Avaya Solution & Interoperability Test Lab

Trivoice TruUC with Avaya Aura® Telephony Infrastructure – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Telephony Infrastructure to interoperate with Trivoice TruUC. Interoperability is accomplished by passing Automatic Numbering Information (ANI) to the Called Party through Extension to Cellular (EC500). This results in Customer Relationship Management (CRM) data being retrieved via the TruUC application activated on the cellular device.

Information in these Application Notes has been obtained through interoperability compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Telephony Infrastructure to interoperate with Trivoice TruUC. Interoperability is accomplished by passing Automatic Numbering Information (ANI) to the Called Party through Extension to Cellular (EC500). This results in CRM data being retrieved via the TruUC application activated on the cellular device.

2. General Test Approach and Test Results

The general test approach was to verify interoperability of Trivoice TruUC with an Avaya Aura® Telephony Infrastructure. All test cases were executed manually.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included the following:

- Calls delivered via Avaya Aura® Telephony Infrastructure using EC500 to a cellular device running the Trivoice TruUC application
- Verification of correct ANI sent to called party
- Calling with Avaya H.323 and SIP telephones
- Retrieval of correct CRM data from Trivoice CRM database

All test cases were performed manually.

Compliance testing focused on proper call handling and verification of functionality between the two systems. Specifically, compliance testing verified that when the calls were placed, ANI was delivered to the Trivoice TruUC application, resulting in retrieval of the correct data from the Trivoice CRM database.

2.2. Test Results

Trivoice TruUC successfully achieved the above objectives. All test cases passed.

2.3. Support

For technical support on Trivoice products, contact Trivoice at 262-347-3970, or refer to http://www.trivoice.co

3. Reference Configuration

Figure 1 illustrates the setup used for compliance testing. The configuration enabled Avaya Aura® Session Manager, Avaya Aura® Communication Manager, to interoperate with Trivoice TruUC by passing ANI to the TruUC application via EC500. Upon receipt of the ANI TruUC triggered a Trivoice CRM database retrieval for specific data associated with the calling party.

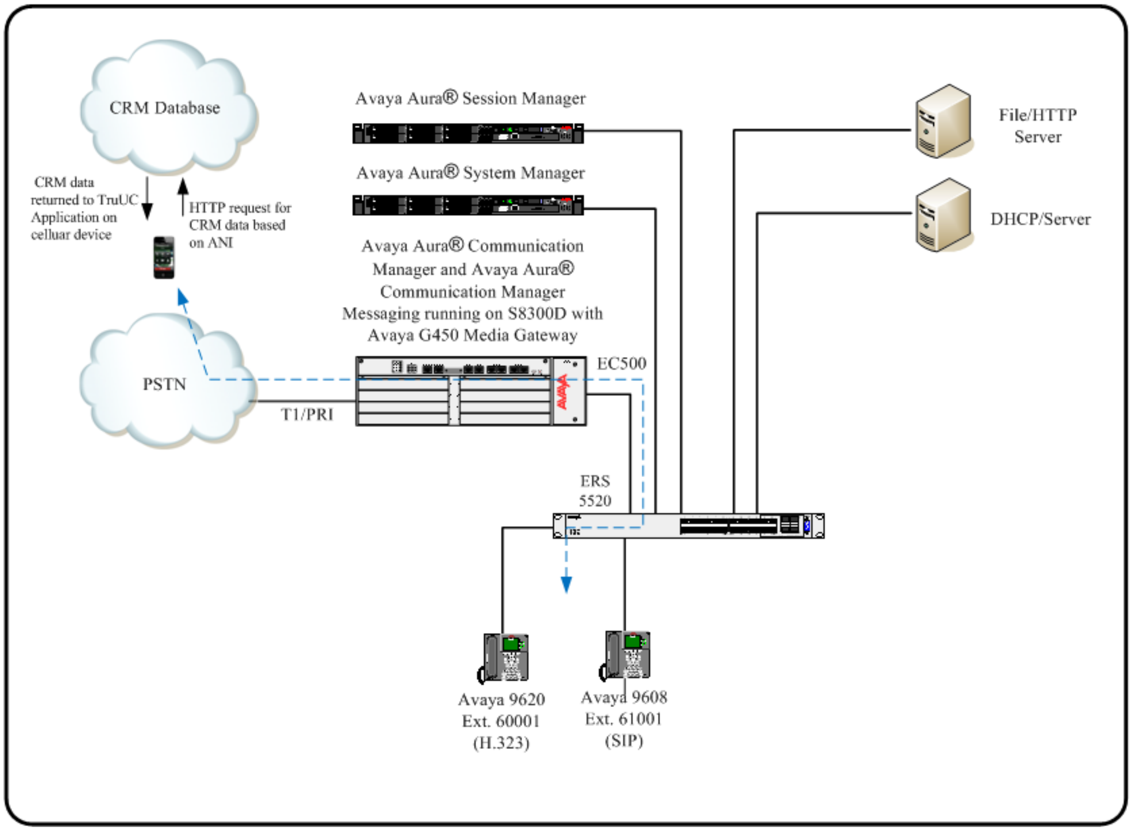


Figure 1: Trivoice TruUC

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya PBX Products	
Avaya S8300D Server running Avaya Aura® Communication Manager	Avaya Aura® Communication Manager 6.2 R016x.02.0.823.0
Avaya G450 Media Gateway MGP	HW 2 FW 31.20.0
Avaya Aura® Session Manager	
Avaya Aura® Session Manager HP Proliant DL360 G7	6.3.1.0.631004
Avaya Aura® System Manager HP Proliant DL360 G7	6.3.0 –ServicePack1
Avaya Endpoints	
Avaya 96xx Series IP Telephones	(H.323 3.1SP2), (SIP 2.6.6.0)
Avaya 96x1 Series IP Telephones	(H.323 6.2), (SIP 6.2)
TRI-VOICE Products	
TruUC	7.1
CRM	Vtiger 5.4
Web Server	Linux Red Hat, X86_64, Running Apache 2.2.23 / PHP 5.2.17 / MySQL 5.5.3
Motorola DROID RAZR	Android Version 4.0.4

