Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.0.1 as an Evolution Server, Avaya Aura® Session Manager R6.1 and Avaya Session Border Controller Advanced for Enterprise to support KPN VoIP Connect Service – Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the KPN 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. KPN 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.

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between KPN 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 Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with KPN 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 VoIP Connect service provided by KPN.

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 KPN
- Incoming PSTN calls made to SIP, H.323 and Digital telephones at the enterprise
- Outgoing calls from the enterprise site completed via KPN to PSTN destinations
- Outgoing calls from the enterprise to the PSTN made from SIP, H.323 and Analogue telephones
- Calls using the G.711A codec
- 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 KPN requiring Avaya response and sent by Avaya requiring KPN response

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the KPN 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
- RTP Payload Type negotiation for DTMF on outgoing calls from a SIP phone failed, change of PT to 101 on the phone was required
- Exact number lengths were used in the dial plan to avoid transmission of a DTMF "#" from the enterprise after call set-up
- Outgoing fax calls were failing before transmission was complete due to possible network issue

2.3. Support

For technical support on KPN products please visit the website at www.kpn.nl or contact an authorized KPN representative.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the KPN 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.

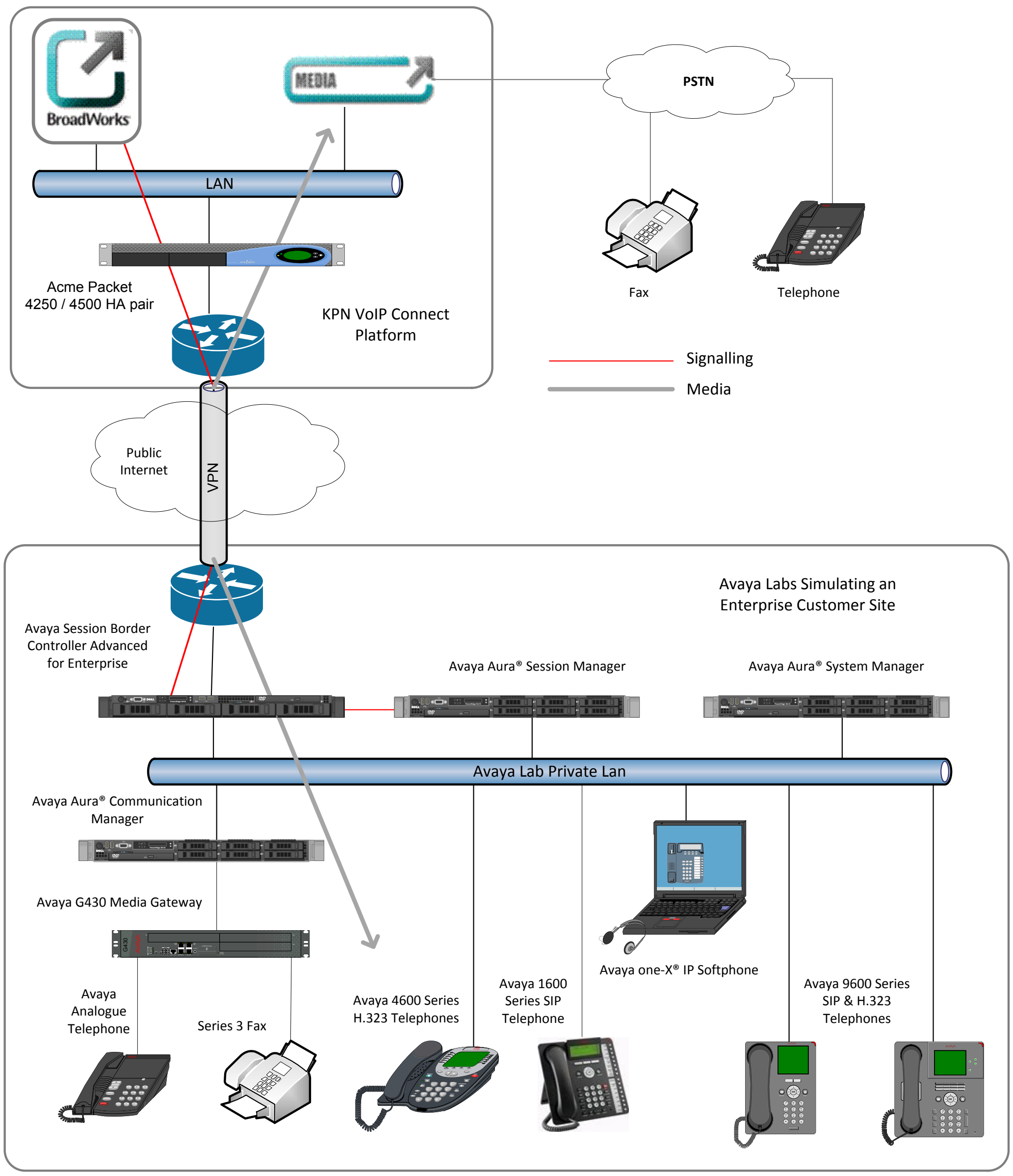


Figure 1: Test Setup KPN VoIP Connect to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server running Communication Manager	Avaya Aura® Communication Manager R6.0.1 (R016x.00.1.510.1) Service Pack 19303 (System Platform 6.0.3.3.3)
Avaya G430 Media Gateway	FW 30.12.1
Avaya S8800 Server running Session Manager	Avaya Aura® Session Manager R6.1 (6.1.5.0.615006)
Avaya S8800 Server running System Manager	Avaya Aura® System Manager R6.1 (System Platform 6.0.3.1.3, Template 6.1.5.0)
Avaya Session Border Controller Advanced for Enterprise Server	Avaya Session Border Controller Advanced for Enterprise 4.0.5.Q02
Avaya 1616 Phone (H.323)	1.22
Avaya 4621 Phone (H.323)	2.901
Avaya 9670 Phone (H.323)	2.0
Avaya 9601 Phone (SIP)	R6.1 SP3
Avaya one–X® Communicator (H.323)	Avaya one–X® Communicator 6.0.1.16-SP1-25226
Analogue Phone	N/A
KPN Equipment	**Software**
IP Multimedia Subsystem	BroadSoft Broadworks version 11
SIP User Agent	Alcatel-Lucent HPSS v3.0.3
SBC	Acme Packet 4250 and 4500

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 KPN VoIP Connect Service. For incoming calls, the Session Manager receives SIP messages from the SBC 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 signaling 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 KPN 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 KPN 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 10
  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
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 Session Border Controller Advanced for Enterprise.
- 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 codec supported by KPN was configured, namely **G.711A**. The **G.726A-32K** and **G.729A** codec's were also specified to ensure correct codec negotiation between KPN and the enterprise site.

```
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.711A           n          2        20
 2: G.726A-32K       n          2        20
 3: G.729A           n          2        20
```

The KPN 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         0
    Modem           off                   0
    TDD/TTY         US                    3
    Clear-channel   n                     0
```

5.5. Administer SIP Signaling Groups

This signaling group (and trunk group) will be used for inbound and outbound PSTN calls to the KPN 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 (recommended 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 signaling group as network region **1**)
- Leave **Far-end Domain** blank (removes the analysis of the far end domain name and subsequent handling of multiple signaling 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)

The default values for the other fields may be used.

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

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                                SIP Enabled LSP? 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 **tie**
- Specify the signaling 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: 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 KPN to prevent unnecessary SIP messages during call setup. Also note that the value for **Redirect On OPTIM Failure** can be increased to allow additional set-up time for calls destined for an EC500 destination.

```
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
```

On **Page 3,** set the **Numbering Format** field to **public.**

```
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,** set the **Network Call Redirection** to **y.** Note that during test, this was only set for the User to User Information test. For all other tests it was set to n.

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

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? y
                    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
                             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 KPN 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 screenshot has been changed to show an example, rather than the real DDI range.

```
change public-unknown-numbering 0                                    Page   1 of   2
                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                  Total Administered: 5
 4  2291          1         31201234560     11       Maximum Entries: 9999
 4  2296          1         31201234561     11
 4  2316          1         31201234562     11    Note: If an entry applies to
 4  2346          1         31201234563     11    a SIP connection to Avaya
 4  2396          1         31201234564     11    Aura(tm) Session Manager,
                                                  the resulting number must
                                                  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 KPN 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 have been used as it was found during test that a greater value resulted in transmission of a DTMF “#” after establishment of the media stream. Calls are sent to route pattern **1**.

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

          Dialed           Total      Route     Call   Node  ANI
          String          Min  Max  Pattern     Type   Num   Reqd
    0                     8    14     1         pubu         n
    00                    13   13     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**.

```
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                                unk-unk   none
 2: 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 KPN can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DDI numbers provided by KPN correlate to the internal extensions assigned within Communication Manager. The entries displayed below translate incoming DDI numbers 0201234560-02012345679 to a 4 digit extension by deleting all of the incoming digits and inserting an extension. Note that the numbers used are an example.

```
change inc-call-handling-trmt trunk-group 1                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 tie             10 0201234560       all 2396
 tie             10 0201234561       all 2346
 tie             10 0201234562       all 2296
 tie             10 0201234563       all 2291
 tie             10 0201234564       all 2316
 tie             10 0201234565       all 6101
 tie             10 0201234566       all 2000
 tie             10 0201234567       all 2400
 tie             10 0201234568       all 6102
 tie             10 0201234569       all 2501
 tie
 tie
 tie
```

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. **00353867899999**)
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing
- Set the **Config Set** to **1**

Other parameters can retain default value

```
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         -     00353867899999   1          1
                                -
```

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

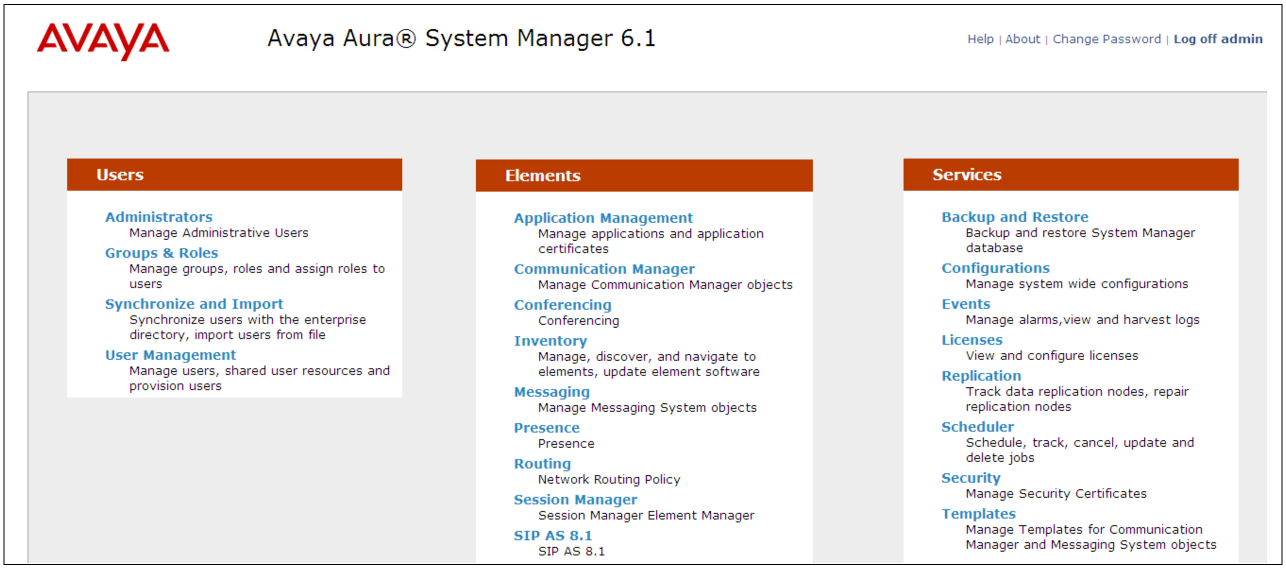
6. Configuring Avaya Aura® Session Manager

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

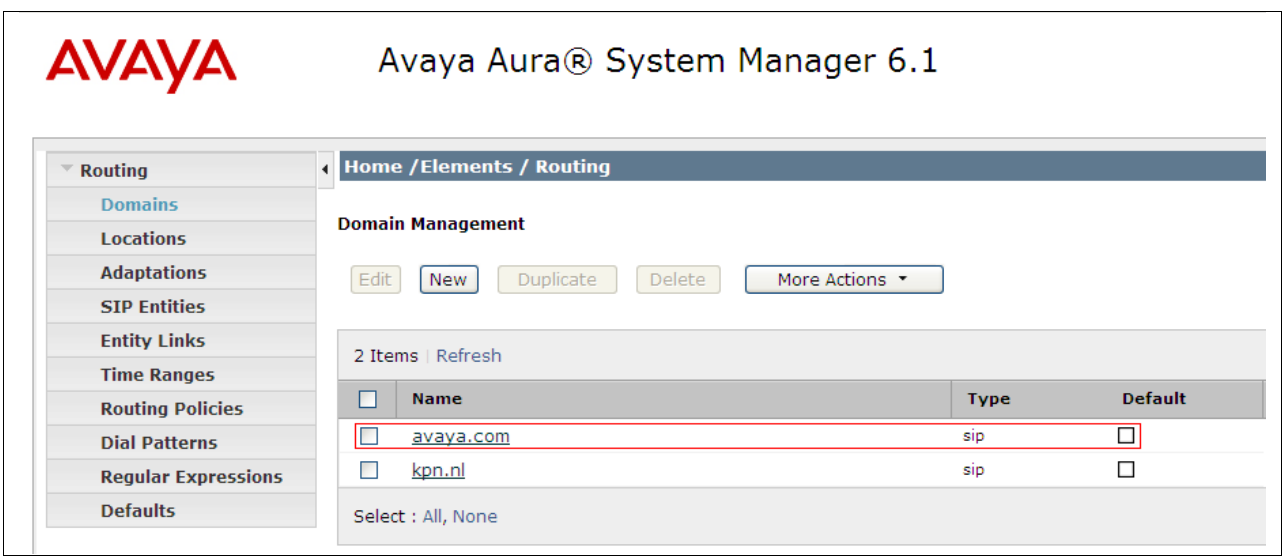
6.1. Log in to Avaya Aura® System Manager

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.



