



Application notes for Configuring Genesis GenAlert to Interoperate with Avaya Communication Server 1000 – Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration consisting of Genesis Systems Corporation GenAlert solution and Avaya Communication Server 1000 Release 7.6.

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 Communication Server 1000 Release 7.6.

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 Communication Server 1000 Release 7.6 (hereafter known as Communication Server 1000).

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 Server 1000.

The GenAlert server connects to Communication Server 1000 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 Communication Server 1000.

When an emergency call is placed, an On Site Notification (OSN) message is generated by Communication Server 1000 and provided as an SNMP trap. GenAlert collects this SNMP trap, compiles all information present in the trap 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 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.

For location identification, Genesis uses the GSQM and PORTSERV modules to collect the Emergency Response Location (ERL) data from Communication Server 1000 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

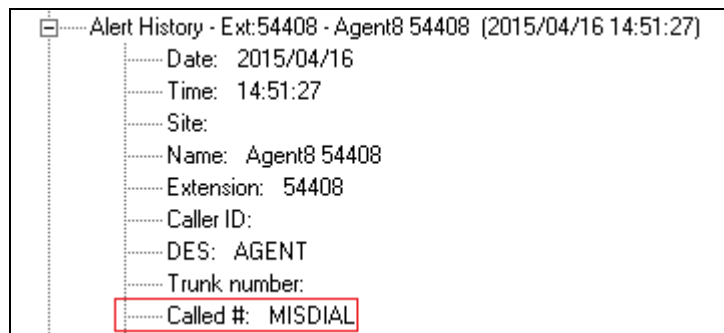
The general test approach was to verify the integration of GenAlert with Communication Server 1000. Various emergency calls were placed from Communication Server 1000 telephones to verify SNMP traps were properly logged and displayed (via pop-up alerts) by GenAlert. GenAlert's email and text message 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 observations:

- 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.
- For location identification, Genesis uses the GSQM and PORTSERV modules which are part of Genesis GenSwitch application and therefore this application will be required.
- If a misdial event occurs, GenAlert will notify of the same by showing *MISDIAL* in the application's *Called #* field as shown in the screen below.



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 Server 1000.*

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

3. Reference Configuration

Figure 1 below illustrates the configuration used to compliance test the Genesis GenAlert solution with Communication Server 1000. 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.

Any 911 calls made by a phone on the Communication Server 1000 was directed to a PSTN phone (not shown) to ring and emulate the receiving end of the 911 call.

