Avaya Solution & Interoperability Test Lab

Application Notes for RedSky Technologies E911 Manager, E911 Anywhere, Emergency On-Site Notification and MyE911 with Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration consisting of Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services, and RedSky E911 Manager, E911 Anywhere, Emergency On-Site Notification and MyE911 Client.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 Aura® Session Manager (Session Manager), Avaya Aura® Communication Manager (Communication Manager) and Avaya Aura® Application Enablement Services (AES), and RedSky E911 Manager, E911 Anywhere and Emergency On-Site Notification.

The purpose of RedSky E911Manager is to provide or update emergency numbering and location information for endpoints on Communication Manager and Session Manager. When a Public Safety Answering Point (PSAP) receives a 911 call, the PSAP searches an Automatic Location Identifier (ALI) database to obtain the specific address/location associated with the Automatic Number Identification (ANI) or the Emergency Location Identification Number (ELIN). ELINs are used to more precisely define the location of a device based on where the device is actually being used, rather than a static location that is generally associated with an ANI of an endpoint or trunk.

RedSky E911 Anywhere is a cloud based service that routes emergency calls to the appropriate PSAP anywhere in the United States as well as provides a proxy for E911 Manager to make updates to the ALI database.

The Emergency On-Site Notification (EON) Client is responsible for alerting the user when a 911 call has been made and all information E911 has about the call. This alert comes in the form of an audible siren as well as an on screen focus. MyE911 Client updates Softphone Users to provision their location to ensure accurate location updates when an emergency call is dialled. If the location is not updated, Softphone user will not be able to logon.

RedSky receives registration information from Session Manager when a SIP Entity Link is established, and when endpoints register with Session Manager. For, SIP Endpoints, the registration information Session Manager provides contains the network address of the endpoint via a SIP PUBLISH message. RedSky in return provides an ELIN associated with the current location of the endpoint via a SIP PUBLISH message. Session Manager uses the ELIN information obtained from RedSky to populate the AP-Loc header in a SIP INVITE when an emergency call is made from a SIP Endpoint. For non-SIP Endpoints, RedSky, via AES' System Management Interface (SMS), retrieves a list of Extensions from Communication Manager and updates the Emergency Location Ext field with an actual ELIN. For calls routed via a SIP Trunk, ELIN is sent in AP-Loc header of a SIP INVITE. For calls routed via a PRI Trunk, ELIN is delivered in Calling Party Number.

Session Managers' support for emergency calling is broader than the emergency services used in North America. Specifics and availability of products and capabilities beyond those used in North America are not covered in these Application Notes. More details can be obtained by consulting with RedSky, or the providers of emergency location solution offered in other locations.

2. General Test Approach and Test Results

The compliance test focused on the interoperability between RedSky E911 Manager, E911 Anywhere, Emergency On-Site Notification and MyE911 Client, with Session Manager, Communication Manager and AES.

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

Interoperability Compliance Testing tested functional tests mentioned below:

- Call setup using SIP (TCP and UDP).
- Codec and DTMF verification using G.711 and Inband, respectively.
- Calls from Analog, Digital, Avaya SIP and H.323 Endpoints.
- Verification of alerts generated by EON Client when dialing emergency number from all types of endpoints.
- Verification of MyE911 Client to update locations for Softphone users.
- Correct ELIN delivery for calls routed via a SIP Trunk and PRI Trunk

In addition to the sunny day scenarios described above, testing included disconnecting network and restarting Entity Links, as well as restarting RedSky servers to verify recoverability of the solution.

Due to the nature of emergency calls, all test calls were routed to the RedSky E911 Anywhere Test System.

2.2. Test Results

All planned test cases were verified and passed.

2.3. Support

Technical support for RedSky products can be obtained at:

- Phone: (866) 778-2435
- Email: support@redskytech.com
- http://www.redskye911.com

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Application Enablement Services
- Avaya Aura® Media Server
- Avaya G450 Media Gateway
- Avaya IP telephones
- RedSky E911 Manager server
- RedSky ELIN Server
- RedSky E911 Anywhere
- RedSky Emergency On-Site Notification Client
- RedSky MyE911 Client

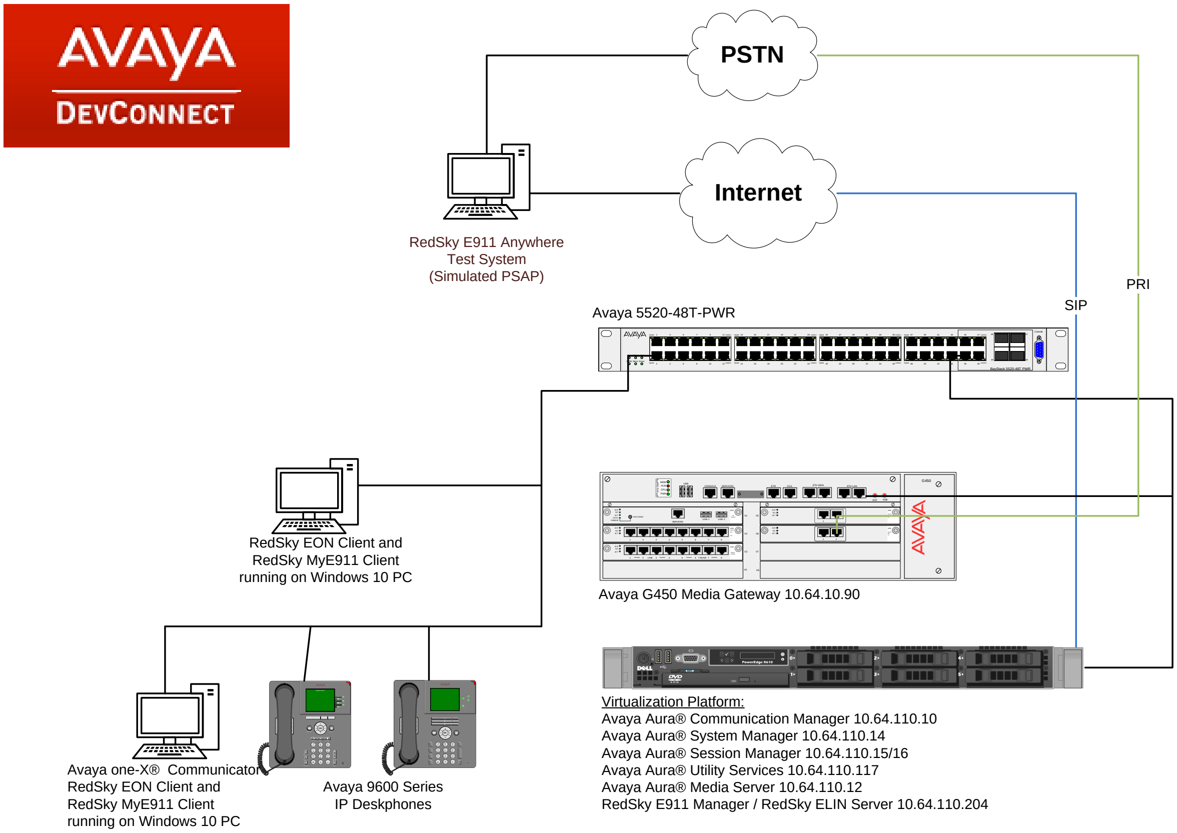

AVAYA
DEVCONNECT
PSTN
Internet
RedSky E911 Anywhere
Test System
(Simulated PSAP)
PRI
SIP
Avaya 5520-48T-PWR
RedSky EON Client and
RedSky MyE911 Client
running on Windows 10 PC
Avaya G450 Media Gateway 10.64.10.90
Virtualization Platform:
Avaya Aura® Communication Manager 10.64.110.10
Avaya Aura® System Manager 10.64.110.14
Avaya Aura® Session Manager 10.64.110.15/16
Avaya Aura® Utility Services 10.64.110.117
Avaya Aura® Media Server 10.64.110.12
RedSky E911 Manager / RedSky ELIN Server 10.64.110.204
Avaya one-X® Communicator
RedSky EON Client and
RedSky MyE911 Client
running on Windows 10 PC
Avaya 9600 Series
IP Deskphones

Figure 1 – Reference Configuration

This reference configuration diagram displays the connectivity between Avaya Environment and RedSky products. RedSky MyE911 client and RedSky Emergency On-Site Notification client were installed on a PC, which ran Avaya one-X® Communicator.

4. Equipment and Software Validated

The following equipment and version were used for the sample configuration provided:

Equipment	Version
Avaya Aura® System Manager	7.0.1.1 SP1
Avaya Aura® Session Manager	7.0.1.1.701114
Avaya Aura® Communication Manager	7.0.1.1.0-FP1SP1
Avaya Aura® Media Server	7.7.0.359
Avaya G450 Media Gateway	37.19.0
Avaya 9600 Series Deskphones	Various
Avaya Aura® Application Enablement Services	7.0.1.0.2.15-0
RedSky Technologies - E911 Manager - E911 Anywhere - Emergency On-Site Notification Client - MyE911 Client	 6.5.5 6.5.5 6.5.5 6.5.5

5. Configure Avaya Aura® Communication Manager

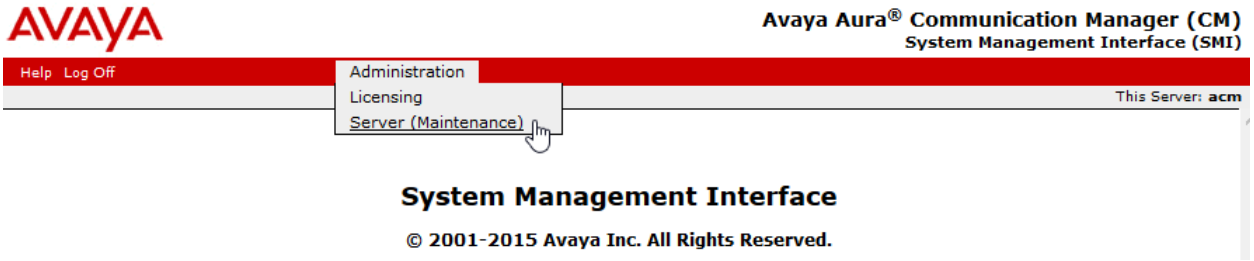
All configurations for Communication Manager are performed via a SAT terminal, unless otherwise noted.

5.1. Add SMS User

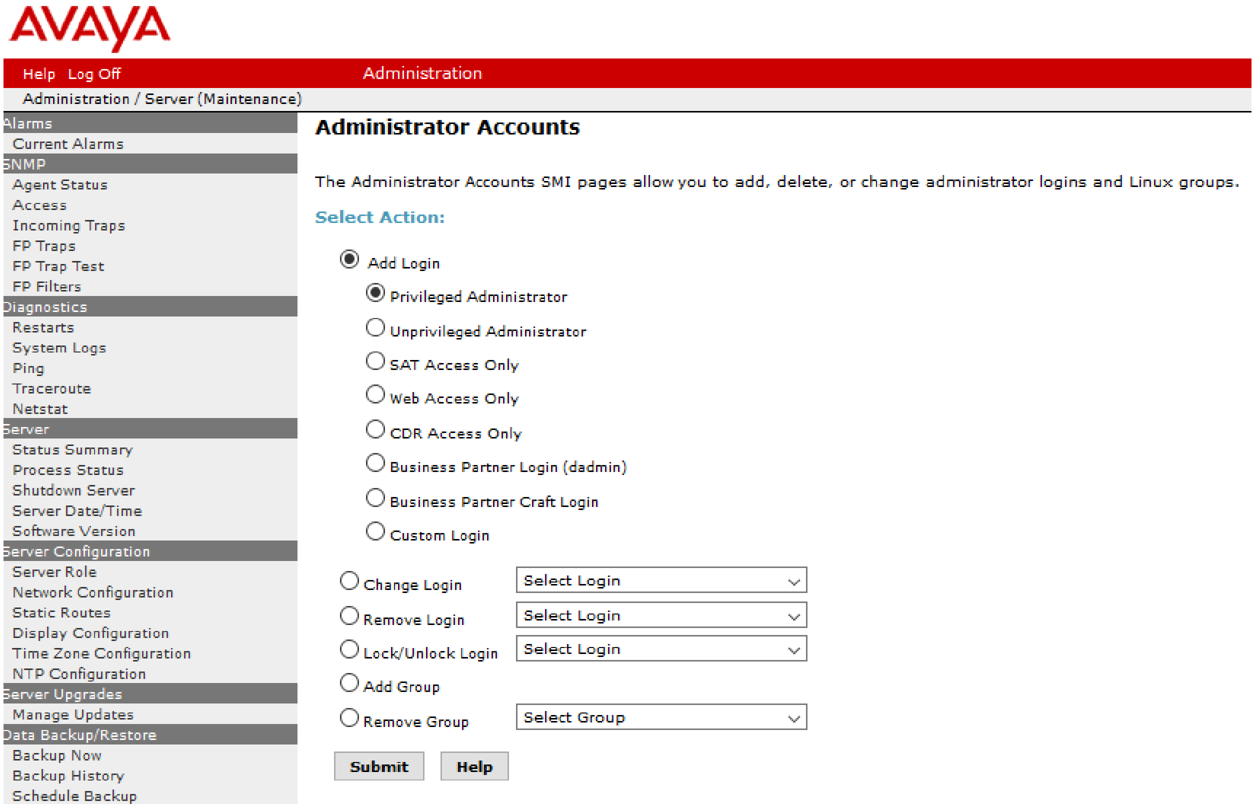
During the compliance test a super-user profile was used when an SMS user was created for RedSky. A list of available profiles can be viewed on Communication Manager using the **list user-profile** command.

```
                                  USER PROFILES

                     Extended
     Profile          Profile     User Profile Name
       0                n         services super-user
       1                n         services manager
       2                n         business partner
       3                n         services
       16               n         call center manager
       17               n         snmp
       18               n         customer super-user
       19               n         customer non-super-user
```

Create an SMS user account on the Communication Manager **System Management Interface** web page, https://<communication-manager-ip-address>. Navigating to **Administration → Server (Maintenance)**


AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help
Log Off
Administration
Licensing
Server (Maintenance)
This Server: acm
System Management Interface
© 2001-2015 Avaya Inc. All Rights Reserved.

On left side menu, select **Administrator Accounts** under **Security**, select **Add Login →** **Privileged Administrator** and **Submit**:



Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

● Add Login
- ● Privileged Administrator
- ○ Unprivileged Administrator
- ○ SAT Access Only
- ○ Web Access Only
- ○ CDR Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ Change Login — Select Login

○ Remove Login — Select Login

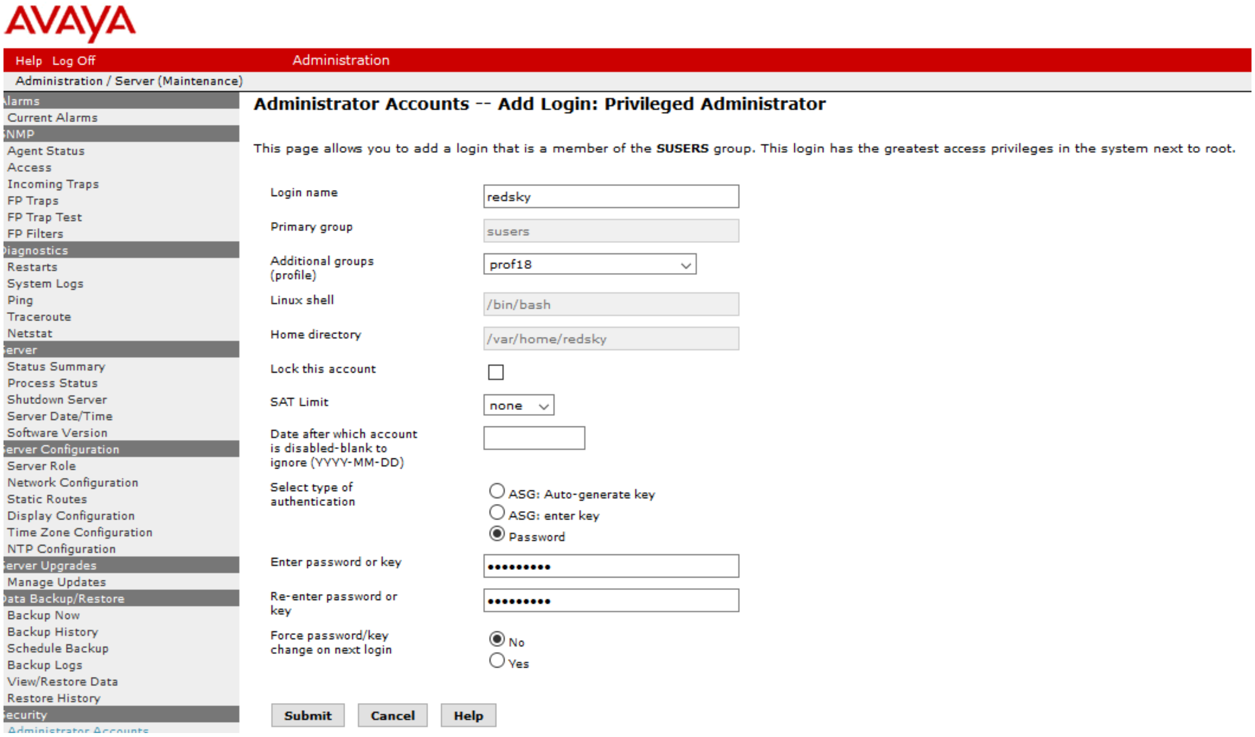
○ Lock/Unlock Login — Select Login

○ Add Group

○ Remove Group — Select Group

On the **Administrator Account – Add Login: Privileged Administrator** page:

- Type in a **Login Name**
- Type in a password in **Enter password or key** and **Re-enter password or key**



Administrator Accounts -- Add Login: Privileged Administrator

This page allows you to add a login that is a member of the **SUSERS** group. This login has the greatest access privileges in the system next to root.

