Avaya Solution & Interoperability Test Lab

# Application Notes for Amcom Enterprise Alert and Amcom ALI Alert with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager – Issue 1.0

## Abstract

These Application Notes contain instructions for Amcom Enterprise Alert and Amcom ALI Alert with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager to successfully interoperate.

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

Amcom Enterprise Alert (Enterprise Alert) and Amcom ALI Alert (ALI Alert) are Enhanced E911 solutions. Enterprise Alert integrates with the Avaya Aura® Communications Manager by integrating with a PRI trunk which routes emergency (911) calls. By monitoring the D channel, Enterprise Alert captures 911 call events, performs ANI substitution, records the call and provides passive monitoring that bridges one or more phones on the call so that internal resources can listen to the call. ALI Alert monitors a crises alert phone to capture 911 call events. It provides the same features as Enterprise Alert except Passive monitoring and call recording. Both solutions rely on Avaya Site Administration to automatically obtain the extension and extension location of the non-IP phones. Both solutions rely on the Amcom Avaya inventory function to automatically obtain extension and MAC address of Avaya IP phones (SIP and H.323). Both solutions rely on Amcom's IP phone tracking function and Avaya's Push interface to automatically obtain the location of each IP phone extension. Link layer discovery is used to track the location of the IP phones' MAC address.
To achieve the above functionality Amcom Enterprise Alerts uses the following Avaya Interfaces:

- Avaya Aura® Communication Manager – PRI Interface (Enterprise Alert)
- Avaya Aura® Communications Manager – Crises Alert phone (ALI Alert)
- Avaya Aura® Application Enablement Services – SMS Interface
- Avaya Aura® Communications Manager – H.323 phone inventory
- Avaya Aura® Session manager – SIP phone inventory
- Avaya Site Administration
- Avaya Aura® Communication Manager and Avaya IP Deskphones – SNMP interface
- Avaya IP Deskphones – Push Interface

# 2. General Test Approach and Test Results

General test approach was to verify that Amcom Enterprise Alert and ALI Alert are able to successfully integrate with various Avaya Interfaces. Function test scenarios are mentioned in **Section 2.1**

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 testing contained functional test scenarios:

- Location information retrieval using Avaya Site Administration and upload to Amcom ALI Database table
- Avaya IP Endpoints extension and MAC address upload to Amcom ALI database table
- Avaya 9600 Deskphone registration to Amcom Push Application
- Update Emergency Location Extension for Avaya IP Endpoints
- Obtain Emergency Location Extension for Avaya IP Endpoints
- Tracking Avaya IP Endpoints
- Bridging on a phone to an active 911 call via a listen only bridge
- Display of 911 caller extension and location on a networked PC via the Amcom Sentry notification feature.

## 2.2. Test Results

All planned test cases passed.

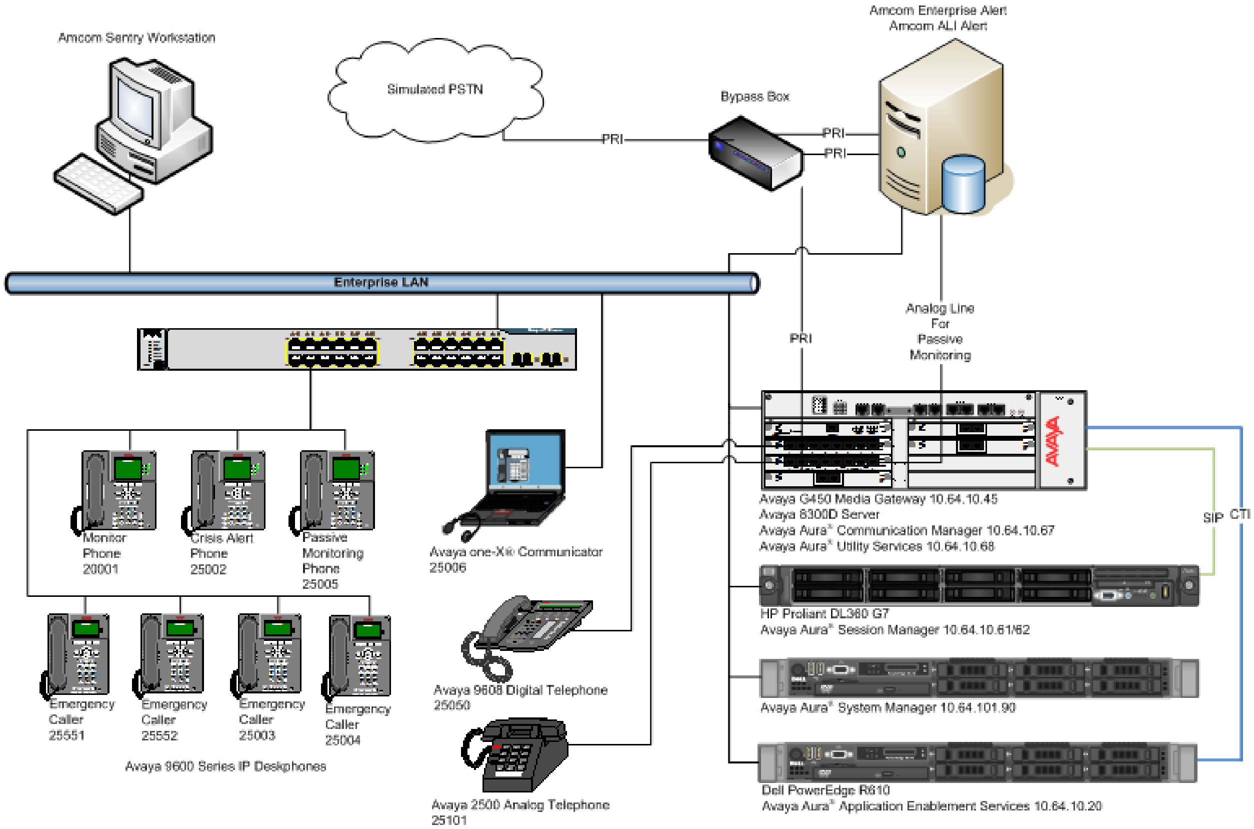
## 2.3. Support

Technical support for the Amcom Enterprise Alert and ALI Alert solution can be obtained by contacting Amcom:

- URL – http://www.amcomsoftware.com
- Phone – (888) 797-7487

# 3. Reference Configuration

**Figure 1** illustrates a sample configuration that consists of Avaya Products and Amcom Enterprise Alert and Amcom ALI Alert. Enterprise Alert uses a configuration that enables the 911 event determination, Passive Monitoring and ANI insertion on the PRI. ALI Alert uses a configuration that uses the Crises Alert phone for 911 call event determination and SMS for ANI insertion (i.e. setting the emergency location extension in the station record).



Amcom Sentry Workstation
Simulated PSTN
PRI
Bypass Box
PRI
PRI
Amcom Enterprise Alert
Amcom ALI Alert
Enterprise LAN
PRI
Analog Line For Passive Monitoring
Monitor Phone 20001
Crisis Alert Phone 25002
Passive Monitoring Phone 25005
Avaya one-X® Communicator 25006
Emergency Caller 25551
Emergency Caller 25552
Emergency Caller 25003
Emergency Caller 25004
Avaya 9600 Series IP Deskphones
Avaya 9608 Digital Telephone 25050
Avaya 2500 Analog Telephone 25101
Avaya G450 Media Gateway 10.64.10.45
Avaya 8300D Server
Avaya Aura® Communication Manager 10.64.10.67
Avaya Aura® Utility Services 10.64.10.68
SIP
CTI
HP Proliant DL360 G7
Avaya Aura® Session Manager 10.64.10.61/62
Avaya Aura® System Manager 10.64.101.90
Dell PowerEdge R610
Avaya Aura® Application Enablement Services 10.64.10.20

**Figure 1:** Test Configuration for Amcom

# 4. Equipment and Software Validated

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

| Equipment/Software | Release/Version |
|---|---|
| Avaya S8300D Server<br>Avaya Aura® Communication Manager | 6.3 SP3<br>R016x.03.0.124.0 |
| Avaya Aura® Session Manager | 6.3 SP5<br>6.3.5.0.635005 |
| Avaya Aura® System Manager | 6.3 SP5<br>6.3.0.8.5682 |
| Avaya G450 Media Gateway | 31.20.0 |
| Avaya Aura® Application Enablement Services | 6.3.0.0.212 |
| Avaya 9600 Series Deskphones | Various – Latest |
| Amcom Enterprise Alert/ALI Alert | 11.1 |

