



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, Avaya Aura® Experience Portal 7.2 and Avaya Session Border Controller for Enterprise 8.0.1 with AT&T IP Toll Free Service – Issue 1.0**

### **Abstract**

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, Avaya Aura® Experience Portal 7.2 and the Avaya Session Border Controller for Enterprise 8.0.1 with the AT&T IP Toll Free service using AT&T's **AVPN** or **MIS/PNT** transport connections.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks. Note that this document do not include the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service, which are covered on separate Application Notes.

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

AT&T is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

## **TABLE OF CONTENTS**

1.	Introduction.....	5
2.	General Test Approach and Test Results.....	6
2.1.	Interoperability Compliance Testing.....	7
2.2.	Test Results .....	8
2.3.	Support .....	9
3.	Reference Configuration.....	10
3.1.	Illustrative Configuration Information .....	12
3.2.	Call Flows .....	13
3.2.1.	Communication Manager Call Flow.....	13
3.2.2.	Experience Portal Call Flows.....	14
4.	Equipment and Software Validated .....	16
5.	Configure Avaya Aura® Communication Manager .....	17
5.1.	System-Parameters Customer-Options .....	17
5.2.	System-Parameters Features .....	19
5.3.	Dial Plan.....	19
5.4.	Node Names .....	20
5.5.	Processor Ethernet.....	20
5.6.	IP Network Regions .....	21
5.6.1.	IP Network Region 1 – Local CPE Region .....	21
5.6.2.	IP Network Region 4 – AT&T Trunk Region .....	23
5.7.	IP Codec Sets .....	24
5.7.1.	Codecs for IP Network Region 1 (calls within the CPE).....	24
5.7.2.	Codecs for IP Network Region 4 (calls from AT&T) .....	25
5.8.	SIP Trunks.....	26
5.8.1.	SIP Trunk for Inbound AT&T calls.....	26
5.8.2.	Local SIP Trunk (Avaya SIP Telephones, Messaging Access, etc.) .....	30
5.9.	Public Numbering .....	31
5.10.	Private Numbering.....	32
5.11.	Route Pattern for Local SIP Trunk.....	32
5.12.	Automatic Alternate Routing (AAR) Dialing .....	33
5.13.	Provisioning for Simulated Call Center Functionality .....	34
5.14.	Avaya G430 Media Gateway Provisioning.....	36
5.15.	Avaya Aura® Media Server Provisioning.....	37
5.16.	Save Translations.....	38
5.17.	Verify TLS Certificates – Communication Manager .....	39
6.	Configure Avaya Aura® Session Manager .....	40
6.1.	System Manager Login and Navigation.....	41
6.2.	SIP Domain .....	42
6.3.	Locations .....	43
6.3.1.	Main Location.....	43
6.3.2.	Common-SBCs Location .....	43
6.4.	Configure Adaptations .....	44
6.4.1.	Adaptation for Avaya Aura® Communication Manager Extensions .....	44
6.4.2.	Adaptation for the AT&T IP Toll Free Service .....	46
6.5.	SIP Entities .....	47

6.5.1.	Avaya Aura® Session Manager SIP Entity .....	47
6.5.2.	Avaya Aura® Communication Manager SIP Entity – Public Trunk .....	49
6.5.3.	Avaya Aura® Communication Manager SIP Entity – Local Trunk.....	50
6.5.4.	Avaya Session Border Controller for Enterprise SIP Entity.....	50
6.5.5.	Avaya Aura® Experience Portal SIP Entity .....	50
6.6.	Entity Links .....	51
6.6.1.	Entity Link to Avaya Aura® Communication Manager – Public Trunk.....	51
6.6.2.	Entity Link to Avaya Aura® Communication Manager – Local Trunk.....	52
6.6.3.	Entity Link for the AT&T IP Toll Free Service via the Avaya SBCE .....	52
6.6.4.	Entity Link to Avaya Aura® Experience Portal .....	52
6.7.	Time Ranges – (Optional) .....	52
6.8.	Routing Policies .....	53
6.8.1.	Routing Policy for AT&T Routing to Avaya Aura® Communication Manager .....	53
6.8.2.	Routing Policy for Inbound Calls to Experience Portal.....	54
6.9.	Dial Patterns .....	55
6.9.1.	Origination Dial Patterns – (Optional).....	55
6.9.2.	Dial Pattern for Inbound Calls to Communication Manager .....	57
6.9.3.	Dial Pattern for Inbound Calls to Experience Portal .....	58
6.10.	Verify TLS Certificates – Session Manager.....	60
7.	Configure Avaya Aura® Experience Portal .....	62
7.1.	Background .....	62
7.2.	Logging In and Licensing .....	63
7.3.	VoIP Connection .....	64
7.4.	Speech Servers .....	65
7.5.	Application References .....	66
7.6.	MPP Servers and VoIP Settings.....	67
7.7.	Configuring RFC2833 Event Value Offered by Experience Portal .....	69
8.	Configure Avaya Session Border Controller for Enterprise .....	70
8.1.	Device Management – Status.....	71
8.2.	TLS Management.....	73
8.2.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise .....	73
8.2.2.	Server Profiles.....	74
8.2.3.	Client Profiles .....	75
8.3.	Network Management.....	76
8.4.	Advanced Options .....	77
8.5.	Media Interfaces .....	78
8.6.	Signaling Interfaces.....	79
8.7.	Server Interworking Profiles .....	80
8.7.1.	Server Interworking Profile – Enterprise .....	80
8.7.2.	Server Interworking – AT&T .....	81
8.8.	Signaling Manipulation .....	83
8.9.	SIP Server Profiles .....	84
8.9.1.	SIP Server Profile – Session Manager .....	84
8.9.2.	SIP Server Profile – AT&T.....	86
8.10.	Routing Profiles.....	88
8.10.1.	Routing Profile – Session Manager.....	88

8.10.2.	Routing Profile – AT&T .....	89
8.11.	Topology Hiding Profiles .....	90
8.11.1.	Topology Hiding – Enterprise Side.....	90
8.11.2.	Topology Hiding – AT&T Side .....	91
8.12.	Application Rules .....	91
8.13.	Media Rules.....	92
8.13.1.	Enterprise – Media Rule.....	92
8.13.2.	AT&T – Media Rule .....	94
8.14.	Signaling Rules.....	95
8.14.1.	Signaling Rule – Enterprise.....	95
8.14.2.	Signaling Rule – AT&T .....	95
8.15.	Endpoint Policy Groups.....	96
8.15.1.	Endpoint Policy Group – Enterprise .....	96
8.15.2.	Endpoint Policy Group – AT&T .....	97
8.16.	Endpoint Flows – Server Flows .....	97
8.16.1.	Server Flows – Enterprise .....	97
8.16.2.	Server Flow – AT&T .....	98
9.	AT&T IP Toll Free Service Configuration.....	99
10.	Verification Steps.....	99
10.1.	AT&T IP Toll Free Service .....	99
10.2.	Avaya Aura® Communication Manager Verification .....	100
10.3.	Avaya Aura® Session Manager Verification .....	101
10.4.	Avaya Session Border Controller for Enterprise Verification.....	103
10.4.1.	Incidents .....	103
10.4.2.	Server Status.....	104
10.4.3.	Protocol Traces.....	104
11.	Conclusion .....	106
12.	References.....	107
13.	Appendix A – Refer Handling by Avaya SBCE.....	108
14.	Appendix B – Configuration for G.711 Fax Testing .....	111

# 1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, Avaya Aura® Experience Portal 7.2 and Avaya Session Border Controller for Enterprise 8.0.1 with the AT&T IP Toll Free service using AT&T Virtual Private Network (AVPN) or Managed Internet Service Private Network Transport (MIS/PNT) connections<sup>1</sup>.

Avaya Aura® Communication Manager 8.1 (Communication Manager) is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Aura® Session Manager 8.1 (Session Manager) is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise.

Avaya Aura® Experience Portal (Experience Portal) provides a single platform for automated voice and multimedia self-service and Interactive Voice Response (IVR) applications. In the sample configuration described in these Application Notes, a basic Experience Portal test call application was used to exercise various inbound SIP call flow scenarios.

The Avaya Session Border Controller for Enterprise 8.0.1 (Avaya SBCE) is the point of connection between Avaya Aura® Session Manager and the AT&T IP Toll Free service. It is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

The AT&T IP Toll Free service, referred to in the remainder of this document as IPTF, is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks utilizing AVPN or MIS/PNT transport.

**Note** – These Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service. That solution is described in a separate document.

---

<sup>1</sup> MIS/PNT transport does not support compressed RTP (cRTP), however AVPN transport does support cRTP.

## 2. General Test Approach and Test Results

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.

The interoperability compliance testing focused on verifying inbound and outbound call flows between IPTF and the Customer Premises Equipment (CPE) containing Communication Manager, Session Manager, Experience Portal and the Avaya SBCE (see **Section 3.2** for call flow examples).

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 these Application Notes, the interface between Avaya systems and the AT&T Toll Free service did not include use of any specific encryption features as requested by AT&T.

## 2.1. Interoperability Compliance Testing

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the IPTF network. Calls were made from the PSTN, across the IPTF network, to the CPE.

The following SIP trunking VoIP features were tested with the IPTF service:

- Inbound PSTN/IPTF calls to Communication Manager stations, Vector Directory Numbers (VDNs), Vectors, and Agents.
- Call and two-way talk path establishment between PSTN and Communication Manager telephones/Agents via IPTF.
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729A and G.711Mu codecs.
- T.38 fax calls via IPTF to Communication Manager fax endpoints.
- G.711 pass-through fax calls via IPTF to Communication Manager fax endpoints.
- DTMF tone transmission using RFC 2833/4733 between Communication Manager and IPTF automated access systems.
- Verify reception of IPTF SIP Multipart/NSS headers, including SDP and XML content.
- IPTF network features such as Legacy Transfer Connect (inband) and Alternate Destination Routing (ADR).
- Long duration calls.
- 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.

An Avaya Remote Worker endpoint (Avaya Equinox SIP softphone) was one of the Avaya endpoints used in the reference configuration. The Remote Worker resides on the public side of the Avaya SBCE (via a TLS connection), and registers/communicates with Avaya Session Manager via Avaya SBCE, as though it was an endpoint residing in the private CPE space. The configuration of the Remote Worker environment is beyond the scope of this document.

## 2.2. Test Results

The test objectives stated in **Section 2.1**, with limitations as noted below, were verified.

1. **IP Toll Free ADR Call Redirection feature in response to a ring-no-answer condition.**  
There is an anomaly in the AT&T VIT lab where the Ring No Answer did not get triggered due to Lab restrictions. However, in production, if there is no answer for 20 seconds, ADR Call Redirection will be invoked.
2. **IP Toll Free ADR Call Redirection feature based on SIP error code response.** The IP Toll Free service can be configured to invoke the ADR Call Redirection feature upon receiving of an error response from the CPE.
  - The following error conditions were producible in the reference configuration and tested successfully: 480 Temporarily Unavailable, 486 Busy Here, 500 Server Internal Error and 503 Service Unavailable.
  - Even though the following error conditions were not producible in the reference configuration, the associated error codes were simulated via an Avaya SBCE signaling manipulation rule, and also tested successfully: 408 Request Timeout, 504 Server Timeout, and 600 Busy Everywhere.
3. **G.726-32 codec support.** While Communication Manager supports G.726-32, the IPTF implementation of G.726-32 results in poor audio quality. Therefore, G.726-32 codec is not supported between Communication Manager and the IPTF service.
4. **T.38/G.729 fax is limited to 9600bps when using the G4xx Media Gateways.** A G430 Media Gateway is used in the reference configuration. As a result, T.38/G.729 fax was limited to 9600 bps. Also note that the sender and receiver of a T.38 fax call may use either Group 3 or Super Group 3 fax machines, but the T.38 fax protocol carries all fax transmissions as Group 3.
5. **G.711 pass-through fax.** Inbound G.711 pass-through fax was tested in addition to T.38 fax. This was done by configuring a separate Communication Manager ip-codec-set (**Section 14**). Faxes using G.711 pass-through generally completed at better line speeds (rates of 14400 bps were observed). However, when the PSTN sender and CPE receiver both used SG3 fax devices, the results were erratic. Due to the unpredictability of pass-through techniques, which only work well on networks with very few hops and with limited end-to-end delay, G.711 fax pass-through is delivered in Communication Manager on a “best effort” basis; its success is not guaranteed, and it should be used at the customer’s discretion. T.38 should be the preferred method for faxing.
6. **IP Toll Free services IP InfoPack and Landline/Mobility test cases could not be executed.** The AT&T supplied IP Toll Free test plan specifies test cases to verify the inbound transmission of INFOPAK and Landline/Mobility data by the IP Toll Free service. Due to network provisioning and lab support issues, these test cases could not be executed.
7. **Removal of unnecessary SIP headers.** In an effort to reduce packet size (or block a header containing private addressing), Session Manager is provisioned to remove SIP headers not required by the AT&T IPTF service (see **Section 6.4.2**). These headers are:
  - AV-Global-Session-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, P-Charging-Vector, P-Location, Av-Secure-IndicationTo help reduce the packet size further, the Avaya SBCE can remove the Avaya “gsid” and “epv” parameters that may be included within the Contact header of outbound messages, by applying a Sigma script to the AT&T SIP server profile. See **Section 8.8**.



8. **Avaya SIP endpoints may generate three Bandwidth headers; b=TIAS:64000, b=CT:64, and b=AS:64, causing AT&T network issues.** Certain Avaya SIP endpoints (e.g., 9641, 9621, and 9608 models) may generate various Bandwidth headers depending on the call flow. It has been observed that sending these Bandwidth headers may cause issues with AT&T services. Therefore, an Avaya SBCE Signaling Manipulation Rule is used to remove these headers (see **Section 8.8**).
9. **Enhanced CID – NSS feature.** The inbound calls to Communication Manager are not exercising the Enhanced CID feature. Although Communication Manager is accepting SIP Multipart/NSS headers, it is neither passing nor acting upon it. It is simply being ignored.
10. **Avaya SBCE inserts a=ptime:20 in the SIP SDP toward Communication Manager.** AT&T includes a=maxptime:30 in the SIP SDP to recommend a ptime value of 30ms, but does not specify a ptime value in the SDP. If no media packetization attribute (ptime) is included in the SIP Session Description Protocol (SDP), Avaya SBCE inserts “a=ptime:20”, specifying 20 milliseconds. Although Communication Manager can be configured to send ptime with a value of 30ms (See **Section 5.7.2**), it will send a ptime value of 20ms when it receives “a=ptime:20” from the Avaya SBCE. This causes the media packetization to be set to 20ms. No issues were found during testing due to this behavior.

## 2.3. Support

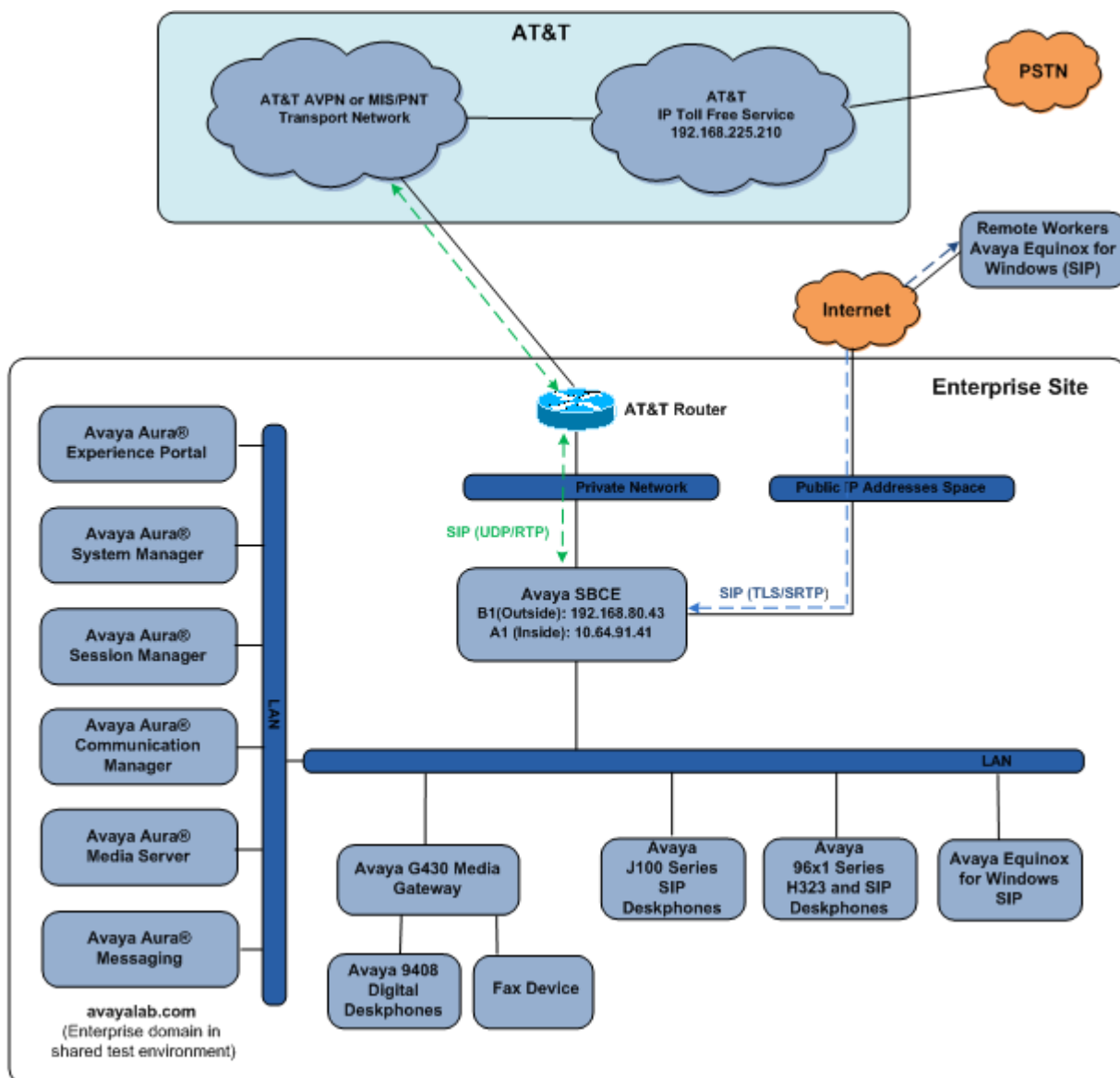
AT&T customers may obtain support information for the AT&T IP Toll Free service by visiting <https://www.business.att.com/products/ip-toll-free.html> or by calling (800) 325-5555.

Avaya customers may obtain documentation and support for Avaya products by visiting the Support page: <http://support.avaya.com>. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus. Customers may also use specific numbers provided on the Support website to directly access specific support and consultation services based upon their Avaya support agreements.

### 3. Reference Configuration

The reference configuration used in these Application Notes is shown in **Figure 1** and consists of several components:

- Session Manager provides core SIP routing and integration services that enables communication between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Avaya SIP endpoints register to Session Manager.
- System Manager provides a common administration interface for centralized management of all Session Manager instances in an enterprise.
- Communication Manager provides the voice communication services for a particular enterprise site. Avaya H.323 endpoints register to Communication Manager.
- The Avaya Media Gateway provides the physical interfaces and resources for Communication Manager. In the reference configuration, an Avaya G430 Media Gateway is used. This solution is extensible to other Avaya Media Gateways.
- Avaya Aura® Media Server provides additional media resources for Communication Manager.
- Experience Portal self-service applications allow callers to automatically obtain assistance or information without the need for agent interaction. Experience Portal can also redirect calls to Communication Manager agents based on the caller's selections to the prompts.
- Avaya Aura® Messaging (Messaging) was used in the reference configuration to provide voice mailbox capabilities. This solution is extensible to other Avaya messaging platforms. The provisioning of Avaya Aura® Messaging is beyond the scope of this document.
- Avaya desk telephones are represented with Avaya 96x1 Series IP Deskphones (running H.323 and SIP firmware), J100 Series IP Deskphones using the SIP software bundle Avaya 9408 Digital Deskphones, as well as Avaya Equinox™ for Windows softphones.
- The Avaya SBCE provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPTF service and the enterprise internal network.
- The IPTF service uses SIP over UDP to communicate with enterprise edge SIP devices, e.g., the Avaya SBCE. Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements, e.g., the Avaya SBCE (e.g., UDP, TCP, or TLS) and Communication Manager (e.g., TCP or TLS). In the reference configuration, Session Manager uses SIP over TLS to communicate with the Avaya SBCE, Experience Portal, Messaging and Communication Manager.
- Inbound calls were placed from the PSTN via the IPTF service, through the Avaya SBCE to Session Manager. Session Manager used the configured dial patterns and routing policies to determine where to send the call (e.g., Communication Manager, Experience Portal). Communication Manager terminated the calls to the appropriate Agent queue, Agent phone, or fax extension.



**Figure 1: Reference configuration**

**Note** – In the reference configuration, the IPTF service delivered 10 DNIS digits, with the format *00000xxxxx*. These DNIS digits are used in the provisioning defined in the following sections, not the dialed digits. The DNIS digit length can vary depending on the customer’s needs. Although during testing 10 digits were used, the total length supported by the IPTF service is 21 digits, including the five leading zeroes.

### 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 specific configurations.

**Note** - The AT&T IP Toll Free service Border Element IP address and DNIS digits, (destination digits specified in the SIP Request URIs sent by the AT&T Toll Free service) are shown in this document as examples. AT&T Customer Care will provide the actual IP addresses and DNIS digits as part of the IP Toll Free provisioning process.

