



DevConnect Program

Application Notes for Configuring Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, Avaya Experience Portal 8.1, Avaya Session Border Controller 8.1 to support WorldNet Telecommunications SIP Trunking Service – 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 8.1, Avaya Aura® Session Manager 8.1, Avaya Aura® Experience Portal 8.1 and Avaya Session Border Controller 8.1 to interoperate with WorldNet Telecommunications SIP Trunking service.

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 WorldNet Telecommunications SIP Trunking service provides customers with PSTN access via a SIP trunk between the enterprise and the WorldNet Telecommunications 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.

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	7
3.	Reference Configuration.....	8
4.	Equipment and Software Validated	11
5.	Configure Avaya Aura® Communication Manager	12
5.1.	Licensing and Capacity	12
5.2.	System Features.....	13
5.3.	IP Node Names.....	15
5.4.	Codecs	16
5.5.	IP Network Regions	18
5.6.	Signaling Group	19
5.7.	Trunk Group	21
5.8.	Calling Party Information.....	25
5.9.	Inbound Routing.....	26
5.10.	Outbound Routing	27
6.	Configure Avaya Aura® Experience Portal	31
6.1.	Background	31
6.2.	Logging in and Licensing.....	32
6.3.	VoIP Connection	34
6.4.	Speech Servers	36
6.5.	Application References	38
6.6.	MPP Servers and VoIP Settings.....	40
6.7.	Configuring RFC2833 Event Value Offered by Experience Portal	44
7.	Configure Avaya Aura® Session Manager	46
7.1.	System Manager Login and Navigation.....	47
7.2.	SIP Domain	49
7.3.	Locations	50
7.4.	Adaptations.....	54
7.4.1.	Adaptation for Avaya Aura® Communication Manager Extensions	54
7.4.2.	Adaptation for Communication Manager header removal	56
7.5.	SIP Entities.....	57
7.6.	Entity Links	62
7.7.	Routing Policies	64
7.8.	Dial Patterns	66
8.	Configure Avaya Session Border Controller	71
8.1.	System Access.....	71
8.2.	Device Management.....	74
8.3.	TLS Management.....	77
8.3.1.	Verify TLS Certificates – Avaya Session Border Controller	77
8.3.2.	Server Profiles.....	79
8.3.3.	Client Profiles	81

8.4.	Network Management	83
8.5.	Media Interfaces	84
8.6.	Signaling Interfaces.....	86
8.7.	Server Interworking.....	88
8.7.1.	Server Interworking Profile – Enterprise	88
8.7.2.	Server Interworking Profile – Service Provider.....	92
8.8.	Signaling Manipulation	95
8.9.	Server Configuration	97
8.9.1.	Server Configuration Profile – Enterprise	97
8.9.2.	Server Configuration Profile – Service Provider	100
8.10.	Routing	104
8.10.1.	Routing Profile – Enterprise.....	104
8.10.2.	Routing Profile – Service Provider	106
8.11.	Topology Hiding.....	107
8.11.1.	Topology Hiding Profile – Enterprise	107
8.11.2.	Topology Hiding Profile – Service Provider.....	109
8.12.	Domain Policies.....	110
8.12.1.	Application Rules	110
8.12.2.	Media Rules.....	112
8.12.3.	Signaling Rules	115
8.13.	End Point Policy Groups	117
8.13.1.	End Point Policy Group – Enterprise	117
8.13.2.	End Point Policy Group – Service Provider.....	118
8.14.	End Point Flows.....	119
8.14.1.	End Point Flow – Worldnet to Enterprise Flow	120
8.14.2.	End Point Flow – Enterprise to Worldnet Flow	121
9.	WorldNet Telecommunications SIP Trunking Service Configuration	122
10.	Verification and Troubleshooting	122
10.1.	General Verification Steps.....	122
10.2.	Communication Manager Verification	122
10.3.	Session Manager Verification	123
10.4.	Avaya SBC Verification	127
11.	Conclusion	134
12.	References.....	134
13.	Appendix A – Avaya Session Border Controller – Refer Handling	135
14.	Appendix B – SigMa Scripts	138

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the WorldNet Telecommunications network and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 8.1 (Communication Manager), Avaya Aura® Session Manager 8.1 (Session Manager), Avaya Experience Portal 8.1 (Experience Portal) and Avaya Session Border Controller 8.1 (Avaya SBC) and various Avaya endpoints, listed in **Section 4**.

The WorldNet Telecommunications SIP Trunking service 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”, “WorldNet Telecommunications” or “WorldNet” 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 DevConnect 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.

For the testing associated with these Application Notes, the interface between Avaya systems and WorldNet utilized UDP/RTP.

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 WorldNet. Incoming PSTN calls were terminated to the following endpoints: Avaya J129 IP Deskphones (SIP), Avaya J179 IP Deskphones (H.323), Avaya 96x1 IP Deskphones (SIP), Avaya 2420 Digital Deskphones, Avaya one-X® Communicator softphone (H.323 and SIP), Avaya Workplace client for Windows (SIP) and analog Deskphones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya Workplace client for Windows (SIP).
- Outgoing calls to the PSTN were originated from the various Avaya endpoints mentioned above. Calls were routed via WorldNet 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.729 and G.711MU.
- 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, Avaya vector digit collection steps).
- Experience Portal use of SIP REFER to redirect inbound calls, via the Avaya SBC, to the appropriate Communication Manager agent extension.
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment.
- Call and two-way talk path establishment between callers and Communication Manager agents following redirection from Experience Portal.
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- EC500 (Extension to Cellular) calls.
- Routing inbound vector call to call center agent queues.
- 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 [8] in the **References** section for additional information on this topic.

The following items were not tested:

- REFER message for call redirection was not tested for reasons noted under **Section 2.2**
- Inbound toll-free calls, outbound Toll-Free calls, 911 calls (emergency), “0” calls (Operator), local directory assistance and international calls were not tested.

2.2. Test Results

Interoperability testing of the WorldNet Telecommunications SIP Trunking Service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the observations/limitations noted below:

- **Call transfer to the PSTN using the SIP REFER method** – Calls from the PSTN to the enterprise that were transferred back out to the PSTN network using the SIP REFER method did not work properly. With SIP REFER enabled in Communication Manager, during call transfers to the PSTN, the SIP REFER message was accepted by WorldNet with a “202 Accepted” and a “SIP Notify” message response, but the trunk resources were not released, as expected. The reason is that the “SIP Notify” message contained “403 Forbidden” response from the far end. For the compliance test the SIP REFER method was left disabled in Communication Manager (**Sections 5.7**). With REFER disabled, blind and attended call transfers to the PSTN are allowed to complete, with the caveat that Communication Manager resources are not released from the call path, two trunk circuits remain seized for the duration of the call.
- **XML information in SIP UPDATES** – During call transfer scenarios to the PSTN, WorldNet responded with "415 Unsupported media type" to SIP UPDATE messages sent by Communication Manager that contained XML information in the SDP. Since this information has no relevance to WorldNet, a Sigma script was used in the Avaya SBC to remove the unwanted XML information from being sent to WorldNet. See **Section 8.8** and **14**.
- **Fax support** – WorldNet doesn’t support T.38 fax, G.711 pass-through is the preferred fax method for WorldNet. G.711 pass-through fax was tested, but it behaved unreliably. Outbound fax calls (Avaya → PSTN) using G.711 pass-through were successful, but inbound fax calls (PSTN → Avaya) failed. The issue related to G.711 pass-through fax failing during the compliance test may be related to the unpredictability of G.711 pass-through techniques, which only works well on networks with very few hops and with limited end-to-end delay.

During the test, it was observed that the audio codec order on calls from the PSTN to the enterprise (inbound calls) contained G.729 as the preferred codec (first in the list), followed by G.711MU (second in the list). For this reason, the codec order configuration

in Communication Manager was matched to the same audio codec order received on calls from WorldNet (inbound calls) (**Section 5.4**). For G.711 pass-through fax to work the codec order needs to have G.711MU as the first codec choice. This can be accomplished by configuring a different Communication Manager ip-codec-set form to use G.711MU codec as the first codec choice and setting Fax Mode to off. The network region of the G450 Media Gateway hosting the fax machine can then be changed from the enterprise region (used for voice calls), to the one that utilized this ip-codec-set.

- **Support of E.164 number format** – The SIP trunk to WorldNet was configured as **public** in Communication Manager. When the **public** format is use, Communication Manager automatically inserts a “+” sign, preceding the numbers in the “From”, “Contact” and “P-Asserted Identity” (PAI) headers. During the test inbound calls from WorldNet to the enterprise contained 10-digit numbers in the headers of INVITE messages (e.g., **7879571234**), for this reason, a SigMa script was added to remove the “+” from headers of SIP messages being sent to WorldNet. It should be noted that WorldNet also supports the E.164 number format (+17879571234). If the E.164 numbering format is preferred during customer deployments Communication Manager can be configured to include the “+1” preceding the numbers in SIP headers, also by removing the SigMa script mentioned above.
- **Avaya Experience Portal** – Call from the PSTN to Experience Portal that are transferred back out to the PSTN via Experience Portal (e.g., choosing option 5) may contain a “+” that is inserted by Avaya Session Manager to the number in the “Refer-To” header of the REFER message, this will result in a “No Route Found” error message generated by Session Manager if the “+” is not included in Session Manager’s Dial Patterns, needed to route calls to WorldNet. To solve this issue a dial patten containing “+” needs to be added to Session Manager (refer to **Section 7.8**).
- **SIP header optimization:** There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider’s network. These headers were removed with the purpose of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider’s network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector and P-Location (**Section 7.4.2**).

2.3. Support

For support of WorldNet Telecommunications SIP Trunking Service visit the corporate Web page at: <https://www.worldnetpr.com/en/voice-service/>

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

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the WorldNet Telecommunications SIP Trunking Service through a public Internet WAN connection.

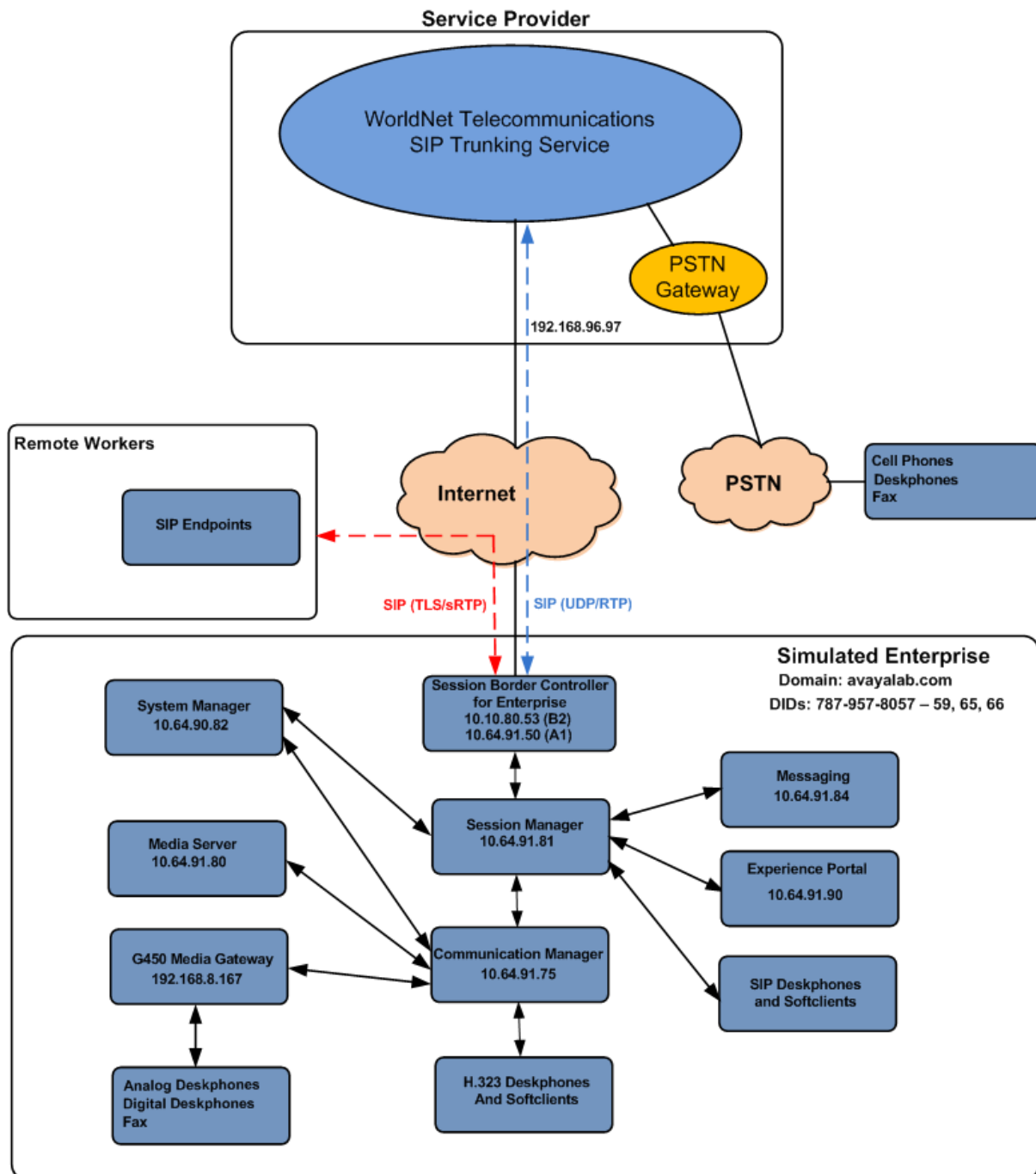


Figure 1: Avaya SIP Enterprise Solution connected to WorldNet Telecommunications SIP Trunking Service

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.
- Avaya Messaging.
- Avaya Media Server.
- Avaya Experience Portal.
- Avaya G450 Media Gateway.
- Avaya 96x1 Series IP Deskphones (SIP).
- Avaya J179 IP Deskphones (H.323).
- Avaya J129 IP Deskphones (SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Workplace Client 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 SBC. 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 Workplace Client for Windows (SIP). 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 [9] in the **References** section for additional information on this topic.

The Avaya SBC 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 SBC, protecting in this way the enterprise against any SIP-based attacks. The Avaya SBC 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 SBC 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 SBC for egress to the WorldNet 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.

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 G450 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 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 Avaya Messaging are not directly related to the interoperability tests with the WorldNet network SIP Trunking service, they are not included in these Application Notes.

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

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	8.1.3.8 (Feature Pack 3 Service Pack 8)
Avaya Aura® System Manager	8.1.3.8 Build No. - 8.1.0.0.733078 Software Update Revision No: 8.1.3.8.1015708 Service Pack 8
Avaya Aura® Session Manager	8.1.3.8 8.1.3.8.813807
Avaya Session Border Controller	8.1.3.2 8.1.3.2-38-22279
Avaya Experience Portal	8.1.2.0.0202
Avaya Aura® Messaging	7.2 Service Pack 3
Avaya Aura® Media Server	8.0.2.163
Avaya G450 Media Gateway	G450_sw_41_38_0
Avaya J129 Series IP Deskphones (SIP)	4.1.1.0.7
Avaya J179 IP Deskphones (H.323)	6.8.5.4.10
Avaya 96x1 Series IP Deskphones (SIP)	Version 7.1.15.2.1
Avaya Workplace Client for Windows (SIP)	3.34.0.118
Avaya one-X® Communicator	6.2.SP14
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
WorldNet Telecommunications	
Metaswitch	CFS: V9.3.20
Oracle SBC	Acme Packet 4600 SCZ8.1.0 GA (Build 33)

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 SBC 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 6.7.0) 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 WorldNet Telecommunications SIP Trunking Service. 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 G450 Media Gateway and the Avaya 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 capture 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 **4000** licenses are available and **130** 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:			4000	0		
Maximum Concurrently Registered IP Stations:			1000	1		
Maximum Administered Remote Office Trunks:			4000	0		
Max Concurrently Registered Remote Office Stations:			1000	0		
Maximum Concurrently Registered IP eCons:			68	0		
Max Concur Reg Unauthenticated H.323 Stations:			100	0		
Maximum Video Capable Stations:			2400	0		
Maximum Video Capable IP Softphones:			1000	4		
Maximum Administered SIP Trunks:			4000	130		
Max Administered Ad-hoc Video Conferencing Ports:			4000	0		
Max Number of DS1 Boards with Echo Cancellation:			80	0		

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? y
    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	
AMS801	10.64.91.80	
IP500v2	10.5.5.180	
IPOSE	10.64.19.170	
SM	10.64.91.81	
SM-IPv6	fd22:305b:b390:14e6::6	
aes	10.10.0.196	
default	0.0.0.0	
procr	10.64.91.75	
procr6	fd22:305b:b390:14e6::5	

(9 of 9 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

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 7 was used for this purpose. Enter the corresponding codec in the **Audio Codec** column of the table. Codecs **G.729** and **G.711MU** were used during the compliance test. Other audio codecs may be supported by WorldNet Telecommunications.

