# AVAYA

**Avaya Solution & Interoperability Test Lab**

# Application Notes for configuring Enghouse Interactive Communications Portal 9.0 using CTI Media Gateway with Avaya Aura® Session Manager R6.3 and Avaya Aura® Communication Manager R7.0 - Issue 1.0

## Abstract

These Application Notes describe the configuration steps for Enghouse Interactive Communications Portal 9.0 using CTI Media Gateway to successfully interoperate with Avaya Aura® Session Manager R6.3 and Avaya Aura® Communication Manager R7.0. Communications Portal is an IVR application that connects to Session Manager as a SIP Entity.

Readers should pay attention to section 2, in particular the scope of testing as outlined in Section 2.1 as well as the observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

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

SJW; Reviewed:
SPOC 10/6/2015

Solution & Interoperability Test Lab Application Notes
©2015 Avaya Inc. All Rights Reserved.

1 of 41
EHCP9MG_CM70

# 1. Introduction

These Application Notes describe the configuration steps for Enghouse Interactive Communications Portal 9.0 to successfully interoperate with Avaya Aura® Session Manager R6.3 and Avaya Aura® Communication Manager R7.0.

Enghouse Interactive Communications Portal (formerly Syntellect Communications Portal) is an open, standards-based platform with integrated application development and management components.
- Voice self-service solutions, such as interactive voice response (IVR), interactive voice and video response (IVVR), outbound dialing, and speech-enabled self-service systems.
- SMS, email, standards-based voice mail.
- Contact center solutions, including outbound dialing, intelligent routing applications and screen pop applications.
- Unified communications solutions, including standards-based voice-mail systems and applications that combine traditional voice, IP telephony, video messaging, SMS, email, and fax communication.

# 2. General Test Approach and Test Results

The IVR application telephony functionality of Communications Portal 9.0 (CP) was the only module tested. This IVR application (CP script) connects to Session Manager as a SIP Trunk entity and can be integrated with Communication Manager by passing SIP calls to and from the PBX. Session Manager directs the call over SIP trunks to CP scripts which in turn handles the call depending on the digits dialed using SIP signaling. Communications Portal utilizes CTI Media Gateway driver to perform all telephony functions on the server. This CTI Media Gateway facilitates the Communications Portal connectivity to Session Manager.

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 test included both feature functionality and serviceability testing. The feature functionality testing focused on placing various calls to the Communications Portal IVR:

- **Basic Inbound/Outbound** – Tests inbound calls to Enghouse Interactive Communications Portal.
- **Call Hold** – Tests held calls to/from Enghouse Interactive Communications Portal.
- **Call Transfer** – Tests transferred calls to/from Enghouse Interactive Communications Portal.
- **IVR Functionality** – Tests of various IVR features like is ANI/DNIS detection, leaving voice message/voice mail (Recording), DTMF collection, Barge-in and Trombone Referral on the Enghouse Interactive Communications Portal.
- **Failover/Service** – Tests the behaviour of Enghouse Interactive Communications Portal when there are certain failed conditions.

The serviceability testing focused on verifying the ability of Communications Portal to recover from disconnection and reconnection to the Avaya solution.

## 2.2. Test Results

All functionality and serviceability test cases were completed successfully, however the following was observed only when shuffling was on (**Direct IP to IP Audio Connections** set to **Y**).

- From a H.323 or SIP IP desk phone on Communication Manager calling to the Communications Portal IVR system playing an announcement via SIP trunk (Session Manager), then pressing Hold/Resume in quick succession leads to the loss of RTP. This is due to the reINVITE being sent by Communication Manager before the ACK is received by Communications Portal and a "491 request pending" is received. This may be causing this issue, simply due to a delay and the reINVITE/ACK sequence going out of sync. Note that is not an issue if Hold/Resume is used in a "normal" fashion or when shuffling is off (**Direct IP to IP Audio Connections** set to **N**).

## 2.3. Support

Technical support can be obtained for Enghouse Interactive as follows:

USA
- Email:        scpsupport@enghouse.com
- Website:      http://enghouseinteractive.com/support.php
- Phone:        +1 800.788.9730 Self-Service
- Phone:        +1 800.872.2272 Live-Service

EMEA
- Email:        supportenvox@syntellect.com
- Website:      http://enghouseinteractive.co.uk/support/contact_support/
- Phone:        +44 203 357 3001

# 3. Reference Configuration

The configuration in **Figure 1** will be used to compliance test Enghouse Interactive Communications Portal 9.0 with Session Manager and Communication Manager using SIP signalling over SIP trunks to route calls from Communication Manager to Communications Portal 9.0.
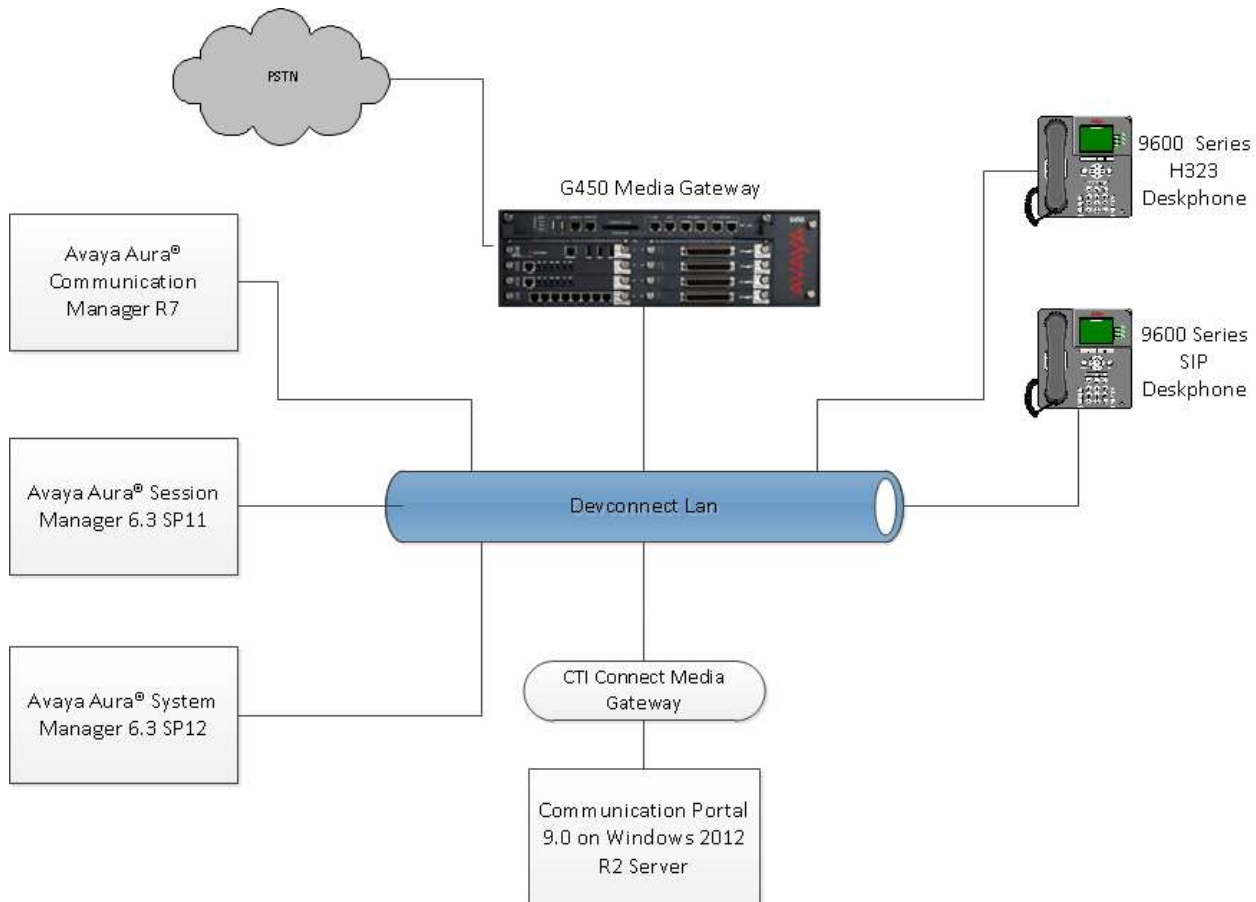


**Figure 1: Connection of Enghouse Interactive Communications Portal 9.0 with Avaya Aura® Session Manager R6.3 and Avaya Aura® Communication Manager R7.0**

SJW; Reviewed:
SPOC 10/6/2015
Solution & Interoperability Test Lab Application Notes
©2015 Avaya Inc. All Rights Reserved.
5 of 41
EHCP9MG_CM70

# 4. Equipment and Software Validated

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

| Equipment/Software | Release/Version |
|---|---|
| Avaya Aura® System Manager running on a Virtual Platform | R6.3 SP12<br>Build 6.3.0.8.5682-6.3.8.4903<br>Software Update Revision 6.3.12.9.3022 |
| Avaya Aura® Session Manager running on a Virtual Platform | R6.3 SP11<br>6.3.11.0.631103 |
| Avaya Aura® Communication Manager running on a Virtual Platform | R7.0 SP6<br>R017x.00.0.411<br>Update: 7.0.0.1.0-SP1 |
| Avaya G430 Gateway | 36.14.0 /1 |
| Avaya 9630 H323 Deskphone | H.323 Release 3.2 |
| Enghouse Interactive Communications Portal running on Windows 2012 Server<br>CTI Connect Media Gateway | Communications Portal 9.0 PRC5<br>CTI Connect Media Gateway 8.2 |

# 5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration operations described in this section can be summarized as follows:
- Verify System Parameters Customer Options.
- System Features and Access Codes.
- Administer Dial Plan.
- Administer Route Selection for Communications Portal calls.
- Configure SIP Trunk.

