Avaya Solution & Interoperability Test Lab

Application Notes for RedSky Technologies E911 Manager, E911 Anywhere and Emergency On-Site Notification with Avaya Aura® Session Manager R6.2, Avaya Aura® Communication Manager R6.2 and Avaya Aura® Application Enablement Services R6.2 – 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 and Emergency On-Site Notification.

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, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services, 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 registered with Avaya Aura® 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.

Avaya Aura® Session Manager offers a unique interface to ELIN servers, enabling an enterprise to manage emergency location information for users who register SIP endpoints. Though static definitions of emergency location information have been, and continue to be offered through the Avaya platforms, dynamic ELIN information permits enterprise users to register a SIP endpoint in alternate locations such as meeting rooms, and for the emergency location information to be updated to reflect the current location of the user should the endpoint need to place an emergency call.

RedSky registers to Avaya Aura® Application Enablement Services' DMCC service to receive Crisis Alerts.

2. General Test Approach and Test Results

The compliance test focused on the interoperability between RedSky E911 Manager, E911 Anywhere and Emergency On-Site Notification, and Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

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

RedSky receives registration information from Session Manager when a SIP Entity Link is established, and when endpoints register with Session Manager. The registration information Session Manager provides contains the network address of the endpoint. RedSky compares this address to administered IP Address ranges and returns the ELIN associated with the current location of the endpoint. Session Manager uses the ELIN information obtained from RedSky to associate ANI with the device and stores this in the registration data for the endpoint. Should a 911 call be placed, the ELIN information stored in Session Manager would be included in the header of the invite sent to the far end of the Entity Link configured for handling emergency calls. This function is independent of the RedSky server meaning that in a worst case scenario, once ELIN information was provided to Session Manager, the RedSky server could be unreachable and the proper ELIN information would still be sent.

Session Managers' support for emergency calling is broader than the 911 service 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.

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

2.2. Test Results

All planned test cases were verified and passed. For serviceability testing, the RedSky E911 Manager was able to supply station emergency numbering information to Session Manager after connection to the server was disconnected and reconnected, as well as after reset of Communication Manager, Session Manager and the RedSky E911 Manager server. RedSky Manager was tested in a cloud configuration, but can also be installed on a customers' local network.

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 G450 Media Gateway
- Avaya IP telephones
- RedSky E911 Manager server
- RedSky ELIN Server
- RedSky E911 Anywhere
- RedSky Emergency On-Site Notification Client

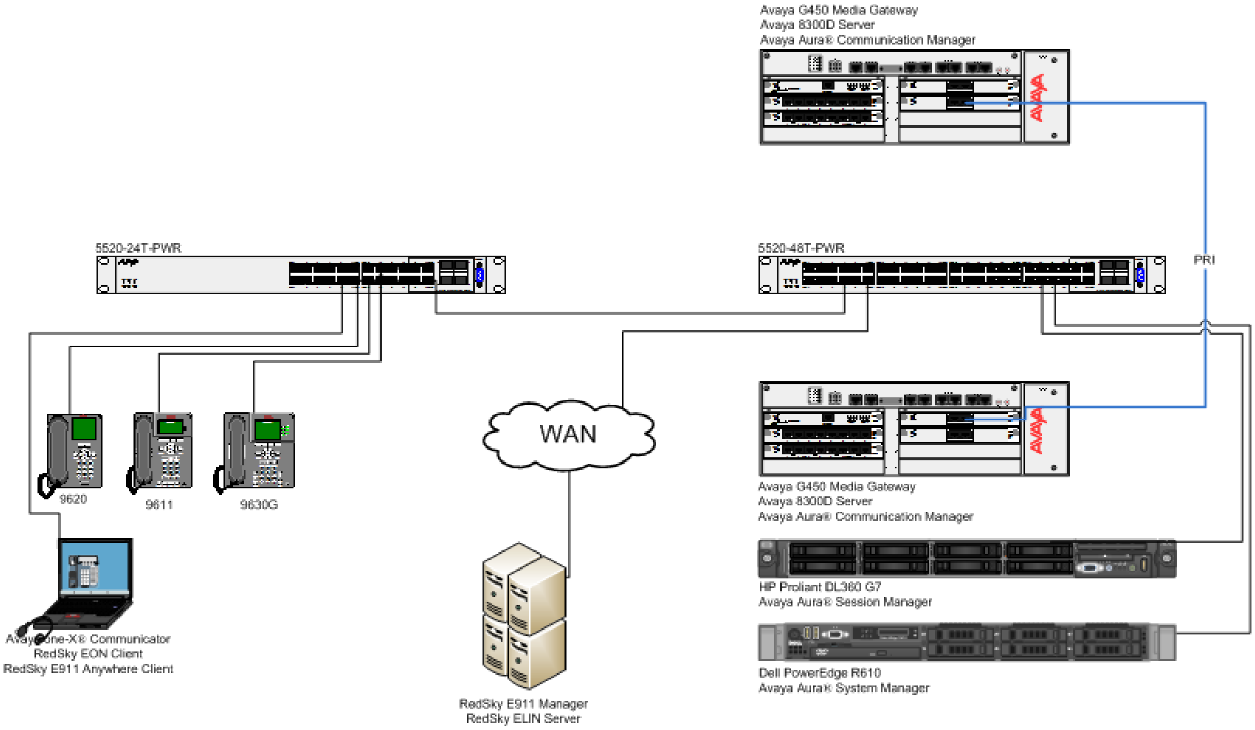


Figure 1 – RedSky E911 Manager Configuration

4. Equipment and Software Validated

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

Equipment	Version
Avaya Aura® System Manager	6.2.12.0

Equipment	Version
Avaya Aura® Session Manager	6.2 SP3
Avaya Aura® Communication Manager	6.2 SP3
Avaya G450 Media Gateway	31.20.1
Avaya 9600 Series SIP Phones	6.2.3
Avaya Aura® Application Enablement Services	6.2
RedSky Technologies - E911 Manager - E911 Anywhere - Emergency On-Site Notification Client	 6.3.3 (20101216-0845 rev:9427) 6.3.3 (20101216-0845 rev:9427) 14652

5. Configure Avaya Aura® Communication Manager

Communication Manager used an existing configuration with SIP trunks to connect to Session Manager and CTI link to AES. Configuration of those aspects of the integration was standard and not directly relevant to the interoperability of RedSky E911 Manager. These application notes will not cover those aspects of the configuration.

5.1. Add SMS User

RedSky E911 Manager uses the Application Enablement Services SMS interface to query for administered Stations and Agents for use in administering the application.

A privileged user was used in this test; however, a local administrator would want to restrict the user account. This involves creating a user profile at the SAT, and then creating and assigning the user to the profile in the web admin pages.

Use **add user-profile *n*** command, where ***n*** is an available profile.
On Page 1, set the following features to **y**:

- Shell Access
- Call Center B
- Routing and Dial Plan J
- Security K
- Stations M
- Trunking P

```
add user-profile 30                                          Page   1 of  41
                                USER PROFILE 30

User Profile Name: RedSky SMS

       This Profile is Disabled? n               Shell Access? y
Facility Test Call Notification? n   Acknowledgement Required? n
     Grant Un-owned Permissions? n           Extended Profile? n

             Name           Cat Enbl           Name                Cat Enbl
                    Adjuncts A   n            Routing and Dial Plan J   y
                 Call Center B   y                         Security K   y
                    Features C   n                          Servers L   n
                    Hardware D   n                         Stations M   y
                 Hospitality E   n                System Parameters N   n
                          IP F   n                     Translations O   n
                 Maintenance G   n                         Trunking P   y
Measurements and Performance H   n                            Usage Q   n
               Remote Access I   n                      User Access R   n
```

On Page 3, set permission to **r-** for the following:

- agent B
- agent-loginID B
- alias Station M

```
add user-profile 30                                           Page   3 of  41
                                  USER PROFILE 30
 Set Permissions For Category:    To:         Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                     aesvcs link A    --
                   aesvcs-server A    --
                           agent B    r-
                   agent-loginID B    r-
                          alarms H    --
                   alias station M    r-
         alphanumeric-dial-table J    --
                   alternate-frl C    --
                         amw all G    --
                        amw asai G    --
                       amw audix G    --
                         amw pms G    --
           analog-testcall board G    --
```

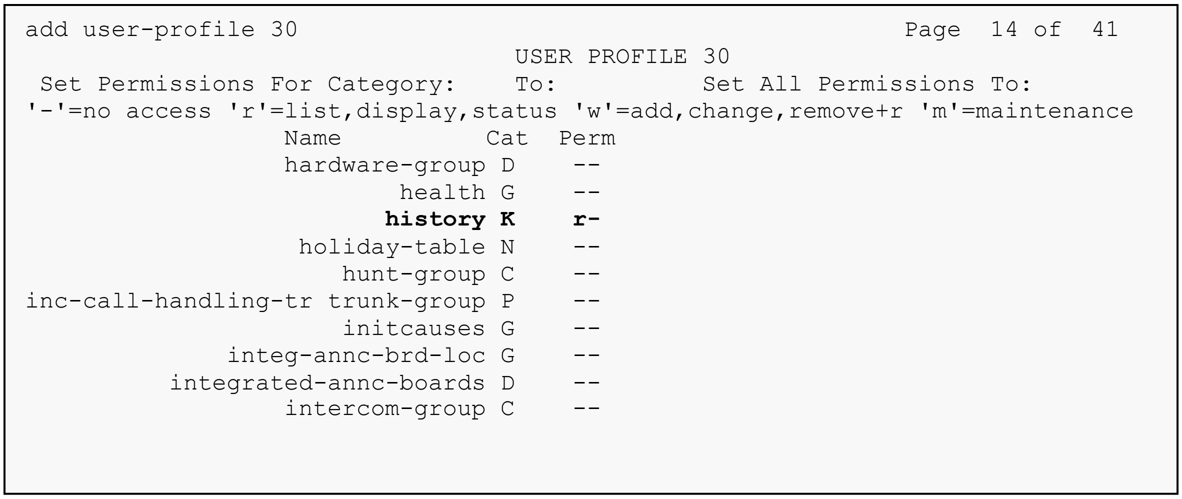
On Page 12, set permission to **r-** for the following:

- emergency J
- enp-number-plan J

```
add user-profile 30                                           Page  12 of  41
                                  USER PROFILE 30
 Set Permissions For Category:    To:         Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                       emergency J    r-
                 enp-number-plan J    r-
                     environment G    --
                          errors G    --
                             esm G    --
                             ess L    --
                    ess clusters L    --
               ess port-networks L    --
                ethernet-options F    --
                          events G    --
        exp-holiday-coverage-tbl N    --
           extended-pickup-group C    --
           extended-user-profile R    --
               extension-station M    --
                  extension-type M    --
```

On Page 14, set permission to **r-** for the following:

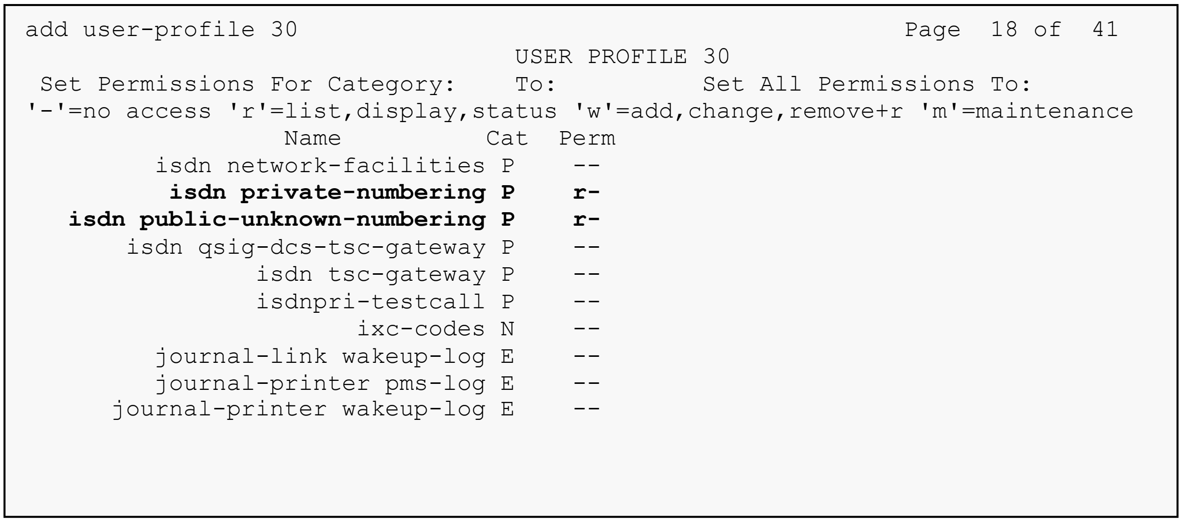
- history K



```
add user-profile 30                                         Page  14 of  41
                                  USER PROFILE 30
 Set Permissions For Category:    To:          Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                  hardware-group D    --
                          health G    --
                         history K    r-
                   holiday-table N    --
                      hunt-group C    --
inc-call-handling-tr trunk-group P    --
                      initcauses G    --
              integ-annc-brd-loc G    --
          integrated-annc-boards D    --
                  intercom-group C    --
```

On Page 18, set the permission to **r-** for the following:

- isdn private-numbering P
- isdn public-unknown-numbering P



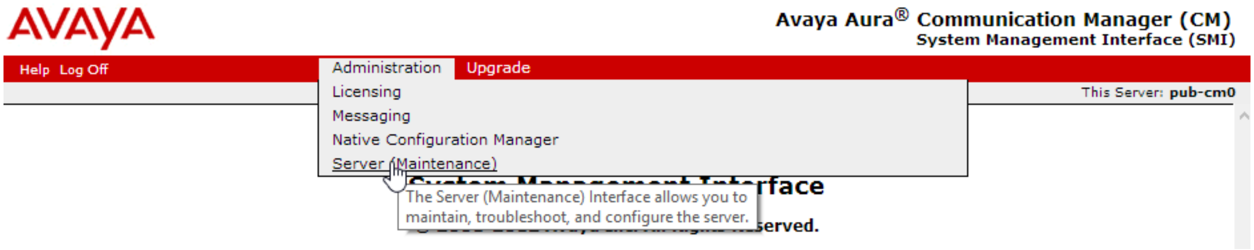
```
add user-profile 30                                         Page  18 of  41
                                  USER PROFILE 30
 Set Permissions For Category:    To:          Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
         isdn network-facilities P    --
          isdn private-numbering P    r-
   isdn public-unknown-numbering P    r-
       isdn qsig-dcs-tsc-gateway P    --
                isdn tsc-gateway P    --
                isdnpri-testcall P    --
                       ixc-codes N    --
         journal-link wakeup-log E    --
         journal-printer pms-log E    --
      journal-printer wakeup-log E    --
```

On Page 29, set the permission to **r-** for the following:

- private-numbering
- public-unknown-numbering

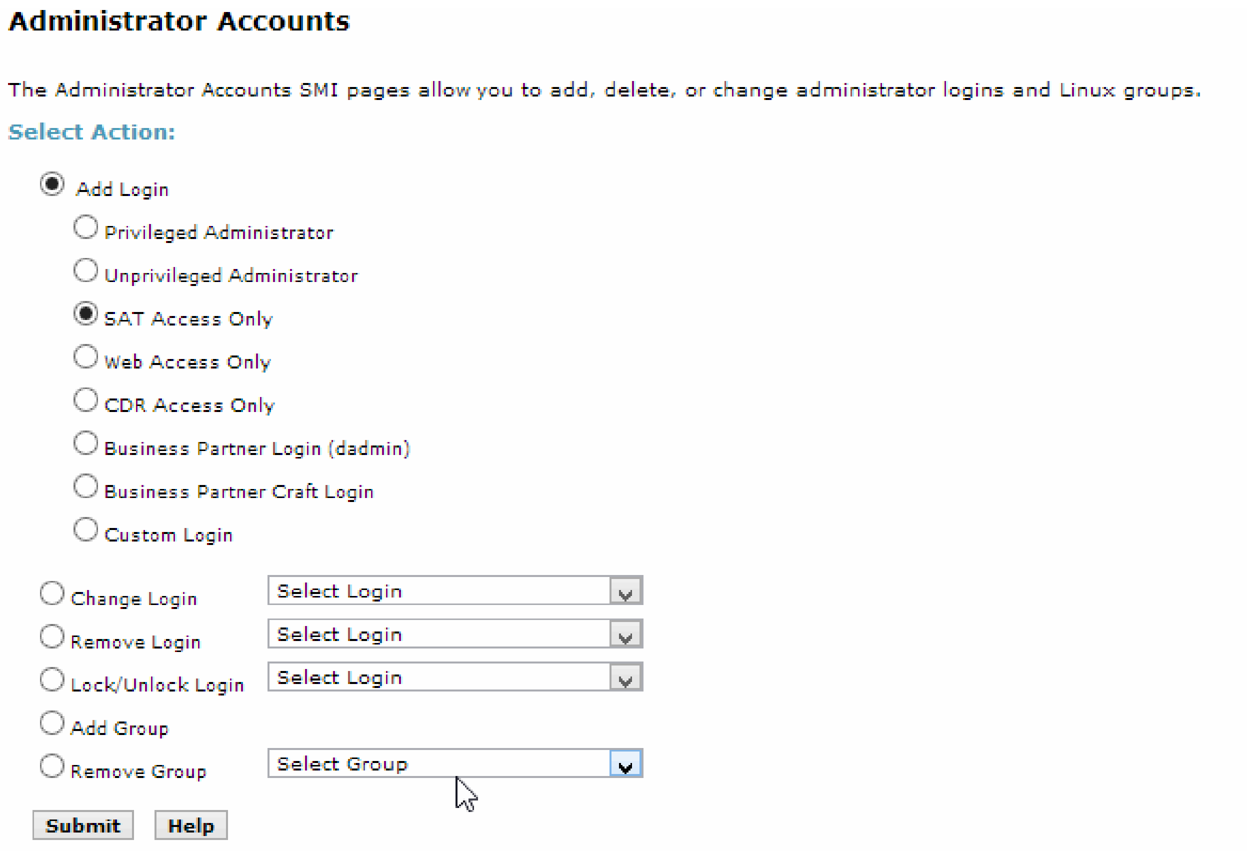
```
add user-profile 30                                           Page  29 of  41
                                  USER PROFILE 30
 Set Permissions For Category:    To:          Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                   port-location D    --
                    port-network D    --
                  power-shutdown G    --
     precedence-routing analysis J    --
precedence-rout digit-conversion J    --
 precedence-routing route-chosen J    --
                    pri-endpoint P    --
               private-numbering P    r-
          processor-ip-interface A    --
                    profile-base R    --
        public-unknown-numbering P    r-
```

Create a 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
Upgrade
Licensing
Messaging
Native Configuration Manager
Server (Maintenance)
This Server: pub-cm0
System Management Interface

The Server (Maintenance) Interface allows you to maintain, troubleshoot, and configure the server.

Select **Administrator Accounts** under **Security**. Select **Add Login** and **SAT Access Only**. Click **Submit**.



Administrator Accounts

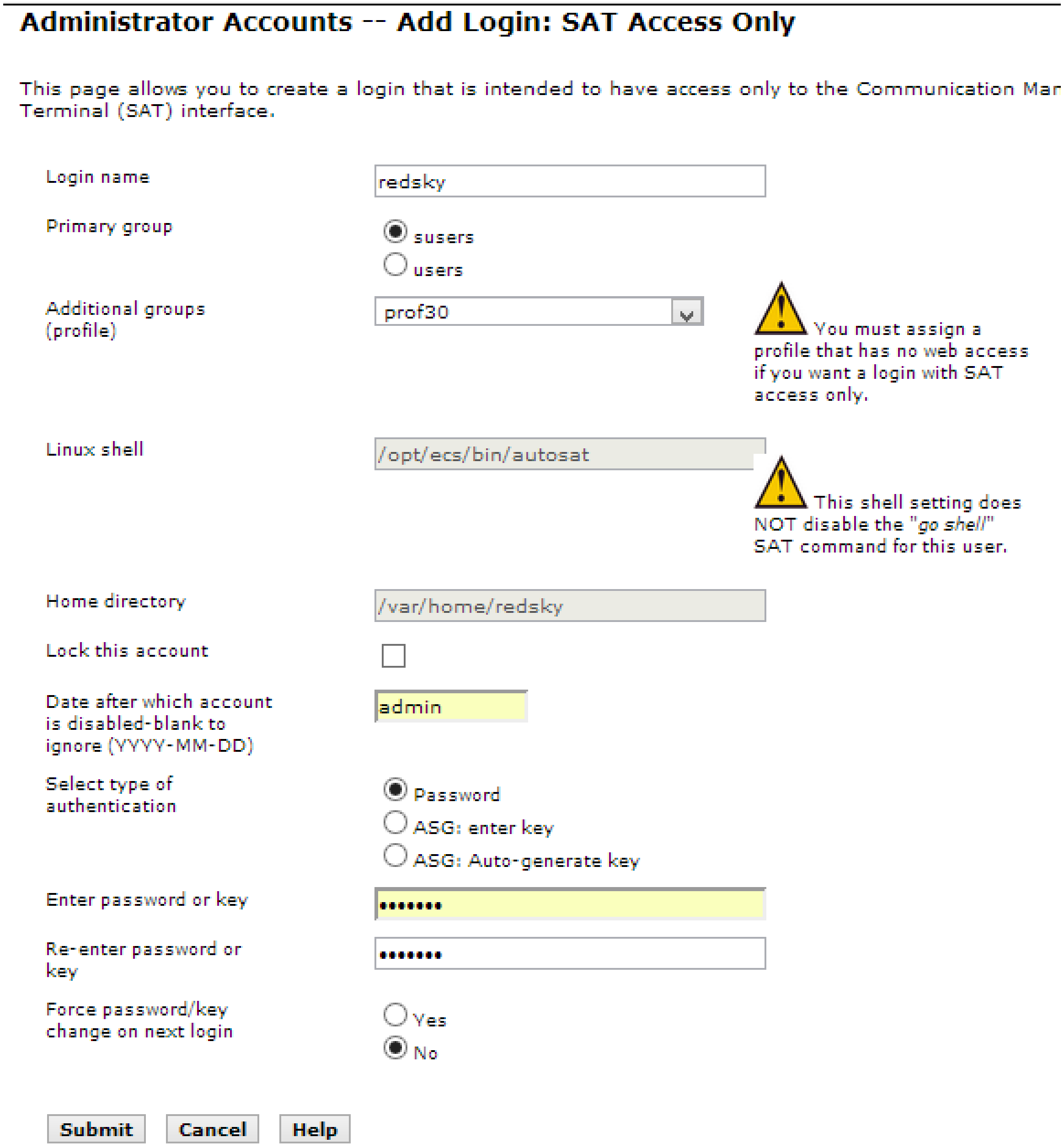
The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

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: SAT Access Only** page:

- Type in a **Login Name**
- For **Additional Groups**, set it to the user-profile added above. i.e. prof30
- Type in a password in **Enter password or key** and **Re-enter password or key**



Administrator Accounts -- Add Login: SAT Access Only

This page allows you to create a login that is intended to have access only to the Communication Mar
Terminal (SAT) interface.

Login name	redsky
Primary group	● susers ○ users
Additional groups (profile)	prof30
Linux shell	/opt/ecs/bin/autosat
Home directory	/var/home/redsky
Lock this account	☐
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	admin
Select type of authentication	● Password ○ ASG: enter key ○ ASG: Auto-generate key
Enter password or key	•••••••
Re-enter password or key	•••••••
Force password/key change on next login	○ Yes ● No

You must assign a profile that has no web access if you want a login with SAT access only.

This shell setting does NOT disable the "*go shell*" SAT command for this user.

5.2. Configure ARS Routing

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 trunk to Session Manager
- Set **Call Type** to **alrt**

```
                              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
```

5.3. Configure Public Unknown Numbering

E911 Manager uses the Public Unknown Numbering 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 numbering format for ANI used when placing 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.
- CPN Prefix combined with the ELE must match an ELIN that is configured in E911 Manager.

During Compliance Test, extensions starting with 2 that were 5 digits in length and trunk group number 1 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: 0
 5  2               1                         5        Maximum Entries: 240

                                                    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.
```

5.4. Configure Crisis Alert

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

Following configuration is performed via SAT.

Add a station that will be used by RedSky E911 Manager to receive Crisis Alerts when 911 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 station 54100                                            Page   1 of   5
                                     STATION

Extension: 54100                         Lock Messages? n              BCC: 0
     Type: 9630                          Security Code: 12345           TN: 1
     Port: IP                          Coverage Path 1:                COR: 1
     Name: CrisisAlert                 Coverage Path 2:                COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 54100
            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
```

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

```
add station 54100                                            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 audibly 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 station extension and navigate to **Page 4** to configure **SITE DATA**.

```
change station 54201                                            Page   4 of   4
                                     STATION
 SITE DATA
       Room: D4-H30                                     Headset? n
       Jack: 3                                          Speaker? n
      Cable: Cat5e                                     Mounting: d
      Floor: 4                                     Cord Length: 0
   Building: D                                       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 911 calls. Use **change route-pattern n** where **n** is the route pattern designed to the 911 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

```
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: y y y y y n  n            rest                                          none
```

5.8. Emergency Call Trunk Group

There is no specific trunk group configuration required. However, there does need to be a trunk group defined, in this case trunk group 1. 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 Session Manager and was pre-configured.

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

Group Number: 1                   Group Type: sip           CDR Reports: y
  Group Name: to_SM_Public               COR: 1        TN: 1       TAC: *001
   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
```

5.9. Configure AES connection

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 host 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:      aes6_tr1          devconnect123         y        in use
      2:      AES_21_46         Interop123456         y        in use
      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, to add a CTI link.

- 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: 6201
     Type: ADJ-IP
                                                                        COR: 1
     Name: TSAPI
```

6. Configure Avaya Aura® Application Enablement Services

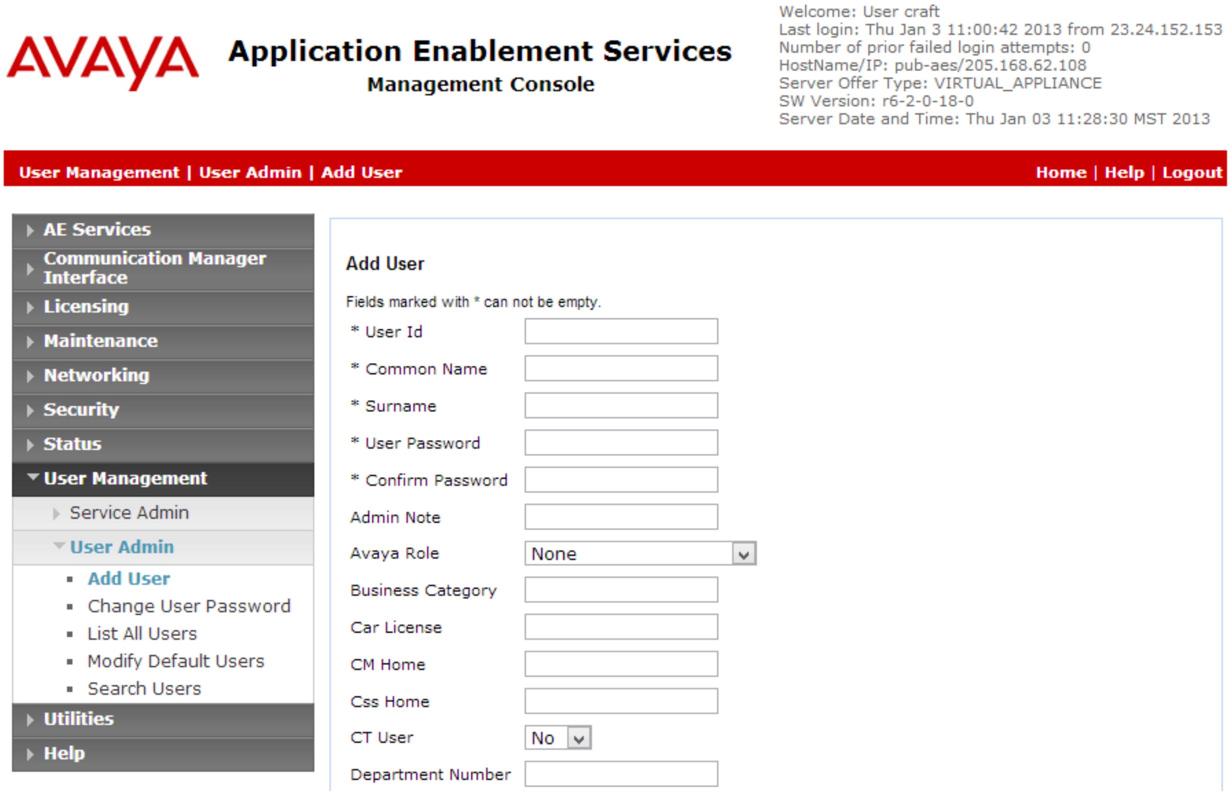
Configuration of Avaya Aura® Application Enablement Services requires the following:

- Creating a user account for E911 Manager
- Creating a Switch Connection to Communication Manager
- Creating TSAPI Link

6.1. Configure User Account for E911 Manager

All administration is performed via a web browser, using URL 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**.



