



**Avaya Solution & Interoperability Test Lab**

---

**Application notes for Configuring Genesis GenAlert to Interoperate with Avaya Aura® Communication Manager – Issue 1.0**

**Abstract**

These Application Notes describe a compliance-tested configuration consisting of Genesis Systems Corporation GenAlert solution and Avaya Aura® Communication Manager Release 7.0.

Genesis GenAlert is a web or client based real-time emergency reporting package that provides on-site notification when an emergency call has been placed. This compliance test focused on the interoperability of Genesis GenAlert with Avaya Aura® Communication Manager Release 7.0.

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 a compliance-tested configuration consisting of Genesis Systems Corporation GenAlert (hereafter known as GenAlert) solution and Avaya Aura® Communication Manager Release 7.0 (hereafter known as Communication Manager).

GenAlert offers a web & client based real-time emergency reporting package that detects when 911 is called and notifies either by SMS text message, screen pop, email, and / or even sounding an alarm. This compliance test focused on the interoperability of GenAlert with Communication Manager.

The GenSwitch application of the Genesis server connects to Communication Manager Telnet port 5023 to collect station information and then the GenAlert module collects any alerts 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 alerts and station information generated by Communication Manager.

When an emergency call is placed, an alert is generated by Communication Manager. GenAlert collects this alert, compiles all information present in the alert and presents it in a user friendly form via screen pop, email, SMS text message or sounding an alarm.

The solution contains two modules under the GenStart application. One module named GCOM collects the raw alert 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.

For Emergency Location Extension, Building, Floor, Room, Jack, Cable and Name identification, Genesis uses the GSQM and PORTSERV modules to collect these data from Communication Manager and uses the same during an emergency call.

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 Communication Manager. Various emergency calls were placed from Communication Manager Telephones to verify alerts 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 observations:

- Emergency alert notification using email and text can be delayed since these are dependent on the email servers and local Telco providers.
- For location identification, Genesis uses the GSQM and PORTSERV modules which are part of Genesis GenSwitch application and therefore this application will be required.
- Building information configured in the Communication Manager Station form is not retained and therefore in the emergency alerts, no building information will be provided. Avaya is aware of this issue and is working towards a resolution.

**Note:** *Genesis GenAlert is an alerting application only and does not do any location discovery of the devices. Location discovery of devices using this application is the responsibility of the user by programming it in Avaya Communication Manager.*

