



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, Avaya Experience Portal 8.1 and Avaya Session Border Controller for Enterprise 10.1 with AT&T IP Flexible Reach - Enhanced Features – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, Avaya Experience Portal 8.1 and Avaya Session Border Controller for Enterprise 10.1, with the AT&T IP Flexible Reach - Enhanced Features service, using AT&T's **AVPN** or **ADI/PNT** transport connections.

The AT&T Flexible Reach is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for their voice communication needs. The AT&T IP Flexible Reach-Enhanced Features service is a SIP based service which includes additional network-based features which are not part of IP Flexible Reach service.

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	10
2.4.	SIP Message – Packet Optimization	10
3.	Reference Configuration.....	11
3.1.	Illustrative Configuration Information	13
3.2.	Call Flows	14
3.2.1.	Communication Manager Basic Flows.....	14
3.2.2.	Network Based Blind Transfer Call Flow (Communication Manager Vector).....	17
3.2.3.	Network Based Attended/Unattended Transfer Call Flow initiated by Communication Manager Station.....	18
3.2.4.	Experience Portal Call Flows.....	19
4.	Equipment and Software Validated	22
5.	Configure Avaya Aura® Communication Manager.....	23
5.1.	Verify Licensed Features	23
5.2.	System-Parameters Features	25
5.3.	Dial Plan.....	26
5.4.	Node Names	26
5.5.	Processor Ethernet Configuration	27
5.6.	IP Network Regions	27
5.6.1.	IP Network Region 1 – Local CPE Region	27
5.6.2.	IP Network Region 4 – AT&T Trunk Region	29
5.7.	IP Codec Sets	30
5.7.1.	Codecs for IP Network Region 1 (calls within the CPE).....	30
5.7.2.	Codecs for IP Network Region 4 (calls to/from AT&T)	31
5.8.	SIP Trunks.....	32
5.8.1.	SIP Trunk for Inbound/Outbound AT&T calls.....	32
5.8.2.	Local SIP Trunk (Avaya SIP Telephone, Messaging Access, etc.).....	36
5.9.	Public Numbering	37
5.10.	Private Numbering.....	38
5.11.	Route Patterns.....	38
5.11.1.	Route Pattern for National Calls to AT&T	38
5.11.2.	Route Pattern for International Calls to AT&T.....	39
5.11.3.	Route Pattern for Service Calls to AT&T	40
5.11.4.	Route Pattern for Calls within the CPE.....	40
5.12.	Automatic Route Selection (ARS) Dialing	41
5.13.	Automatic Alternate Routing (AAR) Dialing	41
5.14.	Avaya G430 Media Gateway Provisioning	42
5.15.	Avaya Aura® Media Server Provisioning.....	43
5.16.	Save Translations.....	44
5.17.	Verify TLS Certificates – Communication Manager	45
6.	Configure Avaya Aura® Session Manager	46
6.1.	System Manager Login and Navigation.....	47

6.2.	SIP Domain	48
6.3.	Locations	49
6.3.1.	Main Location	49
6.3.2.	CM-TG-5 Location	49
6.3.3.	Common-SBCs Location	50
6.4.	Configure Adaptations	50
6.4.1.	Adaptation for Avaya Aura® Communication Manager Extensions	50
6.4.2.	Adaptation for the AT&T IP Flexible Reach – Enhanced Features Service	52
6.5.	SIP Entities	53
6.5.1.	Avaya Aura® Session Manager SIP Entity	53
6.5.2.	Avaya Aura® Communication Manager SIP Entity – Public Trunk	55
6.5.3.	Avaya Aura® Communication Manager SIP Entity – Local Trunk.....	56
6.5.4.	Avaya Session Border Controller for Enterprise SIP Entity	56
6.5.5.	Avaya Messaging SIP Entity	56
6.5.6.	Avaya Experience Portal SIP Entity	56
6.6.	Entity Links	57
6.6.1.	Entity Link to Avaya Aura® Communication Manager – Public Trunk.....	57
6.6.2.	Entity Link to Avaya Aura® Communication Manager – Local Trunk.....	58
6.6.3.	Entity Link for the AT&T IP Flexible Reach – Enhanced Features Service via the Avaya SBCE	58
6.6.4.	Entity Link to Avaya Messaging	58
6.6.5.	Entity Link to Avaya Experience Portal	58
6.7.	Time Ranges – (Optional)	59
6.8.	Routing Policies	59
6.8.1.	Routing Policy for AT&T Inbound Calls to Communication Manager	59
6.8.2.	Routing Policy for Inbound Routing to Avaya Messaging.....	61
6.8.3.	Routing Policy for Inbound Calls to Experience Portal.....	61
6.8.4.	Routing Policy for Outbound Calls to AT&T.....	61
6.9.	Dial Patterns	62
6.9.1.	Matching Inbound PSTN Calls to Avaya Aura® Communication Manager	63
6.9.2.	Matching Outbound Calls to AT&T	65
6.10.	Verify TLS Certificates – Session Manager.....	66
7.	Avaya Experience Portal.....	70
7.1.	Background	70
7.2.	Logging In and Licensing	71
7.3.	Verify TLS Certificates – Experience Portal	73
7.4.	VoIP Connection	74
7.5.	Speech Servers	76
7.6.	Application References	77
7.7.	MPP Servers and VoIP Settings.....	78
7.8.	Configuring RFC2833 Event Value Offered by Experience Portal	81
8.	Configure Avaya Session Border Controller for Enterprise	82
8.1.	Device Management – Status	83
8.2.	TLS Management.....	85
8.2.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise	85
8.2.2.	Server Profiles.....	86

8.2.3.	Client Profiles	88
8.3.	Network Management	90
8.4.	Advanced Options	92
8.5.	Media Interfaces	93
8.6.	Signaling Interfaces	94
8.7.	Server Interworking Profiles	95
8.7.1.	Server Interworking Profile – Enterprise	95
8.7.2.	Server Interworking – AT&T	96
8.8.	Signaling Manipulation	98
8.9.	SIP Server Profiles	99
8.9.1.	SIP Server Profile – Session Manager	99
8.9.2.	SIP Server Profile – AT&T	101
8.10.	Routing Profiles	103
8.10.1.	Routing Profile – Session Manager	103
8.10.2.	Routing Profile – AT&T	104
8.11.	Topology Hiding Profiles	105
8.11.1.	Topology Hiding – Enterprise	105
8.11.2.	Topology Hiding – AT&T	106
8.12.	Application Rules	107
8.13.	Media Rules	108
8.13.1.	Enterprise – Media Rule	108
8.13.2.	AT&T – Media Rule	110
8.14.	Signaling Rules	111
8.14.1.	Signaling Rule – Enterprise	111
8.14.2.	Signaling Rule – AT&T	112
8.15.	Endpoint Policy Groups	112
8.15.1.	End Point Policy Group – Enterprise	112
8.15.2.	Endpoint Policy Group – AT&T	114
8.16.	Endpoint Flows – Server Flows	115
8.16.1.	Server Flows – Enterprise	115
8.16.2.	Server Flow – AT&T	116
9.	AT&T IP Flexible Reach – Enhanced Features Configuration	116
10.	Verification Steps	116
10.1.	AT&T IP Flexible Reach – Enhanced Features	116
10.2.	Avaya Aura® Communication Manager Verification	118
10.3.	Avaya Aura® Session Manager Verification	120
10.4.	Avaya Session Border Controller for Enterprise Verification	123
10.4.1.	Incidents	123
10.4.2.	Server Status	124
10.4.3.	Diagnostic	125
10.4.4.	Tracing	125
11.	Conclusion	127
12.	References	128
13.	Appendix A – Avaya SBCE – Refer Handling	129
14.	Appendix B – Avaya SBCE – SigMa Script File	132

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, Avaya Experience Portal 8.1 and Avaya Session Border Controller for Enterprise Release 10.1, with the AT&T IP Flexible Reach - Enhanced Features service using AT&T Virtual Private Network (AVPN) or AT&T Dedicated Internet Service (ADI/PNT) transport connections.

Avaya Aura® Communication Manager 10.1 (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 10.1 (Session Manager) is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise.

Avaya 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 application was used to exercise various SIP call flow scenarios.

The Avaya Session Border Controller for Enterprise 10.1 (Avaya SBCE) is the point of connection between Session Manager and the AT&T IP Flexible Reach - Enhanced Features (IPFR-EF) service and is used to not only secure the SIP trunk, but also to adjust the SIP signaling and media for interoperability.

The AT&T Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for their voice communication needs. The AT&T IP Flexible Reach-Enhanced Features service is a SIP based service which includes additional network-based features which are not part of IP Flexible Reach service. The AT&T IP Flexible Reach - Enhanced Features service utilizes AT&T's AVPN¹ or ADI/PNT² transport services.

Note – The AT&T IP Flexible Reach - Enhanced Features service will be referred to as IPFR-EF in the remainder of this document.

¹ AVPN supports compressed RTP (cRTP).

² ADI/PNT does not 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 IPFR-EF and the Customer Premises Equipment (CPE) containing Communication Manager, Session Manager, Experience Portal and Avaya SBCE (see **Section 3.2** for call flow examples).

The test environment consisted of:

- A simulated enterprise with Communication Manager, Session Manager, System Manager (for Session Manager provisioning) Experience Portal, Avaya SBCE, Avaya phones, and fax machines (Ventafax application). Avaya Messaging (Messaging) is used to provide voicemail capabilities for the CPE.
- IPFR-EF service test lab circuit, connected to the simulated enterprise via AVPN transport.

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

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

For the testing associated with this Application Note, the interface between Avaya systems and the AT&T IP Flexible Reach service did not include use of any specific encryption features as requested by AT&T.

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

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 AT&T IPFR-EF network. Calls were made between the PSTN, via the AT&T IPFR-EF network, and the CPE.

The following SIP trunking VoIP features were tested with the IPFR-EF service:

- Inbound and outbound voice calls between telephones controlled by the CPE and the PSTN using G.729A and G.711MU codecs. Phone types included SIP, H.323, digital and analog telephones at the enterprise.
- DTMF using RFC 2833
 - Outbound call to PSTN application requiring post-answer DTMF (e.g., an IVR or voice mail system).
 - Inbound call from PSTN to Avaya CPE application requiring post-answer DTMF (e.g., Messaging, Experience Portal, Communication Manager vector digit collection steps).
- Requests for privacy for Communication Manager outbound calls to the PSTN, as well as privacy requests for inbound calls from the PSTN to Communication Manager users.
- SIP OPTIONS messages used to monitor the health of the SIP trunks between the CPE and AT&T.
- Additional PSTN numbering plans (e.g., operator assist, toll-free and International).
- Telephony features such as hold, transfer, and conference.
- SIP Diversion Header for call redirection.
 - Call Forwarding
 - EC500
- Long duration calls.
- Inbound/Outbound fax calls using T.38 or G.711MU.
- Failover test between primary and secondary AT&T Border Elements.
- AT&T IPFR-EF service features such as:
 - Simultaneous Ring
 - Sequential Ring
 - Call Forward – Always
 - Call Forward – Busy
 - Call Forward – Ring No Answer
 - “Blind” and “Attended” transfers utilizing Refer messaging.
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements and/or music on hold) and Automatic Speech Recognition.
- Experience Portal use of SIP REFER to redirect inbound calls, via the Avaya SBCE, to the appropriate Communication Manager agent extension.
- Call and two-way talk path establishment between callers and Communication Manager agents following redirection from Experience Portal.
- Inbound calls to a self-service Experience Portal application which forwards the call to another PSTN number over the IPFR-EF service, using SIP INVITE and SIP REFER methods.

Avaya Remote Worker endpoints were used in the reference configuration. A Remote Worker is a SIP endpoint that resides in the untrusted network, registered to Session Manager at the enterprise, using Transport Layer Security (TLS), via the Avaya SBCE. Remote Workers offer the same functionality as any other endpoint at the enterprise. The SIP endpoints used as Remote Workers included Avaya Workplace Client for Windows and Avaya Agent for Desktop.

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

Note – Documents used to provision the test environment are listed in **Section 12**. In the following sections, references to these documents are indicated by the notation [x], where x is the document reference number.

2.2. Test Results

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

- 1) **Network-Based Consultative Call Transfer (Attended transfer)**. During consultative/attended call transfers to the PSTN, it was observed that on J100 series phones with SIP firmware AT&T responded with "481 Malformed or Unexpected" errors messages followed by "200 Minimal Impact". This behavior was not observed on phones with H.323 firmware. There was no user impact.
- 2) **IPFR-EF Simultaneous Ring and Sequential Ring - Loss of calling display information on Communication Manager stations**. If the Communication Manager station associated with these IPFR-EF "secondary" number for Simultaneous Ring and Sequential Ring scenarios answers the call, the phone may not display all the calling information. By default, Communication Manager expects a display update from the network in the P-Asserted-Identity (PAI) header. However, the subsequent network signaling does not contain a PAI header, and the From header must be used instead. The recommended workaround is described in **Section 5.8.1**, where Communication Manager will retrieve the display information using the *From* header.
- 3) **T.38 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 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.
- 4) **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.

- 5) **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 SigMa script (**Section 8.8**) is used to remove these headers.
- 6) **SIP OPTIONS** – The AT&T IPFR-EF service is configured to send SIP OPTIONS messages with a Max-Forwards header value of “0”. This is by design from AT&T and Avaya SBCE correctly responded with “483 Too Many Hops”. AT&T considers this response acceptable to keep the trunk in service. However, an incident is logged on the Avaya SBCE for each OPTIONS message received with Max-Forwards=0. To prevent the incident log from being filled with these route failure messages, an optional SigMa script (**Section 8.8**) can be added to the Avaya SBCE to change the Max-Forwards value to an acceptable value to reach Communication Manager.
- 7) **Experience Portal consultative call transfer.** The Experience Portal test application used for compliance testing performs consultative call transfer of inbound calls that are transferred back to AT&T using SIP INVITE, with the original calling party number in the From and P-Asserted Identity headers, and it does not contain a Diversion header. In this scenario, since none of the headers in the outbound INVITE contains a number recognizable by the AT&T network, consultative call transfers out the AT&T IPFR-EF service fail. As a workaround, a SigMa script file (**Section 8.8**) was created to modify the P-Asserted-Identity header on outbound INVITES from Experience Portal to the PSTN, with the DID number assigned to Experience Portal, known to AT&T.
In addition, Experience Portal blind transfers out to AT&T using SIP REFER were tested successfully. Also, consultative and blind transfers from Experience Portal to Communication Manager were successful as well.
- 8) **Some Avaya SIP endpoints use different RFC2833 DTMF Payload Type than defined in CM trunk provisioning.** Although Communication Manager can specify the default RFC2833 payload type to be used on the SIP trunk to AT&T (payload type 100 in the compliance test), outbound calls originating from some Avaya SIP Deskphones and softphones used payload type 101 in requests on the SIP trunk to AT&T. The payload type on these SIP endpoints is ultimately controlled by the 46xxsettings file that is loaded on the phones. Calls originating from these endpoints had the payload type dynamically negotiated with AT&T to type 101 during the call setup. No issues were found during testing as a result of this behavior.
- 9) **Emergency 911/E911 Services Limitations and Restrictions.** Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) documented in these Application Notes will properly operate with AT&T IPFR-EF to complete 911/E911 calls. 911/E911 was not tested during the compliance test; therefore, it is the customer’s responsibility to ensure proper operation with the equipment/software vendor. While AT&T IPFR-EF services support 911/E911 calling capabilities under certain Calling Plans, there are circumstances when the 911/E911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at <http://new.serviceguide.att.com>. Such circumstances include, but are not limited to, relocation

of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

2.3. Support

For more information on the AT&T IP Flexible Reach service visit:

<https://www.business.att.com/products/sip-trunking.html>. AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

2.4. SIP Message – Packet Optimization

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

In the sample configuration, the following headers were removed:

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

To help reduce the packet size further, the Avaya SBCE can remove the Avaya “*epv*” parameter that may be included within the Contact header of outbound messages, by applying a Sigma script to the AT&T SIP server profile. See **Sections 8.8** and **8.9.2**.

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the compliance testing, with the AT&T IPFR-EF service test lab circuit, connected to the simulated enterprise site via AVPN transport.

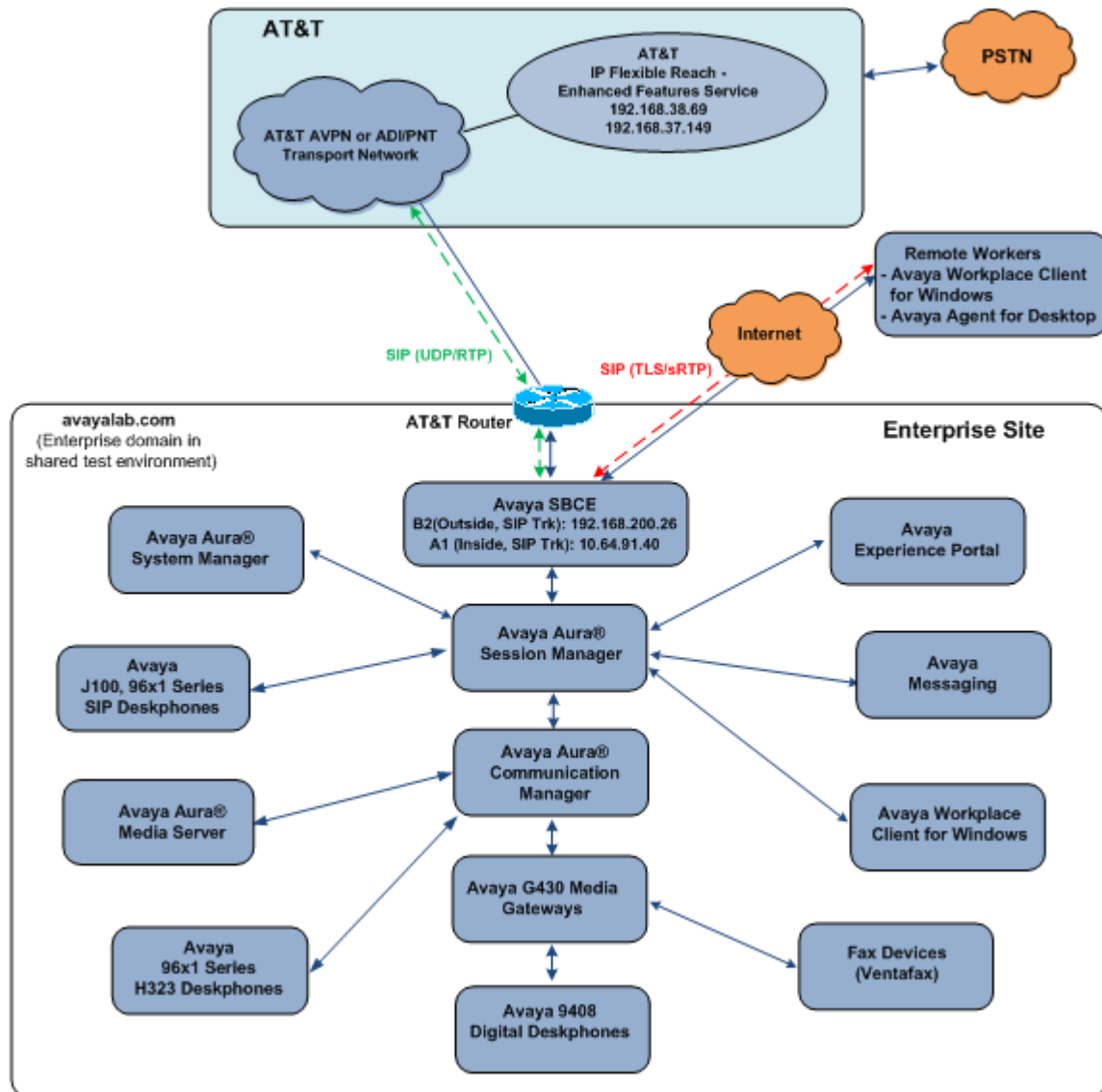


Figure 1: Reference configuration

The following components were used in the reference configuration:

- Avaya Session Border Controllers for Enterprise
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Avaya Aura® Communication Manager
- Avaya Experience Portal
- Avaya G430 Media Gateway
- Avaya Aura® Media Server
- Avaya Messaging
- Avaya 96X1 Series IP Deskphones using the SIP and H.323 software bundles
- J100 Series IP Deskphones using the SIP and H.323 software bundles
- Avaya Workplace Client for Windows
- Avaya Agent for Desktop
- Avaya 2420 Digital Phones
- Ventafax fax software

Avaya Aura® System Manager provides a common administration interface for centralized management of Session Manager and Communication Manager. Avaya Messaging was used in the reference configuration to provide voice mailbox capabilities. This solution is extensible to other messaging platforms. The provisioning of Avaya Messaging is beyond the scope of this document.

Note that while an Avaya G430 Media Gateway and an Avaya Media Server are used in the reference configuration, this solution is extensible to other Avaya Media Gateways.

The Avaya SBCE provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPFR-EF service and the enterprise internal network.

The IPFR-EF service Border Element (BE) uses SIP over UDP to communicate with enterprise edge SIP devices, (e.g., the Avaya SBCE in this sample configuration). Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements. In the reference configuration, Session Manager uses SIP over TLS to communicate with the Avaya SBCE, Experience Portal, Messaging and Communication Manager.

Testing was performed using an IPFR-EF service test lab circuit.

3.1. Illustrative Configuration Information

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

Note – The IPFR-EF service Border Element IP address and DID/DNIS digits are shown in this document as examples. AT&T Customer Care will provide the actual IP addresses and DID/DNIS digits as part of the IPFR-EF provisioning process.

