

Avaya Solution & Interoperability Test Lab

# Application Notes for Configuring Telia Norway SIP Trunk with Avaya Aura<sup>®</sup> Communication Manager 8.1.3, Avaya Aura<sup>®</sup> Session Manager 8.1.3, Avaya Aura<sup>®</sup> Experience Portal 8.1 and Avaya Session Border Controller for Enterprise 8.1.3 – Issue 1.0

### Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Telia Norway and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura<sup>®</sup> Session Manager 8.1.3, Avaya Aura<sup>®</sup> Communication Manager 8.1.3, Avaya Aura<sup>®</sup> Experience Portal 8.1, Avaya Session Border Controller for Enterprise 8.1.3 and various Avaya endpoints.

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.

Telia Norway is a member of the Avaya 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.	INT	RODUCTION	4
2.	GEN	ERAL TEST APPROACH AND TEST RESULTS	4
	2.1.	INTEROPERABILITY COMPLIANCE TESTING	5
	2.2.	TEST RESULTS	6
	2.3.	SUPPORT	6
3.	REF	ERENCE CONFIGURATION	7
4.	EQU	JIPMENT AND SOFTWARE VALIDATED	8
5.	CON	NFIGURE AVAYA AURA® COMMUNICATION MANAGER	10
	5.1.	LICENSING AND CAPACITY	10
	5.2.	System Features	12
	5.3.	IP NODE NAMES	13
	5.4.	CODECS	
	5.5.	IP NETWORK REGION FOR MEDIA GATEWAY, MEDIA SERVER	
	5.6.	CONFIGURE IP INTERFACE FOR PROCR	
	5.7.	SIGNALING GROUP	
	5.8.	TRUNK GROUP	
	5.9.	CALLING PARTY INFORMATION.	
	5.10.	Outbound Routing	
	5.11.	INCOMING CALL HANDLING TREATMENT CONTACT CENTER CONFIGURATION	
	5.12.	CONTACT CENTER CONFIGURATION         1. Announcements	
		1. Announcements	
	5.13.	AVAYA AURA® COMMUNICATION MANAGER STATIONS	
	5.14.	SAVE AVAYA AURA® COMMUNICATION MANAGER STATIONS	
6.		FIGURE AVAYA AURA® SESSION MANAGER	
υ.			
	6.1.	AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION	
	6.2.	SPECIFY SIP DOMAIN	
	6.3.	ADD LOCATION	
	6.4.	ADD SIP ENTITIES	
		. Configure Session Manager SIP Entity Configure Communication Manager SIP Entity	
		Configure Communication Manager SIF Entity	
		. Configure Avaya Session Boraer Controller SH Emily	
	6.5.	ADD ENTITY LINKS	
		CONFIGURE TIME RANGES	
	6.7.	ADD ROUTING POLICIES	•••••••••••
	6.8.	ADD DIAL PATTERNS	
7.	CON	FIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	54
	7.1.	LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	
	7.2.	TLS MANAGEMENT	
		. Installing TLS Certificate	
		. TLS Client Profile	
		. TLS Server Profile	
	7.3.	Server Interworking	
	7.3.1	. Configure Server Interworking Profile - Avaya Site	
		Configure Server Interworking Profile – Telia Norway SIP Trunk Site	64
	7.4.	CONFIGURE SIGNALING MANIPULATION	65

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	2 of 104
SPOC 4/3/2022	©2022 Avaya Inc. All Rights Reserved.	TN_CMSM81SBC81

7.	7.5. Configure Services	
	7.5.1. Configure SIP Server – Avaya Site	
	7.5.2. Configure SIP Server – Telia Norway SIP Trunk	
7.	7.6. ROUTING	71
	7.6.1. Configure Routing – Avaya Site	
	7.6.2. Configure Routing – Telia Norway SIP Trunk Site	
7.	7.7. TOPOLOGY HIDING	74
	7.7.1. Configure Topology Hiding – Avaya Site	
	7.7.2. Configure Topology Hiding Profile – Telia Norway SIP Trunk site	
7.	7.8. Domain Policies	
	7.8.1. Create Application Rules	
	7.8.2. Create Media Rules	77
	7.8.3. Create Endpoint Policy Groups	
7.	7.9. Network & Flows	
	7.9.1. Manage Network Settings	
	7.9.2. Create Media Interfaces	
	7.9.3. Create Signaling Interfaces	
	7.9.4. Configuration Server Flows	
	7.9.4.1 Create End Point Flows – SMVM Flow	
	7.9.4.2 Create End Point Flows – Telia Norway SIP Trunk Flow	
8.	CONFIGURE AVAYA AURA® EXPERIENCE PORTAL	
8.	8.1. BACKGROUND	
8.	8.2. LOGGING IN AND LICENSING	
8.	8.3. VOIP CONNECTION	
8.	8.4. SPEECH SERVERS	
8.	8.5. Application	
8.	8.6. MPP Servers and VoIP Settings	
8.	8.7. CONFIGURING RFC2833 EVENT VALUE OFFERED BY EXPERIENCE PORT.	AL99
9.	TELIA NORWAY SIP TRUNK CONFIGURATION	
10.	VERIFICATION STEPS	
11.	CONCLUSION	
12.	REFERENCES	
13.	APPENDIX A - SIGMA SCRIPT	

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Telia Norway and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura<sup>®</sup> Session Manager 8.1.3, Avaya Aura<sup>®</sup> Communication Manager 8.1.3, Avaya Aura<sup>®</sup> Experience Portal 8.1, Avaya Session Border Controller for Enterprise (Avaya SBCE) 8.1.3 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with Telia Norway SIP Trunk are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

# 2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to Telia Norway SIP Trunk via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager, Experience Portal and the Avaya SBCE with various types of Avaya phones.

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 this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with this Application Note, the interface between Avaya systems and the Telia Norway SIP Trunk Service included the use of encryption features as requested by Telia Norway.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

# 2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various Avaya deskphone types including H.323, SIP, digital, and analog at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider
- Outgoing PSTN calls from various Avaya deskphone types including H.323, SIP, digital, and analog at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider
- Inbound and outbound PSTN calls to/from softphones. Two Avaya soft phones were used during the test: Avaya one-X<sup>®</sup> Communicator (1XC) and Avaya Workplace Client for Windows. 1XC supports two work modes (Computer and Other Phone). Each supported mode was tested. 1XC also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Both protocols were tested. Avaya Workplace Client for Windows was used during the test as a simple SIP endpoint for basic inbound and outbound calls
- SIP transport using TLS, port 6004, between the Avaya enterprise and Telia Norway
- Direct IP-to-IP Media (also known as "Shuffling") over a SIP Trunk. Direct IP-to-IP Media allows Communication Manager to reconfigure the RTP path after call establishment directly between the Avaya phones and the Avaya SBCE releasing media processing resources on the Avaya Media Gateway or Avaya Media Server
- Codec G.711MU, G.711A, G.729A
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors
- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call transfer, conference, off-net call forwarding, forwarding to Avaya Aura<sup>®</sup> Messaging and EC500 mobility (extension to cellular)
- SIP re-Invite in off-net call transfer
- Call Center scenarios
- T.38 and G.711 passthrough fax
- DTMF RFC2833
- Remote Worker (Use Avaya Agent for Desktop)
   Note: Remote Worker was tested as part of this solution. The configuration necessary to support remote worker is beyond the scope of these Application Notes and are not included in these Application Notes. For these configuration details, see Reference [10] in Section 12
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements and/or music on hold)

Items not supported include the following:

- Telia Norway does not support Registration/Authentication
- Telia Norway does not support the outbound operator assisted call
- Telia Norway supports outbound/inbound toll-free service in production, however it is not available in their test lab during the compliance testing.

### 2.2. Test Results

Interoperability testing of Telia Norway was completed with successful results for all test cases.

### 2.3. Support

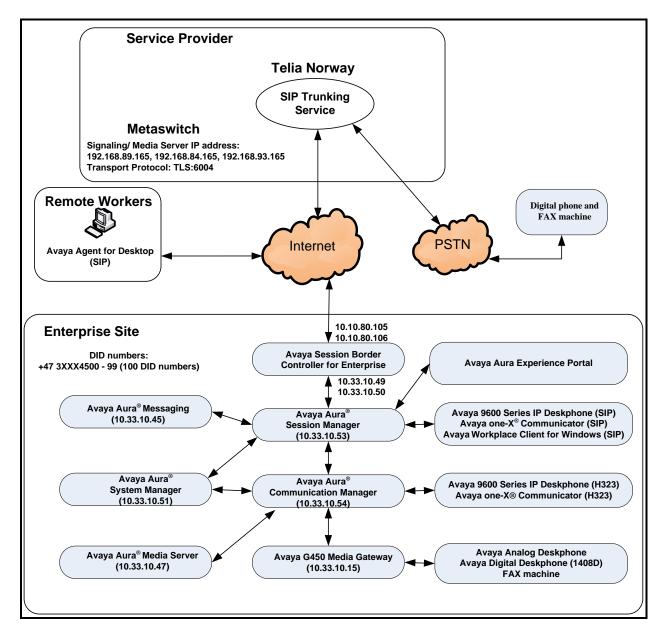
For technical support on the Avaya products described in these Application Notes visit: <u>http://support.avaya.com</u>

For technical support on Telia Norway SIP Trunking, contact Telia Norway at website: <u>http://telia.no</u>

# 3. Reference Configuration

**Figure 1** illustrates a sample Avaya SIP-enabled enterprise solution connected to Telia Norway SIP Trunk. This was the configuration used during the compliance test.

For confidentiality and privacy purposes, actual public IP Addresses used during the test have been masked and replaced with fictitious IP Addresses throughout the document.



#### Figure 1: Avaya IP Telephony Network and Telia Norway SIP Trunk

Note: The compliance testing was done over the internet, but Telia Norway only provide SIP trunking service over private Telia Norway access network services.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	7 of 104
SPOC 4/3/2022	©2022 Avaya Inc. All Rights Reserved.	TN_CMSM81SBC81

# 4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components			
Equipment/Software	Release/Version		
Avaya Aura <sup>®</sup> Communication Manager	8.1.3.3.0.890.27168		
running on VMware <sup>®</sup> -based Avaya appliance			
Avaya G450 Media Gateway	HW2 FW41.16		
– MM711AP Analog	HW46 FW096		
– MM712AP Digital	HW10 FW014		
– MM710AP	HW5 FW020		
Avaya Aura <sup>®</sup> Session Manager	8.1.3.3.813310		
running on VMware <sup>®</sup> -based Avaya appliance			
Avaya Aura <sup>®</sup> System Manager	8.1.3.3		
running on VMware <sup>®</sup> -based Avaya appliance	Build 8.1.0.0.733078		
	Revision 8.1.3.3.1013529 SP3		
Avaya Aura <sup>®</sup> Messaging	7.2 SP2		
running on VMware <sup>®</sup> -based Avaya appliance			
Avaya Aura <sup>®</sup> Media Server	8.0.2.43		
running on VMware <sup>®</sup> -based Avaya appliance			
Avaya Session Border Controller for Enterprise	8.1.3.0-31-21052		
running on VMware <sup>®</sup> -based Avaya appliance			
Avaya Aura® Experience Portal running on	8.1.0.0.0223		
VMware <sup>®</sup> -based Avaya appliance			
Avaya 9621G IP Deskphone (SIP)	Avaya <sup>®</sup> Deskphone SIP 7.1.14.2		
Avaya 9621G IP Deskphone (H.323)	Avaya <sup>®</sup> IP Deskphone		
	6.8.5.1		
Avaya 9641 IP Deskphone (H.323)	Avaya <sup>®</sup> IP Deskphone		
	6.8.5.1		
Avaya Digital Deskphone (1408D)	R48		
Avaya Workplace Client for Windows (SIP)	3.23.0.64		
Avaya one-X <sup>®</sup> Communicator (H.323 & SIP)	6.2.14.15-SP14P7		
Avaya Agent for Desktop (SIP)	2.0.6.5.3003		
Avaya Analog Deskphone	N/A		
VentaFax	7.10.258.664		
Telia Norway SIP T	runk Components		
Equipment/Software	Release/Version		
Metaswitch Perimeta SBC	V4.9.30		

#### **Table 1: Equipment and Software Tested**

The specific configuration above was used for the compliance test. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

**Note**: It is assumed the general installation of VMware<sup>®</sup>- based Avaya Appliance Virtualization Platform, Avaya Aura<sup>®</sup> Communication Manager, Avaya Aura<sup>®</sup> System Manager, Avaya Aura<sup>®</sup> Session Manager, Avaya Aura<sup>®</sup> Experience Portal, Avaya Aura<sup>®</sup> Messaging, Avaya Aura<sup>®</sup> Media Server and Avaya Media Gateway has been previously completed and is not discussed in this document.

# 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for Telia Norway SIP Trunk.

The 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.

## 5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 4000 SIP trunks are available and 100 are in use. 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.

display system-parameters customer-options OPTIONAL FEATURES			<b>2</b> of 12
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	4000	0	
Maximum Concurrently Registered IP Stations:	1000	1	
Maximum Administered Remote Office Trunks:		0	
Maximum Concurrently Registered Remote Office Stations:		0	
Maximum Concurrently Registered IP eCons:	68	0	
Max Concur Registered Unauthenticated H.323 Stations:		0	
Maximum Video Capable Stations:		0	
Maximum Video Capable IP Softphones:		5	
Maximum Administered SIP Trunks:		100	
Maximum Administered Ad-hoc Video Conferencing Ports:		0	
Maximum Number of DS1 Boards with Echo Cancellation:		0	

Figure 2: System-Parameters Customer-Options Form – Page 2

On Page 4, verify that ARS is set to y.

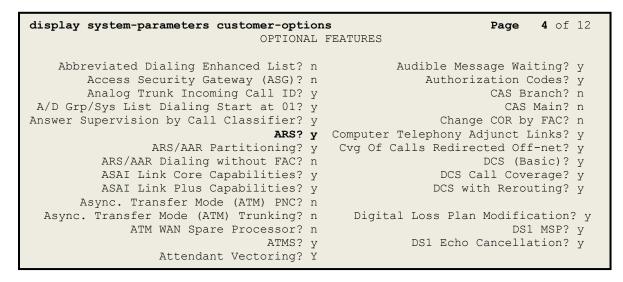


Figure 3: System-Parameters Customer-Options Form – Page 4

On Page 6, verify that Private Networking and Processor Ethernet are set to y.

```
6 of 12
display system-parameters customer-options
                                                                Page
                               OPTIONAL FEATURES
               Multinational Locations? n
                                                      Station and Trunk MSP? y
Multiple Level Precedence & Preemption? n
                                              Station as Virtual Extension? y
                    Multiple Locations? n
                                            System Management Data Transfer? n
         Personal Station Access (PSA)? y
                                                        Tenant Partitioning? y
                        PNC Duplication? n
                                                Terminal Trans. Init. (TTI)? y
                                                        Time of Day Routing? y
                  Port Network Support? n
                                               TN2501 VAL Maximum Capacity? y
                       Posted Messages? y
                                                       Uniform Dialing Plan? y
                    Private Networking? y
                                              Usage Allocation Enhancements? y
              Processor and System MSP? y
                    Processor Ethernet? y
                                                         Wideband Switching? y
                                                                    Wireless? n
                         Remote Office? y
         Restrict Call Forward Off Net? y
                 Secondary Data Module? y
```

Figure 4: System-Parameters Customer-Options Form – Page 6

### 5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** for allowing inbound calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to be transferred back to the PSTN then leave the field set to **none**.

```
change system-parameters featuresPage1 of19FEATURE-RELATED SYSTEM PARAMETERS<br/>Self Station Display Enabled? nTrunk-to-Trunk Transfer: allAutomatic Callback with Called Party Queuing? nAutomatic Callback - No Answer Timeout Interval (rings): 3<br/>Call Park Timeout Interval (minutes): 10Off-Premises Tone Detect Timeout Interval (seconds): 20<br/>AAR/ARS Dial Tone Required? y
```

#### Figure 5: System-Parameters Features Form – Page 1

On **Page 9**, verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **anonymous** for both. The value of **anonymous** is replaced for restricted numbers and unavailable numbers (refer to **Section 5.8**).

```
Page 9 of 19
change system-parameters features
                       FEATURE-RELATED SYSTEM PARAMETERS
CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
  CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous
DISPLAY TEXT
                                      Identity When Bridging: principal
                                       User Guidance Display? n
Extension only label for Team button on 96xx H.323 terminals? n
INTERNATIONAL CALL ROUTING PARAMETERS
          Local Country Code:
         International Access Code:
SCCAN PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n
CALLER ID ON CALL WAITING PARAMETERS
    Caller ID on Call Waiting Delay Timer (msec): 200
```

#### Figure 6: System-Parameters Features Form – Page 9

### 5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP Addresses as below:

- Media Server: Name: AMS, IP Address: 10.33.10.47
- Session Manager: Name: bvwasm2, IP Address: 10.33.10.53
- Communication Manager: Name: procr, IP Address: 10.33.10.54

These node names will be needed for defining the service provider signaling group in **Section 5.7**.

```
2
change node-names ip
                                                           Page 1 of
                               IP NODE NAMES
                  IP Address
Name
AMS
                 10.33.10.47
                 10.33.10.53
bvwasm2
default
                 0.0.0.0
procr
                 10.33.10.54
procr6
                  ::
```

#### Figure 7: Node-Names IP Form

### 5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. In the compliance test, **ip-codec-set 1** was used for this purpose. Telia Norway supports the **G.711A**, **G.711MU**, **G.729A** codecs. The **Media Encryption** was set as **1-srtp-aescm128-hmac80**, **2-srtp-aescm128-hmac32**, **none** in order priority. Default values can be used for all other fields.

```
        Audio
        Silence
        Frames
        Packet
        Audio
        Silence
        Frames
        Packet
        Audio
        Silence
        Size(ms)
        I
        I
        G.711A
        n
        2
        20
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I
        I</
```

#### Figure 8: IP-Codec-Set Form – Page 1

HV; Reviewed: SPOC 4/3/2022

Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved. On Page 2, set the FAX Mode to t.38-G711-fallback.

```
change ip-codec-set 1
                                                                       2 of 2
                                                                Page
                          IP CODEC SET
                              Allow Direct-IP Multimedia? n
                        ModeRedundancyPackett.38-G711-fallback0ECM: y FB-Timer: 4
                                                                   Packet Size(ms)
   FAX
   Modem
                        off
                                             0
   TDD/TTY
                        US
                                             3
   H.323 Clear-channel n
                                             0
                                             0
    SIP 64K Data
                                                                                20
                        n
```

Figure 9: IP-Codec-Set Form – Page 2

## 5.5. IP Network Region for Media Gateway, Media Server

Network region provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, both Avaya G450 Media Gateway and Avaya Media Server were tested and used region 1. For the compliance test, IP network region 1 was chosen for the service provider trunk.

Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **bvwdev.com**. This name appears in the From header of SIP messages originating from this IP region
- Enter a descriptive name in the **Name** field
- Enable IP-IP Direct Audio (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media Gateway or Avaya Media Server. Set both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes**. Shuffling can be further restricted at the trunk level on the Signaling Group form in **Section 5.7**
- Set the Codec Set field to the IP codec set defined in Section 5.4
- Default values can be used for all other fields

```
change ip-network-region 1
                                                              Page 1 of 20
                              TP NETWORK REGION
 Region: 1
Location: 1
                 Authoritative Domain: bvwdev.com
   Name: procr
                               Stub Network Region: n
MEDIA PARAMETERS
     PARAMETERS
Codec Set: 1
                              Intra-region IP-IP Direct Audio: yes
                             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
```

#### Figure 10: IP-Network-Region Form

Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved. The following display command shows that **media-gateway 1** is an Avaya G450 Media Gateway configured for Network Region 1. It can also be observed that the Controller IP Address is the Avaya Processor Ethernet (10.33.10.54), and that the gateway MGP IPv4 Address is 10.33.10.15. These fields are not configured in this screen, but just display the current information for the Media Gateway.

```
display media-gateway 1
                                                               Page 1 of
                                                                            2
                            MEDIA GATEWAY 1
                   Type: g450
                   Name: g450
             Serial No: 12TGXXX00244
   Link Encryption Type: any-ptls/tls Enable CF? n
         Network Region: 1
                                           Location: 1
                                           Site Data:
          Recovery Rule: none
             Registered? y
  FW Version/HW Vintage: 41 .16 .0 /2
       MGP IPV4 Address: 10.33.10.15
       MGP IPV6 Address:
  Controller IP Address: 10.33.10.54
            MAC Address: 3c:4a:73:6b:c5:a8
  Mutual Authentication? optional
```

Figure 11: Media Gateway – Page 1

The following screen shows Page 2 for Media Gateway 1. The gateway has an MM712 media module supporting Avaya digital phones in slot V1, an MM711 supporting analog phones on slot V2, and the capability to provide announcements and music on hold via "gatewayannouncements" in logical slot V9.

```
display media-gateway 1
                                                                  Page 2 of
                                                                                2
                             MEDIA GATEWAY 1
                                 Type: g450
      Module Type
MM712
                                                       DSP Type FW/HW version
MP80 170 7
Slot
                              Name
V1:
                              DCP MM
V2:
      MM711
                              ANA MM
V3:
V4:
V5:
V6:
V7:
V8:
                                                     Max Survivable IP Ext: 8
V9:
       gateway-announcements ANN VMM
```

Figure 12: Media Gateway – Page 2

HV: Reviewed:

SPOC 4/3/2022

Solution & Interoperability Test Lab Application Notes	16 of 104
©2022 Avaya Inc. All Rights Reserved.	TN_CMSM81SBC81

The following display command shows that **media-server 1** is an Avaya Media Server configured for **Network Region 1**. It can also be observed that the **Node Name: AMS** (Defined in **Section 5.3**) and the **Signaling Group: 11** (Defined in **Section 5.7**) have been used. These fields are not configured in this screen, but just display the current information for the Media Server.

```
display media-server 1

MEDIA SERVER

Media Server ID: 1

Signaling Group: 11

Voip Channel License Limit: 80

Dedicated Voip Channel Licenses: 80

Mode Name: AMS

Note Name: AMS

Decation: 1

Announcement Storage Area: ANNC-44de7b8-ade78-0000c29acfea
```

Figure 13: Media Server

## 5.6. Configure IP Interface for procr

Use the **change ip-interface procr** command to change the Processor Ethernet (procr) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the procr for SIP Trunk signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones. Ensure **Enable Interface** is **y** and **Network Region** is **1**.

```
      change ip-interface procr
      IP INTERFACES

      IP INTERFACES
      Target socket load: 4800

      Enable Interface? y
      Allow H.323 Endpoints? y<br/>Allow H.248 Gateways? y<br/>Gatekeeper Priority: 5

      Network Region: 1
      IPV4 PARAMETERS

      Node Name: procr<br/>Subnet Mask: /24
      IP Address: 10.33.10.54
```

#### Figure 14: IP-Interface Form

## 5.7. Signaling Group

Use the **add signaling-group** command to create signaling groups.

For the compliance test, signaling group **20** was used for the signaling group between Communication Manager and Session Manager. It was used for outbound and inbound calls between the service provider and the enterprise. It was configured using the parameters highlighted below. Note: The signaling group between Communication Manager and Session Manager used for SIP phones, Messaging are not mentioned in these Application Notes.

- Set the Group Type field to sip
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager
- Set the **Transport Method** to the value of **tls** (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager
- Set the Near-end Node Name to procr. This node name maps to the IP Address of Communication Manager as defined in Section 5.3
- Set the **Far-end Node Name** to **bvwasm2**. This node name maps to the IP Address of Session Manager as defined in **Section 5.3**
- Set the Near-end Listen Port and Far-end Listen Port to a valid unused port for TLS, such as 5061

- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**
- Set the **Far-end Domain** to **bvwdev.com**, the enterprise domain
- Set **Direct IP-IP Audio Connections** to **y**. This setting will enable media shuffling on the SIP trunk so that Communication Manager will re-route media traffic directly between the SIP trunk and the enterprise endpoint. Note that the Avaya G450 Media Gateway or Avaya Media Server will not remain in the media path of all calls between the SIP trunk and the endpoint
- Set the Alternate Route Timer (sec) to 6. This defines the number of seconds Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval
- Default values may be used for all other fields

Page 1 of 2 add signaling-group 20 SIGNALING GROUP Group Number: 20 IMS Enabled? n Tran Group Type: sip Transport Method: tls Q-SIP? n IP Video? n Enforce SIPS URI for SRTP? y Peer Detection Enabled? y Peer Server: SM Prepend '+'to Outgoing Calling/Alerting/Diverting/connected Public Numbers? y Remove '+' from Incoming Called/Calling/Alerting/Diverting/connected Numbers? n Near-end Node Name: procr Near-end Listen Port: 5061 Far-end Node Name: bywasm2 Far-end Listen Port: 5061 Far-end Network Region: 1 Far-end Secondary Node Name: Far-end Domain: bvwdev.com Bypass If IP Threshold Exceeded? n Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload Session Establishment Timer(min): 3 IP Audio Connections? y IP Audio Hairpinning? n Enable Layer 3 Test? y Initial IP-IP Direct Media? n H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6

#### Figure 15: Signaling-Group 20

For the compliance test, signaling group **11** was used for the signaling group between Communication Manager and Media Server. It was configured using the parameters highlighted below.

- Set the Group Type field to sip
- Set the **Transport Method** to the value of **tls** (Transport Layer Protocol). The transport method specified here is used between Communication Manager and Media Server
- Set the **Peer Detection Enabled** field to **n** and **Peer Server** to **AMS**
- Set the Near-end Node Name to procr. This node name maps to the IP Address of Communication Manager as defined in Section 5.3

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	19 of 104
SPOC 4/3/2022	©2022 Avaya Inc. All Rights Reserved.	TN_CMSM81SBC81

- Set the **Far-end Node Name** to **AMS**. This node name maps to the IP Address of Media Server as defined in **Section 5.3**
- Set the Near-end Listen Port to 9061 and Far-end Listen Port to a valid unused port for TLS, such as 5071
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**
- Set the Far-end Domain to 10.33.10.47 (This is Media Server IP Address)

```
      change signaling-group 11
      Page 1 of 2

      SIGNALING GROUP
      SIGNALING GROUP

      Group Number: 11
      Group Type: sip
Transport Method: tls

      Peer Detection Enabled? n Peer Server: AMS

      Near-end Node Name: procr
Near-end Listen Port: 9061

      Far-end Node Name: contraction for the server: frame the server the serv
```

#### Figure 16: Signaling-Group 11

### 5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group for Session Manager created in **Section 5.7**.

For the compliance test, trunk group **20** was used for both outbound and inbound calls to the service provider. It was configured using the parameters highlighted below.

- Set the Group Type field to sip
- Enter a descriptive name for the Group Name
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field. (e.g., **\*020**). Note: Refer to **Section 5.10** for adding \* in dialing plan
- Set Class of Restriction (COR) to 1
- Set **Direction** to **two-way** for trunk group **20**
- Set the **Service Type** field to **public-ntwrk**
- Set Member Assignment Method to auto
- Set the **Signaling Group** to the signaling group configured in **Section 5.7**. Trunk group 20 was associated to signaling group 20
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk
- Default values were used for all other fields

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes
SPOC 4/3/2022	©2022 Avaya Inc. All Rights Reserved.

add trunk-group 20 Page 1 of 4				
	TRUNK GROUP			
Group Number: 20	Group Type: sip CDR Reports: y			
Group Name: SIP Trunks	COR: 1 TN: 1 TAC: *020			
Direction: two-way	Outgoing Display? n			
Dial Access? n	Night Service:			
Queue Length: 0				
Service Type: public-ntwrk	Auth Code? n			
	Member Assignment Method: auto Signaling Group: 20 Number of Members: 50			

Figure 17: Trunk-Group – Page 1

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to the service provider. This value defines the interval that UPDATEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

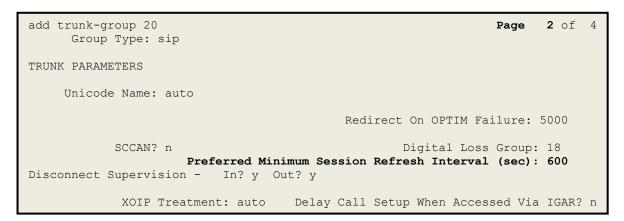


Figure 18: Trunk-Group – Page 2

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end (refer to **Section 5.9** for the public-unknown-numbering format). The compliance test used 10-digit numbering format. Thus, **Numbering Format** was set to **public** and the **Numbering Format** field in the route pattern was set to **public** unk (see **Section 5.10**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to y. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2** if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if an enterprise user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

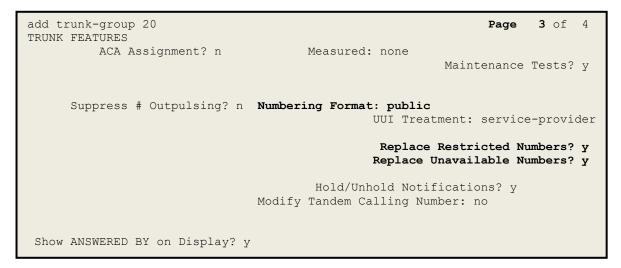


Figure 19: Trunk-Group – Page 3

On **Page 4**, the **Network Call Redirection** field should be set to **n** so that Communication Manager will not send SIP REFER, Telia Norway does not support SIP REFER in off-net call redirection.

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **y**. Note: For voice mail purposes, Communication Manager sends SIP Invite with History Info to Avaya Aura Messaging.

add trunk-group 20 PROTOCOL VARIATIONS	<b>Page 4</b> of 4
Mark Users as Phone? Prepend '+' to Calling/Alerting/Diverting/Connected Number? Send Transferring Party Information? Network Call Redirection?	n n
Send Diversion Header? Support Request History? Telephone Event Payload Type:	y Y
Convert 180 to 183 for Early Media? Always Use re-INVITE for Display Updates? Identity for Calling Party Display: Block Sending Calling Party Location in INVITE? Accept Redirect to Blank User Destination? Enable Q-SIP? Interworking of ISDN Clearing with In-Band Tones:	n P-Asserted-Identity n n n

Figure 20: Trunk-Group – Page 4

## 5.9. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "P-Asserted-Identity" headers. Since public numbering was selected to define the format of this number (Section 5.8), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs), and it is used to authenticate the caller.

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single public-unknown-numbering entry can be applied for all extensions. In the compliance test, stations with a 4-digit extension beginning with **45** will send the calling party number as the **CPN Prefix** plus the extension number.

**Note**: The entry applies to SIP connection to Session Manager, therefore the resulting number must be a complete E.164 number. Communication Manager automatically inserts a '+' in front of user number in From, P-Asserted-Identity, Contact, and Diversion headers.

change public-unknown-numbering 0 Page 1 of 2 NUMBERING - PUBLIC/UNKNOWN FORMAT				
			Total	
Ext Ext	Trk	CPN	CPN	
Len Code	Grp(s)	Prefix	Len	
			Total Administered: 1	
			Maximum Entries: 240	
4 45	20	473XXX	10	
			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.	

Figure 21: Public-Unknown-Numbering Form

## 5.10. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit **9** is used as the ARS access code. Enterprise callers will dial **9** to reach an "outside line". This configuration is illustrated below. Use the **change dialplan analysis** command to define the **Dialed String** as following:

- **Dialed String** beginning with **45** for extension (**ext**)
- **Dialed String** beginning with **48** for extension (**udp**)
- **Dialed String** beginning with **9** for feature access code (**fac**)
- **Dialed String** beginning with \* for dial access code (**dac**). It is used for Trunk Access Code (TAC) defined on Trunk Group 20 in **Section 5.8**

change dialplan analys:	s	Page 1 of 12
	DIAL PLAN ANALYSIS TABLE Location: all	E Percent Full: 2
189       4       e         3       4       e         45       4       e         48       4       u         800       4       e         9       1       f	e String Length Type et t t t	Dialed Total Call String Length Type

Figure 22: Dialplan–Analysis Form

Use the **change feature-access-codes** command to configure **9** as the **Auto Route Selection** (**ARS**) – **Access Code 1**.

change feature-access-codes	Page	1 of	11
FEATURE ACCESS CODE (FAC)	-		
Abbreviated Dialing List1 Access Code:			
Abbreviated Dialin3g List2 Access Code:			
Abbreviated Dialing List3 Access Code:			
Abbreviated Dial - Prgm Group List Access Code:			
Announcement Access Code: *111			
Answer Back Access Code:			
Attendant Access code:			
Auto Alternate Routing (AAR) Access Code:			
Auto Route Selection (ARS) - Access Code 1: 9 Access Cod	e 2:		
Automatic Callback Activation: Deactivation	:		
Call Forwarding Activation Busy/DA: All: Deactivation	:		
Call Forwarding Enhanced Status: Act: Deactivation	:		
Call Park Access Code:			
Call Pickup Access Code:			
CAS Remote Hold/Answer Hold-Unhold Access Code:			
CDR Account Code Access Code:			
Change COR Access Code:			
Change Coverage Access Code:			
Conditional Call Extend Activation: Deactivat	ion:		
Contact Closure Open Code: Close Cod	e:		

Figure 23: Feature–Access-Codes Form

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit **9**. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to **Route Pattern 20** which contains the SIP trunk group to the service provider (as defined next).

change ars analysis	0						Page	1 of	2
			ARS DIGIT A Locat	ANALYSIS			Percent Fi	ıll: 1	
Dialed String 1613 47	Tot Min <b>11</b> 2	al Max 11 10	Route Pattern 20 20	Call Type <b>pubu</b> pubu	Node Num	ANI Reqd <b>n</b> <b>n</b>			

Figure 24: ARS-Analysis Form

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used in route pattern **20** for the compliance test.

- **Pattern Name**: Enter a descriptive name
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **20** was used
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Inserted Digits**: Enter the single digit **p** which is used for fully qualified E.164 numbers. Communication Manager inserts a plus (+) digit to the digit.
- **Numbering Format**: Set this field to **pub-unk** since public-unknown-numbering format should be used for this route (see **Section 5.8**)

change route-pattern 20 Page 1 of 3 Pattern Number: 5 Pattern Name: SP SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Intw Dgts 1: 20 0 n user p 2: n user user 3: n 4: n user 5: n user 6: user n BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR 0 1 2 M 4 W Request Dgts Format Subaddress 1: yyyyyn n rest pub-unk none 2: ууууул п rest none 3: yyyyyn n rest none 4: y y y y y n n rest none 5: y y y y y n n rest none rest none 6: ууууул п

#### Figure 25: Route–Pattern Form

Use the **change cor 1** command to change the Class of Restriction (COR) for the outbound call over SIP trunk. Set **Calling Party Restriction**: **none**. This setting allows the outbound call using feature access code (fac) 9 over SIP trunks.

change cor 1 Page 1 of 23 CLASS OF RESTRICTION COR Number: 1 COR Description: FRL: 0 APLT? y Can Be Service Observed? n Calling Party Restriction: none Can Be A Service Observer? n Called Party Restriction: none Forced Entry of Account Codes? n Time of Day Chart: 1 Direct Agent Calling? n Facility Access Trunk Test? n Priority Queuing? n Restriction Override: none Restricted Call List? n Can Change Coverage? n Access to MCT? y Fully Restricted Service? n Group II Category For MFC: 7 Hear VDN of Origin Annc.? n Send ANI for MFE? n Add/Remove Agent Skills? n MF ANI Prefix: Automatic Charge Display? n Hear System Music on Hold? y PASTE (Display PBX Data on Phone)? n Can Be Picked Up By Directed Call Pickup? n Can Use Directed Call Pickup? n Group Controlled Restriction: inactive

Figure 26: Class of Restriction Form

HV; Reviewed: SPOC 4/3/2022

Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved. 28 of 104 TN\_CMSM81SBC81

# 5.11. Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by the service provider is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group **20**. Use the **change inc-call-handling-trmt trunk-group 20** to convert incoming DID numbers as follows:

- The incoming DID number +473XXX4504 to 1810 by deleting 11 of the incoming digits for voicemail testing purpose. (1810 is voice mail pilot number)
- The incoming DID number +473XXX4507 to 4800 by deleting 11 of the incoming digits for Experience Portal testing purpose
- The incoming DID number +473XXX to 4-digit extension by deleting 7 of the incoming digits for inbound call testing purpose.

change inc-call-h	handling-trm	t trunk-group 20		Page	1 of	3
INCOMING CALL HANDLING TREATMENT						
Service/	Number	Number	Del Insert			
Feature	Len	Digits				
public-ntwrk	11	+473XXX4504	11 1810			
public-ntwrk	11	+473XXX4507	11 4800			
public-ntwrk	11	+473XXX	7			

Figure 27: Inc-Call-Handling-Trmt Form

## 5.12. Contact Center Configuration

This section describes the basic commands used to configure Announcements, Hunt-Groups, Vector Directory Numbers (VDNs) and corresponding vectors. These vectors contain steps that invoke Communication Manager to perform various call-related functions.

### 5.12.1. Announcements

Various announcements will be used within the vectors. In the sample configuration, these announcements were sourced by the Avaya G450 Media Gateway. The following abridged list command summarizes the announcements used in conjunction with the vectors in this section. To add an announcement extension, use the command "add announcement <extension>". The extension is an unused extension number.

list announcement				
Announcement	ANNOU	JNCEMENTS/AUDIO SOUR	CES	Num of
Extension 1898	Type integrated	Name	Source 001V9	Files
1899	integrated		001V9	1

#### Figure 28: Announcement Configuration

### 5.12.2. ACD Configuration for Call Queued for Handling by Agent

This section provides a simple example configuration for VDN, vector, hunt-group, and agent-loginID used to queue inbound calls for handling by an agent.

