



Application Notes for Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0 and Avaya Session Border Controller for Enterprise 8.0 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 8.0, Avaya Aura® Session Manager 8.0, Avaya Aura® Experience Portal 7.2 and Avaya Session Border Controller for Enterprise 8.0, to interoperate with the CenturyLink SIP Trunking service on Perimeta/BroadWorks Platform using Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP). These Application Notes update previously published Application Notes with newer versions of Communication Manager, Session Manager, and Avaya Session Border Controller for Enterprise.

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.

The CenturyLink SIP Trunking service provides 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	9
3.	Reference Configuration	10
4.	Equipment and Software Validated	13
5.	Configure Avaya Aura® Communication Manager	14
5.1.	Licensing and Capacity	14
5.2.	System Features.....	15
5.3.	IP Node Names.....	17
5.4.	Codecs	18
5.5.	IP Network Regions	20
5.6.	Signaling Group	21
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® Experience Portal	33
6.1.	Background	33
6.2.	Logging in and Licensing.....	34
6.3.	VoIP Connection	36
6.4.	Speech Servers	37
6.5.	Application References	38
6.6.	MPP Servers and VoIP Settings.....	39
6.7.	Configuring RFC2833 Event Value Offered by Experience Portal	43
7.	Configure Avaya Aura® Session Manager	44
7.1.	System Manager Login and Navigation.....	45
7.2.	SIP Domain	47
7.3.	Locations	47
7.4.	Adaptations.....	50
7.5.	SIP Entities	52
7.6.	Entity Links	55
7.7.	Routing Policies	57
7.8.	Dial Patterns	58
8.	Configure Avaya Session Border Controller for Enterprise	61
8.1.	System Access.....	61
8.2.	Device Management.....	63
8.3.	TLS Management.....	65
8.4.	Network Management	65
8.5.	Media Interfaces.....	66
8.6.	Signaling Interfaces.....	68

8.7.	Server Interworking.....	70
8.7.1.	Server Interworking Profile – Enterprise.....	70
8.7.2.	Server Interworking Profile – Service Provider.....	73
8.8.	Signaling Manipulation.....	75
8.9.	Server Configuration.....	78
8.9.1.	Server Configuration Profile – Enterprise	78
8.9.2.	Server Configuration Profile – Service Provider	80
8.10.	Routing	83
8.10.1.	Routing Profile – Enterprise.....	83
8.10.2.	Routing Profile – Service Provider	85
8.11.	Topology Hiding.....	86
8.11.1.	Topology Hiding Profile – Enterprise	86
8.11.2.	Topology Hiding Profile – Service Provider.....	88
8.12.	Domain Policies.....	89
8.12.1.	Application Rules.....	89
8.12.2.	Media Rules.....	90
8.12.3.	Signaling Rules	92
8.13.	End Point Policy Groups	93
8.13.1.	End Point Policy Group – Enterprise	93
8.13.2.	End Point Policy Group – Service Provider.....	94
8.14.	End Point Flows.....	95
8.14.1.	End Point Flow – Enterprise	96
8.14.2.	End Point Flow – Service Provider	97
9.	CenturyLink SIP Trunking Service on Perimeta/BroadWorks Platform Configuration	98
10.	Verification and Troubleshooting.....	98
10.1.	General Verification Steps.....	98
10.2.	Communication Manager Verification.....	98
10.3.	Session Manager Verification	99
10.4.	Avaya SBCE Verification	102
11.	Conclusion	107
12.	References.....	107
13.	Appendix A: SigMa Scripts	108
14.	Appendix A – Avaya Session Border Controller for Enterprise – Refer Handling.....	111

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 8.0 (Communication Manager), Avaya Aura® Session Manager 8.0 (Session Manager), Avaya Aura® Experience Portal 7.2 (Experience Portal), Avaya Session Border Controller for Enterprise 8.0 (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 J179 IP Deskphones (H.323), 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:
 - Outbound call to PSTN application requiring DTMF (e.g., an IVR or voice mail system).
 - Inbound call from PSTN to Avaya CPE application requiring DTMF (e.g., Aura® Messaging, Experience Portal, Avaya vector digit collection steps).
- 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.
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements and/or music on hold).
- Experience Portal use of SIP REFER to redirect inbound calls, via the Avaya SBCE, to the appropriate Communication Manager agents and extensions.
- Call and two-way talk path establishment between callers and Communication Manager agents and extensions following redirection from Experience Portal.

- 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. Consult reference [12] in the **References** section for additional information on this topic.

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

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

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

- Network Call Redirection using the “302 Moved Temporarily” method is not supported by CenturyLink.

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.
- **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 **Sections 8.8** and **13**.
- **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.
- **T.38 Fax Support** – CenturyLink supports T.38 fax, but it will not perform fax tone detection, thus CenturyLink will never send a re-INVITE to switch from voice to T.38. If the **FAX Mode** field on the Communication Manager **ip-codec-set** form page 2 is set to

“**t.38-standard**” (see **Section 5.4**), Communication Manager will send the proper re-INVITE to T.38 for both, inbound and outbound fax calls. Fax modes **pass-through** and **t.38-G711-fallback** are not supported by Communication Manager when SRTP media encryption is used on the public side (between the enterprise and the Service Provider). The only fax mode supported by Communication Manager with SRTP media encryption on the public side is **t.38-standard**.

- **Outbound T.38 Fax interworking with codec 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 outbound T.38 fax calls from the enterprise to the PSTN to timeout since the re-INVITE for T.38 fax negotiation was never received from CenturyLink, for reasons mentioned in the above observation. 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 and the **FAX Mode** field in the Communication Manager **ip-codec-set** form page 2 should be set to “**t.38-standard**”. This issue is under investigation by CenturyLink.
- **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 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 or in a response of “Unsupported Media Type” from the Service Provider. The work around is to set the **Extensions** to **Lync** in the Avaya SBCE, as shown in **Section 8.7.2**. This issue is under investigation by Avaya.
- **Calls to Experience Portal fail with Extensions set to Lync in the Avaya SBCE** – Setting the **Extensions** to **Lync** in the Avaya SBCE, as mentioned in the above observation, caused inbound calls from the PSTN to Experience Portal to be dropped by CenturyLink with a “BYE” message. The issue is related to a missing SDP parameter in the 200 OK message the Avaya SBCE sends CenturyLink, the missing parameter name is “**Content-Type: application/sdp**”. The issue was fixed with a Signaling Manipulation script (SigMa) on the Avaya SBCE, the script adds “**Content-Type: application/sdp**” to the **200 OK** message the Avaya SBCE sends CenturyLink. Refer to **Sections 8.8 and 13**. This issue is under investigation by Avaya.
- **Network Packets Limitation of 1500 bytes** – CenturyLink network SIP packet size limitation is 1500 bytes. Therefore, it is necessary to reduce the packet size of SIP messages sent to CenturyLink by removing unused SIP headers. If this limitation is not met CenturyLink will ignore (will not process) the SIP messages it receives from the

Avaya SBCE, resulting in call failure. Removal of unused SIP headers was accomplished via a Signaling Manipulation script (SigMa) in the Avaya SBCE. Refer to **Section 8.8** and **13**.

- **Incorrect Call Display on call transfers to the PSTN Phone** – Call display was not properly updated on PSTN phones involved in 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.
- **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 call shuffling (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 8.8** and **13**. 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 types, H.323 or SIP.
- **Removal of unwanted xml element information from the SDP in SIP messages sent to CenturyLink** – A Signaling Manipulation script (SigMa) on the Avaya SBCE was created to remove unwanted xml element information from the SDP in SIP messages the Avaya SBCE sent CenturyLink, the xml elements were causing calls to fail. Refer to **Sections 8.8** and **13**.
- **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-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector and P-

Location (Refer to **Section 7.4**). To help reduce the packet size further, the Avaya SBCE can remove the “*gsid*” and “*epv*” parameters that may be included within the Contact header by applying a Sigma script to the CenturyLink’s server configuration. Refer to **Section 8.8**, and **13**.

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.

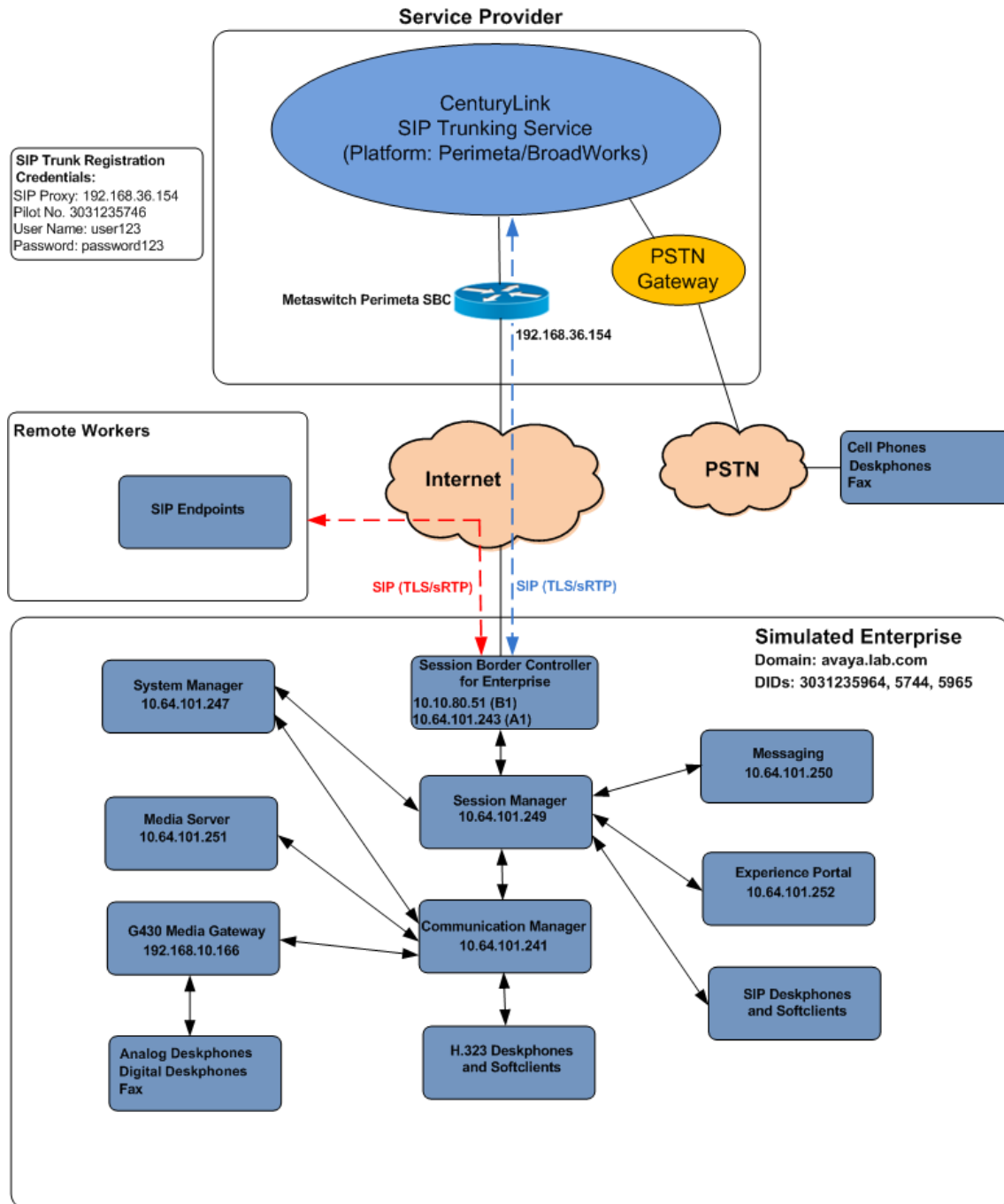


Figure 1: Avaya SIP Enterprise Solution connected to CenturyLink SIP Trunking Service

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 Aura® Experience Portal.
- Avaya G430 Media Gateway.
- Avaya 96x1 Series IP Deskphones (H.323 and SIP).
- Avaya J179 IP Deskphones (H.323).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Equinox™ for Windows softphone (SIP).
- Avaya digital and analog telephones.
- Ventafax fax software.

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 reference [11] 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 (Communication Manager or Experience Portal) and on which link to send the call.

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 8.0 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.

The 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.

The Avaya Aura® Experience Portal was also used during the compliance test to verify various SIP call flow scenarios with CenturyLink SIP trunking service.

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, between Avaya components) and outside of the enterprise (public network side, between the Avaya enterprise and CenturyLink).

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager	8.0.1.1.0 (00.0.822.0-25183)
Avaya Aura® Session Manager	8.0.1.1 (8.0.1.1.801103)
Avaya Aura® System Manager	8.0.1.1 Build No. 8.0.0.0.931077 Software Update Rev. No. 8.0.1.1.039340
Avaya Session Border Controller for Enterprise	ASBCE 8.0 8.0.0.0-19-16991
Avaya Aura® Messaging	7.1 Patch 1
Avaya Aura® Media Server	8.0.0 SP3 8.0.0.15
Avaya G430 Media Gateway	g430_sw_40_25_0
Avaya Aura® Experience Portal	7.2.2.0.2065
Avaya 96x1 Series IP Deskphones (SIP)	Version 7.1.4.0.11
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.8003
Avaya J179 IP Deskphones (H.323)	Version 6.8003
Avaya one-X® Communicator (H.323, SIP)	6.2.13.1-SP13
Avaya Equinox for Windows (SIP)	3.5.1.21.5
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
CenturyLink	
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 **30000** 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 2
      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: 30000 120
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
    Maximum Number of DS1 Boards with Echo Cancellation: 688 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? all
  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*.

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 SRTP: best-effort

On **Page 2**, set the **Fax Mode** to *t.38-standard* and **ECM** to *y*.

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		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y		RSVP Enabled? n
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	A	M
dst rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Intervening Prio Shr Regions	Dyn CAC	A	G	L	R		t
1	2	y	NoLimit			n						e
2	2								all			t
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	Clustered? <u>n</u>	
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>			
Bypass If IP Threshold Exceeded? <u>n</u>			
Incoming Dialog Loopbacks: <u>eliminate</u>	RFC 3389 Comfort Noise? <u>n</u>		
DTMF over IP: <u>rtp-payload</u>	Direct IP-IP Audio Connections? <u>y</u>		
Session Establishment Timer(min): <u>3</u>	IP Audio Hairpinning? <u>n</u>		
Enable Layer 3 Test? <u>n</u>	Initial IP-IP Direct Media? <u>n</u>		
H.323 Station Outgoing 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 4
                                     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 4
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>	
		Preferred Minimum Session Refresh Interval(sec): <u>600</u>
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 4

TRUNK FEATURES

ACA Assignment? ☒ Measured: none Maintenance Tests? y

Suppress # Outpulsing? ☐ **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 4
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.

```
change private-numbering 1
```

```
Page    1 of   2
```

```
NUMBERING - PRIVATE FORMAT
```

Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len
<u>4</u>	<u>3</u>	<u> </u>	<u> </u>	<u>4</u>
<u>4</u>	<u>5</u>	<u> </u>	<u> </u>	<u>4</u>
<u>4</u>	<u>3042</u>	<u>2</u>	<u>3031235964</u>	<u>10</u>
<u>4</u>	<u>3044</u>	<u>2</u>	<u>3031235965</u>	<u>10</u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>

Total Administered: 3
Maximum Entries: 540

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	3031235964	10	3042		
public-ntwrk	10	3031235965	10	3044		
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	—	—	—	—		
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

Page 1 of 12

DIAL PLAN ANALYSIS TABLE

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® Experience Portal

These Application Notes assume that the necessary Experience Portal licenses have been installed and basic Experience Portal administration has already been performed. Consult [9] in the **References** section for further details if necessary.

