



Avaya Solution & Interoperability Test Lab

Application notes for Configuring RedSky E911 Manager® with Avaya™ Communication Server 1000 Release 7.6 – Issue 1.1

Abstract

These Application Notes describes a compliance-tested configuration consisting of Avaya™ Communication Server 1000 Release 7.6 and RedSky E911 Manager®. MyE911®, Emergency On-Site Notification (EON) Client, and E911 Anywhere® are also part of this Red Sky solution.

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 Avaya Communication Server 1000 Release 7.6 (hereafter referred to as CS1000) and the RedSky E911 Manager® (hereafter referred to as E911M).

MyE911®, Emergency On-Site Notification (EON) Client, and E911 Anywhere® (E911A) are also part of this Red Sky solution.

The E911M is a cloud-based or on-premise solution that acts as an External Discovery Manager (DM) of the CS1000 Emergency Service provides location information of registered endpoints to CS1000.

E911M is also responsible to keep the Automatic Location Identification (ALI) database updated. This is typically done by sending ALI data to E911A, a Redsky cloud-based solution; however traditional PS-ALI methods may also be used. ALI database is used by Public Safety Answering Point (PSAP) to search for specific address/location of CS1000 endpoint using Calling Line Identification (CLID).

Note: Every CLID must be provisioned with the E911M before it can be useful when an emergency call is made. This requires that a preconfigured CLID is provisioned for every potential emergency caller location in the environment.

The E911M provides On-Site Notification (OSN) Alerter that captures OSN records on CS1000 and provides alerts via email, text, or a “screen pop” to end users when the 911 call is made. The EON Client receives notifications from E911M and provides screen pops on a user’s computer.

MyE911® provides 911 protections to Avaya softphone users. MyE911® is installed on a user’s laptop. Every time the softphone is launched, MyE911®preempts the registration process and requires the user to identify their location to the enterprise. The user may select a location from the validated list of Corporate or Personal favorites or create a new location. Once this action is performed, the softphone is immediately released for use and the CLID has been updated with appropriate ALI data.

2. General Test Approach and Test Results

This section details the general approach to the testing, what was covered, and results of the testing. If the testing was successfully concluded but it was necessary to implement workarounds or certain non-critical features did not work, it should be noted in **Section 2.2**.

This section describes the general test approach used to verify the interoperability of the E911M with the Avaya CS1000 Emergency Service Release 7.6. There are two major components to E911, location provisioning and emergency calling.

Devices are first added and provisioned in the CS1000 then synced with E911M through a download process. E911M then runs a location discovery on devices that support it and writes

back an ERL ID to CS1000. Finally, locations are updated appropriately through E911 Anywhere® or a traditional ALI provider.

The compliance testing focused on verifying the generation of ALI records and not on the transfer of ALI records to ALI databases.

When an emergency call is placed, E911M reads OSN record on CS1000 and gets the CLID. The E911M uses this CLID information to look up a corresponding Emergency Response Location (ERL) which contains Building Name, Floor, Room and Emergency Location Information Number (ELIN) in E911M database and sends an alert email, text, or “screen pop” which can be used by security personal on site.

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 the RedSky E911 Manager® with the Emergency Service on the CS1000.

- The compliance testing focused on verifying the generation of ALI records and not on the transfer of ALI records to ALI databases.
- Calls are routed to the correct designated number and call events are logged by E911M when 911 calls were placed from CS1000 analog, digital and IP deskphones.
- When the 911 calls were made, verify an email is sent to security personal on site with following information: Customer, PBX, ELIN, Extension, Building Name, Building UID, Address and Location (Room, Floor).
- When the 911 calls were made, verify an EON is activated as on screen alert with the following information: Customer, PBX, ELIN, Extension, Building Name, Building UID, Address and Location (Room, Floor) and alert comes in the form of an audible siren.
- Change IP addresses of existing IP phones on CS1000 system, verifying that RedSky E911M can correctly identify these new IP address and update the ERL for those phones.
- Modify phone information such as ERL, Call Party Name Display (CPND), Office Data Administration System Station Designator (DES) on CS1000, perform the Call Server download on E911M, verifying consistency of phone information reported in the RedSky E911 Manager to CS1000.
- Verify consistency of ERL table updated and listed on CS1000 to E911M.
- When Avaya softphone user starts to launch their softphone, MyE911 will pop-up to ask softphone user select a valid location listed on the screen which according to their current location before let the login process of Avaya softphone continue.

2.2. Test Results

The RedSky E911 Manager® Solution successfully passed compliance testing. RedSky E911 Manager® was able to retrieve station emergency numbering and location information from Avaya Communication Server 1000. The objectives of Section 2.1 were verified with following observations:

- Need to allow extra time for E911M to complete processing of downloaded data. Although log event shows that the download is completed, E911M downloaded data processing may still be in progress.
- E911M only updates ERL value on IP phone which has IP address in the previously configured IP Range. If an ERL is manually assigned for IP phones on CS1000 and the IP range on E911M does not cover this phone, ERL will not be updated nor displayed on E911M for this phone. As a result, the ERL shown in alert email for this phone is UNKNOWN.
- When a softphone user's location has been changed on myE911, this location is updated on E911M database but not on CS1000. The CS1000 administrator needs to manually start the download process on E911M to have the new location/ERL updated on CS1000.
- When user receives an alert for 911 call, time shown in the alert is the time on E911M server not the CS1000 time.

2.3. Supports

For technical support on the RedSky E911 Manager solution, contact at:

- Web: <http://www.redsky911.com/>
- Email: support@redskytech.com

3. Reference Configuration

Figure 1 below illustrates the reference configuration used during compliance testing. The RedSky E911 Manager Solution was installed on CentOS Release 6.2 Linux server.

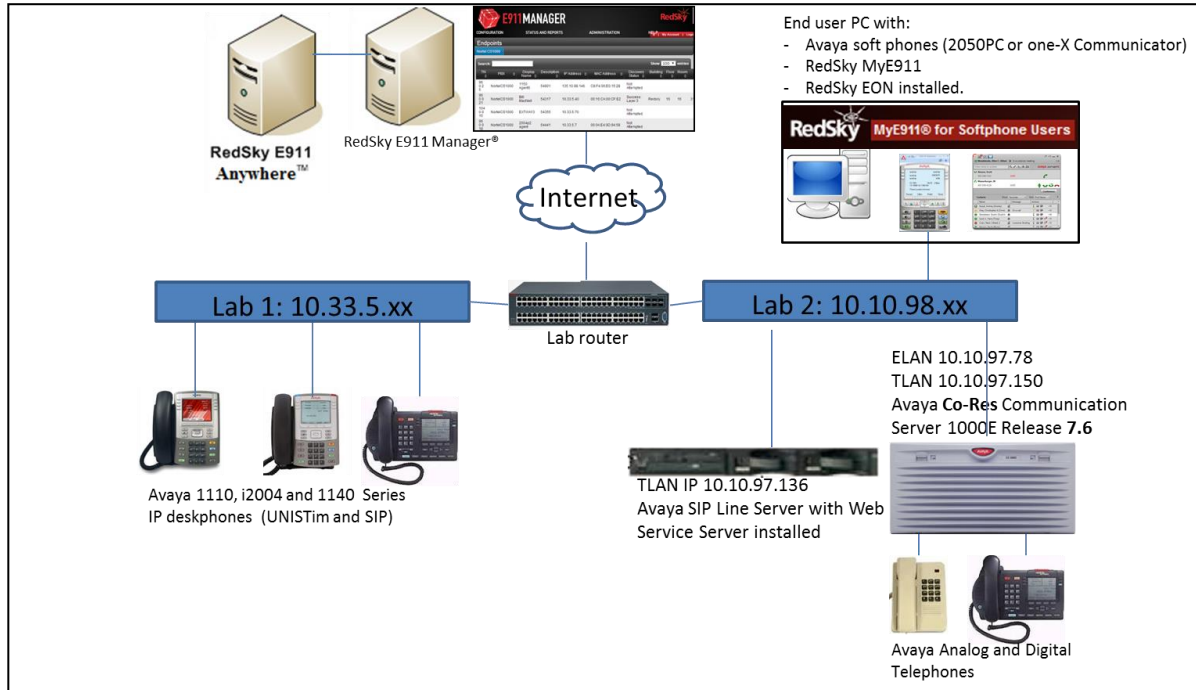


Figure 1: RedSky E911 Manager Solution and Avaya Communication Server 1000 Emergency Service

4. Equipment and Software Validated

Equipment	Software Version
Avaya Communication Server 1000 Co-Res	Call Server (CPPM): 7.65 P+ 4121
Avaya SIP Line Server	Signaling Server (CPPM): 7.65.16
Avaya Softphones 2050PC Avaya one-X Communicator	Release 3.4 CS6.1.1.02
Avaya Communication Server 1000 IP Desk phones 1110 1165E 2004P1	0623C8Q 0626C8V 0602B76
CentOS Linux server	Release 6.2
RedSky E911 Manager®	6.3.5
RedSky MyE911® for Softphone	Server version 17559 Client version 17024
RedSky Emergency On-Site Notification (EON) Client	17559
RedSky E911 Anywhere®	6.3.5

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 customer staffs are 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.
337	ESA_EXTERNAL_DM	ESA External DM Interface	Allows the use of an external Discover Manager (and corresponding LIS) to provide advanced location determination for IP phones. Additionally, the External Discovery Manager is charged separately.