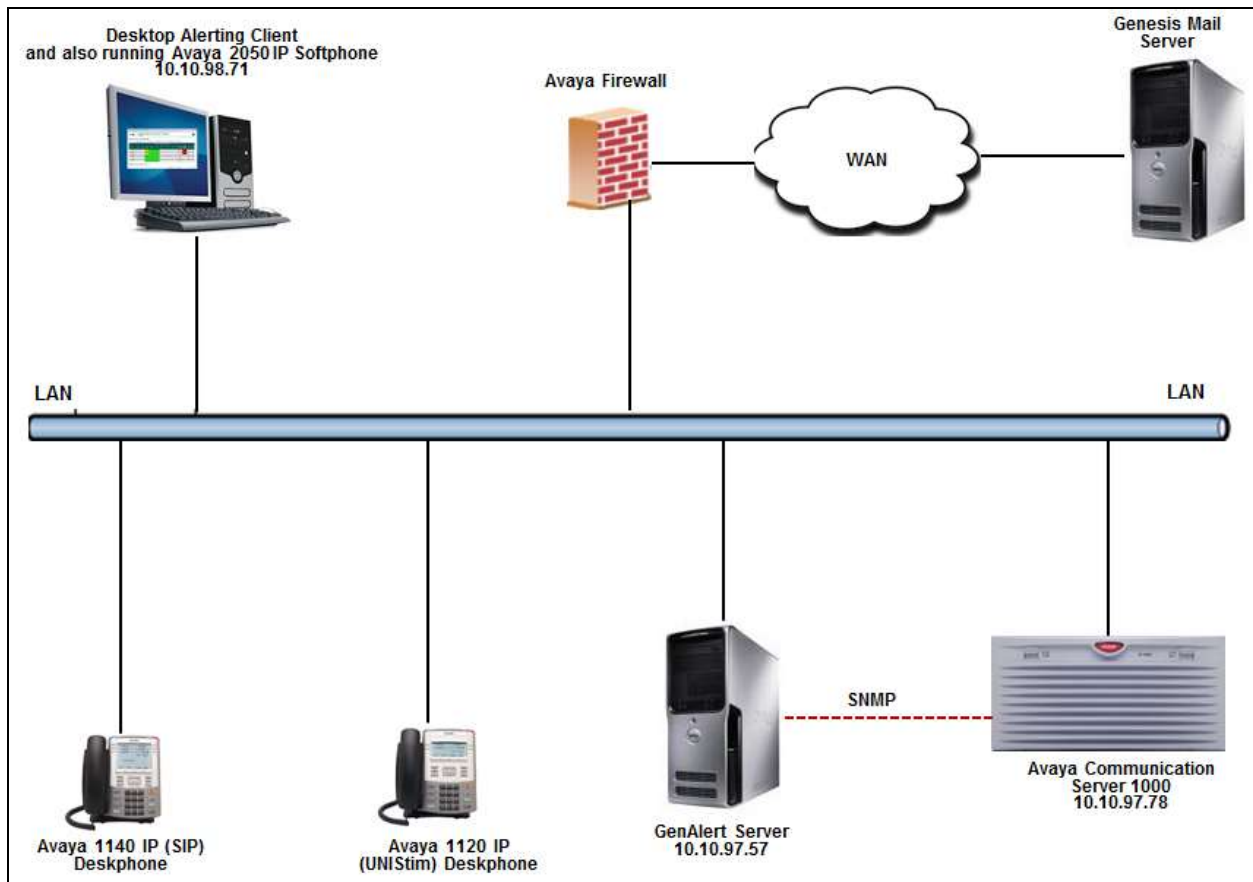


Figure 1: Genesis GenAlert Solution with Avaya Communication Server 1000

4. Equipment and Software Validated

Equipment/Software	Release/Version
Avaya Communication Server 1000	7.65 SP6
Avaya IP Phones: <ul style="list-style-type: none">• 1120(UNISlim)• 1140 (SIP)• 2050 IP Softphone	0624C8V 4.04.10 4.4 SP3
Genesis: GenAlert installed on MS Windows 7 Professional SP1 GenStart Module	3.3.3 4.15

5. Configure Avaya Communication Server 1000

This section assumes that the Communication Server 1000 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 Server 1000. However a brief description of the call routing used during compliance testing and SNMP configuration will be explained in this document.

5.1. Configure SNMP

Access the Communication Server 1000 Element Manager via the Unified Communication Manager or System Manager (not shown).

Navigate to **System** → **Alarms** → **SNMP** (not shown) to add the system that is going to collect the SNMP traps. In this case it would be the GenAlert system. Screen below shows the values used during compliance testing. Ensure that the **Enable trap sending** box under **Options** is checked. Enter the IP address of the GenAlert system that will collect the SNMP traps in the **IP address 1** field under **Trap Destination**. For **Port 1** enter *162*. Click on **Save** (not shown) to complete the configuration.

The screenshot displays the 'SNMP Configuration' page in the Avaya CS1000 Element Manager. The page is divided into several sections:

- System Info:** Fields for System name (System Name), System contact (System Contact), System location (System Location), Navigation site name (Navigation Site No), and Navigation system name (Navigation System).
- Management Information Base Access:** Fields for Administrator group 1 (admingroup1), Administrator group 2 (admingroup2), Administrator group 3 (admingroup3), System management read (otm123), and System management read/write (otm321).
- Alarm:** Fields for Trap community (public), Alarm threshold (None), and a note: 'Alarms below this threshold will be suppressed.'
- Options:** A checkbox for 'Enable trap sending' is checked.
- Trap Destination:** Fields for IP address 1 (10.10.97.57) and Port 1 (162).