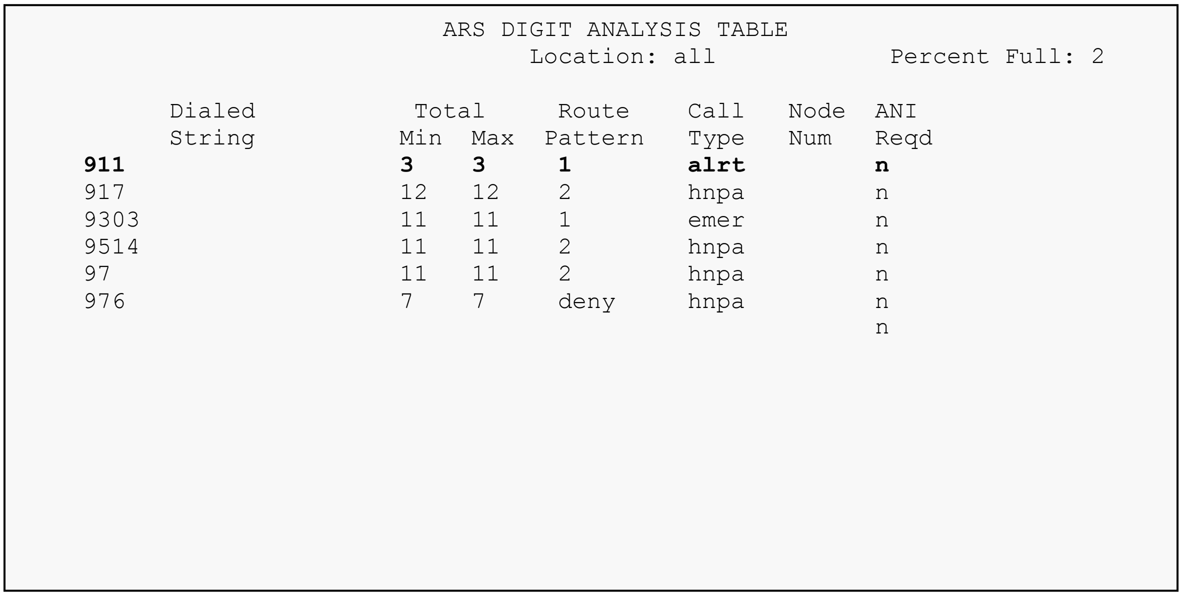
Login name	redsky
Primary group	susers
Additional groups (profile)	prof18
Linux shell	/bin/bash
Home directory	/var/home/redsky
Lock this account	□
SAT Limit	none
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Select type of authentication	○ ASG: Auto-generate key ○ ASG: enter key ● Password
Enter password or key	•••••••••
Re-enter password or key	•••••••••
Force password/key change on next login	● No ○ Yes

5.2. Configure ARS Routing

Configure ars analysis for emergency calls. Use **change ars analysis 911** to configure routing for 911 calls. Add an entry as follows:

- Type in **911** for **Dialed String**
- Set **Total Min** and **Max** to **3**
- Set **Route Pattern** to the route pattern used for the SIP trunk to Session Manager
- Set **Call Type** to **alrt**

If emergency calls are routed via an ISDN Trunk, type in the appropriate value for **Route Pattern.**



```
                              ARS DIGIT ANALYSIS TABLE
                                    Location: all            Percent Full: 2

          Dialed           Total      Route     Call   Node  ANI
          String          Min  Max  Pattern     Type   Num   Reqd
    911                   3    3     1          alrt         n
    917                   12   12    2          hnpa         n
    9303                  11   11    1          emer         n
    9514                  11   11    2          hnpa         n
    97                    11   11    2          hnpa         n
    976                   7    7     deny       hnpa         n
                                                             n
```

Note: Any number that is used to route emergency calls must be added in the ARS table as Call Type of **alrt** type. Setting a dial string to **alrt** has two purposes:

- When an emergency call is made, a crisis alert is sent to the station that is being monitored by RedSky
- In a scenario, where emergency calls are route to PSAP via an ISDN trunk, setting the dial string to **alrt** ensures that the ELIN in AP-Loc header gets converted to Calling Party Number.

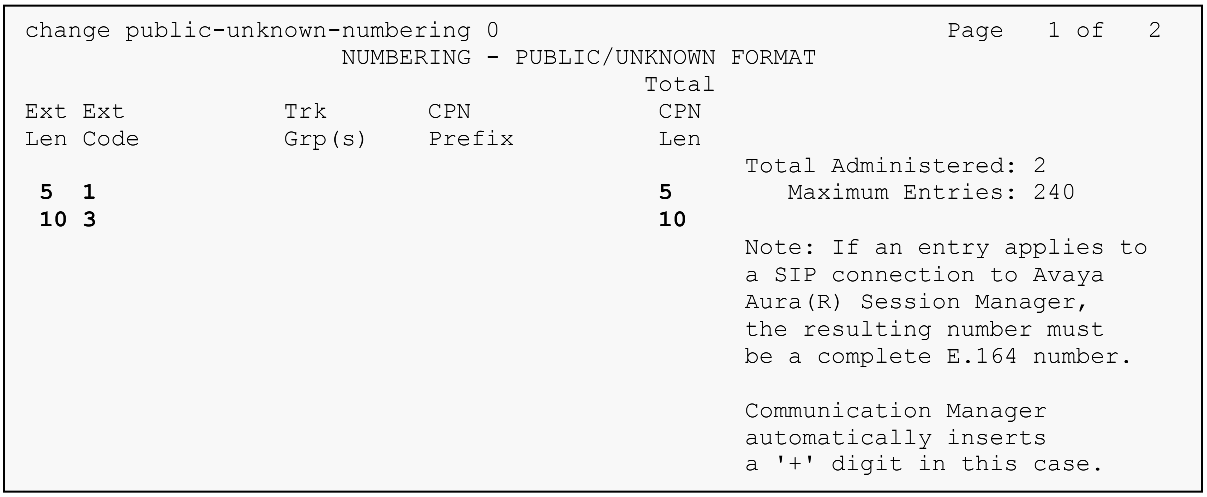
5.3. Configure Public Unknown Numbering

RedSky E911 Manager uses the Public Unknown Number Table to determine the digits that should be written to the Emergency Location Extension (ELE) field, such that the proper ELIN can be out pulsed. Use **change public-unknown-numbering 0** to configure routing for 911 calls.

The requirements are as follows:

- Extension length must equal to the length of the ELE that E911 Manager will write back.
- Extension code must specify the leading digit(s) of the ELE that E911 Manager will write back.
- The appropriate emergency trunk group must be specified.

During Compliance Test, extensions starting with 1 that were 5 digits in length were used.



```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                  Total Administered: 2
 5  1                                       5        Maximum Entries: 240
 10 3                                       10
                                                  Note: If an entry applies to
                                                  a SIP connection to Avaya
                                                  Aura(R) Session Manager,
                                                  the resulting number must
                                                  be a complete E.164 number.

                                                  Communication Manager
                                                  automatically inserts
                                                  a '+' digit in this case.
```

5.4. Configure Crisis Alert

RedSky E911 Manager registers to DMCC service using stations that are administered with IP Softphone enabled in Communication Manager to receive Crisis Alerts.

Add a station that will be used by RedSky E911 Manager to receive Crisis Alerts when emergency calls are placed. Use **add station *n*** command to add a station, where ***n*** is an available extension.

On Page 1:

- Set **Type** to **9630**
- Type in a desired name in **Name**
- Type in a **Security Code**
- Set **IP SoftPhone** to **y**

```
add change station 11001                                      Page   1 of   5
                                     STATION

Extension: 11001                       Lock Messages? n             BCC: M
     Type: 9630                        Security Code: ******         TN: 1
     Port: S00104                    Coverage Path 1:               COR: 1
     Name: RedSky Station            Coverage Path 2:               COS: 1
                                     Hunt-to Station:             Tests? y
STATION OPTIONS
                Location:                  Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 11001
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                  Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal               Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? y

                                               IP Video Softphone? y
                              Short/Prefixed Registration Allowed: default

                                              Customizable Labels? y
```

One Page 4, under **BUTTON ASSIGNMENTS**, add an entry for **crss-alert**.

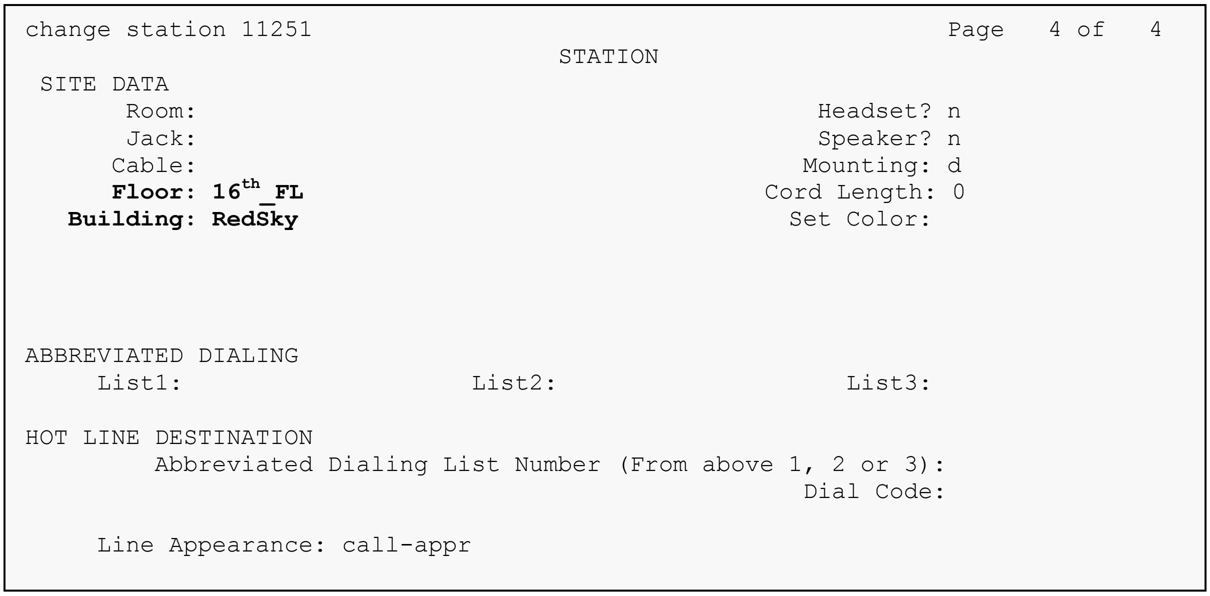
```
add station 11001                                           Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                           Headset? n
       Jack:                                           Speaker? n
      Cable:                                          Mounting: d
      Floor:                                      Cord Length: 0
   Building:                                        Set Color:

ABBREVIATED DIALING
     List1:                   List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                          5:
 2: call-appr                          6:
 3: call-appr                          7:
 4: crss-alert                         8:
```

Next, use **change system-parameters crisis-alert** and set **Every User Responds** to **y**. This ensures that the physical telephones configured with **crss-alert** buttons will continue to be alerted audibility and visually after the RedSky EON server acknowledges the Crisis Alert.

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

ALERT STATION
    Every User Responds? y

ALERT PAGER
            Alert Pager? n
```

5.5. Digital/Analog Phones

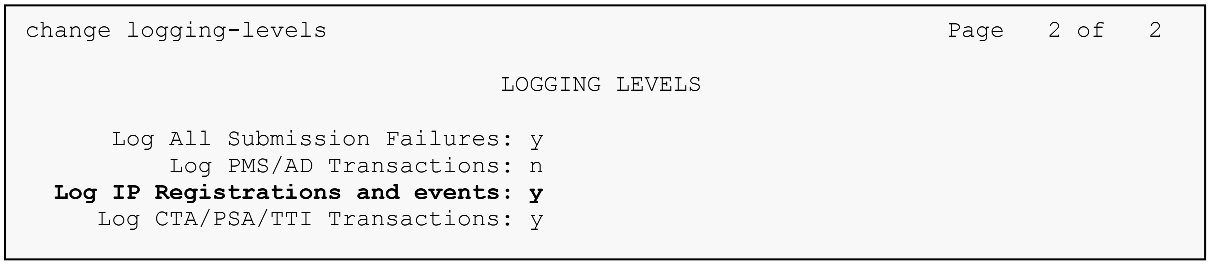
For Analog or Digital phones, the **SITE DATA** page must be utilized to determine their location. E911 Manager reads the **Building**, **Room**, and **Floor** fields to map the location. In order to properly identify the location of a Digital or Analog phone, the **Building** field should match the **Building ID** that is configured in E911 Manager. Additionally, supplemental information may be placed in the **Room** or **Floor** fields. Use **change station *n*** where ***n*** is an analog or digital extension; navigate to **Page 4** to configure **SITE DATA**.



```
change station 11251                                          Page   4 of   4
                                     STATION
 SITE DATA
       Room:                                           Headset? n
       Jack:                                           Speaker? n
      Cable:                                          Mounting: d
      Floor: 16th_FL                               Cord Length: 0
   Building: RedSky                                  Set Color:




ABBREVIATED DIALING
     List1:                   List2:                     List3:

HOT LINE DESTINATION
         Abbreviated Dialing List Number (From above 1, 2 or 3):
                                                       Dial Code:

     Line Appearance: call-appr
```

5.6. IP Phone Registration

In order for E911 Manager to determine when an IP phone registers or unregisters, the logging level for **Log IP Registrations and events** must be set to **Y**. Use **change logging-levels** and navigate to page 2 to verify the logging level.



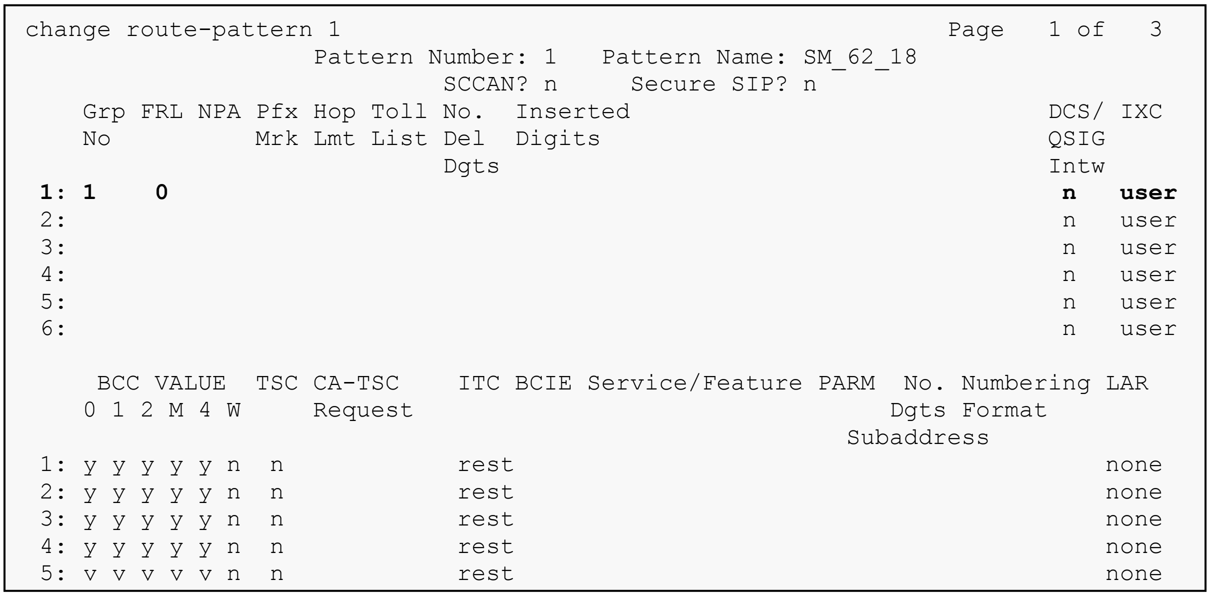
```
change logging-levels                                         Page   2 of   2

                                 LOGGING LEVELS

      Log All Submission Failures: y
          Log PMS/AD Transactions: n
  Log IP Registrations and events: y
     Log CTA/PSA/TTI Transactions: y
```

5.7. Emergency Route Pattern

Configure ars route pattern for emergency calls. Use **change route-pattern n** where **n** is the route pattern configured for the emergency number in the ars analysis table as mentioned in **Section 5.2**.

- Provide a descriptive name in **Pattern Name**
- Set **Grp No** to the trunk group associated with Session Manager

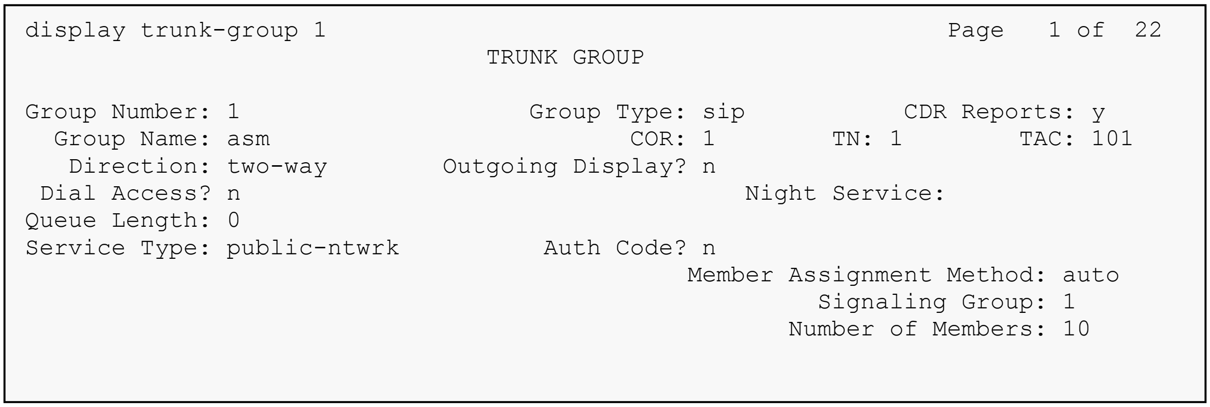
If emergency calls are to be routed via an ISDN Trunk, provide appropriate value for **Grp No**.



