Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.2 as an Evolution Server, Avaya Aura® Session Manager R6.2 and Avaya Session Border Controller Advanced for Enterprise to support QSC VoIP Connect Service – Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the QSC VoIP Connect service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller Advanced for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server. QSC is a member of the DevConnect Service Provider program.

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.

NOTE: This Application Note focused on the SIP Trunking aspect of the Avaya Session Border Controller Advanced for Enterprise. Advanced enterprise capabilities such as Remote Worker "a.k.a. Remote SIP Endpoints", dual forking, and TLS/SRTP were not tested. As a result, the Avaya Session Border Controller for Enterprise is also considered Compliance Tested for this solution.

NOTE: This Application Note is applicable with Avaya Aura® 6.2 which is currently in Controlled Introduction. Avaya Aura® 6.2 will be Generally Available in Summer 2012.

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between QSC VoIP Connect service and an Avaya SIP-enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller Advanced for Enterprise (ASBCAE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with QSC VoIP Connect service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the Enterprise customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Session Border Controller. The enterprise site was configured to use the SIP Trunk service provided by QSC.

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 test included the following:

- Incoming calls to the enterprise site from the PSTN routed to the DDI numbers assigned by QSC
- Incoming PSTN calls made to SIP, H.323 and Analogue telephones at the enterprise
- Outgoing calls from the enterprise site completed via QSC to PSTN destinations
- Outgoing calls from the enterprise to the PSTN made from SIP, H.323 and Analogue telephones
- Calls using the G.711A, G.711MU and G.729 codecs
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones
- Call coverage and call forwarding for endpoints at the enterprise site
- Transmission and response of SIP OPTIONS messages sent by QSC requiring Avaya response and sent by Avaya requiring QSC response

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the QSC VoIP Connect service with the following observations:

- No inbound toll free numbers were tested as none were available from the Service Provider
- No Emergency Services numbers tested as test calls to these numbers should be pre-arranged with the Operator
- Direct media to SIP phones is not established unless Initial IP-IP Direct Media is set on the CM
- Callers hear silence and calls do not fail immediately when no codec match is found due to numerous network re-attempts when 488 “Not Acceptable Here” is sent by the CM
- Calls forwarded to the PSTN fail unless the CLI of the forwarding number is inserted in the P-Asserted-ID header using a script on the ASBCAE
- Conferences established on incoming calls are limited to two PSTN users
- Incoming T38 fax transmission is unsuccessful from Avaya Test Lab premises but successful from QSC premises, thought to be a local network issue
- Outgoing fax calls fail unless the G.711 format and attributes are removed from the SDP in the re-INVITE using a script on the ASBCAE
- When the trunk is congested, callers hear silence and calls do not fail immediately due to numerous network re-attempts when 500 “Service Unavailable” is sent by the CM
- When signalling has failed, callers hear silence and calls do not fail immediately due to numerous network re-attempts when 500 “Server Link Monitor Status Down” is sent by the SM

2.3. Support

For technical support on QSC products please visit the website at www.QSC.de or contact an authorized QSC representative.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the QSC VoIP Connect Service. Located at the Enterprise site is a Session Border Controller, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), Avaya 16xx series IP telephones (with SIP firmware) Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone running on a laptop PC configured for H.323.

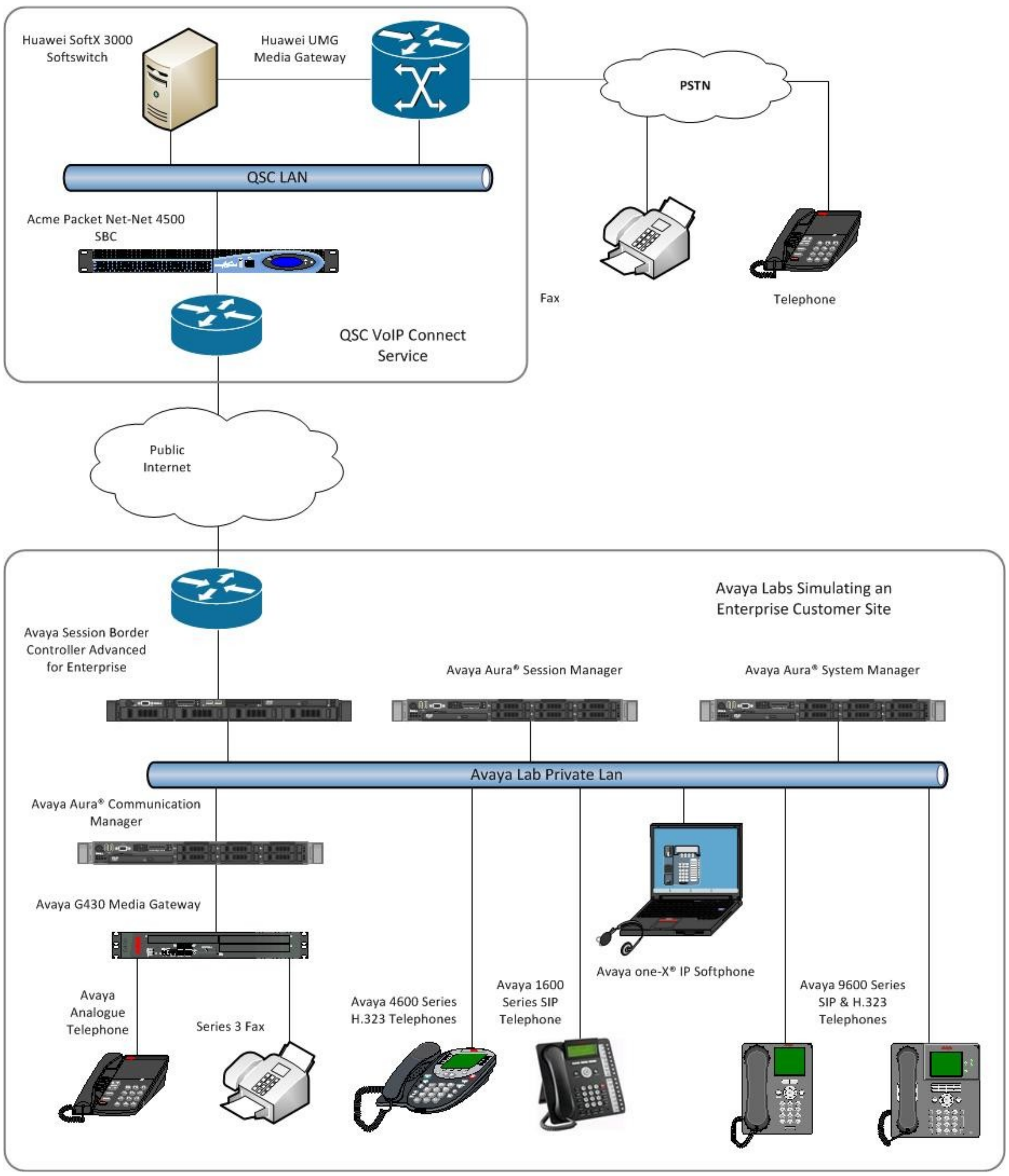


Figure 1: Test Setup QSC VoIP Connect to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment	Software
Avaya	
Avaya S8800 Server	Avaya Aura® Communication Manager R6.2 (R016x.02.0.823.0)
Avaya G430 Media Gateway	FW 30.12.1
Avaya S8800 Server	Avaya Aura® Session Manager R6.2 (6.2.0.0.620120)
Avaya S8800 Server	Avaya Aura® System Manager R6.2 (System Platform 6.2.0.0.27, Template 6.2.12.0)
Avaya Session Border Controller Advanced for Enterprise Server	Avaya Session Border Controller Advanced for Enterprise 4.0.5.Q02
Avaya 1616 Phone (H.323)	1.301
Avaya 4621 Phone (H.323)	2.902
Avaya 9630 Phone (H.323)	3.103
Avaya 9601 Phone (SIP)	R6.1 SP3
Avaya 9630 Phone (SIP)	R2.6 SP6
Avaya one–X® Communicator (H.323) on Lenovo T510 Laptop PC	Avaya one–X® Communicator 6.1.3.08-SP3-Patch2-35791
Analogue Phone	N/A
QSC	
Acme Packet NetNet 4500 SBC	SCX6.2.0 MR-9 GA
Huawei SoftX 3000	V300R010
Huawei UMG	NA
SIP Proxy Kamailio	3.1
SIP Configuration File	20120410_ayaya_devconnect_test.gz

Note: At the time of test, Communication Manager R6.2 was in Control Induction phase prior to being made GA.

5. Configure Avaya Aura ® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP Signalling associated with the QSC VoIP Connect Service. For incoming calls, the Session Manager receives SIP messages from the Avaya Session Border Controller Advanced for Enterprise and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Session Border Controller at the enterprise site that then sends the SIP messages to the QSC network. Communication Manager Configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the Avaya S8800 Servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the QSC network, and any other SIP trunks used.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 3
             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 20
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

On **Page 4**, verify that **IP Trunks** field is 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? n
                  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

           IP Attendant Consoles? y
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM100** and **10.10.9.61** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
SM100              10.10.9.61
Sipera-SBC         10.10.9.71
default            0.0.0.0
procr              10.10.9.52
procr6             ::
```

5.3. Administer IP Network Region

Use the **change ip-network-region 1** command to set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra**- and **Inter-Region**) is enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled, the media stream is established directly between the enterprise end-point and the internal media interface of the ASBCAE.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** is used.

```
change ip-network-region 1                                          Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: default
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
```

5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the IP Network Region form, **Section 5.3.** Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codecs supported by QSC were configured, namely **G.729**, **G.711A** and **G.711MU**.

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

The QSC VoIP Connect service supports T.38 for transmission of fax. Navigate to **Page 2** to configure T.38 by setting the **Fax Mode** to **t.38-standard** as shown below.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



                    Mode                Redundancy
    FAX             t.38-standard        1
    Modem           off                  0
    TDD/TTY         US                   3
    Clear-channel   n                    0
```

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the QSC VoIP Connect service. During test, this was configured to use **TCP** and port **5060** to facilitate tracing and fault analysis. It is recommended however, to use TLS (Transport Layer Security) and the default TLS port of **5061** for security. Configure the **Signaling Group** using the **add signaling-group x** command as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **tcp**
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Far-end Node Name** to the Session Manager (node name **SM100** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (Commonly used TCP port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region **1**)
- Leave **Far-end Domain** blank (removes the analysis of the far end domain name and subsequent handling of multiple signalling groups where it is not required)
- Set **Direct IP-IP Audio Connections** to **y**
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)
- If direct media is required on SIP phones, set **Initial IP-IP Direct Media** to **y** (left as **n** for this test to observe shuffling on H.323 phones)

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: tcp
        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: SM100
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        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
```

5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group x** command, where **x** is an available trunk group. On **Page 1** of this form:

- Set the **Group Type** field to **sip**
- Choose a descriptive **Group Name**
- Specify a trunk access code (**TAC**) consistent with the dial plan
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **public-netwrk** – this setting is required when using the Diversion header
- Specify the signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**
- Specify the **Number of Members** supported by this SIP trunk group

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

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: Group 1                     COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

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 QSC to prevent unnecessary SIP messages during call setup.

