



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 for Enterprise 10.1 to support Cincinnati Bell 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 for Enterprise 10.1 to interoperate with Cincinnati Bell Business 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 Cincinnati Bell Business SIP Trunking service provides customers with PSTN access via a SIP trunk between the enterprise and the Cincinnati Bell Business network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	6
2.3.	Support	7
3.	Reference Configuration.....	8
4.	Equipment and Software Validated	11
5.	Configure Avaya Aura® Communication Manager	12
5.1.	Licensing and Capacity	12
5.2.	System Features.....	13
5.3.	IP Node Names.....	15
5.4.	Codecs	16
5.5.	IP Network Regions	18
5.6.	Signaling Group	19
5.7.	Trunk Group	21
5.8.	Calling Party Information.....	25
5.9.	Inbound Routing.....	26
5.10.	Outbound Routing	27
6.	Configure Avaya Aura® Experience Portal	31
6.1.	Background	31
6.2.	Logging in and Licensing.....	32
6.3.	VoIP Connection	34
6.4.	Speech Servers	36
6.5.	Application References	38
6.6.	MPP Servers and VoIP Settings.....	40
6.7.	Configuring RFC2833 Event Value Offered by Experience Portal	44
7.	Configure Avaya Aura® Session Manager	46
7.1.	System Manager Login and Navigation.....	47
7.2.	SIP Domain	49
7.3.	Locations	50
7.4.	Adaptations.....	54
7.4.1.	Adaptation for Avaya Aura® Communication Manager Extensions	54
7.4.2.	Adaptation for Communication Manager header removal	56
7.5.	SIP Entities.....	57
7.6.	Entity Links	61
7.7.	Routing Policies	63
7.8.	Dial Patterns	65
8.	Configure Avaya Session Border Controller for Enterprise	69
8.1.	System Access.....	69
8.2.	Device Management.....	72
8.3.	TLS Management.....	75
8.3.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise	75
8.3.2.	Server Profiles.....	77
8.3.3.	Client Profiles	79

8.4.	Network Management	81
8.5.	Media Interfaces	82
8.6.	Signaling Interfaces.....	84
8.7.	Server Interworking.....	86
8.7.1.	Server Interworking Profile – Enterprise	86
8.7.2.	Server Interworking Profile – Service Provider.....	90
8.8.	Signaling Manipulation	93
8.9.	Server Configuration	95
8.9.1.	Server Configuration Profile – Enterprise	95
8.9.2.	Server Configuration Profile – Service Provider	97
8.10.	Routing	99
8.10.1.	Routing Profile – Enterprise.....	99
8.10.2.	Routing Profile – Service Provider	101
8.11.	Topology Hiding.....	102
8.11.1.	Topology Hiding Profile – Enterprise	102
8.11.2.	Topology Hiding Profile – Service Provider.....	104
8.12.	Domain Policies.....	105
8.12.1.	Application Rules	105
8.12.2.	Media Rules.....	107
8.12.3.	Signaling Rules	110
8.13.	End Point Policy Groups	111
8.13.1.	End Point Policy Group – Enterprise	111
8.13.2.	End Point Policy Group – Service Provider.....	112
8.14.	End Point Flows.....	113
8.14.1.	End Point Flow – SP to SM Flow	114
8.14.2.	End Point Flow – SM to SP Flow	115
9.	Cincinnati Bell SIP Trunking Service Configuration	116
10.	Verification and Troubleshooting	116
10.1.	General Verification Steps.....	116
10.2.	Communication Manager Verification	116
10.3.	Session Manager Verification	117
10.4.	Avaya SBCE Verification	120
11.	Conclusion	127
12.	References.....	127
13.	Appendix A – Avaya Session Border Controller for Enterprise – Refer Handling.....	128
14.	Appendix B – SigMa Scripts	132

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the Cincinnati Bell Business 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 Experience Portal 8.1 (Experience Portal) and Avaya Session Border Controller for Enterprise 10.1 (Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

The Cincinnati Bell Business 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”, “Cincinnati Bell”, “Cincinnati Bell Business” or “CBTS” will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

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

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

2.1. Interoperability Compliance Testing

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

- Static IP SIP Trunk authentication.
- Response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to DID numbers assigned by Cincinnati Bell. Incoming PSTN calls were terminated to the following endpoints: Avaya J129 IP Deskphones (SIP), Avaya J179 IP Deskphones (H.323), Avaya 96x1 IP Deskphones (SIP), Avaya 2420 Digital Deskphones, Avaya one-X® Communicator softphone (H.323 and SIP), Avaya Workplace client for Windows (SIP) and analog Deskphones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya Workplace client for Windows (SIP).
- Outgoing calls to the PSTN were originated from the various Avaya endpoints mentioned above. Calls were routed via Cincinnati Bell 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 codec: G.711MU (Note: Other audio codecs may be supported by Cincinnati Bell, G.711MU was the only codec being offered by Cincinnati Bell during the compliance test).
- 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 SBCE, 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, outbound Toll-Free calls, 911 calls (emergency), “0” calls (Operator), local directory assistance and international calls were not tested.

2.2. Test Results

Interoperability testing of the Cincinnati Bell 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:

- **Fax support:** Fax calls using the T.38 protocol failed during the compliance test. G.711 pass-through fax was also tested, but it behaved unreliably. The issue related to G.711 pass-through fax failing during the compliance test may be related to the unpredictability of G.711 pass-through techniques, which only works well on networks with very few hops and with limited end-to-end delay. The issue related to T.38 fax calls failing is related to the PSTN carriers used by Cincinnati Bell to route calls to the PSTN, not all PSTN carriers used by Cincinnati Bell support T.38. This issue could be resolved by Cincinnati Bell selecting specific PSTN carriers that do support T.38 and routing T.38 fax traffic via these PSTN carriers.
- In specific call transfer scenarios to the PSTN, Cincinnati Bell sent "415 Unsupported media type" responses to UPDATES sent from Communication Manager that contained XML transfer information. Since this information has no relevance to the service provider, a Sigma script was used on the Avaya SBCE to remove the unwanted XML information from being sent to Cincinnati Bell. See **Section 8.8** and **14**.
- The Experience Portal test application used for compliance testing performs consultative call transfer of inbound calls that are transferred back to the PSTN using SIP INVITE, with the original calling party number in the From and P-Asserted Identity headers, and it does not contain a Diversion header. In this scenario, since none of the headers in the outbound INVITE contains a number recognizable by the Cincinnati Bell network, Experience Portal consultative call transfers out the Cincinnati Bell network failed. As a workaround, a SigMa script was created on the Avaya SBCE to modify the P-Asserted-Identity header on outbound INVITES from Experience Portal to the PSTN, with the DID number assigned to Experience Portal, known to Cincinnati Bell (See **Section 8.8** and **14**). In addition, Experience Portal blind transfers out to Cincinnati Bell using SIP REFER were tested successfully. Also, consultative and blind transfers from Experience Portal to Communication Manager were successful as well.
- **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**).

2.3. Support

For support of Cincinnati Bell SIP Trunking Service visit the corporate Web page at:

<https://www.altafiber.com/business/support/sip-trunking-support>

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 Cincinnati Bell SIP Trunking Service through a public Internet WAN connection.

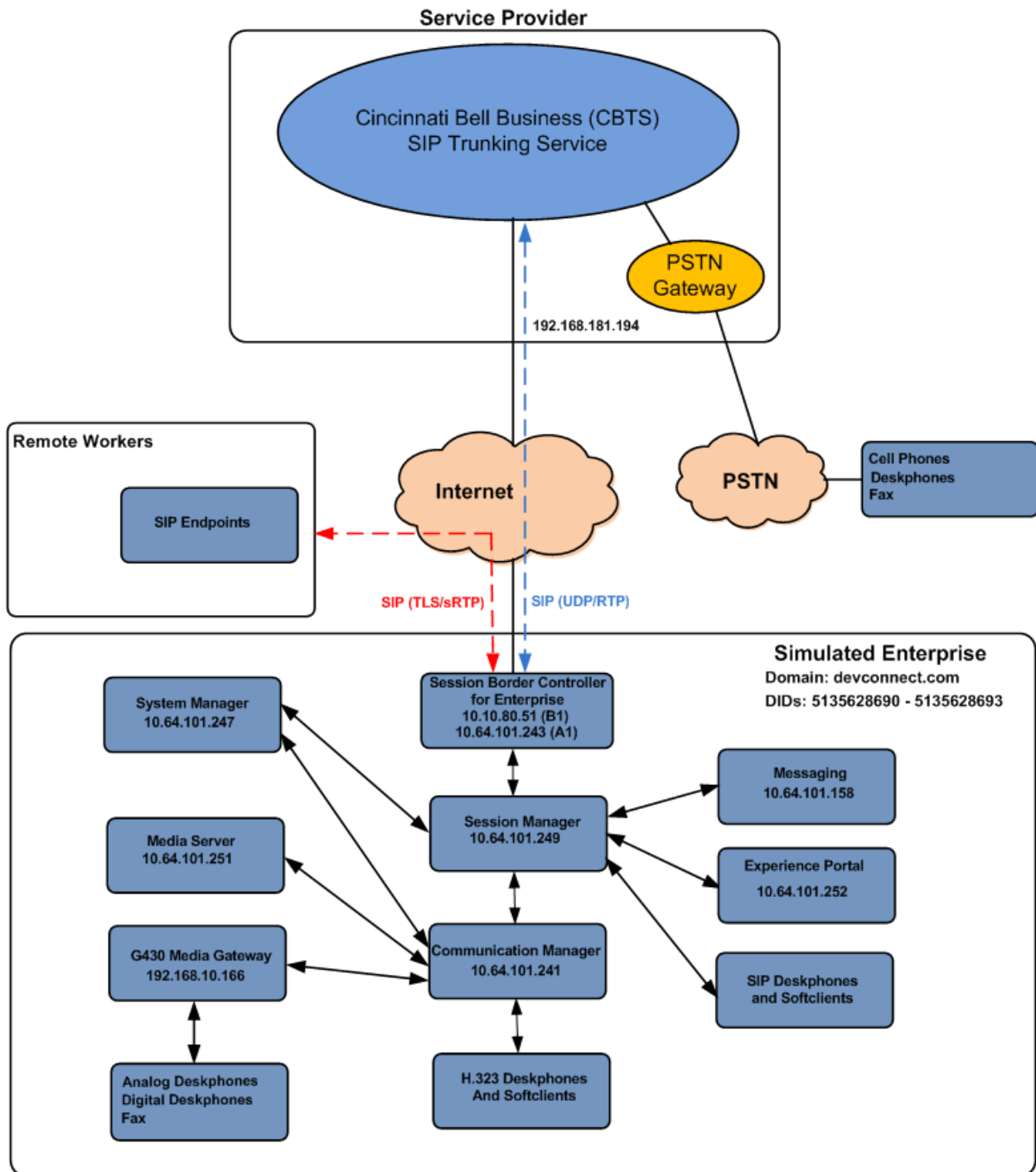


Figure 1: Avaya SIP Enterprise Solution connected to Cincinnati Bell Business SIP Trunking Service

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

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya Messaging.
- Avaya 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 one-X® Communicator softphones (H.323 and SIP).
- Avaya Workplace Client for Windows softphone (SIP).
- 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 SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test using only the Avaya 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 SBCE was located at the edge of the enterprise. Its public side was connected to the public Internet, while its private side was connected to the enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flowed through the Avaya SBCE, protecting in this way the enterprise against any SIP-based attacks. The Avaya SBCE also performed network address translation at both the IP and SIP layers.

For inbound calls, the calls flowed from the service provider to the Avaya SBCE then to Session Manager. Session Manager used the configured dial patterns (or regular expressions) and routing policies to determine the recipient (Communication Manager or Experience Portal) and on which link to send the call.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager.

Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the Avaya SBCE for egress to the Cincinnati Bell 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 Cincinnati Bell network SIP Trunking service, they are not included in these Application Notes.

