AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring eTelemetry LENS-N High Availability (HA) Version 1.4.14 with Avaya Communication Server 1000 Emergency Services Release 7.5 – Issue 1.0

Abstract

These Application Notes describe a solution comprised of Avaya Communication Server 1000 Release 7.5 and the eTelemetry LENS-N High Availability (HA) Solution. During the compliance testing, the LENS-N HA Solution was able to operate as an on-site notification of the Avaya Communication Server 1000 Release 7.5 emergency system.

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 provide detailed configurations of Avaya Communication Server 1000 Emergency Service Release 7.5 (hereafter referred to as Avaya CS1000) and eTelemetry LENS-N Solution (hereafter referred to as LENS). LENS (Locate911 Emergency Notification System) is a network appliance used to receive SNMP traps from CS1000 system when emergency 911 calls are made by the CS1000 telephones. LENS will inform on-site personnel that a 911 call has been placed and provides accurate location information. The 911 notifications are sent using eTelemetry's Windows-based LENS Alert Agent, and can also be transmitted via email and/or SMS to multiple devices.

2. General Test Approach and Test Results

This section describes the general test approach used to verify the interoperability of the eTelemetry LENS-N Solution with the Avaya CS1000 Emergency Service Release 7.5. This section also covers the test results.

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

2.1. Interoperability Compliance Testing

The general test approach was to verify the integration of the Locate911 Solution with the Emergency Service on the Avaya CS1000. Verifying the failover mechanism of the LENS-N HA system to ensure the secondary LENS server can take over and resume operation as if it is a primary server. Various emergency calls were placed from Avaya CS1000 IP telephones to an emergency number to verify the events were properly logged by the LENS in a timely manner. LENS will in turn generate the alert notification via the Windows Alert Agent which is an eTelemetry Windows application installed on a Windows server. The IP phones were moved between different switches and ports within the network to verify that the LENS-N solution accurately report the information, in the notification, of the emergency call in term of caller ID, extension, date and time, site, location and Emergency Response Location. 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 eTelemetry LENS-N HA Solution successfully passed compliance testing.

2.3. Supports

For technical support on eTelemetry LENS-N HA, please contact eTelemetry technical support at:

- Phone: 1–888–266–6513
- Email: support@etelemetry.com
- Web: http://www.etelemetry.com/support.aspx

3. Reference Configuration

Figure 1 below illustrates the reference configuration used during compliance testing. The eTelemetry LENS-N server management port (TLAN) is connecting to the CS1000 via network route layer 2 switch.
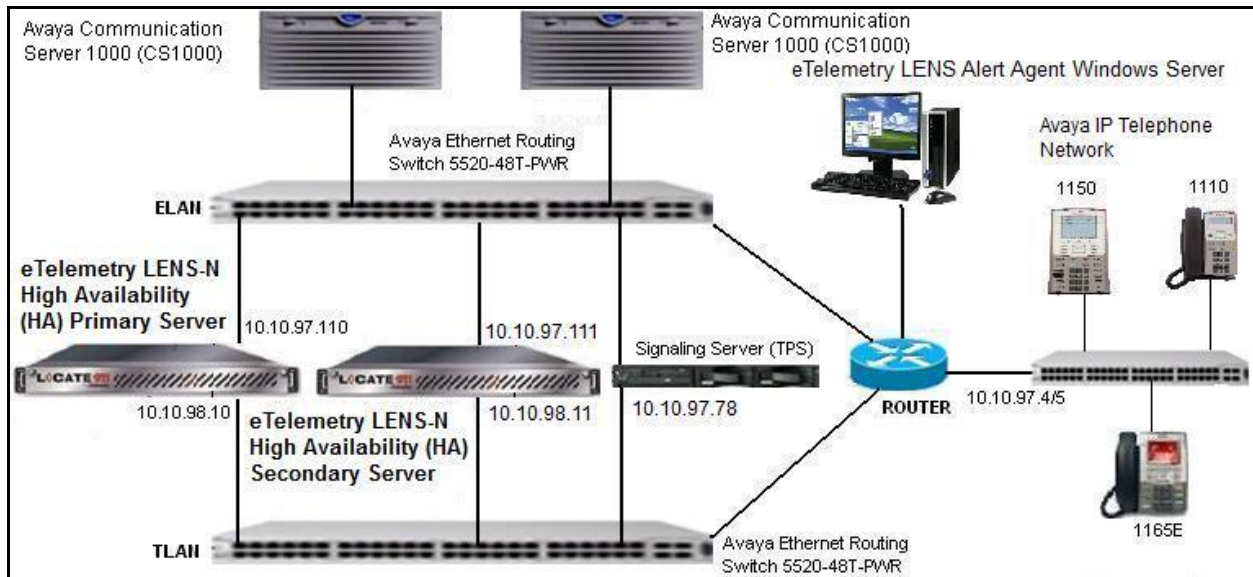

Figure 1: eTelemetry LENS-N HA System and Avaya Communication Server 1000 Emergency Service

QT; Reviewed:
SPOC 11/10/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

4 of 24
LENS-NHA-CS1K75

4. Equipment and Software Validated

Equipment	Software Version
Avaya CS1000E	Call Server: 7.50Q Signaling Server: 7.50.17
Avaya CS1000 IP Phones	1110, 1165E, 1150
eTelemetry LENS-N HA Servers	1.4.14
eTelemetry LENS-N Alert Agent for Window	1.5.4.1
Avaya Ethernet Routing Switch 5520-48T-PWR	FW: 6.0.0.13 SW: v6.2.2.024

The following packages must be enabled in the keycode file in order for the Emergency Service Access feature to operate successfully.

