



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura ® Communication Manager R10.1, Avaya Aura ® Session Manager R10.1 and Avaya Session Border Controller for Enterprise R10.1 to support Tele2 SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Tele2 SIP Trunk Service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Aura® Communication Manager R10.1, Avaya Aura® Session Manager R10.1 and Avaya Session Border Controller for Enterprise R10.1.

The Tele2 SIP Platform provides PSTN access via a SIP trunk connected to the Tele2 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.

Tele2 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.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	5
2.3.	Support	6
3.	Reference Configuration	7
4.	Equipment and Software Validated	8
5.	Configure Avaya Aura® Communication Manager	9
5.1.	Confirm System Features	9
5.2.	Administer IP Node Names.....	10
5.3.	Administer IP Network Region.....	11
5.4.	Administer IP Codec Set	12
5.5.	Administer SIP Signaling Groups	13
5.6.	Administer SIP Trunk Groups.....	14
5.7.	Administer Calling Party Number Information	16
5.8.	Administer Route Selection for Outbound Calls.....	16
5.9.	Administer Incoming Digit Translation	18
5.10.	EC500 Configuration.....	19
6.	Configuring Avaya Aura® Session Manager	20
6.1.	Log in to Avaya Aura® System Manager.....	20
6.2.	Administer SIP Domain	21
6.3.	Administer Locations	22
6.4.	Administer Adaptations.....	25
6.5.	Administer SIP Entities	27
6.5.1.	Avaya Aura® Session Manager SIP Entity	28
6.5.2.	Avaya Aura® Communication Manager SIP Entity	29
6.5.3.	Avaya Session Border Controller for Enterprise SIP Entity.....	30
6.6.	Administer Entity Links	31
6.7.	Administer Routing Policies	32
6.8.	Administer Dial Patterns	33
7.	Configure Avaya Session Border Controller for Enterprise	35
7.1.	Access Avaya Session Border Controller for Enterprise	35
7.2.	Define Network Management	37
7.3.	Define TLS Profiles	40
7.3.1.	Certificates	40
7.3.2.	Client Profile	41
7.3.3.	Server Profile	42
7.4.	Define Interfaces	43
7.4.1.	Signalling Interfaces	43
7.4.2.	Media Interfaces.....	44
7.5.	Define Server Interworking.....	45
7.5.1.	Server Interworking Avaya.....	45
7.5.2.	Server Interworking – Tele2	47
7.6.	Signalling Manipulation.....	49

7.7.	Define Servers	51
7.7.1.	Server Configuration – Avaya	51
7.7.2.	Server Configuration – Tele2	53
7.8.	Routing	55
7.8.1.	Routing – Avaya	55
7.8.2.	Routing – Tele2	56
7.9.	Topology Hiding	58
7.10.	Domain Policies	59
7.10.1.	Media Rules	60
7.11.	End Point Policy Groups	61
7.11.1.	End Point Policy Group – Session Manager	61
7.11.2.	End Point Policy Group – Tele2	62
7.12.	Server Flows	63
8.	Tele2 SIP Trunk Configuration	66
9.	Verification Steps	66
10.	Conclusion	68
11.	Additional References	69
12.	Appendix A: SigMa Scripts	70
13.	Appendix B: MEX Testing	71
13.1.1.	Configure Session Manager – Dial Pattern	72
13.1.2.	Configure Communication Manager	73
14.	Appendix C: Configure for Special Numbers	77
14.1.	Configure Communication Manager	77
14.2.	Session Manager Adaptation for Special Service Numbers	78
15.	Appendix D: Configure for Service Numbers	80
15.1.	Configure Communication Manager	80
15.2.	Session Manager Adaptation for Service Numbers	81

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Tele2 SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura® Communication Manager R10.1 (Communication Manager); Avaya Aura® Session Manager R10.1 (Session Manager) and Avaya Session Border Controller for Enterprise R10.1 (Avaya SBCE).

Customers using this Avaya SIP-enabled enterprise solution with the Tele2 SIP Trunk 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 Tele2 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.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using the Tele2 SIP Trunk Service, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via the Tele2 SIP Trunk Service to PSTN destinations, calls made from SIP and H.323 telephones.
- Incoming and Outgoing PSTN calls to/from Avaya one-X® Communicator and Avaya Workplace for Windows soft phones.
- Calls using G.711A codec.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using T.38 and G.711 passthrough fax transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Routing inbound vector call to call center agent queues.
- Additional MEX call testing. With Tele2 SIP Trunk, MEX calls from MEX enabled mobile phones are tromboned in the Avaya PBX and returned as normal Business Trunk calls. The MEX implementation relies on IN triggers on the PSTN side which prefixes the called number with a routing number used for routing the call towards the Avaya PBX.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Tele2 SIP Trunking Service with the following observations:

- It was observed when performing Blind Transfer to PSTN numbers on inbound calls (i.e. PSTN (A) -> Avaya (B) -> Blind Transfer -> PSTN (C)) from Avaya SIP handsets, that Tele2 was responding with a “403 Forbidden”. The reason Tele2 was responding with “403 Forbidden” is that the Avaya SIP handsets populate the P-Asserted-Identity Header with the originating caller (A) CLID. Tele2 require the P-Asserted-Identity Header to be populated with the CLID of a known Tele2 number (B) on their SIP platform. In order for Blind Transfers to PSTN to complete successfully, a SigMa script was created on the Avaya SBCE to populate the P-Asserted-Identity Header with a known Tele2 CLID number on the Tele2 SIP platform. The details of the Sigma Script are outlined in **Section 7.6**.
- During the initial configuration of the test environment SIP trunk connection between Avaya and Tele2, it was observed that the Avaya SBCE was responding to OPTIONs from Tele2 with a “483 Too Many Hops” response and thus the trunk failed to establish. It was diagnosed that the Max-Forwards Header within OPTIONs had a value =0. Normally a Service Provider sets a value of Max-Forwards=69. A SigMa script was created to change the Max-Forwards value from 0 to 69 on all inbound OPTIONs from Tele2. The details of the Sigma Script and how to configure the script on the Avaya

SBCE are outlined in **Section 7.6. Note:** Only apply this SigMa script if experiencing the above issue.

- Tele2 sends a cryptic Contact Header (e.g. Contact: [sip:IMZ12hrdsASFH12ASD/r/n](tel:sip:IMZ12hrdsASFH12ASD/r/n)) in its SIP Requests and Responses and is working as design. It was observed when making an outbound call from Avaya H.323 handsets, that the Avaya handset screen displayed the Tele2 cryptic Contact Header information instead of the dialled number information. A Session Manager Adaptation called Orange Adapter needs to be applied the Tele2 Session Manager Adaptation in **Section 6.4**. Orange Adapter modifies how Session Manager generates the P-Asserted-Identity header in a request or a response if it is not present on ingress from Tele2. The default behavior of the Session Manager is overridden and the PAI is generated from the From header in requests and To header in responses so that the Orange Adapter generates a PAI Header from the From Header in Requests and the To Header in responses. With the Orange Adapter applied, the Avaya H.323 handsets displayed the dialled number information instead of the Tele2 cryptic Contact Header information on outbound calls.
- All unwanted Avaya proprietary SIP headers and MIME was stripped on outbound calls using the Adaptation Module in Session Manager.
- Tele2 do not support codec G.729 and therefore was not tested.
- No inbound toll free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.

2.3. Support

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

For technical support on Tele2 products please contact the Tele2 support team:

Telephone National: 90 444

Telephone International: +46 772 23 23 23

Web: <https://www.tele2.se/foretag/support/kontakt>

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Tele2 SIP trunk service. 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 IP telephone (with SIP firmware), Avaya 16xx series IP telephones (with H.323 firmware), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Avaya Workplace for Windows running on laptop PCs.