Component	Illustrative Value in these Application Notes
<b>Avaya Aura® System Manager</b>	
IP Address	10.64.90.82
<b>Avaya Aura® Session Manager</b>	
IP Address	10.64.91.81
<b>Avaya Aura® Communication Manager</b>	
IP Address	10.64.91.75
Communication Manager dialplan	89xxx = Stations 2xxxx = Agents 71xxx = Agent skill queue VDNs
<b>Avaya Aura® Messaging</b>	
IP Address	10.64.91.84
<b>Avaya Aura® Experience Portal</b>	
IP Address	10.64.91.90
<b>Avaya Session Border Controller for Enterprise (SBCE)</b>	
IP Address of Inside (Private) Interface	10.64.91.41
IP Address of Outside (Public) Interface	192.168.80.43 (see note below)
<b>AT&amp;T IP Toll Free Border Element</b>	
IP Address	192.168.225.210

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

**Note** – For security reasons, the actual IP addresses of the Avaya SBCE and AT&T BE are not included in this document. However, as placeholders in the following configuration sections, the IP address of **192.168.80.43** (Avaya SBCE public interface) and **192.168.225.210** (AT&T BE IP address) are specified.

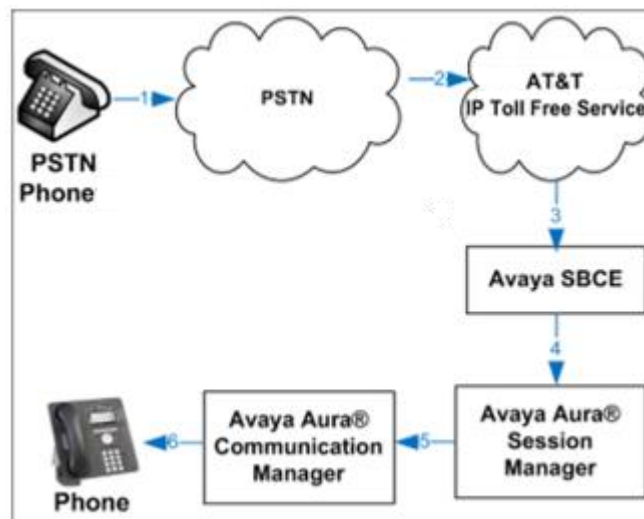
## 3.2. Call Flows

To understand how inbound AT&T IP Toll Free service calls are handled in the Avaya CPE environment, three basic call flows are described in this section.

### 3.2.1. Communication Manager Call Flow

In the general call flow shown on **Figure 2** below, an inbound IPTF service call arrives at the Avaya SBCE and is subsequently routed to Session Manager and to Communication Manager.

1. A PSTN telephone originates a call to an IPTF service number.
2. The PSTN routes the call to the IPTF service network.
3. The IPTF 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 Routing Policies, determines 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 an Agent queue or telephone.



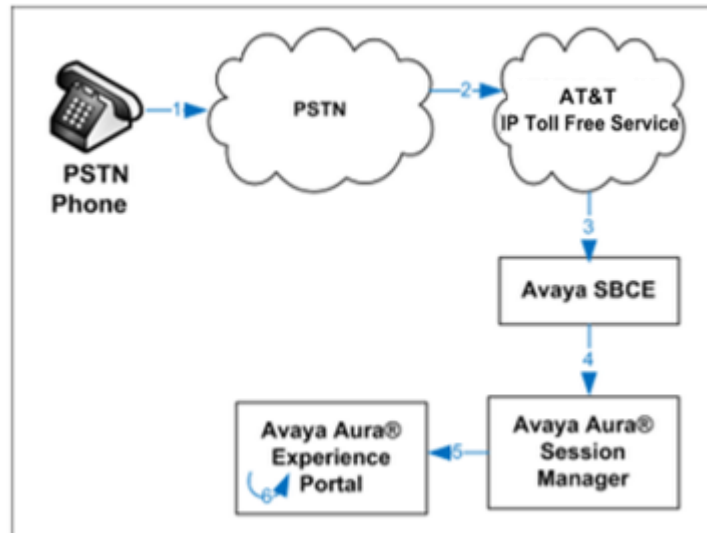
**Figure 2: Inbound AT&T IP Toll Free Service Call to an Agent queue/telephone**

**Note:** The IPTF service features such as Legacy Transfer Connect and Alternate Destination Routing utilize this call flow as well.

### 3.2.2. Experience Portal Call Flows

The call scenario illustrated on **Figure 3** below shows an inbound call arriving and remaining on Experience Portal.

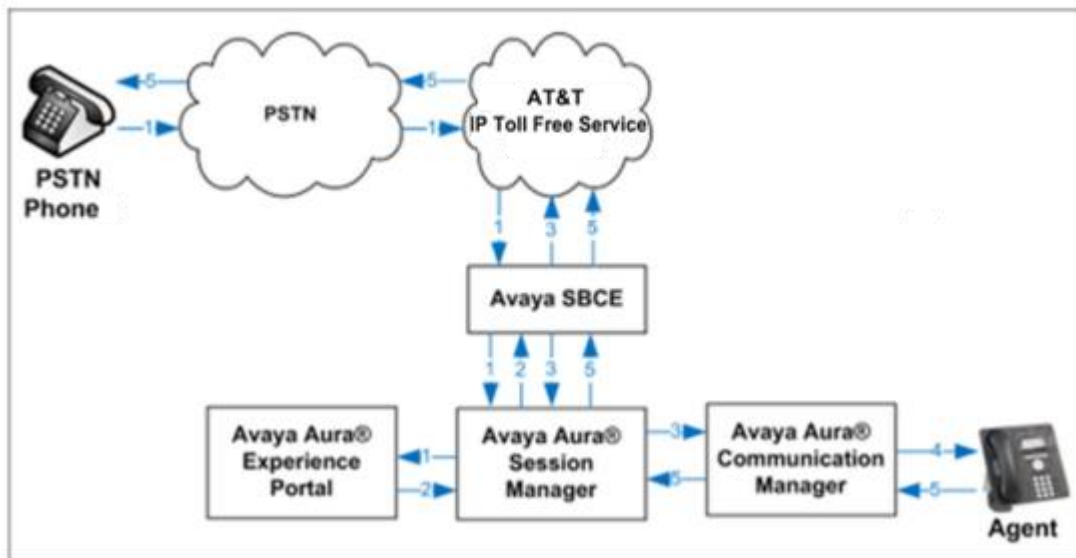
1. A PSTN phone originates a call to an IPTF number.
2. The PSTN routes the call to the IPTF network.
3. IPTF routes the call to the Avaya SBCE.
4. The Avaya SBCE performs any necessary SIP header modifications and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header 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 3: Inbound Call Handling Entirely by Avaya Aura® Experience Portal**

The next call scenario illustrated on **Figure 4** below shows an inbound call arriving on Experience Portal, and transferred to an agent in Communication Manager.

1. Same as the first five steps from the previous 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 4: Avaya Aura® Experience Portal Transfers Call to Avaya Aura® Communication Manager**

**Note:** See **Appendix A, Section 13** for configuration information on the Avaya SBCE Refer Handling option for Experience Portal

## 4. Equipment and Software Validated

The following equipment and software was used for the reference configuration described in these Application Notes.

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	8.1.0.2 (Service Pack 2)
Avaya Aura® Session Manager	8.1.0.0.810007
Avaya Aura® System Manager	8.1.0.0.079880
Avaya Aura® Experience Portal	7.2.3.0.0441
Avaya Session Border Controller for Enterprise	8.0.1.0-10-17555
Avaya Aura® Messaging	7.1 SP 1
Avaya Aura® Media Server	8.0.1.121
Avaya G430 Media Gateway	41.10.0
Avaya 96x1 Series IP Deskphone (H.323)	6.8202
Avaya 96x1 Series IP Deskphone (SIP)	7.1.6.1.3
Avaya J129 IP Deskphone (SIP)	4.0.2.1.3
Avaya 9408 Digital Deskphone	20.06
Avaya Equinox for Windows	3.6.4.31.2
Fax device	Ventafax 7.10

**Table 2: Equipment and Software Versions**



## 5. Configure Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed. Consult [5] and [6] in the References section for further details if necessary.

**Note** – In the following sections, only the parameters that are highlighted in **bold** text are applicable to these application notes. Other parameter values may or may not match based on local configurations.

### 5.1. System-Parameters Customer-Options

This section reviews the Communication Manager licenses and features that are required for the reference configuration described in these Application Notes.

**NOTE - For any required features that cannot be enabled in the steps that follow, contact an authorized Avaya account representative to obtain the necessary licenses.**

**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 5 of the form, verify that the Media Encryption Over IP field is set to y.**

display system-parameters customer-options		Page 5 of 12
OPTIONAL FEATURES		
Emergency Access to Attendant? y		IP Stations? y
Enable 'dadmin' Login? y		
Enhanced Conferencing? y		ISDN Feature Plus? n
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n		ISDN-BRI Trunks? y
Enterprise Wide Licensing? n		ISDN-PRI? y
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	
IP Trunks? y		
IP Attendant Consoles? y		

**Step 3 - 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**.

<b>change system-parameters features</b>	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**.

<b>change dialplan analysis</b>	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 **10.64.91.81**).
- Media Server (e.g., **AMS** and **10.64.91.86**). The Media Server node name is only needed if a Media Server is present.

<b>change node-names ip</b>		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
<b>AMS</b>	<b>10.64.91.86</b>	
<b>SM</b>	<b>10.64.91.81</b>	
default	0.0.0.0	
<b>procr</b>	<b>10.64.91.75</b>	
procr6	::	

## 5.5. Processor Ethernet

The **display 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>display 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: 10.64.91.75
Subnet Mask: /24		

## 5.6. IP Network Regions

Network regions provide a means to logically group resources such as codecs, UDP port ranges, and inter-region communication. 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 4 was associated to components used specifically for the AT&T SIP trunk access.

### 5.6.1. 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 (see **Section 6.2**).
- 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.
- **UDP Port Min**: – Set to **16384** (AT&T requirement).
- **UDP Port Max**: – Set to **32767** (AT&T requirement).

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: avayalab.com	
Name: Enterprise	Stub Network Region: n	
MEDIA PARAMETERS		
Codec Set: 1	Intra-region IP-IP Direct Audio: yes	
UDP Port Min: 16384	Inter-region IP-IP Direct Audio: yes	
UDP Port Max: 32767	IP Audio Hairpinning? n	
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
AUDIO RESOURCE RESERVATION PARAMETERS		
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

**Note** – The port range for Region 1 does not have to be in the range required by AT&T. However, the same range was used here in the reference configuration.

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

- Verify that **RTCP Reporting to Monitor Server Enabled** is set to **y**.

change ip-network-region 1	Page 2 of 20
IP NETWORK REGION	
RTCP Reporting to Monitor Server Enabled? y	
RTCP MONITOR SERVER PARAMETERS	
Use Default Server Parameters? y	

**Step 3** - 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 **4** in the **dst rgn** column, enter **4** for the codec set (this means region 1 is permitted to talk to region 4 and it will use codec set 4 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
<b>dst</b>	<b>codec</b>	<b>direct</b>	<b>WAN-BW-limits</b>		<b>Video</b>	<b>Intervening</b>		<b>Dyn</b>	A	G	c
<b>rgn</b>	<b>set</b>	<b>WAN</b>	<b>Units</b>	<b>Total</b>	<b>Norm</b>	<b>Prio</b>	<b>Shr</b>	<b>Regions</b>	<b>CAC</b>	R	L
<b>1</b>	<b>1</b>									all	e
2	2	y	NoLimit						n		t
3	1	y	NoLimit						n		t
4	4	y	NoLimit						n		t

## 5.6.2. IP Network Region 4 – AT&T Trunk Region

Repeat the steps in **Section 5.6.1** with the following changes:

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

- Enter a descriptive name (e.g., **AT&T**).
- Enter **4** for the **Codec Set** parameter.

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

- Set codec set **4** for **dst rgn 1**.
- Note that **dst rgn 4** is pre-populated with codec set **4** (from page 1 provisioning).

change ip-network-region 4										Page	4	of	20
Source Region: 4		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	4	y	NoLimit							n		t	
2	4	y	NoLimit							n		t	
3	3	y	NoLimit							n		t	
4	4												
										all			

**Note:** An additional IP Network Region and IP Codec Set were created in the reference configuration, used to test G.711 pass-through fax. Details of this optional configuration can be found in **Section 14**.

## 5.7. 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.

**Note** – The IPTF service offers G.729A, G.726-32, and G.711MU codecs in their Invite SDP. G.726-32 codec is supported by Communication Manager, but testing found issues when G.726-32 codec is used (see **Section 2.2, item 2**). In addition, some calls could require support of G.729B (silence suppression). Therefore G.729B is also included in the codec lists.

### 5.7.1. 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**, **G.729A**, and **G.729B** are included in the codec list. Note that the packet interval size will default to 20ms. Under **Media Encryption**, ensure **1-srtp-aescm128-hmac80** is included to support Secure Real-time Transport Protocol (SRTP).

<b>change ip-codec-set 1</b>				<b>Page 1 of 2</b>
IP CODEC SET				
Codec Set: 1				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)	
1: G.711MU	n	2	20	
2: G.729A	n	2	20	
3: G.729B	n	2	20	
<b>Media Encryption</b>			Encrypted SRTP: enforce-unenc-srtp	
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>				<b>Page 2 of 2</b>
IP CODEC SET				
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	Redundancy	ECM: y	Packet Size (ms)
<b>FAX</b>	<b>t.38-standard</b>	<b>0</b>		
Modem	off	0		
TDD/TTY	US	3		
H.323 Clear-channel	n	0		
SIP 64K Data	n	0		20



## 5.7.2. Codecs for IP Network Region 4 (calls from AT&T)

**Step 1** - Repeat the steps in **Section 5.7.1** with the following changes.

- Provision the codecs in the order shown below. Note that the order of G.729A and G.729B codecs may be reversed as required.
- Set **Frames Per Pkt** to **3**. This will auto-populate **30** for the **Packet Size (ms)** field, and specify a PTIME value of 30 in the SDP (recommended by AT&T). See **Section 2.2, Item 9** for limitations with the packet size.

change ip-codec-set 4				Page	1 of 2
IP CODEC SET					
Codec Set: 4					
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)		
1: G.729A	n	3	30		
2: G.729B	n	3	30		
3: G.711MU	n	3	30		
Media Encryption				Encrypted SRTCP: enforce-unenc-srtcp	
1: 1-srtp-aescm128-hmac80					
2: none					
change ip-codec-set 4				Page	2 of 2
IP CODEC SET					
Allow Direct-IP Multimedia? n					
	Mode	Redundancy	ECM: y	Packet Size (ms)	
FAX	t.38-standard	0			
Modem	off	0			
TDD/TTY	US	3			
H.323 Clear-channel	n	0			
SIP 64K Data	n	0		20	

**Note:** An additional IP Network Region and IP Codec Set were created in the reference configuration, used to test G.711 pass-through fax. Details of this optional configuration can be found in **Section 14**.

## 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 IPTF access – SIP Trunk 4. This trunk will use TLS port 5064
- Internal CPE access (e.g., Avaya SIP telephones, 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** – While TLS is used as the transport protocols between the Avaya CPE components, UDP was used between the Avaya SBCE and the IPTF service. See the note in **Section 6.5** regarding the use of TLS transport protocol in the CPE.

### 5.8.1. SIP Trunk for Inbound AT&T calls

This section describes the steps for administering the SIP trunk to Session Manager used for inbound IPTF calls. This trunk corresponds to the **CM-TG4** SIP Entity defined in **Section 6.5.2**.

#### 5.8.1.1 Signaling Group 4

**Step 1** - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **4**), 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 systems 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 **5064**.
- **Far-end Network Region** – Set the IP network region to **4**, as set in **Section 5.6.2**.
- **Far-end Domain** – Enter **avayalab.com**. This is the domain provisioned for Session Manager in **Section 6.2**.
- **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).
- **Enable Layer 3 Test** – Set to **y**. This directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.

<b>add signaling-group 4</b>		Page 1 of 2
SIGNALING GROUP		
Group Number: 4	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	Clustered? n
Peer Detection Enabled? y	Peer Server: SM	
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: 5064	Far-end Listen Port: 5064	
	Far-end Network Region: 4	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n	
H.323 Station Outgoing 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 4

**Step 1** - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., 4). On **Page 1** of the **trunk-group** form, provision the following:

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **ATT IPTF**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **\*04**).
- **Direction** – Set to **incoming**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **Step 1** (e.g., 4).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **20**).

<b>add trunk-group 4</b>		Page 1 of 21
TRUNK GROUP		
Group Number: 4	Group Type: sip	CDR Reports: y
Group Name: ATT IPTF	COR: 1	TN: 1 TAC: *04
Direction: incoming	Outgoing Display? n	
Dial Access? n	Night Service:	
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 4	
	Number of Members: 20	

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

- Set the **Preferred Minimum Session Refresh Interval (sec)**: to **900**.

<b>add trunk-group 4</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 4</b>	<b>Page 3 of 21</b>
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
<b>Numbering Format: public</b>	
	UII Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
	Hold/Unhold Notifications? y
Show ANSWERED BY on Display? y	

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

- Set **Telephone Event Payload Type** to the RTP payload type recommended by the IPTF service (e.g., **100**).

**Note** – The IPTF service does not support History Info header. As shown below, by default this header is supported by Communication Manager. In the reference configuration, any History Info headers sent by Communication Manager are automatically removed from SIP signaling by Session Manager, as part of the AttAdapter (see **Section 6.4.2**). Alternatively, History Info may be disabled here.

<b>add trunk-group 4</b>	<b>Page 4 of 21</b>
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? n	
Support Request History? y	
<b>Telephone Event Payload Type: 100</b>	
Shuffling with SDP? n	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? 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.)

This trunk corresponds to the **CM-TG3** SIP Entity defined 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 5.6.1**.

### 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 **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**), is used to convert Communication Manager local extensions to IPTF DNIS numbers, for inclusion in any SIP headers directed to the IPTF 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 any Communication Manager station extensions and their corresponding IPTF DNIS number (for the public trunk):

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the Communication Manager station extension (e.g., SIP phone **89324**). (Not shown).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **4**).
- **CPN Prefix** – Enter the corresponding IPTF DNIS number (e.g., **0000011041**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

**Step 3** - Add any Communication Manager Agent skill VDN extensions and their corresponding IPTF DNIS number (for the public trunk):

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the Communication Manager extension (e.g., Skill VDN **71041**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **4**).
- **CPN Prefix** – Enter the corresponding IPTF DNIS number (e.g., **0000011041**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

**Step 4** - Repeat **Steps 2** and **3** for all IPTF DNIS numbers and their corresponding Communication Manager station, Skill, or Agent extensions.

change public-unknown-numbering 5 ext-digits 71041					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	71041	4	0000011041	15	Total Administered: 20
5	71042	4	0000021042	15	Maximum Entries: 240
5	71043	4	0000031043	15	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	71044	4	0000041044	15	
					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**), 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 Communication Manager extension patterns defined in the Dial Plan in **Section 5.3** (e.g., **20, 71, 89**).
- **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 1					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	12	3		5	Total Administered: 6
5	14	3		5	Maximum Entries: 540
5	20	3		5	
5	71	3		5	
5	89	3		5	

## 5.11. Route Pattern for Local SIP Trunk

Route Patterns are used to direct calls to the Local SIP trunk for access to SIP phones or other destinations in the CPE. This form specifies the local SIP trunk (e.g., 3), based on the route-pattern selected by the AAR table in **Section 5.12** (e.g., calls SIP phone extensions).

**Note** – As IPTF is an inbound only service, no outbound route patterns are defined for the public SIP trunk.



**Step 1** - Enter the **change route-pattern 3** command and enter the following:

- In the **Grp No** column enter **3** for SIP trunk 3 (local trunk).
- In the **FRL** column enter **0** (zero).
- 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:									
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted				DCS/	IXC		
No		Mrk	Lmt	List	Del	Digits				QSIG				
										Dgts	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 Alternate Routing (AAR) Dialing

AAR is used to direct calls to the local SIP trunk for Avaya SIP telephones, using the route pattern defined in **Section 5.11**.

**Step 1** - Enter the following:

- **Dialed String** - In the reference configuration all SIP telephones used extensions in the range 89xxx, therefore enter **89**.
- **Min & Max** - Enter **5**.
- **Route Pattern** - Enter **3**.
- **Call Type** - Enter **lev0**.

<b>change aar analysis 0</b>										Page 1 of 2
AAR DIGIT ANALYSIS TABLE										
Location: all										Percent Full: 1
	<b>Dialed</b>	<b>Total</b>		<b>Route</b>	<b>Call</b>	<b>Node</b>	<b>ANI</b>			
	<b>String</b>	<b>Min</b>	<b>Max</b>	<b>Pattern</b>	<b>Type</b>	<b>Num</b>	<b>Reqd</b>			
20		5	5	3	lev0		n			
<b>89</b>		<b>5</b>	<b>5</b>	<b>3</b>	<b>lev0</b>		<b>n</b>			

## 5.13. Provisioning for Simulated Call Center Functionality

In the reference configuration, a Call Center environment (skill queues and Agents) was simulated on Communication Manager. The administration of Communication Manager Call Center type elements – Agents, skills (hunt groups), vectors, and Vector Directory Numbers (VDNs) are beyond the scope of these Application Notes. Consult [6] and [10] in the References section for further details. The samples that follow are provided for reference purposes only.

