



# **Application Notes for Avaya Aura® Communication Manager, Avaya Aura® Session Manager Rel. 7.1 and Avaya Session Border Controller for Enterprise Rel. 7.2 with CenturyLink SIP Trunking Service on Perimeta/BroadWorks Platform using TLS – Issue 1.0**

## **Abstract**

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service on an enterprise solution consisting of Avaya Aura® Communication Manager Rel. 7.1.2, Avaya Aura® Session Manager Rel. 7.1.2 and Avaya Session Border Controller for Enterprise Rel. 7.2.1, to interoperate with the CenturyLink SIP Trunking service on Perimeta/BroadWorks Platform using TLS and SRTP.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints. For privacy, Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) were used inside of the enterprise (private network side) and outside of the enterprise (public network side).

The CenturyLink SIP Trunking service provide customers with PSTN access via a SIP trunk between the enterprise and the CenturyLink network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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.

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

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results .....	6
2.3.	Support .....	8
3.	Reference Configuration .....	9
4.	Equipment and Software Validated .....	12
5.	Configure Avaya Aura® Communication Manager .....	13
5.1.	Licensing and Capacity .....	13
5.2.	System Features.....	14
5.3.	IP Node Names.....	16
5.4.	Codecs .....	17
5.5.	IP Network Regions .....	19
5.6.	Signaling Group .....	20
5.7.	Trunk Group .....	23
5.8.	Calling Party Information.....	27
5.9.	Inbound Routing.....	28
5.10.	Outbound Routing .....	29
6.	Configure Avaya Aura® Session Manager .....	33
6.1.	System Manager Login and Navigation.....	34
6.2.	SIP Domain .....	35
6.3.	Locations .....	35
6.4.	Adaptations.....	38
6.5.	SIP Entities .....	40
6.6.	Entity Links .....	43
6.7.	Routing Policies .....	45
6.8.	Dial Patterns .....	46
7.	Configure Avaya Session Border Controller for Enterprise .....	49
7.1.	System Access.....	49
7.2.	System Management .....	51
7.3.	Network Management .....	54
7.4.	Media Interfaces .....	55
7.5.	Signaling Interfaces.....	57
7.6.	Server Interworking.....	59
7.6.1.	Server Interworking Profile – Enterprise.....	59
7.6.2.	Server Interworking Profile – Service Provider.....	62
7.7.	Signaling Manipulation .....	64
7.8.	Server Configuration .....	66
7.8.1.	Server Configuration Profile – Enterprise .....	66
7.8.2.	Server Configuration Profile – Service Provider .....	68
7.9.	Routing .....	72
7.9.1.	Routing Profile – Enterprise .....	72

7.9.2.	Routing Profile – Service Provider .....	73
7.10.	Topology Hiding.....	74
7.10.1.	Topology Hiding Profile – Enterprise.....	74
7.10.2.	Topology Hiding Profile – Service Provider.....	76
7.11.	Domain Policies.....	77
7.11.1.	Application Rules.....	77
7.11.2.	Media Rules.....	78
7.11.3.	Signaling Rules .....	82
7.12.	End Point Policy Groups .....	83
7.12.1.	End Point Policy Group – Enterprise .....	83
7.12.2.	End Point Policy Group – Service Provider.....	84
7.13.	End Point Flows.....	85
7.13.1.	End Point Flow – Enterprise .....	86
7.13.2.	End Point Flow – Service Provider .....	87
8.	CenturyLink SIP Trunking Service on Perimeta/BroadWorks Platform Configuration .....	88
9.	Verification and Troubleshooting .....	88
9.1.	General Verification Steps .....	88
9.2.	Communication Manager Verification.....	88
9.3.	Session Manager Verification .....	89
9.4.	Avaya SBCE Verification .....	91
10.	Conclusion .....	96
11.	References.....	96
12.	Appendix A: SigMa Script.....	97

# 1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the CenturyLink network on Perimeta/BroadWorks Platform and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Rel. 7.1.2 (Communication Manager), Avaya Aura® Session Manager Rel. 7.1.2 (Session Manager), Avaya Session Border Controller for Enterprise Rel. 7.2.1 (Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

For privacy, Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) were used inside of the enterprise (private network side) and outside of the enterprise (public network side).

The CenturyLink SIP Trunking service on Perimeta/BroadWorks Platform referenced within these Application Notes is designed for business customers. Customers using this service with this Avaya enterprise solution 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 analog and/or ISDN-PRI.

The terms “Service Provider” or “CenturyLink” will be used interchangeably throughout these Application Notes.

## 2. General Test Approach and Test Results

A simulated CPE site containing all the equipment for the Avaya SIP-enabled enterprise solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the network via a broadband connection to the public Internet.

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 only (private network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

## 2.1. Interoperability Compliance Testing

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

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to DID numbers assigned by CenturyLink. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x1 Series IP Deskphones (H.323 and SIP), Avaya 2420 Digital Deskphones, Avaya one-X® Communicator softphone (H.323 and SIP), Avaya Equinox softphone (SIP) and analog Deskphones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya 96x1 Deskphones (SIP).
- Outgoing calls to the PSTN were routed via CenturyLink's network to various PSTN destinations.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper Codec negotiation and two-way speech-path. Testing was performed with codecs: G.711MU and G.729.
- No matching codecs.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- EC500 (Extension to Cellular) calls.
- Routing inbound vector call to call center agent queues.
- T.38 fax.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.

**Note** – Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes.

Items that are supported but that were not tested includes the following:

- Inbound toll-free calls and 911 calls (emergency) calls.

## 2.2. Test Results

Interoperability testing of the CenturyLink SIP Trunking Service on Perimeta/BroadWorks Platform with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the observations/limitations noted below:

- **OPTIONS** – CenturyLink does not send OPTIONS messages to the Avaya enterprise network but it does respond to OPTIONS messages it receives from the Avaya enterprise, this was sufficient to maintain the SIP trunk link up in service.
- **481 Call/Transaction does not exist** – After a call from the PSTN to the enterprise is successfully transferred back to another PSTN party using the SIP REFER method, CenturyLink accepted the SIP REFER messages sent by Communication Manager with “202 Accepted”, which resulted in the SIP trunk channels being released with BYE messages, as expected. After the SIP trunk channels were released CenturyLink would send “481 Call/Transaction Does Not Exist” in response to a BYE message sent by Communication Manager, this was caused by CenturyLink not sending NOTIFY messages to Communication Manager to update the state of the call transfer. This behaviour had no negative impact on the transferred call and SIP trunk resources were released successfully after the call transfer, as expected. It’s being mentioned here simply as an observation.
- **URI in PAI Header should be set to the Pilot Number** – For EC500 (Extension to Cellular) and for calls that are forwarded to the PSTN CenturyLink SIP trunking specification requires the URI in the PAI header to be the pilot number. This was accomplished by using a Signaling Manipulation script (SigMa) in the Avaya SBCE. Refer to **Section 7.7**.
- **Outbound T.38 Fax issue with G.729** – CenturyLink supports codecs G.711MU and G.729, for outbound T.38 fax calls from the enterprise to the PSTN, the initial voice/audio connection was always set up by CenturyLink with codec G.729, instead of G.711MU. This was always the case, even if the codec priority order sent by Communication Manager had G.711MU listed first and G.729 second. This behavior caused Communication Manager to timeout, since it never detected fax tone from the far end, the re-INVITE for T.38 fax negotiation was never sent by CenturyLink. The solution to this issue is to configure Communication Manager to only support codec G.711MU, instead of G.711MU and G.729 both. Note that the testing was done with codecs G.711MU and G.729 both configured in Communication Manager, as shown in **Section 5.4**. Thus, if T.38 fax is required by the enterprise, only codec G.711MU should be configured in Communication Manager. This issue is under investigation by CenturyLink. It should also be noted that fax modes “pass-through” and “t.38-G711-fallback” are not supported by Communication Manager with SRTP media encryption, only T.38 fax is supported with the media encryption configuration used during the compliance test.
- **One-way audio on Avaya one-X® Communicator softphones** – Calls originated from the Avaya one-X® Communicator softphone (in SIP mode) to the PSTN resulted in one-way audio. The cause is related to the codec priority order in the final ACK message CenturyLink receives from the Avaya one-X® Communicator softphone (in SIP mode)

during the shuffling of the call (shuffling = during the establishment of direct media connection between endpoints). The Avaya one-X® Communicator softphone (in SIP mode) sends the codec priority order with G.711MU listed first and G.729 listed second in the final ACK message it sends to establish direct media connection between endpoints. The one-way audio issue appears to be related to a codec mismatch caused by CenturyLink not being able to prioritize codecs and accept the first codec listed in the ACK message it receives. The initial voice/audio connection was always set up by CenturyLink with codec G.729, instead of G.711MU. The workaround is to include a signaling manipulation script (SigMa) for the CenturyLink Server Configuration profile on the Avaya SBCE to remove codec G.729 from the final ACK message sent by the Avaya one-X® Communicator softphone (in SIP mode) during the establishment of direct media connection between endpoints, thus only sending codec G.711MU to CenturyLink. Refer to **Section 7.7**. The one-way audio issue was only observed on the Avaya one-X® Communicator softphone in SIP mode (not in H.323 mode), this behavior was not observed with any other softphone or Deskphones type, H.323 or SIP.

- **Incorrect Call Display on call transfers to the PSTN Phone** – Call display was not properly updated on PSTN phones involved in a call transfers. After successful call transfers to the PSTN, the PSTN phone did not display the actual connected party, instead the DID number assigned to the Communication Manager station that initiated the transfer was displayed.
- **SIP NCR using SIP REFER when Redirected Party is busy** – This was not tested since it requires the service provider to support sending intermediate call states (100 Trying, 180 Ringing, etc.) of the referred call back to the referring party. This is done via NOTIFY messages in response to the REFER request, before the referring party is disconnected. CenturyLink doesn't send NOTIFY messages with SIP REFER during call redirection scenarios.
- **No media encryption in re-INVITE messages** – Setting the **Extensions** to **Lync** in the Avaya SBCE fixes an issue with media encryption (SRTP) in re-INVITE messages sent by the Avaya SBCE to CenturyLink. The issue is that re-INVITE messages do not include media encryption information in the SDP. The cause for this behavior in the Avaya SBCE is related to the use of SIP, instead of SIPS URI in SIP messages the Avaya SBCE receives from CenturyLink, if the Avaya SBCE receives SIP, instead of SIPS in the URI messages, the Avaya SBCE will not include media encryption information in the SDP of re-INVITE messages it sends back to the Service Provider, resulting in the call being rejected by the Service Provider if media encryption (SRTP) is enforced, which was the case with CenturyLink. The work around is to set the **Extensions** to **Lync** in the Avaya SBCE, as shown in **Section 7.6.2**.
- **SIP header optimization** – There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider's network. These headers were removed with the purpose of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider's network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector and P-Location (**Section 6.4**).

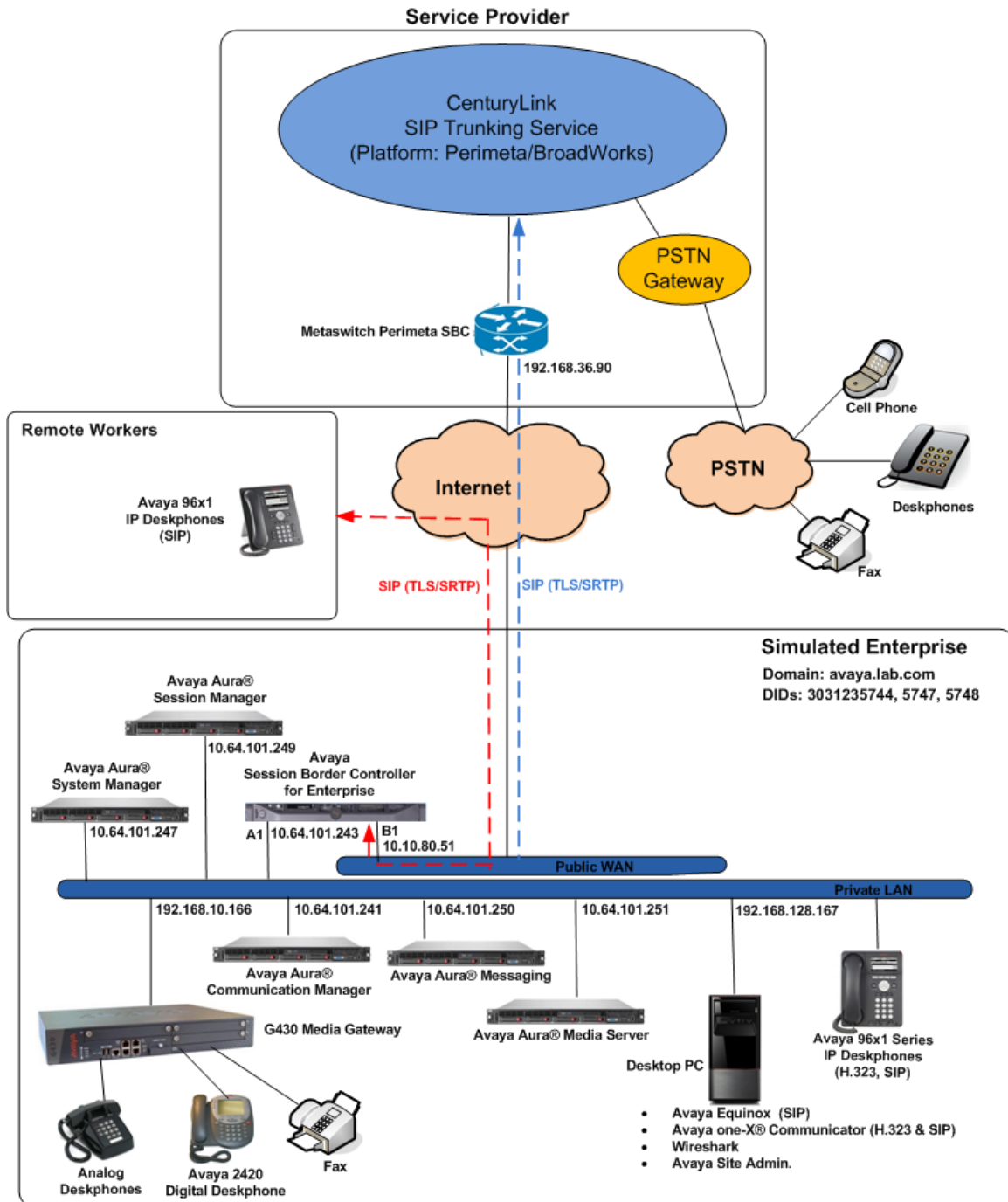
## 2.3. Support

For support of CenturyLink SIP Trunking Service on Perimeta/BroadWorks Platform visit the corporate Web page at: <http://www.centurylink.com/business/voice/sip-trunk.html>



### 3. Reference Configuration

**Figure 1** illustrates the sample Avaya SIP-enabled enterprise solution, connected to the CenturyLink SIP Trunking Service on Perimeta/BroadWorks Platform through a public Internet WAN connection.