```
Add 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
```

On **Page 3**, set the **Numbering Format** field to **public**. This ensures delivery of CLI with leading "+" indicating E.164 format

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



                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

On **Page 4** of this form:

- Set **Prepend '+' to Calling Number** to **y** to ensure delivery of number in E.164 format
- Set **Send Diversion Header** to **y** so that the header is sent for call forwarding and EC500
- Set **Support Request History** to **n** as QSC does not support History Info
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by QSC
- Set **Always Use re-INVITE for Display Updates** to **y** to allow correct operation of fax

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

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? y
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? y
                  Support Request History? n
             Telephone Event Payload Type: 101


       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? y
       Identity for Calling Party Display: P-Asserted-Identity
                           Enable Q-SIP? n
```

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number. In the test configuration, individual stations were mapped to send numbers allocated from the QSC DDI range supplied. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Note that the digits identifying the DDI range are not shown.

```
change public-unknown-numbering 1                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                 Total Administered: 7
 4  2000          1         49221nnnnnnn0   13      Maximum Entries: 9999
 4  2291          1         49221nnnnnnn4   13
 4  2296          1         49221nnnnnnn3   13    Note: If an entry applies to
 4  2316          1         49221nnnnnnn5   13    a SIP connection to Avaya
 4  2346          1         49221nnnnnnn2   13    Aura(R) Session Manager,
 4  2396          1         49221nnnnnnn1   13    the resulting number must
 4  2400          1         49221nnnnnnn7   13    be a complete E.164 number.
```

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the QSC VoIP Connect Service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

```
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: *69
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 7
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
```

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0 or 00. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

```
change ars analysis 0                                           Page   1 of   2
                            ARS DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 0

          Dialed           Total      Route     Call   Node  ANI
          String          Min  Max   Pattern    Type   Num   Reqd
    0                     8    14     1         pubu         n
    00                    13   17     1         pubu         n
    00353                 10   14     1         pubu         n
    0044                  12   14     1         pubu         n
    01                    7    14     1         pubu         n
    01989                 5    7      1         pubu         n
    0221                  12   14     1         pubu         n
    0800                  11   11     1         pubu         n
    118                   5    6      1         pubu         n
```

Use the **change route-pattern x** command to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**. Set the **Numbering Format** to **intl-pub**.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: all calls
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                               DCS/ IXC
    No          Mrk Lmt List Del  Digits                                 QSIG
                             Dgts                                        Intw
 1: 1    0                                                                n   user
 2:                                                                       n   user
 3:                                                                       n   user
 4:                                                                       n   user
 5:                                                                       n   user
 6:                                                                       n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                               intl-pub  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
```

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from QSC can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by QSC for testing are assigned to the internal extensions of the test equipment configured within the Communication Manager. The **change inc-call-handling-trmt trunk-group x** command is used to translate numbers +49221nnnnnnn0 to +49221 nnnnnnn 9 to the 4 digit extension by deleting all of the incoming digits and inserting the extension number. Note that the significant digits beyond the city code have been obscured.

```
change inc-call-handling-trmt trunk-group 1                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    14 +49221nnnnnnn0   all 2000
 public-ntwrk    14 +49221nnnnnnn1   all 2396
 public-ntwrk    14 +49221nnnnnnn2   all 2346
 public-ntwrk    14 +49221nnnnnnn3   all 2296
 public-ntwrk    14 +49221nnnnnnn4   all 2291
 public-ntwrk    14 +49221nnnnnnn5   all 2316
 public-ntwrk    14 +49221nnnnnnn6   all 6101
 public-ntwrk    14 +49221nnnnnnn7   all 2400
 public-ntwrk    14 +49221nnnnnnn8   all 6102
 public-ntwrk    14 +49221nnnnnnn9   all 2501
```

5.10. EC500 Configuration

When EC500 is enabled on the Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2396. Use the command **change off-pbx-telephone station mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension
- For **Application** enter **EC500**
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration
- For the **Phone Number** enter the phone that will also be called (e.g. **0035386xxxxxxx**)
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing
- Set the **Config Set** to **1**