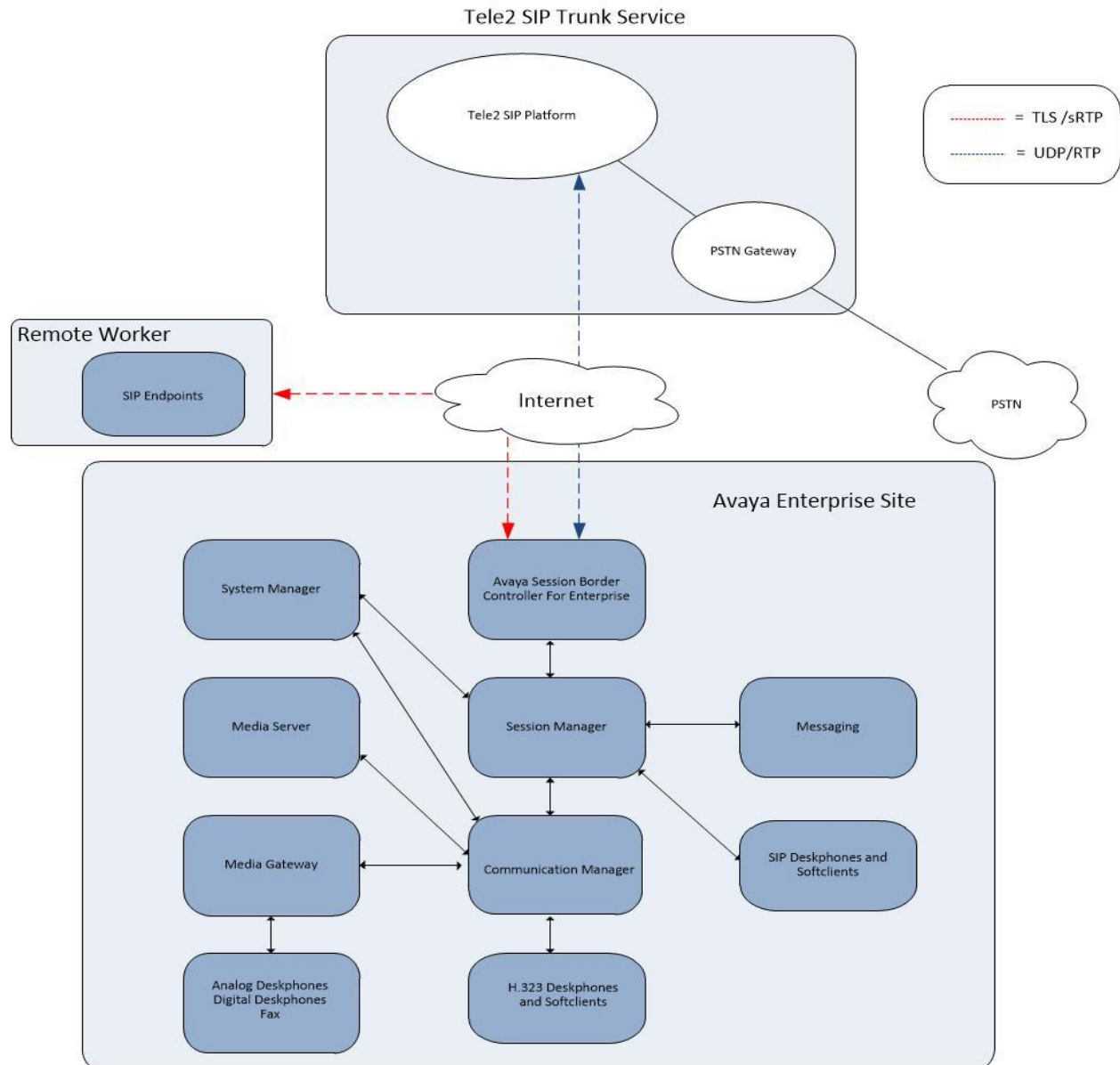


Figure 1: Test Setup Tele2 SIP Trunk Service to Avaya Enterprise

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	10.1.0.0 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.0.0614119
Avaya Aura® Session Manager	10.1.0.0.1010019
Avaya Aura® Communication Manager	10.1 SP1 - 27293
Avaya Session Border Controller for Enterprise	10.1.0.0-32-21432
Avaya G430 Media Gateway	42.4.0
Avaya Aura® Media Server	v.8.0.2.SP9
Avaya Aura® Messaging	7.2 SP3
Avaya 1600 IP Deskphone (H.323)	1.3.12
Avaya 96x1 IP DeskPhone (H.323)	6.8.5
Avaya 9611 IP DeskPhone (SIP)	7.1.15
Avaya 9608 IP DeskPhone (SIP)	7.1.15
Avaya J179 IP Deskphone (SIP)	4.0.11.0
Avaya one-X® Communicator (H.323 & SIP)	6.2.14.15 -SP14-Patch 7
Avaya Workplace for Windows (SIP)	3.23.0.64
Avaya 1408 Digital Telephone	R48
Analogue Handset	N/A.
Analogue Fax	N/A
Tele2 SIP Platform	
Oracle ACME SBC 4600	SCZ8.4.0 Patch 10 (Build 562)
Destiny Telepo UCaaS platform	5.2.20885

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 Tele2 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 Tele2 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 Tele2 SIP Trunking Service and any other SIP trunks used.

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

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

display system-parameters customer-options		Page 5 of 12
OPTIONAL FEATURES		
Emergency Access to Attendant? y		IP Stations? y
Enable 'dadmin' Login? y		
Enhanced Conferencing? y		ISDN Feature Plus? n
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n		ISDN-BRI Trunks? y
Enterprise Wide Licensing? n		ISDN-PRI? y
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? 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 codecs supported by Tele2 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 Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711A	n	2	20

Media Encryption

1: srtplib-aescm128-hmac80
2: none

Encrypted SRTCP: enforce-unenc-srtcp

Tele2 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-standard**.
- Leave **ECM** at default value of **y**.

change ip-codec-set 2 Page 2 of 2

IP MEDIA PARAMETERS

Allow Direct-IP Multimedia? n

FAX	Mode	Redundancy	ECM	Packet Size (ms)
Modem	t.38-standard	0	y	
TDD/TTY	off	0		
H.323 Clear-channel	US	3		
SIP 64K Data	n	0		
				20

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Tele2 SIP Trunking Service. 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-ntwrk**.
- Specify the signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**.
- Specify the **Number of Members** 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	Night Service:	
Dial Access? n			
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 Tele2 to prevent unnecessary SIP messages during call setup. During testing, a value of **180** was used.

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): 180			
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 “+”.

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
	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 **n**.
- Set **Network Call Direction** to **n**.
- Set **Send Diversion Header** to **y**.
- Set **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **101** as requested by Tele2.
- Set **Always Use re-INVITE for Display Updates** to **y**.
- Set the **Identity for Calling Party Display** to **From**.

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? n	
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: From
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					
Total					
Ext	Trk	CPN			
Len	Code	Grp(s)	Prefix	Len	
Total Administered: 4					
4	6102	1	46101xxxxx20	11	
Maximum Entries: 240					
4	6010	1	46101xxxxx21	11	
4	6020	1	46101xxxxx22	11	
4	6104	1	46101xxxxx23	11	
Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.					
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 Tele2 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 **00**. 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	17	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 **intl-pub**.

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				intl-pub				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:	v	v	v	v	v	n	n	rest								none				

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Tele2 can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DDI numbers provided by Tele2 SIP platform correlate to the internal extensions assigned within Communication Manager. The entries displayed below translate incoming DDI numbers **+46101xxxxxx20**, **+46101xxxxxx21**, **+46101xxxxxx22** and **+46101xxxxxx23** to a 4-digit extension by deleting all of the incoming digits and inserting an extension.

change inc-call-handling-trmt trunk-group 1					Page 1 of 3	
INCOMING CALL HANDLING TREATMENT						
Service/ Feature	Number Len	Del	Insert Digits			
public-ntwrk	14		+46101xxxxxx20	all	6102	
public-ntwrk	14		+46101xxxxxx21	all	6010	
public-ntwrk	14		+46101xxxxxx22	all	6020	
public-ntwrk	14		+46101xxxxxx23	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** if required by the routing configuration, none was required during testing.
- For the **Phone Number** enter the phone that will also be called (e.g. **0035389434xxxx**).
- Set the **Trunk Selection** to **ars** so that the ARS table will be used for routing.
- Set the **Config Set** to **1**.

change off-pbx-telephone station-mapping 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

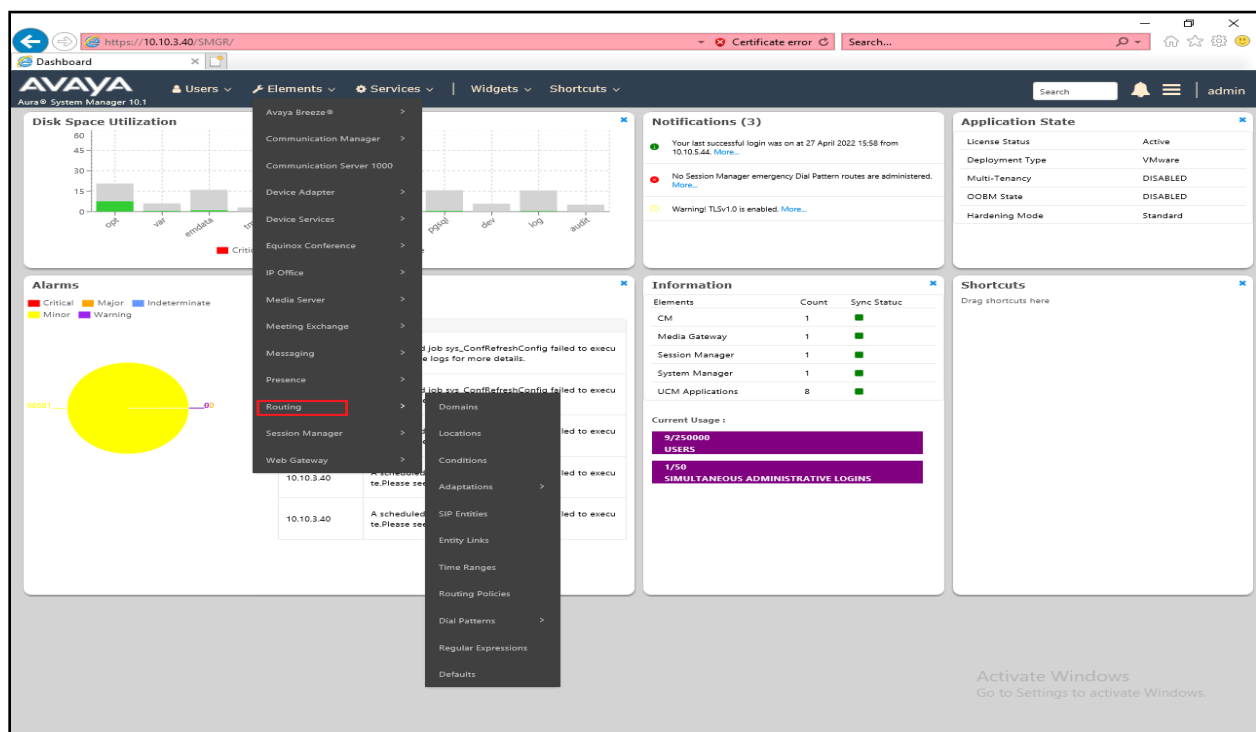
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- 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.

Administration of Session Manager Routing Policies

A Routing Policy consists of routing elements such as "Domains", "Locations", "SIP Entities", etc.

The recommended order of routing element administration (that means the overall routing workflow) is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Conditions" (if Flexible Routing or Regular Expression Adaptations are in use)
- Step 4: Create "Adaptations"
- Step 5: Create "SIP Entities"
 - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
 - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
 - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 6: Create the "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"
- Step 7: Create "Time Ranges"
 - Align with the tariff information received from the Service Providers
- Step 8: Create "Routing Policies"
 - Assign the appropriate "Routing Destination" and "Time Of Day"
 - (Time Of Day = assign the appropriate "Time Range" and define the "Ranking")
- Step 10: Create "Dial Patterns"
 - Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"
- Step 11: Create "Regular Expressions"
 - Assign the appropriate "Routing Policies" to the "Regular Expressions"

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.

Domain Management

New Edit Delete Duplicate More Actions

1 Item Filter: Enable

Name	Type	Notes
avaya.com	sip	

Select : All, None

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 following screenshot shows the location details named **Session Manager**. This location is assigned to the SIP Entity called Session Manager in **Section 6.5.1**.

Location Details

CommitCancel

General

* Name:

Session Manager

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

The location pattern is a way of using subnets to further refine the location information, this may be useful for endpoints that could be logged in from different subnets. This was not used during testing. If required, scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string.