```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: SM_62_18
                             SCCAN? n     Secure SIP? 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  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 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: v v v v v n  n            rest                                         none
```

5.8. Emergency Call Trunk Group

Configure the trunk group; use **display trunk-group 1.** There is no specific trunk group configuration, however, there does need to be a trunk group defined. This trunk-group number is the trunk group used when configuring the AES in E911 Manager. Please note that this trunk group is used for routing calls to and from Session Manager and was pre-configured.



```
display trunk-group 1                                           Page   1 of  22
                                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: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

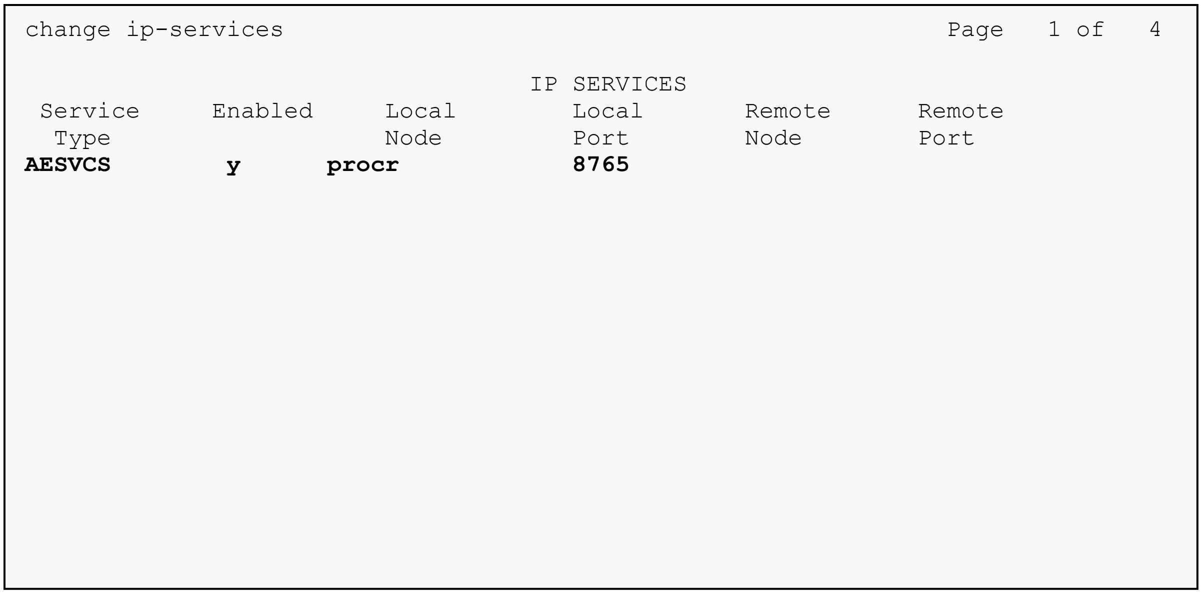
5.9. Configure AES connection

Use **change node-names ip** command to add an entry for AES. Type in a **Name** for AES and AES IP address in **IP Address.**

```
hange node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
acms                10.64.110.18
aes                 10.64.110.15
ams                 10.64.110.16
asm                 10.64.110.13
cms17               10.64.10.85
default             0.0.0.0
procr               10.64.110.10
procr6              ::




( 13 of 13   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Use **change ip-services** command to add an entry for AES. On Page 1,

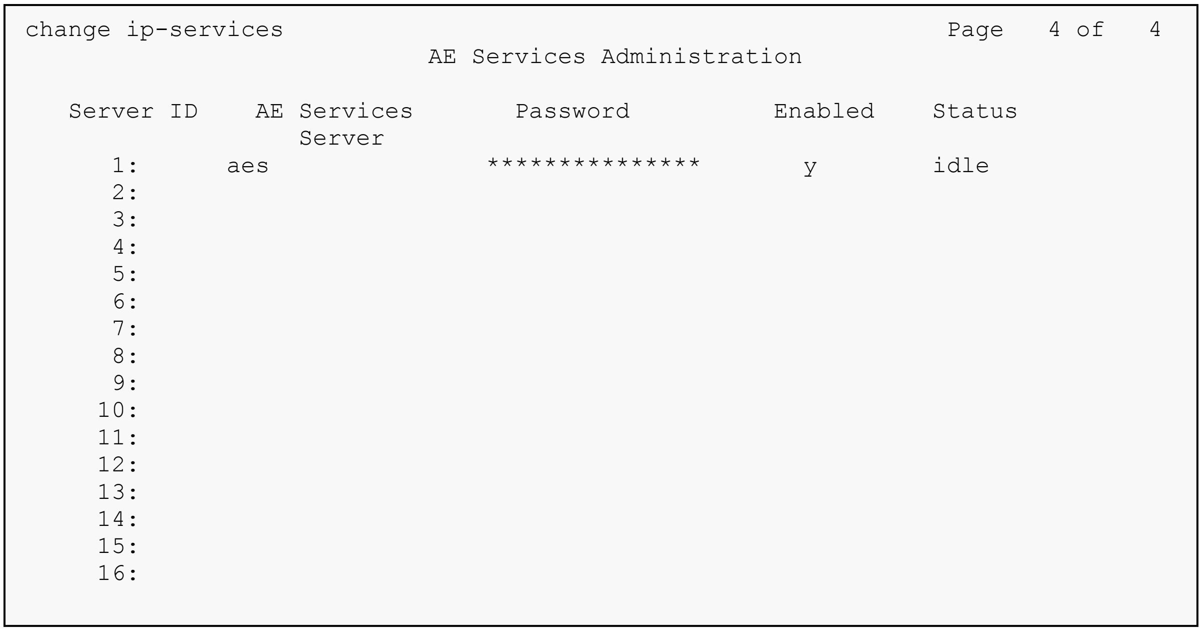
- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.



```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y      procr            8765
```

On Page 4 of the IP Services form, enter the following values:

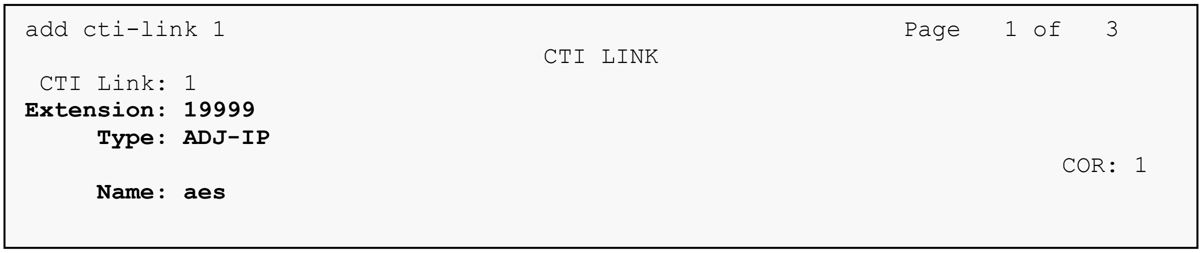
- In the **AE Services Server** field, type the name obtained from the Application Enablement Services server.
- In the **Password** field, type a password to be administered on the Application Enablement Services server.
- In the **Enabled** field, type **y**.



```
change ip-services                                              Page   4 of   4
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      aes              ***************        y        idle
      2:
      3:
      4:
      5:
      6:
      7:
      8:
      9:
     10:
     11:
     12:
     13:
     14:
     15:
     16:
```

Use **add cti-link *n*** command, where ***n*** is an available CTI link number.

- In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.



