Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller for Enterprise 10.1 in High Availability Configuration to support BT Wholesale Hosted SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller for Enterprise 10.1 in High Availability Configuration, to support BT Wholesale Hosted SIP Trunking Service using Enterprise Trunks.

The test was performed to verify SIP trunk registration and features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consultative), conference, and voice mail. Calls were placed between the public switched telephone network (PSTN) and various Avaya endpoints. Testing included failover scenarios of the Avaya Session Border Controller for Enterprise.

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

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

Table of Contents

1. Introduction 5
2. General Test Approach and Test Results 6
  2.1. Interoperability Compliance Testing 7
  2.2. Test Results 8
  2.3. Support 9
3. Reference Configuration 10
4. Equipment and Software Validated 13
5. Configure Avaya Aura® Communication Manager 14
  5.1. Verify Licensed Features 14
  5.2. System – Parameters Features 16
  5.3. Dial Plan 16
  5.4. IP Node Names 17
  5.5. IP Codec Sets 18
    5.5.1. Codecs for IP Network Region 1 (calls within the CPE) 18
    5.5.2. Codecs for IP Network Region 7 (calls to/from BT) 19
  5.6. IP Network Regions 20
    5.6.1. IP Network Region 1 – Local CPE Region 20
    5.6.2. IP Network Region 7 – BT Trunk Region 22
  5.7. SIP Trunks 23
    5.7.1. SIP Trunk for Inbound/Outbound BT calls 23
    5.7.2. Local SIP Trunk (Avaya SIP Telephones, Messaging Access, etc.) 27
  5.8. Public Numbering 28
  5.9. Private Numbering 29
  5.10. Route Patterns 29
    5.10.1. Route Pattern for Calls to BT 29
    5.10.2. Route Pattern for Calls within the CPE 30
  5.11. Automatic Route Selection (ARS) Dialing 31
  5.12. Automatic Alternate Routing (AAR) Dialing 31
  5.13. Avaya G430 Media Gateway Provisioning 32
  5.14. Avaya Aura® Media Server Provisioning 33
  5.15. Save Translations 34
6. Configure Avaya Aura® Session Manager 35
  6.1. System Manager Login and Navigation 36
  6.2. SIP Domain 37
  6.3. Locations 37
    6.3.1. Main Location 38
    6.3.2. CM-TG7 Location 38
    6.3.3. SBCs Location 38
  6.4. Configure Adaptations 39
    6.4.1. Adaptation for Avaya Aura® Communication Manager 39
    6.4.2. Adaptation for the BT SIP Trunking service 41
  6.5. SIP Entities 42
    6.5.1. Avaya Aura® Session Manager SIP Entity 43
    6.5.2. Avaya Aura® Communication Manager SIP Entity – Public Trunk 45

6.5.3. Avaya Aura® Communication Manager SIP Entity – Local Trunk 46
6.5.4. Avaya Session Border Controller for Enterprise SIP Entity 46
6.6. Entity Links 47
6.6.1. Entity Link to Avaya Aura® Communication Manager – Public Trunk 47
6.6.2. Entity Link to Avaya Aura® Communication Manager – Local Trunk 48
6.6.3. Entity Link for the BT SIP Trunking service via the Avaya SBCE 48
6.7. Time Ranges 49
6.8. Routing Policies 49
6.8.1. Routing Policy for Inbound Calls to Avaya Aura® Communication Manager 49
6.8.2. Routing Policy for Outbound Calls to BT 51
6.9. Dial Patterns 52
6.9.1. Matching Inbound PSTN Calls to Avaya Aura® Communication Manager 52
6.9.2. Matching Outbound Calls to BT/PSTN 54
7. Configure Avaya Session Border Controller for Enterprise 55
7.1. Device Management – Status 56
7.2. TLS Management 58
7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise 58
7.2.2. Server Profiles 59
7.2.3. Client Profiles 60
7.3. Network Management 61
7.4. Media Interfaces 62
7.5. Signaling Interfaces 63
7.6. Server Interworking Profile 64
7.6.1. Server Interworking Profile – Enterprise 64
7.6.2. Server Interworking Profile – Service Provider 65
7.7. Signaling Manipulation 67
7.8. SIP Server Profiles 68
7.8.1. SIP Server Profile – Session Manager 68
7.8.2. SIP Server Profile – Service Provider 70
7.9. Routing Profiles 73
7.9.1. Routing Profile – Session Manager 73
7.9.2. Routing Profile – Service Provider 74
7.10. Topology Hiding Profile 75
7.10.1. Topology Hiding – Enterprise 75
7.10.2. Topology Hiding – Service Provider 76
7.11. Application Rules 76
7.12. Media Rules 77
7.12.1. Media Rule – Enterprise 77
7.12.2. Media Rule – Service Provider 78
7.13. Signaling Rules 79
7.13.1. Signaling Rule – Enterprise 79
7.13.2. Signaling Rule – Service Provider 79
7.14. Endpoint Policy Groups 80
7.14.1. End Point Policy Group - Enterprise 80
7.14.2. End Point Policy Group – Service Provider 81
7.15. End Point Flows – Server Flows 82

7.15.1. Server Flow – Enterprise 82
7.15.2. Server Flow – Service Provider 83
8. BT Wholesale Hosted SIP Trunking Service Configuration 84
9. Verification and Troubleshooting 85
9.1. General Verification Steps 85
9.2. Communication Manager Verification 85
9.3. Session Manager Verification 86
9.4. Avaya Session Border Controller for Enterprise Verification 88
9.4.1. Device Management 88
9.4.2. Alarms 88
9.4.3. Incidents 89
9.4.4. Server Status 90
9.4.5. Tracing 91
10. Conclusion 93
11. Additional References 93
12. Appendix B – Avaya SBCE – SigMa Script File 94

1. Introduction

These Application Notes describe the configuration of an Avaya SIP-enabled enterprise solution consisting of Avaya Aura® Session Manager Release 10.1, Avaya Aura® Communication Manager Release 10.1 and Avaya Session Border Controller for Enterprise Release 10.1, to support the BT Wholesale Hosted SIP Trunking service using Enterprise Trunks. In the reference configuration, the Avaya Session Border Controller for Enterprise (Avaya SBCE) is deployed in a High Availability (HA) configuration.

The Avaya SBCE is the point of connection between Avaya CPE and the BT Wholesale Hosted SIP Trunking service. It is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling and media for interoperability.

Enterprises might deploy the Avaya SBCE in High Availability mode to ensure signaling and media preservation in the event of any hardware or software failures of the Session Border Controller server. High availability requires a minimum of two Avaya SBCE devices and one standalone Element Management System (EMS) server.

The BT Wholesale Hosted SIP Trunking Service referenced within these Application Notes is designed for business customers. Customers using this service with this Avaya solution are able to place and receive PSTN calls via a broadband wide area network (WAN) connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

The terms "service provider", "BT", "BT SIP Trunking" or "BT Wholesale SIP Trunking" will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to BT's network via the public Internet, as depicted in **Figure 1**, and exercise the features and functionalities listed in **Section 2.1**.

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

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

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

2.1. Interoperability Compliance Testing

To verify SIP trunk interoperability the following features and functionalities were exercised during the interoperability compliance test:

- Public DNS "SRV" record queries to establish SIP trunk connections to BT SIP servers.
- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, Digital and Analog telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider's network.
- Outgoing PSTN calls from Avaya endpoints, including SIP and H.323, Digital and Analog telephones at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider's network.
- Incoming and outgoing PSTN calls to/from Avaya Workplace Client for Windows (SIP).
- Caller ID presentation.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two-way speech-path. Testing was performed with codecs: G.711A, G.711U, G.722 64K and G.729(a), BT's preferred codec order.
- Proper early media transmissions.
- 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., Aura® Messaging, Communication Manager vector digit collection steps).
- Outbound calls to the BT SIP platform using Class 5 CLI
- SIP Trunk Registration after SBCE HA failover.
- Call preservation of active calls after SBCE HA failover.
- Processing of new inbound and outbound calls after SBCE HA failover.
- Resilience testing with primary SBC failure on the BT side.
- Avaya Remote Worker functionality, using Avaya Workplace for Windows and Avaya Agent for Desktop softphones, registered to Session Manager via a separate Avaya SBCE.

Items not supported or not tested included the following:

- T.38 and G.711 passthrough fax are supported but were not tested.
- Inbound and Outbound toll-free calls were not tested.
- 0, 0+10 digits, Directory Assistance and Emergency calls were not tested.
- International calls were not tested.
- Network Call Redirection using the "302 Moved Temporarily" method is not supported.
- SIP User-to-User Information (UUI) is not supported.

2.2. Test Results

Interoperability testing of BT Wholesale Hosted SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **SIP OPTIONS Messages** – During the compliance test BT did not send SIP OPTIONS messages to the Avaya CPE. Session Manager did send SIP OPTIONS messages to BT via the Avaya SBCE. This was sufficient to keep the SIP trunk in service.
- **Session Interval Too Small** – Initially Communication Manager replied with a "422 Session Interval Too Small" to the INVITES received from BT. The Preferred Min Session Refresh setting on the Trunk Group (**Section 5.7.1.2**) was changed from the default 600 to 450 seconds (half of the 900 seconds offered on the BT Invite), resolving the issue.
- **Avaya phones screens show character string on outbound calls** –BT sends a long cryptic character string in the Contact Header of its SIP Requests and Responses, and it does not send a PAI header. On outbound calls made from Avaya endpoints, it was observed that the phones screens displayed the BT cryptic Contact header information, instead of the dialed number. An Adaptation was created in Session Manager (**Section 6.4.2**) using the "Orange Adapter" and applied to SIP Entity corresponding to the Avaya SBCE. This Adapter modifies how Session Manager generates the P-Asserted-Identity (PAI) header in a request or response, if the header is not present on ingress. The default behavior of the Session Manager is overridden and the PAI is generated from the From header in requests and To header in responses from BT. With the Orange Adapter in place, the Avaya sets displayed the dialed number information instead of the BT Contact header information on outbound calls.
- **Unsupported Media Type** – BT sent a "415 Unsupported Media Type" error message to the UPDATES with XML information during calls transferred back to BT. A SigMa script was added script on the Avaya SBCE to remove the XML information from the SDP of outbound UPDATES to BT on transferred calls, resolving the error. See **Section 7.7**.
- **"+" on origination headers** – BT does not support the "+" on E.164 formatted numbers used by Communication Manager for the Calling Line Identification in the origination headers on outbound calls. A Session Manager Adaptation was used to remove the "+" in the From and P-Asserted Identity headers. See **Section 6.4.2**. A SigMa script was also needed on the Avaya SBCE to remove the "+" in the Diversion header of inbound calls that are forwarded back to the PSTN. See **Section 7.7**.
- **Avaya SBCE DNS-SRV – Failover is supported but no fall back to primary BT SIP server**: The Avaya SBCE was configured to use DNS/SRV record queries for the BT SIP Server profile, and with **Register with the Priority Server** selected. It was observed that the Avaya SBCE will failover and register to the secondary BT SIP server when a fault was introduced into the primary BT SIP server, as expected, but no fall back to the primary SIP server was attempted after the primary SIP server was back in service. This issue is under investigation by Avaya.

- **Avaya SBCE DNS-SRV – The Avaya SBCE keeps sending REGISTER messages to the primary server**: With the Avaya SBCE configured to use DNS/SRV record queries and to Register with the Priority Server, and a fault was introduced into the primary BT SIP server, it was observed that the Avaya SBCE kept sending REGISTER messages to the primary server for approximately two minutes after falling back and registering with the secondary BT SIP Server. If the BT primary server came back in service while the SBCE was still sending these REGISTERs, an error condition occurred with duplicated address of records on the BT platform, and calls failed until the current registration TTL expired, clearing the condition. This issue is under investigation by Avaya.

2.3. Support

For support on BT Wholesale Hosted SIP Trunking Service visit the corporate Web page at: https://www.btwholesale.com/help-and-support.html

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

3. Reference Configuration

Figure 1 illustrates the test configuration used for the DevConnect compliance testing. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the BT Wholesale Hosted SIP Trunking Service through the public Internet.

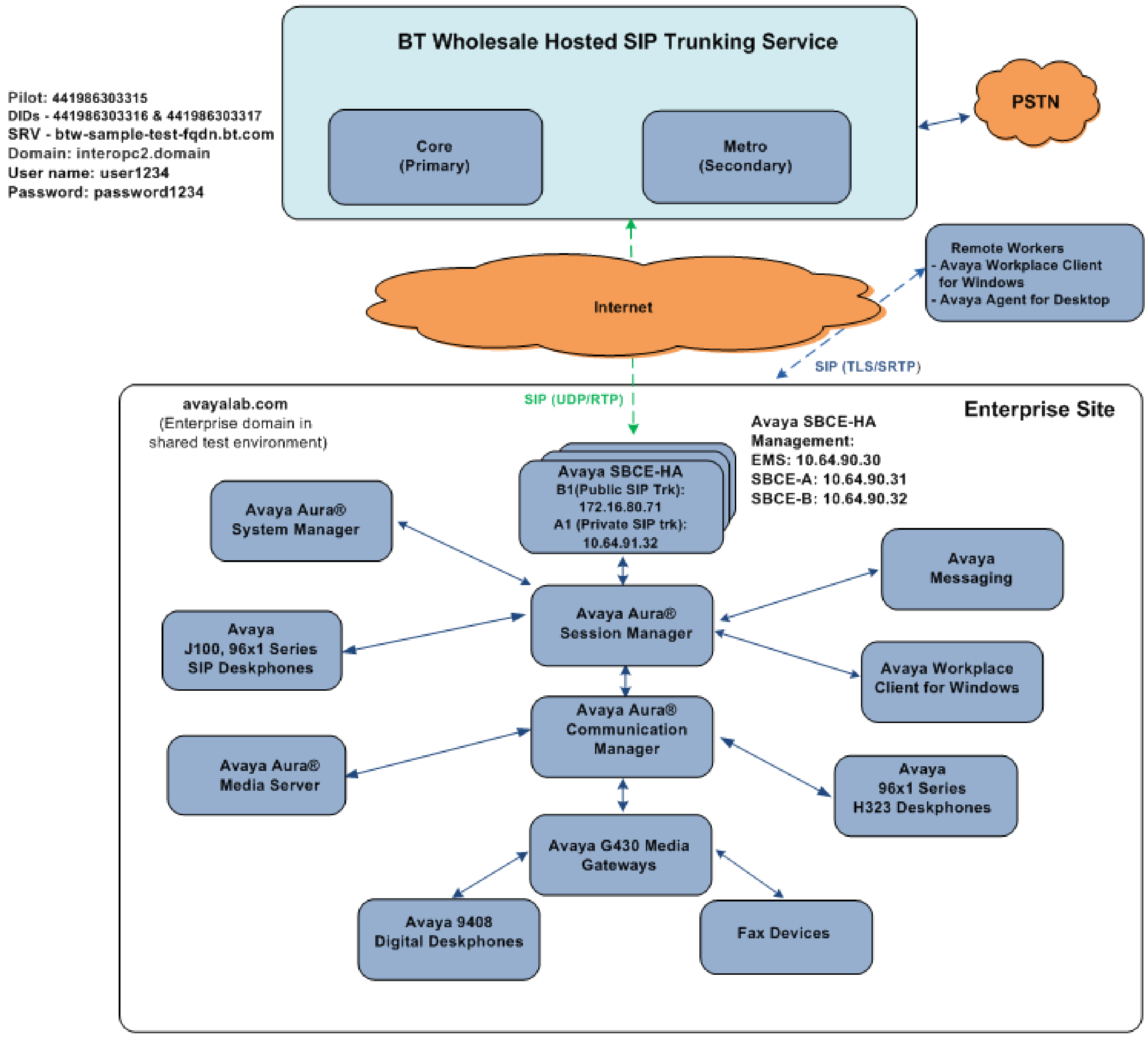


Figure 1: Avaya Interoperability Test Lab Configuration

Note – For security reasons, public IP addresses and FQDNs used in the reference configuration for the Avaya SBCE and the service provider are not included in this document. However, as placeholders in the following configuration sections, the IP addresses **172.16.80.71** (Avaya SBCE "Public" interface B1), and **btw-sample-test-fqdn.bt.com** (BT SBCs FQDN), are specified. In addition, DID numbers shown in this document are masked as well.

In an actual customer configuration, the enterprise site may include additional network components between the service provider and the Avaya SBCE, such as a router or data firewall. All SIP and RTP traffic between the service provider and the Avaya SBCE must be allowed to pass through these devices.

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

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise HA.
- Avaya Messaging.
- Avaya Aura® Media Server.
- Avaya G430 Media Gateway.
- Avaya 96X1 Series IP Deskphones using the SIP and H.323 software bundle
- J100 Series IP Deskphones using the SIP software bundle
- Avaya Workplace Client for Windows
- Avaya Agent for Desktop
- Avaya 9400 Series Digital Phones

The Avaya SBCE is located at the edge of the enterprise. It has two physical interfaces, interface B1 is used to connect to the public network, while interface A1 is used to connect to the private network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. The Avaya SBCE provides network address translation at both the IP and SIP layers.

In the reference configuration, the Avaya SBCE is deployed in High Availability mode, where the HA pair is deployed within the enterprise in a parallel mode configuration. High availability requires a minimum of two Avaya SBCE devices and one standalone Element Management System (EMS) server. The Avaya SBCE HA can be deployed as a pair either in the enterprise DMZ or core, or geographically dispersed where each Avaya SBCE resides in a separate, physical facility, over a network with minimum or no latency. In the reference configuration, the Avaya SBCEs run on a VMware platform. This solution is extensible to other Avaya Session Border Controller for Enterprise platforms as well.

In the SBCE HA configuration, the active SBCE is the primary server through which all signaling packets are routed. The interface ports on the standby SBCE do not process any traffic. When a failure is detected on the primary SBCE by the Avaya Element Management System (EMS), the network interface ports of the original primary SBCE are automatically disabled and the network interface ports of the standby are enabled, thus becoming the new active server.

High availability requires Gratuitous Address Resolution Protocol (GARP) support on the connected network elements. When the primary Avaya SBCE fails over, the secondary Avaya SBCE broadcasts a GARP message to announce that the secondary Avaya SBCE is now receiving requests. The GARP message announces that a new MAC address is associated with the Avaya SBCE IP address. Devices that do not support GARP must be on a different subnet with a GARP-aware router or L3 switch to avoid direct communication with the SBCE.

In the reference configuration, BT used a single FQDN that resolved primary and secondary SIP servers on the BT network. The Avaya SBCE used DNS/SRV record queries to obtain these servers details (IP addresses, ports, priority, etc.), and it was configured to register with the BT server with the highest priority. If the highest priority server was found non-functional on DNS TTL expiry, the SBCE would then register with the second highest priority server.

The transport protocol/port between the Avaya SBCE public interface and BT, across the public Internet, was UDP/5060. TLS/5061 was used to connect the private interface of the Avaya SBCE to the Enterprise network.

For inbound calls, the calls flowed from BT's network to the Avaya SBCE, then to Session Manager. Session Manager used the configured dial patterns (or regular expressions) and routing policies to determine the trunk where to send the call to Communication Manager.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the Avaya SBCE for egress to the service provider's network.

A separate SIP trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk without affecting other enterprise SIP traffic. This trunk carried both inbound and outbound traffic.

Avaya Remote Worker endpoints (Avaya Workplace for Windows and Avaya Agent for Desktop) were used in the reference configuration. Remote Worker endpoints reside on the public side of an Avaya SBCE, and registers/communicates with Session Manager / Communication Manager as though it was an endpoint residing in the private CPE space. The Remote Worker uses protocols Transport Layer Security (TLS) for signaling, and Secure Real-time Transport Protocol (SRTP) for media.

Note – The configuration of the Remote Worker is beyond the scope of this document. Refer to the Avaya SBCE documentation on the **Additional References** section for information on Remote Worker deployments.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® System Manager	10.1.0.1.0614394
Avaya Aura® Session Manager	10.1.0.1.1010105
Avaya Aura® Communication Manager	10.1.0.10-SP1 Update ID 10.1.0.974.0-27372
Avaya Session Border Controller for Enterprise HA	10.1.0.0-32-21432 Hotfix (sbce-10.1.0.0-34-21958-hotfix-05192022.tar.gz)
Avaya Aura® Media Server	10.1.0.77
Avaya Messaging	10.8 SP1
Avaya G430 Media Gateway	42.4
Avaya 96x1 Series IP Deskphone (H.323)	6.8511
Avaya J100 IP Deskphones (SIP, J169, J179)	4.0.12.0.6
Avaya 96x1 Series IP Deskphone (SIP)	7.1.15.0.14
Avaya 9408 Digital Deskphone	2.00
Avaya Workplace Client for Windows	3.26.0.64
Avaya Agent for Desktop	2.0.6.20.3004
BT Wholesale Hosted SIP Trunking Service	
Acme Packet 6350	SCZ8.4p7k
BroadWorks	R24

Table 1: Equipment and Software Versions

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager to work with the BT Wholesale Hosted SIP Trunking service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider. It is assumed that the general installation of Communication Manager, the Avaya G430 Media Gateway and the Avaya Aura® Media Server has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

5.1. Verify Licensed Features

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

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: 12000  0
           Maximum Concurrently Registered IP Stations: 2400   2
             Maximum Administered Remote Office Trunks: 12000  0
Maximum Concurrently Registered Remote Office Stations: 2400   0
              Maximum Concurrently Registered IP eCons: 128    0
  Max Concur Registered Unauthenticated H.323 Stations: 100    0
                        Maximum Video Capable Stations: 36000  0
                   Maximum Video Capable IP Softphones: 2400   6
                       Maximum Administered SIP Trunks: 12000  60
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 688    0
```

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 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)?
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y               Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? Y
```

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
                                              System Management Data Transfer? n
          Personal Station Access (PSA)? y              Tenant Partitioning? y
                        PNC Duplication? n      Terminal Trans. Init. (TTI)? y
                   Port Network Support? n              Time of Day Routing? y
                        Posted Messages? 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

Enter the **display system-parameters features** command. On **Page 1** of the form, verify that **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.

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

- 5-digit extensions with a **Call Type** of **ext** beginning with 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 5.7**.

```
change dialplan analysis                                         Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 1

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length 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. IP 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**

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Communication Manager processor ethernet interface ***(*proc**r) and the Session Manager security module (**SM**). These node names will be needed for defining the service provider signaling group in **Section 5.7**.

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

5.5. 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.

5.5.1. Codecs for IP Network Region 1 (calls within the CPE)

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.722-64K**, **G.711A**, **G.711MU** and **G.729A** are included in the codec list.

```
change ip-codec-set 1                                          Page   1 of   2

                          IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.722-64K                   2        20
 2: G.711MU          n          2        20
 3: G.711A           n          2        20
 4: G.729A           n          2        20
 5:

     Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
```

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

                                           Redun-                      Packet
                          Mode             dancy                       Size(ms)
    FAX                   t.38-standard    0     ECM: y
    Modem                 off              0
    TDD/TTY               US               3
    H.323 Clear-channel   n                0
    SIP 64K Data          n                0                           20

Media Connection IP Address Type Preferences
 1: IPv4
 2:
```

5.5.2. Codecs for IP Network Region 7 (calls to/from BT)

This IP codec set will be used for BT calls. Repeat the steps in **Section 5.5.1** with the following changes:

On **Page 1**, provision the codecs in the order shown below, as preferred by BT:

```
change ip-codec-set 7                                          Page   1 of   2

                          IP MEDIA PARAMETERS
    Codec Set: 7

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711A           n          2        20
 2: G.711MU          n          2        20
 3: G.722-64K                   2        20
 4: G.729A           n          2        20
 5:


     Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
```

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

```
change ip-codec-set 7                                          Page   2 of   2

                          IP MEDIA PARAMETERS

                              Allow Direct-IP Multimedia? n



                                                    Redun-                    Packet
                    Mode                            dancy
Size(ms)
FAX                 t.38-standard                   0    ECM: y
Modem               off                             0
TDD/TTY             US                              3
H.323 Clear-channel n                               0
SIP 64K Data        n                               0                         20


Media Connection IP Address Type Preferences
 1: IPv4
 2:
```

5.6. IP Network Regions

Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G430 Media Gateway and Avaya Media Server are in region 1. To provide testing flexibility, network region 7 was associated with other components used specifically for the BT testing.

5.6.1. IP Network Region 1 – Local CPE Region

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

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

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

On **page 4** of the form:

- Verify that next to region **1** in the **dst rgn** column, the codec set is **1**.
- Next to region **7** in the **dst rgn** column, enter **7** for the codec set (this means region 1 is permitted to talk to region 7 and it will use codec set 7 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      S M
                                                                     G  A   y t
 dst codec direct   WAN-BW-limits   Video      Intervening       Dyn A  G   n c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions           CAC R  L   c e
 1    1                                                                all
 2    2     y    NoLimit                                             n      y t
 3
 4
 5    5     y    NoLimit                                             n      y t
 6    6     y    NoLimit                                             n      y t
 7    7     y    NoLimit                                             n      y t
```

5.6.2. IP Network Region 7 – BT Trunk Region

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

On **Page 1** of the form:

- Enter a descriptive name (e.g., **BT**).
- Enter **7** for the **Codec Set** parameter.

```
change ip-network-region 7                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1        Authoritative Domain: avayalab.com
    Name: BT                      Stub Network Region: n
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
      Codec Set: 7                Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 4** of the form:

- Set codec set **7** for **dst rgn 1**.
- Note that **dst rgn 7** is pre-populated with codec set **7** (from page 1 provisioning).

```
change ip-network-region 7                                    Page   4 of  20

 Source Region: 7     Inter Network Region Connection Management     I     S M
                                                                     G  A  y t
 dst codec direct   WAN-BW-limits   Video      Intervening       Dyn A  G  n c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions           CAC R  L  c e
 1    7     y    NoLimit                                             n     y t
 2
 3
 4
 5
 6
 7    7                                                                 all
 8
```

5.7. 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 BT access – SIP Trunk 7. This trunk will use TLS port 5067.
- 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 BT Wholesale SIP Trunking service.

5.7.1. SIP Trunk for Inbound/Outbound BT calls

This section describes the steps for administering the SIP trunk to Session Manager used for the BT SIP Trunking service calls. Trunk Group 7 is defined. This trunk corresponds to the **CM-TG7** SIP Entity defined later in **Section 6.5.2**.