Feature Packaging Requirement

Package	Mnemonic	Name	Description
329	ESA	Emergency Services Access	Defines an emergency number as being dial-able without a prefix. Recognizes the emergency call and provides special treatment and route to CAMA, PRI or other trunks. Provides flexible ANI number translation for DID numbers and sends out the ANI with the call to enable the PSAP to look up the caller. Includes Enhanced Routing functionality, Multiple ESDNs, and Misdial Prevention.
330	ESA_ SUPP	ESA Supplementary	Provides networking support by routing node-to-node ANI info for forwarding to a PSAP. Converts incoming ISDN to CAMA tandem which allows CLID forwarding via out-pulsed CAMA. Also provides On-Site-Notification (OSN) so that the customer staff is aware of the call. This includes OSN phones per ERL.
331	ESA_CLMP	ESA Calling Number Mapping	Provides flexible ANI number translation for non-DID numbers (i.e. to translate non-DID numbers to DID numbers). This includes Dynamic ELIN functionality.

5. Configure the Avaya CS1000 - Emergency Service Access (ESA)

This section describes the steps to configure Emergency Service Access (ESA) on an Avaya CS1000 system using Element Manager Web portal. Repeat these steps for other Avaya CS1000 systems in the Avaya CS1000 network. For more information, see [1].

5.1. Log in to Unified Communications Management (UCM) and Element Manager (EM)

Use a web browser to launch the Avaya CS1000 UCM web portal at http://<IP Address or FQDN> where <IP address or FQDN> is the UCM Framework IP address or FQDN for UCM server. Login with the username/password which was defined during the primary security server configuration. For more information, see [2].

- On the **Elements** page of Unified Communications Management, under the **Element Name** column, click the server name to navigate to Element Manager for that server.

QT; Reviewed:
SPOC 11/10/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

6 of 24
LENS-NHA-CS1K75

The Avaya CS1000 Element Manager (EM) page appears as shown.

5.2. ESA Service Parameters Configuration

On the EM page, navigate to **System → Emergency Services → Service Parameters**. The
Service Parameters page appears below.

- On the **Service Parameters** page, from the **Location Information Services (LIS)** list,
  select **External Discovery Manager (EXT/DM)**.
- Enable the **Reuse oldest ELIN during overflow (DYNAMIC_ELIN_REUSE)**
  parameter.
- Click **Submit**.
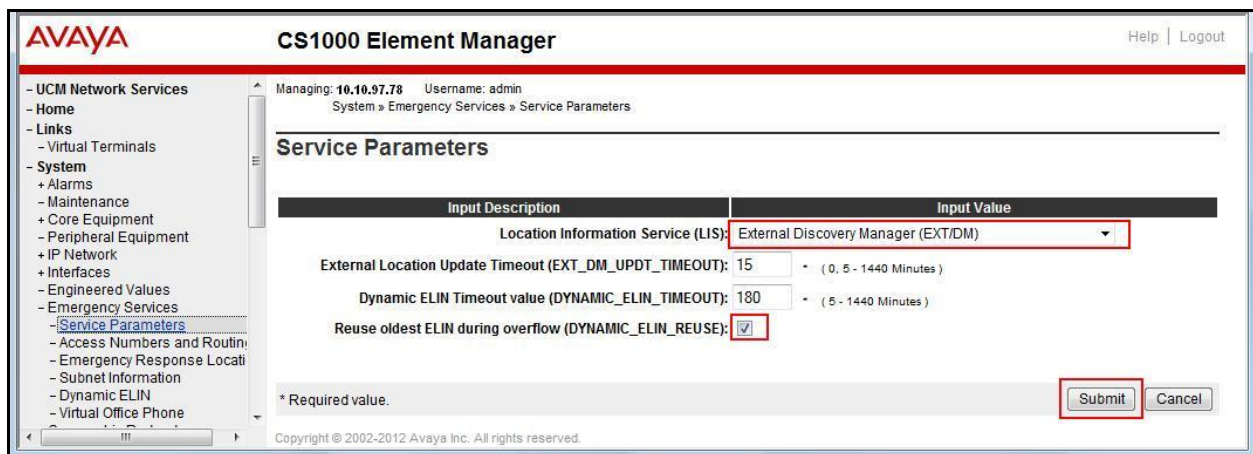
5.3. Access Numbers and Routing Configuration

On the EM page, navigate to **System → Emergency Services → Access Numbers and Routing**. If there was no ESA Access Numbers and Routing configured, the **Add Customer x Emergency Services Directory Number** page appears as shown in figure below.

- On the **Add Customer x Emergency Services Directory Number** page, enter a directory number in the **Directory Number** text box.
- Enter directing digits in the **Directing Digits** text box.
- Enter Default Calling Number in the **Default Calling Number** text box.
- Enter a local extension DN, which will be alerted when an emergency call is coming, for **On-Site Notification System DN** text box.
- At the **Routing Method** attribute, select **Route List Index** and choose the appropriate value available from the pull down menu.
- Check the **Misdial Prevention** box.
- 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**.

5.4. Emergency Response Location (ERL) Configuration

On the EM page, navigate to **System → Emergency Services → Emergency Response Location**. If there was no ERL created, a dialog appears asking for your confirmation to create a new ERL. Click **OK**. The **Add Emergency Response Location** page appears (not shown).

- On the **Add Emergency Response Location** page, enter ERL number in the **Emergency Response Location (ERL)** text box.
- Enter the site name in the **Site Name (SITENAME)** text box.
- Enter the location description in the **Location Description (LOCDESC)** text box.
- From the **Routing Method** pull down list, select a routing method and enter corresponding **route number/route list index** in the next text box as shown.
- Enter the **Static ELIN (LOCATOR)** number in textbox.
- Click **Submit**.

5.5. Configure the Avaya CS1000 - Alarms

This section describes the steps to configure Alarms on the Avaya CS1000 system using SNMP Profile Manager. This is to generate alarms when 911 calls are made and sending the alarms to the management port of Locate911 server for trap/alert. Repeat these steps for other Avaya CS1000 systems in the Avaya CS1000 network. For more information, see [3].

