DevConnect Program

Application Notes for IBM Watson Assistant with Avaya Session Border Controller 10.1 and Avaya Aura® 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate IBM Watson Assistant with Avaya Session Border Controller 10.1 (Avaya SBC) and Avaya Aura® 10.1. Watson Assistant is a conversational artificial intelligence platform in the cloud, that interfaces with the Avaya SBC via SIP trunk. PSTN calls initially arrive to the Avaya Aura® Enterprise site and are routed out to the IBM Watson Assistant service via Avaya SBC and SIP trunk.

Watson Assistant interacts with callers to answer their questions and perform transactions using their voice in a conversational style. If required, Watson Assistant can transfer the call to an agent back at the enterprise via SIP REFER message, and provide context and screen pops via User-to-User Information (UUI).

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

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

©2023 Avaya Inc. All Rights Reserved.

Table of Contents

©2023 Avaya Inc. All Rights Reserved.

©2023 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the configuration steps required to integrate IBM Watson Assistant with Avaya Session Border Controller 10.1 and Avaya Aura® 10.1.

IBM Watson Assistant is a virtual assistant platform in the cloud, which provides an omni-channel experience regardless of how the user chooses to communicate, delivering a consistent, personalized, and convenient end-user experience without clients needing to migrate their technology stack. The assistant operates through a voice interface, which can be integrated with phone systems. It also operates in text-based forms, can be integrated into an SMS-based setting, and other messaging solutions like Facebook, Messenger, WhatsApp, etc.

In the solution under test, Watson Assistant interfaces with the Avaya SBC via SIP trunk. The Avaya SBC provides access to a contact center on Avaya Aura® Communication Manager and Avaya Aura® Session Manager at an enterprise site.

Watson Assistant interacts with callers to answer their questions and perform transactions using their voice in a conversational style. If required, the assistant can transfer the call to an agent back at the enterprise via SIP REFER message, and provide context and screen pops via User-to-User Information (UUI).

The general call flow is as follows:

1. Caller places a call from the PSTN to the Avaya Aura® enterprise site.
2. The call is then routed to Watson Assistant via a SIP trunk from the Avaya SBC to the IBM Voice Gateway in the cloud, using TLS-encrypted SIP signaling and SRTP media.
3. Caller interacts with Watson Assistant using their voice in a conversational style.
4. Upon request, Watson Assistant can transfer the call to a live agent via a SIP REFER, sending caller information (e.g., customer number and authentication status) in UUI. It is up to the client to use the UUI data, as needed, in the systems the agent uses.
5. The PSTN caller is connected to an agent.
6. The call to Watson Assistant is disconnected.

©2023 Avaya Inc. All Rights Reserved.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on customer calls to the enterprise site, being routed to IBM Watson Assistant via the Avaya SBC SIP trunk to the IBM Voice Gateway. A sample Watson Assistant application answered the calls and provide service to customers via voice commands. If required, Watson Assistant transferred the call via REFER to an agent on the enterprise, sending the User-to User information (UUI) in the Refer-To header.

The UUI sent by Watson Assistant was verified to be delivered by the Avaya SBC via SIP tracing, presented on agent deskphones via UUI button, and processed by Avaya Enablement Services using the Dashboard tool in AES.

The serviceability test cases focused on simulating a network outage and also a restart on the Avaya SBC. Calls to Watson Assistant were verified to complete successfully after the network was restored and Avaya SBC came back in service.

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 these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with this Application Note, the interface between Avaya SBC and IBM Watson Assistant used TLS encryption for SIP signaling, and SRTP encryption for the media.

TLS/SRTP encryption was also used internally on the enterprise between Avaya SBC and the Avaya Aura® servers and endpoints.

©2023 Avaya Inc. All Rights Reserved.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establish SIP trunk between Avaya SBC and Watson Assistant using TLS transport.
- Responses from Watson Assistant to SIP OPTIONS messages sent by Avaya SBC.
- Inbound PSTN calls routed from Communication Manager to the Avaya SBC and to the SIP trunk to Watson Assistant.
- IBM Watson Assistant providing service to callers via a sample IVR application, and callers able to navigate the application using their speech.
- Proper call transfers from Watson Assistant to an agent on the enterprise using REFER, when the caller request live agent assistance.
- Inbound transferred calls from Watson Assistant received on agents using Avaya SIP and H.323 Deskphones, as well as on Remote Workers agents logged into Session Manager via the Avaya SBC.
- Verify Watson Assistant provided User-to-User (UUI) information in the Refer-To header of REFER message when transferring call to live agents.
- Verify UUI data is presented on agent deskphones via UUI button, and processed by Avaya Enablement Services using the Dashboard tool.
- Proper disconnect when the call is abandoned by the caller before it is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Telephony features, such as holding and resuming calls to Watson Assistant, agents transferring calls to Watson Assistant, and adding Watson Assistant to a conference,
- SIP signaling encrypted using TLS 1.2.
- Audio encrypted using SRTP.
- Codec G.711U.
- Verify service is restored after a network outage.
- Verify service is restored after an Avaya SBC restart.

2.2. Test Results

Interoperability testing of IBM Watson Assistant with the Avaya solution was completed with successful results for all test cases. The following observations are noted for the sample configuration described in these Application Notes.

- **Response to SIP OPTIONS** − IBM Watson Assistant returns a “404 Not Found” to the OPTIONS sent by the Avaya SBC. This response is enough to keep the trunk in service on the Avaya SBC and does not have any effect on the service. IBM Watson Assistant does not send OPTIONS to the Avaya SBC.

2.3. Support

Technical support on IBM Watson Assistant can be obtained through the following:
Phone: +1 (866) 403-7638
Web: https://cloud.ibm.com/unifiedsupport/supportcenter

©2023 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the compliance testing.

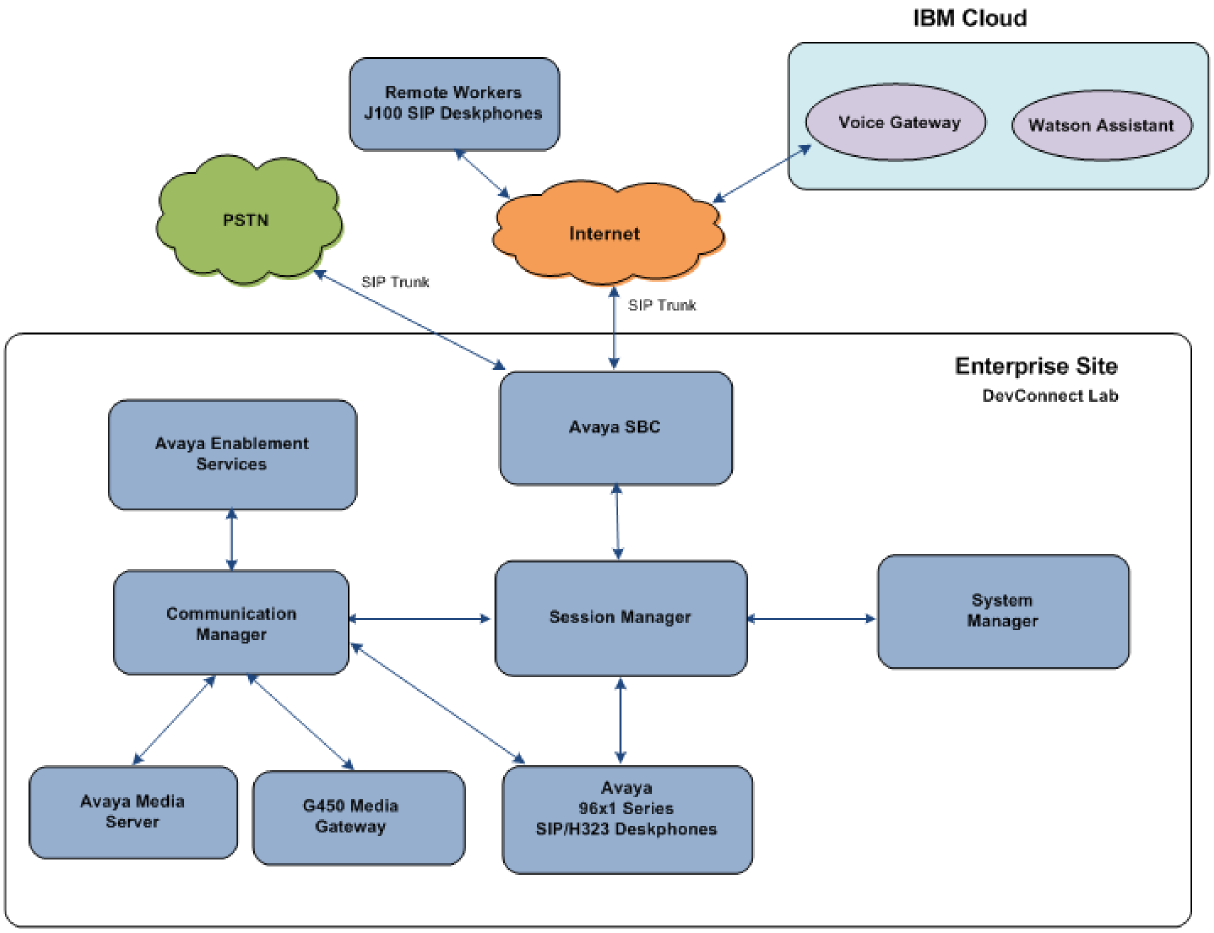


Figure 1: Test Configuration

A simulated enterprise site containing the Avaya SBC, Session Manager, Communication Manager and the rest of the Avaya Aura® infrastructure was installed at the DevConnect Lab. The Avaya SBC connected the enterprise site to IBM Watson Assistant via a TLS SIP trunk to the IBM Voice Gateway. All customer calls were initially routed from the PSTN through the enterprise site and then to Watson Assistant.

A PSTN carrier in the lab provided Direct Inward Dial (DID) 10-digit numbers. One of the DID numbers was mapped by Session Manager to the corresponding Communication Manager Vector Directory Number (VDN), where a vector routed the call to the number expected by Watson Assistant. In similar fashion, if Watson Assistant transferred the call via REFER back to an agent on the enterprise, the destination number contained in the Refer-To header of the REFER was matched to another VDN in Communication Manager, where a vector sent the call to an agent queue.

©2023 Avaya Inc. All Rights Reserved.

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

The following Avaya components were used in the reference configuration in the DevConnect Lab:

- Avaya Session Border Controller
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Enablement Services
- Avaya G430 Media Gateway
- Avaya Media Server
- Avaya 96X1 Series IP Deskphones using the SIP and H.323 software bundle
- J100 Series IP Deskphones using the SIP software bundle

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager	10.1.3.1.0716418 Service Pack 1 Hotfix 1013116418
Avaya Aura® Session Manager	10.1.3.1.1013103
Avaya Aura® Communication Manager	10.1.3.0.1-FP3P1 Update ID 01.0.974.0-27893
Avaya Session Border Controller	10.1.2.0-64-23285 HotFix-1
Avaya Aura® Enablement Services	10.1.3 (FP10.1.3.0.0.11) AES-10.1-SSP-013 (security patch)
Avaya Aura® Media Server	Media Server 10.1.0.154 Appliance Version 10.0.0.14
Avaya G450 Media Gateway	42.24
Avaya 96x1 Series IP Deskphone (H.323)	6.8.5.4.10
Avaya J100 IP Deskphones (J169, J179)	4.1.2.0.11
Avaya 96x1 Series IP Deskphone (SIP)	7.1.15.2.1

©2023 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® Communication Manager

This section covers the configuration steps required to establish a SIP trunk between Communication Manager and Session Manager. This trunk that will carry the calls to IBM Watson Assistant. Call routing configuration and sample VDN and vectors are also shown. Communication Manager is configured through the System Access Terminal (SAT).

Note – The initial installation, configuration, and licensing of the Avaya servers and media gateways for Communication Manager are assumed to have been previously completed and are not discussed in this document. Similarly, the configuration of the call center, including agents, skill/hunt group, etc. is outside the scope of these Application Notes.

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      1
         Maximum Administered Remote Office Trunks: 12000      0
Max Concurrently Registered Remote Office Stations:  2400      0
          Maximum Concurrently Registered IP eCons:  128       0
     Max Concur Reg Unauthenticated H.323 Stations:   100      0
                    Maximum Video Capable Stations:  36000     0
               Maximum Video Capable IP Softphones:   2400     1
                   Maximum Administered SIP Trunks: 12000    110
  Max Administered Ad-hoc Video Conferencing Ports: 12000      0
   Max Number of DS1 Boards with Echo Cancellation: 688        0
```


©2023 Avaya Inc. All Rights Reserved.

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

```
display system-parameters customer-options                      Page   4 of  12
                                OPTIONAL FEATURES

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

On **Page 5** of the form, verify that **IP Trunks** are enabled. Since SIP REFER messages will be used, verify that the **ISDN/SIP Network Call Redirection** feature is enabled. Since SRTP will be required, verify that the **Media Encryption Over IP** feature is enabled.

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

           IP Attendant Consoles? y
```


©2023 Avaya Inc. All Rights Reserved.

5.2. 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:
    - The digits **1**, **2**, **3**, **5** and **7** for Communication Manager extensions and VDNs.
- 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 form in **Section 5.6.2**.

```
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
```

5.3. 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 and Session Manager node names and IP address are entered during installation. Enter the **change node-names ip** command, and verify the node name and IP address for the following:

- Communication Manager (e.g., **procr** and **10.64.91.87**).
- Session Manager SIP signaling interface (e.g., **SM** and **10.64.91.85**).

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
AMS10               10.64.91.88
SM                  10.64.91.85
aes                 10.64.91.95
default             0.0.0.0
procr               10.64.91.87
```


©2023 Avaya Inc. All Rights Reserved.

5.4. IP Codec Set

Use the **change ip-codec-set x** command, where **x** is the number of an IP codec set used for calls between the enterprise and IBM Watson Assistant (e.g., **4**). Note the codec set number since it will be used in the IP Network Region covered in the next section. **G.711MU** was used. For the compliance test, **Media Encryption** was used internally on the enterprise between the Avaya SBC and Communication Manager, as shown below.

```
change ip-codec-set 4                                           Page   1 of   2

                          IP MEDIA PARAMETERS
    Codec Set: 4

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2:
 3:
 4:
 5:
 6:
 7:

     Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
```


©2023 Avaya Inc. All Rights Reserved.

5.5. IP Network Region

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 (not shown). To provide testing flexibility, network region **9** was associated with other components used specifically for the calls to IBM Watson Assistant..

Enter **change ip-network-region x**, where **x** is the number of an unused IP network region (e.g., region **4**). Populate the form with the following values:

- Enter a descriptive name (e.g., **Watson Assistant**).
- Enter the enterprise domain (e.g., **avayalab.com**) in the **Authoritative Domain** field.
- Enter **4** 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 4                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 4       NR Group: 1
Location: 1       Authoritative Domain: avayalab.com
    Name: Watson Assistant            Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 4              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
```


©2023 Avaya Inc. All Rights Reserved.

On **Page 4** of the form:

- Next to region **1** in the **dst rgn** column, enter **4** for the codec set (this means region 1 is permitted to talk to region 4 and it will use codec set 4 to do so). The **direct WAN** and **Units** columns will self-populate with **y** and **No Limit** respectively.
- Note that **dst rgn 4** is pre-populated with codec set **4** (from page 1 provisioning).
- Let all other values default for this form.

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

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


©2023 Avaya Inc. All Rights Reserved.

5.6. SIP Trunk to Session Manager

A new SIP Trunk (Trunk Group 4) was defined in the reference configuration between Communication Manager and Session Manager, to carry inbound and outbound traffic to Watson Assistant. This trunk will use TLS port 5064. Note that this port is different to the port assigned to other trunks to Session Manager. This is necessary so Session Manager can distinguish the traffic on the trunk to Watson Assistant, from the traffic on other trunks used on the enterprise.

5.6.1. Signaling Group 4

SIP trunks are defined on Communication Manager by provisioning a Signaling Group and a corresponding Trunk Group. Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **4**), and provision the following:

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**.
- The **Transport Method** field was 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 5.3**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.3** (e.g., **SM**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5064**.
- **Far-end Network Region** – Set the IP network region to **4**, as set in **Section 5.5**.
- **Far-end Domain** – Enter the enterprise domain, e.g., **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 **n**, indicating that Communication Manager should not use shuffling for media redirection on this trunk.

```
change signaling-group 4                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 4              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM                       Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: SM
 Near-end Listen Port: 5064                Far-end Listen Port: 5064
                                        Far-end Network Region: 4

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? n
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```


©2023 Avaya Inc. All Rights Reserved.

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

5.6.2. Trunk Group 4

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

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **Watson Assistant**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., ***04**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group previously administered (e.g., **4**).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **10**).

```
add trunk-group 4                                                Page   1 of  21
                                TRUNK GROUP

Group Number: 4                    Group Type: sip          CDR Reports: y
  Group Name: Watson Assistant              COR: 1        TN: 1        TAC: *04
   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: 4
                                                     Number of Members: 10
```

On **Page 3** of the **Trunk Group** form set **UUI Treatment** to **shared**. Accept all other defaults.

```
add trunk-group 4                                                Page   3 of  21
TRUNK FEATURES
             ACA Assignment? n           Measured: none
                                                        Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: public
                                               UUI Treatment: shared
                                             Maximum Size of UUI Contents: 128
                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no
               Send UCID? n



 Show ANSWERED BY on Display? y
```


©2023 Avaya Inc. All Rights Reserved.

On **Page 5** of the trunk group form, set **Telephone Event Payload Type** to **101**. All other fields retained their default values.

```
add trunk-group 4                                                   Page   5 of   5
                              PROTOCOL VARIATIONS
                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n

                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 101
                                       Shuffling with SDP? n

                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
     Resend Display UPDATE Once on Receipt of 481 Response? n
                        Identity for Calling Party Display: 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. Route Patterns

Route Patterns are used to direct outbound calls via the public or local CPE SIP trunks.
This form defines the public SIP trunk, based on the route-pattern selected by the AAR table next in **Section 5.8**. 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 14 is used for calls to IBM Watson Assistant.

Enter the **change route-pattern x** command, where **x** is the number of an unused route pattern (e.g., **14**).to configure a route pattern for calls to IBM Watson Assistant and enter the following parameters:

- In the **Grp No** column, enter 4 for trunk group 4.
- In the **FRL** column enter **0** (zero).
- In the **Numbering Format** column, enter **pub-unk**.

