Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R7.0 as an Evolution Server, Avaya Aura® Session Manager R7.0 and Avaya Session Border Controller for Enterprise R7.0 to support Swisscom VoIP Gate service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Swisscom VoIP Gate service and an Avaya SIP enabled enterprise solution.

The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server. Swisscom is a member of the DevConnect Service Provider program.

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

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

©2016 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Swisscom's VoIP Gate service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Customers using this Avaya SIP-enabled enterprise solution with Swisscom VoIP Gate 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 Avaya SBCE. The enterprise site was configured to use the SIP trunking service provided by Swisscom. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section** Error! Reference source not found..

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

To verify SIP trunking interoperability the following features and functionality were exercised during the interoperability compliance test:

- Incoming PSTN calls to various phone types including H.323, SIP, Digital and Analogue telephones at the enterprise.
- All inbound PSTN calls were routed to the enterprise across the SIP trunk from the Service Provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, Digital, and Analogue telephones at the enterprise.
- All outbound PSTN calls were routed from the enterprise across the SIP trunk to the Service Provider.
- Calls using the G.711A codec.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using G.711 pass-through transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- Inbound and outbound PSTN calls to/from Avaya One-X® Communicator Softphone clients.

©2016 Avaya Inc. All Rights Reserved.

- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, call mute, transfer, and conference.
- Off-net call forwarding and mobile twinning.

2.2. Test Results

Interoperability testing of the test configuration was completed with successful results for Swisscom's VoIP Gate service with the following observations:

- The Swisscom VoIP Gate was unable to handle SIP messages with an Avaya proprietary parameter in the Contact header. The parameter "+avaya-cm-keep-mpro" is present with a value of "no" when Initial IP-IP Direct Media is enabled on Communication Manager SIP Trunk. A SigMa script on the Avaya SBCE was required to remove the parameter "+avaya-cm-keep-mpro". The details of the Sigma Script and how to configure the script on the Avaya SBCE are outlined in **Section 7.2.7**.
- G.729 codec is not supported by Swisscom.
- No inbound toll free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- Access to Emergency Services was not tested as no test call had been booked by the Service Provider with the Emergency Services Operator. However both three and four digit numbering format replicating Emergency Service's numbering formats was tested successfully.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com.

For technical support on Swisscom products please contact the Swisscom support team:

- Email: ent.Incident-Voice@swisscom.com

3. Reference Configuration

The following equipment in **Figure 1** illustrates the test configuration. The test configuration shows an Enterprise site connected to Swisscom VoIP Gate service. Located at the Enterprise site is an Avaya Session Border Controller for Enterprise, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 16xx series IP telephones (with H.323 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.

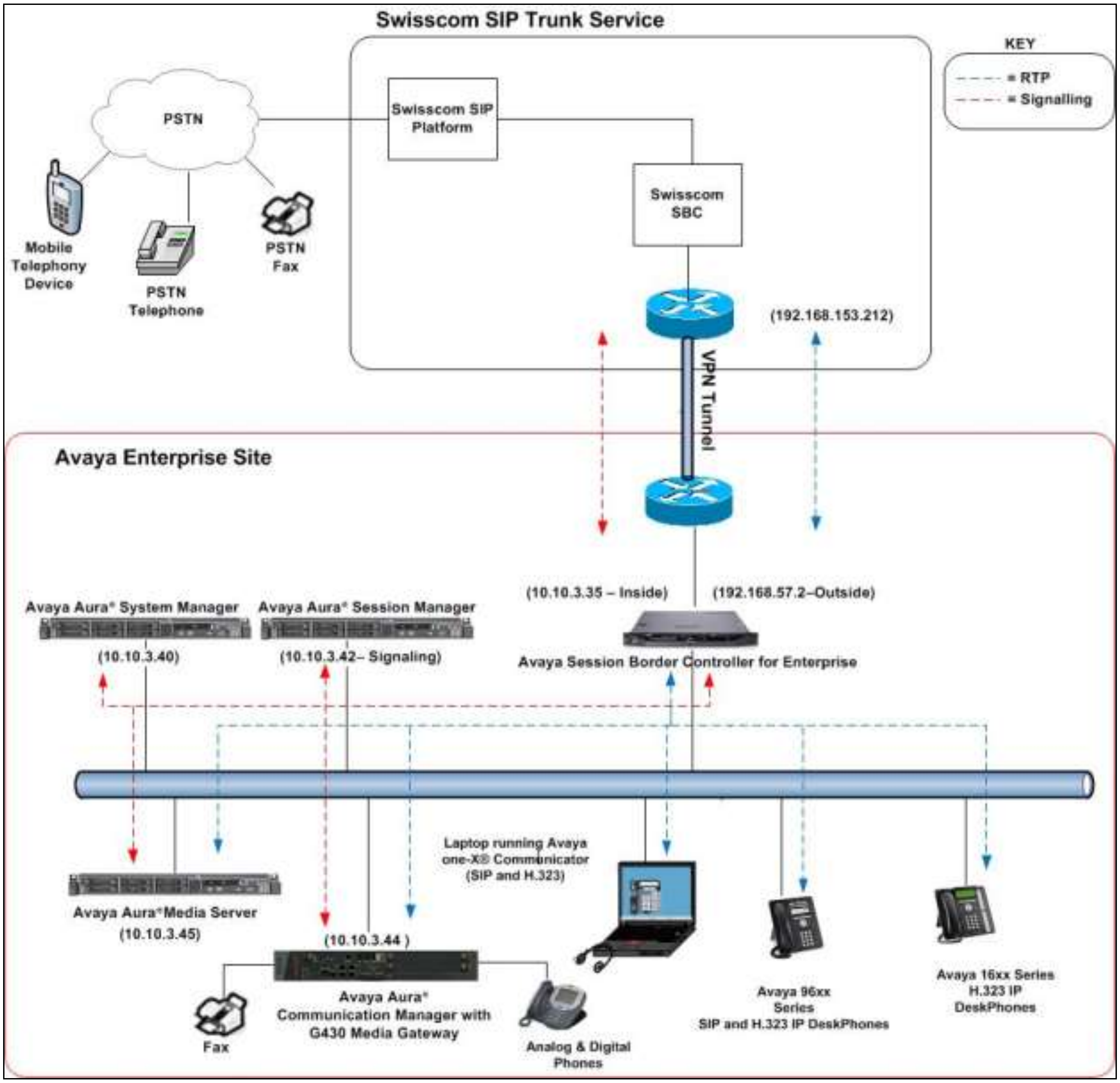


Figure 1: Test Setup Swisscom VoIP Gate Service to Avaya Enterprise

©2016 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Dell PowerEdge R620 running System Manager on VM Version 8	7.0.0.2 - Build No. - 7.0.0.0.16266-7.0.9.7002010 Software Update Revision No: 7.0.0.2.4416
Dell PowerEdge R620 running Session Manager on VM Version 8	7.0.0.2.700201
Avaya S8300D Server running Avaya Aura® Communication Manager	R017x.00.0.441.0 (23012)
Avaya G430 Media Gateway	7.0.1.0 (g430_sw_37_38.0)
Avaya Aura® Media Server	7.7.0.236
Avaya Session Border Controller for Enterprise	7.0.1-03-8739
Avaya 1600 IP Deskphone (H.323)	1.3.9
Avaya 9670 IP DeskPhone (H.323)	6.6
Avaya 96x0 IP DeskPhone (H.323)	6.6
Avaya 9611 IP DeskPhone (SIP)	7.0
Avaya 9608 IP DeskPhone (SIP)	7.0
Avaya 9621 IP DeskPhone (SIP)	7.0
Avaya 9608 IP DeskPhone (SIP)	7.0
Avaya one–X® Communicator (H.323 & SIP) on Lenovo T510 Laptop PC	6.2.11.03-FP11
Analogue Handset	N/A
Analogue Fax	N/A
Swisscom	
SBC	Genband Q20 load v8.3.17.4 GbLinux 8.3.0-54 Media hk-8.3-24_sb.x86_64
SSL	MCP_17.0.7.13_2014-03-17-1238
GWC	GC170BU
C20 Core	CVM17 - SWC000013.PPC3

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 Swisscom VoIP Gate. For incoming calls, Session Manager receives SIP messages from the Avaya SBCE 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

©2016 Avaya Inc. All Rights Reserved.

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 Session Manager. Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Swisscom 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 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 Swisscom SIP 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: 41000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 4000  10
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
```


©2016 Avaya Inc. All Rights Reserved.

On **Page 5**, verify that **IP Trunks** field is set to **y.**

```
display system-parameters customer-options                          Page   5 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? y
  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 Session Manager. In this case, **SM** and **10.10.3.42** 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
SM                  10.10.3.42
ASM                 10.10.3.45
default             0.0.0.0
procr               10.10.3.44
procr6              ::
```


©2016 Avaya Inc. All Rights Reserved.

5.3. Administer IP Network Region

Use the **change ip-network-region x** command where x is the desired network-region 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 Avaya SBCE.
- 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.
- The rest of the fields can be left at default values.

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


©2016 Avaya Inc. All Rights Reserved.

5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the IP Network Region form in **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 Swisscom was configured, namely **G.711A**.

```
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
```

Swisscom VoIP Gate service supports G.711 pass-through for transmission of fax. Navigate to **Page 2** and define fax properties as follows:

- Set the **FAX - Mode** to **pass-through**.
- Leave **ECM** at default value of **y**.

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

                          IP CODEC SET

                              Allow Direct-IP Multimedia? n



                                                                     Packet
                          Mode                    Redundancy         Size(ms)
    FAX                   pass-through             0            ECM: y
    Modem                 off                      0
    TDD/TTY               US                       3
    H.323 Clear-channel   n                        0
    SIP 64K Data          n                        0                 20
```


©2016 Avaya Inc. All Rights Reserved.

5.5. Administer SIP Signalling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Swisscom VoIP Gate network. 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 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 Session Manager (node name **SM** 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 (allows Communication Manager to accept calls from any SIP domain on the associated trunk).
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from Communication Manager).
- Set **Direct IP-IP Audio Connections** to **y**.
- Set **Initial IP-IP Direct Media** to **y** to enable Direct Media.
- Set **H.323 Station Outgoing Direct Media** to **y**.

The default values for the other fields may be used.

```
add 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
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

   Near-end Node Name: procr                 Far-end Node Name: SM
 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? y
H.323 Station Outgoing Direct Media? y            Alternate Route Timer(sec): 6
```

5.6. Administer SIP Trunk Group

A trunk group is associated with the signalling 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**.
- 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** administered for 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: OUTSIDE CALL               COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? n
 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 Swisscom to prevent unnecessary SIP messages during call setup. During the compliance testing, **Preferred Minimum Session Refresh Interval (sec)** was set to **150**.

```
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): 150

 Disconnect Supervision - In? y  Out? y


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


 Caller ID for Service Link Call to H.323 1xC: station-extension
```


©2016 Avaya Inc. All Rights Reserved.

On **Page 3**, set the **Numbering Format** field to **public**. This allows delivery of CLI in E164 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 **Mark Users as Phone** to **n**.
- Set **Send Transferring Party Information** to **n**.
- Set **Network Call Direction** to **n**.
- Set **Send Diversion Header** to **y**.
- Set **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Swisscom.
- Set **Always Use re-INVITE for Display Updates** to **y**.
- Set the **Identity for Calling Party Display** to **P-Asserted-Identity**.

```
PROTOCOL VARIATIONS

                                         Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n
          Build Refer-To URI of REFER From Contact For NCR? 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
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
```


©2016 Avaya Inc. All Rights Reserved.

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering x** command to configure Communication Manager to send the calling party number in the format required. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones.

```
change public-unknown-numbering                               Page   1 of   2
                          NUMBERING - PUBLIC/UNKNOWN FORMAT
                                                 Total
Ext Ext            Trk        CPN                 CPN
Len Code           Grp(s)     Prefix              Len
                                                        Total Administered: 6
 4  6010           1          4124xxxxx30         11       Maximum Entries: 240
 4  6020           1          4124xxxxx31         11
 4  6030           1          4124xxxxx32         11    Note: If an entry applies to
 4  6100           1          4124xxxxx33         11    a SIP connection to Avaya
 4  6102           1          4124xxxxx34         11    Aura(R) Session Manager,
 4  6104           1          4124xxxxx35         11    the resulting number must
                                                        be a complete E.164 number.

                                                        Communication Manager
                                                        automatically inserts
                                                        a '+' digit in this case.
```

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 Swisscom's VoIP Gate 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:
```


©2016 Avaya Inc. All Rights Reserved.

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**. 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                     11   14     1        pubu          n
    00                    13   15     1        pubu          n
    0035391               13   13     1        pubu          n
    030                   10   10     1        pubu          n
    0800                  8    10     1        pubu          n
    0900                  8    8      1        pubu          n
```

Use the **change route-pattern x** command, where **x** is an available route pattern, 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**. **Numbering Format** is applied to CLI and is used to set TDM signalling parameters such as type of number and numbering plan indicator. This doesn't have the same significance in SIP calls and during testing it was set to **unk-unk**.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1      Pattern Name:
                             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
 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
```

©2016 Avaya Inc. All Rights Reserved.

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 Swisscom 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 Swisscom correlate to the internal extensions assigned within Communication Manager. The entries displayed below translate incoming DDI numbers **+4124xxxxx30**, **+4124xxxxx31**, **+4124xxxxx32**, **+4124xxxxx33**, **+4124xxxxx34** and **+4124xxxxx35** to a 4 digit extension by deleting all of the incoming digits and inserting an extension. Public DDI numbers have been masked for security purposes.