Component	Illustrative Value in these Application Notes
Avaya Aura® Session Manager	
IP Address	10.64.91.81
Avaya Aura® Communication Manager	
IP Address	10.64.91.75
Avaya Aura® System Manager	
IP Address	10.64.90.82
Avaya Messaging	
IP Address	10.64.91.145
Avaya Experience Portal	
IP Address	10.64.91.90
Avaya Session Border Controller for Enterprise (SBCE)	
IP Address of A1 Inside (Private) Interface	10.64.91.40
IP Address of B2 Outside (Public) Interface	192.168.200.26 (see note below)
AT&T Border Element	
IP Addresses	192.168.38.69 192.168.37.149

Table 1: Network Values Used in these Application Notes

Note – The Avaya SBCE Outside interface communicates with AT&T Border Elements (BEs) located in the AT&T IP Flexible Reach network. 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 addresses of **192.168.200.26** (Avaya SBCE public interface), **192.168.38.69** and **192.168.37.149** (AT&T BE IP addresses) are specified.

3.2. Call Flows

To understand how IPFR-EF service calls are handled by the Avaya CPE environment, several basic call flows are described in this section. However, for brevity, not all possible call flows are described.

3.2.1. Communication Manager Basic Flows

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

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

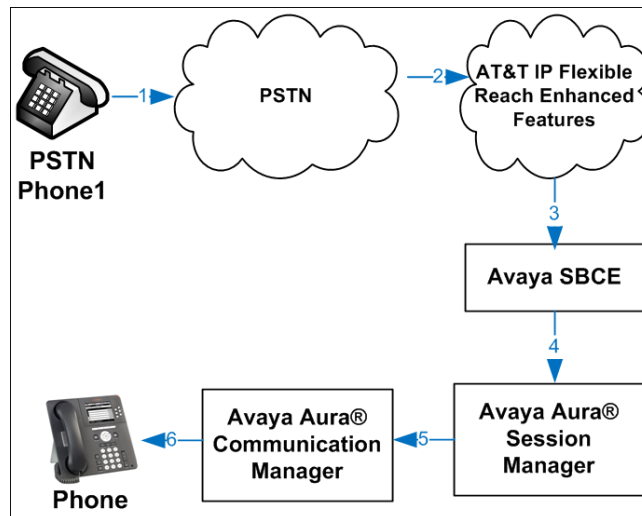


Figure 2: Inbound IPFR-EF Call

The second call scenario illustrated is an outbound call initiated on Communication Manager, routed to Session Manager, and is subsequently sent to the Avaya SBCE for delivery to the IPFR-EF service.

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

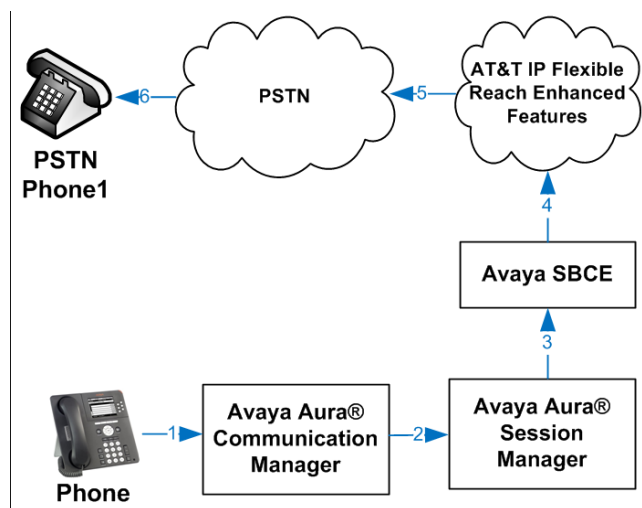


Figure 3: Outbound IPFR-EF Call

The third call scenario illustrated is an inbound IPFR-EF service call that arrives at the Avaya SBCE, to Session Manager, and subsequently Communication Manager. Communication Manager routes the call to a destination station; however, the station has set Call Forward to an alternate destination. Without answering the call, Communication Manager redirects the call back to the IPFR-EF service for routing to the alternate destination.

Note – In cases where calls are forwarded to an alternate destination such as an 8xx numbers, the IPFR-EF service requires the use of SIP Diversion Header for the redirected call to complete (see **Section 5.8.1**).

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

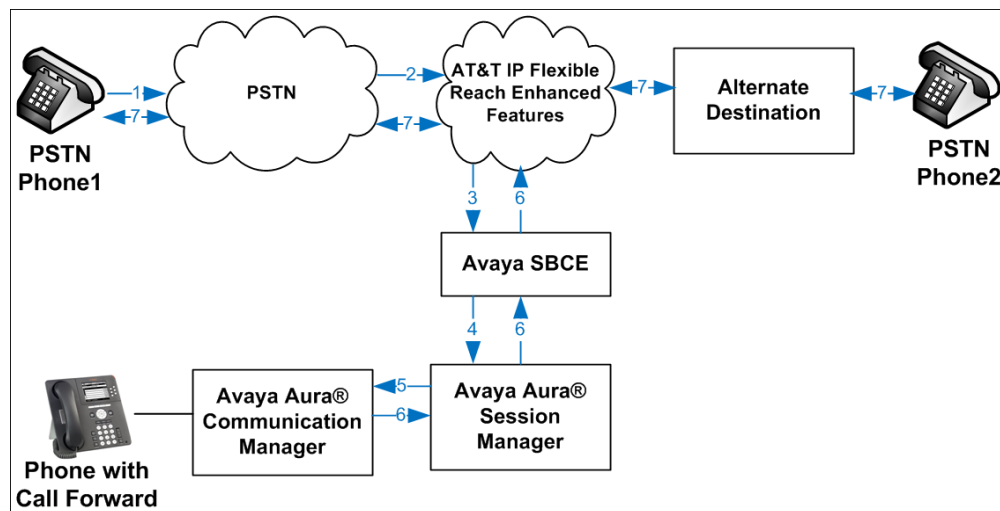


Figure 4: Station Re-directed (e.g., Call Forward) IPFR-EF Call

3.2.2. Network Based Blind Transfer Call Flow (Communication Manager Vector)

This section describes the call flow for IPFR-EF using SIP REFER to perform Network Based Blind Transfer. The REFER is generated by an inbound call to a Communication Manager Vector. The call scenario illustrated in **Figure 5** below is an inbound IPFR-EF call that arrives on Session Manager and is subsequently routed to Communication Manager, which in turn routes the call to a vector. The vector answers the call and, using REFER (without the Replaces parameter) redirects the call back to the IPFR-EF service for routing to an alternate destination.

1. A PSTN phone originates a call to an IPFR-EF number.
2. The PSTN routes the call to the IPFR-EF network.
3. IPFR-EF routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any necessary SIP header modifications and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Communication Manager routes the call to a VDN/Vector, which answers the call and plays an announcement, and attempts to redirect the call using a SIP REFER message. The REFER message specifies the alternate destination in its Refer-To header, and is routed back through Session Manager on to the Avaya SBCE. The Avaya SBCE sends the REFER to the IPFR-EF service.
7. IPFR-EF places a call to the alternate destination specified in the REFER, and upon answer, connects the calling party to the alternate party.
8. IPFR-EF clears the call on the redirecting/referring party (Communication Manager).

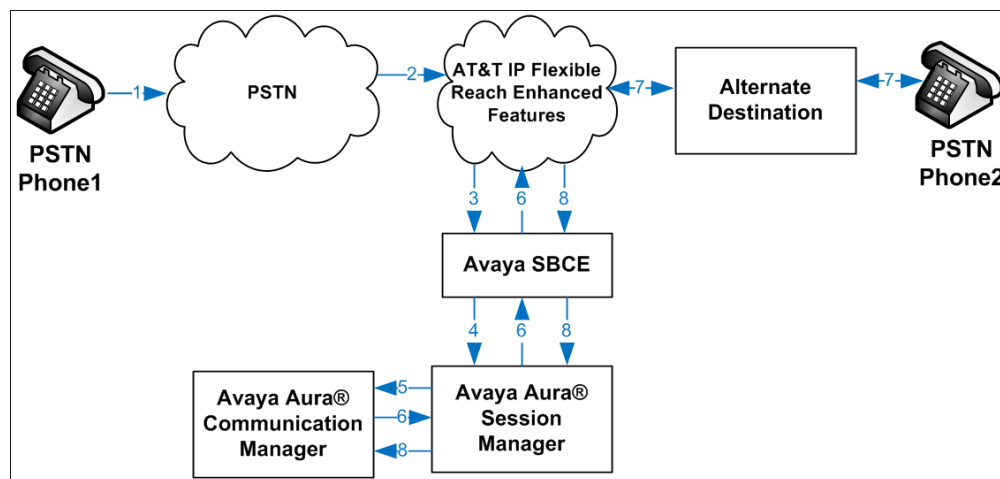


Figure 5: Network Based Blind Transfer Using REFER (Communication Manager Vector)

3.2.3. Network Based Attended/Unattended Transfer Call Flow initiated by Communication Manager Station

This section describes the call flow for IPFR-EF using SIP REFER to perform an Attended or Unattended Transfer. The call scenario illustrated in **Figure 6** below is an inbound IPFR-EF call that arrives on Session Manager and is subsequently routed to Communication Manager, which in turn routes the call to a station. The station answers the call and transfers it back out to a second PSTN destination. Communication Manager initiates a new call back out to Session Manager, the Avaya SBCE, and to the IPFR-EF service network. Communication Manager completes the transfer, using REFER (with the Replaces parameter), to the IPFR-EF service to connect the two active calls together.

1. A PSTN phone originates a call to an IPFR-EF number.
2. The PSTN routes the call to the IPFR-EF network.
3. IPFR-EF routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any necessary SIP header modifications and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Communication Manager. Communication Manager routes the call to a station.
6. The station answers the call and then transfers it to a new PSTN destination. Communication Manager initiates a new call back out to Session Manager, the Avaya SBCE, and to the IPFR-EF service network. Communication Manager redirects the call using a SIP REFER message when the transfer is completed by the station. The REFER message specifies the active call to replace and is routed back through Session Manager on to the Avaya SBCE. The Avaya SBCE sends the REFER to the IPFR-EF service.
7. IPFR-EF replaces the call with the alternate destination specified in the REFER and connects the calling party to the alternate party.
8. IPFR-EF clears the existing calls to Communication Manager.

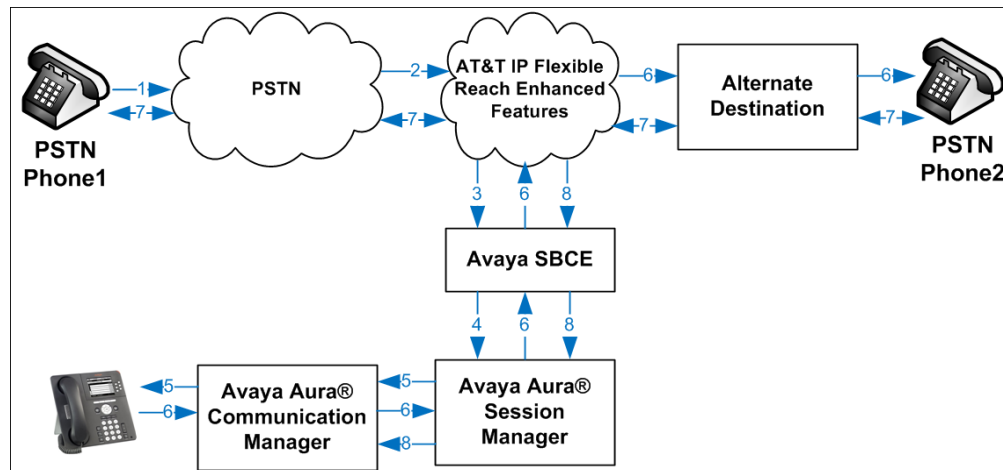


Figure 6: Attended/Unattended Transfer Using REFER (Communication Manager Station)

3.2.4. Experience Portal Call Flows

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

1. A PSTN phone originates a call to an IPFR-EF number.
2. The PSTN routes the call to the IPFR-EF network.
3. IPFR-EF 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.

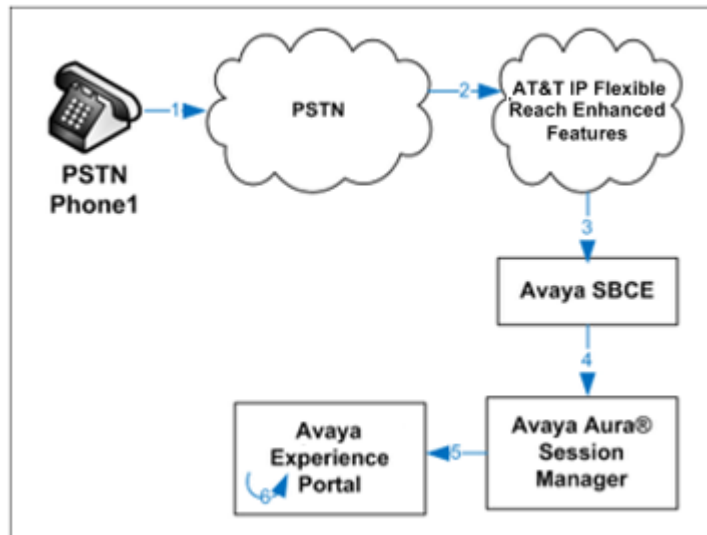


Figure 7: Inbound Call Handling Entirely by Avaya Experience Portal

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

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

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

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.

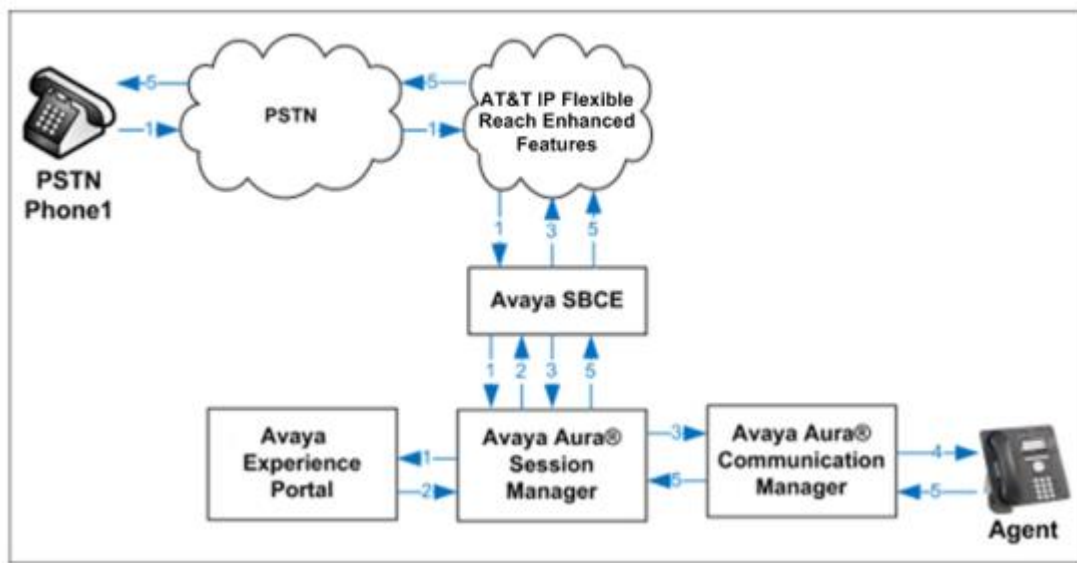


Figure 8: Avaya Experience Portal Transfers Call to Avaya Aura® Communication Manager

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

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

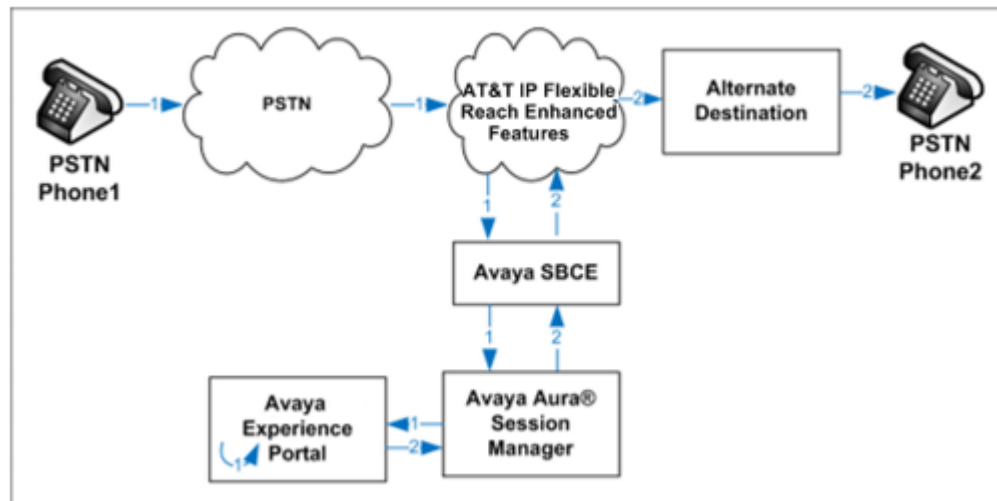


Figure 9: Inbound Call transferred by Experience Portal to another PSTN number

The Experience Portal test application used for compliance testing can perform blind or consultative call transfers of inbound calls that are to be transferred back to the PSTN. This is done in similar fashion to the network based transfer call flows shown previously for Communication Manager (**Section 3.2.2** and **Section 3.2.3**).

On a blind transfer, Experience Portal sends a REFER without the Replaces parameter back to IPFR-EF. On consultative transfers, Experience Portal places a new outbound call, sending a SIP INVITE out to the IPFR-EF network. Once the new call is answered, Experience Portal sends a REFER with Replaces parameter to the network. In both cases, IPFR-EF replaces the call with the alternate destination specified in the REFER and connects the calling party to the alternate party directly, clearing the existing calls to Experience Portal.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager	10.1.0.2 Service Pack 2 Build No. - 10.1.0.0.537353 Software Update Revision No: 10.1.0.2.0715160 Hot Fix - 1010215160
Avaya Aura® Session Manager	10.1.0.2.Service Pack 2 (10.1.0.2.1010219)
Avaya Aura® Communication Manager	10.1 Service Pack 1 (01.0.974.0-27372)
Avaya Session Border Controller for Enterprise	ASBCE 10.1 10.1.0.0-32-21432
Avaya Experience Portal	8.1.2.0.0202
Avaya Aura® Media Server	10.1.0 Service Pack 1
Avaya Messaging	10.8 SP1 (IXM-10.8.20.1406)
Avaya G430 Media Gateway	42.8.0
Avaya 96x1 Series IP Deskphone (H.323)	6.8.5.2.3
Avaya J179 IP Deskphone (H.323)	6.8.5.2.3
Avaya 96x1 Series IP Deskphone (SIP)	7.1.15.0.14
Avaya Workplace Client for Windows	3.31.2
Avaya Agent for Desktop	2.0.6.25
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
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 documents 5 – 9 in the References section for additional information.

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. Verify Licensed Features

Note – This section describes steps to verify Communication Manager feature settings that are required for the reference configuration described in these Application Notes. Depending on access privileges and licensing, some or all of the following settings might only be viewed, and not modified.

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
Maximum Administered SIP Trunks:			4000	75
Max Administered Ad-hoc Video Conferencing Ports:			4000	0
Max Number of DS1 Boards with Echo Cancellation:			80	0

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

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

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

display system-parameters customer-options		Page 5 of 12
OPTIONAL FEATURES		
Emergency Access to Attendant? y	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	Media Encryption Over IP? y	
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 4 - On **Page 6** of the form, verify that the **Processor Ethernet** field is set to **y**.

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

5.2. System-Parameters Features

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

change system-parameters features	Page 1 of 19
FEATURE-RELATED SYSTEM PARAMETERS	
Self Station Display Enabled? y	
Trunk-to-Trunk Transfer: all	
Automatic Callback with Called Party Queuing? n	
Automatic Callback - No Answer Timeout Interval (rings): 3	
Call Park Timeout Interval (minutes): 10	
Off-Premises Tone Detect Timeout Interval (seconds): 20	
AAR/ARS Dial Tone Required? y	
Music (or Silence) on Transferred Trunk Calls? all	
DID/Tie/ISDN/SIP Intercept Treatment: attendant	
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred	
Automatic Circuit Assurance (ACA) Enabled? n	
Abbreviated Dial Programming by Assigned Lists? n	
Auto Abbreviated/Delayed Transition Interval (rings): 2	
Protocol for Caller ID Analog Terminals: Bellcore	
Display Calling Number for Room to Room Caller ID Calls? n	

5.3. Dial Plan

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

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

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

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

5.4. Node Names

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

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

- Session Manager SIP signaling interface (e.g., **SM** and **10.64.91.81**).
- Media Server (e.g., **AMS** and **10.64.91.86**). The Media Server node name is only needed if a Media Server is present.