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

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager	10.1.2 Feature Pack 2 (01.0.974.0-27783)
Avaya Aura® Session Manager	10.1.2 Feature Pack 2 (10.1.2.0.1012016)
Avaya Aura® System Manager	10.1.2.0 Service Pack 2 Build No. - 10.1.0.0.537353 Software Update Revision No: 10.1.2.0.0715476
Avaya Session Border Controller for Enterprise	ASBCE 10.1 10.1.0.0-32-21432 (sbce-10.1.0.0-34-22640-hotfix-11102022)
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 2
Avaya G430 Media Gateway	g430_sw_42.18.0
Avaya J100 Series IP Deskphones (SIP)	Version 4.1.0.0.7
Avaya J179 IP Deskphones (H.323)	6.8.5.2.3
Avaya 96x1 IP Deskphones (SIP)	7.1.15.2.1
Avaya Workplace Client for Windows (SIP)	3.32.0.75
Avaya one-X® Communicator client (SIP & H.323)	6.2.14.1-SP14
Avaya Agent for Desktop	2.0.6.25.3006
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
Cincinnati Bell	
Cisco Broadworks	R24
Ribbon SBC	09.02.04R002

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

Note – The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the previous table were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 6.7.0) 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 Cincinnati Bell 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		6
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

      Name      IP Address      IP NODE NAMES
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
```

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. Only codec **G.711MU** was used during the compliance. Other audio codecs may be supported by Cincinnati Bell.

HG; Reviewed: Solution & Interoperability Test Lab Application Notes 16 of 133
SPOC 5/4/2023 ©2023 Avaya Inc. All Rights Reserved. CBTSAura101EP81

On **Page 2**, in general, the **FAX Mode** is set to **t.38fallback** to allow the fax call to fallback to G.711 fax if the call terminates on a gateway in the CBTS network that does not support T.38. However, in the case of CBTS this setting will result in all outbound fax calls using G.711 fax due to the observation in **Section 2.2**. To force the use of T.38, the **FAX Mode** may be set to **t.38-standard**. However, if the far-end gateway does not support T.38 then the fax call will fail.

change ip-codec-set 2

Page 2 of 2

IP MEDIA PARAMETERS

Allow Direct-IP Multimedia? n

	Mode		Redun-	Packet
			dancy	Size (ms)
FAX	t.38fallback	XMT: udptl	0	ECM: y
Modem	off		0	FB-Timer: 4
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        Attendant Vectoring? y
```