Welcome: User craft
Last login: Thu Jan 3 11:00:42 2013 from 23.24.152.153
Number of prior failed login attempts: 0
HostName/IP: pub-aes/205.168.62.108
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-2-0-18-0
Server Date and Time: Thu Jan 03 11:28:30 MST 2013

Add User

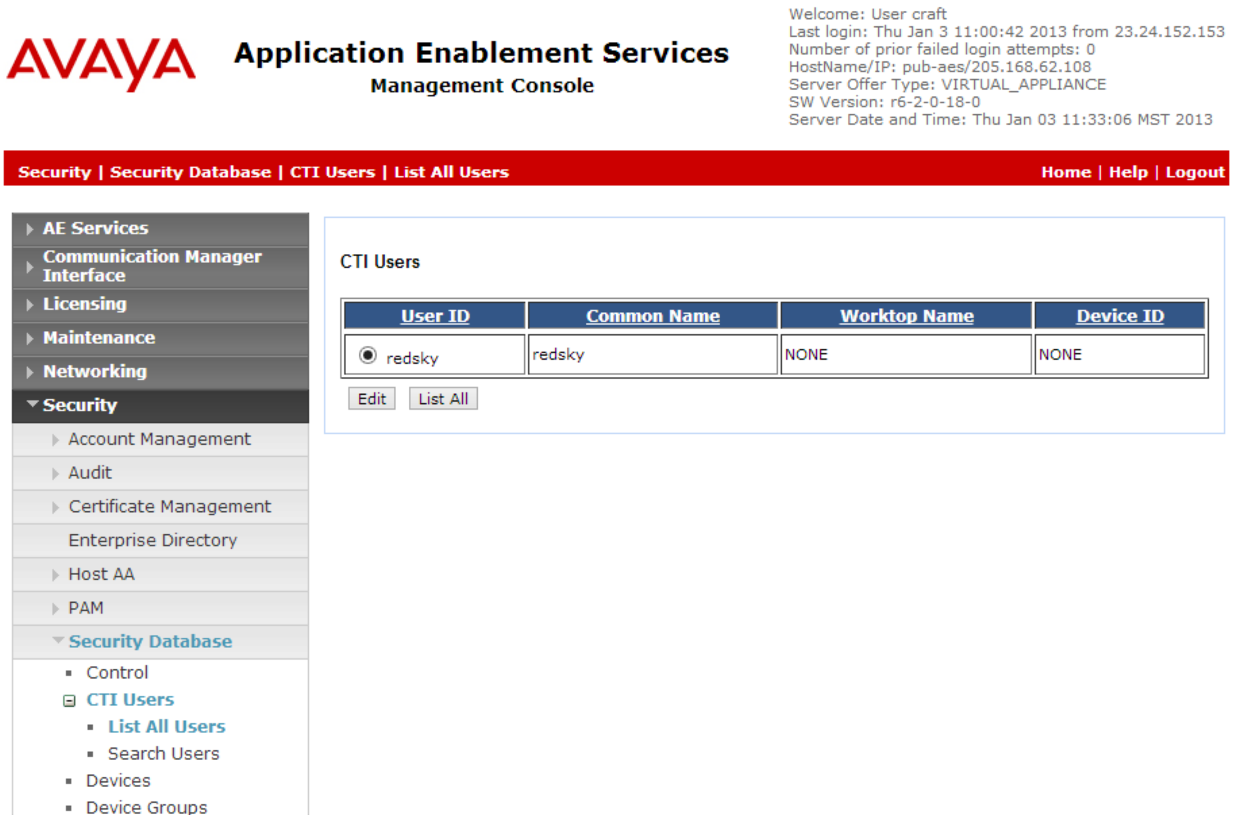
Fields marked with * can not be empty.

* User Id	
* Common Name	
* Surname	
* User Password	
* Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	No
Department Number	

Fill in **User Id, Common Name, Surname, User Password** and **Confirm Password**. Set the **CT User** to **Yes,** and **Apply**.

If the Security Database is enabled on Application Enablement Services, set the RedSky user account to Unrestricted Access to enable any device (station, ACD extension, DMCC port) to be used implicitly. This step avoids the need to duplicate administration.

Navigate to **Security → Security Database → CTI Users → List All Users**.

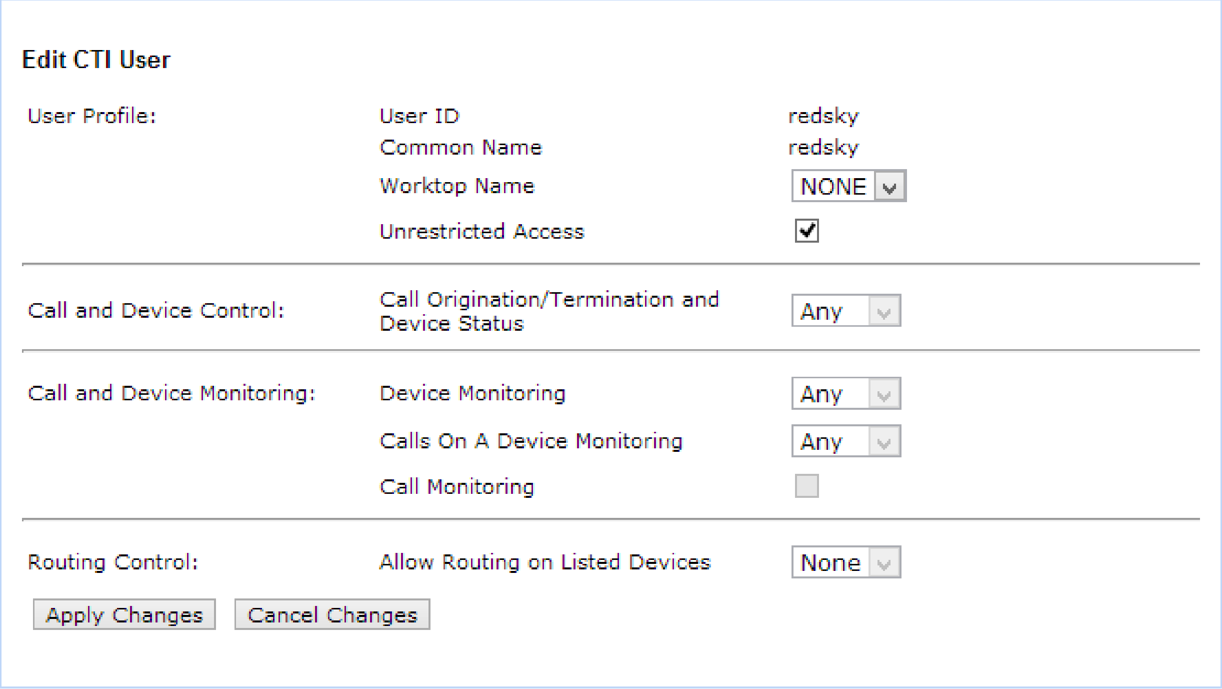


Welcome: User craft
Last login: Thu Jan 3 11:00:42 2013 from 23.24.152.153
Number of prior failed login attempts: 0
HostName/IP: pub-aes/205.168.62.108
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-2-0-18-0
Server Date and Time: Thu Jan 03 11:33:06 MST 2013

CTI Users

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

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



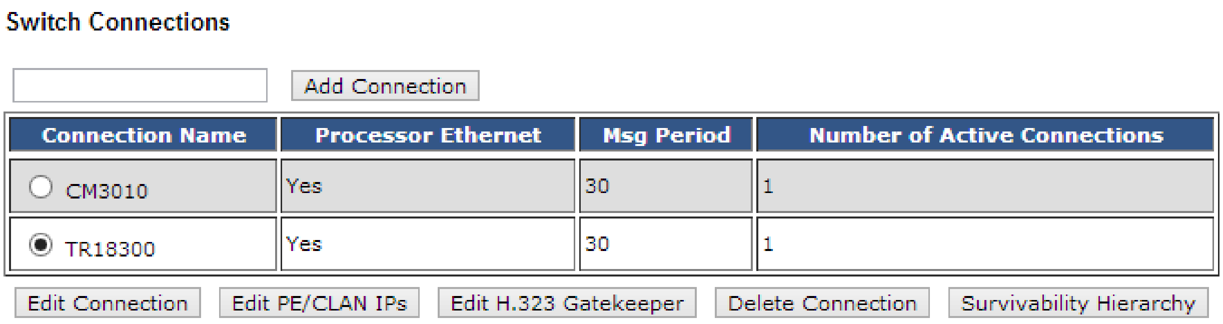
Edit CTI User

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

6.2. Configure Communication Manager Switch Connections

To add links to 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.

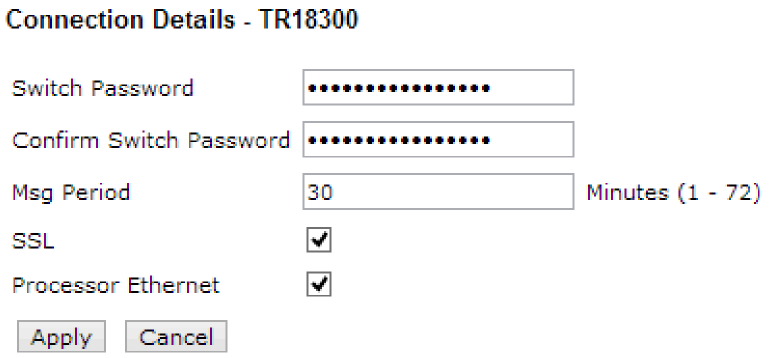
This was previously configured as **TR18300** for this test environment:



Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
○ CM3010	Yes	30	1
● TR18300	Yes	30	1

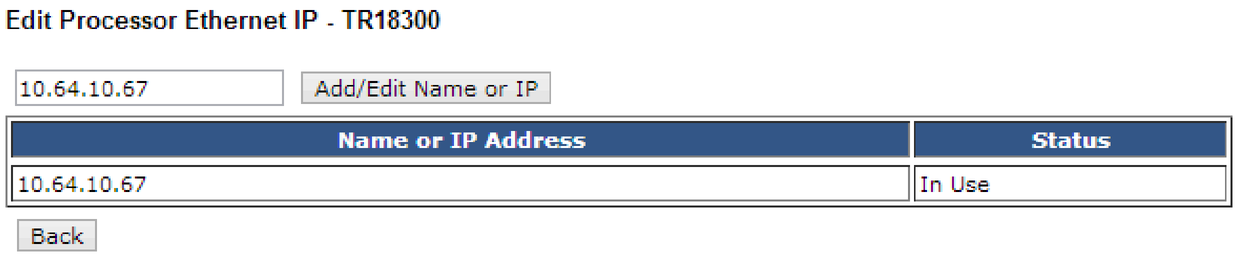
Use the **Edit Connection** button shown above to configure the connection. Enter the **Switch Password** and check the **Processor Ethernet** box if the **procr** interface is used, as shown below. This must match the password configured when adding AESVCS connection in Communication Manager.



Connection Details - TR18300

Switch Password	••••••••••••••••
Confirm Switch Password	••••••••••••••••
Msg Period	30 Minutes (1 - 72)
SSL	☑
Processor Ethernet	☑

Use the **Edit PE/CLAN IPs** button (shown in this section's first screen shot above) to configure the **procr** or **CLAN** IP Address(es) for TSAPI message traffic.

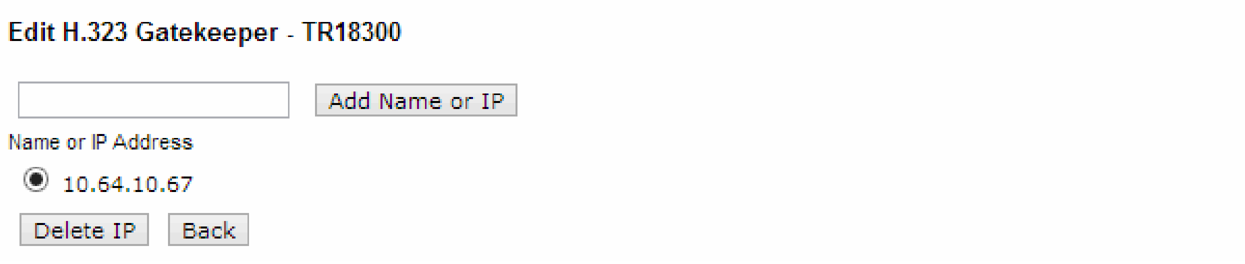


Edit Processor Ethernet IP - TR18300

10.64.10.67

Name or IP Address	Status
10.64.10.67	In Use

Use the **Edit H.323 Gatekeeper** button (shown in this section's first screen capture above) to configure the **procr** or **CLAN** IP Address(es).