**Note:** The configuration of PSTN trunks and routes are outside the scope of these Application Notes.

## 5.1. Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that **Maximum Administered SIP Trunks** has sufficient capacity. Each call that receives IVR treatment from Communications Portal uses a minimum of one SIP trunk. Calls that are routed back to stations commissioned on Communication Manager, or calls that are routed back to Communication Manager to access the PSTN, use 2 SIP trunks.

```
display system-parameters customer-options                      Page   2 of  11
                              OPTIONAL FEATURES

IP PORT CAPACITIES                                             USED
                  Maximum Administered H.323 Trunks: 12000 250
          Maximum Concurrently Registered IP Stations: 18000 2
            Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                    Maximum Video Capable Stations: 18000 0
              Maximum Video Capable IP Softphones: 18000 0
                    Maximum Administered SIP Trunks: 24000 319
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
```

On **Page 3**, ensure that both **ARS** and **ARS/AAR Partitioning** are 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
```

On **Page 5**, ensure that **Uniform Dialing Plan** is set to **y**.

```
display system-parameters customer-options                        Page   5 of  11
                              OPTIONAL FEATURES

                 Multinational Locations? n          Station and Trunk MSP? y
  Multiple Level Precedence & Preemption? n      Station as Virtual Extension? y
                      Multiple Locations? n
                                              System Management Data Transfer? n
            Personal Station Access (PSA)? y              Tenant Partitioning? y
                       PNC Duplication? n      Terminal Trans. Init. (TTI)? y
                   Port Network Support? y               Time of Day Routing? y
                       Posted Messages? y      TN2501 VAL Maximum Capacity? y
                                                      Uniform Dialing Plan? y
                     Private Networking? y      Usage Allocation Enhancements? y
```

## 5.2. System Features and Access Codes

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 10** for supporting documentation.

```
display system-parameters features                           Page   1 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
                             Self Station Display Enabled? n
                                Trunk-to-Trunk Transfer: all
                  Automatic Callback with Called Party Queuing? n
     Automatic Callback - No Answer Timeout Interval (rings): 3
                         Call Park Timeout Interval (minutes): 10
          Off-Premises Tone Detect Timeout Interval (seconds): 20
                                AAR/ARS Dial Tone Required? y

              Music (or Silence) on Transferred Trunk Calls? no
                      DID/Tie/ISDN/SIP Intercept Treatment: attd
       Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                     Automatic Circuit Assurance (ACA) Enabled? n




                Abbreviated Dial Programming by Assigned Lists? n
        Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
   Display Calling Number for Room to Room Caller ID Calls? n
```

Use the **display feature-access-codes** command to verify that a FAC (feature access code) has been defined for both AAR and ARS. Note that **8** is used for AAR and **9** for ARS routing.

```
display 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: *25    Deactivation: #25
```

## 5.3. Administer Dial Plan

It was decided for compliance testing that all calls beginning with 43 with a total length of 4 digits were to be sent across the SIP trunk to Session Manager and therefore to Communications Portal. In order to achieve this, automatic alternate routing (aar) would be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this.

Type **change dialplan analysis**, in order to make changes to the dial plan. Ensure that **43** is added with a **Total Length** of **4** and a **Call Type** of **udp**.

```
change 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          4    ext
   3          4    ext
   43         4    udp
   5          4    ext
   6          4    ext
   7          3    dac
   8          1    fac
   9          1    fac
   *          3    fac
   #          3    fac
```

## 5.4. Administer Route Selection for Communications Portal Calls

As digits **43**xx were defined in the dial plan as udp (**Section 5.3**) use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **43** that are **4** digits in length will be matched. No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

```
change uniform-dialplan 8                                         Page   1 of   2
                          UNIFORM DIAL PLAN TABLE
                                                        Percent Full: 0

   Matching                  Insert              Node
   Pattern      Len Del      Digits      Net Conv Num
   43            4   0                   aar  n
                                              n
```

Use the **change aar analysis** x command to further configure the routing of the dialed digits. Calls to Communications Portal begin with **43** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

```
change aar analysis 4                                             Page   1 of   2
                          AAR DIGIT ANALYSIS TABLE
                               Location: all           Percent Full: 1

   Dialed                    Total    Route    Call   Node  ANI
   String                  Min  Max  Pattern   Type   Num   Reqd
   43                       4    4      1       unku         n
```

Use the **change route-pattern _n_** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Route Pattern Number 1** is used to route calls to trunk group **(Grp No) 1**, this is the SIP Trunk configured in **Section 5.5**.

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

## 5.5. Configure SIP Trunk

In the Node Names IP form, note the IP Address of the **procr** and the Session Manager (**SM63vmpg**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

```
display node-names ip                                          Page   1 of   2
                              IP NODE NAMES
    Name              IP Address
AES63VMPG          10.10.40.30
PGDECT             10.10.40.50
SM63vmpg           10.10.40.34
default            0.0.0.0
procr              10.10.40.31
procr6             ::
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.2**. In this configuration, the domain name is **devconnect.local**. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

```
display ip-network-region 1                                    Page   1 of  20
                           IP NETWORK REGION
  Region: 1
Location: 1        Authoritative Domain: devconnect.local
    Name: Default region
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: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
       Audio PHB Value: 46
       Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
       Audio 802.1p Priority: 6
       Video 802.1p Priority: 5     AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                  RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
           Keep-Alive Count: 5
```

In the **IP Codec Set** form, select the audio codec's supported for calls routed over the SIP trunk to Communications Portal. The form is accessed via the **change ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.729**, **G.711MU** (mu-law) and **G.711A** (a-law), which are supported by Communications Portal.

```
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.729             n             2        20
 2: G.711MU           n             2        20
 3: G.711A            n             2        20
 4:
 5:
```

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the desired transport method, for compliance testing this was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM63vmpg**), as per **Section 5.5**.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above**.** This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- Leave the **Far-end Domain** field blank to allow Communication Manager to accept any domain.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The default values for the other fields may be used.

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

 Group Number: 1                  Group Type: sip
  IMS Enabled? n          Transport Method: tls
        Q-SIP? n
    IP Video? n                                 Enforce SIPS URI for SRTP? y
 Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr              Far-end Node Name: SM63vmpg
 Near-end Listen Port: 5061             Far-end Listen Port: 5061
                                      Far-end Network Region: 1

Far-end Domain:
                                         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
```

Configure the **Trunk Group** form as shown below.  This trunk group is used for calls to and from Communications Portal. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

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

Group Number: 1                    Group Type: sip        CDR Reports: y
  Group Name: SIP TRK                     COR: 1      TN: 1      TAC: *11
    Direction: two-way       Outgoing Display? y
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie               Auth Code? n
                                         Member Assignment Method: auto
                                                   Signaling Group: 1
                                                 Number of Members: 10
```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Enghouse to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away, for the compliance test a value of **600** was used.

```
change trunk-group 1                                      Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

    Unicode Name: auto

                                      Redirect On OPTIM Failure: 5000

          SCCAN? n                              Digital Loss Group: 18
                    Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


           XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? N
```

Settings on **Page 3** can be left as default. However the **Numbering Format** in the example below is set to **private**.

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



                   Numbering Format: private
                                                UUI Treatment: service-provider

                                            Replace Restricted Numbers? n
                                           Replace Unavailable Numbers? n



                            Modify Tandem Calling Number: no


 Show ANSWERED BY on Display? y
```

Settings on **Page 4** are as follows.

```
change trunk-group 1                                              Page   4 of  21
                           PROTOCOL VARIATIONS

                                      Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                  Send Transferring Party Information? y
                            Network Call Redirection? n

                                 Send Diversion Header? n
                                Support Request History? y
                          Telephone Event Payload Type: 101