5. Configure Avaya Communication Server 1000

This assumes that CS1000 is installed and in operational state.

This section will describe steps to configure:

- Emergency Service Access to route the call to simulated PSAP,
- SNMP to generate alarms when 911 calls are made and sending the alarms to the E911M server.
- User for E911M to access and make SOAP request to the CS1000.

5.1. Configure Emergency Service Access (ESA) on CS1000

This section describes the steps to configure Emergency Service Access (ESA) on a CS1000 system using Element Manager Web portal. The values used in this guide may be unique to the example shown. User will have to use values that are unique to their site, where this solution is being deployed e.g. site's IP address, extension numbers and etc.

This section describes steps to create Emergency Services Directory Numbers (ESDN), and how to dial it with and without dial Access Code (AC). No On-Site Notification station is configured in ESA. During compliance test, office phone **613-967-5280** is use as simulated PSAP number. When user dials 911, the call is routed to this office phone.

Note: It is importance that while covering the 911 ESDN programming, make sure to cover the AC1/AC2 + 911 as well. Example AC1 is 9 and AC 2 is 6. If 9-911 (or 6+911) is not configured properly to 911, there could have different operations and results between 911 and 9-911. This is one of the most common configuration errors in the field. Make sure comparing the operation of 911 and 9-911 having the same outcome will confirm proper configuration.

For more information about multiple ESDN, dial ESDN with access code. See **Emergency Service Access Fundamental** document listed in reference **Section 9**.

The following ESA configuration was configured during compliance test:

- Verify OSN is configured in Teletype (TTY)
- Configure Service Parameter.
- Configure Digit Manipulation Index.
- Configure Route List Index.
- Configure Emergency Service Directory Numbers.
- Configure AC + ESDN

5.1.1. Verify OSN is configured in TTY

The Teletype (TTY) output message type, OSN, is used for printing OSN system messages. E911M will monitor TTY output from the CS1000 for emergency calls. Using LD 22 to verify that **OSN** is configured in **USER** filed of TTY as shown below:

```
REQ PRT
TYPE ADAN TTY 11

ADAN      TTY 11

USER MTC SCH BUG OSN
...
REQ ****
```

5.1.2. Configure Service Parameter

This section describes steps to logon CS1000 Element Manager and steps to configure the CS1000 to use an External Discovery Manager DM interfaces to keep the location data of an IP telephone up to date.

In IE launch System Manager at <http://<IP Address or FQDN>> where <IP address or FQDN> is the IP address or FQDN of System Manager, login with the appropriated credential. In System Manager, click on **Communication Server 1000** as shown below:

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at April 11, 2014 10:25 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Users	Elements	Services
Administrators Manage Administrative Users	Communication Manager Manage Communication Manager 5.2 and higher elements	Backup and Restore Backup and restore System Manager database
Directory Synchronization Synchronize users with the enterprise directory	Communication Server 1000 Manage Communication Server 1000 elements	Bulk Import and Export Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
Groups & Roles Manage groups, roles and assign roles to users	Conferencing Manage Conferencing Multimedia Server objects	Configurations Manage system wide configurations
User Management Manage users, shared user	IP Office	

In **Elements** page, click the server name to navigate to Element Manager for that server, as show below, **EM on sip175** is selected.

At the bottom, when user moves the mouse over to **EM on sip175**, it shows the **Security ObjectID of CS1000** as highlighted in screenshot below. This information is needed when create Call Server on E911M in **Section 6.3**.

Avaya Aura® System Manager 6.3

Host Name: devsmgr.bvwdev.com User Name: admin

Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

Search Reset

Element Name	Element Type	Release	Address	Description
devsmgr.bvwdev.com (primary)	Base OS	7.6	10.10.97.196	Base OS element.
EM on sip175	CS1000	7.6	10.10.97.78	New element.
cpm3.bvwdev.com (member)	Linux Base	7.6	10.10.97.150	Base OS element.
sip175.bvwdev.com (member)	Linux Base	7.6	10.10.97.136	Base OS element.

https://sip175.bvwdev.com/emWeb_6-0/SECURE_OBJECT_ID/com.nortel.ems.CS1000/600810cd-b115-11e2-b01b-f1677c8c77f8/index.jsp

The **CS1000 Element Manager** page launch as shown below:

CS1000 Element Manager

Managing: 10.10.97.78 Username: admin

System Overview

System Overview

IP Address: 10.10.97.78

Type: Avaya Communication Server 1000E CPPM Linux

Version: 4121

Release: 765 P +

On the **CS100 Element Manager** page, navigate to **System → Emergency Services → Service Parameters**. The **Service Parameters** page appears as shown below.

On the **Service Parameters** page fill the form as shown:

- **Location Information Services (LIS):** select **External Discovery Manager (EXT/DM)**.
- Leave other fields as default.

Click **Submit** to save changes.

Input Description	Input Value
Location Information Service (LIS):	External Discovery Manager (EXT/DM)
External Location Update Timeout (EXT_DM_UPDT_TIMEOUT):	15 (0, 5 - 1440 Minutes)
Dynamic ELIN Timeout value (DYNAMIC_ELIN_TIMEOUT):	180 (5 - 1440 Minutes)
Reuse oldest ELIN during overflow (DYNAMIC_ELIN_REUSE):	<input type="checkbox"/>

5.1.3. Configure Digit Manipulation Index

As mentioned above, during the compliance test, when user dials 911, the call will be routed to simulated PSAP number, which is lab PSTN phone, 613-967-5280. This section will describe the steps on how to configure Digit Manipulation Index to route to that number. This configuration is an example used during compliance test. The configuration maybe deployed differently at customer site. Refer to section 9, for document on how to setup DMI in CS1000 in details.

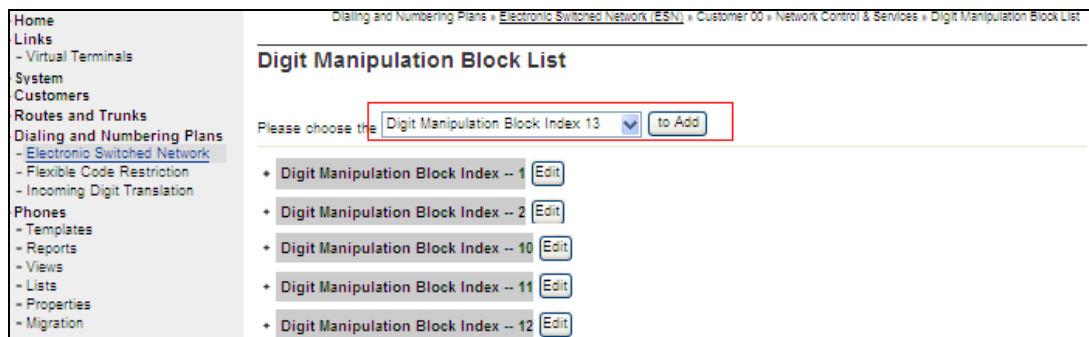
On the CS100 Element Manager page, navigate to **Dialing and Numbering Plans → Electronic Switched Network**. Select **Customer**, during compliance test, **Customer 00** is selected as shown below:

Electronic Switched Network (ESN)	
- Customer	Customer 00
- Network Control & Services	<ul style="list-style-type: none"> - Network Control Parameters (NCTL) - ESN Access Codes and Parameters (ESN) - Digit Manipulation Block (DGT) - Home Area Code (HNPA)

On the ESN page, select **Digit Manipulation Block** as shown below:



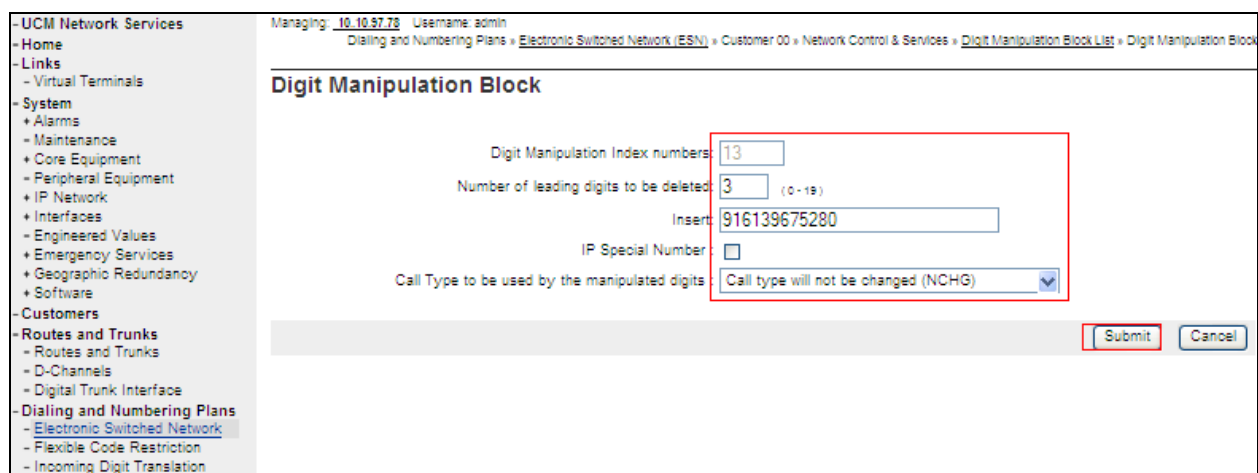
In the **Digit Manipulation Block List** page, a next available **Digit Manipulation Block Index** (DMI) is shown on the dropdown list, click on **Add** to a new DMI as shown below:



In the Digit Manipulation Block detail screen, enter the following information as shown below:

- **Digit manipulation Index Number:** this is read-only field and show the number of new DMI, 13.
- **Number of leading digit to be deleted:** enter 3.
- **Insert:** enter simulate PSAP number, example 613-967-5280.
- **Call Type to be used by the manipulated digits:** select **Call Type will not be changed(NCHG)**.