```
change inc-call-handling-trmt trunk-group 1                     Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    12 +4124xxxxx30     all 6010
 public-ntwrk    12 +4124xxxxx31     all 6020
 public-ntwrk    12 +4124xxxxx32     all 6030
 public-ntwrk    12 +4124xxxxx33     all 6100
 public-ntwrk    12 +4124xxxxx34     all 6102
 public-ntwrk    12 +4124xxxxx35     all 6104
```

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 6102. 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**.
- For the **Phone Number** enter the phone that will also be called (e.g.**0035389434xxxx**).
- 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 6102                   Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number      Trunk        Config  Dual
 Extension                 Prefix                       Selection    Set     Mode
 6102             EC500        -      0035389434xxxx        1          1
-
```

Note: The phone number shown is for a mobile phone used for testing at Avaya Labs and is in international format. To use facilities for calls coming in from EC500 mobile phones, the number received in Communication Manager must exactly match the number specified in the above table.

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

©2016 Avaya Inc. All Rights Reserved.

6. Configuring Avaya Aura® Session Manager

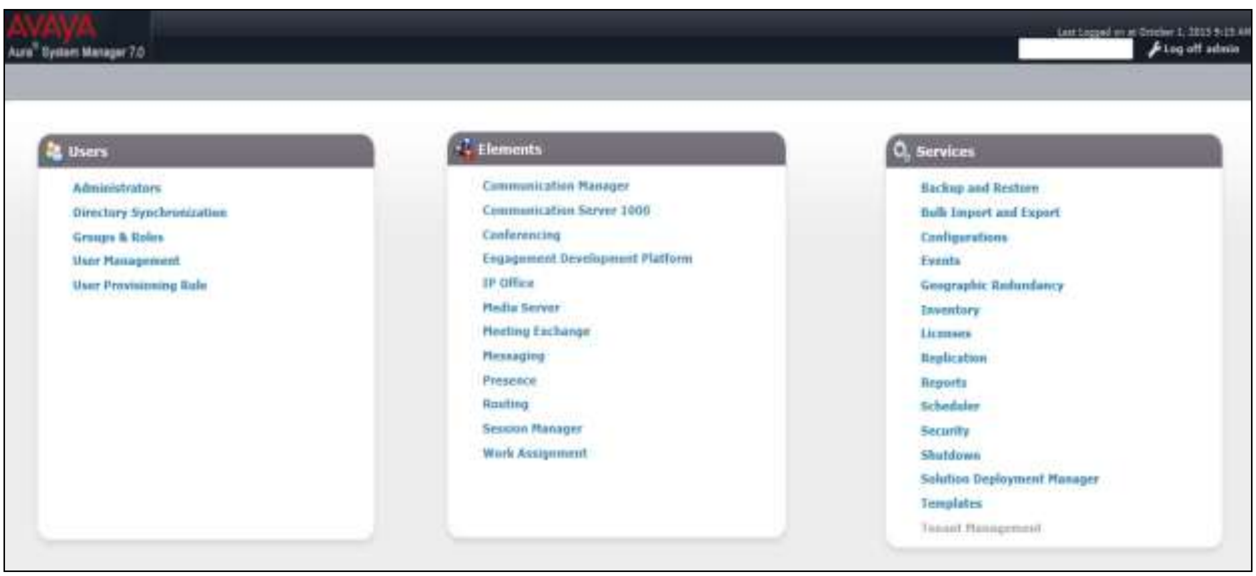
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager.
- Administer SIP Domain.
- Administer SIP Location.
- Administer Adaptations.
- Administer SIP Entities.
- Administer Entity Links.
- Administer Routing Policies.
- Administer Dial Patterns.

It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

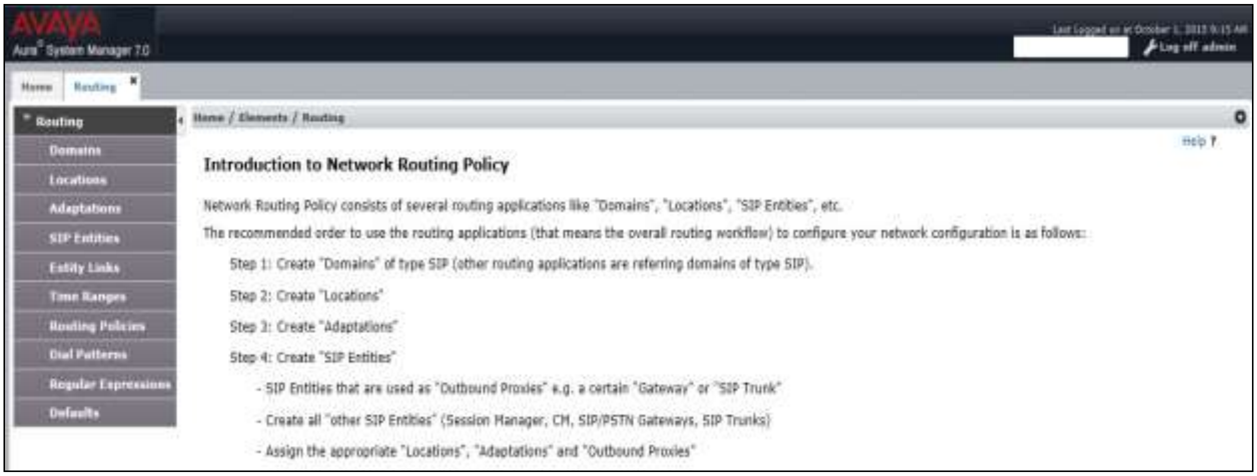
6.1. Log in to Avaya Aura® System Manager

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.



©2016 Avaya Inc. All Rights Reserved.

Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown above to bring up the **Introduction to Network Routing Policy** screen.



6.2. Administer SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. Expand **Elements → Routing** and select **Domains** from the left navigation menu, click **New** (not shown)**.** Enter the following values and use default values for remaining fields.

- **Name** Enter a Domain Name**.** In the sample configuration, **avaya.com** was used.
- **Type** Verify **SIP** is selected.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.

©2016 Avaya Inc. All Rights Reserved.

6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

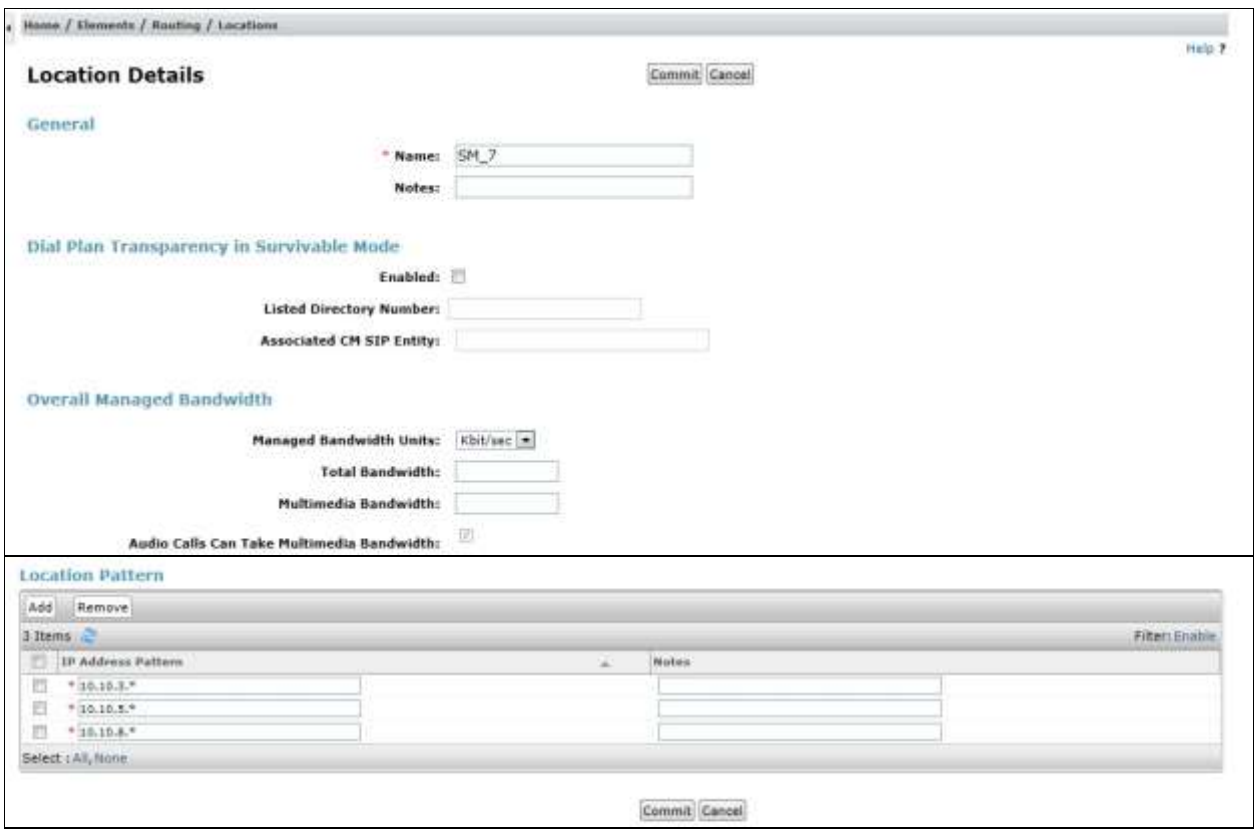
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity.

In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screenshot below shows the Location **SM_7** defined for the compliance testing.



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. In order to improve interoperability with third party elements, Session Manager 7.0 incorporates the ability to use Adaptation modules to remove specific SIP headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements

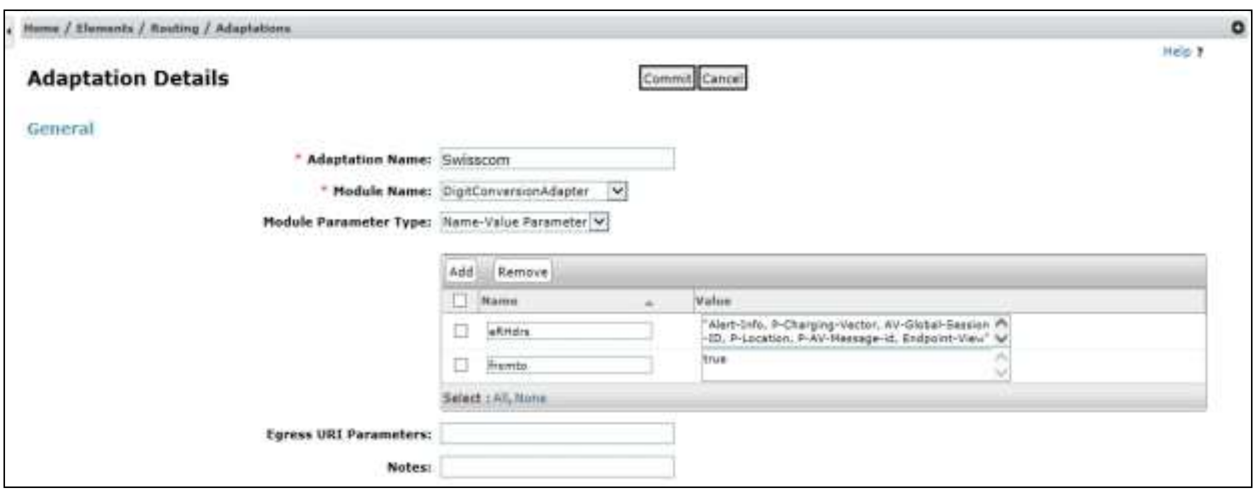
For the compliance test, an Adaptation named "**Swisscom**" was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, and P-Location. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

To add an adaptation, under the **Routing** tab select **Adaptations** on the left hand menu and then click on the **New** button (not shown). Under **Adaptation Details** →**General**:

- **Adaption Name**: Enter an appropriate name such as **Swisscom**.
- **Module Name**: Select **DigitConversionAdapter**.
- **Modular Parameter Type**: Select **Name-Value Parameter**.

Click Add to add the name and value parameters.

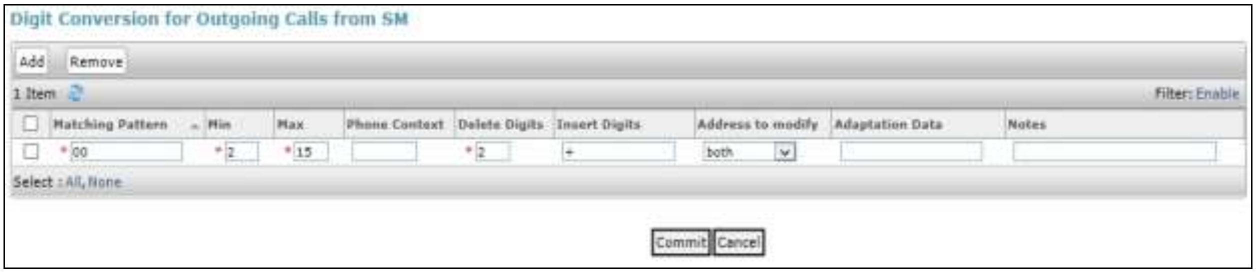
- **Name**: Enter **eRHdrs**. This parameter will remove the specific headers from messages in the egress direction.
- **Value**: Enter **AV-Global-Session-ID**, **AV-Correlation-ID**, **Alert-Info**, **Endpoint-View**, **P-AV-Message-ID**, **P-Charging-Vector**, **P-Location**.
- **Name**: Enter **fromto**. Modifies From and To header of a message.
- **Value**: Enter **true**.