The following screens show an example ACD hunt group. On page 1, note the bolded values.

display <b>hunt-group 13</b>	Page 1 of 3
HUNT GROUP	
GROUP NUMBER: 13 Group Name: SP	ACD? Y Queue? Y
GROUP EXTENSION: 3211	Vector? y
GROUP TYPE: UCD-MIA	-
TN: 1	
COR: 1	MM Early Answer? n
SECURITY CODE: 1234 Local Agent	Preference? n
ISDN/SIP Caller Display:	
Queue Limit: unlimited Calls Warning Threshold: Port: Time Warning Threshold: Port:	

#### **Figure 29: Hunt Group Configuration – Page 1**

HV; Reviewed: SPOC 4/3/2022 Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved. The following screens show an example ACD hunt group. On the abbreviated page 2 shown below, note that **Skill** is set to **y**.

display hunt-group 13		Page	2 of	3
	HUNT GROUP			
Skill? y	Expected Call Handling Time (sec)			
AAS? n	Service Level Target (% in sec):	80 in 2	0	

### Figure 30: Hunt Group Configuration – Page 2

VDN 4506, shown below, is associated with vector 3

display vdn 4506	VECTOR DIRECTORY NUMBER		Page	1 of	3
	EXTENSION: 4506 Name*: Contact Center DESTINATION: VECTOR NUMBER	3			
	Attendant Vectoring? n Meet-me Conferencing? n Allow VDN Override? n	2			
	COR: 1 TN*: 1 Measured: none				

Figure 31: VDN Configuration

In this simple example, vector 3 briefly plays ring back, then plays announcement 1899 (Step 02). This is an announcement heard when the call is first answered before the call is queued to the skill 13 (Step 03). If an agent is immediately available to handle the call, the call will be delivered to the agent. If an agent is not immediately available, the call will be queued, and the caller will hear announcement 1898 (Step 05). Once an agent becomes available, the call will be delivered to the agent.

display vector 3 Page 1 of 6 CALL VECTOR Name: Contact Center Number: 3Name: Contact CenterMultimedia? nAttendant Vectoring? nMeet-me Conf? n Lock? n Basic? y EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y Prompting? y LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y Variables? y 3.0 Enhanced? y 01 wait-time 2 secs hearing ringback 02 announcement 1899 03 queue-to skill 13 pri m 04 wait-time 2 secs hearing silence 05 announcement 1898 06 goto step 3 if unconditionally

#### Figure 32: Vector 3 Configuration

The following screen illustrates an example agent-loginID 3311. In the sample configuration, an Avaya IP Deskphone logged in using agent-loginID 3311 and the configured password to staff and take a call for skill 13.

```
add agent-loginID 3311
                                                              Page 1 of
                                                                             2
                                  AGENT LOGINID
                Login ID: 3311
                                                                   AAS? n
                    Name: SP
                                 LWC Reception. -
LWC Log External Calls? n
AUDIX Name for Messaging:
                                                                 AUDIX? n
                      TN: 1
                                                       LWC Reception: spe
                     COR: 1
           Coverage Path:
           Security Code: 1234
                                         LoginID for ISDN/SIP Display? n
                                                             Password: 1234
                                               Password (enter again): 1234
                                                          Auto Answer: station
                                                    MIA Across Skills: system
                                            ACW Agent Considered Idle: system
                                            Aux Work Reason Code Type: system
                                              Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                             Forced Agent Logout Time:
```

#### Figure 33: Agent-loginID Configuration – Page 1

HV; Reviewed: SPOC 4/3/2022

Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved. The following abridged screen shows Page 2 for agent-loginID 3311. Note that the Skill Number (SN) has been set to 13.

```
Display agent-loginID 3311

AGENT LOGINID

Direct Agent Skill:

Call Handling Preference: skill-level

SN RL SL SN RL SL

1: 13 1 16:

2: 17:
```

#### Figure 34: Agent LoginID Configuration – Page 2

To enable a telephone or one- $X^{\otimes}$  Agent client to log in with the agent-loginID shown above, ensure that **Expert Agent Selection (EAS) Enabled** is set to **y** as shown in the screen below.

```
change system-parameters features Page 11 of 19
FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
EAS
Expert Agent Selection (EAS) Enabled? y
Minimum Agent-LoginID Password Length: 4
```

#### Figure 35: Enable Expert Agent Selection

2 of

Page

Service Objective? n

Local Call Preference? n

2

## 5.13. Avaya Aura<sup>®</sup> Communication Manager Stations

In the sample configuration, a 4-digit station extension was used with the format 4500. Use the **add station 4500** command to add an Avaya H.323 IP Deskphone.

- Enter Type: 9621, Name: H323-4500, Security Code: 1234, Coverage Path 1: 1, IP SoftPhone: y (if using this extension as a Softphone such as Avaya one-X<sup>®</sup> Communicator)
- Leave other values as default

add station 4500 Page 1 of 5 STATION Extension: 4500 Lock Messages? n BCC: 0 Security Code: \* Coverage Path 1: 1 Coverage Path 2: nt-to Station: Type: 9621 TN: 1 COR: 1 COS: 1 Port: S000055 Name: H323-4500 Tests? v Hunt-to Station: STATION OPTIONS Time of Day Lock Table: Loss Group: 19 Personalized Ringing Pattern: 1 Speakerphone: 2-way Display Language: English able GK Node Name Message Lamp Ext: 4500 Survivable GK Node Name: Survivable COR: internal Media Complex Ext: Survivable Trunk Dest? y IP SoftPhone? y IP Video softphone? n Short/Prefixed Registration Allowed: default Customizable Labels?  ${f y}$ 

#### Figure 36: Add-Station Form

### 5.14. Save Avaya Aura<sup>®</sup> Communication Manager Configuration Changes

Use the **save translation** command to save the configuration.

# 6. Configure Avaya Aura<sup>®</sup> Session Manager

This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP Domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Time Ranges, which define the time-based-routing
- Routing Policies, which define route destinations and control call routing between the SIP Entities
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call

It may not be necessary to create all the items above when configuring 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. Avaya Aura<sup>®</sup> System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL as **https://<ip-address>/SMGR**, where **<ip-address>** is the IP Address of System Manager. At the **System Manager Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button (not shown). The initial screen shown below is then displayed.

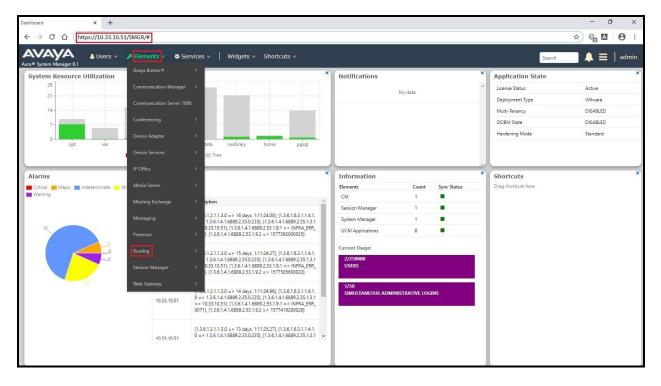


Figure 37: System Manager Home Screen

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

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

System Manager 8.1	Lusers v ≯ Elements v & Services v   Widgets v Shortcuts v Search ↓ ≡   adm
me Routing	
	Administration of Session Manager Routing Policies
Domains	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:
Locations	Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
Conditions	Step 2: Create "Locations"
	Step 3: Create "Conditions" (If Flexible Routing or Regular Expression Adaptations are in use)
Adaptations	Step 4: Create "Adaptations"
SIP Entities	Step 5: Create "SIP Entities"
Entity Links	- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
Entry Entrs	- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
Time Ranges	- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
Routing Policies	Step 6: Create the "Entity Links"
	- Between Session Managers
Dial Patterns	- Between Session Managers and "other SIP Entities"
Regular Expressions	Step 7: Create "Time Ranges"
	- Align with the tariff information received from the Service Providers
Defaults	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"
	Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".
	IMPORTANT: the appropriate dial patterns are defined and assigned after "Routing Policies" using "Dial patterns". That's why this overall routing workflow can be interpreted as
	"Dial Pattern driven approach to define Routing Policies"
	That means (with regard to steps listed above):
	Step 8: "Routing Polices" are defined
	Step 9: "Dial Patterns" are defined and assigned to "Routing Policies" and "Locations" (one step)
	Step 10: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

#### **Figure 38: Network Routing Policy**

# 6.2. Specify SIP Domain

Create a SIP Domain for each domain of which Session Manager will need to be aware of in order to route calls. For the compliance test, this includes the enterprise domain **bvwdev.com**.

Navigate to **Routing**  $\rightarrow$  **Domains** in the left-hand navigation pane and click the **New** button in the right pane. In the new right pane that appears (not shown), fill in the following:

- **Name**: Enter the domain name
- **Type**: Select **sip** from the pull-down menu
- Notes: Add a brief description (optional)

Click **Commit** (not shown) to save.

The screen below shows the existing entry for the enterprise domain.

Aura® System Manager 8.1	Users → 🖌 Elements → 🗣 Services → 📔 Widgets → Shortcuts →	🔺 🗮   admin
Home Routing		
Routing	Domain Management	Help ?
Domains	New Edit Delete Duplicate More Actions •	
Locations	1 Rem 🗇	Filter: Enable
Conditions	Name Type Notes	
Adaptations ×	bywdev.com sip Select : All, None	

**Figure 39: Domain Management** 

## 6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Belleville-GSSCP**, which includes all equipment in the enterprise including Communication Manager, Session Manager and Avaya SBCE.

To add a Location, navigate to **Routing**  $\rightarrow$  **Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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)

Click Commit to save.

AVAYA Aura® System Manager 8.1	▲ Users × 🖌 Elements × 🌣 Services × 📔 Widgets × Shortcut		Search 🔔 🚍 🛛 admin
Home Routing			
Routing	Location Details	Commit Cancel	Help ?
Domains	General		
Locations		Belleville-GSSCP	
Conditions	Notes:		
Adaptations	<ul> <li>Dial Plan Transparency in Survivable Mode</li> </ul>		
SIP Entities	Enabled:		
Entity Links	Listed Directory Number:		
Time Ranges	Associated CM SIP Entity:		
Routing Policies	Overall Managed Bandwidth		
Dial Patterns	Managed Bandwidth Units:	Kbit/sec •	
	Total Bandwidth:		
Regular Expressions	Multimedia Bandwidth:		
Defaults	Audio Calls Can Take Multimedia Bandwidth:	8	
	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 Kblt/sec •	
	Alarm Threshold		
	Overall Alarm Threshold:	80 • %	
	Multimedia Alarm Threshold:	80 • %	
	* Latency before Overall Alarm Trigger:	5 Minutes	
<	* Latency before Multimedia Alarm Trigger:	5 Minutes	
	Location Pattern		

#### **Figure 40: Location Configuration**

HV; Reviewed: SPOC 4/3/2022

Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved. In the **Location Pattern** section, click **Add** to enter **IP Address Pattern**. The following patterns were used in testing:

- IP Address Pattern: 10.33.1.\*, 10.33.10.\*, 10.33.100.\*
- Click **Commit** to save

Loca	tion Pattern		
Add	Remove		
3 Iter	ms 🥲		
	IP Address Pattern	7	*
	* 10.33.1.*		
	* 10.33.10.*		
	* 10.33.100.*		
Selec	t : All, None		
		Commit Cancel	

#### Figure 41: IP Ranges Configuration

Note: Call bandwidth management parameters should be set per customer requirement.

#### 6.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager, which includes Communication Manager, Experience Portal and Avaya SBCE.

Navigate to **Routing**  $\rightarrow$  **SIP Entities** in the left-hand navigation pane and click on the New button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

In the General section, enter the following values. Use default values for all remaining fields.

•	Name:	Enter a descriptive name
٠	FQDN or IP Address	Enter the FQDN or IP Address of the SIP Entity that is
		used for SIP signaling
٠	Туре:	Select Session Manager for Session Manager, CM for
		Communication Manager, Voice Portal for Experience Portal and
		SIP Trunk for Avaya SBCE configuration
٠	Adaptation:	This field is only present if <b>Type</b> is not set to <b>Session Manager</b> .
		Adaptation modules were not used in this configuration
٠	Location:	Select the Location that applies to the SIP Entity being created. For
		the compliance test, all components were located in Location
		Belleville-GSSCP
٠	Time Zone:	Select the time zone for the Location above

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	40 of 104
SPOC 4/3/2022	©2022 Avaya Inc. All Rights Reserved.	TN_CMSM81SBC81

In this configuration, there are four SIP Entities:

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Avaya Session Border Controller SIP Entity
- Experience Portal SIP Entity

#### 6.4.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **bvwasm2**. The IP Address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.10.53**. The user will need to select the specific values for the **Location** and **Time Zone**.

Aura® System Manager 8.1	Users ∨ 🖌 Elements ∨ 🌢 Services ∨   Widgets ∨ Shortcut	ls ∽ Search 🌲 🗮   admir	ń
Home Routing			
Routing	SIP Entity Details	Help 7 Commit: Cancel	•
Domains	General		
Locations	* Name: * IP Address:	bvwasm2	l
Conditions	SIP FQDN:		l
Adaptations ~	Type:	Session Manager	
SIP Entities	Notes:		l
Entity Links	Location:	Belleville-GSSCP *	
	Outbound Proxy:	×	
Time Ranges	Time Zone:	America/Toronto 🔹	
Routing Policies	Minimum TLS Version:	Use Global Setting *	
Dial Patterns 🗸 🗸	Credential name:		l
Regular Expressions	Monitoring SIP Link Monitoring:	Use Session Manager Configuration V	
Defaults		Use Session Manager Configuration V	

Figure 42: Session Manager SIP Entity

To define the ports used by Session Manager, scroll down to the **Listen Ports** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

In the **Listen Ports** section, click **Add** and enter the following values. Use default values for all remaining fields:

- Port: Port number on which Session Manager listens for SIP requests
- **Protocol**: Transport protocol to be used with this port
- **Default Domain**: The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain

Defaults can be used for the remaining fields. Click **Commit** (not shown) to save.

The compliance test used port **5061** with **TLS** for connecting to Communication Manager, to Avaya SBCE and to Experience Portal.

Listen Ports         TCP Failover port:         TLS Failover port:				
Add Remove				
4 Items 🍣				Filter: Enable
Listen Ports	*	Protocol Default Domain	Notes	
5061		TLS V bvwdev.com		
Select : All, None				

Figure 43: Session Manager SIP Entity Port

#### 6.4.2. Configure Communication Manager SIP Entity

The following screen shows the addition of the Communication Manager SIP Entity named **CM8**. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to Communication Manager, it is necessary to create a separate SIP Entity for Communication Manager in addition to the one created during Session Manager installation. The original SIP entity is used with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP Address of Communication Manager **10.33.10.54**. Note that **CM** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

AVAYA Aura® System Manager 8.1	Users ∨ 🖌 Elements ∨ 🌣 Services ∨   Widgets ∨ Shortcul	is v Search 🌲 🚍 🕴 admin
Home Routing		
Routing ^	SIP Entity Details	Commit Cancel
Locations	* Name: * FQDN or IP Address:	
Conditions	Туре:	CM •
Adaptations ~	Notes:	
SIP Entities	Adaptation:	
Entity Links		Belleville-GSSCP •
Time Ranges	* SIP Timer B/F (in seconds):	
Routing Policies	Minimum TLS Version:	Use Global Setting •
Dial Patterns 🗸 🗸	Credential name:	
	Securable:	
Regular Expressions	Call Detail Recording:	none
Defaults	Loop Detection Loop Detection Mode:	On v
	Loop Count Threshold:	
	Loop Detection Interval (in msec):	
	Monitoring	
		Link Monitoring Enabled
	* Proactive Monitoring Interval (in seconds):	900
	* Reactive Monitoring Interval (in seconds):	120
	* Number of Tries:	1
	* Number of Successes:	1
	CRLF Keep Alive Monitoring:	Use Session Manager Configuration *

Figure 44: Communication Manager SIP Entity

#### 6.4.3. Configure Avaya Session Border Controller SIP Entity

The following screen shows the addition of Avaya SBCE SIP entity named **SBCE**. The **FQDN** or **IP Address** field is set to the IP Address of the SBCE's private network interface **10.33.10.49**. Note that **SIP Trunk** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

AVAYA Aura® System Manager 8.1	Users ×	ts v Search 🌲 🚍   admin
Home Routing		
Routing ^ Domains	SIP Entity Details	Commit Cancel
Locations	General * Name:	
Conditions	* FQDN or IP Address: Type:	SIP Trunk
Adaptations 🗸	Notes:	
SIP Entities	Adaptation:	•
Entity Links		Belleville-GSSCP •
Time Ranges	* SIP Timer B/F (in seconds):	America/Toronto •
Routing Policies	Minimum TLS Version:	
	Credential name:	
Dial Patterns 🗸 🗸	Securable:	
Regular Expressions	Call Detail Recording:	egress T
Defaults	Loop Detection	
	Loop Detection Mode:	
	Loop Count Threshold:	
	Loop Detection Interval (in msec):	200
	Monitoring	
	2,24	Link Monitoring Enabled
	* Proactive Monitoring Interval (in seconds):	
	* Reactive Monitoring Interval (in seconds):	
	* Number of Tries:	
	* Number of Successes:	
	CRLF Keep Alive Monitoring:	Use Session Manager Configuration V

Figure 45: Avaya SBCE SIP Entity

## 6.4.4. Configure Avaya Aura<sup>®</sup> Experience Portal SIP Entity

The following screen shows the addition of the Avaya Experience Portal SIP entity named **Experience Portal**. The **FQDN** or **IP Address** field is set to the IP Address of the Experience Portal interface **10.33.1.23**. Note that **Voice Portal** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

Aura® System Manager 8.1	Users 🗸 🎤 Elements 🗸 🔹 Services 🗸   Widgets 🗸 Sł	nortcuts ~	
Home Routing			
Routing	SIP Entity Details		Commit
Domains	General		
Locations			Experience Portal
Conditions		* FQDN or IP Address:	10.33.1.23
	L L	Notes:	
Adaptations ~			
SIP Entities		Adaptation:	<b>v</b>
Entity Links			Belleville-GSSCP V
Time Ranges			America/Toronto 🗸
		imer B/F (in seconds):	
Routing Policies		Minimum TLS Version: Credential name:	ose Global Setting V
Dial Patterns 🛛 🗸 🗸		Securable:	с <u> </u>
Regular Expressions		Call Detail Recording:	
Defaults	Loop Detection	Loop Detection Mode:	On v
		Loop Count Threshold:	
	Loop Detecti	ion Interval (in msec):	200
	M		
	Monitoring	SIP Link Monitoring:	Use Session Manager Configuration 🗸
	CRLF	Keep Alive Monitoring:	Use Session Manager Configuration 🗸
	Supports (	Call Admission Control:	
	Share	d Bandwidth Manager:	
	Primary Session Manager B	andwidth Association:	~
	Backup Session Manager B	andwidth Association:	~
<	Entity Links		
		ansport with DNS SRV:	

**Figure 46: Experience Portal SIP Entity** 

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

## 6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Three Entity Links were created: one to Communication Manager for use only by the service provider traffic, one to the Avaya SBCE and one to the Experience Portal.