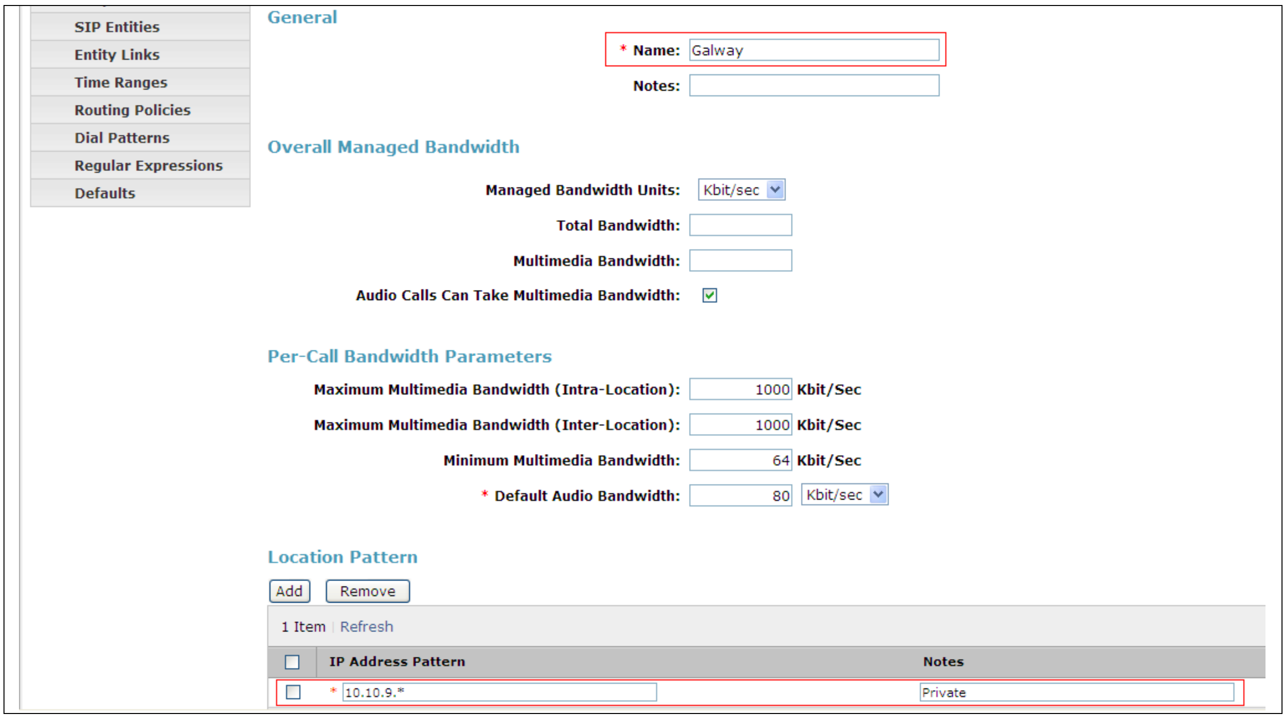
6.2. Administer SIP Domain

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 in this sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu [not shown]. 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.

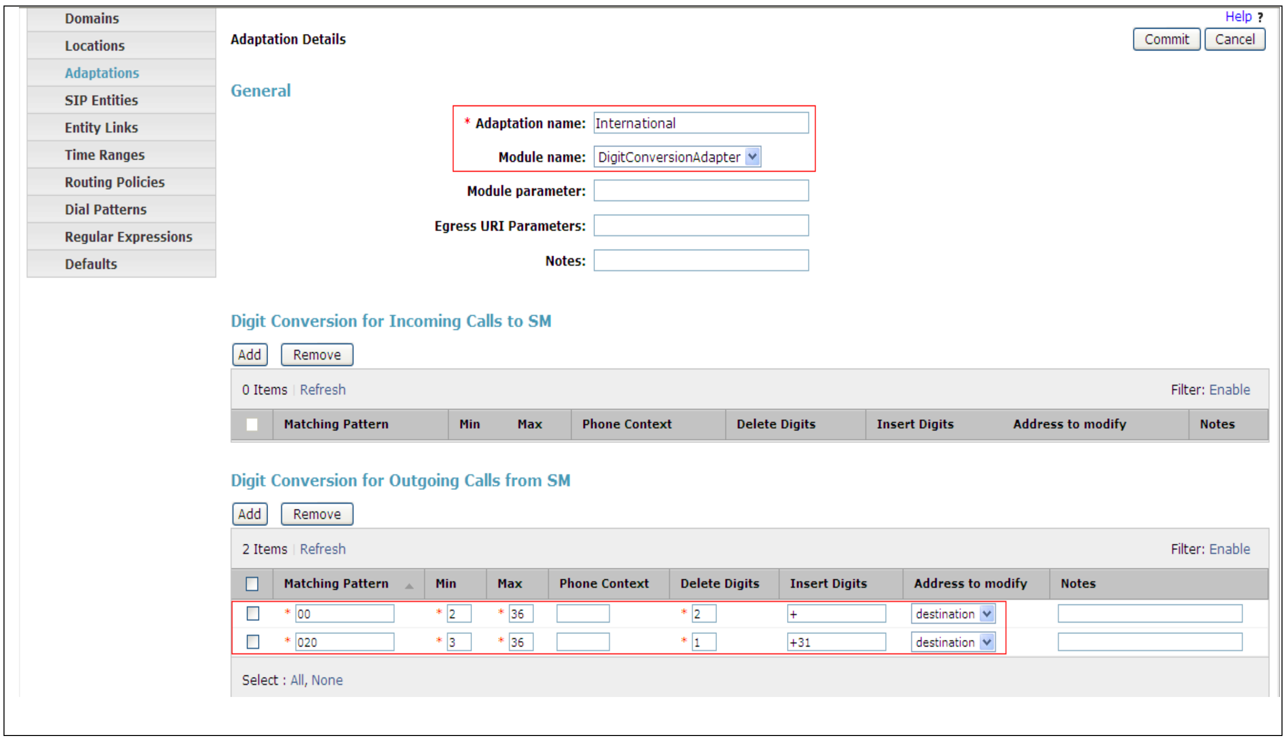


6.4. Administer Adaptations

Adaptations can be used to modify the called party number to meet network requirements. The example shown was used in this test to convert the called number to E.164 format. The module **DigitConversionAdaptor** is used to convert numbers in the following way:

- International Numbers – remove the international dialing prefix (00) and replace with a "+"
- National Numbers – remove the leading zero and replace with a "+" followed by the country code

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:**

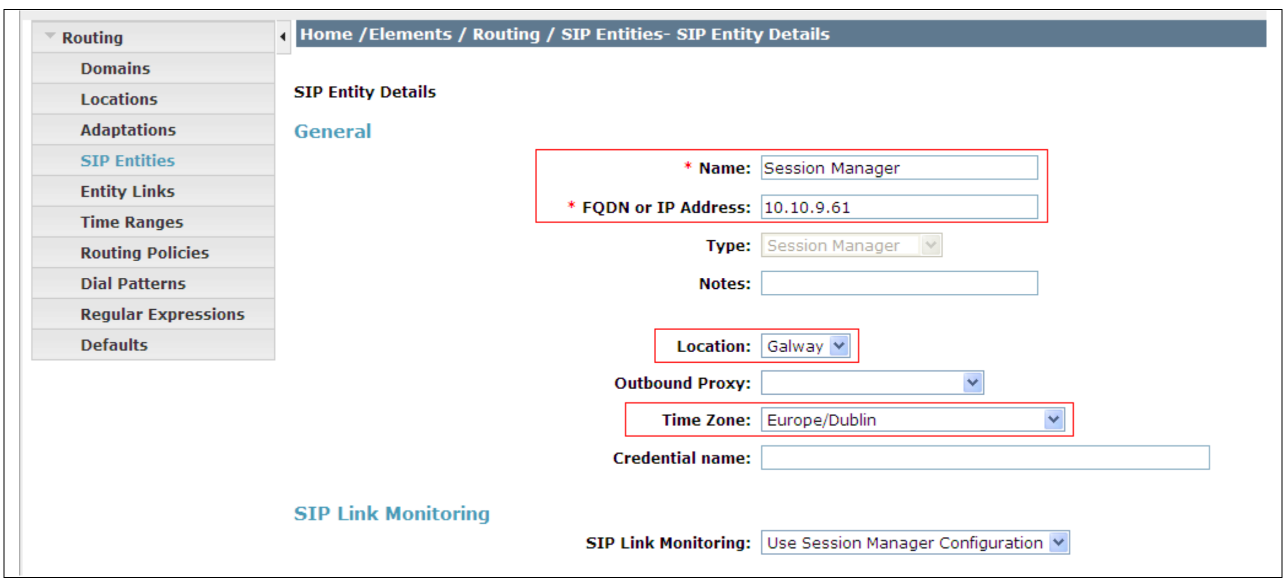
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **Gateway** for the Session Border Controller SIP entity
- In the **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

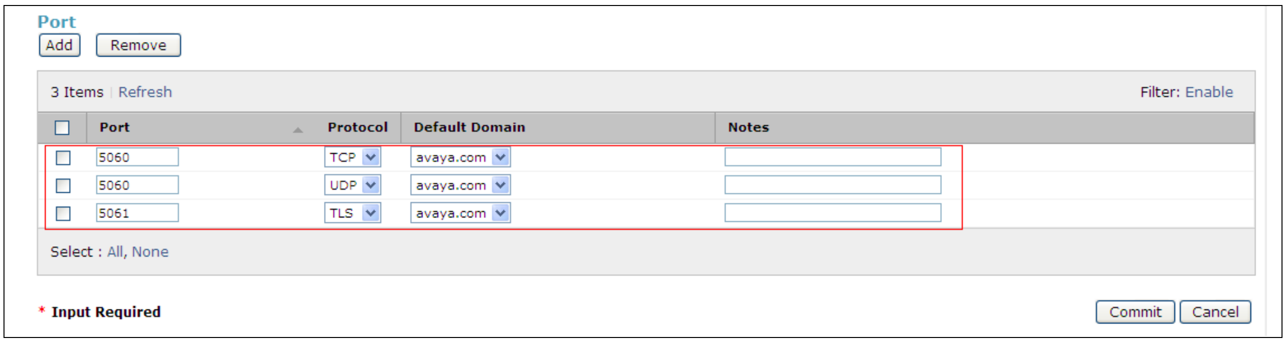
6.5.1. Avaya Aura® Session Manager SIP Entity

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.