©2016 Avaya Inc. All Rights Reserved.

Scroll down the page and under **Digit Conversion for Outgoing Calls to SM**, click the **Add** button and specify the digit manipulation to be performed as follows:

- Enter the leading digits that will be matched in the Matching Pattern field.
- In the **Min** and **Max** fields set the minimum and maximum digits allowed in the digit string to be matched.
- In the **Delete Digits** field enter the number of leading digits to be removed.
- In the **Insert Digits** field specify the digits to be prefixed to the digit string.
- In the **Address to modify** field specify the digits to manipulate by the adaptation. In this configuration the dialed number is the target so **both** have been selected.



This will ensure any outbound numbers will have the 00 digits removed and + digit inserted to convert to E.164 format before being presented to the Swisscom VoIP Gate.

©2016 Avaya Inc. All Rights Reserved.

6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to 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 **SIP Trunk** for the Avaya SBCE 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.

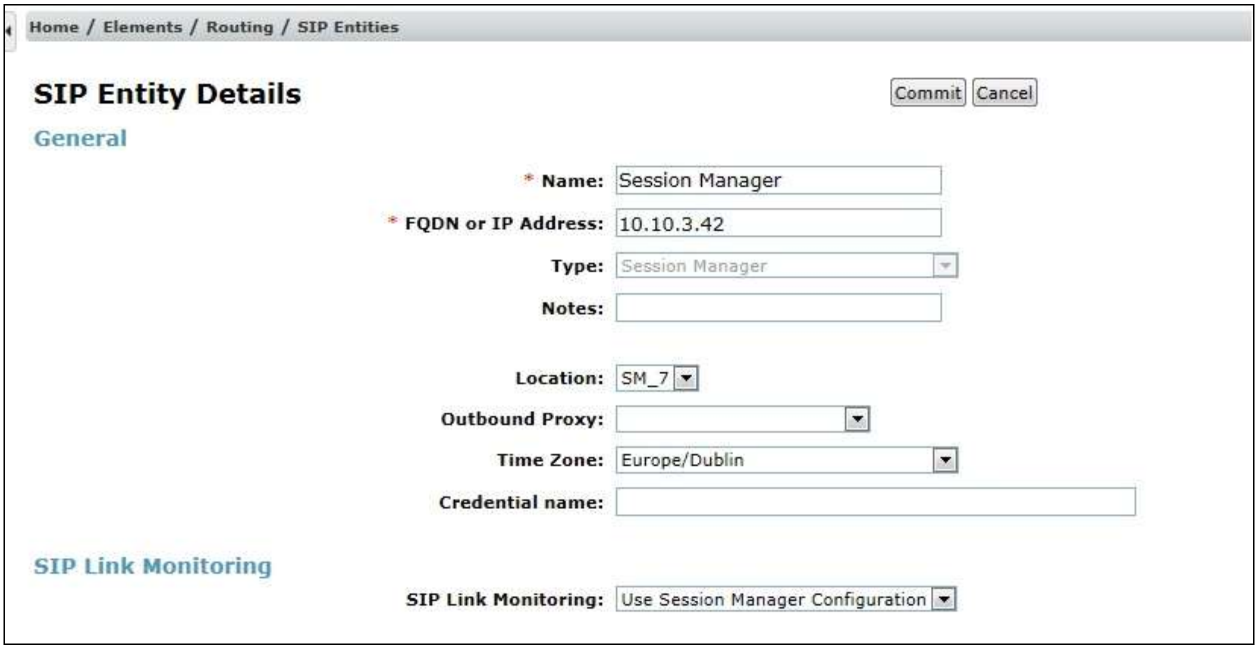
In this configuration there are three SIP Entities.

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Avaya SBCE SIP Entity

©2016 Avaya Inc. All Rights Reserved.

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 and **Type** is **Session Manager**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.



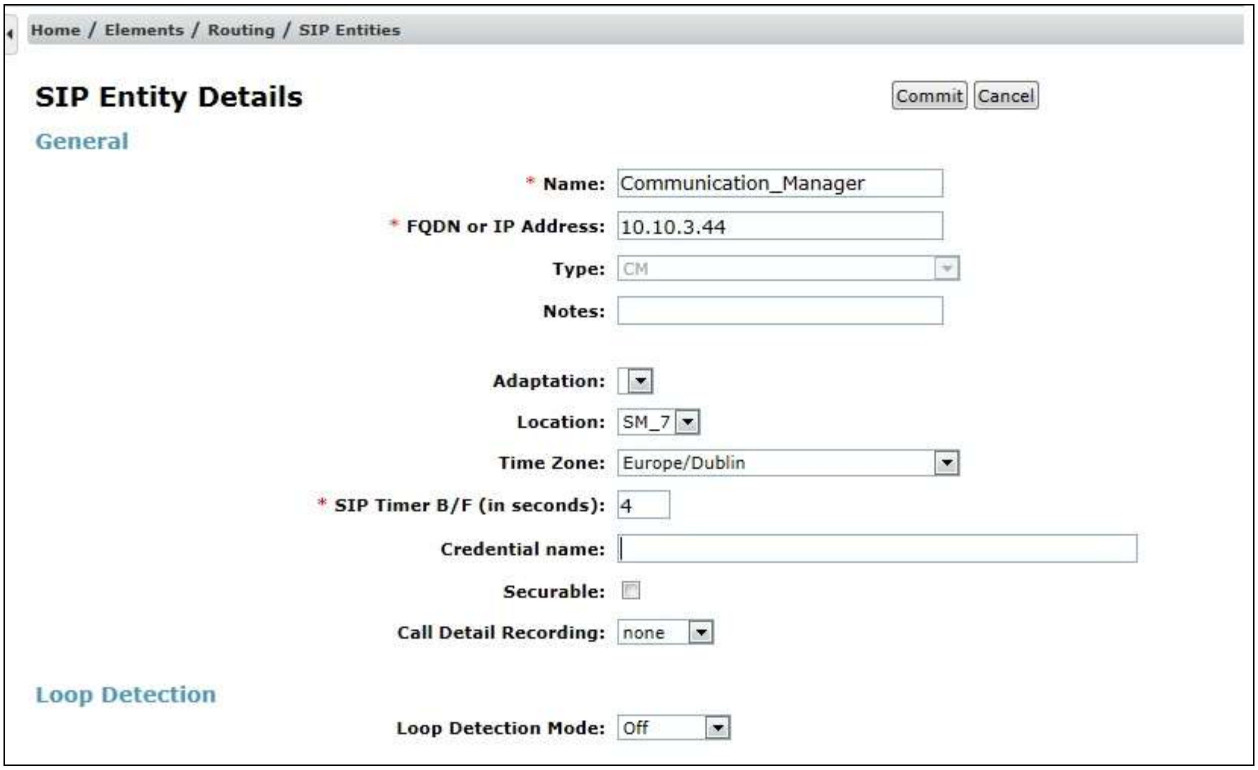
Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- 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 the domain added in **Section 6.2** as the default domain.

©2016 Avaya Inc. All Rights Reserved.

6.5.1.1 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 and **Type** is **CM**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

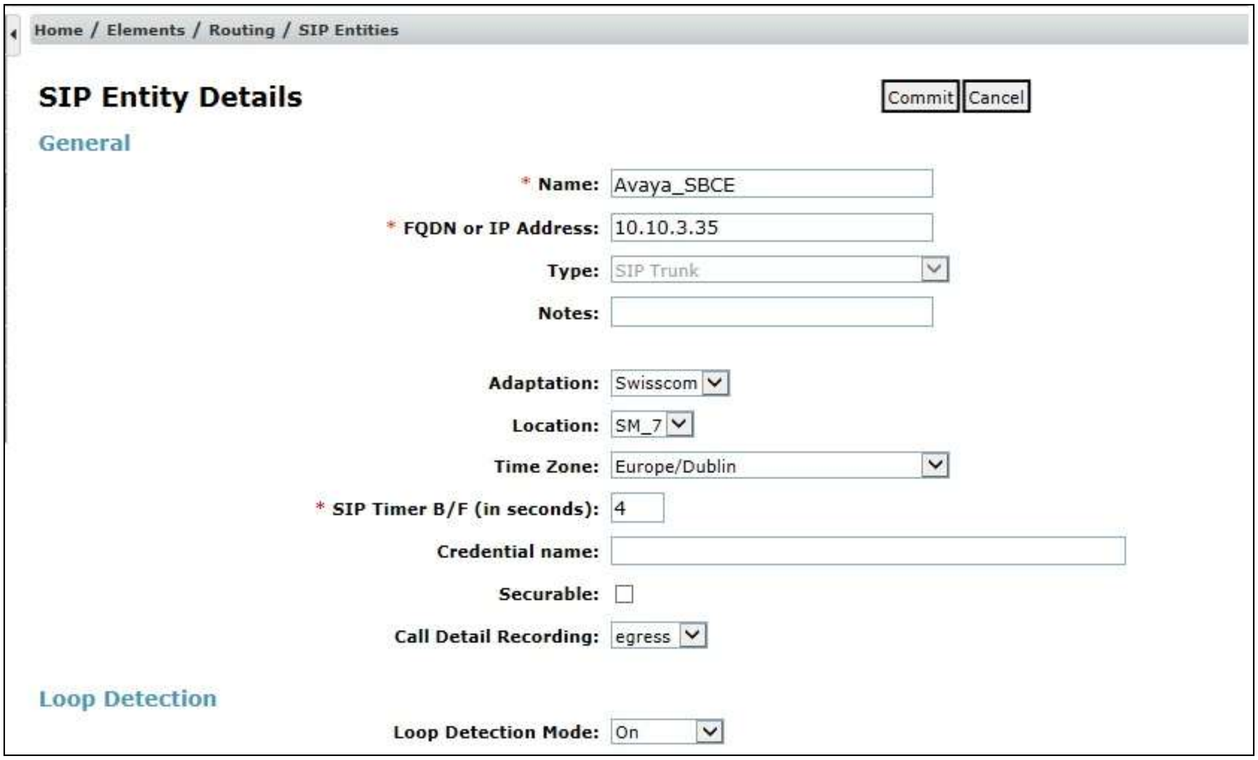


Other parameters can be set for the SIP Entity as shown in the following screenshot, but for test, these were left at default values.

©2016 Avaya Inc. All Rights Reserved.

6.5.2. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set **Type** to **SIP Trunk**. Set **Adaptation** to the adaptation defined in **Section 6.4**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.



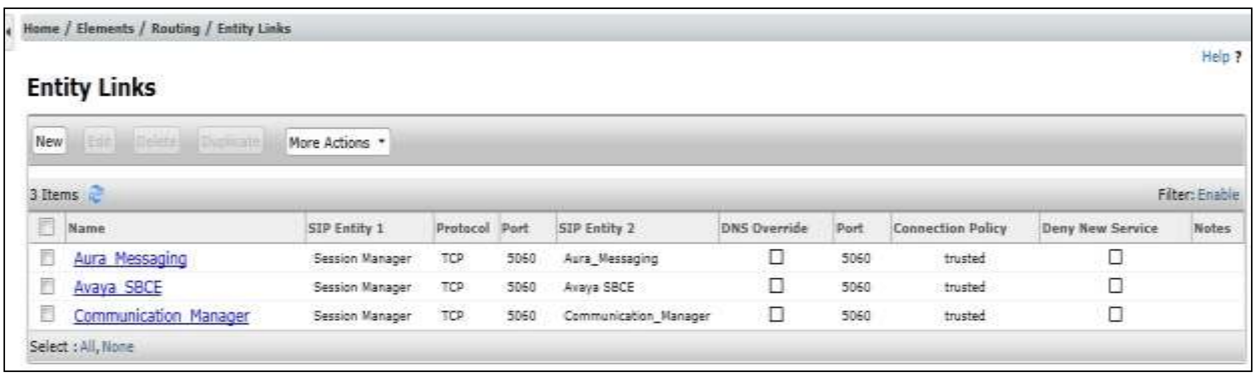
©2016 Avaya Inc. All Rights Reserved.

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 **Protocol** field enter the transport protocol to be used to send SIP requests.
- 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 **Trusted** from the drop-down menu to make the other system trusted.

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



Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
Aura_Messaging	Session Manager	TCP	5060	Aura_Messaging	☐	5060	trusted	☐	
Avaya_SBCE	Session Manager	TCP	5060	Avaya SBCE	☐	5060	trusted	☐	
Communication_Manager	Session Manager	TCP	5060	Communication_Manager	☐	5060	trusted	☐	

©2016 Avaya Inc. All Rights Reserved.

