



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, Avaya Experience Portal 8.1 and Avaya Session Border Controller for Enterprise 10.1 with Verizon Business IP Trunking Service – Issue 1.0

## Abstract

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 10.1, Avaya Aura® Communication Manager Release 10.1, Avaya Experience Portal 8.1 and Avaya Session Border Controller for Enterprise Release 10.1 with the Verizon Business IP Trunking service. These Application Notes update previously published Application Notes with newer versions of Communication Manager, Session Manager, and Avaya Session Border Controller for Enterprise.

The Verizon Business IP Trunking service offer referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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, utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IP Trunking service.

# Table of Contents

1.	Introduction.....	5
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing .....	6
2.2.	Test Results .....	7
2.3.	History Info and Diversion Headers .....	8
2.4.	SIP Header Removal.....	9
2.5.	Support.....	9
3.	Reference Configuration.....	10
3.1.	Illustrative Configuration Information.....	12
3.3.	Call Flows .....	13
3.3.1	Communication Manager.....	13
3.3.2	Experience Portal.....	16
4.	Equipment and Software Validated .....	19
5.	Configure Avaya Aura® Communication Manager .....	20
5.1.	Verify Licensed Features .....	20
5.2.	System-Parameters Features .....	22
5.3.	Dial Plan.....	23
5.4.	Node Names.....	23
5.5.	Processor Ethernet Configuration .....	24
5.6.	IP Codec Sets .....	25
5.6.1	Codecs for IP Network Region 1 (calls within the CPE).....	25
5.6.2	Codecs for IP Network Region 2 (calls to/from Verizon) .....	26
5.7.	Network Regions .....	27
5.7.1	IP Network Region 1 – Local CPE Region .....	27
5.7.2	IP Network Region 2 – Verizon Trunk Region .....	28
5.8.	SIP Trunks .....	29
5.8.1	SIP Trunk for Inbound/Outbound Verizon calls.....	29
5.8.2	Local SIP Trunk (Avaya SIP Telephones, Messaging Access, etc.) .....	33
5.9.	Public Numbering .....	34
5.10.	Private Numbering.....	35
5.11.	Route Patterns .....	35
5.11.1	Route Pattern for National Calls to Verizon .....	35
5.11.2	Route Pattern for International Calls to Verizon .....	36
5.11.3	Route Pattern for Service Calls to Verizon.....	37
5.11.4	Route Pattern for Calls within the CPE .....	37
5.12.	Automatic Route Selection (ARS) Dialing.....	38
5.13.	Automatic Alternate Routing (AAR) Dialing.....	38
5.14.	Avaya G430 Media Gateway Provisioning .....	39
5.15.	Avaya Aura® Media Server Provisioning.....	40
5.16.	Save Translations .....	41
5.17.	Verify TLS Certificates – Communication Manager.....	42
6.	Configure Avaya Aura® Session Manager .....	43
6.1.	System Manager Login and Navigation .....	44
6.2.	SIP Domain.....	45
6.3.	Locations.....	45

6.3.1	Main Location .....	45
6.3.2	CM-TG1 Location .....	46
6.3.3	SBCs Location .....	46
6.4.	Configure Adaptations .....	47
6.4.1	Adaptation for Avaya Aura® Communication Manager.....	47
6.4.2	Adaptation for the Verizon Business IP Trunking service .....	49
6.5.	SIP Entities.....	51
6.5.1	Avaya Aura® Session Manager SIP Entity .....	52
6.5.2	Avaya Aura® Communication Manager SIP Entity – Public Trunk .....	54
6.5.3	Avaya Aura® Communication Manager SIP Entity – Local Trunk.....	55
6.5.4	Avaya Session Border Controller for Enterprise SIP Entity.....	55
6.5.5	Avaya Messaging SIP Entity .....	55
6.5.6	Avaya Experience Portal SIP Entity .....	55
6.6.	Entity Links.....	56
6.6.1	Entity Link to Avaya Aura® Communication Manager – Public Trunk.....	56
6.6.2	Entity Link to Avaya Aura® Communication Manager – Local Trunk.....	57
6.6.3	Entity Link for the Verizon Business IP Trunking service via the Avaya SBCE.....	57
6.6.4	Entity Link to Avaya Messaging .....	57
6.6.5	Entity Link to Avaya Experience Portal .....	57
6.7.	Time Ranges .....	58
6.8.	Routing Policies .....	58
6.8.1	Routing Policy for Verizon Inbound Calls to Avaya Aura® Communication Manager .....	58
6.8.2	Routing Policy for Inbound Calls to Avaya Messaging .....	60
6.8.3	Routing Policy for Inbound Calls to Experience Portal.....	60
6.8.4	Routing Policy for Outbound Calls to Verizon.....	60
6.9.	Dial Patterns.....	61
6.9.1	Origination Dial Patterns – (Optional).....	61
6.9.2	Dial Pattern for Inbound PSTN Calls to Avaya Aura® Communication Manager..	63
6.9.3	Dial Pattern for Inbound Calls to Experience Portal .....	64
6.9.4	Dial Pattern for Outbound Calls to Verizon/PSTN.....	66
6.10.	Verify TLS Certificates – Session Manager .....	67
7.	Avaya Experience Portal.....	69
7.1.	Background .....	69
7.2.	Logging In and Licensing .....	70
7.3.	Verify TLS Certificates – Experience Portal .....	71
7.4.	VoIP Connection.....	72
7.5.	Speech Servers .....	74
7.6.	Application References .....	75
7.7.	MPP Servers and VoIP Settings .....	76
7.8.	Configuring RFC2833 Event Value Offered by Experience Portal.....	78
8.	Configure Avaya Session Border Controller for Enterprise .....	79
8.1.	Device Management – Status.....	80
8.2.	TLS Management.....	82
8.2.1	Verify TLS Certificates – Avaya Session Border Controller for Enterprise .....	82
8.2.2	Server Profiles.....	83

8.2.3	Client Profiles .....	85
8.3.	Network Management.....	87
8.4.	Media Interfaces.....	88
8.5.	Signaling Interfaces .....	89
8.6.	Server Interworking Profiles.....	90
8.6.1	Server Interworking Profile – Enterprise.....	90
8.6.2	Server Interworking Profile – Verizon .....	91
8.7.	Signaling Manipulation.....	92
8.8.	SIP Server Profiles.....	93
8.8.1	SIP Server Profile – Session Manager.....	93
8.8.2	SIP Server Profile – Verizon.....	95
8.9.	Routing Profiles .....	97
8.9.1	Routing Profile – Session Manager .....	97
8.9.2	Routing Profile – Verizon .....	98
8.10.	Topology Hiding Profiles .....	99
8.10.1	Topology Hiding – Enterprise .....	99
8.10.2	Topology Hiding – Verizon .....	100
8.11.	Application Rules.....	101
8.12.	Media Rules .....	102
8.12.1	Enterprise – Media Rule .....	102
8.12.2	Verizon – Media Rule.....	104
8.13.	Signaling Rules .....	105
8.13.1	Signaling Rule – Enterprise .....	105
8.13.2	Signaling Rule – Verizon.....	106
8.14.	Endpoint Policy Groups.....	106
8.14.1	End Point Policy Group - Enterprise .....	106
8.14.2	Endpoint Policy Groups – Verizon .....	107
8.15.	Endpoint Flows – Server Flows.....	108
8.15.1	Server Flow – Enterprise .....	108
8.15.2	Server Flow – Verizon .....	109
9.	Verizon Business IP Trunking Services Suite Configuration.....	110
9.1.	Service Access Information .....	110
10.	Verification Steps.....	111
10.1.	Avaya Aura® Communication Manager Verifications .....	111
10.2.	Avaya Aura® Session Manager Verification .....	113
10.3.	Avaya Session Border Controller for Enterprise Verification.....	115
10.3.1	Incidents.....	115
10.3.2	Server Status .....	116
10.3.3	Diagnostics.....	117
10.3.4	Tracing .....	118
11.	Conclusion .....	119
12.	Additional References.....	120
12.1.	Avaya .....	120
12.2.	Verizon Business .....	120
13.	Appendix A – Avaya SBCE – Refer Handling.....	121
14.	Appendix B – Avaya SBCE – SigMa Script File .....	123

# 1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 10.1, Avaya Aura® Communication Manager Release 10.1, Avaya Experience Portal 8.1 and Avaya Session Border Controller for Enterprise Release 10.1 with the Verizon Business IP Trunking service. The Verizon Business IP Trunking service provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

Note that the terms “Verizon Business IP Trunking”, “Verizon IPT” and “service provider” will be used interchangeably throughout these Application Notes.

## 2. General Test Approach and Test Results

The test approach was manual testing of inbound and outbound calls using the Verizon Business IP Trunking service on a production Verizon PIP access circuit, as shown in **Figure 1**.

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. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with this Application Note, the interface between Avaya systems and the Verizon Business Trunking service did not include use of any specific encryption features as requested by Verizon.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products wherever possible.

## 2.1. Interoperability Compliance Testing

Compliance testing scenarios for the configuration described in these Application Notes included the following:

- Inbound and outbound voice calls between telephones controlled by Communication Manager and the PSTN can be made using G.711MU or G.729A codecs. Phone types included SIP, H.323, digital and analog telephones at the enterprise.
- Proper disconnect when the call is abandoned by the caller before it is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect for calls that are not answered.
- Proper response to busy endpoints.
- DTMF using RFC 2833
  - Outbound call to PSTN application requiring post-answer DTMF (e.g., an IVR or voice mail system).
  - Inbound call from PSTN to Avaya CPE application requiring post-answer DTMF (e.g., Messaging, Experience Portal, Communication Manager vector digit collection steps).
- Additional PSTN numbering plans (e.g., International, operator assist, 411).
- Hold / Retrieve with music on hold.
- Blind and Consultative call transfer using two approaches
  - REFER approach (Communication Manager Network Call Redirection flag on trunk group form set to “y”).
  - INVITE approach (Communication Manager Network Call Redirection flag on trunk group form set to “n”).
- Conference calls.
- SIP Diversion Header for call redirection
  - Call Forwarding
  - EC500
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements and/or music on hold) and Automatic Speech Recognition.
- Experience Portal use of SIP REFER to redirect inbound calls, via the Avaya SBCE, to the appropriate Communication Manager agent extension.
- Call and two-way talk path establishment between callers and Communication Manager agents following redirection from Experience Portal.
- Inbound calls to a self-service Experience Portal application which forwards the call to 8YY or any other PSTN number over Verizon IPT service using SIP REFER.
- Long hold time calls.
- Avaya Remote Worker operation via Avaya SBCE. The SIP endpoints used as Remote Workers included Avaya Workplace Client for Windows and Avaya Agent for Desktop.

**Note:** The configuration of the Remote Worker functionality is beyond the scope of this document.

## 2.2. Test Results

Interoperability testing of Verizon Business IP Trunking service was completed with successful results for all test cases. The following limitations are noted for the sample configuration described in these Application Notes.

1. Even though T.38 fax was provisioned on the Verizon Business IP Trunking production circuit used to verify these Application Notes, Verizon never sent a re-Invite to transition to T.38 fax.

If the **FAX Mode** field on the Communication Manager ip-codec-set form (**Section 5.6**) is set to **t.38-standard**, Communication Manager will send the re-Invite to T.38 for both inbound and outbound fax calls, but will not fallback to G.711 should the Verizon network reject the Communication Manager attempt to transition to T.38 by sending a 488 Not Acceptable message.

When the **FAX Mode** is set to **t.38fallback**, Communication Manager will send a re-Invite to T.38 for inbound fax calls, and relies on the far end to send a re-Invite to T.38 for outbound calls. Communication Manager assumes T.38 fax is not supported for an outbound fax call unless an Invite for T.38 is received from the far end. Since Verizon never sent a T.38 re-Invite, Communication Manager falls back to G.711, resulting in an outbound fax sent using G.711, even though the circuit is provisioned for T.38. Inbound fax calls negotiated properly to T.38.

2. The Verizon Business IP Trunking service node used in the compliance tests does not support E.164 formatted numbers on the SIP origination headers, for the Calling Line Identification for outbound calls. An adaptation in Session Manager is used to convert the E.164 numbers Communication Manager used in the sample configuration for Calling Line Identification (e.g., From and P-Asserted Identity headers) into 10-digit numbers. See **Section 6.4.2**.
3. During testing it was found that on the cases of blind Call Transfer to the PSTN performed from Avaya 9611 and J169 SIP telephones in the lab, the outbound INVITE built by Communication Manager after getting the REFER from the phone/Session Manager, contained in the From header the 11 digit number assigned to the transferring party, but was missing the + sign in front of the number for E.164 format. In this situation the call transfers were failing. A Session Manager adaptation was used to correct this limitation. With the adaptation in place, the call transfers were successful. This issue is currently under investigation by Avaya.
4. The Experience Portal test application used for compliance testing performs consultative call transfer of inbound calls that are transferred back to Verizon 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 Verizon network, consultative call transfers out the Verizon Business IP Trunking fail. As a workaround, a SigMa script file (**Section 8.7**) 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 Verizon. In addition, Experience Portal blind transfers out to

Verizon using SIP REFER were tested successfully. Also, consultative and blind transfers from Experience Portal to Communication Manager were successful as well.

5. In specific attended call transfer scenarios to the PSTN, Verizon 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 Verizon. See **Section 8.7**.
6. Emergency 911/E911 Services Limitations and Restrictions - Although Verizon provides 911/E911 calling capabilities, 911 capabilities were not tested; therefore, it is the customer's responsibility to ensure proper operation with its equipment/software vendor.
7. Verizon Business IP Trunking service does not support G.711A codec for domestic service (EMEA only).
8. Verizon Business IP Trunking service does not support G.729B codec.

### **2.3. History Info and Diversion Headers**

The Verizon Business IP Trunking service does not support SIP History Info headers. Instead, the Verizon Business IP Trunking service requires that the SIP Diversion header be sent for redirected calls. The Communication Manager SIP trunk group form provides the options for specifying whether History Info headers or Diversion headers are sent.

If Communication Manager sends the History Info header, Session Manager can convert the History Info header into the Diversion header. This is performed by specifying the "*VerizonAdapter*" adaptation in Session Manager. See **Section 6.4.2**.

The Communication Manager Call Forwarding or Extension to Cellular (EC500) features may be used for the call scenarios testing the Diversion header.



## 2.4. SIP Header Removal

To support advanced SIP telephony features in the Avaya Aura® enterprise environment, certain proprietary headers may be included in the SIP message sent toward Verizon. These extra headers can cause the SIP message to become larger than the specified Maximum Transmission Unit (MTU) and create fragmented UDP packets. These fragmented packets may not be re-assembled properly on the far-end by Verizon's equipment, for instance, when packets arrive out of order. To prevent fragmented packets, any unnecessary or proprietary headers should be removed from the SIP message before being sent to Verizon. Session Manager can remove these headers by specifying the “*eRHdrs*” parameter within the “*VerizonAdapter*” adaptation. See **Section 6.4.2**.

In the sample configuration, the following headers were removed:

- AV-Global-Session-ID
- Alert-Info
- Endpoint-View
- P-AV-Message-Id
- P-Charging-vector
- P-Location
- AV-Secure-Indication

To help reduce the packet size further, the Avaya SBCE can remove the “*epv*” parameter that may be included within the Contact header by applying a Sigma script to the Verizon server configuration. See **Sections 8.7** and **8.8.2**.

## 2.5. Support

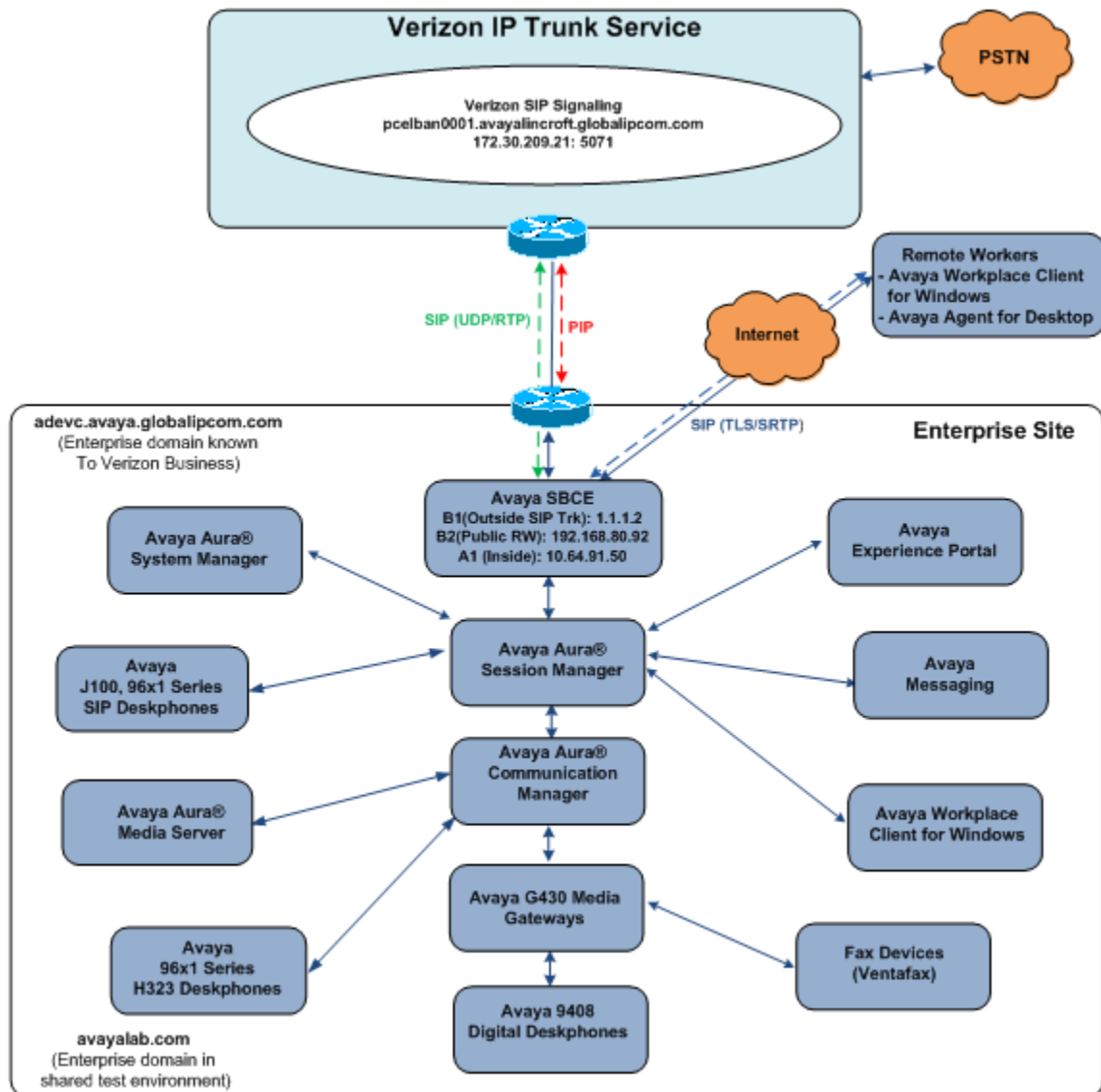
For technical support on the Avaya products described in these Application Notes visit <https://support.avaya.com>

For technical support on Verizon Business IP Trunking service offer, visit online support at <https://www.verizon.com/business/support/>

### 3. Reference Configuration

**Figure 1** illustrates the sample configuration used for the compliance testing. The Avaya CPE location simulates a customer site. The PIP service defines a secure MPLS connection between the Avaya CPE T1 connection and the Verizon service node.

The Avaya SBCE receives traffic from the Verizon Business IP Trunking service on port 5060 and sends traffic to the Verizon Business IP Trunking service on port 5071, using UDP protocol for network transport (required by the Verizon Business IP Trunking service).



### Figure 1: Avaya Interoperability Test Lab Configuration

**Note** – These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning described in this document.

The Verizon Business IP Trunking service provided Direct Inward Dial (DID) 10-digit numbers. These DID numbers can be mapped by Session Manager or Communication Manager to Avaya telephone extensions.

Verizon Business IP Trunking service used FQDN *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE environment was known to Verizon Business IP Trunking service as FQDN *adevc.avaya.globalipcom.com*. Access to the Verizon Business IP Trunking service was added to a configuration that already used domain “avayalab.com” at the enterprise. As such, the Avaya SBCE is used to adapt the “avayalab.com” domain to the domain known to Verizon (see **Section 8.10.2**). These Application Notes indicate a configuration that would not be required in cases where the CPE domain in Communication Manager and Session Manager match the CPE domain known to the Verizon Business IP Trunking service.

**Note** – The Fully Qualified Domain Names and IP addressing specified in these Application Notes apply only to the reference configuration shown in **Figure 1**. Verizon Business customers will use their own FQDNs and IP addressing as required.

In summary, the following components were used in the reference configuration.

- Verizon Business IP Trunking network Fully Qualified Domain Name (FQDN)
  - *pcelban0001.avayalincroft.globalipcom.com*
- Avaya CPE Fully Qualified Domain Name (FQDN) known to Verizon
  - *adevc.avaya.globalipcom.com*
- Avaya Session Border Controllers for Enterprise
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya G430 Media Gateway
- Avaya Media Server
- Avaya Messaging
- Avaya Experience Portal
- Avaya 96X1 Series IP Deskphones using the SIP and H.323 software bundle
- J100 Series IP Deskphones using the SIP software bundle
- Avaya Workplace Client for Windows
- Avaya Agent for Desktop
- Avaya 9408 Digital Phones
- Ventafax fax software

### 3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the reference configuration described in these Application Notes and are for illustrative purposes only. Customers must obtain and use the specific values for their own configurations.

**Note** – The Verizon IPT SIP proxy IP address and DID/DNIS digits shown in this document are examples. Verizon will provide the actual IP addresses and DID/DNIS digits as part of the Verizon IPT provisioning process.

Component	Illustrative Value in these Application Notes
<b>Avaya Aura® Session Manager</b>	
IP Address	10.64.91.85
<b>Avaya Aura® System Manager</b>	
IP Address	10.64.90.84
<b>Avaya Aura® Communication Manager</b>	
IP Address	10.64.91.87
<b>Avaya Aura® Media Server</b>	
IP Address	10.64.91.88
<b>Avaya G430 Media Gateway</b>	
IP Address	192.168.7.150
<b>Avaya Messaging</b>	
IP Address	10.64.19.90
<b>Avaya Experience Portal</b>	
IP Address	10.64.91.90
<b>Avaya Session Border Controller for Enterprise (SBCE)</b>	
IP Address of A1 Inside (Private) Interface	10.64.91.50
IP Address of B1 Outside (Public) Interface, SIP Trunking	1.1.1.2 (see note below)
<b>Verizon IPT</b>	
IP Address	172.30.209.21

**Table 1: Network Values Used in these Application Notes**

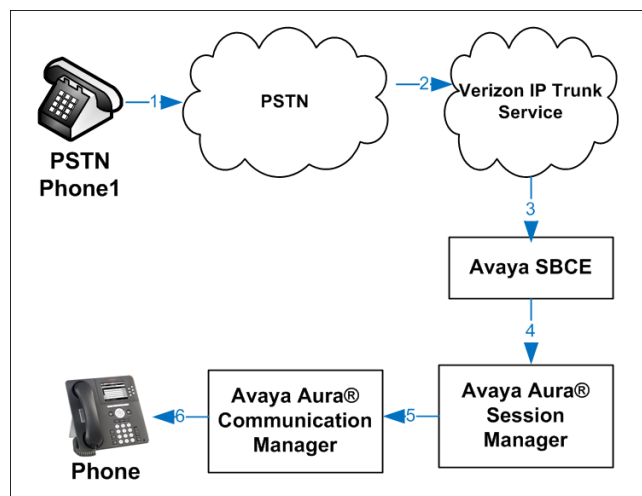
### 3.3. Call Flows

To understand how Verizon Business IP Trunking service calls are handled by the Avaya CPE environment, several call flows are described in this section.

#### 3.3.1 Communication Manager

The first call scenario illustrated is an inbound Verizon Business IP Trunking service call that arrives at the Avaya SBCE, to Session Manager, and is subsequently routed to Communication Manager, which in turn routes the call to a phone or fax endpoint.

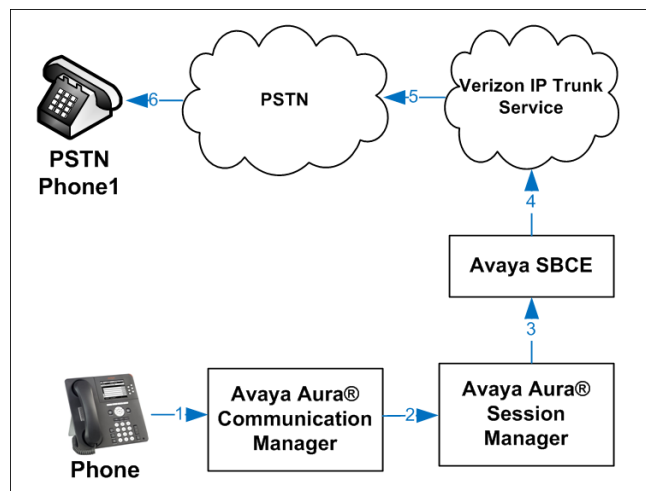
1. A PSTN phone originates a call to a Verizon Business IP Trunking service number.
2. The PSTN routes the call to the Verizon Business IP Trunking service network.
3. The Verizon Business IP Trunking service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs IP address translations and any necessary SIP header modifications and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Depending on the called number, Communication Manager routes the call to a phone or fax endpoint.



**Figure 2: Inbound Verizon Call**

The second call scenario illustrated is an outbound call initiated on Communication Manager, routed to Session Manager, and is subsequently sent to the Avaya SBCE for delivery to the Verizon Business IP Trunking service.

1. A Communication Manager phone or fax endpoint originates a call to a Verizon Business IP Trunking service number for delivery to the PSTN.
2. Communication Manager routes the call to Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to the Avaya SBCE.
4. The Avaya SBCE performs IP address translations and any necessary SIP header modifications and routes the call to the Verizon Business IP Trunking service.
5. The Verizon Business IP Trunking service delivers the call to the PSTN.

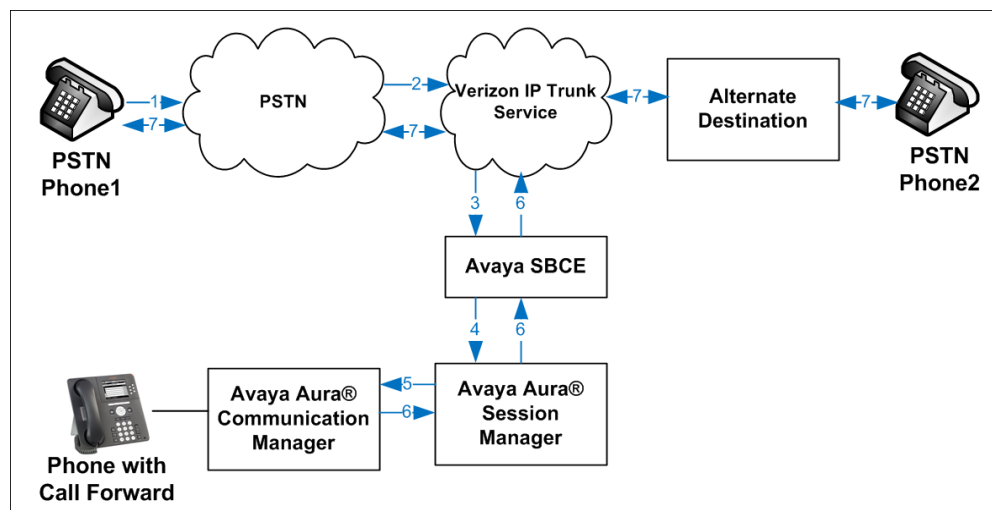


**Figure 3: Outbound Verizon Call**

The third call scenario illustrated is an inbound Verizon Business IP Trunking service call that arrives at the Avaya SBCE, to Session Manager, and subsequently Communication Manager. Communication Manager routes the call to a destination station; however, the station has set Call Forward to an alternate destination. The same scenario applies when EC500 is activated on the destination station. Without answering the call, Communication Manager redirects the call back to the Verizon Business IP Trunking service for routing to the alternate destination.