Leave other fields as default and click **Submit** to add new DMI.

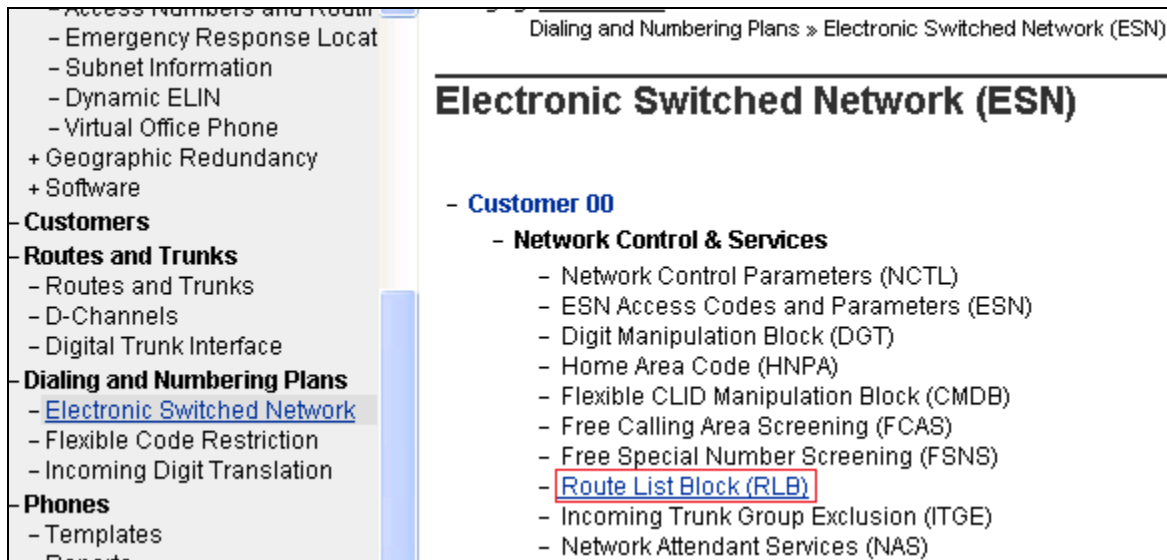


New **DMI 13** is created and listed in **Digit Manipulation Block List** page(not shown).

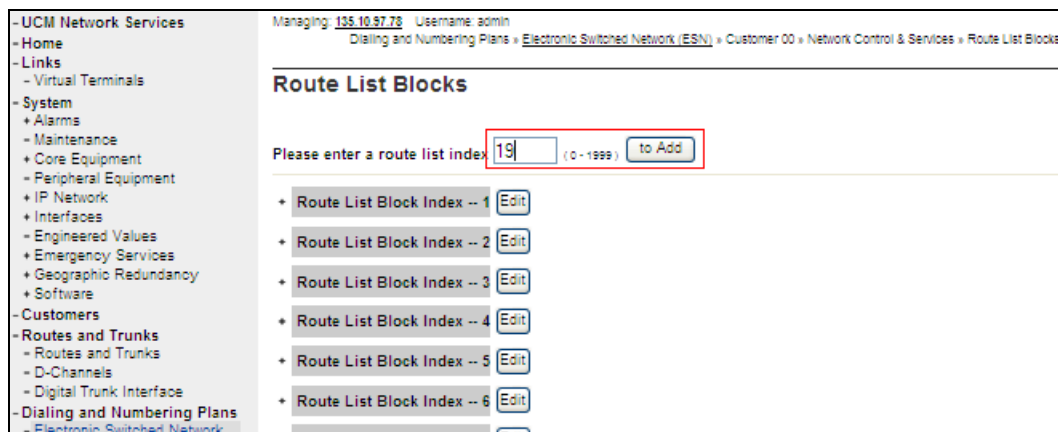
5.1.4. Configure Route List Index

This section will describe step need to create Route List Index (RLI) which will be used in creation of Emergency Services Directory Number (ESDN).

On the **Electronic Switched Network** page, select **Route List Block** as show below:



The **Route List Blocks** page launch, enter an available **Route List Index**, example: **19**, click on **Add** to a new RLI.



The detail page of new **Route List Block** is displayed, enter the following information for RLI as shown in below:

- **Route List Index:** This is read-only field. It should show new RLI value that is matched with the number which has been entered in previous step.
- **Digit manipulation Index:** Select DMI created in **Section 5.1.3**, which is **13**.
- **Route Number:** Select an active route that is used to route the call to outside In this testing , Route **1** is used..

Leave other fields as default value and click **Submit** to add new RLI.

Route List Block

General Properties

Number of Alternate Routing Attempts: 5 (1-10)

Initial Set: 0 (0-64)

Set Minimum Facility Restriction Level: []

Overlap Length: 0 (0-24)

Extended Local Calls: ☐

Route List Index: 19

Entry Number for the Route List: 0 (0-63)

Indexes

Time of Day Schedule: 0 [v]

Facility Restriction Level: 0 (0-7)

Digit Manipulation Index: 13 [v]

ISL D-Channel Down Digit Manipulation Index: 0 (0-1999)

Free Calling Area Screening Index: 0 [v]

Free Special Number Screening Index: 0 [v]

Business Network Extension Route: ☐

Incoming CLID Table: 0 (0-100)

Options

Local Termination entry: ☐

Route Number: 1 [v]

Skip Conventional Signaling: ☐

Display Originator's Information: ☐

Use Tone Detector: ☐

Conversion to LDN: ☐

Expensive Route: ☐

Strategy on Congestion: No Reroute (NRR) [v]

QSIG Alternate Routing Causes: QSIG Alternate Routing Cause 1 [v]

Preferred Routing: Preferred Route 1 [v]

ISDN Drop Back Busy: Drop Back Disabled (DBD) [v]

ISDN Off-Hook Queuing Option: ☐

Off-Hook Queuing Allowed: ☐

Call Back Queuing Allowed: ☐

VNS Options

Entry is a VNS Route: ☐

Submit **Cancel**

New **RLI 19** is created and listed in Route List Blocks page (not shown).

5.1.5. Configure Emergency Service Directory Numbers

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

The screenshot shows the 'Add Customer 0 Emergency Services Directory Number' configuration page. The left sidebar contains a navigation menu with 'Access Numbers and Routing' highlighted. The main content area has the following fields:

- Directory Number: [] *
- Directing Digits: [] *
- Default Calling Number: []
- On-Site Notification Station DN: []
- Routing Method:
 - ☒ Route Number: 1 [v]
 - ☐ Route List Index: [] [v]
- Misdial Prevention: ☐
- Misdial Delay: 2 [v] (seconds)
- Last ESDN Digit Repetition: ☒

At the bottom, there is a note '* Required value.' and 'Save' and 'Cancel' buttons.

Enter the following information as shown below:

- **Directory Number:** enter **911**.
- **Directing Digit:** enter **911**.
- **Routing Method:** select **Route List Index** and choose the appropriate value available from pull down menu, example **RLI 19**.
- **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 'Edit Emergency Services Directory Number Entry 0' configuration page. The left sidebar is the same as the previous screenshot. The main content area has the following fields:

- Directory Number: 911 *
- Directing Digits: 911 *
- Routing Method:
 - ☐ Route Number: [] [v]
 - ☒ Route List Index: 19 [v]
- Misdial Prevention: ☒
- Misdial Delay: 2 [v] (seconds)
- Last ESDN Digit Repetition: ☒

At the bottom, there is a note '* Required value.' and 'Save' and 'Cancel' buttons.