5.7.1.1 Signaling Group 7

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

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **Peer Detection Enabled?** is set to **y**. The system will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.4** (e.g., **SM**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5067**.
- **Far-end Network Region** – Set the IP network region to **7**, as set in **Section 5.6.2**.
- **Far-end Domain** – Enter **avayalab.com**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized directly to the associated stations, to reduce the use of media resources on the Avaya Media Gateway when possible (known as shuffling).
- **Initial IP-IP Direct Media** is set to the default value **n**.
- **H.323 Station Outgoing Direct Media** is set to the default value **n**.

```
change signaling-group 7                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                 Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM                    Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: SM
 Near-end Listen Port: 5067                Far-end Listen Port: 5067
                                        Far-end Network Region: 7

Far-end Domain: avayalab.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

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

5.7.1.2 Trunk Group 7

Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **7**). On **Page 1** of the **trunk-group** form, provision the following:

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **BT**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., ***07**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **Section 5.7.1.1** (e.g., **7**).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **10**).

```
add trunk-group 1                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 7                   Group Type: sip          CDR Reports: y
  Group Name: BT        T                COR: 1        TN: 1        TAC: *07
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk         Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 7
                                                     Number of Members: 10
```

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

- Set the **Preferred Minimum Session Refresh Interval (sec):** to **450**. This entry will actually cause a value of 900 to be generated in the SIP Session-Expires header pertaining to active call session refresh. See **Section 2.2**.

```
add trunk-group 7                                               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): 450

 Disconnect Supervision - In? y  Out? y

             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n

Caller ID for Service Link Call to H.323 1xC: station-extension
```

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

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

```
add trunk-group 7                                               Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                    Maintenance Tests? y

   Suppress # Outpulsing? n  Numbering Format: public
                                              UUI Treatment: service-provider

                                               Replace Restricted Numbers? n
                                              Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y
```

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

- Set **Network Call Redirection** to **y**.
- Verify that **Send Diversion Header** is set to **y**.
- Set **Support Request History** to **n**.
- Set **Telephone Event Payload Type** to the RTP payload type used by BT (e.g., **101**).

```
add trunk-group 7                                                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? n
                              Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
     Resend Display UPDATE Once on Receipt of 481 Response? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
          Enable Q-SIP? n
          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                      Request URI Contents: may-have-extra-digits
```

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

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

5.7.2.1 Signaling Group 3

Repeat the steps in **Section 5.7.1.1** with the following changes:

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

5.7.2.2 Trunk Group 3

Repeat the steps in **Section 5.7.1.2** with the following changes:

- 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 5.7.2.1** (e.g., **3**).
- On **Page 3** of the **Trunk Group** form;
  - Set **Numbering Format** to **private**.
- On **Page 4** of the **Trunk Group** form:
  - Set **Network Call Redirection** to **n**.
  - Set **Send Diversion Header** to **n**.
  - Verify **Identity for Calling Party Display** is set to **P-Asserted-Identity** (default).

Use default values for all other settings.

5.8. Public Numbering

The calling party information is sent in the SIP "From", "Contact" and "PAI" headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, three DID numbers are assigned by the service provider for testing. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions.

Note: On the sample screen below, note that since these entries apply to a SIP connection to Session Manager (Trunk Group 7), the resulting number must be complete E.164 number. Communication Manager automatically will insert a "+" in front of the user number in the From, P-Asserted-Identity, Contact and Diversion headers. Since BT does not accept this "+" sign in the origination headers, it was later removed by means of an Adaptation in Session Manager (**Section 6.4.2**) and a SigMa script on the Avaya SBCE (**Section 7.7**).

```
change public-unknown-numbering 5                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                              Total
Ext Ext               Trk       CPN            CPN
Len Code              Grp(s)    Prefix         Len
                                                  Total Administered: 53
 5  50231             7         441986303315     12    Maximum Entries: 240
 5  50232             7         441986303316     12
 5  50238             7         441986303317     12 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.

                                                  Communication Manager
                                                  automatically inserts
                                                  a '+' digit in this case.
```

5.9. Private Numbering

In the reference configuration, the private-numbering form, (used in conjunction with the **Numbering Format: private** setting in **Section 5.7.2.2**), is used to send Communication Manager local extension numbers to Session Manager, for inclusion in any SIP headers directed to SIP endpoints and Messaging.

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

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

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext                  Trk        Private           Total
Len Code                 Grp(s)     Prefix            Len
 5  1                    11                           5  Total Administered: 11
 5  5                    3                            5     Maximum Entries: 540
 5  14                   3                            5
 5  20                   3                            5
```

5.10. Route Patterns

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

5.10.1. Route Pattern for Calls to BT

This form defines the public SIP trunk, based on the route-pattern selected by the ARS table later in **Section 5.11**. 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 7 is used for calls to the PSTN test numbers provided by BT in the testing environment..

Enter the **change route-pattern 7** command to configure the parameters for the service provider trunk route pattern, and enter the following:

- In the **Grp No** column, enter **7** for public trunk 7, and the **FRL** column enter **0** (zero).
- Under **Numbering Format** enter **pub-unk**.

```
change route-pattern 7                                          Page   1 of   4
                    Pattern Number: 7      Pattern Name: To BT
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 7    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

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

5.10.2. 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 5.12** (e.g., calls to Avaya SIP telephone extensions or Messaging).

Step 1 - Repeat the steps in **Section 5.10.1** 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 **Numbering Format** column, across from line **1:** enter **lev0-pvt**.

```
change route-pattern 3                                          Page   1 of   3
                    Pattern Number: 3      Pattern Name: ToSM Enterprise
    SCCAN? n    Secure SIP? n     Used for SIP stations? y
    Primary SM: SM              Secondary SM:
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 3    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format
1: y y y y y n  n            rest                              lev0-pvt  none
```

5.11. 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 5.10**).

Enter the **change ars analysis 019** command and enter the following:

- In the **Dialed String** column enter a matching dial pattern (e.g., **019**). These digits matched the prefix of the BT provided PSTN test numbers (019xxxxxxxx).
- 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., **7**).
- In the **Call Type** column enter **pubu** (selections other than **pubu** may be appropriate, based on the digits defined here).

Repeat these steps for all other outbound call strings as needed.

```
change ars analysis 019                                          Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 1

          Dialed            Total     Route    Call   Node   ANI
          String           Min  Max  Pattern   Type   Num    Reqd
    019                    11   11    7        pubu          n
    101xxxx0               8    8     deny     op            n
    101xxxx0               18   18    deny     op            n
    101xxxx01              16   24    deny     iop           n
    101xxxx011             17   25    deny     intl          n
    101xxxx1               18   18    deny     fnpa          n
    10xxx0                 6    6     deny     op            n
```

5.12. Automatic Alternate Routing (AAR) Dialing

AAR is used for outbound Communication Manager calls within the CPE.

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

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

Repeat these steps and create an entry for Messaging access extension (not shown).

```
change aar analysis 0                                            Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 1

          Dialed            Total     Route    Call   Node   ANI
          String           Min  Max  Pattern   Type   Num    Reqd
    50                     5    5     3        lev0          n
```

5.13. 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 [**8**] on the Additional References section.

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)#***).

- Enter the **show system** command and copy down the G430 serial number.
- Enter the **set mgc list x.x.x.x** command where x.x.x.x is the IP address of the Communication Manager Procr (e.g., **10.64.91.87**, see **Section 5.4**).
- Enter the **copy run start** command to save the G430 configuration.

From the Communication Manager SAT, enter **add media-gateway x** where x is an available Media Gateway identifier (e.g. **1**). On the Media Gateway form, enter the following parameters:

- **Type** = **g430**.
- **Name** = a descriptive name (e.g., **G430-1**).
- **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)#***).

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

```
display media-gateway 1                                         Page   1 of   2
                             MEDIA GATEWAY 1

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

5.14. 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 the Media Server documentation in the **Additional References** section for additional information.

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).

On the Media Server Element Manager, navigate to **Home → System Configuration → Signaling Protocols → SIP →Node and Routes** and add the Communication Manager Procr interface IP address (e.g., **10.64.91.87**, see **Section 5.4**) as a trusted node (not shown).