Edit H.323 Gatekeeper - TR18300

Name or IP Address

● 10.64.10.67

6.3. Configure TSAPI Link

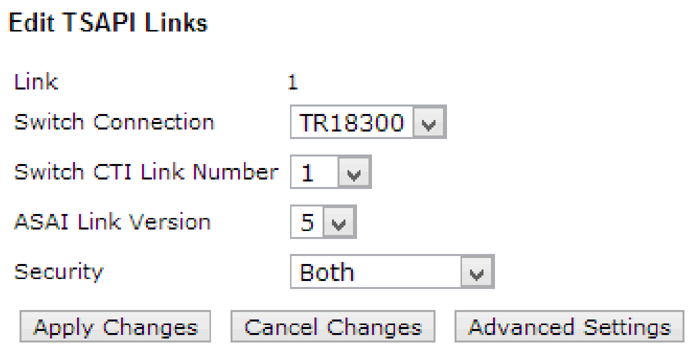
Navigate to the **AE Services** → **TSAPI** → **TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link** (not shown).

Select a **Switch Connection** using the drop down menu. Select the **Switch CTI Link Number** using the drop down menu. The **Switch CTI Link Number** must match the number configured in the **cti-link** form for Communication Manager.

If the application will use Encrypted Links, select **Encrypted** in the **Security** selection box.

Click **Apply Changes**.

Configuration shown below was previously configured.



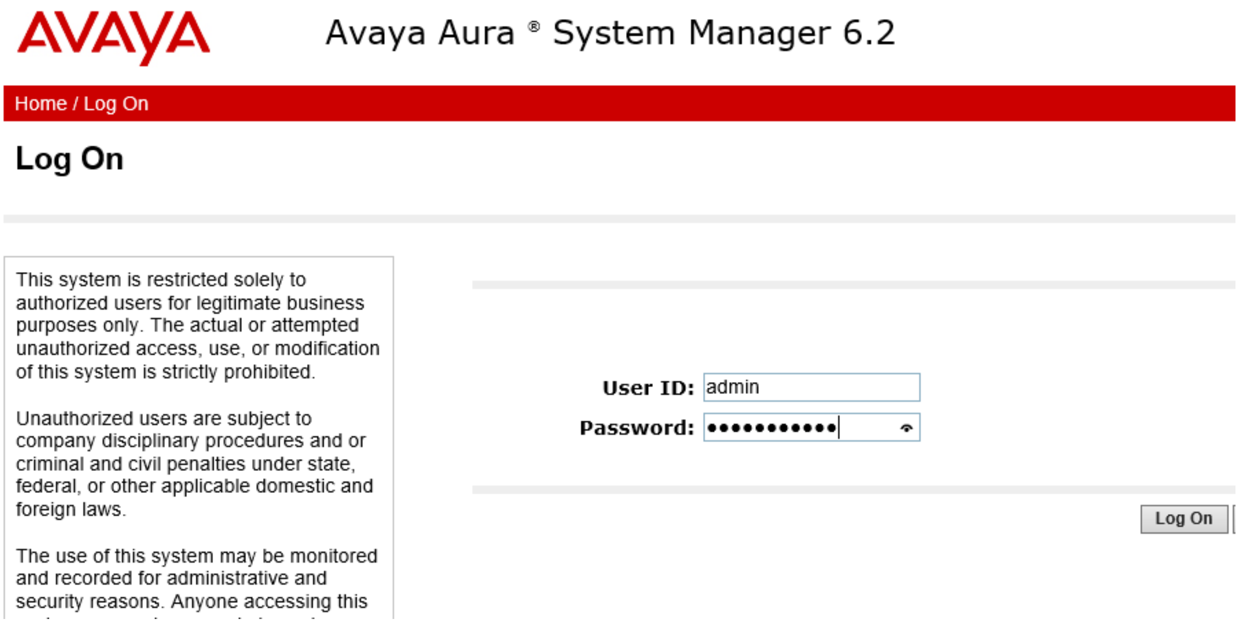
Edit TSAPI Links

Link	1
Switch Connection	TR18300
Switch CTI Link Number	1
ASAI Link Version	5
Security	Both

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 of the System Manager. Log in using appropriate credentials.



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

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

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this

User ID: admin

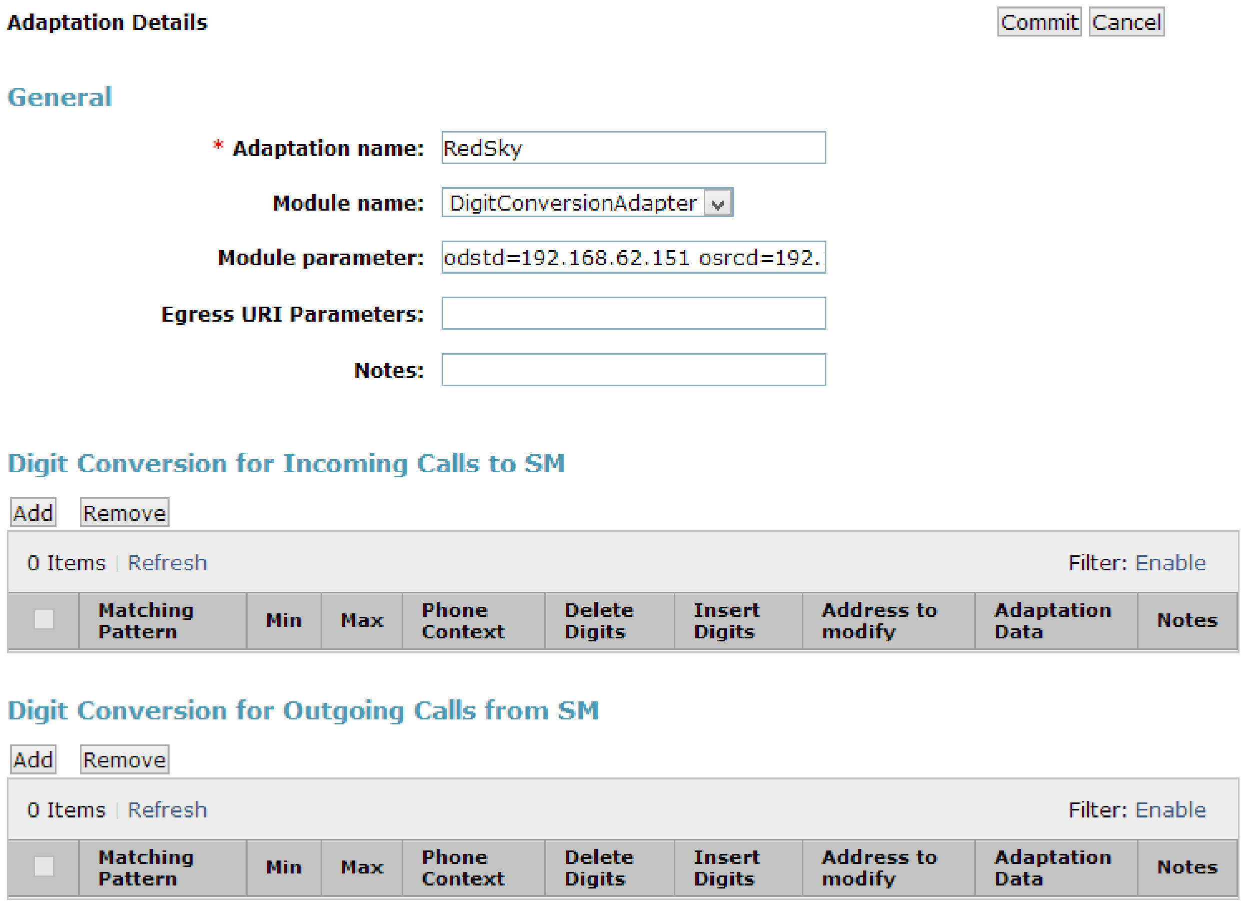
Password: ●●●●●●●●●●●

7.1. Add an Adaptation

Navigate to **Routing → Adaptations**. 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
  - odstd=<RedSky-E911-Manager-IP-Address> osrcd=<Session-Manager-IP-Address> fromto=true
  - During Compliance Test, **odstd=192.168.62.151 osrcd=192.168.62.18 fromto=true,** was used.

Click **Commit** to save changes.



Adaptation Details

General

* Adaptation name: RedSky

Module name: DigitConversionAdapter

Module parameter: odstd=192.168.62.151 osrcd=192.

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

☐	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

Digit Conversion for Outgoing Calls from SM

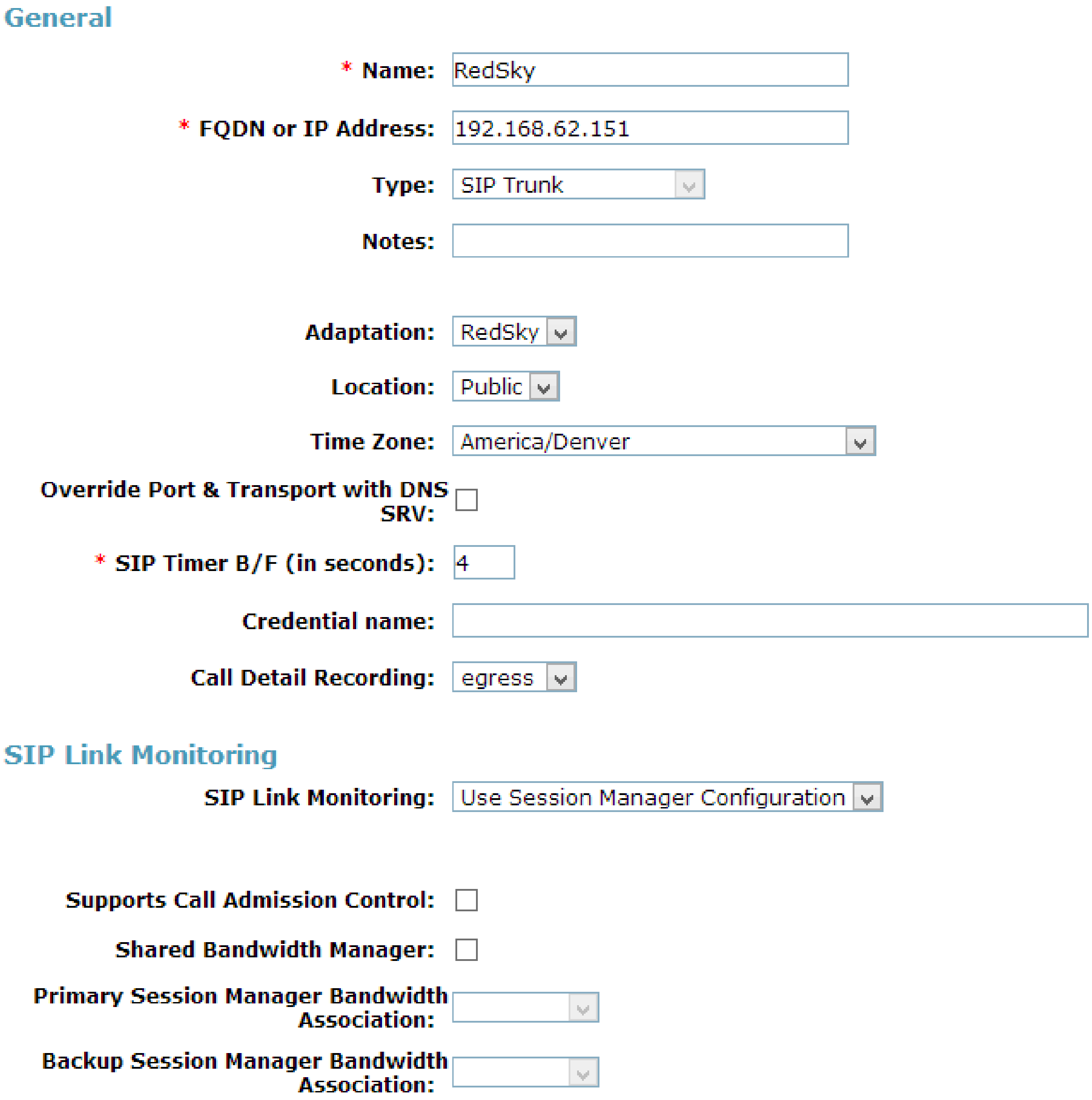
☐	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

7.2. Add a SIP Entity

Navigate to **Routing → SIP Entities.** Click **New** to add a new SIP entity for RedSky E911 Manager.

- Type in a name in **Name.**
- Type in IP address of RedSky E911 Manager 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.

Click **Commit** to save changes.



General

* Name: RedSky
* FQDN or IP Address: 192.168.62.151
Type: SIP Trunk
Notes:
Adaptation: RedSky
Location: Public
Time Zone: America/Denver
Override Port & Transport with DNS SRV: ☐
* SIP Timer B/F (in seconds): 4
Credential name:
Call Detail Recording: egress

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐
Shared Bandwidth Manager: ☐
Primary Session Manager Bandwidth Association:
Backup Session Manager Bandwidth Association:

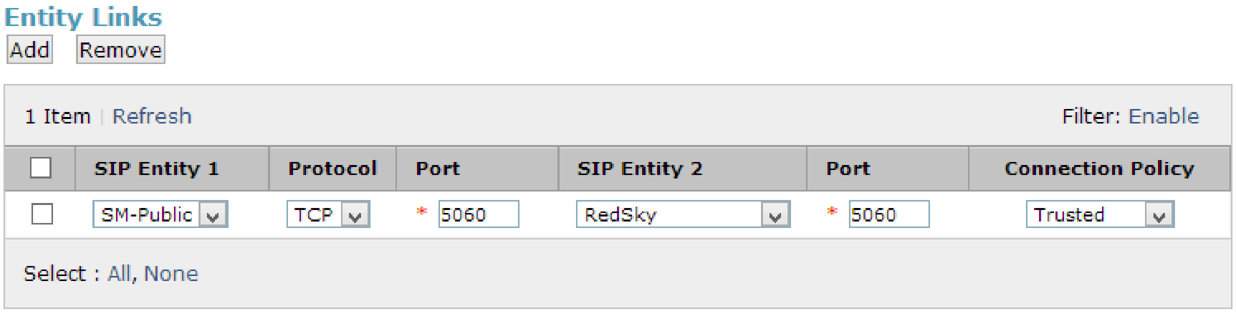
Note: Another SIP Entity will need to be added as an ELIN server. Instead of **SIP Trunk**, select **ELIN server**, when adding a SIP Entity. This is not shown in this document.