**Note** – In cases where calls are forwarded to an alternate destination, the Verizon Business IP Trunking service requires the use of SIP Diversion Header for the redirected call to complete (see **Section 5.8**).

1. A PSTN phone originates a call to a Verizon Business IP Trunking service number.
2. The PSTN routes the call to the Verizon Business IP Trunking service network.
3. The Verizon Business IP Trunking service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any necessary SIP header modifications and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Because the Communication Manager phone has set Call Forward to another Verizon Business IP Trunking service number, Communication Manager initiates a new call back out to Session Manager, the Avaya SBCE, and to the Verizon Business IP Trunking service network.
7. The Verizon Business IP Trunking service places a call to the alternate destination, and upon answering Communication Manager connects the calling party to the target party.

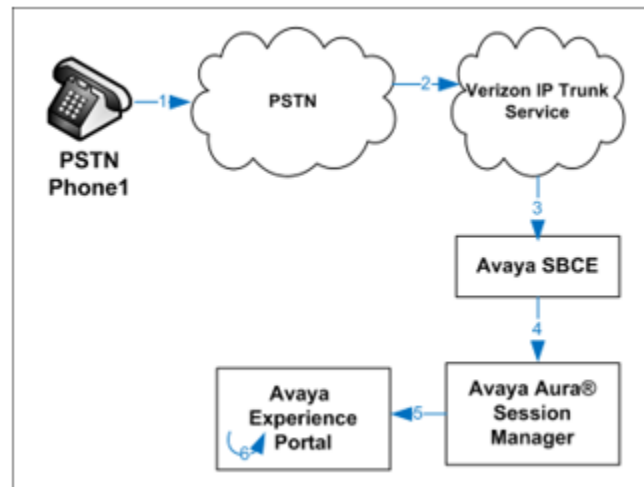


**Figure 4: Station Re-directed (e.g., Call Forward) Verizon Call**

### 3.3.2 Experience Portal

The first call scenario illustrated below is an inbound call arriving and remaining on Experience Portal.

1. A PSTN phone originates a call to a Verizon Business IP Trunking service number.
2. The PSTN routes the call to the Verizon Business IP Trunking service network.
3. The Verizon Business IP Trunking service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs any necessary SIP header modifications and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Experience Portal.
6. Experience Portal matches the called party number to a VXML and/or CCXML application script, answers the call, and handles the call according to the directives specified in the application. In this scenario, the application sufficiently meets the caller's needs or requests, and thus the call does not need to be transferred to Communication Manager.

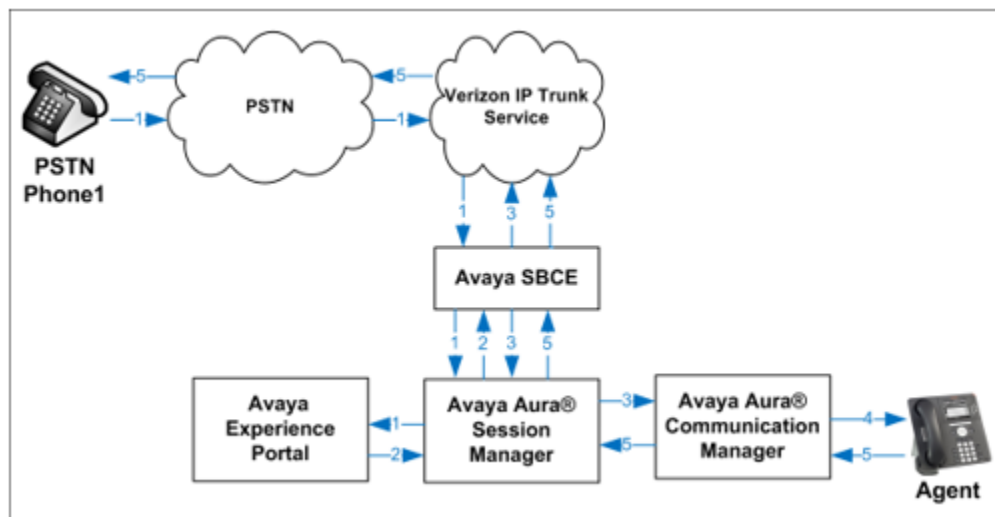


**Figure 5: Inbound Call Handling Entirely by Avaya Experience Portal**



The second call scenario illustrated below is an inbound call arriving on Experience Portal and transferred to Communication Manager without determining whether an agent is available or not.

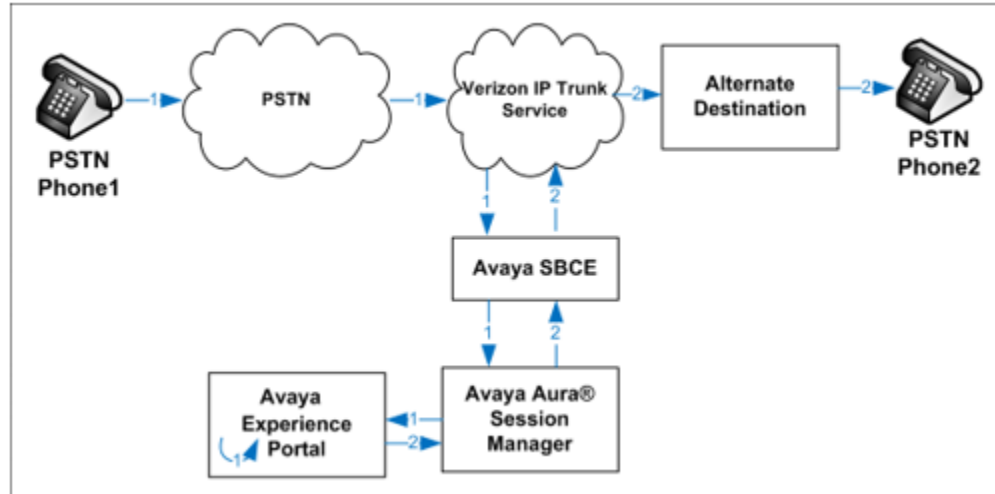
1. Same as the first five steps from the first call scenario.
2. In this scenario, when the caller selects an option requesting an agent, Experience Portal redirects the call by sending a SIP REFER to the Avaya SBCE.
3. The Avaya SBCE sends a SIP INVITE to the Communication Manager (via Session Manager) for the selected skill. In addition, the Avaya SBCE places the inbound call on hold.
4. Communication Manager routes the call to the agent.
5. When the agent answers, the Avaya SBCE takes the call off hold and the caller is connected to the agent.



**Figure 6: Avaya Experience Portal Transfers Call to Avaya Aura® Communication Manager**

The third call scenario illustrated below is an inbound call arriving on Experience Portal and forwarded to an 8YY number or any other PSTN number over the Verizon network.

1. Same as the first six steps from the first call scenario.
2. In this scenario, the application is sufficient to meet the caller's requests, and thus the call needs to be forwarded to another PSTN number. Based upon the selection, Experience Portal forwards the call to an appropriate PSTN number which can be a regular PSTN number or an 8YY number.



**Figure 7: Inbound Call forwarded by Experience Portal to another PSTN number**

## 4. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

Equipment/Software	Release/Version
Avaya Aura® System Manager	10.1.0.1.0614394
Avaya Aura® Session Manager	10.1.0.1.1010105
Avaya Aura® Communication Manager	10.1.0.10-SP1 Update ID 10.1.0.974.0-27372
Avaya Session Border Controller for Enterprise	10.1.0.0-32-21432 Hotfix (sbce-10.1.0.0-34-21958-hotfix-05192022.tar.gz)
Avaya Experience Portal	8.1.1.0.0121
Avaya Aura® Media Server	10.1.0.77
Avaya Messaging	10.8 SP1
Avaya G430 Media Gateway	42.4
Avaya 96x1 Series IP Deskphone (H.323)	6.8511
Avaya J100 IP Deskphones (J169, J179)	4.0.12.0.6
Avaya 96x1 Series IP Deskphone (SIP)	7.1.15.0.14
Avaya Workplace Client for Windows	3.26.0.64
Avaya Agent for Desktop	2.0.6.20.3004
Avaya 9408 Digital Deskphone	20.06
Fax device	Ventafax 7.10

**Table 2: Equipment and Software Used in the Sample Configuration**

## 5. Configure Avaya Aura® Communication Manager

This section illustrates an example configuration allowing SIP signaling via the “Processor Ethernet” of Communication Manager to Session Manager.

**Note** – The initial installation, configuration, and licensing of the Avaya servers and media gateways for Communication Manager are assumed to have been previously completed and are not discussed in these Application Notes.

### 5.1. Verify Licensed Features

**Note** – This section describes steps to verify Communication Manager feature settings that are required for the reference configuration described in these Application Notes. Depending on access privileges and licensing, some or all of the following settings might only be viewed, and not modified. If any of the required features are not set, and cannot be configured, contact an authorized Avaya account representative to obtain the necessary licenses/access.

**Step 1** - Enter the **display system-parameters customer-options** command. On **Page 2** of the form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of expected SIP trunks.

display system-parameters customer-options			Page	2 of 12
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:	4000	0		
Maximum Concurrently Registered IP Stations:	1000	2		
Maximum Administered Remote Office Trunks:	4000	0		
Max Concurrently Registered Remote Office Stations:	1000	0		
Maximum Concurrently Registered IP eCons:	68	0		
Max Concur Reg Unauthenticated H.323 Stations:	100	0		
Maximum Video Capable Stations:	2400	0		
Maximum Video Capable IP Softphones:	1000	6		
<b>Maximum Administered SIP Trunks:</b>	<b>4000</b>	<b>75</b>		
Max Administered Ad-hoc Video Conferencing Ports:	4000	0		
Max Number of DS1 Boards with Echo Cancellation:	80	0		

**Step 2 - On Page 4 of the form, verify that ARS is enabled.**

display system-parameters customer-options		Page 4 of 12
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
<b>ARS? y</b>	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? n	DCS Call Coverage? y	
ASAI Link Plus Capabilities? n	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n		
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification? y	
ATM WAN Spare Processor? n	DS1 MSP? y	
ATMS? y	DS1 Echo Cancellation? y	
Attendant Vectoring? y		

**Step 3 - On Page 5 of the form, verify that the Enhanced EC500, IP Trunks, and ISDN-PRI, features are enabled. If the use of SIP REFER messaging will be required verify that the ISDN/SIP Network Call Redirection feature is enabled. If the use of SRTP will be required verify that the Media Encryption Over IP feature is enabled.**

display system-parameters customer-options		Page 5 of 12
OPTIONAL FEATURES		
Emergency Access to Attendant? y	<b>IP Stations? y</b>	
Enable 'dadmin' Login? y		
Enhanced Conferencing? y	ISDN Feature Plus? n	
<b>Enhanced EC500? y</b>	<b>ISDN/SIP Network Call Redirection? y</b>	
Enterprise Survivable Server? n	ISDN-BRI Trunks? y	
Enterprise Wide Licensing? n	<b>ISDN-PRI? y</b>	
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	<b>Media Encryption Over IP? y</b>	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y	
<b>IP Trunks? y</b>		
IP Attendant Consoles? y		

**Step 4 - On Page 6 of the form, verify that the **Processor Ethernet** field is set to **y**.**

display system-parameters customer-options		Page 6 of 12
OPTIONAL FEATURES		
Multinational Locations? n	Station and Trunk MSP? y	
Multiple Level Precedence & Preemption? n	Station as Virtual Extension? y	
Multiple Locations? n		
Personal Station Access (PSA)? y	System Management Data Transfer? n	
PNC Duplication? n	Tenant Partitioning? y	
Port Network Support? y	Terminal Trans. Init. (TTI)? y	
Posted Messages? y	Time of Day Routing? y	
	TN2501 VAL Maximum Capacity? y	
	Uniform Dialing Plan? y	
Private Networking? y	Usage Allocation Enhancements? y	
Processor and System MSP? y		
<b>Processor Ethernet? y</b>	Wideband Switching? y	
	Wireless? n	
Remote Office? y		
Restrict Call Forward Off Net? y		
Secondary Data Module? y		

## 5.2. System-Parameters Features

**Step 1 - Enter the **display system-parameters features** command. On **Page 1** of the form, verify that the **Trunk-to-Trunk Transfer** is set to **all**.**

change system-parameters features		Page 1 of 19
FEATURE-RELATED SYSTEM PARAMETERS		
Self Station Display Enabled? y		
<b>Trunk-to-Trunk Transfer: all</b>		
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		

### 5.3. Dial Plan

The dial plan defines how digit strings will be used locally by Communication Manager. The following dial plan was used in the reference configuration.

**Step 1** - Enter the **change dialplan analysis** command to provision the following dial plan.

- 5-digit extensions with a **Call Type** of **ext** beginning with:
  - The digits **1, 5, 7** and **8** for Communication Manager extensions.
- 3-digit dial access code (indicated with a **Call Type** of **dac**), e.g., access code **\*xx** for SIP Trunk Access Codes (TAC). See the trunk forms in **Section 5.8**.

change dialplan analysis			Page 1 of 12						
DIAL PLAN ANALYSIS TABLE									
Location: all									
Percent Full: 1									
	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1		5	ext						
2		5	ext						
3		5	ext						
4		5	ext						
5		5	ext						
60		3	ext						
66		2	fac						
7		5	ext						
8		5	ext						
9		1	fac						
*		3	dac						

### 5.4. Node Names

Node names define IP addresses to various Avaya components in the enterprise. In the reference configuration a Processor Ethernet (procr) based Communication Manager platform is used. Note that the Communication Manager procr name and IP address are entered during installation. The procr IP address was used to define the Communication Manager SIP Entities in **Section 6.5**

**Step 1** - Enter the **change node-names ip** command, and add a node name and IP address for the following:

- Session Manager SIP signaling interface (e.g., **SM** and **10.64.91.85**).
- Media Server (e.g., **AMS10** and **10.64.91.88**). The Media Server node name is only needed if a Media Server is present.

change node-names ip		Page	1 of	2
		IP NODE NAMES		
Name	IP Address			
AMS10	10.64.91.88			
SM	10.64.91.85			
default	0.0.0.0			
procr	10.64.91.87			
procr6	::			

## 5.5. Processor Ethernet Configuration

The **change ip-interface procr** command can be used to verify the Processor Ethernet (procr) parameters defined during installation.

- Verify that **Enable Interface?**, **Allow H.323 Endpoints?**, and **Allow H248 Gateways?** fields are set to **y**.
- In the reference configuration the procr is assigned to **Network Region: 1**.
- The default values are used for the remaining parameters.

<b>change ip-interface procr</b>		Page 1 of 2
IP INTERFACES		
Type: PROCR	Target socket load: 4800	
<b>Enable Interface? y</b>	<b>Allow H.323 Endpoints? y</b>	
<b>Network Region: 1</b>	<b>Allow H.248 Gateways? y</b>	
	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr	IP Address: 10.64.91.87	
Subnet Mask: /24		



## 5.6. IP Codec Sets

Use the **change ip-codec-set** command to define a list of codecs to use for calls within the enterprise, and for calls between the enterprise and the service provider.

### 5.6.1 Codecs for IP Network Region 1 (calls within the CPE)

**Step 1** - Enter the **change ip-codec-set x** command, where **x** is the number of an IP codec set used for internal calls (e.g., **1**). On **Page 1** of the **ip-codec-set** form, ensure that **G.711MU**, and **G.729A** are included in the codec list.

<b>change ip-codec-set 1</b>				Page	1 of	2
IP Codec Set						
Codec Set: 1						
Audio	Silence	Frames	Packet			
Codec	Suppression	Per Pkt	Size (ms)			
1: G.722-64K		2	20			
2: <b>G.711MU</b>	<b>n</b>	<b>2</b>	<b>20</b>			
3: <b>G.729A</b>	<b>n</b>	<b>2</b>	<b>20</b>			
Media Encryption				Encrypted SRTCP: enforce-unenc-srtcp		
1: 1-srtp-aescm128-hmac80						
2: none						

**Step 2** - On **Page 2** of the **ip-codec-set** form, set **FAX Mode** to **t.38-standard**, and **ECM** to **y**.

<b>change ip-codec-set 1</b>				Page	2 of	2
IP MEDIA PARAMETERS						
Allow Direct-IP Multimedia? y						
Maximum Call Rate for Direct-IP Multimedia : 15360:Kbits						
Maximum Call Rate for Priority Direct-IP Multimedia : 15360:Kbits						
	Mode	Redun-		Packet		
		dancy		Size (ms)		
<b>FAX</b>	<b>t.38-standard</b>	<b>0</b>	<b>ECM: y</b>			
Modem	off	0				
TDD/TTY	US	3				
H.323 Clear-channel	n	0				
SIP 64K Data	n	0		20		
Media Connection IP Address Type Preferences						
1: IPv4						
2:						

## 5.6.2 Codecs for IP Network Region 2 (calls to/from Verizon)

This IP codec set will be used for Verizon Business IP Trunking calls. Repeat the steps in **Section 5.6.1** with the following changes:

On **Page 1**, provision the codecs in the order shown below.

change ip-codec-set 2

Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 2

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.729A	n	2	20
2: G.711MU	n	2	20
3:			

Media Encryption

Encrypted SRTP: enforce-unenc-srtp

1: 1-srtp-aescm128-hmac80
2: none

On **Page 2**, set **FAX Mode** to **t.38fallback**, **XMT** to **udptl**, **ECM** to **y**, and **FB-Timer** to **4**. See **Section 2.2** for limitations regarding fax.

change ip-codec-set 2

Page 2 of 2

IP MEDIA PARAMETERS

Allow Direct-IP Multimedia? y

Maximum Call Rate for Direct-IP Multimedia: 384:Kbits

Maximum Call Rate for Priority Direct-IP Multimedia: 384:Kbits

	Mode		Redun- dancy		Packet Size (ms)
<b>FAX</b>	<b>t.38fallback</b>	<b>XMT: udptl</b>	0	<b>ECM: y</b>	<b>FB-Timer: 4</b>
Modem	off		0		
TDD/TTY	US		3		
H.323 Clear-channel	n		0		
SIP 64K Data	n		0		20

Media Connection IP Address Type Preferences

1: IPv4
2:

## 5.7. Network Regions

Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G430 Media Gateway and Avaya Media Server are in region 1. To provide testing flexibility, network region 2 was associated with other components used specifically for the Verizon testing.

### 5.7.1 IP Network Region 1 – Local CPE Region

**Step 1** - Enter **change ip-network-region x**, where **x** is the number of an unused IP network region (e.g., region 1). This IP network region will be used to represent the local CPE. Populate the form with the following values:

- Enter a descriptive name (e.g., **Enterprise**).
- Enter the enterprise domain (e.g., **avayalab.com**) in the **Authoritative Domain** field.
- Enter **1** for the **Codec Set** parameter.
- **Intra-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.
- **Inter-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1	NR Group: 1	
Location: 1	Authoritative Domain: avayalab.com	
Name: Enterprise	Stub Network Region: n	
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3329		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y	RSVP Enabled? n	
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

**Step 2** - On **page 4** of the form:

- Verify that next to region **1** in the **dst rgn** column, the codec set is **1**.
- Next to region **2** in the **dst rgn** column, enter **2** for the codec set (this means region 1 is permitted to talk to region 2 and it will use codec set 2 to do so). The **direct WAN** and **Units** columns will self-populate with **y** and **No Limit** respectively.
- Let all other values default for this form.

change ip-network-region 1										Page	4	of	20
Source Region: 1		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	1										all		
2	2	y	NoLimit						n		t		

## 5.7.2 IP Network Region 2 – Verizon Trunk Region

Repeat the steps in **Section 5.7.1** with the following changes:

**Step 1** - On **Page 1** of the form (not shown):

- Enter a descriptive name (e.g., **Verizon**).
- Enter **2** for the **Codec Set** parameter.

**Step 2** - On **Page 4** of the form:

- Set codec set **2** for **dst rgn 1**.
- Note that **dst rgn 2** is pre-populated with codec set **2** (from page 1 provisioning).

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													

## 5.8. SIP Trunks

SIP trunks are defined on Communication Manager by provisioning a Signaling Group and a corresponding Trunk Group. Two SIP trunks are defined on Communication Manager in the reference configuration:

- Inbound/outbound Verizon access – SIP Trunk 1. This trunk will use TLS port 5081.
- Internal CPE access (e.g., Avaya SIP telephones, Messaging, etc.) – SIP Trunk 3. This trunk will use TLS port 5061.

Note that different ports are assigned to each trunk. This is necessary so Session Manager can distinguish the traffic on the service provider trunk, from the traffic on the trunk used for other enterprise SIP traffic.

**Note** – Although TLS is used as the transport protocols between the Avaya CPE components, UDP was used between the Avaya SBCE and the Verizon IP Trunk service. See the note in **Section 6.5** regarding the use of TLS transport protocols in the CPE.

### 5.8.1 SIP Trunk for Inbound/Outbound Verizon calls

This section describes the steps for administering the SIP trunk to Session Manager used for Verizon IP Trunk service calls. Trunk Group 1 is defined. This trunk corresponds to the **CM-TG1** SIP Entity defined later in **Section 6.5.2**.

#### 5.8.1.1 Signaling Group 1

**Step 1** - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., 1), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **Peer Detection Enabled?** is set to **y**. The system will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.4** (e.g., **SM**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5081**.
- **Far-end Network Region** – Set the IP network region to **2**, as set in **Section 5.6.2**.
- **Far-end Domain** – Enter **avayalab.com**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized directly to the associated stations, to reduce the use of media resources on the Avaya Media Gateway when possible (known as shuffling).
- **Initial IP-IP Direct Media** is set to the default value **n**.
- **H.323 Station Outgoing Direct Media** is set to the default value **n**.

<b>change signaling-group 1</b>		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	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: 5081	Far-end Listen Port: 5081	
	Far-end Network Region: 2	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Use the default parameters on **page 2** of the form (not shown).

### 5.8.1.2 Trunk Group 1

**Step 1** - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **1**). On **Page 1** of the **trunk-group** form, provision the following:

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **Verizon IPT**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **\*01**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **Section 5.8.1.1** (e.g., **1**).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **10**).

<b>add trunk-group 1</b>		Page 1 of 21
TRUNK GROUP		
Group Number: 1	Group Type: sip	CDR Reports: y
Group Name: Verizon IPT	COR: 1	TN: 1 TAC: *01
Direction: two-way	Outgoing Display? n	
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 1	
	Number of Members: 10	

**Step 2 - On Page 2 of the Trunk Group form:**

- Set the **Preferred Minimum Session Refresh Interval(sec):** to **900**. This entry will actually cause a value of 1800 to be generated in the SIP Session-Expires header pertaining to active call session refresh.

<b>add trunk-group 1</b>	<b>Page 2 of 21</b>
Group Type: sip	
TRUNK PARAMETERS	
Unicode Name: auto	
Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18
<b>Preferred Minimum Session Refresh Interval(sec): 900</b>	
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	

**Step 3 - On Page 3 of the Trunk Group form:**

- Set **Numbering Format** to **public**.

<b>add trunk-group 1</b>	<b>Page 3 of 21</b>
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	<b>Numbering Format: public</b>
	UI Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

**Step 4 - On Page 4 of the Trunk Group form:**

- Verify **Network Call Redirection** is set to **y**.
- Set **Telephone Event Payload Type** to the RTP payload type recommended by Verizon (e.g., **101**).
- Set **Convert 180 to 183 for Early Media** to **y**.

**Note** – The Verizon Business IP Trunking service does not support History Info header. As shown below, by default this header is supported by Communication Manager. In the reference configuration, the History Info header is automatically removed from SIP signaling by Session Manager, as part of the *VerizonAdapter* (see **Section 6.4.2**). The adapter additionally inserts a Diversion header on EC500 and Call Forward calls that are redirected back to the Verizon Business IP Trunking service. Alternatively, History Info may be disabled here with the Diversion Header enabled.

```
add trunk-group 1                                     Page 4 of 21
                                                    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? n
                                                    Support Request History? y
                                                    Telephone Event Payload Type: 101
                                                    Shuffling with SDP? n

                                                    Convert 180 to 183 for Early Media? y
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
```



## 5.8.2 Local SIP Trunk (Avaya SIP Telephones, Messaging Access, etc.)

Trunk Group 3 corresponds to the **CM-TG3** SIP Entity defined later in **Section 6.5.3**

### 5.8.2.1 Signaling Group 3

Repeat the steps in **Section 5.8.1.1** with the following changes:

**Step 1** - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **3**).

**Step 2** - Set the following parameters on page 1:

- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061**
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 5.7.1**.

### 5.8.2.2 Trunk Group 3

Repeat the steps in **Section 5.8.1.2** with the following changes:

**Step 1** - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **3**). On **Page 1** of the **trunk-group** form:

- **Group Name** – Enter a descriptive name (e.g., **SM Enterprise**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **\*03**).
- **Service Type** – Set to **tie**.
- **Signaling Group** – Set to the number of the signaling group administered in **Section 5.8.2.1** (e.g., **3**).

**Step 2** - On **Page 2** of the **Trunk Group** form:

- Same as **Section 5.8.1.2**

**Step 3** - On **Page 3** of the **Trunk Group** form:

- Set **Numbering Format** to **private**.

**Step 4** - On **Page 4** of the **Trunk Group** form:

- Set **Network Call Redirection** to **n**.
- Set **Send Diversion Header** to **n**.
- Verify **Identity for Calling Party Display** is set to **P-Asserted-Identity** (default).

Use default values for all other settings.

## 5.9. Public Numbering

In the reference configuration, the public-unknown-numbering form, (used in conjunction with the **Numbering Format: public** setting in **Section 5.8.1.2**), is used to convert Communication Manager local extensions to Verizon public numbers, for inclusion in any origination SIP headers directed to the Verizon Business IP Trunking service via the public trunk.

**Step 1** - Enter **change public-unknown-numbering 5 ext-digits xxxxx**, where xxxxx is the 5-digit extension number to change.

**Step 2** - Add each Communication Manager station extension and their corresponding Verizon DNIS numbers (for the public trunk to Verizon). Communication Manager will insert these Verizon DNIS numbers in E.164 format into the From, Contact, and PAI headers as appropriate:

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter a Communication Manager extension (e.g., **12001**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **1**).
- **Private Prefix** – Enter the corresponding Verizon DNIS number (e.g., **17329450231**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **11**).

change public-unknown-numbering 5 ext-digits 12001					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	12001	1	17329450231	11	Total Administered: 46
5	14006	1	17329450236	11	Maximum Entries: 240
5	14007	1	17329450237	11	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
5	14008	1	17329450238	11	
5	50	1	173294	11	
					Communication Manager automatically inserts a '+' digit in this case.

## 5.10. Private Numbering

In the reference configuration, the private-numbering form, (used in conjunction with the **Numbering Format: private** setting in **Section 5.8.2.2**), is used to send Communication Manager local extension numbers to Session Manager, for inclusion in any SIP headers directed to SIP endpoints and Messaging.

