DevConnect Program

Application Notes for Fonolo Voice Call-Backs Version 3.9 using Cloud SIP Connect with Avaya Session Border Controller Release 10.1 and Avaya Aura® 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs version 3.9 using Cloud SIP Connect to interoperate with Avaya Session Border Release 10.1 and Avaya Aura® 10.1. Fonolo Voice Call-Back is a call center solution in the cloud, that interfaces with Avaya Session Border Controller via SIP trunk.

Readers should pay attention to **Section** Error! Reference source not found., in particular the scope of testing as outlined in **Section** Error! Reference source not found. as well as the observations noted in **Section** Error! Reference source not found., 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.

1. Introduction

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs (VCB) using Cloud SIP Connect to interoperate with Avaya Session Border Controller (Avaya SBC) using SIP trunk. Fonolo VCB provides functionality to replace hold-time with a call-back and during this compliance testing was hosted on the cloud by Fonolo.

When a caller encounters a scenario where no agents are available in a call center environment and Communication Manager is part of the environment, the caller is presented with options by the call center to either continue waiting in the queue or receive a call back from the call center. If the caller chose the latter, then the call center directs the caller to Fonolo VCB via Avaya SBC SIP trunks where Fonolo VCB then provides a message to the caller to leave a call back number, so that Fonolo VCB can call back the caller when an agent becomes available. Once Fonolo VCB receives the confirmed call back number from the caller, Fonolo VCB uses SIP trunks through Avaya SBC to call back into the call center and wait in the queue until an agent becomes available. When an agent becomes available, Fonolo VCB informs the agent that there is a call waiting and if the agent would like to get connected to the caller. If the agent accepts to connect to the caller, Fonolo VCB calls the caller and connects the caller with the available agent.

In the application notes, the terms Fonolo VCB and Fonolo Cloud SIP Connect terms are interchangeably used.

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 Fonolo VCB via Avaya SBC SIP trunk to Fonolo Cloud SIP Connect. Calls were placed manually from users on the PSTN to a call center Vector Directory Number (VDN).

The serviceability test cases focused on simulating a network outage and a restart on Avaya SBC. Calls to Fonolo VCB 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 Fonolo VCB using Cloud SIP Connect 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.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third-party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third-party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g., jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another and may affect the reliability or performance of the overall solution. Different network elements (e.g., session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third-party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

2.1. Interoperability Compliance Testing

The Fonolo VCB is hosted in a cloud environment by Fonolo. SIP trunk was used to connect the Fonolo VCB using Cloud SIP Connect with Avaya SBC. The following features and functionality were covered during compliance testing:

- Establish SIP trunk between Avaya SBC and Fonolo VCB using TLS transport.
- Responses from Fonolo VCB to SIP OPTIONS messages sent by Avaya SBC.
- Inbound PSTN calls routed from Communication Manager to Avaya SBC and to the SIP trunk to Fonolo VCB.
- Incoming PSTN to call center can be redirected to the Fonolo VCB via the SIP trunks based on vector. Outgoing calls from the Fonolo VCB to call center agent via Avaya SBC when PSTN callers decide on call back.

- Fonolo VCB places outbound calls to the PSTN caller via Avaya SBC who had selected the call back option and merge the call between the caller and available agents.
- DTMF transmission to ensure that options selected by the caller and agent is accepted correctly by Fonolo VCB.
- Telephony features such as holding and resuming call to Fonolo VCB, session refresh timer, agents transferring calls to another agent during the voice call-back and adding an agent or supervisor into a conference during the voice call-back.
- User-to-User Information (UUI) is sent from the enterprise to the Fonolo VCB and verify UUI data is sent back to agent deskphones via UUI button.
- Proper disconnect when the call is abandoned by PSTN caller.
- Proper disconnect when the call is abandoned by agent.
- 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

All test cases were successfully executed and passed.

2.3. Support

Technical support on Fonolo VCB can be obtained through the following:

- **Phone:** + 1-855-366-2500 (Toll-free)
- **Web:** https://fonolo.com/contact/
- **Email:** support@fonolo.com.

3. Reference Configuration

A simulated enterprise site consisting of Communication Manager, Session Manager and System Manager was used during compliance testing. As shown in **Figure 1**, SIP trunks were used to connect Fonolo VCB with Avaya Session Border Controller. Avaya Session Border Controller also had a SIP trunk to connect to SIP Service Provider for external call to PSTN. A skill set queue was configured on Communication Manager with some agents belonging to this queue.