Primary ESDN is added as shown in below screenshot:

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 Customer 0

Default Calling Number :

On-Site Notification Station DN :

Emergency Services Directory Numbers

Add...
Delete
Refresh

	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

5.1.6. Configure Access Code + ESDN

In the **Avaya Emergency Service Access Fundamentals** document, page 106 **ESDNs and access code (AC) configuration** list detail steps on how to configure to dial any ESDN as AC+ESDN. There are 2 way to achieve this: configure 911 as a Special Number in AC1 and AC2 or configure AC1/AC2+911 as an alternate ESDN for example, configure 9+911 and 6+911 as ESDN so that the access codes 9 and 6 are part of the ESDN itself. This section will describes step to configure AC1/AC2+911 as an alternate ESDN where 911 is a primary ESDN, 9911 is first and 6911 is second entry in ESDN table as 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
 - Subnet Information
 - Dynamic ELIN
 - Virtual Office Phone
 - + Geographic Redundancy
 - + Software
- Customers
- Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
- Dialing and Numbering Plans
 - Electronic Switched Network

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 Customer 0

Default Calling Number :

On-Site Notification Station DN :

Emergency Services Directory Numbers

Add...
Delete
Refresh

	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
<input type="radio"/>	1	9911	RLI	20	911	YES	2	YES
<input type="radio"/>	2	6911	RLI	20	911	YES	2	YES

Number of ESDN blocks printed = 3

First, following step in Section 5.1.3 to add new DGT, completed the form with following details:

- **Number of leading digits to be deleted: 4**
- **Insert :** enter PSAP number, example: **916139675280**.
- Leave other fields as default.

Click **Submit** to save new DGT. Below is the detail of new created **DGT 15**:

Digit Manipulation Block List

Please choose the Digit Manipulation Block Index -- 19 to Add

- + Digit Manipulation Block Index -- 1 Edit
- + Digit Manipulation Block Index -- 2 Edit
- + Digit Manipulation Block Index -- 3 Edit
- + Digit Manipulation Block Index -- 4 Edit
- + Digit Manipulation Block Index -- 5 Edit
- + Digit Manipulation Block Index -- 6 Edit
- Digit Manipulation Block Index -- 15 Edit

Number of leading digits to be deleted: 4
Insert: 916139675280
Call Type to be used by the manipulated digits : NCHG

Second, following Section 5.1.4 to add new RLB, completed the form with following details:

- **Digit manipulation Index:** select DMI created in step 1, which is **15**.
- **Route Number:** select an active route to route the call to outside, example Route **1** is selected.
- Leave other fields as default.

Click **Submit** to save new RLI. Below is the detail of new created **RLB 20**:

Route List Block List

- + Route List Block Index -- 12 Edit
- + Route List Block Index -- 13 Edit
- Route List Block Index -- 20 Edit

Initial Set: 0
Number of Alternate Routing Attempts: 5
Set Minimum Facility Restriction Level: 0

- Data Entry Index -- 0 Edit

Route Number: 1
Expensive Route: N
Facility Restriction Level: 0
Digit Manipulation Index: 15
ISL D-Channel Down Digit Manipulation Index: 0
Free Calling Area Screening Index: 0
Free Special Number Screening Index: 0
Business Network Extension Route: NO

Third, following Section 5.1.5, to add new ESDN, completed the form with following details:

- **Directory Number:** enter **9911**.
- **Directing Digit:** enter **911**.
- **Routing Method:** select **Route List Index** and choose the appropriate value available from pull down menu, example select RLI created in step 2, **RLI 20**.
- **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**. Perform the same step again for **6911** ESDN.

The screenshot shows a web-based configuration interface. On the left is a navigation tree with categories: Links, System, Customers, Routes and Trunks, and D-Channels. The 'System' category is expanded, showing sub-items like Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Interfaces, Engineered Values, Emergency Services, Service Parameters, Access Numbers and Routing (highlighted), Emergency Response Location, Subnet Information, Dynamic ELIN, and Virtual Office Phone. The main area is titled 'Add Customer 0 Emergency Services Directory Number'. It contains the following fields: 'ESDN Entry' (dropdown set to 1), 'Directory Number' (text box with 9911), 'Directing Digits' (text box with 911), 'Routing Method' (radio buttons for 'Route Number' and 'Route List Index', with 'Route List Index' selected and a dropdown set to 20), 'Misdial Prevention' (checkbox checked), 'Misdial Delay' (dropdown set to 2, with '(seconds)' next to it), and 'Last ESDN Digit Repetition' (checkbox checked). At the bottom, there is a note '* Required value.' and 'Save' and 'Cancel' buttons.

5.1.7. Emergency Response Location (ERL)

During compliance test, there is no need to configure ERL on CS1000, as ERL database will be updated on CS1000 from E911M at a schedule time. Verify this ERL table on CS1000 is mentioned in **Section 7.1**.

5.2. Configure SNMP Trap on Avaya Communication Server 1000

This section describes the steps to configure SNMP Profile Manager. This is to generate alarms when 911 calls are made and allows E911M able to get near real-time data updates from the CS1000.

5.2.1. Create a New SNMP Profile

Refer to **Section 5.1.1** 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 below.

On the **SNMP Profile Manager** page, navigate to **SNMP Profile**. The **SNMP Profiles** page appears as shown as below. Click **Add** to add new SNMP Profile.

	Profile Name ▲	Profile Type	Version	Status
1	CUSTOM- .10.97.150-Alarm	Alarm	1.0	Not Assigned
2	CUSTOM- .10.97.171-Alarm	Alarm	1.0	Not Assigned
3	CUSTOM- .10.97.172-Alarm	Alarm	1.0	Not Assigned
4	CUSTOM- .10.97.78-Alarm	Alarm	1.0	Not Assigned
5	CUSTOM- .10.97.90-Alarm	Alarm	1.0	Assigned
6	CUSTOM- .10.97.92-Alarm	Alarm	1.0	Not Assigned

The **New SNMP Profile** page appears. Enter a name in the **Profile Name** text box, example **RedSky**. From the **Profile Type** list, select **ALARM**. 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 E911M ELAN IP addresses and ports (port 162 by default) in the **Trap Destinations**. Click **Save**.

SNMP Profile Manager

Profile Name: RedSky

Profile Type: ALARM

Trap community: public

Alarm Threshold: None

Option: ☒ Enable trap sending

Trap Destinations:

IPAddress1: 190.153 Port1: 162

IPAddress2: Port2:

Save Cancel

5.2.2. 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 as below. Select the element (example: **cpppm3**) that will be assigned to the newly created SNMP profile (**RedSky**). Click **Next**.

AVAYA SNMP Profile Manager Help Logout

«UCM Network Services

SNMP Profile

SNMP Distribution

SNMP Target Selection

Select the elements or group of elements for viewing and assigning SNMP Profiles

Network

- Element Manager
- Signaling Servers
- car2-sps
- car2-cores
- ☒ cpppm3
- Ungrouped Elements

Next

Copyright © 2008-2010, Avaya Inc. All rights reserved.

The **SNMP Profile Distribution** page appears, as shown below. Select a Network Element (ELAN IP address of CS1000 call server) then click the **Assign** button.

«UCM Network Services
SNMP Profile
SNMP Distribution

SNMP Profile Distribution

SNMP Profile Distribution page is used to assign profiles to the Network Elements

Assign...

<input checked="" type="checkbox"/>	Element Name ^	IP Address	Current SysInfo Profile	Current MIB Access Profile
<input checked="" type="checkbox"/>	EM on cpppm3	10.10.97.78	Default-SysInfo	Default-MibAccess

Next

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 this example: **RedSky**. Click **Save**.

«UCM Network Service:
SNMP Profile
SNMP Distribution

SNMP Profile Distribution Details [EM on sip175]

SysInfo Profile: Default-SysInfo

MIB Access Profile: Default-MibAccess

Alarm Profile: RedSky

View Save Cancel

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

«UCM Network Service:
SNMP Profile
SNMP Distribution

SNMP Profiles

SNMP Profiles are used for configuring Network Elements

Add... Delete

<input type="checkbox"/>	Profile Name ^	Profile Type	Version	Status
<input type="checkbox"/>	Default-Alarm	Alarm	1.0	Not Assigned
<input type="checkbox"/>	Default-MibAccess	MibAccess	1.0	Assigned
<input type="checkbox"/>	Default-SysInfo	SysInfo	1.0	Assigned
<input type="checkbox"/>	Prognosis	Alarm	1.0	Not Assigned
<input type="checkbox"/>	RedSky	Alarm	3.0	Assigned

5.3. Create user for E911 Manager® to access Avaya Communication Server 1000 web services

This section will describe steps to create Role and User, used on E911M to allow E911M makes SOAP request to the CS1000.

5.3.1. Create Role

Refer to **Section 5.1.1** to see how to login into the Unified Communications Management (UCM). From the UCM Home page, navigate to **Security → Roles**. The **Add New Role** page is displayed. Enter the following information in the page:

- **Role Name:** enter any descriptive name, example: **e911**.
- **Role Description:** enter any description, example: **Role for e911 Manager**.

Click **Commit and Continue** to move to **Role Details** page.

Add New Role

Step1: Identify the new role.
Enter a role name and description

*** Role Name:** e911 (1-26) (Allowed characters are a-z, A-Z, 0-9, - and _)

*** Role Description:** Role for e911 Manager Minimum 1 character

Note: The new role must be saved before you map element permissions.

***Required** **Commit and Continue** **Cancel**

In **Role Details** page, click **Add Mapping** button to add mapping for e911 role as shown below.