The screenshot shows a web interface titled "Location Pattern". At the top, there are "Add" and "Remove" buttons. Below them is a table with 0 items and a "Filter: Enable" link. The table has two columns: "IP Address Pattern" and "Notes". There is a checkbox next to the "IP Address Pattern" header. At the bottom right, there are "Commit" and "Cancel" buttons.

Although routing based on location was not used on Session Manager during testing, separate locations were also defined for both Communication Manager and Avaya SBCE.

The following screenshot shows the location details named **Communication Manager**. This location is assigned to the SIP Entity called Communication Manager in **Section 6.5.2**.

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

- General**: Contains a required field for "Name" (set to "Communication Manager") and a "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 (set to "Kbit/sec"), "Total Bandwidth" and "Multimedia Bandwidth" fields, and a checked checkbox for "Audio Calls Can Take Multimedia Bandwidth".

The following screenshot shows the location details named **Avaya SBCE**. This location is assigned to the SIP Entity called Avaya SBCE in **Section 6.5.3**.

Location Details

CommitCancel

General

* Name:

Avaya SBCE

Notes:

Dial Plan Transparency in Survivable Mode

Enabled:

☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec▼

Total Bandwidth:

Multimedia Bandwidth:

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 and remove headers from messages received from Tele2. 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 R10.1 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 “**Tele2**” 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**:

- **Adaption Name:** Enter an appropriate name such as **Tele2**.
- **Module Name:** Select **OrangeAdapter**.
- **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	
Name	Value		
<input type="checkbox"/> eRHdrs	"P-AV-Message-Id, P-Charging-Vector, P-Location, Endpoint-View, P-Conference, Alert-		
<input type="checkbox"/> fromto	true		
<input type="checkbox"/> MIME	no		

Select : All, None

Egress URI Parameters:

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.

Digit Conversion for Outgoing Calls from SM

Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 00353	* 5	* 15		* 2	+	both		
<input type="checkbox"/>	* 0046	* 4	* 15		* 2	+	both		

Select : All, None

Commit Cancel

This will ensure outgoing numbers matching 00353 and 0046 will have 00 digits deleted and have + inserted therefore 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 three SIP Entities.

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

6.5.1. Avaya Aura® Session Manager SIP Entity

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

SIP Entity Details

CommitCancel

General

* Name: Session Manager

* IP Address: 10.10.3.42

SIP FQDN:

Type: Session Manager

Notes:

Location: Session Manager

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 for Communication Manager in **Section 6.3** and the **Time Zone** to the appropriate time zone.

SIP Entity Details

CommitCancel

General

* Name: Communication Manager

* FQDN or IP Address: 10.10.3.44

Type: CM

Notes:

Adaptation:

Location: Communication Manager

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

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 for Avaya SBCE 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: 10.10.3.35

Type: SIP Trunk

Notes:

Adaptation: Tele2

Location: Avaya SBCE

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"/>	Aura_Messaging	Session Manager	TLS	5061	Aura_Messaging	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Avaya_SBCE	Session Manager	TLS	5061	Avaya_SBCE	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<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"/>	

Select : All, None

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

CommitCancel

General

* Name: to_Communication_Manager

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Communication Manager	10.10.3.44	CM	

Time of Day

AddRemoveView Gaps/Overlaps

1 Item Filter: Enable

<input type="checkbox"/>	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 Tele2 SIP trunk.

Routing Policy Details

CommitCancel

General

* Name: to_Avaya_SBCE

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya_SBCE	10.10.3.35	SIP Trunk	

Time of Day

AddRemoveView 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 for the Tele2 SIP Trunk.

Dial Pattern Details

CommitCancel

General

* Pattern:00353

* Min:5

* Max:15

Emergency Call:☐

SIP Domain:avaya.com

Notes:

Originating Locations and Routing Policies

AddRemove

1 Item

<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		to_Avaya_SBCE	0	<input type="checkbox"/>	Avaya_SBCE	

Select : All, None

Denied Originating Locations

AddRemove

0 Items

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

CommitCancel

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

Dial Pattern Details

CommitCancel

General

* Pattern:+46

* Min:3

* Max:16

Emergency Call:☐

SIP Domain:avaya.com

Notes:

Originating Locations and Routing Policies

AddRemove

1 Item

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

Select : All, None

Denied Originating Locations

AddRemove

0 Items

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

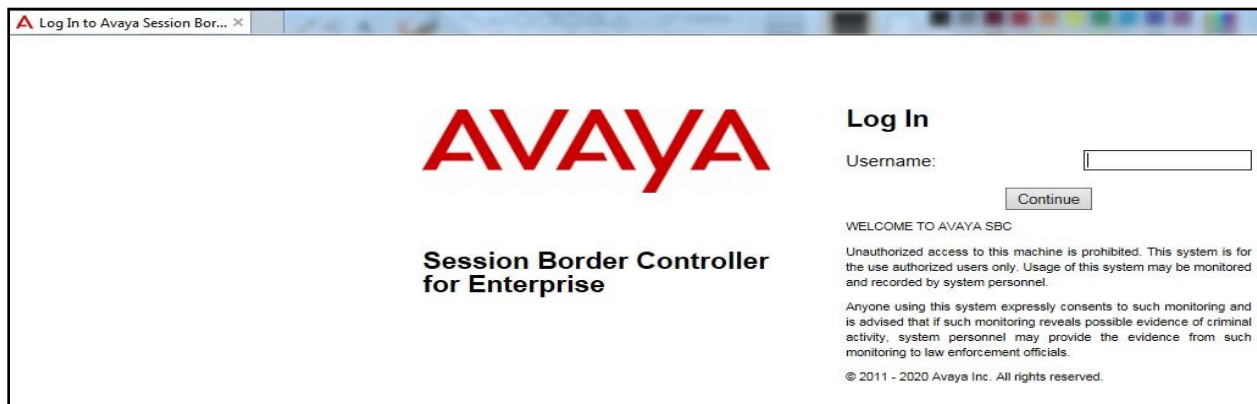
CommitCancel

7. Configure Avaya Session Border Controller for Enterprise

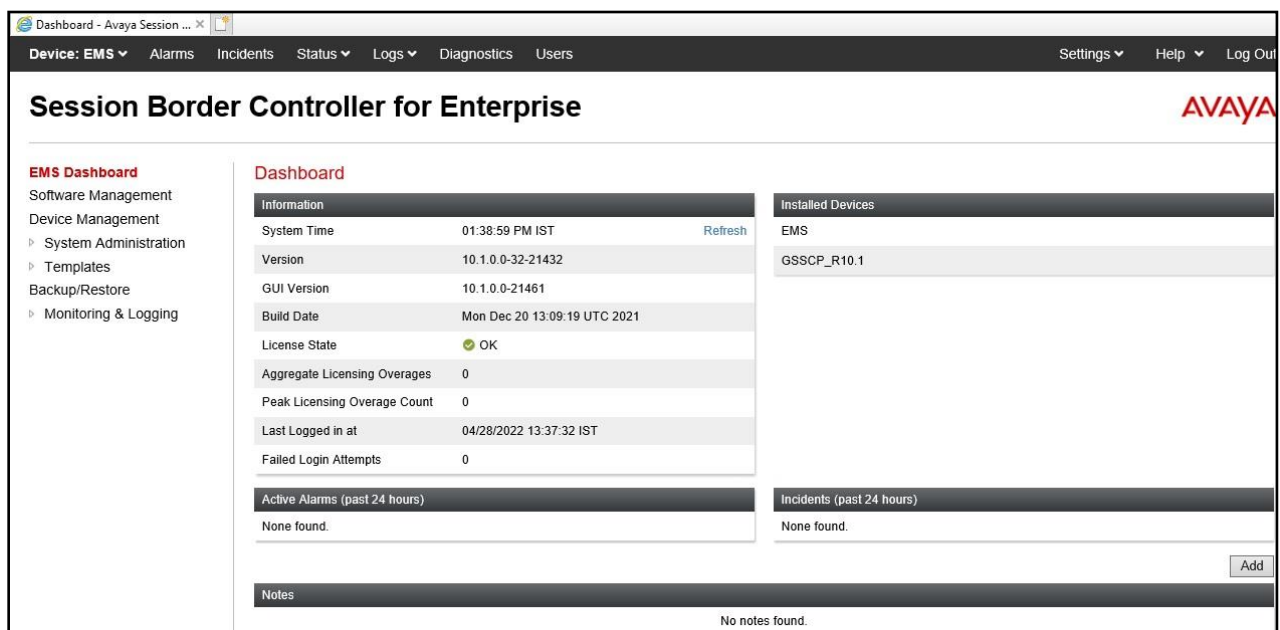
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP 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_R10.1** 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_R10.1** is shown. To view the configuration of this device, click **View** (the third option from the right).

Device Management - Avaya... X

Device: GSSCP_R10.1 Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

EMS
GSSCP_R10.1

Device Controller for Enterprise

AVAYA

Device Management

Devices Updates Licensing Key Bundles License Compliance

Device Name	Management IP	Version	Status						
GSSCP_R10.1	10.10.2.60	10.1.0.0-32-21432	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_R10.1

General Configuration

Appliance Name	GSSCP_R10.1
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	0	0
Advanced Sessions	0	0
Scoopis Video Sessions	0	0
CES Sessions	0	0
Transcoding Sessions	0	0
AMR	<input checked="" type="checkbox"/>	
Premium Sessions	0	0
CLID	---	
Encryption	<input checked="" type="checkbox"/>	

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.10.3.35	10.10.3.35	255.255.255.0	10.10.3.1	A1
192.168.122.57	192.168.122.57	255.255.255.128	192.168.122.9	B1

DNS Configuration

Primary DNS	8.8.8.8
Secondary DNS	8.8.4.4
DNS Location	DMZ
DNS Client IP	192.168.122.57

Management IP(s)

IP #1 (IPv4)	10.10.2.60
--------------	------------

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.

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 populated: '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 of the 'Interface' field. Below these fields is a table with three columns: 'IP Address', 'Public IP', and 'Gateway Override'. The first row contains '192.168.122.57', 'Use IP Address', and 'Use Default'. A 'Delete' button is to the right of the first row. At the bottom of the dialog is a 'Finish' button.