**Step 1** - Add all Communication Manager local extension patterns (for the local trunk).

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the Communication Manager extension patterns defined in the Dial Plan in **Section 5.3** (e.g., **5**, **14** and **20**).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **3**).
- **Total Len** - Enter the total number of digits after the digit conversion (e.g., **5**).

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	1	11		5	Total Administered: 11
5	5	3		5	Maximum Entries: 540
5	14	3		5	
5	20	3		5	

## 5.11. Route Patterns

Route Patterns are used to direct outbound calls via the public or local CPE SIP trunks.

### 5.11.1 Route Pattern for National Calls to Verizon

This form defines the public SIP trunk, based on the route-pattern selected by the ARS table later in **Section 5.12**. The routing defined in this section is simply an example and not intended to be prescriptive. Other routing policies may be appropriate for different customer networks. In the reference configuration, route pattern 1 is used for national calls, route pattern 2 is used for international calls, and route pattern 4 is used for service calls.

**Step 1** - Enter the **change route-pattern 1** command to configure a route pattern for national calls and enter the following parameters:

- In the **Grp No** column, enter **1** for public trunk 1, and the **FRL** column enter **0** (zero).
- In the **Pfx mrk** column, enter **1** to ensure a 1 + 10 digits are sent to the service provider for FNPA calls.
- In the **Inserted Digits** column, enter **p** to have Communication Manager insert a plus sign (+) in front of the number dialed to convert it to an E.164 formatted number.

<b>change route-pattern 1</b>										Page 1 of 3
Pattern Number: 1      Pattern Name: To PSTN SIP Trk										
SCCAN? n      Secure SIP? n      Used for SIP stations? n										
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits	DCS/ QSIG	IXC	
1: 1	0		1				p	n	user	
2:								n	user	
3:								n	user	
BCC VALUE      TSC      CA-TSC      ITC BCIE      Service/Feature      PARM      Sub      Numbering      LAR										
0 1 2 M 4 W      Request      Dgts Format										
1: y	y	y	y	y	n	n	rest		none	

## 5.11.2 Route Pattern for International Calls to Verizon

Repeat the steps in **Section 5.11.1** to add a route pattern for international calls with the following changes:

**Step 1** - Enter the **change route-pattern 2** command and enter the following parameters:

- In the **Grp No** column, enter **1** for public trunk 1, and the **FRL** column enter **0** (zero).
- In the **Pfx mrk** column, leave blank (default).
- In the **No. Del Digits** column, enter **3** to have Communication Manager remove the international 011 prefix from the number.
- In the **Inserted Digits** column, enter **p** to have Communication Manager insert a plus sign (+) in front of the number dialed to convert it to an E.164 formatted number.

<b>change route-pattern 2</b>										Page 1 of 3
Pattern Number: 2      Pattern Name: 011 to E.164										
SCCAN? n      Secure SIP? n      Used for SIP stations? n										
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits	DCS/ QSIG	IXC	
1: 1	0					3	p	n	user	
2:								n	user	
3:								n	user	
BCC VALUE      TSC      CA-TSC      ITC BCIE      Service/Feature      PARM      Sub      Numbering      LAR										
0 1 2 M 4 W      Request      Dgts Format										
1: y	y	y	y	y	n	n	rest		none	

### 5.11.3 Route Pattern for Service Calls to Verizon

Repeat the steps in **Section 5.11.1** to add a route pattern for x11 and other service numbers that do not require a leading plus sign:

**Step 1** - Enter the **change route-pattern 4** command and enter the following parameters:

- In the **Grp No** column, enter **1** for public trunk 1, and the **FRL** column enter **0** (zero).
- In the **Pfx mrk** column, leave blank (default).
- In the **Inserted Digits** column, leave blank (default).

change route-pattern 4														Page 1 of 3			
Pattern Number: 4														Pattern Name: Service Numbers			
SCCAN? n														Secure SIP? n		Used for SIP stations? n	
<b>Grp FRL NPA Pfx Hop Toll No. Inserted</b>														DCS/ IXC			
<b>No Mrk Lmt List Del Digits</b>														QSIG			
														Intw			
1: 1 0														n user			
2:														n user			
3:														n user			
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM Sub														Numbering LAR			
0 1 2 M 4 W Request														Dgts Format			
1: y y y y y n n														rest none			

### 5.11.4 Route Pattern for Calls within the CPE

This form defines the Route pattern for the local SIP trunk, based on the route-pattern selected by the AAR table in **Section 5.13** (e.g., calls to Avaya SIP telephone extensions or Messaging).

**Step 1** - Repeat the steps in **Section 5.11.1** with the following changes:

- In the **Grp No** column enter **3** for SIP trunk 3 (local trunk).
- In the **FRL** column enter **0** (zero).
- In the **Pfx mrk** column, leave blank (default).
- In the **Inserted Digits** column, leave blank (default).
- In the **Numbering Format** column, across from line **1**: enter **lev0-pvt**.

change route-pattern 3														Page 1 of 3			
Pattern Number: 3														Pattern Name: ToSM Enterprise			
SCCAN? n														Secure SIP? n		Used for SIP stations? y	
Primary SM: SM														Secondary SM:			
<b>Grp FRL NPA Pfx Hop Toll No. Inserted</b>														DCS/ IXC			
<b>No Mrk Lmt List Del Digits</b>														QSIG			
														Intw			
1: 3 0														n user			
2:														n user			
3:														n user			
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM Sub														Numbering LAR			
0 1 2 M 4 W Request														Dgts Format			
1: y y y y y n n														rest lev0-pvt none			

## 5.12. Automatic Route Selection (ARS) Dialing

The ARS table is selected based on the caller dialing the ARS access code (e.g., **9**) as defined in **Section 5.3**. The access code is removed and the ARS table matches the remaining outbound dialed digits and sends them to the designated route-pattern (see **Section 5.11**).

**Step 1** - Enter the **change ars analysis 1720** command and enter the following:

- In the **Dialed String** column enter a matching dial pattern (e.g., **1720**). Note that the best match will route first, that is 1720555xxxx will be selected before 17xxxxxxxxx.
- In the **Min** and **Max** columns enter the corresponding digit lengths, (e.g., **11** and **11**).
- In the Route Pattern column select a route-pattern to be used for these calls (e.g., **1**).
- In the **Call Type** column enter **fnpa** (selections other than **fnpa** may be appropriate, based on the digits defined here).

**Step 2** - Repeat **Step 1** for all other outbound call strings.

change ars analysis 1720						Page 1 of 2	
ARS DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 1	
Dialed String		Total		Route	Call	Node	ANI
		Min	Max	Pattern	Type	Num	Reqd
1720		11	11	1	fnpa		n
18		11	11	1	fnpa		n
19		11	11	1	fnpa		n
1900		11	11	deny	fnpa		n
1900555		11	11	deny	fnpa		n
1xxx976		11	11	deny	fnpa		n
311		3	3	4	svcl		n
011		10	18	2	intl		n
411		3	3	4	svcl		n
5		10	10	1	fnpa		n

## 5.13. Automatic Alternate Routing (AAR) Dialing

AAR is used for outbound calls within the CPE.

**Step 1** - Enter the **change aar analysis 0** command and enter the following:

- **Dialed String** - In the reference configuration all SIP telephones used extensions in the range 50xxx, therefore enter **50**.
- **Min & Max** – Enter **5**.
- **Route Pattern** – Enter **3**.
- **Call Type** – Enter **lev0**.

**Step 2** - Repeat **Step 1** and create an entry for Messaging access extension (not shown).

change aar analysis 0							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all						Percent Full: 1		
	Dialed	Total		Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
50		5	5	3	lev0		n	

## 5.14. Avaya G430 Media Gateway Provisioning

In the reference configuration, an Avaya G430 Media Gateway is provisioned. The G430 is used for local DSP resources, announcements, Music On Hold, etc.

**Note** – Only the Media Gateway provisioning associated with the G430 registration to Communication Manager is shown below. For more information on the provisioning of the Medias Gateway see [8] in the Additional Reference section.

**Step 1** - Use SSH to connect to the G430 (not shown). Note that the Media Gateway prompt will contain “???” if the Media Gateway is not registered to Communication Manager (e.g., *G430-???(super)#*).

**Step 2** - Enter the **show system** command and copy down the G430 serial number.

**Step 3** - Enter the **set mgc list x.x.x.x** command where x.x.x.x is the IP address of the Communication Manager Procr (e.g., **10.64.91.87**, see **Section 5.5**).

**Step 4** - Enter the **copy run start** command to save the G430 configuration.

**Step 5** - From Communication Manager SAT, enter **add media-gateway x** where x is an available Media Gateway identifier (e.g., **1**).

**Step 6** – On the Media Gateway form (not shown), enter the following parameters:

- Set **Type** = **g430**.
- Set **Name** = a descriptive name (e.g., **G430-1**).
- Set **Serial Number** = enter the serial number copied from **Step 2**.
- Set the **Link Encryption Type** parameter as desired (**any-ptls/tls** was used in the reference configuration).
- Set **Network Region** = **1**.

Wait a few minutes for the G430 to register to Communication Manager. When the Media Gateway registers, the G430 SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., *G430-001(super)#*).

**Step 7** - Enter the **display media-gateway 1** command and verify that the G430 has registered.

```
display media-gateway 1                                     Page 1 of 2
                                     MEDIA GATEWAY 1
                                     Type: g430
                                     Name: G430-1
                                     Serial No: 11IS31439520
Link Encryption Type: any-ptls/tls      Enable CF? n
Mutual Authentication: optional
Network Region: 1                      Location: 1
Use for IP Sync? n                     Site Data:
Recovery Rule: none
Registered: y
Gateway Mode: Enterprise
FW Version/HW Vintage: 42 .4 .0 /1
MGP IPV4 Address: 192.168.7.150
MGP IPV6 Address:
Controller IP Address: 10.64.91.87
MAC Address: 00:1b:4f:53:37:69
```

## 5.15. Avaya Aura® Media Server Provisioning

In the reference configuration, an Avaya Aura® Media Server is provisioned. The Media Server is used, along with the G430 Media Gateway, for local DSP resources, announcements, and Music On Hold.

**Note** – Only the Media Server provisioning associated with Communication Manager is shown below. See [9] and [10] for additional information.

- Step 1** - Access the Media Server Element Manager web interface by typing “https://x.x.x.x:8443” (where x.x.x.x is the IP address of the Media Server) (not shown).
- Step 2** - On the Media Server Element Manager, navigate to **Home → System Configuration → Signaling Protocols → SIP → Node and Routes** and add the Communication Manager Procr interface IP address (e.g., 10.64.91.87, see Section 5.4) as a trusted node (not shown).
- Step 3** - On Communication Manager, enter the **add signaling-group x** command where x is an unused signaling group (e.g., 80), and provision the following:
- **Group Type** – Set to **sip**.
  - **Transport Method** – Set to **tls**
  - Verify that **Peer Detection Enabled?** – Set to **n**.
  - **Peer Server** to **AMS**.
  - **Near-end Node Name** – Set to the node name of the **procr** noted in Section 5.4.
  - **Far-end Node Name** – Set to the node name of Media Server as administered in Section 5.4 (e.g., AMS10).
  - **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061**.
  - **Far-end Network Region** – Set the IP network region to **1**, as set in Section 5.7.1.
  - **Far-end Domain** – Automatically populated with the IP address of the Media Server.

```
add signaling-group 80                                     Page 1 of 2
                                                         SIGNALING GROUP

Group Number: 80           Group Type: sip
                          Transport Method: tls

Peer Detection Enabled? n Peer Server: AMS

Near-end Node Name: procr      Far-end Node Name: AMS10
Near-end Listen Port: 5061     Far-end Listen Port: 5061
                               Far-end Network Region: 1

Far-end Domain: 10.64.91.88
```



**Step 4** - On Communication Manager, enter the **add media-server x** command where x is an available Media Server identifier (e.g., **1**). Enter the following parameters:

- **Signaling Group** – Enter the signaling group previously configured for Media Server (e.g., **80**).
- **Voip Channel License Limit** – Enter the number of VoIP channels for this Media Server (based on licensing) (e.g., **300**).
- **Dedicated Voip Channel Licenses** – Enter the number of VoIP channels licensed to this Media Server (e.g., **300**).
- Remaining fields are automatically populated based on the signaling group provisioning for the Media Server.

```
add media-server 1                                     Page 1 of 1
                                                    MEDIA SERVER

Media Server ID: 1

    Signaling Group: 80
    Voip Channel License Limit: 300
    Dedicated Voip Channel Licenses: 300

Node Name: AMS10
Network Region: 1
Location: 1
Announcement Storage Area: ANNC-be99ad1a-1f39-41e5-ba04-000c29f8f3f3
```

## 5.16. Save Translations

After the Communication Manager provisioning is completed, enter the command **save translation**.

## 5.17. Verify TLS Certificates – Communication Manager

**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 Communication Manager. Follow the steps below to verify the certificates used by Communication Manager.

**Step 1** - From a web browser, type in “https://<ip-address>”, where “<ip-address>” is the IP address or FQDN of Communication Manager. Follow the prompted steps to enter appropriate **Logon ID** and **Password** credentials to log in (not shown).

**Step 2** - Click on **Administration** at the top of the page and select **Server (Maintenance)** (not shown). Click on **Security** → **Trusted Certificate** and verify the System Manager CA certificate is present in the Communication Manager trusted repository.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) for server cm10. The left sidebar contains a navigation menu with categories: Administration / Server (Maintenance), Data Backup/Restore, Security, and Miscellaneous. The main content area is titled "Trusted Certificates" and includes a description: "This page provides management of the trusted security certificates present on this server." Below this is a legend for Trusted Repositories: A = Authentication, Authorization and Accounting Services (e.g., LDAP), C = Communication Manager, W = Web Server, R = Remote Logging. A table lists three certificates:

Select File	Issued To	Issued By	Expiration Date	Trusted By
<input type="radio"/> SystemManager10CA.crt	System Manager CA	System Manager CA	Tue Jan 29 2047	A C W R
<input type="radio"/> apr-ca.crt	Avaya Product Root CA	Avaya Product Root CA	Sun Aug 14 2033	C R
<input type="radio"/> sip_product_root.crt	SIP Product Certificate Authority	SIP Product Certificate Authority	Tue Aug 17 2027	C R

At the bottom of the table are buttons: Display, Add, Remove, Copy, and Help.

**Step 3** - Click on **Security** → **Server/Application Certificates** and verify the server identity certificate, signed by the System Manager CA is present in the certificate repository.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) for server cm10. The left sidebar is the same as in the previous screenshot. The main content area is titled "Server/Application Certificates" and includes a description: "This page provides management of the server/application certificates present on this server." Below this is a legend for Certificate Repositories: A = Authentication, Authorization and Accounting Services (e.g., LDAP), C = Communication Manager, W = Web Server, R = Remote Logging. A table lists one certificate:

Select File	Issued To	Issued By	Expiration Date	Installed In
<input type="radio"/> server.crt	cm10.avayalab.com	System Manager CA	Sat Mar 02 2024	A C W R

At the bottom of the table are buttons: Display, Add, Remove, Copy, and Help.

## 6. Configure Avaya Aura® Session Manager

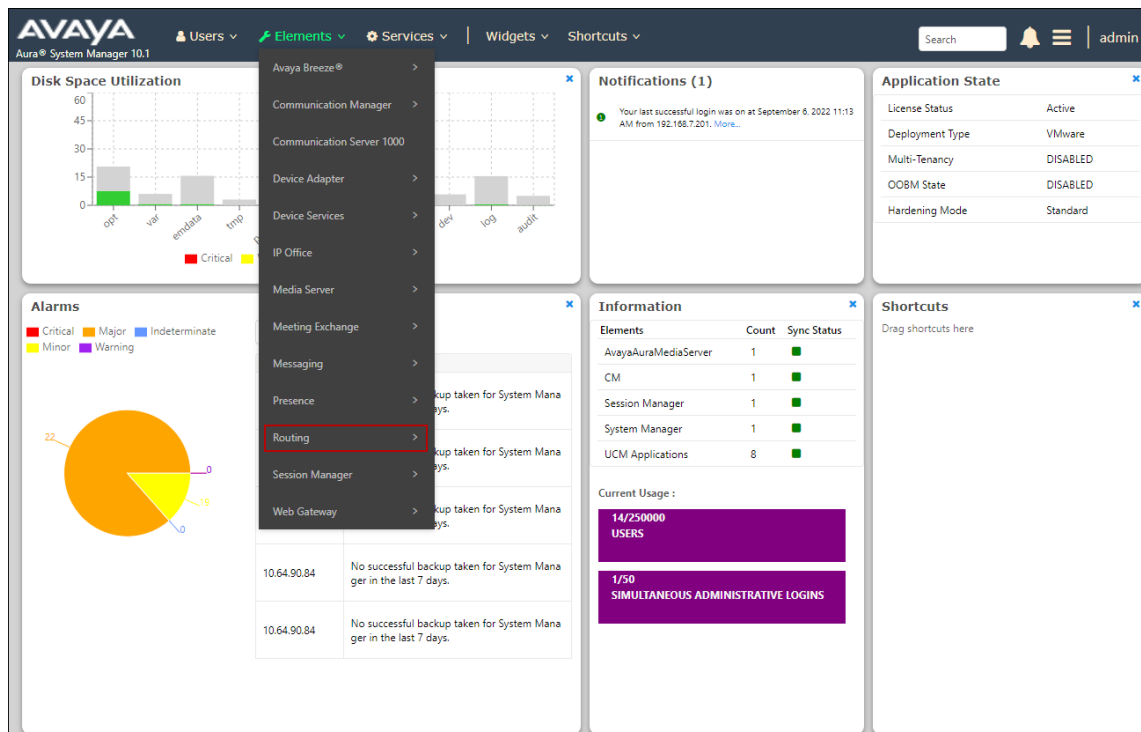
This section provides the procedures for configuring Session Manager to process inbound and outbound calls between Communication Manager and the Avaya SBCE. In the reference configuration, all Session Manager provisioning is performed via System Manager.

- Define a SIP Domain.
- Define a Location for Customer Premises Equipment (CPE).
- Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager and the Avaya SBCE.
- Define SIP Entities corresponding to Session Manager, Communication Manager, the Avaya SBCE, Messaging and Experience Portal.
- Define Entity Links describing the SIP trunks between Session Manager, Communication Manager, Messaging and Experience Portal, as well as the SIP trunks between Session Manager and the Avaya SBCE.
- Define Routing Policies associated with the Communication Manager, Messaging, Experience Portal and the Avaya SBCE.
- Define Dial Patterns, which govern which Routing Policy will be selected for inbound and outbound call routing.
- Verify TLS Certificates.

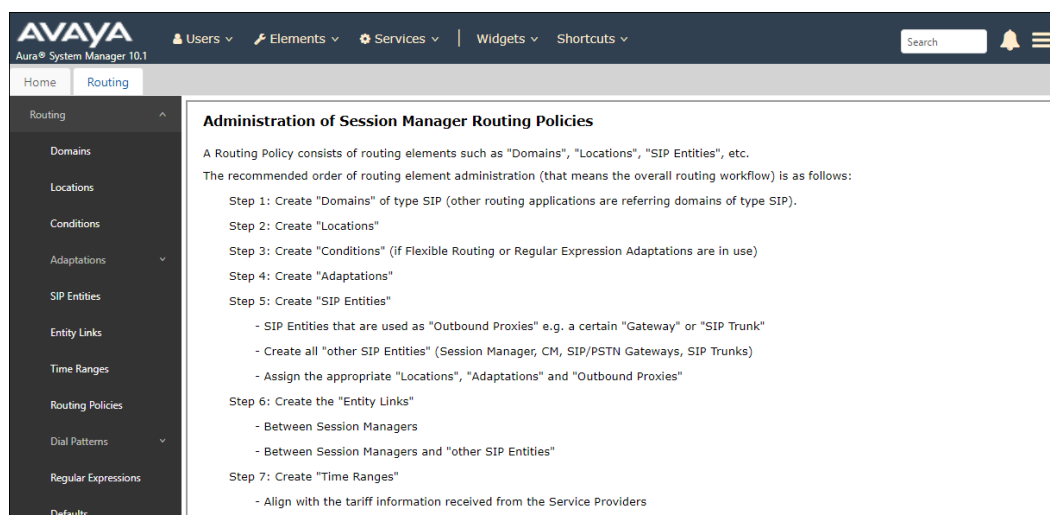
**Note** – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult [1]- [4] in the Additional References section for further details.

## 6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). Once logged in, the **Home** screen is displayed. From the **Home** screen, under the **Elements** heading, select **Routing**.



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



## 6.2. SIP Domain

**Step 1** - Select **Domains** from the left navigation menu. In the reference configuration, domain **avayalab.com** was defined.

**Step 2** - Click **New**. Enter the following values and use default values for remaining fields.

- **Name:** Enter the enterprise SIP Domain Name. In the sample screen below, **avayalab.com** is shown.
- **Type:** Verify **sip** is selected.
- **Notes:** Add a brief description.

**Step 3** - Click **Commit** (not shown) to save.



## 6.3. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. In the reference configuration, three Locations are specified:

- **Main** – The customer site containing System Manager, Session Manager and local SIP endpoints.
- **CM-TG-1** – Communication Manager trunk group 1 designated for Verizon.
- **SBCs** – Avaya SBCE.

### 6.3.1 Main Location

**Step 1** - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the Location (e.g., **Main**).
- **Notes:** Add a brief description.

**Step 2** - Click **Commit** to save.

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Location Details

CommitCancel

General

\* Name:

Main

Notes:

Avaya SIL

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

\* Minimum Multimedia Bandwidth:

64

Kbit/Sec

\* Default Audio Bandwidth:

80

Kbit/sec

Alarm Threshold

Overall Alarm Threshold:

80

%

### 6.3.2 CM-TG1 Location

To configure the Communication Manager Trunk Group 1 Location, repeat the steps in **Section 6.3.1** with the following changes (not shown):

- **Name** – Enter a descriptive name (e.g., **CM-TG1**).

### 6.3.3 SBCs Location

To configure the Avaya SBCE Location, repeat the steps in **Section 6.3.1** with the following changes (not shown):

- **Name** – Enter a descriptive name (e.g., **SBCs**).

## 6.4. Configure Adaptations

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

- Calls from Verizon (**Section 6.4.1**) - Modification of SIP messages sent to Communication Manager extensions.
  - The Verizon DNIS number digit string in the Request URI is replaced with the associated Communication Manager extensions/VDN.
- Calls to Verizon (**Section 6.4.2**) - Modification of SIP messages sent by Communication Manager extensions.
  - The History-Info header is converted to a Diversion header automatically by the **VerizonAdapter**.
  - Avaya SIP headers not required by Verizon are removed (see **Section 2.4**).

### 6.4.1 Adaptation for Avaya Aura® Communication Manager

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

**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:

1. A descriptive **Name**, (e.g., **CM-TG1-VzIPT**).
2. Select **DigitConversionAdapter** from the **Module Name** drop down.
3. Select **Name-Value Parameter** from the **Module Parameter Type** drop down:
  - **Name: “fromto”      Value: “true”**
    - This adapts the From and To headers along with the Request-Line and PAI headers.
  - **Name: “osrcd”      Value: “avayalab.com”**
    - This enables the source domain to be overwritten with the enterprise domain “avayalab.com”. For example, for inbound PSTN calls from Verizon to Communication Manager, the PAI header will contain “avayalab.com”.

**Note** – Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion.

The screenshot shows the 'Adaptation Details' page in the Avaya Aura Session Manager Administration interface. The left sidebar contains a navigation menu with 'Routing' selected, and 'Adaptations' highlighted. The main content area is titled 'Adaptation Details' and includes a 'General' tab. The form fields are as follows:

- Adaptation Name:** CM-TG1-VzIPT
- Module Name:** DigitConversionAdapter
- Module Parameter Type:** Name-Value Parameter

Below these fields is a table for adding parameters:

Name	Value
fromto	true
osrcd	avayalab.com

At the bottom of the form, there are fields for 'Egress URI Parameters' (empty) and 'Notes' (CM - Vz - IPT). Buttons for 'Commit' and 'Cancel' are located at the top right of the form area.

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

1. **Example 1 – destination extension:** 7329450231 is a DNIS string sent in the Request URI by the Verizon Business IP Trunking service that is associated with Communication Manager extension 12001.

- Enter **7329450231** in the **Matching Pattern** column.
- Enter **10** in the **Min/Max** columns.
- Enter **10** in the **Delete Digits** column.
- Enter **12001** in the **Insert Digits** column.
- Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
- Enter any desired notes.

**Step 4** - Repeat **Step 3** for all additional Verizon DNIS numbers/Communication Manager extensions.

**Step 5** - Click on **Commit**.

**Note** – No **Digit Conversion for Incoming Calls to SM** were required in the reference configuration.

**Note** – In the reference configuration, the Verizon Business IP Trunking service delivered 10-digit DNIS numbers.

**Digit Conversion for Outgoing Calls from SM**

Add Remove

4 Items Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 7329450	* 10	* 10		* 5		destination ▼		Verizon DIDs
<input type="checkbox"/>	* 7329450228	* 10	* 10		* 10	12001	destination ▼		
<input type="checkbox"/>	* 7329450229	* 10	* 10		* 10	12000	destination ▼		analog fax
<input type="checkbox"/>	* 7329450231	* 10	* 10		* 10	12001	destination ▼		

Select : All, None

Commit Cancel



## 6.4.2 Adaptation for the Verizon Business IP Trunking service

The Adaptation administered in this section is used for modification of SIP messages from Communication Manager to Verizon. Repeat the steps in **Section 6.4.1** with the following changes.

**Step 1** - In the **Adaptation Details** page, enter:

1. A descriptive **Name**, (e.g., **SBC1-Adaptation for Verizon**).
2. Select **VerizonAdapter** from the **Module Name** drop down menu. The VerizonAdapter will automatically remove History-Info headers, (which the Verizon Business IP Trunking service does not support), sent by Communication Manager (see **Section 5.8.1**) and replace them with Diversion headers.

**Step 2** - In the **Module Parameter Type**: field select **Name-Value Parameter** from the menu.

**Step 3** - In the **Name-Value Parameter** table, enter the following:

1. **Name** – Enter **eRHdrs**
  - **Value** – Enter the following Avaya headers to be removed by Session Manager.  
**“AV-Global-Session-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, P-Charging-Vector, P-Location, AV-Correlation-ID, Av-Secure-Indication”**

Home Routing

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

**Adaptation Details** Commit Cancel Help ?

**General**

\* Adaptation Name: SBC1-Adaptation for Verizon

\* Module Name: VerizonAdapter

Module Parameter Type: Name-Value Parameter

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

Select : All, None

Egress URI Parameters:

Notes: SBC - Verizon IPT

**Step 4** - Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the outbound digits to Verizon that need to be converted to 10-digit numbers).

1. As described in **Section 2.2, Item 2**, the E.164 formatted numbers sent by Communication Manager's public-unknown numbering table (**Section 5.9**) on the outbound origination headers, need to be converted to 10 digit numbers expected by Verizon.
  - Enter + in the **Matching Pattern** column.
  - Enter **12** in the **Min/Max** columns.
  - Enter **2** in the **Delete Digits** column.
  - Specify that this should be applied to the SIP **origination** headers in the **Address to modify** column.
  - Enter any desired notes
2. As described in **Section 2.2, Item 3**, during certain call transfer scenarios the From header on the INVITEs arriving from Communication Manager contained 11 digits numbers, without the "+". These numbers also need to be converted to the 10 digit numbers expected by Verizon. Repeat the steps on 1 above with the following differences:
  - Enter 1 in the **Matching Pattern** column.
  - Enter **11** in the **Min/Max** columns.
  - Enter **1** in the **Delete Digits** column.