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.



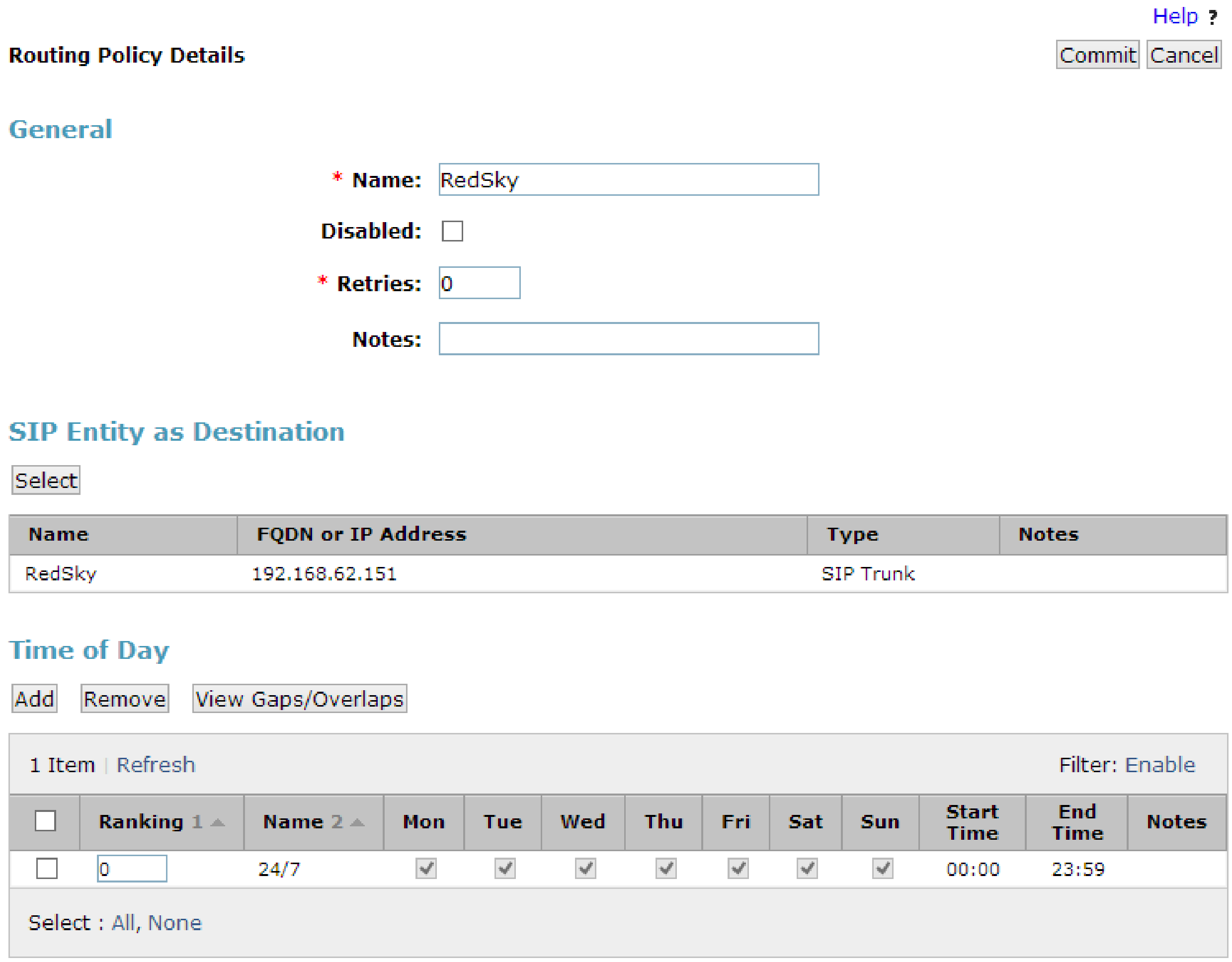
☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
☐	SM-Public	TCP	* 5060	RedSky	* 5060	Trusted

7.4. Add a Routing Policy

Navigate to **Routing → Routing Policies.** Click **New** to add a new Routing Policy for RedSky E911 Manager.

- 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** and click **Select** (not shown).
- Under **Time of Day**, select a time range. During compliance test, a pre-configured time range was used.

Click **Commit** to save changes.



Routing Policy Details

General

* Name: RedSky

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
RedSky	192.168.62.151	SIP Trunk	

Time of Day

1 Item

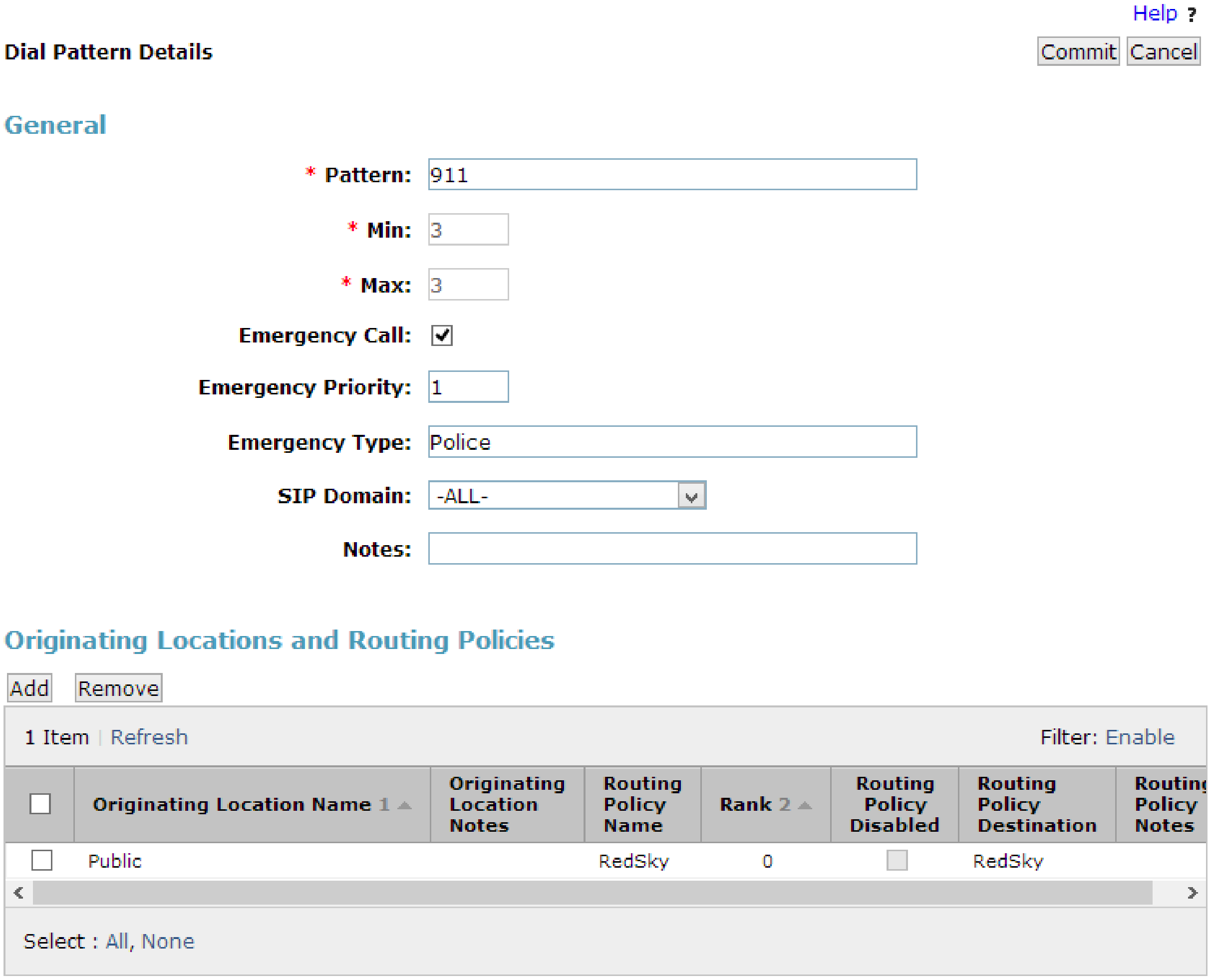
☐	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	

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 previous step

Click **Commit** to save changes.



Dial Pattern Details

General

* **Pattern:** 911

* **Min:** 3

* **Max:** 3

Emergency Call: ☑

Emergency Priority: 1

Emergency Type: Police

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

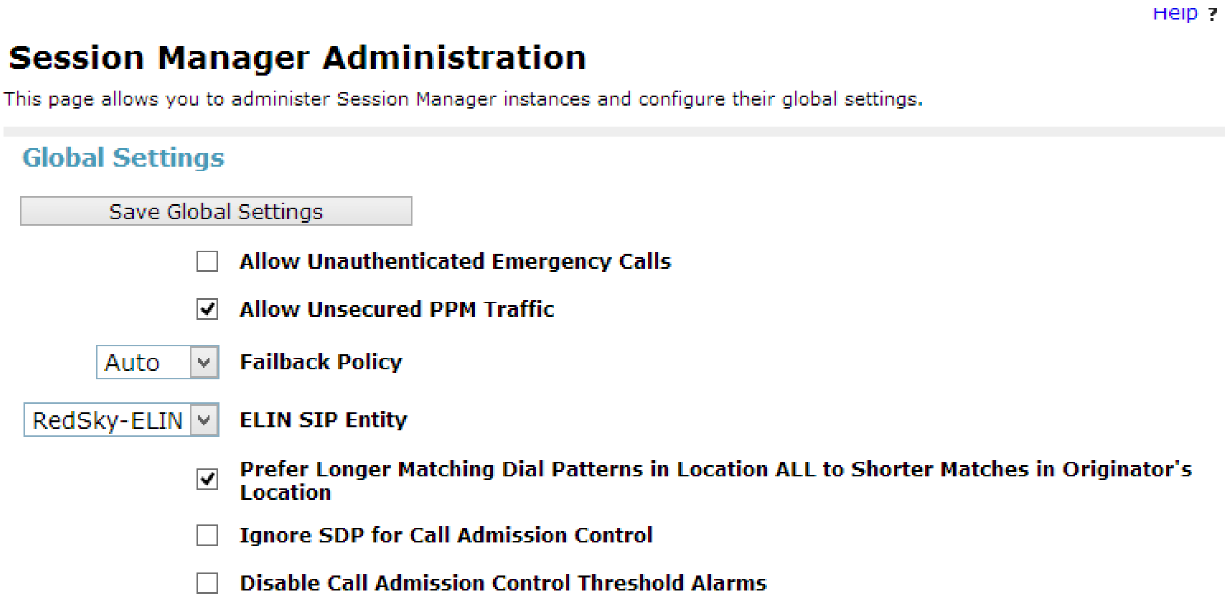
1 Item | Refresh Filter: Enable

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routin Policy Notes
☐	Public		RedSky	0	☐	RedSky	

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 **Save** under **Global Settings** to save the change.



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

Auto Failback Policy

RedSky-ELIN ELIN SIP Entity

☑ Prefer Longer Matching Dial Patterns in Location ALL to Shorter Matches in Originator's Location

☐ Ignore SDP for Call Admission Control

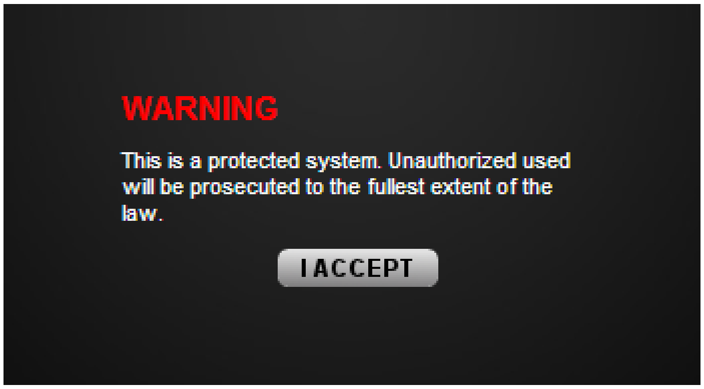
☐ Disable Call Admission Control Threshold Alarms

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 a RedSky Engineer.

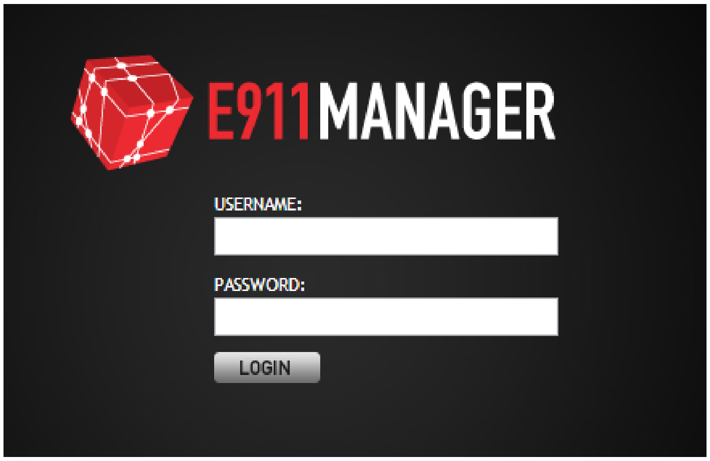
8.1. RedSky E911 Manager Configuration Details

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. Log in using appropriate credentials.