6.1. Background

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

References to the Voice XML and/or Call Control XML applications are administered on Experience Portal, along with one or more called numbers for each application reference. When an inbound call arrives at Experience Portal, the called party DID number is matched against those administered called numbers. If a match is found, then the corresponding application is accessed to handle the call. If no match is found, Experience Portal informs the caller that the call cannot be handled and disconnects the call¹.

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

¹ An application may be configured with “inbound default” as the called number, to process all inbound calls that do not match any other application references.

6.2. Logging in and Licensing

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

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

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

The screenshot displays the Avaya Aura Experience Portal Manager web interface. At the top, the Avaya logo is on the left, and the user 'epadmin' is welcomed on the right, with a timestamp 'Last logged in Jan 29, 2019 at 11:55:28 AM PST'. Below the header, a navigation menu on the left lists categories like User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration, each with sub-items. The main content area is titled 'Avaya Aura® Experience Portal Manager' and includes a brief description of the EPM application. It features sections for 'Installed Components' (Media Processing Platform, Email Service, HTML Service, SMS Service) and a 'Legal Notice' section containing the 'AVAYA GLOBAL SOFTWARE LICENSE TERMS'.

Avaya Aura® Experience Portal Manager

Avaya Aura® Experience Portal Manager (EPM) is the consolidated web-based application for administering Experience Portal. Through the EPM interface you can configure Experience Portal, check the status of an Experience Portal component, and generate reports related to system operation.

Installed Components

Media Processing Platform
Media Processing Platform (MPP) is an Avaya media processing server. When an MPP receives a call from a PBX, it invokes a VoiceXML (or CCXML) application on an application server. It then communicates with ASR and TTS servers as necessary to process the call.

Email Service
Email Service is an Experience Portal feature which provides e-mail capabilities.

HTML Service
HTML Service is an Experience Portal feature which supports web applications with HTML5 capabilities. It includes support for browser based services for mobile devices.

SMS Service
SMS Service is an Experience Portal feature which provides SMS capabilities.

Legal Notice

AVAYA GLOBAL SOFTWARE LICENSE TERMS
REVISED: May 1, 2017

THESE GLOBAL SOFTWARE LICENSE TERMS ("SOFTWARE LICENSE TERMS") GOVERN THE USE OF PROPRIETARY SOFTWARE AND THIRD-PARTY PROPRIETARY SOFTWARE LICENSED THROUGH AVAYA. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR ENTIRETY, BEFORE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (AS DEFINED IN SECTION A BELOW). BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU," "YOUR," AND "END USER"), AGREE TO THESE SOFTWARE LICENSE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA"). IF YOU ARE ACCEPTING THESE SOFTWARE LICENSE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND

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

AVAYA

Welcome, epadmin
Last logged in Jan 29, 2019 at 11:55:28 AM PST

Press **F11** to exit full screen

Avaya Aura® Experience Portal 7.2.0 (ExperiencePortal)

Expand All | Collapse All

▼ User Management
Roles
Users
Login Options

▼ Real-time Monitoring
System Monitor
Active Calls
Port Distribution

▼ System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

▼ System Management
Application Server
EPM Manager
MPP Manager
Software Upgrade
System Backup

▼ System Configuration
Applications
EPM Servers
MPP Servers
SNMP
Speech Servers
VoIP Connections
Zones

▼ Security
Certificates
Licensing

▼ Reports
Standard
Custom
Scheduled

▼ Multi-Media Configuration
Email
HTML
SMS

You are here: [Home](#) > [Security](#) > [Licensing](#)

Licensing

This page displays the Experience Portal license information that is currently in effect. Experience Portal uses Avaya License Manager (WebLM) to control the number of telephony ports that are used.

License Server Information

License Server URL:	https://10.64.101.247:52233/WebLM/LicenseServer
Last Updated:	Dec 4, 2018 3:20:00 PM PST
Last Successful Poll:	Feb 5, 2019 1:34:37 PM PST

Licensed Products

Product	Value
Experience Portal	100
Announcement Ports:	100
ASR Connections:	10
Email Units:	1
Enhanced Media Encryption:	100
Enhanced Call Classification:	10
HTML Units:	100
SIP Signaling Connections:	10
SMS Units:	100
Telephony Ports:	100
TTS Connections:	100
Video Server Connections:	1
Zones:	7
Version:	Feb 5, 2019 1:34:37 PM PST
Last Successful Poll:	Dec 4, 2018 3:19:59 PM PST
Last Changed:	

Allocations **Help**

6.3. VoIP Connection

This section defines a SIP trunk between Experience Portal and Session Manager (**Sections 7.5 and 7.6**).

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

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

The screenshot shows the Avaya Aura Experience Portal 7.2.0 (ExperiencePortal) interface. The left sidebar contains a navigation menu with the following items: User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration (highlighted), and Security. Under System Configuration, the following items are listed: Applications, EPM Servers, MPP Servers, SNMP, Speech Servers, VoIP Connections (highlighted), Zones, and Certificates. The main content area shows the 'VoIP Connections' page. At the top, it says 'You are here: Home > System Configuration > VoIP Connections'. Below this, it says 'VoIP Connections'. A message states: 'This page displays a list of Voice over Internet Protocol (VoIP) servers that Experience Portal communicates with. You can configure multiple SIP connections, but only one SIP connection can be enabled at any one given time.' Below the message, there is a table with the following columns: Name, Enable, Proxy Transport, Proxy/DNS Server Address, Proxy Server Port, Listener Port, SIP Domain, and Maximum Simultaneous Calls. The table contains one entry: EP_SIP, Yes, TLS, 10.64.101.249, 5061, 5061, avaya.lab.com, 100. Below the table, there are three buttons: Add, Delete, and Help. The 'Add' button is highlighted with a red box.

Step 2 - Configure a SIP connection as follows:

- **Name** – Set to a descriptive name (e.g., **EP_SIP**).
- **Enable** – Set to **Yes**.
- **Proxy Server Transport** – Set to **TLS**.
- Select **Proxy Servers**, and enter:
 - **Proxy Server Address** = **10.64.101.249** (the IP address of the Session Manager signaling interface defined in **Section 7.5**).
 - **Port** = **5061**
 - **Priority** = **0** (default)
 - **Weight** = **0** (default)
- **Listener Port** – Set to **5061**.
- **SIP Domain** – Set to **avaya.lab.com** (see **Section 7.2**).
- **Consultative Transfer** – Select **REFER**.
- **SIP Reject Response Code** – Select **ASM (503)**.
- **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In the reference configuration a value of **100** was used.
- Select **All Calls can be either inbound or outbound**.

- **SRTP Enable = Yes**
- **Encryption Algorithm = AES_CM_128**
- **Authentication Algorithm = HMAC_SHA1_80**
- **RTCP Encryption Enabled = No**
- **RTP Authentication Enabled = Yes**
- Click on **Add** to add SRTP settings to the **Configured SRTP List**
- Use default values for all other fields.
- Click **Save**.

AVAYA Welcome, epadmin
Last logged in Jan 29, 2019 at 11:55:28 AM PST

Avaya Aura® Experience Portal 7.2.0 (ExperiencePortal)

Expand All | Collapse All

- ▼ **User Management**
 - Roles
 - Users
 - Login Options
- ▼ **Real-time Monitoring**
 - System Monitor
 - Active Calls
 - Port Distribution
- ▼ **System Maintenance**
 - Audit Log Viewer
 - Trace Viewer
 - Log Viewer
 - Alarm Manager
- ▼ **System Management**
 - Application Server
 - EPN Manager
 - MPP Manager
 - Software Upgrade
- ▼ **System Configuration**
 - Applications
 - EPN Servers
 - MPP Servers
 - SNMP
 - Speech Servers
 - VoIP Connections
- ▼ **Security**
 - Zones
 - Certificates
 - Licensing
- ▼ **Reports**
 - Standard
 - Custom
 - Scheduled
- ▼ **Multi-Media Configuration**
 - Email
 - HTML
 - SMS

Name: EP_SIP
Enable: ☒ Yes ☐ No
Proxy Transport: TLS
☒ Proxy Servers ☐ DNS SRV Domain

Address	Port	Priority	Weight	
10.64.101.249	5061	0	0	Remove

Additional Proxy Server
Listener Port: 5061
SIP Domain: avaya.lab.com
P-Asserted-Identity:
Maximum Redirection Attempts: 0
Consultative Transfer: ☐ INVITE with REPLACES ☒ REFER
SIP Reject Response Code: ☒ ASM (503) ☐ SES (480) ☐ Custom 503

SIP Timers
T1: 250 milliseconds
T2: 2000 milliseconds
B and F: 4000 milliseconds

Call Capacity
Maximum Simultaneous Calls: 100
☒ All Calls can be either inbound or outbound
☐ Configure number of inbound and outbound calls allowed

SRTP
Enable: ☒ Yes ☐ No
Encryption Algorithm: ☒ AES_CM_128 ☐ NONE
Authentication Algorithm: ☒ HMAC_SHA1_80 ☐ HMAC_SHA1_32
RTCP Encryption Enabled: ☐ Yes ☒ No
RTP Authentication Enabled: ☒ Yes ☐ No **Add**

Configured SRTP List
 SRTP-Yes,AES_CM_128,HMAC_SHA1_80,RTCP Encryption-No,RTP Authentication-Yes **Remove**

Save Apply Cancel Help

6.4. Speech Servers

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

ASR speech server:

Avaya Aura® Experience Portal 7.2.0 (ExperiencePortal)

Welcome, eadmin
Last logged in Jan 29, 2019 at 11:55:28 AM PST

You are here: [Home](#) > System Configuration > Speech Servers

Speech Servers

This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with.

ASR **TTS**

Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed ASR Resources	Languages
NuanceASR	Yes	10.64.101.154	Nuance	MRCP V1 4900	10	English(USA) en-US	

Add **Delete** **Customize** **Help**

TTS speech server:

Avaya Aura® Experience Portal 7.2.0 (ExperiencePortal)

Welcome, eadmin
Last logged in Jan 29, 2019 at 11:55:28 AM PST

You are here: [Home](#) > System Configuration > Speech Servers

Speech Servers

This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with.

ASR **TTS**

Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed TTS Resources	Voices
Nuance	Yes	10.64.101.154	Nuance	MRCP V1 4900	10	English(USA) en-US Jennifer F	

Add **Delete** **Customize** **Help**

6.5. Application References

This section describes the steps for administering a reference to the VXML and/or CCXML applications residing on the application server. In the sample configuration, the applications were co-resident on one Experience Portal server, with IP Address 10.64.101.252.

Step 1 - In the left pane, navigate to **System Configuration** → **Applications**. On the **Applications** page (not shown), click **Add** to add an application and configure as follows:

- **Name** – Set to a descriptive name (e.g., **Test2_APP**).
- **Enable** – Set to **Yes**. This field determines which application(s) will be executed based on their defined criteria.
- **Type** – Select **VoiceXML**, **CCXML**, or **CCXML/VoiceXML** according to the application type.
- **VoiceXML** and/or **CCXML URL** – Enter the necessary URL(s) to access the VXML and/or CCXML application(s) on the application server. In the sample screen below, the Experience Portal test application on a single server is referenced.

- **Speech Servers ASR and TTS** – Select the appropriate ASR and/or TTS servers as necessary.
- **Application Launch** – Set to **Inbound**.
- **Called Number** – Enter the number to match against an inbound SIP INVITE message and click **Add**. In the sample configuration illustrated in these Application Notes, the dialed DID number 3031235744 provided by CenturyLink was used. Repeat to define additional called party numbers as needed. Inbound calls with these called party numbers will be handled by the application defined in this section.

Avaya Aura® Experience Portal 7.2.0 (ExperiencePortal)

Welcome, epadmin
Last logged in Jan 29, 2019 at 11:55:28 AM PST

You are here: [Home](#) > [System Configuration](#) > [Applications](#) > [Change Application](#)

Change Application

Use this page to change the configuration of an application.

Name: Test2_APP
 Enable: ☒ Yes ☐ No
 Type:
 Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum
 Requested:
 URI
☒ Single ☐ Fail Over ☐ Load Balance
 CCXML URL: **Verify**
 Mutual Certificate Authentication: ☐ Yes ☒ No
 Basic Authentication: ☐ Yes ☒ No

Speech Servers

ASR:
 Languages:
 Selected Languages:
 TTS:
 Voices:
 Selected Voices:

Application Launch

☒ Inbound ☐ Inbound Default ☐ Outbound
☒ Number ☐ Number Range ☐ URI
 Called Number: **Add**
 Remove

Speech Parameters **Reporting Parameters** **Advanced Parameters**

Save **Apply** **Cancel** **Help**

6.6. MPP Servers and VoIP Settings

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

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

AVAYA Welcome, eadmin
Last logged in Jan 29, 2019 at 11:55:28 AM PST

Avaya Aura® Experience Portal 7.2.0 (ExperiencePortal)

You are here: [Home](#) > System Configuration > MPP Servers

MPP Servers

This page displays the list of Media Processing Platform (MPP) servers in the Experience Portal system. When an MPP receives a call from a PBX, it invokes a VoiceXML application on an application server and communicates with ASR and TTS servers as necessary to process the call.

<input type="checkbox"/>	Name	Host Address	Network Address (VoIP)	Network Address (MRCP)	Network Address (AppSvr)	Maximum Simultaneous Calls	Trace Level
<input type="checkbox"/>	MPP	10.64.101.252	<Default>	<Default>	<Default>	10	Use MPP Settings

Add **Delete**

MPP Settings **Browser Settings** **Video Settings** **VoIP Settings** **Help**

Step 2 - Enter any descriptive name in the **Name** field (e.g., **MPP**) and the IP address of the MPP server in the **Host Address** field and click **Continue** (not shown). Note that the Host Address used is the same IP address assigned to Experience Portal.

Step 3 - The certificate page will open. Check the **Trust this certificate** box (not shown). Once complete, click **Save**.

