



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R8.1, Avaya Aura® Session Manager R8.1 and Avaya Session Border Controller for Enterprise R8.1 to support M-net Premium SIP Trunk Service using TLS - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the M-net Premium SIP Service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Aura® Communication Manager R8.1, Avaya Aura® Session Manager R8.1 and Avaya Session Border Controller for Enterprise R8.1 using Transport Layer Security (TLS) for signalling and Secured Real-Time Protocol (SRTP) for media encryption.

The M-net Premium SIP Platform 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 Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura ® Communication Manager R8.1 (Communication Manager); Avaya Aura ® Session Manager R8.1 (Session Manager) and Avaya Session Border Controller for Enterprise R8.1 (Avaya SBCE).

Customers using this Avaya SIP-enabled enterprise solution with the M-net Premium SIP Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. 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 platform.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For security, TLS and SRTP was used internally to the enterprise between Avaya products and external public SIP trunk connection between Avaya SBCE and M-net Premium SIP platform.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using the M-net SIP platform, calls made to SIP, H.323, Digital and Analogue telephones at the enterprise.
- Outgoing calls from the enterprise site completed via the M-net SIP platform to PSTN destinations, calls made from SIP, H.323, Digital and Analogue telephones.
- Incoming and Outgoing PSTN calls to/from Avaya one-X® Communicator and Avaya Workplace Client for Windows soft phones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya 96x1 Deskphones (SIP).
- Calls using G.711A codec.
- Fax calls to/from Client a group 3 fax machine to a PSTN-connected fax machine using T.38-g.711 fallback transmission.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, call mute, transfer, and conference.
- Off-net call forwarding and mobile twinning.
- Routing inbound vector call to call center agent queues.

2.2. Test Results

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

- Mobility features such as on-net and off-net calling were not tested as the From Header CLID containing the mobility number on inbound calls to M-net SIP Trunk service was automatically changed by M-net to a CLID number recognizable to the M-net SIP network.
- G.729 codec is not supported by M-net and therefore was not tested.
- When testing inbound call failure handling, multiple SIP INVITE messages were observed and the SIP Trunk went out of service for a short period of time. This was not a SIP interoperability issue, instead it was a PSTN interconnect issue where the fault condition resulted in rapidly repeated re-routing attempts. The test cases where this behaviour was observed were inbound calls to an unallocated number and inbound calls with no matching codec's.

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 platform. Located at the Enterprise site is an Avaya SBCE, Session Manager and Communication Manager. Endpoints are Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya J179 series SIP telephones, Avaya digital telephone, Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Avaya Workplace Client for Windows running on laptop PCs. Additionally, the reference configuration included remote worker functionality. Remote worker is a SIP endpoint that resides in the untrusted network, registered to Session Manager at the enterprise via the Avaya SBCE. Remote Worker functionality was successfully tested using Avaya 96x1 SIP Deskphones. The configuration required to support remote workers are beyond the scope of these Application Notes. Please refer to reference [16] in the **References** section for additional information..

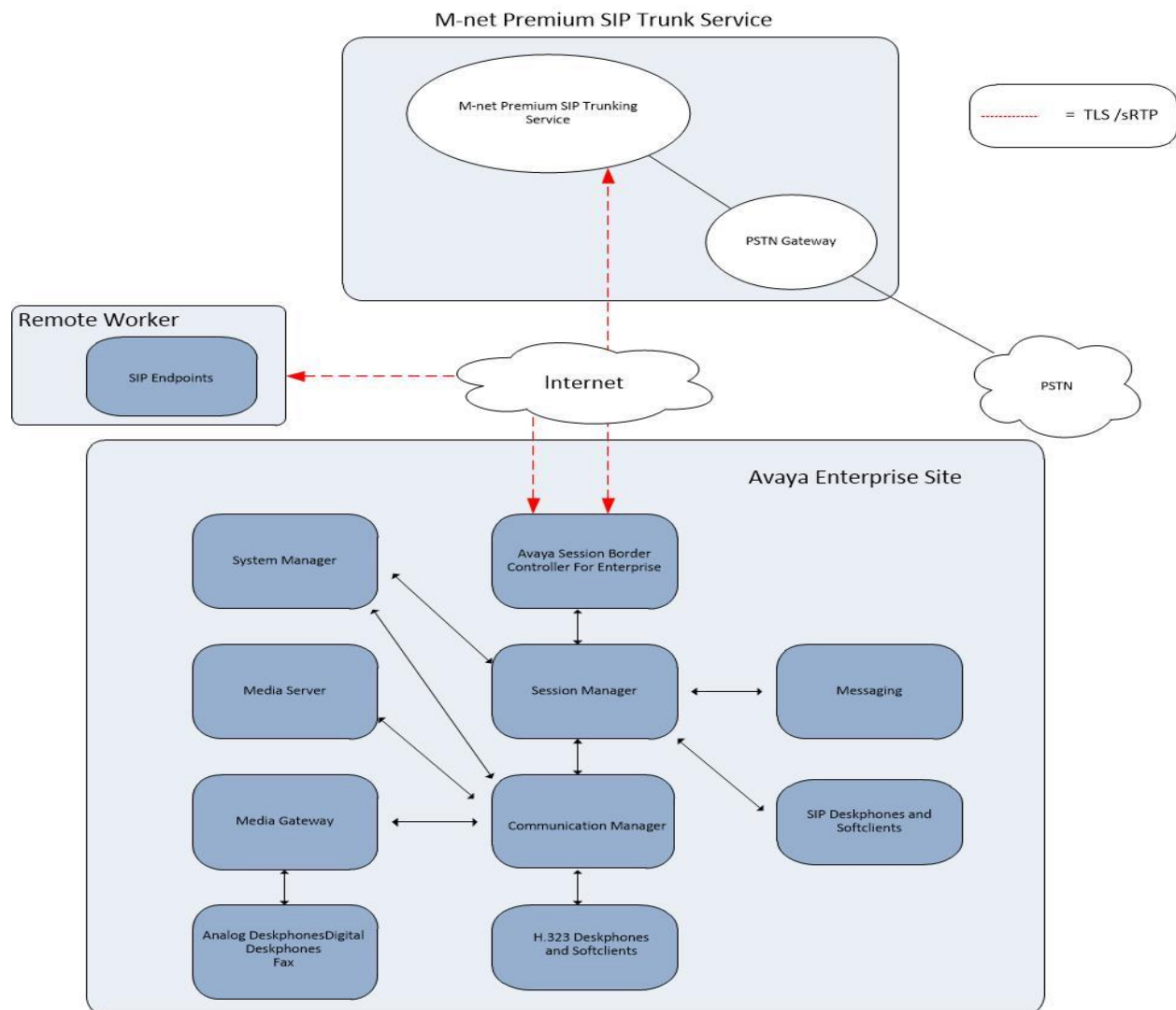


Figure 1: Test Setup M-net Premium SIP Service to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® System Manager	8.1.3.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.1.1012244 Service Pack 1
Avaya Aura® Session Manager	8.1.3.1.813113
Avaya Aura® Communication Manager	8.1.3.1 – 26766
Avaya Session Border Controller for Enterprise	8.1.2.0-31-19809
Avaya G430 Media Gateway	41.34.1
Avaya Aura® Media Server	v.8.0.2.163
Avaya 96x1 IP DeskPhone (H.323)	6.8.5
Avaya 9611 IP DeskPhone (SIP)	7.1.12
Avaya J179 IP Deskphone (SIP)	4.0.8.0
Avaya one-X® Communicator (H.323 & SIP)	6.2.14.13 -SP14-Patch5
Avaya Workplace Client for Windows	3.17.0.65.16
Avaya 1408 Digital Phone	R48
Avaya 98390 Analogue Phone	N/A
Analogue Fax	N/A
M-net	
Metaswitch Perimeta SBC and IPX (Class 4 Switch/Routing and SBC)	V4.7.30_SU95
Metaswitch CFS (Class 5 Switch)	V9.6.20_SU6

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 Trunking Service. 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 network, and any other SIP trunks used.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	0
Maximum Concurrently Registered IP Stations:		18000	3
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		414	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		41000	0
Maximum Video Capable IP Softphones:		18000	0
Maximum Administered SIP Trunks:		24000	10
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
Maximum TN2501 VAL Boards:		128	0
Maximum Media Gateway VAL Sources:		250	1
Maximum TN2602 Boards with 80 VoIP Channels:		128	0
Maximum TN2602 Boards with 320 VoIP Channels:		128	0
Maximum Number of Expanded Meet-me Conference Ports:		300	0

On **Page 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? y	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y		Multifrequency Signaling? y
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y		Multimedia IP SIP Trunking? y
IP Trunks? y		
IP Attendant Consoles? y		

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for Session Manager. In this case, **Session Manager** and **10.10.3.42** 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.

display node-names ip		IP NODE NAMES
Name	IP Address	
AMS	10.10.3.45	
Session_Manager	10.10.3.42	
default	0.0.0.0	
procr	10.10.3.44	
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 a PSTN call is shuffled or the call is set up with initial IP-IP direct media, the media stream is established directly between the enterprise end-point and the internal media interface of the Avaya SBCE.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** is used.
- The rest of the fields can be left at default values.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 2
Location: Authoritative Domain: avaya.com
Name: Trunk Stub Network Region: n
MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes
Codec Set: 1 Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048 IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

5.4. Administer IP Codec Set

Open the IP Codec Set form for the codec set specified in the IP Network Region form in **Section 5.3** by typing **change ip-codec set n** where **n** is the chosen value of the configuration for the SIP Trunk. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codec supported by M-net were configured, namely **G.711A**.