Digit Conversion for Outgoing Calls from SM										
Add		Remove								
3 Items										Filter: Enable
<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes	
<input type="checkbox"/>	* +	* 12	* 12		* 2		origination		E.164 to 10 Digit Calling Party conversion	
<input type="checkbox"/>	* 1	* 11	* 11		* 1		origination		11 to 10 digit Calling Party Conversion	
<input type="checkbox"/>	* +1303248	* 12	* 12		* 2		origination	7329450821	Unscreened ANI - Diversion header	

Select : All, None

**Note** – The Screened Telephone Number (STN) provided by Verizon for this test is 7329450821. Typically, customers would have one or more STN; one for every location. A central Session Manager could be used to pass multiple STNs to Verizon based on a **Matching Pattern** (i.e., a user's Calling Line Identification). The STN would then be entered in the **Adaptation Data** field as shown above.

## 6.5. SIP Entities

In this section, SIP Entities are administered for the following SIP network elements:

- Session Manager (**Section 6.5**).
- Communication Manager for Verizon trunk access (**Section 6.5.2**) – This entity, and its associated Entity Link (using TLS with port 5081), is for calls to/from Verizon and Communication Manager via the Avaya SBCE.
- Communication Manager for local trunk access (**Section 6.5.3**) – This entity, and its associated Entity Link (using TLS with port 5061), is primarily for traffic between Avaya SIP telephones and Communication Manager, as well as calls to Messaging.
- Avaya SBCE (**Section 6.5.4**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from the Verizon Business IP Trunking service via the Avaya SBCE.
- Messaging (**Section 6.5.5**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from Messaging.
- Experience Portal (**Section 6.5.6**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from Experience Portal.

**Note** – In the reference configuration, TLS is used as the transport protocol between Session Manager and Communication Manager (ports 5061 and 5081), and to the Avaya SBCE (port 5061). The connection between the Avaya SBCE and the Verizon Business IP Trunking service uses UDP/5071 per Verizon requirements.

### 6.5.1 Avaya Aura® Session Manager SIP Entity

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

**Step 2** - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name** – Enter a descriptive name (e.g., **Session Manager**).
- **FQDN or IP Address** – Enter the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **10.64.91.85**).
- **Type** – Verify **Session Manager** is selected.
- **Location** – Select location **Main** (**Section 6.3.1**).
- **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
- **Time Zone** – Select the time zone in which Session Manager resides.
- **Minimum TLS Version** – Select the TLS version, or select **Use Global Settings** to use the default TLS version, configurable at the global level (**Elements**→**Session Manager**→**Global Settings**).

**Step 3** - In the **Monitoring** section of the **SIP Entity Details** page configure as follows:

- Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
- Use the default values for the remaining parameters.

**SIP Entity Details** [Commit] [Cancel]

**General**

\* Name: Session Manager

\* IP Address: 10.64.91.85

SIP FQDN:

Type: Session Manager

Notes:

Location: Main

Outbound Proxy:

Time Zone: America/Denver

Minimum TLS Version: Use Global Setting

Credential name:

**Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

**Step 4** - Scrolling down to the **Listen Port** section of the **SIP Entity Details** page. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.6**. Click on **Add** and provision entries as follows:

- **Port** – Enter **5061**.
- **Protocol** – Select **TLS**.
- **Default Domain** – Select a SIP domain administered in **Section 6.26.2** (e.g., **avayalab.com**).

**Step 5** - Repeat **Step 4** to provision entries for any other listening ports used by Session Manager, for example:

- **5060** for **Port** and **TCP** for **Protocol**.
- **5060** for **Port** and **UDP** for **Protocol**.

**Step 6** - Enter any notes as desired and leave all other fields on the page blank/default.

**Step 7** - Click on **Commit**.

Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/> 5060	TCP	avayalab.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/> 5060	UDP	avayalab.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/> 5061	TLS	avayalab.com	<input checked="" type="checkbox"/>	

**Note** – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 6.6**. The **SIP Responses to an OPTIONS Request** section of the form is not used in the reference configuration.

## 6.5.2 Avaya Aura® Communication Manager SIP Entity – Public Trunk

**Step 1** - In the **SIP Entities** page, click on **New** (not shown).

**Step 2** - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name** – Enter a descriptive name (e.g., **CM-TG1**).
- **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Section 5.5** (e.g., **10.64.91.87**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **CM-TG1-VzIPT** administered in **Section 6.4.1**.
- **Location** – Select the **CM-TG1** Location administered in **Section 6.3.2**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Link Monitoring** section of the **SIP Entity Details** page select:
  - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field and use the default values for the remaining parameters.

**Step 3** - Click on **Commit**.

**SIP Entity Details** [Commit] [Cancel]

**General**

\* **Name:** CM-TG1

\* **FQDN or IP Address:** 10.64.91.87

**Type:** CM

**Notes:** Trunk Group 1 - CM to Vz IPT

**Adaptation:** CM-TG1-VzIPT

**Location:** CM-TG1

**Time Zone:** America/Denver

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

**Minimum TLS Version:** Use Global Setting

**Credential name:**

**Securable:** ☐

**Call Detail Recording:** none

**Loop Detection**

**Loop Detection Mode:** On

**Loop Count Threshold:** 5

**Loop Detection Interval (in msec):** 200

**Monitoring**

**SIP Link Monitoring:** Use Session Manager Configuration

**CRLF Keep Alive Monitoring:** Use Session Manager Configuration

**Supports Call Admission Control:** ☐

**Shared Bandwidth Manager:** ☐

### 6.5.3 Avaya Aura® Communication Manager SIP Entity – Local Trunk

To configure the Communication Manager Local trunk SIP Entity, repeat the steps in **Section 6.5.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **CM-TG3**).
- **Adaptations** – Leave this field blank.
- **Location** – Select Location **Main** administered in **Section 6.3.1**.

### 6.5.4 Avaya Session Border Controller for Enterprise SIP Entity

Repeat the steps in **Section 6.5.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **SBCE-90\_Vz1**).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.64.91.50**, see **Section 8.5**).
- **Type** – Select **SIP Trunk**.
- **Adaptations** – Select Adaptation **SBC1-Adaptation for Verizon** (**Section 6.4.2**).
- **Location** – Select Location **SBCs** administered in **Section 6.3.3**.

### 6.5.5 Avaya Messaging SIP Entity

Repeat the steps in **Section 6.5.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **Avaya Messaging**).
- **FQDN or IP Address** – Enter the IP address of Messaging (e.g., **10.64.19.90**).
- **Type** – Select **Messaging**.
- **Adaptations** – Leave this field blank.
- **Location** – Select Location **Main** administered in **Section 6.3.1**.

### 6.5.6 Avaya Experience Portal SIP Entity

Repeat the steps in **Section 6.5.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **Experience Portal**).
- **FQDN or IP Address** – Enter the IP address of Experience Portal (e.g., **10.64.91.90**).
- **Type** – Select **Voice Portal**.
- **Adaptations** – Leave this field blank.
- **Location** – Select Location **Main** administered in **Section 6.3.1**.

## 6.6. Entity Links

In this section, Entity Links are administered for the following connections:

- Session Manager to Communication Manager Public trunk (**Section 6.6.1**).
- Session Manager to Communication Manager Local trunk (**Section 6.6.2**).
- Session Manager to Avaya SBCE (**Section 6.6.3**).
- Session Manager to Messaging (**Section 6.6.4**).
- Session Manager to Experience Portal (**Section 6.6.5**).

**Note** – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages configured in **Section 6.5**.

**Note** – See the information in **Section 6.5** regarding the transport protocols and ports used in the reference configuration.

### 6.6.1 Entity Link to Avaya Aura® Communication Manager – Public Trunk

**Step 1** - In the left pane under **Routing**, click on **Entity Links**, then click on **New** (not shown).

**Step 2** - Continuing in the **Entity Links** page, provision the following:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **SM to CM TG1**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 6.5** for Session Manager (e.g., **Session Manager**).
- **Protocol** – Select **TLS** (see **Section 5.8.1**).
- **SIP Entity 1 Port** – Enter **5081**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.2** for the Communication Manager public entity (e.g., **CM-TG1**).
- **SIP Entity 2 Port** – Enter **5081** (see **Section 5.8.1**).
- **Connection Policy** – Select **trusted**.
- Leave other fields as default.

**Step 3** - Click on **Commit**.

The screenshot displays the 'Entity Links' configuration page in the Avaya Aura Configuration Manager. The left-hand navigation pane is expanded to 'Routing', and 'Entity Links' is the active selection. The main content area shows a table with one configured entity link. The table columns are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, and Connection Policy. The single entry has the following values: Name 'SM to CM TG1', SIP Entity 1 'Session Manager', Protocol 'TLS', Port '5081', SIP Entity 2 'CM-TG1', Port '5081', DNS Override 'No', and Connection Policy 'trusted'. Above the table, there are 'Commit' and 'Cancel' buttons. Below the table, there is a 'Select : All, None' dropdown. A 'Filter: Enable' link is also present in the top right of the table area.

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
<input type="checkbox"/>	* SM to CM TG1	* Session Manager	TLS	* 5081	* CM-TG1	* 5081	<input type="checkbox"/>	trusted



## 6.6.2 Entity Link to Avaya Aura® Communication Manager – Local Trunk

To configure this Entity Link, repeat the steps in **Section 6.6.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **SM to CM TG3**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.3** for the Communication Manager local entity (e.g., **CM-TG3**).
- **SIP Entity 2 Port** – Enter **5061** (see **Section 5.8.2**).

## 6.6.3 Entity Link for the Verizon Business IP Trunking service via the Avaya SBCE

To configure this Entity Link, repeat the steps in **Section 6.6.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **SM to SBCE90\_Vz1**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.4** for the Avaya SBCE entity (e.g., **SBC90\_Vz1**).
- **SIP Entity 2 Port** – Enter **5061**.

## 6.6.4 Entity Link to Avaya Messaging

To configure this Entity Link, repeat the steps in **Section 6.6.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to Messaging (e.g., **SM to Messaging**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.5** for the Messaging entity (e.g., **Avaya Messaging**).
- **SIP Entity 2 Port** – Enter **5061**.

## 6.6.5 Entity Link to Avaya Experience Portal

To configure this Entity Link, repeat the steps in **Section 6.6.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to Messaging (e.g., **SM to Experience Portal**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.6** for the Experience Portal entity (e.g., **Experience Portal**).
- **SIP Entity 2 Port** – Enter **5061**.

## 6.7. Time Ranges

**Step 1** - In the left pane under **Routing**, click on **Time Ranges**. In the **Time Ranges** page click on **New**.

**Step 2** - Continuing in the **Time Ranges** page, enter a descriptive **Name**, check the checkbox(s) for the desired day(s) of the week, and enter the desired **Start Time** and **End Time**.

**Step 3** - Click on **Commit** (not shown). Repeat these steps to provision additional time ranges as required.

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
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	

## 6.8. Routing Policies

In this section, the following Routing Policies are administered:

- Inbound calls to Communication Manager extensions (**Section 6.8.1**).
- Inbound calls to Messaging (**Section 6.8.2**).
- Inbound calls to Experience Portal (**Section 6.8.3**).
- Outbound calls to Verizon/PSTN (**Section 6.8.4**).

### 6.8.1 Routing Policy for Verizon Inbound Calls to Avaya Aura® Communication Manager

This Routing Policy is used for inbound calls from Verizon.

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

**Step 2** - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing Verizon calls to Communication Manager (e.g., **To CM TG1**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

**Step 3** - In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the **SIP Entities** list page will open.

**Routing Policy Details** [Commit] [Cancel]

**General**

\* Name: To CM TG1

Disabled: ☐

\* Retries: 0

Notes: Trunk Group 1 PSTN1 to CM

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
------	--------------------	------	-------

**Time of Day**

Add Remove View Gaps/Overlaps

**Step 4** - In the **SIP Entities** list page, select the SIP Entity administered in **Section 6.5.2** for the Communication Manager public SIP Entity (**CM-TG1**), and click on **Select**.

**SIP Entities** Help ?

New Edit Delete Duplicate More Actions

16 Items Filter: Enable

<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	<a href="#">Aura Messaging</a>	10.64.91.84	Messaging	Aura Messaging on VMware host 162
<input type="checkbox"/>	<a href="#">Avaya Messaging</a>	10.64.19.90	Other	Windows Server 2016 host 161
<input type="checkbox"/>	<b>CM-TG1</b>	10.64.91.87	CM	Trunk Group 1 - CM to Vz IPT
<input type="checkbox"/>	<a href="#">CM-TG2</a>	10.64.91.87	CM	Trunk Group 2 Vz IPCC
<input type="checkbox"/>	<a href="#">CM-TG3</a>	10.64.91.87	CM	Enterprise
<input type="checkbox"/>	<a href="#">CM-TG5</a>	10.64.91.87	CM	Trunk Group 5 - CM to ATT IPFR
<input type="checkbox"/>	<a href="#">CM-TG6</a>	10.64.91.87	CM	CM TG6 IX Messaging
<input type="checkbox"/>	<a href="#">CM-TG7</a>	10.64.91.87	CM	Trunk Group 7 BT
<input type="checkbox"/>	<a href="#">Experience Portal</a>	10.64.91.90	Voice Portal	EP on VMware host 162
<input type="checkbox"/>	<a href="#">SBCE-100_Vz2</a>	10.64.91.100	SIP Trunk	Vz SBC2
<input type="checkbox"/>	<a href="#">SBCE-101</a>	10.64.91.101	SIP Trunk	2nd A1 interface on SBCE-100- CPaaS
<input type="checkbox"/>	<a href="#">SBCE30_HA</a>	10.64.91.32	SIP Trunk	SBCE HA on VMware host 162
<input type="checkbox"/>	<a href="#">SBCE-70_IPFR</a>	10.64.91.40	SIP Trunk	SBCE for AT&T IPFR
<input type="checkbox"/>	<a href="#">SBCE-70_TollFree</a>	10.64.91.41	SIP Trunk	SBCE for IPTF testing
<input type="checkbox"/>	<a href="#">SBCE-90_Vz1</a>	10.64.91.50	SIP Trunk	Verizon SBC1 to PSTN

Select : All, None Page 1 of 2

**Step 5** - Returning to the **Routing Policy Details** page in the **Time of Day** section, click on **Add**.

**Step 6** - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 6.7**, and click on **Select**.

**Step 7** - Returning to the **Routing Policy Details** page in the **Time of Day** section, enter a **Ranking** of **0**.

**Step 8** - No **Regular Expressions** were used in the reference configuration.

**Step 9** - Click on **Commit**.

**Note** – Once the **Dial Patterns** are defined (**Section 6.9**) they will appear in the **Dial Pattern** section of this form.

**Routing Policy Details** Commit Cancel Help ?

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
CM-TG1	10.64.91.87	CM	Trunk Group 1 - CM to Vz IPT

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

### 6.8.2 Routing Policy for Inbound Calls to Avaya Messaging

This routing policy is for inbound calls to Avaya Messaging for message retrieval. Repeat the steps in **Section 6.8.1** with the following differences:

- Enter a descriptive **Name** (e.g., **To Messaging**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 6.5.5** for Messaging (e.g., **Avaya Messaging**).

### 6.8.3 Routing Policy for Inbound Calls to Experience Portal

This routing policy is for inbound calls to Experience Portal. Repeat the steps in **Section 6.8.1** with the following differences:

- Enter a descriptive **Name** (e.g., **To Experience Portal**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 6.5.6** for Experience Portal (e.g., **Experience Portal**).

### 6.8.4 Routing Policy for Outbound Calls to Verizon

This Routing Policy is used for outbound calls to Verizon. Repeat the steps in **Section 6.8.1** with the following differences:

- Enter a descriptive **Name** for routing calls to the Verizon Business IP Trunking service via the Avaya SBCE (e.g., **To SBC1 Verizon**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 6.5.4** for the Avaya SBCE SIP Entity (e.g., **SBCE-90\_Vz1**).

## 6.9. Dial Patterns

In this section, Dial Patterns are administered matching the following calls:

- Origination Dial Pattern for inbound calls arriving from the local area code (**Section 6.9.2**).
- Inbound PSTN calls via the Verizon Business IP Trunking service to Communication Manager (**Section 6.9.22**).
- Inbound PSTN calls via the Verizon Business IP Trunking service to Experience Portal (**Section 6.9.23**).
- Outbound calls to Verizon/PSTN (**Section 04**).

### 6.9.1 Origination Dial Patterns – (Optional)

One of the routing enhancements in Session Manager release 8.1 is the addition of Origination Dial Patterns functionality. This configuration is optional. Origination Dial Pattern sets can be created to include digits patterns, which are matched by Session Manager to make more granular routing decisions, allowing the use of different routes for calls arriving to Session Manager from the same Originating Location. This is done by matching the number present in the From header of the incoming INVITE. More information can be found on [2] on the References section if necessary.

In the reference configuration, an Origination Dial Pattern set was created to route inbound calls originating from the local area code to Experience Portal, while calls from other area codes are routed to Communication Manager.

**Note:** To enable the use of Origination Dial Patterns, **Enable Flexible Routing** needs to be checked, under **Elements → Session Manager → Global Settings**.

The screenshot shows the 'Global Settings' page in the Session Manager interface. The left sidebar contains navigation links: Session Manager, Dashboard, Session Manager Admin..., Global Settings (selected), Communication Profile..., Network Configuration, Device and Location..., Application Configur..., System Status, System Tools, and Performance. The main content area is titled 'Global Settings' and includes a 'Commit' button, a 'Cancel' button, and a 'View Defaults' button. Below the title is a subtitle 'Administer settings that apply to all Session Managers'. The settings are organized into two columns. The left column includes: 'Failback Policy' (Auto), 'Allow Unauthenticated Emergency Calls' (checked), 'ELIN SIP Entity' (None), 'Ignore SDP for Call Admission Control' (unchecked), 'Disable Call Admission Control Threshold Alarms' (unchecked), 'Disable Loop Detection Alarms' (unchecked), '\*Loop Detection Alarms Threshold (hours)' (24), 'Enable Dial Plan Ranges' (unchecked), 'Enable Regular Expression Adaptations' (unchecked), 'Enable Flexible Routing' (checked and highlighted with a red box), 'Set Precedence for Routing' (Dial Patterns), 'Set Dial Patterns Precedence' (a table with columns 'Precedence Order' and 'Dial Patterns' showing 'Destination', 'Location', and 'Origination' in order), and 'Enable Load Balancer' (unchecked). The right column includes: 'Enable IPv6' (unchecked), 'Allow Unsecured PPM Traffic' (checked), 'Minimum SIP Entity TLS Version' (1.2), 'Minimum Endpoint TLS Version' (1.0), 'TLS Endpoint Certificate Validation' (None), 'Enable End to End Secure Call Indication' (checked), 'Enable Military Support' (unchecked), 'Enable Application Sequence for Emergency Calls' (checked), 'Emergency Call Resource-Priority Headers' (empty text field), 'Enable Implicit Users Applications for SIP users' (checked), and 'Enable SIP Resiliency' (unchecked).

**Step 1** - In the left pane under **Routing**, expand the **Dial Patterns** tab. Select **Origination Dial Patterns Sets** and click on **New** (not shown).

**Step 2** - In the **General** section of the **Origination Dial Pattern Set Details** page, enter a descriptive name (e.g., **Calls from local area code**).

**Step 3** - In the **Origination Dial Patterns** section, click on **New**.

Routing

Origination Dial Pattern Set Details

Commit Cancel

General

Name: Calls from local area code

Notes:

Origination Dial Patterns

New Edit Delete

0 Items

Pattern	Min	Max	SIP Domain	Notes
---------	-----	-----	------------	-------

Filter: Enable

Commit Cancel

**Step 3** - In the **Origination Dial Patterns** page, provision the following:

- **Pattern** – Enter **786**, the starting digits corresponding to the local area code.
- **Min** and **Max** – Enter **10**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.
- Click on **Commit**.

Origination Dial Patterns

Commit Cancel

1 Item

Pattern	Min	Max	SIP Domain	Notes
786	10	10	avayalab.com	

Select : All, None

Commit Cancel

**Step 4** – Back at the **Origination Dial Pattern Set Details** page, click on **Commit**.

Routing

Origination Dial Pattern Set Details

Commit Cancel

General

Name: Calls from local area code

Notes:

Origination Dial Patterns

New Edit Delete

1 Item

Pattern	Min	Max	SIP Domain	Notes
786	10	10	avayalab.com	

Select : All, None

Commit Cancel

## 6.9.2 Dial Pattern for Inbound PSTN Calls to Avaya Aura® Communication Manager

In the reference configuration inbound calls from the Verizon Business IP Trunking service sent 10 DNIS digits in the SIP Request URI. The DNIS pattern must be matched for further call processing.

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

**Step 2** - In the **General** section of the **Dial Pattern Details** page, provision the following:

- **Pattern** – Enter **7329450**. Note – The Adaptation defined for Communication Manager in **Section 6.4.1** will convert the various 732-945-0xxx numbers into their corresponding Communication Manager extensions.
- **Min** and **Max** – Enter **10**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.

**Dial Pattern Details** Commit Cancel Help ?

**General**

\* **Pattern:**

\* **Min:**

\* **Max:**

**Emergency Call:** ☐

**SIP Domain:**

**Notes:**

**Originating Locations, Origination Dial Pattern Sets, and Routing Policies**

Add Remove

0 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
--------------------------	---------------------------	----------------------------	-----------------------------------	------------------------------------	---------------------	------	-------------------------	----------------------------	----------------------

**Step 3** - Scroll down to the **Originating Locations, Origination Dial Patterns and Routing Policies** section of the **Dial Pattern Details** page and click on **Add**.

**Step 4** - In the **Originating Location**, check the checkbox corresponding to the Avaya SBCE location, e.g., **SBCs**.

**Step 5** - In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy administered for routing calls to the Communication Manager public trunk in **Section 6.8.1** (e.g., **To CM TG1**) and click on **Select**.

**Originating Location**

Select

Cancel

Help

**Originating Location**

☐ Apply The Selected Routing Policies to All Originating Locations

7 Items

Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	CM-TG1	
<input type="checkbox"/>	CM-TG5	
<input type="checkbox"/>	CM TG7	CM Trunk to BT
<input type="checkbox"/>	Experience Portal	
<input type="checkbox"/>	Main	Avaya SIL
<input type="checkbox"/>	Remote Access	Remote Workers Access from SBCE-90
<input checked="" type="checkbox"/>	SBCs	

Select : All, None

**Origination Dial Pattern Sets**

1 Item

Filter: Enable

<input type="radio"/>	Name	Notes
<input type="radio"/>	Calls from local area code	

Select : None

**Routing Policies**

11 Items

Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To Aura Messaging	<input type="checkbox"/>	Aura Messaging	
<input checked="" type="checkbox"/>	To CM TG1	<input type="checkbox"/>	CM-TG1	Trunk Group 1 Verizon to CM
<input type="checkbox"/>	To CM TG3	<input type="checkbox"/>	CM-TG3	Enterprise Traffic
<input type="checkbox"/>	To CM TG5	<input type="checkbox"/>	CM-TG5	Trunk Group 5 AT&T to CM
<input type="checkbox"/>	To CM TG7	<input type="checkbox"/>	CM-TG7	Trunk Group 7 Inbound from BT
<input type="checkbox"/>	To Experience Portal	<input type="checkbox"/>	Experience Portal	

**Step 6** - Returning to the Dial Pattern Details page and click on **Commit**.

**Step 7** - Repeat **Steps 1-6** for any additional inbound dial patterns from Verizon.

### 6.9.3 Dial Pattern for Inbound Calls to Experience Portal

In the reference configuration, one the Verizon IPT DID numbers, 7329450232, was assigned for inbound calls to Experience Portal.

**Step 1** - In the **General** section of the **Dial Pattern Details** page, repeat the steps shown in **Section 6.9.2**, with the following changes:

- **Pattern** – Enter the DID number assigned for calls to Experience Portal (e.g., **7329450232**).
- **Min** – Enter **10**.
- **Max** – Enter **10**



**Dial Pattern Details** Commit Cancel [Help ?](#)

**General**

\* **Pattern:**

\* **Min:**

\* **Max:**

**Emergency Call:** ☐

**SIP Domain:**

**Notes:**

**Originating Locations, Origination Dial Pattern Sets, and Routing Policies**

Add Remove

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"/>									

**Step 2** – On the **Originating Locations, Origination Dial Patterns Sets and Routing Policies** page, repeat the steps shown in **Section 6.9.2** with the following addition:

- Check the checkbox for the Origination Dial pattern Set corresponding to calls from the local area code, defined in **Section 6.9.1** (e.g., **Calls from local area code**).
- In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy administered for routing calls to Experience Portal in **Section 6.8.3** and click on **Select**.

**Originating Location** Select Cancel

**Originating Location**

☐ Apply The Selected Routing Policies to All Originating Locations

7 Items Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	CM-TG1	
<input type="checkbox"/>	CM-TG5	
<input type="checkbox"/>	CM TG7	CM Trunk to BT
<input type="checkbox"/>	Experience Portal	
<input type="checkbox"/>	Main	Avaya SIL
<input type="checkbox"/>	Remote Access	Remote Workers Access from SBCE-90
<input checked="" type="checkbox"/>	SBCs	

Select : All, None

**Origination Dial Pattern Sets**

1 Item Filter: Enable

<input type="radio"/>	Name	Notes
<input checked="" type="radio"/>	Calls from local area code	

Select : None

**Routing Policies**

11 Items Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To Aura Messaging	<input type="checkbox"/>	Aura Messaging	
<input type="checkbox"/>	To CM TG1	<input type="checkbox"/>	CM-TG1	Trunk Group 1 Verizon to CM
<input type="checkbox"/>	To CM TG3	<input type="checkbox"/>	CM-TG3	Enterprise Traffic
<input type="checkbox"/>	To CM TG5	<input type="checkbox"/>	CM-TG5	Trunk Group 5 AT&T to CM
<input type="checkbox"/>	To CM TG7	<input type="checkbox"/>	CM-TG7	Trunk Group 7 Inbound from BT
<input checked="" type="checkbox"/>	To Experience Portal	<input type="checkbox"/>	Experience Portal	

With this configuration, calls to this Verizon IPT DID number originating from the local area code will be routed to Experience Portal, while calls to this same number originating from area codes other than the local area will still be routed to Communication Manager, following the dial pattern shown previously in **Section 6.9.2**.

## 6.9.4 Dial Pattern for Outbound Calls to Verizon/PSTN

In this section, Dial Patterns are administered for all outbound calls to Verizon/PSTN. In the reference configuration E.164 numbers were used for national and international calls. Non-E.164 numbers were used for service numbers, e.g., x11, 1411, 5551212, etc.

**Step 1** - Repeat the steps shown in **Section 6.9.2**, with the following changes:

- In the **General** section of the **Dial Pattern Details** page, enter a dial pattern for routing calls to Verizon/PSTN (e.g., +). This will match any outbound call prefixed with a plus sign (+), such as an E.164 formatted number.
- Enter a **Min** pattern of **10**.
- Enter a **Max** pattern of **36**.
- In the **Routing Policies** section of the **Originating Locations, Origination Dial Patterns and Routing Policies** page, check the checkboxes corresponding to the Communication Manager Originating Location (e.g., **CM-TG1**) and the Routing Policy administered for routing calls to Verizon in **Section 6.8.4** (e.g., **To SBC1 Verizon**).

