



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R7.0.1, Avaya Aura® Session Manager R7.0.1 and Avaya Session Border Controller for Enterprise R7.1 to support M-net Premium SIP-Trunk - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the M-net Premium SIP-Trunk 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.

The M-net Premium SIP-Trunk provides PSTN access via a SIP Trunk connected to the M-net Voice over Internet Protocol (VoIP) network as an alternative to legacy analogue or digital trunks.

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

M-net 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 M-net Premium SIP-Trunk (SIP Trunk) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura® Communication Manager R7.0.1; Avaya Aura® Session Manager R7.0.1; Avaya Session Border Controller for Enterprise R7.1; Endpoints as described in **Section 3**. Note that the shortened names Communication Manager, Session Manager and Avaya SBCE will be used throughout the remainder of the document. Customers using this Avaya SIP-enabled enterprise solution with the M-net Premium 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 connect to the M-net SIP Trunk.

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 M-net SIP Trunk, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via M-net SIP Trunk to PSTN destinations, calls made from SIP and H.323 telephones.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator and Avaya Equinox for Windows soft phones.
- Calls using the G.711A Law and G.729A codec's.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using G.711.
- 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 between the Avaya SBCE and the SIP and H.323 telephones.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by the M-net SIP Trunk requiring Avaya response and sent by Avaya requiring M-net response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the M-net SIP Trunk with the following observations:

- The user part of the Contact header URI coming from the network is a string of characters rather than a diallable PSTN number. The Session Manager copies this string of characters into the P-Asserted-Identity header which is sent to the Communication Manager. This is then displayed on H.323 extensions as the “Answered By” number. To display a meaningful number rather than the string of characters, an Adaptation was used on the Session Manager that causes it to take the user part of the From header URI for the P-Asserted-Identity rather than the Contact header. The Adaptation is described in **Section 6.4**.
- When making an inbound call to an unassigned enterprise extension, the call took 90 seconds to fail. There were numerous attempts to establish the call before a failure tone was played to the calling party.
- When testing codec negotiation on an outbound international call from an analogue extension, it was observed that even though payload type 100 was specified, telephone events were not received from the network for DTMF. The call was successful for outbound calls to a national destination.
- When making an inbound call with no matching codec, the enterprise sends “488 Not Acceptable Here”. During testing, the network did not fail the call when it received this response and continued to send INVITE messages in an attempt to establish the call.
- Throughout the testing there were issues related to delays in signalling between the enterprise and the network. One of the tests where this was particularly apparent was long duration call hold. The network was sending a re-INVITE for session refresh approximately every 5 minutes. In some cases, the network did not receive the 200 OK within half a second and sent another re-INVITE. If this was received by the enterprise after it had sent a 200 OK, the call failed. To work around this issue, the SIP timer was changed on the Avaya SBCE to one second. In addition, the session refresh was set to 280 seconds on Communication Manager, as described in **Section 5.6**, so that there was signalling activity before the re-INVITE was received from the network.
- It was observed that when testing blind call transfer, the network responded to SIP REFER with a NOTIFY message that contained “403 Forbidden”. As it was not supported in this case, network redirect was turned off on Communication Manager preventing the sending of SIP REFER. In addition, Communication Manager was configured to use re-INVITE as opposed to UPDATE which appeared to be causing poor quality media after blind call transfer.
- Originating calls from EC500 mobile phones were not identified as belonging to a Communication Manager extension as they did not match the EC500 Phone Number described in **Section 5.10**. The Session Manager was populating the P-Asserted-Identity header with the user part of the Contact header URI coming from M-net. To resolve this, an Adaptation was used on the Session Manager as described in the first observation on the called party number displayed on H.323 extensions.

- As mentioned previously, there were issues related to delays in signalling between the enterprise and the network for the duration of the testing. One consequence of this was that the EC500 idle appearance FNE did not work when the 200 OK answer message was sent immediately by Communication Manager, but the network did not received it within 500ms of sending the initial INVITE and sent a duplicate. To work around this, a vector was used to introduce a short delay before the 200 OK answer message was sent.
- Test calls to an extension with EC500 that were answered by the EC500 mobile with confirmed answer enabled were not successful. Pressing a button on the phone did not answer the call. This feature is not critical for SIP compliance.
- Some tests were carried out with initial IP-IP direct media disabled while diagnosing call failures. With this disabled, the call is set up first with a media path between the endpoint and the media gateway, then the call is "Shuffled" so that a direct media path is established between the endpoint and the internal interface of the Avaya SBCE. Shuffling was used initially with Consultative transfer to internal extension by Avaya one-X® Communicator. Initial IP-IP direct media was re-enabled once network issues had been diagnosed.
- When making inbound calls to one-X Communicator in "Other Phone" mode and either transferring or conferencing the call, no ringback was heard on the "Other Phone". When making the call with initial IP-IP direct media disabled (see previous issue), ringback was heard. This was considered to be an issue in the test environment and not a SIP interoperability issue.
- Long duration calls were failing for the same reason described in the observations of long duration call hold. Changing the "Preferred Minimum Session Refresh Interval (sec)" to 280 on Communication Manager worked around this issue.

Items not tested include the following:

- No Inbound Toll-Free access was available for testing
- No test call was made to Emergency Services as a test call was not booked with the Emergency Services Operator.
- T.38 Fax was not tested as it is not supported by M-net. G.711 fax was tested successfully.

2.3. Support

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

For technical support on the M-net Premium SIP Trunk Service, please contact M-net at www.m-net.de.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the M-net SIP Trunk. Located at the enterprise site is an Avaya SBCE, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series IP telephones (with SIP and H.323 firmware), Avaya 1600 series IP telephone (with H.323 firmware), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Avaya Equinox for Windows running on laptop PCs.

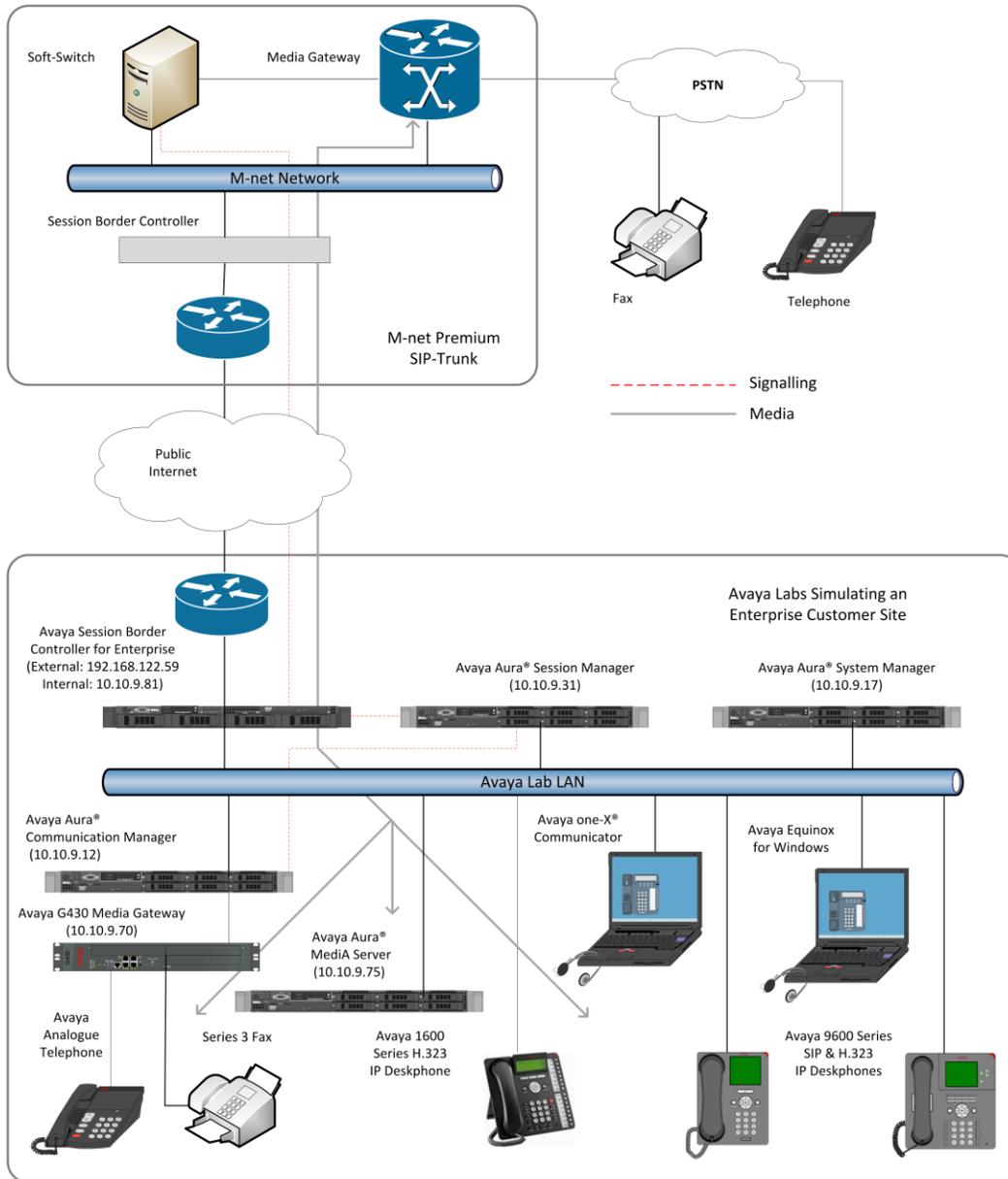


Figure 1: Test Setup M-net Premium SIP Trunk to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Session Manager	7.0.1.2.701230
Avaya Aura® System Manager	7.0.1.2.086224 – SP2
Avaya Aura® Communication Manager	7.0.1.2.0 0-23523 – FP1 SP2
Avaya Session Border Controller for Enterprise	7.1.0.2-01-13249 – SP2
Media Server	7.8.0.268
Avaya G430 Media Gateway	37.41.0
Avaya IP Handsets:	
SIP 96x0	2.6.10
SIP 9608	7.0.1.4 r6
H.323 96x0	3.2.7B
H.323 9608	6.6.4.01
H.323 1616	1.3.10
Avaya One-X Communicator	6.2.12.04 – SP12
Avaya Equinox for Windows	3.0.2.11
Avaya 2400 Series Digital Handsets	N/A
Analogue Handset	N/A
Analogue Fax	N/A
M-net	
Metaswitch Perimeta SBC and IPX (Class 4 Switch/Routing and SBC)	4.0.40
Metaswitch CFS (Class 5 Switch)	9.2

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 M-net Premium SIP-Trunk. For incoming calls, Session Manager receives SIP messages from the Avaya SBCE and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the M-net 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 M-net SIP Trunk and any other SIP trunks used.