In addition to the codec's, the **Media Encryption** is defined here. For the compliance test, a value of **srtplib-aescm128-hmac80** was used.

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

                                IP MEDIA PARAMETERS

Codec Set: 2

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

Media Encryption                                Encrypted SRTCP: enforce-unenc-srtcp
1: srtplib-aescm128-hmac80
2: none
```

M-net Premium SIP Trunk supports T.38 for transmission of fax. Navigate to **Page 2** and define fax properties as follows:

- Set the **FAX - Mode** to **t.38-g711-fallback**.
- Leave **ECM** at default value of **y**.

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

                                IP MEDIA PARAMETERS

                                Allow Direct-IP Multimedia? n

                                Mode                                Redun-
                                t.38-G711-fallback 0          dancy
                                off                    0          ECM: y FB-Timer:4
                                US                      3
                                n                        0
                                n                        0          Packet
                                SIP 64K Data           20          Size (ms)

Media Connection IP Address Type Preferences
1: IPv4
2:
```

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 platform. Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set **Group Type** to **sip**.
- Set **Transport Method** to **tls**.
- 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. The standard value for TLS is **5061**.
- 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 **1**).
- Leave **Far-end Domain** blank to allow Communication Manager to accept calls from any SIP domain on the associated trunk.
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from Communication Manager).
- Set **Direct IP-IP Audio Connections** to **y**.
- Set **Initial IP-IP Direct Media** to **y**.
- Set **H.323 Station Outgoing Direct Media** to **y**.

The default values for the other fields may be used.

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

5.6. Administer SIP Trunk Groups

A trunk group is associated with the signalling 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-netwrk**.
- Specify the signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**.
- Specify the **Number of Members** administered for this SIP trunk group.

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: OUTSIDE CALL	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 1		
	Number of Members: 10		

On **Page 2** of the trunk-group form, the Preferred **Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with M-net to prevent unnecessary SIP messages during call setup.

add trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 900			
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto		Delay Call Setup When Accessed Via IGAR? n	
Caller ID for Service Link Call to H.323 1xC: station-extension			

On **Page 3**, set the **Numbering Format** field to **public**. This allows delivery of CLI in format of E.164 with leading “+”. Also, set the **Hold/Unhold Notifications** to **n**.

add trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: public
	UII Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? n
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

On **Page 4** of this form:

- Set **Mark Users as Phone** to **y**.
- Set **Send Transferring Party Information** to **y**.
- Set **Network Call Redirection** to **n**.
- Set **Send Diversion Header** to **y**.
- Set **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **101** as requested by M-net.
- Set **Always Use re-INVITE for Display Updates** to **y**.
- Set the **Identity for Calling Party Display** to **P-Asserted-Identity**.

add trunk-group 2	Page 4 of 21
PROTOCOL VARIATIONS	
	Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
	Send Transferring Party Information? y
	Network Call Redirection? n
	Send Diversion Header? y
	Support Request History? n
	Telephone Event Payload Type: 101
	Convert 180 to 183 for Early Media? n
	Always Use re-INVITE for Display Updates? y
	Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
	Enable Q-SIP? N
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
	Request URI Contents: may-have-extra-digits

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number in the format required. These calling party numbers are sent in the SIP From, Contact and PAI headers as well as the Diversion header for forwarded calls. The numbers are displayed on display-equipped PSTN telephones with any reformatting performed in the network. The public numbering table is used for numbers in E.164 format.

change public-unknown-numbering 0						Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT						
Ext	Trk	CPN	CPN	Total		
Len	Code	Grp(s)	Prefix	Len		
4	6010	1	4989xxxxxxx10	13		Total Administered: 4
4	6102	1	4989xxxxxxx11	13		Maximum Entries: 240
4	6020	1	4989xxxxxxx12	13		
4	6030	1	4989xxxxxxx13	13		Note: If an entry applies to
4	6104	1	4989xxxxxxx14	13		a SIP connection to Avaya
						Aura(R) Session Manager,
						the resulting number must
						be a complete E.164 number.
						Communication Manager
						automatically inserts
						a '+' digit in this case.

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the M-net Premium SIP Trunking Service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to invoke ARS directly. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *69		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 7		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning **0**. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Max	Route Pattern	Call Type	Node Num	ANI Reqd	
0	11	14	1	pubu		n	
00	13	15	1	pubu		n	
0035391	13	13	1	pubu		n	
030	10	10	1	pubu		n	
0800	8	10	1	pubu		n	
0900	8	8	1	pubu		n	

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**. **Numbering Format** is applied to CLI and is used to set TDM signalling parameters such as type of number and numbering plan indicator. This doesn't have the same significance in SIP calls and during testing it was set to **pub-unk**.

change route-pattern 1														Page 1 of 3
Pattern Number: 1							Pattern Name:							
SCCAN? n							Secure SIP? n							
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits					QSIG		
							Dgts					Intw		
1: 1		0										n	user	
2:												n	user	
3:												n	user	
4:												n	user	
5:												n	user	
6:												n	user	
	BCC	VALUE	TSC	CA-TSC		ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR		
	0	1	2	M	4	W		Request		Dgts	Format			
										Subaddress				
1:	y	y	y	y	y	n	n		rest		pub-unk	none		
2:	y	y	y	y	y	n	n		rest			none		
3:	y	y	y	y	y	n	n		rest			none		
4:	y	y	y	y	y	n	n		rest			none		
5:	y	y	y	y	y	n	n		rest			none		
6:	y	y	y	y	y	n	n		rest			none		

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DID calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from M-net can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DID numbers provided by M-net correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers **+4989xxxxxxxx** to a 4 digit extension by deleting all of the incoming digits and inserting an extension. Public DID numbers have been masked for security purposes.

change inc-call-handling-trmt trunk-group 1					Page	1 of	3
INCOMING CALL HANDLING TREATMENT							
Service/ Feature	Number Len	Number Digits	Del Insert				
public-ntwrk	14	+4989xxxxxxxx10	all 6010				
public-ntwrk	14	+4989xxxxxxxx11	all 6102				
public-ntwrk	14	+4989xxxxxxxx12	all 6020				
public-ntwrk	14	+4989xxxxxxxx13	all 6030				
public-ntwrk	14	+4989xxxxxxxx14	all 6104				

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 6102. Use the command **change off-pbx-telephone station-mapping x** where **x** is Communication Manager station.

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration.
- For the **Phone Number** enter the phone that will also be called (e.g. **0035389434xxxx**).
- Set the **Trunk Selection** to **ARS**.
- Set the **Config Set** to **1**.

change off-pbx-telephone station-mapping 6102							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
6102	EC500	-		0035389434xxxx	ARS	1	

Note: The phone number shown is for a mobile phone in the Avaya Lab. To use facilities for calls coming in from EC500 mobile phones, the calling party number received in Communication Manager must exactly match the number specified in the above table.

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

6. Configuring Avaya Aura® Session Manager

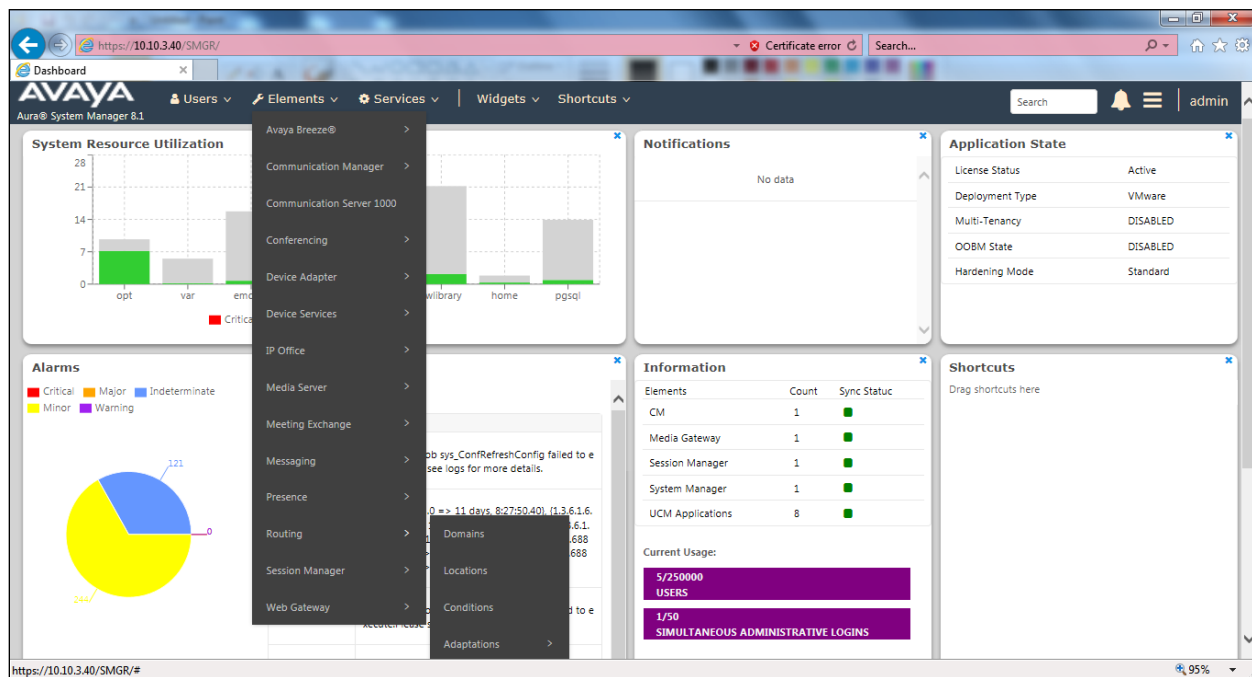
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