**Dial Pattern Details** Commit Cancel Help ?

**General**

\* Pattern: +

\* Min: 10

\* Max: 36

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: E.164 Public Numbers

**Originating Locations, Origination Dial Pattern Sets, and Routing Policies**

Add Remove

5 Items

<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"/>	CM-TG1				To SBC1 Verizon	0	<input type="checkbox"/>	SBCE-90_Vz1	To SBCE10-90 Verizon

Select : All, None

**Denied Originating Locations and Origination Dial Pattern Sets**

Add Remove

0 Items

<input type="checkbox"/>	Originating Location	Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes
--------------------------	----------------------	-------	-----------------------------------	------------------------------------

**Step 2** - Repeat **Step 1** to add any additional locations and outbound patterns as required.

**Dial Patterns** Help ?

New Edit Delete Duplicate More Actions

4 Items Found Filter: Disable, Apply, Clear

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	±	10	36	<input type="checkbox"/>			avayalab.com	outbound Outbound E.164 Public Numbers
<input type="checkbox"/>	1411	4	4	<input type="checkbox"/>			avayalab.com	Outbound PSTN Information
<input type="checkbox"/>	5551212	7	7	<input type="checkbox"/>			avayalab.com	Outbound Directory Service
<input type="checkbox"/>	x11	3	3	<input type="checkbox"/>			avayalab.com	Outbound Services

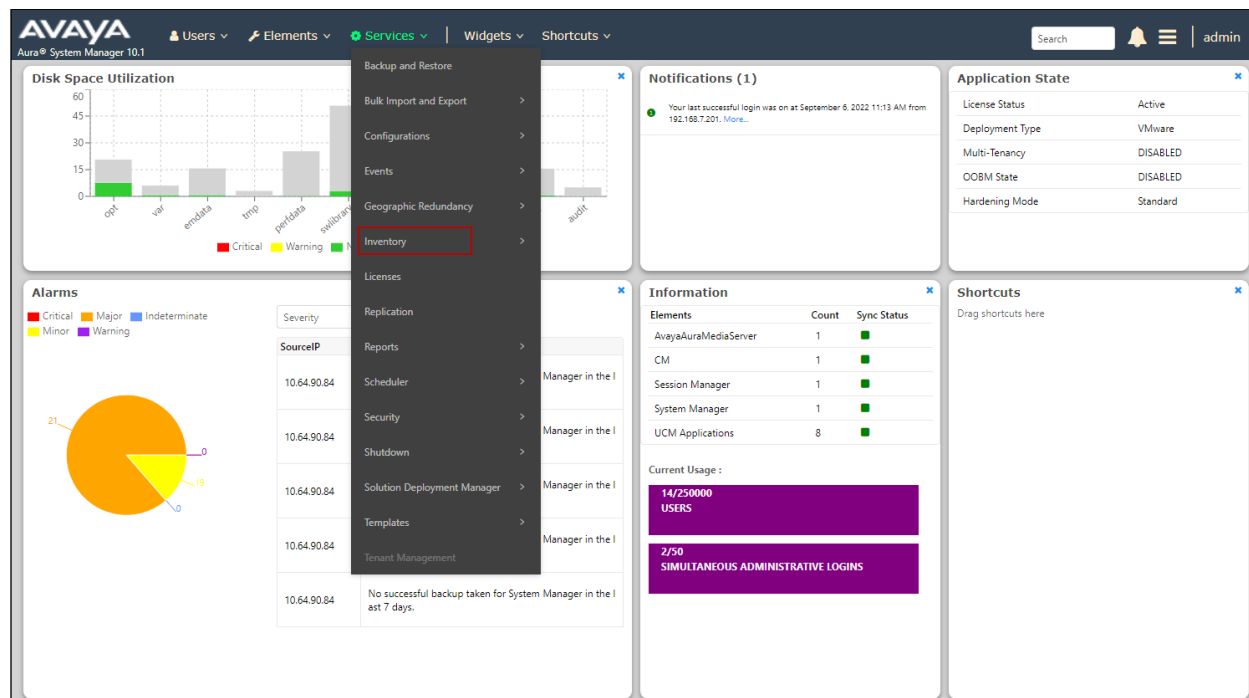
Select : All, None

## 6.10. Verify TLS Certificates – Session Manager

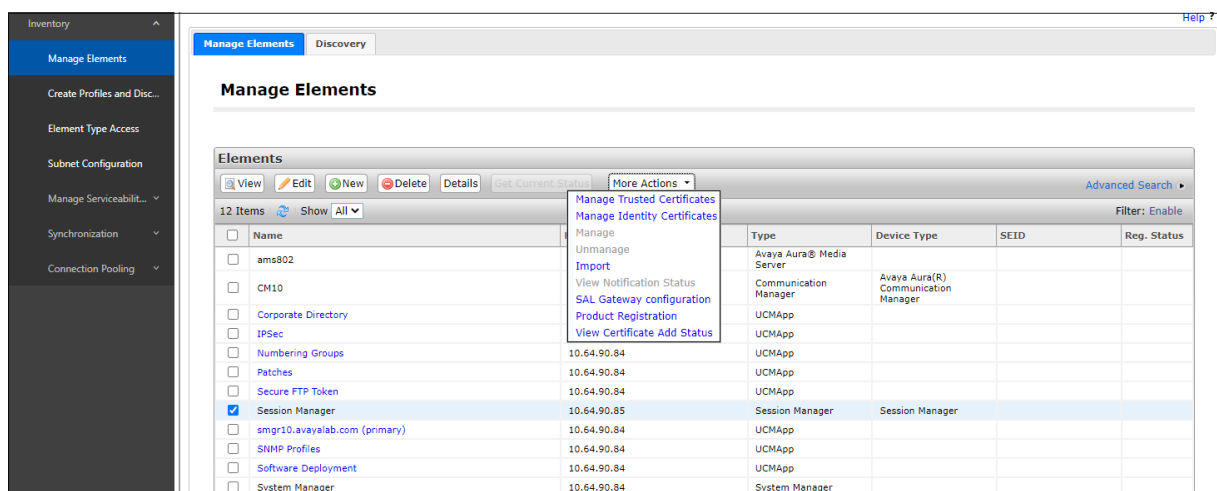
**Note** – Testing was done with System Manager signed identity certificates. The procedure to obtain and install certificates is outside the scope of these Application Notes.

The following procedures show how to verify the certificates used by Session Manager.

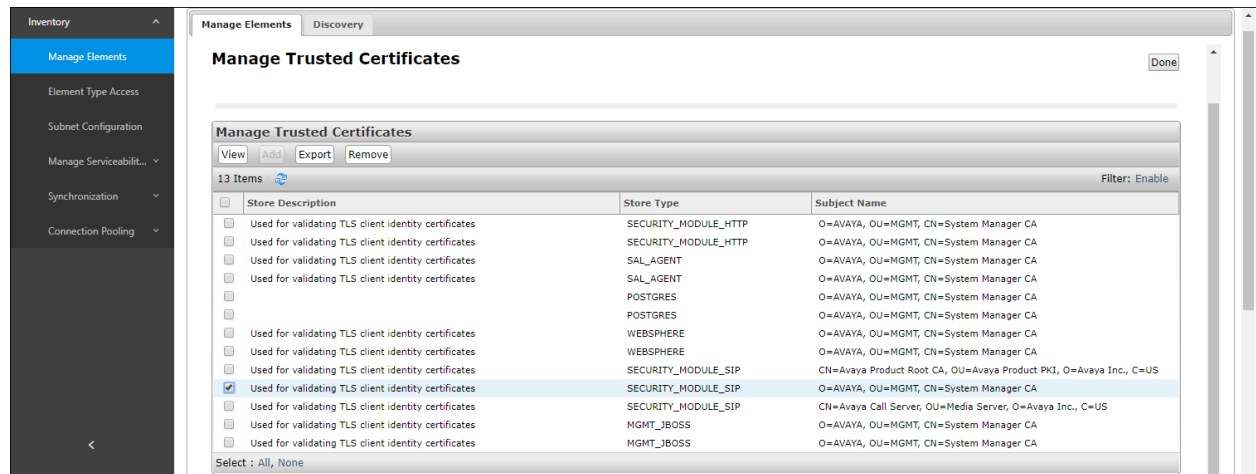
**Step 1** - From the **Home** screen, under the **Services** heading, select **Inventory**.



**Step 2** - In the left pane under **Inventory**, click on **Manage Elements** and select the Session Manager element, e.g., **Session Manager**. Click on **More Actions** → **Manage Trusted Certificates**.

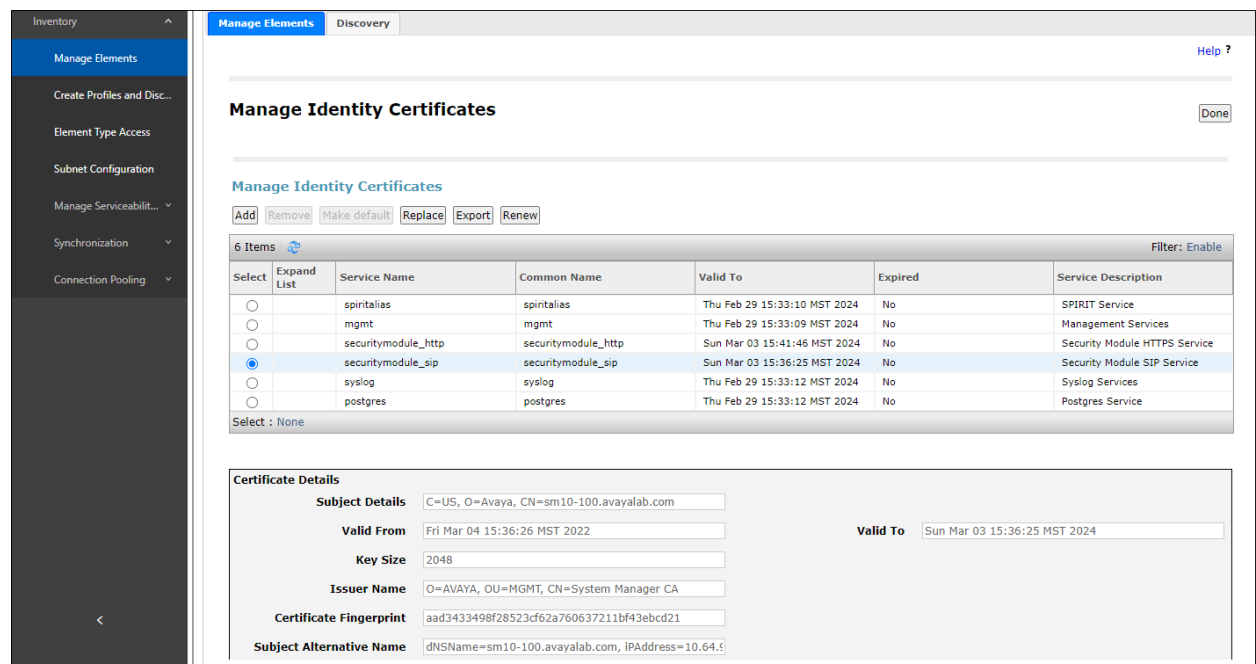


**Step 3** - Verify the **System Manager Certificate Authority** certificate is listed in the trusted store, **SECURITY\_MODULE\_SIP**. Click **Done** to return to the previous screen.



**Step 4** - With **Session Manager** selected, click on **More Actions** → **Manage Identity Certificates** (not shown).

**Step 5** - Verify the **Security Module SIP** service has a valid identity certificate signed by System Manager. If the **Subject Details** and **Subject Alternative Name** fields of the System Manager signed certificate need to be updated, click **Replace**, otherwise click **Done** (not shown).



## 7. Avaya 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 [13] and [14] in the Additional References section for further details if necessary.

### 7.1. 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 DNIS 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 call<sup>1</sup>.

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 Verizon Business IP Trunk 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.

---

<sup>1</sup> 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.

## 7.2. 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.

The screenshot shows the Avaya Experience Portal Manager (EPM) interface. The top header includes the Avaya logo, a welcome message for 'epadmin', and the last login time. The left sidebar contains a navigation menu with categories like User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration. The main content area is titled 'Avaya Experience Portal Manager' and provides an overview of the EPM application. It lists installed components: Media Processing Platform (MPP), Email Service, HTML Service, and SMS Service, each with a brief description. A 'Legal Notice' section is also visible, containing the Avaya Global Software License Terms, revised as of June 1st, 2020.

**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.

The screenshot displays the 'Licensing' page in the Avaya Experience Portal. It shows the current license information and a table of licensed products. The 'License Server Information' section includes the URL, last update time, and last successful poll. The 'Licensed Products' section lists various services and their corresponding license counts.

Licensed Products	
Experience Portal	
Announcement Ports:	100
ASR Connections:	100
Call Anchoring Ports:	100
Conversation Speech Connections:	0
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:	Sep 9, 2022 12:46:52 PM EDT
Last Changed:	Nov 3, 2020 3:02:12 PM EST

## 7.3. Verify TLS Certificates – Experience Portal

In the reference configuration, TLS transport is used for the communication between Session Manager and Experience Portal. Follow the steps below to verify the certificates used by Experience Portal.

**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.

**Step 1** – In the left pane, navigate to **Security** → **Certificates**. On the **Trusted Certificates** tab, verify the System Manager CA certificate is present in the certificate repository.

The screenshot shows the 'Certificates' page in the Experience Portal. The left navigation pane is expanded to 'Security' > 'Certificates'. The main content area has tabs for 'EP Signing Certificate', 'EPM Identity Certificates', 'MPP Identity Certificates', and 'Trusted Certificates'. The 'Trusted Certificates' tab is active, displaying a table with columns 'Name', 'Type', and 'Certificate'. A single entry is visible: 'SMGR10 SIP Connection'. The 'Certificate' column shows detailed information: Owner: O=AVAYA,OU=MGHT,CN=System Manager CA; Issuer: O=AVAYA,OU=MGHT,CN=System Manager CA; Serial Number: 6f244e9957723c04b80852fbf2ab81e946d5c0e; Signature Algorithm: SHA256withRSA; Version: 3; Valid from: January 28, 2022 9:31:13 AM EST until January 29, 2047 9:31:12 AM EST; Certificate Fingerprints (MD5 and SHA-256); Key Usage (Digital Signature, Key Cert Sign, CRL Sign); Basic Constraints (CA: true, Path Len Constraint: 2147483647). At the bottom are buttons for 'Import', 'Upload', 'Delete', and 'Help'.

**Step 2** – Select the **EP Signing Certificate** → **Certificate** tab and verify the server identity certificate, signed by the System Manager CA is present.

The screenshot shows the 'Certificates' page with the 'EP Signing Certificate' tab active. A 'Certificate Signing Request' dialog box is open, showing details for a 'Security Certificate'. The details include: Owner: C=US,ST=CO,L=Thornton,O=AVAYA,OU=SIL,CN=ep.avayalab.com; Issuer: O=AVAYA,OU=MGHT,CN=System Manager CA; Serial Number: 6668d6ac72835e5fc07ad66d9439c028dc3a190c; Signature Algorithm: SHA256withRSA; Version: 3; Valid from: March 11, 2022 12:18:26 PM EST until January 29, 2047 9:31:12 AM EST; Certificate Fingerprints (MD5 and SHA-256); Key Usage (Digital Signature, Key Cert Sign, CRL Sign); Basic Constraints (CA: true, Path Len Constraint: 2147483647); Subject Alternative Name (IP Address: 10.64.91.90). An 'Export' button is visible in the top right of the dialog.

## 7.4. VoIP Connection

This section defines a SIP trunk between Experience Portal and Session Manager.

**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.

Name	Enable	Proxy Transport	Proxy/DNS Server Address	Proxy Server Port	Listener Port	SIP Domain	Maximum Simultaneous Calls
SM10	Yes	TLS	10.64.91.85	5061	5061	avayalab.com	10

**Step 2** - Configure a SIP connection as follows:

- **Name** – Set to a descriptive name (e.g., **SM10**).
- **Enable** – Set to **Yes**.
- **Proxy Server Transport** – Set to **TLS**.
- Select **Proxy Servers**, and enter:
  - **Proxy Server Address** = **10.64.91.85** (the IP address of the Session Manager signaling interface defined in **Section 6.5**).
  - **Port** = **5061**
  - **Priority** = **0** (default)
  - **Weight** = **0** (default)
- **Listener Port** – Set to **5061**.
- **SIP Domain** – Set to **avayalab.com** (see **Section 6.2**).
- **Consultative Transfer** – Select **INVITE with REPLACES**.
- **SIP Reject Response Code** – Select **ASM (503)**.
- **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In the reference configuration a value of **10** was used.
- Select **All Calls can be either inbound or outbound**.
- **SRTP Enable** = **Yes**
- **Encryption Algorithm** = **AES\_CM\_128**
- **Authentication Algorithm** = **HMAC\_SHA1\_80**
- **RTCP Encryption Enabled** = **No**
- **RTP Authentication Enabled** = **Yes**
- 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: SM10

Enable: ☒ Yes ☐ No

Proxy Transport: **TLS** ▼

☒ Proxy Servers ☐ DNS SRV Domain

Address	Port	Priority	Weight	
10.64.91.85	5061	0	0	Remove

[Additional Proxy Server](#)

Listener Port: 5061

SIP Domain: avayalab.com

P-Asserted-Identity:

Maximum Redirection Attempts: 2

Consultative Transfer: ☒ INVITE with REPLACES ☐ REFER

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

### SIP Timers

T1: 250 milliseconds

T2: 2000 milliseconds

B and F: 4000 milliseconds

### Call Capacity

Maximum Simultaneous Calls: 10

☒ All Calls can be either inbound or outbound

☐ Configure number of inbound and outbound calls allowed

### SRTP

Enable: ☒ Yes ☐ No

Encryption Algorithm: ☒ AES\_CM\_128 ☐ NONE

Authentication Algorithm: ☒ HMAC\_SHA1\_80 ☐ HMAC\_SHA1\_32

RTCP Encryption Enabled: ☐ Yes ☒ No

RTP Authentication Enabled: ☒ Yes ☐ No

**Add**

## 7.5. Speech Servers

The installation and administration of the ASR and TTS 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.

Expand All | Collapse All

- ▶ User Management
- ▶ Real-time Monitoring
- ▶ System Maintenance
- ▶ System Management
  - ▼ System Configuration
    - Applications
    - EPM Servers
    - MPP Servers
    - SNMP
    - Speech Servers
    - VoIP Connections
    - Zones
  - ▼ Security
  - ▶ Reports
  - ▶ Multi-Media Configuration

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"/>	LVASR	Yes	10.64.101.83	Nuance	MRCP V2 TCP	5060	10	en-US

Add

Delete

Customize

Help

## 7.6. Application References

This section describes the steps for administering a reference to the VXML and/or CCXML applications residing on the application server. In the sample configuration, the applications were co-resident on one Experience Portal server, with IP Address 10.64.91.90.

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

- **Name** – Set to a descriptive name (e.g., **Test-ccxml**).
- **Enable** – Set to **Yes**. This field determines which application(s) will be executed based on their defined criteria.
- **Type** – Select **VoiceXML**, **CCXML**, or **CCXML/VoiceXML** according to the application type.
- **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 Verizon IP Trunk DID number 732-945-0232 was used. Repeat to define additional called party numbers as needed. Inbound Verizon Business calls with these called party numbers will be handled by the application defined in this section.

The screenshot shows the 'Change Application' configuration page. The left sidebar contains a navigation menu with categories like User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration. The main content area is titled 'Change Application' and includes a breadcrumb trail: 'You are here: Home > System Configuration > Applications > Change Application'. Below the title is a description: 'Use this page to change the configuration of an application.' The configuration fields include: Name (Test-ccxml), Enable (Yes/No radio buttons, Yes is selected), Type (CCXML dropdown), Reserved SIP Calls (None/Minimum/Maximum radio buttons, None is selected), Requested (empty field), URI (Single/Fail Over/Load Balance radio buttons, Single is selected), CCXML URL (http://10.64.91.90/mpp/misc/avptestapp/root.ccxml with a Verify button), Mutual Certificate Authentication (Yes/No radio buttons, No is selected), Basic Authentication (Yes/No radio buttons, No is selected), ASR Speech Servers (expandable section), TTS Speech Servers (expandable section), Application Launch (Inbound/Inbound Default/Outbound radio buttons, Inbound is selected), Called Number (Number/Number Range/URI radio buttons, Number is selected), a list of called numbers (55556, 7329450232, 8668512649) with an Add button and a Remove button, SIP Header Source (Any dropdown), Speech Parameters (expandable section), Reporting Parameters (expandable section), and Advanced Parameters (expandable section). At the bottom are Save, Apply, Cancel, and Help buttons.

## 7.7. 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

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"/>	mpp1	10.64.91.90	<Default>	<Default>	<Default>	11	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., **mpp1**) and the IP address of the MPP server in the **Host Address** field and click **Continue** (not shown).

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

Expand All | Collapse All

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

### Change MPP Server

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

Name: mpp1

Host Address: 10.64.91.90

Network Address (VoIP): <Default>

Network Address (MRCP): <Default>

Network Address (AppSvr): <Default>

Maximum Simultaneous Calls: 11

Restart Automatically: ☒ Yes ☐ No

#### MPP Certificate

Owner: C=US,O=Avaya Experience Portal,OU=EPM,CN=ep.avayalab.com  
Issuer: C=US,ST=Colorado,L=Thornton,O=AVAYA,OU=SIL,CN=ep.avayalab.com  
Serial Number: e32233254b61c27f1d381aee6e99f596  
Signature Algorithm: SHA256withRSA  
Version: 3  
Valid from: November 3, 2020 9:42:55 AM EST until November 3, 2030 9:42:55 AM EST  
Certificate Fingerprints  
MD5: b0:0b:ee:5d:e5:20:d6:62:66:5a:68:1e:53:bf:e4:f4  
SHA: 78:a6:2a:dc:9c:d6:a5:ae:78:b4:a5:63:b7:5f:f5:1a:50:cb:dc:a9  
SHA-256: 90:5b:08:e2:86:31:34:a4:d2:df:5a:67:23:34:84:cc:29:ba:32:5b:8d:9e:4f:04:b9:e9:95:9b:47:23:d2:c7  
Basic Constraints:  
CA: false  
Path Len Constraint: undefined  
Subject Alternative Names  
DNS Name: ep  
DNS Name: ep.avayalab.com  
IP Address: 10.64.91.90  
IP Address: fe80:0:0:0:20c:29ff:fe52:204

Categories and Trace Levels >

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

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

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

Expand All | Collapse All

▶ User Management  
▶ Real-time Monitoring  
▶ System Maintenance  
▶ System Management  
▼ System Configuration  
Applications  
EPM Servers  
MPP Servers  
SNMP  
Speech Servers  
VoIP Connections  
Zones  
▶ Security  
▶ Reports  
▶ Multi-Media Configuration

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

### VoIP Settings

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

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

RTCP Monitor Settings

Host Address:

Port:

VoIP Audio Formats

MPP Native Format:

- In the Codecs section set:
  - Set **Packet Time** to **20**.
  - Verify the **G729 Codec** is enabled.
  - Set **G729 Discontinuous Transmission** to **No (G.729A)**.
  - Set the **Offer Order** to the preferred codec. In the sample configuration, **G729** is the first codec, followed by **G711ulaw**, then **G711aLaw**.
- Use default values for all other fields.

**Step 5** - Click on **Save**.

Expand All | Collapse All

▶ User Management  
▶ Real-time Monitoring  
▶ System Maintenance  
▶ System Management  
▼ System Configuration  
Applications  
EPM Servers  
MPP Servers  
SNMP  
Speech Servers  
VoIP Connections  
Zones  
▶ Security  
▶ Reports  
▶ Multi-Media Configuration

Station:

RTCP Monitor Settings

Host Address:

Port:

VoIP Audio Formats

MPP Native Format:

Codecs

Offer

Enable	Codec	Order
<input checked="" type="checkbox"/>	G729	1
<input checked="" type="checkbox"/>	G711uLaw	2
<input checked="" type="checkbox"/>	G711aLaw	3

Packet Time:  milliseconds

G729 Discontinuous Transmission: ☐ Yes ☒ No

Answer

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

G729 Discontinuous Transmission: ☐ Yes ☐ No ☒ Either

G729 Reduced Complexity Encoder: ☒ Yes ☐ No

QoS Parameters

	VLAN	Diffserv
H.323:	6	46
SIP:	6	46
RTSP:	6	46

## 7.8. Configuring RFC2833 Event Value Offered by Experience Portal

For incoming calls from Verizon services to Experience Portal, Verizon specifies the value 101 for the RFC2833 telephone-events that signal DTMF digits entered by the user. When Experience Portal answers, the SDP from Experience Portal matches this Verizon 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 specifies the value 127 for the RFC2833 telephone-events. Optionally, the value that is offered by Experience Portal can be changed, and this section outlines the procedure that can be performed by an Avaya authorized representative.

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

After saving the file with the change, restart the MPP server for the change to take effect. As shown below, the MPP may be restarted using the **Restart** button available via the Experience Portal GUI at **System Management → MPP Manager**. Note that the **State** column shows when the MPP is running after the restart.

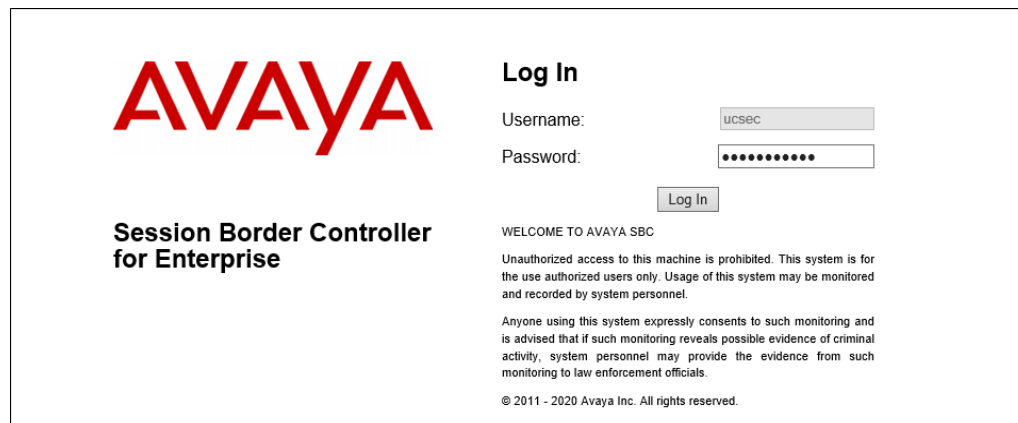
The screenshot shows the 'MPP Manager' interface in the Experience Portal. The left sidebar contains a navigation menu with categories like User Management, Real-time Monitoring, System Maintenance, System Configuration, Security, Reports, and Multi-Media Configuration. The main content area is titled 'MPP Manager (Sep 9, 2022 1:28:21 PM EDT)' and includes a 'Refresh' button. Below the title, a message states: '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.' A table displays the status of MPPs, with a 'Last Poll' timestamp of 'Sep 9, 2022 1:28:02 PM EDT'. The table has columns for Server Name, Mode, State, Config, Auto Restart, Restart Schedule (Today, Recurring), and Active Calls (In, Out). One MPP, 'mpp1', is listed with a checked checkbox, 'Online' mode, 'Running' state, 'OK' config, 'Yes' auto restart, 'No' today restart, 'None' recurring restart, 0 in-calls, and 0 out-calls. Below the table, there are sections for 'State Commands' (Start, Stop, Restart, Reboot, Halt, Cancel) and 'Mode Commands' (Offline, Test, Online). A 'Restart/Reboot Options' section allows selecting 'One server at a time' (selected) or 'All servers'. A 'Help' button is located at the bottom left.