- Agent form – **Page 1**

display agent-loginID 20001		Page	1 of 2
AGENT LOGINID			
Login ID: 20001	AAS? n		
Name: Agent 1	AUDIX? n		
TN: 1	Check skill TNs to match agent TN? n		
COR: 2			
Coverage Path: 1	LWC Reception: spe		
Security Code:	LWC Log External Calls? n		
Attribute:	AUDIX Name for Messaging:		
LoginID for ISDN/SIP Display? n			
Password:			
Password (enter again):			
Auto Answer: acd			
MIA Across Skills: system			
AUX Agent Remains in LOA Queue: system			
AUX Agent Considered Idle (MIA): system			
ACW Agent Considered Idle: system			
Work Mode on Login: system			
Aux Work Reason Code Type: system			
Logout Reason Code Type: system			
Maximum time agent in ACW before logout (sec): system			
Forced Agent Logout Time: :			
WARNING: Agent must log in again before changes take effect			

- Agent form – **Page 2**

display agent-loginID 20001		Page	2 of 2
AGENT LOGINID			
Direct Agent Skill:		Service Objective? n	
Call Handling Preference: skill-level		Local Call Preference? n	
SN	RL SL	SN	RL SL
1: 1	1	16:	

- Skill 1 Hunt Group form – Page 1

display hunt-group 1		Page 1 of 4
HUNT GROUP		
Group Number: 1		ACD? y
Group Name: Agent Group		Queue? y
Group Extension: 19991		Vector? y
Group Type: ucd-mia		
TN: 1		
COR: 1		MM Early Answer? n
Security Code:		Local Agent Preference? n
ISDN/SIP Caller Display: grp-name		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	

- Skill 1 VDN form – Page 1

display vdn 71041		Page 1 of 3
VECTOR DIRECTORY NUMBER		
Extension: 71041		
Name*: ATT Toll-Free 1		
<b>Destination: Vector Number</b>	<b>4</b>	
Attendant Vectoring? n		
Meet-me Conferencing? n		
Allow VDN Override? n		
COR: 1		
TN*: 1		
Measured: none		

- Skill 1 Vector form – Page 1

display vector 4		Page 1 of 6
CALL VECTOR		
Number: 4	Name: Call Center	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n Lock? n
Basic? y	EAS? y G3V4 Enhanced? y	ANI/II-Digits? y ASAI Routing? y
Prompting? y	LAI? y G3V4 Adv Route? y	CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y	
01 #	Wait hearing ringback	
02 wait-time	2	secs hearing ringback
03 #	Play greeting and collect 1 digit	
04 collect	1	digits after announcement 11001 for none
05 goto step	7	if digits = 1
06 stop		
07 #	Simple queue to skill with recurring announcement until available	
<b>08 queue-to</b>	<b>skill 1</b>	<b>pri m</b>
09 announcement	11004	
10 wait-time	30	secs hearing music
11 goto step	8	if unconditionally
12 stop		

## 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 additional information for the provisioning of the Medias Gateway see [7] in the References 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., **10.64.91.75**, 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
Network Region: 1                      Location: 1
Use for IP Sync? n                     Site Data:
Recovery Rule: none
Registered? y
FW Version/HW Vintage: 41 .9 .0 /1
MGP IPv4 Address: 10.64.91.91
MGP IPv6 Address:
Controller IP Address: 10.64.91.75
MAC Address: 00:1b:4f:53:37:69
Mutual Authentication? optional
```

## 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 [8] and [9] in the References section 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., **10.64.91.75**, 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., **AMS**).
- **Near-end Listen Port** – Set to **9061** (default).
- **Far-end Listen Port** – Set to **5061** (default).
- **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 5.6.1**.
- **Far-end Domain** – Automatically populated with the IP address of the Media Server.

```
add signaling-group 60                                     Page 1 of 2
                                                         SIGNALING GROUP

Group Number: 60                Group Type: sip
                                Transport Method: tls

Peer Detection Enabled? n    Peer Server: AMS

Near-end Node Name: procr      Far-end Node Name: AMS
Near-end Listen Port: 9061     Far-end Listen Port: 5061
                                Far-end Network Region: 1

