Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.2 as an Evolution Server, Avaya Aura® Session Manager R6.2 and Avaya Session Border Controller for Enterprise R4.0.5 to Support Swisscom SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Swisscom SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager as an Evolution Server and Avaya Session Border Controller for Enterprise. Swisscom is a member of the DevConnect Global SIP 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 to configure Session Initiation Protocol (SIP) trunking between Swisscom SIP Trunk 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 Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with the Swisscom SIP Trunk 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.

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 Trunk Service provided by Swisscom.

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by Swisscom. Incoming PSTN calls were made to H.323, SIP, Digital and Analogue telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via Swisscom to PSTN. Outgoing calls from the enterprise to the PSTN were made from H.323, SIP, Digital and Analogue telephones.
- Calls using G.729 and G.711A codec's.
- DTMF transmission using RFC 2833 with successful Vector navigation for inbound and outbound calls.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using the T.38 mode
- 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 was used during this test.
- Call coverage and call forwarding for endpoints at the enterprise site.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Swisscom SIP Trunk Service with the following observations:

- Swisscom only support SIP History-Info Headers for call re-direction. For billing purposes, the CS2K on the Swisscom network only refers to the first line of information on the History-Info Headers. However, this info required for billing purposes was contained in the second line of the History-Info Headers. The solution was to delete the first line of information from the History-Info Headers using a SigMa script. The details of the Sigma Script are outlined in **Section 7.2.8**.
- Outgoing calls from SIP phones failed initially and required a script on the Avaya SBCE to remove unused media and headers and shorten the length of the INVITE. The details of the Sigma Script are outlined in **Section 7.2.8**.
- All tests were completed using H.323, SIP, Digital and Analogue phone types. The Avaya one-X® Communicator was used to test soft client functionality.
- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- No emergency calls to the operator were tested
- Inbound and Outbound fax was tested using T.38 standard.

2.3. Support

For technical support on Swisscom products please contact the Swisscom support team: Email: cbu.incident-voice@swisscom.com

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Swisscom SIP Trunk 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 46xx series IP telephones (with H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware) Avaya A175 Desktop Video Device running Flare Experience, 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 SIP.

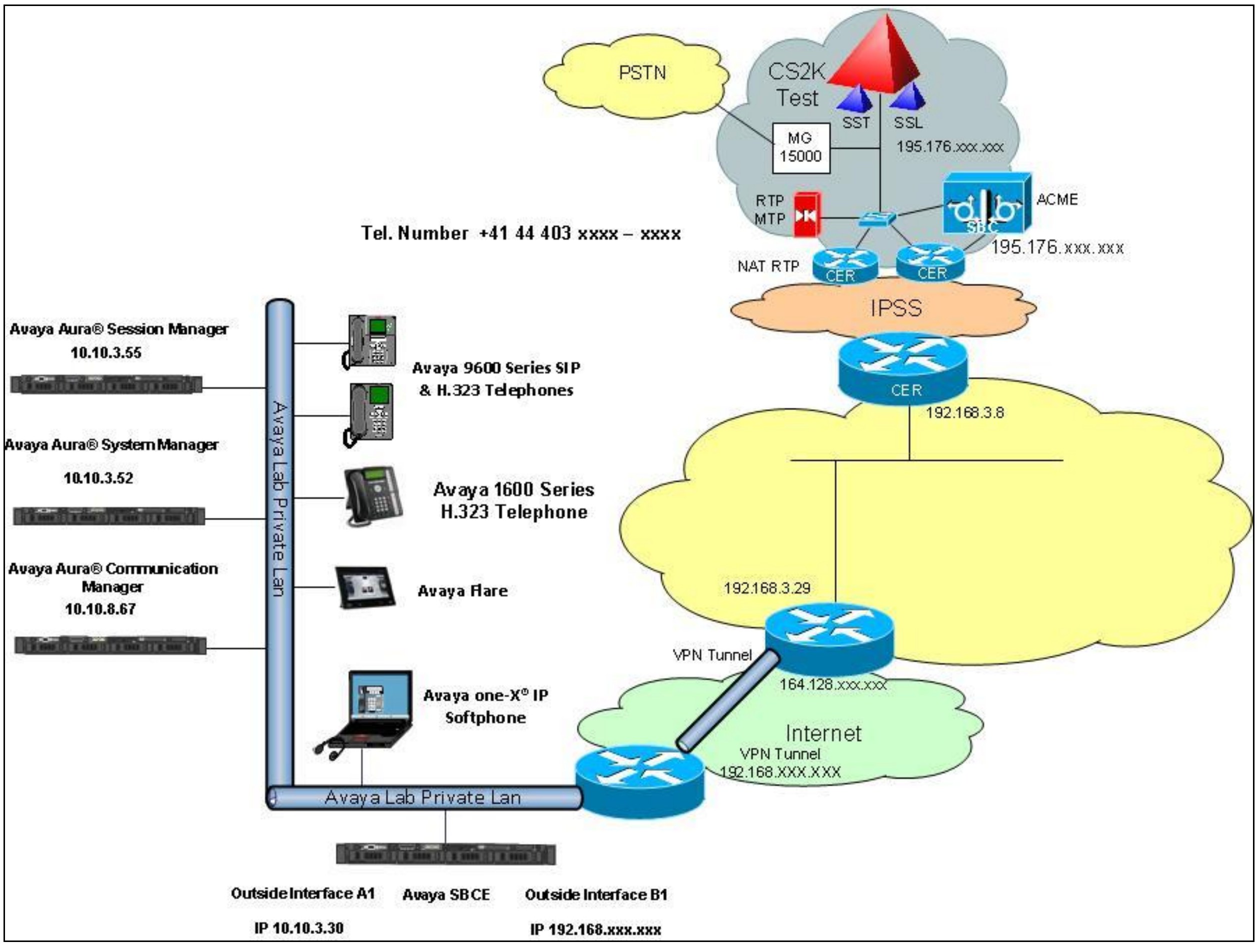


Figure 1: Test Setup Swisscom SIP Trunking to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server	Avaya Aura® Communication Manager R6.2 (R016x.02.0.823.0)
Avaya G430 Media Gateway MM711 Analogue MM712 Digital MGP Firmware	 HW31 FW093 HW07 FW009 30.12.1
Avaya S8800 Server	Avaya Aura® Session Manager R6.2 SP3 (6.2.0.0.15669 -6.2.12.307)
Avaya S8800 Server	Avaya Aura® System Manager R6.2 (6.2.0.0.15669-6.2.12.9) Update revision No: 6.2.15.1.1959
Dell R310	Avaya Session Border Controller for Enterprise. (4.0.5.Q19)
Avaya 9620 Phone (H.323)	3.11
Avaya 9620 Phone (SIP)	2.6.4.0
Avaya 2420 Digital Phone	N/A
Analog Phone	N/A
Avaya 4620 Phone (H.323)	2.9
Avaya one-X® Communicator	6.1
Avaya Desktop Video Device	1.0.2
Swisscom	
SBC	ACME Net-Net 4250 Firmware SC6.1.0 MR-11 GA (Build 1018) Build Date=02/21/12
SSL	MCP_14.0.9.11_2012-10-05-0857
GWC	GC150BT (CPCI6115)
C20 Core	CVM 15 PPC_3PC_CORE BCS 57 BN built on 2010-DEC-12 at 13:41:00 using csnwc13cz, Patch state of February 06, 2013

Note: Swisscom configuration kept internally for support reference.

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 SIP Trunking service. For incoming calls, the 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 may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Swisscom. 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 Server 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 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: 4000  10
```

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? y
                  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? n               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? n
                       IP Trunks? y

           IP Attendant Consoles? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signaling group between Communication Manager and Session Manager. Type **change node-names ip** to make changes to the **IP Node Names**. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM100** and **10.10.3.55** are the **Name** and **IP Address** for the Session Manager. Also note the **procr** name as this is the interface that Communication Manager will use as the SIP signaling interface to Session Manager.

```
change node-names ip
                                  IP NODE NAMES
    Name              IP Address
 procr              10.10.8.67
 SM100              10.10.3.55
 default            0.0.0.0
```

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-region** and **Inter-region**) is set to yes to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources
- 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** was used

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Default NR
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 35000                     IP Audio Hairpinning? n
   UDP Port Max: 50001
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                  RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
```

5.4. Administer IP Codec Set

Use the **change ip-codec-set** command 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's supported by Swisscom were configured, namely **G.711A** and **G.729**.

```
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.729            n          2        20
```

Swisscom 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

Add a signaling group and trunk group for inbound and outbound PSTN calls to Swisscom SIP Trunk Service and configure using TCP (Transmission Control Protocol) and tcp port of 5060. Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set the **Group Type** field to **sip**
- The **Transport Method** field is set to **tcp**
- Set the **Near-end Node Name** to the processor interface (node name **procr**). This value is taken from the **IP Node Names** form shown in **Section 5.2**
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name (**SM100**), also shown in **Section 5.2**
- Ensure that the recommended TCP port value of **5060** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields
- In the **Far-end Network Region** field, enter the IP Network Region configured in **Section 6.2.** This field logically establishes the far-end for calls using this signaling group as network region **1**
- The **Direct IP-IP Audio Connections** field is set to **y**
- The **Initial IP-IP Early Media** field is set to **y**
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833

The 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



   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? y
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 n** command, where **n** 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, i.e. **101**
- 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: smpub                   COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                                    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.

```
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): 1800
```

On **Page 3,** set the **Numbering Format** field to **private.** This prevents the number to be sent to Swisscom with the + used in the E164 numbering format.

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

                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                              Modify Tandem Calling Number:
```

On **Page 4** of this form:

- Set **Send Transferring Party Information** to **y** to ensure that the transferring party number is sent. This information is used by the Swisscom network for call transfer.
- Set **Network Call Redirection** to **y** as this allows call redirection to be managed by the Swisscom SIP Service instead of the CM. As a result, trunks that the CM would otherwise retain to accomplish a trunk-to-trunk transfer are released after the call redirection takes place.
- Set **Send Diversion Header** to **n** to remove the Diversion Header. This information is not used and increases the size of the INVITE unnecessarily.
- Set **Support Request History** to **y** to ensure the History-Info Header is sent. This information is used by the Swisscom network for call redirection.
- 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** as the most effective method employed by the CM of modifying an existing dialogue.

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

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? y
                 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? y
            Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
                                Enable Q-SIP? n
```

5.7. Administer Calling Party Number Information

In this section the Calling Party Number sent when making a call using the SIP trunk is specified.

5.7.1. Set Private Numbering

Use the **change private-numbering 0** command to configure Communication Manager to send the calling party number. In the sample configuration, all stations with a **4**-digit extension beginning with **6** will send the calling party number **0041444xxxxxxx** to Swisscom SIP Trunk Service. This calling party number will be sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Public DID numbers have been masked for security purposes.

```
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: 1
 4  6             1          0041444xxxxxxx  14    Maximum Entries: 240
```

5.8. Administer Route Selection for Outbound Calls

In these Application Notes, the Automatic Route Selection (ARS) feature will be used to route outbound calls via the SIP trunk to Swisscom SIP Trunk Service. In the sample configuration, the single digit **9** is used as the ARS access code. Avaya telephone users will dial **9** to reach an outside line. Use the **change feature-access-codes** command to configure or observe **9** as the **Auto Route Selection (ARS) - Access Code 1**.

```
change feature-access-codes                                        Page   1 of   9
                               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: *37
                       Answer Back Access Code: *12
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 7
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2: *99
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *87    All: *88    Deactivation: #88
   Call Forwarding Enhanced Status:        Act:        Deactivation:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. A small sample of dial patterns are illustrated here. Further administration of ARS is beyond the scope of these Application Notes. The example entries shown will match outgoing calls to numbers beginning with **0** or **00**. Calls are sent to **Route Pattern 1**, which contains the previously configured SIP Trunk Group.