# 5. Configure Avaya Aura® Communication Manager

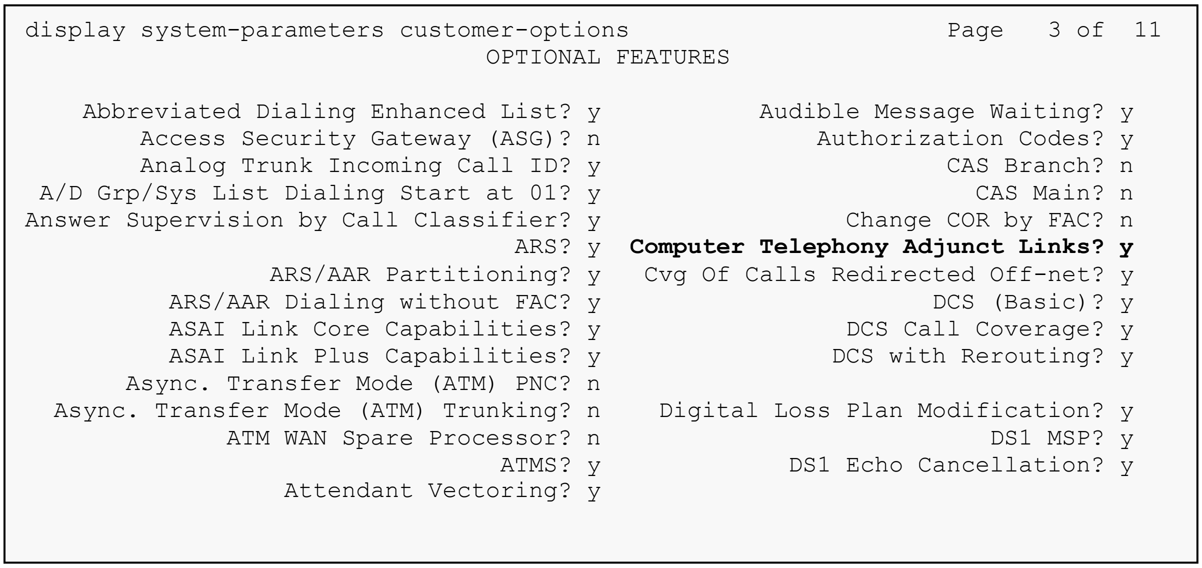
This section contains steps necessary to configure Amcom Enterprise Alert and Amcom ALI Alert successfully with Communication Manager.

All configurations in Communication Manager were performed via SAT terminal.

## 5.1. Verify Feature and License

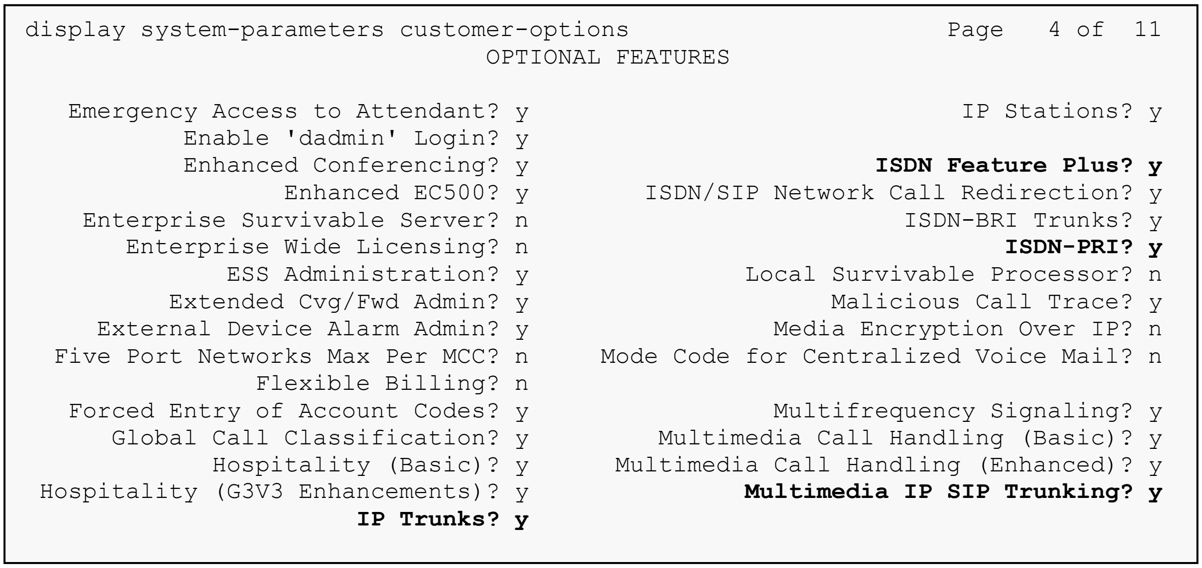
Enter the **display system-parameters customer-options** command and ensure that the following features are enabled.

