



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Avaya Aura® Communication Manager R6.3, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise with Enterprise TLS and SRTP to support Vodafone Germany SIP Trunk Service - Issue 1.0**

## **Abstract**

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Vodafone Germany SIP Trunk 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. Within the Enterprise, TLS was used for transport of signalling and SRTP was used for transport of media to provide a secure solution. Vodafone Germany is a member of the DevConnect Service Provider program.

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

# 1. Introduction

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

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 PSTN phones using the SIP Trunk provided by Vodafone, calls made to analogue, SIP and H.323 endpoints at the enterprise.
- Outgoing calls from the enterprise site completed via Vodafone SIP Trunk to PSTN destinations, calls made from analogue, SIP and H.323 endpoints.
- Calls using the G.711A, G.729 and G.726-32 codecs.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media (also known as “shuffling”) with SIP and H.323 telephones.
- Secure transport of media within the enterprise using SRTP and transport of signalling using TLS.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by Vodafone SIP Trunk requiring Avaya response and sent by Avaya requiring Vodafone response.

## 2.2. Test Results

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

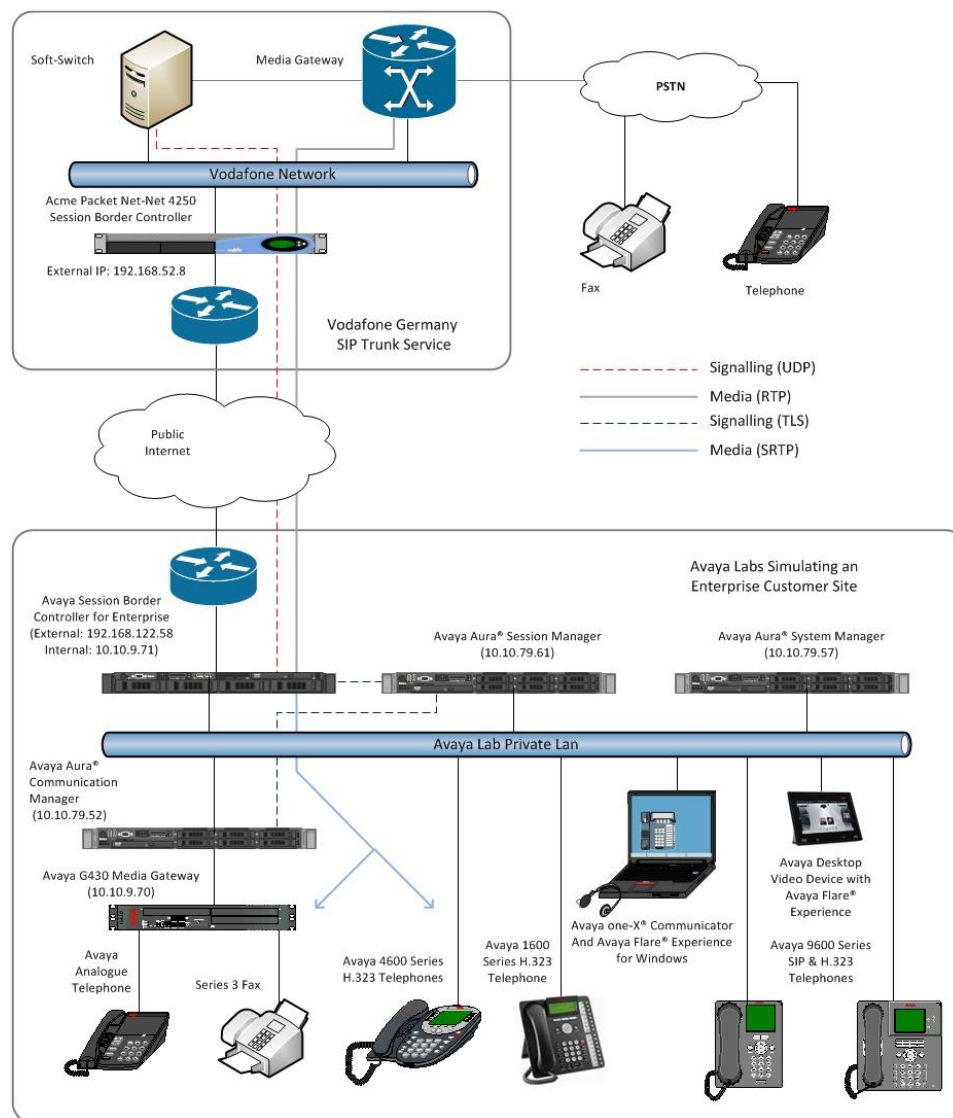
- During testing, there was a lag of over one second in the media on some outbound calls. This was thought to be an issue with the test network.
- When a call was put on hold in the network, there was no signalling to the enterprise to indicate that the call is on hold. This meant the test was not a valid test of SIP trunk functionality.
- Placing a call on hold for longer than twenty minutes resulted in a disconnect (BYE) from the network.
- At the time of testing, T.38 fax was not supported on the Vodafone SIP trunk.
- When testing mobility, EC500 Confirmed Answer was not successful. This function is not critical for SIP certification.
- Avaya one-X® Communicator did not function correctly when connected via SIP and tests were not completed. Although outbound calls were successful, inbound calls were rejected with SIP “488 Not Acceptable Here”. The fault appears to be unsuccessful negotiation of SRTP for the media. Fault report ONEXC-8777 is outstanding for this issue.

## 2.3. Support

For technical support on Vodafone Germany products please visit the website at [www.vodafone.de](http://www.vodafone.de) or contact an authorized Vodafone representative.

### 3. Reference Configuration

**Figure 1** illustrates the test configuration. The test configuration shows an Enterprise site connected to Vodafone SIP Trunk. 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 (audio only), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Avaya Flare® Experience for Windows running on a laptop PC. Within the enterprise, TLS was used for secure signalling transport and SRTP for media.



**Figure 1: Test Setup Vodafone Germany SIP Trunk to Avaya Enterprise**

## 4. Equipment and Software Validated

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

| Equipment/Software  | Release/Version   |
|---|---|
| <b>Avaya</b>  |   |
| Dell PowerEdge R620 running Session Manager on VM Version 8       | 6.3.4.0.634014<br>VMware Tools: 9.0.0.15210 (782409)                      |
| Dell PowerEdge R620 running System Manager on VM Version 8        | 6.3.8.0 Build No. 6.3.0.8.5682<br>Patch 6.3.8.2651 Build No. 6.3.4.4.1904 |
| Dell PowerEdge R620 running Communication Manager on VM Version 8 | R016x.03.0.124.0 patch 21106  |
| Avaya Session Border Controller Advanced for Enterprise Server    | 6.2.0.Q48   |
| G430 Media Gateway  | FW Version/HW Vintage: 34.5.1/1   |
| Avaya 1616 Phone (H.323)  | 1.3 Maintenance Release 4   |
| Avaya 4621 Phone (H.323)  | 2.9 SP 2  |
| Avaya 96x0 Phone (H.323)  | 3.2.1   |
| Avaya A175 Desktop Video Device (SIP)                             | Flare Experience Release 1.1.2  |
| Avaya 9630 Phone (SIP)  | R2.6.9  |
| Avaya 9608 Phone (SIP)  | R6.3.0  |
| Avaya one-X® Communicator (H.323) on Lenovo T510 Laptop PC        | 6.1.9.04-SP9-132  |
| Avaya Flare experience for Windows on Lenovo T510 Laptop PC       | Release 1.1.3.14  |
| Analogue Handset  | NA  |
| Analogue Fax  | NA  |
| <b>Vodafone</b>   |   |
| ACME Net-Net 4250 SBC   | SC6.1.0 MR-5 GA (Build 704)   |
| Italtel iSSW Softswitch   | 20.50.40  |

## 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 Vodafone SIP Trunk. For incoming calls, the Session Manager receives SIP messages from the Avaya SBC for Enterprise (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 Vodafone 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 Vodafone SIP Trunk 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:                        | 24000 | 10   |      |    |
| Maximum Administered Ad-hoc Video Conferencing Ports:   | 24000 | 0    |      |    |
| Maximum Number of DS1 Boards with Echo Cancellation:    | 522   | 0    |      |    |
| Maximum TN2501 VAL Boards:                              | 128   | 0    |      |    |
| Maximum Media Gateway VAL Sources:                      | 250   | 1    |      |    |
| Maximum TN2602 Boards with 80 VoIP Channels:            | 128   | 0    |      |    |
| Maximum TN2602 Boards with 320 VoIP Channels:           | 128   | 0    |      |    |
| Maximum Number of Expanded Meet-me Conference Ports:    | 300   | 0    |      |    |

On **Page 4**, verify that **IP Trunks** field is set to **y**. Check also that **Media Encryption Over IP** is set to **y** so that SRTP can be used within the enterprise.

|  |   |  |
|--|---|--|
| display system-parameters customer-options |   | Page 4 of 11                           |
| OPTIONAL FEATURES                          |   |  |
| Emergency Access to Attendant? y           |   | IP Stations? y                         |
| Enable 'dadmin' Login? y                   |   |  |
| Enhanced Conferencing? y                   |   | ISDN Feature Plus? n                   |
| Enhanced EC500? y                          | ISDN/SIP Network Call Redirection? y    |  |
| Enterprise Survivable Server? n            |   | ISDN-BRI Trunks? y                     |
| Enterprise Wide Licensing? n               |   | ISDN-PRI? y                            |
| ESS Administration? y                      | Local Survivable Processor? n           |  |
| Extended Cvg/Fwd Admin? y                  | Malicious Call Trace? y                 |  |
| External Device Alarm Admin? y             | Media Encryption Over IP? 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 the Session Manager. In this case, **SMVM1** and **10.10.79.61** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

|                       |                    |               |
|-----------------------|--------------------|---------------|
| display node-names ip |                    | IP NODE NAMES |
| Name                  | IP Address         |               |
| <b>SMVM1</b>          | <b>10.10.79.61</b> |               |
| default               | 0.0.0.0            |               |
| procr                 | 10.10.79.52        |               |
| procr6                | ::                 |               |