5. Configure Avaya Aura® Communication Manager

This section describes the steps required for Communication Manager to support the configuration in **Figure 1**. The following pages provide step-by-step instructions on how to administer parameters specific to the Trivoice TruUC solution only. The assumption is that the appropriate license and authentication files have been installed on the servers and that login and password credentials are available and that the reader has a basic understanding of the administration of Communication Manager and Session Manager. It is assumed that all other connections, e.g., to PSTN, to LAN, are configured and will not be covered in this document. The reader will need access to the System Administration Terminal screen (SAT). For detailed information on the installation, maintenance, and configuration of Communication Manager, please refer to**[1]**.

5.1. Configure Node-Names IP

In the **Node-Names IP** form, assign the name and IP address of Session Manager. This is used to terminate the SIP Entity Link with Session Manager. The names will be used in the signaling group configuration configured later.
Enter the **change node-names ip** command. Specify node names and management IP address for Session Manager.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
cms                 10.64.10.85
default             0.0.0.0
iq1                 10.64.50.15
msgserver           10.64.50.52
procr               10.64.50.52
procr6              ::
sm5031              10.64.50.31















( 7  of 7    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
```

5.2. IP Codec Set and IP Network Region

Enter the **change ip-codec-set g** command, where **g** is a number between 1 and 7, inclusive, and enter **G.711MU** for **Audio Codec**. This IP codec set will be selected later in the IP Network Region form to define which codecs may be used within an IP network region.

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

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2:
 3:
 4:
 5:
 6:
 7:


     Media Encryption
 1: none
 2:
 3:
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **d4f27.com**. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media gateway. The **IP Network Region** form also specifies the **IP Codec Set** to be used for Desk Phone calls. This IP codec set is used when its corresponding network region (i.e., IP Network Region 1) is specified in the SIP signaling groups.

Enter the **change ip-network-region h** command, where **h** is a number between 1 and 250, inclusive. On page 1 of the **ip-network-region** form, set **Codec Set** to the number of the IP codec set configured in **Step 1**. Accept the default values for the other fields.

```
change ip-network-region 1                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: d4f27.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
```

5.3. Configure Signaling and Trunk Groups

Add a signaling group for calls that need to be routed to SIP Endpoints registered with Session Manager. Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form as shown below:

- Set the **Group Type** field to **sip**.
- Specify the Communication Manager (procr) and the Session Manager as the two end-points of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values were configured in the **IP Node Names** form shown in **Section 5.1**.
- Compliance testing used **tls** and port value of **5061** in the **Near-end Listen Port** and the **Far-end Listen Port** fields. If the **Far-end Network Region** field is configured, the codec for the call will be selected from the IP codec set assigned to that network region.
- Enter the domain name in the **Far-end Domain** field. In this configuration, the domain name is **d4f27.com**.
- The **DTMF over IP** field is set to the default value of **rtp-payload**. Avaya Communication Manager supports DTMF transmission using RFC 2833.
- The default values for the other fields may be used.

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

 Group Number: 2             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others



   Near-end Node Name: procr                  Far-end Node Name: sm5031
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: d4f27.com
                                          Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate               RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload          Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                  IP Audio Hairpinning? n
         Enable Layer 3 Test? y                 Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

Configure the **Trunk Group** form shown below for outgoing calls to be routed to Interactive Intelligence via Session Manager.

- Set the **Group Type** field to **sip**.
- Enter a meaningful name/description for **Group Name.**
- Enter a **Trunk Access Code (TAC)** that is valid under the provisioned dial plan
- Set the **Service Type** field to **tie**.
- Specify the **Signaling Group** associated with this trunk group.
- Specify the **Number of Members** supported by this SIP trunk group
- The default values for the other fields may be used.

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

Group Number: 20                   Group Type: sip          CDR Reports: y
  Group Name: To Session Manager          COR: 1        TN: 1        TAC: *002
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type:                       Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 10
```

5.4. Dial Plan and Access Codes

The dial plan defines what digit strings are defined as extensions and access codes. Feature access codes (fac) can be used to invoke specific PBX features.

Use the **display dialplan analysis** command to display the dial plan. This information will be used in subsequent steps and sections. Extensions beginning with 6 were used for the Avaya Endpoints.

```
display dialplan analysis                                      Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 2

    Dialed    Total  Call      Dialed    Total  Call      Dialed    Total  Call
    String    Length Type      String    Length Type      String    Length Type
   2            8    ext
   3            5    aar
   4            5    ext
   5            5    udp
   6            5    ext
   7            5    ext
   8            1    fac
   9            1    fac
   *            4    dac
```

Use the **change feature-access-codes** command to assign feature access codes for **AAR** and **ARS** (if not already assigned) that is consistent with the existing dial plan. .

```
change feature-access-codes                                    Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                   CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

5.5. Configure Route Pattern

A route pattern is configured to use the trunk defined in**5.3**. The route pattern can also be configured to perform digit manipulation on outgoing calls if necessary. Calls destined for SIP endpoints registered with Session Manager will be routed using the route pattern defined below.

When configuring a route pattern, use the **change route-pattern x** command, where **x** is an available route pattern number. For the compliance test, route pattern 3 was selected. Set the parameters as shown below.

- For the **Pattern Name**, enter a descriptive name.
- Set the **Grp No** to the trunk group number created in**5.3**.
- Set the **FRL** (Facility Restriction Level) to a value that allows all users access to the trunk that need to use it. The value of **0** is the least restrictive. This is the value used for the compliance test.
- Default values may be used for all other fields.