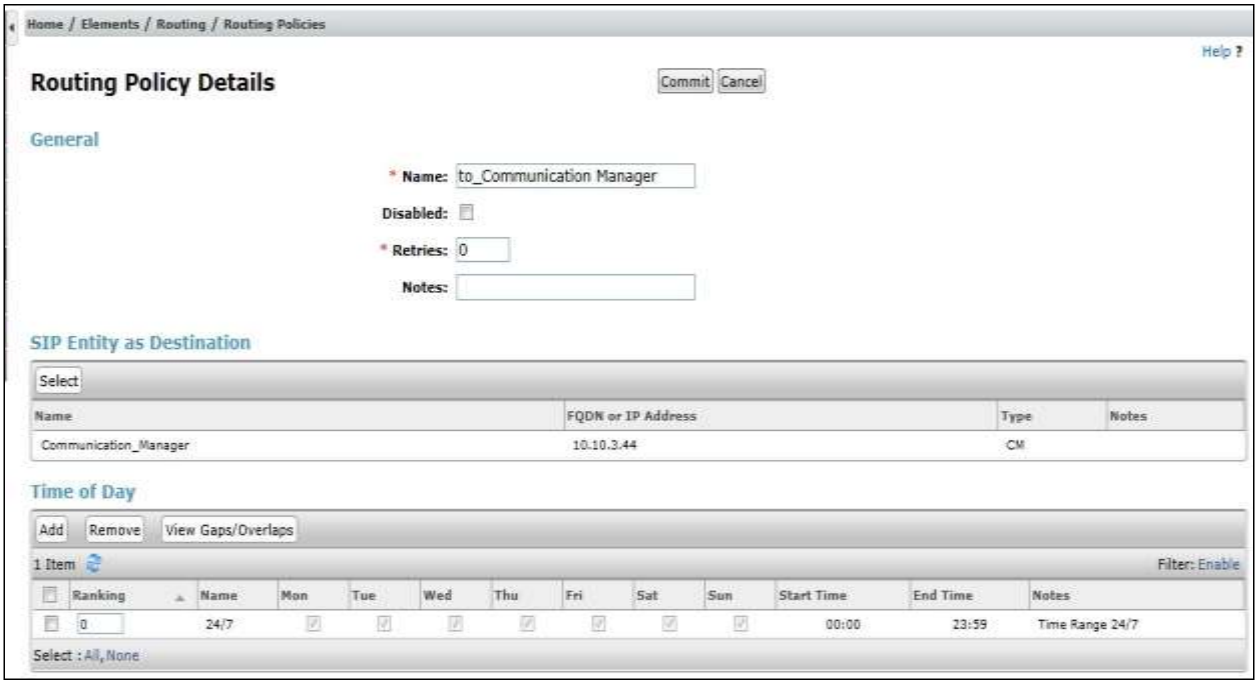
6.7. Administer Routing Policies

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**:

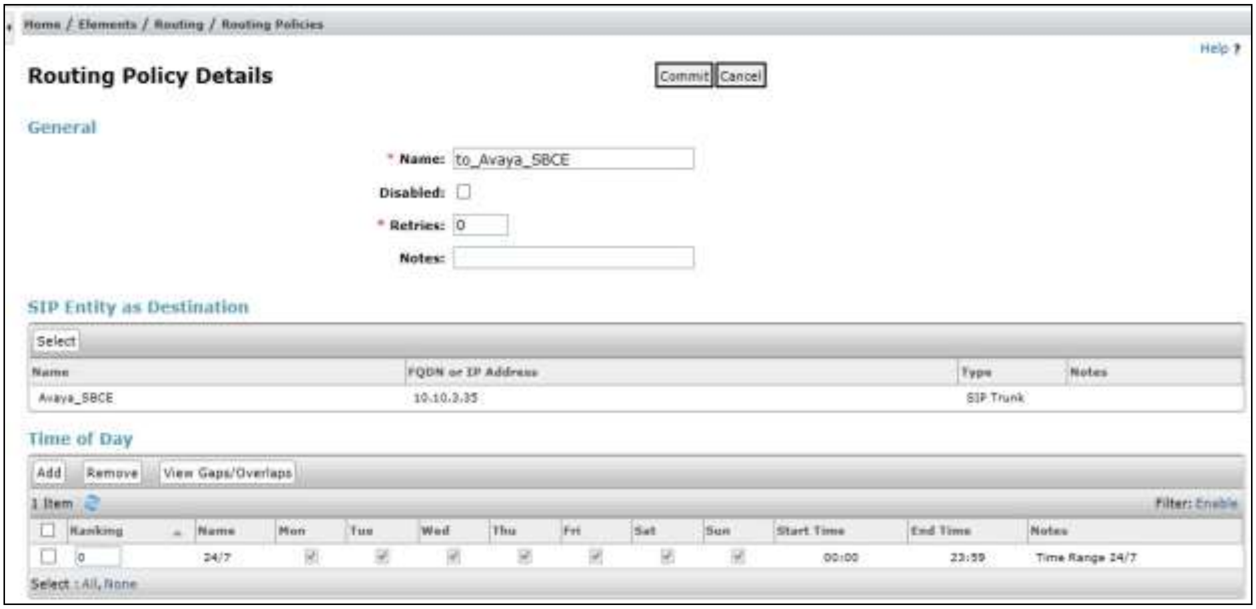
- Enter an informative name in the **Name** field.
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies.
- Under **Time of Day**, click **Add**, and then select the time range.

The following screen shows the routing policy for Communication Manager.



©2016 Avaya Inc. All Rights Reserved.

The following screen shows the Routing Policy for the Avaya SBCE.



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**:

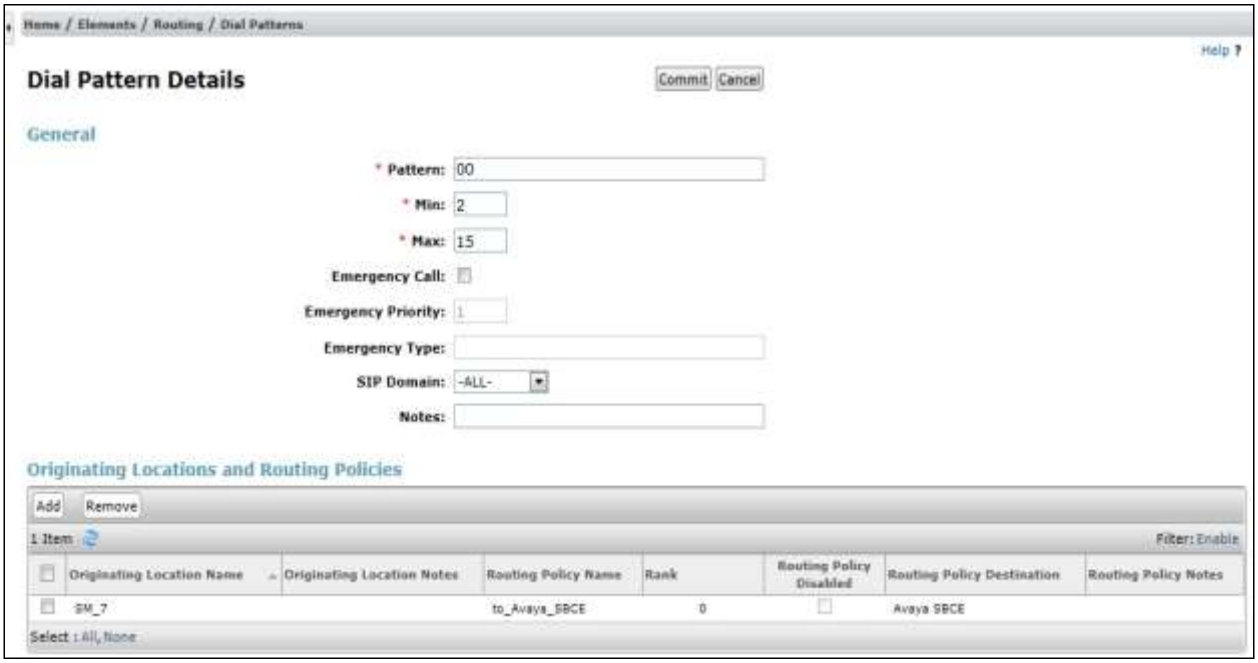
- In the **Pattern** field enter a dialled number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialled number.
- In the **Max** field enter the maximum length of the dialled number.
- In the **SIP Domain** field select **ALL** or alternatively one of those configured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

Under **Originating Locations and Routing Policies**:

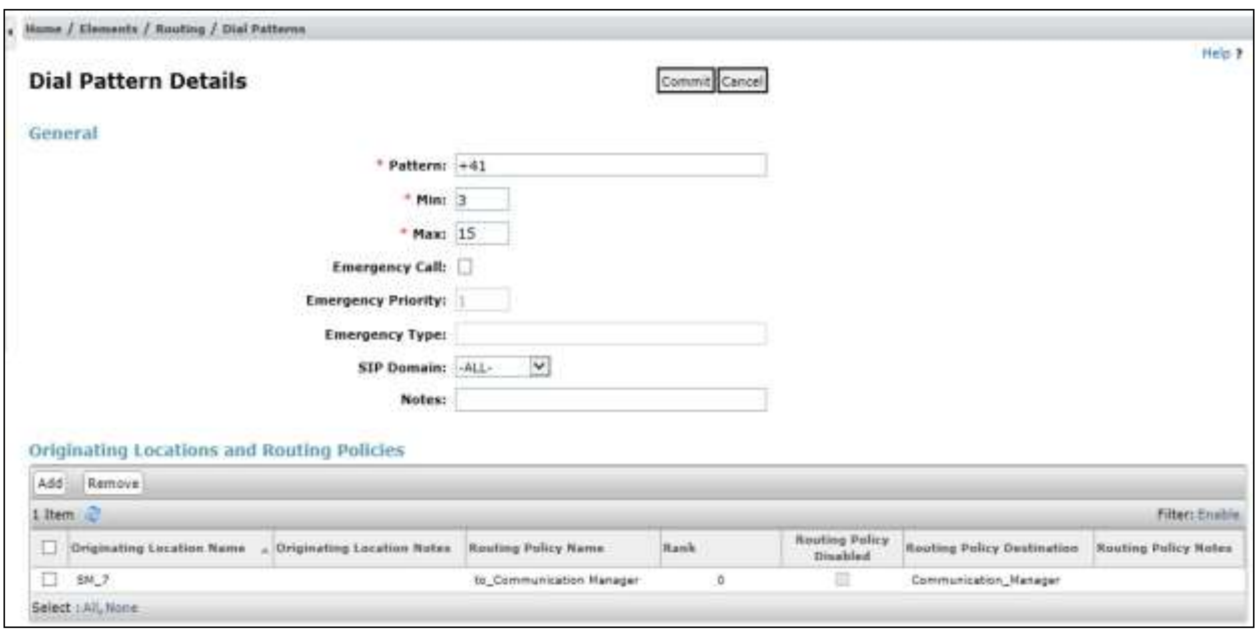
- Click **Add**, in the resulting screen (not shown).
- Under **Originating Location**, select the location defined in **Section 6.3** or **ALL**.
- Under **Routing Policies** select one of the routing policies defined in **Section 6.7**.
- Click **Select** button to save.

©2016 Avaya Inc. All Rights Reserved.

The following screen shows an example dial pattern configured for the Avaya SBCE.



The following screen shows the test dial pattern configured for Communication Manager.



©2016 Avaya Inc. All Rights Reserved.

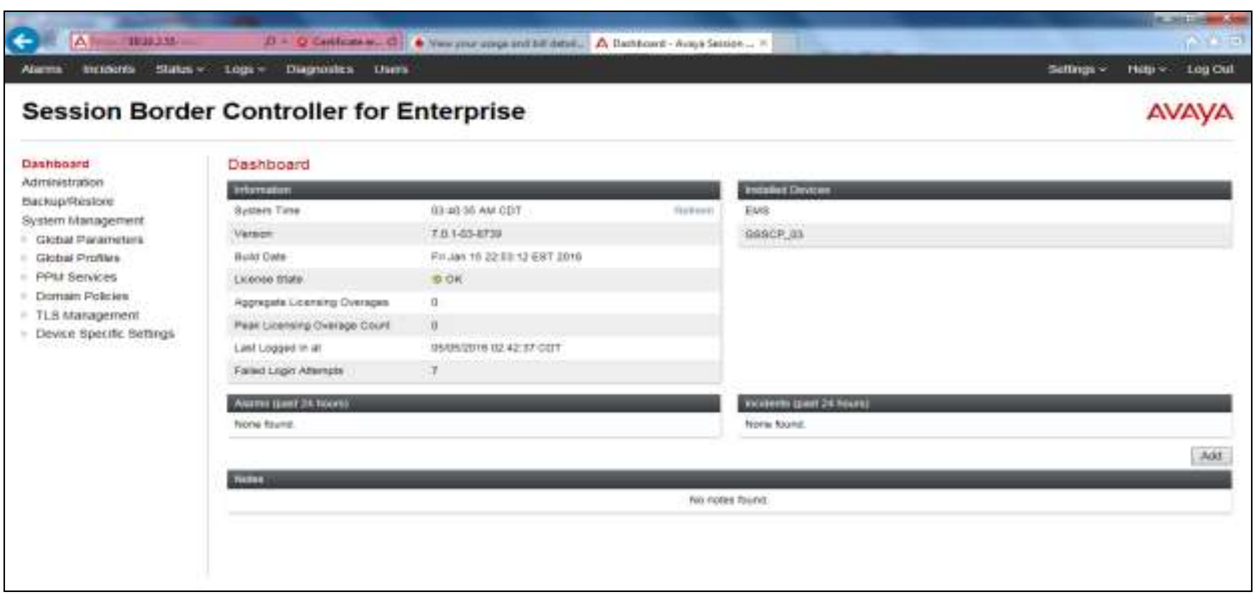
7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