<code>display system-parameters customer-options</code>		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
	Maximum Administered H.323 Trunks:	4000	0
	Maximum Concurrently Registered IP Stations:	2400	3
	Maximum Administered Remote Office Trunks:	4000	0
	Maximum Concurrently Registered Remote Office Stations:	2400	0
	Maximum Concurrently Registered IP eCons:	68	0
	Max Concur Registered Unauthenticated H.323 Stations:	100	0
	Maximum Video Capable Stations:	2400	0
	Maximum Video Capable IP Softphones:	2400	0
	Maximum Administered SIP Trunks:	4000	20
	Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0
	Maximum Number of DS1 Boards with Echo Cancellation:	80	0

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

```

display system-parameters customer-options                               Page 5 of 12
                                OPTIONAL FEATURES

Emergency Access to Attendant? y                                     IP Stations? y
  Enable 'dadmin' Login? y
  Enhanced Conferencing? y                                           ISDN Feature Plus? n
    Enhanced EC500? y                                               ISDN/SIP Network Call Redirection? y
Enterprise Survivable Server? n                                       ISDN-BRI Trunks? y
  Enterprise Wide Licensing? n                                       ISDN-PRI? y
    ESS Administration? y                                           Local Survivable Processor? n
  Extended Cvg/Fwd Admin? y                                         Malicious Call Trace? y
  External Device Alarm Admin? y                                     Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n                                   Mode Code for Centralized Voice Mail? n
    Flexible Billing? n
  Forced Entry of Account Codes? y                                   Multifrequency Signaling? y
  Global Call Classification? y                                       Multimedia Call Handling (Basic)? y
    Hospitality (Basic)? y                                           Multimedia Call Handling (Enhanced)? y
  Hospitality (G3V3 Enhancements)? y                               Multimedia IP SIP Trunking? y
    IP Trunks? y

IP Attendant Consoles? y
  
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for Session Manager using the **change node-names ip** command. In this case, **Session_Manager** and **10.10.9.31** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** IP address as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

```

change node-names ip                                               IP NODE NAMES

  Name          IP Address
AMS             10.10.9.75
Session_Manager  10.10.9.31
default        0.0.0.0
procr          10.10.9.12
procr6         ::
  
```

5.3. Administer IP Network Region

Use the **change ip-network-region n** command where **n** is the chosen value of the configuration for the SIP Trunk. 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 direct media is used on a PSTN call, 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 **2** is used.
- The rest of the fields can be left at default values.

```
change ip-network-region 2                                     Page 1 of 20
                                                              IP NETWORK REGION
Region: 2
Location:      Authoritative Domain: avaya.com
Name: Trunk    Stub Network Region: n
MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes
                Inter-region IP-IP Direct Audio: yes
                IP Audio Hairpinning? n
Codec Set: 2
UDP Port Min: 2048
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
H.323 IP ENDPOINTS      AUDIO RESOURCE RESERVATION PARAMETERS
                        RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

Note: In the test configuration, ip-network-region 1 was used within the enterprise and ip-network-region 2 was used for the SIP Trunk.

5.4. Administer IP Codec Set

Use the **change ip-codec set n** command where **n** is the codec set specified in the IP Network Region form in **Section 5.3**. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codec preferred by M-net was configured, namely **G.711A** and **G.729A**.

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

IP CODEC SET

Codec Set: 2

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711A	n	2	20
2: G.729A	n	2	20

Navigate to **Page 2** to define the transmission method for fax. M-net do not support T.38 so this was set to **off**. This setting allows transmission of fax using G.711.

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

IP CODEC SET

Allow Direct-IP Multimedia? n

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

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the M-net SIP Trunk. During test, this was configured to use TCP and port 5060. Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set **Group Type** to **sip**.
- Set **Transport Method** to required protocol. Although TLS is recommended for security, **tcp** was used during testing.
- Set **Peer Detection Enabled** to **y** allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Far-end Node Name** to Session Manager interface (node name **Session_Manager** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** as required, during testing, **5060** was used. These must correspond to those used on the Session Manager Entity Links (See **Section 6.6**).
- 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 region **2**).
- Leave **Far-end Domain** blank (allows Communication Manager to accept calls from any SIP domain on the associated trunk).
- Set **DTMF over IP** to **rtp--payload** which uses telephone events according to RFC 2833 for DTMF transmission.
- Set **Direct IP-IP Audio Connections** to **y** to avoid unnecessary use of resources
- Set **Initial IP-IP Direct Media** and **H.323 Station Outgoing Direct Media** to **y**. This initiates direct media when the call is set up without the need for shuffling.

```
add signaling-group 2                               Page 1 of 2
                                                    SIGNALING GROUP
Group Number: 2                                   Group Type: sip
IMS Enabled? n                                   Transport Method: tcp
Q-SIP? n
IP Video? n                                     Enforce SIPS URI for SRTP? 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
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr                         Far-end Node Name: Session_Manager
Near-end Listen Port: 5060                       Far-end Listen Port: 5060
                                                    Far-end Network Region: 2
Far-end Domain:
                                                    Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate             RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload                       Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3              IP Audio Hairpinning? n
Enable Layer 3 Test? n                          Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? y         Alternate Route Timer(sec): 6
```

5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group n** command, where **n** is an available trunk group for the SIP Trunk. 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** if the Diversion header is to be supported.
- 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 2                                     Page 1 of 21
                                                    TRUNK GROUP
Group Number: 2                                     Group Type: sip          CDR Reports: y
  Group Name: SIP_Trunk                            COR: 1                  TN: 1          TAC: 102
  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: 2
                                                    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 M-net to prevent unnecessary SIP messages during call setup. During testing, a value of **280** was used that sets the SIP Min-SE header to 560. With this setting, re-INVITE messages for Session Refresh were sent every 280 seconds which was slightly less than the interval at which Session Refresh messages were received from the network. This worked around the problems with long duration hold and long duration calls described in **Section 2.2**.

```
add trunk-group 2                                     Page 2 of 21
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                                    Redirect On OPTIM Failure: 5000
  SCCAN? n                                         Digital Loss Group: 18
                                                    Preferred Minimum Session Refresh Interval(sec): 280
Disconnect Supervision - In? y Out? y
```

On **Page 3**, set the **Numbering Format** field to **public** as M-net use E.164 numbering with preceding “+” in the SIP messages.

```

change trunk-group 2                                     Page 3 of 21
TRUNK FEATURES
    ACA Assignment? n                               Measured: none
                                                    Maintenance Tests? y

    Suppress # Outpulsing? n  Numbering Format: public
                                                    UUI Treatment: service-provider
                                                    Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n
                                                    Hold/Unhold Notifications? y
    Modify Tandem Calling Number: no
  
```

On **Page 4** of this form:

- Set **Network Call Redirection** to **n** as SIP “302 Moved Temporarily” and REFER are not supported by M-net.
- Set **Send Diversion Header** to **y** so that the DDI number assigned to the extension is passed for forwarded calls.
- Set **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **100** to match the value preferred by M-net (this Payload Type is not applied to calls from SIP end-points).
- During testing, **Always Use re-INVITE for Display Updates** was set to **y** as a timing issue was observed with UPDATE messages. This is unlikely to be an issue in the live network and a setting of **n** could be used.
- Set **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on Communication Manager extension.

```

change trunk-group 2                                     Page 4 of 21
                                                    PROTOCOL VARIATIONS
    Mark Users as Phone? n
    Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
    Send Transferring Party Information? n
    Network Call Redirection? n
    Send Diversion Header? y
    Support Request History? n
    Telephone Event Payload Type: 100

    Convert 180 to 183 for Early Media? n
    Always Use re-INVITE for Display Updates? y
    Identity for Calling Party Display: From
    Block Sending Calling Party Location in INVITE? n
    Accept Redirect to Blank User Destination? n
    Enable Q-SIP? n
  
```

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number E.164 format. Communication Manager automatically prefixes a “+” to the numbers when this table is used. These calling party numbers are sent in the SIP From, Contact and PAI headers. The numbers are displayed on display-equipped PSTN telephones with any reformatting performed in the network.

change public-unknown-numbering 0					Page 1 of 2	
NUMBERING - PUBLIC/UNKNOWN FORMAT						
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len		
4	2	1		4	Total Administered: 10	
4	600	2	49895527nnnn9	13	Maximum Entries: 240	
4	2000	2	49895527nnnn0	13	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.	
4	2001	2	49895527nnnn8	13		
4	2291	2	49895527nnnn2	13		
4	2316	2	49895527nnnn3	13		
4	2391	2	49895527nnnn1	13		
4	2400	2	49895527nnnn4	13		
4	2401	2	49895527nnnn7	13		
4	7001	2	49895527nnnn5	13		
						Communication Manager automatically inserts a '+' digit in this case.

Note: During testing the extension numbers were reformatted to national numbers for Trunk Group 2 only. The numbers were analysed for Trunk Group 1 but not reformatted.