HG; Reviewed: Avaya DevConnect Application Notes 16 of 139
 SPOC 9/26/2023 ©2023 Avaya Inc. All Rights Reserved. WN-CMSMEPSBC-81

On **Page 2**, the **FAX Mode** was set to **off**. WorldNet doesn't support T.38 fax (refer to **Section 2.2**).

change ip-codec-set 7

Page 2 of 2

IP MEDIA PARAMETERS

Allow Direct-IP Multimedia? n

	Mode	Redun- dancy	Packet Size (ms)
FAX	off	0	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

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 7 was chosen for the service provider trunk. Use the **change ip-network-region 7** command to configure region 7 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avayalab.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 7                                     Page 1 of 20
                                                                IP NETWORK REGION
    Region: 7          NR Group: 7
    Location: 1        Authoritative Domain: avayalab.com
    Name: SP Region    Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
    Codec Set: 7       Inter-region IP-IP Direct Audio: yes
    UDP Port Min: 2048                               IP Audio Hairpinning? n
    UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
    Call Control PHB Value: 46
    Audio PHB Value: 46
    Video PHB Value: 26
802.1P/Q PARAMETERS
    Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS      RSVP Enabled? n
    H.323 Link Bounce Recovery? y
    Idle Traffic Interval (sec): 20
    Keep-Alive Interval (sec): 5
    Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region 7 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 **7** will be used for calls between region 7 (the service provider region) and region 1 (the rest of the enterprise).

change ip-network-region 7										Page	4	of	20			
Source Region: 7 Inter Network Region Connection Management										I		S	M			
										G	A	y	t			
dst	codec	direct	WAN-BW-limits		Video		Intervening			Dyn	A	G	n	c		
rgn	set	WAN	Units	Total	Norm	Prio	Shr	Regions	CAC	R	L	c	e			
1	7	y	NoLimit											n	y	t
2	7	y	NoLimit											n	y	t
3																
4																
5																
6																
7	7										all					
8																
9																
10																
11	3	y	NoLimit											n	y	t
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 7 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 **5067**.
- 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**.
- Default values may be used for all other fields.

```

change signaling-group 7                                     Page 1 of 2
                                SIGNALING GROUP

Group Number: 7                      Group Type: sip
  IMS Enabled? n                    Transport Method: tls
    Q-SIP? n
    IP Video? n                      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y Peer Server: SM                  Clustered? n
  Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
  Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
  Alert Incoming SIP Crisis Calls? n
    Near-end Node Name: procr                      Far-end Node Name: SM
    Near-end Listen Port: 5067                    Far-end Listen Port: 5067
                                              Far-end Network Region: 7

Far-end Domain: avayalab.com

Incoming Dialog Loopbacks: eliminate                      Bypass If IP Threshold Exceeded? n
  DTMF over IP: rtp-payload                                RFC 3389 Comfort Noise? n
  Session Establishment Timer(min): 3                      Direct IP-IP Audio Connections? y
    Enable Layer 3 Test? y                                IP Audio Hairpinning? n
  H.323 Station Outgoing Direct Media? n                  Initial IP-IP Direct Media? n
                                              Alternate Route Timer(sec): 6

```

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 7 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 7		Page 1 of 4	
TRUNK GROUP			
Group Number: 7	Group Type: sip	CDR Reports: y	
Group Name: Service Provider	COR: 1	TN: 1	TAC: *07
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n	Member Assignment Method: auto	
		Signaling Group: 7	
		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 7                                     Page 2 of 4
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                         Redirect On OPTIM Failure: 5000

      SCCAN? n                                         Digital Loss Group: 18
          Preferred Minimum Session Refresh Interval(sec): 600

Disconnect Supervision - In? y  Out? y

      XOIP Treatment: auto      Delay Call Setup When Accessed Via IGAR? n

Caller ID for Service Link Call to H.323 1xC: station-extension
```

On **Page 3**:

- Set the **Numbering Format** field to **public**. This 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. The **Numbering Format** was set to **public** and the **Numbering Format** in the route pattern was set to **pub-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 7

Page 3 of 4

TRUNK FEATURES

ACA Assignment? n

Measured: none

Maintenance Tests? y

Suppress # Outpulsing? n

Numbering Format: public

UII Treatment: service-provider

Replace Restricted Numbers? y

Replace Unavailable Numbers? y

Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y

On **Page 4**:

- Set the **Network Call Redirection** field to **n**. With this setting, Communication Manager will not use the SIP REFER method for the redirection of PSTN calls that are transferred back to the SIP trunk.
- 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 WorldNet Telecommunications.
- Verify that **Identity for Calling Party Display** is set to **P-Asserted-Identity**.
- Default values were used for all other fields.

change trunk-group 7	Page 4 of 4
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
Shuffling with SDP? n	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Resend Display UPDATE Once on Receipt of 481 Response? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-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 assigned by the service provider are shown. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions. Ext Codes: **50231**, **50234** and **50242** with the respective CPN Prefix (DID numbers) are the only extensions relevant to this Application Notes.

change public-unknown-numbering 5 ext-digits 50231					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	50231	7	7879578057	10	Total Administered: 75
5	50234	7	7879578059	10	Maximum Entries: 240
5	50236	7	0366719618	10	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
5	50239	7	7879578057	10	
5	50242	7	7879578065	10	
5	71025	6	000008884571025	15	
5	71026	6	000008884571026	15	Communication Manager automatically inserts a '+' digit in this case.
5	71041	4	0000011041	10	
5	71042	4	0000021042	10	
5	71043	4	0000031043	10	
5	71044	4	0000041044	10	
5	71057	4	000004153571057	15	
5	71058	4	000004153581058	15	
5	71059	4	000004153591059	15	
5	71060	4	000004153601060	15	

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 (refer to **Section 7.4.1**). If the DID number sent by WorldNet 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 7					Page	1	of	3
INCOMING CALL HANDLING TREATMENT								
Service/ Feature	Number Len	Number Digits	Del	Insert				
public-ntwrk	10	7879578057	10	50231				
public-ntwrk	10	7879578059	10	50234				
public-ntwrk	10	7879578065	10	50242				
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								

5.10.Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an “outside line”. This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with **9** of length **1**, as a feature access code (**fac**).

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 3		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	5	ext	8	5	ext			
2	5	ext	9	1	fac			
222	7	ext	*	3	dac			
3	5	ext	#	3	fac			
4	5	ext						
40	4	ext						
5	5	ext						
60	3	ext						
62	4	ext						
63	4	ext						
66	2	fac						
67	4	ext						
68	6	ext						
7	5	ext						
77	4	ext						

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

```
change feature-access-codes                                     Page 1 of 11
FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code: *10
Abbreviated Dialing List2 Access Code:
Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code:
Announcement Access Code: *19
Answer Back Access Code: #40
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code: 66
Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
Automatic Callback Activation: *33      Deactivation: #33
Call Forwarding Activation Busy/DA: *30    All: *31    Deactivation: #30
Call Forwarding Enhanced Status:      Act:      Deactivation:
Call Park Access Code: *40
Call Pickup Access Code: *41
CAS Remote Hold/Answer Hold-Unhold Access Code: *42
CDR Account Code Access Code:
Change COR Access Code:
Change Coverage Access Code:
Conditional Call Extend Activation:      Deactivation:
Contact Closure      Open Code: *80      Close Code: #80
```

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

change ars analysis 17							Page	1 of	2
ARS DIGIT ANALYSIS TABLE							Percent Full: 2		
Location: all									
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd			
17	3	3	7	svcl		n			
1720	11	11	7	fnpa		n			
17555	5	5	4	svcl		n			
1786	11	11	7	fnpa		n			
17865901024	11	11	8	fnpa		n			
18	13	21	7	pubu		n			
1800	11	11	7	pubu		n			
19	11	11	1	fnpa		n			
1900	11	11	deny	fnpa		n			
1900555	11	11	deny	fnpa		n			
19008764533	11	11	1	natl		n			
1908	11	11	7	fnpa		n			
1910	11	11	7	fnpa		n			
1954	11	11	1	fnpa		n			
1xxx976	11	11	deny	fnpa		n			

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 7 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 **pub-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 7
Page 1 of 4

Pattern Number: 7 **Pattern Name: Serv. Provider**

SCCAN? n Secure SIP? n Used for SIP stations? n

Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/	IXC
No	Mrk	Lmt	List	Del	Digits	Intw	QSIG		
1: 7	0		1					n	user
2:								n	user
3:								n	user
4:								n	user
5:								n	user
6:								n	user

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

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 Avaya 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.

AVAYA

Welcome, epadmin
Last logged in today at 6:34:35 AM MDT

Avaya Experience Portal 8.1.2 (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**
 - 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

Avaya Experience Portal Manager

Avaya 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: June 1st, 2020

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, THE END USER, ON BEHALF OF THEMSELF AND THE ENTITY FOR WHOM THEY ARE DOING SO (HEREINAFTER REFERRED TO AS "END USER"), AGREE TO THESE SOFTWARE LICENSE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN END USER AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA"). IF THE END USER IS ACCEPTING THESE SOFTWARE LICENSE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, THE END USER REPRESENTS THAT THEY HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE SOFTWARE LICENSE

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.

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

Licensing


[Refresh](#)

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://10.64.91.90:8443/WebLM/LicenseServer



Last Updated:


Nov 3, 2020 1:02:12 PM MST

Last Successful Poll:

Aug 9, 2023 6:45:18 AM MDT

Licensed Products

Experience Portal



Announcement Ports:

100

ASR Connections:

100

Call Anchoring Ports:

100

Conversation Speech Connections:

100

Email Units:

10

Enable Media Encryption:

1

Enhanced Call Classification:

100

Google ASR Connections:

10

Google Dialogflow Connections:

10

HTML Units:

100

SIP Signaling Connections:

100

SMS Units:

10

Telephony Ports:

100

TTS Connections:

100

Video Server Connections:

100

Zones:

1

Version:

8

Last Successful Poll:

Aug 9, 2023 6:45:18 AM MDT

Last Changed:

Aug 3, 2023 1:03:32 PM MDT

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.

AVAYA

Welcome, epadmin
Last logged in today at 6:34:35 AM MDT

Avaya Experience Portal 8.1.2 (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
 - EPM Manager
 - MPP Manager
 - Software Upgrade
 - System Backup
- ▼ System Configuration
 - Applications
 - EPM Servers
 - MPP Servers
 - SNMP
 - Speech Servers
 - VoIP Connections
 - Zones
- ▼ Security

You are here: [Home](#) > System Configuration > VoIP Connections

VoIP Connections

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.

- The information that you entered has been saved.

H.323 SIP

<input type="checkbox"/>	Name	Enable	Proxy Transport	Proxy/DNS Server Address	Proxy Server Port	Listener Port	SIP Domain	Maximum Simultaneous Calls
<input type="checkbox"/>	SM8	Yes	TLS	10.64.91.81	5061	5061	avayalab.com	10

Add **Delete** **Help**

Step 2 - Configure a SIP connection as follows:

- **Name** – Set to a descriptive name (e.g., **SM8**).
- **Enable** – Set to **Yes**.
- **Proxy Server Transport** – Set to **TLS**.
- Select **Proxy Servers**, and enter:
 - **Proxy Server Address** = **10.64.91.81** (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 **avayalab.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 **10** was used.
- Select **All Calls can be either inbound or outbound**.

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

Welcome, epadmin
Last logged in today at 6:44:40 AM MDT

Avaya Experience Portal 8.1.2 (ExperiencePortal)
Home Help Logoff

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

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 > System Configuration > VoIP Connections > Change SIP Connection

Change SIP Connection

Use this page to change the configuration of a SIP connection.

Name: SM8

Enable: ☒ Yes ☐ No

Proxy Transport: TLS

☒ Proxy Servers ☐ DNS SRV Domain

Address	Port	Priority	Weight	
10.64.91.81	5061	0	0	Remove

Additional Proxy Server

Listener Port: 5061

SIP Domain: avayalab.com

P-Asserted-Identity:

Maximum Redirection Attempts: 2

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: 10

☒ 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

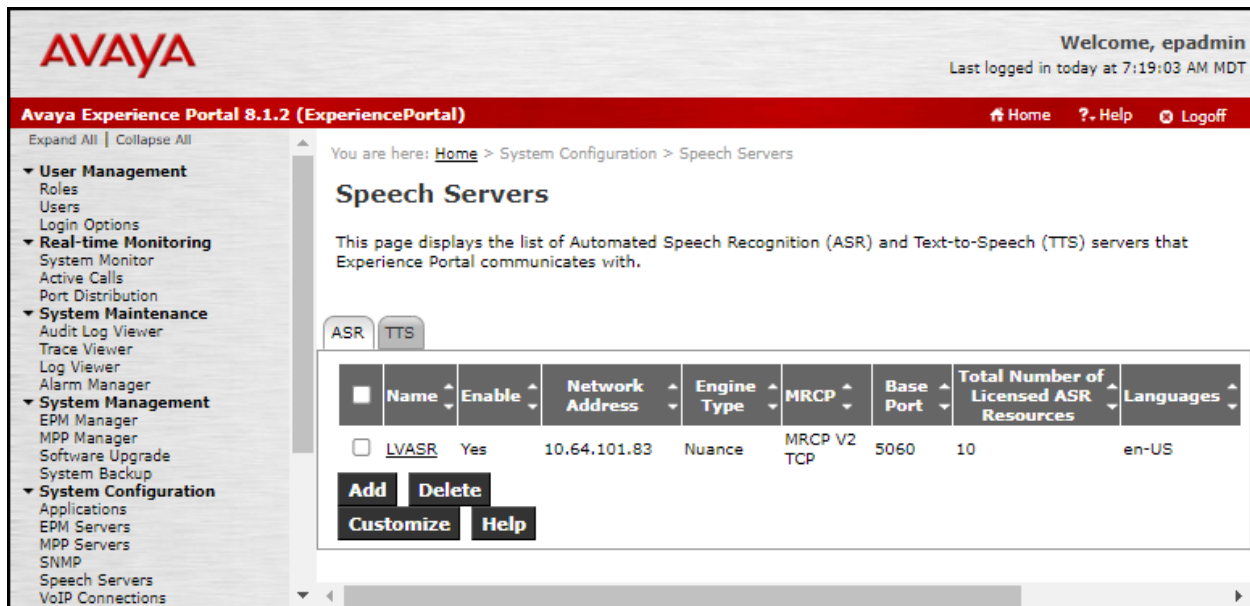
Remove

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:



The screenshot shows the Avaya Experience Portal 8.1.2 (ExperiencePortal) interface. The top navigation bar includes the Avaya logo, a welcome message for 'epadmin', and the last login time '7:19:03 AM MDT'. The main navigation menu on the left lists various system management and configuration options. The current page is 'Speech Servers', which displays a table of configured servers. The table has columns for Name, Enable, Network Address, Engine Type, MRCP, Base Port, Total Number of Licensed ASR Resources, and Languages. One server, 'LVASR', is listed with the following details: Enabled (Yes), Network Address (10.64.101.83), Engine Type (Nuance), MRCP (MRCP V2 TCP), Base Port (5060), Total Number of Licensed ASR Resources (10), and Languages (en-US). Below the table are buttons for 'Add', 'Delete', 'Customize', and 'Help'.

Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed ASR Resources	Languages
LVASR	Yes	10.64.101.83	Nuance	MRCP V2 TCP	5060	10	en-US

TTS speech server:

AVAYA Welcome, epadmin
Last logged in today at 7:19:03 AM MDT

Avaya Experience Portal 8.1.2 (ExperiencePortal) Home Help Logoff

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**
 - EPM Manager
 - MPP Manager
 - Software Upgrade
 - System Backup
- ▼ **System Configuration**
 - Applications
 - EPM Servers
 - MPP Servers
 - SNMP
 - Speech Servers
 - VoIP Connections

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

<input type="checkbox"/>	Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed TTS Resources	Voices
<input type="checkbox"/>	LVTTS	Yes	10.64.101.83		MRCP V2 TCP	5060	10	en-US Chris M

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 10.64.91.90.

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

- **Name** – Set to a descriptive name (e.g., **Test-ccxml**).
- **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, **CCXML** was selected.
- **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.
- **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 **7879578066** provided by WorldNet was used. Inbound calls with this called party number will be handled by the application defined in this section.

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**
 - 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](#) > [System Configuration](#) > [Applications](#) > [Change Application](#)

Change Application

Use this page to change the configuration of an application.

Name: Test-cxxml
 Enable: ☒ Yes ☐ No
 Type: CCXML
 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

ASR Speech Servers

Engine Types Selected Engine Types
 ASR:

Nuance

Languages Selected Languages

Resources:

N Best List Length:

Speech Complete Timeout: milliseconds

Speech Incomplete Timeout: milliseconds

Vendor Parameters:

TTS Speech Servers

Voices Selected Voices
 TTS:

Application Launch

☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number:

Add

Remove

SIP Header Source:

Speech Parameters

Reporting Parameters

Advanced Parameters

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**.

The screenshot shows the Avaya Experience Portal 8.1.2 (ExperiencePortal) interface. The top header includes the Avaya logo, the user 'Welcome, epadmin', and the login time 'Last logged in today at 7:39:44 AM MDT'. The left navigation pane lists various system management options, with 'System Configuration' expanded to show 'MPP Servers'. The main content area is titled 'MPP Servers' and includes a description: '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.' Below the description is a table with the following columns: Name, Host Address, Network Address (VoIP), Network Address (MRCP), Network Address (AppSvr), Maximum Simultaneous Calls, and Trace Level. The table contains one entry: 'mpp1' with Host Address '10.64.91.90' and Maximum Simultaneous Calls '11'. Below the table are 'Add' and 'Delete' buttons. At the bottom of the page are buttons for 'MPP Settings', 'Browser Settings', 'Video Settings', 'VoIP Settings', and 'Help'.

Name	Host Address	Network Address (VoIP)	Network Address (MRCP)	Network Address (AppSvr)	Maximum Simultaneous Calls	Trace Level
<input type="checkbox"/> mpp1	10.64.91.90	<Default>	<Default>	<Default>	11	Use MPP Settings

Step 2 - Enter any descriptive name in the **Name** field (e.g., **MPP1**) 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, epadmin
Last logged in today at 7:39:44 AM MDT

Avaya Experience Portal 8.1.2 (ExperiencePortal) Home Help Logoff

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**
 - 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](#) > [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: mpp1
Host Address: 10.64.91.90
Network Address (VoIP): <Default>
Network Address (MRCP): <Default>
Network Address (AppSvr): <Default>
Maximum Simultaneous Calls: 11
Restart Automatically: ☒ Yes ☐ No

MPP Certificate