7.1. Accessing Avaya Session Border Controller for Enterprise

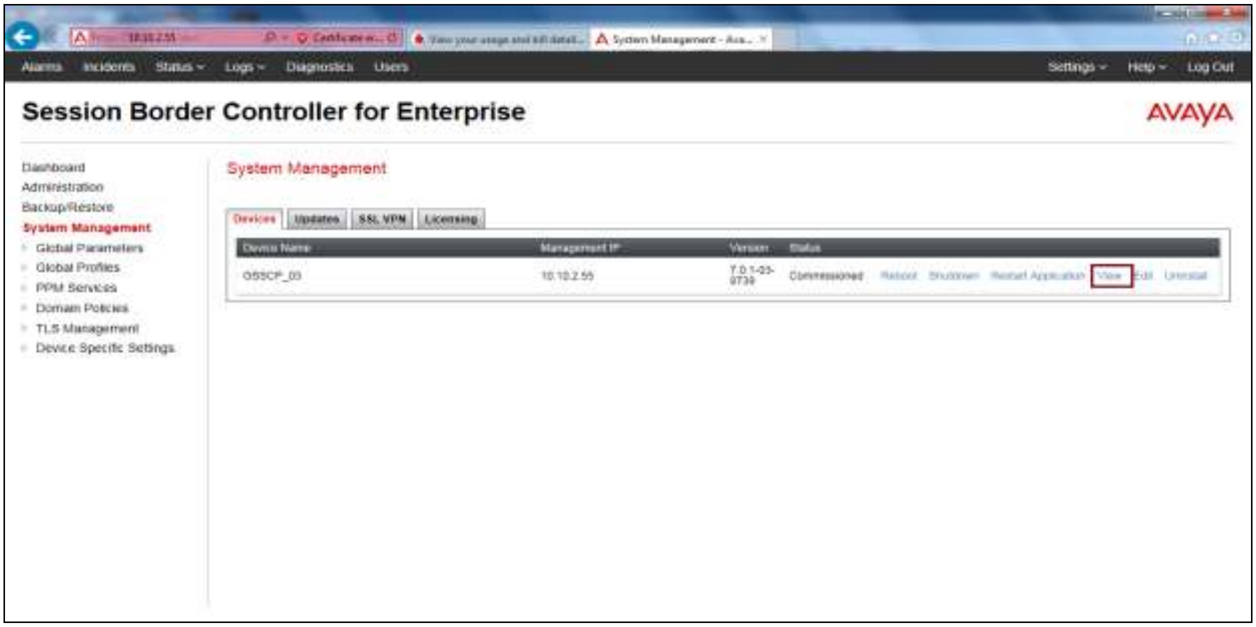
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.

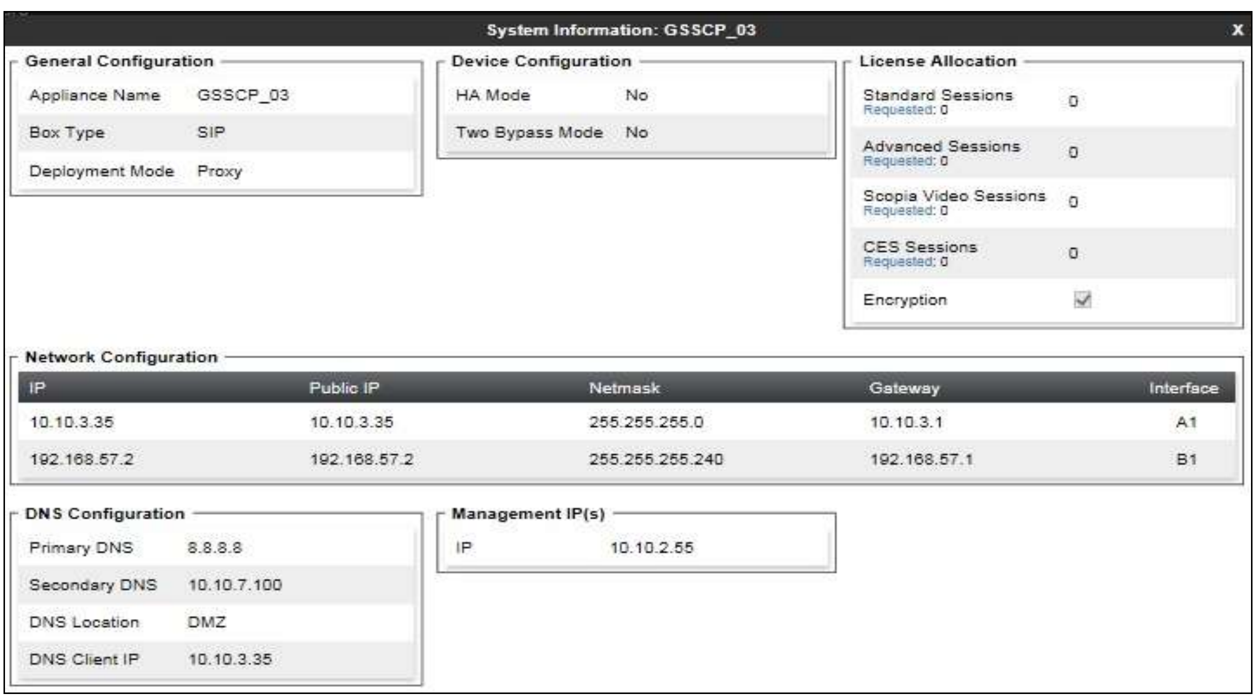


©2016 Avaya Inc. All Rights Reserved.

To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP-03** is shown. To view the configuration of this device, click **View** (the third option from the right).



The **System Information** screen shows the **General Configuration**, **Device Configuration**, **License Allocation**, **Network Configuration**, **DNS Configuration** and **Management IP** information.



©2016 Avaya Inc. All Rights Reserved.

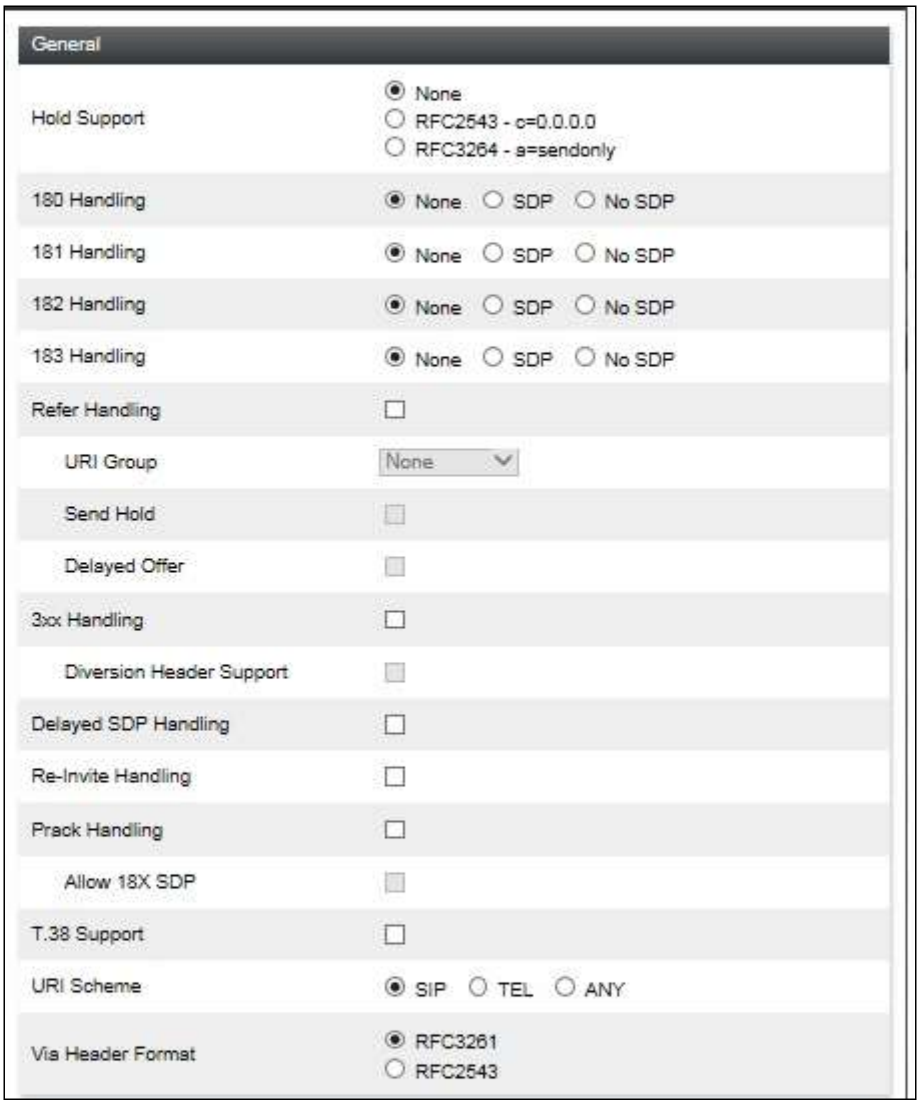
7.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.2.1. Server Interworking Avaya

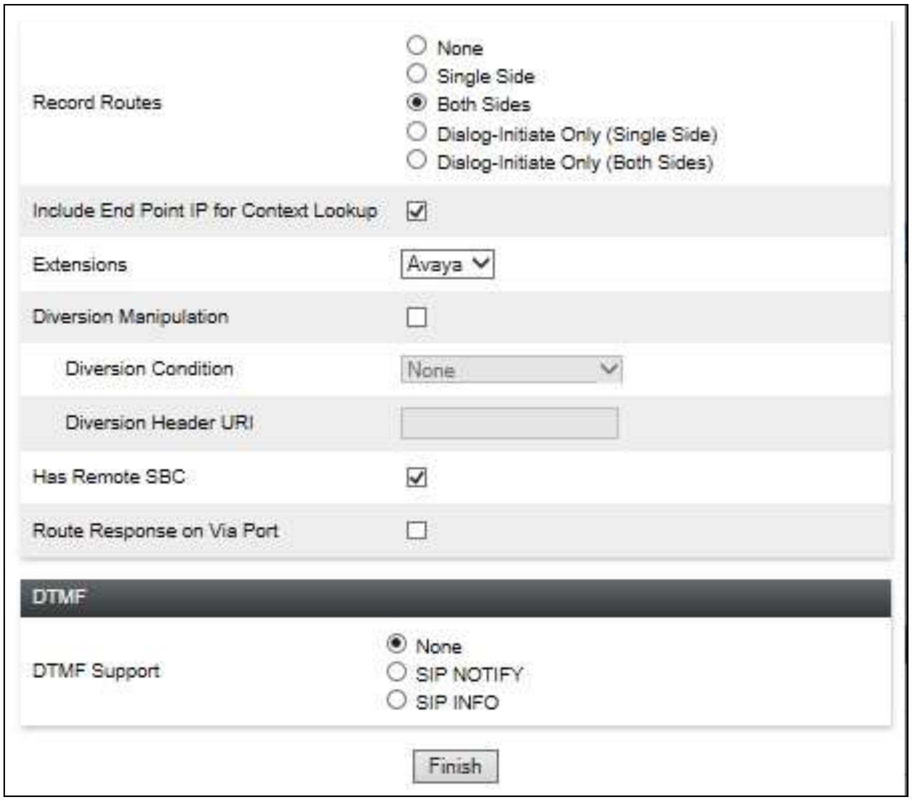
Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles → Server Interworking** and click on **Add**.

- Enter profile name such as Avaya and click **Next** (Not Shown).
- Check **Hold Support = None**.
- All other options on the **General** Tab can be left at default.



©2016 Avaya Inc. All Rights Reserved.

Default values can be used for the **Advanced Settings** window. Click **Finish**.