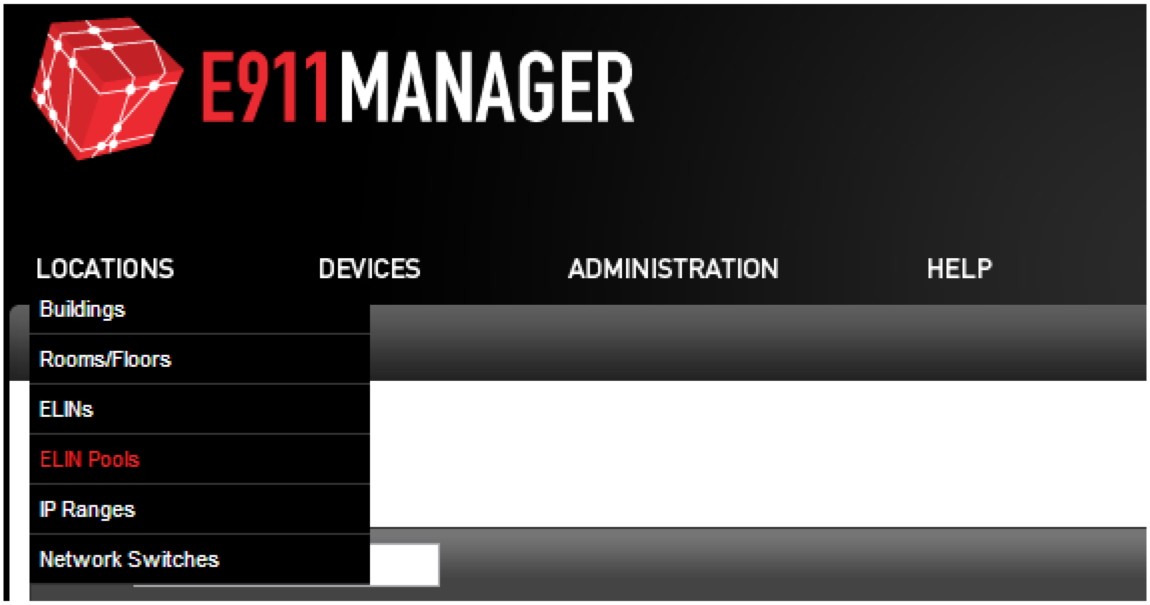
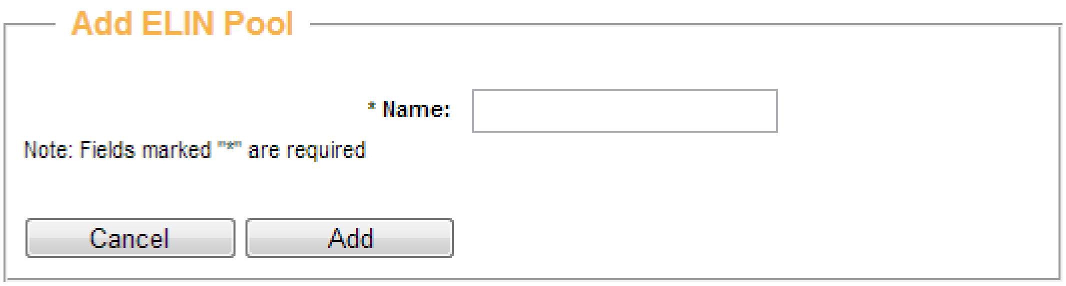
WARNING

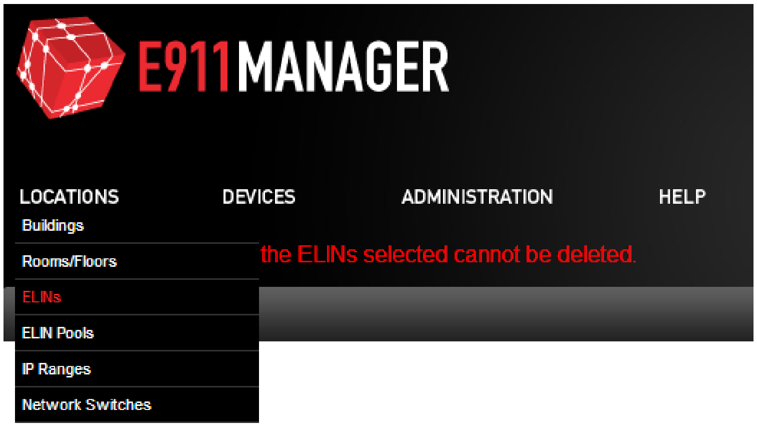
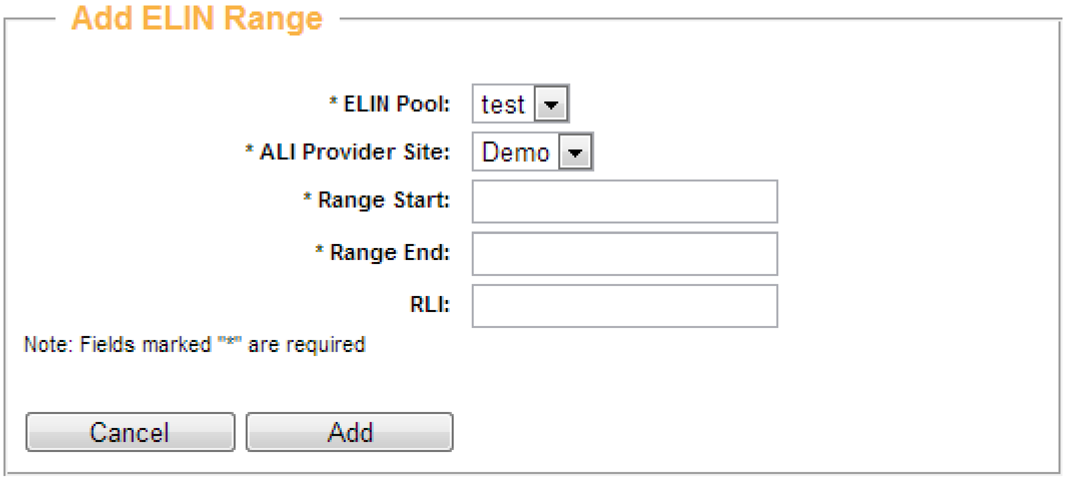
This is a protected system. Unauthorized used will be prosecuted to the fullest extent of the law.



In general, the steps are as follows:

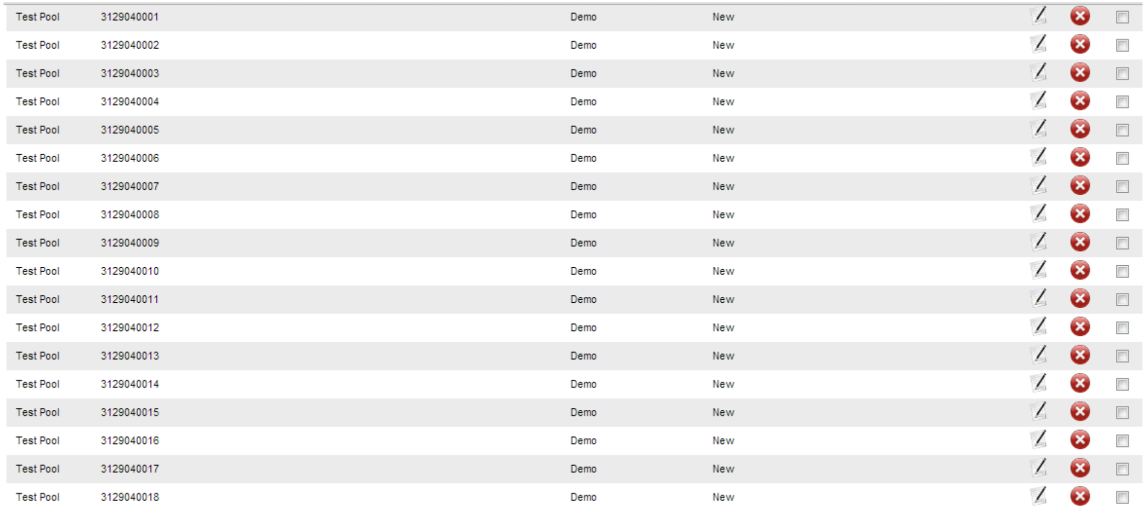
- Define an ELIN Pool
- Create an ELIN Range
- Administer Session Manager Link
- Administer AES Link
- Define Locations – Building and Location
- Administer the IP Address Ranges

Step	Description
1.	**Define an ELIN Pool** Select **ELIN Pools** from the **LOCATIONS** menu.  E911MANAGER LOCATIONS DEVICES ADMINISTRATION HELP Buildings Rooms/Floors ELINs ELIN Pools IP Ranges Network Switches 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.  Add ELIN Pool * Name: Note: Fields marked "*" are required

Step	Description
2.	**Define an ELIN Range** Select **ELINs** from the **LOCATIONS** menu  E911MANAGER LOCATIONS DEVICES ADMINISTRATION HELP Buildings Rooms/Floors ELINs ELIN Pools IP Ranges Network Switches the ELINs selected cannot be deleted. Click the **Add ELIN Range** button. Select an ELIN Pool and ALI Provider Site. Enter start range and end range in Range Start and Range End fields, respectively, and click **Add.**  Add ELIN Range * ELIN Pool: test * ALI Provider Site: Demo * Range Start: * Range End: RLI: Note: Fields marked "*" are required Once the ELINs are added, the following screen is displayed.

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

Once the ELINs are added, the following screen is displayed.

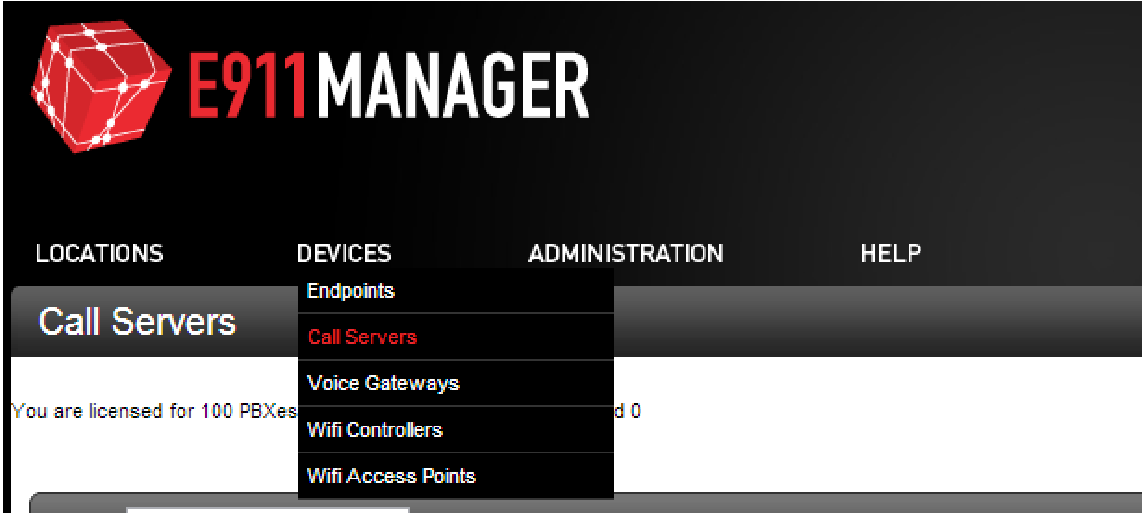


<table>
<tr><td>Test Pool</td><td>3129040001</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040002</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040003</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040004</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040005</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040006</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040007</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040008</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040009</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040010</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040011</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040012</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040013</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040014</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040015</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040016</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040017</td><td>Demo</td><td>New</td><td>☐</td></tr>
<tr><td>Test Pool</td><td>3129040018</td><td>Demo</td><td>New</td><td>☐</td></tr>
</table>

</td></tr>
<tr><td>**3.**</td><td>

Administer the Session Manager link (Optional)

Select **Call Servers** from the **DEVICES** 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.