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

5.5. Processor Ethernet Configuration

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.

```
display ip-interface procr                                     Page 1 of 2
                                                              IP INTERFACES
Type: PROCR
Target socket load: 4800
Enable Interface? y                                           Allow H.323 Endpoints? y
Allow H.248 Gateways? y                                       Gatekeeper Priority: 5
Network Region: 1
                                                              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).

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.

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	

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	t	
dst rgn	codec set	direct	WAN	Units	WAN-BW-limits	Video	Intervening	Dyn	A	G	c	
					Total	Norm	Prio	Shr	Regions	CAC	R L e	
1	1										all	
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 rgn	codec set	direct	WAN	Units	WAN-BW-limits	Video	Intervening	Dyn	A	G	c	
					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	

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.

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** and **G.729A** are included in the codec list. Note that the packet interval size will default to 20ms. Set the **Media Encryption** based on customer requirements. In the reference configuration, **1-srtp-aescm128-hmac80** was the preferred crypto suite, with **none** set as the second option.

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

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

change ip-codec-set 1				Page	2 of	2
IP MEDIA PARAMETERS						
Allow Direct-IP Multimedia? y						
Maximum Call Rate for Direct-IP Multimedia : 15360:Kbits						
Maximum Call Rate for Priority Direct-IP Multimedia : 15360:Kbits						
	Mode	Redun- dancy	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		
Media Connection IP Address Type Preferences						
1: IPv4						
2:						

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

This IP codec set will be used for IPFR-EF calls. Repeat the steps in **Section 5.7.1** with the following changes:

- Provision the codecs in the order shown below.
- 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** for limitations.

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.711MU	n	3	30

Media Encryption

1: 1-srtp-aescm128-hmac80

2: none

Encrypted SRTCP: enforce-unenc-srtcp

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

5.8. SIP Trunks

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

- Inbound/outbound AT&T access – SIP Trunk 5. This trunk will use TLS port 5065.
- Internal CPE access (e.g., Avaya SIP telephones, Messaging, etc.) – SIP Trunk 3. This trunk will use TLS port 5061.

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

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

5.8.1. SIP Trunk for Inbound/Outbound AT&T calls

This section describes the steps for administering the SIP trunk to Session Manager used for IPFR-EF calls. Trunk Group 5 is defined. This trunk corresponds to the **CM-TG5** SIP Entity defined in **Section 6.5.2**.

5.8.1.1 Signaling Group 5

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 system will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.4** (e.g., **SM**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5065**.
- **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.
- **Initial IP-IP Direct Media** is set to **n**.

- **H.323 Station Outgoing Direct Media** is set to **n**.
- Use the default parameters on **page 2** of the form (not shown).

add signaling-group 5		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	
Peer Detection Enabled? y	Peer Server: SM	Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5065	Far-end Listen Port: 5065	
	Far-end Network Region: 4	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

5.8.1.2 Trunk Group 5

Step 1 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **5**). 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 IPFR**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., ***05**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **Section 5.8.1.1** (e.g., **5**).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **10**).

add trunk-group 5		Page 1 of 21
TRUNK GROUP		
Group Number: 5	Group Type: sip	CDR Reports: y
Group Name: ATT IPFR	COR: 5	TN: 1
Direction: two-way	Outgoing Display? n	TAC: *05
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 5	
	Number of Members: 10	

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

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

add trunk-group 5	Page 2 of 21
Group Type: sip	
TRUNK PARAMETERS	
Unicode Name: auto	
Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 900	
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**.

add trunk-group 5	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
Maintenance Tests? y	
Numbering Format: public	
UUI Treatment: service-provider	
Replace Restricted Numbers? y	
Replace Unavailable Numbers? y	
Hold/Unhold Notifications? y	
Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y	

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

- Verify **Network Call Redirection** is set to **y**.
- Set **Send Diversion Header** to **y**. This is required for Communication Manager station Call Forward scenarios to IPFR-EF service.
- Set **Telephone Event Payload Type** to the RTP payload type recommended by the IPFR-EF service (e.g., **100**).
- Set **Identity for Calling Party Display** to **From**. Note that the display issue described in **Section 2.2, Item 1** may be resolved by setting the **Identity for Calling Party Display** parameter to **From**.

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

```
add trunk-group 5                                     Page 4 of 21
                                                    PROTOCOL VARIATIONS

                                                    Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                                                    Send Transferring Party Information? n
                                                    Network Call Redirection? y
Build Refer-To URI of REFER From Contact For NCR? n
                                                    Send Diversion Header? y
                                                    Support Request History? y
                                                    Telephone Event Payload Type: 100
                                                    Shuffling with SDP? n

                                                    Convert 180 to 183 for Early Media? n
                                                    Always Use re-INVITE for Display Updates? n
Resend Display UPDATE Once on Receipt of 481 Response? n
                                                    Identity for Calling Party Display: From
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 Telephone, Messaging Access, etc.)

Trunk Group 3 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 5.8.1.2**), is used to convert Communication Manager local extensions to IPFR-EF DNIS numbers, for inclusion in any SIP headers directed to the IPFR-EF service via the public trunk.

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

Step 2 - Add each Communication Manager station extension and their corresponding IPFR-EF DNIS numbers (for the public trunk to AT&T). Communication Manager will insert these AT&T DNIS numbers in E.164 format into the From, Contact, and PAI headers as appropriate. In the reference configuration, a range of extensions were added as follows:

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the first two digits for Communication Manager extensions (e.g., **54** for extension range 54xxx, and **59** for extension range 59xxx).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **5**).
- **Private Prefix** – Enter the corresponding IPFR-EF DNIS number prefix (e.g., **146955** and **130355**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **11**).

change public-unknown-numbering 5 ext-digits 5					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	14	5	17325552754	11	Total Administered: 46
5	50	4	173255	11	Maximum Entries: 240
5	54	5	146955	11	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
5	59	5	130355	11	
5	10001	2	18665553221	11	
					Communication Manager automatically inserts a '+' digit in this case.

5.10. Private Numbering

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

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

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the Communication Manager extension patterns defined in the Dial Plan in **Section 5.3** (e.g., **54** and **59**).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **3**).
- **Total Len** - Enter the total number of digits after the digit conversion (e.g., **5**).

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	10	3		5	Total Administered: 6
5	11	3		5	Maximum Entries: 540
5	12	3		5	
5	54	3		5	
5	59	3		5	

5.11. Route Patterns

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

5.11.1. Route Pattern for National Calls to AT&T

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

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

- In the **Grp No** column, enter **5** for public trunk 5, and the **FRL** column enter **0** (zero).
- In the **Pfx Mrk** column, enter **1** to ensure 1 + 10 digits are sent to the service provider for FNPA calls.
- In the **Inserted Digits** column, enter **p** to have Communication Manager insert a plus sign (+) in front of the number dialed to convert it to an E.164 formatted number.

change route-pattern 1												Page 1 of 3		
Pattern Number: 1												Pattern Name: To PSTN SIP Trk		
SCCAN? n				Secure SIP? n				Used for SIP stations? n						
Grp		FRL	NPA	Pfx	Hop	Toll	No.	Inserted		DCS/ IXC				
No				Mrk	Lmt	List	Del	Digits		QSIG				
										Intw				
1: 5		0		1				p		n user				
2:										n user				
3:										n user				
BCC		VALUE		TSC	CA-TSC		ITC		BCIE	Service/Feature	PARM	Sub	Numbering	LAR
0 1 2 M 4 W				Request								Dgts	Format	
1: y y y y y n				n				rest						none

5.11.3. Route Pattern for Service Calls to AT&T

Repeat the steps in **Section 5.11.1** to add a route pattern for x11 and IPFR-EF Call Forward feature access codes calls that do not require a leading plus sign, with the following changes:

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

- In the **Grp No** column, enter **5** for public trunk 5, and the **FRL** column enter **0** (zero).
- In the **Pfx Mrk** column, leave blank (default).
- In the **Inserted Digits** column, leave blank (default).

change route-pattern 4														Page 1 of 3			
Pattern Number: 4														Pattern Name: Service Numbers			
SCCAN? n														Secure SIP? n		Used for SIP stations? n	
Grp FRL NPA Pfx Hop Toll No. Inserted														DCS/ IXC			
No Mrk Lmt List Del Digits														QSIG			
														Intw			
1: 5 0														n user			
2:														n user			
3:														n user			
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM Sub Numbering LAR																	
0 1 2 M 4 W Request Dgts Format																	
1: y y y y y n n rest														none			

5.11.4. Route Pattern for Calls within the CPE

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

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

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

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

5.12. Automatic Route Selection (ARS) Dialing

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

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

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

Step 2 - Repeat **Step 1** for all other outbound call strings. In addition, IPFR-EF Call Forward feature access codes ***7** and ***9** are defined here as well.

change ars analysis 1720						Page 1 of 2	
ARS DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 1	
Dialed String	Total		Route	Call	Node	ANI	
	Min	Max	Pattern	Type	Num	Reqd	
1720	11	11	1	fnpa		n	
18	11	11	1	fnpa		n	
19	11	11	1	fnpa		n	
1900	11	11	deny	fnpa		n	
1900555	11	11	deny	fnpa		n	
1xxx976	11	11	deny	fnpa		n	
*7	3	16	4	svcl		n	
*9	3	16	4	svcl		n	
311	3	3	4	svcl		n	
011	10	18	2	intl		n	
411	3	3	4	svcl		n	

5.13. Automatic Alternate Routing (AAR) Dialing

AAR is used for outbound calls within the CPE.

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

- **Dialed String** - In the reference configuration all SIP telephones used extensions in the range 54xxx, therefore enter **54**.
- **Min & Max** – Enter **5**
- **Route Pattern** – Enter **3**
- **Call Type** – Enter **lev0**

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

change aar analysis 0							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all						Percent Full: 1		
	Dialed	Total		Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
54		5	5	3	lev0		n	

5.14. Avaya G430 Media Gateway Provisioning

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

Note – Only the Media Gateway provisioning associated with the G430 registration to Communication Manager is shown below. For 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 5.4**).