```
Owner: C=US,O=Avaya Experience Portal,OU=epm,CN=ep.avayalab.com
Issuer: C=US,ST=CO,L=Thornton,O=AVAYA,OU=SIL,CN=ep.avayalab.com
Serial Number: 8555d57728b031341f5ce96beeb44f9
Signature Algorithm: SHA256withRSA
Version: 3
Valid from: October 28, 2022 2:19:57 PM MDT until October 28, 2032 2:19:57 PM MDT
Certificate Fingerprints
MD5: 72:41:1c:a8:85:10:22:75:e5:80:5b:79:11:8c:9e:5c
SHA: 38:cc:29:b3:3a:bf:bb:22:c2:65:dc:d4:c4:4c:a0:ea:59:ef:b4:ff
SHA-256: c4:44:d9:c2:f7:1a:5a:25:fa:db:9d:bb:48:6d:9c:8a:56:74:7f:eb:86:a2:81:1e:c9:6f:24:de:a6:6f:b1:5b
Basic Constraints:
CA: false
Path Len Constraint: undefined
Subject Alternative Names
DNS Name: ep
DNS Name: ep.avayalab.com
IP Address: 10.64.91.90
IP Address: fe80:0:0:0:20c:29ff:fe75:a39d
```

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, epadmin
Last logged in today at 7:39:44 AM MDT

Avaya Experience Portal 8.1.2 (ExperiencePortal) Home Help Logoff

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
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](#) > [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 **G.729** and **G711uLaw**, are enabled (check marks). Set the **Offer** and Answer **Order** as shown. In the sample configuration **G729** is the preferred codec, with **Order 1**, followed by **G711uLaw** with **Order 2**.
 - On the codec Answer set **G729 Discontinuous Transmission** to **Either**.
- Use default values for all other fields.

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

Codecs ▾

Offer

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

Packet Time:

20 ▾

 milliseconds

G729 Discontinuous Transmission:
 ☐ Yes
 ☒ No

Answer

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

G729 Discontinuous Transmission:
 ☐ Yes
 ☐ No
 ☒ Either

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 the service provider to Experience Portal, the service provider 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 the service provider 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.

AVAYA Welcome, epadmin
Last logged in today at 7:39:44 AM MDT

Avaya Experience Portal 8.1.2 (ExperiencePortal) Home ? Help Logoff

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**
 - 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](#) > System Management > MPP Manager

MPP Manager (Aug 9, 2023 8:12:13 AM MDT)

[Refresh](#)

This page displays the current state of each MPP in the Experience Portal system. To enable the state and mode commands, select one or more MPPs. To enable the mode commands, the selected MPPs must also be stopped.

Last Poll: Aug 9, 2023 8:12:07 AM MDT

<input type="checkbox"/>	Server Name	Mode	State	Config	Auto Restart	Restart Schedule		Active Calls	
						Today	Recurring	In	Out
<input type="checkbox"/>	mmp1	Online	Running	OK	Yes	No	None	2	0

State Commands

[Start](#) [Stop](#) [Restart](#) [Reboot](#) [Halt](#) [Cancel](#)

Mode Commands

[Offline](#) [Test](#) [Online](#)

Restart/Reboot Options

☒ One server at a time
☐ All servers

[Help](#)

7. Configure Avaya Aura® Session Manager

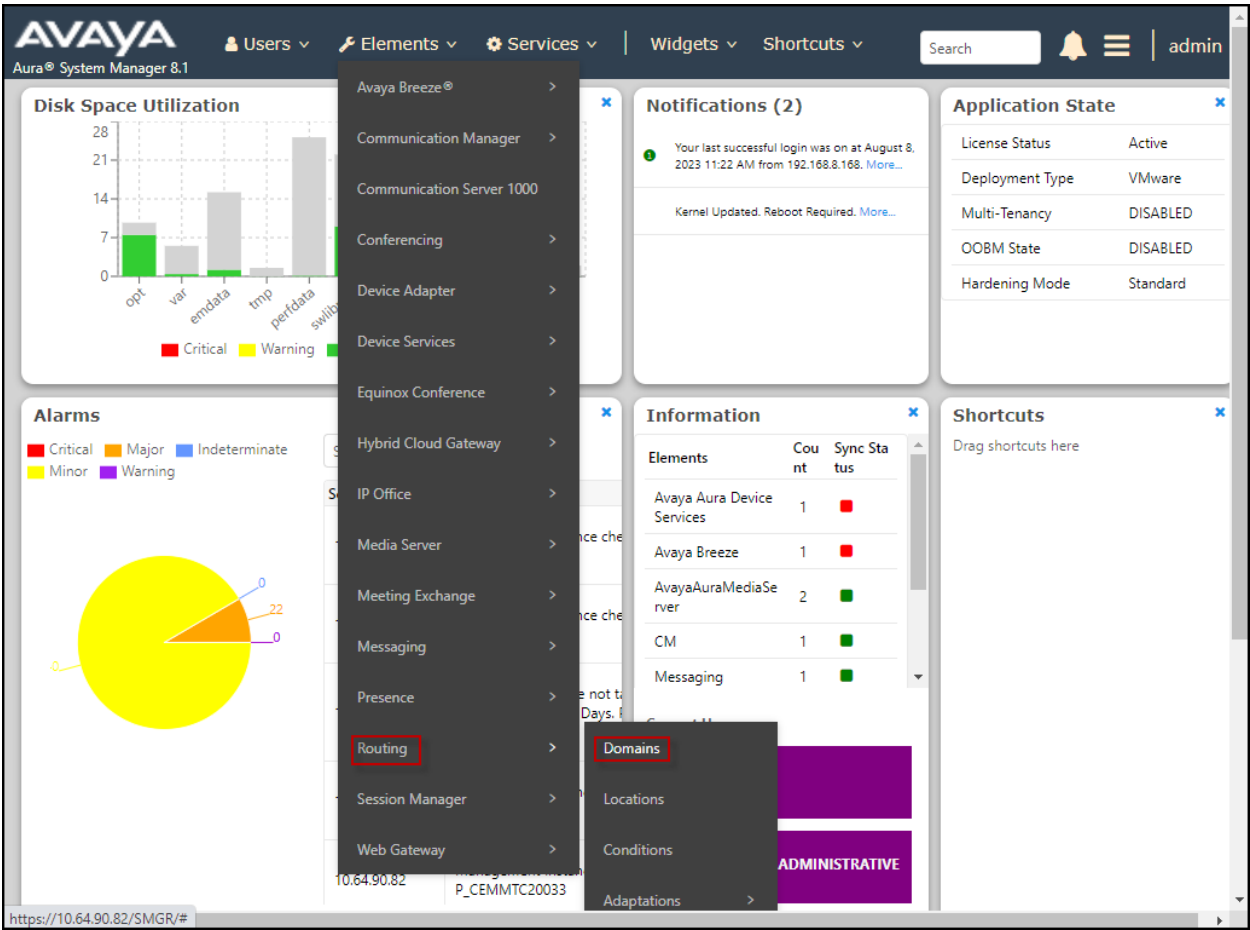
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- 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 SBC.
- 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 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 8.1 web 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 (admin) are also present. The left-hand navigation pane is expanded to the 'Routing' section, with 'Domains' selected. 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 item listed is 'avayalab.com' with a type of 'sip'. Above the table, there are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A 'Filter: Enable' link is also visible. The bottom of the table shows a 'Select : All, None' option.

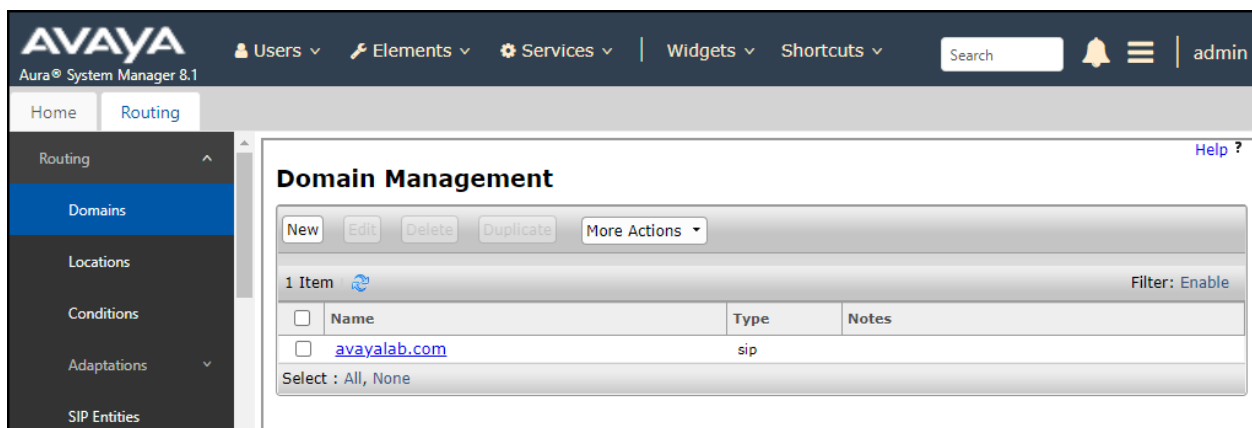
Name	Type	Notes
avayalab.com	sip	

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, **avayalab.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 (not shown).

The screen below shows the entry for the enterprise 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 **Main**.

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 8.1 web interface. The top navigation bar includes the Avaya logo, version information, and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled 'admin' are also present. The left-hand navigation pane shows a tree structure with 'Routing' selected, and 'Locations' highlighted under the 'Routing' category. The main content area is titled 'Location Details' and contains several sections: 'General' with fields for 'Name' (set to 'Main') and 'Notes' (set to 'Avaya DevConnect'); 'Dial Plan Transparency in Survivable Mode' with an 'Enabled' checkbox; 'Listed Directory Number' and 'Associated CM SIP Entity' fields; and 'Overall Managed Bandwidth' with a 'Managed Bandwidth Units' dropdown (set to 'Kbit/sec'), 'Total Bandwidth' and 'Multimedia Bandwidth' fields, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'. 'Commit' and 'Cancel' buttons are located at the top right of the form area.

The following screen shows the location details for the location for **Communication Manager** named **CM TG7**. Later, this location will be assigned to the SIP Entity corresponding to Communication Manager. Other location parameters (not shown) retained the default values.

The screenshot displays the Avaya Aura System Manager 8.1 web 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 (admin) are also present. The left sidebar shows a navigation menu with options like Home, Routing, Domains, Locations (selected), Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and contains three sections: 'General' with fields for Name (CM TG7) and Notes (CM-TG-7); 'Dial Plan Transparency in Survivable Mode' with an 'Enabled' checkbox and fields for Listed Directory Number and Associated CM SIP Entity; and 'Overall Managed Bandwidth' with a dropdown for Managed Bandwidth Units (set to kbit/sec), fields for Total Bandwidth and Multimedia Bandwidth, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'. 'Commit' and 'Cancel' buttons are located at the top right of the form area.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ admin

Home Routing

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

Location Details Commit Cancel [Help ?](#)

General

* Name: CM TG7

Notes: CM-TG-7

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: kbit/sec ▾

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

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

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes the Avaya logo, version information, and a menu with options like Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled 'admin' are also present. The left sidebar shows a navigation tree with 'Routing' selected, and 'Locations' highlighted under the 'Routing' section. 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' is set to 'Common-SBCs' and 'Notes' are 'SBC to PSTN'. 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 input fields for 'Total Bandwidth' and 'Multimedia Bandwidth'. A checkbox for 'Audio Calls Can Take Multimedia Bandwidth' is checked.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ | admin

Home Routing

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

Location Details Commit Cancel Help ?

General

* Name: Common-SBCs

Notes: SBC to PSTN

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec ▾

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

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

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and menu items for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar shows a navigation tree with 'Routing' selected, and 'Locations' highlighted. 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' is set to 'Experience Portal'. The 'Dial Plan Transparency in Survivable Mode' section has 'Enabled' set to 'No'. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' as 'Kbit/sec', with 'Total Bandwidth' and 'Multimedia Bandwidth' fields. The 'Audio Calls Can Take Multimedia Bandwidth' checkbox is checked. 'Commit' and 'Cancel' buttons are located at the top right of the form.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ | admin

Home Routing

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

Location Details Commit Cancel Help ?

General

* Name: Experience Portal

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec ▾

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

7.4. Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers sent to/from WorldNet Telecommunications. In the reference configuration the following Adaptations were used:

- Calls from WorldNet - Modification of SIP messages sent to Communication Manager extensions.
 - The WorldNet DID number digit string in the Request URI is replaced with the associated Communication Manager extensions/VDN (**Section Error!** Reference source not found.).
- Calls to WorldNet - Modification of SIP messages sent by Communication Manager extensions.
 - Avaya SIP headers not required by WorldNet are removed (**Section 0**).

7.4.1. Adaptation for Avaya Aura® Communication Manager Extensions

The Adaptation administered in this section is used for modification of SIP messages to Communication Manager extensions from WorldNet.

Step 1 - In the left pane under **Routing**, click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown).

Step 2 - In the **Adaptation Details** page, enter:

- A descriptive **Name**, (e.g., **CM TG7 SP**).
- Select **DigitConversionAdapter** from the **Module Name** drop-down.

The screenshot shows the 'Adaptation Details' configuration page. On the left, a sidebar under 'Routing' has 'Adaptations' selected. The main area is titled 'Adaptation Details' and contains a 'General' tab. The form fields are as follows:

- * Adaptation Name:** CM TG7 SP
- Notes:** (empty text box)
- * Module Name:** DigitConversionAdapter (dropdown menu)
- Type:** digit
- State:** enabled (dropdown menu)
- Module Parameter Type:** (empty dropdown menu)
- Egress URI Parameters:** (empty text box)

At the top right of the form are 'Commit' and 'Cancel' buttons.

Step 3 - Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the inbound digits from WorldNet that need to be replaced with their associated Communication Manager extensions before being sent to Communication Manager).

Example 1

- Enter **7879578059** in the **Matching Pattern** column.
- Enter **10** in the **Min/Max** columns.
- Enter **10** in the **Delete Digits** column.

- Enter **50234** in the **Insert Digits** column (50234 is the Communication Manager extension number).
- Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
- Enter any desired notes.

Step 4 - Repeat **example 1 above** for all additional WorldNet DID numbers/Communication manager extensions.

Step 5 - Click on **Commit**.

Note – In the reference configuration, the WorldNet service delivered 10-digit DID numbers.

Digit Conversion for Outgoing Calls from SM

3 Items

Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 7879578059	* 10	* 10		* 10	50234	destination ▼		
<input type="checkbox"/>	* 7879578065	* 10	* 10		* 10	50242	destination ▼		
<input type="checkbox"/>	* 7879578066	* 10	* 10		* 10	12000	destination ▼		

Select : All, None

7.4.2. Adaptation for Communication Manager header removal

The Adaptation administered in this section is used for modification of SIP messages from Communication Manager to WorldNet. Repeat the steps in **Section Error! Reference source not found.** with the following changes.

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

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

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

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The main content area is titled 'Adaptation Details' and has a 'General' tab selected. The configuration fields are as follows:

- Adaptation Name:** Header_Optimization
- Notes:** (empty)
- Module Name:** DigitConversionAdapter
- Type:** digit
- State:** enabled
- Module Parameter Type:** Name-Value Parameter

Below these fields is a table with 'Add' and 'Remove' buttons. The table has two columns: 'Name' and 'Value'.

Name	Value
eRHdrs	AV-Global-Session-ID,Alert-Info,Endpoint-View,P-AV-Message-Id,P-Charging-Vector,P-Location,AV-Correlation-ID,Av-Secure-Indication

At the bottom of the table, it says 'Select : All, None'.

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 SBC and 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 SBC 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.
- **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 8.1 web interface. The top navigation bar includes the Avaya logo, the version number 'Aura® System Manager 8.1', and several menu items: 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. Below this, a secondary navigation bar shows 'Home' and 'Routing'. A left-hand sidebar contains a list of configuration categories: 'Routing', 'Domains', 'Locations', 'Conditions', 'Adaptations', 'SIP Entities' (which is highlighted in blue), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'SIP Entity Details' and features a 'Commit' button and a 'Cancel' button in the top right corner. The form is divided into two sections: 'General' and 'Monitoring'. In the 'General' section, the following fields are visible: 'Name' (set to 'Session Manager'), 'IP Address Family' (set to 'Both'), 'IPv4 Address' (set to '10.64.91.81'), 'IPv6 Address' (empty), 'SIP FQDN' (empty), 'Type' (set to 'Session Manager'), 'Notes' (empty), 'Location' (set to 'Main'), 'Outbound Proxy' (empty), 'Time Zone' (set to 'America/Denver'), 'Minimum TLS Version' (set to 'Use Global Setting'), and 'Credential name' (empty). The 'Monitoring' section contains two fields: 'SIP Link Monitoring' (set to 'Use Session Manager Configuration') and 'CRLF Keep Alive Monitoring' (set to 'Use Session Manager Configuration').

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Home Routing

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

SIP Entity Details Commit Cancel

General

* Name: Session Manager

* IP Address Family: Both ▾

* IPv4 Address: 10.64.91.81

IPv6 Address:

SIP FQDN:

Type: Session Manager ▾

Notes:

Location: Main ▾

Outbound Proxy: ▾

Time Zone: America/Denver ▾

Minimum TLS Version: Use Global Setting ▾

Credential name:

Monitoring

SIP Link Monitoring: Use Session Manager Configuration ▾

CRLF Keep Alive Monitoring: Use Session Manager Configuration ▾

The following screen shows the addition of the **CM-TG7** 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**. For **Type** Select **CM** for Communication Manager. On the **Adaptation** field, the adaptation module **CM TG7 SP** previously defined in **Section 7.4.1** was selected. Select the location that applies to the SIP Entity being created, defined in **Section 7.3**. Select the **Time Zone**. Click **Commit** to save.

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The left sidebar shows the navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields and values:

- Name:** CM-TG7
- * IP Address Family:** IPv4 **Tolerance:** ☐
- * FQDN or IPv4 Address:** 10.64.91.75
- Type:** CM
- Notes:** CM Trunk Group 7 for SP
- Adaptation:** CM TG7 SP
- Location:** CM TG7
- Time Zone:** America/Denver
- * SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty field)
- Securable:** ☐
- Call Detail Recording:** none

At the top right of the form, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

The following screen shows the addition of the **SBC1** SIP Entity for the Avaya SBC:

- The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**).
- For **Type** Select **SIP Trunk**.
- On the **Adaptation** field, the adaptation module **Header_Optimization** previously defined in **Section 7.4.2** was selected.
- Select the location that applies to the SIP Entity being created, defined in **Section 7.3**.
- Select the **Time Zone**.
- Click **Commit** to save.

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The left sidebar shows a navigation menu with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and includes 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing the following fields:

- Name:** SBC1
- IP Address Family:** IPv4 **Tolerance:** ☐
- FQDN or IPv4 Address:** 10.64.91.50
- Type:** SIP Trunk
- Notes:** Avaya SBC-1 to PSTN
- Adaptation:** Header_Optimization
- Location:** Common-SBCs
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty field)
- Securable:** ☐
- Call Detail Recording:** egress

The 'Loop Detection' section at the bottom shows **Loop Detection Mode:** Off.

The following screen shows the addition of the **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 displays the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and a menu with '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' expanded, containing 'Domains', 'Locations', 'Conditions', 'Adaptations', 'SIP Entities' (highlighted), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'SIP Entity Details' and includes 'Commit' and 'Cancel' buttons. It is divided into three sections: 'General', 'Loop Detection', and 'Monitoring'. The 'General' section contains fields for Name (ExperiencePortal), IP Address Family (IPv4), Tolerance (checkbox), FQDN or IPv4 Address (10.64.91.90), Type (Voice Portal), Notes, Adaptation, Location (Experience Portal), Time Zone (America/Denver), SIP Timer B/F (4), Minimum TLS Version (Use Global Setting), Credential name, Securable (checkbox), and Call Detail Recording (none). The 'Loop Detection' section has Loop Detection Mode (On), Loop Count Threshold (5), and Loop Detection Interval (200). The 'Monitoring' section has SIP Link Monitoring and CRLF Keep Alive Monitoring, both set to 'Use Session Manager Configuration'.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ | admin

Home Routing

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

SIP Entity Details Commit Cancel Help ?

General

* Name: ExperiencePortal

* IP Address Family: IPv4 ▾ Tolerance: ☐

* FQDN or IPv4 Address: 10.64.91.90

Type: Voice Portal ▾

Notes:

Adaptation: ▾

Location: Experience Portal ▾

Time Zone: America/Denver ▾

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

Minimum TLS Version: Use Global Setting ▾

Credential name:

Securable: ☐

Call Detail Recording: none ▾

Loop Detection

Loop Detection Mode: On ▾

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

Monitoring

SIP Link Monitoring: Use Session Manager Configuration ▾

CRLF Keep Alive Monitoring: Use Session Manager Configuration ▾

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 SBC 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 named **SM to CM TG7**. 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 **5067** were used.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left navigation pane is expanded to 'Routing' > 'Entity Links'. The main area displays the 'Entity Links' configuration page. At the top, there are 'Commit' and 'Cancel' buttons. Below is a table with one item, 'SM to CM TG7'. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, IP Address Family, DNS Override, Connection Policy, Deny New Service, and Notes. The values for the first row are: Name: SM to CM TG7, SIP Entity 1: Session Manager, Protocol: TLS, Port: 5067, SIP Entity 2: CM-TG7, Port: 5067, IP Address Family: IPv4, DNS Override: (unchecked), Connection Policy: trusted, Deny New Service: (unchecked), and Notes: (empty). Below the table, there is a 'Select : All, None' dropdown. At the bottom, there are 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	IP Address Family	DNS Override	Connection Policy	Deny New Service	Notes
SM to CM TG7	Session Manager	TLS	5067	CM-TG7	5067	IPv4	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

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

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left sidebar contains a menu with options: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links (selected), and Time Ranges. The main content area is titled "Entity Links" and includes "Commit" and "Cancel" buttons. Below the title, there is a table with 11 columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, IP Address Family, DNS Override, Connection Policy, Deny New Service, and Notes. A single row is displayed with the following values: Name: "SM to SBC1", SIP Entity 1: "Session Manager", Protocol: "TLS", Port: "5061", SIP Entity 2: "SBC1", Port: "5061", IP Address Family: "IPv4", DNS Override: (unchecked), Connection Policy: "trusted", Deny New Service: (unchecked), and Notes: (empty). Below the table, there is a "Select : All, None" dropdown and another "Commit" and "Cancel" button.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	IP Address Family	DNS Override	Connection Policy	Deny New Service	Notes
* SM to SBC1	* Session Manager	TLS	* 5061	* SBC1	* 5061	IPv4	<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 8.1 interface. The left sidebar contains a menu with options: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links (selected), and Time Ranges. The main content area is titled "Entity Links" and includes "Commit" and "Cancel" buttons. Below the title, there is a table with 11 columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, IP Address Family, DNS Override, Connection Policy, Deny New Service, and Notes. A single row is displayed with the following values: Name: "SM to ExperiencePortal", SIP Entity 1: "Session Manager", Protocol: "TLS", Port: "5061", SIP Entity 2: "ExperiencePortal", Port: "5061", IP Address Family: "IPv4", DNS Override: (unchecked), Connection Policy: "trusted", Deny New Service: (unchecked), and Notes: (empty). Below the table, there is a "Select : All, None" dropdown and another "Commit" and "Cancel" button.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	IP Address Family	DNS Override	Connection Policy	Deny New Service	Notes
* SM to ExperiencePortal	* Session Manager	TLS	* 5061	* ExperiencePortal	* 5061	IPv4	<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**. Two routing policies were added: An incoming policy with Communication Manager as the destination and an outbound policy with the Avaya SBC as the destination and 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 SBC and the Experience Portal.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ | admin

Home Routing

Routing Policies

Routing Policy Details

Commit Cancel

General

* Name: To CM TG7

Disabled: ☐

* Retries: 0

Notes: Inbound calls from UCI

SIP Entity as Destination

Select

Name	IP Address Family	FQDN or IPv4 Address	FQDN or IPv6 Address	Type	Notes
CM-TG7	IP4	10.64.91.75		CM	CM Trunk Group 7 for SP

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

AVAYA

Aura® System Manager 8.1

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Routing Policy Details

Commit

Cancel

Help ?

General

* Name:

To SBC1

Disabled:

☐

* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	IP Address Family	FQDN or IPv4 Address	FQDN or IPv6 Address	Type	Notes
SBC1	IPv4	10.64.91.50		SIP Trunk	Avaya SBC-1 to PSTN

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item

Filter: Enable

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

Select : All, None

AVAYA

Aura® System Manager 8.1

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Routing Policy Details

Commit

Cancel

Help ?

General

* Name:

To Experience Portal

Disabled:

☐

* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	IP Address Family	FQDN or IPv4 Address	FQDN or IPv6 Address	Type	Notes
ExperiencePortal	IPv4	10.64.91.90		Voice Portal	

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item

Filter: Enable

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

Select : All, None

7.8. Dial Patterns

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

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

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria, or select “**ALL**” to route incoming calls to all SIP domains.
- **Notes:** Add a brief description (optional).
- In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria (**Section 7.3**).
- Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria (**Section 7.7**). Click **Select** (not shown).
- Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to Communication Manager. In the examples, calls to 10-digit numbers starting with **787** arriving from location **Common-SBCs**, used route policy **To CM TG7** to Communication Manager. The SIP Domain was set to **avayalab.com**.

AVAYA
Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾

[admin](#)

[Home](#) | [**Routing**](#)

Routing ↑
 Domains
 Locations
 Conditions
 Adaptations ▾
 SIP Entities
 Entity Links
 Time Ranges
Routing Policies
 Dial Patterns ↑
 Dial Patterns

Dial Pattern Details

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

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain: ▾

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

1 Item		Filter: Enable					
<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Common-SBCs	SBC to PSTN	To CM TG7	0	<input type="checkbox"/>	CM-TG7	Inbound calls from UCI

Select : All, None

The example in this screen shows the 11-digit dialed numbers for outbound calls, beginning with **1**, arriving from the **CM TG7** location, will use route policy **To SBC1**, which sends the call out to the PSTN via Avaya SBC and the service provider SIP trunk. The SIP Domain was set to **avayalab.com**.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ admin

Home Routing

Routing ▾

- Domains
- Locations
- Conditions
- Adaptations ▾
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies**
- Dial Patterns ▾
- Dial Patterns <

Dial Pattern Details Commit Cancel Help ?

General

* **Pattern:** 1

* **Min:** 1

* **Max:** 36

Emergency Call: ☐

SIP Domain: avayalab.com ▾

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name ▴	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	CM TG7	CM-TG-7	To SBC1	0	<input type="checkbox"/>	SBC1	

Select : All, None

The example in the screen below shows the dial pattern “+” needed when calls from the PSTN to Experience Portal are transferred back out to the PSTN via Experience Portal (e.g., choosing option 5) which may contain a “+” that is inserted by Session Manager to the number in the “Refer-To” header of the REFER message from Experience Portal, this will result in a “No Route Found” error message generated by Session Manager if the “+” is not included in Session Manager’s Dial Patterns (refer to **Section 7.8**).

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ | admin

Home Routing

Routing ▾

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

Dial Pattern Details

Commit Cancel

General

* Pattern: +

* Min: 10

* Max: 36

Emergency Call: ☐

SIP Domain: avayalab.com ▾

Notes: E.164 Public Numbers

Originating Locations and Routing Policies

Add Remove

13 Items 🔁 Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Common-SBCs	SBC to PSTN	To SBC1	0	<input type="checkbox"/>	SBC1	

The following screen illustrates an example dial pattern used to verify inbound calls from the PSTN to Experience Portal. In the sample configuration one of the DID numbers provided by the service provider (7879578066) was used as a test number to route calls from the PSTN to Experience Portal, arriving from location **Common-SBCs**, used routing policy **To Experience Portal**. The SIP Domain was set to **avayalab.com**.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search [] admin

Home Routing

Routing ▾

- Domains
- Locations
- Conditions
- Adaptations ▾
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies**
- Dial Patterns ▾
- Regular Expressions

Dial Pattern Details [Commit] [Cancel] [Help ?]

General

* Pattern: 7879578066

* Min: 10

* Max: 36

Emergency Call: ☐

SIP Domain: avayalab.com ▾

Notes: []

Originating Locations and Routing Policies

[Add] [Remove]

1 Item [Filter: Enable]

<input type="checkbox"/>	Originating Location Name ▾	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Common-SBCs	SBC to PSTN	To Experience Portal	0	<input type="checkbox"/>	ExperiencePortal	

Select : All, None

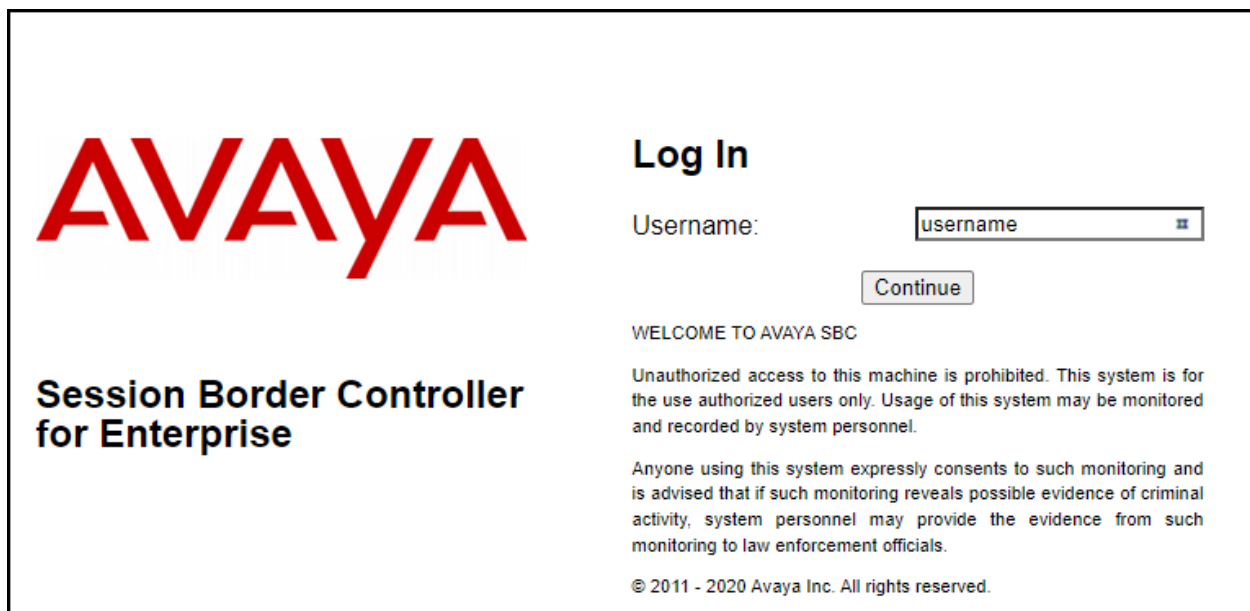
Repeat the above procedures as needed to define additional dial patterns.

8. Configure Avaya Session Border Controller

This section describes the configuration of the Avaya SBC. It is assumed that the initial installation of the Avaya SBC, 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 SBC consult the Avaya SBC documentation in the **References** section.

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.



The image shows the login page of the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise' in bold black font. On the right, under the heading 'Log In', there is a 'Username:' label followed by a text input field containing the placeholder 'username'. Below the input field is a 'Continue' button. Further down, the text 'WELCOME TO AVAYA SBC' is displayed, followed by a disclaimer: 'Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.' Below this is a consent statement: 'Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.' At the bottom, the copyright notice '© 2011 - 2020 Avaya Inc. All rights reserved.' is shown.

Once logged in, on the top left of the screen, under **Device:** select the device being managed, **SBCE8-90** in the sample configuration.

Device: SBCE8-90 Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

EMS
SBCE8-90

er Controller for Enterprise

AVAYA

EMS Dashboard

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

Dashboard

Information	
System Time	01:51:19 PM MDT Refresh
Version	8.1.3.2-38-22279
GUI Version	8.1.3.2-22253
Build Date	Tue Aug 02 21:33:44 UTC 2022
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	08/09/2023 13:47:49 MDT
Failed Login Attempts	0

Installed Devices

- EMS
- SBCE8-90

Active Alarms (past 24 hours)

Incidents (past 24 hours)

The left navigation pane contains the different available menu items used for the configuration of the Avaya SBC. 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.

Device: SBCE8-90 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

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

Dashboard

Information	
System Time	01:53:31 PM MDT Refresh
Version	8.1.3.2-38-22279
GUI Version	8.1.3.2-22253
Build Date	Tue Aug 02 21:33:44 UTC 2022
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	08/09/2023 13:47:49 MDT
Failed Login Attempts	0

Installed Devices

- EMS
- SBCE8-90

8.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named **SBCE8-90** is shown. 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 SBC, 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 web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Device: SBCE8-90' and the 'Session Border Controller for Enterprise' title with the Avaya logo. The left sidebar lists navigation options: EMS Dashboard, Software Management, Device Management (highlighted), Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled 'Device Management' and contains a tabbed interface with 'Devices', 'Updates', 'Licensing', 'Key Bundles', and 'License Compliance'. The 'Devices' tab is active, showing a table with columns for Device Name, Management IP, Version, and Status. A single device, SBCE8-90, is listed with a management IP of 10.64.90.90, version 8.1.3.2-38-22279, and a status of 'Commissioned'. Action links for Reboot, Shutdown, Restart Application, View, Edit, and Uninstall are provided for the device.

Device Name	Management IP	Version	Status
SBCE8-90	10.64.90.90	8.1.3.2-38-22279	Commissioned

To view the network configuration assigned to the Avaya SBC, click **View** on the screen above. The **System Information** window is displayed, containing the current device configuration and network settings. Note that **DNS configuration** is required for this solution.

System Information: SBCE8-90

General Configuration

Appliance NameSBCE8-90

Box TypeSIP

Deployment ModeProxy

Device Configuration

HA ModeNo

Two Bypass ModeNo

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	10	100
Advanced Sessions	10	100
Scopia Video Sessions	10	100
CES Sessions	10	100
Transcoding Sessions	10	100
AMR	<input type="checkbox"/>	
Premium Sessions	0	0
CLID	---	