5.5.1. Log in to Unified Communications Management (UCM) and SNMP Profile Manager

Refer to **Section 5.1** to see how to login into the Unified Communications Management (UCM). From the UCM Home page, navigate to **Network → CS1000 Services → SNMP Profiles**. The **SNMP Profile Manager** page appears as shown.
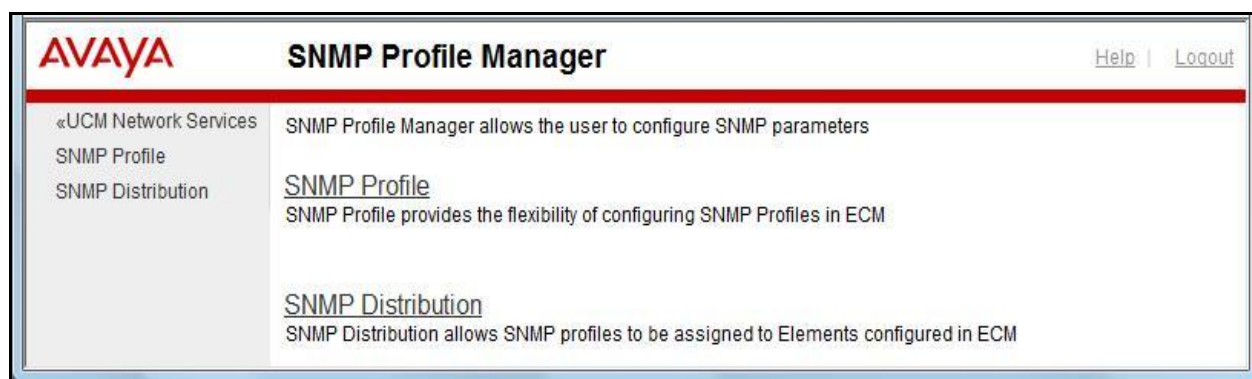
5.5.2. Create a New SNMP Profile

On the **SNMP Profile Manager** page, navigate to **SNMP Profile**. The **SNMP Profiles** page appears as shown below. On the **SNMP Profiles** page, click **Add**.
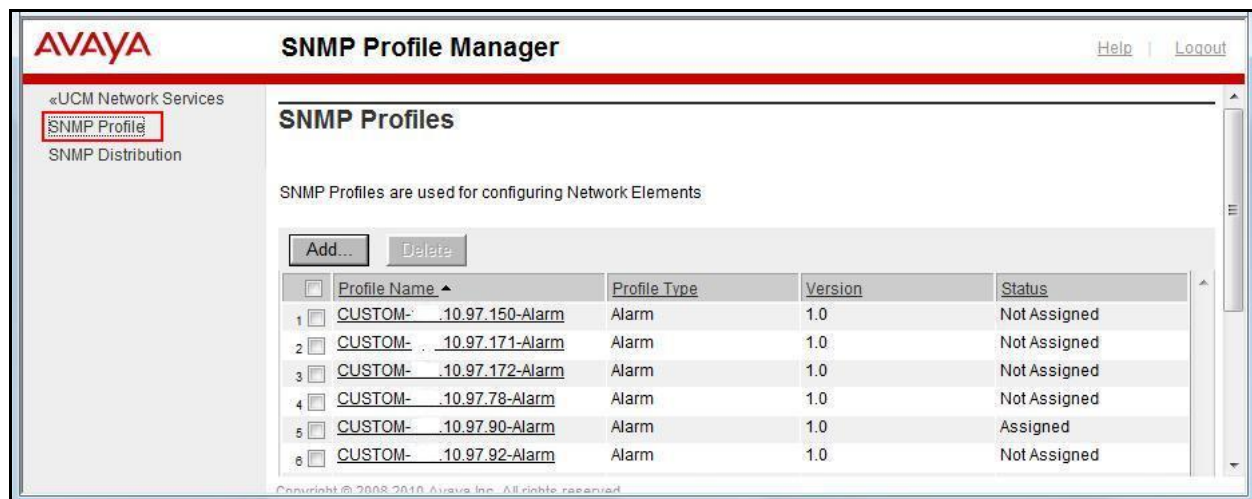
The **New SNMP Profile** page appears.
- Enter a name in the **Profile Name** text box.
- From the **Profile Type** list, select **ALARM** (not shown).
- Additional parameters appear after a profile type is selected. Enter a trap community in the **Trap Community** text box. The string is "public" (without quotes) by default.
- Ensure that the **Option** check box is checked to enable trap sending.
- Enter Locate911 Management IP addresses and ports (port 162 by default) in the **Trap Destinations**.
- Click **Save**.

Note: For Locate911 HA configuration, the **Trap Destination** can be programmed to send SNMP trap to secondary **IP address2** and **port2**.

5.5.3. Assign an SNMP Profile to a Network Element.

On the **SNMP Profile Manager** page, navigate to **SNMP Distribution**. The **SNMP Target Selection** page is as show below.