### 5.3. Administer IP Network Region

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

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



## 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 codecs supported by Vodafone were configured, namely **G.711A**, **G.729** and **G.726-32**. The **Media Encryption** fields are present if **Media Encryption Over IP** is set to **y** in the **system-parameters customer-options** form defined in **Section 5.1**. If SRTP is to be used for media within the enterprise, select the encryption. For the interoperability test, **1-srtp-aescm128-hmac80** was selected.

change ip-codec-set 1 Page 1 of 2

IP Codec Set

Codec Set: 1

| Audio Codec      | Silence Suppression | Frames Per Pkt | Packet Size (ms) |
|------------------|---------------------|----------------|------------------|
| 1: <b>G.729</b>  | <b>n</b>            | <b>2</b>       | <b>20</b>        |
| 2: <b>G.711A</b> | <b>n</b>            | <b>2</b>       | <b>20</b>        |
| 3:               |                     |                |                  |
| 4:               |                     |                |                  |
| 5:               |                     |                |                  |
| 6:               |                     |                |                  |
| 7:               |                     |                |                  |

Media Encryption

1: **1-srtp-aescm128-hmac80**

2:

3:

Vodafone SIP Trunk does not support T.38 for transmission of fax. To allow transmission using G.711, Navigate to **Page 2** and set the **FAX - Mode** to **t.38-G711-fallback**.

change ip-codec-set 1 Page 2 of 2

IP Codec Set

Allow Direct-IP Multimedia? n

|               | Mode                      | Redundancy |        |
|---------------|---------------------------|------------|--------|
| <b>FAX</b>    | <b>t.38-G711-fallback</b> | 0          | ECM: y |
| Modem         | off                       | 0          |        |
| TDD/TTY       | US                        | 3          |        |
| Clear-channel | n                         | 0          |        |

**Note:** The fax **Mode** can be set to **off** to allow transport of fax using G.711. During test **t.38-G711-fallback** was used so that incoming fax calls set up with G729 would renegotiate to G.711. This renegotiation did not take place for outgoing fax calls and as a result they were only successful when G.711 was the first codec negotiated.

## 5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Vodafone SIP Trunk network. During test, this was configured to use TLS and port 5061 to represent the security requirements for signalling that may be in place at the customer's site.

Configure the **Signaling Group** using the **add signaling-group x** command as follows:

- Set **Group Type** to **sip**.
- Set **Transport Method** to **tls**.
- Set **Enforce SIPS URI for SRTP?** to **n** as SRTP and TLS are only used within the enterprise and are not to be used end to end.
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Far-end Node Name** to the Session Manager (node name **SMVM1** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5061** (Common TLS 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 the CM to accept calls from any SIP domain on the associated trunk ).
- Set **Direct IP-IP Audio Connections** to **y**.
- Leave DTMF over IP at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager).

The default values for the other fields may be used.

| add signaling-group 1   |   | Page 1 of 2 |
|---|---|-------------|
| SIGNALING GROUP   |   |             |
| Group Number: 1   | Group Type: sip                           |             |
| IMS Enabled? n  | Transport Method: tls                     |             |
| Q-SIP? n  | Enforce SIPS URI for SRTP? n              |             |
| IP Video? n   | 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: SMVM1                  |             |
| Near-end Listen Port: 5061  | Far-end Listen Port: 5061                 |             |
| Far-end Network Region: 1   |   |             |
| Far-end Domain:   |   |             |
| Incoming Dialog Loopbacks: eliminate  | Bypass If IP Threshold Exceeded? n        |             |
| DTMF over IP: rtp-payload   | RFC 3389 Comfort Noise? n                 |             |
| Session Establishment Timer(min): 3   | Direct IP-IP Audio Connections? y         |             |
| Enable Layer 3 Test? y  | IP Audio Hairpinning? n                   |             |
| H.323 Station Outgoing Direct Media? n  | Initial IP-IP Direct Media? n             |             |
| Alternate Route Timer(sec): 6   |   |             |

## 5.6. Administer SIP Trunk Group

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

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

|                            |                     |                                |          |
|----------------------------|---------------------|--------------------------------|----------|
| add trunk-group 1          |                     | Page 1 of 21                   |          |
| TRUNK GROUP                |                     |                                |          |
| Group Number: 1            | Group Type: sip     | CDR Reports: y                 |          |
| Group Name: 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 Vodafone 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: 10000 |  |
| SCCAN? n   | Digital Loss Group: 18 |                                  |  |
| Preferred Minimum Session Refresh Interval(sec): 900 |                        |                                  |  |
| Disconnect Supervision - In? y Out? y                |                        |                                  |  |

On **Page 3**, set the **Numbering Format** field to **private**. This allows delivery of CLI in formats other than E.164 with leading “+”. In test, CLI was sent as the national number with no leading zeros. This format was successfully verified in the network.

|                                  |                                |
|----------------------------------|--------------------------------|
| add trunk-group 1                | Page 3 of 21                   |
| TRUNK FEATURES                   |                                |
| ACA Assignment? n                | Measured: none                 |
|                                  | Maintenance Tests? y           |
| <b>Numbering Format: private</b> |                                |
|                                  | UI Treatment: service-provider |
|                                  | Replace Restricted Numbers? n  |
|                                  | Replace Unavailable Numbers? n |

On **Page 4** of this form:

- Set **Send Transferring Party Information** to **y**.
- Set **Send Diversion Header** to **y**.
- Set **Support Request History** to **n** as the required information for forwarded, transferred and mobility calls will be sent in the Diversion and Transferring Party Information headers.
- Set the **Telephone Event Payload Type** to **98**.
- Set the **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on the Communication Manager extension.

|   |   |
|---|---|
| add trunk-group 1   | Page 4 of 21                                      |
| PROTOCOL VARIATIONS   |   |
|   | Mark Users as Phone? n                            |
| Prepend '+' to Calling/Alerting/Diverting/Connected Number? n |   |
|   | Send Transferring Party Information? y            |
|   | Network Call Redirection? n                       |
|   | <b>Send Diversion Header? y</b>                   |
|   | <b>Support Request History? n</b>                 |
|   | <b>Telephone Event Payload Type: 98</b>           |
|   | Convert 180 to 183 for Early Media? n             |
|   | Always Use re-INVITE for Display Updates? n       |
|   | <b>Identity for Calling Party Display: From</b>   |
|   | Block Sending Calling Party Location in INVITE? n |
|   | Accept Redirect to Blank User Destination? n      |
|   | Enable Q-SIP? n                                   |

**Note:** The Payload Type is a dynamic value and the meaning is agreed during codec negotiation which was tested successfully. The value used is therefore not critical, 98 is shown as that is the value used during testing. The Payload Type defined on Communication Manager is not applied to calls from SIP end-points.

## 5.7. Administer Calling Party Number Information

Use the **change private-unknown-numbering** command to configure Communication Manager to send the calling party number in the format required. In test, calling party number was sent as the national number with leading zero as the format expected in the network for calling party number verification. This calling party number is sent in the SIP From, Contact and PAI headers as well as the Diversion header for forwarded calls. The number is displayed on display-equipped PSTN telephones with any reformatting performed in the network.

| change private-numbering 0 |      |        |               |       | Page 1 of 2           |
|----------------------------|------|--------|---------------|-------|-----------------------|
| NUMBERING - PRIVATE FORMAT |      |        |               |       |                       |
| Ext                        | Ext  | Trk    | Private       | Total |                       |
| Len                        | Code | Grp(s) | Prefix        | Len   |                       |
| 4                          | 2000 | 1      | 069138nnnn100 | 13    | Total Administered: 9 |
| 4                          | 2208 | 1      | 069138nnnn103 | 13    | Maximum Entries: 540  |
| 4                          | 2316 | 1      | 069138nnnn105 | 13    |                       |
| 4                          | 2346 | 1      | 069138nnnn102 | 13    |                       |
| 4                          | 2396 | 1      | 069138nnnn101 | 13    |                       |
| 4                          | 2400 | 1      | 069138nnnn106 | 13    |                       |
| 4                          | 2401 | 1      | 069138nnnn106 | 13    |                       |
| 4                          | 2460 | 1      | 069138nnnn107 | 13    |                       |
| 4                          | 2611 | 1      | 069138nnnn104 | 13    |                       |

**Note:** The private numbers in the above screenshot have been modified for security.

## 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 Vodafone SIP Trunk. 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          |  |                |
| <b>Auto Route Selection (ARS) - Access Code 1: 9</b> |  | Access Code 2: |

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0. 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 String            | Total Min | Total Max | Route Pattern | Call Type | Node Num | ANI Req'd |                 |
| 0                        | 11        | 14        | 1             | pubu      |          | n         |                 |
| 00                       | 13        | 15        | 1             | pubu      |          | n         |                 |
| 0035391                  | 13        | 13        | 1             | pubu      |          | n         |                 |
| 0800                     | 8         | 14        | 1             | pubu      |          | n         |                 |
| 118                      | 3         | 6         | 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   |     |      |                 |      |               |     |

## 5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the Communication Manager extensions. The incoming digits sent in the INVITE message from Vodafone can be manipulated as necessary to route calls to the desired extension. During test, the incoming DDI numbers were changed in the Session Manager to the Communication Manager Extension number using an adaptation. When done this way, there is no requirement for any incoming digit translation in the Communication Manager. If incoming digit translation is required, use the **change inc-call-handling-trmt trunk-group x** command where **x** is the Trunk Group defined in Section 5.6.

|   |        |        |            |              |  |
|---|--------|--------|------------|--------------|--|
| change inc-call-handling-trmt trunk-group 1 |        |        |            | Page 1 of 30 |  |
| INCOMING CALL HANDLING TREATMENT            |        |        |            |              |  |
| Service/                                    | Number | Number | Del Insert |              |  |
| Feature                                     | Len    | Digits |            |              |  |

**Note:** One reason for configuring the enterprise in this way is to ensure that the message waiting indicator is successfully sent to SIP extensions when a voice mail message is available and unread.