**Figure 1: Avaya SIP Enterprise Solution connected to CenturyLink SIP Trunking Service**

The Avaya components used to create the simulated enterprise customer site included:

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya Aura® Messaging.
- Avaya Aura® Media Server.
- Avaya G430 Media Gateway.
- Avaya 96x1 Series IP Deskphones (H.323 and SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Equinox softphone (SIP).
- Avaya digital and analog telephones.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to Session Manager at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test using only the Avaya 96x1 SIP Deskphones. For signaling, Transport Layer Security (TLS) and for media, Secure Real-time Transport Protocol (SRTP) was used on Avaya 96x1 SIP Deskphones used to test remote worker functionality. Other Avaya SIP endpoints that are supported in a Remote Worker configuration deployment were not tested.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult [9] in the **References** section for additional information on this topic.

The Avaya SBCE was located at the edge of the enterprise. Its public side was connected to the public Internet, while its private side was connected to the enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flowed through the Avaya SBCE, protecting in this way the enterprise against any SIP-based attacks. The Avaya SBCE also performed network address translation at both the IP and SIP layers.

For inbound calls, the calls flowed from the service provider to the Avaya SBCE then to Session Manager. Session Manager used the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case Communication Manager) and on which link to send the call. Once the call arrived at Communication Manager, further incoming call treatment, such as incoming digit translation was performed.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns (or regular expressions) and

routing policies to determine the route to the Avaya SBCE for egress to the CenturyLink network.

A separate SIP trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk without affecting other enterprise SIP traffic. This trunk carried both inbound and outbound traffic.

As part of the Avaya Aura® version 7.1.2 release, Communication Manager incorporates the ability to use the Avaya Aura® Media Server (AAMS) as a media resource. The AAMS is a software-based, high density media server that provides DSP resources for IP-based sessions. Media resources from both the AAMS and a G430 Media Gateway were utilized during the compliance test. The configuration of the AAMS is not discussed in this document. For more information on the installation and administration of the AAMS in Communication Manager refer to the AAMS documentation listed in the **References** section.

Avaya Aura® Messaging was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of Message Waiting Indicator (MWI) messages to the enterprise telephones. Since the configuration tasks for Messaging are not directly related to the interoperability tests with the CenturyLink network SIP Trunking service, they are not included in these Application Notes.

For the compliance testing associated with this Application Notes, encryption capabilities were used for security, TLS transport for signaling and SRTP for media was used inside of the enterprise (private network side, in between Avaya components) and outside of the enterprise (public network side, in between the Avaya enterprise and CenturyLink).

**Note** - The configuration tasks required to support TLS transport for signaling and SRTP for media inside of the enterprise (private network side, in between Avaya components) and outside of the enterprise (public network side, in between the Avaya enterprise and CenturyLink) are beyond the scope of these Application Notes; hence they are not discussed in this document.

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya Aura® Communication Manager	7.1.2.0 (R017x.01.0.532.0 Patch 24184)
Avaya Aura® Session Manager	7.1.2.0.712004
Avaya Aura® System Manager	7.1.2.0 Build No. - 7.1.0.0.1125193 Software Update Revision No: 7.1.2.0.057353 Feature Pack 2
Avaya Session Border Controller for Enterprise	7.2.1-05-14222
Avaya Aura® Messaging	MSG-00.0.441.0-017_0004
Avaya Aura® Media Server	7.8.0.355_2017.11.15
Avaya G430 Media Gateway	38.21.0
Avaya 96x1 Series IP Deskphones (SIP)	Version 7.1.2.0.13
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.6506
Avaya one-X® Communicator (H.323, SIP)	6.2.12.21-SP12-Patch11
Avaya Equinox (SIP)	3.3.1.60
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
<b>CenturyLink</b>	
BroadSoft BroadWorks	R21.SP1
Metaswitch Perimeta SBC	V4.1.40_SU15_P01.02

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

**Note** – The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the previous table were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 6.0.0) platforms. Consult the installation documentation on the **References** section for more information.

## 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager to work with the CenturyLink SIP Trunking Service on Perimeta/BroadWorks Platform. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider. It is assumed that the general installation of Communication Manager, the Avaya G430 Media Gateway and the Avaya Aura® Media Server has been previously completed and is not discussed here.

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. Some screens captures will show the use of the **change** command instead of the **add** command, since the configuration used for the testing was previously added.

### 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 and from the service provider. The example shows that **24000** licenses are available and **120** 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.

```
display system-parameters customer-options                               Page 2 of 12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 12000 0
      Maximum Concurrently Registered IP Stations: 18000 1
      Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
      Maximum Concurrently Registered IP eCons: 414 0
      Max Concur Registered Unauthenticated H.323 Stations: 100 0
      Maximum Video Capable Stations: 41000 0
      Maximum Video Capable IP Softphones: 18000 6
      Maximum Administered SIP Trunks: 24000 120
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
      Maximum Number of DS1 Boards with Echo Cancellation: 522 0

(NOTE: You must logoff & login to effect the permission changes.)
```

## 5.2. System Features

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

```
display system-parameters features                                     Page 1 of 19
FEATURE-RELATED SYSTEM PARAMETERS
  Self Station Display Enabled? n
  Trunk-to-Trunk Transfer: all
  Automatic Callback with Called Party Queuing? n
  Automatic Callback - No Answer Timeout Interval (rings): 3
  Call Park Timeout Interval (minutes): 10
  Off-Premises Tone Detect Timeout Interval (seconds): 20
  AAR/ARS Dial Tone Required? y

  Music (or Silence) on Transferred Trunk Calls? no
  DID/Tie/ISDN/SIP Intercept Treatment: attendant
  Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
  Automatic Circuit Assurance (ACA) Enabled? n

  Abbreviated Dial Programming by Assigned Lists? n
  Auto Abbreviated/Delayed Transition Interval (rings): 2
  Protocol for Caller ID Analog Terminals: Bellcore
  Display Calling Number for Room to Room Caller ID Calls? n
```

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 *restricted* for restricted calls and *unavailable* for unavailable calls.

```
display system-parameters features                                     Page 9 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: unavailable

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
```

### 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 of Communication Manager (**procr**) and the Session Manager security module (**SM**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
ASBCE_A1	10.64.101.243	
SM	10.64.101.249	
default	0.0.0.0	
media_server	10.64.101.251	
procr	10.64.101.241	
procr6	::	
( 6 of 6 administered node-names were displayed )		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		



## 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. For the compliance test, ip-codec-set 2 was used for this purpose. Enter the corresponding codec in the **Audio Codec** column of the table. CenturyLink supports audio codecs *G.711MU* and *G.729*.

**Note** - If T.38 fax is required by the enterprise, only codec G.711MU should be configured (refer to **Section 2.2**).

change ip-codec-set 2 Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 2

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1:	G.711MU	n	2	20
2:	G.729	n	2	20
3:		-	-	
4:		-	-	
5:		-	-	
6:		-	-	
7:		-	-	

Media Encryption

1: 1-srtp-aescm128-hmac80

2: none

3:

4:

5:

Encrypted SRTCP: best-effort

On **Page 2**, set the **Fax Mode** to *t.38-standard* (refer to **Section 2.2**).

change ip-codec-set 2

Page 2 of 2

IP MEDIA PARAMETERS

Allow Direct-IP Multimedia? n

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

Media Connection IP Address Type Preferences

1: IPv4

2:

## 5.5. IP Network Regions

Create a separate IP network region for the service provider trunk group. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP Network Region 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avaya.lab.com** as assigned to the shared test environment in the Avaya test lab. This domain name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to **yes**, the default setting. This will enable **IP-IP Direct Audio** (shuffling), to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway and Media Server. Shuffling can be further restricted at the trunk level on the Signaling Group form if needed.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values may be used for all other fields.

change ip-network-region 2		Page 1 of 20
IP NETWORK REGION		
Region: 2	NR Group: 2	
Location: 1	Authoritative Domain: avaya.lab.com	
Name: SP Region	Stub Network Region: n	
MEDIA PARAMETERS		
Codec Set: 2	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: 3349		
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		
RSVP Enabled? n		
H.323 IP ENDPOINTS		
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The following example shows the settings used for the compliance test. It indicates that codec set **2** will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

change ip-network-region 2										Page 4 of 20		
Source Region: 2      Inter Network Region Connection Management										I		M
dst rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Intervening Prio Shr Regions	Dyn CAC	A	G		G	A	t
1	2	y	NoLimit							n		t
2	2										all	
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												

## 5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used and was configured using the parameters highlighted below, shown on the screen on the next page:

- 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 the Session Manager.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and Session Manager. For the compliance test, *tls* was used.
- 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 is a Session Manager.

**Note:** Once the **Peer-Server** field is updated to *SM*, the system changes the default values of the following fields, setting them to display-only:

- **Prepend ‘+’ to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to *y*.
- **Remove ‘+’ from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to *n*.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *SM*. 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 instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to *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 the domain of the enterprise.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to *y*. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to *n*, then the Avaya Media Gateway or Media Server will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway and Media Server, these resources may be depleted during high call volume preventing additional calls from completing.
- Default values may be used for all other fields

change signaling-group 2		Page 1 of 2	
SIGNALING GROUP			
Group Number: 2	Group Type: sip		
IMS Enabled? <u>n</u>	Transport Method: <u>tls</u>		
Q-SIP? <u>n</u>			
IP Video? <u>n</u>	Enforce SIPS URI for SRTP? <u>y</u>		
Peer Detection Enabled? <u>y</u>	Peer Server: SM		
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? <u>y</u>			
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? <u>n</u>			
Alert Incoming SIP Crisis Calls? <u>n</u>			
Near-end Node Name: <u>procr</u>	Far-end Node Name: <u>SM</u>		
Near-end Listen Port: <u>5071</u>	Far-end Listen Port: <u>5071</u>		
	Far-end Network Region: <u>2</u>		
Far-end Domain: <u>avaya.lab.com</u>			
Incoming Dialog Loopbacks: <u>eliminate</u>	Bypass If IP Threshold Exceeded? <u>n</u>		
DTMF over IP: <u>rtp-payload</u>	RFC 3389 Comfort Noise? <u>n</u>		
Session Establishment Timer(min): <u>3</u>	Direct IP-IP Audio Connections? <u>y</u>		
Enable Layer 3 Test? <u>n</u>	IP Audio Hairpinning? <u>n</u>		
H.323 Station Outgoing Direct Media? <u>n</u>	Initial IP-IP Direct Media? <u>n</u>		
	Alternate Route Timer(sec): <u>6</u>		

## 5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 2 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.
- Set the **Service Type** field to *public-ntwrk*.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**.
- 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.

```
change trunk-group 2                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 2      Group Type: sip      CDR Reports: y
Group Name: Service Provider      COR: 1      TN: 1      TAC: 602
Direction: two-way      Outgoing Display? n
Dial Access? n      Night Service: _____
Queue Length: 0
Service Type: public-ntwrk      Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 2
                                     Number of Members: 10
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. The default value of **600** seconds was used.

change trunk-group 2		Page 2 of 21
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: <u>auto</u>		
Redirect On OPTIM Failure: <u>5000</u>		
SCCAN? <u>n</u>	Digital Loss Group: <u>18</u>	
<b>Preferred Minimum Session Refresh Interval(sec): <u>600</u></b>		
Disconnect Supervision - In? <u>y</u> Out? <u>y</u>		
XOIP Treatment: <u>auto</u> Delay Call Setup When Accessed Via IGAR? <u>n</u>		
Caller ID for Service Link Call to H.323 1xC: <u>station-extension</u>		



On Page 3:

- Set the **Numbering Format** field to *private*. This field specifies the format of the calling party number (CPN) sent to the far-end. When *public* format is used, Communication Manager automatically inserts a “+” sign, preceding the numbers in the “From”, “Contact” and “P-Asserted Identity” (PAI) headers. To keep uniformity with the format used by CenturyLink, the **Numbering Format** was set to *private* and the **Numbering Format** in the route pattern was set to *unk-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 has enabled CPN block.

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

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

  Show ANSWERED BY on Display? y
```

On Page 4:

- Set the **Network Call Redirection** field to **y**. With this setting, Communication Manager will use the SIP REFER method, which is supported by CenturyLink, for the redirection of PSTN calls that are transferred back to the SIP trunk (refer to **Section 2.2**).
- Set the **Send Diversion Header** field to **y** and **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **101**, the value preferred by CenturyLink.
- Verify that **Identity for Calling Party Display** is set to **P-Asserted-Identity**.
- Default values were used for all other fields.

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

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, three DID numbers were assigned by the service provider for testing. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions.

[illegible]

## 5.9. Inbound Routing

In general, the “incoming call handling treatment” form 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 using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by CenturyLink is left 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. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

change inc-call-handling-trmt trunk-group 2					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/ Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	10	3031235744	10	3042	
public-ntwrk	10	3031235747	10	3044	
public-ntwrk	10	3031235748	10	3050	
public-ntwrk					
public-ntwrk					
public-ntwrk					
public-ntwrk					
public-ntwrk					
public-ntwrk					
public-ntwrk					
public-ntwrk					
public-ntwrk					
public-ntwrk					
public-ntwrk					
public-ntwrk					
public-ntwrk					
public-ntwrk					
public-ntwrk					

## 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 common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with **9** of length **1**, as a feature access code (*fac*).

change dialplan analysis			DIAL PLAN ANALYSIS TABLE						Page 1 of 12
			Location: all			Percent Full: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	13	udp							
1	4	dac							
2	4	ext							
3	4	ext							
4	4	udp							
5	4	ext							
6	3	dac							
7	4	ext							
8	1	fac							
9	1	fac							
*	3	dac							
#	2	dac							

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 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:	_____	
Abbreviated Dialing List2 Access Code:	_____	
Abbreviated Dialing List3 Access Code:	_____	
Abbreviated Dial - Prgm Group List Access Code:	_____	
Announcement Access Code:	#7 _____	
Answer Back Access Code:	_____	
Attendant Access Code:	_____	
Auto Alternate Routing (AAR) Access Code:	8 _____	
Auto Route Selection (ARS) - Access Code 1:	9 _____	Access Code 2: _____
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:	_____	Deactivation: _____
Contact Closure Open Code:	_____	Close Code: _____

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 2, which contains the SIP trunk group to the service provider.

list ars analysis							Page 8
ARS DIGIT ANALYSIS REPORT							
Location: all							
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Number	ANI Req	
178	11	11	deny	fnpa		n	
1786	11	11	2	fnpa		n	
179	11	11	deny	fnpa		n	
180	11	11	deny	fnpa		n	
1800	11	11	2	fnpa		n	
1800555	11	11	deny	fnpa		n	
1809	11	11	2	hnpa		n	
181	11	11	deny	fnpa		n	
182	11	11	deny	fnpa		n	
183	11	11	deny	fnpa		n	
184	11	11	deny	fnpa		n	
185	11	11	deny	fnpa		n	
press CANCEL to quit -- press NEXT PAGE to continue							

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 for route pattern 2 in the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider.
- **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.
- **Pfx Mrk:** Set to **1** to ensure 1 + 10 digits are sent to the service provider for long distance numbers in the North American Numbering Plan (NANP).
- **Numbering Format:** Set to *unk-unk*. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

change route-pattern 2															Page 1 of 3	
Pattern Number: 2															Pattern Name: <u>Serv. Provider</u>	
SCCAN? <u>n</u> Secure SIP? <u>n</u> Used for SIP stations? <u>n</u>																
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Dgts					DCS/ QSIG Intw	IXC			
1:	<u>2</u>	<u>0</u>		<u>1</u>								<u>n</u>	<u>user</u>			
2:												<u>n</u>	<u>user</u>			
3:												<u>n</u>	<u>user</u>			
4:												<u>n</u>	<u>user</u>			
5:												<u>n</u>	<u>user</u>			
6:												<u>n</u>	<u>user</u>			

BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	Sub	Numbering	LAR	
0	1	2	M	4	W	Request		Dgts	Format		
1:	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>n</u>	<u>n</u>		<u>rest</u>	<u>unk-unk</u>	<u>none</u>
2:	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>n</u>	<u>n</u>		<u>rest</u>		<u>none</u>
3:	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>n</u>	<u>n</u>		<u>rest</u>		<u>none</u>
4:	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>n</u>	<u>n</u>		<u>rest</u>		<u>none</u>
5:	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>n</u>	<u>n</u>		<u>rest</u>		<u>none</u>
6:	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>n</u>	<u>n</u>		<u>rest</u>		<u>none</u>

**Note** - Enter the **save translation** command (not shown) to save all the changes made to the Communication Manager configuration in the previous sections.