Far-end Domain: 10.64.91.86
```

**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: AMS
      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**.

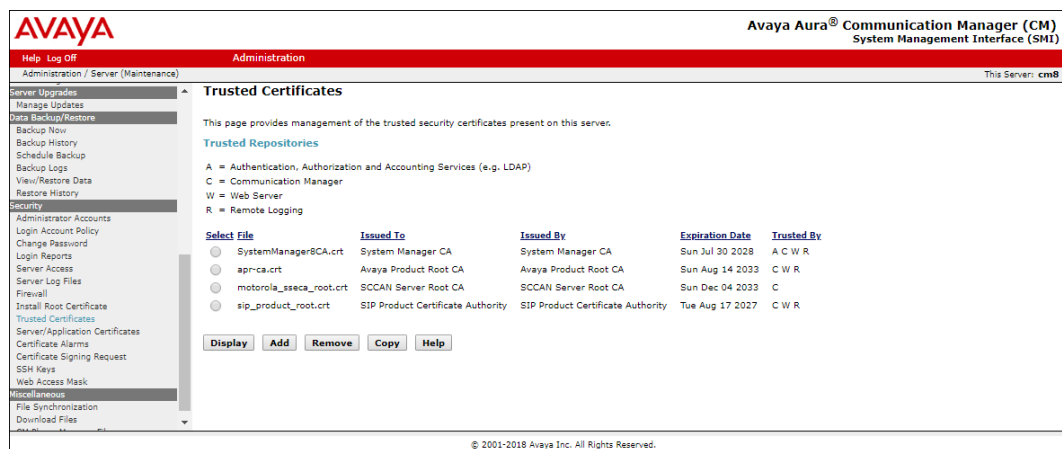
## 5.17. Verify TLS Certificates – Communication Manager

**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.

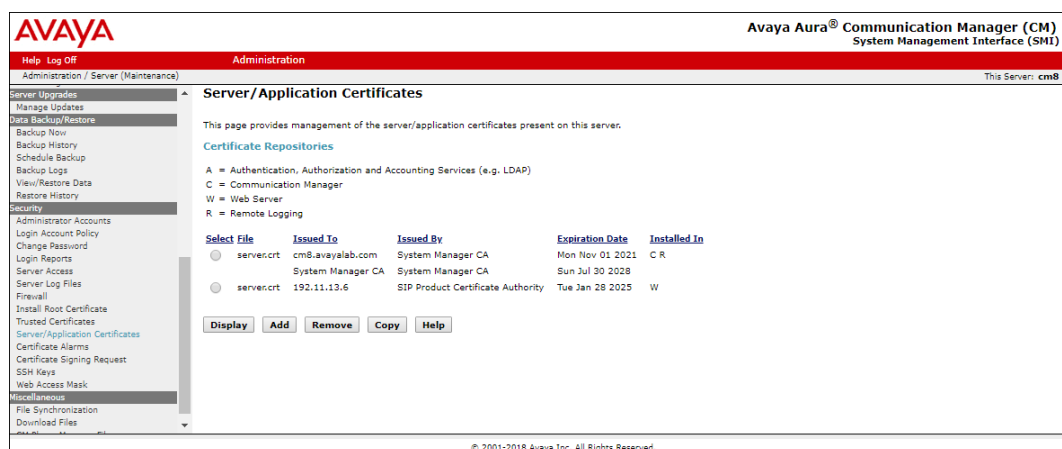
In the reference configuration, TLS transport is used for the communication between Session Manager and Communication Manager. The following procedures show how to verify the certificates used by Communication Manager.

**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.



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



## 6. Configure Avaya Aura® Session Manager

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

This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Communication Manager and Session Manager, and the SIP trunk between Session Manager and the Avaya SBCE. In addition, provisioning for calls to Avaya Experience Portal and Messaging are described.

Session Manager serves as a central point for supporting SIP-based communication services in an enterprise. Session Manager connects and normalizes disparate SIP network components and provides a central point for external SIP trunking to the PSTN. The various SIP network components are represented as SIP Entities and the connections/trunks between Session Manager and those components are represented as Entity Links.

When calls arrive at Session Manager from a SIP Entity, Session Manager applies SIP protocol and numbering modifications to the calls. These modifications, referred to as Adaptations, are sometimes necessary to resolve SIP protocol differences between disparate SIP Entities, and also serve the purpose of normalizing the calls to a common or uniform numbering format, which allows for simpler administration of routing rules in Session Manager. Session Manager then matches the calls against certain criteria embodied in profiles termed Dial Patterns and determines the destination SIP Entities based on Routing Policies specified in the matching Dial Patterns. Lastly, before the calls are routed to the respective destinations, Session Manager again applies Adaptations in order to bring the calls into conformance with the SIP protocol interpretation and numbering formats expected by the destination SIP Entities.

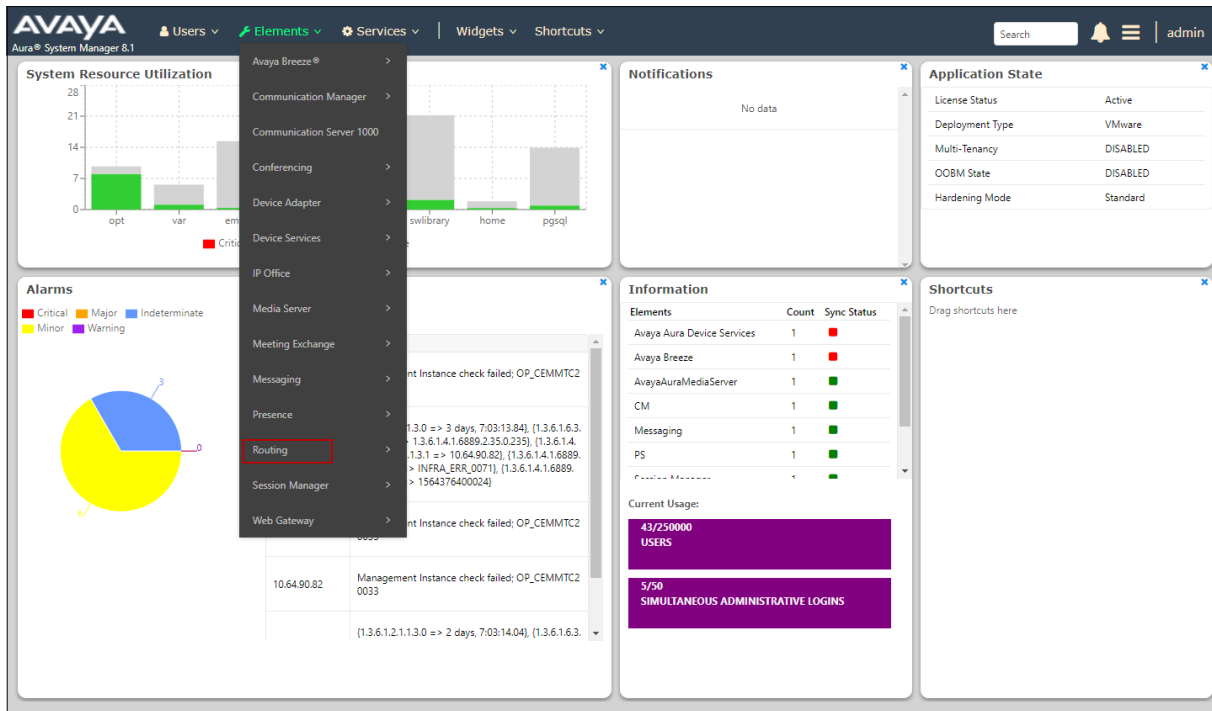
The following administration activities will be described:

- 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 the 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.

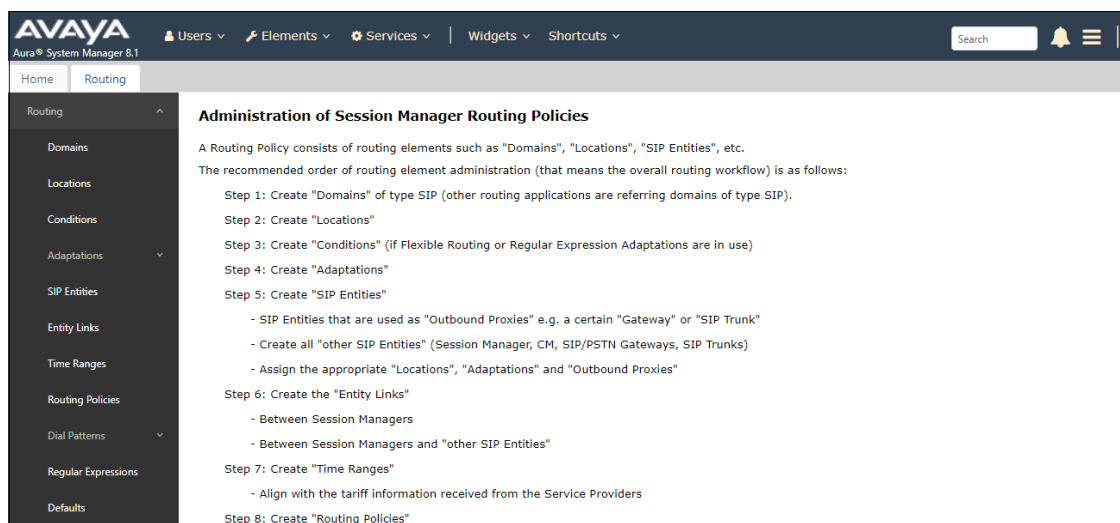


## 6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, **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.



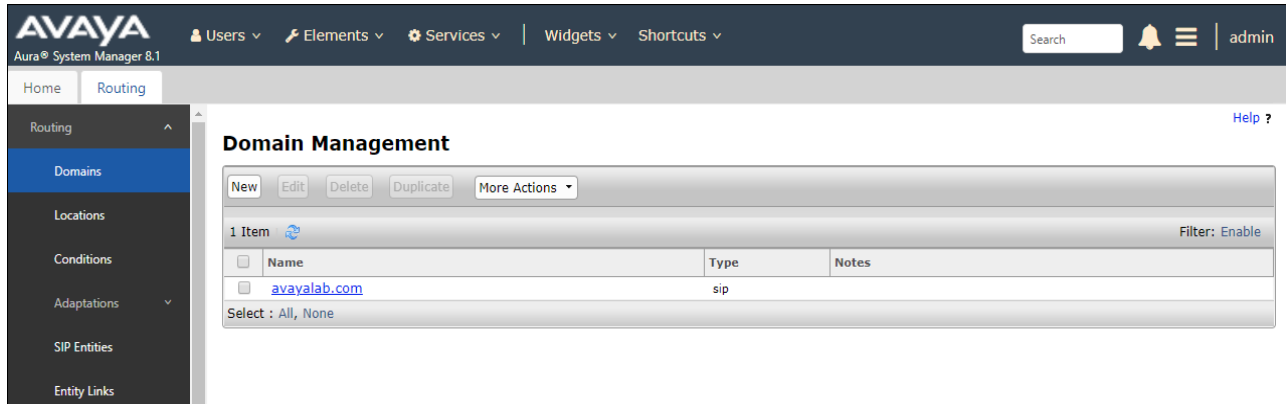
## 6.2. SIP Domain

**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** to save (not shown).



## 6.3. Locations

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

- **Main** – The customer site containing System Manager, Session Manager, Communication Manager, SIP endpoints, etc.
- **Common SBCs**– This site contains the 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.

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The left-hand navigation pane shows the 'Locations' menu item selected. The main content area is titled 'Location Details' and includes a 'Commit' button. The 'General' section contains fields for 'Name' (set to 'Main') and 'Notes' (set to 'Avaya SIL'). Below this, the 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox. The 'Overall Managed Bandwidth' section includes fields for 'Managed Bandwidth Units' (set to 'Kbit/sec'), 'Total Bandwidth', and 'Multimedia Bandwidth', along with a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section contains fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth' (set to '64 Kbit/Sec'), and 'Default Audio Bandwidth' (set to '80 Kbit/sec'). The 'Alarm Threshold' section includes fields for 'Overall Alarm Threshold' and 'Multimedia Alarm Threshold' (both set to '80 %'), and checkboxes for 'Latency before Overall Alarm Trigger' and 'Latency before Multimedia Alarm Trigger' (both set to '5 Minutes'). At the bottom, there is a 'Location Pattern' section with an 'Add' button and a table with columns for 'IP Address Pattern' and 'Notes'.

### 6.3.2. Common-SBCs Location

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

- **Name:** Enter a descriptive name for the Location (e.g., **Common-SBCs**).

## 6.4. Configure Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers sent to/from AT&T to Communication Manager.

- Inbound messages - Modification of SIP messages sent to Communication Manager extensions. (**Section 6.4.1**)
  - The AT&T called number digit string in the Request URI is replaced with the associated Communication Manager extensions defined for Agent skill queue VDNs/telephones.
- Outbound messages - Modification of SIP messages sent by Communication Manager extensions. (**Section 6.4.2**)
  - The History-Info header is removed automatically by the **AttAdapter**.
  - Avaya SIP headers not required by AT&T are removed.

### 6.4.1. Adaptation for Avaya Aura® Communication Manager Extensions

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

**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-TG4-IPTF**).
2. Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select **<click to add module>** and enter **DigitConversionAdapter**).

The screenshot shows the 'Adaptation Details' configuration page. On the left, a navigation pane under 'Routing' has 'Adaptations' selected. The main content area is titled 'Adaptation Details' and includes a 'General' tab. The form contains the following fields: 'Adaptation Name' with the value 'CM-TG4-IPTF', 'Module Name' with a dropdown menu showing 'DigitConversionAdapter', 'Module Parameter Type' with a dropdown arrow, 'Egress URI Parameters' with an empty text box, and 'Notes' with the text 'CM - ATT - IPTF'. At the top right of the form are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

**Step 3** - Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the inbound digits from AT&T that need to be replaced with their associated Communication Manager extensions before being sent to Communication Manager). 0000011041 is a DNIS string sent in the Request URI by the IPTF service that is associated with Communication Manager Agent/VDN skill queue 71041.

- Enter **0000011041** in the **Matching Pattern** column.
- Enter **10** in the **Min/Max** columns.
- Enter **6** in the **Delete Digits** column.
- Enter **7** in the **Insert Digits** column to convert the number to 71041, a Vector Directory Number (VDN) in Communication Manager.
- 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 IPTF DNIS numbers//Communication Manager extensions.

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

Digit Conversion for Outgoing Calls from SM										
Add		Remove								
5 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"/>	*0000011041	*10	*10		*6	7	destination ▼		10 digit DNIS to VDN Conversion	
<input type="checkbox"/>	*0000021042	*10	*10		*6	7	destination ▼		10 digit DNIS to VDN Conversion	
<input type="checkbox"/>	*0000031043	*10	*10		*6	7	destination ▼		10 digit DNIS to VDN Conversion	
<input type="checkbox"/>	*0000041044	*10	*10		*6	7	destination ▼		10 digit DNIS to VDN Conversion	
<input type="checkbox"/>	*0000051045	*10	*10		*6	7	destination ▼		10 digit DNIS to VDN Conversion	

Select : All, None

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

## 6.4.2. Adaptation for the AT&T IP Toll Free Service

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

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

- A descriptive **Name**, (e.g., **SBC1-Adaptation for ATT**).
- Select **AttAdapter** from the **Module Name** drop down menu (if no module name is present, select **<click to add module>** and enter **AttAdapter**). The AttAdapter will automatically remove History-Info headers, (which the IPTF service does not support), sent by Communication Manager (see **Section 5.8.1**).

**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:

- **Name** – Enter **eRHdrs**
- **Value** – Enter the following Avaya headers to be removed by Session Manager. Note that each header name is separated by a comma with no spaces in between. If spaces are used after the comma, the string needs to be enclosed in quotes:  
**AV-Global-Session-ID,Alert-Info,Endpoint-View,P-AV-Message-Id,P-Charging-Vector,P-Location,AV-Correlation-ID,Av-Secure-Indication**

**Note** – As shown in the screen below, no Incoming or Outgoing Digit Conversion was required in the reference configuration.

The screenshot shows the 'Adaptation Details' configuration page. On the left is a navigation menu with options: Routing, Domains, Locations, Conditions, Adaptations (selected), Regular Expression..., SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a 'General' tab and buttons for 'Commit' and 'Cancel'. The configuration fields are as follows:

- Adaptation Name:** SBC1-Adaptation for ATT
- Module Name:** AttAdapter (selected from a dropdown)
- Module Parameter Type:** Name-Value Parameter (selected from a dropdown)

Below these fields is a table for Name-Value Parameters:

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

Below the table is a 'Select' dropdown menu with options: All, None. Further down are fields for 'Egress URI Parameters' and 'Notes' (SBC - ATT IPTF).

There are two sections for digit conversion, both currently showing '0 Items':

- Digit Conversion for Incoming Calls to SM:** Includes a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes. A 'Filter: Enable' link is present.
- Digit Conversion for Outgoing Calls from SM:** Includes a similar table and a 'Filter: Enable' link.

## 6.5. SIP Entities

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

- Session Manager (**Section 6.5.1**). Note that this Entity is normally created during Session Manager installation but is shown here for completeness.
- Communication Manager for AT&T access (**Section 6.5.2**) – This entity, and its associated Entity Link (using TLS with port 5064, is for calls from the IPTF service to Communication Manager via the Avaya SBCE.
- Communication Manager for local access (**Section 6.5.3**) – This entity, and its associated Entity Link (using TLS with port 5061), is primarily used for traffic between Avaya SIP telephones and Communication Manager.
- Avaya SBCE (**Section 6.5.4**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls from the IPTF service via the Avaya SBCE.
- Experience Portal (**Section 6.5.5**) – 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 5064), and to the Avaya SBCE (port 5061). The connection between the Avaya SBCE and the AT&T IPTF service uses UDP/5060 per AT&T 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., **10.64.91.81**).
- **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 **SIP 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.

**Step 4** - Scrolling down to the **Port** section of the **SIP Entity Details** page, click on **Add** and provision entries as follow:

- **Port** – Enter **5061**
- **Protocol** – Select **TLS**
- **Default Domain** – Select a SIP domain administered in **Section 6.2** (e.g., **avayalab.com**)

**Step 5** - Repeat **Step 4** to provision entries for any other listening ports used by Session Manager for SIP telephones. These are separate from the ports defined for the Entity Links in **Section 6.6**.

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

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

**Note** – The **Entity Links** section of these forms (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-TG4**).
- **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Sections 5.4** and **5.5** (e.g., **10.64.91.75**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **CM-TG4-IPTF** administered in **Section 6.4.1**.
- **Location** – Select a Location **Main** administered in **Section 6.3.1**.
- **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**.

The screenshot shows the 'SIP Entity Details' page with the 'General' tab selected. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- Name:** CM-TG4
- FQDN or IP Address:** 10.64.91.75
- Type:** CM
- Notes:** Trunk Group 4 - ATT IPTF
- Adaptation:** CM-TG4-IPTF
- Location:** Main
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty field)
- Securable:** ☐
- Call Detail Recording:** none

The 'Loop Detection' section contains:

- Loop Detection Mode:** On
- Loop Count Threshold:** 5
- Loop Detection Interval (in msec):** 200

The 'Monitoring' section contains:

- SIP Link Monitoring:** Use Session Manager Configuration
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration

### 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-Toll Free**).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.64.91.41**), see **Section 8.3**.
- **Type** – Select **SIP Trunk**.
- **Adaptations** – Select Adaptation **SBC1-Adaptation for ATT** (**Section 6.4.2**).
- **Location** – Select Location **Common-SBCs** administered in **Section 6.3.2**.

### 6.5.5. Avaya Aura® Experience Portal SIP Entity

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

- **Name** – Enter a descriptive name (e.g., **ExperiencePortal**).
- **FQDN or IP Address** – Enter the IP address of Experience Portal (e.g., **10.64.91.90**, see **Section 3.1**).
- **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 Experience Portal (**Section 6.6.4**).

**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 TG4**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 6.5.1** for Session Manager (e.g., **Session Manager**).
- **SIP Entity 1 Port** – Enter **5064**.
- **Protocol** – Select **TLS** (see **Section 5.8.1**).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.2** for the Communication Manager public entity (e.g., **CM-TG4**).
- **SIP Entity 2 Port** – Enter **5064** (see **Section 5.8.1**).
- **Connection Policy** – Select **trusted**.

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

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
* SM to CM TG4	* Session Manager	TLS	* 5064	* CM-TG4	* 5064	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

## 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 AT&T IP Toll Free 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 SBCE-TollFree**).
- **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., **SBCE-Toll Free**).
- **SIP Entity 2 Port** – Enter **5061**.

## 6.6.4. Entity Link to Avaya Aura® 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 ExperiencePortal**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.5** for the Experience Portal entity (e.g., **ExperiencePortal**).
- **SIP Entity 2 Port** – Enter **5061**.

## 6.7. Time Ranges – (Optional)

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

**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**. 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 Experience Portal (**Section 6.8.2**).

### 6.8.1. Routing Policy for AT&T Routing to Avaya Aura® Communication Manager

This Routing Policy is used for inbound calls from IPTF.

**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 AT&T calls to Communication Manager (e.g., **To CM TG4**), 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 Entity list page will open.

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

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**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-TG4**), and click on **Select**.

SIP Entities				
13 Items				
	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	Aura Messaging	10.64.91.84	Messaging	Aura Messaging
<input type="radio"/>	Breeze	10.64.91.18	Avaya Breeze	
<input type="radio"/>	CM-TG1	10.64.91.75	CM	Trunk Group 1 - CM to Vz-IPT
<input type="radio"/>	CM-TG2	10.64.91.75	CM	Trunk Group 2 - Vz-Toll-Free inbound
<input type="radio"/>	CM-TG3	10.64.91.75	CM	Trunk Group 3 - CM to Enterprise
<input checked="" type="radio"/>	CM-TG4	10.64.91.75	CM	Trunk Group 4 - ATT IPTF
<input type="radio"/>	CM-TG5	10.64.91.75	CM	Trunk Group 5 - ATT IPFR
<input type="radio"/>	IP500	10.64.19.70	Other	IP Office
<input type="radio"/>	Presence	10.64.91.18	Presence Services	
<input type="radio"/>	SBC1	10.64.91.50	SIP Trunk	Avaya SBC-1 to PSTN
<input type="radio"/>	SBC2	10.64.91.100	SIP Trunk	Avaya SBC-2 to PSTN
<input type="radio"/>	SBCE-ATT	10.64.91.40	SIP Trunk	SBCE for AT&T testing
<input type="radio"/>	SBCE-Toll Free	10.64.91.41	SIP Trunk	SBCE for IPTF testing
Select : None				

**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.

The screenshot shows the 'Routing Policy Details' form in the 'Time of Day' section. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (selected), Dial Patterns, Regular Expressions, and Defaults. The main form area has a 'Commit' button and a 'Cancel' button. The 'General' section includes fields for 'Name' (To CM TG4), 'Disabled' (unchecked), 'Retries' (0), and 'Notes' (Trunk Group 4 PSTN4 to CM). The 'SIP Entity as Destination' section has a 'Select' button and a table with columns: Name, FQDN or IP Address, Type, and Notes. The table contains one row: CM-TG4, 10.64.91.75, CM, Trunk Group 4 - ATT IPTF. The 'Time of Day' section has an 'Add' button, a 'Remove' button, and a 'View Gaps/Overlaps' button. Below these is a table with columns: Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes. The table contains one row: 0, 24/7, and checkboxes for Mon through Sun, all of which are checked. The Start Time is 00:00 and the End Time is 23:59. The table has a 'Filter: Enable' button and a 'Select: All, None' button.

Name	FQDN or IP Address	Type	Notes
CM-TG4	10.64.91.75	CM	Trunk Group 4 - ATT IPTF

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

## 6.8.2. 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 6.5.5** for Experience Portal (e.g., **ExperiencePortal**).

## 6.9. Dial Patterns

In this section, the following task are administered:

- Origination Dial Pattern for inbound calls arriving from the local area code.
- Dial Pattern for inbound PSTN calls via the IPTF service to Communication Manager.
- Dial Pattern for inbound PSTN calls via the IPTF service to Experience Portal.

### 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**.

**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**.

**Origination Dial Pattern Set Details** Commit Cancel Help ?

**General**

\* **Name:**

**Notes:**

**Origination Dial Patterns**

New Edit Delete

0 Items Filter: Enable

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

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 Help ?

1 Item Filter: Enable

Pattern	Min	Max	SIP Domain	Notes
<input type="checkbox"/> *786331	*10	*10	avayalab.com	

Select : All, None

Commit Cancel

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

**Origination Dial Pattern Set Details** Commit Cancel Help ?

**General**

\* Name:

Notes:

**Origination Dial Patterns**

New Edit Delete

1 Item Filter: Enable

Pattern	Min	Max	SIP Domain	Notes
<input type="checkbox"/> 786	10	10	avayalab.com	

Select : All, None

Commit Cancel



## 6.9.2. Dial Pattern for Inbound Calls to Communication Manager

**Note** – In the reference configuration inbound calls from the IPTF service sent 10 DNIS digits in the SIP Request URI. Be sure to match on the digit string specified in the AT&T Request URI, not the digit string of the number dialed. They may be different.

**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** – In the reference configuration, AT&T sends a 10-digit number in the Request URI with the format 00000xxxxx. Enter **00000**.
- **Min** – Enter **6**.
- **Max** – Enter **21**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.

**Note** – The Adaptation defined for Communication Manager in **Section 6.4.1** will convert the various 00000xxxxx numbers into their corresponding Communication Manager extensions.

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

**General**

\* **Pattern:** 00000

\* **Min:** 6

\* **Max:** 21

**Emergency Call:** ☐

**SIP Domain:** avayalab.com

**Notes:** ATT TF Inbound

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

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

1 Item

	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"/>	Common-SBCs	SBC to PSTN			To CM TG4	0	<input type="checkbox"/>	CM-TG4	Trunk Group 4 PSTN4 to CM

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

**Step 4** - In the **Originating Location** section of the **Originating Locations, Origination Dial Pattern Sets and Routing Policies** page, check the checkbox corresponding to the location assigned to the Avaya SBCE in **Section 6.3.2**, e.g., **Common-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 TG4**). Click on **Select** (not shown).

**Originating Location**

Select

Cancel

**Originating Location**

☐ Apply The Selected Routing Policies to All Originating Locations

5 Items

Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	CM-TG-5	CM-TG-5
<input checked="" type="checkbox"/>	Common-SBCs	SBC to PSTN
<input type="checkbox"/>	Experience Portal	
<input type="checkbox"/>	Main	Avaya SIL
<input type="checkbox"/>	RemoteAccess	Remote Access from SBCE1

Select : All, None

**Origination Dial Pattern Sets**

☐ Calls from local area code

1 Item

Filter: Enable

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

Select : None

**Routing Policies**

☐ To AAM
☐ To CM TG1
☐ To CM TG2
☐ To CM TG3
☒ To CM TG4
☐ To CM-TG5
☐ To CM TG7
☐ To Experience Portal

Disabled

Destination

Notes

13 Items

Filter: Enable

<input type="checkbox"/>	To AAM	<input type="checkbox"/>	Aura Messaging	
<input type="checkbox"/>	To CM TG1	<input type="checkbox"/>	CM-TG1	Trunk Group 1 PSTN1 to CM
<input type="checkbox"/>	To CM TG2	<input type="checkbox"/>	CM-TG2	Trunk Group 2 VzIPCC to CM
<input type="checkbox"/>	To CM TG3	<input type="checkbox"/>	CM-TG3	Enterprise Traffic
<input checked="" type="checkbox"/>	To CM TG4	<input type="checkbox"/>	CM-TG4	Trunk Group 4 PSTN4 to CM
<input type="checkbox"/>	To CM-TG5	<input type="checkbox"/>	CM-TG5	Trunk Group 5 PSTN to CM
<input type="checkbox"/>	To CM TG7	<input type="checkbox"/>	CM-TG7	Incoming calls from Masergy
<input type="checkbox"/>	To Experience Portal	<input type="checkbox"/>	ExperiencePortal	

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

**Step 7** - Repeat **Steps 1-6** for any additional inbound dial patterns from AT&T to Communication Manager.

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

In the reference configuration, one the AT&T IPTF numbers, corresponding to DNIS 0000021042, 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 DNIS digits corresponding to the AT&T IPTF number assigned for calls to Experience Portal (e.g., **0000021042**).
- **Min** – Enter **10**.
- **Max** – Enter **10**

Routing

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

Dial Pattern Details

CommitCancel

Help ?

General

\* Pattern: 0000021042

\* Min: 10

\* Max: 10

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: AT&T IPTF for Exp Portal (local area)

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

AddRemove

0 Items

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
<div>Denied Originating Locations and Origination Dial Pattern Sets</div> <div>AddRemove</div> <div>0 Items</div>								

**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**).

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

5 Items

Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	CM-TG-5	CM-TG-5
<input checked="" type="checkbox"/>	Common-SBCs	SBC to PSTN
<input type="checkbox"/>	Experience Portal	
<input type="checkbox"/>	Main	Avaya SIL
<input type="checkbox"/>	RemoteAccess	Remote Access from SBCE1

Select : All, None

Originating 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

13 Items

Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To AAM	<input type="checkbox"/>	Aura Messaging	
<input type="checkbox"/>	To CM TG1	<input type="checkbox"/>	CM-TG1	Trunk Group 1 PSTN1 to CM
<input type="checkbox"/>	To CM TG2	<input type="checkbox"/>	CM-TG2	Trunk Group 2 VzIPCC to CM
<input type="checkbox"/>	To CM TG3	<input type="checkbox"/>	CM-TG3	Enterprise Traffic
<input type="checkbox"/>	To CM TG4	<input type="checkbox"/>	CM-TG4	Trunk Group 4 PSTN4 to CM
<input type="checkbox"/>	To CM-TG5	<input type="checkbox"/>	CM-TG5	Trunk Group 5 PSTN to CM
<input type="checkbox"/>	To CM TG7	<input type="checkbox"/>	CM-TG7	Incoming calls from Masergy
<input checked="" type="checkbox"/>	To Experience Portal	<input type="checkbox"/>	ExperiencePortal	
<input type="checkbox"/>	To SBC1	<input type="checkbox"/>	SBC1	
<input type="checkbox"/>	To SBC2	<input type="checkbox"/>	SBC2	

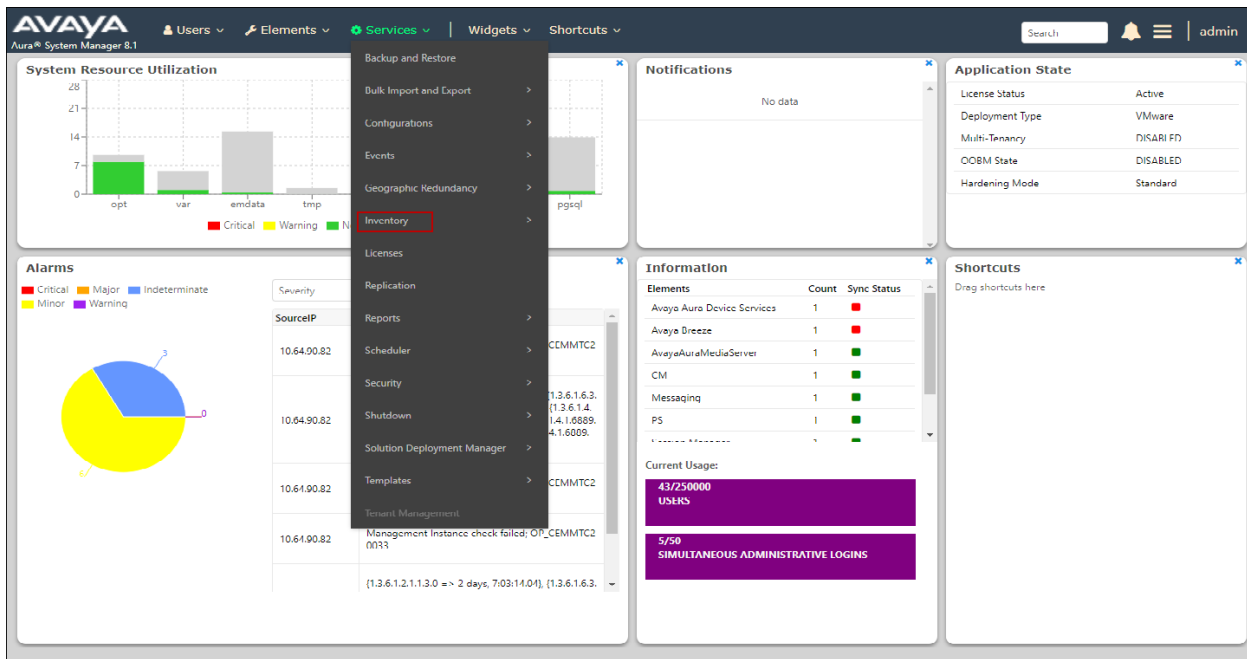
With this configuration, calls to this IPTF number originating from the local area code will be routed to Experience Portal, while calls to this same number originating from area codes other than the local area will still be routed to Communication Manager, following the dial pattern shown previously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

## 6.10. Verify TLS Certificates – Session Manager

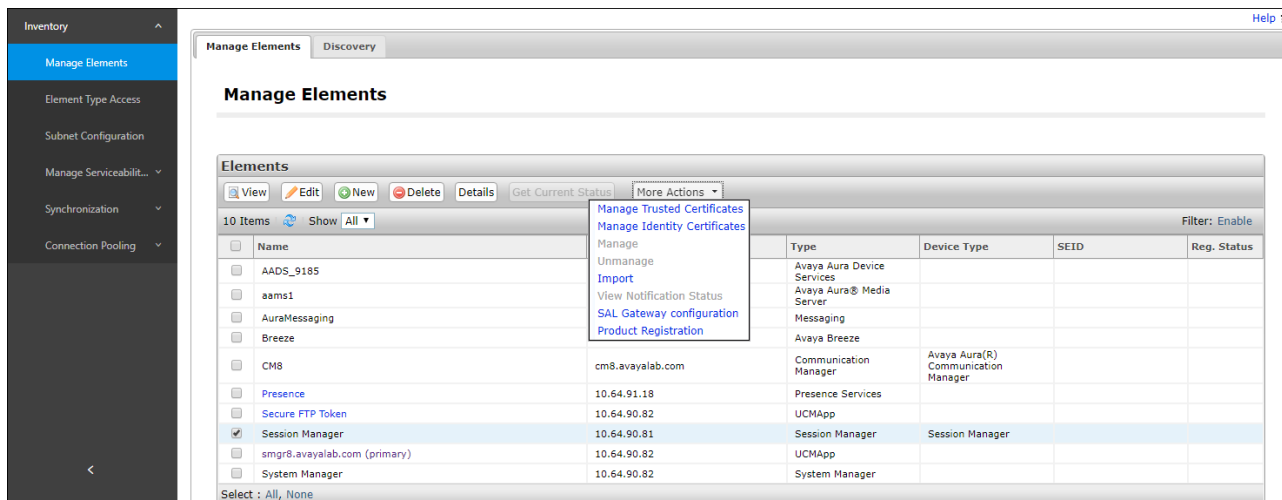
**Note** – Testing was done with System Manager signed identity certificates. The procedure to obtain and install certificates is outside the scope of these Application Notes.

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

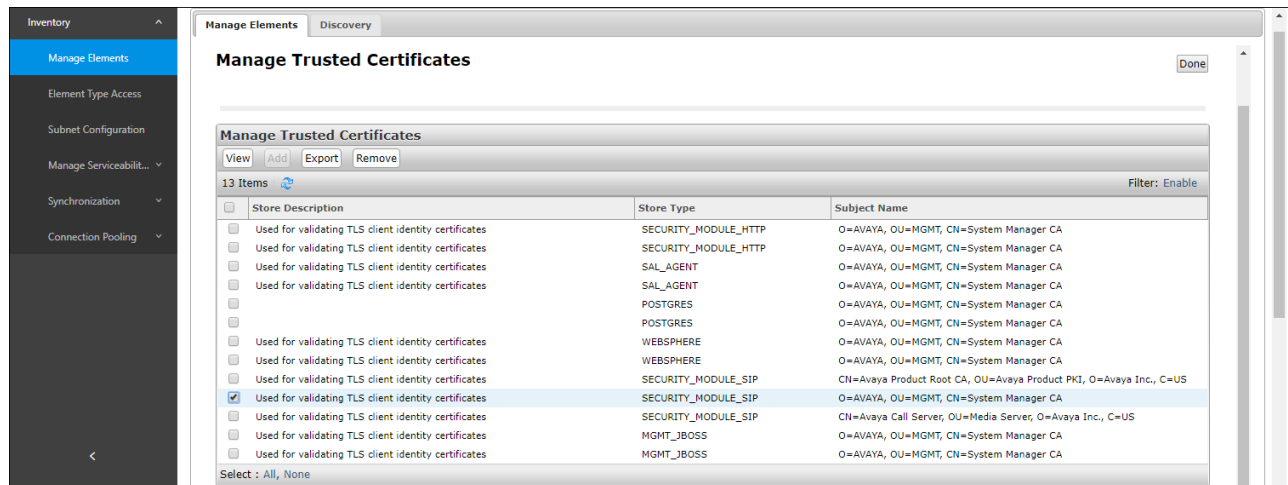
**Step 1** - From the **Home** screen, under the **Services** heading, select **Inventory**.



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

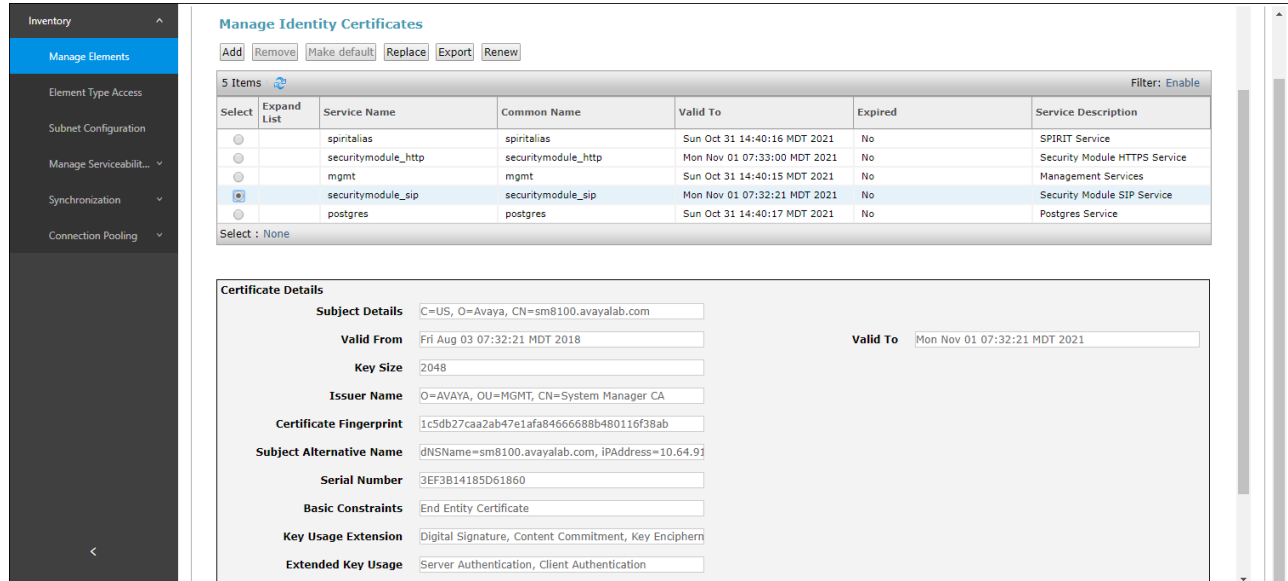


**Step 3** - Verify the System Manager Certificate Authority certificate is listed in the trusted store, **SECURITY\_MODULE\_SIP**. Click **Done** to return to the previous screen.



**Step 4** - With Session Manager selected, click on **More Actions** → **Configure 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**.



## 7. Configure Avaya Aura® Experience Portal

These Application Notes assume that the necessary Experience Portal licenses have been installed and basic Experience Portal administration has already been performed. Consult [13] and [14] in the 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>2</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 AT&T IPTF 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>2</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.

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

**Avaya Aura® Experience Portal 7.2.3 (ExperiencePortal)**

Welcome, eadmin  
Last logged in Oct 9, 2019 at 7:14:38 AM PDT

Home ?- Help Logoff

You are here: Home

### Avaya Aura® Experience Portal Manager

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

#### Installed Components

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