AVAYA Welcome, eadmin
Last logged in Jan 29, 2019 at 11:55:28 AM PST

Avaya Aura® Experience Portal 7.2.0 (ExperiencePortal)

You are here: [Home](#) > System Configuration > [MPP Servers](#) > Change MPP Server

Change MPP Server

Use this page to change the configuration of an MPP. Take care when changing the MPP Trace Logging Thresholds. Do not set Trace Levels to Finest if your Experience Portal system has heavy call traffic. The system might experience performance issues if Trace Levels are set to Finest. Set Trace Levels to Finest only when you are troubleshooting the system.

Name: MPP
Host Address: 10.64.101.252
Network Address (VoIP): <Default>
Network Address (MRCP): <Default>
Network Address (AppSvr): <Default>
Maximum Simultaneous Calls: 10
Restart Automatically: ☒ Yes ☐ No

MPP Certificate

```
Owner: CN=hg-aep-thornton.avaya.lab.com,O=Avaya,OU=EPH
Issuer: CN=hg-aep-thornton.avaya.lab.com,O=Avaya,OU=EPH
Serial Number: 0bed8d8c7243144
Signature Algorithm: SHA256withRSA
Valid from: November 16, 2018 10:24:54 AM PST until November 13, 2028 10:24:54 AM PST
Certificate Fingerprints
MD5: c8:38:2d:e6:7e:55:fc:e7:a0:bb:69:91:20:60:0b:e4
SHA: 36:bc:ca:02:1f:a8:9a:d0:37:32:33:00:7f:3d:71:99:a9:10:53:08
SHA-256: ff:80:8a:07:92:d5:55:cd:0b:a5:7f:fd:d8:d2:52:5e:16:14:da:a1:66:c6:f2:dd:2e:26:8d:88:49:12:ee:f0
Subject Alternative Names
DNS Name: hg-aep-thornton
DNS Name: hg-aep-thornton.avaya.lab.com
IP Address: 10.64.101.252
```

Categories and Trace Levels >

Save **Apply** **Cancel** **Help**

Step 4 - Click **VoIP Settings** tab on the screen displayed in **Step 1**, and the following screen is displayed.

- In the Port Ranges section, default ports were used.

AVAYA Welcome, eadmin
Last logged in Jan 29, 2019 at 11:55:28 AM PST

Avaya Aura® Experience Portal 7.2.0 (ExperiencePortal)

You are here: [Home](#) > [System Configuration](#) > [MPP Servers](#) > VoIP Settings

VoIP Settings

Voice over Internet Protocol (VoIP) is the process of sending voice data through a network using one or more standard protocols such as H.323 and Real-time Transfer Protocol (RTP). Use this page to configure parameters that affect how voice data is transferred through the network. Note that if you make any changes to this page, you must restart all MPPs.

Port Ranges

	Low	High
UDP:	11000	30999
TCP:	31000	33499
MRCP:	34000	36499
H.323 Station:	37000	39499

RTCP Monitor Settings

Host Address:
Port:

VoIP Audio Formats

MPP Native Format:

Codecs

QoS Parameters

Out of Service Threshold (% of VoIP Resources)

Call Progress

Miscellaneous

Save **Apply** **Cancel** **Help**

- In the Codecs section set:
 - Set **Packet Time** to **20**.
 - Verify Codecs **G711uLaw** and **G729** are enabled (check marks). Set the **Offer** and Answer **Order** as shown. In the sample configuration **G711uLaw** is the preferred codec, with **Order 1**, followed by **G729**, with **Order 2**.
 - On the codec Offer set **G729 Discontinuous Transmission** to **No** (for G.729A).
- Use default values for all other fields.

Step 5 - Click on **Save** (not shown).

AVAYA Welcome, epadmin
Last logged in yesterday at 7:18:57 AM PDT

Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal) Home ? Help Logoff

Expand All Collapse All

You are here: Home > System Configuration > MPP Servers > VoIP Settings

VoIP Settings

Voice over Internet Protocol (VoIP) is the process of sending voice data through a network using one or more standard protocols such as H.323 and Real-time Transfer Protocol (RTP). Use this page to configure parameters that affect how voice data is transferred through the network. Note that if you make any changes to this page, you must restart all MPPs.

Port Ranges

	Low	High
UDP:	11000	30999
TCP:	31000	33499
MRCP:	34000	36499
H.323 Station:	37000	39499

RTCP Monitor Settings

Host Address:

Port:

VoIP Audio Formats

MPP Native Format:

Codecs

Offer

Enable	Codec	Order
<input checked="" type="checkbox"/>	G711uLaw	1
<input checked="" type="checkbox"/>	G729	2
<input type="checkbox"/>	G711aLaw	

Packet Time: milliseconds

G729 Discontinuous Transmission: ☐ Yes ☒ No

Answer

Enable	Codec	Order
<input checked="" type="checkbox"/>	G711uLaw	1
<input type="checkbox"/>	G711aLaw	
<input checked="" type="checkbox"/>	G729	2

G729 Discontinuous Transmission: ☐ Yes ☐ No ☒ Either

G729 Reduced Complexity Encoder: ☒ Yes ☐ No

QoS Parameters

Out of Service Threshold (% of VoIP Resources)

Call Progress

Miscellaneous

6.7. Configuring RFC2833 Event Value Offered by Experience Portal

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

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

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

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

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

The screenshot shows the Avaya Experience Portal 7.2.0 GUI. The top navigation bar includes the Avaya logo, user information (Welcome, epadmin), and a timestamp (Last logged in Jan 29, 2019 at 11:55:28 AM PST). The main content area is titled 'MPP Manager (Feb 5, 2019 2:34:27 PM PST)'. It contains a table with the following data:

Server Name	Mode	State	Config	Auto Restart	Restart Schedule	Active Calls		
					Today	Recurring	In	Out
MPP	Online	Running	OK	Yes	No	None	0	0

Below the table, there are two sections: 'State Commands' with buttons for Start, Stop, Restart, Reboot, Halt, and Cancel; and 'Mode Commands' with buttons for Offline, Test, and Online. The Restart button is highlighted in red. There is also a 'Restart/Reboot Options' section with radio buttons for 'One server at a time' and 'All servers'.

7. 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, Experience Portal 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.

7.1. 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; under **elements** select **Routing** → **Domains**.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The 'Elements' menu is expanded, showing a list of system components. The 'Routing' option is highlighted, and its sub-menu is visible, with 'Domains' selected. The main dashboard area contains several widgets: 'System Resource Utilization' (a bar chart showing utilization for 'opt', 'var', and 'emdata'), 'Alarms' (empty), 'Notifications' (empty), 'Application State' (showing license status as 'Active'), 'Information' (a table of system components and their sync status), and 'Shortcuts' (empty). The 'Information' table is as follows:

Elements	GNRL	Sync Status
CM	1	■
Messaging	1	■
Session Manager	1	■
System Manager	1	■
UCM Applications	16	■

Below the table, the 'Current Usage' section shows two bars: '6/250000 USERS' and '1/50 SIMULTANEOUS ADMINISTRATIVE LOGINS'.

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.

The screenshot displays the Avaya Aura System Manager 8.0 web interface. The top navigation bar includes the Avaya logo, the text "Aura® System Manager 8.0", and several menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled "admin" are also present. Below the top bar, a secondary navigation bar shows "Home" and "Routing x". The left-hand navigation pane is expanded, showing a tree structure under the "Routing" category. The "Domains" item is highlighted in blue. Other items in the tree include Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "Domain Management" and features a "Help ?" link. Below the title is a toolbar with buttons for "New", "Edit", "Delete", "Duplicate", and a "More Actions" dropdown. A status bar indicates "1 Item" and a "Filter: Enable" option. A table lists the domain configuration:

<input type="checkbox"/>	Name	Type	Notes
<input type="checkbox"/>	avaya.lab.com	sip	HG V-Domain

Below the table, there is a "Select : All, None" option and a scroll bar.

7.2. 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 displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts' menus, along with a search bar and a user profile 'admin'. The left-hand navigation pane shows 'Routing' selected, with 'Domains' highlighted. The main content area is titled 'Domain Management' and features a table with one item. The table has columns for 'Name', 'Type', and 'Notes'. The entry shows 'avaya.lab.com' as the Name, 'sip' as the Type, and 'HG V-Domain' as the Notes. Below the table, there is a 'Select : All, None' option.

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

7.3. 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 8.0 interface. The top navigation bar includes the Avaya logo, version information, and user roles (Users, Elements, Services, Widgets, Shortcuts). A search bar and a user profile icon (admin) are also present. The left sidebar shows a tree view with 'Routing' selected, and 'Locations' highlighted under it. The main content area is titled 'Location Details' and contains a 'General' section. In this section, the '* Name' field is set to 'Session Manager' and the 'Notes' field is set to 'VMware Session Manager'. Below this, 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'. The 'Overall Managed Bandwidth' section includes a 'Managed Bandwidth Units' dropdown set to 'Kbit/sec', and fields for 'Total Bandwidth' and 'Multimedia Bandwidth'. 'Commit' and 'Cancel' buttons are located at the top right of the form.

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 8.0 interface as the previous one, but with the 'Name' field set to 'Communication Manager' and the 'Notes' field set to 'VMware Communication Manager'. All other fields and the overall layout remain identical to the first screenshot.

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 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.0', and user options like 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also present. The left sidebar shows a tree view with 'Routing' selected, and 'Locations' highlighted under it. The main content area is titled 'Location Details' and contains three sections: 'General', 'Dial Plan Transparency in Survivable Mode', and 'Overall Managed Bandwidth'. In 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 empty fields for 'Listed Directory Number' and 'Associated CM SIP Entity'. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' set to 'Kbit/sec' and empty fields for 'Total Bandwidth' and 'Multimedia Bandwidth'. 'Commit' and 'Cancel' buttons are located at the top right of the form.

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

This screenshot shows the same Avaya Aura System Manager 8.0 interface as the previous one, but with the 'Location Details' for 'Lab Others'. The navigation path remains the same. In the 'General' section, the '* Name' field is now 'Lab Others' and the 'Notes' field is 'VMware Lab others'. The other sections, including the 'Dial Plan Transparency in Survivable Mode' and 'Overall Managed Bandwidth' settings, remain unchanged from the previous screenshot.

7.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 8.0 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-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 8.0 interface. The top navigation bar includes the Avaya logo, version information, and user roles (Users, Elements, Services, Widgets, Shortcuts). A search bar and a user profile icon (admin) are also present. The left sidebar shows a tree view with categories like Routing, Domains, Locations, Conditions, Adaptations, Regular Expression..., SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The 'Routing' category is expanded, and the 'Adaptations' sub-item is selected.

The main content area is titled 'Adaptation Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the following fields are visible:

- * Adaptation Name:** CM_Outbound_Header_Removal
- * Module Name:** DigitConversionAdapter
- Module Parameter Type:** Name-Value Parameter

Below these fields is a table for defining parameters:

Name	Value
eRHdrs	"Alert-Info, P-Charging-Vector, AV-Correlation-ID, P-AV-Message-id, P-Location, Endpoint-View"

Below the table, there are fields for 'Egress URI Parameters' and 'Notes'. At the bottom, there is a section titled 'Digit Conversion for Incoming Calls to SM' with an 'Add' button and a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes. The table currently shows 0 items.

7.5. SIP Entities

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

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, *SIP Trunk* (or *Other*) for the Avaya SBCE and *Voice Portal* for the Experience Portal.
 - **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.
1. **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 7.3**.
- **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 displays the Avaya Aura System Manager 8.0 interface. The left navigation pane shows the 'SIP Entities' menu item highlighted. The main content area is titled 'SIP Entity Details' and is divided into 'General' and 'Monitoring' sections. The 'General' section contains the following fields:

- Name:** Session Manager
- IP Address:** 10.64.101.249
- SIP FQDN:**
- Type:** Session Manager (dropdown)
- Notes:** VMware Session Manager
- Location:** Session Manager (dropdown)
- Outbound Proxy:**
- Time Zone:** America/New_York (dropdown)
- Minimum TLS Version:** Use Global Setting (dropdown)
- Credential name:**

The 'Monitoring' section contains the following fields:

- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)
- CRLF Keep Alive Monitoring:** CRLF Monitoring Disabled (dropdown)

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 7.3**. Select the **Time Zone**.

The screenshot displays the Avaya Aura System Manager 8.0 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.0', and tabs for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also present. The left sidebar shows a navigation menu with 'Routing' selected, and a sub-menu where 'SIP Entities' is highlighted. The main content area is titled 'SIP Entity Details' with a 'General' tab. The form contains the following fields: 'Name' (Communication Manager Trunk 2), 'FQDN or IP Address' (10.64.101.241), 'Type' (CM), 'Notes' (Used for SP Testing), 'Adaptation' (empty), 'Location' (Communication Manager), 'Time Zone' (America/New_York), 'SIP Timer B/F (in seconds)' (4), 'Minimum TLS Version' (Use Global Setting), 'Credential name' (empty), 'Securable' (unchecked), and 'Call Detail Recording' (none). 'Commit' and 'Cancel' buttons are located at the top right of the form area.

* Name:	Communication Manager Trunk 2
* FQDN or IP Address:	10.64.101.241
Type:	CM
Notes:	Used for SP Testing
Adaptation:	
Location:	Communication Manager
Time Zone:	America/New_York
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	<input type="checkbox"/>
Call Detail Recording:	none

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 7.4** was selected.
- Select the location that applies to the SIP Entity being created, defined in **Section 7.3**.
- Select the **Time Zone**.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar has a 'Routing' menu with 'SIP Entities' highlighted. The main area is titled 'SIP Entity Details' with a 'General' tab. The form contains the following fields:

- 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
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** none

Buttons for 'Commit' and 'Cancel' are at the top right of the form.

The following screen shows the addition of the *Avaya Experience Portal* SIP Entity:

- The **FQDN or IP Address** field is set to the IP address of the Experience Portal (see **Figure 1**).
- Select the location that applies to the SIP Entity being created, defined in **Section 7.3**.
- Select the **Time Zone**.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar has a 'Routing' menu with 'SIP Entities' highlighted. The main area is titled 'SIP Entity Details' with a 'General' tab. The form contains the following fields:

- Name:** Avaya Experience Portal
- FQDN or IP Address:** 10.64.101.252
- Type:** Voice Portal
- Notes:** SIP Trunk to Avaya Experience Poi
- Adaptation:** (empty)
- Location:** Lab Others
- Time Zone:** America/Fortaleza
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** none

Buttons for 'Commit' and 'Cancel' are at the top right of the form.