## 6. Configure Avaya Aura® Session Manager

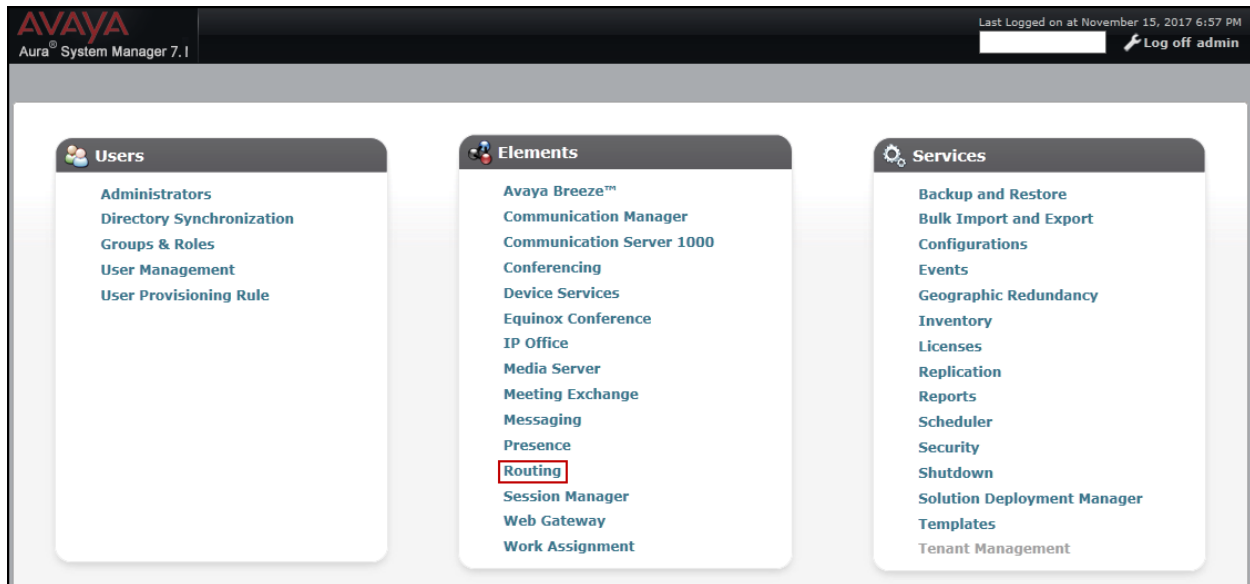
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Locations that can be occupied by SIP Entities.
- Adaptation module to perform header manipulations.
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.

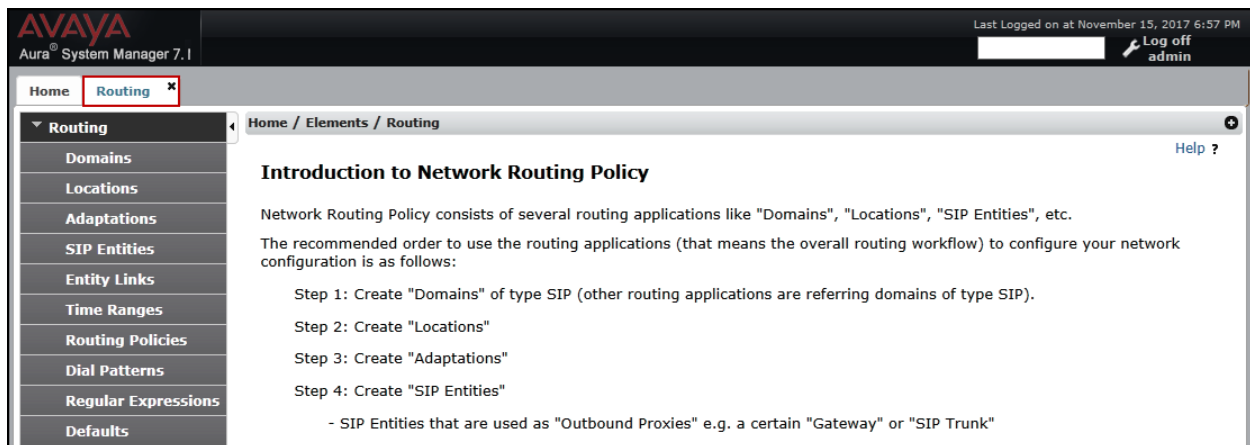
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

## 6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed; click on **Routing**.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items discussed in this section will be located under the **Routing** link shown below.



## 6.2. SIP Domain

Create an entry for each SIP domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this was the enterprise domain, **avaya.lab.com**. Navigate to **Routing → Domains** 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:

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

The screen below shows the entry for the enterprise domain.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top header includes the Avaya logo and 'Aura® System Manager 7.1'. The right header shows 'Last Logged on at November 15, 2017 6:57 PM' and a 'Log off admin' button. The left navigation pane has 'Home' and 'Routing' tabs, with 'Routing' selected. Under 'Routing', 'Domains' is highlighted. The main content area is titled 'Domain Management' and shows a table with one entry. The table has columns for 'Name', 'Type', and 'Notes'. The entry is 'avaya.lab.com', 'sip', and 'HG V-Domain' respectively. The 'Name' and 'Notes' fields are highlighted with red boxes. The table also has a 'Filter: Enable' button and a 'Select : All, None' option.

Name	Type	Notes
avaya.lab.com	sip	HG V-Domain

## 6.3. Locations

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

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

The following screen shows the location details for the location named **Session Manager**. Later, this location will be assigned to the SIP Entity corresponding to Session Manager. Other location parameters (not shown) retained the default values.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text "Aura® System Manager 7.1", and a "Last Logged on at November 15, 2017 6:57 PM" timestamp. A "Log off admin" button is visible. The left sidebar contains a menu with "Routing" selected and highlighted. The main content area shows the "Location Details" page for "Session Manager". The breadcrumb trail is "Home / Elements / Routing / Locations". The "General" section includes a red-bordered input field for "\* Name:" containing "Session Manager" and a "Notes:" field containing "VMware Session Manager". The "Dial Plan Transparency in Survivable Mode" section has an "Enabled:" checkbox (unchecked), a "Listed Directory Number:" field, and an "Associated CM SIP Entity:" field. "Commit" and "Cancel" buttons are at the top right.

The following screen shows the location details for the location named **Communication Manager**. Later, this location will be assigned to the SIP Entity corresponding to Communication Manager. Other location parameters (not shown) retained the default values.

This screenshot shows the same Avaya Aura System Manager 7.1 interface as the previous one, but for the "Communication Manager" location. The "Routing" menu item is still selected. The "Location Details" page for "Communication Manager" is displayed. The breadcrumb trail remains "Home / Elements / Routing / Locations". In the "General" section, the red-bordered "\* Name:" field now contains "Communication Manager", and the "Notes:" field contains "VMware Communication Manager". The "Dial Plan Transparency in Survivable Mode" section and other fields are identical to the previous screenshot. "Commit" and "Cancel" buttons are present at the top right.

The following screen shows the location details for the location named *Avaya SBCE*. Later, this location will be assigned to the SIP Entity corresponding to the Avaya SBCE. Other location parameters (not shown) retained the default values.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top header shows the Avaya logo and 'Aura System Manager 7.1'. The user is logged in as 'admin' on November 15, 2017, at 6:57 PM. The breadcrumb trail is 'Home / Elements / Routing / Locations'. The left sidebar menu has 'Locations' selected under the 'Routing' category. The main content area is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' section, the '\* Name' field is set to 'Avaya SBCE' and the 'Notes' field is 'VMware Avaya SBCE'. The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox that is unchecked, and fields for 'Listed Directory Number' and 'Associated CM SIP Entity'.

AVAYA  
Aura System Manager 7.1

Last Logged on at November 15, 2017 6:57 PM  
Log off admin

Home Routing

Home / Elements / Routing / Locations

Location Details

Commit Cancel

Help ?

General

\* Name: Avaya SBCE

Notes: VMware Avaya SBCE

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

## 6.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 7.0 incorporates the ability to use Adaptation modules to remove specific headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements.

For the compliance test, an Adaptation named ***CM\_Outbound\_Header\_Removal*** was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector and P-Location. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

Navigate to **Routing → Adaptations** 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:

- **Adaptation Name:** Enter an appropriate name.
- **Module Name:** Select the *DigitConversionAdapter* option.
- **Module Parameter Type:** Select *Name-Value Parameter*.

Click **Add** to add the name and value parameters, as follows:

- **Name:** Enter *eRHdrs*. This parameter will remove the specified headers from messages in the egress direction.
- **Value:** Enter “*Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View*”
- Click **Commit** to save.

The screen below shows the adaptation created for the compliance test. This adaptation will later be applied to the SIP Entity corresponding to the Avaya SBCE. All other fields were left at their default values.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', and a user status area showing 'Last Logged on at November 15, 2017 6:57 PM' and a 'Log off admin' button. The left sidebar contains a menu with 'Routing' selected, and sub-items like 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Adaptation Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the 'Adaptation Name' is 'CM\_Outbound\_Header\_Removal', the 'Module Name' is 'DigitConversionAdapter', and the 'Module Parameter Type' is 'Name-Value Parameter'. Below this is a table with columns 'Name' and 'Value'. The table contains one entry with 'Name' 'eRHdrs' and 'Value' '"Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-id, P-'. The 'Add' and 'Remove' buttons are at the top of the table, and a 'Select : All, None' option is at the bottom.

Home / Elements / Routing / Adaptations

**Adaptation Details** [Commit] [Cancel] [Help ?]

**General**

\* Adaptation Name: CM\_Outbound\_Header\_Removal

\* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
eRHdrs	"Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-id, P-

Select : All, None

## 6.5. SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya SBCE. Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling (see **Figure 1**).
- **Type:** Select *Session Manager* for Session Manager, *CM* for Communication Manager and *SIP Trunk* (or *Other*) for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.
- Click **Commit** to save.

The following screen shows the addition of the *Session Manager* SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 7.1', and a user status bar showing 'Last Logged on at November 15, 2017 6:57 PM' and 'Log off admin'. The left navigation pane has a 'Routing' tab selected, with a sub-menu showing 'Domains', 'Locations', 'Adaptations', 'SIP Entities' (highlighted), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'SIP Entity Details' and has a 'General' tab. The form contains the following fields: 'Name' (Session Manager), 'FQDN or IP Address' (10.64.101.249), 'Type' (Session Manager), 'Notes' (VMware Session Manager), 'Location' (Session Manager), 'Outbound Proxy' (empty), 'Time Zone' (America/New\_York), and 'Minimum TLS Version' (Use Global Setting). The 'Commit' and 'Cancel' buttons are located at the top right of the form.



The following screen shows the addition of the *Communication Manager Trunk 2* SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the “**procr**” interface in Communication Manager, as seen in **Section 5.3**. Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', and a user session summary showing 'Last Logged on at November 15, 2017 6:57 PM' and a 'Log off admin' button. A breadcrumb trail reads 'Home / Elements / Routing / SIP Entities'. The left sidebar contains a menu with 'Routing' selected, and sub-items including Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the form contains the following fields:
 

- \* Name:** Communication Manager Trunk 2
- \* FQDN or IP Address:** 10.64.101.241
- Type:** CM (dropdown menu)
- Notes:** Used for SP Testing
- Adaptation:** (empty dropdown menu)
- Location:** Communication Manager (dropdown menu)
- Time Zone:** America/New\_York (dropdown menu)

The following screen shows the addition of the *Avaya SBCE* SIP Entity for the Avaya SBCE:

- The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**).
- On the **Adaptation** field, the adaptation module *CM\_Outbound\_Header\_Removal* previously defined in **Section 6.4** was selected.
- Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.

AVAYA  
Aura® System Manager 7.1

Last Logged on at November 15, 2017 6:57 PM  
Log off  
admin

Home Routing

Routing  
Domains  
Locations  
Adaptations  
SIP Entities  
Entity Links  
Time Ranges  
Routing Policies  
Dial Patterns  
Regular Expressions  
Defaults

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

Help ?

General

\* Name: Avaya SBCE

\* FQDN or IP Address: 10.64.101.243

Type: SIP Trunk

Notes: VMware Avaya SBCE

Adaptation: CM\_Outbound\_Header\_Removal

Location: Avaya SBCE

Time Zone: America/New\_York

## 6.6. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing** → **Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu (**Section 6.5**).
- **Protocol:** Select the transport protocol used for this link (**Section 5.6**).
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end (**Section 5.6**).
- **SIP Entity 2:** Select the name of the other system from the drop-down menu (**Section 6.5**).
- **Port:** Port number on which the other system receives SIP requests from Session Manager (**Section 5.6**).
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.
- Click **Commit** to save.

The screen below shows 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 5.6**. *TLS* transport and port *5071* were used.

AVAYA  
Aura System Manager 7.1

Last Logged on at November 15, 2017 6:57 PM  
Log off admin

Home Routing

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
<input type="checkbox"/>	*Session_Manager_CN	*Session Manager	TLS	*5071	*Communication Manager Trunk 2	*5071	<input type="checkbox"/>	trusted

Select : All, None

The Entity Link to the Avaya SBCE is shown below; *TLS* transport and port *5061* were used.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a navigation menu with the following items: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (highlighted), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and includes 'Commit' and 'Cancel' buttons. Below the title, there is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, and Connection Policy. The table contains one item with the following values: Name: \*Session\_Manager\_AS\*, SIP Entity 1: Session Manager, Protocol: TLS, Port: \*5061, SIP Entity 2: \*Avaya SBCE, Port: \*5061, DNS Override: ☐, and Connection Policy: trusted. The table also includes a 'Filter: Enable' button and a 'Select: All, None' dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
*Session_Manager_AS*	Session Manager	TLS	*5061	*Avaya SBCE	*5061	<input type="checkbox"/>	trusted

## 6.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added: an incoming policy with Communication Manager as the destination, and an outbound policy to the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed:

- In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies (**Section 6.5**) 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 screens show the Routing Policies for Communication Manager and the Avaya SBCE.

AVAYA  
Aura® System Manager 7.1

Last Logged on at November 15, 2017 6:57 PM

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

Help ?

General

\* Name: To CM Trunk 2

Disabled: ☐

\* Retries: 0

Notes: For inbound calls to CM via Trunk

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Communication Manager Trunk 2	10.64.101.241	CM	Used for SP Testing

AVAYA  
Aura® System Manager 7.1

Last Logged on at November 21, 2017 8:32 AM

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

Help ?