One Page 3, verify **Computer Telephone Adjunct Links** is set to **y.**



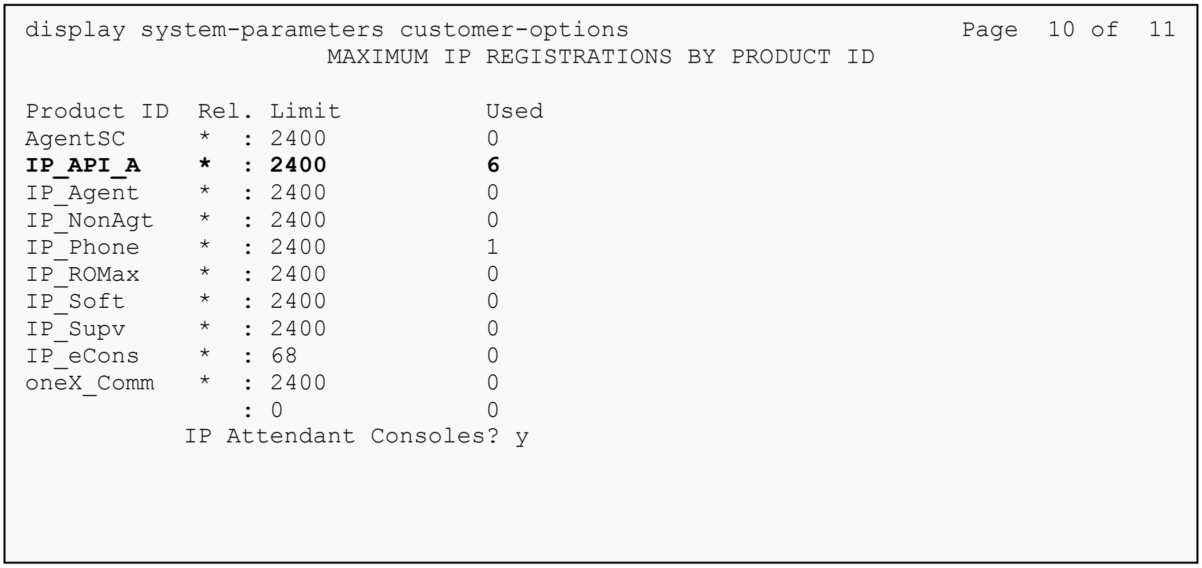
```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? y                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

On Page 4, verify **ISDN Feature Plus, ISDN-PRI, IP Trunks** and **Multimedia IP SIP Trunking** are set to **y.**



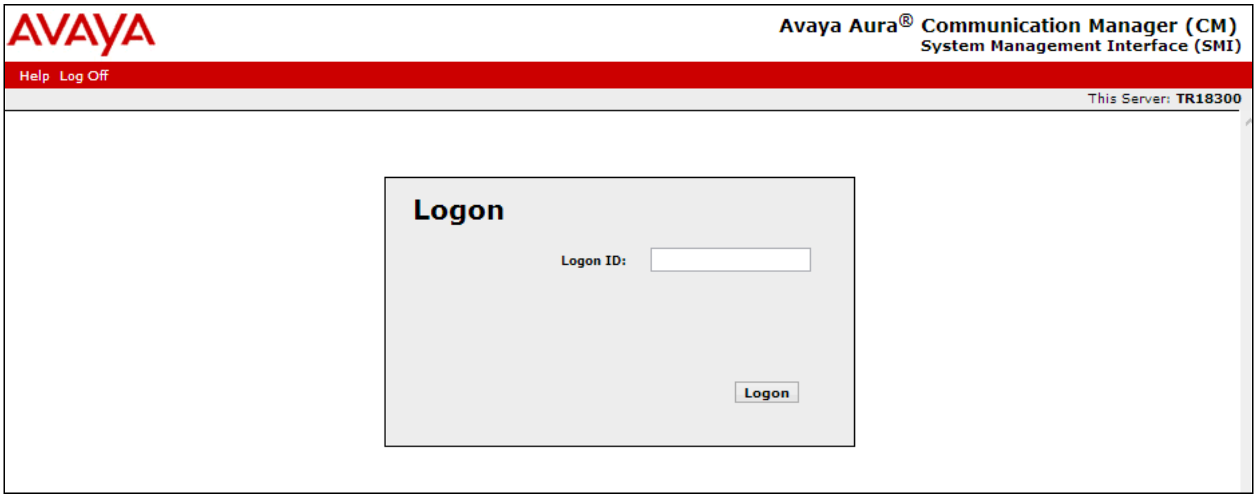
```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                        ISDN Feature Plus? y
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? y               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? y                 Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                 Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y               Multimedia IP SIP Trunking? y
                       IP Trunks? y
```

On Page 10, verify **IP_API_A** has a sufficient limit.

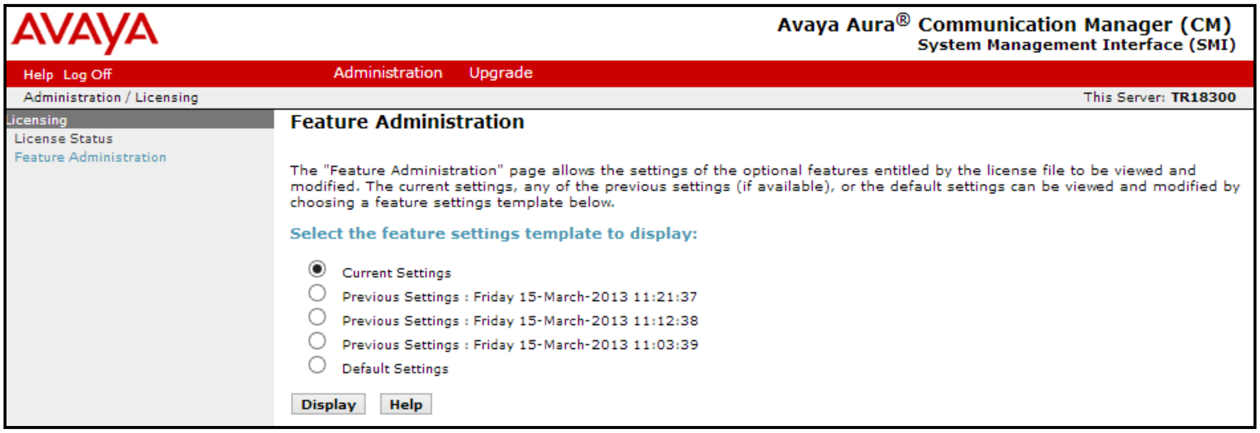


```
display system-parameters customer-options                       Page  10 of   11
                     MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit          Used
AgentSC     *  : 2400           0
IP_API_A    *  : 2400           6
IP_Agent    *  : 2400           0
IP_NonAgt   *  : 2400           0
IP_Phone    *  : 2400           1
IP_ROMax    *  : 2400           0
IP_Soft     *  : 2400           0
IP_Supv     *  : 2400           0
IP_eCons    *  : 68             0
oneX_Comm   *  : 2400           0
               : 0              0
           IP Attendant Consoles? y
```

From a web browser, use the http://<ip-address>, where ip-address is the ip address of Communication Manager, URL to access System Management Interface for Communication Manager. Log in using appropriate credentials.


Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
This Server: TR18300
Logon
Logon ID:
Logon

Navigate to **Administration → Licensing → Feature Administration**. Select **Current Settings** and click **Display**.



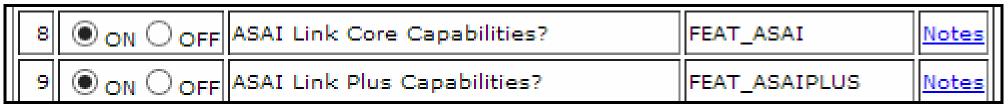
Feature Administration

The "Feature Administration" page allows the settings of the optional features entitled by the license file to be viewed and modified. The current settings, any of the previous settings (if available), or the default settings can be viewed and modified by choosing a feature settings template below.

Select the feature settings template to display:

● Current Settings
○ Previous Settings : Friday 15-March-2013 11:21:37
○ Previous Settings : Friday 15-March-2013 11:12:38
○ Previous Settings : Friday 15-March-2013 11:03:39
○ Default Settings

Verify **ASAI Link Core Capabilities** and **ASAI Link Plus Capabilities** are available and turned on.



| | | | | |
|---|---|---|---|---|
| 8 | ● ON ○ OFF | ASAI Link Core Capabilities? | FEAT_ASAI | Notes |
| 9 | ● ON ○ OFF | ASAI Link Plus Capabilities? | FEAT_ASAIPLUS | Notes |

## 5.2. Configure Site Data

To configure specific building codes for a site, use **change site-data** command.
One **Page 1**, add entries for building codes. For compliance test, two entries of **ABC** and **EFG** were added.

```
change site-data                                                Page   1 of   4
                   SITE DATA USER DEFINITION
                     VALID BUILDING FIELDS



  ABC
  EFG
```

## 5.3. Configure Stations

Use **add station *n*** command to add a station, where ***n*** is an available station extension. This station will be used my Amcom Enterprise Alert as a monitoring station for Crisis Alert. Configure the station as follows, on Page 1:

- In **Name** field, enter a descriptive name
- Set **Type** to the type of the telephones
- Enter a **Security Code**
- Set **IP SoftPhone** to **y**

```
add station 25002                                            Page   1 of   5
                                     STATION

Extension: 25002                         Lock Messages? n               BCC: 0
     Type: 9630                          Security Code: 123456           TN: 1
     Port: IP                          Coverage Path 1: 1               COR: 1
     Name: IP Station 1                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: 25001
            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? n
                              Short/Prefixed Registration Allowed: default
```

One Page 4, enter a building code in **Building** (one of the buildings added in **Section 5.2**) and under **BUTTON ASSIGNMENTS**, add **crss-alert** and **release,** as shown below:

```
add station 25002                                            Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                            Headset? n
       Jack:                                            Speaker? n
      Cable:                                           Mounting: d
      Floor:                                        Cord Length: 0
   Building: EFG                                      Set Color:

ABBREVIATED DIALING
     List1:                   List2:                    List3:




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

Add another station for an Incoming DID. For example if the incoming DID is 732-277-2872, use the last five digits as a station extension. This station is a virtual station that will be used by Amcom Enterprise alert to remotely perform call forwarding for callbacks from PSAP.