```
change off-pbx-telephone station-mapping 2396                   Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number     Trunk       Config  Dual
 Extension                 Prefix                      Selection   Set     Mode
 2396             EC500         -     00353867818306    1           1
                                -
```

Save Communication Manager changes by entering **save translation** to make them permanent.

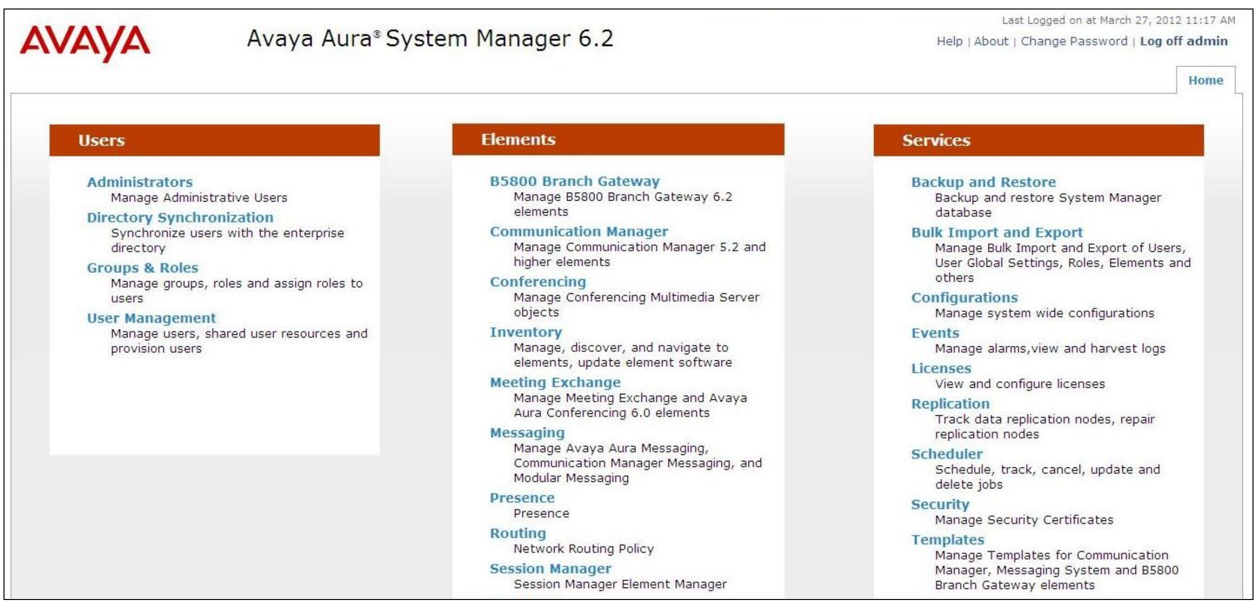
6. Configuring Avaya Aura® Session Manager

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

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Application for Avaya Aura® Communication Manager
- Administer Application Sequence for Avaya Aura® Communication Manager
- Administer SIP Extensions

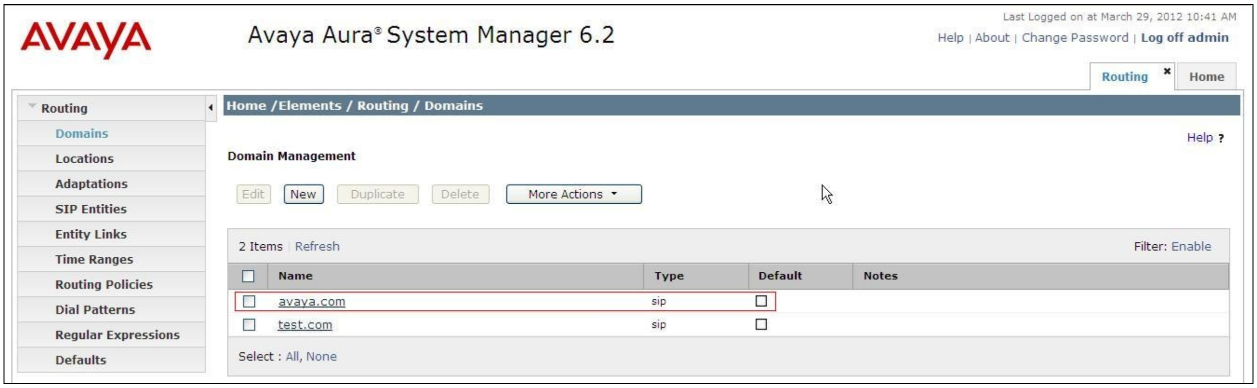
6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering **http://<FQDN >/SMGR**, where <**FQDN**> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the Home tab will be presented with menu options shown below.



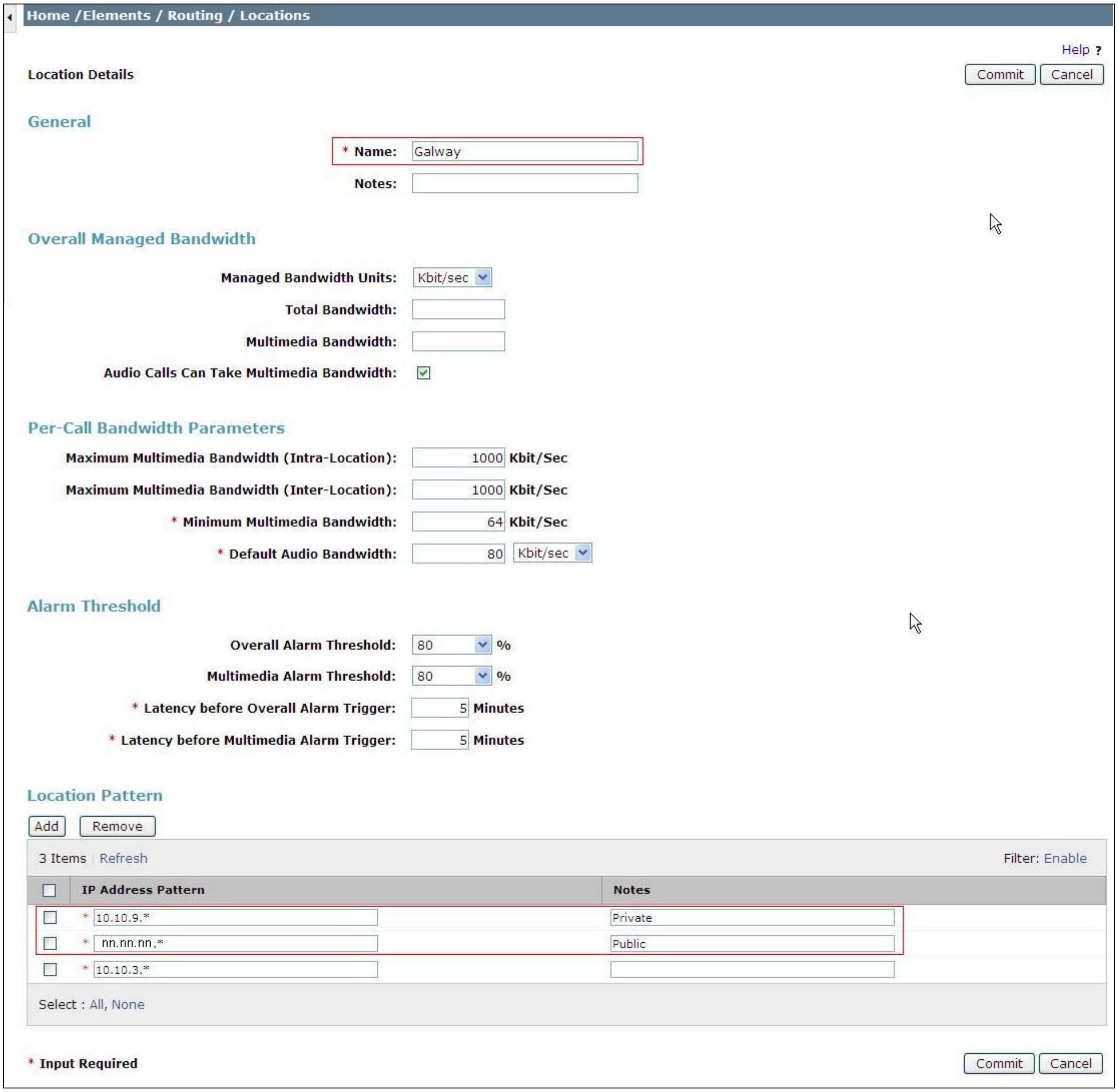
6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **avaya.com**) and optionally a description for the domain in the Notes field. Click **Commit** to save changes.



6.3. Administer Locations

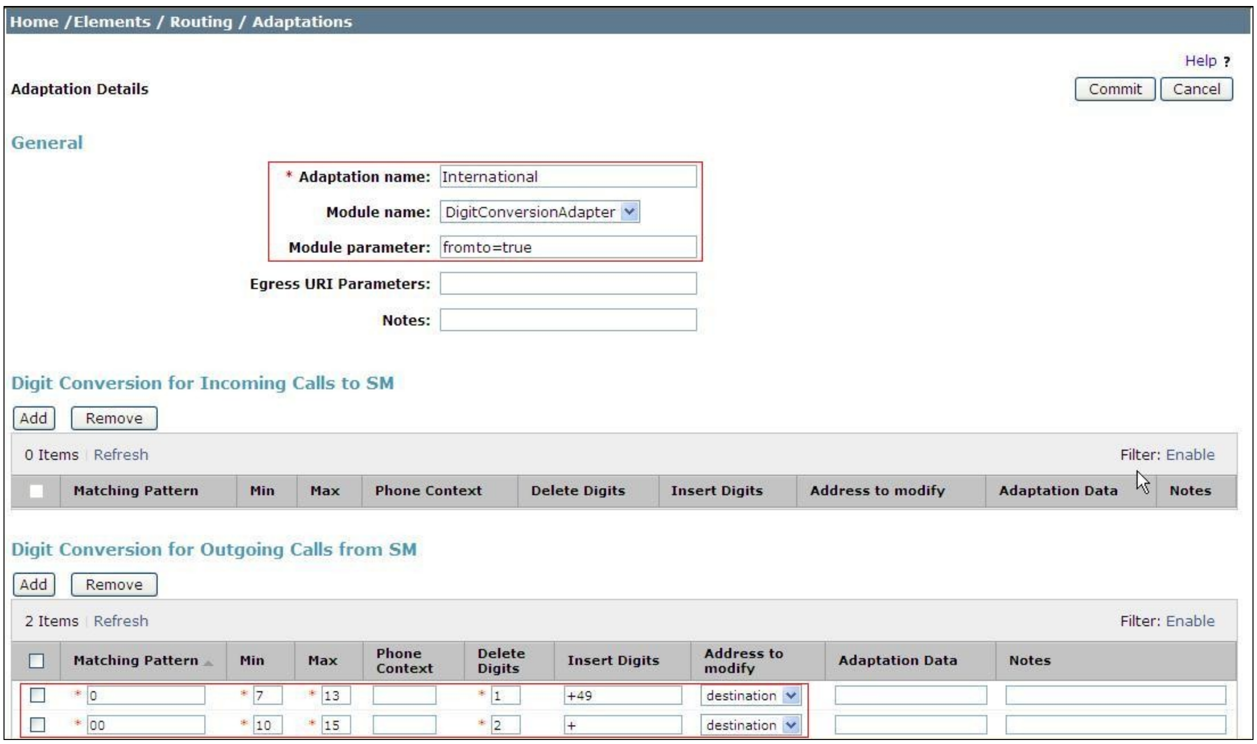
Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu. Under **General**, in the **Name** field, enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the test enterprise.



6.4. Administer Adaptations

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. Additionally, the called and calling party numbers can also be modified using **Digit Conversion** when **fromto=true** is entered in the **Module Parameters**. The example shown was used in test to convert the called numbers in the Request URI and To headers to E.164 format to be consistent with the calling party numbers in the From header.

DigitConversionAdaptor is used and leading zeros are analysed. Both national and international numbers are converted, though in test only international numbers were used. The two leading zeros of the international number are removed and replaced with a "+". These rules are applied to the destination addresses.



6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity. Under **General**:

- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **Gateway** for the Session Border Controller SIP entity
- In the **Adaptation** field select the appropriate adaptation defined in **Section 6.4**, in test **International** was selected for the ASBCAE to convert called party numbers to E.164 format with a leading "+"
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

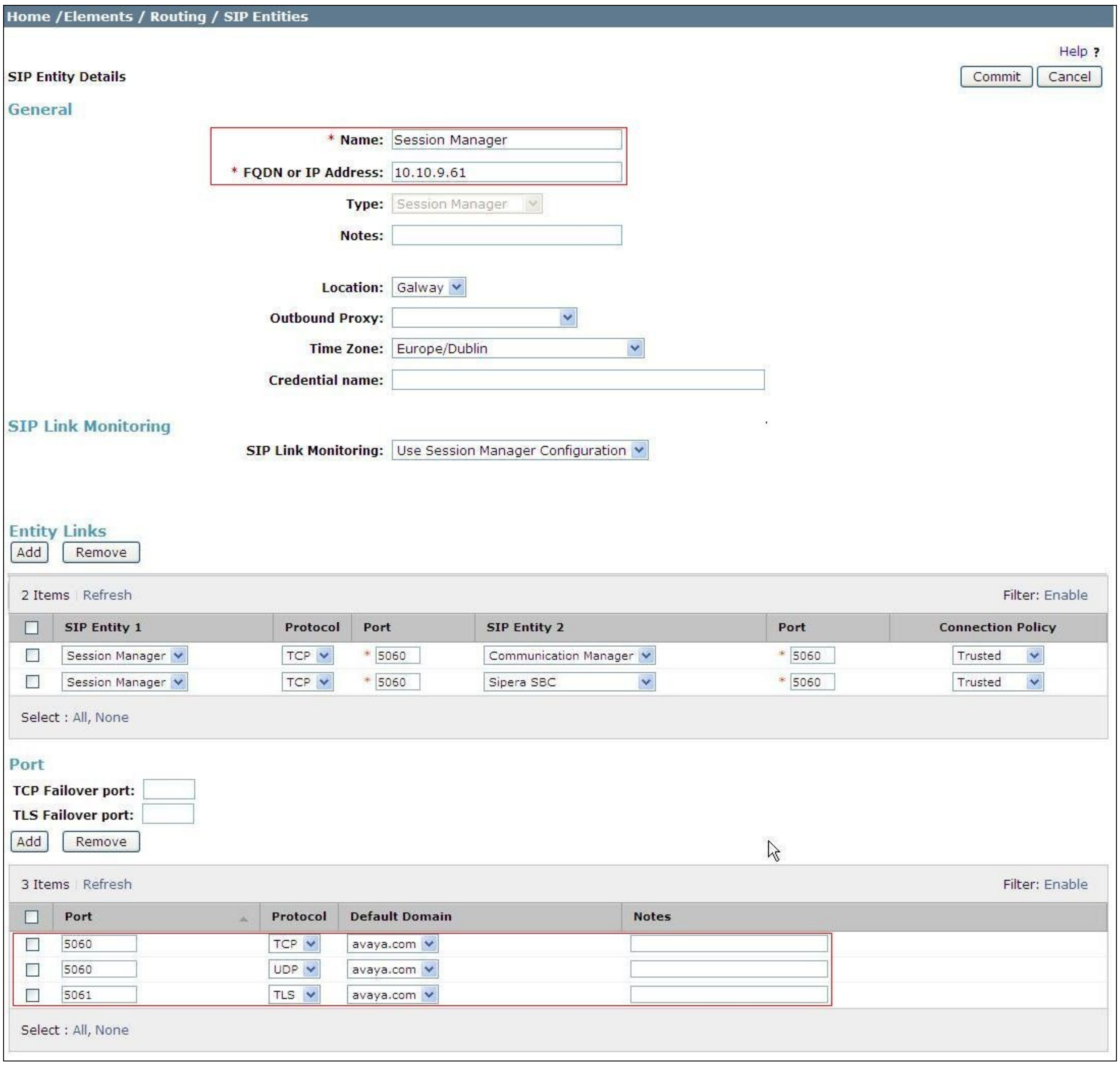
In this configuration there are three SIP Entities:

- Avaya Aura® Session Manager SIP Entity
- Avaya Aura® Communication Manager SIP Entity
- Avaya Session Border Controller Advanced for Enterprise SIP Entity

6.5.1. Avaya Aura® Session Manager SIP Entity

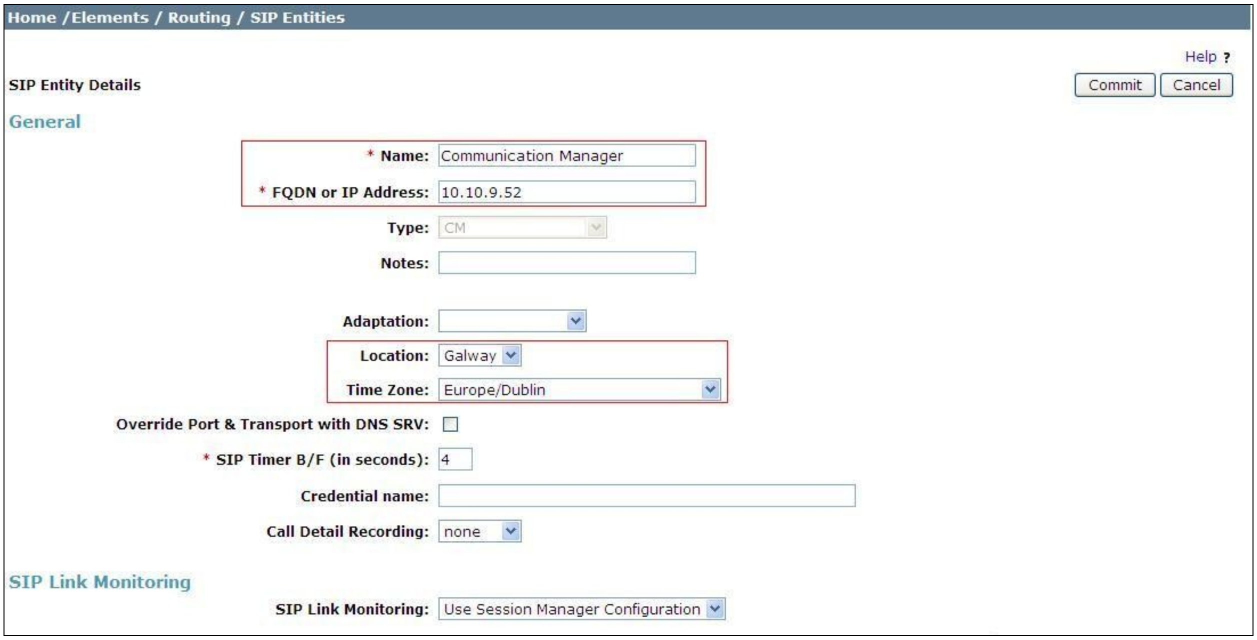
The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface. The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- In the **Port** field enter the port number on which the system listens for SIP requests
- In the **Protocol** field enter the transport protocol to be used for SIP requests
- In the **Default Domain** field, from the drop down menu select **avaya.com** as the default domain



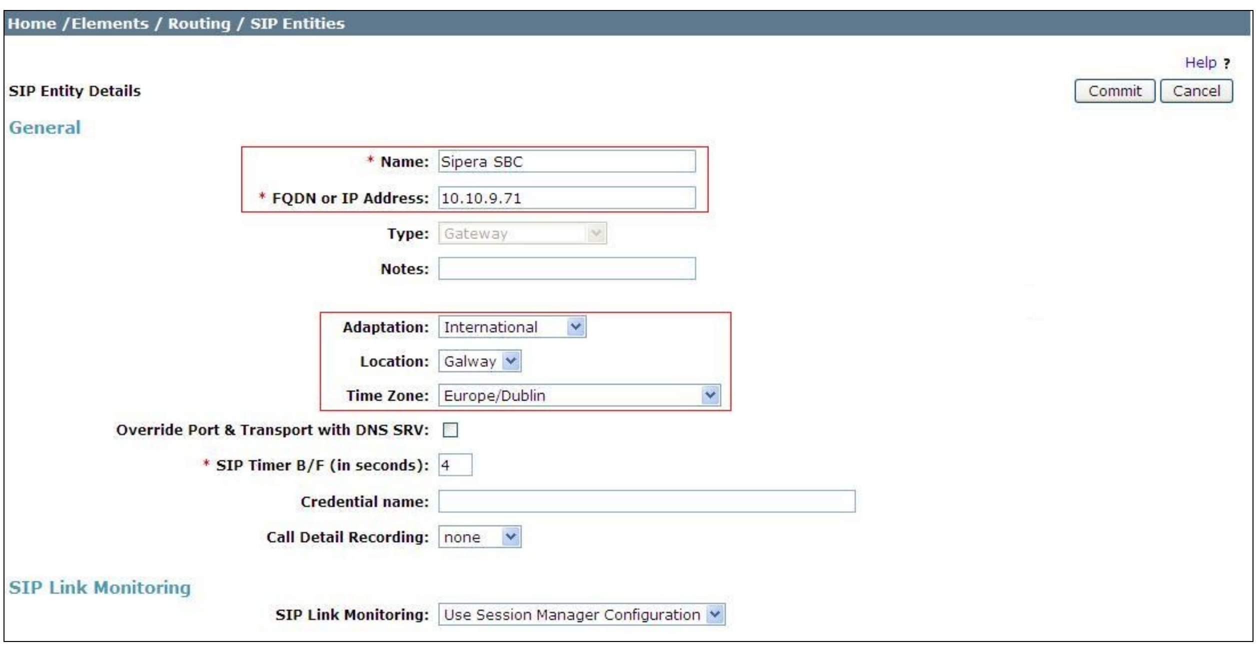
6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling.



6.5.3. Avaya Session Border Controller Advanced for Enterprise SIP Entity