```
change route-pattern 14                                           Page   1 of   3
                    Pattern Number:14      Pattern Name: To Watson Assistant
    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: 4    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                                 pub-unk  none
```


©2023 Avaya Inc. All Rights Reserved.

5.8. AAR Call Routing

In the testing environment, **31000** was the provisioned number which needs to be dialed on the enterprise across the SIP trunk to reach the IBM Watson Assistant. Configure the **Uniform Dial Plan** to steer calls to Watson Assistant to AAR as shown below.

```
change uniform-dialplan 3                                       Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                           Insert                Node
  Pattern             Len Del        Digits       Net Conv Num
 31000                5   0                       aar n
```

SIP calls to Session Manager are routed over the SIP trunk via AAR call routing. Configure the AAR analysis form and add an entry to route calls to **31000** to use **Route Pattern 9** as shown below.

```
change aar analysis 31000                                          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
    31000                 5    5      14        aar          n
```


©2023 Avaya Inc. All Rights Reserved.

5.9. Call Center and Vectors

For the compliance test, a basic call center was configured on Communication Manager, consisting of agents, hunt/skill group, VDNs, and vectors. The call center configuration is outside the scope of these Application Notes and will not be covered. The sample vectors used are shown to illustrate the call flows.

Device Type	Extension
VDN Inbound Call	10041
VDN REFER	21014
Skill Group	1
Agent IDs	20001, 20002

Inbound PSTN calls are routed to VDN 10041. This VDN is mapped to vector **41**, shown below. The vector routes the call to **31000**, sending the call to Communication Manager Trunk Group 4 to Session Manager for Watson Assistant,

```
change vector 41                                                Page   1 of   6
                                  CALL VECTOR

    Number: 41              Name: PSTN Inbound to IBM
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 route-to     number 31000                    cov n if unconditionally
03
04
```

Watson Assistant can transfer the call to a live agent by sending a SIP REFER. In the example of the reference configuration, 21014 was the number provisioned in Watson Assistant to be sent in the Refer-To header of the REFER. The following vector was invoked when VDN 21014 is called. The vector queues the call to skill group **1** to route the call to an available agent, or if no agent is available plays music to the caller until one becomes available.

```
change vector 15                                                Page   1 of   6
                                  CALL VECTOR