IP Address	Public IP	Gateway Override
192.168.122.57	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
10.10.3.35	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	
A1_Internal	10.10.3.1	255.255.255.0	A1	10.10.3.35	Edit Delete
B1_External	192.168.122.9	255.255.255.128	B1	192.168.122.57	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

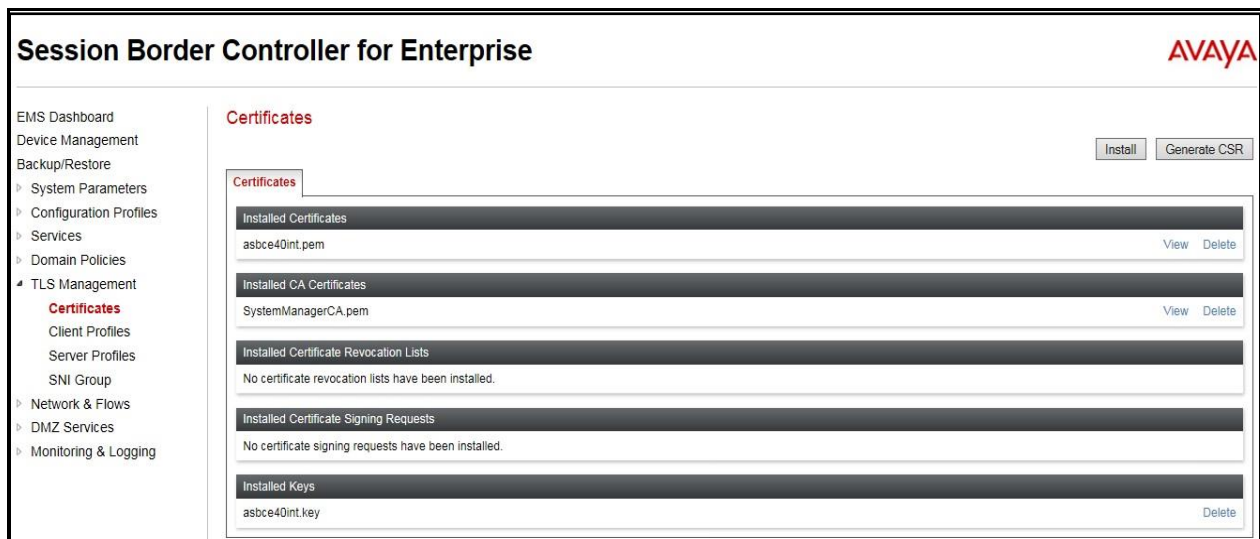
For the compliance test, TLS transport is used for signalling on the SIP trunk between Session Manager and the Avaya SBCE. Compliance testing was done using identity certificates signed by a local certificate authority. The generation and installation of these certificates are beyond the scope of these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



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).

The screenshot displays the 'Client Profiles: GSSCP_Client' configuration window. On the left, a sidebar shows 'Client Profiles' with 'GSSCP_Client' selected. The main area is divided into two sections. The top section, 'Client Profile', contains a 'TLS Profile' table with fields: Profile Name (GSSCP_Client), Certificate (asbce40int.pem), and SNI (Enabled). Below this is a 'Certificate Verification' table with fields: Peer Verification (Required), Peer Certificate Authorities (SystemManagerCA.pem), Peer Certificate Revocation Lists (---), Verification Depth (1), and Extended Hostname Verification (disabled). The bottom section contains 'Renegotiation Parameters' (Renegotiation Time: 0, Renegotiation Byte Count: 0) and 'Handshake Options' (Version: TLS 1.2, 1.1, 1.0; Ciphers: Default; Value: HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH). Buttons for 'Add', 'Delete', and 'Edit' are visible.

Client Profiles: GSSCP_Client	
Click here to add a description.	
Client Profile	
TLS Profile	
Profile Name	GSSCP_Client
Certificate	asbce40int.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

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).

The screenshot displays the configuration interface for a server profile named 'GSSCP_Server'. The interface is divided into several sections:

- Server Profiles: GSSCP_Server**: A header at the top left with 'Add' and 'Delete' buttons.
- Server Profiles**: A sidebar on the left showing 'GSSCP_Server' as the selected profile.
- Server Profile**: The main configuration area, which includes:
 - TLS Profile**: A section with fields for 'Profile Name' (GSSCP_Server), 'Certificate' (asbce40int.pem), and 'SNI Options' (None).
 - Certificate Verification**: A section with fields for 'Peer Verification' (Optional), 'Peer Certificate Authorities' (---), 'Peer Certificate Revocation Lists' (---), 'Verification Depth' (1), and 'Extended Hostname Verification' (checkbox).
 - Renegotiation Parameters**: A section with fields for 'Renegotiation Time' (0) and 'Renegotiation Byte Count' (0).
 - Handshake Options**: A section with fields for 'Version' (checkboxes for TLS 1.2, TLS 1.1, TLS 1.0), 'Ciphers' (radio buttons for Default, FIPS, Custom), and 'Value' (HIGH:IDH:IADH:IMD5:1aNULL:1eNULL:@STRENGTH).
- Edit**: A button at the bottom right of the configuration area.

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 **TCP** port number, **5060** is used for the Tele2 SIP Trunk.
- Click **Finish**.

Signaling Interface						
Signaling Interface						
Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Signaling_External	192.168.122.57 B1_External (B1, VLAN 0)	5060	---	---	None	Edit Delete
Signaling_Internal	10.10.3.35 A1_Internal (A1, VLAN 0)	5060	---	5061	GSSCP_Server	Edit Delete

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	
Media_Internal	10.10.3.35 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
Media_External	192.168.122.57 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, Tele2 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.

Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
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 checked="" 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

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**.

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides <input type="radio"/> Dialog-Initiate Only (Single Side) <input type="radio"/> Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	<input checked="" type="checkbox"/>
Extensions	Avaya ▼
Diversion Manipulation	<input type="checkbox"/>
Diversion Condition	None ▼
Diversion Header URI	<input type="text"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Relay INVITE Replace for SIPREC	<input type="checkbox"/>
MOBX Re-INVITE Handling	<input type="checkbox"/>
DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP Notify <input type="radio"/> RFC 2833 Relay & SIP Notify <input type="radio"/> SIP Info <input type="radio"/> RFC 2833 Relay & SIP Info <input type="radio"/> Inband
<input type="button" value="Finish"/>	

7.5.2. Server Interworking – Tele2

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 Tele2 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.

Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
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 checked="" 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

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**.

Record Routes

☐ None

☐ Single Side

☒ Both Sides

☐ Dialog-Initiate Only (Single Side)

☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup ☒

Extensions None ▾

Diversion Manipulation ☐

Diversion Condition None ▾

Diversion Header URI

Has Remote SBC ☒

Route Response on Via Port ☐

Relay INVITE Replace for SIPREC ☐

DTMF

DTMF Support

☒ None

☐ SIP Notify

☐ SIP Info

☐ Inband

Finish

7.6. Signalling Manipulation

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

During compliance testing, a script was required to change the Max-Forwards value from 0 to 69 on all inbound OPTIONS from Tele2. Initially, the Avaya SBCE was responding to OPTIONS from Tele2 with a “483 Too Many Hops” response and thus the trunk failed to establish. It was diagnosed that the Max-Forwards Header within OPTIONS had a value =0. Normally a Service Provider sets a value of Max-Forwards=69 and a SigMa script was required to change the Max-Forwards value from 0 to 69 on all inbound OPTIONS from Tele2.

It was observed when performing Blind Transfer to PSTN numbers on inbound calls (i.e. PSTN (A) -> Avaya (B) -> Blind Xfer -> PSTN (C)) from Avaya SIP handsets, that Tele2 was responding with a “403 Forbidden”. The reason Tele2 was responding with “403 Forbidden” is that the Avaya SIP handsets populate the P-Asserted-Identity with the originating caller (A) CLID. When performing Blind Transfer to PSTN calls, Tele2 require the P-Asserted-Identity Header to be populated with the CLID of a known number (B) on the Tele2 SIP platform. In order for Blind Transfer to PSTN calls to complete successfully, a SigMa script was created on the Avaya SBCE to populate the P-Asserted-Identity Header with a known Tele2 CLID number on the SIP platform. When Avaya SIP handsets attempt a blind transfer, the SIP handset inserts a Referred-By Header into the outbound INVITE. This scripts checks to see if a Referred-By Header is present and if present, it will populate the P-Asserted-Identity Header with the From Head CLID and the Blind Transfer is executed successfully.

To define the signalling manipulation, navigate to **Configuration Profiles → Signaling Manipulations** and click on **Add** and enter a title. A new blank Signaling Manipulation Editor window will pop up. The script text is as follows:


```

/*Script to populate Max-Forwards Header */

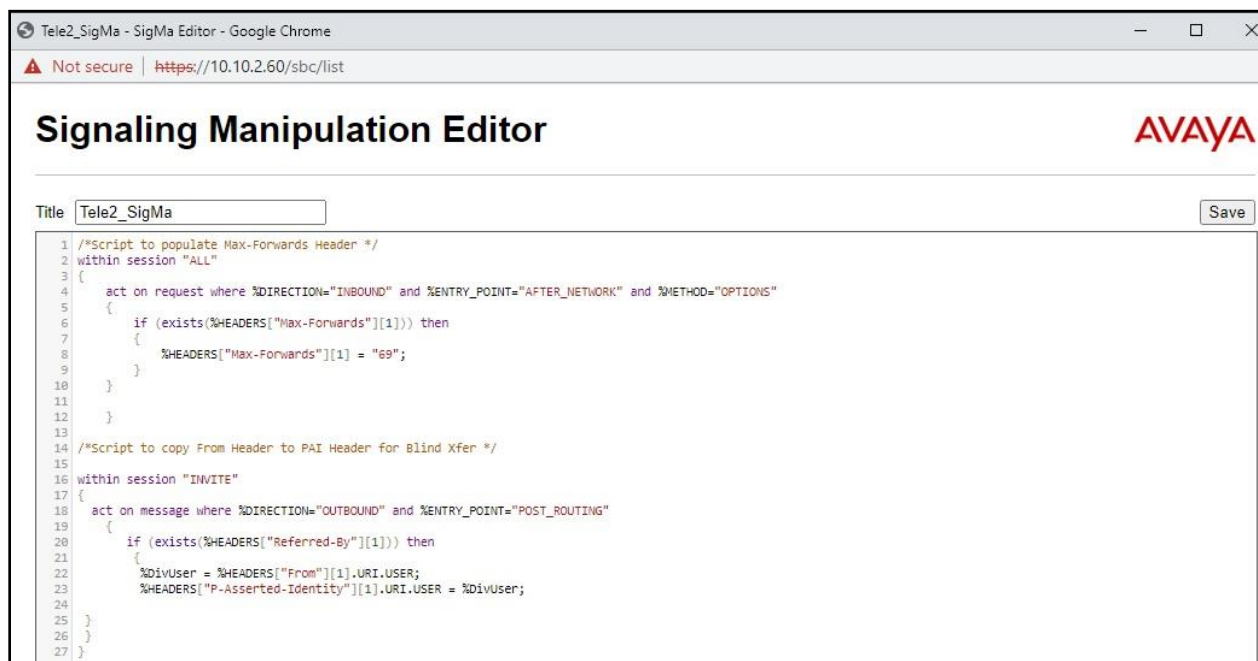
within session "ALL"
{
    act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and
    %METHOD="OPTIONS"
    {
        if (exists(%HEADERS["Max-Forwards"][1])) then
        {
            %HEADERS["Max-Forwards"][1] = "69";
        }
    }
}

/*Script to copy From Header to PAI Header for Blind Transfer */

within session "INVITE"
{
    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
        if (exists(%HEADERS["Referred-By"][1])) then
        {
            %DivUser = %HEADERS["From"][1].URI.USER;
            %HEADERS["P-Asserted-Identity"][1].URI.USER = %DivUser;
        }
    }
}

