



DevConnect Program

Application Notes for Configuring Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, Avaya Experience Portal 8.1, Avaya Session Border Controller 10.1 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 10.1, Avaya Aura® Session Manager 10.1, Avaya Aura® Experience Portal 8.1 and Avaya Session Border Controller 10.1 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.....	4
2.2.	Test Results	6
2.3.	Support	8
3.	Reference Configuration.....	9
4.	Equipment and Software Validated	12
5.	Configure Avaya Aura® Communication Manager	13
5.1.	Licensing and Capacity	13
5.2.	System Features.....	14
5.3.	IP Node Names.....	16
5.4.	Codecs	17
5.5.	IP Network Regions	19
5.6.	Signaling Group	20
5.7.	Trunk Group	22
5.8.	Calling Party Information.....	26
5.9.	Inbound Routing.....	27
5.10.	Outbound Routing	28
6.	Configure Avaya Aura® Experience Portal	32
6.1.	Background	32
6.2.	Logging in and Licensing.....	33
6.3.	VoIP Connection	35
6.4.	Speech Servers	37
6.5.	Application References	39
6.6.	MPP Servers and VoIP Settings.....	41
6.7.	Configuring RFC2833 Event Value Offered by Experience Portal	46
7.	Configure Avaya Aura® Session Manager	48
7.1.	System Manager Login and Navigation.....	49
7.2.	SIP Domain	51
7.3.	Locations	52
7.4.	Adaptations.....	56
7.4.1.	Adaptation for Avaya Aura® Communication Manager Extensions	56
7.4.2.	Adaptation for Communication Manager header removal	58
7.5.	SIP Entities.....	59
7.6.	Entity Links	63
7.7.	Routing Policies	65
7.8.	Dial Patterns	67
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	85
8.6.	Signaling Interfaces.....	87
8.7.	Server Interworking.....	89
8.7.1.	Server Interworking Profile – Enterprise	89
8.7.2.	Server Interworking Profile – Service Provider.....	93
8.8.	Signaling Manipulation	96
8.9.	Server Configuration	97
8.9.1.	Server Configuration Profile – Enterprise	97
8.9.2.	Server Configuration Profile – Service Provider	99
8.10.	Routing	103
8.10.1.	Routing Profile – Enterprise.....	103
8.10.2.	Routing Profile – Service Provider	104
8.11.	Topology Hiding.....	105
8.11.1.	Topology Hiding Profile – Enterprise	105
8.11.2.	Topology Hiding Profile – Service Provider.....	107
8.12.	Domain Policies.....	108
8.12.1.	Application Rules	108
8.12.2.	Media Rules.....	110
8.12.3.	Signaling Rules	113
8.13.	End Point Policy Groups	114
8.13.1.	End Point Policy Group – Enterprise	114
8.13.2.	End Point Policy Group – Service Provider.....	115
8.14.	End Point Flows.....	116
8.14.1.	End Point Flow – SP to SM Flow	117
8.14.2.	End Point Flow – SM to SP Flow	118
9.	WorldNet Telecommunications SIP Trunking Service Configuration.....	119
10.	Verification and Troubleshooting	119
10.1.	General Verification Steps.....	119
10.2.	Communication Manager Verification	119
10.3.	Session Manager Verification	120
10.4.	Avaya SBC Verification	123
11.	Conclusion	128
12.	References.....	128
13.	Appendix A – Avaya Session Border Controller – Refer Handling.....	129
14.	Appendix B – SigMa Scripts	132

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 10.1 (Communication Manager), Avaya Aura® Session Manager 10.1 (Session Manager), Avaya Aura® Experience Portal 8.1 (Experience Portal), Avaya Session Border Controller 10.1 (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 (private network side) only. The interface between Avaya systems and WorldNet did not utilize security and encryption capabilities, UDP/RTP was used. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

2.1. Interoperability Compliance Testing

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

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to DID numbers assigned by WorldNet.
Incoming PSTN calls were terminated to the following endpoints: Avaya J129 IP Deskphones (SIP), Avaya 96x1 Series IP Deskphones (SIP), Avaya J179 IP Deskphones (H.323), Avaya one-X® Communicator softphone (H.323 and SIP), Avaya Agent for Desktop (SIP), Avaya Workplace client for Windows (SIP), Avaya 2420 Digital Deskphones 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 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.722 and G.711MU, with G.722 being the preferred codec.
- 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 [9] in the **References** section for additional information on this topic.

The following items were not tested:

- Inbound toll-free calls, 911 calls (emergency), “0” calls (Operator), 0+10 digits calls (Operator Assisted) were not tested.
- T.38 fax: 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 successfully.

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:

- **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 in the SDP from being sent to WorldNet. Refer to **Section 8.8** and **14**.
- **481 Call/Transaction Does Not exist** – After a call from the PSTN to the enterprise is successfully transferred to another PSTN party using the SIP REFER method, WorldNet accepted the SIP REFER messages sent by Communication Manager with “202 Accepted”, which resulted in SIP trunk resources being released with BYE messages, as expected. During the process of releasing the trunk resources, after the acceptance of the SIP REFER message, it was observed that WorldNet sent a “BYE” followed by a “reINVITE”, which resulted in the Avaya SBC responding with “481 Call/Transaction Does Not Exist”. This behaviour had no negative impact on the transferred call, SIP trunk resources were released successfully after the call transfer. It is being mentioned here simply as an observation.
- **Support of E.164 number format** – The SIP trunk to WorldNet was configured as **public** in Communication Manager. When the **public** format is used, 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. Refer to **Section 8.8** and **14**.
- **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 the 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 the public Internet.

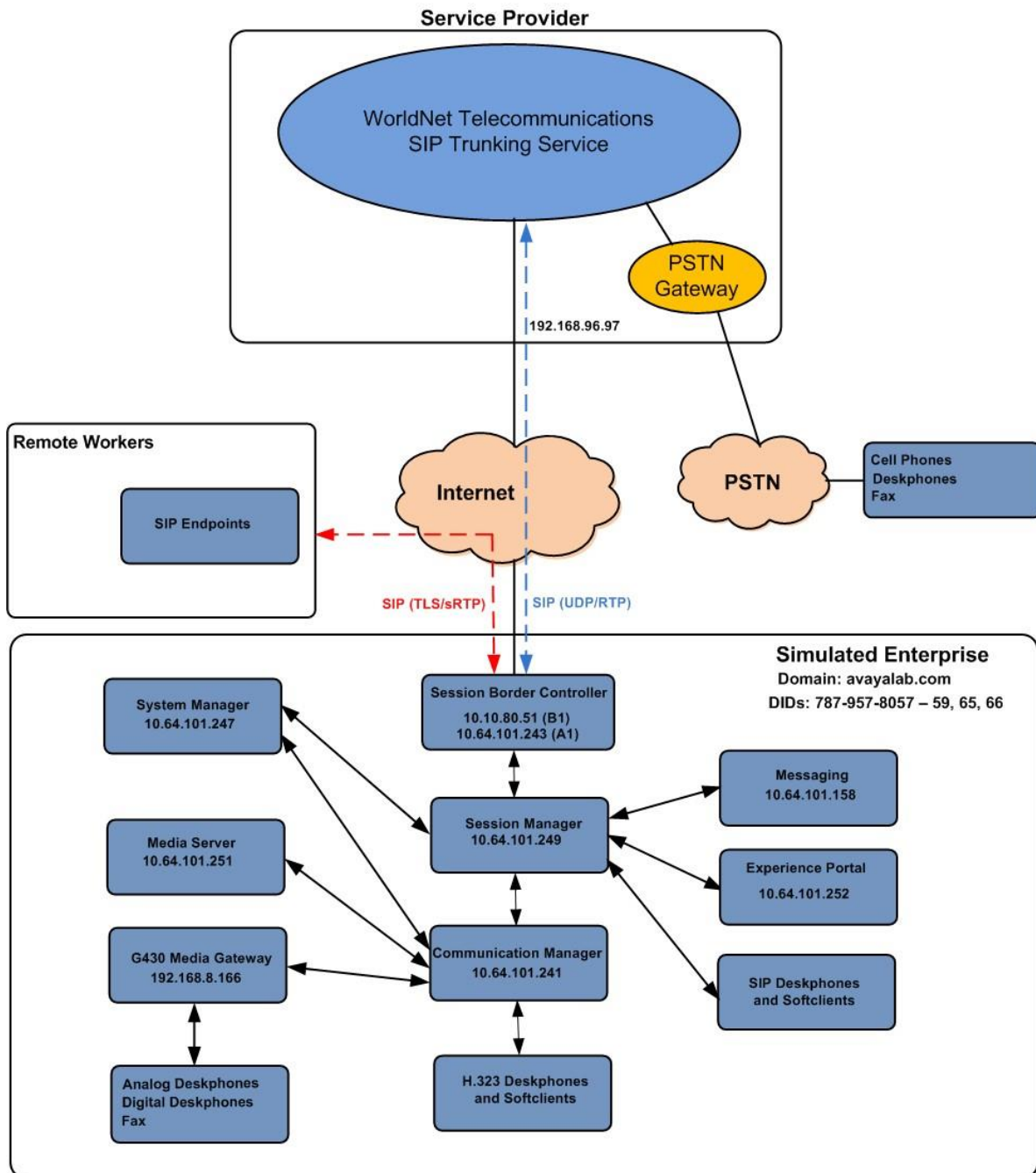


Figure 1: Avaya SIP Enterprise Solution connected to WorldNet Telecommunications SIP Trunking Service.

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 Aura® Media Server.
- Avaya Experience Portal.
- Avaya G430 Media Gateway.
- Avaya 96x1 Series IP Deskphones (SIP).
- Avaya J179 IP Deskphones (H.323).
- Avaya J129 IP Deskphones (SIP).
- Avaya Workplace Client for Windows softphone (SIP).
- Avaya one-X® Communicator (SIP, H.323).
- Avaya Agent for Desktop (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 G430 Media Gateway were utilized during the compliance test. The configuration of the AAMS is not discussed in this document. For more information on the installation and administration of the AAMS in Communication Manager refer to the AAMS documentation listed in the **References** section.

The Avaya 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 Telecommunications 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 WorldNet Telecommunications 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	10.1.3.0.1 (01.0.974.0-27893)
Avaya Aura® Session Manager	10.1.3 (10.1.3.0.1013007)
Avaya Aura® System Manager	10.1.3.0 Build No. - 10.1.0.0.537353 Software Update Revision No: 10.1.3.0.0715713 Feature Pack 3
Avaya Session Border Controller	10.1.2.0 10.1.2.0-64-23285
Avaya Experience Portal	8.1.2.0.0202
Avaya Messaging	10.8 Service Pack 1 (IXM-10.8.20.1406)
Avaya Aura® Media Server	10.1.0 Service Pack 3
Avaya G430 Media Gateway	G430_sw_42_22_0
Avaya 96x1 Series IP Deskphones (SIP)	Version 7.1.15.2.1
Avaya J129 Series IP Deskphones (SIP)	Version 4.1.1.0.7
Avaya J179 IP Deskphones (H.323)	6.8.5.4.10
Avaya Workplace Client for Windows (SIP)	3.34.0.118
Avaya Agent for Desktop (SIP)	2.0.6.26.3001
Avaya one-X® Communicator (SIP, H.323)	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 G430 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 **40000** licenses are available and **230** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

display system-parameters customer-options		Page 2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks:	12000	0
Maximum Concurrently Registered IP Stations:	18000	1
Maximum Administered Remote Office Trunks:	12000	0
Max Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Reg Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	41000	0
Maximum Video Capable IP Softphones:	18000	7
Maximum Administered SIP Trunks:	40000	230
Max Administered Ad-hoc Video Conferencing Ports:	24000	0
Max Number of DS1 Boards with Echo Cancellation:	999	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? n
          Trunk-to-Trunk Transfer: all
        Automatic Callback with Called Party Queuing? n
        Automatic Callback - No Answer Timeout Interval (rings): 3
          Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
          AAR/ARS Dial Tone Required? y

        Music (or Silence) on Transferred Trunk Calls? all
        DID/Tie/ISDN/SIP Intercept Treatment: attendant
        Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
          Automatic Circuit Assurance (ACA) Enabled? n

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

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

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

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

DISPLAY TEXT
                                Identity When Bridging: principal
                                User Guidance Display? n
    Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
    Local Country Code:
    International Access Code:

SCCAN PARAMETERS
    Enable Enbloc Dialing without ARS FAC? n

CALLER ID ON CALL WAITING PARAMETERS
    Caller ID on Call Waiting Delay Timer (msec): 200
```

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and the Session Manager security module (**SM**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip                                     Page 1 of 2
                                     IP NODE NAMES
      Name                IP Address
ASBCE_A1                10.64.101.243
SM                    10.64.101.249
default                0.0.0.0
media_server           10.64.101.251
procr                10.64.101.241
procr6                 ::

( 6 of 6 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```


5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. Enter the corresponding codec in the **Audio Codec** column of the table. WorldNet supports audio codecs **G.722-64K** and **G.711MU**. Under **Media Encryption 1**: select **1-srtp-aescm128-hmac80**, under **Encrypted SRTCP** select **best-effort**.

change ip-codec-set 2Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 2

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.722-64K		2	20
2: G.711MU	n	2	20
3:			
4:			
5:			
6:			
7:			

Media Encryption

Encrypted SRTCP: best-effort

1: 1-srtp-aescm128-hmac80

2: none

3:

4:

5:

On **Page 2**, set the **Fax Mode** to **off** (refer to **Section 2.1**).

change ip-codec-set 2		Page 2 of 2	
IP MEDIA PARAMETERS			
Allow Direct-IP Multimedia? n			
	Mode	Redun-	Packet
FAX	off	dancy	Size (ms)
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 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

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

```
change ip-network-region 2                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 2              NR Group: 2
Location: 1            Authoritative Domain: devconnect.com
Name: SP Region        Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 2           Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048     IP Audio Hairpinning? n
UDP Port Max: 3349
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5    AUDIO RESOURCE RESERVATION PARAMETERS
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 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The following example shows the settings used for the compliance test. It indicates that codec set **2** will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

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

5.6. Signaling Group

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

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and Session Manager. For the compliance test, **tls** was used.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer is a Session Manager.

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

- **Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to **y**.
- **Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to **n**.

- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM**. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5071**.
- Set the **Far-end Network Region** to the IP network region defined for the Service Provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to **y**.
- Default values may be used for all other fields.

change signaling-group 2		Page 1 of 2
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? y	Priority 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: 5071	Far-end Listen Port: 5071	
	Far-end Network Region: 2	
Far-end Domain: devconnect.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? n	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 2 was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

change trunk-group 2		Page 1 of 4	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: Service Provider	COR: 1	TN: 1	TAC: 602
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n	Member Assignment Method: auto	
		Signaling Group: 2	
		Number of Members: 10	

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

```
change trunk-group 2                                     Page 2 of 4
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: 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 **private** 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 2		Page 3 of 4
TRUNK FEATURES		
ACA Assignment? n	Measured: none	
		Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: public	
	UI 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 **y**. With this setting, Communication Manager will 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.
- Verify that **Identity for Calling Party Display** is set to **P-Asserted-Identity**.
- Default values were used for all other fields.

change trunk-group 2	Page 4 of 4
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? 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, four 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.

change public-unknown-numbering 1					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	3			4	Total Administered: 7
4	5			4	Maximum Entries: 9999
5	8			5	Note: If an entry applies to
4	3042	2	7879578057	10	a SIP connection to Avaya
4	3044	2	7879578059	10	Aura(R) Session Manager,
4	3045	2	7879578066	10	the resulting number must
4	5015	2	7879578065	10	be a complete E.164 number.
					Communication Manager automatically inserts a '+' digit in this case.

5.9. Inbound Routing

In general, the “incoming call handling treatment” form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by 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. The screenshot below only shows one DID entry as an example, for the compliance test Session Manager was used to perform digit conversion using an Adaptation (refer to **Section 7.4.1**).

change inc-call-handling-trmt trunk-group 2					Page	1	of	30
INCOMING CALL HANDLING TREATMENT								
Service/ Feature	Number Len	Number Digits	Del	Insert				
public-ntwrk	10	7879578057	10	3042				
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								

5.10.Outbound Routing

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

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 2		
	Dialed String	Total Call Length Type		Dialed String	Total Call Length Type		Dialed String	Total Call Length Type
0		13 udp						
1		4 ext						
2		4 ext						
3		4 ext						
4		4 udp						
5		4 ext						
6		3 dac						
66		2 fac						
7		5 ext						
8		5 ext						
9		1 fac						
*		3 dac						
#		2 dac						

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

```

change feature-access-codes                                     Page 1 of 11
                                FEATURE ACCESS CODE (FAC)
    Abbreviated Dialing List1 Access Code:
    Abbreviated Dialing List2 Access Code:
    Abbreviated Dialing List3 Access Code:
    Abbreviated Dial - Prgm Group List Access Code:
        Announcement Access Code: #7
        Answer Back Access Code:
        Attendant Access Code:
    Auto Alternate Routing (AAR) Access Code: 66
Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
        Automatic Callback Activation:      Deactivation:
    Call Forwarding Activation Busy/DA:      All:      Deactivation:
    Call Forwarding Enhanced Status:      Act:      Deactivation:
        Call Park Access Code:
        Call Pickup Access Code:
    CAS Remote Hold/Answer Hold-Unhold Access Code:
        CDR Account Code Access Code:
        Change COR Access Code:
        Change Coverage Access Code:
    Conditional Call Extend Activation:      Deactivation:
        Contact Closure      Open Code:      Close Code:

```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2, which contains the SIP trunk group to the service provider.

change ars analysis 17							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
170	11	11	deny	fnpa		n	
1700	11	11	deny	fnpa		n	
171	11	11	deny	fnpa		n	
172	11	11	2	fnpa		n	
1720	11	11	2	fnpa		n	
174	11	11	deny	fnpa		n	
175	11	11	deny	fnpa		n	
176	11	11	deny	fnpa		n	
177	11	11	deny	fnpa		n	
1786	11	11	2	fnpa		n	
1787	11	11	2	fnpa		n	
179	11	11	deny	fnpa		n	
180	11	11	deny	fnpa		n	
1800	11	11	2	fnpa		n	
1800555	11	11	deny	fnpa		n	

change ars analysis 411							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
411	3	3	3	svcl		n	
415	6	16	11	intl		n	
443	10	10	2	hnpa		n	
5	7	7	2	hnpa		n	
5005	4	4	2	locl		n	
5006	4	4	2	locl		n	
5007	4	4	2	locl		n	
5008	4	4	2	locl		n	
555	7	7	deny	hnpa		n	
6	7	7	2	hnpa		n	
61	11	11	2	hnpa		n	
611	3	3	2	svcl		n	
61293	11	11	2	hnpa		n	
63	8	8	2	hnpa		n	
631	10	10	2	hnpa		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 2 in the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk:** Set to 1 to ensure 1 + 10 digits are sent to the Service Provider for long distance numbers in the North American Numbering Plan (NANP).
- **Numbering Format:** Set to **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 2													Page 1 of 4	
Pattern Number: 2													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			QSIG			
								Dgts			Intw			
1:	2	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						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 WorldNet Telecommunications SIP Trunking Service. In production, enterprises can develop their own VXML and/or CCXML applications to meet specific customer self-service needs or consult Avaya Professional Services and/or authorized Avaya Business Partners. The development and deployment of VXML and CCXML applications is beyond the scope of these Application Notes.

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

6.2. Logging in and Licensing

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

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

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

The screenshot displays the Avaya Experience Portal Manager web application. At the top, the Avaya logo is on the left, and a welcome message 'Welcome, epadmin' with the last login time 'Last logged in today at 2:27:51 PM MDT' is on the right. Below this is a red navigation bar with 'Avaya Experience Portal 8.1.2 (ExperiencePortal)' on the left and 'Home', 'Help', and 'Logoff' links on the right. A left-hand navigation pane lists various categories: User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration, each with sub-items. The main content area, titled 'Avaya Experience Portal Manager', contains an introduction to the EPM interface, a list of installed components (Media Processing Platform, Email Service, HTML Service, SMS Service) with brief descriptions, and a 'Legal Notice' section. The legal notice includes the 'AVAYA GLOBAL SOFTWARE LICENSE TERMS' and states they were revised on June 1st, 2020. It details the proprietary nature of the software and the agreement between the end user and Avaya Inc. or its affiliates.

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.

Welcome, epadmin
Last logged in Jul 17, 2023 at 8:16:34 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](#) > 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://10.64.101.252:8443/WebLM/LicenseServer	
Last Updated:	Sep 21, 2022 6:49:13 AM MDT	
Last Successful Poll:	Jul 24, 2023 2:26:38 PM 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:	100	
Google Dialogflow Connections:	100	
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:	Jul 24, 2023 2:26:38 PM MDT	
Last Changed:	Mar 7, 2023 1:26:38 PM MST	

Allocations Help

6.3. VoIP Connection

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

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

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

Avaya Experience Portal 8.1.2 (ExperiencePortal)

Welcome, epadmin
Last logged in Jul 17, 2023 at 8:16:34 AM MDT

Expand All | Collapse All

VoIP Connections

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

H.323 **SIP**

Name	Enable	Proxy Transport	Proxy/DNS Server Address	Proxy Server Port	Listener Port	SIP Domain	Maximum Simultaneous Calls
<input type="checkbox"/> Session Manager	Yes	TLS	10.64.101.249	5061	5061	devconnect.com	10

Add **Delete** **Help**

Step 2 - Configure a SIP connection as follows:

- **Name** – Set to a descriptive name (e.g., **Session Manager**).
- **Enable** – Set to **Yes**.
- **Proxy Server Transport** – Set to **TLS**.
- Select **Proxy Servers**, and enter:
 - **Proxy Server Address** = **10.64.101.249** (the IP address of the Session Manager signaling interface defined in **Section 7.5**).
 - **Port** = **5061**
 - **Priority** = **0** (default)
 - **Weight** = **0** (default)
- **Listener Port** – Set to **5061**.
- **SIP Domain** – Set to **devconnect.com** (see **Section 7.2**).

- **Consultative Transfer** – Select **INVITE with REPLACES**.
- **SIP Reject Response Code** – Select **ASM (503)**.
- **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In the reference configuration a value of **10** was used.
- Select **All Calls can be either inbound or outbound**.
- **SRTP Enable** = **Yes**
- **Encryption Algorithm** = **AES_CM_128**
- **Authentication Algorithm** = **HMAC_SHA1_80**
- **RTCP Encryption Enabled** = **No**
- **RTP Authentication Enabled** = **Yes**
- Click on **Add** to add SRTP settings to the **Configured SRTP List**
- Use default values for all other fields.
- Click **Save**.

AVAYA Welcome, epadmin
Last logged in today at 2:27:51 PM MDT

Avaya Experience Portal 8.1.2 (ExperiencePortal) Home ? Help Logoff

Expand All | Collapse All

System Configuration

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: Session Manager

Enable: ☒ Yes ☐ No

Proxy Transport: **TLS**

☒ Proxy Servers ☐ DNS SRV Domain

Address	Port	Priority	Weight	
10.64.101.249	5061	0	0	Remove

[Additional Proxy Server](#)

Listener Port: 5061

SIP Domain: devconnect.com

P-Asserted-Identity:

Maximum Redirection Attempts: 0

Consultative Transfer: ☒ INVITE with REPLACES ☐ REFER

SIP Reject Response Code: ☒ ASM (503) ☐ SES (480) ☐ Custom 503

SIP Timers

T1: 250 milliseconds

T2: 2000 milliseconds

B and F: 4000 milliseconds

Call Capacity

Maximum Simultaneous Calls: 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

Remo

Save Apply Cancel Help

6.4. Speech Servers

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

ASR speech server:

AVAYA Welcome, epadmin
Last logged in today at 2:27:51 PM 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 > Speech Servers

Speech Servers

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

ASR TTS

	Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed ASR Resources	Languages
<input type="checkbox"/>	NuanceASR	Yes	10.64.101.154	Nuance	MRCP V1	4900	10	English(USA) en-US

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

TTS speech server:

The screenshot displays the Avaya Experience Portal 8.1.2 (ExperiencePortal) interface. The top header shows the Avaya logo, a welcome message for 'epadmin', and the last login time. The left sidebar contains a navigation menu with categories like User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration. The main content area is titled 'Speech Servers' and includes a breadcrumb trail: 'You are here: Home > System Configuration > Speech Servers'. Below the title, a description states: 'This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with.' There are two tabs, 'ASR' and 'TTS', with 'TTS' being the active tab. A table lists the configured TTS servers. The table has columns for a checkbox, Name, Enable, Network Address, Engine Type, MRCP, Base Port, Total Number of Licensed TTS Resources, and Voices. One server is listed: 'Nuance' with 'Yes' for Enable, '10.64.101.154' for Network Address, 'Nuance' for Engine Type, 'MRCP V1' for MRCP, '4900' for Base Port, '10' for Total Number of Licensed TTS Resources, and 'English(USA) en-US Jennifer F' for Voices. Below the table are buttons for 'Add', 'Delete', 'Customize', and 'Help'.

AVAYA Welcome, epadmin
Last logged in today at 2:27:51 PM 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 > 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"/>	Nuance	Yes	10.64.101.154	Nuance	MRCP V1	4900	10	English(USA) en-US Jennifer F

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

6.5. Application References

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

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

- **Name** – Set to a descriptive name (e.g., **Test2_APP**).
- **Enable** – Set to **Yes**. This field determines which application(s) will be executed based on their defined criteria.
- **Type** – Select **VoiceXML**, **CCXML**, or **CCXML/VoiceXML** according to the application type.
- **VoiceXML** and/or **CCXML URL** – Enter the necessary URL(s) to access the VXML and/or CCXML application(s) on the application server. In the sample screen below, the Experience Portal test application on a single server is referenced.
- **Speech Servers ASR** and **TTS** – Select the appropriate ASR and/or TTS servers as necessary.
- **Application Launch** – Set to **Inbound**.
- **Called Number** – Enter the number to match against an inbound SIP INVITE message and click **Add**. In the sample configuration illustrated in these Application Notes, the dialed DID number **7879578066** provided by the service provider was used. Inbound calls with this called party number will be handled by the application defined in this section.

AVAYA

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

Change Application

Use this page to change the configuration of an application.

Name:Test2_App

Enable:☒ Yes ☐ No

Type:CCXML

Reserved SIP Calls:☒ None ☐ Minimum ☐ Maximum

Requested:

URI

☒ Single ☐ Fail Over ☐ Load Balance

CCXML URL:http://10.64.101.252/Identifier/mpp/misc/avptestapp/root.ccxml

Verify

Mutual Certificate Authentication:☐ Yes ☒ No

Basic Authentication:☐ Yes ☒ No

ASR Speech Servers

Engine Types

Selected Engine Types

ASR:<None>

Nuance

Nuance

Languages

Selected Languages

<None>

English(USA) en-US

Resources:Acquire on call start and retain

N Best List Length:

Speech Complete Timeout: milliseconds

Speech Incomplete Timeout: milliseconds

Vendor Parameters:

TTS Speech Servers

Voices

Selected Voices

TTS:Nuance

<None>

English(USA) en-US Jennifer F

Application Launch

☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number:

Add

5135628693

13032851998

7879578066

Remove

SIP Header Source:Any

Speech Parameters

Reporting Parameters

Advanced Parameters

Save

Apply

Cancel

Help

6.6. MPP Servers and VoIP Settings

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

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

The screenshot displays the Avaya Experience Portal 8.1.2 (ExperiencePortal) interface. The top header shows the Avaya logo and the user 'Welcome, epadmin' with a logoff link. 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: 'MPP' with Host Address '10.64.101.252', Network Address (VoIP) '<Default>', Network Address (MRCP) '<Default>', Network Address (AppSvr) '<Default>', Maximum Simultaneous Calls '1', and Trace Level 'Use MPP Settings'. Below the table are 'Add' and 'Delete' buttons. At the bottom, there are tabs 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
MPP	10.64.101.252	<Default>	<Default>	<Default>	1	Use MPP Settings

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

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

AVAYA Welcome, epadmin
Last logged in today at 2:27:51 PM 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: MPP
Host Address: 10.64.101.252
Network Address (VoIP): <Default>
Network Address (MRCP): <Default>
Network Address (AppSvr): <Default>
Maximum Simultaneous Calls: 1
Restart Automatically: ☒ Yes ☐ No

MPP Certificate