7.6. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Three Entity Links were created; an entity link to Communication Manager for use only by service provider traffic, an entity link to the Avaya SBCE and an entity link to Experience Portal. 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 7.5**).
- **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 7.5**).
- **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.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The left navigation pane shows the 'Entity Links' option selected. The main content area is titled 'Entity Links' and contains a table with one row of configuration data. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The configuration shown is for a link named '*Session_Manager_Ch' connecting to '*Session Manager' using the 'TLS' protocol on port '5071', and to '*Communication Manager Trunk 2' on port '5071' with a 'Trusted' connection policy. The 'Deny New Service' checkbox is unchecked. There are 'Commit' and 'Cancel' buttons at the top and bottom of the configuration area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
*Session_Manager_Ch	*Session Manager	TLS	5071	*Communication Manager Trunk 2	5071	<input type="checkbox"/>	Trusted	<input type="checkbox"/>	

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 8.0 interface. The left sidebar has a menu with 'Entity Links' highlighted. The main area is titled 'Entity Links' and contains a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The row shows a link from '*Session_Manager_AS' to '*Q Session Manager' using 'TLS' on port '5061' to '*Q Avaya SBCE' on port '5061'. The 'Connection Policy' is set to 'trusted'. There are 'Commit' and 'Cancel' buttons at the top and bottom of the table.

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

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

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar has a menu with 'Entity Links' highlighted. The main area is titled 'Entity Links' and contains a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The row shows a link from '*Session Manager Ava' to '*Q Session Manager' using 'TLS' on port '5061' to '*Q Avaya Experience Portal' on port '5061'. The 'Connection Policy' is set to 'trusted'. There are 'Commit' and 'Cancel' buttons at the top and bottom of the table.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
*Session Manager Ava	*Q Session Manager	TLS	5061	*Q Avaya Experience Portal	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

7.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 7.5**. Three routing policies were added; an incoming policy with Communication Manager as the destination, an outbound policy to the Avaya SBCE as the destination, an incoming policy with Experience Portal as the destination. 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 7.5**) 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, the Avaya SBCE and the Experience Portal.

AVAYA Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Routing ×

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

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

Time of Day

Add Remove View Gaps/Overlaps

1 Item

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

Select : All, None

- The following screen illustrates an example dial pattern used to verify inbound PSTN calls to Communication Manager. 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**.

59 of 115
CCMSM80SBC80TLS

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**.

The screenshot shows the 'Dial Pattern Details' page in the Avaya Aura System Manager 8.0 interface. The 'General' tab is active. The 'Pattern' field is set to '1', with 'Min' and 'Max' both set to '11'. The 'SIP Domain' is set to 'avaya.lab.com'. The 'Emergency Call' checkbox is unchecked. Below the 'General' tab, the 'Originating Locations and Routing Policies' table shows one item:

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

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to Experience Portal. In the sample configuration one of the DID numbers provided by CenturyLink was used as a test number to route calls from the PSTN to Experience Portal, arriving from location **Avaya SBCE**, used route policy **To Avaya Experience Portal**. The SIP Domain was set to **avaya.lab.com**.

The screenshot shows the 'Dial Pattern Details' page in the Avaya Aura System Manager 8.0 interface. The 'General' tab is active. The 'Pattern' field is set to '3031235744', with 'Min' set to '10' and 'Max' set to '36'. The 'SIP Domain' is set to 'avaya.lab.com'. The 'Emergency Call' checkbox is unchecked. Below the 'General' tab, the 'Originating Locations and Routing Policies' table shows one item:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Avaya SBCE	VMware Avaya SBCE	To Avaya Experience Portal	0	<input type="checkbox"/>	Avaya Experience Portal	To Avaya Experience Portal

Repeat the above procedures as needed to define additional dial patterns.


8. 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, between Avaya and CenturyLink) are beyond the scope of these Application Notes; hence it's not discussed in detail in this document. Consult reference [8] in the **References** section for additional information on this topic.

8.1. 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.



**Session Border Controller
for Enterprise**

Log In

Username:

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2019 Avaya Inc. All rights reserved.

Once logged in, on the top left of the screen, under **Device:** select the device being managed, *Avaya_SBCE* in the sample configuration.

The screenshot shows the Avaya SBCE dashboard for the 'Device: EMS' configuration. The top navigation bar includes 'Device: EMS', 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar shows the 'EMS Dashboard' with a red box around 'Avaya_SBCE'. The main content area is titled 'Dashboard' and contains several sections: 'Information' (System Time: 08:13:13 AM MDT, Version: 8.0.0.0-19-16991, Build Date: Sat Jan 26 21:58:11 UTC 2019, License State: OK, Aggregate Licensing Overages: 0, Peak Licensing Overage Count: 0, Last Logged in at: 04/01/2019 08:11:58 MDT, Failed Login Attempts: 0), 'Installed Devices' (EMS, Avaya_SBCE), 'Active Alarms (past 24 hours)' (None found), and 'Incidents (past 24 hours)' (None found).

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.

The screenshot shows the Avaya SBCE dashboard for the 'Device: Avaya_SBCE' configuration. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar shows the 'EMS Dashboard' with a red box around 'Avaya_SBCE'. The main content area is titled 'Dashboard' and contains several sections: 'Information' (System Time: 04:06:22 PM MDT, Version: 8.0.0.0-19-16991, Build Date: Sat Jan 26 21:58:11 UTC 2019, License State: OK, Aggregate Licensing Overages: 0, Peak Licensing Overage Count: 0, Last Logged in at: 03/28/2019 15:55:54 MDT, Failed Login Attempts: 0), 'Installed Devices' (EMS, Avaya_SBCE), 'Active Alarms (past 24 hours)' (None found), and 'Incidents (past 24 hours)' (Avaya_SBCE: No Subscriber Flow Matched).

8.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the 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 displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: Avaya_SBCE, Alarms (1), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo. The left sidebar lists various management options, with "Device Management" highlighted. The main content area, titled "Device Management", contains tabs for Devices, Updates, SSL VPN, Licensing, and Key Bundles. The "Devices" tab is active, showing a table of managed devices. The table has columns for Device Name, Management IP, Version, and Status. A single device, "Avaya_SBCE", is listed with a blurred management IP, version "8.0.0.0-19-16991", and status "Commissioned". To the right of the table, there are action buttons: Reboot, Shutdown, Restart Application, View (highlighted with a red box), Edit, and Uninstall.

Device Name	Management IP	Version	Status
Avaya_SBCE	[Blurred]	8.0.0.0-19-16991	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

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
Requested: 2000 2000
Advanced Sessions
Requested: 2000 2000
Scopia Video Sessions
Requested: 500 500
CES Sessions
Requested: 0 0
Transcoding Sessions
Requested: 0 0
CLID ---
Encryption
Available: Yes ☒

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 shown above 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.

8.3. TLS Management

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

It is assumed that generation and installation of certificates and the creation of TLS Profiles on the Avaya SBCE have been previously completed, as it's not discussed in this document. Refer to item [8] in **Section 12**.

8.4. 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 the **Network & Flows** on the left-side menu. 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.

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

Session Border Controller for Enterprise

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Network & Flows
Network Management
Media Interface
Signaling Interface

Network Management

Interfaces
Networks

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.

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

Session Border Controller for Enterprise

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Network & Flows
Network Management
Media Interface
Signaling Interface

Network Management

Interfaces
Networks

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

8.5. 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 **Network & Flows** menu on the left-hand side, 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**.

The screenshot shows the 'Add Media Interface' dialog box with the following fields:

- Name:** Private_med
- IP Address:** Network_A1 (A1, VLAN 0) (selected from a dropdown menu)
- IP Address:** 10.64.101.243 (selected from a dropdown menu)
- Port Range:** 35000 - 40000
- Finish:** A button at the bottom right.

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

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 the 'Add Media Interface' dialog box with the following fields:

- Name:** Public_med
- IP Address:** Network_B1 (B1, VLAN 0) (selected from a dropdown menu)
- IP Address:** 10.10.80.51 (selected from a dropdown menu)
- Port Range:** 35000 - 40000
- Finish:** A button at the bottom right.

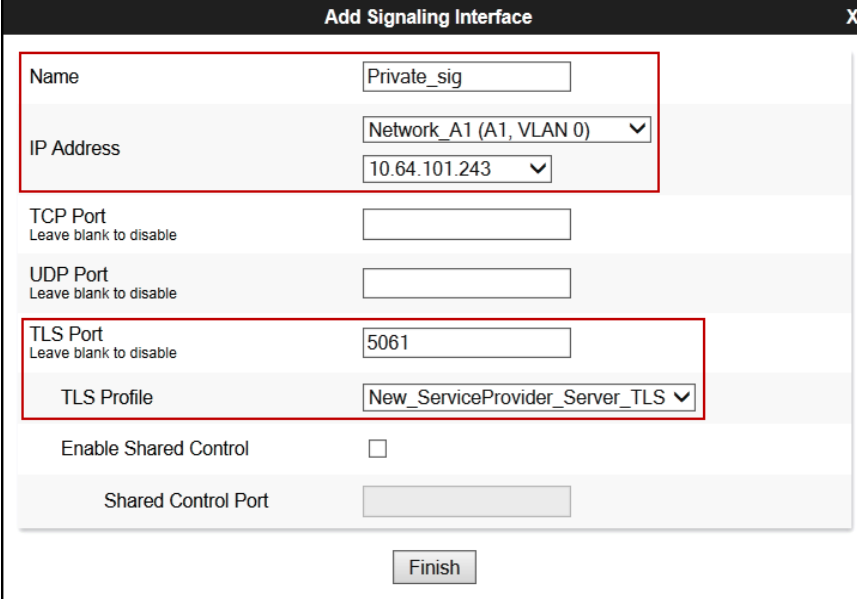
A red rectangular box highlights the Name, IP Address dropdowns, and Port Range fields.

8.6. 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 **Network & Flows** menu on the left-hand side, 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 7.6**.
- Select a **TLS Profile**.
- Click **Finish**.



The screenshot shows the 'Add Signaling Interface' window with the following fields and values:

Field	Value
Name	Private_sig
IP Address	Network_A1 (A1, VLAN 0) / 10.64.101.243
TCP Port	
UDP Port	
TLS Port	5061
TLS Profile	New_ServiceProvider_Server_TLS
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

A 'Finish' button is located at the bottom right of the window.

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 in the sample configuration.
- Select a **TLS Profile**.
- Click **Finish**.

Add Signaling Interface X

Name	Public_sig
IP Address	Network_B1 (B1, VLAN 0) 50.207.80.51
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	5061
TLS Profile	CenturyLink_Server
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

8.7. 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).

8.7.1. 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 left navigation pane includes sections like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), and PPM Services. Under Global Profiles, 'Server Interworking' is highlighted. The main content area is titled 'Interworking Profiles: avaya-ru' and features a list of profiles including 'cs2100', 'avaya-ru' (highlighted), 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd...', 'Avaya-SM', 'SP-General', 'Avaya-IPO', 'Avaya-CS1000', and 'Avaya-CM'. A 'Clone' button is visible. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below this, tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced' are shown. The 'General' tab is active, displaying a table of settings:

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

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

The 'Clone Profile' dialog box is shown with the following fields:

- Profile Name: avaya-ru
- Clone Name: Avaya-SM (highlighted with a red box)
- Buttons: Finish

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**.

The screenshot shows a dialog box titled "Editing Profile: Avaya-SM" with a close button (X) in the top right corner. The "General" tab is selected. The following options are visible:

- Hold Support:** Radio buttons for ☒ None, ☐ RFC2543 - c=0.0.0.0, and ☐ RFC3264 - a=sendonly.
- 180 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 181 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 182 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 183 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- Refer Handling:** ☐
- URI Group:** A dropdown menu showing "None".
- Send Hold:** ☐
- Delayed Offer:** ☒
- 3xx Handling:** ☐
- Diversion Header Support:** ☐
- Delayed SDP Handling:** ☐
- Re-Invite Handling:** ☐
- Prack Handling:** ☐
- Allow 18X SDP:** ☐
- T.38 Support:** ☒ (This row is highlighted with a red border in the original image).
- URI Scheme:** Radio buttons for ☒ SIP, ☐ TEL, and ☐ ANY.
- Via Header Format:** Radio buttons for ☒ RFC3261 and ☐ RFC2543.

A "Finish" button is located at the bottom center of the dialog box.

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 (3), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left sidebar lists various configuration categories, with 'Global Profiles' expanded to show 'Server' and 'Interworking' (highlighted with a red box). The 'Interworking Profiles' list on the right includes several profiles, with 'Avaya-SM' highlighted (also with a red box). The main content area is titled 'Interworking Profiles: Avaya-SM' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a description field. A tabbed interface at the top of the settings area includes 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced' (highlighted with a red box). The 'Advanced' tab contains a table of settings:

Setting	Value
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

Below the table is a 'DTMF' section with a 'DTMF Support' setting set to 'None' and an 'Edit' button.

8.7.2. 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**.

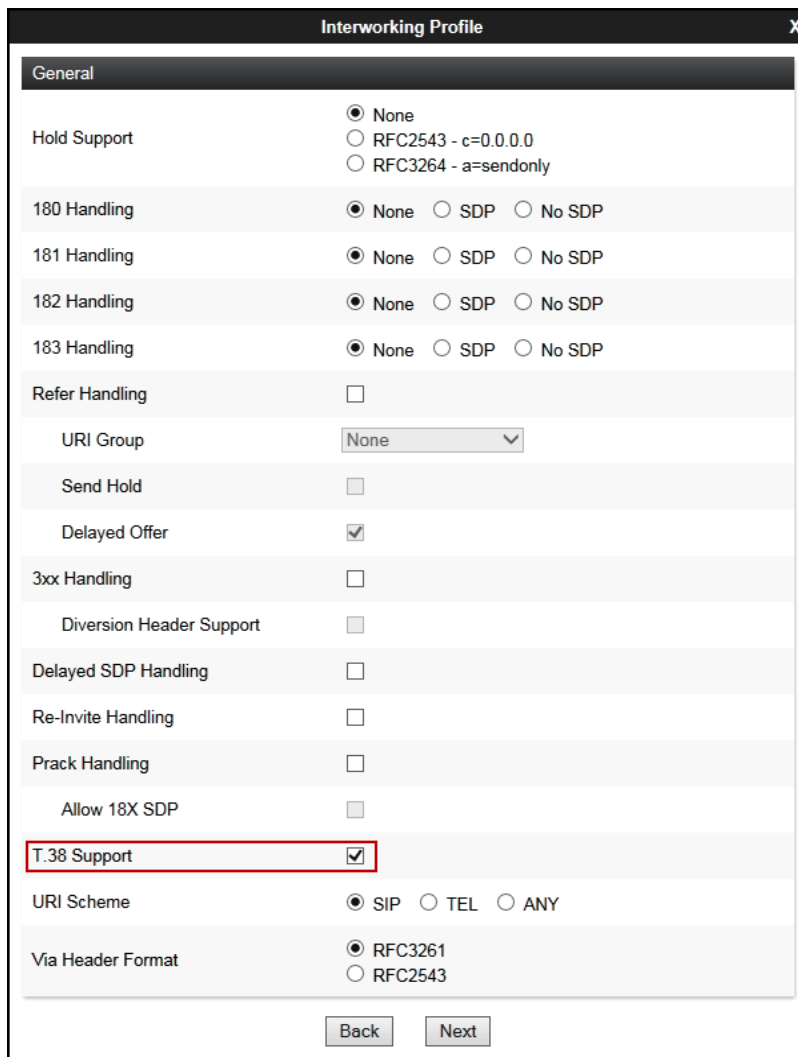


Interworking Profile

Profile Name SP-General x

Next

- On the General tab, check **T.38 Support**.
- Click **Next** until the **Advanced** 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 None 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 **Advanced** tab select **Lync** under the **Extensions** pull down menu (refer to **Section 2.2**), then click **Finish**.