Role Details (e911)

Host Name: devsmgr.bvwdev.com User Name: admin

Identification

Role Name: e911

Description: Role for e911 Manager Minimum 1 character

Commit **Cancel**

Element/Service Permissions **Assigned Users**

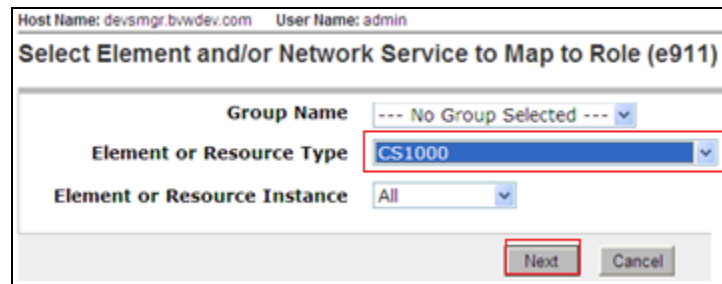
Add Mapping... **Delete Mapping** **Copy All From...**

Name	Permissions
------	-------------

In the **Select Element and/or Network Service to Map to Role (e911)** select as shown:

- **Element or Resource Type:** select CS1000
- Leave other fields as default.

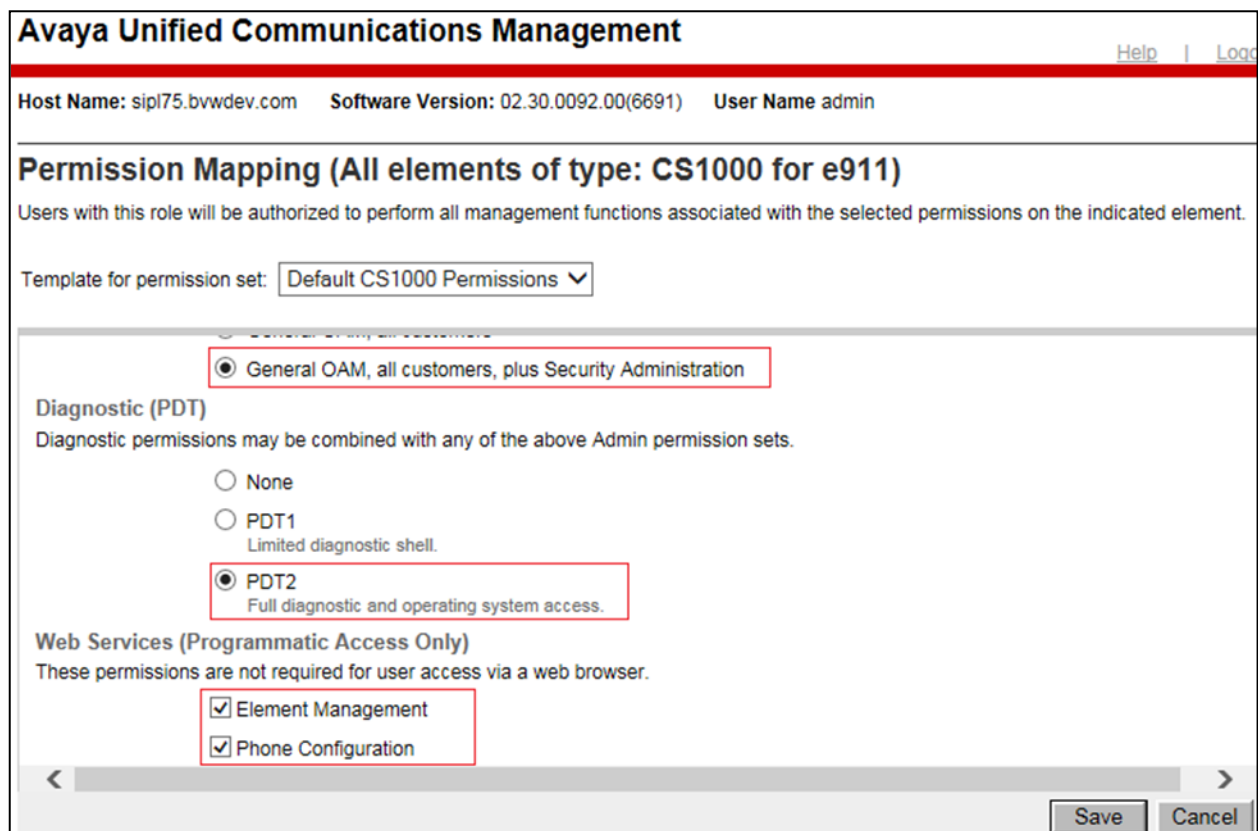
Click **Next**.



In the **Permission Mapping (All elements of type: CS1000 for e911)**, make sure to check all the selection as shown below:

- **General OAM, all customers, plus Security Administration.**
- **PDT2**
- **Element Management and Phone Configuration.**

Click **Save** to save all changes.



In the **Role Details (e911)** page, click **Commit** to complete final step to create new Role (not shown). The **e911** role mapping is added as shown below:

Role Details (e911)

Identification

Role Name:

Description: 1-x characters

Element/Service Permissions **Assigned Users**

	Name	Permissions
1 <input type="checkbox"/>	All elements of type: CS1000	All Customers, Account Admin, Config Prompts, CSO Am User, Enable Host Mode, Key Code Change, Root Access, Security Admin, Unrestricted Access, Specific Customer-Tenant access , PDT2 Access, (22) Print Routine 3 , Phone Configuration, Element Management

New Role **e911** is added in Roles page.

Network Elements CS 1000 Services Corporate Directory IPSec Numbering Groups Patches SNMP Profiles Secure FTP Token Software Deployment User Services Security Roles Policies Active Sessions		Host Name: devsmgr.bvwdev.com User Name: admin	
<input type="checkbox"/>	CS1000 CLI Register	0	Patching Manager All elements of type: Secure FTP Token Manager All elements of type: Snmp Manager All elements of type: Linux Base All elements of type: Media Card All elements of type: Media Gateway Controller Register/Unregister an individual CS1000 Element (MC, MC32S, MGC, VGMC) from the device's local OAM CLI
<input type="checkbox"/>	Discovery Admin	0	All elements of type: Discovery Management All elements of type: operation All elements of type: scheduleroperation Default Role for Discovery Management
<input checked="" type="checkbox"/>	e911	0	All elements of type: CS1000 Role for e911 Manager

5.3.2. Add new user

From the UCM Home page, navigate to **User Services → Administrative Users**. In the Administrative Users page, click **Add** button (not shown). In the **Add New Role** page enter the following information for user as shown below:

- **User ID** enter descriptive user name, example: **e911**
- **Authentication Type**: select **Local**.
- **Temporary password**: enter password for user.
- **Re-enter password**: re-enter password to confirm the correct password.

Click **Commit and Continue** button.

Host Name: devsmgr.bwdev.com User Name: admin

Add New Administrative User

Step1: Identify the new user.
Enter the user's full name and select an authentication type and User ID. Locally authenticated users also required a temporary password.

User ID: e911 (1-31) (Allowed characters are a-z, A-Z, 0-9, - and _)

Authentication Type: ☒ Local ☐ External

Full Name: E911 Manager

Temporary password: [masked]

Re-enter password: [masked]

Allowed characters in the password are: a-zA-Z0-9[]{}<>./=:!@#\$%^&*~?'. The length of your password must be at least 8 characters.

Note: The new user must be saved before you may assign roles.

Commit and Continue Cancel

Select the Role for this new user, select **Role** that created above, in this case it is **e911** as shown below and click **Commit**.

Add New Administrative User

Step2: Assign Role(s)
Selected roles authorize the user for associated features and element permissions.

Roles

Role ID	Role Name	Permissions	Role Description
10	Discovery Admin	All elements of type: Discovery Management All elements of type: operation All elements of type: scheduleroperation	Default Role for Discovery Management
11	e911	All elements of type: CS1000	Role for e911 Manager
12	End-User	All elements of type: operation	End-User
13	MemberRegistrar	All elements of type: IPsec Manager	Member Registrar Role

Commit Cancel

New user **e911** is added. To change the temporary password to permanent password, try to login System Manager as mention in **Section 5.1** using new created **e911** user name and password (not shown), the next screen will ask user to change their temporary password as shown below.

AVAYA Avaya Aura[®] System Manager 6.3

Home / Log On

Log On

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

You must change your temporary password to continue

New Password:

Confirm Password:

Ch

6. RedSky E911 Manager® Configuration

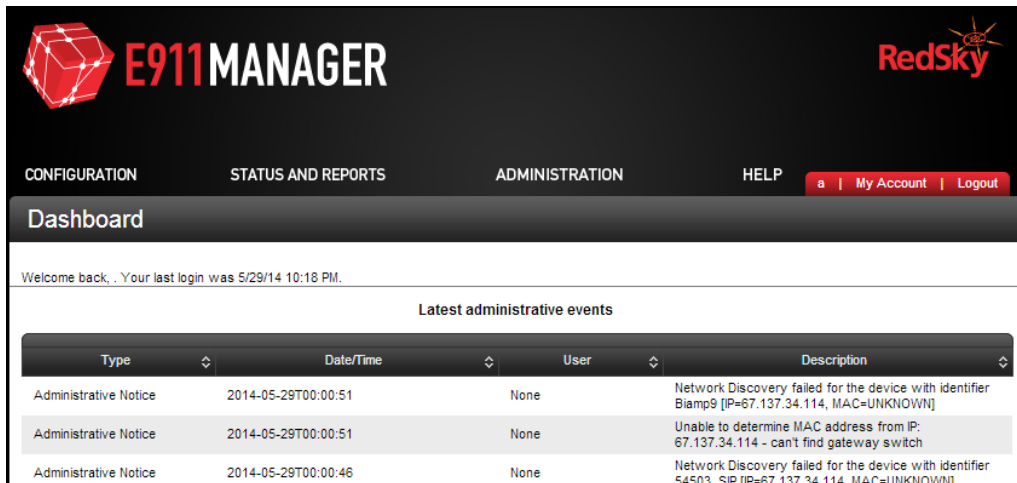
RedSky Administrator installs, configures, and customizes the RedSky E911Manager for their customers. Database such as ALI Provider Sites, ELIN Pools, and Buildings are pre-configured by RedSky, therefore how to setup these are out of scope in this application notes. This section only describes the interface configuration, so that the E911M can be integrated with CS1000.