    Number: 15              Name: basic queue
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 queue-to     skill 1    pri h
03 wait-time    30  secs hearing music
14 goto step    2              if unconditionally
03 stop
```


©2023 Avaya Inc. All Rights Reserved.

6. Configure Avaya Aura® Session Manager

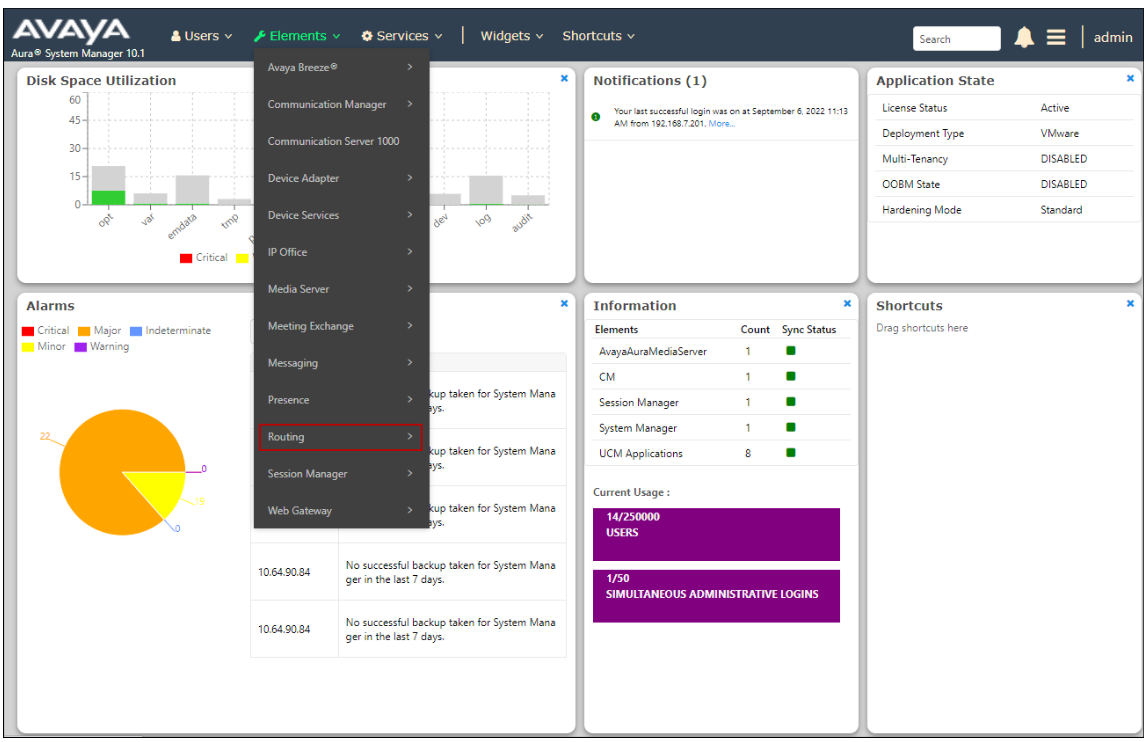
This section provides the procedures for configuring Session Manager. The procedure includes adding the following items:

- SIP Domain
- Locations
- SIP Entities for Communication Manager and Avaya SBC
- Entity Links, which defines the SIP trunk parameters used by Session Manager when routing calls to/from Communication Manager and Avaya SBC
- Routing Policies and Dial Patterns

Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult the documentation in Additional References section for further details.

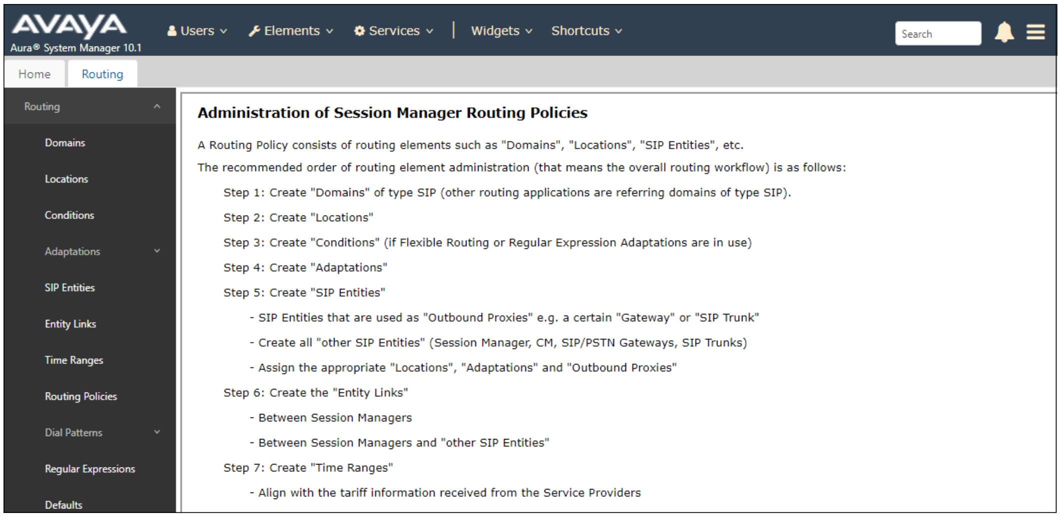
6.1. System Manager Login and Navigation

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**.



©2023 Avaya Inc. All Rights Reserved.

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 used. 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.

©2023 Avaya Inc. All Rights Reserved.

6.3. Locations

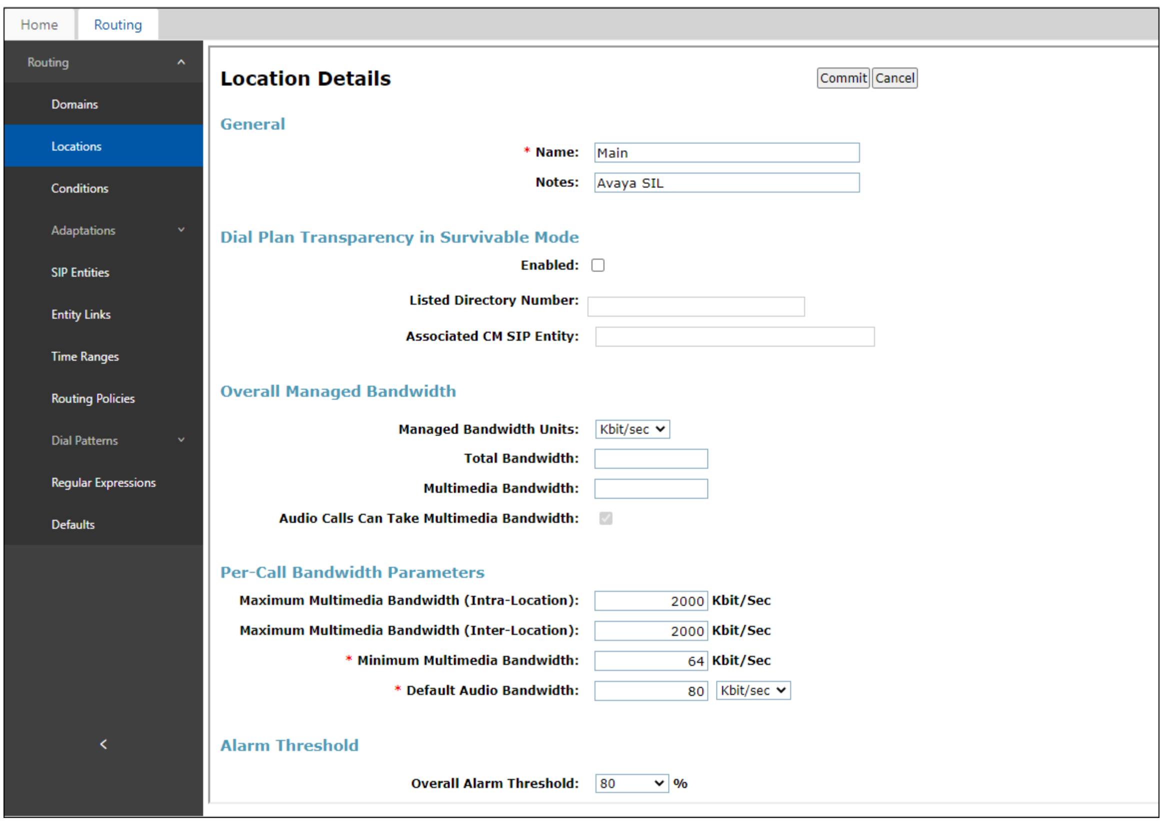
Locations identify logical and/or physical locations where SIP Entities reside, used for routing purposes. In the reference configuration, three locations are specified:

- **Main** – The customer site containing System Manager, Session Manager and other local servers and SIP endpoints.
- **CM-TG-4** – Communication Manager trunk group 4, designated for Watson Assistant calls.
- **SBCs** – Avaya SBC

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.
- Click **Commit** to save.



©2023 Avaya Inc. All Rights Reserved.

6.3.2. CM-TG4 Location

To configure the Communication Manager Trunk Group 4 location, repeat the steps in **Section 6.3.1** with the following changes (not shown):

- **Name:** Enter a descriptive name for the Location (e.g., **CM-TG-4**).

6.3.3. SBCs Location

To configure the Avaya SBC 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. SIP Entities

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

- Session Manager (**Section 6.4.1**) − This SIP Entity should be existing in the configuration, defined during the Session Manager installation.
- Communication Manager trunk access to IBM Watson Assistant (**Section 6.4.2**) – This entity, and its associated Entity Link (using TLS with port 5064), is for traffic between Communication Manager and Session Manager associated to Watson Assistant calls.
- Avaya SBC (**Section 6.4.3**) – This entity, and its associated Entity Link (using TLS and port 5061), is for traffic between Session Manager and the Avaya SBC associated to Watson Assistant calls.

Note – In the reference configuration, TLS is used as the transport protocol between Session Manager and Communication Manager (ports 5064), and to the Avaya SBC (port 5061). The connection between the Avaya SBC and the IBM Voice Gateway uses TLS port 5061 per IBM requirements.

©2023 Avaya Inc. All Rights Reserved.

6.4.1. Avaya Aura® Session Manager SIP Entity

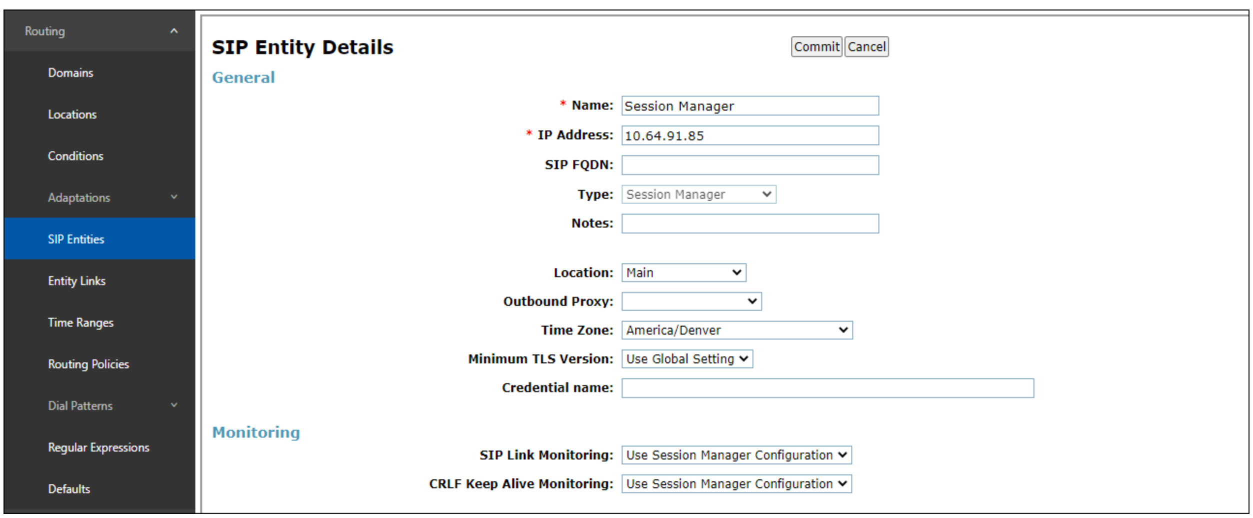
This SIP Entity should be already existing in the configuration, defined during the Session Manager installation. It is shown here for completeness.

In the left pane under **Routing**, click on **SIP Entities**. The screen below shows the Session Manager SIP Entity details in the reference configuration:

- **Name –** A descriptive name (e.g., **Session Manager**).
- **FQDN or IP Address –** This is 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** – Leave blank.
- **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**).

The **Monitoring** section of the **SIP Entity Details** page is configured as follows:

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

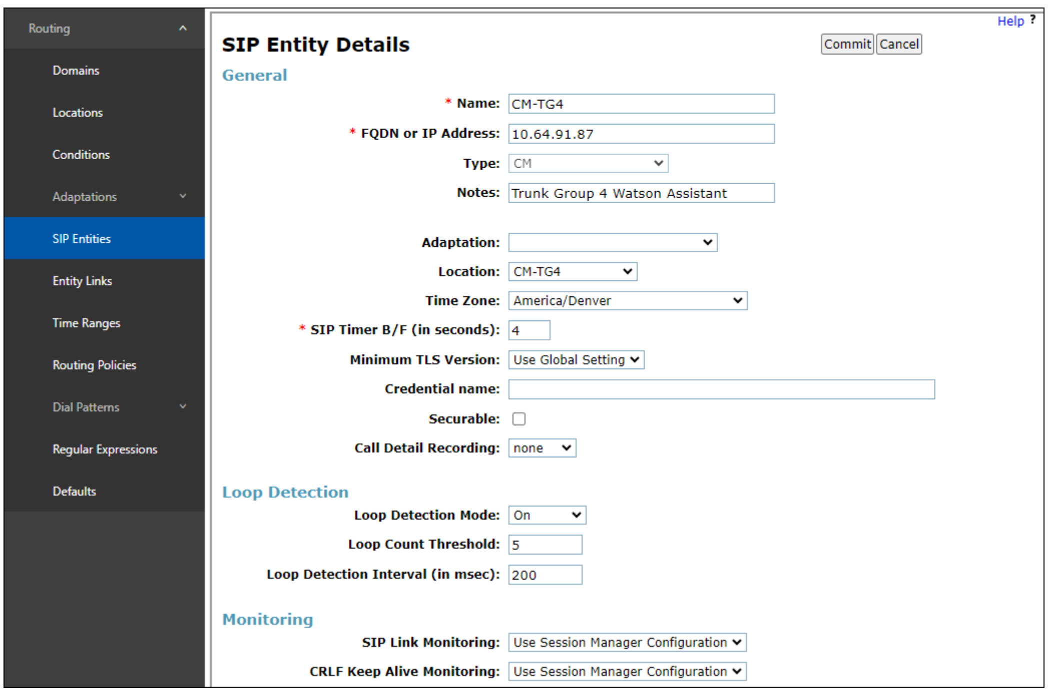


©2023 Avaya Inc. All Rights Reserved.

6.4.2. Avaya Aura® Communication Manager SIP Entity – Trunk Group 4

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-TG4**).
- **FQDN or IP Address –** Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Section 5.3** (e.g., **10.64.91.87**).
- **Type –** Select **CM**.
- **Location** – Select the **CM-TG4** Location administered in **Section 6.3.2**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **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**.

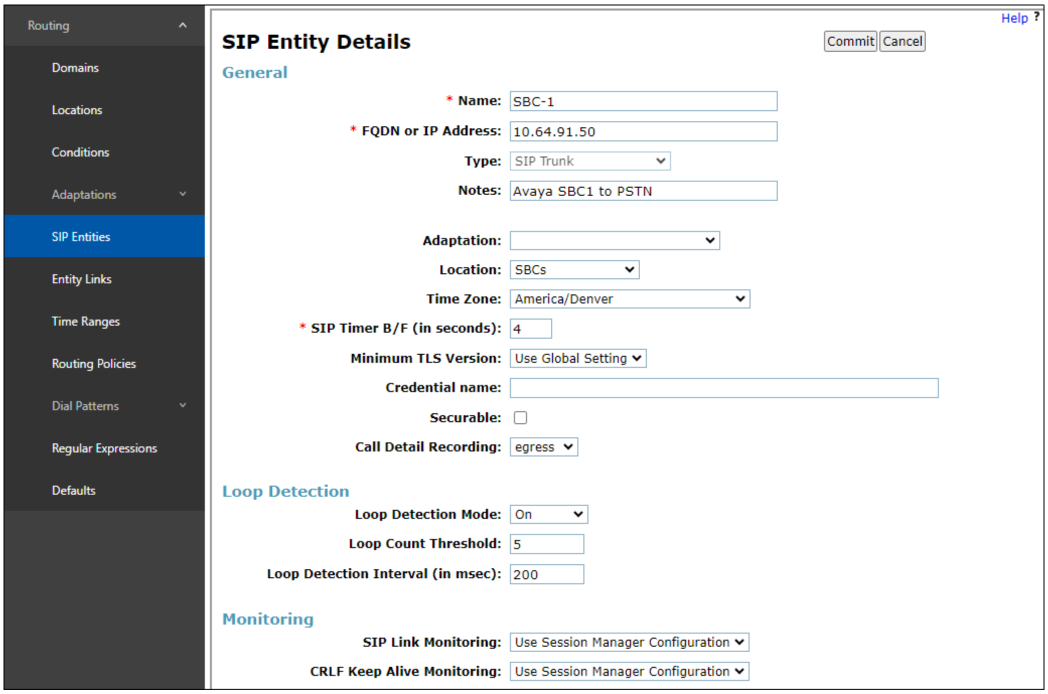


©2023 Avaya Inc. All Rights Reserved.

6.4.3. Avaya Session Border Controller SIP Entity

Repeat the steps in **Section 6.4.2** with the following changes:

- **Name –** Enter a descriptive name (e.g., **SBC-1**).
- **FQDN or IP Address –** Enter the IP address of the A1 (private) interface of the Avaya SBC (e.g., **10.64.91.50**, see **Section 7.4**).
- **Type –** Select **SIP Trunk**.
- **Location –** Select Location **SBCs** administered in **Section 6.3.3**.



Note – The Avaya SBC SIP Entity and associated Entity Link were already defined in the reference configuration, in use for other SIP trunks. They are reused in the configuration for the Watson Assistant trunk.

©2023 Avaya Inc. All Rights Reserved.

6.5. Entity Links

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

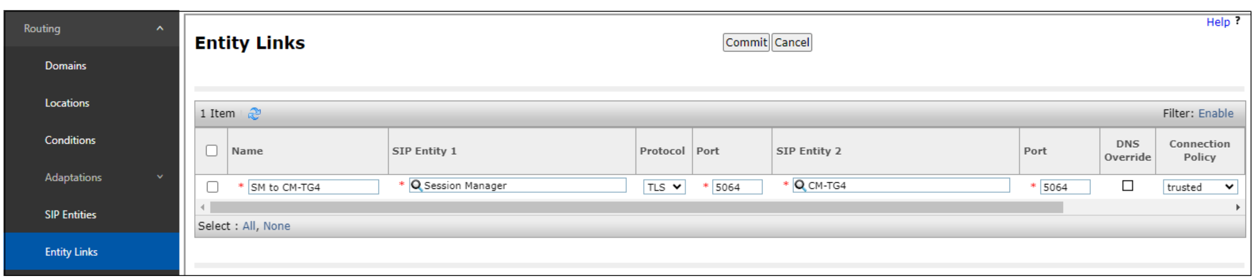
- Session Manager to Communication Manager Trunk Group 4 (**Section 6.5.1**).
- Session Manager to Avaya SBC (**Section 6.5.2**).

Note – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages configured in **Section 6.4**.

6.5.1. Entity Link to Avaya Aura® Communication Manager Trunk Group 4

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 TG4**).
- SIP Entity 1 – Select the SIP Entity administered in **Section 6.4.1** for Session Manager (e.g., Session Manager).
- **Protocol** – Select **TLS** (see **Section 5.6.1**).