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

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

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

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

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

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

```
display media-gateway 1                                     Page 1 of 2
                                     MEDIA GATEWAY 1
                                     Type: g430
                                     Name: G430-1
                                     Serial No: 11IS31439520
Link Encryption Type: any-ptls/tls      Enable CF? n
Mutual Authentication: optional
Network Region: 1                      Location: 1
Use for IP Sync? n                    Site Data:
Recovery Rule: none
Registered: y
FW Version/HW Vintage: 42 .8 .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 80                                     Page 1 of 2
                                     SIGNALING GROUP

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

Peer Detection Enabled? n    Peer Server: AMS

Near-end Node Name: procr                Far-end Node Name: 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**.

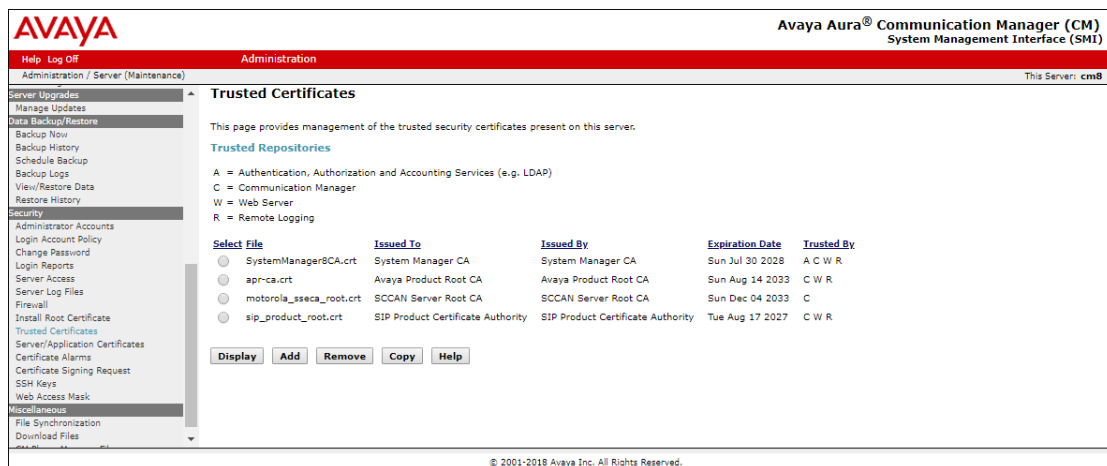
5.17. Verify TLS Certificates – Communication Manager

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.

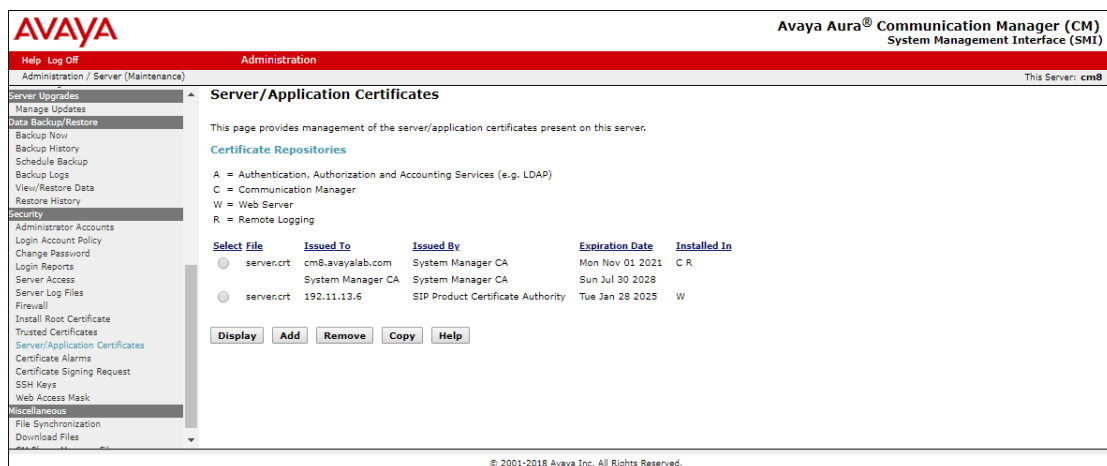
In the reference configuration, TLS transport is used for the communication between Session Manager and Communication Manager. Follow the steps below to verify the certificates used by Communication Manager.

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

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



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



6. Configure Avaya Aura® Session Manager

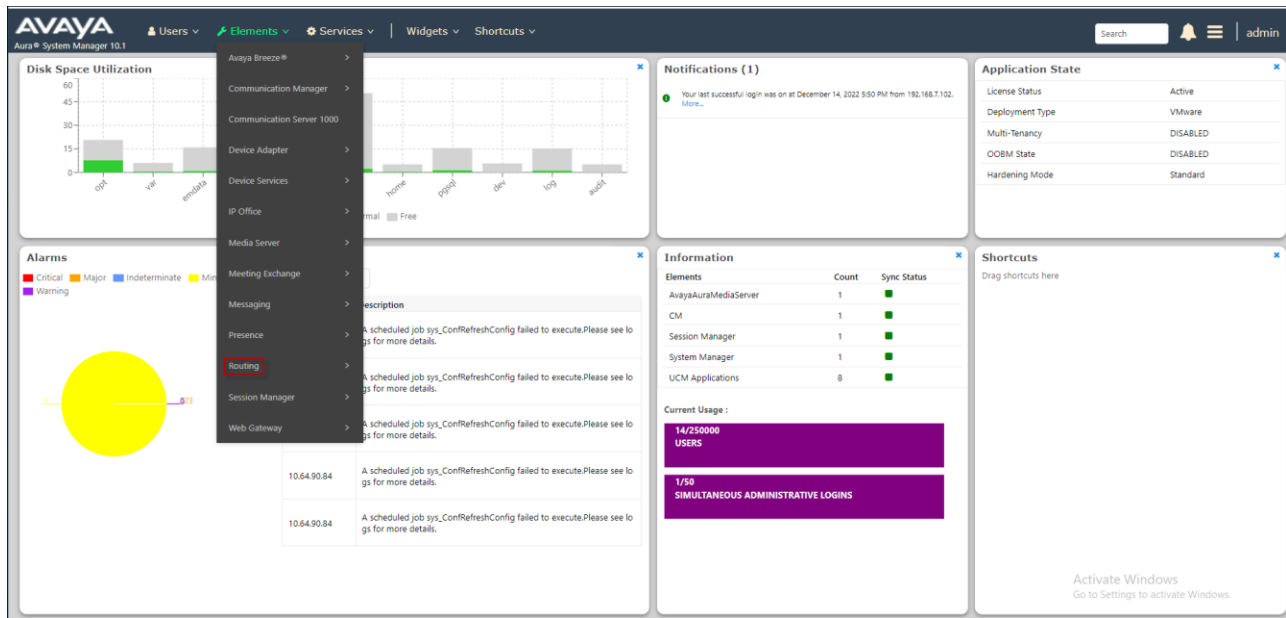
Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult [1] - [4] in the References section for further details.

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

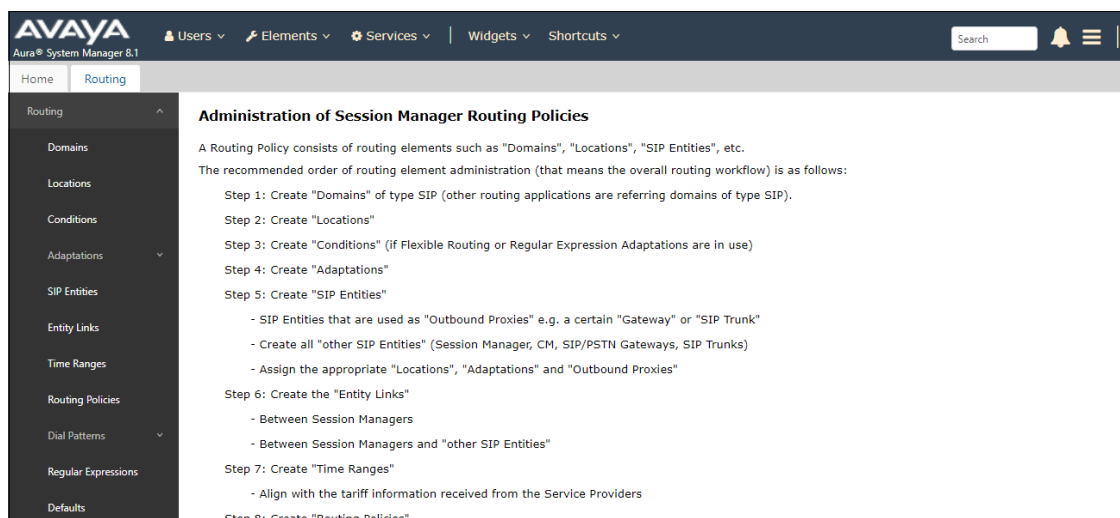
- Define a SIP Domain.
- Define a Location for Customer Premises Equipment (CPE).
- Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager and the Avaya SBCE.
- Define SIP Entities corresponding to Session Manager, Communication Manager, the Avaya SBCE, Messaging and Experience Portal.
- Define Entity Links describing the SIP trunks between Session Manager, Communication Manager, Messaging and Experience Portal, as well as the SIP trunks between 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** (not shown). 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.

The screenshot shows the 'Domain Management' interface. On the left is a navigation menu with 'Routing' expanded, showing 'Domains', 'Locations', 'Adaptations', 'SIP Entities', and 'Entity Links'. The main panel is titled 'Domain Management' and contains a toolbar with 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below the toolbar, it says '1 Item' with a refresh icon. A table displays the domain information:

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

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

6.3. Locations

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

- **Main** – The customer site containing System Manager, Session Manager, Experience Portal, Messaging and local SIP endpoints.
- **CM-TG-5** – Communication Manager trunk group 5 designated for AT&T.
- **Common SBCs** – Avaya SBCE

6.3.1. Main Location

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

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

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

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The left-hand navigation pane is expanded to show the 'Locations' menu item. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' section contains the following fields: 'Name' (set to 'Main'), 'Notes' (set to 'Avaya SIL'), 'Dial Plan Transparency in Survivable Mode' (Enabled checkbox is unchecked), 'Listed Directory Number' (empty), and 'Associated CM SIP Entity' (empty). The 'Overall Managed Bandwidth' section includes 'Managed Bandwidth Units' (set to 'kbit/sec'), 'Total Bandwidth' (empty), 'Multimedia Bandwidth' (empty), and 'Audio Calls Can Take Multimedia Bandwidth' (checked). The 'Per-Call Bandwidth Parameters' section shows 'Maximum Multimedia Bandwidth (Intra-Location)' (2000 kbit/Sec), 'Maximum Multimedia Bandwidth (Inter-Location)' (2000 kbit/Sec), 'Minimum Multimedia Bandwidth' (64 kbit/Sec), and 'Default Audio Bandwidth' (80 kbit/Sec). The 'Alarm Threshold' section includes 'Overall Alarm Threshold' (80 %), 'Multimedia Alarm Threshold' (80 %), 'Latency before Overall Alarm Trigger' (5 Minutes), and 'Latency before Multimedia Alarm Trigger' (5 Minutes). The 'Location Pattern' section at the bottom shows a table with 0 items, a filter set to 'Enable', and a column for 'IP Address Pattern'.

6.3.2. CM-TG-5 Location

To configure the Communication Manager Trunk Group 5 Location, repeat the steps in **Section 6.3.1** with the following changes (not shown):

- **Name** – Enter a descriptive name (e.g., **CM-TG-5**).

6.3.3. Common-SBCs Location

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

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

6.4. Configure Adaptations

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

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

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 TG5 ATT IPFR**).
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' highlighted. The main content area has a title 'Adaptation Details' and a 'General' tab. Below the tab, there are several input fields: 'Adaptation Name' with the value 'CM TG5 ATT IPFR', 'Module Name' with a dropdown menu showing 'DigitConversionAdapter', 'Module Parameter Type' with a dropdown menu, 'Egress URI Parameters' with an empty text box, and 'Notes' with the value 'CM - ATT - IPFR'. At the top right of the main area are 'Commit' and 'Cancel' buttons. A 'Help ?' link is also visible in the top right corner.

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).

1. **Example 1 – destination extension range:** 30355593xx is a range of DNIS digits sent in the Request URI by the IPFR-EF service that is associated with Communication Manager extension range 59300 thru 59399.
 - Enter **30355593** in the **Matching Pattern** column.
 - Enter **10** in the **Min/Max** columns.

- Enter **5** in the **Delete Digits** column.
- Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
- Enter any desired notes.

Step 4 - Repeat **Step 3** for all additional AT&T DNIS numbers/Communication manager extensions.

Step 5 - Click on **Commit**.

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

Note – In the reference configuration, the AT&T IPFR-EF service delivered 10-digit DNIS numbers.

Digit Conversion for Outgoing Calls from SM

2 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"/>	* 30355593	* 10	* 10		* 5		destination ▼		10 digit DNIS to extension
<input type="checkbox"/>	* 46955548	* 10	* 10		* 5		destination ▼		10 digit DNIS to extension

Select : [All](#), [None](#)

6.4.2. Adaptation for the AT&T IP Flexible Reach – Enhanced Features 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:

1. A descriptive **Name**, (e.g., **SBC1-Adaptation for ATT**).
2. 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 IPFR-EF 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:

1. **Name** – Enter **eRHdrs**
2. **Value** – Enter the following Avaya headers to be removed by Session Manager. Note that each header name is separated by a comma.
 - **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.

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

General

* **Adaptation Name:** SBC1-Adaptation for ATT

* **Module Name:** AttAdapter

Module Parameter Type: Name-Value Parameter

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

Select : All, None

Egress URI Parameters:

Notes: SBC - ATT IPTF

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

Filter: Enable

Digit Conversion for Outgoing Calls from SM

Add Remove

0 Items

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

Filter: Enable

6.5. SIP Entities

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

- Session Manager (**Section 6.5.1**).
- Communication Manager for AT&T trunk access (**Section 6.5.2**) – This entity, and its associated Entity Link (using TLS with port 5065), is for calls to/from AT&T and Communication Manager via the Avaya SBCE.
- Communication Manager for local trunk access (**Section 6.5.3**) – This entity, and its associated Entity Link (using TLS with port 5061), is primarily for traffic between Avaya SIP telephones and Communication Manager, as well as calls to Messaging.
- Avaya SBCE (**Section 6.5.4**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from the IPFR-EF service via the Avaya SBCE.
- Messaging (**Section 6.5.5**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from Messaging.
- Experience Portal (**Section 6.5.6**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from Experience Portal.

Note – In the reference configuration, TLS is used as the transport protocol between Session Manager and Communication Manager (ports 5061 and 5065), and to the Avaya SBCE (port 5061). The connection between the Avaya SBCE and the AT&T IPFR-EF 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., **SessionManager**).
- **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 **Listen Port** section of the **SIP Entity Details** page. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.6**. Click on **Add** and provision entries as follows:

- **Port** – Enter **5061**
- **Protocol** – Select **TLS**
- **Default Domain** – Select a SIP domain administered in **Section 6.2** (e.g., **avayalab.com**)
- **Endpoint** – Check the checkbox to have this port be used for SIP endpoint registration.

Step 5 - Enter any notes as desired and leave all other fields on the page blank/default.

Step 6 - Click on **Commit**.

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

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

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-TG5**).
- **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Section 5.5** (e.g., **10.64.91.75**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **CM TG5 ATT IPFR** administered in **Section 6.4.1**.
- **Location** – Select Location **CM-TG-5** administered in **Section 6.3.2**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Link Monitoring** section of the **SIP Entity Details** page select:
 - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field and use the default values for the remaining parameters.

Step 3 - Click on **Commit**.

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-TG5
- FQDN or IP Address:** 10.64.91.75
- Type:** CM
- Notes:** Trunk Group 5 - ATT IPFR
- Adaptation:** CM TG5 ATT IPFR
- Location:** CM-TG-5
- Time Zone:** America/Denver
- * SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:**
- 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-ATT**).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.64.91.40**, see **Section 0**).
- **Type** – Select **SIP Trunk**.
- **Adaptations** – Select Adaptation **SBC1-Adaptation for ATT** (**Section 6.4.2**).
- **Location** – Select Location **Common-SBCs** administered in **Section 6.3.3**.

6.5.5. Avaya Messaging SIP Entity

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

- **Name** – Enter a descriptive name (e.g., **Avaya Messaging**).
- **FQDN or IP Address** – Enter the IP address of Messaging (e.g., **10.64.91.145**, see **Section 3.1**).
- **Type** – Select **Other**.
- **Adaptations** – Leave this field blank.
- **Location** – Select Location **Main** administered in **Section 6.3.1**.

6.5.6. Avaya Experience Portal SIP Entity

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

- **Name** – Enter a descriptive name (e.g., **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 Messaging (**Section 6.6.4**).
- Session Manager to Experience Portal (**Section 6.6.5**).

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

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

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

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

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

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **SM to CM TG5**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 6.5.1** for Session Manager (e.g., **SessionManager**).
- **Protocol** – Select **TLS** (see **Section 5.8.1**).
- **SIP Entity 1 Port** – Enter **5065**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.2** for the Communication Manager public entity (e.g., **CM-TG5**).
- **SIP Entity 2 Port** – Enter **5065** (see **Section 5.8.1**).
- **Connection Policy** – Select **trusted**.
- Leave other fields as default.

Step 3 - Click on **Commit**.

The screenshot displays the 'Entity Links' configuration page. On the left, a navigation menu under 'Routing' includes 'Domains', 'Locations', 'Conditions', 'Adaptations', 'SIP Entities', 'Entity Links' (highlighted), and 'Time Ranges'. The main content area is titled 'Entity Links' and contains a table with one item. The table columns are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The single entry shows 'SM to CM TG5' as the Name, 'Session Manager' as SIP Entity 1, 'TLS' as the Protocol, '5065' as the Port, 'CM-TG5' as SIP Entity 2, '5065' as the Port, an unchecked 'DNS Override' box, 'trusted' as the Connection Policy, an unchecked 'Deny New Service' box, and an empty 'Notes' field. 'Commit' and 'Cancel' buttons are located at the top right and bottom right of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
* SM to CM TG5	* Session Manager	TLS	* 5065	* CM-TG5	* 5065	<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 Flexible Reach – Enhanced Features 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**).
- **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-ATT**).
- **SIP Entity 2 Port** – Enter **5061**.

6.6.4. Entity Link to Avaya Messaging

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

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

6.6.5. Entity Link to Avaya Experience Portal

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

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

The screenshot shows the 'Time Ranges' configuration page. The left sidebar has 'Routing' expanded, and 'Time Ranges' is selected. The main area is titled 'Time Ranges' and contains a table with one item named '24/7'.

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	Time Range 24/7

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 Avaya Messaging (**Section 6.8.2**).
- Inbound calls to Experience Portal (**Section 6.8.3**).
- Outbound calls to AT&T/PSTN (**Section 6.8.4**).

6.8.1. Routing Policy for AT&T Inbound Calls to Communication Manager

This Routing Policy is used for inbound calls from AT&T.

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-TG5**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

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

The screenshot shows the 'Routing Policy Details' page. The left sidebar has 'Routing' expanded, and 'Routing Policies' is selected. The main area is titled 'Routing Policy Details' and contains a 'General' section and a 'SIP Entity as Destination' section.

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM-TG5	10.64.91.75	CM	Trunk Group 5 - ATT IPFR

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-TG5**), 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 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 6.7.7**, and click on **Select**.

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

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

Step 9 - Click on **Commit**.

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

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

Routing Policy Details
Commit
Cancel

General

Name: To CM-TG5
Disabled:
Retries: 0
Notes: Trunk Group 5 PSTN to CM

SIP Entity as Destination
Select

Name	FQDN or IP Address	Type	Notes
CM-TG5	10.64.91.75	CM	Trunk Group 5 - ATT IPFR

Time of Day
Add
Remove
View Gaps/Overlaps

1 Item

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 Routing to Avaya Messaging

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

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

6.8.3. Routing Policy for Inbound Calls to Experience Portal

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

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

6.8.4. Routing Policy for Outbound Calls to AT&T

This Routing Policy is used for Outbound calls to AT&T. Repeat the steps in **Section 6.8.1** with the following differences:

- Enter a descriptive **Name** for routing calls to the AT&T IPFR-EF service via the Avaya SBCE (e.g., **To SBCE-ATT**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 6.5.4** for the Avaya SBCE SIP Entity (e.g., **SBCE-ATT**).

6.9. Dial Patterns

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

- Inbound PSTN calls via the IPFR-EF service to Communication Manager (**Section 6.9.1**).
- Outbound calls to AT&T (**Section 6.9.2**).

Note: One of the routing enhancements in Session Manager release 10.1 is the addition of Origination Dial Pattern sets functionality. This configuration is optional. Origination Dial Pattern sets can be created to include digits patterns, that can be matched by Session Manager to make more granular routing decisions, like the use of alternate routes or call restriction for calls arriving to Session Manager from different users out of the same Originating Location. This is done by matching the number present in the From header of the call. More information can be found on [2] on the References section.

Origination Dial Patterns were not used in the reference configuration.

If Origination Dial Patterns are to be used in the customer configuration, **Enable Flexible Routing** needs to be checked under **Elements → Session Manager → Global Settings**.

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

Precedence Order	Dial Patterns
1	Destination
2	Location
3	Origination

6.9.1. Matching Inbound PSTN Calls to Avaya Aura® Communication Manager

In the reference configuration inbound calls from the IPFR-EF service sent 10 DNIS digits in the SIP Request URI (for security purposes, these digits are represented in this document as 303555xxxx). The DNIS pattern must be matched for further call processing. Depending on customer deployments, the IPFR-EF service may send different DNIS digit lengths.

Note – Be sure to match on the DNIS digits specified in the AT&T Request URI, not the DID dialed digits. 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** – Enter **303555**. Note – The Adaptation defined for Communication Manager in **Section 6.4.1** will convert the various 303-555-xxxx numbers into their corresponding Communication Manager extensions.