```

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



7.7. Define Servers

Servers are defined for each server connected to the Avaya SBCE. In this case, Tele2 is connected as the Trunk Server and Session Manager is connected as the Call Server.

7.7.1. 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:

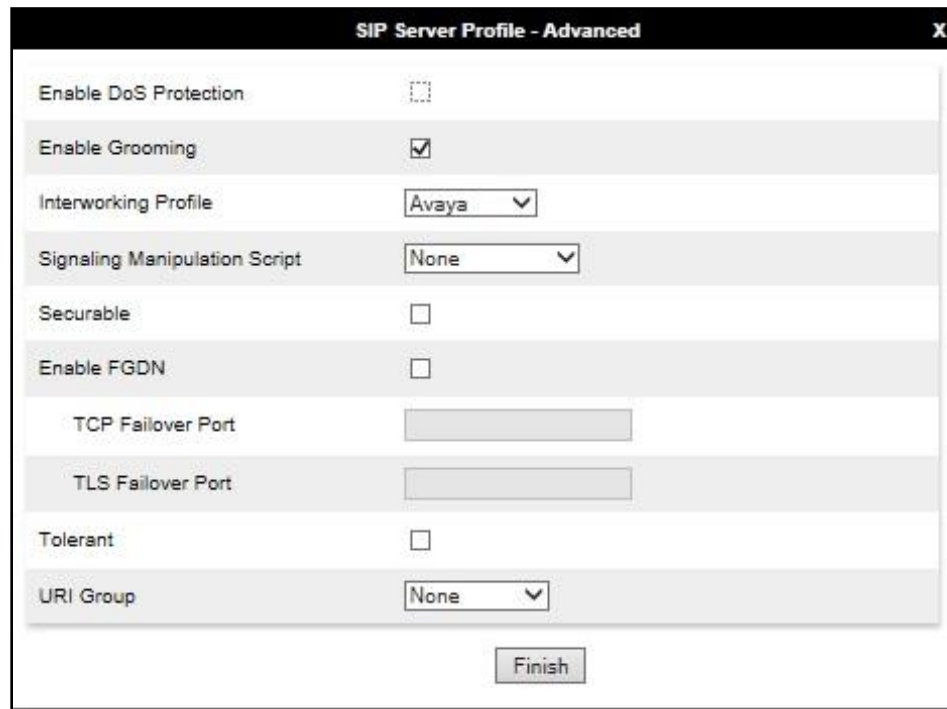
- Select **Server Type** to be **Call Server**.
- Select **TLS Client Profile** to be **GSSCP_Client** as defined in **Section 7.3.2**.
- Enter **IP Address / FQDN** to **10.10.3.42** (Session Manager IP Address).
- For **Port**, enter **5061**.
- For **Transport**, select **TLS**.
- Click on **Next** (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' in a dropdown menu. The 'SIP Domain' field is empty. The 'DNS Query Type' is set to 'NONE/A' in a dropdown menu. The 'TLS Client Profile' is set to 'GSSCP_Client' in a dropdown menu. 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' (selected in a dropdown). 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 center of the window is a button labeled "Finish".

7.7.2. Server Configuration – Tele2

To define the Tele2 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**.
- For **DNS Query Type**, select **SRV**.
- For **FQDN**, enter **siptrunk-internet.tele2.se** (Tele2 SIP Platform).
- For **Transport**, select **TCP**.
- Click on **Next** (not shown).

The screenshot shows the 'SIP Server Profile - General' 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 rows of configuration fields: 'Server Type' with a dropdown menu set to 'Trunk Server', 'SIP Domain' with an empty text box, 'DNS Query Type' with a dropdown menu set to 'SRV', and 'TLS Client Profile' with a dropdown menu set to 'None'. 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 'FQDN' column contains the text 'siptrunk-internet.tele2.se'. The 'Port' column is empty. The 'Transport' column has a dropdown menu set to 'TCP'. A 'Delete' button is located to the right of the table.

In the new window that appears, enter the following values as Tele2 require authentication to connect to the Tele2 SIP trunk:

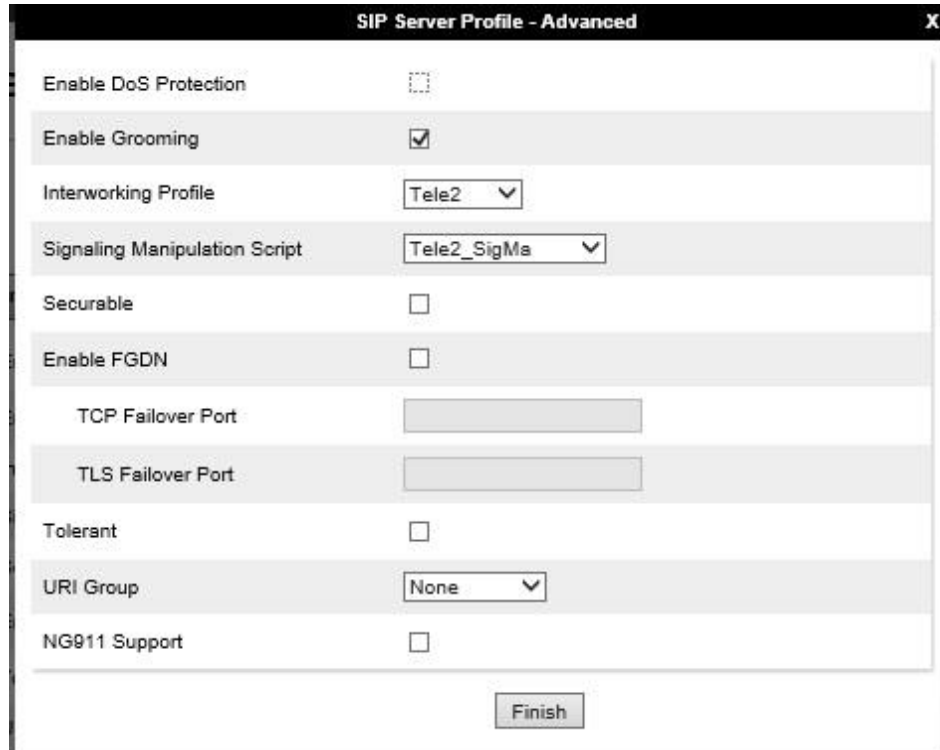
- **Enabled Authentication:** Checked.
- **User Name:** Enter username provided by the Service Provider.
- **Realm:** Enter realm details provided by the Service Provider.
- **Password** Enter password provided by the Service Provider.
- **Confirm Password** Re-enter password provided by the Service Provider.

The screenshot shows the 'SIP Server Profile - Authentication' window. It contains four rows of configuration fields: 'Enable Authentication' with a checked checkbox, 'User Name' with a text box containing 'sipxxxxxctbt19629820', 'Realm' with a text box and the instruction '(Leave blank to detect from server challenge)', 'Password' with a text box and the instruction '(Leave blank to keep existing password)', and 'Confirm Password' with an empty text box.

Click on **Next** (not shown) to use default entries on the **Heartbeat**, **Registration** and **Ping** tabs as registration to the Tele2 SIP trunk was not required during testing.

On the Advanced tab:

- Check **Enable Grooming**.
- Select **Tele2** for **Interworking Profile**.
- Select **Tele2_SigMa** for **Signaling Manipulation Script**.
- Click **Finish**.



The screenshot shows the 'SIP Server Profile - Advanced' configuration window. It contains the following settings:

Setting	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Tele2
Signaling Manipulation Script	Tele2_SigMa
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"/>

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

7.8. 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 Tele2 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.

7.8.1. Routing – Avaya

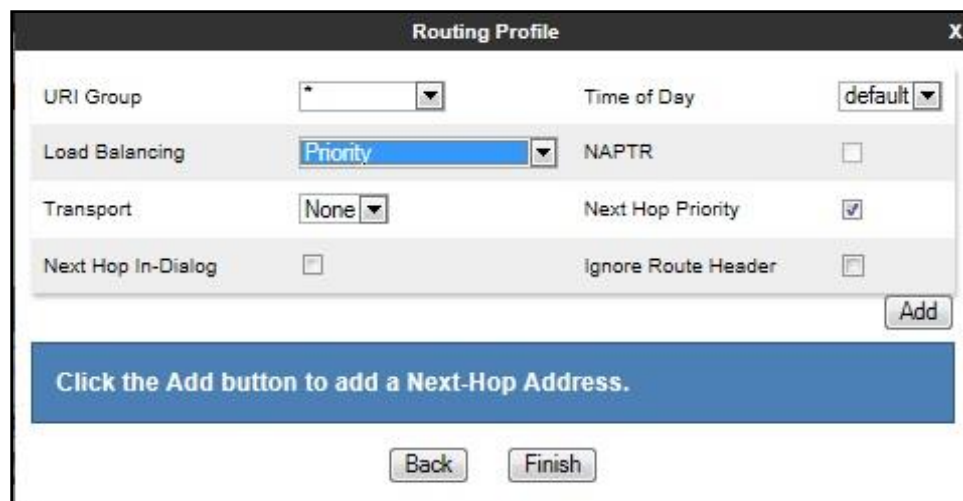
Create a Routing Profile for Session Manager.