Encryption	<input checked="" type="checkbox"/>	
Available: Yes		

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
				A1
				A1
10.64.91.50	10.64.91.50	255.255.255.0	10.64.91.1	A1
				B1
				B2
10.10.80.53	10.10.80.53	255.255.255.128	10.10.80.1	B2
				B2
				B2

DNS Configuration

Primary DNS172.30.209.4

Secondary DNS

DNS LocationDMZ

DNS Client IP1.1.1.2

Management IP(s)

IP #1 (IPv4)10.64.90.90

The highlighted IP addresses in the **System Information** screen shown above are the ones used for the SIP trunk to WorldNet Telecommunications and are the ones relevant to these Application Notes. Other IP addresses assigned to the Avaya SBC **A1**, **B1** and **B2** 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 SBC (10.64.91.50) was used to connect to the enterprise network, while its public interface (10.10.80.53) 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

Note – Testing was done with System Manager signed identity certificates. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

In the reference configuration, TLS transport is used for the communication between Session Manager and Avaya SBC. The following procedures show how to create the client and server profiles to support the TLS connection.

8.3.1. Verify TLS Certificates – Avaya Session Border Controller

Once logged in, on the top left of the screen, under **Device:** select the device being managed, **SBCE8-90** in the sample configuration.



Step 1 - Select **TLS Management** → **Certificates** from the left-hand menu. Verify the following:

- System Manager CA certificate is present in the **Installed CA Certificates** area.
- System Manager CA signed identity certificate is present in the **Installed Certificates** area.
- Private key associated with the identity certificate is present in the **Installed Keys** area (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE8-90, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. The left sidebar contains a menu with options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (selected), Certificates (highlighted), Client Profiles, Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled 'Certificates' and features two tabs: 'Certificates' (active) and 'Keys'. Below the tabs, there are two sections: 'Installed Certificates' and 'Installed CA Certificates'. Each section contains a table of certificates with 'View' and 'Delete' links. The 'Installed Certificates' section lists 'sbce90_internal.pem' and 'ucsec.pem'. The 'Installed CA Certificates' section lists 'AvayaDeviceEnrollmentCAchain.crt', 'avayaitrootca2.pem', 'entrust_g2_ca.cer', 'SystemManagerCA.pem', and 'ucsec.pem'.

Installed Certificates	
sbce90_internal.pem	View Delete
ucsec.pem	View Delete

Installed CA Certificates	
AvayaDeviceEnrollmentCAchain.crt	View Delete
avayaitrootca2.pem	View Delete
entrust_g2_ca.cer	View Delete
SystemManagerCA.pem	View Delete
ucsec.pem	View Delete

8.3.2. Server Profiles

Step 1 - Select **TLS Management** → **Server Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbce90_internal.pem**, from pull down menu.
- **Peer Verification = None.**
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.

Edit Profile X

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile

Profile Name: Inside_Server

Certificate: sbce90_internal.pem

SNI Options: None

SNI Group: None

Certificate Verification

Peer Verification: None

Peer Certificate Authorities: AvayaDeviceEnrollmentCAchain.crt, avayaitrootca2.pem, entrust_g2_ca.cer, SystemManagerCA.pem

Peer Certificate Revocation Lists:

Verification Depth: 0

Next

The following screen shows the completed TLS **Server Profile** form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE8-90, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo.

On the left, a sidebar menu lists various management options, with 'Server Profiles' highlighted under the 'TLS Management' section.

The main content area is titled 'Server Profiles: Inside_Server'. It features an 'Add' button and a 'Delete' button. Below this, a list of server profiles shows 'Inside_Server' selected. A 'Click here to add a description.' link is also present.

The 'Server Profile' configuration form for 'Inside_Server' is shown, containing the following sections:

- TLS Profile**
 - Profile Name: Inside_Server
 - Certificate: sbce90_internal.pem
 - SNI Options: None
- Certificate Verification**
 - Peer Verification: None
 - Extended Hostname Verification: ☐
- Renegotiation Parameters**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**
 - Version: ☒ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0
 - Ciphers: ☒ Default ☐ FIPS ☐ Custom
 - Value: HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

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

8.3.3. Client Profiles

Step 1 - Select **TLS Management** → **Client Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbce90_internal.pem**, from pull down menu.
- **Peer Verification = Required.**
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **SystemManagerCA.pem**.
- **Verification Depth:** enter **1**.
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile

Profile Name:

Certificate:

SNI: ☐ Enabled

Certificate Verification

Peer Verification: Required

Peer Certificate Authorities:

Peer Certificate Revocation Lists:

Verification Depth:

Extended Hostname Verification: ☐

Server Hostname:

The following screen shows the completed TLS **Client Profile** form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE8-90, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo.

On the left, a sidebar menu lists various management options, with 'Client Profiles' highlighted under 'TLS Management'. The main content area is titled 'Client Profiles: Inside_Client' and features an 'Add' button and a 'Delete' button. A list of client profiles shows 'Inside_Client' as the selected profile.

The configuration form for 'Inside_Client' is displayed, containing the following sections:

- TLS Profile**
 - Profile Name: Inside_Client
 - Certificate: sbce90_internal.pem
 - SNI: ☐ Enabled
- Certificate Verification**
 - Peer Verification: Required
 - Peer Certificate Authorities: SystemManagerCA.pem
 - Peer Certificate Revocation Lists: ---
 - Verification Depth: 1
 - Extended Hostname Verification: ☐
- Renegotiation Parameters**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**
 - Version: ☒ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0
 - Ciphers: ☒ Default ☐ FIPS ☐ Custom

8.4. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBC. 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 (**10.64.91.50**) and public (**10.10.80.53**) sides of the Avaya SBC are the ones relevant to these Application Notes.

On the **Interfaces** tab, verify the **Administrative Status** is **Enabled** for the **A1** and **B2** interfaces. Click the buttons under the **Status** column, if necessary, to enable the interfaces.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: SBCE8-90', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the Avaya logo. The left sidebar lists various management sections, with 'Network Management' highlighted under 'Network & Flows'. The main content area is titled 'Network Management' and features two tabs: 'Interfaces' (active) and 'Networks'. An 'Add VLAN' button is located in the top right of the interface section. Below the tabs is a table with three columns: 'Interface Name', 'VLAN Tag', and 'Status'.

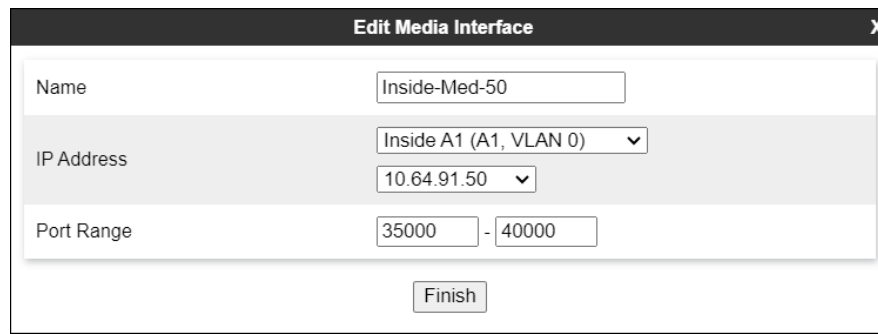
Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Disabled
B2		Enabled

8.5. Media Interfaces

Media Interfaces were created to specify the IP address and port range in which the Avaya SBC will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBC 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**.



Edit Media Interface X	
Name	Inside-Med-50
IP Address	Inside A1 (A1, VLAN 0) 10.64.91.50
Port Range	35000 - 40000
Finish	

A Media Interface facing the public side was similarly created with the name **Outside-Med-B2-53**, 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 of **35000-40000**.
- Click **Finish**.

Edit Media Interface X

Name	Outside-Med-B2-53
IP Address	Public B2 (B2, VLAN 0) 10.10.80.53
Port Range	35000 - 40000

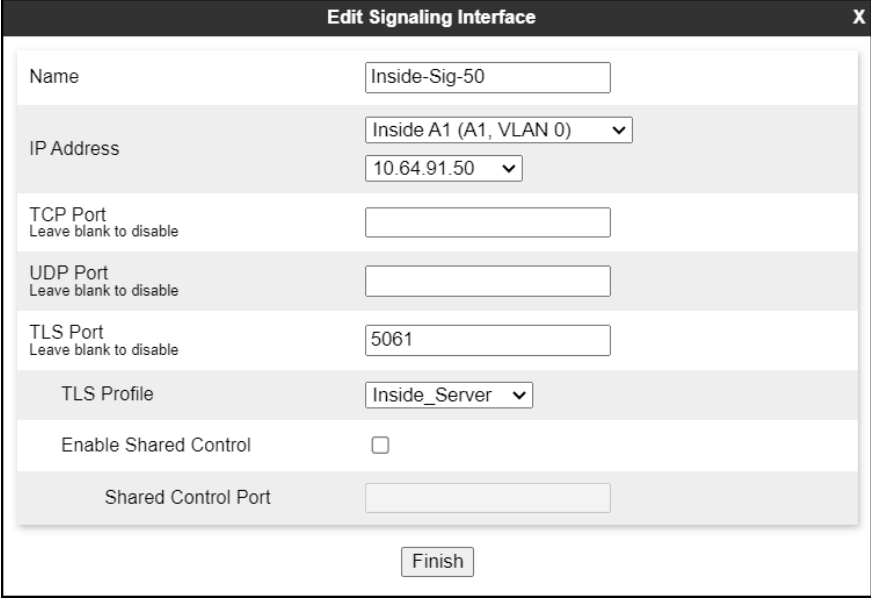
Finish

8.6. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBC 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** (**Section 8.3.2**).
- Click **Finish**.



The screenshot shows a web-based configuration window titled "Edit Signaling Interface" with a close button (X) in the top right corner. The window contains several input fields and a "Finish" button at the bottom. The fields are as follows:

Field Label	Value / Selection
Name	Inside-Sig-50
IP Address	Inside A1 (A1, VLAN 0) (dropdown) 10.64.91.50 (dropdown)
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	Inside_Server (dropdown)
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

A second Signaling Interface with the name **Outside-Sig-B2-53** 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 **5060** for **UDP Port**, since UDP port 5060 is used to listen for signaling traffic from WorldNet Telecommunications in the sample configuration.
- Click **Finish**.

Edit Signaling Interface X	
Name	Outside-Sig-B2-53
IP Address	Public B2 (B2, VLAN 0) 10.10.80.53
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	
TLS Profile	None
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 **Configuration 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 displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE8-90, Alarms, 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.

The left navigation pane lists various management options, with "Configuration Profiles" expanded to show "Server Interworking" selected. The main content area is titled "Interworking Profiles: avaya-ru" and includes an "Add" button and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new profile instead."

The configuration is organized into tabs: General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced. The "General" tab is active, showing 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	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	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

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

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



The image shows a 'Clone Profile' dialog box with a dark header bar containing the title 'Clone Profile' and a close button 'X'. The main area has a light gray background. It contains two input fields: 'Profile Name' with the text 'Enterprise Interwk' and 'Clone Name' with the text 'Enterprise Interwk'. Below these fields is a 'Finish' button.

Clone Profile	
Profile Name	Enterprise Interwk
Clone Name	Enterprise Interwk
<div>Finish</div>	

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

Device: SBCE8-90 ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

Domain DoS

Server Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

URN Profile

Recording Profile

H248 Profile

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Interworking Profiles: Enterprise Interwk

Add

Interworking Profiles

cs2100

avaya-ru

Enterprise In...

VZ REFER H...

SIP Provider I...

RenameCloneDelete

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

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	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	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

Edit

HG; Reviewed:
SPOC 9/26/2023

Avaya DevConnect Application Notes
©2023 Avaya Inc. All Rights Reserved.

90 of 139
WN-CMSMEPSBC-81

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 Device: SBCE8-90, Alarms, 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 under "Configuration Profiles", including "Server", "Interworking", "Media Forking", "Routing", "Topology Hiding", "Signaling Manipulation", "URI Groups", "SNMP Traps", "Time of Day Rules", "FGDN Groups", "Reverse Proxy Policy", "URN Profile", "Recording Profile", "H248 Profile", "Services", "Domain Policies", "TLS Management", "Network & Flows", and "DMZ Services".

The main content area is titled "Interworking Profiles: Enterprise Interwk". It features an "Add" button and a list of profiles: "cs2100", "avaya-ru", "Enterprise In...", "VZ REFER H...", and "SIP Provider I...". The "Enterprise In..." profile is selected, and its settings are displayed in the "Advanced" tab.

The "Advanced" tab settings include:

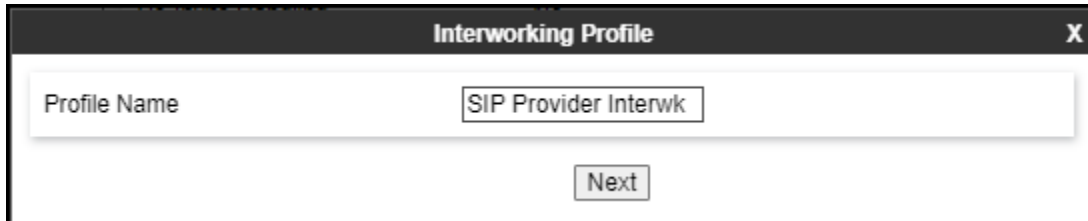
- Record Routes: Both Sides
- Include End Point IP for Context Lookup: Yes
- Extensions: Avaya
- Diversion Manipulation: No
- Has Remote SBC: Yes
- Route Response on Via Port: No
- Relay INVITE Replace for SIPREC: No
- MOBX Re-INVITE Handling: No
- NATing for 301/302 Redirection: Yes
- DTMF: DTMF Support: None

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

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**.



The screenshot shows a web-based dialog box titled "Interworking Profile". It features a close button (X) in the top right corner. The main content area contains a text input field with the label "Profile Name" and the text "SIP Provider Interwk" entered. Below the input field is a "Next" button.

- Click **Next** until the last tab is reached then click **Finish** on the last tab leaving remaining fields with default values (not shown).

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

Device: SBCE8-90 ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration ProfilesDomain DoS**Server Interworking**Media ForkingRoutingTopology HidingSignaling ManipulationURI GroupsSNMP TrapsTime of Day RulesFGDN GroupsReverse Proxy PolicyURN ProfileRecording ProfileH248 Profile▸ Services▸ Domain Policies▸ TLS Management▸ Network & Flows▸ DMZ Services▸ Monitoring & Logging

Interworking Profiles: SIP Provider Interwk

AddRenameCloneDelete

Interworking Profiles

cs2100avaya-ruEnterprise Int...VZ REFER H...**SIP Provider...**

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

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	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	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

Edit

HG; Reviewed:
SPOC 9/26/2023

Avaya DevConnect Application Notes
©2023 Avaya Inc. All Rights Reserved.

93 of 139
WN-CMSMEPSBC-81

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

Device: SBCE8-90 ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration ProfilesDomain DoS**Server Interworking**Media ForkingRoutingTopology HidingSignaling ManipulationURI GroupsSNMP TrapsTime of Day RulesFGDN GroupsReverse Proxy PolicyURN ProfileRecording ProfileH248 Profile▸ Services▸ Domain Policies

Interworking Profiles

Add

cs2100

avaya-ru

Enterprise Int...

VZ REFER H...

SIP Provider...

Interworking Profiles: SIP Provider Interwk

RenameCloneDelete

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader Manipulation**Advanced**

Record RoutesBoth Sides

Include End Point IP for Context LookupNo

ExtensionsNone

Diversion ManipulationNo

Has Remote SBCYes

Route Response on Via PortNo

Relay INVITE Replace for SIPRECNo

MOBX Re-INVITE HandlingNo

NATing for 301/302 RedirectionYes

DTMF

DTMF SupportNone

Edit

HG; Reviewed:
SPOC 9/26/2023

Avaya DevConnect Application Notes
©2023 Avaya Inc. All Rights Reserved.

94 of 139
WN-CMSMEPSBC-81

8.8. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBC 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 [7] 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**):


- Remove unwanted XML information from SDP in UPDATES from being sent to WorldNet.
- Remove the “+” sign preceding the number from SIP headers before sending to WorldNet.

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

To create the SigMa script to be applied to the Server Configuration Profile corresponding to the Service Provider, on the left navigation pane, select **Configuration Profiles → Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add** (not shown).

- For **Title** enter a name, the name **WorldNet** was chosen in this example.
- Copy the complete script from **Appendix B**.

Signaling Manipulation Editor



Title

Save