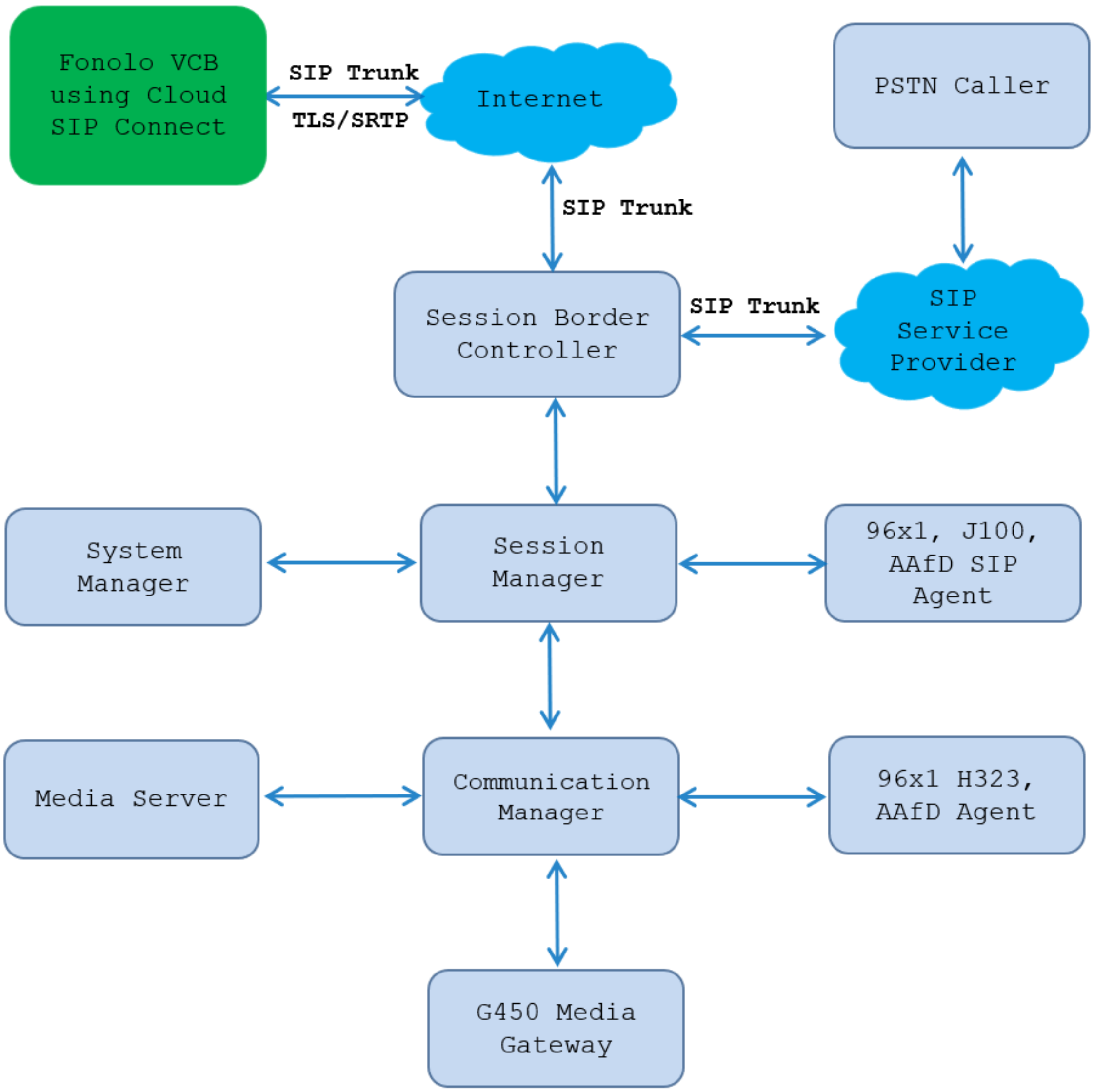


Figure 1: Test Configuration Diagram

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® 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 SIP Deskphones (J169, J179)	4.1.2.0.11
Avaya 96x1 Series IP Deskphone (SIP)	7.1.15.2.1
Avaya Agent for Desktop Softphone (SIP)	2.0.6.25
Fonolo Voice Call-Backs using Cloud SIP Connect	V.3.9

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. 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.

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.