                          Convert 180 to 183 for Early Media? n
                     Always Use re-INVITE for Display Updates? n
                          Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
              Accept Redirect to Blank User Destination? y
                                              Enable Q-SIP? n
```

# 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® Session Manager
- Configure SIP Domain
- Configure Location
- Configure SIP Entities
- Configure Routing Policies
- Configure Dial Patterns

## 6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering **http://<FQDN >/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager or **http://<IP Adddress >/SMGR**. Log in using appropriate credentials.
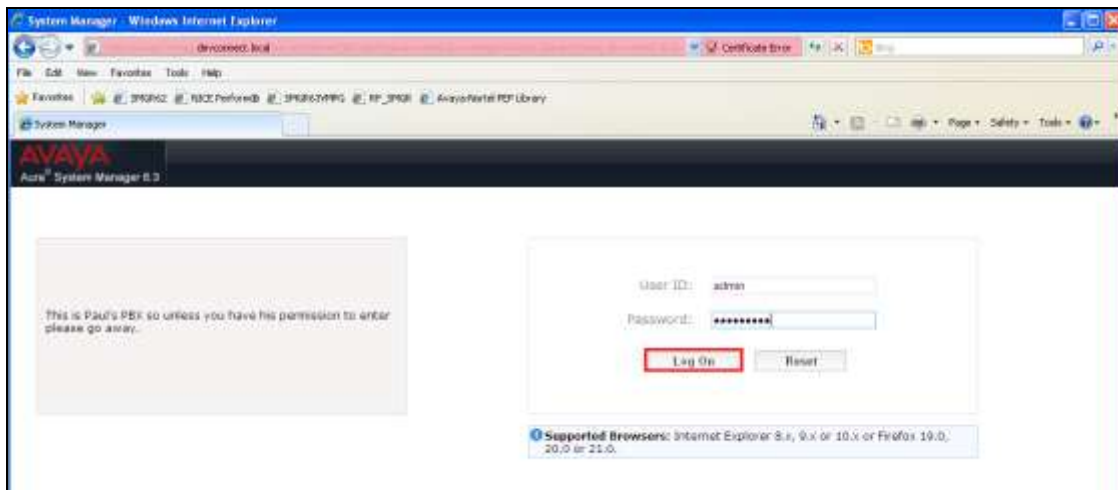


Once logged ion click on **Routing** as highlighted.
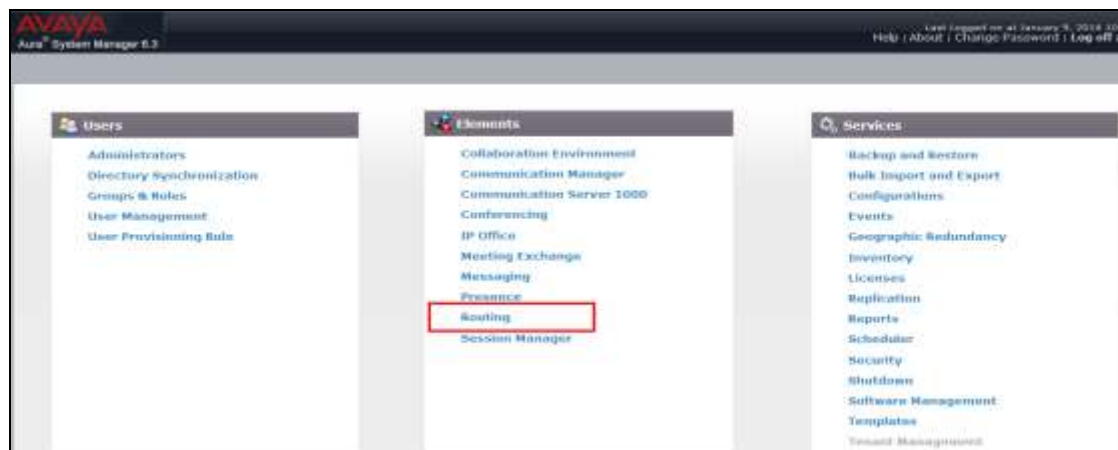
## 6.2. Configure SIP Domain

Click on **Domains** in the left window. If there is not a domain already configured click on **New** highlighted below.
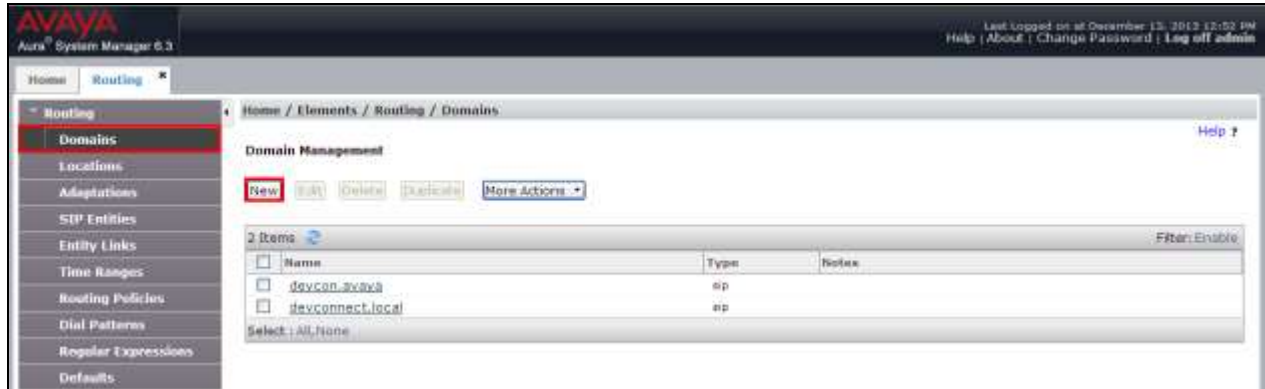


Enter the name of the domain note this was referenced in **Section 5.5**. The **Type** should be **sip**. Click on **Commit** once done.



## 6.3. Configure Location

Select **Locations** from the left window and select **New** from the main window.

Enter a suitable name for the location and scroll down to the bottom of the page and enter the IP addresses associated with the location in the case there are two ranges **10.10.40.x** and **192.168.50.x** and click on **Add**. Once completed, click on **Commit** to continue.

## 6.4. Configure Adaptation

To configure a new Adaptation select **Adaptations** from the left window and click on **New** from the main window.
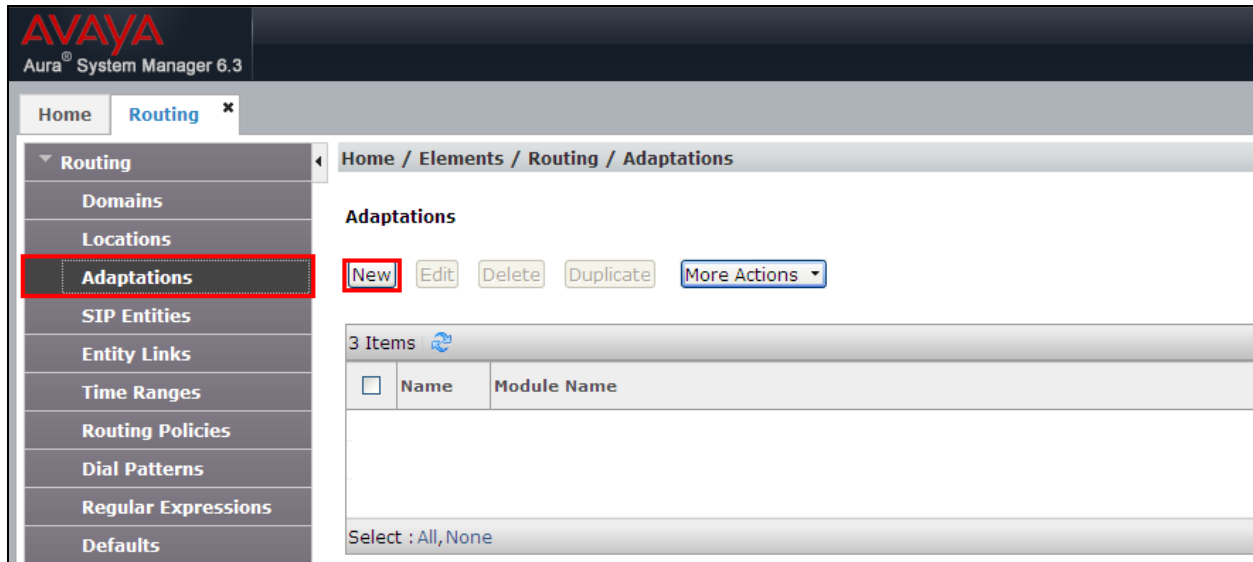


Enter a suitable **Name** and select **DigitConversionAdapter** for the **Module Name.** Select **Name-Value Parameter** as the **Module Parameter Type**. Add the following Parameters:

| Name | Value |
|------|-------|
| • fromto | true |
| • iodstd | "domain" |
| • iosrcd | "domain" |

SJW; Reviewed:
SPOC 10/6/2015

Solution & Interoperability Test Lab Application Notes
©2015 Avaya Inc. All Rights Reserved.