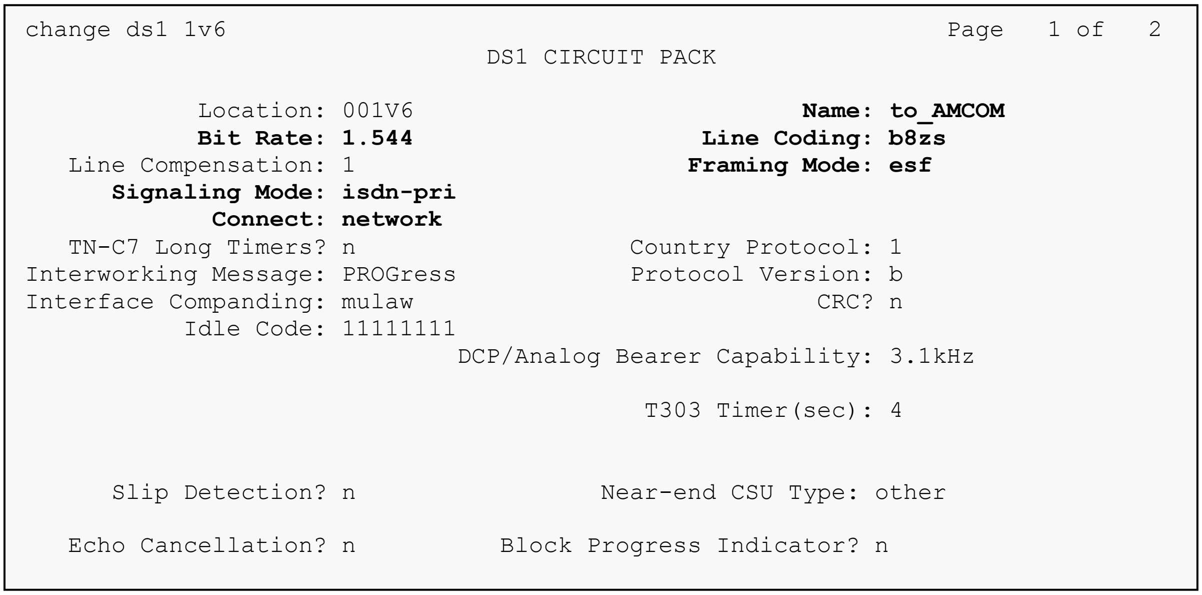
- In **Name** field, enter a descriptive name
- Set **Type** to **9630**
- Enter a **Security Code**

```
add station 72872                                            Page   1 of   5
                                     STATION

Extension: 72872                         Lock Messages? n             BCC: 0
     Type: 9630                          Security Code: 123456         TN: 1
     Port: IP                          Coverage Path 1:               COR: 1
     Name: DID Station 1               Coverage Path 2:               COS: 1
                                       Hunt-to Station:             Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 72872
            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? n

                                                          IP Video? n
                              Short/Prefixed Registration Allowed: default
```

## 5.4. Configure DS1

For an available T1 card on the Avaya gateway, use **change ds1 *n***, where ***n*** is the location of the T1 card. PRI trunk from this T1 card will be connected to Amcom Enterprise Alert on PBX port. Configure as follows:

- Type in a descriptive name in **Name** field
- Set **Bit Rate** to **1.544**
- Set **Line Coding** to **b8zs**
- Set **Framing Mode** to **esf**
- Set **Signaling Mode** to **isdn-pri**
- Set **Connect** to **network**



```
change ds1 1v6                                                  Page   1 of   2
                                DS1 CIRCUIT PACK

            Location: 001V6                           Name: to_AMCOM
            Bit Rate: 1.544                    Line Coding: b8zs
   Line Compensation: 1                       Framing Mode: esf
      Signaling Mode: isdn-pri
             Connect: network
   TN-C7 Long Timers? n                   Country Protocol: 1
Interworking Message: PROGress            Protocol Version: b
Interface Companding: mulaw                           CRC? n
           Idle Code: 11111111
                              DCP/Analog Bearer Capability: 3.1kHz

                                           T303 Timer(sec): 4


      Slip Detection? n                 Near-end CSU Type: other

   Echo Cancellation? n          Block Progress Indicator? n
```

## 5.5. Configure Signaling Group

User **add signaling-group *n***, where ***n*** is an available signaling group number, to add a signaling group. Configure as follows:

- Set **Group Type** to **isdn-pri**
- Set the **Primary D-Channel** according to the DS1 configured. Use channel number 24 as a D-Channel
- Set **TSC Supplementary Service Protocol** to **b**
- Once the trunk group has been configured return to this form and set the **Trunk Group for Channel Selection**

```
add signaling-group 2                                             Page   1 of   5
                                SIGNALING GROUP

 Group Number: 2               Group Type: isdn-pri
                    Associated Signaling? y         Max number of NCA TSC: 0
                       Primary D-Channel: 001V624     Max number of CA TSC: 0
                                                    Trunk Group for NCA TSC:
       Trunk Group for Channel Selection:          X-Mobility/Wireless Type: NONE
      TSC Supplementary Service Protocol: b           Network Call Transfer? n
```

## 5.6. Configure Trunk Group

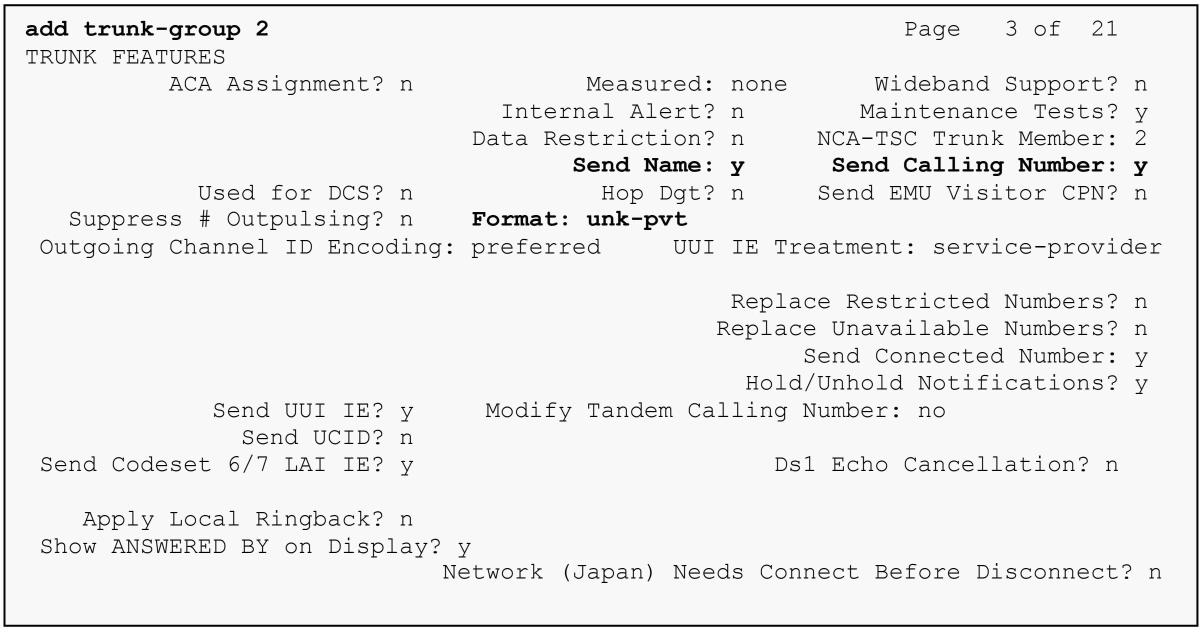
Use **add trunk-group *n***, where ***n*** is an available trunk group number, to add a trunk group. On Page 1, configure as follows:

- Set **Group Type** to **isdn**
- Provide a descriptive name in **Group Name**
- Set **TAC** according to the dial plan
- Set **Carrier Medium** to **PRI/BRI**
- Set **Service Type** to **tie**

```
add trunk-group 2                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 2                   Group Type: isdn          CDR Reports: r
  Group Name: to_AMCOM                   COR: 1        TN: 1        TAC: *002
   Direction: two-way       Outgoing Display? n         Carrier Medium: PRI/BRI
 Dial Access? y             Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n           TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
```

