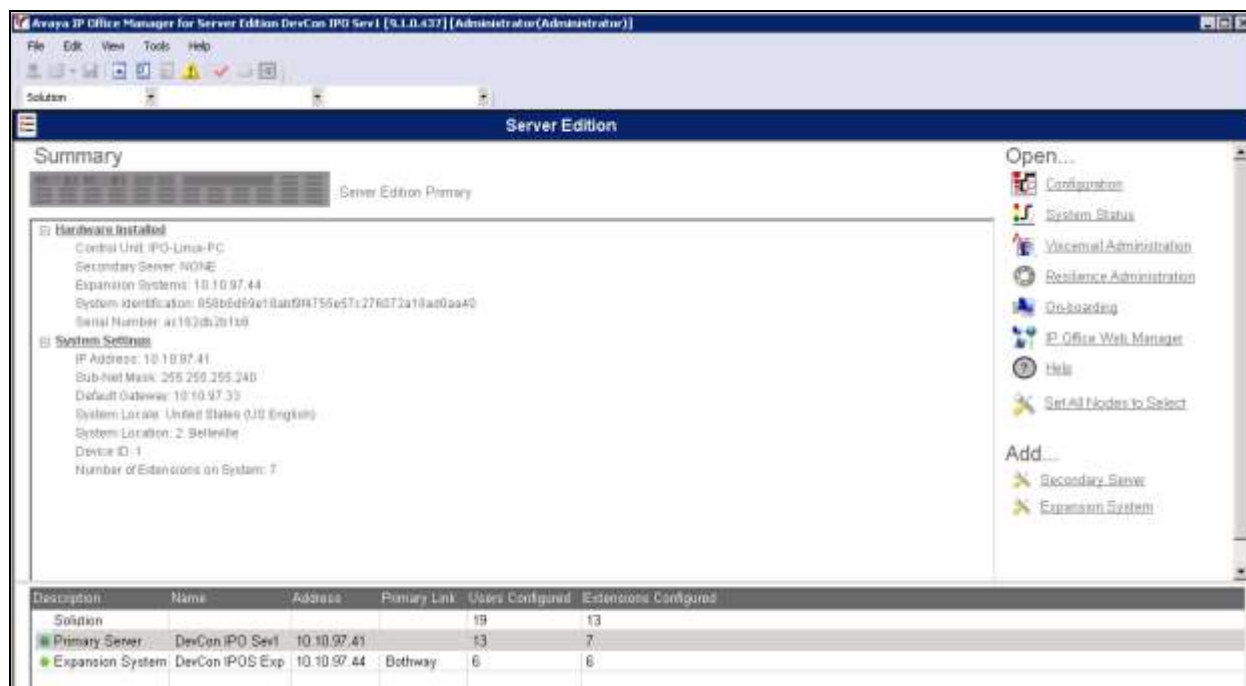
## 5. Configure Avaya IP Office

This section describes the Avaya IP Office Server Edition configuration necessary to support integration with the Genesis GenAlert solution. It is assumed that the initial installation and provisioning of the Server Edition Primary Server and Expansion System has been previously completed and therefore is not covered in these Application Notes. For information on these installation tasks, refer to reference [1] in the **Additional References** section.

The solution is configured through the Avaya IP Office Server Edition Manager PC application. From the PC running the IP Office Manager application, select **Start → All Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, and select the proper Avaya IP Office Server Edition system. Log in using appropriate credentials.



The Solution View screen will appear, similar to the one shown below. This screen includes the system inventory of the servers and links for administration and configuration tasks.



In the screens presented in these sub-sections, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center and the Details pane on the right side. These panes will be referenced throughout the rest of this section.

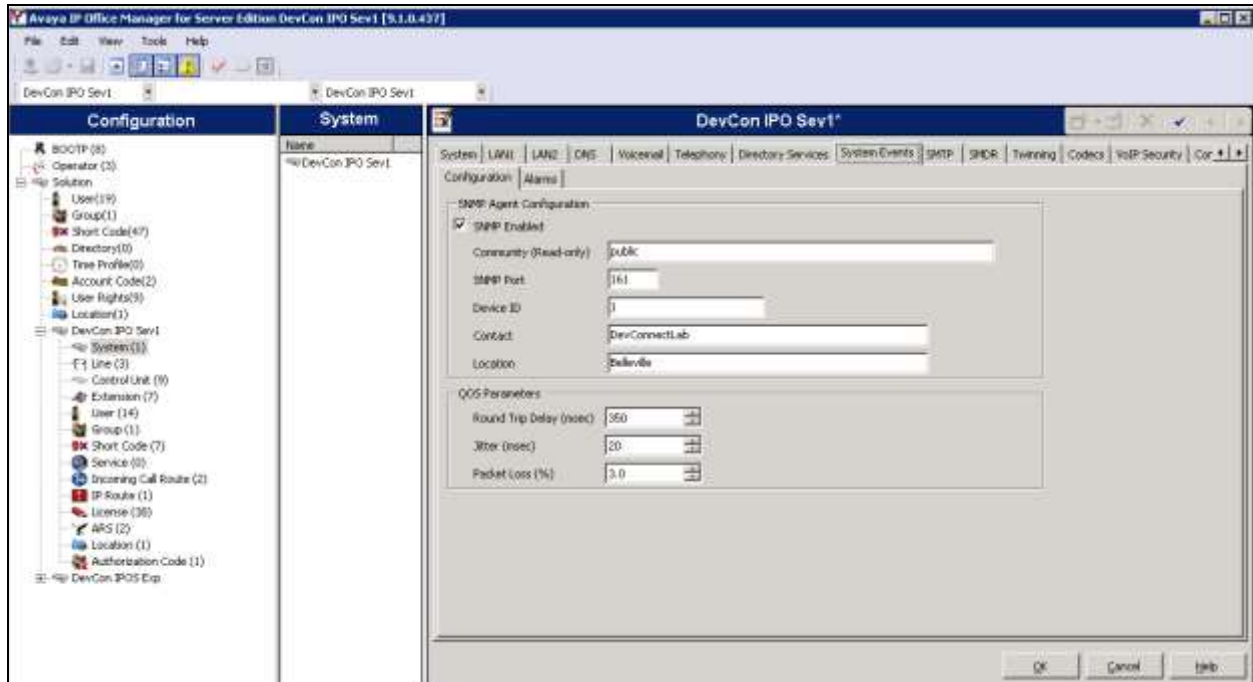
Note that the Navigation pane includes solution settings, under the Solution menu, which apply to all the systems in the Server Edition solution, and individual system settings, each grouped under the Primary Server and the Expansion System menus.

