Avaya Solution & Interoperability Test Lab

Application Notes for 911 ETC CrisisConnect® for VoIP and 911 ETC CrisisConnect® for Softphone with Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya one-X® Communicator – Issue 1.0

Abstract

These Application Notes describe configuration steps required for 911 ETC CrisisConnect® for VoIP and 911 ETC CrisisConnect® for Softphone to interoperate with Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya one-X® Communicator.

911 ETCs' CrisisConnect® for VoIP solution enables E911 call routing to the correct Public Safety Answering Point (PSAP) and delivers the caller's address directly to the PSAP operator's panel in order to provide immediate emergency assistance.

911 ETCs' CrisisConnect® for Softphones uses the 911 ETC VoIP Positioning Center service to allow Avaya one-X® Communicator users to provision a location in near real-time.

The compliance testing was focused on routing E911 calls from Avaya Aura® Session Manager to 911 CrisisConnect, which in turn, performed call routing to the correct PSAP. Please note that, at the moment, only in-band DTMF is supported by 911 ETC.

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 configuration steps required for 911 ETC CrisisConnect® for VoIPs and 911 ETC CrisisConnect® for Softphone to interoperate with Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya one-X® Communicator.

911 ETC provides a VoIP Positioning Center (VPC) Service that is able to deliver 911 calls to U.S. and Canada PSAPs independent of the region the call originates from. 911 ETC provides two methods for customers to interconnect for E911 call routing – PSTN and SIP.

If a customer chooses to interconnect via PSTN, 911 ETC issues the customer "Access line" (E.164, DID) number. The access numbers are specific to the customer and are used to identify that the call originated from the customer.

CrisisConnect® for Softphones uses the 911 ETC VoIP Positioning Center (VPC) service to allow Avaya one-X® Communicator users to provision a location in near real-time. CrisisConnect® for VoIP is a required service. Avaya one-X® Communicator in Road Warrior mode is required. 911 ETC provides the SoftLoc™ server software and a distributable client software package to be installed on computers where the Avaya one-X® Communicator is installed.

SoftLoc™ Client assists/requires users of soft phones to provision their current location to ensure accurate routing of an outgoing 911 call. It was developed because of concerns by 911 ETC's customers that soft phone users will ignore critical location information when logging onto their soft phones.

SoftLoc™ Client runs as a Windows system-tray application and quietly waits for the user to launch a configured soft phone application. Upon launch, SoftLoc™ will appear above all other applications and reminds the user to provision an emergency location. Up to three frequently-used locations can be saved to the remote emergency server and quickly provisioned with just a few mouse clicks. If the user chooses not to provision an emergency location, the soft phone application will be forcibly closed. Responsibility, and therefore liability, is placed back upon the user and accurate location information is ensured in the event of an emergency.

2. General Test Approach and Test Results

The compliance test focused on verifying that 911 ETC CrisisConnect® for Softphone can update users' location information in real time and 911 ETC CrisisConnect® for VoIP can perform appropriate call routing.

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 compliance test validated the ability of 911 ETC CrisisConnect® for Softphone and CrisisConnect® for VoIP to update users' address information in near real time, route emergency calls and provide ALI information to PSAP. Feature tests also included the following:

- Call setup using SIP (UDP).
- Codec verification using G.711.
- Calls from Analog, Digital, One-X® Communicator and Avaya 9600 Series IP Endpoints.
- Mis-provision of ANI in 911 ETC database, which resulted in call getting routed to Emergency Call Relay Center (ECRC).
- Verification of alerts generated when dialing emergency number from all types of endpoints.

Failover tests were also performed for the cases where the SIP trunk to 911 ETC is down (SIP 408) and a negative response from 911 ETC (SIP 503), which resulted in alternate routing to secondary route.

For this test effort, only calls related to audio, and PSAP ALI, were placed by dialing 911. Rest of the test calls, due to the nature of emergency calling, were placed to 933. 933 is an Address Verification Service provided by 911 ETC.

2.2. Test Results

All planned test cases were passed.

2.3. Support

Technical support for 911 ETC CrisisConnect® can be obtained through the following:

- Web: http://www.911etc.com/contact-us
- E-mail: support@911etc.com
- Phone: (480) 719-8556

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- 911 ETC CrisisConnect® for VoIP
- SoftLoc™ Server
- SoftLoc™ Client
- Avaya one-X® Communicator

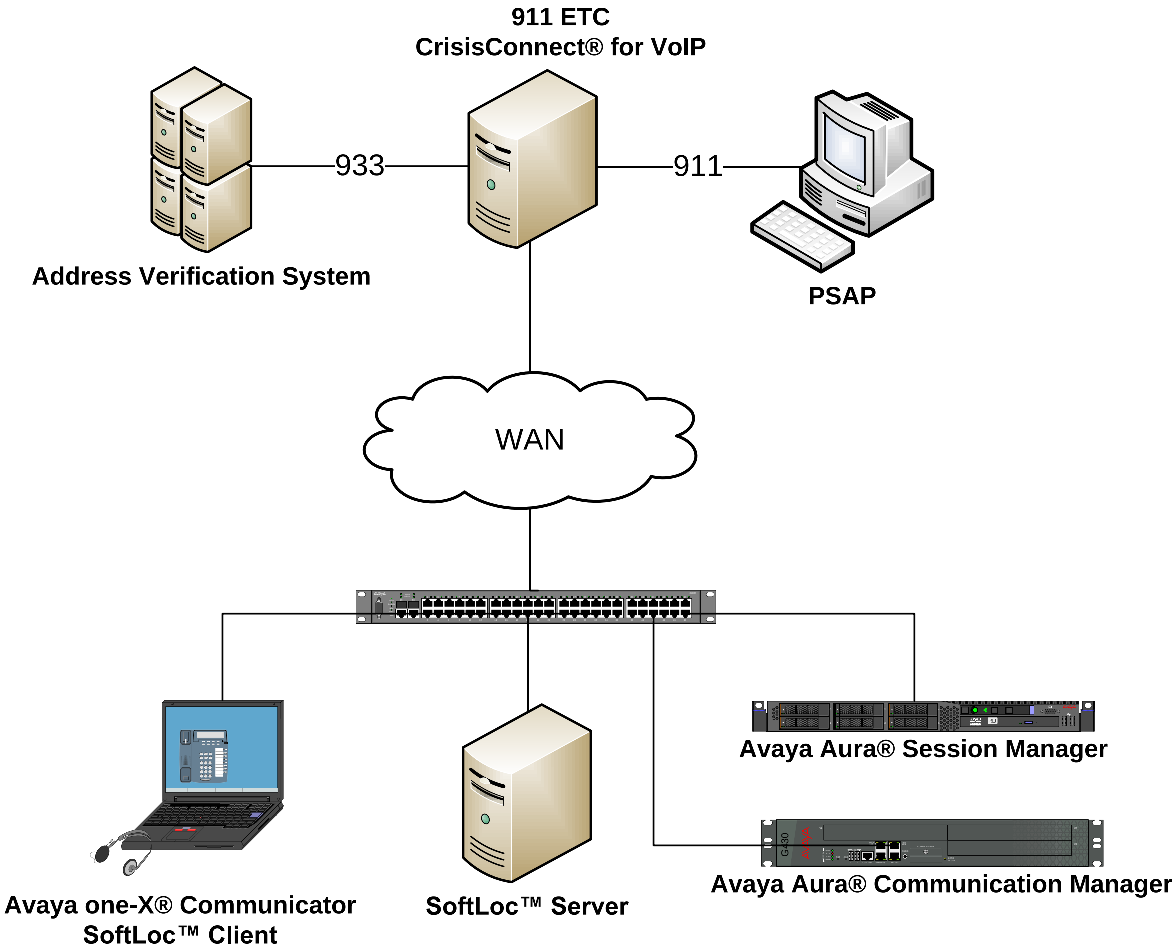


Figure 1 – Test Configuration

4. Equipment and Software Validated

The following equipment and version were used in the reference configuration described above:

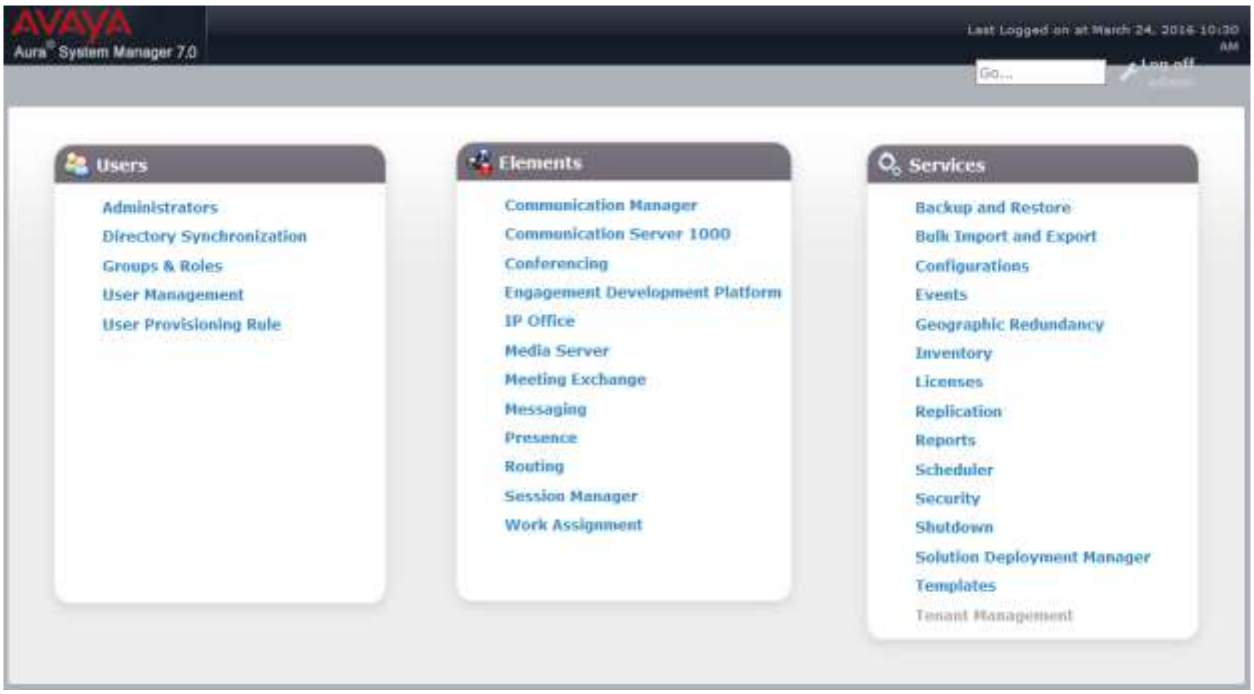
Component	Firmware Version	Description
Avaya G430 Media Gateway Avaya Aura® Communication Manager	7.0	Runs Communication Manager (CM) call processing software.
Avaya Aura® Session Manager	7.0	SIP routing engine
Avaya one-X® communicator	6.2 SP 11	Softphone client
CrisisConnect® for VoIP	5.2.3	Emergency Call Routing services
CrisisConnect® SoftLoc™ Server	2.1.5.0	Location Server
CrisisConnect® SoftLoc™ Client	2.1.5.0	SoftLoc™ Client

5. Configure Avaya Aura® Session Manager

This section provides the steps for configuring Session Manager to communicate with 911 ETC. For more details, see the administration guide.

Session Manager is configured using browser access to System Manager. Enter the URL of System Manager such as https://<hostname>/network-login/SMGR where <hostname> is the ip address or qualified domain name of the System Manager. Login using appropriate credentials.

The home page is a navigation screen as shown below. Each of these links will open a new tab from which to navigate to the details of the managed environment. Click on **Routing**.

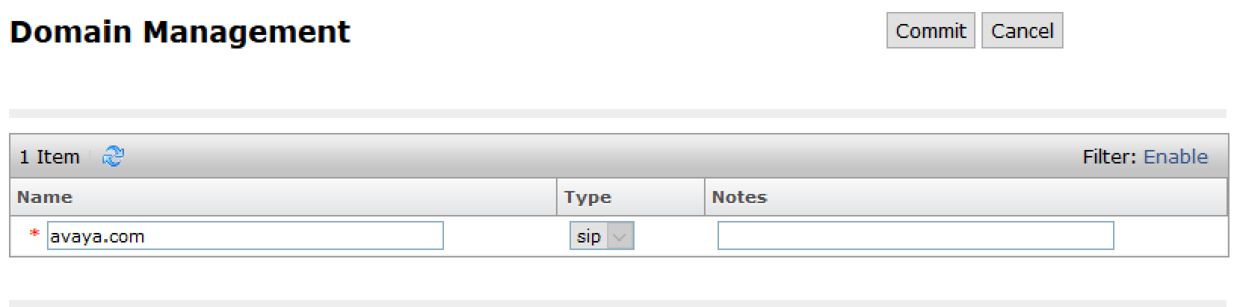


5.1. Configure Domain

One the left pane, click on **Domains**. On the **Domains** page, click on **New**.

- For **Name** field, type in the domain
- Set the **Type** to **sip**

For Compliance testing, avaya.com sip domain was used.

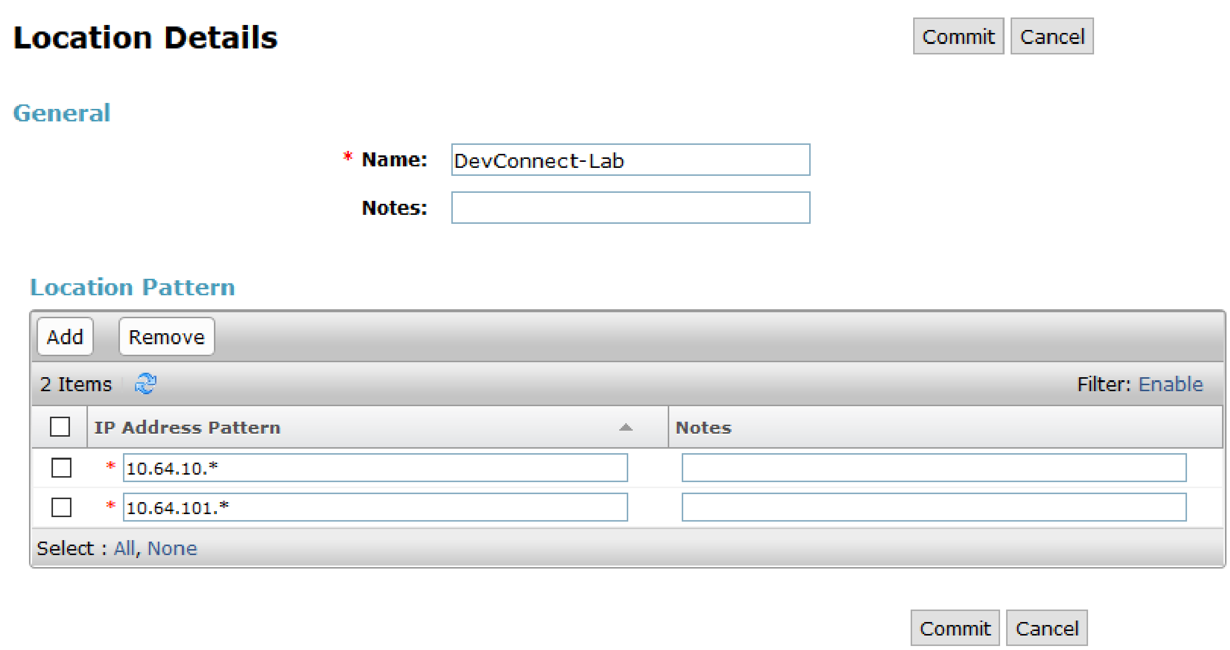


5.2. Configure Location

On the left pane, click on **Locations.** On the **Location** page, click on **New**.

- Enter the **Name** of the location
- Add a **Location Pattern**

For Compliance testing the following information was used.



5.3. Configure SIP Entity and Entity Link

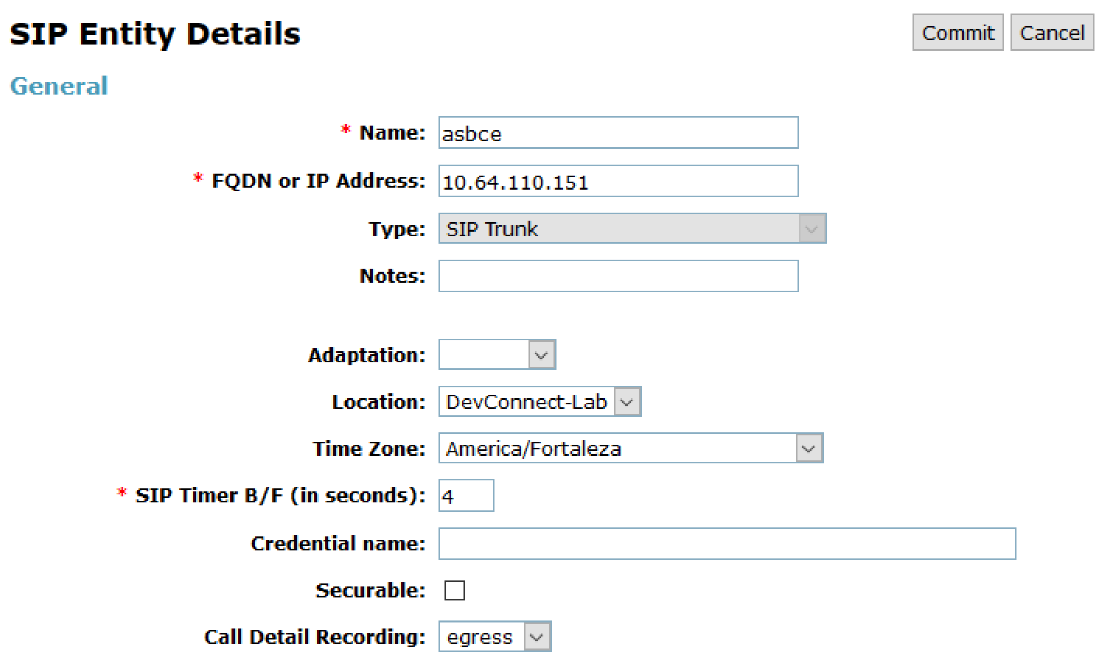
During Compliance testing, calls to 911 ETC were routed via Avaya Session Border Controller for Enterprise (ASBCE). SIP Entity and Entity link to ASBCE were configured as follows. On the left pane, click on **SIP Entities.** On the **SIP Entity** page, click on **New**.