- 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. Inside, there is a text field labeled 'Profile Name' containing the text 'Avaya'. 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 configuration options. The options are arranged in a grid-like fashion. 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'.

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

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

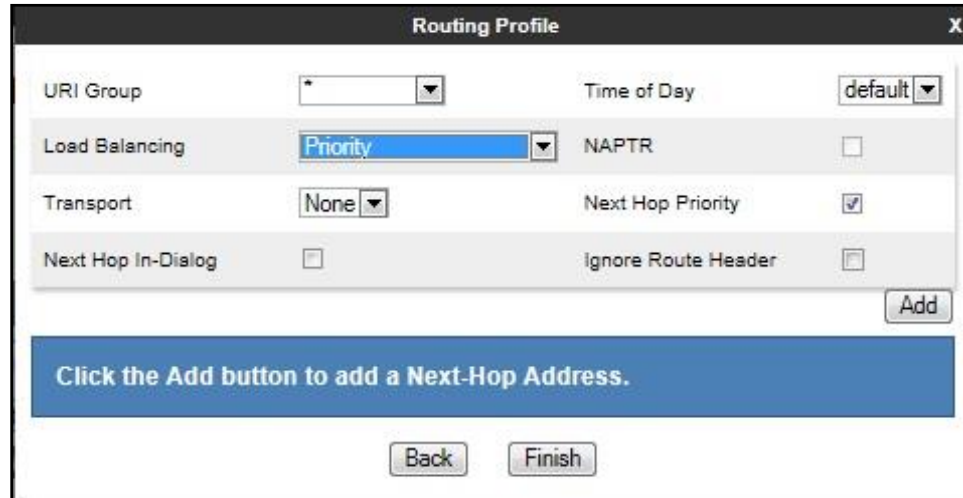
- **Priority/Weight = 1.**
- **SIP Server Profile = Avaya (Section 7.7.1)** from drop down menu.
- **Next Hop Address = Select 10.10.3.42:5061(TLS)** from drop down menu.
- Click **Finish**.

7.8.2. Routing – Tele2

Create a Routing Profile for Tele2 SIP network.

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

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

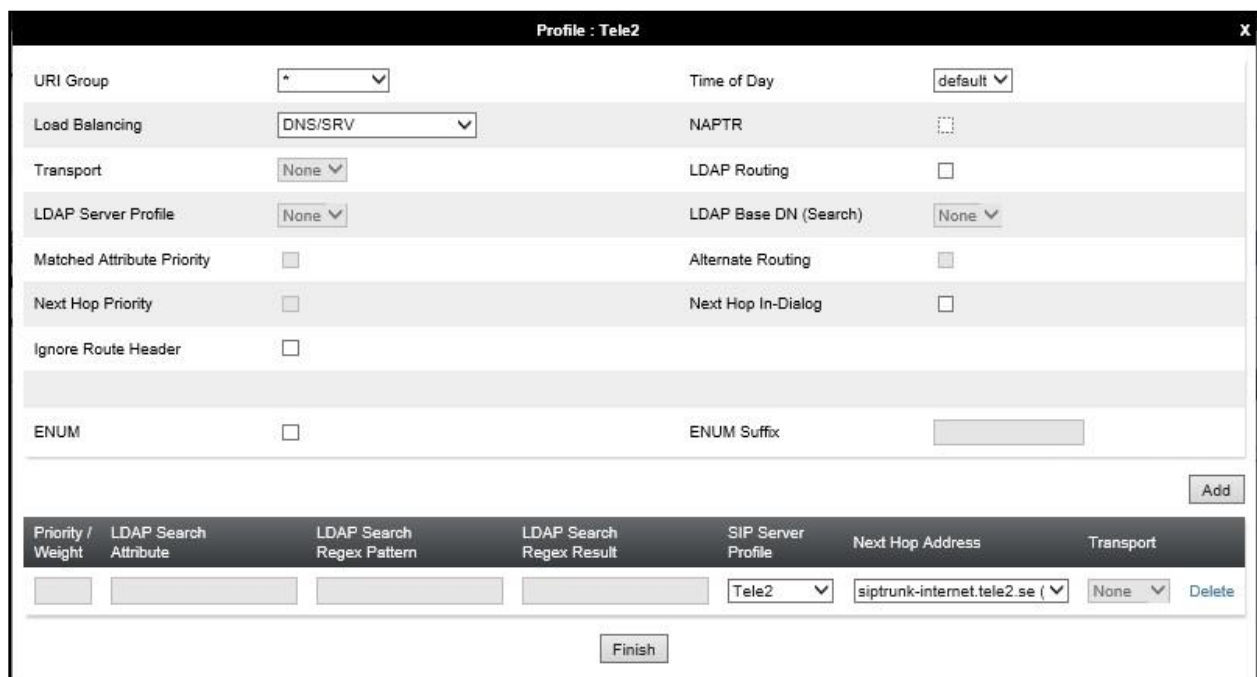


The screenshot shows the 'Routing Profile' window. It contains the following fields and controls:

- URI Group:** A dropdown menu with an asterisk (*) as the selected value.
- Time of Day:** A dropdown menu with 'default' selected.
- Load Balancing:** A dropdown menu with 'Priority' selected.
- NAPTR:** An unchecked checkbox.
- Transport:** A dropdown menu with 'None' selected.
- Next Hop Priority:** A checked checkbox.
- Next Hop In-Dialog:** An unchecked checkbox.
- Ignore Route Header:** An unchecked checkbox.
- Add:** A button located at the bottom right of the form area.
- Instructional Bar:** A blue bar with the text 'Click the Add button to add a Next-Hop Address.'
- Back:** A button at the bottom center.
- Finish:** A button at the bottom right, next to the Back button.

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

- **Load Balancing** = DNS/SRV.
- **SIP Server Profile** = Tele2 (Section 7.7.2) from drop down menu.
- **Next Hop Address** = Select siptrunk-internet.tele2.se from drop down menu.
- Click **Finish**.



The screenshot shows the 'Profile : Tele2' window. It contains the following fields and controls:

- URI Group:** A dropdown menu with an asterisk (*) as the selected value.
- Time of Day:** A dropdown menu with 'default' selected.
- Load Balancing:** A dropdown menu with 'DNS/SRV' selected.
- NAPTR:** An unchecked checkbox.
- Transport:** A dropdown menu with 'None' selected.
- LDAP Routing:** An unchecked checkbox.
- LDAP Server Profile:** A dropdown menu with 'None' selected.
- LDAP Base DN (Search):** A dropdown menu with 'None' selected.
- Matched Attribute Priority:** An unchecked checkbox.
- Alternate Routing:** An unchecked checkbox.
- Next Hop Priority:** An unchecked checkbox.
- Next Hop In-Dialog:** An unchecked checkbox.
- Ignore Route Header:** An unchecked checkbox.
- ENUM:** An unchecked checkbox.
- ENUM Suffix:** A text input field.
- Add:** A button located at the bottom right of the form area.
- Table:** A table with 7 columns: Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, and Transport. The table contains one row with the following values: (empty), (empty), (empty), (empty), 'Tele2', 'siptrunk-internet.tele2.se', and 'None'. There is a 'Delete' button next to the 'Transport' column.
- Finish:** A button at the bottom center.

7.9. 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

Tele2

Click here to add a description.

Topology Hiding

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

Edit

To define Topology Hiding for Tele2, 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 Tele2 and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **bt19629820.siptrunk.tele2.net**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Tele2

Add

Topology Hiding Profiles

default

cisco_th_profile

Avaya

Tele2

Rename

Clone

Delete

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	bt19629820.siptrunk.tele2.net
Via	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
From	IP/Domain	Overwrite	bt19629820.siptrunk.tele2.net
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	bt19629820.siptrunk.tele2.net
Record-Route	IP/Domain	Auto	---

Edit

7.10.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 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 the defaults and then make the necessary changes to the new rule.

7.10.1. Media Rules

A media rule defines the processing to be applied to the selected media. For the compliance test, a media rule was created for Session Manager to use SRTP, while the predefined **default-low-med** media rule was used for the Tele2 SIP trunk.

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 'Media Rules' menu and a list of rules: 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', and 'Avaya_SRTP' (highlighted in red). Above the list is an 'Add' button. The main area has a title bar with 'Rename', 'Clone', and 'Delete' buttons. Below the title bar is a description field with the text 'Click here to add a description.' and 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' (SRTP_AES_CM_128_HMAC_SHA1_80, RTP), 'SRTP Context Reset on SSRC Change' (checkbox), 'Encrypted RTCP' (checkbox), 'MKI' (checkbox), 'Lifetime' (Any), and 'Interworking' (checkbox). The 'Video Encryption' section has the following fields: 'Preferred Formats' (RTP) and 'Interworking' (checkbox).

For the compliance test, the default media rule **default-low-med** was used for Tele2.

Media Rules: default-low-med

Add Filter By Device... Clone

Media Rules

- default-low-med
- default-low-med-enc
- default-high
- default-high-enc
- avaya-low-med-enc
- Avaya_SRTP

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Encryption Codec Prioritization Advanced QoS

Audio Encryption

Preferred Formats RTP

Interworking ☒

Video Encryption

Preferred Formats RTP

Interworking ☒

Miscellaneous

Capability Negotiation ☐

Edit

7.11. 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 Tele2 SIP trunk. The end point policy group is applied to the traffic as part of the end point flow defined in **Section 7.12**.

7.11.1. 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**.