The following screen shows the SIP Entity for the Session Border Controller. The **FQDN or IP Address** field is set to the IP address of the Session Border Controller private network interface.

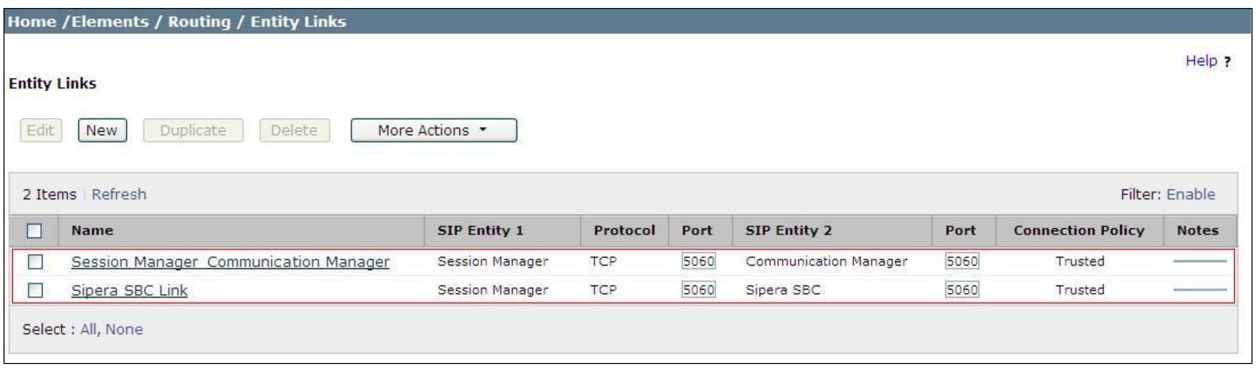


6.6. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select **Session Manager**
- In the **Port** field enter the port number to which the other system sends its SIP requests
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- Select the **Trusted** tick box to make the other system trusted
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in this configuration.



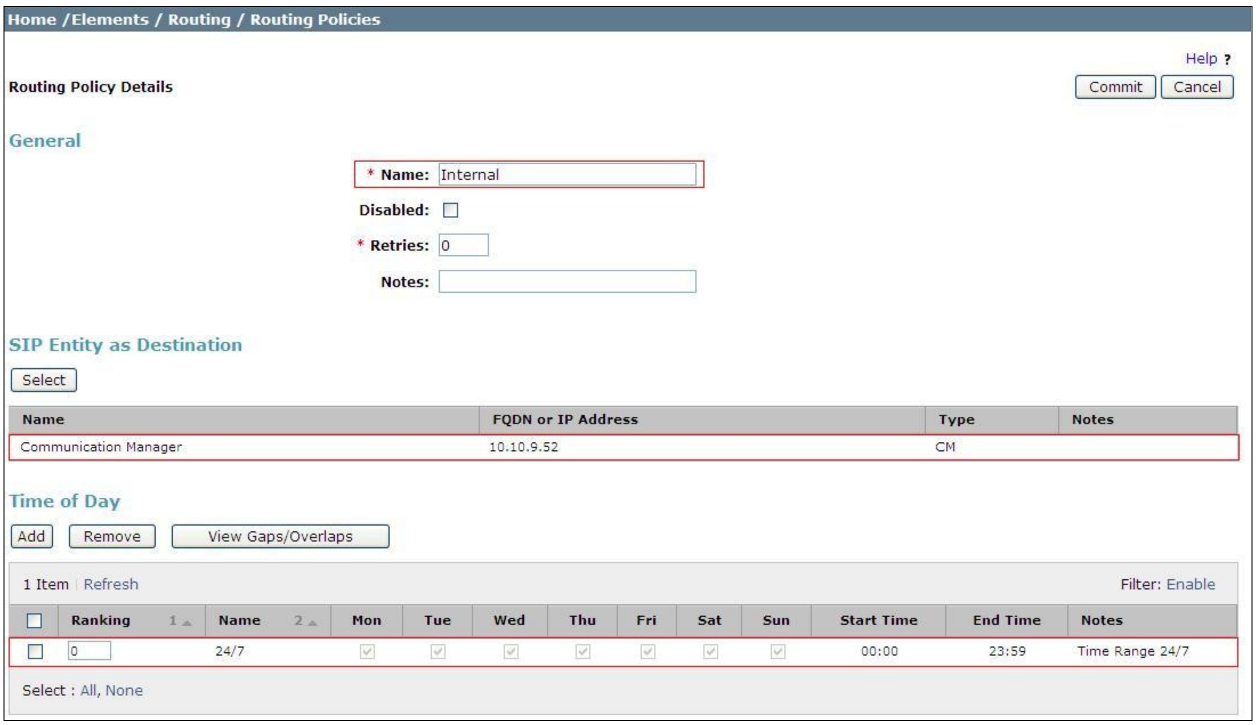
6.7. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

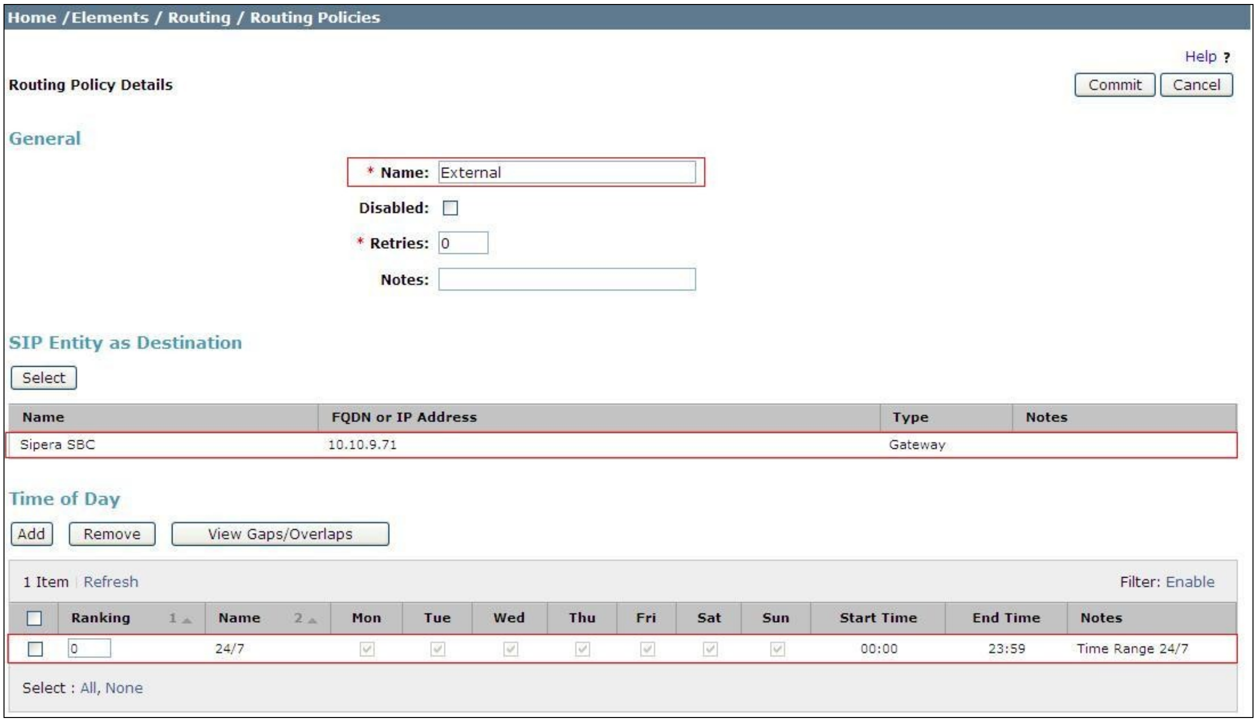
Under **General**:

- Enter an informative name in the **Name** field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies
- Under **Time of Day**, click **Add**, and then select the time range

The following screen shows the routing policy for Communication Manager.



The following screen shows the routing policy for the Session Border Controller.



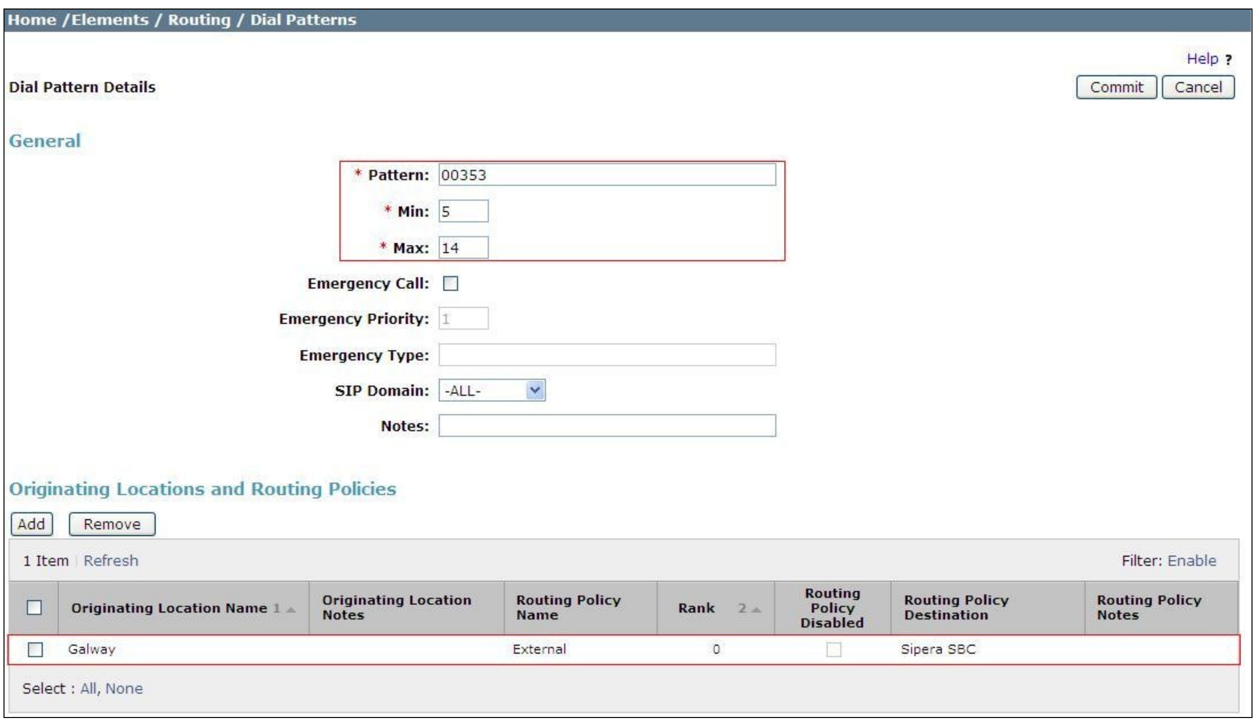
6.8. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

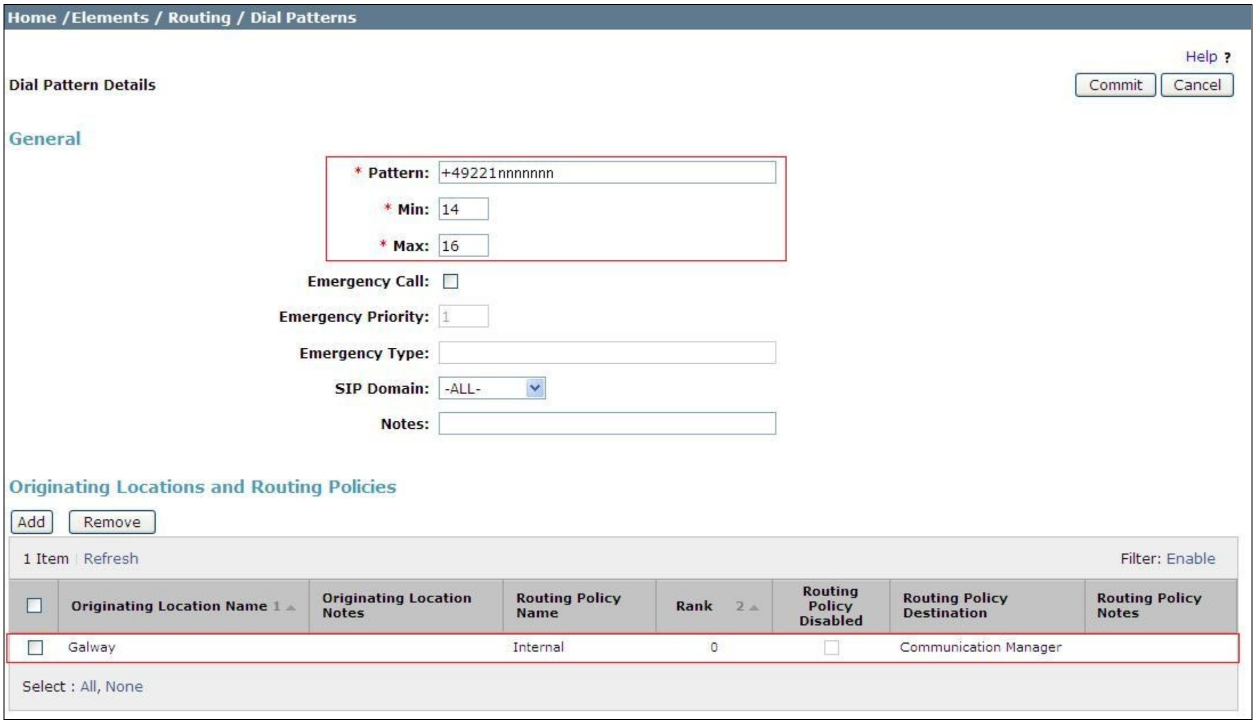
Under **General**:

- In the **Pattern** field enter a dialled number or prefix to be matched
- In the **Min** field enter the minimum length of the dialled number
- In the **Max** field enter the maximum length of the dialled number
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section 6.2**

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown), under **Originating Location** select **ALL** and under **Routing Policies** select one of the routing policies defined in **Section 6.6**, click **Select** button to save. The following screen shows an example dial pattern configured for the Session Border Controller which will route the calls out to the QSC VoIP Connect service.



The following screen shows the test dial pattern configured for Communication Manager. Note that the last seven digits are not shown.

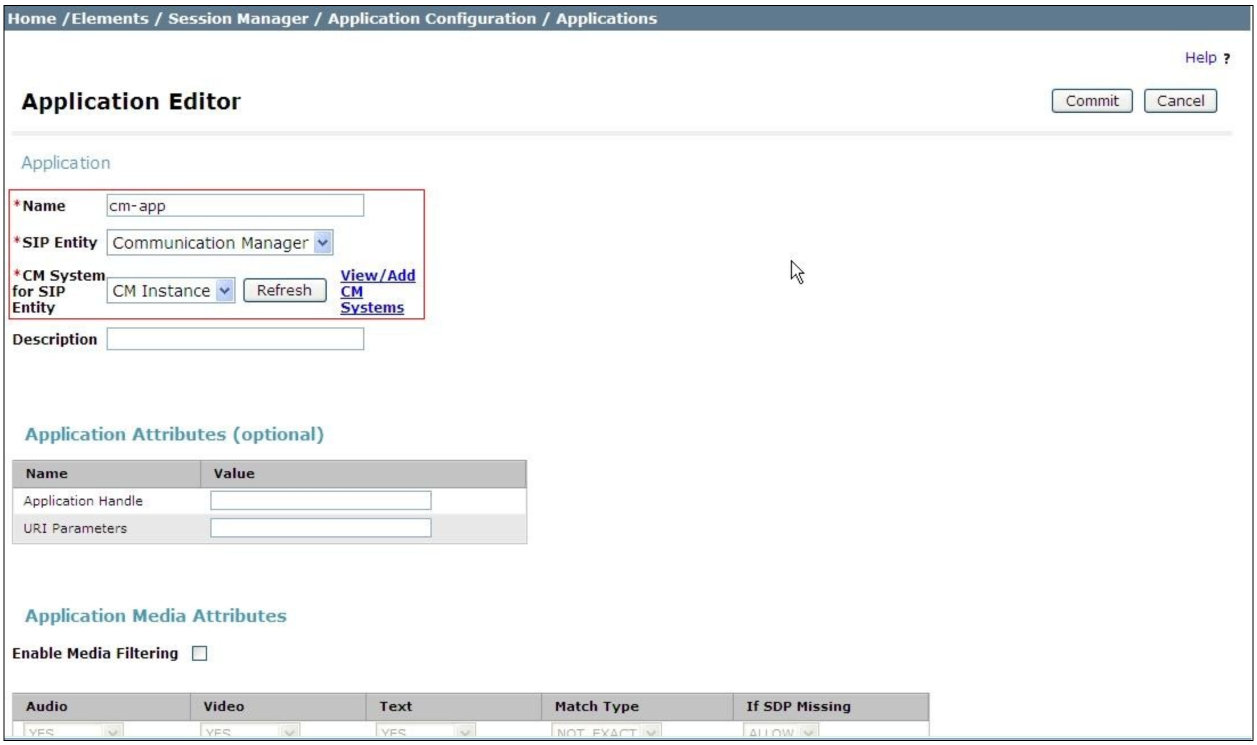


6.9. Administer Application for Avaya Aura® Communication Manager

From the home tab select **Session Manager** from the menu. In the resulting tab from the left panel menu select **Application Configuration → Applications** and click **New**.

- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for the Communication Manager
- In the **CM System for SIP Entity** field select the SIP entity for the Communication Manager

Select **Commit** to save the configuration.

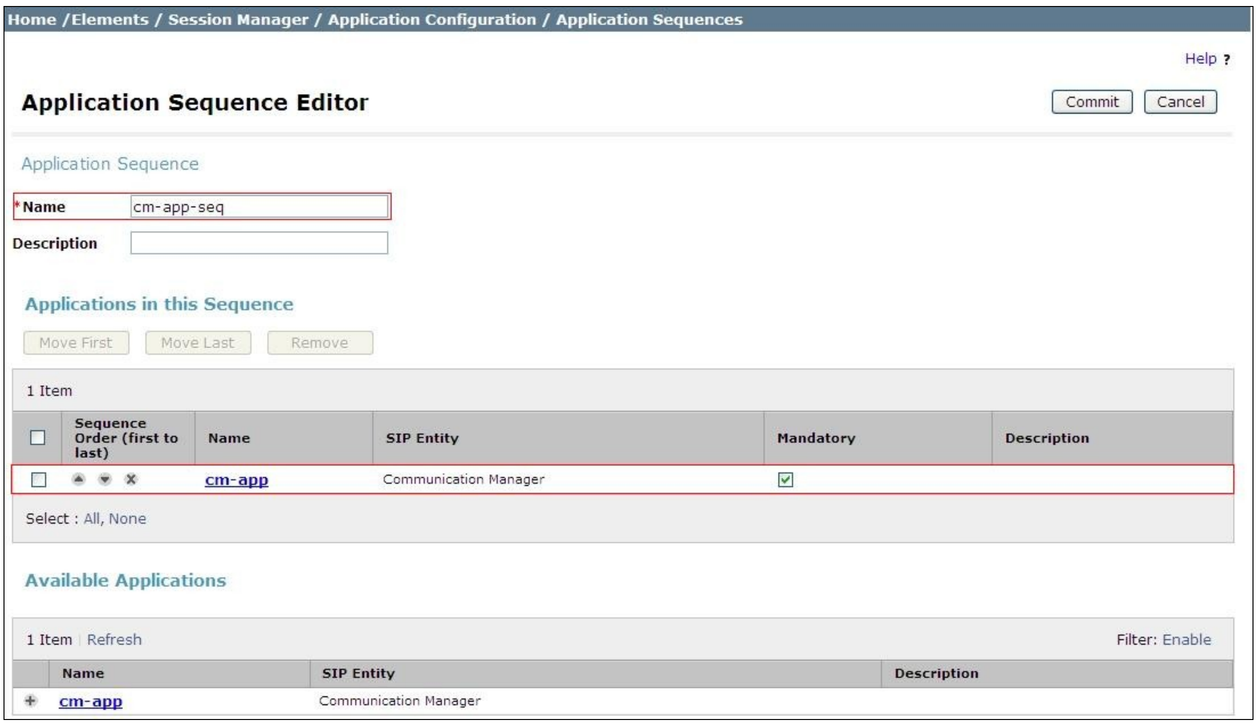


6.10. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Session Manager → Application Configuration → Application Sequences** and click on **New**.

- In the **Name** field enter a descriptive name
- Under **Available Applications**, click the + sign in front of the appropriate application instance. When the screen refreshes the application should be displayed under the **Applications in this Sequence** heading

Select **Commit**.

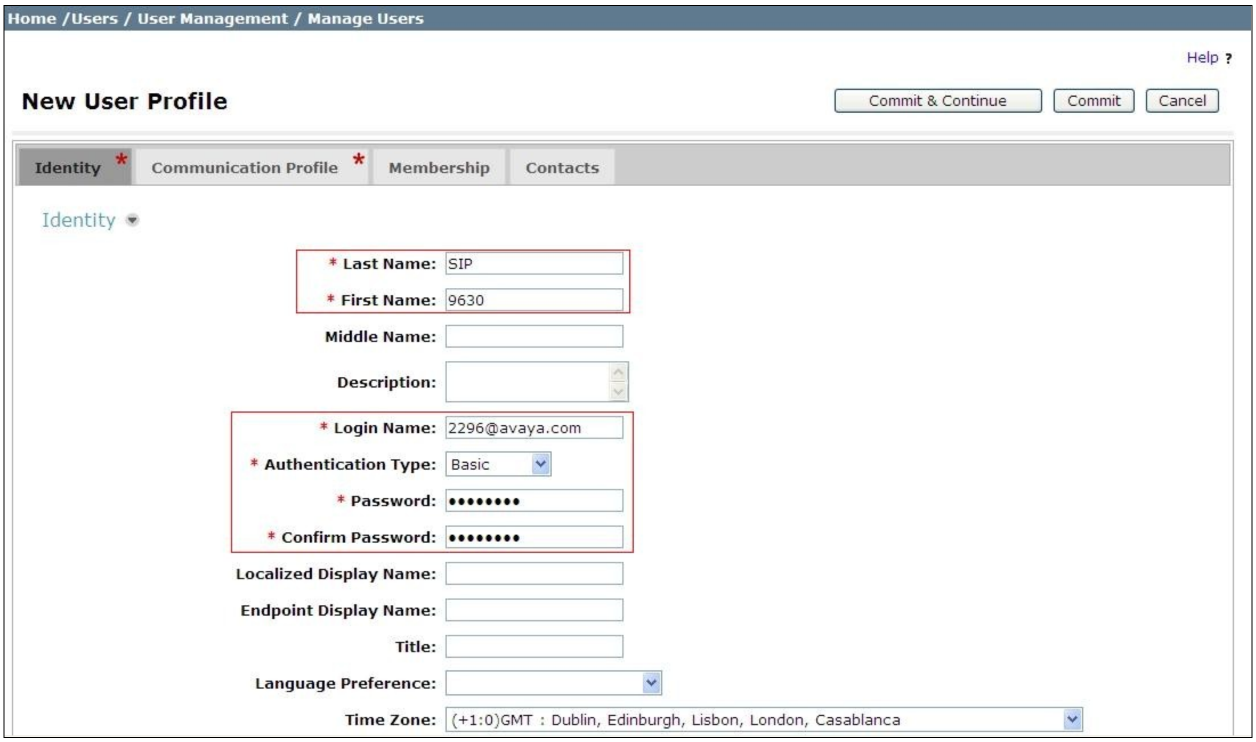


6.11. Administer SIP Extensions

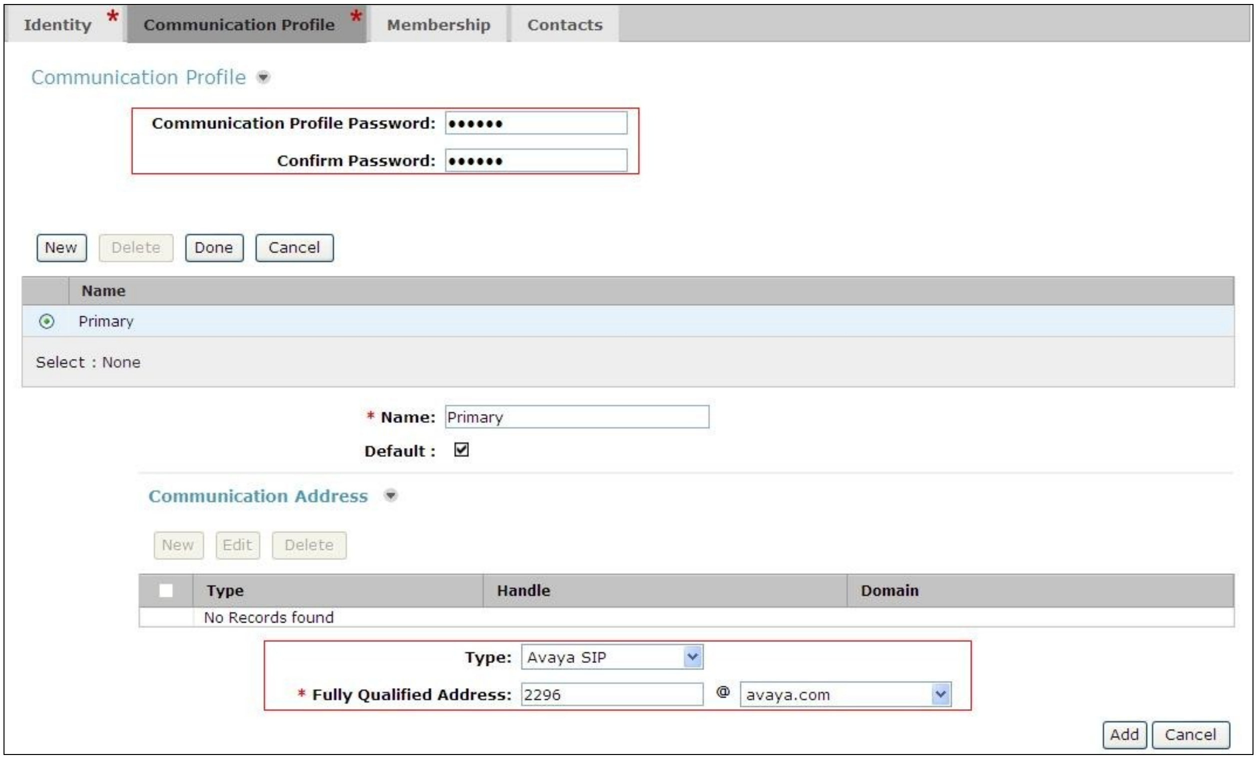
SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. From the Home tab select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of **user@domain** (e.g. **2296@avaya.com**) which is used to create the user's primary handle
- The **Authentication Type** should be **Basic**
- In the **Password/Confirm Password** fields enter an alphanumeric password

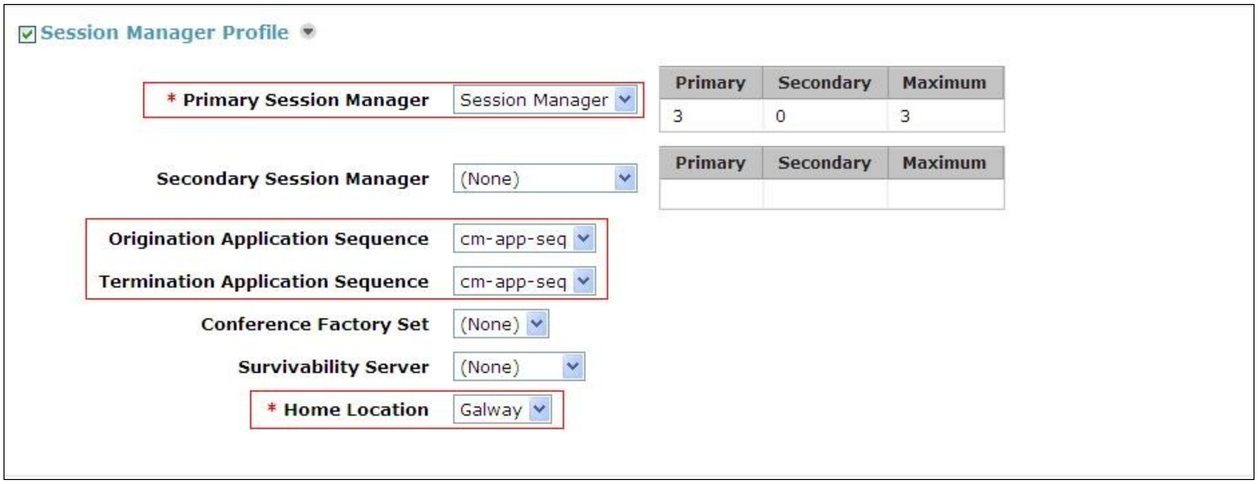