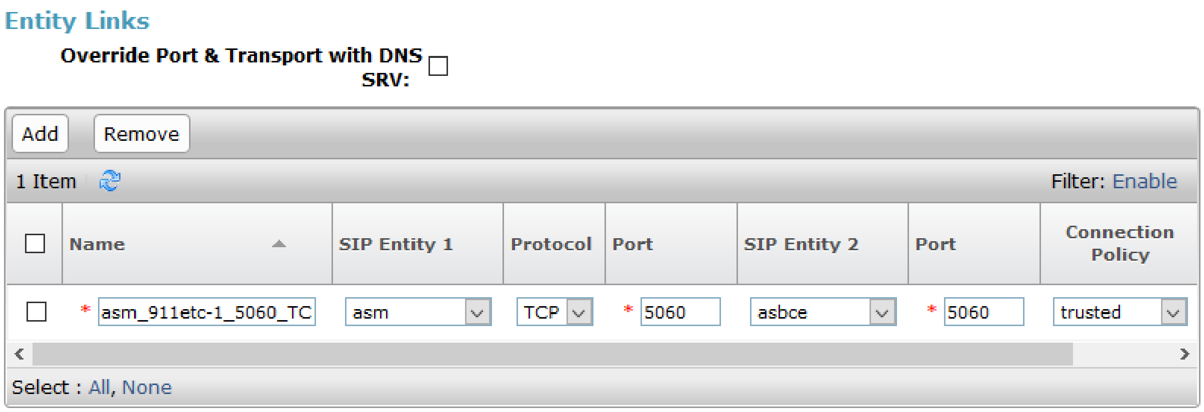
- Enter the **Name** and **FQDN or IP Address**
- Type in the IP Address of **FQDN or IP Address**
- Select the location configured in **Section 5.2** from the **Location** drop down menu

Under **Entity Link**, select **Add.**

- Type in a name in **Name**
- For **SIP Entity 1** select Session Manager, preconfigured asm in this case.
- For **Protocol** select **TCP**
- For **SIP Entity 2** select the SIP Entity that is currently being configured.

For Compliance testing the following information was used.



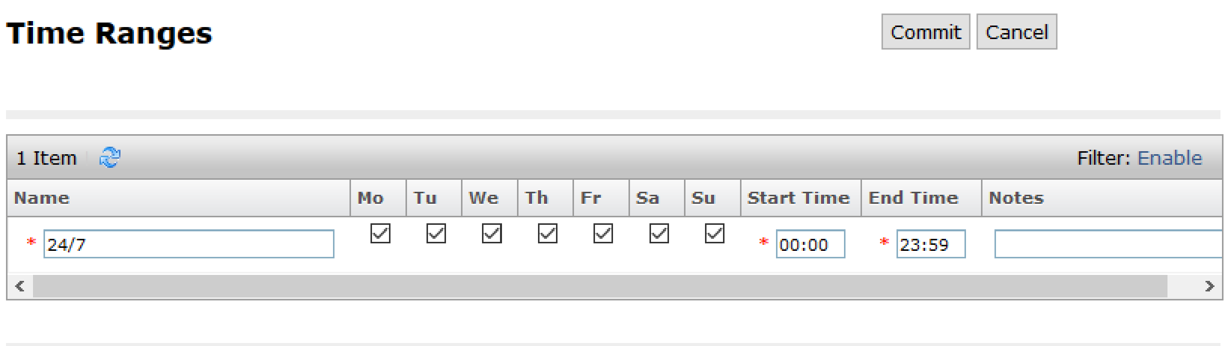


5.4. Configure Time Range

On the left pane, Click on **Time Ranges**. On the Time Range page, click on **New**.

- Type in the **Name** of the time range
- Select the Days and **Start Time** and **End Time** used for all days

For Compliance testing the following information was used.

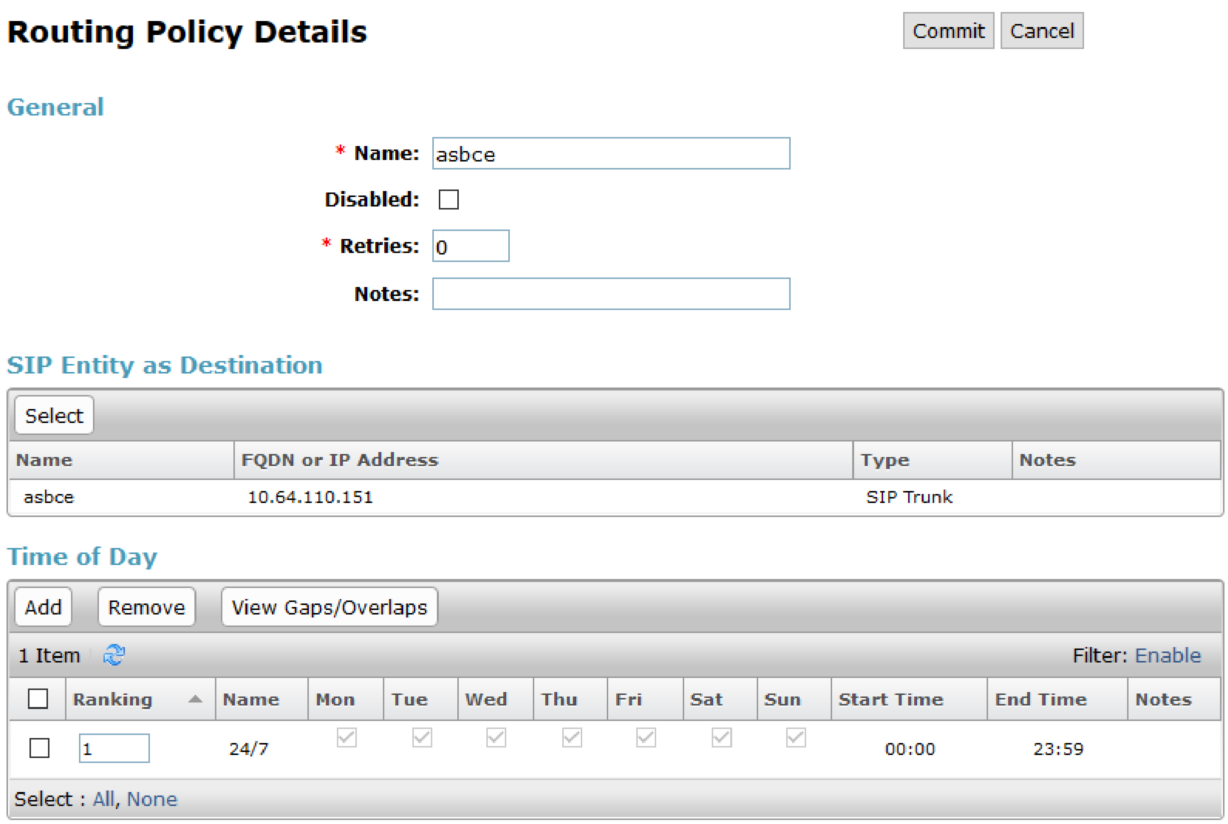


5.5. Configure Routing Policy

On the left pane, click on **Routing Policy.** On the **Routing Policy** page, click on **New**.