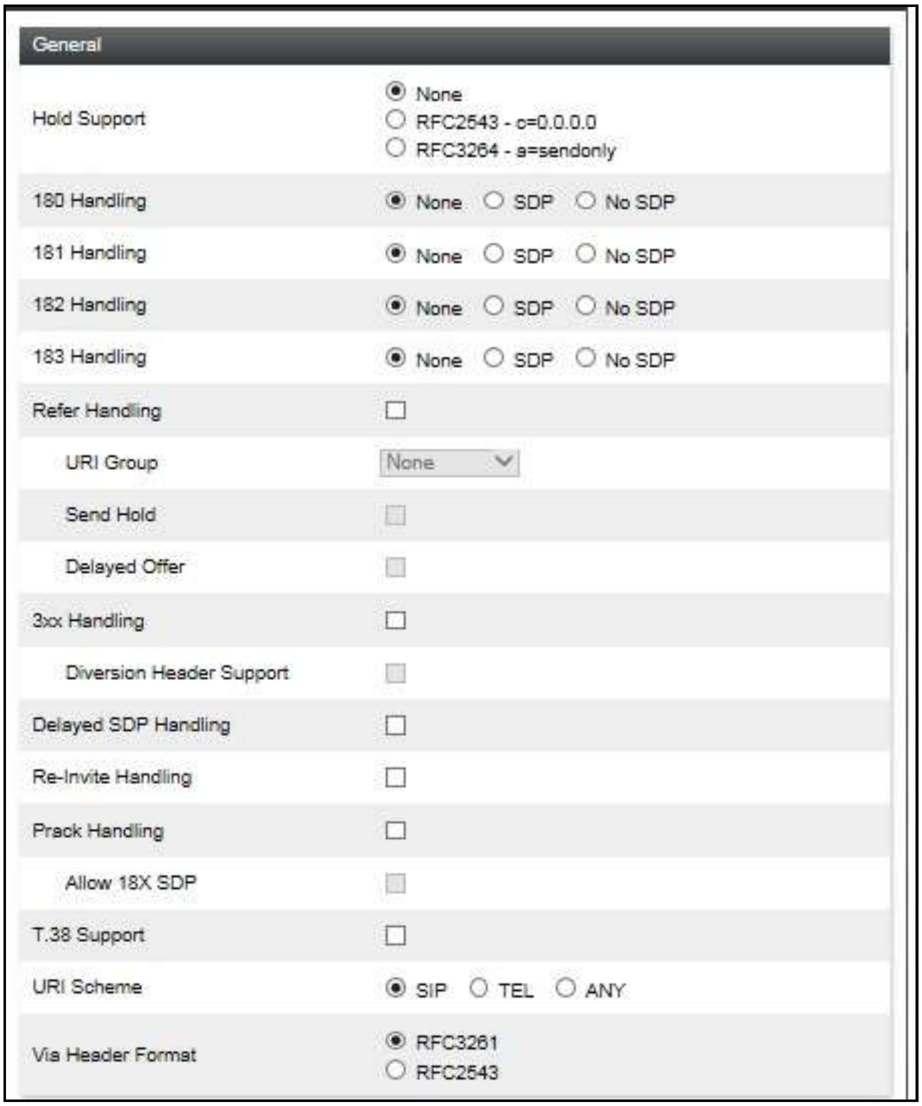
©2016 Avaya Inc. All Rights Reserved.

7.2.2. Server Interworking – Swisscom

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles → Server Interworking** and click on **Add**.

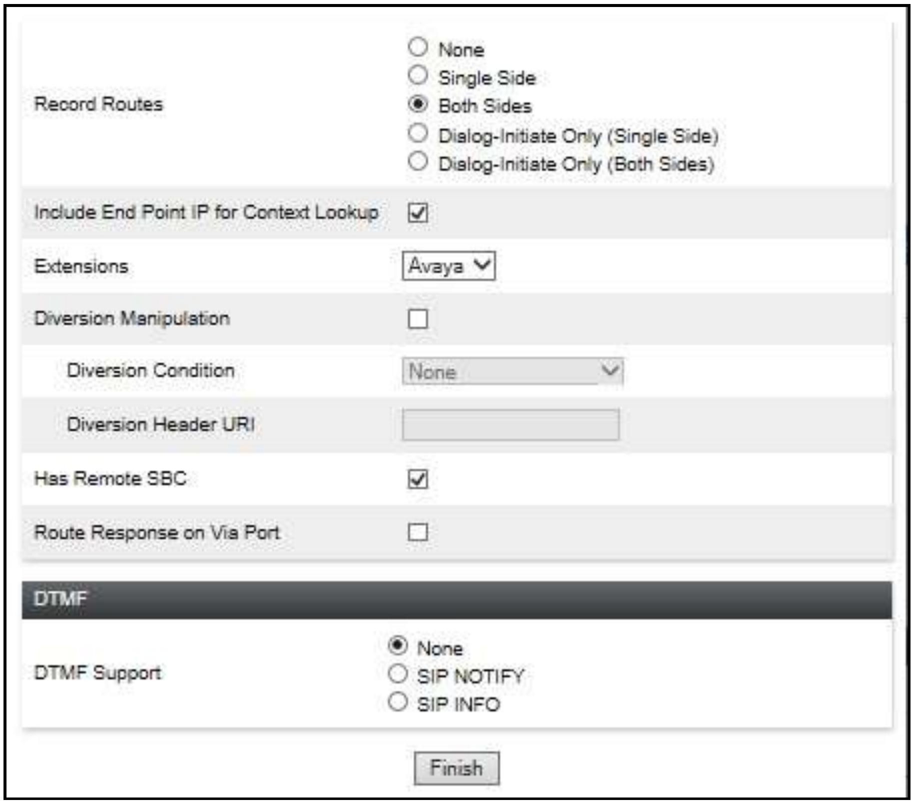
- Enter profile name such as Swisscom and click **Next** (Not Shown).
- Check **Hold Support = None**.
- All other options on the **General** Tab can be left at default.

Click on **Next** on the following screens.



©2016 Avaya Inc. All Rights Reserved.

Default values can be used for the **Advanced Settings** window. Click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

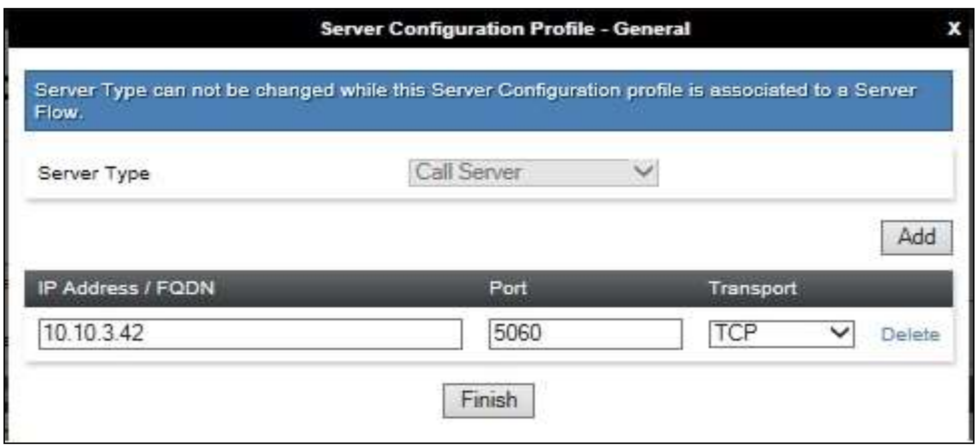
7.2.3. Server Configuration– Avaya

Servers are defined for each server connected to the Avaya SBCE. In this case, Swisscom is connected as the Trunk Server and Session Manager is connected as the Call Server.

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow the configuration and management of various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signalling parameters and some advanced options.

From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

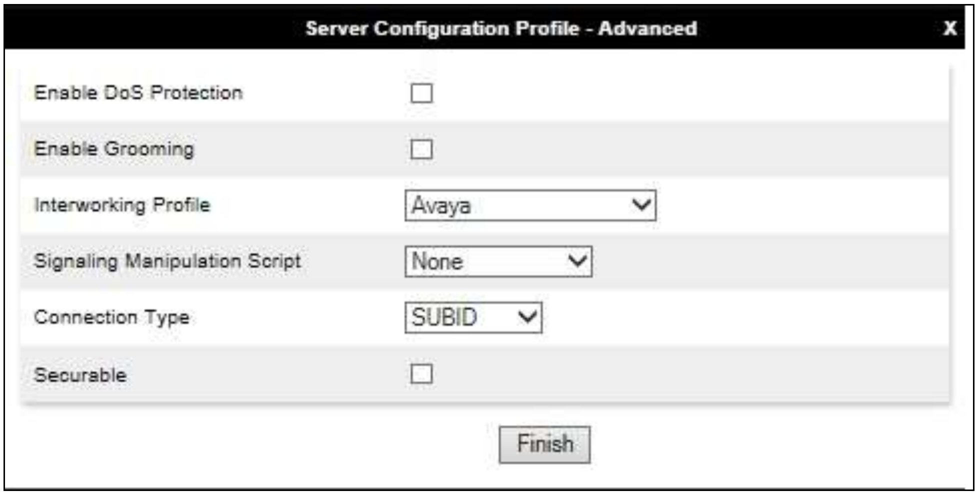
- Select **Server Type** to be **Call Server**.
- Enter **IP Address / FQDN** to **10.10.3.42** (Session Manager IP Address).
- For **Port**, enter **5060**.
- For **Transport,** select **TCP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



©2016 Avaya Inc. All Rights Reserved.

On the **Advanced** tab:

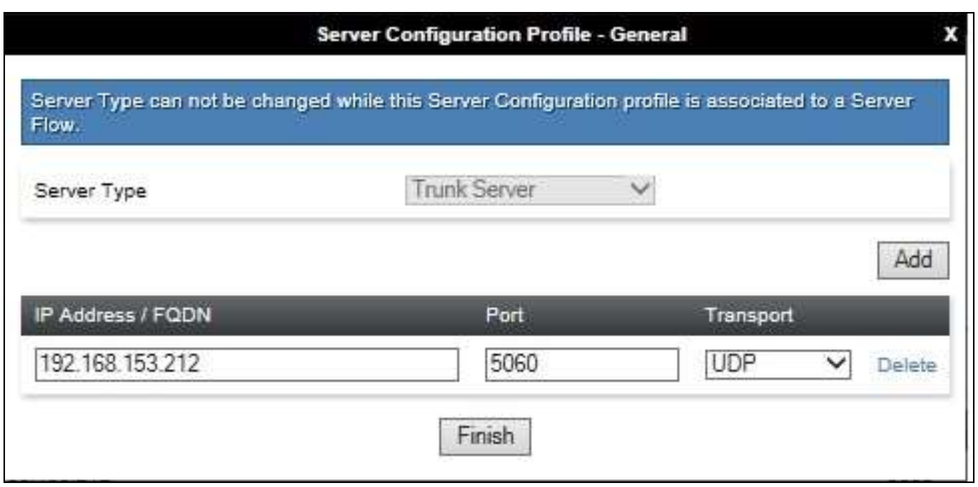
- Select **Avaya** for **Interworking Profile**.
- Click **Finish**.



7.2.4. Server Configuration – Swisscom

To define the Swisscom SBC as a Trunk Server, navigate to **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

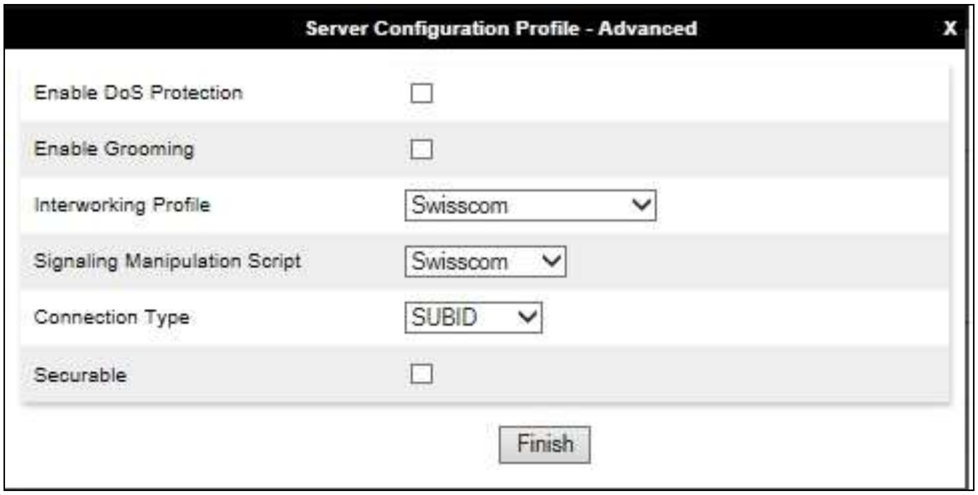
- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **192.168.153.212** (Swisscom SBC IP Address).
- For **Port**, enter **5060**.
- For **Transport,** select **UDP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



©2016 Avaya Inc. All Rights Reserved.

On the Advanced tab:

- Select **Swisscom** for Interworking Profile.
- Select **Swisscom** for **Signaling Manipulation Script** as defined in **Section 7.2.7**.
- Click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

7.2.5. Routing

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

Routing information is required for routing to Session Manager on the internal side and Swisscom addresses 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.

7.2.5.1 Routing – Avaya

Create a Routing Profile for Session Manager.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

The Routing Profile window will open. Use the default values displayed and click **Add**.

©2016 Avaya Inc. All Rights Reserved.

On the **Next Hop Address** window, set the following:

- **Priority/Weight** = **1**.
- **Server Configuration** = **Avaya** (**Section 7.2.3**) from drop down menu.
- **Next Hop Address** = Select **10.10.3.42:5060 TCP** from drop down menu.
- Click **Finish**.

7.2.5.2 Routing – Swisscom

Create a Routing Profile for Swisscom.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

©2016 Avaya Inc. All Rights Reserved.

The Routing Profile window will open. Use the default values displayed and click **Add**.

On the **Next Hop Address** window, set the following:

- **Priority/Weight** = **1**.
- **Server Configuration** = **Swisscom** (**Section 7.2.4**) from drop down menu.
- **Next Hop Address** = Select **192.168.153.212:5060 UDP** from drop down menu.
- Click **Finish**.