For each form where modifications have been made, the user must click the **OK** button to submit the changes. After all changes have been made to the system, click **File → Save Configuration**.

**Note: The sub-sections below show the steps required to configure SNMP traps and emergency calls for Primary server only. The same steps MUST be performed for each Secondary Server and Expansion System within a solution using the appropriate values for each server/expansion system.**

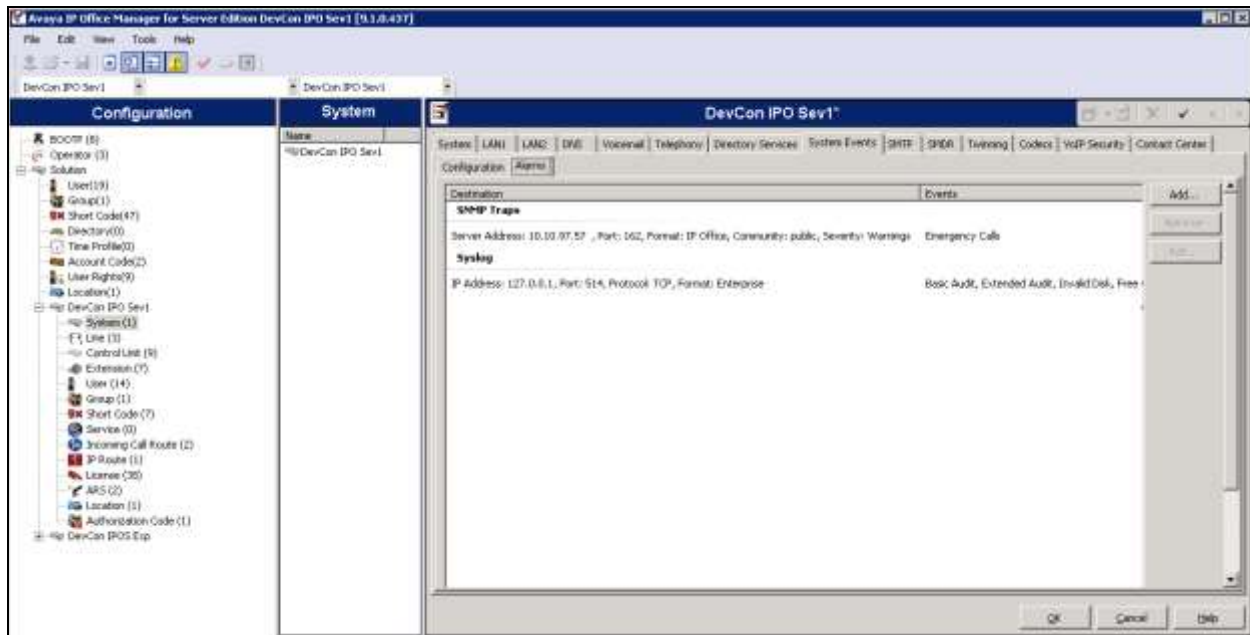
## 5.1. Configure SNMP Traps for Emergency Calls

To configure SNMP traps for Emergency calls on the Primary Server, complete the following steps. Navigate to the Primary system, in this case, **DevCon IPO Sev1** → **System (1)** in the Navigation pane and then select the **System Events** tab in the Details pane. Under the **Configuration** sub-tab, check the box for **SNMP Enabled**. Fill in the remaining fields with values appropriate for the site. The screen below shows the values used during compliance testing.





Click the **Alarms** sub-tab, and click the **Add...** button on the right side of the Details pane.



In the **New Alarm** section, select the **Trap** radio button. For **Server Address**, enter the IP Address of the Genesis GenAlert Solution server. This is the IP address of the SNMP server to which trap information is sent. Enter the SNMP transmit **Port** (default = 162). The SNMP **Community** value entered for the transmitted traps must be matched by the receiving SNMP server. Select **IP Office** for **Format**. The **Minimum Security Level** can be left at the default level of **Warnings**.

New Alarm

Destination:

☒ Trap ☐ Syslog ☐ Email

Server Address: 10.10.97.57

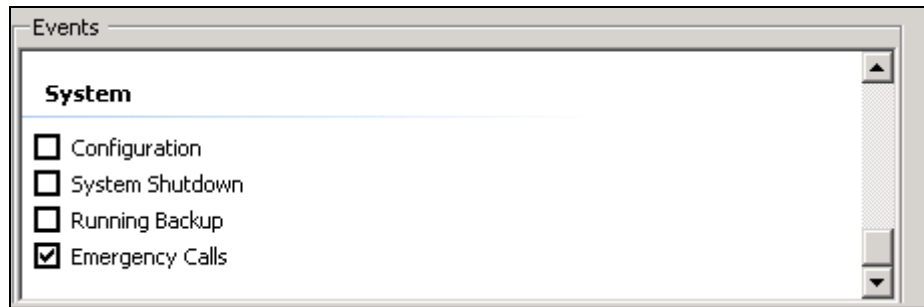
Port: 162

Community: public

Format: IP Office

Minimum Severity Level: Warnings

In the **Events** section, scroll to the bottom and check **Emergency Calls**.