- Type in the **Name** for Routing Policy
- Under **SIP Entity as a destination** click **Select**
  - Select SIP Entity configure in **Section 5.3** (not shown)
- Select a **Time Range** added in **Select 5.4**

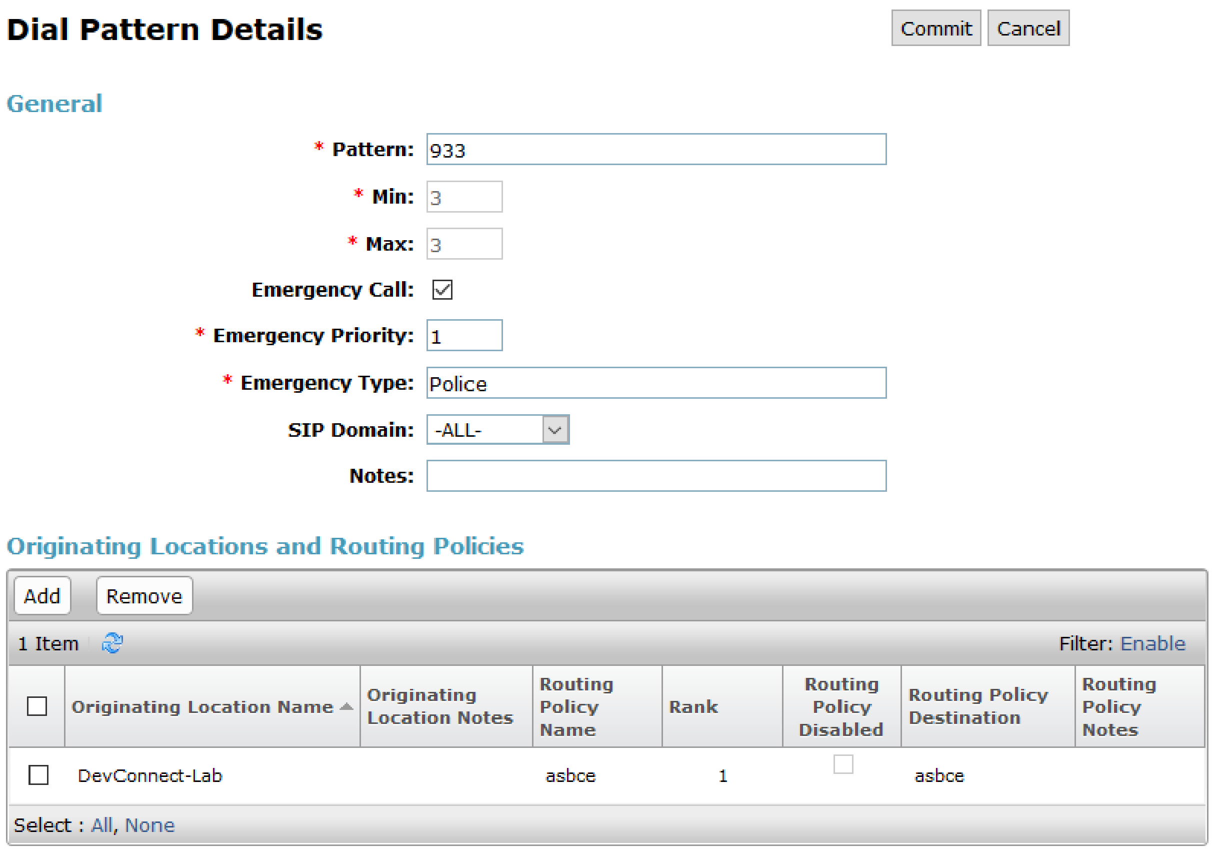
For Compliance testing the following information was used.



5.6. Configure Dial Pattern

On the left pane, click on **Dial Patterns.** On **Dial Patterns** page, click on **New**.

- Set **Pattern** to **933**
- Set **Min** and **Max to** 3
- Set **SIP Domain** to the domain configured in **Section 5.1**
- Add **Originating Locations and Routing Policies** (not shown)
    - Select location configured in **Section 5.2**
    - Select Routing Policy configured in **Section 5.5**
- Type in a number in **Emergency Priority**
- Type in the nature of the dial pattern number in **Emergency Type**
- Add a **Dial Pattern** for **911** as well (not shown).



6. Configure Avaya Aura® Communication Manager

This section describes the Communication Manager configuration to support connectivity to the Session Manager and related functionality.

The configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

6.1. Configure Node Names

Use the **change node-names ip** command to create node names for Session Manager. The example below shows the node names and IP addresses used for the compliance test. These node names will be used in the administration of other forms in Communication Manager.

```
change node-names ip asm                                         Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
asm                 10.64.110.13
cms17               10.64.10.85
default             0.0.0.0
procr               10.64.110.10
procr6              ::
```

6.2. Configure Location

Use the **change locations** command to configure for a specific location. During the compliance test, **location 1** was as shown below:

```
change locations                                                Page   1 of   1
                                   LOCATIONS

                ARS Prefix 1 Required For 10-Digit NANP Calls? y

Loc  Name          Timezone DST     City/ ARS Atd      Disp   Prefix   Proxy Sel
 No                 Offset          Area  FAC FAC      Parm              Rte Pat
1    Main            + 00:00  0                         1
2    Branch          + 00:00  0                         1
3                        :
4                        :
5                        :
6                        :
7                        :
8                        :
9                        :
10                       :
11                       :
12                       :
13                       :
14                       :
```

6.3. Configure Network Map

To configure a single extension for a given network address, use the **change ip-network-map** command. Specify the **IP Address** range and assign an extension in **Emergency Location Ext**. When an emergency call is placed from a phone in the specified range, the Emergency Location Ext that is configured will be used as the Calling Party Number.

```
change ip-network-map                                           Page   1 of  63
                               IP ADDRESS MAPPING

                                              Subnet Network     Emergency
 IP Address                                   Bits   Region VLAN Location Ext
 -------------------------------------------- ------ ------ ---- -------------
 FROM: 10.64.10.0                             /24    1      n    11001
   TO: 10.64.10.255
 FROM:                                        /             n
   TO:
 FROM:                                        /             n
   TO:
 FROM:                                        /             n
   TO:
 FROM:                                        /             n
   TO:
 FROM:                                        /             n
   TO:
 FROM:                                        /             n
   TO:
 FROM:                                        /             n
```

6.4. Configure Network Region

The Communication Manager, Session Manager and VoIP (H.323/SIP) endpoints were located in a single IP network region (IP network region 1) using the parameters described below. Use the **display ip-network-region** command to view these settings. By default, both all elements will also be in IP network region 1 unless specifically placed in a separate region using the **ip-network-map** command. The example below shows the values used for the compliance test.

- A descriptive name was entered for the **Name** field.
- Set the **Location** to the location configured in previous section.
- **IP-IP Direct Audio** (shuffling) was enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway or Avaya Aura® Media Server. This is the default setting. Shuffling can be further restricted at the trunk level on the **Signaling Group** form.
- The **Codec Set** field was set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected. This is the codec set that will be used for calls between the 911 ETC and Communication Manager, via Session Manager since all components are in IP network region 1.
- The default values were used for all other fields.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Main                  Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

6.5. Configure Codecs

Use the **change ip-codec-set 1** command to define the codecs used by IP codec set 1. 911 ETC recommends use of G.711MU codec. However, G729 was also successfully tested. For compliance test, G.711MU was primarily used.

```
change ip-codec-set 1                                       Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2:
 3:
```

6.6. Configure Signaling Group

Use the **add signaling-group *n*** command, where ***n*** is an unused signaling group, to create a new signaling group for each SIP trunk to Session Manager. For compliance test, signaling group 1 was created for the trunk to the Session Manager. Signaling group 1 was configured using the parameters highlighted below. Default values were used for all other fields.

- Set the **Group Type** to ***sip***.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Communication Manager.
- Set the **Far-end Node Name** to ***asm***.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to ***5061***.
- Set the **Far-end Network Region** to ***1***. This is the IP network region which contains the Session Manager.
- The default values were used for all other fields.

```
add signaling-group 1                                       Page   1 of   3
                                SIGNALING GROUP

 Group Number: 1             Group Type: sip
  IMS Enabled? n       Transport Method: tls
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                Far-end Node Name: asm
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1

Far-end Domain: avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                  Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 6
```

6.7. Configure Trunk Group

Use the **add trunk-group *n*** command, where ***n*** is an unused trunk group, to create a new trunk group for each SIP trunk to Session Manager. For the compliance test, trunk group 1 was created for the trunk to Session Manager. Trunk group 1 was configured using the parameters highlighted below.

On **Page 1**:

- Set the **Group Type** to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** to ***tie***.
- Set the **Member Assignment Method** to ***auto***.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of channels available in this trunk. For the compliance test, the number of members was chosen to be ***10***.
- The default values were used for all other fields.

```
add trunk-group 1                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 1                   Group Type: sip           CDR Reports: y
  Group Name: asm                        COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 1
                                                    Number of Members: 10
```

On **Page 3**:

- Set the **Format** field to ***private***. This field specifies the format of the calling party number sent to the far-end.
- The default values were used for all other fields.

```
add trunk-group 1                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no
```

6.8. Configure Private Numbering

Public unknown numbering defines the calling party number to be sent to the far-end. An entry was created that will be used by the trunk groups defined in **Section 6.7**. In the example shown below, all calls originating from a 5-digit extension beginning with 1 and routed across any trunk group will be sent as a 11-digit calling number.

```
change private-numbering 0                                        Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext            Trk        Private          Total
Len Code           Grp(s)     Prefix           Len
 5  1                         1303538          11       Total Administered: 3
 10 7                                          10        Maximum Entries: 540
```

6.9. Configure Automatic Route Selection (ARS)

For the compliance test, ARS was used to route emergency calls to 911 ETC via Session Manager. The dialed string of 9 was configured as the feature access code (FAC) for ARS. Use the **change ars analysis** command to create an entry in the ARS table. Accessing ARS without first dialing the FAC, is only possible if the **ARS/AAR Dialing without FAC** field is enabled. Use the **display system-parameters customer-options** command to view its current state. In either case, the preceding 9 is removed by ARS before searching the table for a matching entry.