```
Owner: C=US,O=Avaya Experience Portal,OU=epm,CN=hg-aep-thornton
Issuer: CN=hg-aep-thornton.avaya.lab.com,OU=EPM CA 1663716251357,O=Avaya
Serial Number: cf1eb5f145c075628238785014fb799b
Signature Algorithm: SHA256withRSA
Version: 3
Valid from: November 1, 2022 9:57:34 AM MDT until November 1, 2032 9:57:34 AM MDT
Certificate Fingerprints
MD5: 9d:d9:5a:3f:46:66:8a:47:5e:f4:5f:e6:20:31:b2:12
SHA: bd:72:0a:d1:8c:89:d1:1e:de:fa:8c:c0:25:41:ba:29:a4:ca:46:98
SHA-256: 9a:93:03:7c:b2:8c:d1:97:4b:72:d2:97:ed:8f:5d:c6:66:39:67:e1:3e:ad:36:e6:d6:28:e3:25:29:01:3b:54
Basic Constraints:
CA: false
Path Len Constraint: undefined
Subject Alternative Names
DNS Name: hg-aep-thornton
IP Address: 10.64.101.252
IP Address: fe80:0:0:0:250:56ff:feab:931d
```

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 2:27:51 PM 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:	<input type="text" value="11000"/>	<input type="text" value="30999"/>
TCP:	<input type="text" value="31000"/>	<input type="text" value="33499"/>
MRCP:	<input type="text" value="34000"/>	<input type="text" value="36499"/>
H.323 Station:	<input type="text" value="37000"/>	<input type="text" value="39499"/>

RTCP Monitor Settings ▼

Host Address:

Port:

VoIP Audio Formats ▼

MPP Native Format:

Codecs ▶

QoS Parameters ▶

Out of Service Threshold (% of VoIP Resources) ▶

Call Progress ▶

Miscellaneous ▶

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

- In the Codecs section set:
 - Set **Packet Time** to **20**.
 - Verify Codecs **G711uLaw** is enabled (check marks). Set the **Offer** and Answer **Order** as shown. In the sample configuration **G711uLaw** is the preferred codec, with **Order 1**. Note that **G711uLaw** is the only codec in the list that is supported by both, Experience Portal and WorldNet.
- Use default values for all other fields.

Step 5 - Click on **Save**.

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: audio/basic

Codecs

Offer

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

Packet Time: 20 milliseconds

G729 Discontinuous Transmission: ☒ Yes ☐ No

Answer

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

G729 Discontinuous Transmission: ☐ Yes ☐ No ☒ Either

G729 Reduced Complexity Encoder: ☐ Yes ☐ No

QoS Parameters

Out of Service Threshold (% of VoIP Resources)

Call Progress

Miscellaneous

Save Apply Cancel Help

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 2:27:51 PM 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 (Jul 24, 2023 2:59:45 PM 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: Jul 24, 2023 2:59:31 PM MDT

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

State Commands

Start Stop Restart Reboot Halt Cancel

Mode Commands

Offline Test Online

Help

Restart/Reboot Options

☒ One server at a time
☐ All servers

HG; Reviewed:
SPOC 10/25/2023

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

47 of 133
WN-CMSMSBC10EP8

7. Configure Avaya Aura® Session Manager

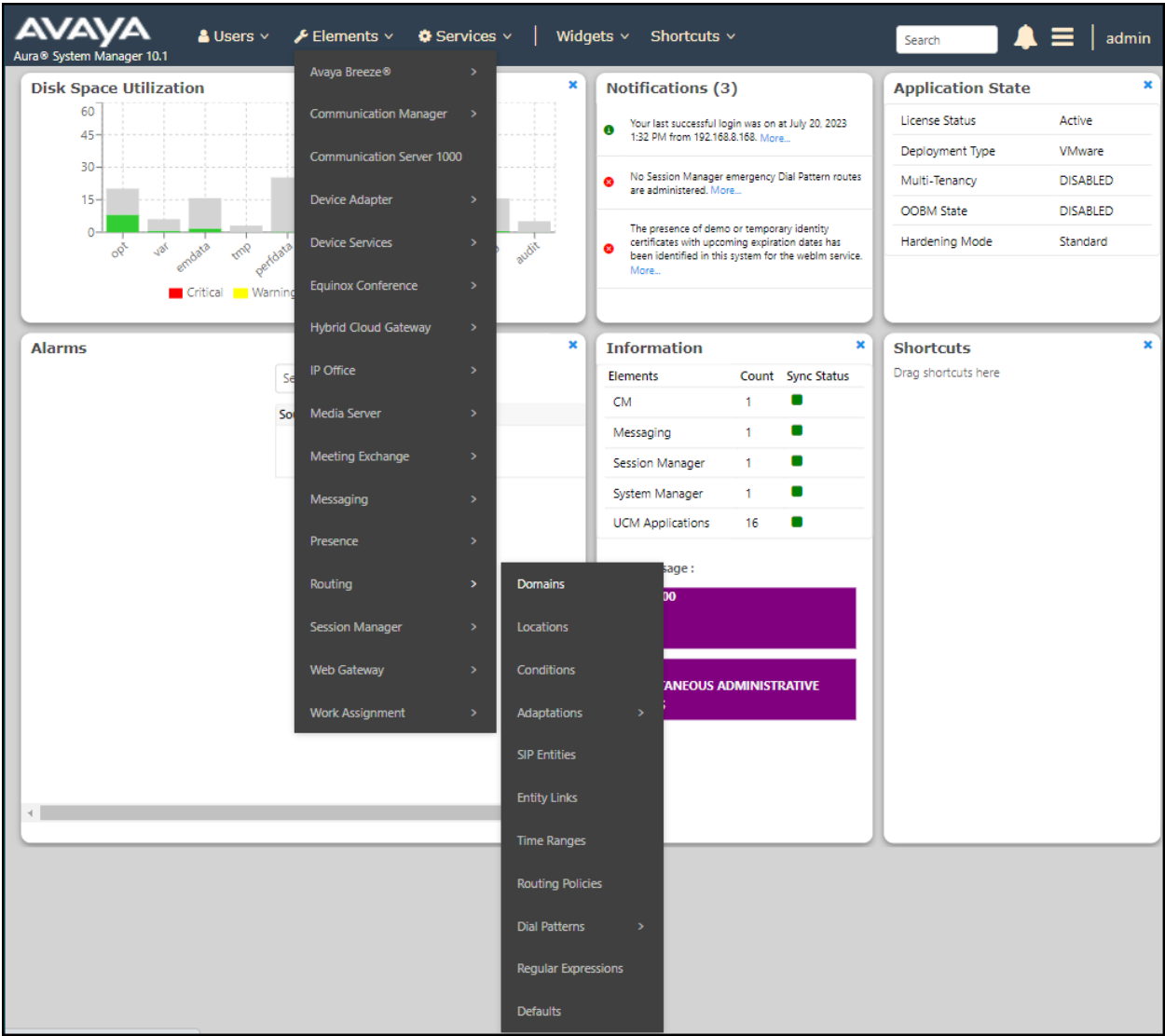
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- 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.
- SIP Entities corresponding to Communication Manager, Session Manager 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 10.1 web interface. The top navigation bar includes the Avaya logo, version information, and various menu items like Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon 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 'devconnect.com' with a type of 'sip'. Below the table, there is a 'Select : All, None' option.

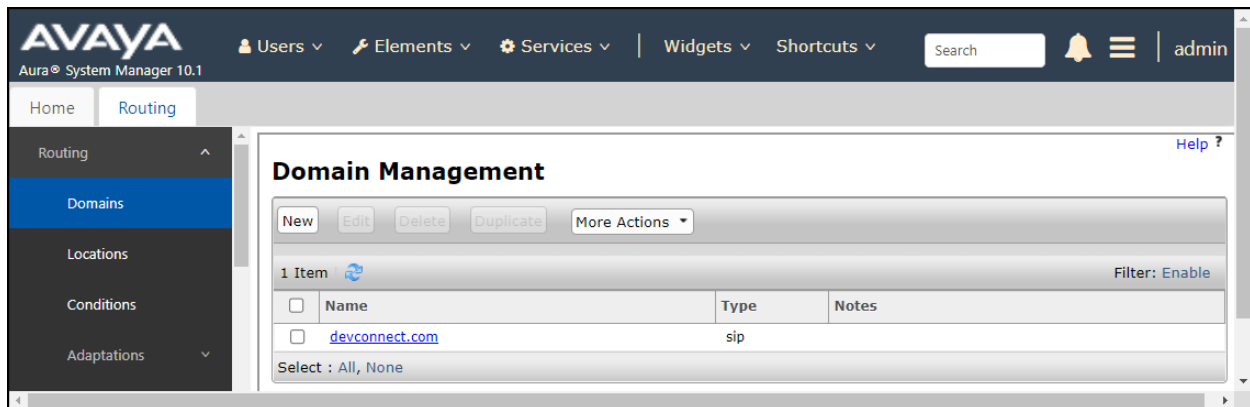
Name	Type	Notes
devconnect.com	sip	

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, **devconnect.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 **Session Manager**. Later, this location will be assigned to the SIP Entity corresponding to Session Manager. Other location parameters (not shown) retained the default values.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The left-hand navigation pane is open, showing the 'Routing' section with 'Locations' selected. The main content area shows the configuration for a location named 'Session Manager'. The 'Name' field is set to 'Session Manager' and the 'Notes' field is set to 'VMware Session Manager'. Below these fields, there are two sections: 'Dial Plan Transparency in Survivable Mode' and 'Overall Managed Bandwidth'. The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox which is unchecked, and two input fields for 'Listed Directory Number' and 'Associated CM SIP Entity'. The 'Overall Managed Bandwidth' section has a 'Managed Bandwidth Units' dropdown set to 'Kbit/sec', and two input fields for 'Total Bandwidth' and 'Multimedia Bandwidth'. At the bottom, there is a checkbox for 'Audio Calls Can Take Multimedia Bandwidth' which is checked.

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

Awaya

Aura System Manager 10.1

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

CommitCancel

Help

General

* Name:

Communication Manager

Notes:

VMware Communication Manager

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 named **Avaya SBC**. 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 'Location Details' configuration page in the Avaya Aura System Manager 10.1 interface. The left sidebar shows a navigation menu with 'Locations' selected. The main content area is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains fields for 'Name' (Avaya SBC) and 'Notes' (VMware Avaya SBC). The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox 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), 'Total Bandwidth' and 'Multimedia Bandwidth' input fields, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'.

AVAYA
Aura® System Manager 10.1

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 <

Location Details Commit Cancel Help ?

General

* Name: Avaya SBC

Notes: VMware Avaya SBC

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

The screenshot displays the Avaya Aura System Manager 10.1 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 (admin) are also present. The left sidebar shows a tree view 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 'Lab Others' and the 'Notes' are 'VMware Lab others'. 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 dropdown for 'Managed Bandwidth Units' set to 'Kbit/sec', and input fields for 'Total Bandwidth' and 'Multimedia Bandwidth'. At the bottom, the 'Audio Calls Can Take Multimedia Bandwidth' checkbox is checked. 'Commit' and 'Cancel' buttons are located in the top right corner of the form area.

AVAYA
Aura® System Manager 10.1

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

Location Details

Commit Cancel Help ?

General

* Name: Lab Others

Notes: VMware Lab others

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. In the reference configuration the following Adaptations were used:

- Calls from WorldNet (**Section Error! Reference source not found.**) - 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.
- Calls to WorldNet (**Section Error! Reference source not found.**) - Modification of SIP messages sent by Communication Manager extensions.
 - Avaya SIP headers not required by WorldNet are removed.

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.

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., **Map-DID-CM-Ext**).
- Select **DigitConversionAdapter** from the **Module Name** drop-down.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar has a 'Routing' section with 'Adaptations' selected. The main content area is titled 'Adaptation Details' and contains a 'General' tab. The form fields are as follows:

- * Adaptation Name:** Map-DID-CM-Ext
- Notes:** Map Inbound DIDs to CM Extensions
- * Module Name:** DigitConversionAdapter (dropdown)
- Type:** digit
- State:** enabled (dropdown)
- Module Parameter Type:** (empty dropdown)
- Egress URI Parameters:** (empty text box)

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

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 **7879578057** in the **Matching Pattern** column.
- Enter **10** in the **Min/Max** columns.

- Enter **10** in the **Delete Digits** column.
- Enter **3042** in the **Insert Digits** column (3042 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 each additional WorldNet DID numbers/Communication manager extensions.

Step 5 - Click on **Commit**.

Note – WorldNet Telecommunications SIP Trunking Service sent 10-digit DID numbers, as shown.

Digit Conversion for Outgoing Calls from SM

Add Remove

4 Items

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify
<input type="checkbox"/>	* 7879578057	* 10	* 10		* 10	3042	destination ▼
<input type="checkbox"/>	* 7879578059	* 10	* 10		* 10	3044	destination ▼
<input type="checkbox"/>	* 7879578065	* 10	* 10		* 10	5015	destination ▼
<input type="checkbox"/>	* 7879578066	* 10	* 10		* 10	3045	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:** Select **Name-Value Parameter**.

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

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

The screenshot displays the Avaya Aura System Manager 10.1 interface. The left sidebar shows a navigation menu with options like Routing, Domains, Locations, Conditions, Adaptations, Regular Expressions, Device Mappings, SIP Entities, Entity Links, and Time Ranges. The 'Adaptations' section is expanded, and the 'CM_Outbound_Header_Removal' adaptation is selected. The main panel shows the 'Adaptation Details' for this adaptation, with the 'General' tab active. The 'Adaptation Name' is 'CM_Outbound_Header_Removal', the 'Module Name' is 'DigitConversionAdapter', the 'Type' is 'digit', and the 'State' is 'enabled'. The 'Module Parameter Type' is 'Name-Value Parameter'. Below this, there is a table with two columns: 'Name' and 'Value'. The table contains one entry with 'Name' as 'eRHdrs' and 'Value' as 'Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View'. The 'Add' button is visible above the table, and the 'Remove' button is visible below the table. The 'Egress URI Parameters' field is empty at the bottom.

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