## 5.10. EC500 Configuration

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

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** if required by the routing configuration. The normal ARS code is not required here.
- For the **Phone Number** enter the phone that will also be called (e.g. **0035389434nnnn**).
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing.
- Set the **Config Set** to **1**.

|   |             |        |    |                |           |        |      |    |   |
|---|-------------|--------|----|----------------|-----------|--------|------|----|---|
| change off-pbx-telephone station-mapping 2396 |             |        |    |                |           | Page   | 1    | of | 3 |
| STATIONS WITH OFF-PBX TELEPHONE INTEGRATION   |             |        |    |                |           |        |      |    |   |
| Station                                       | Application | Dial   | CC | Phone Number   | Trunk     | Config | Dual |    |   |
| Extension                                     |             | Prefix |    |                | Selection | Set    | Mode |    |   |
| 2396  | EC500       | -      |    | 0035389434nnnn | 1         | 1      |      |    |   |
| -   |             |        |    |                |           |        |      |    |   |

**Note:** The phone number shown is for a mobile phone used for testing at Avaya Labs and is in international format with international dialling prefix 00. 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 configuration by entering **save translation**

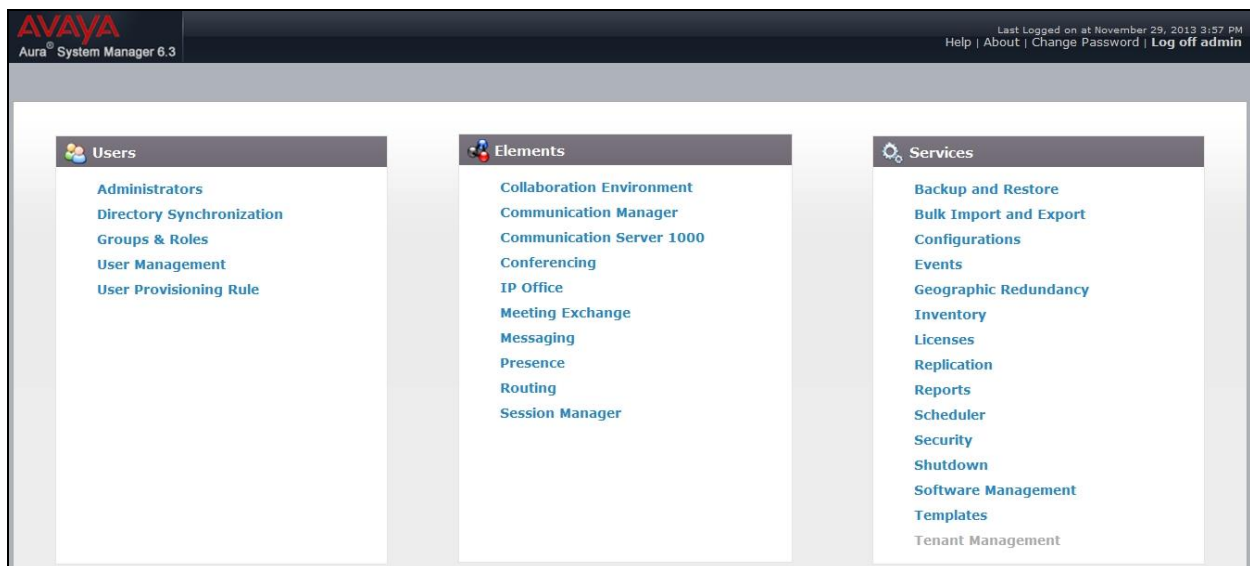
## 6. Configuring Avaya Aura® Session Manager

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

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

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

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





## 6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name of the enterprise site or a name agreed with Vodafone; this will be the same as specified in the Authoritative Domain specified in the IP Network Region on Communication Manager. Refer to **Section 5.3** for details. In test, **avaya.com** was used. Optionally, a description for the domain can be entered in the Notes field (not shown). Click **Commit** to save changes.

The screenshot shows the 'Domain Management' interface. On the left is a navigation menu with 'Routing' selected, and 'Domains' highlighted. The main area shows a breadcrumb 'Home / Elements / Routing / Domains' and a 'Domain Management' section with buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below this is a table with one item: 'avaya.com' of type 'sip'. A 'Filter: Enable' link is on the right.

| Name      | Type | Notes |
|-----------|------|-------|
| avaya.com | sip  |       |

**Note:** If the existing domain name used in the enterprise equipment does not match that used in the network, a Session Manager adaptation can be used to change it, or it can be changed on the Avaya SBCE.

## 6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu. Under **General**, in the **Name** field, enter an informative name for the location.

The screenshot shows the 'Location Details' form. It has a 'General' section with a required 'Name' field containing 'Galway' and an empty 'Notes' field. 'Commit' and 'Cancel' buttons are at the top right.

**Name:** Galway

**Notes:**

Scroll down for bandwidth configuration. During testing, these were left at default values.

**Dial Plan Transparency in Survivable Mode**

Enabled: ☒

Listed Directory Number:

Associated CM SIP Entity:

**Overall Managed Bandwidth**

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

**Per-Call Bandwidth Parameters**

Maximum Multimedia Bandwidth (Intra-Location):  Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):  Kbit/Sec

\* Minimum Multimedia Bandwidth:  Kbit/Sec

\* Default Audio Bandwidth:  Kbit/sec

Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, \* is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the test enterprise.

**Alarm Threshold**

Overall Alarm Threshold:  %

Multimedia Alarm Threshold:  %

\* Latency before Overall Alarm Trigger:  Minutes

\* Latency before Multimedia Alarm Trigger:  Minutes

**Location Pattern**

2 Items

| IP Address Pattern                               | Notes         |
|--|---------------|
| <input checked="" type="checkbox"/> * 10.10.79.* | Lab VMWare    |
| <input checked="" type="checkbox"/> * 10.10.9.*  | Lab Equipment |

Select : All, None

## 6.4. Administer Adaptations

Calls from Vodafone are received at the enterprise in national format with leading “0” on the Request URI. An Adaptation specific to Vodafone is used to convert the called number to an extension number as defined in the Communication Manager before onward routing to Communication Manager SIP Entity and removes the requirement for incoming digit manipulation on Communication Manager. It is also applied to messages coming from Communication Manager so that the SIP PUBLISH message for message waiting indicator on SIP end-points is handled correctly.

On the **Routing** tab select **Adaptations** from the left-hand menu. Click on **New** (not shown).

- In the **Adaptation name** field, enter a descriptive title for the adaptation.
- In the **Module name** enter **DigitConversionAdapter**. This is used for simple digit conversion adaptations.
- In the **Module parameter** field, select **Name-Value Parameter** in the **Module Parameter Type** drop down menu and enter **fromto** with a value of **true** in the resultant dialogue box. This will apply the adaptation to the From and To headers as well as the Request URI.

Home / Elements / Routing / Adaptations

**Adaptation Details** Commit Cancel

**General**

\* Adaptation Name: VFDE\_PSTN

Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Add Remove

| <input type="checkbox"/> | Name   | Value |
|--------------------------|--------|-------|
| <input type="checkbox"/> | fromto | true  |

Select : All, None

Egress URI Parameters:

Notes:

Scroll down and in the section **Digit Conversion for Incoming Calls to SM**, click on **Add**. An additional row will appear. This allows information to be entered for the manipulation of numbers coming from the network. This is where the called party number is translated from national format to the extension number for termination of calls on Communication Manager.

The screenshot below shows a translation for each called party number. This is not normally necessary where the extension number forms part of the national number. When this is the case, a deletion of the leading digits is required.

- Under **Matching Pattern** enter the DDI number as received from the network.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the incoming DDI number.
- Under **Delete Digits** enter the number of digits to delete to leave only the extension number remaining, during test all had to be deleted as the extension number did not form part of the national number.
- Under **Insert Digits** enter digits to be inserted. During test, this was the full extension number. If the extension number forms part of the DDI number, there will be no entry required here.
- Under **Address to Modify** choose **destination** from the drop down box to apply this rule to the To and Request-Line headers only.