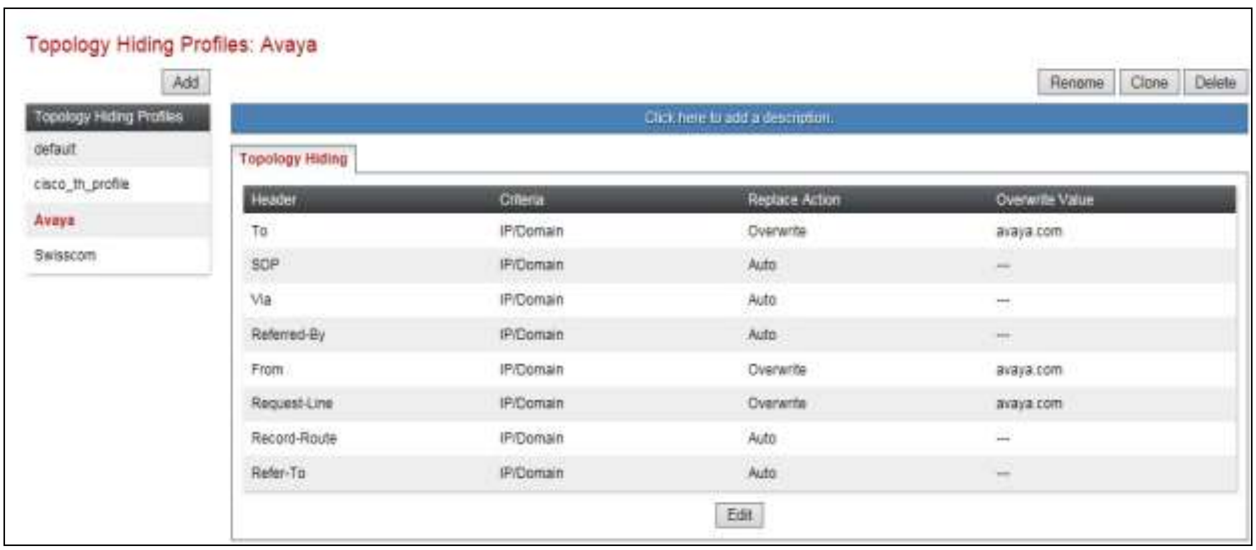
©2016 Avaya Inc. All Rights Reserved.

7.2.6. 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 with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for Session Manager, navigate to **Global Profiles → Topology Hiding** from menu on the left hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

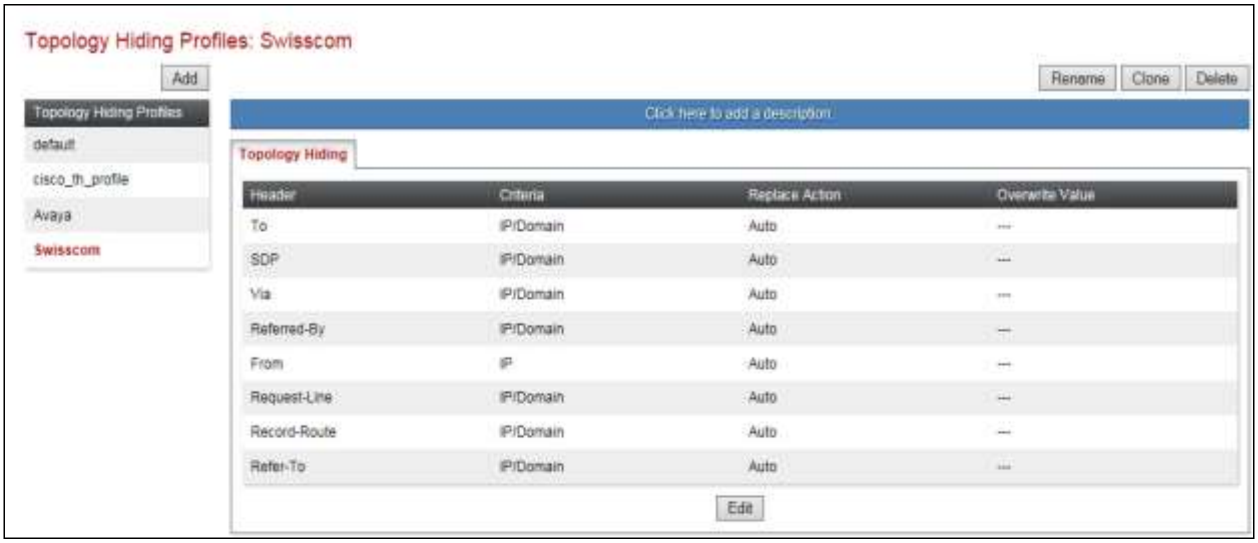
- Enter a descriptive Profile Name such as **Avaya**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **avaya.com**.
- Click **Finish** (not shown).



©2016 Avaya Inc. All Rights Reserved.

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

- In the **Profile Name** field enter a descriptive name for Swisscom and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Auto** under **Replace Action**.
- Click **Finish** (not shown).



7.2.7. Signalling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa. The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE

During compliance testing, an issue was also found with the handling of an Avaya specific parameter in the Contact Header. The Avaya proprietary parameter "+avaya-cm-keep-mpro=no" is present when Initial IP-IP Direct Media is enabled on Communication Manager SIP Trunk. A script was required to remove the proprietary parameter "+avaya-cm-keep-mpro" from the Contact Header.

©2016 Avaya Inc. All Rights Reserved.

To define the signalling manipulation to delete bandwidth attributes from the SDP and the Avaya proprietary parameter from the Contact Header, navigate to **Dashboard → Global Profiles → Signaling Manipulation** and click on **Add** and enter a title. A new blank SigMa Editor window will pop up. The script text is as follows:

```
/*Script to remove attribute (+avaya-cm-keep-mpro) from Contact Header */

within session "INVITE"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
       if (exists(%HEADERS["Contact"][1].PARAMS["+avaya-cm-keep-mpro"])) then
        {
           remove(%HEADERS["Contact"][1].PARAMS["+avaya-cm-keep-mpro"]);
            }
        }
    }
```

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

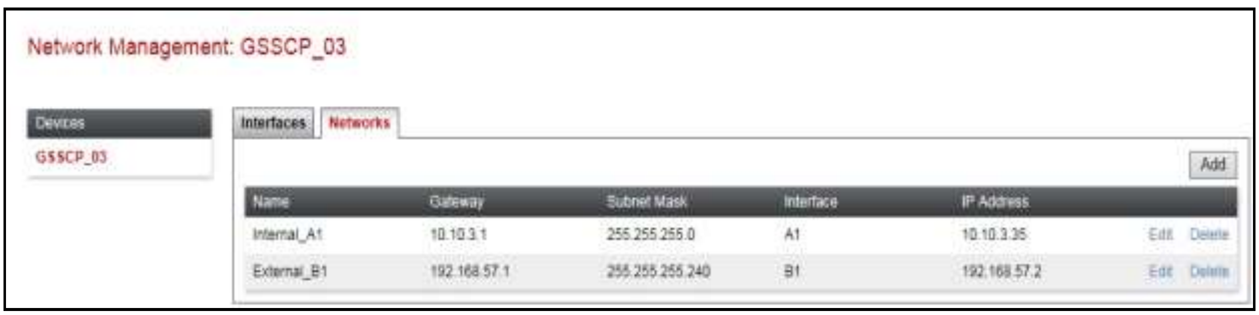
©2016 Avaya Inc. All Rights Reserved.

7.3. Define Network Information

Network information is required on the Avaya SBCE 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 Avaya SBCE can have only one interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** from the menu on the left-hand side and click on **Add**. 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** to save the information.
- Click on **Add**.
- Define the external IP address with screening mask and assign to interface **B1.**
- Select **Save** to save the information.
- Click on **System Management** in the main menu.
- Select **Restart Application** indicated by an icon in the status bar (not shown).



Select the **Interface Configuration** Tab and use the **Toggle** button to enable the interfaces.

©2016 Avaya Inc. All Rights Reserved.

7.4. Define Interfaces

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

7.4.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings → Signaling Interface** from the menu on the left hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

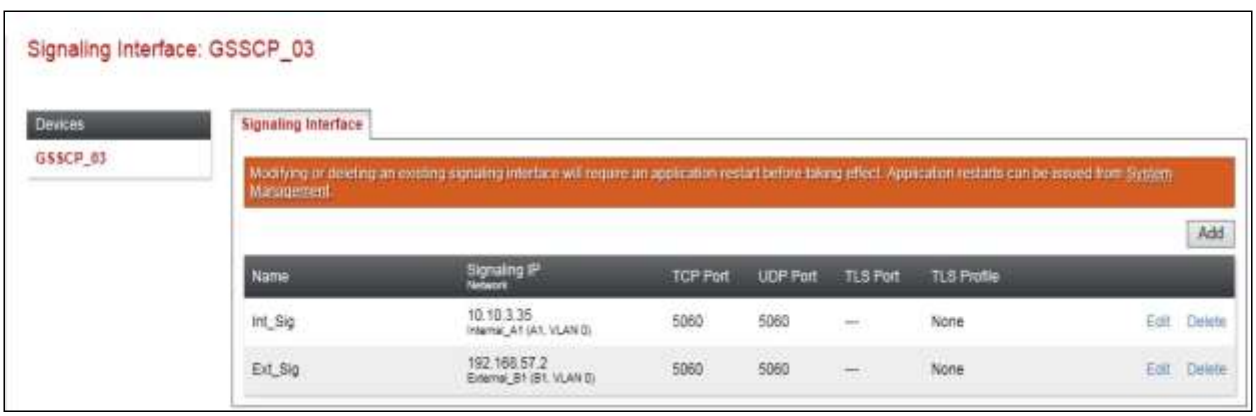
To enter details of transport protocol and ports for the SIP signalling on the internal interface:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- For **Signaling IP**, select the **internal** signalling interface IP addresses defined in **Section 7.3**.
- Select **TCP** port number, **5060** is used for Session Manager.

To enter details of transport protocol and ports for the SIP signalling on the external interface:

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **Signaling IP**, select the **external** signalling interface IP address defined in **Section 7.3**.
- Select **UDP** port number, **5060** is used for the Swisscom VoIP Gate.

The following screen shows the Signalling Interfaces created in the sample configuration for the inside and outside IP interfaces.



  ©2016 Avaya Inc. All Rights Reserved.

7.4.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings → Media Interface** from the 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.

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings → Media Interface** from the 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.

To enter details of the media IP and RTP port range on the internal interface to be used in the server flow:

- 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.
- For **Media IP**, select the **internal** media interface IP address defined in **Section 7.3**.
- Select **RTP port** ranges for the media path with the enterprise end-points.

To enter details of the media IP and RTP port range on the external interface to be used in the server flow.

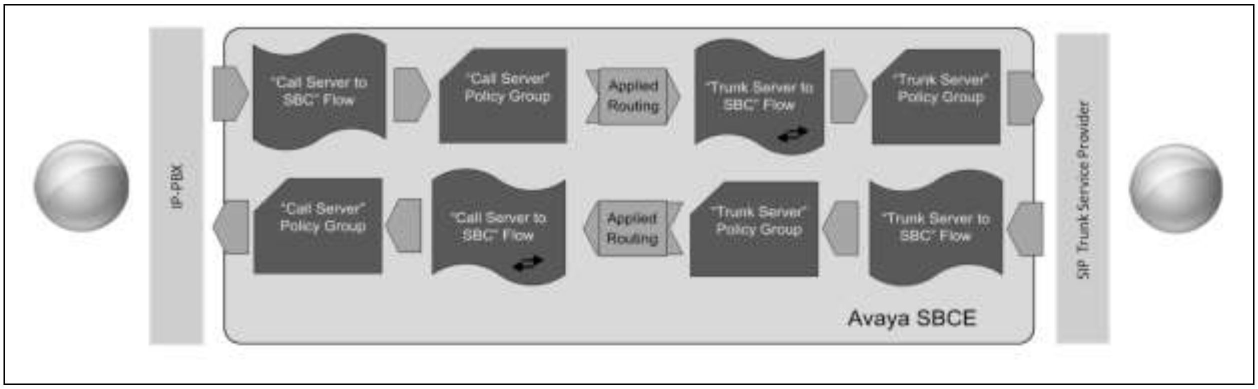
- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **Media IP**, select the **external** media interface IP address defined in **Section 7.3**.
- Select **RTP port** ranges for the external media path.

The following screen shows the Media Interfaces created in the sample configuration for the inside and outside IP interfaces.

©2016 Avaya Inc. All Rights Reserved.

7.5. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to Swisscom’s VoIP Gate and incoming flows from Swisscom s VoIP Gate to Session Manager. This configuration ties all the previously entered information together so that signalling can be routed from Session Manager to the PSTN via the Swisscom network and vice versa. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



This configuration ties all the previously entered information together so that calls can be routed from Session Manager to Swisscom VoIP Gate service and vice versa. The following screenshot shows all configured flows.

Subscriber Flows | Server Flows

Add

Hover over a row to see its description.