- **Min and Max** – Enter **10**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.

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

General

* Pattern: 303555

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: AT&T DIDs

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-TG5	0	<input type="checkbox"/>	CM-TG5	Trunk Group 5 PSTN to CM

Select : All, None

Denied Originating Locations and Origination Dial Pattern Sets

Add Remove

0 Items

Originating Location	Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes
----------------------	-------	-----------------------------------	------------------------------------

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

Step 4 – In the **Originating Location**, check the checkbox corresponding to the Avaya SBCE location, 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-TG5**), and click on **Select**.

Originating Location

SelectCancel

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"/>	Main	Avaya SIL
<input type="checkbox"/>	RemoteAccess	Remote Access from SBCE1

Select : All, None

Origination Dial Pattern Sets

1 Item

Filter: Enable

Name	Notes
------	-------

Routing Policies

14 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 checked="" 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	
<input type="checkbox"/>	To IP500	<input type="checkbox"/>	IP500	

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.

HG:Reviewed
SPOC 3/23/2023

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

64 of 133
AuSBC101EP81-FR

6.9.2. Matching Outbound Calls to AT&T

In this section, Dial Patterns are administered for all outbound calls to AT&T. In the reference configuration 1xxxxyyxxxx, x11, and 011 international calls were verified. In addition, IPFR-EF Call Forward feature access codes *7 and *9 (e.g., *71yyyzzzxxxx & *91yyyzzzxxxx) are specified.

Step 1 - Repeat the steps shown in **Section 6.9.1**, with the following changes:

- In the **General** section of the **Dial Pattern Details** page, enter a dial pattern for routing calls to AT&T/PSTN (e.g., +). This will match any outbound call prefixed with a plus sign (+), such as an E.164 formatted number.
- Enter a **Min** pattern of **10**.
- Enter a **Max** pattern of **36**.
- In the **Routing Policies** section of the **Originating Locations, Origination Dial Patterns and Routing Policies** page, check the checkbox for the Originating Location corresponding to the Communication Manager Trunk Group 5 (e.g., **CM-TG-5**) and the Routing Policy administered for routing calls to AT&T in **Section 6.8.4** (e.g., **To SBCE-ATT**).

Dial Pattern Details

CommitCancel

Help ?

General

* Pattern: +

* Min: 10

* Max: 36

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: E.164 Public Numbers

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

AddRemove

8 Items

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	CM-TG-5	CM-TG-5			To SBCE-ATT	0	<input type="checkbox"/>	SBCE-ATT	

Step 2 - Repeat **Step 1** to add patterns for IPFR-EF Call Forward access codes with patterns *7 and *9, and Min=2/Max=36.

Step 3 - Repeat **Step 1** to add any additional outbound patterns as required.

Dial Patterns

NewEditDeleteDuplicateMore Actions

43 Items

Filter: Enable

<input type="checkbox"/>	Pattern	Min	▲	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	0	1		36	<input type="checkbox"/>			avayalab.com	0+ NANPA
<input type="checkbox"/>	*7	2		36	<input type="checkbox"/>			-ALL-	ATT -IPflex feature code
<input type="checkbox"/>	*9	2		36	<input type="checkbox"/>			-ALL-	ATT -IPflex feature code
<input type="checkbox"/>	x11	3		3	<input type="checkbox"/>			avayalab.com	Outbound Services
<input type="checkbox"/>	911	3		3	<input checked="" type="checkbox"/>	All Emergency	1	-ALL-	
<input type="checkbox"/>	9999	4		36	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	1411	4		4	<input type="checkbox"/>			avayalab.com	Outbound PSTN Information
<input type="checkbox"/>	15555	5		5	<input checked="" type="checkbox"/>	test EMERG	1	-ALL-	Test emergency outbound
<input type="checkbox"/>	12xxx	5		5	<input type="checkbox"/>			-ALL-	Enterprise Extensions
<input type="checkbox"/>	11000	5		5	<input type="checkbox"/>			-ALL-	Messaging Pilot number
<input type="checkbox"/>	7	5		5	<input type="checkbox"/>			-ALL-	CM VDNs
<input type="checkbox"/>	89	5		5	<input type="checkbox"/>			-ALL-	Enterprise Extensions
<input type="checkbox"/>	50	5		5	<input type="checkbox"/>			-ALL-	Enterprise Extensions
<input type="checkbox"/>	14xxx	5		5	<input type="checkbox"/>			-ALL-	Enterprise Extensions
<input type="checkbox"/>	5551212	7		7	<input type="checkbox"/>			avayalab.com	Outbound Directory Service

Select : All, None

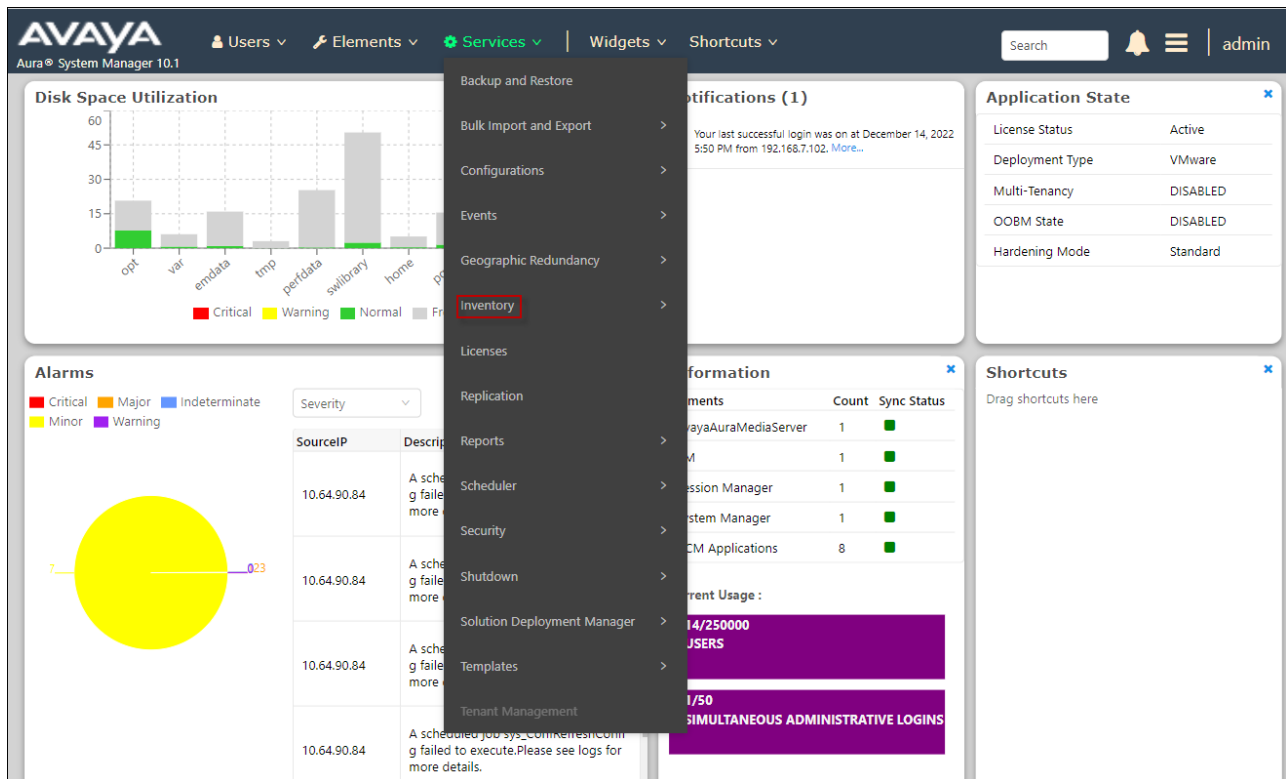
Page 1 of 3

6.10. Verify TLS Certificates – Session Manager

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

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

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



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

The screenshot displays the Avaya Session Manager web interface. On the left, the 'Inventory' menu is expanded, and 'Manage Elements' is selected. The main content area is titled 'Manage Elements' and contains a table of system elements. The 'Session Manager' element is selected, and the 'More Actions' dropdown menu is open, showing 'Manage Trusted Certificates' as the first option.

Name	Node	Element Type	SEID	Reg. Status
ams802	10.64.91.88			
CM10	10.64.91.87			
Corporate Directory	10.64.90.84			
IPSec	10.64.90.84			
Numbering Groups	10.64.90.84	UCMApp		
Patches	10.64.90.84	UCMApp		
Secure FTP Token	10.64.90.84	UCMApp		
Session Manager	10.64.90.85	Session Manager	Session Manager	
smgr10.avayalab.com (primary)	10.64.90.84	UCMApp		
SNMP Profiles	10.64.90.84	UCMApp		
Software Deployment	10.64.90.84	UCMApp		
System Manager	10.64.90.84	System Manager		

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.

The screenshot shows a web application interface for managing certificates. On the left is a dark sidebar with navigation options: Inventory, Manage Elements (selected), Create Profiles and Disc..., Element Type Access, Subnet Configuration, Manage Serviceabilit..., Synchronization, and Connection Pooling. The main area has tabs for 'Manage Elements' and 'Discovery'. Below the tabs is a 'Manage Trusted Certificates' section with a 'Done' button. A table titled 'Manage Trusted Certificates' contains 7 items. The table has columns for 'Store Description', 'Store Type', and 'Subject Name'. The sixth row is highlighted, showing 'Used for validating TLS client identity certificates' for 'SECURITY_MODULE_SIP' with subject 'O=AVAYA, OU=MGMT, CN=System Manager CA'. At the bottom, there is a 'Select : All, None' option.

	Store Description	Store Type	Subject Name
<input type="checkbox"/>	Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	SAL_AGENT	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	POSTGRES	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	WEBSPHERE	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS server identity certificates	SYSLOG	O=AVAYA, OU=MGMT, CN=System Manager CA
<input checked="" type="checkbox"/>	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	MGMT_JBOSS	O=AVAYA, OU=MGMT, CN=System Manager CA

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

Step 5 - Verify the **securitymodule_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**.

Manage Identity Certificates

Buttons: Add, Remove, Make default, Replace, Export, Renew

6 Items Filter: Enable

Select	Expand List	Service Name	Common Name	Valid To	Expired	Service Description
<input type="radio"/>		spiritalias	spiritalias	Thu Feb 29 15:33:10 MST 2024	No	SPIRIT Service
<input type="radio"/>		mgmt	mgmt	Thu Feb 29 15:33:09 MST 2024	No	Management Services
<input type="radio"/>		securitymodule_http	securitymodule_http	Sun Mar 03 15:41:46 MST 2024	No	Security Module HTTPS Service
<input checked="" type="radio"/>		securitymodule_sip	securitymodule_sip	Sun Mar 03 15:36:25 MST 2024	No	Security Module SIP Service
<input type="radio"/>		syslog	syslog	Thu Feb 29 15:33:12 MST 2024	No	Syslog Services
<input type="radio"/>		postgres	postgres	Thu Feb 29 15:33:12 MST 2024	No	Postgres Service

Select : None

Certificate Details

Subject Details C=US, O=Avaya, CN=sm10-100.avayalab.com

Valid From Fri Mar 04 15:36:26 MST 2022 **Valid To** Sun Mar 03 15:36:25 MST 2024

Key Size 2048

Issuer Name O=AVAYA, OU=MGMT, CN=System Manager CA

Certificate Fingerprint aad3433498f28523cf62a760637211bf43ebcd21

Subject Alternative Name dNSName=sm10-100.avayalab.com, iPAddress=10.64.1

Serial Number 6F17C6AF3506437FDFBE9E1966A56BE710763F92

Basic Constraints End Entity Certificate

Key Usage Extension Digital Signature, Content Commitment, Key Encipherment

Extended Key Usage Server Authentication, Client Authentication

7. Avaya Experience Portal

These Application Notes assume that the necessary Experience Portal licenses have been installed and basic Experience Portal administration has already been performed. Consult [13] and [14] in the 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 call³.

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 IPFR-EF 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.

³ 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.

The screenshot displays the Avaya Experience Portal Manager web interface. At the top, the Avaya logo is on the left, and the user 'epadmin' is welcomed on the right, with a timestamp 'Last logged in today at 6:23:08 AM MST'. Below this is a red navigation bar with 'Avaya Experience Portal 8.1.2 (ExperiencePortal)' on the left and 'Home', 'Help', and 'Logoff' links on the right. A left-hand sidebar contains a tree menu with categories like 'User Management', 'Real-time Monitoring', 'System Maintenance', 'System Configuration', 'Security', 'Reports', and 'Multi-Media Configuration'. The main content area, titled 'Avaya Experience Portal Manager', includes a 'You are here: Home' breadcrumb, a description of the EPM application, and sections for 'Installed Components' (Media Processing Platform, Email Service, HTML Service, SMS Service) and a 'Legal Notice' section containing the 'AVAYA GLOBAL SOFTWARE LICENSE TERMS'.

Avaya Experience Portal Manager

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

Installed Components

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

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

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

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

Legal Notice

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

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

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

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

Licensing

[Refresh](#)

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

License Server Information

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

Licensed Products

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

7.3. Verify TLS Certificates – Experience Portal

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

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

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

The screenshot shows the 'Certificates' page in the Experience Portal. The left navigation pane is expanded to 'Security' > 'Certificates'. The main content area shows the 'Trusted Certificates' tab selected. Below the tabs, there is a table with columns 'Name', 'Type', and 'Certificate'. The table contains one entry: 'SMGR10 SIP Connection'. To the right of this entry, the details of the certificate are displayed, including the Owner, Issuer, Serial Number, Signature Algorithm, Version, Valid from date, Certificate Fingerprints, Key Usage, and Basic Constraints.

Name	Type	Certificate
SMGR10 SIP Connection		<p>Owner: O=AVAYA,OU=MGHT,CN=System Manager CA Issuer: O=AVAYA,OU=MGHT,CN=System Manager CA Serial Number: 6f244e9957723c84b08952fbf2bb81e946d5c0e Signature Algorithm: SHA256withRSA Version: 3 Valid from: January 28, 2022 7:31:13 AM MST until January 29, 2047 7:31:12 AM MST Certificate Fingerprints MD5: e6:4a:e8:11:1e:37:ec:29:9e:14:ea:49:65:a4:ba:10 SHA: 0f:40:23:8a:c8:d0:6e:3c:52:b0:37:c9:65:3a:ad:11:ee:3f:61:30 SHA-256: aa:2d:58:39:2d:8c:9e:1a:2b:4e:7e:d8:97:4e:51:62:d8:89:44:00:5f:e7:32:a6:53:d6:b9:5e:53:08:99:fe Key Usage: Digital Signature Key Cert Sign CRL Sign Basic Constraints: CA: true Path Len Constraint: 2147483647</p>

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

The screenshot shows the 'Certificates' page in the Experience Portal. The left navigation pane is expanded to 'Security' > 'Certificates'. The main content area shows the 'EP Signing Certificate' tab selected. Below the tabs, there is a table with columns 'Name', 'Type', and 'Certificate'. The table contains one entry: 'Certificate Signing Request'. To the right of this entry, the details of the certificate are displayed, including the Owner, Issuer, Serial Number, Signature Algorithm, Version, Valid from date, Certificate Fingerprints, Key Usage, and Basic Constraints.

Name	Type	Certificate
Certificate Signing Request		<p>Owner: C=US,ST=CO,L=Thornton,O=AVAYA,OU=SIL,CN=ep.avayalab.com Issuer: O=AVAYA,OU=MGHT,CN=System Manager CA Serial Number: 6668d6ac72835e5fc07ad66d9439c828dc3a190c Signature Algorithm: SHA256withRSA Version: 3 Valid from: March 11, 2022 10:18:26 AM MST until January 29, 2047 7:31:12 AM MST Certificate Fingerprints MD5: eb:f7:57:96:3b:d4:92:38:b2:5f:b2:11:b6:a4:6b:28 SHA: 67:72:94:4f:fe:b0:b0:81:99:84:21:5b:94:ac:5c:51:b2:e5:9b:cb SHA-256: 94:37:ec:0c:5c:c4:11:5f:45:f7:9e:55:84:82:6c:65:5a:69:30:ba:70:71:e5:2a:04:ac:90:57:a5:7a:ba:67 Key Usage: Digital Signature Key Cert Sign CRL Sign Basic Constraints: CA: true Path Len Constraint: 2147483647 Subject Alternative Name IP Address: 10.64.91.90</p>

7.4. VoIP Connection

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

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

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

Expand All | Collapse All

User Management
Roles
Users
Login Options

Real-time Monitoring
System Monitor
Active Calls
Port Distribution

System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

System Management
EPM Manager
MPP Manager
Software Upgrade
System Backup

System Configuration
Applications
EPM Servers
MPP Servers
SNMP

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

VoIP Connections

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

H.323 SIP

<input type="checkbox"/>	Name	Enable	Proxy Transport	Proxy/DNS Server Address	Proxy Server Port	Listener Port	SIP Domain	Maximum Simultaneous Calls
<input type="checkbox"/>	SM10	Yes	TLS	10.64.91.xx	5061	5061	avayalab.com	10

Add **Delete** **Help**

Step 2 - Configure a SIP connection as follows:

- **Name** – Set to a descriptive name (e.g., **SM10**).
- **Enable** – Set to **Yes**.
- **Proxy Server Transport** – Set to **TLS**.
- Select **Proxy Servers**, and enter:
 - **Proxy Server Address** = **10.64.91.xx** (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 **INVITE with REPLACES**.
- **SIP Reject Response Code** – Select **ASM (503)**.
- **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In the reference configuration a value of **10** was used.
- Select **All Calls can be either inbound or outbound**.
- **SRTP Enable** = **Yes**
- **Encryption Algorithm** = **AES_CM_128**
- **Authentication Algorithm** = **HMAC_SHA1_80**
- **RTCP Encryption Enabled** = **No**
- **RTP Authentication Enabled** = **Yes**
- Use default values for all other fields.

- Click **Save**.

Expand All | Collapse All

▼ User Management

Roles

Users

Login Options

▼ Real-time Monitoring

System Monitor

Active Calls

Port Distribution

▼ System Maintenance

Audit Log Viewer

Trace Viewer

Log Viewer

Alarm Manager

▼ System Management

EPM Manager

MPP Manager

Software Upgrade

System Backup

▼ System Configuration

Applications

EPM Servers

MPP Servers

SNMP

Speech Servers

VoIP Connections

Zones

▼ Security

Certificates

Licensing

▼ Reports

Standard

Custom

Scheduled

▼ Multi-Media Configuration

Email

HTML

SMS

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

Change SIP Connection

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

Name: SM10

Enable: ☒ Yes ☐ No

Proxy Transport: TLS ▼

☒ Proxy Servers ☐ DNS SRV Domain

Address	Port	Priority	Weight	
10.64.91.81	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

Configured SRTP List

<No SRTP List>

7.5. 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

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

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

Speech Servers

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

ASR

TTS

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

Add

Delete

Customize

Help

7.6. Application References

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

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 dialed IPFR-EP DID number 303-555-9329 was used. Repeat to define additional called party numbers as needed. Inbound AT&T IPFR-EP calls with these called party numbers will be handled by the application defined in this section.

Expand All | Collapse All

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:

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](#)

[Remove](#)

SIP Header Source:

Speech Parameters [▶](#)

Reporting Parameters [▶](#)

Advanced Parameters [▶](#)

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

7.7. MPP Servers and VoIP Settings

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

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

The screenshot shows the 'MPP Servers' configuration page. The left pane has a navigation menu with 'System Configuration' expanded, showing 'Applications', 'EPM Servers', 'MPP Servers', 'SNMP', 'Speech Servers', 'VoIP Connections', 'Zones', 'Security', 'Reports', and 'Multi-Media Configuration'. The main content area has a breadcrumb 'You are here: Home > System Configuration > MPP Servers' and a title 'MPP Servers'. Below the title is a description: 'This page displays the list of Media Processing Platform (MPP) servers in the Experience Portal system. When an MPP receives a call from a PBX, it invokes a VoiceXML application on an application server and communicates with ASR and TTS servers as necessary to process the call.' A table lists the MPP servers:

<input type="checkbox"/>	Name	Host Address	Network Address (VoIP)	Network Address (MRCP)	Network Address (AppSvr)	Maximum Simultaneous Calls	Trace Level
<input type="checkbox"/>	mpe01	10.64.91.90	<Default>	<Default>	<Default>	11	Use MPP Settings

Below the table are 'Add' and 'Delete' buttons. At the bottom of the page are tabs for 'MPP Settings', 'Browser Settings', 'Video Settings', 'VoIP Settings', and '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

- ▶ 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](#) > Change MPP Server

Change MPP Server

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

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

MPP Certificate