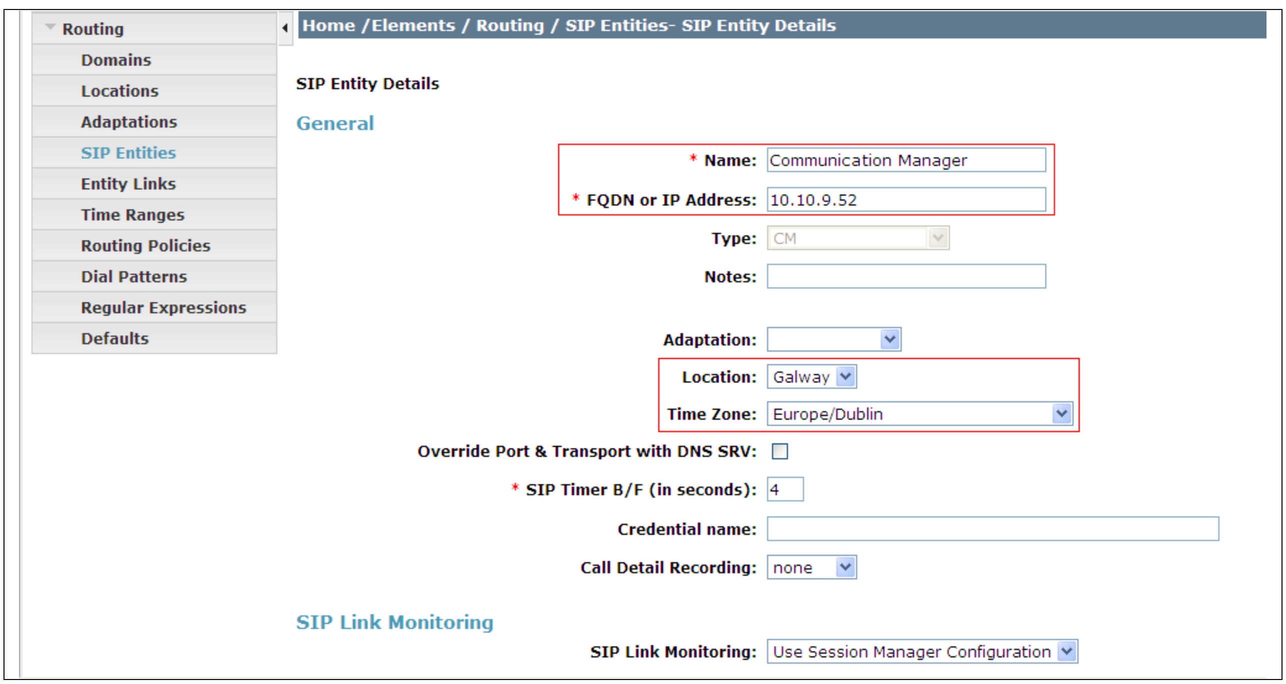
The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add,** then edit the fields in the resulting new row.

- 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
- Click **Commit**.



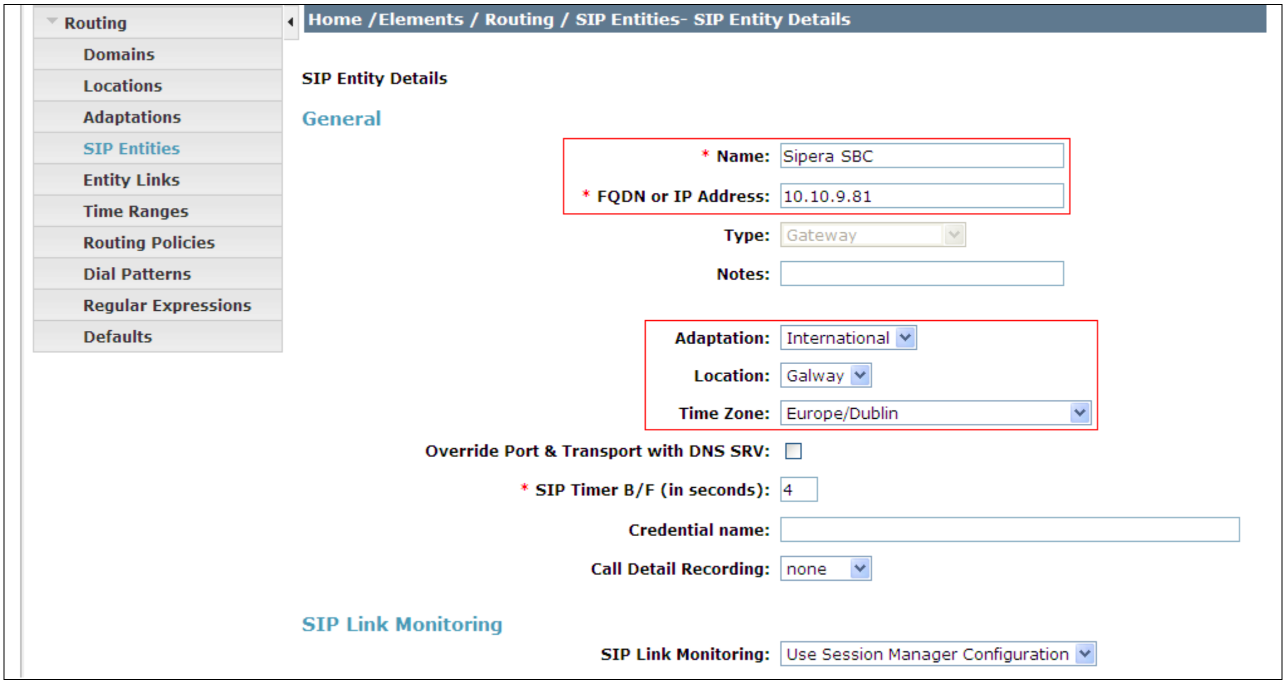
6.5.2. Avaya Aura® Communication Manager SIP Entity

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 (see **Figure 1**).

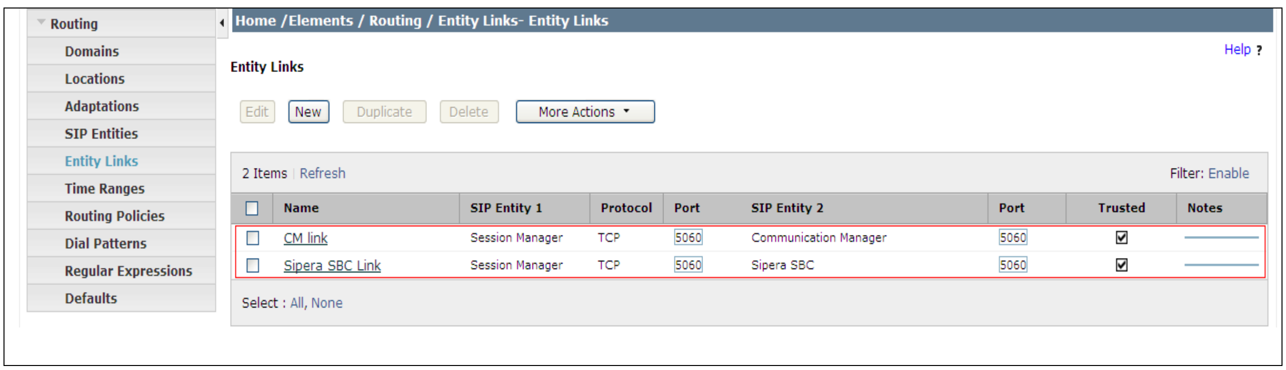


6.6. Administer Entity Links

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.



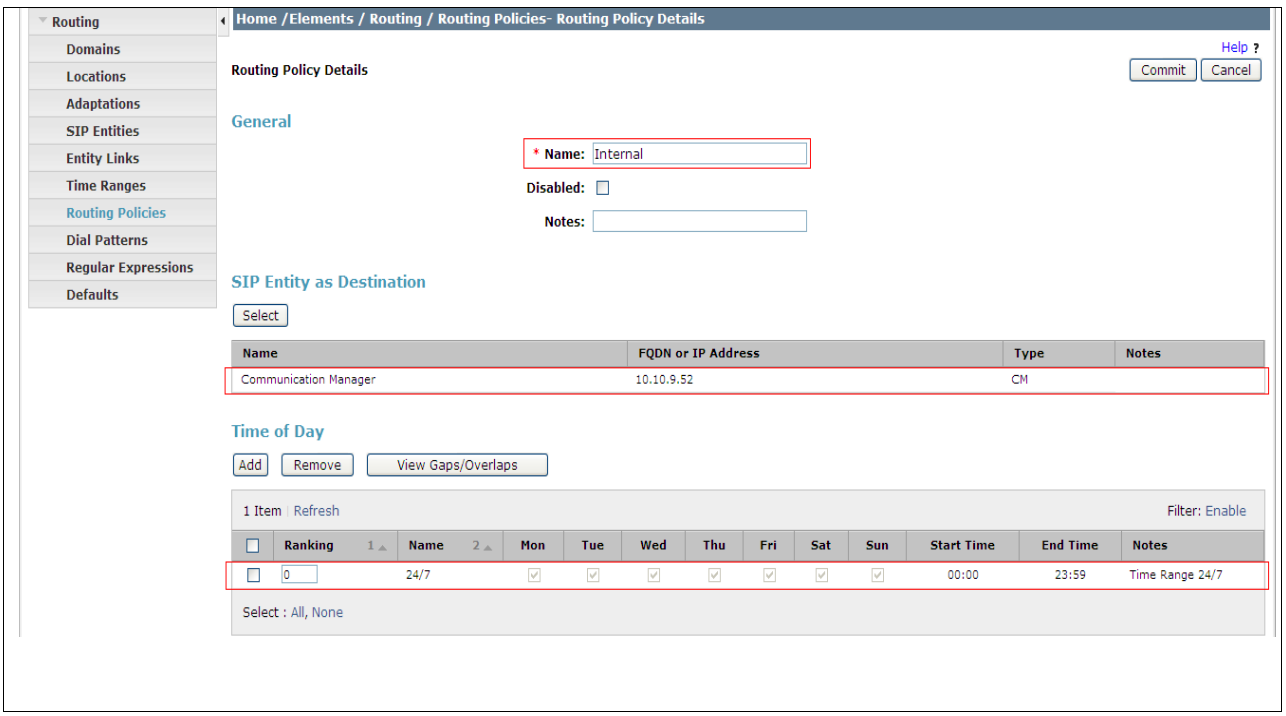
6.7. Administer Routing Policies

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).

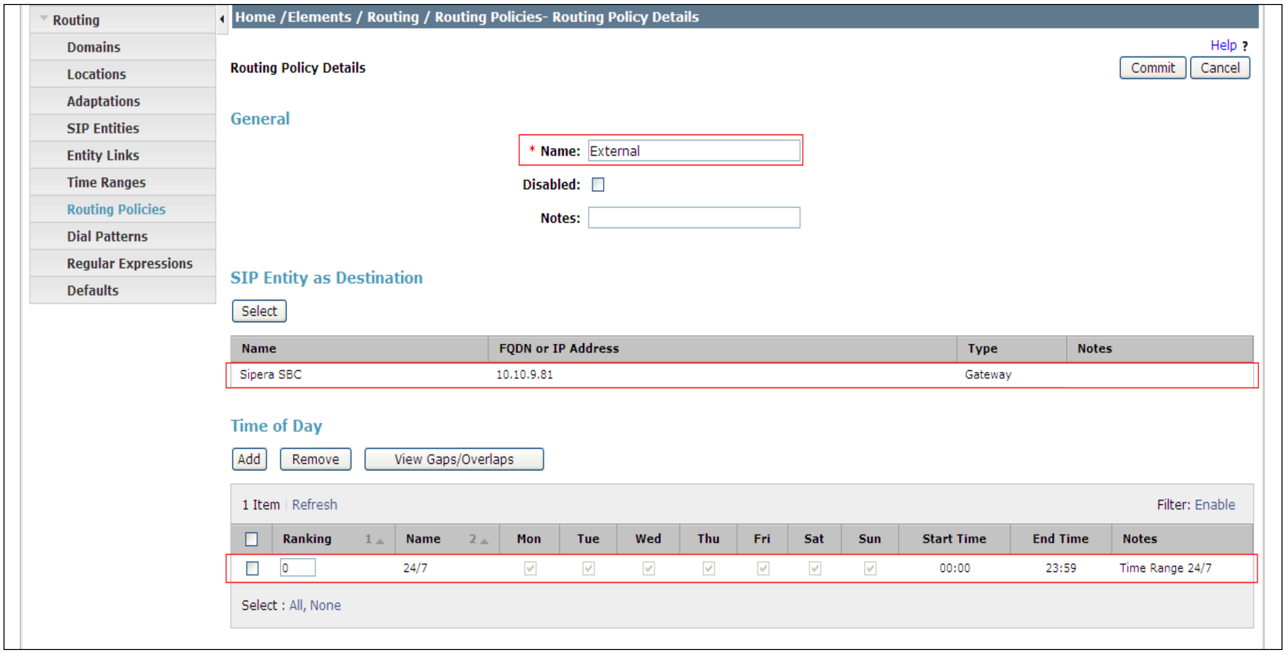
Under **General:**

- Enter an informative name in the **Name** field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity from the pop-up window (not shown) to which this routing policy applies
- Under **Time of Day**, click **Add**, and then select the default **24/7** or a previously created time range if required