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the M-net network. 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: 8		
Auto Route Selection (ARS) - Access Code 1: 9 Access Code 2:		

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls with leading **0**. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. The example shows international numbers with country code **353** for Ireland and area code **91** for Galway. Calls are sent to **Route Pattern 2**.

```
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 Reqd
0	8	12	2	pubu		n
00	13	15	2	pubu		n
0035391	13	13	2	pubu		n
1	3	4	2	pubu		n
118	5	6	2	pubu		n

Use the **change route-pattern n** command, where **n** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **2** is used to route calls to trunk group **2**. **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 2
```

Page 1 of 3

Pattern Number: 2 Pattern Name: SIP_Endpoints

SCCAN? n Secure SIP? n Used for SIP stations? n

Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits	DCS/ QSIG	IXC
1: 2	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	Sub	Numbering	LAR
	0	1	2	M	4	W	Request		Dgts	Format	
1:	y	y	y	y	y	n	n			unk-unk	none
2:	y	y	y	y	y	n	n				none
3:	y	y	y	y	y	n	n				none
4:	y	y	y	y	y	n	n				none
5:	y	y	y	y	y	n	n				none
6:	y	y	y	y	y	n	n				none

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to Communication Manager extensions. The incoming digits sent in the INVITE message from M-net can be manipulated as necessary to route calls to the desired extension. Use the **change inc-call-handling-trmt trunk-group x** command where **x** is the Trunk Group defined in **Section 5.6**. In the example shown, 13 digits numbers are received in E.164 format with a “+” prefix used in SIP to indicate an international number. The preceding “+” and all digits are deleted and the extension number is inserted. Note that some of the DDI digits have been obscured.

```
change inc-call-handling-trmt trunk-group 2                               Page 1 of 3
```

INCOMING CALL HANDLING TREATMENT				
Service/ Feature	Number Len	Number Digits	Del	Insert
public-ntwrk	14	+49895527nnnn0	14	2000
public-ntwrk	14	+49895527nnnn1	14	2391
public-ntwrk	14	+49895527nnnn2	14	2291
public-ntwrk	14	+49895527nnnn3	14	2316
public-ntwrk	14	+49895527nnnn4	14	2400
public-ntwrk	14	+49895527nnnn5	14	6005
public-ntwrk	14	+49895527nnnn6	14	6001
public-ntwrk	14	+49895527nnnn7	14	2401
public-ntwrk	14	+49895527nnnn8	14	2001
public-ntwrk	14	+49895527nnnn9	14	6002
public-ntwrk				

5.10. EC500 Configuration

When EC500 is enabled on a 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 2291. Use the command **change off-pbx-telephone station-mapping x** where **x** is a 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, none was required during testing.
- For the **Phone Number** enter the phone that will also be called (e.g. **00353914nnnn3**).
- Set the **Trunk Selection** to **ars** so that the ARS table will be used for routing.
- Set the **Config Set** to **1**.

```
change off-pbx-telephone station-mapping 2291                          Page 1 of 3
```

STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
2291	OPS	-		2291	aar	1	
2291	EC500	-		00353914nnnn3	ars	1	

Note: The phone number shown is for a test phone in the Avaya Lab. To use facilities such as Feature Name Extension (FNE) for calls coming in from EC500 mobile phones, the calling party number received by Communication Manager in the P-Asserted-Identity header must exactly match the number specified in the above table. In the solution tested, the P-Asserted-Identity header is inserted by the Session Manager using the information in the Contact header. This did not function initially as the Contact header from M-net does not contain the calling party number, see **Section 2.2** for details. This was resolved using an Adaptation in the Session Manager as described in **Section 6.4**.

Save Communication Manager configuration by entering **save translation**.

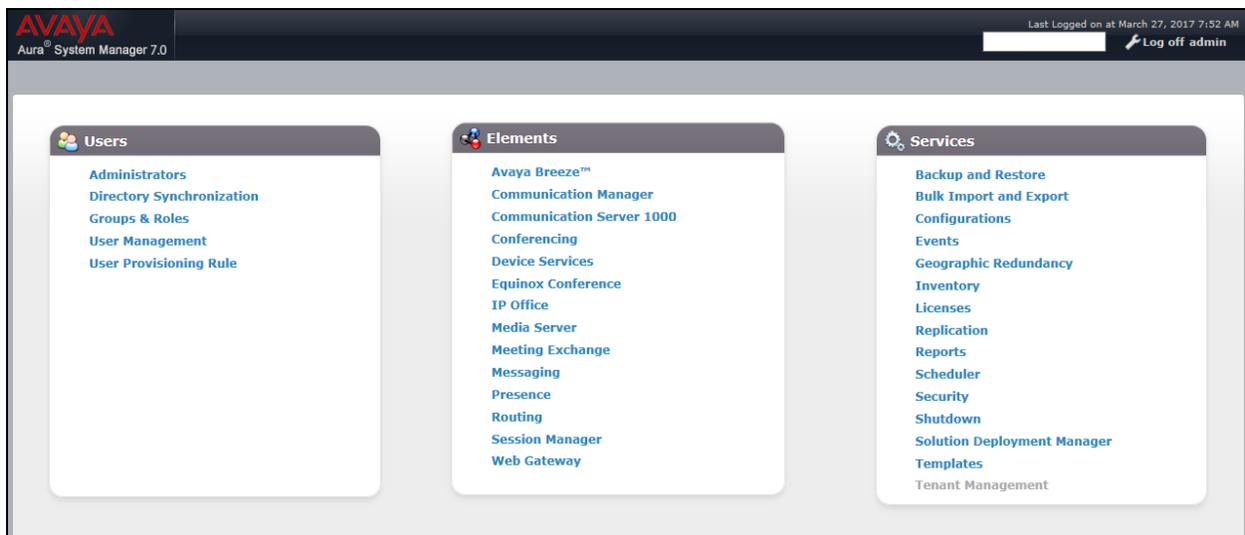
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured by opening a web browser to 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

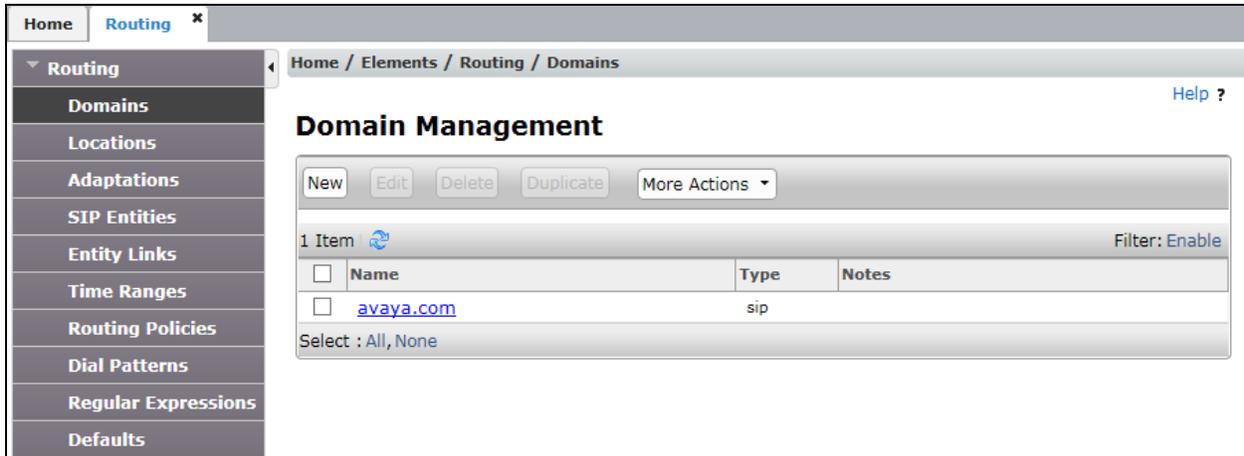
6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a web browser and 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** screen 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 **Elements, Home** screen menu and in the resulting tab select **Domains** from the 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 M-net; 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. Click **Commit** to save changes.



The screenshot shows the 'Domain Management' interface. The breadcrumb trail is 'Home / Elements / Routing / Domains'. The left-hand navigation menu includes 'Routing', 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The 'Domains' menu item is selected. The main content area displays 'Domain Management' with a table containing one entry: 'avaya.com' with type 'sip'. Action buttons like 'New', 'Edit', 'Delete', and 'Duplicate' are visible at the top.

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 (see **Section 6.4**).

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 and Session Manager routing. One location is added to the sample configuration for all of the enterprise SIP entities and another for the M-net SIP Trunk. On the **Routing** tab select **Locations** from the left hand menu (not shown). Under **General**, in the **Name** field, enter an informative name for the location. Define bandwidth requirements, during testing these were left at default values.

Home / Elements / Routing / Locations

Location Details

General

* Name:

Notes:

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:

Alarm Threshold

Overall Alarm Threshold: %

Multimedia Alarm Threshold: %

* Latency before Overall Alarm Trigger: Minutes

* Latency before Multimedia Alarm Trigger: Minutes

The location pattern is a way of using subnets to further refine the location information, this may be useful for endpoints that could be logged in from different subnets. This was not used during testing. If required, 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.

The screenshot shows a web interface titled "Location Pattern". At the top, there are "Add" and "Remove" buttons. Below them, it says "0 Items" with a refresh icon and a "Filter: Enable" option. A table is displayed with the following structure:

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>		

At the bottom right, there are "Commit" and "Cancel" buttons.

Although routing based on location was not used on Session Manager during testing, a separate location was defined for the M-net SIP Trunk called Service_Provider. The bandwidth parameters were left at default values and are not shown here.

The screenshot shows a web interface titled "Location". On the left is a sidebar menu with the following items: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, and Regular Expressions. The main content area has a breadcrumb "Home / Elements / Routing / Locations" and a "Help ?" link. Below the breadcrumb, there are "New", "Edit", "Delete", "Duplicate", and "More Actions" buttons. It says "2 Items" with a refresh icon and a "Filter: Enable" option. A table is displayed with the following structure:

<input type="checkbox"/>	Name	Correlation	Notes
<input type="checkbox"/>	Galway Lab	<input type="checkbox"/>	
<input type="checkbox"/>	Service Provider	<input type="checkbox"/>	

At the bottom of the table, it says "Select : All, None".