- Select the element that will be assigned to the newly created SNMP profile.
- Click **Next**.
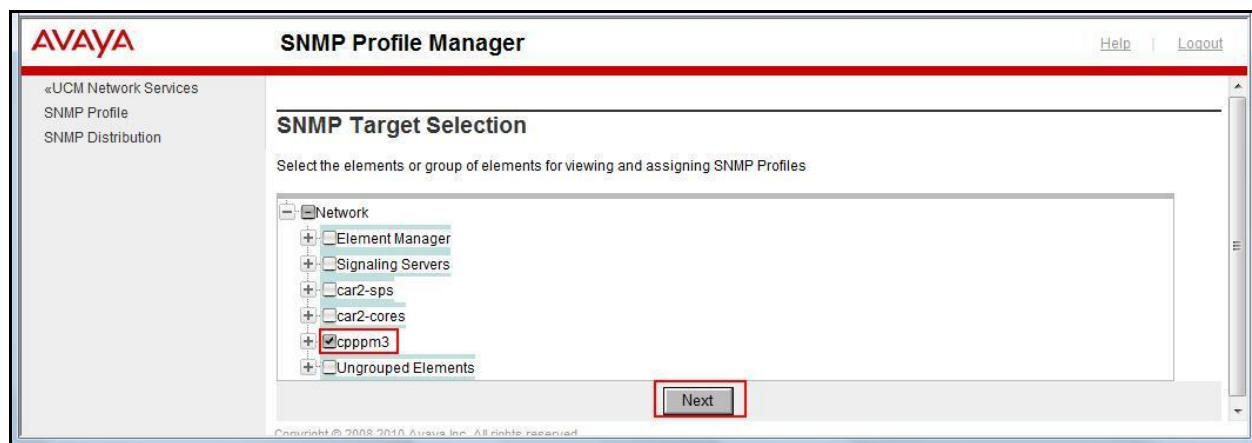
The **SNMP Profile Distribution** page appears as shown below.

- Select a Network Element (ELAN IP address of Avaya CS1000 call server).
- Click the **Assign** button.
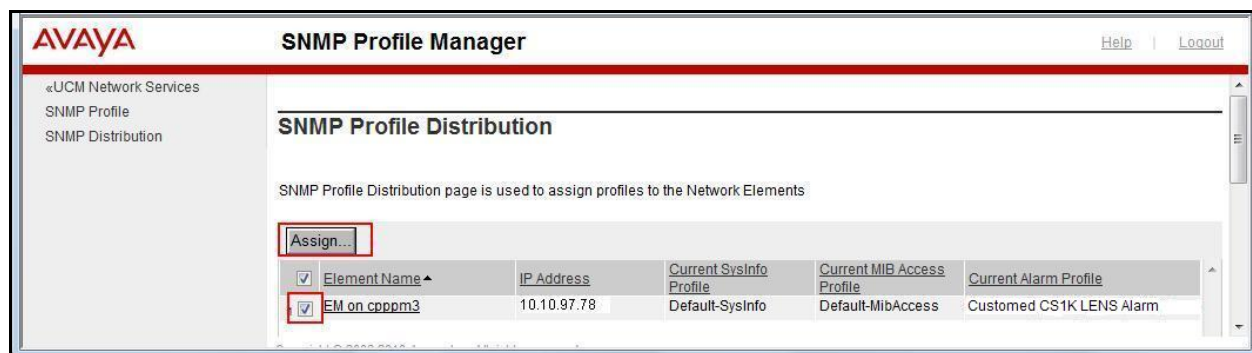
The **SNMP Profile Distribution Details** page appears as shown below.
- On the **SNMP Profile Distribution Details** page, from the **Alarm Profile** list, select the profile created in **Section 5.5.2**.
- Click **Save**.

After assigning the newly created SNMP profile to the network element, the newly created profile will be shown in the **SNMP Profile Manager** under the **SNMP Profiles** page as shown below.

QT; Reviewed:
SPOC 11/10/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

13 of 24
LENS-NHA-CS1K75

6. LENS-N HA Configuration

It is assumed that the LENS-N HA server has been installed and properly configured ready for the integration with Avaya CS1000. Please refer to the LENS-N HA Users Guide documentation which can be obtained by contacting eTelemetry. This section below only provides the set-up to configure the LENS-N HA to interoperate with Avaya CS1000.

6.1. Login to web management console of Locate 911

Access the LENSN HA services web interface by opening a web browser and entering the following URL; **http://<Mangerment Services IPAddress**>. Enter appropriate information below:

- Enter the **User** name.
- Enter assigned **Password.**
- Check the checkbox of **I accept the terms in the license agreement**.
- Click on **Login** button.

After login, the LENS-N HA server displays the **Control Panel** page.

QT; Reviewed:
SPOC 11/10/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

15 of 24
LENS-NHA-CS1K75

6.2. Configure Avaya Settings

Navigate to **Control Panel → Management Consoles → Manage Avaya Settings**. The following fields should be filled in as follows:

- **OSN Map Link Label** is entered as Emergency Map Link
- **OSN Map Link** is the URL to an external map for a specific ERL; http://www.company.com/maps.php
- **ISSS Mode of Operation** is turned off in this testing.

6.3. Configure LENS-N HA Redundancy

Navigate to **Control Panel → Management Consoles → Manage Redundancy Configuration**. Set the parameters as follows.

- **Secondary IP** should be the IP address of the secondary server.
- **Service IP** is the management IP address of the server cluster.
- Enter **Pingable Device #1 IP** address to verify network connectivity of the HA configuration.
- Enter **Pingable Device #2 IP** address to verify network connectivity of the HA configuration.
- **Poll Cycle** is set to **5**.
- **Maximum Ping Failures** is set to **3**.
- **Auto Toggle Back** is **15** in this testing.
- Click **Commit.**