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? 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
  Attendant Vectoring? y
```

On Page 3:

- Set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. When **public** format is used, Communication Manager automatically inserts a “+” sign, preceding the numbers in the “From”, “Contact” and “P-Asserted Identity” (PAI) headers. **Private** numbering format was used to keep uniformity with the numbering format used by CBTS (CBTS doesn’t support E.164 numbering format which includes the “+” sign). The **Numbering Format** was set to **private** and the **Numbering Format** in the route pattern was set to **unk-unk** (see **Section 5.10**).
- Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call has enabled CPN block.

change trunk-group 2		Page 3 of 4
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: private	
	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 Cincinnati Bell.
- 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 private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, three DID numbers 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 private-numbering 1					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext	Ext	Trk	Private	Total		
Len	Code	Grp(s)	Prefix	Len		
4	3			4	Total Administered: 6	
4	5			4	Maximum Entries: 540	
5	8			5		
4	3041	2	5135628690	10		
4	3044	2	5135628691	10		
4	3045	2	5135628692	10		

5.9. Inbound Routing

In general, the “incoming call handling treatment” form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary (refer to **Section 7.4.1**). If the DID number sent by Cincinnati Bell is left unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

change inc-call-handling-trmt trunk-group 2					Page	1	of	30
INCOMING CALL HANDLING TREATMENT								
Service/ Feature	Number Len	Number Digits	Del	Insert				
public-ntwrk	10	5135628690	10	3041				
public-ntwrk	10	5135628691	10	3044				
public-ntwrk	10	5135628692	10	5015				
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								
public-ntwrk								

5.10.Outbound Routing

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

change dialplan analysis			DIAL PLAN ANALYSIS TABLE						Page	1 of	12
			Location: all						Percent Full: 2		
	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type		
0		13	udp								
1		4	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							Percent Full: 1	
Location: all								
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		
178	11	11	deny	fnpa		n		
1786	11	11	2	fnpa		n		
179	11	11	deny	fnpa		n		
180	11	11	deny	fnpa		n		
1800	11	11	2	fnpa		n		
1800555	11	11	deny	fnpa		n		

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.
- **Numbering Format:** Set to **Unk-unk**. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

change route-pattern 2

Page 1 of 4

Pattern Number: 2

Pattern Name: Serv. Provider

SCCAN? n

Secure SIP? n

Used for SIP stations? n

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

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

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

6. Configure Avaya Aura® Experience Portal

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

6.1. Background

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

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

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

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

6.2. Logging in and Licensing

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

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

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

AVAYA Welcome, epadmin
Last logged in today at 6:23:08 AM MST

Avaya Experience Portal 8.1.2 (ExperiencePortal) Home ? Help Logoff

Expand All | Collapse All

You are here: Home

Avaya Experience Portal Manager

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

Installed Components

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

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

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

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

Legal Notice

AVAYA GLOBAL SOFTWARE LICENSE TERMS
REVISED: June 1st, 2020

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

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


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

Licensing


[Refresh](#)

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

License Server Information

License Server URL:	https://10.64.91.90:8443/WebLM/LicenseServer	
Last Updated:	Nov 3, 2020 1:02:12 PM MST	
Last Successful Poll:	Jan 31, 2023 6:42:27 AM MST	

Licensed Products

Experience Portal		
Announcement Ports:	100	
ASR Connections:	100	
Call Anchoring Ports:	100	
Conversation Speech Connections:	100	
Email Units:	10	
Enable Media Encryption:	1	
Enhanced Call Classification:	100	
Google ASR Connections:	10	
Google Dialogflow Connections:	10	
HTML Units:	100	
SIP Signaling Connections:	100	
SMS Units:	10	
Telephony Ports:	100	
TTS Connections:	100	
Video Server Connections:	100	
Zones:	1	
Version:	8	
Last Successful Poll:	Jan 31, 2023 6:42:27 AM MST	
Last Changed:	Oct 31, 2022 7:24:23 AM MDT	

6.3. VoIP Connection

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

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

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

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

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

VoIP Connections

This page displays a list of Voice over Internet Protocol (VoIP) servers that Experience Portal communicates with. You can configure multiple SIP connections, but only one SIP connection can be enabled at any one given time.

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 **100** was used.
- Select **All Calls can be either inbound or outbound**.
- **SRTP Enable** = **Yes**.
- **Encryption Algorithm** = **AES_CM_128**
- **Authentication Algorithm** = **HMAC_SHA1_80**.
- **RTCP Encryption Enabled** = **No**.
- **RTP Authentication Enabled** = **Yes**.
- Click on **Add** to add SRTP settings to the **Configured SRTP List**.

- Use default values for all other fields.
- Click **Save**.

Expand All | Collapse All

▼ **User Management**
Roles
Users
Login Options

▼ **Real-time Monitoring**
System Monitor
Active Calls
Port Distribution

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

▼ **System Management**
EPM Manager
MPP Manager
Software Upgrade
System Backup

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

▼ **Security**
Certificates
Licensing

▼ **Reports**
Standard
Custom
Scheduled

▼ **Multi-Media Configuration**
Email
HTML
SMS

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

Change SIP Connection

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

Name: 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

Remove

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

6.4. Speech Servers

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

ASR speech server:

Expand All | Collapse All

▼ User Management

Roles

Users

Login Options

▼ Real-time Monitoring

System Monitor

Active Calls

Port Distribution

▼ System Maintenance

Audit Log Viewer

Trace Viewer

Log Viewer

Alarm Manager

▼ System Management

EPM Manager

MPP Manager

Software Upgrade

System Backup

▼ System Configuration

Applications

EPM Servers

MPP Servers

SNMP

Speech Servers

VoIP Connections

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

Speech Servers

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

ASR

TTS

<input type="checkbox"/>	Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed 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:

Expand All | Collapse All

▼ User Management

Roles

Users

Login Options

▼ Real-time Monitoring

System Monitor

Active Calls

Port Distribution

▼ System Maintenance

Audit Log Viewer

Trace Viewer

Log Viewer

Alarm Manager

▼ System Management

EPM Manager

MPP Manager

Software Upgrade

System Backup

▼ System Configuration

Applications

EPM Servers

MPP Servers

SNMP

Speech Servers

VoIP Connections

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

Speech Servers

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

ASR

TTS

<input type="checkbox"/>	Name ▲▼	Enable ▲▼	Network Address ▲▼	Engine Type ▲▼	MRCP ▲▼	Base Port ▲▼	Total Number of Licensed TTS Resources ▲▼	Voices ▲▼
<input type="checkbox"/>	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 **5135628693** provided by the service provider was used. Inbound calls with this called party number will be handled by the application defined in this section.

Expand All | Collapse All

▼ **User Management**
Roles
Users
Login Options

▼ **Real-time Monitoring**
System Monitor
Active Calls
Port Distribution

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

▼ **System Management**
EPM Manager
MPP Manager
Software Upgrade
System Backup

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

▼ **Security**
Certificates
Licensing

▼ **Reports**
Standard
Custom
Scheduled

▼ **Multi-Media Configuration**
Email
HTML
SMS

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

Change Application

Use this page to change the configuration of an application.

Name: Test2_App
Enable: ☒ Yes ☐ No
Type: CCXML
Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum
Requested:

URI

☒ Single ☐ Fail Over ☐ Load Balance
CCXML URL: **Verify**

Mutual Certificate Authentication: ☐ Yes ☒ No
Basic Authentication: ☐ Yes ☒ No

ASR Speech Servers

Engine Types
ASR: <None>

Selected Engine Types
Nuance

Nuance

Languages
<None>

Selected Languages
English(USA) en-US

Resources:

N Best List Length:

Speech Complete Timeout: milliseconds
Speech Incomplete Timeout: milliseconds

Vendor Parameters:

TTS Speech Servers

Voices
TTS: Nuance
<None>

Selected Voices
English(USA) en-US Jennifer F

Application Launch

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

 Remove
SIP Header Source:

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**.

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

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

MPP Servers

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

<input type="checkbox"/>	Name	Host Address	Network Address (VoIP)	Network Address (MRCP)	Network Address (AppSvr)	Maximum Simultaneous Calls	Trace Level
<input type="checkbox"/>	MPP	10.64.101.252	<Default>	<Default>	<Default>	1	Use MPP Settings
<input type="checkbox"/>	MPP	10.64.101.252	<Default>	<Default>	<Default>	1	Use MPP Settings

Add

Delete

MPP Settings

Browser Settings

Video Settings

VoIP Settings

Help

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

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

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

HG; Reviewed:
SPOC 5/4/2023

Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

41 of 133
CBTSAura101EP81

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.

[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** , **G729**, **G711aLaw**, are enabled (check marks). Set the **Offer** and Answer **Order** as shown. In the sample configuration **G711uLaw** is the preferred codec, with **Order 1**, followed by **G729** with **Order 2** and **G711aLaw** with **Order 3**.
 - On the codec Answer set **G729 Discontinuous Transmission** to **Either**.
- Use default values for all other fields.

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

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	Codecs ▼		
	Offer		
	Enable	Codec	Order
	<input checked="" type="checkbox"/>	G711uLaw	1
	<input checked="" type="checkbox"/>	G729	2
	<input checked="" type="checkbox"/>	G711aLaw	3
	Packet Time: <input type="text" value="20"/> milliseconds		
	G729 Discontinuous Transmission: <input checked="" type="radio"/> Yes <input type="radio"/> No		
	Answer		
	Enable	Codec	Order
<input checked="" type="checkbox"/>	G711uLaw	1	
<input checked="" type="checkbox"/>	G729	2	
<input checked="" type="checkbox"/>	G711aLaw	3	
G729 Discontinuous Transmission: <input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Either			
G729 Reduced Complexity Encoder: <input checked="" type="radio"/> Yes <input type="radio"/> No			

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.

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

You are here: [Home](#) > System Management > MPP Manager

MPP Manager (Mar 23, 2023 1:39:29 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: Mar 23, 2023 1:39:10 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

Restart/Reboot Options

☒ One server at a time

☐ All servers

HG; Reviewed:
SPOC 5/4/2023

Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

45 of 133
CBTSAura101EP81

7. Configure Avaya Aura® Session Manager

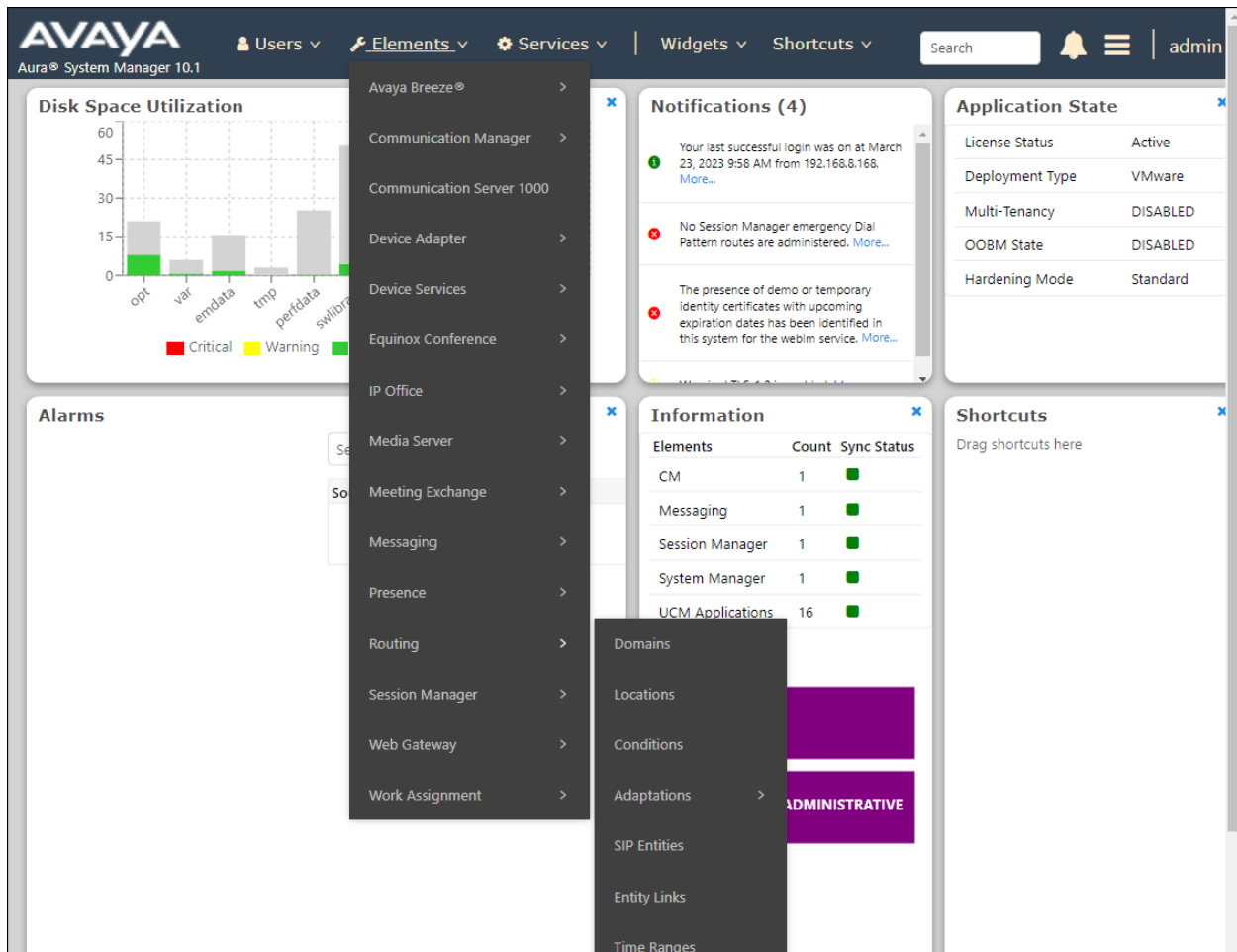
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

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

7.1. System Manager Login and Navigation

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



The 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 shows the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, version information, and links for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile (admin) are also present. The left sidebar shows a navigation tree with 'Routing' selected, and 'Domains' highlighted. The main content area is titled 'Domain Management' and features a table with one item, 'devconnect.com', of type 'sip'. The table has columns for Name, Type, and Notes. A 'Filter: Enable' link is visible in the top right of the table area. 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.



The screenshot displays the 'Domain Management' interface. On the left is a navigation pane with 'Routing' expanded and 'Domains' selected. The main area shows a table with one item: 'devconnect.com' with type 'sip'. Above the table are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below the table is a 'Select' dropdown set to 'All'.

<input type="checkbox"/>	Name	Type	Notes
<input type="checkbox"/>	devconnect.com	sip	

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 top navigation bar includes the Avaya logo, version information, and user roles (Users, Elements, Services, Widgets, Shortcuts). A search bar and user profile (admin) are also present. The left-hand navigation pane shows a tree structure with 'Routing' selected, and 'Locations' highlighted under the 'Routing' category. The main content area is titled 'Location Details' and contains several sections: 'General' with fields for 'Name' (Session Manager) and 'Notes' (VMware Session Manager); 'Dial Plan Transparency in Survivable Mode' with an 'Enabled' checkbox and fields for 'Listed Directory Number' and 'Associated CM SIP Entity'; 'Overall Managed Bandwidth' with a dropdown for 'Managed Bandwidth Units' (Kbit/sec) and fields for 'Total Bandwidth' and 'Multimedia Bandwidth'; and 'Per-Call Bandwidth Parameters' with fields for 'Maximum Multimedia Bandwidth (Intra-Location)' and 'Maximum Multimedia Bandwidth (Inter-Location)', both set to 2000 Kbit/Sec. 'Commit' and 'Cancel' buttons are located at the top right of the form.

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

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 'admin' are also present. The left sidebar shows a navigation menu with 'Routing' selected, and sub-items like Domains, Locations (highlighted), Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and contains several sections: 'General' with fields for Name (Communication Manager) and Notes (VMware Communication Manager); 'Dial Plan Transparency in Survivable Mode' with an 'Enabled' checkbox and input fields for 'Listed Directory Number' and 'Associated CM SIP Entity'; 'Overall Managed Bandwidth' with a 'Managed Bandwidth Units' dropdown (set to Kbit/sec) and input fields for 'Total Bandwidth' and 'Multimedia Bandwidth'; and 'Per-Call Bandwidth Parameters' with input fields for 'Maximum Multimedia Bandwidth (Intra-Location)' and 'Maximum Multimedia Bandwidth (Inter-Location)', both set to 2000 Kbit/Sec. 'Commit' and 'Cancel' buttons are at the top right of the form.