- SIP Entity 1 **Port** – Enter **5064**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.4.2** for the Communication Manager trunk entity (e.g., **CM-TG4**).
- SIP Entity 2 **Port** – Enter **5064** (see **Section 5.6.1**).
- **Connection Policy** – Select **trusted**.
- Leave other fields as default.
- Click on **Commit**.

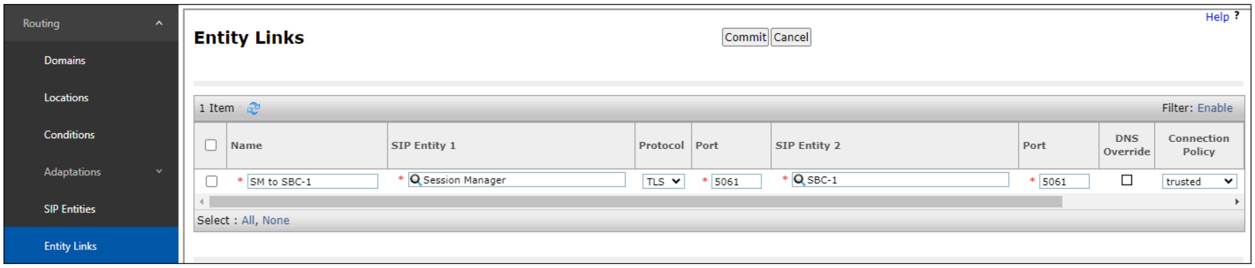


©2023 Avaya Inc. All Rights Reserved.

6.5.2. Entity Link to the Avaya SBC

To configure this Entity Link, repeat the steps in **Section 6.5.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBC (e.g., **SM to SBC-1**).
- **Protocol** – Select **TLS**.
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.4.3** for the Avaya SBC entity (e.g., **SBC-1**).
- **SIP Entity 2 Port** – Enter **5061**.



©2023 Avaya Inc. All Rights Reserved.

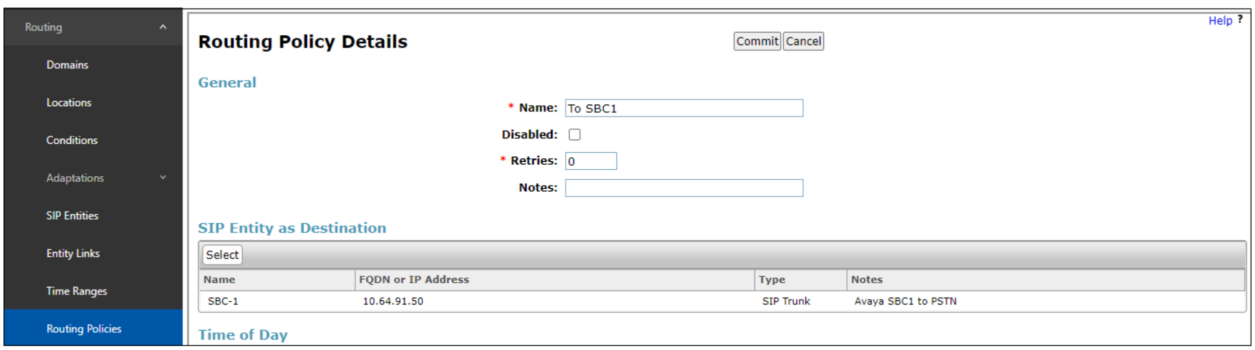
6.6. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**.

Note – The following routing policy for outbound calls to the Avaya SBC was already in place in the reference configuration, and was reused for the outbound calls via the Avaya SBC to IBM Watson Assistant.

In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** or click the policy if already exists (not shown).

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** (e.g., **To SBC1**), 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 (not shown) and select the SIP Entity administered in **Section 6.4.3** for the Avaya SBC.



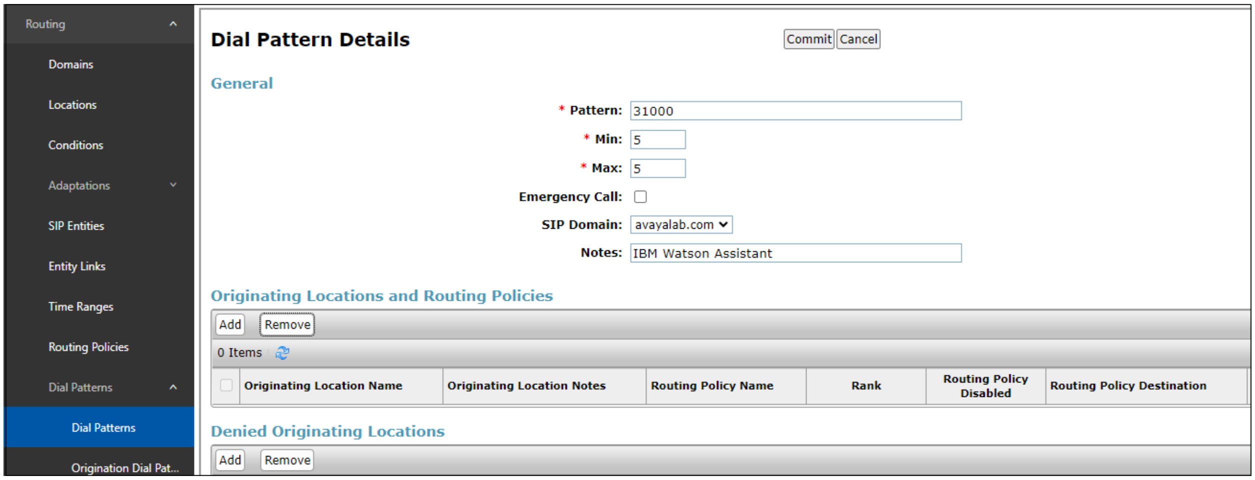
Note – Since call transfers from Watson Assistant to Avaya agents is achieved via in-dialog REFER messages, there was no need to create an inbound routing policy to Communication Manager Trunk Group 4.

6.7. Dial Patterns

Dial patterns are defined to direct calls to the appropriate SIP Entity. In the sample configuration, dial pattern 31000 was routed to the IBM Watson Assistant, through the Avaya SBC.

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. In the **General** section of the **Dial Pattern Details** page, provision the following:

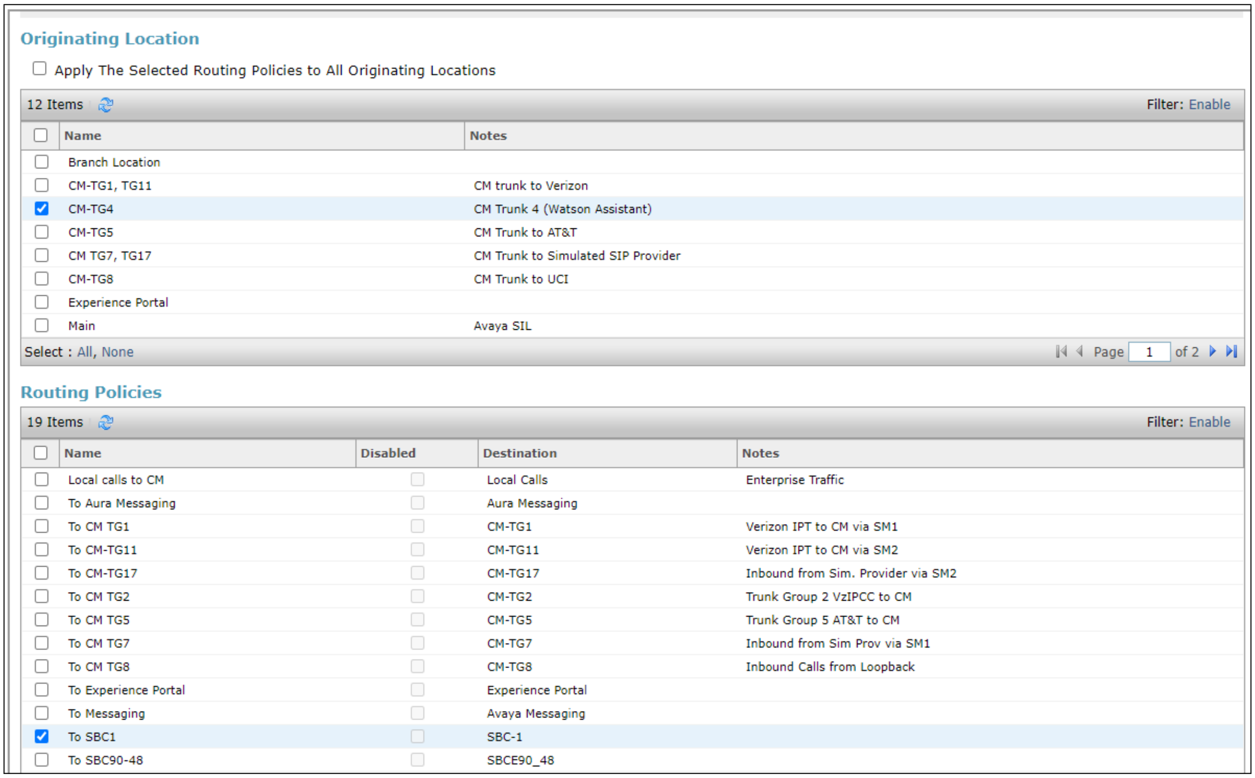
- **Pattern** – Enter the dialed number or prefix (e.g., **31000**).
- **Min** and **Max** – Minimum and maximum length of dialed number (e.g., **5)**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.



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

©2023 Avaya Inc. All Rights Reserved.

- Under **Originating Location**, click the checkbox corresponding to the Communication Manager location for the trunk group used for Watson Assistant calls, e.g., **CM-TG4**.
- In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy administered for routing calls to the Avaya SBC (e.g., **to SBC1**) and click on **Select** (not shown).



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

©2023 Avaya Inc. All Rights Reserved.

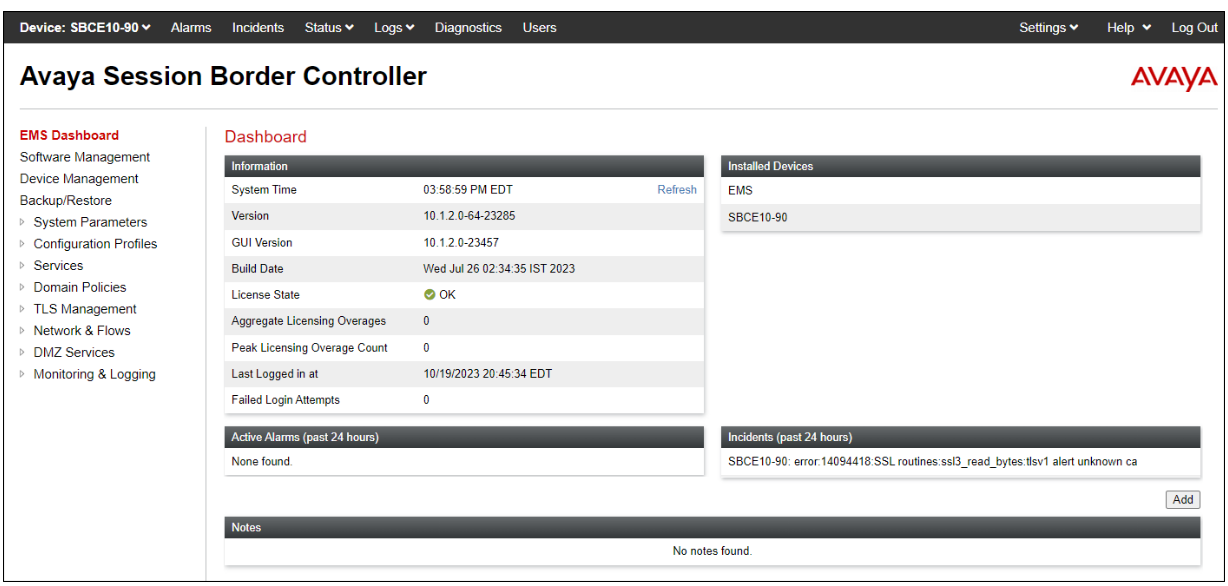
7. Configure Avaya Session Border Controller

This section covers the configuration of the Avaya SBC. It is assumed that the initial provisioning of the Avaya SBC, including the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and provisioning of the Avaya SBC consult the 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 SBC. Log in using the appropriate credentials.

Note: This section will focus on the Avaya SBC routing and connectivity to Session Manager and IBM Watson Assistant. Other configuration for PSTN trunks, remote workers, etc. is not covered. For security reasons, public IP addresses and FQDNs will be redacted in these Application Notes.

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



©2023 Avaya Inc. All Rights Reserved.

7.1. TLS Management

Note – The Avaya SBC in the test configuration used identity certificates signed by Avaya System Manager for the TLS internal connections to Session Manager and other Avaya systems. The procedure to create and obtain these certificates, and the creation of TLS Client and Server Profiles for these internal connections is outside the scope of these Application Notes.

In the reference configuration, TLS transport is used for the communication between the Avaya SBC and IBM Watson Assistant. This section covers the installation of the root certificate and the configuration of the TLS client profile, used in the connection to IBM Watson Assistant.

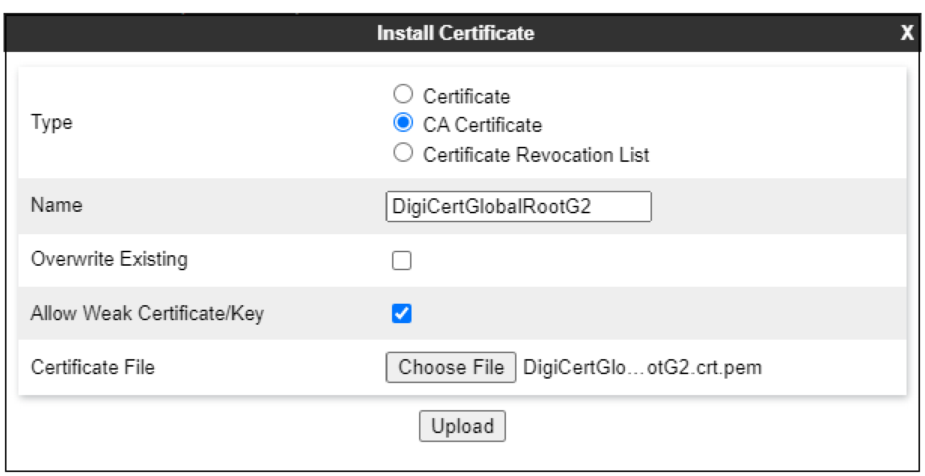
7.1.1. Install CA Certificate

The TLS connection from Avaya SBC to IBM Watson Assistant uses a server authentication scheme. In this method of connection, the client (Avaya SBC) initiates a request to the server for a secure session. The server then sends its identity certificate to the client. The client checks the received server identity certificate against the trusted Certification Authority (CA) certificates that are saved in its trust store, to verify that the server identity certificate is signed by a CA that the client trusts. DigiCert was used as the trusted CA by IBM Watson Assistant, so the DigiCert Global Root G2 certificate needed to be downloaded and imported into Avaya SBC trust store.

Note – The DigiCertGlobalRootG2 certificate may have been installed by default on the Avaya SBC. If the certificate is already listed under Installed CA Certificates, proceed to **Section 7.1.2**.

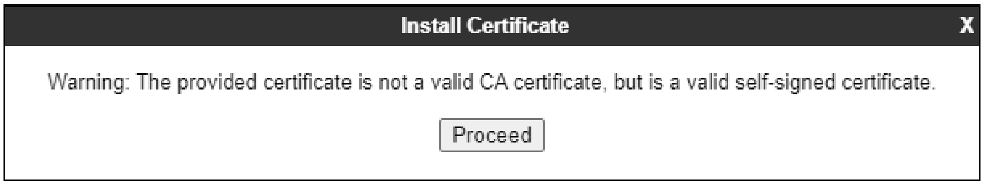
Navigate to **TLS Management → Certificates** and select **Install**.

- Type: select **CA Certificate**.
- Enter a **Name** for the certificate, i.e., **DigiCertGlobalRootG2** was used in the reference configuration, matching the filename of the DigiCert Global Root G2 CA certificate that was previously downloaded. This is not a requirement, as the name of the certificate could be made something different, but it was done in this way for clarity.
- Check the **Allow Weak Certificate/Key** box.
- **Certificate File**: browse and select the file previously downloaded.
- Click **Upload**.