5.2. Configure Routing

Navigate to **Dialing and Numbering Plans** → **Electronic Switched Network** → **Digit Manipulation Block** (not shown) to add a new Digit Manipulation Block. During compliance testing, Digit Manipulation Index Number **13** was added as shown in the screen below. The following values were configured,

- **Number of leading digits to be deleted:** 3; when a user dials 911, all of these are deleted.
- **Insert:** 916139675280; after deleting the above digits, 916139675280 are inserted instead and the call is routed to this number. During compliance testing, 6139675280 is used as simulated PSAP number. When user dials 911, the call is routed to this phone.
- **Call Type to be used by the manipulated digits:** Select *Call type will not changed (NCHG)* from the drop down list.

The screenshot displays the AVAYA CS1000 Element Manager interface. The top navigation bar shows the user is logged in as 'admin' and is currently viewing the 'Digit Manipulation Block List' configuration page. The left sidebar contains a tree view of system components, with 'Dialing and Numbering Plans' and 'Electronic Switched Network' expanded. The main content area is titled 'Digit Manipulation Block' and contains the following configuration fields:

- Digit Manipulation Index numbers: 13
- Number of leading digits to be deleted: 3 (0-16)
- Insert: 916139675280
- IP Special Number:
- Call Type to be used by the manipulated digits: Call type will not be changed (NCHG)

Navigate to **Dialing and Numbering Plans** → **Electronic Switched Network** → **Route List Block** (not shown) to add a new Route List Block. During compliance testing, Route List Block Index **19** was added as shown in the screen below. The following values were configured,

- **Digit manipulation Index:** 13; this was the value configured above during compliance testing.
- **Route Number:** 1; this was an active route that is used to route the call during compliance testing.

Retain default values for all other fields.

The screenshot displays the 'Data Entry of a Route List Block' configuration page in the Avaya CS1000 Element Manager. The page title is 'Data Entry of a Route List Block' and the sub-header is 'Route List Block Index: 19'. The left sidebar shows a navigation tree with 'Dialing and Numbering Plans' selected. The main content area is divided into sections: 'General Properties', 'Indexes', 'Options', and 'VNS Options'. In the 'Indexes' section, the 'Digit Manipulation Index' is set to 13, and the 'Route Number' is set to 1. Other fields like 'Time of Day Schedule', 'Facility Restriction Level', 'ISL D-Channel Down Digit Manipulation Index', 'Free Calling Area Screening Index', 'Free Special Number Screening Index', 'Business Network Extension Route', and 'Incoming CUID Tattle' are also visible. The 'Options' section includes checkboxes for 'Local Termination entry', 'Skip Conventional Signaling', 'Use Tone Detector', 'Conversion to LDN', 'Expensive Route', and 'ISDN Off-Hook Queuing Option', along with dropdown menus for 'Strategy on Congestion', 'OSIG Alternate Routing Causes', 'Preferred Routing', and 'ISDN Drop Back Busy'. The 'VNS Options' section has a checkbox for 'Entry is a VNS Router'.

5.3. Configure Emergency Service Access (ESA)

Navigate to **System** → **Emergency Services** → **Access Numbers and Routing** to add an Emergency Service Directory Number. If there was no ESA Access Numbers and Routing configured, the **Emergency Services Directory Number** page appears as shown below.

The screenshot shows the configuration page for adding a new Emergency Services Directory Number. The breadcrumb trail is System > Emergency Services > Access Numbers and Routing > Add Customer 0 Emergency Services Directory. The page title is 'Add Customer 0 Emergency Services Directory Number'. The left sidebar shows the navigation menu with 'Access Numbers and Routing' highlighted. The main form contains the following fields: Directory Number (required), Directing Digits (required), Default Calling Number, On-Site Notification Station DN, Routing Method (with radio buttons for Route Number and Route List Index), Misdial Prevention (checkbox), Misdial Delay (2 seconds), and Last ESDN Digit Repetition (checked). There are 'Save' and 'Cancel' buttons at the bottom right and a '* Required value.' note at the bottom left.

Enter the following information as shown below,

- **Directory Number:** 911
- **Directing Digit:** 911
- **Routing Method:** Select *Route List Index* and choose the appropriate value available from pull down menu. During compliance testing 19 was selected as configured previously in **Section 5.2**.
- **Misdial Prevention**, a dialog box appears asking for your confirmation to enable the feature, click *OK*. The remaining fields were left at their default values. Click **Save**.