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

Defaults

Location Details Commit Cancel 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: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): Kbit/Sec

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

The screenshot displays the '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 a 'Commit' button and a 'Cancel' button. The configuration is organized into several sections:

- General**: Contains fields for 'Name' (set to 'Avaya SBCE') and 'Notes' (set to 'VMware Avaya SBCE').
- Dial Plan Transparency in Survivable Mode**: Includes an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field.
- Overall Managed Bandwidth**: Includes a 'Managed Bandwidth Units' dropdown (set to 'Kbit/sec'), 'Total Bandwidth' and 'Multimedia Bandwidth' fields, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'.
- Per-Call Bandwidth Parameters**: Includes a 'Maximum Multimedia Bandwidth (Intra-Location)' field (set to '2000 Kbit/Sec') and a 'Maximum Multimedia Bandwidth' field.

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 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and menu items for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled 'admin' are also present. The left sidebar shows a navigation tree with 'Routing' selected, and sub-items like Domains, Locations (highlighted), Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and contains several sections: 'General' with fields for Name (Lab Others) and Notes (VMware Lab others); 'Dial Plan Transparency in Survivable Mode' with an 'Enabled' checkbox and fields for Listed Directory Number and Associated CM SIP Entity; 'Overall Managed Bandwidth' with a dropdown for Managed Bandwidth Units (Kbit/sec) and input fields for Total Bandwidth and Multimedia Bandwidth; and 'Per-Call Bandwidth Parameters' with input fields for Maximum Multimedia Bandwidth (Intra-Location) and Maximum Multimedia Bandwidth (Inter-Location), both set to 2000 Kbit/Sec. 'Commit' and 'Cancel' buttons are located at the top right 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

Defaults

<

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: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

7.4. Adaptations

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

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

7.4.1. Adaptation for Avaya Aura® Communication Manager Extensions

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

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 'Adaptation Details' page in the Session Manager interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, Locations, Conditions, Adaptations (selected), Regular Expressions, and Device Mappings. The main content area is titled 'Adaptation Details' and has a 'General' tab selected. The form fields are as follows:

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

Buttons for 'Commit' and 'Cancel' are located in the top right corner of the form.

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

Example 1

- Enter **5135628690** in the **Matching Pattern** column.
- Enter **10** in the **Min/Max** columns.
- Enter **10** in the **Delete Digits** column.

- Enter **3041** in the **Insert Digits** column (3041 is the Communication Manager extension number).
- Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
- Enter any desired notes.

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

Step 5 - Click on **Commit**.

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

Digit Conversion for Outgoing Calls from SM

Add Remove

3 Items Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
* 5135628690	* 10	* 10		* 10	3041	destination ▼		
* 5135628691	* 10	* 10		* 10	3044	destination ▼		
* 5135628692	* 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 Cincinnati Bell. 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 shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations (selected), Conditions, Adaptations, Adaptations, Regular Expressions, Device Mappings, SIP Entities, Entity Links, and Time Ranges. The main content area is titled 'Adaptation Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' tab is active, showing the following fields:

- Adaptation Name:** CM_Outbound_Header_Removal
- Notes:** (empty text box)
- Module Name:** DigitConversionAdapter (dropdown menu)
- Type:** digit (dropdown menu)
- State:** enabled (dropdown menu)
- Module Parameter Type:** Name-Value Parameter (dropdown menu)

Below these fields is a table for adding parameters:

Add Remove	
Name	Value
<input type="checkbox"/> eRHdrs	"Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View"

Below the table is a 'Select' dropdown menu with options: All, None. At the bottom, there is an 'Egress URI Parameters' text box.

7.5. SIP Entities

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling (see **Figure 1**).
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager, **SIP Trunk** (or **Other**) for the Avaya SBCE and **Voice Portal** for the Experience Portal.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If Adaptations were to be created, here is where they would be applied to the entity.
- **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 left navigation pane shows the 'Routing' menu expanded, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains two sections: 'General' and 'Monitoring'. The 'General' section includes the following fields:

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

The 'Monitoring' section includes the following fields:

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

The top navigation bar includes the Avaya logo, 'Users', 'Elements', 'Services', 'Widgets', 'Shortcuts', a search bar, a notification bell, and the user 'admin'. The bottom of the page shows the 'Commit' and 'Cancel' buttons.

The following screen shows the addition of the **Communication Manager Trunk 2** SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the “**procr**” interface in Communication Manager, as seen in **Section 5.3**. 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 the navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields and values:

- Name:** Communication Manager Trunk 2
- * 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/New_York
- * 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. A 'Help' link is also visible in the top right corner of the main content area.

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

- The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**).
- 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, version information, and user roles (Users, Elements, Services, Widgets, Shortcuts). A search bar and a user profile icon (admin) are also present. The left sidebar shows a navigation menu with options like Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows:

- Name:** Avaya SBCE
- FQDN or IP Address:** 10.64.101.243
- Type:** SIP Trunk
- Notes:** VMware Avaya SBCE
- Adaptation:** CM_Outbound_Header_Removal
- Location:** Avaya SBCE
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty 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 visible.

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 a menu with 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar is located on the right. The left sidebar shows a navigation tree with 'Routing' selected, and sub-items like 'Domains', 'Locations', 'Conditions', 'Adaptations', 'SIP Entities' (highlighted), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows:

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

Below the General tab, there are two more sections:

- Loop Detection:**
 - Loop Detection Mode:** On
 - Loop Count Threshold:** 5
 - Loop Detection Interval (in msec):** 200
- Monitoring:**
 - SIP Link Monitoring:** Use Session Manager Configuration
 - CRLF Keep Alive Monitoring:** Use Session Manager Configuration

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

7.6. Entity Links

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

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu (**Section 7.5**).
- **Protocol:** Select the transport protocol used for this link (**Section 5.6**).
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end (**Section 5.6**).
- **SIP Entity 2:** Select the name of the other system from the drop-down menu (**Section 7.5**).
- **Port:** Port number on which the other system receives SIP requests from Session Manager (**Section 5.6**).
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.
- Click **Commit** to save.

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

The screenshot displays the Avaya Aura System Manager 10.1 interface. The left navigation pane is expanded to 'Entity Links'. The main area shows a table with one item, 'Session_Manager_CM_T', which is linked to 'Session Manager' (SIP Entity 1) and 'Communication Manager Trunk 2' (SIP Entity 2). The protocol is set to 'TLS' and the port is '5071'. The connection policy is 'trusted'.

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

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

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar has a menu with options: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links (selected), and Time Ranges. The main content area is titled 'Entity Links' and contains a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The row shows a link between 'Session Manager_Avaya' and 'Session Manager' (SIP Entity 1) and 'Avaya SBCE' (SIP Entity 2) using the 'TLS' protocol on port '5061'. The 'Connection Policy' is set to 'trusted' and 'Deny New Service' is unchecked. There are 'Commit' and 'Cancel' buttons at the top and bottom of the table.

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

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

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar has a menu with options: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links (selected), and Time Ranges. The main content area is titled 'Entity Links' and contains a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The row shows a link between 'Session Manager_Avaya' and 'Session Manager' (SIP Entity 1) and 'Avaya Experience Portal' (SIP Entity 2) using the 'TLS' protocol on port '5061'. The 'Connection Policy' is set to 'trusted' and 'Deny New Service' is unchecked. There are 'Commit' and 'Cancel' buttons at the top and bottom of the table.

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

7.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 7.5**. Two routing policies were added: An incoming policy with Communication Manager as the destination and an outbound policy with the Avaya SBCE as the destination and an incoming policy with Experience Portal as the destination. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed:

- In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies (**Section 7.5**) and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below.
- Use default values for remaining fields.
- Click **Commit** to save.

The following screens show the Routing Policies for Communication Manager, the Avaya SBCE and the Experience Portal.

AVAYA
Aura® System Manager 10.1

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

Home Routing ×

Routing Policies

Routing Policy Details

Commit Cancel Help ?

General

* Name: To CM Trunk 2

Disabled: ☐

* Retries: 0

Notes: For inbound calls to CM via Trunk 2

SIP Entity as Destination

Select

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

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

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

Defaults

Routing Policy Details

CommitCancel

Help

General

* Name:

Avaya_SBCE

Disabled:

* Retries:

0

Notes:

For outbound calls to SP via ASBCE

SIP Entity as Destination

Select

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

Time of Day

AddRemoveView Gaps/Overlaps

1 Item

Filter: Enable

	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
	0	24/7								00:00	23:59	Time Range 24/7

Select : All, None

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

Defaults

Routing Policy Details

CommitCancel

Help

General

* Name:

To Avaya Experience Portal

Disabled:

* Retries:

0

Notes:

To Avaya Experience Portal

SIP Entity as Destination

Select

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

AddRemoveView Gaps/Overlaps

1 Item

Filter: Enable

	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
	0	24/7								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.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to Communication Manager. In the examples, calls to 12-digit numbers starting with **513** arriving from location **Avaya SBCE**, used route policy **To CM Trunk 2** to Communication Manager. The SIP Domain was set to **devconnect.com**.

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 ...

Regular Expressions

Dial Pattern Details

CommitCancel

Help

General

* Pattern: 513

* Min: 3

* Max: 36

Emergency Call: ☐

SIP Domain: devconnect.com

Notes:

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

AddRemove

1 Item

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"/>	Avaya SBCE	VMware Avaya SBCE			To CM Trunk 2	0	<input type="checkbox"/>	CM-TG2	For inbound calls to CM via Trunk 2

Select : All, None

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

AVAYA
Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾

Search 🔍 | admin

Home | **Routing**

Adaptations
Regular Expressi...
Device Mappings
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns ▾
Dial Patterns
Origination Dial ...
Regular Expressions
Defaults

Dial Pattern Details

Commit Cancel

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"/>	Avaya SBCE	VMware Avaya SBCE			To CM Trunk 2	0	<input type="checkbox"/>	CM-TG2	For inbound calls to CM via Trunk 2
<input type="checkbox"/>	Communication Manager	VMware Communication Manager			To SP SBCE	0	<input type="checkbox"/>	Avaya SBCE	For outbound calls to SP via ASBCE
<input type="checkbox"/>	Lab Others	VMware Lab others			To SP SBCE	0	<input type="checkbox"/>	Avaya SBCE	For outbound calls to SP via ASBCE

The following screen illustrates an example dial pattern used to verify inbound calls from the PSTN to Experience Portal. In the sample configuration one of the DID numbers provided by the service provider (5135628693) was used as a test number to route calls from the PSTN to Experience Portal, arriving from location **Avaya SBCE**, used routing policy **SP to Avaya Experience Portal**. The SIP Domain was set to **devconnect.com**.

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 ...
- Regular Expressions

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 5135628693

* Min: 10

* Max: 36

Emergency Call: ☐

SIP Domain: devconnect.com ▾

Notes:

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

Add Remove Filter: Enable

1 Item

<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"/>	Avaya SBCE	VMware Avaya SBCE			SP to Avaya Experience Portal	0	<input type="checkbox"/>	Avaya Experience Portal	To Avaya Experience Portal

Select : All, None

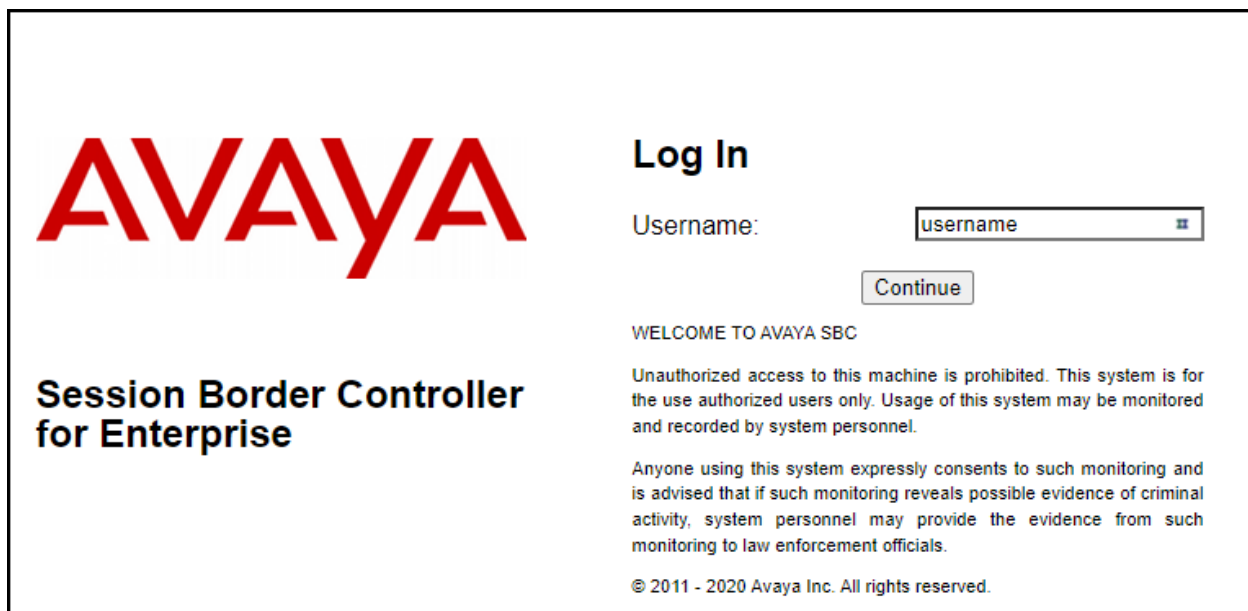
Repeat the above procedures as needed to define additional dial patterns.

8. Configure Avaya Session Border Controller for Enterprise

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

8.1. System Access

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



The image shows the login page of the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, the "Log In" section contains a "Username:" label, a text input field with "username" inside, 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 - 2020 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_SBCE** in the sample configuration.

The screenshot shows the Avaya SBCE 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 Dashboard' with sub-items: 'Software Management', 'Device Management', 'System Administration', 'Templates', 'Backup/Restore', and 'Monitoring & Logging'. The main content area is titled 'Dashboard' and features the Avaya logo. It contains several sections: 'Information' (System Time, Version, GUI Version, Build Date, License State, Aggregate Licensing Overages, Peak Licensing Overage Count, Last Logged in at, Failed Login Attempts), 'Installed Devices' (listing EMS and Avaya_SBCE), 'Active Alarms (past 24 hours)' (None found), and 'Incidents (past 24 hours)' (Avaya_SBCE: Registration Successful, Server is UP).