The alarms configured above trigger when IP Office determines that an emergency call has been dialed and the call has been routed, regardless of whether the call is successful. For example, if an emergency call is dialed, but all lines/trunks are down, an SNMP trap will still be generated when IP Office attempts to route the emergency call. The trap will contain all the same information whether or not the emergency call is actually successful.

## 5.2. Configure Emergency Calls

IP Office Manager expects the configuration of each system to contain at least one short code that is set to use the Dial Emergency feature. If no such short code is present in the configuration, then Manager will display an error warning. The importance of the Dial Emergency feature is that it overrides all external call barring that may have been applied to the user whose dialing has been matched to the short code. You must still ensure that no other short code or extension match occurs that would prevent the dialing of an emergency number being matched to the short code.

The short code (or codes) can be added as a system short code or as an ARS record short code. If the Dial Emergency short code is added at the solution level, that short code is automatically replicated into the configuration of all servers in the network and must be suitable for dialing by users on all systems. Separate Dial Emergency short codes can be added to the configuration of an individual system. Those short codes will only be useable by users currently hosted on the system including users who have hot-desked onto an extension supported by the system. For compliance testing, short codes were configured for the individual systems.

It is the installer's/administrator's responsibility to ensure that a Dial Emergency short code or codes are useable by all users. It is also their responsibility to ensure that either:

- The trunks that the resulting call may be routed on are matched to the physical location where emergency service will be dispatched.
- or
- The outgoing calling line ID number sent with the call matches the physical location from which the user is dialing.

When configuring locations, consult local guidelines. For example, regions may require identification based on building or building floor. Floors may be subdivided based on number of staff or the location of hazardous materials. Typically, fire alarm planning will have defined zones based on these or similar requirements.

Routing of emergency calls is based on a call resolving to a Dial Emergency short code. Based on the location value for the extension making the call, routing is performed as configured in the Emergency ARS.

To configure and test emergency call routing within Avaya IP Office perform the following steps:

1. Create a Dial Emergency short code.

Note that the Line Group ID value in the Dial Emergency short code is the fallback route. If the system cannot find a location or an Emergency ARS, it will try to use the Line Group ID to route the call.

2. Create an ARS containing a Dial Emergency short code.
3. Create a Location and set the Emergency ARS to the ARS created in step 2.
4. Open the Extn tab for an extension that will use the location defined in step 3 and set the Location value to the location defined in step 3.

Note that once you define a location, you must set a system Location value on the **System → System** page.

For non-IP based extensions, the system location value is used as the default. For IP based extensions, the location value is set to Automatic. An attempt is made to match the extension's IP address to the subnet configured in the location. If the match cannot be made, the location value defaults to the system location value.

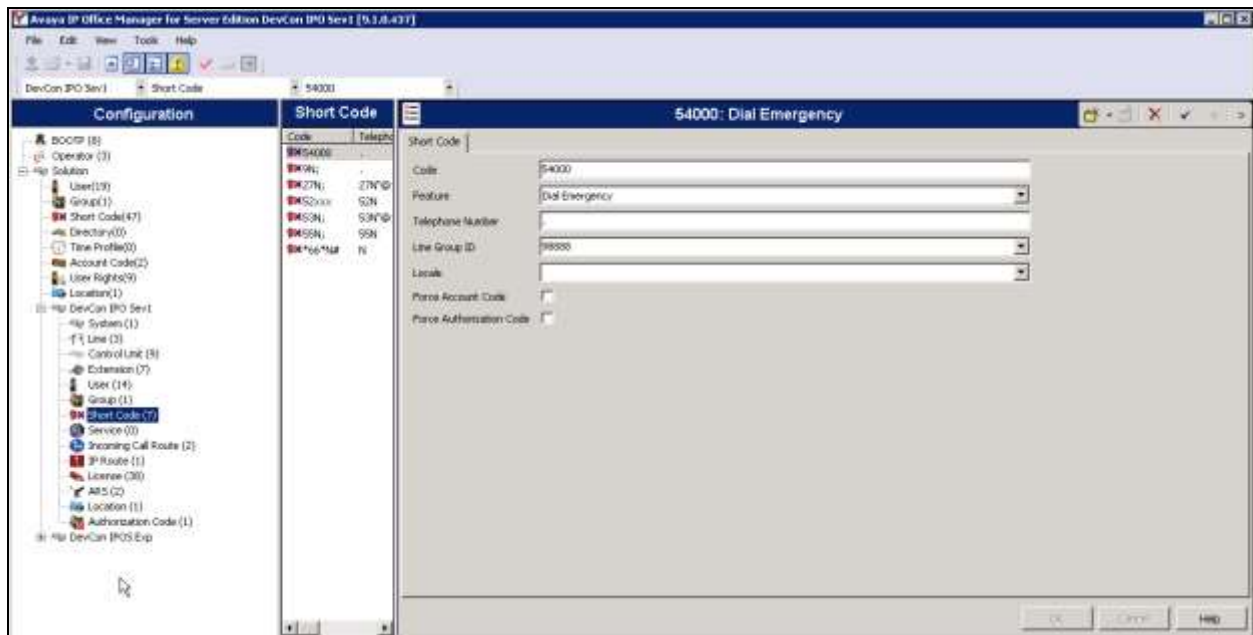
5. To test an emergency call, from the extension used in step 3, dial the Dial Emergency short code. IP Office checks the location value and determines the emergency ARS set for the location. Once the emergency ARS is found, IP Office will try to match the Telephone Number in the Dial Emergency short code to a short code in the ARS and use it to make the emergency call.