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 10.1 interface. The top navigation bar includes the Avaya logo, system version (10.1), and menu items: Users, Elements, Services, Widgets, Shortcuts, Search, and admin. The left navigation pane shows the Routing menu expanded, with SIP Entities selected. The main content area displays the SIP Entity Details form, which is divided into General and Monitoring sections. The General section includes fields for Name, IP Address, SIP FQDN, Type, Notes, Location, Outbound Proxy, Time Zone, Minimum TLS Version, and Credential name. The Monitoring section includes fields for SIP Link Monitoring and CRLF Keep Alive Monitoring. The form is titled "SIP Entity Details" and has "Commit" and "Cancel" buttons at the top right.

Field	Value
Name	Session Manager
IP Address	10.64.101.249
SIP FQDN	
Type	Session Manager
Notes	VMware Session Manager
Location	Session Manager
Outbound Proxy	
Time Zone	America/Denver
Minimum TLS Version	Use Global Setting
Credential name	
SIP Link Monitoring	Use Session Manager Configuration
CRLF Keep Alive Monitoring	CRLF Monitoring Disabled

The following screen shows the addition of the **CM-TG2** 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 **Map-DID-CM-Ext** 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 10.1 web interface. The left sidebar shows a 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-TG2
- FQDN or IP Address:** 10.64.101.241
- Type:** CM
- Notes:** Used for SP Testing
- Adaptation:** Map-DID-CM-Ext
- Location:** Communication Manager
- 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
- Loop Detection Mode:** Off

Buttons for 'Commit' and 'Cancel' are located at the top right of the form area. A 'Help ?' link is also present.

The following screen shows the addition of the **Avaya SBC** 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 **CM_Outbound_Header_Removal** 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 10.1 web interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 10.1', and various menu items like '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 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows:

Field	Value
Name	Avaya SBC
FQDN or IP Address	10.64.101.243
Type	SIP Trunk
Notes	VMware Avaya SBC
Adaptation	CM_Outbound_Header_Removal
Location	Avaya SBC
Time Zone	America/Denver
SIP Timer B/F (in seconds)	4
Minimum TLS Version	Use Global Setting
Credential name	
Securable	<input type="checkbox"/>
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 **Avaya Experience Portal** SIP Entity:

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

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and tabs for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile icon are also present. The left sidebar shows a navigation menu with 'Routing' selected, and a sub-menu with '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:** Avaya Experience Portal
- * FQDN or IP Address:** 10.64.101.252
- Type:** Voice Portal (dropdown)
- Notes:** SIP Trunk to Avaya Experience Portal
- Adaptation:** (dropdown)
- Location:** Lab Others (dropdown)
- Time Zone:** America/Denver (dropdown)
- * SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting (dropdown)
- Credential name:** (text field)
- Securable:** ☐
- Call Detail Recording:** none (dropdown)

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.

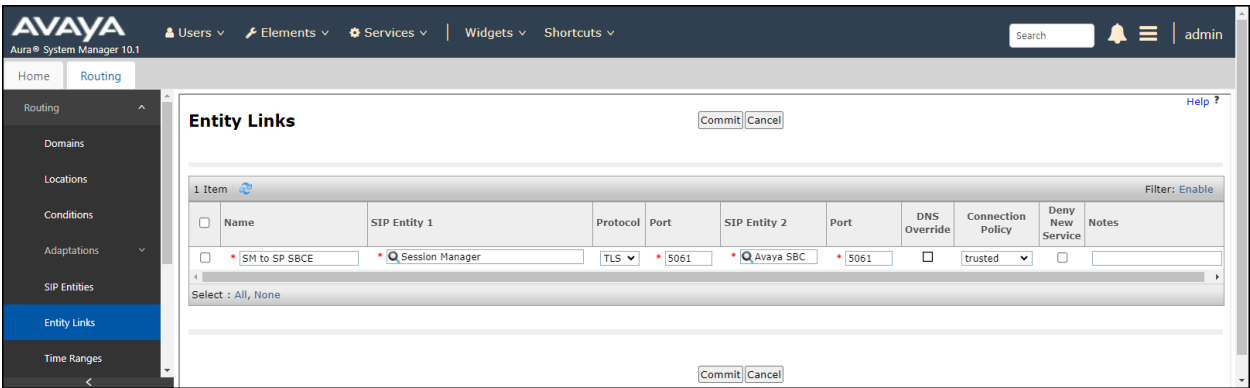
The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**. TLS transport and port **5071** were used.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left navigation pane is expanded to 'Routing' > 'Entity Links'. The main area shows a table with one item, 'SM to CM TG2'. The configuration details are as follows:

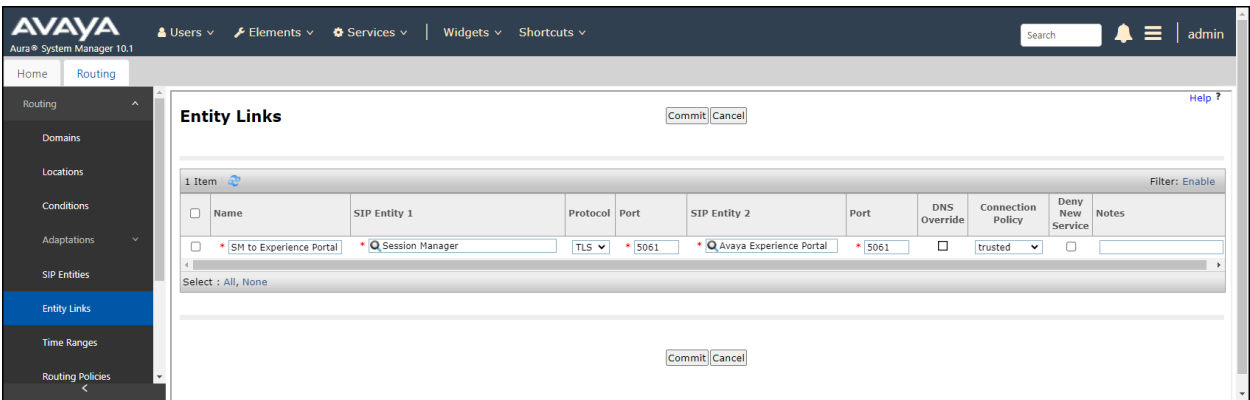
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
SM to CM TG2	Session Manager	TLS	5071	CM-TG2	5071	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

Buttons for 'Commit' and 'Cancel' are visible at the top and bottom of the table.

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



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



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, 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, Avaya SBC and Experience Portal.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The left navigation pane shows the 'Routing' menu expanded, with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- Name:** To CM Trunk 2
- Disabled:** ☐
- Retries:** 0
- Notes:** For inbound calls to CM via Trunk 2

The 'SIP Entity as Destination' section features a 'Select' button and a table with the following data:

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

The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It shows 1 item with the following details:

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

At the bottom, there is a 'Select' dropdown set to 'All, None' and a 'Filter: Enable' link.

AVAYA
Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾admin

Home Routing ×

Routing ^

 Domains

 Locations

 Conditions

 Adaptations ▾

 SIP Entities

 Entity Links

 Time Ranges

Routing Policies

 Dial Patterns ▾

 Regular Expressions

 Defaults

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Avaya Experience Portal	10.64.101.252	Voice Portal	SIP Trunk to Avaya Experince Portal

Time of Day

1 Item ↻
Filter: Enable

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

Select : All, None

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.

AVAYA
Aura® System Manager 10.1

Users | Elements | Services | Widgets | Shortcuts | Search | admin

Home Routing

Routing

- Domains
- Locations
- Conditions
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Origination Dial...

Dial Pattern Details

Commit Cancel

General

* Pattern: 787

* Min: 3

* Max: 36

Emergency Call: ☐

SIP Domain: devconnect.com

Notes:

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

Add Remove

1 Item Filter: Enable

	Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Avaya SBC	VMware Avaya SBC			To CM Trunk 2	0	<input type="checkbox"/>	CM-TG2	For inbound calls to CM via Trunk 2

Select : All, None

[illegible]

The example in this screen shows 11-digit dialed numbers for outbound calls, as follows:

- Beginning with **1**, arriving from the **Communication Manager** location, will use route policy **To SP SBC**, which sends the call out to the PSTN via Avaya SBC and the service provider SIP trunk. The SIP Domain was set to **devconnect.com**. This is for calls originated from Communication Manager stations to the PSTN.
- Beginning with **1**, arriving from the **Lab Others** location, will use route policy **To SP SBC**, which sends the call out to the PSTN via Avaya SBC and the service provider SIP trunk. The SIP Domain was set to **devconnect.com**. This is for calls transfers from Experience Portal to the PSTN.

AVAYA

Aura® System Manager 10.1

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

Origination Dial Pat...

Regular Expressions

Defaults

Dial Pattern Details

Commit Cancel

Help ?

General

* Pattern:

1

* Min:

11

* Max:

11

Emergency Call:

☐

SIP Domain:

devconnect.com ▾

Notes:

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

Add Remove

3 Items

Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>									
<input type="checkbox"/>	Communication Manager	VMware Communication Manager			To SP SBC	0	<input type="checkbox"/>	Avaya SBC	For outbound calls to SP via ASBC
<input type="checkbox"/>	Lab Others	VMware Lab others			To SP SBC	0	<input type="checkbox"/>	Avaya SBC	For outbound calls to SP via ASBC

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 screenshot shows the Avaya Session Border Controller login interface. On the left, the Avaya logo is displayed in red, with the text "Avaya Session Border Controller" below it. On the right, the "Log In" section contains a "Username:" label, a text input field, and a "Continue" button. Below the login fields, there is a "WELCOME TO AVAYA SBC" message, followed by a disclaimer: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." and a consent statement: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, the copyright notice "© 2011 - 2023 Avaya Inc. All rights reserved." is visible.

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

The screenshot displays the Avaya Border Controller web interface. At the top, a navigation bar includes 'Device: EMS', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. Below this, a sidebar on the left lists 'EMS' and 'Avaya_SBC' (highlighted with a red box). The main content area is titled 'Avaya Border Controller' and features the AVAYA logo. The 'EMS Dashboard' section on the left includes links for 'Software Management', 'Device Management', 'System Administration', 'Templates', 'Backup/Restore', and 'Monitoring & Logging'. The central 'Dashboard' area contains an 'Information' table with system details, an 'Installed Devices' list, and sections for 'Active Alarms (past 24 hours)' and 'Incidents (past 24 hours)'. The URL at the bottom left is 'https://10.64.101.242/sbc/#'.

Information	
System Time	01:13:46 PM EDT Refresh
Version	10.1.2.0-64-23285
GUI Version	10.1.2.0-23278
Build Date	Tue May 16 08:55:42 IST 2023
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	07/21/2023 10:51:08 EDT
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBC

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: Avaya_SBC ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

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	01:15:36 PM EDT Refresh
Version	10.1.2.0-64-23285
GUI Version	10.1.2.0-23278
Build Date	Tue May 16 08:55:42 IST 2023
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	07/21/2023 10:51:08 EDT
Failed Login Attempts	0

Active Alarms (past 24 hours)

Installed Devices

EMS

Avaya_SBC

Incidents (past 24 hours)