The following screen shows the routing policy for Communication Manager



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



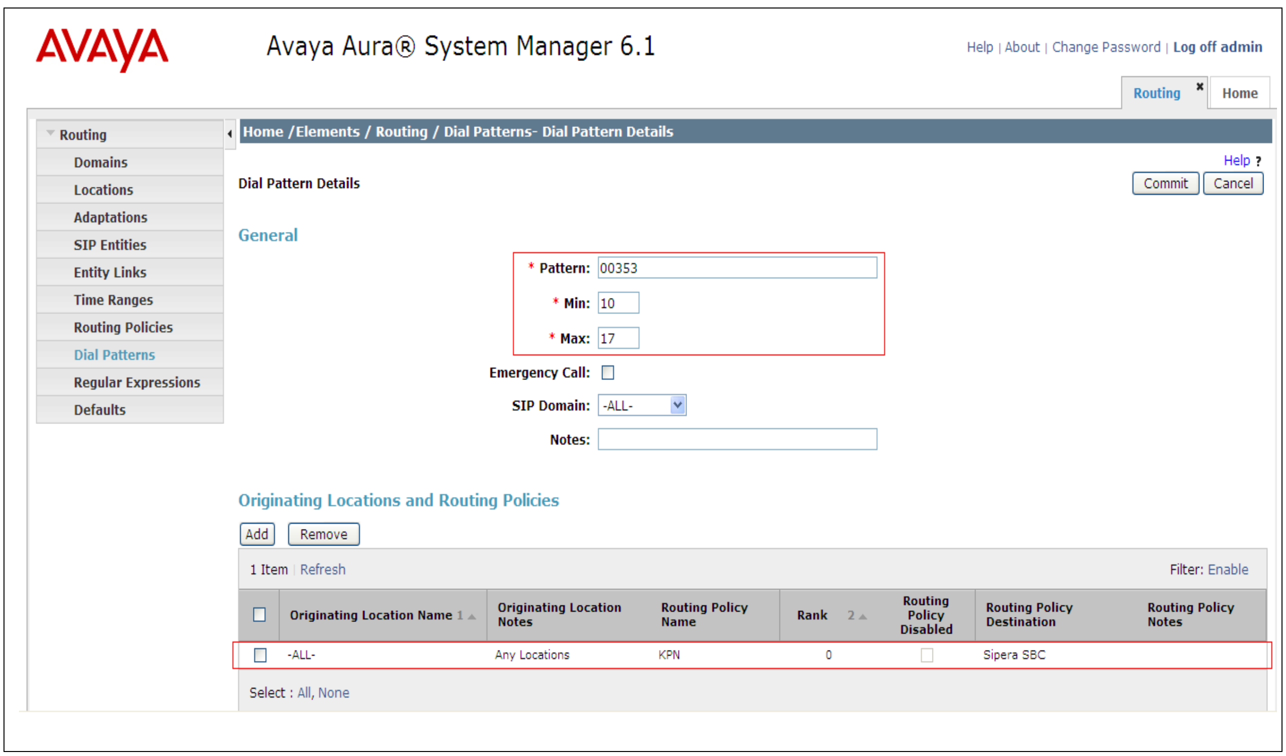
6.8. Administer Dial Patterns

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).

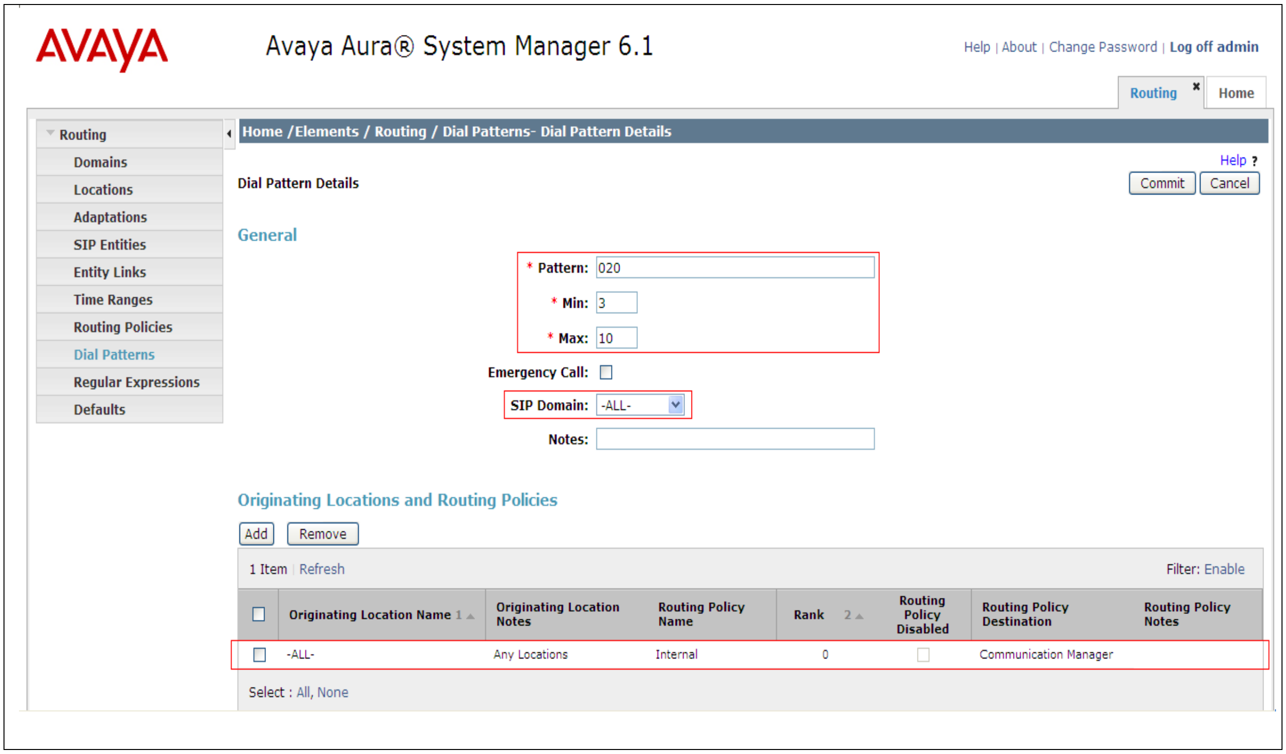
Under **General:**

- 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 6.7**. 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 KPN VoIP Connect service.



The following screen shows an example dial pattern configured for Communication Manager.

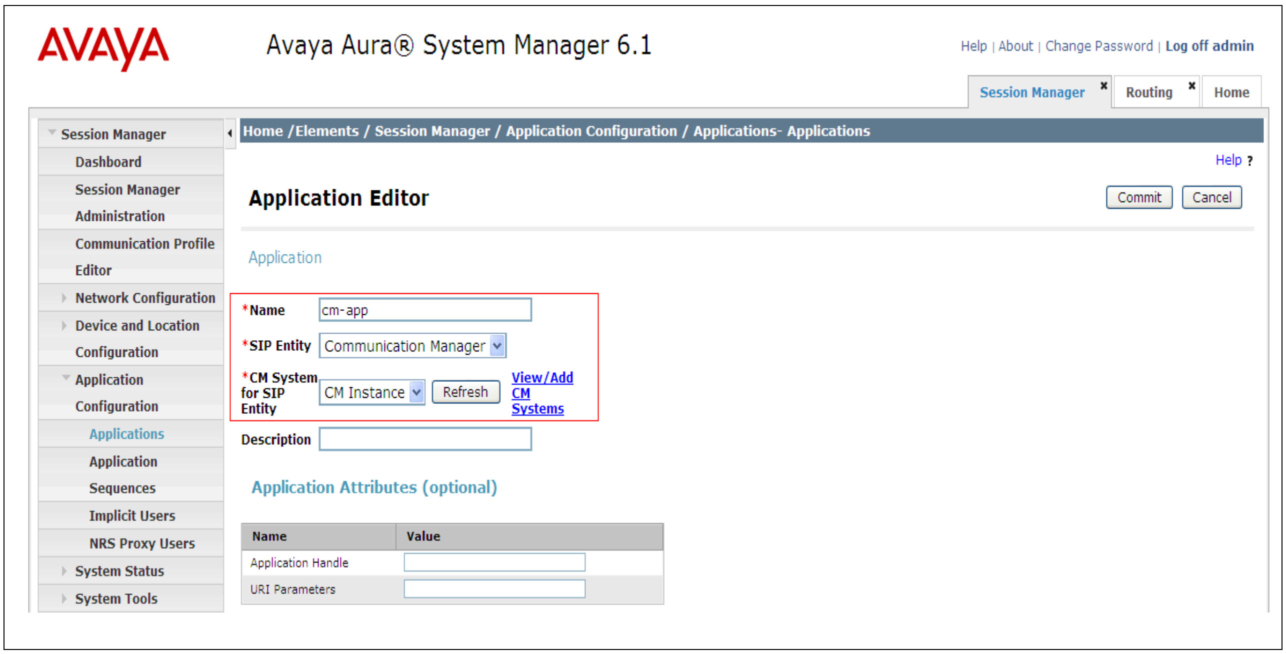


6.9. Administer Application for Avaya Aura® Communication Manager

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.

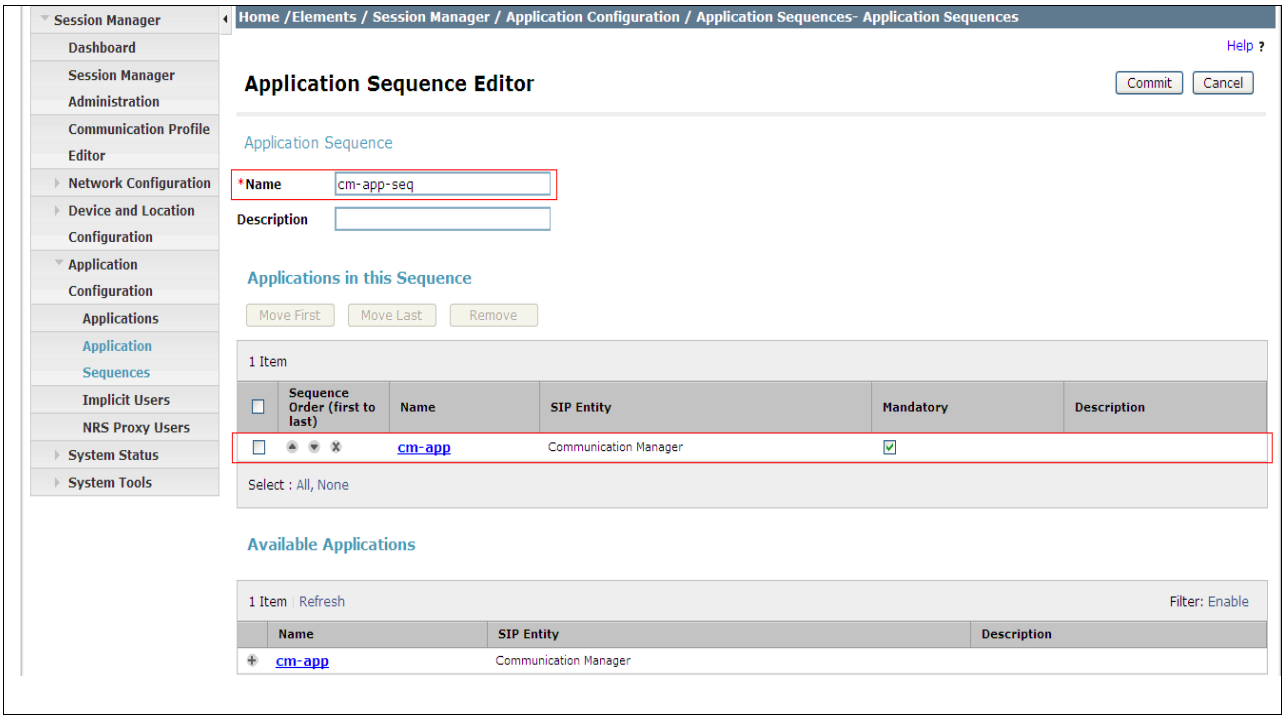


6.10. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Session Manager → Application Configuration → Application Sequences** and click on **New** (not shown).