The sections below show the configuration used during compliance testing.

### 5.3. Short Code

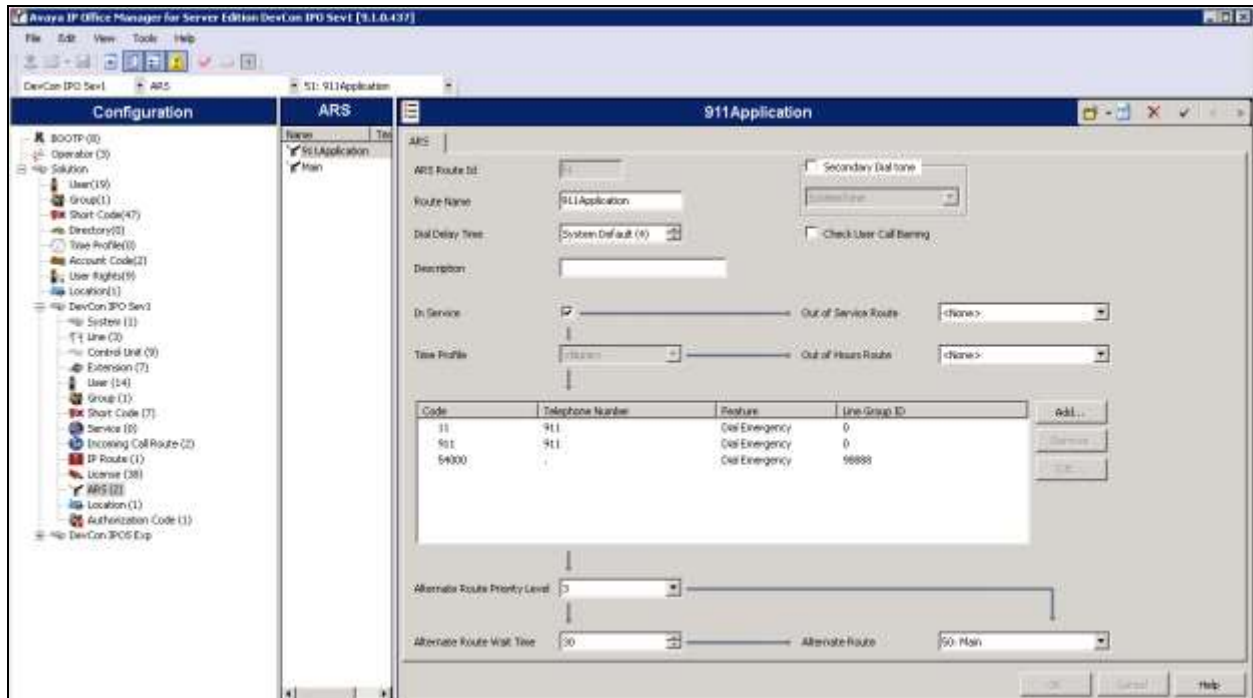
On the left Navigation pane, right-click **Short Code** for the Primary Server and select **New** (not shown). The screen below shows short code 54000 was created. For compliance testing, calls to 54000 were used to test emergency calls rather than placing actual 911 calls. Set the **Feature** to *Dial Emergency*. The **Telephone Number** was set to “.” to leave the dialed number unaltered.

Note that the **Line Group ID** value in the Dial Emergency short code here is the fallback route. If the system cannot find a location or an Emergency ARS, it will try to use the **Line Group ID** to route the call.



## 5.4. ARS

On the left Navigation pane, right-click **ARS** for the Primary Server and select **New** (not shown). Provide a descriptive **Route Name** and ensure **In Service** is checked. Click the **Add...** button on the right to add an ARS short code.



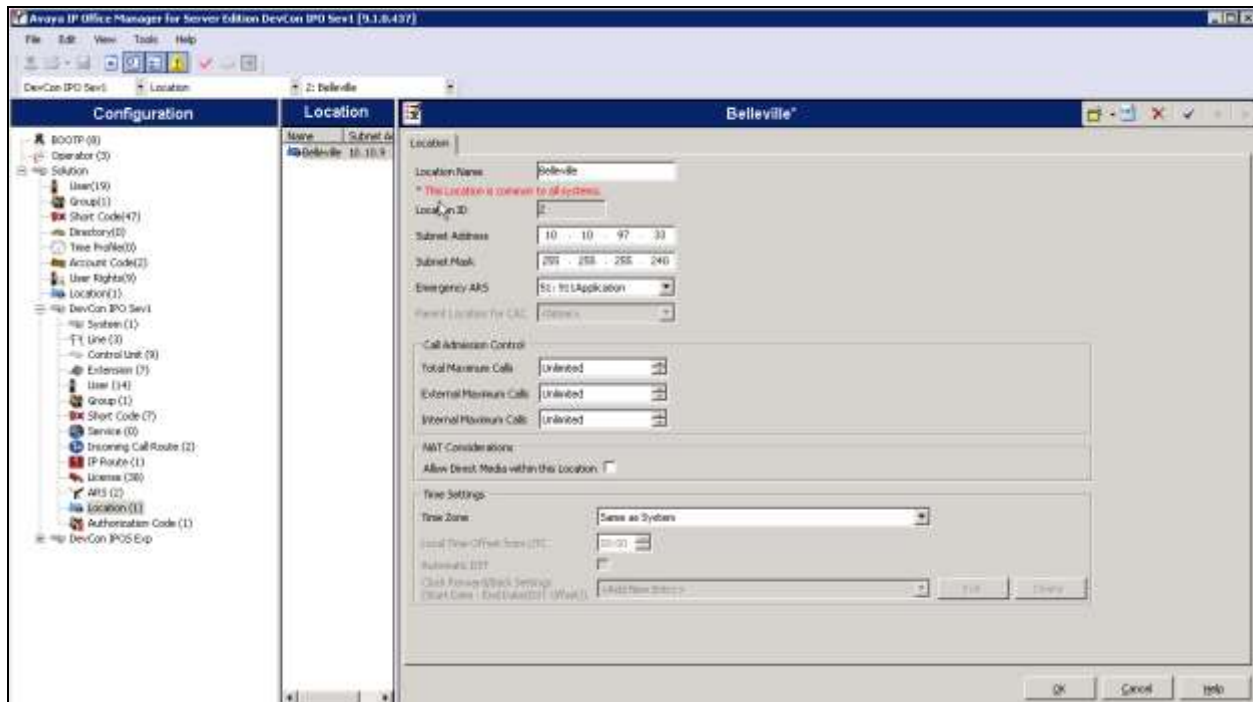
The screen below shows short code 54000 was created. For compliance testing, calls to 54000 were used to test emergency calls rather than placing actual 911 calls. Set the **Feature** to *Dial Emergency*. The **Telephone Number** was set to "." to leave the dialed number unaltered. Set the **Line Group ID** value to the line to be used to route emergency calls (configuration of lines/trunks are assumed to already be in place and is outside the scope of this document).