On Communication Manager, enter the **add signaling-group x** command where x is an unused signaling group (e.g., **80**), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**
- Verify that **Peer Detection Enabled?** – Set to **n**.
- **Peer Server** to **AMS**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of Media Server as administered in **Section 5.4** (e.g., **AMS10**).
- **Near-end Listen Port** and **Far-end Listen Port** – The default ports **9061** and **5061** are used. These ports may be changed to other values if desired.
- **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: AMS10
 Near-end Listen Port: 9061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: 10.64.91.88
```

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

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

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

                    Media Server ID: 1

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

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

5.15. Save Translations

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

6. Configure Avaya Aura® Session Manager

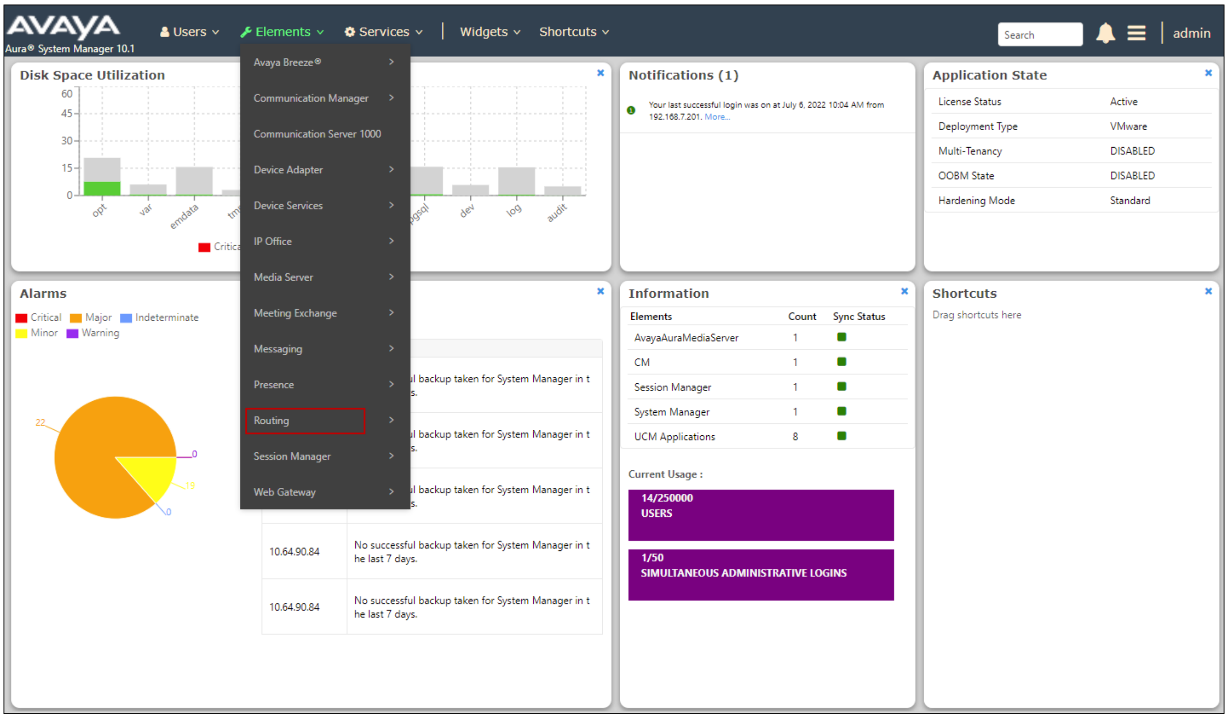
This section provides the procedures for configuring Session Manager to process inbound and outbound calls between Communication Manager and the Avaya SBCE. In the reference configuration, all Session Manager provisioning is performed via System Manager.

- Define a SIP Domain.
- Define Locations containing the 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 and the Avaya SBCE.
- Define Entity Links describing the SIP trunks between Session Manager and Communication Manager, as well as the SIP trunks between the Session Manager and the Avaya SBCE.
- Define Routing Policies associated with the Communication Manager and the Avaya SBCE.
- Define Dial Patterns, which govern which Routing Policy will be selected for inbound and outbound call routing.
- Verify TLS Certificates.

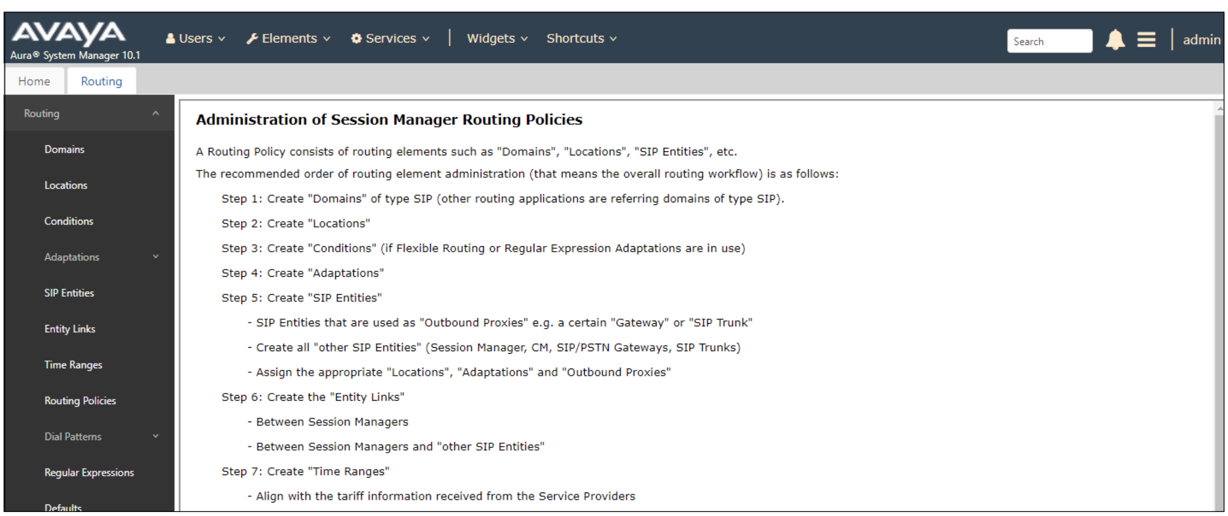
Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult **[1]- [4]** in the **Additional References** section for further details.

6.1. System Manager Login and Navigation

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



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



6.2. SIP Domain

Select **Domains** from the left navigation menu. In the reference configuration, domain **avayalab.com** was defined. Click **New**. Enter the following values and use default values for remaining fields.

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

Click **Commit** (not shown) to save.

6.3. Locations

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

- **Main** – The customer site containing System Manager, Session Manager, Messaging and local SIP endpoints.
- **CM-TG7** – Communication Manager trunk group 7 designated for BT.
- **SBCs** – Avaya SBCE.

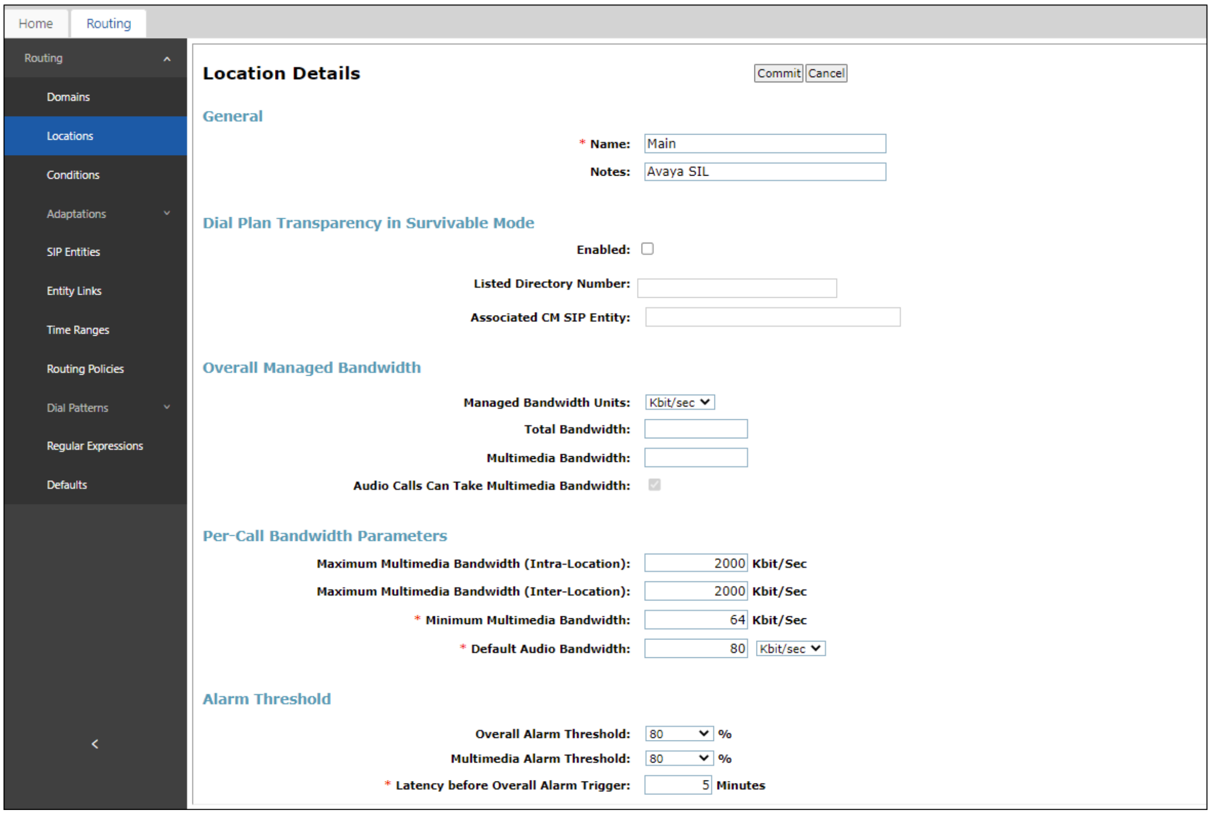
6.3.1. Main Location

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.

In the **Location Pattern** section, click **Add** and enter the following values (not shown).

- **IP Address Pattern:** Leave blank.
- **Notes:** Add a brief description.
- Click **Commit** to save.



6.3.2. CM-TG7 Location

To configure the Communication Manager Trunk Group 7 Location, repeat the steps in **Section 6.3.1** with the following changes (not shown):

- **Name** – Enter a descriptive name (e.g., **CM-TG7**).

6.3.3. SBCs Location

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

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

6.4. Configure Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers between Communication manager and the service provider.

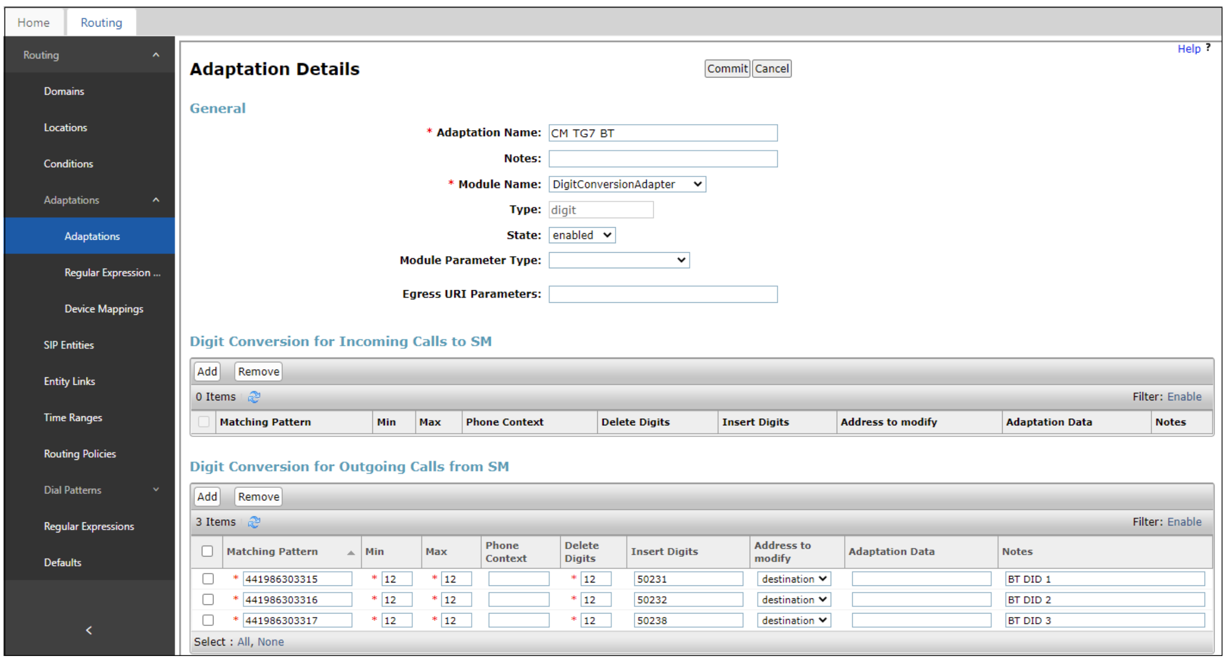
6.4.1. Adaptation for Avaya Aura® Communication Manager

The Adaptation administered in this section is used to replace the BT DID number digit string on the inbound Request URI with the associated Communication Manager extension/VDN, before being sent out to the Communication Manager SIP trunk.

In the **left** pane under **Routing**, click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown).

In the **Adaptation Details** page, enter:

- A descriptive **Name**, (e.g., **CM TG7 BT**).
- Select **DigitConversionAdapter** from the **Module Name** drop down.



On the **Digit Conversion for Outgoing Calls from SM** section, click **Add**.

Note – In the reference configuration, BT delivered 12 digit DID numbers on inbound calls, starting with digits 44.

In the example**, 441986303315** is a DNIS string sent in the Request URI by the BT SIP Trunking service, that is associated with Communication Manager extension **50231**.

- Enter **441986303315** in the **Matching Pattern** column.
- Enter **12** in the **Min/Max** columns.
- Enter **12** in the **Delete Digits** column.
- Enter **50231** in the **Insert Digits** column.
- Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
- Enter any desired notes.

Repeat these steps for all additional BT DID numbers/Communication Manager extensions. Click on **Commit** when done.

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

6.4.2. Adaptation for the BT SIP Trunking service

The Adaptation administered in this section is used to:

1. Remove Avaya proprietary SIP headers not required by BT on outbound messages.
2. Modify the default Session Manager behavior when generating the P-Asserted-Identity (PAI) header in a request or response, if the header is not present on ingress, by use of the "Orange Adapter" module. See **Section 2.2**.
3. Remove the "+" sign in the origination headers of outbound messages. See **Section 2.2**.

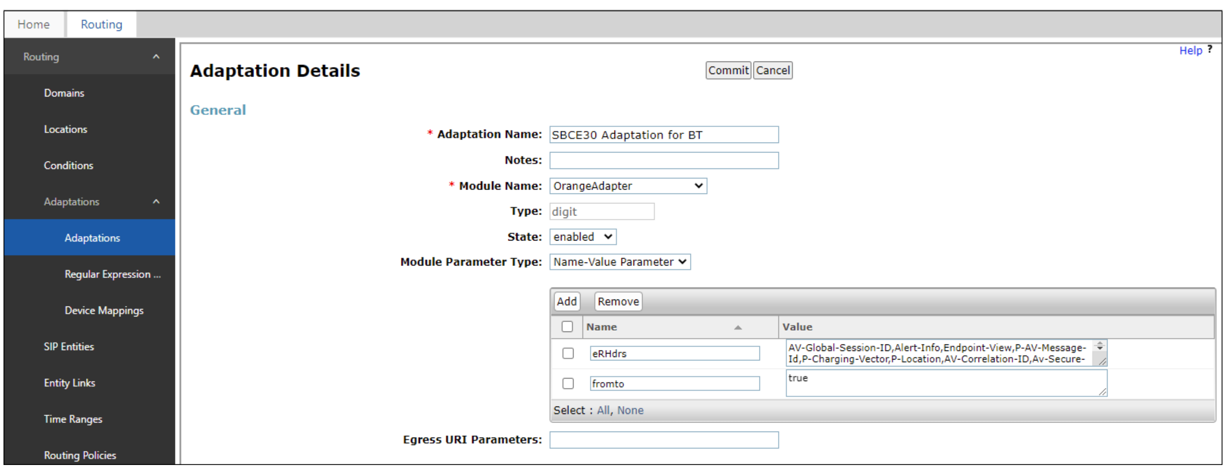
Repeat the steps in **Section 6.4.1** with the following changes.

In the **Adaptation Details** page, enter:

- A descriptive **Name**, (e.g., **SBC30 Adaptation for BT**).
- Select **OrangeAdapter** from the **Module Name** drop down menu.
- In the **Module Parameter Type**: field select **Name-Value Parameter** from the menu.

Click **Add** to add the name and value parameters.

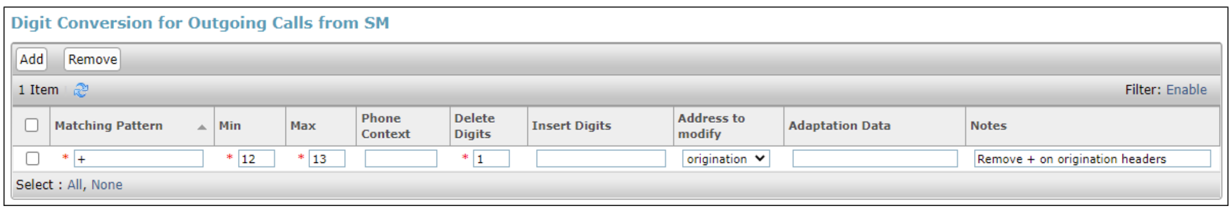
- **Name**: Enter **eRHdrs**. This parameter will remove the specified headers from messages in the egress direction.
    - **Value**: Enter **AV-Global-Session-ID,Alert-Info,Endpoint-View,P-AV-Message-Id,P-Charging-Vector,P-Location,AV-Correlation-ID,Av-Secure-Indication**
- **Name**: "**fromto**". This adapts the From and To headers along with the Request-Line and PAI headers.
    - **Value**: "**true**"



As described in **Section 2.2**, the “+” from the E.164 numbers used by Communication Manager in the origination headers (e.g., From and P-Asserted Identity headers) needs to be removed before the messages are being sent out to BT.

Scroll down to the **Digit Conversion for Outgoing Calls from SM** section and click **Add**..

- Enter **+** in the **Matching Pattern** column.
- Enter **12** in the **Min** column.
- Enter **13** in the **Max** column.
- Enter **1** in the **Delete Digits** column.
- Specify that this should be applied to the SIP **origination** headers in the **Address to modify** column.
- Enter any desired notes



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 BT trunk access (**Section 6.5.2**) – This entity, and its associated Entity Link (using TLS with port 5067), is for calls to/from BT 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 BT SIP Trunking service via the Avaya SBCE.

Note – In the reference configuration, TLS is used as the transport protocol between Session Manager and Communication Manager (ports 5061 and 5067), and to the Avaya SBCE (port 5061). The connection between the Avaya SBCE and the BT Wholesale SIP Trunking service uses UDP ports 5060 per BT requirements.

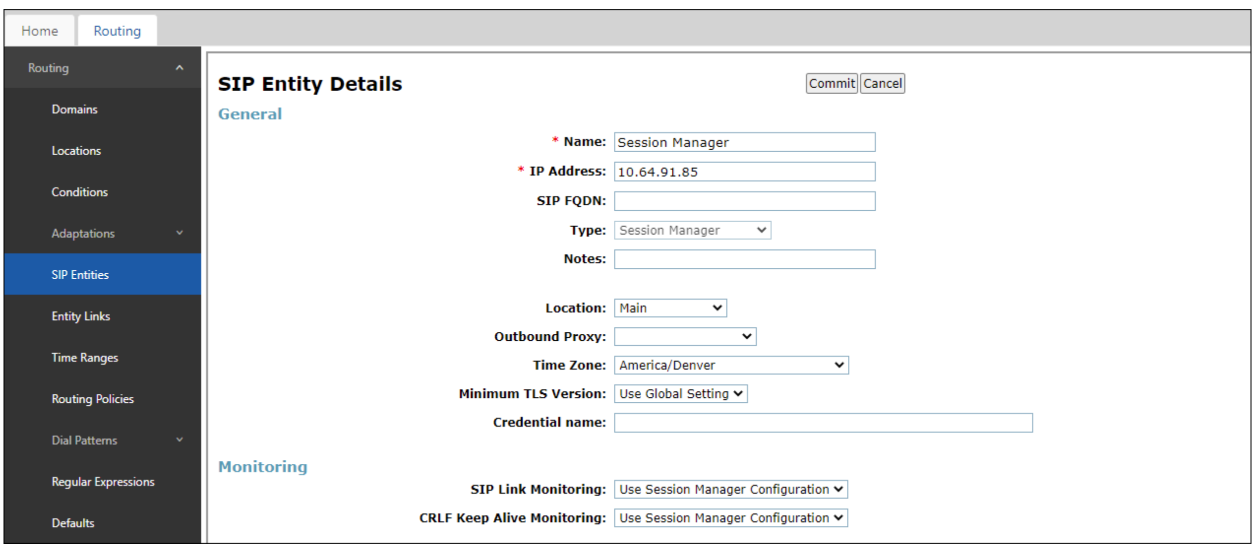
6.5.1. Avaya Aura® Session Manager SIP Entity