20 of 41
EHCP9MG_CM70
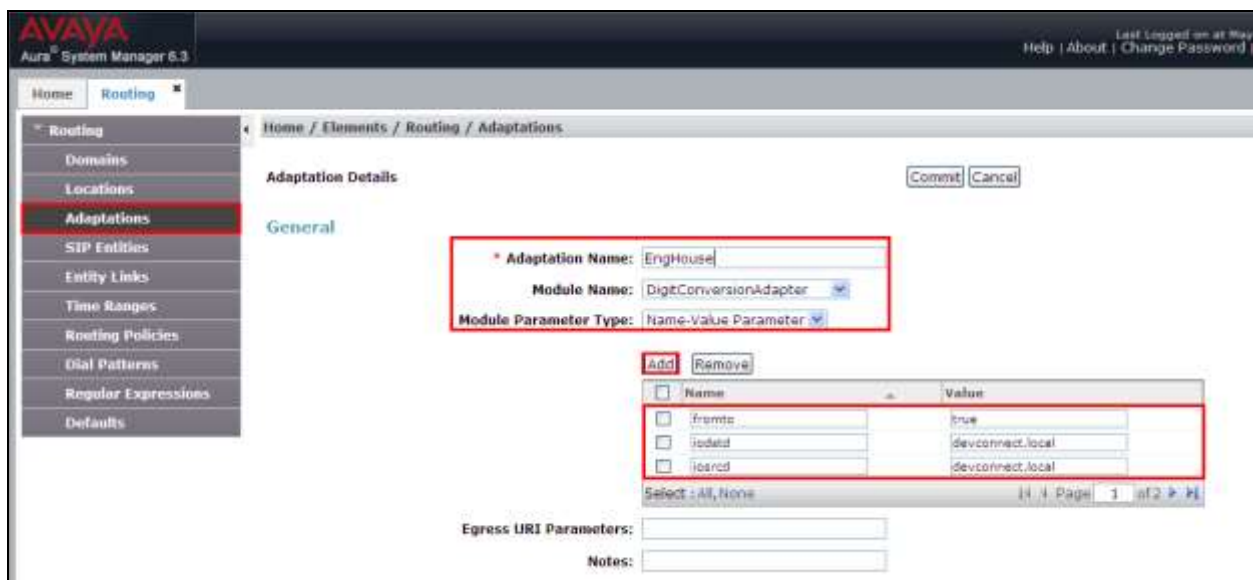
Continue to add the following Parameters:

**Name**             **Value**
- odstd          "Communications Portal IP Address"
- osrcd          "Session Manager IP Address"

Click on **Commit** once completed.

## 6.5. Configure SIP Entity for Enghouse Interactive Communications Portal

Select **SIP Entities** from the left window and click on **New** in the main window.
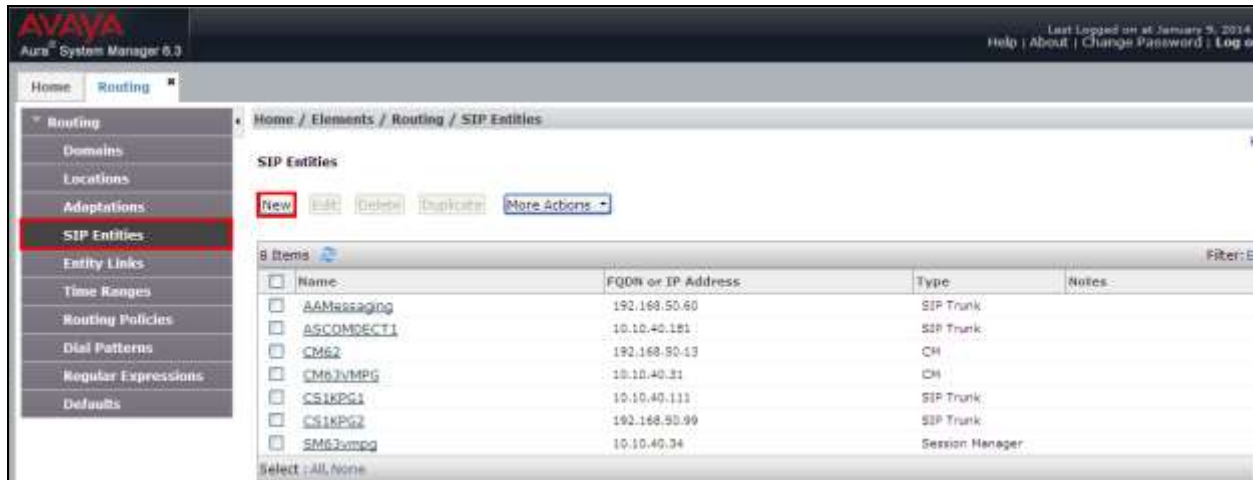


Enter a suitable **Name** and ensure that the **Adaptation** that was created in **Section 6.4** is used. Enter the **Location** that was configured in **Section 6.2** and the correct **Time Zone**.
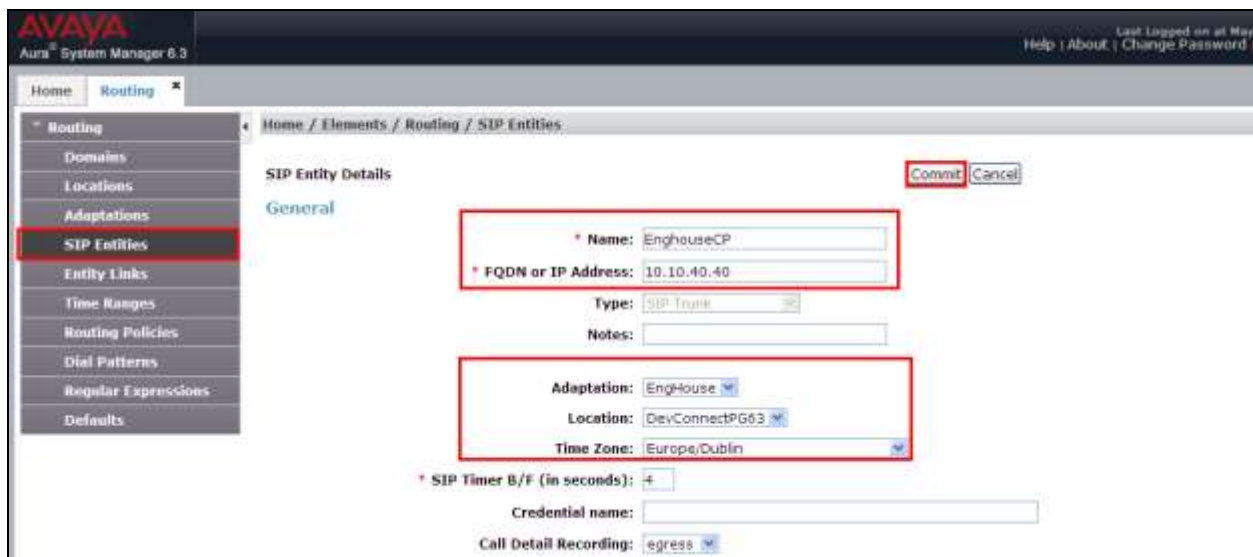
## 6.6. Configure Entity Link for Enghouse Interactive Communications Portal

Select **Entity Link** from the left window and click on **New** in the main window.



Select the correct **SIP Entity** that was created in **Section 6.5** and ensure that **TCP** is used as the **Protocol**. Note the **Port** is **5060**.

## 6.7. Configure Routing Policy for Enghouse Interactive Communications Portal

Select **Routing Policies** from the left window and click on **New** in the main window.
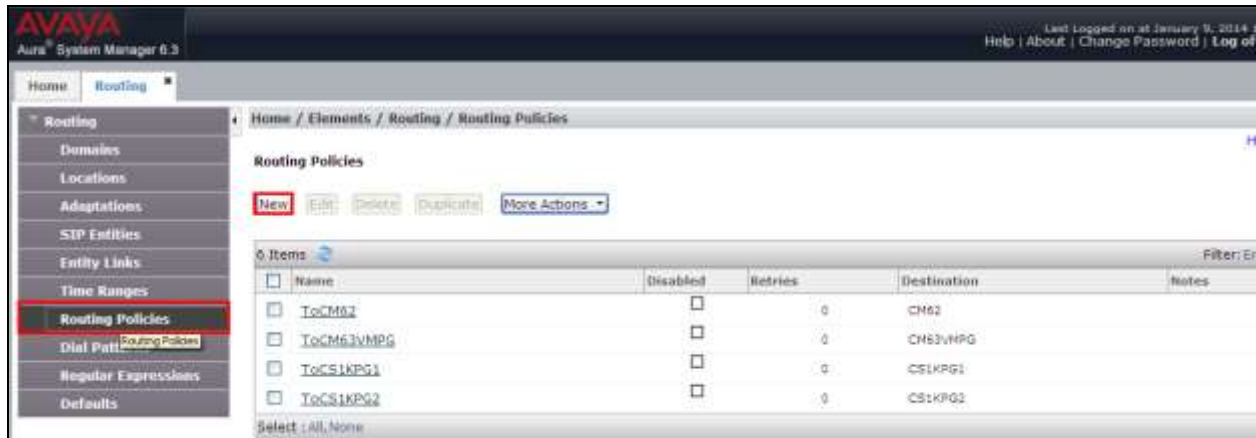


Enter a suitable **Name** and click on **Select** highlighted in order to associate this routing policy with a SIP Entity.
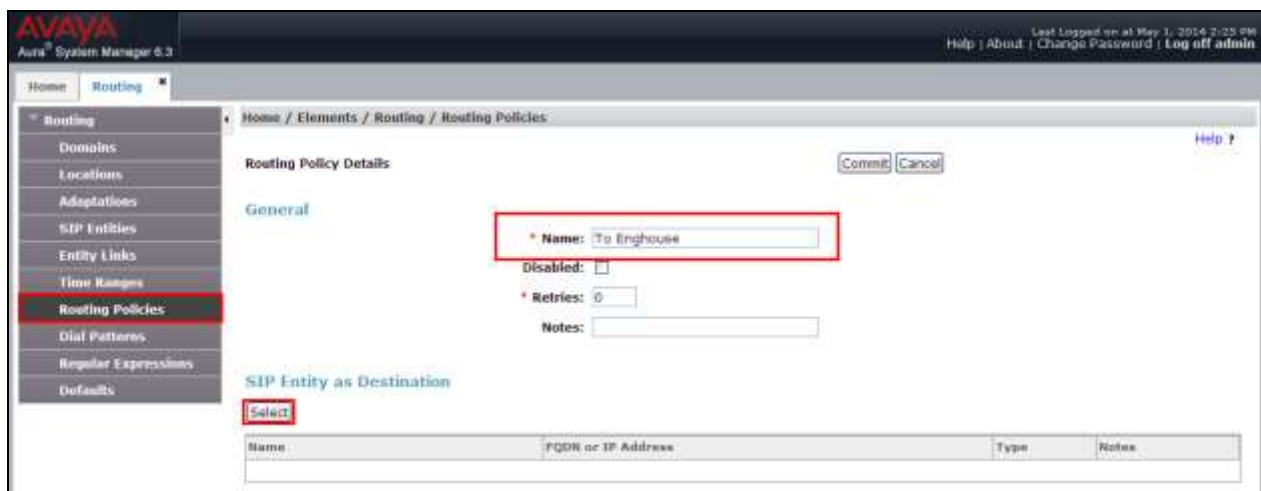
Select the **EnghouseCP** SIP Entity created in **Section 6.5** and click on **Commit** when done (not shown).
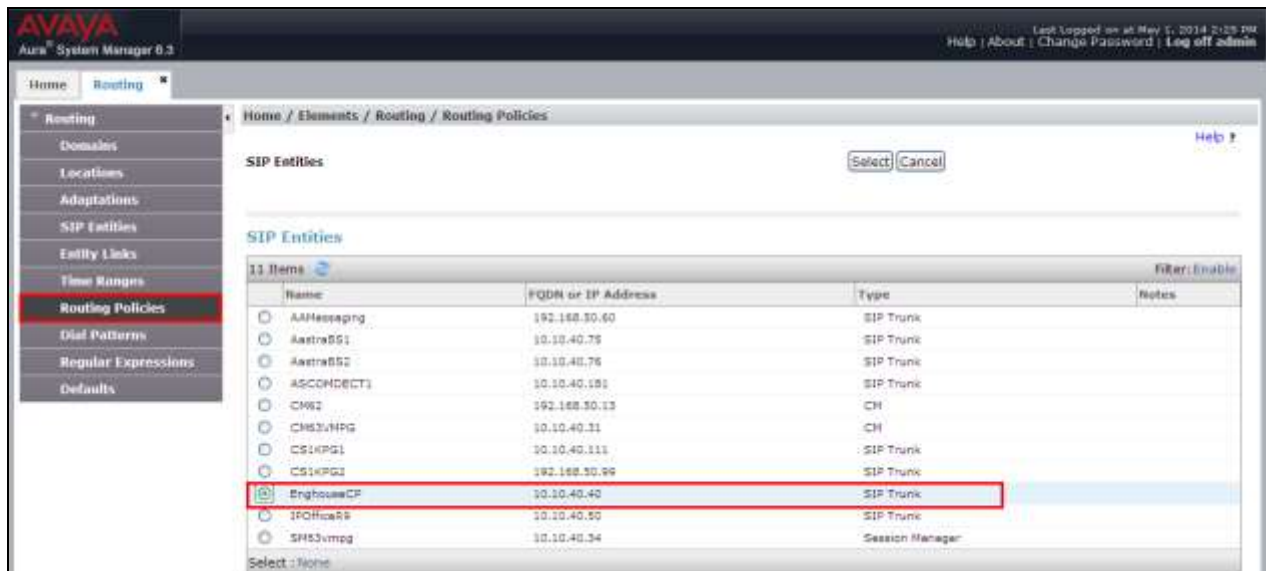


## 6.8. Configure Dial Pattern for Enghouse Interactive Communications Portal

In order to route calls to the Communications Portal a dial pattern is created pointing to the SIP Entity. Select **Dial Patterns** from the left window and click on **New** in the main window.

Enter the number to be routed noting this will be the same number outlined in **Section 5.4**. Note the **SIP Domain** is that configured in **Section 6.2**. Click on **Add** to select the SIP Entity.



Tick on the **Originating Location** as shown below and select the **Enghouse** Routing Policy. Click on **Select** once complete (not shown).