```
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                      10    11    1         pubu         n
    00                     13    14    1         pubu         n
```

Use the **change route-pattern** 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: tosm100
                             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
```

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DID 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 DID numbers provided by Swisscom correlate to the internal extensions assigned within Communication Manager. The **change inc-call-handling-trmt trunk-group 1** command is used to translate numbers **+41444nnnnn0** to **+41444nnnnn9** to the 4 digit extension by deleting **all** of the incoming digits and inserting the extension number. Note that the significant digits beyond the city code have been obscured.

```
change inc-call-handling-trmt trunk-group 1                    Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    12 +41444nnnnn0     all 6100
 public-ntwrk    12 +41444nnnnn1     all 6102
 public-ntwrk    12 +41444nnnnn2     all 6003
 public-ntwrk    12 +41444nnnnn3     all 6004
 public-ntwrk    12 +41444nnnnn4     all 6104
 public-ntwrk    12 +41444nnnnn5     all 6006
```

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 6100. 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. **0035386nnnnnnn**)
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing
- Set the **Config Set** to **1**

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

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 6100             EC500        -      0035386nnnnnnn   1          1
                               -
```

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

6. Configuring Avaya Aura® Session Manager

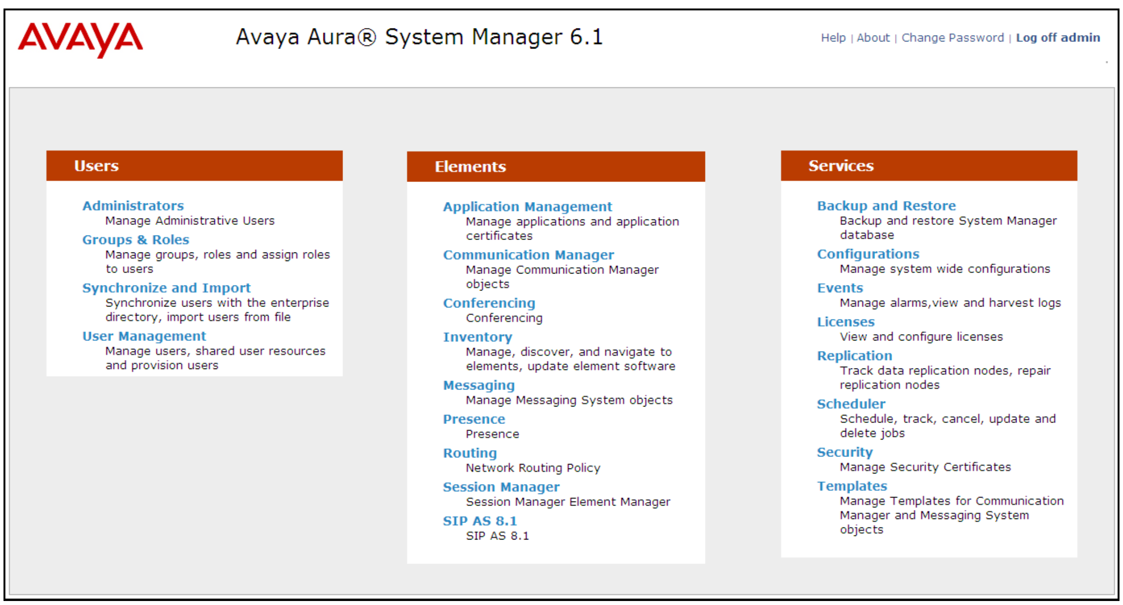
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- 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

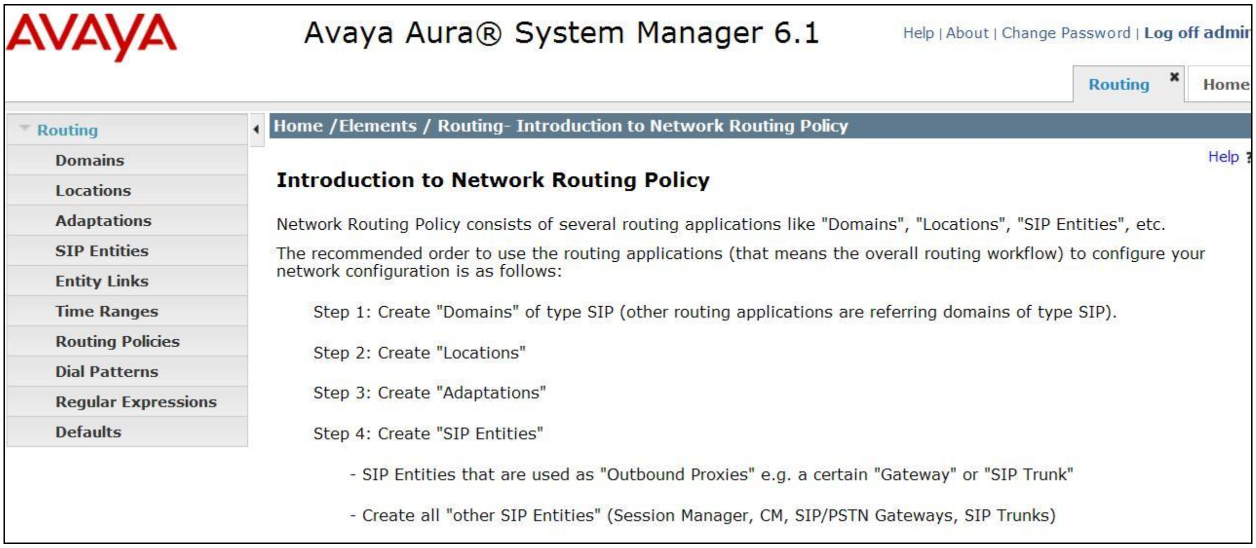
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. Log in to Avaya Aura® System Manager

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL https://<ip-address>/SMGR, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed.



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.

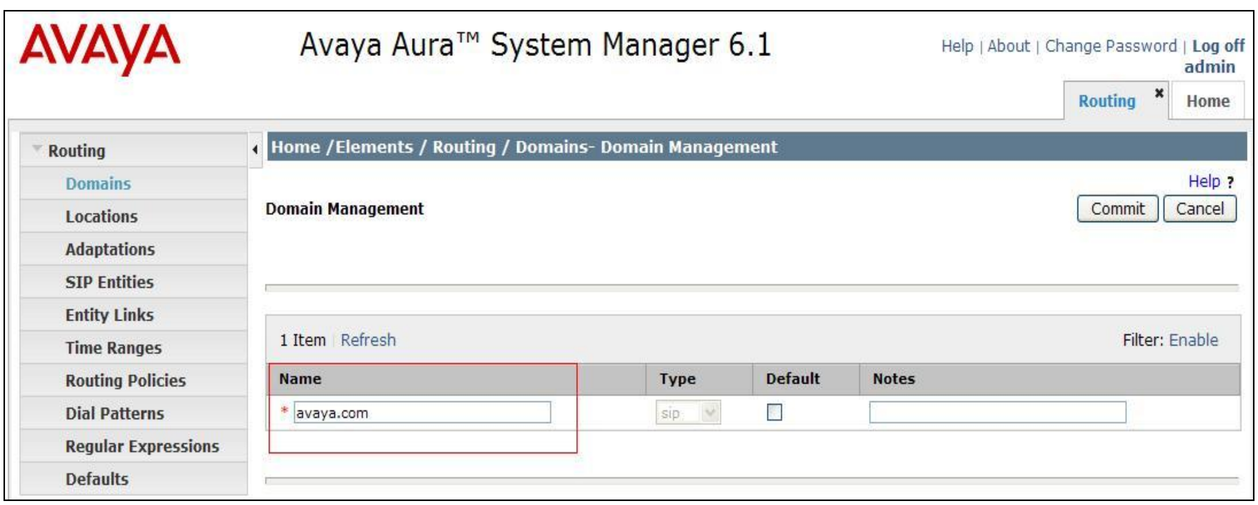


6.2. Administer SIP domain

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.



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:

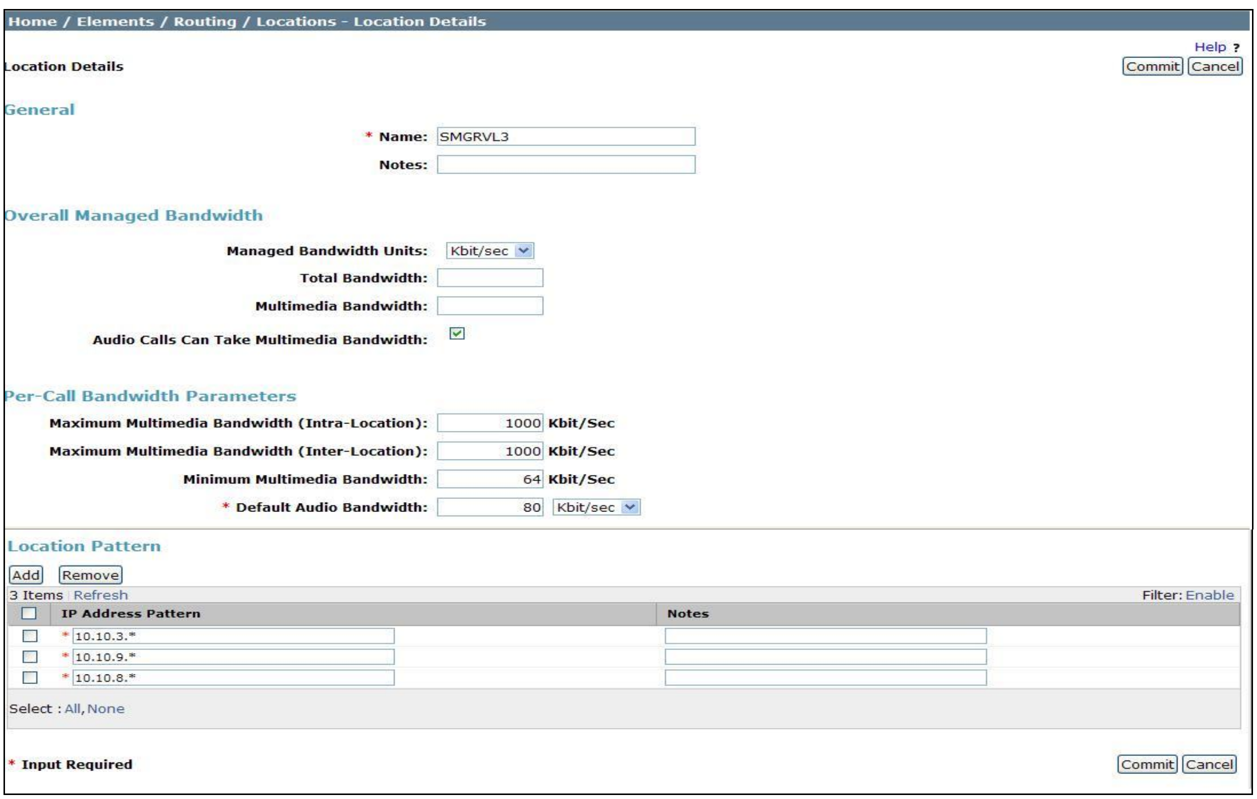
- **Name:** Enter a descriptive name for the location
- **Notes:** Add a brief description (optional)

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]

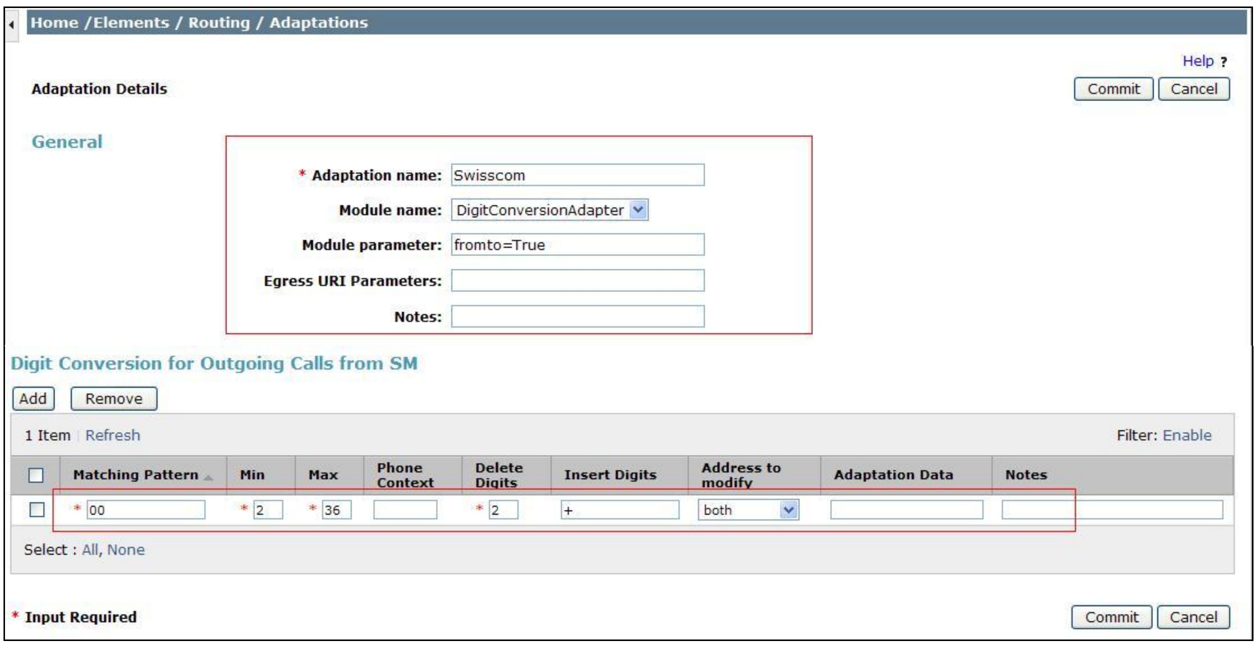
Click **Commit** to save. The screenshot below shows the Location defined for the simulated enterprise.



6.4. Administer Adaptations

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

DigitConversionAdaptor is used and leading zeros are analyzed. Both national and international numbers are converted with national numbers requiring the prefixing of the country code. The two leading zeros of the international number are removed and replaced with a "+".These rules are applied to the destination addresses.



6.5. Administer SIP Entities

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