### Digit Conversion for Incoming Calls to SM

Add
Remove

9 Items
Filter: Enable

|                          | Matching Pattern | Min | Max | Phone Context | Delete Digits | Insert Digits | Address to modify | Adaptation Data | Notes |
|--------------------------|------------------|-----|-----|---------------|---------------|---------------|-------------------|-----------------|-------|
| <input type="checkbox"/> | *069138nnnn100   | *13 | *13 |               | *13           | 2000          | destination       |                 |       |
| <input type="checkbox"/> | *069138nnnn101   | *13 | *13 |               | *13           | 2396          | destination       |                 |       |
| <input type="checkbox"/> | *069138nnnn102   | *13 | *13 |               | *13           | 2346          | destination       |                 |       |
| <input type="checkbox"/> | *069138nnnn103   | *13 | *13 |               | *13           | 2208          | destination       |                 |       |
| <input type="checkbox"/> | *069138nnnn104   | *13 | *13 |               | *13           | 2611          | destination       |                 |       |
| <input type="checkbox"/> | *069138nnnn105   | *13 | *13 |               | *13           | 2316          | destination       |                 |       |
| <input type="checkbox"/> | *069138nnnn106   | *13 | *13 |               | *13           | 2401          | destination       |                 |       |
| <input type="checkbox"/> | *069138nnnn107   | *13 | *13 |               | *13           | 6103          | destination       |                 |       |
| <input type="checkbox"/> | *069138nnnn108   | *13 | *13 |               | *13           | 2501          | destination       |                 |       |

Select : All, None

### Digit Conversion for Outgoing Calls from SM

Add
Remove

0 Items
Filter: Enable

|  | Matching Pattern | Min | Max | Phone Context | Delete Digits | Insert Digits | Address to modify | Adaptation Data | Notes |
|--|------------------|-----|-----|---------------|---------------|---------------|-------------------|-----------------|-------|
|--|------------------|-----|-----|---------------|---------------|---------------|-------------------|-----------------|-------|

Commit
Cancel

**Note:** In the above screenshots the DDI numbers are partially obscured.

## 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 the 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 **Adaptation** field (not available for the Session Manager SIP Entity), select the appropriate Adaptation from the drop down menu.
- In the **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field enter the time zone for the SIP Entity.

In this configuration there are three SIP Entities:

- Avaya Aura® Session Manager SIP Entity.
- Avaya Aura® Communication Manager SIP Entity.
- Avaya Session Border Controller for Enterprise (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 signalling interface.

The screenshot shows a web-based configuration interface for SIP Entities. The breadcrumb trail at the top is "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details" with "Commit" and "Cancel" buttons in the top right. The "General" tab is selected. The form contains the following fields:

- Name:** VM79\_SM
- FQDN or IP Address:** 10.10.79.61
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text area)
- Location:** Galway (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Credential name:** (empty text area)

Below the General section is the "SIP Link Monitoring" section, which contains a dropdown menu set to "Use Session Manager Configuration".

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

**Port**

TCP Failover port:

TLS Failover port:

3 Items Filter: Enable

| <input type="checkbox"/> | Port | Protocol | Default Domain | Notes                |
|--------------------------|------|----------|----------------|----------------------|
| <input type="checkbox"/> | 5060 | TCP      | avaya.com      | <input type="text"/> |
| <input type="checkbox"/> | 5060 | UDP      | avaya.com      | <input type="text"/> |
| <input type="checkbox"/> | 5061 | TLS      | avaya.com      | <input type="text"/> |

Select : All, None

### 6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. Set the **Adaptation** to that defined in **Section 6.4**, the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities

**SIP Entity Details**

**General**

\* **Name:**

\* **FQDN or IP Address:**

**Type:**

**Notes:**

**Adaptation:**

**Location:**

**Time Zone:**

\* **SIP Timer B/F (in seconds):**

**Credential name:**

**Call Detail Recording:**

**Note:** The adaptation selected for Communication Manager modifies the called party number when it corresponds to the DDI number for the enterprise. This is an unusual case as the majority of calls are going out to the PSTN. It is useful to apply it to Communication Manager, however, as the message waiting indicator for SIP endpoints is sent to the address in the contact header, i.e. the DDI number of the extension. The adaptation ensures the message waiting indicator is sent correctly to the SIP endpoint.

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

The screenshot shows two configuration sections. The first section, 'Loop Detection', has a 'Loop Detection Mode' dropdown menu set to 'Off'. The second section, 'SIP Link Monitoring', has a 'SIP Link Monitoring' dropdown menu set to 'Use Session Manager Configuration'.

### 6.5.3. 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 the **Adaptation** to that defined in **Section 6.4**, the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

The screenshot shows the 'SIP Entity Details' configuration page for 'ASBCE\_45'. The 'General' tab is selected. The 'Name' field is 'ASBCE\_45'. The 'FQDN or IP Address' field is '10.10.9.71'. The 'Type' dropdown is set to 'SIP Trunk'. The 'Notes' field is empty. The 'Adaptation' dropdown is set to 'VFDE\_PSTN'. The 'Location' dropdown is set to 'Galway'. The 'Time Zone' dropdown is set to 'Europe/Dublin'. The 'SIP Timer B/F (in seconds)' field is '4'. The 'Credential name' field is empty. The 'Call Detail Recording' dropdown is set to 'egress'. The page has a breadcrumb trail 'Home / Elements / Routing / SIP Entities' and 'Commit' and 'Cancel' buttons.

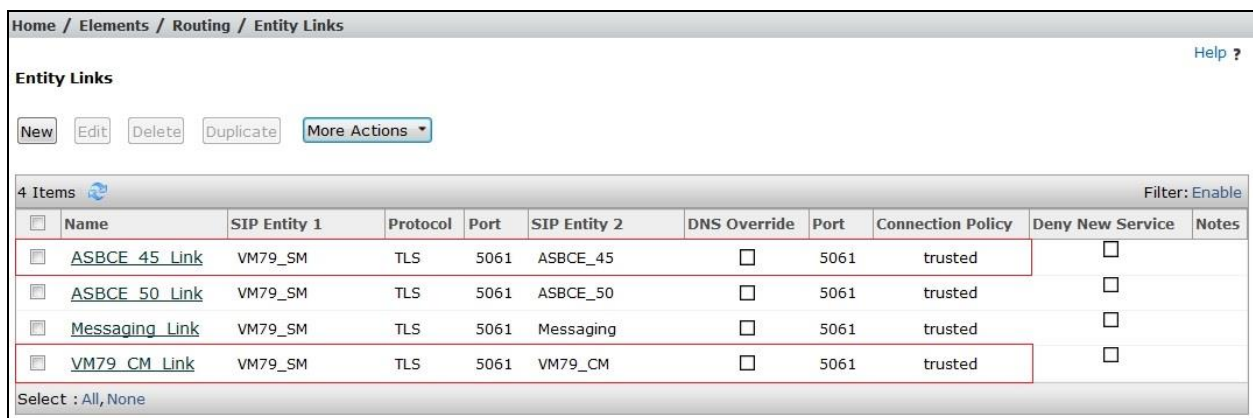


## 6.6. Administer Entity Links

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

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



| Home / Elements / Routing / Entity Links |                |              |          |      |              |                          |      |                   |                          | Help ? |
|--|----------------|--------------|----------|------|--------------|--------------------------|------|-------------------|--------------------------|--------|
| Entity Links                             |                |              |          |      |              |                          |      |                   |                          |        |
| New Edit Delete Duplicate More Actions   |                |              |          |      |              |                          |      |                   |                          |        |
| 4 Items Filter: Enable                   |                |              |          |      |              |                          |      |                   |                          |        |
| <input type="checkbox"/>                 | Name           | SIP Entity 1 | Protocol | Port | SIP Entity 2 | DNS Override             | Port | Connection Policy | Deny New Service         | Notes  |
| <input type="checkbox"/>                 | ASBCE_45_Link  | VM79_SM      | TLS      | 5061 | ASBCE_45     | <input type="checkbox"/> | 5061 | trusted           | <input type="checkbox"/> |        |
| <input type="checkbox"/>                 | ASBCE_50_Link  | VM79_SM      | TLS      | 5061 | ASBCE_50     | <input type="checkbox"/> | 5061 | trusted           | <input type="checkbox"/> |        |
| <input type="checkbox"/>                 | Messaging_Link | VM79_SM      | TLS      | 5061 | Messaging    | <input type="checkbox"/> | 5061 | trusted           | <input type="checkbox"/> |        |
| <input type="checkbox"/>                 | VM79_CM_Link   | VM79_SM      | TLS      | 5061 | VM79_CM      | <input type="checkbox"/> | 5061 | trusted           | <input type="checkbox"/> |        |
| Select : All, None                       |                |              |          |      |              |                          |      |                   |                          |        |

**Note:** The **Messaging\_Link** Entity Link is used for the Avaya Aura ® Messaging system and is not described in this document.

## 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.



Home / Elements / Routing / Routing Policies Help ?

**Routing Policy Details** Commit Cancel

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

| Name    | FQDN or IP Address | Type | Notes |
|---------|--------------------|------|-------|
| VM79_CM | 10.10.79.52        | CM   |       |

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

| Ranking                    | Name | Mon                                 | Tue                                 | Wed                                 | Thu                                 | Fri                                 | Sat                                 | Sun                                 | Start Time | End Time | Notes           |
|----------------------------|------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|------------|----------|-----------------|
| <input type="checkbox"/> 0 | 24/7 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 00:00      | 23:59    | Time Range 24/7 |

Select : All, None

The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed to the PSTN via the Vodafone SIP Trunk.

Home / Elements / Routing / Routing Policies Help ?