```
add cti-link 1                                               Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 19999
     Type: ADJ-IP
                                                                        COR: 1
     Name: aes
```

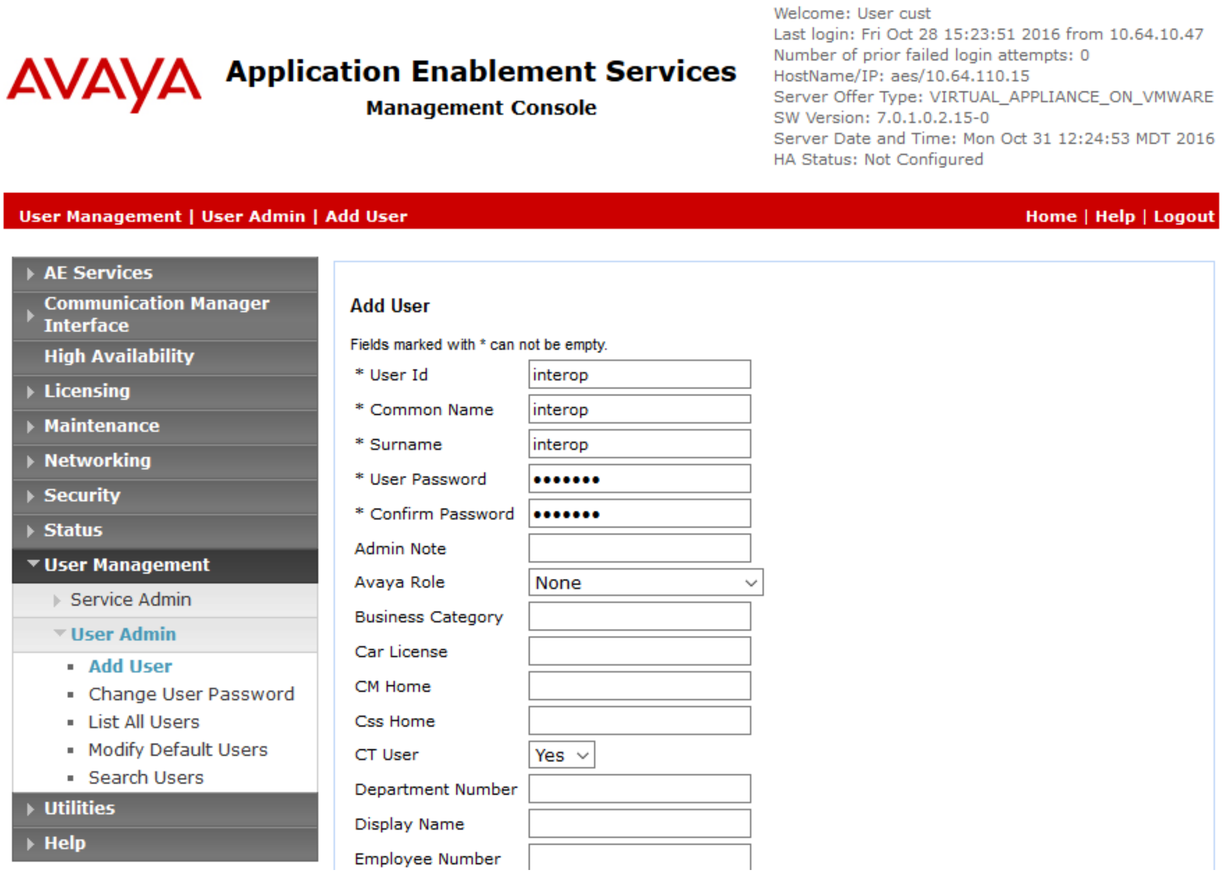
6. Configure Avaya Aura® Application Enablement Services

Configuration of Avaya Aura® Application Enablement Services requires a user account be configured for RedSky E911 Manager.

6.1. Configure Application Enablement Services Details

All administration is performed by web browser, https://<aes-ip-address>/

A user needs to be created for RedSky E911 Manager to communicate with AES. Navigate to **User Management → User Admin → Add User**. Fill in **User Id, Common Name, Surname, User Password** and **Confirm Password**. Set the **CT User** to **Yes,** and **Apply**.



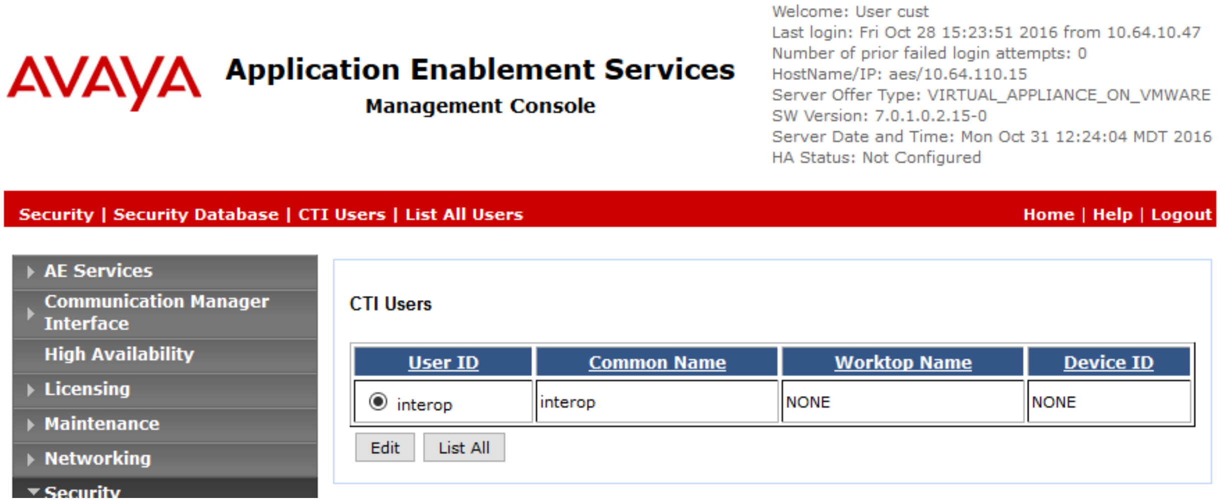
Welcome: User cust
Last login: Fri Oct 28 15:23:51 2016 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.110.15
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Mon Oct 31 12:24:53 MDT 2016
HA Status: Not Configured

Add User

Fields marked with * can not be empty.

* User Id	interop
* Common Name	interop
* Surname	interop
* User Password	•••••••
* Confirm Password	•••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	

On the left side menu, navigate to **Security → Security Database → CTI Users → List All Users**.



AVAYA Application Enablement Services Management Console

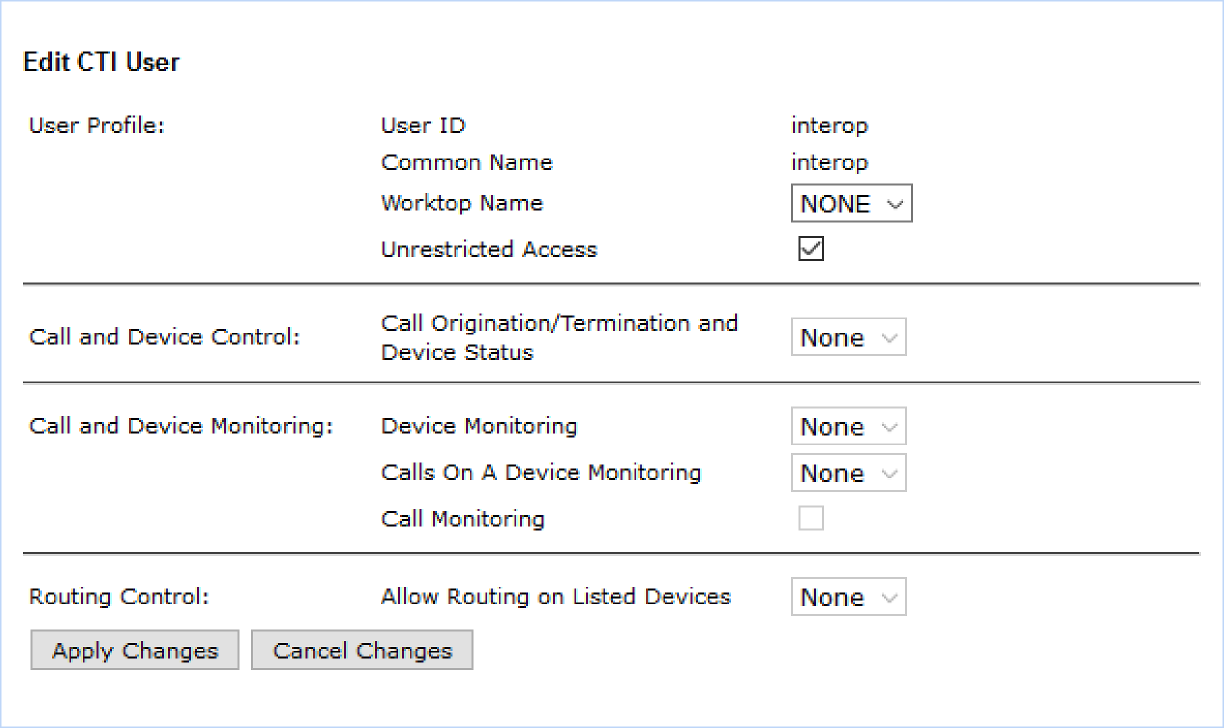
Welcome: User cust
Last login: Fri Oct 28 15:23:51 2016 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.110.15
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Mon Oct 31 12:24:04 MDT 2016
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users
Home | Help | Logout
AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security

CTI Users

User ID	Common Name	Worktop Name	Device ID
● interop	interop	NONE	NONE

Select the recently added user and click **Edit**. Check the box for **Unrestricted Access** and click **Apply Changes**.



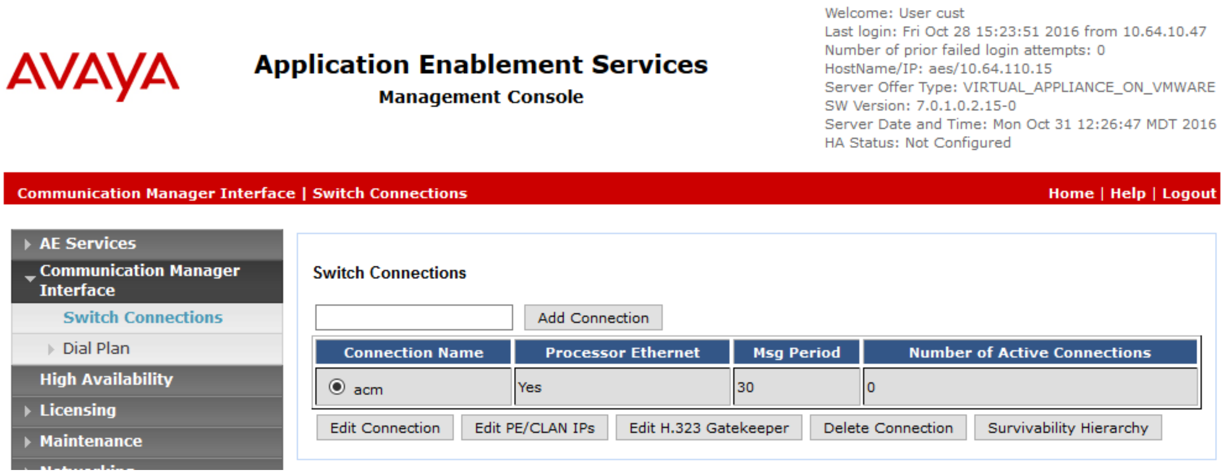
Edit CTI User

User Profile:	User ID	interop
	Common Name	interop
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	□
Routing Control:	Allow Routing on Listed Devices	None

6.2. Configure Communication Manager Switch Connections

To add links to the Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection. Click the **Add Connection** button.

This was previously configured as **acm** for this test environment:

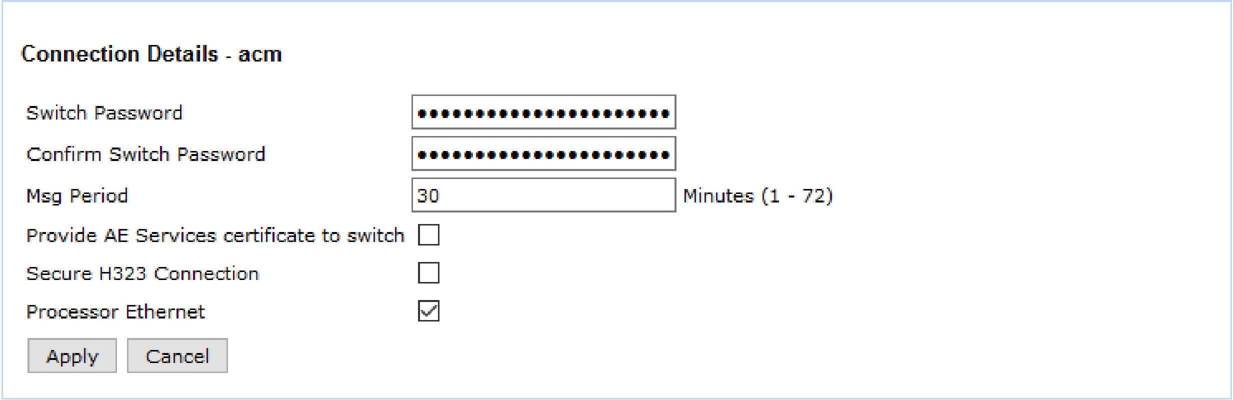


Welcome: User cust
Last login: Fri Oct 28 15:23:51 2016 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.110.15
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Mon Oct 31 12:26:47 MDT 2016
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● acm	Yes	30	0

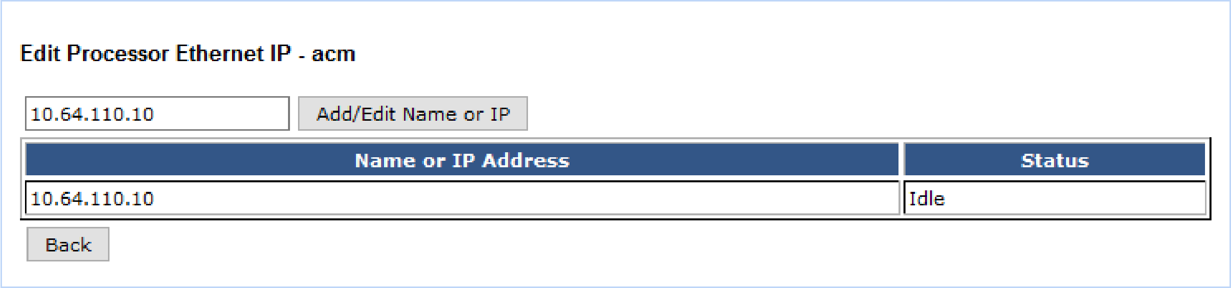
Use the **Edit Connection** button shown above to configure the connection. Enter the **Switch Password** and check the **Processor Ethernet** box if using the **procr** interface, as shown below. This must match the password configured when adding AESVCS connection in Communication Manager.



Connection Details - acm

Switch Password	••••••••••••••••••••••
Confirm Switch Password	••••••••••••••••••••••
Msg Period	30 Minutes (1 - 72)
Provide AE Services certificate to switch	□
Secure H323 Connection	□
Processor Ethernet	☑

Use the **Edit PE/CLAN IPs** button (shown in this section's first screen shot above) to configure the **procr** of Communication Manager.

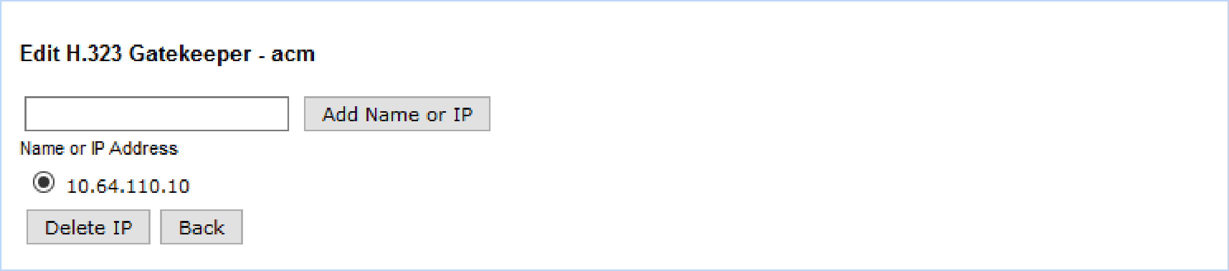


Edit Processor Ethernet IP - acm

10.64.110.10

Name or IP Address	Status
10.64.110.10	Idle

Use the **Edit H.323 Gatekeeper** button (shown in this section's first screen capture above) to configure the IP Address of Communication Manager.



Edit H.323 Gatekeeper - acm

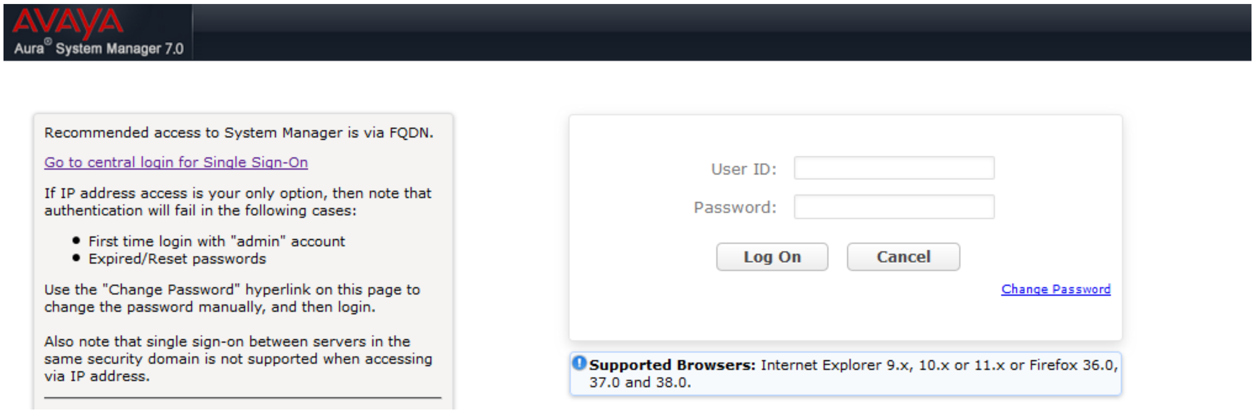
Name or IP Address

● 10.64.110.10

7. Configure Avaya Aura® Session Manager

This section provides the steps for configuring Session Manager to communicate with the RedSky E911 Manager.

Session Manager is configured using System Manager. Enter the URL of System Manager such as https://<system-manager-ip-address>/SMGR. Log in using appropriate credentials.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

Password:

Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

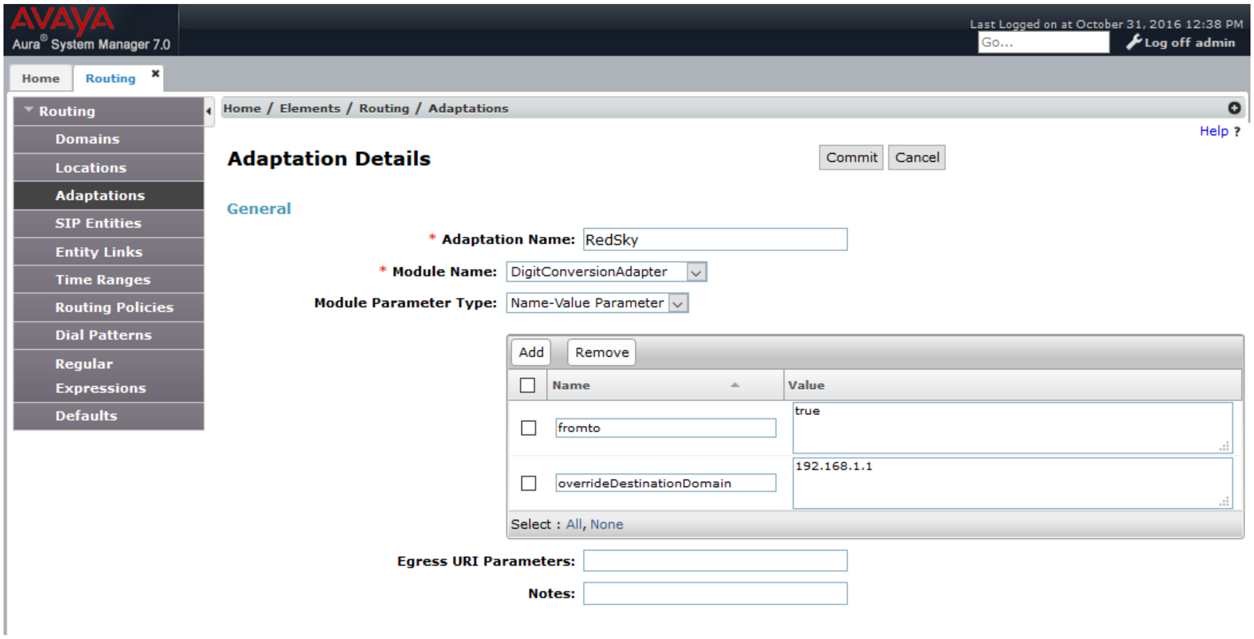
7.1. Add Adaptation

Navigate to **Routing → Adaptation**. Click **New** to add a new Adaptation.

- Type in a name in **Adaptation Name.**
- Select **DigitConversionAdapter** for **Module Name**.
- In the **Module Parameter**, type in the following
  - overrideDestinationDomain=<RedSky-IP-Address>
  - During Compliance Test, **overrideDestinationDomain=192.168.1.1** and **fromto=true,** were used.

Click **Commit** to save changes.

Adding this adaptation will replace the domain of Request URI and To header with the IP Address configured in **overrideDestinationDomain,** when SIP calls are placed. During compliance test, avaya.com was replaced with 192.168.1.1.



Adaptation Details

General

* Adaptation Name: RedSky

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

□	Name	Value
□	fromto	true
□	overrideDestinationDomain	192.168.1.1

Egress URI Parameters:

Notes:

For security reason, real IP Address has been changed with a private one.

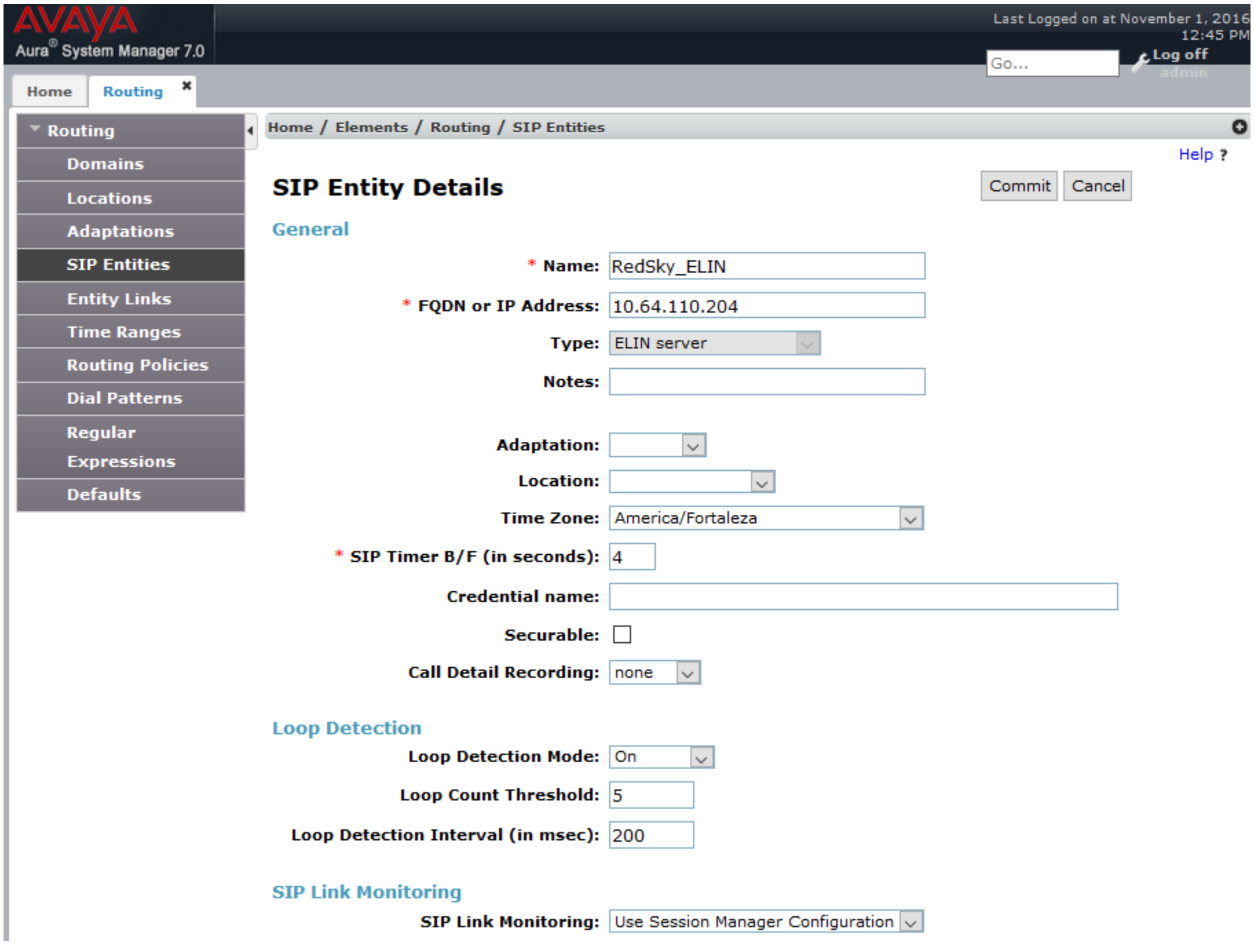
7.2. Add a SIP Entity

Navigate to **Routing → SIP Entities.** Click **New** to add a new SIP entity for RedSky ELIN Server.

- Type in a name in **Name.**
- Type in IP address of RedSky ELIN Server in **FQDN or IP Address.**
- Set **Type** to **ELIN server.**
- Set **Location** to a configured Location.

Click **Commit** to save changes.

During the compliance test a single RedSky ELIN server was used. If multiple RedSky ELIN servers are configured, use an FQDN for **FDQN or IP Address** field and add entries for the FQDN in **Session Manager → Network Configuration → Local Host Name Resolution.**



SIP Entity Details

General

* Name: RedSky_ELIN
* FQDN or IP Address: 10.64.110.204
Type: ELIN server
Notes:

Adaptation:
Location:
Time Zone: America/Fortaleza
* SIP Timer B/F (in seconds): 4
Credential name:
Securable: □
Call Detail Recording: none

Loop Detection

Loop Detection Mode: On
Loop Count Threshold: 5
Loop Detection Interval (in msec): 200

SIP Link Monitoring

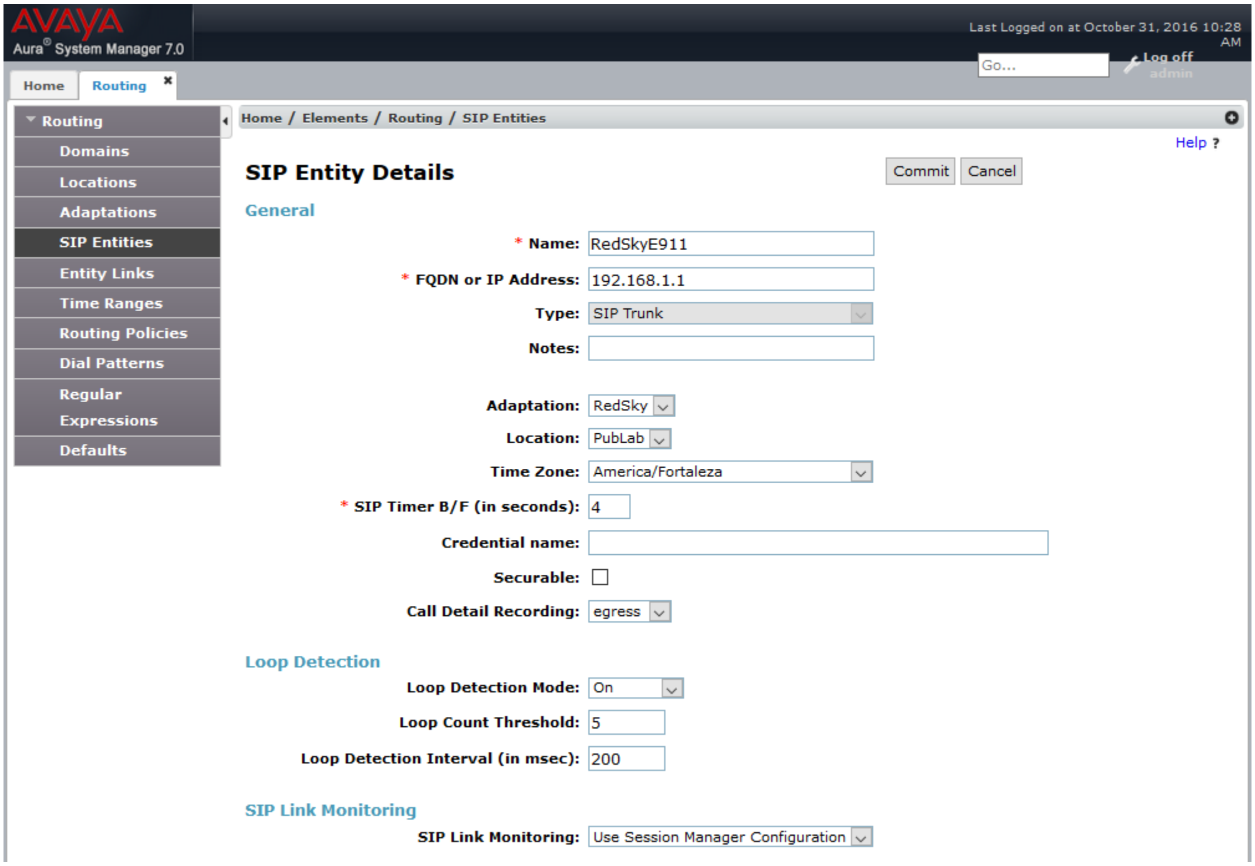
SIP Link Monitoring: Use Session Manager Configuration

Add another SIP Entity for emergency call routing to RedSky E911 Anywhere. If emergency calls are to be routed via an ISDN Trunk, skip this configuration.

- Type in a name in **Name.**
- Type in IP address of RedSky in **FQDN or IP Address.**
- Set **Type** to **SIP Trunk.**
- Set **Adaptation** to the adaptation added in previous step.
- Set **Location** to a configured Location.

For security reason, real IP Address has been changed with a private one.

Click **Commit** to save changes.



SIP Entity Details

General

* Name:	RedSkyE911
* FQDN or IP Address:	192.168.1.1
Type:	SIP Trunk
Notes:	
Adaptation:	RedSky
Location:	PubLab
Time Zone:	America/Fortaleza
* SIP Timer B/F (in seconds):	4
Credential name:	
Securable:	□
Call Detail Recording:	egress

Loop Detection

Loop Detection Mode:	On
Loop Count Threshold:	5
Loop Detection Interval (in msec):	200

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

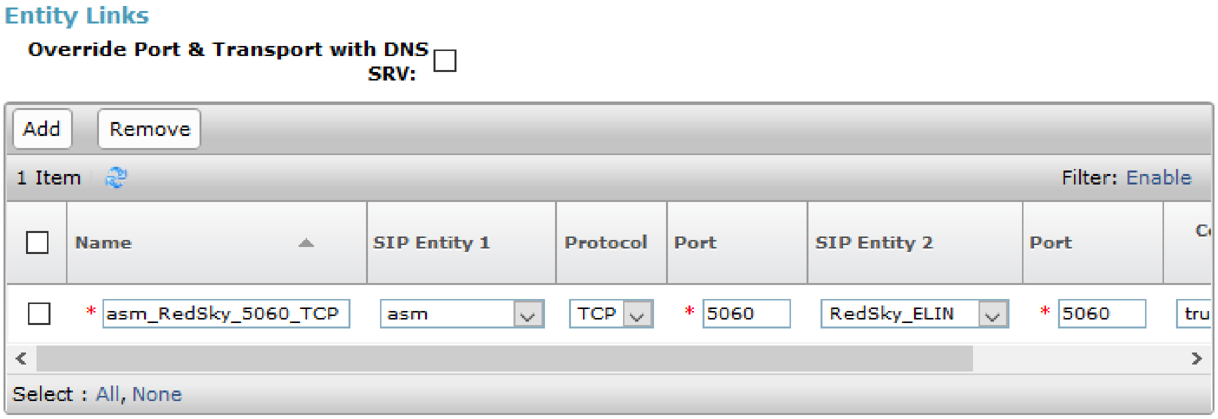
7.3. Add an Entity Link

Once the SIP Entity is added, edit it. At the bottom of the page click **Add** under **Entity Links**.

- Set **SIP Entity 1** to Session Manager's SIP Entity
- Set **Protocol** to **TCP**
- Set **Port** to **5060**
- Set **SIP Entity 2** to the SIP Entity added in the previous step
- Set **Port** to **5060**

Click **Commit** to save the changes.

Following screen captures shows Entity Link added for RedSky ELIN Server



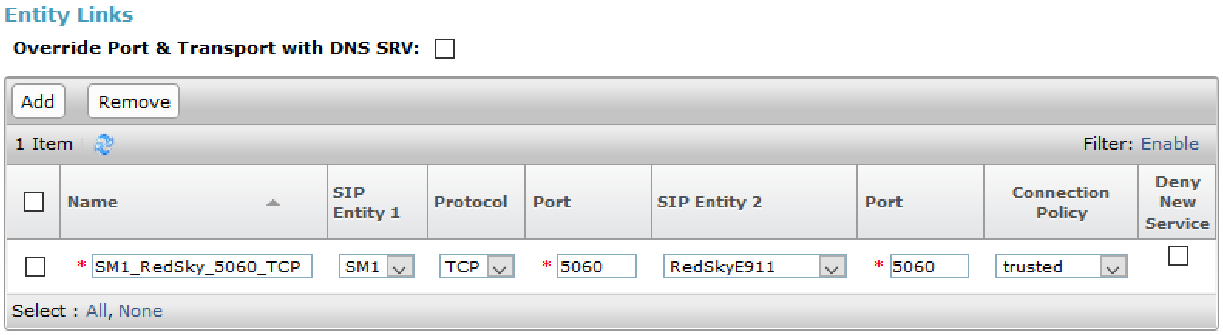
Entity Links

Override Port & Transport with DNS SRV: □

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	C
□	* asm_RedSky_5060_TCP	asm	TCP	* 5060	RedSky_ELIN	* 5060	tru

Select : All, None

Following screen capture shows Entity Link added for emergency call routing to RedSky E911 Anywhere. If emergency calls are to be routed via an ISDN Trunk, skip this configuration.



Entity Links

Override Port & Transport with DNS SRV: □

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	* SM1_RedSky_5060_TCP	SM1	TCP	* 5060	RedSkyE911	* 5060	trusted	□

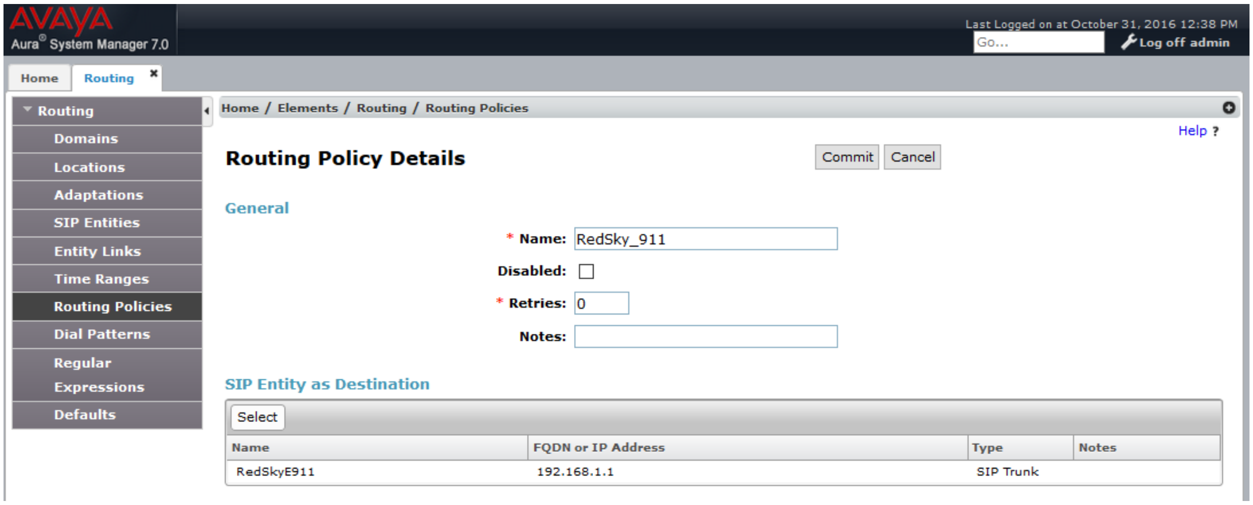
Select : All, None

7.4. Add a Routing Policy

If emergency calls are to be routed via an ISDN Trunk, skip this configuration. Navigate to **Routing → Routing Policies.** Click **New** to add a new Routing Policy for RedSky E911 Anywhere.

- Type in the **Name** for Routing Policy.
- Under **SIP Entity as a destination**, click **Select**. From the **SIP Entity List** select the SIP Entity configured in **Section 7.2** (RedSkyE911) and click **Select** (not shown).

Click **Commit** to save changes.



Routing Policy Details

General

* Name: RedSky_911

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
RedSkyE911	192.168.1.1	SIP Trunk	

7.5. Add a Dial Pattern

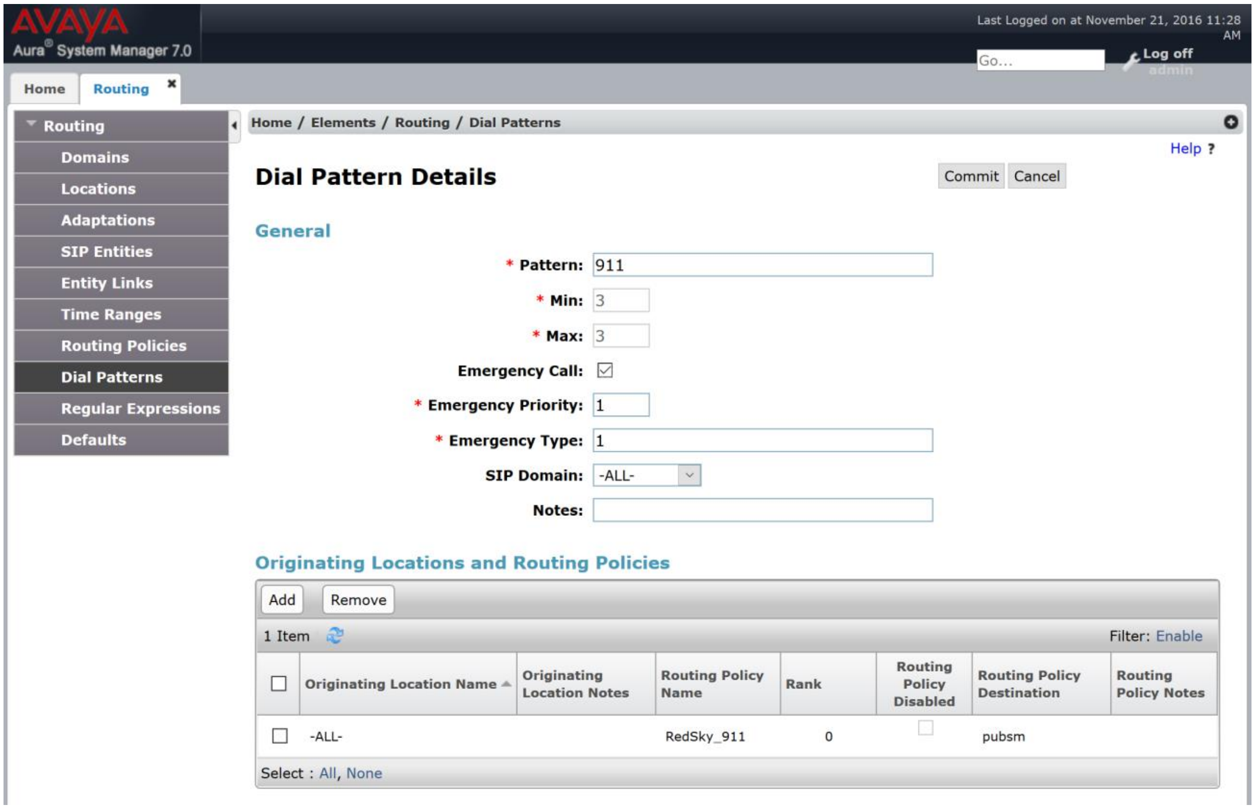
Navigate to **Routing → Dial Patterns.** Click **New** to add a new Dial Pattern for RedSky E911 Manager. On **Dial Patterns** page, click on **New**

- Set **Pattern** to **911**
- Set **Min** and **Max to** 3
- Check box for **Emergency Call**
- Type in **Emergency Priority**
- Type in **Emergency Type**
- Under **Originating Locations and Routing Policies**, click **Add** (New screen not shown)
    - Select a location configured
    - Select the Routing Policy configured in for RedSky E911 Anywhere

Click **Commit** to save changes.

If emergency calls are to be routed via an ISDN Trunk, select the Communication Manager Routing Policy.

For emergency calls Session Manager skips any application sequencing and it goes straight to the final destination as per the Dial Pattern. Session Manager emergency calls are those, where the Dial Pattern has the **Emergency Call** box checked.



Dial Pattern Details

General

* Pattern:	911
* Min:	3
* Max:	3
Emergency Call:	☑
* Emergency Priority:	1
* Emergency Type:	1
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

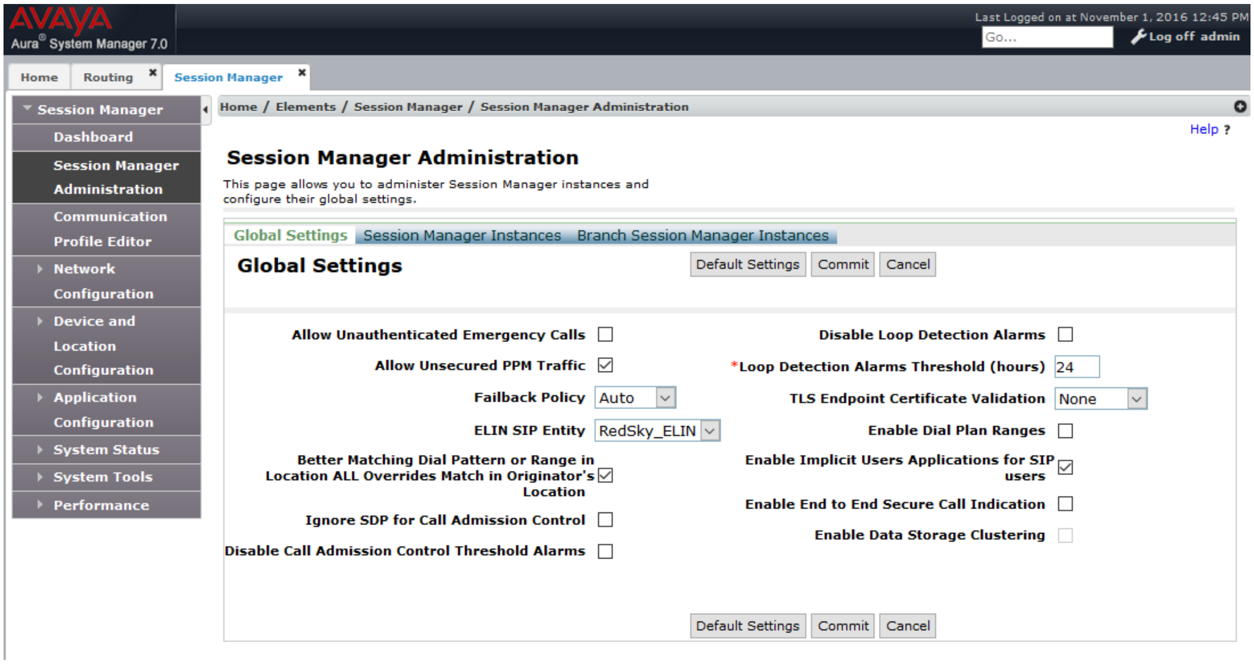
1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		RedSky_911	0	□	pubsm	

Select : All, None

7.6. Configure ELIN SIP Entity

Navigate to **Home → Session Manager → Session Manager Administration**. From the **ELIN SIP Entity** drop down menu, select the SIP Entity added for RedSky ELIN Server. Click **Commit** to save the change.


AVAYA
Aura® System Manager 7.0
Last Logged on at November 1, 2016 12:45 PM
Go...
Log off admin
Home
Routing
Session Manager
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Performance
Home / Elements / Session Manager / Session Manager Administration
Help ?
Global Settings
Session Manager Instances
Branch Session Manager Instances
Default Settings
Commit
Cancel

Session Manager Administration

This page allows you to administer Session Manager instances and configure their global settings.

Global Settings

Allow Unauthenticated Emergency Calls □