This section will describe steps to create:

- ERLs
- IP Ranges
- Call Servers
- User for Softphone user and Import mapping for MyE911 Softphone user.

6.1. Create ERLs

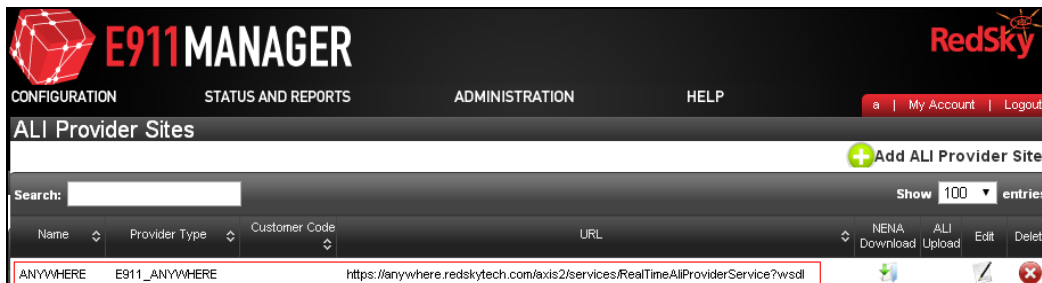
To login E911M web interface by opening a web browser and entering appropriated URL: example <https://try.redsky.com>. The screen bellow is displayed as shown below:



The screenshot shows the RedSky E911 Manager web interface. The top navigation bar includes 'CONFIGURATION', 'STATUS AND REPORTS', 'ADMINISTRATION', and 'HELP'. A user menu on the right shows 'My Account' and 'Logout'. The main content area is titled 'Dashboard' and displays a welcome message: 'Welcome back, . Your last login was 5/29/14 10:18 PM.' Below this is a section for 'Latest administrative events' with a table listing recent events.

Type	Date/Time	User	Description
Administrative Notice	2014-05-29T00:00:51	None	Network Discovery failed for the device with identifier Blamp9 [IP=67.137.34.114, MAC=UNKNOWN]
Administrative Notice	2014-05-29T00:00:51	None	Unable to determine MAC address from IP: 67.137.34.114 - can't find gateway switch
Administrative Notice	2014-05-29T00:00:46	None	Network Discovery failed for the device with identifier 54503_SIP [IP=67.137.34.114, MAC=UNKNOWN]

Verify ALI Provider Sites is pre-configured by navigate to **Configuration → ALI Provider Sites**, below is an example of E911A used as ALI Provider during compliance test:



The screenshot shows the 'ALI Provider Sites' page in the RedSky E911 Manager. It features a search bar, a table of provider sites, and a '+ Add ALI Provider Site' button. The table has columns for Name, Provider Type, Customer Code, URL, NENA Download, ALI Upload, Edit, and Delete. A red box highlights the first entry in the table.

Name	Provider Type	Customer Code	URL	NENA Download	ALI Upload	Edit	Delete
ANYWHERE	E911_ANYWHERE		https://anywhere.redskytech.com/axis2/services/RealTimeAliProviderService?wsdl				

Verify ELIN Pools is pre-configured by navigate to **Configuration → ELIN Pools**, below is an example of ELIN Pool used during compliance test:


Name
ANYWHERE

Verify ELINs is pre-configured by navigate to **Configuration → ELINs**, below is an example of ELINs used during compliance test:

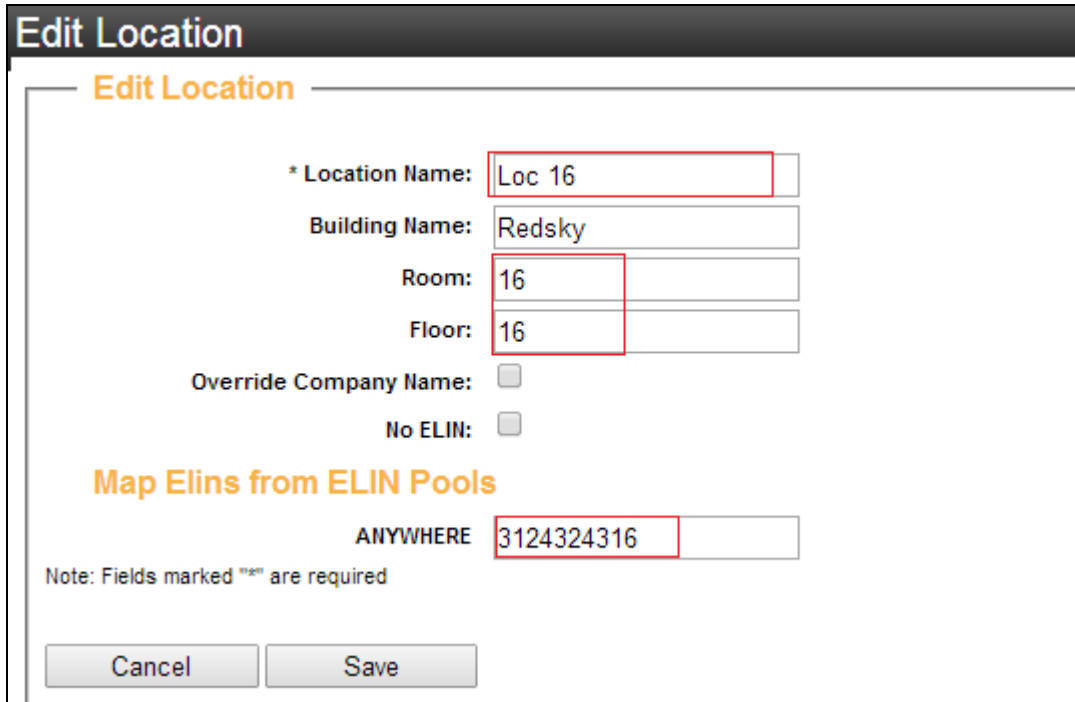
ELIN Pool	Phone Number	Username	Building Name	Location Name	ALI Provider Site	Validation Status	Error Message	RLI	Edit	Delete
ANYWHERE	3124324315	as	Redsky	loc21	ANYWHERE	Valid	SUCCESS			
ANYWHERE	3124324318	as1	Redsky	loc21	ANYWHERE	Valid	SUCCESS			
ANYWHERE	3124324321		Redsky	loc21	ANYWHERE	Valid	SUCCESS			
ANYWHERE	3124324320	as2	Redsky	Loc 17	ANYWHERE	Valid	SUCCESS			
ANYWHERE	3124324317		Redsky	Loc 17	ANYWHERE	Valid	SUCCESS			
ANYWHERE	3124324316		Redsky	Loc 16	ANYWHERE	Valid	SUCCESS			

Verify Buildings is pre-configured by navigate to **Configuration → Building**, below is an example of Building used during compliance test.

Building Name	Unique ID	Building Type	Address	MSAG Status	Level of Service	Edit	Delete
Redsky	Redsky	Corporate	925 W Chicago Ave, Chicago, IL 60642	VALID	Enhanced		

To create ERLs navigate to **Configuration → ERLs**, click on  **Add ERL** icon to add new ERL, below is an example of ERLs **Loc 16** for Room **16** and Floor **16** and this ERL belong to ELIN **3124324316** created during compliance test. Click **Add** to add new ERL (not shown), in below screenshot is detail of existing ERL created during initial setup for compliance test.

Note: Since **Loc 16** is created first therefor its ID is 1 (not shown in the ERL detail page on E911M), when E911M synchronized with CS1000, this will be added as ERL 1 on Communication Server. And so on for other ERLs.