General

\* Name: Avaya SBCE

Disabled: ☐

\* Retries: 0

Notes: For outbound calls to SP via ASB

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.64.101.243	SIP Trunk	VMware Avaya SBCE

## 6.8. Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to the service provider and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

In the **General** section, enter the following values:

- **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, or select “**ALL**” to route incoming calls to all SIP domains.
- **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 (**Section 6.3**).
- Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria (**Section 6.7**). Click **Select** (not shown).
- Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to 10-digit numbers starting with **303**, arriving from location **Avaya SBCE**, used route policy **To CM Trunk 2** to Communication Manager. The SIP Domain was set to **avaya.lab.com**

**AVAYA**  
Aura® System Manager 7.1

Last Logged on at May 21, 2018 11:02 AM  
[Log off admin](#)

Home **Routing**

Home / Elements / Routing / Dial Patterns

### Dial Pattern Details

[Commit](#) [Cancel](#) [Help ?](#)

**General**

\* Pattern: 303

\* Min: 10

\* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.lab.com

Notes:

**Originating Locations and Routing Policies**

[Add](#) [Remove](#) Filter: Enable

1 Item

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Avaya SBCE	VMware Avaya SBCE	To CM Trunk 2	0	<input type="checkbox"/>	Communication Manager Trunk 2	For inbound calls to CM via Trunk 2

Select : All, None

**Denied Originating Locations**

[Add](#) [Remove](#) Filter: Enable

0 Items

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

Repeat this procedure as needed to define additional dial patterns for other range of numbers assigned by the service provider to the enterprise, to be routed to Communication Manager.

The example in this screen shows the 11-digit dialed numbers for outbound calls, beginning with **1**, arriving from the **Communication Manager** location, will use route policy **Avaya SBCE**, which sends the call out to the PSTN via Avaya SBCE and the service provider SIP trunk. The SIP Domain was set to **avaya.lab.com**.

**AVAYA**  
Aura® System Manager 7.1

Last Logged on at April 23, 2018 8:16 PM  
Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

### Dial Pattern Details

Commit Cancel

Help ?

**General**

\* Pattern: 1  
\* Min: 11  
\* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.lab.com

Notes:

**Originating Locations and Routing Policies**

Add Remove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Communication Manager	VMware Communication Manager	Avaya SBCE	0	<input type="checkbox"/>	Avaya SBCE	For outbound calls to SP via ASBCE

Select : All, None

**Denied Originating Locations**

Add Remove

0 Items

Filter: Enable

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

Repeat this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the service provider's network via the Avaya SBCE.



## 7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **References** section.

**Note** - The configuration tasks required to support TLS transport for signaling and SRTP for media inside of the enterprise (private network side, in between Avaya components) and outside of the enterprise (public network side, in between the Avaya enterprise and CenturyLink) are beyond the scope of these Application Notes; hence they are not discussed in this document.

### 7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.




The screenshot shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in a large, stylized red font. Below it, the text "Session Border Controller for Enterprise" is written in a bold, black font. On the right, the "Log In" section contains a "Username:" label, a text input field, and a "Continue" button. Below the login fields, there is a "WELCOME TO AVAYA SBC" message, followed by a disclaimer: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." and a consent statement: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, the copyright notice "© 2011 - 2017 Avaya Inc. All rights reserved." is visible.

Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.

[Alarms](#) [Incidents](#) [Status ▾](#) [Logs ▾](#) [Diagnostics](#) [Users](#) [Settings ▾](#) [Help ▾](#) [Log Out](#)

# Session Border Controller for Enterprise



Dashboard

Administration

Backup/Restore

System Management

- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies
- TLS Management
- Device Specific Settings

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

The following certificates are expired:

- Clearcom\_Cert.crt (Certificate)

Information

System Time	01:17:36 PM EDT	<a href="#">Refresh</a>
Version	7.2.1.0-05-14222	
Build Date	Tue Oct 31 00:06:46 UTC 2017	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	05/17/2018 13:06:07 EDT	
Failed Login Attempts	0	

Active Alarms (past 24 hours)

None found.

Installed Devices

EMS

Avaya\_SBCE

Incidents (past 24 hours)

Avaya\_SBCE : No Subscriber Flow Matched

Avaya\_SBCE : No Subscriber Flow Matched

Avaya\_SBCE : No Subscriber Flow Matched

Avaya\_SBCE : No Subscriber Flow Matched

Avaya\_SBCE : No Subscriber Flow Matched

[Add](#)

Notes

No notes found.

## 7.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named *Avaya\_SBCE* is shown. The management IP address that was configured during installation is blurred out for security reasons, the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is *Commissioned*, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the Avaya logo. The left sidebar contains a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management (highlighted with a red box), Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'System Management' and features five tabs: Devices (highlighted with a red box), Updates, SSL VPN, Licensing, and Key Bundles. Below the tabs is a table listing installed devices. The table has columns for Device Name, Management IP, Version, Status, and a set of action links. One device, 'Avaya\_SBCE', is listed with a blurred Management IP, version '7.2.1.0-05-14222', and status 'Commissioned'. The 'View' link in the action column for this device is highlighted with a red box.

Device Name	Management IP	Version	Status	Reboot	Shutdown	Restart Application	View	Edit	Uninstall
Avaya_SBCE	[Blurred]	7.2.1.0-05-14222	Commissioned						

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, containing the current device configuration and network settings.

System Information: Avaya\_SBCE
X

**General Configuration**

Appliance Name	Avaya_SBCE
Box Type	SIP
Deployment Mode	Proxy

**Device Configuration**

HA Mode	No
Two Bypass Mode	No

**License Allocation**

Standard Sessions <small>Requested: 2000</small>	2000
Advanced Sessions <small>Requested: 2000</small>	2000
Scopia Video Sessions <small>Requested: 500</small>	500
CES Sessions <small>Requested: 0</small>	0
Transcoding Sessions <small>Requested: 0</small>	0
Encryption	<input checked="" type="checkbox"/>

**Network Configuration**

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.101.243	10.64.101.243	255.255.255.0	10.64.101.1	A1
				A1
				A1
				B1
				B1
10.10.80.51	10.10.80.51	255.255.255.128	10.10.80.1	B1

**DNS Configuration**

Primary DNS	8.8.8.8
Secondary DNS	7.7.7.7
DNS Location	DMZ
DNS Client IP	10.10.80.51

**Management IP(s)**

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

The highlighted IP addresses in the **System Information** screen are the ones used for the SIP trunk to CenturyLink, and are the ones relevant to these Application Notes. Other IP addresses assigned to the Avaya SBCE **A1** and **B1** interfaces are used to support remote workers and other SIP trunks, and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

In the reference configuration, the private interface of the Avaya SBCE (10.64.101.243) was used to connect to the enterprise network, while its public interface (10.10.80.51) was used to connect to the public network. See **Figure 1**.

On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.

## 7.3. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, *Avaya\_SBCE* in the sample configuration. On the **Networks** tab, verify or enter the network information as needed.

Note that in the configuration used during the compliance test, the IP addresses assigned to the private (*10.64.101.243*) and public (*10.10.80.51*) sides of the Avaya SBCE are the ones relevant to these Application Notes.

Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

### Session Border Controller for Enterprise

AVAYA

Dashboard  
Administration  
Backup/Restore  
System Management  
▸ Global Parameters  
▸ Global Profiles  
▸ PPM Services  
▸ Domain Policies  
▸ TLS Management  
▸ Device Specific Settings  
    **Network Management**  
    Media Interface

Network Management: Avaya\_SBCE

Devices  
Avaya\_SBCE

Interfaces Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address		
Network_A1	10.64.101.1	255.255.255.0	A1	10.64.101.243,	Edit	Delete
Network_B1	10.10.80.1	255.255.255.128	B1	10.10.80.51	Edit	Delete

On the **Interfaces** tab, verify the **Administrative Status** is **Enabled** for the **A1** and **B1** interfaces. Click the buttons under the **Status** column if necessary to enable the interfaces.

## 7.4. Media Interfaces

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which it will accept media from the Call Server or the trunk server.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown).

- On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- The **Port Range** was left at the default values of **35000-40000**.
- Click **Finish**.

A Media Interface facing the public side was similarly created with the name ***Public\_med***, as shown below.

- Under **IP Address**, the network and IP address to be associated with this interface was selected.
- The **Port Range** was left at the default values.
- Click **Finish**.

The screenshot shows a window titled "Add Media Interface" with a close button (X) in the top right corner. The window contains the following fields:

- Name:** A text box containing "Public\_med".
- IP Address:** A dropdown menu showing "Network\_B1 (B1, VLAN 0)" with a downward arrow, and a text box below it containing "10.10.80.51" with a downward arrow.
- Port Range:** Two text boxes containing "35000" and "40000" separated by a hyphen.
- Finish:** A button at the bottom center of the window.

A red rectangular box highlights the "Name", "IP Address", and "Port Range" fields.

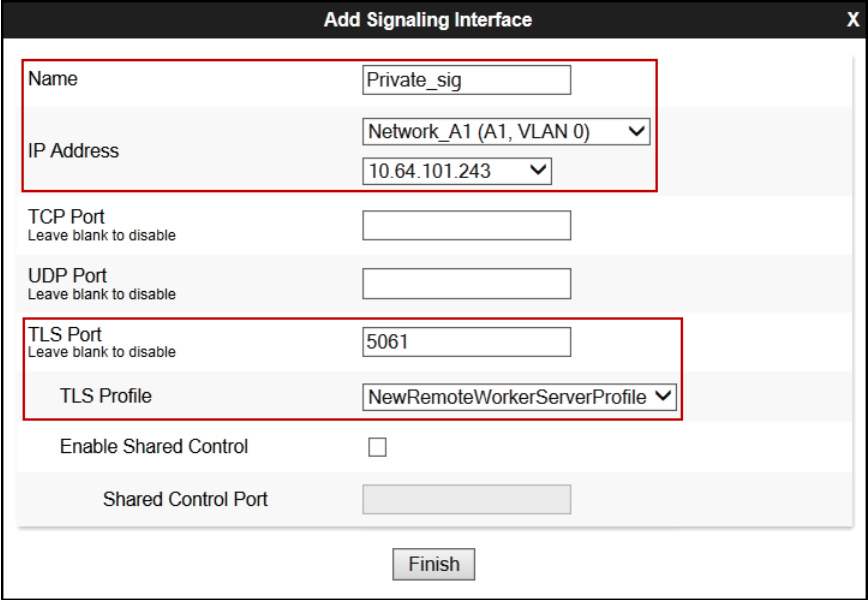


## 7.5. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in the connected networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown).

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.6**.
- Select a **TLS Profile**.
- Click **Finish**.



The screenshot shows a web-based configuration window titled "Add Signaling Interface" with a close button (X) in the top right corner. The form contains several fields and a "Finish" button at the bottom. Two red rectangular boxes highlight specific sections of the form. The first box encloses the "Name" field (containing "Private\_sig"), the "IP Address" section (which includes a network dropdown menu showing "Network\_A1 (A1, VLAN 0)" and an IP address dropdown menu showing "10.64.101.243"), and the "TLS Port" field (containing "5061"). The second box encloses the "TLS Profile" dropdown menu (showing "NewRemoteWorkerServerProfile"). Other fields include "TCP Port" and "UDP Port" (both with the instruction "Leave blank to disable"), and an "Enable Shared Control" checkbox which is currently unchecked. A "Shared Control Port" field is also present but appears to be disabled or greyed out.

Add Signaling Interface	
Name	Private_sig
IP Address	Network_A1 (A1, VLAN 0)
	10.64.101.243
TCP Port	
Leave blank to disable	
UDP Port	
Leave blank to disable	
TLS Port	5061
Leave blank to disable	
TLS Profile	NewRemoteWorkerServerProfile
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	
Finish	

A second Signaling Interface with the name **Public\_sig** was similarly created in the service provider's direction.

- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from CenturyLink.
- Select a **TLS Profile**.
- Click **Finish**.

The screenshot shows the 'Add Signaling Interface' dialog box. The 'Name' field is 'Public\_sig'. The 'IP Address' section has a dropdown for 'Network\_B1 (B1, VLAN 0)' and another dropdown for '10.10.80.51'. The 'TCP Port' and 'UDP Port' fields are empty. The 'TLS Port' field contains '5061'. The 'TLS Profile' dropdown is set to 'CenturyLink\_Server'. The 'Enable Shared Control' checkbox is unchecked. The 'Shared Control Port' field is empty. The 'Finish' button is at the bottom.

## 7.6. 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).

### 7.6.1. Server Interworking Profile – Enterprise

Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Global Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select *avaya-ru* from the list of pre-defined profiles. Click **Clone**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. The left navigation pane lists various configuration areas, with "Global Profiles" expanded to show "Server Interworking". The main content area is titled "Interworking Profiles: avaya-ru" and features an "Add" button and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new profile instead." Below this, there are tabs for General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced. The "General" tab is active, showing a table of configuration parameters.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No

- Enter a descriptive name for the cloned profile.
- Click **Finish**.

The screenshot shows a "Clone Profile" dialog box. It has a title bar with "Clone Profile" and a close button (X). The dialog contains two input fields: "Profile Name" with the value "avaya-ru" and "Clone Name" with the value "Avaya-SM". A red rectangle highlights the "Clone Name" field. At the bottom of the dialog is a "Finish" button.

Click **Edit** on the newly cloned *Avaya-SM* interworking profile:

- On the **General** tab, check **T.38 Support**.
- Leave remaining fields with default values.
- Click **Finish**.

Editing Profile: SP-General

General

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

180 Handling ☒ None ☐ SDP ☐ No SDP

181 Handling ☒ None ☐ SDP ☐ No SDP

182 Handling ☒ None ☐ SDP ☐ No SDP

183 Handling ☒ None ☐ SDP ☐ No SDP

Refer Handling ☐

URI Group

Send Hold ☐

Delayed Offer ☐

3xx Handling ☐

Diversion Header Support ☐

Delayed SDP Handling ☐

Re-Invite Handling ☐

Prack Handling ☐

Allow 18X SDP ☐

**T.38 Support ☒**

URI Scheme ☒ SIP ☐ TEL ☐ ANY

Via Header Format ☒ RFC3261  
☐ RFC2543

Finish

The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs contain no entries.

The **Advanced** tab settings are shown on the screen below:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Global Profiles' and 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: Avaya-SM' and features a list of profiles on the left, including 'Avaya-SM' which is selected. The right side of the interface shows the configuration for the selected profile, with tabs for General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced. The 'Advanced' tab is active, displaying settings for Record Routes, Include End Point IP for Context Lookup, Extensions, Diversion Manipulation, Has Remote SBC, Route Response on Via Port, Relay INVITE Replace for SIPREC, and MOBX Re-INVITE Handling. A DTMF section at the bottom shows 'DTMF Support' set to 'None'. Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible throughout the interface.

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

## Session Border Controller for Enterprise

AVAYA

Dashboard  
Administration  
Backup/Restore  
System Management  
▸ Global Parameters  
▾ Global Profiles  
    Domain DoS  
    **Server Interworking**  
    Media Forking  
    Routing  
    Server Configuration  
    Topology Hiding  
    Signaling Manipulation  
    URI Groups  
    SNMP Traps  
    Time of Day Rules  
    FGDN Groups  
    Reverse Proxy Policy  
    RADIUS  
▸ PPM Services

### Interworking Profiles: Avaya-SM

Add Rename Clone Delete

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation **Advanced**

Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No

DTMF

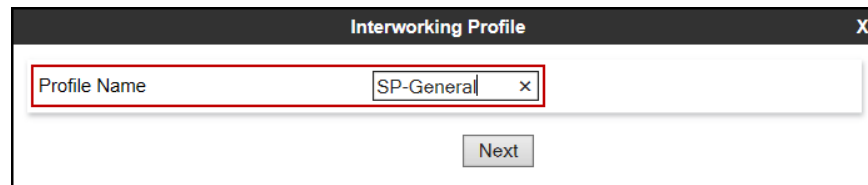
DTMF Support	None
--------------	------

Edit

## 7.6.2. Server Interworking Profile – Service Provider

A second interworking profile in the direction of the SIP trunk was created, by adding a new profile in this case. Select **Global Profiles → Server Interworking** on the left navigation pane and click **Add** (not shown).