```
change route-pattern 3                                          Page   1 of   3
                    Pattern Number: 3   Pattern Name: To sm5031
                             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                    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
 6: y y y y y n  n            rest                                         none
```

5.6. Configure Automatic Alternate Routing

Automatic Alternate Routing (AAR) is used to route calls to SIP Endpoint Registered with Session Manager.

When creating entries in the AAR DIGIT ANALYSIS TABLE, use the **change aar analysis x** command, where **x** is the first digit in the dialed string to be entered. Create an entry to reach the mobile user extensions supported by the configuration in **Figure 1**. The extensions are reached using the aar table entry **6**. When creating the entries, enter the parameters as defined below.

- For the **Dialed String**, enter the extensions reachable via Session Manager.
- Set the **Total Min** and **Total Max** fields to the number length.
- Set the **Route Pattern** to the route pattern defined in 5.5that directs calls to the trunk connected to the Avaya Aura® Session Manager.
- Set the **Call Type** to **aar**.

```
change aar analysis 6                                            Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 2

          Dialed            Total     Route    Call   Node   ANI
          String          Min  Max  Pattern    Type   Num    Reqd
    61                    5    5      3        aar           n
    69997                 5    5      99       aar           n
    8                     7    7      254      aar           n
    9                     12   12     1        aar           n
```

5.7. Configure EC500

5.7.1. Configure Stations and Off-PBX Station Mapping For Mobile Devices

Each mobile device will be associated with a station extension configured on Communication Manager. The station extension may represent a physical desk phone or an extension with no phone logged in to it. In the case of the compliance test extensions 60002 and 61006 were configured on Communication Manager.

To associate a mobile device to each of these station extensions requires an off-pbx station mapping as shown below.

In general, a mobile device will be associated with an existing desk phone for which the Communication Manager Station extension will already be configured. However, in the case of mobile devices that are not associated with a physical phone then a station must be added.

Use the **add station 60002** command to create the station for this user. Enter a value for phone **Type:** and enter a description in the **Name:** field.

```
add station 60002                                               Page   1 of   5
                                     STATION

Extension: 60002                           Lock Messages? n             BCC: 0
     Type: 9608                            Security Code: 123456         TN: 1
     Port: IP                            Coverage Path 1:               COR: 1
     Name: User1                         Coverage Path 2:               COS: 1
                                         Hunt-to Station:
STATION OPTIONS
                Location:                      Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 44444
            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

                                              Customizable Labels? y
```

On **Page 4** under BUTTON ASSIGNMENTS, add an **ec500** button. This step needs to be completed for all extensions associated with mobile users, both existing extensions and new ones.

```
add station 60002                                               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: ec500      Timer? n                8:

    voice-mail
```

To create the mapping between a desktop extension and a mobile device, use the **add off-pbx-telephone station-mapping x** command, where **x** is the desktop extension to be mapped. Multiple station extensions can be added at the same time. Enter the parameters as described below.

- Enter the desktop extension for the **Station Extension**.
- Enter **EC500** for the **Application**.
- Enter the mobile extension for the **Phone Number.**
- Enter **aar** for **Trunk Selection**. This instructs Communication Manager to use the AAR tables to determine how to route this call.
- Enter an off-pbx-telephone configuration set to use with this call. The default values for configuration set 1 were used for compliance testing.

```
add off-pbx-telephone station-mapping                        Page   1 of   3
                    STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station         Application Dial   CC  Phone Number    Trunk        Config  Dual
 Extension                   Prefix                     Selection    Set     Mode
 60002             EC500        -     17205551212        ars         1
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- SIP Entities corresponding to Session Manager, and Communication Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager

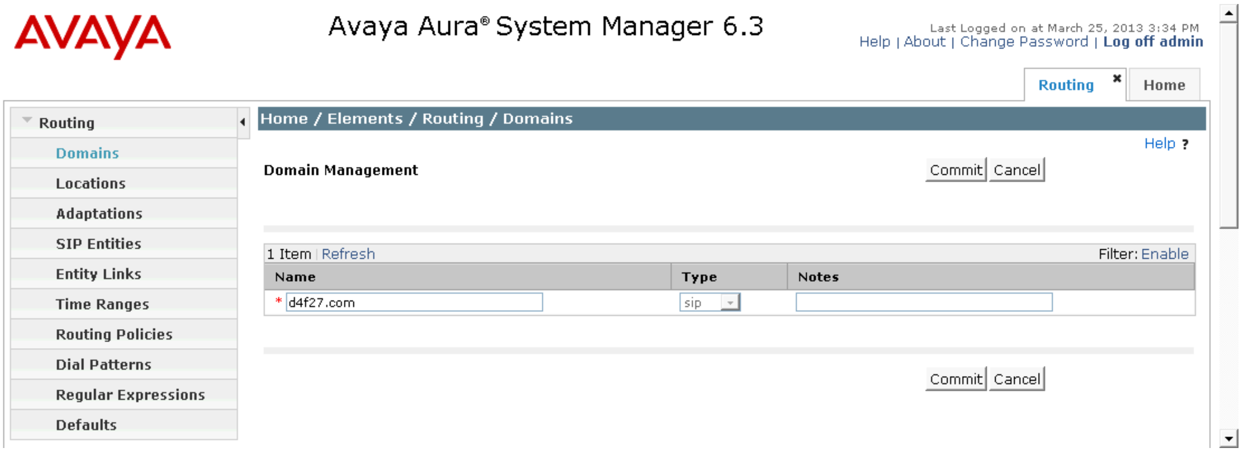
Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL "https://<*ip-address*>/SMGR", where <*ip-address*> is the IP address of System Manager. Log in with the appropriate credentials.