With the new Routing Policy in place, click on **Commit** as shown below.

SJW; Reviewed:
SPOC 10/6/2015

Solution & Interoperability Test Lab Application Notes
©2015 Avaya Inc. All Rights Reserved.

27 of 41
EHCP9MG_CM70

## 6.9. Configure Avaya Aura® Communication Manager SIP Entity

Select **SIP Entities** from the left window and click on **New** in the main window.
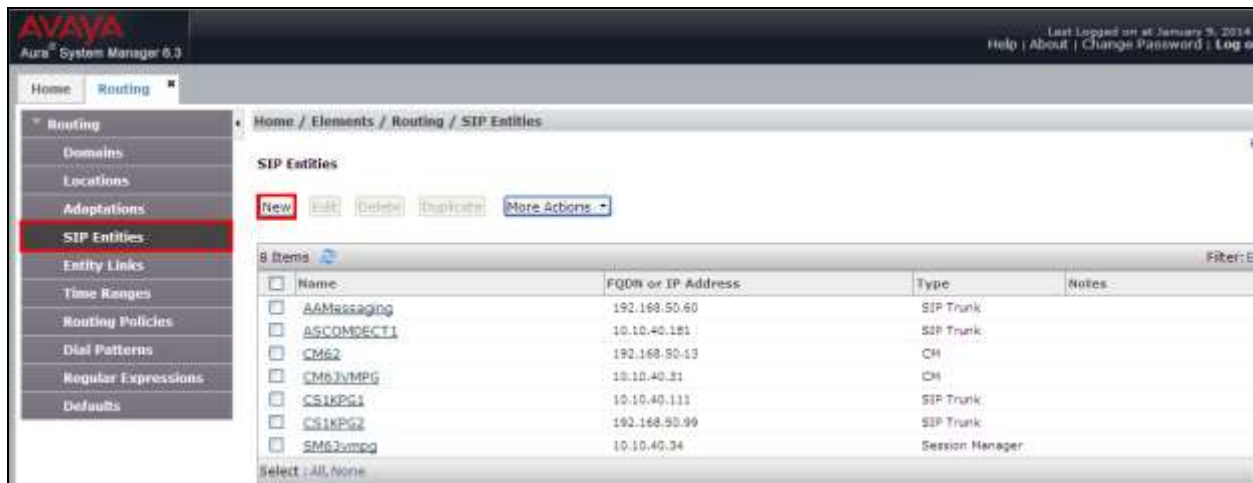


Enter a suitable **Name** and ensure the **Location** that was configured in **Section 6.2** and the correct **Time Zone** is entered.
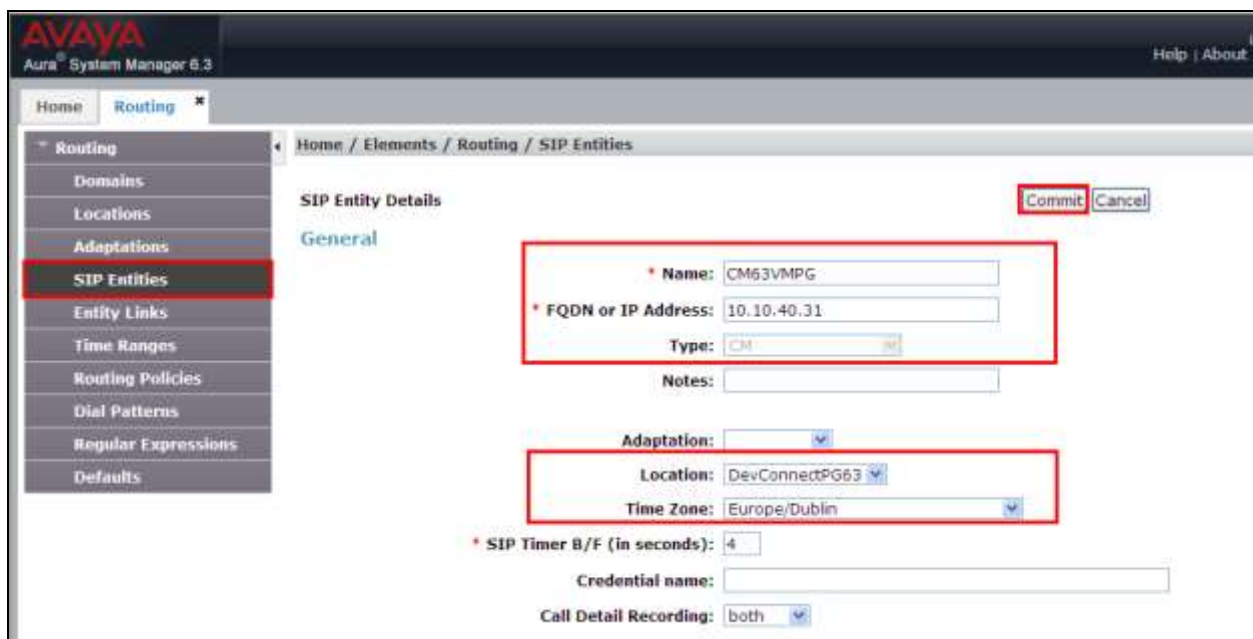
## 6.10. Configure Avaya Aura® Communication Manager Entity Link

Select **Entity Link** from the left window and click on **New** in the main window.
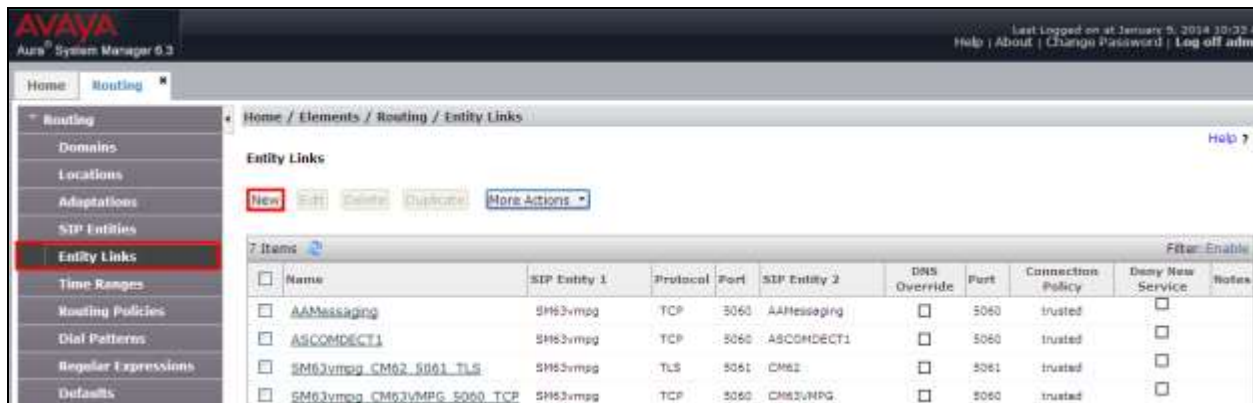


Select the correct **Sip Entity** that was created in **Section 6.9** and ensure that **TCP** is used as the **Protocol**. Note the **Port** is **5060**.

SJW; Reviewed:
SPOC 10/6/2015
Solution & Interoperability Test Lab Application Notes
©2015 Avaya Inc. All Rights Reserved.
29 of 41
EHCP9MG_CM70
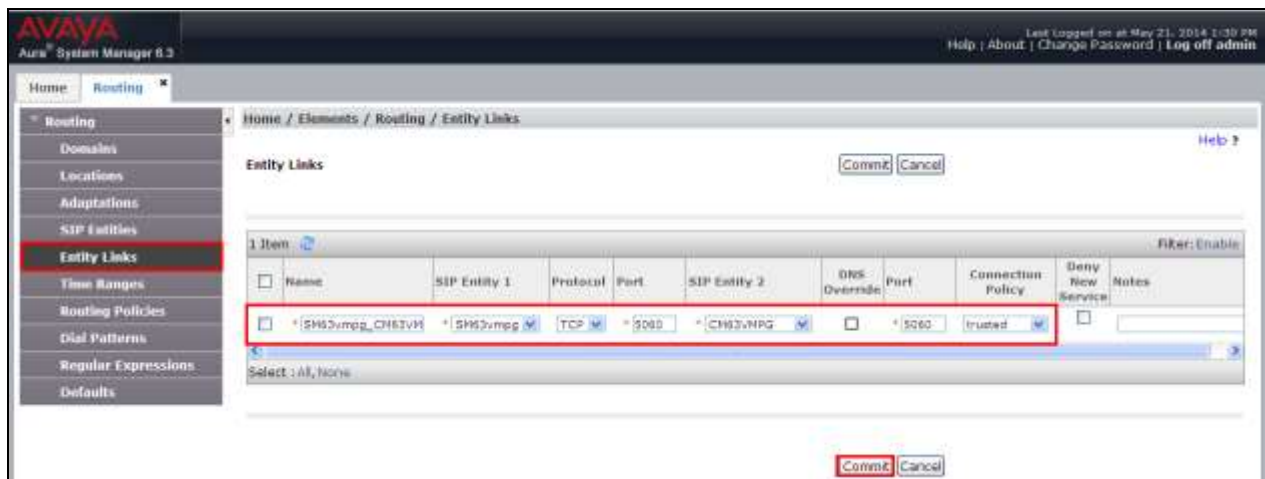
## 6.11. Configure Avaya Aura® Communication Manager Routing Policy

Select **Routing Policies** from the left window and click on **New** in the main window.



Enter a suitable **Name** and click on **Select** highlighted in order to associate this routing policy with a SIP Entity. Select the **Communication Manager** SIP Entity created in **Section 6.9** (not shown) and click on **Commit** when done.
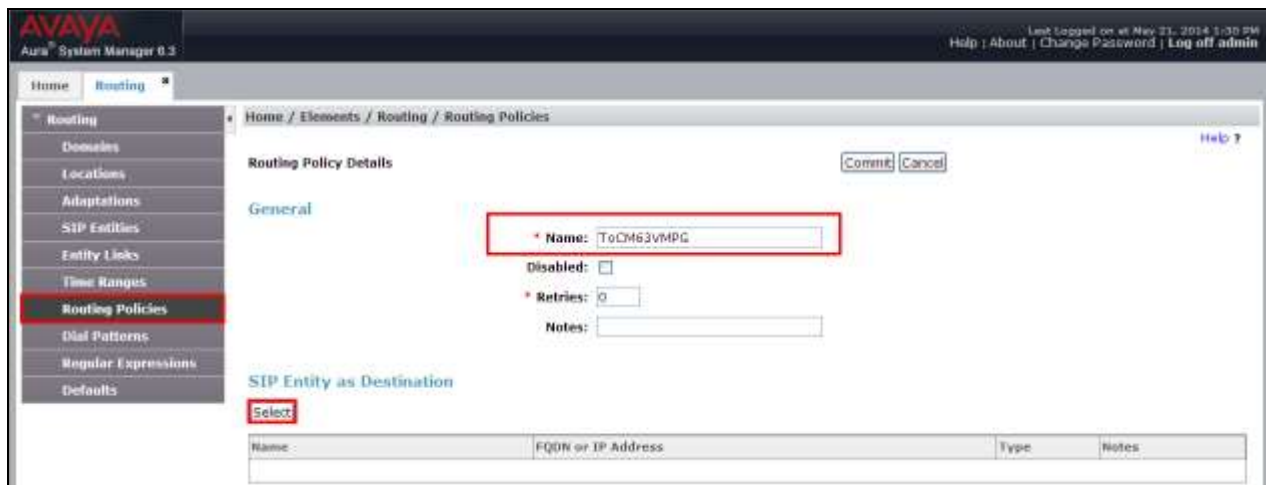
Select the Communication Manager SIP Entity as shown below and click on **Select**.
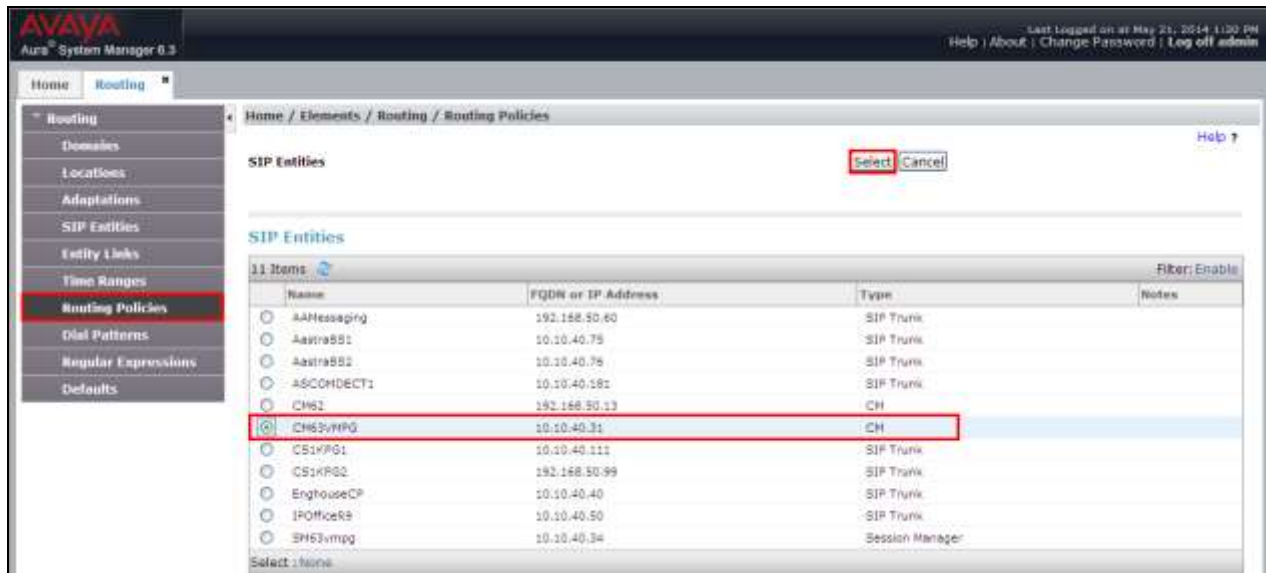


Once this is select the original screen is shown with the selected SIP Entity in place as highlighted below. Click on **Commit** once this is shown.
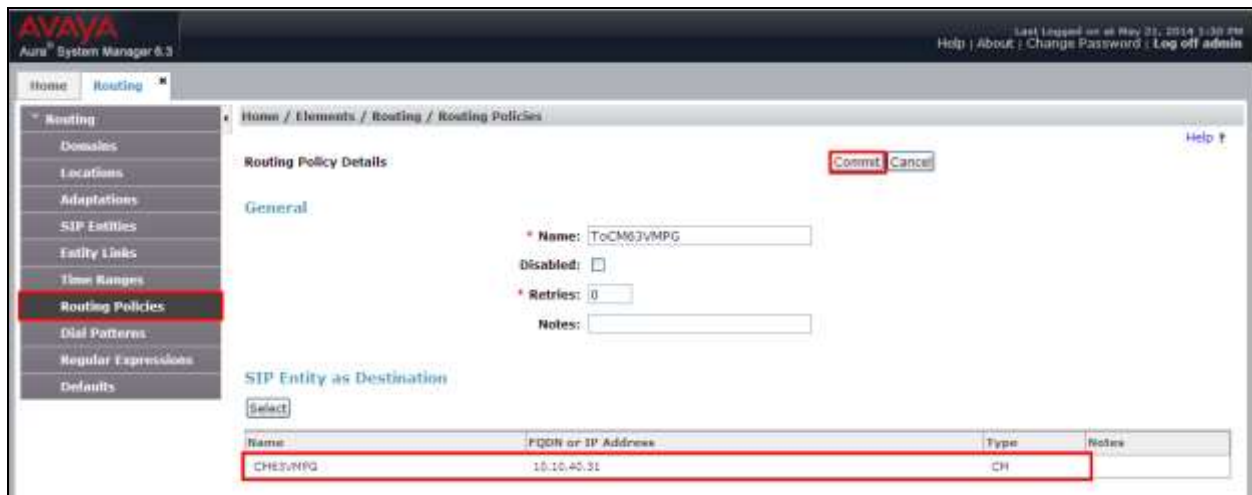
## 6.12. Configure Avaya Aura® Communication Manager Dial Pattern

In order to route calls to Communication Manager a dial pattern is created pointing to the SIP Entity. Select **Dial Patterns** from the left window and click on **New** in the main window.
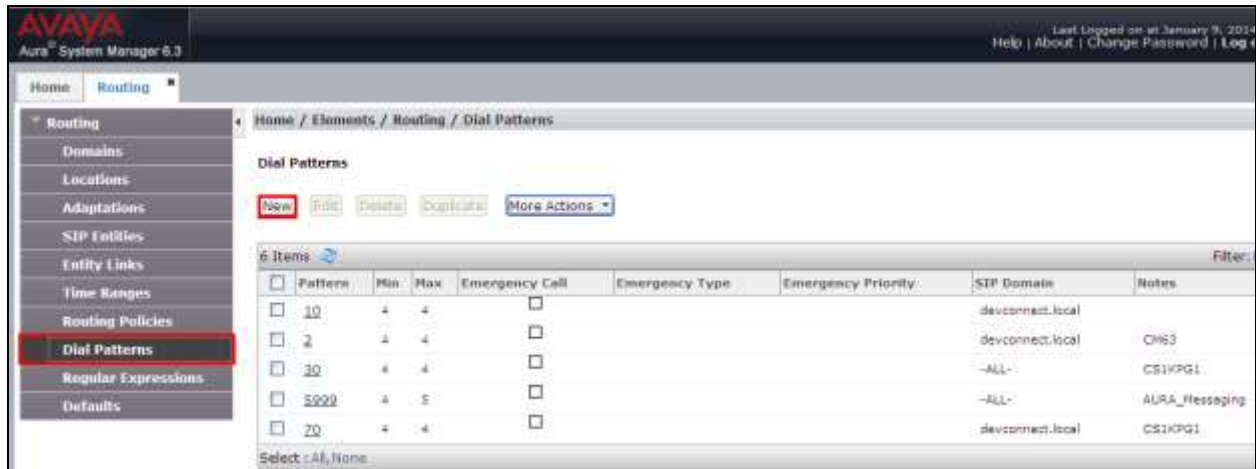