**Routing Policy Details** Commit Cancel

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

| Name     | FQDN or IP Address | Type      | Notes |
|----------|--------------------|-----------|-------|
| ASBCE_45 | 10.10.9.71         | SIP Trunk |       |

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

| Ranking                    | Name | Mon                                 | Tue                                 | Wed                                 | Thu                                 | Fri                                 | Sat                                 | Sun                                 | Start Time | End Time | Notes           |
|----------------------------|------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|------------|----------|-----------------|
| <input type="checkbox"/> 0 | 24/7 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 00:00      | 23:59    | Time Range 24/7 |

Select : All, None

## 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** and enter details 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.

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

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel Help ?

**General**

\* Pattern: 0

\* Min: 8

\* Max: 15

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

**Originating Locations and Routing Policies**

Add Remove

1 Item Filter: Enable

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled  | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|---------------------|------|--------------------------|----------------------------|----------------------|
| <input type="checkbox"/> | -ALL-                     |                            | External_ASBCE_45   |      | <input type="checkbox"/> | ASBCE_45                   |                      |

Select : All, None

The following screen shows the test dial pattern configured for Communication Manager which identifies the extension number. All extension numbers used during testing were four digit numbers starting with 2.

Home / Elements / Routing / Dial Patterns Help ?

**Dial Pattern Details** Commit Cancel

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

1 Item Filter: Enable

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled  | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|---------------------|------|--------------------------|----------------------------|----------------------|
| <input type="checkbox"/> | -ALL-                     |                            | Internal_VM79_CM    |      | <input type="checkbox"/> | VM79_CM                    |                      |

Select : All, None

**Note:** The above configuration is used where the called party number has been converted to an extension number on Communication Manager using an adaptation. If an adaptation is not used, a dial pattern will be required for the incoming DDI number.

## 6.9. Administer Application for Avaya Aura® Communication Manager

The Application for SIP endpoints should already be defined, the following is shown for information. From the **Home** tab select **Session Manager** from the menu. In the resulting tab from the left panel menu select **Application Configuration** → **Applications** and click **New**.

- In the **Name** field enter a name for the application.
- In the **SIP Entity** field select the SIP entity for the Communication Manager.
- In the **CM System for SIP Entity** field select the SIP entity for the Communication Manager and select **Commit** to save the configuration.

Home Session Manager \* User Management \*

Home / Elements / Session Manager / Application Configuration / Applications

**Application Editor** Commit Cancel

**Application**

\*Name:

\*SIP Entity:

\*CM System for SIP Entity:   [View/Add CM Systems](#)

Description:

## 6.10. Administer Application Sequence for Avaya Aura® Communication Manager

The Application Sequence for SIP endpoints should already be defined, the following is shown for information. From the left panel navigate to **Session Manager → Application Configuration → Application Sequences** and click on **New**.

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

Home / Elements / Session Manager / Application Configuration / Application Sequences [Help ?](#)

### Application Sequence Editor

**Application Sequence**

\*Name

Description

**Applications in this Sequence**

1 Item

| <input type="checkbox"/> | Sequence Order<br>(first to last) | Name                        | SIP Entity | Mandatory                           | Description |
|--------------------------|-----------------------------------|-----------------------------|------------|-------------------------------------|-------------|
| <input type="checkbox"/> | 1                                 | <a href="#">VM79_CM_App</a> | VM79_CM    | <input checked="" type="checkbox"/> |             |

Select : All, None

**Available Applications**

1 Item [Filter: Enable](#)

| <input type="checkbox"/> | Name                        | SIP Entity | Description |
|--------------------------|-----------------------------|------------|-------------|
| <input type="checkbox"/> | <a href="#">VM79_CM_App</a> | VM79_CM    |             |

## 6.11. Administer SIP Extensions

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

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields.
- In the **Login Name** field enter a unique system login name in the form of user@domain e.g. **2401@avaya.com** which is used to create the user's primary handle.
- The **Authentication Type** should be **Basic**.
- In the **Password/Confirm Password** fields enter an alphanumeric password.
- Set the **Language Preference** and **Time Zone** (not shown) as required.

The screenshot shows the 'Identity' tab of a user provisioning interface. At the top, there are tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. Below the tabs is a 'User Provisioning Rule' dropdown. The 'Identity' section contains several fields: 'Last Name' (Comm), 'Last Name (Latin Translation)' (Comm), 'First Name' (one-X), 'First Name (Latin Translation)' (one-X), 'Middle Name' (empty), 'Description' (empty), 'Login Name' (2401@avaya.com), 'Authentication Type' (Basic), 'Password' (masked with dots), 'Confirm Password' (masked with dots), 'Localized Display Name' (empty), 'Endpoint Display Name' (empty), 'Title' (empty), and 'Language Preference' (English (United Kingdom)).

On the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it.

The screenshot shows the 'Communication Profile' tab of the same user provisioning interface. It features a 'Communication Profile Password' field (masked with dots) and a 'Confirm Password' field (masked with dots). Below these are buttons for 'New', 'Delete', 'Done', and 'Cancel'. A section titled 'Name' shows a list with 'Primary' selected. Below this, the 'Name' field is set to 'Primary' and the 'Default' checkbox is checked. At the bottom, there is a 'Communication Address' section with buttons for 'New', 'Edit', and 'Delete'. Below these buttons is a table with columns 'Type', 'Handle', and 'Domain'. The table currently shows 'No Records found'.

Expand the **Communication Address** section and click **New**. For the **Type** field select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.

**Communication Address**

New Edit Delete

| Type             | Handle | Domain |
|------------------|--------|--------|
| No Records found |        |        |

Type: Avaya SIP

\* Fully Qualified Address: 2401 @ avaya.com

Add Cancel

Expand the **Session Manager Profile** section.

- Make sure the **Session Manager Profile** check box is checked.
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field.
- Select the appropriate application sequence from the drop-down menu in the **Origination Sequence** field configured in **Section 6.10**.
- Select the appropriate application sequence from the drop-down menu in the **Termination Sequence** field configured in **Section 6.10**.
- Select the appropriate location from the drop-down menu in the **Home Location** field.

☒ **Session Manager Profile**

**SIP Registration**

\* Primary Session Manager: VM79\_SM

Secondary Session Manager: (None)

Survivability Server: (None)

Max. Simultaneous Devices: 1

Block New Registration When Maximum Registrations Active? ☐

| Primary | Secondary | Maximum |
|---------|-----------|---------|
| 1       | 0         | 1       |

**Application Sequences**

Origination Sequence: VM79\_CM\_App\_Seq

Termination Sequence: VM79\_CM\_App\_Seq

**Call Routing Settings**

\* Home Location: Galway

Conference Factory Set: (None)

Expand the **Endpoint Profile** section.

- Select the Communication Manager SIP Entity from the **System** drop-down menu.
- Select **Endpoint** from the drop-down menu for **Profile Type**.
- Enter the extension in the **Extension** field.
- Select the desired template from the **Template** drop-down menu.
- In the **Port** field **IP** is automatically inserted.
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box.
- Select **Commit** (Not Shown) to save changes and the System Manager will add the Communication Manager user configuration automatically.

The screenshot shows the 'CM Endpoint Profile' configuration form. It includes the following fields and options:

- System:** CM\_VM\_Element (dropdown)
- Profile Type:** Endpoint (dropdown)
- Use Existing Endpoints:** ☐
- Extension:** 2401 (text input) with an **Endpoint Editor** button
- Template:** 9630SIP\_DEFAULT\_CM\_6\_3 (dropdown)
- Set Type:** 9630SIP (text input)
- Security Code:** (text input)
- Port:** IP (text input)
- Voice Mail Number:** (text input)
- Preferred Handle:** (None) (dropdown)
- Enhanced Callr-Info display for 1-line phones:** ☐
- Delete Endpoint on Unassign of Endpoint from User or on Delete User:** ☒
- Override Endpoint Name and Localized Name:** ☒



## 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. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented. Log in using username ucsec and the appropriate password.



The login screen features the Avaya logo on the left and a 'Log In' section on the right. The 'Log In' section includes fields for 'Username:' and 'Password:', a 'Log In' button, and a disclaimer text block.

**AVAYA**

**Log In**

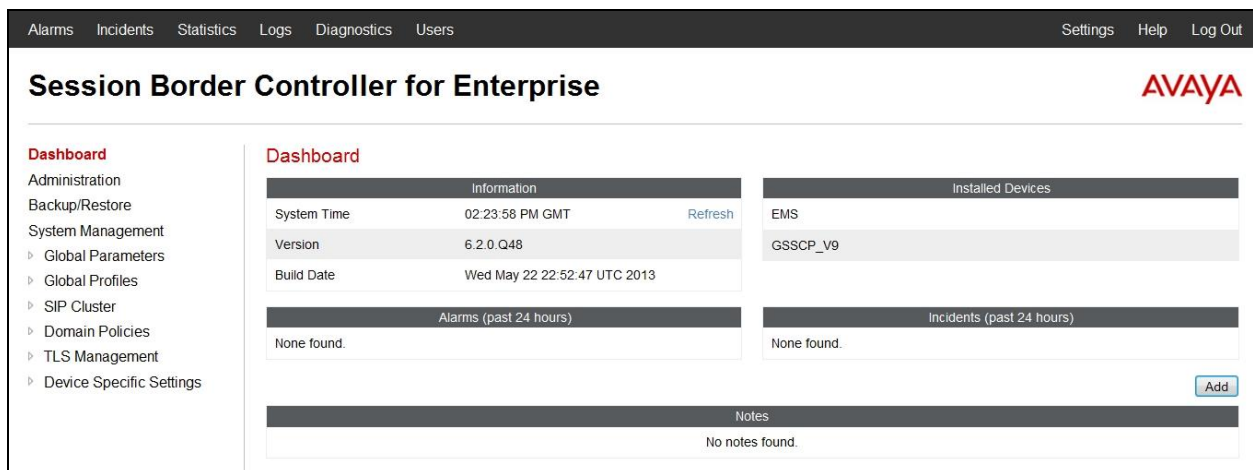
Username:

Password:

**Session Border Controller for Enterprise**

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

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.