6.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **Domains** on the left and clicking the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

- **Name:** The authoritative domain name (e.g., d4f27.com).
- **Type:** Select SIP
- **Notes:** Descriptive text (optional).

Click **Commit**.



6.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

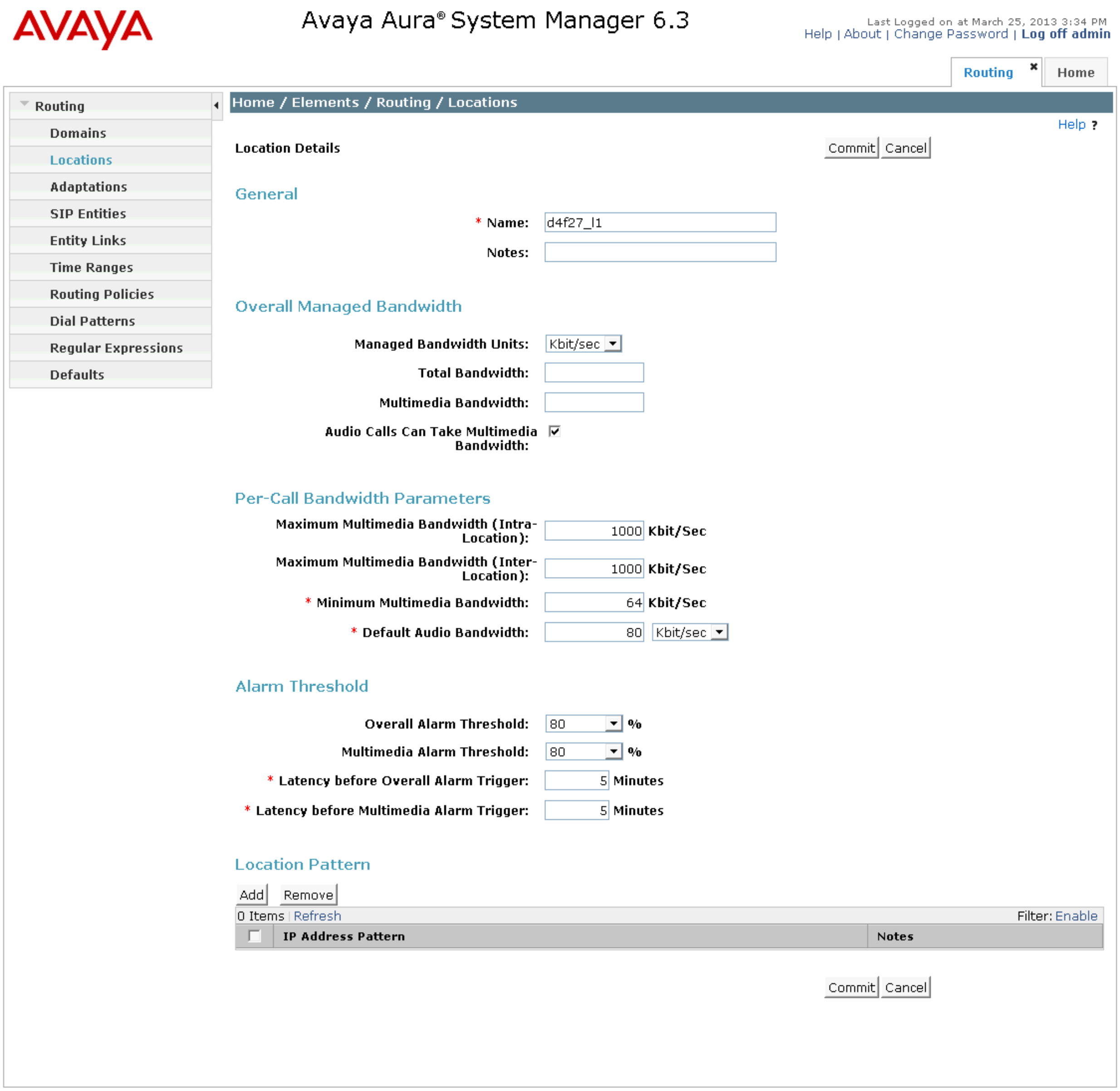
Under General:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

Under Location Pattern:

- **IP Address Pattern:** A pattern used to logically identify the location.
- **Notes:** Descriptive text (optional).

The screen below shows the addition of the *Public* location, where Communication Manager and Session Manager reside. Click **Commit** to save the Location definition.


AVAYA
Avaya Aura® System Manager 6.3
Last Logged on at March 25, 2013 3:34 PM
Help | About | Change Password | Log off admin
Routing
Home
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Home / Elements / Routing / Locations
Help ?
Location Details
Commit
Cancel
General
* Name:
d4f27_l1
Notes:
Overall Managed Bandwidth
Managed Bandwidth Units:
Kbit/sec
Total Bandwidth:
Multimedia Bandwidth:
Audio Calls Can Take Multimedia Bandwidth:
Per-Call Bandwidth Parameters
Maximum Multimedia Bandwidth (Intra-Location):
1000
Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location):
1000
Kbit/Sec
* Minimum Multimedia Bandwidth:
64
Kbit/Sec
* Default Audio Bandwidth:
80
Kbit/sec
Alarm Threshold
Overall Alarm Threshold:
80
%
Multimedia Alarm Threshold:
80
%
* Latency before Overall Alarm Trigger:
5
Minutes
* Latency before Multimedia Alarm Trigger:
5
Minutes
Location Pattern
Add
Remove
0 Items | Refresh
Filter: Enable
IP Address Pattern
Notes
Commit
Cancel

6.3. Add SIP Entities

In the sample configuration, a SIP Entity is added for Session Manager, and Communication Manager.