In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page click on **New** (not shown). In the **General** section of the **SIP Entity Details** page, provision the following:

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

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

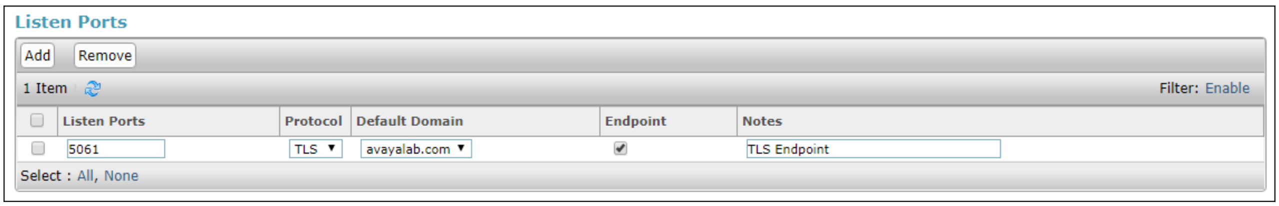
- Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
- Use the default values for the remaining parameters.



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**).

Enter any notes as desired and leave all other fields on the page blank/default. Click on **Commit**.

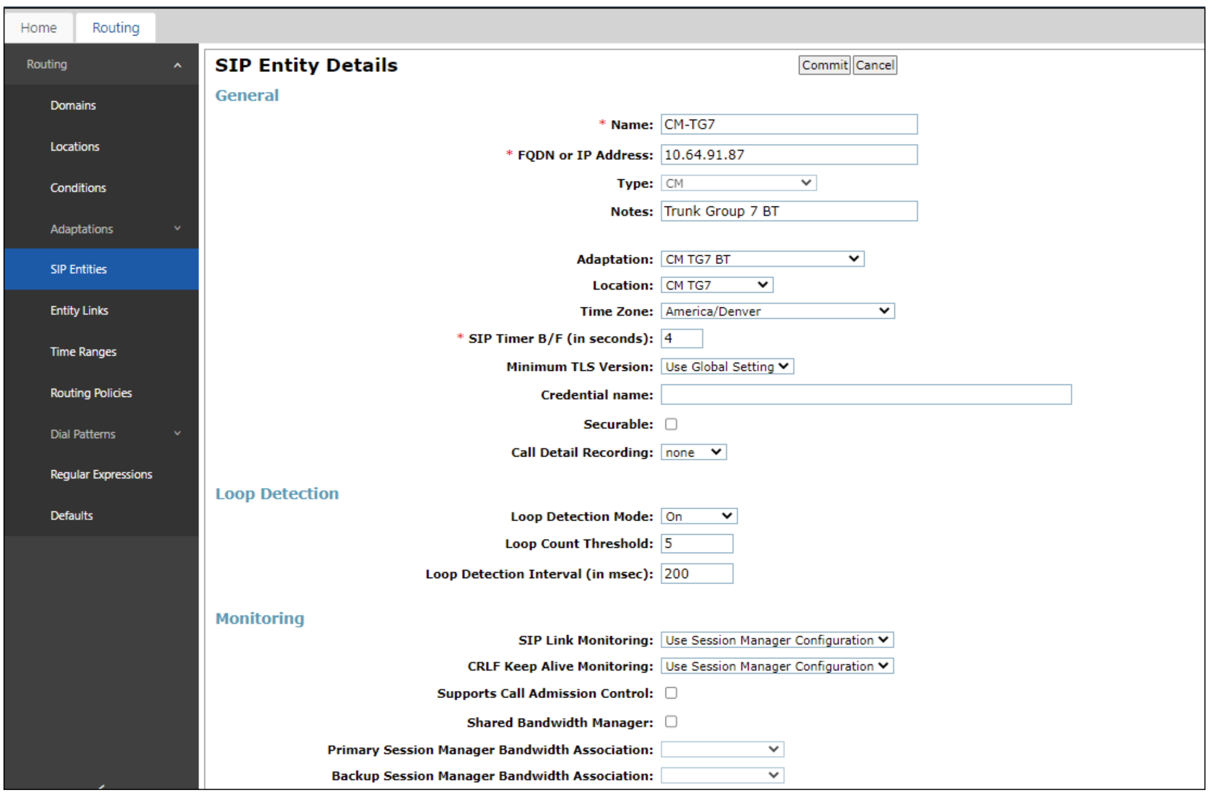


Note – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 6.6**. The **SIP Responses to an OPTIONS Request** section of the form is not used in the reference configuration.

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

In the **SIP Entities** page, click on **New** (not shown). In the **General** section of the **SIP Entity Details** page, provision the following:

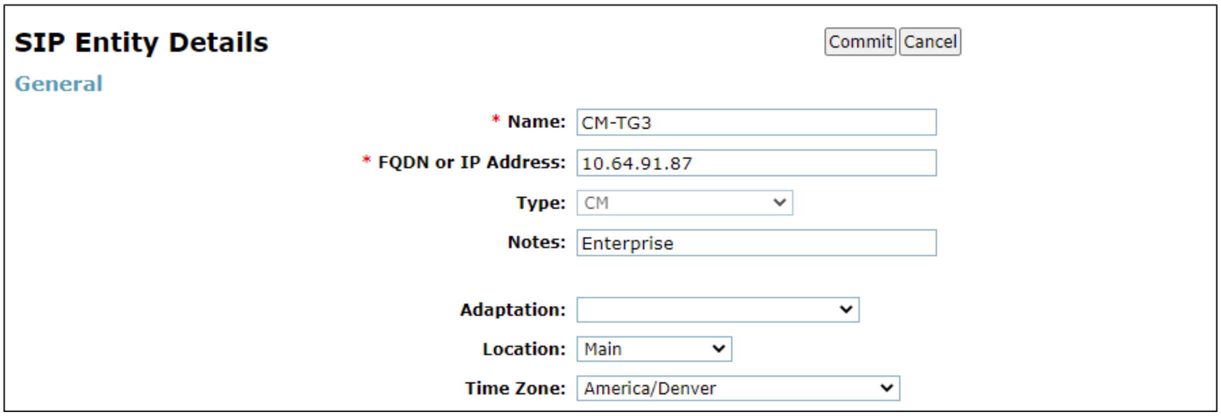
- **Name** – Enter a descriptive name (e.g., **CM-TG7**).
- **FQDN or IP Address –** Enter the IP address of Communication Manager Processor Ethernet (procr) shown in **Section 5.4** (e.g., **10.64.91.87**).
- **Type –** Select **CM**.
- **Adaptation –** Select the Adaptation **CM TG7 BT** administered in **Section 6.4.1**.
- **Location** – Select the Location **CM TG7** 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.
- Click on **Commit**.



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:

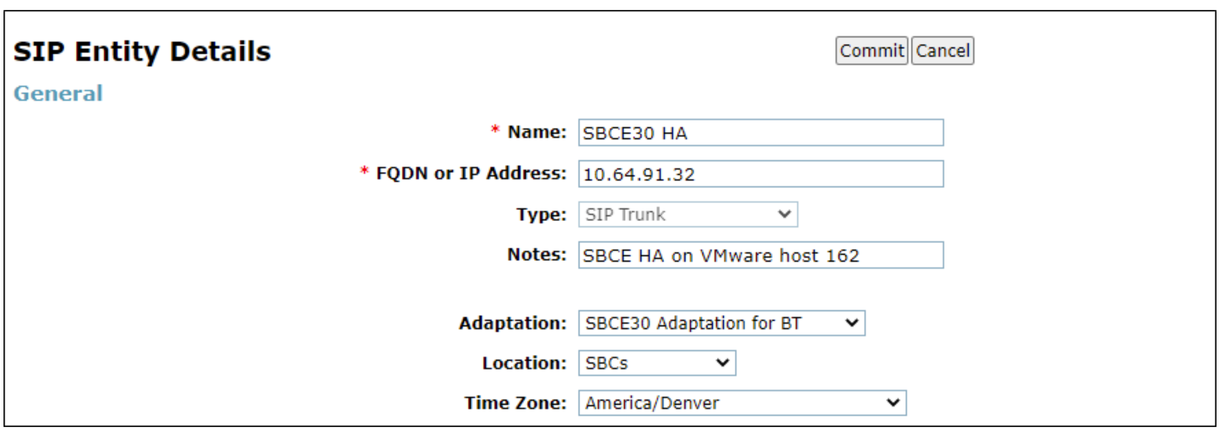
- **Name** – Enter a descriptive name (e.g., **CM-TG3**).
- **Adaptations** – Leave this field blank.
- **Location** – Select location **Main** (**Section 6.3.1**).



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., **SBC30 HA**).
- **FQDN or IP Address –** Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.64.91.32**, see **Section 7.5**).
- **Type –** Select **SIP Trunk**.
- **Adaptations –** Select Adaptation **SBC30 Adaptation for BT** (**Section 0**).
- **Location –** Select Location **SBCs** administered in **Section 6.3.3**.



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**).

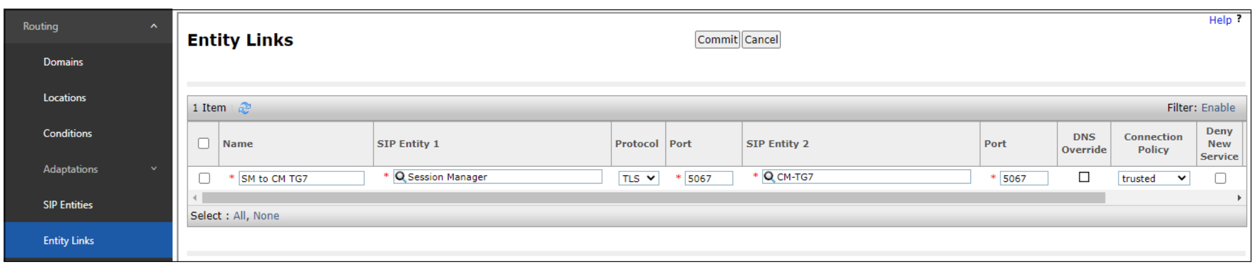
Note – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages configured in **Section 6.5**.

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

In the left pane under **Routing**, click on **Entity Links**, then click on **New** (not shown). Continuing in the **Entity Links** page, provision the following:

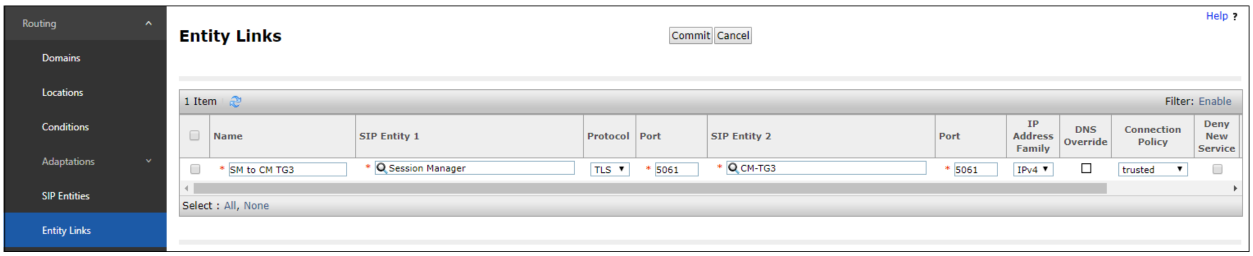
- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **SM to CM TG7**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 6.5.1** for Session Manager (e.g., **Session Manager**).
- **Protocol** – Select **TLS** (see **Section 5.7.1**).
- SIP Entity 1 **Port** – Enter **5067**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.2** for the Communication Manager public entity (e.g., **CM-TG7**).
- SIP Entity 2 **Port** – Enter **5067** (see **Section 5.7.1**).
- **Connection Policy** – Select **trusted**.
- Leave other fields as default.
- Click on **Commit**.



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:

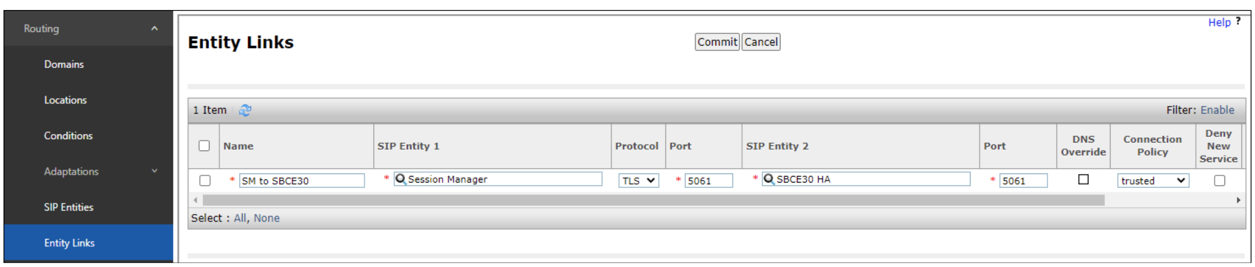
- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **SM to CM TG3**).
- SIP Entity 1 **Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.3** for the Communication Manager local entity (e.g., **CM-TG3**).
- SIP Entity 2 **Port** – Enter **5061** (see **Section 5.7.2**).



6.6.3. Entity Link for the BT SIP Trunking service via the Avaya SBCE

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

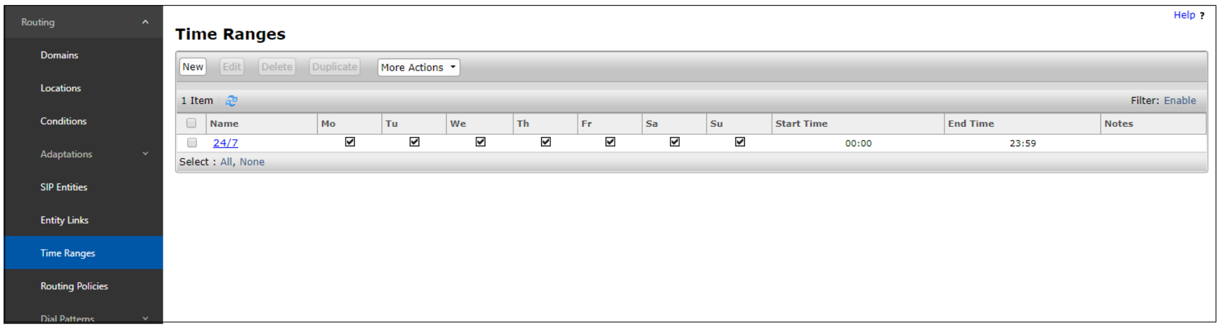
- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **SM to SBC30**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.4** for the Avaya SBCE entity (e.g., **SBC30 HA**).
- **SIP Entity 2 Port** – Enter **5061**.



6.7. Time Ranges

In the left pane under **Routing**, click on **Time Ranges**. In the **Time Ranges** page click on **New**. 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**. Click on **Commit** (not shown).

Repeat these steps to provision additional time ranges as required.



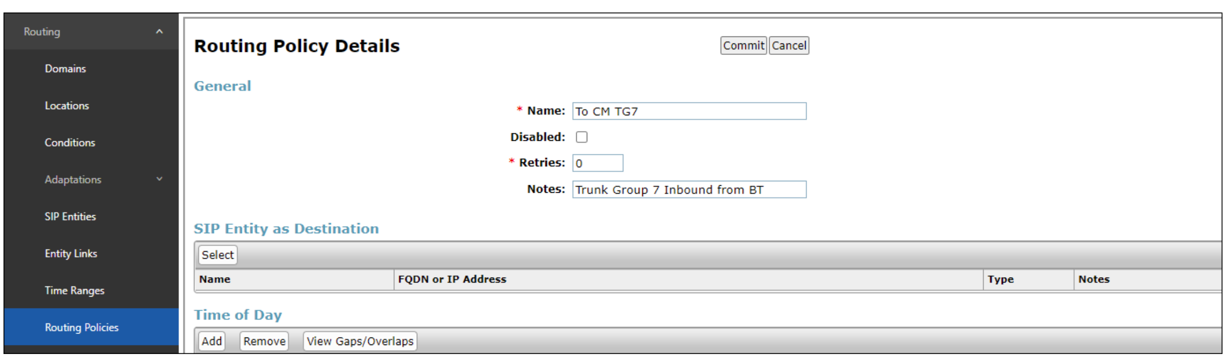
6.8. Routing Policies

In this section, the following Routing Policies are administered:

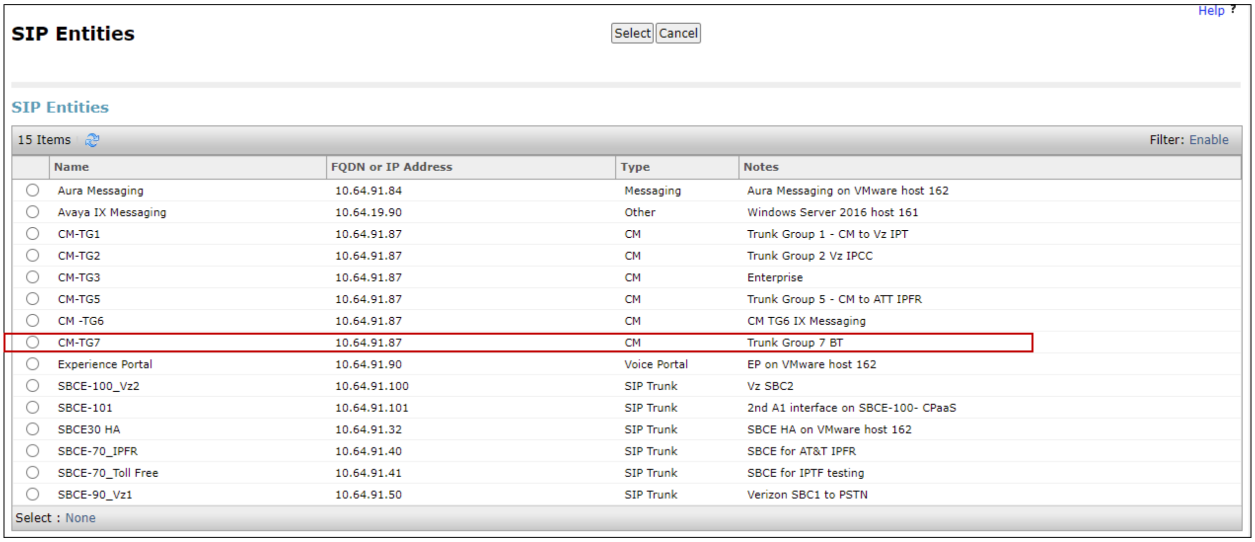
- Inbound calls to Communication Manager extensions (**Section 6.8.1**).
- Outbound calls to BT/PSTN (**Section 6.8.22**).

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

This Routing Policy is used for inbound calls from BT. In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown). In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing inbound BT calls to Communication Manager (e.g., **To CM TG7**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the **SIP Entities** list page will open.



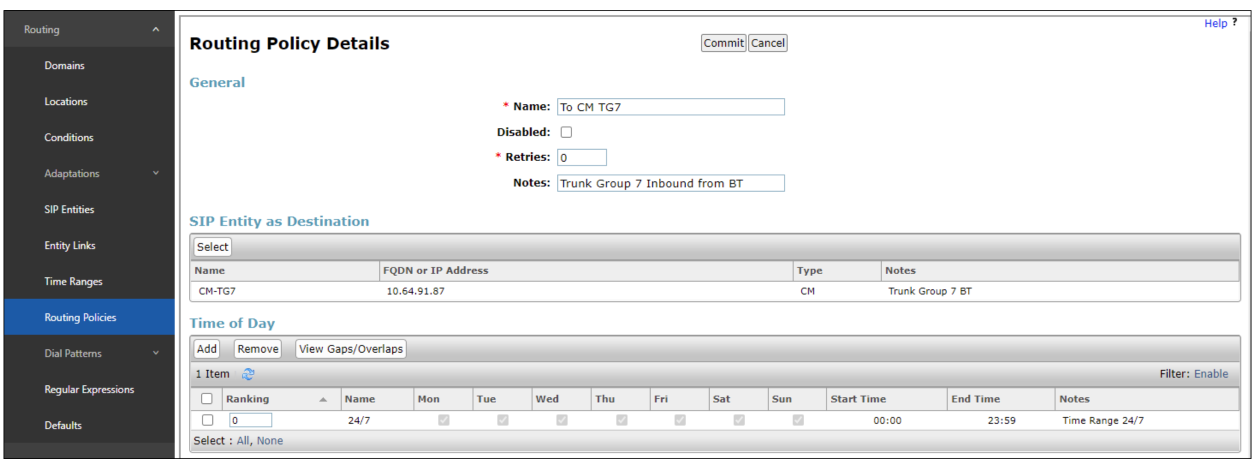
In the **SIP Entities** list page, select the SIP Entity administered in **Section 6.5.2** for the Communication Manager public SIP Entity (**CM-TG7**), and click on **Select**.



Returning to the **Routing Policy Details** page in the **Time of Day** section, click on **Add**. In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 6.7**, and click on **Select**. Returning to the **Routing Policy Details** page in the **Time of Day** section, enter a **Ranking** of **0**, and click on **Commit**.

No **Regular Expressions** were used in the reference configuration.

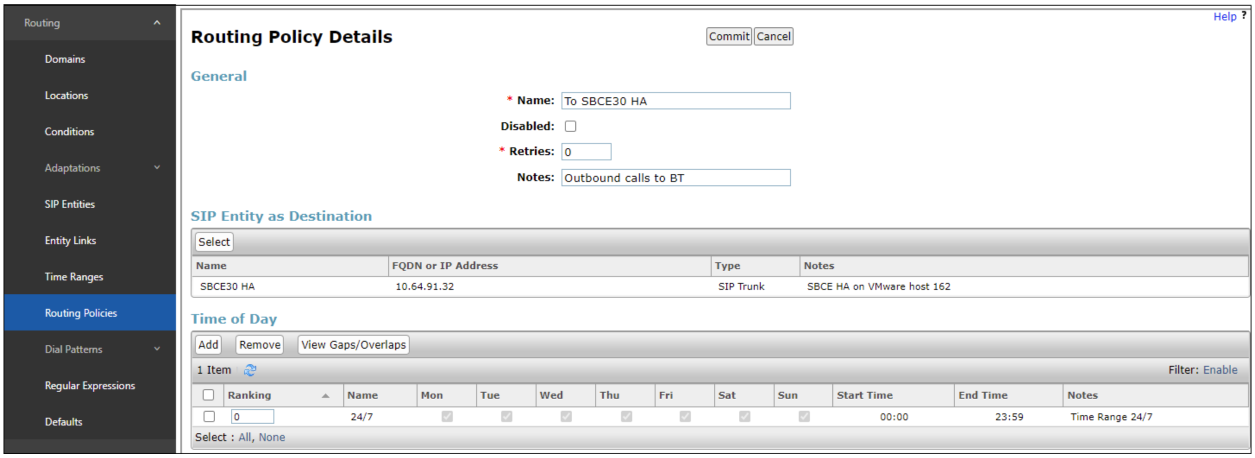
Note – Once the **Dial Patterns** are defined (**Section 6.9**) they will appear in the **Dial Pattern** section of this form.



6.8.2. Routing Policy for Outbound Calls to BT

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

- Enter a descriptive **Name** (e.g., **To SBC30 HA**).
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 6.5.4** for the Avaya SBCE SIP Entity (e.g., **SBC30 HA**).



6.9. Dial Patterns

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

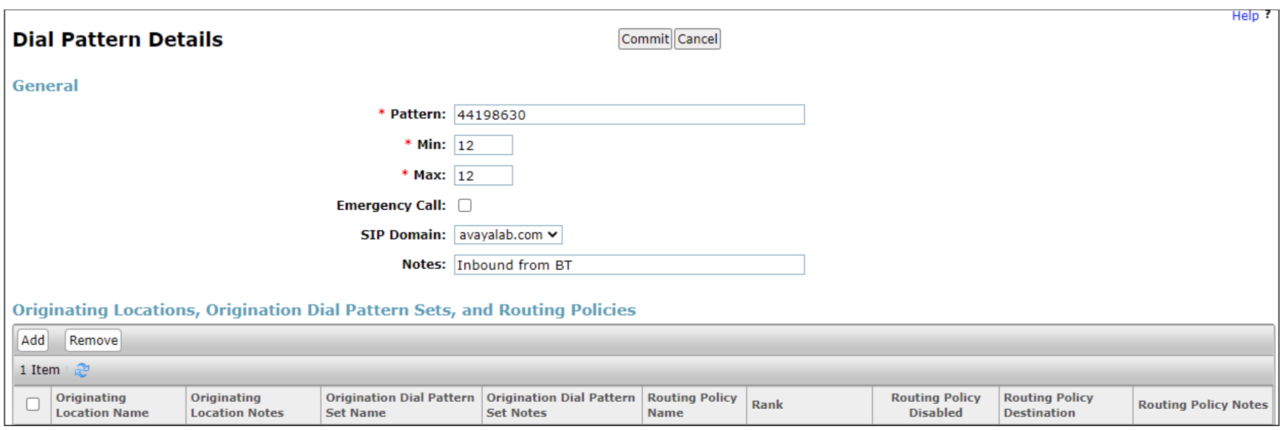
- Inbound PSTN calls via BT SIP Trunking service to Communication Manager (**Section 6.9.1**).
- Outbound calls to BT/PSTN (**Section 6.9.2**).

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

In the reference configuration, BT sent 12 digit DID numbers starting with 44198630 in the SIP Request URI of inbound calls. The DID pattern must be matched for further call processing.

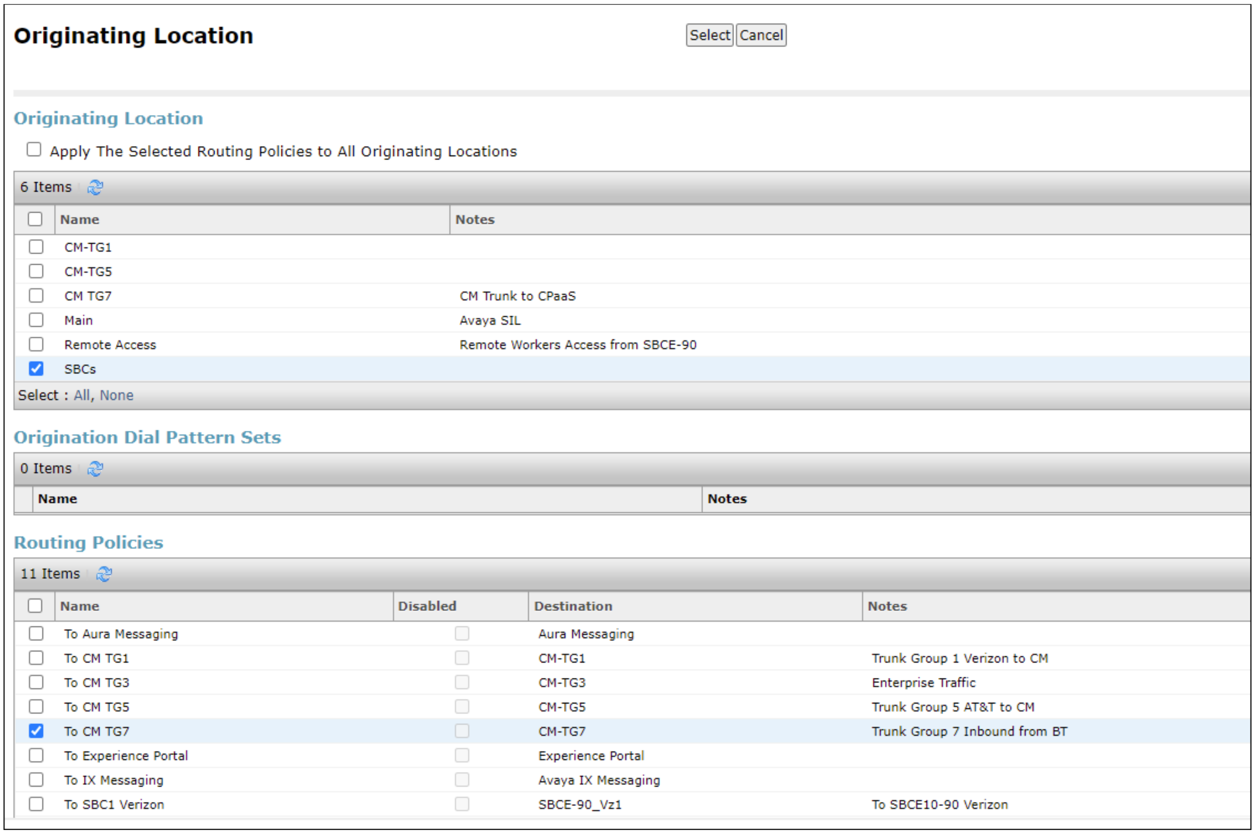
In the left pane under **Routing**, click on **Dial Patterns**. In the **Dial Patterns** page click on **New** (not shown). In the **General** section of the **Dial Pattern Details** page, provision the following:

- **Pattern** – Enter **44198630**. Note – The Adaptation defined for Communication Manager in **Section 6.4.1** will convert the various 441986300xxx numbers into their corresponding Communication Manager extensions.
- **Min** and **Max** – Enter **12**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.



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

In the **Originating Location**, check the checkbox corresponding to the Avaya SBCE location, e.g., **SBCs**. 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 TG7**) and click on **Select**.



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

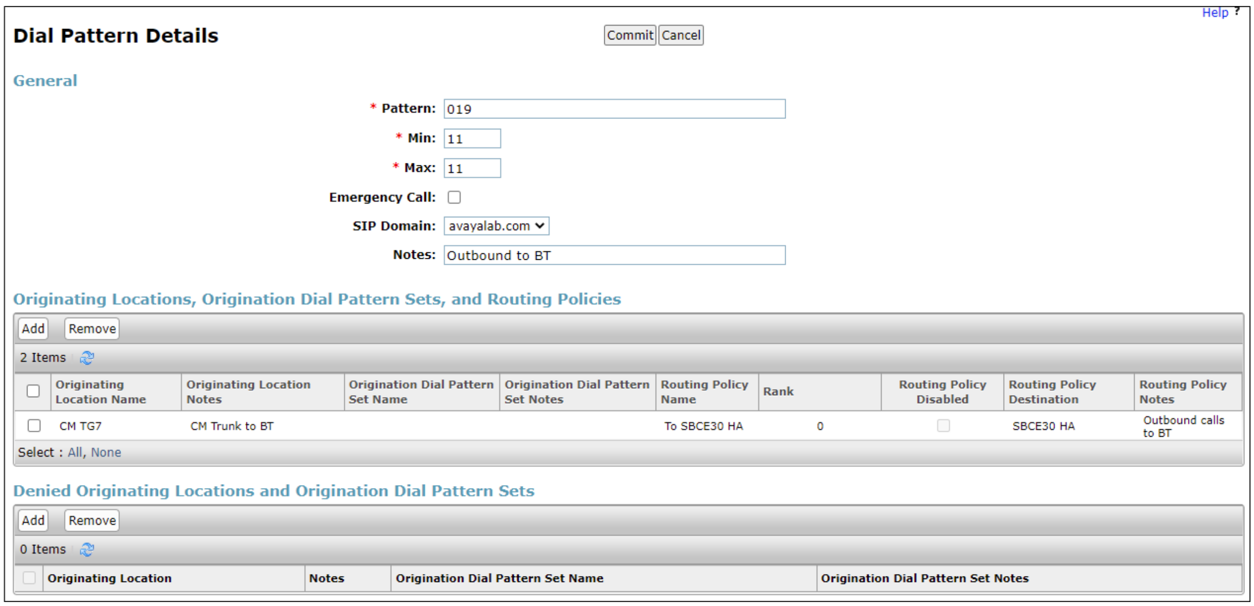
Repeat these steps for any additional inbound dial patterns from BT.

6.9.2. Matching Outbound Calls to BT/PSTN

In this section, Dial Patterns are administered for all outbound calls to BT/PSTN. In the reference configuration, BT required 11 digit numbers starting with 019 to be sent to their network.

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 BT/PSTN (e.g., **019**).
- Enter a **Min** and Max pattern of **11**.