6.4. Administer Adaptations

Session Manager Adaptations can be used to alter parameters in the SIP message headers, during compliance testing, two were used. One Adaptation was used on the Communication Manager SIP Entity to convert the Calling Party Numbers sent from Session Manager to diallable formats for display on Communication Manager extensions. The other was used on the Avaya SBCE SIP Entity to remove Avaya proprietary headers from messages sent from Session Manager. This Adaptation also used the From header to create the P-Asserted-Identity header as opposed to the default behavior of using the Contact header (See **Section 2.2**).

6.4.1. Communication Manager

Calling Party Numbers were received from the network in E.164 format with leading "+", so the Adaption was used to convert to national numbers with a single zero and international numbers with two zeros.

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. During testing **Diallable** was used.
- In the **Module Name** drop down menu, select **DigitConversionAdapter**. This is used for simple digit conversion adaptations.
- In the **Module Parameter Type** drop down menu, select **Name-Value Parameter**.
- In the **Name** field, type **fromto**.
- In the **Value** field, type **true**.
- Scroll down and in the section **Digit Conversion for Outgoing Calls from SM**, click on **Add**. An additional row will appear (not shown) for digit manipulation.

Home / Elements / Routing / Adaptations Help ?

Adaptation Details

General

* **Adaptation Name:**

* **Module Name:**

Module Parameter Type:

Add		Remove	
<input type="checkbox"/>	Name		Value
<input type="checkbox"/>	fromto		true

Select : All, None

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
--------------------------	------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

Digit Conversion for Outgoing Calls from SM

Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
<input type="checkbox"/>	*+	*12	*15		*1	00	origination	
<input type="checkbox"/>	*+49	*12	*15		*3	0	origination	

Select : All, None

The screenshot shows how the calling party numbers in messages going to Communication Manager were analysed for testing. Digits were deleted and inserted so that calling party numbers beginning with “+49” were prefixed with 0 for national numbers and numbers beginning with “+” and any other country code were prefixed with 00 for international numbers.

6.4.2. Avaya SBCE

Communication Manager and Session Manager make use of Avaya proprietary SIP headers to facilitate the full suite of Avaya functionality within the enterprise. These are not required on the SIP trunk however, and make the SIP messages unnecessarily large. A Session Manager Adaptation is used to remove proprietary headers. 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** drop down menu, select **OrangeAdapter**.
- In the **Module Parameter Type** drop down menu, select **Name-Value Parameter**.
- In the **Name** box, type **eRHdrs**
- In the **Value** box, type the list of headers to be deleted. During testing, the following list was used: **"P-AV-Message-Id, P-Charging-Vector, Av-Global-Session-ID, P-Location, Endpoint-View, P-Conference, Alert-Info"**.
- Scroll down and in the section **Digit Conversion for Outgoing Calls from SM**, click on **Add**. An additional row will appear (not shown) for digit manipulation.

Home / Elements / Routing / Adaptations Help ?

Adaptation Details

Commit Cancel

General

* Adaptation Name:

* Module Name:

Module Parameter Type:

Add Remove	
<input type="checkbox"/> Name	Value
<input type="checkbox"/> eRHdrs	"P-AV-Message-Id, P-Charging-Vector, Av-Global-Session-ID, P-Location, Endpoint-View, P-Conference, Alert-Info"
<input type="checkbox"/> fromto	true

Select : All, None

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*0	*10	*15		*1	+49	destination		
<input type="checkbox"/>	*00	*12	*17		*2	+	destination		

Select : All, None

Commit Cancel

The screenshot shows how the called party numbers in messages going to the Avaya SBCE were analysed for testing. Digits were deleted and inserted so that dialled numbers beginning with “0” were prefixed with “+49” for national numbers and numbers beginning with “00” were prefixed with “+” for international numbers.

The **OrangeAdapter** module includes **DigitConversionAdpater** for simple digit conversion and provides the additional functionality of changing the way the P-Asserted-Identity header is populated where it is not received from the Service Provider. The default action is to use information in the Contact header. This module uses the From header instead which resolves issues with the number displayed on H.323 extensions and calls from EC500 mobiles as described in **Section 2.2**. The full functionality of the OrangeAdapter module is described in the Session Manager Administration Guide referenced in **Section 11**.

6.5. Administer SIP Entities

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

Under **General**:

- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP Entity, **CM** for a Communication Manager SIP Entity and **SIP Trunk** for the Avaya SBCE SIP Entity.
- In the **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 four SIP Entities:

- Avaya Aura® Session Manager SIP Entity.
- Avaya Aura® Communication Manager SIP Entity for the SIP Endpoints.
- Avaya Aura® Communication Manager SIP Entity for the SIP Trunk.
- Avaya Session Border Controller for Enterprise (Avaya SBCE) SIP Entity for PSTN destinations.

There is also a SIP Entity for Avaya Aura® Messaging but that is not described in this document.

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.

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

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 **Listen Ports**, click **Add**, then edit the fields in the resulting new row.

- In the **Listen Ports** 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.
- Click on **Commit** (not shown).

Listen Ports

TCP Failover port:

TLS Failover port:

Add Remove

3 Items Filter: Enable

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	TCP	avaya.com	<input checked="" type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	UDP	avaya.com	<input checked="" type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	TLS	avaya.com	<input checked="" type="checkbox"/>	<input type="text"/>

Select : All, None

6.5.2. Avaya Aura® Communication Manager SIP Entities

The following screen shows one of the SIP entities for Communication Manager which is configured as an Evolution Server. This SIP Entity is used for the SIP Trunk. 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** and set the **Location** to that defined in **Section 6.3**.

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:

Securable:

Call Detail Recording: ▼

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

Loop Detection

Loop Detection Mode: ▼

Loop Count Threshold:

Loop Detection Interval (in msec):

SIP Link Monitoring

SIP Link Monitoring: ▼

Supports Call Admission Control:

Shared Bandwidth Manager:

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Note: The Adaptation assigned is that defined in **Section 6.4.1**. Note also that a second SIP Entity for Communication Manager is defined for SIP Endpoints. In the test environment this is named “CM_SIP_Endpoints”. The parameters are the same apart from the Adaptation, and the two are assigned to different Entity Links, as described in **Section 6.6**, so that different ports can be used. It is these different ports that distinguish between traffic for SIP Endpoints and traffic for the SIP Trunk.

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The screenshot shows the SIP Entity for the Avaya SBCE used for PSTN destinations. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface used for PSTN fixed calls (see **Figure 1**). Set the **Adaptation** to that defined in **Section 6.4.2**, the **Location** to that defined in **Section 6.3** for the SIP Trunk, and the **Time Zone** to the appropriate time zone.

The screenshot displays the 'SIP Entity Details' configuration page. At the top right, there are 'Commit' and 'Cancel' buttons. The page is titled 'SIP Entity Details' and has a 'General' tab selected. The configuration fields are as follows:

- Name:** ASBCE
- FQDN or IP Address:** 10.10.9.81
- Type:** SIP Trunk (dropdown menu)
- Notes:** (empty text field)
- Adaptation:** Header_Removal (dropdown menu)
- Location:** Service_Provider (dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Securable:**
- Call Detail Recording:** egress (dropdown menu)

Note: The **Location** selected would allow routing based on origination if required. This is used in Dial Patterns as described in **Section 6.8**. It was not required during testing.

6.6. Administer Entity Links

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

- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field select **Session Manager**.
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**.
- In the **Port** field enter the port number to which the other system expects to receive SIP requests.
- Leave the **Connection Policy** drop down menu at the default value of **trusted** to make the other system trusted.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.
- Click **Commit** (not shown) to save changes. The screenshot shows the Entity Links used in this configuration.

<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_Link	Session_Manager	TCP	5060	ASBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM_Endpoint link	Session_Manager	TLS	5061	CM_SIP_Endpoints	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM_Trunk_Link	Session_Manager	TCP	5060	CM Trunk	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Messaging_Link	Session_Manager	TCP	5060	Messaging	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

Note: There are two Entity Links for Communication Manager, one for the SIP Endpoints and the other for the SIP Trunk. These are differentiated by **Protocol** and **Port**. 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, defined in **Section 6.5**, to which this routing policy applies (not shown).
- Under **Time of Day**, click **Add**, and then select the time range. **24/7** is provided as a default.

The following screen shows the routing policy for calls inbound from the SIP Trunk to Communication Manager.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM Trunk	10.10.9.12	CM	

Time of Day

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"/>	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 PSTN destinations via M-net SIP Trunk.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ASBCE	10.10.9.81	SIP Trunk	

Time of Day

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"/>	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**, in the resulting screen (not shown).
- Under **Originating Location**, select one of the locations defined in **Section 6.3** if routing depending on originating location is required. Alternatively, select **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 all calls starting with zero to the PSTN via M-net SIP Trunk.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call:

Emergency Priority:

Emergency Type:

SIP Domain: ▼

Notes:

Originating Locations and Routing Policies

1 Item Filter: Enable

	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		PSTN_Outbound	0	<input type="checkbox"/>	ASBCE	

Select : All, None

Note: Additional dial patterns (not shown) will be required for PSTN numbers that do not start with zero, for example directory enquiries. This was tested with a dial pattern of 3 to 6 digit numbers starting with 1.

The next screenshot shows the test dial pattern configured for Communication Manager. This is used to analyze the DDI numbers assigned to the extensions on Communication Manager. Some of the digits of the pattern to be matched have been obscured.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details

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"/>	Service_Provider		CM_Inbound	0	<input type="checkbox"/>	CM Trunk	

Select : All, None

Note: A specific location for the SIP Trunk was used for routing to Communication Manager. If required, an additional policy could be added to route calls differently if they originated within the enterprise. This may be useful if there is a requirement to route calls from one Communication Manager DDI number to another via the network.