Interworking Profile

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

8.8. 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 reference [8] in the **References** section for more information on this topic.

A single Sigma script was 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, 3031235746, this information is provided by CenturyLink.
- Remove unused headers to comply with CenturyLink 1500 bytes max SIP packet size limitation.
- Remove unwanted xml element information from the SDP in SIP messages sent to CenturyLink.
- Remove the unused gsid and epv parameters from the Contact header.
- Correct one-way audio issue on outbound calls from Avaya one-X Communicator (SIP mode) to the PSTN.
- Correct an issue with the Avaya SBCE not including "Content-Type: application/sdp" header in 200 OK messages it sends to the Service Provider when the "Lync" extension is assigned to the Service Provider Server Interworking profile.

The scripts will later be applied to the Server Configuration profiles corresponding to the Service Provider (toward CenturyLink) in **Section 8.9.2**.

To create the SigMa script on the left navigation pane, select **Configuration Profiles** → **Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

- For **Title** enter a name, the name *CenturyLink SP Side* was chosen in this example.
- Copy and paste the entire script shown below or from **Appendix A**.
- Click **Save**.

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

```
//For Call Forward and Mobile features CenturyLink requires the pilot number in the PAI.  
within session "All"  
{
```

```

    act on request where %DIRECTION="OUTBOUND" and
    %ENTRY_POINT="POST_ROUTING"
    {

        if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("3031235746")) then
        {
            %var="this does nothing, match for DID number passed";
        }
        else
        {
            %HEADERS["P-Asserted-Identity"][1].URI.USER = "3031235746";
        }
    }
}

```

//Removes unused headers to comply with CenturyLink 1500 bytes max packet size limitation.
within session "ALL"

```

{
    act on message where %DIRECTION="OUTBOUND" and
    %ENTRY_POINT="POST_ROUTING"
    {

```

```

        remove(%HEADERS["User-Agent"][1]);
        remove(%HEADERS["Accept-Language"][1]);
        remove(%HEADERS["Min-SE"][1]);
        remove(%HEADERS["P-Location"][1]);
        remove(%HEADERS["Av-Global-Session-ID"][1]);
        remove(%HEADERS["Reason"][1]);
        remove(%HEADERS["Session-Expires"][1]);
        remove(%HEADERS["P-Conference"][1]);

```

```

//Remove gsid and epv parameters from Contact header.
        remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
        remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);

```

//Remove unwanted xml element information from the SDP in SIP messages sent to CenturyLink.

```

        remove(%BODY[1]);
    }
}

```

//Corrects 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 the 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");
    }
}

//Corrects an issue with the Avaya SBCE not including "Content-Type: application/sdp" header
//in 200 OK SIP messages it sends to the Service Provider when the "Lync" extension is assigned
to
//the Service Provider Server Interworking profile.
within session "INVITE"
{

    act on response where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING" and %RESP_CODE="200"
    {
        print "SigmaStart";
        if(exists(%SDP[1])) then
        {
            if(!exists(%HEADERS["Content-Type"][1])) then
            {
                %HEADERS["Content-Type"][1]="application/sdp";
            }