## 2.3. Support

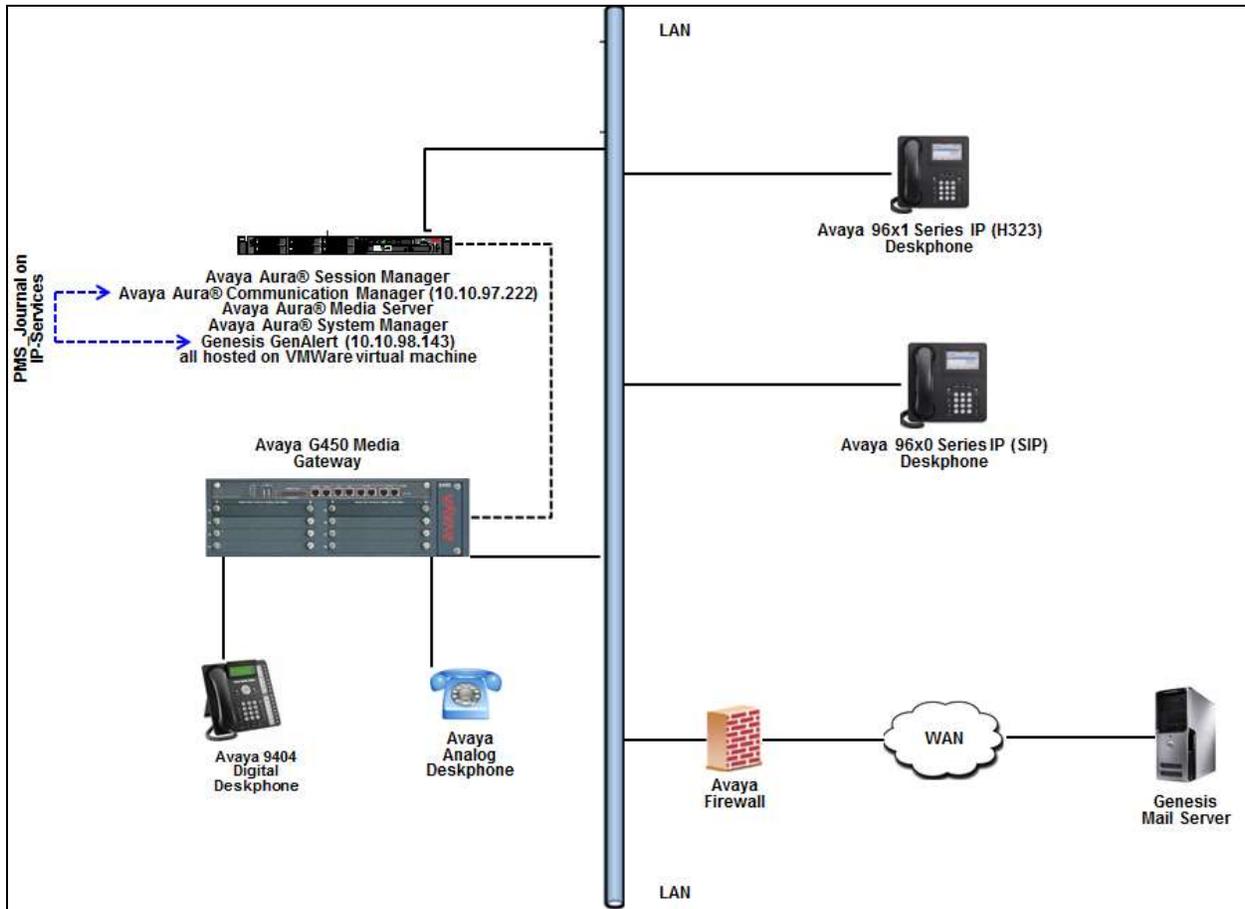
Information, Documentation and Technical support for Genesis products can be obtained at:

- 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 Communication Manager. The Genesis GenAlert Solution and the screen pop client were installed on a Windows 2008 Server Standard R2 SP1 OS. For email verification, a Genesis mail server was used and for SMS texting, a local Telco provider was used.

Any 911 calls made by a phone on Communication Manager were not sent over the PSTN and was only used to generate alerts.



**Figure 1: Genesis GenAlert Solution with Avaya Aura® Communication Manager**

## 4. Equipment and Software Validated

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	7.0.0.3.0-SP3 (R017x.00.0.441.0)
Avaya Aura® Session Manager	7.0.0.2.700201
Avaya Aura® System Manager	7.0.0.2 Build No. - 7.0.0.0.16266-7.0.9.7002010 Software Update Revision No: 7.0.0.2.4416
Avaya Aura® Media Server	7.7.0.292
Avaya G450 Media Gateway	37 .21 .0 /1
Avaya IP Deskphones: <ul style="list-style-type: none"> <li>• 9641 (H.323)</li> <li>• 9621 (SIP)</li> </ul>	6.6115 7.0.0.39
Avaya Digital Deskphone (9404)	R 0.15 V21
Avaya Analog Deskphone	N/A
Genesis:	
GenAlert installed on MS Windows Server 2008 R2 Standard SP1 OS on a VM Ware system	3.4.5
GenStart Module	4.16

## 5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Configure Server Access
- Configure Site Data
- Configure Stations
- Configure Crisis Alert
- Administer IP Node Names
- Configure PMS\_JOURNAL Port
- Configure Hospitality
- Configure ARS Routing

Assumption is made that the Communication Manager is correctly installed and configured to make emergency calls. It is beyond the scope of this document to explain in detail the configuration required to make emergency calls from Communication Manager.