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

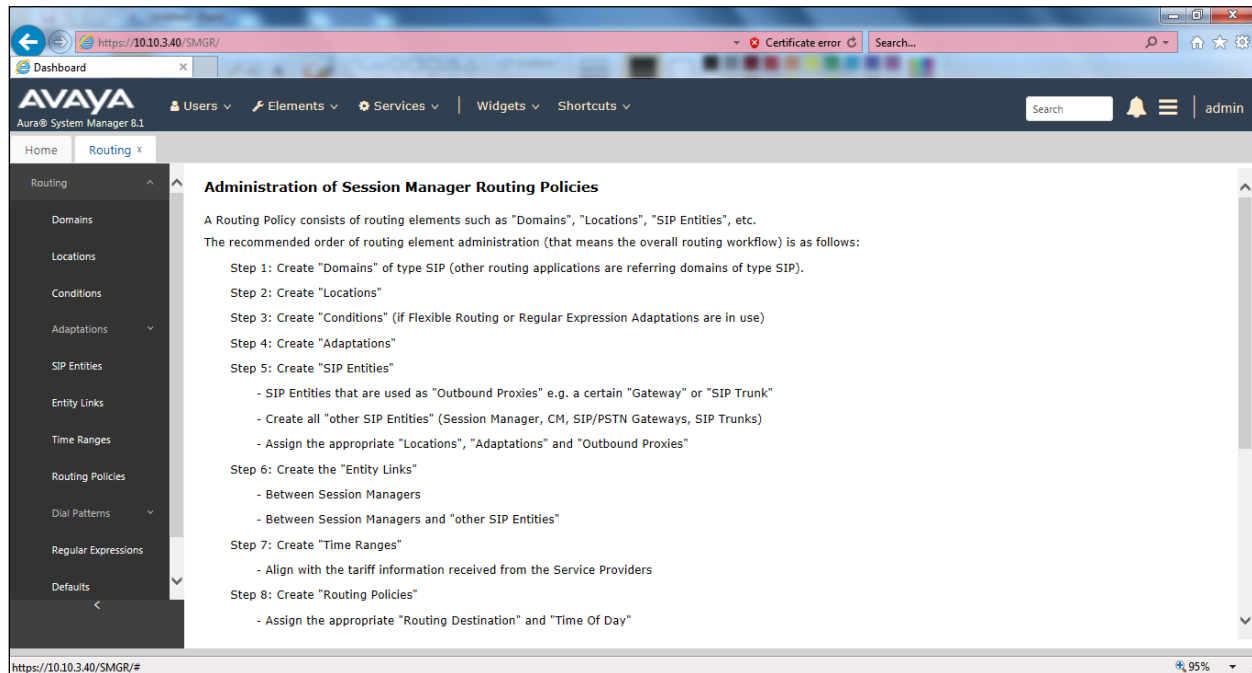
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a web browser 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 Dashboard tab will be presented with menu options shown below.



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

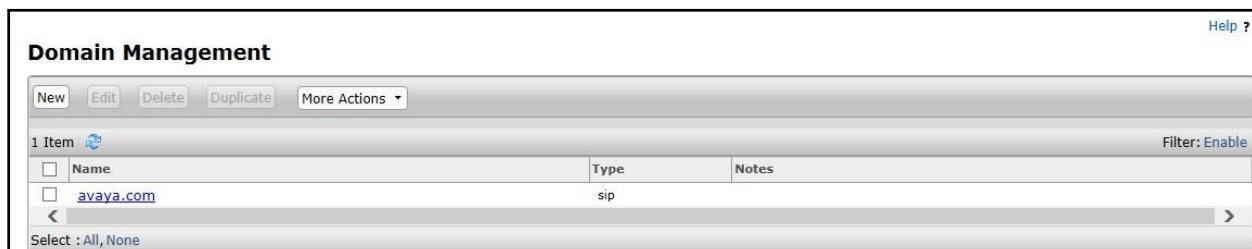


6.2. Administer SIP Domain

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

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

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



6.3. Administer Locations

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

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

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

In the **Location Pattern** section, click **Add** (not shown) and enter the following values.

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

Click **Commit** to save. The screenshot below shows the Location **SMGR_8** defined for the compliance testing.

The screenshot shows a web form titled "Location Details" with "Commit" and "Cancel" buttons in the top right. The form is divided into three sections: "General", "Dial Plan Transparency in Survivable Mode", and "Overall Managed Bandwidth".

- General**: Contains a required field "Name:" with the value "SMGR_8" and an optional "Notes:" field.
- Dial Plan Transparency in Survivable Mode**: Contains an "Enabled:" checkbox (unchecked), a "Listed Directory Number:" field, and an "Associated CM SIP Entity:" field.
- Overall Managed Bandwidth**: Contains a "Managed Bandwidth Units:" dropdown menu set to "Kbit/sec", a "Total Bandwidth:" field, a "Multimedia Bandwidth:" field, and a checked checkbox for "Audio Calls Can Take Multimedia Bandwidth:".

6.4. Administer Adaptations

Session Manager Adaptations can be used to alter parameters in the SIP message headers. An Adaptation was used during testing to remove Avaya proprietary headers from messages sent. Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. In order to improve interoperability with third party elements, Session Manager R8.1 incorporates the ability to use Adaptation modules to remove specific SIP headers that are either Avaya proprietary unnecessary for non-Avaya elements. For the compliance test, an Adaptation named “**Mnet**” was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, and P-Location. These headers contain private information from the enterprise and also add unnecessary size to outbound messages, while they have no significance to the service provider.

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

- **Adaptation Name:** Enter an appropriate name such as **M-net**.
- **Module Name:** Select **DigitConversionAdapter**.
- **Modular Parameter Type:** Select **Name-Value Parameter**.

Click **Add** to add the name and value parameters.

- **Name:** Enter **eRHdrs**. This parameter will remove the specific headers from messages in the egress direction.
- **Value:** Enter **AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, P-Location**.
- **Name:** Enter **fromto**. Modifies From and To header of a message.
- **Value:** Enter **true**.
- **Name:** Enter **MIME**. Remove MIME message bodies from Session Manager.
- **Value:** Enter **no**.

Adaptation Details [Commit] [Cancel]

General

* **Adaptation Name:**

Notes:

* **Module Name:**

Type:

State:

Module Parameter Type:

Add Remove	
<input type="checkbox"/> Name	Value
<input type="checkbox"/> eRHdrs	"P-AV-Message-Id, P-Charging-Vector, P-Location, Endpoint-View, P-Conference, Alert-Info, Correlation-ID, Accept-
<input type="checkbox"/> fromto	true
<input type="checkbox"/> MIME	no

Select : All, None

Egress URI Parameters:

As M-net require a prefix 0 to be inserted before all national (0) dialled numbers and + for all international (00) dialled numbers for calls to route correctly, the below **Digit Conversion for Outgoing Calls from SM** was created and will match outgoing calls to national and international numbers beginning with 0 and 00 respectively.

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

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

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*0	*1	*16		*0	0	both		
<input type="checkbox"/>	*00353	*5	*16		*2	+	both		

This will ensure any outgoing national numbers matching 0 will have a prefix 0 inserted and any outgoing international numbers matching 00 will have prefix's 00 deleted and have + inserted being converted to E.164 format before being forwarded to the Avaya SBCE.

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 Entities.
- 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.

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

6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface and **Type** is **Session Manager**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

SIP Entity Details

CommitCancel

General

* Name:Session Manager

* IP Address:10.10.3.42

SIP FQDN:

Type:Session Manager

Notes:

Location:SMGR_8

Outbound Proxy:

Time Zone:Europe/Dublin

Minimum TLS Version:Use Global Setting

Credential name:

Monitoring

SIP Link Monitoring:Use Session Manager Configuration

CRLF Keep Alive Monitoring:Use Session Manager Configuration

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

- In the **Port** field enter the port number on which the system listens for SIP requests.
- In the **Protocol** field enter the transport protocol to be used for SIP requests.
- In the **Default Domain** field, from the drop-down menu select the domain added in **Section 6.2** as the default domain.

Port

TCP Failover port:

TLS Failover port:

AddRemove

3 Items

Filter: Enable

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

Select : All, None

6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. 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 **Location** to that defined in **Section 6.3**.