To add an Entity Link, navigate to **Routing**  $\rightarrow$  **Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

- Name: Enter a descriptive name
- **SIP Entity 1**: Select the Session Manager being used
- **Protocol**: Select the transport protocol used for this link
- **Port**: Port number on which Session Manager will receive SIP requests from the far-end
- SIP Entity 2: Select the name of the other system as defined in Section 6.4
- **Port**: Port number on which the other system receives SIP requests from the Session Manager
- Connection Policy: Select trusted. Note: If trusted is not selected, calls from the associated SIP Entity specified in Section 6.4 will be denied

Click **Commit** to save.

The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.7**.

Aura® System Manager 8.1	Users 🗸 🎤 Elements 🗸 🏘	Services 🗸   Widgets 🗸	Shortcuts ~					Search		▲ =	admin
Home Routing											
Routing	Entity Links			Con	nmit Cancel						Help ?
Domains	<b>_</b>										
Locations	1 Item 🥭									Filt	ter: Enable
Conditions	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes	
Adaptations 🗸 🗸	* SM_CM_TLS_5061	* Q bvwasm2	TLS V	* 5061	* Q CM8	* 5061		trusted <b>*</b>			
SIP Entities	Select : All, None										•
Entity Links											

Figure 47: Communication Manager Entity Link

The following screen illustrates the Entity Links to Avaya SBCE. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 7.5.1**, **7.6.1** and **7.9.3**.

AVAYA Aura® System Manager 8.1	Users 🗸 🎤 Elements 🗸 🔹 S	Services ->   Widgets -> S	hortcuts ~					Search		▲ =	admin
Home Routing											
Routing ^	Routing ^ Entity Links				Commit Cancel						
Domains											
Locations	1 Item 🍣									Fi	lter: Enable
Conditions	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes	
Adaptations 🗸 🗸	SM_SBCE_TLS_5061	* Q bywasm2	TLS V	* 5061	* Q SBCE	* 5061		trusted 🔻			
SIP Entities	Select : All, None										•
Entity Links											

Figure 48: Avaya SBCE Entity Link

The following screen illustrates the Entity Links to Experience Portal. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 8.3**.

Aura® System	Manager 8.1		sers 🗸 🎤 Elements 🗸 🔅	Services v   Widgets v	Shortcuts ~					
Home	Routing									
Routing		^	Entity Links			Commit Cano	el			
Dom	ains									
Locat	tions		1 Item							
Cond	litions		Name	SIP Entity 1	Prot	ocol Port	SIP Entity 2	Port	DNS Override	Connection Policy
Adap	tations	~	Select : All, None	O bywasm2	TL	♥ * 5061	* O Experience Portal	* 5061		trusted 💙
SIP E	ntities									
Entity	/ Links					Commit Canc	el			

**Figure 49: Experience Portal Entity Link** 

# 6.6. Configure Time Ranges

Time Ranges are configured for time-based-routing. In order to add a Time Range, select **Routing**  $\rightarrow$  **Time Ranges** and then click **New** button. The Routing Policies shown subsequently will use the 24/7 range since time-based routing was not the focus of these Application Notes.

Aura® System Manager 8.1	Users 🗸 🎤 Elements	s 🗸 🧔 Service	s~   Wic	lgets v Sh	ortcuts v					Search	🗌 🙏 🚍   admin
Home Routing											
Routing	Time Ranges										Help 7
Domains	New Edit Delete Oupflate More Actions										
Locations	1 Item 🥲										Filter: Enable
Conditions	Name	Mo	Ти	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
Adaptations 🗸 🗸	Select : All, None	R	Y	¥	Y	P	Y	¥	00100	23:59	
SIP Entities											
Entity Links											
Time Ranges											

#### Figure 50: Time Ranges

HV; Reviewed:
SPOC 4/3/2022

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

## 6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Three Routing Policies must be added: one for Communication Manager, one for Experience Portal and one for Avaya SBCE.

To add a Routing Policy, navigate to **Routing**  $\rightarrow$  **Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

In the General section, enter the following values. Use default values for all remaining fields.

- Name: Enter a descriptive name
- Notes: Add a brief description (optional)

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP Entity to which this Routing Policy applies and click **Select**. The selected SIP Entity displays on the Routing Policy Details page as shown below. Use default values for remaining fields.

Click **Commit** to save.

The following screen shows the **Routing Policy Details** for the policy named **SP Inbound Calls** associated with incoming PSTN calls from Telia Norway to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **CM8**.

AVAYA Aura® System Manager 8.1	≜ Users ∨ 🖌 Elements ∨ 🔅 Services ∨	Widgets v Shortcuts v
Home Routing		
Routing	Routing Policy Details	Commit Cancel
Domains	General	
Locations		* Name: SP Inbound Calls
Conditions		Disabled:  * Retries: 0
Adaptations	×	Notes:
SIP Entities	SIP Entity as Destination	
Entity Links	Select	
Time Ranges	Name	FQDN or IP Address
	CM8	10.33.10.54
Routing Policies	Time of Day	

Figure 51: Routing to Communication Manager

The following screen shows the **Routing Policy Details** for the policy named **SP Outbound Calls** associated with outgoing calls from Communication Manager to the PSTN via Telia Norway SIP Trunk through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.

AVAYA Aura® System Manager 8.1	🛔 Users 🗸 🎤 Elements 🗸 🔅 Services 🕈	∽   Widgets ∨ Shortcuts ∨
Home Routing		
Routing	A Routing Policy Details	Commit Cancel
Domains	General	
Locations		* Name: SP Outbound Calls
Conditions		Disabled:
Adaptations	ler −	* Retries: 0 Notes:
SIP Entities	SIP Entity as Destination	
Entity Links	Select	
Time Ranges	Name	FQDN or IP Address
	SBCE	10.33.10.49
Routing Policies	Time of Day	

#### Figure 52: Routing to Telia Norway SIP Trunk

The following screen shows the **Routing Policy Details** for the policy named **To-ExperiencePortal** associated with outgoing calls to Experience Portal. Observe the **SIP Entity as Destination** is the entity named **Experience Portal**.

AVAYA Aura® System Manager 8.1	Lusers ∨ ≯Elements ∨ ♦Services ∨   Widgets ∨ Shortcuts	v
Home Routing		
Routing	A Routing Policy Details	Commit
Domains	General	
Locations		* Name: To-ExperiencePortal
Conditions		Disabled:
Adaptations		* Retries: 0
Adaptations		Notes:
SIP Entities	SIP Entity as Destination	
Entity Links	Select	
Time Ranges	Name	FQDN or IP Address
Routing Policies	Experience Portal Time of Day	10.33.1.23

**Figure 53: Routing to Experience Portal** 

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

## 6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from Communication Manager to Telia Norway SIP Trunk through the Avaya SBCE and vice versa. Dial Patterns define which Route Policy will be selected as route destination for a particular call based on the dialed digits, destination Domain and originating Location.

To add a Dial Pattern, navigate to **Routing**  $\rightarrow$  **Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

In the General section, enter the following values. Use default values for all remaining fields.

•	Pattern:	Enter a dial string that will be matched against the Request-URI of the
		call

- Min: Enter a minimum length used in the match criteria
- Max: Enter a maximum length used in the match criteria
- **SIP Domain**: Enter the destination domain used in the match criteria
- Notes: Add a brief description (optional)

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating Location for use in the match criteria. Lastly, select the Routing Policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Three examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN, one for inbound calls from the PSTN to the enterprise and one for calls to Experience Portal. Other Dial Patterns were similarly defined.

The first example shows that outbound 12-digit dialed numbers that begin with +1613 and have a destination SIP Domain of bvwdev.com uses Routing Policy Name as SP Outbound Calls which is defined in Section 6.7.

🔳   admin
Help ?
Filter: Enable
tes

#### Figure 54: Dial Pattern +1613

Note that in real deployments, appropriate restriction can be exercised per customer business policies.

Also note that **-ALL-** was selected for **Originating Location Name**. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed back to the PSTN.

The second example shows that inbound 11-digit numbers that start with +47 use **Routing Policy Name** as **SP Inbound Calls** which is defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by Telia Norway.

AVAYA Aura® System Manager 8.1	Users ∨ 🖌 Elements ∨ 🌢 Services ∨	Widgets 🗸 Shortcuts 🗸					Search	≡   admin
Home Routing								
Routing	Dial Pattern Details	Com	nmit Cancel					Help ?
Domains			_					ļ
Locations	General							ļ
tocations		* Pattern: +47						ļ
Conditions		* Min: 3						ļ
Adaptations 😪		* Max: 11						1
SAME STOLAGE AVE.		Emergency Call:						
SIP Entities		SIP Domain: bvw/						
Entity Links		Notes: SP In	nbound Calls					
	Originating Locations and Routing Polic	cies						
Time Ranges	Add Remove							
Routing Policies	1 Item 🥭							Filter: Enable
Dial Patterns	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Not	tes
	Belleville-GSSCP		SP Inbound Calls	0		CM8		
Dial Patterns	Select : All, None							
and the second s	Protect Autobastics Franktions							

Figure 55: Dial Pattern +47

The third example shows that the inbound PSTN calls to Experience Portal use **Routing Policy Name** as **To-ExperiencePortal** which is defined in **Section 6.7**.

AVAYA Aura® System Manager 8.1	Users v ≯ Elements v ♦ Services v   Widgets v Shortcuts v				
Home Routing					
Routing	Dial Pattern Details	Commit Cancel			
Domains	General				
Locations	*	Pattern: 4800			
Conditions		* Min: 4			
		* Max: 4			
Adaptations 🗸 🗸	Emerge	ncy Call: 🗌			
SIP Entities	SIP	Domain: bvwdev.com 🗸			
Entity Links		Notes: Experience Portal			
Time Ranges	Originating Locations and Routing Policies				
This runges	Add Remove				
Routing Policies	1 Item 🧶				
Dial Patterns	Originating Location Name Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination
or a reaction	-ALL-	To-ExperiencePortal	0	0	Experience Portal
Dial Patterns	Select : All, None				

Figure 56: Dial Pattern\_4800

The following screen illustrates a list of dial patterns used for inbound and outbound calls between the enterprise and the PSTN.

	Dial Patterns     Help ?       New Edit Delete Duplicate More Actions •											
49 It	ems 🎅							Filter	r: Enable			
	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes				
	+1613	5	12				bvwdev.com	SP Outbound Calls				
	45	2	4				bvwdev.com	Telia Norway SIP Phones				
	+47	3	11				bvwdev.com	SP Inbound Calls				
	+47112	6	6				bvwdev.com	Telia Norway Outbound Calls				
Selec	t : All, None							14 4 Page 1	of 4 🕨 🕅			

Figure	57:	Dial	Pattern	List
--------	-----	------	---------	------

# 7. Configure Avaya Session Border Controller for Enterprise

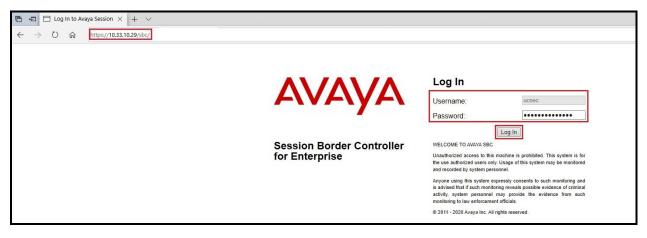
This section describes the configuration of the Avaya SBCE necessary for interoperability with the Session Manager and the Telia Norway.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Telia Norway system resides on the Public side of the network.

**Note**: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, refer to the documentation listed in **Section 12** of these Application Notes.

# 7.1. Log in to Avaya Session Border Controller for Enterprise

Access the web interface by typing "**https://x.x.x./sbc/**" (where x.x.x.x is the management IP of the Avaya SBCE).



Enter the Username and Password and click on Log In button.

Figure 58: Avaya SBCE Login

Select **Device** as **SBCE** and the **Dashboard** main page will appear as shown below.

Device: SBCE - Alarms	Incidents Status 🛩 Logs 🛩 Diagnos	tics Users			Settings 🛩	Help 👻 Log Out
Session Bord	er Controller for Ente	rprise				AVAYA
EMS Dashboard	Dashboard					
Software Management	Information			Installed Devices		
Device Management Backup/Restore	System Time	11:15:25 PM EST	Refresh	EMS		
<ul> <li>System Parameters</li> </ul>	Version	8.1.3.0-31-21052		SBCE		
Configuration Profiles	GUI Version	8.1.3.0-21036				
Services	Build Date	Mon Jul 26 23:26:22 UTC 2021				
<ul> <li>Domain Policies</li> <li>TLS Management</li> </ul>	License State	O OK				
<ul> <li>Network &amp; Flows</li> </ul>	Aggregate Licensing Overages	0				
DMZ Services	Peak Licensing Overage Count	0				
Monitoring & Logging	Last Logged in at	01/21/2022 11:48:51 EST				
	Failed Login Attempts	0				
	Active Alarms (past 24 hours)			Incidents (past 24 hours)		
	None found.			SBCE: No Subscriber Flow Matched		
				SBCE: No Subscriber Flow Matched		
				SBCE: No Subscriber Flow Matched		
				SBCE: No Subscriber Flow Matched		
				SBCE: No Subscriber Flow Matched		

Figure 59: Avaya SBCE Dashboard

To view system information that has been configured during installation, navigate to **Device Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **SBCE** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.

Session Borde	er Controller for Enterpr	ise			Αναγα
EMS Dashboard Software Management Device Management System Administration	Device Management           Devices         Updates         Licensing         Key Bundli	es			
Templates	Device Name	Management IP	Version	Status	
<ul> <li>Backup/Restore</li> <li>Monitoring &amp; Logging</li> </ul>	SBCE	10.33.10.29	8.1.3.0-31-21052	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

Figure 60: Avaya SBCE Device Management

The System Information screen shows General Configuration, Device Configuration, Network Configuration, DNS Configuration and Management IP(s) information provided during installation and corresponds to Figure 1.

			System Inform	nation: SBCE		x
General Configuration	on		Device Configuratio		- License Allocation —	
	SBCE		2-9-80 (1-6-82 (63 99 (99 (99 (99 (99 (99 (99 (99 (99 (99	No	Standard Sessions Requested: 0	512
	SIP Proxy		Two Bypass Mode	No	Advanced Sessions Requested: 0	512
Deployment Mode	Рюху				Scopia Video Sessions Requested: 0	512
					CES Sessions Requested: 0	512
					Transcoding Sessions Requested: 0	512
					CLID	
					Encryption Available: Yes	
Network Configuration						
		Public IP	Netv	work Prefix or Subnet Mas	k Gateway	Interface
10.33.10.49		Public IP 10.33.10.49		work Prefix or Subnet Mas 255.255.0	k Gateway 10.33.10.1	Interface A1
			255			
10.33.10.49		10.33.10.49	255 255	255.255.0	10.33.10.1	A1
10.33.10.49 10.33.10.50	8	10.33.10.49 10.33.10.50	255 255 255	255.255.0 255.255.0	10.33.10.1 10.33.10.1	A1 A1
10.33.10.49 10.33.10.50 10.10.80.105	8	10.33.10.49 10.33.10.50 10.10.80.105	255 255 255	255.255.0 255.255.0 255.255.128	10.33.10.1 10.33.10.1 10.10.80.1	A1 A1 B1
10.33.10.49 10.33.10.50 10.10.80.105 10.10.80.106 DNS Configuration	8	10.33.10.49 10.33.10.50 10.10.80.105	255 255 255 255 Management IP(s)	255.255.0 255.255.0 255.255.128	10.33.10.1 10.33.10.1 10.10.80.1	A1 A1 B1
10.33.10.49 10.33.10.50 10.10.80.105 10.10.80.106		10.33.10.49 10.33.10.50 10.10.80.105	255 255 255 255 Management IP(s)	255.255.0 255.255.0 255.255.128 255.255.128	10.33.10.1 10.33.10.1 10.10.80.1	A1 A1 B1
10.33.10.49           10.33.10.50           10.10.80.105           10.10.80.106           DNS Configuration           Primary DNS         10           Secondary DNS         10		10.33.10.49 10.33.10.50 10.10.80.105	255 255 255 255 Management IP(s)	255.255.0 255.255.0 255.255.128 255.255.128	10.33.10.1 10.33.10.1 10.10.80.1	A1 A1 B1

Figure 61: Avaya SBCE System Information

# 7.2. TLS Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. Avaya security products utilize TLS primarily to facilitate secure communications with remote users.

The server authentication comes into play for encrypted connections, such as TLS. The client initiates a request to the server for secure session, the server then sends its identity certificate to the client. The client checks the received server identity certificate against the trusted Certification Authority (CA) certificates that are saved in its trust store, to verify that the server identity certificate is indeed signed by a CA that the client trusts. There has to be a trusted CA, which is used to create and sign the server identity certificate.

The client authentication is similar to server authentication, except that the roles are reversed. The client authentication comes into play for encrypted connections with mutual authentication, and applies in addition to server authentication. The server also sends a request to the client for the client identity certificate, the client then sends its identity certificate to the server, and the server checks the received client identity certificate against the CA certificates that are saved in its trust store, to verify that the client identity certificate is indeed signed by a CA that the server trusts.

The following section describes TLS certificate installation so that clients authenticate servers or, optionally, servers authenticate clients.

#### 7.2.1. Installing TLS Certificate

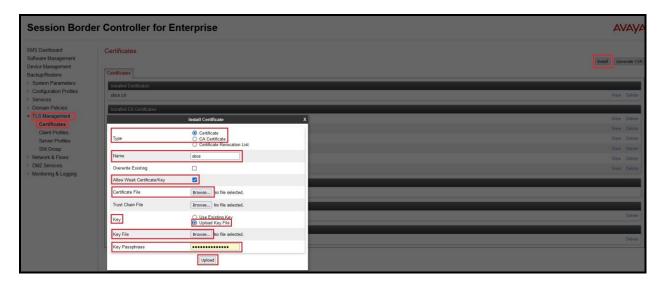
To manage the TLS parameters for Telia Norway:

- Avaya provided the root certificate used to sign the Avaya identity certificate to Telia Norway. Telia Norway also provided the root certificate used to sign the Telia Norway identity certificate, this certificate was installed on Avaya SBCE as a Certificate Authority (CA) certificate.
- Once these procedures were completed, the client and server profiles were created.

The following procedures show how to install the certificates:

From the left hand site menu, select **TLS Management**  $\rightarrow$  **Certificates** and click on **Install** button located in the upper-right hand

- Select **Type**: **Certificate** for installing the Identity Certificate, or **CA Certificate** for installing the root certificates
- Enter Name: sbce for installing Avaya Identity Certificate, Telia for installing Telia Norway CA Certificate
- Click on Allow Weak Certificate/Key box
- Click **Browse** button to navigate to the **Certificate File**. Choose the certificates accordingly
- Check **Upload Key File** button in **Key** section (This option is only for installing the Certificate) and click **Browse** button to navigate to the **Key File**. Choose the keys accordingly
- Enter Key Passphrase
- Click **Upload** and then click **Install**



**Figure 62 – Certificate Installation** 

Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved. The following screen shows the installed certificates.