For the current compliance test, only the user dialed string of 9911 was tested.

```
change ars analysis 9                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 2

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    9                     7    7     2        hnpa         n
    911                   3    3     1        emer         n
    933                   3    3     1        emer         n
```

6.10.Configure Route Pattern

Use the **change route pattern *n*** command, where ***n*** is an unused route pattern, to create a separate route pattern for each of the dialed strings used for emergency calls in the ARS table. Set the **Pattern Name** field to a descriptive name. Create an entry in the table for each trunk that will be used in an attempt to complete the emergency call.

The example below shows route pattern 1 used in the compliance test. Route pattern 1 was accessed when ARS matches on a dialed string of 911 and 933. For the first entry, set the **Grp No.** field to the trunk group of Session Manager (trunk group 1). Set the Facility Restriction Level (**FRL**) of the trunk to an appropriate level to allow authorized users to access the trunk. The level of ***0*** is the least restrictive.

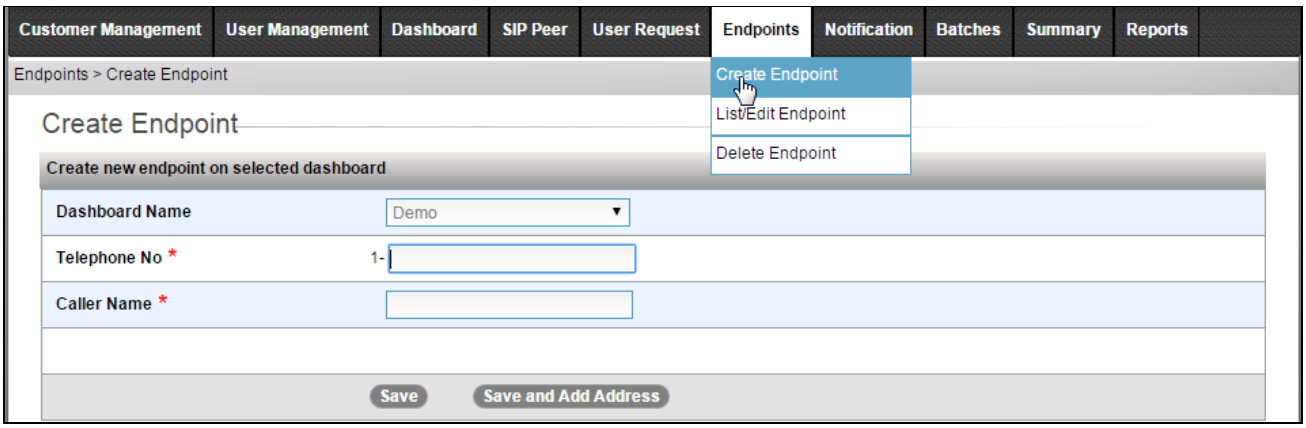
```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1      Pattern Name:
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 1    0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                                        none
 2: y y y y y n  n            rest                                        none
 3: y y y y y n  n            rest                                        none
 4: y y y y y n  n            rest                                        none
 5: y y y y y n  n            rest                                        none
 6: y y y y y n  n            rest                                        none
```

7. Configure 911 ETC CrisisConnect® for VoIP

Customer and 911 ETC need to exchange SIP peering information. 911 ETC will configure their Session Border Controllers based on peering information provided by customer. 911 ETC can provide dashboard access to the customer on request. Data needs to be provisioned prior to testing. Below are the steps to provision data via 911 ETC dashboard.

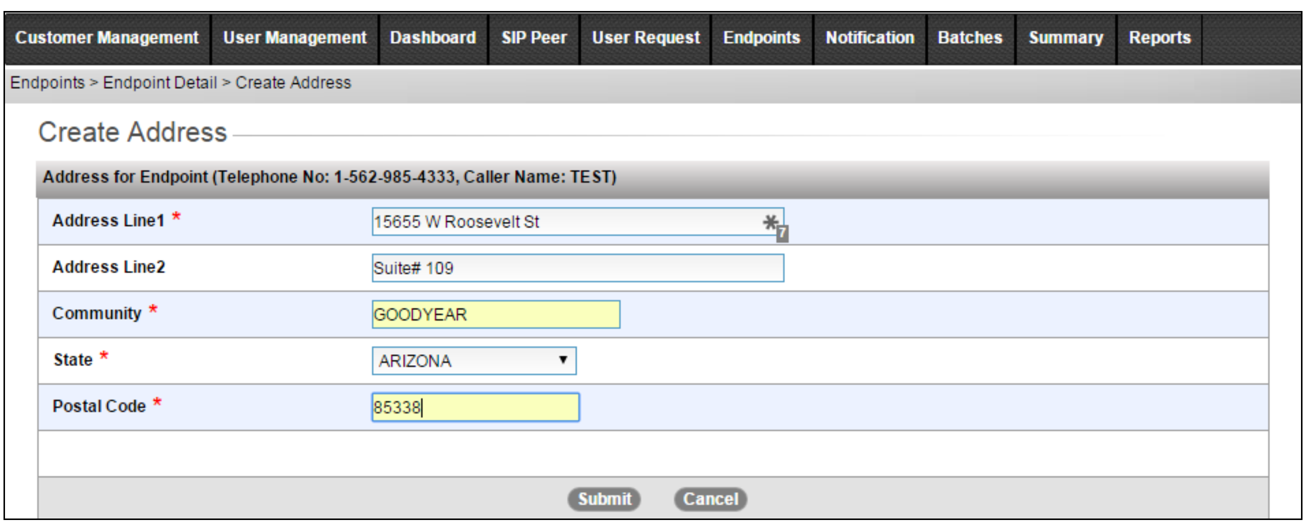
1. 911 ETC will setup customer and dashboard.

2. Configure endpoint: Select **Endpoints → Create Endpoint**; Type in **Telephone No** and **Caller Name** and click S**ave and Add Address**.

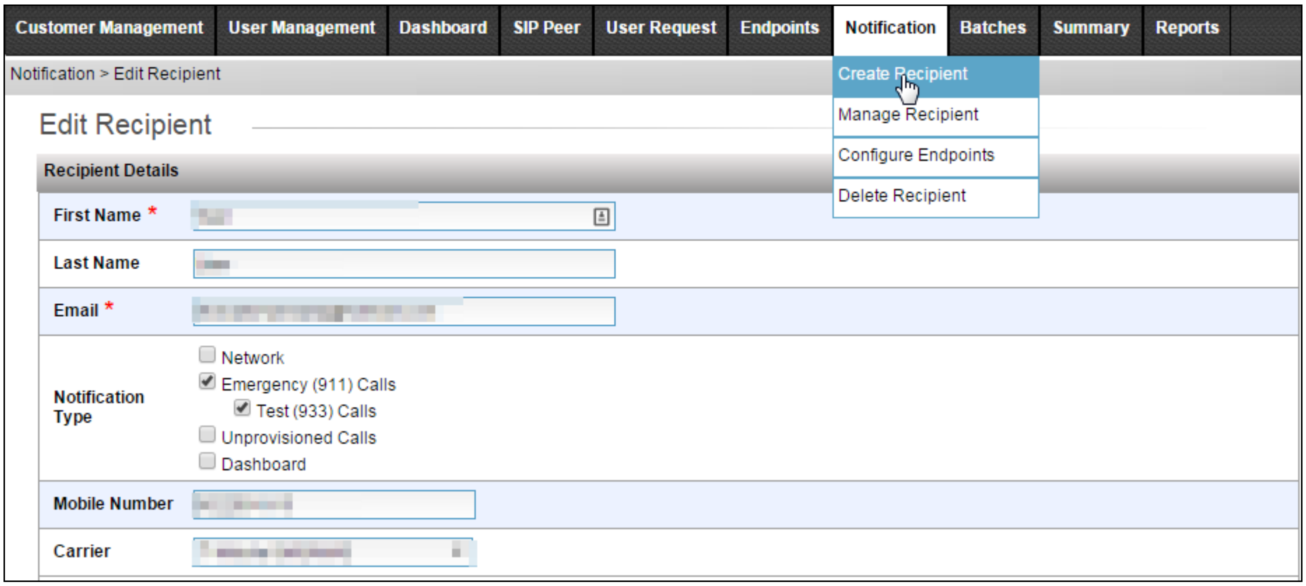


3. Enter **Address Line1** and **Address Line2**, **Community**, **State** and **Postal Code** and click **Submit**.

   Note: **Address ine2** contains all the additional information pertaining to an address, i.e., Suite 109. Address Line2 is an optional parameter.