5.1. Verify Communication Manager License

Log in to the System Access Terminal to verify that the Communication Manager license has the appropriate permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

If additional license is required, contact an authorized Avaya Sales or Reseller representative.

```
display system-parameters customer-options                      Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                           USED
                 Maximum Administered H.323 Trunks: 12000     10
       Maximum Concurrently Registered IP Stations: 18000      7
         Maximum Administered Remote Office Trunks: 12000      0
Max Concurrently Registered Remote Office Stations: 18000      0
          Maximum Concurrently Registered IP eCons:  414       0
     Max Concur Reg Unauthenticated H.323 Stations:   100      0
                    Maximum Video Capable Stations:  41000     4
               Maximum Video Capable IP Softphones:  18000    11
                   Maximum Administered SIP Trunks: 40000     30
  Max Administered Ad-hoc Video Conferencing Ports: 24000      0
   Max Number of DS1 Boards with Echo Cancellation: 999    0
```

5.2. Administer IP Node Names

Use the “change node-names ip” command (not shown) and add an entry for Session Manager. In this case, **SM10** and **10.33.1.42** are entered as **Name** and **IP Address**. Note the **procr** and **10.33.1.43** entry, which is the node **Name** and **IP address** for the processor board. These values will be used later to configure the SIP signaling to Session Manager in **Section 5.5**.

```
change node-names ip!
                                   IP NODE NAMES
    Name              IP Address
AMS1                10.33.1.30
default             0.0.0.0
SM10                10.33.1.42
lsp                 10.33.1.7
procr               10.33.1.43
```

5.3. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number. Update the audio codec types in the **Audio Codec** fields as necessary. The codec shown below was used in the compliance testing.

```
change ip-codec-set 3                                             Page   1 of   2

                           IP MEDIA PARAMETERS
    Codec Set: 1

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

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

5.4. Administer IP Network Region

Use the “change ip-network-region n” command, where “n” is the existing far-end network region number used by the SIP signaling group from **Section** Error! Reference source not found.**5**.

For **Authoritative Domain**, enter the applicable domain for the network. Enter a descriptive **Name**. Enter “yes” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter an available codec set number for integration with Fonolo VCB.

```
change ip-network-region 3                                   Page   1 of  20
                               IP NETWORK REGION
  Region: 3       NR Group: 1
Location: 1       Authoritative Domain: avayalab.com
    Name: Loc-1                  Stub Network Region: n
MEDIA PARAMETERS                 Intra-region IP-IP Direct Audio: yes
      Codec Set: 3               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
```

5.5. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “3”. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Group Type:** Set it as“sip”,
- **Transport Method:** Set is as “tls”.
- **Near-end Node Name:** Enter the “procr”interface of Communication Manager.
- **Far-end Node Name:** Enter the node name for Session Manager.
- **Near-end Listen Port:** Enter the TLS port for the SIP trunk to Session Manager.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** Enter the existing network region to use with Session Manager.

- **Far-end Domain:** The applicable SIP domain name for the network.
- **Direct IP-IP Audio Connections?:** **Set is as** “y”.

```
change signaling-group 3                                       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? n
  Peer Detection Enabled? n  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: interopASM
 Near-end Listen Port: 5063                 Far-end Listen Port: 5063
                                         Far-end Network Region: 3

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
```

5.6. Administer SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “1”. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Group Type:** Set is as “sip”.
- **Group Name:** **Enter a** descriptive name.
- **TAC:** Enter an available trunk access code.
- **Service Type:** **Set is as** “public-ntwrk”.
- **Signaling Group:** Enter the signaling group that has been created in **Section 5.5**.

```
change trunk-group 3                                           Page   1 of   5
                                TRUNK GROUP

Group Number: 3                  Group Type: sip          CDR Reports: r
  Group Name: To-ServiceProvider        COR: 1        TN: 1        TAC: #03
   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: 3
                                                    Number of Members: 10
```

Navigate to **Page 3** and enter “private” for **Numbering Format**.

```
change trunk-group 3                                              Page   3 of   4
TRUNK FEATURES
          ACA Assignment? n            Measured: both
                                                        Maintenance Tests? y



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

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y


                                Modify Tandem Calling Number: no


 Show ANSWERED BY on Display? y
```

Navigate to **Page 4** and enter “y” for the **Convert 180 to 183 for Early Media?** field as shown below.

```
change trunk-group 3                                              Page   4 of   4
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? y
                                   Support Request History? y
                              Telephone Event Payload Type: 101


                       Convert 180 to 183 for Early Media? y
                  Always Use re-INVITE for Display Updates? y

                       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. Administer Dial Plan

This section provides a sample dial plan used for routing calls with dialed digits 78xxx to Fonolo VCB. Use the "change dialplan analysis 0" command and add an entry to specify the use of digits pattern **78**, as shown below.

```
change dialplan analysis                                      Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 5

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
 0             3  fac      33            4  ext      #            3  dac
 1             4  ext      34            4  ext
 1             11 udp      45            4  aar
 78            5  udp      46            4  aar
```

5.8. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 78xxx to Fonolo VCB. Note that other routing methods may be used. Use the "change uniform-dialplan 0" command and add an entry to specify the use of AAR for routing of digits **78**xxx, as shown below.