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

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

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

#### Legal Notice

AVAYA GLOBAL SOFTWARE LICENSE TERMS  
REVISED: May 22, 2019

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

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

You are here: Home > Security > Licensing

### Licensing

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

**License Server Information**

License Server URL:	https://10.64.91.90:8443/WebLM/LicenseServer
Last Updated:	Oct 24, 2018 2:19:25 PM PDT
Last Successful Poll:	Oct 15, 2019 6:24:07 AM PDT

**Licensed Products**

Product	Count	Status
Experience Portal		
Announcement Ports:	100	
ASR Connections:	100	
Call Anchoring Ports:	0	
Email Units:	10	
Enable Media Encryption:	1	
Enhanced Call Classification:	100	
Google ASR Connections:	0	
Google Dialogflow Connections:	0	
HTML Units:	100	
SIP Signaling Connections:	100	
SMS Units:	10	
Telephony Ports:	100	
TTS Connections:	100	
Video Server Connections:	100	
Zones:	1	
Version:	7	
Last Successful Poll:	Oct 15, 2019 6:24:07 AM PDT	
Last Changed:	Aug 14, 2019 6:34:46 PM PDT	

## 7.3. 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.

Expand All | Collapse All

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

### VoIP Connections

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

H.323 SIP

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

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

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

- **Name** – Set to a descriptive name (e.g., **SM8**).
- **Enable** – Set to **Yes**.
- **Proxy Server Transport** – Set to **TLS**.
- Select **Proxy Servers**, and enter:
  - **Proxy Server Address** = **10.64.91.81** (the IP address of the Session Manager signaling interface defined in **Section 6.5.1**).
  - **Port** = **5061**
  - **Priority** = **0** (default)
  - **Weight** = **0** (default)
- **Listener Port** – Set to **5061**.
- **SIP Domain** – Set to **avayalab.com** (**Section 6.2**).
- **Consultative Transfer** – Select **REFER**.
- **SIP Reject Response Code** – Select **ASM (503)**.
- **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In the reference configuration a value of **10** was used.
- Select **All Calls can be either inbound or outbound**.
- **SRTP Enable** = **Yes**
- **Encryption Algorithm** = **AES\_CM\_128**
- **Authentication Algorithm** = **HMAC\_SHA1\_80**
- **RTCP Encryption Enabled** = **No**
- **RTP Authentication Enabled** = **Yes**
- Use default values for all other fields.
- Click **Save**.



Expand All | Collapse All

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

## Change SIP Connection

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

Name: SM8

Enable: ☒ Yes ☐ No

Proxy Transport: TLS

☒ Proxy Servers ☐ DNS SRV Domain

Address	Port	Priority	Weight	
10.64.91.81	5061	0	0	Remove

[Additional Proxy Server](#)

Listener Port: 5061

SIP Domain: avayalab.com

P-Asserted-Identity:

Maximum Redirection Attempts: 2

Consultative Transfer: ☐ INVITE with REPLACES ☒ REFER

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

### SIP Timers

T1: 250 milliseconds

T2: 2000 milliseconds

B and F: 4000 milliseconds

### Call Capacity

Maximum Simultaneous Calls: 10

☒ All Calls can be either inbound or outbound

☐ Configure number of inbound and outbound calls allowed

### SRTP

Enable: ☒ Yes ☐ No

Encryption Algorithm: ☒ AES\_CM\_128 ☐ NONE

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

RTCP Encryption Enabled: ☐ Yes ☒ No

RTP Authentication Enabled: ☒ Yes ☐ No

**Add**

### Configured SRTP List

<No SRTP List>

## 7.4. Speech Servers

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

Expand All | Collapse All

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

## Speech Servers

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

ASR TTS

	Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed ASR Resources	Languages
<input type="checkbox"/>	LVASR	Yes	10.64.101.83	LumenVox	MRCP V2 TCP	5060	10	en-US

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

## 7.5. Application References

This section describes the steps for administering a reference to the VXML and/or CCXML applications residing on the application server. In the sample configuration, the applications were co-resident on one Experience Portal server, with IP Address 10.64.90.91.

**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.
- **ASR and TTS Speech Servers** – 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 IPTF DNIS number 0000021042 was used (**Section 6.9.3**). Repeat to define additional called party numbers as needed. Inbound AT&T IPTF calls with these called party numbers will be handled by the application defined in this section.

Expand All | Collapse All

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

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

### Change Application

Use this page to change the configuration of an application.

Name: Test-ccxml

Enable: ☒ Yes ☐ No

Type: CCXML

Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum

Requested:

URI

☒ Single ☐ Fail Over ☐ Load Balance

CCXML URL:  [Verify](#)

Mutual Certificate Authentication: ☐ Yes ☒ No

Basic Authentication: ☐ Yes ☒ No

ASR Speech Servers ▶

TTS Speech Servers ▶

Application Launch ▼

☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number:  [Add](#)

8668512649

3032489329

0000021042

[Remove](#)

SIP Header Source: Any

Speech Parameters ▶

Reporting Parameters ▶

Advanced Parameters ▶

[Save](#) [Apply](#) [Cancel](#) [Help](#)

## 7.6. MPP Servers and VoIP Settings

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

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

Expand All | Collapse All

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: CN=ep.avayalab.com,O=Avaya,OU=EPH  
Issuer: CN=ep.avayalab.com,O=Avaya,OU=EPH  
Serial Number: 89f44cd176674542  
Signature Algorithm: SHA256withRSA  
Valid from: October 17, 2018 11:03:28 AM PDT until October 14, 2028 11:03:28 AM PDT  
Certificate Fingerprints  
MD5: dd:26:1a:d3:d1:62:d3:04:55:40:1b:98:0b:38:44:46  
SHA: 4d:26:ba:2f:55:8d:3b:5f:8e:d0:6f:ee:7f:48:49:22:38:79:ae:bf  
SHA-256: 17:6d:d2:9a:9b:ee:e3:35:da:67:c2:99:38:e6:14:03:c7:84:1d:94:a9:a0:f9:ac:66:57:da:28:43:59:ae:c7  
Subject Alternative Names  
DNS Name: ep  
DNS Name: ep.avayalab.com  
IP Address: 10.64.91.90

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

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

For incoming calls from AT&T IPTF services to Experience Portal, AT&T specifies the value 100 for the RFC2833 telephone-events that signal DTMF digits entered by the user. When Experience Portal answers, the SDP from Experience Portal matches this offered value.

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

- Access Experience Portal via the command line interface.
- Navigate to the following directory: /opt/Avaya/ ExperiencePortal /MPP/config
- Edit the file mppconfig.xml.
- Search for the parameter “mpp.sip.rfc2833.payload”. If there is no such parameter specified, add a line such as the following to the file, where the value 100 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">100</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 the MPP is running after the restart completion.

The screenshot shows the Experience Portal MPP Manager GUI. 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 "MPP Manager (Oct 15, 2019 7:30:39 AM PDT)" and includes a "Refresh" button. Below the title, there is a descriptive text and a "Last Poll" timestamp. A table displays the current state of each MPP. The table has columns for Server Name, Mode, State, Config, Auto Restart, Restart Schedule (Today, Recurring), and Active Calls (In, Out). The first row shows mpp1 in Online Running state with OK config and Yes auto restart. Below the table, there are sections for State Commands (Start, Stop, Restart, Reboot, Halt, Cancel), Mode Commands (Offline, Test, Online), and Restart/Reboot Options (One server at a time, All servers). A Help button is located at the bottom left of the main content area.

Server Name	Mode	State	Config	Auto Restart	Restart Schedule	Active Calls		
					Today	Recurring	In	Out
mpp1	Online	Running	OK	Yes	No	None	0	0

## 8. Configure Avaya Session Border Controller for Enterprise

**Note:** Only the Avaya SBCE provisioning required for the reference configuration is described in these Application Notes.

**Note:** The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to [11] and [12] in the References section for additional information.

**Note:** The Avaya SBCE supports a Remote Worker configuration whereby Communication Manager SIP endpoints residing on the public side of the Avaya SBCE, can securely register/operate as a “local” Communication Manager station in the private CPE. While Remote Worker functionality was tested in the reference configuration, Remote Worker provisioning is beyond the scope of this document.

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.



**AVAYA**

**Session Border Controller  
for Enterprise**

**Log In**

Username:

Password:

WELCOME TO AVAYA SBC

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

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

© 2011 - 2019 Avaya Inc. All rights reserved.

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 displays 'Session Border Controller for Enterprise' and the Avaya logo. The left-hand menu lists 'EMS Dashboard' with sub-items: Device Management, System Administration, Backup/Restore, and Monitoring & Logging. The main content area is titled 'Dashboard' and contains several sections: 'Information' (System Time, Version, Build Date, License State, Aggregate Licensing Overages, Peak Licensing Overage Count, Last Logged in at, Failed Login Attempts), 'Installed Devices' (listing EMS SBCE8-70), 'Active Alarms (past 24 hours)' (None found), 'Incidents (past 24 hours)' (None found), and 'Notes' (No notes found).

## 8.1. Device Management – Status

**Step 1** - 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 **SBCE8-70** is shown. Verify that the **Status** column shows **Commissioned**. If not, contact your Avaya representative.

**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, specifically the 'Device Management' section. The left-hand menu is updated to show 'Device Management' as the selected option. The main content area is titled 'Device Management' and contains a tabbed interface with 'Devices', 'Updates', 'SSL VPN', 'Licensing', and 'Key Bundles'. The 'Devices' tab is active, displaying a table of installed devices. The table has columns for Device Name, Management IP, Version, Status, and a set of action links. The table shows one device, SBCE8-70, with Management IP 10.64.90.70, Version 8.0.1.0-10-17555, and Status Commissioned. The action links for this device are Reboot, Shutdown, Restart Application, View, Edit, and Uninstall.



**Step 2** - Click on **View** to display the **System Information** screen. The screen shows the **Network Configuration, DNS Configuration** and **Management IP(s)** information provided during installation and corresponds 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 AT&T.

System Information: SBCE8-70

X

General Configuration

Appliance Name

SBCE8-70

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

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.91.40	10.64.91.40	255.255.255.0	10.64.91.1	A1
10.64.91.41	10.64.91.41	255.255.255.0	10.64.91.1	A1
192.168.80.43	192.168.80.43	255.255.255.128	192.168.80.1	B1
				B1
				B1
				B2

DNS Configuration

Primary DNS

10.64.19.201

Secondary DNS

DNS Location

DMZ

DNS Client IP

10.64.91.40

Management IP(s)

IP #1 (IPv4)

10.64.90.70



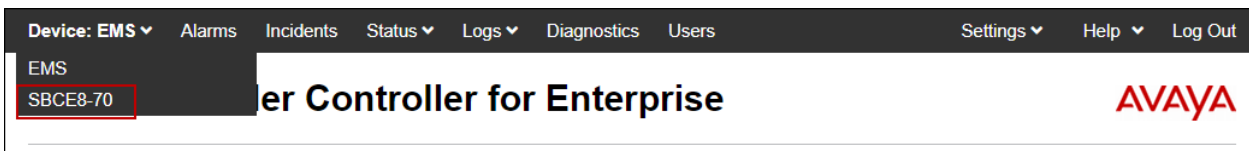
## 8.2. TLS Management

**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.

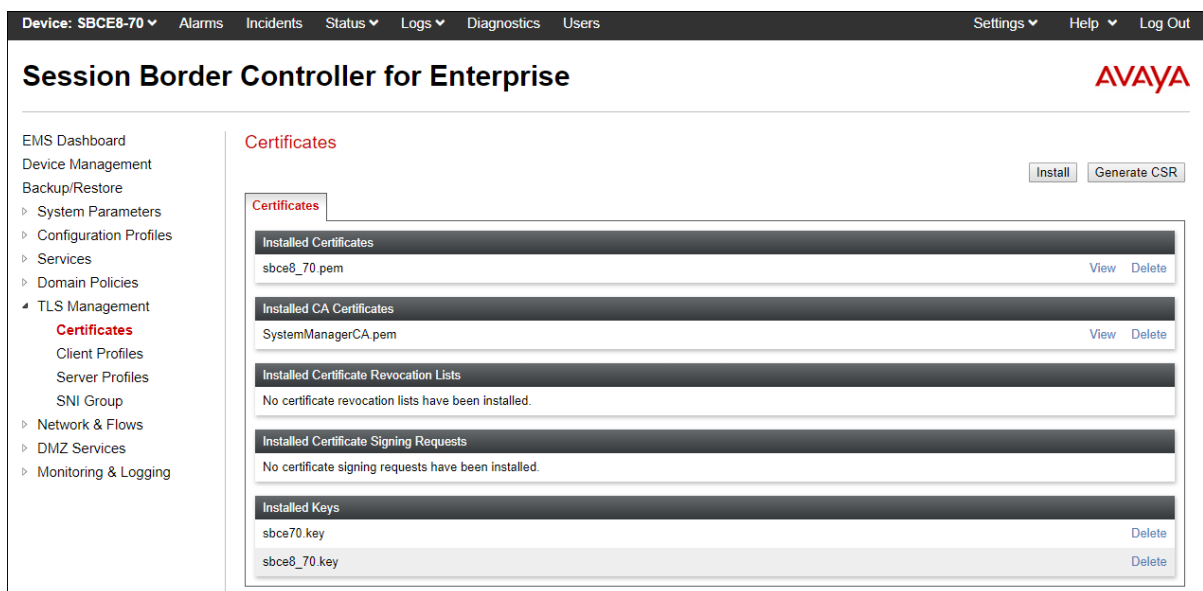
### 8.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

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 a descriptive name. (e.g., **sbce8\_70Server**).
- **Certificate:** select the identity certificate, e.g., **sbce8\_70.pem**, from pull down menu.
- **Peer Verification** = **None**.
- Click **Next**.

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

The 'Edit Profile' dialog box shows the configuration for a TLS profile. At the top, there is a warning message: "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." Below the warning, the 'TLS Profile' section contains: Profile Name (sbce8\_70Server), Certificate (sbce8\_70.pem), SNI Options (None), and SNI Group (None). The 'Certificate Verification' section contains: Peer Verification (None), Peer Certificate Authorities (SystemManagerCA.pem), Peer Certificate Revocation Lists (empty), and Verification Depth (0). A 'Next' button is at the bottom right.

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

The screenshot shows the 'Session Border Controller for Enterprise' interface. On the left is a navigation menu with 'TLS Management' expanded, showing 'Server Profiles' as the active section. The main area displays the 'Server Profiles: sbce8\_70Server' list with an 'Add' button. Below the list, the 'Server Profile' configuration form is shown, mirroring the 'Edit Profile' dialog. It includes sections for TLS Profile, Certificate Verification, Renegotiation Parameters, and Handshake Options. The 'Handshake Options' section shows TLS 1.2 selected, with a list of ciphers: HIGH:IDH:ADH:IMD5:1aNULL:1eNULL:@STRENGTH. An 'Edit' button is at the bottom right of the form.

### 8.2.3. Client Profiles

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

- **Profile Name:** enter a descriptive name (e.g., **sbce8\_70Client**)
- **Certificate:** select the identity certificate, e.g., **sbce8\_70.pem**, from pull down menu.
- **Peer Verification = Required.**
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **SystemManagerCA.pem**.
- Enter 1 under **Verification Depth**. Click **Next**.

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

The 'Edit Profile' dialog box shows the configuration for a TLS Client Profile. At the top, a warning message states: 'WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.' The 'TLS Profile' section includes fields for 'Profile Name' (sbce8\_70Client), 'Certificate' (sbce8\_70.pem), and 'SNI' (Enabled). The 'Certificate Verification' section includes 'Peer Verification' (Required), 'Peer Certificate Authorities' (SystemManagerCA.pem), 'Peer Certificate Revocation Lists' (empty), 'Verification Depth' (1), 'Extended Hostname Verification' (disabled), and 'Server Hostname' (empty). A 'Next' button is at the bottom.

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

The 'Session Border Controller for Enterprise' interface shows the 'Client Profiles' section. The profile 'sbce8\_70Client' is selected. The 'Client Profile' form is displayed with the following details: 'TLS Profile' (Profile Name: sbce8\_70Client, Certificate: sbce8\_70.pem, SNI: Enabled), 'Certificate Verification' (Peer Verification: Required, Peer Certificate Authorities: SystemManagerCA.pem, Peer Certificate Revocation Lists: ---, Verification Depth: 1, Extended Hostname Verification: disabled), 'Renegotiation Parameters' (Renegotiation Time: 0, Renegotiation Byte Count: 0), and 'Handshake Options' (Version: TLS 1.2, TLS 1.1, TLS 1.0; Ciphers: Default, FIPS, Custom; Value: HIGH IDH IADH IMD5 IaNULL IaNULL @STRENGTH). An 'Edit' button is at the bottom.

## 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. Navigate to **Networks & Flows → Network Management**. On the **Networks** tab, verify the IP addresses assigned to the interfaces. The following screen shows the enterprise interface is assigned to **A1** and the interface towards AT&T is assigned to **B1**.

**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 (private) and B1 (public) interfaces are used. To enable an interface, click the corresponding **Disabled** link under the Status column to change it to **Enabled**.

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. The following Avaya SBCE IP addresses and associated interfaces were used in the sample configuration:

- **B1: 192.168.80.43** – IP address configured for the AT&T IPTF service. This address is known to AT&T. See **Section 3**.
- **A1: 10.64.91.41** – IP address configured for AT&T IPTF service to Session Manager.

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'. There are also 'Edit' and 'Delete' links for each row. The configurations listed are Inside-A1, Outside-B1, Outside-B1-IPv6, and Outside-B2.

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
Inside-A1	10.64.91.1	255.255.255.0	A1	10.64.91.40, 10.64.91.41	Edit	Delete
Outside-B1	192.168.80.1	255.255.255.128	B1	192.168.80.43	Edit	Delete
Outside-B1-IPv6		64	B1		Edit	Delete
Outside-B2		255.255.255.248	B2		Edit	Delete

## 8.4. Advanced Options

AT&T required the UDP port ranges of the media to be configured in the **16384 – 32767** range. However, by default ranges 12000 to 21000 and 22000 to 31000 are already allocated by the Avaya SBCE for internal use. The following steps reallocate the port ranges used by the Avaya SBCE, so the range required by AT&T can be defined on the Avaya SBCE Media Interfaces (**Section 8.5**).

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

**Step 2** - Select the **Port Ranges** tab.

**Step 3** - In the **Signaling Port Range** row, change the range to **12000 – 16380**

**Step 4** - In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000 – 51000**.

**Step 5** – In the **Listen Port Range** row, change the range to **6000 – 6999**.

**Step 6** – In the **HTTP Port Range** row, change the range to **51001 – 62000**.

**Step 7** - Select **Save**. Note that changes to these values require an application restart (see **Section 8.1**).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu includes options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, and Network & Flows. Under Network & Flows, the 'Advanced Options' link is highlighted. The main content area is titled 'Advanced Options' and features several tabs: Periodic Statistics, Feature Control, SIP Options, Network Options, Port Ranges (which is selected), RTCP Monitoring, and Load Monitoring. A warning message states: 'Changes to the settings below require an application restart before taking effect. Application restarts can be issued from Device Management.' Below this, the 'Port Range Configuration' section contains four rows of settings, each with two input fields separated by a hyphen: 'Signaling Port Range' (12000 - 16380), 'Config Proxy Internal Signaling Port Range' (42000 - 51000), 'Listen Port Range' (6000 - 6999), and 'HTTP Port Range' (51001 - 62000). A 'Save' button is located at the bottom right of the configuration area.

Port Range Configuration	
Signaling Port Range	12000 - 16380
Config Proxy Internal Signaling Port Range	42000 - 51000
Listen Port Range	6000 - 6999
HTTP Port Range	51001 - 62000

## 8.5. Media Interfaces

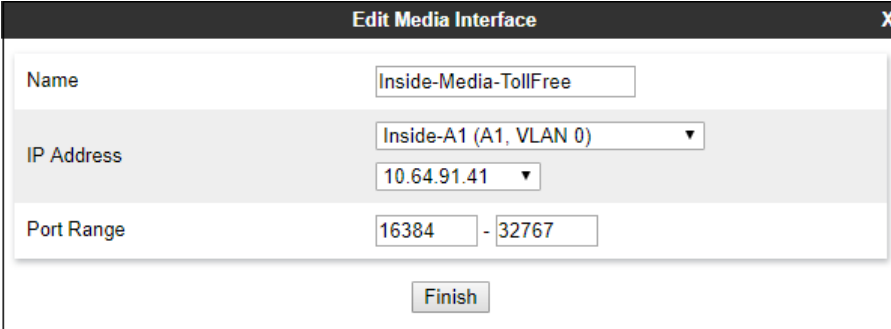
Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which the SBCE will accept media from the connected server. Note that some ports in the range required by AT&T were already allocated by the Avaya SBCE for internal use, by default. **Section 8.4** shows the steps required to reallocate the port ranges used by the Avaya SBCE, so the range required by AT&T could be accommodated.

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

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

- **Name:** **Inside-Media-TollFree**
- **IP Address:** Select **Inside-A1 (A1, VLAN0)** and **10.64.91.41**
- **Port Range:** **16384 – 32767**

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



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

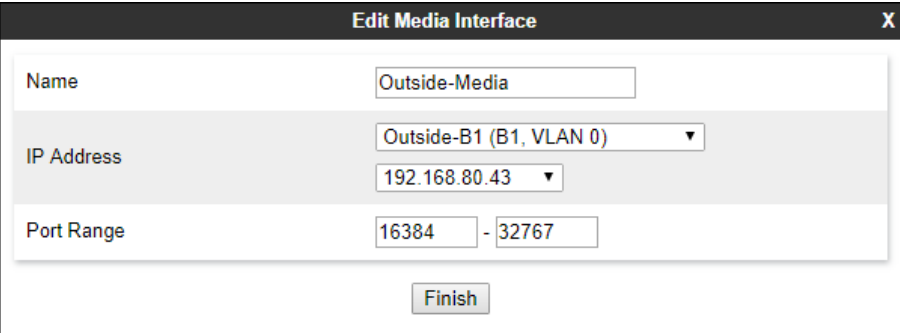
Field	Value
Name	Inside-Media-TollFree
IP Address	Inside-A1 (A1, VLAN 0) 10.64.91.41
Port Range	16384 - 32767

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

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

- **Name:** **Outside-Media**
- **IP Address:** Select **Outside-B1 (B1, VLAN0)** and **192.168.80.43**
- **Port Range:** **16384 – 32767**

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



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

Field	Value
Name	Outside-Media
IP Address	Outside-B1 (B1, VLAN 0) 192.168.80.43
Port Range	16384 - 32767

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

## 8.6. 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 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:** Inside-Sig-TollFree-41
- **IP Address:** Select **Inside-A1 (A1, VLAN0)** and **10.64.91.41**
- **TLS Port:** 5061
- **TLS Profile:** Select the TLS server profile created in **Section 8.2.2**

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

The screenshot shows the 'Edit Signaling Interface' window with the following fields:

- Name:** Inside-Sig-TollFree-41
- IP Address:** Inside-A1 (A1, VLAN 0) (dropdown), 10.64.91.41 (dropdown)
- TCP Port:** (empty field, text below: Leave blank to disable)
- UDP Port:** (empty field, text below: Leave blank to disable)
- TLS Port:** 5061 (text below: Leave blank to disable)
- TLS Profile:** sbce8\_70Server (dropdown)
- Enable Shared Control:** (checkbox, unchecked)
- Shared Control Port:** (empty field)
- Finish** button

**Step 4** - Select **Add** again, and enter the following:

- **Name:** Outside-Signaling
- **IP Address:** Select **Outside-B1 (B1, VLAN0)** and **192.168.80.43**
- **UDP Port:** 5060. Click **Finish**.

The screenshot shows the 'Edit Signaling Interface' window with the following fields:

- Name:** Outside-Signaling
- IP Address:** Outside-B1 (B1, VLAN 0) (dropdown), 192.168.80.43 (dropdown)
- TCP Port:** (empty field, text below: Leave blank to disable)
- UDP Port:** 5060 (text below: Leave blank to disable)
- TLS Port:** (empty field, text below: Leave blank to disable)
- TLS Profile:** None (dropdown)
- Enable Shared Control:** (checkbox, unchecked)
- Shared Control Port:** (empty field)
- Finish** button

## 8.7. Server Interworking Profiles

The Server Interworking profiles include 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.

In the sample configuration, separate Server Interworking Profiles were created for the enterprise and AT&T IPTF service.

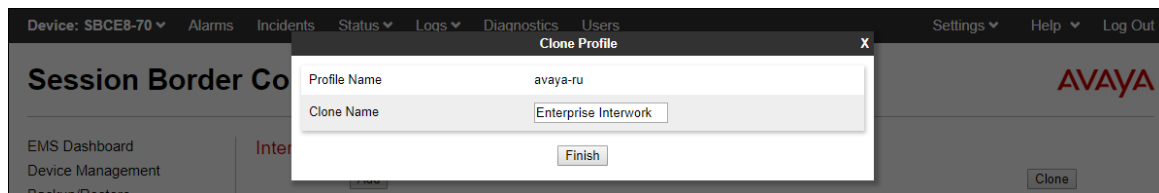
### 8.7.1. Server Interworking Profile – Enterprise

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.

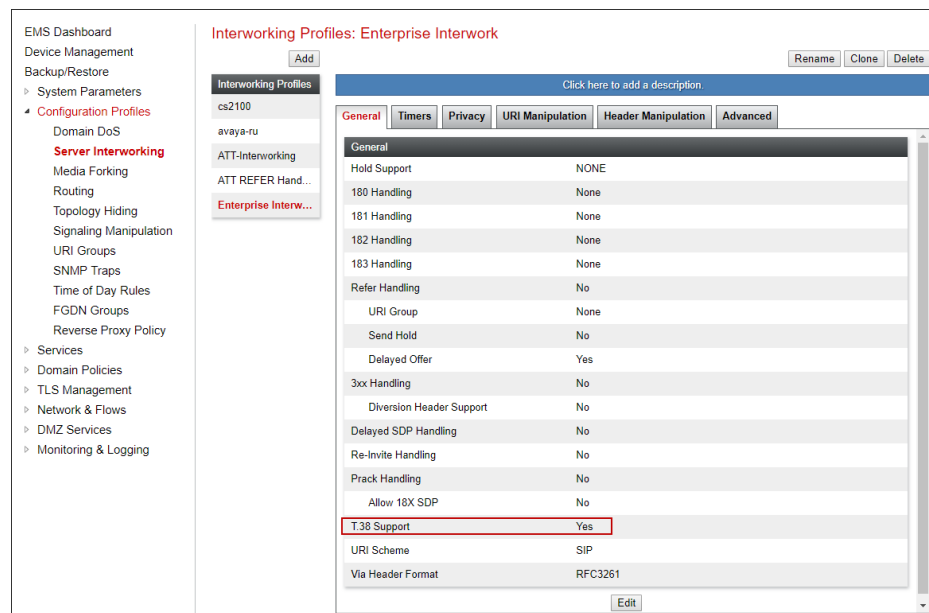
**Step 3** - Enter profile name: (e.g., **Enterprise Interwork**), and click **Finish** to continue.



**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).

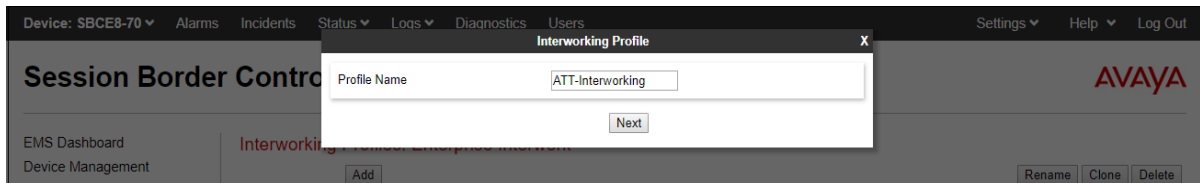




## 8.7.2. Server Interworking – AT&T

Repeat the steps shown in **Section 8.7.1** to add an Interworking Profile for the connection to AT&T via the public network, with the following changes:

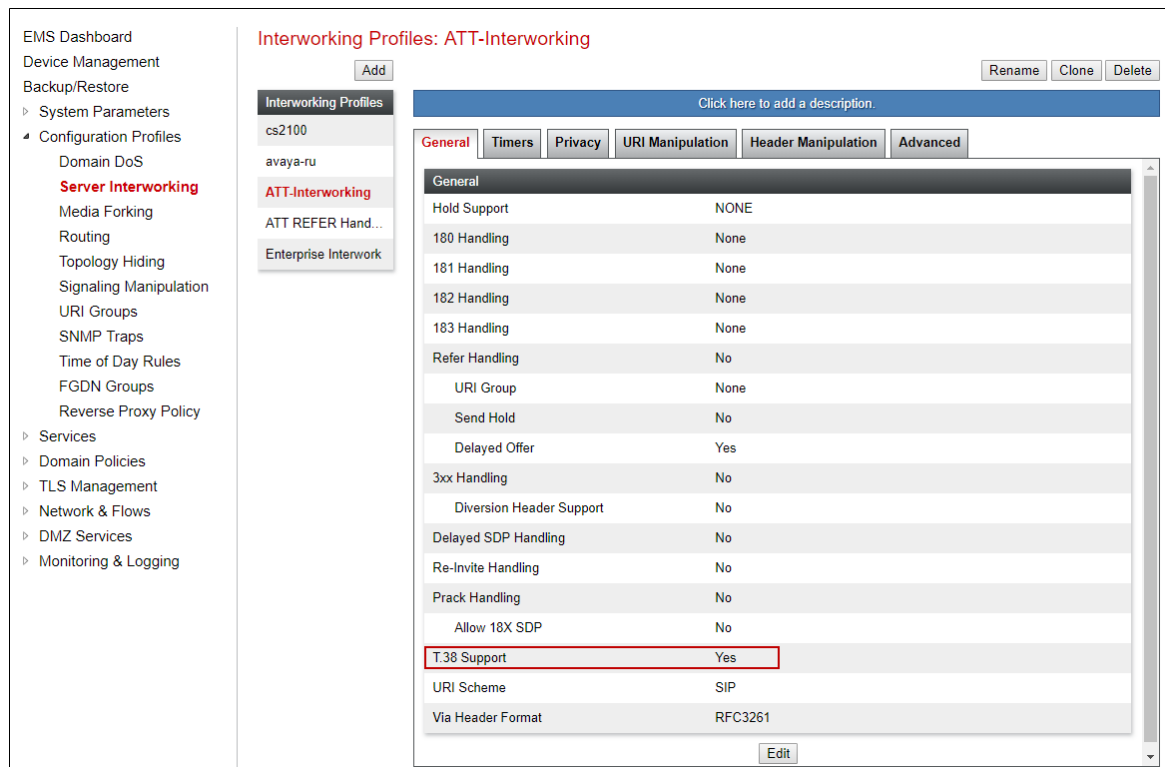
**Step 1** - Select **Add Profile** and enter a profile name: (e.g., **ATT-Interworking**) and click **Next**.



The screenshot shows the 'Session Border Controller' interface. A modal dialog titled 'Interworking Profile' is open. It has a 'Profile Name' input field containing 'ATT-Interworking' and a 'Next' button. The background interface shows the 'Add' button for 'Interworking Profiles'.

**Step 2** - The **General** screen will open:

- Default values are used with the exception of **T.38 Support** set to **Yes**



The screenshot shows the 'Interworking Profiles: ATT-Interworking' configuration screen. The 'General' tab is selected. The 'T.38 Support' option is highlighted with a red box and set to 'Yes'. Other options include 'Hold Support' (NONE), '180 Handling' (None), '181 Handling' (None), '182 Handling' (None), '183 Handling' (None), 'Refer Handling' (No), 'URI Group' (None), 'Send Hold' (No), 'Delayed Offer' (Yes), '3xx Handling' (No), 'Diversion Header Support' (No), 'Delayed SDP Handling' (No), 'Re-Invite Handling' (No), 'Prack Handling' (No), 'Allow 18X SDP' (No), 'URI Scheme' (SIP), and 'Via Header Format' (RFC3261).

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

**Step 3** – On the **Timers** tab, the **Trans Expire** timer is set to the allotted time the Avaya SBCE will try the first primary server before trying the secondary server, if one exists.

The screenshot shows the 'Interworking Profiles: ATT-Interworking' configuration page. On the left is a sidebar with a list of profiles: 'cs2100', 'avaya-ru', 'ATT-Interworking' (highlighted in red), 'ATT REFER Handl...', and 'Enterprise Interwork'. Above the list are 'Add', 'Rename', 'Clone', and 'Delete' buttons. The main area has a blue header with 'Click here to add a description.' and a tabbed interface with 'General', 'Timers' (active), 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'Timers' tab contains a table of SIP Timers:

SIP Timers	
Min-SE	---
Init Timer	---
Max Timer	---
Trans Expire	4 seconds
Invite Expire	---
Retry After	---

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

**Step 4** - Click **Next** to accept default parameters for the **Privacy**, **URI Manipulation**, and **Header Manipulation** tabs (not shown).

**Step 5** – On the **Advanced/DTMF** tab:

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

The screenshot shows the 'Interworking Profiles: ATT-Interworking' configuration page with the 'Advanced' tab selected. The sidebar and top navigation are the same as in the previous screenshot. The 'Advanced' tab contains a table of configuration options:

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

Below this table is a section titled 'DTMF' with a single row:

DTMF	
DTMF Support	None

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

## 8.8. Signaling Manipulation

Signaling Manipulations (SigMa) scripts are used by the Avaya SBCE 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 8.7**) or Signaling Rules (**Section 8.14**) do not meet the desired result. Refer to References [11] for information on the Avaya SBCE scripting language.

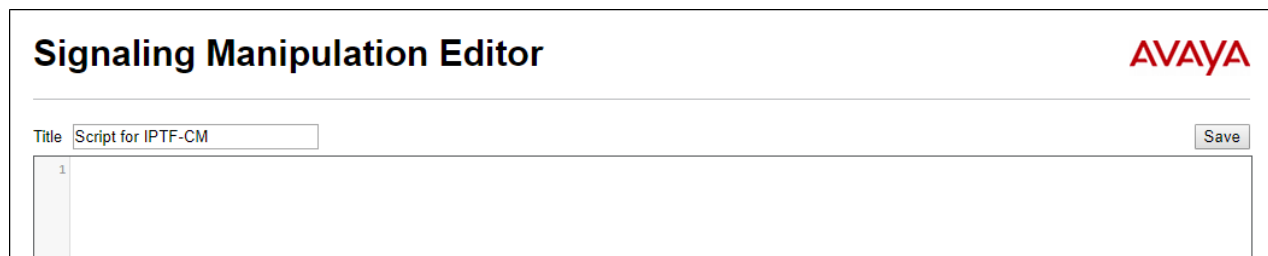
A Sigma script was created during the compliance test to address the following interoperability issues:

- Remove the gsid and epv parameters from outbound Contact headers. (**Section 2.2, Item 7**).
- Remove the Bandwidth headers sent by some Avaya SIP endpoints. (**Section 2.2, Item 8**).

**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., **Script for IPTF-CM**).



**Step 3** - Copy and paste the script below in the editor window.

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

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

//Remove Bandwidth from SDP
        %BODY[1].regex_replace("b=(TIAS|AS|CT):(\d+)\r\n", "");

    }
}
-----
```