8.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named **Avaya_SBC** is shown. The management IP address that was configured during installation is blurred out for security reasons; the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya 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 (SBC) management interface. At the top, a navigation bar includes 'Device: Avaya_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Avaya Session Border Controller' with the AVAYA logo. On the left, a sidebar lists navigation options: EMS Dashboard, Software Management, Device Management (highlighted), Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, and Network & Flows. The main content area is titled 'Device Management' and contains tabs for '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, 'Avaya_SBC', is listed with a blurred management IP, version '10.1.2.0-64-23285', and status 'Commissioned'. Action links for 'Reboot', 'Shutdown', 'Restart Application', 'View', 'Edit', and 'Uninstall' are provided for the device.

Device Name	Management IP	Version	Status
Avaya_SBC	[Blurred]	10.1.2.0-64-23285	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: Avaya_SBC

X

General Configuration

Appliance Name	Avaya_SBC
Box Type	SIP
Deployment Mode	Proxy
HA Mode	No

Management IP(s)

IP #1 (IPv4)	10.64.101.242
--------------	---------------

DNS Configuration

Primary DNS	75.75.75.75
Secondary DNS	75.75.76.76
DNS Location	DMZ
DNS Client IP	10.10.80.51

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	100	200
Advanced Sessions	100	200
Scopia Video Sessions	0	0
CES Sessions	0	0
Transcoding Sessions	100	200
AMR	<input type="checkbox"/>	
Premium Sessions	0	0
CLID	---	
Encryption Available: Yes	<input checked="" type="checkbox"/>	

Network Configuration

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

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

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

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

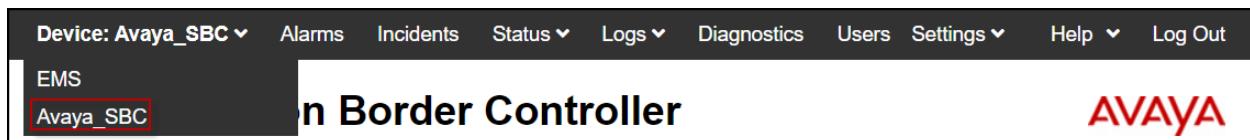
8.3. TLS Management

Note – Testing was done with System Manager signed identity certificates to enable TLS encryption inside of the enterprise (private network side). Identity certificates signed by a 3rd party trusted certificate authority (CA) for enhanced security to enable TLS encryption inside of the enterprise (private network side) can also be used. The procedure to create/obtain the required TLS certificates is outside the scope of these Application Notes and it's not discussed in these Application Notes.

The following procedures show how to create client and server profiles to support TLS encryption inside of the enterprise (private network side) in the Avaya SBC.

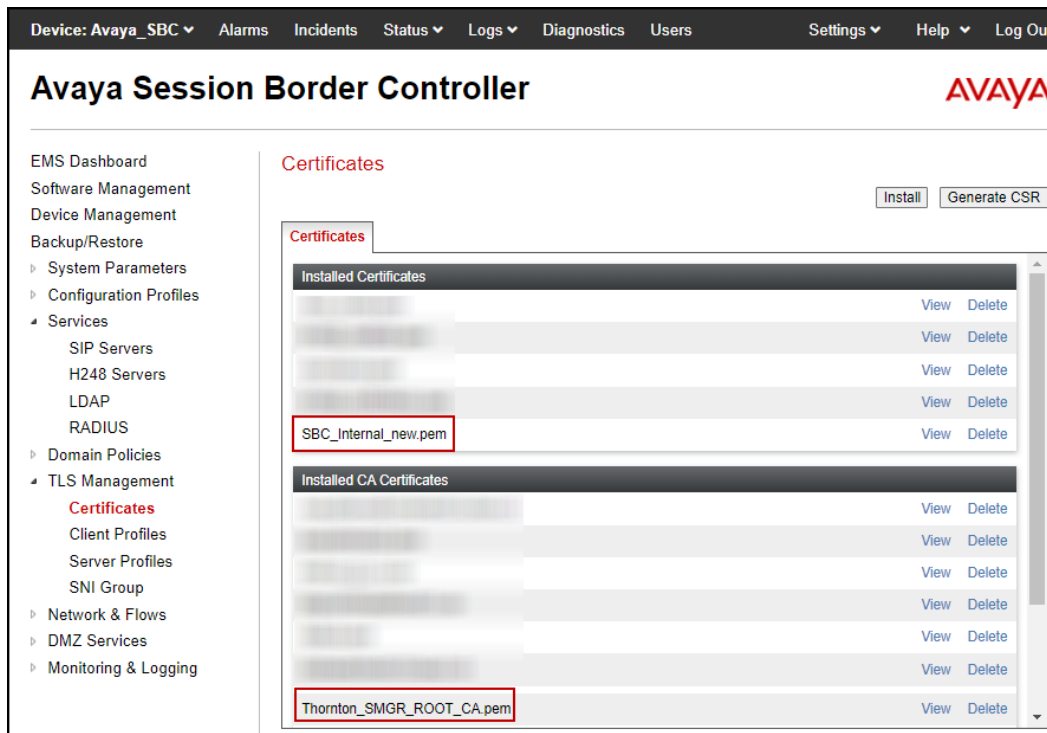
8.3.1. Verify TLS Certificates – Avaya Session Border Controller

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



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

- Verify the System Manager Root CA certificate is present in the **Installed CA Certificates** area, this certificate is required to enable TLS encryption inside of the enterprise (private network side). This Root CA certificate needs to be manually downloaded from System Manager and installed in the Avaya SBC; this Root CA certificate doesn't come pre-loaded in the Avaya SBC. Certificates from a 3rd party trusted Certificate Authority (CA) could be used for TLS encryption inside of the enterprise (private network side) instead of using Avaya System Manager as the Certificate Authority.
- Verify the identity certificate signed by the System Manager CA is present in the **Installed Certificates** area.
- Verify the Private key associated with the identity certificate signed by the System Manager CA is present in the **Installed Keys** area (not shown).



8.3.2. Server Profiles

8.3.2.1 Inside Server Profile

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

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

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

The screenshot shows the 'Edit Profile' dialog box with the following fields and values:

- Profile Name:** SBC_Internal_new
- Certificate:** SBC_Internal_new.pem
- SNI Options:** None
- SNI Group:** None
- Peer Verification:** None
- Peer Certificate Authorities:** AvayaDeviceEnrollmentCAchain.crt, avayaitrootca2.pem, entrust_g2_ca.cer, DigiCertGlobalRootCA.cer
- Peer Certificate Revocation Lists:** (Empty list)
- Verification Depth:** 0

A 'Next' button is located at the bottom right of the dialog box.

The following screen shows the completed **Inside_Server** profile form:

The screenshot displays the Avaya Session Border Controller (SBC) configuration interface. The top navigation bar includes links for Device: Avaya_SBC, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo.

On the left, a sidebar menu lists various configuration options, with 'Server Profiles' highlighted. The 'Server Profiles' section includes a list of profiles: 'Outside_Server', 'Inside_Server', 'Clearcom_O...', 'sbclnternal', 'SBC_Interna...', and 'IPO_Inside_...'. The 'SBC_Interna...' profile is selected.

The main content area shows the configuration for the 'SBC_Interna...' profile. It includes a 'Server Profile' tab and a 'Click here to add a description.' button. The configuration is organized into several sections:

- TLS Profile**
 - Profile Name: SBC_Internal_new
 - Certificate: SBC_Internal_new.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 1.3 ☒ TLS 1.2
 - Ciphers: ☒ Default ☐ FIPS ☐ Custom
 - Value: DEFAULT:ISHA

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

8.3.3. Client Profiles

8.3.3.1 Inside Client Profile

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

- **Profile Name:** enter a descriptive name, **SBC_Internal_new** was used.
- **Certificate:** select the identity certificate, e.g., **SBC_Internal_new.pem**, from the pull-down menu.
- **Peer Verification:** Select **Required** from the pull-down menu.
- **Peer Certificate Authorities:** select the Root CA certificate used to verify the identity certificate received from Session Manager, e.g., **Thornton_SMGR_ROOT_CA.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:

Next

The following screen shows the completed **Inside_Client** profile form:

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

On the left, a sidebar menu lists various management options, with "Client Profiles" highlighted. The main content area is titled "Client Profiles: SBC_Internal_new" and features an "Add" button and a "Delete" button. Below the title, there is a blue bar with the text "Click here to add a description.".

The "Client Profile" configuration form is displayed, containing several sections:

- TLS Profile**:
 - Profile Name: SBC_Internal_new
 - Certificate: SBC_Internal_new.pem
 - SNI: ☐ Enabled
- Certificate Verification**:
 - Peer Verification: Required
 - Peer Certificate Authorities: Thornton_SMGR_ROOT_CA.pem
 - Peer Certificate Revocation Lists: ---
 - Verification Depth: 1
 - Extended Hostname Verification: ☐
- Renegotiation Parameters**:
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**:
 - Version: ☒ TLS 1.3 ☒ TLS 1.2
 - Ciphers: ☒ Default ☐ FIPS ☐ Custom
 - Value: DEFAULT:ISHA

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

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 (**10.64.101.243**) and public (**10.10.80.51**) sides of the Avaya SBC are the ones relevant to these Application Notes.

The screenshot shows the Avaya Session Border Controller web interface. The top navigation bar includes 'Device: Avaya_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Avaya Session Border Controller' and the 'AVAYA' logo. On the left, a sidebar menu lists various management options, with 'Network Management' highlighted under the 'Network & Flows' section. The main content area is titled 'Network Management' and features two tabs: 'Interfaces' and 'Networks'. The 'Networks' tab is active, showing a table with two entries: 'Network_A1' and 'Network_B1'. Each entry lists its gateway, subnet mask, interface, and IP address, with 'Edit' and 'Delete' links for each. An 'Add' button is located in the top right corner of the table area.

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Network_A1	10.64.101.1	255.255.255.0	A1	10.64.101.243, 10.64.101.244, 10.64.101.245	Edit Delete
Network_B1	10.10.80.1	255.255.255.128	B1	10.10.80.23, 10.10.80.24, 10.10.80.51	Edit Delete

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

Device: Avaya_SBC ▾

Alarms

Incidents

Status ▾

Logs ▾

Diagnostics

Users

Settings ▾

Help ▾

Log Out

Avaya Session Border Controller

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

▾ Network & Flows

Network Management

Media Interface

Network Management

Interfaces

Networks

Add VLAN

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

8.5. Media Interfaces

Media Interfaces were created to specify the IP address and port range in which the Avaya 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: Private_med

IP Address: Network_A1 (A1, VLAN 0) 10.64.101.243

Port Range: 35000 - 40000

Finish

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

- Under **IP Address**, the network and IP address to be associated with this interface was selected.
- The **Port Range** was left at the default values of **35000-40000**.
- Click **Finish**.

Edit Media Interface X

Name

IP Address

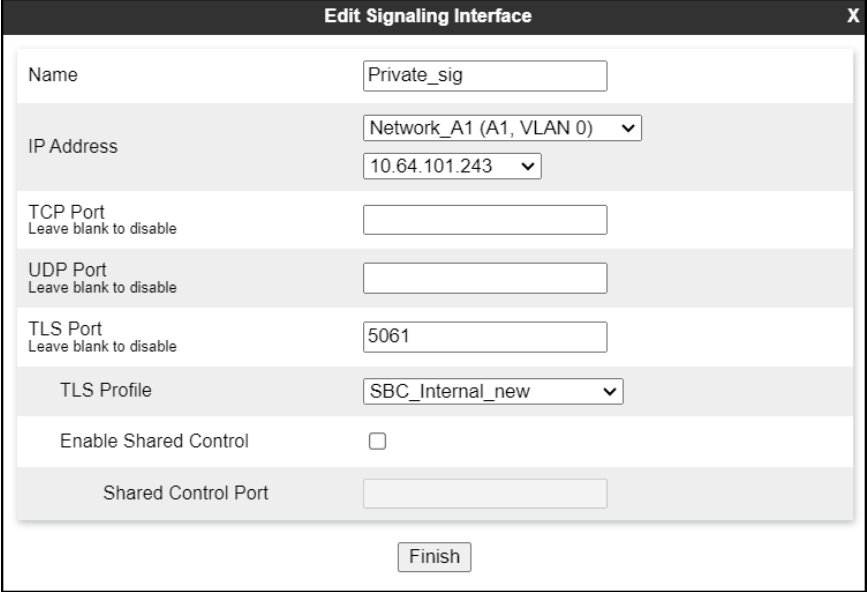
Port Range -

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 8.3.2.1**).
- Click **Finish**.

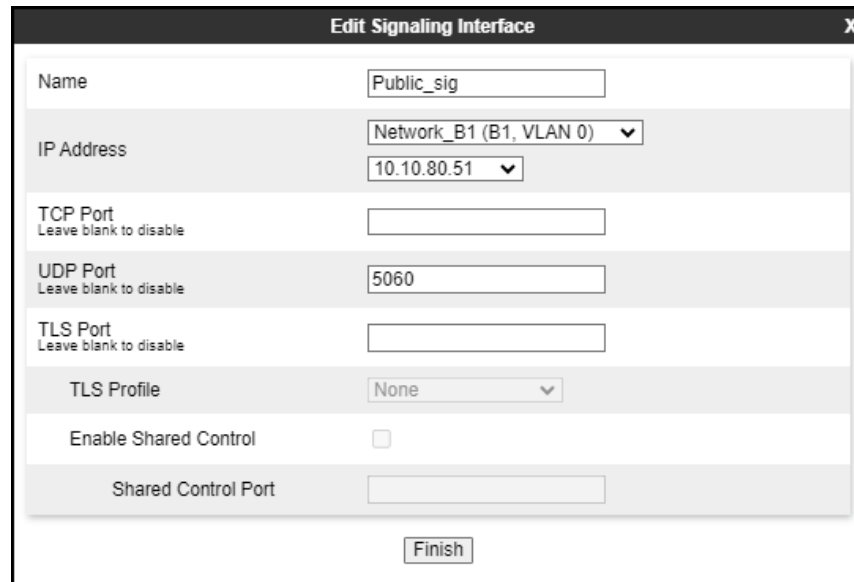


The screenshot shows a web-based configuration window titled "Edit Signaling Interface" with a close button (X) in the top right corner. The form contains the following fields and controls:

- Name:** A text input field containing "Private_sig".
- IP Address:** A section with two dropdown menus. The first dropdown is set to "Network_A1 (A1, VLAN 0)" and the second dropdown is set to "10.64.101.243".
- TCP Port:** A text input field with the label "Leave blank to disable" below it.
- UDP Port:** A text input field with the label "Leave blank to disable" below it.
- TLS Port:** A text input field containing "5061" with the label "Leave blank to disable" below it.
- TLS Profile:** A dropdown menu set to "SBC_Internal_new".
- Enable Shared Control:** A checkbox that is currently unchecked.
- Shared Control Port:** A text input field.
- Finish:** A button at the bottom center of the form.

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

- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5060** for **UDP Port**, since UDP port 5060 is used to listen for signaling traffic from WorldNet in the sample configuration.
- Click **Finish**.



The screenshot shows a configuration window titled "Edit Signaling Interface" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Name:** A text field containing "Public_sig".
- IP Address:** A section with a dropdown menu showing "Network_B1 (B1, VLAN 0)" and a text field below it containing "10.10.80.51".
- TCP Port:** A text field, with the instruction "Leave blank to disable" below it.
- UDP Port:** A text field containing "5060", with the instruction "Leave blank to disable" below it.
- TLS Port:** A text field, with the instruction "Leave blank to disable" below it.
- TLS Profile:** A dropdown menu showing "None".
- Enable Shared Control:** An unchecked checkbox.
- Shared Control Port:** A text field.
- Finish:** A button at the bottom center of the window.

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** (not shown).

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

The left navigation pane lists various configuration options, with 'Configuration Profiles' expanded to show 'Server Interworking'.

The main content area is titled 'Interworking Profiles: avaya-ru'. It features an 'Add' button and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.'

The 'General' tab is selected, showing a table of configuration parameters:

General	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No

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

Clone Profile

X

Profile Name

avaya-ru

Clone Name

Avaya-SM

Finish

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

- On the **General** tab, set **SIPS Required** to **No** (not shown).
- Leave remaining fields with default values.
- Click **Finish** (not shown).

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

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

On the left, a sidebar menu lists various configuration options under 'Configuration Profiles', including 'Server Interworking' which is highlighted. The main content area is titled 'Interworking Profiles: Avaya-SM' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons.

The 'Interworking Profiles' list on the left includes: avaya-ru, OCS-Edge-S..., cisco-ccm, cups, OCS-FrontEn..., **Avaya-SM**, Avaya-IPO, Avaya-CS1000, Avaya-CM, cs2100, and SP-General.

The 'Avaya-SM' profile is selected, and the 'General' tab is active. The 'General' tab settings are displayed in a table:

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	No
Mediasec	No

An 'Edit' button is located at the bottom right of the 'General' tab settings.

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

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

On the left, a sidebar menu lists various management options, with "Configuration Profiles" expanded to show "Server", "Interworking", "Media Forking", "Routing", "Topology Hiding", "Signaling Manipulation", "URI Groups", "SNMP Traps", "Time of Day Rules", "FGDN Groups", "Reverse Proxy Policy", "URN Profile", and "Recording Profile".

The main content area is titled "Interworking Profiles: Avaya-SM". It features a list of profiles on the left, including "avaya-ru", "OCS-Edge-S...", "cisco-ccm", "cups", "OCS-FrontEn...", "Avaya-SM" (highlighted in red), "Avaya-IPO", "Avaya-CS1000", "Avaya-CM", "cs2100", and "SP-General". An "Add" button is located above this list.

On the right, the "Advanced" tab is selected, showing a table of settings for the "Avaya-SM" profile. The table has two columns: the setting name and its value. The settings are:

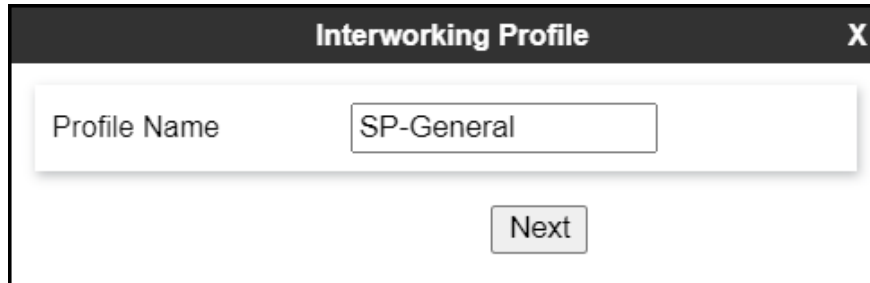
Click here to add a description.	
Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

Below the table, there is a section for "DTMF" settings, showing "DTMF Support" set to "None". An "Edit" button is located at the bottom right of the settings area.

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 dialog box titled "Interworking Profile" with a close button "X" in the top right corner. The dialog contains a "Profile Name" label and a text input field with the value "SP-General". Below the input field is a "Next" button.

- On the **General** tab, set **SIPS Required** to **No** (not shown).
- Leave remaining fields with default values.
- 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: Avaya_SBC ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Avaya Session Border Controller

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

IP/URI Blocklist Profile

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Interworking Profiles: SP-General

Add

Interworking Profiles

avaya-ru

OCS-Edge-S...

cisco-ccm

cups

OCS-FrontEn...

Avaya-SM

Avaya-IPO

Avaya-CS1000

Avaya-CM

cs2100

SP-General

Click here to add a description.

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

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	No
Mediasec	No

Edit

HG; Reviewed:
SPOC 10/25/2023

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

94 of 133
WN-CMSMSBC10EP8

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

Device: Avaya_SBC ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

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 ProfileIP/URI Blocklist Profile▸ Services

Interworking Profiles: SP-General

AddRenameCloneDelete

Interworking Profiles

avaya-ruOCS-Edge-S...cisco-ccmcupsOCS-FrontEn...Avaya-SMAvaya-IPOAvaya-CS1000Avaya-CMcs2100**SP-General**

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader Manipulation**Advanced**

Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	None
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
--------------	------

Edit

HG; Reviewed:
SPOC 10/25/2023

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

95 of 133
WN-CMSMSBC10EP8

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

A single Sigma script was created during the compliance test to correct the following interoperability issues (refer to **Section 2.2**):

- 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) 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**.

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

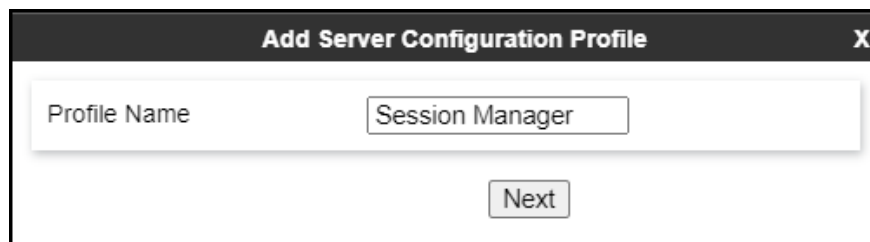
8.9. Server Configuration

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

8.9.1. Server Configuration Profile – Enterprise

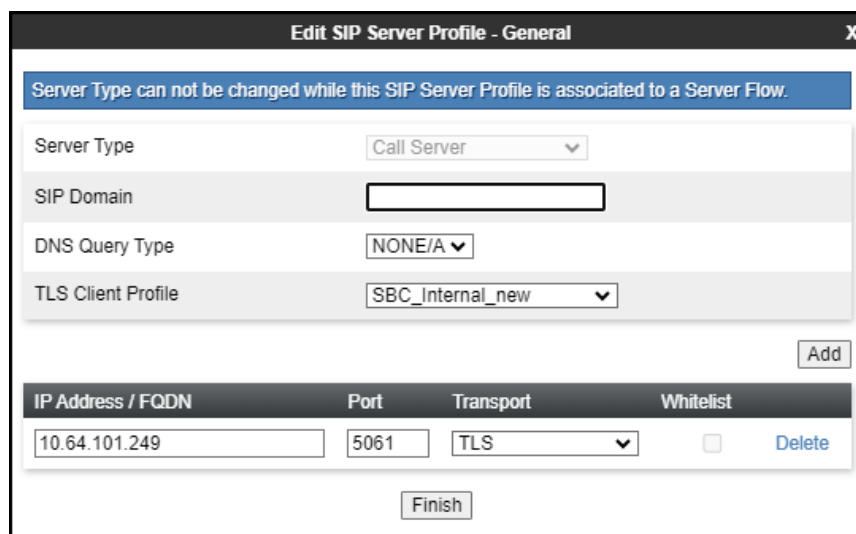
From the **Services** menu on the left-hand navigation pane, select **SIP Servers** and click the **Add** button (not shown) to add a new profile for the Call Server.

- 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" which contains the text "Session Manager". Below this field, there is a "Next" button.

- On the **Edit SIP Server Profile – General** tab select **Call Server** from the drop-down menu under the **Server Type**.
- On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 7.5**).
- Enter **5061** under **Port** and select **TLS** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously created in **Section 7.6**.
- Select a **TLS Profile** (**Section 8.3.3.1**).
- Click **Next** (not shown).



The screenshot shows the "Edit SIP Server Profile - General" configuration page. At the top, there is a warning message: "Server Type can not be changed while this SIP Server Profile is associated to a Server Flow." Below this, there are several configuration fields:

- Server Type:** A dropdown menu set to "Call Server".
- SIP Domain:** An empty text input field.
- DNS Query Type:** A dropdown menu set to "NONE/A".
- TLS Client Profile:** A dropdown menu set to "SBC_Internal_new".

Below these fields is an "Add" button. Underneath, there is a table with the following data:

IP Address / FQDN	Port	Transport	Whitelist
10.64.101.249	5061	TLS	<input type="checkbox"/>

At the bottom of the table, there is a "Delete" button. Below the table is a "Finish" button.

- 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 **Avaya-SM** from the **Interworking Profile** drop-down menu (**Section 8.7.1**).
- Click **Finish**.

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

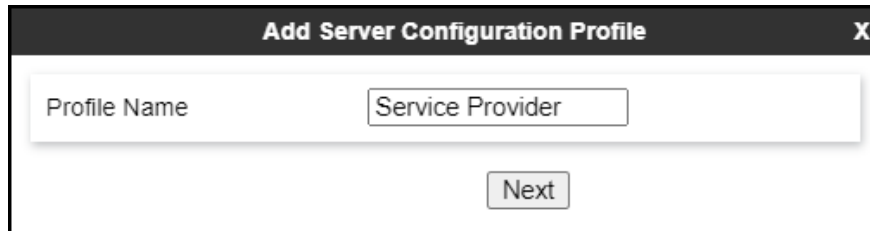
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-SM
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

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

8.9.2. Server Configuration Profile – Service Provider

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

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

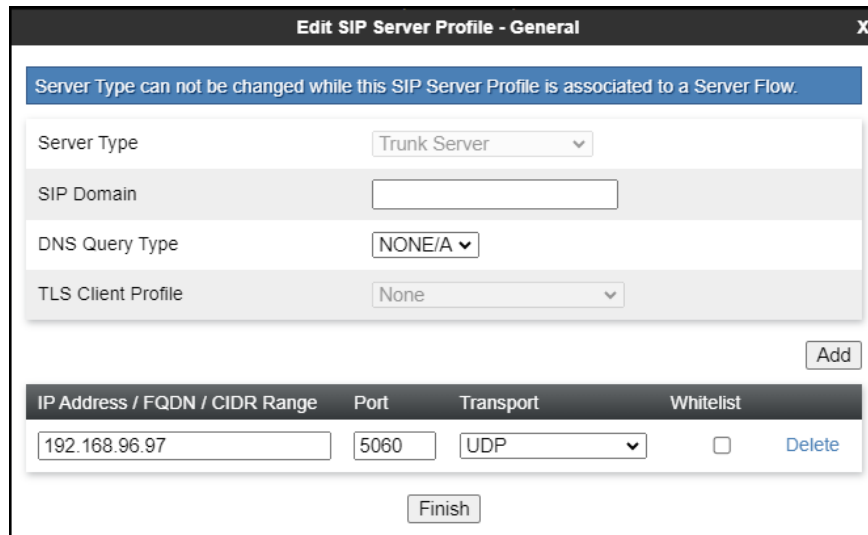


Add Server Configuration Profile X

Profile Name: Service Provider

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 SIP proxy server IP address for signaling). This information was provided by WorldNet.
- Enter **5060** under **Port** and select **UDP** for **Transport**.
- Click **Next** (not shown).



Edit SIP Server Profile - General X

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

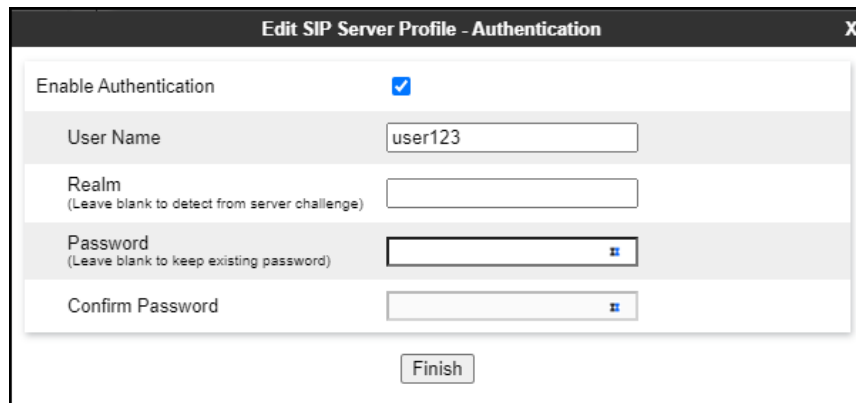
Add

IP Address / FQDN / CIDR Range	Port	Transport	Whitelist
192.168.96.97	5060	UDP	<input type="checkbox"/>

Finish

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	
Enable Authentication	<input checked="" type="checkbox"/>
User Name	<input type="text" value="user123"/>
Realm <small>(Leave blank to detect from server challenge)</small>	<input type="text"/>
Password <small>(Leave blank to keep existing password)</small>	<input type="password"/>
Confirm Password	<input type="password"/>
<input type="button" value="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 (10.10.80.51) and the enterprise domain (devconnect.com), as shown on the screen below.
 - **To URI:** Use WorldNet's proxy IP address (192.168.96.97), 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="10.10.80.51@devconnect.c"/>
To URI	<input type="text" value="192.168.96.97@192.168.96.97"/>
<input type="button" value="Finish"/>	

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

- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).
- On the **Add Server Configuration Profile – Advanced** tab:
 - Check **Uncheck Grooming** (not required for UDP transport).
 - Select **SP-General** from the **Interworking Profile** drop-down menu (**Section 8.7.2**).