6.9. Administer Application for Avaya Aura® Communication Manager

From the **Home** screen select **Session Manager** from the Elements menu. In the resulting tab from the left panel menu select **Application Configuration** → **Applications** and click **New** (not shown).

- In the **Name** field enter a name for the application.
- In the **SIP Entity** field select the SIP Entity for Communication Manager Endpoints described in **Section 6.5**.
- In the **CM System for SIP Entity** field select the appropriate Communication Manager from the System Manager inventory and select **Commit** to save the configuration.

The screenshot displays the Avaya Aura Application Editor interface. The breadcrumb navigation at the top reads: Home / Elements / Session Manager / Application Configuration / Applications. The left-hand navigation menu includes: Session Manager (expanded), Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, and Applications (selected). The main content area is titled "Application Editor" and contains a "Commit" button and a "Cancel" button. Below this is the "Application" configuration section with the following fields:

- *Name:** CM_App
- *SIP Entity:** CM_SIP_Endpoints
- *CM System for SIP Entity:** CM1_Element (with a Refresh button and a link to View/Add CM Systems)
- Description:** (empty text box)

Note: The Application described here and the Application Sequence described in the next section are likely to have been defined during installation. The configuration is shown here for reference. Note also that the Communication Manager SIP Entity selected is that set up specifically for SIP endpoints. In the test environment there is also a Communication Manager SIP Entity that is used specifically for the SIP Trunk and is not to be used in this case.

6.10. Administer Application Sequence for Avaya Aura® Communication Manager

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

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

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 (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	<input type="button" value="▲"/> <input type="button" value="▼"/> <input type="button" value="✕"/>	CM_App	CM_SIP_Endpoints	<input checked="" type="checkbox"/>	

Select : All, None

Available Applications

1 Item Filter: Enable

	Name	SIP Entity	Description
<input type="button" value="+"/>	CM_App	CM_SIP_Endpoints	

*Required

6.11. Administer SIP Extensions

The SIP extensions are likely to have been defined during installation. The configuration shown in this section is for reference. SIP extensions are registered with Session Manager and use Communication Manager for their feature and configuration settings. From the **Home** screen select **User Management** from the **Users** 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. **2291@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** as required.

The screenshot shows the 'New User Profile' form in the 'User Management' application. The form is divided into four tabs: 'Identity' (selected), 'Communication Profile', 'Membership', and 'Contacts'. The 'Identity' tab contains the following fields:

- User Provisioning Rule:** A dropdown menu.
- Last Name:** SIP
- Last Name (Latin Translation):** SIP
- First Name:** 9608
- First Name (Latin Translation):** 9608
- Middle Name:** (empty)
- Description:** (empty)
- Login Name:** 2291@avaya.com
- User Type:** Basic
- Password:** (masked with dots)
- Confirm Password:** (masked with dots)
- Localized Display Name:** (empty)
- Endpoint Display Name:** (empty)
- Title:** (empty)
- Language Preference:** English (United Kingdom)
- Time Zone:** (+1:0)GMT : Dublin, Edinburgh
- Employee ID:** (empty)
- Department:** (empty)
- Company:** (empty)

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

Communication Profile

Communication Profile Password:

Confirm Password:

Name
<input checked="" type="radio"/> Primary

Select : None

* Name:

Default :

Communication Address

Type	Handle	Domain
No Records found		

Session Manager Profile

CM Endpoint Profile

*Required

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

Type	Handle	Domain
No Records found		

Type:

* Fully Qualified Address: @

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

Primary	Secondary	Maximum
6	0	6

Secondary Session Manager

Survivability Server

Max. Simultaneous Devices ▾

Block New Registration When Maximum Registrations Active?

Application Sequences

Origination Sequence ▾

Termination Sequence ▾

Call Routing Settings

* Home Location ▾

Conference Factory Set ▾

Call History Settings

Enable Centralized Call History?

Expand the **Endpoint Profile** section.

- Select Communication Manager Element 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.
- Enter a **Voice Mail Number** if required. In the test environment, this was **7000**
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box.

The screenshot shows the configuration form for a CM Endpoint Profile. The form is titled "CM Endpoint Profile" and is expanded. It contains the following fields and options:

- System:** CM1_Element (dropdown)
- Profile Type:** Endpoint (dropdown)
- Use Existing Endpoints:**
- Extension:** 2291 (text field). A link "Display Extension Ranges" is visible above the field. A button "Endpoint Editor" is located to the right of the field.
- Template:** 9608SIP_DEFAULT_CM_7_0 (dropdown)
- Set Type:** 9608SIP (text field)
- Security Code:** (empty text field)
- Port:** IP (text field)
- Voice Mail Number:** 7000 (text field)
- Preferred Handle:** (None) (dropdown)
- Calculate Route Pattern:**
- Sip Trunk:** aar (text field)
- 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:**
- Allow H.323 and SIP Endpoint Dual Registration:**

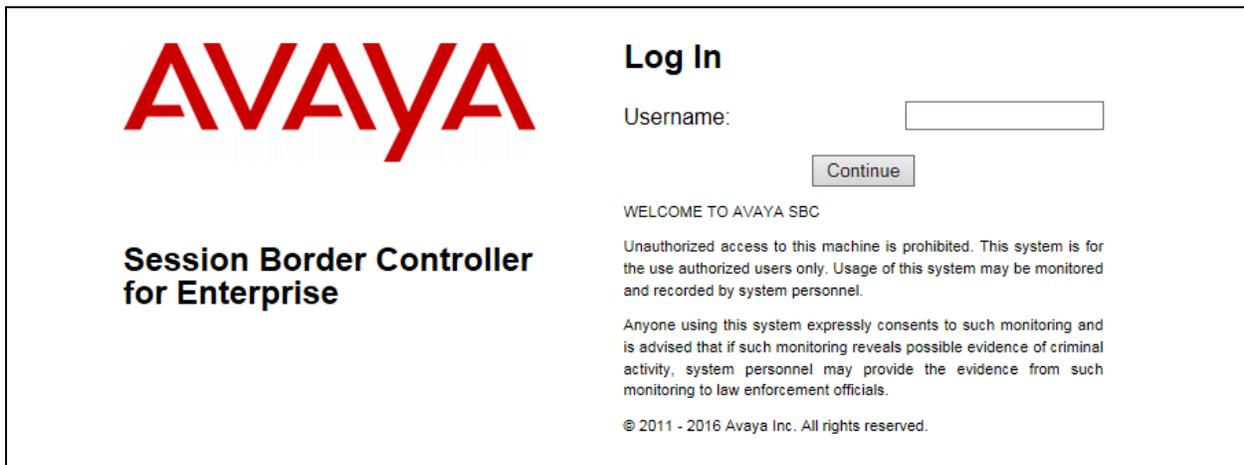
Select **Commit** (Not Shown) to save changes and the System Manager will add Communication Manager user configuration automatically.

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya 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.

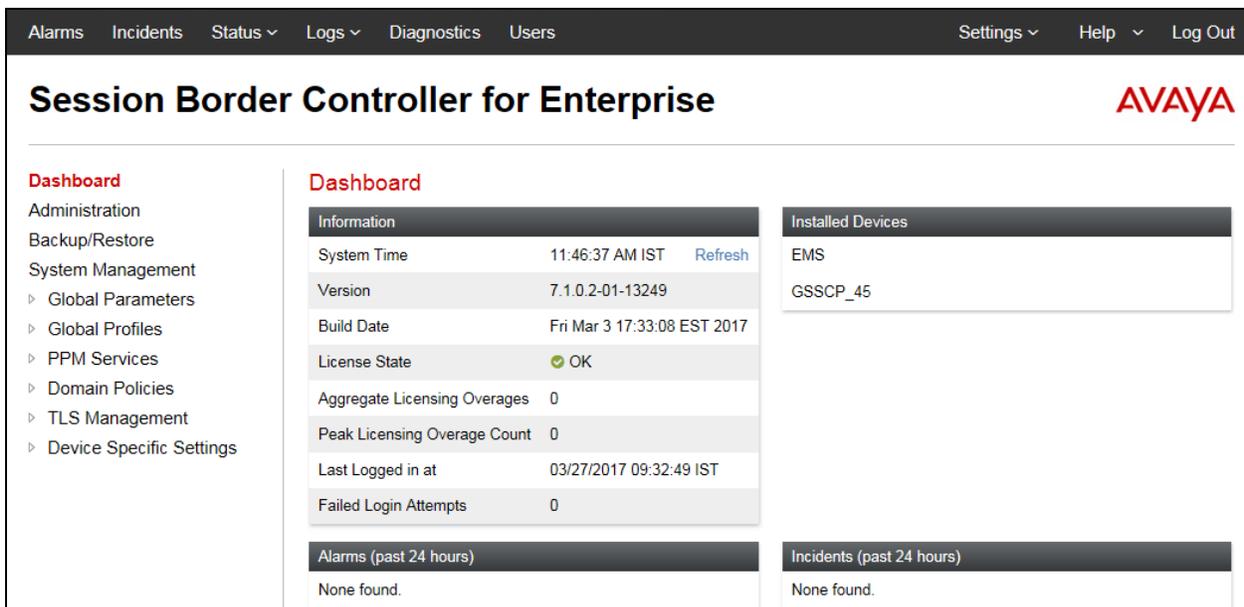
7.1. Access Avaya Session Border Controller for Enterprise

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 the appropriate username and password.



The login screen features the Avaya logo in red on the left. To the right, under the heading "Log In", there is a "Username:" label followed by a text input field and a "Continue" button. Below the input field, a message reads: "WELCOME TO AVAYA SBC. Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials. © 2011 - 2016 Avaya Inc. All rights reserved."