Allow Unsecured PPM Traffic ☑

Failback Policy: Auto

ELIN SIP Entity: RedSky_ELIN

Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location ☑

Ignore SDP for Call Admission Control □

Disable Call Admission Control Threshold Alarms □

Disable Loop Detection Alarms □

*Loop Detection Alarms Threshold (hours): 24

TLS Endpoint Certificate Validation: None

Enable Dial Plan Ranges □

Enable Implicit Users Applications for SIP users ☑

Enable End to End Secure Call Indication □

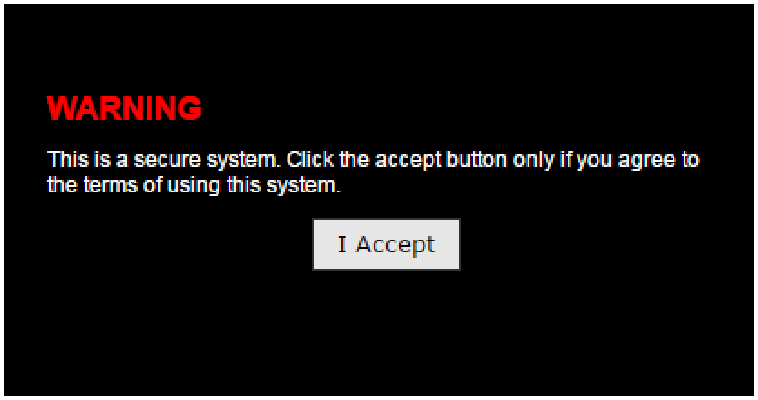
Enable Data Storage Clustering □

8. Configure RedSky E911 Manager

This section provides the steps for configuring the RedSky E911 Manager to provide ELIN information to Avaya Aura® Session Manager. All configuration for compliance testing was performed by a RedSky Engineer.

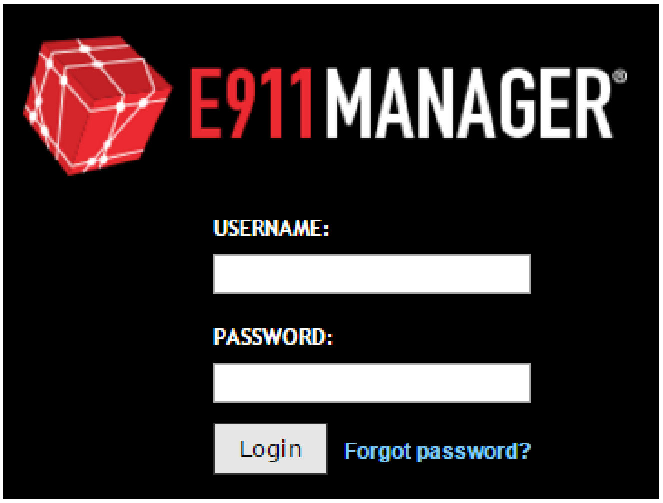
8.1. RedSky E911 Manager Configuration Details

RedSky E911 Manager is configured using a web browser. Enter the URL of the RedSky E911 server such as https://<hostname> where <hostname> is the ip address or fully qualified domain name of the RedSky server. Click **I ACCEPT** on the warning page. Login using appropriate credentials.



WARNING

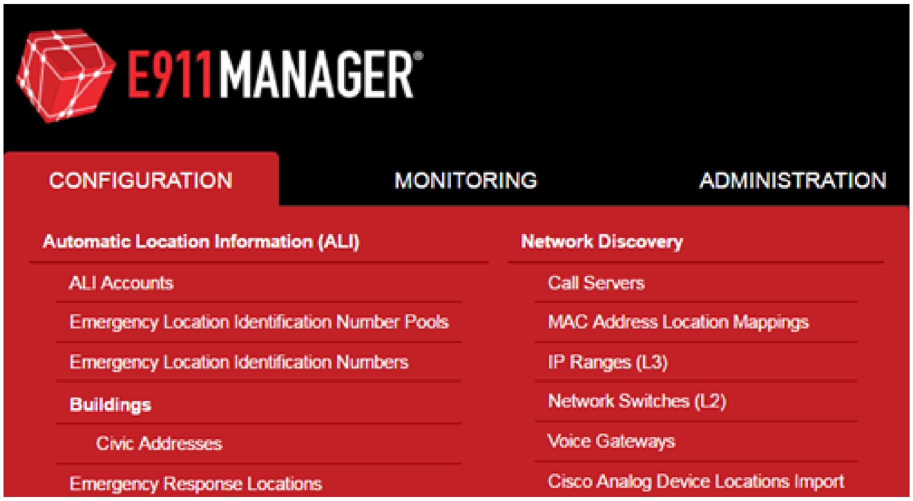
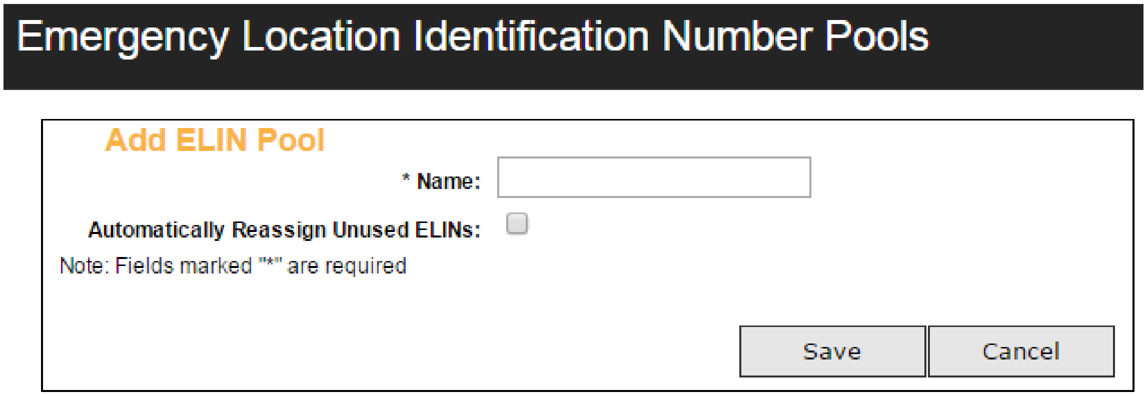
This is a secure system. Click the accept button only if you agree to the terms of using this system.



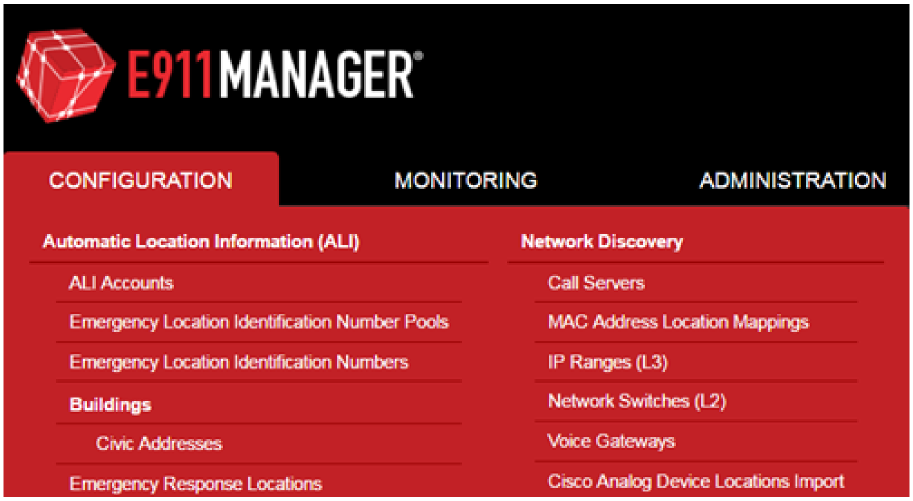
In general, the steps are as follows:

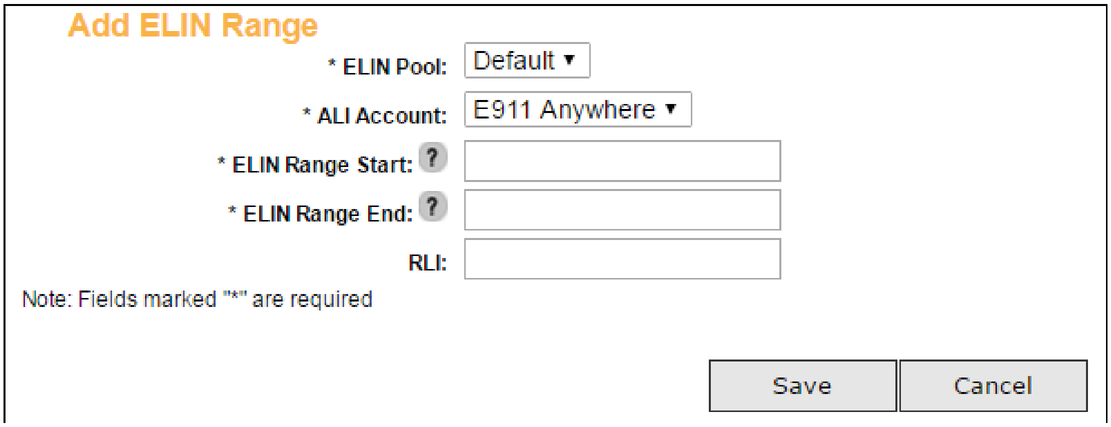
- Define an ELIN Pool
- Create an ELIN Range
- Define a Call Server
- Define a building

- Create locations and tie the location to an ELIN
- Administer the IP Address Ranges

Step	Description
1.	**Define an ELIN Pool** Select **Emergency Location Identification Number Pools** from the **CONFIGURATION** menu and click the **Add ELIN Pool** button. Give the new ELIN Pool a name and click **Add**. In the compliance test, a single ELIN Pool was used; however it is possible to administer more than one ELIN Pool by repeating the process.  E911MANAGER CONFIGURATION MONITORING ADMINISTRATION Automatic Location Information (ALI) ALI Accounts Emergency Location Identification Number Pools Emergency Location Identification Numbers Buildings Civic Addresses Emergency Response Locations Network Discovery Call Servers MAC Address Location Mappings IP Ranges (L3) Network Switches (L2) Voice Gateways Cisco Analog Device Locations Import  Emergency Location Identification Number Pools Add ELIN Pool * Name: Automatically Reassign Unused ELINs: □ Note: Fields marked "*" are required

Step	Description
2.	**Define an ELIN Range** Select **Emergency Location Identification Numbers** from the **CONFIGURATION** menu and click the **Add ELIN Range** button. Select an ELIN Pool from the dropdown and pick an **ALI Account**. Finally define the starting 10 digit number and ending 10 digit number.

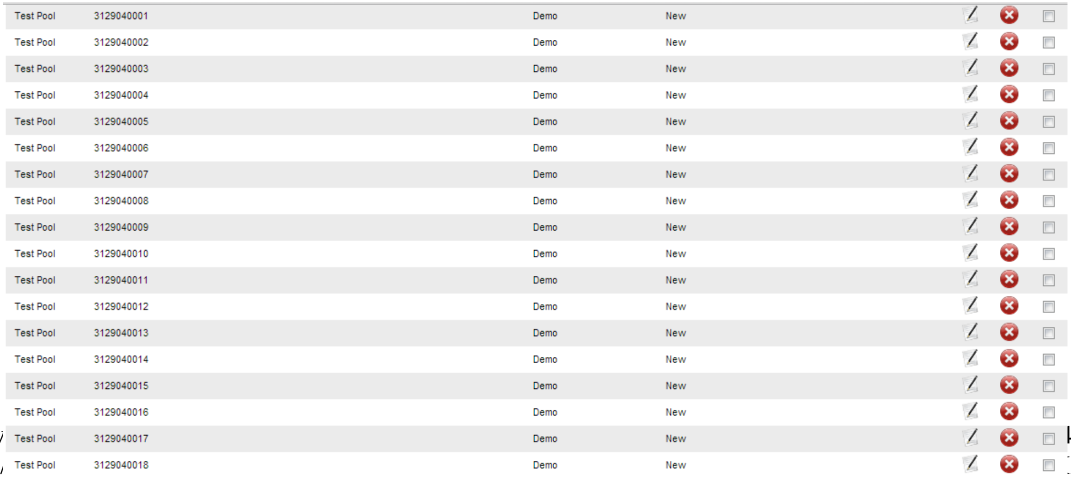

E911MANAGER®
CONFIGURATION
MONITORING
ADMINISTRATION
Automatic Location Information (ALI)
ALI Accounts
Emergency Location Identification Number Pools
Emergency Location Identification Numbers
Buildings
Civic Addresses
Emergency Response Locations
Network Discovery
Call Servers
MAC Address Location Mappings
IP Ranges (L3)
Network Switches (L2)
Voice Gateways
Cisco Analog Device Locations Import



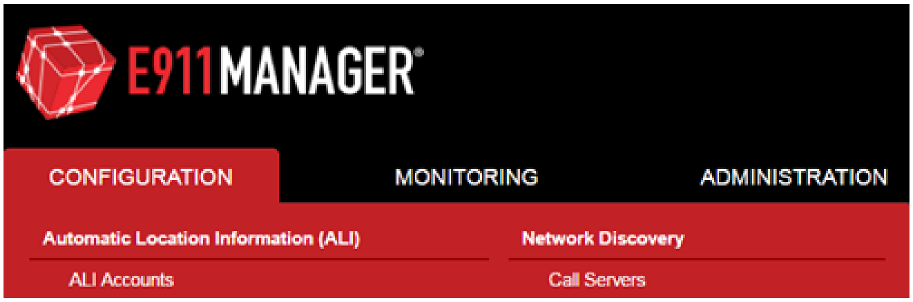
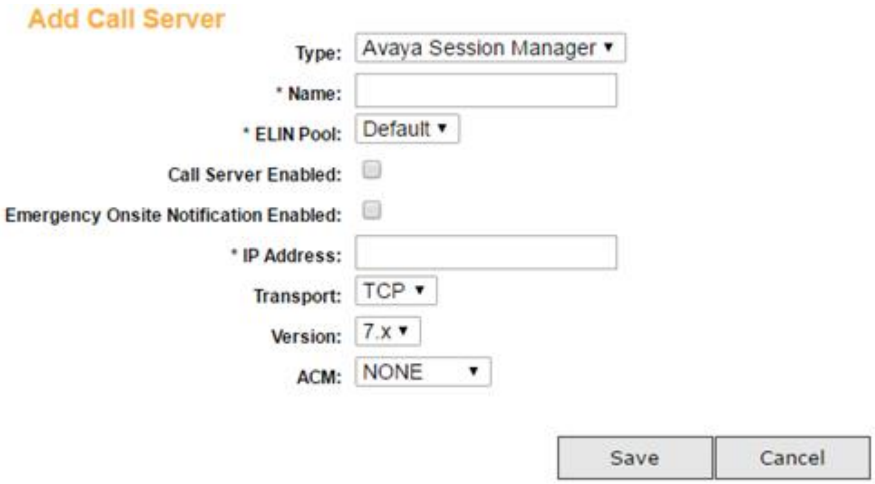
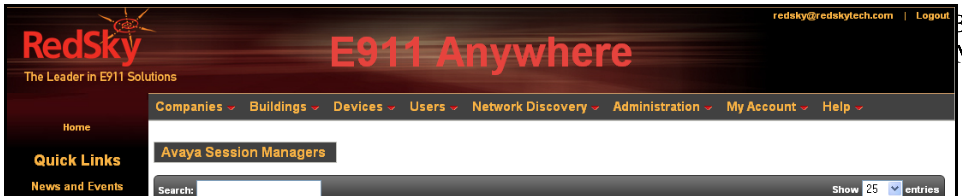
Add ELIN Range

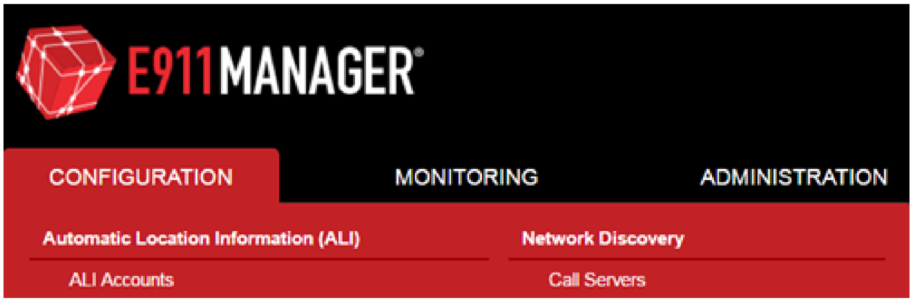
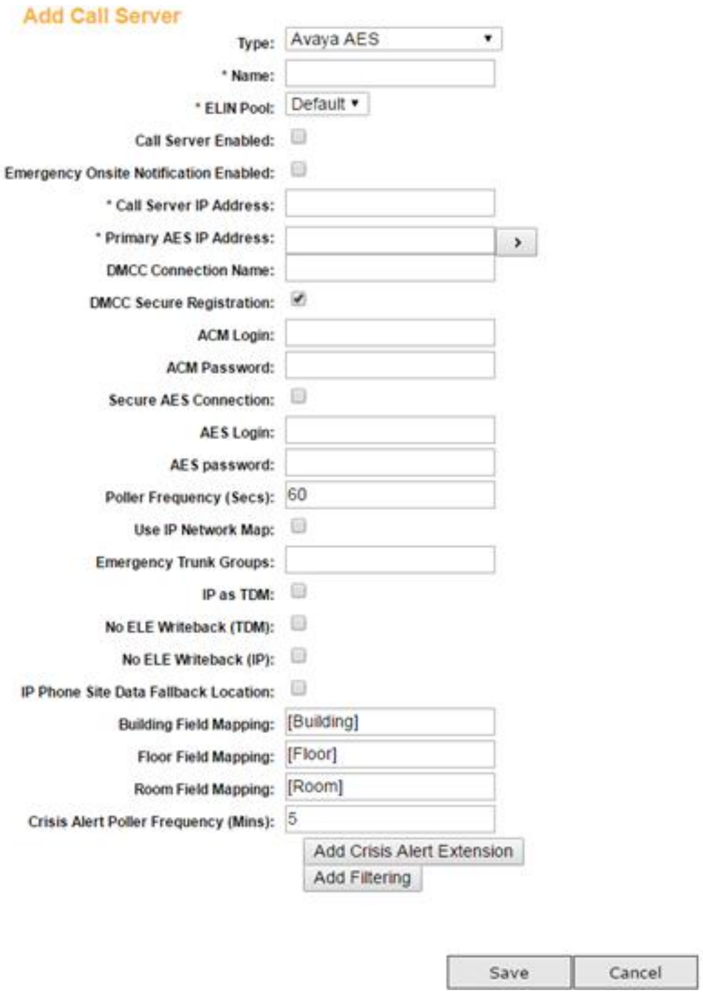
* ELIN Pool:	Default ▾
* ALI Account:	E911 Anywhere ▾
* ELIN Range Start: ?	
* ELIN Range End: ?	
RLI:	

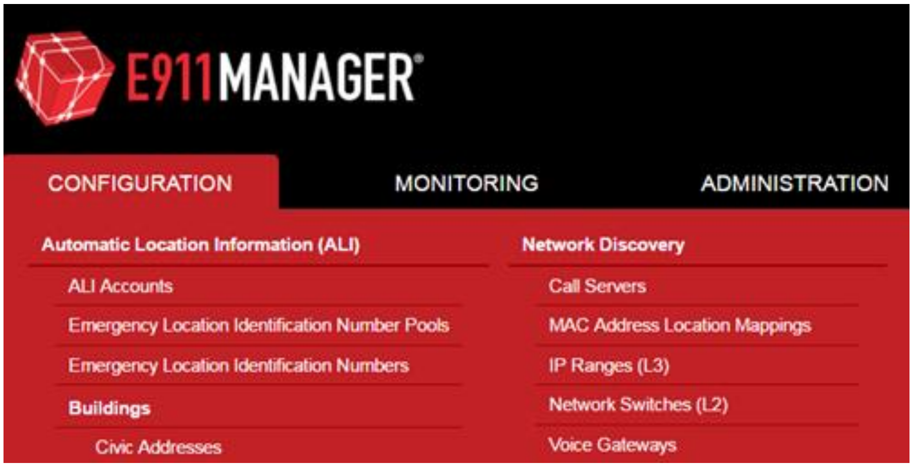
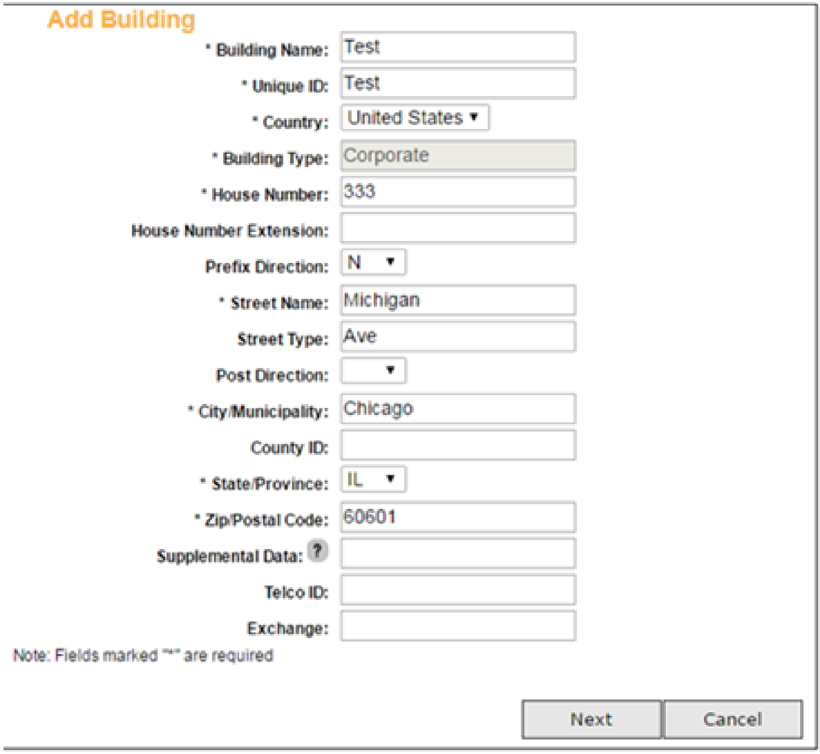
Note: Fields marked "*" are required



Test Pool	3129040001	Demo	New	✎	✖	□
Test Pool	3129040002	Demo	New	✎	✖	□
Test Pool	3129040003	Demo	New	✎	✖	□
Test Pool	3129040004	Demo	New	✎	✖	□
Test Pool	3129040005	Demo	New	✎	✖	□
Test Pool	3129040006	Demo	New	✎	✖	□
Test Pool	3129040007	Demo	New	✎	✖	□
Test Pool	3129040008	Demo	New	✎	✖	□
Test Pool	3129040009	Demo	New	✎	✖	□
Test Pool	3129040010	Demo	New	✎	✖	□
Test Pool	3129040011	Demo	New	✎	✖	□
Test Pool	3129040012	Demo	New	✎	✖	□
Test Pool	3129040013	Demo	New	✎	✖	□
Test Pool	3129040014	Demo	New	✎	✖	□
Test Pool	3129040015	Demo	New	✎	✖	□
Test Pool	3129040016	Demo	New	✎	✖	□
Test Pool	3129040017	Demo	New	✎	✖	□
Test Pool	3129040018	Demo	New	✎	✖	□

Step	Description
3.	**Administer the Session Manager link (Optional)** Select **Call Servers** from the **CONFIGURATION** menu and click the **Add Call Server** button to administer the Session Manager(s). In the compliance test, a single Session Manager was used; however it is possible to administer more than one Session Manager by repeating the process. When Session Manager is administered properly, a connection will automatically be established between servers. Enter the **IP address** of Session Manager**,** give the call server a **Name**, select the **"Avaya Session Manager" Type,** and check **"Call Server Enabled"**. Enter the **Transport** protocol to match the entry in **Section 7.3**. **TLS** is recommended for security reasons.  E911MANAGER CONFIGURATION MONITORING ADMINISTRATION Automatic Location Information (ALI) ALI Accounts Network Discovery Call Servers  Add Call Server Type: Avaya Session Manager ▾ * Name: * ELIN Pool: Default ▾ Call Server Enabled: □ Emergency Onsite Notification Enabled: □ * IP Address: Transport: TCP ▾ Version: 7.x ▾ ACM: NONE ▾ Select **View** from the **Network Discovery → Avaya Session Managers** menu to review the administered entries (not shown).  redsky@redskytech.com | Logout RedSky The Leader in E911 Solutions E911 Anywhere Companies Buildings Devices Users Network Discovery Administration My Account Help Home Quick Links News and Events Avaya Session Managers Search: Show 25 entries

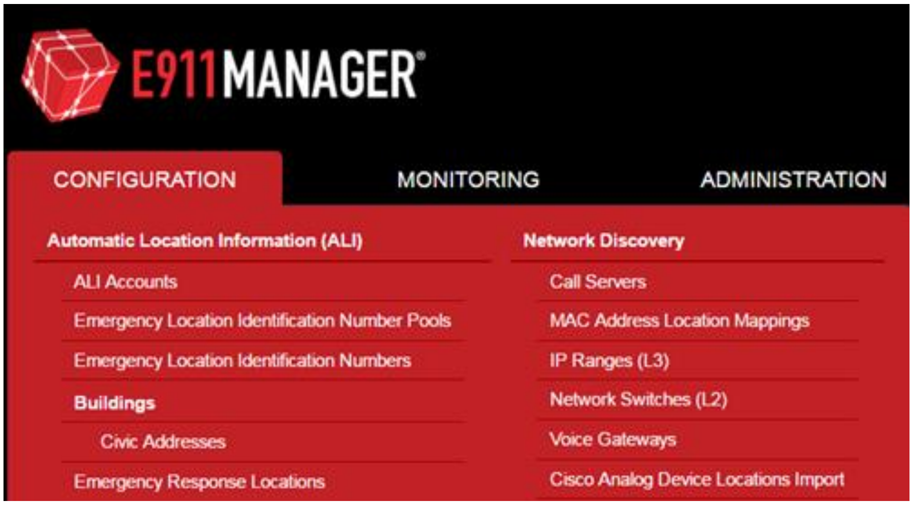
Step	Description
4.	**Administer the Avaya AES link (Optional)** Select **Call Servers** from the **CONFIGURATION** menu and click the **Add Call Server** button to administer the Avaya AES(s). In the compliance test, a single Avaya AES was used; however it is possible to administer more than one Avaya AES by repeating the process. When Avaya AES is administered properly, a connection will automatically be established between servers.  E911MANAGER® CONFIGURATION MONITORING ADMINISTRATION Automatic Location Information (ALI) ALI Accounts Network Discovery Call Servers Give the call server a **Name** and change the **Type** to **Avaya AES** if not set already. Check “**Call Server Enabled**”, fill in the “**DMCC Connection Name**”, fill in the **Emergency Trunk Groups** associated with emergency calls, and fill in the rest of the required fields. Finally, fill in the **ACM Login** and **ACM Password** from **Section 5.1**. Fill in the **AES Login**, and fill in the **AES password** from **Section 6.1**.  Add Call Server Type: Avaya AES ▾ * Name: * ELIN Pool: Default ▾ Call Server Enabled: □ Emergency Onsite Notification Enabled: □ * Call Server IP Address: * Primary AES IP Address: › DMCC Connection Name: DMCC Secure Registration: ☑ ACM Login: ACM Password: Secure AES Connection: □ AES Login: AES password: Poller Frequency (Secs): 60 Use IP Network Map: □ Emergency Trunk Groups: IP as TDM: □ No ELE Writeback (TDM): □ No ELE Writeback (IP): □ IP Phone Site Data Fallback Location: □ Building Field Mapping: [Building] Floor Field Mapping: [Floor] Room Field Mapping: [Room] Crisis Alert Poller Frequency (Mins): 5 Add Crisis Alert Extension Add Filtering Save Cancel

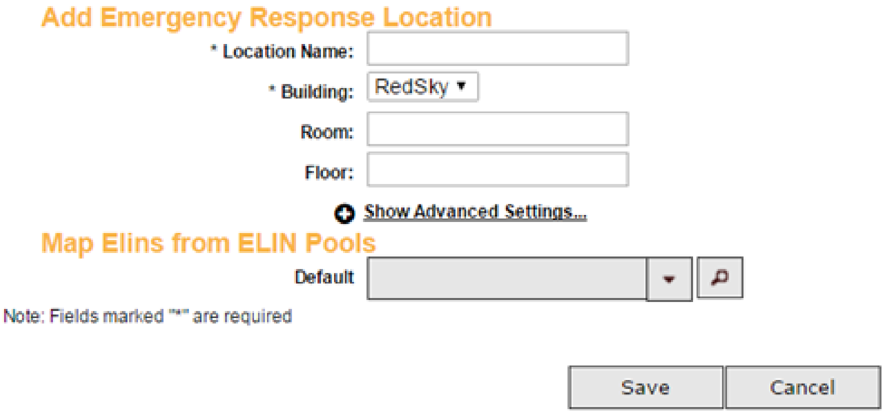
Step	Description
5.	**Define the Company Locations (Buildings)** Location administration involves defining one or more Buildings, one or more Locations within each building, and one or more network IP Ranges associated with each Location, and assigning ELINs to each IP Range. It is also possible to define devices such as phones. However, this is not necessary as this would be redundant with administration in Communication Manager and Session Manager. Device definitions are overridden with IP Address based location information if it differs from the statically defined device location information. Click **the Civic Addresses** from the **CONFIGURATION → Buildings** menu to administer general location information. Multiple Buildings may be administered by repeating the process. For the compliance test, two buildings were defined. Click **Next** then **Save** to complete the entry.  E911MANAGER CONFIGURATION MONITORING ADMINISTRATION Automatic Location Information (ALI) ALI Accounts Emergency Location Identification Number Pools Emergency Location Identification Numbers Buildings Civic Addresses Network Discovery Call Servers MAC Address Location Mappings IP Ranges (L3) Network Switches (L2) Voice Gateways  Add Building * Building Name: Test * Unique ID: Test * Country: United States * Building Type: Corporate * House Number: 333 House Number Extension: Prefix Direction: N * Street Name: Michigan Street Type: Ave Post Direction: * City/Municipality: Chicago County ID: * State/Province: IL * Zip/Postal Code: 60601 Supplemental Data: Telco ID: Exchange: Note: Fields marked "*" are required

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>6.</td><td>

Define the Company Locations (Emergency Response Locations)

Click the **Emergency Response Locations** from the **CONFIGURATION** menu to administer general location information. Click on the **Add ERL** button. Multiple locations may be administered by repeating the process.


E911MANAGER®
CONFIGURATION
MONITORING
ADMINISTRATION
Automatic Location Information (ALI)
ALI Accounts
Emergency Location Identification Number Pools
Emergency Location Identification Numbers
Buildings
Civic Addresses
Emergency Response Locations
Network Discovery
Call Servers
MAC Address Location Mappings
IP Ranges (L3)
Network Switches (L2)
Voice Gateways
Cisco Analog Device Locations Import



Add Emergency Response Location

* Location Name:

* Building: RedSky ▾

Room:

Floor:

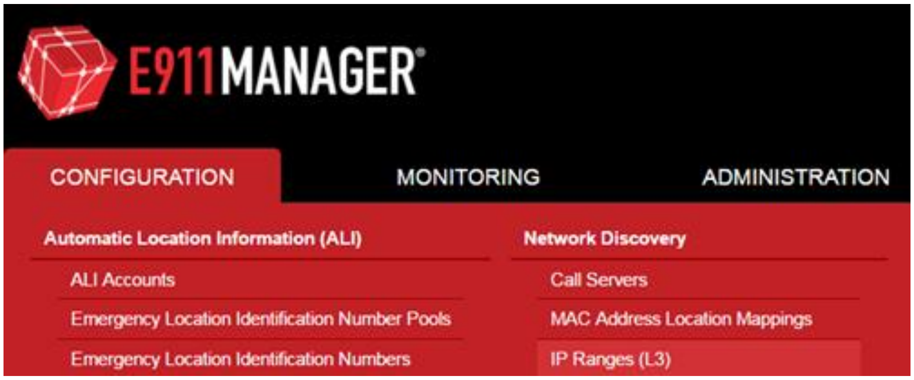
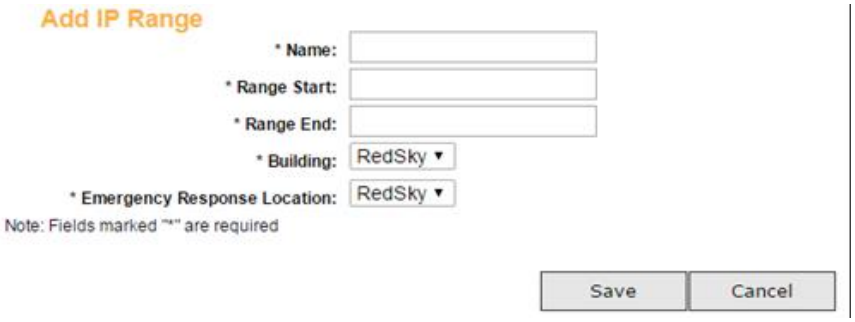
Show Advanced Settings...

Map Elins from ELIN Pools

Default

Note: Fields marked "*" are required

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

Step	Description
7.	**Administer the IP Address Ranges** Click **Add Rang button** from the **CONFIGURATION → IP Ranges (L3)** menu to administer the IP Address Ranges that will be associated with each location. For the Compliance Test, one address range entry was created for each Location.  E911MANAGER® CONFIGURATION MONITORING ADMINISTRATION Automatic Location Information (ALI) ALI Accounts Emergency Location Identification Number Pools Emergency Location Identification Numbers Network Discovery Call Servers MAC Address Location Mappings IP Ranges (L3)  Add IP Range * Name: * Range Start: * Range End: * Building: RedSky ▾ * Emergency Response Location: RedSky ▾ Note: Fields marked "*" are required Save Cancel

9. Verification Steps

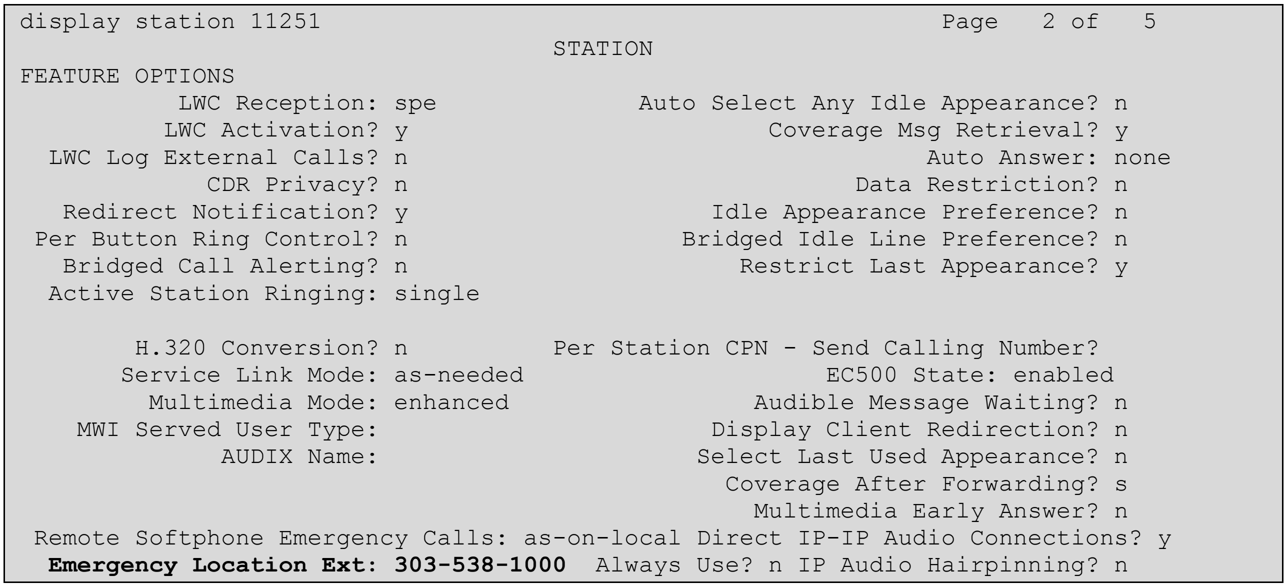
For SIP Endpoints, the following command was executed on the command line of the Session Manager in order to validate the ELIN information provided by RedSky E911 Manager:

```
[cust@asm ~]$ sm cons get allreg
RegistrationKey[commProfileSetId:155,
contactHashKey:sip:11101@10.64.10.47:50283;transport=tcp]=RegistrationData[expirationT
ime=Wed Nov 02 12:35:49 MDT 2016, callId=1_138c8463ac0c21582da96d_R@10.64.10.47,
lastRegistrationInterruption=Never, cSeq=4, elin=3035381000, elinTStamp=Wed Nov 02
11:35:49 MDT 2016, sendNoSubNotify=false, endpointAdapter=null, avayaEndpoint=true]
RegistrationKey[commProfileSetId:200,
contactHashKey:sip:11111@10.80.130.150:50697;rinstance=cd43bf5312ed5f20]=RegistrationD
ata[expirationTime=Wed Nov 02 12:11:43 MDT 2016,
callId=81133MDNhZWE4MTIyZmI4MWQ4ZmQyZDdkN2M0NTI3MzE2NDI,
lastRegistrationInterruption=Never, cSeq=686, elin=3035381000, elinTStamp=Wed Nov 02
11:11:43 MDT 2016, sendNoSubNotify=false, endpointAdapter=null, avayaEndpoint=true]
RegistrationKey[commProfileSetId:203,
```

Alternatively, using the traceSM tool on Session Manager, verify ELIN is sent by RedSky E911 Manager in SIP PUBLISH when a SIP Endpoint registers to Session Manager.

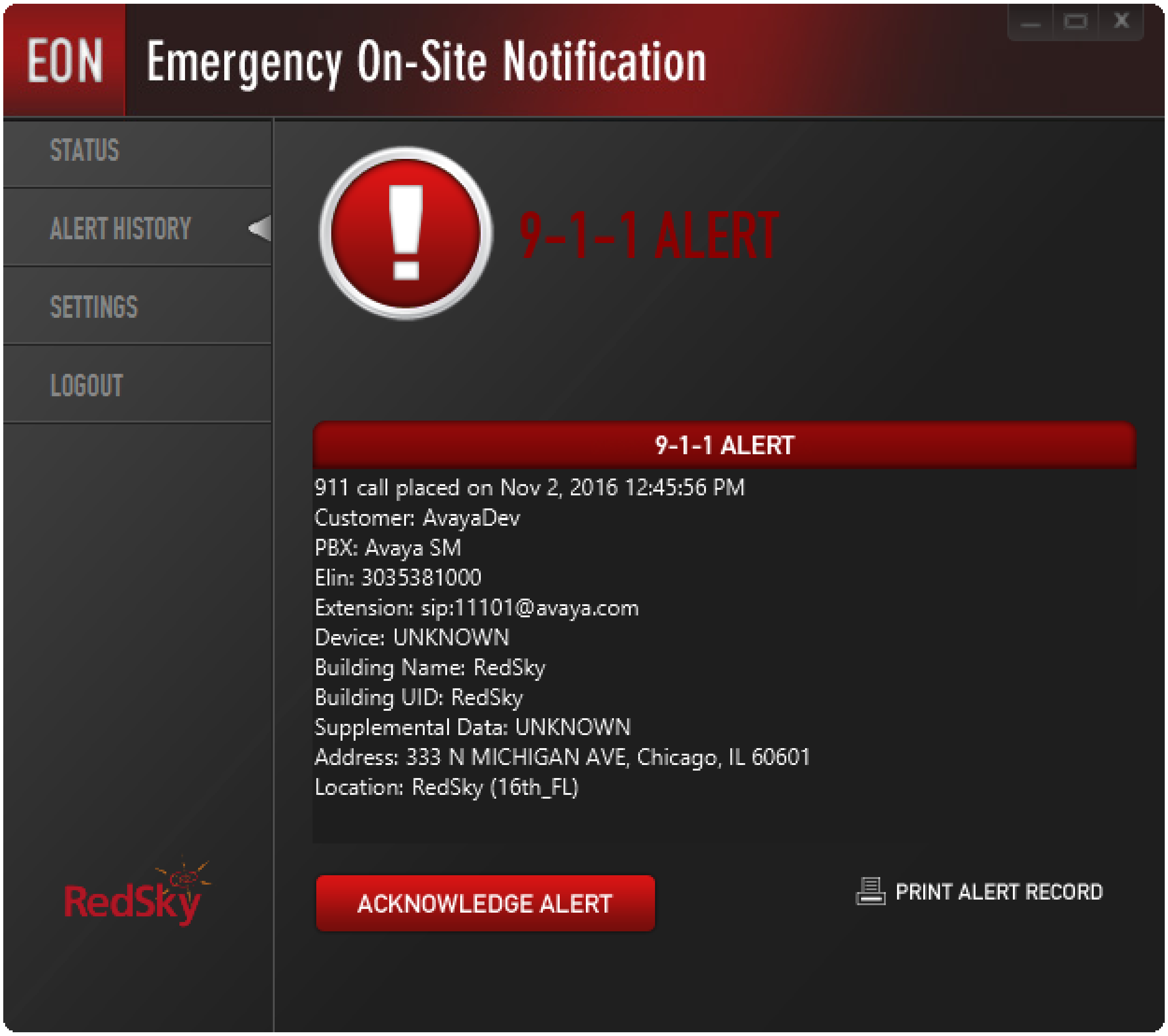
```
PUBLISH sip:10.64.110.13;transport=tcp SIP/2.0
Call-ID: 8994d60cbea3d262206654dbc6269bcf@0.0.0.0
CSeq: 1 PUBLISH
From: <sip:10.64.110.204>;tag=93560456_4dfa9705_af0854de_44f644db
To: <sip:10.64.110.13>
Max-Forwards: 70
User-Agent: Mobicents Sip Servlets 3.0.0-SNAPSHOT
Via: SIP/2.0/TCP 10.64.110.204:5060;branch=z9hG4bK44f644db_af0854de_2173b150-25b0-
4f4f-a166-d21ce5844bcd
Content-Type: application/reginfo+xml
Event: reg
Expires: 0
Content-Length: 767