        }
        print "SigmaEnd";
    }
}

```

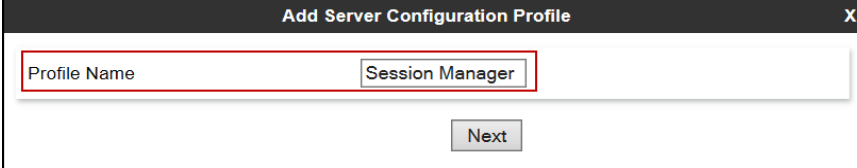
8.9. Server Configuration

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).

8.9.1. Server Configuration Profile – Enterprise

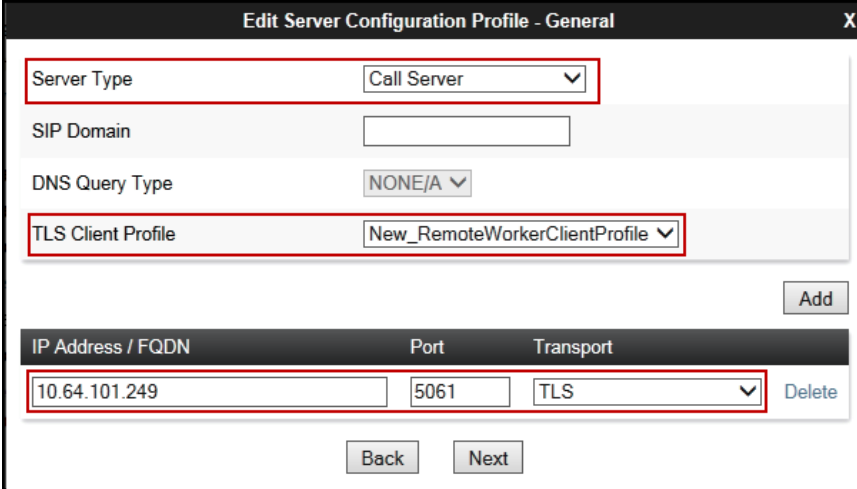
From the **Services** menu on the left-hand navigation pane, select **SIP Servers** and click the **Add** button (not shown) to add a new profile for the Call Server.

- 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 SIP Server Profile – General** tab select **Call Server** from the drop-down menu under the **Server Type**.
- On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 7.5**).
- 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 7.6**.
- Select a **TLS 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 dialog contains several fields and a table:

- Server Type**: A dropdown menu set to "Call Server".
- SIP Domain**: An empty text input field.
- DNS Query Type**: A dropdown menu set to "NONE/A".
- TLS Client Profile**: A dropdown menu set to "New_RemoteWorkerClientProfile".
- Add**: A button to the right of the TLS Client Profile dropdown.
- Table**: A table with three columns: "IP Address / FQDN", "Port", and "Transport".

IP Address / FQDN	Port	Transport
10.64.101.249	5061	TLS
- Delete**: A button to the right of the table.
- Back** and **Next**: Buttons 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 check **Enable Grooming**, select **Avaya-SM** from the **Interworking Profile** drop-down menu (Section 8.7.1).
- Click **Finish**.

Add SIP Server Profile - Advanced

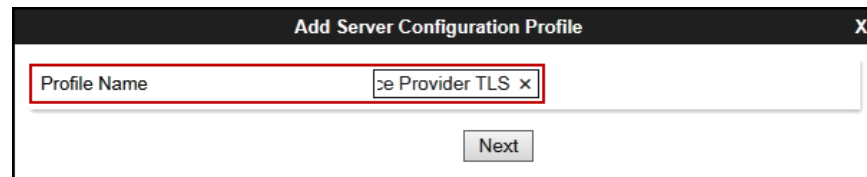
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-SM ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>
URI Group	None ▼

Back Finish

8.9.2. Server Configuration Profile – Service Provider

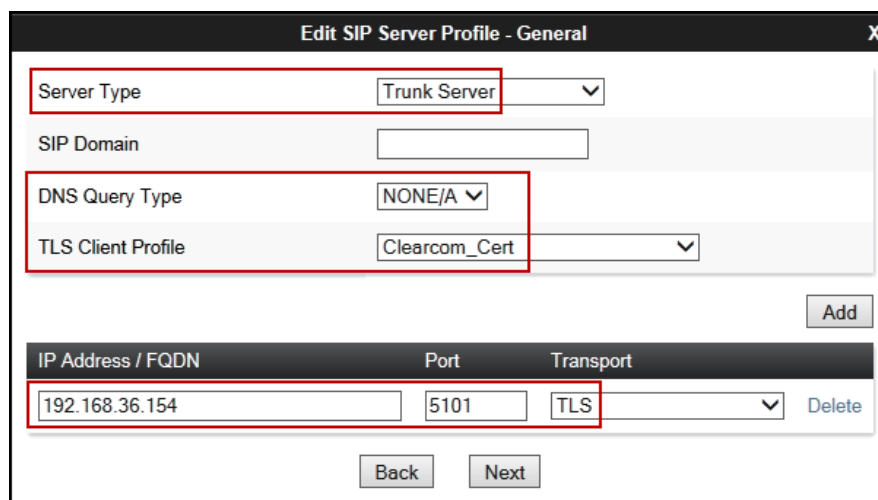
Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

- 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" which contains the text "ce Provider TLS" followed by a small 'x' icon. Below this 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, *192.168.36.154* (the IP address of CenturyLink's 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 Profile**.
- Click **Next**.



The screenshot shows a dialog box titled "Edit SIP Server Profile - General". It has a close button (X) in the top right corner. The main area contains several fields: "Server Type" (dropdown menu showing "Trunk Server"), "SIP Domain" (text input field), "DNS Query Type" (dropdown menu showing "NONE/A"), and "TLS Client Profile" (dropdown menu showing "Clearcom_Cert"). Below these fields is an "Add" button. At the bottom, there is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The first row of the table contains the values "192.168.36.154", "5101", and "TLS". To the right of the table is a "Delete" button. Below the table 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 SIP Server Profile - Authentication". Inside, there is a red rectangular box highlighting the authentication configuration fields. These fields include a checked "Enable Authentication" checkbox, a "User Name" field containing "user123", a "Realm" field with the instruction "(Leave blank to detect from server challenge)", a "Password" field with masked characters, and a "Confirm Password" field also with masked characters. Below the highlighted area, there are "Back" and "Next" buttons.

Click **Next** on the **Add Server Configuration Profile - Heartbeat** window (not shown).

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

- Check the **Register with ALL Servers** box.
- On **Refresh Interval** 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 CenturyLink, **60** 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 (3031235746) and CenturyLink's SIP Proxy IP address (192.168.36.154), as shown on the screen below. This information is provided by CenturyLink.
 - **To URI:** Use the pilot number (3031235746) and CenturyLink's SIP Proxy IP address (192.168.36.154), as shown on the screen below. This information is provided by CenturyLink.
- Click **Next** until the **Add Server Configuration Profile - Advanced** window is reached.

Add SIP Server Profile - Registration	
Register with All Servers	<input checked="" type="checkbox"/>
Register with Priority Server	<input type="checkbox"/>
Refresh Interval	60 seconds
From URI	.5746@192.168.36.154
To URI	3031235746@192.168.36.154
<div>Back Next</div>	

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

- Verify **Enable Grooming** is checked (enabled by default).
- Select **SP-General** from the **Interworking Profile** drop-down menu (Section 8.7.2).
- Select the **CenturyLink SP Side** from the **Signaling Manipulation Script** drop down menu (Sections 8.8 and Section 13).
- Click **Finish**.

Add SIP Server Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile SP-General ▼

Signaling Manipulation Script CenturyLink SP Side ▼

Securable ☐

Enable FGDN ☐

TCP Failover Port 5060

TLS Failover Port 5061

Tolerant ☐

URI Group None ▼

Back Finish

8.10.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.

8.10.1. Routing Profile – Enterprise

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

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

Routing Profile

Profile Name Route_to_SM

Next

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **SIP Server Profile**, 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 8.9.1**.
- Defaults were used for all other parameters.
- Click **Finish**.

Routing Profile

URI Group: Time of Day:

Load Balancing: NAPTR: ☐

Transport: LDAP Routing: ☐

LDAP Server Profile: LDAP Base DN (Search):

Matched Attribute Priority: ☒ Alternate Routing: ☒

Next Hop Priority: ☒ Next Hop In-Dialog: ☐

Ignore Route Header: ☐

ENUM: ☐ ENUM Suffix:

Add

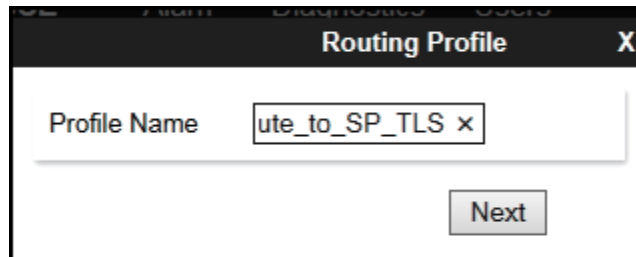
Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Session Manager	10.64.101.249:5061 (TLS)	None	Delete

Back **Finish**

8.10.2. 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**.

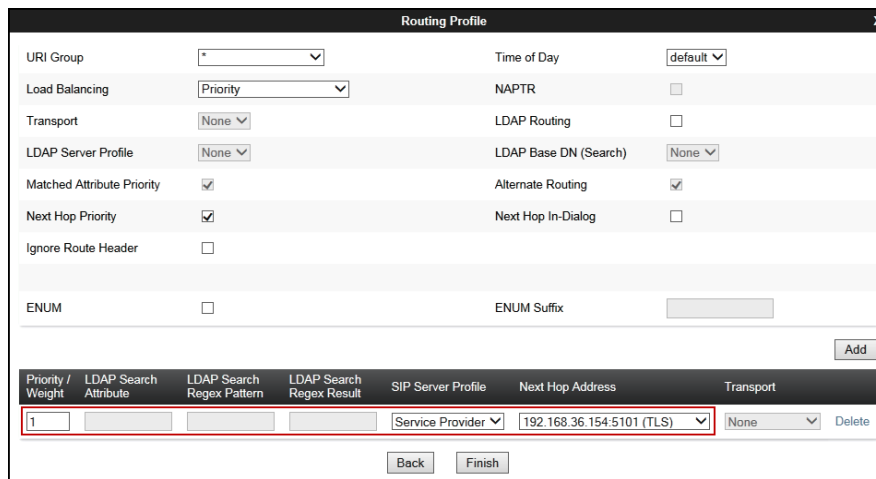


Routing Profile

Profile Name

Next

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter *1*.
- Under **SIP Server Profile**, select *Service Provider TLS*.
- The **Next Hop Address** is populated automatically with *192.168.36.154:5101 (TLS)* CenturyLink's SIP Proxy IP address, Port and Transport, Server Configuration Profile defined in **Section 8.9.2**.
- Click **Finish**.



Routing Profile

URI Group Time of Day

Load Balancing NAPTR ☐

Transport LDAP Routing ☐

LDAP Server Profile LDAP Base DN (Search)

Matched Attribute Priority ☒ Alternate Routing ☒

Next Hop Priority ☒ Next Hop In-Dialog ☐

Ignore Route Header ☐

ENUM ☐ ENUM Suffix

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Service Provider	192.168.36.154:5101 (TLS)	None	Delete

Back Finish

8.11.Topology Hiding

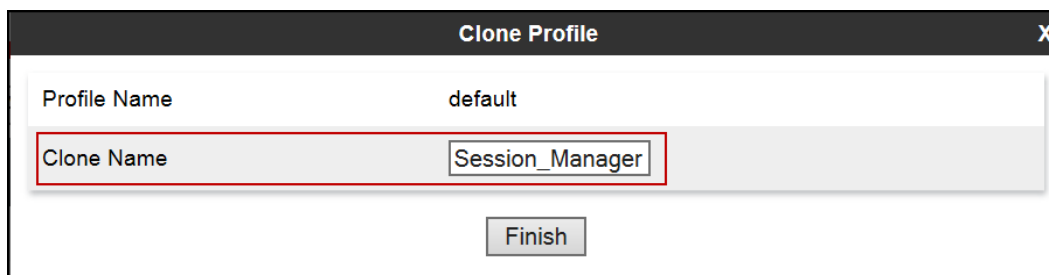
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

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.

8.11.1. 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 with a dark header bar containing the title 'Clone Profile' and a close button 'X'. The main area is white and contains two input fields. The first field, labeled 'Profile Name', has the value 'default'. The second field, labeled 'Clone Name', is highlighted with a red rectangular border and contains the text 'Session_Manager'. Below these 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 7.2**.
- 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 first three rows are highlighted with a red border: "To", "Request-Line", and "From". In these rows, the "Criteria" is "IP/Domain", the "Replace Action" is "Overwrite", and the "Overwrite Value" is "avaya.lab.com". Each row has a "Delete" button to its right. The remaining five rows ("Record-Route", "Referred-By", "SDP", "Via", and "Refer-To") have "Auto" as the "Replace Action" and an empty "Overwrite Value" field. At the bottom of the window is a "Finish" button.

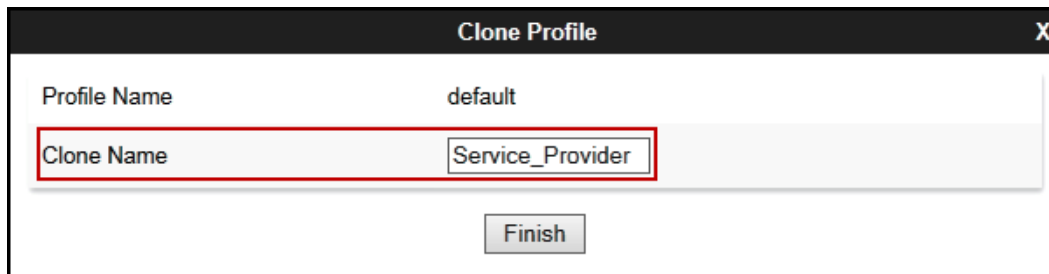
Header	Criteria	Replace Action	Overwrite Value	
To	IP/Domain	Overwrite	avaya.lab.com	Delete
Record-Route	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	avaya.lab.com	Delete
From	IP/Domain	Overwrite	avaya.lab.com	Delete
Referred-By	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
Via	IP/Domain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

Finish

8.11.2. 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**.



Clone Profile

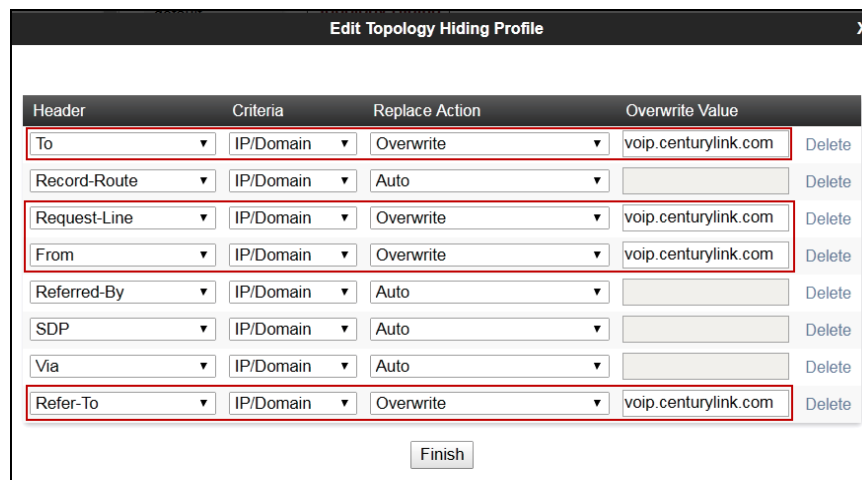
Profile Name: default

Clone Name: Service_Provider

Finish

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**.



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

Finish

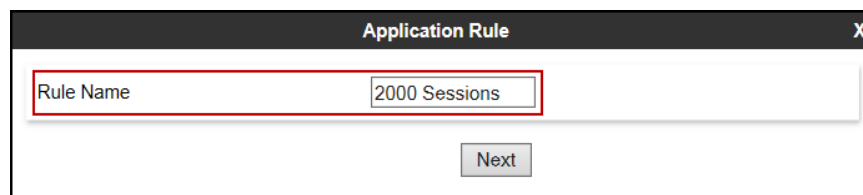
8.12.Domain Policies

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.

8.12.1.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 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**.

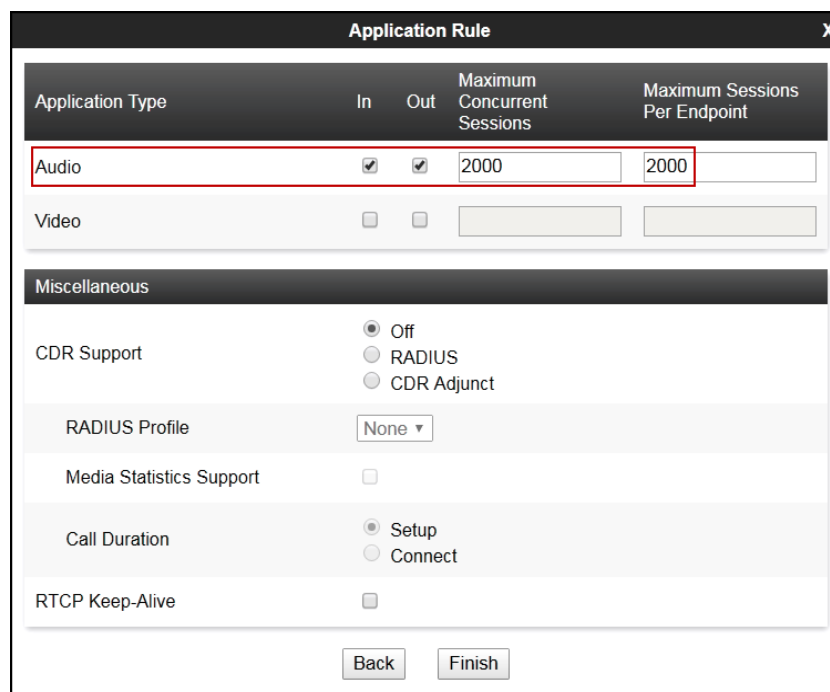


Application Rule

Rule Name: 2000 Sessions

Next

- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **2000** for Audio. Repeat for video if needed.
- Click **Finish**.



Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support: ☒ Off ☐ RADIUS ☐ CDR Adjunct

RADIUS Profile: None

Media Statistics Support: ☐

Call Duration: ☒ Setup ☐ Connect

RTCP Keep-Alive: ☐

Back Finish

8.12.2. 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, one media rule (shown below) was created toward Session Manager and a default media rule was used 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, if needed
- Under Miscellaneous verify that **Capability Negotiation** is checked.
- Click **Next**.

The screenshot shows the 'Media Rule' configuration window. It is divided into three main sections: Audio Encryption, Video Encryption, and Miscellaneous. In the Audio Encryption section, 'Preferred Format #1' is set to 'SRTP_AES_CM_128_HMAC_SHA1_80', 'Preferred Format #2' is set to 'RTP', 'Preferred Format #3' is set to 'NONE', 'Encrypted RTCP' is unchecked, 'MKI' is unchecked, 'Lifetime' is set to '2^4', and 'Interworking' is checked. The Video Encryption section has identical settings. In the Miscellaneous section, 'Capability Negotiation' is checked. At the bottom, there are 'Back' and 'Next' buttons.

- 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, if needed.
- Under Miscellaneous verify that *Capability Negotiation* is checked.
- Click **Next**.

The screenshot shows the 'Media Rule' configuration window. It is divided into three main sections: Audio Encryption, Video Encryption, and Miscellaneous. In the Audio Encryption section, 'Preferred Format #1' is set to 'SRTP_AES_CM_128_HMAC_SHA1_80', 'Preferred Format #2' is set to 'SRTP_AES_CM_128_HMAC_SHA1_32', 'Preferred Format #3' is set to 'NONE', 'Encrypted RTCP' is unchecked, and 'Interworking' is checked. The Video Encryption section has identical settings. In the Miscellaneous section, 'Capability Negotiation' is checked. At the bottom, there are 'Back' and 'Next' buttons.

Section	Setting	Value
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	<input type="checkbox"/>
	MKI	<input type="checkbox"/>
	Lifetime	2^ <input type="text"/>
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	<input type="checkbox"/>
	MKI	<input type="checkbox"/>
	Lifetime	2^ <input type="text"/>
Miscellaneous	Capability Negotiation	<input checked="" type="checkbox"/>

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

8.12.3. 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 sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Domain Policies. The 'Domain Policies' section is expanded, showing 'Signaling Rules' as the selected option. The main content area is titled 'Signaling Rules: default' and features a list of rules on the left, with 'default' selected. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' The 'default' rule is configured with the following settings:

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		<input checked="" type="checkbox"/>				
Action	Allow		Multipart Action	Allow		
Exception List			Exception List			

An 'Edit' button is located at the bottom right of the configuration area.

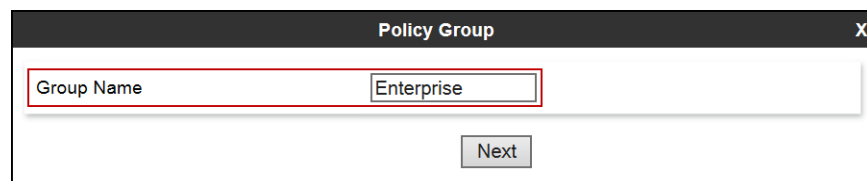
8.13.End Point Policy Groups

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.

8.13.1. 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).

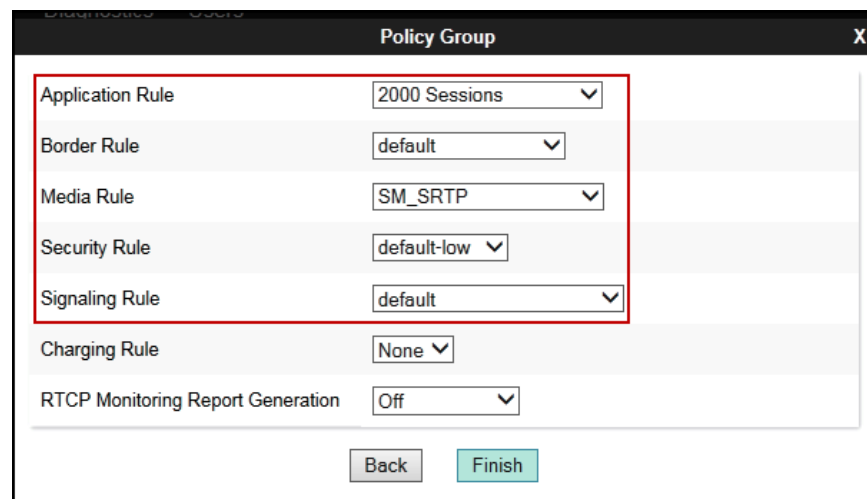
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



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". A red rectangular box highlights this input field. Below the input field, there is a button labeled "Next".

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