Information	
System Time	10:32:53 AM EDT Refresh
Version	10.1.0.0-32-21432
GUI Version	10.1.0.0-21432
Build Date	Thu Dec 02 21:33:10 UTC 2021
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	05/03/2022 10:22:18 EDT
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBCE

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
Avaya_SBCE: Registration Successful, Server is UP

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

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

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

Certificates

Client Profiles

Server Profiles

SNI Group

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Dashboard

Information	
System Time	11:26:02 AM EDT Refresh
Version	10.1.0.0-32-21432
GUI Version	10.1.0.0-22609
Build Date	Thu Nov 10 12:33:00 UTC 2022
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	03/27/2023 11:12:42 EDT
Failed Login Attempts	0

Active Alarms (past 24 hours)	
None found.	

Installed Devices	
EMS	
Avaya_SBCE	

Incidents (past 24 hours)	
None found.	

8.2. Device Management

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

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

Session Border Controller for Enterprise

AVAYA

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

Device Management

Devices Updates Licensing Key Bundles License Compliance

Device Name	Management IP	Version	Status
Avaya_SBCE	[Blurred]	10.1.0.0-32-21432	Commissioned

Reboot Shutdown Restart Application View Edit Uninstall

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

System Information: Avaya_SBCE

General Configuration

Appliance Name	Avaya_SBCE
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

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	<input checked="" type="checkbox"/>	
Available: Yes		

Network Configuration

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

DNS Configuration

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

Management IP(s)

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

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

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

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

8.3. TLS Management

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

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

8.3.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

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



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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The left-hand menu lists various management options, with 'TLS Management' and 'Certificates' highlighted. The main content area, titled 'Certificates', features 'Install' and 'Generate CSR' buttons. It contains two sections: 'Installed Certificates' and 'Installed CA Certificates'. Each section lists certificates with their names and associated 'View' and 'Delete' actions.

Installed Certificates	
[blurred]	View Delete
[blurred]	View Delete
[blurred]	View Delete
sbcInternal.pem	View Delete

Installed CA Certificates	
[blurred]	View Delete
[blurred]	View Delete
[blurred]	View Delete
[blurred]	View Delete
[blurred]	View Delete
default.pem	View Delete

8.3.2. Server Profiles

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

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

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

Edit Profile X

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

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

TLS Profile

Profile Name: sbcInternal

Certificate: sbcInternal.pem

SNI Options: None

SNI Group: None

Certificate Verification

Peer Verification: None

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

Peer Certificate Revocation Lists:

Verification Depth: 0

Next

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the Avaya logo on the right.

On the left is a sidebar menu with the following items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (expanded), Certificates, Client Profiles, **Server Profiles** (highlighted), SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging.

The main content area is titled 'Server Profiles: sbcInternal' and features an 'Add' button. Below this is a list of server profiles: 'Outside_Server', 'Inside_Server', 'Clearcom_Outside_Server', 'IPO_Inside_Server', 'Remote_Worker_Dec17', and 'sbcInternal' (selected and highlighted in red). A 'Delete' button is located at the top right of the profile list.

The selected 'sbcInternal' profile is shown in a detailed view with the following configuration:

- TLS Profile**
 - Profile Name: sbcInternal
 - Certificate: sbcInternal.pem
 - SNI Options: None
- Certificate Verification**
 - Peer Verification: None
 - Extended Hostname Verification: ☐
- Renegotiation Parameters**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**
 - Version: ☒ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0
 - Ciphers: ☒ Default ☐ FIPS ☐ Custom
 - Value: HIGH:IDH:1ADH:1MD5:1aNULL:1eNULL:@STRENGTH

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

8.3.3. Client Profiles

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

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

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

The screenshot shows a web-based configuration window titled "Edit Profile" with a close button (X) in the top right corner. The window contains two main sections: "TLS Profile" and "Certificate Verification".

Warning Message: A red banner at the top states: "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 Section:

- Profile Name:** A text input field containing "sbclInternal".
- Certificate:** A dropdown menu showing "sbclInternal.pem".
- SNI:** A checkbox labeled "Enabled" which is currently unchecked.

Certificate Verification Section:

- Peer Verification:** A label with the value "Required" next to it.
- Peer Certificate Authorities:** A dropdown menu showing "default.pem".
- Peer Certificate Revocation Lists:** An empty dropdown menu.
- Verification Depth:** A text input field containing the number "1".
- Extended Hostname Verification:** A checkbox which is currently unchecked.
- Server Hostname:** An empty text input field.

At the bottom right of the form is a "Next" button.

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

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

Session Border Controller for EnterpriseAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services▸ Domain Policies▸ TLS ManagementCertificates**Client Profiles**Server ProfilesSNI Group▸ Network & Flows▸ DMZ Services▸ Monitoring & Logging

Client Profiles: sbcInternal

AddDelete

Client Profiles

CenturyLink_ClientOutside_ClientClearcom_Outside_ClientRemote_Worker_Dec17MiguelsOutsideProfileInside_ClientIPO_Inside_Client**sbcInternal**

Click here to add a description.

Client Profile

TLS Profile

Profile Name

sbcInternal

Certificate

sbcInternal.pem

SNI

☐ Enabled

Certificate Verification

Peer Verification

Required

Peer Certificate Authorities

default.pem

Peer Certificate Revocation Lists

Verification Depth

1

Extended Hostname Verification

☐

Renegotiation Parameters

Renegotiation Time

0

Renegotiation Byte Count

0

Handshake Options

Version

☒ TLS 1.2☐ TLS 1.1☐ TLS 1.0

Ciphers

☒ Default☐ FIPS☐ Custom

Value

HIGH:IDH:IADH:IMD5:1aNULL:1eNULL:@STRENG

Edit

HG; Reviewed:
SPOC 5/4/2023

Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

80 of 133
CBTSAura101EP81

8.4. Network Management

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

Select **Network Management** from the **Network & Flows** on the left-side menu. On the **Networks** tab, verify or enter the network information as needed.

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

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.

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

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

8.5. Media Interfaces

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

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (not shown).

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

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

- Name:** A text input field containing "Private_med".
- IP Address:** A section with two dropdown menus. The first dropdown shows "Network_A1 (A1, VLAN 0)" and the second dropdown shows "10.64.101.243".
- Port Range:** Two text input fields containing "35000" and "40000" separated by a hyphen.
- Finish:** A button at the bottom center of the dialog.

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

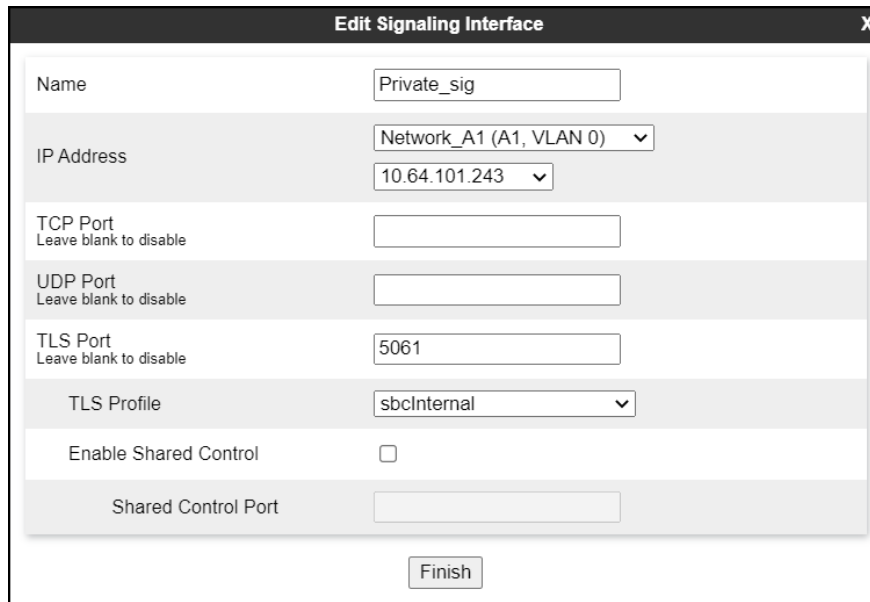
Port Range -

8.6. Signaling Interfaces

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

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (not shown).

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 7.6**.
- Select a **TLS Profile** (**Section 8.3.2**).
- Click **Finish**.



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

- Name:** A text input field containing "Private_sig".
- IP Address:** A section with two dropdown menus. The first menu is set to "Network_A1 (A1, VLAN 0)" and the second menu is set to "10.64.101.243".
- TCP Port:** A text input field with the instruction "Leave blank to disable" below it.
- UDP Port:** A text input field with the instruction "Leave blank to disable" below it.
- TLS Port:** A text input field containing "5061" with the instruction "Leave blank to disable" below it.
- TLS Profile:** A dropdown menu set to "sbcInternal".
- Enable Shared Control:** A checkbox that is currently unchecked.
- Shared Control Port:** A text input field.
- Finish:** A button located 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 Cincinnati Bell in the sample configuration.
- Click **Finish**.

Edit Signaling Interface	
Name	Public_sig
IP Address	Network_B1 (B1, VLAN 0) 10.10.80.51
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	
Finish	

8.7. Server Interworking

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

8.7.1. Server Interworking Profile – Enterprise

Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Configuration Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select **avaya-ru** from the list of pre-defined profiles. Click **Clone** (not shown).

Device: Avaya_SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users

Session Border Controller for Enterprise

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: avaya-ru

Add

Interworking Profiles

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

OCS-FrontEnd-Server

Avaya-SM

Avaya-IPO

Avaya-CS1000

Avaya-CM

cs2100

SP-General

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

General Timers Privacy URI Manipulation Header Manipulation Advanced

General

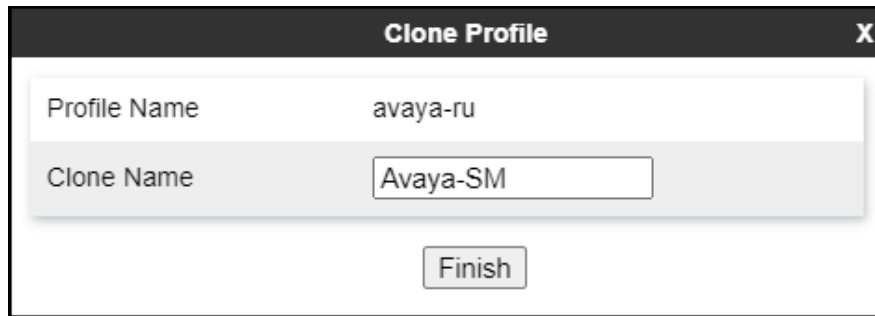
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme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

HG; Reviewed:
SPOC 5/4/2023

Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

86 of 133
CBTSAura101EP81

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



The image shows a 'Clone Profile' dialog box with a dark header bar containing the title 'Clone Profile' and a close button 'X'. The dialog contains two input fields: 'Profile Name' with the value 'avaya-ru' and 'Clone Name' with the value 'Avaya-SM'. A 'Finish' button is located at the bottom center of the dialog.

Clone Profile	
Profile Name	avaya-ru
Clone Name	Avaya-SM
<div>Finish</div>	

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

- On the **General** tab, set **SIPS Required** to **No**.
- On the **General** tab, check **T.38 Support** to enable it.
- Leave remaining fields with default values.
- Click **Finish** (not shown).

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

Device: Avaya_SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users

Session Border Controller for Enterprise

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: Avaya-SM

Add

Interworking Profiles

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

OCS-FrontEnd-Server

Avaya-SM

Avaya-IPO

Avaya-CS1000

Avaya-CM

cs2100

SP-General

Click here

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

Yes

URI Scheme

SIP

Via Header Format

RFC3261

SIPS Required

No

Mediasec

No

HG; Reviewed:
SPOC 5/4/2023

Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

88 of 133
CBTSAura101EP81

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

Device: Avaya_SBCE ▾

Alarms

Incidents

Status ▾

Logs ▾

Diagnostics

Users

Session Border Controller for Enterprise

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

Interworking Profiles: Avaya-SM

Add

Interworking Profiles

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

OCS-FrontEnd-Server

Avaya-SM

Avaya-IPO

Avaya-CS1000

Avaya-CM

cs2100

SP-General

Click here to add a device

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

Record Routes

Both Sides

Include End Point IP for Context Lookup

Yes

Extensions

Avaya

Diversion Manipulation

No

Has Remote SBC

Yes

Route Response on Via Port

No

Relay INVITE Replace for SIPREC

No

MOBX Re-INVITE Handling

No

NATing for 301/302 Redirection

Yes

DTMF

DTMF Support

None

Edit

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**.
- On the **General** tab, set **SIPS Required** to **No** (not shown).
- On the **General** tab, check **T.38 Support** to enable it (not shown).



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.

- 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_SBCE ▾

Alarms

Incidents

Status ▾

Logs ▾

Diagnostics

Users

Session Border Controller for Enterprise

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-Server

cisco-ccm

cups

OCS-FrontEnd-Server

Avaya-SM

Avaya-IPO

Avaya-CS1000

Avaya-CM

cs2100

SP-General

Click here

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

General

Hold Support

180 Handling

181 Handling

182 Handling

183 Handling

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

Via Header Format

SIPS Required

Mediasec

None

None

None

None

No

None

No

Yes

No

No

No

No

Yes

SIP

RFC3261

No

No

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

Device: Avaya_SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsers

Session Border Controller for Enterprise

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

Interworking Profiles: SP-General

Add

Interworking Profiles

avaya-ruOCS-Edge-Servercisco-ccmcupsOCS-FrontEnd-ServerAvaya-SMAvaya-IPOAvaya-CS1000Avaya-CMcs2100**SP-General**

Click here to add new profile

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

HG; Reviewed:
SPOC 5/4/2023

Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

92 of 133
CBTSAura101EP81

8.8. Signaling Manipulation

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

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

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

- Remove unwanted XML information in UPDATES from being sent to CBTS.
- Modify the P-Asserted-Identity header on outbound INVITEs from Experience Portal to the PSTN, with the DID number assigned to Experience Portal, known to CBTS.

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

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

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



The screenshot shows the Avaya Signaling Manipulation Editor interface. At the top, the title "Signaling Manipulation Editor" is displayed in large black font, and the Avaya logo is in the top right corner. Below the title bar, there is a "Title" field containing the text "CBTS" and a "Save" button. The main area is a code editor with a light blue background, showing a script with line numbers 1 through 26. The script is a SigMa script for manipulating SIP messages.