 - Select **WorldNet** from the **Signaling Manipulation Script** drop down menu (**Sections 8.8 and Appendix B**).
- Click **Finish**.

Edit SIP Server Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General ▼
Signaling Manipulation Script	WorldNet ▼
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	

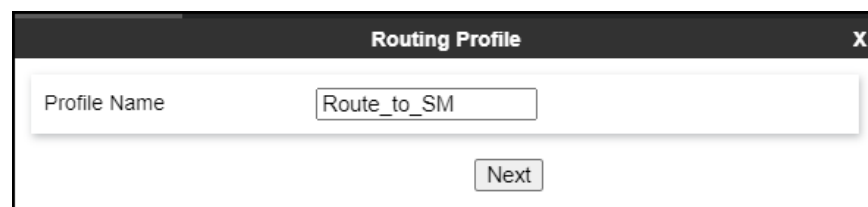
8.10.Routing

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

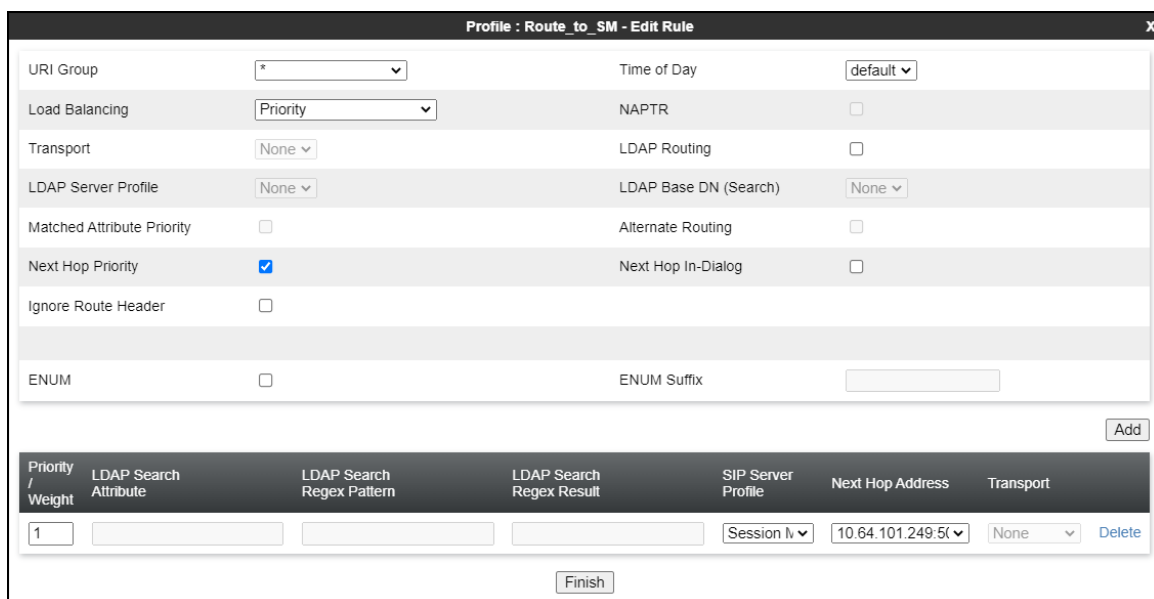
To create the inbound route, select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select **Add** (not shown).

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



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

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **SIP Server Profile**, select **Session Manager**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Session Manager Server Configuration Profile in **Section 8.9.1**.
- Defaults were used for all other parameters.
- Click **Finish**.



The screenshot shows a window titled "Profile : Route_to_SM - Edit Rule" with a close button (X) in the top right corner. The window contains several configuration options and a table of rules.

Configuration options:

- URI Group: * (dropdown)
- Time of Day: default (dropdown)
- Load Balancing: Priority (dropdown)
- NAPTR: ☐
- Transport: None (dropdown)
- LDAP Routing: ☐
- LDAP Server Profile: None (dropdown)
- LDAP Base DN (Search): None (dropdown)
- Matched Attribute Priority: ☐
- Alternate Routing: ☐
- Next Hop Priority: ☒
- Next Hop In-Dialog: ☐
- Ignore Route Header: ☐
- ENUM: ☐
- ENUM Suffix: (text input)

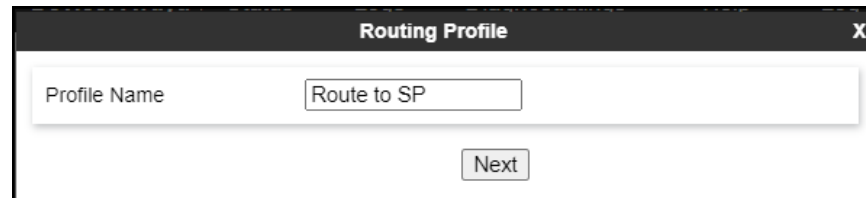
Buttons: Add, Finish

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Session M	10.64.101.249:5060	None	Delete

8.10.2. Routing Profile – Service Provider

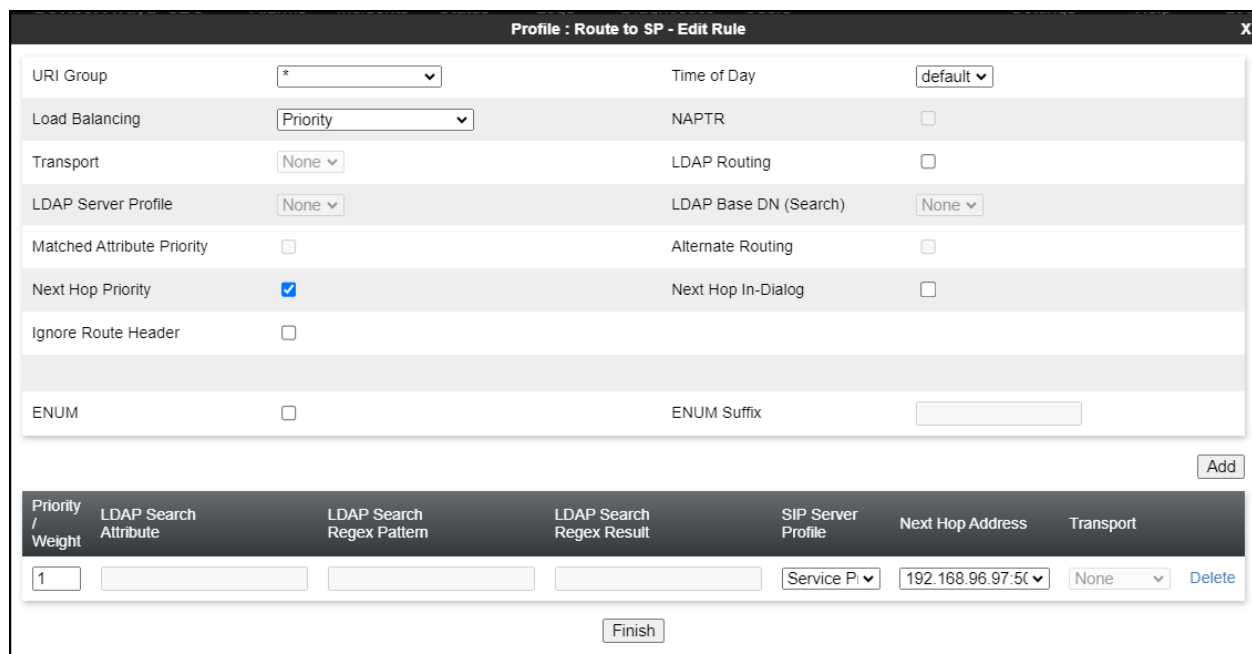
Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

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



A dialog box titled "Routing Profile" with a close button (X) in the top right corner. It contains a text input field labeled "Profile Name" with the value "Route to SP" entered. Below the input field is a "Next" button.

- Under **Load Balancing** select **Priority**.
- Click the **Add** button to enter the next-hop address.
- Under **SIP Server Profile**, select **Service Provider**, under **Priority/Weight** enter **1**.
- The **Next Hop Address** is populated automatically with **192.168.96.97:5061 (UDP)**. WorldNet SIP Proxy IP address for signaling, Port and Transport, Server Configuration Profile defined in **Section 8.9.2**.
- Click **Finish**



A dialog box titled "Profile : Route to SP - Edit Rule" with a close button (X) in the top right corner. It contains a form with various settings:

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	

Below the form is an "Add" button. At the bottom is a table with columns: Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, Transport, and a Delete button.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Service P	192.168.96.97:5061	None	Delete

Below the table is a "Finish" button.

8.11.Topology Hiding

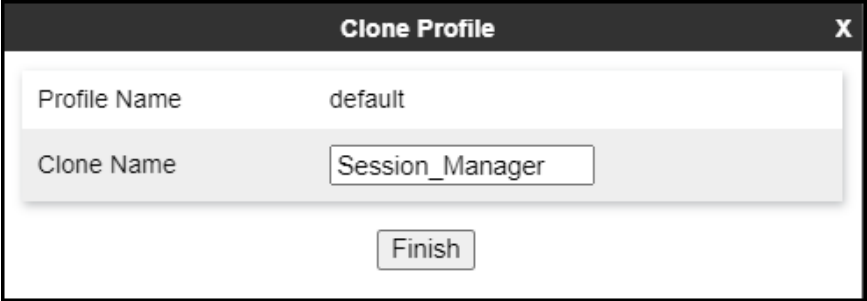
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

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).

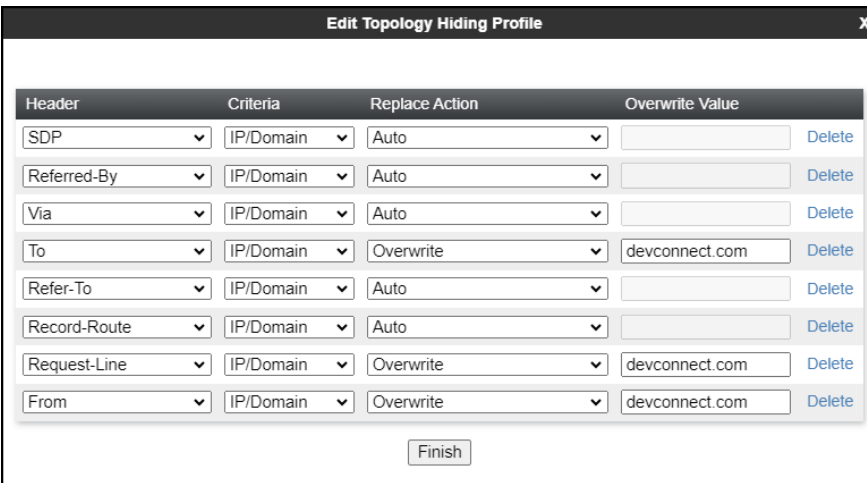
- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



Clone Profile	
Profile Name	default
Clone Name	Session_Manager
<button>Finish</button>	

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

- For the, **From**, **To** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **devconnect.com**, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 7.2**.
- Default values were used for all other fields.
- Click **Finish**.



The screenshot shows a window titled "Edit Topology Hiding Profile" with a close button (X) in the top right corner. Inside the window is a table with four columns: "Header", "Criteria", "Replace Action", and "Overwrite Value". There are nine rows of data, each with a "Delete" link on the right. The "To" and "Request-Line" rows have "devconnect.com" entered in the "Overwrite Value" field, while the others are empty. Below the table is a "Finish" button.

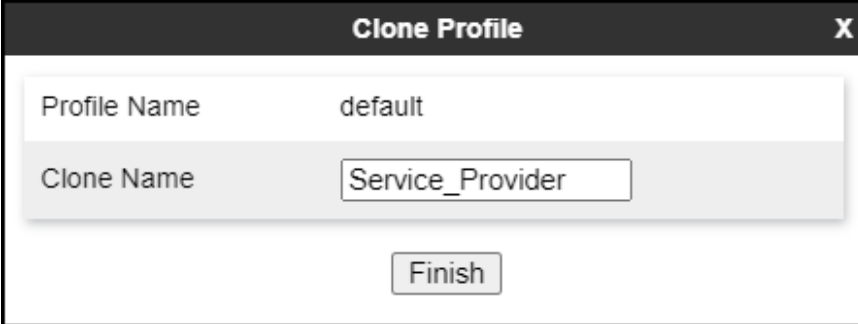
Header	Criteria	Replace Action	Overwrite Value	
SDP	IP/Domain	Auto		Delete
Referred-By	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	devconnect.com	Delete
Refer-To	IP/Domain	Auto		Delete
Record-Route	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	devconnect.com	Delete
From	IP/Domain	Overwrite	devconnect.com	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**. (leave with default values, no changes were made).



Clone Profile		X
Profile Name	default	
Clone Name	<input type="text" value="Service_Provider"/>	
<input type="button" value="Finish"/>		

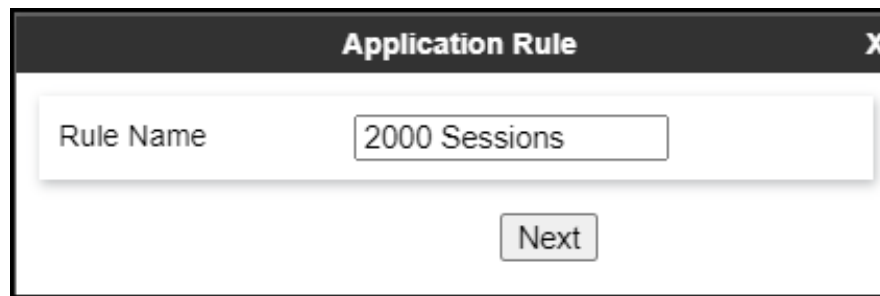
8.12.Domain Policies

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

8.12.1.Application Rules

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

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



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 "2000 Sessions". 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** to recommended values, the value of **2000** for Audio. Repeat for video if needed, 100 sessions each was used for video in the sample configuration.
- Click **Finish**.

Editing Rule: 2000 Sessions

X

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="2000"/>	<input type="text" value="2000"/>
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="100"/>	<input type="text" value="100"/>

Miscellaneous

CDR Support

☒ Off
☐ RADIUS
☐ CDR Adjunct

RADIUS Profile

None ▾

Media Statistics Support

☐

Call Duration

☒ Setup
☐ Connect

RTCP Keep-Alive

☐

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, the existing **default-low-med** was used toward the Service Provider.

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

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter **SM_SRTP**.
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption, if needed.
- Under Miscellaneous verify that **Capability Negotiation** is checked.
- Click **Next**.

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 Leave blank to match any value.	2^
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 Leave blank to match any value.	2^
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).

The existing **default-low-med** rule was used toward the Service provider, shown below.

The screenshot displays the Avaya Session Border Controller (SBC) configuration interface. The top navigation bar includes 'Device: Avaya_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo.

On the left, a sidebar lists various configuration categories: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies (Application Rules, Border Rules, **Media Rules**, Security Rules, Signaling Rules, Charging Rules, End Point Policy Groups, Session Policies), TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging.

The main content area is titled 'Media Rules: default-low-med'. It features an 'Add' button and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active, showing settings for Audio Encryption, Video Encryption, and Miscellaneous.

Audio Encryption	
Preferred Formats	RTP
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption	
Preferred Formats	RTP
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input type="checkbox"/>

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

8.12.3. Signaling Rules

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

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

Avaya Session Border Controller

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▾ Domain Policies
 Application Rules
 Border Rules
 Media Rules
 Security Rules
 Signaling Rules
 Charging Rules
 End Point Policy Groups
 Session Policies
▸ TLS Management
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging

Signaling Rules: default

Add

Clone

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

General Requests Responses Request Headers Response Headers Signaling QoS UCID

Inbound

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

Outbound

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

Content-Type Policy

Enable Content-Type Checks	<input checked="" type="checkbox"/>		
Action	Allow	Multipart Action	Allow
Exception List	Exception List		

Edit

HG; Reviewed:
SPOC 10/25/2023

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

113 of 133
WN-CMSMSBC10EP8

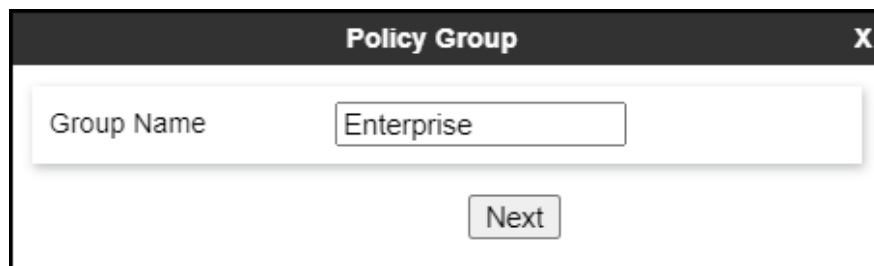
8.13.End Point Policy Groups

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).

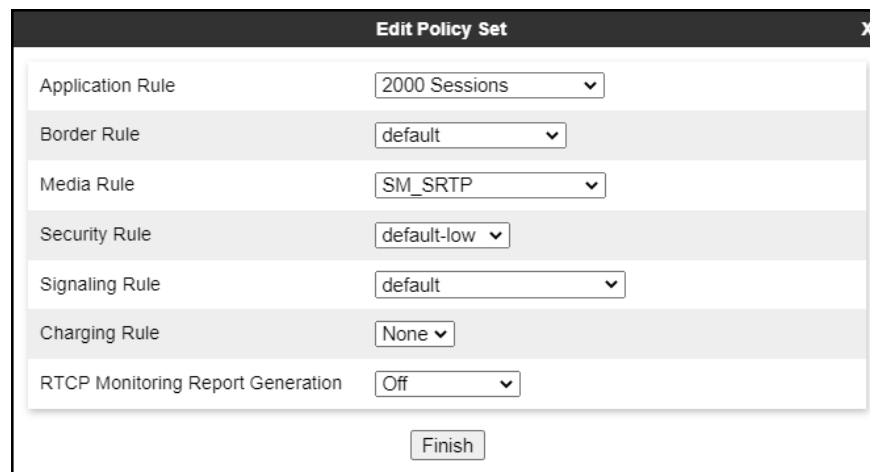
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



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 label "Group Name" followed by a text input field containing the word "Enterprise". Below the input field, there is a button labeled "Next".

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

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

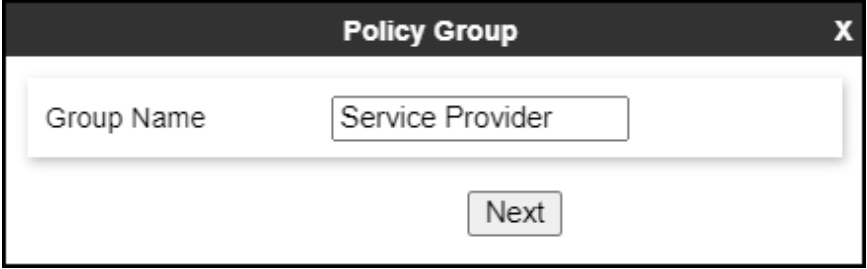


The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains a list of policy rules, each with a label and a dropdown menu. The selected values are: Application Rule (2000 Sessions), Border Rule (default), Media Rule (SM_SRTP), Security Rule (default-low), Signaling Rule (default), Charging Rule (None), and RTCP Monitoring Report Generation (Off). A "Finish" button is located at the bottom right of the dialog.

8.13.2. End Point Policy Group – Service Provider

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

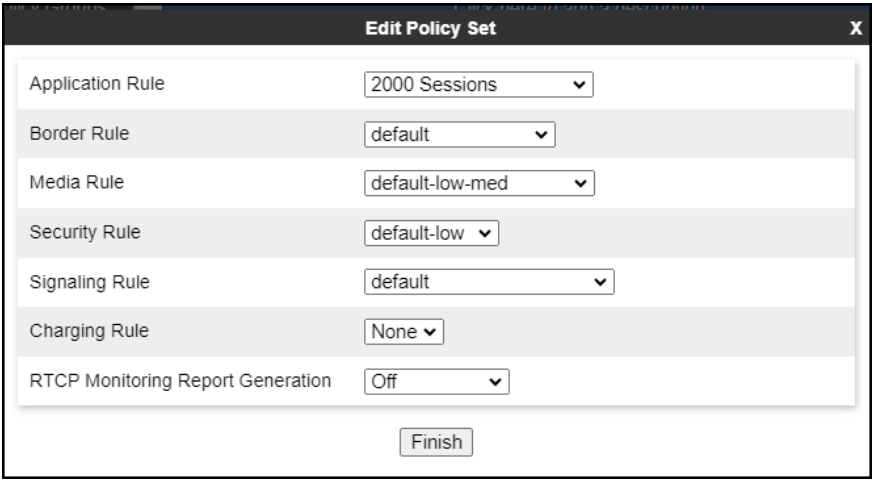
- Enter an appropriate name in the **Group Name** field (**Service Provider** was used).
- Click **Next**.



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

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

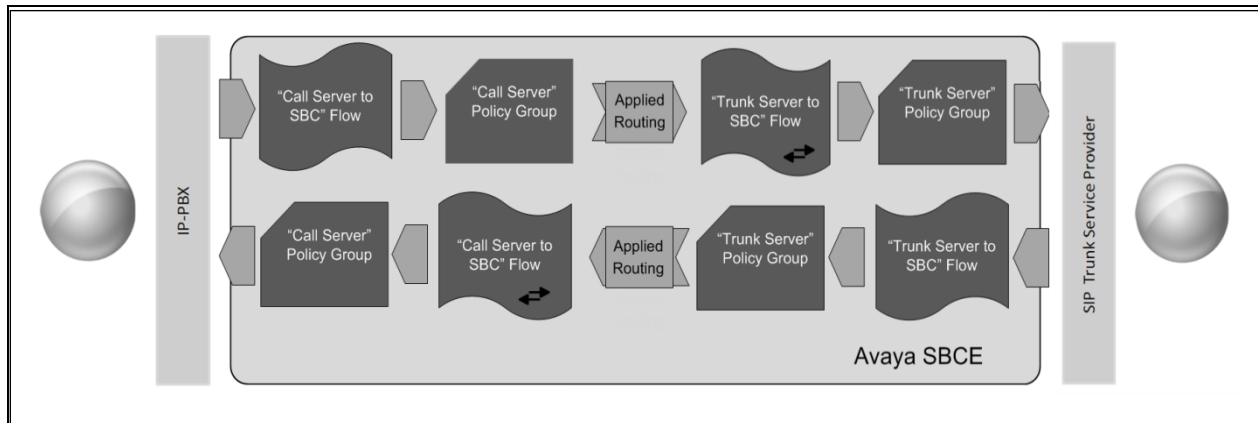
- **Application Rule: 2000 Sessions** (Section 8.12.1).
- **Border Rule: default**.
- **Media Rule: default-low-med** (Section 8.12.2).
- **Security Rule: default-low**.
- **Signaling Rule: default** (Section 8.12.3).
- Click **Finish**.