On the **Communication Profile** tab enter a numeric **Communication Profile Password** and confirm it, then expand the **Communication Address** section and click **New**. For the **Type** field select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.



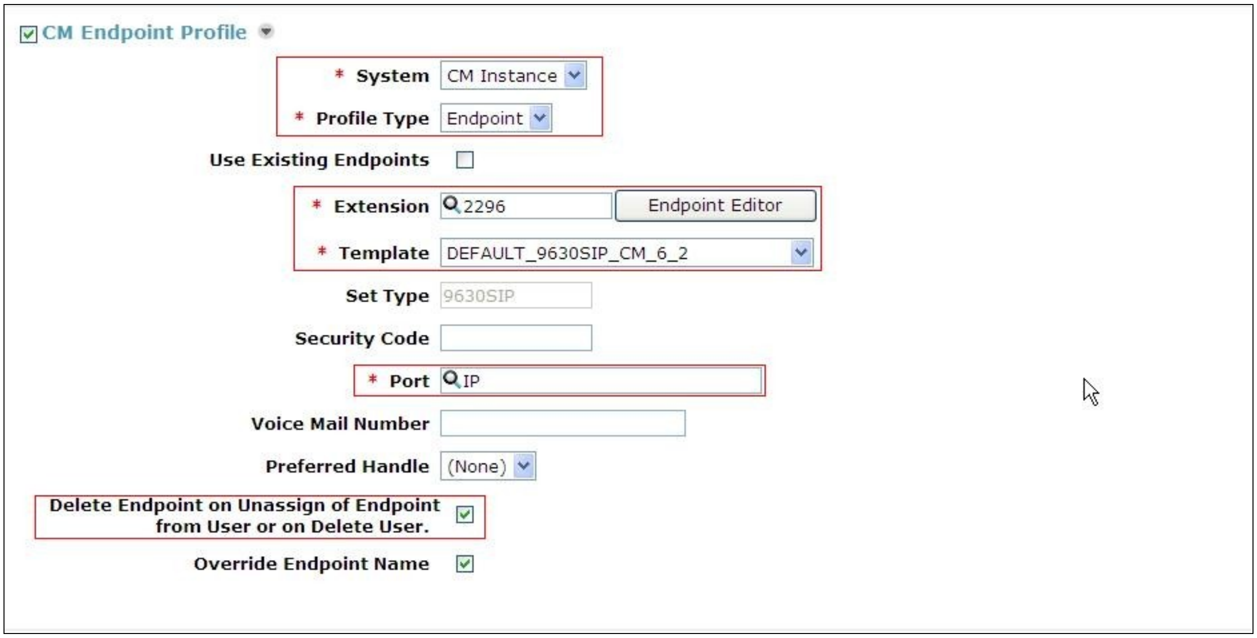
Expand the **Session Manager Profile** section.

- Make sure the **Session Manager** check box is checked
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field
- Select the appropriate application sequence from the drop-down menu in the **Origination Application Sequence** field configured in **Section 6.9**
- Select the appropriate application sequence from the drop-down menu in the **Termination Application Sequence** field configured in **Section 6.9**
- Select the appropriate location from the drop-down menu in the **Home Location** field



Expand the **Endpoint Profile** section.

- Select the Communication Manager SIP Entity from the **System** drop-down menu
- Select **Endpoint** from the drop-down menu for **Profile Type**
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- For the **Port** field select **IP**
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box
- Select **Commit** to save changes and the System Manager will add the Communication Manager user configuration automatically



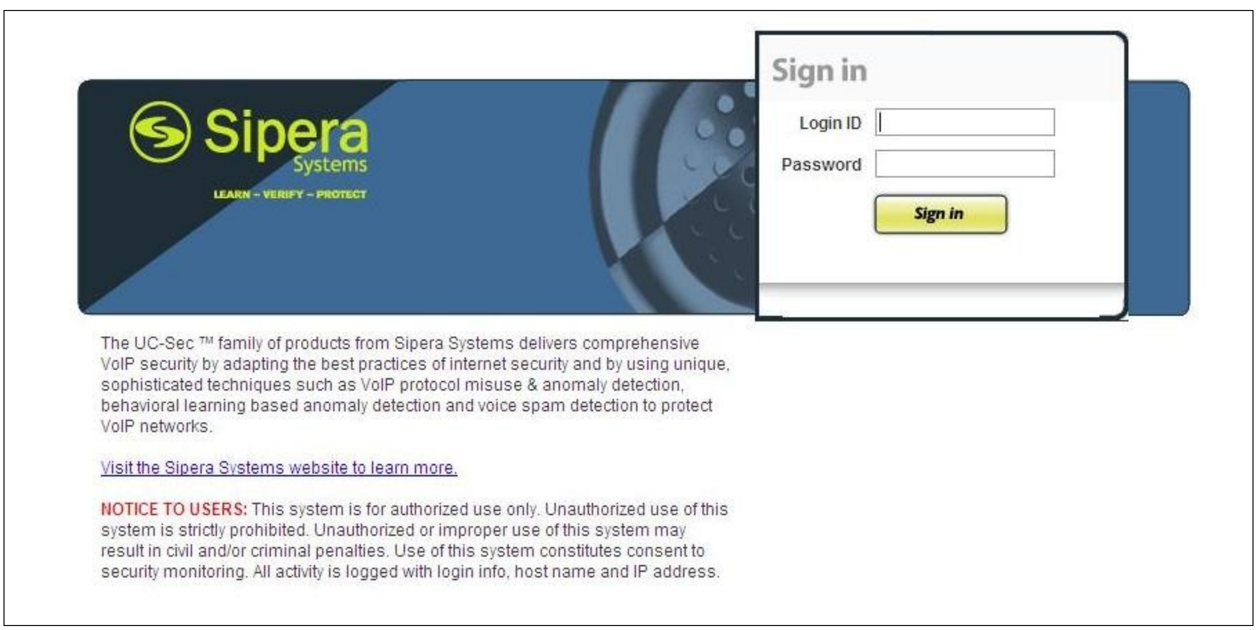
7. Configure Avaya Session Border Controller Advanced for Enterprise

This section describes the configuration of the Session Border Controller. At the time of writing the Avaya Session Border Controller Advanced for Enterprise was badged as the Sipera E-SBC (Enterprise Session Border Controller) developed for Unified Communications Security (UC-Sec). The Avaya Session Border Controller Advanced for Enterprise is administered using the E-SBC Control Center.

7.1. Access Avaya Session Border Controller Advanced for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. Select the **UC-Sec Control Center.**

Log in with the appropriate credentials.

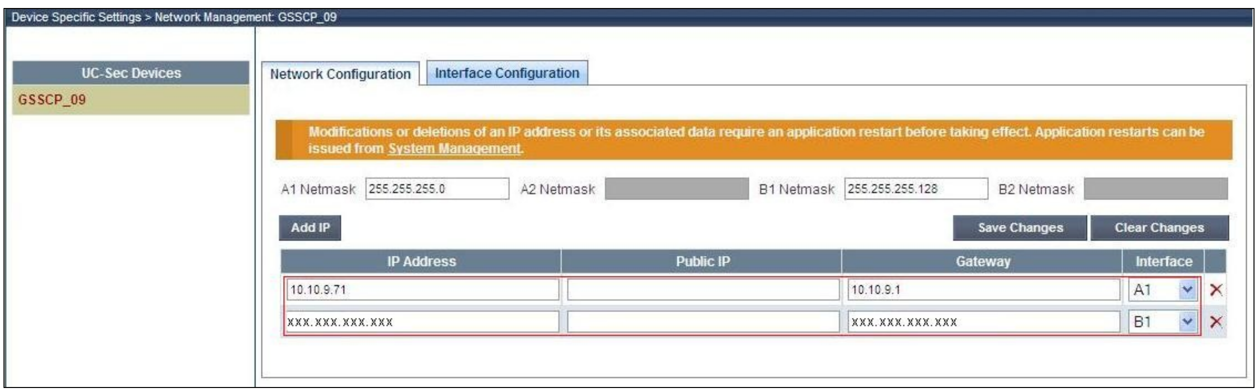


7.2. Define Network Information

Network information is required on the ASBCAE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the ASBCAE can have only one interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** in the **UC-Sec Control Center** menu on the left hand side and click on **Add IP**. Enter details in the blank box that appears at the end of the list

- Define the internal IP address with screening mask and assign to interface **A1**
- Select **Save** (not shown) to save the information
- Click on **Add IP**
- Define the external IP address with screening mask and assign to interface **B1**
- Select **Save** (not shown) to save the information
- Select the **Network Configuration** tab and change the state of interfaces **A1** and **B1** to **Enabled** (not shown)



- Click on **System Management** in the main menu
- Select **Restart Application** indicated by an icon in the status bar

7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

7.3.1. Signalling Interfaces

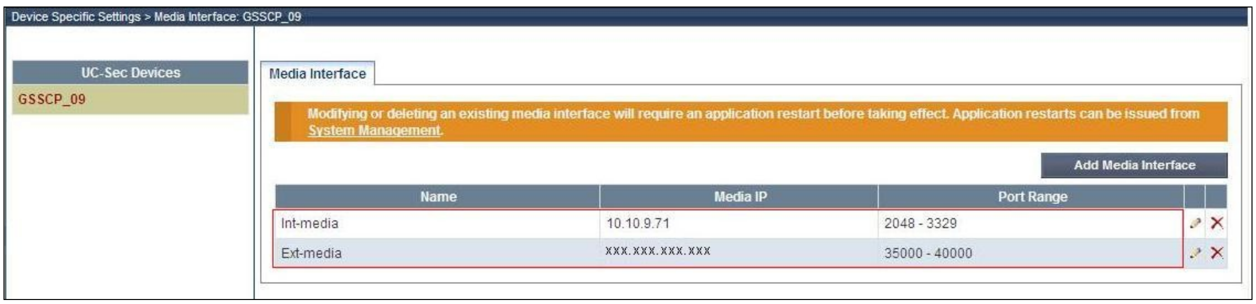
To define the signalling interfaces on the ASBCAE, navigate to **Device Specific Settings → Signalling Interface** in the **UC-Sec Control Center** menu on the left hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here

- Select **Add Signalling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal signalling interface
- Select an **internal** signalling interface IP address defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5060** is used for QSC
- Select **Add Signalling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external signalling interface