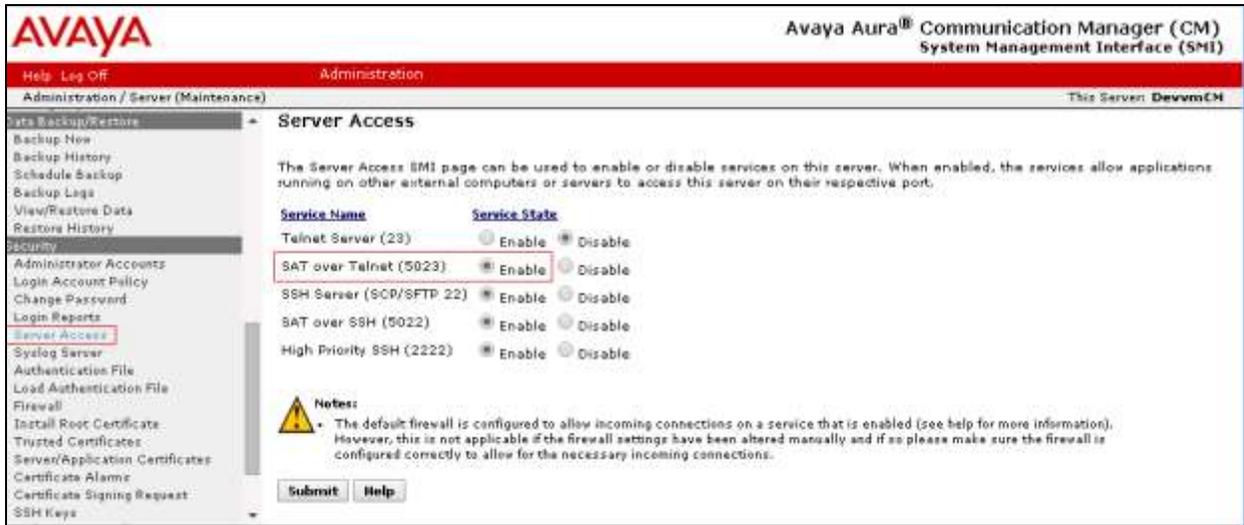
### 5.1. Configure Server Access

From a web browser, use the `http://<ip-address>`, where ip-address is the ip address of Communication Manager URL to access System Management Interface for Communication Manager. Log in using appropriate credentials.



The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI) login page. The page features a red header bar with the Avaya logo on the left and the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" on the right. Below the header, there is a "Help Log Off" link on the left and "This Server: DevvmCM" on the right. The main content area is a light gray box titled "Logon" containing a "Logon ID:" label, a text input field, and a "Logon" button.

Navigate to **Administration** → **Server (Maintenance)** → **Security** → **Server Access** and ensure that the **SAT over Telnet (5023)** is enabled. This is the port that the Genesis GenSwitch will connect to Communication Manager to collect the required station information.



## 5.2. Configure Site Data

To configure specific building codes and floor information for a site, use **change site-data** command.

On Page 1, add entries for building fields. For compliance test, two entries of **AA1** and **AA2** were added. On Page 3, add entries for floor fields. For compliance test, one entry of **AA1-F1** was added.

```

change site-data                                     Page 1 of 4
SITE DATA USER DEFINITION
VALID BUILDING FIELDS

AA1
AA2

change site-data                                     Page 3 of 4
SITE DATA USER DEFINITION
VALID FLOOR FIELDS

AA1-F1
  
```

### 5.3. Configure Stations

Use **add station *n*** command to add a station, where ***n*** is an available station extension. This station is an example station that was used during compliance testing to dial an emergency call. Configure the station as follows, on Page 1:

- In **Name** field, enter a descriptive name
- Set **Type** to the type of the telephones
- Enter a **Security Code**

```
add station 56102                                     Page 1 of 5
                                                    STATION
Extension: 56102                                     Lock Messages? n          BCC: M
  Type: 9641                                         Security Code: *         TN: 1
Port: S00002                                         Coverage Path 1:         COR: 1
  Name: OneOTwo                                     Coverage Path 2:         COS: 1
                                                    Hunt-to Station:         Tests? y

STATION OPTIONS
Loss Group: 19                                       Time of Day Lock Table:
Speakerphone: 2-way                                  Personalized Ringing Pattern: 1
Display Language: english                            Message Lamp Ext: 56102
Survivable GK Node Name:                             Mute Button Enabled? y
Survivable COR: internal                             Button Modules: 0
Survivable Trunk Dest? y                             Media Complex Ext:
                                                    IP SoftPhone? y
                                                    IP Video Softphone? y
Short/Prefixed Registration Allowed: default
                                                    Customizable Labels? y
```