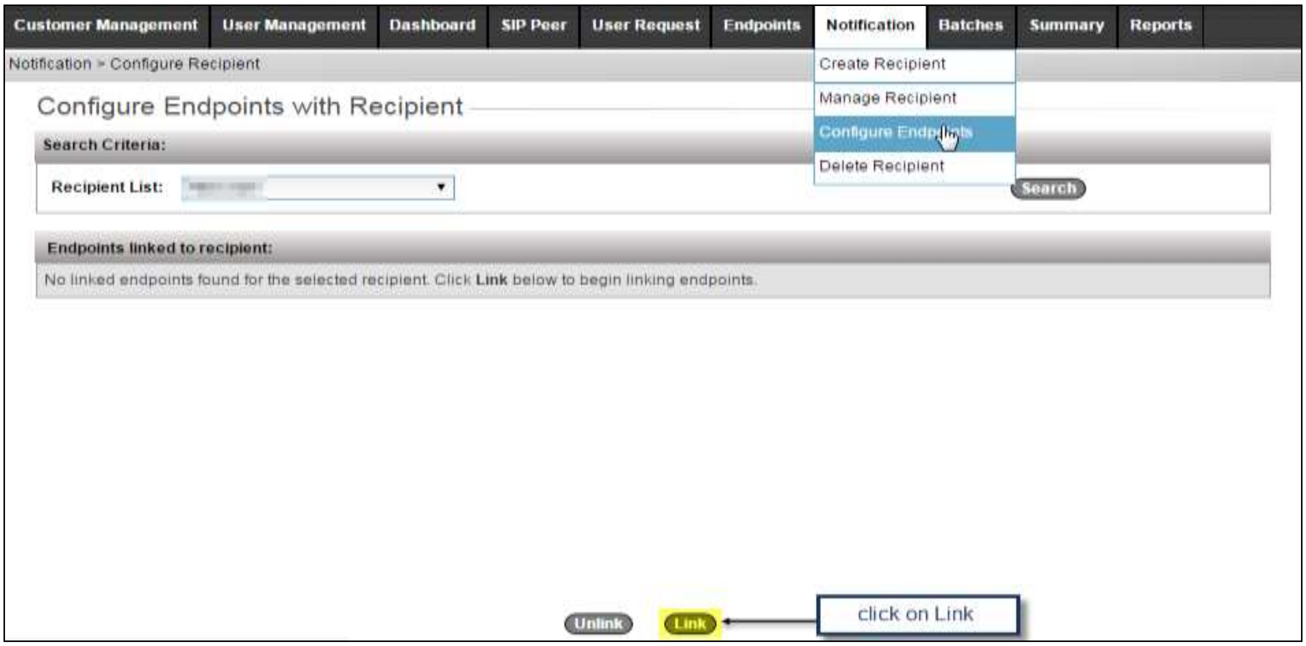
4. In order to create a recipient for Text and Email notification, select **Notifications → Create Recipient**. Provision **First** and **Last Name**, **Email**, **Notification Type**, **Mobile Number** and **Carrier**.



Note:

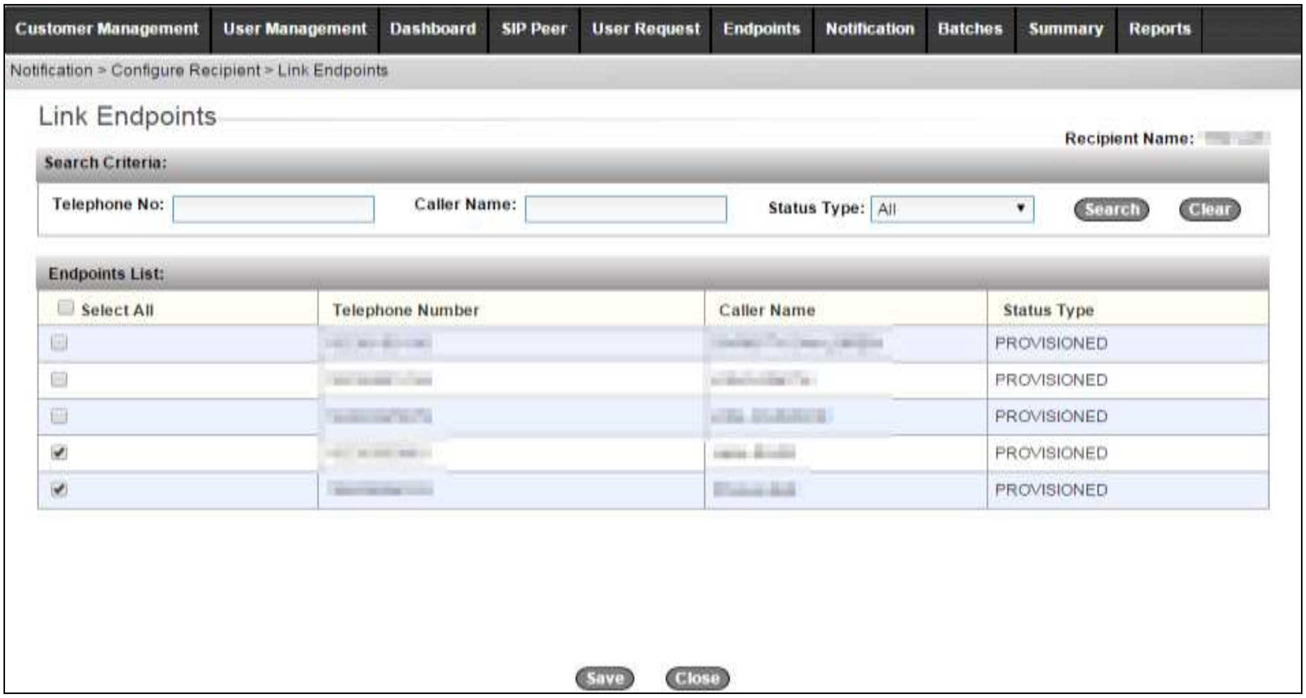
- Notifications may be truncated when using SMS as carriers generally limit SMS messages to 160 characters. If possible, select an MMS enabled carrier.
- SMS and MMS notifications make use of the carrier's email-to-SMS gateway. Carriers may limit usage or place other restrictions on messages.
- Carriers may apply a fee for received SMS/MMS messages. Consult your carrier for fees associated with received SMS/MMS messages.

5. To link a recipient to specific endpoints in the dashboard, so that the recipient receives notifications only when specific endpoints makes an emergency call, select **Notification → Configure Endpoints** and then click **Link** at the bottom.