The screenshot shows the configuration page for editing an existing Emergency Services Directory Number. The breadcrumb trail is System > Emergency Services > Access Numbers and Routing > Edit Emergency Services Directory Num. The page title is 'Edit Emergency Services Directory Number Entry 0'. The left sidebar shows the navigation menu with 'Access Numbers and Routing' highlighted. The main form contains the following fields: Directory Number (911), Directing Digits (911), Routing Method (with radio buttons for Route Number and Route List Index, where Route List Index is selected and set to 19), Misdial Prevention (checked), Misdial Delay (2 seconds), and Last ESDN Digit Repetition (checked). There are 'Save' and 'Cancel' buttons at the bottom right and a '* Required value.' note at the bottom left.

Screen below shows the completed configuration.

Access Numbers and Routing

Emergency Services Directory Number (ESDN) is used to handle emergency calls and hence treated with high priority.

Emergency Services Access Data for

Default Calling Number :

On-Site Notification Station DN :

Emergency Services Directory Numbers

	Entry	Directory Number	Routing Method	Route Value	Directing Digits	Misdial Prevention	Misdial Delay	Last ESDN Digit Repetition
<input checked="" type="radio"/>	Primary	911	RLI	19	911	YES	2	YES

5.4. Configure Emergency Response Location (ERL)

Navigate to **System** → **Emergency Services** → **Emergency Response Location** to add an Emergency Response Location.

Click on **Add** from the screen shown below.

- Links
- Virtual Terminals
- System
- + Alarms
- Maintenance
- + Core Equipment
- Peripheral Equipment
- + IP Network
- + Interfaces
- Engineered Values
- Emergency Services
- Service Parameters
- Access Numbers and Routing
- [Emergency Response Location](#)

Emergency Response Location

Goto ERL

ERL	State	Site Name	Location Description	Route Number	Route List Index	Access Code	Prepend Digits	Static ELIN	On-Site Notification DN
-----	-------	-----------	----------------------	--------------	------------------	-------------	----------------	-------------	-------------------------

Configure the following fields as shown in the screen below,

- **Emergency Response Location (ERL):** Enter an appropriate number.
- **Site Name (SITENAME):** Enter a descriptive site name.
- **Location Description (LOCDESC):** Enter a descriptive location name.
- **Static ELIN (LOCATOR):** Enter a valid location entry.

Rest of the fields were left at default values during compliance testing. Click on **Submit** to complete the configuration.

Input Description	Input Value
Emergency Response Location (ERL):	3 *
Site Name (SITENAME):	DevConnect
Location Description (LOCDESC):	LOC 16
Routing Method (ROUTING):	Route Number (RT)
Access Code (AC):	Null (NULL)
Prepend Digits (PREPEND):	
Static ELIN (LOCATOR):	3124124124
On-Site Notification DN (OSDN):	

Screen below shows an entry of an ERL added during compliance testing.

ERL	State	Site Name	Location Description	Route Number	Route List Index	Access Code	Prepend Digits	Static ELIN	On-Site Notification DN
3	ENL	DEVCONNECT	LOC 16					3124124124	

Note: Genesis GenSwitch service will collect the above information using **PRT ERL** command in overlay **LD 117** at a scheduled time or on demand and use this information to populate the required fields for location identification during an emergency call.

6. Configure Genesis GenAlert Solution

It is assumed that the GenAlert software has been installed, configured, and is ready for the integration with Avaya Communication Server 1000. 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 Server 1000.

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 left is the Genesis logo with the tagline "UNIFIED SOLUTIONS". 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" button, a message box stating "Please login for system access.", and a form with "Username:" and "Password:" labels, two input fields, and a "Login" button. The Genesis logo and "SYSTEMS CORPORATION" are at the bottom left, and the copyright notice "Copyright © 2015 Genesis Systems Corporation" is at the bottom right.