One Page 4, enter the site data information, as shown below. The floor and building information is configured based on the information configured in **Section 5.2**.

```
add station 56102                                     Page 4 of 5
                                                    STATION
SITE DATA
  Room: 1                                           Headset? n
  Jack: 2                                           Speaker? n
  Cable: 3                                          Mounting: d
  Floor: AA1-F1                                    Cord Length: 0
  Building: AA1                                    Set Color:

ABBREVIATED DIALING
List1:                                             List2:                    List3:

BUTTON ASSIGNMENTS
1: call-appr                                       5: release
2: call-appr                                       6: after-call            Grp:
3: call-appr                                       7: aux-work             RC:   Grp:
4: auto-in                                         8: manual-in            Grp:

voice-mail
```

## 5.4. Configure Crisis Alert

Use `change system-parameters crisis-alert` command and set **Every User Responds** to **y**.

```
change system-parameters crisis-alert                               Page 1 of 1
                               CRISIS ALERT SYSTEM PARAMETERS

ALERT STATION
  Every User Responds? y

ALERT PAGER
  Alert Pager? N
```

## 5.5. Administer IP Node Names

Use the `change node-names ip` command to create a new node name for the server running GenAlert. This node name is associated with the IP Address of the server. In the sample configuration **GenAlert** was used for the name and **10.10.98.143** was used for the IP address. Also, take note of the node name **procr**. It will be used in the next step. The **procr** entry on this form was previously administered.

```
change node-names ip                                             Page 1 of 2
                               IP NODE NAMES

  Name          IP Address
  GenAlert      10.10.98.143
  procr         10.10.97.222
```

## 5.6. Configure PMS\_JOURNAL Port

Use the `change ip-services` command to define the **PMS\_JOURNAL** service on Communication Manager. GenAlert will listen on this port to capture any emergency alerts that will be generated by Communication Manager. To define a **PMS\_JOURNAL** service, provide the following information:

- **Service Type:** **PMS\_JOURNAL**
- **Local Node:** **procr** [For the Communication Manager used during compliance testing, set the Local Node to the node name of the processor board.]
- **Local Port:** **0**
- **Remote Node:** **GenAlert** [The Remote Node is set to the node name previously defined in **Section 5.5**.]
- **Remote Port:** **8901** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in GenAlert. See **Section 6.2**]

```
change ip-services                                               Page 1 of 4
                               IP SERVICES

  Service      Enabled      Local      IP SERVICES      Remote      Remote
  Type         Type          Node       Local           Node         Port
  PMS_JOURNAL  y              procr      0               GenAlert     8901
```

For this solution the Reliable Session Protocol (RSP) is not used. On Page 3 of the ip-services form, set the **Reliable Protocol** field to n.

```
change ip-services
```

Page 3 of 4

Service Type	Reliable Protocol	SESSION LAYER TIMERS				Connectivity Timer
		Packet Resp Timer	Session Message Cntr	Connect Cntr	SPDU Cntr	
PMS_JOURNAL	n	30	3	3	60.	

## 5.7. Configure Hospitality

Use **change system-parameters hospitality** command to assign the **PMS\_JOURNAL** configured in Section 5.6 to **Journal/Schedule Endpoint** field as shown below.

```
change system-parameters hospitality
```

Page 1 of 3

HOSPITALITY

Message Waiting Configuration: act-nopms  
 Controlled Restrictions Configuration: act-nopms  
 Housekeeper Information Configuration: act-nopms  
 Number of Housekeeper ID Digits: 0  
 PMS Log Endpoint:  
**Journal/Schedule Endpoint: PMS\_JOURNAL**  
 Client Room Coverage Path Configuration: act-nopms

## 5.8. Configure ARS Routing

Use the **change ars analysis 911** command to configure 911 calls to route them appropriately and enable crisis alerts. The following configuration shows that when 911 is dialed, the call is routed over route 1 and a crisis alert is generated by Communication Manager.