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 for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. A left-hand navigation menu includes: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled "Dashboard" and contains several panels: "Information" (System Time: 11:46:37 AM IST, Version: 7.1.0.2-01-13249, Build Date: Fri Mar 3 17:33:08 EST 2017, License State: OK, Aggregate Licensing Overages: 0, Peak Licensing Overage Count: 0, Last Logged in at: 03/27/2017 09:32:49 IST, Failed Login Attempts: 0), "Installed Devices" (EMS, GSSCP_45), "Alarms (past 24 hours)" (None found), and "Incidents (past 24 hours)" (None found).

7.2. Define Network Management

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that in the test environment only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external.

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**.

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Internal	10.10.9.1	255.255.255.0	A1	10.10.9.81	Edit Delete

Enter details for the external interfaces in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the external physical interface to be used from the **Interface** drop down menu. In the test environment, this was **B1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the external IP address of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

Name	External	
Default Gateway	192.168.122.9	
Network Prefix or Subnet Mask	255.255.255.128	
Interface	B1	
<input type="button" value="Add"/>		
IP Address	Public IP	Gateway Override
192.168.122.59	Use IP Address	Use Default
<input type="button" value="Delete"/>		
<input type="button" value="Finish"/>		

Click on **Add** to define the internal interface if required. Enter details in the dialogue box (not shown):

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the internal physical interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address for the Avaya SBCE in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

The following screenshot shows the completed Network Management configuration:

Network Management: GSSCP_45

Devices: GSSCP_45

Interfaces | Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
Internal	10.10.9.1	255.255.255.0	A1	10.10.9.81	Edit	Delete
External	192.168.122.9	255.255.255.128	B1	192.168.122.59	Edit	Delete

Select the **Interface Configuration** tab and click on the **Status** of the physical interface to toggle the state. Change the state to **Enabled** where required.

Network Management: GSSCP_45

Devices: GSSCP_45

Interfaces | Networks

Add VLAN

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Disabled

Message from webpage

Are you sure you wish to change the status of Interface to Enabled?

OK Cancel

Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted. Click on **System Management** in the main menu and select **Restart Application**.

The screenshot shows the 'System Management' section of a web interface. On the left is a navigation menu with 'System Management' selected. The main content area has tabs for 'Devices', 'Updates', 'SSL VPN', 'Licensing', and 'Key Bundles'. Below the tabs is a table with the following data:

Device Name	Management IP	Version	Status
GSSCP_45	10.10.2.45	7.1.0.2-01-13249	Commissioned

Below the table, there are several action buttons: 'Reboot', 'Shutdown', 'Restart Application' (highlighted with a red box), 'View', 'Edit', and 'Uninstall'.

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 TCP used for transport of signalling between Session Manager and the Avaya SBCE, and UDP for transport of signalling between the Avaya SBCE and the M-net SIP Trunk. A signalling and media interface was required on both the internal and external sides of the Avaya SBCE. This document shows the configuration for TCP and UDP, if additional security is required, it's recommended to use TLS and port 5061.

7.3.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** in the main menu on the left hand side. Click on **Add**.

The screenshot shows the 'Signaling Interface: GSSCP_45' configuration page. On the left, the navigation menu has 'Device Specific Settings' expanded to 'Signaling Interface'. The main content area has a sub-tab for 'Signaling Interface'. A warning message in a red box states: 'Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is an 'Add' button and a blue instruction box that says 'Use the add button to create a new Signaling Interface.'

Details of transport protocol and ports for the external and internal SIP signalling are entered in the dialogue box.

- In the **Name** field enter a descriptive name for the external signalling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was IP address **192.168.122.59** for the Avaya SBCE interface on the SIP Trunk.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for the M-net SIP Trunk.
- Click on **Finish**

Name	External
IP Address	External (B1, VLAN 0) 192.168.122.59
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

The internal signalling interface is defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal signalling interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.
- Select **TCP** port number, **5060** is used for Session Manager.

The following screenshot shows details of the signalling interfaces:

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
External	192.168.122.59 External (B1, VLAN 0)	---	5060	---	None	Edit Delete
Internal	10.10.9.81 Internal (A1, VLAN 0)	5060	---	---	None	Edit Delete

Note: In the test environment, the internal IP address was **10.10.9.81**.

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. Click on **Add**.

Details of the RTP port ranges for the internal and external media streams are entered in the dialogue box. The IP addresses for media can be the same as those used for signalling.

- In the **Name** field enter a descriptive name for the external media interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was IP address **192.168.122.59**.
- Define the RTP **Port Range** for the media path with the M-net SIP Trunk, during testing this was left at default values of **35000 - 40000**.

The internal media interfaces are defined in the same way; the dialogue box is not shown:

- 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.
- In the **IP Address** drop down menus, select the internal network interface and IP address.

The following screenshot shows details of the media interfaces:

Name	Media IP Network	Port Range	
External	192.168.122.59 External (B1, VLAN 0)	35000 - 40000	Edit Delete
Internal	10.10.9.81 Internal (A1, VLAN 0)	35000 - 40000	Edit Delete

Note: In the test environment, the internal IP address was **10.10.9.81** and the port range was left at default values.

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the M-net 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 M-net SIP Trunk, highlight the **avaya-ru** profile and click on **Clone**.

Parameter	Value
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

A pop-up menu is generated. In the **Name** field enter a descriptive name for the M-net network and click **Finish**.

Clone Profile

Profile Name: avaya-ru

Clone Name: SIP_Trunk

Finish

The screenshot over the page shows the cloned profile in the **General** tab, no editing is required.

Editing Profile: SIP_Trunk

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

URI Group

Send Hold

Delayed Offer

3xx Handling

Diversion Header Support

Delayed SDP Handling

Re-Invite Handling

Prack Handling

Allow 18X SDP

T.38 Support

URI Scheme SIP TEL ANY

Via Header Format RFC3261
 RFC2543

Select the **Timers** tab if any timers need to be set. During testing there were issues with delays in signalling traffic and the **Init Timer** corresponding to SIP round trip timer T1 was increased to **1000** to reduce the instances of duplicated messages. In the live network it may be desirable to reduce this timer as call failure handling can be invoked more rapidly.

Editing Profile: SIP_Trunk

All fields are optional.

SIP Timers

Min-SE seconds, [90 - 86400]

Init Timer milliseconds, [50 - 1000]

Max Timer milliseconds, [200 - 8000]

Trans Expire seconds, [1 - 64]

Invite Expire seconds, [180 - 300]

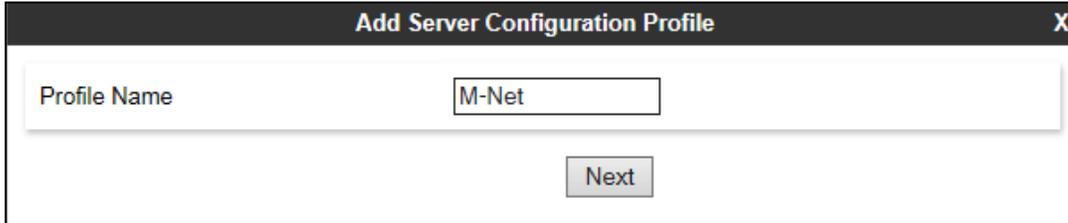
Select the **Advanced** tab. Set **Record Routes** to **None** as this header is not used by the network and select **None** in the **Extensions** drop down menu. Ensure that the **Has Remote SBC** box is checked. Click on **Finish**.

Repeat the process to define Server Interworking for Session Manager. In the Advanced tab (not shown), leave the settings at the original values cloned from the avaya-ru profile. **Record Routes** is set to **Both Sides** as the Session Manager uses the Record-Route header and **Avaya** is selected in the **Extension** drop down menu.

7.5. Define Servers

A server definition is required for each server connected to the Avaya SBCE. The M-net SIP Trunk is connected as a Trunk Server. Session Manager is connected as a Call Server. To define the M-net SIP Trunk Server, navigate to **Global Profiles** → **Server Configuration** in the main menu on the left hand side. Click on **Add**.

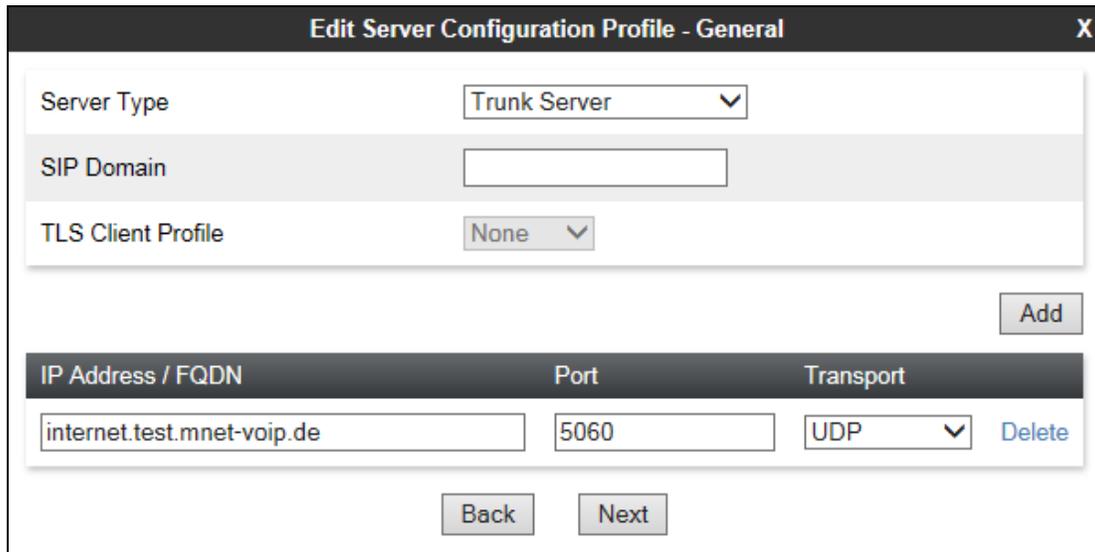
Enter an appropriate name in the pop-up menu and click on **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "M-Net". Below the input field is a "Next" button.