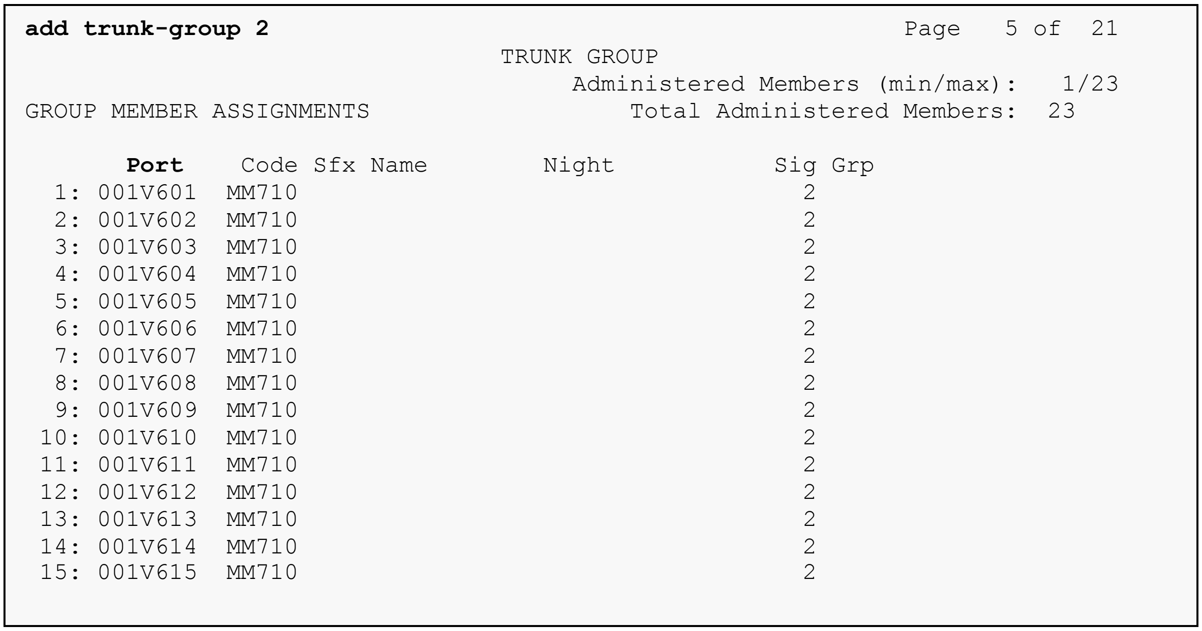
On Page 3, configure as follows:

- Set **Send Name** and **Send Calling Number** to **y**
- Set **Format** to **unk-pvt**



```
add trunk-group 2                                             Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none      Wideband Support? n
                                 Internal Alert? n       Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member: 2
                                      Send Name: y      Send Calling Number: y
            Used for DCS? n               Hop Dgt? n     Send EMU Visitor CPN? n
   Suppress # Outpulsing? n    Format: unk-pvt
 Outgoing Channel ID Encoding: preferred     UUI IE Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
                                                      Send Connected Number: y
                                                  Hold/Unhold Notifications? y
             Send UUI IE? y     Modify Tandem Calling Number: no
               Send UCID? n
 Send Codeset 6/7 LAI IE? y                         Ds1 Echo Cancellation? n

    Apply Local Ringback? n
 Show ANSWERED BY on Display? y
                             Network (Japan) Needs Connect Before Disconnect? n
```

On Page 5 and 6, add the **Port** 1-23 according to the location of the T1 board on Avaya Media Gateway.

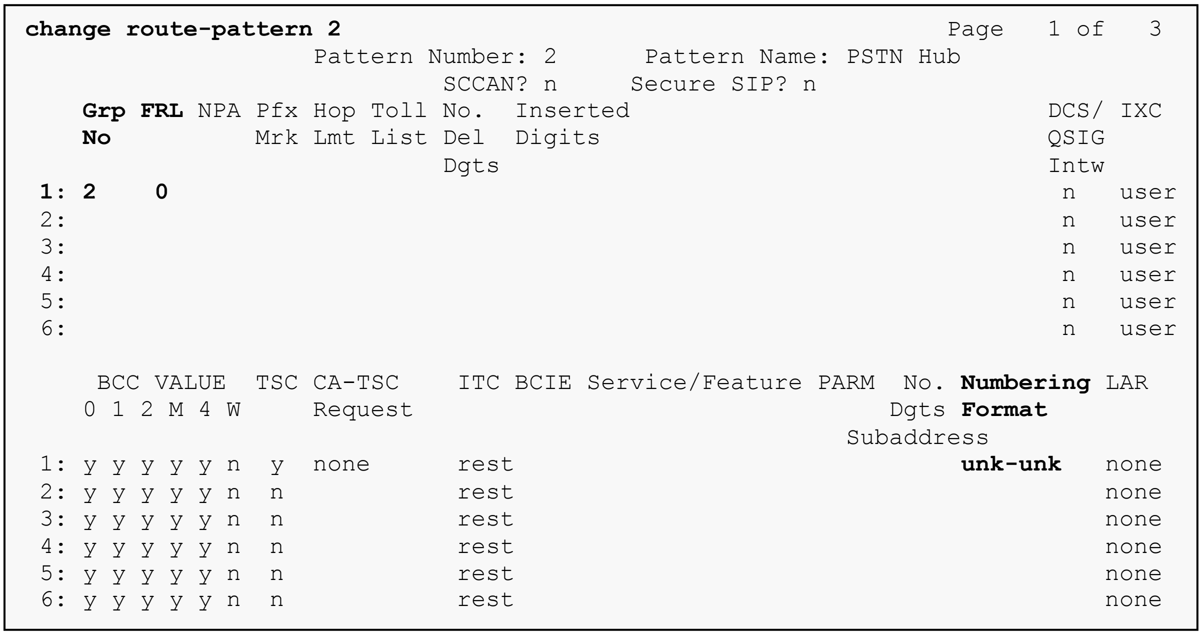


```
add trunk-group 2                                             Page   5 of  21
                                 TRUNK GROUP
                                      Administered Members (min/max):   1/23
GROUP MEMBER ASSIGNMENTS                  Total Administered Members:  23

       Port    Code Sfx Name        Night           Sig Grp
  1: 001V601  MM710                                   2
  2: 001V602  MM710                                   2
  3: 001V603  MM710                                   2
  4: 001V604  MM710                                   2
  5: 001V605  MM710                                   2
  6: 001V606  MM710                                   2
  7: 001V607  MM710                                   2
  8: 001V608  MM710                                   2
  9: 001V609  MM710                                   2
 10: 001V610  MM710                                   2
 11: 001V611  MM710                                   2
 12: 001V612  MM710                                   2
 13: 001V613  MM710                                   2
 14: 001V614  MM710                                   2
 15: 001V615  MM710                                   2
```

## 5.7. Configure Route Pattern

Configure route pattern to use the trunk group configured in previous section. Use **change route-pattern 2** command, and configure as follows:

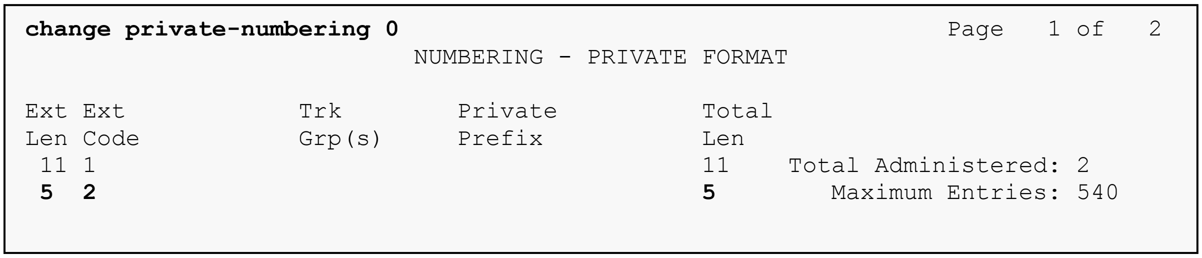
- Set **Grp No** for Line 1 to the trunk group configure in previous section
- Set **FRL** to **0**
- Set **Number Format** to **unk-unk** as configured in the screen capture below.



```
change route-pattern 2                                          Page   1 of   3
                    Pattern Number: 2      Pattern Name: PSTN Hub
                             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: 2    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  y  none      rest                               unk-unk   none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

## 5.8. Configure Private Numbering

Use **change private-number 0** command to configure the private numbering. This will ensure that the calling party number is sent to Amcom Enterprise Alerts when a call is placed from any of the Avaya Endpoints. For the test configuration, extensions starting with 2 and 5 digits long were used.



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

Ext Ext            Trk        Private          Total
Len Code           Grp(s)     Prefix           Len
 11 1                                          11    Total Administered: 2
 5  2                                          5        Maximum Entries: 540
```

## 5.9. Configure Crisis Alert

Use **change system-parameters crisis-alert** command and set **Every User Respond** to **y.**