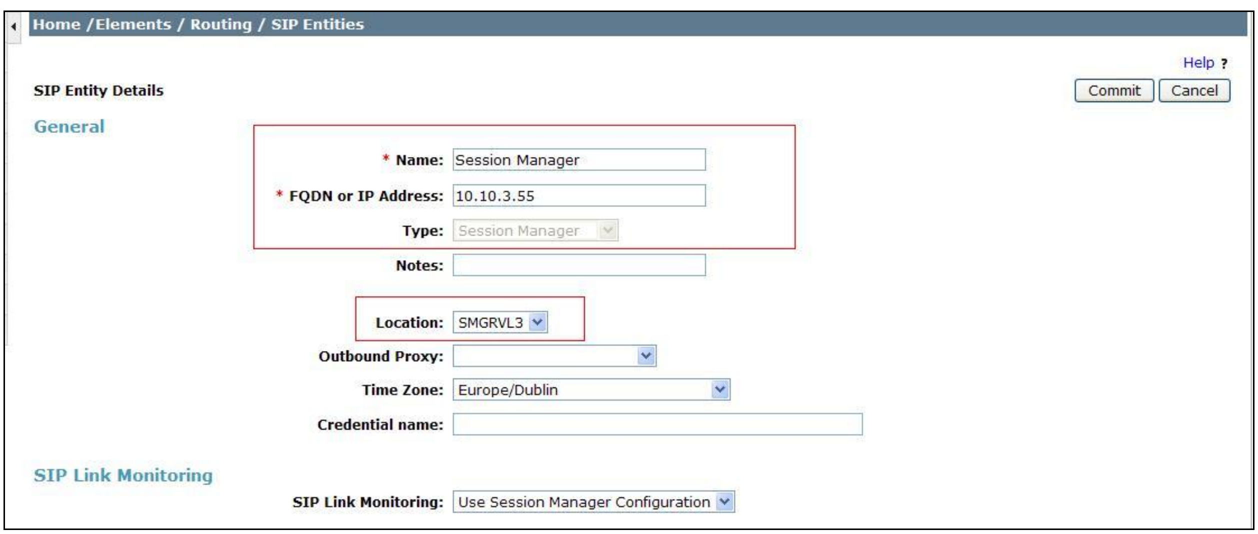
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP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

In this configuration there are three SIP Entities.

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

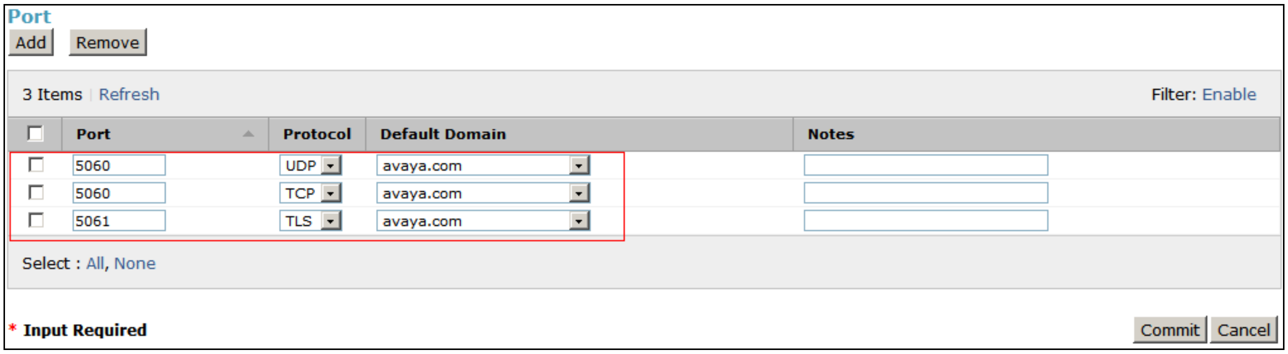
6.5.1. Avaya Aura® Session Manager SIP Entity

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 signaling interface.



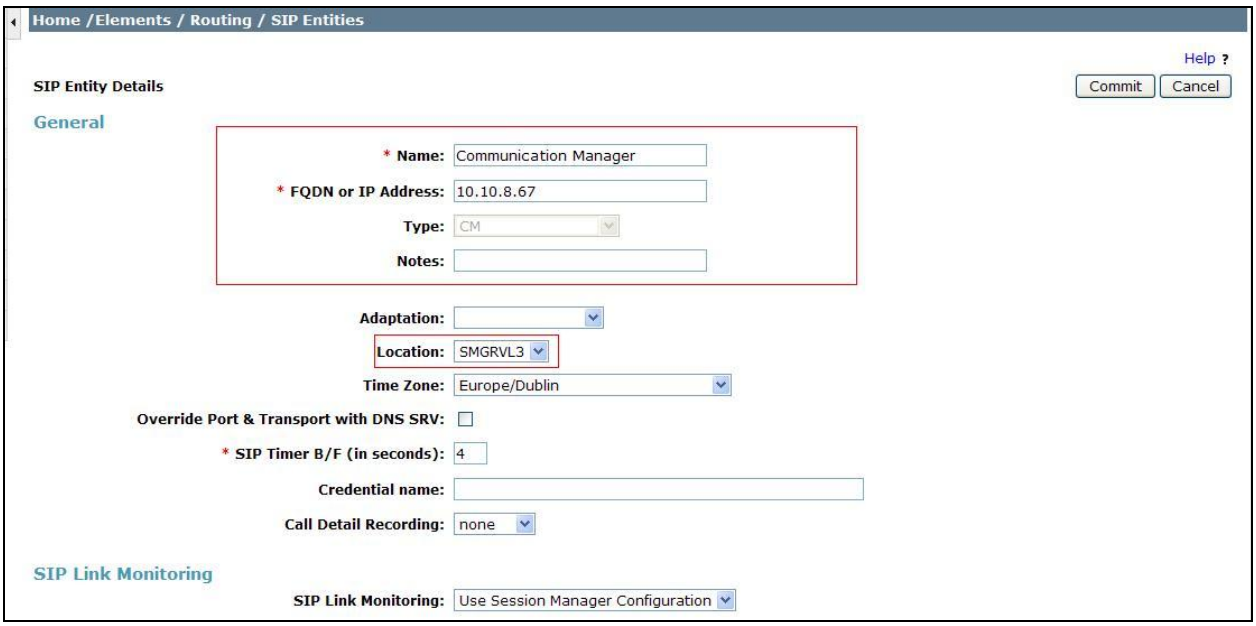
The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add,** then edit the fields in the resulting new row.

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



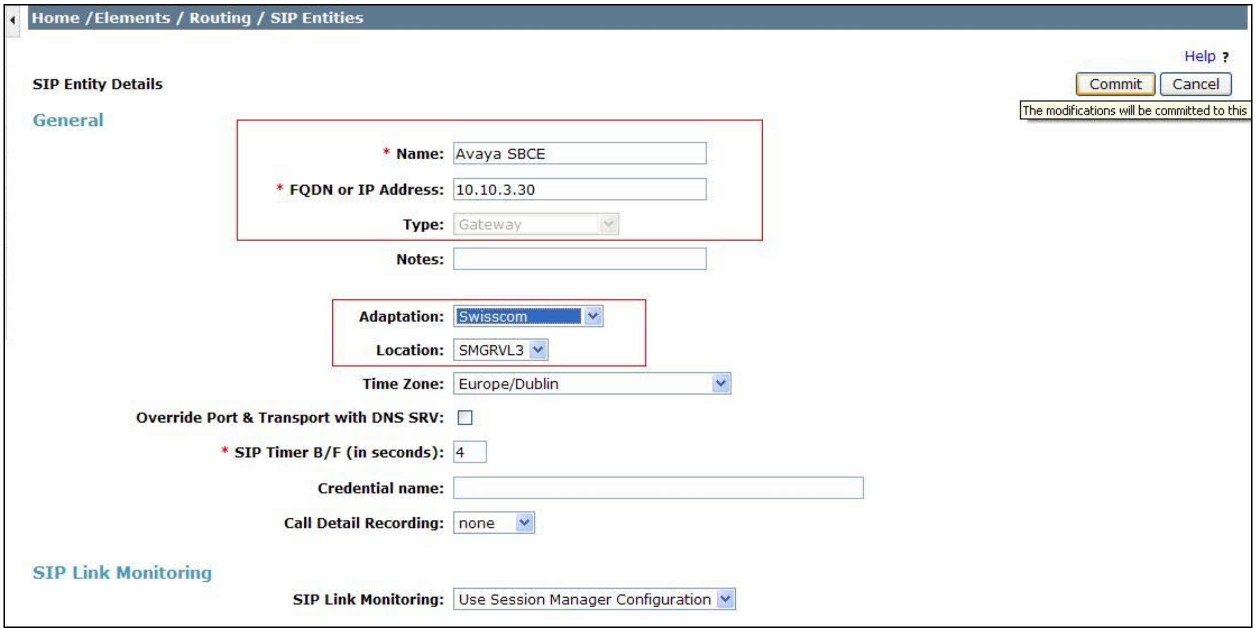
6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screens show the SIP entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of the Interface that will be providing SIP signaling. The entity **Type** is set to **CM**.



6.5.3. Avaya Session Border Controller for Enterprise SIP Entities

The following screen shows the SIP entity for the Avaya SBCE used for routing calls. The **FQDN or IP Address** field is set to the IP address of the private interfaces administered in **Section 7** of this document.

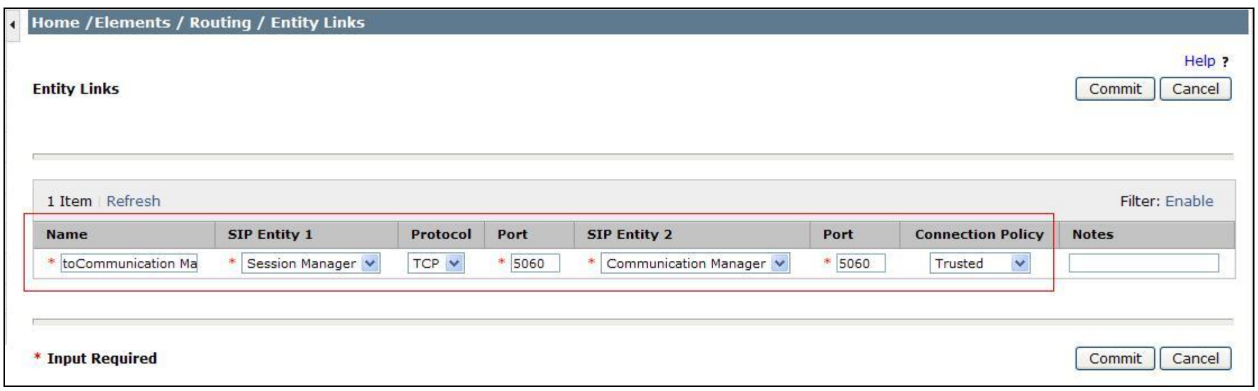


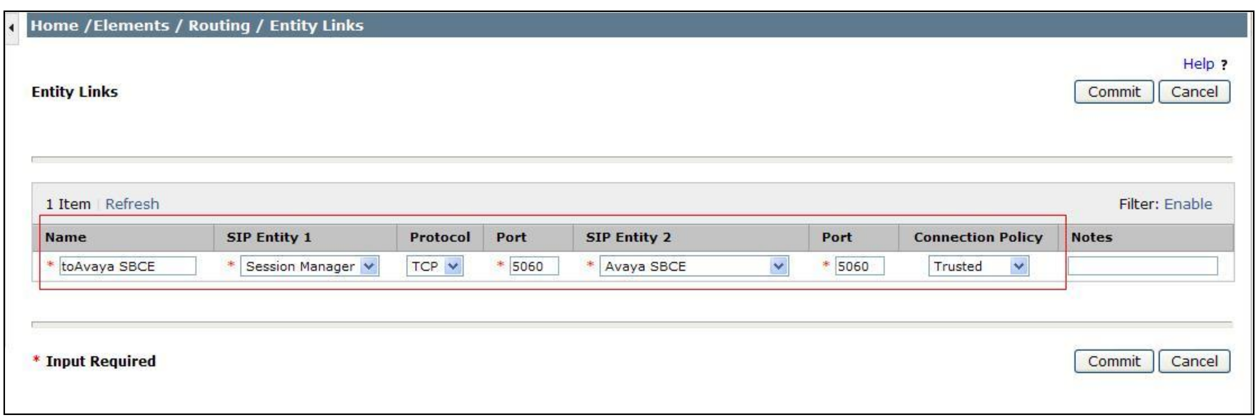
6.6. Administer Entity Links

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 . 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 **SessionManager**
- 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
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

Click **Commit** (not shown) to save changes. The following screen shows the Entity Links used in this configuration.





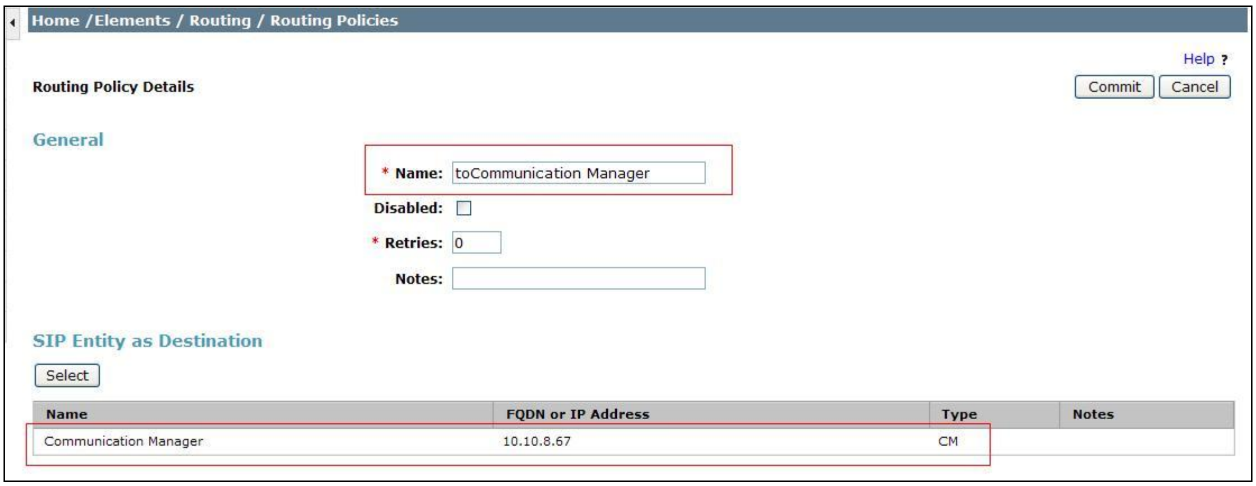
6.7. Administer Routing Policies

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

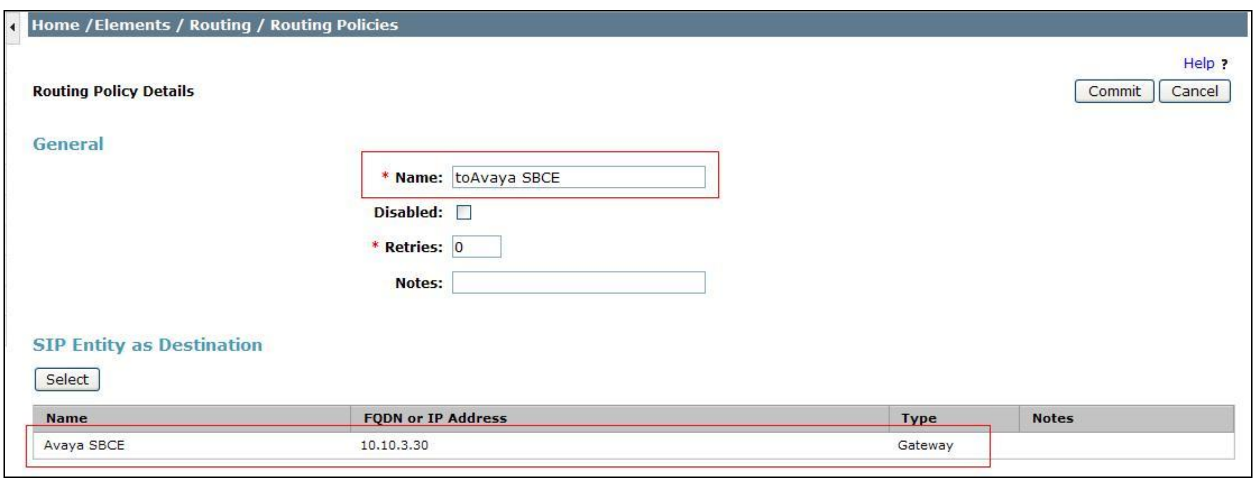
Under **General**:

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

The following screen shows the routing policy for Communication Manager:



The following screens show the routing policy for Avaya SBCE:



6.8. Administer Dial Patterns

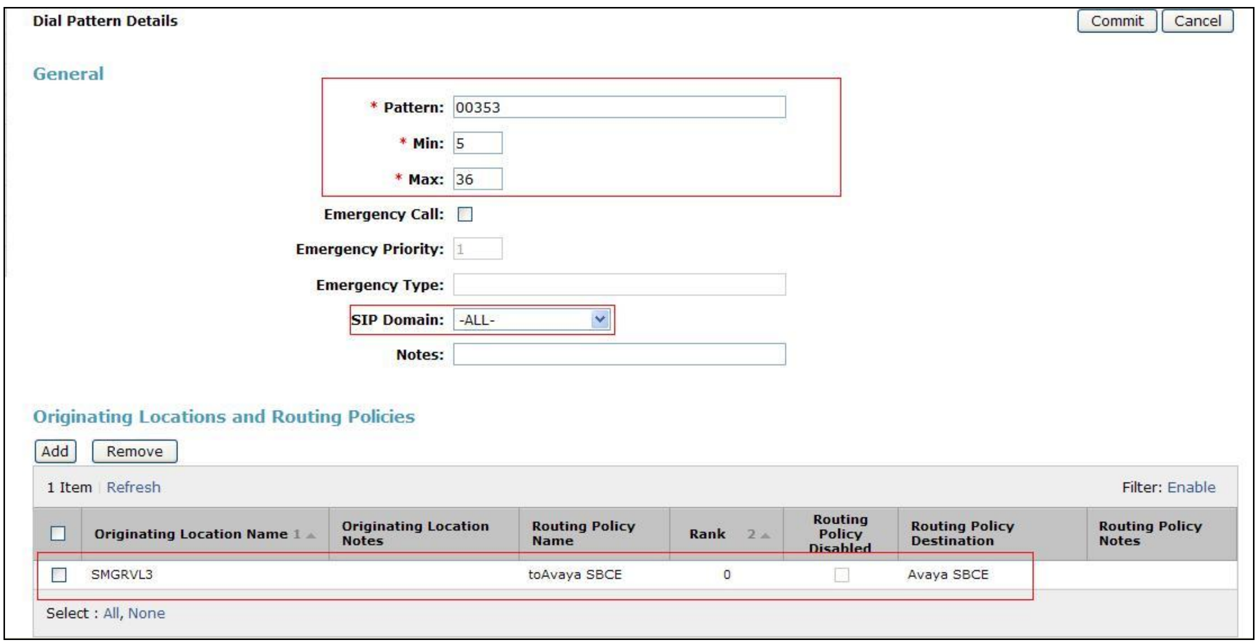
A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

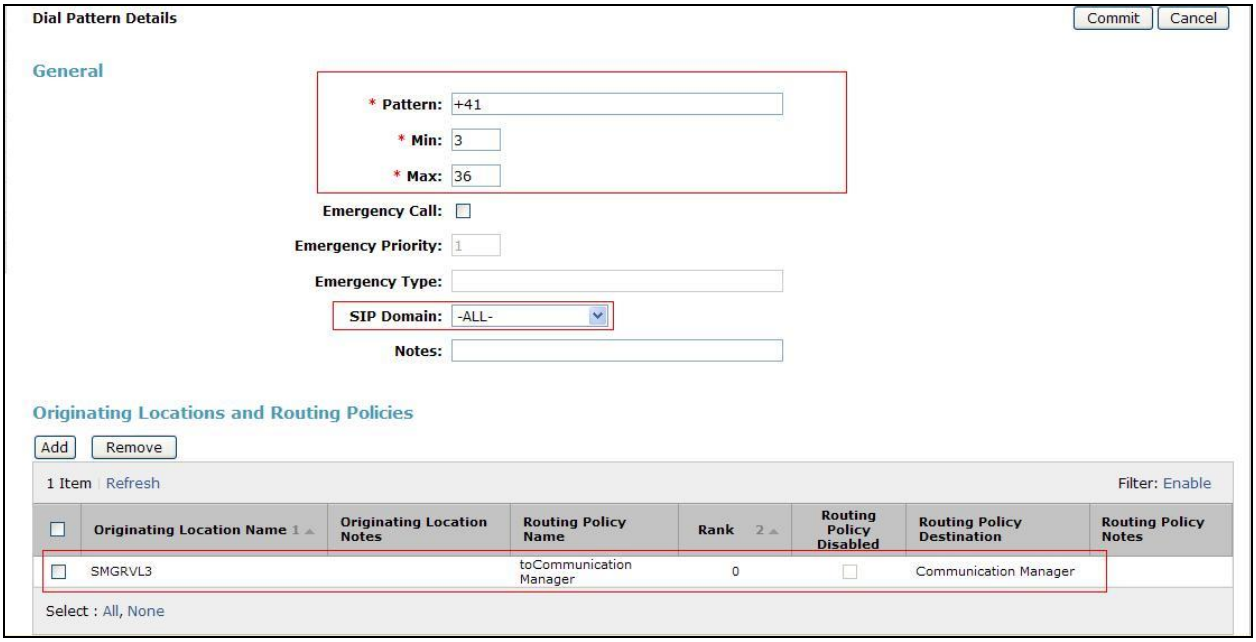
- In the **Pattern** field enter a dialed number or prefix to be matched
- In the **Min** field enter the minimum length of the dialed number
- In the **Max** field enter the maximum length of the dialed number
- In the **SIP Domain** field select **–ALL-**

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown) under **Originating Location** select **Locations** created in **Section 6.3** and under **Routing Policies** select one of the routing policies defined in **Section 6.7**. Click **Select** button to save (not shown).

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the PSTN via the Swisscom SIP trunk service.



The following screen shows the test dial pattern configured for Communication Manager. Note that the number format received from Swisscom was E.164 with leading +.

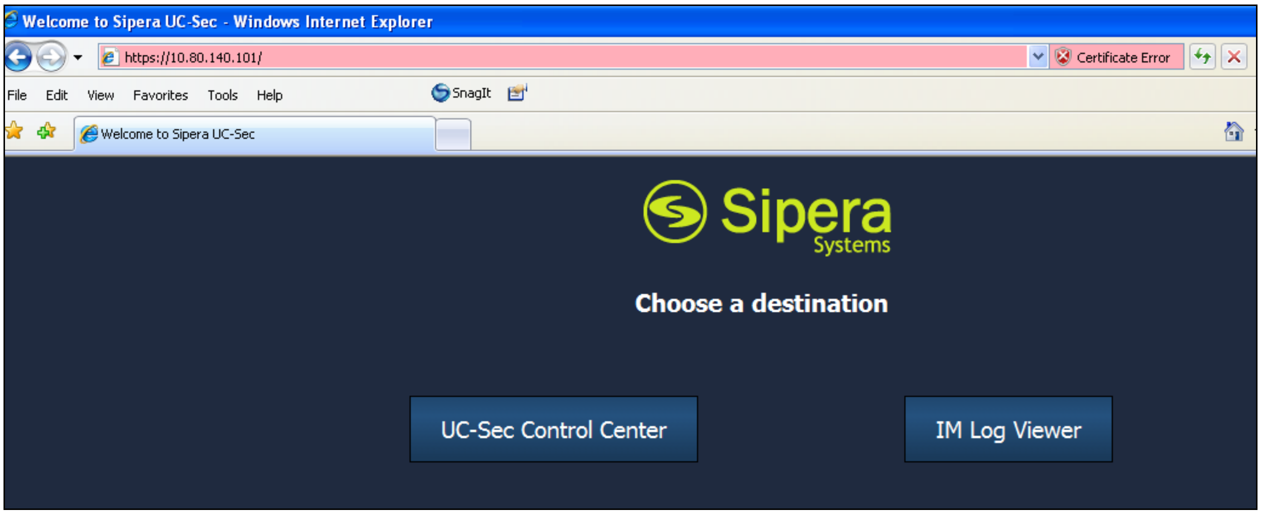


7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. The Avaya SBCE is administered using the UC-Sec Control Center.

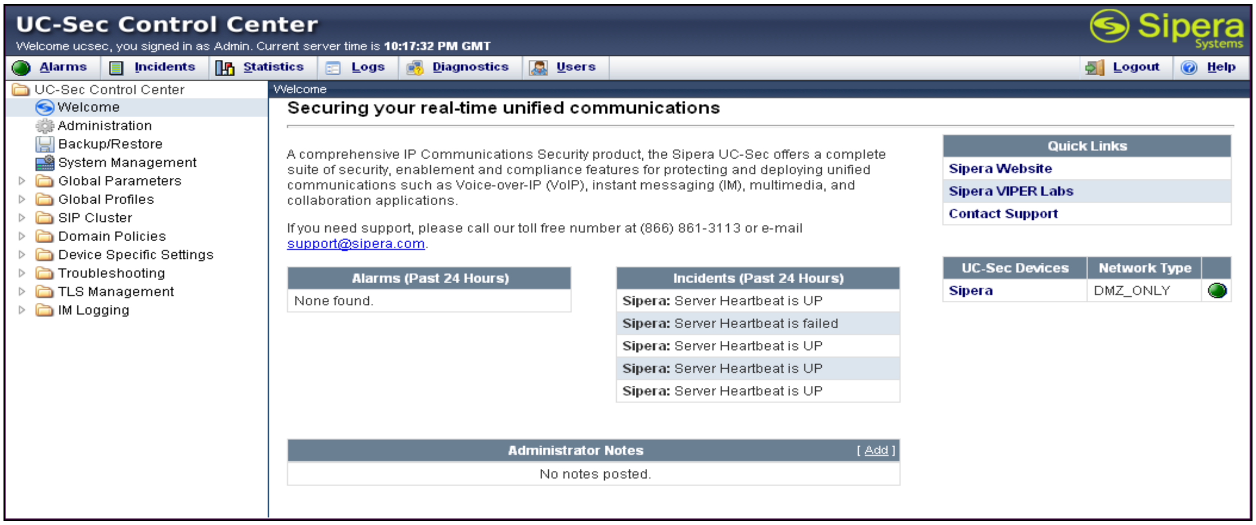
7.1. Accessing UC-Sec Control Centre

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. Select the **UC-Sec Control Center**.