```
1 within session "ALL"
2
3 {
4   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
5   {
6
7     //Removes + signs from headers
8     %HEADERS["To"][1].URI.USER.regex_replace("\+", "");
9     %HEADERS["From"][1].URI.USER.regex_replace("\+", "");
10    %HEADERS["Contact"][1].URI.USER.regex_replace("\+", "");
11    %HEADERS["Diversion"][1].URI.USER.regex_replace("\+", "");
12    %HEADERS["P-Asserted-Identity"][1].URI.USER.regex_replace("\+", "");
13
14    //Remove unwanted xml element information from the SDP in SIP messages sent to the Service Provider.
15    remove(%BODY[1]);
16
17   }
18 }
```

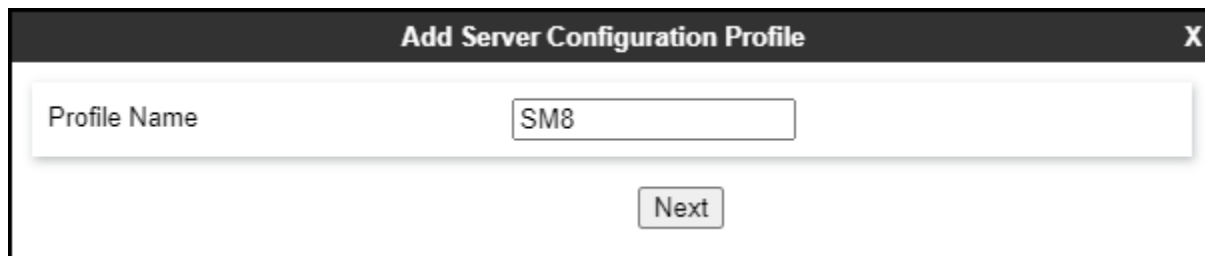

8.9. Server Configuration

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

8.9.1. Server Configuration Profile – Enterprise

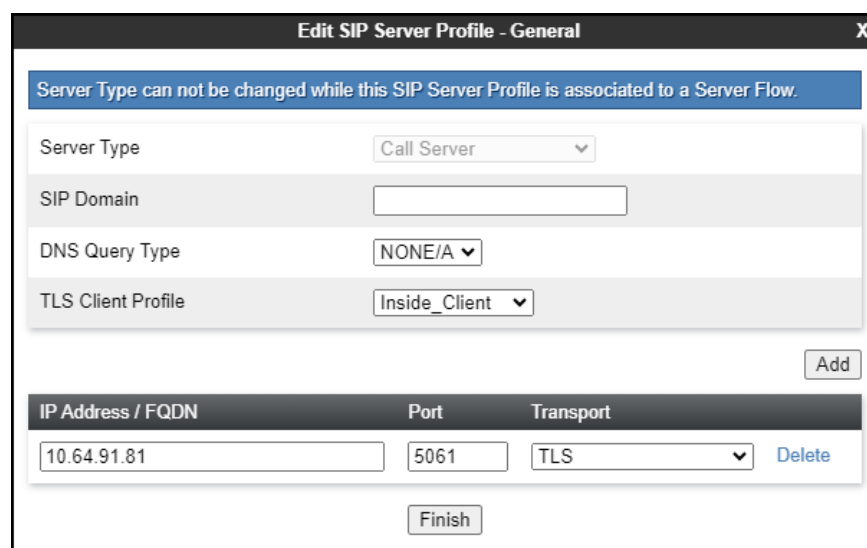
From the **Services** menu on the left-hand navigation pane, select **SIP Servers** and click the **Add** button (not shown) to add a new profile for the Call Server.

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



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "SM8". Below this field is a button labeled "Next".

- 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** (**Section 8.3.3**).
- Click **Next** until the **Add Server Configuration Profile - Heartbeat** tab is reached (not shown).



The screenshot shows a dialog box titled "Edit SIP Server Profile - General" with a close button (X) in the top right corner. A blue banner at the top states: "Server Type can not be changed while this SIP Server Profile is associated to a Server Flow." Below this, there are several fields: "Server Type" (dropdown menu set to "Call Server"), "SIP Domain" (empty text field), "DNS Query Type" (dropdown menu set to "NONE/A"), and "TLS Client Profile" (dropdown menu set to "Inside_Client"). To the right of these fields is an "Add" button. Below these fields is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The first row contains the values "10.64.91.81", "5061", and "TLS". To the right of the table is a "Delete" link. At the bottom of the dialog is a "Finish" button.

- On the **Add Server Configuration Profile - Heartbeat** tab:
 - Check **Enable Heartbeat**.
 - Select **OPTIONS** from the **Method** drop-down menu.
 - **Frequency**: Enter the amount of time (in seconds) between OPTIONS messages that will be sent from the enterprise to the Service Provider Proxy Server, **120** seconds was the value used during the compliance test.
 - Enter the **From URI** and **To URI** fields as shown below using the enterprise domain (e.g., avayalab.com).
- Click **Next** (not shown).

Edit SIP Server Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS ▼
Frequency	120 seconds
From URI	SBC@avayalab.com
To URI	SM@avayalab.com
<div>Finish</div>	

- 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** (required for TLS transport).
 - Select **Enterprise Interwk** from the **Interworking Profile** drop-down menu (Section 8.7.1).
- Click **Finish**.

The screenshot shows a configuration window titled "Edit SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains a list of settings, each with a label and a control element (checkbox or dropdown menu). The settings are as follows:

Setting	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Enterprise Interwk
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

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

8.9.2. Server Configuration Profile – Service Provider

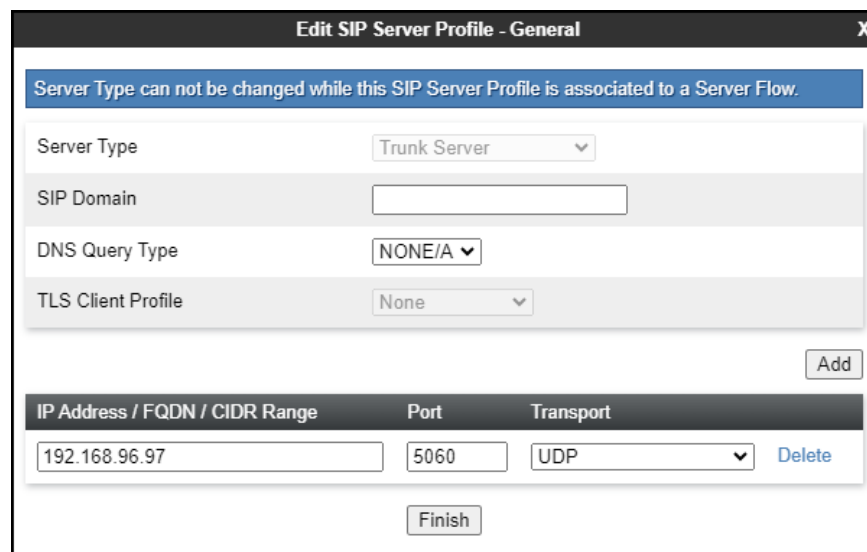
Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

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



The screenshot shows a dialog box titled "Add Server Configuration Profile" with 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 "Worldnet". Below this field is a button labeled "Next".

- 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, enter **192.168.96.97** (WorldNet's SIP proxy IP address). This information was provided by WorldNet.
- Enter **5060** under **Port** and select **UDP** for **Transport**.
- Click **Next**.



The screenshot shows a dialog box titled "Edit SIP Server Profile - General" with a close button (X) in the top right corner. A blue banner at the top states: "Server Type can not be changed while this SIP Server Profile is associated to a Server Flow." Below this, there are several fields: "Server Type" (dropdown menu showing "Trunk Server"), "SIP Domain" (empty text field), "DNS Query Type" (dropdown menu showing "NONE/A"), and "TLS Client Profile" (dropdown menu showing "None"). An "Add" button is located to the right of these fields. Below these fields is a table with three columns: "IP Address / FQDN / CIDR Range", "Port", and "Transport". The table contains one row with the values "192.168.96.97", "5060", and "UDP". A "Delete" link is next to the "UDP" value. At the bottom of the dialog is a "Finish" button.

IP Address / FQDN / CIDR Range	Port	Transport
192.168.96.97	5060	UDP

On the **Add SIP Server Profile - Authentication** tab:

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- Leave **Realm** blank.
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click Next (not shown).

Edit SIP Server Profile - Authentication X

Enable Authentication ☒

User Name

Realm
(Leave blank to detect from server challenge)

Password
(Leave blank to keep existing password)

Confirm Password

Finish

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

On the **Add SIP Server Profile - Registration** tab:

- Check the **Register with All Servers** box.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider. **120** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
 - **From URI**: Use the Avaya SBC public IP address and the enterprise domain, as shown on the screen below.
 - **To URI**: Use WorldNet's proxy IP address, as shown on the screen below.
 - Click **Next** (not shown).

Edit SIP Server Profile - Registration	
Register with All Servers	<input checked="" type="checkbox"/>
Register with Priority Server	<input type="checkbox"/>
Refresh Interval	<input type="text" value="120"/> seconds
From URI	<input type="text" value="10.10.80.53@avayalab.com"/>
To URI	<input type="text" value="192.168.96.97@192.168.96."/>
<input type="button" value="Finish"/>	

- Click **Next** on the **Add SIP Server Profile - Ping** window (not shown).

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

- Uncheck **Enable Grooming** (not required for UDP transport).
- Select **SIP Provider Interwk** from the **Interworking Profile** drop-down menu (**Section 8.7.2**).
- Select the **Worldnetpr** from the **Signaling Manipulation Script** drop down menu (**Sections 8.8 and Appendix B**).
- Click **Finish**.

The screenshot shows a window titled "Edit SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains a list of configuration options, each with a label and a control element (checkbox or dropdown menu). The options are: "Enable DoS Protection" (checkbox), "Enable Grooming" (checkbox), "Interworking Profile" (dropdown menu showing "SIP Provider Interwk"), "Signaling Manipulation Script" (dropdown menu showing "Worldnetpr"), "Securable" (checkbox), "Enable FGDN" (checkbox), "TCP Failover Port" (text input field), "TLS Failover Port" (text input field), "Tolerant" (checkbox), "URI Group" (dropdown menu showing "None"), and "NG911 Support" (checkbox). A "Finish" button is located at the bottom right of the window.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SIP Provider Interwk ▼
Signaling Manipulation Script	Worldnetpr ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼
NG911 Support	<input type="checkbox"/>

Finish

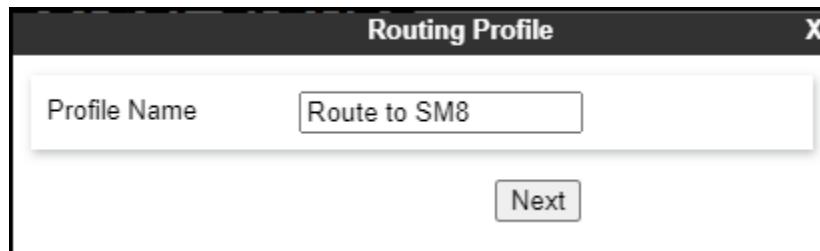
8.10.Routing

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 SBC 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**.



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a label "Profile Name" followed by a text input field containing the text "Route to SM8". Below the input field, there is a button labeled "Next".

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **SIP Server Profile**, select **SM8**. 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**.

Profile : Route to SM8 - Edit Rule
X

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

Add

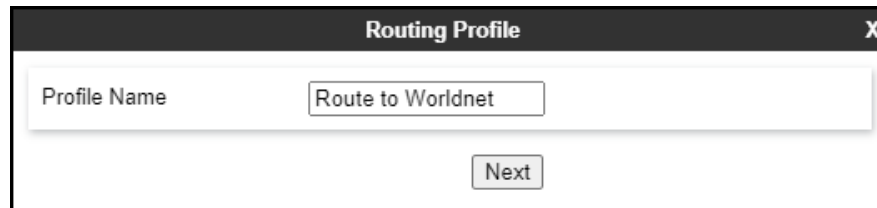
Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				SM8	10.64.91.81:50	None	Delete

Finish

8.10.2. Routing Profile – Service Provider

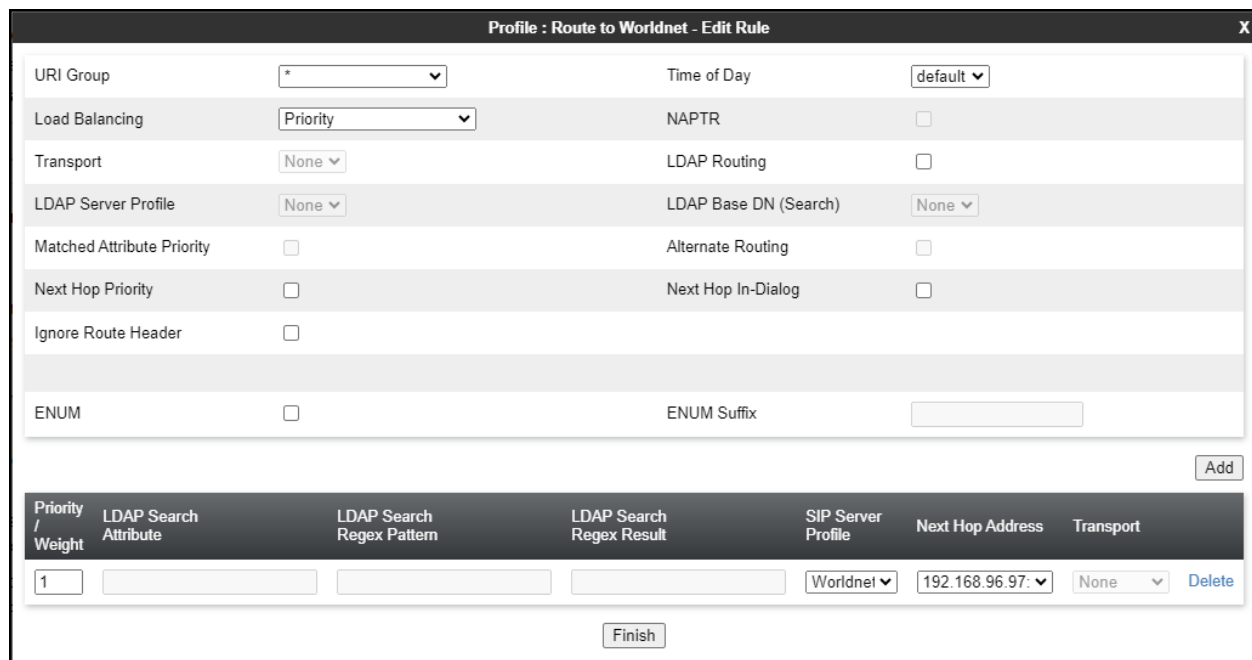
Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

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



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

- Click the **Add** button to enter the next-hop address.
- Under **SIP Server Profile**, select **Worldnet**.
- The **Next Hop Address** is populated automatically with **192.168.96.97:5060 (UDP)**. WorldNet SIP Proxy IP address, Port and Transport, Server Configuration Profile defined in **Section 8.9.2**.
- Click **Finish**



The image shows a dialog box titled "Profile : Route to Worldnet - Edit Rule" with a close button (X) in the top right corner. The dialog contains various configuration options for a routing profile. At the bottom, there is a table with columns for Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, and Transport. The table has one row with values: 1, (empty), (empty), (empty), Worldnet, 192.168.96.97, and None. There is a "Delete" link next to the last row. Below the table is a "Finish" button.

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
*	default	Priority	<input type="checkbox"/>	None	<input type="checkbox"/>	None	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Worldnet	192.168.96.97	None	Delete

8.11.Topology Hiding

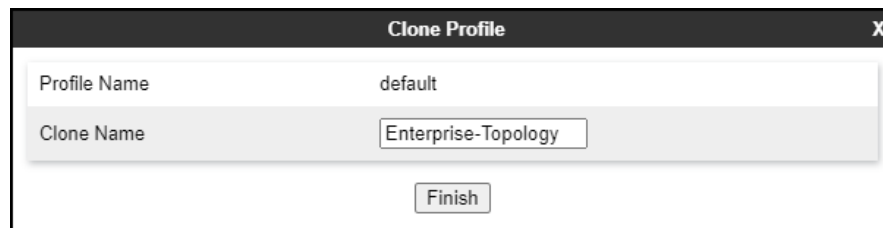
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

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 **Configuration 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 dialog has a light gray background. It contains two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'Enterprise-Topology'. Below these fields is a 'Finish' button.

On the newly cloned **Enterprise-Topology** 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 **avayalab.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**.

Edit Topology Hiding Profile X

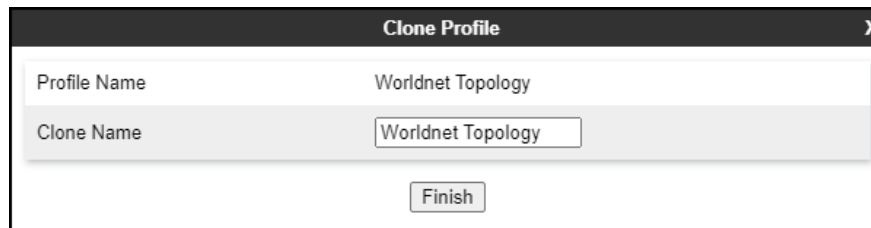
Header	Criteria	Replace Action	Overwrite Value	
Refer-To ▼	IP/Domain ▼	Auto ▼		Delete
To ▼	IP/Domain ▼	Overwrite ▼	avayalab.com	Delete
Referred-By ▼	IP/Domain ▼	Auto ▼		Delete
Record-Route ▼	IP/Domain ▼	Auto ▼		Delete
SDP ▼	IP/Domain ▼	Auto ▼		Delete
From ▼	IP/Domain ▼	Overwrite ▼	avayalab.com	Delete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

Finish

8.11.2. Topology Hiding Profile – Service Provider

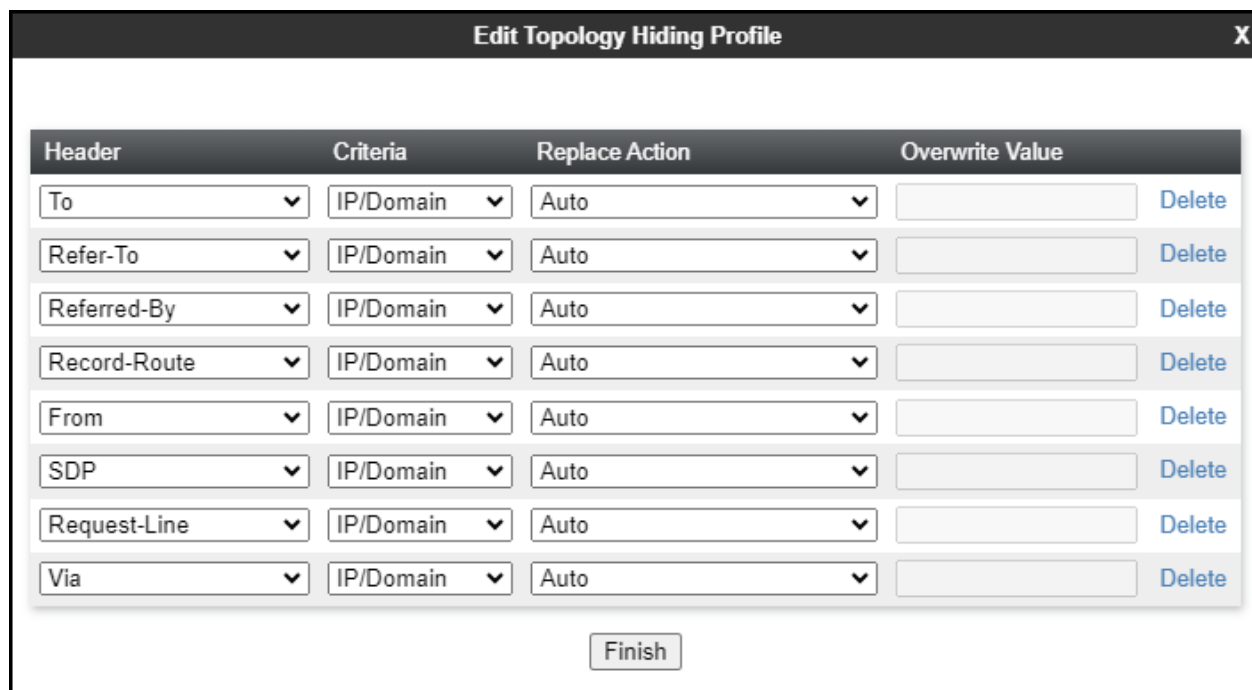
To add the Topology Hiding Profile in the service provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select **default** from the list of pre-defined profiles and click the **Clone** button (not shown).

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