- In the **Routing Policies** section of the **Originating Locations, Origination Dial Patterns and Routing Policies** page, check the checkboxes corresponding to the Communication Manager Originating Location (e.g., **CM-TG7**) and the Routing Policy administered for routing calls to BT in **Section 6.8.2** (e.g., **To SBC30 HA**).



Repeat these steps to add any additional outbound patterns as required.

7. Configure Avaya Session Border Controller for Enterprise

In the reference configuration, Avaya SBCE in High Availability mode is deployed as the edge device between the CPE and the BT Wholesale Hosted SIP Trunking Service..

Avaya SBCE HA pairs can be deployed in an enterprise in a parallel mode configuration. In the parallel configuration the signaling packets are routed only to the Active (primary) Avaya SBCE which performs all data processing: the interface ports on the stand-by Avaya SBCE do not process any traffic. The Management interfaces on the Avaya SBCE appliances have different IP addresses, but the signaling/media interfaces have the same IP address.

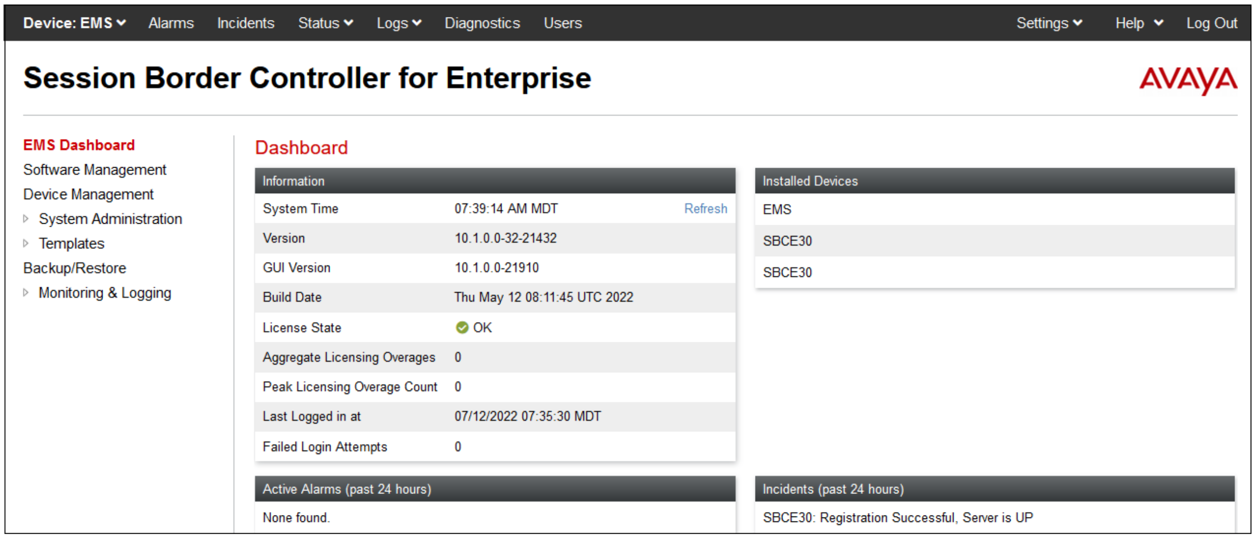
Note: The SBCE can only be deployed in HA mode if the HA feature is enabled on the license file. If the required feature is not enabled, contact an authorized Avaya sales representative.

It is assumed that the software installation and initial provisioning of the Avaya EMS and SBCE HA pair of servers, including the assignment of the management interfaces IP Addresses and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

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

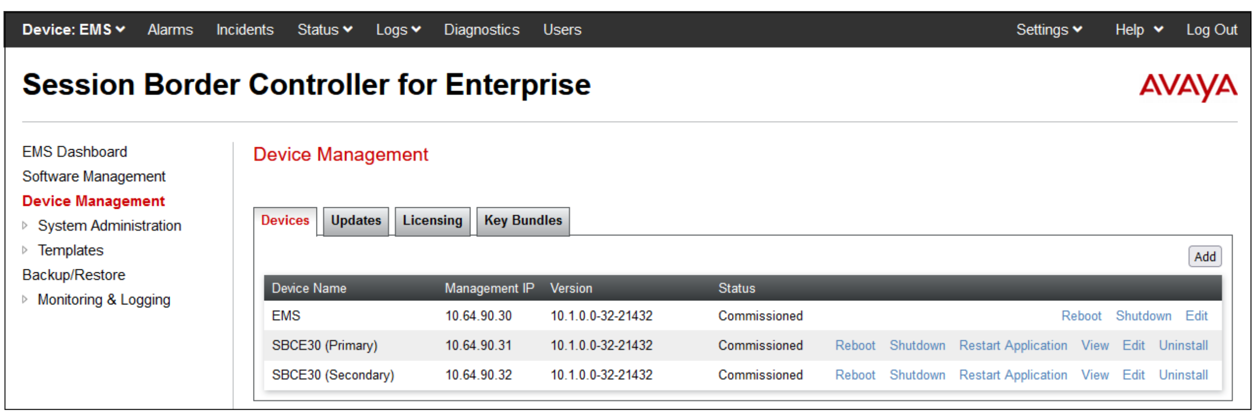
The EMS Dashboard page of the Avaya SBCE will appear. Note that the installed software version is displayed. Verify that the **License State** is **"OK"**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

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



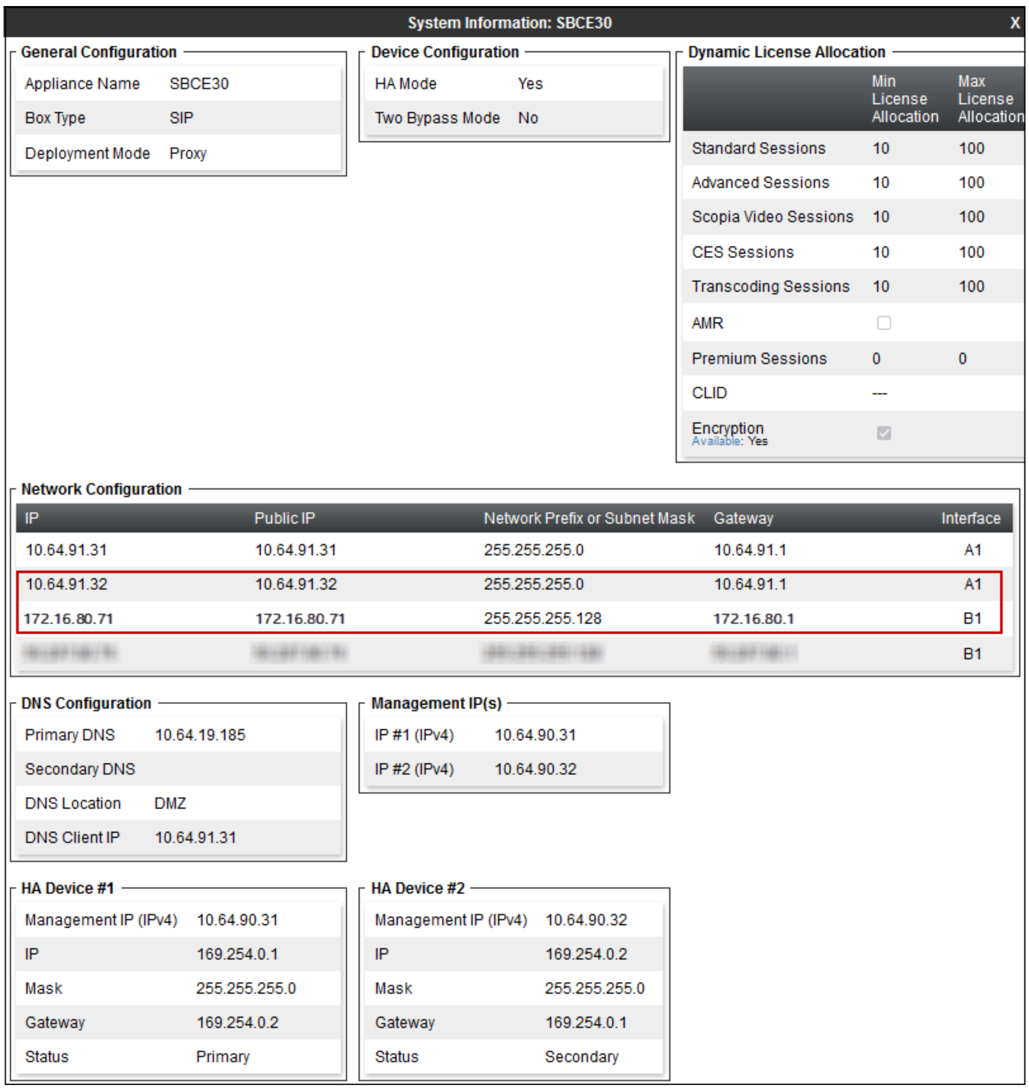
7.1. Device Management – Status

Select **Device Management** on the left-hand menu. A list of installed devices is shown on the **Devices** tab on the right pane. In the case of the sample configuration, this includes the **EMS** and the SBCE HA pair **SBCE30 (Primary)** and **SBCE30 (Secondary)**. To view the configuration of the SBCE devices, click **View** on the screen below.



The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information previously provided. On the **Device Configuration** area, **HA Mode** is set to **Yes**. Under **Network Configuration**, the highlighted interface **A1** is used to connect the SBCE to the internal enterprise private network. In the shared test environment, the highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to BT. Other IP addresses assigned to interfaces **A1** and **B1** on the screen below are used to support other solutions and are not the focus of these Application Notes. Note that the two SBCE HA appliances will share the same IP addresses for signaling and media on interfaces **A1** and **B1**.

At the bottom of the screen, the specific IP configuration for the two HA devices and current status is show. In the example, IP addresses **10.64.90.31** and **10.64.90.32** correspond to the Management Interface **M1** on each SBCE. IP addresses **169.254.0.1** and **169.254.0.2** are automatically assigned during installation, and correspond to interface **M2** on each SBCE, used for the layer 2 HA link between the two servers.



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

7.2. TLS Management

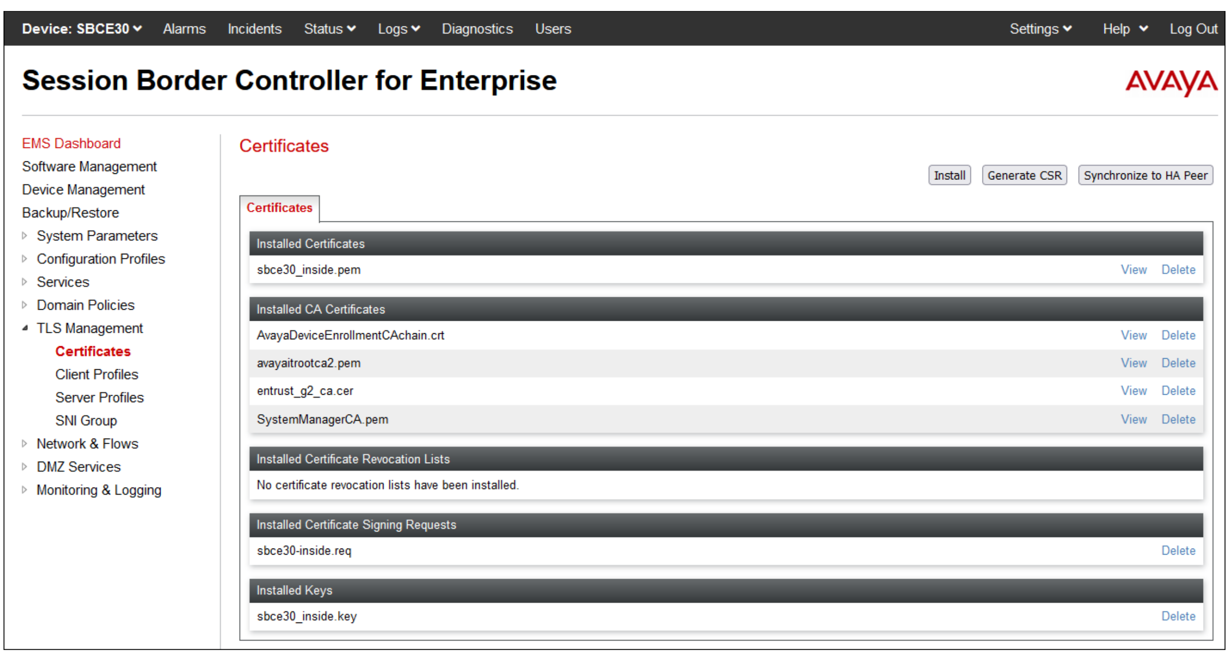
In the reference configuration, TLS transport is used for the communication between Session Manager and the Avaya SBCE. The following procedures show how to view the certificates and configure the profiles to support the TLS connection.

Note – Testing was done using identity certificates signed by a local certificate authority. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

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

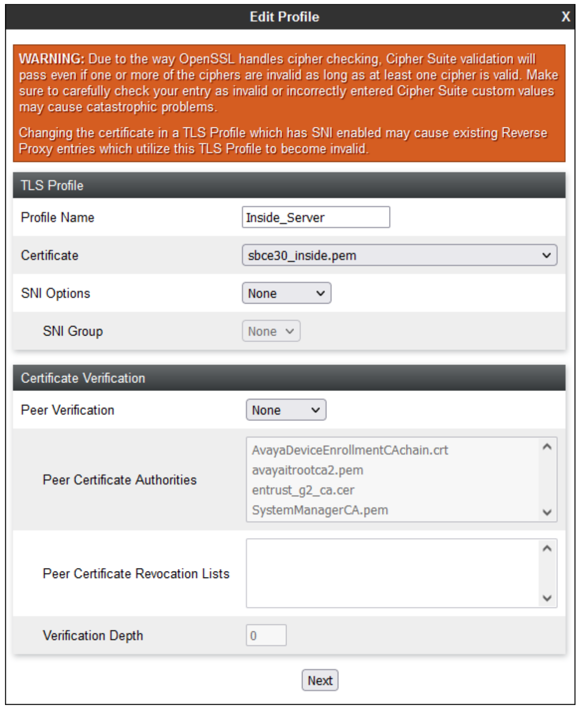
To access the SBCE configuration menus, select the SBCE device from the top navigation menu.

Select **TLS Management → Certificates** from the left-hand menu. Verify the root CA certificate is present in the **Installed CA Certificates** area. The signed identity certificate is present in the **Installed Certificates** area. The private key associated with the identity certificate is present in the **Installed Keys** area.

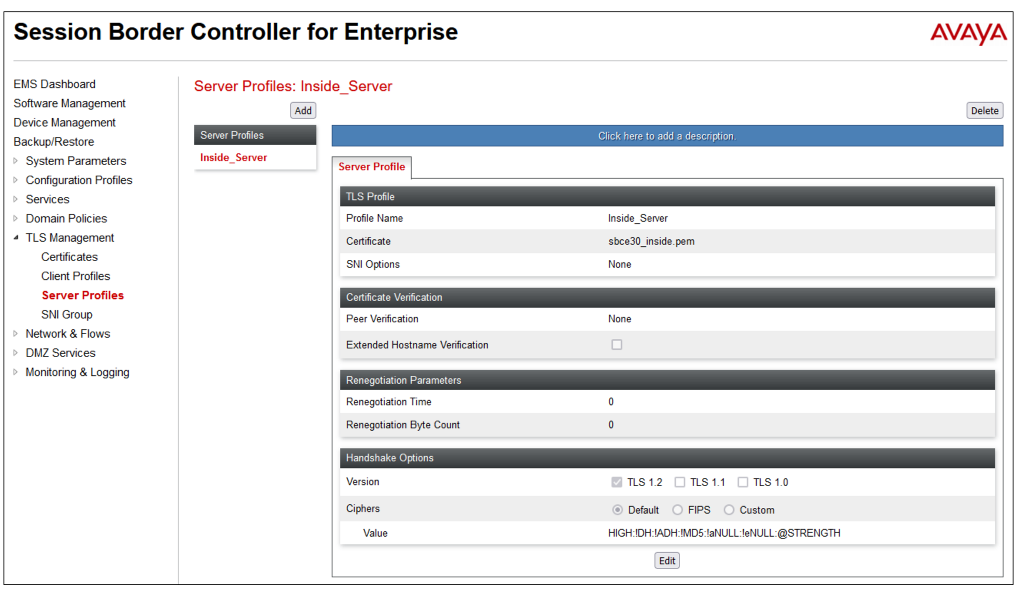


7.2.2. Server Profiles

Navigate to **TLS Management → Server Profiles** and click the **Add** button to add a new profile or select an existing profile. Enter a descriptive **Profile Name** such as **Inside_Server** show below. Select the Avaya SBCE identity certificate for the inside interface from the **Certificate** drop-down menu. In the reference configuration this is **sbce30_inside.pem**. Select **None** from the **Peer Verification** drop-down menu. Click **Next** and accept default values for the next screen, then click **Finish** (not shown).

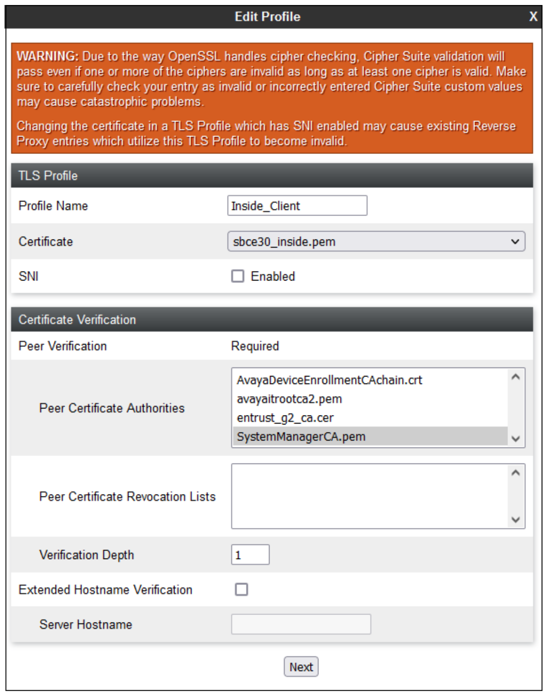


The following screen shows the completed TLS **Server Profile** form:

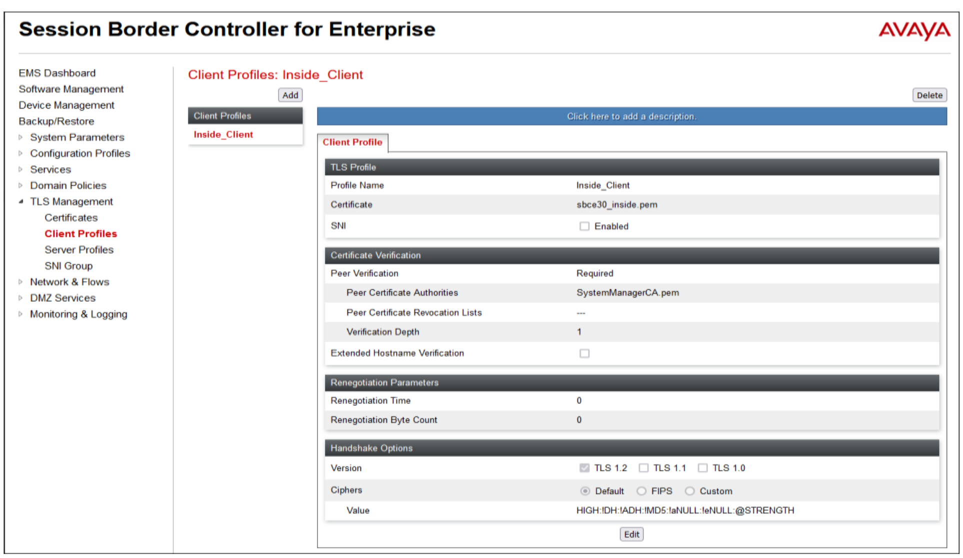


7.2.3. Client Profiles

Navigate to **TLS Management → Client Profiles** and click the **Add** button to add a new profile or select an existing profile. Enter a descriptive **Profile Name**, such as **Inside_Client** shown below. Select the identity certificate from the **Certificate** drop-down menu. In the reference configuration this is **sbce30_inside.pem**. The **Peer Certificate Authorities** field is set to the root certificate used to verify the certificate received from Session Manager, e.g., **SystemManagerCA.pem**. The **Verification Depth** field is set to **1**. Click **Next** and accept default values for the next screen and click **Finish** (not shown).

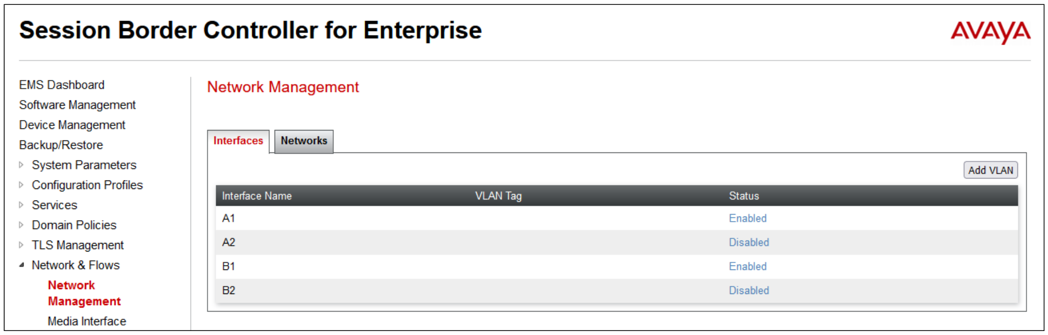


The following screen shows the completed TLS **Client Profile** form:



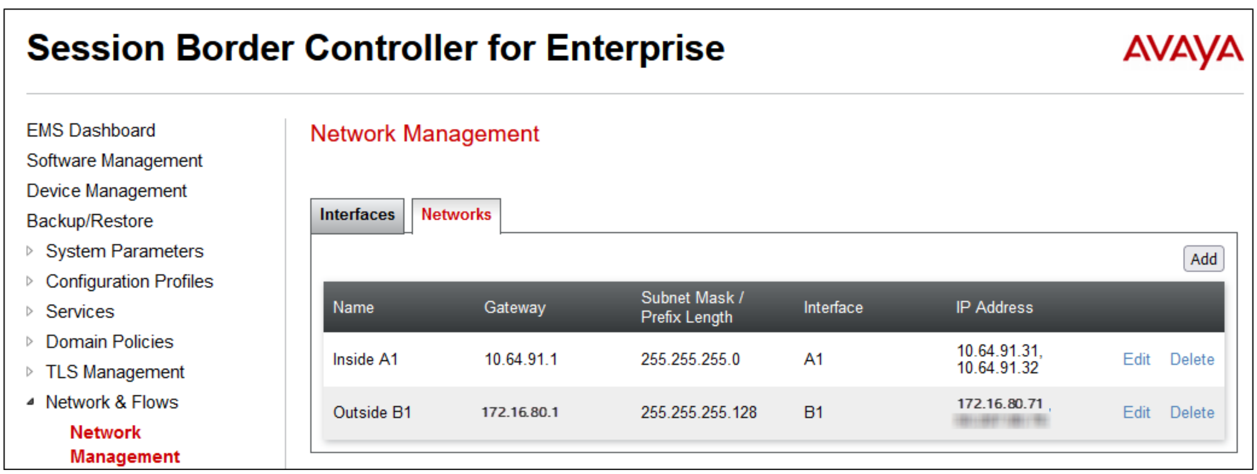
7.3. Network Management

The Network Management screen is where the network interface settings are configured and enabled. Some of these values are specified during installation. Navigate to **Networks & Flows → Network Management** from the menu on the left-hand side. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 and B1 are used.



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

- **A1**: **10.64.91.32** – "Inside" IP address, toward Session Manager.
- **B1: 172.16.80.71** – "Outside" IP address toward the BT SIP trunk.

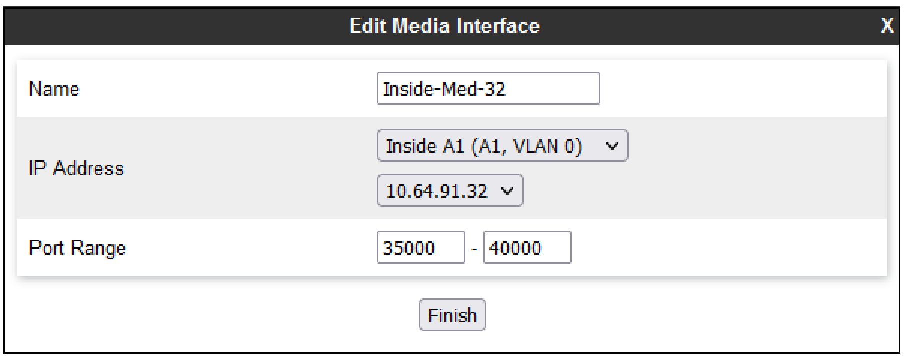


7.4. Media Interfaces

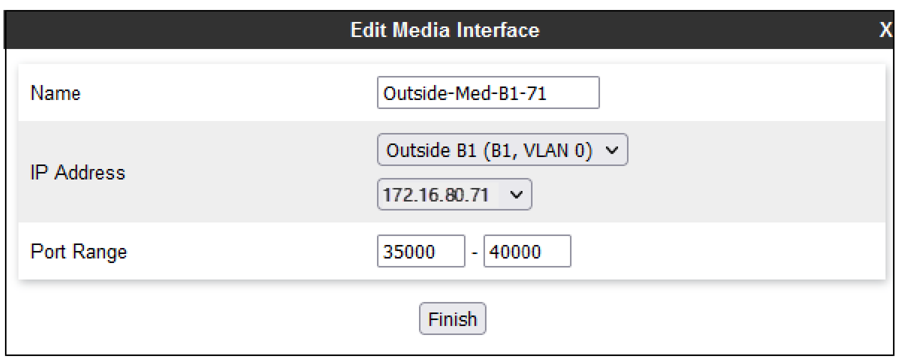
Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which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

To create a new Media Interface, navigate to Select **Network & Flows → Media Interface** from the menu on the left-hand side and select **Add** (not shown).

The screen below shows the **Inside-Med-32** Media Interface created toward the Session Manager. On the **IP Address** drop-down menus, **Inside-A1 (A1,VLAN0)** and **10.64.91.32** are selected. Default **Port Range** values are used.



The screen below shows the **Outside-Med-B1-71** Media Interface created toward BT. On the **IP Address** drop-down menus, **Outside-B1 (B1,VLAN0)** and **172.16.80.71** are selected. Default **Port Range** values are used.

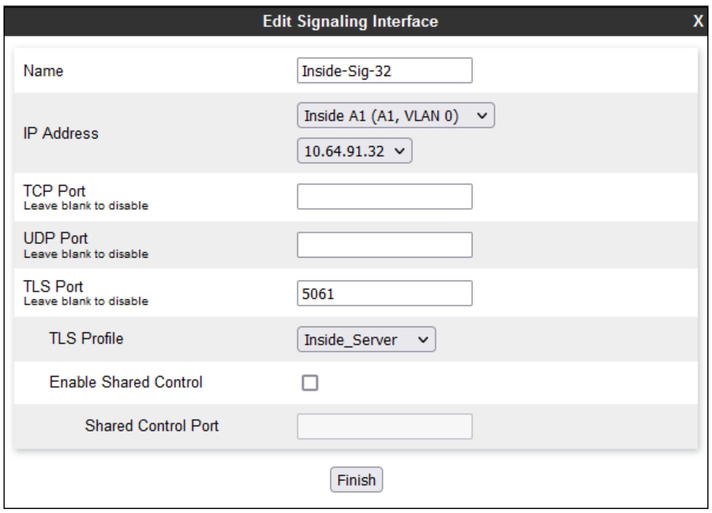


7.5. Signaling Interfaces

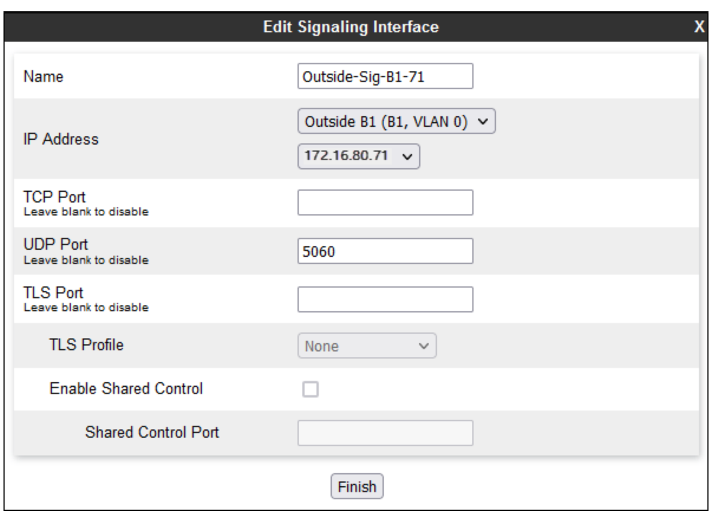
The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to Select **Network & Flows → Media Interface** from the menu on the left-hand side and select **Add** (not shown).

The screen below shows the **Inside-Sig-32** Signaling Interface created toward the Session Manager. On the **IP Address** drop-down menus, **Inside-A1 (A1,VLAN0)** and **10.64.91.32** are selected. **TLS Port 5061** is used. The TLS server profile created in **Section 7.2.2** (e.g., **Inside_Server**) is selected on the TLS Profile drop-down menu.