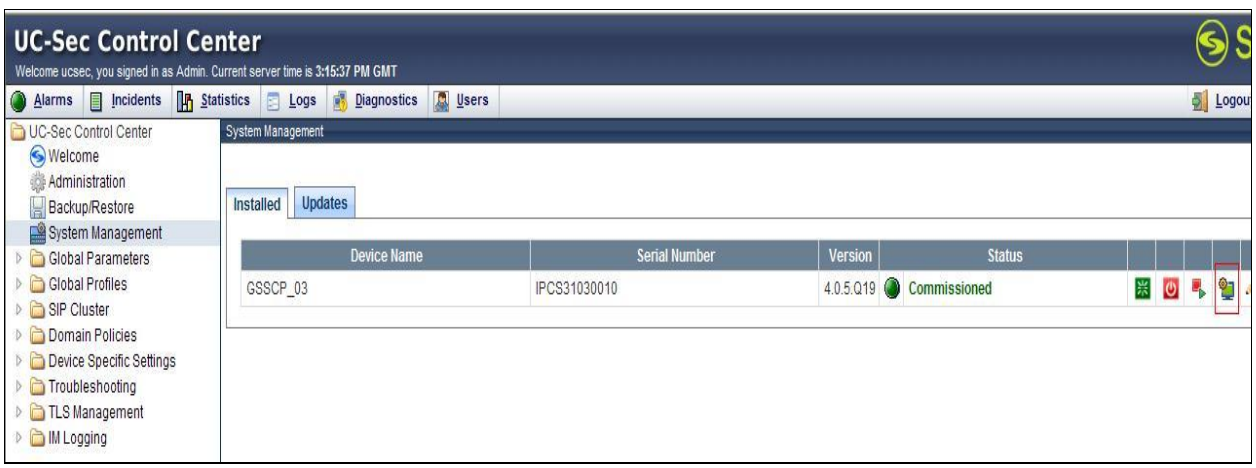


Select **UC-Sec Control Center** and enter the **Login ID** and **Password**.

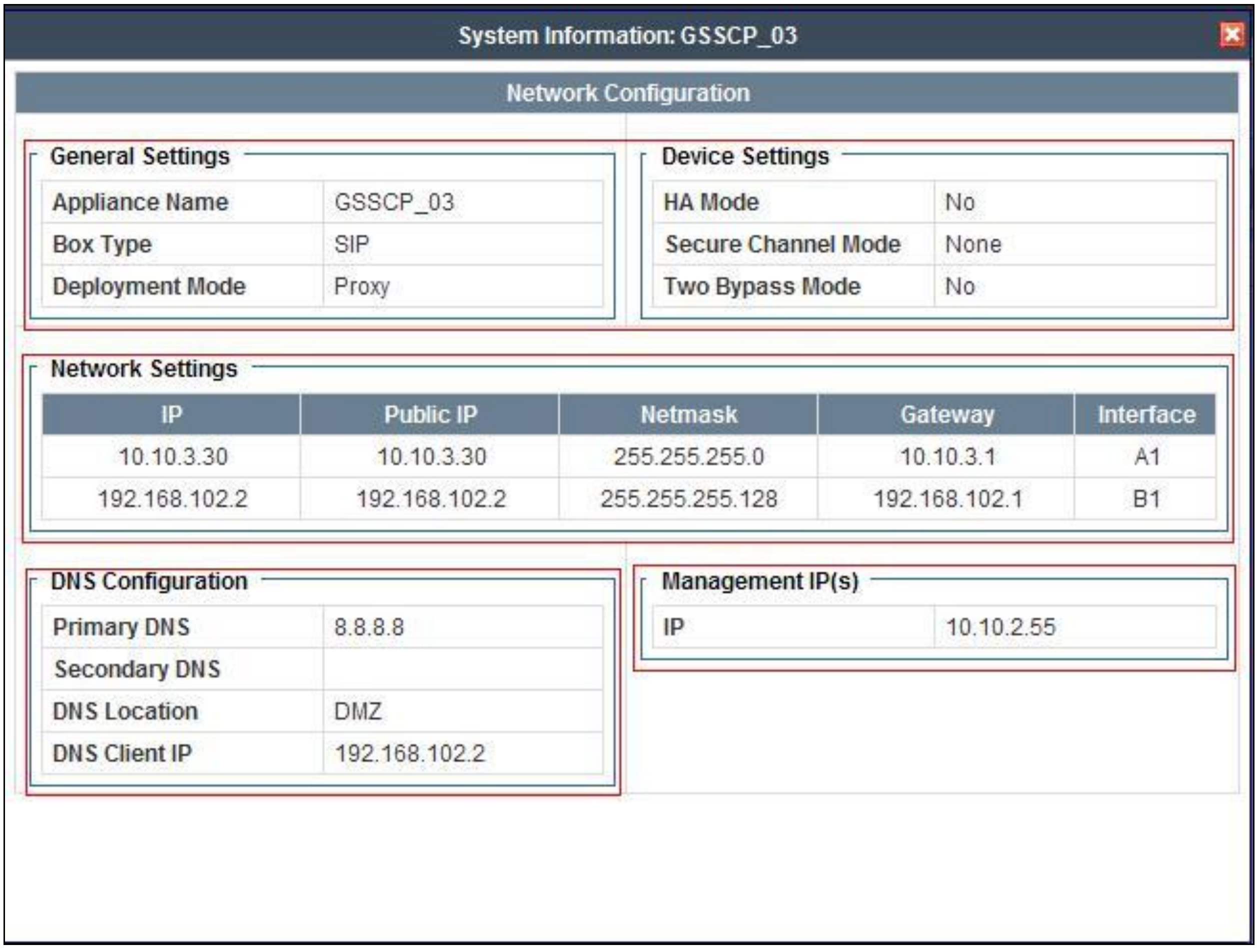
The main page of the UC-Sec Control Center will appear.



To view system information that was configured during installation, navigate to **UC-Sec Control Center → 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 the monitor icon (the third icon from the right).



The **System Information** screen shows the **Network Settings, DNS Configuration** and **Management IP** information provided during installation. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.



7.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all UC-Sec appliances.

7.2.1. Server Internetworking Avaya Side

Server Internetworking allows you to configure and manage 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 Profile.** Enter **Profile Name: SM3_CS** and click **Next.**

- Enter profile name such as **SM3_CS** and click **Next** (Not Shown)
- **Check Hold Support= RFC3264**
- **Check T.38 Support**
- All other options on the **General** Tab can be left at default

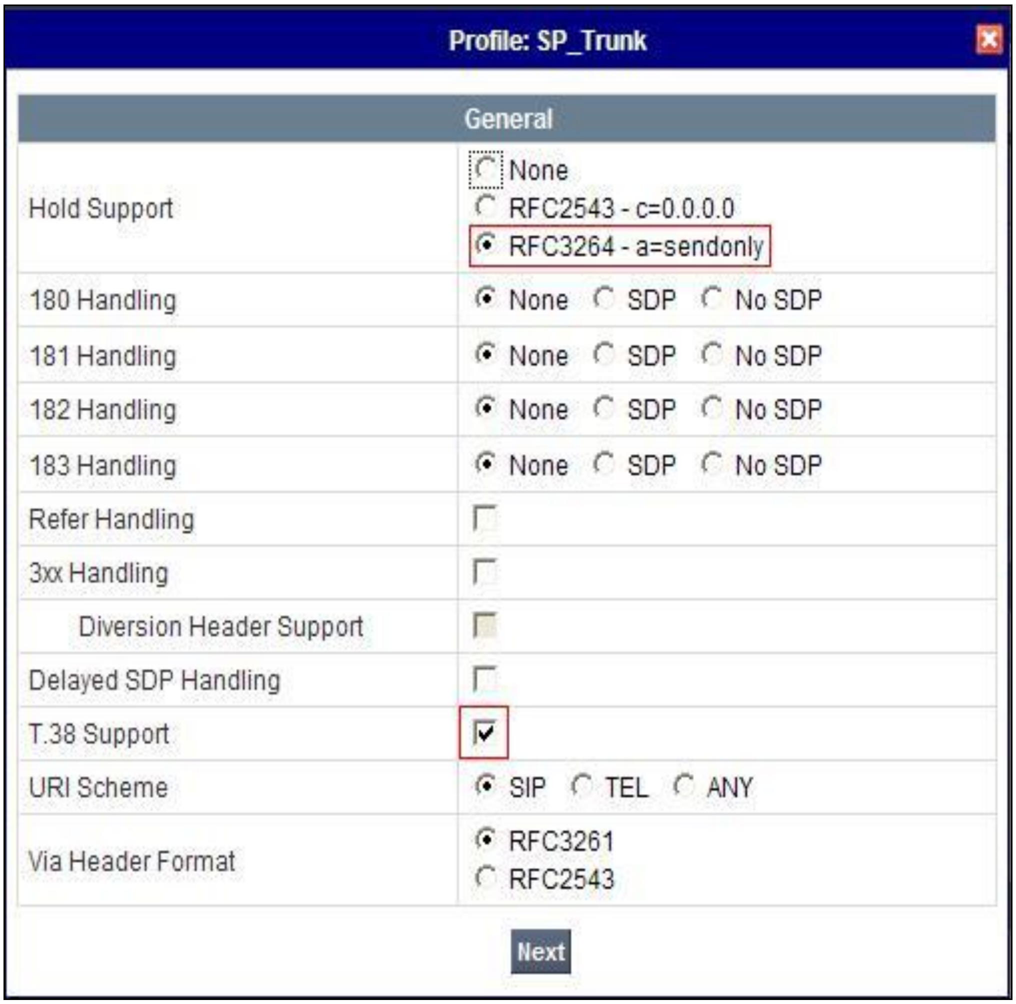
Click on **Next** on the following screens and then **Finish**.

7.2.2. Server Internetworking – Swisscom side

Server Internetworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and T.38. From the lefthand menu select **Global Profiles → Server Interworking** and click on **Add Profile.** Enter profile name**: SP_Trunk** and click on **Next.**

- Enter profile name such as **SP_Trunk** and click **Next** (Not Shown)
- **Check Hold Support= RFC3264**
- **Check T.38 Support**
- All other options on the **General** Tab can be left at default

Click on **Next** on the following screens and then **Finish**.



7.2.3.Routing – Avaya side

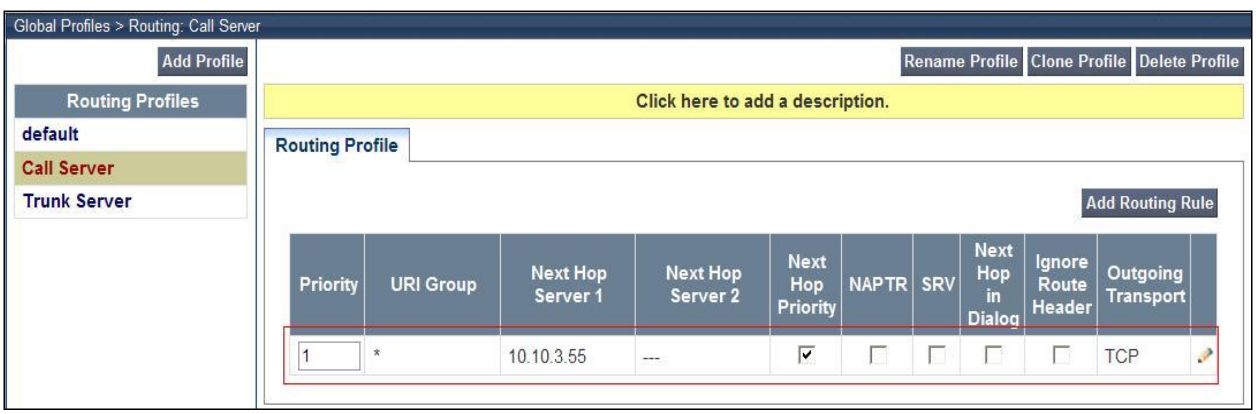
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport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

Create a Routing Profile for Session Manager and a Routing Profile for Swisscom SIP Trunk. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.
In the new window that appears, enter the following values. Use default values for all remaining fields:

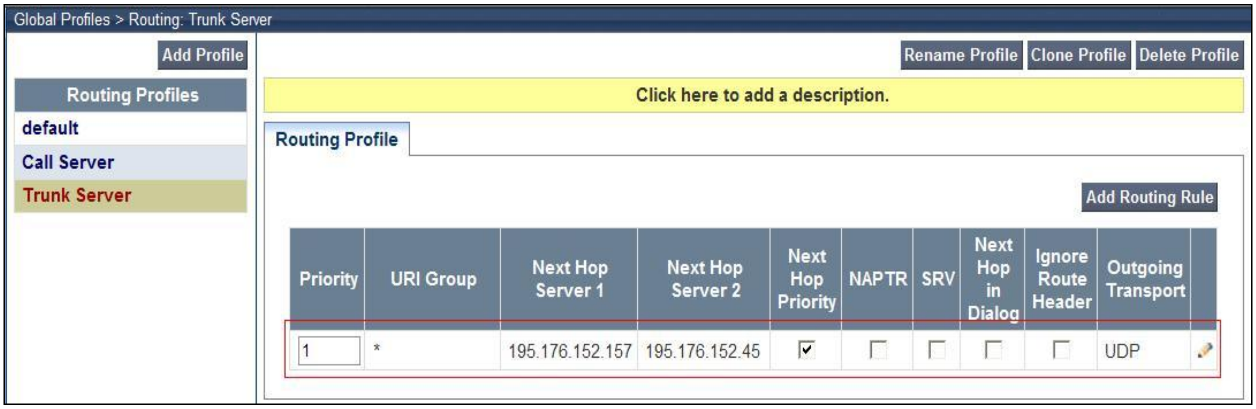
- **URI Group:** Select “*” from the drop down box
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server
- **Routing Priority Based on Next Hop Server**: Checked
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets

Click **Finish**.

The following screen shows the Routing Profile to Session Manager. The Outgoing Transport and port number must match the Avaya SBCE Entity Link created on Session Manager in **Section 6.6**.



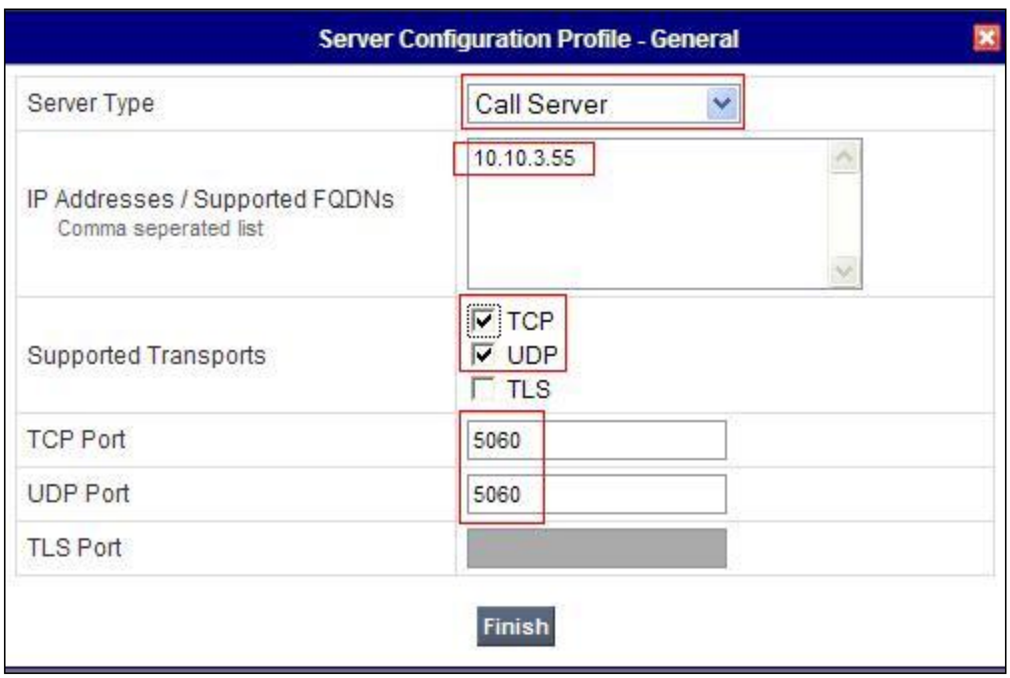
The following screen shows the Routing Profile to Swisscom.



7.2.4. Server Configuration– Avaya Aura® Session Manager

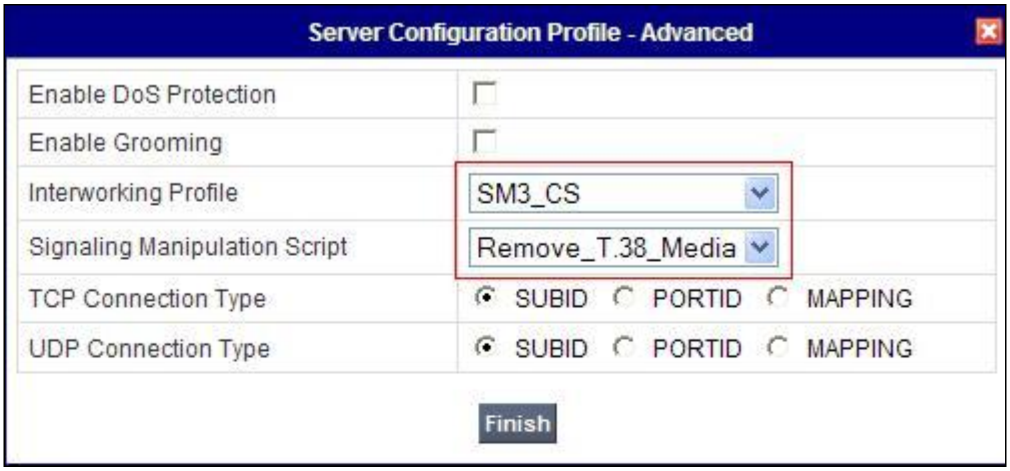
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options. From the lefthand menu select **Global Profiles → Server Configuration** and click on **Add Profile**. Enter **Profile Name: SM3_Call-Server**. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**
- Enter **IP Addresses / Supported FQDNs** to **10.10.3.55** (Session Manager IP Address)
- For **Supported Transports,** check **UDP** and **TCP**