- 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.**

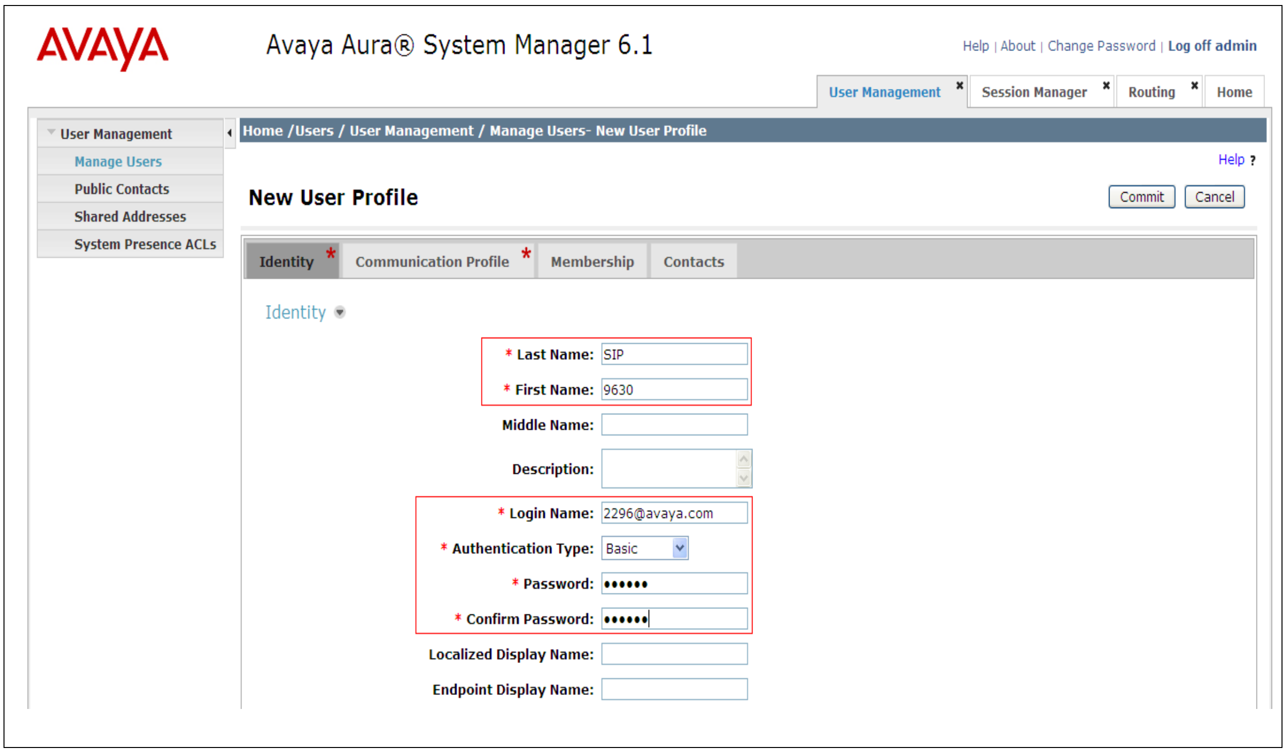


6.11. Administer SIP Extensions

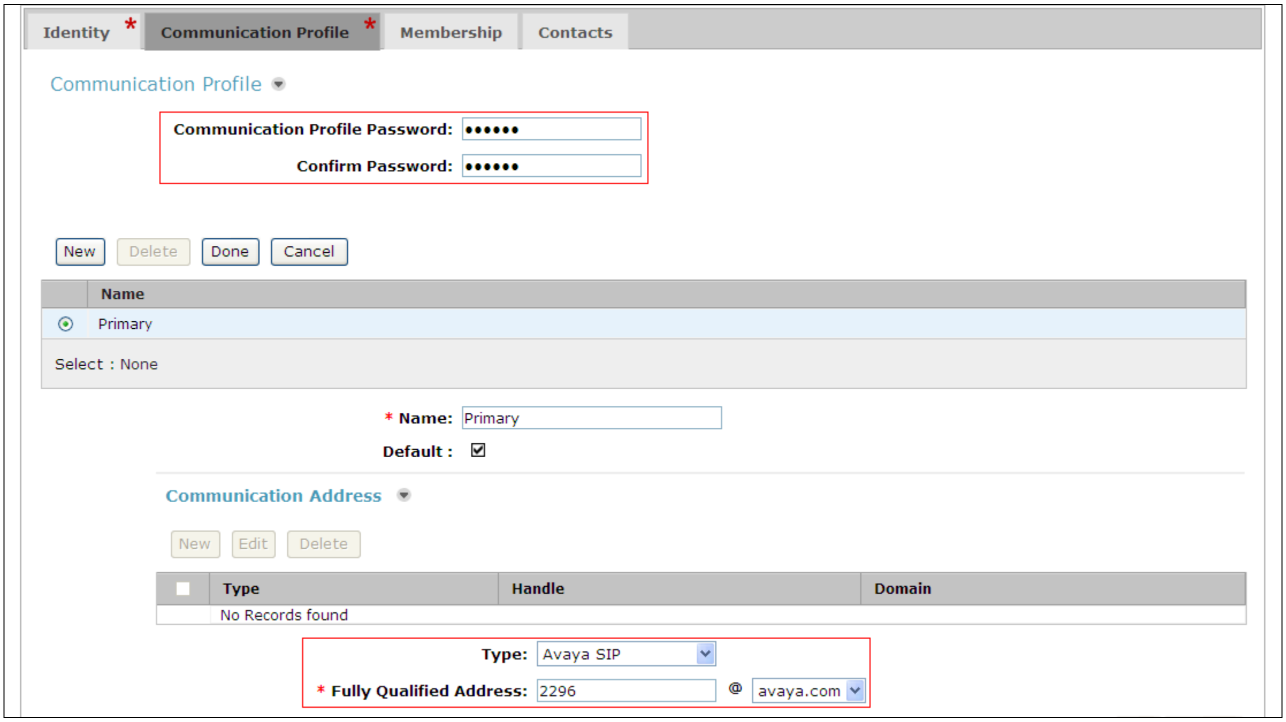
SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. From the Home tab select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

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

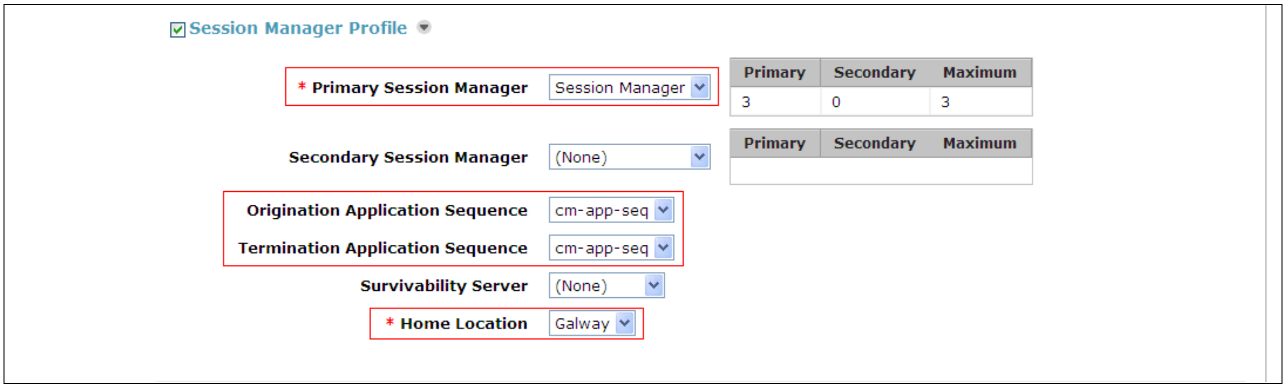


On the **Communication Profile** tab enter a numeric **Communication Profile Password** and confirm it, then expand the **Communication Address** section and click **New.** For the **Type** field select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button (not shown).



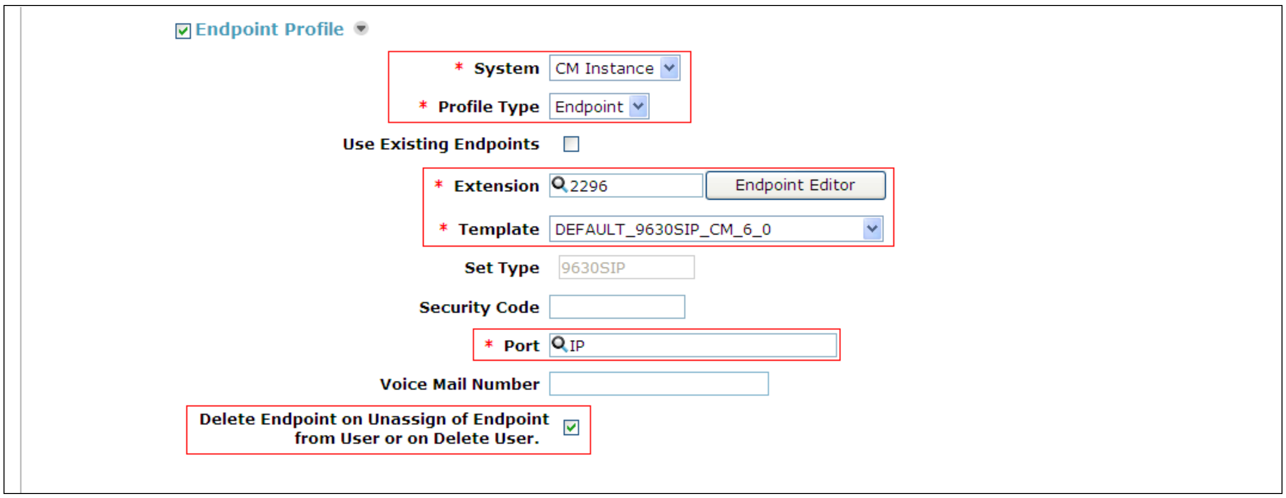
Expand the **Session Manager Profile** section.

- 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 6.10**
- Select the appropriate application sequence from the drop-down menu in the **Termination Application Sequence** field configured in **Section 6.10**
- Select the appropriate location from the drop-down menu in the **Home Location** field


Session Manager Profile
* Primary Session Manager
Session Manager
Primary
Secondary
Maximum
3
0
3
Secondary Session Manager
(None)
Primary
Secondary
Maximum
Origination Application Sequence
cm-app-seq
Termination Application Sequence
cm-app-seq
Survivability Server
(None)
* Home Location
Galway

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** (not shown) to save changes and the System Manager will add the Communication Manager user configuration automatically

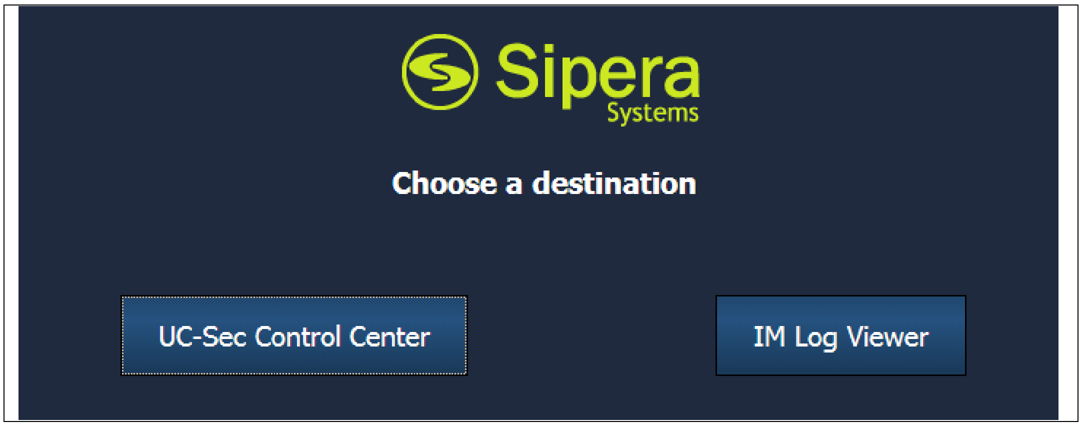


7. Configure Avaya Session Border Controller Advanced for Enterprise

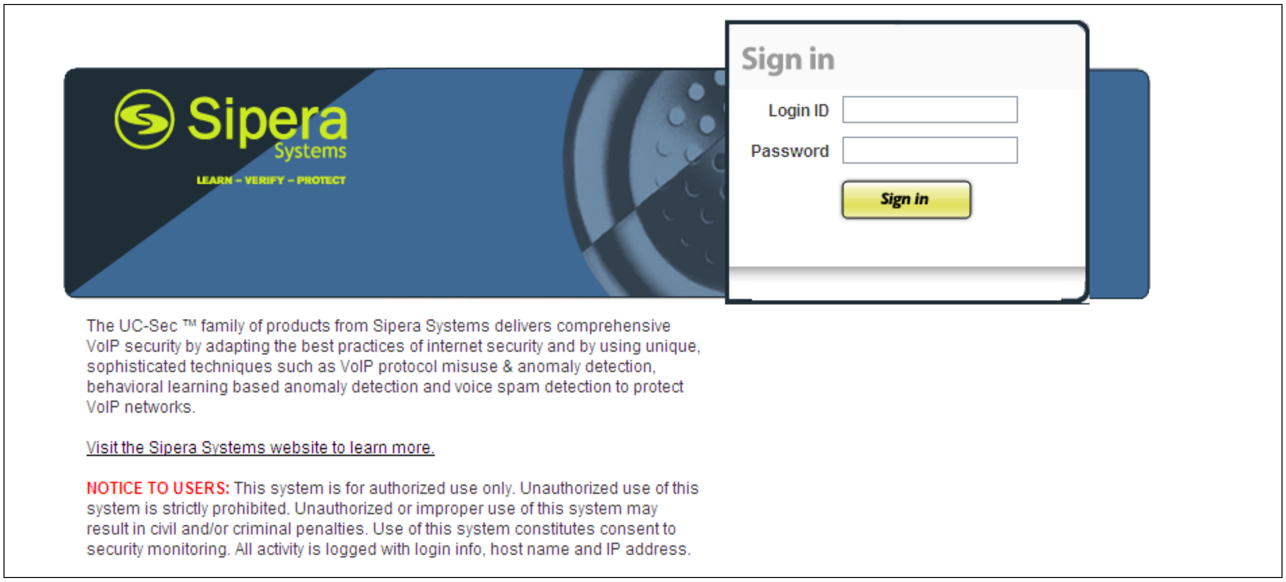
This section describes the configuration of the Session Border Controller. At the time of writing the Avaya Session Border Controller Advanced for Enterprise was badges as the Sipera E-SBC (Enterprise Session Border Controller) developed for Unified Communications Security (UC-Sec). The Avaya Session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