Enter the number to be routed noting this will be extension numbers of the Communication Manager deskphones, in this case **2xxx**. Note the **SIP Domain** is that configured in **Section 6.2**. Click on **Add** to select the SIP Entity.

SJW; Reviewed:
SPOC 10/6/2015
Solution & Interoperability Test Lab Application Notes
©2015 Avaya Inc. All Rights Reserved.
32 of 41
EHCP9MG_CM70
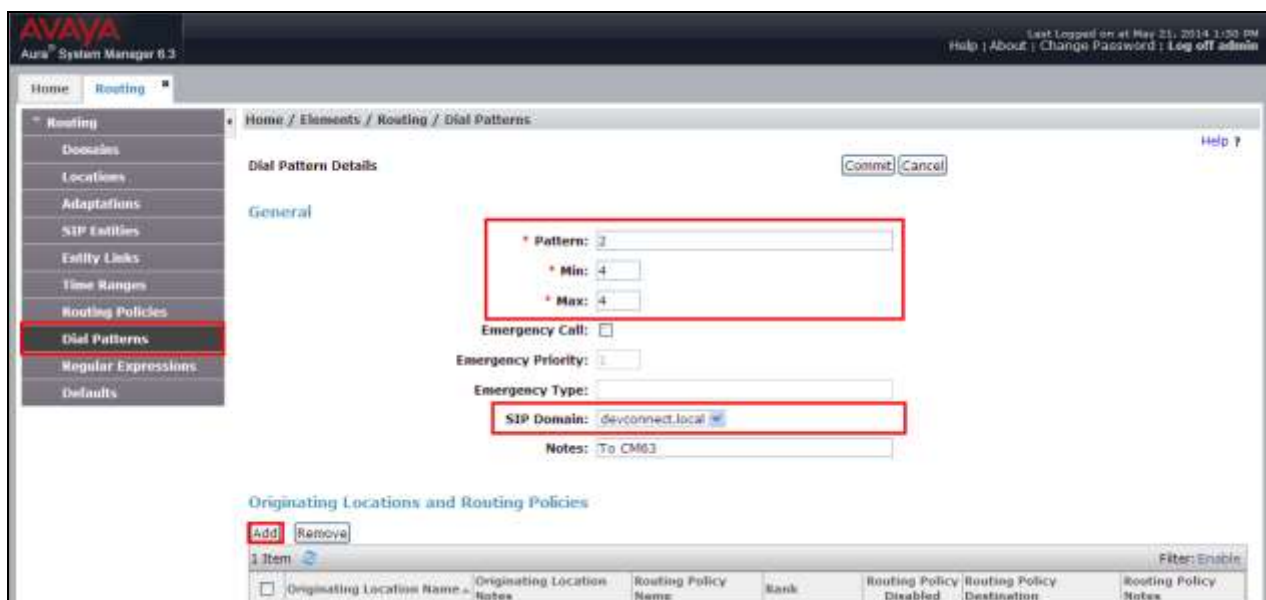
Tick on the **Originating Location** as shown below and select the **Communication Manager** Routing Policy. Click on **Select** once complete.



When **Select** above is clicked, the original screen will appear showing this selected Routing Policy as is highlighted below. Once this is shown correctly, click on **Commit** to finish.

SJW; Reviewed:
SPOC 10/6/2015
Solution & Interoperability Test Lab Application Notes
©2015 Avaya Inc. All Rights Reserved.
33 of 41
EHCP9MG_CM70

# 7. Configuration of Enghouse Interactive Communications Portal 9.0

This section describes the steps required to configure Enghouse Interactive Communications Portal 9.0 to interoperate with Avaya Aura® Communication Manager 7.0. These steps include:

- Media Gateway Driver Configuration
- Configuration file creation
- Change Outbound Dial plan
- Set the SIP transfer type parameter

## 7.1. Media Gateway driver configuration

When using Media Gateway perform the following steps to modify the configuration parameters in the Media Gateway configuration files.

- Create the avaya.xml gateway configuration file
- Change the outbound dial plan
- Set the SIP transfer type parameter

## 7.2. Create the avaya.xml gateway configuration file

To configure CP for this integration, prepare a gateway configuration file by performing the following steps.

- In the <Media Gateway install folder>\conf\sip_profiles\external folder, create a new text (.txt) file named *avaya.xml* with the following content. By default, Media Gateway is installed to C:\Program Files\Enghouse Interactive\Media Gateway.
- <include>
- <gateway name="AVAYA">
- Enter the IP address of you're the IP Office in the **realm** parameter value.
- <param name="realm" value="xxx.xxx.xxx.xxx"/>
- <param name="username" value="not-used"/>