The 'Clone Profile' dialog box has a title bar with 'Clone Profile' and a close button 'X'. It contains two input fields: 'Profile Name' with the value 'Worldnet Topology' and 'Clone Name' with the value 'Worldnet Topology'. Below these fields is a 'Finish' button.

- Default values were used for all other fields.



The 'Edit Topology Hiding Profile' dialog box has a title bar with 'Edit Topology Hiding Profile' and a close button 'X'. It contains a table with the following columns: Header, Criteria, Replace Action, and Overwrite Value. The table has 8 rows, each with a 'Delete' button. Below the table is a 'Finish' button.

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

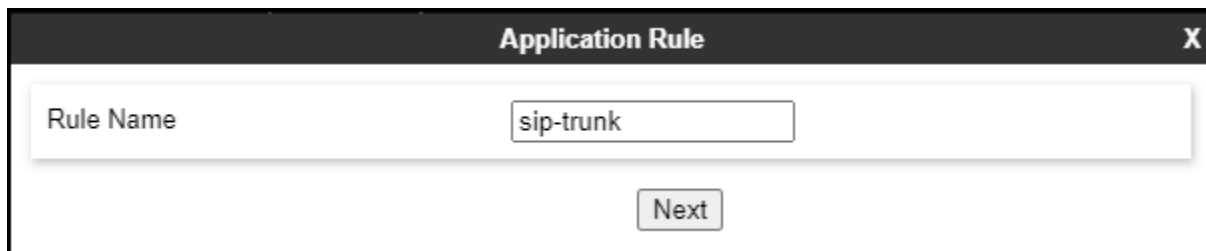
8.12.Domain Policies

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., **sip-trunk**.
- Click **Next**.



The screenshot shows a web-based configuration window titled "Application Rule". It features a close button (X) in the top right corner. The main content area contains a label "Rule Name" and a text input field with the value "sip-trunk". Below the input field is a "Next" button.

- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint**, the value of **200** for Audio was used. 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"/>	200	
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 SBC security product. For the compliance test, one media rule (shown below) was created toward Session Manager and a default-low-med media rule was cloned and 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 **enterprise-med-rule**.
- 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** (not shown).

Media Encryption
X

Audio Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	RTP
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	RTP
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous

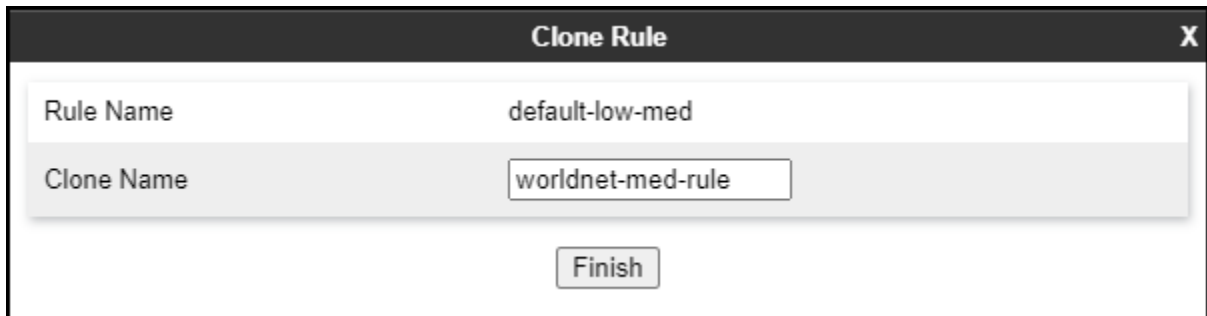
Capability Negotiation	<input checked="" type="checkbox"/>
------------------------	-------------------------------------

Finish

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

To add a media rule in the Service Provider direction, from the menu on the left-hand side, select **Domain Policies → Media Rules** (not shown).

- Select the **default-low-med** rule and click **clone** (not shown).
- Under **Clone Rule** enter the name of the Media Rule, e.g., **worldnet-med-rule**.
- Click **finish**.



Clone Rule		X
Rule Name	default-low-med	
Clone Name	worldnet-med-rule	
<div>Finish</div>		

8.12.3. Signaling Rules

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

To add a signaling rule in the Enterprise direction, from the menu on the left-hand side, select **Domain Policies** → **Signaling Rule** (not shown).

- Select the **default** rule and click **clone** (not shown).
- Under **Clone Rule** enter the name of the Media Rule, e.g., **enterprise-sig-rule** (not shown).
- Click **finish** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE8-90, Alarms, 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 management options, with 'Domain Policies' expanded to show 'Signaling Rules'. The 'enterprise-sig-rule' is selected in the list.

The main content area is titled 'Signaling Rules: enterprise-sig-rule'. It features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a tabbed interface with tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling'. The 'General' tab is active, showing a description field and a 'QoS' section with a 'UCID' dropdown.

The 'Inbound' section contains a table with the following data:

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

The 'Outbound' section contains a similar table:

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

The 'Content-Type Policy' section includes a checkbox for 'Enable Content-Type Checks' (checked), an 'Action' dropdown set to 'Allow', a 'Multipart Action' dropdown set to 'Allow', and an 'Exception List' field.

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

To add a signaling rule in the Service Provider direction, from the menu on the left-hand side, select **Domain Policies → Signaling Rule**.

- Select the **default** rule and click **clone**.
- Under **Clone Rule** enter the name of the Media Rule, e.g., **Worldnet-sig-rule**.
- Click **finish**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: SBCE8-90', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo.

On the left, a sidebar menu lists various management options, with 'Domain Policies' expanded to show 'Signaling Rules'. The 'Signaling Rules' list on the left includes 'default', 'No-Content-T...', 'Vz-trk-sig-rule', 'nw-sig-rule', 'enterprise-sig...', 'Vz-trk-SigRul...', and 'Worldnet-sig...' (highlighted in red).

The main content area is titled 'Signaling Rules: Worldnet-sig-rule'. It features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. A blue bar prompts 'Click here to add a description.' Below this are tabs for 'General' (selected), 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling'. Under the 'General' tab, there are sub-tabs for 'QoS' and 'UCID'.

The configuration is divided into 'Inbound' and 'Outbound' sections, each with a table of settings:

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

The 'Content-Type Policy' section includes:

- Enable Content-Type Checks:** ☒
- Action:** Allow, Multipart Action, Allow
- Exception List:** Exception List

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

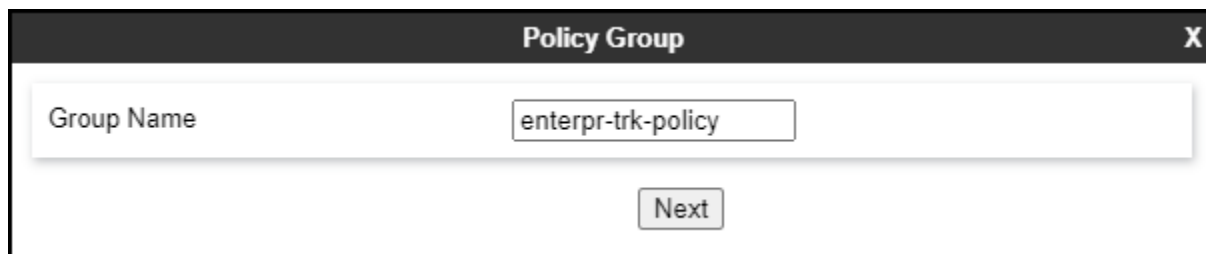
8.13.End Point Policy Groups

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 SBC. 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).

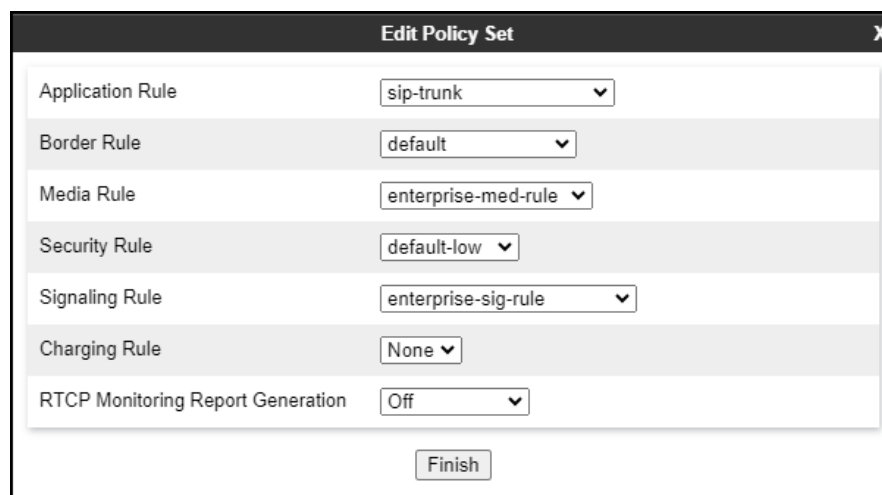
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



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 "enterpr-trk-policy". Below the input field, there is a button labeled "Next".

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

- **Application Rule:** sip-trunk (Section 8.12.1).
- **Border Rule:** default.
- **Media Rule:** enterprise-med-rule (Section 8.12.2).
- **Security Rule:** default-low.
- **Signaling Rule:** enterprise-sig-rule (Section 8.12.3).
- Click **Finish**.

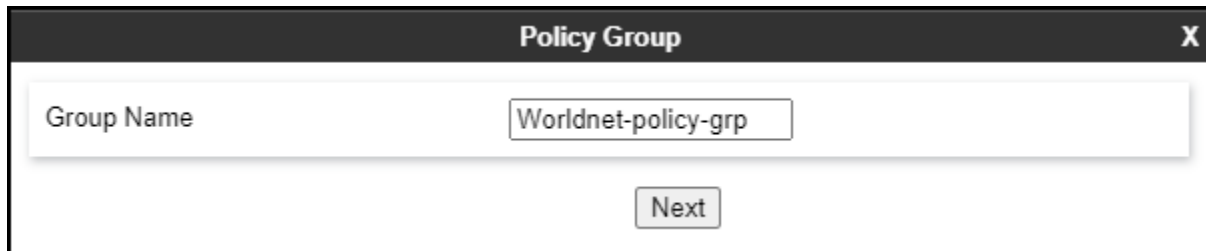


The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains several rows, each with a label and a dropdown menu. The labels are "Application Rule", "Border Rule", "Media Rule", "Security Rule", "Signaling Rule", "Charging Rule", and "RTCP Monitoring Report Generation". The dropdown menus contain the following values: "sip-trunk", "default", "enterprise-med-rule", "default-low", "enterprise-sig-rule", "None", and "Off". At the bottom of the dialog, there is a button labeled "Finish".

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).

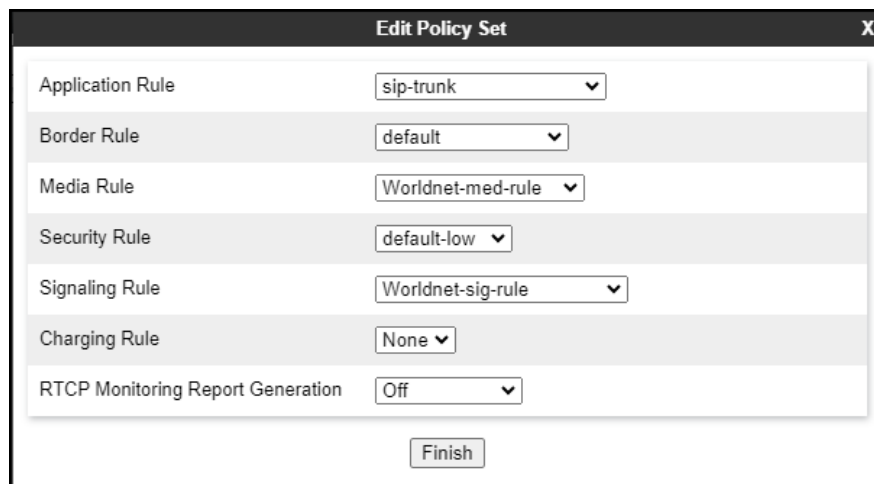
- Enter an appropriate name in the **Group Name**.
- Click **Next**.



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 "Worldnet-policy-grp". Below the input field, there is a button labeled "Next".

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

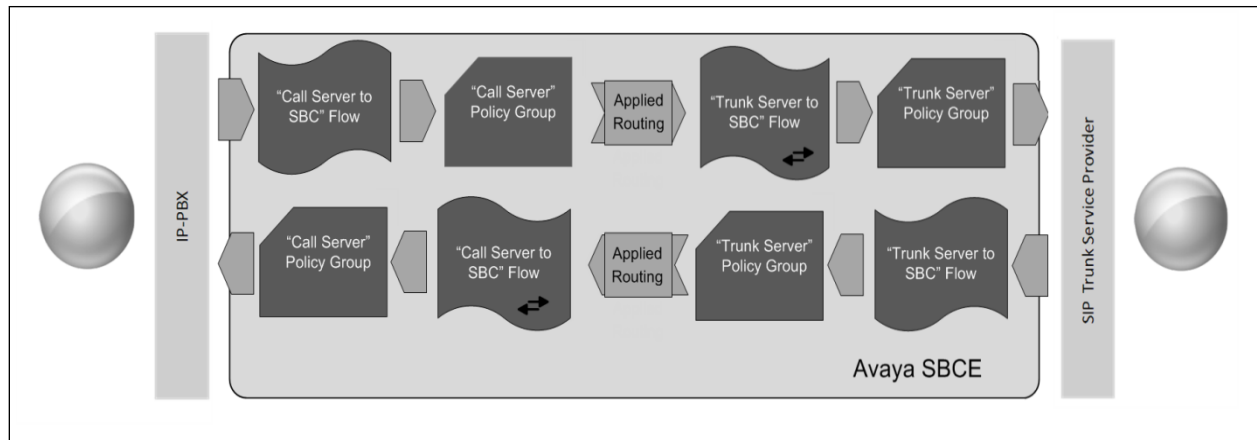
- **Application Rule: sip-trunk** (Section 8.12.1).
- **Border Rule: default**.
- **Media Rule: Worldnet-med-rule** (Section 8.12.2).
- **Security Rule: default-low**.
- **Signaling Rule: Worldnet-sig-rule** (Section 8.12.3).
- Click **Finish**.



The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains several rows, each with a label and a dropdown menu. The labels are "Application Rule", "Border Rule", "Media Rule", "Security Rule", "Signaling Rule", "Charging Rule", and "RTP Monitoring Report Generation". The corresponding dropdown values are "sip-trunk", "default", "Worldnet-med-rule", "default-low", "Worldnet-sig-rule", "None", and "Off". At the bottom of the dialog, there is a button labeled "Finish".

8.14.End Point Flows

When a packet is received by Avaya SBC, 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 SBC 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 – Worldnet to Enterprise Flow

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), set parameters as shown below, click **Finish**. The screen below shows the flow named **Worldnet to Enterprise Flow** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections.

Note – Ensure “Link Monitor from Peer” is checked. Selecting **Link Monitoring from Peer** enables Avaya SBC to send a 200 OK response for a match of the SIP OPTIONS request with a server flow. If you clear **Link Monitoring from Peer** check box, then OPTIONS request will be relayed to the destination server.

Edit Flow: Worldnet to Enterprise Flow X

Flow Name	Worldnet to Enterprise Flow
SIP Server Profile	Worldnet
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside-Sig-50
Signaling Interface	Outside-Sig-B2-53
Media Interface	Outside-Med-B2-53
Secondary Media Interface	None
End Point Policy Group	Worldnet-policy-grp
Routing Profile	Route to SM8
Topology Hiding Profile	Worldnet Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input checked="" type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	

Finish

8.14.2. End Point Flow – Enterprise to Worldnet Flow

A second Server Flow with the name **Enterprise to Worldnet Flow** was similarly created in the Service Provider direction. To create the call flow toward the Service Provider, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown), set parameters as shown below, click **Finish**. The flow uses the interfaces, policies, and profiles defined in previous sections.

Edit Flow: Enterprise to Worldnet FlowX

Flow Name	Enterprise to Worldnet Flow
SIP Server Profile	SM8
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Outside-Sig-B2-53
Signaling Interface	Inside-Sig-50
Media Interface	Inside-Med-50
Secondary Media Interface	None
End Point Policy Group	enterpr-trk-policy
Routing Profile	Route to Worldnet
Topology Hiding Profile	Enterprise-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	
Finish	

9. WorldNet Telecommunications SIP Trunking Service Configuration

To use WorldNet Telecommunications SIP Trunking Service, a customer must request the service from WorldNet Telecommunications using the established sales processes. The process can be started by contacting WorldNet Telecommunications via the corporate web site at:

<https://www.worldnetpr.com/en/voice-service/>

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

WorldNet Telecommunications will provide the following information:

- Trunk registration credentials.
- DID numbers.
- Supported codecs and order of preference.
- Any IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices (firewall).

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:

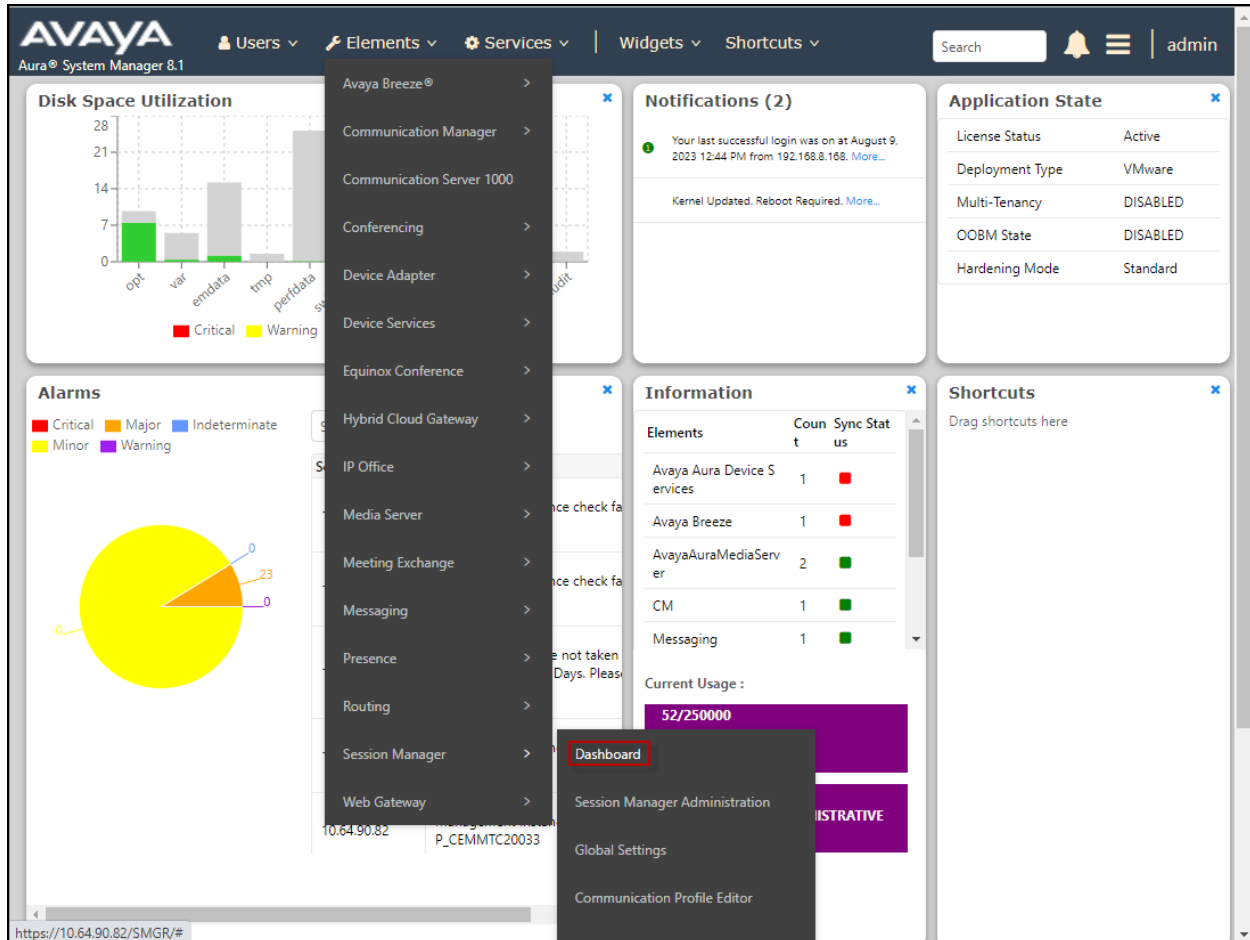
- **list trace station** <extension number>
Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>
Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>
Displays signaling group service state.
- **status trunk** <trunk group 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 **3** alarms out of the **9** Entities defined.

Session Manager Dashboard

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

Session Manager Instances

Service State: [v] Shutdown System: [v] EASG: [v] Clear Logs: [v] As of 3:33 PM