Policy Set

Application Rule default

Border Rule default

Media Rule Avaya_SRTP

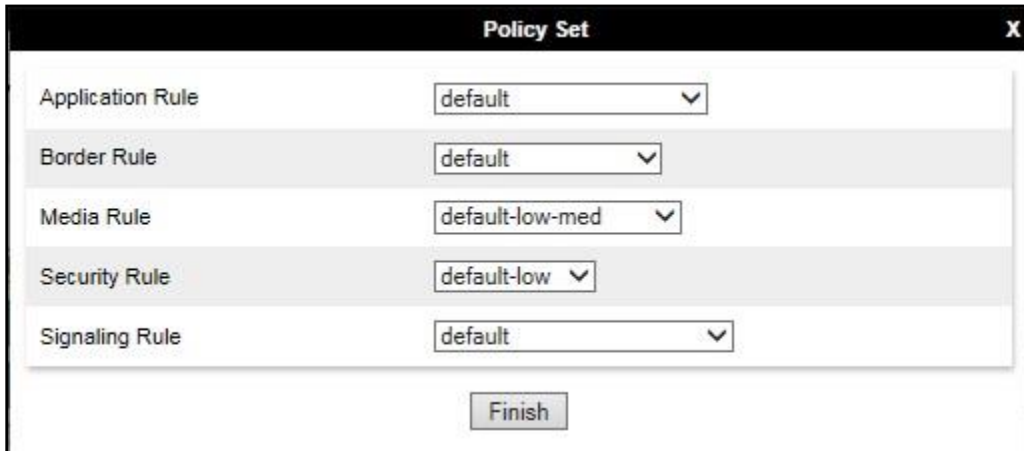
Security Rule default-low

Signaling Rule default

Finish

7.11.2. End Point Policy Group – Tele2

For the compliance test, the predefined End Point Policy **default-low** was used for the Tele2 End Point Policy Group.



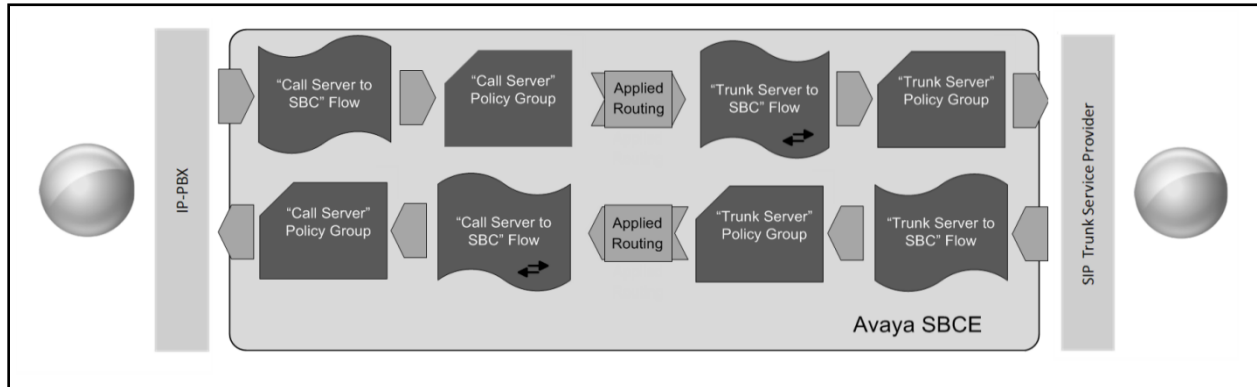
The screenshot shows a 'Policy Set' configuration window with a black title bar and a close button (X) in the top right corner. The window contains a list of five rules, each with a corresponding dropdown menu. The rules and their selected values are:

Rule Type	Selected Value
Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default

At the bottom center of the window is a 'Finish' button.

7.12. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to Tele2's SIP Trunk and incoming flows from Tele2'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 Tele2 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.

[Click here to add a row description.](#)

SIP Server: Avaya

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Call_Server	*	Signaling_External	Signaling_Internal	Avaya	Tele2	View Clone Edit Delete

SIP Server: Tele2

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

To define the inbound Server Flow for the Tele2 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 Tele2 SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the Tele2 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 **default-low**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.8.1**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Tele2 SIP Trunk defined in **Section 7.9** 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	Tele2
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Signaling_Internal

Profile	
Signaling Interface	Signaling_External
Media Interface	Media_External
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	Tele2
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>

To define the outbound server flow for Session Manager to the Tele2 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 Tele2 SIP Trunk defined in **Section 7.8.2**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.9** and click **Finish** (not shown).

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

Criteria Section:

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

Profile Section:

Signaling Interface	Signaling_Internal
Media Interface	Media_Internal
Secondary Media Interface	None
End Point Policy Group	Avaya
Routing Profile	Tele2
Topology Hiding Profile	Avaya
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>

8. Tele2 SIP Trunk Configuration

The configuration of the Tele2 equipment used to support Tele2's SIP Trunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on Tele2 equipment and system configuration please contact an authorized Tele2 representative.

9. Verification Steps

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

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

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.

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

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

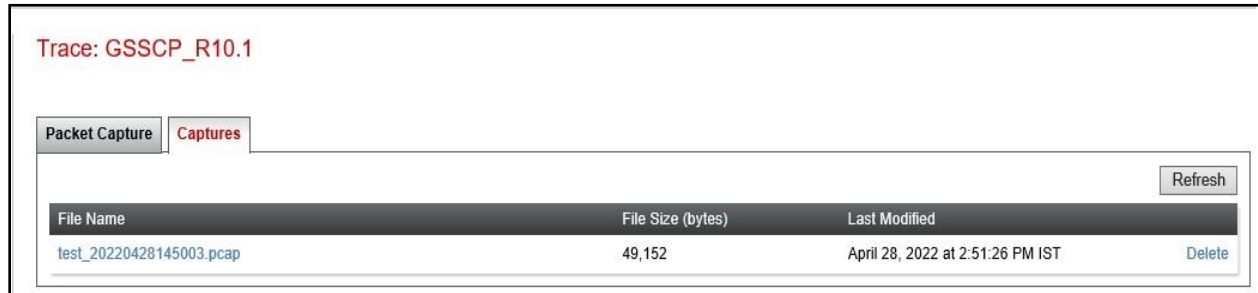
Trace: GSSCP_R10.1

Packet Capture
Captures

Packet Capture Configuration

Status	Ready
Interface	B1 ▾
Local Address IP[:Port]	All ▾ : <input type="text"/>
Remote Address *, ^:Port, IP, IP:Port	<input type="text" value="*"/>
Protocol	All ▾
Maximum Number of Packets to Capture	<input type="text" value="10000"/>
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	<input type="text" value="test.pcap"/>
<input type="button" value="Start Capture"/> <input type="button" value="Clear"/>	

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



The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response to OPTIONS in the form of a 200 OK will be seen from the Tele2 network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura ® Communication Manager R10.1, Avaya Aura ® Session Manager 10.1 and Avaya Session Border Controller for Enterprise R10.1 to the Tele2 SIP platform. The Tele2 SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

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 10.1, Apr 2022
- [2] *Upgrading Avaya Aura® applications*, Release 10.1, Apr 2022
- [3] *Deploying Avaya Aura® applications from System Manager*, Release 10.1, Apr 2022
- [4] *Deploying Avaya Aura® Communication Manager*, Release 10.1, Apr 2022
- [5] *Administering Avaya Aura® Communication Manager*, Release 10.1, Apr 2022
- [6] *Upgrading Avaya Aura® Communication Manager*, Release 10.1, Apr 2022
- [7] *Deploying Avaya Aura® System Manager*, Release 10.1, Apr 2022
- [8] *Upgrading Avaya Aura® System Manager*, Release 10.1, Apr 2022
- [9] *Administering Avaya Aura® System Manager*, Release 10.1, Apr 2022
- [10] *Deploying Avaya Aura® Session Manager*, Release 10.1 Apr 2022
- [11] *Upgrading Avaya Aura® Session Manager*, Release 10.1, Apr 2022
- [12] *Administering Avaya Aura® Session Manager*, Release 10.1, Apr 2022
- [13] *Deploying Avaya Session Border Controller for Enterprise*, Release 10.1, Dec 2021
- [14] *Upgrading Avaya Session Border Controller for Enterprise*, Release 10.1 Dec 2021
- [15] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1, Dec 2021
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

12.Appendix A: SigMa Scripts

Following is the Signaling Manipulation script that were used in the configuration of the Avaya SBCE as explained in **Section 7.6**. When adding these scripts as instructed in **Sections 7.7.2** enter a name for the script in the Title

```
/*Script to populate Max-Forwards Header */
within session "ALL"
{
    act on request where %DIRECTION="INBOUND" and
%ENTRY_POINT="AFTER_NETWORK" and %METHOD="OPTIONS"
    {
        if (exists(%HEADERS["Max-Forwards"][1])) then
        {
            %HEADERS["Max-Forwards"][1] = "69";
        }
    }
}

/*Script to copy From Header to PAI Header for Blind Xfer */

within session "INVITE"
{
    act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
    {
        if (exists(%HEADERS["Referred-By"][1])) then
        {
            %DivUser = %HEADERS["From"][1].URI.USER;
            %HEADERS["P-Asserted-Identity"][1].URI.USER = %DivUser;
        }
    }
}
```


13. Appendix B: MEX Testing

Mobile phones may be assigned to the Tele2 Business Trunk service as Mobile Extensions (MEX). Tele2 offer two standards versions of MEX, Standard Mex and Forced MEX.

Standard Mex

When a MEX mobile phone is in state Standard Mex then calls originated by the mobile phone will be routed through the SIP-PBX. The SIP-PBX will receive an incoming Invite containing the R1 prefix as described below. Incoming calls to the MEX mobile phone will be routed directly without passing the SIP-PBX.

Forced Mex.

When a MEX mobile phone is in state Forced Mex then calls originated by the mobile phone as well as calls to the mobile phone will be routed through the SIP-PBX. For calls originated by the MEX mobile phone the SIP-PBX will receive an incoming Invite containing the R1 prefix as described below. Incoming calls to the MEX mobile phone will be routed through the SIP-PBX. When forwarding a Forced Mex call to the SIP-PBX the SP-SSE will set the mobile phone number or the corresponding fix number in the request URI and the To header. Whether the fixed or the mobile number is used is a provisioning issue, device by device.

In this compliance testing, the below test extensions and MEX enabled mobile numbers can only be used in Sweden to be able to trigger MEX services.

MEX 1 fixed number = +46101xxxx20 (MEX1 enabled mobile= +46735963567) extension 6100.

MEX 2 fixed number = +46101xxxx21 (MEX2 enabled mobile= +46735963544) extension 6102.

R1 number: 225 and Prefix: +46736.

13.1.1. Configure Session Manager – Dial Pattern

There are two examples of dial patterns defined in this configuration: 0046 and 225.