```
1 within session "ALL"
2
3 {
4   act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
5   {
6
7     //Remove unwanted xml element information from the SDP in SIP messages sent to the Service Provider.
8     remove(%BODY[1]);
9
10  }
11  }
12
13  // OPTIONAL Experience Portal - modify PAI Header
14  within session "INVITE"
15  {
16    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
17    {
18      if (%INITIAL_REQUEST = "true") then
19      {
20        if (%HEADERS["User-Agent"][1].regex_match("Avaya\\-VoicePortal")) then
21        {
22          %HEADERS["P-Asserted-Identity"][1].URI.USER = "5135628693";
23        }
24      }
25    }
26  }
```

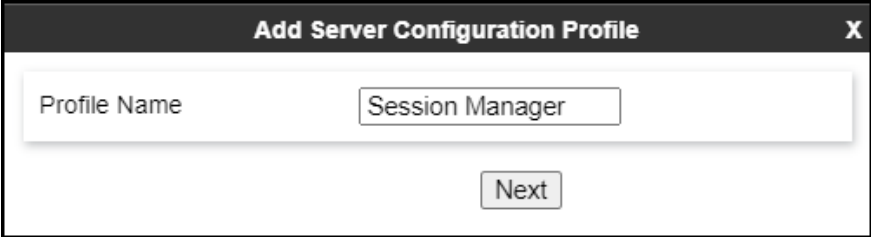
8.9. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and Cincinnati Bell 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.

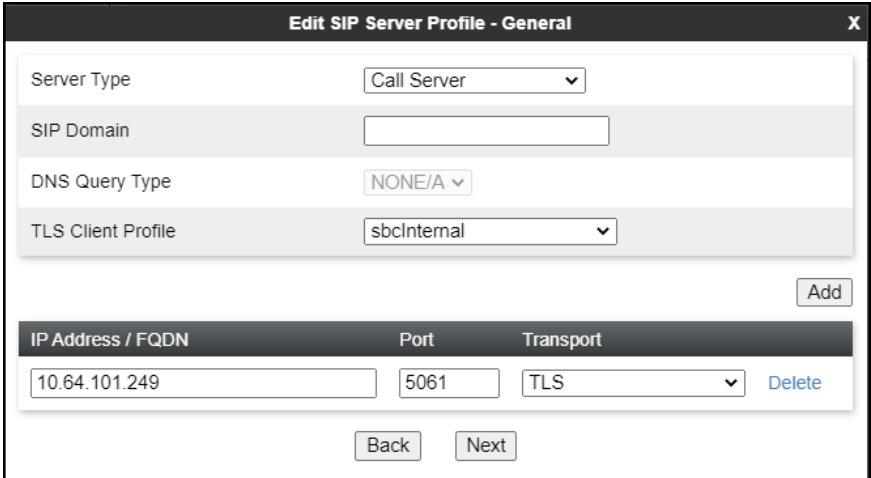
- Enter an appropriate **Profile Name** similar to the screen below.
- Click **Next**.



Add Server Configuration Profile X

Profile Name

- On the **Edit SIP Server Profile – General** tab select **Call Server** from the drop-down menu under the **Server Type**.
- On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 7.5**).
- Enter **5061** under **Port** and select **TLS** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously created in **Section 7.6**.
- Select a **TLS Profile** (**Section 8.3.3**).
- Click **Next**.



Edit SIP Server Profile - General X

Server Type

SIP Domain

DNS Query Type

TLS Client Profile

IP Address / FQDN	Port	Transport	
<input type="text" value="10.64.101.249"/>	<input type="text" value="5061"/>	<input type="text" value="TLS"/>	<input type="button" value="Delete"/>

- 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 a list of configuration options, each with a label and a control element (checkbox or dropdown menu). The options are: "Enable DoS Protection" (checkbox, unchecked), "Enable Grooming" (checkbox, checked), "Interworking Profile" (dropdown menu, set to "Avaya-SM"), "Signaling Manipulation Script" (dropdown menu, set to "None"), "Securable" (checkbox, unchecked), "Enable FGDN" (checkbox, unchecked), "TCP Failover Port" (text input, set to "5060"), "TLS Failover Port" (text input, set to "5061"), "Tolerant" (checkbox, unchecked), "URI Group" (dropdown menu, set to "None"), and "NG911 Support" (checkbox, unchecked). At the bottom of the window, there are two buttons: "Back" and "Finish".

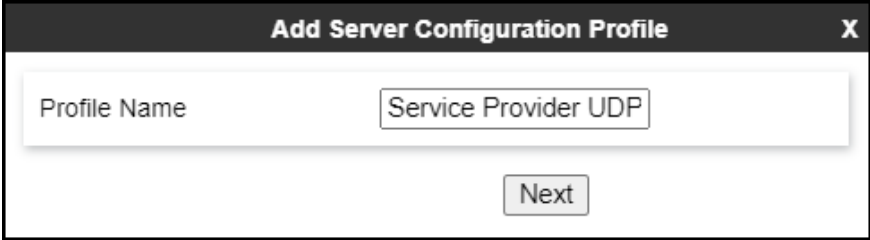
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-SM
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>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

Back Finish

8.9.2. Server Configuration Profile – Service Provider

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

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

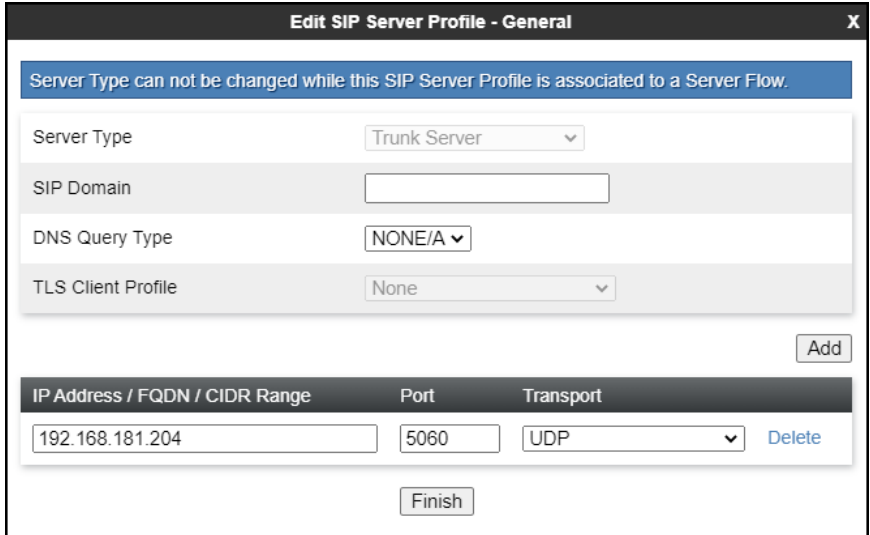


Add Server Configuration Profile X

Profile Name

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 **192.168.181.204** (Cincinnati Bell SIP proxy IP address). This information was provided by Cincinnati Bell.
- Enter **5060** under **Port** and select **UDP** for **Transport**.
- Click **Next**.



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

SIP Domain

DNS Query Type

TLS Client Profile

Add

IP Address / FQDN / CIDR Range	Port	Transport	
<input type="text" value="192.168.181.204"/>	<input type="text" value="5060"/>	<input type="text" value="UDP"/>	Delete

Finish

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

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

- Check the **Enable Heartbeat** box.
- Method: Select **OPTIONS**.
- **Frequency**: Enter the amount of time (in seconds) between SIP OPTIONS messages that will be sent from the enterprise to the Service Provider Proxy Server. **300** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the OPTIONS messages are built using the following:
 - **From URI**: Enter **OPTIONS** and the public IP address of the Avaya SBCE (10.10.80.51), as shown on the screen below.
 - **To URI**: Enter **OPTIONS** and Cincinnati Bell's SIP Proxy IP address (192.168.181.204), as shown on the screen below.
 - Click **Next**.

Edit SIP Server Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS ▾
Frequency	300 seconds
From URI	OPTIONS@10.10.80.51
To URI	OPTIONS@192.168.181.204
Finish	

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

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

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

Add SIP Server Profile - Advanced

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	CBTS
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"/>

Back Finish

8.10.Routing

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

8.10.1. Routing Profile – Enterprise

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

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

Routing Profile

Profile Name: Route_to_SM

Next

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

Profile : Route_to_SM - Edit Rule

URI Group

*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

☒

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

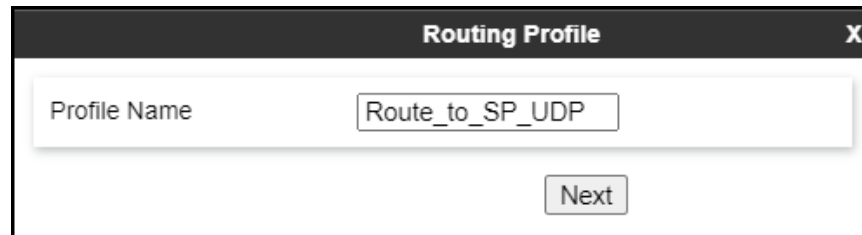
Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Session Manager	10.64.101.249:5060	None	Delete

Finish

8.10.2. Routing Profile – Service Provider

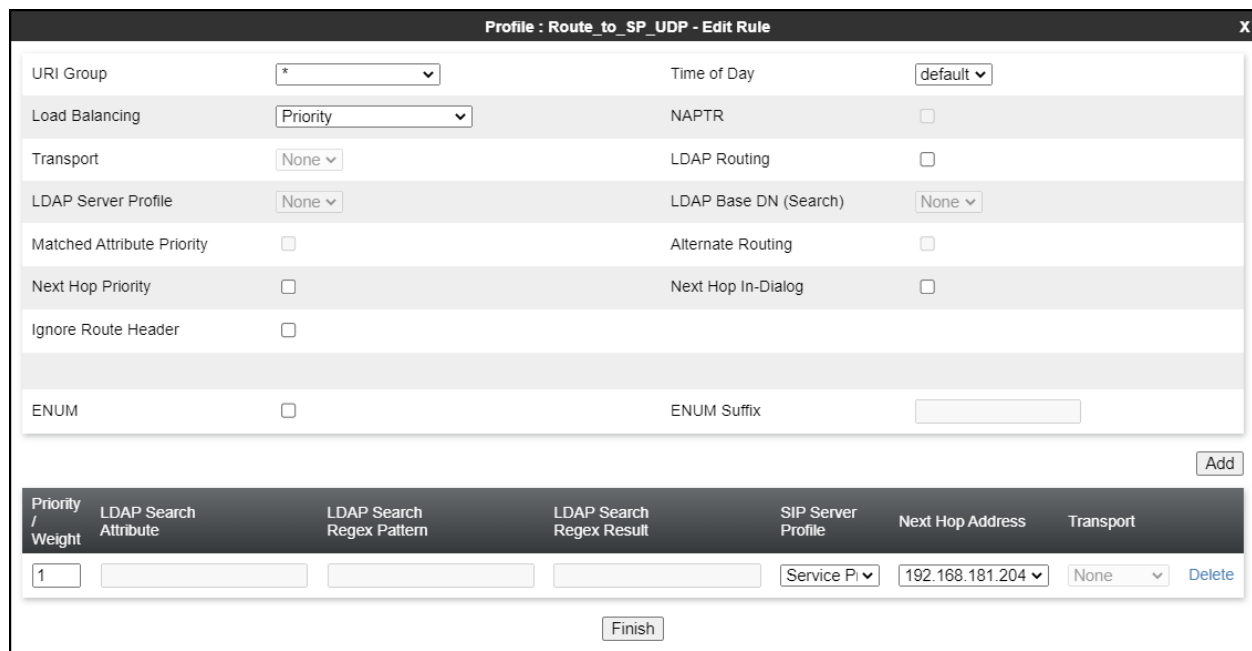
Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

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



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

- Under **Load Balancing** select **Priority**.
- Click the **Add** button to enter the next-hop address.
- Under **SIP Server Profile**, select **Service Provider UDP**.
- The **Next Hop Address** is populated automatically with **192.168.181.204:5060 (UDP)**. Cincinnati Bell SIP Proxy IP address, Port and Transport, Server Configuration Profile defined in **Section 8.9.2**.
- Click **Finish**



The image shows a dialog box titled "Profile: Route_to_SP_UDP - Edit Rule" with a close button (X) in the top right corner. The dialog contains several configuration fields and a table at the bottom.

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 type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	

At the bottom right of the dialog is an **Add** button.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Service P	192.168.181.204	None	Delete

At the bottom center of the dialog is a **Finish** button.

8.11.Topology Hiding

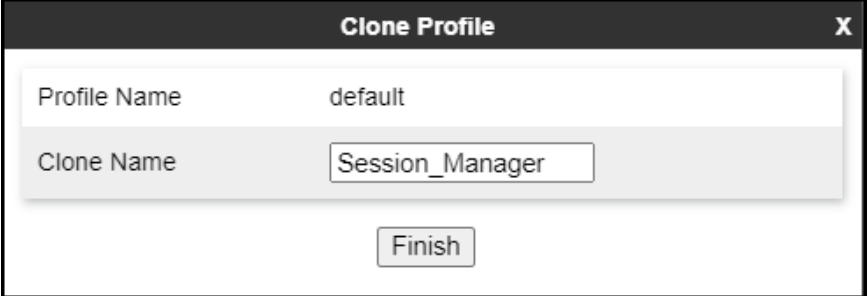
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

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**.

Edit Topology Hiding ProfileX

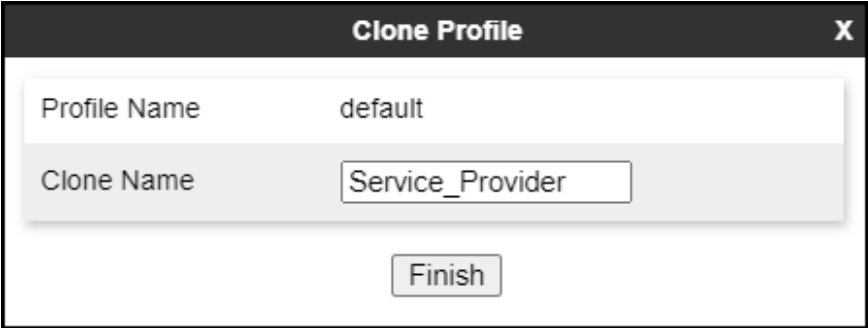
Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Overwrite	devconnect.com	Delete
SDP	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
From	IP/Domain	Overwrite	devconnect.com	Delete
Referred-By	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	devconnect.com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

Finish

8.11.2. Topology Hiding Profile – Service Provider

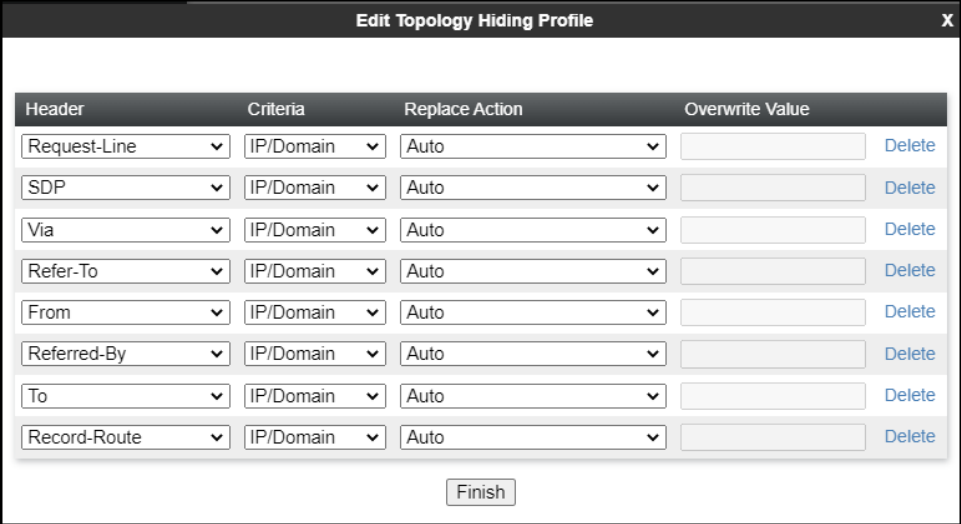
To add the Topology Hiding Profile in the service provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select **default** from the list of pre-defined profiles and click the **Clone** button (not shown).

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



The 'Clone Profile' dialog box has a title bar with 'Clone Profile' and a close button 'X'. It contains two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'Service_Provider'. A 'Finish' button is located at the bottom center.

- Default values were used for all other fields.



The 'Edit Topology Hiding Profile' dialog box has a title bar with 'Edit Topology Hiding Profile' and a close button 'X'. It contains a table with the following data:

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

A 'Finish' button is located at the bottom center.

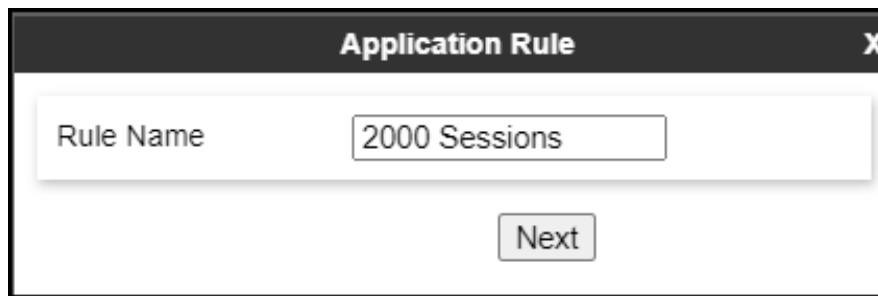
8.12.Domain Policies

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 SBCE security product. For the compliance test, one media rule (shown below) was created toward Session Manager and a default media rule was used toward the Service Provider.

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

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

Media Encryption
X

Audio Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

RTP

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

2^

Leave blank to match any value.

Interworking

☒

Symmetric Context Reset

☒

Key Change in New Offer

☐

Video Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

RTP

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

2^

Leave blank to match any value.

Interworking

☒

Symmetric Context Reset

☒

Key Change in New Offer

☐

Miscellaneous

Capability Negotiation