The dashboard has a top navigation bar with links: Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is titled 'Session Border Controller for Enterprise' and features a left-hand menu and several data panels.

**Session Border Controller for Enterprise**

**Dashboard**

**Information**

|             |                              |                         |
|-------------|------------------------------|-------------------------|
| System Time | 02:23:58 PM GMT              | <a href="#">Refresh</a> |
| Version     | 6.2.0.Q48                    |                         |
| Build Date  | Wed May 22 22:52:47 UTC 2013 |                         |

**Installed Devices**

|          |
|----------|
| EMS      |
| GSSCP_V9 |

**Alarms (past 24 hours)**

None found.

**Incidents (past 24 hours)**

None found.

**Notes**

No notes found.

[Add](#)

**Left-hand Menu:**

- Dashboard
- Administration
- Backup/Restore
- System Management
  - Global Parameters
  - Global Profiles
  - SIP Cluster
  - Domain Policies
  - TLS Management
  - Device Specific Settings



## 7.2. 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** in the main 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 **Netmask** for interfaces A1 and B1.
- Define the internal IP address and Gateway and assign to interface **A1**.
- Click on **Add**.
- Define the external IP address and Gateway 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).

Session Border Controller for Enterprise

Network Management: GSSCP\_V9

Devices: GSSCP\_V9

Network Configuration | Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask: 255.255.255.0 | A2 Netmask: | B1 Netmask: 255.255.255.128 | B2 Netmask: | Add | Save | Clear

| IP Address     | Public IP | Gateway        | Interface |        |
|----------------|-----------|----------------|-----------|--------|
| 10.10.9.71     |           | 10.10.9.1      | A1        | Delete |
| 192.168.122.58 |           | 192.168.122.51 | B1        | Delete |

Select the **Interface Configuration** tab and click on **Toggle State** to enable the interfaces.

Network Management: GSSCP\_V9

Devices: GSSCP\_V9

Network Configuration | Interface Configuration

| Name | Administrative Status |        |
|------|-----------------------|--------|
| A1   | Enabled               | Toggle |
| A2   | Disabled              | Toggle |
| B1   | Enabled               | Toggle |
| B2   | Disabled              | Toggle |

## 7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces. Testing was carried out with TLS used for transport of signalling between the Session Manager and the Avaya SBCE. This document shows the configuration for TLS, if another transport protocol is required, substitute it where TLS is specified.

### 7.3.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** (not shown) in the main menu on the left hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

- 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 internal signalling interface.
- For **Signaling IP**, select an **internal** signalling interface IP address defined in **Section 7.2**
- Select **TLS** port number, **5061** is used for the Session Manager.
- When the TLS port number is defined, an additional field (not shown) becomes available for **TLS Profile**, select the predefined Avaya profile **Avaya\_Server**.
- 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 an **external** signalling interface IP address defined in **Section 7.2**.
- Select **UDP** port number, **5060** is used for the Vodafone SIP Trunk.

Signaling Interface: GSSCP\_V9

Devices  
GSSCP\_V9

Signaling Interface

Add

| Name    | Signaling IP   | TCP Port | UDP Port | TLS Port | TLS Profile  | Edit | Delete |
|---------|----------------|----------|----------|----------|--------------|------|--------|
| Int_Sig | 10.10.9.71     | ---      | ---      | 5061     | Avaya_Server | Edit | Delete |
| Ext_Sig | 192.168.122.58 | ---      | 5060     | ---      | None         | Edit | Delete |

### 7.3.2. Media Interfaces

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

- Select **Add** and enter details of the internal media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select an **internal** media interface IP address defined in **Section 7.2**.
- Select **RTP port** ranges for the media path with the enterprise end-points.
- Select **Add** and enter details of the external media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **Media IP**, select an **external** media interface IP address defined in **Section 7.2**.
- Select **RTP port** ranges for the media path with Vodafone SIP Trunk.

Media Interface: GSSCP\_V9

Devices

GSSCP\_V9

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

| Name    | Media IP       | Port Range  | Edit | Delete |
|---------|----------------|-------------|------|--------|
| Int_Med | 10.10.9.71     | 2048 - 3329 | Edit | Delete |
| Ext_Med | 192.168.122.58 | 2048 - 3329 | Edit | Delete |

**Note:** During test the port ranges for the internal and external media interfaces were set to the default values used on Communication Manager.

## 7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, Vodafone SIP Trunk is connected as the Trunk Server and the Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the main menu on the left hand side. To define Server Interworking for the Session Manager, highlight the **avaya-ru** profile which is a factory setting appropriate for Avaya equipment and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown).

- In the **Clone Name** field enter a descriptive name for the Session Manager and click **Finish** – in test **ASM9** was used.
- In the **General** tab (not shown) Select **Edit** and enter details in the pop-up menu.
- Check the **T.38** box then click **Next** and **Finish** (not shown).

Alarms Incidents Statistics Logs Diagnostics Users

### Session Border Controller for Enterprise

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles Domain DoS Fingerprint **Server Interworking** Phone Interworking Media Forking Routing Server Configuration Topology Hiding Signaling Manipulation URI Groups

#### Interworking Profiles: ASM9

Add

Interworking Profiles

- cs2100
- avaya-ru
- OCS-Edge-Server
- cisco-ccm
- cups
- Sipera-Halo
- OCS-FrontEnd-Ser...
- ASM9**
- VFDE

General

Hold Support

- ☒ None
- ☐ RFC2543 - c=0.0.0.0
- ☐ RFC3264 - a=sendonly

180 Handling

- ☒ None
- ☐ SDP
- ☐ No SDP

181 Handling

- ☒ None
- ☐ SDP
- ☐ No SDP

182 Handling

- ☒ None
- ☐ SDP
- ☐ No SDP

183 Handling

- ☒ None
- ☐ SDP
- ☐ No SDP

Refer Handling

☐

3xx Handling

☐

Diversion Header Support

☐

Delayed SDP Handling

☐

T.38 Support

☒

URI Scheme

- ☒ SIP
- ☐ TEL
- ☐ ANY

Via Header Format

- ☒ RFC3261
- ☐ RFC2543

Next

- In the **Advanced** tab (not shown) Select **Edit** and enter details in the pop-up menu
- Uncheck the **AVAYA Extensions** box

| Editing Profile: ASM9                   |  |
|---|--|
| Record Routes                           | <input type="radio"/> None<br><input type="radio"/> Single Side<br><input checked="" type="radio"/> Both Sides |
| Topology Hiding: Change Call-ID         | <input type="checkbox"/>   |
| Call-Info NAT                           | <input type="checkbox"/>   |
| Change Max Forwards                     | <input type="checkbox"/>   |
| Include End Point IP for Context Lookup | <input type="checkbox"/>   |
| OCS Extensions                          | <input type="checkbox"/>   |
| AVAYA Extensions                        | <input type="checkbox"/>   |
| NORTEL Extensions                       | <input type="checkbox"/>   |
| Diversion Manipulation                  | <input type="checkbox"/>   |
| Diversion Header URI                    | <input type="text"/>   |
| Metaswitch Extensions                   | <input type="checkbox"/>   |
| Reset on Talk Spurt                     | <input type="checkbox"/>   |
| Reset SRTP Context on Session Refresh   | <input type="checkbox"/>   |
| Has Remote SBC                          | <input checked="" type="checkbox"/>  |

To define Server Interworking for Vodafone SIP Trunk, highlight the previously defined profile for the Session Manager and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown).

- In the **Clone Name** field enter a descriptive name for server interworking profile for Vodafone SIP Trunk and click **Finish** – in test **VFDE** was used.
- Select **Edit** and enter details in the pop-up menu.
- Check the **T.38** box.
- Select **Next** three times and **Finish**.

## 7.5. Define Servers

A server definition is required for each server connected to the Avaya SBCE. In this case, Vodafone SIP Trunk is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define the Session Manager, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** and enter details in the pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next** (not shown).
- In the **Server Type** drop down menu, select **Call Server**.
- In the **IP Addresses / Supported FQDNs** box, type the Session Manager SIP interface address which is the same as that defined for the Session Manager SIP Entity in Section 6.5.1.
- If TLS is to be used for the signalling transport between the Session Manager and the Avaya SBCE, check **TLS** in **Supported Transports**.
- Define the **TLS** port for SIP signalling, **5061** is used for the Session Manager and click **Finish**.

The screenshot displays the 'Edit Server Configuration Profile - General' window. On the left, a sidebar titled 'Server Configuration: ASM9\_Call\_Server' contains an 'Add' button and a list of server profiles: 'Server Profiles', 'ASM9\_Call\_Server' (highlighted), and 'SP\_Trunk\_Server'. The main area has two tabs: 'General' and 'Authentication'. The 'General' tab is active, showing the following configuration fields: 'Server Type' is a dropdown menu set to 'Call Server'; 'IP Addresses / Supported FQDNs' is a text box containing '10.10.79.61' with a note 'Separate entries with commas'; 'Supported Transports' includes three checkboxes: 'TCP' (unchecked), 'UDP' (unchecked), and 'TLS' (checked); 'TCP Port' is an empty text box; 'UDP Port' is an empty text box; 'TLS Port' is a text box containing '5061'. A 'Finish' button is located at the bottom right of the main panel.