```

Owner: C=US,O=Avaya Experience Portal,OU=epm,CN=ep.avayalab.com
Issuer: C=US,ST=CO,L=Thornton,O=AVAYA,OU=SIL,CN=ep.avayalab.com
Serial Number: 855d57728b031341f5ce96beeb44f9
Signature Algorithm: SHA256withRSA
Version: 3
Valid from: October 28, 2022 2:19:57 PM MDT until October 28, 2032 2:19:57 PM MDT
Certificate Fingerprints
MD5: 72:41:1c:a8:85:10:22:75:e5:80:5b:79:11:8c:9e:5c
SHA: 38:cc:29:b3:3a:bf:bb:22:c2:65:dc:d4:c4:4c:a0:ea:59:ef:b4:ff
SHA-256: c4:44:d9:c2:f7:1a:5a:25:fa:db:9d:bb:48:6d:9c:8a:56:74:7f:eb:86:a2:81:1e:c9:6f:24:de:a6:6f:b1:5b
Basic Constraints:
CA: false
Path Len Constraint: undefined
Subject Alternative Names
DNS Name: ep
DNS Name: ep.avayalab.com
IP Address: 10.64.91.90
IP Address: fe80:0:0:0:20c:29ff:fe75:a39d

```

Categories and Trace Levels ▶

Save Apply Cancel Help

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

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

Expand All | Collapse All

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

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

VoIP Settings

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

Port Ranges ▼

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

RTCP Monitor Settings ▼

Host Address:

Port:

VoIP Audio Formats ▼

MPP Native Format:

- In the Codecs section set:
 - Set **Packet Time** to **20**.
 - Verify the **G729 Codec** is enabled.
 - Set **G729 Discontinuous Transmission** to **No** (G.729A).
 - Set the **Offer Order** to the preferred codec. In the sample configuration, **G729** is the first codec, followed by **G711uLaw**, then **G711aLaw**.
- Use default values for all other fields.

Step 5 - Click on **Save**.

Expand All | Collapse All

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

Station:

RTCP Monitor Settings ▼

Host Address:

Port:

VoIP Audio Formats ▼

MPP Native Format:

Codecs ▼

Offer

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

Packet Time: milliseconds

G729 Discontinuous Transmission: ☐ Yes ☒ No

Answer

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

G729 Discontinuous Transmission: ☐ Yes ☐ No ☒ Either

G729 Reduced Complexity Encoder: ☒ Yes ☐ No

QoS Parameters ▼

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

7.8. Configuring RFC2833 Event Value Offered by Experience Portal

For incoming calls from AT&T IPFR-EP 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 displays the 'MPP Manager' interface within the Experience Portal. The left sidebar shows a navigation menu with 'System Management' expanded, highlighting 'MPP Manager'. The main content area shows the current state of MPP1 as 'Online Running'. Below the table, there are buttons for 'Start', 'Stop', 'Restart', 'Reboot', 'Halt', and 'Cancel'. The 'Restart' button is highlighted. To the right of these buttons, there are 'Restart/Reboot Options' with radio buttons for 'One server at a time' (selected) and 'All servers'. At the bottom left, there is a 'Help' button.

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

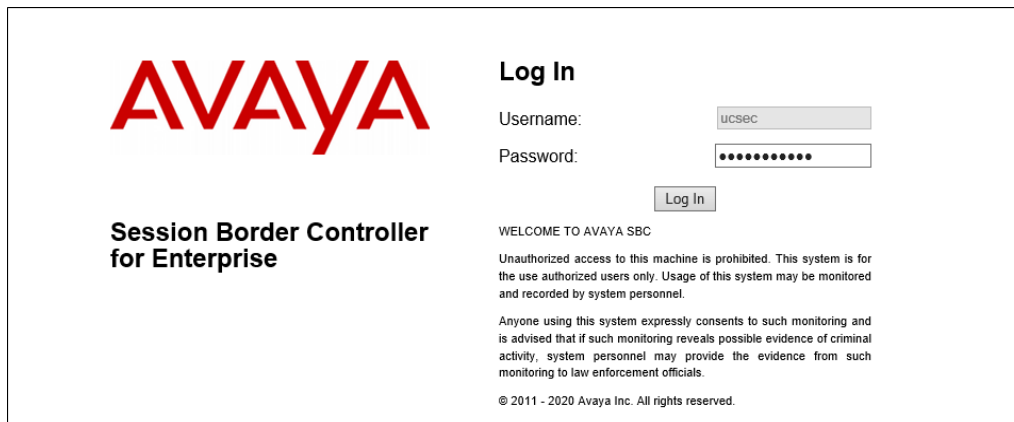
8. Configure Avaya Session Border Controller for Enterprise

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 [10] and [11] 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.



The screenshot shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, under the heading "Log In", there are input fields for "Username:" (containing "ucsec") and "Password:" (masked with dots). A "Log In" button is positioned below the password field. Below the login fields, a "WELCOME TO AVAYA SBC" message is followed by a disclaimer: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." and a consent statement: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, the copyright notice "© 2011 - 2020 Avaya Inc. All rights reserved." is visible.

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

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

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) 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", "Software Management", "Device Management" (with sub-items: System Administration, Templates, Backup/Restore, Monitoring & Logging), and "Monitoring & Logging". The main content area is titled "Dashboard" and contains two panels. The "Information" panel displays system details: System Time (09:38:08 AM EST), Version (10.1.1.0-35-21872), GUI Version (10.1.1.0-21872), Build Date (Mon Apr 18 07:57:04 UTC 2022), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), and Last Logged in at (01/30/2023 11:04:32 EST). The "Installed Devices" panel shows a list of devices, including EMS and SBCE10-70.

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 **SBCE10-70** 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 (SBCE) EMS Dashboard, specifically the "Device Management" section. The top navigation bar is the same as the previous screenshot. The left-hand menu is updated to show "Device Management" as the selected option. The main content area is titled "Device Management" and contains four tabs: "Devices", "Updates", "Licensing", and "Key Bundles". The "Devices" tab is selected, displaying a table of installed devices. The table has columns for Device Name, Management IP, Version, and Status. A single device, SBCE10-70, is listed with a Management IP of 10.64.90.70, Version 10.1.1.0-35-21872, and Status Commissioned. Below the table, there are links for 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 **B2** IP addresses are the ones relevant to the configuration of the SIP trunk to AT&T.

General Configuration		Device Configuration		Dynamic License Allocation		
Appliance Name	SBCE10-70	HA Mode	No		Min License Allocation	Max License Allocation
Box Type	SIP	Two Bypass Mode	No	Standard Sessions	10	100
Deployment Mode	Proxy			Advanced Sessions	10	100
				Scopia Video Sessions	10	100
				CES Sessions	10	100
				Transcoding Sessions	10	100
				AMR	<input checked="" type="checkbox"/>	
				Premium Sessions	10	100
				CLID	---	
				Encryption	<input checked="" type="checkbox"/>	
				Available:	Yes	

Network Configuration				
IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.91.40	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
10.64.91.42	10.64.91.42	255.255.255.0	10.64.91.1	A1
192.168.200.26	192.168.200.26	255.255.255.248	192.168.200.25	B2

DNS Configuration		Management IP(s)	
Primary DNS	10.64.19.185	IP #1 (IPv4)	10.64.90.70
Secondary DNS			
DNS Location	DMZ		
DNS Client IP	10.64.91.40		

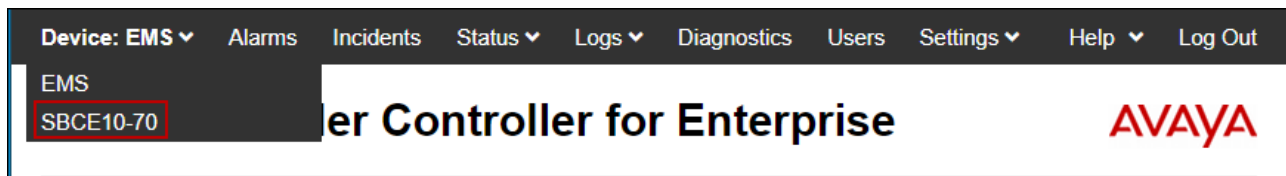
8.2. TLS Management

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.

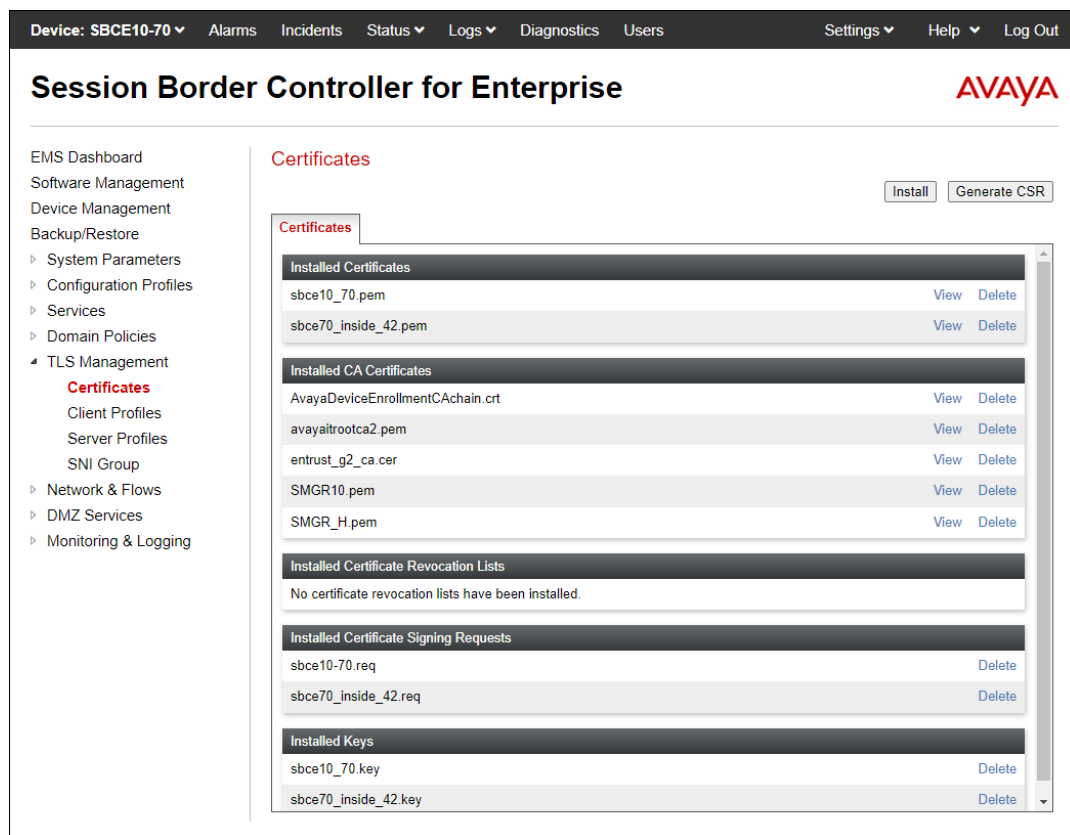
8.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

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., **Inside_Server**).
- **Certificate:** select the identity certificate, e.g., **sbce10_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 screenshot shows a dialog box titled "Edit Profile" with a close button (X) in the top right corner. At the top, there is a warning message in an orange box: "WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems. Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid." Below the warning, the dialog is divided into two main sections: "TLS Profile" and "Certificate Verification". The "TLS Profile" section contains four fields: "Profile Name" (text input with "Inside_Server"), "Certificate" (dropdown menu with "sbce10_70.pem"), "SNI Options" (dropdown menu with "None"), and "SNI Group" (dropdown menu with "None"). The "Certificate Verification" section contains three fields: "Peer Verification" (dropdown menu with "None"), "Peer Certificate Authorities" (list box containing "AvayaDeviceEnrollmentCAchain.crt", "avayaitrootca2.pem", "entrust_g2_ca.cer", and "SMGR10.pem"), and "Peer Certificate Revocation Lists" (empty list box). At the bottom of the dialog, there is a "Verification Depth" field (text input with "0") and a "Next" button.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with the following items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (expanded), Certificates, Client Profiles, **Server Profiles** (highlighted), SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled "Server Profiles: Inside_Server" and includes an "Add" button and a "Delete" button. Below the title, there is a "Server Profile" tab and a "Click here to add a description." link. The form contains the following sections:

- TLS Profile**
 - Profile Name: Inside_Server
 - Certificate: sbce10_70.pem
 - SNI Options: None
- Certificate Verification**
 - Peer Verification: None
 - Extended Hostname Verification: ☐
- Renegotiation Parameters**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**
 - Version: ☒ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0
 - Ciphers: ☒ Default ☐ FIPS ☐ Custom
 - Value: HIGH:IDH:ADH:IMD5:1aNULL:1eNULL:@STRENGTH

An "Edit" button is located 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., **Inside_Client**)
- **Certificate:** select the identity certificate, e.g., **sbce10_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., **SMGR10.pem**.
- Enter 1 under **Verification Depth**. Click **Next**.

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

Edit Profile

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

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

TLS Profile

Profile Name:

Certificate:

SNI: ☐ Enabled

Certificate Verification

Peer Verification: Required

Peer Certificate Authorities:

Peer Certificate Revocation Lists:

Verification Depth:

Extended Hostname Verification: ☐

Server Hostname:

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with categories like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (expanded), Certificates, Client Profiles (highlighted), Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled 'Client Profiles: Inside_Client' and includes an 'Add' button and a 'Delete' button. Below this is a list of client profiles: 'Inside_Client' (selected) and 'Inside_Client_42'. The 'Inside_Client' profile is expanded, showing the following configuration:

TLS Profile	
Profile Name	Inside_Client
Certificate	sbce10_70.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	SMGR10.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

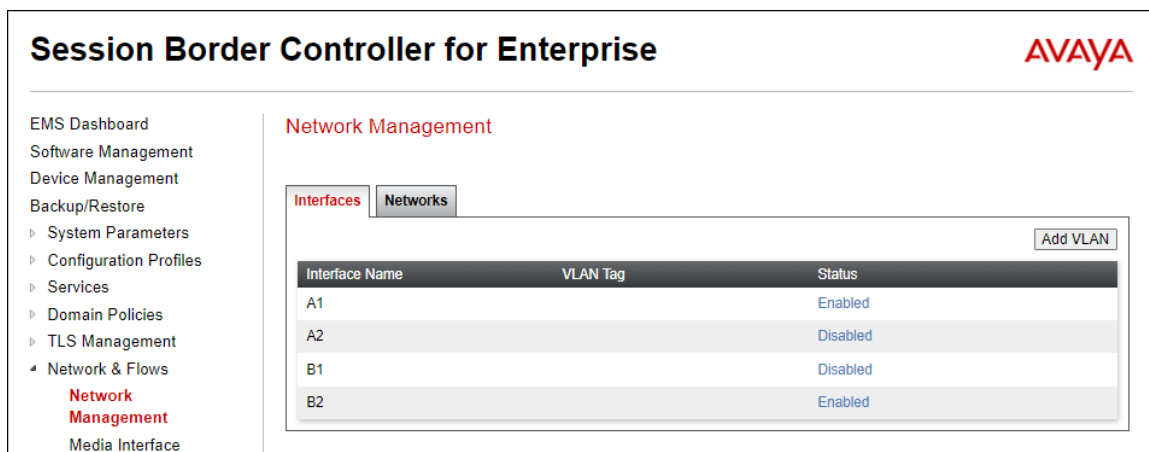
An 'Edit' button is located at the bottom right of the configuration area.

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 **B2**.

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 B2 (public) interfaces are used. To enable an interface, click the corresponding **Disabled** link under the Status column to change it to **Enabled**.



Session Border Controller for Enterprise AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▾ Network & Flows
 Network Management
 Media Interface

Network Management

Interfaces **Networks** Add VLAN

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

Step 3 - Select the **Networks** tab to display the IP provisioning for the A1 and B2 interfaces. The following Avaya SBCE IP addresses and associated interfaces were used in the sample configuration:

- **B2: 192.168.200.26** – IP address configured for the AT&T IPFR-EF service. This address is known to AT&T. See **Section 3**.
- **A1: 10.64.91.40** – IP address configured for AT&T IPFR-EF service to Session Manager.

Device: SBCE10-70 ▾
Alarms
Incidents
Status ▾
Logs ▾
Diagnostics
Users
Settings ▾
Help ▾
Log Out

Session Border Controller for Enterprise

AVAYA

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

Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows

Network Management

Interfaces

Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address		
Inside-A1	10.64.91.1	255.255.255.0	A1	10.64.91.40, 10.64.91.41, 10.64.91.42	Edit	Delete
					Edit	Delete
					Edit	Delete
					Edit	Delete
Outside-B2	192.168.200.25	255.255.255.248	B2	192.168.200.26	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 shows the 'Session Border Controller for Enterprise' web interface. The left-hand navigation menu includes 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', and 'Network & Flows'. Under 'Network & Flows', 'Advanced Options' is selected. The main content area is titled 'Advanced Options' and contains several tabs: 'Periodic Statistics', 'Feature Control', 'SIP Options', 'Network Options', 'Port Ranges' (which is active), 'RTCP Monitoring', and 'Load'. Below the tabs, a warning message states: 'Changes to the settings below require an application restart before taking effect. Application restarts can be issued from [Device Management](#).' The 'Port Range Configuration' section contains four rows of configuration fields: '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.

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. As mentioned in **Section 0**, the AT&T IPFR-EF service specifies that customers use RTP ports in the range of **16384 – 32767**. Both inside and outside ports have been changed to this range, though only the outside port range is required by the AT&T IPFR-EF service.

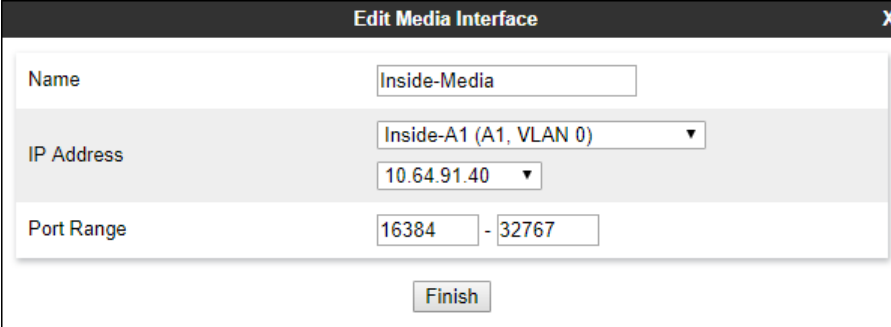
Some ports in the range required by AT&T were already allocated by the Avaya SBCE for internal use, by default. **Section 0** shows the steps required to reallocate the port ranges used by the Avaya SBCE, so the range required by AT&T could be accommodated.

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
- **IP Address:** Select **Inside-A1 (A1, VLAN0)** and **10.64.91.40**
- **Port Range:** **16384 – 32767**

Step 3 - Click **Finish**.



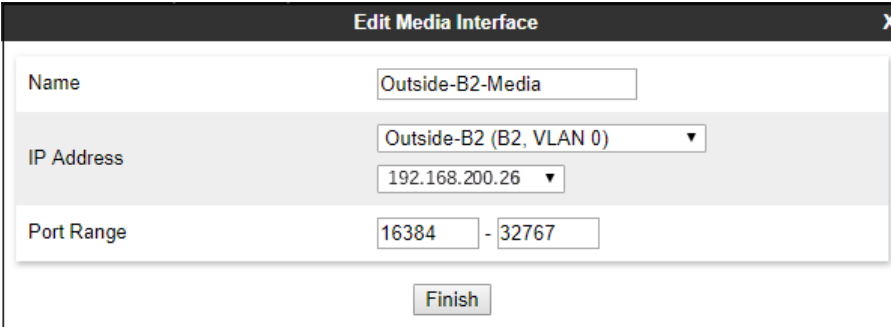
The screenshot shows the 'Edit Media Interface' window with the following configuration:

Edit Media Interface	
Name	Inside-Media
IP Address	Inside-A1 (A1, VLAN 0) 10.64.91.40
Port Range	16384 - 32767
Finish	

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

- **Name:** Outside-B2-Media
- **IP Address:** Select **Outside-B2 (B2, VLAN0)** and **192.168.200.26**
- **Port Range:** **16384 – 32767**

Step 5 - Click **Finish**.



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

Edit Media Interface	
Name	Outside-B2-Media
IP Address	Outside-B2 (B2, VLAN 0) 192.168.200.26
Port Range	16384 - 32767
Finish	

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-40
- **IP Address:** Select **Inside-A1 (A1, VLAN0)** and **10.64.91.40**
- **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 configuration:

Field	Value
Name	Inside-Sig-40
IP Address	Inside-A1 (A1, VLAN 0) / 10.64.91.40
TCP Port	Leave blank to disable
UDP Port	Leave blank to disable
TLS Port	5061
TLS Profile	sbce8_70Server
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

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

- **Name:** Outside-B2-Signaling
- **IP Address:** Select **Outside-B2 (B2, VLAN0)** and **192.168.200.26**
- **UDP Port:** 5060

Step 5 - Click **Finish**.

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

Field	Value
Name	Outside-B2-Signaling
IP Address	Outside-B2 (B2, VLAN 0) / 192.168.200.26
TCP Port	Leave blank to disable
UDP Port	5060
TLS Port	Leave blank to disable
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

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 IPFR-EF service.

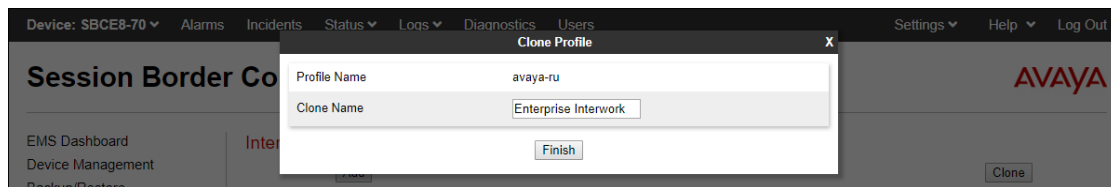
8.7.1. Server Interworking Profile – Enterprise

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.

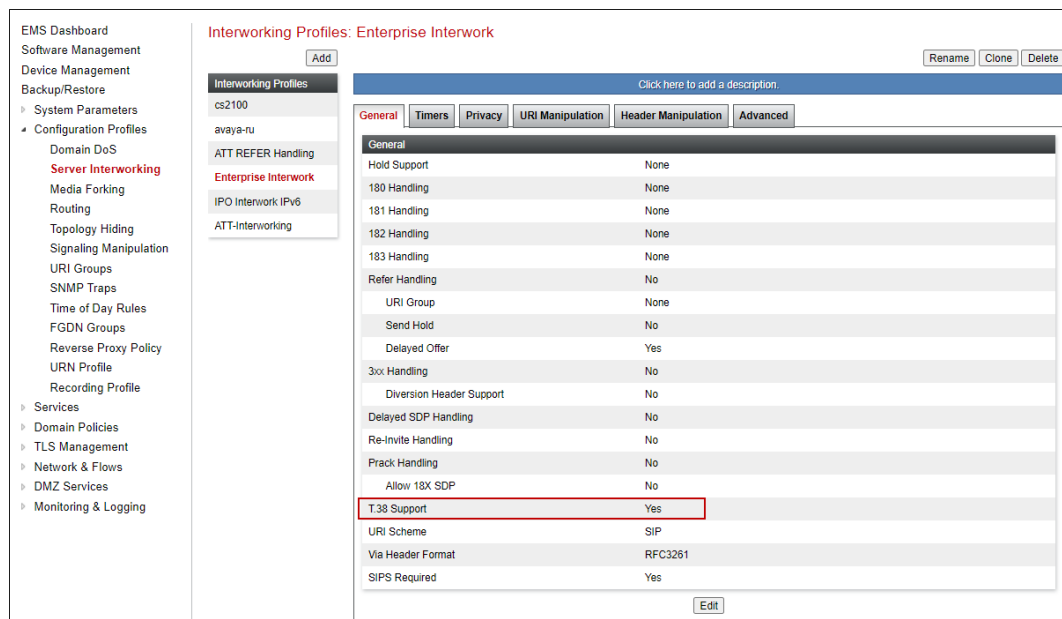
Step 3 - Enter profile name: (e.g., **Enterprise Interwork**), and click **Finish** to continue.



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.

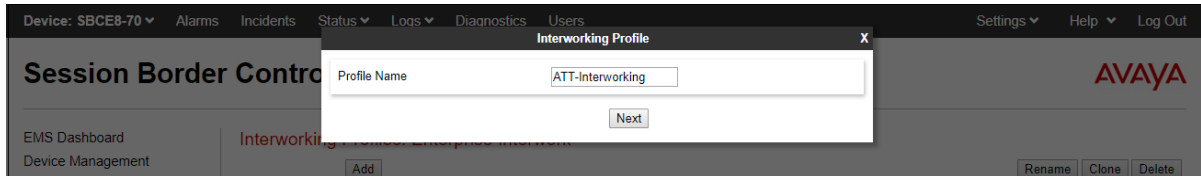
- Check **T38 Support**.
- All other options can be left with default values. Click **Finish** (not shown).



8.7.2. Server Interworking – AT&T

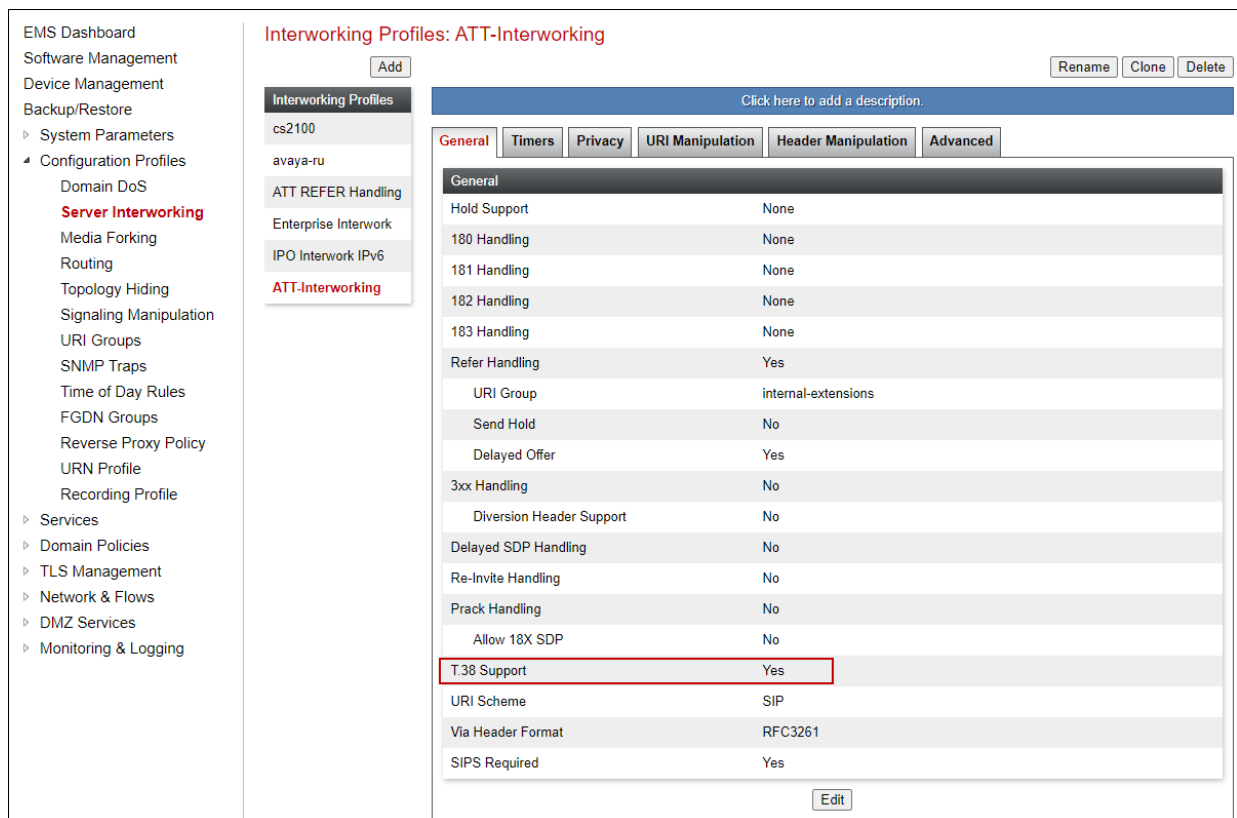
Repeat the steps shown in **Section 8.7.1** to add an Interworking Profile for the connection to AT&T via the public network, with the following changes:

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



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

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



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 screen shows the value used during the compliance testing. See **Sections 8.9.2** and **8.10.2** for multiple AT&T border elements configuration.

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 REFER Handling', 'Enterprise Interwork', 'IPO Interwork IPv6', and 'ATT-Interworking' (which is highlighted in red). Above the list are 'Add', 'Rename', 'Clone', and 'Delete' buttons. The main area has a blue header with the text 'Click here to add a description.' Below this is a tabbed interface with tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'Timers' tab is selected. It contains a section titled 'SIP Timers' with a table of settings:

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, now on the 'Advanced' tab. The sidebar and top navigation are the same as in the previous screenshot. The 'Advanced' tab is selected. It contains a table of settings:

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

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

DTMF Support	None
--------------	------

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

8.8. Signaling Manipulation

Signaling Manipulations are SigMa scripts the Avaya SBCE can use to manipulate SIP headers/messages. In the reference configuration, a 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**) does not meet the desired result. Refer to References [10] for information on the Avaya SBCE scripting language.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor.

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

- Remove the epv parameter from outbound Contact headers. See **Section 2.4**.
- Remove the Bandwidth headers sent by some Avaya SIP endpoints. See **Section 2.2**.
- Change the value of the Max-Forwards header on the SIP OPTIONS messages sent by AT&T from “0” to “30”, to be able to reach Communication Manager. See **Section 2.2**.
- Modify the P-Asserted-Identity header of outbound INVITEs from Experience Portal to the PSTN, with a DID number known to AT&T. See **Section 2.2**.

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

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

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

- Enter a name for the script in the **Title** box (e.g., **Script for IPFR-CM**).
- Copy and paste the script from **Section 14** in this document.