**New Short Code**

Code	54000	OK Cancel
Feature	Dial Emergency	
Telephone Number	.	
Line Group ID	98888	
Locale		
Force Account Code	<input type="checkbox"/>	
Force Authorization Code	<input type="checkbox"/>	

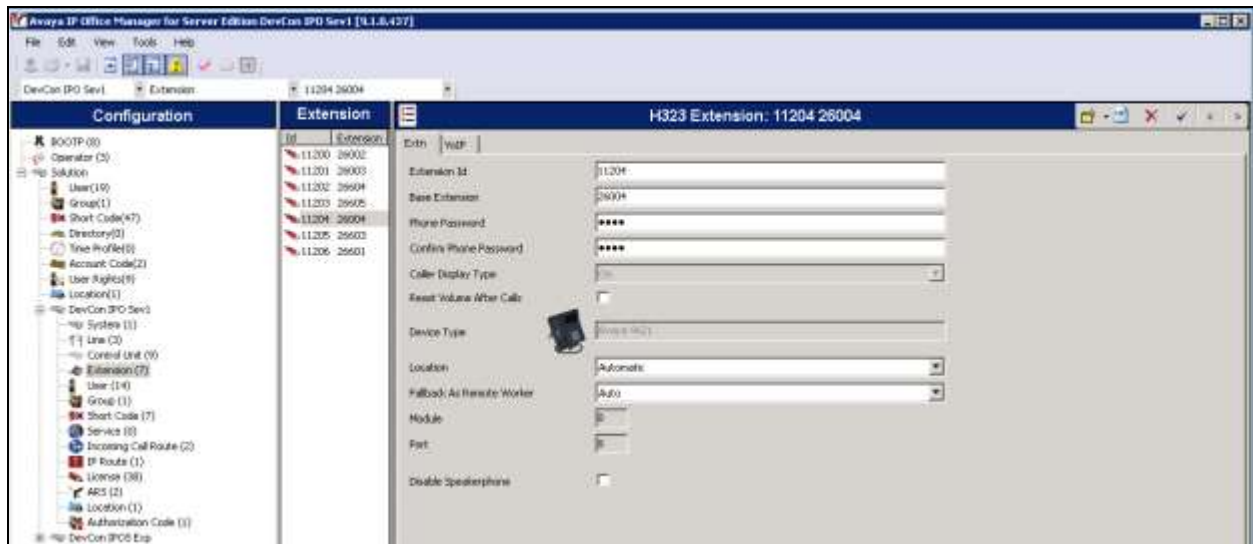
## 5.5. Locations

On the left Navigation pane, right-click **Location** for the Primary Server and select **New** (not shown). Enter a **Location Name**. Note, **Location Name** field accepts characters; this field will be used to match the Location value displayed in GenAlert (see **Section 7.2**). Use the **Subnet Address** and **Subnet mask** fields to define the IP addresses associated with this Location. The subnet where these IP addresses reside must be unique across all configured Locations. Set **Emergency ARS** to the ARS entry created in **Section 5.4**.



## 5.6. Extensions

Associate each extension with a Location. On the left Navigation pane, click **Extension** for the Primary Server and then select a desired extension to configure from the middle Group pane. In the Details Pane on the right, set the **Location** for the extension. The **Location** can be set to *Automatic* or to a specific Location that was configured in the previous section.





## 6. Configure Genesis GenAlert Solution

It is assumed that the GenAlert server has been installed, configured, and is ready for the integration with Avaya IP Office. The GenAlert Software Users Guide can be obtained by contacting Genesis. The sub-sections below only provide the steps required to configure the Genesis GenAlert Solution to interoperate with Avaya IP Office.

### 6.1. Genesis GenAlert Web Interface

Access the Genesis web interface by opening a web browser and entering the following URL: <http://localhost/GenWeb>. Login to the web interface using the proper credentials.