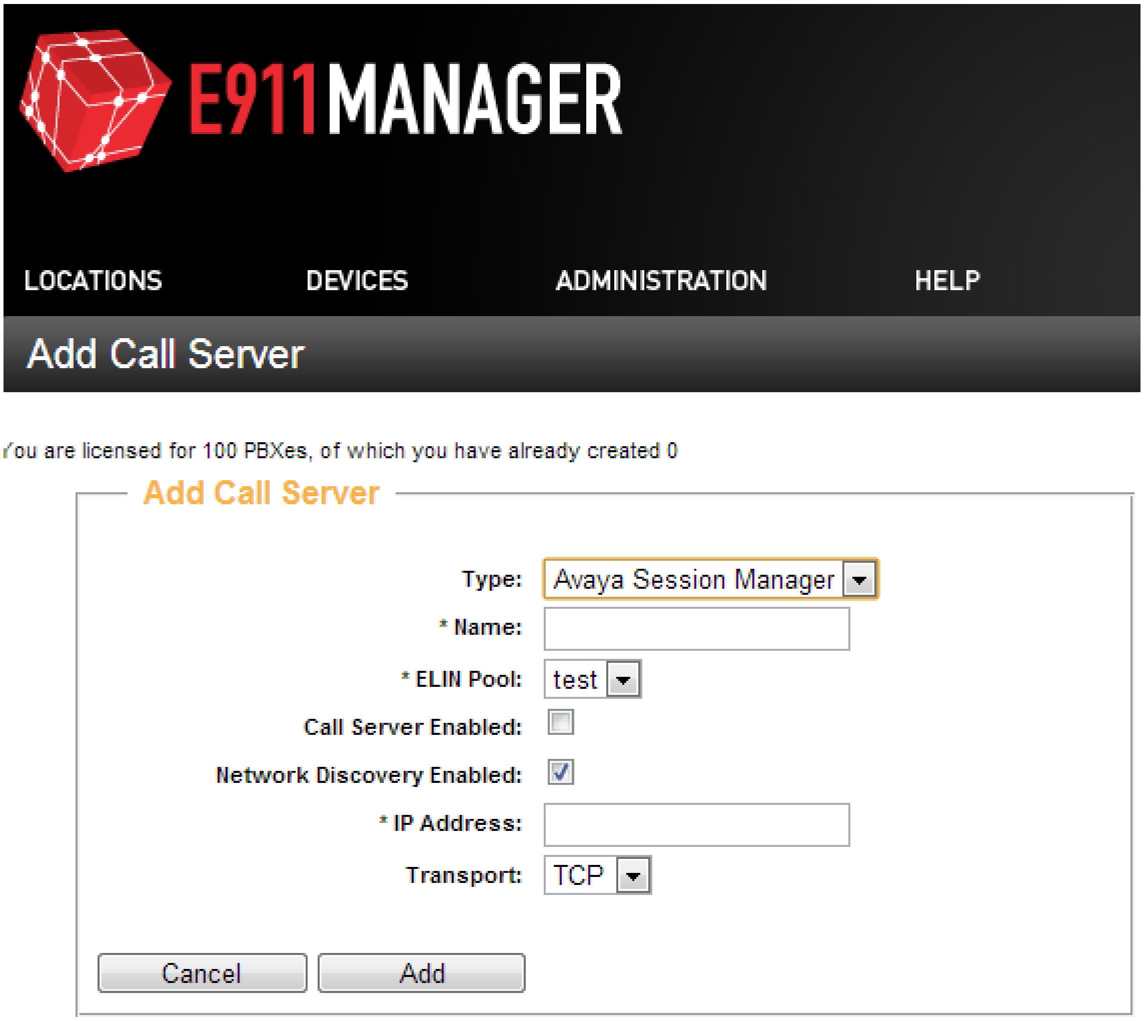


You are licensed for 100 PBXes … d 0

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

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

Enter the **IP address,** 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, but during the compliance testing **TCP** was used.



ou are licensed for 100 PBXes, of which you have already created 0

Add Call Server

Type: Avaya Session Manager

* Name:

* ELIN Pool: test

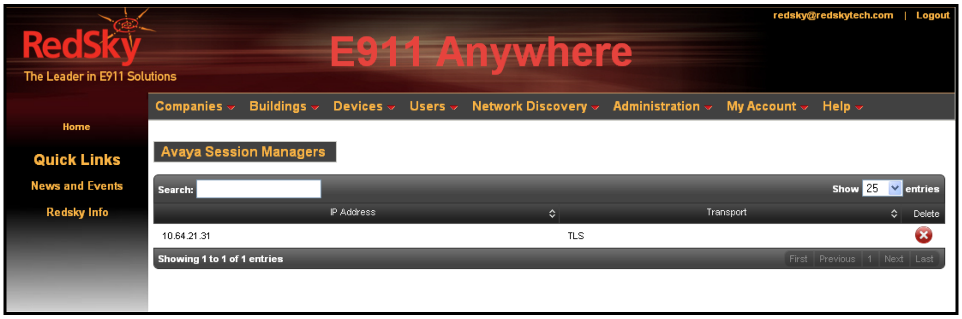
Call Server Enabled: ☐

Network Discovery Enabled: ☑

* IP Address:

Transport: TCP

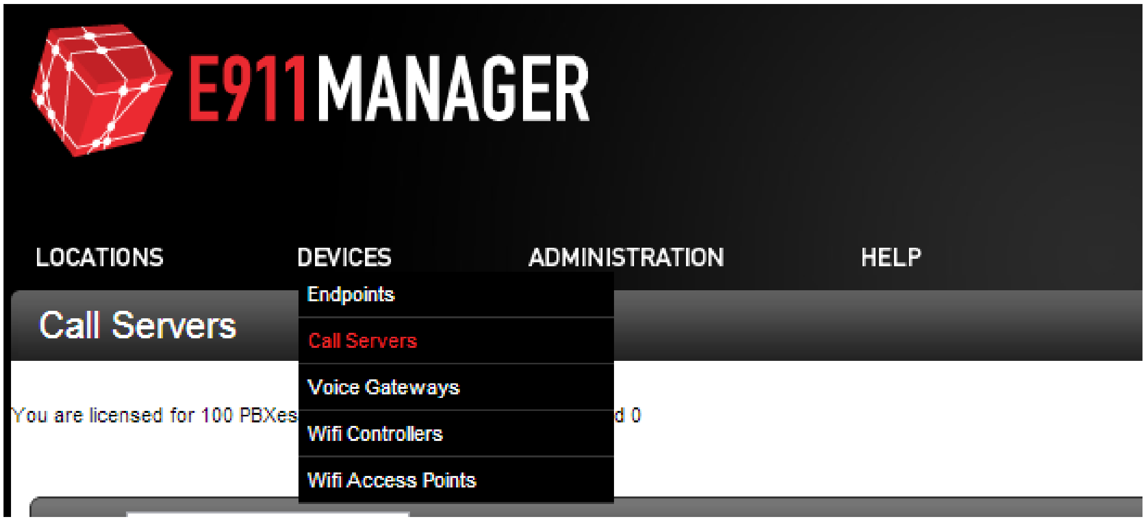
Select **View** from the **Network Discovery > Avaya Session Managers** menu to review the administered entries.

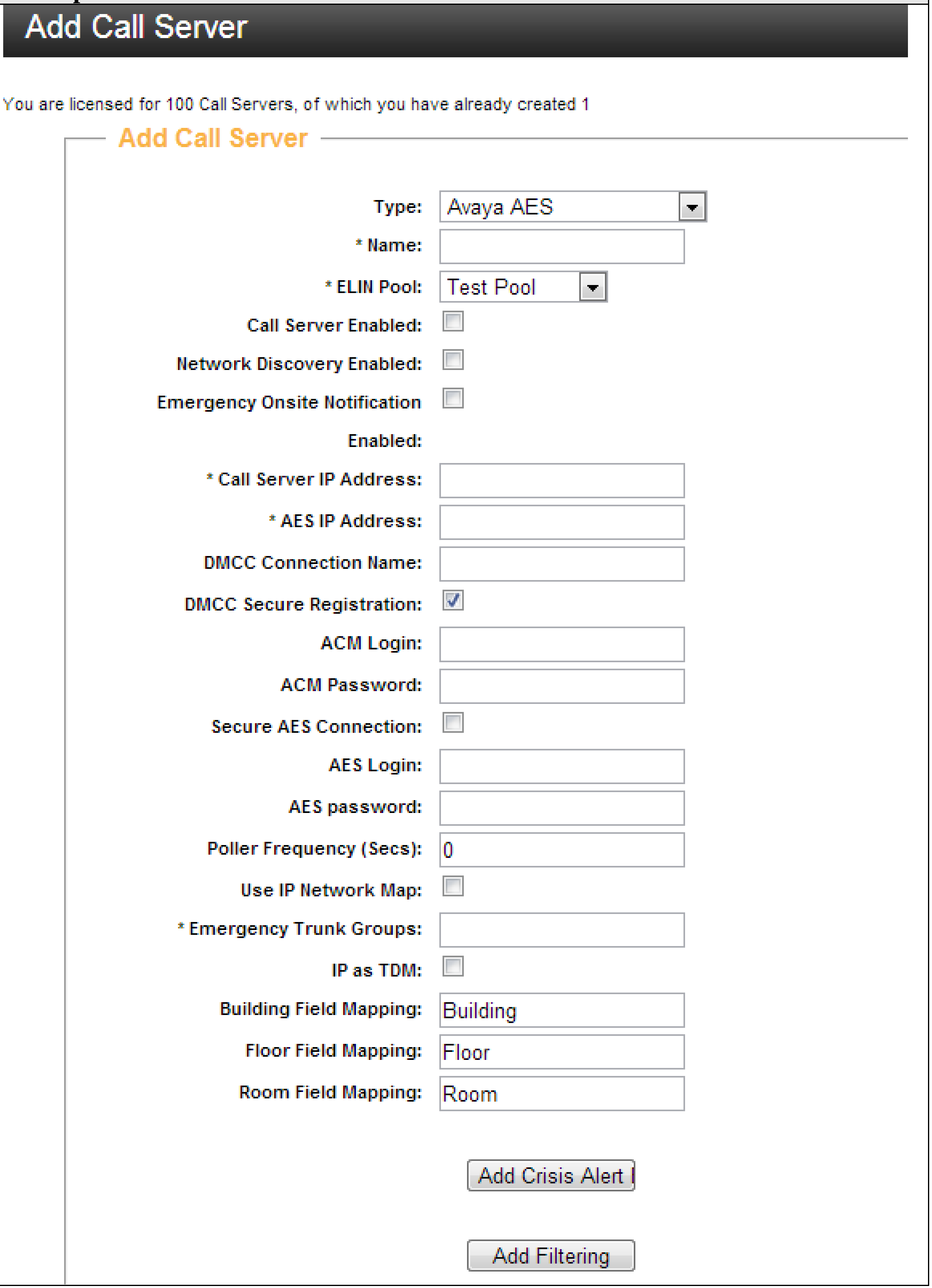


<table>
<tr><th>IP Address</th><th>Transport</th><th>Delete</th></tr>
<tr><td>10.64.21.31</td><td>TLS</td><td>☒</td></tr>
</table>

Showing 1 to 1 of 1 entries

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

Step	Description
4.	**Administer the Avaya AES link (Optional)** Select **Call Servers** from the **DEVICES** 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 LOCATIONS DEVICES ADMINISTRATION HELP Call Servers Endpoints Call Servers Voice Gateways Wifi Controllers Wifi Access Points You are licensed for 100 PBXes d 0 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 trunk group associated with emergency calls, and fill in the rest of the required fields. Finally, fill in the ACM login with username@ACM_IP_Address, fill in the ACM password, fill in the AES login, and fill in the AES password.

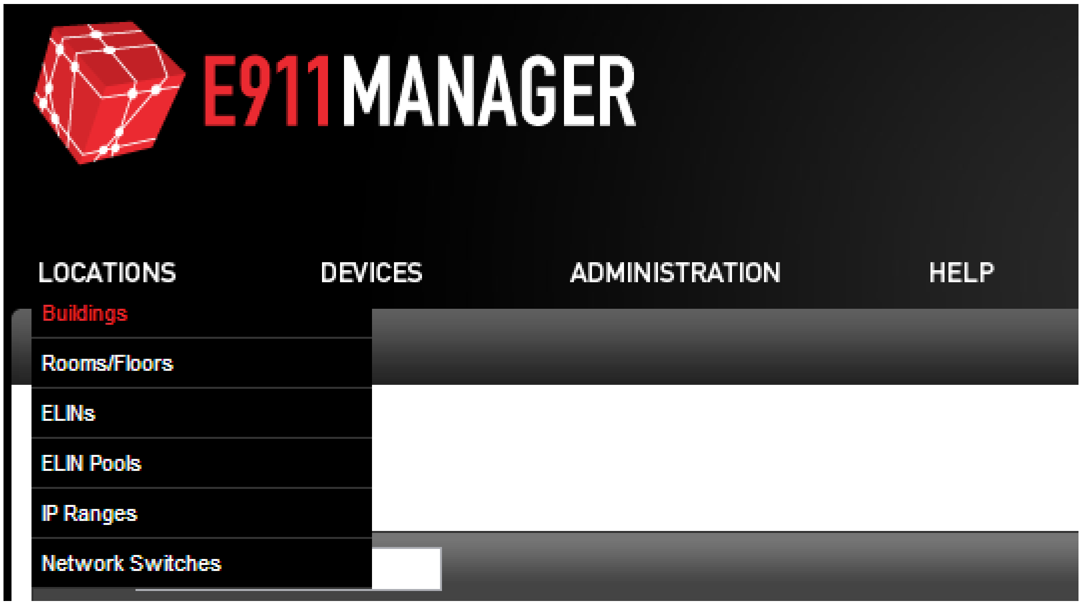
Step	Description
	

Add Call Server

You are licensed for 100 Call Servers, of which you have already created 1

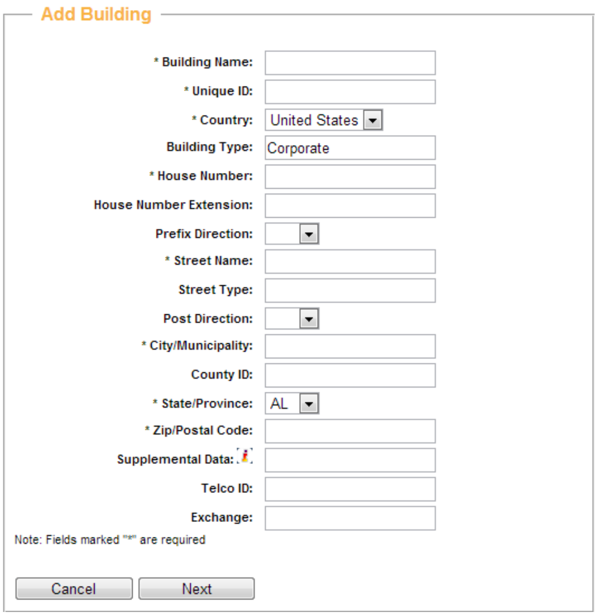
Add Call Server

Type: Avaya AES
* Name:
* ELIN Pool: Test Pool
Call Server Enabled: ☐
Network Discovery Enabled: ☐
Emergency Onsite Notification Enabled: ☐
* Call Server IP Address:
* AES IP Address:
DMCC Connection Name:
DMCC Secure Registration: ☑
ACM Login:
ACM Password:
Secure AES Connection: ☐
AES Login:
AES password:
Poller Frequency (Secs): 0
Use IP Network Map: ☐
* Emergency Trunk Groups:
IP as TDM: ☐
Building Field Mapping: Building
Floor Field Mapping: Floor
Room Field Mapping: Room

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 **Add Building** from the **Location->Buildings** menu to administer general location information. Multiple Buildings may be administered by repeating the process. For the compliance test, two buildings were defined.  E911MANAGER LOCATIONS DEVICES ADMINISTRATION HELP Buildings Rooms/Floors ELINs ELIN Pools IP Ranges Network Switches

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

Click **Validate** then **Add** to complete the entry.