- Set **Dialed String** to **911**
- Set **Total Min** and **Max** to **3**
- Set **Route Pattern** to a valid pattern that is already configured in Communication Manager. During compliance testing **1** was used.
- Set **Call Type** to **alrt**

```
change ars analysis 911
```

Page 1 of 2

ARS DIGIT ANALYSIS TABLE  
 Location: all                      Percent Full: 2

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
911	3	3	1	alrt		n

## 6. Configure Genesis GenAlert Solution

It is assumed that the GenAlert software has been installed, configured, and is ready for the integration with Communication Manager. 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 Communication Manager.

### 6.1. Genesis GenAlert Web Interface

Access the Genesis web interface on the server it was installed, 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 left is the "Genesis UNIFIED SOLUTIONS" logo. To its right is a yellow diamond-shaped warning sign with a black tree icon. The background features a bridge over water. A navigation bar contains the following menu items: MACs, Call Accounting, Directory, Traffic, ACD, 911, and Fraud. The main content area includes a "Login" section with a sub-header "Please login for system access." and a "Login" button. To the right of this section are input fields for "Username:" and "Password:", followed by a "Login" button. At the bottom left is the "Genesis SYSTEMS CORPORATION" logo. At the bottom right, the copyright notice reads "Copyright © 2016 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 left is the Genesis logo with the tagline "UNIFIED SOLUTIONS". To its right is a yellow diamond-shaped warning sign with a black silhouette of a tree. The background of the header features a bridge over water. Below the header is a navigation bar with tabs for "MACs", "Call Accounting", "Directory", "Traffic", "ACD", "911", and "Fraud". The main content area displays "Site 001 - AVAYA DEVCONNECT LAB - AVAYA CM" and a welcome message: "Welcome admin. The current server date is Monday, February 29, 2016 10:10:31 AM". On the left, there is a sidebar menu with "Change Site" and "Logout" options, and a "Site Selection" section under "Administration" containing "Change password", "Manage user accounts", and "Logout". The "Select a site to access:" section shows a radio button selected for "001 - AVAYA DEVCONNECT LAB - AVAYA CM". At the bottom left is the Genesis Systems Corporation logo, and at the bottom right is the copyright notice: "Copyright © 2016 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 001 - AVAYA DEVCONNECT LAB - AVAYA CM

► 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 CM switch

Action Plan

Contact List

Email Settings

Reports and Listings

Serial Connection

GCOM Direct connection

Configure the following fields:

- **PBX Connection method:** Select *Telnet connection (serial to IP, Avaya CM)*
- **Site name:** A descriptive name.
- **TCP port:** Enter the matching TCP port mentioned in **Section 5.6**.

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

The screenshot displays the configuration page for 'Site 001 - AVAYA DEVCONNECT LAB - AVAYA CM'. The interface includes a top navigation bar with tabs for 'MACs', 'Call Accounting', 'Directory', 'Traffic', 'ACD', '911', and 'Fraud'. A left sidebar contains a 'Change Site | Logout' link and a 'GenAlert 911' section with sub-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 configuration area is titled 'PBX Connection method:' and features five radio button options: 'SNMP connection (IP Office, CS1000)', 'Serial port capture (Meridian)', 'Telnet connection (serial to IP, Avaya CM)' (selected and highlighted with a red box), 'Avaya IP Office DevLink', and 'Duplicate of an existing GCOM connection'. Below this, the 'Site name:' field contains 'AVAYA DEVCONNECT LAB - AVAYA CM' (highlighted with a red box). The 'Gcom location:' field is 'localhost:7840' with a note that 'localhost:7840' is the default. Under 'Telnet Settings:', the 'IP address / host:' field is empty, and the 'TCP port:' field contains '8901' (highlighted with a red box). At the bottom, there are 'Cancel', 'Help', and 'Save' buttons within a dashed border.