- **TCP Port:5060**
- **UDP Port: 5060**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



On the **Advanced** tab

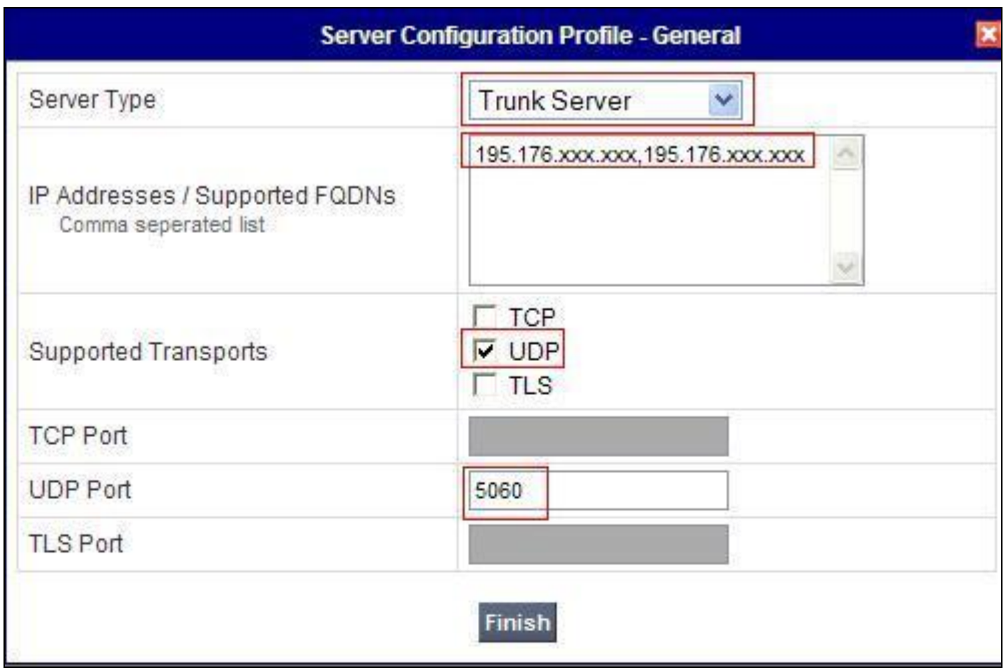
- Select **SM3_CS** for **Interworking Profile**
- Select **Remove_T.38_Media** for **Signaling Manipulation Script**
  Note: Signaling Manipulation Scripting is discussed in **Section 7.8**
- Click **Finish**



7.2.5. Server Configuration– Swisscom side

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add Profile**. Enter Name as **SP_Trunk_Server**. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** as **Trunk Server**
- Set **IP Address** to **195.176.xxx.xxx** (Swisscom Trunk Server)
- **Supported Transports**: Check **UDP**
- **UDP Port: 5060**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



On the **Advanced** tab

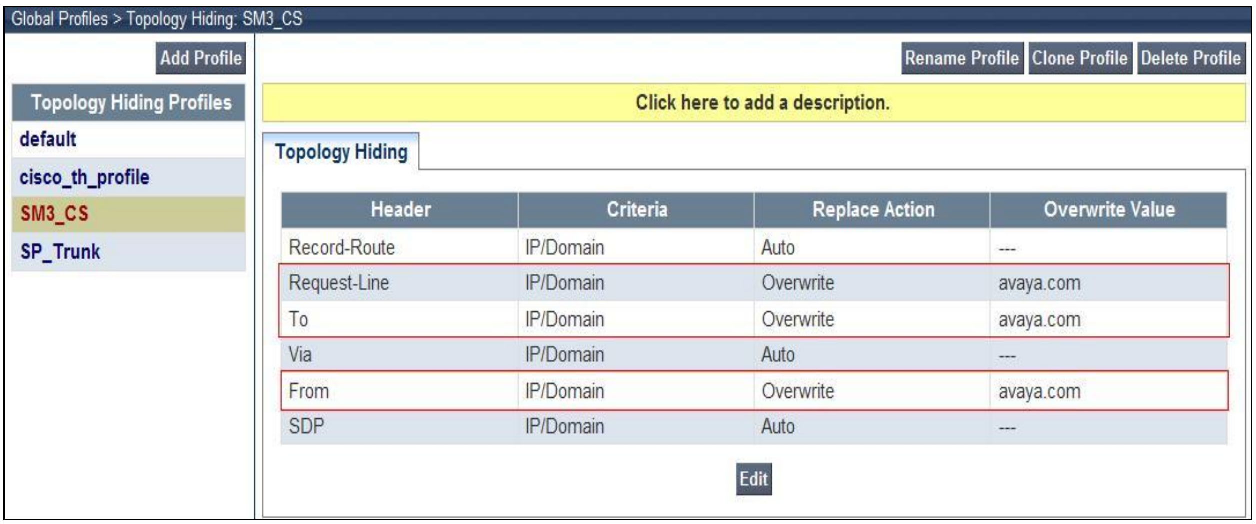
- Select **SP_Trunk** for **Interworking Profile**
- Select **Remove_History_Info** for **Signaling Manipulation Script**
  Note: Signaling Manipulation Scripting is discussed in **Section 7.8**
- Click **Finish**

7.2.6. Topology Hiding – Avaya Side

The **Topology Hiding** screen manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. Navigate to **Global Profiles → Topology Hiding** (not shown).

- Click **default** profile and select **Clone Profile** (not shown)
- Enter Profile Name : **SM3_CS**
- Under the **Header** field for **To, From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For **Override Value** type **avaya.com**
- Click **Finish** (not shown)

The screen below is a result of the details configured above.

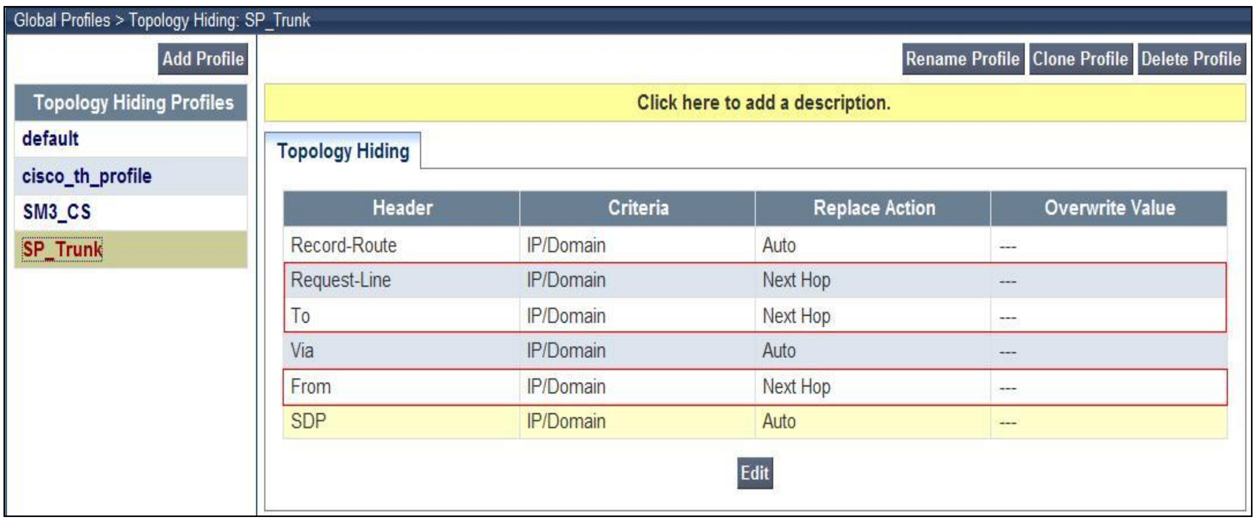


7.2.7. Topology Hiding – Swisscom Side

The **Topology Hiding** screen manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. Navigate to **Global Profiles → Topology Hiding** (not shown).

- Click **default** profile and select **Clone Profile** (not shown)
- Enter Profile Name : **SP_Trunk**
- For the Header **To, From** and **Request Line** select **IP/Domain** under **Criteria** and **Next Hop** under **Replace Action**
- Click **Finish** (not shown)

The screen below is a result of the details configured above.



7.2.8. Signaling 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.

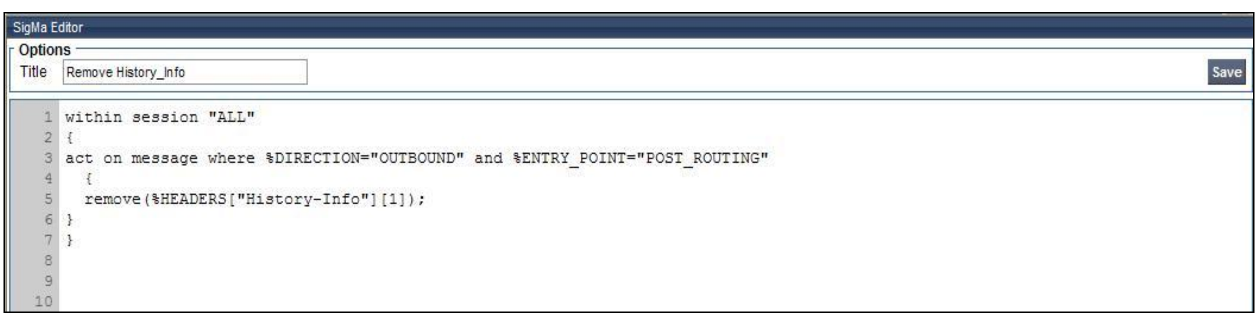
Two of these issues could not be resolved by other methods such as **Server Interworking** and **Signaling Rules**. The first issue is that Swisscom only support SIP History-Info Headers for call re-direction. For billing purposes, the CS2K on the Swisscom network only refers to the first line of information on the History-Info Headers. However, this info required for billing purposes was contained in the second line of the History-Info Headers. The solution was to delete the first line of information from the History-Info Headers using a SigMa script.

The second issue is that calls from SIP phones were failing, apparently because of additional media and information in the INVITE. The solution was to remove the additional media and unused headers from the INVITE using a SigMa script.

To define the signalling manipulation to delete the first line of information from the History-Info Headers, navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script** and enter a title. A new blank SigMa Editor window will pop up.