6.4. Configure LENS Alert Agent for Windows

To set up LENS Alert Agent for Windows, navigate to **Control Panel → Download eTelemetry Software → LENS Alert Agent for Windows**, to download the LENS Alert Agent application on a Windows based server.
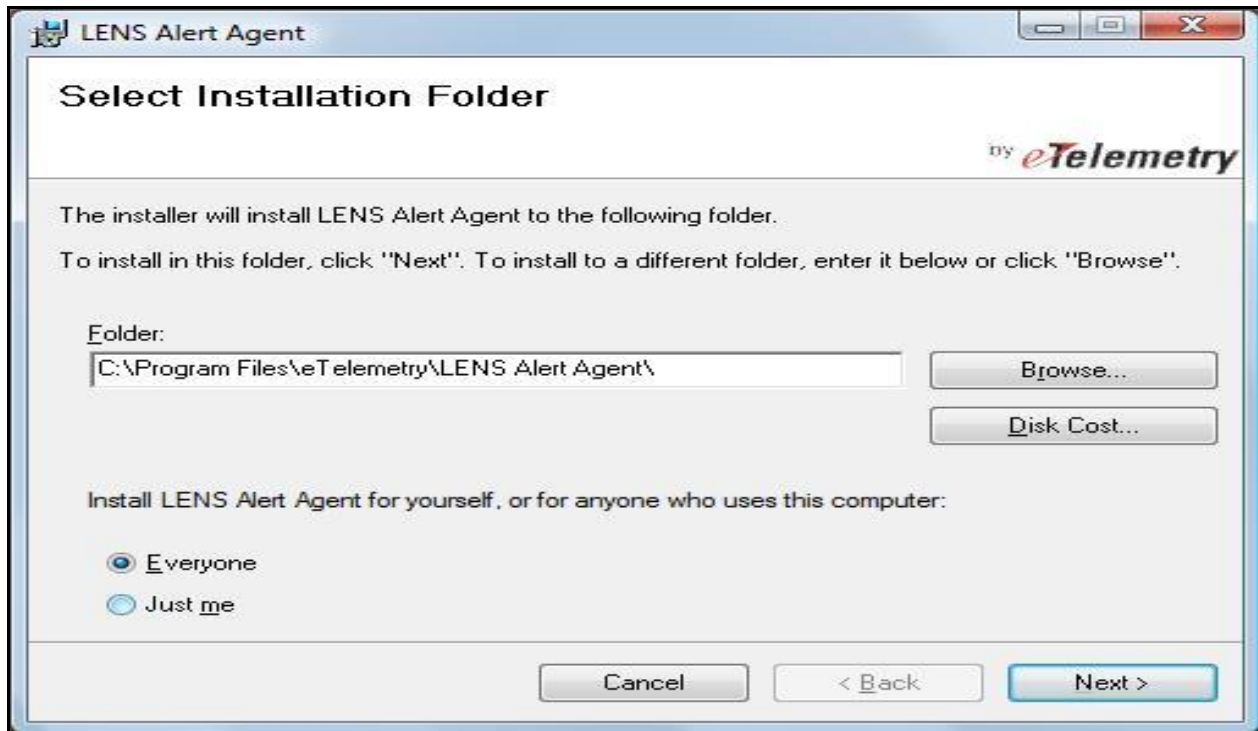
Note: For Windows server specific requirement, please contact eTelemetry for details.
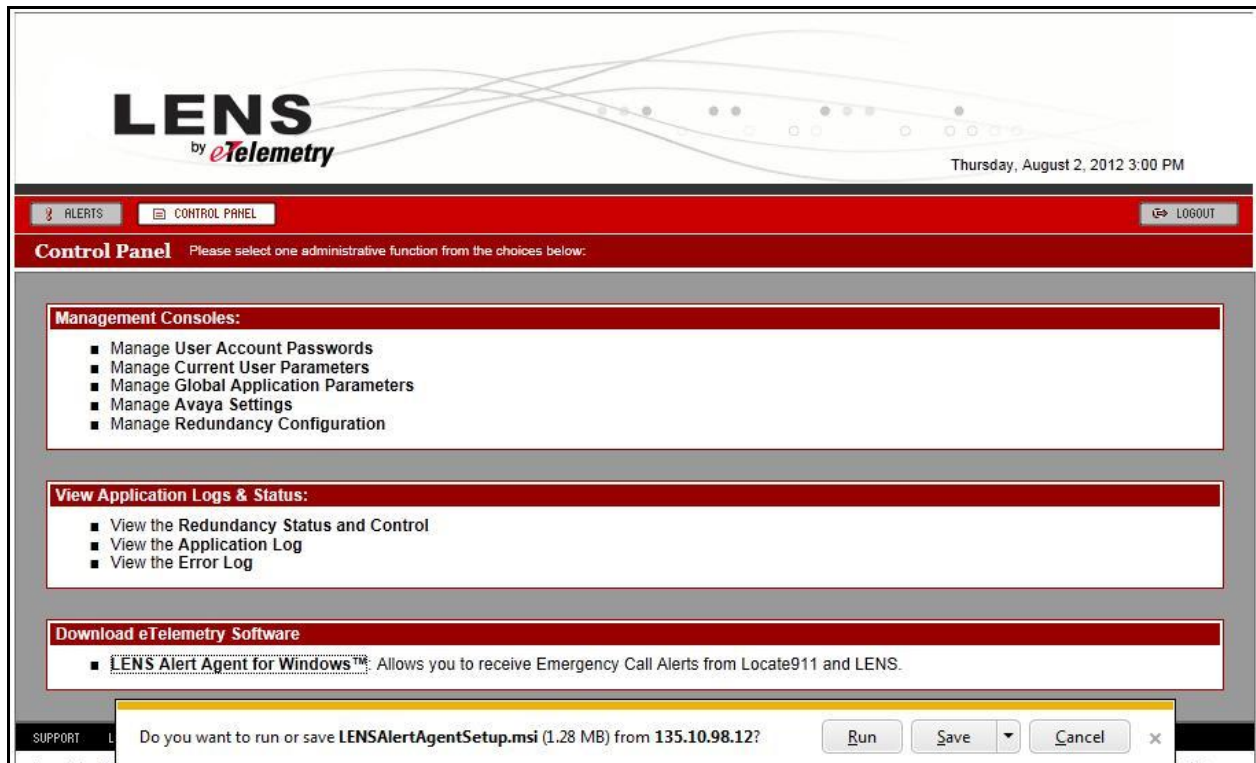
Click on **Run** to install the LENS Alert Agent application. Enter management service IP address in the **Hostname/IP address** text box.
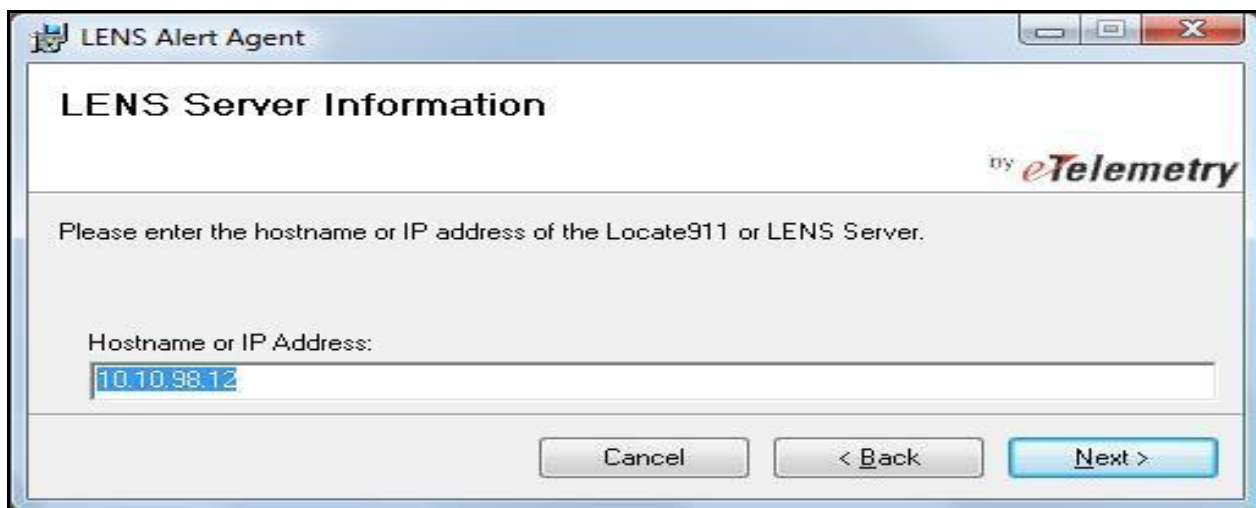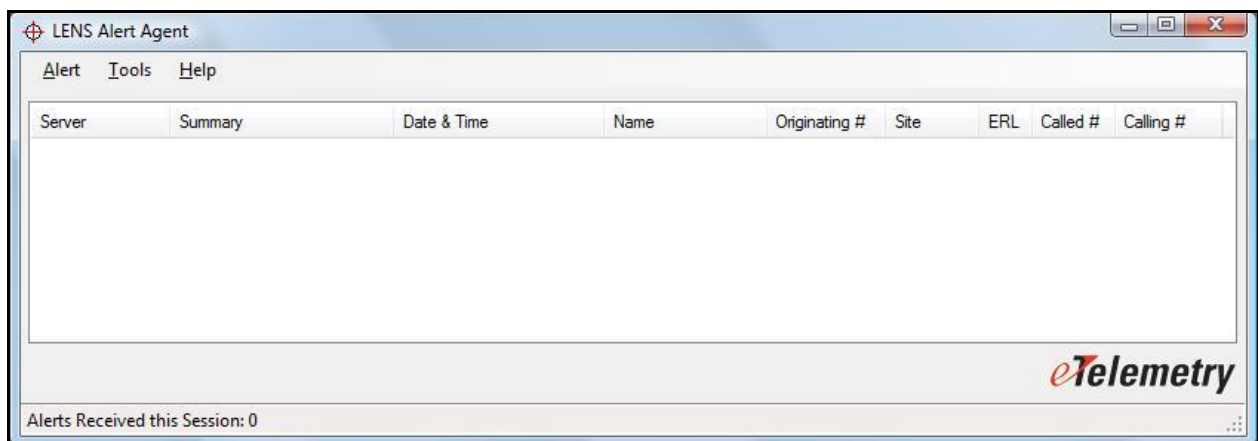
Click **Next** to choose the folder where the application can be installed.