### 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 001 - AVAYA DEVCONNECT LAB - AVAYA CM

► 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: [Redacted]

Use SSL if available

From email address: awayadev@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: awayadev@buyge

SMTP password: [Masked]

Cancel Help OK

**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 a descriptive name in the **List name** field. To add entries under **List members**, 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 left is the logo "Genesis UNIFIED SOLUTIONS" with a yellow diamond icon containing a tree. A navigation bar includes tabs for "MACs", "Call Accounting", "Directory", "Traffic", "ACD", "911", and "Fraud". Below the navigation bar, the site identifier "Site 001 - AVAYA DEVCONNECT LAB - AVAYA CM" is shown. On the left, a sidebar menu contains sections: "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", and "Events: Send test call". The main content area is titled "Distribution list settings:" and includes a "List name:" field with the value "Test". Below it is a "List members:" list box containing "emailaddress@avaya.com" and "1234567890@msg.telco.com", with a "Remove Selected" button to its right. A "New email address:" field is positioned below the list, with an "Add to list" button to its right. At the bottom, a dashed box encloses "Cancel", "Help", and "Save" buttons.

## 7. Verification Steps

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

### 7.1. Verify Emergency Alerts on Avaya Aura® Communication Manager

Use the **list emergency** command to verify the alerts that was generated by Communication Manager as shown below.

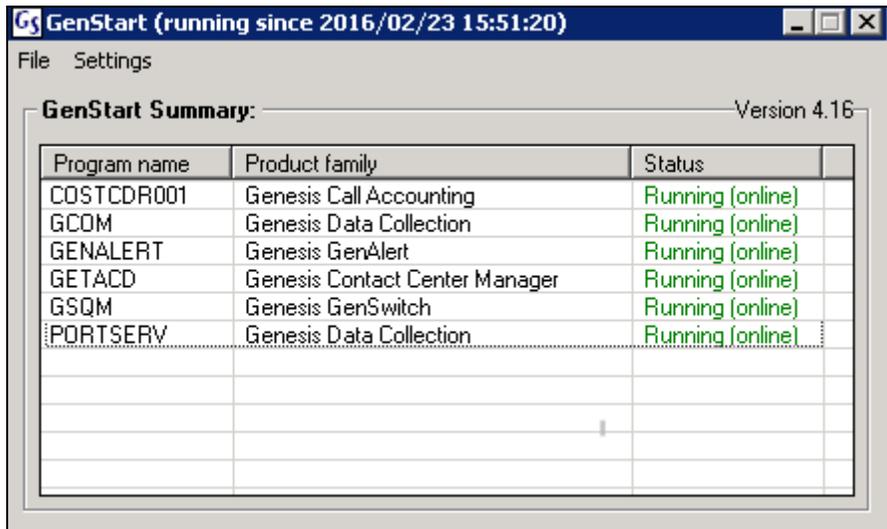
```
list emergency
```

EMERGENCY ACCESS CALLS				
Caller	Event	Type of Call	Time	
56102	attd crisis alert	ars alrt call type	02:55 P	
56102	attd crisis alert	ars alrt call type	02:56 P	
56204	attd crisis alert	ars alrt call type	02:56 P	
56204	attd crisis alert	ars alrt call type	02:56 P	
56401	attd crisis alert	ars alrt call type	02:57 P	
56401	attd crisis alert	ars alrt call type	02:57 P	
56102	attd crisis alert	ars alrt call type	03:21 P	
56401	attd crisis alert	ars alrt call type	03:23 P	
56204	attd crisis alert	ars alrt call type	03:23 P	
56501	attd crisis alert	ars alrt call type	03:24 P	
56204	attd crisis alert	ars alrt call type	03:32 P	
56204	attd crisis alert	ars alrt call type	03:34 P	
56204	attd crisis alert	ars alrt call type	03:40 P	
56204	attd crisis alert	ars alrt call type	03:41 P	

## 7.2. Verify Genesis Services

Verify that the Genesis Contact Center Manager (**GCOM**) and Genesis GenAlert (**GENALERT**) services are online by selecting **show** from the **GenStart** icon  in the Windows System Tray on the Genesis server.

Also verify that Genesis GenSwitch (**GSQM**) and Genesis Data Collection (**PORTSERV**) services are online and running. These services are required to collect the additional information of any station that dials 911.