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 displays 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 tree icon. The background features a bridge over water. A navigation bar contains the following items: MACs, Call Accounting, Directory, Traffic, ACD, 911 (highlighted), and Fraud. Below the navigation bar, the current site is identified as 'Site 001 - AVAYA DEVCONNECT LAB - CS1000'. A welcome message reads: 'Welcome admin. The current server date is Thursday, April 09, 2015 3:12:11 PM'. On the left, a sidebar menu includes 'Change Site | Logout', 'Site Selection', and 'Administration' with sub-items: 'Change password', 'Manage user accounts', and 'Logout'. The main content area is titled 'Select a site to access:' and contains two radio button options: '001 - AVAYA DEVCONNECT LAB - CS1000' (which is selected and highlighted with a red box) and '002 - AVAYA DEVCONNECT LAB - IP OFFICE'. At the bottom left is the Genesis Systems Corporation logo. At the bottom right, the copyright notice reads: '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 001 - AVAYA DEVCONNECT LAB - CS1000

▸ 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 CS1000 switch

Action Plan

Contact List

Email Settings

Reports and Listings

Serial Connection

GCOM Direct connection

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 Communication Server 1000 to monitor for SNMP traps. During compliance testing only one Communication Server 1000 was monitored.

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

Genesis
UNIFIED SOLUTIONS

MACs Call Accounting Directory Traffic ACD 911 Fraud

Site 001 - AVAYA DEVCONNECT LAB - CS1000

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

PBX Connection method:

SNMP connection (IP Office, CS1000)
 Serial port capture (Meridian)
 Telnet connection (serial to IP, Avaya CM)
 Avaya IP Office DevLink
 Duplicate of an existing GCOM connection

Site name: AVAYA DEVCONNECT LAB - CS1000

Gcom location: localhost:7840 ('localhost:7840' is default)

SNMP Settings:

SNMP port: 162

PBX Settings: (Required for filtering SNMP data in multi-site installations)

PBX IP address: 10.10.97.78 (separate multiple IPs with commas)

Cancel Help Save

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 001 - AVAYA DEVCONNECT LAB - CS1000

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: avayadew@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: avayadew@buyge

SMTP password:

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 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 menu are visible. The main content area is titled 'Site 001 - AVAYA DEVCONNECT LAB - CS1000'. On the left, a sidebar menu shows 'System Maintenance' > 'Update contact list' highlighted. The main panel, 'Distribution list settings', shows a list named 'Emergency Mail List' with two members: 'test@avaya.com' (selected) and '6131234567@msg.tel.com'. Below the list is a 'New email address' input field and an 'Add to list' button. At the bottom, there are 'Cancel', 'Help', and 'Save' buttons. The Genesis logo is also present at the bottom left of the page.

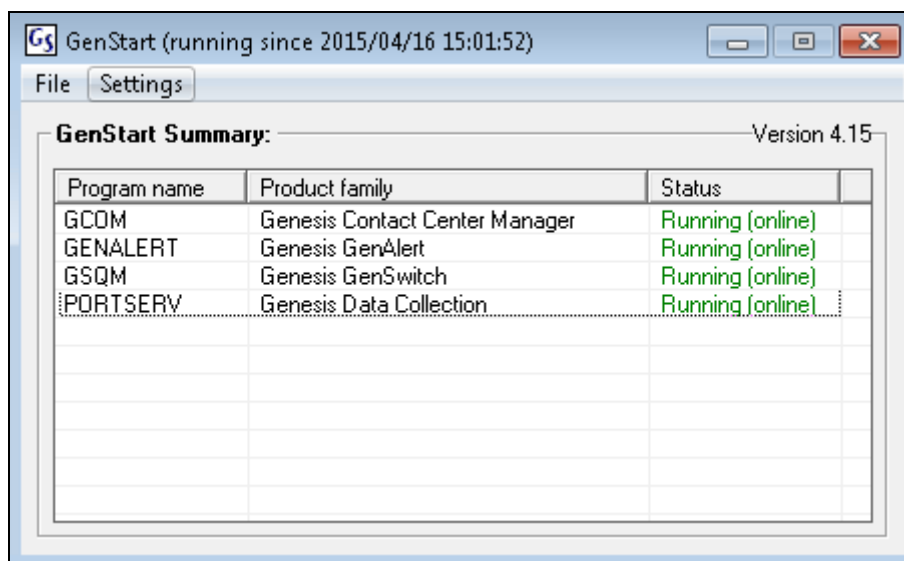
7. Verification Steps

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

7.1. Verify Genesis Services

Verify that the Genesis Contact Center Manager (**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.