Dial Pattern Details

Commit

Cancel

General

* Pattern:

0046

* Min:

4

* Max:

20

Emergency Call:

☐

SIP Domain:

avaya.com

Notes:

Originating Locations and Routing Policies

Add

Remove

1 Item

<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		to_Avaya_SBCE	0	<input type="checkbox"/>	Avaya_SBCE	

Select : All, None

Denied Originating Locations

Add

Remove

0 Items

<input type="checkbox"/>	Originating Location	Notes
<input type="checkbox"/>		

Commit

Cancel

Figure 93: Dial Pattern_0046

Dial Pattern Details

Commit

Cancel

General

* Pattern:

225

* Min:

3

* Max:

20

Emergency Call:

☐

SIP Domain:

avaya.com

Notes:

Originating Locations and Routing Policies

Add

Remove

1 Item

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

Select : All, None

Denied Originating Locations

Add

Remove

0 Items

<input type="checkbox"/>	Originating Location	Notes
<input type="checkbox"/>		

Commit

Cancel

Figure 94: Dial Pattern_225

CMN; Reviewed:
SPOC 7/13/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

72 of 83
Tele2_CMSMSBC10

13.1.2. Configure Communication Manager

1. Configure off-pbx- telephone station-mapping for extension 6100

change off-pbx-telephone station-mapping 6100							Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual		
Extension		Prefix			Selection	Set	Mode		
6100	EC500	-		0046735963567	ars	1			
		-							

Figure 95: Station-Mapping_6100

2. Configure station 6100

change station 6100		Page	2 of	5
STATION				
FEATURE OPTIONS				
LWC Reception: spe	Auto Select Any Idle Appearance? n			
LWC Activation? y	Coverage Msg Retrieval? y			
LWC Log External Calls? n	Auto Answer: none			
CDR Privacy? n	Data Restriction? n			
Redirect Notification? y	Idle Appearance Preference? n			
Per Button Ring Control? n	Bridged Idle Line Preference? n			
Bridged Call Alerting? n	Restrict Last Appearance? y			
Active Station Ringing: single	EMU Login Allowed? n			
H.320 Conversion? n	Per Station CPN - Send Calling Number?			
Service Link Mode: as-needed	EC500 State: enabled			
Multimedia Mode: enhanced	Audible Message Waiting? n			
MWI Served User Type:	Display Client Redirection? n			
AUDIX Name:	Select Last Used Appearance? n			
	Coverage After Forwarding? s			
	Multimedia Early Answer? n			
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y			
Emergency Location Ext: 6100	Always Use? n IP Audio Hairpinning? n			

Figure 96: Station 6100 – Page 2

change station 6100		Page 4 of 5
STATION		
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5:	
2: call-appr	6:	
3: call-appr	7:	
4: ec500 Timer? n	8:	
voice-mail		

Figure 97: Station 6100 – Page 4

3. Configure off-pbx- telephone station-mapping for extension 6102

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	-		0046735963544	ars	1	
		-					

Figure 98: Station-Mapping_6102

4. Configure station 6102

change station 6102	Page 2 of 5
STATION	
FEATURE OPTIONS	
LWC Reception: spe	Auto Select Any Idle Appearance? n
LWC Activation? y	Coverage Msg Retrieval? y
LWC Log External Calls? n	Auto Answer: none
CDR Privacy? n	Data Restriction? n
Redirect Notification? y	Idle Appearance Preference? n
Per Button Ring Control? n	Bridged Idle Line Preference? n
Bridged Call Alerting? n	Restrict Last Appearance? y
Active Station Ringing: single	
	EMU Login Allowed? n
H.320 Conversion? n	Per Station CPN - Send Calling Number?
Service Link Mode: as-needed	EC500 State: enabled
Multimedia Mode: enhanced	Audible Message Waiting? n
MWI Served User Type:	Display Client Redirection? n
AUDIX Name:	Select Last Used Appearance? n
	Coverage After Forwarding? s
	Multimedia Early Answer? n
Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y	
Emergency Location Ext: 6102	Always Use? n IP Audio Hairpinning? n

Figure 98: Station 6102 – Page 2

change station 6102	Page 4 of 5
STATION	
SITE DATA	
Room:	Headset? n
Jack:	Speaker? n
Cable:	Mounting: d
Floor:	Cord Length: 0
Building:	Set Color:
ABBREVIATED DIALING	
List1:	List2:
	List3:
BUTTON ASSIGNMENTS	
1: call-appr	5:
2: call-appr	6:
3: call-appr	7:
4: ec500	8:
Timer? n	
voice-mail	

Figure 99: Station 6102 – Page 4

5. Configure incoming-call-handling

change inc-call-handling-trmt trunk-group 1					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/ Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	17	225	3	9	
public-ntwrk	8	22590400	all	990400	

Figure 100: Incoming Call Handling

6. Configure Dialplan

change dialplan analysis			Page 1 of 12
DIAL PLAN ANALYSIS TABLE			
Location: all			Percent Full: 4
Dialed String	Total Length	Call Type	
9	1	fac	

Figure 101: Dialplan

7. Configure ARS

change ars analysis 00							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	
00	13	17	1	pubu		n	

Figure 102: ARS Analysis

14. Appendix C: Configure for Special Numbers

Calls from PBX to Emergency, Police, Inquire, Healthcare, Public or Special Service number services, service numbers are required a prefix/suffix before being sent to the Tele2 platform. The prefix/suffix needs to be added by the PBX. The prefix provided by Tele2 during the compliance testing was **+46379** and is required for the number series starting on 112, 11414, 118, 1177, 11313 and 116. The suffix **447** is required for the number series starting on 112, 11414, 1177 and 11313. 118 required the suffix **118** and 116 required the suffix **000**. This information should be requested of Tele2 at time of installation.

Example:

- Calling Emergency number 112: The PBX sends +46379112447
- Calling Police number 11414: The PBX sends + 4637911414447.
- Calling Inquire number 118: The PBX sends +46379118118.
- Calling Healthcare number 1177: The PBX sends +463791177447.
- Calling Public Information number 11313: The PBX sends + 4637911313447.
- Calling Special Service number 116: The PBX sends + 46379116000.

14.1. Configure Communication Manager

1. Configure Dialplan

change dialplan analysis			Page 1 of 12
DIAL PLAN ANALYSIS TABLE			
Location: all			Percent Full: 4
Dialed String	Total Length	Call Type	
9	1	fac	

Figure 110: Dialplan

2. Configure ARS

change ars analysis 0							Page 1 of 2	
ARS DIGIT ANALYSIS TABLE								
Location: all							Percent Full: 1	
Dialed String	Total Min Max		Route Pattern	Call Type	Node Num	ANI Reqd		
11	2	6	1	pubu		n		

Figure 111: ARS Analysis

14.2. Session Manager Adaptation for Special Service Numbers

As per **Section 6.4**, Session Manager 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. The Tele2 adaptation created in **Section 6.4** was used to modify and meet the numeric prefix and suffix requirements requested by Tele2 for certain numbers as described in **Section 13** above.

Adaptation Details [Commit] [Cancel]

General

* Adaptation Name: Tele2

Notes:

* Module Name: OrangeAdapter

Type: digit

State: enabled

Module Parameter Type: Name-Value Parameter

Name	Value
eRHdrs	"P-AV-Message-Id, P-Charging-Vector, P-Location, Endpoint-View, P-Conference, Alert-
fromto	true
MIME	no

Select : All, None

Egress URI Parameters:

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.

Digit Conversion for Outgoing Calls from SM

Add Remove

6 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 112	* 3	* 3		* 3	+46379112447	both		
<input type="checkbox"/>	* 11313	* 5	* 5		* 5	+4637911313447	both		
<input type="checkbox"/>	* 11414	* 5	* 5		* 5	+4637911414447	both		
<input type="checkbox"/>	* 116	* 3	* 3		* 3	+46379116000	both		
<input type="checkbox"/>	* 1177	* 4	* 4		* 4	+463791177447	both		
<input type="checkbox"/>	* 118	* 3	* 3		* 3	+46379118118	both		

Select : All, None

Commit Cancel

The screenshot above highlights the modifications made to Emergency, Police and Special Service numbers etc. as requested by Tele2.

15. Appendix D: Configure for Service Numbers

Calls from PBX to Service number services are also required a prefix before being sent to the Tele2 platform. The prefix needs to be added by the PBX. The prefix provided by Tele2 during the compliance testing was **+46379** and is required for the Service number series starting on 90[1-9]xx numbers (e.g. 90510, 90400, 90200).

Example:

- Calling Service Number 90510: The PBX sends +4637990510.
- Calling Service Number 90400: The PBX sends +4637990400.
- Calling Service Number 90200: The PBX sends +4637990200.

15.1. Configure Communication Manager

1. Configure Dialplan

change dialplan analysis			Page 1 of 12		
DIAL PLAN ANALYSIS TABLE					
Location: all			Percent Full: 4		
Dialed String	Total Length	Call Type			
9	1	fac			

Figure 110: Dialplan

2. Configure ARS

change ars analysis 0							Page 1 of 2	
ARS DIGIT ANALYSIS TABLE								
Location: all							Percent Full: 1	
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd		
90	2	6	1	pubu		n		

Figure 111: ARS Analysis

15.2. Session Manager Adaptation for Service Numbers

As per **Section 6.4**, Session Manager 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. The Tele2 adaptation created in **Section 6.4** was used to modify and meet the numeric prefix and suffix requirements requested by Tele2 for certain numbers as described in **Section 14** above.

Adaptation Details [Commit] [Cancel]

General

* Adaptation Name: Tele2

Notes:

* Module Name: OrangeAdapter

Type: digit

State: enabled

Module Parameter Type: Name-Value Parameter

Name	Value
eRHdrs	"P-AV-Message-Id, P-Charging-Vector, P-Location, Endpoint-View, P-Conference, Alert-
fromto	true
MIME	no

Select : All, None

Egress URI Parameters:

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.

Digit Conversion for Outgoing Calls from SM

Add Remove

3 Items
Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 90200	* 5	* 5		* 5	+4637990200	both		
<input type="checkbox"/>	* 90400	* 5	* 5		* 5	+4637990400	both		
<input type="checkbox"/>	* 90510	* 5	* 5		* 5	+4637990510	both		

Select : All, None

Commit Cancel

The screenshot above highlights the modifications made to Service numbers as requested by Tele2.

©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.