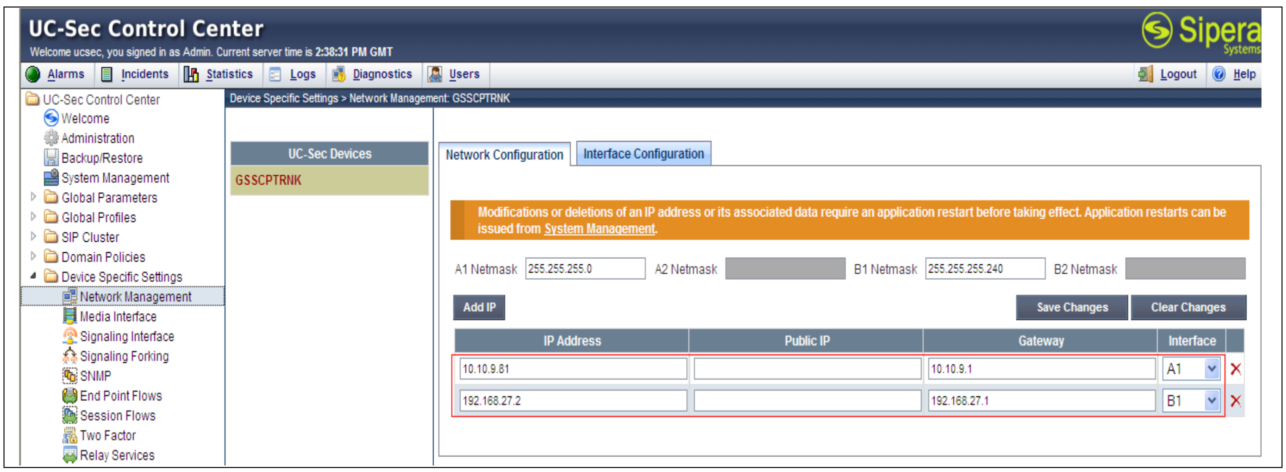
Log in with the appropriate credentials.



7.2. Define Network Information

To define the network information for the Avaya Session Border Controller Advanced for Enterprise, click on the **Device Specific Settings** to expand the options, then select **Network Management**.

- Click on **Add IP**
- 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 left pane
- Select **Restart Application** indicated by an icon in the status bar (not shown)



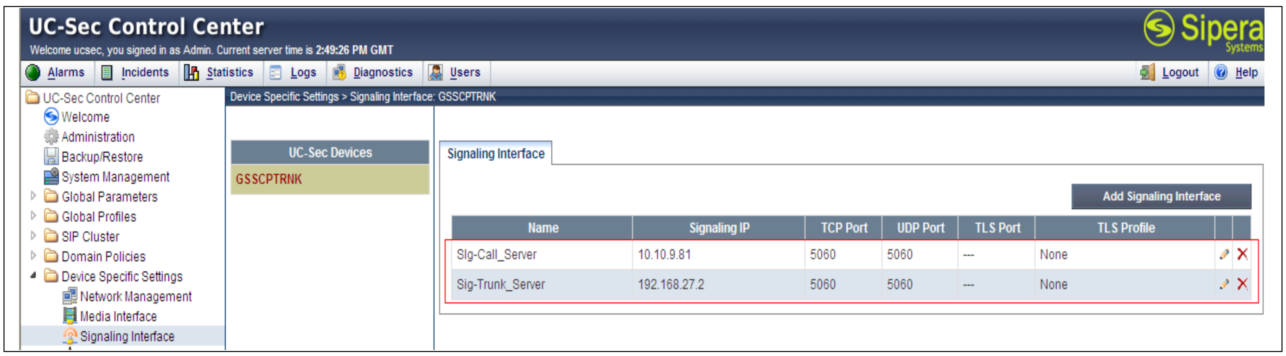
7.3. Define Interfaces

To define the signaling and media interfaces for the Avaya Session Border Controll Advanced for Enterprise, click on the **Device Specific Settings** to expand the options.

7.3.1. Signaling Interfaces

Select **Signaling Interface** from the menu options.

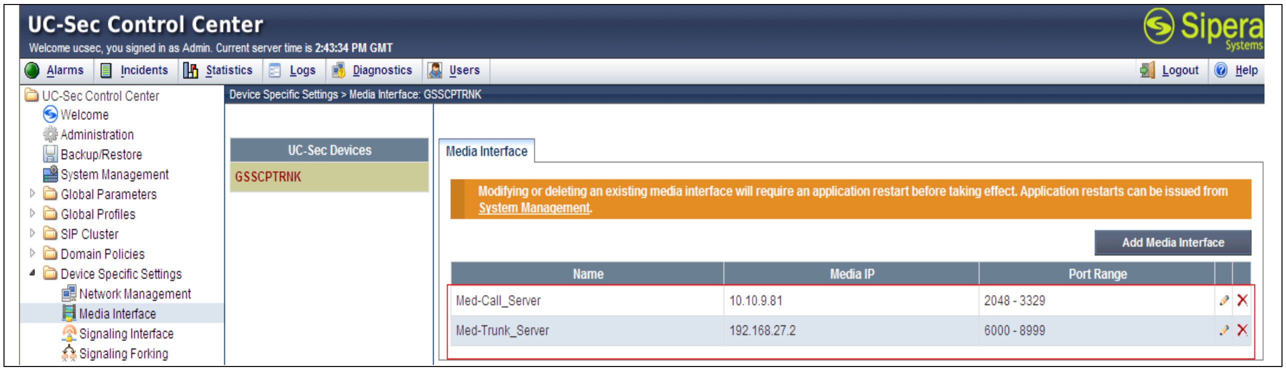
- Select **Add Signaling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal signalling interface
- Select an **internal** interface IP address defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, usually **5060**
- Select **Add Signaling 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** interface IP address defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, usually **5060**



7.3.2. Media Interfaces

Select **Media Interface** from the menu options. The IP addresses for media can be the same as those used for signaling.

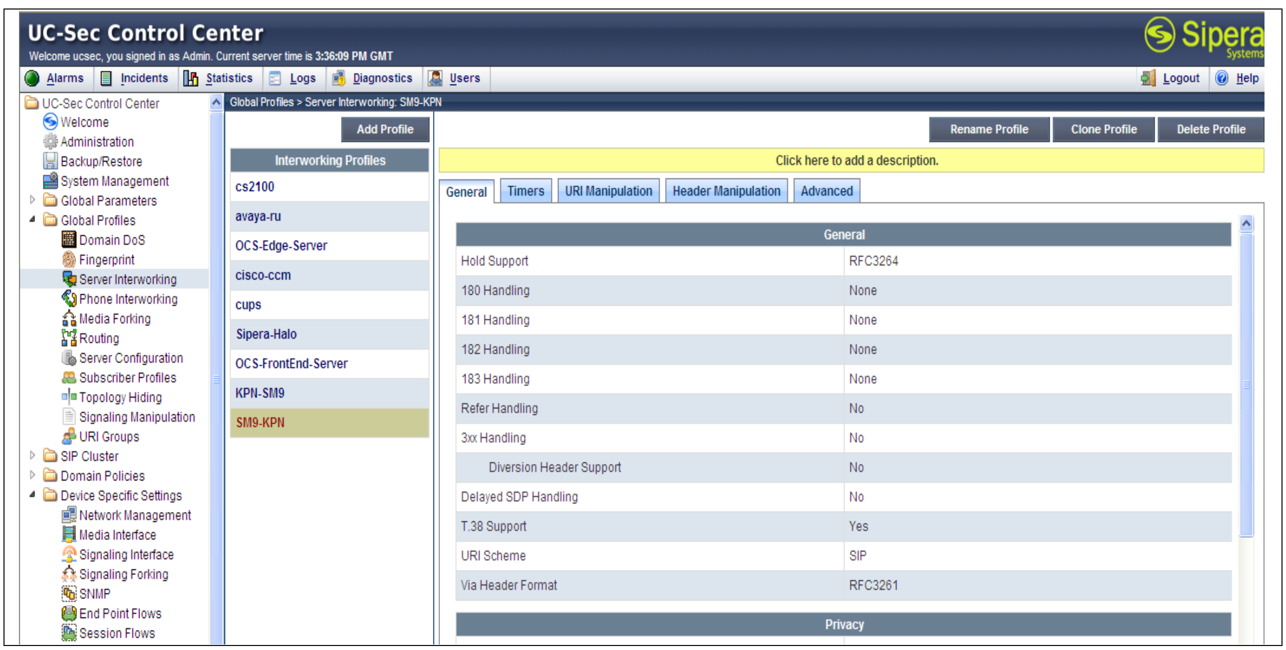
- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface
- Select an **internal** interface IP address defined in **Section 7.2**
- Select RTP port ranges for the media path with the enterprise end-points
- 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** interface IP address defined in **Section 7.2**
- Select RTP port ranges for the media path with the KPN SBC



7.4. Define Server Interworking

Server interworking is defined for the KPN SBC and the Session Manager. To define the Session Manager server interworking, first click on **Global Profiles** to expand the menu options.

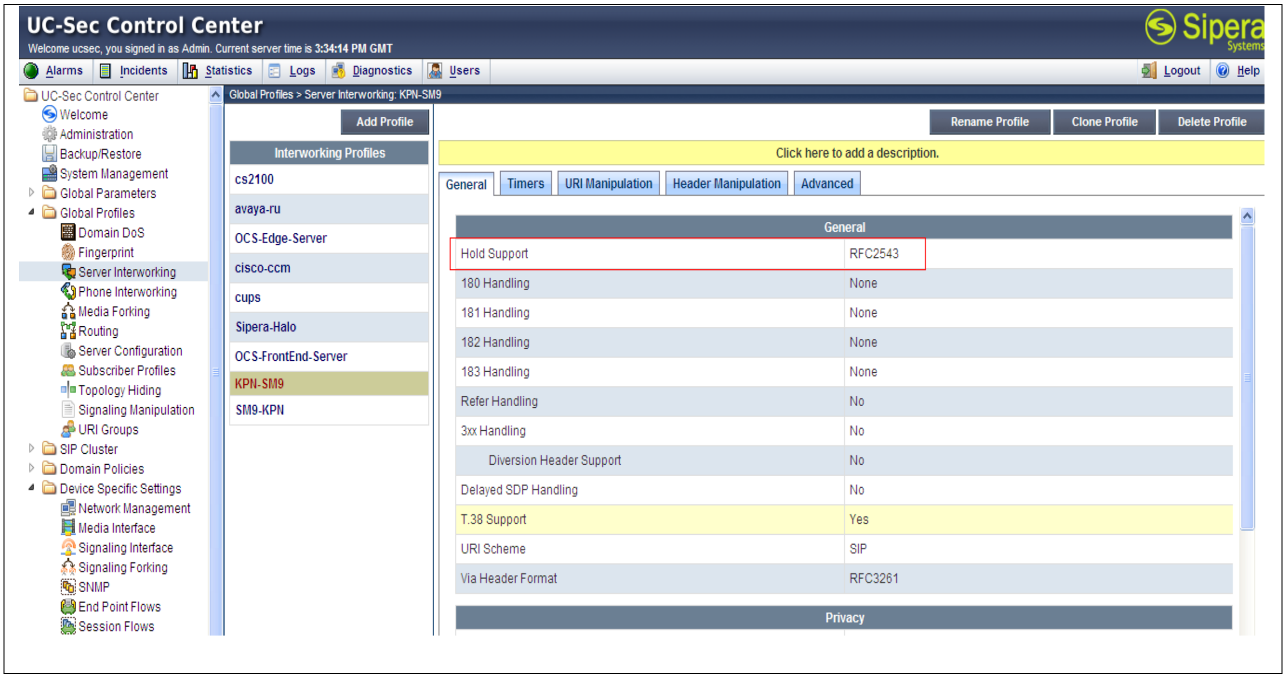
- Highlight the avaya-ru profile and select **Clone Profile**
- In the **Name** field enter a descriptive name for server interworking profile for the Session Manager
- Click on **Finish**
- Select **Edit** (not shown) and enter details in the pop-up menu
- Check the T.38 box, then click **Next** and **Finish**



To define the KPN trunk server interworking, first click on **Global Profiles** to expand the menu options.