```
1 within session "ALL"
2 {
3   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
4   {
5     //Remove epv parameter from Contact header to hide internal topology
6     remove %HEADERS["Contact"] [1].URI_PARAMS["epv"];
7
8     //Remove Bandwidth from SDP
9     %BODY[1].regex_replace("b=(TIAS|AS|CT):(\d+)\r\n","");
10
11   }
12 }
13
14 //OPTIONAL - Change AT&T Max-Forwards value from 0 to 30
15 within session "OPTIONS"
16 {
17   act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
18   {
19     %HEADERS["Max-Forwards"] [1] = "30";
20   }
21 }
22
23 // OPTIONAL Experience Portal - modify PAI Header
24 within session "INVITE"
25 {
26   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
27   {
28     if (%INITIAL_REQUEST = "true") then
29     {
30       if (%HEADERS["User-Agent"] [1].regex_match("Avaya\\-VoicePortal")) then
31       {
32
```

Step 3 - 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

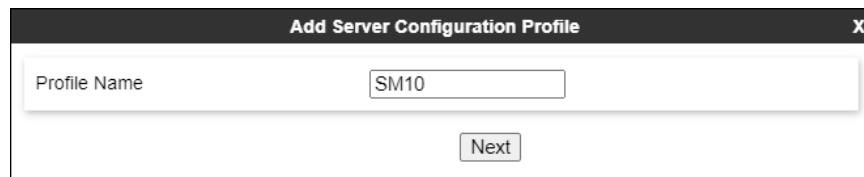
The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

8.9.1. SIP Server Profile – Session Manager

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

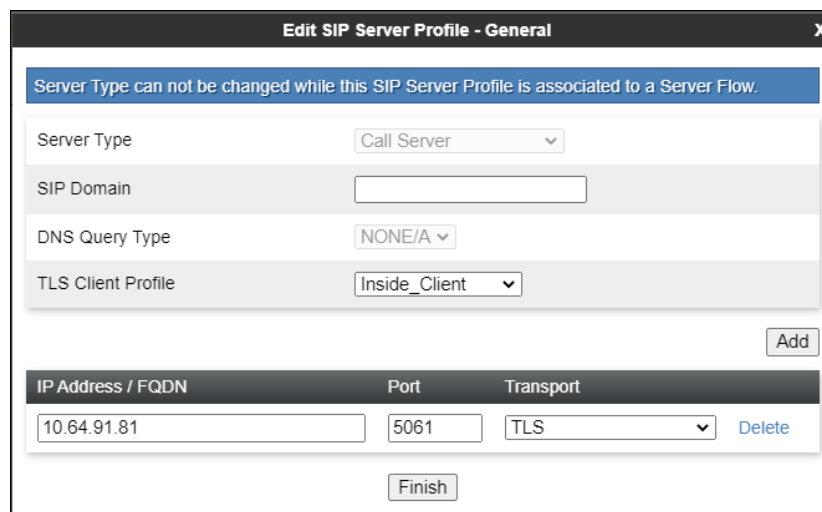
Step 1 - Select **Services** → **SIP Servers** from the left-hand menu.

Step 2 - Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **SM10**) 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., **Inside_Client**)
- **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 IPFR-EF service may provide a Primary and Secondary Border Element. This section describes the Avaya SBCE provisioning to support this redundant configuration.

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-trk-svr**) and select **Next** (not shown).

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

- **Server Type:** Select **Trunk Server**
- **IP Address/FQDN:** **192.168.38.69** (AT&T Border Element IP address)
- **Transport:** Select **UDP**
- **Port:** **5060**

Step 3 – For the additional AT&T Border Element IP addresses, click **Add** and enter the following:

- **IP Address/FQDN:** **192.168.37.149** (AT&T Border Element IP address)
- **Transport:** Select **UDP**
- **Port:** **5060**
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish** and proceed to the next tab.

IP Address / FQDN	Port	Transport	
192.168.38.69	5060	UDP	Delete
192.168.37.149	5060	UDP	Delete

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 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.

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

- Enable Heartbeat**: A checkbox that is checked.
- Method**: A drop-down menu showing 'OPTIONS'.
- Frequency**: A text input field containing '300', followed by the label 'seconds'.
- From URI**: A text input field containing 'SBCE@avaya.com'.
- To URI**: A text input field containing 'IPFR@att.com'.
- Finish**: A button at the bottom right.

Note - Avaya SBCE will issue OPTIONS messages to the primary (192.168.38.69) and secondary (192.168.37.149) border elements. If the SBCE fails to get a response to the OPTIONS sent to 192.168.38.69, the SBCE will redirect outbound calls to 192.168.37.149.

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

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

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

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

- Enable DoS Protection**: A checkbox that is unchecked.
- Enable Grooming**: A checkbox that is unchecked.
- Interworking Profile**: A drop-down menu showing 'ATT-Interworking'.
- Signaling Manipulation Script**: A drop-down menu showing 'Script for IPFR-CM'.
- Securable**: A checkbox that is unchecked.
- Enable FGDN**: A checkbox that is unchecked.
- TCP Failover Port**: A text input field.
- TLS Failover Port**: A text input field.
- Tolerant**: A checkbox that is unchecked.
- URI Group**: A drop-down menu showing 'None'.
- Finish**: A button at the bottom right.

8.10. Routing Profiles

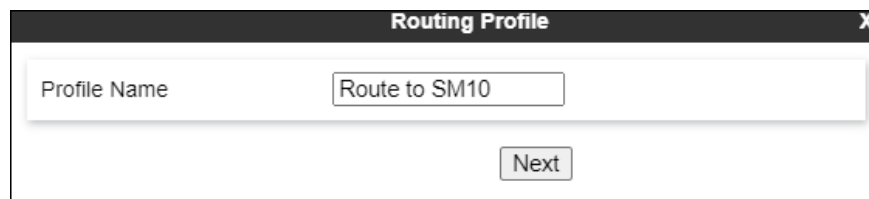
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and determine which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport 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 SM10**) and click **Next**.

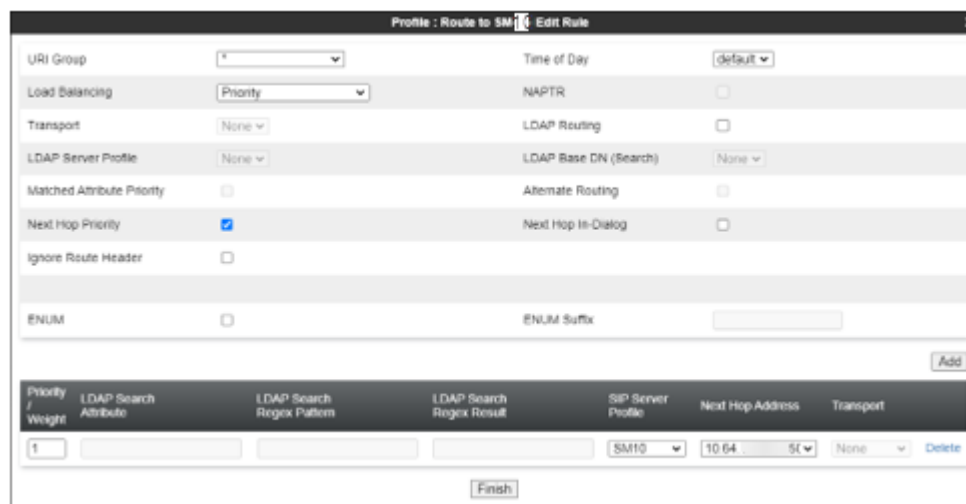


The image shows a 'Routing Profile' configuration window. It has a title bar with 'Routing Profile' and a close button 'X'. Inside, there is a 'Profile Name' label followed by a text input field containing 'Route to SM10'. Below the input field is a 'Next' button.

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** = **SM10** (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 on **Finish**.



The image shows a 'Profile : Route to SM10 Edit Rule' window. It has a title bar with 'Profile : Route to SM10 Edit Rule' and a close button 'X'. The window is divided into two main sections. The top section contains various settings: 'URI Group' (dropdown), 'Time of Day' (dropdown), 'Load Balancing' (dropdown), 'NAPTR' (checkbox), 'Transport' (dropdown), 'LDAP Routing' (checkbox), 'LDAP Server Profile' (dropdown), 'LDAP Base DN (Search)' (dropdown), 'Matched Attribute Priority' (checkbox), 'Alternate Routing' (checkbox), 'Next Hop Priority' (checkbox, checked), 'Next Hop In-Dialog' (checkbox), 'Ignore Route Header' (checkbox), 'ENUM' (checkbox), and 'ENUM Suffix' (text input). The bottom section contains a table with columns: 'Priority / Weight', 'LDAP Search Attribute', 'LDAP Search Regex Pattern', 'LDAP Search Regex Result', 'SIP Server Profile', 'Next Hop Address', 'Transport', and 'Delete'. The table has one row with values: '1', an empty field, an empty field, an empty field, 'SM10', '10.64.91.81:5061', 'None', and 'Delete'. Below the table is a 'Finish' button.

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 IPFR**).

Step 2 - On the **Next-Hop Address** window, for the first routing rule (AT&T Primary Border Element), populate the following fields:

- **Priority/Weight = 1**
- **Server Configuration = ATT-trk-svr** (from **Section 8.9.2**).
- **Next Hop Address:** select **192.168.38.69:5060 (UDP)**.

Step 3 - For the second routing rule (AT&T Secondary Border Element) click **Add** and enter the following:

- **Priority/Weight = 2**
- **Server Configuration = ATT-trk-svr** (from **Section 8.9.2**).
- **Next Hop Address:** select **192.168.37.149:5060 (UDP)**.

Step 4 - Click **Finish**.

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

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	Delete
1				ATT-trk-svr	192.168.38.69:5060 (UDP)	None	Delete
2				ATT-trk-svr	192.168.37.149:5060 (UDP)	None	Delete

Note – If desired, the **Load Balancing** parameter may be used to modify how the two defined AT&T Border Elements are accessed. **Priority** was used in the Reference Configuration.

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.

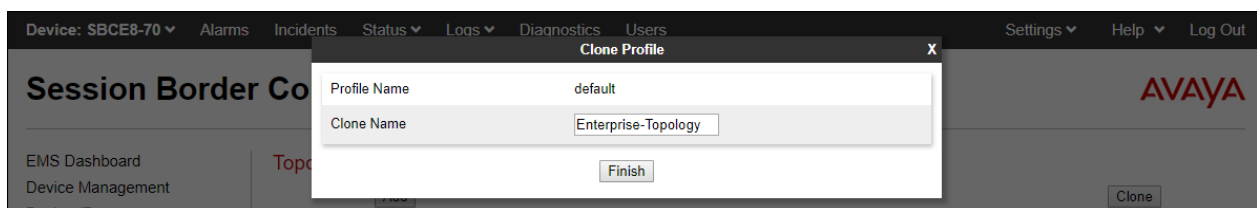
8.11.1. Topology Hiding – Enterprise

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

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.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu includes: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies (expanded), Application Rules (highlighted), Border Rules, Media Rules, Security Rules, Signaling Rules, Charging Rules, End Point Policy, and Groups. The main content area is titled 'Application Rules: sip-trunk' and features an 'Add' button. Below this is a list of application rules: default, default-trunk, default-subscriber-low, default-subscriber-high, default-server-low, default-server-high, and sip-trunk (highlighted). To the right of the list are buttons for 'Rename', 'Clone', and 'Delete'. The 'Application Rule' configuration window for 'sip-trunk' is open, showing a table for 'Application Rule' with columns: Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The table lists 'Audio' with 'In' and 'Out' checked and 'Maximum Concurrent Sessions' set to 200, and 'Video' with 'In' and 'Out' unchecked. Below the table is a 'Miscellaneous' section with 'CDR Support' set to 'Off' and 'RTCP Keep-Alive' set to 'No'. An 'Edit' button is at the bottom of the configuration window.

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

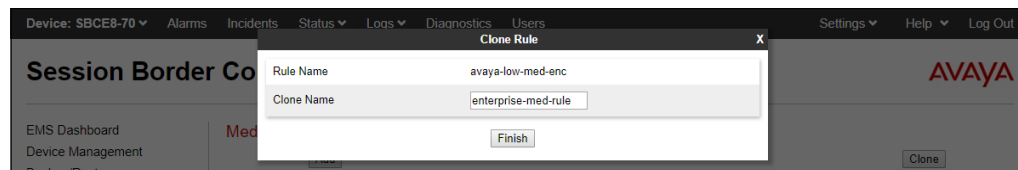
In the sample configuration, the default Media Rule **avaya-low-med-enc** was cloned to create the enterprise Media Rule, and modified as shown below:

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**.

Media Encryption

Audio Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

RTP

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

2⁴

Interworking

☒

Symmetric Context Reset

☒

Key Change in New Offer

☐

Video Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

RTP

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

2⁴

Interworking

☒

Symmetric Context Reset

☒

Key Change in New Offer

☐

Miscellaneous

Capability Negotiation

☒

Finish

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

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

Domain Policies

Application Rules

Border Rules

Media Rules

Security Rules

Signaling Rules

Charging Rules

End Point Policy Groups

Session Policies

TLS Management

Network & Flows

DMZ Services

Monitoring & Logging

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

entrp-med-rule-ANAT

Click here to add a description.

Encryption

Codec Prioritization

Advanced

QoS

MKI

☐

Lifetime

Any

Interworking

☒

Symmetric Context Reset

☒

Key Change in New Offer

☐

Video Encryption

Preferred Formats

SRTP_AES_CM_128_HMAC_SHA1_80
RTP

Encrypted RTCP

☐

MKI

☐

Lifetime

Any

Interworking

☒

Symmetric Context Reset

☒

Key Change in New Offer

☐

Miscellaneous

Capability Negotiation

☒

Edit

Rename

Clone

Delete

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 displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with categories like EMS Dashboard, Software Management, 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, DMZ Services, and Monitoring & Logging. The main content area is titled 'Media Rules: att-med-rule' and includes an 'Add' button. Below this 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 (selected), enterprise-med-rule, and entrp-med-rule-ANAT. The configuration panel for 'att-med-rule' has tabs for Encryption, Codec Prioritization, Advanced, and QoS. The 'Encryption' tab is active, showing settings for Audio Encryption (Preferred Formats: RTP, Interworking: checked, Symmetric Context Reset: checked, Key Change in New Offer: unchecked) and Video Encryption (Preferred Formats: RTP, Interworking: checked, Symmetric Context Reset: checked, Key Change in New Offer: unchecked). There is also a 'Miscellaneous' section with 'Capability Negotiation' unchecked. An 'Edit' button is at the bottom right of the configuration panel.

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

This screenshot shows the same 'Media Rules: att-med-rule' configuration page, but with the 'QoS' tab selected. The 'Media QoS Marking' section shows 'Enabled' checked and 'QoS Type' set to 'DSCP'. Below this, the 'Audio QoS' section shows 'Audio DSCP' set to 'EF', and the 'Video QoS' section shows 'Video DSCP' set to 'EF'. An 'Edit' button is located at the bottom right of the configuration panel.

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.

Session Border Controller for Enterprise



EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▾ Domain Policies

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

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Signaling Rules: enterprise-sig-rule

Add

RenameCloneDelete

Signaling Rules

- default
- No-Content-Ty...
- att-sig-rule
- enterprise-si...**
- ATT-TRK-BUSY
- ATT-TF-OPTI...

Click here to add a description.

GeneralRequestsResponsesRequest HeadersResponse HeadersSignaling QoS

UCID

Inbound

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

Outbound

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

Content-Type Policy

Enable Content-Type Checks☒

Action	Allow	Multipart Action	Allow
--------	-------	------------------	-------

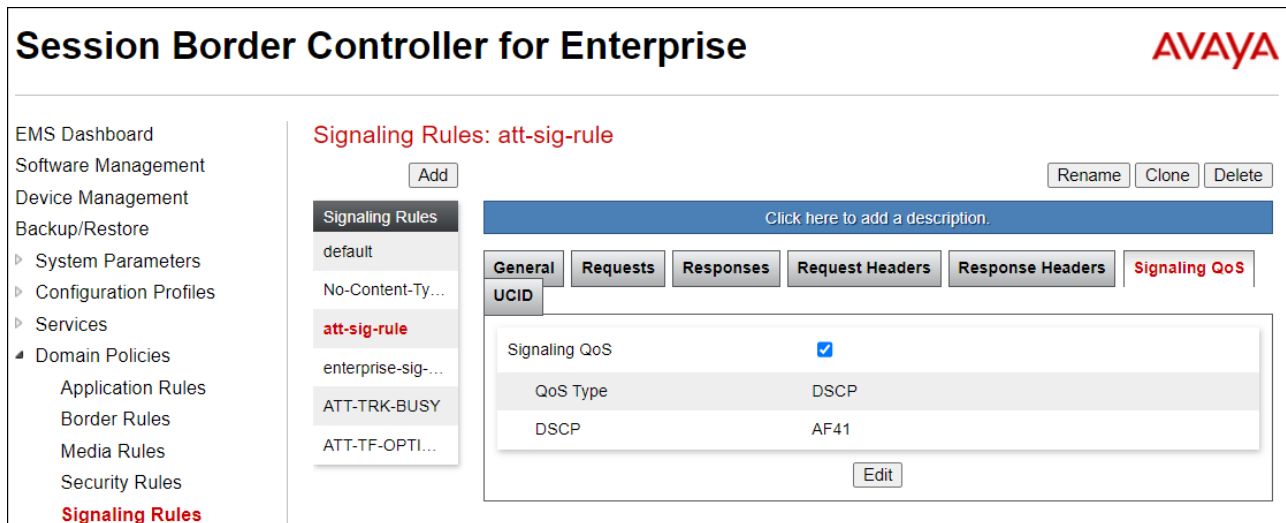
HG:Reviewed
SPOC 3/23/2023

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

111 of 133
AuSBC101EP81-FR

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**.



8.15. Endpoint Policy Groups

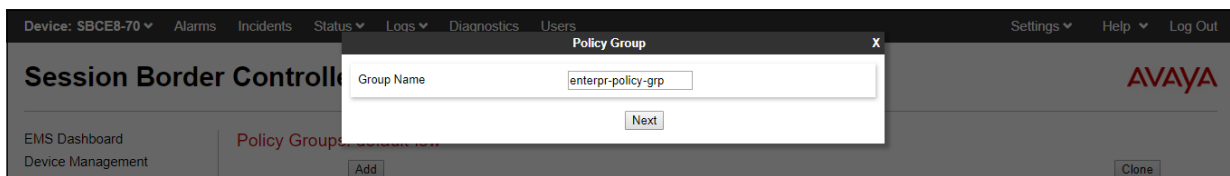
The rules created within the Domain Policies are assigned to an End Point Policy Group. The End Point Policy Group is then applied to a Server Flow in **Section 0**.

8.15.1. End Point Policy Group – Enterprise

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

Step 2 - Select **Add**.

- 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 0**).
- **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.

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▾ Domain Policies

Application Rules

Border Rules

Media Rules

Security Rules

Signaling Rules

Charging Rules

End Point Policy Groups

Policy Groups: enterpr-policy-grp

Add

RenameCloneDelete

Policy Groups

default-low

default-low-enc

default-med

default-med-enc

default-high

default-high-enc

avaya-def-low-...

avaya-def-hig...

avaya-def-hig...

att-policy-group

Click here to add a description.

Hover over a row to see its description.

Policy Group

Summary

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

HG:Reviewed
SPOC 3/23/2023

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

113 of 133
AuSBC101EP81-FR

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 0**)

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

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

Session Border Controller for Enterprise

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

Policy Groups: att-policy-group

Add

Policy Groups

default-low
default-low-enc
default-med
default-med-enc
default-high
default-high-enc
avaya-def-low-...
avaya-def-hig...
avaya-def-hig...
att-policy-gro...

RenameCloneDelete

Click here to add a description.
Click here to add a row description.

Policy Group

Summary

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

HG:Reviewed
SPOC 3/23/2023

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

114 of 133
AuSBC101EP81-FR

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 IPFR-EF service. These flows use the interfaces, policies, 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 for IPFR**
- **Server Configuration:** **SM10** (Section 8.9.1).
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** **Outside-B2-Signaling** (Section 8.6).
- **Signaling Interface:** **Inside-Sig-40** (Section 8.6).
- **Media Interface:** **Inside-Media** (Section 8.5).
- **End Point Policy Group:** **enterpr-policy-grp** (Section 8.15.1).
- **Routing Profile:** **Route to ATT IPFR** (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 for IPFR	
Criteria	Profile
Flow Name	SM Flow for IPFR
Server Configuration	SM10
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Outside-B2-Signaling
Signaling Interface	Inside-Sig-40
Media Interface	Inside-Media
Secondary Media Interface	None
End Point Policy Group	enterpr-policy-grp
Routing Profile	Route to ATT IPFR
Topology Hiding Profile	Enterprise-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>

8.16.2. 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., **IPFR flow to SM**.
- **Server Configuration:** **ATT-trk-svr** (Section 8.9.2).
- **Received Interface:** **Inside-Sig-40** (Section 8.6).
- **Signaling Interface:** **Outside-B2-Signaling** (Section 8.6).
- **Media Interface:** **Outside-B2-Media** (Section 8.5).
- **End Point Policy Group:** **att-policy-group** (Section 8.15.2).
- **Routing Profile:** **Route to SM10** (Section 8.10.1).
- **Topology Hiding Profile:** **SIP-Trunk-Topology** (Section 8.11.2).

View Flow: IPFR Flow for SM	
Criteria	
Flow Name	IPFR Flow for SM
Server Configuration	ATT-trk-svr
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside-Sig-40
Profile	
Signaling Interface	Outside-B2-Signaling
Media Interface	Outside-B2-Media
Secondary Media Interface	None
End Point Policy Group	att-policy-group
Routing Profile	Route to SM10
Topology Hiding Profile	SIP Trunk-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>

9. AT&T IP Flexible Reach – Enhanced Features Configuration

Information regarding the AT&T IPFR-EF service offer can be obtained at <https://www.business.att.com/products/sip-trunking.html> or by contacting an AT&T sales representative.

The reference configuration described in these Application Notes is located in the Avaya Solutions and Interoperability Test Lab. AT&T provided the IPFR-EF service border element IP addresses, the access DID numbers, and the associated DNIS digits used in the reference configuration. In addition, the AT&T IPFR-EF features, and their associated access numbers are also provisioned and assigned by AT&T.

10. Verification Steps

The following steps may be used to verify the configuration.

10.1. AT&T IP Flexible Reach – Enhanced Features

The following scenarios may be executed to verify Communication Manager, Session Manager, Avaya SBCE, and the AT&T IPFR-EF service interoperability:

- Place inbound and outbound calls, answer the calls, and verify that two-way talk path exists.
- Verify that calls remain stable and disconnect properly.
- Verify basic call functions such as hold, transfer, and conference.
- Verify the use of DTMF signaling.
- Place an inbound call to a telephone, but do not answer the call. Verify that the call covers to voicemail (e.g., Aura® Messaging). Retrieve voicemail messages either locally or from PSTN.
- Using the appropriate IPFR-EF access numbers and codes, verify that the following features are successful:
 - Network based Simultaneous Ring – The “primary” and “secondary” endpoints ring, and either may be answered.
 - Network based Sequential Ring (Locate Me) – Verify that after the “primary” endpoint rings for the designated time, the “secondary” endpoint rings and may be answered.
 - Network based Call Forwarding Always (CFA/CFU), Network based Call Forwarding Ring No Answer (CF-RNA), Network based Call Forwarding Busy (CF-Busy), Network based Call Forwarding Not Reachable (CF-NR) – Verify that based on each feature criteria, and calls are successfully redirected and may be answered.
- Inbound / Outbound T.38 fax.
- SIP OPTIONS monitoring of the health of the SIP trunk.
- Incoming and outgoing calls using the G.729 and G.711 ULAW codecs.

10.2. Avaya Aura® Communication Manager Verification

This section illustrates verifications examples in Communication Manager.

The following edited Communication Manager *list trace tac* trace output shows an incoming call received on trunk group 5, member 1. The adaptation in Session Manager has previously converted the IPFR-EF DNIS number included in the Request URI, to the Communication Manager extension 89321, before sending the INVITE to Communication Manager.

Note that initially the Avaya Media Server (**10.64.91.86**) is included on the media path.

```
list trace tac *05                                     Page 1

LIST TRACE

time          data
12:43:32 TRACE STARTED 02/02/2021 CM Release String cold-01.0.890.0-26685
12:43:39 SIP<INVITE sips:89321@avayalab.com SIP/2.0
12:43:39 Call-ID: b3748730389d0e46e0370310b623bb77
12:43:39 active trunk-group 5 member 1 cid 0xfe7
12:43:39 SIP>SIP/2.0 180 Ringing
12:43:39 Call-ID: b3748730389d0e46e0370310b623bb77
12:43:39 dial 89321
12:43:39 ring station 89321 cid 0xfe7
12:43:39 Alerting party uses public-unknown-numbering
12:43:39 G729 ss:off ps:20
12:43:39 rgn:4 [10.64.91.40]:17192
12:43:39 rgn:1 [10.64.91.86]:6138
12:43:39 G72264K ss:off ps:20
12:43:39 rgn:1 [192.168.7.103]:23216
12:43:39 rgn:1 [10.64.91.86]:6140
12:43:42 SIP>SIP/2.0 200 OK
12:43:42 Call-ID: b3748730389d0e46e0370310b623bb77
12:43:42 active station 89321 cid 0xfe7
12:43:42 Connected party uses public-unknown-numbering
```

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

The following screen shows **Page 2** of the output of the **status trunk 5/x** command (where x is the trunk group member active on the call, **1** in the example) pertaining to this same call. Note the signaling using port **5065** between Communication Manager and Session Manager. Note that after “shuffling” is completed, the media is “ip-direct” from the IP Telephone (**192.168.7.103**) to the inside IP address of Avaya SBCE (**10.64.91.40**), releasing the media resources in the Media Server.

```

status trunk 5/1                                     Page 2 of 3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling   IP Address                               Port
  Near-end:   10.64.91.75                               : 5065
  Far-end:    10.64.91.81                               : 5065
H.245 Near:
H.245 Far:
  H.245 Signaling Loc:                               H.245 Tunneled in Q.931? no

Audio Connection Type: ip-direct      Authentication Type: None
  Near-end Audio Loc:                               Codec Type: G.729
  Audio      IP Address                               Port
  Near-end:   192.168.7.103                               : 23216
  Far-end:    10.64.91.40                               : 17192

```

The screen below shows **Page 3** of the output of the **status trunk 5/1** command pertaining to this same call. Note that G729 and SRTP are used.