- Enter a descriptive name for the new profile.
- Click **Next**.

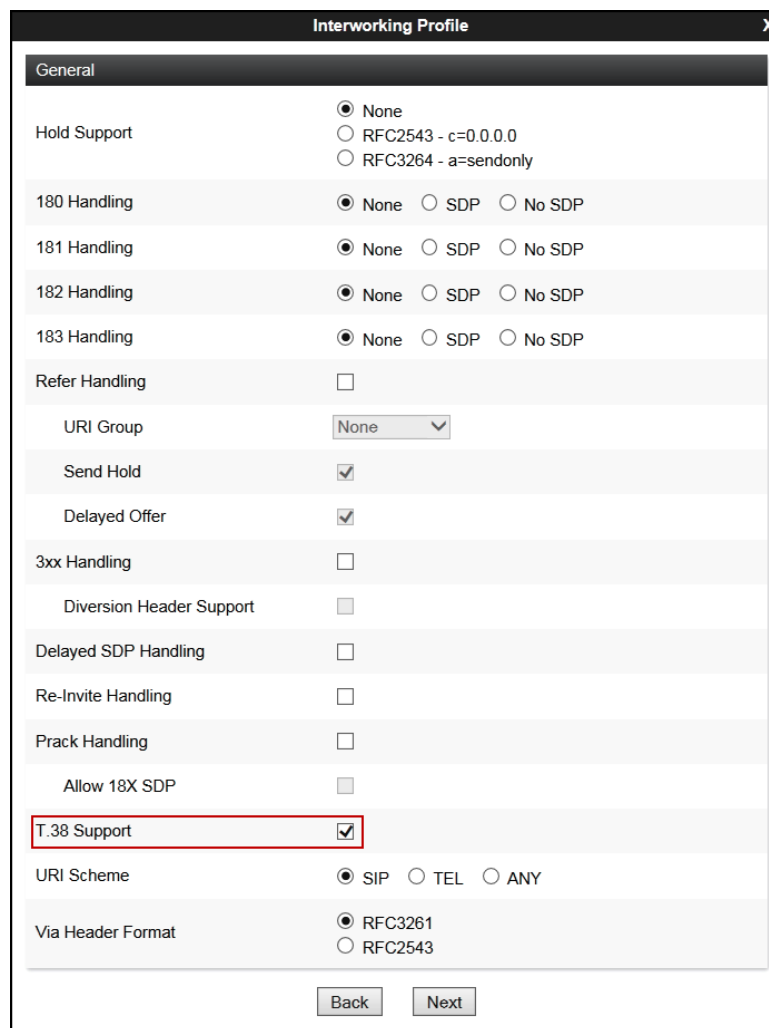


Interworking Profile

Profile Name  x

Next

On the **General** tab, check **T.38 Support**, click **Next** until the last tab is reached (not shown).



Interworking Profile

General

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

180 Handling ☒ None ☐ SDP ☐ No SDP

181 Handling ☒ None ☐ SDP ☐ No SDP

182 Handling ☒ None ☐ SDP ☐ No SDP

183 Handling ☒ None ☐ SDP ☐ No SDP

Refer Handling ☐

URI Group  v

Send Hold ☒

Delayed Offer ☒

3xx Handling ☐

Diversion Header Support ☐

Delayed SDP Handling ☐

Re-Invite Handling ☐

Prack Handling ☐

Allow 18X SDP ☐

**T.38 Support ☒**

URI Scheme ☒ SIP ☐ TEL ☐ ANY

Via Header Format ☒ RFC3261 ☐ RFC2543

Back Next

On the last tab select **Lync** under the **Extensions** pull down menu, then click **Finish**.

Interworking Profile

X

Record Routes

☐ None

☐ Single Side

☒ Both Sides

☐ Dialog-Initiate Only (Single Side)

☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup

☐

Extensions

Lync

Diversion Manipulation

☐

Diversion Condition

None

Diversion Header URI

Has Remote SBC

☒

Route Response on Via Port

☐

Relay INVITE Replace for SIPREC

☐

MOBX Re-INVITE Handling

☐

DTMF

DTMF Support

☒ None

☐ SIP Notify

☐ RFC 2833 Relay & SIP Notify

☐ SIP Info

☐ RFC 2833 Relay & SIP Info

☐ Inband

Back

Finish

## 7.7. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform granular header manipulations on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult [8] in the **References** section for more information on this topic.

Sigma scripts were created during the compliance test to correct the following interoperability issues (refer to **Section 2.2**):

- For EC500 (Extension to Cellular) and for calls that are forwarded to the PSTN the URI in PAI Header should be set to the Pilot Number.
- One-way audio issue with outbound calls from Avaya one-X® Communicator softphone (in SIP mode) to the PSTN.

The script will later be applied to the Server Configuration profile corresponding to the service provider in **Section 7.8.2**.

On the left navigation pane, select **Global Profiles → Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

- For **Title** enter a name, the name **CTL** was chosen in this example.
- Copy the complete script from **Appendix A**.
- Click **Save**.



# Signaling Manipulation Editor



Title CTL

Save

```
1 //This script is to be applied to the Service Provider Server Configuration
2
3 //For Call Forward and Mobile features where CenturyLink requires PAI to be the pilot number.
4 within session "All"
5 {
6     act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
7     {
8
9         if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("3031235745")) then
10         {
11             %var="this does nothing, match for DID number passed";
12         }
13         else
14         {
15             %HEADERS["P-Asserted-Identity"][1].URI.USER = "3031235745";
16         }
17     }
18 }
19
20 //Fixes one-way audio issue on outbound calls from Avaya one-X Communicator (SIP mode) to the
21 //PSTN. Removes codec G.729 (18) from final ACK on outbound calls originated from Avaya one-X
22 //Communicator to PSTN.
23 within session "INVITE"
24 {
25     act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and %METHOD="ACK"
26     {
27         |
28         %BODY[1].regex_replace("0 18 120","0 120");
29     }
```

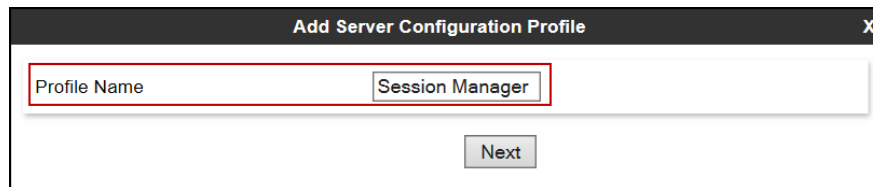
## 7.8. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and CenturyLink SIP Proxy (Trunk Server).

### 7.8.1. Server Configuration Profile – Enterprise

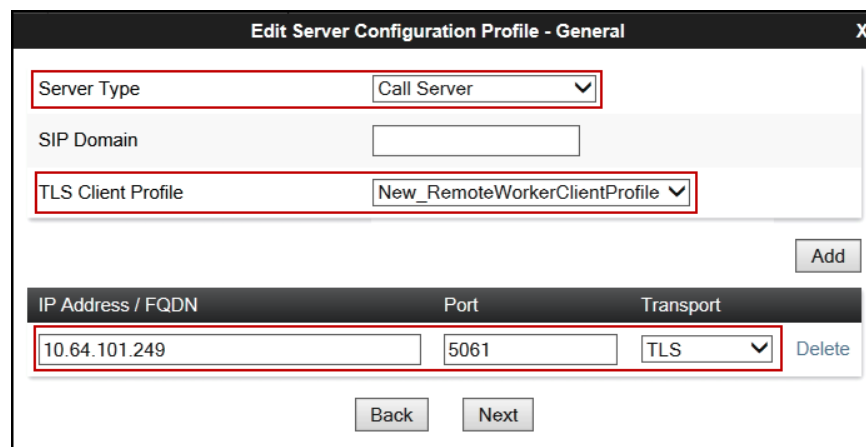
From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server.

- Enter an appropriate **Profile Name** similar to the screen below.
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "Session Manager". Below this field is a "Next" button.

- On the **Edit Server Configuration Profile – General** tab select **Call Server** from the drop-down menu under the **Server Type**.
- Select a **TLS Profile**.
- On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 6.5**).
- Enter **5061** under **Port** and select **TLS** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously created in **Section 6.6**.
- Click **Next**.



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

- Server Type**: A dropdown menu set to "Call Server".
- SIP Domain**: An empty text input field.
- TLS Client Profile**: A dropdown menu set to "New\_RemoteWorkerClientProfile".
- Add**: A button located to the right of the TLS Client Profile dropdown.
- IP Address / FQDN**: A text input field containing "10.64.101.249".
- Port**: A text input field containing "5061".
- Transport**: A dropdown menu set to "TLS".
- Delete**: A button located to the right of the Transport dropdown.
- Back** and **Next**: Buttons located at the bottom of the dialog.

- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).
- On the **Add Server Configuration Profile – Advanced** tab select *Avaya-SM* from the **Interworking Profile** drop-down menu (Section 7.6.1).
- Click **Finish**.

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

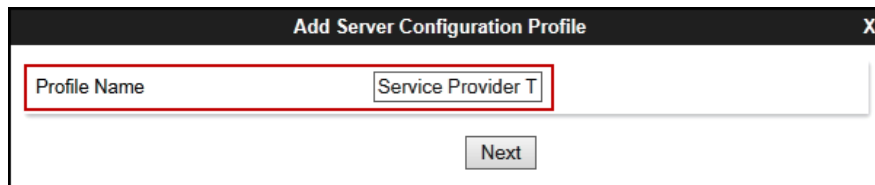
- Enable DoS Protection: ☐
- Enable Grooming: ☐
- Interworking Profile: A dropdown menu with "Avaya-SM" selected. This row is highlighted with a red rectangular border.
- Signaling Manipulation Script: A dropdown menu with "None" selected.
- Securable: ☐
- Enable FGDN: ☐
- TCP Failover Port: A text input field containing "5060".
- TLS Failover Port: A text input field containing "5061".
- Tolerant: ☐
- URI Group: A dropdown menu with "None" selected.

At the bottom of the window, there are two buttons: "Back" and "Finish".

### 7.8.2. Server Configuration Profile – Service Provider

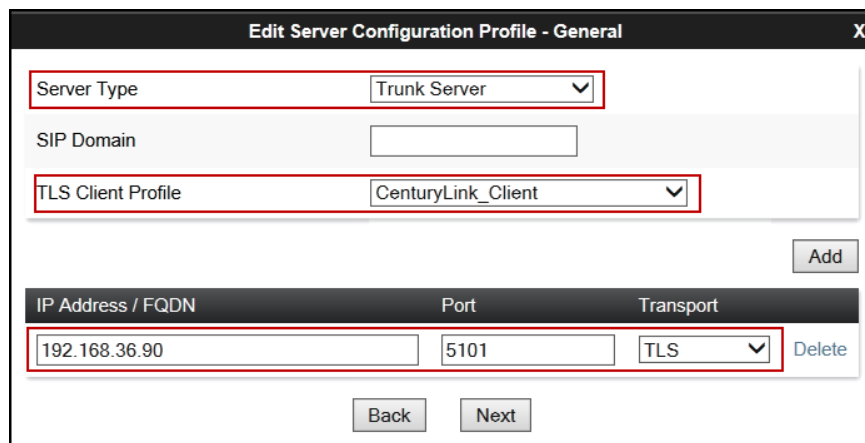
Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

- Enter an appropriate **Profile Name** similar to the screen below (*Service Provider TLS* was used).
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. The main area contains a text input field labeled "Profile Name" with the text "Service Provider T" entered. Below the input field is a "Next" button.

- On the **Edit Server Configuration Profile - General** Tab select *Trunk Server* from the drop-down menu for the **Server Type**.
- On the **IP Addresses / FQDN** field, *192.168.36.90* (the IP address of the service provider SIP proxy server. This information was provided by CenturyLink).
- Enter *5101* under **Port**, and select **TLS** for **Transport** (The port number was provided by CenturyLink).
- Select a **TLS Client Profile**.
- Click **Next**.



The screenshot shows a dialog box titled "Edit Server Configuration Profile - General". It has a close button (X) in the top right corner. The main area contains several fields: "Server Type" (a dropdown menu set to "Trunk Server"), "SIP Domain" (an empty text field), "TLS Client Profile" (a dropdown menu set to "CenturyLink\_Client"), and an "Add" button. Below these fields is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The table contains one row with the values "192.168.36.90", "5101", and "TLS" (selected from a dropdown). There is a "Delete" button next to the row. At the bottom of the dialog are "Back" and "Next" buttons.

On the **Add Server Configuration Profile - Authentication** window:

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by CenturyLink for SIP trunk registration.
- Leave the **Realm** blank.
- Enter **Password** credential provided by CenturyLink for SIP trunk registration.

Click **Next**.

The screenshot shows a window titled "Add Server Configuration Profile - Authentication". Inside the window, there is a form with the following elements:

- A checkbox labeled "Enable Authentication" which is checked.
- A text input field labeled "User Name" containing the text "User123".
- A text input field labeled "Realm" with the instruction "(Leave blank to detect from server challenge)".
- A text input field labeled "Password".
- A text input field labeled "Confirm Password".

A red rectangular box highlights the "Enable Authentication" checkbox and the "User Name" field. At the bottom of the window, there are two buttons: "Back" and "Next".

On the **Add Server Configuration Profile - Heartbeat** window:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop-down menu.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider, **120** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
  - **From URI**: Use the **Pilot Number (3031235745)** and CenturyLink's SIP Proxy IP address (**192.168.36.90**), as shown on the screen below. (This information was provided by CenturyLink).
  - **To URI**: Use the **Pilot Number (3031235745)** and CenturyLink's SIP Proxy IP address (**192.168.36.90**), as shown on the screen below. (This information was provided by CenturyLink).
  - Click **Next** until the **Add Server Configuration Profile - Advanced** window is reached.

The screenshot shows a window titled "Add Server Configuration Profile - Heartbeat". Inside the window, there is a form with the following fields and values:

- Enable Heartbeat**: ☒
- Method**: REGISTER (selected from a dropdown menu)
- Frequency**: 120 seconds
- From URI**: 3031235745@192.168.
- To URI**: 35745@192.168.36.90

At the bottom of the form, there are two buttons: "Back" and "Next". A red rectangle highlights the "Enable Heartbeat", "Method", "Frequency", "From URI", and "To URI" fields.

On the **Add Server Configuration Profile - Advanced** window:

- Select **SP-General** from the **Interworking Profile** drop-down menu (**Section 7.6.2**).
- Select the **CTL** from the **Signaling Manipulation Script** drop-down menu (**Sections 7.7** and **Section 12**).
- Click **Finish**.