- Highlight the previously created profile and select **Clone Profile** In the **Name** field enter a descriptive name for server interworking profile for the KPN SBC
- Click on **Finish**

- Select **Edit** (not shown) and enter details in the pop-up menu
- Check the T.38 box
- Check **RFC2543 c=0.0.0.0** option in **Hold Support**
- Click **Next** and **Finish**

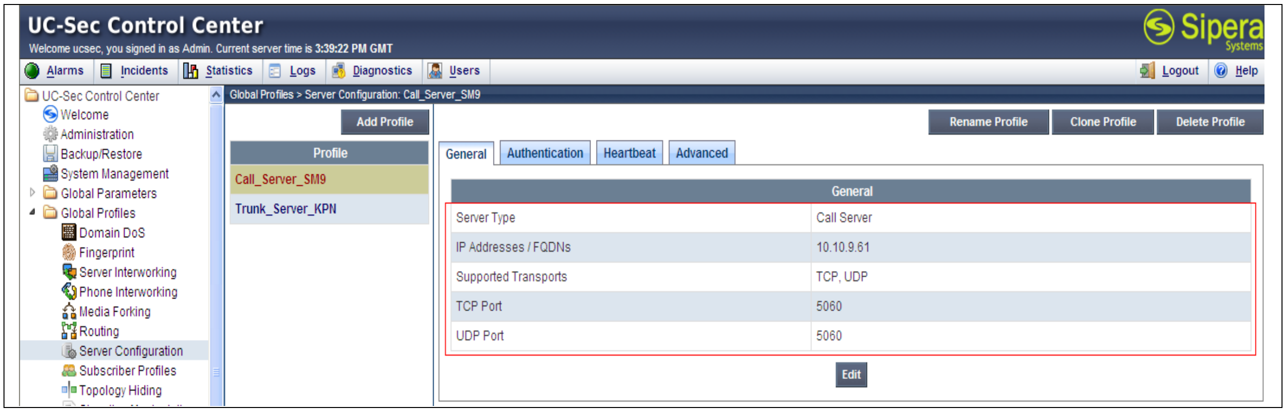


7.5. Define Servers

To define the servers and add the additional IP address for the KPN SBC, click on **Global Profiles** to expand the menu. Select **Server Configuration** to add the Call Server which is the Session Manager**.**

- Select **Add Profile**
- In the **Profile Name** pop-up 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 **internal** interface IP address defined in **Section 7.2**
- Check **TCP** and **UDP** in **Supported Transports**
- Define the **TCP port** and **UDP port** for SIP signaling, **5060** is recommended
- Click **Next** three times then select the **Interworking Profile** for the Session Manager defined in **Section 7.4** from the drop down menu
- Click **Finish**

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

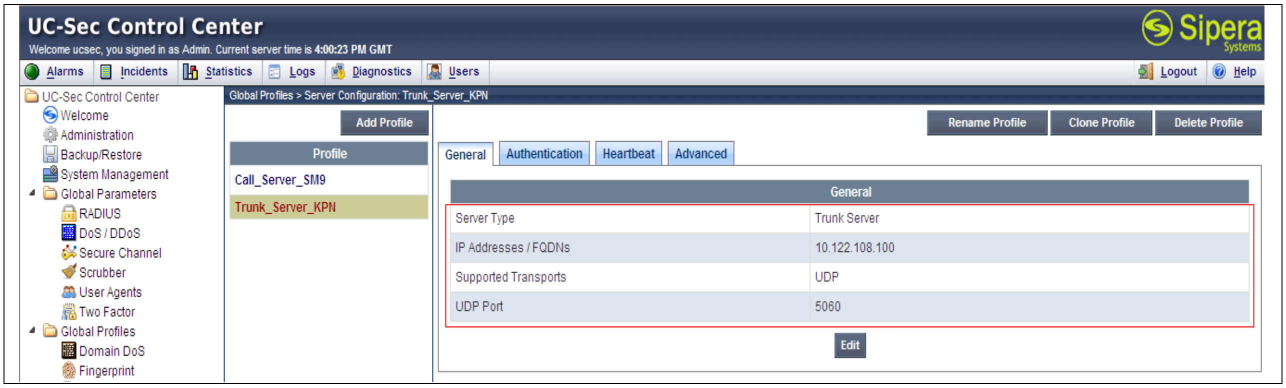


The **Adavanced** tab shows the **Interworking Profile**

Select **Server Configuration** to add the Trunk Server which is the KPN SBC**.**

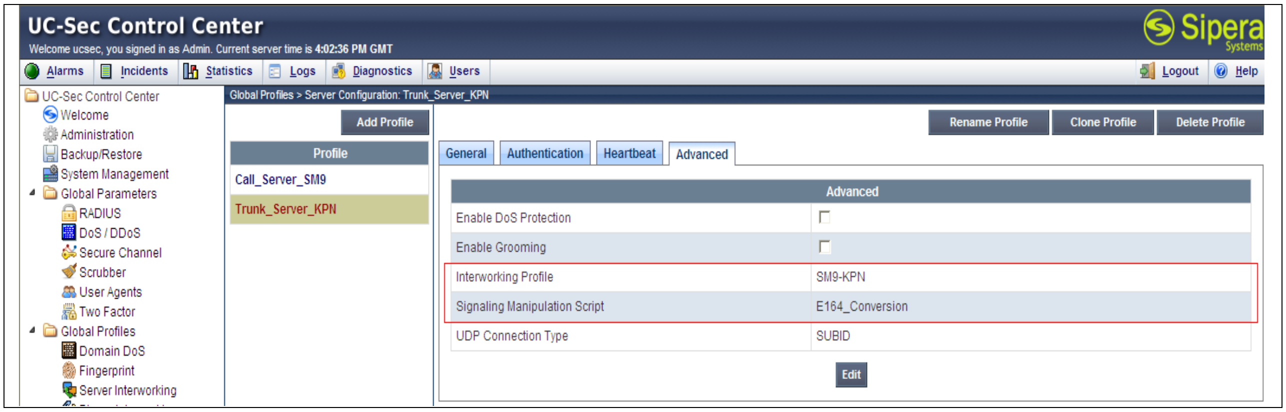
- Select **Add Profile**
- In the **Profile Name** pop-up field enter a descriptive name for the KPN SBC and click **Next**
- In the **Server Type** drop down menu select **Call Server**
- In the **IP Addresses / Supported FQDNs** box type the **external** interface IP address defined in **Section 7.2**
- Check **TCP** and **UDP** in **Supported Transports**
- Define the **TCP port** and **UDP port** for SIP signaling, **5060** is recommended
- Click **Next** three times then select the **Interworking Profile** for the KPN SBC defined in **Section 7.4** from the drop down menu
- Click **Finish**

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

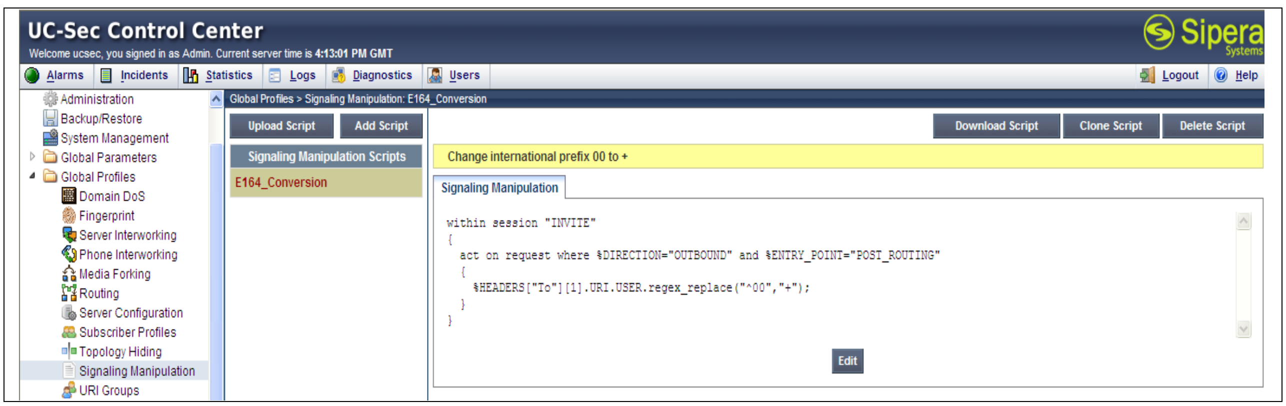

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 4:00:23 PM GMT
Sipera
Systems
Alarms
Incidents
Statistics
Logs
Diagnostics
Users
Logout
Help
UC-Sec Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
RADIUS
DoS / DDoS
Secure Channel
Scrubber
User Agents
Two Factor
Global Profiles
Domain DoS
Fingerprint
Global Profiles > Server Configuration: Trunk_Server_KPN
Add Profile
Rename Profile
Clone Profile
Delete Profile
Profile
Call_Server_SM9
Trunk_Server_KPN
General
Authentication
Heartbeat
Advanced
General
Server Type
Trunk Server
IP Addresses / FQDNs
10.122.108.100
Supported Transports
UDP
UDP Port
5060
Edit

During the test, a script was written to change the user address in the “To” field to E.164 format for consistency. Test calls were made successfully without this, but it is shown here for information.

- Select the server **Interworking Profile** defined in **Section 7.4**
- Select the **E.164_Conversion** script in the **Signaling Manipulation Script** field



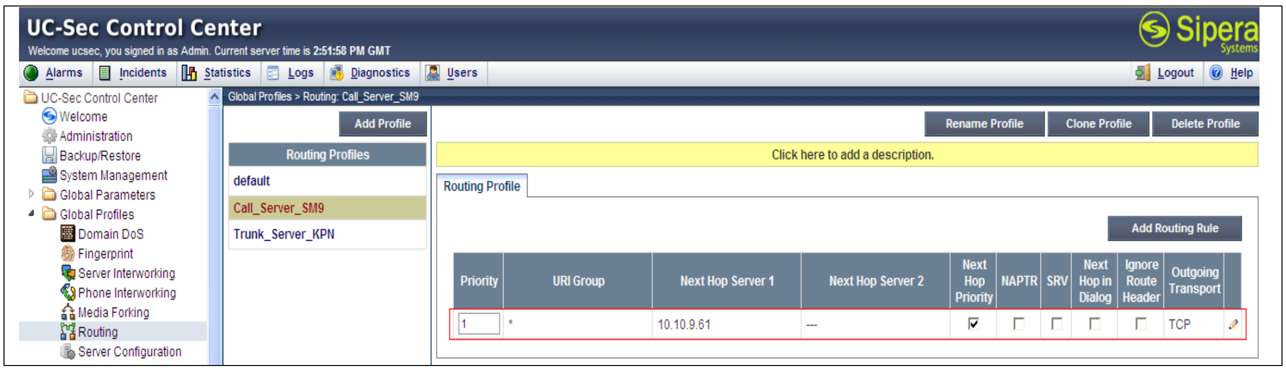
The **E164_Conversion** script is shown here for information.