The screen below shows the **Outside-Sig-B1-71** Signaling Interface created toward BT. On the **IP Address** drop-down menus, **Outside-B1 (B1,VLAN0)** and **172.16.80.71** are selected. **UDP Port 5060** is used.



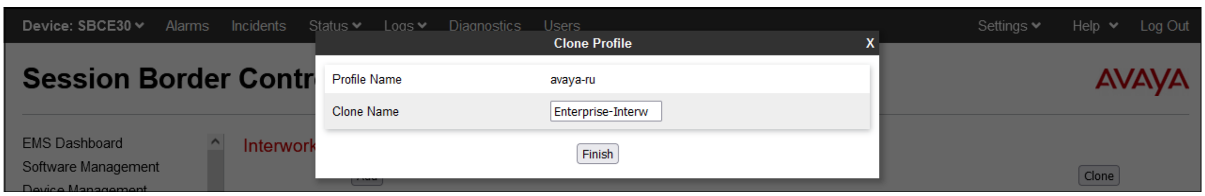
7.6. Server Interworking Profile

The Server Internetworking profile includes parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

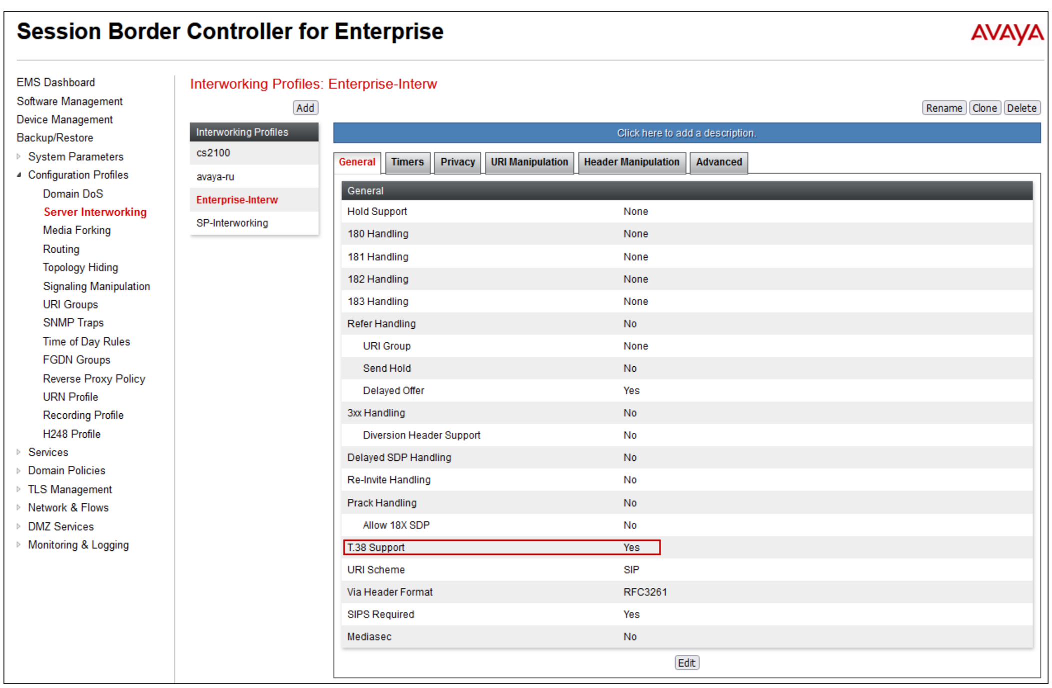
In the reference configuration, separate Server Interworking Profiles were created for the enterprise and the BT Wholesale Hosted SIP Trunking service.

7.6.1. Server Interworking Profile – Enterprise

In the reference configuration, the enterprise Server Interworking profile was cloned from the default **avaya-ru** profile. To clone a Server Interworking Profile for the enterprise, navigate to **Configuration Profiles → Server Interworking**, select the **avayu-ru** profile and click the **Clone** button. Enter a **Clone Name** and click **Finish** to continue.

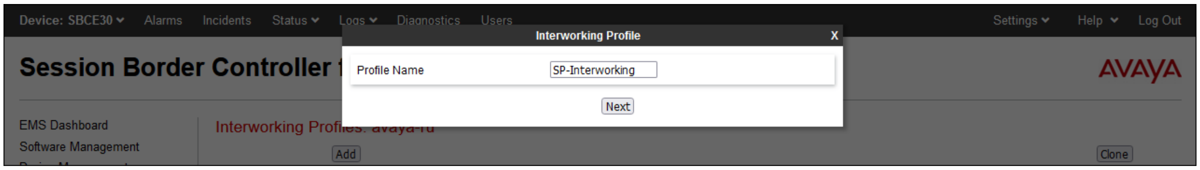


The following screen shows the **Enterprise-Interwk** profile used in the reference configuration, with **T.38 Support** set to **Yes**. To modify the profile, scroll down to the bottom of the screen and click **Edit**. Select the **T.38 Support** parameter and then click **Next** and then **Finish** (not shown). Default values can be used for all other fields.

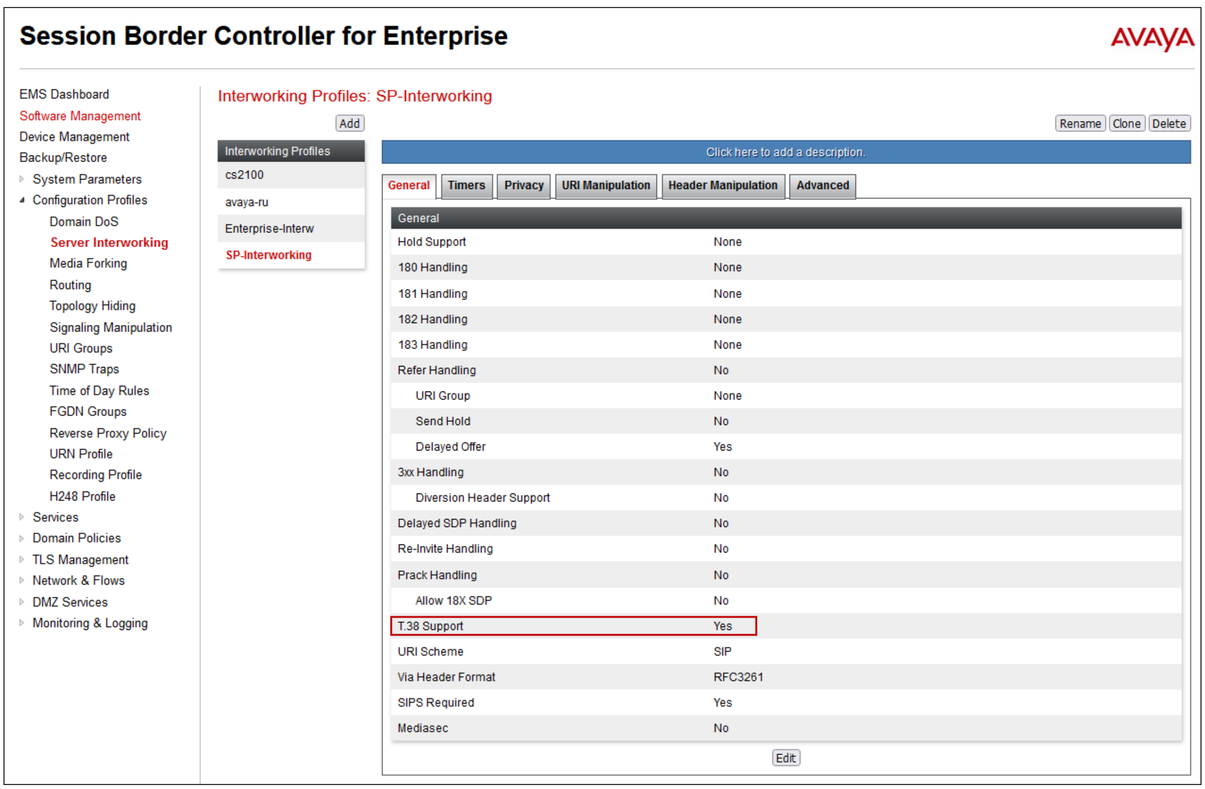


7.6.2. Server Interworking Profile – Service Provider

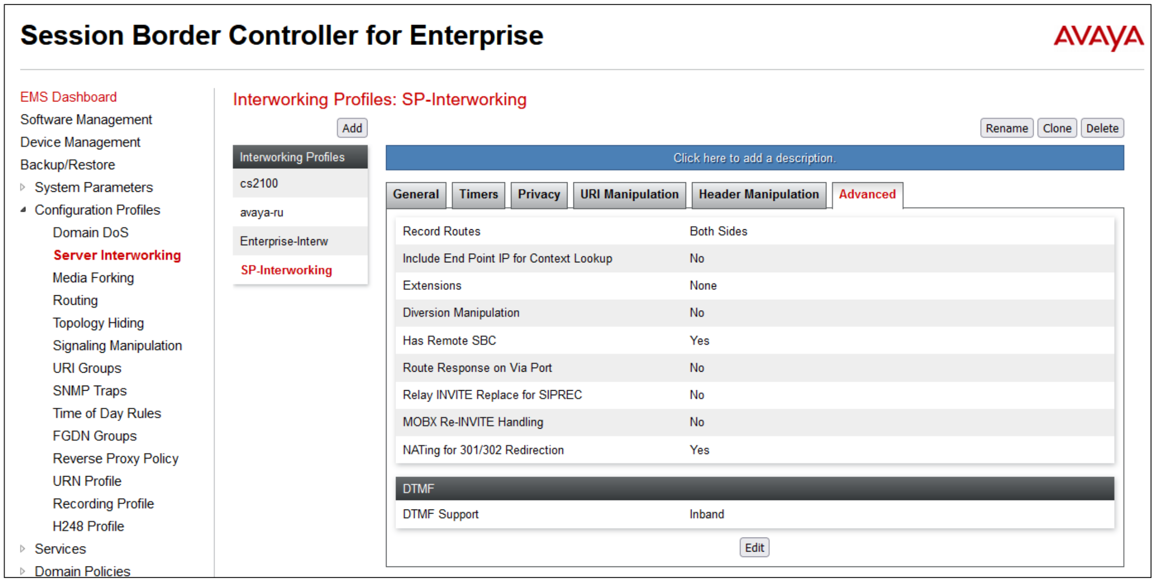
To create a new Server Interworking Profile for BT, navigate to **Configuration Profiles → Server Interworking** and click **Add** as shown below. Enter a **Profile Name** and click **Next**.



The following screens show the **SP-Interworking** profile used in the reference configuration. On the **General** tab, default values are used with the exception of **T.38 Support** which is set to **Yes**.



Default parameters were used for the **Timers**, **Privacy**, **URI Manipulation**, and **Header Manipulation** tabs (not shown). On the **Advanced** tab, **Record Routes** is set to **Both Sides**. Default values can be used for all other fields.



7.7. 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 7.6**) or Signaling Rules (**Section 7.13**) does not meet the desired result.

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 (See **Section 2.2**):

- Remove the "+" in the user part of the Diversion header on calls that are forwarded to the PSTN.
- Remove XML information from UPDATE messages on calls that are transferred back to BT

Select **Configuration Profiles → Signaling Manipulation** from the menu on the left. Click **Add Script** (not shown) and the script editor window will open.

- Enter a name for the script in the **Title** box (e.g., **BT_Script_1**).
- Copy and paste the script from **Section 12**.
- Click on **Save.** The script editor will test for any errors, and the window will close. This script will later be applied to the BT Server Configuration profile.
-

During the compliance test, BT requested to perform a Class 5 CLIP PBX passthrough test case. In this scenario, the CPE should be able to send a Class 5 CLIP on the From header and the user number (DID) on the P-Asserted-Identity header in outbound calls. This can be achieved by including additional configuration on the SigMa script above. This configuration is optional, and only required if the BT Class 5 CLI PBX passthrough feature is used.

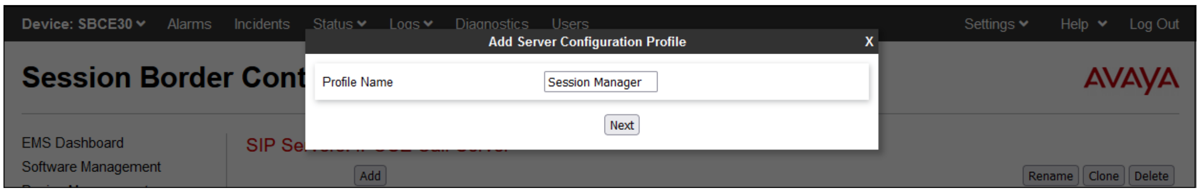
The details of the scripts, including the optional configuration, appear on **Section 12**.

7.8. SIP Server Profiles

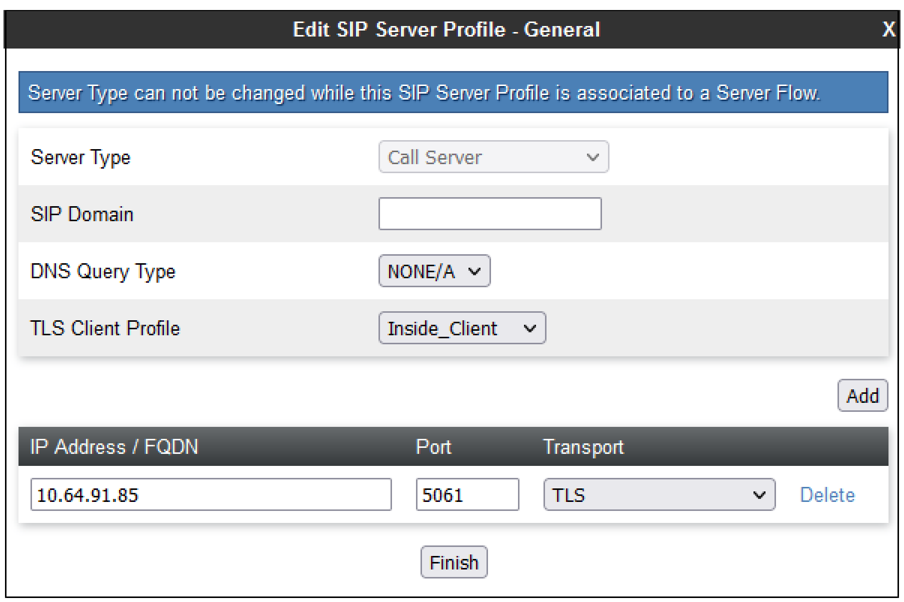
The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

7.8.1. SIP Server Profile – Session Manager

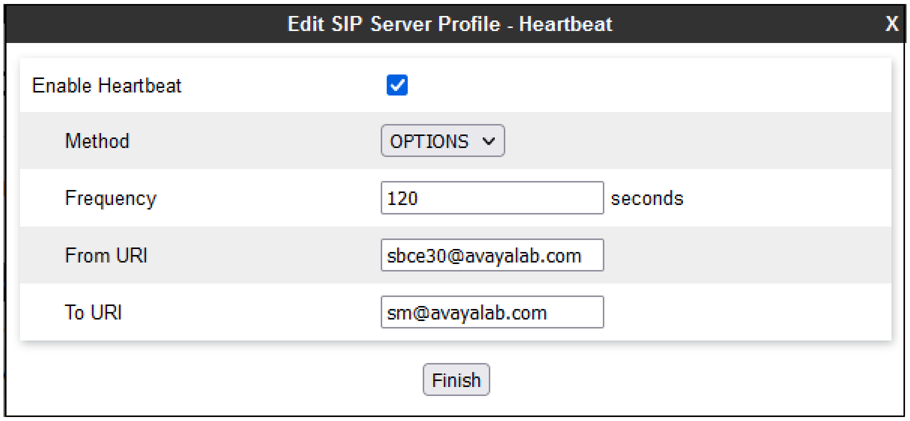
To add a SIP Server Profile for Session Manager, navigate to **Services → SIP Servers** on the left-hand menu and click **Add**. Enter a descriptive name for the new profile and click **Next**.



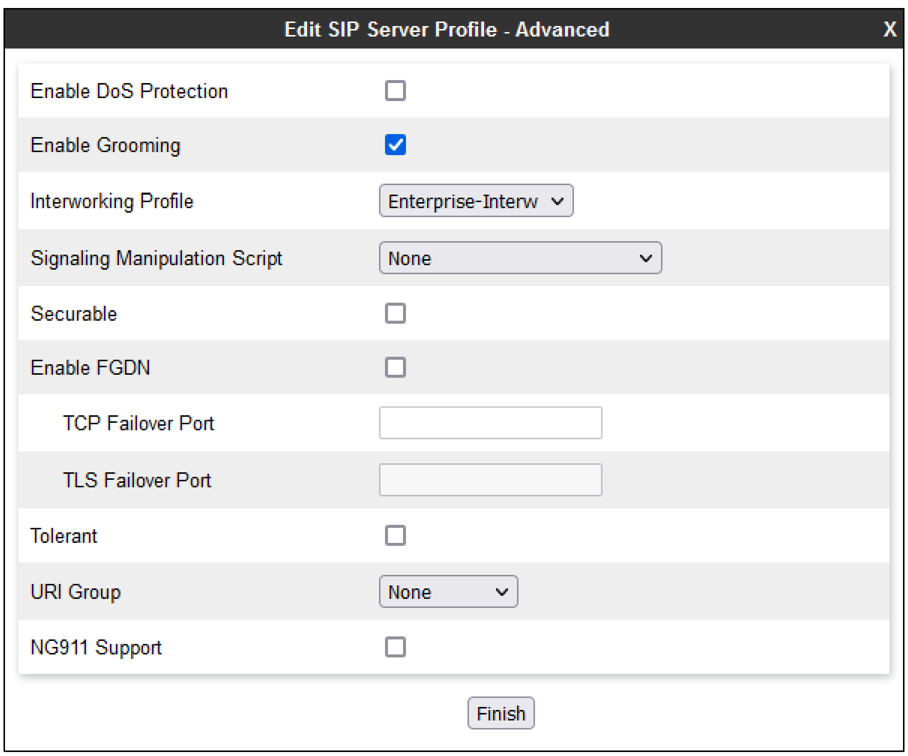
The following screen illustrate the SIP Server Profile named **Session Manager**. In the **General** parameters, the **Server Type** is set to **Call Server**. In the **IP Address / FQDN** field, the IP Address of Session Manager Security Module is entered. This IP address is **10.64.91.85**. Under **Port**, **5061** is entered, and the **Transport** parameter is set to **TLS**. TLS profile **Inside_Client** created in **Section 7.2.3** is selected for **TLS Client Profile**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



Default values can be used on the **Authentication** tab. Click **Next** (not shown) to proceed to the **Heartbeats** tab. The Avaya SBCE can be configured to source "heartbeats" in the form of PINGs or SIP OPTIONS towards Session Manager. Check the **Enable Heartbeat** box and select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE.

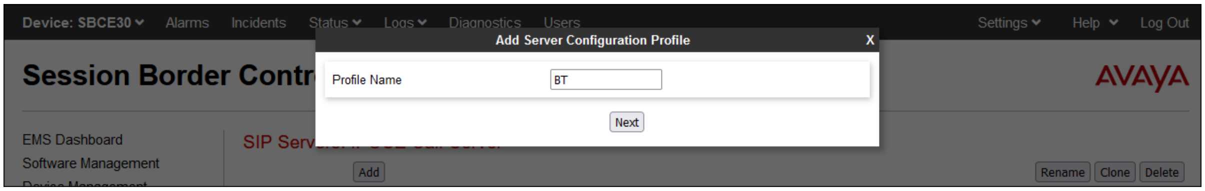


On the **Advanced** tab, select the **Enable Grooming** checkbox. The **Interworking Profile** is set to the **Enterprise-Interwk** profile created in **Section 7.6.1**.

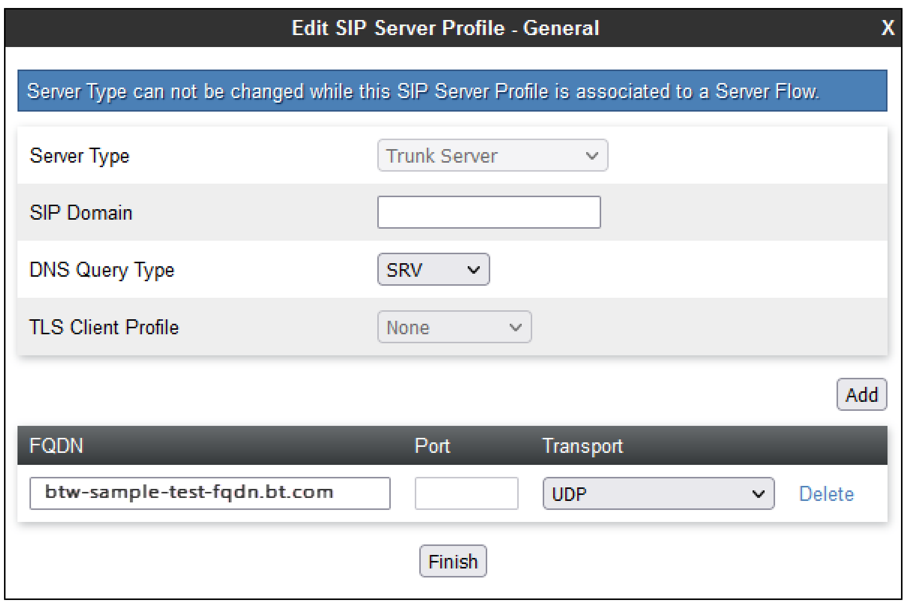


7.8.2. SIP Server Profile – Service Provider

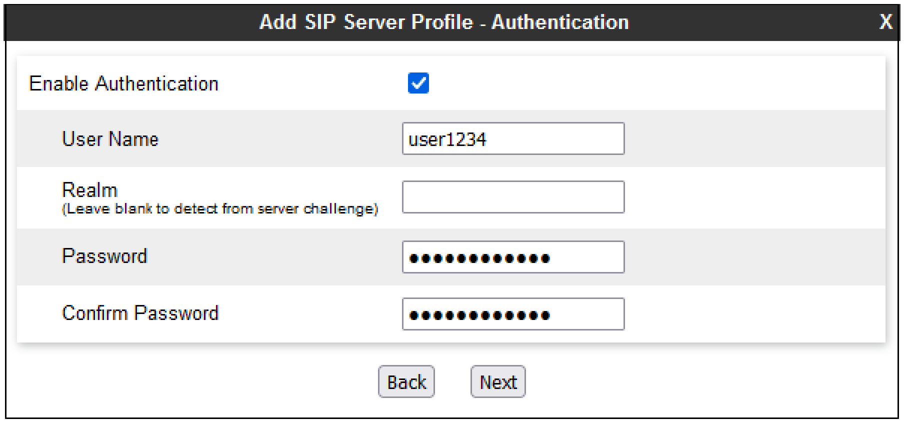
To add a SIP Server Profile for BT, navigate to **Services → SIP Servers** and click **Add**. Enter a descriptive name for the new profile and click **Next**.



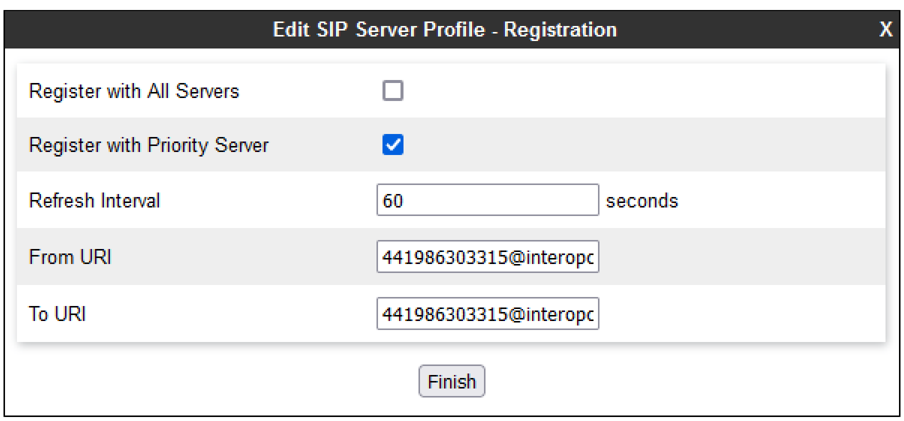
The following screens illustrate the SIP Server Profile named **BT**. In the **General** parameters, the **Server Type** is set to **Trunk Server**. The **DNS Query Type** is set to **SRV**. In the **IP Address / FQDN** field, the BT-provided SIP proxy server FQDN is entered. In the example below, this is **btw-sample-test-fqdn.bt.com**. The **Transport** parameter is set to **UDP**. Note that the **Port** field is grayed out, since the port number is discovered via the DNS SRV query. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



On the **Authentication** tab, the **Enable Authentication** box is checked. On the **User Name** and **Password** fields, enter the credential information provided by BT for the SIP trunk registration. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.

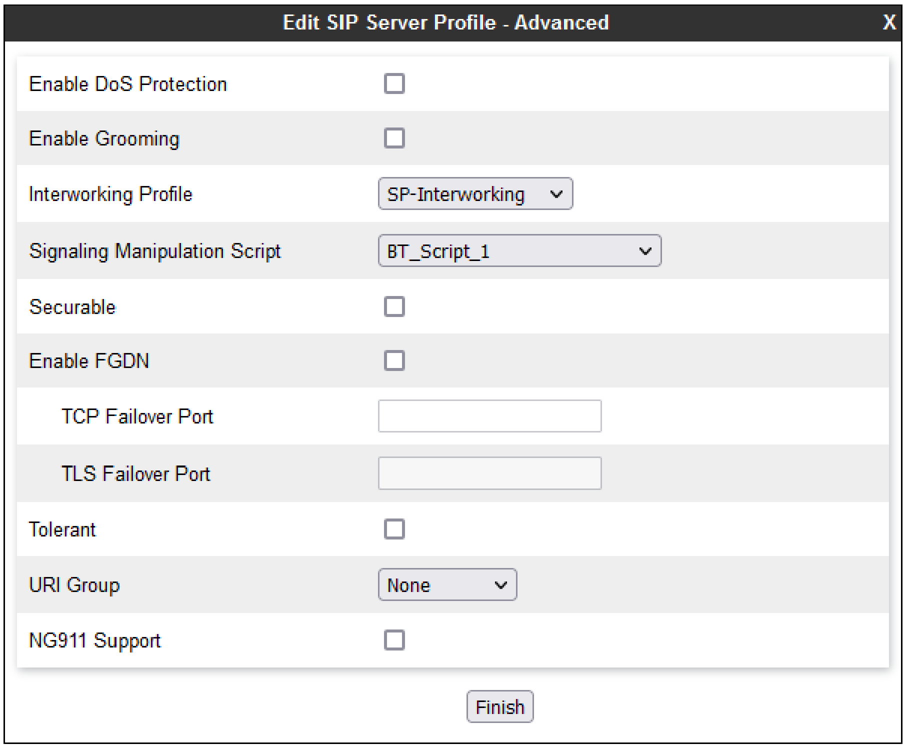


No changes are made on the **Heartbeat** tab (not shown). On the **Registration** tab, check the **Register with Priority Server** box. Under **Refresh Interval**, enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with BT. **60** seconds was the value used during the compliance test. The **From URI** and **To URI** entries for the REGISTER messages are built using the pilot number and domain name assigned by BT to the SIP trunk. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



On the **Advanced** window, enter the following:

- **Enable Grooming** is not used for UDP connections and is left unchecked.
- Select the **SIP Provider Interwk** (created in **Section 7.6.2**), for **Interworking Profile**.
- Select the **BT_Script_1** (created in **Section 7.7**) for **Signaling Manipulation Script**.
- Select **Finish**.

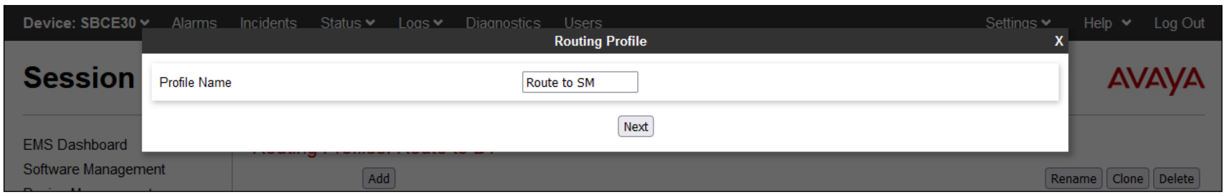


7.9. Routing Profiles

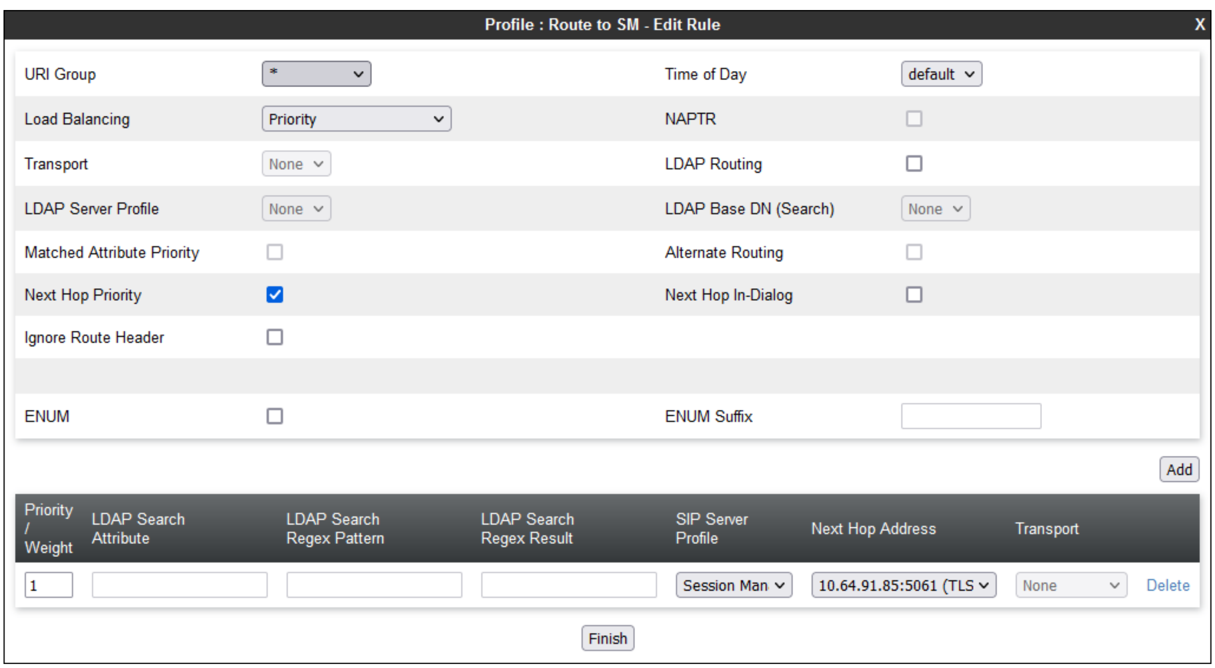
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport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

7.9.1. Routing Profile – Session Manager

To add a routing profile for Session Manager, navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.

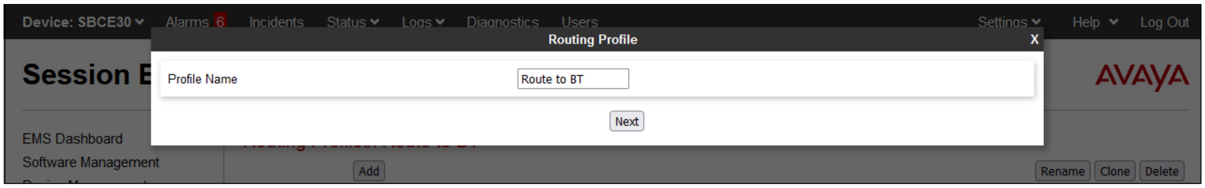


The following screen shows the Routing Profile R**oute to SM** created in the reference configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to **1**. The Session Manager **SIP Server Profile**, created in **Section 7.8.1**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the SIP Server Profile, and **Transport** becomes greyed out. Click **Finish**.