**Add Server Configuration Profile - Advanced**

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile SP-General ▼

Signaling Manipulation Script CTL ▼

Securable ☐

Enable FGDN ☐

TCP Failover Port 5060

TLS Failover Port 5061

Tolerant ☐

URI Group None ▼

Back Finish

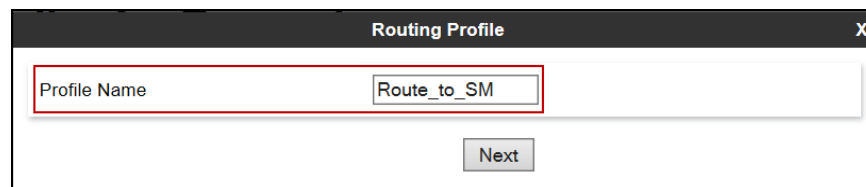
## 7.9. Routing

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 SIP trunk.

### 7.9.1. Routing Profile – Enterprise

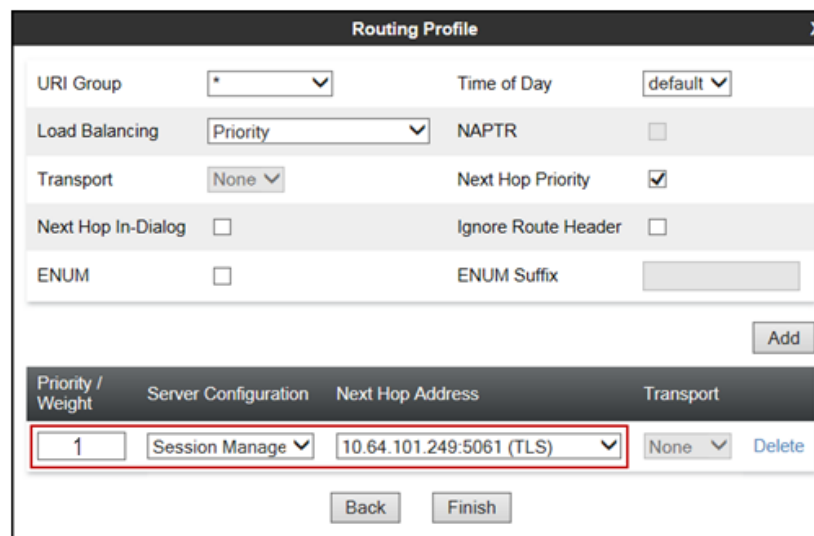
To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown).

- Enter an appropriate **Profile Name** similar to the example below.
- Click **Next**.



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Route\_to\_SM". Below the input field is a button labeled "Next".

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **Server Configuration**, select **Session Manager**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Session Manager Server Configuration Profile in **Section 7.8.1**.
- Defaults were used for all other parameters.
- Click **Finish**.



The screenshot shows the "Routing Profile" dialog box with various configuration options. The "URI Group" is set to "\*", "Time of Day" is "default", "Load Balancing" is "Priority", "NAPTR" is unchecked, "Transport" is "None", "Next Hop Priority" is checked, "Next Hop In-Dialog" is unchecked, "Ignore Route Header" is unchecked, "ENUM" is unchecked, and "ENUM Suffix" is empty. An "Add" button is visible. Below these options is a table with four columns: "Priority / Weight", "Server Configuration", "Next Hop Address", and "Transport". The first row in the table has the following values: "1", "Session Manage", "10.64.101.249:5061 (TLS)", and "None". A "Delete" button is next to the "None" value. At the bottom of the dialog are "Back" and "Finish" buttons.

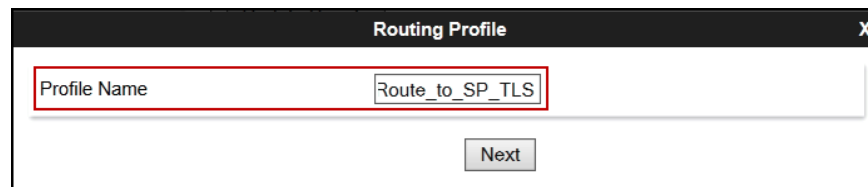
Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Session Manage	10.64.101.249:5061 (TLS)	None



### 7.9.2. Routing Profile – Service Provider

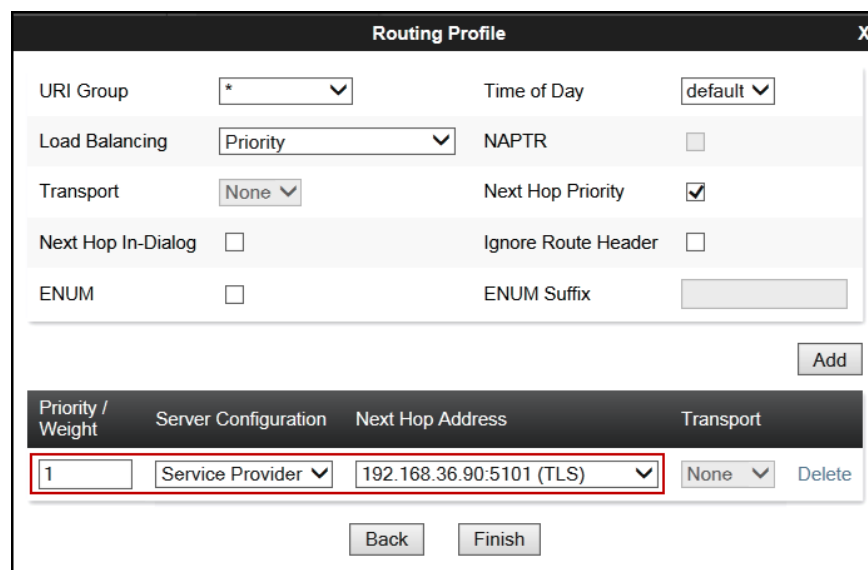
Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

- Enter an appropriate **Profile Name** similar to the example below (*Route\_to\_SP\_TLS* was used).
- Click **Next**.



The image shows a 'Routing Profile' dialog box. It has a title bar with 'Routing Profile' and a close button 'X'. Inside, there is a text input field labeled 'Profile Name' containing the text 'Route\_to\_SP\_TLS'. Below the input field is a 'Next' button.

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter *1*.
- **Server Configuration**: Select *Service Provider TLS*.
- The **Next Hop Address** is populated automatically with *192.168.36.90:5101 (TLS)* CenturyLink's SIP Proxy IP address, Port and Transport, Server Configuration Profile defined in **Section 7.8.2**.
- Click **Finish**.



The image shows a 'Routing Profile' dialog box with various configuration options and a table. The options include URI Group (set to '\*'), Time of Day (set to 'default'), Load Balancing (set to 'Priority'), NAPTR (unchecked), Transport (set to 'None'), Next Hop Priority (checked), Next Hop In-Dialog (unchecked), Ignore Route Header (unchecked), ENUM (unchecked), and ENUM Suffix (empty). There is an 'Add' button. Below these options is a table with the following columns: Priority / Weight, Server Configuration, Next Hop Address, and Transport. The table contains one entry: Priority / Weight is '1', Server Configuration is 'Service Provider', Next Hop Address is '192.168.36.90:5101 (TLS)', and Transport is 'None'. There is a 'Delete' button next to the entry. At the bottom are 'Back' and 'Finish' buttons.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Service Provider	192.168.36.90:5101 (TLS)	None

## 7.10. Topology Hiding

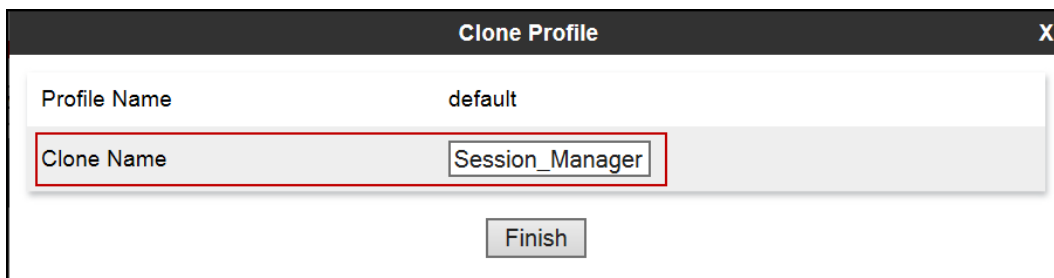
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, the default Topology Hiding Profile was cloned and modified accordingly. Only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

### 7.10.1. Topology Hiding Profile – Enterprise

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select *default* from the list of pre-defined profiles and click the **Clone** button (not shown).

- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



The screenshot shows a 'Clone Profile' dialog box. It has a title bar with 'Clone Profile' and a close button 'X'. Inside, there are two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'Session\_Manager'. The 'Clone Name' field is highlighted with a red rectangle. Below the fields is a 'Finish' button.

On the newly cloned *Session\_Manager* profile screen, click the **Edit** button (not shown).

- For the, **From**, **To** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **avaya.lab.com**, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.2**.
- Default values were used for all other fields.
- Click **Finish**.

The screenshot shows a window titled "Edit Topology Hiding Profile" with a close button (X) in the top right corner. Inside the window is a table with four columns: "Header", "Criteria", "Replace Action", and "Overwrite Value". There are eight rows in the table, each representing a different SIP header. The "Header" column contains: "SDP", "To", "From", "Refer-To", "Via", "Record-Route", "Request-Line", and "Referred-By". The "Criteria" column for all rows is "IP/Domain". The "Replace Action" column contains "Auto" for "SDP", "Refer-To", "Via", "Record-Route", and "Referred-By", and "Overwrite" for "To", "From", and "Request-Line". The "Overwrite Value" column is empty for "SDP", "Refer-To", "Via", "Record-Route", and "Referred-By", and contains "avaya.lab.com" for "To", "From", and "Request-Line". Each row has a "Delete" button to its right. The rows for "To", "From", and "Request-Line" are highlighted with a red border. At the bottom center of the window is a "Finish" button.

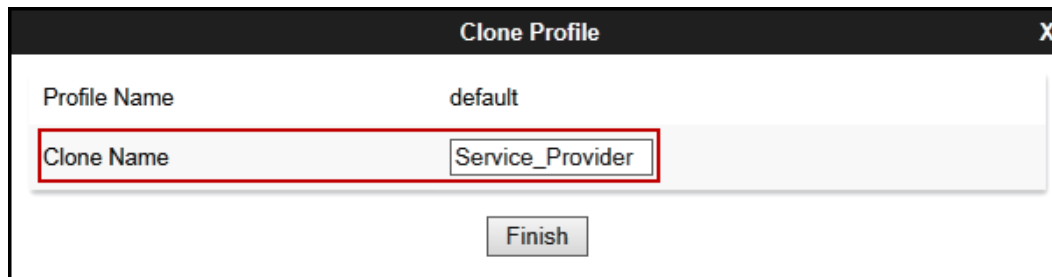
Header	Criteria	Replace Action	Overwrite Value	
SDP	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	avaya.lab.com	Delete
From	IP/Domain	Overwrite	avaya.lab.com	Delete
Refer-To	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
Record-Route	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	avaya.lab.com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

Finish

### 7.10.2. Topology Hiding Profile – Service Provider

To add the Topology Hiding Profile in the service provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select **default** from the list of pre-defined profiles and click the **Clone** button (not shown).

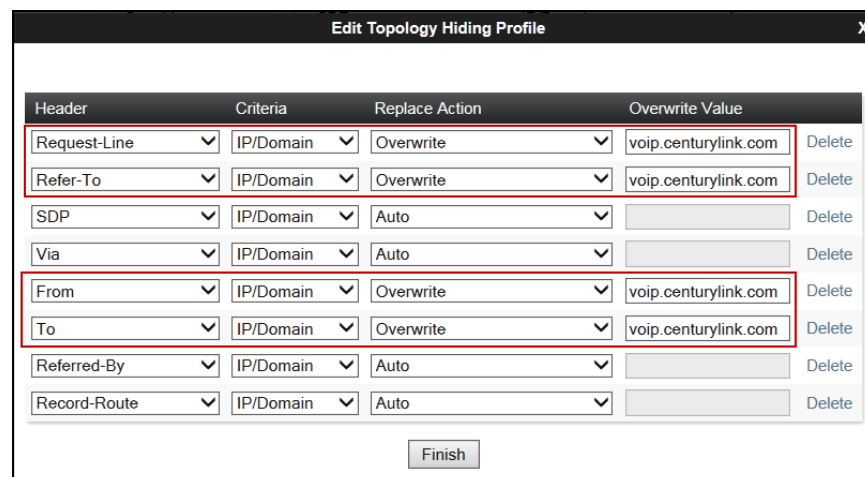
- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



The screenshot shows a 'Clone Profile' dialog box. It has a title bar with 'Clone Profile' and a close button 'X'. Inside, there's a 'Profile Name' field with the value 'default'. Below it is a 'Clone Name' field with the value 'Service\_Provider'. At the bottom is a 'Finish' button.

On the newly cloned **Service\_Provider** profile screen, click the **Edit** button (not shown).

- For the, **From**, **To**, **Request-Line** and **Refer-To** headers, select **Overwrite** in the **Replace Action** column and enter CenturyLink's SIP domain **voip.centurylink.com** in the **Overwrite Value** column of these headers, as shown below.
- Default values were used for all other fields.
- Click **Finish**.



The screenshot shows an 'Edit Topology Hiding Profile' dialog box. It contains a table with the following columns: Header, Criteria, Replace Action, Overwrite Value, and Delete. The table has 8 rows. The first four rows are highlighted with red boxes. The 'Request-Line' and 'Refer-To' rows have 'Overwrite' as the action and 'voip.centurylink.com' as the value. The 'From' and 'To' rows also have 'Overwrite' as the action and 'voip.centurylink.com' as the value. The other two rows have 'Auto' as the action and an empty 'Overwrite Value' field. A 'Finish' button is at the bottom.

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

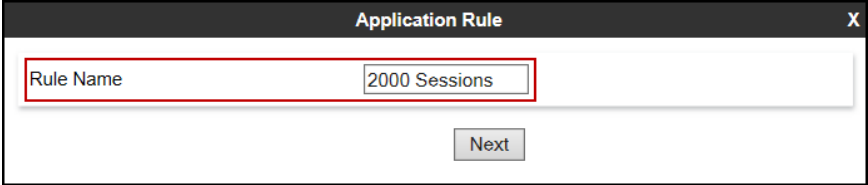
## 7.11. Domain Policies

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

### 7.11.1. Application Rules

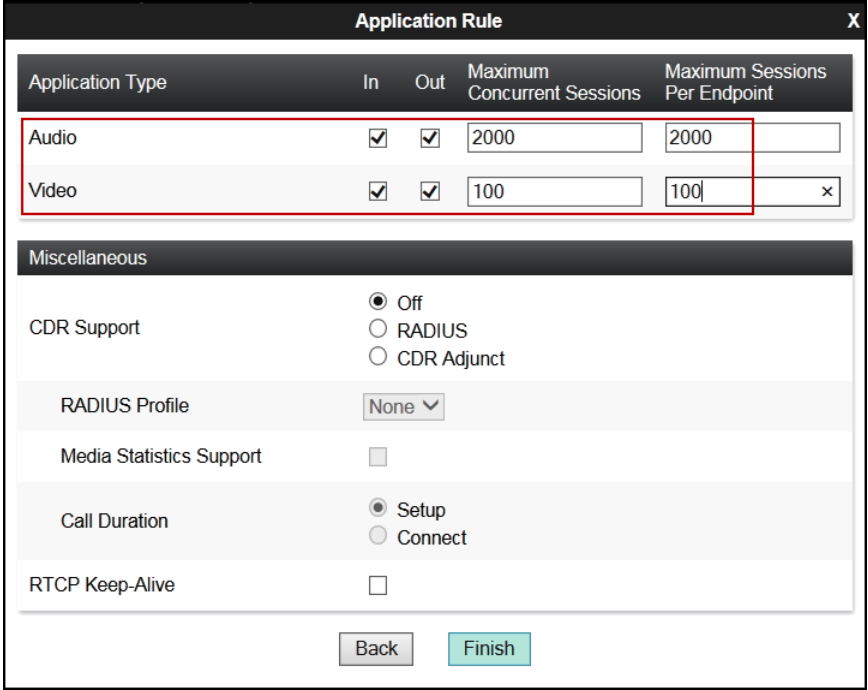
Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies** → **Application Rules**, click on the **Add** button to add a new rule.