SIP Entity Details

CommitCancel

General

* Name:

Communication Manager

* FQDN or IP Address:

10.10.3.44

Type:

CM

▼

Notes:

Adaptation:

▼

Location:

SMGR_8

▼

Time Zone:

Europe/Dublin

▼

* SIP Timer B/F (in seconds):

4

Minimum TLS Version:

Use Global Setting

▼

Credential name:

Securable:

☐

Call Detail Recording:

none

▼

Loop Detection

Loop Detection Mode:

On

▼

Loop Count Threshold:

5

Loop Detection Interval (in msec):

200

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:

Off

▼

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

▼

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE used for PSTN destinations. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (See **Section 7.4.1**). Set the **Adaptation** to that defined in **Section 6.4**, the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

SIP Entity Details

CommitCancel

General

* Name:Avaya_SBCE

* FQDN or IP Address:10.10.3.30

Type:SIP Trunk

Notes:

Adaptation:Mnet

Location:SMGR_8

Time Zone:Europe/Dublin

* SIP Timer B/F (in seconds):4

Minimum TLS Version:Use Global Setting

Credential name:

Securable:

Call Detail Recording:egress

Loop Detection

Loop Detection Mode:On

Loop Count Threshold:5

Loop Detection Interval (in msec):200

6.6. Administer Entity Links

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

- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field select **Session Manager**.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**.
- In the **Port** field enter the port number to which the other system expects to receive SIP requests.
- Select **Trusted** from the drop-down menu to make the other system trusted.

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

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	Communication Manager	Session Manager	TLS	5061	Communication Manager	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Experience Portal	Session Manager	TLS	5061	Experience_Portal	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	to Avaya SBCE	Session Manager	TLS	5061	Avaya_SBCE	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

6.7. Administer Routing Policies

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

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

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

Routing Policy Details [Commit] [Cancel]

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Communication Manager	10.10.3.44	CM	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

The following screen shows the routing policy for Avaya SBCE for the M-net Premium SIP trunk.

Routing Policy Details [Commit] [Cancel]

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya_SBCE	10.10.3.30	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

6.8. Administer Dial Patterns

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

Under **General**:

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

Under **Originating Locations and Routing Policies**:

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

The following screen shows an example dial pattern configured from the Avaya SBCE to the M-net Premium SIP Trunk.

Dial Pattern Details

CommitCancel

Help ?

General

* Pattern: 00353

* Min: 6

* Max: 16

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

AddRemove

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"/>	SMGR_8		to_Avaya_SBCE	1	<input type="checkbox"/>	Avaya_SBCE	

Select : All, None

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

Dial Pattern Details

CommitCancel

Help ?

General

* Pattern: +4989

* Min: 5

* Max: 15

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

AddRemove

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"/>	SMGR_8		to_Communication_Manager	0	<input type="checkbox"/>	Communication Manager	

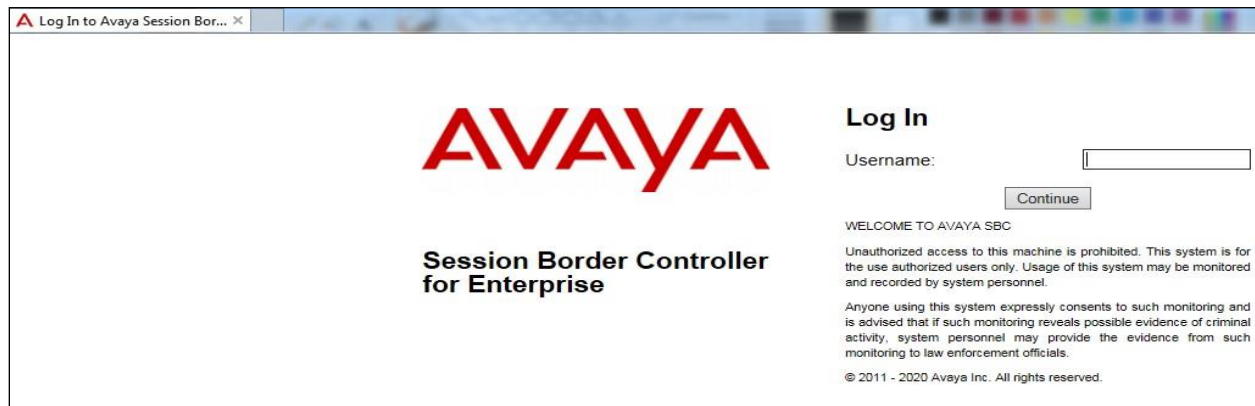
Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

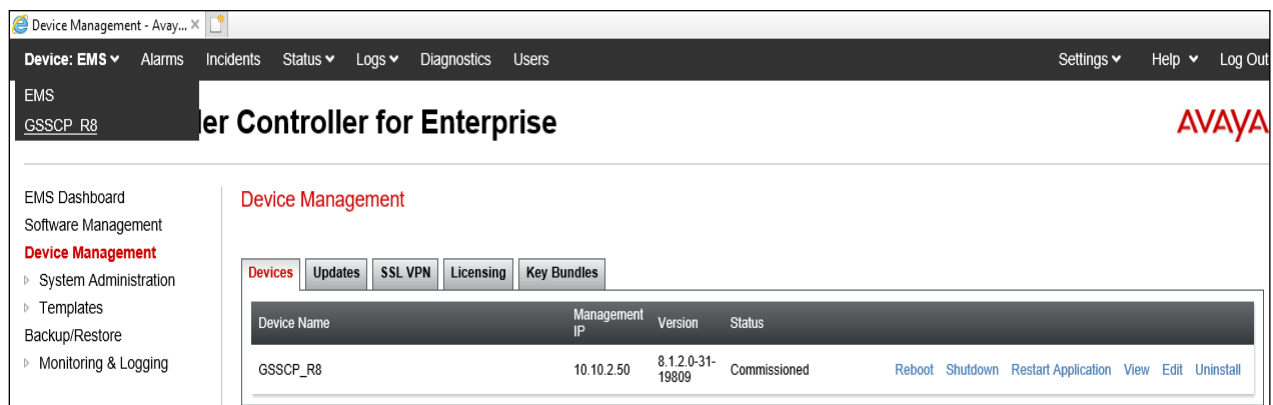
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP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

7.1. Access Avaya Session Border Controller for Enterprise

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



Once logged in, on the top-left of the screen, under **Device:** select the required device from the drop-down menu. with a menu on the left-hand side. In this case, **GSSCP_R8** is used as a starting point for all configuration of the Avaya SBCE.



To view system information that was configured during installation, navigate to **Device Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP_R8** is shown. To view the configuration of this device, click **View** (the third option from the right).

Device Management - Avaya... X

Device: GSSCP_R8 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging

Device Management

Devices Updates SSL VPN Licensing Key Bundles License Compliance

Device Name	Management IP	Version	Status	
GSSCP_R8	10.10.2.50	8.1.2.0-31-19809	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

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

System Information: GSSCP_R8 X

General Configuration

Appliance Name: GSSCP_R8
Box Type: SIP
Deployment Mode: Proxy

Device Configuration

HA Mode: No
Two Bypass Mode: No

License Allocation

Standard Sessions Requested: 0
Advanced Sessions Requested: 0
Scopia Video Sessions Requested: 0
CES Sessions Requested: 0
Transcoding Sessions Requested: 0
Premium Sessions Requested: 0
CLID: ---
Encryption Available: Yes ☒

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.10.3.30	10.10.3.30	255.255.255.0	10.10.3.1	A1
192.168.122.52	192.168.122.52	255.255.255.128	192.168.122.9	B1

DNS Configuration

Primary DNS: 8.8.8.8
Secondary DNS:
DNS Location: DMZ
DNS Client IP: 192.168.122.52

Management IP(s)

IP #1 (IPv4): 10.10.2.50

7.2. Define Network Management

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one physical interface assigned.

To define the network information, navigate to **Network & Flows → Network Management** in the main menu on the left-hand side and click on **Add**. 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 **Network Prefix or 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.

The screenshot shows a 'Network' dialog box with a warning banner at the top: 'Modifications to the interfaces and IP addresses are service impacting and take effect immediately. If changes are made, sessions using this network will be dropped.' Below the banner, the following fields are filled: 'Name' is 'B1_External', 'Default Gateway' is '192.168.122.9', 'Network Prefix or Subnet Mask' is '255.255.255.128', and 'Interface' is 'B1'. An 'Add' button is to the right. Below these fields is a table with three columns: 'IP Address', 'Public IP', and 'Gateway Override'. The 'IP Address' column contains '192.168.122.52', 'Public IP' contains 'Use IP Address', and 'Gateway Override' contains 'Use Default'. A 'Delete' button is to the right of the table. At the bottom is a 'Finish' button.

IP Address	Public IP	Gateway Override
192.168.122.52	Use IP Address	Use Default

Click on **Add** to define the internal interfaces or Edit if it was defined during installation of the Avaya SBCE. Enter details in the dialogue box:

- 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 **Network Prefix or 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 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.

Network X

Modifications to the interfaces and IP addresses are service impacting and take effect immediately. If changes are made, sessions using this network will be dropped.

Name: A1_Internal x

Default Gateway: 10.10.3.1

Network Prefix or Subnet Mask: 255.255.255.0

Interface: A1 v

Add

IP Address	Public IP	Gateway Override
10.10.3.30	Use IP Address	Use Default

Delete

Finish

The following screenshot shows the completed Network Management configuration:

Network Management

Interfaces Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
A1_Internal	10.10.3.1	255.255.255.0	A1	10.10.3.30	Edit	Delete
B1_External	192.168.122.9	255.255.255.128	B1	192.168.122.52	Edit	Delete

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



Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- Click on **Device Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

A status box will appear that will indicate when the restart is complete.