Click **Next** to confirm the installation (not shown). Then click **Close** to finish the installation process (not shown).
The LENS Alert Agent is now running and ready to provide on-site notification when there is an emergency call made on CS1000.
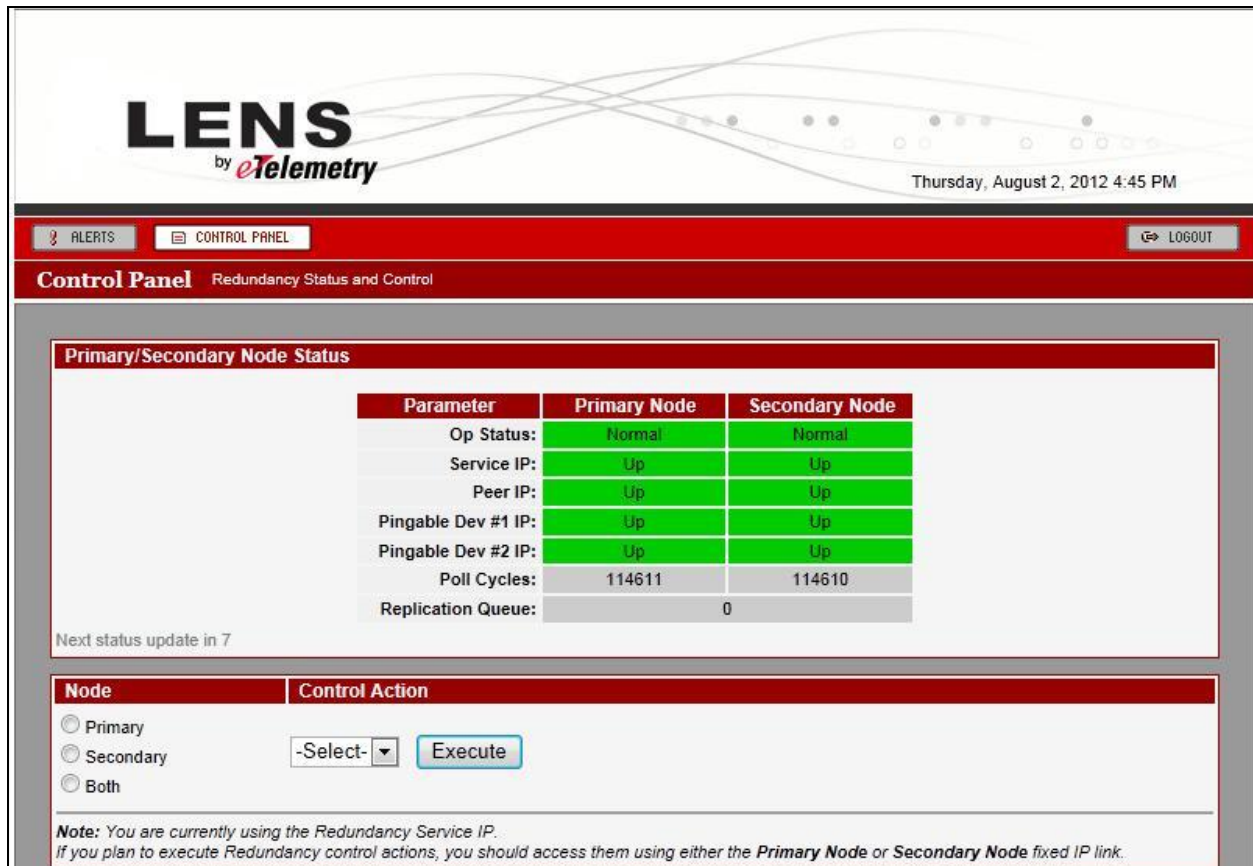
7. Verification Steps