Session Bord	er Controller for Enterprise	Αναγα
EMS Dashboard Software Management Device Management Backup/Restore	Certificates	[Install] [Generate CSR]
System Parameters     Configuration Profiles     Services     Domain Policies	Installed Cartificates Soce.cet Installed CA. Cartificates	View Delete
TLS[Management]     Certificates     Client Profiles	Telda pom New_SMGR2022 pem	View Delete View Delete

#### Figure 63 – The installed certificates

Note: To manage TLS parameters for Avaya enterprise site is not mentioned in this document. There has to be a trusted CA, which is used to create and sign the server identity certificate. During the compliance test in the lab environment demo certificates were used. Demo certificates are not recommended in a production environment. Consult the appropriate Avaya product documentation for further information regarding security certificate and encryption capabilities supported by Avaya product.

#### 7.2.2. TLS Client Profile

From the menu on the left-hand side, select **TLS Management → Client Profiles** 

- Select Add to create a TLS client profile
- Enter **Profile Name**: **Telia\_Client**
- Select Certificate: sbce.crt
- The **Peer Verification** is always **Required**
- Select Peer Certificate Authorities: Telia.pem
- Enter Verification Depth: 5
- Click **Next** and then click **Finish** (Not shown)

Session Borde	r Controller for Enter	rprise	
EMS Dashboard Software Management Device Management	Client Profiles: Telia_Client		
Backup/Restore	Client Profiles		New Profile X
<ul> <li>System Parameters</li> </ul>	AvayaSBCClient	WARNING: Due to the way OpenSSI	handles cipher checking, Cipher Suite validation will
<ul> <li>Configuration Profiles</li> <li>Services</li> </ul>	Telia_Client	pass even if one or more of the ciphers	renues cipier creating, cipier Suite variation win a re-invalid as long as at least one cipher is valid. Make nvalid or incorrectly entered Cipher Suite custom values
<ul> <li>Domain Policies</li> <li>TLS Management</li> </ul>		TLS Profile	
Certificates		Profile Name	Telia_Client
Client Profiles		Certificate	sbce.crt v
SNI Group		SNI	Enabled
Network & Flows		Certificate Verification	
DMZ Services		Peer Verification	Required
Monitoring & Logging		Feel vehication	
		Peer Certificate Authorities	avayaitrootca2.pem ^ entrust_g2_ca.cer SMGR71.pem Telia.pem
		Peer Certificate Revocation Lists	<b>^</b>
		Verification Depth	5
		Extended Hostname Verification	
		Server Hostname	
			Next

Figure 64 – TLS Client Profile - Telia Norway site

#### 7.2.3. TLS Server Profile

From the menu on the left-hand side, select TLS Management  $\rightarrow$  Server Profiles

- Select Add to create a TLS server profile
- Enter **Profile Name**: **Telia\_Server**
- Select Certificate: sbce.crt
- Select **Peer Verification**: None
- Click **Next** and then click **Finish** (Not shown)

# **Session Border Controller for Enterprise**

EMS Dashboard	Server Profiles: Telia_Serve	ər
Software Management	Ad	a
Device Management	Server Profiles	
Backup/Restore		
System Parameters		New Profile
Configuration Profiles Services Domain Policies TLS Management	pass even if one or more of the ciphers	handles cipher checking, Cipher Suite validation will s are invalid as long as at least one cipher is valid. Make nvalid or incorrectly entered Cipher Suite custom values
Certificates	TLS Profile	
Client Profiles	Profile Name	Telia_Server
Server Profiles		
SNI Group	Certificate	sbce.crt v
Network & Flows	SNI Options	None V
DMZ Services		
Monitoring & Logging	SNI Group	None V
	Certificate Verification	
	Peer Verification	None V
	Peer Certificate Authorities	AvayaDeviceEnrollmentCAchain.crt avayaitrootca2.pem entrust_g2_ca.cer SMGR71.pem
	Peer Certificate Revocation Lists	~ ~
	Verification Depth	
		Next

Figure 65 – TLS Server Profile – Telia Norway site

## 7.3. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

#### 7.3.1. Configure Server Interworking Profile - Avaya Site

Server Interworking profile allows administrator to configure and manage various SIP call server specific capabilities such as call hold, 180 handling, etc.

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Server Interworking

- Select avaya-ru in Interworking Profiles
- Click Clone
- Enter Clone Name: SMVM and click Finish (not shown)
- Select SMVM in Interworking Profiles
- Select **General** tab and click **Edit** button
- Check **T.38 Support** option and click **Finish** (not shown)

The following screen shows that Session Manager server interworking profile (named: SMVM) was added.

SSION DOIGC	er Controller for Ente	rprise		AVA
Dashboard vare Management :e Management	Interworking Profiles: SMVM			Rename Clone D
up/Restore	Interworking Profiles		Click here to add a description.	
stem Parameters	cs2100	General Timers Privacy URI Manipulation	Header Manipulation Advanced	
nfiguration Profiles Domain DoS	avaya-ru	General		
Server Interworking	SMVM	Held Support	None	
Media Forking		180 Handling	None	
Routing		181 Handling	None	
Topology Hiding		182 Handling	None	
ignaling Manipulation JRI Groups		183 Handling	None	
SNMP Traps		Refer Handling	No	
me of Day Rules		URI Group	None	
GDN Groups		Send Hold	No	
everse Proxy Policy		Delayed Offer	Yes	
tN Profile cording Profile		3xx Handling	No	
8 Profile		Diversion Header Support	No	
es		Delayed SDP Handling	No	
n Policies		Re-Invite Handling	No	
anagement rk & Flows		Prack Handling	No	
ervices		Allow 18X SDP	No	
oring & Logging		T.38 Support	Yes	
		URI Scheme	SIP	
		Via Header Format	RFC3261	
		SIPS Required	Yes	
		Mediasec	No	

Figure 66: Server Interworking – Avaya site

#### 7.3.2. Configure Server Interworking Profile – Telia Norway SIP Trunk Site

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Server Interworking  $\rightarrow$  Add

- Enter **Profile Name**: **SP** (not shown)
- Click **Next** button to leave all options at default
- Click **Finish** (not shown)
- Select **SP** in **Interworking Profiles**
- Select **General** tab and click **Edit** button
- Check **T.38 Support** option and click **Finish** (not shown)

The following screen shows that Telia Norway server interworking profile (named: **SP**) was added.

Session Borde	r Controller for Ente	rprise		
EMS Dashboard Software Management Device Management Backup/Restore	Interworking Profiles: SP			Click here to add a desc
<ul> <li>System Parameters</li> <li>Configuration Profiles</li> <li>Domain DoS</li> <li>Server Interworking</li> </ul>	cs2100 avaya-ru SMVM	General Timers Privacy URI Manipulation General Hold Support	Header Manipulation Advanced	
Media Forking Routing Topology Hiding	SP	180 Handling 181 Handling 182 Handling	Non Non Non	e
Signaling Manipulation URI Groups SNMP Traps Time of Day Rules		183 Handling Refer Handling URI Group	Non No No	e
FGDN Groups Reverse Proxy Policy URN Profile Recording Profile		Send Hold Delayed Offer 3xx Handling	No Yes No	
H248 Profile <ul> <li>Services</li> <li>Domain Policies</li> <li>TLS Management</li> </ul>		Diversion Header Support Delayed SDP Handling Re-Invite Handling	No No	
<ul> <li>Network &amp; Flows</li> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>		Prack Handling Allow 18X SDP T.38 Support	No No Yes	]
		URI Scheme Via Header Format SIPS Required	SIP RFC Yes	3261
		Mediasec	No	Edit

#### Figure 67: Server Interworking – Telia Norway SIP Trunk site

# 7.4. Configure Signaling Manipulation

The SIP signaling header manipulation feature adds the ability to add, change and delete any of the headers and other information in a SIP message.

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Signaling Manipulation  $\rightarrow$  Add

- Enter script **Title**: **SP**. In the script editing window, enter the text exactly as shown in the below screenshot to perform the following:
  - Change sips to sip for SIP headers
  - Remove un-wanted headers by Telia Norway
  - Click **Save** (not shown)

EMS Dashboard	Signaling Manipulation Scr	ipts: SP
Software Management Device Management Device Management Backup/Restore System Parameters Configuration Profiles Domain DoS Server Interworking Media Forking Routing Topology Hiding Signaling Manipulation URI Groups SNMP Traps Time of Day Rules FGDN Groups Reverse Proxy Policy	Signaling Wanipulation Scr Upload Ac Signaling Manipulation Scripts SP	<pre>Signaling Manipulation within session "ALL" {     act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING         {         //Change the SIPs to SIP         //KHADERS["Request_Line"][1].regex_replace("sips","sip");         %HEADERS["FRAW"][1].regex_replace("sips","sip");         %HEADERS["Contact"][1].regex_replace("sips","sip");         %HEADERS["Contact"][1].regex_replace("sips","sip");         %HEADERS["Contact"][1].regex_replace("sips","sip");         %HEADERS["Diversion"][1].regex_replace("sips","sip");         %HEADERS["Diversion"][1].regex_replace("sips","sip");         %HEADERS["History-Info"][3]);         remove(%HEADERS["History-Info"][2]);         remove(%HEADERS["History-Info"][1]);         remove(%HEADERS["P-AV-Message-Id"][1]);         remove(%HEADERS["P-AV-Message-Id"][1]);         remove(%HEADERS["P-AV-Message-Id"][1]);         remove(%HEADERS["AU-AND-Isession-ID"][1]);         remove(%HEADERS["AU-AND-Isession-ID"][1]);</pre>
URN Profile Recording Profile		<pre>remove(%HEADERS["P-Location"][1]); } </pre>
H248 Profile		

#### Figure 68: Signaling Manipulation

**Note**: See **Appendix A** in **Section 13** for the reference of this signaling manipulation (SigMa) script.

#### 7.5. Configure Services

#### 7.5.1. Configure SIP Server – Avaya Site

The **SIP** Servers screen contains six tabs: General, Authentication, Heartbeat, Registration, Ping and Advanced. Together, these tabs allow one to configure and manage various SIP call server specific parameters such as port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select Services  $\rightarrow$  SIP Servers  $\rightarrow$  Add

#### Enter Profile Name: SMVM

On **General** tab, enter the following:

- Server Type: Select Call Server
- **TLS Client Profile**: Select **AvayaSBCClient**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
- IP Address/FQDN: 10.33.10.53 (Session Manager IP Address)
- Port: 5061
- Transport: TLS
- Click **Finish** (not shown)

Device: SBCE - Alarms	Incidents Status 🛩 Logs 🛩 D	iagnostics Users			Settin	gs ✔ Help ✔ Log Out
Session Borde	r Controller for E	nterprise				Αναγα
EMS Dashboard Device Management Backup/Restore System Parameters Configuration Profiles Services LDAP	SIP Servers: SMVM Add Server Profiles SMVM	General Authentication Heartbe Server Type TLS Client Profile DNS Query Type	at Registration Ping Advanced Call Server AvayaSBCClic NONE/A	ant		Rename Cione Delete
RADIUS <ul> <li>Domain Policies</li> </ul>		IP Address / FQDN 10.33.10.53		Port 5061	Transport TLS	
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> <li>DMZ Services</li> </ul>				Edit		

Figure 69: SIP Server – General - Avaya site

On the **Advanced** tab:

- Enable Grooming box is checked
- Select **SMVM** for **Interworking Profile** (see Section 7.3.1)
- Click **Finish** (not shown)

Enable D	oS Protection					
Enable G	Enable Grooming					
Interwork	king Profile					SMVM
Signaling	Manipulation Scrip	t				None
Securab	le					
Enable F	GDN					
Tolerant						
URI Grou	μ					None
NG911 S	Support					

Figure 70: SIP Server – Advanced - Avaya site

#### 7.5.2. Configure SIP Server – Telia Norway SIP Trunk

From the menu on the left-hand side, select Services  $\rightarrow$  SIP Servers  $\rightarrow$  Add

The Telia Norway signaling server IP addresses are 192.168.89.165, 192.168.84.65, 192.168.93.165

#### Enter **Profile Name: SP**

On General tab, enter the following:

- Server Type: Select Trunk Server
- TLS Client Profile: Select Telia\_Client (See Section 7.2.2)
- **IP Address/FQDN: 192.168.89.165, 192.168.84.165, 192.168.93.165** (Telia Norway signaling server IP addresses)
- Port: 6004
- Transport: TLS
- Click **Finish** (not shown)

Session Border Controller for Enterprise							
EMS Dashboard Software Management Device Management Backup/Restore > System Parameters > Configuration Profiles Services SIP Servers	SIP Servers: SP Server Profiles SMVM	Add Ceneral Authentication Heart Server Type TLS Cient Profile DNS Query Type	Registration Ping Advanced	Trunk Sever Telia Client NONE/A			
H248 Servers		IP Address / FQDN		Port	Transport		
LDAP RADIUS		192.168.89.165		6004	TLS		
<ul> <li>Domain Policies</li> </ul>		192.168.93.165		6004	TLS		
TLS Management		192.168.84.165		6004	TLS		
<ul> <li>Network &amp; Flows</li> <li>DMZ Services</li> </ul>				Edit			

Figure 71: SIP Server – General – Telia Norway

On **Heartbeat** tab, enter the following:

- Check Enable Heartbeat
- Select Method: OPTIONS
- Set Frequency: 60 seconds
- Input **From URI**: **ping@customer.3z8t533yh4mf7uj.net** (Telia Norway provides this information)
- Input **To URI**: **ping@ep.xxx.telia.no** (Telia Norway provides this information)

ble Heartbeat	
Method	OPTIONS
Frequency	60 seconds
From URI	ping@customer.3z8t533yh4mf7uj.net
To URI	ping@ep.xxx.telia.no

Figure 72: SIP Server – Heartbeat – Telia Norway

On the **Advanced** tab, enter the following:

- Check Enable Grooming option
- Interworking Profile: SP (see Section 7.3.2)
- Signaling Manipulation Script: SP (see Section 7.4)
- Click **Finish** (not shown)

Enable D	DoS Protection			
Enable 0	Grooming			
Interwork	king Profile			SP
Signaling	g Manipulation Scrip	t		SP
Securab	le			
Enable F	GDN			
Tolerant				
URI Grou	qu			None
NG911 S	Support			

Figure 73: SIP Server – Advanced – Telia Norway

## 7.6. Routing

Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the service provider

#### 7.6.1. Configure Routing – Avaya Site

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Routing and click Add as highlighted below.

Enter Profile Name: SP\_To\_SMVM and click Next button (Not Shown)

- Select Load Balancing: Priority
- Check Next Hop Priority
- Click Add button to add a Next-Hop Address
- Priority/Weight: 1
- SIP Server Profile: SMVM (see Section 7.5.1)
- Next Hop Address: 10.33.10.53:5061 (TLS) (Session Manager IP address)
- Click Finish

Session Border Controller for Enterprise							
EMS Dashboard Software Management	Routing Profiles: SP	_To_SMV	Μ				
Device Management Backup/Restore	Routing Profiles						Click here to add
<ul> <li>System Parameters</li> </ul>	default		Routing Profile	1			
<ul> <li>Configuration Profiles</li> </ul>	To SMVM RW		Routing Profile				
Domain DoS	default RW		Update Priority				
Server Interworking	AS TO SMVM		Priority	URI Group	Time of Day	Load Balancing	
Media Forking	AS IN SMMM			Routing P	rofile		<b>X</b> 3.1
Routing Topology Hiding	URI Group	*	~		Time of Day	default 🗸	
Signaling Manipulation URI Groups	Load Balancing	Priority	<b>v</b> ]		NAPTR		
SNMP Traps	Transport	None 🗸			LDAP Routing		
Time of Day Rules FGDN Groups	LDAP Server Profile	None 🗸			LDAP Base DN (Search)	None 🗸	
Reverse Proxy Policy	Matched Attribute Priority				Alternate Routing		
URN Profile Recording Profile	Next Hop Priority				Next Hop In-Dialog		
H248 Profile	Ignore Route Header						
Services							
Domain Policies	ENUM				ENUM Suffix		
TLS Management	LINOW	U			LINUW SUIIX	<u>*</u> 3	
Network & Flows							Add
DMZ Services	Priority LDAD Course					_	
Monitoring & Logging	/ LDAP Search / Attribute	LDAP Search Regex Patter			Profile Next Hop Address	Transport	
	1			SMVM	✓ 10.33.10.53:5061	(TLS) V None	✓ Delete
				Back	Finish		

Figure 74: Routing to Session Manager

### 7.6.2. Configure Routing – Telia Norway SIP Trunk Site

The Routing Profile allows one to manage parameters related to routing SIP signaling messages.

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Routing and click Add as highlighted below.