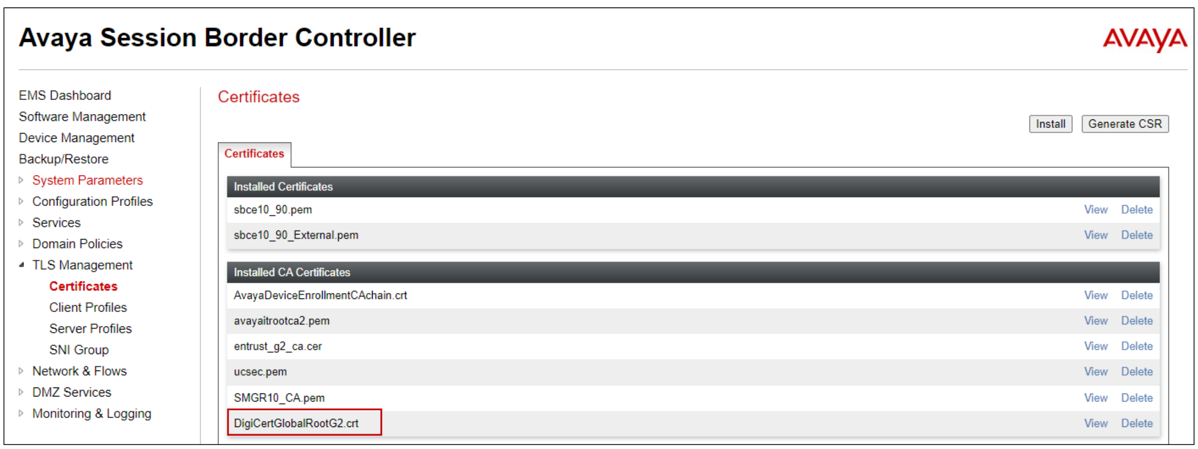
©2023 Avaya Inc. All Rights Reserved.

The **Install Certificate** window displays this message:



- Click the **Proceed** button.
- A window displays the certificate details. Click the **Install** button (not shown).
- An Install Certificate window displays this message: “CA Certificate installation successful.”
- Click the **Finish** button.

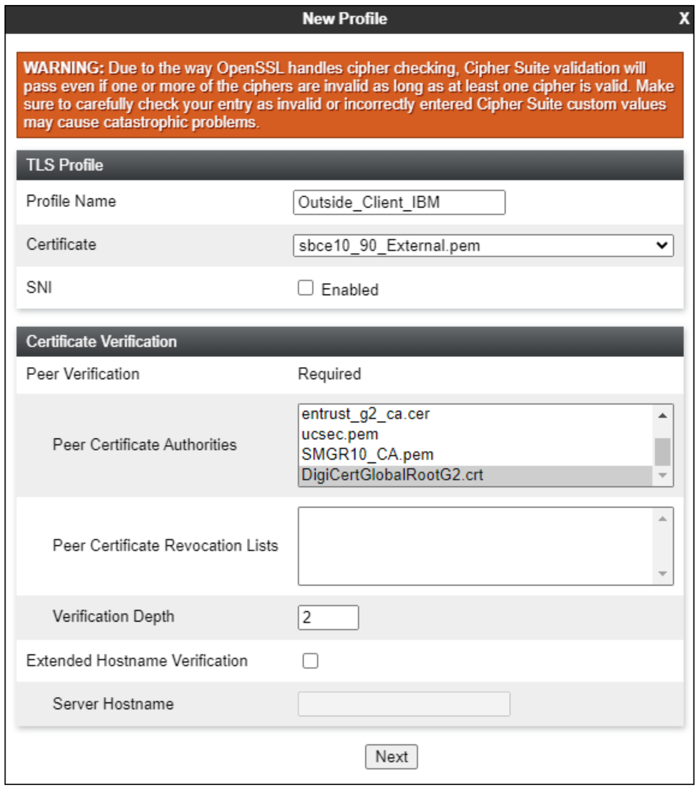
The screen below shows the installed certificate:



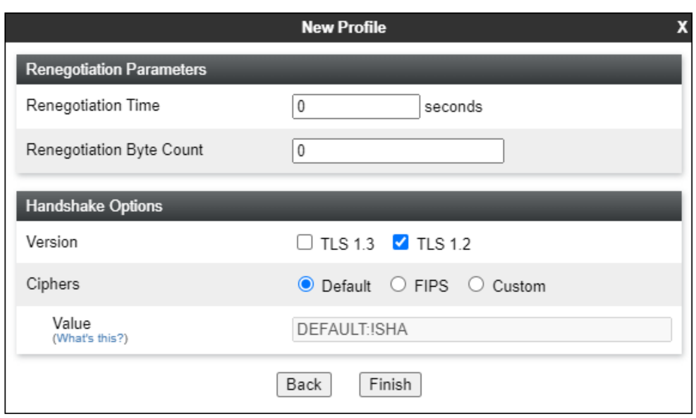
7.1.2. Client Profile for Watson Assistant

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

- **Profile Name:** enter descriptive name.
- **Certificate:** select the existing SBC identity certificate from the pull-down menu.
- **Peer Verification** = **Required**.
- **Peer Certificate Authorities:** Select the **DigiCertGlobalRootG2.pem** certificate.
- **Verification Depth:** enter **2**.
- Click **Next**.

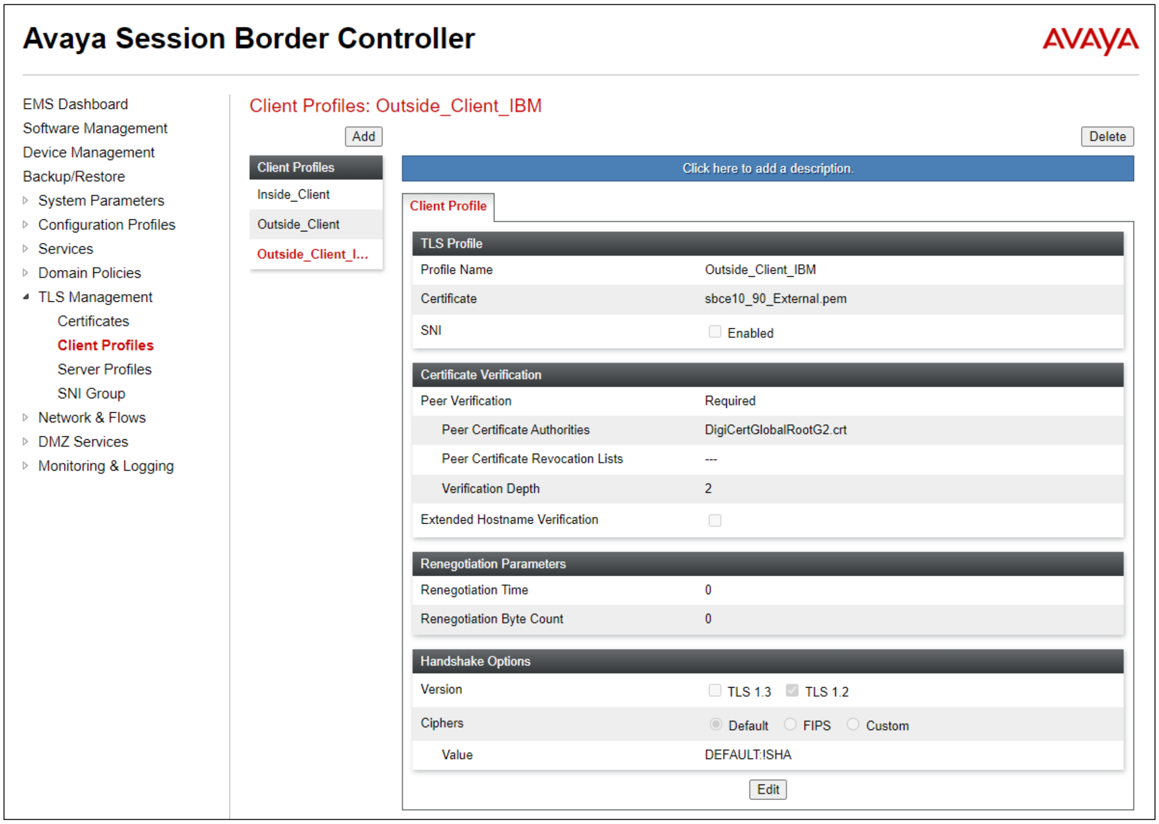


Uncheck the **TLS 1.3** box on next screen and click **Finish**.



©2023 Avaya Inc. All Rights Reserved.

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

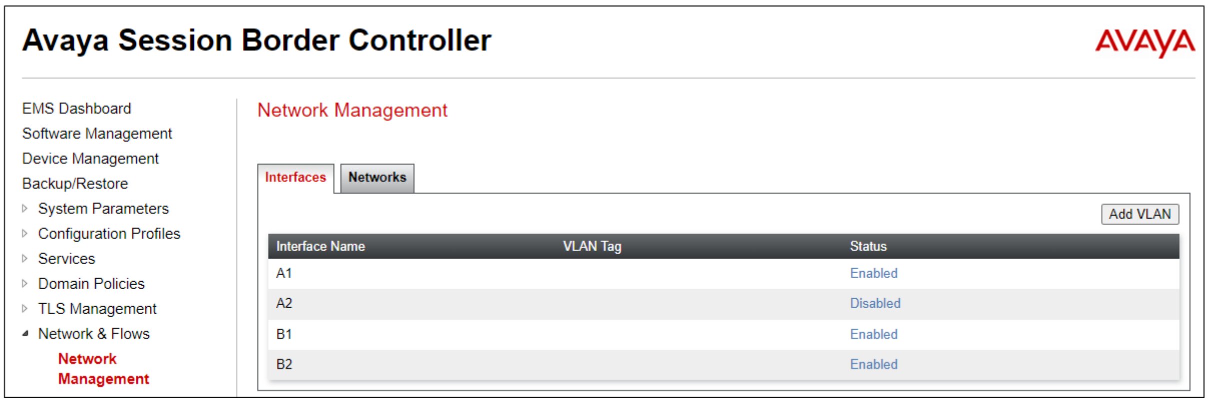


©2023 Avaya Inc. All Rights Reserved.

7.2. Network Management

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

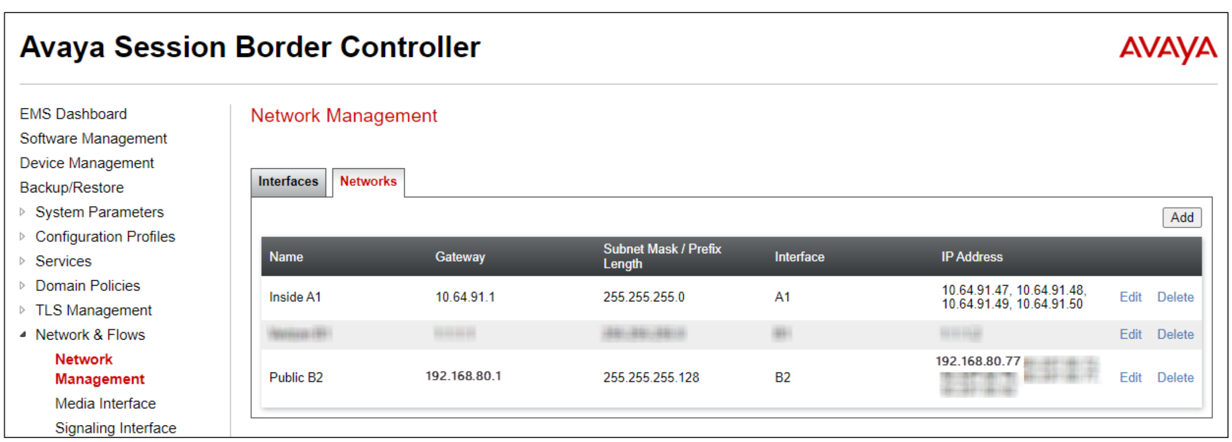
Select **Networks & Flows → Network Management** from the menu on the left-hand side. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 and B2 are used.



Select the **Networks** tab to display the IP provisioning for the A1 and B2 interfaces. Some of these values are specified during installation. Addresses can be added, modified or deleted by selecting **Edit** on each interface.

The following IP addresses were assigned to be used by Watson Assistant traffic:

- **A1**: **10.64.91.50** – "Inside" IP address, toward Session Manager.
- **B2: 192.168.80.77** – "Outside" IP address toward the SIP trunk to IBM Watson Assistant.



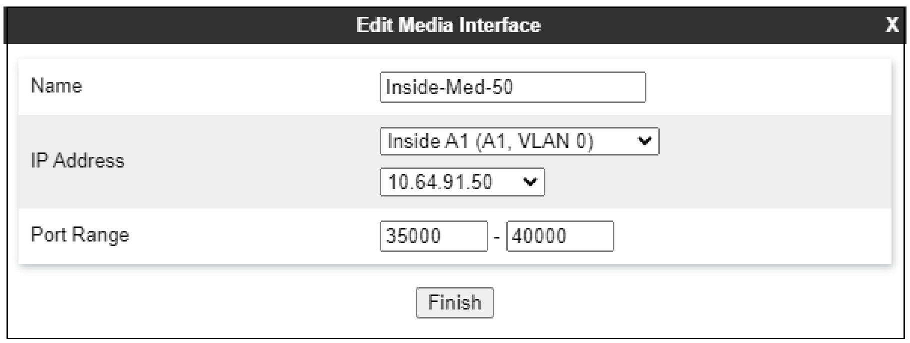
©2023 Avaya Inc. All Rights Reserved.

Note: Public IP addresses and FQDNs used in the reference configuration have been masked or changed to private IP addresses for security reasons.

7.3. Media Interfaces

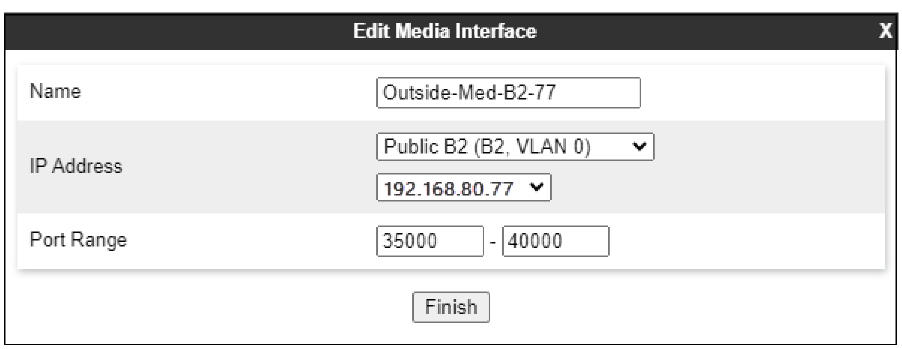
To add to the internal media interface toward the enterprise select **Network & Flows → Media Interface** from the menu on the left-hand side. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name**: Enter an appropriate name (e.g., **Inside-Med-50**).
- **IP Address**: Select **Inside-A1 (A1,VLAN0)** and the IP address used for traffic towards Communication Manager (e.g., **10.64.91.50**) from the drop-down menus.
- **Port Range**: **35000** – **40000**.
- Click **Finish**.



Select **Add** (not shown) to add to the external media interface toward Watson Assistant.
Enter the following:

- **Name**: Enter an appropriate name (e.g., **Outside-Media-B2**).
- **IP Address**: Select **Public B2 (B2, VLAN0)** and the IP address used for the SIP trunk to Watson Assistant (e.g., **192.168.80.77**) from the drop-down menus.
- **Port Range**: **35000** – **40000**.
- Click **Finish**.

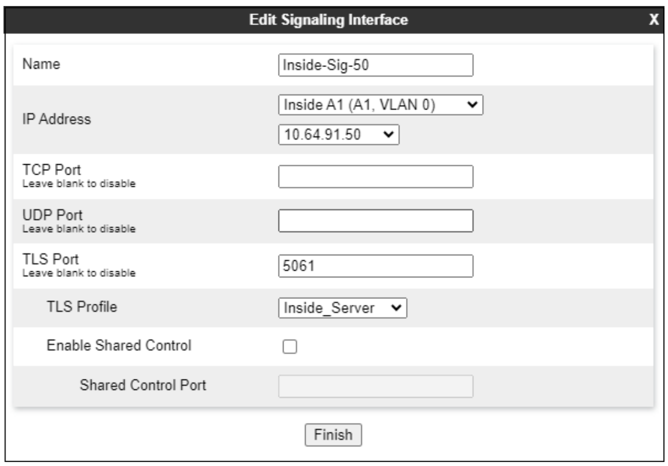


©2023 Avaya Inc. All Rights Reserved.

7.4. Signaling Interfaces

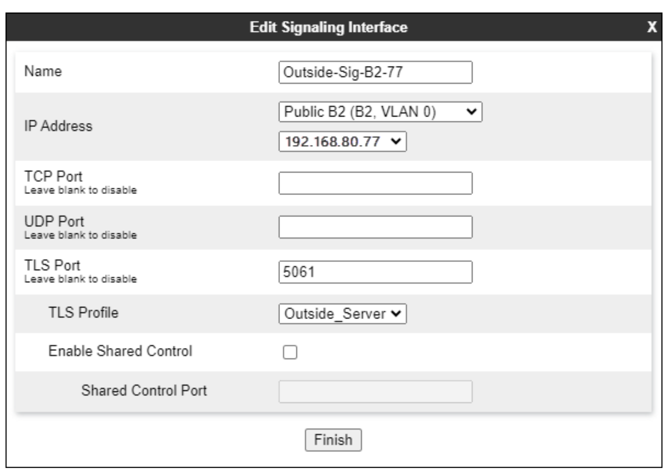
Select **Network & Flows → Signaling Interface** from the menu on the left-hand side.
Select **Add** (not shown) to add to the internal signaling interface toward the enterprise. Enter the following:

- **Name**: Enter an appropriate name (e.g., **Inside-Sig-50**).
- **IP Address**: Select **Inside A1 (A1, VLAN0)** and **10.64.91.50**.
- **TLS Port**: **5061**.
- **TLS Profile**: Select the existing TLS server profile on the enterprise (e.g., **Inside_Server**). See **Note** on **Section 7.1**.
- Click **Finish**.



Select **Add** (not shown), to add to the external signaling interface toward the Watson Assistant.

- **Name**: Enter an appropriate name (e.g., **Outside-Sig-B2-77**).
- **IP Address**: Select **Outside B2 (B2, VLAN0)** and **192.168.80.77.**
- **TLS Port**: **5061.**
- **TLS Profile**: Select the existing TLS server profile on the enterprise (e.g., **Outside_Server**). See **Note** on **Section 7.1**.



©2023 Avaya Inc. All Rights Reserved.

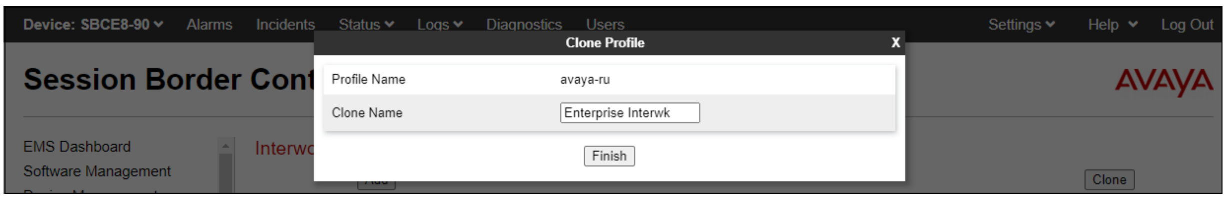
7.5. Server Interworking Profiles

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBC and a connected server. The Server Interworking profiles shown were already in place and reused in the configuration to Watson Assistant, their provisioning is covered here for completeness.

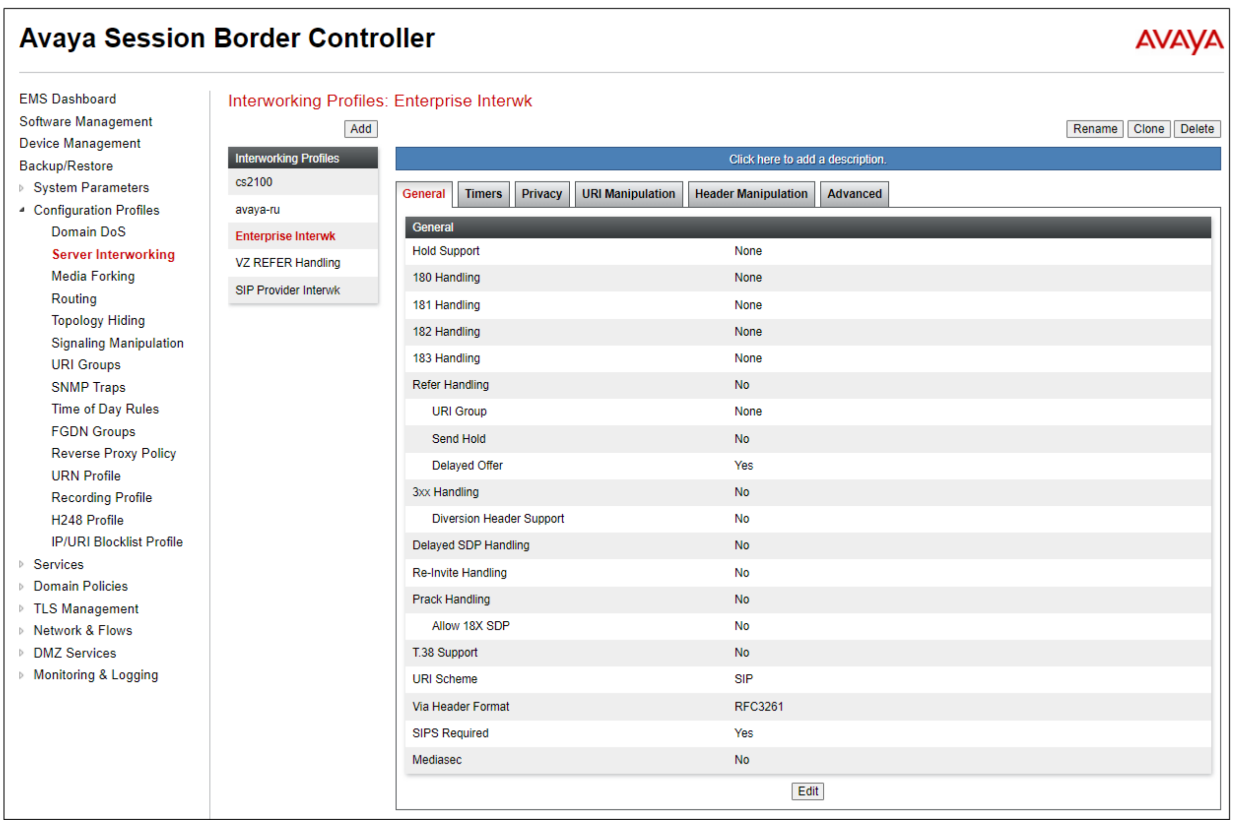
7.5.1. Server Interworking Profile for Session Manager

The Session Manager server interworking profile was cloned from the **avaya-ru** profile and left unmodified. Select **Configuration Profiles → Server Interworking** from the left-hand menu.

- Select the pre-defined **avaya-ru** profile and click the **Clone** button.
- Enter profile name: (e.g., **Enterprise Interwk**), and click **Finish** to continue.

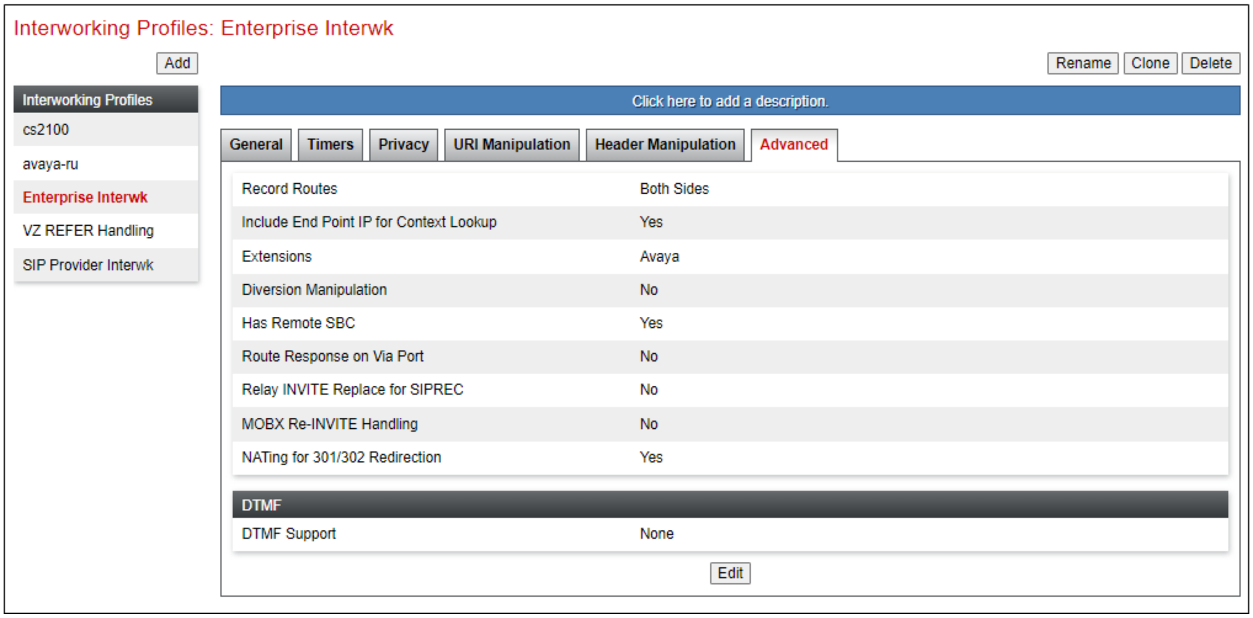


The General tab below shows the default settings used.



©2023 Avaya Inc. All Rights Reserved.

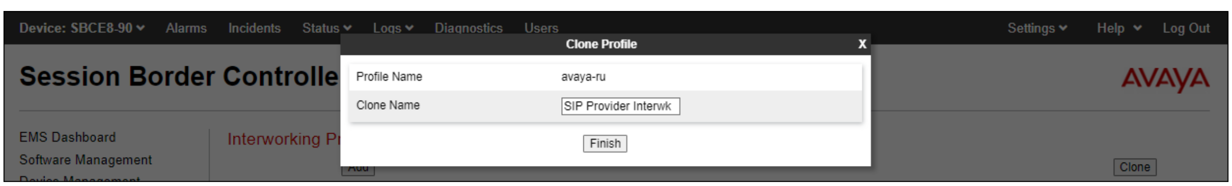
The Advanced tab below shows the default settings used.



7.5.2. Server Interworking Profile for Watson Assistant

The server interworking profile used in the connection to the Watson Assistant SIP server was also cloned from the **avaya-ru** profile and left unchanged. Select **Configuration Profiles → Server Interworking** from the left-hand menu.

- Select the pre-defined **avaya-ru** profile and click the **Clone** button.
- Enter profile name: (e.g., **SIP Provider Interwk**), and click **Finish**.



©2023 Avaya Inc. All Rights Reserved.

7.6. SIP Server Profiles

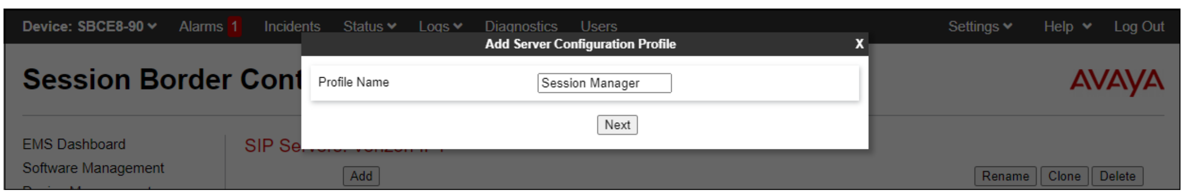