- Under **Rule Name** enter the name of the profile, e.g., **2000 Sessions**.
- Click **Next**.



The screenshot shows a window titled "Application Rule" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Rule Name" which contains the text "2000 Sessions". This field is highlighted with a red rectangular box. Below the input field, there is a "Next" button.

- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the values of **2000** for Audio and **100** for Video were used in the sample configuration.
- Click **Finish**.



The screenshot shows a window titled "Application Rule" with a close button (X) in the top right corner. The window contains a table with the following columns: "Application Type", "In", "Out", "Maximum Concurrent Sessions", and "Maximum Sessions Per Endpoint". The table has two rows: "Audio" and "Video". The "Audio" row is highlighted with a red rectangular box. In the "Audio" row, the "In" and "Out" checkboxes are checked, "Maximum Concurrent Sessions" is set to 2000, and "Maximum Sessions Per Endpoint" is set to 2000. In the "Video" row, the "In" and "Out" checkboxes are checked, "Maximum Concurrent Sessions" is set to 100, and "Maximum Sessions Per Endpoint" is set to 100. Below the table, there is a "Miscellaneous" section with various options: "CDR Support" (radio buttons for Off, RADIUS, CDR Adjunct), "RADIUS Profile" (dropdown menu set to None), "Media Statistics Support" (checkbox), "Call Duration" (radio buttons for Setup, Connect), and "RTCP Keep-Alive" (checkbox). At the bottom of the window, there are "Back" and "Finish" buttons.

### 7.11.2. Media Rules

Media Rules allow 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 to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, two media rules (shown below) were used; one toward Session Manager and one toward the Service Provider.

To add a media rule in the Session Manager direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter **SM\_SRTP**.
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select **SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80**.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous verify that **Capability Negotiation** is checked.
- Click **Next**.

Media Encryption
X

Audio Encryption

Preferred Format #1
SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80

Preferred Format #2
RTP

Preferred Format #3
NONE

Encrypted RTCP
☐

MKI
☐

Lifetime  
Leave blank to match any value.
2^

Interworking
☒

Video Encryption

Preferred Format #1
SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80

Preferred Format #2
RTP

Preferred Format #3
NONE

Encrypted RTCP
☐

MKI
☐

Lifetime  
Leave blank to match any value.
2^

Interworking
☒

Miscellaneous

Capability Negotiation
☒

Finish

- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

To add a media rule in the Service Provider direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter *ServiceProvider\_SRTP* (not shown).
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select *SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80*.
- Under Audio Encryption, **Preferred Format #2**, select *SRTP\_AES\_CM\_128\_HMAC\_SHA1\_32*.
- Under Audio Encryption, **Preferred Format #3**, verify *NONE* is selected, this setting will enforce media to CenturyLink to be encrypted.
- Under Audio Encryption, uncheck *Encrypted RTCP*.
- Under Audio Encryption, check *Interworking*.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous verify that *Capability Negotiation* is checked.
- Click **Next**.



Media Encryption

X

Audio Encryption

Preferred Format #1

SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80

Preferred Format #2

SRTP\_AES\_CM\_128\_HMAC\_SHA1\_32

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

Leave blank to match any value.

2^

Interworking

☒

Video Encryption

Preferred Format #1

SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80

Preferred Format #2

SRTP\_AES\_CM\_128\_HMAC\_SHA1\_32

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

Leave blank to match any value.

2^

Interworking

☒

Miscellaneous

Capability Negotiation

☒

Finish

### 7.11.3. Signaling Rules

For the compliance test, the **default** signaling rule was used.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Domain Policies' and 'Signaling Rules' highlighted. The main content area is titled 'Signaling Rules: default' and features a warning message: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID'. The 'General' tab is active, showing sections for 'Inbound' and 'Outbound' rules, and a 'Content-Type Policy' section. The 'Inbound' and 'Outbound' sections each have a table with columns for 'Requests', 'Non-2XX Final Responses', 'Optional Request Headers', and 'Optional Response Headers', all set to 'Allow'. The 'Content-Type Policy' section includes a checkbox for 'Enable Content-Type Checks' (checked), an 'Action' table with 'Allow' and 'Multipart Action' (set to 'Allow'), and an 'Exception List' field. An 'Edit' button is located at the bottom right of the configuration area.

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

## Session Border Controller for Enterprise

AVAYA

Dashboard  
Administration  
Backup/Restore  
System Management  
‣ Global Parameters  
‣ Global Profiles  
‣ PPM Services  
‣ **Domain Policies**  
  Application Rules  
  Border Rules  
  Media Rules  
  Security Rules  
  **Signaling Rules**  
  End Point Policy Groups  
  Session Policies  
‣ TLS Management  
‣ Device Specific Settings

### Signaling Rules: default

Add Filter By Device... Clone

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

**Signaling Rules**  
**default**  
No-Content-Typ...  
SessMgr\_CM\_S...  
OPTIONS  
Remote Workers  
Remove\_Update  
Contact  
Remove PAI  
Remove PAI\_1  
Remove\_headers  
Remove Record...  
Test

**General** Requests Responses Request Headers Response Headers Signaling QoS UCID

**Inbound**

Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

**Outbound**

Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

**Content-Type Policy**

Enable Content-Type Checks ☒

Action	Allow	Multipart Action	Allow
--------	-------	------------------	-------

Exception List Exception List

Edit

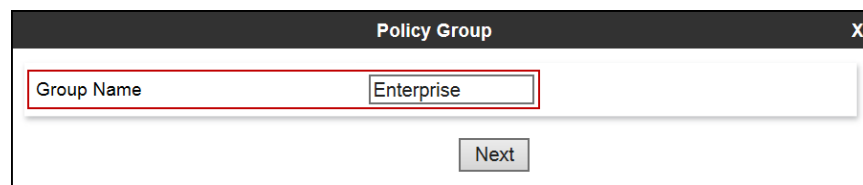
## 7.12. End Point Policy Groups

End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups.

### 7.12.1. End Point Policy Group – Enterprise

To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

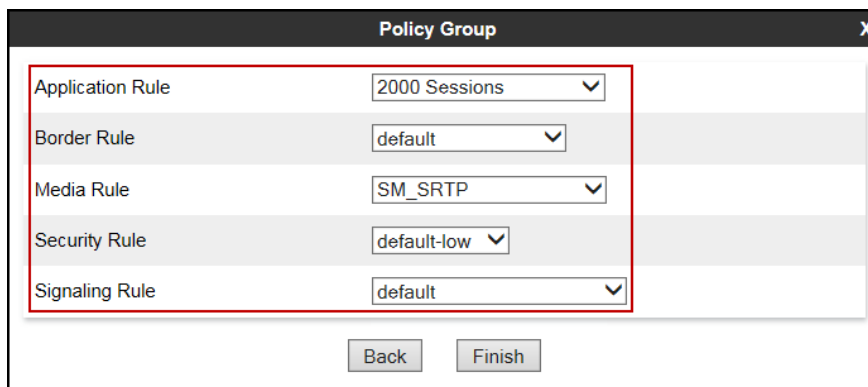
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" which contains the text "Enterprise". This field is highlighted with a red rectangular box. Below the input field, there is a "Next" button.

Under the **Policy Group** tab enter the following:

- **Application Rule:** *2000 Sessions* (Section 7.11.1).
- **Border Rule:** *default*.
- **Media Rule:** *SM\_SRTP* (Section 7.11.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default* (Section 7.11.3).
- Click **Finish**.

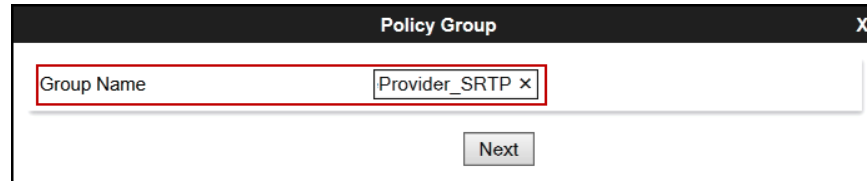


The screenshot shows the "Policy Group" dialog box with several dropdown menus. The "Application Rule" is set to "2000 Sessions", "Border Rule" is set to "default", "Media Rule" is set to "SM\_SRTP", "Security Rule" is set to "default-low", and "Signaling Rule" is set to "default". These dropdowns are grouped within a red rectangular box. At the bottom of the dialog, there are "Back" and "Finish" buttons.

### 7.12.2. End Point Policy Group – Service Provider

To create an End Point Policy Group for the Service Provider, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

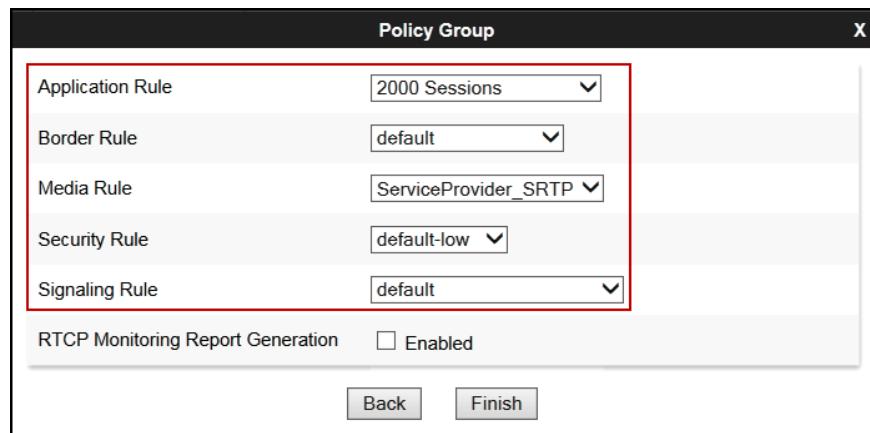
- Enter an appropriate name in the **Group Name** field (*ServiceProvider\_SRTP* was used).
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" which contains the text "Provider\_SRTP" followed by a small 'x' icon. Below the input field is a "Next" button.

Under the **Policy Group** tab enter the following:

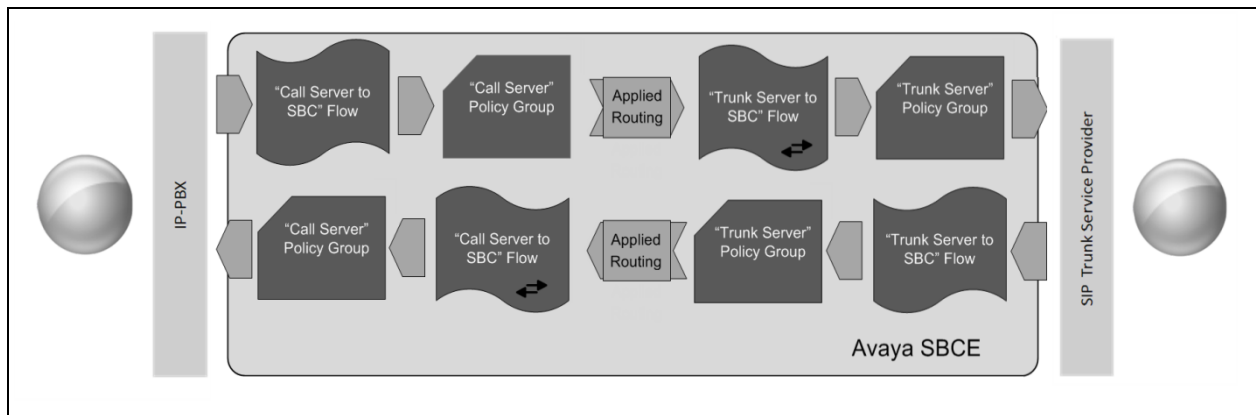
- **Application Rule:** *2000 Sessions* (Section 7.11.1).
- **Border Rule:** *default*.
- **Media Rule:** *ServiceProvider\_SRTP* (Section 7.11.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default* (Section 7.11.3).
- Click **Finish**.



The screenshot shows the "Policy Group" dialog box with several dropdown menus. The "Application Rule" is set to "2000 Sessions", "Border Rule" is set to "default", "Media Rule" is set to "ServiceProvider\_SRTP", "Security Rule" is set to "default-low", and "Signaling Rule" is set to "default". Below these dropdowns is a checkbox for "RTCP Monitoring Report Generation" which is currently unchecked. At the bottom of the dialog are "Back" and "Finish" buttons.

### 7.13. End Point Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP trunk call.



The **End-Point Flows** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

### 7.13.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named *Session\_Manager\_Flow* created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for the Service Provider in **Section 7.9.2**, which is the reverse route of the flow. Click **Finish**.

Edit Flow: Session_Manager_Flow	
Flow Name	Session_Manager_Flow
Server Configuration	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig
Signaling Interface	Private_sig
Media Interface	Private_med
Secondary Media Interface	None
End Point Policy Group	Enterprise
Routing Profile	Route_to_SP_TLS
Topology Hiding Profile	Session_Manager
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

### 7.13.2. End Point Flow – Service Provider

A second Server Flow with the name *SIP\_Trunk\_Flow\_TLS* was similarly created in the Service Provider direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in **Section 7.9.1**, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Click **Finish**.

Edit Flow: SIP_Trunk_Flow_TLS	
Flow Name	SIP_Trunk_Flow_TLS
Server Configuration	Service Provider TLS
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
Secondary Media Interface	None
End Point Policy Group	ServiceProvider_SRTP
Routing Profile	Route_to_SM
Topology Hiding Profile	Service_Provider
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

## 8. CenturyLink SIP Trunking Service on Perimeta/BroadWorks Platform Configuration

To use CenturyLink SIP Trunking Service on Perimeta/BroadWorks Platform, a customer must request the service from CenturyLink using the established sales processes. The process can be started by contacting CenturyLink via the corporate web site at:

<http://www.centurylink.com/business/voice/sip-trunk.html>

During the signup process, CenturyLink and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to CenturyLink's network.

CenturyLink will provide the following information:

- CenturyLink SIP proxy server IP address, SIP signaling transport (TLS was used) and port number (5101 was used).
- TLS certificate requirements (These requirements are beyond the scope of these Application Notes; hence they are not discussed in this document).
- SIP trunk registration credentials.
- DID and pilot numbers.
- Supported codecs and order of preference.
- Etc.

## 9. Verification and Troubleshooting

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 commands that can be used to troubleshoot the solution.

### 9.1. General Verification Steps

- 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.
- 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.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

### 9.2. Communication Manager Verification

The following commands can be entered in the Communication Manager SAT terminal to verify the SIP trunk functionality:

- **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 signaling-group** <signaling group number>



Displays signaling group service state.

- **status trunk** <trunk group number>  
Displays trunk group service state.
- **status station** <extension number>  
Displays signaling and media information for an active call on a specific station.