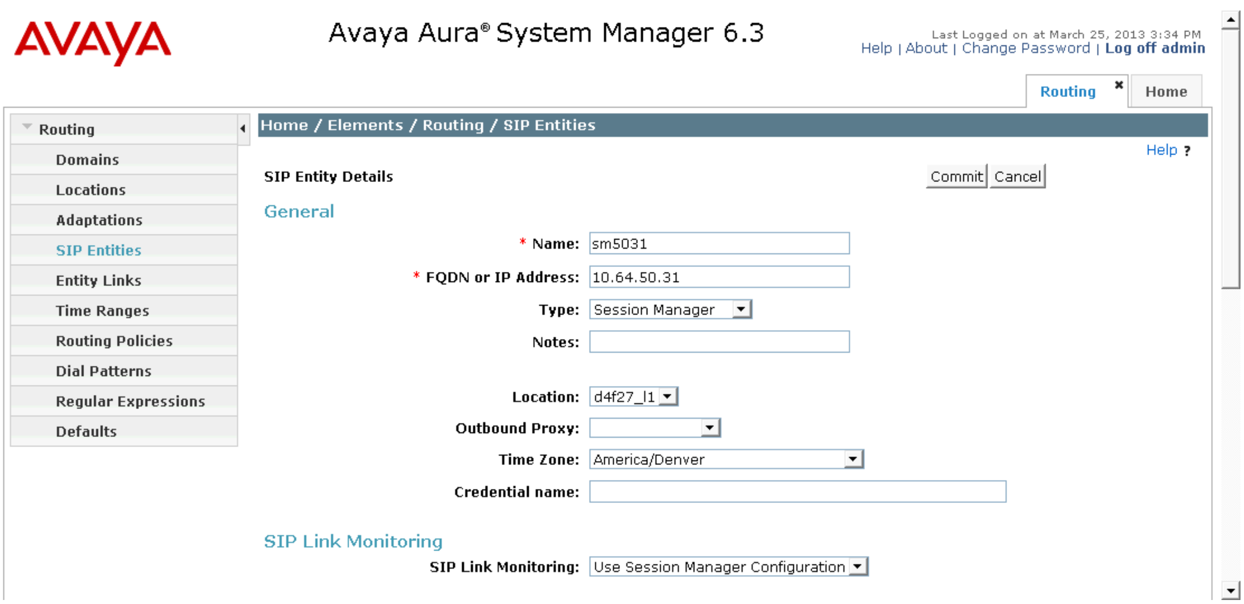
6.3.1. Avaya Aura® Session Manager

A SIP Entity must be added for Session Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under General:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface on Session Manager.
- **Type:** Select Session Manager.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save each SIP Entity definition.



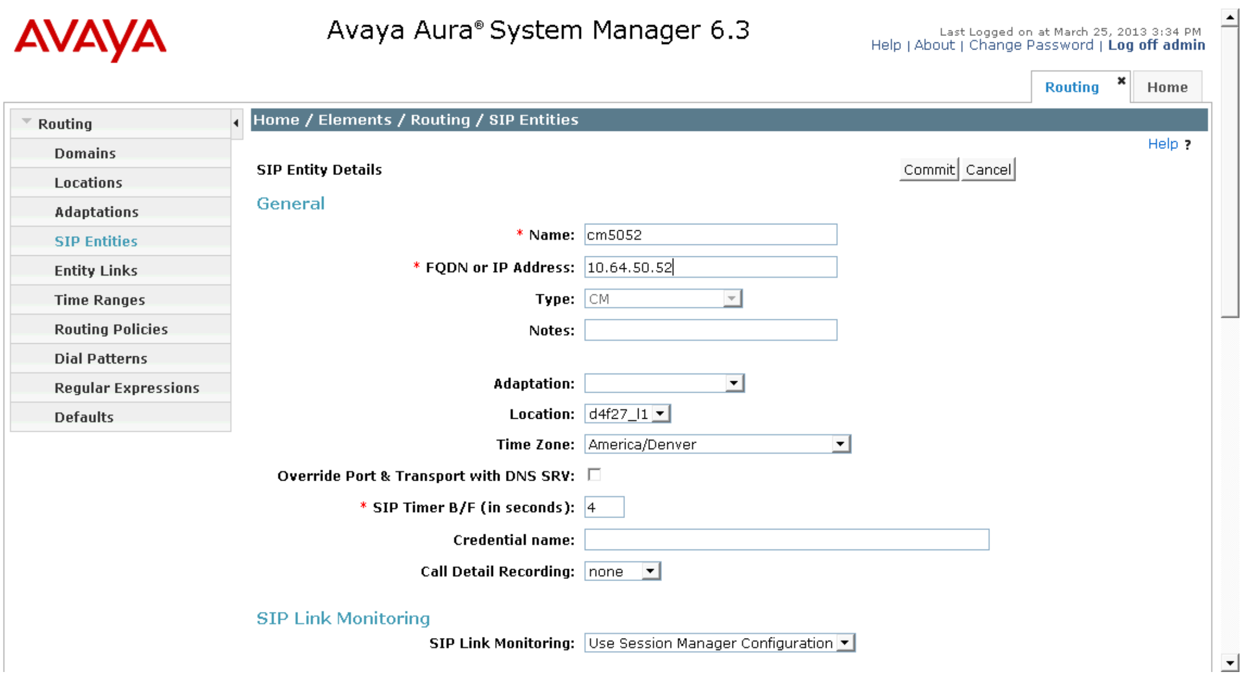
6.3.2. Avaya Aura® Communication Manager

A SIP Entity must be added for Communication Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under General:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., S8300D blade) in the G450 telephony system.
- **Type:** Select CM.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save each SIP Entity definition.