```

status trunk 5/1                                     Page 3 of 3
                                SRC PORT TO DEST PORT TALKPATH

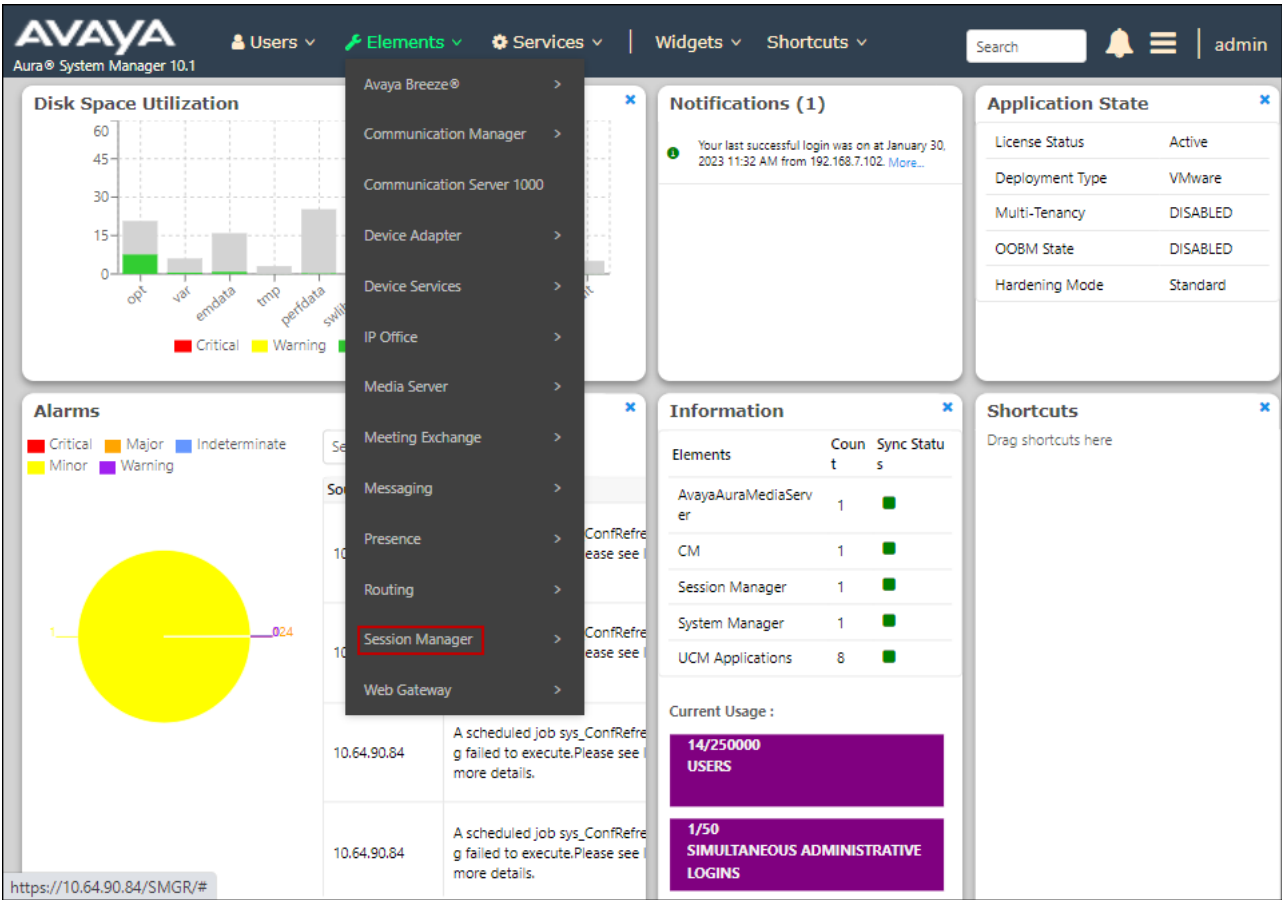
src port: T000051
T000051:TX:10.64.91.40:17192/g729/20ms/1-srtp-aescm128-hmac80
S000559:RX:192.168.7.103:23216/g729a/20ms/1-srtp-aescm128-hmac80

```

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. Note that the **Test Passed**, **Alarms**, **Service State** and **Data Replication** columns all show good status.

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Session Manager

Session Manager

Dashboard

Session Manager ...

Global Settings

Communication Pro...

Network Configur...

Device and Locati...

Application Confi...

System Status

Session Manager Dashboard

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

Session Manager Instances

Service State

Shutdown System

EASG

Clear Logs

As of 11:48 AM

1 Item

Show

All

Filter: Enable

	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Load Factor	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Profile	Version
<input type="checkbox"/>	Session Manager	Core	✓	0/0/0	Up	Accept New Service	0/0/0	1/17	0	2/2	✓	✓	Normal	Enabled	1	10.1.0.2.1010219

Select : All, None

HG:Reviewed
SPOC 3/23/2023

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

121 of 133
AuSBC101EP81-FR

In the example, the entry **1/17** under the **Entity Monitoring** column shows that there are alarms on 1 out of the 17 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									
17 Items Filter: Enable									
	SIP Entity Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	SBCE30 HA	IPv4	10.64.91.32	5061	TLS	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
<input type="radio"/>	UCSP SIP GW	IPv4	Entity is not monitored	0	---	N.A.	DOWN		NOTMONITORED
<input type="radio"/>	SBCE-70 Toll Free	IPv4	Entity is not monitored	0	---	N.A.	DOWN		NOTMONITORED
<input type="radio"/>	Aura Messaging	IPv4	Entity is not monitored	0	---	N.A.	DOWN		NOTMONITORED
<input type="radio"/>	CM-TG5	IPv4	10.64.91.87	5065	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG6	IPv4	10.64.91.87	5066	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG1	IPv4	10.64.91.87	5081	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Avaya Messaging	IPv4	10.64.19.90	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	SBCE-90 Vz1	IPv4	10.64.91.50	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG8	IPv4	10.64.91.87	5068	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG3	IPv4	10.64.91.87	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	SBCE-70 IPFR	IPv4	10.64.91.40	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
<input type="radio"/>	Experience Portal	IPv4	10.64.91.90	5061	TLS	FALSE	UP	200 OK	UP

Note – On the **SBCE-ATT** 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 forwards the Session Manager generated OPTIONS on to the AT&T IPFR-EF Border Element, it is the AT&T Border Element that is generating the 405, and the Avaya SBCE sends the response back to Session Manager.

Other Session Manager useful verification and troubleshooting tools include:

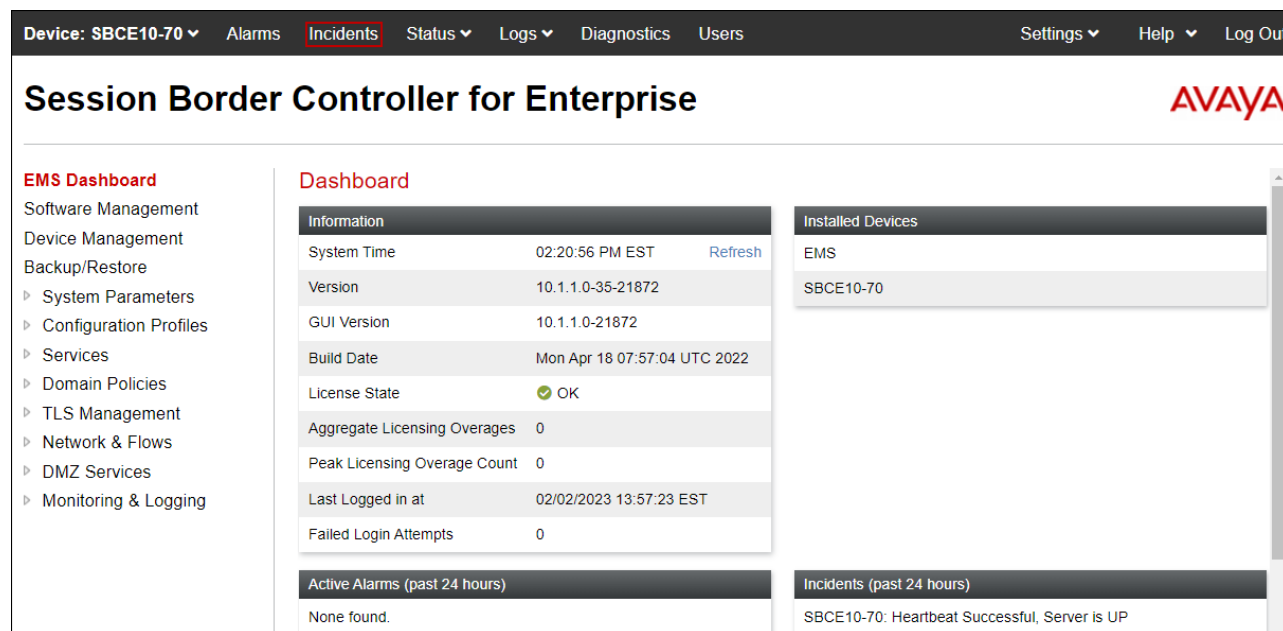
- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System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

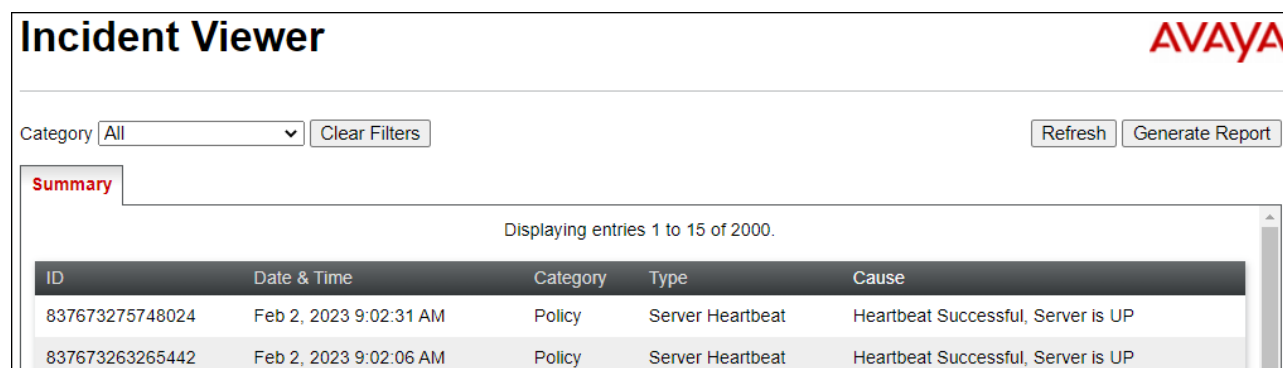
This section provides verification steps that may be performed with the Avaya SBCE.

10.4.1. Incidents

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



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.



ID	Date & Time	Category	Type	Cause
837673275748024	Feb 2, 2023 9:02:31 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
837673263265442	Feb 2, 2023 9:02:06 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP

10.4.2. Server Status

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

The screenshot shows the Avaya SBCE interface. The top navigation bar includes 'Device: SBCE10-70', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The 'Status' menu is open, showing options: 'SIP Statistics', 'Periodic Statistics', 'User Registrations', 'Server Status' (highlighted with a red box), 'Performance Status', and 'IP / URI Blocklist'. The left sidebar shows 'Device Management' as the active section, with sub-items like 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', and 'TLS Management'. The main content area shows a table with columns: 'Device Name', 'Management IP', 'Version', and 'Status'. The table contains one row for 'SBCE10-70' with management IP '10.64.90.70' and version '10.1.1.0-35-21872'. The status is 'Commissioned'. Below the table are buttons for 'Reboot', 'Shutdown', 'Restart Application', 'View', 'Edit', and 'Uninstall'.

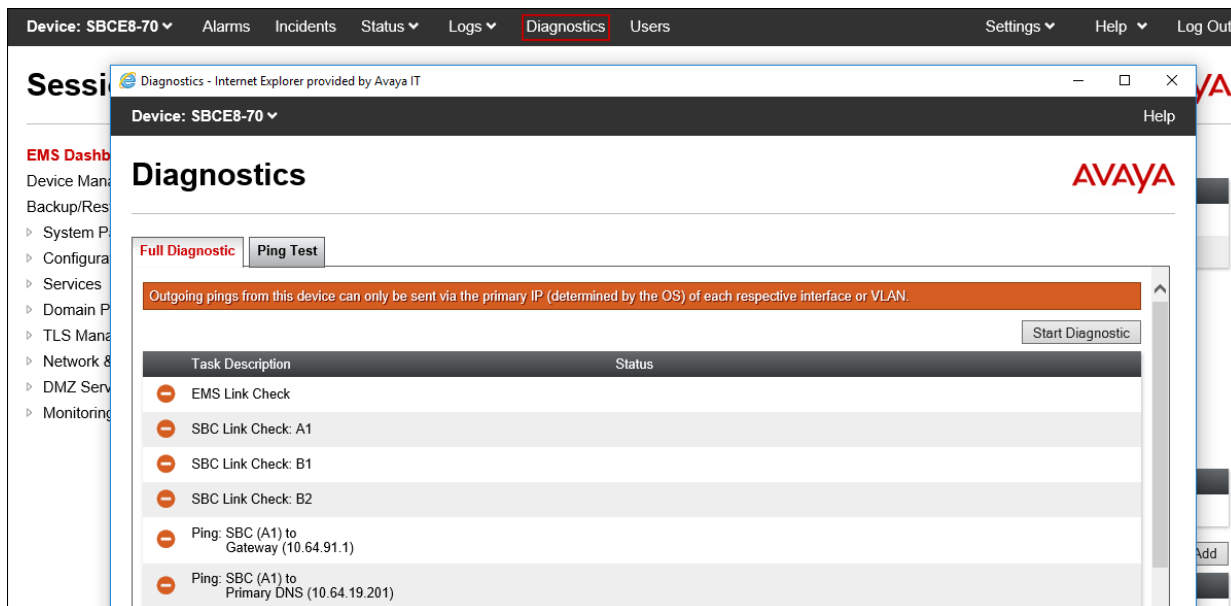
The **Server Status** screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat to be enabled on the SIP Server Configuration profiles, as configured in **Section 8.9**.

The screenshot shows the 'Status' screen in the Avaya SBCE interface. The 'Server Status' tab is selected. The table displays the following data:

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
IPOSE-Call-Server	10.64.19.170	10.64.19.170	5061	TLS	UP	UNKNOWN	02/02/2023 09:02:31 EST
SM10	10.64.91.85	10.64.91.85	5061	TLS	UP	UNKNOWN	02/02/2023 09:02:06 EST
Session Manager H	10.64.101.249	10.64.101.249	5061	TLS	UP	UNKNOWN	02/02/2023 09:02:06 EST
ATT-trk-svr	10.64.38.69	10.64.38.69	5060	UDP	UP	UNKNOWN	02/02/2023 09:02:06 EST
ATT-trk-svr	10.64.37.149	10.64.37.149	5060	UDP	UP	UNKNOWN	02/02/2023 09:02:06 EST

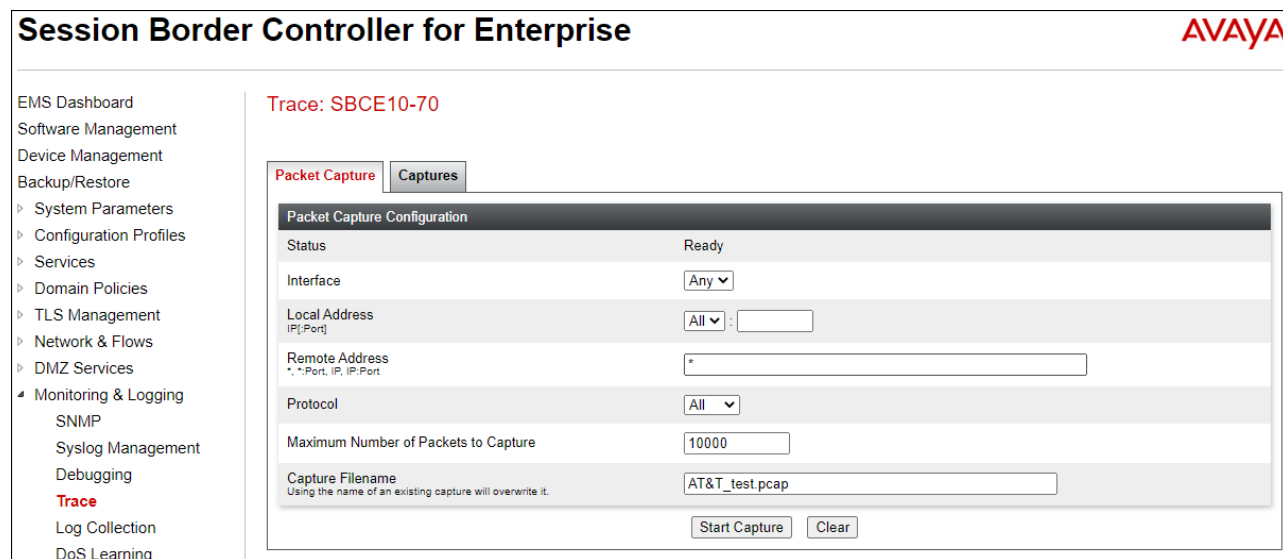
10.4.3. Diagnostic

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



10.4.4. Tracing

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



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

AVAYA

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

Trace: SBCE10-70

Packet CaptureCaptures

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 <small>IP[:Port]</small>	All :
Remote Address <small>*, *,Port, IP, IP:Port</small>	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	ATT_test.pcap

Stop Capture

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

Session Border Controller for Enterprise

AVAYA

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

Trace: SBCE10-70

Packet CaptureCaptures

Refresh

File Name	File Size (bytes)	Last Modified	
ATT_test_20230202143546.pcap	516,096	February 2, 2023 at 2:36:50 PM EST	Delete

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 10.1, Avaya Aura® Session Manager 10.1, Avaya Experience Portal 8.1 and the Avaya Session Border Controller for Enterprise 10.1 can be configured to interoperate successfully with the AT&T IP Flexible Reach – Enhanced Features service, within the constraints described in **Section 2.2**.

Testing was performed on a production AT&T IP Flexible Reach – Enhanced Features 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 10.1.x, Issue 2, March 2022
- [2] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 4, September 2022
- [3] *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 10.1.x, Issue 4, September 2022
- [4] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 7, September 2022

Avaya Aura® Communication Manager

- [5] *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 10.1.x, Issue 6, January 2023
- [6] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 3, December 2022
- [7] *Administering Avaya G430 Branch Gateway*, Release 10.1, Issue 2, July 2022
- [8] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 10.1.x, Issue 4, July 2022
- [9] *Integrating Avaya Aura® Media Server with Avaya Aura® Communication Manager*, Release 8.0.x, May 2020

Avaya Session Border Controller for Enterprise

- [10] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1.x, Issue 2, January 2023
- [11] *Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform*, Release 10.1.x, Issue 1, December 2021

Avaya Messaging

- [12] *Avaya OfficeLink™ Integration with Avaya Aura CM and Session Manager* 8, July 2019

Avaya Experience Portal

- [13] *Administering Avaya Experience Portal*, Release 8.1.2, Issue 1, October 2022
- [14] *Implementing Avaya Experience Portal on a single server*, Release 8.1.2, Issue 1, October 2022

AT&T IP Flexible Reach - Enhanced Features Service:

- [15] *AT&T IP Flexible Reach – Product Description*
<https://www.business.att.com/content/dam/attbusiness/briefs/voice-and-collaboration-ip-flex-reach-product-brief.pdf>

13. Appendix A – Avaya SBCE – Refer Handling

One of the important capabilities to the Experience Portal environment is the Avaya SBCE Refer Handling option. As described in **Section 3.2.4**, 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:** **59[0-9]{3}@.*** This will match 5-digit local extensions starting with 59, e.g., 59001.
- 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 59[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



EMS Dashboard

Software Management

Device Management

Backup/Restore

System Parameters

Configuration Profiles

- Domain DoS
- Server Interworking
- Media Forking
- Routing
- Topology Hiding
- Signaling Manipulation
- URI Groups**
- SNMP Traps

URI Groups: internal-extensions

Add

RenameDelete

URI Groups

Emergency

internal-exte...

Click here to add a description.

URI Group

Add

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
59[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**.

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The left-hand menu shows the navigation path: EMS Dashboard > Software Management > Device Management > Backup/Restore > System Parameters > Configuration Profiles > Server Interworking. The main area is titled "Interworking Profiles: ATT-Interworking" and features a list of profiles on the left, including "cs2100", "avaya-tu", "ATT REFER Handling", "Enterprise Interwork", "IPO Interwork IPv6", "ATT-Interworking" (highlighted in red), and "SP-Interworking". The "ATT-Interworking" profile is selected, and its configuration is shown in the main panel. The "General" tab is active, displaying a table of configuration parameters. The "Refer Handling" row is highlighted with a red border, showing "Refer Handling" set to "No" and "URI Group" set to "internal-extensions". Other parameters include "Hold Support" (None), "180 Handling" (None), "181 Handling" (None), "182 Handling" (None), "183 Handling" (None), "Send Hold" (No), "Delayed Offer" (Yes), "3xx Handling" (No), "Diversion Header Support" (No), "Delayed SDP Handling" (No), "Re-Invite Handling" (No), "Prack Handling" (No), "Allow 18X SDP" (No), "T.38 Support" (Yes), "URI Scheme" (SIP), "Via Header Format" (RFC3261), "SIPS Required" (Yes), and "MediaSec" (No). The interface includes buttons for "Rename", "Clone", and "Delete" at the top right, and an "Edit" button at the bottom right. A watermark "idows" and the text "activate Windows." are visible in the bottom right corner.

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

14. Appendix B – Avaya SBCE – SigMa Script File

Details of the Signaling Manipulation script used in the configuration of the Avaya SBCE, in Section 8.8

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

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

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

    }
}

//OPTIONAL - Change AT&T Max-Forwards value from 0 to 30
within session "OPTIONS"
{
    act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {
        %HEADERS["Max-Forwards"][1] = "30";
    }
}

// OPTIONAL Experience Portal - modify PAI Header

within session "INVITE"
{
    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
        if (%INITIAL_REQUEST = "true") then
        {
            if (%HEADERS["User-Agent"][1].regex_match("Avaya\-VoicePortal")) then
            {
                %HEADERS["P-Asserted-Identity"][1].URI.USER = "3035559329";
            }
        }
    }
}
```

©2023 Avaya Inc. All Rights Reserved.

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

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