Edit Location

Edit Location

* Location Name:

Building Name:

Room:

Floor:

Override Company Name: ☐

No ELIN: ☐

Map Elins from ELIN Pools

ANYWHERE

Note: Fields marked * are required

6.2. Configure IP Range

This section describe step to create IP Range mapping with existing ERLs. To create IP Range navigate to **Configuration → IP Range**, click on **+** icon to add new IP Range, below is an example of **IP Range 1** for Private IP network, this IP Range belong to ERL **Loc 17**, Building **RedSky**:

Edit IP Range

Edit IP Range

* IP Range Name: Range 1

* Lower IP: 10.33.5.1

* Upper IP: 10.33.5.225

Building: Redsky ▼


Location: Loc 17 ▼

Note: Fields marked * are required

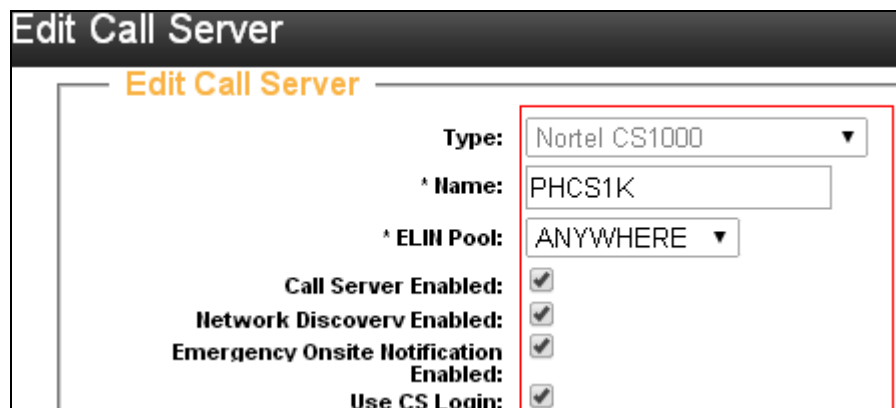
Cancel Save

Note: Since E911M only able to assign ERL to IP deskphone only, user need to manually assign ERL to TNB of analog and digital phone on CS1000.

6.3. Configure Call Servers

To create Call Server, navigate to **Configure → Call Server**, click on  icon to add new Call Server. Below is detail of existing Call Server created and used during compliance test:

- **Type** selects **Nortel CS1000**
- **Name** enters any descriptive name, example **PHCS1K**.
- **ELIN Pool** selects appropriate Pool.
- **Call Server Enable**, **Network Discovery Enable**, **Emergency Onsite Notification** and **Use CS Login** checkboxes are checked.



Edit Call Server

Type: Nortel CS1000 ▼

*** Name:** PHCS1K

*** ELIN Pool:** ANYWHERE ▼

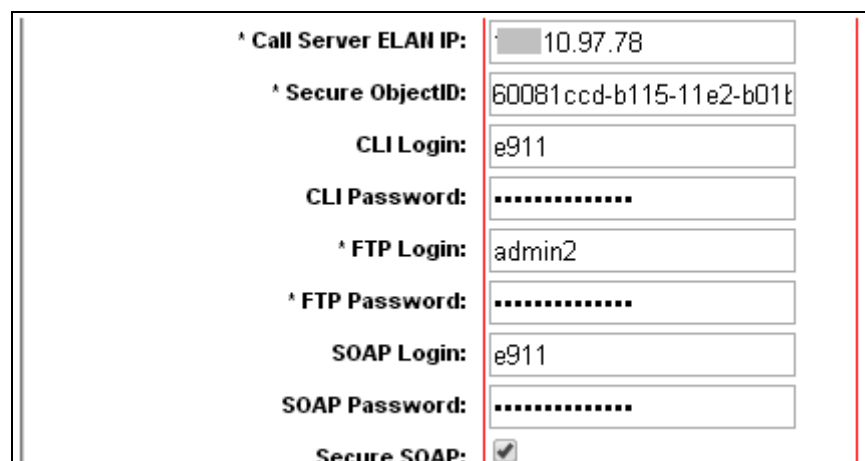
Call Server Enabled: ☒

Network Discovery Enabled: ☒

Emergency Onsite Notification Enabled: ☒

Use CS Login: ☒

- **Call Server ELAN IP** enters ELAN of CS1000, example 10.10.97.78
- **Secure ObjectID** enter CS1000 Secure ObjectID, see **Section 5.1.2** to open the EM of CS1000, right click on Element **EM for sip175**, select Copy Shortcut to copy the link to Clipboard, open any text editor to paste the link. Extract **Secure ObjectID**.
- **CLI Login/Password** enters User name/Password created in **Section 5.3.2**.
- **FTP Login/Password** enters login credential to login CS1000 ftp – example admin2/admin2's password.
- **SOAP Login/Password** enters User name/Password created in **Section 5.3.2**.
- Check **Secure SOAP** checkbox



*** Call Server ELAN IP:** 10.97.78

*** Secure ObjectID:** 60081ccd-b115-11e2-b01b

CLI Login: e911

CLI Password:

*** FTP Login:** admin2

*** FTP Password:**

SOAP Login: e911

SOAP Password:

Secure SOAP: ☒

- **Inventory Report Path** enter path to inventory file on CS1000 ftp, example:
/var/opt/Nortel/cs/fs/u/db/inv
- **Signaling Server IP** enters CS1000 Signaling Server IP address.
- **SNMP Trap Sources** enter ELAN, TLAN IP address of CS1000 and Signaling Server IP.

* Inventory Report Path:	<input type="text" value="/var/opt/nortel/cs/fs/u/db/inv"/>
* Signaling Server IP:	<input type="text" value="10.97.136"/>
SNMP Trap Sources:	<input type="text" value="10.97.136, 10.97.136"/>
<input type="button" value="Add Filtering"/>	

Click **Add** to add new Call Server. See below figure of new created **Call Server PHCS1K**. Once the call server is add, click on **Download** icon to synchronize data between CS1000 and E911M as shown below:

You are licensed for 1 Call Servers, of which you have already created 1

Search:	Show 100 entries							
Call Server Name	IP Address	Type	Elin Pool	Sync ERLs	View ERLs	Download	Edit	Delete
PHCS1K	10.97.78	Nortel CS1000	ANYWHERE					


Showing 1 to 1 of 1 entries

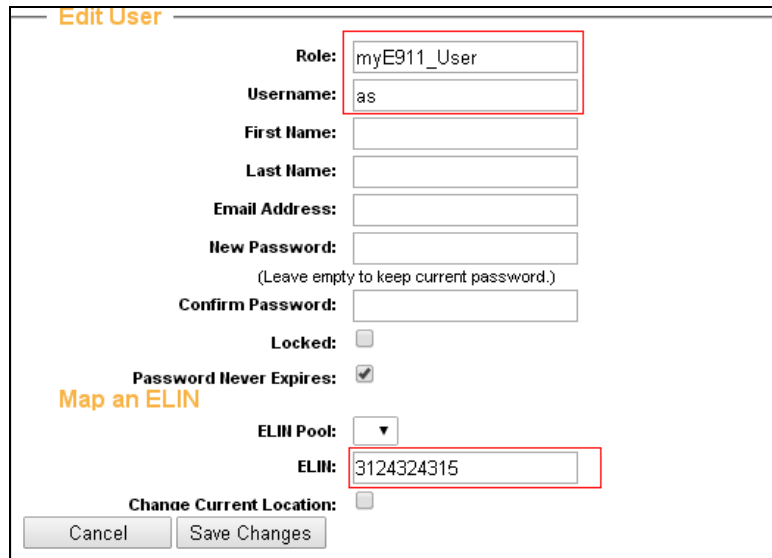
First Previous 1 Next Last

When the download complete, navigate to **Status and Reports → Endpoints** to view the list of endpoint is updated on E911M as show below.

Endpoints												
Nortel CS1000												
Search:		Show 100 entries										
TN	PBX	Display Name	Description	IP Address	MAC Address	Discovery Status	Building	Floor	Room	ELIN	Discover	
960119	PHCS1K	Tango 11403	TANGO	135.10.98.80		Success: Layer 3	Redsky	21	21	3124324318		
96000	PHCS1K	Hai Vo	54000	10.33.5.15	00:0A:E4:05:C8:A5	Success: Layer 3	Redsky	17	17	3124324317		
4031	PHCS1K	54550, 3904	PHUONG									
104003	PHCS1K		DEV1	10.33.5.57		Success: Layer 3	Redsky	16	16	3124324316		

6.4. Add user for MyE911® softphone

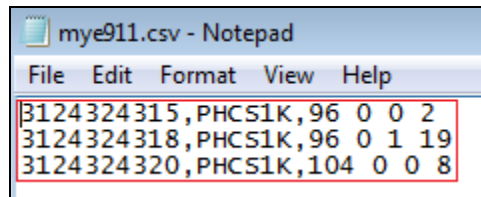
To add new user for MyE911, navigate to **Administration** → **User**, click on  icon to add new user, **ROLE** selects **myE911_User** from the list, enter appropriated user name and password, each user is mapped to available ELIN. Click **Add** to add new user. Below is example of exiting user created during compliance test.