6.4. Add Entity Links

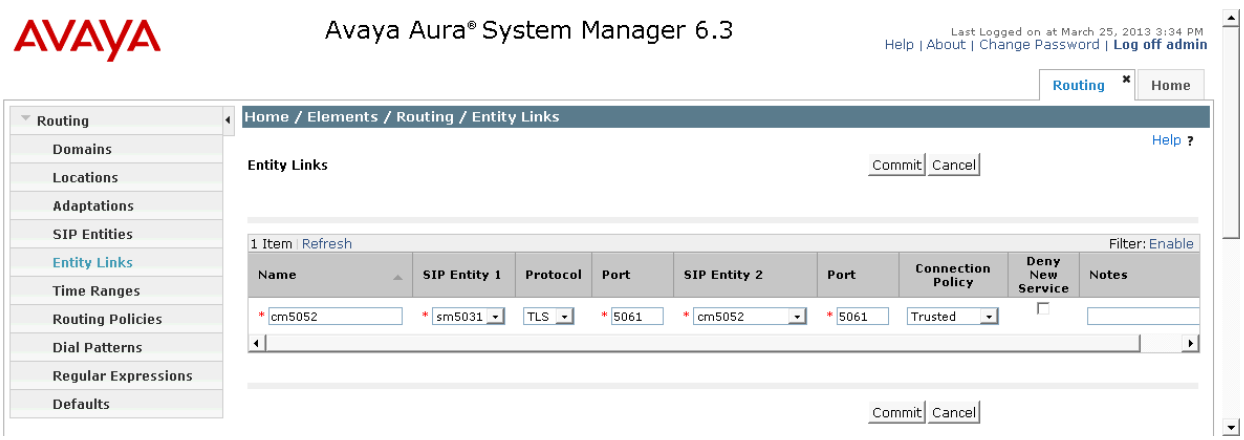
The SIP trunk from Session Manager to Communication Manager are described by Entity Links. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select *TLS* as the transport protocol.
- **Port:** Port number to which the other system sends SIP Requests (e.g., *5061* for TLS).
- **SIP Entity 2:** Select the Session Manager.
- **Port:** Port number to which the other system sends SIP Requests (e.g., *5061* for TLS).
- **Connection Policy:** Select *Trusted*.

Repeat configuration for Communication Manage.

The following screens display the configuration of the entity link is for the connection between Session Manager and Communication Manager.

Session Manager ←→ Communication Manager



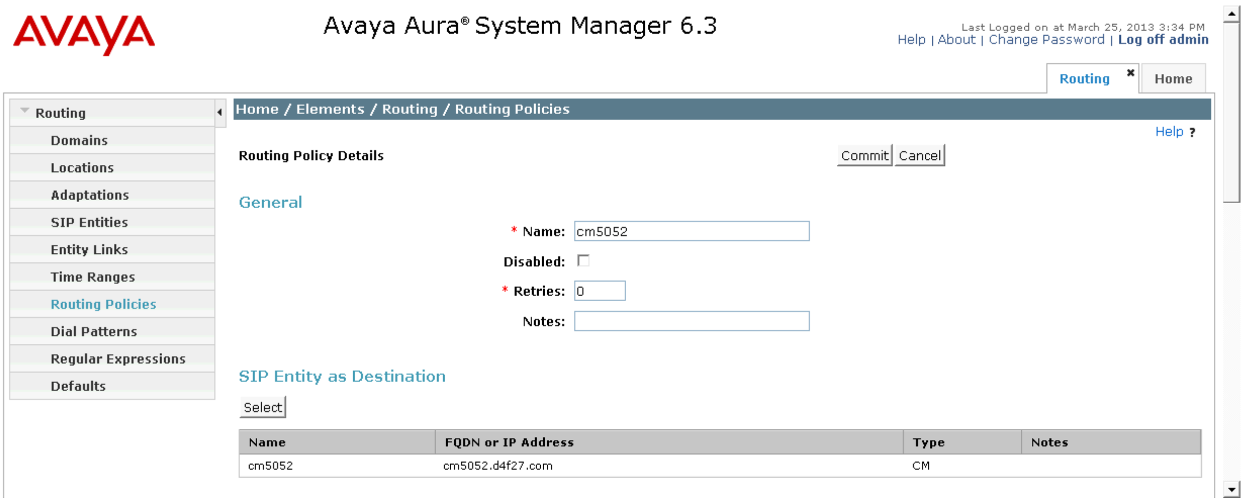
6.5. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.3**. One routing policy was added for Communication Manager. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:
Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:
Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screen shows the Routing Policy for Communication Manager.