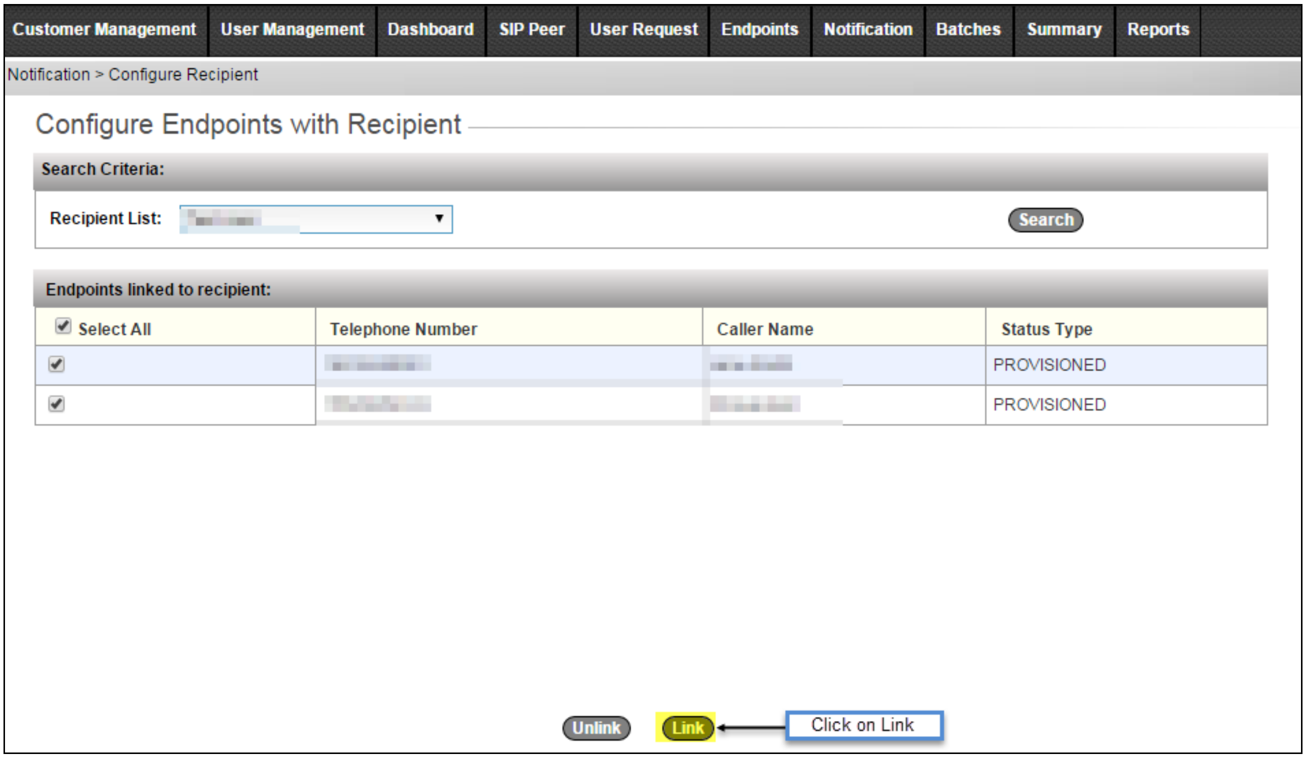


6. Select the endpoints that need to be configured for receiving notifications; click **Save**.

Note: If the recipient is not linked to an endpoint or endpoints, it will receive notification for every endpoint in the dashboard that makes an emergency call.



7. Select all the endpoints and click **Link** at the bottom.



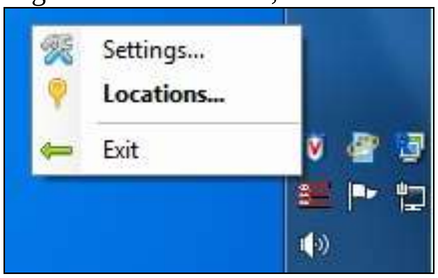
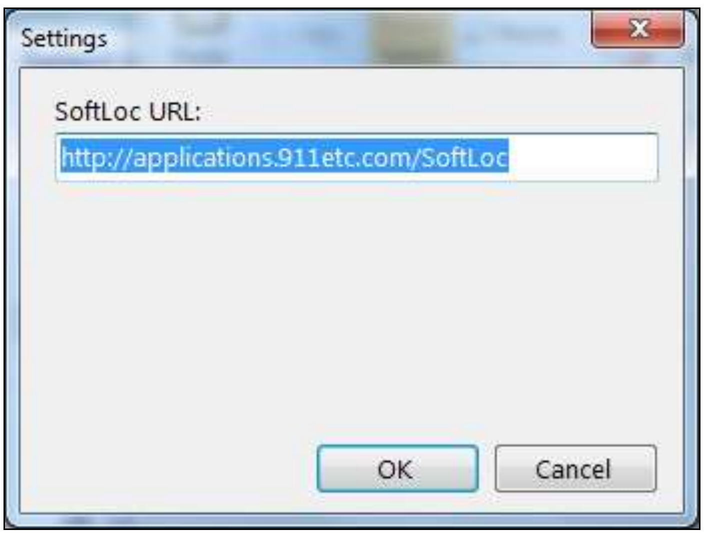
8. Configure 911 ETC CrisisConnect® for SoftPhones

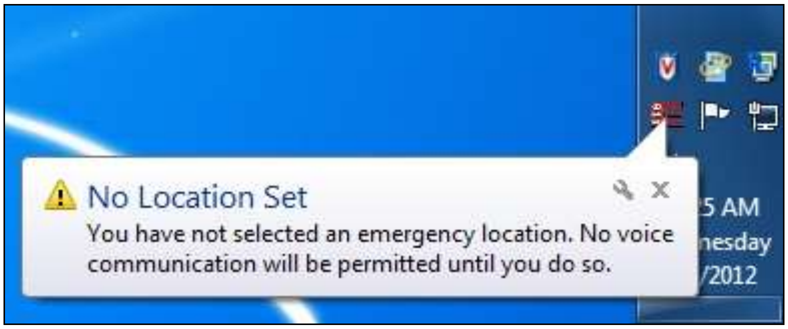
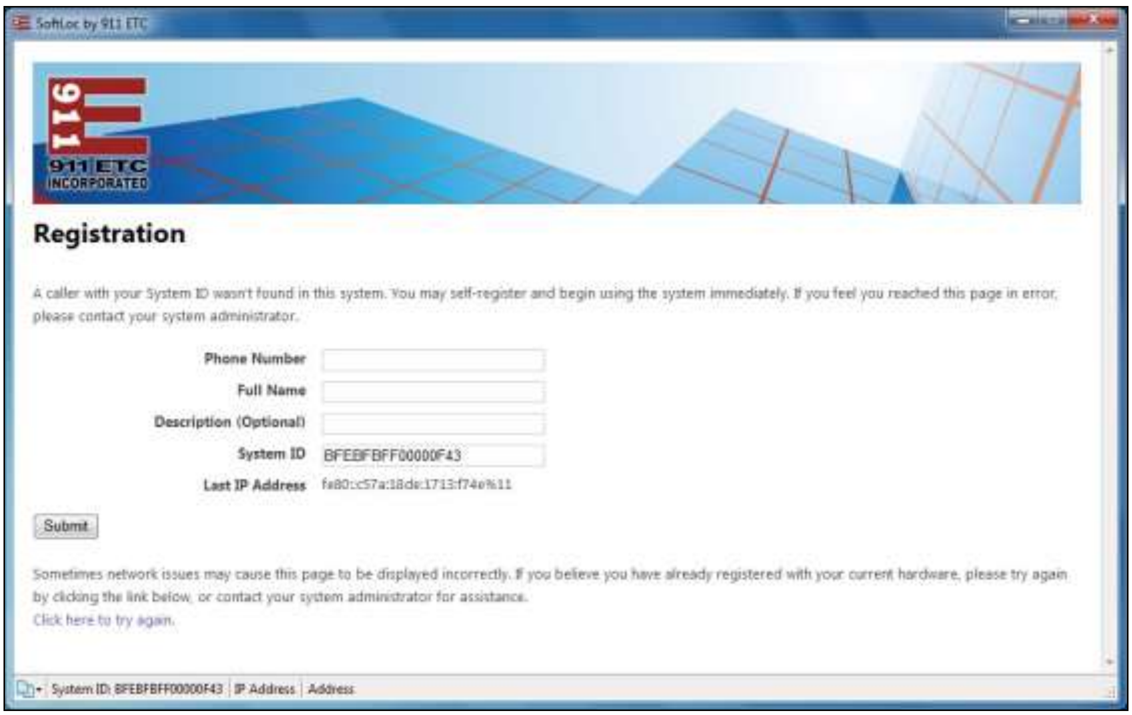
Step	Description
1.	SoftLoc™ server is configured using a browser. Enter the URL of SoftLoc™ server such as http://<hostname>/SoftLoc where <hostname> is the IP address or qualified domain name of the SoftLoc™ server. Login using appropriate credentials.