☒

Finish

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

- For the compliance test, the **default-low-med** Media Rule was used in the Service Provider direction, shown below.

Media Encryption

Audio Encryption

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

Video Encryption

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

Miscellaneous

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

Finish

8.12.3. Signaling Rules

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

Device: Avaya_SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsers

Session Border Controller for Enterprise

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

Signaling Rules

default

No-Content-Type-Checks

SessMgr_CM_SigRule

OPTIONS

Remote Workers

Remove_Update

Contact

Remove PAI

Remove PAI_1

Remove_headers

Remove Record Route

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

GeneralRequestsResponsesRequest HeadersResponse HeadersSignaling QoSUCID

Inbound

RequestsAllow

Non-2XX Final ResponsesAllow

Optional Request HeadersAllow

Optional Response HeadersAllow

Outbound

RequestsAllow

Non-2XX Final ResponsesAllow

Optional Request HeadersAllow

Optional Response HeadersAllow

Content-Type Policy

Enable Content-Type Checks☒

ActionAllowMultipart ActionAllow

Exception ListException List

Edit

HG; Reviewed:
SPOC 5/4/2023

Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

110 of 133
CBTSAura101EP81

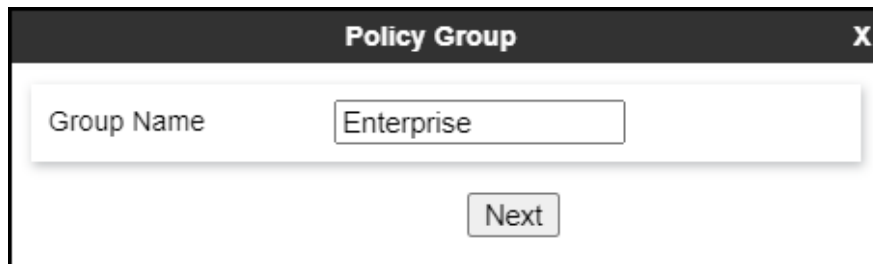
8.13.End Point Policy Groups

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

8.13.1. End Point Policy Group – Enterprise

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

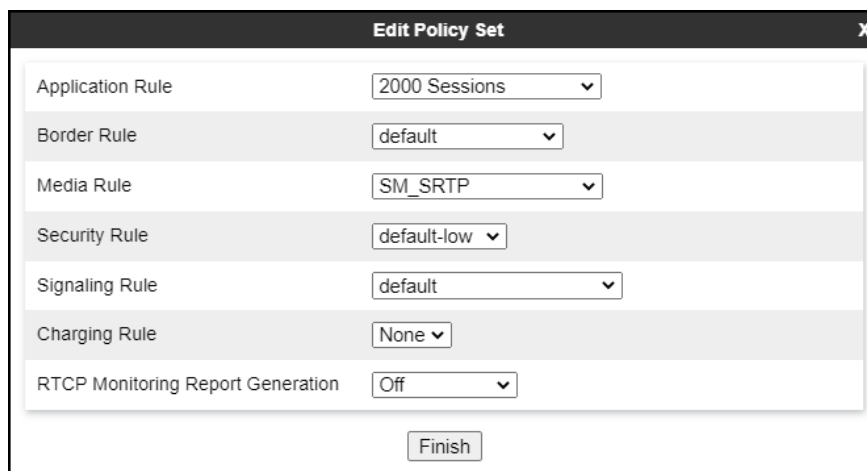
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



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

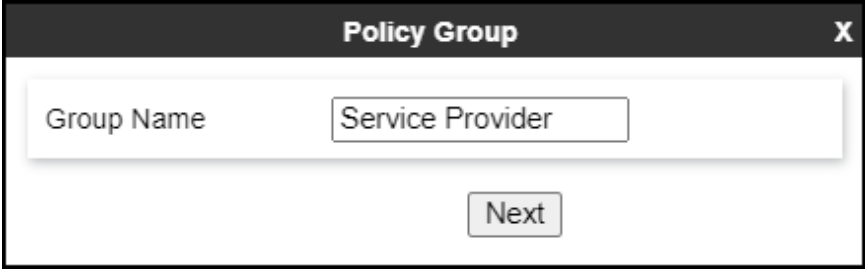


The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains several rows, each with a label and a dropdown menu. The labels and their corresponding dropdown values are: "Application Rule" (2000 Sessions), "Border Rule" (default), "Media Rule" (SM_SRTP), "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".

8.13.2. 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).

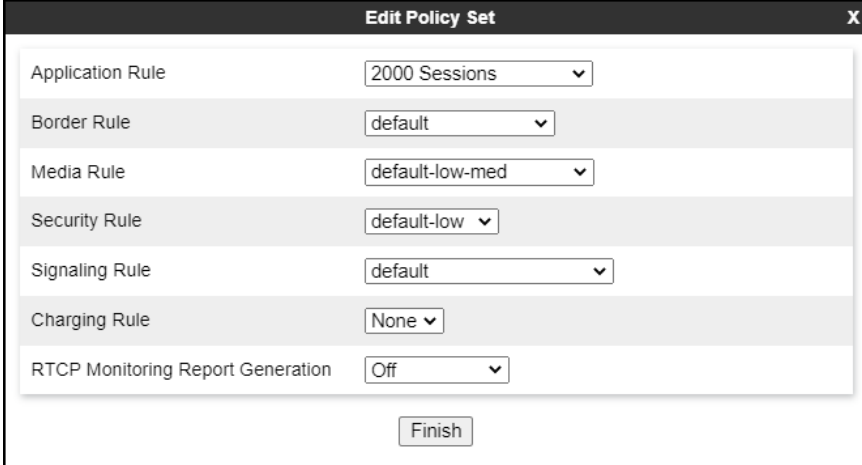
- Enter an appropriate name in the **Group Name** field (**Service Provider** was used).
- Click **Next**.



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 the input field, there is a button labeled "Next".

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

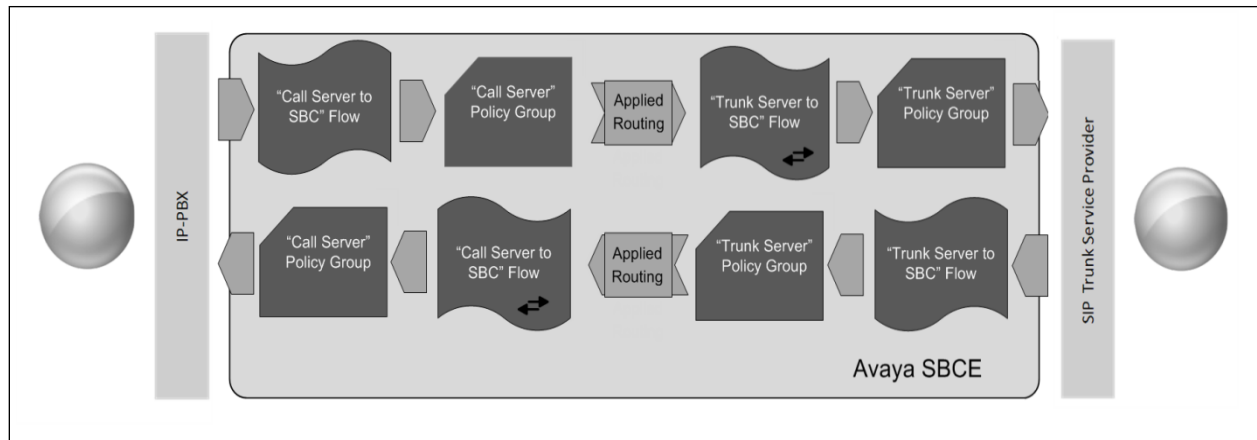
- **Application Rule: 2000 Sessions** (Section 8.12.1).
- **Border Rule: default**.
- **Media Rule: default-low-med** (Section 8.12.2).
- **Security Rule: default-low**.
- **Signaling Rule: default** (Section 8.12.3).
- Click **Finish**.



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 are "Application Rule", "Border Rule", "Media Rule", "Security Rule", "Signaling Rule", "Charging Rule", and "RTCP Monitoring Report Generation". The corresponding dropdown values are "2000 Sessions", "default", "default-low-med", "default-low", "default", "None", and "Off". At the bottom of the dialog, there is a button labeled "Finish".

8.14.End Point Flows

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



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

8.14.1. End Point Flow – 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.

Edit Flow: SP to SM Flow X

Flow Name	SP to SM Flow
SIP Server Profile	Service Provider UDP ▾
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 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 X

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_UDP ▼
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. Cincinnati Bell SIP Trunking Service Configuration

To use Cincinnati Bell SIP Trunking Service, a customer must request the service from Cincinnati Bell using the established sales processes. The process can be started by contacting Cincinnati Bell via the corporate web site at: <https://www.altafiber.com/business/support/sip-trunking-support>

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

Cincinnati Bell will provide the following information:

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

10. Verification and Troubleshooting

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

10.1.General Verification Steps

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

10.2.Communication Manager Verification

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

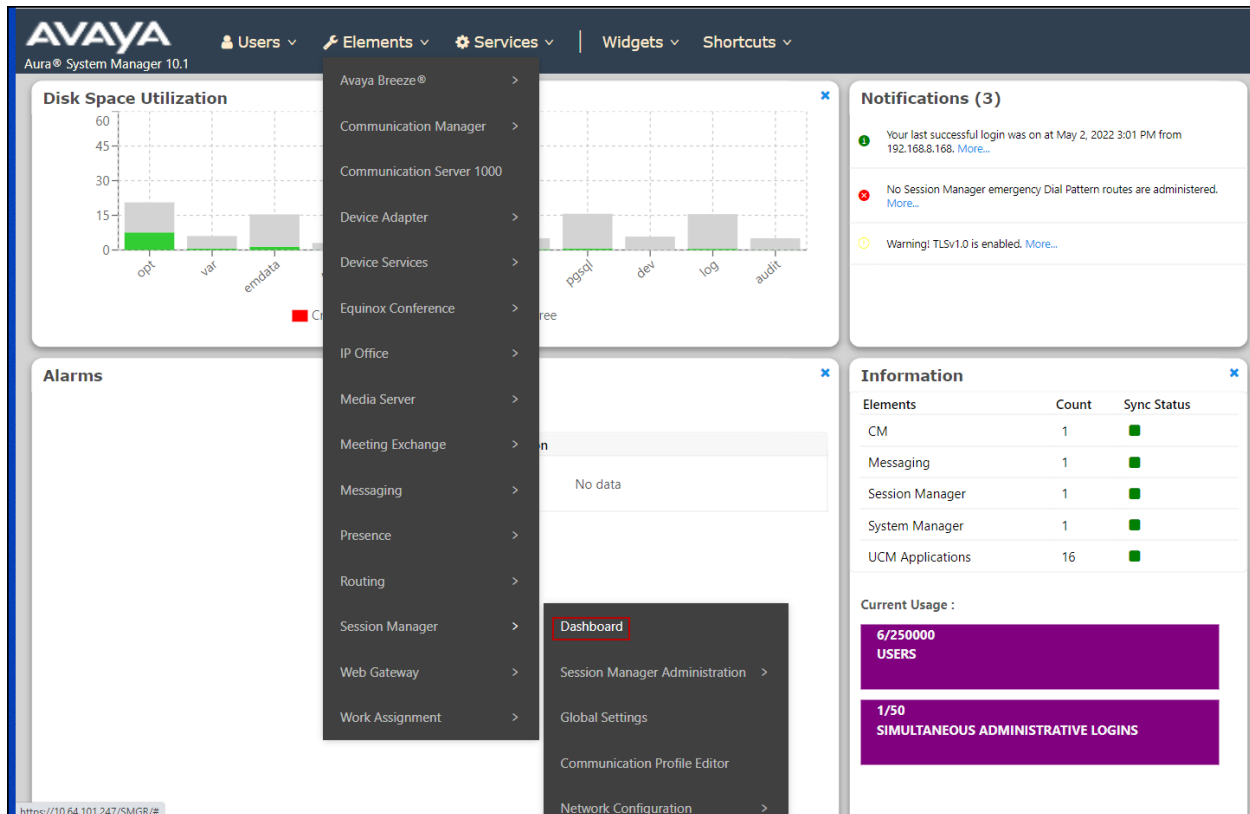
- **list trace station** <extension number>
Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>
Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>
Displays signaling group service state.
- **status trunk** <trunk group number>
Displays trunk group service state.
- **status station** <extension number>

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

10.3.Session Manager Verification

The Session Manager configuration may be verified via System Manager.

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



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

In the **Entity Monitoring** column, Session Manager shows that there are **3** alarms out of the **9** Entities defined.

Session Manager Dashboard

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

Session Manager Instances

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

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	2/10	0	2/2	✓	✓	Normal	Enabled	3	10.1.2.0.1012016

Select : All, None

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

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 Show All Filter: Enable

SIP Entity Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
Avaya SBCE	IPv4	10.64.101.243	5061	TLS	FALSE	DOWN	500 Server Internal Error	DOWN
AA-Messaging	IPv4	10.64.101.250	5060	TCP	FALSE	DOWN	408 Request Timeout	DOWN
Avaya Experience Portal	IPv4	10.64.101.252	5061	TLS	FALSE	UP	200 OK	UP
CM-TG5	IPv4	10.64.101.241	5075	TLS	FALSE	UP	200 OK	UP
CM-TG1	IPv4	10.64.101.241	5061	TLS	FALSE	UP	200 OK	UP
CM-TG108	IPv4	10.64.101.241	5068	TLS	FALSE	UP	200 OK	UP
Avaya Messaging	IPv4	10.64.101.158	5061	TLS	FALSE	UP	200 OK	UP
SBCE-ATT	IPv4	10.64.91.42	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
CM-TG2	IPv4	10.64.101.241	5071	TLS	FALSE	UP	200 OK	UP
CM-TG98	IPv4	10.64.101.241	5065	TLS	FALSE	UP	500 Service Unavailable(Signaling Resources Unavailable)	UP

Select : None

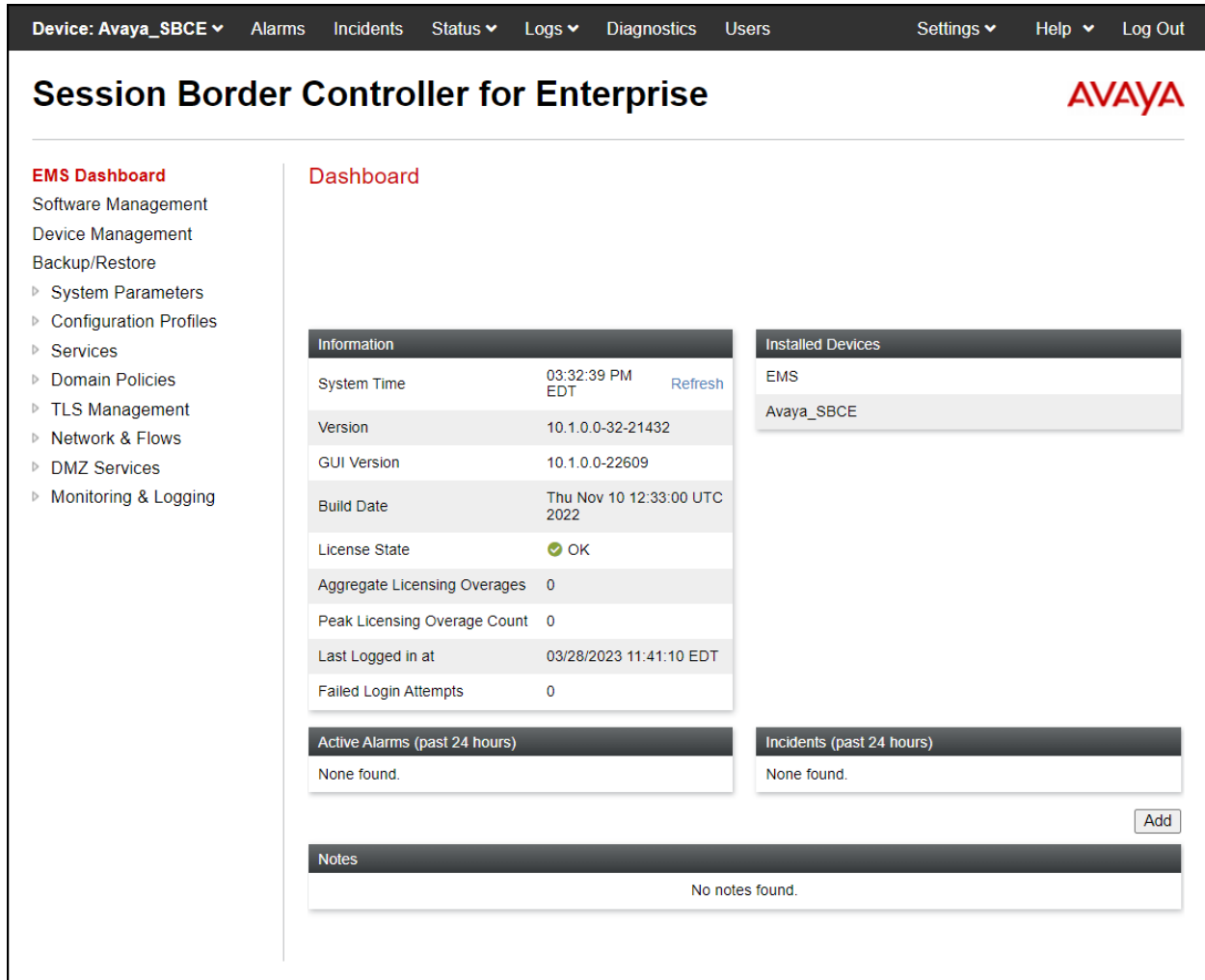
Other Session Manager useful verification and troubleshooting tools include:

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

10.4.Ayaya SBCE Verification

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

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



The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. At the top, a dark navigation bar contains the text "Device: Avaya_SBCE" followed by menu items: Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. Below this, the main header area features the title "Session Border Controller for Enterprise" and the Avaya logo. A left-hand sidebar lists the "EMS Dashboard" with sub-items: Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled "Dashboard" and contains several panels. The "Information" panel lists system details: System Time (03:32:39 PM EDT with a Refresh link), Version (10.1.0.0-32-21432), GUI Version (10.1.0.0-22609), Build Date (Thu Nov 10 12:33:00 UTC 2022), License State (OK with a green checkmark), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged In at (03/28/2023 11:41:10 EDT), and Failed Login Attempts (0). The "Installed Devices" panel shows a list with "EMS" and "Avaya_SBCE". The "Active Alarms (past 24 hours)" and "Incidents (past 24 hours)" panels both display "None found.". An "Add" button is located to the right of the incidents panel. The "Notes" panel at the bottom shows "No notes found.". The Avaya logo is positioned in the top right corner of the dashboard area.

Information	
System Time	03:32:39 PM EDT Refresh
Version	10.1.0.0-32-21432
GUI Version	10.1.0.0-22609
Build Date	Thu Nov 10 12:33:00 UTC 2022
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged In at	03/28/2023 11:41:10 EDT
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBCE

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

Notes
No notes found.

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

Device: Avaya_SBCE ▾

Help

EMS

Avaya_SBCE

AVAYA

Alarms

☒ ID

Details

State

Time

Device

No alarms found for this device.

Clear Selected

Clear All

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

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

Session Border Controller for Enterprise

EMS Dashboard

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

Dashboard

Information	