1 Item [Refresh] Show: [All] Filter: Enable

	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Load Factor	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Profile	Version
<input type="checkbox"/>	Session Manager	Core	✓	0/0/0	Up	Accept New Service	0/0/0	2/10	0	2/2	✓	✓	Normal	Enabled	3	10.1.2.0.1012016

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.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and user information (admin). The left sidebar contains a menu with 'Session Manager' selected. The main content area displays a table with 24 items, filtered by 'Enable'. The table columns are: SIP Entity Name, Session Manager IP Address Family, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The table shows 10 rows of data, all with 'UP' Link Status.

SIP Entity Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
CM-TG17	IPv6	fd22:305b:b390:14e6::5	5077	TLS	FALSE	UP	500 Service Unavailable(Signaling Resources Unavailable)	UP
CM-TG16	IPv6	fd22:305b:b390:14e6::5	5076	TLS	FALSE	UP	500 Service Unavailable(Signaling Resources Unavailable)	UP
CM-TG9	IPv4	10.64.91.75	5069	TLS	FALSE	UP	500 Service Unavailable(Signaling Resources Unavailable)	UP
CM-TG4	IPv4	10.64.91.75	5064	TLS	FALSE	UP	500 Service Unavailable(Signaling Resources Unavailable)	UP
CM-TG7	IPv4	10.64.91.75	5067	TLS	FALSE	UP	200 OK	UP
CM-TG3	IPv4	10.64.91.75	5061	TLS	FALSE	UP	200 OK	UP
CM-TG2	IPv4	10.64.91.75	5071	TLS	FALSE	UP	200 OK	UP
CM-TG1	IPv4	10.64.91.75	5081	TLS	FALSE	UP	200 OK	UP
CM-TG5	IPv4	10.64.91.75	5065	TLS	FALSE	UP	500 Service Unavailable(Signaling Resources Unavailable)	UP

The table shows 24 items in total. The bottom of the table has a 'Select : None' dropdown and a pagination bar showing 'Page 2 of 2'.

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 SBC 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: SBCE8-90 **Alarms** Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

EMS Dashboard

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

Dashboard

Information	
System Time	12:00:25 PM MDT Refresh
Version	8.1.3.2-38-22279
GUI Version	8.1.3.2-22253
Build Date	Tue Aug 02 21:33:44 UTC 2022
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	08/09/2023 13:48:32 MDT
Failed Login Attempts	0

Installed Devices

EMS
SBCE8-90

Active Alarms (past 24 hours) **Incidents (past 24 hours)**

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

Device: EMS ▾

Help

EMS

SBCE8-90

AVAYA

Alarms

☒ 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.

Device: SBCE8-90 | Alarms | **Incidents** | Status | Logs | Diagnostics | Users | Settings | Help | Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

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

Dashboard

Information	
System Time	12:00:25 PM MDT Refresh
Version	8.1.3.2-38-22279
GUI Version	8.1.3.2-22253
Build Date	Tue Aug 02 21:33:44 UTC 2022
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	08/09/2023 13:48:32 MDT
Failed Login Attempts	0

Installed Devices

- EMS
- SBCE8-90

Active Alarms (past 24 hours) | **Incidents (past 24 hours)**

The following screen shows the Incident Viewer page.

Device: SBCE8-90 | Help

Incident Viewer

AVAYA

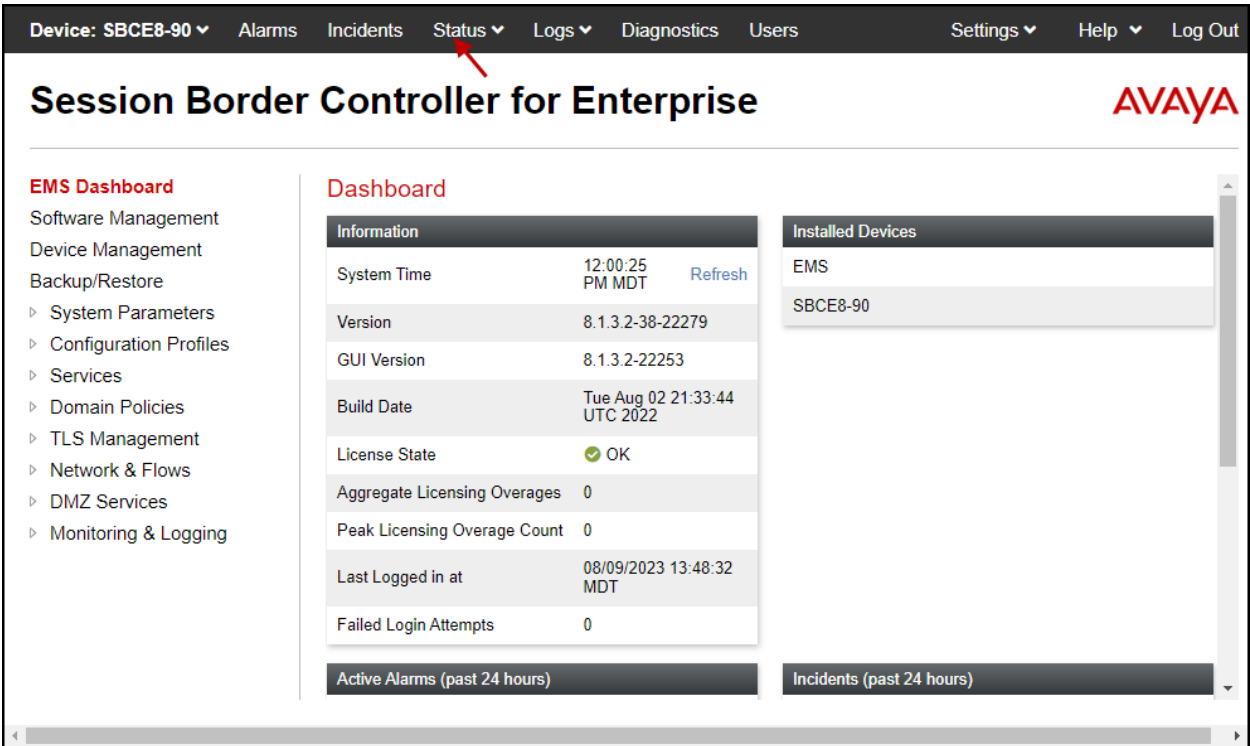
Category: **All** | [Clear Filters](#) | [Refresh](#) | [Generate Report](#)

Summary

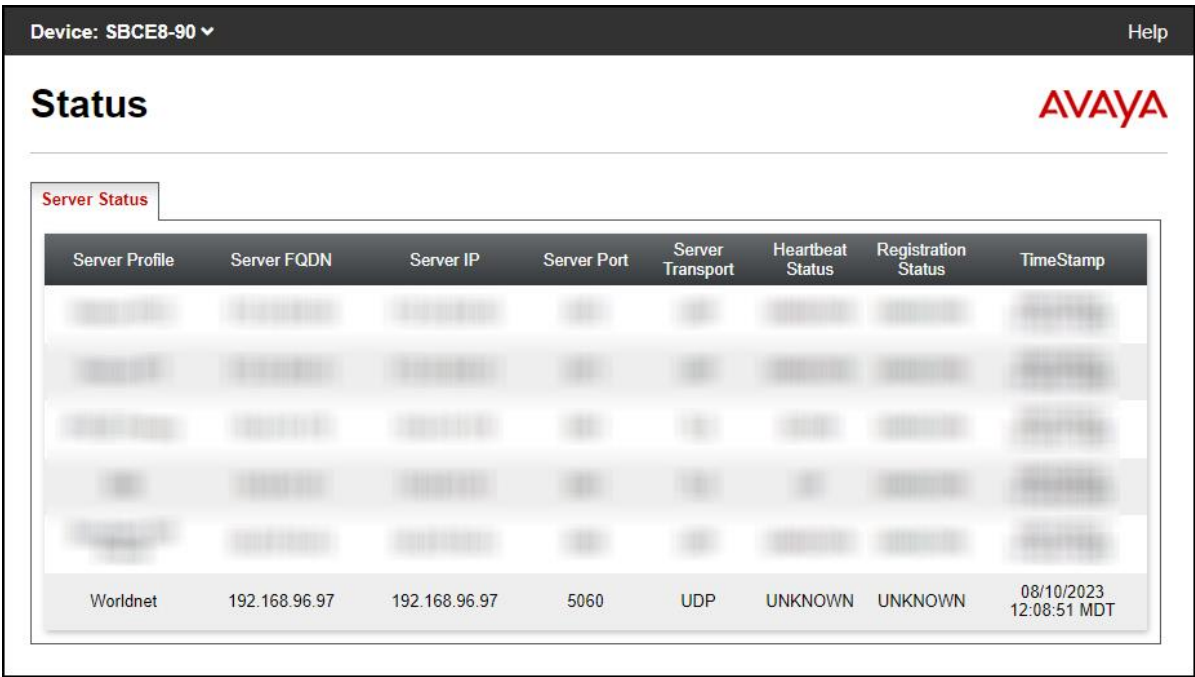
Displaying entries 1 to 15 of 2004.

ID	Date & Time	Category	Type	Cause
845845379823487	Aug 10, 2023 12:05:59 PM	TLS Certificate	TLS Handshake Failed	error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca

Status: This screen provides the registration status of the servers.



The following screen shows the WorldNet Telecommunications server status. Note that the **Registration Status** should show “**REGISTERED**”. It’s showing as “**UNKNOWN**” in the screenshot below because the trunk was down at the far-end (WorldNet).



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

Information	
System Time	12:00:25 PM MDT Refresh
Version	8.1.3.2-38-22279
GUI Version	8.1.3.2-22253
Build Date	Tue Aug 02 21:33:44 UTC 2022
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	08/09/2023 13:48:32 MDT
Failed Login Attempts	0

Installed Devices
EMS
SBCE8-90

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

Device: SBCE8-90

Help

Diagnostics

Full Diagnostic Ping Test

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

Source Device / IP: A1

Destination IP: 10.64.91.81

Ping

Pinging 10.64.91.81

Average ping from 10.64.91.48 [A1] to 10.64.91.81 is 0.188ms.

Additionally, the Avaya SBC 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**.

The screenshot displays the Avaya SBC Enterprise web interface. At the top, a navigation bar includes 'Device: SBCE8-90', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left sidebar lists various management options, with 'Monitoring & Logging' expanded to show 'Trace' as the selected option. The main content area is titled 'Trace: SBCE8-90' and features two tabs: 'Packet Capture' (active) and 'Captures'. The 'Packet Capture Configuration' section includes the following fields: 'Status' (Ready), 'Interface' (B2), 'Local Address' (All), 'Remote Address' (*), 'Protocol' (All), 'Maximum Number of Packets to Capture' (10000), and 'Capture Filename' (Worldnetpr.pcap). 'Start Capture' and 'Clear' buttons are located at the bottom of the configuration area.

Packet Capture Configuration	
Status	Ready
Interface	B2
Local Address <small>IP[:Port]</small>	All :
Remote Address <small>*, *-Port, IP, IP:Port</small>	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	Worldnetpr.pcap

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

Device: SBCE8-90 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging
 SNMP
 Syslog Management
 Debugging
 Trace
 Log Collection

Trace: SBCE8-90

Packet Capture Captures

Last Modified ▾ Descending ▾ Sort Reset Refresh

File Name	File Size (bytes)	Last Modified	
Worldnetpr_20230810122331.pcap	8,192	August 10, 2023 at 12:23:56 PM MDT	Delete
Worldnetpr_Blind_Xfer_20230802085226.pcap	430,080	August 2, 2023 at 8:53:11 AM MDT	Delete
Feature-10b_20230214132433.pcap	978,944	February 14, 2023 at 1:25:33 PM MST	Delete
Feature-10a_20230214131613.pcap	962,560	February 14, 2023 at 1:17:10 PM MST	Delete
Test_20210518082812.pcap	811,008	May 18, 2021 at 8:29:04 AM MDT	Delete
Test_20210323073427.pcap	221,184	March 23, 2021 at 7:34:52 AM MDT	Delete

Also, the **traceSBC** tool can be used to monitor the SIP signaling messages between the Service provider and the Avaya SBC.

11. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, Avaya Aura® Experience Portal 8.1 and Avaya Session Border Controller 8.1, to connect to the WorldNet Telecommunications SIP Trunking service, 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 8.1.x, Issue 6, February 2023.
- [2] *Administering Avaya Aura® Communication Manager*, Release 7.1.3, Issue 10, March 2021.
- [3] *Administering Avaya Aura® System Manager* for Release 8.1.x, Issue 26, February 2023.
- [4] *Deploying Avaya Aura® System Manager in a Virtualized Environment*, Release 8.1.x, Issue 9, February 2023.
- [5] *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in a Virtualized Environment*, Release 8.0.x., Issue 5, December 2019.
- [6] *Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform*, Release 8.1.x, Issue 7, August 2021.
- [7] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 7, January 2023.
- [8] Application Notes for Configuring Remote Workers with Avaya Session Border Controller for Enterprise 8.1 on the Avaya Aura® Platform - *Issue 1.0*.
- [9] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.x, Issue 15, October 2022.
- [10] *Administering Avaya Experience Portal*, Release 8.1.2, Issue 1, October 2022
- [11] *Implementing Avaya Experience Portal on a single server*, Release 8.1.2, Issue 1, October 2022
- [12] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [13] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

13. Appendix A – Avaya Session Border Controller – Refer Handling

One of the capabilities important to the Experience Portal environment is the Avaya SBC 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 SBC. Enabling the Refer Handling option causes the Avaya SBC to intercept and process the REFER and generate a new SIP INVITE messages back to the CPE (e.g., Communication Manager).

Note – If Experience Portal is not included as part of the Avaya Enterprise equipment Refer Handling should not be used, it should be left unchecked/disabled.

Edit the existing **SIP Provider Interwk** Server Interworking Profile to enable Refer Handling.

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

Step 2 - Select the **SIP Provider Interwk** Server Interworking Profile created in **Section 8.7.2** and click **Edit**

- Check **Refer Handling**.
- Select **Finish**.

Editing Profile: SIP Provider Interwk

General

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

180 Handling ☒ None ☐ SDP ☐ No SDP

181 Handling ☒ None ☐ SDP ☐ No SDP

182 Handling ☒ None ☐ SDP ☐ No SDP

183 Handling ☒ None ☐ SDP ☐ No SDP

Refer Handling ☒

URI Group

Send Hold ☐

Delayed Offer ☒

3xx Handling ☐

Diversion Header Support ☐

Delayed SDP Handling ☐

Re-Invite Handling ☐

Prack Handling ☐

Allow 18X SDP ☐

T.38 Support ☒

URI Scheme ☒ SIP ☐ TEL ☐ ANY

Via Header Format ☒ RFC3261
☐ RFC2543

SIPS Required ☒

Mediasec Handling ☐

Finish

Following is the **SIP Provider Interw**k Server Interworking profile after editing.

Device: SBCE8-90 ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

Domain DoS

Server Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

URN Profile

Recording Profile

H248 Profile

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Interworking Profiles

cs2100

avaya-ru

Enterprise Int...

VZ REFER H...

SIP Provider...

Interworking Profiles: SIP Provider Interw

Add

RenameCloneDelete

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

General

Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	Yes
URI Group	None
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
SIPS Required	Yes
Mediasec	No

Edit

HG; Reviewed:
SPOC 9/26/2023

Avaya DevConnect Application Notes
©2023 Avaya Inc. All Rights Reserved.

137 of 139
WN-CMSMEPSBC-81

14. Appendix B – SigMa Scripts

Following is the Signaling Manipulation script that was used in the configuration of the Avaya SBC. Add the scripts as instructed in **Sections 8.8**, enter a name for the script in the Title and copy/paste the entire scripts shown below.

within session "ALL"

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

//Removes + signs from headers
%HEADERS["To"][1].URI.USER.regex_replace("\+", "");
%HEADERS["From"][1].URI.USER.regex_replace("\+", "");
%HEADERS["Contact"][1].URI.USER.regex_replace("\+", "");
%HEADERS["Diversion"][1].URI.USER.regex_replace("\+", "");
%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_replace("\+", "");

//Remove unwanted xml element information from the SDP in SIP messages sent to the Service
Provider.
remove(%BODY[1]);

}
}
```

©2023 Avaya LLC All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.