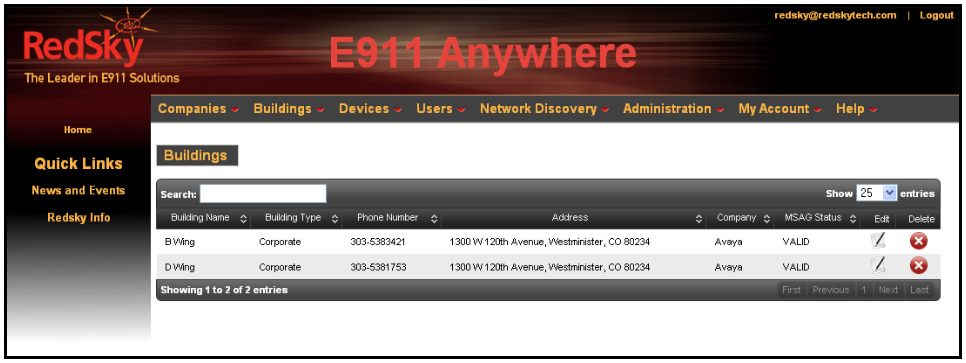


Add Building

* Building Name:
* Unique ID:
* Country: United States
Building Type: Corporate
* House Number:
House Number Extension:
Prefix Direction:
* Street Name:
Street Type:
Post Direction:
* City/Municipality:
County ID:
* State/Province: AL
* Zip/Postal Code:
Supplemental Data:
Telco ID:
Exchange:

Note: Fields marked "*" are required

Select **View** from the **Buildings** menu to see the administered entries.



Buildings

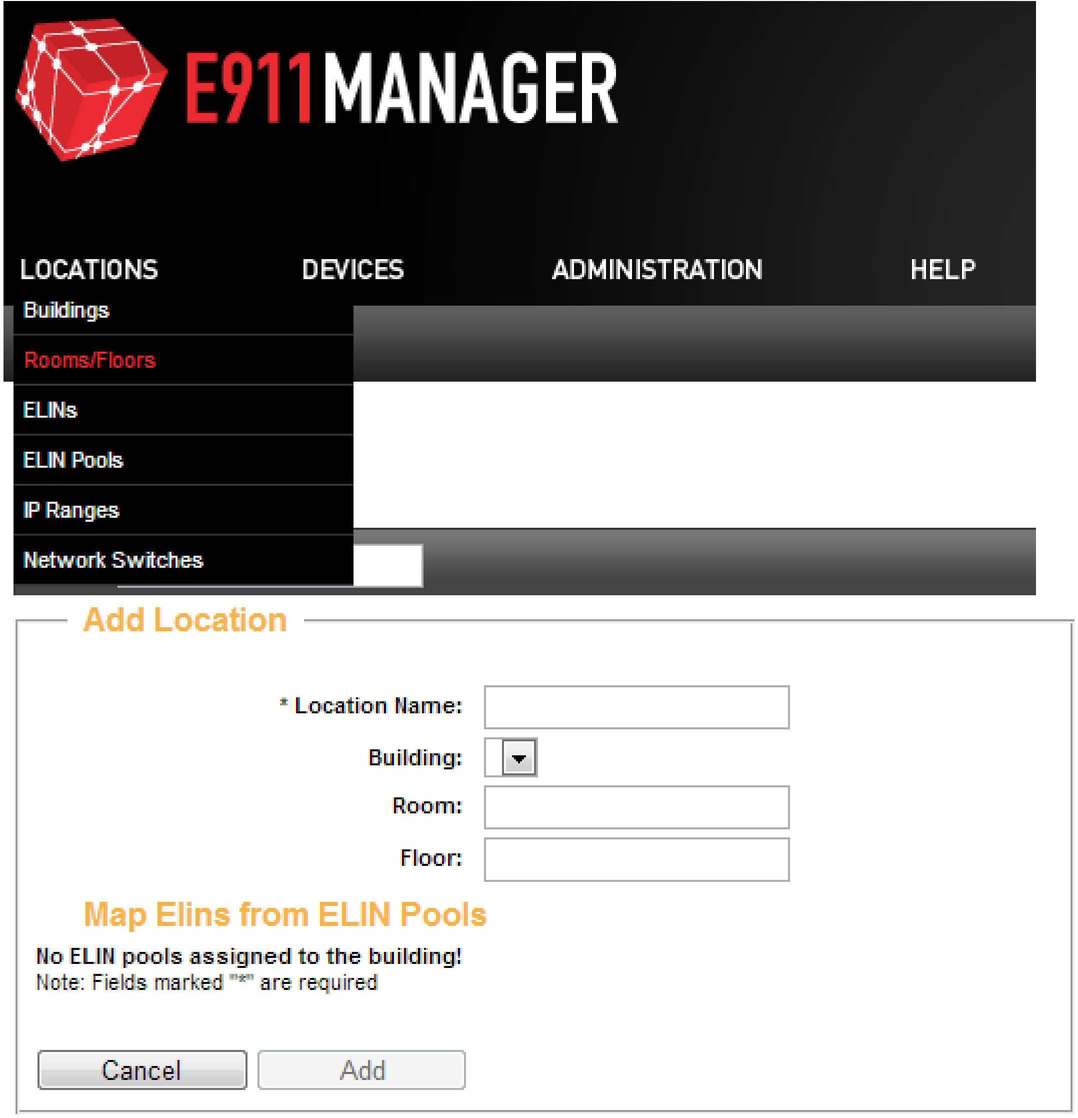
Search:

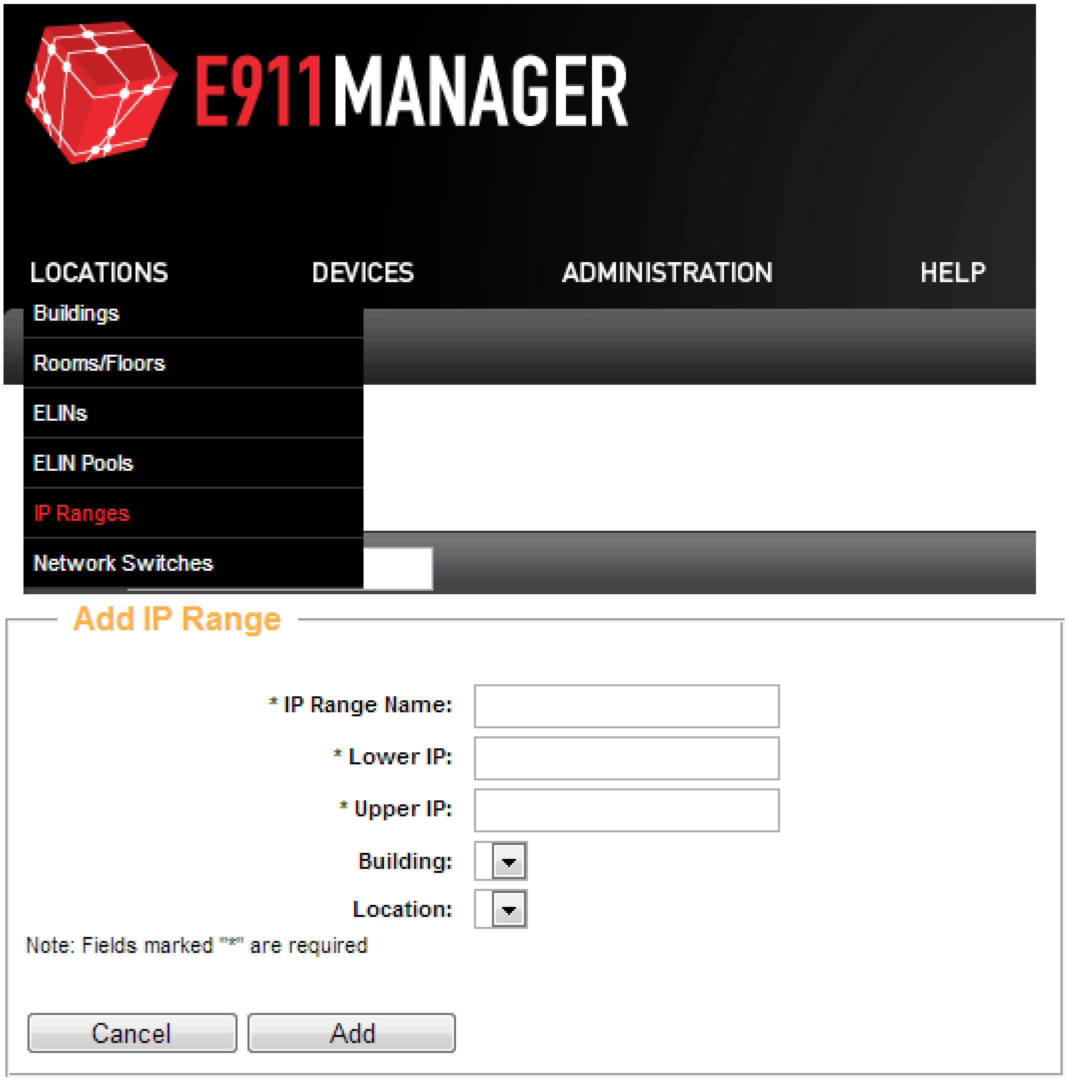
Show 25 entries

<table>
<tr><th>Building Name</th><th>Building Type</th><th>Phone Number</th><th>Address</th><th>Company</th><th>MSAG Status</th><th>Edit</th><th>Delete</th></tr>
<tr><td>B Wing</td><td>Corporate</td><td>303-5383421</td><td>1300 W 120th Avenue, Westminister, CO 80234</td><td>Avaya</td><td>VALID</td><td></td><td></td></tr>
<tr><td>D Wing</td><td>Corporate</td><td>303-5381753</td><td>1300 W 120th Avenue, Westminister, CO 80234</td><td>Avaya</td><td>VALID</td><td></td><td></td></tr>
</table>

Showing 1 to 2 of 2 entries

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

Step	Description
6.	**Define the Company Locations (Locations)** Click the **Add Location** from the **Location->Room/Floors** menu to administer general location information. Multiple locations may be administered by repeating the process.  E911MANAGER LOCATIONS DEVICES ADMINISTRATION HELP Buildings Rooms/Floors ELINs ELIN Pools IP Ranges Network Switches Cancel Add Add Location * Location Name: Building: Room: Floor: Map Elins from ELIN Pools No ELIN pools assigned to the building! Note: Fields marked "*" are required

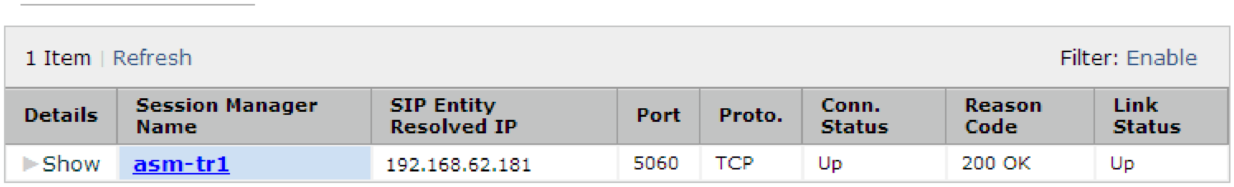
Step	Description
7.	**Administer the IP Address Ranges** Click **Add Range** from the **Locations > IP Ranges** menu to administer the IP Address Ranges that will be associated with each location. For the Compliance Test, one address range entry was created for each Location.  E911MANAGER LOCATIONS DEVICES ADMINISTRATION HELP Buildings Rooms/Floors ELINs ELIN Pools IP Ranges Network Switches Cancel Add **Add IP Range** * IP Range Name: * Lower IP: * Upper IP: Building: Location: Note: Fields marked "*" are required

9. Verification Steps

The following command was executed on the command line of the Session Manager in order to validate the ELIN information provided by RedSky:

```
[root@SM21 craft]# sm cons get allreg
RegistrationKey[commProfileId:55, contactHashKey:sip:54101@10.64.22.204:5061;avaya-sc-
enabled;transport=tls]=RegistrationData[expirationTime=Wed Dec 22 13:57:57 MST 2012,
callId=25_15477c-44ed1a064d27961e_R@10.64.22.204, cSeq=56, elin=3035381753]
RegistrationKey[commProfileId:51, contactHashKey:sip:54102@10.64.22.202:5061;avaya-sc-
enabled;transport=tls]=RegistrationData[expirationTime=Wed Dec 22 14:28:46 MST 2012,
callId=17_154d226e0098314d279bbf_R@10.64.22.202, cSeq=28, elin=3035381753]
RegistrationKey[commProfileId:53, contactHashKey:sip:54103@10.64.22.203:5061;avaya-sc-
enabled;transport=tls]=RegistrationData[expirationTime=Wed Dec 22 14:15:27 MST 2012,
callId=1_1c9429-2c2220014d2ef57f_R@10.64.22.203, cSeq=2, elin=3035381753]
[root@SM21 craft]#
```

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 Manager 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.



Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	asm-tr1	192.168.62.181	5060	TCP	Up	200 OK	Up

10. Conclusion

The RedSky E911 Manager successfully demonstrated the ability to retrieve the IP Address of SIP Endpoints registered with Avaya Aura® Session Manager and return the Emergency Location Identification Number (ELIN) corresponding to the network location of the Endpoint. 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 detect and update endpoints registered with Avaya Aura® Session Manager using layer 2 and layer 3 discovery. This provides customers the convenience of not having to manually keep both systems in synchronization.

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.