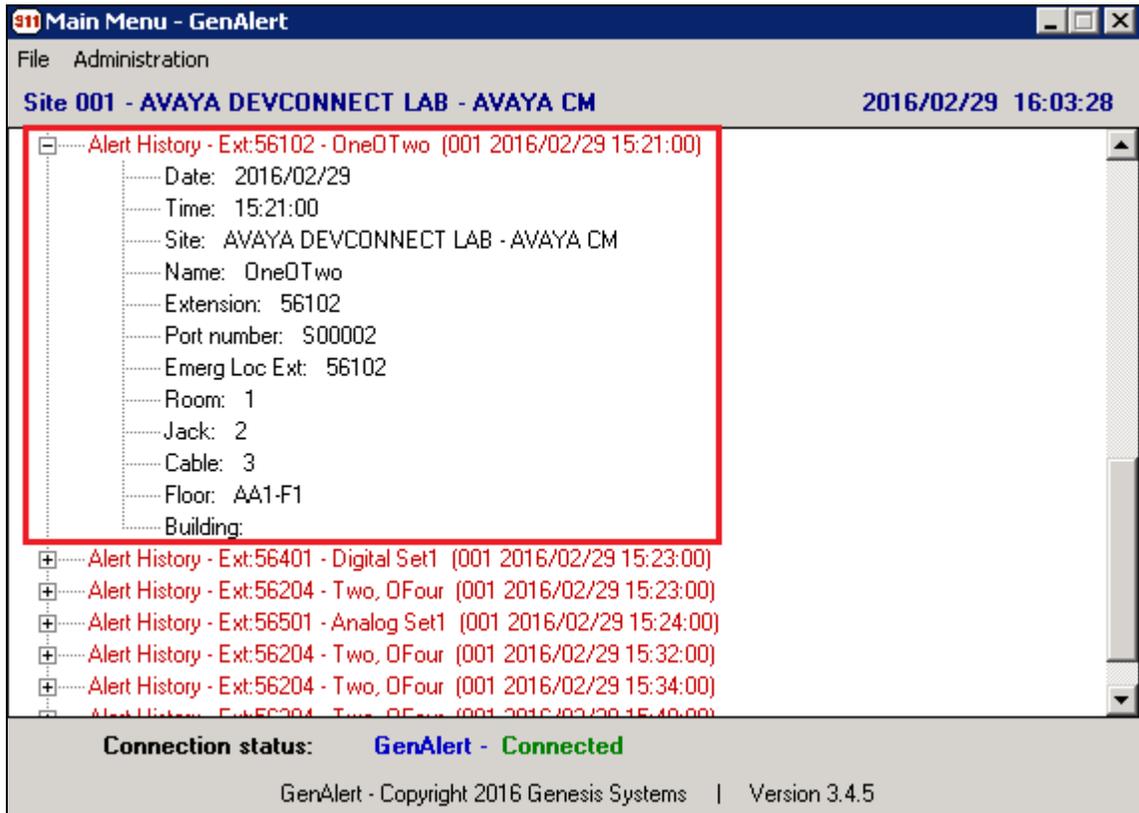


The screenshot shows the GenStart application window with the title bar "GenStart (running since 2016/02/23 15:51:20)". The window contains a "GenStart Summary" section with a table listing various services and their status.

Program name	Product family	Status
COSTCDR001	Genesis Call Accounting	Running (online)
GCOM	Genesis Data Collection	Running (online)
GENALERT	Genesis GenAlert	Running (online)
GETACD	Genesis Contact Center Manager	Running (online)
GSQM	Genesis GenSwitch	Running (online)
PORTSERV	Genesis Data Collection	Running (online)

### 7.3. 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 Aura® Communication Manager 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. *Implementing Avaya Aura® Session Manager* Document ID 03-603473.
2. *Administering Avaya Aura® Session Manager*, Doc ID 03-603324.
3. *Deploying Avaya Aura® System Manager*, Release 7.0.
4. *Administering Avaya Aura® System Manager for Release 7.0*, Release 7.0.
5. *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*.
6. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.7.
7. *Administering Avaya Aura® Communication Manager*, Release 7.0, 03-300509.
8. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, 555-245-205.

Product documentation for the Genesis GenAlert Solution can be found at <http://www.buygenesis.com/software/911-alerts/genalert.htm>.

---

**©2016 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).