The screenshot displays the Genesis GenAlert web interface. At the top, there is a header banner with the 'Genesis UNIFIED SOLUTIONS' logo on the left, a yellow diamond-shaped warning sign in the center, and a background image of a bridge. Below the banner is a navigation bar with tabs for 'MACs', 'Call Accounting', 'Directory', 'Traffic', 'ACD', '911', and 'Fraud'. The main content area features a login section on the left with a 'Login' link and the text 'Please login for system access.'. To the right of this section are input fields for 'Username:' and 'Password:', followed by a 'Login' button. At the bottom left of the main area is the 'Genesis SYSTEMS CORPORATION' logo. The footer at the bottom right contains the text 'Copyright © 2015 Genesis Systems Corporation'.

## 6.2. Configure Switch Settings

From the main page displayed below, select the required site and then navigate to the section **911**. Note that site/s is configured by Genesis based on licenses purchased.

The screenshot shows the Genesis Unified Solutions administration interface. At the top, there is a header with the Genesis logo and a navigation bar containing links: MACs, Call Accounting, Directory, Traffic, ACD, **911**, and Fraud. The **911** link is highlighted with a red box. Below the navigation bar, the current site is identified as "Site 001 - AVAYA DEVCONNECT LAB - CS1000". A welcome message states: "Welcome admin. The current server date is Wednesday, April 01, 2015 3:38:25 PM". On the left, there is a sidebar with a "Change Site | Logout" button and a "Site Selection" section. Under "Administration:", there are links for "Change password", "Manage user accounts", and "Logout". In the main content area, under "Select a site to access:", there are two radio button options: "001 - AVAYA DEVCONNECT LAB - CS1000" and "002 - AVAYA DEVCONNECT LAB - IP OFFICE". The "002" option is selected and highlighted with a red box. At the bottom of the page, there is a footer with the Genesis Systems Corporation logo and the copyright notice: "Copyright © 2015 Genesis Systems Corporation".

From the screen shown below, navigate to **System Configuration** → **Update switch settings**.

**Genesis**  
UNIFIED SOLUTIONS

MACs | Call Accounting | Directory | Traffic | ACD | 911 | Fraud

Site 002 - AVAYA DEVCONNECT LAB - IP OFFICE

► [Change Site](#) | [Logout](#)

**GenAlert 911**

**Reports:**

- » Manual reports

**View:**

- » System Help

**System Maintenance:**

- » Update front screen
- » Update action plan
- » Update contact list

**System Configuration:**

- » Update switch settings
- » Configure email settings

**Events:**

- » Send test call

Avaya IP Office switch

Serial Connection

GCOM Direct connection

Recent 911 call activity:

Configure the following fields,

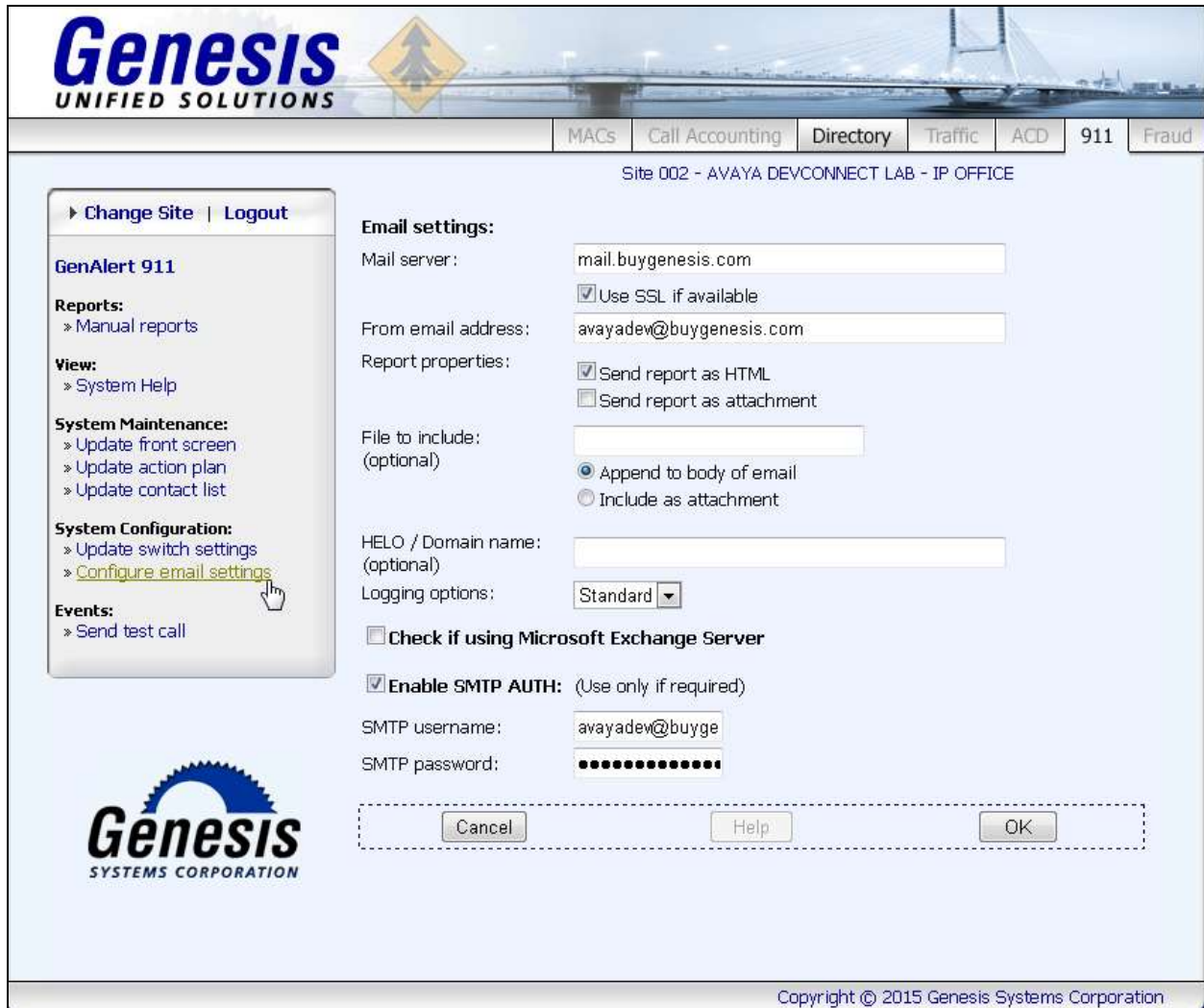
- **PBX Connection method:** Select *SNMP connection (IP Office, CS1000)*
- **Site name:** A descriptive name.
- **SNMP port:** Enter the matching SNMP traps port mentioned in **Section 5.1**.
- **PBX IP address:** IP addresses of the systems to monitor for SNMP traps. During compliance testing both Primary and Expansion systems were monitored.