6.6. Add Dial Patterns

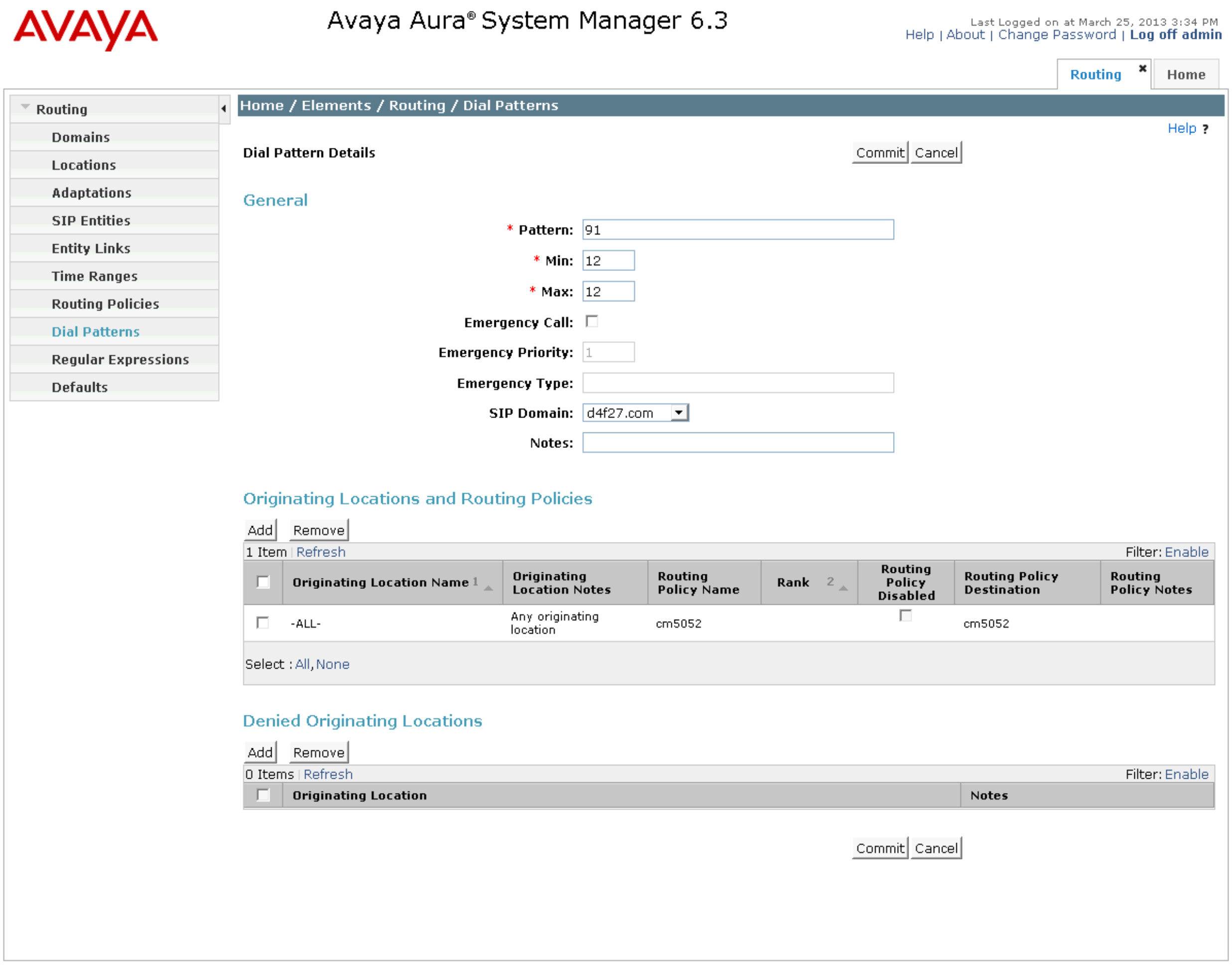
Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration, 12-digit numbers beginning with “91” will be routed to Communication Manager. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **Notes** Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:
Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screen shows the dial pattern definitions for local extensions on Communication Manager.



7. Configuring Trivoice TruUC

Installation and configuration of Trivoice TruUC for compliance testing was performed by Trivoice Professional Services. The Reference implementation and TruUC were tested on Red Hat version 5.3. Customer installation and configuration will also be done by Trivoice, therefore, not included in these Application Notes. Please contact Trivoice for support. 2.3

7.1. TruUC Installation on the Mobile Device

Trivoice will provide the user with a URL for downloading the TruUC Application to be installed on the mobile device. Once TruUC is installed, and the application has been enabled, by tapping the Trivoice icon. Caller-id included in an incoming call will be inserted in to a pre-programmed URL that is used to retrieve CRM data associated with the calling party number.

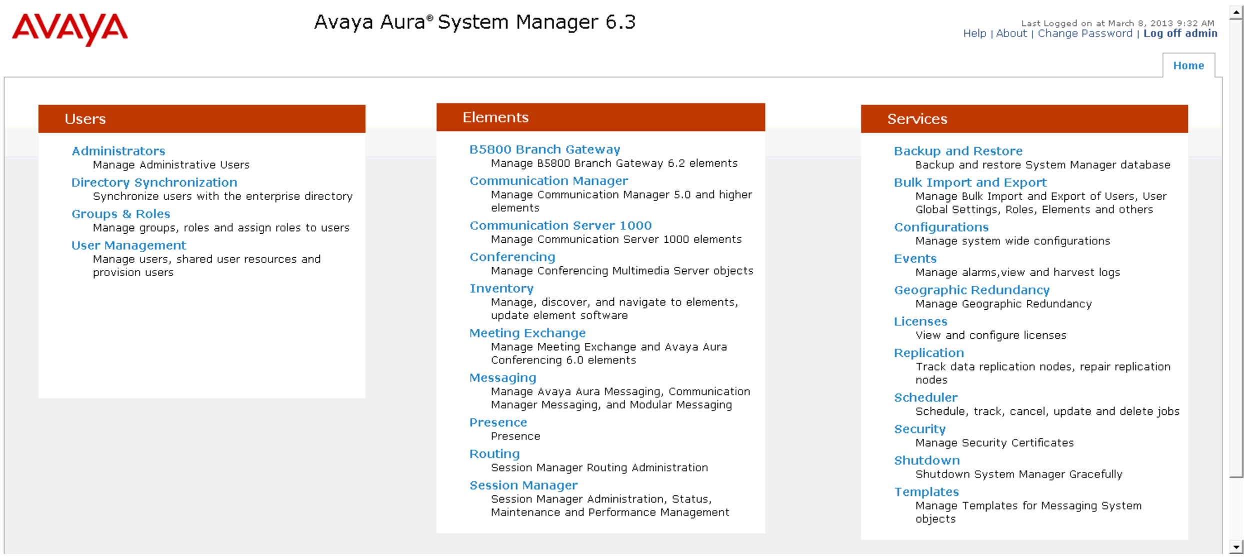
8. Verification Steps

The following steps may be used to verify the configuration:

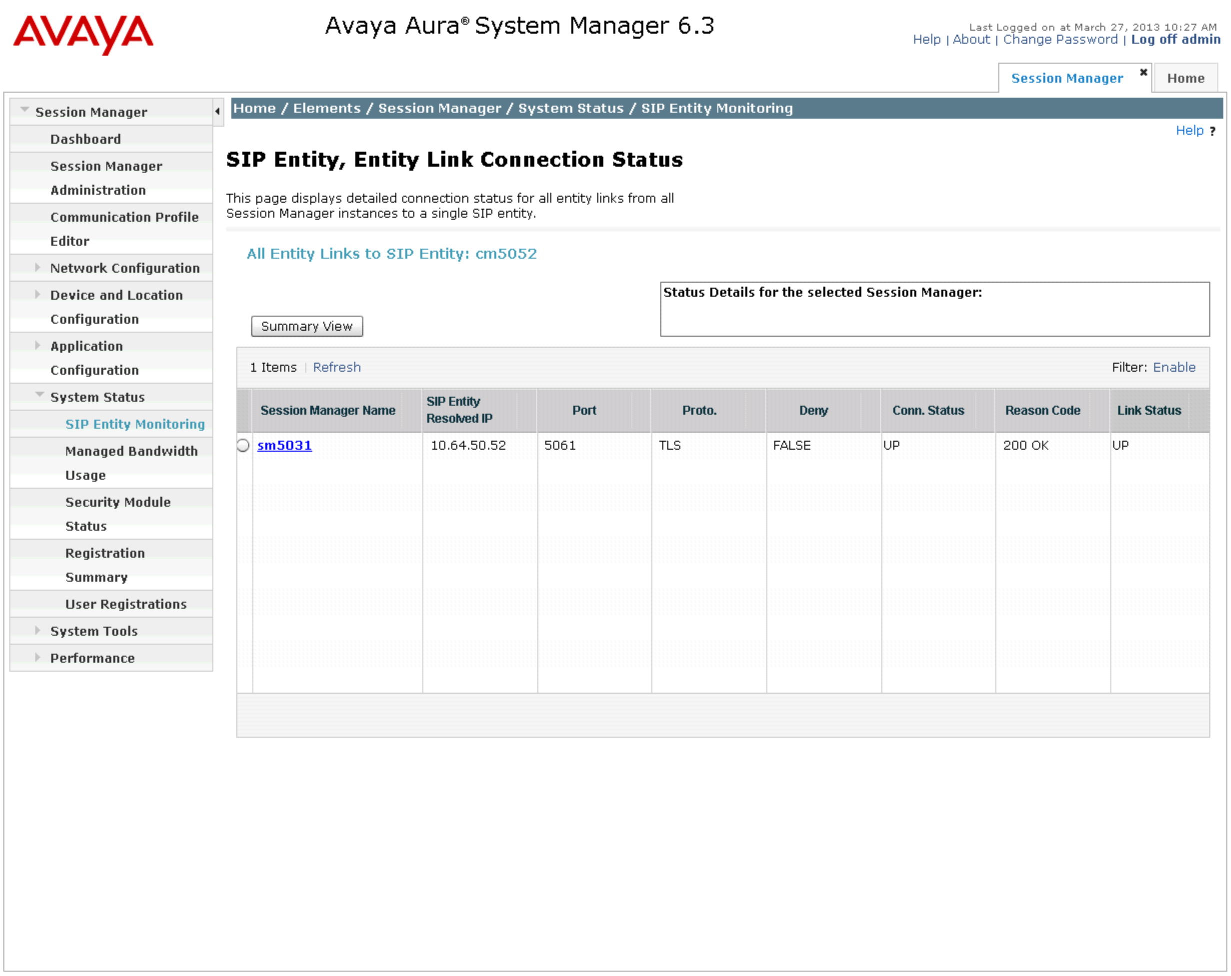
8.1. Verify SIP Entity Link Avaya Aura® Session Manager

Verification can be accomplished by accessing the browser-based GUI of System Manager using the URL "https://<*ip-address*>/SMGR", where <*ip-address*> is the IP address of System Manager. Log in with the appropriate credentials.

From the *Home* tab select → *Session Manager* → *System Status* → *SIP Entity Monitoring*

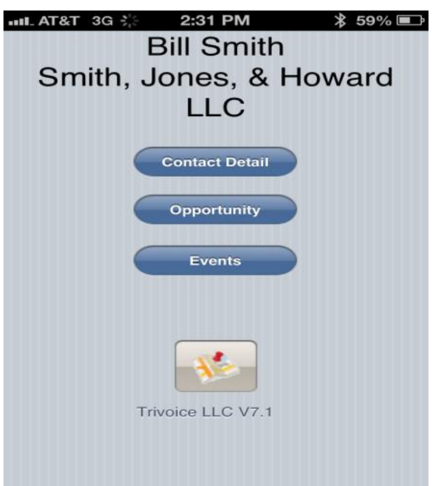


From the *SIP Entity Link Monitoring Status Summary* page (not shown) left-click on the desired Session Manager then left-click on the desired *SIP Entity Name* to display the screen below. Verify that the *Conn. Status* and *Link Status* are both UP



8.2. Verify Trivoice TruUC

Verification can be accomplished by launching the application and receiving the data on an incoming call based on the web services written for this installation.



9. Conclusion

These Application Notes have described the administration steps required to configure Trivoice TruUC to interoperate within an Avaya Aura® Telephony Infrastructure. The solution verified proper EC500 call handling by Avaya Aura® Communication Manager, and CRM data retrieval by Trivoice TruUC as depicted in **Figure 1.**

10. Additional References

The documents referenced below were used for additional support and configuration information.

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

[1] *Administering Avaya Aura® Communication Manager*, Doc # 03-300509
[2] *Administering Avaya Aura® Session Manager*, Doc # 03-603324

Product documentation for Trivoice TruUC products may be found at http://www.trivoice.co

[3] TruUC Installation and Configuration

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.