### 9.3. Session Manager Verification

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager** → **System Status** → **SIP Entity Monitoring**. Click the Session Manager instance (*Session Manager* in the example below).

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The left sidebar contains a navigation menu with categories like Session Manager, Network, Device and Location, Application, System Status, and Managed. The 'System Status' category is expanded, and 'SIP Entity Monitoring' is selected. The main content area is titled 'SIP Entity Link Monitoring Status Summary' and includes a 'Run Monitor' button. Below this is a table showing the status of monitored entities. The table has columns for Session Manager, Type, and a group of 'Monitored Entities' (Down, Partially Up, Up, Not Monitored, Deny, Total). One row is visible, showing 'Session Manager' of type 'Core' with 1 Down, 0 Partially Up, 5 Up, 0 Not Monitored, 0 Deny, and a Total of 6. A 'Filter: Enable' button is located at the top right of the table area.

Session Manager	Type	Monitored Entities					
		Down	Partially Up	Up	Not Monitored	Deny	Total
<a href="#">Session Manager</a>	Core	1	0	5	0	0	6

Verify that the state of the Session Manager links to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is **UP**, like shown on the screen below.

**Session Manager Entity Link Connection Status**

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

**All Entity Links for Session Manager: Session Manager**

Summary View

Status Details for the selected Session Manager:

SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<a href="#">CS1K7.6</a>	IPv4	172.16.5.60	5085	UDP	FALSE	DOWN	408 Request Timeout	DOWN
<a href="#">Avaya SBCE</a>	IPv4	10.64.101.243	5061	TLS	FALSE	UP	200 OK	UP
<a href="#">Communication Manager Trunk 1</a>	IPv4	10.64.101.241	5061	TLS	FALSE	UP	200 OK	UP
<a href="#">AA-Messaging</a>	IPv4	10.64.101.250	5060	TCP	FALSE	UP	200 OK	UP
<a href="#">Communication Manager Trunk 2</a>	IPv4	10.64.101.241	5071	TLS	FALSE	UP	200 OK	UP
<a href="#">Communication Manager Trunk 98</a>	IPv4	10.64.101.241	5065	TLS	FALSE	UP	200 OK	UP

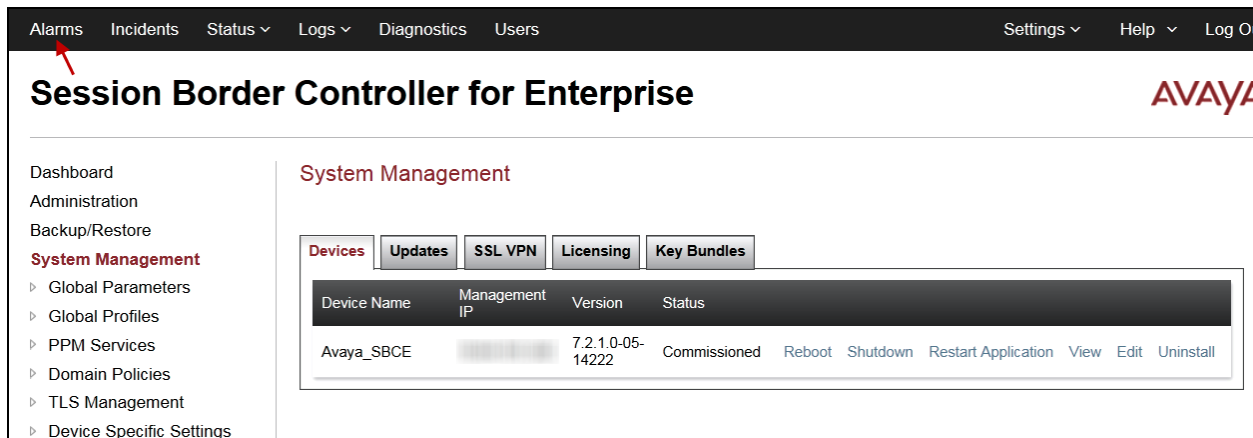
Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** – The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Enter the requested data to run the test.

## 9.4. Avaya SBCE Verification

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

**Alarms:** This screen provides information about the health of the SBC.



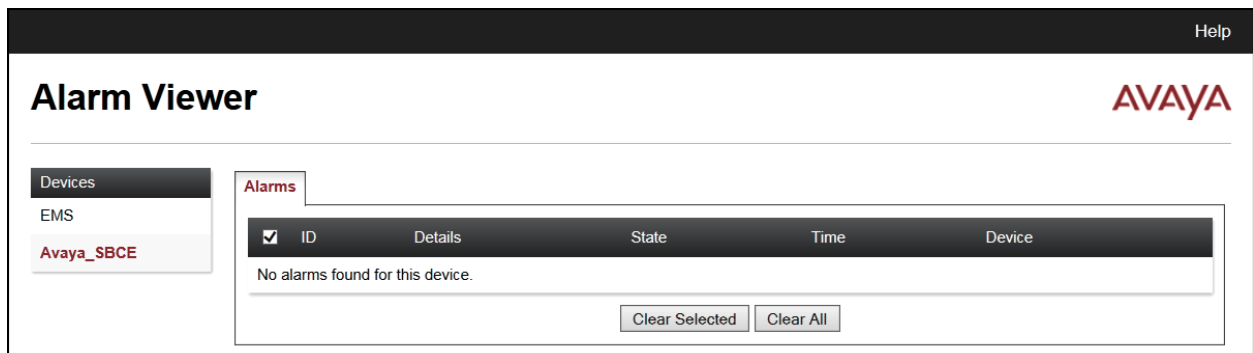
**Session Border Controller for Enterprise**

**System Management**

Devices | Updates | SSL VPN | Licensing | Key Bundles

Device Name	Management IP	Version	Status	
Avaya_SBCE		7.2.1.0-05-14222	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

The following screen shows the **Alarm Viewer** page.



**Alarm Viewer**

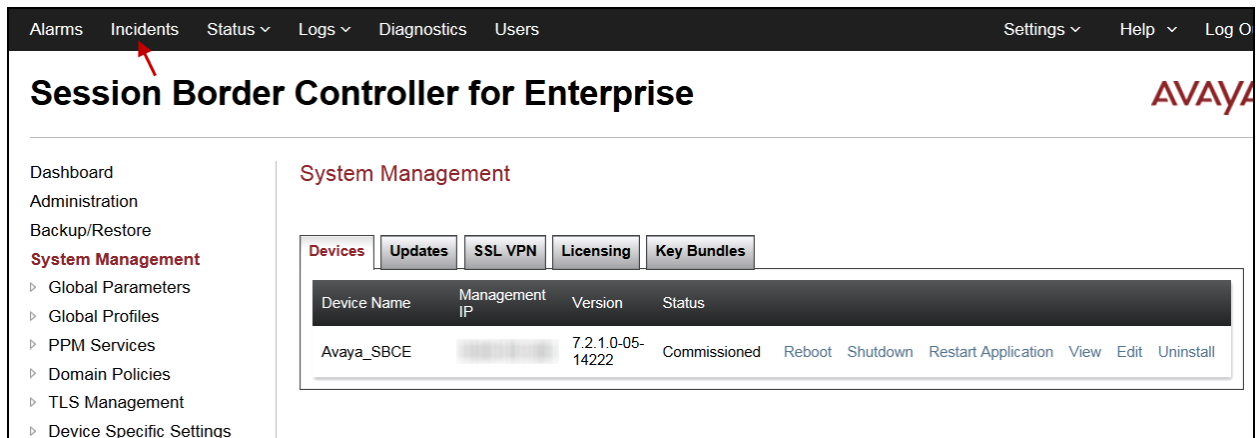
Devices | EMS | **Avaya\_SBCE**

**Alarms**

<input checked="" type="checkbox"/>	ID	Details	State	Time	Device
No alarms found for this device.					

Clear Selected Clear All

**Incidents** : Provides detailed reports of anomalies, errors, policies violations, etc.



**Session Border Controller for Enterprise** AVAYA

Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log O

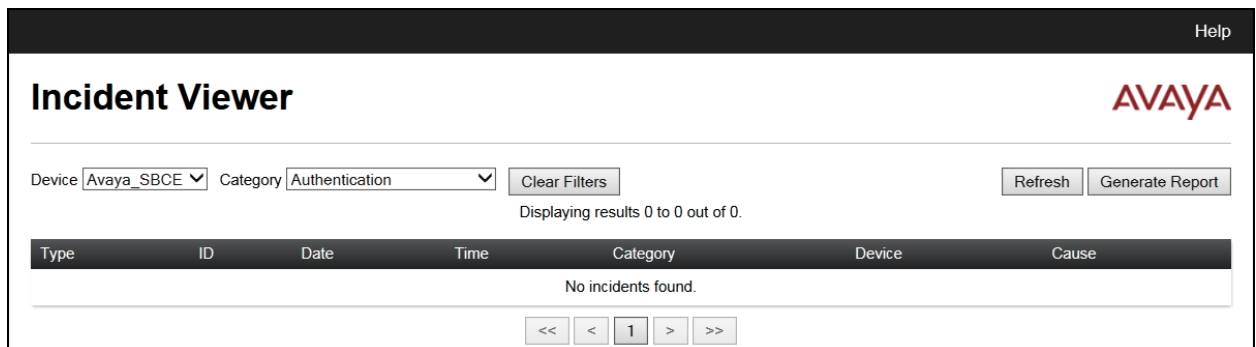
Dashboard  
Administration  
Backup/Restore  
**System Management**  
‣ Global Parameters  
‣ Global Profiles  
‣ PPM Services  
‣ Domain Policies  
‣ TLS Management  
‣ Device Specific Settings

**System Management**

Devices Updates SSL VPN Licensing Key Bundles

Device Name	Management IP	Version	Status	
Avaya_SBCE		7.2.1.0-05-14222	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

The following screen shows the Incident Viewer page.



**Incident Viewer** AVAYA

Device Avaya\_SBCE ▾ Category Authentication ▾ Clear Filters Refresh Generate Report

Displaying results 0 to 0 out of 0.

Type	ID	Date	Time	Category	Device	Cause
No incidents found.						

<< < 1 > >>

**Diagnostics:** This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

Alarms Incidents Status ▾ Logs ▾ **Diagnostics** Users Settings ▾ Help ▾ Log O

## Session Border Controller for Enterprise

AVAYA

Dashboard  
Administration  
Backup/Restore  
**System Management**  
‣ Global Parameters  
‣ Global Profiles  
‣ PPM Services  
‣ Domain Policies  
‣ TLS Management  
‣ Device Specific Settings

### System Management

Devices Updates SSL VPN Licensing Key Bundles

Device Name	Management IP	Version	Status	
Avaya_SBCE		7.2.1.0-05-14222	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

The following screen shows the Diagnostics page with the results of a ping test.

Help

## Diagnostics

AVAYA

Full Diagnostic Ping Test

Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.

Source Device / IP A1 ▾

Destination IP 10.64.101.249

Ping

Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as *pcap* files. Navigate to **Device Specific Settings** → **Troubleshooting** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

The screenshot displays the Avaya SBCE web interface. At the top, a navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left-hand sidebar lists various system management options, with "Device Specific Settings" and "Trace" highlighted. The main content area is titled "Trace: Avaya\_SBCE" and contains two tabs: "Packet Capture" (selected) and "Captures". The "Packet Capture Configuration" form includes the following fields: Status (Ready), Interface (Any), Local Address (All), Remote Address (\*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (CenturyLink.pcap). "Start Capture" and "Clear" buttons are located at the bottom of the form.

Packet Capture Configuration	
Status	Ready
Interface	Any
Local Address IP[:Port]	All
Remote Address *, *Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename Using the name of an existing capture will overwrite it.	CenturyLink.pcap

Once the capture is stopped, click the **Captures** tab and select the proper *pcap* file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. The left sidebar contains a menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Troubleshooting. The "Troubleshooting" category is expanded, showing options like Debugging, Trace, DoS Learning, and Logs Collection. The "Trace" option is selected. The main content area is titled "Trace: Avaya\_SBCE" and features two tabs: "Packet Capture" and "Captures". The "Captures" tab is active, displaying a table of captured files. The table has columns for File Name, File Size (bytes), and Last Modified. A single entry is shown: "CenturyLink\_20180510180559.pcap" with a size of 1,040,384 bytes and a timestamp of May 10, 2018 6:06:35 PM EDT. A "Delete" button is visible next to the entry. A "Refresh" button is located at the top right of the table area.

File Name	File Size (bytes)	Last Modified
CenturyLink_20180510180559.pcap	1,040,384	May 10, 2018 6:06:35 PM EDT

For TLS the **traceSBC** tool can be used to monitor the SIP signaling messages between the Service provider and the Avaya SBCE.

## 10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 7.1.2, Avaya Aura® Session Manager 7.1.2 and Avaya Session Border Controller for Enterprise 7.2.1, to connect to the CenturyLink SIP Trunking service on Perimeta/BroadWorks Platform using TLS and SRTP, as shown in **Figure 1**.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the observations/limitations described in **Sections 2.1** and **2.2**.

## 11. References

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

- [1] *Deploying Avaya Aura® Communication Manager*, Release 7.1.3, Issue 5, May 2018.
- [2] *Administering Avaya Aura® Communication Manager*, Release 7.1.3, Issue 7, May 2018.
- [3] *Administering Avaya Aura® System Manager* for Release 7.1.3, Issue 13, May 2018.
- [4] *Deploying Avaya Aura® System Manager*, Release 7.1.3, Issue 7, May 2018.
- [5] *Deploying Avaya Aura® Session Manager*, Release 7.1.3, Issue 5, May 2018.
- [6] *Administering Avaya Aura® Session Manager*, Release 7.1.3, Issue 4, May 2018.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.2.2, Issue 7, April 2018.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 7.2.2, Issue 9, April 2018.
- [9] *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*.
- [10] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.8, Issue 4, December 2017.
- [11] *Implementing and Administering Avaya Aura® Media Server*. Release 7.8, Issue 6, December 2017.
- [12] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [13] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>



## 12.Appendix A: SigMa Script

Following is the Signaling Manipulation script that was used in the configuration of the Avaya SBCE, **Section 7.7**. When adding this script as instructed in **Section 7.8.2** enter a name for the script in the Title (e.g., *CTL*) and copy/paste the entire script shown below. Note that the Pilot number shown below as “3031235745” will need to be changed with the correct Pilot number provided by CenturyLink.

---

### Title: CTL

```
//This script is to be applied to the Service Provider Server Configuration

//For Call Forward and Mobile features where CenturyLink requires PAI to be the pilot number.
within session "All"
{
    act on request where %DIRECTION="OUTBOUND" and
    %ENTRY_POINT="POST_ROUTING"
    {

        if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("3031235745")) then
        {
            %var="this does nothing, match for DID number passed";
        }
        else
        {
            %HEADERS["P-Asserted-Identity"][1].URI.USER = "3031235745";
        }
    }
}

//Fixes one-way audio issue on outbound calls from Avaya one-X Communicator (SIP mode)to
the
//PSTN. Removes codec G.729 (18)from final ACK on outbound calls originated from Avaya
one-X
//Communicator to PSTN.
within session "INVITE"
{
    act on message where %DIRECTION="OUTBOUND" and
    %ENTRY_POINT="POST_ROUTING" and %METHOD="ACK"
    {

        %BODY[1].regex_replace("0 18 120","0 120");
    }
}
```

---

**©2018 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).