```
within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
  remove(%HEADERS["History-Info"][1]);
}
}
```

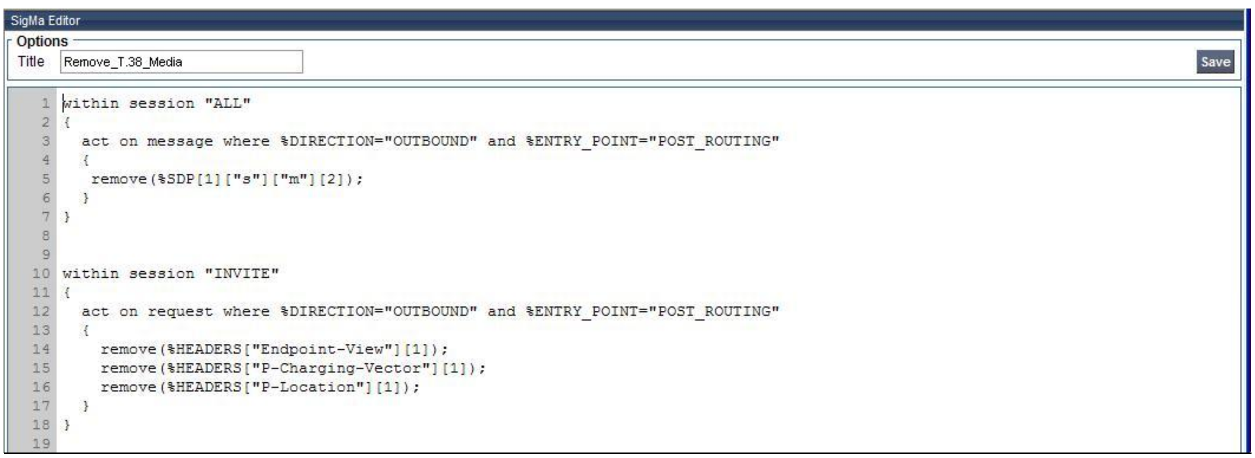
Once entered and saved, the script appears as shown in the following screenshot:



To define the signalling manipulation to remove the additional media and unused headers from the INVITE, navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script** and enter a title. A new blank SigMa Editor window will pop up.

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


within session "INVITE"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Endpoint-View"][1]);
    remove(%HEADERS["P-Charging-Vector"][1]);
    remove(%HEADERS["P-Location"][1]);
  }
}
```