System Time	03:32:39 PM EDT Refresh
Version	10.1.0.0-32-21432
GUI Version	10.1.0.0-22609
Build Date	Thu Nov 10 12:33:00 UTC 2022
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	03/28/2023 11:41:10 EDT
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBCE

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found. [Add](#)

Notes

No notes found.

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

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

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

Session Border Controller for Enterprise

EMS Dashboard

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

Dashboard

Information	
System Time	03:32:39 PM EDT Refresh
Version	10.1.0.0-32-21432
GUI Version	10.1.0.0-22609
Build Date	Thu Nov 10 12:33:00 UTC 2022
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	03/28/2023 11:41:10 EDT
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBCE

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found. [Add](#)

Notes
No notes found.

The following screen shows the Cincinnati Bell server status.

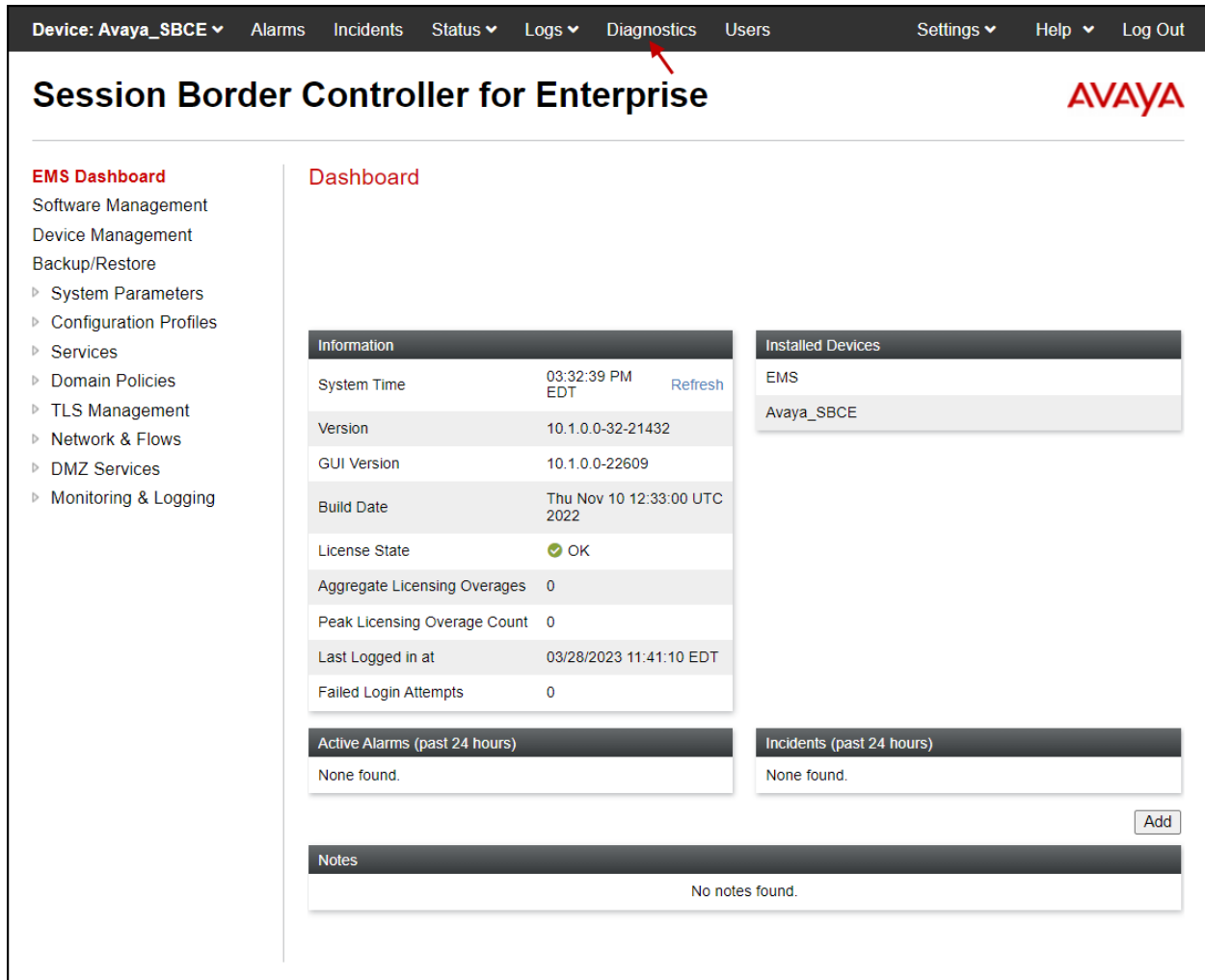
Device: Avaya_SBCE ▾ [Help](#)

Status

Server Status

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
Service Provider UDP	.181.204	181.204	5060	UDP	UP	UNKNOWN	03/28/2023 15:41:11 EDT

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



The screenshot shows the Avaya SBCE Dashboard. The top navigation bar includes links for Device: Avaya_SBCE, Alarms, Incidents, Status, Logs, **Diagnostics** (highlighted with a red arrow), Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo. On the left, the "EMS Dashboard" menu lists various management options. The main content area is titled "Dashboard" and contains several sections: "Information" (System Time, Version, GUI Version, Build Date, License State, etc.), "Installed Devices" (listing EMS and Avaya_SBCE), "Active Alarms (past 24 hours)", "Incidents (past 24 hours)", and "Notes".

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

Session Border Controller for Enterprise

EMS Dashboard

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

Dashboard

Information	
System Time	03:32:39 PM EDT Refresh
Version	10.1.0.0-32-21432
GUI Version	10.1.0.0-22609
Build Date	Thu Nov 10 12:33:00 UTC 2022
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged In at	03/28/2023 11:41:10 EDT
Failed Login Attempts	0

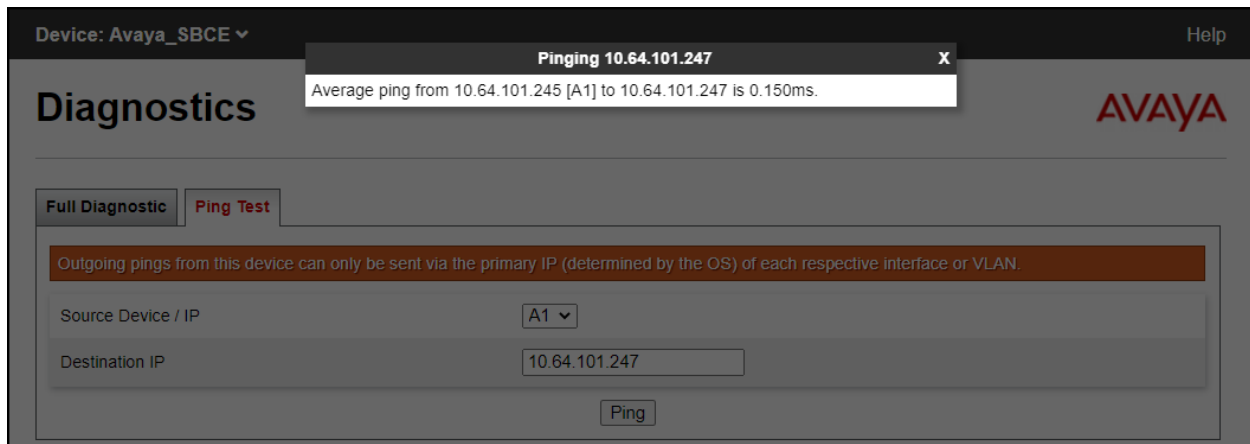
Installed Devices
EMS
Avaya_SBCE

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found. [Add](#)

Notes
No notes found.

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



The screenshot shows the Avaya SBCE Diagnostics page. The top navigation bar includes links for Device: Avaya_SBCE, Help, and a "Pinging 10.64.101.247" status bar. The main header reads "Diagnostics" with the AVAYA logo. Below the header, there are tabs for "Full Diagnostic" and "Ping Test". A message states: "Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN." The "Ping Test" section includes a "Source Device / IP" dropdown menu set to "A1", a "Destination IP" input field set to "10.64.101.247", and a "Ping" button.

Device: Avaya_SBCE ▾ Help

Diagnostics

Pinging 10.64.101.247 x
Average ping from 10.64.101.245 [A1] to 10.64.101.247 is 0.150ms.

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: 10.64.101.247

[Ping](#)

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

Device: Avaya_SBCE ▾

Alarms

Incidents

Status ▾

Logs ▾

Diagnostics

Users

Settings ▾

Help ▾

Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▾ Monitoring & Logging

SNMP

Syslog Management

Debugging

Trace

Log Collection

DoS Learning

CDR Adjunct

Trace: Avaya_SBCE

Packet Capture

Captures

Packet Capture Configuration

Status

Ready

Interface

Any ▾

Local Address
IP:Port

All ▾ :

Remote Address
*, *Port, IP, IP:Port

Protocol

All ▾

Maximum Number of Packets to Capture

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

Start Capture

Clear

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo on the right. A left sidebar lists various management options, with 'Monitoring & Logging' expanded to show 'Trace' in red. The main content area is titled 'Trace: Avaya_SBCE' and features two tabs: 'Packet Capture' and 'Captures' (which is active). Below the tabs is a table listing captured files. The table has columns for 'File Name', 'File Size (bytes)', and 'Last Modified'. A single entry is shown: 'CBTS_20230328154731.pcap' with a size of 118,784 bytes and a timestamp of March 28, 2023 at 3:47:48 PM EDT. A 'Delete' link is present next to the file name. A 'Refresh' button is located in the top right corner of the table area.

File Name	File Size (bytes)	Last Modified
CBTS_20230328154731.pcap	118,784	March 28, 2023 at 3:47:48 PM EDT

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

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 for Enterprise 10.1, to connect to the Cincinnati Bell 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 for Enterprise on a Virtualized Environment Platform*, Release 10.1, Issue 1, December 2021.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1, Issue 1, December 2021.
- [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 for Enterprise – Refer Handling

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

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

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.

Create a URI Group for numbers intended for Communication Manager.

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

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

Step 3 - Enter the following:

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

Edit URI X

Each entry should match a valid SIP URI.

WARNING: Invalid or incorrectly entered regular expressions may cause unexpected results.

Note: This regular expression is case-insensitive.

Ex: [0-9]{3,5}\ user@domain\ com, (simple|advanced)\ -user[A-Z]{3}@.*

Scheme: ☒ sip:/sips: ☐ tel:

Type: ☐ Plain ☐ Dial Plan ☒ Regular Expression

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

Finish

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', '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 lists navigation options: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles (expanded), Domain DoS, Server Interworking, Media Forking, Routing, Topology Hiding, Signaling Manipulation, and URI Groups (highlighted in red). The main content area is titled 'URI Groups: internal-extensions' and features an 'Add' button. Below this is a list of URI Groups: 'URI Groups', 'Emergency', 'internal-exte...', 'test', 'Trunk 1', and 'Trunk 2'. The 'internal-exte...' group is selected, showing a description field with the placeholder 'Click here to add a description.' and an 'Add' button. Below the description is a 'URI Listing' table with one entry: '3[0-9]{3}@.*', which has 'Edit' and 'Delete' links. The bottom of the interface shows the 'URI Groups' section in the sidebar.

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**.
- **URI Group: internal-extensions**.
- Select **Finish**.

Editing Profile: SP-General

General

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

Finish

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

Device: Avaya_SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsers

Session Border Controller for Enterprise

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▸ Domain Policies▸ TLS Management▸ Network & Flows▸ DMZ Services▸ Monitoring & Logging

Interworking Profiles: SP-General

Add

Interworking Profiles

avaya-ruOCS-Edge-Servercisco-ccmcupsoCS-FrontEnd-ServerAvaya-SMAvaya-IPOAvaya-CS1000Avaya-CMcs2100**SP-General**

Click here to add new profile

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

General

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

HG; Reviewed:
SPOC 5/4/2023

Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

131 of 133
CBTSAura101EP81

14. Appendix B – SigMa Scripts

Following is the Signaling Manipulation script that was used in the configuration of the Avaya SBCE. 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 request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
```

```
//Remove unwanted xml element information from the SDP in SIP messages sent to the Service
Provider.
```

```
remove(%BODY[1]);
```

```
}
}
```

```
// OPTIONAL Experience Portal - modify PAI Header
```

```
within session "INVITE"
```

```
{
act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
    if (%INITIAL_REQUEST = "true") then
    {
        if (%HEADERS["User-Agent"][1].regex_match("Avaya\\-VoicePortal")) then
        {
            %HEADERS["P-Asserted-Identity"][1].URI.USER = "5135628693";
        }
    }
}
}
```

©2023 Avaya Inc. All Rights Reserved.

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

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