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

ALERT STATION
    Every User Responds? y

ALERT PAGER
            Alert Pager? n
```

## 5.10. Configure ARS Routing

Use the **change ars analysis 911** command to configure 911 calls to route to Amcom Emergency Alerts and enable crisis alerts. The following configuration shows that when 911 is called, the call is routed to Amcom Emergency Alerts and a crisis alert is sent to all the phones that are configured with crss-alert buttons.

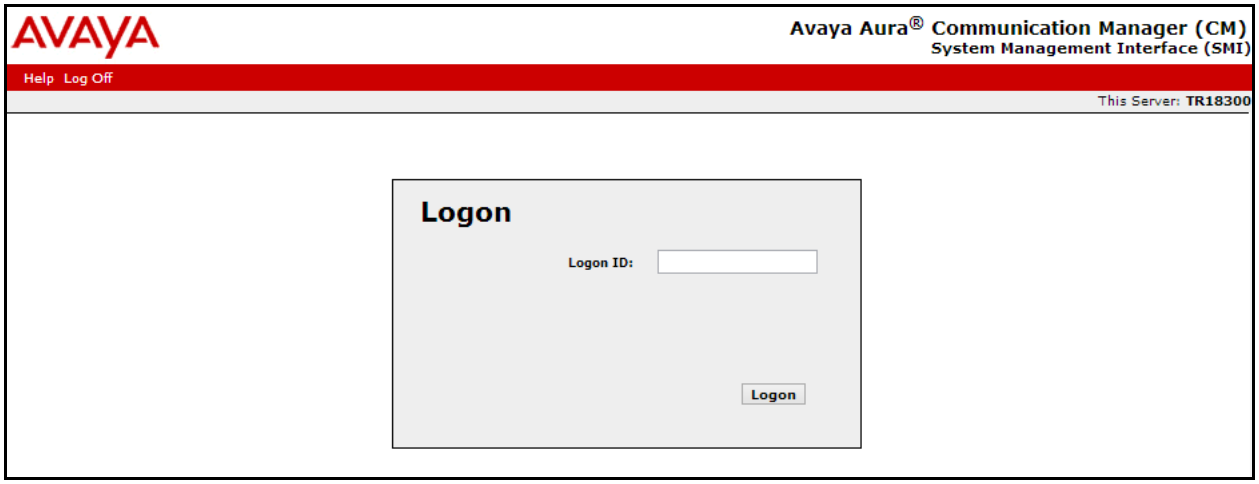
- Set **Dialed String** to **911**
- Set **Total Min** and **Max** to **3**
- Set **Route Pattern** to the pattern configured in **Section 5.6**
- Set **Call Type** to **alrt**