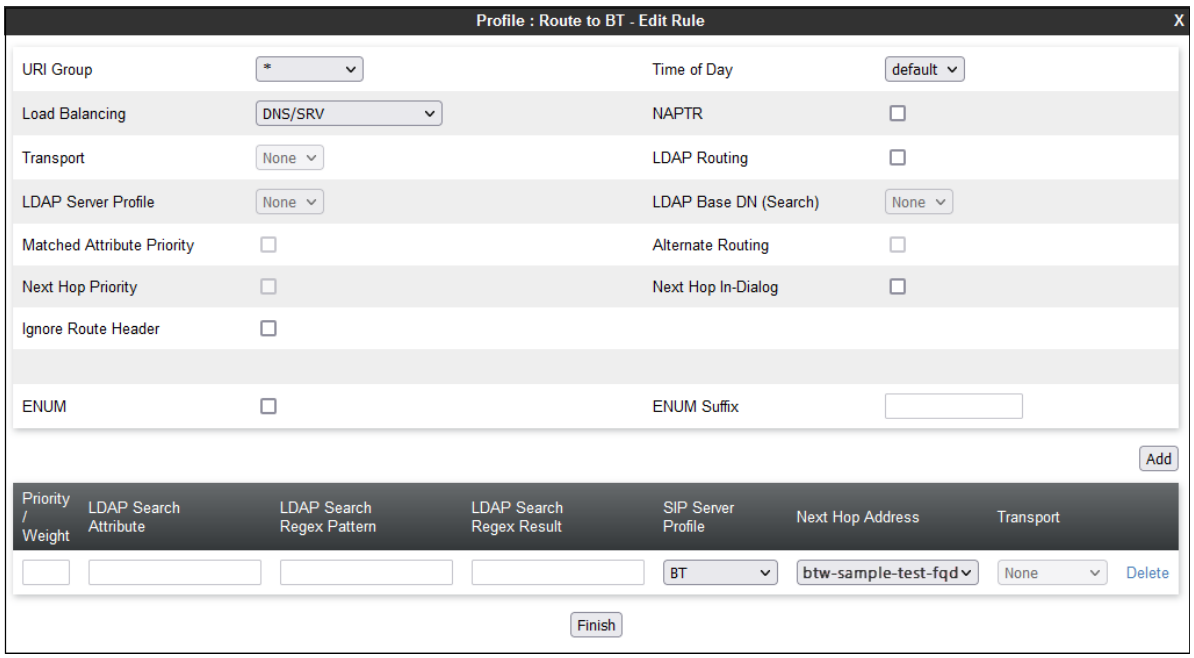


7.9.2. Routing Profile – Service Provider

Similarly add a Routing Profile to the BT Wholesale Hosted SIP Trunking Service.



The following screen shows the Routing Profile **Route to BT** created in the reference configuration. In the top portion of the profile, the **Load Balancing** parameter is set to **DNS/SRV**. Under **SIP Server Profile**, the **BT** profile, created in **Section 7.8.2**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the SIP Server Profile, and **Transport** becomes greyed out. Click **Finish**.



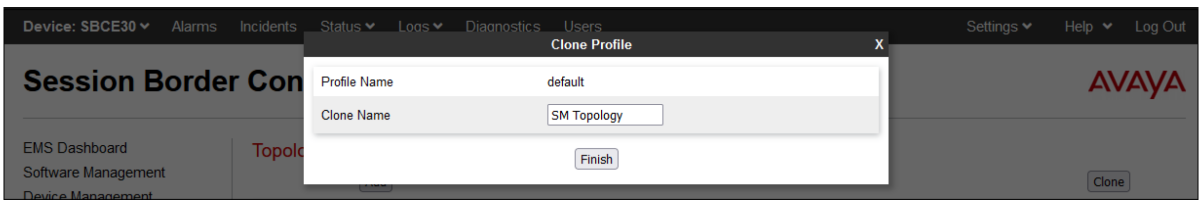
7.10. Topology Hiding Profile

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.

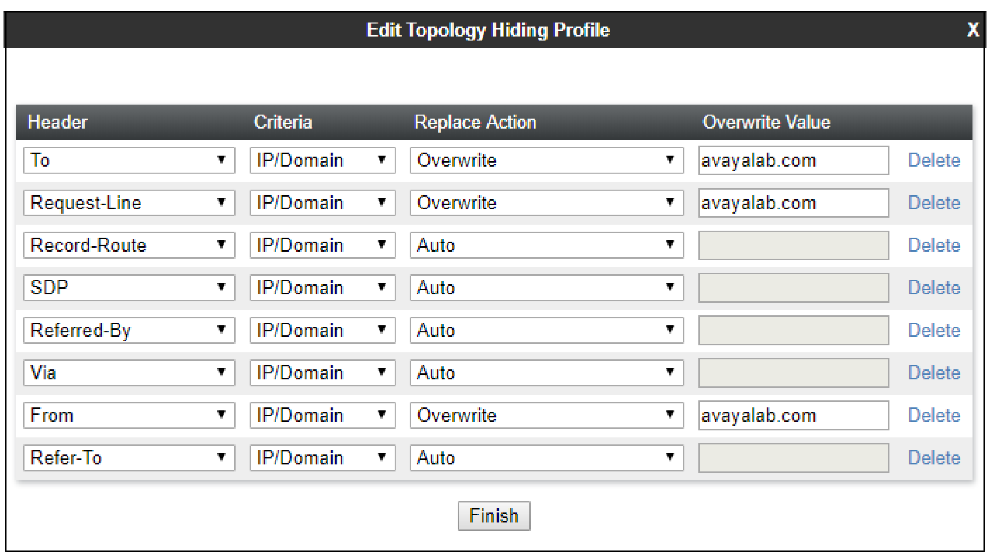
Topology Hiding can also be used as an interoperability tool to adapt the host portion of the SIP headers, to the IP addresses or domains expected on the service provider and the enterprise networks.

7.10.1. Topology Hiding – Enterprise

In the sample configuration, the enterprise Topology Hiding profile was cloned from the **default** profile and then modified. Select **Configuration Profiles → Topology Hiding** from the left-hand menu. Select the pre-defined **default** profile and click the **Clone** button. Enter profile name (e.g., **SM Topology**) and click **Finish** to continue.

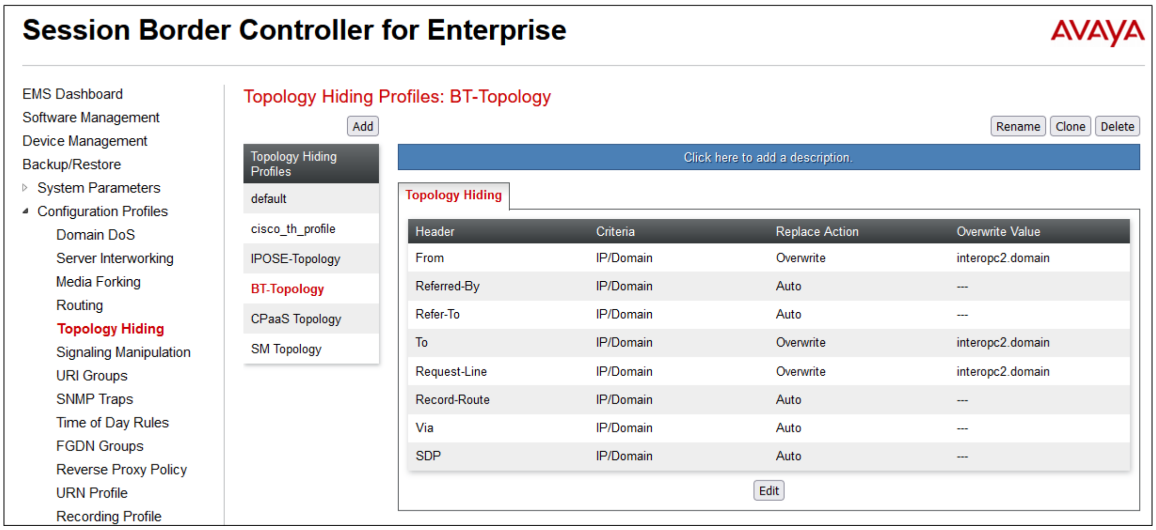


Edit the newly created **Enterprise-Topology** profile. For the **Request-Line**, **To** and **From** headers select **Overwrite** under the **Replace Action** column. Enter the domain of the enterprise (e.g., **avayalab.com**) on the **Overwrite Value** field. Click **Finish**.



7.10.2. Topology Hiding – Service Provider

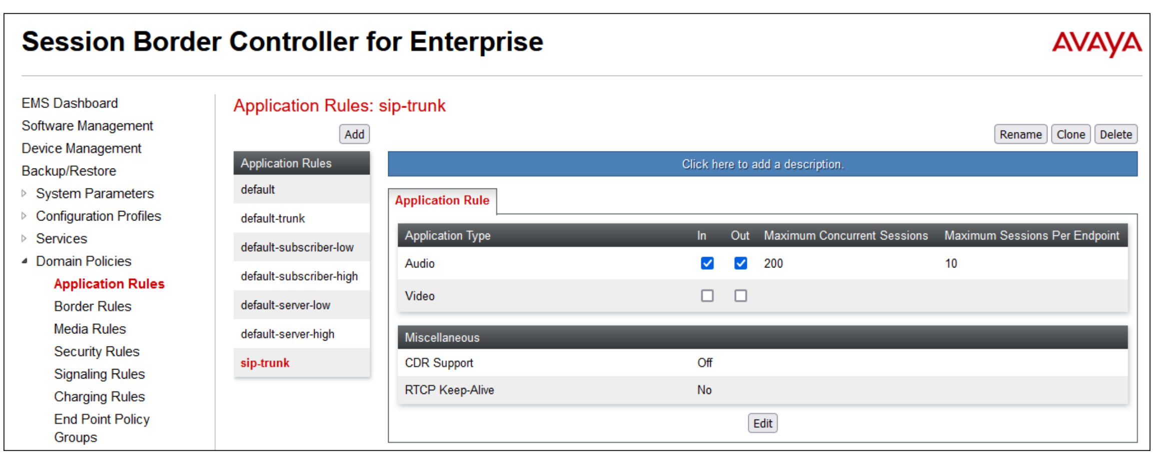
Similarly create a Topology Hiding profile for the Avaya SBCE connection to BT. Enter a Profile Name (e.g., **BT Topology**). For the **Request-Line**, **To** and **From** headers, **Overwrite** is selected under the **Replace Action** column. The domain used by the service provider on the SIP trunk (e.g., **interopc2.domain**) is entered on the **Overwrite Value** field.



7.11. Application Rules

Application Rules define which types of SIP-based Unified Communications applications the Avaya SBCE security device will protect. In addition, the maximum number of concurrent voice and video sessions the network will process are set, in order to prevent resource exhaustion.

Select **Domain Policies → Application Rules** from the left-side menu as shown below. Click the **Add** button to add a new profile, or select an existing topology hiding profile to edit. In the reference configuration, the **sip-trunk** profile was created for the enterprise and BT. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Audio** application to a value slightly larger than the licensed sessions. For example, if licensed for 150 sessions set the values to **200**. The **Maximum Session Per Endpoint** was set to **10**.



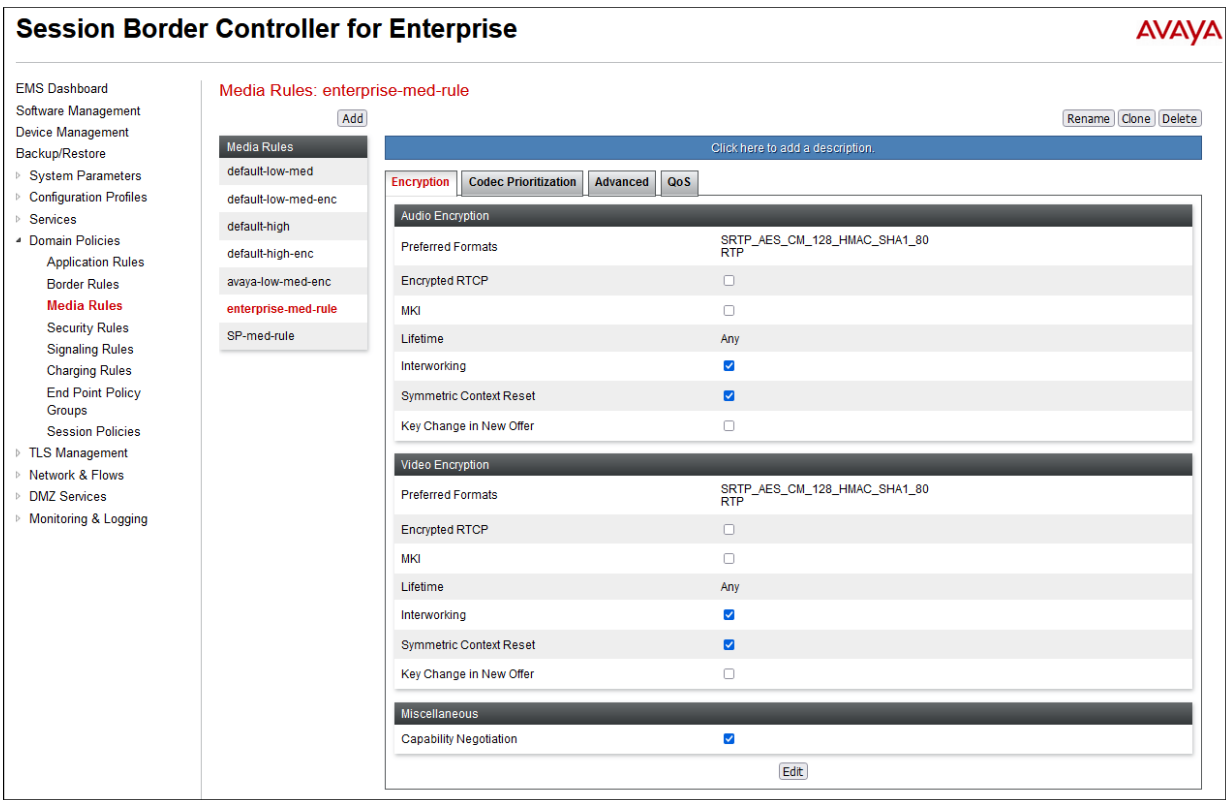
7.12. Media Rules

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

7.12.1. Media Rule – Enterprise

To create a Media Rule for the enterprise, select **Domain Policies → Media Rules** from the left-side menu. In the sample configuration, the default **avaya-low-med-enc** rule was cloned, and then modified as shown on the screen below. With the **avaya-low-med-enc** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown).

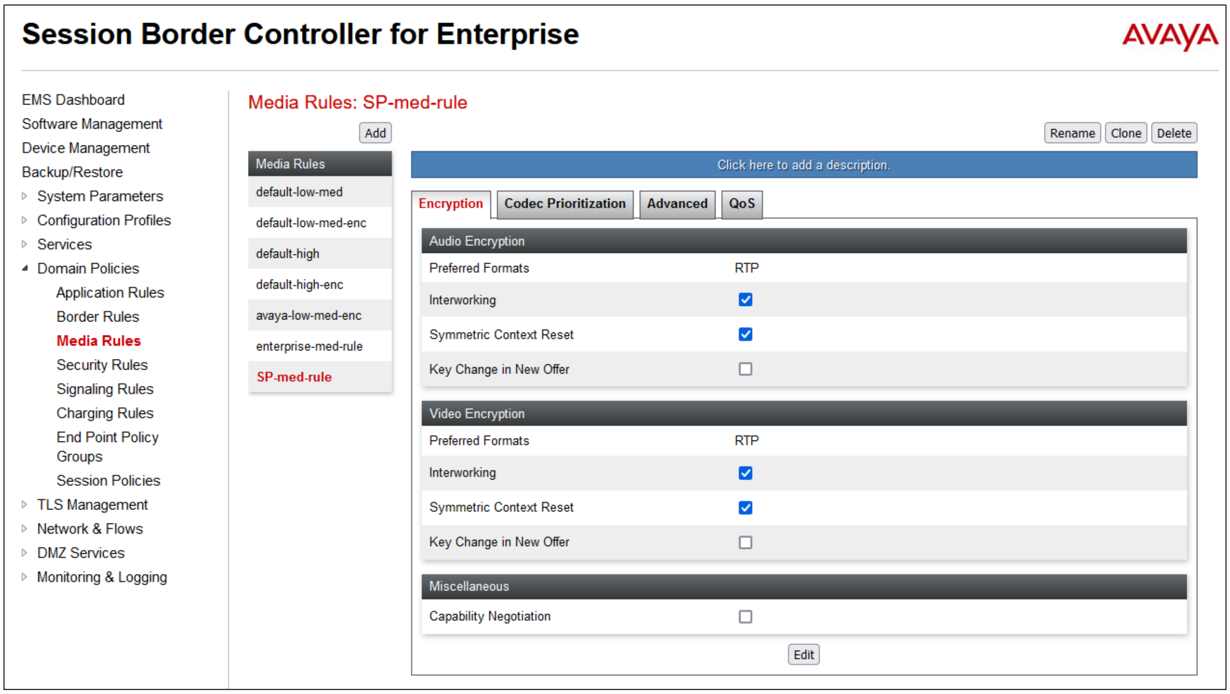
The Media Rule **enterprise-med-rule** created for the enterprise is shown below. The **Preferred Formats** are changed to include **SRTP_AES_CM_128_HMAC_SHA1_80** as the first choice and **RTP** as second. In the **Miscellaneous** section, **Capability Negotiation** is checked. All other fields retained their default cloned value.



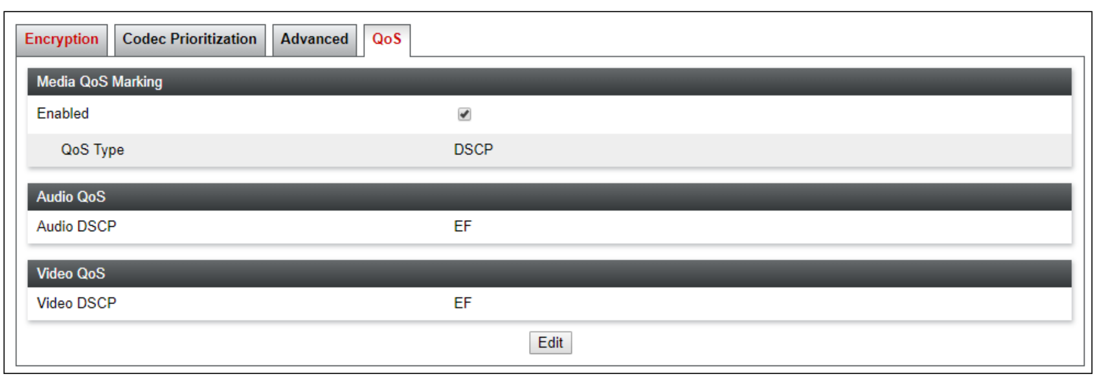
7.12.2. Media Rule – Service Provider

Similarly, a Media Rule is created for BT. In this case, the **default-low-med** profile was cloned. With the **default-low-med** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown).

The Media Rule named **SP-med-rule**, used for BT in the sample configuration is shown below.



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

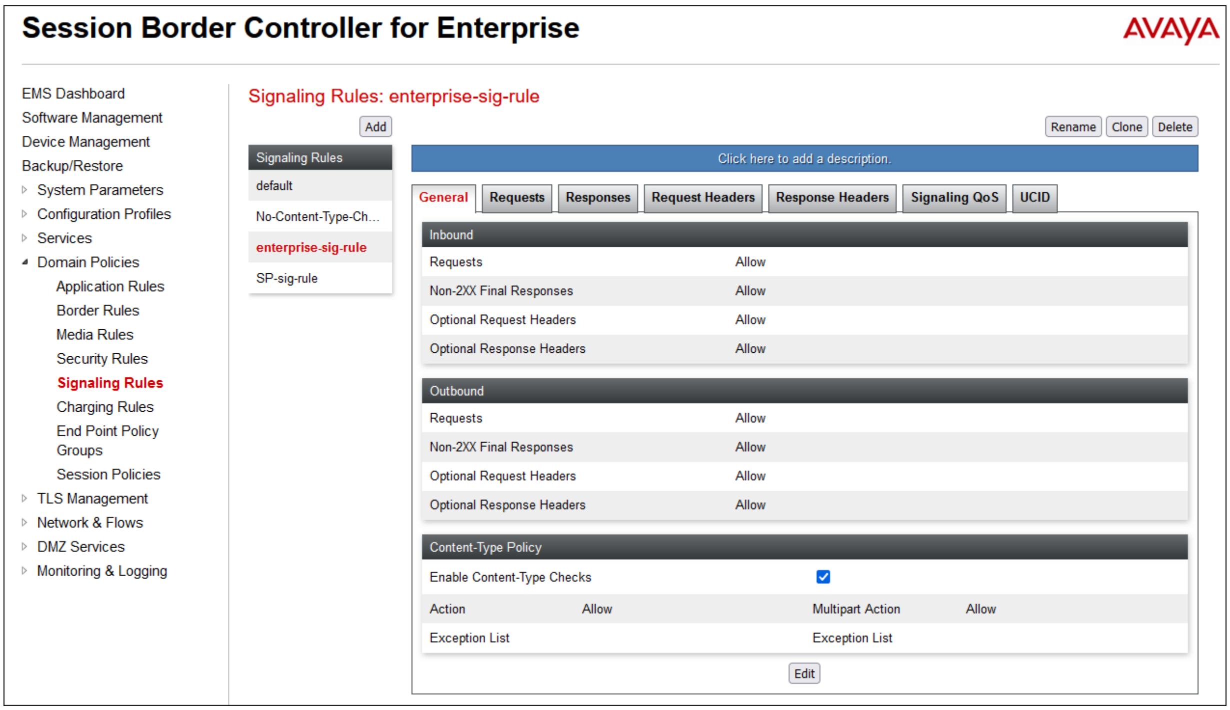


7.13. Signaling Rules

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

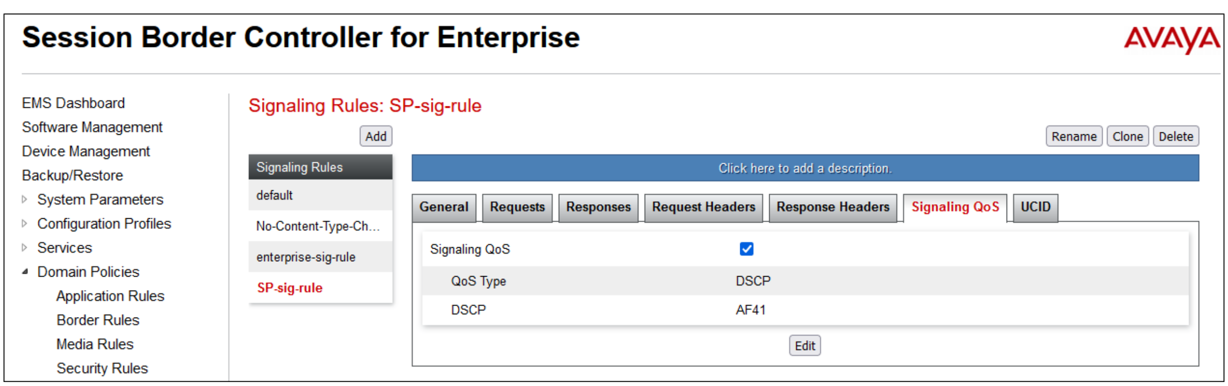
7.13.1. Signaling Rule – Enterprise

Navigate to **Domain Policies → Signaling Rules**. With the **default** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown). In the reference configuration, signaling rule **enterprise-sig-rule** is unchanged from the default rule.



7.13.2. Signaling Rule – Service Provider

A signaling rule **SP-sig-rule** was similarly cloned from the default rule and used for BT, and also left unchanged from the default rule. Note the DSCP value **AF41** for assured forwarding (default value) used for **Signaling QoS.**



7.14. Endpoint Policy Groups

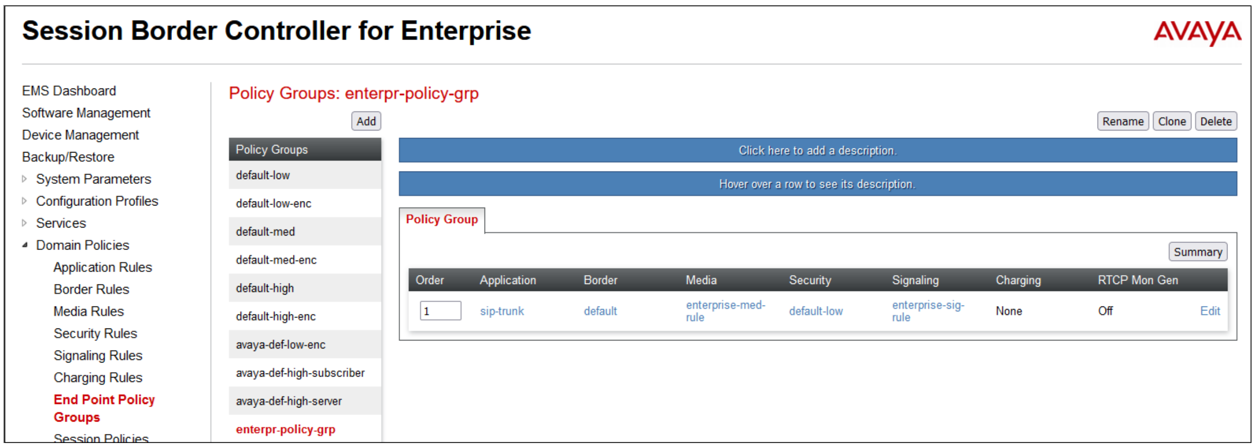
The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is latter applied to a Server Flow in **Section 7.15**.

7.14.1. End Point Policy Group - Enterprise

To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on **Add**. On the **Policy Group** window (not shown), select the following.

- **Application Rule**: **sip-trunk** (created in **Section 7.11**).
- **Border Rule**: **default**.
- **Media Rule**: **enterprise-med-rule** (created in **Section 7.12.1**).
- **Security Rule**: **default-low**.
- **Signaling Rule**: **enterprise-sig-rule** (created in **Section 7.13.1**).
- Select **Finish**.

The following screen shows the completed **enterpr-policy-grp** created for the enterprise.

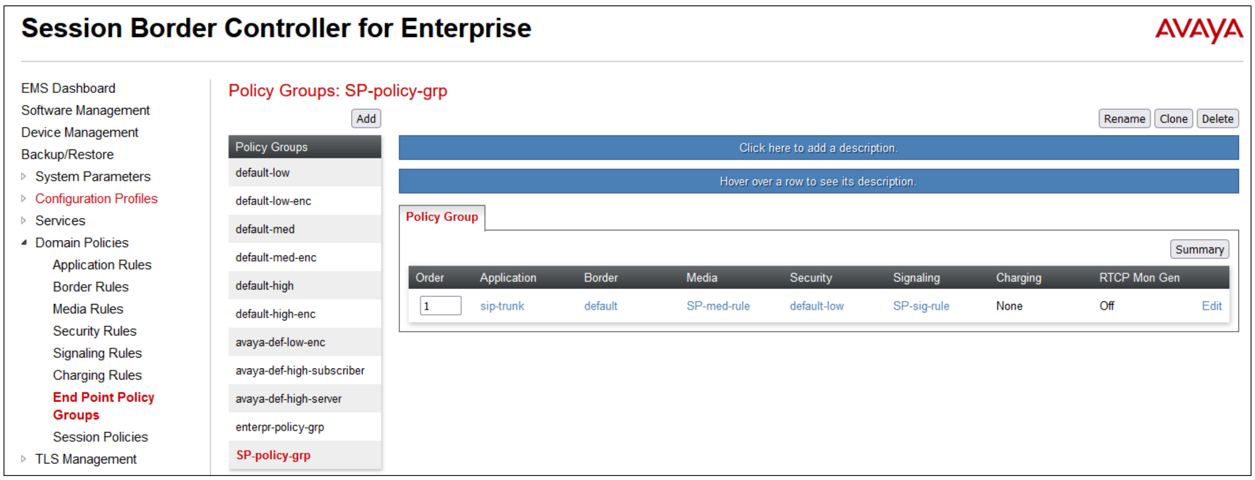


7.14.2. End Point Policy Group – Service Provider

Repeat the steps from **Section 7.14.1** to create the End Policy Group for BT.

- **Application Rule**: **sip-trunk** (created in **Section 7.11**).
- **Border Rule**: **default**.
- **Media Rule**: **SP-med-rule** (created in **Section 7.12.2**).
- **Security Rule**: **default-low**.
- **Signaling Rule**: **SP-sig-rule** (created in **Section 7.13.2**).
- Select **Finish**.

The following screen shows completed the **SP-policy-grp** created for BT.



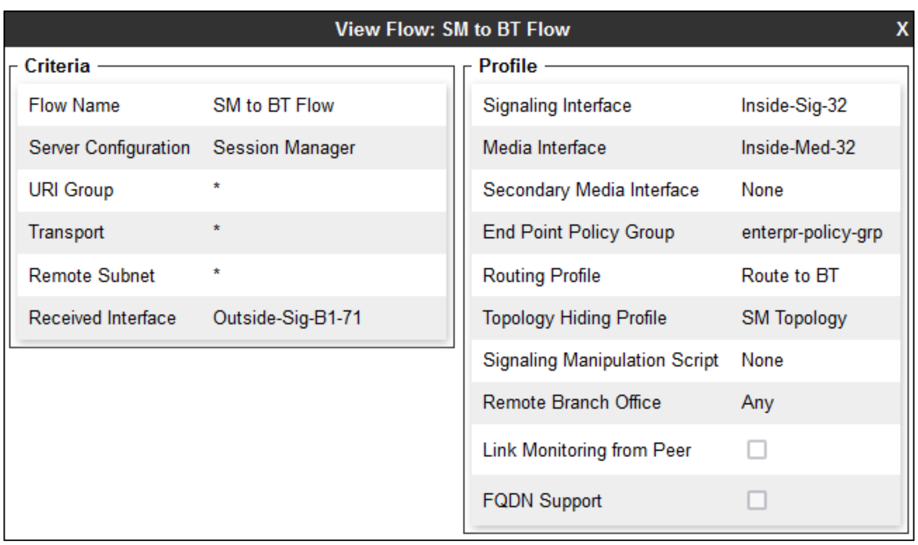
7.15. End Point Flows – Server Flows

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

7.15.1. Server Flow – Enterprise

To create a Server Flow, navigate to **Network and Flows → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown) and enter the following:

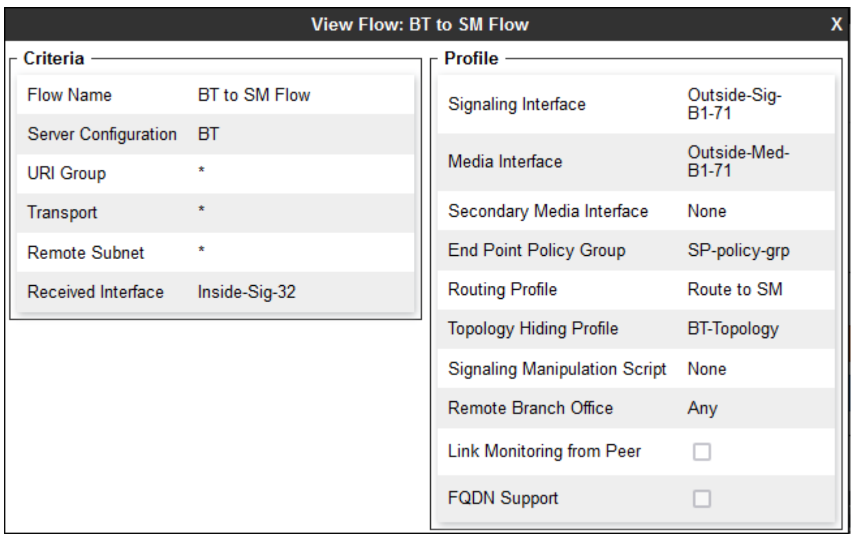
- **Flow Name**: Enter a name for the flow, e.g., **SM to BT Flow**.
- **Server Configuration**: **Session Manager** (**Section 7.8.1**).
- **URI Group**: *
- **Transport**: *
- **Remote Subnet**: *
- **Received Interface**: **Outside-Sig-B1-71** (**Section 7.5**).
- **Signaling Interface**: **Inside-Sig-32** (**Section 7.5**).
- **Media Interface**: **Inside-Med-32** (**Section 7.4**).
- **End Point Policy Group**: **enterpr-policy-grp** (**Section 7.14.1**).
- **Routing Profile**: **Route to BT** (**Section 7.9.2**).
- **Topology Hiding Profile**: **SM Topology** (**Section 7.10.1**).
- Let other fields at the default values.
- Click **Finish** (not shown).



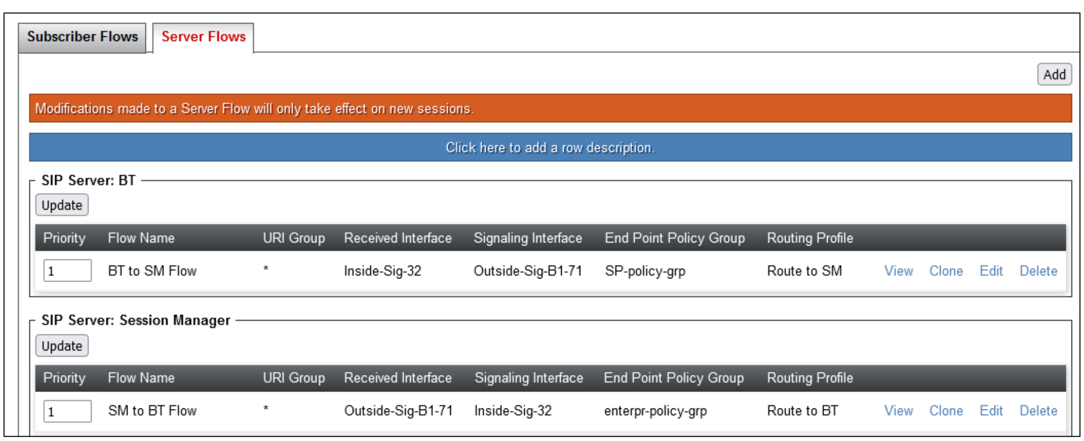
7.15.2. Server Flow – Service Provider

Repeat the steps from **Section 7.15.1**, with the following changes:

- **Flow Name**: Enter a name for the flow, e.g., **BT to SM Flow**.
- **Server Configuration**: **BT** (**Section 7.8.2**).
- **URI Group**: *
- **Transport**: *
- **Remote Subnet**: *
- **Received Interface**: **Inside-Sig-32** (**Section 7.5**).