Retain default values for all other fields and click on **Save** to complete the configuration.

The screenshot displays the Genesis Unified Solutions web interface. At the top, there is a header with the Genesis logo and a navigation bar with tabs: MACs, Call Accounting, Directory, Traffic, ACD, 911, and Fraud. The main content area is titled "Site 002 - AVAYA DEVCONNECT LAB - IP OFFICE". On the left, a sidebar contains links for "Change Site" and "Logout", and a "GenAlert 911" section with links for "Reports" (Manual reports), "View" (System Help), "System Maintenance" (Update front screen, Update action plan, Update contact list), "System Configuration" (Update switch settings, Configure email settings), and "Events" (Send test call). The main content area has a "PBX Connection method:" section with radio buttons for "SNMP connection (IP Office, CS1000)" (selected), "Serial port capture (Meridian)", "Telnet connection (serial to IP, Avaya CM)", "Avaya IP Office DevLink", and "Duplicate of an existing GCOM connection". Below this are fields for "Site name:" (AVAYA DEVCONNECT LAB - IP OFFICE), "Gcom location:" (localhost:7840), and "SNMP Settings:" (SNMP port: 162). The "PBX Settings:" section includes a note "(Required for filtering SNMP data in multi-site installations)" and a "PBX IP address:" field (10.10.97.44,10.10.97) with a note "(separate multiple IPs with commas)". At the bottom of the main content area are "Cancel", "Help", and "Save" buttons. The footer features the Genesis Systems Corporation logo and the text "Copyright © 2015 Genesis Systems Corporation".

### 6.3. Configure Email Settings

For compliance testing Genesis mail server was used. To configure the email settings, navigate to **System Configuration → Configure email settings**. The values shown in the screen below were configured for compliance testing.



**Genesis**  
UNIFIED SOLUTIONS

MACs | Call Accounting | **Directory** | Traffic | ACD | 911 | Fraud

Site 002 - AVAYA DEVCONNECT LAB - IP OFFICE

Change Site | Logout

**GenAlert 911**

**Reports:**  
» Manual reports

**View:**  
» System Help

**System Maintenance:**  
» Update front screen  
» Update action plan  
» Update contact list

**System Configuration:**  
» Update switch settings  
» Configure email settings

**Events:**  
» Send test call

**Email settings:**

Mail server: mail.buygenesis.com  
☒ Use SSL if available

From email address: awayadew@buygenesis.com

Report properties:  
☒ Send report as HTML  
☐ Send report as attachment

File to include: (optional)  
  
☒ Append to body of email  
☐ Include as attachment

HELO / Domain name: (optional)

Logging options: Standard

☐ Check if using Microsoft Exchange Server

☒ Enable SMTP AUTH: (Use only if required)

SMTP username: awayadew@buyge

SMTP password: .....

Cancel Help OK

**Genesis**  
SYSTEMS CORPORATION

Copyright © 2015 Genesis Systems Corporation



## 6.4. Configure Contact List

Emergency alerts can be forwarded to emails and also sent as SMS text messages via GenAlert. To configure email addresses or mobile numbers, navigate to **System Maintenance** → **Update contact list** as shown in the screen below. Enter the required email address or mobile number in the **New email address** field and click on **Add to list**. Click on **Save** to complete adding the required members.

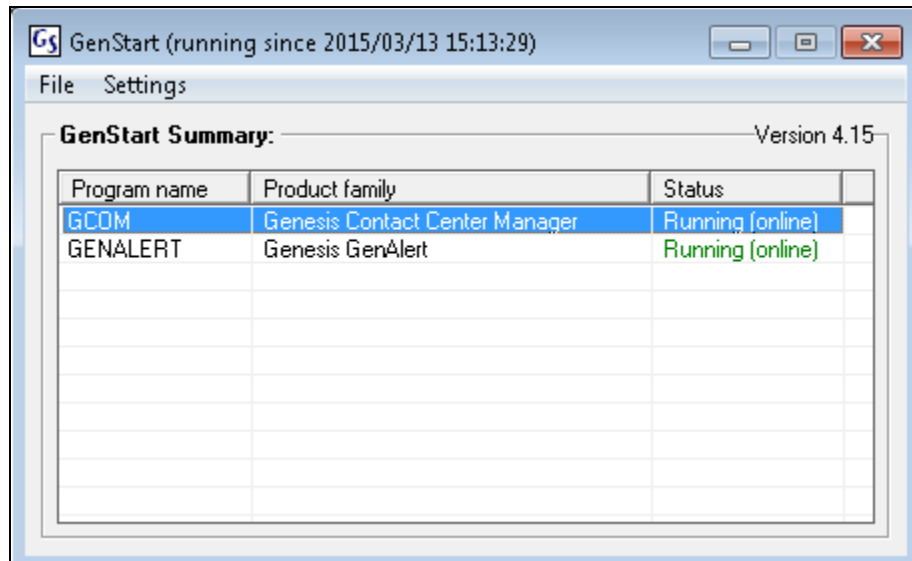
The screenshot displays the Genesis Unified Solutions web interface. At the top, the Genesis logo and a navigation bar with tabs like MACs, Call Accounting, Directory, Traffic, ACD, 911, and Fraud are visible. The current site is identified as 'Site 002 - AVAYA DEVCONNECT LAB - IP OFFICE'. On the left, a sidebar menu includes options like 'Change Site', 'Logout', 'GenAlert 911', 'Reports', 'View', 'System Maintenance' (with 'Update contact list' highlighted), 'System Configuration', and 'Events'. The main content area is titled 'Distribution list settings:' and shows a list named 'Emergency Mail List' with two members: 'sat@avaya.com' and '6136132333@msg.tel.com'. A 'Remove Selected' button is next to the list. Below the list is a 'New email address:' field with an 'Add to list' button. At the bottom of the form area are 'Cancel', 'Help', and 'Save' buttons. The footer includes the Genesis Systems Corporation logo and a copyright notice for 2015.