Enter details in the dialogue box.

- In the **Server Type** drop down menu, select **Trunk Server**.
- Click on **Add** to enter an IP address
- In the **IP Addresses / FQDN** box, type the M-net SIP Trunk FQDN.
- In the **Port** box, enter the port to be used for the SIP Trunk.
- In the **Transport** drop down menu, select **UDP**.
- Click on **Next**.



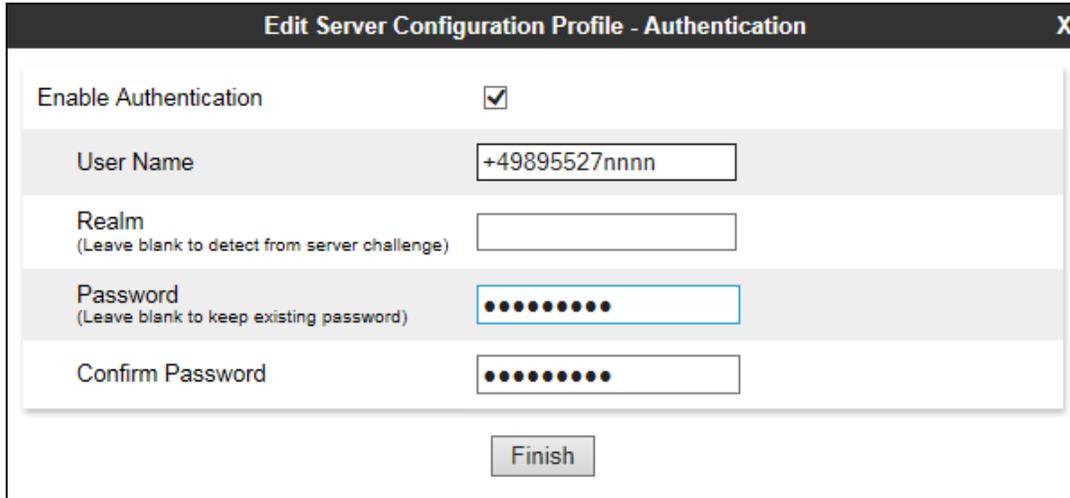
The screenshot shows a dialog box titled "Edit Server Configuration Profile - General" with a close button (X) in the top right corner. The dialog contains several fields and a table:

- Server Type**: A dropdown menu set to "Trunk Server".
- SIP Domain**: An empty text input field.
- TLS Client Profile**: A dropdown menu set to "None".
- Add**: A button to add a new entry to the table.
- Table**: A table with three columns: "IP Address / FQDN", "Port", and "Transport". The first row contains the values "internet.test.mnet-voip.de", "5060", and "UDP". A "Delete" button is located to the right of the first row.
- Back** and **Next**: Buttons at the bottom of the dialog.

Note: The FQDN used during testing was for the test system only and is shown as an example. At the time of writing, some customers were using **business.m-call.de** which is due to be shut down. This will be changed to **business.mnet-voip.de**. When the change is made, the new FQDN will be entered in the **IP Address/FQDN** field as shown above.

Click on **Next** and enter the authentication details required for the M-net SIP trunk:

- Check the **Enable Authentication** box
- Enter the **User Name** provided by M-net
- Leave the **Realm** blank to use server settings
- Enter and confirm the **Password** provided by M-net



Edit Server Configuration Profile - Authentication

Enable Authentication

User Name

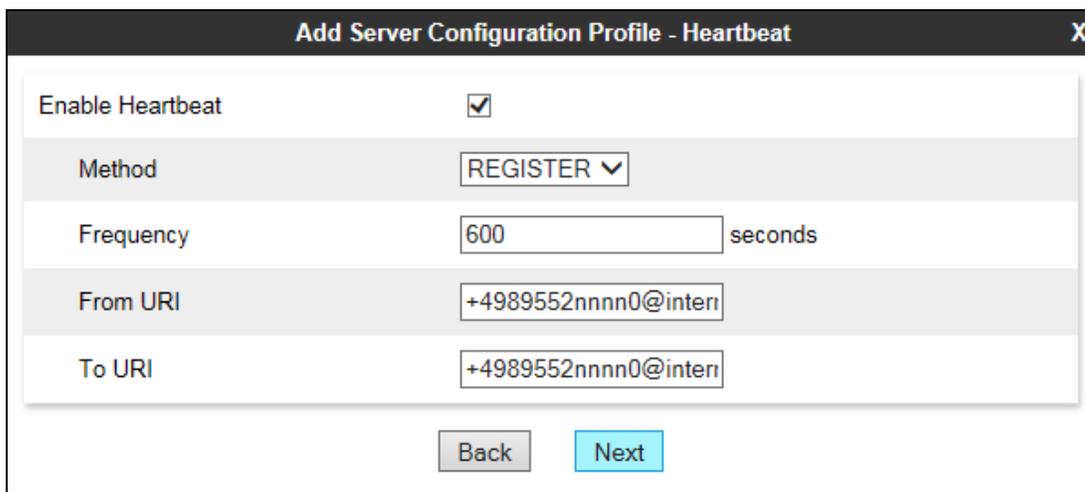
Realm
(Leave blank to detect from server challenge)

Password
(Leave blank to keep existing password)

Confirm Password

Click on **Next** again and enter the details for registration of the Avaya SBCE with the M-net SIP Trunk. Registration is set up using the Heartbeat function of the Avaya SBCE as follows:

- Check the **Enable Heartbeat** box.
- Select **REGISTER** from the **Method** drop down menu.
- Enter a **Frequency** value. A value of **600** was used during testing so that registration took place every 10 minutes. This ensured that registration took place well within the expiry time of 1200 seconds received from M-net in the expires parameter of the Contact header.
- Enter a **From URI** and **To URI**. The Authentication User Name and M-net domain were used during testing.



Add Server Configuration Profile - Heartbeat

Enable Heartbeat

Method

Frequency seconds

From URI

To URI

Click on **Next** again to get to the final dialogue box. This contains the **Advanced** settings:

- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for M-net SIP Trunk defined in **Section 7.4**.
- Leave the other fields at default settings.
- Click **Finish**.

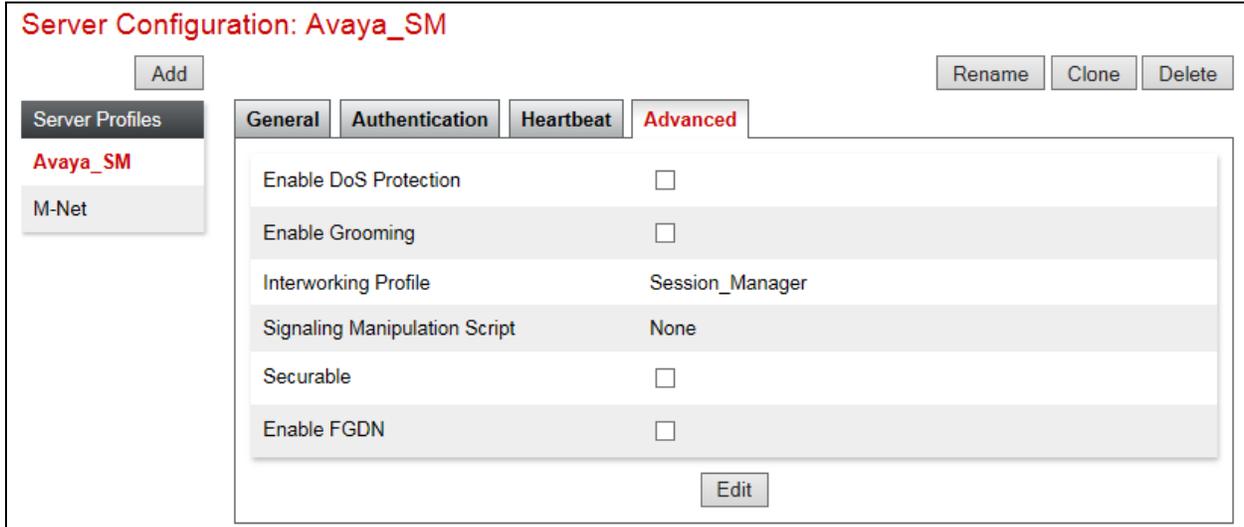
Use the process described to define the Call Server configuration for Session Manager if not already defined. Leave the Authentication and Heartbeat settings at default values.

- Ensure that **Call Server** is selected in the **Server Type** drop down menu in the **General** dialogue box (not shown).
- Ensure that the Interworking Profile defined for Session Manager in **Section 7.4** is selected in the **Interworking Profile** drop down menu in the **Advanced** dialogue box (not shown).