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

7.1. Verify LENS-N HA Configuration

Navigate to **Control Panel → View Application Logs & Status → View Redundancy Status and Control**, both primary and secondary Locate911 nodes should have green display indicating that they are both up and functioning in normal operation.

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
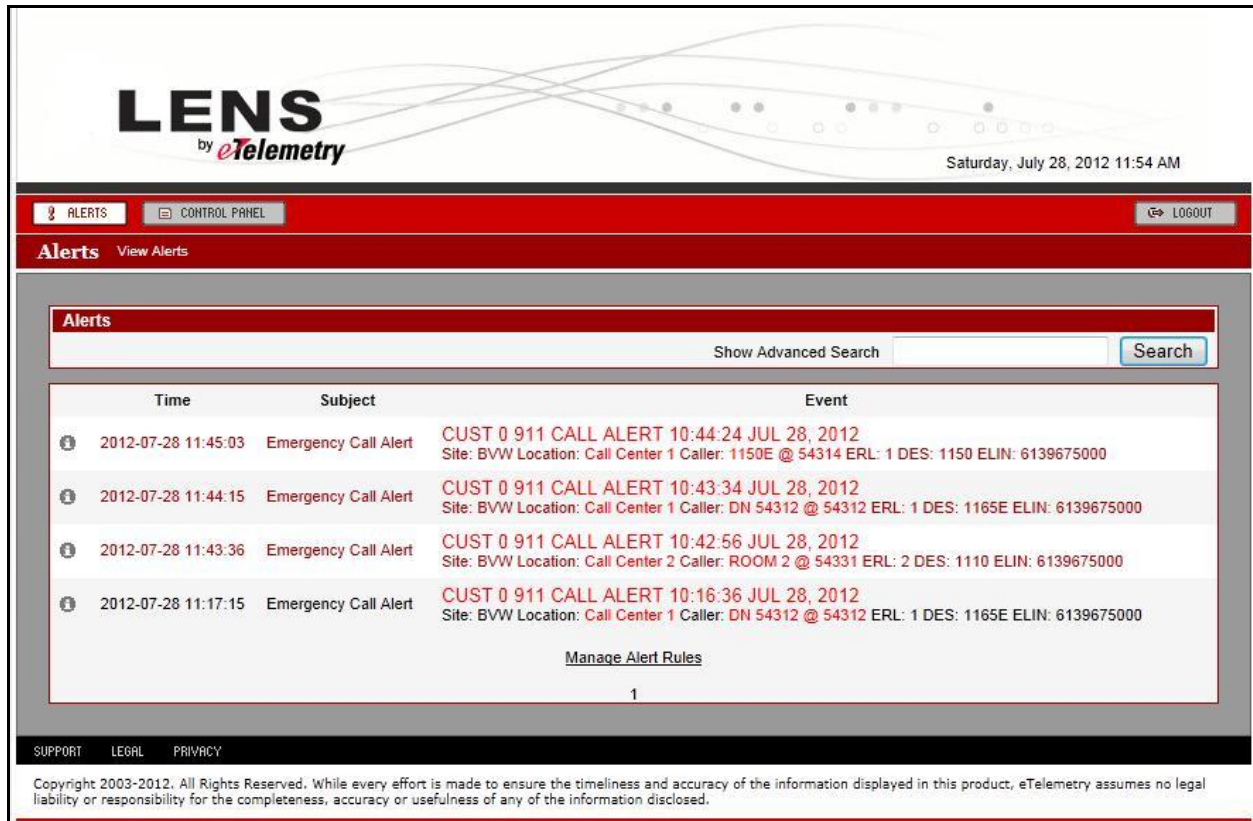
7.2. Verify 911 Call Alert on LENS Server

Making emergency 911 calls from CS1000 IP telephones, then log in to the LENS web management services interface as shown in **Section 6.1**. Navigate to **Alert** on the system toolbar. The emergency call events should be listed as shown.