<?xml version="1.0" encoding="UTF-8"?>
<reginfo state="partial" version="0" xmlns="urn:ietf:params:xml:ns:reginfo"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <registration aor="sip:11101@avaya.com" id="a105" state="active">
    <contact id="c105--1615807468--456956109-1" state="active" event="registered"
duration-registered="0" q="1.0" xmlns="">
      <uri>sip:11101@10.64.10.47:52138;transport=tcp</uri>
      <unknown-param name="+sip.instance"> "&lt;urn:uuid:912f105d-6f5a-5b33-b262-
af7e9602cf65&gt;" </unknown-param>
      <unknown-param name="reg-id"> "1" </unknown-param>
      <unknown-param name="avaya-actions"> "presence.initiate-pubsub" </unknown-param>
      <elin>3035381000</elin>
    </contact>
  </registration>
</reginfo>
```

For non-SIP Endpoints, validate that the ELE was populated by RedSky E911 Manager. On Communication Manager, via a SAT terminal, use display station command and navigate to Page 2. Verify **Emergency Location Ext.** has been populated.



```
display station 11251                                           Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe            Auto Select Any Idle Appearance? n
          LWC Activation? y                       Coverage Msg Retrieval? y
  LWC Log External Calls? n                                  Auto Answer: none
             CDR Privacy? n                             Data Restriction? n
   Redirect Notification? y                   Idle Appearance Preference? n
 Per Button Ring Control? n                 Bridged Idle Line Preference? n
   Bridged Call Alerting? n                     Restrict Last Appearance? y
  Active Station Ringing: single