- <param name="password" value="not-used"/>
- <param name="register" value="false"/>
- <param name="caller-id-in-from" value="false"/>
- <param name="register-transport" value="tcp"/>
- </gateway>
- </include>

## 7.3. Change the outbound dial plan

To configure CP for this integration, you must change the outbound dial plan configuration file by performing the following steps.

- In the <Media Gateway install folder>\conf\autoload_configs folder, edit the csdialplan.conf.xml file.
- Comment the following line:
  <!-- <param pattern="^(.+@.+)$" value="sofia/external/$1"/> -->
- Add the following line immediately below the line you commented:
  **<param pattern="^(.+@.+)$" value="sofia/gateway/AVAYA/$1"/>**
- Save the changes.

## 7.4. Set the SIP transfer type parameter

By default, the SIP transfer type is set to Refer. You must change transfer type to re-Invite with following steps.

- In the <Media Gateway install folder>\conf\autoload_configs folder, edit the csinterface.conf.xml file.
- Change the parameter **<param name="sip_transfer_type" value="refer"/>** to **<param name="sip_transfer_type" value="reinvite"/>**.
- Save the changes.

To complete the CP configuration, you must stop the CP engine, stop the Media Gateway service (if it is already started) and restart the CP Engine.

To configure the Media Gateway Driver open the **CP Console 9.0** by double clicking on the shortcut as shown below.
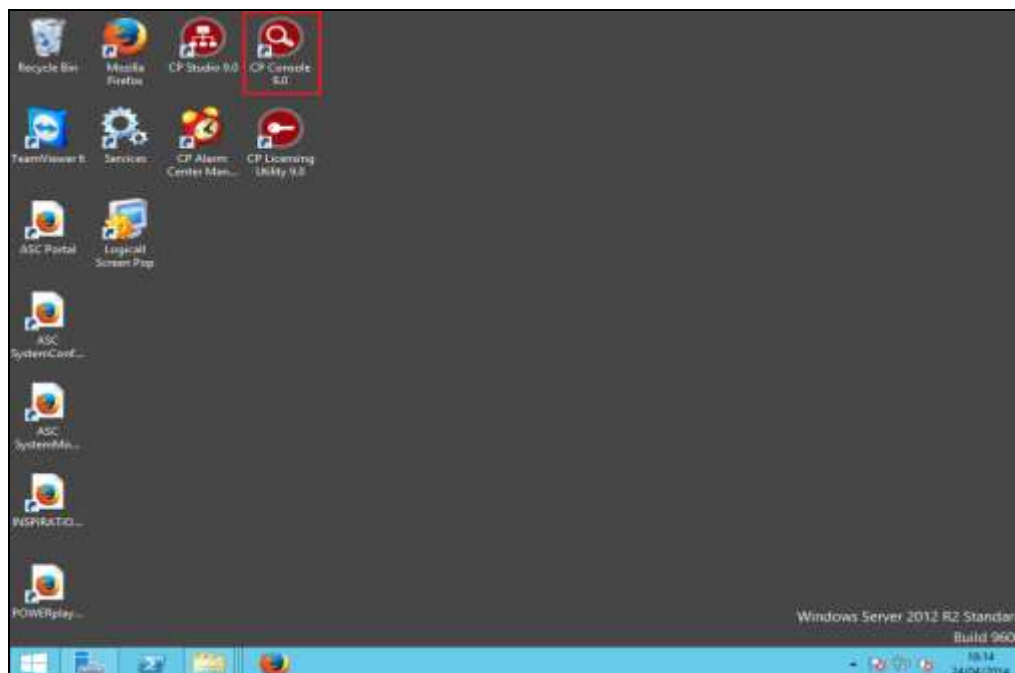
In the left window, navigate to **Servers** →**[Server Name]**→**Engine Settings**→**Drivers**→**Media Gateway Driver**.
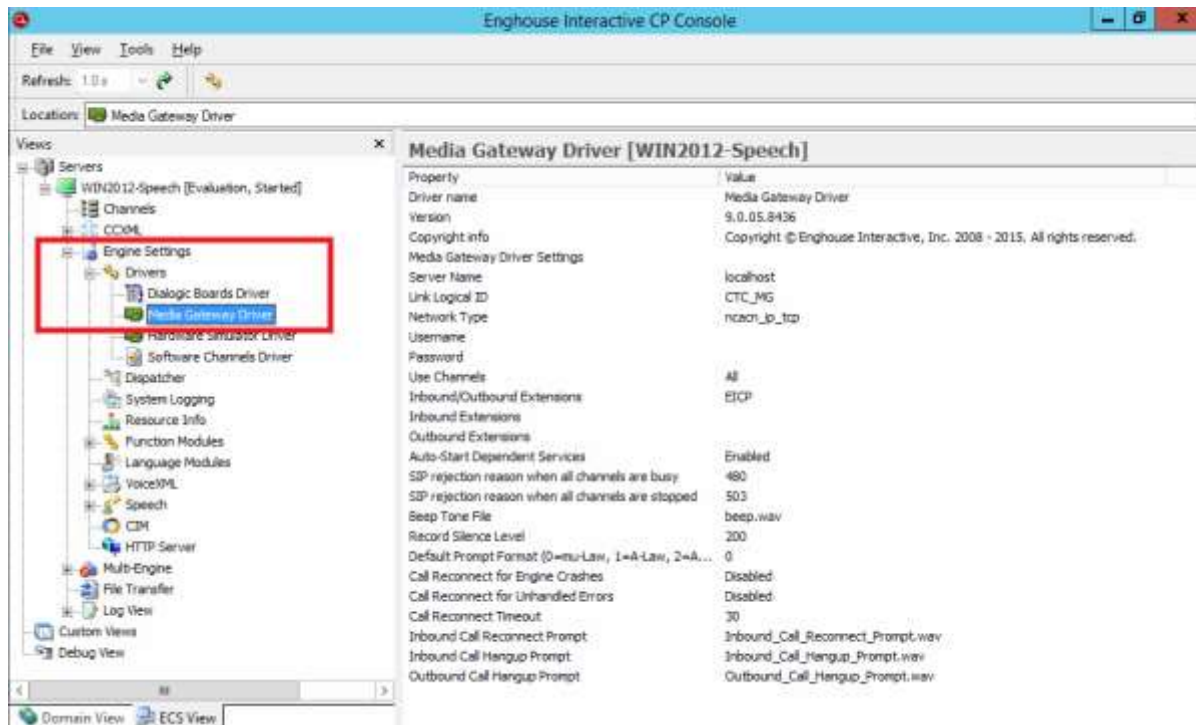


Please note that configuration of Communications Portal with regards to the setup of the IVR is outside the scope of these Application Notes, for more information on this setup please refer to **Section 10** of these Application Notes.
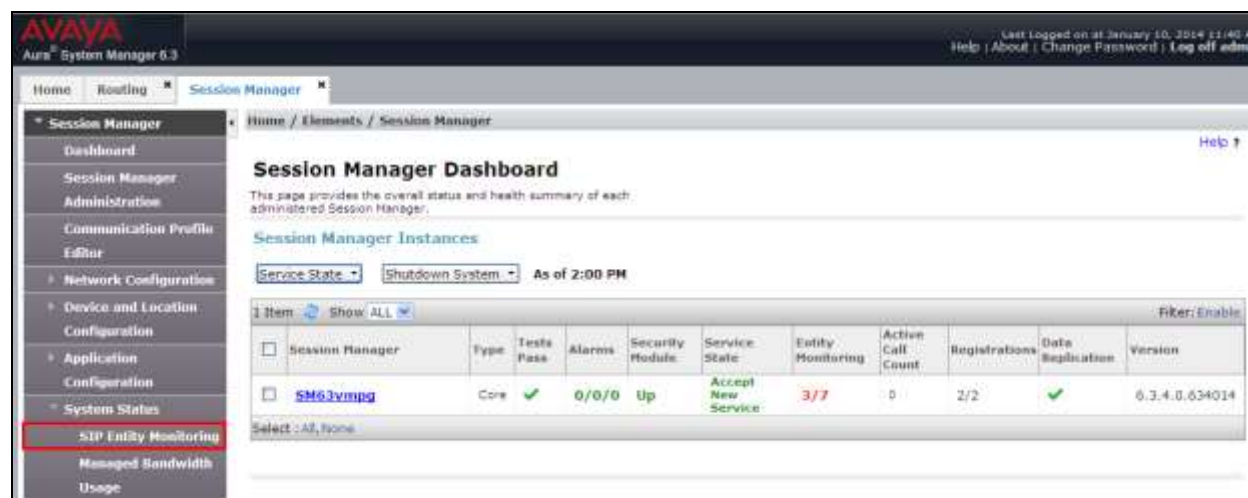
# 8. Verification Steps

To verify a successful configuration of Enghouse Interactive Communications Portal and Session Manager/Communication Manager a call is placed from a Communication Manager telephone to the Communications Portal with the caller getting answered successfully hearing clear and audible speech.