**Step 4** - Click on **Save**. The script editor will test for any errors, and the window will close. This script is applied to the AT&T SIP Server profile in **Section 8.9.2**.

## 8.9. SIP Server Profiles

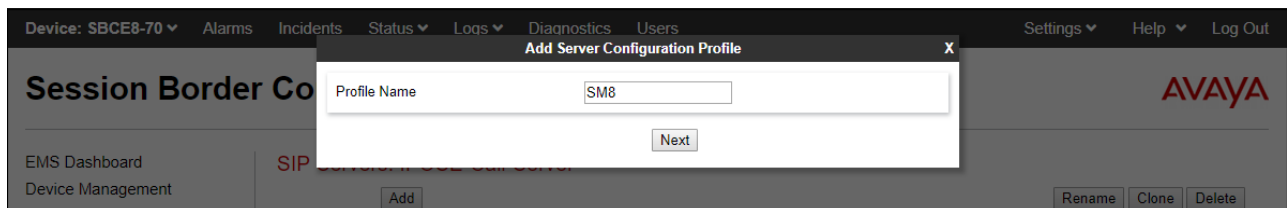
The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

### 8.9.1. SIP Server Profile – Session Manager

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

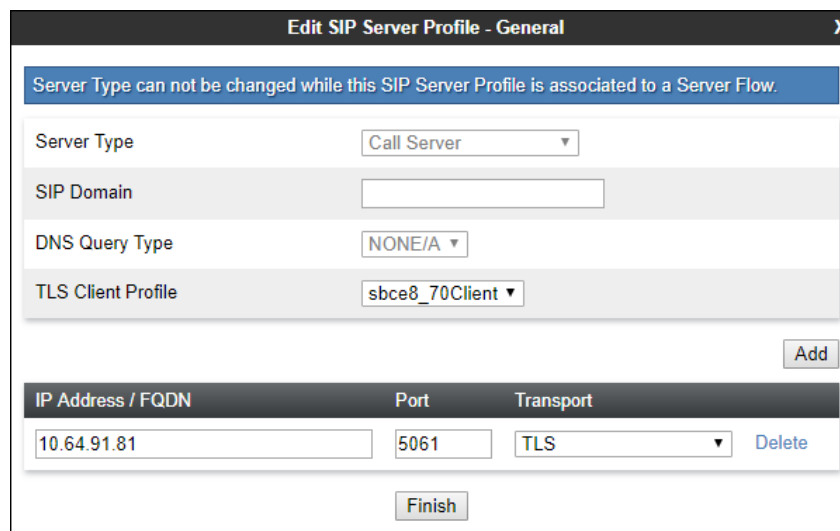
**Step 1** - Select **Services** → **SIP Servers** from the left-hand menu.

**Step 2** - Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **SM8**) and click **Next**.



**Step 3** - The **Edit SIP Server 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., **sbce8\_70Client**)
- **IP Address/FQDN**: **10.64.91.81** (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.



**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' window. It contains the following fields and values:

Field	Value
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	sbce70@avayalab.com
To URI	sm@avayalab.com

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

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

**Step 7** – On the **Advanced** tab:

- Select the **Enterprise Interwork** (created in **Section 8.7.1**), 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' window. It contains the following fields and values:

Field	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Enterprise Interwork
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

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

### 8.9.2. SIP Server Profile – AT&T

**Note** – The AT&T IPTF service may provide a Primary and Secondary Border Element. This section describes the connection to a single (Primary) Border Element.

Repeat the steps in **Section 8.9.1**, with the following changes, to create a SIP Server Profile for the Avaya SBCE connection to AT&T.

**Step 1** - Select **Add** and enter a Profile Name (e.g., **ATT-TollFree-trk-svr**) and select **Next** (not shown).

**Step 2** - On the **General** window (not shown), enter the following.

- Select **Server Type: Trunk Server**
- **IP Address/FQDN: 192.168.225.210** (AT&T Border Element IP address)
- **Port: 5060**
- Select **Transport: UDP**
- Click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.

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

Server Type	Trunk Server
SIP Domain	
DNS Query Type	NONE/A
TLS Client Profile	None

Add

IP Address / FQDN	Port	Transport
192.168.225.210	5060	UDP

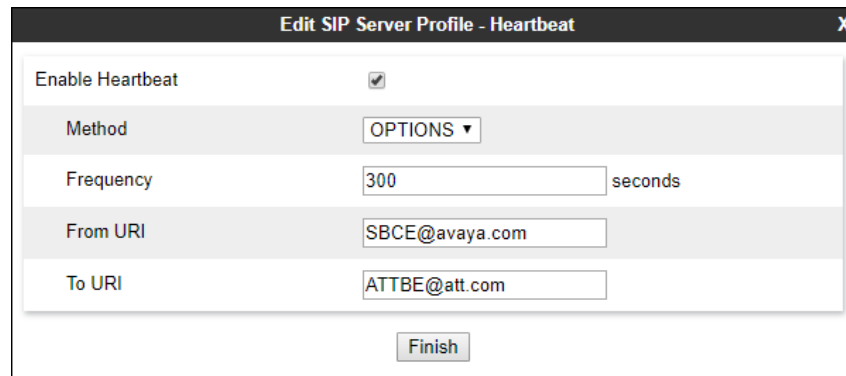
Delete

Finish

**Step 3** – Default values can be used on the **Authentication** tab.

**Step 4** – On the **Heartbeat** tab, check the **Enable Heartbeat** box to have the Avaya SBCE source “heartbeats” toward AT&T. This configuration is optional.

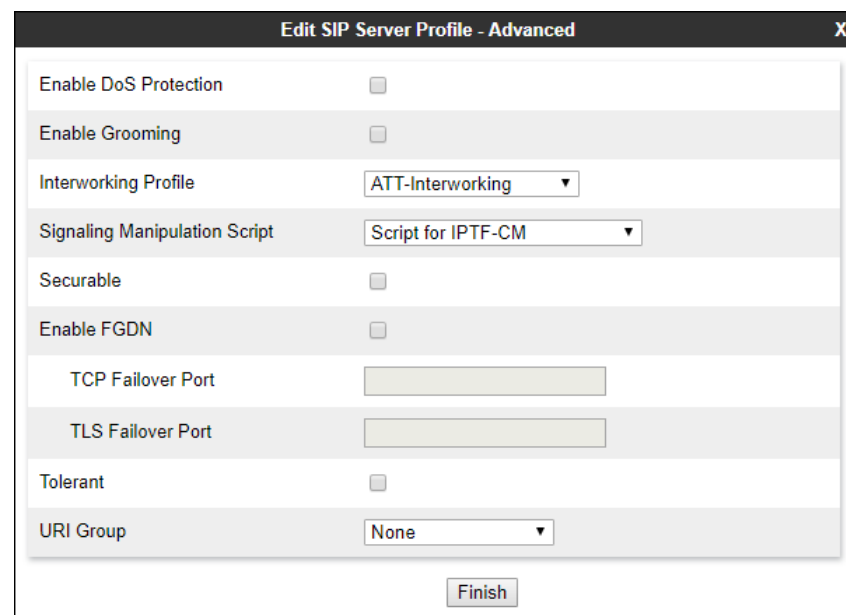
- Select **OPTIONS** from the **Method** drop-down menu.
- Select the desired frequency that the SBCE will source OPTIONS toward AT&T.
- Make logical entries in the **From URI** and **To URI** fields that will be used in the OPTIONS headers.



Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS ▼
Frequency	300 seconds
From URI	SBCE@avaya.com
To URI	ATTBE@att.com
<b>Finish</b>	

**Step 5** - On the **Advanced** window, enter the following.

- **Enable Grooming** is not used for UDP connections and is left unchecked.
- Select **ATT-Interworking** (created in **Section 8.7.2**), for **Interworking Profile**.
- Select the **Script for IPTF-CM** (created in **Section 8.8**) for **Signaling Manipulation Script**.
- Select **Finish**



Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	ATT-Interworking ▼
Signaling Manipulation Script	Script for IPTF-CM ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None ▼
<b>Finish</b>	

## 8.10. Routing Profiles

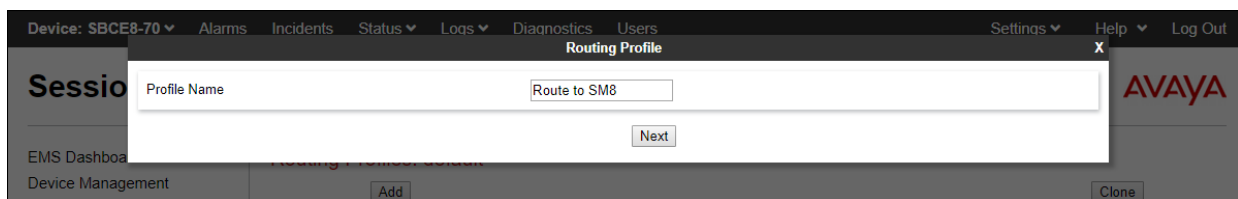
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and determine which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport 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 AT&T.

### 8.10.1. 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**.

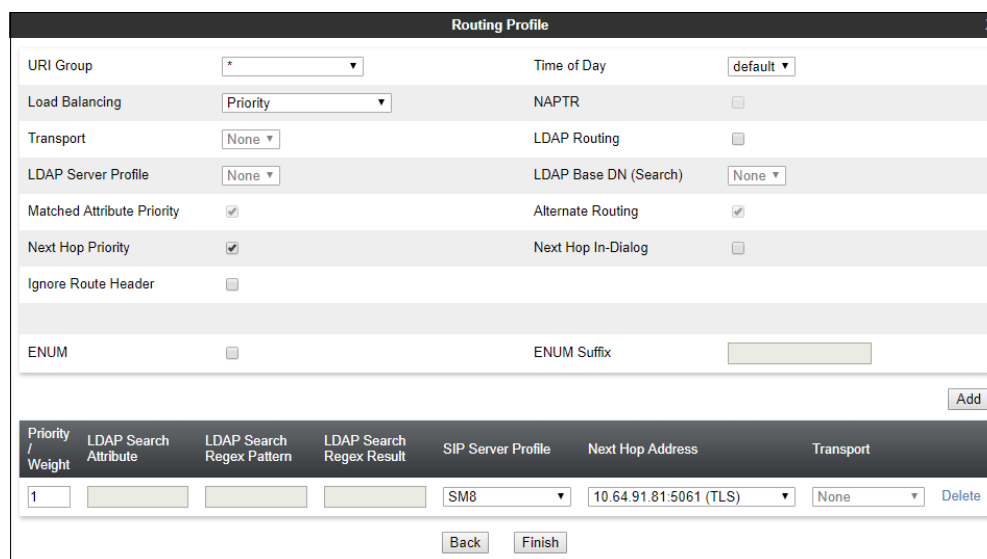
**Step 2** - Enter a **Profile Name**: (e.g., **Route to SM8**) and click **Next**.

The screenshot shows the 'Routing Profile' configuration window. At the top, there's a navigation bar with 'Device: SBCE8-70' and various menu items like 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. Below this, the 'Routing Profile' window is open, showing a 'Profile Name' field with the text 'Route to SM8' and a 'Next' button. The background shows a sidebar with 'Session Manager' and 'EMS Dashboard'.

**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: SM8** (from Section 8.9.1).
- **Next Hop Address:** Verify that the **10.64.91.81:5061 (TLS)** entry from the drop-down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out. Click **Finish**.

The screenshot shows the 'Routing Profile' configuration window with the 'Next-Hop Address' section expanded. The 'Add' button is visible. Below the main configuration area, 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 shows '1' in the Priority field, 'SM8' in the SIP Server Profile field, and '10.64.91.81:5061 (TLS)' in the Next Hop Address field. The Transport field is grayed out and set to 'None'. There are 'Back' and 'Finish' buttons at the bottom.



## 8.10.2. Routing Profile – AT&T

Repeat the steps in **Section 8.10.1**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to AT&T.

**Step 1** - Enter a Profile Name: (e.g., **Route to ATT IPTF**).

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

- **Priority/Weight: 1**
- **Server Configuration: ATT-TollFree-trk-svr (from Section 8.9.2).**
- **Next Hop Address:** Verify that the **192.168.225.210:5060 (UDP)** entry from the drop-down menu is selected (AT&T Border Element IP address).
- Click **Finish**.

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

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				ATT-TollFree-trk-	192.168.225.210:5060 (UDP)	None

Delete

Back Finish

## 8.11. 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 integrity of the network. It hides the topology of the enterprise network from external networks.

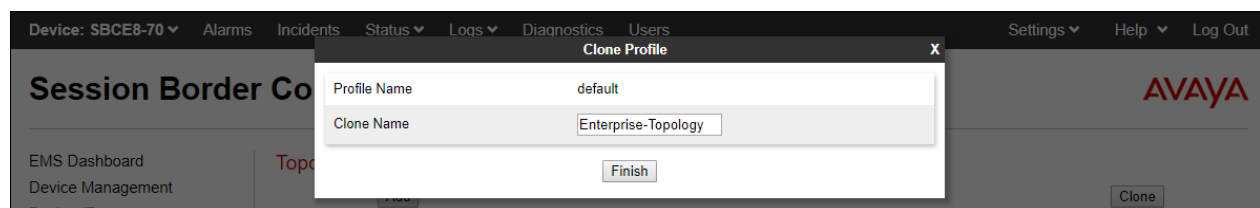
### 8.11.1. Topology Hiding – Enterprise Side

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

### 8.11.2. Topology Hiding – AT&T Side

Repeat the steps in **Section 8.11.1**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to AT&T.

**Step 1** - Enter a Profile Name (e.g., **SIP-Trunk-Topology**).

**Step 2** - Use the default values for all fields.

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

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

Finish

### 8.12. 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** - Select the **default-trunk** rule.

**Step 3** - Select the **Clone** button, and the **Clone Rule** window will open (not shown).

- In the **Clone Name** field enter the new Application Rule name (e.g., **sip-trunk**).
- Click **Finish** (not shown). The completed **Application Rule** is shown below.

Session Border Controller for Enterprise

Application Rules: sip-trunk

Application Rules

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

Miscellaneous

CDR Support: Off

RTCP Keep-Alive: No

## 8.13. Media Rules

Media Rules are used to define media encryption and QoS parameters. Separate media rules are created for the enterprise and AT&T.

### 8.13.1. Enterprise – Media Rule

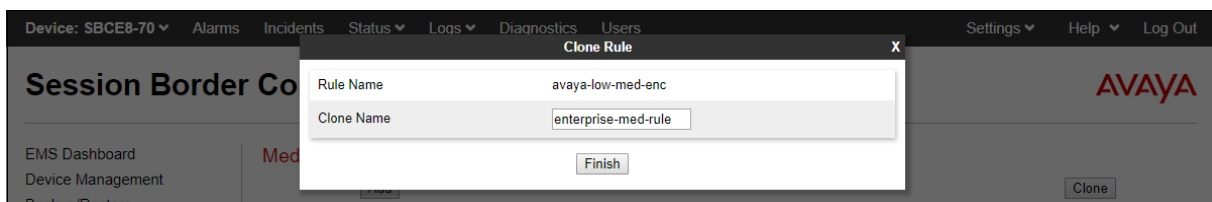
In the sample configuration, the default Media Rule **avaya-low-med-enc** was cloned to create the enterprise Media Rule, and modified as shown below:

**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.

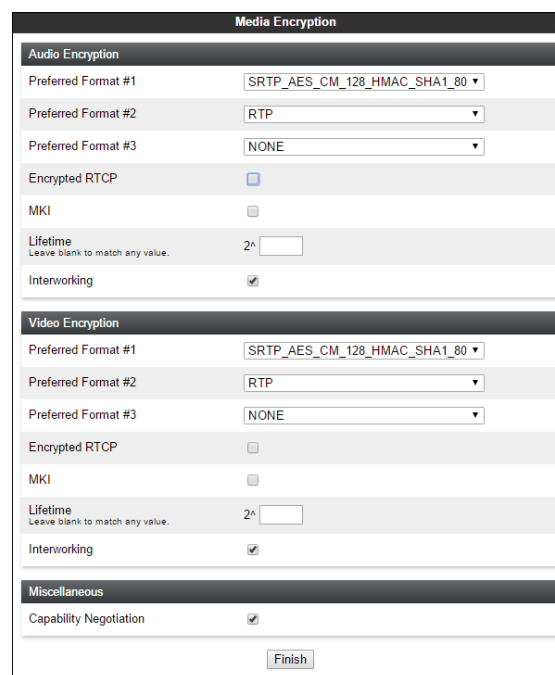
- In the **Clone Name** field enter the new Media Rule name (e.g., **enterprise-med-rule**)
- Click **Finish**. The newly created rule will be displayed.



**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**.

The screenshot shows the 'Media Encryption' configuration window. It is divided into three sections: 'Audio Encryption', 'Video Encryption', and 'Miscellaneous'. In the 'Audio Encryption' section, 'Preferred Format #1' is 'SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80', 'Preferred Format #2' is 'RTP', 'Preferred Format #3' is 'NONE', 'Encrypted RTCP' is unchecked, 'MKI' is unchecked, 'Lifetime' is '2h', and 'Interworking' is checked. The 'Video Encryption' section has identical settings. In the 'Miscellaneous' section, 'Capability Negotiation' is checked. A 'Finish' button is at the bottom.

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

## Session Border Controller for Enterprise

EMS Dashboard

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

Domain Policies

- Application Rules
- Border Rules
- Media Rules**
- Security Rules
- Signaling Rules
- Charging Rules
- End Point Policy Groups
- Session Policies

TLS Management

Network & Flows

DMZ Services

Monitoring & Logging

### Media Rules: enterprise-med-rule

Add

Media Rules

- default-low-med
- default-low-med-enc
- default-high
- default-high-enc
- avaya-low-med-enc
- att-med-rule
- enterprise-med-rule**

RenameCloneDelete

Click here to add a description.

EncryptionCodec PrioritizationAdvancedQoS

Audio Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

Video Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

Miscellaneous

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

Edit

MAA: Reviewed  
SPOC 11/25/2019

Solution & Interoperability Test Lab Application Notes  
©2019 Avaya Inc. All Rights Reserved.

93 of 113  
Au81SBC8EP-IPTF

## 8.13.2. AT&T – Media Rule

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

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

The completed **att-med-rule** screen is shown below.

The screenshot shows the 'Media Rules: att-med-rule' configuration page. On the left is a navigation menu with categories like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, Application Rules, Border Rules, Media Rules (highlighted), Security Rules, Signaling Rules, Charging Rules, End Point Policy Groups, Session Policies, TLS Management, Network & Flows, and DMZ Services. The main content area has a title 'Media Rules: att-med-rule' and an 'Add' button. Below the title is a list of media rules: default-low-med, default-low-med-enc, default-high, default-high-enc, avaya-low-med-enc, att-med-rule (highlighted), and enterprise-med-rule. The main configuration area has tabs for Encryption, Codec Prioritization, Advanced, and QoS. The Encryption tab is active, showing sections for Audio Encryption and Video Encryption. Audio Encryption has Preferred Formats set to RTP and Interworking checked. Video Encryption also has Preferred Formats set to RTP and Interworking checked. There is a Miscellaneous section with Capability Negotiation unchecked. An 'Edit' button is at the bottom right.

DSCP values **EF** for expedited forwarding (default value) are used for Media **QoS**.

This screenshot shows the 'QoS' tab of the 'Media Rules: att-med-rule' configuration page. The 'QoS' tab is active, showing sections for Media QoS Marking, Audio QoS, and Video QoS. Media QoS Marking has 'Enabled' checked and 'QoS Type' set to DSCP. Audio QoS has 'Audio DSCP' set to EF. Video QoS has 'Video DSCP' set to EF. An 'Edit' button is at the bottom right. The AVAYA logo is in the top right corner.

## 8.14. Signaling Rules

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

### 8.14.1. 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 (not shown).

- In the **Rule Name** field enter the new Signaling Rule name (e.g., **enterprise-sig-rule**)
- Click **Finish**.

Signaling Rule **enterprise-sig-rule** show below was left unchanged from the default rule.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left-hand side menu is expanded to 'Domain Policies' > 'Signaling Rules'. The main content area is titled 'Signaling Rules: enterprise-sig-rule'. It features a list of signaling rules on the left: 'default', 'No-Content-Type-Ch...', 'att-sig-rule', 'enterprise-sig-rule' (highlighted in red), and 'ATT-TF-408-test-sig'. The 'enterprise-sig-rule' is selected, and its configuration is displayed on the right. The configuration is divided into several tabs: 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID'. The 'General' tab is active, showing 'Inbound' and 'Outbound' sections. The 'Inbound' section has 'Requests' set to 'Allow', 'Non-2XX Final Responses' set to 'Allow', 'Optional Request Headers' set to 'Allow', and 'Optional Response Headers' set to 'Allow'. The 'Outbound' section has 'Requests' set to 'Allow', 'Non-2XX Final Responses' set to 'Allow', 'Optional Request Headers' set to 'Allow', and 'Optional Response Headers' set to 'Allow'. The 'Content-Type Policy' section has 'Enable Content-Type Checks' checked, 'Action' set to 'Allow', 'Multipart Action' set to 'Allow', and an 'Exception List' field. There is an 'Add' button at the top left of the rule list and an 'Edit' button at the bottom right of the configuration area.

### 8.14.2. Signaling Rule – AT&T

Signaling Rule **att-sig-rule** was similarly cloned from the **default** rule and used for AT&T. Note that the DSCP value **AF41** for assured forwarding (default value) is set for **Signaling QoS**.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left-hand side menu is expanded to 'Domain Policies' > 'Signaling Rules'. The main content area is titled 'Signaling Rules: att-sig-rule'. It features a list of signaling rules on the left: 'default', 'No-Content-Type-Ch...', 'att-sig-rule' (highlighted in red), 'enterprise-sig-rule', and 'ATT-TF-408-test-sig'. The 'att-sig-rule' is selected, and its configuration is displayed on the right. The configuration is divided into several tabs: 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID'. The 'Signaling QoS' tab is active, showing 'Signaling QoS' checked, 'QoS Type' set to 'DSCP', and 'DSCP' set to 'AF41'. There is an 'Add' button at the top left of the rule list and an 'Edit' button at the bottom right of the configuration area.

## 8.15. Endpoint Policy Groups

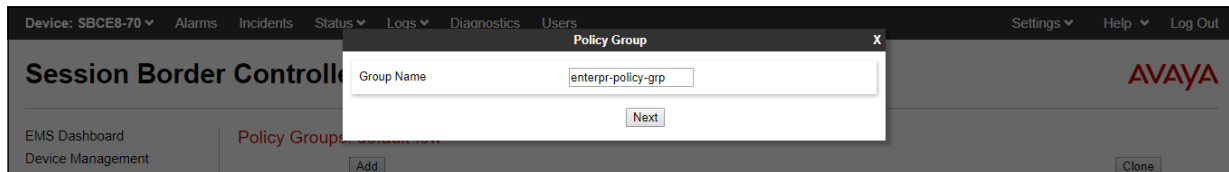
The rules created within the Domain Policies are assigned to an End Point Policy Group. The End Point Policy Group is then applied to a Server Flow in **Section 8.16**.

### 8.15.1. Endpoint Policy Group – Enterprise

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

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

- Enter a name for the Policy Group (e.g., **enterpr-policy-grp**)
- Click **Next**.

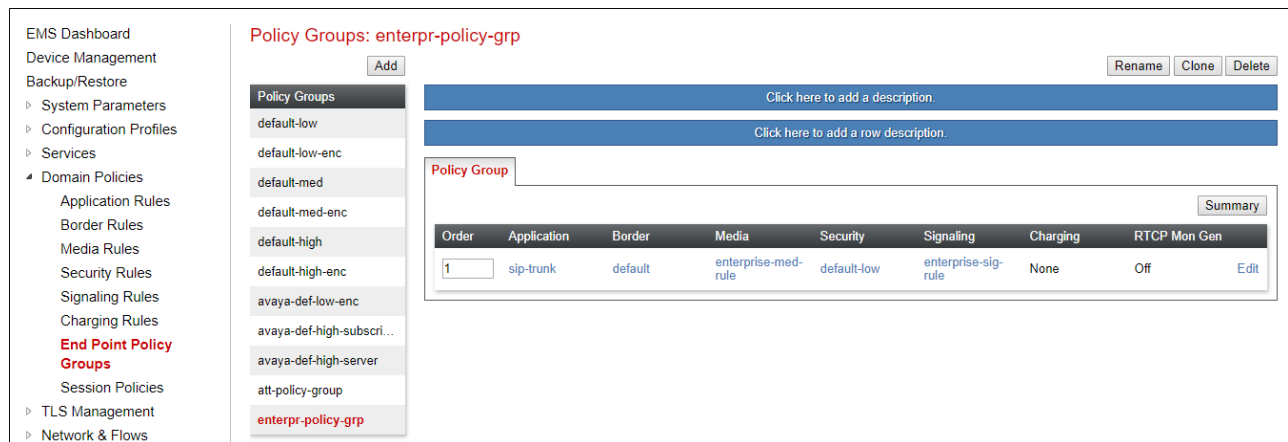


**Step 3** – On the **Policy Group** window (not shown), select the following.

- **Application Rule:** sip-trunk (created in **Section 8.128.12**).
- **Border Rule:** default.
- **Media Rule:** enterprise-med-rule (created in **Section 8.13.1**).
- **Security Rule:** default-low.
- **Signaling Rule:** enterprise-sig-rule (created in **Section 8.14.1**).

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

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





## 8.15.2. Endpoint Policy Group – AT&T

**Step 1** - Repeat steps 1 through 4 from Section 8.15.1 with the following changes:

- **Group Name:** att-policy-group
- **Media Rule:** att-med-rule (created in Section 8.13.2)
- **Signaling Rule:** att-sig-rule (created in Section 8.14.2)

**Step 2** - Select **Finish** (not shown).

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

EMS Dashboard  
Device Management  
Backup/Restore  
System Parameters  
Configuration Profiles  
Services  
Domain Policies  
Application Rules  
Border Rules  
Media Rules  
Security Rules  
Signaling Rules  
Charging Rules  
End Point Policy Groups  
Session Policies

Policy Groups: att-policy-group

Add

Rename Clone Delete

Click here to add a description.

Click here to add a row description.

Policy Group

Summary

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

Edit

## 8.16. Endpoint Flows – Server Flows

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

Create separate Server Flows for the enterprise and AT&T IPTF service. These flows use the interfaces, polices, and profiles defined in previous sections.

### 8.16.1. Server Flows – Enterprise

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

**Step 2** - Select the **Server Flows** tab (not shown).

**Step 3** - Select **Add** (not shown) and enter the following:

- **Flow Name:** Enter a name for the flow, e.g., **SM Flow Toll Free**
- **Server Configuration:** **SM8** (Section 8.9.1).
- **URI Group:** \*
- **Transport:** \*
- **Remote Subnet:** \*
- **Received Interface:** **Outside-Signaling** (Section 8.6).
- **Signaling Interface:** **Inside-Sig-TollFree-41** (Section 8.6).
- **Media Interface:** **Inside-Media-TollFree** (Section 8.5).

- **End Point Policy Group:** enterpr-policy-grp (Section 8.15.1).
- **Routing Profile:** Route to ATT IPTF (Section 8.10.2).
- **Topology Hiding Profile:** Enterprise-Topology (Section 8.11.1).
- Let other fields at the default values.

**Step 4** - Click **Finish** (not shown).

View Flow: SM Flow Toll Free	
<b>Criteria</b>	
Flow Name	SM Flow Toll Free
Server Configuration	SM8
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Outside-Signaling
<b>Profile</b>	
Signaling Interface	Inside-Sig-TollFree-41
Media Interface	Inside-Media-TollFree
Secondary Media Interface	None
End Point Policy Group	enterpr-policy-grp
Routing Profile	Route to ATT IPTF
Topology Hiding Profile	Enterprise-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

## 8.16.2. Server Flow – AT&T

**Step 1** - Repeat steps 1 through 4 from Section 8.16.1, with the following changes:

- **Flow Name:** Enter a name for the flow, e.g., **ATT IPTF Flow**.
- **Server Configuration:** **ATT-TollFree-trk-svr** (Section 8.9.2).
- **Received Interface:** **Inside-Sig-TollFree-41** (Section 8.6).
- **Signaling Interface:** **Outside-Signaling** (Section 8.6).
- **Media Interface:** **Outside-Media** (Section 8.5).
- **End Point Policy Group:** **att-policy-group** (Section 8.15.2).
- **Routing Profile:** **Route to SM8** (Section 8.10.1).
- **Topology Hiding Profile:** **SIP-Trunk-Topology** (Section 8.11.2).