SIP Server Profiles are required for each server connected to Avaya SBC. A new server profile was created for IBM Watson Assistant. The SIP Server Profile for Session Manager was already in place and reused in the configuration. Follow the steps in **Section 7.6.1** if one doesn't exists.

Note –Avaya SBC in the test configuration used identities certificates signed by Avaya System Manager for the TLS internal connections to Session Manager. The procedure to create and obtain these certificates and the creation of TLS client and server profiles for these connections is outside the scope of these Application Notes.

7.6.1. SIP Server Profile – Session Manager

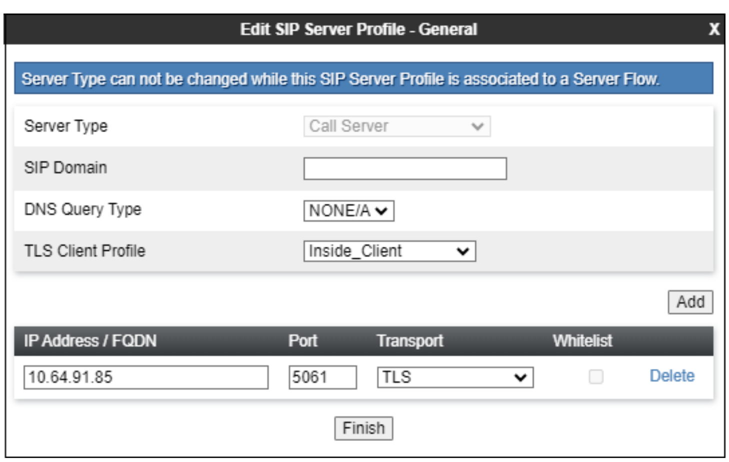
This section defines the SIP Server Profile for the Avaya SBC connection to Session Manager.

- Select **Services → SIP Servers** from the left-hand menu.
- Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **Session Manager**) and click **Next**.



The **Add Server Configuration Profile** window will open.

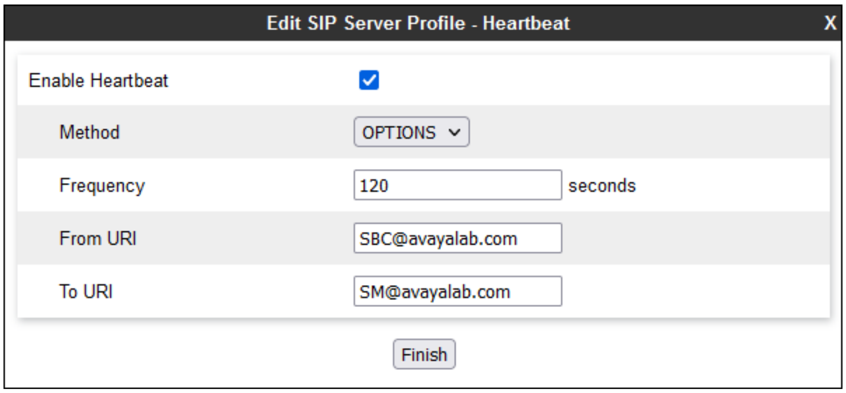
- **Server Type**: **Call Server**.
- **TLS Client Profile**: Select the existing TLS client profile on the enterprise (e.g., **Inside_Client**).
- **IP Address**: **10.64.91.85** (Session Manager Security Module IP address).
- Select **Port**: **5061**, **Transport**: **TLS**.
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



©2023 Avaya Inc. All Rights Reserved.

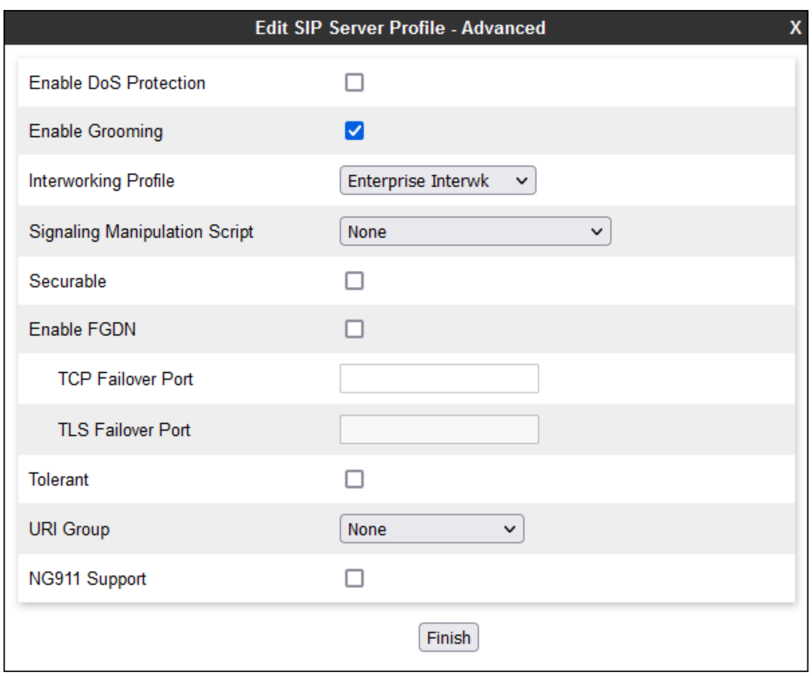
Default values can be used on the **Authentication** tab. On the **Heartbeat** tab, check the **Enable Heartbeat** box to have Avaya SBC source "heartbeats" toward Session Manager.

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



Default values are used on the **Registration** and **Ping** tabs. On the **Advanced** tab:

- Select the **Enterprise Interwk** (**Section 7.5.1**), for **Interworking Profile**.
- Since TLS transport is specified, then the **Enable Grooming** option should be enabled.
- In the **Signaling Manipulation Script** field select **none**.
- Select **Finish**.

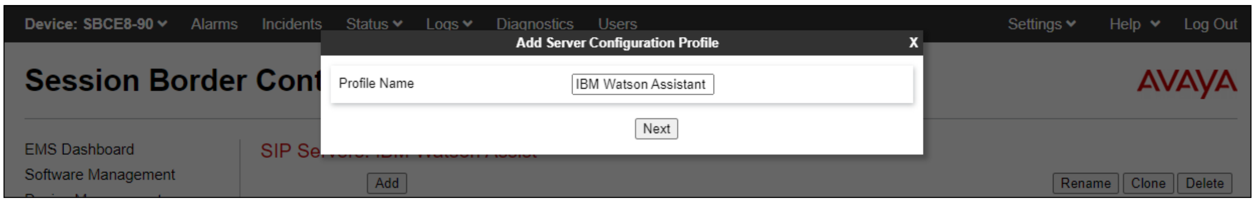


©2023 Avaya Inc. All Rights Reserved.

7.6.2. SIP Server Profile – Watson Assistant

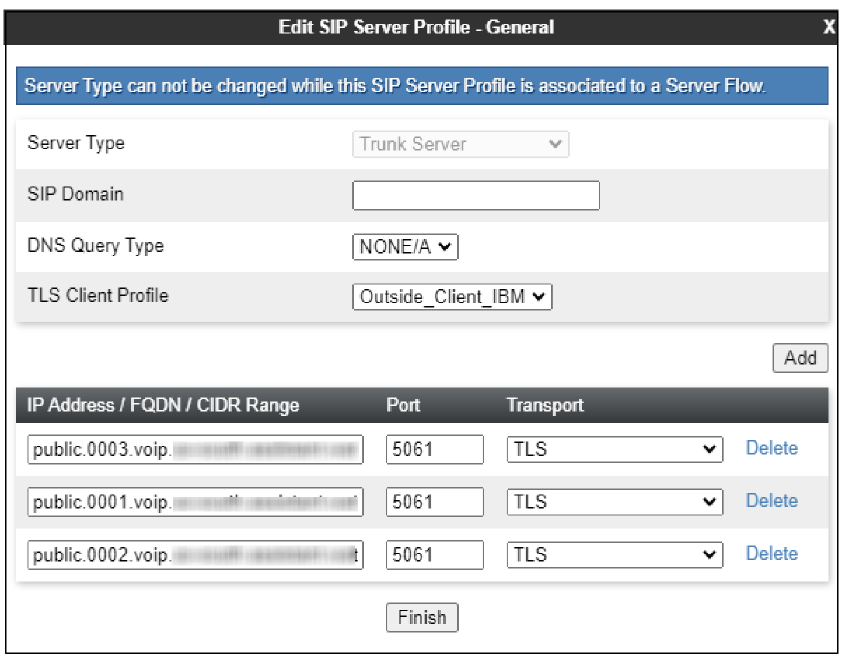
Repeat the steps in **Section 7.6.1**, with the following changes, to create a SIP Server Profile for the Avaya SBC connection to Watson Assistant.

Select **Add** and enter a Profile Name (e.g., **IBM Watson Assistant**) and select **Next**.



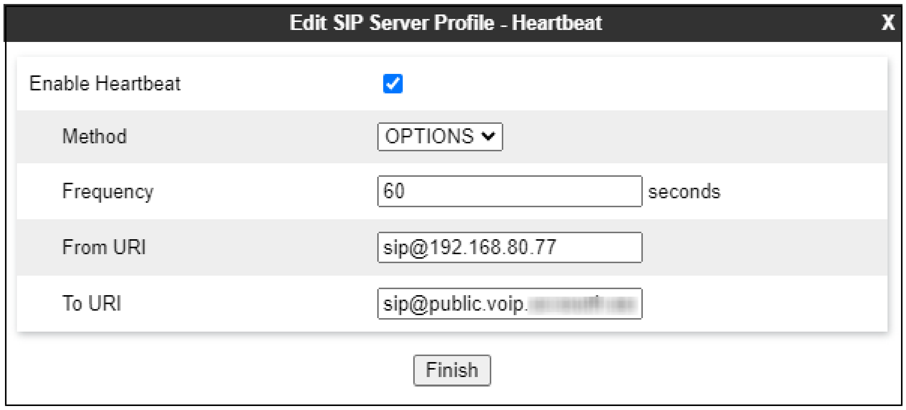
On the **General** window, enter the following:

- **Server Type: Trunk Server**.
- **TLS Client Profile**: Select the client profile created in **Section 7.1.2**.
- Select **Add** and enter the FQDNs for the SIP connections to Watson Assistant, provided by IBM. The service used in the reference configuration consists of three sites, hence the three FQDNs.
- Select **Port**: **5061**, **Transport**: **TLS**.
- If adding the profile, click **Next** (not shown) to proceed to next tab.

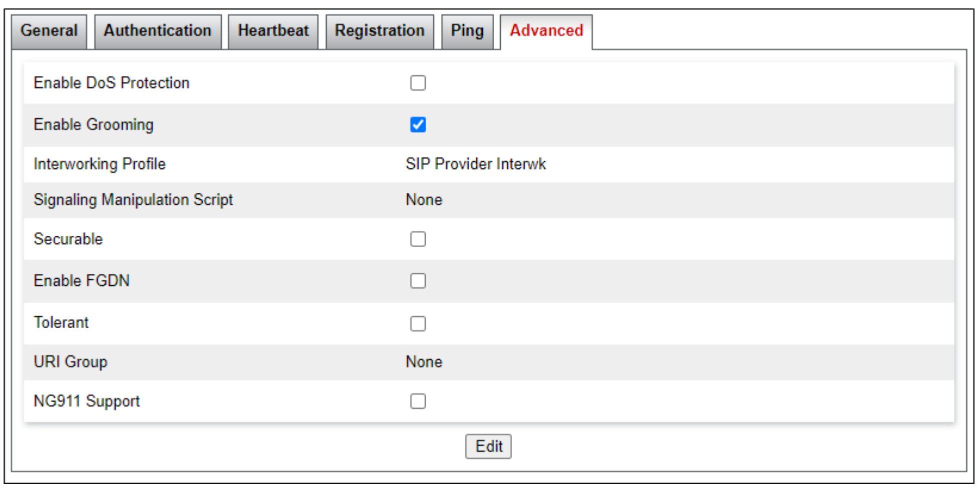


©2023 Avaya Inc. All Rights Reserved.

Default values are used on the **Authentication** tab. On the **Heartbeat** tab, check the **Enable Heartbeat** box to optionally have the Avaya SBC source “heartbeats” toward the Watson Assistant SIP server. The screen below shows the values used in the reference configuration.



Default values are used on the **Registration** and **Ping** tabs. On the **Advanced** window, **Enable Grooming** is selected. Select the **SIP Provider Interwk** (**Section 7.5.2**), for **Interworking Profile**. All other parameters retain their default values.



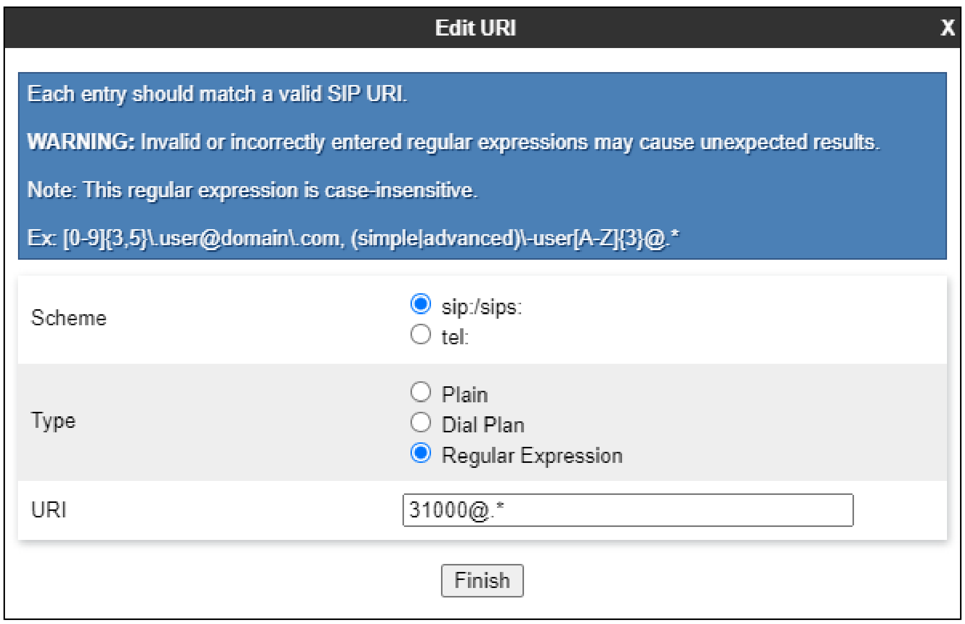
©2023 Avaya Inc. All Rights Reserved.

7.7. URI Groups

A URI Group was created to assist in routing calls to Watson Assistant, to differentiate the traffic on calls arriving from Session Manager to the Avaya SBC, on the same internal interface used for other types of calls.

Select **Configuration Profiles → URI Groups** from the left-hand menu. Select **Add** and enter a descriptive **Group Name**, e.g., **Watson Assistant**, and select **Next** (not shown).
Enter the following:

- **Scheme**: **sip:/sips:**
- **Type: Regular Expression**
- **URI: 31000@.***
- Select **Finish**.



©2023 Avaya Inc. All Rights Reserved.

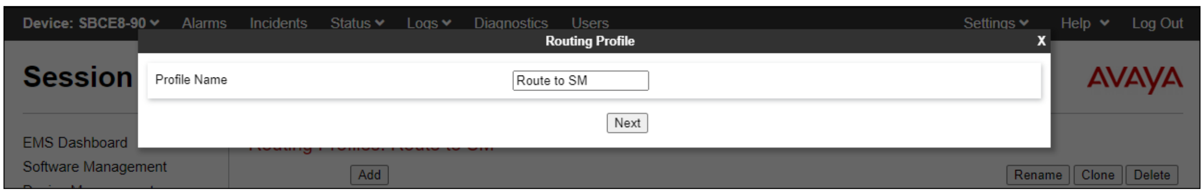
7.8. Routing Profiles

Routing Profiles are used to specify the next-hop for a SIP message. A routing profile is applied after the traffic has matched an End Point Flow defined in **Section 7.12**. The IP addresses and ports defined here will be used as destination addresses for signaling.

7.8.1. Routing Profile – Session Manager

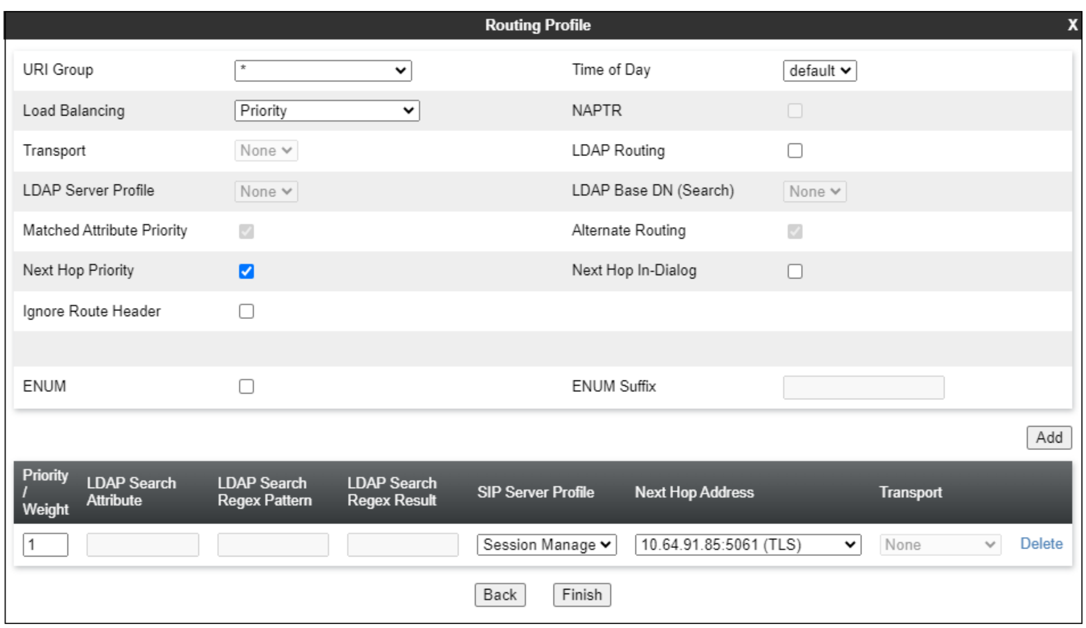
A routing profile for inbound calls to Session Manager was already in place, and it was reused in the configuration for Watson Assistant. Follow the steps below to create a routing profile to the Session Manager if one doesn't already exist.

Navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** (e.g., **Route to SM**) and click **Next** to continue.



The Routing Rule window will open. The parameters in the top portion of the profile are left at their default settings. Click the **Add** button. The Next-Hop Address section will open at the bottom of the profile. Populate the following fields:

- **Priority/Weight**: **1**
- **SIP Server Profile**: **Session Manager** (from **Section 7.6.1**).
- **Next Hop Address:** Verify that the **10.64.91.85:5061 (TLS)** entry from the drop-down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out. Click **Finish**.

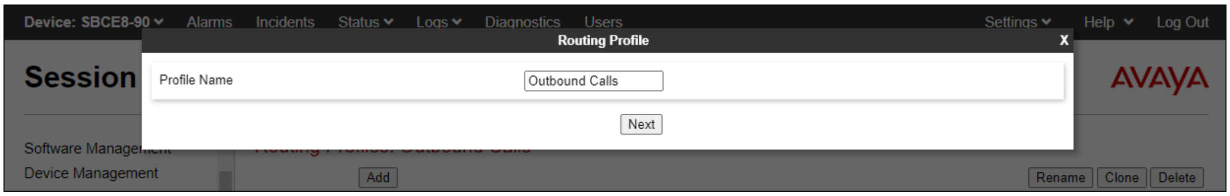


©2023 Avaya Inc. All Rights Reserved.

7.8.2. Routing Profile – Watson Assistant

A routing profile for outbound calls was already in place, and it was modified and reused in the configuration for Watson Assistant.

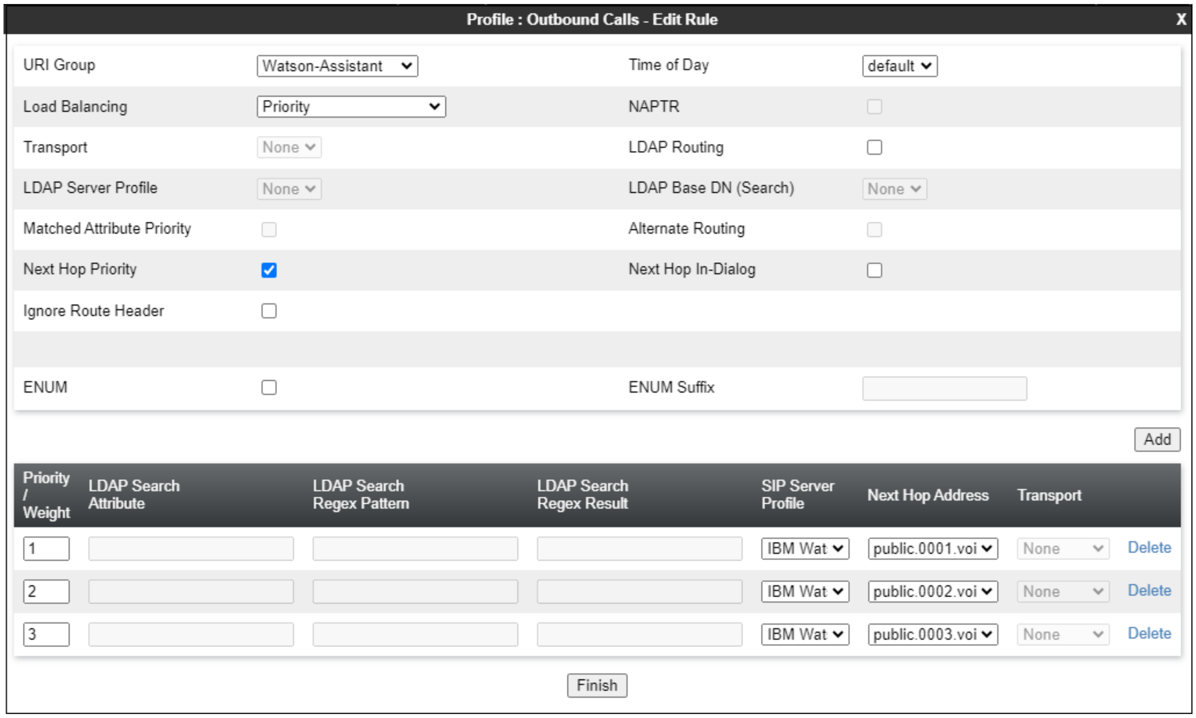
Navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** (e.g., **Outbound Calls**) and click **Next** to continue. If the profile already exists, select the profile and click **Add** on the right side of the screen to add a new routing rule to the profile.



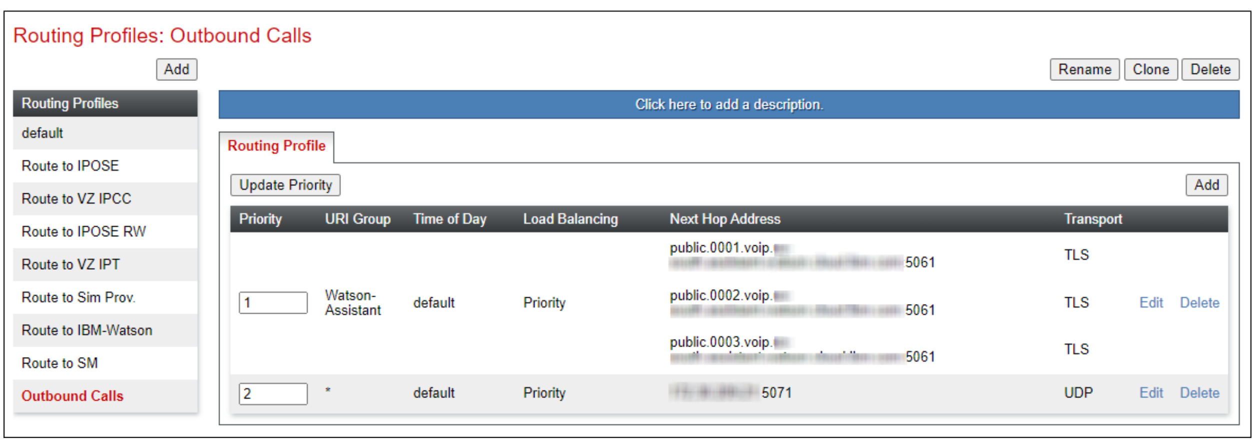
On the Routing Rule window, under **URI Group** select the **Watson Assistant** URI Group created in **Section 7.7**. Click the **Add** button. The Next-Hop Address section will open at the bottom of the profile. Populate the following fields:

- **Priority/Weight**: **1**
- **SIP Server Profile:** Select **IBM Watson Assistant** (from **Section 7.6.2**).
- **Next Hop Address:** Select the FQDN of the first site.
- Click the **Add** button to add a second Next-Hop Address.
- **Priority/Weight**: **2**
- **SIP Server Profile:** Select **IBM Watson Assistant**.
- **Next Hop Address:** Select the FQDN of the second site.
- Click the **Add** button to add a third Next-Hop Address.
- **Priority/Weight**: **3**
- **SIP Server Profile:** Select **IBM Watson Assistant**.
- **Next Hop Address:** Select the FQDN of the third site.
- Click **Finish**.

©2023 Avaya Inc. All Rights Reserved.



In the reference configuration, an existing routing rule was already in place for outbound calls on a SIP trunk to the PSTN. Back at the **Routing Profile** screen, with the **Outbound Calls** profile selected, assign a **Priority 1** to the newly created rule for calls to Watson Assistant, and **Priority 2** to the existing rule for PSTN calls, as shown on the screen below. Click the **Update Priority** button.



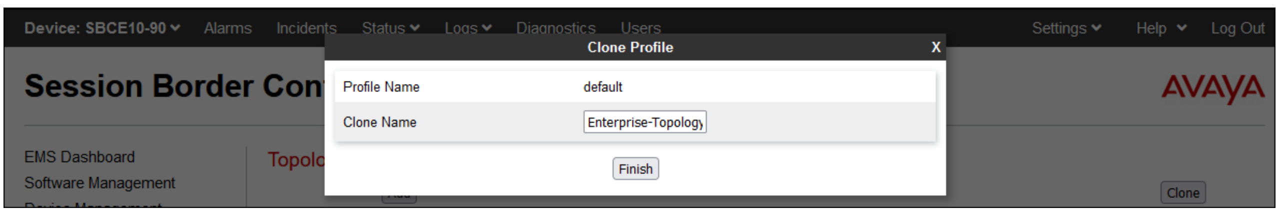
©2023 Avaya Inc. All Rights Reserved.

7.9. Topology Hiding Profile

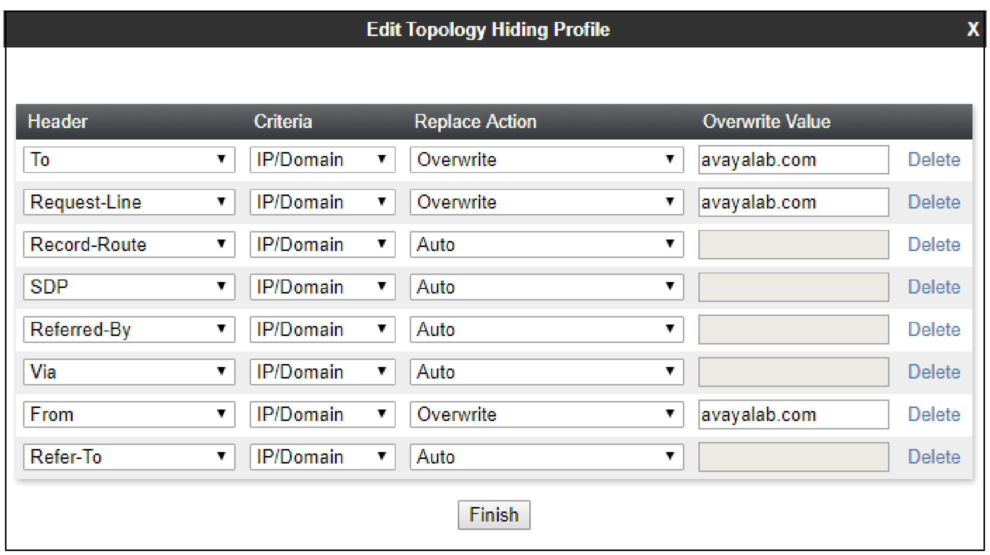
The **Topology Hiding** profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the security of the network. It hides the topology of the enterprise network from external networks.

In the sample configuration, the existing enterprise Topology Hiding Profile was reused. This profile was previously cloned from the **default** profile and then modified, to adapt the host portion of the SIP headers, to the domain expected on the enterprise network. The configuration is shown here for completeness.

- 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., **Enterprise-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**.



©2023 Avaya Inc. All Rights Reserved.

7.10. Media Rules

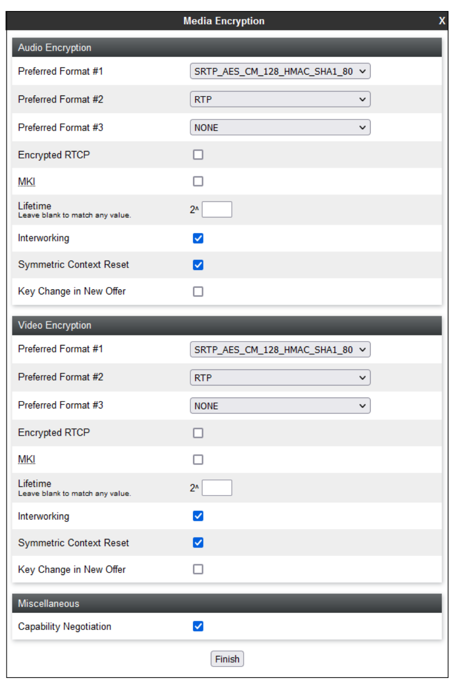
Media Rules define packet parameters for the RTP media, such as encryption techniques and QoS settings. A media rule for the enterprise (Session Manager) was already existing, and re-used in this configuration. This configuration is show here for completeness. A new media rule was created for Watson Assistant.

7.10.1. Enterprise – Media Rule

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

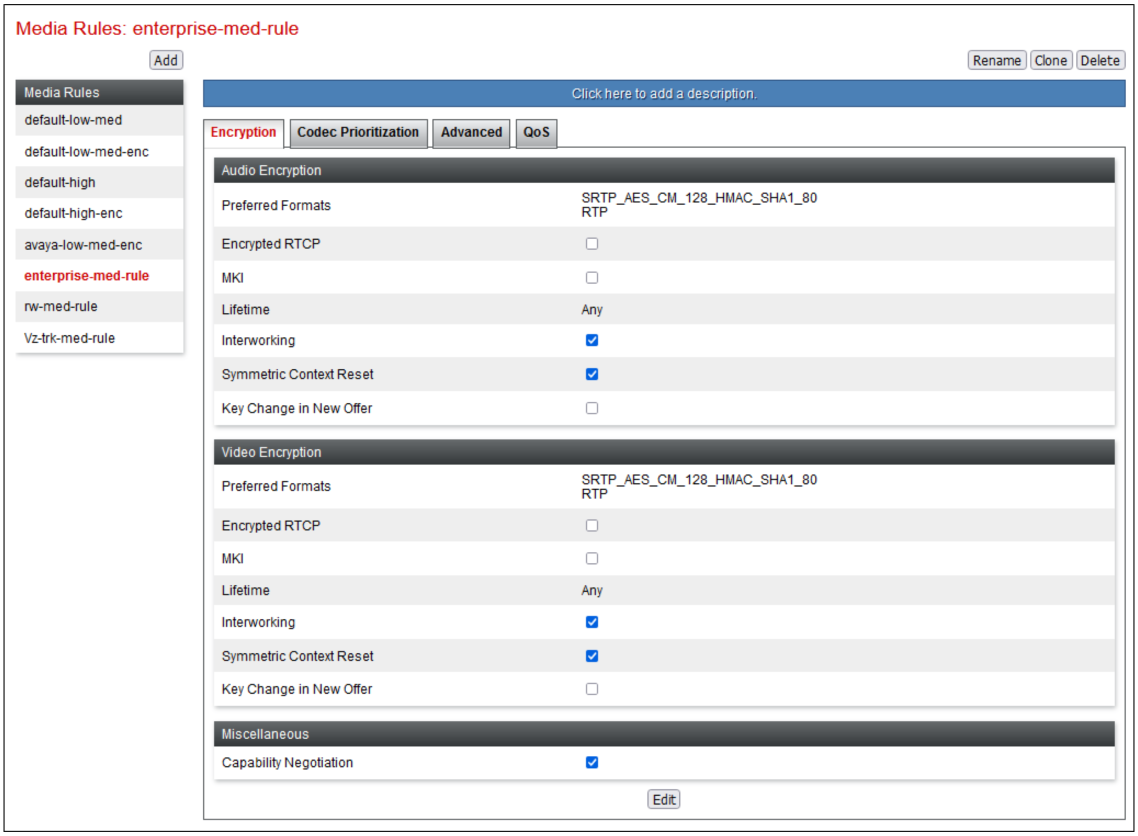
- Select **Domain Policies → Media Rules** from the left-hand side menu (not shown).
- From the Media Rules menu, select the **avaya-low-med-enc** rule.
- Select **Clone** button, and the **Clone Rule** window will open.
- In the **Clone Name** field enter the new Media Rule name (e.g., **enterprise-med-rule**)
- Click **Finish.** The newly created rule will be displayed.

- On the **enterprise med rule** just created, select the **Encryption** tab.
- Click the **Edit** button and the **Media Encryption** window will open.
- In the **Audio Encryption** section, select **RTP** for **Preferred Format #2**.
- In the **Video Encryption** section, select **RTP** for **Preferred Format #2**.
- In the **Miscellaneous** section, select **Capability Negotiation**.
- Click **Finish**.



©2023 Avaya Inc. All Rights Reserved.

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



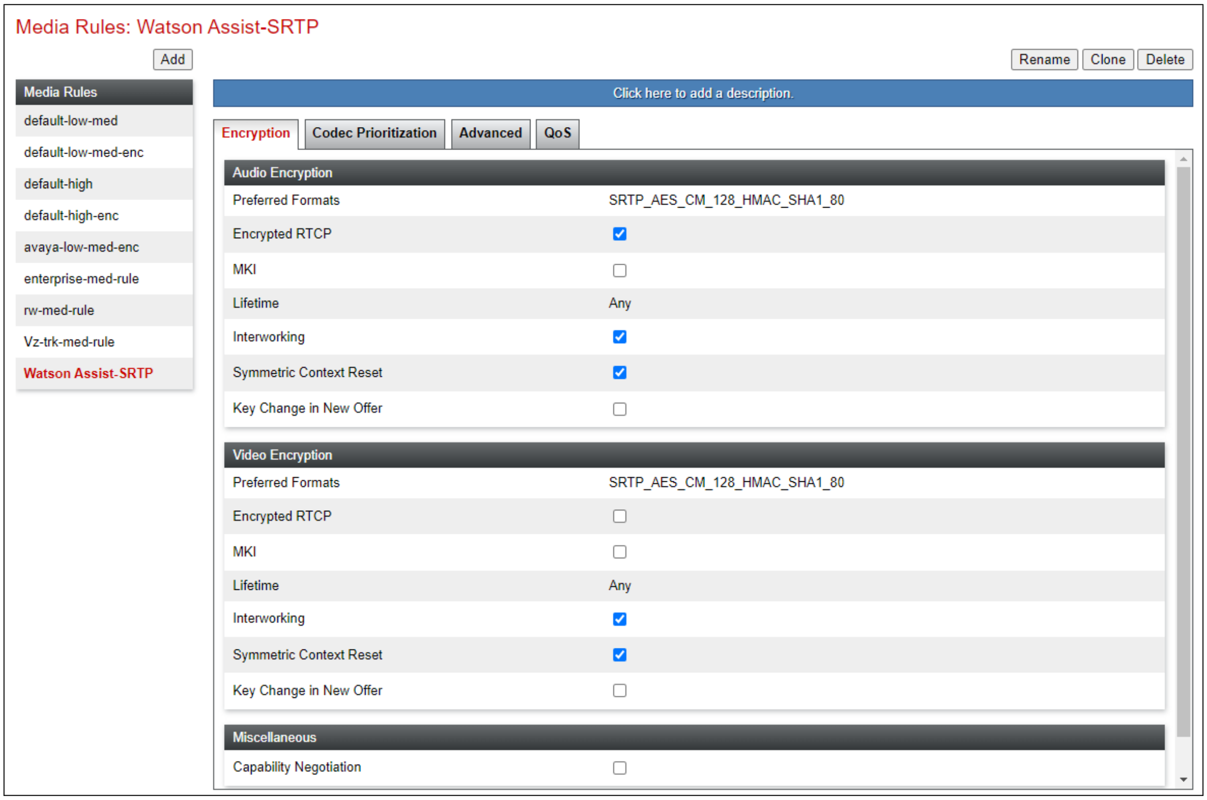
©2023 Avaya Inc. All Rights Reserved.

7.10.2. Watson Assistant – Media Rule

Repeat the steps in **Section 7.10.1**, with the following changes, to create a Media Rule for Watson Assistant.

1. Clone the **default-high-enc** profile.
2. In the **Clone Name** field enter the new Media Rule name (e.g., **Watson Assist-SRTP**).

The completed **Watson Assist-SRTP** media rule is shown on the screen below.



Note that SRTP is strictly enforced for the media in the connection to Watson Assistant, RTP is not allowed.

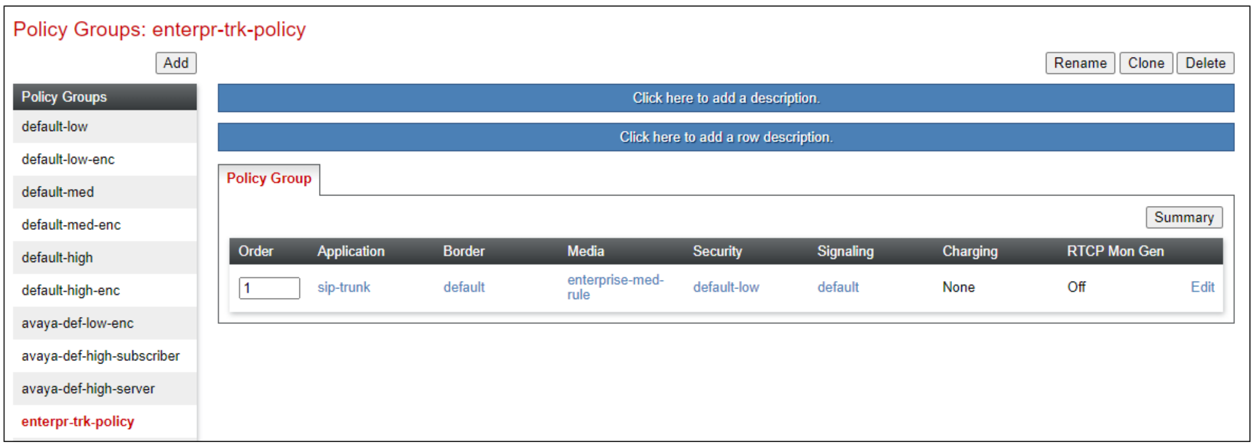
©2023 Avaya Inc. All Rights Reserved.

7.11. Endpoint Policy Groups

Endpoint policy groups are set of Domain Policies that will be applied to traffic between Avaya SBC and a connected server. The Endpoint Policy Group is applied to the traffic as part of the Server Flows defined later in **Section 7.12**. A new Endpoint Policy Group was defined for Watson Assistant, while a Policy Group for the enterprise (Session Manager) was already existing, and re-used in this configuration.

7.11.1. Endpoint Policy Group – Enterprise

The following Policy Group named **enterprise-policy-gr** was already defined in Avaya SBC for the enterprise, using the values shown on the screen below. The Media Rule is the **enterprise-med-rule** shown on **Section 7.10.1**. The Policy Group was reused in the configuration for Watson Assistant without making any changes, but it is shown here for completeness.



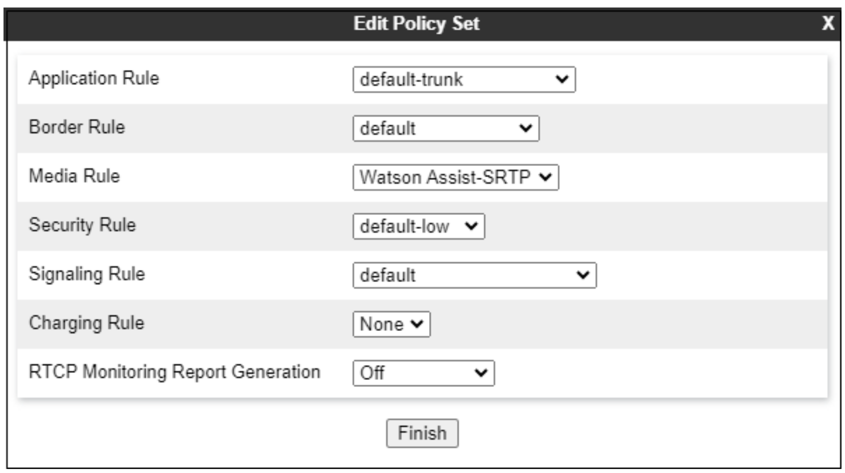
©2023 Avaya Inc. All Rights Reserved.

7.11.2. Endpoint Policy Group – Watson Assistant

To create a new Endpoint Policy Group for Watson Assistant, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the right pane, select **Add**. Enter a **Group Name** e.g., **Watson Assist Policy**, (not shown) and click **Next** to continue.

On the **Policy Group** window select the following predefined default set of rules on the SBC:

- **Application Rule**: **default-trunk**.
- **Border Rule**: **default**.