7.3. Define TLS Profiles

For the compliance test, TLS transport is used for signalling on the SIP trunk between Session Manager and the Avaya SBCE. Compliance testing was done using identity certificates signed by a local certificate authority. The generation and installation of these certificates are beyond the scope of these Application Notes.

The following procedures show how to view the certificates and configure the Client and Server profiles to support the TLS connection.

7.3.1. Certificates

To view the certificates currently installed on the Avaya SBCE, navigate to **TLS Management** → **Certificates**:

- Verify that an Avaya SBCE identity certificate (**asbce40int.pem**) is present under **Installed Certificates**.
- Verify that certificate authority root certificate (**SystemManagerCA.pem**) is present under **Installed CA certificates**.
- Verify that private key associated with the identity certificate (**asbce40int.key**) is present under **Installed Keys**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar contains a navigation menu with the following items: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (selected), Certificates (highlighted), Client Profiles, Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled "Certificates" and includes "Install" and "Generate CSR" buttons. It is divided into five sections: "Installed Certificates" showing "asbce40int.pem" with "View" and "Delete" links; "Installed CA Certificates" showing "SystemManagerCA.pem" with "View" and "Delete" links; "Installed Certificate Revocation Lists" with a message "No certificate revocation lists have been installed."; "Installed Certificate Signing Requests" with a message "No certificate signing requests have been installed."; and "Installed Keys" showing "asbce40int.key" with a "Delete" link.

7.3.2. Client Profile

To create a new client profile, navigate to **TLS Management** → **Client Profile** in the left pane and click **Add** (not shown).

- Set **Profile Name** to a descriptive name. **GSSCP_Client** was used in the compliance testing.
- Set **Certificate** to the identity certificate **asbce40int.pem** used in the compliance testing.
- **Peer Verification** is automatically set to **Required**.
- Set **Peer Certificate Authorities** to the **SystemManagerCA.pem** identity certificate.
- Set **Verification Depth** to **1**.

Click **Next** to accept default values for the next screen and click **Finish** (not shown).

Client Profiles: GSSCP_Client

Add Delete

Client Profiles

- GSSCP_Client
- Mnet_Client

Click here to add a description.

Client Profile

TLS Profile

Profile Name	GSSCP_Client
Certificate	asbce40.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	SystemManagerCA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters

Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options

Version	<input checked="" type="checkbox"/> TLS 1.2 <input checked="" type="checkbox"/> TLS 1.1 <input checked="" type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

7.3.3. Server Profile

To create a new server profile, navigate to **TLS Management** → **Server Profile** in the left pane and click **Add** (not shown).

- Set **Profile Name** to a descriptive name. **GSSCP_Server** was used in the compliance testing
- Set **Certificate** to the identity certificate **asbce40int.pem** used in the compliance testing.
- Set **Peer Verification** to **Optional**.

Click **Next** to accept default values for the next screen and click **Finish** (not shown).

Server Profiles: GSSCP_Server

AddDelete

Server Profiles

Mnet_Server

GSSCP_Server

Click here to add a description.

Server Profile

TLS Profile

Profile Name

GSSCP_Server

Certificate

asbce40.pem

SNI Options

None

Certificate Verification

Peer Verification

Optional

Peer Certificate Authorities

Peer Certificate Revocation Lists

Verification Depth

1

Extended Hostname Verification

☐

Renegotiation Parameters

Renegotiation Time

0

Renegotiation Byte Count

0

Handshake Options

Version

☒ TLS 1.2 ☒ TLS 1.1 ☒ TLS 1.0

Ciphers

☒ Default ☐ FIPS ☐ Custom

Value

HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

Note: Please contact a M-net representative to obtain the necessary security certificates and installation information about applying certs to the Avaya SBCE. During compliance testing, test certificates were issued by M-net in order to encrypt the SIP trunk connection between the Avaya and M-net SIP platforms. The Client and Server Profiles details created with the M-net test certs are detailed in the screen shots below.

The following screen shows the Client Profile configured for M-net.

Client Profiles: Mnet_Client

Add

Delete

Client Profiles

GSSCP_Client

Mnet_Client

Click here to add a description.

Client Profile

TLS Profile

Profile Name

Mnet_Client

Certificate

asbce40.pem

SNI

☐ Enabled

Certificate Verification

Peer Verification

Required

Peer Certificate Authorities

SystemManagerCA.pem
mnet_CA.crt
mnet_INT.crt

Peer Certificate Revocation Lists

Verification Depth

2

Extended Hostname Verification

☐

Renegotiation Parameters

Renegotiation Time

0

Renegotiation Byte Count

0

Handshake Options

Version

☒ TLS 1.2 ☒ TLS 1.1 ☐ TLS 1.0

Ciphers

☒ Default ☐ FIPS ☐ Custom

Value

HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

The following screen shows the Server Profile configured for M-net.

Server Profiles: Mnet_Server

Add

Delete

Server Profiles

Mnet_Server

GSSCP_Server

Click here to add a description.

Server Profile

TLS Profile

Profile Name

Mnet_Server

Certificate

asbce40.pem

SNI Options

None

Certificate Verification

Peer Verification

None

Extended Hostname Verification

☐

Renegotiation Parameters

Renegotiation Time

0

Renegotiation Byte Count

0

Handshake Options

Version

☒ TLS 1.2 ☒ TLS 1.1 ☒ TLS 1.0

Ciphers

☒ Default ☐ FIPS ☐ Custom

Value

HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

7.4. Define Interfaces

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

7.4.1. Signalling Interfaces

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

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

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- For **Signaling IP**, select the **A1_Internal** signalling interface IP addresses defined in **Section 7.2**.
- Select **TLS** port number, **5061** is used for Session Manager.
- Select a **TLS Profile** defined in **Section 7.3.3** from the drop-down menu.
- Click **Finish**.

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

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **Signaling IP**, select the **B1_external** signalling interface IP address defined in **Section 7.2**.
- Select **TLS** port number, **5061** is used for the M-net Premium SIP Trunk.
- Select a **TLS Profile** defined in **Section 7.3.3** from the drop-down menu.
- Click **Finish**.

Signaling Interface					
Signaling Interface					
Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile
Sig_Int	10.10.3.30 A1_Internal (A1, VLAN 0)	5060	---	5061	GSSCP_Server
Sig_Ext	192.168.122.52 B1_External (B1, VLAN 0)	5060	---	5061	Mnet_Server

7.4.2. Media Interfaces

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

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

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select the **A1_Internal** media interface IP address defined in **Section 7.2**.
- For **Port Range**, enter **35000-40000**.
- Click **Finish**.

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

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **Media IP**, select the **B1_External** media interface IP address defined in **Section 7.2**.
- Select **Port Range**, enter **35000-40000**.
- Click **Finish**.

Media Interface

Media Interface

Add

Name	Media IP Network	Port Range	
Med_Int	10.10.3.30 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
Med_Ext	192.168.122.52 B1_External (B1, VLAN 0)	35000 - 40000	Edit Delete

7.5. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, M-net is connected as the Trunk Server and Session Manager is connected as the Call Server.

7.5.1. Server Interworking Avaya

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

→ **Server Interworking** and click on **Add**.

- Enter profile name such as Avaya and click **Next** (Not Shown).
- Check **Hold Support** = **None**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

The screenshot shows a configuration window titled "Profile: Avaya". The "General" tab is selected. The configuration options are as follows:

Option	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly <input type="radio"/> Microsoft Teams
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
SIPS Required	<input type="checkbox"/>

On the **Advanced** Tab:

- Check **Record Routes = Both Sides**.
- Ensure **Extensions = Avaya**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

The screenshot shows a configuration window titled "Profile: Avaya" with a close button (X) in the top right corner. The window is divided into two main sections. The top section contains various configuration options with their current values: "Record Routes" is set to "Both Sides" (selected with a radio button); "Include End Point IP for Context Lookup" is checked; "Extensions" is set to "Avaya" (shown in a dropdown menu); "Diversion Manipulation" is unchecked; "Diversion Condition" is set to "None" (shown in a dropdown menu); "Diversion Header URI" is an empty text field; "Has Remote SBC" is checked; "Route Response on Via Port" is unchecked; "Relay INVITE Replace for SIPREC" is unchecked; "MOBX Re-INVITE Handling" is unchecked; and "NATing for 301/302 Redirection" is unchecked. The bottom section is titled "DTMF" and contains "DTMF Support" options: "None>" is selected (radio button), and other options include "SIP Notify>", "RFC 2833 Relay & SIP Notify>", "SIP Info>", "RFC 2833 Relay & SIP Info>", and "Inband>". At the bottom of the window is a "Finish" button.