```
change ars analysis 911                                     Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    911                   3    3     2        alrt         n
```

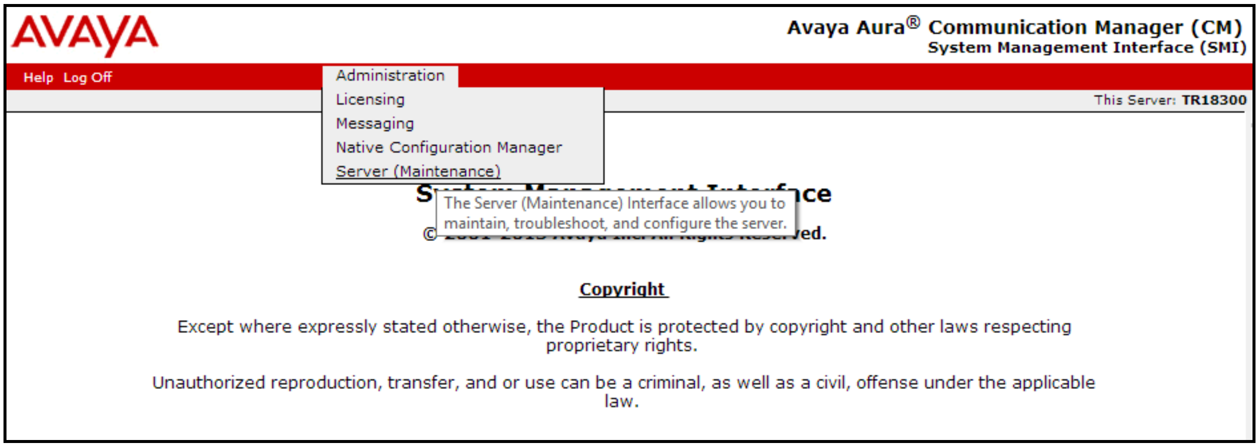
## 5.11. Add a User

Add a user for Amcom Enterprise Alert to provide access for Avaya Site Administration and SMS interface.

Navigate to https://<ip-address> where ip-address is the ip-address of Communication Manager and log in using appropriate credentials.


AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
This Server: TR18300
Logon
Logon ID:
Logon

Navigate to **Administration → Server Maintenance**.


AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
Administration
Licensing
Messaging
Native Configuration Manager
Server (Maintenance)
This Server: TR18300

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

System Management Interface

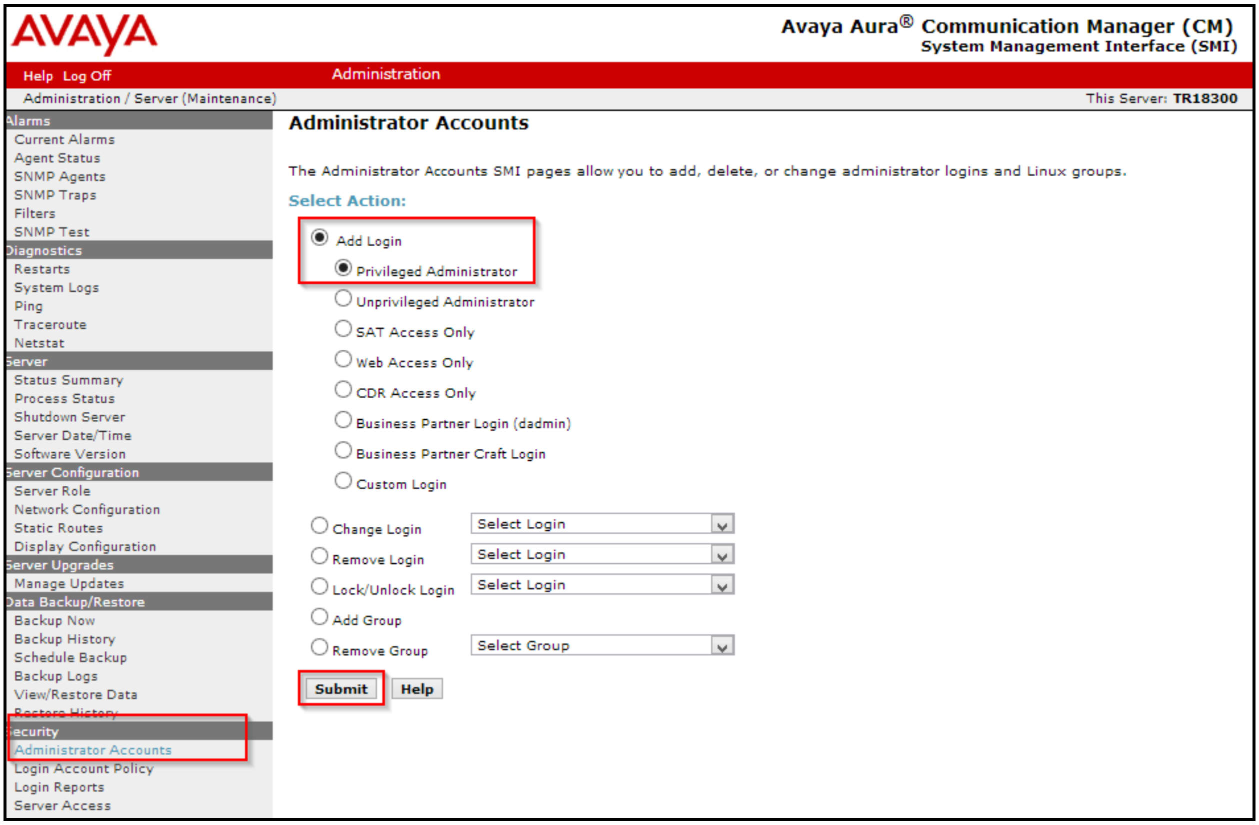
© 2001-2013 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

On the left pane, navigate to **Security → Administrator Accounts**, and select **Add Login → Privileged Administrator;** 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

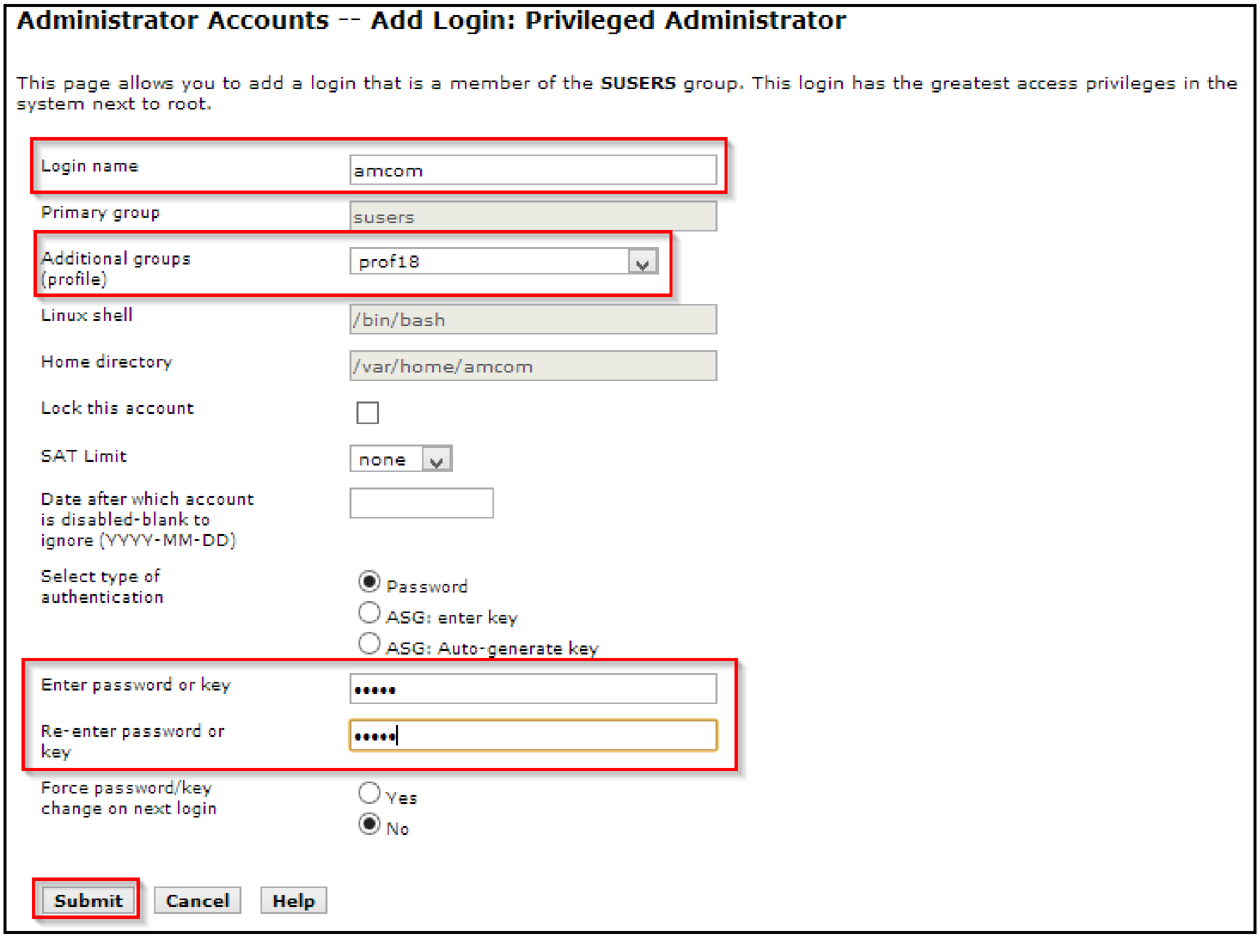
○ Remove Login — Select Login

○ Lock/Unlock Login — Select Login

○ Add Group

○ Remove Group — Select Group

- Type in a **Login Name.**
- Set **Additional Groups** to a profile configured in Communication Manager. Please note that this profile was pre-configured in Communication Manager and is not shown in this document. To add a profile in Communication Manager via SAT, use the **add user-profile** command.
- Type in a password in **Enter Password or key** and **Re-enter password or key**.
- Click **Submit** when done.



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

### 5.12. Configure AES connection

An existing standard configuration was used for AES connection and is directly not relevant for this document. Thus, it is not captured in this document.

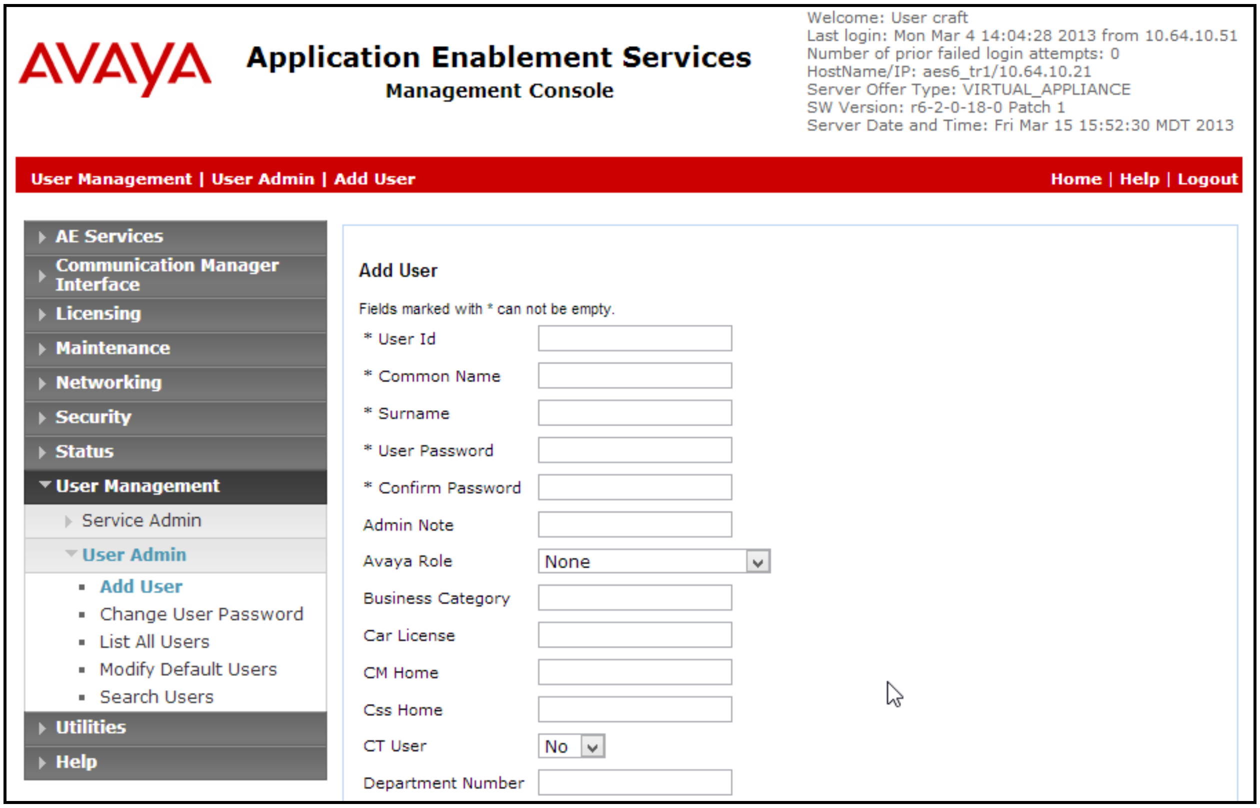
# 6. Configure Avaya Aura® Application Enablement Services

Configuration of Application Enablement Services requires a user account to be configured for Amcom Enterprise Alert.

## 6.1. Configure User

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

A user needs to be created for Amcom Enterprise Alert to communicate with AES. Navigate to **User Management → User Admin → Add User**.



Welcome: User craft
Last login: Mon Mar 4 14:04:28 2013 from 10.64.10.51
Number of prior failed login attempts: 0
HostName/IP: aes6_tr1/10.64.10.21
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-2-0-18-0 Patch 1
Server Date and Time: Fri Mar 15 15:52:30 MDT 2013

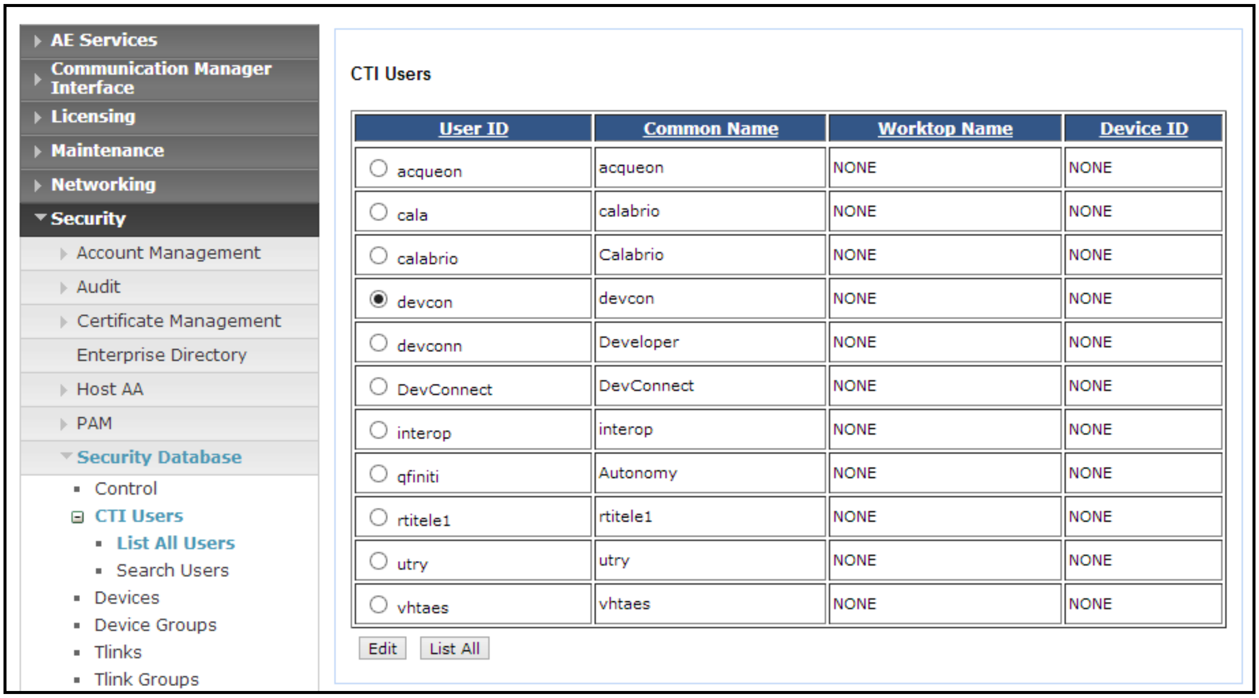
Add User

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**.

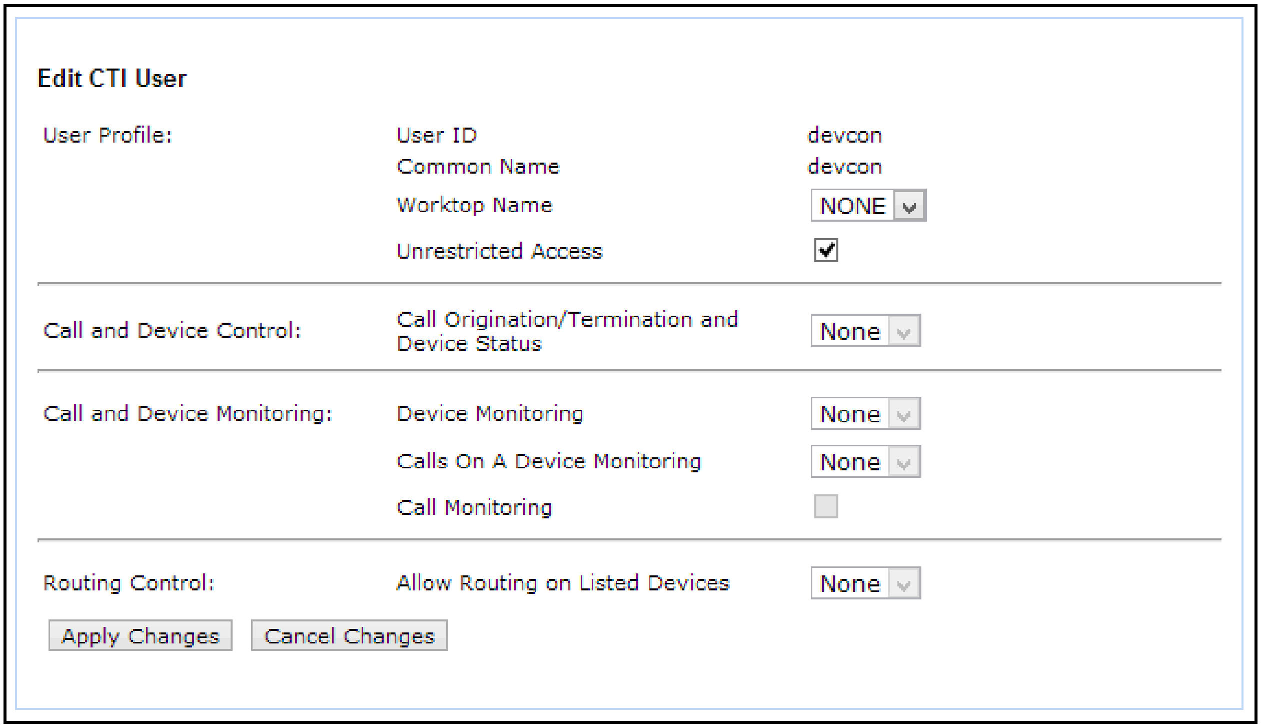
Navigate to **Security → Security Database → CTI Users → List All Users**.



CTI Users

| User ID | Common Name | Worktop Name | Device ID |
|---|---|---|---|
| ○ acqueon | acqueon | NONE | NONE |
| ○ cala | calabrio | NONE | NONE |
| ○ calabrio | Calabrio | NONE | NONE |
| ● devcon | devcon | NONE | NONE |
| ○ devconn | Developer | NONE | NONE |
| ○ DevConnect | DevConnect | NONE | NONE |
| ○ interop | interop | NONE | NONE |
| ○ qfiniti | Autonomy | NONE | NONE |
| ○ rtitele1 | rtitele1 | NONE | NONE |
| ○ utry | utry | NONE | NONE |
| ○ vhtaes | vhtaes | 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 | devcon |
| | Common Name | devcon |
| | 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 |

## 7. Configure 46xxSetting.txt

To configure the Push and Subscribe setting for Avaya 9600 Series IP Deskphones, configure the 46xxSetting.txt file with the following settings. Once configured, reboot the phones to take the change.