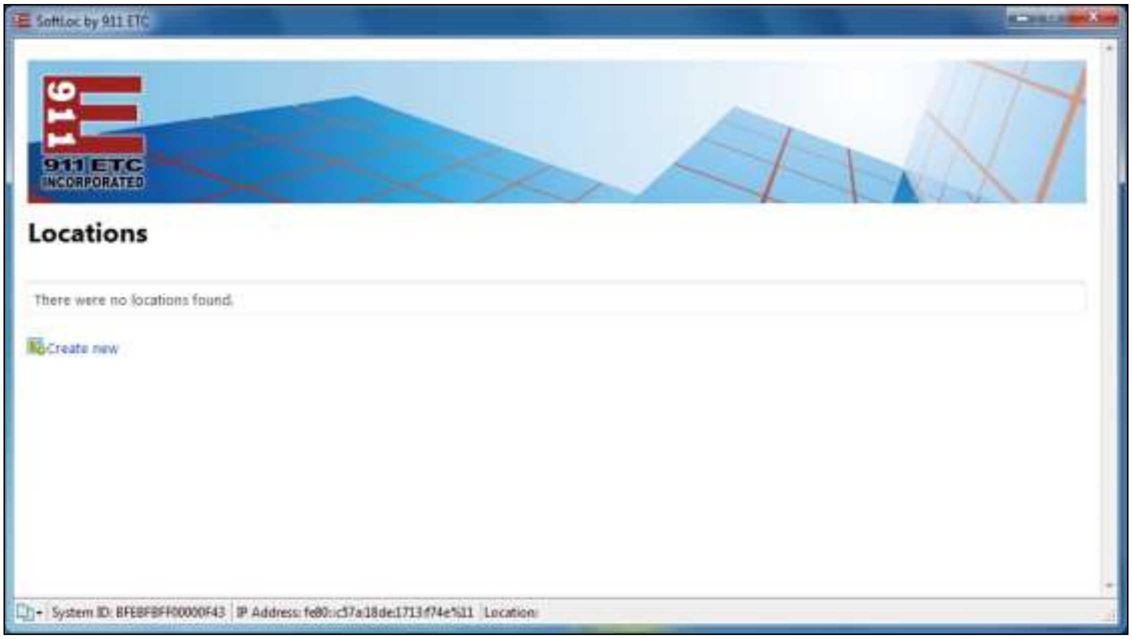
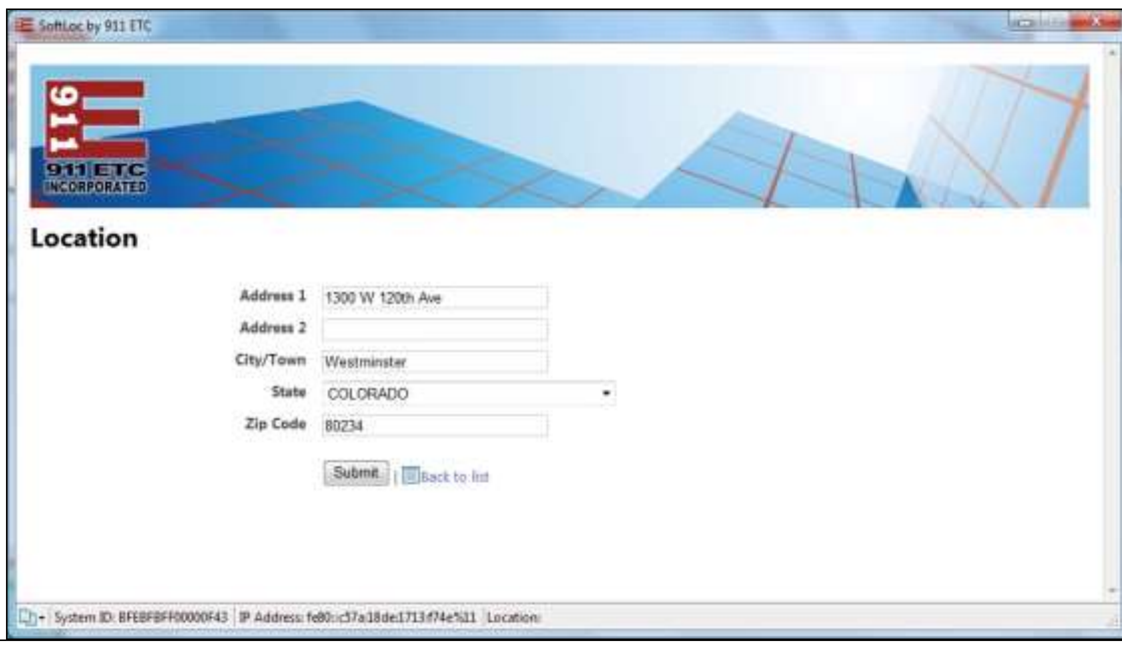
Step	Description
2.	Click on the **Applications** tab, and ensure that **Force soft phone to quit if no location is specified** box is checked 
3.	On the **Applications** page, click on **Create new** • Type in **onexcui.exe** and click on **Create new** 

Step	Description
4.	Newly added Application will show on the **Application** page 

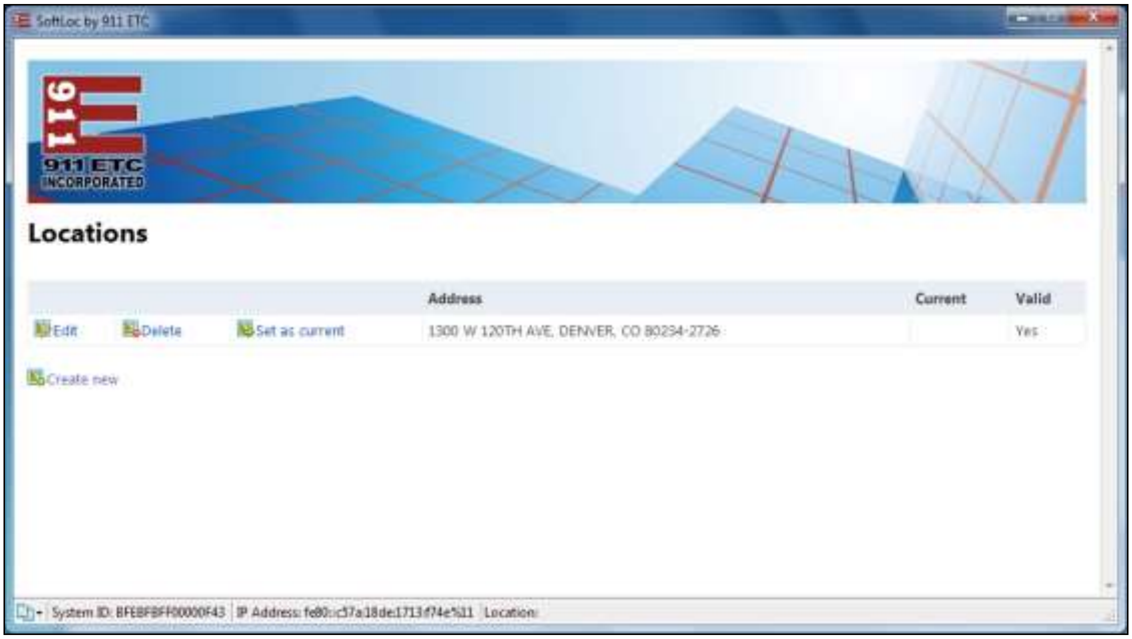
8.1. Configure SoftLoc™ Client

Step	Description
1.	After a SoftLoc™ Client is installed on a workstation that has Avaya one-X® Communicator client installed, 911 ETC icon will appear in the task bar area of Windows desktop • Right click on the icon, and click on settings 
2.	A pop up window will appear; type in the URL of SoftLoc™ server. E.g. http://<hostname>:8080 where <hostname> is the IP address or qualified domain name of the SoftLoc™ server 

Step	Description
3.	A notification will pop up in the notification area of windows desktop, alerting user that a Location needs to be set. Click on the Notification. 
4.	A pop up window with Registration page will appear, prompting user to register. Fill in the registration information and submit. 

Step	Description
5.	After registration is completed, **Locations** page is displayed. 
6.	Click on **Create new** and fill in users' address information. **Submit** once done. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>7.</td><td>Users’ address will now be displayed in Locations page.



</td></tr>
<tr><td>8.</td><td>Click on Set as current to make the address as user’s current address. Current will show up under current column confirming that the address has been set as user’s current address. User can add up to 3 addresses.

</td></tr>
</table>

9. Verification Steps

911 ETC suggests that calls to 933 (Address Verification Systems) are placed to confirm the routing to 911 ETC. After the configuration is complete, verify that the Address Verification System can be reached by dialing 933.

Verify that an email or SMS notification is received. Below are the screen captures of Email and SMS notifications.

Email:

911/933 Call Notification

An emergency call has occurred and you are registered to receive notifications.
Call details:
Subscriber Name: **AvayaTest_6**
Location: **12121 GRANT ST, THORNTON, CO 80241**
Telephone: **13035381002**
Call Start Time: **2/25/2016 2:36:28 PM MST**
Call Status: **Started**
Location information was retrieved from the **'AvayaAura Test'** dashboard.
If you believe this notification is in error, please contact customer service at (480)719-8556 or by email at customerservice@911etc.com so that we can assist.
Thank you,
Customer Service
911 Emergency Telecom Company
(480)719-8556
customerservice@911etc.com

SMS:

911 Emergency Call Notification
Subscriber Name: Keyur Amin
Location: 12121 Grant St, RM 205, Thornton, CO 80241
Telephone: 13035380123
Call Start Time: 2/17/2016 1:50:08 PM
Call Status: Started

10. Conclusion

911 ETC's CrisisConnect® successfully completed compliance testing. These Application Notes describe the procedures required to configure the connectivity between Avaya Aura® environment and the 911 ETC CrisisConnect® as shown in **Figure 1**.

11. Additional References

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

[1] *Deploying Avaya Aura® System Manager, Release 7.0, August 2015*

[2] *Administering Avaya Aura® System Manager, Release 7.0, August 2015*

[3] *Deploying Avaya Aura® Session Manager on VMWare, Release 7.0, August 2015*

[4] *Administering Avaya Aura® Session Manager, Release 7.0, August 2015*

[5] *Deploying Avaya Aura® Communication Manager in Virtualized Environment, Release 7.0, August 2015*

[6] *Deploying and Updating Avaya Aura® Media Server Appliance, Release 7.7, October 2015*

[7] *Implementing Avaya Aura® Media Server, Release 7.7, January 2016*

[8] *Deploying Avaya Aura® Communication Manager Messaging, Release 7.0, September 2015*

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.