- **Application Rule:** *2000 Sessions* (Section 8.12.1).
- **Border Rule:** *default*.
- **Media Rule:** *SM_SRTP* (Section 8.12.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default* (Section 8.12.3).
- Click **Finish**.

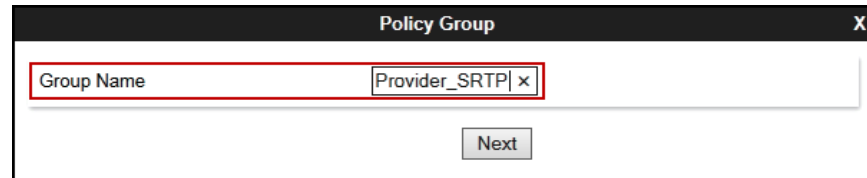


The screenshot shows the "Policy Group" dialog box with several dropdown menus. A red rectangular box highlights the first five rules: Application Rule (2000 Sessions), Border Rule (default), Media Rule (SM_SRTP), Security Rule (default-low), and Signaling Rule (default). Below these, the Charging Rule is set to None and RTCP Monitoring Report Generation is set to Off. At the bottom, there are two buttons: "Back" and "Finish". The "Finish" button is highlighted in blue.

8.13.2. 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).

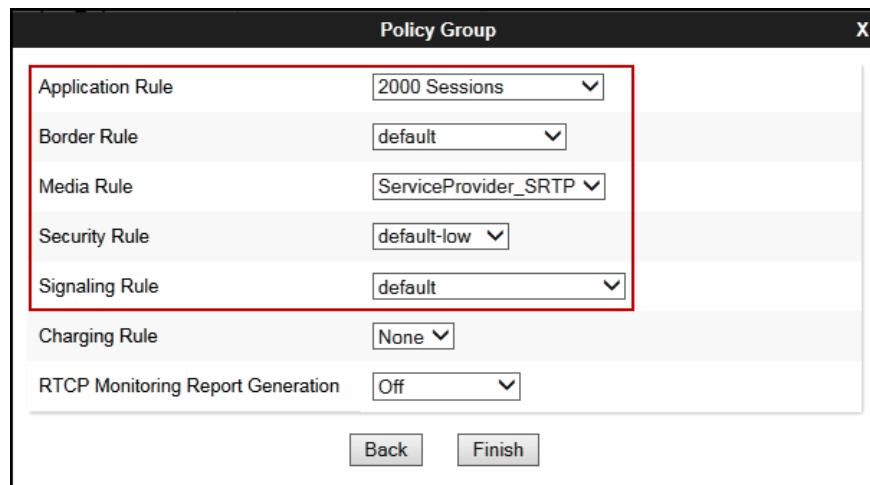
- Enter an appropriate name in the **Group Name** field (*ServiceProvider_SRTP* was used).
- Click **Next**.



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" containing 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:

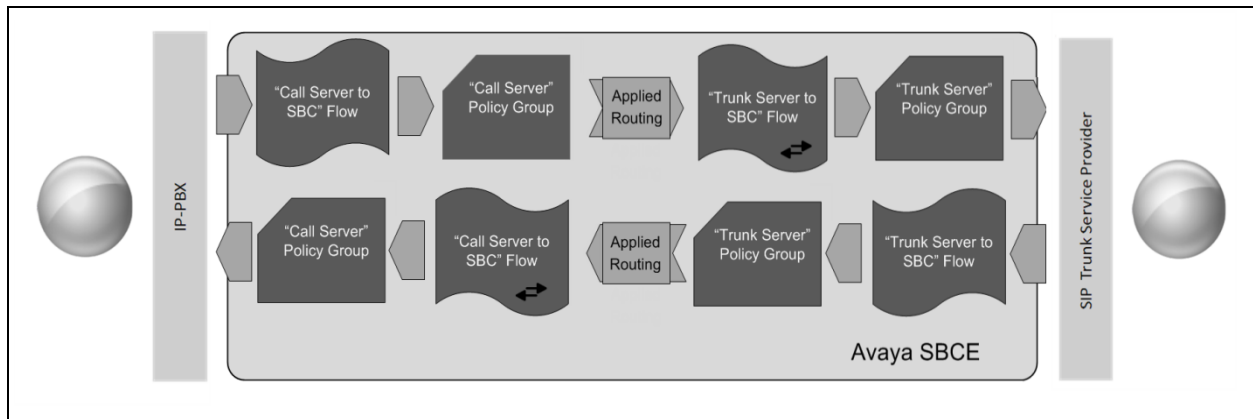
- **Application Rule:** *2000 Sessions* (Section 8.12.1).
- **Border Rule:** *default*.
- **Media Rule:** *ServiceProvider_SRTP* (Section 8.12.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default* (Section 8.12.3).
- Click **Finish**.



The screenshot shows the "Policy Group" dialog box with several configuration options. A red box highlights the first five options: Application Rule (2000 Sessions), Border Rule (default), Media Rule (ServiceProvider_SRTP), Security Rule (default-low), and Signaling Rule (default). Below these are Charging Rule (None) and RTCP Monitoring Report Generation (Off). At the bottom are "Back" and "Finish" buttons.

8.14.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.

8.14.1. 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 8.10.2**, which is the reverse route of the flow. Click **Finish**.

Flow Name	Session_Manager_Flow
SIP Server Profile	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
Link Monitoring from Peer	<input type="checkbox"/>

Finish

8.14.2. 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 8.10.1**, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Click **Finish**.

Flow Name	SIP_Trunk_Flow_TLS
SIP Server Profile	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
Link Monitoring from Peer	<input type="checkbox"/>

Finish

9. 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).
- SIP trunk registration credentials.
- TLS certificate requirements (These requirements are beyond the scope of these Application Notes; hence it's not discussed in this document).
- DID and pilot numbers.
- Supported codecs and order of preference.
- Etc.

10. 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.

10.1.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.

10.2.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.

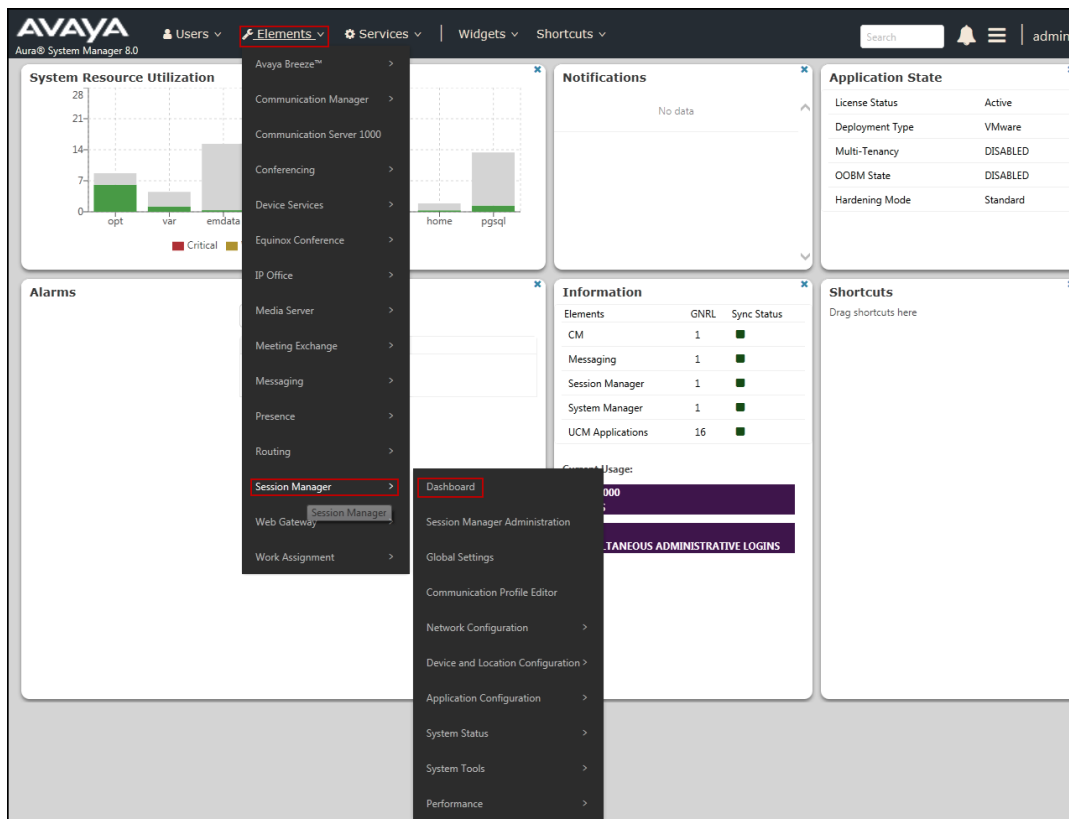
- **status station** <extension number>

Displays signaling and media information for an active call on a specific station.

10.3.Session Manager Verification

The Session Manager configuration may be verified via System Manager.

Step 1 - Using the procedures described in **Section 7**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**, then select **Dashboard**.



Step 2 - The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns all show good status.

In the **Entity Monitoring** column, Session Manager shows that there are **2** alarms out of the **7** Entities defined.

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State: [Dropdown] Shutdown System: [Dropdown] EASG: [Dropdown] As of 1:40 PM

1 Item Show All Filter: Enable

	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Version
<input type="checkbox"/>	Session Manager	Core	0/0/0	Up	Accept New Service	2/7	0	1/1	✓	✓	Normal	Enabled	8.0.1.1.801103	

Select: All, None

Verify that the state of the Session Manager links under the **Conn. Status** and **Link Status** columns are **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.

Status Details for the selected Session Manager:

All Entity Links for Session Manager: Session Manager

Summary View

7 Items Filter: Enable

	SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	Avaya SBCE	IPv4	10.64.101.243	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Avaya Experience Portal	IPv4	10.64.101.252	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Communication Manager Trunk 1	IPv4	10.64.101.241	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	AA-Messaging	IPv4	10.64.101.250	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Communication Manager Trunk 2	IPv4	10.64.101.241	5071	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Communication Manager Trunk 98	IPv4	10.64.101.241	5065	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CS1K7.6	IPv4	172.16.5.60	5085	UDP	FALSE	DOWN	408 Request Timeout	DOWN

Select: None

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.

10.4.Ayaya 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.

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

Session Border Controller for Enterprise

EMS Dashboard

- Device Management
- Backup/Restore
 - System Parameters
 - Configuration Profiles
 - Services
 - Domain Policies
 - TLS Management
 - Network & Flows
 - DMZ Services
 - Monitoring & Logging

Dashboard

Information	
System Time	12:03:08 PM MDT Refresh
Version	8.0.0.0-19-16991
Build Date	Sat Jan 26 21:58:11 UTC 2019
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	03/29/2019 11:24:17 MDT
Failed Login Attempts	0

Installed Devices	
EMS	1
Avaya_SBCE	

Active Alarms (past 24 hours)	
None found.	

Incidents (past 24 hours)	
Avaya_SBCE: No Subscriber Flow Matched	

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

Help

Alarm Viewer

Devices

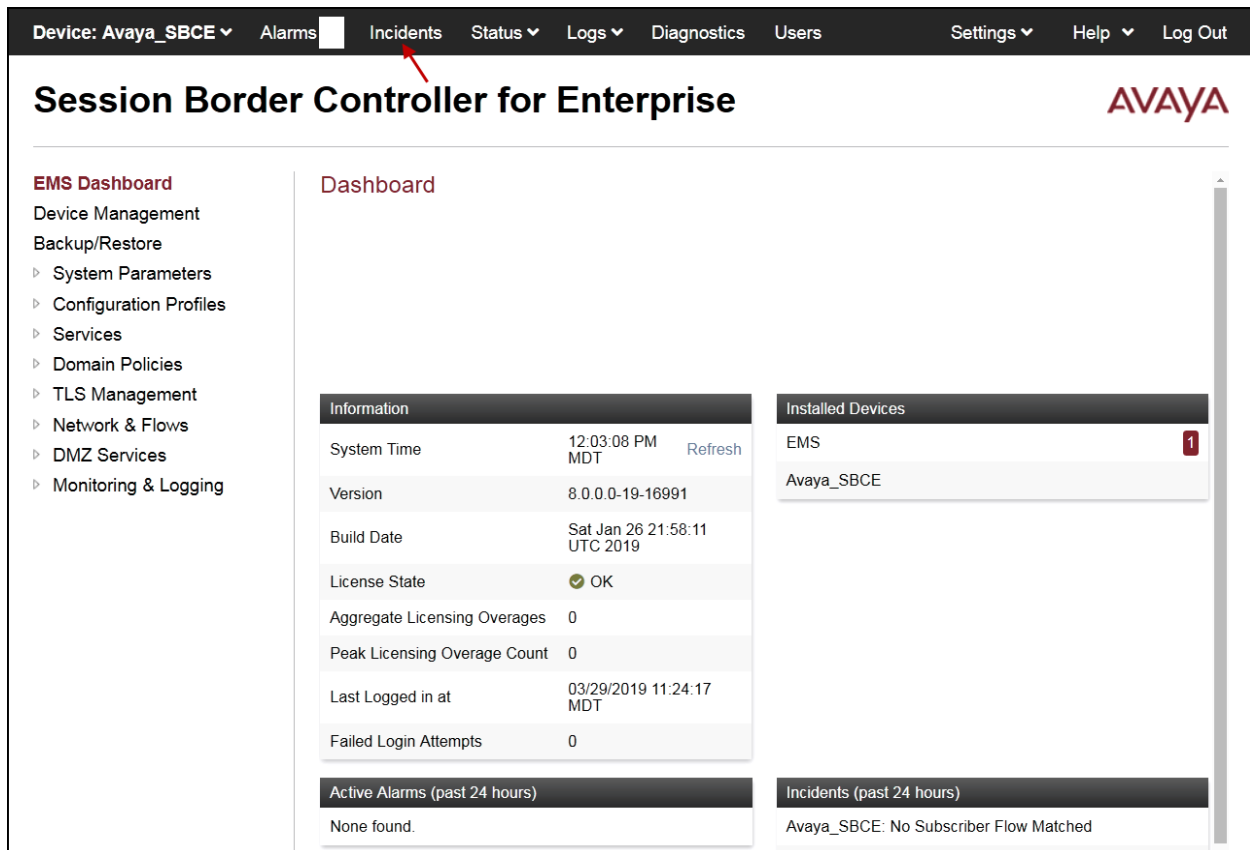
- EMS
- Avaya_SBCE

Alarms

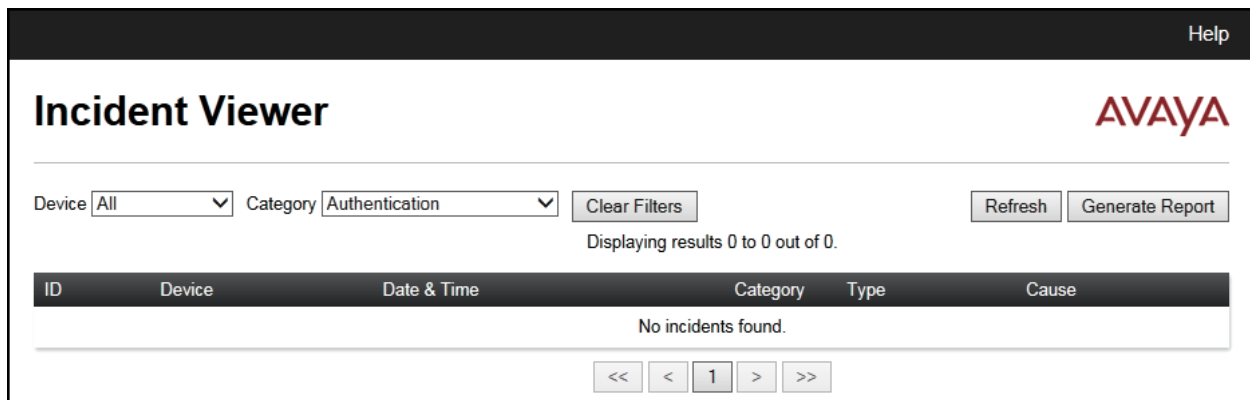
<input checked="" type="checkbox"/>	ID	Details	State	Time	Device
No alarms found for this device.					

Clear Selected Clear All

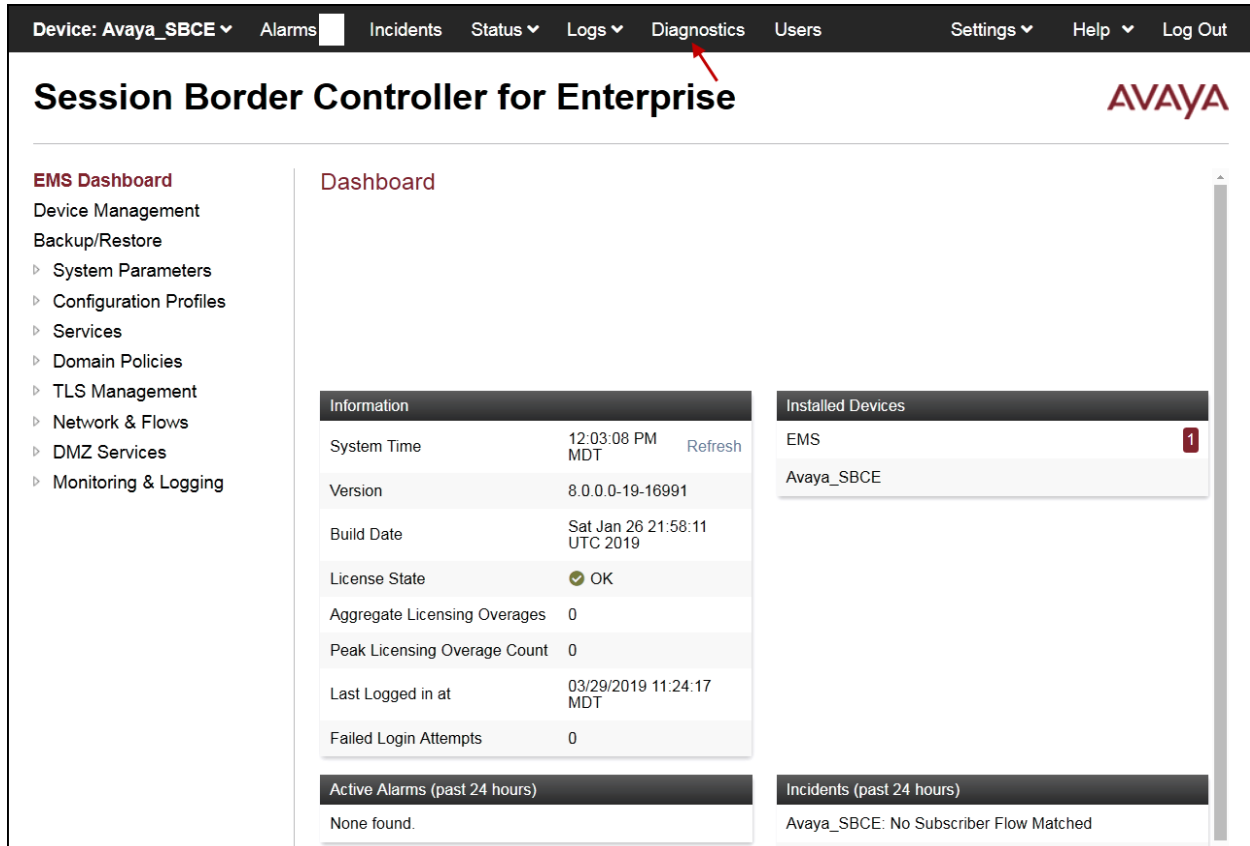
Incidents : Provides detailed reports of anomalies, errors, policies violations, etc.



The following screen shows the Incident Viewer page.

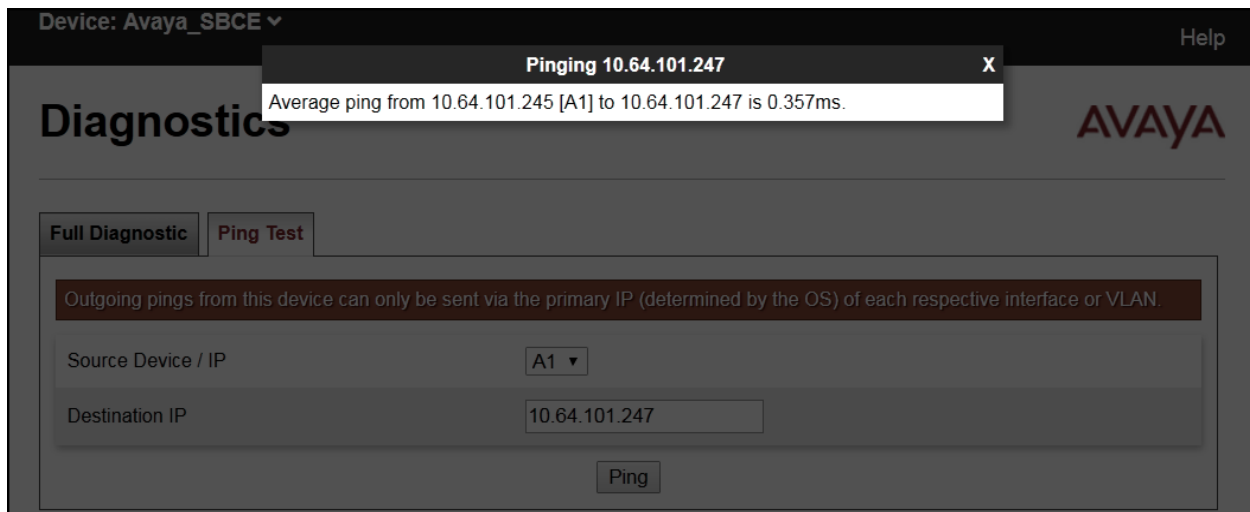


Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.



The screenshot shows the Avaya SBCE Dashboard. The top navigation bar includes links for Device: Avaya_SBCE, Alarms, Incidents, Status, Logs, Diagnostics (highlighted with a red arrow), Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo. The left sidebar lists the EMS Dashboard menu items: Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled "Dashboard" and contains several sections: Information (System Time: 12:03:08 PM MDT, Version: 8.0.0.0-19-16991, Build Date: Sat Jan 26 21:58:11 UTC 2019, License State: OK, Aggregate Licensing Overages: 0, Peak Licensing Overage Count: 0, Last Logged in at: 03/29/2019 11:24:17 MDT, Failed Login Attempts: 0), Installed Devices (EMS, Avaya_SBCE), Active Alarms (past 24 hours: None found), and Incidents (past 24 hours: Avaya_SBCE: No Subscriber Flow Matched).

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



The screenshot shows the Avaya SBCE Diagnostics page. The top navigation bar includes links for Device: Avaya_SBCE, Help, and a Ping Test button. The main header reads "Diagnostics" with the AVAYA logo. The left sidebar lists the Diagnostics menu items: Full Diagnostic and Ping Test. The main content area is titled "Diagnostics" and contains a section for "Ping Test" with a "Ping" button. A tooltip is displayed over the "Ping" button, showing the results of a ping test: "Pinging 10.64.101.247" and "Average ping from 10.64.101.245 [A1] to 10.64.101.247 is 0.357ms." Below the tooltip, there is a form for configuring the ping test. The form includes a "Source Device / IP" dropdown menu set to "A1" and a "Destination IP" text box set to "10.64.101.247". A note states: "Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN."

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 **Monitor & Logging** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

Device: Avaya_SBCE ▾ Alarms 1 Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▾ **Monitoring & Logging**

SNMP

Syslog Management

Debugging

Trace

Log Collection

DoS Learning

CDR Adjunct

Trace: Avaya_SBCE

Packet Capture

Captures

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

Capture Filename
Using the name of an existing capture will overwrite it.

Start Capture

Clear

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 SBCE web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header is 'Session Border Controller for Enterprise' with the AVAYA logo. The left sidebar lists various management options, with 'Monitoring & Logging' selected and 'Trace' highlighted. The main content area is titled 'Trace: Avaya_SBCE' and contains a 'Captures' tab. Below the tab is a table of captured files.

File Name	File Size (bytes)	Last Modified	
Blind_Xfer_20190325155823.pcap	1,859,584	March 25, 2019 3:59:11 PM MDT	Delete

Also, the **traceSBC** tool can be used to monitor the SIP signaling messages between the Service provider and the Avaya SBCE, this tool is helpful when troubleshooting TLS related issues.

11. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0, Avaya Aura® Experience Portal 7.2, and Avaya Session Border Controller for Enterprise 8.0, to connect to the CenturyLink SIP Trunking service on Perimeta/BroadWorks Platform using Transport Layer Security (TLS) and Secure Real-time Transport Protocol (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**.

12. 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 in a Virtualized Environment*, Release 8.0.1, Issue 4, February 2019.
- [2] *Administering Avaya Aura® Communication Manager*, Release 8.0.1, Issue 3, December 2018.
- [3] *Administering Avaya Aura® System Manager* for Release 8.0.1, Issue 7, January 2019.
- [4] *Deploying Avaya Aura® System Manager in a Virtualized Environment*, Release 8.0.1, Issue 4, February 2019.
- [5] *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in a Virtualized Environment*, Release 8.0.1, Issue 4, February 2019.
- [6] *Administering Avaya Aura® Session Manager*, Release 8.0.1, Issue 3, December 2018.
- [7] *Deploying Avaya Session Border Controller in a Virtualized Environment*, Release 8.0, Issue 2, March 2019.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 8.0, Issue 1, February 2019.
- [9] *Administering Avaya Aura® Experience Portal*, Release 7.2.2, Issue 1, March 2019
- [10] *Implementing Avaya Aura® Experience Portal on a single server*, Release 7.2.2, Issue 1, July 2019
- [11] *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*.
- [12] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0, Issue 6, March 2019.
- [13] *Implementing and Administering Avaya Aura® Media Server*. Release 8.0, Issue 3, November 2018.
- [14] *Planning for and Administering Avaya Equinox for Android, iOS, Mac, and Windows*. Release 3.5.5, Issue 1, March 2019.
- [15] *Administering Avaya one-X® Communicator*. Release 6.2, Feature Pack 10, November 2015.
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [17] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

13. Appendix A: SigMa Scripts

Following are the Signaling Manipulation scripts that were used in the configuration of the Avaya SBCE, **Section 8.8**. When adding these scripts as instructed in **Sections 8.9.2** enter a name for the script in the Title (e.g., *CenturyLink SP Side*) and copy/paste the entire scripts shown below.

The following SigMa scripts will:

- 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, 3031235746, this information is provided by CenturyLink.
- Remove unused headers to comply with CenturyLink 1500 bytes max SIP packet size limitation.
- Remove unwanted xml element information from the SDP in SIP messages sent to CenturyLink.
- Remove the unused gsid and epv parameters from the Contact header.
- Correct one-way audio issue on outbound calls from Avaya one-X Communicator (SIP mode) to the PSTN.
- Correct an issue with the Avaya SBCE not including "Content-Type: application/sdp" header in 200 OK messages it sends to the Service Provider when the "Lync" extension is assigned to the Service Provider Server Interworking profile

Note that the Pilot number shown below as “3031235746” will need to be changed with the correct Pilot number provided by CenturyLink.

Title: *CenturyLink SP Side*

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

//For Call Forward and Mobile features CenturyLink requires the pilot number in the PAI within session "All"