- Select an **external** signalling interface IP address (not shown) defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5060** is used for QSC

7.3.2. Media Interfaces

To define the media interfaces on the ASBCAE, navigate to **Device Specific Settings → Signalling Interface** in the **UC-Sec Control Center** menu on the left hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

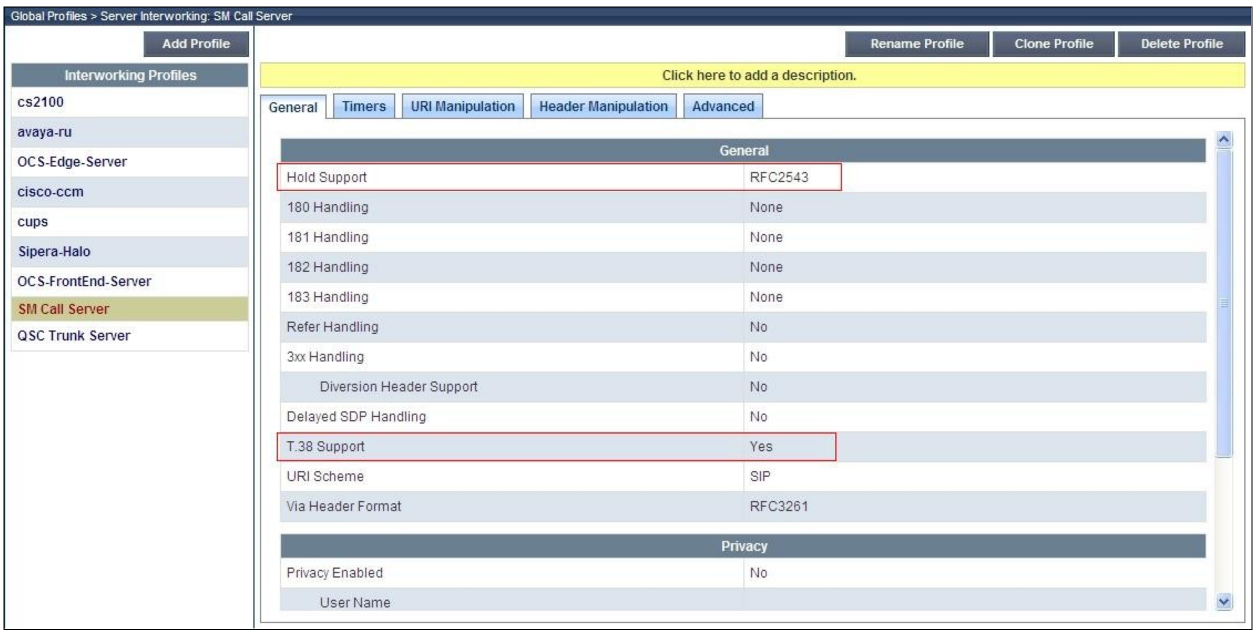
- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface
- Select an **internal** media interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the media path with the enterprise end-points
- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external media interface
- Select an **external** media interface IP address (not shown) defined in **Section 7.2**
- Select **RTP port** ranges for the media path with the QSC SBC



7.4. Define Server Interworking

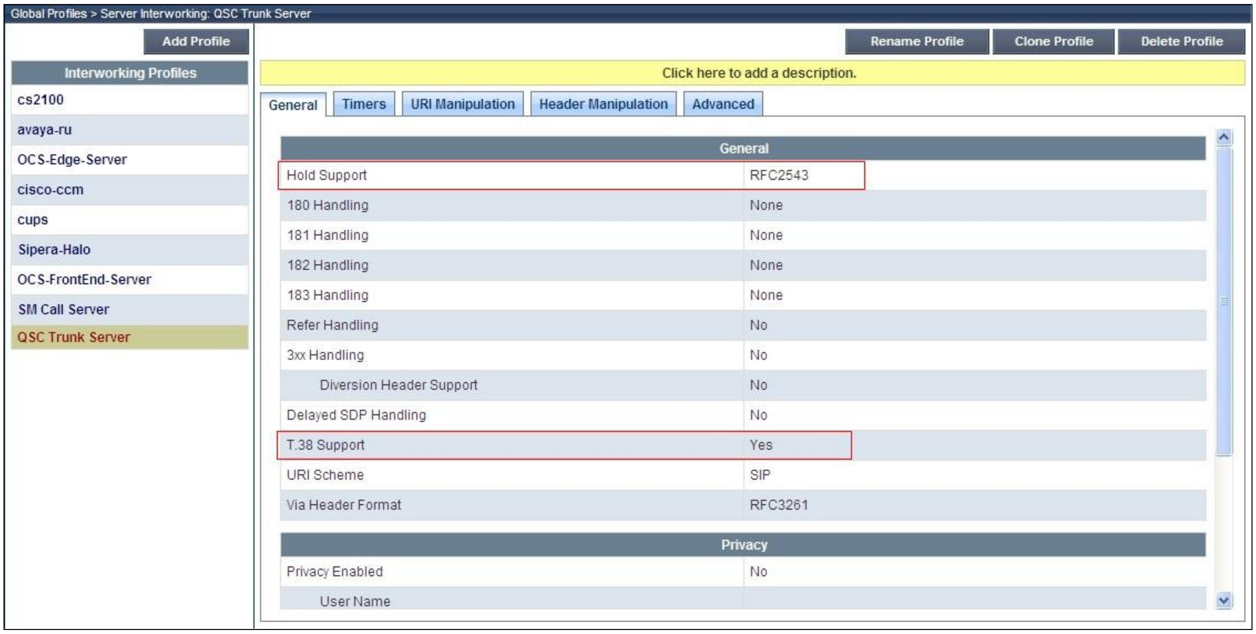
Server interworking is defined for each server connected to the ASBCAE. In this case, the QSC SBC is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define server interworking on the ASBCAE, navigate to **Global Profiles → Server interworking** in the **UC-Sec Control Center** menu on the left hand side. To define Server Interworking for the Session Manager, highlight the **avaya-ru** profile which is a factory setting appropriate for Avaya equipment and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile**

- In the **Clone Name** field enter a descriptive name for the Session Manager and click **Finish**
- Select **Edit** and enter details in the pop-up menu.
- Check the **T.38** box
- Change the **Hold Support** RFC to **RFC2543** then click **Next** and **Finish**



To define Server Interworking for the QSC SBC, highlight the previously defined profile for the Session Manager and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile**

- In the **Clone Name** field enter a descriptive name for server interworking profile for the QSC SBC and click **Finish**
- Select **Edit** and enter details in the pop-up menu
- Check the **T.38** box
- Select **Next** three times and **Finish**



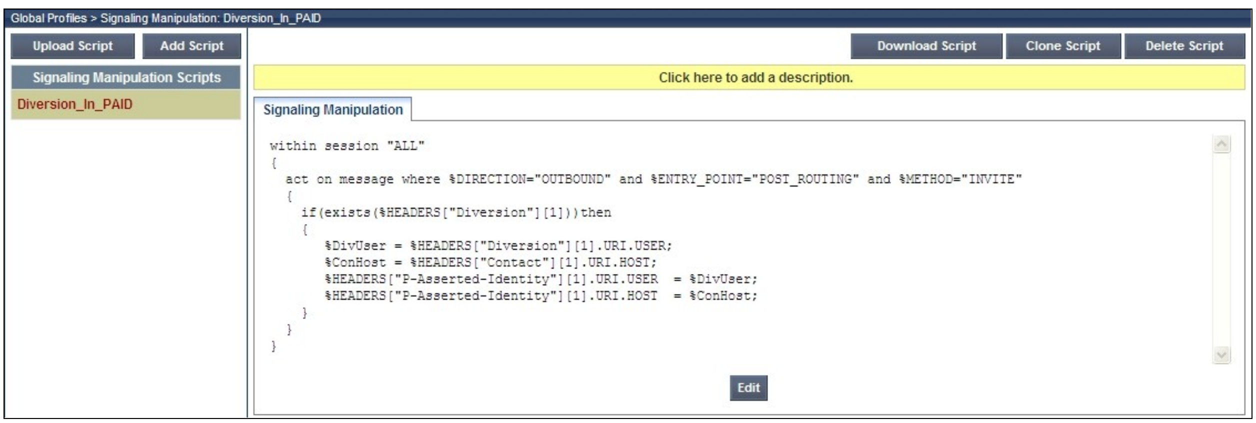
7.5. Define Signalling Manipulation

Signalling manipulation is required in some cases to ensure effective interworking. During test, some issues were found in the interworking between the QSC VoIP Connecting service and the enterprise. Two of these issues could not be resolved by other methods such as **Server Interworking** and **Signaling Rules.** The first issue is that call forwarding to a PSTN number could only be routed correctly when the CLI of the forwarding number was present in the P-Asserted-ID header. The second issue is that outgoing fax failed when G711 was presented as an alternative option in the SDP in the re-INVITE sent by the QSC network.

To define the signalling manipulation to take the user portion of the Diversion header and insert it into the P-Asserted-ID header, navigate to **Global Profiles → Signaling Manipulation** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Script** and enter a title and the script in the script editor. The title in the example is **Diversion_in_PAID**. The script text is as follows:

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and
%METHOD="INVITE"
  {
    if(exists(%HEADERS["Diversion"][1]))then
    {
       %DivUser = %HEADERS["Diversion"][1].URI.USER;
       %ConHost = %HEADERS["Contact"][1].URI.HOST;
       %HEADERS["P-Asserted-Identity"][1].URI.USER  = %DivUser;
       %HEADERS["P-Asserted-Identity"][1].URI.HOST  = %ConHost;
    }
  }
}
```