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



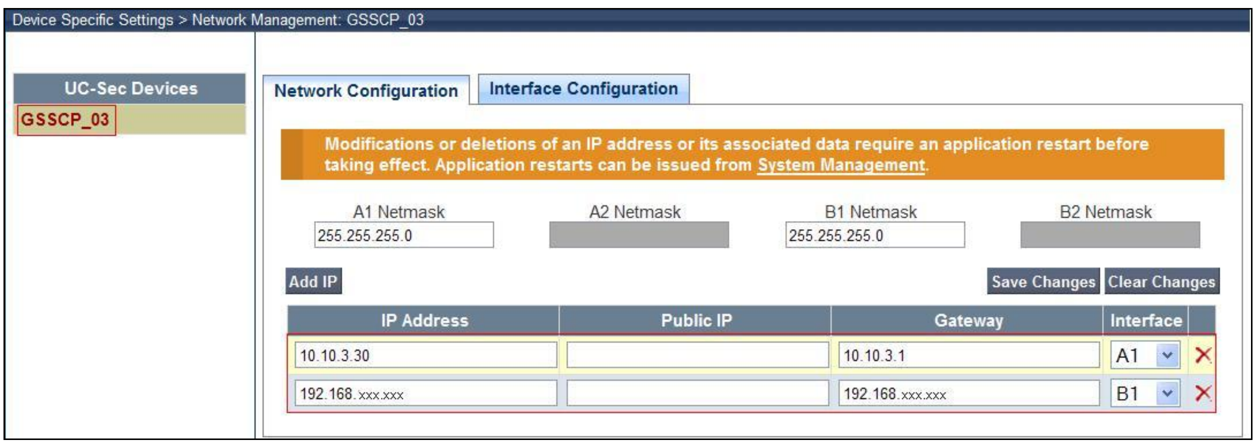
7.3. Device Specific Settings

The Device Specific Settings feature allows aggregation of system information to be viewed, and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network.

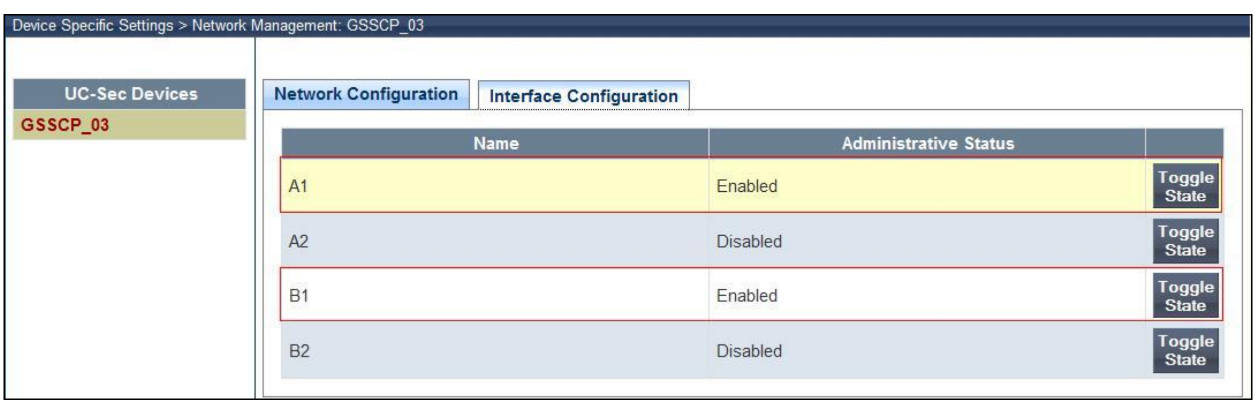
7.3.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **UC-Sec Control Center → Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the external interface is assigned to **B1**.



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

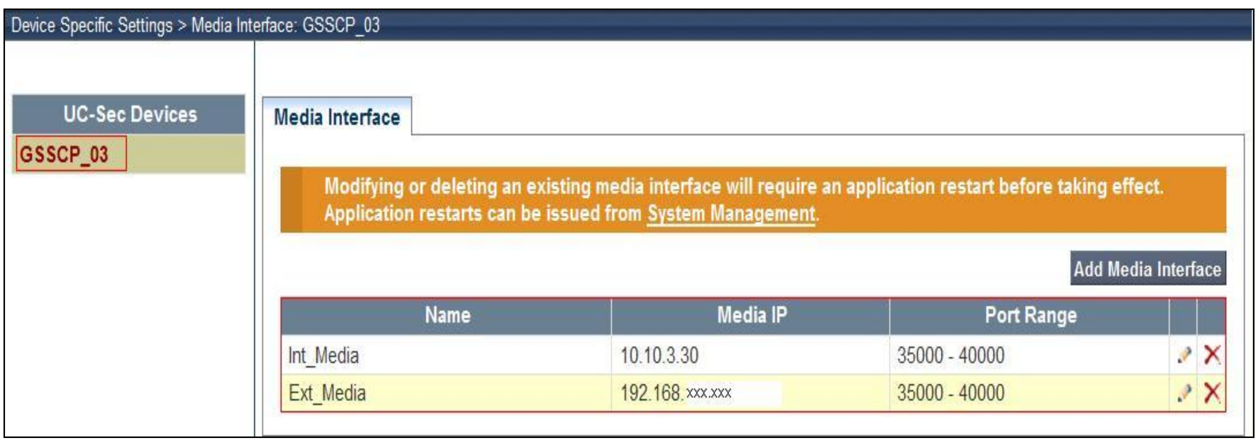


7.3.2. Media Interface

The Media Interface screen allows the IP address and ports to be set for transporting Media over the SIP trunk. The Avaya SBCE listens for SIP media on the defined ports.
To create a new Media Interface, navigate to **UC-Sec Control Center → Device Specific Settings → Media Interface** and click **Add Media Interface**.