- **Media Rule**: **Watson Assist-SRTP**. (**Section 7.10.2**)
- **Security Rule**: **default-low**.
- **Signaling Rule**: **default**.
- **Charging Rule**: **None**.
- **RTCP Monitoring Report Generation**: **Off**.
- Select **Finish**.



The completed Policy Group is shown on the screen below.

©2023 Avaya Inc. All Rights Reserved.

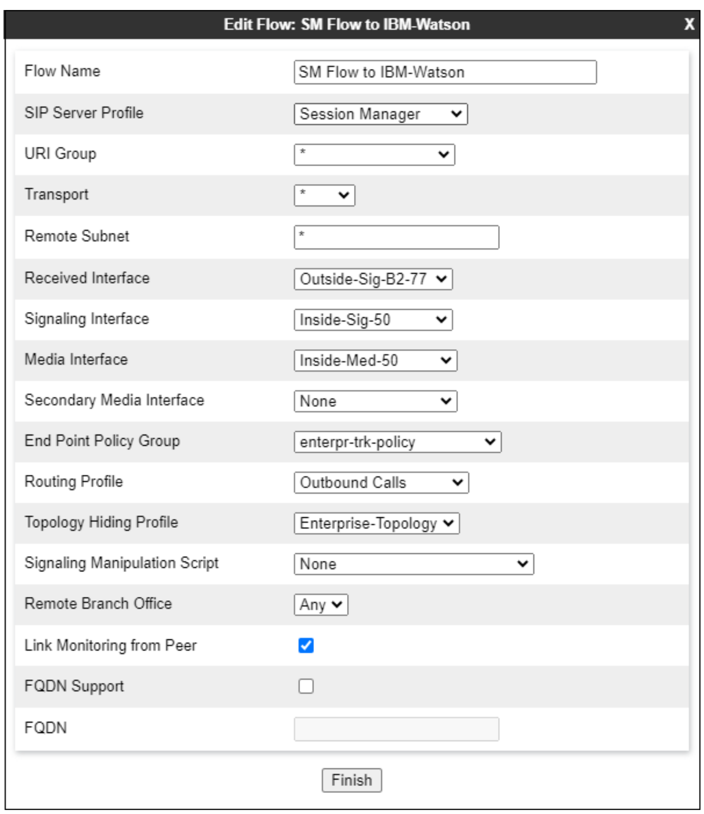
7.12. Endpoint Flows – Server Flows

Server Flows combine the interfaces, polices, and profiles defined in the previous sections into inbound and outbound flows. When a packet is received by Avaya SBC, 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. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Two flows are involved in every call, the source endpoint flow and the destination endpoint flow.

7.12.1. Server Flows – Session Manager

Select **Network and Flows → Endpoint Flows** from the menu on the left-hand side, and select the **Server Flows** tab and click **Add** (not shown). Enter the following parameters:

- **Flow Name**: **SM Flow to IBM-Watson**.
- **SIP Server Profile**: **Session Manager** (**Section 7.6.1**).
- **URI Group**, **Transport**, **Remote Subnet**: *****
- **Received Interface**: **Outside-sig-B2-77** (**Section 7.4**).
- **Signaling Interface**: **Inside-Sig-50** (**Section 7.4**).
- **Media Interface**: **Inside-Med-50** (**Section 7.3**).
- **End Point Policy Group**: **enterpr-trk-policy** (**Section 7.11.1**).
- **Routing Profile**: **Outbound Calls** (**Section 7.8.2**).
- **Topology Hiding Profile**: **Enterprise Topology** (**Section 7.9**).
- Check the **Link Monitoring from Peer** box.
- Let other fields at the default values. Click **Finish**.

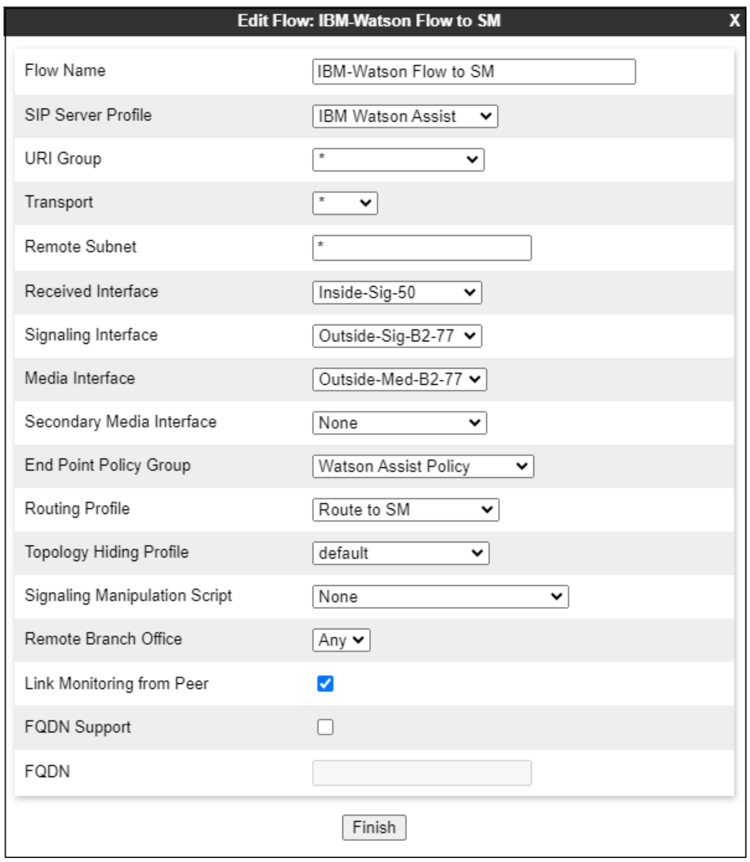


©2023 Avaya Inc. All Rights Reserved.

7.12.2. Server Flow – Watson Assistant

The screen below shows the Server Flow for Watson Assistant created in the reference configuration, with the following parameters:

- **Flow Name**: **IBM-Watson Flow to SM**.
- **SIP Server Profile**: **IBM Watson Assist** (**Section 7.6.2**).
- **URI Group**, **Transport**, **Remote Subnet**: *
- **Received Interface**: **Inside-Sig-50** (**Section 7.4**).
- **Signaling Interface**: **Outside-Sig-B2-77 (Section 7.4**).
- **Media Interface**: **Outside-Med-B2-77** (**Section 7.3**).
- **End Point Policy Group**: **Watson Assist Policy** (**Section 7.11.2**).
- **Routing Profile**: **Route to SM** (**Section 7.8.1**).
- **Topology Hiding Profile**: **default**.
- Check the **Link Monitoring from Peer** box.
- Let other fields at the default values.
- Click **Finish**.



©2023 Avaya Inc. All Rights Reserved.

8. Watson Assistant Configuration

The configuration of Watson Assistant is performed by IBM technical personnel. To complete the provisioning, IBM will require the following information:

- Avaya SBC public IP address or FQDN.
- Number used at the enterprise to send the calls to Watson Assistant.
- Agent queues (e.g., skill group or VDN extension) where Watson Assistant will transfer calls to the contact center.

9. Verification Steps

Complete the following general steps to verify correct functionality of the Avaya configuration with Watson Assistant.

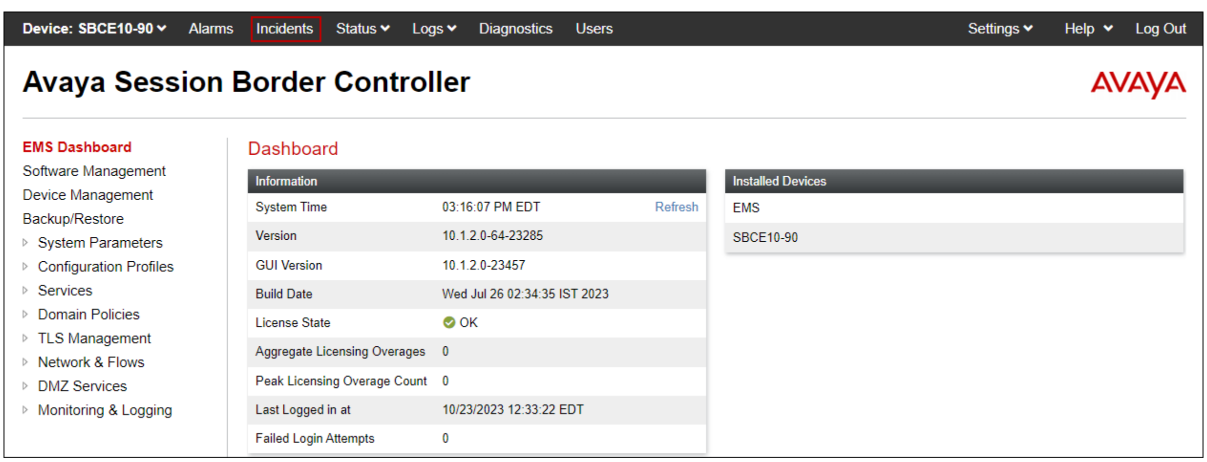
- Place a call to Watson Assistant and verify the application answers and the appropriate greeting is heard.
- Caller navigates through the application using speech. Verify Watson Assistant provides the requested information.
- Watson Assistant transfers call to an agent when requested. Verify the transferred call is established with two-way audio.
- Verify UUI data is provided to the agent.
- Caller terminates the call successfully.

9.1. Avaya SBC

This section provides verification steps that may be performed on the Avaya SBC.

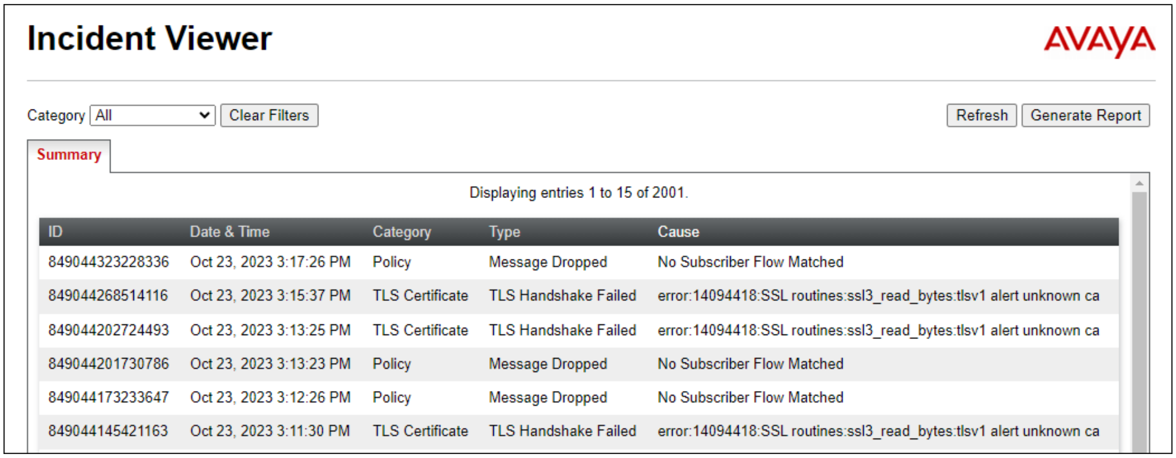
9.1.1. Incidents

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



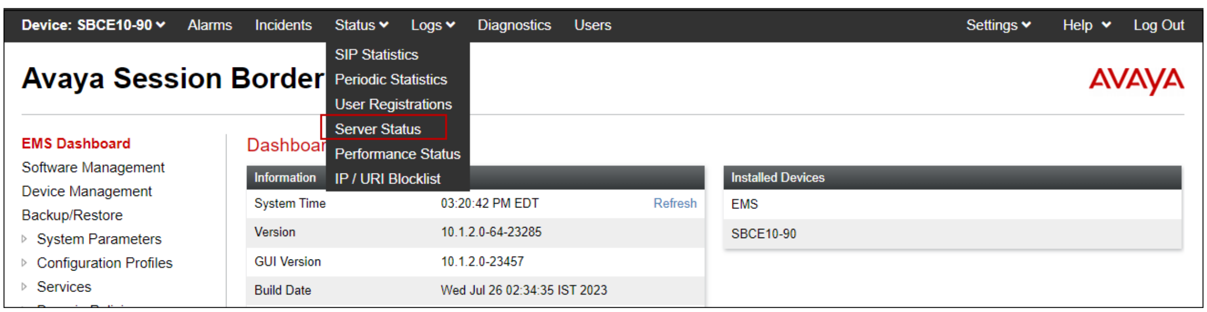
©2023 Avaya Inc. All Rights Reserved.

Use the Incident Viewer to verify server heartbeats and to troubleshoot routing and other failures.

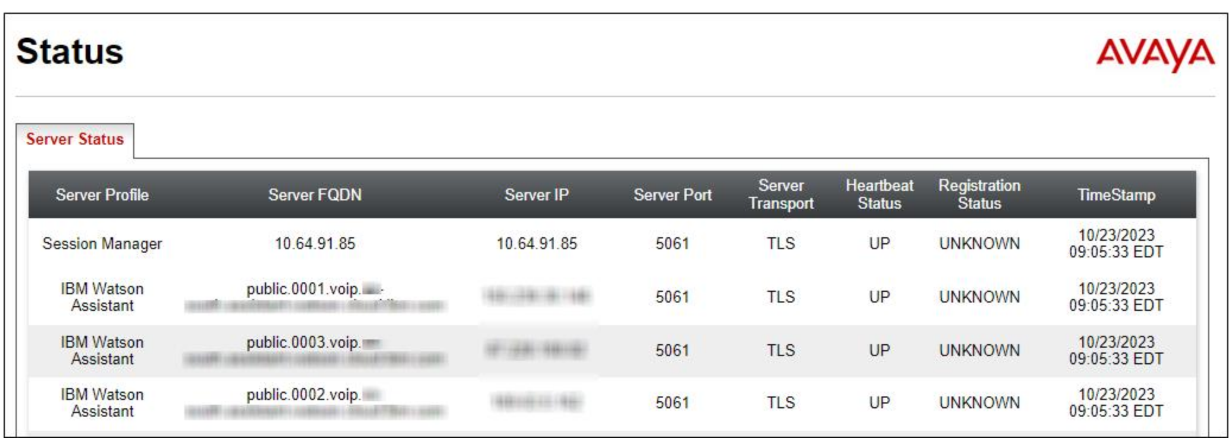


9.1.2. Server Status

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



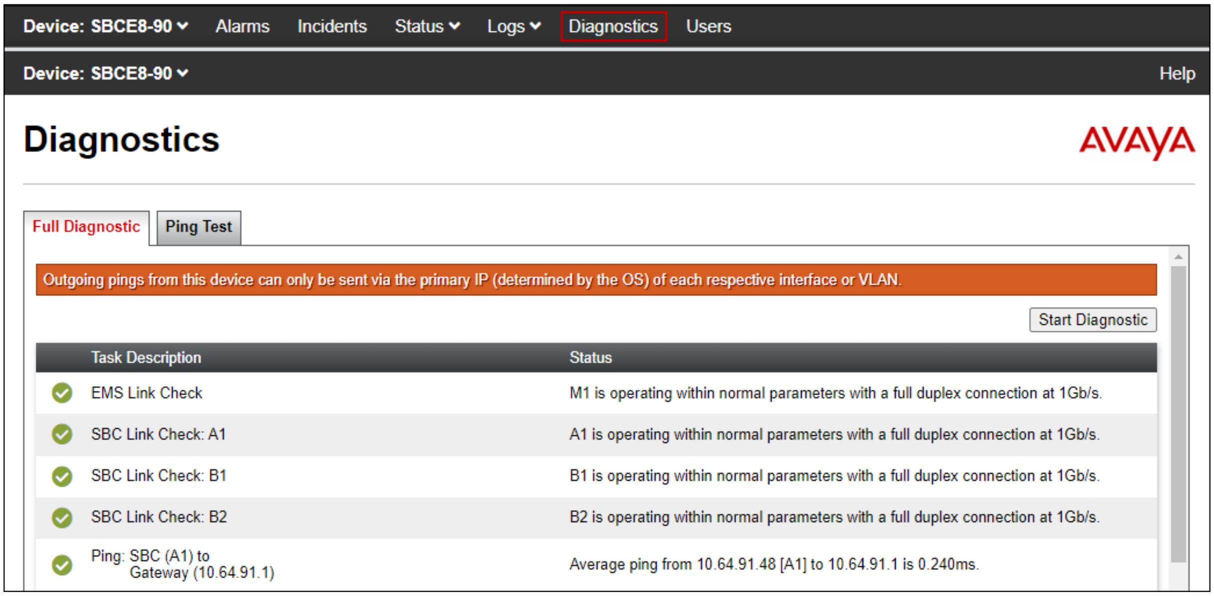
The **Server Status** screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat to be enabled on the SIP Server Configuration profiles, as configured in **Section 7.6**.



©2023 Avaya Inc. All Rights Reserved.

9.1.3. Diagnostics

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



9.1.4. Tracing

tracesSBC is an Avaya Session Border Controller command line tool for traffic analysis. Log into the Avaya SBC command line management interface to run this command.

©2023 Avaya Inc. All Rights Reserved.

10.Conclusion

These Application Notes have described the configuration steps required to integrate IBM Watson Assistant with Avaya Session Border Controller 10.1 and Avaya Aura 10.1. IBM Watson Assistant connected to the Avaya contact center via a SIP trunk through the Avaya SBC. Callers were able to interact with Watson Assistant using their speech to retrieve and provide information. In addition, the assistant was able to transfer the call to an agent when requested by the caller, and send caller information in UUI. All test cases passed with the observation notes on **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

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

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, June 2023.
[2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 12, September 2023.
[3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023
[4] *Administering Avaya Session Border Controller*, Release 10.1.x, Issue 5, October 2023.

©2023 Avaya Inc. All Rights Reserved.

©2023 Avaya LLC. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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