Once entered and saved, the script appears as shown in the following screenshot:



Note: This script relies on the existence of the Diversion header. This is included for the forwarded calls by configuration of the Communication Manager as described in **Section 5.6**

To define the signalling manipulation to remove the G.711 alternative from the SDP in the re-INVITE sent by the QSC network for outgoing fax, navigate to **Global Profiles → Signaling Manipulation** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Script** and enter a title and the script in the script editor. The script text is as follows:

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and
%METHOD="INVITE"
  {
   remove(%SDP[1]["s"]["m"][2]);
  }
}
```

Once entered and saved, the script appears as shown in the following screenshot:

Note: The above script removes all second sets of formats and attributes. During test with QSC, the only case where this occurred was in the re-INVITE for fax calls. For these calls, the first set of formats and attributes was for T.38, and the second was for G.711. This is applied where the re-INVITE is sent from the ASBCAE to the Session Manager.

7.6. Define Servers

Servers are defined for each server connected to the ASBCAE. In this case, the QSC SBC is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define the Session Manager, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- In the **Server Type** drop down menu, select **Call Server**
- In the **IP Addresses / Supported FQDNs** box, type the Session Manager SIP interface address which is the same as that defined on the Communication Manager in **Section 5.2**
- Check **TCP** and **UDP** in **Supported Transports**
- Define the **TCP** and **UDP** ports for SIP signalling, 5060 is used for QSC
- Click **Next** three times then select the **Interworking Profile** for the Session Manager defined in **Section 7.4** from the drop down menu
- Select the **G711_Alt_Removal Signaling Manipulation Script** defined in **Section 7.5** from the drop down menu and click **Finish**

The **General** tab on the resultant screen shows the **IP addresses**, **TCP Port** and **UDP Port** entered.

The **Advanced** tab on the resultant screen shows the **Interworking Profile** for the call server defined in **Section 7.4.**

To define the QSC SBC as a Trunk Server, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for the QSC SBC and click Next
- In the **Server Type** drop down menu, select **Trunk Server**
- In the **IP Addresses / Supported FQDNs** box, type the IP address of the QSC SBC (not shown)
- Check **TCP** and **UDP** in **Supported Transports**
- Define the **TCP** and **UDP** ports for SIP signaling, **5060** is used for QSC
- Click **Next** three times then select the **Interworking Profile** for the QSC SBC defined in **Section 7.4** from the drop down menu
- Select the **Diversion_In_PAID Signaling Manipulation Script** defined in **Section 7.5** from the drop down menu and click **Finish**

The **General** tab on the resultant screen shows the **IP addresses**, **TCP Port** and **UDP Port** entered.

The **Advanced** tab on the resultant screen shows the **Interworking Profile** for the trunk server defined in **Section 7.4.**

7.7. Define Routing

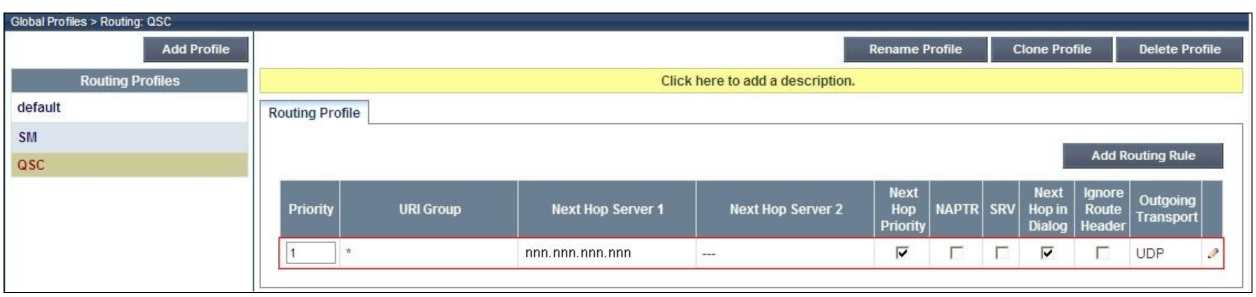
Routing information is required for routing to the Session Manager on the internal side and the QSC SBC on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used. To define routing to the Communication Manager, navigate to **Global Profiles → Routing** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- Enter the Session Manager SIP interface address and port in the **Next Hop Server 1** field
- Check the **Next Hop in Dialog** box
- Select **TCP** for the **Outgoing Transport**
- Click **Finish**

Note: Unless default port 5060 is used, this must be included in the next hop IP address.

To define routing to the QSC SBC, navigate to **Global Profiles Routing** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the QSC SBC and click **Next**
- Enter the QSC SBC IP address and port in the **Next Hop Server 1** field
- Check the **Next Hop in Dialog** box
- Select **UDP** for the **Outgoing Transport**
- Click **Finish**



7.8. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten or next hop IP addresses can be used. As IP addressing was used in test instead of domain names, there was little requirement for topology hiding. IP addresses are translated to the ASBCAE external addresses using NAT. To define Topology Hiding for the Session Manager, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- If the required Header is not shown, click on **Add Header**
- Select **Request-Line** as the required header from the **Header** drop down menu
- Select the required action from the **Replace Action** drop down menu, **Next Hop** was used for test

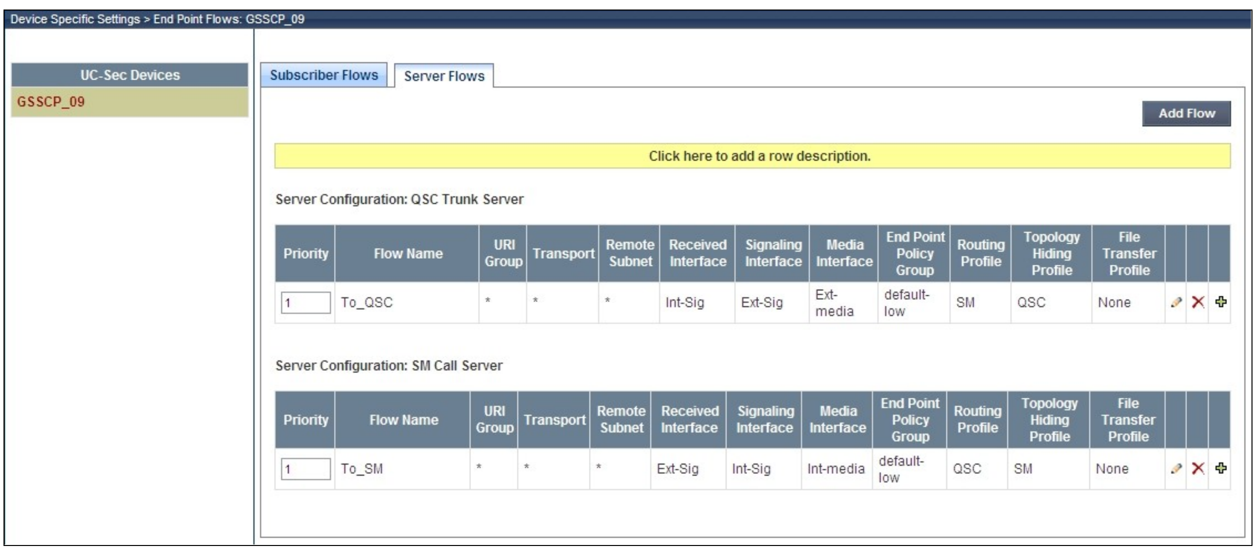
Note: The use of **Next Hop** results in the IP address being inserted in the host portion of the Request-URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used for the **Request-Line** header with the required domain names entered in the **Overwrite Value** field. Different domain names could be used for the enterprise and the QSC network.

To define Topology Hiding for the QSC SBC, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the QSC SBC and click **Next**
- If the required Header is not shown, click on **Add Header**
- Select **Request-Line** as the required header from the **Header** drop down menu
- Select the required action from the **Replace Action** drop down menu, **Next Hop** was used for test

7.9. Server Flows

Server Flows combine the previously defined profiles into an outgoing flow from the Session Manager to the QSC SBC and an incoming flow from the QSC SBC to the Session Manager. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to the QSC SBC and vice versa. The information for all Server Flows is shown on a single screen on the ASBCAE.



To define an outgoing Server Flow, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the outgoing server flow to the QSC SBC
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**
- In the **Signalling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.7**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the QSC SBC defined in **Section 7.8** and click **Finish**

Server Configuration: QSC Trunk Server

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	To_QSC	*	*	*	Int-Sig	Ext-Sig	Ext-media	default-low	SM	QSC	None			

An incoming Server Flow is defined as a reversal of the outgoing Server Flow

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the incoming server flow to the Session Manager
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**
- In the **Signalling Interface** drop-down menu, select the internal SIP signalling defined in **Section 7.3**
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**
- In the **Routing Profile** drop-down menu, select the routing profile of the QSC SBC defined in **Section 7.7**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.8** and click **Finish**

Server Configuration: SM Call Server

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	To_SM	*	*	*	Ext-Sig	Int-Sig	Int-media	default-low	QSC	SM	None			

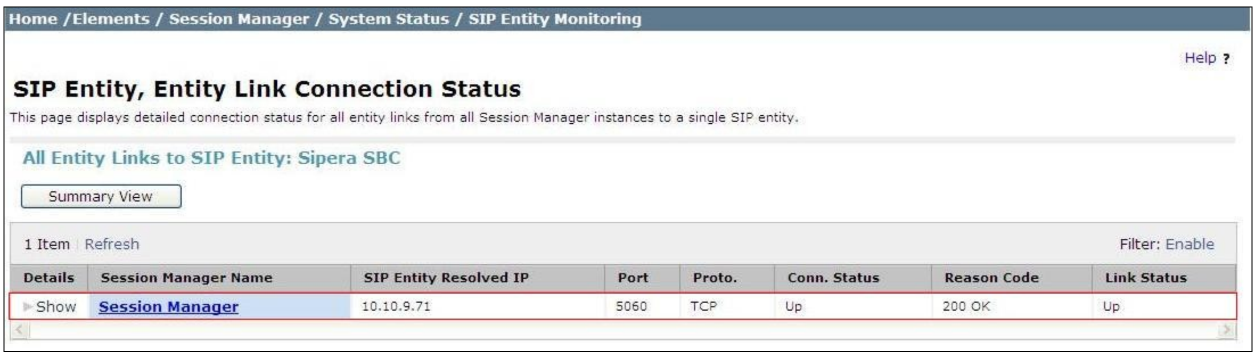
8. Service Provider Configuration

The configuration of the QSC equipment used to support the QSC VoIP Connecting service is outside of the scope of these Application Notes and will not be covered. To obtain further information on QSC equipment and system configuration please contact an authorised QSC representative.

9. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

1. From System Manager Home Tab click on Session Manager and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.



2. From the Communication Manager SAT interface run the command **status trunk n** where **n** is a previously configured SIP trunk. Observe if all channels on the trunk group display **in-service/idle**.