View Flow: ATT IPTF Flow	
<b>Criteria</b>	
Flow Name	ATT IPTF Flow
Server Configuration	ATT-TollFree-trk-svr
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside-Sig-TollFree-41
<b>Profile</b>	
Signaling Interface	Outside-Signaling
Media Interface	Outside-Media
Secondary Media Interface	None
End Point Policy Group	att-policy-group
Routing Profile	Route to SM8
Topology Hiding Profile	SIP Trunk-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

## 9. AT&T IP Toll Free Service Configuration

AT&T provides the IPTF service border element IP address, the access DID numbers, and the associated DNIS digits used in the reference configuration. In addition, the AT&T IPTF features, and their associated access numbers, are also assigned by AT&T. AT&T requires that the Avaya SBCE public (B1) IP address be provided to the IPTF service, as part of the provisioning process. For more information, consult reference [15].

## 10. Verification Steps

The following steps may be used to verify the configuration.

### 10.1. AT&T IP Toll Free Service

The following scenarios may be executed to verify functionality with the AT&T IPTF service:

1. Place an inbound call, answer the calls, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.
4. Using the appropriate IPTF access numbers and DTMF codes, verify that the following IPTF features are successful:
  - a. Legacy Transfer Connect DTMF triggered Agent Hold, Conference and Transfer capabilities
  - b. Alternate Destination Routing call redirection capabilities based on Busy, Ring-No-Answer, and other SIP error codes.
5. Inbound fax using T.38 or G.711. See **Section 2.2** for limitations.
6. SIP OPTIONS monitoring of the health of the SIP trunk.

## 10.2. Avaya Aura® Communication Manager Verification

The following examples are only a few of the monitoring commands available on Communication Manager. See [6] for more information.

- Tracing a SIP trunk.
  1. From the Communication Manager console connection enter the command ***list trace tac xxx***, where ***xxx*** is a trunk access code defined for the SIP trunk to AT&T (e.g., \*04). Note that in the trace shown below, Session Manager has previously converted the IPTF DNIS number included in the Request URI, to the Communication Manager VDN 71041, before sending the INVITE to Communication Manager.

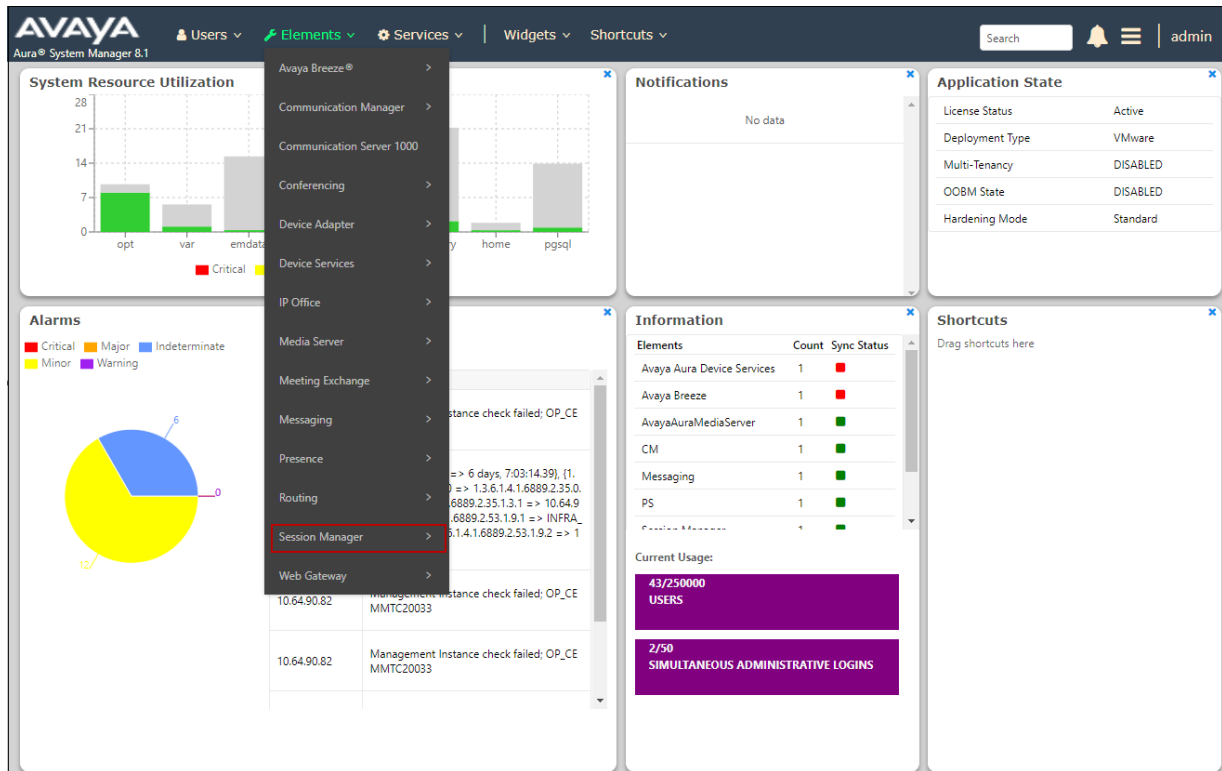
```
list trace tac *04                                     Page 1
LIST TRACE
time          data
13:35:53 TRACE STARTED 11/06/2019 CM Release String cold-01.0.890.0-25578
13:36:04 SIP<INVITE sips:71041@avayalab.com SIP/2.0
13:36:04      Call-ID: 31ebc87eee7ec97b24e184164efeeae18
13:36:04      active trunk-group 4 member 1      cid 0xf6b
13:36:04      0 0 ENTERING TRACE cid 3947
13:36:04      4 1 vdn e71041 bsr appl 0 strategy 1st-found override n
13:36:04      4 1 AVDN: 71041 AVRDN:
13:36:04      4 1 # Wait hearing ringback...
13:36:04      4 2 wait 2 secs hearing ringback
13:36:04 SIP>SIP/2.0 180 Ringing
13:36:04      Call-ID: 31ebc87eee7ec97b24e184164efeeae18
13:36:04      dial 71041
13:36:04      ring vector 4      cid 0xf6b
13:36:04      G729 ss:off ps:20
13:36:04      rgn:4 [10.64.91.41]:16924
13:36:04      rgn:1 [10.64.91.91]:16394
13:36:04      xoip options: fax:T38 modem:off tty:US uid:0x50001f
13:36:04      xoip ip: [10.64.91.91]:16394
13:36:06      4 3 # Play greeting and collect 1 d...
13:36:06      4 4 collect 1 digits after annn 11001 for none
13:36:06 SIP>SIP/2.0 200 OK
```

- Other useful Communication Manager commands are, ***list trace station***, ***list trace vdn***, ***list trace vector***, ***list trace trunk***, ***list trace station***, ***status trunk***, and ***status station***.

## 10.3. 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. Verify that the **Tests Pass**, **Alarms**, **Service State**, and **Data Replication** columns, all show good status.

Session Manager

Dashboard

Session Manager Admin...

Global Settings

Communication Profile ...

Network Configuration

Device and Location ...

Application Configur...

System Status

System Tools

Help ?

Session Manager Dashboard

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

Session Manager Instances

Service State

Shutdown System

EASG

As of 1:45 PM

1 Item

Show All

Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Version
<input type="checkbox"/>	<a href="#">Session Manager</a>	Core	✓	0/0/0	Up	Accept New Service	2/15	0	5/6	✓	✓	Normal	Enabled	8.1.0.0.810007

Select : All, None

In the example, the entry **2/15** under the **Entity Monitoring** column shows that there are alarms on 2 out of the 15 Entities being monitored by Session Manager. 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

15 Items Filter: Enable

	SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	<a href="#">Aura Messaging</a>	IPv4	10.64.91.84	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">Breeze</a>	IPv4	10.64.91.18	5061	TLS	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
<input type="radio"/>	<a href="#">CM-TG1</a>	IPv4	10.64.91.75	5081	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">CM-TG2</a>	IPv4	10.64.91.75	5071	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">CM-TG3</a>	IPv4	10.64.91.75	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">CM-TG4</a>	IPv4	10.64.91.75	5064	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">CM-TG5</a>	IPv4	10.64.91.75	5065	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">CM-TG7</a>	IPv4	10.64.91.75	5067	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">ExperiencePortal</a>	IPv4	10.64.91.90	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">Presence</a>	IPv4	10.64.91.18	5061	TLS	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
<input type="radio"/>	<a href="#">SBC1</a>	IPv4	10.64.91.50	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">SBC2</a>	IPv4	10.64.91.100	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">SBC2-101</a>	IPv4	10.64.91.101	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">SBCE-ATT</a>	IPv4	10.64.91.40	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
<input type="radio"/>	<a href="#">SBCE-Toll Free</a>	IPv4	10.64.91.41	5061	TLS	FALSE	UP	405 Method Not Allowed	UP

Select : None

**Note** – On the **SBCE-Toll Free** Entity from the list of monitored entities above, the **Reason Code** column indicates that Session Manager has received a SIP **405 Method Not Allowed** response to the SIP OPTIONS it generated. This response is sufficient for SIP Link Monitoring to consider the link up. Also note that the Avaya SBCE sends the Session Manager generated OPTIONS on to the AT&T IPTF Border Element, and it is the AT&T Border Element that is generating the 405 response, and the Avaya SBCE sends it back to Session Manager.

Other Session Manager useful verification and troubleshooting tools include:

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

## 10.4. Avaya Session Border Controller for Enterprise Verification

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

### 10.4.1. Incidents

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

Device: SBCE8-70 Alarms **Incidents** Status Logs Diagnostics Users Settings Help Log Out

### Session Border Controller for Enterprise

**EMS Dashboard**

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

**Dashboard**

**Information**

System Time	08:15:41 AM MDT	<a href="#">Refresh</a>
Version	8.0.1.0-10-17555	
Build Date	Tue Jul 30 22:53:51 UTC 2019	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	10/16/2019 09:07:57 MDT	
Failed Login Attempts	0	

**Installed Devices**

EMS
SBCE8-70

**Active Alarms (past 24 hours)**

None found.

**Incidents (past 24 hours)**

SBCE8-70: Call Audit Cleanup

Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures. Further Information can be obtained by clicking on an incident in the incident viewer.

### Incident Viewer

Device: All Category: All Clear Filters Refresh Generate Report

Displaying results 1 to 15 out of 2000.

ID	Device	Date & Time	Category	Type	Cause
785619498994851	SBCE8-70	Oct 16, 2019 9:16:37 AM	Media Anomaly Detection	Media Inactivity Detected From Both Parties	Call Audit Cleanup
785616619198423	SBCE8-70	Oct 16, 2019 7:40:38 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
785616619190094	SBCE8-70	Oct 16, 2019 7:40:38 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
785616503469695	SBCE8-70	Oct 16, 2019 7:36:46 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
785616503469585	SBCE8-70	Oct 16, 2019 7:36:46 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
785616501493307	SBCE8-70	Oct 16, 2019 7:36:42 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
785616501482423	SBCE8-70	Oct 16, 2019 7:36:42 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
785317561958470	SBCE8-70	Oct 9, 2019 9:32:03 AM	Policy	Routing Failure	Max forwards Exceeded
785317555809802	SBCE8-70	Oct 9, 2019 9:31:51 AM	Policy	Routing Failure	Max forwards Exceeded

## 10.4.2. Server Status

The **Server Status** screen 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 interface. The top navigation bar includes "Device: SBCE8-70", "Alarms", "Incidents", "Status" (selected), "Logs", "Diagnostics", and "Users". The left sidebar shows the "EMS Dashboard" and various configuration options. The main content area displays the "Server Status" information, including "System Time", "Version", "Build Date", "License State", and "Aggregate Licensing Overages".

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 8.9**.

The screenshot shows the Avaya SBCE interface. The top navigation bar includes "Device: SBCE8-70", "Alarms", "Incidents", "Status" (selected), "Logs", "Diagnostics", and "Users". The left sidebar shows the "EMS Dashboard" and various configuration options. The main content area displays the "Status" information, including a table of connected SIP Servers.

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
SM8	10.64.91.81	10.64.91.81	5061	TLS	UP	UNKNOWN	11/06/2019 14:55:44 MST
IPOSE-Call-Server	10.64.19.170	10.64.19.170	5061	TLS	UP	UNKNOWN	11/06/2019 14:55:58 MST
ATT-TollFree-trk-svr	192.168.225.210	192.168.225.210	5060	UDP	UP	UNKNOWN	11/06/2019 14:52:36 MST

## 10.4.3. Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces. 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 Avaya SBCE interface. The top navigation bar includes "Device: SBCE8-70", "Alarms", "Incidents", "Status", "Logs", "Diagnostics", and "Users". The left sidebar shows the "EMS Dashboard" and various configuration options. The main content area displays the "Packet Capture" configuration form, including fields for "Status", "Interface", "Local Address", "Remote Address", "Protocol", "Maximum Number of Packets to Capture", and "Capture Filename".



**Note** – Specifying **All** in the **Interface** field will result in the Avaya SBCE capturing traffic from both the A1 and B1 interfaces defined in the reference configuration. Also, when specifying the **Maximum Number of Packets to Capture**, estimate a number large enough to include all packets for the duration of the test.

When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, hit the **Stop Capture** button at the bottom.

## Session Border Controller for Enterprise

EMS Dashboard  
Device Management  
Backup/Restore  
System Parameters  
Configuration Profiles  
Services  
Domain Policies  
TLS Management  
Network & Flows  
DMZ Services  
Monitoring & Logging  
SNMP  
Syslog Management  
Debugging  
**Trace**  
Log Collection  
DoS Learning  
CDR Adjunct

### Trace: SBCE8-70

**Packet Capture** Captures

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

**Packet Capture Configuration**  
Status: In Progress  
Interface: Any  
Local Address: All  
Remote Address: \*  
Protocol: All  
Maximum Number of Packets to Capture: 10000  
Capture Filename: test1.pcap  
Stop Capture

Select the **Captures** tab to view the files created during the packet capture.

## Session Border Controller for Enterprise

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

### Trace: SBCE8-70

**Packet Capture** **Captures**

File Name	File Size (bytes)	Last Modified	
test1_20190724082944.pcap	696,320	July 24, 2019 8:30:26 AM MDT	Delete

Refresh

The packet capture file can be downloaded and then viewed using a Network Protocol Analyzer like WireShark.

## 11. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, Avaya Aura® Experience Portal 7.2 and the Avaya Session Border Controller for Enterprise 8.0.1, can be configured to interoperate successfully with the AT&T IP Toll Free service, within the constraints described in **Section 2.2**.

Testing was performed on a simulated AT&T IP Toll Free service circuit. The reference configuration shown in these Application Notes is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

## 12. References

The Avaya product documentation is available at <http://support.avaya.com> unless otherwise noted.

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

- [1] *Deploying Avaya Aura® Session Manager and Branch Session Manager in Virtualized Environment*, Release 8.1, Issue 1, June 2019
- [2] *Administering Avaya Aura® Session Manager*, Release 8.1, Issue 1, June 2019
- [3] *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.1.x, Issue 2, July 2019
- [4] *Administering Avaya Aura® System Manager for Release 8.1*, Release 8.1.x, Issue 3, July 2019

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

- [5] *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 8.1.x, Issue 2, August 2019
- [6] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 3, August 2019
- [7] *Administering Avaya G430 Branch Gateway*, Release 8.1.x, Issue 1, June 2019
- [8] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.x, Issue 7, June 2019
- [9] *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*, Issue 1.1, June 2018
- [10] *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010

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

- [11] *Administering Avaya Session Border Controller for Enterprise*, Release 8.0.x, Issue 4, August 2019
- [12] *Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment*, Release 8.0.x, Issue 3, August 2019

### **Avaya Aura® Experience Portal**

- [13] *Administering Avaya Aura® Experience Portal*, Release 7.2.3, Issue 1, September 2019
- [14] *Implementing Avaya Aura® Experience Portal on a single server*, Release 7.2.3, Issue 1, September 2019

### **AT&T IP Toll Free Service**

- [15] *AT&T IP Toll Free Service – Product Description*  
<https://www.business.att.com/products/ip-toll-free.html>

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

One of the important capabilities to the Experience Portal environment is the Avaya SBCE Refer Handling option. As described in **Section 3.2.2**, 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 AT&T.

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:** 89[0-9]{3}@.\* This will match 5-digit local extensions starting with 89, e.g., 89001.
- 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**

89[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**.

**Session Border Controller for Enterprise**

URI Groups: internal-extensions

URI Listing

89[0-9][3]@.*	Edit	Delete
71[0-9][3]@.*	Edit	Delete
20[0-9][3]@.*	Edit	Delete
50[0-9][3]@.*	Edit	Delete

Edit the existing AT&T 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 ATT-Interworking Profile created in **Section 8.7.2** and click **Edit**

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

**Session Border Controller for Enterprise**

Interworking Profiles: ATT-Interworking

General

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

Note that with the Refer Handling option enabled on the Avaya SBCE, the INVITE generated by the SBCE towards the 5 digit internal extensions is routed by Session Manager to Communication Manager via the local trunk (Trunk Group 3 in the reference configuration), not on the trunk group assigned for inbound calls from AT&T (Trunk Group 4). See **Section 5.8**. Depending on the codec priorities listed on the IP Codec Sets on the network regions associated to each trunk, this may cause the codec originally negotiated on the inbound call from AT&T to Experience Portal (i.e., G729A) to be re-negotiated to a different codec (i.e., G711U), once the call is transferred by Experience Portal to an internal extension in Communication Manager.

To avoid the issue described above, use the **change-ip-network-map** in Communication Manager to assign the IP address of the internal interface of the Avaya SBCE (10.61.91.41) to the network region associated to inbound calls from AT&T (e.g., network region 4, **Section 5.6.2**). With this setting, all calls arriving from the inside interface of the Avaya SBCE to a Communication Manager destination will be associated to network region 4, which uses IP Codec Set 4 for calls between region 4 (IPTF calls) and region 1 (the rest of the CPE).

**Step 1** - Enter the **change ip-network-map** command in Communication Manager and enter the following:

- **FROM / TO: 10.64.91.41**
- **Subnet Bits: 32**
- **Network Region: 4**

change ip-network-map

Page 1 of 63

IP ADDRESS MAPPING

IP Address	Subnet Bits	Network Reg	VLAN	Emergency Location	Ext
FROM: 10.64.91.41	/32	4	n		
TO: 10.64.91.41					
FROM:	/		n		
TO:					

## 14. Appendix B – Configuration for G.711 Fax Testing

During the compliance test, in order to perform G.711 pass-through fax testing, the network region assigned to the G430 Media Gateway where the fax machine was connected was changed from region 1 (**Section 5.14**) to region 3. This network region utilized IP Codec Set 3 for calls between region 3 and region 4 (IPTF calls). Creating a dedicated network region and ip-codec-set for G.711 pass-through fax allowed for fax calls from this G430 Media Gateway to begin with codec G.711MU, while voice calls to other Media Gateways, Media Servers, and IP endpoints belonging to region 1, will continue to request G.729A as the first codec choice. (**Section 5.7.2**).

This configuration is shown here for completeness and is only needed if G.711 pass-through is preferred to T.38 fax. See **Section 2.2** for limitations.

To create the IP Network Region 3 used for G.711 fax testing, repeat the steps in **Section 5.6.1** with the following changes:

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

- Enter a descriptive name (e.g., **G711 Fax**).
- Enter **3** for the **Codec Set** parameter.

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

- Set codec set **3** for **dst rgn 4**.
- Note that **dst rgn 3** is pre-populated with codec set **3** (from page 1 provisioning).

change ip-network-region 3										Page 4 of 20		
Source Region: 3		Inter Network Region Connection Management								I	M	
										G	A	t
<b>dst</b>	<b>codec</b>	direct	WAN-BW-limits		Video	Intervening			Dyn	A	G	c
<b>rgn</b>	<b>set</b>	WAN	Units	Total	Norm	Prio	Shr	Regions	CAC	R	L	e
1	1	y	NoLimit							n		t
2	2	y	NoLimit							n		t
3	3										all	
4	3	y	NoLimit							n		t

Repeat the steps in **Section 5.7.1** to create IP Codec Set 3 with the following changes:

**Step 1 - On Page 1 of the form**

- Provision the codecs in the order shown below. Note that **G.711MU** is listed as the preferred codec.
- Set **Frames Per Pkt** to **3**. This will auto-populate **30** for the **Packet Size (ms)** field, and specify a PTIME value of 30 in the SDP.

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

- Set the **Fax Mode** to **off**.

change ip-codec-set 3

Page 1 of 2

IP CODEC SET

Codec Set: 3

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711MU	n	3	30
2: G.729A	n	3	30
3: G.729B	n	3	30

Media Encryption

1: 1-srtp-aescm128-hmac80

2: none

Encrypted SRTCP: enforce-unenc-srtcp

change ip-codec-set 3

Page 2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? n

	Mode	Redundancy	Packet Size (ms)
FAX	off	0	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	



---

**©2019 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by <sup>TM</sup> and <sup>®</sup> 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).