Enter Profile Name: SMVM\_To\_SP and click Next button (not shown)

- Load Balancing: Priority
- Check Next Hop Priority
- Click Add button to add a Next-Hop Address
- Priority/Weight: 1; SIP Server Profile: SP (see Section 7.5.2); Next Hop Address: 192.168.89.165:6004 (TLS) (Telia Norway signaling server IP address)
- Priority/Weight: 2; SIP Server Profile: SP (see Section 7.5.2); Next Hop Address: 192.168.84.165:6004 (TLS) (Telia Norway signaling server IP address)
- Priority/Weight: 3; SIP Server Profile: SP (see Section 7.5.2); Next Hop Address: 192.168.93.165:6004 (TLS) (Telia Norway signaling server IP address)
- Click **Finish**

Session Border	Controller for	Enterp	rise					
EMS Dashboard Software Management Device Management	Routing Profiles: SM	/M_To_SP						
Backup/Restore								
System Parameters	default	Real	uting Profile					
Configuration Profiles	To SMVM RW	Ko						
Domain DoS	default_RW		odate Priority					
Server Interworking				Routing Profile				x
Media Forking Routing	URI Group	*	•	Time	e of Day	default 🗸		
Topology Hiding Signaling Manipulation	Load Balancing	Priority	~	NAF	PTR			
URI Groups	Transport	None 🗸		LDA	AP Routing			
SNMP Traps Time of Day Rules	LDAP Server Profile	None 🗸		LDA	AP Base DN (Search)	None 🗸		
FGDN Groups	Matched Attribute Priority			Alte	mate Routing			
Reverse Proxy Policy URN Profile	Next Hop Priority			Nex	t Hop In-Dialog			
Recording Profile	Ignore Route Header							
H248 Profile								
<ul> <li>Services</li> <li>Domain Policies</li> </ul>	ENUM			ENU	JM Suffix			
TLS Management     Network & Flows								Add
DMZ Services     Monitoring & Logging	Priority / / Weight	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Т	ransport	
	1			(SP 🗸	192.168.89.165:6004 (	TLS) 💙 🗍	None	✓ Delete
	2			SP 🗸	192.168.84.165:6004 (	TLS) V	None	✓ Delete
	3			SP v	192.168.93.165:6004 (	TLS) V	None	✓ Delete
				Back Finish				

Figure 75: Routing to Telia Norway SIP Trunk

## 7.7. Topology Hiding

The Topology Hiding screen allows an administrator to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

### 7.7.1. Configure Topology Hiding – Avaya Site

From the menu on the left-hand side, select **Configuration Profiles**  $\rightarrow$  **Topology Hiding** 

- Select **default** in **Topology Hiding Profiles**
- Click Clone
- Enter Clone Name: SP\_To\_SMVM and click Finish (not shown)
- Select **SP\_To\_SMVM** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- For the Header **From**,
  - In the Criteria column select IP/Domain
  - In the **Replace Action** column select: **Overwrite** In the **Overwrite Value** column: **bvwdev.com**
- For the Header **To**,
  - In the Criteria column select IP/Domain
  - In the Replace Action column select: Overwrite
  - In the **Overwrite Value** column: **bvwdev.com**
- For the Header **Request-Line**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev.com**

Note: bvwdev.com is SIP domain of enterprise

Click **Finish** (not shown)

Session Borde	er Controller for I	Enterprise			AV
EMS Dashboard Software Management Device Management	Topology Hiding Profiles	s: SP_To_SMVM			Rename Clone
ackup/Restore	Topology Hiding Profiles			Click here to add a description.	
System Parameters Configuration Profiles	default cisco_th_profile	Topology Hiding			
Domain DoS		Header	Critena	Replace Action	Overwrite Value
Server Interworking	SP_To_SMVM	Refer-To	IP/Domain	Auto	-
Media Forking		То	IP/Domain	Overwrite	bwwdev.com
Routing		From	IP/Domain	Overwrite	bwwdev.com
Topology Hiding Signaling Manipulation		Record-Route	IP/Domain	Auto	<u> </u>
URI Groups		Referred-By	IP/Domain	Auto	
SNMP Traps		Request-Line	IP/Domain	Overwrite	bwwdev.com
Time of Day Rules		Via	IP/Domain	Auto	
FGDN Groups		SDP	IP/Domain	Auto	490
Reverse Proxy Policy URN Profile				Edit	

### Figure 76: Topology Hiding To Session Manager

### 7.7.2. Configure Topology Hiding Profile – Telia Norway SIP Trunk site

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Topology Hiding

- Select **default** in **Topology Hiding Profiles**
- Click Clone
- Enter Clone Name: SMVM\_To\_SP and click Finish (not shown)
- Select **SMVM\_To\_SP** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- For the Header **To**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **ep.xxx.telia.no** (Telia Norway provided this information)
- For the Header **From**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **customer.3z8t533yh4mf7uj.net** (Telia Norway provided this information)
- For the Header **Request-Line**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **ep.xxx.telia.no** (Telia Norway provided this information)
- Click **Finish** (not shown)

Session Borde	r Controller for	Enterprise			AVA)
Software Management Device Management Backup/Restore	Topology Hiding Profile	s: SMVM_To_SP Add Topology Hiding		Dick here to add a description	Rename Core De
Configuration Profiles Domain DoS	cisco_th_profile SP_To_SMVM	Header	Criteria	Reptace Action	Overwrite Value
Server Interworking	SMVM To SP	Refer-To	IP/Domain	Auto	
Media Forking	10 SP	То	IP/Domain	Overwrite	ep.xxx.telia.no
Routing		Record-Route	IP/Domain	Auto	Sec. 1
Topology Hiding Signaling Manipulation		Referred-By	IP/Domain	Auto	-
URI Groups		From	IP/Domain	Overwrite	customer.3z8t533yh4mf7uj.net
SNMP Traps		Request-Line	IP/Domain	Overwrite	ep.xxx telia.no
Time of Day Rules		Via	IP/Domain	Auto	-
FGDN Groups		SDP	IP/Domain	Auto	-
Reverse Proxy Policy		-		[mail]	
URN Profile Recording Profile				Edit	

Figure 77: Topology Hiding To Telia Norway

## 7.8. Domain Policies

The Domain Policies feature allows administrator to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or an administrator can create a custom domain policy.

### 7.8.1. Create Application Rules

Application rules define the type of SBC-based Unified Communication (UC) applications Avaya SBCE protects. You can also determine the maximum number of concurrent voice and video sessions that your network can process before resource exhaustion.

From the menu on the left-hand side, select **Domain Policies**  $\rightarrow$  **Application Rules** 

- Select **default** from **Application Rules** and click **Clone** button:
- Enter Clone Name (e.g., SIP-Trunk) and click Finish (not shown)
- Click on **SIP-Trunk** from **Application Rules**, then click **Edit** button:
- In the **Audio** field:
  - Check In and Out
  - Enter an appropriate value in the **Maximum Concurrent Sessions** field (e.g., **2000**), and the same value in the **Maximum Session Per Endpoint** field
  - Leave the **CDR Support** field at **Off** and the **RTCP Keep-Alive** field unchecked (**No**)

Device: SBCE - Alarms	Incidents Status 🗸 Logs	s♥ Diagnostics Users			Settings 🗸	Help 🗸	Log Out
Session Bord	er Controller f	or Enterprise				AV	/AYA
EMS Dashboard Device Management	Application Rules:	SIP-Trunk			Rename	Clone	Delete
Backup/Restore <ul> <li>System Parameters</li> <li>Configuration Profiles</li> </ul>	Application Rules default	Application Rule	Click here to	add a description.			
<ul> <li>Services</li> <li>Domain Policies</li> <li>Application Rules</li> </ul>	default-trunk default-subscriber-low default-subscriber-high	Application Type Audio	In Ou V		Maximum Ses 2000	sions Per E	ndpoint
Border Rules Media Rules Security Rules	default-server-low default-server-high	Video		]		_	
Signaling Rules Charging Rules	SIP-Trunk	Miscellaneous CDR Support RTCP Keep-Alive	Off			_	
End Point Policy Groups Session Policies	RW_AR	IN INCOMPANY	NU	Edit			

Click on **Finish** (not shown)

Figure 78: Application Rule

### 7.8.2. Create Media Rules

Media rule feature allows one to define RTP media packet parameters, such as prioritizing encryption techniques and packet encryption techniques. Together, these media-related parameters define a strict profile that is associated with other SIP specific policies. You can also define how Avaya SBCE must handle media packets that adhere to the set parameters.

From the menu on the left-hand side, select **Domain Policies**  $\rightarrow$  **Media Rules** 

- Select **default-low-med** from **Media Rules** and click **Clone** button:
- Enter Clone Name (e.g., SMVM) and click Finish (not shown)
- Click on **SMVM** from **Media Rules**, then click **Edit** button:
- For Audio Encryption, select the followings:
  - Preferred Format #1: RTP
  - Preferred Format #2: SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80
  - Preferred Format #3: SRTP\_AES\_CM\_128\_HMAC\_SHA1\_32
- Click **Finish** button to apply the changes.

Session Borde	er Controller for Er	nterprise		AVAYA
			Media Encryption	x
EMS Dashboard	Media Rules: SMVM	Audio Encryption		
Software Management Device Management	1	dd Preferred Format #1	[RTP ~]	Rename Clone Delete
Backup/Restore	Media Roles	Preferred Format #2	SRTP_AES_CM_128_HMAC_SHA1_80 V	Click here to add a description
System Parameters	default-low-med	Preferred Format #3	SRTP_AES_CM_128_HMAC_SHA1_32 V	
<ul> <li>Configuration Profiles</li> <li>Services</li> </ul>	default-low-med-enc default-high	Encrypted RTCP		
Domain Policies	default-high-enc	МКІ	0	P.AES.CM_128_HMAC_SHA1_80 P.AES.CM_128_HMAC_SHA1_32
Application Rules Border Rules	avaya-low-mad-enc	Lifetime Leave blank to match any value.	2*	P_AES_CM_128_HMAC_SHA1_32
Media Rules Security Rules		Interworking		
Signaling Rules		Symmetric Context Reset		
Charging Rules End Point Policy		Key Change in New Offer		
Groups		Video Encryption		
Session Policies TLS Management		Preferred Format #1	RTP 🗸	
<ul> <li>Network &amp; Flows</li> </ul>		Preferred Format #2	NONE	
Network Management Media Interface		Preferred Format #3	NONE	
Signaling Interface		Encrypted RTCP		
End Point Flows Session Flows		MKI		
Advanced Options		Lifetime Leave blank to match any value.	2*	
<ul> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>		Interworking	2	
		Symmetric Context Reset		
		Key Change in New Offer		Edt
		Miscellaneous		
		Capability Negotiation		
			Finish	

Figure 79: Media Rule 1

From the menu on the left-hand side, select **Domain Policies**  $\rightarrow$  **Media Rules** 

- Select **default-high-enc** from **Media Rules** and click **Clone** button:
- Enter Clone Name (e.g., SP) and click Finish (not shown)
- Click on **SP** from **Media Rules**, then click **Edit** button:
- For **Audio Encryption**, select the followings:
  - Preferred Format #1: SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80
  - Preferred Format #2: SRTP\_AES\_CM\_128\_HMAC\_SHA1\_32
- Click **Finish** button to apply the changes.

hboard	Media Rules: SP				
Management anagement		Add	Media Encryption	x	Rename
estore	Media Rolent default-low-med	Audio Encryption		Click here to add a description.	
Parameters Iration Profiles	default-low-med-enc	Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ¥		
5	default-high	Preferred Format #2	SRTP_AES_CM_128_HMAC_SHA1_32 V		
Policies ication Rules	default-high-enc	Preferred Format #3	NONE	AES_CM_128_HMAC_SHA1_80 AES_CM_128_HMAC_SHA1_32	
ter Rules	avaya-low-med-enc	Encrypted RTCP			
lia Rules urity Rules	IPO	MKI			
aling Rules	SMVM1	Lifetime Leave blank to match any value.	2*		
rging Rules Point Policy	SP1 SMVM	Interworking			
ıps	SP	Symmetric Context Reset			
sion Policies nagement		Key Change in New Offer			
k & Flows		Video Encryption			
vork Management ia Interface		Preferred Format #1	RTP v		
aling Interface		Preferred Format #2	NONE ~		
Point Flows sion Flows		Preferred Format #3	NONE		
inced Options		Encrypted RTCP			
ervices ing & Logging		MKI			
		Lifetime Leave blank to match any value.	24	Edd	
		Interworking	<b>Ø</b>		
		Symmetric Context Reset	8		
		Key Change in New Offer	0		
		Miscellaneous			

#### Figure 80: Media Rule 2

### 7.8.3. Create Endpoint Policy Groups

The End Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): Application, Border, Media, Signaling, Security, Charging and RTCP Monitoring Report Generation, each of which was created using the procedures contained in the previous sections. A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

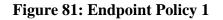
From the menu on the left-hand side, select **Domain Policies** → **End Point Policy Groups** 

- Select Add.
- Enter Group Name: SMVM
  - Application Rule: SIP-Trunk (See in Section 7.8.1)
  - Border Rule: default

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	78 of 104
SPOC 4/3/2022	©2022 Avaya Inc. All Rights Reserved.	TN_CMSM81SBC81

- Media Rule: SMVM (See in Section 7.8.2)
- Security Rule: default-low
- Signaling Rule: default
- Select **Finish** (not shown)

Session Bord	er Controller for Ent	erprise								AVAYA
EMS Dashboard Software Management Device Management	Policy Groups: SMVM	]							Rename	Clone
Backup/Restore	Policy Groups	1				Click here to add a description	on,			
System Parameters	default-low				1	lover over a row to see its desc	notion.			
Configuration Profiles	default-low-enc		1							
Services	default-med	Policy Group								
Domain Policies     Application Rules	default-med-enc									Summary
Border Rules	default-high	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
Media Rules	default-high-enc	1	SIP-Trunk	default	SMVM	default-low	default	None	Off	Edit
Security Rules Signaling Rules	avaya-def-low-enc									
Charging Rules	avaya-def-high-subscriber									
End Point Policy	avaya-def-high-server									
Groups Session Policies	SMVM									
TLS Management										



From the menu on the left-hand side, select **Domain Policies** → **End Point Policy Groups** 

- Select Add.
- Enter Group Name: SP
  - Application Rule: SIP-Trunk (See in Section 7.8.1)
  - Border Rule: default
  - Media Rule: SP (See in Section 7.8.2)
  - Security Rule: default-low
  - Signaling Rule: default
- Select **Finish** (not shown)

Session Bord	er Controller for E	interprise								AVAYA
EMS Dashboard Software Management Device Management	Policy Groups: SP	Add							Renam	e Clone Delete
Backup/Restore	Policy Groups					Click here to add a description	on.			
System Parameters	default-low					Hover over a row to see its desc	notion.			
Configuration Profiles	default-low-enc		1							
Services	default-med	Policy Group								
<ul> <li>Domain Policies</li> <li>Application Rules</li> </ul>	default-med-enc									Summary
Border Rules	default-high	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
Media Rules	default-high-enc	1	SIP-Trunk	default	SP	default-low	default	None	Off	Edit
Security Rules Signaling Rules	avaya-def-low-enc									
Charging Rules	avaya-def-high-subscriber									
End Point Policy	avaya-def-high-server									
Groups	SMVM									
Session Policies <ul> <li>TLS Management</li> </ul>	SP									
Network & Flows										

Figure 82: Endpoint Policy 2

## 7.9. Network & Flows

The Network & Flows feature for SIP allows one to view aggregate system information and manage various device-specific parameters which determine how a particular device will function when deployed in the network.

### 7.9.1. Manage Network Settings

From the menu on the left-hand side, select Network & Flows → Network Management.

- Select **Networks** tab and click the **Add** button to add a network for the inside interface as follows:
  - Name: Network\_A1
  - Default Gateway: 10.33.10.1
  - Subnet Mask: 255.255.255.0
  - Interface: A1 (This is the Avaya SBCE inside interface)
  - Click the Add button to add the IP Address for inside interface: 10.33.10.49
  - Click the **Finish** button to save the changes

Device: SBCE - Alarms						
Session Borde	r Controller for Enterpris	se				Αναγα
EMS Dashboard Device Management Backup/Restore > System Parameters	Network Management					
Configuration Profiles     Services     Domain Policies	Name Gateway Network B1	Subne	t Mask / Prefix Length Add Network	Interface	IP Address	Edit Delete
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> <li>Network</li> <li>Management</li> <li>Media Interface</li> <li>Signaling Interface</li> </ul>	Network_A1	Name Default Gateway Network Prefix or Subnet Mask	Network_A1 10.33.10.1 255.255.255.0			Edit Delete
End Point Flows Session Flows Advanced Options > DMZ Services > Monitoring & Logging		Interface IP Address 10.33.10.49	A1 ~ Public IP Use IP Address	Gateway Override	Add	
			Finish			

Figure 83: Network Management – Inside Interface

From the menu on the left-hand side, select **Network & Flows** → **Network Management**.

- Select **Networks** tab and click **Add** button to add a network for the outside interface as follows:
  - Name: Network\_B1
  - Default Gateway: 10.10.80.1
  - Subnet Mask: 255.255.255.128
  - Interface: B1 (This is the Avaya SBCE outside interface)
  - Click the Add button to add the IP Address for outside interface: 10.10.80.106
  - Click the **Finish** button to save the changes

Device: SBCE - Alarms	ncidents Status 🗸 Logs 🖌 Diagnostics	s Users		Settings 🗸 Help 🖌 Log Out
Session Borde	r Controller for Enter	orise		Αναγα
EMS Dashboard Device Management Backup/Restore System Parameters	Network Management			
Configuration Profiles  Services  Domain Policies	Name Gat	eway Subnet Mask /	Prefix Length Interface	Add IP Address
<ul> <li>TLS Management</li> </ul>	Network_B1		Add Network	Edit Delete
Network & Flows     Network     Management	Network_A1	Name Default Gateway	Network_B1 10.10.80.1	Edit Delete
Media Interface		Network Prefix or Subnet Mask	255.255.255.128	
Signaling Interface End Point Flows		Interface	B1 ~	
Session Flows Advanced Options				Add
DMZ Services			Public IP Gateway Override	
Monitoring & Logging		10.10.80.106 ×	Jse IP Address Use Default	Delete
			Finish	

Figure 84: Network Management – Outside Interface

From the menu on the left-hand side, select Network & Flows → Network Management

- Select the **Interfaces** tab
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state

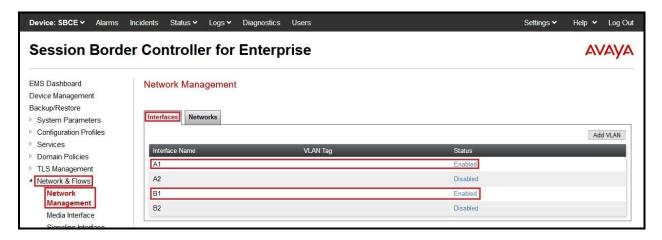


Figure 85: Network Management – Interface Status

### 7.9.2. Create Media Interfaces

Media Interfaces define the IP Addresses and port ranges in which the Avaya SBCE will accept media streams on each interface. The default media port range on the Avaya SBCE can be used for both inside and outside ports.

From the menu on the left-hand side, **Device Specific Settings**  $\rightarrow$  **Media Interface** 

- Select the **Add** button and enter the following:
  - Name: OutsideMedia
  - **IP Address**: Select **Network\_B1 (B1, VLAN 0)** and **10.10.80.106** (External IP address toward Telia Norway)
  - Port Range: 35000 40000
  - Click **Finish** (not shown)
- Select the **Add** button and enter the following:
  - Name: InsideMedia
  - IP Address: Select Network\_A1 (A1, VLAN 0) and 10.33.10.49 (Internal IP address toward Session Manager)
  - Port Range: 35000 40000
  - Click **Finish** (not shown)

Device: SBCE - Alarms	Incidents Status 🗸 Logs 🗸 Diagnostics	s Users		Settings 🗸	Help 🗸	Log Out
Session Bord	ler Controller for Enter	prise			A	VAYA
EMS Dashboard Device Management Backup/Restore System Parameters Configuration Profiles	Media Interface					Add
<ul> <li>Services</li> <li>Domain Policies</li> </ul>	Name	Media IP Network	Port Range			
TLS Management	OutsideMedia	10.10.80.106 Network_B1 (B1, VLAN 0)	35000 - 40000		Edit	Delete
<ul> <li>Network &amp; Flows</li> <li>Network Management</li> </ul>	InsideMedia	10.33.10.49 Network A1 (A1, VLAN 0)	35000 - 40000		Edit	Delete
Media Interface						

Figure 86: Media Interface

### 7.9.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select Network & Flows → Signaling Interface

- Select the **Add** button and enter the following:
  - Name: OutsideTLS
  - **IP Address**: Select **Network\_B1 (B1, VLAN 0)** and **10.10.80.106** (External IP address toward Telia Norway)
  - TLS Port: 6004
  - TLS Profile: Telia\_Server (See in Section 7.2.3)
  - Click **Finish** (not shown)

From the menu on the left-hand side, select Network & Flows → Signaling Interface

- Select the **Add** button and enter the following:
  - Name: InsideTLS
  - **IP Address**: Select **Network\_A1 (A1, VLAN 0)** and **10.33.10.49** (Internal IP address toward Session Manager)
  - TLS Port: 5061
  - **TLS Profile:** AvayaSBCServer. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
  - Click **Finish** (not shown)

**Note**: For the external interface, the Avaya SBCE was configured to listen for TLS on port 6004 the same as Telia Norway used. For the internal interface, the Avaya SBCE was configured to listen for TLS on port 5061.

d gement	Signaling Interface						
rment e imeters	Signaling Interface						Ade
Profiles	Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
cies ment	InsideTLS	10.33.10.49 Network_A1 (A1, VLAN 0)	-	-	5061	AvayaSBCServer	Edit Delete
	OutsideTLS	10.10.80.106 Network, B1 (B1, VLAN 0)	-		6004	Telia_Server	Edit Delete

#### **Figure 87: Signaling Interface**

### 7.9.4. Configuration Server Flows

Server Flows allow an administrator to categorize trunk-side signaling and apply a policy.