7.6. Define Routing

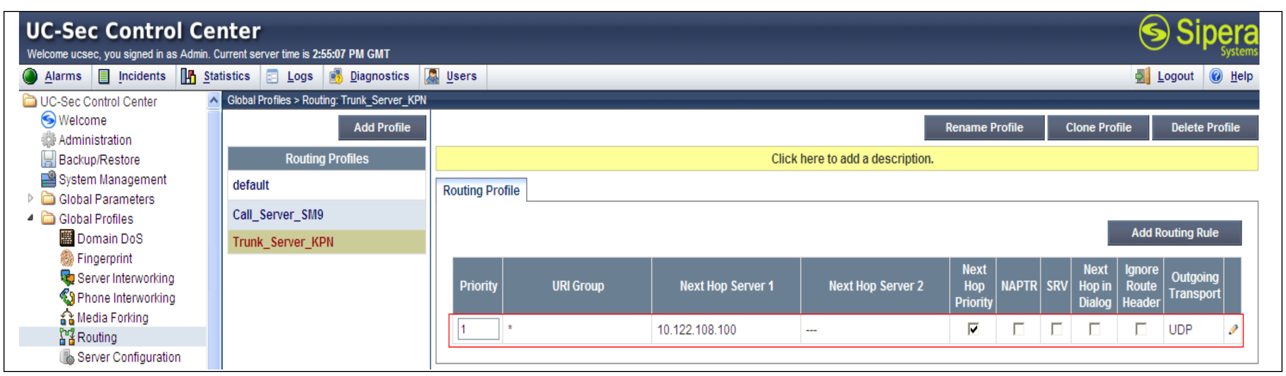
To define routing to the Session Manager, click on **Global Profiles** to expand the menu. Select **Routing.**

- Select **Add Profile**
- In the **Profile Name** pop-up field enter a descriptive name for the Session Manager and click **Next**
- Enter the Session Manager SM100 IP address in the **Next Hop Server 1** field
- Select TCP for the **Outgoing Transport** and click **Finish**



To define routing to the Session Manager, create an additional profile

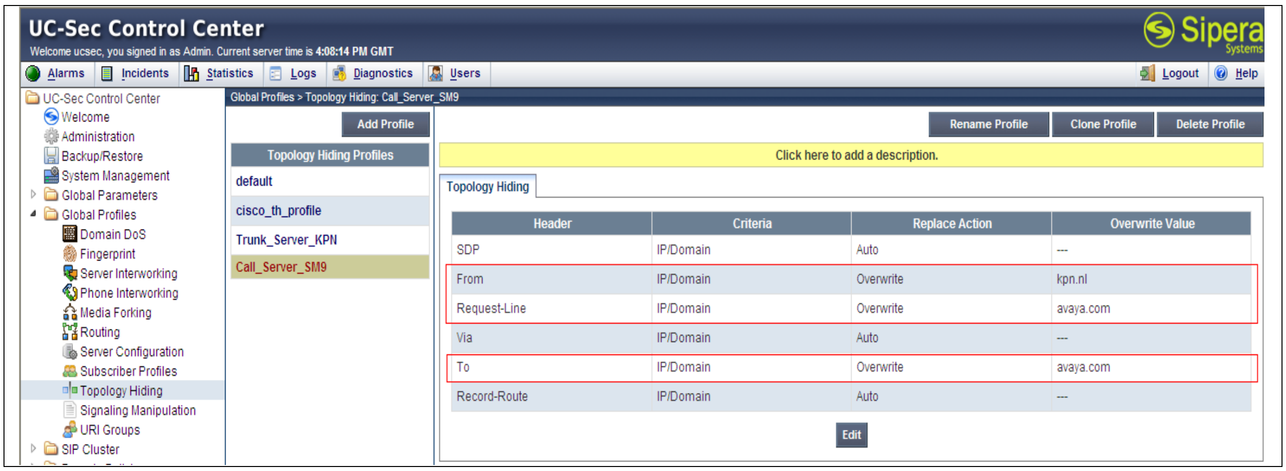
- Select **Add Profile**
- In the **Profile Name** pop-up field enter a descriptive name for the KPN SBC and click **Next**
- Enter the KPN SBC IP address in the **Next Hop Server 1** field
- Select **UDP** for the **Outgoing Transport** and click **Finish**



7.7. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. To define Topology Hiding for the Session Manager, click on **Global Profiles** to expand the menu and select **Topology Hiding**

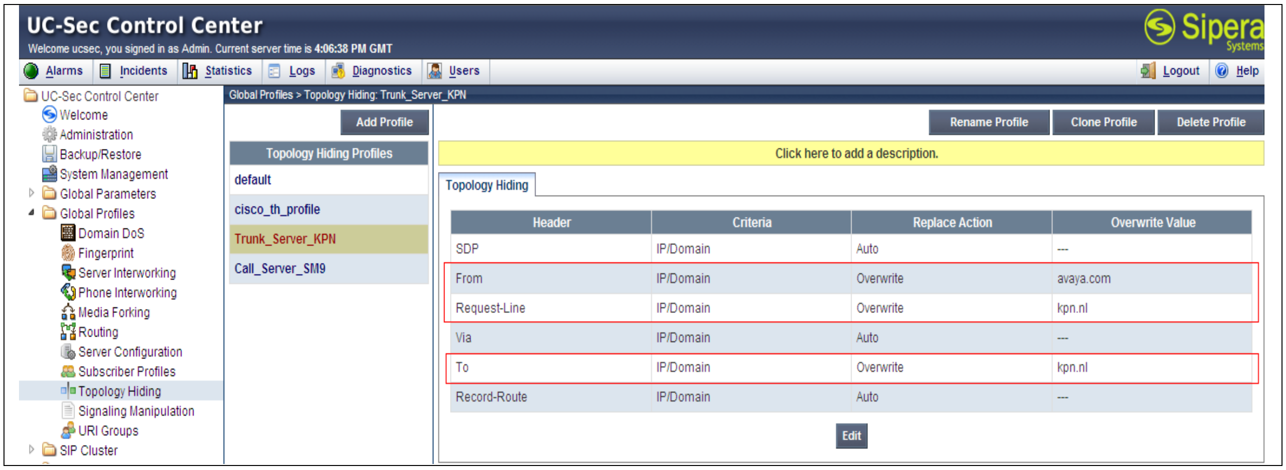
- Select **Add Profile**
- In the **Profile Name** pop-up field enter a descriptive name for the Session Manager and click **Next**
- **Overwrite** the **From** field with a domain name provided by KPN
- **Overwrite** the **Request-Line** field and **To** field with a local domain name, **avaya.com** is used as an example, then click **Finish**



Note: A single domain name could be used for the enterprise and the KPN network.

To define Topology Hiding for the KPN SBC, create an additional profile

- Select **Add Profile**
- In the **Profile Name** pop-up field enter a descriptive name for the KPN SBC and click **Next**
- **Overwrite** the **From** field with a local domain name, **avaya.com** is used as an example
- **Overwrite** the **Request-Line** field and **To** field with a domain name provided by KPN and click **Finish**



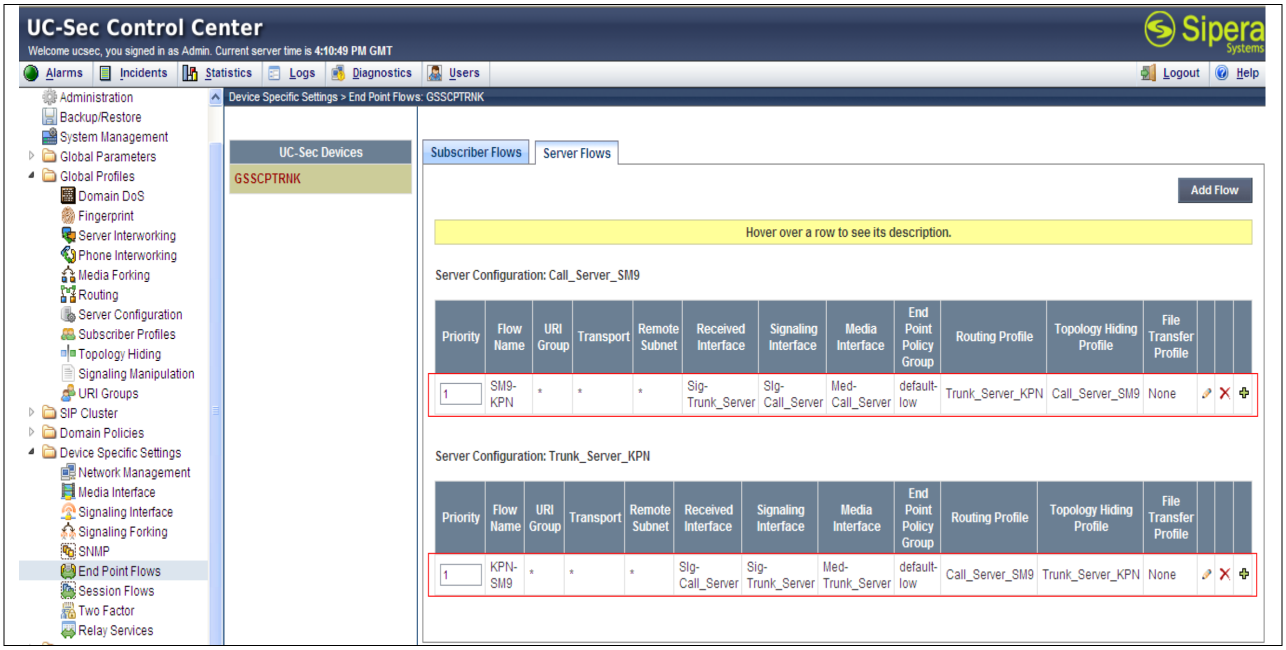
7.8. Server Flows

Server Flows combine the previously defined profiles into an outgoing flow from the Session Manager to the KPN SBC and an incoming flow from the KPN SBC to the Session Manager. To define an outgoing Server Flow, click on **Device Specific Settings** to expand the menu and select **End Point Flows.**

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the **Add Flow** pop-up
- In the **Flow Name** field enter a descriptive name for the outgoing server flow
- In the **Received Interface** field, select the SIP signalling interface for the KPN SBC
- In the **Signaling Interface** field, select the SIP signalling interface for the Session Manager
- In the **Media Interface** field, select the media interface for the Session Manager
- In the **Routing Profile** field, select the routing profile of the KPN SBC
- In the **Topology Hiding Profile** field, select the top[ology hiding profile of the Session Manager

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

- Select **Add Flow** and enter details in the **Add Flow** pop-up
- In the **Flow Name** field enter a descriptive name for the incoming server flow
- In the **Received Interface** field, select the SIP signalling interface for the Session Manager
- In the **Signaling Interface** field, select the SIP signalling interface for the KPN SBC
- In the **Media Interface** field, select the media interface for the KPN SBC
- In the **Routing Profile** field, select the routing profile of the Session Manager
- In the **Topology Hiding Profile** field, select the topology hiding profile of the KPN SBC


UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 4:10:49 PM GMT
Alarms
Incidents
Statistics
Logs
Diagnostics
Users
Logout
Help
Device Specific Settings > End Point Flows: GSSCPTRNK
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Fingerprint
Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration
Subscriber Profiles
Topology Hiding
Signaling Manipulation
URI Groups
SIP Cluster
Domain Policies
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
SNMP
End Point Flows
Session Flows
Two Factor
Relay Services
UC-Sec Devices
GSSCPTRNK
Subscriber Flows
Server Flows
Add Flow
Hover over a row to see its description.
Server Configuration: Call_Server_SM9
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
SM9-KPN
*
*
*
Sig-Trunk_Server
Sig-Call_Server
Med-Call_Server
default-low
Trunk_Server_KPN
Call_Server_SM9
None
Server Configuration: Trunk_Server_KPN
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
KPN-SM9
*
*
*
Sig-Call_Server
Sig-Trunk_Server
Med-Trunk_Server
default-low
Call_Server_SM9
Trunk_Server_KPN
None

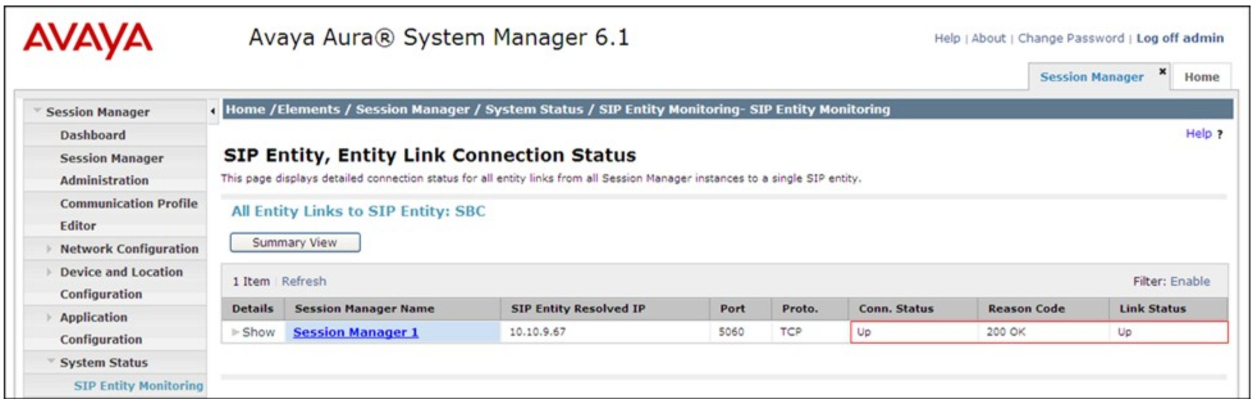
8. Service Provider Configuration

The configuration of the KPN equipment used to support the KPN VoIP Connect service is outside of the scope of these Application Notes and will not be covered. To obtain further information on KPN equipment and system configuration please contact an authorised KPN 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 KPN VoIP Connect Service. KPN VoIP Connect Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2.**

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 6.0.3, February 2011.

[2] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.

[3] *Administering Avaya Aura® Communication Manager*, Release 6.0.1, April 2011.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* August 2010, Document Number 555-245-205.

[5] *Installing and Upgrading Avaya Aura® System Manager Release 6.1*, November 2010.

[6] *Installing and Configuring Avaya Aura® Session Manager*, April 2011, Document Number 03-603473

[7] *Administering Avaya Aura® Session Manager,* October 2011, Document Number 03-603324.

[8] E-SBC (*Avaya Session Border Controller Advanced for Enterprise) Administration Guide*, November 2011

[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.