```
{
  act on request where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("3031235746")) then
    {
      %var="this does nothing, match for DID number passed";
    }
    else
    {
      %HEADERS["P-Asserted-Identity"][1].URI.USER = "3031235746";
    }
  }
}
```

```

    }
  }
}

```

//Removes unused headers to comply with CenturyLink 1500 bytes max packet size limitation.
within session "ALL"

```

{
  act on message where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {

```

```

    remove(%HEADERS["User-Agent"][1]);
    remove(%HEADERS["Accept-Language"][1]);
    remove(%HEADERS["Min-SE"][1]);
    remove(%HEADERS["P-Location"][1]);
    remove(%HEADERS["Av-Global-Session-ID"][1]);
    remove(%HEADERS["Reason"][1]);
    remove(%HEADERS["Session-Expires"][1]);
    remove(%HEADERS["P-Conference"][1]);

```

//Remove gsid and epv parameters from Contact header.

```

    remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
    remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);

```

//Remove unwanted xml element information from the SDP in SIP messages sent to CenturyLink.

```

    remove(%BODY[1]);
  }
}

```

//Corrects 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 the 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");
  }
}

```

```
//Corrects an issue with the Avaya SBCE not including "Content-Type: application/sdp" header
//in 200 OK SIP messages it sends to the Service Provider when the "Lync" extension is assigned
to
//the Service Provider Server Interworking profile.
within session "INVITE"
{

    act on response where %DIRECTION="OUTBOUND" and
    %ENTRY_POINT="POST_ROUTING" and %RESP_CODE="200"
    {
        print "SigmaStart";
        if(exists(%SDP[1])) then
        {
            if(!exists(%HEADERS["Content-Type"][1])) then
            {
                %HEADERS["Content-Type"][1]="application/sdp";
            }

        }
        print "SigmaEnd";
    }
}
```

14. Appendix A – Avaya Session Border Controller for Enterprise – Refer Handling

One of the capabilities important to the Experience Portal environment is the Avaya SBCE Refer Handling option. Experience Portal inbound call processing may include call redirection to Communication Manager agents, or other CPE destinations. This redirection is accomplished by having Experience Portal send SIP REFER messaging to the Avaya SBCE. Enabling the Refer Handling option causes the Avaya SBCE to intercept and process the REFER and generate a new SIP INVITE messages back to the CPE (e.g., Communication Manager).

As an additional option, the Refer Handling feature can also specify *URI Group* criteria as a discriminator, whereby SIP REFER messages matching the URI Group criteria are processed by the Avaya SBCE, while SIP REFER messages that do not match the URI Group criteria, are passed through to the Service Provider.

Create a URI Group for numbers intended for Communication Manager.

Step 1 - Select **Configuration Profiles → URI Groups** from the left-hand menu.

Step 2 - Select **Add** and enter a descriptive **Group Name**, e.g., **internal-extension**, and select **Next** (not shown).

Step 3 - Enter the following:

- **Scheme:** **sip:/sips:**
- **Type:** **Regular Expression**
- **URI:** **3[0-9]{3}@.*** This will match 4-digit local extensions starting with 3, e.g., 3041 or 3042.
- Select **Finish**.

The screenshot shows a 'URI Group' configuration window. At the top, it states 'Each entry should match a valid SIP URI.' and includes a 'WARNING' about invalid regular expressions. Below this, a 'Note' says 'This regular expression is case-insensitive.' and an example is provided: 'Ex: [0-9]{3,5}\.user@domain\.com, (simple|advanced)\.user[A-Z]{3}@.*'. The configuration fields are: 'Scheme' with radio buttons for 'sip:/sips:' (selected) and 'tel:'; 'Type' with radio buttons for 'Plain', 'Dial Plan', and 'Regular Expression' (selected); and 'URI' with a text box containing '3[0-9]{3}@.*'. At the bottom are 'Back' and 'Finish' buttons.

Step 4 - For additional entries, select **Add** on the right-hand side of the URI Group tab and repeat **Step 3**.

Device: Avaya_SBCE ▾Alarms 1IncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardDevice ManagementBackup/Restore▸ System Parameters▸ Configuration ProfilesDomain DoSServer InterworkingMedia ForkingRoutingTopology HidingSignaling ManipulationURI GroupsSNMP TrapsTime of Day RulesFGDN GroupsReverse Proxy Policy▸ Services▸ Domain Policies▸ TLS Management▸ Network & Flows▸ DMZ Services▸ Monitoring & Logging

URI Groups: internal-extensionsAddRenameDelete

URI GroupsEmergencyinternal-extensio...

Click here to add a description.

URI GroupAdd

URI Listing3[0-9]{3}@.*EditDelete

Edit the existing **SP-General** Server Interworking Profile to enable Refer Handling and assign the newly created URI Group (refer to **Section 8.7.2**).

Step 1 - Select **Configuration Profiles → Server Interworking** from the left-hand menu (not shown).

Step 2 - Select the **SP-General** Server Interworking Profile created in **Section 8.7.2** and click **Edit**

- Check **Refer Handling**.
- **URI Group: internal-extensions**
- Select **Finish**.

Editing Profile: SP-General

General

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

Finish

Following is the SP-General Server Interworking profile after editing.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: Avaya_SBCE, Alarms (1), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo.

On the left, a sidebar menu lists various configuration options, with "Configuration Profiles" and "Server Interworking" highlighted. The main content area is titled "Interworking Profiles: SP-General" and features an "Add" button and "Rename", "Clone", and "Delete" buttons. A description field is present with the text "Click here to add a description."

The "General" tab is selected, showing a table of configuration parameters. The "Refer Handling" row is highlighted, showing "Yes" for "Refer Handling" and "internal-extensions" for "URI Group".

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

An "Edit" button is located at the bottom right of the configuration table.

©2019 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.