Server Name	Mode	State	Config	Auto Restart	Restart Schedule	Active Calls		
					Today	Recurring	In	Out
<input checked="" type="checkbox"/> mpp1	Online	Running	OK	Yes	No	None	0	0

## 8. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the initial provisioning of the Avaya SBCE, including 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 provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

Use a WEB browser to access the Element Management Server (EMS) web interface, and enter `https://ipaddress/sbc` in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBCE. Log in using the appropriate credentials.



The screenshot displays the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is shown in red, with the text "Session Border Controller for Enterprise" below it. On the right, under the heading "Log In", there are input fields for "Username:" (containing "UCSEC") and "Password:" (masked with dots). A "Log In" button is positioned below the password field. Below the login fields, a "WELCOME TO AVAYA SBC" message is displayed, followed by a disclaimer: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." 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.

The EMS Dashboard page of the Avaya SBCE will appear. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

**Note** – The provisioning described in the following sections use the menu options listed in the left-hand column shown below.

The screenshot shows the Avaya Session Border Controller for Enterprise EMS Dashboard. The top navigation bar includes links for Device: EMS, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo. The left sidebar lists the EMS Dashboard and various management options. The main content area is titled "Dashboard" and contains several sections:

- Information:** A table showing system details.
 

System Time	09:23:39 AM EDT	<a href="#">Refresh</a>
Version	10.1.0.0-32-21432	
GUI Version	10.1.0.0-21910	
Build Date	Thu May 12 08:11:45 UTC 2022	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	09/12/2022 09:22:36 EDT	
Failed Login Attempts	0	
- Installed Devices:** A table showing the installed device.
 

EMS
SBCE10-90
- Active Alarms (past 24 hours):** A section showing "None found."
- Incidents (past 24 hours):** A section showing "None found."
- Notes:** A section showing "No notes found."

## 8.1. Device Management – Status

Select **Device Management** on the left-hand menu. A list of installed devices is shown on the **Devices** tab on the right pane. In the case of the sample configuration, a single device named **SBCE10-90** is shown. Verify that the **Status** column shows **Commissioned**. If not, contact your Avaya representative. To view the configuration of this device, click **View** on the screen below.

**Note** – Certain Avaya SBCE configuration changes require that the underlying application be restarted. To do so, click on **Restart Application** shown below.

The screenshot shows the Avaya Session Border Controller for Enterprise EMS Dashboard with the **Device Management** section selected. The left sidebar lists the EMS Dashboard and various management options. The main content area is titled "Device Management" and contains several tabs: **Devices**, **Updates**, **Licensing**, and **Key Bundles**. The **Devices** tab is selected, showing a table of installed devices:

Device Name	Management IP	Version	Status	Reboot	Shutdown	Restart Application	View	Edit	Uninstall
SBCE10-90	10.64.90.90	10.1.0.0-32-21432	Commissioned						



The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation, corresponding to **Figure 1**. In the shared test environment, the highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to Verizon. Other IP addresses assigned to interfaces **A1** and **B2** on the screen below are used to support remote workers and are not the focus of these Application Notes. Note that the **Management IP** must be on a separate subnet from the IP interfaces designated for SIP traffic.

System Information: SBCE10-90

General Configuration

Appliance Name SBCE10-90  
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	10	100
Advanced Sessions	10	100
Scopia Video Sessions	10	100
CES Sessions	10	100
Transcoding Sessions	10	100
AMR	<input checked="" type="checkbox"/>	
Premium Sessions	10	100
CLID	---	
Encryption	<input checked="" type="checkbox"/>	
Available:	Yes	

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.91.48	10.64.91.48	255.255.255.0	10.64.91.1	A1
10.64.91.49	10.64.91.49	255.255.255.0	10.64.91.1	A1
10.64.91.50	10.64.91.50	255.255.255.0	10.64.91.1	A1
1.1.1.2	1.1.1.2	255.255.255.0	1.1.1.1	B1
10.127.0.10	10.127.0.10	255.255.255.0	10.127.0.1	B2
10.127.0.11	10.127.0.11	255.255.255.0	10.127.0.1	B2
10.127.0.12	10.127.0.12	255.255.255.0	10.127.0.1	B2

DNS Configuration

Primary DNS 10.64.19.185  
Secondary DNS 172.30.209.4  
DNS Location DMZ  
DNS Client IP 1.1.1.2

Management IP(s)

IP #1 (IPv4) 10.64.90.90

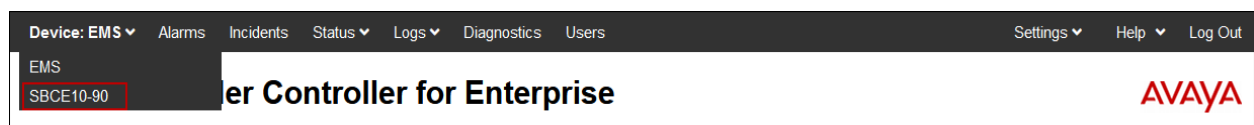
## 8.2. TLS Management

**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.

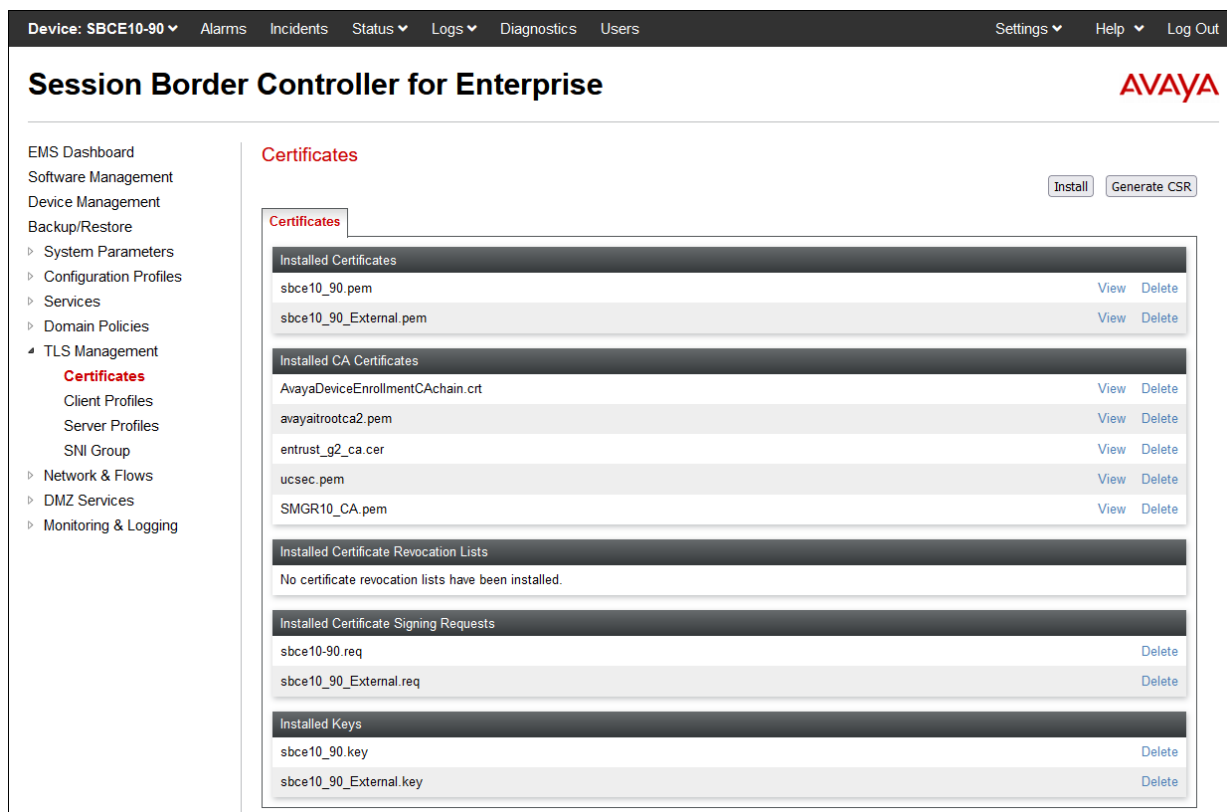
### 8.2.1 Verify TLS Certificates – Avaya Session Border Controller for Enterprise

To access the SBCE configuration menus, select the SBCE device from the top navigation menu.



**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.



## 8.2.2 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., **sbce10\_90.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:

Certificate:

SNI Options:

SNI Group:

**Certificate Verification**

Peer Verification:

Peer Certificate Authorities:

Peer Certificate Revocation Lists:

Verification Depth:

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

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

Server Profiles: Inside\_Server

Add

Delete

Server Profiles

Inside\_Server

Outside\_Server

Click here to add a description.

Server Profile

TLS Profile

Profile Name

Inside\_Server

Certificate

sbce10\_90.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

Edit

MAA; Reviewed:  
SPOC 10/14/2022

Solution & Interoperability Test Lab Application Notes  
©2022 Avaya Inc. All Rights Reserved.

84 of 124  
Aura101EP81VzIP

### 8.2.3 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., **sbce10\_90.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., **SMGR10\_CA.pem**.
- **Verification Depth:** enter **1**.
- 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:

Certificate:

SNI: ☐ Enabled

**Certificate Verification**

Peer Verification: Required

Peer Certificate Authorities:

Peer Certificate Revocation Lists:

Verification Depth:

Extended Hostname Verification: ☐

Server Hostname:

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

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

Client Profiles: Inside\_Client

AddDelete

Client Profiles  
Inside\_Client  
Outside\_Client

Click here to add a description.

Client Profile

TLS Profile

Profile Name

Inside\_Client

Certificate

sbce10\_90.pem

SNI

☐ Enabled

Certificate Verification

Peer Verification

Required

Peer Certificate Authorities

SMGR10\_CA.pem

Peer Certificate Revocation Lists

---

Verification Depth

1

Extended Hostname Verification

☐

Renegotiation Parameters

Renegotiation Time

0

Renegotiation Byte Count

0

Handshake Options

Version

☒ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0

Ciphers

☒ Default ☐ FIPS ☐ Custom

Value

HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

### 8.3. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

**Step 1** - Select **Networks & Flows** → **Network Management** from the menu on the left-hand side.

**Step 2** - The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 and B1 are used.

The screenshot shows the 'Session Border Controller for Enterprise' interface with the 'Network Management' section active. The 'Interfaces' tab is selected, displaying a table of network interfaces. The table has three columns: 'Interface Name', 'VLAN Tag', and 'Status'. The interfaces listed are A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Enabled). There is an 'Add VLAN' button in the top right corner of the table area.

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

**Step 3** - Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however, some of these values may not be changed if associated provisioning is in use.

- **A1: 10.64.91.50** – “Inside” IP address, toward Session Manager.
- **B1: 1.1.1.2** – “Outside” IP address toward the Verizon SIP trunk. This address is known to Verizon.

The screenshot shows the 'Session Border Controller for Enterprise' interface with the 'Network Management' section active. The 'Networks' tab is selected, displaying a table of network configurations. The table has five columns: 'Name', 'Gateway', 'Subnet Mask / Prefix Length', 'Interface', and 'IP Address'. The configurations listed are 'Inside A1', 'Verizon B1', and 'Public B2'. Each row has 'Edit' and 'Delete' buttons. There is an 'Add' button in the top right corner of the table area.

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Inside A1	10.64.91.1	255.255.255.0	A1	10.64.91.48, 10.64.91.49, 10.64.91.50	Edit Delete
Verizon B1	1.1.1.1	255.255.255.0	B1	1.1.1.2	Edit Delete
Public B2		255.255.255.128	B2		Edit Delete

## 8.4. Media Interfaces

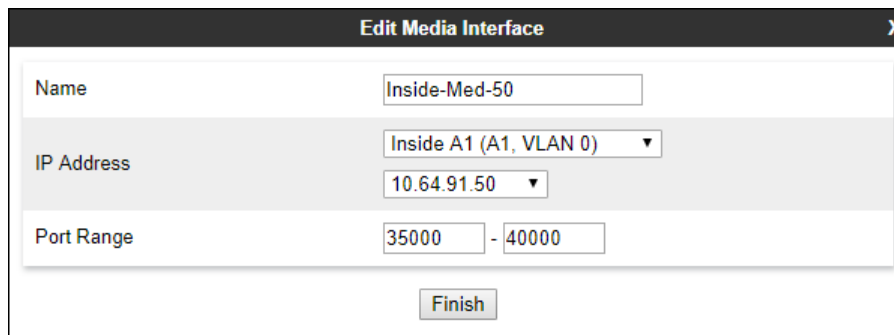
Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which the SBCE will accept media from the connected server. Create a SIP Media Interface for both the inside and outside IP interfaces.

**Step 1** - Select **Network & Flows** → **Media Interface** from the menu on the left-hand side.

**Step 2** - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name:** Enter an appropriate name (e.g., **Inside-Med-50**).
- **IP Address:** Select **Inside-A1 (A1,VLAN0)** and **10.64.91.50** from the drop-down menus.
- **Port Range:** **35000 – 40000**.

**Step 3** - Click **Finish**.



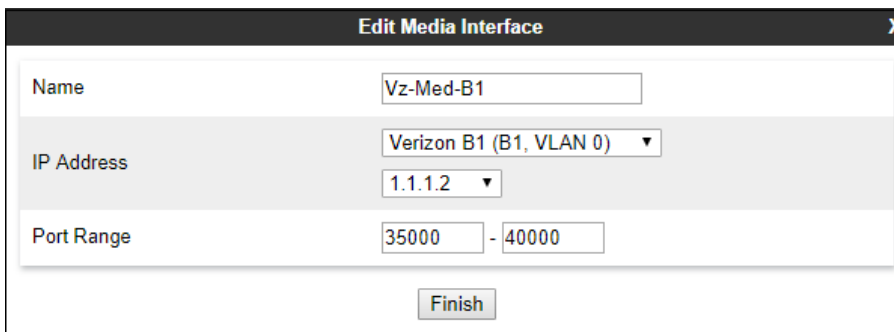
The screenshot shows the 'Edit Media Interface' window with the following configuration:

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

**Step 4** - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name:** Enter an appropriate name (e.g., **Vz-Med-B1**).
- **IP Address:** Select **Verizon-B1 (B1,VLAN0)** and **1.1.1.2** from the drop-down menus.
- **Port Range:** **35000 – 40000**.

**Step 5** - Click **Finish**.



The screenshot shows the 'Edit Media Interface' window with the following configuration:

Edit Media Interface	
Name	Vz-Med-B1
IP Address	Verizon B1 (B1, VLAN 0) 1.1.1.2
Port Range	35000 - 40000
Finish	



## 8.5. Signaling Interfaces

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces.

**Step 1** - Select **Network & Flows** → **Signaling Interface** from the menu on the left-hand side.

**Step 2** - Select **Add** (not shown) and enter the following:

- **Name:** Enter an appropriate name (e.g., **Inside-Sig-50**).
- **IP Address:** Select **Inside A1 (A1,VLAN0)** and **10.64.91.50**.
- **TLS Port:** **5061**.
- **TLS Profile:** Select the TLS server profile created in **Section 8.2.2** (e.g., **Inside\_Server**)

**Step 3** - Click **Finish**.

The screenshot shows the 'Edit Signaling Interface' dialog box with the following configuration:

Field	Value
Name	Inside-Sig-50
IP Address	Inside A1 (A1, VLAN 0) (10.64.91.50)
TCP Port	(Leave blank to disable)
UDP Port	(Leave blank to disable)
TLS Port	5061
TLS Profile	Inside_Server
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	(Leave blank)

Finish

**Step 4** - Select **Add** (not shown), and enter the following:

- **Name:** Enter an appropriate name (e.g., **Vz-Sig-B1**).
- **IP Address:** Select **Verizon B1 (B1,VLAN0)** and **1.1.1.2**.
- **UDP Port:** **5060**.

**Step 5** - Click **Finish**.

The screenshot shows the 'Edit Signaling Interface' dialog box with the following configuration:

Field	Value
Name	Vz-Sig-B1
IP Address	Verizon B1 (B1, VLAN 0) (1.1.1.2)
TCP Port	(Leave blank to disable)
UDP Port	5060
TLS Port	(Leave blank to disable)
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	(Leave blank)

Finish

## 8.6. Server Interworking Profiles

The Server Interworking Profile includes parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below. Create separate Server Interworking Profiles for the enterprise and the service provider.

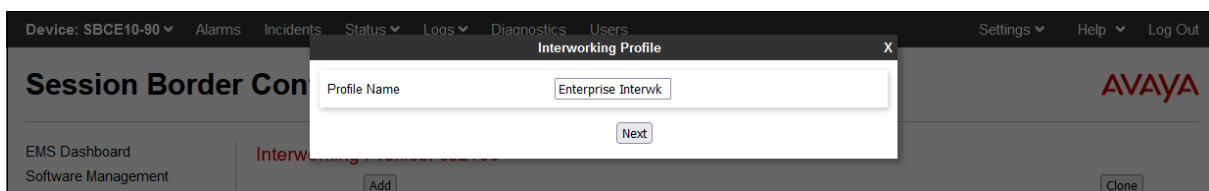
### 8.6.1 Server Interworking Profile – Enterprise

In the sample configuration, the enterprise Server Interworking profile was cloned from the default **avaya-ru** profile and then modified.

**Step 1** - Select **Configuration Profiles → Server Interworking** from the left-hand menu.

**Step 2** - Select the pre-defined **avaya-ru** profile and click the **Clone** button.

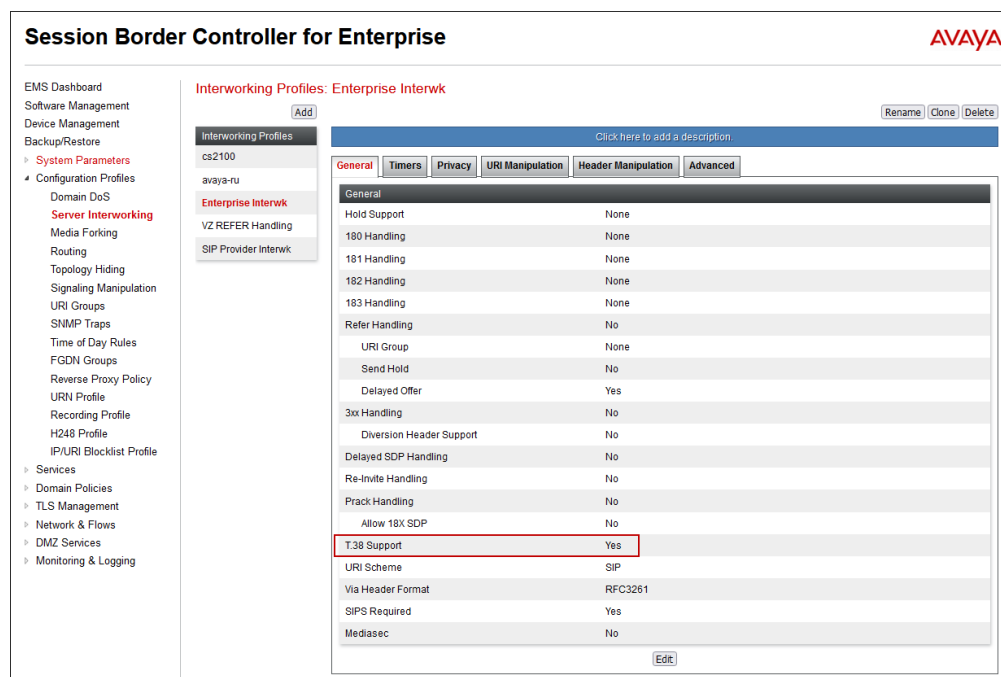
**Step 3** - Enter profile name: (e.g., **Enterprise Interwk**), and click **Finish** to continue.



**Step 4** - The new Enterprise Interwork profile will be listed. Select it, scroll to the bottom of the Profile screen, and click on **Edit**.

**Step 5** - The **General** screen will open.

- Check **T38 Support**.
- All other options can be left with default values. Click **Finish** (not shown).



## 8.6.2 Server Interworking Profile – Verizon

In the sample configuration, the Server Interworking profile for Verizon was created by adding a new profile.

**Note** – See **Section 13** for additional steps necessary for Experience Portal to redirect calls to Communication Manager using SIP REFER.

**Step 1** - Select **Add Profile** and enter a profile name: (e.g., **SIP Provider Interwk**) and click **Next** (not shown).

**Step 2** - The **General** screen will open (not shown):

- Check **T38 Support**.
- All other options can be left as default.
- Click **Next**.

**Step 3** - The **SIP Timers** and **Privacy** screens will open (not shown), accept default values for these screens by clicking **Next**.

**Step 4** - The **Advanced/DTMF** screen will open:

- In the **Record Routes** field, check **Both Sides**.
- All other options can be left as default.
- Click **Finish** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The left sidebar shows the navigation menu with 'Server Interworking' highlighted. The main content area shows the 'Interworking Profiles: SIP Provider Interwk' configuration page. The 'Advanced' tab is selected, showing the following settings:

Field	Value
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

Below the main settings, the 'DTMF' section is visible, showing 'DTMF Support' set to 'None'. An 'Edit' button is located at the bottom right of the configuration area.

## 8.7. Signaling Manipulation

Signaling Manipulations are SigMa scripts the Avaya SBCE can use to manipulate SIP headers/messages. In the reference configuration, one signaling manipulation script is used.

**Note** – Use of the Signaling Manipulation scripts require higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should only be used in cases where the use of Server Interworking Profiles (**Section 8.6**) or Signaling Rules (**Section 8.13**) does not meet the desired result. Refer to Additional References [11] for information on the Avaya SBCE scripting language.

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.

A Sigma script was created during the compliance test to correct the following interoperability issues:


- Remove the “epv” parameter from the outbound Contact header. See **Section 2.4**
- Remove unwanted XML information in UPDATES from being sent to Verizon.
- 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 Verizon. See **Section 2.2**

The details of the script appear on **Section 14**.

**Step 1** - Select **Configuration Profiles → Signaling Manipulation** from the menu on the left.

**Step 2** - Click **Add Script** (not shown) and the script editor window will open.

- Enter a name for the script in the **Title** box (e.g., **Vz IPT Script for EP**).
- Copy and paste the script from **Section 14**.



```
1 within session "ALL"
2 {
3     act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
4     {
5
6         //Remove epv parameter from Contact header to hide internal topology
7         remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
8
9         //Remove unwanted xml information
10        remove(%BODY[1]);
11    }
12 }
13
14 // OPTIONAL Experience Portal - modify PAI Header
15 within session "INVITE"
16 {
17     act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
18     {
19         if (%INITIAL_REQUEST = "true") then
20         {
21             if (%HEADERS["User-Agent"][1].regex_match("Avaya\\-VoicePortal")) then
22             {
23                 %HEADERS["P-Asserted-Identity"][1].URI.USER = "7329450232";
24             }
25         }
26     }
27 }
28 }
29 }
```

**Step 3** - Click on **Save**. The script editor will test for any errors, and the window will close. This script will later be applied to the Verizon Server Configuration profile in **Section 8.8.2**.

## 8.8. SIP Server Profiles

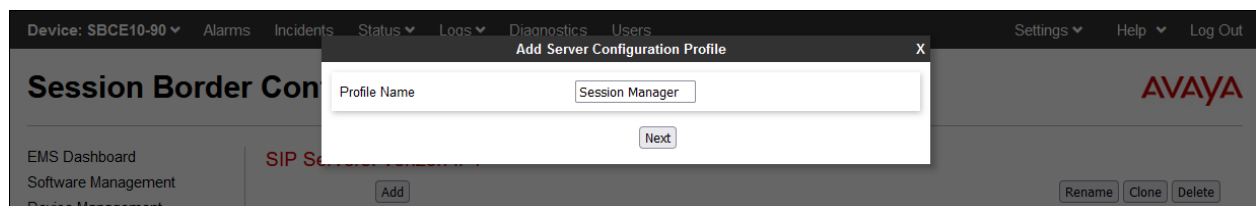
The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

### 8.8.1 SIP Server Profile – Session Manager

This section defines the SIP Server Profile for the Avaya SBCE connection to Session Manager.

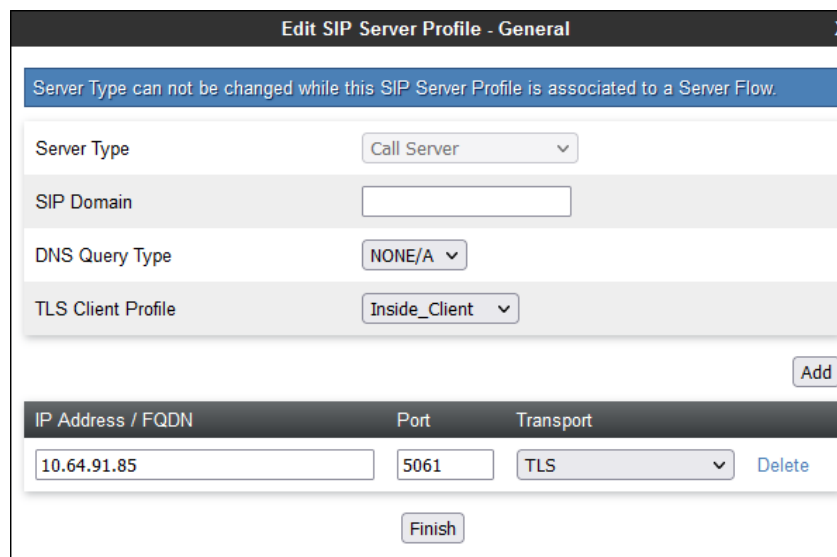
**Step 1** - Select **Services** → **SIP Servers** from the left-hand menu.

**Step 2** - Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **Session Manager**) and click **Next**.

The screenshot shows the 'Add Server Configuration Profile' dialog box. It has a title bar with 'Add Server Configuration Profile' and a close button. Inside, there is a text input field labeled 'Profile Name' containing the text 'Session Manager'. Below the input field is a 'Next' button. The background shows the Avaya Session Border Controller interface with a sidebar menu and a top navigation bar.

**Step 3** - The **Add Server Configuration Profile** window will open.

- Select **Server Type**: **Call Server**.
- **SIP Domain**: Leave blank (default).
- **DNS Query Type**: Select **NONE/A** (default).
- **TLS Client Profile**: Select the profile create in **Section 8.2.3** (e.g., **Inside\_Client**).
- **IP Address**: **10.64.91.85** (Session Manager Security Module IP address).
- Select **Port**: **5061**, **Transport**: **TLS**.
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish** and proceed to the next tab.

The screenshot shows the 'Edit SIP Server Profile - General' window. It has a title bar with 'Edit SIP Server Profile - General' and a close button. Below the title bar is a blue banner with the text 'Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.' The main area contains several configuration fields: 'Server Type' (Call Server), 'SIP Domain' (empty), 'DNS Query Type' (NONE/A), and 'TLS Client Profile' (Inside\_Client). Below these fields is an 'Add' button. At the bottom, there is a table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'. The table contains one row with the values '10.64.91.85', '5061', and 'TLS'. To the right of the table is a 'Delete' button. At the very bottom is a 'Finish' button.

**Step 4** – Default values can be used on the **Authentication** tab.

**Step 5** – On the **Heartbeat** tab, check the **Enable Heartbeat** box to have the Avaya SBCE source “heartbeats” toward Session Manager. This configuration is optional.

- Select **OPTIONS** from the **Method** drop-down menu.
- Select the desired frequency that the SBCE will source OPTIONS toward Session Manager.
- Make logical entries in the **From URI** and **To URI** fields that will be used in the OPTIONS headers.