Server Configuration: Avaya

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Call_Server	*	Ext_Sig	Int_Sig	default-low	Swisscom	View	Clone	Edit	Delete

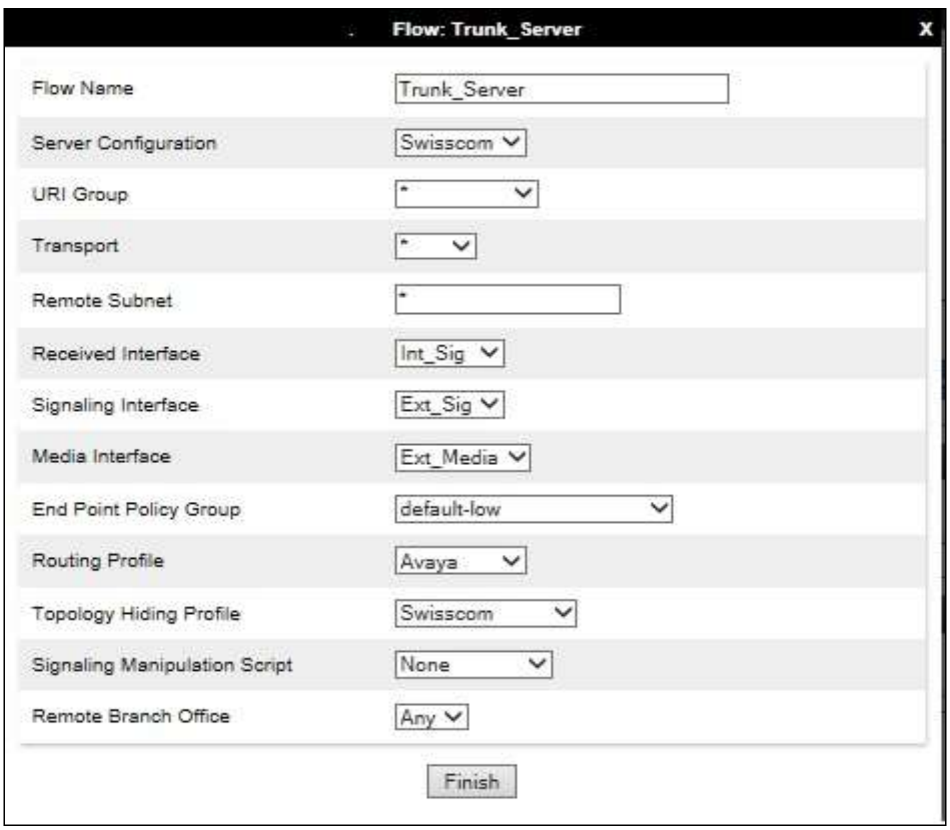
Server Configuration: Swisscom

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Trunk_Server	*	Int_Sig	Ext_Sig	default-low	Avaya	View	Clone	Edit	Delete

©2016 Avaya Inc. All Rights Reserved.

To define a Server Flow for the Swisscom VoIP Gate, navigate to **Device Specific Settings → End Point Flows**.

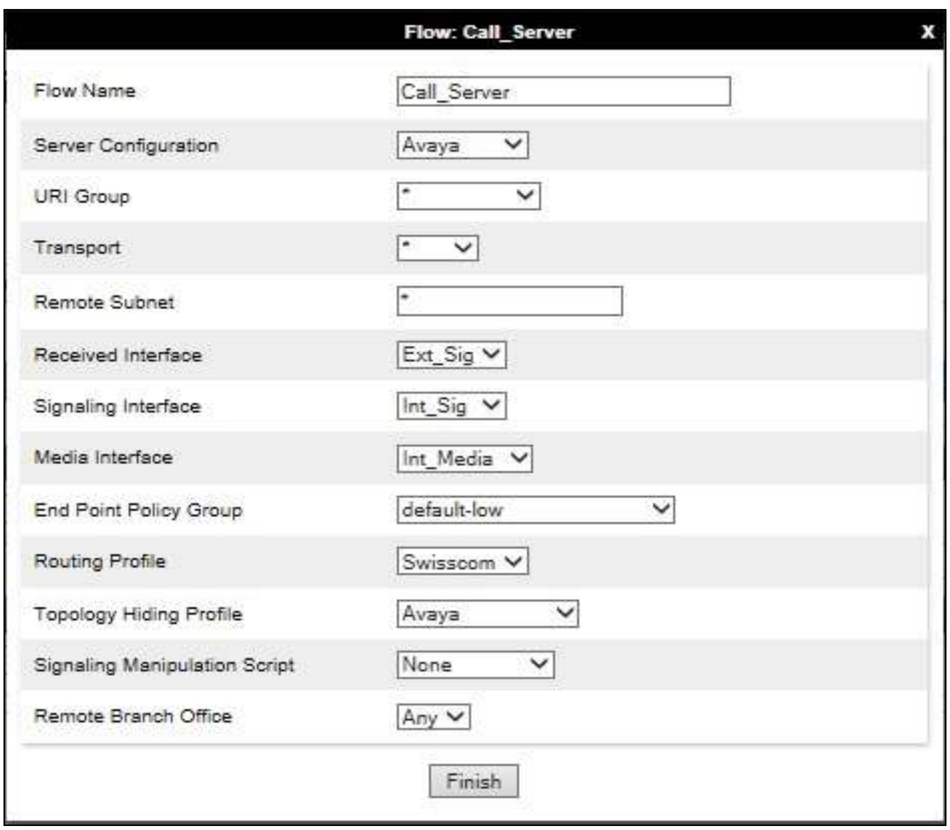
- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Swisscom VoIP Gate, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the Swisscom server configuration defined in **Section 7.2.4**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for the Swisscom VoIP Gate is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Swisscom VoIP Gate is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**. This is the interface that media bound for Swisscom VoIP Gate is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager Office defined in **Section 7.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Swisscom VoIP Gate defined in **Section 7.2.6** and click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

To define a Server Flow for Session Manager, 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 server flow for Session Manager, in the test environment **Call_Server** was used.
- In the **Server Configuration** drop-down menu, select the Session Manager server configuration defined in **Section 7.2.3**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Swisscom VoIP Gate defined in **Section 7.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.2.6** and click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

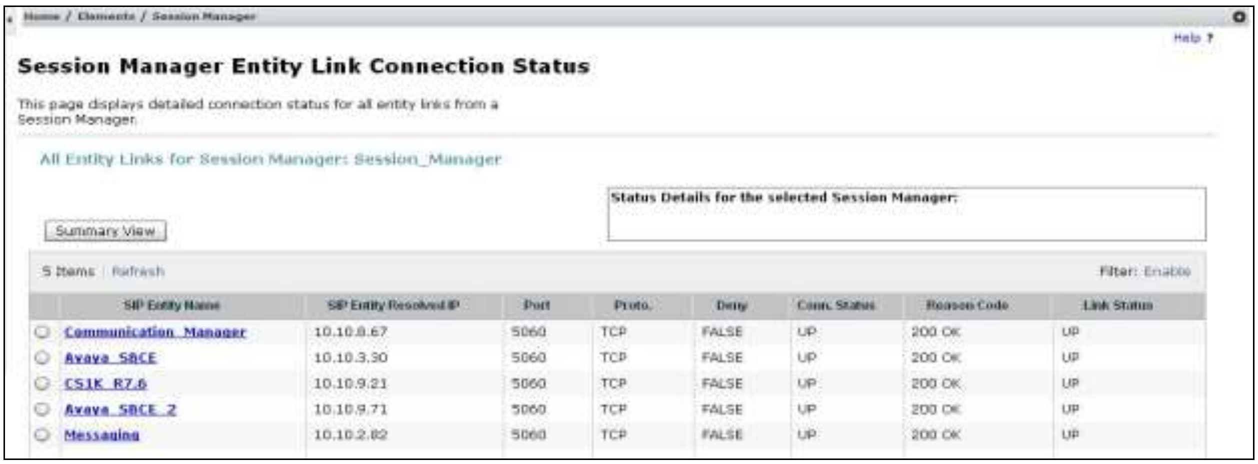
8. Swisscom VoIP Gate Service Configuration

The configuration of the Swisscom equipment used to support Swisscom's VoIP Gate service is outside of the scope of these Application Notes and will not be covered. To obtain further information on Swisscom equipment and system configuration please contact an authorized Swisscom 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 Entities 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**.

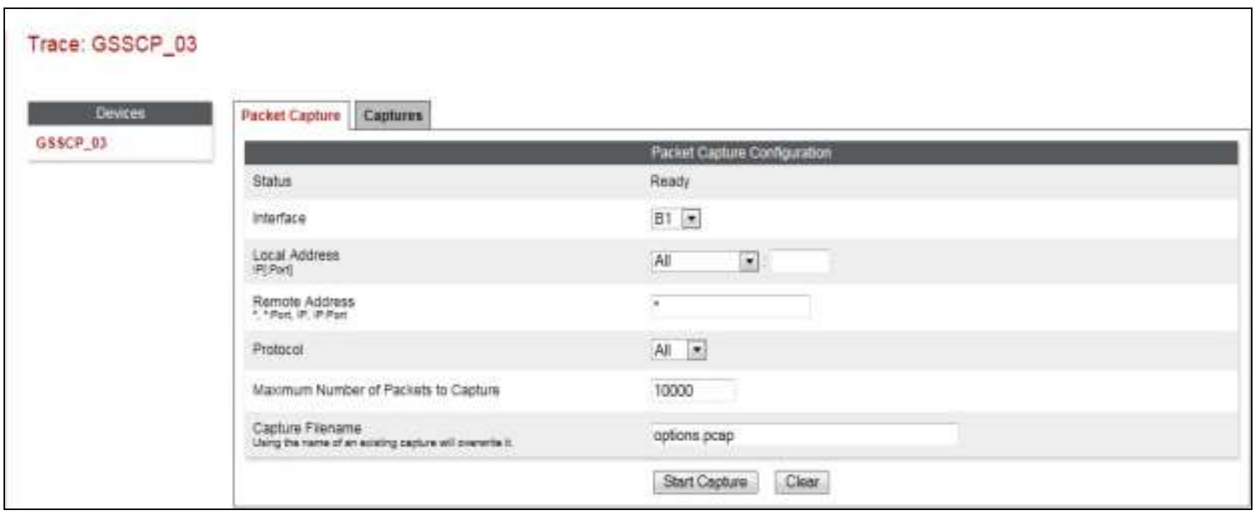
```
status trunk 1

                              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
```


©2016 Avaya Inc. All Rights Reserved.

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.
7. Should issues arise with the SIP trunk, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from Session Manager via the Avaya SBCE to the network SBCs are receiving a response.

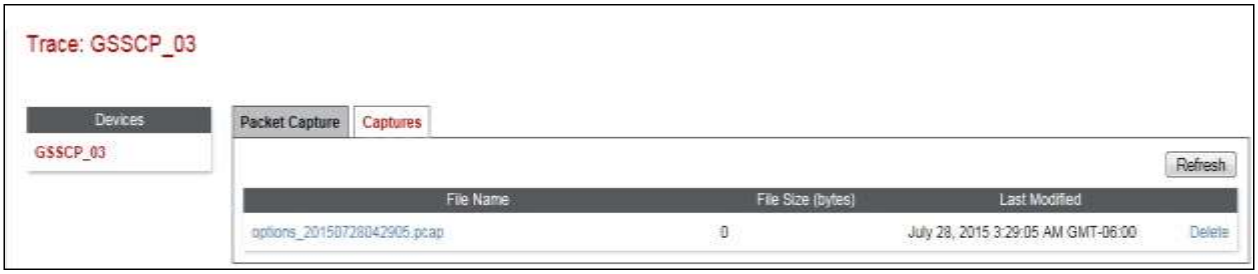
To define the trace, navigate to **Device Specific Settings → Advanced Options → Troubleshooting → Trace** in the main menu on the left hand side and select the **Packet Capture** tab.

- Select the SIP trunk interface from the **Interface** drop down menu.
- Select **All** from the **Local Address** drop down menu.
- Enter the IP address of the network SBC in the **Remote Address** field or enter a * to capture all traffic.
- Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example.
- Specify the filename of the resultant pcap file in the **Capture Filename** field.
- Click on **Start Capture**.



©2016 Avaya Inc. All Rights Reserved.

To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.



The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response in the form of a 200 OK will be seen from the Swisscom network.

©2016 Avaya Inc. All Rights Reserved.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R7.0 as an Evolution Server, Avaya Aura® Session Manager R7.0 and Avaya Session Border Controller for Enterprise to Swisscom VoIP Gate service. Swisscom VoIP Gate 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. Additional References

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

[1] *Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*, May 2016

[2] *Avaya Aura® Communication Manager 7.0 Documentation library*, May 2016

[3] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide* Release 7.0 May 2016

[4] *Implementing Avaya Aura® System Manager* Release 7.0, May 2016

[5] *Upgrading Avaya Aura® System Manager to Release 7.0*, May 2016

[6] *Administering Avaya Aura® System Manager* Release 7.0, May 2016

[7] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide* Release 7.0, May 2016

[8] *Implementing Avaya Aura® Session Manager* Release 7.0, May 2016

[9] *Upgrading Avaya Aura® Session Manager* Release 7.0, May 2016

[10] *Administering Avaya Aura® Session Manager* Release 7.0, May 2016

[11] *Deploying Avaya Session Border Controller for Enterprise* Release 7.0, Aug 2015

[12] *Upgrading Avaya Session Border Controller for Enterprise* Release 7.0, Aug 2015

[13] *Administering Avaya Session Border Controller for Enterprise* Release 7.0, Aug 2015

[14] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/

©2016 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.