- **Signaling Interface**: **Outside-Sig-B1-71 (Section 7.5**).
- **Media Interface**: **Outside-Med-B1-71** (**Section 7.4**).
- **End Point Policy Group**: **SP-policy-grp** (**Section 7.14.2**).
- **Routing Profile**: **Route to SM** (**Section 7.9.1**).
- **Topology Hiding Profile**: **BT Topology** (**Section 7.10.2**).
- Let other fields at the default values.
- Click **Finish** (not shown).



The following screen capture shows the newly created **Server Flows**.



8. BT Wholesale Hosted SIP Trunking Service Configuration

To use BT Wholesale Hosted SIP Trunking Service, a customer must request the service from BT using the established sales processes. To obtain further information on BT equipment and system configuration please contact an authorized BT representative.

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

BT is responsible for the configuration of BT Wholesale Hosted SIP Trunking Service. The customer will need to provide the public IP address used to reach the Avaya Session Border Controller for Enterprise at the enterprise, the public IP address assigned to interface B1.

BT will provide the customer the necessary information to configure the Avaya enterprise solution, following the steps discussed in the previous sections, including:

BT will provide the following information:

- SIP Trunk registration credentials (User Name, Password, etc.).
- BT's Domain Name and SIP Proxy FQDN.
- DNS IP addresses.
- DID numbers, etc.

9. Verification and Troubleshooting

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

9.1. General Verification Steps

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

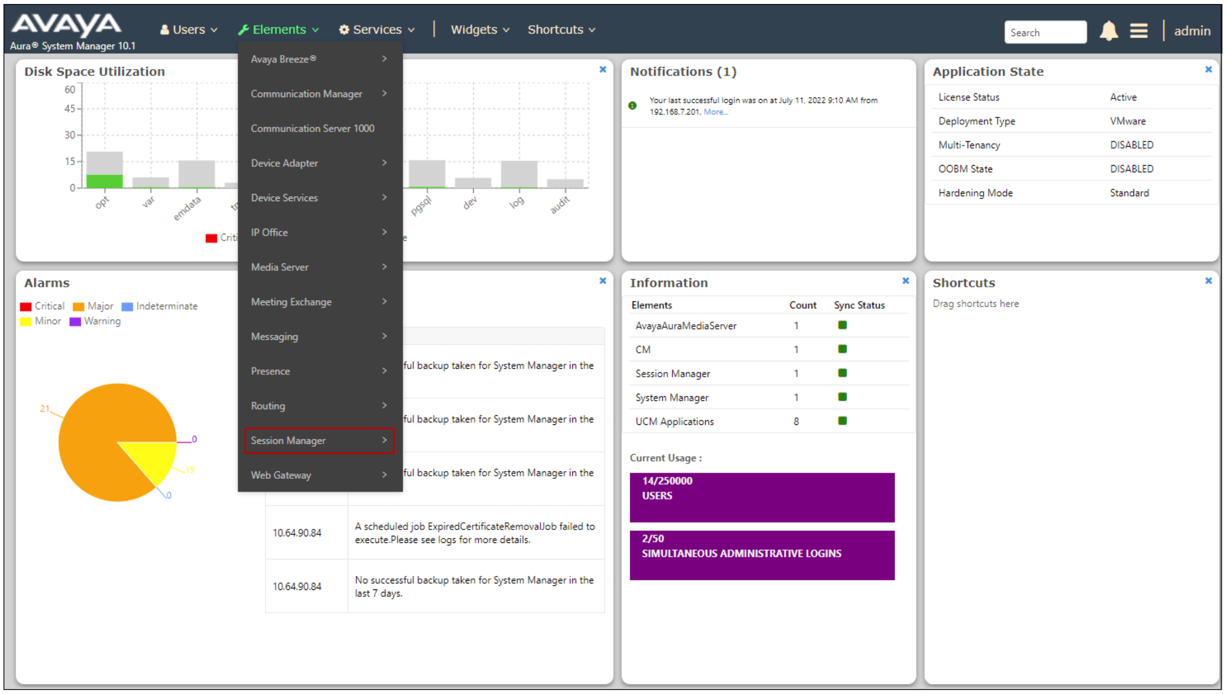
9.2. Communication Manager Verification

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

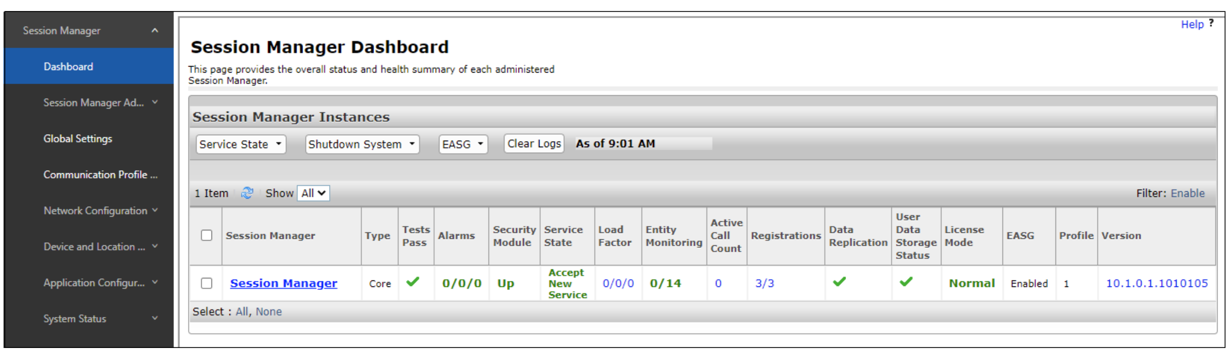
- **list trace station** <extension number>
  Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>
  Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>
  Displays signaling group service state.
- **status trunk** <trunk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

9.3. Session Manager Verification

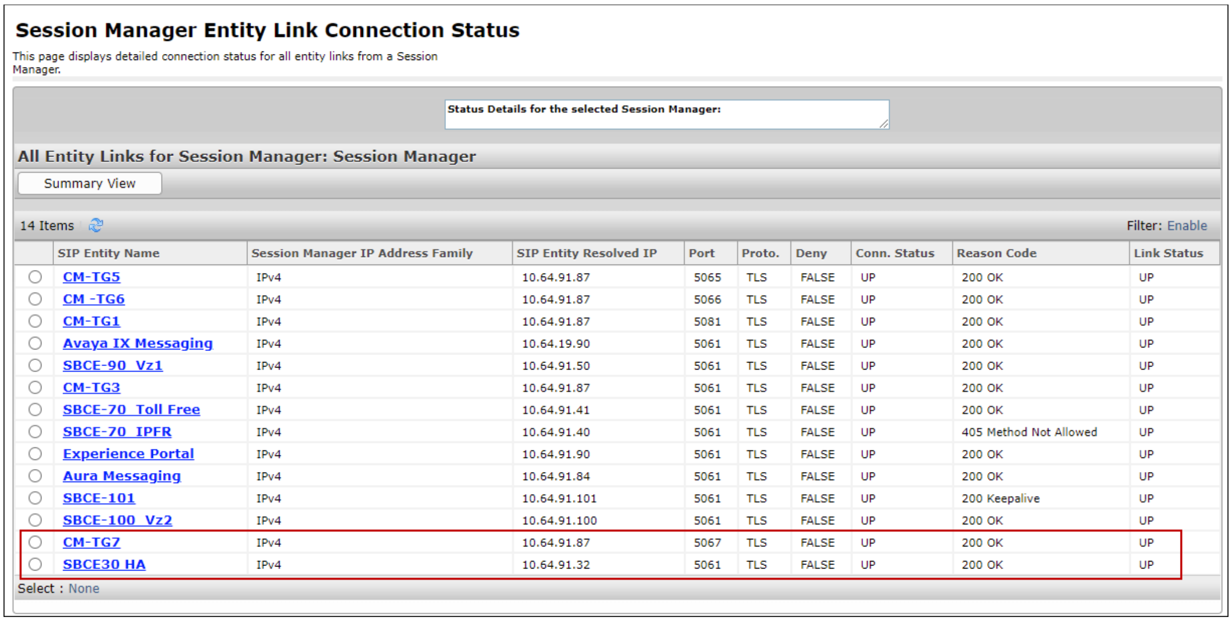
The Session Manager configuration may be verified via System Manager. Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.



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



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



Session Manager Entity Link Connection Status

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

Status Details for the selected Session Manager:

All Entity Links for Session Manager: Session Manager

Summary View

14 Items Filter: Enable

	SIP Entity Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	CM-TG5	IPv4	10.64.91.87	5065	TLS	FALSE	UP	200 OK	UP
○	CM -TG6	IPv4	10.64.91.87	5066	TLS	FALSE	UP	200 OK	UP
○	CM-TG1	IPv4	10.64.91.87	5081	TLS	FALSE	UP	200 OK	UP
○	Avaya IX Messaging	IPv4	10.64.19.90	5061	TLS	FALSE	UP	200 OK	UP
○	SBCE-90 Vz1	IPv4	10.64.91.50	5061	TLS	FALSE	UP	200 OK	UP
○	CM-TG3	IPv4	10.64.91.87	5061	TLS	FALSE	UP	200 OK	UP
○	SBCE-70 Toll Free	IPv4	10.64.91.41	5061	TLS	FALSE	UP	200 OK	UP
○	SBCE-70 IPFR	IPv4	10.64.91.40	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
○	Experience Portal	IPv4	10.64.91.90	5061	TLS	FALSE	UP	200 OK	UP
○	Aura Messaging	IPv4	10.64.91.84	5061	TLS	FALSE	UP	200 OK	UP
○	SBCE-101	IPv4	10.64.91.101	5061	TLS	FALSE	UP	200 Keepalive	UP
○	SBCE-100 Vz2	IPv4	10.64.91.100	5061	TLS	FALSE	UP	200 OK	UP
○	CM-TG7	IPv4	10.64.91.87	5067	TLS	FALSE	UP	200 OK	UP
○	SBCE30 HA	IPv4	10.64.91.32	5061	TLS	FALSE	UP	200 OK	UP

Select : None

Other Session Manager useful verification and troubleshooting tools include:

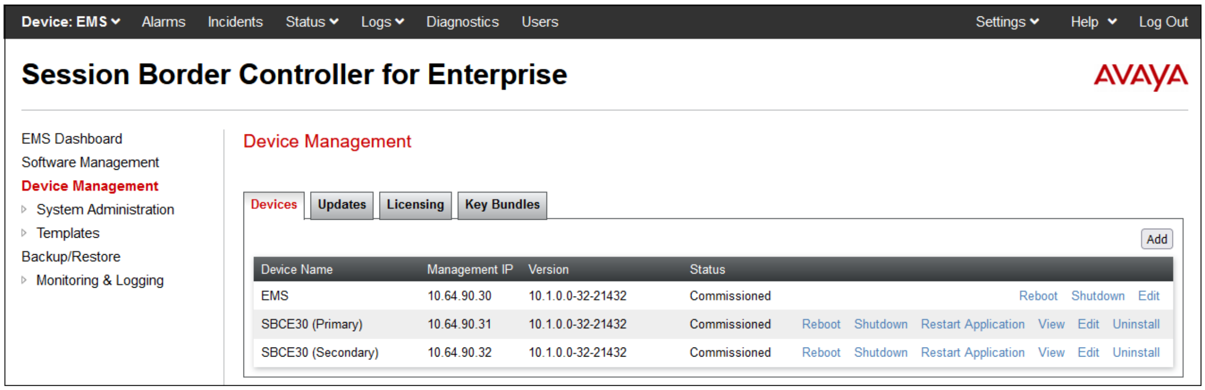
- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System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

9.4. Avaya Session Border Controller for Enterprise Verification

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

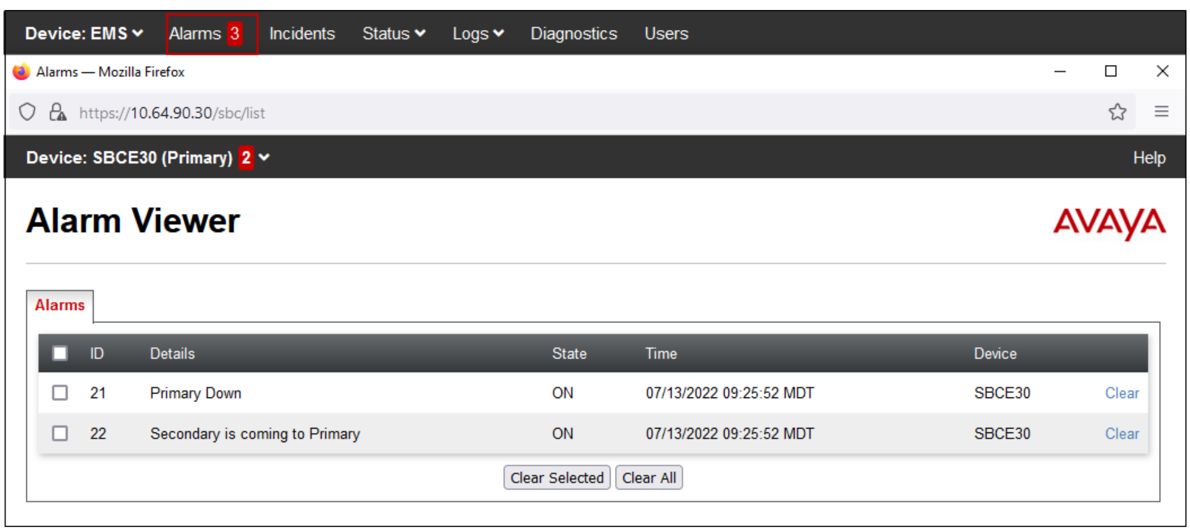
9.4.1. Device Management

The Device Management screen provides general information of the devices under control of the EMS, as well as the Primary / Secondary status of each SBCE appliance.



9.4.2. Alarms

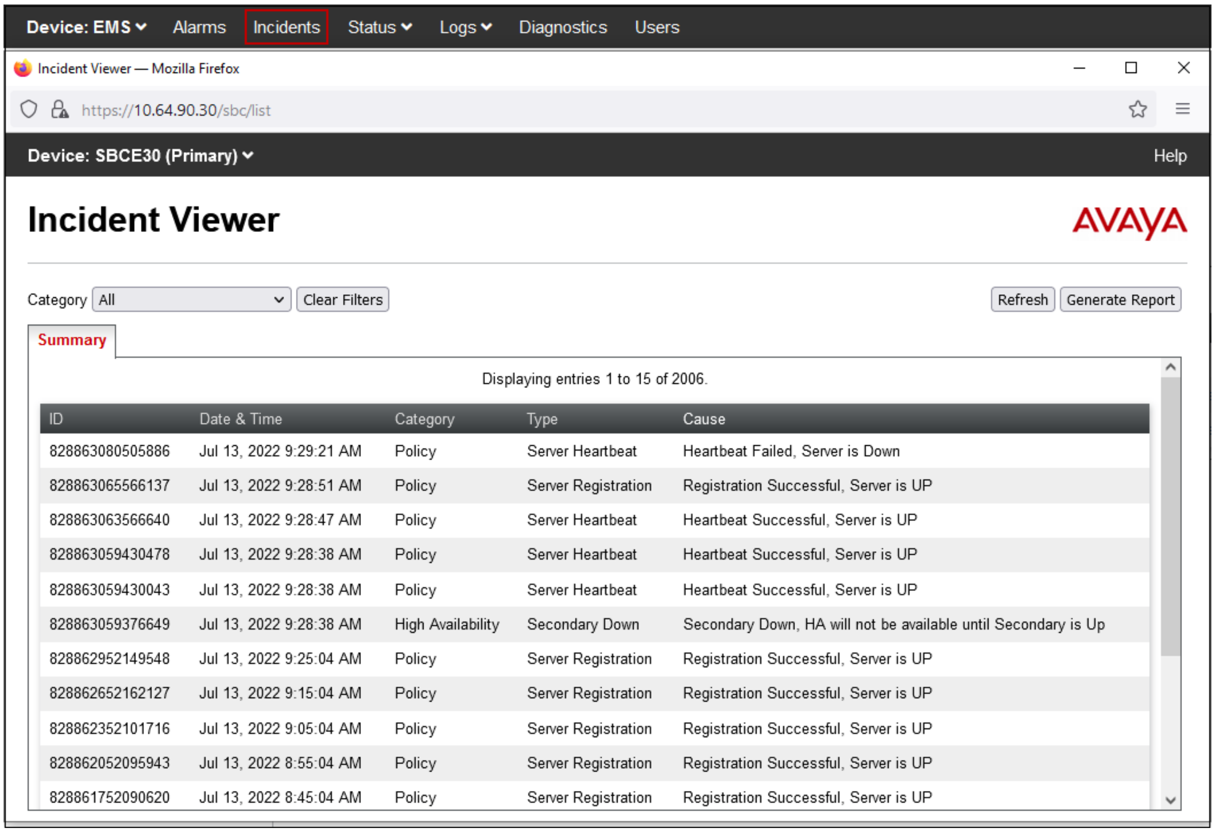
The Alarms log is accessed from the Avaya SBCE top navigation menu as highlighted in the screen shot below, and selecting the desired device.



9.4.3. Incidents

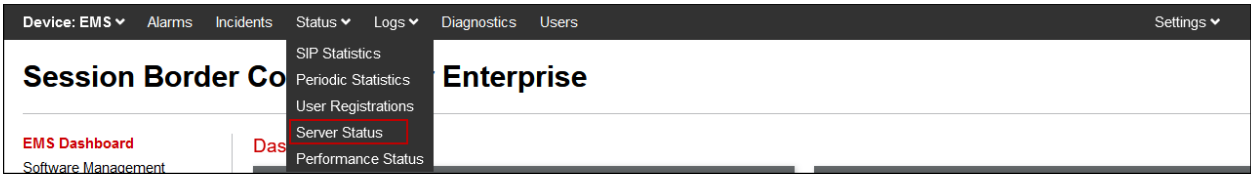
The Incident Viewer can be accessed from the Avaya SBCE top navigation menu and selecting the desired device.

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

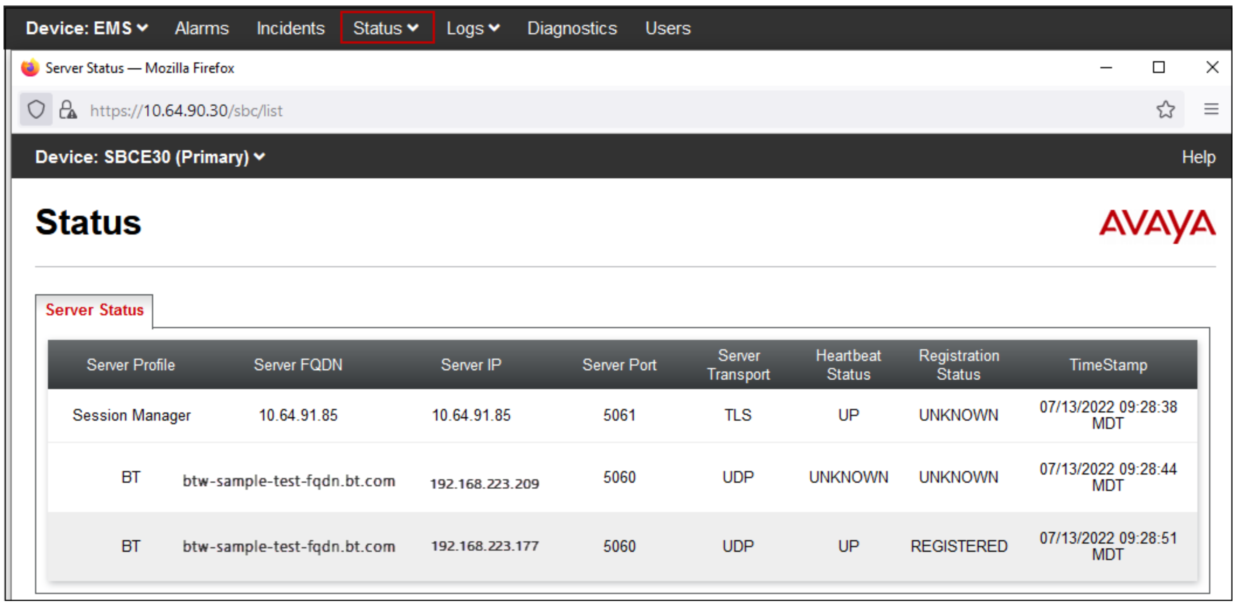


9.4.4. Server Status

The **Server Status** can be access from the Avaya SBCE top navigation menu by selecting the **Status** menu, **Server Status** and choosing the desired device.



The **Server Status** screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat or Registration to be enabled on the SIP Server Configuration profiles, as configured in **Section 7.8**.

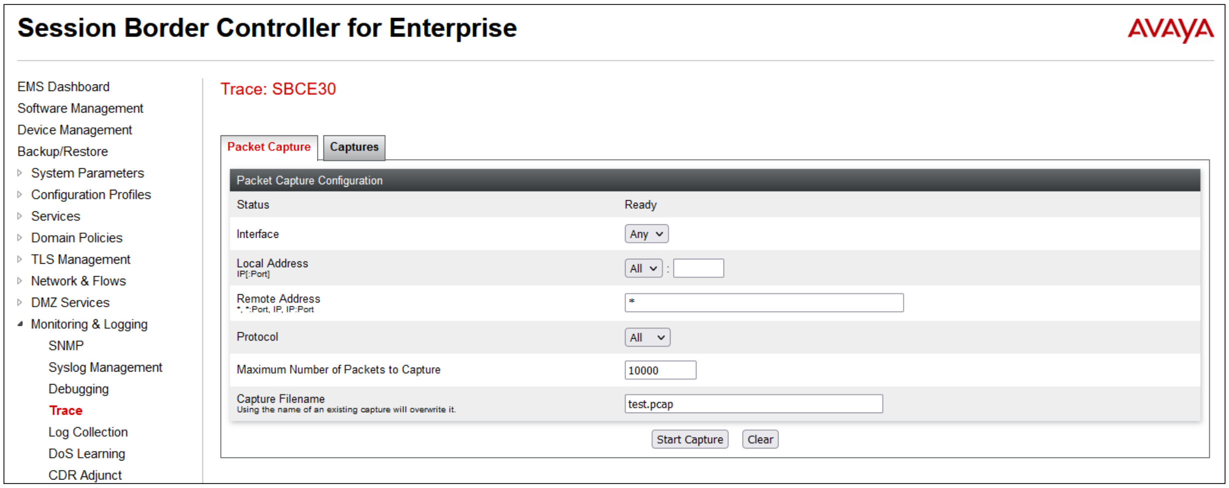


Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
Session Manager	10.64.91.85	10.64.91.85	5061	TLS	UP	UNKNOWN	07/13/2022 09:28:38 MDT
BT	btw-sample-test-fqdn.bt.com	192.168.223.209	5060	UDP	UNKNOWN	UNKNOWN	07/13/2022 09:28:44 MDT
BT	btw-sample-test-fqdn.bt.com	192.168.223.177	5060	UDP	UP	REGISTERED	07/13/2022 09:28:51 MDT

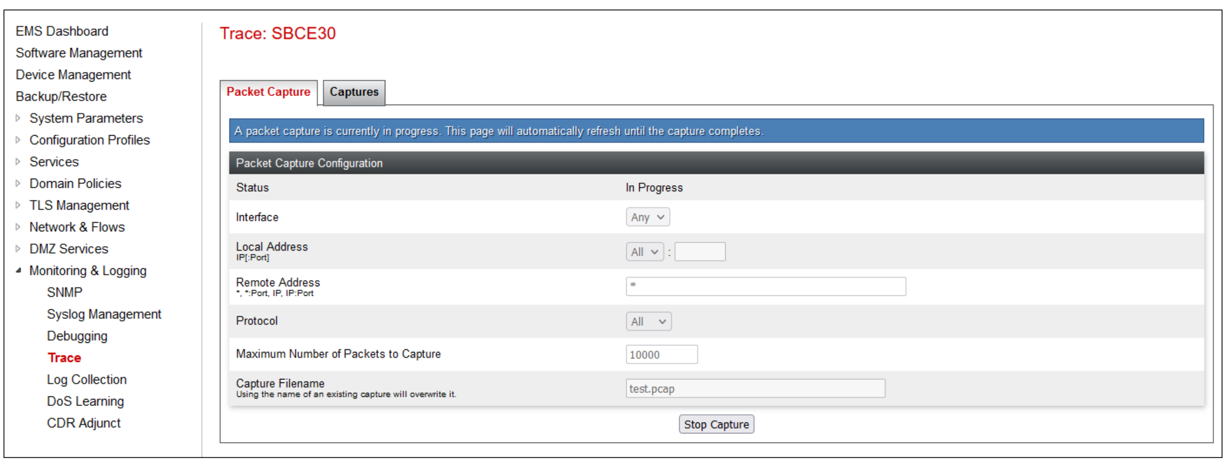
Note that the Avaya SBCE registers only with the BT server with the highest priority, retrieved from the DNS SRV query, as configured on **Section 7.8**.

9.4.5. Tracing

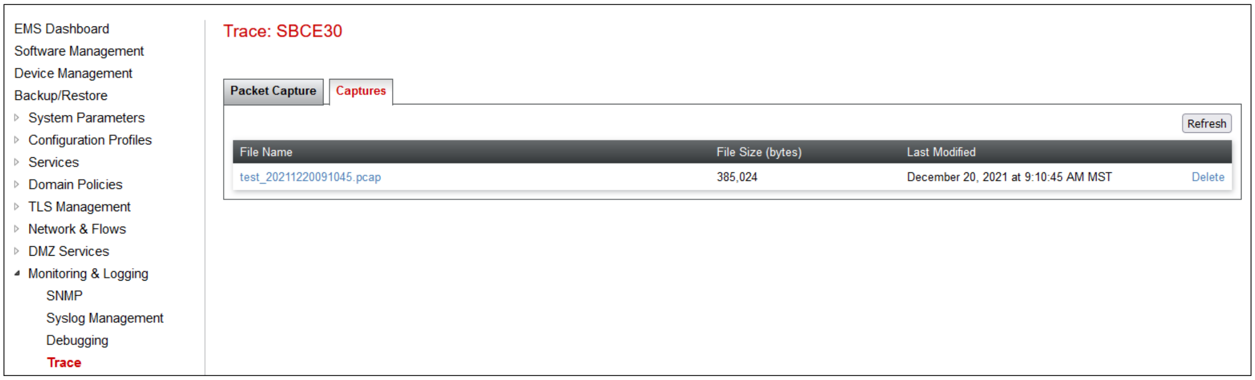
To take a call trace, navigate to **Monitoring & Logging → Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.



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



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



Also, the **traceSBC** tool can be used to monitor the SIP signaling messages between the Service provider and the Avaya SBCE. The tool is run from the SBCE CLI command.

10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller for Enterprise 10.1 in a High Availability configuration to connect to BT Wholesale Hosted SIP Trunking Service using Enterprise Trunks. The BT Wholesale Hosted SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 0**.

11. Additional References

This section references documentation relevant to these Application Notes. In general, Avaya product documentation is available at http://support.avaya.com.

Avaya Aura® Session Manager/System Manager

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

Avaya Aura® Communication Manager

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

Avaya Session Border Controller for Enterprise

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

12. Appendix B – Avaya SBCE – SigMa Script File

Details of the Signaling Manipulation script used in the configuration of the Avaya SBCE, in **Section 7.7**.

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

// Remove + from Diversion header
%HEADERS["Diversion"][1].URI.USER.regex_replace("\+","");

// Remove unsupported XML information
       remove(%BODY[1]);

    }
}
```

The optional Signaling Manipulation script below additionally includes the necessary header manipulation to support Class 5 CLIP, if the feature is to be enabled by BT and the user on the SIP trunk. Note that in the example, the Class 5 CLIP of 08001234567 was provided by BT during the testing.

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

//Remove + from Diversion header
%HEADERS["Diversion"][1].URI.USER.regex_replace("\+","");

// Remove unsupported XML information
       remove(%BODY[1]);

//Insert Pilot number in the FROM header for Class 5 CLIP
  %fromuser = %HEADERS["From"][1].URI.USER;
  %HEADERS["From"][1].URI.USER = "08001234567";

    }
}
```

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.