        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                 EC500 State: enabled
         Multimedia Mode: enhanced                  Audible Message Waiting? n
    MWI Served User Type:                        Display Client Redirection? n
              AUDIX Name:                       Select Last Used Appearance? n
                                                  Coverage After Forwarding? s
                                                    Multimedia Early Answer? n
 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 303-538-1000  Always Use? n IP Audio Hairpinning? n
```

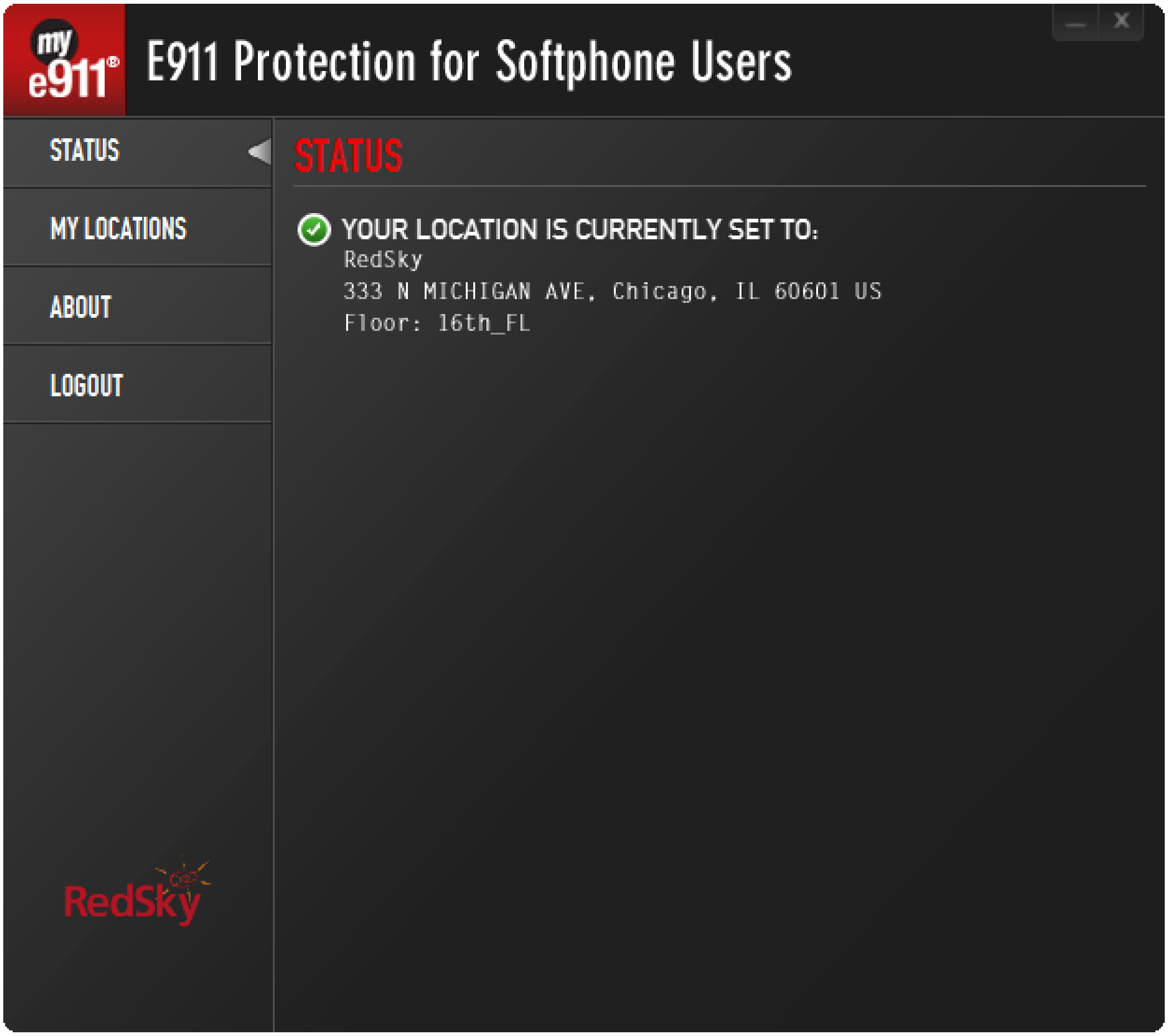
To validate Emergency Alerts are generated successfully, place a test emergency call and verify the EON client receives the alert. Test emergency call may need to be scheduled with appropriate PSAP. Place calls from both SIP and non-SIP Endpoints. Following screen capture displays an Emergency Alert that was received for an emergency call dialed from a SIP Endpoint.



9-1-1 ALERT

911 call placed on Nov 2, 2016 12:45:56 PM
Customer: AvayaDev
PBX: Avaya SM
Elin: 3035381000
Extension: sip:11101@avaya.com
Device: UNKNOWN
Building Name: RedSky
Building UID: RedSky
Supplemental Data: UNKNOWN
Address: 333 N MICHIGAN AVE, Chicago, IL 60601
Location: RedSky (16th_FL)

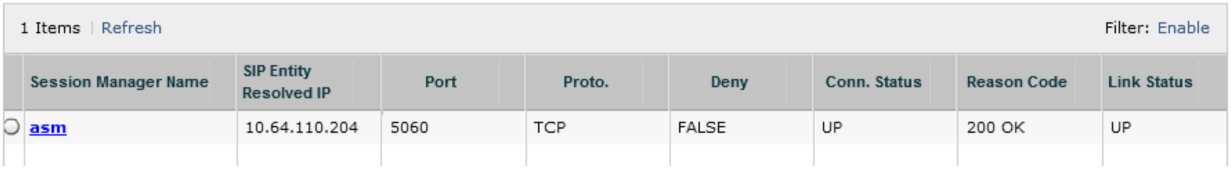
For Softphone users, validate that the location is set correctly on myE911 client.



STATUS

YOUR LOCATION IS CURRENTLY SET TO:
RedSky
333 N MICHIGAN AVE, Chicago, IL 60601 US
Floor: 16th_FL

From the System Manager web interface, navigate to **Home → Session Manager → System Status → SIP Entity Monitoring**. Under **All Monitored SIP Entities**, click on the SIP Entity for RedSky E911 Anywhere or RedSky ELIN Server. Verify the **Conn. Status** and **Link Status** are **Up**. This ensures the SIP Connectivity between RedSky and Session Manager. Perform this step for both entities added for RedSky.



1 Items | Refresh

Filter: Enable

	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	asm	10.64.110.204	5060	TCP	FALSE	UP	200 OK	UP

10. Conclusion

The RedSky E911 Manager successfully demonstrated the ability to send ELIN to Avaya Aura® Communication Manager and Avaya Aura® Session Manager. While the general location information a company may have on file with the Automatic Location Identifier (ALI) database providers can be matched to an ANI from the Calling Party Number sent over public networks, this information may not be precise, and could in fact be incorrect given the roaming nature of IP endpoints as well as the distributed nature of modern communications systems. The precision afforded to enterprises using a RedSky ELIN server solution can make a significant difference in response times in the event of an emergency. RedSky E911 Manager also successfully demonstrated the ability to ensure softphone users update their locations and send emergency alerts when an emergency call is placed from an Avaya Aura® environment. RedSky E911 Anywhere successfully demonstrated the ability to route emergency calls.

11. Additional References

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

[1] Administering Avaya Aura® Communication Manager, Release 6.2, Document 03-3005089, Issue 7.0, December 2012

[2] Administering Avaya Aura® Session Manager, Release 6.2, Document 03-603324, July 2012

Product information for RedSky Technologies E911 Manager may be found at http://www.redskye911com.

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.