Setting	Value
Record Routes	Both Sides
Include End Point IP for Context Lookup	Checked
Extensions	Avaya
Diversion Manipulation	Unchecked
Diversion Condition	None
Diversion Header URI	
Has Remote SBC	Checked
Route Response on Via Port	Unchecked
Relay INVITE Replace for SIPREC	Unchecked
MOBX Re-INVITE Handling	Unchecked
NATing for 301/302 Redirection	Unchecked
DTMF	
DTMF Support	None>

Finish

7.5.2. Server Interworking – M-net

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

- Enter profile name such as **M-net** and click **Next** (Not Shown).
- Check **Hold Support** = **None**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

The screenshot shows the 'Profile: Mnet' configuration window with the 'General' tab selected. The window has a title bar with 'Profile: Mnet' and a close button 'X'. The 'General' tab is highlighted. The configuration options are as follows:

Option	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3284 - a=sendonly <input type="radio"/> Microsoft Teams
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None (dropdown)
Send Hold	<input type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3281 <input type="radio"/> RFC2543
SIPS Required	<input type="checkbox"/>

On the **Advanced** Tab:

- Check **Record Routes = Both Sides**.
- Ensure **Extensions = None**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

The screenshot shows a configuration window titled "Profile: Mnet" with a close button (X) in the top right corner. The window is divided into two main sections: "Record Routes" and "DTMF".

Record Routes Section:

- Record Routes:** A radio button group with five options: "None", "Single Side", "Both Sides" (selected), "Dialog-Initiate Only (Single Side)", and "Dialog-Initiate Only (Both Sides)".
- Include End Point IP for Context Lookup:** A checkbox that is checked.
- Extensions:** A dropdown menu set to "None".
- Diversion Manipulation:** A checkbox that is unchecked.
- Diversion Condition:** A dropdown menu set to "None".
- Diversion Header URI:** An empty text input field.
- Has Remote SBC:** A checkbox that is checked.
- Route Response on Via Port:** A checkbox that is unchecked.
- Relay INVITE Replace for SIPREC:** A checkbox that is unchecked.
- MOBX Re-INVITE Handling:** A checkbox that is unchecked.
- NATing for 301/302 Redirection:** A checkbox that is unchecked.

DTMF Section:

The "DTMF" section is separated by a dark header bar. It contains a radio button group for "DTMF Support" with six options: "None>" (selected), "SIP Notify>", "RFC 2833 Relay & SIP Notify>", "SIP Info>", "RFC 2833 Relay & SIP Info>", and "Inband>".

At the bottom of the window is a "Finish" button.

7.6. Define Servers

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

7.6.1. Server Configuration – Avaya

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

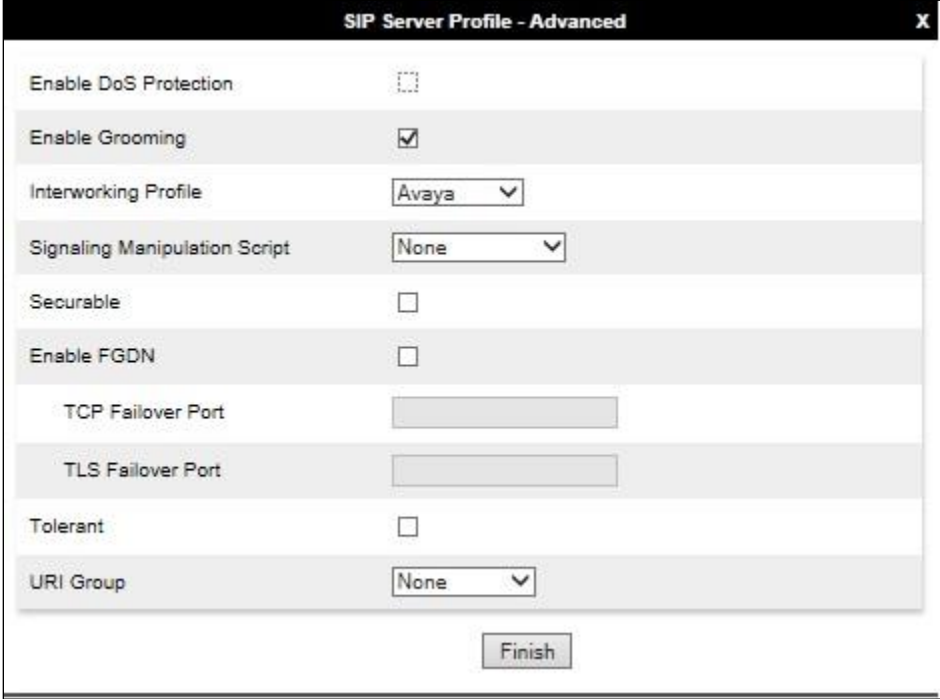
- Select **Server Type** to be **Call Server**.
- Select **TLS Client Profile** to be **GSSCP_Client** as defined in **Section 7.3.2**.
- Enter **IP Address / FQDN** to **10.10.3.42** (Session Manager IP Address).
- For **Port**, enter **5061**.
- For **Transport**, select **TLS**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

The screenshot shows the 'SIP Server Profile - General' configuration window. At the top, a blue banner states: 'Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.' Below this, the 'Server Type' is set to 'Call Server'. The 'SIP Domain' field is empty. The 'DNS Query Type' is set to 'NONE/A'. The 'TLS Client Profile' is set to 'GSSCP_Client'. An 'Add' button is located to the right of these fields. Below the main configuration area is a table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'. The first row contains the values '10.10.3.42', '5061', and 'TLS'. A 'Delete' button is located to the right of the table.

IP Address / FQDN	Port	Transport
10.10.3.42	5061	TLS

On the **Advanced** tab:

- Check **Enable Grooming**.
- Select **Avaya** for **Interworking Profile**.
- Click **Finish**.



The screenshot shows a configuration window titled "SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains several settings:

Setting	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None

At the bottom right of the window is a "Finish" button.

7.6.2. Server Configuration – M-net

To define the M-net Trunk Server, navigate to **Services → SIP Servers** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Trunk Server**.
- Set **DNS Query Type** to **SRV**.
- Select **TLS Client Profile** to be **Mnet_Client** defined for M-net.
- Enter **IP Address / FQDN** to **business.mnet-voip.de** (M-net SIP Platform).
- For **Transport**, select **TLS**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

The screenshot shows the 'SIP Server Profile - General' configuration window. At the top, a blue banner states: 'Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.' Below this, there are four configuration fields: 'Server Type' is set to 'Trunk Server', 'SIP Domain' is empty, 'DNS Query Type' is set to 'SRV', and 'TLS Client Profile' is set to 'Mnet_Client'. An 'Add' button is located to the right of these fields. Below the fields is a table with three columns: 'FQDN', 'Port', and 'Transport'. The first row contains the values 'business.mnet-voip.de', an empty port field, and 'TLS'. A 'Delete' button is located to the right of the table.

FQDN	Port	Transport
business.mnet-voip.de		TLS

In the new Authentication window that appears, enter the following values as M-net require authentication to connect to their network:

- **Enabled Authentication:** Checked
- **User Name:** Enter username provided by the Service Provider.
- **Realm:** Enter realm details provided by the Service Provider or leave blank to be detected by the server challenge.
- **Password** Enter password provided by the Service Provider.
- **Confirm Password** Re-enter password provided by the Service Provider.

Click **Next** to continue (not shown).



The screenshot shows a window titled "SIP Server Profile - Authentication". It contains the following fields and controls:

- Enable Authentication:** A checkbox that is checked.
- User Name:** A text input field containing the value "+4989xxxxxx30".
- Realm:** A text input field with the instruction "(Leave blank to detect from server challenge)".
- Password:** A text input field with the instruction "(Leave blank to keep existing password)".
- Confirm Password:** An empty text input field.

In the new Registration window that appears, enter the following values.

- **Register with Priority Server:** Check.
- **Refresh Interval** Choose the desired frequency in seconds the Avaya SBCE will send SIP REGISTERS.
- **From URI:** Enter an URI to be sent in the FROM header for SIP REGISTERS.
+4989xxxxxx30@business.mnet-voip.de was used in the compliance testing.
- **TO URI:** Enter an URI to be sent in the TO header for SIP REGISTERS.
+4989xxxxxx30@business.mnet-voip.de was used in the compliance testing.

Click **Next** to continue (not shown).

SIP Server Profile - Registration	
Register with All Servers	<input type="checkbox"/>
Register with Priority Server	<input checked="" type="checkbox"/>
Refresh Interval	90 seconds
From URI	+4989xxxxxx30@busin
To URI	+4989xxxxxx30@busin

On the Advanced tab:

- Select **Mnet** for **Interworking Profile**.
- Check **Enable Grooming**.
- Click **Finish**.

SIP Server Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Mnet
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>
<input type="button" value="Finish"/>	

7.7. Routing

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

Routing information is required for routing to Session Manager on the internal side and M-net address on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

7.7.1. Routing – Avaya

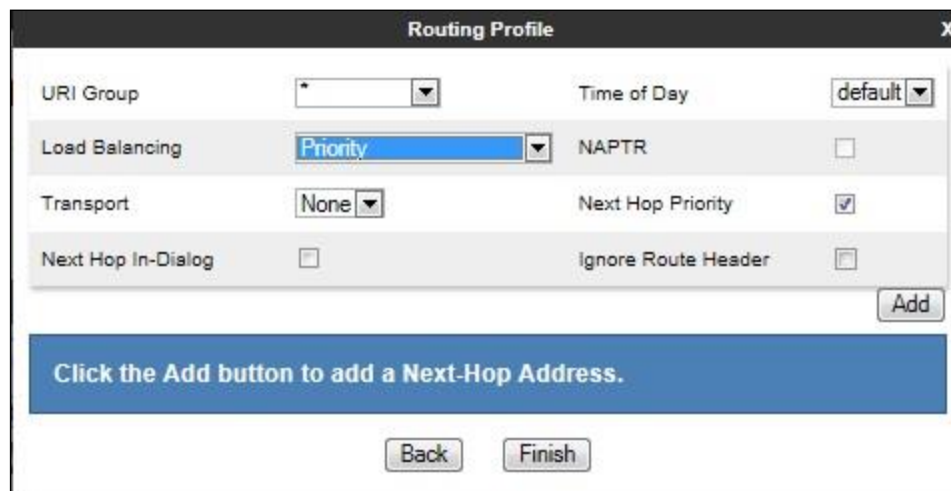
Create a Routing Profile for Session Manager.