The 'Edit User' form contains the following fields and options:

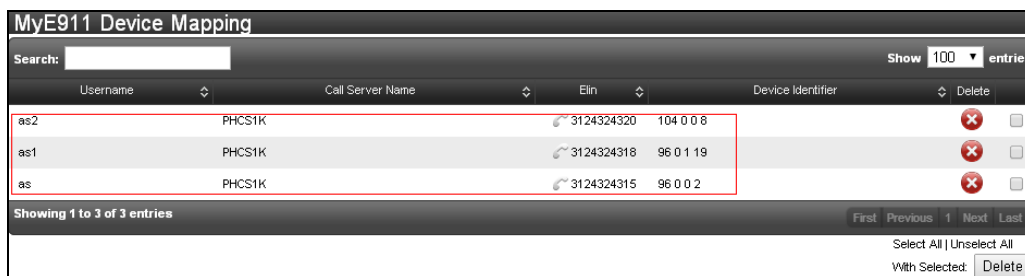
- Role:** myE911_User
- Username:** as
- First Name:** (empty)
- Last Name:** (empty)
- Email Address:** (empty)
- New Password:** (empty)
- (Leave empty to keep current password.)
- Confirm Password:** (empty)
- Locked:** ☐
- Password Never Expires:** ☒
- Map an ELIN:** (orange text)
- ELIN Pool:** (dropdown menu)
- ELIN:** 3124324315
- Change Current Location:** ☐
- Buttons:** Cancel, Save Changes


Next step is to perform import mapping for softphone user, navigate to **Configure** → **Import** → **MyE911® Device Mapping**, preparing import file follow this format: ELIN of MyE911® user, Call Server Name, Softphone TN as shown below.



```
3124324315,PHCS1K,96 0 0 2
3124324318,PHCS1K,96 0 1 19
3124324320,PHCS1K,104 0 0 8
```

To verify the list of myE911 device, navigate to **Administration** → **MyE911 Device Mapping**, list of imported softphone is added into the list as shown below.




Username	Call Server Name	Elin	Device Identifier	Delete
as2	PHCS1K	3124324320	104 0 0 8	
as1	PHCS1K	3124324318	96 0 1 19	
as	PHCS1K	3124324315	96 0 0 2	

Showing 1 to 3 of 3 entries

First Previous 1 Next Last

Select All | Unselect All

With Selected: 

7. Verification Steps

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

7.1. Verify ERL is updated on Avaya Communication Server 1000

Once the synchronization is complete, on CS1000 Element Manager, navigate to **System → Emergency Services → Emergency Response Location**; verify ERL is added accordingly to ERL data on E911M.

ERL	State	Site Name	Location Description	Route Number	Route List Index	Access Code	Prepend Digits	Static ELIN	On-Site Notification DN
2	ENL	REDSKY	LOC15					3124324315	
3	ENL	REDSKY	LOC16					3124324316	
4	ENL	REDSKY	LOC17					3124324317	

7.2. Verify Inventory table on CS1000

SSH to CS1000 using appropriate login credential, using `ld 117` enter command **locrpt all**. Verify the endpoint listed on E911M for IP phone is match with this report such as TN, ERL, and Location Description.

7.3. Verify Endpoints Detected

Allow the E911M enough time to download all data from CS1000. Access the E911M web interface as described in **Section 6**. When the download complete, navigate to **Status and Reports → Endpoints** to view the list of endpoint is updated on E911M as show below. List will display all register IP phones, digital and analog phones on CS1000. For IP phone within IP ranges E911M will assign ERL to appropriated phone, for digital and analog user must manually manage them on CS1000.

TN	PBX	Display Name	Description	IP Address	MAC Address	Discovery Status	Building	Floor	Room	ELIN	Discover
960119	PHCS1K	Tango 11403	TANGO	135.10.98.80		Success: Layer 3	Redsky	21	21	3124324318	
960000	PHCS1K	Hai Vo	54000	10.33.5.15	00:0A:E4:05:C8:A5	Success: Layer 3	Redsky	17	17	3124324317	
4031	PHCS1K	54550, 3904	PHUONG								
104003	PHCS1K	DEV1	DEV1	10.33.5.57		Success: Layer 3	Redsky	16	16	3124324316	

7.4. Verify On Site Notification Alert Detected

Make a 911 emergency call from one of the detected IP phone. Verify that there is a Notification Alert being generated in event list of E911M.

Events			
Search: <input type="text"/>		Show 100 entries	
Type	Date/Time	User	Description
Login	2014-05-23T11:20:00	a	Logged in: a@135.10.98.75
911 Call Made	2014-05-23T11:19:33	None	911 call made: CallHistoryAuto [id=214, callTime=2014-05-23 11:19:33.437, companyName=Avaya, deviceId=581, username=null, pbxName=PHCS1K, elin=3124324318, extension=54711, address=925 W Chicago Ave, Chicago, IL 60642, buildingUid=Redsky, buildingName=Redsky, locationInfo=loc21 (21, 21), supplementalData=, isE911Call=false, callbackNumber=null]
Administrative Notice	2014-05-23T11:03:14	None	Network Discovery failed for the device with identifier Beth 1120 [IP=10.33.6.3, MAC=00:17:65:FD:BF:55]
Administrative Notice	2014-05-23T10:07:58	None	Network Discovery failed for the device with identifier Blamp9 [IP=67.137.34.114, MAC=UNKNOWN]
Administrative Notice	2014-05-23T10:07:58	None	Unable to determine MAC address from IP: 67.137.34.114 - can't find gateway switch

On end user's PC an on screen alert with the following information: Customer, PBX, ELIN, Extension, Building Name, Building UID, Address and Location (Room, Floor) and alert comes in the form of an audible siren.

EON

Emergency On-Site Notification

STATUS

ALERT HISTORY

ABOUT

LOGOUT

911 call placed on Aug 15, 2014 8:39:33 AM

Customer: Avaya

PBX: PHCS1K

Elin: 3124324318

Extension: 54007

Building Name: Redky

Building UID: Redky

Supplemental Data:

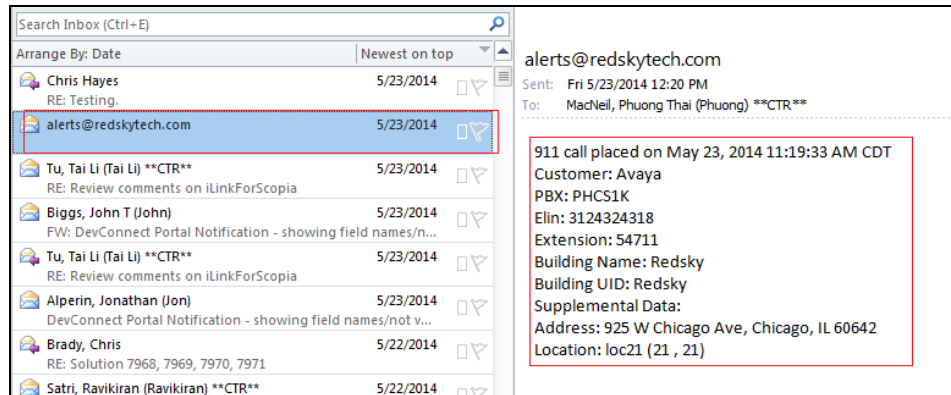
Address: 925 W Chicago Ave, Chicago, IL 60642

Location: 18 (18 , 18)

ACKNOWLEDGE ALERT

PRINT ALERT RECORD

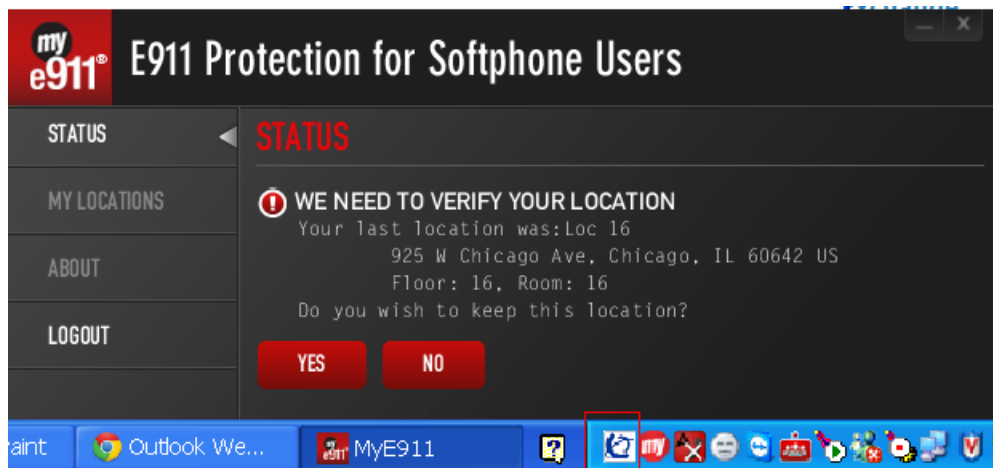
And user received alert email as well.



7.5. Verify MyE911® able to verify location for softphone user

On the client's PC, upon login of MyE911, MyE911 gets a list of softphone executables from Manager, this list is pre-configured by the RedSky administrator. During compliance test Avaya 2050PC and One-X Communicator softphone are used, here is example of the softphone executables list: i2050.exe and onexcui.exe.

MyE911 runs in the background of the client's window's computer. From the background, it checks all processes until it finds a process that was launched from the executables list. When a softphone in said list is detected, MyE911 will force pause it and hide all of its windows until the user confirms their location as shown below.



Once the location is confirm, the softphone will continue its login process and ready for user to make a call.

Note: This location will be update on E911M instantly and only be updated on CS1000 if administrator performs manual update on E911M to CS1000.

8. Conclusion

The RedSky E911 Manager® Solution passed the compliance testing. These Application Notes describe the procedures required for the RedSky E911 Manager® 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 the RedSky E911 Manager® products may be obtained by contacting RedSky Inc.

©2014 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.