## 7. Verification Steps

This section includes some steps that can be followed to verify the configuration.

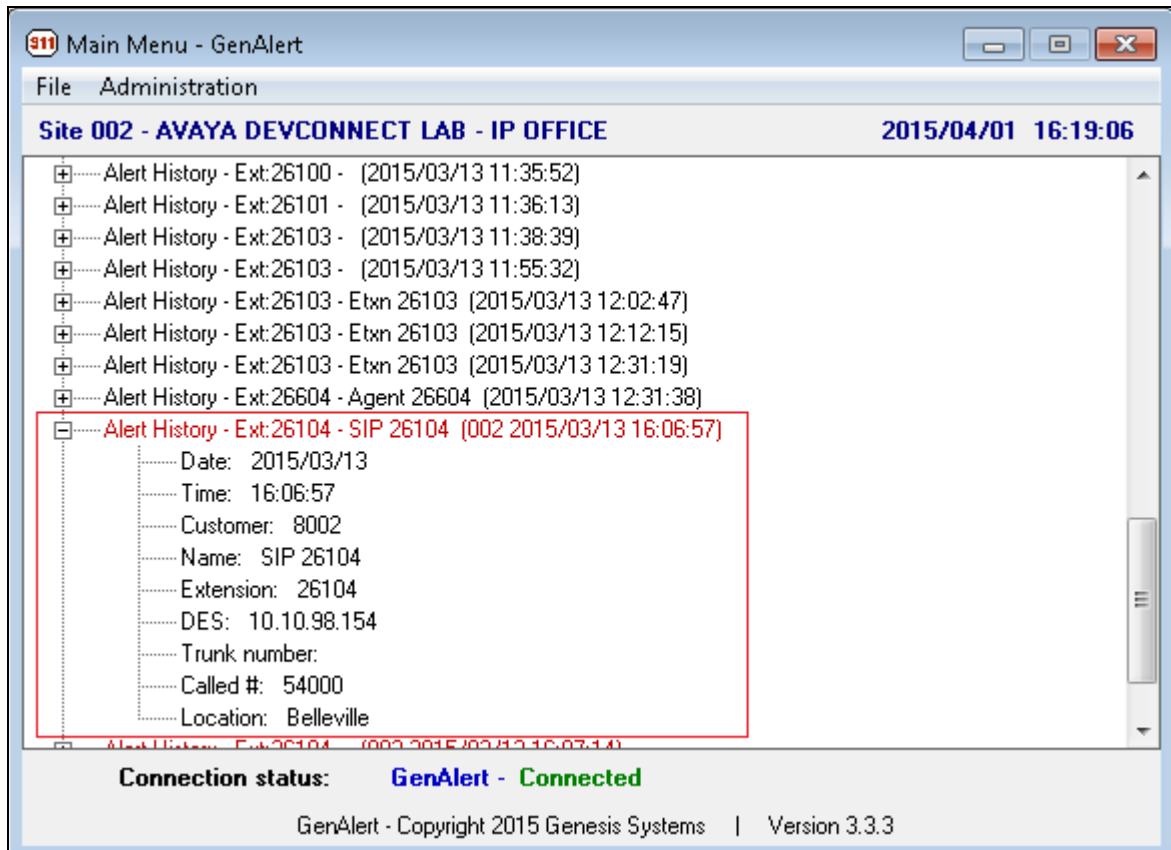
### 7.1. Verify Genesis Services

Verify that the Genesis Data Collection (**GCOM**) and Genesis GenAlert (**GENALERT**) services are online by selecting **show** from the **GenStart** icon (not shown) in the Windows System Tray on the Genesis server.



## 7.2. Verify Emergency Call Messages

Launch the GenAlert application installed on any PC. Generate an emergency call and verify that an alert is generated and the information shown in the alert is accurate as shown in the screen below. The alert information was also received via email and SMS text message and verified for accuracy.





## 8. Conclusion

The Genesis GenAlert Solution passed compliance testing. These Application Notes describe the procedures required for the Genesis GenAlert Solution to interoperate with Avaya IP Office to support the reference configuration shown in **Figure 1**. Refer to **Section 2.2** for testing result details and any observations noted during testing.

## 9. Additional References

Product documentation for Avaya products may be found at: <http://support.avaya.com>.

[1] *Administering Avaya IP Office Platform with Manager* Release 9.1.2 Issue 10.08.

Product documentation for Genesis Call Accounting Solution can be found at <http://www.buygenesis.com/documents.htm>.

---

**©2015 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).