## 8.1. Verify Enghouse Interactive Communications Portal SIP Entity is up

Log in to System Manager as per **Section 6.1**. From the main menu select Session Manager as shown below.
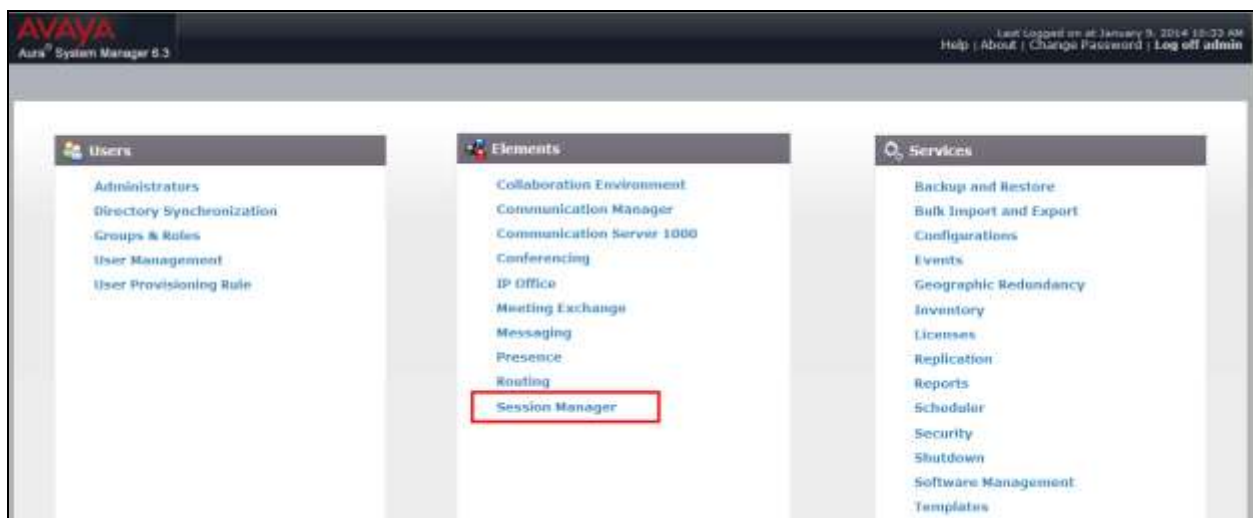


Navigate to **System Status → SIP Entity Monitoring**.

Select the **EnghouseCP** SIP Entity.



Note that both the **Conn. Status** and **Link Status** show **UP**.

## 8.2. Verify Enghouse Interactive Communications Portal IVR script

Open the **CP Console 9.0** by double clicking on the shortcut as shown below.



Channel 1 below has the script **Envox Central** associated with it**,** this should also show as green.
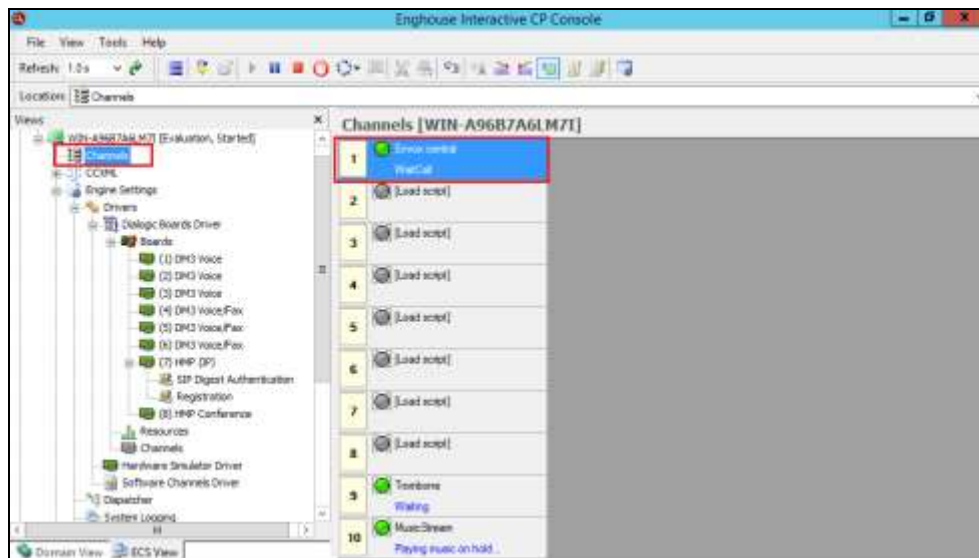
# 9. Conclusion

These Application Notes describe the configuration steps required for Enghouse Interactive Communications Portal 9.0 to successfully interoperate with Avaya Aura® Session Manager R6.3 and Avaya Aura® Communication Manager R6.3. All feature functionality and serviceability test cases were completed successfully as outlined in **Section 2.2.**

# 10.  Additional References

This section references the Avaya and Enghouse product documentation that are relevant to these Application Notes.

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

[1] *Administering Avaya Aura® Communication Manager,* Document ID 03-300509
[2] *Avaya Aura® Communication Manager Feature Description and Implementation,*
     Document ID 555-245-205
[3] *Administering Avaya Aura® Session Manager,* Release 6.3, 03-603324

Product documentation for Enghouse Interactive Communications Portal can be obtained by visiting the following website, www.enghouseinteractive.com

**©2015 Avaya Inc. All Rights Reserved.**
Avaya and the Avaya Logo are trademarks of Avaya Inc.  All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc.  All other trademarks are the property of their respective owners.  The information provided in these Application Notes is subject to change without notice.  The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty.  Users are responsible for their application of any products specified in these Application Notes.

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.