- Select **Add Media Interface**
- **Name**: **Int_Media**
- **Media IP**: **10.10.3.30** (Internal address for calls toward CM)
- **Port Range**: **35000-50000**
- Click **Finish**
- Select **Add Media Interface**
- **Name**: **Ext_Media**
- **Media IP**: **192.168.xxx.xxx** (External address for calls toward Swisscom)
- **Port Range**: **35000-50000**
- Click **Finish**

The following screen shows the Media Interfaces created in the sample configuration for the inside and outside IP interfaces. After the Media Interfaces are created, an application restart is necessary before the changes will take effect.

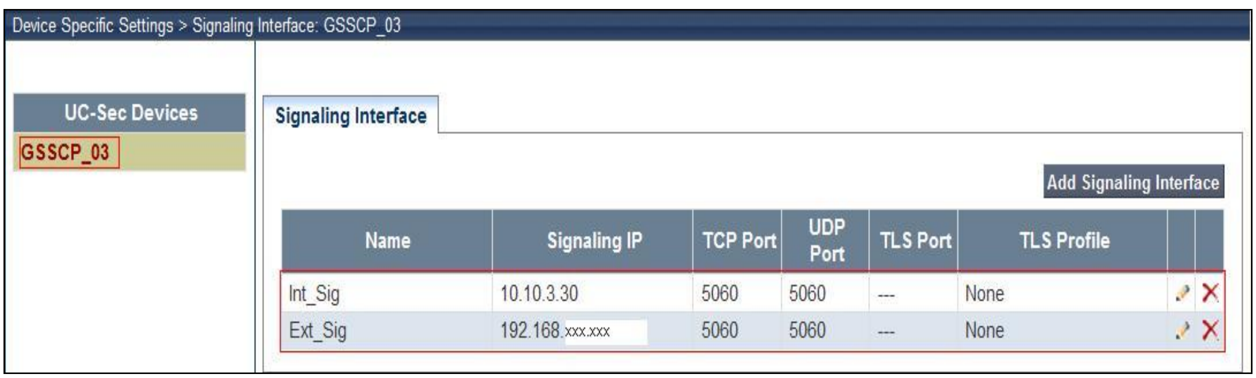


7.3.3. Signalling Interface

The Signalling Interface screen allows the IP Address and ports to be set for transporting signaling messages over the SIP trunk. The Avaya SBCE listens for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces. To create a new Signaling Interface, navigate to **UC-Sec Control Center → Device Specific Settings → Signaling Interface** and click **Add Signaling Interface**.

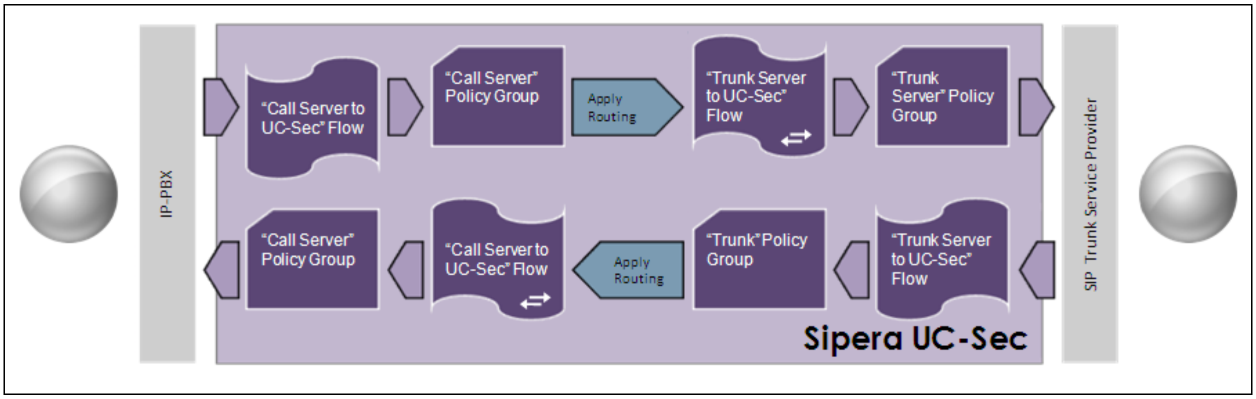
- **Name**: **Int_Sig**
- **Signaling IP**: **10.10.3.30** (Internal address for calls toward CM)
- **TCP Port**: **5060**
- **UDP Port**: **5060**
- Click **Finish**
- Select **Add Signaling Interface**
- **Name**: **Ext_Sig**
- **Signaling IP: 192.168.xxx.xxx** (External address for calls toward Swisscom)
- **TCP Port**: **5060**
- **UDP Port**: **5060**
- Click **Finish**

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



7.3.4. End Point Flows

When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



To create a Server Flow, navigate to **UC-Sec Control Center → Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow**.

- **Flow Name:** Enter a descriptive name
- **Server Configuration:** Select a Server Configuration created in **Section 7.1.5** to assign to the Flow
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy assigned to the Server Configuration
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration

Click **Finish** to save and exit.

The following screen shows the Sever Flow for Session Manager.

SM3_Call_Server

Criteria	
Flow Name	SM3_Call_Server
Server Configuration	SM3_Call_Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Media
End Point Policy Group	default-low
Routing Profile	Trunk Server
Topology Hiding Profile	SM3_CS
File Transfer Profile	None

Finish

The following screen shows the Sever Flow for Swisscom.

SP_Trunk_Server

Criteria	
Flow Name	SP_Trunk_Server
Server Configuration	SP_Trunk_Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
End Point Policy Group	default-low
Routing Profile	Call Server
Topology Hiding Profile	SP_Trunk
File Transfer Profile	None

Finish

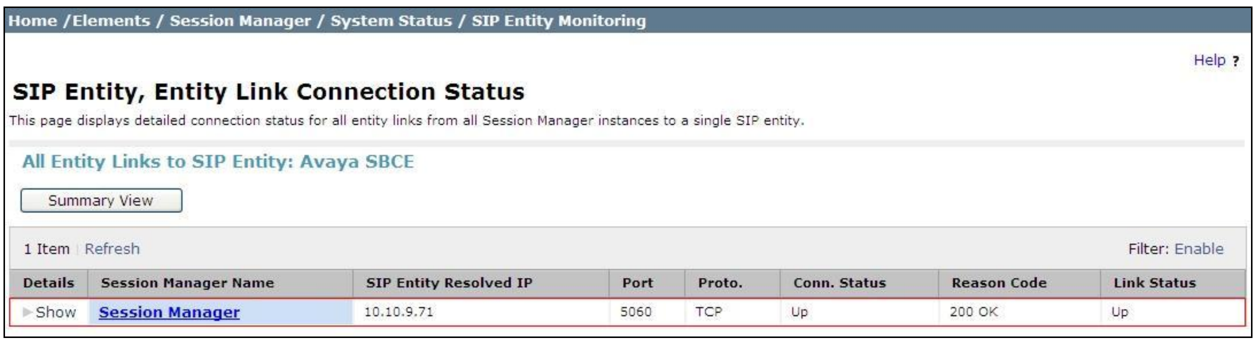
8. Swisscom SIP Service Provider Configuration

The setup for the use of Swisscom is by using the SIP trunk with an authenticated service. The configuration of Swisscoms authentication service to support the SIP trunk service is outside of the scope for these Application Notes and will not be covered. To obtain further information on Swisscoms 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.

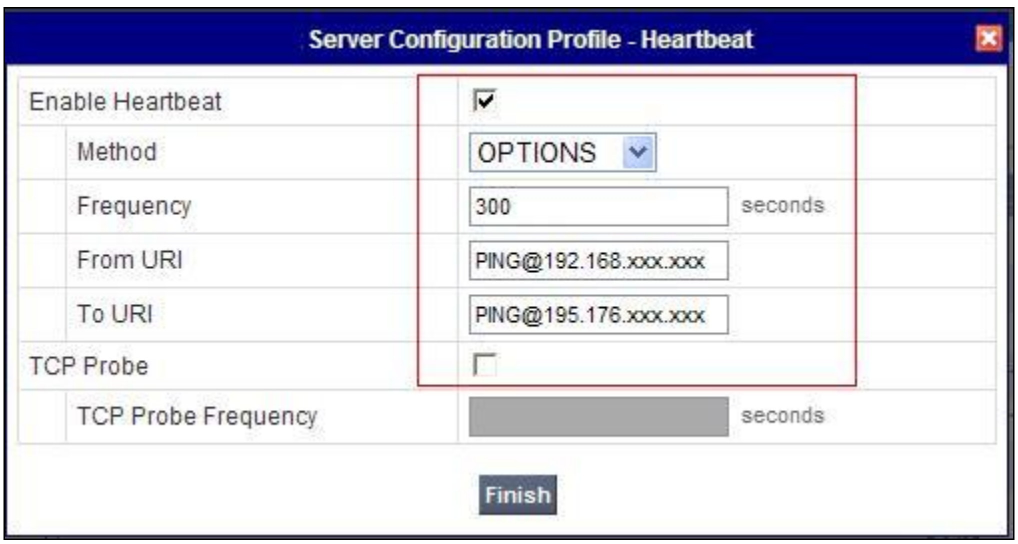
1. From System Manager Home Tab click on Session Manager and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **up**. The screenshot shows the status of the Entity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



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**.

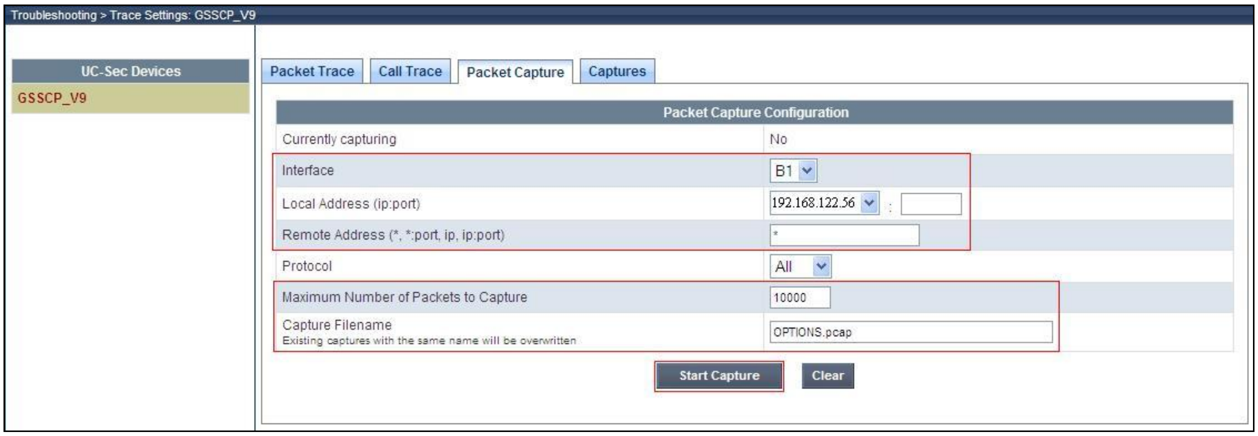
```
status trunk 1

                              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.
7. Should issues arise with the SIP trunk, check from the Avaya SBCE using OPTIONS. This is done by defining the heartbeat in the Server configuration then running a trace. To define the heartbeat, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side and click on the Trunk Server profile. Select the **Heartbeat** tab and click on **Edit**
   - Check the **Enable Heartbeat** box
   - Select **OPTIONS** from the **Method** drop down menu
   - Enter the **Frequency** in seconds, for convenience this can be set to the minimum value of **60** seconds
   - Enter the **From URI** in Fully Qualified Domain Name format
   - Enter the **To URI** in FQDN
   - Click on **Finish**



To define the trace, navigate to **Troubleshooting → Trace Settings** in the **UC-Sec Control Center** menu on the left hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu
- Select the signalling interface IP address from the **Local Address** drop down menu
- Enter the IP address of the Service Provider's 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**



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 200 OK response will be seen from the Service Provider.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to Swisscom SIP trunk service. 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 6.2*, March 2012.

[2] *Administering Avaya Aura® System Platform Release 6.2,* February 2012.

[3] *Administering Avaya Aura® Communication Manager*, Release 6.2, February 2012.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation*, February 2012, Document Number 555-245-205.

[5] *Implementing Avaya Aura® System Manager Release 6.2*, March 2012.

[6] *Implementing Avaya Aura® Session Manager*, February 2012, Document Number 03-603473

[7] *Administering Avaya Aura® Session Manager*, February 2012, Document Number 03-603324.

[8] *Various Application Notes for the Avaya Session Border Controller for Enterprise*, March 2012

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

.

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