The screenshot shows the 'Edit SIP Server Profile - Heartbeat' dialog box. It has a title bar with 'Edit SIP Server Profile - Heartbeat' and a close button 'X'. The dialog contains the following fields:

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS ▼
Frequency	120 seconds
From URI	SBC@avayalab.com
To URI	SM@avayalab.com

At the bottom right, there is a 'Finish' button.

**Step 6** – Default values are used on the **Registration** and **Ping** tabs.

**Step 7** – On the **Advanced** tab:

- Select the **Enterprise Interwk** (created in **Section 8.6**), for **Interworking Profile**.
- Since TLS transport is specified in **Step 3**, then the **Enable Grooming** option should be enabled.
- In the **Signaling Manipulation Script** field select **none**.
- Select **Finish**.

The screenshot shows the 'Edit SIP Server Profile - Advanced' dialog box. It has a title bar with 'Edit SIP Server Profile - Advanced' and a close button 'X'. The dialog contains the following fields:

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

At the bottom right, there is a 'Finish' button.

## 8.8.2 SIP Server Profile – Verizon

Repeat the steps in **Section 8.8.1**, with the following changes, to create a SIP Server Profile for the Avaya SBCE connection to Verizon.

**Step 1** - Select **Add** and enter a Profile Name (e.g., **Verizon IPT**) and select **Next** (not shown).

**Step 2** - On the **General** window, enter the following:

- **Server Type:** Select **Trunk Server**.
- **IP Address:** **172.30.209.21** (Verizon-provided IP address).
- Select **Port:** **5071**, **Transport:** **UDP**, as specified by Verizon.
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish** and proceed to the next tab.

IP Address / FQDN	Port	Transport
172.30.209.21	5071	UDP

**Step 4** – Default values are used on the **Authentication** tab.

**Step 5** – On the **Heartbeat** tab, check the **Enable Heartbeat** box to optionally have the Avaya SBCE source “heartbeats” toward Verizon. The screen below shows the values used in the reference configuration.

Method	OPTIONS
Frequency	60 seconds
From URI	SBC1@adec.avaya.globalipcom.com
To URI	Vz@pcelban0001.avayalincroft.globalipcom.com

**Step 6** – Default values are used on the **Registration** and **Ping** tabs.

**Step 7** – On the **Advanced** window, enter the following:

- **Enable Grooming** is not used for UDP connections and is left unchecked.
- Select the **SIP Provider Interwk** (created in **Section 8.6.2**), for **Interworking Profile**.
- Select the **Vz IPT Script for EP** (created in **Section 8.7**) for **Signaling Manipulation Script**.
- Select **Finish**.

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

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

Finish



## 8.9. Routing Profiles

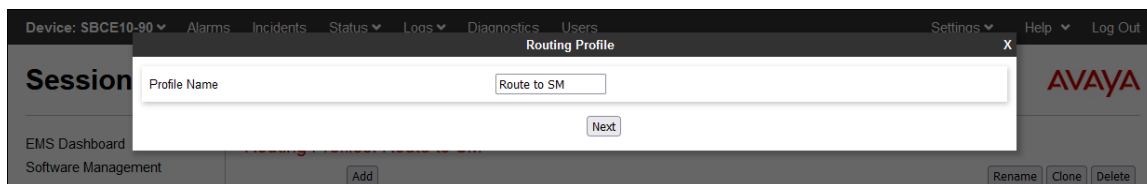
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types. Separate Routing Profiles were created in the reference configuration for Session Manager and Verizon.

### 8.9.1 Routing Profile – Session Manager

This provisioning defines the Routing Profile for the connection to Session Manager.

**Step 1** - Select **Configuration Profiles → Routing** from the left-hand menu, and select **Add**.

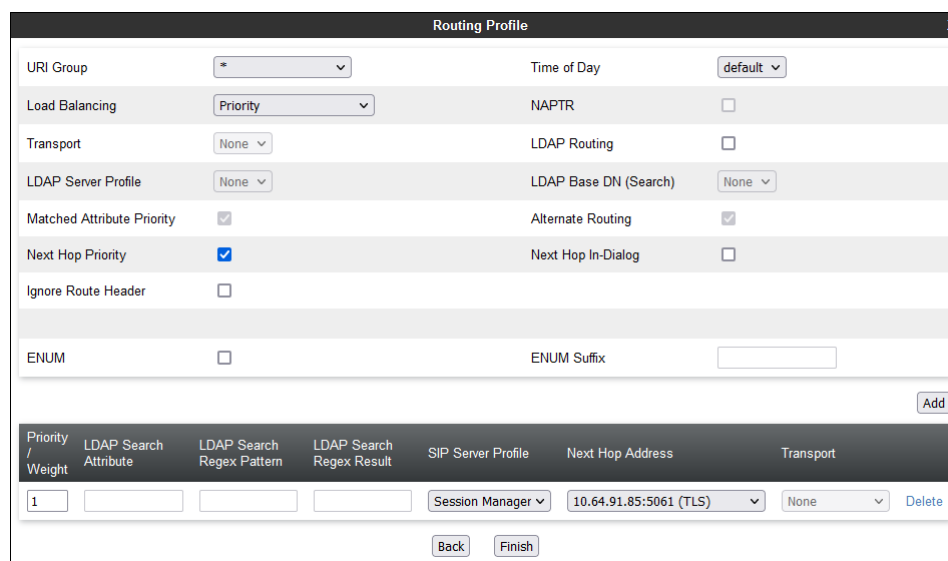
**Step 2** - Enter a **Profile Name**: (e.g., **Route to SM**) and click **Next**.

The screenshot shows a web interface for configuring a Routing Profile. At the top, there's a navigation bar with 'Device: SBCE10-90' and various menu items like 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. Below this, a 'Routing Profile' window is open. It has a 'Profile Name' field containing 'Route to SM' and a 'Next' button. The background shows a sidebar with 'Session Manager' selected and an 'Add' button at the bottom.

**Step 3** - The Routing Profile window will open. The parameters in the top portion of the profile are left at their default settings. Click the **Add** button.

**Step 4** - The **Next-Hop Address** section will open at the bottom of the profile. Populate the following fields:

- **Priority/Weight** = 1
- **SIP Server Profile** = **Session Manager** (from **Section 8.8.1**).
- **Next Hop Address**: Verify that the **10.64.91.85:5061 (TLS)** entry from the drop-down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out. Click on **Finish**.

The screenshot shows the 'Routing Profile' configuration window. It has a title bar with 'Routing Profile' and a close button. The main area is divided into two columns. The left column contains: 'URI Group' (set to '\*'), 'Load Balancing' (set to 'Priority'), 'Transport' (set to 'None'), 'LDAP Server Profile' (set to 'None'), 'Matched Attribute Priority' (checked), 'Next Hop Priority' (checked), 'Ignore Route Header' (unchecked), 'ENUM' (unchecked), and 'ENUM Suffix' (empty). The right column contains: 'Time of Day' (set to 'default'), 'NAPTR' (unchecked), 'LDAP Routing' (unchecked), 'LDAP Base DN (Search)' (set to 'None'), 'Alternate Routing' (checked), 'Next Hop In-Dialog' (unchecked). Below these fields is an 'Add' button. At the bottom, there's a table with columns: 'Priority / Weight', 'LDAP Search Attribute', 'LDAP Search Regex Pattern', 'LDAP Search Regex Result', 'SIP Server Profile', 'Next Hop Address', and 'Transport'. The first row has values: '1', empty, empty, empty, 'Session Manager', '10.64.91.85:5061 (TLS)', and 'None'. Below the table are 'Back' and 'Finish' buttons.

## 8.9.2 Routing Profile – Verizon

Repeat the steps in **Section 8.9.1**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to Verizon.

**Step 1** - On the **Configuration Profiles → Routing** screen, select **Add** and enter a **Profile Name**:  
(e.g., **route to VZ IPT**).

**Step 2** - On the **Next-Hop Address** window, populate the following fields:

- **Priority/Weight = 1**
- **SIP Server Profile = Verizon IPT** (from **Section 8.8.2**).
- **Next Hop Address:** Verify that **172.30.209.21:5071 (UDP)** is selected.

**Step 3** - Click **Finish**.

The screenshot shows the 'Routing Profile' configuration window. The 'URI Group' is set to '\*' and 'Time of Day' is 'default'. 'Load Balancing' is 'Priority', 'NAPTR' is unchecked, 'Transport' is 'None', and 'LDAP Server Profile' is 'None'. 'LDAP Base DN (Search)' is 'None'. 'Matched Attribute Priority' and 'Alternate Routing' are checked. 'Next Hop Priority' is checked, and 'Ignore Route Header' is unchecked. 'ENUM' is unchecked and 'ENUM Suffix' is empty. An 'Add' button is at the bottom right. Below is a table with columns: Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, and Transport. The first row has values: 1, empty, empty, empty, Verizon IPT, 172.30.209.21:5071 (UDP), and None. A 'Delete' link is at the end of the row. 'Back' and 'Finish' buttons are at the bottom.

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

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Verizon IPT	172.30.209.21:5071 (UDP)	None	Delete

## 8.10. Topology Hiding Profiles

The **Topology Hiding** profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the security of the network. It hides the topology of the enterprise network from external networks.

Topology Hiding can also be used as an interoperability tool to adapt the host portion of the SIP headers, to the IP addresses or domains expected on the service provider and the enterprise networks.

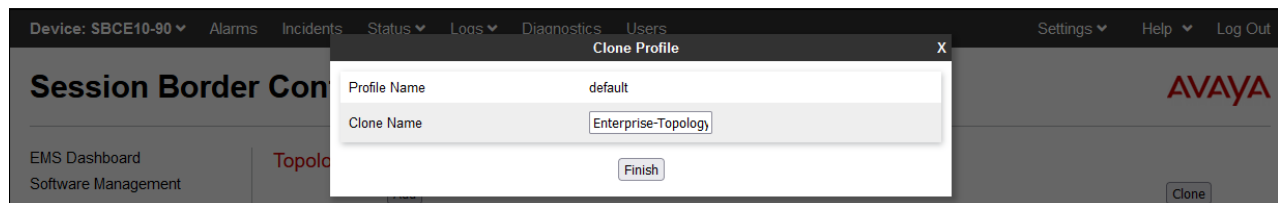
### 8.10.1 Topology Hiding – Enterprise

In the sample configuration, the enterprise Topology Hiding Profile was cloned from the **default** profile and then modified.

**Step 1** - Select **Configuration Profiles → Topology Hiding** from the left-hand menu.

**Step 2** - Select the pre-defined **default** profile and click the **Clone** button.

**Step 3** - Enter profile name: (e.g., **Enterprise-Topology**), and click **Finish** to continue.



**Step 4** - Edit the newly created **Enterprise-Topology** profile.

**Step 5** - For the **Request-Line**, **To** and **From** headers select **Overwrite** under the **Replace Action** column. Enter the domain of the enterprise (e.g., **avayalab.com**) on the **Overwrite Value** field.

**Step 6** - Click **Finish**.

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

Finish

## 8.10.2 Topology Hiding – Verizon

Repeat the steps in **Section 8.10.1**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to Verizon.

- Enter a Profile Name (e.g., **VZ IPT Topology**).
- Overwrite the headers as shown below with the FQDNs known by Verizon.

**Topology Hiding Profiles: VZ IPT Topology**

Add

RenameCloneDelete

Topology Hiding Profiles

default

cisco\_th\_profile

IPOSE-Topology

Vz IPCC Topology

Enterprise-Topology

VZ IPT Topology

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
Referred-By	IP/Domain	Overwrite	adevc.avaya.globalipcom.com
Refer-To	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com
From	IP/Domain	Overwrite	adevc.avaya.globalipcom.com
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com

Edit

## 8.11. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, you can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

**Step 1** - Select **Domain Policies** → **Application Rules** from the left-hand side menu.

**Step 2** - Click the **Add** button to add a new profile, or select an existing topology hiding profile to edit. In the reference configuration, the Application Rule named **sip-trunk** was created for both the enterprise and Verizon. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Audio** application to a value slightly larger than the licensed sessions. For example, if licensed for 150 sessions set the values to **200**. The **Maximum Session Per Endpoint** was set to **10**.

**Step 3** - Click **Finish** (not shown). The completed **Application Rule** is shown below.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left-hand navigation menu includes 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', and 'Domain Policies'. Under 'Domain Policies', 'Application Rules' is selected and highlighted in red. The main content area is titled 'Application Rules: sip-trunk' and features an 'Add' button, a 'Click here to add a description' link, and 'Rename', 'Clone', and 'Delete' buttons. A table lists the configured applications:

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	10
Video	<input type="checkbox"/>	<input type="checkbox"/>		

Below the table, a 'Miscellaneous' section contains two settings: 'CDR Support' set to 'Off' and 'RTCP Keep-Alive' set to 'No'. An 'Edit' button is located at the bottom right of the configuration area.

## 8.12. Media Rules

Media Rules define packet parameters for the RTP media, such as encryption techniques and QoS settings. Separate media rules are created for Verizon and Session Manager.

### 8.12.1 Enterprise – Media Rule

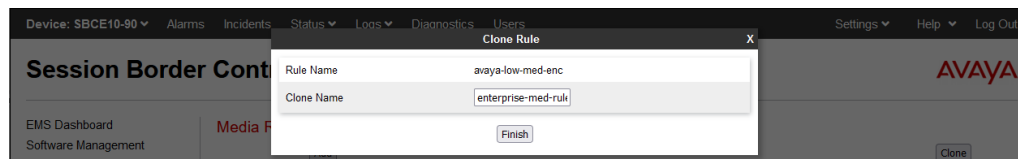
In the sample configuration, the default Media Rule **avaya-low-med-enc** was cloned to create the enterprise Media Rule, and modified as shown below:

**Step 1** - Select **Domain Policies** → **Media Rules** from the left-hand side menu (not shown).

**Step 2** - From the Media Rules menu, select the **avaya-low-med-enc** rule.

**Step 3** - Select **Clone** button, and the **Clone Rule** window will open.

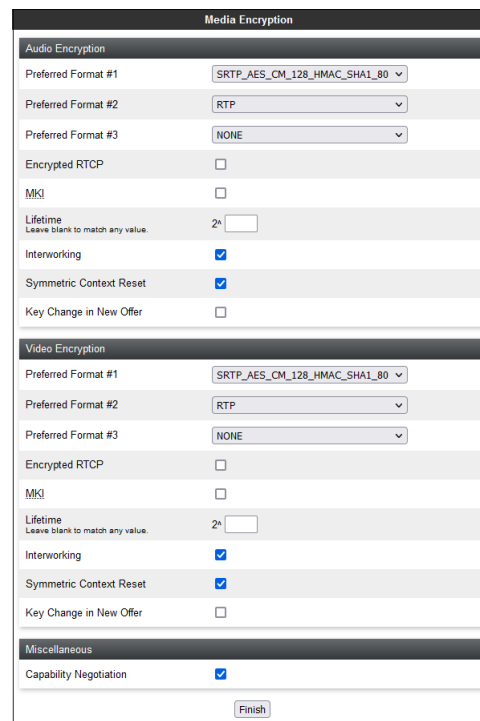
- In the **Clone Name** field enter the new Media Rule name (e.g., **enterprise-med-rule**)
- Click **Finish**. The newly created rule will be displayed.



**Step 4** - On the **enterprise med rule** just created, select the **Encryption** tab.

- Click the **Edit** button and the **Media Encryption** window will open.
- In the **Audio Encryption** section, select **RTP** for **Preferred Format #2**.
- In the **Video Encryption** section, select **RTP** for **Preferred Format #2**.
- In the **Miscellaneous** section, select **Capability Negotiation**.

**Step 5** - Click **Finish**.



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

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

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

The completed **enterprise-med-rule** is shown on the screen below.

**Media Rules: enterprise-med-rule**

Add

RenameCloneDelete

Click here to add a description.

Media Rules

default-low-med

default-low-med-enc

default-high

default-high-enc

avaya-low-med-enc

**enterprise-med-rule**

rw-med-rule

Vz-trk-med-rule

Encryption

Codec Prioritization

Advanced

QoS

Audio Encryption

Preferred Formats

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

RTP

Encrypted RTCP

☐

MKI

☐

Lifetime

Any

Interworking

☒

Symmetric Context Reset

☒

Key Change in New Offer

☐

Video Encryption

Preferred Formats

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

RTP

Encrypted RTCP

☐

MKI

☐

Lifetime

Any

Interworking

☒

Symmetric Context Reset

☒

Key Change in New Offer

☐

Miscellaneous

Capability Negotiation

☒

Edit

## 8.12.2 Verizon – Media Rule

Repeat the steps in **Section 8.12.1**, with the following changes, to create a Media Rule for Verizon.

1. Clone the **default-low-med** profile.
2. In the **Clone Name** field enter the new Media Rule name (e.g., **Vz-trk-med-rule**).

The completed **Vz-trk-med-rule** is shown on the screen below.

The screenshot shows the 'Media Rules: Vz-trk-med-rule' configuration page. On the left is a sidebar with a list of media rules: default-low-med, default-low-med-enc, default-high, default-high-enc, avaya-low-med-enc, enterprise-med-rule, nw-med-rule, and Vz-trk-med-rule (highlighted in red). The main area has tabs for Encryption, Codec Prioritization, Advanced, and QoS. The 'Encryption' tab is active, showing settings for Audio Encryption and Video Encryption. Both sections have 'Preferred Formats' set to RTP, 'Interworking' checked, 'Symmetric Context Reset' checked, and 'Key Change in New Offer' unchecked. A 'Miscellaneous' section at the bottom has 'Capability Negotiation' unchecked. Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

Media Rules	Encryption	Codec Prioritization	Advanced	QoS
default-low-med				
default-low-med-enc				
default-high				
default-high-enc				
avaya-low-med-enc				
enterprise-med-rule				
nw-med-rule				
<b>Vz-trk-med-rule</b>				

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

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

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

DSCP default value **EF** for expedited forwarding (as specified by Verizon) is used for Media **QoS**.

The screenshot shows the 'Media Rules: Vz-trk-med-rule' configuration page with the 'QoS' tab active. It displays settings for Media QoS Marking, Audio QoS, and Video QoS. 'Media QoS Marking' is enabled with 'QoS Type' set to DSCP. 'Audio QoS' and 'Video QoS' both have 'DSCP' set to EF. The sidebar and other UI elements are consistent with the previous screenshot.

Media Rules	Encryption	Codec Prioritization	Advanced	QoS
default-low-med				
default-low-med-enc				
default-high				
default-high-enc				
avaya-low-med-enc				
enterprise-med-rule				
nw-med-rule				
<b>Vz-trk-med-rule</b>				

Media QoS Marking	
Enabled	<input checked="" type="checkbox"/>
QoS Type	DSCP

Audio QoS	
Audio DSCP	EF

Video QoS	
Video DSCP	EF



## 8.13. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. In the reference configuration, Signaling Rules are used to define QoS parameters for the SIP signaling packets.

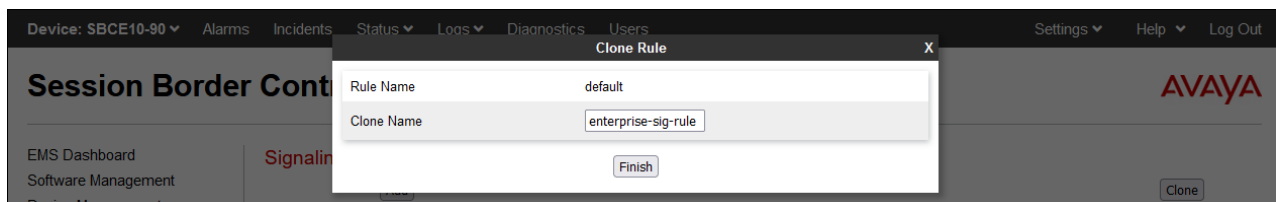
### 8.13.1 Signaling Rule – Enterprise

**Step 1** - Select **Domain Policies** → **Signaling Rules** from the left-hand side menu (not shown).

**Step 2** - From the Signaling Rules menu, select the **default** rule.

**Step 3** - Select the **Clone** button and the **Clone Rule** window will open.

- In the **Rule Name** field enter the new Signaling Rule name (e.g., **enterprise-sig-rule**)
- Click **Finish**. The newly created rule will be displayed.



**Step 4** – On the **enterprise-sig-rule** newly created, select the **Signaling QoS** tab and enter the following:

- Click the **Edit** button and the **Signaling QoS** window will open.
- Verify that **Enabled** is selected.
- Select **DCSP**.
- Select **Value = EF**.

**Step 5** - Click **Finish**.

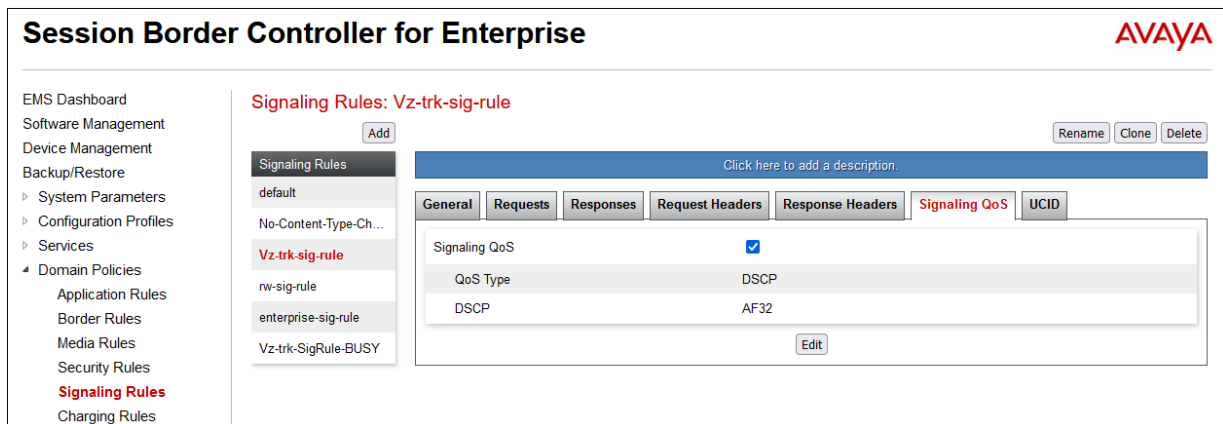


### 8.13.2 Signaling Rule – Verizon

Repeat the steps in **Section 8.13.1**, with the following changes, to create a Media Rule for Verizon.

- Clone the **default** rule.
- In the **Clone Name** field enter the new Media Rule name (e.g., **Vz-trk-sig-rule**).
- On the **Signaling QoS tab** select **Value = AF32** (as specified by Verizon).

The completed **Vz-trk-sig-rule** is shown on the screen below.



## 8.14. Endpoint Policy Groups

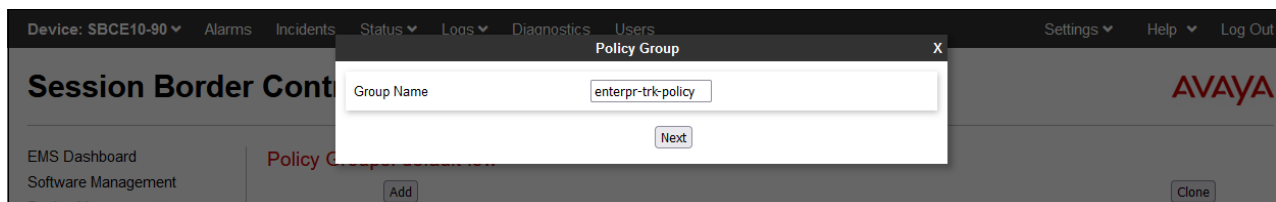
The rules created under the Domain Policy are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 8.15**.

### 8.14.1 End Point Policy Group - Enterprise

**Step 1** - Select **Domain Policies → End Point Policy Groups** from the left-hand side menu.

**Step 2** - Select **Add**.

- **Name:** enterpr-trk-policy.
- Click **Next**.



**Step 3** – On the **Policy Group** window (not shown), select the following.

- **Application Rule:** sip-trunk (created in **Section 8.11**).
- **Border Rule:** default.
- **Media Rule:** enterprise-med-rule (created in **Section 8.12.1**).
- **Security Rule:** default-low.
- **Signaling Rule:** enterprise-sig-rule (created in **Section 8.13.1**).

**Step 4** - Select **Finish**.

The completed Policy Group **enterprise-trk-policy** is shown on the screen below.

The screenshot shows the 'Policy Groups: enterpr-trk-policy' window. On the left is a navigation menu with 'End Point Policy Groups' highlighted. The main area shows a list of policy groups on the left and a detailed view of the 'enterprise-trk-policy' group on the right. The detailed view includes a table with the following data:

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	sip-trunk	default	enterprise-med-rule	default-low	enterprise-sig-rule	None	Off	Edit

## 8.14.2 Endpoint Policy Groups – Verizon

**Step 1** - Repeat steps 1 through 4 from **Section 8.14.1** with the following changes:

- **Group Name:** Vz-policy-grp.
- **Media Rule:** Vz-trk-med-rule (created in **Section 8.12.2**).
- **Signaling Rule:** Vz-trk-sig-rule (created in **Section 8.13.2**).

The completed Policy Group **Vz-policy-grp** is shown on the screen below.

The screenshot shows the 'Policy Groups: Vz-policy-grp' window. On the left is a navigation menu with 'End Point Policy Groups' highlighted. The main area shows a list of policy groups on the left and a detailed view of the 'Vz-policy-grp' group on the right. The detailed view includes a table with the following data:

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	sip-trunk	default	Vz-trk-med-rule	default-low	Vz-trk-sig-rule	None	Off	Edit

## 8.15. Endpoint Flows – Server Flows

Server Flows combine the interfaces, polices, and profiles defined in the previous sections into inbound and outbound flows. When a packet is received by Avaya SBCE, the content of the packet (IP addresses, SIP URIs, etc.) is used to determine which flow it matches, so that the appropriate policies can be applied. Create separate Server Flows for the enterprise and the Verizon IP Trunking Service.

### 8.15.1 Server Flow – Enterprise

**Step 1** - Select **Network and Flows** → **Endpoint Flows** from the menu on the left-hand side (not shown). Select the **Server Flows** tab (not shown).

**Step 2** - Select **Add**, (not shown) and enter the following:

- **Flow Name:** Enter a name for the flow, e.g., **SM Flow for Vz IPT**.
- **Server Configuration:** **Session Manager** (Section 8.8.1).
- **URI Group:** \*
- **Transport:** \*
- **Remote Subnet:** \*
- **Received Interface:** **Vz-Sig-B1** (Section 8.5).
- **Signaling Interface:** **Inside-Sig-50** (Section 8.5).
- **Media Interface:** **Inside-Med-50** (Section 8.4).
- **End Point Policy Group:** **enterpr-trk-policy** (Section 8.14.1).
- **Routing Profile:** **Route to VZ IPT** (Section 8.9.2).
- **Topology Hiding Profile:** **Enterprise-Topology** (Section 8.10.1).
- Let other fields at the default values.