The following screenshot shows the **General** tab of the completed Server Configuration:

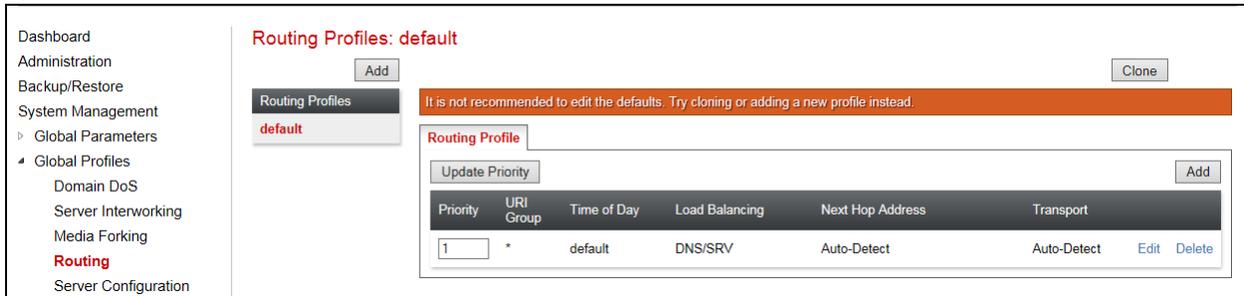
IP Address / FQDN	Port	Transport
10.10.9.31	5060	TCP

The following screenshot shows the **Advanced** tab of the completed Server Configuration:

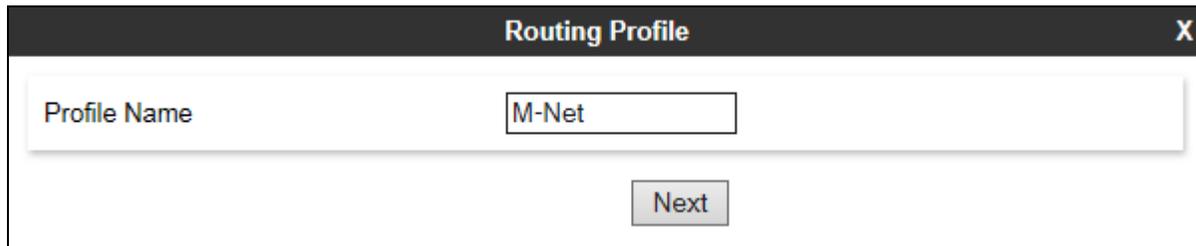


7.6. Define Routing

Routing information is required for routing to the M-net SIP Trunk on the external side and Session Manager on the internal side. The IP addresses and ports defined here will be used as the destination addresses for signalling. To define routing to M-net SIP Trunk, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add**.



Enter an appropriate name in the dialogue box. And click on **Next**.



Enter details for the Routing Profile for the SIP Trunk:

- During testing, **Load Balancing** was not required and was left at the default value of **Priority**.
- Click on **Add** to specify an address for the SIP Trunk.
- Assign a priority in the **Priority / Weight** field, during testing **1** was used.
- Select the Server Configuration defined in **Section 7.5** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>
ENUM	<input type="checkbox"/>	ENUM Suffix	

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	M-Net	internet.test.mnet-voip.de:5060	None	Delete

Repeat the process for the Routing Profile for Session Manager. The following screenshot shows the completed configuration:

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	10.10.9.31	TCP	Edit Delete

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 termination information and the external interfaces for origination information.

To define Topology Hiding for M-net SIP Trunk, navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side. Select the default profile and click on **Clone**.

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

Assign an appropriate name in the dialogue box and click on **Finish**:

Profile Name: default

Clone Name: M-Net

Finish

Highlight the new Topology Hiding profile (not shown) and click on **Edit**. Make changes for the required header.

During testing, only the **From** header was changed.

- Select **IP** or **IP/Domain** from the **Criteria** drop down menu depending on requirements. During testing the default **IP/Domain** was used that hides both domain names and IP addresses.
- Select **Overwrite** in the **Replace Action** drop down menu.
- Define a domain name in the **Overwrite Value** field. Use the domain name defined for the M-Net server settings as shown in **Section 7.5**. During testing **internet.test.mnet-voip.de** was used.

Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	internet.test.mnet-voip
To	IP/Domain	Auto	
Record-Route	IP/Domain	Auto	
SDP	IP/Domain	Auto	
Request-Line	IP/Domain	Auto	
Refer-To	IP/Domain	Auto	
Via	IP/Domain	Auto	
Referred-By	IP/Domain	Auto	

The following screenshot shows the completed **Topology Hiding** configuration for the M-net SIP Trunk.

Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	internet.test.mnet-voip.de
To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---

To define Topology Hiding for Session Manager, follow the same process. During testing, the default profile was used so an additional profile was not required.

7.8. Server Flows

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

To define a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click on **Add**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The page title is "Session Border Controller for Enterprise" with the AVAYA logo in the top right corner. On the left is a navigation menu with categories: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management), and Device Specific Settings (with sub-items: Network Management, Media Interface, Signaling Interface, and End Point Flows). The main content area is titled "End Point Flows: GSSCP_45". It features three tabs: "Devices" (selected), "Subscriber Flows", and "Server Flows". Under the "Devices" tab, there is a list item "GSSCP_45". Under the "Server Flows" tab, there is an "Add" button and a blue instruction box that reads "Use the add button to create a new Server Flow."

Define the Server flow for the M-net SIP Trunk as follows:

- In the **Flow Name** field enter a descriptive name for the server flow for the M-net SIP Trunk, in the test environment **M-Net_Trunk** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the M-net SIP Trunk 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 the 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 the 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 the SIP Trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the M-net SIP Trunk defined in **Section 7.7** and click **Finish**.

Field	Value
Flow Name	M-Net_Trunk
Server Configuration	M-Net
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Internal
Signaling Interface	External
Media Interface	External
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya_SM
Topology Hiding Profile	M-Net
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

Define a Server Flow for Session Manager as follows:

- In the **Flow Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **SM_Call_Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for 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 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 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 Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the M-net SIP Trunk defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select **default** and click **Finish**.

Field	Value
Flow Name	SM_Call_Server
Server Configuration	Avaya_SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	External
Signaling Interface	Internal
Media Interface	Internal
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	M-Net
Topology Hiding Profile	default
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

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

End Point Flows: GSSCP_45

Devices

GSSCP_45

Subscriber Flows

Server Flows

Add

Click here to add a row description.

Server Configuration: Avaya_SM

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile					
1	SM_Call_Server	*	External	Internal	default-low	M-Net	View	Clone	Edit	Delete	

Server Configuration: M-Net

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile					
1	M-Net_Trunk	*	Internal	External	default-low	Avaya_SM	View	Clone	Edit	Delete	

8. Configure the M-net SIP Trunk Equipment

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

9. Verification Steps

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

1. From System Manager **Home** screen 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**.

The screenshot shows the 'Session Manager Entity Link Connection Status' page. The breadcrumb trail is 'Home / Elements / Session Manager / System Status / SIP Entity Monitoring'. The page title is 'Session Manager Entity Link Connection Status'. Below the title, there is a description: 'This page displays detailed connection status for all entity links from a Session Manager.' There is a section for 'All Entity Links for Session Manager: Session_Manager' with a 'Summary View' button. Below that, there is a table with 4 items. The table has the following columns: SIP Entity Name, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. All four items have a 'UP' status.

SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
CM SIP Endpoints	10.10.9.12	5061	TLS	FALSE	UP	200 OK	UP
ASBCE	10.10.9.81	5060	TCP	FALSE	UP	200 OK	UP
CM Trunk	10.10.9.12	5060	TCP	FALSE	UP	200 OK	UP
Messaging	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP

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

```
status trunk 2

TRUNK GROUP STATUS

Member   Port      Service State      Mtce Connected Ports
                   Busy

0002/001 T00011   in-service/idle    no
0002/002 T00012   in-service/idle    no
0002/003 T00013   in-service/idle    no
0002/004 T00014   in-service/idle    no
0002/005 T00015   in-service/idle    no
0002/006 T00016   in-service/idle    no
0002/007 T00017   in-service/idle    no
0002/008 T00018   in-service/idle    no
0002/009 T00019   in-service/idle    no
0002/010 T00020   in-service/idle    no
```

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.
7. Should issues arise with the SIP trunk, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from Session Manager via the Avaya SBCE to the network SBCs are receiving a response.

To define a trace on the Avaya SBCE, 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**.

The screenshot displays the Avaya SBCE configuration interface. On the left is a navigation menu with categories like Dashboard, Administration, and Device Specific Settings. The 'Trace' option is highlighted. The main area shows a 'Trace: GSSCP_45' header and a 'Packet Capture' configuration window. This window includes fields for Interface (B1), Local Address (All), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (SIP_Trunk_Test.pcap). There are 'Start Capture' and 'Clear' buttons at the bottom of the configuration window.

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

Trace: GSSCP_45

Devices: GSSCP_45

Packet Capture Captures Refresh

File Name	File Size (bytes)	Last Modified	
SIP_Trunk_Test_20170329071819.pcap	286,720	March 29, 2017 7:27:16 AM IST	Delete

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R7.0.1, Avaya Aura® Session Manager R7.0.1 and Avaya Session Border Controller for Enterprise R7.1 to M-net Premium SIP-Trunk. M-net Premium SIP-Trunk is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. Additional References

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

- [1] *Migrating and Installing Avaya Appliance Virtualization Platform*, Release 7.0.1, Aug 2016.
- [2] *Upgrading and Migrating Avaya Aura® applications to 7.0.1 from System Manager*, Release 7.0.1, Mar 2017.
- [3] *Deploying Avaya Aura® applications from System Manager*, Release 7.0, Aug 2016
- [4] *Deploying Avaya Aura® Communication Manager*, Oct 2016
- [5] *Administering Avaya Aura® Communication Manager*, Release 7.0.1, May 2016.
- [6] *Deploying Avaya Aura® System Manager*, Release 7.0.1 Aug 2016
- [7] *Upgrading Avaya Aura® Communication Manager*, Release 7.0.1, Oct 2016
- [8] *Upgrading Avaya Aura® System Manager to Release 7.0.1*, Aug 2016.
- [9] *Administering Avaya Aura® System Manager for Release 7.0.1*, Nov 2016
- [10] *Deploying Avaya Aura® Session Manager*, Release 7.0.1 Nov 2016
- [11] *Upgrading Avaya Aura® Session Manager* Release 7.0.1, Mar 2017
- [12] *Administering Avaya Aura® Session Manager* Release 7.0.1, May 2016,
- [13] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.1, Nov 2016
- [14] *Upgrading Avaya Session Border Controller for Enterprise*, Release 7.1, Aug 2016
- [15] *Administering Avaya Session Border Controller for Enterprise*, Release 7.1, Jun 2016
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2017 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.