- Select the **Advanced** tab (not shown).
- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for the Session Manager defined in **Section 7.4**.
- If TLS is to be used between the Session Manager and the Avaya SBCE, select the predefined Avaya TLS client in the **TLS Client Profile** drop down menu. The predefined TLS client on the Avaya SBC used in test was **Avaya\_RU**, on other systems this may be **AvayaSBCClient**.
- Click **Finish**.

**Edit Server Configuration Profile - Advanced**

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile ASM9

TLS Client Profile Avaya\_RU

Signaling Manipulation Script None

TLS Connection Type ☒ SUBID ☐ PORTID ☐ MAPPING

Finish

To define Vodafone SIP Trunk as a Trunk Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** and enter details in the pop-up menu.

- In the **Profile Name** field enter a descriptive name for Vodafone SIP Trunk and click **Next** (not shown).
- In the **Server Type** drop down menu, select **Trunk Server**.
- In the **IP Addresses / Supported FQDNs** box, type the IP address of Vodafone SIP Trunk.
- Check **UDP** in **Supported Transports**.
- Define the **UDP** port for SIP signaling, **5060** is used for Vodafone.
- Click **Finish**.

**Edit Server Configuration Profile - General**

Server Type Trunk Server

IP Addresses / Supported FQDNs  
Separate entries with commas  
192.168.52.8

Supported Transports ☐ TCP ☒ UDP ☐ TLS

TCP Port

UDP Port 5060

TLS Port

Finish

- Select the **Advanced** tab (not shown).
- Select the **Interworking Profile** for the Vodafone SIP Trunk defined in **Section 7.4** from the drop down menu.



## 7.6. Define Routing

Routing information is required for routing to the Session Manager on the internal side and Vodafone SIP Trunk 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 for TCP and UDP, and 5061 for TLS. To define routing to the Session Manager, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Session Manager, in this case **Call Server**, and click **Next**.
- Enter the Session Manager SIP interface address and port in the **Next Hop Server 1** field.
- Select **TLS** for the **Outgoing Transport**.
- Click **Finish**.

To define routing to Vodafone SIP Trunk, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for Vodafone SIP Trunk, in this case a generic name of **Trunk Server** was used, and click **Next**.



- Enter the Vodafone SIP Trunk IP address and port in the **Next Hop Server 1** field.
- Select **UDP** for the **Outgoing Transport**.
- Click **Finish**.

Edit Routing RuleX

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group

\*

Next Hop Server 1

IP, IP:Port, Domain, or Domain:Port

192.168.52.8

Next Hop Server 2

IP, IP:Port, Domain, or Domain:Port

Routing Priority based on

Next Hop Server

☒

Use Next Hop

for In Dialog Messages

☐

Ignore Route Header

for Messages Outside Dialog

☐

NAPTR

☐

SRV

☐

Outgoing Transport

☐ TLS ☐ TCP ☒ UDP

Finish

## 7.7. 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 for destination headers and local IP for source headers. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise, particularly from the Session Manager. 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 the Session Manager, navigate to **Global Profiles → Topology Hiding** in the main 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 the Session Manager and click **Next**.
- If the **Request-Line**, **Record-Route**, **Via** and **To** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu.
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**.
- If the **From** and **SDP** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu.
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten).
- For each of the headers leave the **Replace Action** at the default value of **Auto**.

Topology Hiding Profiles: ASM9

Topology Hiding Profiles

- default
- cisco\_th\_profile
- ASM9**
- VFDE

Click here to add a description.

**Topology Hiding**

| Header       | Criteria  | Replace Action | Overwrite Value |
|--------------|-----------|----------------|-----------------|
| Via          | IP/Domain | Auto           | ---             |
| Record-Route | IP/Domain | Auto           | ---             |
| From         | IP        | Auto           | ---             |
| Request-Line | IP/Domain | Auto           | ---             |
| SDP          | IP        | Auto           | ---             |
| To           | IP/Domain | Auto           | ---             |

**Note:** The use of **Auto** results in an IP address being inserted in the host portion of the header URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used where appropriate, and the required domain names entered in the **Overwrite Value** field. Different domain names can be used for the enterprise and Vodafone SIP Trunk.

To define Topology Hiding for Vodafone SIP Trunk, navigate to **Global Profiles → Topology Hiding** in the main 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 Vodafone SIP Trunk and click **Next**.
- If the **Request-Line**, **Record-Route**, **Via** and **To** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu.
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**.
- If the **From** and **SDP** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu.
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten).

Topology Hiding Profiles: VFDE

Add Rename Clone Delete

Topology Hiding Profiles

default

cisco\_th\_profile

ASM9

**VFDE**

Click here to add a description.

Topology Hiding

| Header       | Criteria  | Replace Action | Overwrite Value |
|--------------|-----------|----------------|-----------------|
| Via          | IP/Domain | Auto           | ---             |
| Record-Route | IP/Domain | Auto           | ---             |
| From         | IP        | Auto           | ---             |
| Request-Line | IP/Domain | Auto           | ---             |
| SDP          | IP        | Auto           | ---             |
| To           | IP/Domain | Auto           | ---             |

Edit

## 7.8. End Point Policy Groups

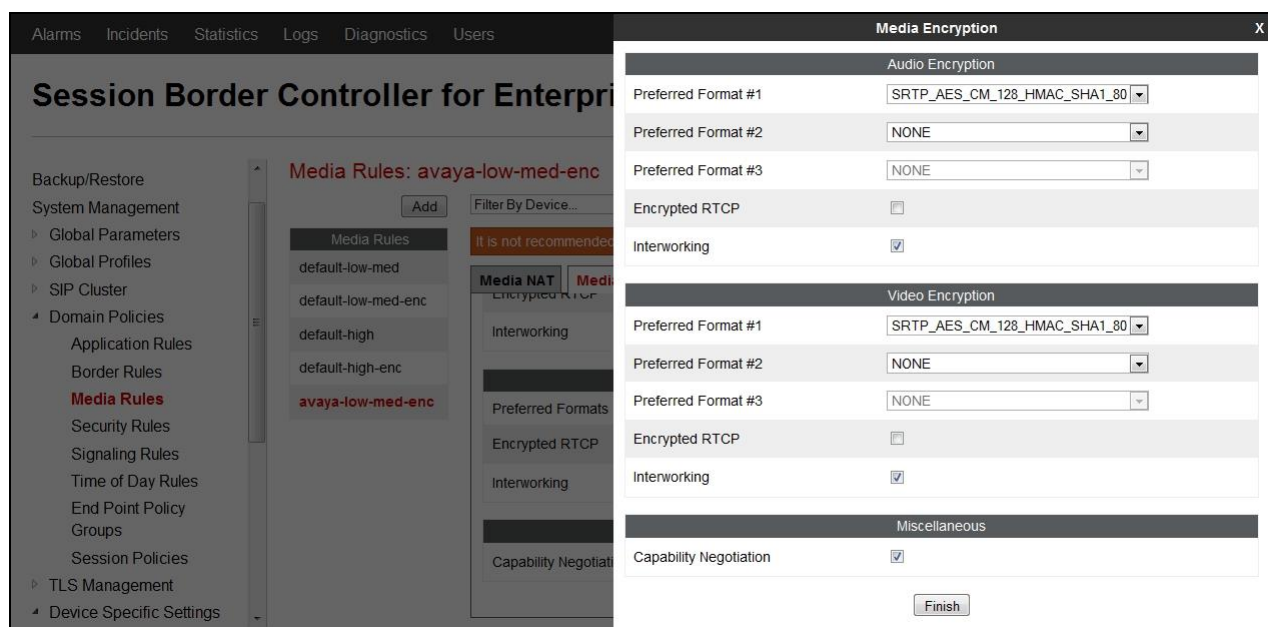
End Point Policy Groups are used to bring together a number of different rules for use in a server flow described in **Section 7.10**. The Vodafone SIP Trunk was tested with SRTP in the enterprise, and a Media Rule was required for conversion between SRTP and RTP.

### 7.8.1. Media Rules

Media rules are a mechanism on the Avaya SBCE to handle any unusual media handling scenarios that may be encountered for a particular Service Provider. In the case of Vodafone SIP Trunk, this was the conversion between SRTP used within the enterprise and RTP used on the SIP Trunk.

To define the media rule, navigate to **Domain Policies** → **Media Rules** in the main menu on the left hand side. Click on **Add** and enter details in the Media Rule pop-up box (not shown). In the **Rule Name** field enter a descriptive name for the Vodafone SIP Trunk media rule and click **Next** and **Next** again, then **Finish**

- Click on the **Media Encryption** tab (not shown) and then click on **Edit**.
- Select the **Preferred Format #1** from the drop down menu, in test **SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80** was used.
- Video is not currently offered as part of the solution, but if required select the preferred format for video.
- Ensure **Interworking** is checked so that the conversion to RTP can take place.
- Leave **Capability Negotiation** unchecked as it is not required in this solution.
- Click **Finish**.



**Note:** Existing media rule **avaya-low-med-enc** was used for testing. To verify an existing rule, click on the **Media Encryption** tab, then check that the settings are consistent with those described above.

## 7.8.2. End Point Policy Group

An End Point Policy Group is required to implement the media rule. To define one for use in the Session Manager server flow, navigate to **Domain Policies** → **End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

- In the **Group Name** field enter a descriptive name for the Session Manager Policy Group, in this case **avaya-def-low-enc**, and click **Next**.
- In the **Application Rule** field, select **default-trunk**.
- Leave the **Application Rule** and **Border Rule** at their default values.