```
SET TPSLIST <ip-address>
SET SUBSCRIBELIST http://<ip-address>/avayapush/processingpage.aspx
SET PUSHCAP 22222
SET PUSHPORT 80
```

<ip-address> is the IP Address of Amcom Enterprise Alert.

# 8. Configure Amcom Enterprise Alert

Amcom installs, configures, and customizes the Enterprise Alert and ALI Alert applications for their end customers.

# 9. Verification

To verify the connectivity to Amcom Enterprise Alert, use status trunk <n> where n is the trunk number of the PRI trunk connected to Amcom Enterprise Alert. Verify **Service State** for all trunk members is **in-service/idle**.

```
status trunk 11

                             TRUNK GROUP STATUS

Member    Port     Service State      Mtce Connected Ports
                                      Busy

0011/001 001V701  in-service/idle    no
0011/002 001V702  in-service/idle    no
0011/003 001V703  in-service/idle    no
0011/004 001V704  in-service/idle    no
0011/005 001V705  in-service/idle    no
0011/006 001V706  in-service/idle    no
0011/007 001V707  in-service/idle    no
0011/008 001V708  in-service/idle    no
0011/009 001V709  in-service/idle    no
0011/010 001V710  in-service/idle    no
```

To verify Amcom ALI Alert, generate a test call that will initiate a crisis alert to a crisis alert configured station. Verify Amcom ALI Alert receives the crisis alert.

# 10. Conclusion

Amcom Enterprise Alert and ALI Alert were able to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

# 11. References

Documentation related to Avaya products may be obtained via http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager*, *Release 6.3.*

[2] *Administering Avaya Aura® Application Enablement Services, Release 6.3, Issue 2, October 2013.*

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.