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



The image shows a 'Routing Profile' window. It has a title bar with 'Routing Profile' and a close button 'X'. Inside, there is a text field labeled 'Profile Name' with the value 'Avaya' entered. Below the text field is a 'Next' button.

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



The image shows a 'Routing Profile' window with various settings. The title bar has 'Routing Profile' and a close button 'X'. The settings are as follows:

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

Below the settings is an 'Add' button. At the bottom, there is a blue banner with the text 'Click the Add button to add a Next-Hop Address.' and two buttons: 'Back' and 'Finish'.

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

- **Priority/Weight = 1.**
- **SIP Server Profile = Avaya (Section 7.6.1)** from drop down menu.
- **Next Hop Address = Select 10.10.3.42:5061 (TLS)** from drop down menu.
- Click **Finish**.

The screenshot shows the 'Profile : Avaya' configuration window. The settings are as follows:

- URI Group: *
- Time of Day: default
- Load Balancing: Priority
- NAPTR: ☐
- Transport: None
- LDAP Routing: ☐
- LDAP Server Profile: None
- LDAP Base DN (Search): None
- Matched Attribute Priority: ☐
- Alternate Routing: ☐
- Next Hop Priority: ☒
- Next Hop In-Dialog: ☐
- Ignore Route Header: ☐
- ENUM: ☐
- ENUM Suffix:

At the bottom, there is a table with the following data:

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Avaya	10.10.3.42:5061 (TLS)	None	Delete

The 'Finish' button is located at the bottom center of the window.

7.7.2. Routing – M-net

Create a Routing Profile for M-net SIP network.

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

The screenshot shows the 'Routing Profile' configuration window. The 'Profile Name' field contains the text 'M-Net'. The 'Next' button is located at the bottom center of the window.

The Routing Profile window will open. The **Load Balancing** parameter is set to **DNS/SRV**. Use the default values displayed for other fields and click **Add**.

Add Routing Rule

URI Group	*	Time of Day	default
Load Balancing	DNS/SRV	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input checked="" type="checkbox"/>	Alternate Routing	<input checked="" type="checkbox"/>
Next Hop Priority	<input type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Click the Add button to add a Next-Hop Address.

Finish

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

- **SIP Server Profile** = **Mnet** (Section 7.6.2) from drop down menu.
- **Next Hop Address** = Select **business.mnet-voip.de (TLS)** from drop down menu.
- Click **Finish**.

Profile : Mnet

URI Group	*	Time of Day	default
Load Balancing	DNS/SRV	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
0				Mnet	business.mnet-voip.de (TLS)	None	Delete

Finish

7.8. Topology Hiding

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

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

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

Topology Hiding Profiles: Avaya

Add

RenameCloneDelete

Topology Hiding Profiles

default

cisco_th_profile

Avaya

Mnet

Click here to add a description.

Topology Hiding

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

Edit

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

- In the **Profile Name** field enter a descriptive name for M-net and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for, **From**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **business.mnet-voip.de**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Mnet

Buttons: Add, Rename, Clone, Delete

Topology Hiding Profiles: default, cisco_th_profile, Avaya, **Mnet**

Click here to add a description.

Topology Hiding

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

Edit

7.9. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

In the reference configuration, only new Media and Signalling rules were defined. All other rules under Domain Policies, linked together on End Point Policy Groups later in this section, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one of the defaults and then make the necessary changes to the new rule.

7.9.1. Media Rules

A media rule defines the processing to be applied to the selected media. For the compliance test, media rules were created for both Session Manager and M-net to use SRTP.

To define the Media Rule for Session Manager, navigate to **Domain Policies** → **Media Rules** in the main menu on the left-hand side. Click on **Add** and enter details in the Media Rule pop-up box (not shown)

- In the **Rule Name** field enter a descriptive name such as **Avaya_SRTP**.
- Set **Preferred Format #1** to **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Set **Preferred Format #2** to **RTP**.
- Uncheck **Encrypted RTCP**.
- Check **Capability Negotiation** under **Miscellaneous** (not shown).

Default values were used for all other fields. Click **Finish** (not shown).

The screenshot shows the 'Media Rules: Avaya_SRTP' configuration window. On the left is a sidebar with a list of media rules: 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', and 'Avaya_SRTP' (which is highlighted in red). Above this list is an 'Add' button. The main area of the window has a title bar with 'Rename', 'Clone', and 'Delete' buttons. Below the title bar is a blue bar with the text 'Click here to add a description.' Underneath this are four tabs: 'Encryption' (selected), 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab contains two sections: 'Audio Encryption' and 'Video Encryption'. The 'Audio Encryption' section has the following fields: 'Preferred Formats' (set to 'SRTP_AES_CM_128_HMAC_SHA1_80' and 'RTP'), 'SRTP Context Reset on SSRC Change' (unchecked), 'Encrypted RTCP' (unchecked), 'MKI' (unchecked), 'Lifetime' (set to 'Any'), and 'Interworking' (unchecked). The 'Video Encryption' section has the following fields: 'Preferred Formats' (set to 'RTP') and 'Interworking' (unchecked).

To define the Media Rule for M-net, navigate to **Domain Policies → Media Rules** in the main menu on the left-hand side. Click on **Add** and enter details in the Media Rule pop-up box (not shown)

- In the **Rule Name** field enter a descriptive name such as **Mnet_SRTP**.
- Set **Preferred Format #1** to **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Check **Encrypted RTCP**.
- Check **Capability Negotiation** under **Miscellaneous**.

Default values were used for all other fields. Click **Finish** (not shown).

Media Rules: Mnet_SRTP

Add

Media Rules

default-low-med

default-low-med-enc

default-high

default-high-enc

avaya-low-med-enc

Avaya_SRTP

Mnet_SRTP

RenameCloneDelete

Click here to add a description.

Encryption

Codec Prioritization

Advanced

QoS

Audio Encryption

Preferred FormatsSRTP_AES_CM_128_HMAC_SHA1_80

Encrypted RTCP☒

MKI☐

LifetimeAny

Interworking☒

Symmetric Context Reset☒

Key Change in New Offer☐

Video Encryption

Preferred FormatsRTP

Interworking☐

Symmetric Context Reset☒

Key Change in New Offer☐

Miscellaneous

Capability Negotiation☒

Edit

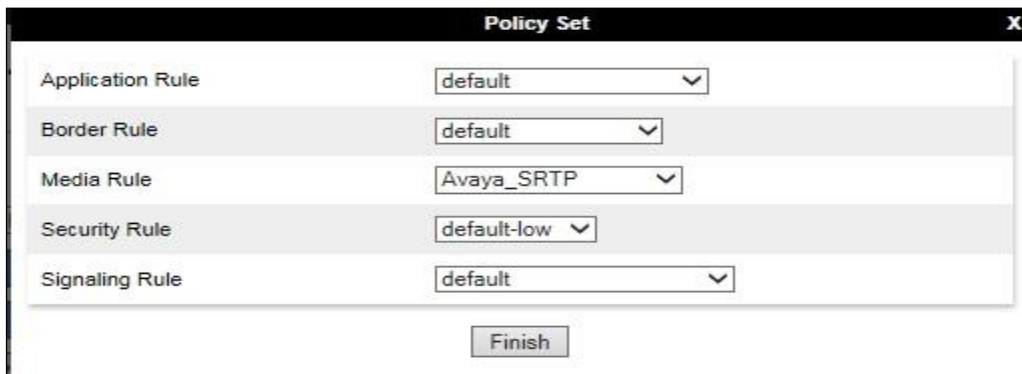
7.10. End Point Policy Groups

An end point policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, one end point policy group must be created for Session Manager and another for the M-net SIP trunk. The end point policy group is applied to the traffic as part of the end point flow defined in **Section 7.11**.

7.10.1. End Point Policy Group – Session Manager

To define an End Point policy for Session Manager, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left-hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

- In the **Group Name** field enter a descriptive name, in this case **Avaya**, and click **Next** (not shown).
- Leave the **Application Rule**, **Border Rule**, **Security Rule** and **Signalling Rule** fields at their default values.
- In the **Media Rule** drop down menu, select the recently added Media Rule called **Avaya_SRTP**.
- Click **Finish**.