- Select the **Media Rule** created in the previous section in the drop down menu.
- Leave the **Security Rule**, **Signalling Rule** and **Time of Day Rule** at their default values.

**Policy Groups: avaya-def-low-enc**

Add Filter By Device...

**Policy Groups**

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc**
- avaya-def-high-sub...

**Policy Group**

Order 1

**Edit Policy Set** X

Application Rule default-trunk

Border Rule default

Media Rule avaya-low-med-enc

Security Rule default-low

Signaling Rule default

Time of Day Rule default

Finish

**Note:** Existing end point policy group **avaya-def-low-enc** was used for testing. To verify an existing end point policy group, check that the settings are consistent with those described above.

## 7.9. Server Flows

Server Flows combine the previously defined profiles into two End Point Server Flows, one for the Session Manager and another for the Vodafone SIP Trunk. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to Vodafone SIP Trunk and vice versa.

To define a Server Flow for the Session Manager, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab (not shown).
- Select **Add Flow** and enter details in the pop-up menu (not shown).
- In the **Name** field (not shown) enter a descriptive name for the server flow for the Session Manager, in this case **ASM Call Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the Session Manager defined in **Section 7.5**.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**. This is the interface that media bound for the Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Vodafone SIP Trunk defined in **Section 7.7**.
- In the **End Point Policy Group** drop down menu, select the policy group defined in **Section 7.9**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.8** and click **Finish**.

| Edit Flow: Session Manager |                  |
|----------------------------|------------------|
| Flow Name                  | Session Manager  |
| Server Configuration       | ASM9_Call_Server |
| URI Group                  | *                |
| Transport                  | *                |
| Remote Subnet              | *                |
| Received Interface         | Ext_Sig          |
| Signaling Interface        | Int_Sig          |
| Media Interface            | Int_Med          |
| End Point Policy Group     | avaya-deflow-enc |
| Routing Profile            | Trunk Server     |
| Topology Hiding Profile    | ASM9             |
| File Transfer Profile      | None             |
| <button>Finish</button>    |                  |

To define a Server Flow for Vodafone SIP Trunk, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab (not shown).
- Select **Add Flow** and enter details in the pop-up menu (not shown).
- In the **Flow Name** field (not shown) enter a descriptive name for the server flow for Vodafone SIP Trunk, in this case a generic name of **Trunk Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the Trunk Server defined in **Section 7.5**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Vodafone SIP Trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Vodafone SIP Trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for Vodafone SIP Trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.7**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Vodafone SIP Trunk defined in **Section 7.8** and click **Finish**.

| Edit Flow: Trunk Server |                 |
|-------------------------|-----------------|
| Flow Name               | Trunk Server    |
| Server Configuration    | SP_Trunk_Server |
| URI Group               | *               |
| Transport               | *               |
| Remote Subnet           | *               |
| Received Interface      | Int_Sig         |
| Signaling Interface     | Ext_Sig         |
| Media Interface         | Ext_Med         |
| End Point Policy Group  | default-low     |
| Routing Profile         | Call Server     |
| Topology Hiding Profile | VFDE            |
| File Transfer Profile   | None            |
| <div>Finish</div>       |                 |



The information for all Server Flows is shown on a single screen on the Avaya SBCE.

**Session Border Controller for Enterprise**

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

System Management

- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- TLS Management
- Device Specific Settings
  - Network Management
  - Media Interface
  - Signaling Interface
  - Signaling Forking
  - End Point Flows**
  - Session Flows
  - Relay Services
  - SNMP
  - Syslog Management

**End Point Flows: GSSCP\_V9**

Devices

GSSCP\_V9

Subscriber Flows Server Flows

Hover over a row to see its description.

**Server Configuration: ASM9\_Call\_Server**

| Priority | Flow Name       | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile |                        |
|----------|-----------------|-----------|--------------------|---------------------|------------------------|-----------------|------------------------|
| 1        | Session Manager | *         | Ext_Sig            | Int_Sig             | avaya-def-low-enc      | Trunk Server    | View Clone Edit Delete |

**Server Configuration: SP\_Trunk\_Server**

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

## 8. Configure Vodafone Germany SIP Trunk Equipment

The configuration of the Vodafone equipment used to support Vodafone SIP Trunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on Vodafone equipment and system configuration please contact an authorized Vodafone representative.

## 9. Verification Steps

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

- 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**.

Home Routing Session Manager

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

**Session Manager Entity Link Connection Status**

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: VM79\_SM

Summary View

Status Details for the selected Session Manager:

| SIP Entity Name | SIP Entity Resolved IP | Port | Proto. | Deny  | Conn. Status | Reason Code | Link Status |
|-----------------|------------------------|------|--------|-------|--------------|-------------|-------------|
| Messaging       | 10.10.2.82             | 5061 | TLS    | FALSE | UP           | 200 OK      | UP          |
| ASBCE_50        | 10.10.9.75             | 5061 | TLS    | FALSE | UP           | 200 OK      | UP          |
| ASBCE_45        | 10.10.9.71             | 5061 | TLS    | FALSE | UP           | 200 OK      | UP          |
| VM79_CM         | 10.10.79.52            | 5061 | TLS    | FALSE | UP           | 200 OK      | UP          |



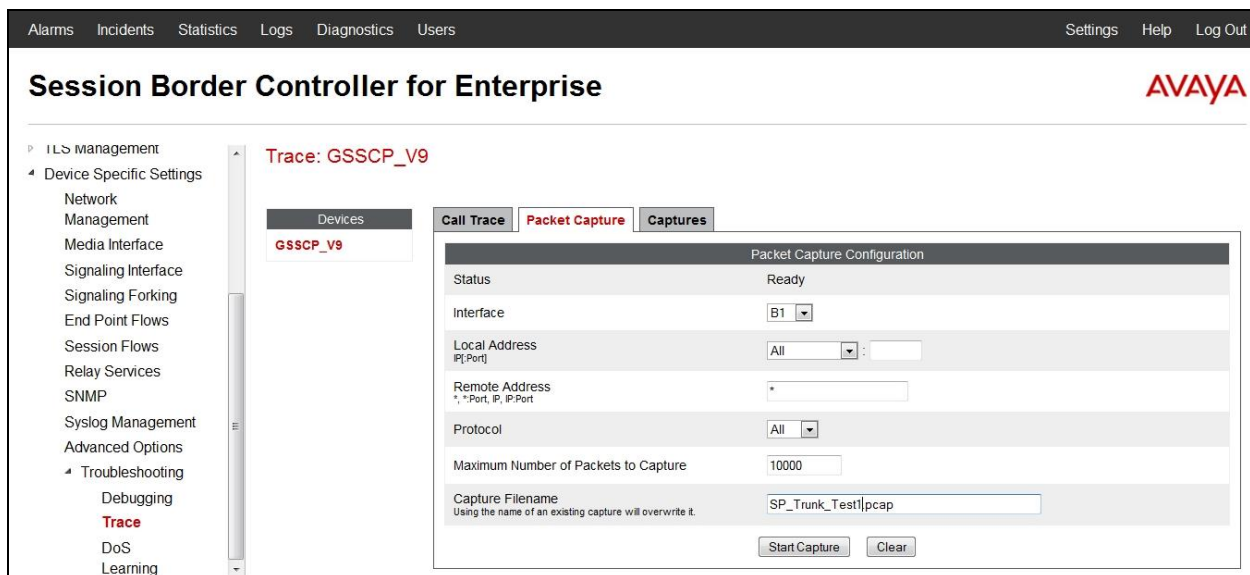
- From the Communication Manager SAT interface run the command **status trunk n** where **n** is a previously configured SIP trunk. Observe if all channels on the trunk group display **in-service/idle**.

| status trunk 1     |        |                 |                              |
|--------------------|--------|-----------------|------------------------------|
| TRUNK GROUP STATUS |        |                 |                              |
| Member             | Port   | Service State   | Mtce Connected Ports<br>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                           |

- Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
- Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.
- Should issues arise with the SIP trunk, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from the 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 the signalling interface IP address or **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**.



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 Vodafone network.

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to Vodafone Germany SIP Trunk Service. Vodafone SIP Trunk 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**. Testing was carried out on Avaya SBC build 6.2.0.Q48. Because of issues observed with SRTP handling during testing with another Service provider, it is recommended to use the latest GA build. At the time of writing, this was 6.2.1 Q7 (FP1)

## 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] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3, May 2013.
- [2] *Administering Avaya Aura® System Platform*, Release 6.3, May 2013.
- [3] *Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*, May 2013
- [4] *Avaya Aura® Communication Manager 6.3 Documentation library*, August 2013.
- [5] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 May 2013
- [6] *Implementing Avaya Aura® System Manager* Release 6.3, May 2013
- [7] *Upgrading Avaya Aura® System Manager to 6.3.2*, May 2013.
- [8] *Administering Avaya Aura® System Manager* Release 6.3, May 2013
- [9] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 May 2013
- [10] *Implementing Avaya Aura® Session Manager* Release 6.3, May 2013
- [11] *Upgrading Avaya Aura® Session Manager* Release 6.3, May 2013
- [12] *Administering Avaya Aura® Session Manager* Release 6.3, June 2013,
- [13] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2 June 2013
- [14] *Upgrading Avaya Session Border Controller for Enterprise* Release 6.2 July 2013
- [15] *Administering Avaya Session Border Controller for Enterprise* Release 6.2 March 2013
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

---

**©2014 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](mailto:devconnect@avaya.com).