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 and their corresponding dropdown values are: "Application Rule" (2000 Sessions), "Border Rule" (default), "Media Rule" (default-low-med), "Security Rule" (default-low), "Signaling Rule" (default), "Charging Rule" (None), and "RTCP Monitoring Report Generation" (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 – SP to SM 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 **SP to SM 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 (Session Manager).

Edit Flow: SP to SM Flow	
Flow Name	SP to SM Flow
SIP Server Profile	Service Provider
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
Secondary Media Interface	None
End Point Policy Group	Service Provider
Routing Profile	Route_to_SM
Topology Hiding Profile	Service_Provider
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 – SM to SP Flow

A second Server Flow with the name **SM to SP 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: SM to SP Flow	
Flow Name	SM to SP Flow
SIP Server Profile	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig
Signaling Interface	Private_sig
Media Interface	Private_med
Secondary Media Interface	None
End Point Policy Group	Enterprise
Routing Profile	Route to SP
Topology Hiding Profile	Session_Manager
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 the WorldNet Telecommunications SIP Trunking Service, a customer must request the service from WorldNet using the established sales processes. The process can be started by contacting WorldNet via the corporate web site at: <https://www.worldnetpr.com/en/voice-service/>

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

WorldNet will provide the following information:

- WorldNet's SIP Proxy server IP address.
- 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:

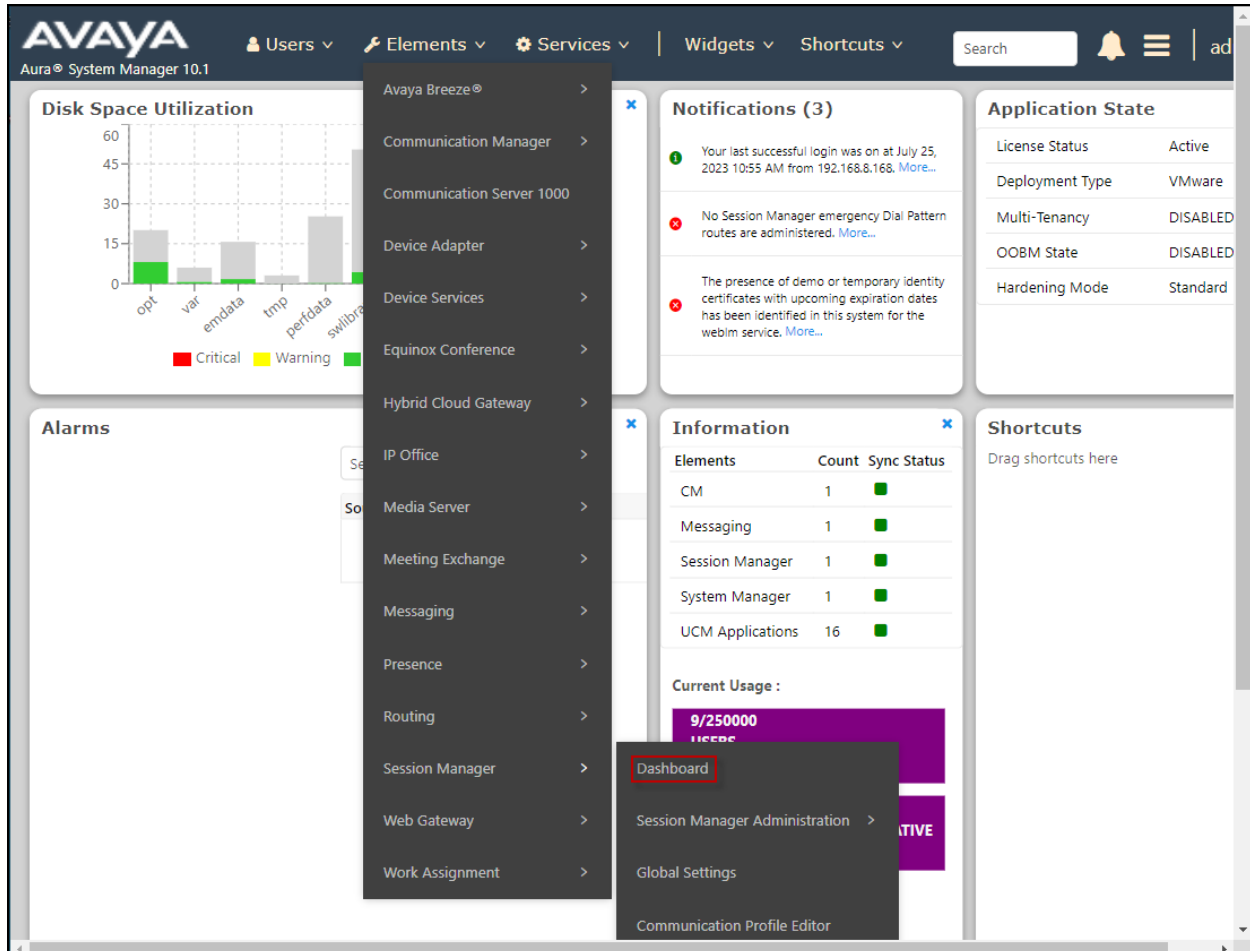
- **list trace station** <extension number>
Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>
Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>
Displays signaling group service state.
- **status trunk** <trunk group 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 **1** alarm out of the **10** Entities defined.

Session Manager Dashboard

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

Session Manager Instances

Service State: Shutdown System: EASG: Clear Logs: As of 11:56 AM

1 Item 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
Session Manager	Core	✓	0/0/0	Up	Accept New Service	0/0/0	1/10	0	3/3	✓	✓	Normal	Enabled	3	10.1.3.0.1013007

Select: All, None

Verify that the state of the Session Manager links under the **Conn. Status** and **Link Status** columns are **UP**, like shown on the screen below.

Session Manager Entity Link Connection Status

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

Status Details for the selected Session Manager:

All Entity Links for Session Manager: Session Manager

Summary View

10 Items Filter: Enable

	SIP Entity Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	Avaya SBC	IPv4	10.64.101.243	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Avaya Experience Portal	IPv4	10.64.101.252	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG5	IPv4	10.64.101.241	5075	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG1	IPv4	10.64.101.241	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG108	IPv4	10.64.101.241	5068	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Avaya Messaging	IPv4	10.64.101.158	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	SBCE-ATT	IPv4	10.64.91.42	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
<input type="radio"/>	CM-TG2	IPv4	10.64.101.241	5071	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG98	IPv4	10.64.101.241	5065	TLS	FALSE	UP	500 Service Unavailable(Signaling Resources Unavailable)	UP
<input type="radio"/>	AA-Messaging	IPv4	10.64.101.250	5061	TLS	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN

Select: None

Other Session Manager useful verification and troubleshooting tools include:

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

10.4.Avyaya 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.

Information	
System Time	12:02:48 PM EDT Refresh
Version	10.1.2.0-64-23285
GUI Version	10.1.2.0-23278
Build Date	Tue May 16 08:55:42 IST 2023
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	07/25/2023 13:13:05 EDT
Failed Login Attempts	0

Installed Devices	
EMS	
Avaya_SBC	

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

ID	Details	State	Time	Device
No alarms found for this device.				

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

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

Avaya Session Border Controller

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	12:02:48 PM EDT Refresh
Version	10.1.2.0-64-23285
GUI Version	10.1.2.0-23278
Build Date	Tue May 16 08:55:42 IST 2023
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	07/25/2023 13:13:05 EDT
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBC

The following screen shows the Incident Viewer page.

Device: Avaya_SBCE ▾ Help

Incident Viewer

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

Summary

Displaying entries 1 to 15 of 2002.

ID	Date & Time	Category	Type	Cause
825835107193461	May 4, 2022 9:16:54 AM	Policy	Server Registration	Registration Successful, Server is UP
825835047173505	May 4, 2022 9:14:54 AM	Policy	Server Registration	Registration Successful, Server is UP

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

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

Avaya Session Border Controller

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	12:02:48 PM EDT Refresh
Version	10.1.2.0-64-23285
GUI Version	10.1.2.0-23278
Build Date	Tue May 16 08:55:42 IST 2023
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	07/25/2023 13:13:05 EDT
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBC

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

Device: Avaya_SBC ▾ Help

Diagnostics

Pinging 10.64.101.249 X
Average ping from 10.64.101.243 [A1] to 10.64.101.249 is 0.253ms.

Full Diagnostic **Ping Test**

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

Source Device / IP: A1 ▾

Destination IP: 10.64.101.249

Ping

Additionally, the Avaya 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**.

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

Avaya Session Border Controller

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

DoS Learning

CDR Adjunct

Trace: Avaya_SBC

Packet Capture

Captures

A packet capture is currently in progress. This page will automatically refresh until the capture completes.

Packet Capture Configuration

Status	In Progress
Interface	Any ▾
Local Address IP[:Port]	All ▾ : <input type="text"/>
Remote Address *, *:Port, IP, IP:Port	<input type="text"/>
Protocol	All ▾
Maximum Number of Packets to Capture	<input type="text" value="10000"/>
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	<input type="text" value="Lumen.pcap"/>
<div>Stop Capture</div>	

Once the capture is stopped, click the **Captures** tab and select the proper .pcap file.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBC) web interface. The top navigation bar includes links for Device, 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 "Monitoring & Logging" expanded to show "Trace" as the selected option. The main content area is titled "Trace: Avaya_SBC" and features two tabs: "Packet Capture" and "Captures". The "Captures" tab is active, displaying a table of captured files. The table has columns for File Name, File Size (bytes), Last Modified, and a Delete link. The files listed are:

File Name	File Size (bytes)	Last Modified	Delete
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

11. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, Avaya Aura® Experience Portal 8.1 and Avaya Session Border Controller 10.1, 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 10.1, Issue 3, April 2022.
- [2] Administering Avaya Aura® Communication Manager, Release 10.1, Issue 1, December 2021.
- [3] Administering Avaya Aura® System Manager for Release 10.1.x, Issue 5, April 2022.
- [4] Deploying Avaya Aura® System Manager in a Virtualized Environment, Release 10.1.x, Issue 2, March 2022.
- [5] Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in a Virtualized Environment , Release 10.1., Issue 2, March 2022.
- [6] Administering Avaya Aura® Session Manager, Release 10.1.x, Issue 3, April 2022.
- [7] Deploying Avaya Session Border Controller on a Virtualized Environment Platform, Release 10.1, Issue 1, December 2021.
- [8] Administering Avaya Session Border Controller, Release 10.1.x, Issue 3, June 2023.
- [9] Application Notes for Configuring Remote Workers with Avaya Session Border Controller for Enterprise 10.1 on the Avaya Aura® Platform - Issue 1.0.
- [10] Deploying and Updating Avaya Aura® Media Server Appliance, Release 10.1.x, Issue 1, April 2022.
- [11] Administering Avaya Experience Portal, Release 8.1.1, Issue 2, February 2022
- [12] Implementing Avaya Experience Portal on a single server, Release 8.1.1, Issue 1, January 2022
- [13] RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>
- [14] 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 messages 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 **SP-General** 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 **SP-General** Server Interworking Profile created in **Section 8.7.2** and click **Edit**.

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

Editing Profile: SP-General

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 SP-General Server Interworking profile after editing.

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

Avaya Session Border Controller

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

IP/URI Blocklist Profile

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Interworking Profiles: SP-General

Add

Interworking Profiles

avaya-ru

OCS-Edge-S...

cisco-ccm

cups

OCS-FrontEn...

Avaya-SM

Avaya-IPO

Avaya-CS1000

Avaya-CM

cs2100

SP-General

Rename Clone Delete

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation Advanced

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	No
Mediasec	No

Edit

14. Appendix B – SigMa Scripts

Following are 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.