```
status trunk 1

                              TRUNK GROUP STATUS

Member    Port     Service State       Mtce Connected Ports
                                       Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
0001/005 T00005   in-service/idle    no
0001/006 T00006   in-service/idle    no
0001/007 T00007   in-service/idle    no
0001/008 T00008   in-service/idle    no
0001/009 T00009   in-service/idle    no
0001/010 T00010   in-service/idle    no
```

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.

4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller Advanced for Enterprise to QSC VoIP Connect Service. The service was successfully tested with a number of observations listed in **Section 2.2**. In a number of cases, configuration of the Avaya Session Border Controller Advanced for Enterprise is required to ensure effective interworking between the enterprise equipment and the network.

11. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Installing and Configuring Avaya Aura® System Platform Release 6.2,* March 2012.
[2] *Administering Avaya Aura® System Platform Release 6.2,* February 2012.
[3] *Administering Avaya Aura® Communication Manager*, Release 6.2, February 2012.
[4] *Avaya Aura® Communication Manager Feature Description and Implementation*, February 2012, Document Number 555-245-205.
[5] *Implementing Avaya Aura® System Manager Release 6.2*, March 2012.
[6] *Implementing Avaya Aura® Session Manager*, February 2012, Document Number 03-603473
[7] *Administering Avaya Aura® Session Manager*, February 2012, Document Number 03-603324.
[8] *Various Application Notes for the Avaya Session Border Controller Advanced for Enterprise*, March 2012
[9] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/

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.