7.3. Verify 911 Call Alert Notification on LENS Alert Agent Window

Making 911 emergency calls from CS1000 IP telephone, verify that there are notification alert pop-up windows being generated.
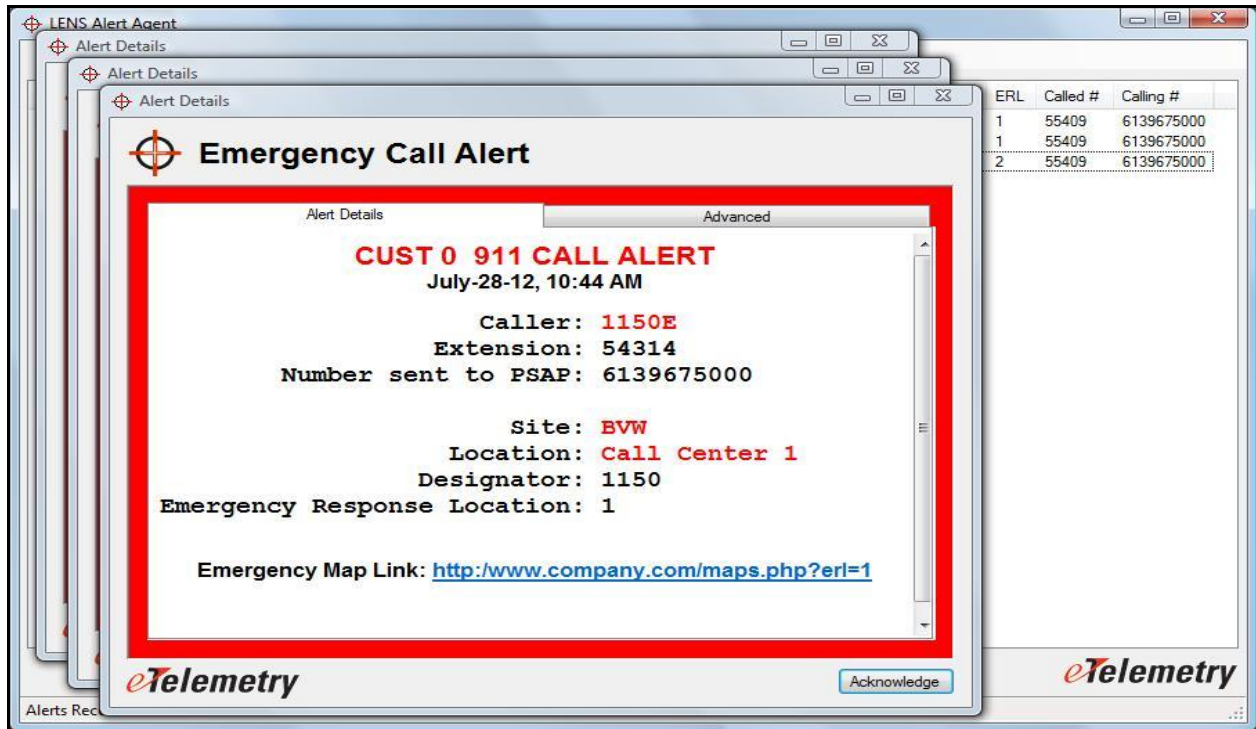
Verify that notification alerts are also generated.
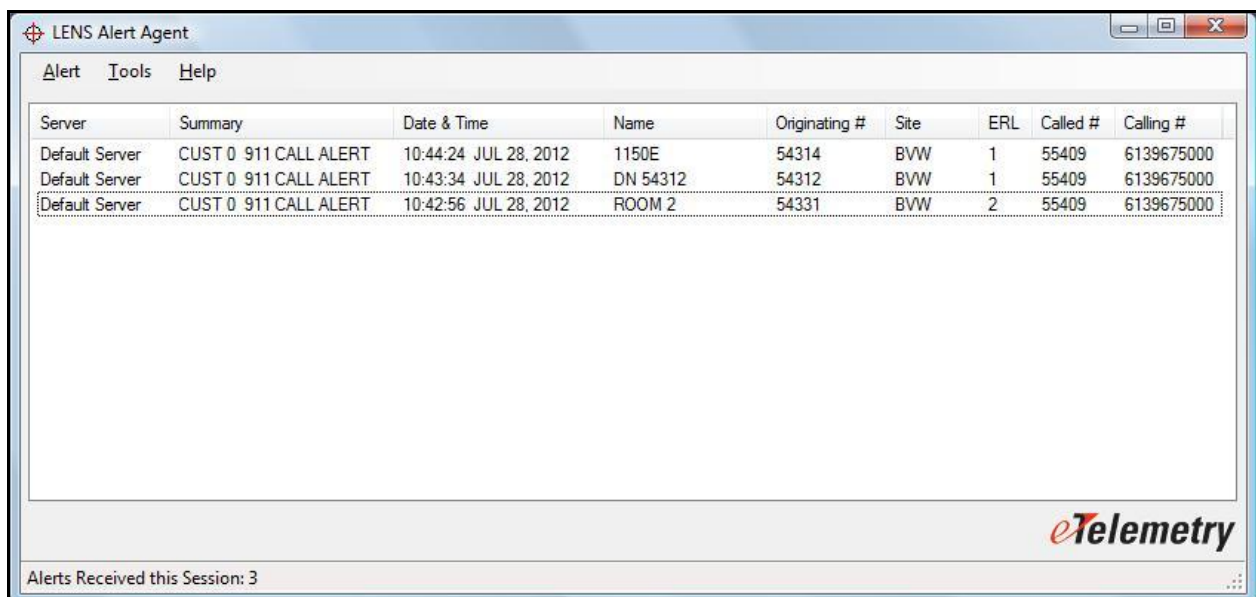
8. Conclusion

The eTelemtry LENS-N HA Solution passed the compliance testing. These Application Notes describe the procedures required for the eTelemetry LENS-N HA Solution to interoperate with Avaya Communication Server 1000 Emergency Services to support the reference configuration shown in **Figure 1**.

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] *NN43001-719, 05.02 Communication Server 1000 Fault Management - SNMP*

Product information for eTelemetry LENS-N HA products can be found at
http://www.etelemetry.com/products/locate911.aspx

©2012 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.