#### 7.9.4.1 Create End Point Flows – SMVM Flow

From the menu on the left-hand side, select **Network & Flows** → **End Point Flows** 

- Select the Server Flows tab
- Select Add, enter Flow Name: SMVM Flow
  - Server Configuration: SMVM (see Section 7.5.1)
  - URI Group: \*
  - Transport: \*
  - Remote Subnet: \*
  - Received Interface: OutsideTLS (see Section 7.9.3)
  - Signaling Interface: InsideTLS (see Section 7.9.3)
  - Media Interface: InsideMedia (see Section 7.9.2)
  - Secondary Media Interface: None
  - End Point Policy Group: SMVM (see Section 7.8.3)
  - Routing Profile: SMVM\_To\_SP (see Section 7.6.2)
  - Topology Hiding Profile: SP\_To\_SMVM (see Section 7.7.1)
  - Leave other parameters as default
  - Click Finish

shboard	End Point Flows					
Management anagement						
Restore	Subscriber Flows Server Flows					
n Parameters uration Profiles						
es n Policies	Modifications made to a Server Flow will					
anagement		Add Flow	X Cicle here to add a row de	nen plion		
rk & Flows	Flow Name	SMVM Flow				
work Management Sa Interface	SIP Server Profile	SMVM ~	Signaling Interface	End Point Policy Group	Routing Profile	
naling Interface	URI Group	· •	InsideTLS	EndPoint-Policy	To_SP	View Clone Edit
Point Flows	Transport	* · •	InsideSIGRW	PO_RW	default_RW	
anced Options	Remote Subnet	•				
ervices ning & Logging	Received Interface	OutsideTLS Y				
ning & Logging	Signaling Interface	InsideTLS ¥	Signaling Interface	End Point Policy Group	Routing Profile	
	Media Interface	InsideMedia v	InsideTLS	SMVM	SMVM_To_SP	View Clone Edit I
	2 Secondary Media Interface	None v	InsideSIGRW	SMVM_RW	default_RW	
	End Point Policy Group	SMVM Y	InsideTLS	SMVM1	SMVM_To_SPWS	View Clone Edit I
	SI Routing Profile	SMVM_To_SP ~				
	Topology Hiding Profile	SP_To_SMVM V	Signaling Interface	End Peint Policy Group	Routing Profile	
	Signaling Manipulation Script	None V	OutsideTLS	SP.	SP_To_SMVM	View Clone Edit I
	SI Remote Branch Office					
		Any v	Signaling Interface	End Point Policy Group	Routing Profile	
	Link Monitoring from Peer	0	OutsideUDP5070	SP1	SPWS_To_SMVM	View Clone Edit I
	FQDN Support	U				

Figure 88: End Point Flow 1

### 7.9.4.2 Create End Point Flows – Telia Norway SIP Trunk Flow

From the menu on the left-hand side, select Network & Flows  $\rightarrow$  End Point Flows There is a Server Flows associated to Telia Norway signaling server.

- Select the Server Flows tab
- Select Add, enter Flow Name: SP Flow
  - Server Configuration: SP (see Section 7.5.2)
  - URI Group: \*
  - Transport: \*
  - Remote Subnet: \*
  - Received Interface: InsideTLS (see Section 7.9.3)
  - Signaling Interface: OutsideTLS (see Section 7.9.3)
  - Media Interface: OutsideMedia (see Section 7.9.2)
  - Secondary Media Interface: None
  - End Point Policy Group: SP (see Section 7.8.3)
  - Routing Profile: SP\_To\_SMVM (see Section 7.6.1)
  - Topology Hiding Profile: SMVM\_To\_SP (see Section 7.7.2)
  - Leave other parameters as default
  - Click **Finish**

Session Borde	r Controller for Ente	erprise				AVAYA		
EMS Dashboard Software Management Device Management	End Point Flows Subscriber Flows Server Flows							
Backup/Restore  System Parameters Configuration Profiles Services	Subscriber Hons Sever Flows Modifications make to a Server Flow and only take effect on prev sessions.							
Domain Policies		Add Flow	X Click here to add a row de	Circle here to add a row description				
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul>	Flow Name	SP Flow						
Network Management Media Interface	SIP Server Profile	SP v	Signaling Interface	End Point Policy Group	Routing Profile			
Signaling Interface	URI Group	· ·	InsideTLS	EndPoint-Policy	To_SP	View Clone Edit Delete		
End Point Flows Session Flows	2 Transport	× •	InsideSIGRW	IPO_RW	default_RW			
Advanced Options	Remote Subnet	*						
<ul> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>	Received Interface	InsideTLS v						
memoring or roughing	Signaling Interface	OutsideTLS v	Signaling Interface	End Point Policy Group	Routing Profile			
	Media Interface	OutsideMedia 🗸	InsideTLS	SMVM	SMVM_To_SP	View Clone Edit Delete		
	Secondary Media Interface	None 🗸	InsideSIGRW	SMVM_RW	default_RW			
	End Point Policy Group	SP v	InsideTLS	SMVM1	SMVM_To_SPWS	View Clone Edit. Delate		
	SI Routing Profile	SP_To_SMVM V			5050321003-8027/29G	1		
	Topology Hiding Profile	SMVM_To_SP v	Signaling Interface Outside11.S	End Point Policy Group	Rooting Profile SP To SMVM	View Clone Edit Delete		
	Signaling Manipulation Script	None 🗸	Construction	17	an _ to_can view			
	Remote Branch Office	Any 🗸	Signaling Interface	Erid Point Policy Group	Routing Profile			
	Link Monitoring from Peer	0	OutsideUDP5070	SP1	SPWS_To_SMVM	View Gione Edit Delete		
	FQDN Support							
	FQDN							
		Finish						

Figure 89: End Point Flow 2

# 8. Configure Avaya Aura<sup>®</sup> Experience Portal

These Application Notes assume that the necessary Experience Portal licenses have been installed and basic Experience Portal administration has already been performed. Consult in the **References [5]- Section 12** for further details if necessary.

## 8.1. Background

Experience Portal consists of one or more Media Processing Platform (MPP) servers and an Experience Portal Manager (EPM) server. A single "server configuration" was used in the reference configuration. This consisted of a single MPP and EPM, running on a VMware environment, including an Apache Tomcat Application Server (hosting the Voice XML (VXML) and/or Call Control XML (CCXML) application scripts), that provide the directives to Experience Portal for handling the inbound calls.

References to the Voice XML and/or Call Control XML applications are administered on Experience Portal, along with one or more called numbers for each application reference. When an inbound call arrives at Experience Portal, the called party DID number is matched against those administered called numbers. If a match is found, then the corresponding application is accessed to handle the call. If no match is found, Experience Portal informs the caller that the call cannot be handled and disconnects the call<sup>1</sup>.

For the sample configuration described in these Application Notes, a simple VXML test application was used to exercise various SIP call flow scenarios with SIP Trunking service. In production, enterprises can develop their own VXML and/or CCXML applications to meet specific customer self-service needs or consult Avaya Professional Services and/or authorized Avaya Business Partners. The development and deployment of VXML and CCXML applications is beyond the scope of these Application Notes.

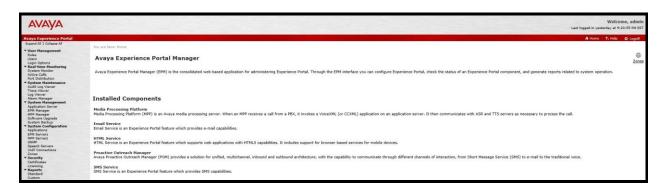
<sup>&</sup>lt;sup>1</sup> An application may be configured with "inbound default" as the called number, to process all inbound calls that do not match any other application references.

## 8.2. Logging in and Licensing

This section describes the steps on Experience Portal for administering a SIP connection to the Session Manager.

**Step 1** - Launch a web browser, enter http://<IP address of the Avaya EPM server>/ in the URL, log in with the appropriate credentials and the following screen is displayed.

**Note** – All page navigation described in the following sections will utilize the menu shown on the left pane of the screenshot below.



**Figure 90: Experience Portal – Home page** 

**Step 2** - In the left pane, navigate to **Security→Licensing**. On the **Licensing** page, verify that Experience Portal is properly licensed. If required licenses are not enabled, contact an authorized Avaya account representative to obtain the licenses.

and All   Collapse All			
and Air I Conapse Air	You are here: <u>Home</u> > Security > Li	cansing	
er Management	Tou are herer <u>mome</u> > becarty > c	cerang	
les	and a second second second		
ers	Licensing		
gin Options	-		
al-time Monitoring			
stem Monitor	This page displays the Experien	ce Portal license information that is currently in effect. Experier	nce Portal use
tive Calls			
rt Distribution	License Server Information	<b>▼</b>	
stem Maintenance lit Log Viewer			
ce Viewer	License Server URL:	https://10.33.1.10:52233/WebLM/LicenseServer	<b>1</b>
Viewer	Last Updated:	Jan 28, 2021 4:33:55 AM EST	C.
m Manager	Last Successful Poll:	Jan 21, 2022 12:38:33 PM EST	
tem Management	Last Successiul Poll.	Jan 21, 2022 12, J0, JJ PH L31	
ication Server			
M Manager	Licensed Products -		
Manager	Licenseu Products •		0.00
ware Upgrade	Experience Portal		J
em Backup	Announcement Ports:	50	
em Configuration	ASR Connections:	250	
ations ervers	Call Anchoring Ports:	250	
ervers ervers	Email Units:	10	
vers	Enable Media Encryption:	250	
h Servers	Enhanced Call Classification:	250	
onnections	Google ASR Connections:	250	
24	Google Dialogflow Connections		
urity		250	
tificates	HTML Units:	50	
ensing	SIP Signaling Connections:		
ports	SMS Units:	10 50	
andard	Telephony Ports:		
tom	TTS Connections:	250	
eduled	Video Server Connections:	250	
ti-Media Configuration	Zones:	10	
ail ML	22 27	723	
5	Version:	8	
4	Last Successful Poll:	Jan 21, 2022 12:38:33 PM EST	
Home	Last Changed:	Apr 11, 2021 11:03:26 PM EDT	
Monitor			- 29
	Proactive Outreach Manage	r	J
	EMAIL Channels:	0	
	External Selection:	0	
	Manual Agents:	0	
	Manual Agents: Maximum Outbound Ports:	0	
	Predictive Agents:	0	
		0	
	Preview Agents: SMS Channels:		
		0	
	Agent Web API Service:	U	
	Administration of the second sec	2	
	Version:	3	
	Expiration Date:	Aug 3, 2021 12:00:00 AM EDT	
	Last Successful Poll:	Jan 21, 2022 12:38:33 PM EST	
	Last Changed:	Sep 2, 2021 12:02:42 AM EDT	

**Figure 91: Experience Portal – License** 

## 8.3. VoIP Connection

This section defines a SIP trunk between Experience Portal and Session Manager.

Step 1 - In the left pane, navigate to System Configuration→VoIP Connections. On the VoIP Connections page, select the SIP tab and click Add to add a SIP trunk.

Note – Only *one* SIP trunk can be active at any given time on Experience Portal.

Expand All   Collapse All	You are here: Home > System Configuration > VoIP Connect	ctions			
▼ User Management					
Roles	VoIP Connections				
Users	VOIP Connections				
Login Options ▼ Real-time Monitoring					
System Monitor	This page displays a list of Voice over Internet Protoc	al () (aTR) annual that Even arises an Rea	and an an an an inclusion of the	Veu ese seefeure endhiele CID -	
Active Calls	This page displays a list of voice over internet Protoc	of (VotP) servers that experience Por	tal communicates with.	You can configure multiple Ste o	connections, but only one site connection
Port Distribution					
<ul> <li>System Maintenance</li> </ul>					
Audit Log Viewer	<ul> <li>The information that you entered has been save</li> </ul>	ed.			
Trace Viewer Log Viewer					
Alarm Manager	H.323 SIP				
* System Management					
Application Server					
EPM Manager	🔲 📕 Zone 🗘 Name 🗘 Enable 🗘 Proxy Transport	t Proxy/DNS Server Address	Proxy Server Port	istener Port SIP Domain	Maximum Simultaneous Calls
MPP Manager		40.00.40.50	5064	0.54	10
Software Upgrade System Backup	Default interopSM Yes TLS	10.33.10.53	5061 5	061 bvwdev.com	10
System Configuration	Add Delete Help				
Applications	Aud Delete Help				
EPM Servers					
MPP Servers					
SNMP Speech Servers					
VoIP Connections					
Zones					
▼ Security					
Certificates					

**Figure 92: Experience Portal – VoIP Connection 1** 

**Step 2** - Configure a SIP connection as follows:

- Name Set to a descriptive name (e.g., interopSM)
- Enable Set to Yes
- **Proxy Transport** Set to **TLS**
- Select **Proxy Servers**, and enter:
  - **Proxy Server Address** = **10.33.10.53** (The IP address of the Session Manager)
  - **Port** = **5061**
  - **Priority** = 0 (default)
  - Weight = 0 (default)
- Listener Port Set to 5061
- **SIP Domain** Set to **bvwdev.com**
- Consultative Transfer Select INVITE with REPLACES
- SIP Reject Response Code Select ASM (503)
- Maximum Simultaneous Calls Set to a number in accordance with licensed capacity. In the reference configuration a value of 10 was used.
- Select All Calls can be either inbound or outbound
- SRTP Enable = Yes
- Encryption Algorithm = AES\_CM\_128
- Authentication Algorithm = HMAC\_SHA1\_80
- **RTCP Encryption Enabled = No**
- **RTP** Authentication Enabled = Yes

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes
SPOC 4/3/2022	©2022 Avaya Inc. All Rights Reserved.

- Click on Add to add SRTP settings to the Configured SRTP List
- Use default values for all other fields
- Click **Save** (Not shown)

You are here: Home > System Configuration > VoIP Connections > Change SIP Connection
Change SIP Connection
Use this page to change the configuration of a SIP connection.
Zone: Default V Name: interopSM
Enable: Ves No
Proxy Transport: TLS V
Proxy Servers O DNS SRV Domain
Address         Port         Priority         Weight           10.33.10.53         5061         0         0         Remove
Additional Proxy Server
Listener Port: 5061
SIP Domain: bvwdev.com
P-Asserted-Identity:
Maximum Redirection Attempts: 0
Consultative Transfer:   INVITE with REPLACES  REFER
SIP Reject Response Code: <ul> <li>ASM (503)</li> <li>SES (480)</li> <li>Custom</li> </ul>
SIP Timers
T1: 250 milliseconds
T2: 2000 milliseconds
B and F: 4000 milliseconds
Call Capacity
Maximum Simultaneous Calls: 10
All Calls can be either inbound or outbound
O Configure number of inbound and outbound calls allowed
SRTP
Enable:      Yes O No
Encryption Algorithm: <ul> <li>AES_CM_128</li> <li>NONE</li> </ul>
Authentication Algorithm: <ul> <li>HMAC_SHA1_80</li> <li>HMAC_SHA1_32</li> </ul>
RTCP Encryption Enabled: O Yes O No
RTP Authentication Enabled:  Yes O No Add
Configured SRTP List
SRTP-Yes,AES_CM_128,HMAC_SHA1_80,RTCP Encryption-No,RTP Authentication-Yes
Remove
Save Apply Cancel Help

**Figure 93: Experience Portal – VoIP Connection 2** 

HV; Reviewed: SPOC 4/3/2022

## 8.4. Speech Servers

The installation and administration of the ASR and TTS Speech Servers are beyond the scope of this document. Some of the values shown below were defined during the Speech Server installations. Note that in the reference configuration the ASR and TTS servers used the same IP address.

ASR speech server:

Expand All   Collapse All	You are here: Home > System Configuration > Speech Servers
▼ User Management	
Roles	Sauce & Sauces
Users	Speech Servers
Login Options	
▼ Real-time Monitoring	
System Monitor Active Calls	This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with.
Port Distribution	
▼ System Maintenance	
Audit Log Viewer	
Trace Viewer	ASR TTS
Log Viewer	
Alarm Manager	■ Zone ^ Name ^ Enable ^ Network Address ^ Engine Type ^ MRCP ^ Base Port ^ Total Number of Languages ^
<ul> <li>System Management</li> </ul>	■ Zone - Maine - Chable - Metwork Address - Engine Type - Metr - Base Port - Licensed ASR Resources - Languages -
Application Server	Default Nuance-ARS Yes 10.33.1.61 Nuance MRCP V2 TCP 5060 2 English(USA) en-US
EPM Manager	
MPP Manager Software Upgrade	Add Delete
System Backup	
▼ System Configuration	Customize Help
Applications	
EPM Servers	
MPP Servers	
SNMP	
Speech Servers	
VoIP Connections	
Zones	

Figure 94: Experience Portal – ASR Speech Server

TTS speech server:

Expand All   Collapse All	You are here: Home > System Configuration > Speech Servers
▼ User Management	
Roles	
Users	Speech Servers
Login Options	
▼ Real-time Monitoring	
System Monitor	This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with.
Active Calls	This page displays the list of Automated Speech Recognition (Fish) and Text to Speech (Tris) servers that experience Fortal communicates with
Port Distribution	
▼ System Maintenance	
Audit Log Viewer	ASR TTS
Trace Viewer	ASK 113
Log Viewer	
Alarm Manager	■ Zone ^ Name ^ Enable ^ Network Address ^ Engine Type ^ MRCP ^ Base Port ^ Total Number of _ Voices ^ Voices ^
<ul> <li>System Management</li> </ul>	■ Zone + Mane + Linable + Metwork Address + Lingine Type + MkCr + Base Fort + Licensed TTS Resources + Volkes +
Application Server	English(USA) en-US Allison F,
EPM Manager	English (USA) on US Ave E
MPP Manager	Default Nuance-TTS Yes 10.33.1.61 Nuance MRCP V2 TCP 5060 2 English(USA) en-US Nathan M,
Software Upgrade	
System Backup	English(USA) en-US Zoe F
<ul> <li>System Configuration</li> </ul>	Add Delete
Applications	Aut
EPM Servers	Customize Help
MPP Servers	Castomize neip
SNMP	
Speech Servers	
VoIP Connections	
Zones Zones	
- Carline	

Figure 95: Experience Portal – TTS Speech Server

## 8.5. Application

This section describes the steps for administering a reference to the VXML and/or CCXML applications residing on the application server. In the sample configuration, the applications were co-resident on one Experience Portal server, with IP Address 10.33.1.23.