The screenshot shows a 'Policy Set' dialog box with a close button (X) in the top right corner. It contains five rows of configuration options, each with a label and a dropdown menu:

Label	Value
Application Rule	default
Border Rule	default
Media Rule	Avaya_SRTP
Security Rule	default-low
Signaling Rule	default

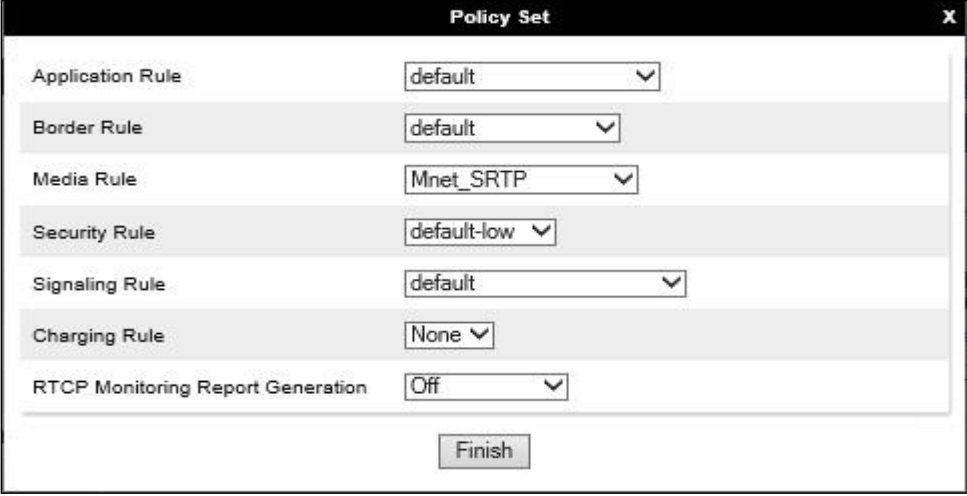
At the bottom center of the dialog box is a 'Finish' button.

7.10.2. End Point Policy Group – M-net

To define an End Point policy for M-net, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left-hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

- In the **Group Name** field enter a descriptive name, in this case **Avaya**, and click **Next** (not shown).
- Leave the **Application Rule**, **Border Rule**, **Security Rule** and **Signalling Rule** fields at their default values.
- In the **Media Rule** drop down menu, select the recently added Media Rule called **Mnet_SRTP**.

Click **Finish**.



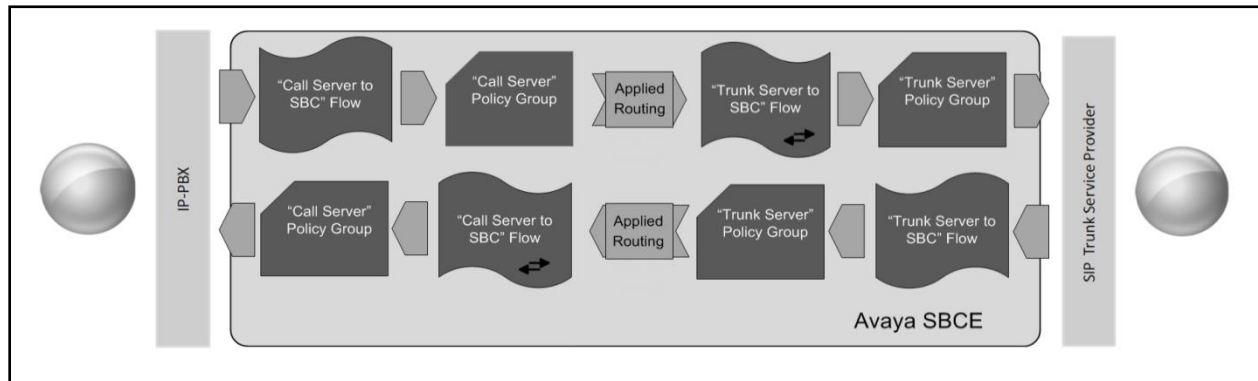
The screenshot shows a 'Policy Set' dialog box with the following configuration:

Field	Value
Application Rule	default
Border Rule	default
Media Rule	Mnet_SRTP
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

At the bottom of the dialog is a 'Finish' button.

7.11. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to M-net's SIP Trunk and incoming flows from M-net's SIP Trunk to Session Manager. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



This configuration ties all the previously entered information together so that calls can be routed from Session Manager to M-net SIP Trunk and vice versa. The following screenshot shows all configured flows.

End Point Flows

Subscriber Flows **Server Flows** Add

Modifications made to a Server Flow will only take effect on new sessions.

Hover over a row to see its description.

SIP Server: Avaya						
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	Call_Server	*	Sig_Ext	Sig_Int	Avaya	Eir View Clone Edit Delete

SIP Server: Eir						
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	Trunk_Server	*	Sig_Int	Sig_Ext	default-low	Avaya View Clone Edit Delete

To define a Server Flow for the M-net Premium SIP Trunk, navigate to **Network & Flows** → **End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for M-net SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the M-net server configuration defined in **Section 7.7.2**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**.
- Set the **End Point Policy Group** to the endpoint policy group **Mnet**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.7.1**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the M-net SIP Trunk defined in **Section 7.8** and click **Finish** (not shown).

The screenshot shows a configuration window titled "Flow: Trunk_Server". It contains two main sections: "Criteria" and "Profile".

Criteria	
Flow Name	Trunk_Server
Server Configuration	Mnet
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Int

Profile	
Signaling Interface	Sig_Ext
Media Interface	Media_Ext
Secondary Media Interface	None
End Point Policy Group	Mnet
Routing Profile	Avaya
Topology Hiding Profile	Mnet
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

To define an incoming server flow for Session Manager from the M-net network, navigate to **Network & Flows → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **Call_Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 7.7.1**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**.
- Set the **End Point Policy Group** to the endpoint policy group **Avaya**.
- In the **Routing Profile** drop-down menu, select the routing profile of the M-net SIP Trunk defined in **Section 7.7.2**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.8** and click **Finish** (not shown).

The screenshot shows a configuration window titled "Flow: Call_Server" with a close button (X) in the top right corner. The window is divided into two main sections: "Criteria" and "Profile".

Criteria Section:

Flow Name	Call_Server
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Ext

Profile Section:

Signaling Interface	Sig_Int
Media Interface	Media_Int
Secondary Media Interface	None
End Point Policy Group	Avaya
Routing Profile	Mnet
Topology Hiding Profile	Avaya
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

8. M-net Premium SIP Trunk Configuration

The configuration of the M-net equipment used to support M-net's SIP Trunk is outside of 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 as listed in [Section 2.3](#).

9. Verification Steps

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

1. From System Manager **Home** tab click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entities from the list and observe if the **Conn Status** and **Link Status** are showing as **UP**.

Session Manager Entity Link Connection Status									
This page displays detailed connection status for all entity links from a Session Manager.									
Status Details for the selected Session Manager: Time Last Down: 12/09/19 11:10:34 Last Message Sent: 12/10/19 10:44:38 Time Last Up: 12/09/19 11:25:56 Last Response Latency (ms): 21									
All Entity Links for Session Manager: Session Manager									
Summary View									
4 Items Filter: Enable									
	SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	Avaya SBCE	IPv4	10.10.3.30	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Communication Manager	IPv4	10.10.3.44	5061	TLS	FALSE	UP	200 OK	UP

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

status trunk 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

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.

10. Conclusion

These Application Notes describe the configuration necessary to successfully connect Avaya Aura ® Communication Manager R8.1, Avaya Aura ® Session Manager 8.1 and Avaya Session Border Controller for Enterprise R8.1 to the M-net Premium SIP platform.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and demonstrates Avaya Aura ® Communication Manager R8.1, Avaya Aura ® Session Manager 8.1 with Avaya Session Border Controller for Enterprise can be configured to interoperate successfully with M-net Premium SIP Trunk Service. The M-net Premium SIP Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. Additional References

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

- [1] *Deploying Avaya Appliance Virtualization Platform*, Release 8.1, Mar 2021.
- [2] *Upgrading Avaya Aura® applications*, Release 8.1, Mar 2021.
- [3] *Deploying Avaya Aura® applications from System Manager*, Release 8.1, Mar 2021.
- [4] *Deploying Avaya Aura® Communication Manager*, Release 8.1, Mar 2021.
- [5] *Administering Avaya Aura® Communication Manager*, Release 8.1, Mar 2021.
- [6] *Upgrading Avaya Aura® Communication Manager*, Release 8.1, Mar 2021.
- [7] *Deploying Avaya Aura® System Manager Release 8.1*, Mar 2021.
- [8] *Upgrading Avaya Aura® System Manager to Release 8.1*, Mar 2021.
- [9] *Administering Avaya Aura® System Manager for Release 8.1*, Mar 2021.
- [10] *Deploying Avaya Aura® Session Manager*, Release 8.1 Mar 2021.
- [11] *Upgrading Avaya Aura® Session Manager Release 8.1*, Mar 2021.
- [12] *Administering Avaya Aura® Session Manager Release 8.1*, Mar 2021.
- [13] *Deploying Avaya Session Border Controller for Enterprise Release 8.1*, Dec 2020.
- [14] *Upgrading Avaya Session Border Controller for Enterprise Release 8.1*, Dec 2020.
- [15] *Administering Avaya Session Border Controller for Enterprise Release 8.1*, Dec 2020.
- [16] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise 8.1 on the Avaya Aura® Platform*, Feb 2021.
- [17] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2022 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.