Also verify that Genesis GenSwitch (**GSQM**) and Genesis Data Collection (**PORTSERV**) services are online and running. These services are required to collect the ERL information that is used for location identification.

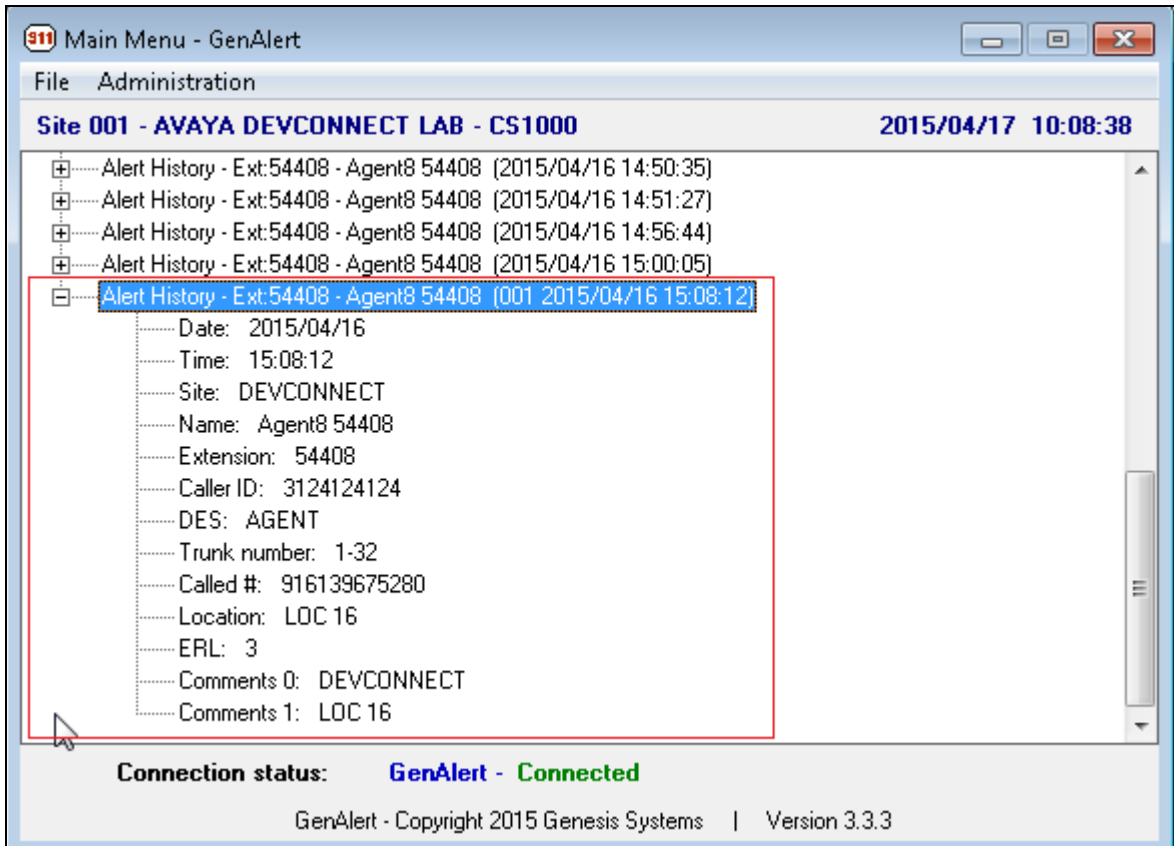


The screenshot shows the GenStart application window. The title bar reads "Gs GenStart (running since 2015/04/16 15:01:52)". The menu bar includes "File" and "Settings". The main content area is titled "GenStart Summary: Version 4.15" and contains a table with the following data:

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

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 Communication Server 1000 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] *NN43001-613, 05.03 Communication Server 1000 Emergency Services Access Fundamentals.*

[2] *NN43001-116, 05.16 Communication Server 1000 Unified Communications Management Common Services Fundamentals.*

[3] *Software Input Output Reference — Administration Avaya Communication Server 1000 7.6 NN43001-611.*

[4] *NN43001-719, 05.02 Communication Server 1000 Fault Management – SNMP.*

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