- Step 1 In the left pane, navigate to System Configuration→Applications. On the Applications page (not shown), click Add to add an application and configure as follows:
  - Name Set to a descriptive name (e.g., Test-VXML)
  - **Enable** Set to **Yes**. This field determines which application(s) will be executed based on their defined criteria
  - **Type** Select **VoiceXML**, **CCXML**, or **CCXML/VoiceXML** according to the application type
  - **VoiceXML** and/or **CCXML URL** Enter the necessary URL(s) to access the VXML and/or CCXML application(s) on the application server. In the sample screen below, the Experience Portal test application on a single server is referenced
  - Speech Servers ASR and TTS Select the appropriate ASR and/or TTS servers as necessary
  - Application Launch Set to Inbound
  - **Called Number** Enter the number to match against an inbound SIP INVITE message and click **Add**. In the sample configuration illustrated in these Application Notes, the dialed DID number 4800 was used. Repeat to define additional called party numbers as needed. Inbound calls with these called party numbers will be handled by the application defined in this section.

You are here: <u>Home</u> >	System Confi	iguration > <u>Applications</u> >	Change Ap	plication	
Change App	lication	n			
Use this page to cha	nge the con	nfiguration of an applicat	ion.		
Zone:	Default				
Name:	Test-VXML				
Enable:	Yes				
Type:	VoiceXM				
Reserved SIP Calls:	None	e 🔍 Minimum 🔍 Maxi	mum		
Requested: URI					
Single Fail (	Over 🔍 Lo	ad Balance			
VoiceXML URL:	https://	/10.33.1.23/mpp/misc/a	vptestapp	/intro.vxml	
Mutual Certificate Au Basic Authentication:		n: • Yes · No • Yes • No			
ASR Speech Server	rs 🔻				
Engine Ty				Selected Er	igine Types
<none></none>	pes		-	Nuance	igine rypes
ASR:			, õ	Compare Anguerre	
Nuance					
Languages			Selected	Languages	
<none></none>		Û Q	English	(USA) en-US	5
Resources:		Acquire on call start	and reta	iin 🔻	
N Best List Length:					
10	magut	0 milliseco	- 10		
Speech Complete Til					
Speech Incomplete	limeout:	milliseco	nas		
Vendor Parameters:			1		
TTS Speech Server	s ▼				
	Voices				Selected Voices
TTS: Nuance V	English(	USA) en-US Ava F USA) en-US Nathan M USA) en-US Zoe F			English(USA) en-US Allison F
Application Launch	. •				
Inbound      In					
Number      Nu					
Called Number:	100	Add			
4800				*	Remove
Speech Parameters	s 🕨				
Reporting Paramet	ters 🕨				
Advanced Paramet	ers 🕨				
Save Apply	Cancel	Help			

### **Figure 96: Experience Portal – Application**

HV; Reviewed: SPOC 4/3/2022 Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved.

95 of 104 TN\_CMSM81SBC81

## 8.6. MPP Servers and VoIP Settings

This section illustrates the procedure for viewing or changing the MPP Settings. In the sample configuration, the MPP Server is co-resident on a single server with the Experience Portal Management server (EPM).

Step 1 - In the left pane, navigate to System Configuration→MPP Servers and the following screen is displayed. Click Add.

Expand All   Collapse All	You are here: Home > System Configuration > MPP Servers
▼ User Management Roles Users	MPP Servers
Login Options • Real-time Monitoring System Monitor Active Calls Port Distribution	This page displays the list of Media Processing Platform (MPP) servers in the Experience Portal system. When an MPP receives a call from a PBX, it invokes
▼ System Maintenance Audit Log Viewer Trace Viewer Log Viewer	■ Zone ↓ Name ↓ Host Address ↓ Network Address ↓ Network Address ↓ Address ↓ Address ↓ Address ↓ Address ↓ Address ↓ Simultaneous Calls ↓ Trace Level ↓
Alarm Manager System Management Application Server EPM Manager MPP Manager	Default mpp80 ep80.bvwdev.com <default> <default> <default> 10 Use MPP Settings Add Delete</default></default></default>
Software Upgrade System Backup • System Configuration Applications	MPP Settings Browser Settings Video Settings VoIP Settings Help
Applications EPM Servers <u>MPP Servers</u> SNMP Speech Servers	

### Figure 97: Experience Portal – MPP Server 1

- Step 2 Enter any descriptive name in the Name field (e.g., mpp80) and the IP address of the MPP server in the Host Address field and click Continue (not shown). Note that the Host Address used is the same IP address assigned to Experience Portal.
- Step 3 The certificate page will open. Check the **Trust this certificate** box (not shown). Once complete, click **Save**.

Expand All   Collapse All	You are here: Home > System Ma	intenance	> System Mo	nitor > mpp80 Details > Change MPP Server				
▼ User Management	noo are neret nome - bystem Ma	menance	- System MO	ntor - mppoo petans - onange mrr berver				
Roles	Change MDD Came							
Users	Change MPP Serve	er						
Login Options								
▼ Real-time Monitoring			1 10.00 000000					
System Monitor	Use this page to change the configuration of an MPP. Take care when changing the MPP Trace Logging Thresholds. Do not set Trace Levels							
Active Calls	to Finest only when you are tr	oublesho	oting the sys	em.				
Port Distribution								
▼ System Maintenance		0 2 8						
Audit Log Viewer	Zone:	Default						
Trace Viewer	Name:	mpp80						
Log Viewer								
Alarm Manager	Host Address:	ep80.bv	wdev.com					
▼ System Management	Network Address (VoIP):	<defau< th=""><th>lt&gt;</th><th></th></defau<>	lt>					
Application Server	Network Address (volt):	~Deruo	1C-2					
EPM Manager	Network Address (MRCP):	<defau< th=""><th>lt&gt;</th><th></th></defau<>	lt>					
MPP Manager		- Derad						
Software Upgrade	Network Address (AppSvr):	<defau< th=""><th>lt&gt;</th><th></th></defau<>	lt>					
System Backup			979000 9					
▼ System Configuration	Maximum Simultaneous Calls:	10						
Applications		1	1					
EPM Servers	Restart Automatically:	O Vor	No No					
MPP Servers	restare reacondedauj r	0165						
SNMP								
Speech Servers	MPP Certificate							
VoIP Connections								
Zones								
▼ Security	Owner: C=US,ST=CO,L=Thornt	on 0=3177	VA OU-STI	Naango burdey com				
Certificates	Issuer: 0=AVAYA, OU=MGMT, CN			n-epot.bvwdeo.com				
Licensing	Serial Number: 52301cea350		lanayer on					
▼ Reports								
Standard	Signature Algorithm: SHA256withRSA Version: 3							
Custom	Version: 3 Valid from: March 1, 2021 11:54:52 AM EST until March 1, 2023 11:54:52 AM EST							
Scheduled	Certificate Fingerprints	11.04.02	AN EST UN	AIT MAICH 1, 2023 11.04.02 AT EST				
▼ Multi-Media Configuration	MD5: b2:56:8c:12:7	2 - 64 - 14 -	54-21-9b-2	- 6b - 49 - 54 - 93 - 7a				
Email				:7b:98:f8:5d:8e:90:45:0e:a8				
HTML				7:31:7f:ce:b8:f9:b3:6b:34:af:81:91:3f:a7:2f:53:eb:83:e8:3e:e9:65:26				
SMS	Key Usage:							
▼ POM	Digital Signature							
POM Home	Non Repudiation							
POM Monitor	Key Encipherment							
	Data Encipherment							
	Key Agreement							
	Extended Key Usages:							
	Client Auth							
	Server Auth							
	Basic Constraints:							
	CA: false							
	Path Len Constrain	t · undet	Fined					
	Subject Alternative Names	o. ander						
	DNS Name: ep80							
	DNS Name: ep80.bvw	dett com						
	IP Address: 10.33							
	11 11412551 101001							
	Categories and Trace Levels							
	categories and trace Levels							
	Save Apply Canc	el H	elp					
	Curres Curres							

### Figure 98: Experience Portal – MPP Server 2

Step 4 - Click VoIP Settings tab on the screen displayed in Step 1.

- In the Port Ranges section, default ports were used. •
- In the Codecs section set: •
  - Set Packet Time to 20
  - Verify Codecs G711uLaw, G711aLaw and G729 are enabled (check marks) in Offer Codec and Answer Codec. Set the Offer Order and Answer Order as shown. In the sample configuration G711uLaw is the preferred codec, with Order 1, followed by G711aLaw with Order 2 and G729 with Order 3. On the codec Offer, set G729 Discontinuous Transmission to No (for G.729A)

• Use default values for all other fields

Step 5 - Click on Save (not shown)

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	97 of 104
SPOC 4/3/2022	©2022 Avaya Inc. All Rights Reserved.	TN_CMSM81SBC81

You are here: <u>Home</u> > System Configuration > <u>MPP Servers</u> > VoIP Settings				
VoIP Settings				
Voice over Internet Protocol (VoIP) is the process of sending voice data through a network using one or more standard protocols such as H.323 and Real-time Transfer Protocol (RTP). Use this page to configure parameters that affect how voice data is transferred through the network. Note that if you make any changes to this page, you must restart all MPPs.				
Port Ranges 🔻				
Low         High           UDP:         11000         30999           TCP:         31000         33499           MRCP:         34000         36499           H.323         37000         39499           Station:         37000         39499				
RTCP Monitor Settings 🔻				
Host Address: Port:				
VoIP Audio Formats 🔻				
MPP Native Format: audio/basic 🔻				
Codecs 🔻				
Enable Codec     Order       Image: Codec order     Image: Codec order				
Packet Time: 20 V milliseconds				
G729 Discontinuous Transmission: 🔍 Yes 💿 No				
Answer				
EnableCodecOrderImage: Second system1Image: Second system2Image: Second system3				
G729 Discontinuous Transmission: 🔍 Yes 🔍 No 💿 Either				
G729 Reduced Complexity Encoder:   Yes No				
QoS Parameters > Out of Service Threshold (% of VoIP Resources) > Call Progress > Miscellaneous >				
Save Apply Cancel Help				

## Figure 99: Experience Portal – MPP Server - VoIP

## 8.7. Configuring RFC2833 Event Value Offered by Experience Portal

The configuration change example noted in this section was not required for any of the call flows illustrated in these Application Notes. For incoming calls from Service Provider (SP) to Experience Portal, SP specifies the value 101 for the RFC2833 telephone-events that signal DTMF digits entered by the user. When Experience Portal answers, the SDP from Experience Portal matches this SP offered value.

When Experience Portal sends an INVITE with SDP as part of an INVITE-based transfer (e.g., bridged transfer), Experience Portal offers the SDP. By default, Experience Portal specifies the value 127 for the RFC2833 telephone-events. Optionally, the value that is offered by Experience Portal can be changed, and this section outlines the procedure that can be performed by an Avaya authorized representative.

- Access Experience Portal via the command line interface.
- Navigate to the following directory: /opt/Avaya/ ExperiencePortal/MPP/config
- Edit the file mppconfig.xml.
- Search for the parameter "mpp.sip.rfc2833.payload". If there is no such parameter specified add a line such as the following to the file, where the value 101 is the value to be used for the RFC2833 events. If the parameter is already specified in the file, simply edit the value assigned to the parameter. cparameter name="mpp.sip.rfc2833.payload">101</parameter>
- In the verification of these Application Notes, the line was added directly above the line where the sip.session.expires parameter is configured.

After saving the file with the change, restart the MPP server for the change to take effect. As shown below, the MPP may be restarted using the **Restart** button available via the Experience Portal GUI at **System Management**  $\rightarrow$  **MPP Manager**.

Note that the **State** column shows when the MPP is running after the restart.

-			
Expand All   Collapse All	You are here: <u>Home</u> > System Management > MPP Manager		
User Management			
Roles			
Users	MPP Manager (Jan 21, 2022 1:31:59 PM EST)		
Login Options			
▼ Real-time Monitoring			
System Monitor	This page displays the current state of each MPP in the Experience Portal system. To enable the state and		
Active Calls			
Port Distribution			
▼ System Maintenance			
Audit Log Viewer	Last Poll: Jan 21, 2022 1:31:39 PM EST		
Trace Viewer			
Log Viewer	Zone Server Name Mode State Config Auto Restart Schedule Active Calls		
Alarm Manager	Zone Server Name Houe State Config Auto Restart Today Recurring In Out		
▼ System Management			
Application Server	Default mpp80 Online Running OK Yes No No None 0 0		
EPM Manager			
MPP Manager			
Software Upgrade	State Commands		
System Backup			
▼ System Configuration	Start Stop Restart Reboot Halt Cancel Restart/Reboot Options		
Applications	Start Stop Restart Reboot Halt Cancel Restart/Reboot Options		
EPM Servers			
MPP Servers	One server at a time		
SNMP	Mode Commands		
Speech Servers	All servers		
VoIP Connections			
Zones	Offline Test Online		
▼ Security			
C. N.C. I.			

**Figure 100: Experience Portal – MPP Manager** 

HV; Reviewed: SPOC 4/3/2022

# 9. Telia Norway SIP Trunk Configuration

Telia Norway is responsible for the configuration of Telia Norway SIP Trunk Service. Customer must provide the IP Address used to reach the Avaya SBCE public interface at the enterprise. Telia Norway will provide the customer necessary information to configure the SIP connection between Avaya SBCE and Telia Norway. Telia Norway also provides the Telia Norway SIP Specification document for reference. This information is used to complete configurations for Communication Manager, Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between Telia Norway SIP Trunk and the enterprise used static IP Addresses.

# 10. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

Verification Steps:

- 1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- 2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
- 3. Verify that the user on the PSTN can end an active call by hanging up.
- 4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Troubleshooting:

- 1. Communication Manager: Enter the following commands using the Communication Manager System Access Terminal (SAT) interface.
  - **list trace station** <extension number> Traces calls to and from a specific station.
  - **list trace tac** <trunk access code number> Trace calls over a specific trunk group.
  - **status station** <extension number> Displays signaling and media information for an active call on a specific station.
  - **status trunk-group** <trunk-group number> Displays trunk-group state information.
  - **status signaling-group** <signaling-group number> Displays signaling-group state information.
- 2. Session Manager:
  - Call Routing Test The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to Elements → Session Manager → System Tools → Call Routing Test. Enter the requested data to run the test.
  - **traceSM** Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.
- 3. Avaya SBCE: Debug logging can be started in two different ways:
  - GUI of the SBC: Monitoring & Logging → Debugging. Check on Debug option
    - SIP only: enable LOG\_SUB\_SIPCC subsystem under SSYNDI process.
    - CALL PROCESSING: enable all subsystems under SSYNDI process.
    - The log files are stored at: /usr/local/ipcs/log/ss/logfiles/elog/SSYNDI.
  - **Command Line Interface**: Login with root user and enter the command: **#traceSBC**. The tool updates the database directly based on which trace mode is selected.

# 11. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura<sup>®</sup> Communication Manager 8.1.3, Avaya Aura<sup>®</sup> System Manager 8.1.3, Avaya Aura<sup>®</sup> Session Manager 8.1.3, Avaya Aura<sup>®</sup> Experience Portal 8.1 and Avaya Session Border Controller for Enterprise 8.1.3 to Telia Norway. This solution successfully passed compliance testing via the Avaya DevConnect Program.

## 12. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya, including the following, is available at: <u>http://support.avaya.com/</u>

#### Avaya Aura<sup>®</sup> Communication Manager

[1] Administering Avaya Aura ®Communication Manager, Release 8.1.x, Issue 12, July 2021

#### Avaya Aura<sup>®</sup> Session Manager/System Manager

- [2] Administering Avaya Aura® Session Manager, Release 8.1.x, Issue 10, September 2021
- [3] Administering Avaya Aura® System Manager, Release 8.1.x, Issue 17, November 2021

#### Avaya Session Border Controller for Enterprise

[4] Avaya Session Border Controller for Enterprise 8.1.3.0 Release Notes, Release 8.1.3.0, Issue 1, August 2021

#### Avaya Aura Experience Portal

[5] Administering Avaya Aura® Experience Portal, Release 8.1, Issue 1, July 2021

#### **Avaya Phones**

- [6] Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones H.323, Release 6.8.2, Issue 1, June 2019
- [7] Installing and Administering Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP Release 7.1.7, Issue 1, October 2019
- [8] Avaya one-X® Communicator Release 6.2 SP14 Release Notes, Issue 1.0, June 2019
- [9] Avaya Workplace Client (Windows) Release 3.23.1 Release Notes, Issue 1.0, December 2021

#### **Remote Worker**

 [10] Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel.
 7.0, Avaya Aura® Communication Manager Rel.
 7.0 and Avaya Aura® Session Managers Rel.
 7.0 - Issue 1.0

#### IETF (Internet Engineering Task Force) SIP Standard Specifications

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

Product documentation for Telia Norway SIP Trunking may be found at: http://telia.no

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	102 of 104
SPOC 4/3/2022	©2022 Avaya Inc. All Rights Reserved.	TN_CMSM81SBC81

# 13. Appendix A - SigMa Script

The following is the Signaling Manipulation script used in the configuration of the SBCE, **Section 7.4**.

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and
%ENTRY POINT="POST ROUTING"
     {
//Change the SIPs to SIP
    %HEADERS["Request_Line"][1].regex_replace("sips","sip");
    %HEADERS["FROM"][1].regex_replace("sips","sip");
    %HEADERS["P-Asserted-Identity"][1].regex_replace("sips","sip");
    %HEADERS["Contact"][1].regex_replace("sips","sip");
    %HEADERS["To"][1].regex_replace("sips","sip");
    %HEADERS["Diversion"][1].regex_replace("sips","sip");
// Remove unwanted Headers
      remove(%HEADERS["History-Info"][3]);
      remove(%HEADERS["History-Info"][2]);
      remove(%HEADERS["History-Info"][1]);
      remove(%HEADERS["P-Charging-Vector"][1]);
      remove(%HEADERS["P-AV-Message-Id"][1]);
      remove(%HEADERS["Av-Global-Session-ID"][1]);
      remove(%HEADERS["P-Location"][1]);
      }
```

}

#### ©2022 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by <sup>®</sup> and <sup>TM</sup> 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