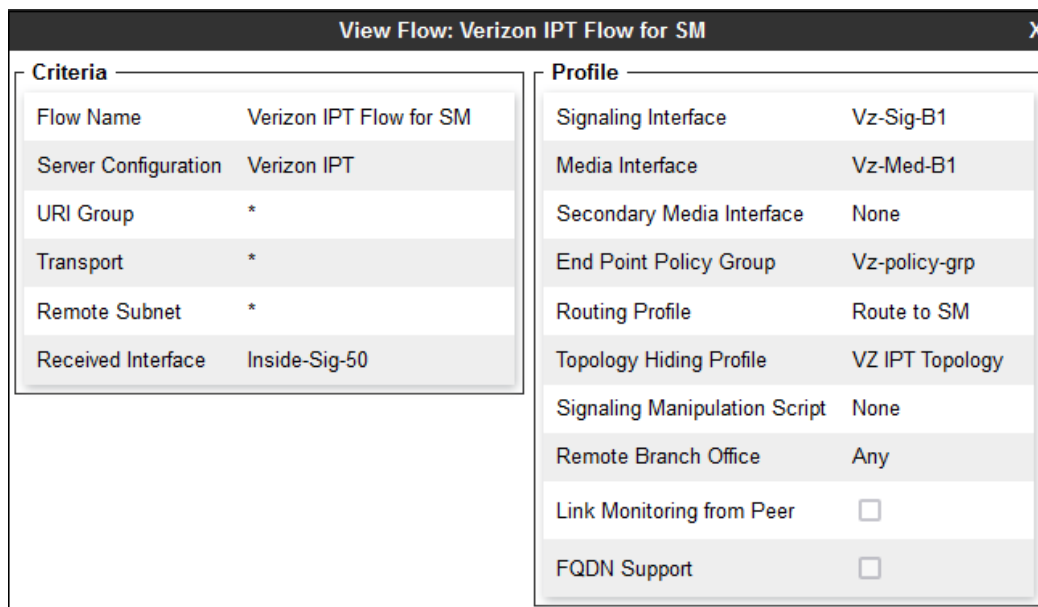
**Step 3** - Click **Finish** (not shown).

View Flow: SM Flow for Vz IPT	
<b>Criteria</b>	
Flow Name	SM Flow for Vz IPT
Server Configuration	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Vz-Sig-B1
<b>Profile</b>	
Signaling Interface	Inside-Sig-50
Media Interface	Inside-Med-50
Secondary Media Interface	None
End Point Policy Group	enterpr-trk-policy
Routing Profile	Route to VZ IPT
Topology Hiding Profile	Enterprise-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>

## 8.15.2 Server Flow – Verizon

**Step 1** - Repeat steps 1 through 3 from **Section 8.15.1**, with the following changes:

- **Flow Name:** Enter a name for the flow, e.g., **Verizon IPT Flow for SM**.
- **Server Configuration:** **Verizon IPT** (Section 8.8.2).
- **URI Group:** \*
- **Transport:** \*
- **Remote Subnet:** \*
- **Received Interface:** **Inside-Sig-50** (Section 8.5).
- **Signaling Interface:** **Vz-Sig-B1** (Section 8.5).
- **Media Interface:** **Vz-Med-B1** (Section 8.4).
- **End Point Policy Group:** **Vz-policy-grp** (Section 8.14.2).
- **Routing Profile:** **Route to SM** (Section 8.9.1).
- **Topology Hiding Profile:** **VZ IPT Topology** (Section 8.10.2).



Criteria	
Flow Name	Verizon IPT Flow for SM
Server Configuration	Verizon IPT
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside-Sig-50

Profile	
Signaling Interface	Vz-Sig-B1
Media Interface	Vz-Med-B1
Secondary Media Interface	None
End Point Policy Group	Vz-policy-grp
Routing Profile	Route to SM
Topology Hiding Profile	VZ IPT Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>

The screen below shows the completed **Server Flows** tab as configured in the shared test environment is shown below.

Subscriber Flows

Server Flows

SIP Server: Session Manager

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SM Flow for Vz IPT	*	Vz-Sig-B1	Inside-Sig-50	enterpr-trk-policy	Route to VZ IPT	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

SIP Server: Verizon IPT

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Verizon IPT Flow for SM	*	Inside-Sig-50	Vz-Sig-B1	Vz-policy-grp	Route to SM	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

## 9. Verizon Business IP Trunking Services Suite Configuration

Information regarding the Verizon Business IP Trunking Services suite offer can be found at <https://www.verizon.com/business/products/voice-collaboration/voip/ip-trunking/> or by contacting a Verizon Business sales representative.

The reference configuration described in these Application Notes is located in the Avaya Solutions and Interoperability Test Lab. Access to the Verizon Business IP Trunking Services suite was via a Verizon Private IP (PIP) T1 connection. Verizon Business provided all of the necessary service provisioning.

### 9.1. Service Access Information

The following service access information (FQDN, ports, DID numbers) was provided by Verizon for the sample configuration.

CPE (Avaya)	Verizon Network
<i>adevc.avaya.globalipcom.com</i> <i>UDP port 5060</i>	<i>pcelban0001.avayalincroft.globalipcom.com</i> <i>UDP Port 5071</i>

IP DID Numbers
732-945-0231
732-945-0232
732-945-0233
732-945-0234
732-945-0235
732-945-0236
732-945-0237
732-945-0238
732-945-0239

## 10. Verification Steps

This section provides example verifications of the Avaya configuration with Verizon Business IP Trunk service.

### 10.1. Avaya Aura® Communication Manager Verifications

This section illustrates verifications from Communication Manager.

The following edited Communication Manager **list trace tac** trace output shows an incoming call received on trunk group 1, member 1. The PSTN telephone dialed 732-945-0231. Session Manager mapped the number received from Verizon to the extension of a Communication Manager telephone (x50231). Note that initially the Avaya Media Server (10.64.91.88) is included on the media path.

```
list trace tac *01Page 1

LIST TRACE

time          data
16:11:37 TRACE STARTED 09/12/2022 CM Release String cold-01.0.974.0-27372
16:11:51 SIP<INVITE sips:50231@avayalab.com SIP/2.0
16:11:51      Call-ID: ab34442253abe9178fa0990a5aa3cc2d
16:11:51      active trunk-group 1 member 1      cid 0x99
16:11:51 SIP>SIP/2.0 183 Session Progress
16:11:51      Call-ID: ab34442253abe9178fa0990a5aa3cc2d
16:11:51      dial 50231
16:11:51      ring station      50231 cid 0x99
16:11:51      Alerting party uses public-unknown-numbering
16:11:51      G729 ss:off ps:20
16:11:51      rgn:2 [10.64.91.50]:35018
16:11:51      rgn:1 [10.64.91.88]:6080
16:11:55 SIP>SIP/2.0 200 OK
16:11:55      Call-ID: ab34442253abe9178fa0990a5aa3cc2d
16:11:55      active station      50231 cid 0x99
16:11:55      Connected party uses public-unknown-numbering
```

The following screen shows **Page 2** of the output of the **status trunk 1/x** command (where x is the trunk group member active on the call, **1** in the example) pertaining to this same call. Note the signaling using port 5081 between Communication Manager and Session Manager. Note the media is “ip-direct” from the IP Telephone (**192.168.7.103**) to the inside IP address of Avaya SBCE (**10.64.91.50**) using codec G.729a.

```

status trunk 1/1                                     Page 2 of 3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling   IP Address                               Port
  Near-end:   10.64.91.87                               : 5081
  Far-end:    10.64.91.85                               : 5081
H.245 Near:
H.245 Far:
H.245 Signaling Loc:                               H.245 Tunneled in Q.931? no

Audio Connection Type: ip-direct                     Authentication Type: None
Near-end Audio Loc:                                   Codec Type: G.729
Audio   IP Address                                   Port
Near-end: 192.168.7.103                               : 2412
Far-end:  10.64.91.50                               : 35018

```

The screen below shows **Page 3** of the output of the **status trunk 1/1** command pertaining to this same call. Note that codec G.729a and SRTP are used.

```

status trunk 1/1                                     Page 3 of 3
                                SRC PORT TO DEST PORT TALKPATH

src port: T00001
T000001:TX:10.64.91.50:35018/g729/20ms/1-srtp-aescm128-hmac80
S000000:RX:192.168.7.103:2412/g729a/20ms/1-srtp-aescm128-hmac80

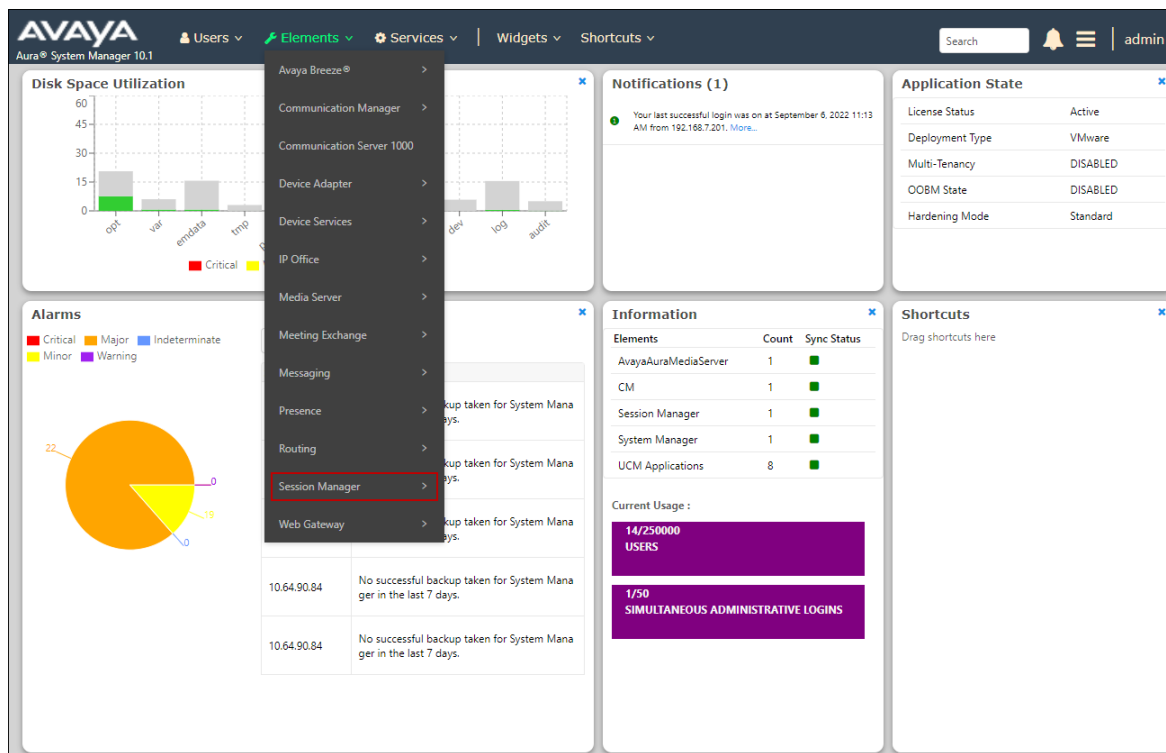
```



## 10.2. Avaya Aura® Session Manager Verification

The Session Manager configuration may be verified via System Manager.

Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.



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

Home	Session Manager	Help ?
<b>Session Manager Dashboard</b>		
This page provides the overall status and health summary of each administered Session Manager.		
<b>Session Manager Instances</b>		
Service State Shutdown System EASG Clear Logs As of 6:39 AM		
1 Item Show All Filter: Enable		
<input type="checkbox"/>	Session Manager	Type Tests Pass Alarms Security Module Service State Load Factor Entity Monitoring Active Call Count Registrations Data Replication User Data Storage Status License Mode EASG Profile Version
<input type="checkbox"/>	Session Manager	Core 0/0/0 Up Accept New Service 0/0/0 0/14 0 3/4 0/0/0 10.1.0.1.1010105
Select : All, None		

Clicking the entry under the **Entity Monitoring** column brings up the **Session Manager Entity Link Connection Status** page. Verify that the state of the Session Manager links of interest, to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is **UP**, like shown on the screen below.

Session Manager Entity Link Connection Status									
This page displays detailed connection status for all entity links from a Session Manager.									
Status Details for the selected Session Manager:									
All Entity Links for Session Manager: Session Manager									
Summary View									
14 Items <span>Filter: Enable</span>									
	SIP Entity Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	<a href="#">CM-TG5</a>	IPv4	10.64.91.87	5065	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">CM-TG6</a>	IPv4	10.64.91.87	5066	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">CM-TG1</a>	IPv4	10.64.91.87	5081	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">Avaya Messaging</a>	IPv4	10.64.19.90	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">SBCE-90_Vz1</a>	IPv4	10.64.91.50	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">CM-TG3</a>	IPv4	10.64.91.87	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">SBCE-70 Toll Free</a>	IPv4	10.64.91.41	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">SBCE-70 IPFR</a>	IPv4	10.64.91.40	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
<input type="radio"/>	<a href="#">Experience Portal</a>	IPv4	10.64.91.90	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">Aura Messaging</a>	IPv4	10.64.91.84	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">SBCE-101</a>	IPv4	10.64.91.101	5061	TLS	FALSE	UP	200 Keepalive	UP
<input type="radio"/>	<a href="#">SBCE-100_Vz2</a>	IPv4	10.64.91.100	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">CM-TG7</a>	IPv4	10.64.91.87	5067	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">SBCE30 HA</a>	IPv4	10.64.91.32	5061	TLS	FALSE	UP	200 OK	UP
Select : None									

Other Session Manager useful verification and troubleshooting tools include:

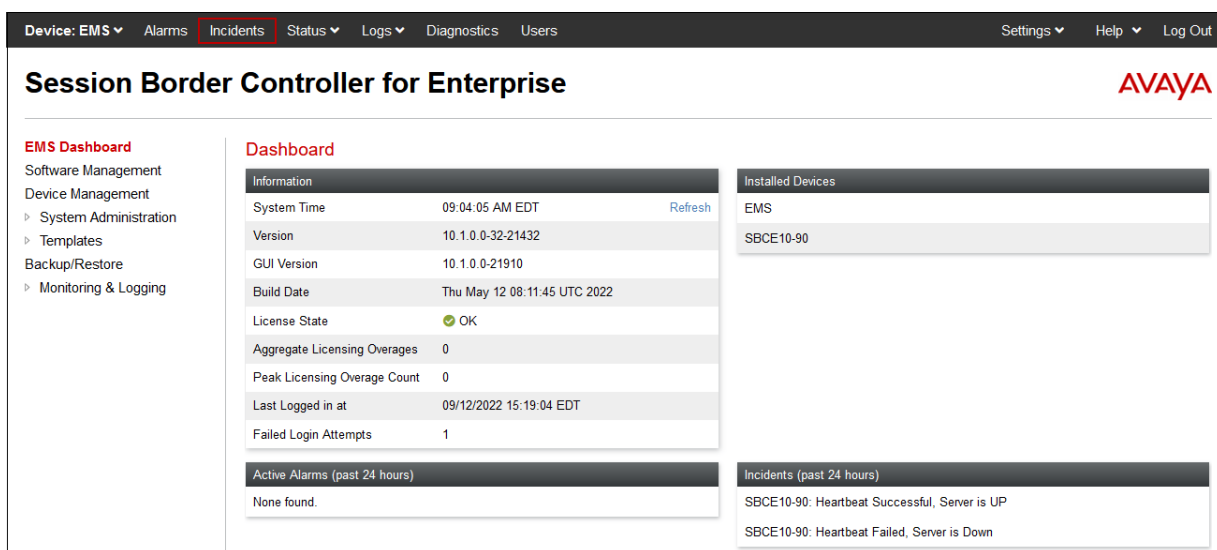
- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System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

## 10.3. Avaya Session Border Controller for Enterprise Verification

This section provides verification steps that may be performed with the Avaya SBCE.

### 10.3.1 Incidents

The Incident Viewer can be accessed from the Avaya top navigation menu as highlighted in the screenshot below.



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

### Session Border Controller for Enterprise

**EMS Dashboard**

- Software Management
- Device Management
  - System Administration
  - Templates
- Backup/Restore
- Monitoring & Logging

**Dashboard**

**Information**

System Time	09:04:05 AM EDT	<a href="#">Refresh</a>
Version	10.1.0.0-32-21432	
GUI Version	10.1.0.0-21910	
Build Date	Thu May 12 08:11:45 UTC 2022	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	09/12/2022 15:19:04 EDT	
Failed Login Attempts	1	

**Installed Devices**

EMS
SBCE10-90

**Active Alarms (past 24 hours)**

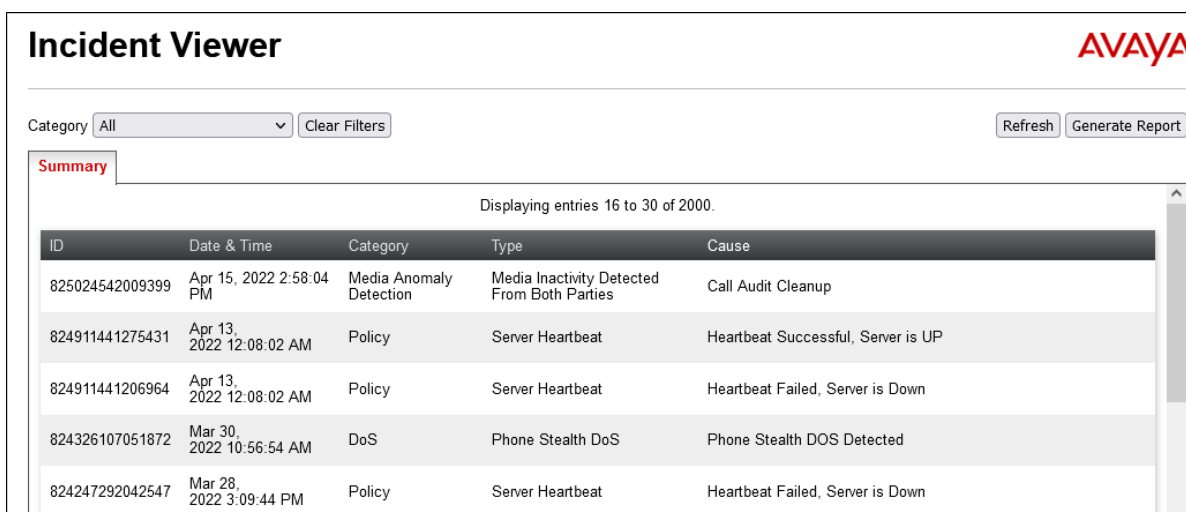
None found.

**Incidents (past 24 hours)**

SBCE10-90: Heartbeat Successful, Server is UP

SBCE10-90: Heartbeat Failed, Server is Down

Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures.



## Incident Viewer

Category: All Clear Filters Refresh Generate Report

**Summary**

Displaying entries 16 to 30 of 2000.

ID	Date & Time	Category	Type	Cause
825024542009399	Apr 15, 2022 2:58:04 PM	Media Anomaly Detection	Media Inactivity Detected From Both Parties	Call Audit Cleanup
824911441275431	Apr 13, 2022 12:08:02 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
824911441206964	Apr 13, 2022 12:08:02 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
824326107051872	Mar 30, 2022 10:56:54 AM	DoS	Phone Stealth DoS	Phone Stealth DOS Detected
824247292042547	Mar 28, 2022 3:09:44 PM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down

Further Information can be obtained by clicking on an incident in the incident viewer.

Incident Information			
General Information			
Incident Type	Media Inactivity Detected From Both Parties	Category	Media Anomaly Detection
Timestamp	April 15, 2022 at 2:58:04 PM EDT	Device	SBCE10-90
Cause	Call Audit Cleanup		
Additional Information			
Media Type	audio	Media Instance	1
Failure Reason	Media Inactivity detected		
Message Data			
Call ID	wlss-b4d359ba-138712447_128420891@10.64.90.90	From	sip:+1188887777@10.64.90.90
To	sip:10.64.90.90	Source IP	1.1.1.2
Destination IP	172.30.205.55		

### 10.3.2 Server Status

The **Server Status** can be accessed from the Avaya SBCE top navigation menu by selecting the **Status** menu, and then **Server Status**.

The screenshot shows the Avaya SBCE Enterprise web interface. The top navigation bar includes 'Device: EMS', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The 'Status' menu is expanded, showing options: 'SIP Statistics', 'Periodic Statistics', 'User Registrations', 'Server Status' (highlighted with a red box), 'Performance Status', and 'IP / URI Blocklist'. The left sidebar contains 'EMS Dashboard', 'Software Management', 'Device Management' (with sub-items: System Administration, Templates, Backup/Restore, Monitoring & Logging), and 'Dev'. The main content area shows 'Enterprise' and a table of device status.

Device Name	Management IP	Version	Status	
SBCE10-90	10.64.90.90	10.1.0.0-32-21432	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

The **Server Status** screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat to be enabled on the SIP Server Configuration profiles, as configured in **Section 8.8**.

Status							
Server Status							
Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
Verizon IPCC	172.30.205.55	172.30.205.55	5072	UDP	UP	UNKNOWN	09/07/2022 14:21:59 EDT
Verizon IPT	172.30.209.21	172.30.209.21	5071	UDP	UP	UNKNOWN	09/13/2022 00:36:53 EDT
Session Manager	10.64.91.85	10.64.91.85	5061	TLS	UP	UNKNOWN	09/07/2022 14:21:59 EDT

### 10.3.3 Diagnostics

This screen provides a **Full Diagnostics** tool to verify the link of each interface and ping the configured next-hop gateways and DNS servers. The **Ping Test** tool can be used to ping specific devices from any Avaya SBCE interface.

Task Description	Status
✓ EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: B1	B1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: B2	B2 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ Ping: SBC (A1) to Gateway (10.64.91.1)	Average ping from 10.64.91.48 [A1] to 10.64.91.1 is 1.931ms.
✓ Ping: SBC (A1) to Primary DNS (10.64.19.185)	Average ping from 10.64.91.48 [A1] to 10.64.19.185 is 0.353ms.
✗ Ping: SBC (A1) to Secondary DNS (172.30.209.4)	Error: Unable to reach 172.30.209.4 from 10.64.91.48 [A1].
✓ Ping: SBC (B1) to Gateway (1.1.1.1)	Average ping from 1.1.1.2 [B1] to 1.1.1.1 is 1.868ms.

## 10.3.4 Tracing

To take a call trace, navigate to **Monitoring & Logging → Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.

The screenshot shows the 'Session Border Controller for Enterprise' interface with the 'AVAYA' logo in the top right. On the left is a navigation menu with options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging. The 'Monitoring & Logging' section is expanded, showing sub-options: SNMP, Syslog Management, Debugging, Trace (highlighted), Log Collection, and DoS Learning. The main content area is titled 'Trace: SBCE10-90' and contains two tabs: 'Packet Capture' (active) and 'Captures'. The 'Packet Capture Configuration' form includes fields for Status (Ready), Interface (Any), Local Address (All), Remote Address (\*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (Test.pcap). 'Start Capture' and 'Clear' buttons are at the bottom.

When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, click the **Stop Capture** button at the bottom (not shown).

Select the **Captures** tab at the top and the capture will be listed; select the **File Name** and choose to open it with an application like Wireshark.

The screenshot shows the 'Captures' tab in the 'Trace: SBCE10-90' section. It features a table with columns 'File Name', 'File Size (bytes)', and 'Last Modified'. Two files are listed: 'Test\_20220602094017.pcap' (503,808 bytes, June 2, 2022 at 9:40:49 AM EDT) and 'Test\_20220601125125.pcap' (581,632 bytes, June 1, 2022 at 12:51:57 PM EDT). Each row has a 'Delete' link. Above the table are filters for 'Last Modified' (dropdown), 'Descending' (dropdown), 'Sort', and 'Reset', along with a 'Refresh' button.

File Name	File Size (bytes)	Last Modified
<a href="#">Test_20220602094017.pcap</a>	503,808	June 2, 2022 at 9:40:49 AM EDT
<a href="#">Test_20220601125125.pcap</a>	581,632	June 1, 2022 at 12:51:57 PM EDT

## 11. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, Avaya Experience Portal 8.1 and Avaya Session Border Controller for Enterprise 10.1 can be configured to interoperate successfully with Verizon Business IP Trunking service. This solution allows Avaya Aura® Communication Manager and Avaya Aura® Session Manager users access to the PSTN using a Verizon Business IP Trunking public SIP trunk service connection.

## 12. Additional References

### 12.1. Avaya

Avaya product documentation, including the following, is available at <http://support.avaya.com>

#### **Avaya Aura® Session Manager/System Manager**

- [1] *Deploying Avaya Aura® Session Manager and Branch Session Manager in Virtualized Environment*, Release 10.1.x, Issue 2, March 2022
- [2] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022
- [3] *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 10.1, Issue 2, March 2022
- [4] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 6, June 2022

#### **Avaya Aura® Communication Manager**

- [5] *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 10.1, Issue 4, June 2022
- [6] *Administering Avaya Aura® Communication Manager*, Release 10.1, Issue 1, December 2021
- [7] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 10.1, Issue 5, April 2022
- [8] *Administering Avaya G430 Branch Gateway*, Release 10.1.x, Issue 1, December 2021
- [9] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 10.1.x, Issue 2, June 2022
- [10] *Implementing and Administering Avaya Aura® Media Server*, Issue 10.1.x, April 2022

#### **Avaya Session Border Controller for Enterprise**

- [11] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1, Issue 1, December 2021
- [12] *Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform*, Release 10.1.x, Issue 1, December 2021
- [13] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 10.1.x, Issue 1, December 2021

#### **Avaya Experience Portal**

- [14] *Administering Avaya Experience Portal*, Release 8.1.1, Issue 2, February 2022
- [15] *Implementing Avaya Experience Portal on a single server*, Release 8.1.1, Issue 1, January 2022

### 12.2. Verizon Business

The following documents may be obtained by contacting a Verizon Business Account Representative.

- [16] *Retail VoIP Interoperability Test Plan*
- [17] *Network Interface Specification Retail VoIP Trunk Interface (for non-registering devices)*



## 13. Appendix A – Avaya SBCE – Refer Handling

One of the capabilities important to the Experience Portal environment is the Avaya SBCE Refer Handling option. As described in **Section 3.3.2**, 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 Verizon.

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-extensions**, and select **Next** (not shown).

**Step 3** - Enter the following:

- **Scheme:** sip:/sips:
- **Type:** Regular Expression
- **URI:** 12[0-9]{3}@.\* This will match 5-digit local extensions starting with 12, e.g., 12001.
- 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: 12[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 shows the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, and URI Groups (highlighted in red). The main area is titled 'URI Groups: internal-extensions'. It features a list of URI Groups with columns for 'URI Group' and actions 'Edit' and 'Delete'. The list contains two entries: '12[0-9](3)@.\*' and '50[0-9](3)@.\*'. An 'Add' button is visible in the top right corner of the list area.

Edit the existing Verizon Server Interworking Profile to enable Refer Handling and assign the newly created URI Group.

**Step 1** - Select **Configuration Profiles → Server Interworking** from the left-hand menu

**Step 2** - Select the Verizon Server Interworking Profile created in **Section 8.6.2** and click **Edit**

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

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left navigation menu has 'Server Interworking' highlighted in red. The main area is titled 'Interworking Profiles: SIP Provider Interwk'. It shows a list of interworking profiles with columns for 'Interworking Profiles' and actions 'Rename', 'Clone', and 'Delete'. The list contains three entries: 'cs2100', 'avaya-ru', and 'SIP Provider Interwk' (highlighted in red). The 'SIP Provider Interwk' profile is selected, and its configuration is displayed in a tabbed interface. The 'General' tab is active, showing a table of configuration parameters. The 'Refer Handling' row is highlighted with a red box, showing 'Refer Handling' set to 'Yes' and 'URI Group' set to 'internal-extensions'.

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

## 14. Appendix B – Avaya SBCE – SigMa Script File

Details of the Signaling Manipulation script used in the configuration of the Avaya SBCE, in **Section 8.7**.

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

//Remove epv parameter from Contact header to hide internal topology
        remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);

//Remove unwanted xml information
        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 = "7329450232";
            }
        }
    }
}
```

---

**©2022 Avaya Inc. All Rights Reserved.**

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

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