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

  Matching                     Insert               Node
  Pattern            Len Del      Digits       Net Conv Num
 1                   11  0                     ars n
 35                  4   0                     aar n
 78                  5   0                     aar n
```

5.9. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is an existing route pattern number to be used to reach Fonolo VCB, in this case “3”. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.6**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.

```
change route-pattern 3                                        Page   1 of   4
                    Pattern Number: 1      Pattern Name: Public SIPTrunk
    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: 3    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                               lev0-pvt  next
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

5.10. Administer AAR Analysis

Use the “change aar analysis 78” command and add an entry to specify how to route calls to 78xxx. In the example shown below, calls with digits **78**xxx will be routed as an AAR call using route pattern “1” from **Section 09**

```
change aar analysis 78                                        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
    78                    5    5     3         aar          n
```

5.11. Administer Agent Login ID

To add an **Agent LoginID**, use the command "**add agent-loginID <agent ID>**" for each agent. In the compliance test, three agent login IDs 1000, 1001 and 1002 were created.

```
add agent-loginID 1000                                        Page   1 of   2
                                 AGENT LOGINID

                Login ID: 1000                                    AAS? n
                    Name: Agent 1000                            AUDIX? n
                      TN: 1
                     COR: 1
           Coverage Path:                             LWC Reception: spe
           Security Code: 1234               LWC Log External Calls? n
           Attribute:                      AUDIX Name for Messaging:

                                       LoginID for ISDN/SIP Display? n
                                                           Password:
                                             Password (enter again):
                                                        Auto Answer:
station
                                                  MIA Across Skills: system
 AUX Agent Considered Idle (MIA)? system   ACW Agent Considered Idle: system
                                           Aux Work Reason Code Type: system
                                             Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                            Forced Agent Logout Time:   :
    WARNING:  Agent must log in again before changes take effect
```

On **Page 2** of the **Agent LoginID** form, set the skill number (**SN**) to hunt group 1, which is the hunt group (skill) that the agents will log into.

```
add agent-loginID 1000                                        Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:                               Service Objective? n
Call Handling Preference: skill-level               Local Call Preference? n

    SN   RL SL          SN   RL SL
 1: 1       1       16:
 2:                 17:
 3:                 18:
 4:                 19:
 5:                 20:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
```

5.12. Administer Hunt Group

This section provides the Hunt Group configuration for the call center agents. Agents will log into Hunt Group 1 configured below. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.11**.

```
add hunt-group 1                                              Page   1 of   4
                              HUNT GROUP

            Group Number: 1                                ACD? y
              Group Name: Skill-1                        Queue? y
         Group Extension: 3320                          Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                    MM Early Answer? n
           Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

5.13. Administer Vector

Use the command "change vector n" while "n" is the vector number from 1-8000. The example of the vector **12** with the basic scripting is shown below. This section provides a sample vector that was used during the compliance testing. When a call is directed to this vector it provides the caller with an option to press "1" for call-back or stay in the queue if all agents are busy. If caller presses "1", then the call is routed to Fonolo VCB with number "78000", in "Step 8" a line was added to send UUI information to Fonolo VCB for testing purposes.

```
change vector 12                                               Page   1 of   6
                                  CALL VECTOR

    Number: 12              Name: To-Fonolo
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    5   secs hearing 1104     then silence
02 goto step    11           if staffed-agents   in skill 1           =  0
03 goto step    7            if expected-wait    for skill 1    pri m  >= 10
04 queue-to     skill 1    pri m
05
06
07 collect      1    digits after announcement 1107     for none
08 set          A      = digits   CATR   0123456789
09 route-to     number 78000                    cov n if digit           =  1
10 goto step    4            if unconditionally
11 disconnect   after announcement none
12 stop
```

5.14. Administer VDN

Use the “add vdn n” command to add a VDN number. In the **Destination** field, enter **Vector Number** 12 as configured in **Section 5.13** above and keep other fields at their default values.

```
add vdn 3340                                                    Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 3340
                                 Name*: Contact Center 1
                           Destination: Vector Number        12
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: both     Report Adjunct Calls as ACD*? n
        Acceptable Service Level (sec): 20
        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:
```

6. Configure Avaya Aura® Session Manager

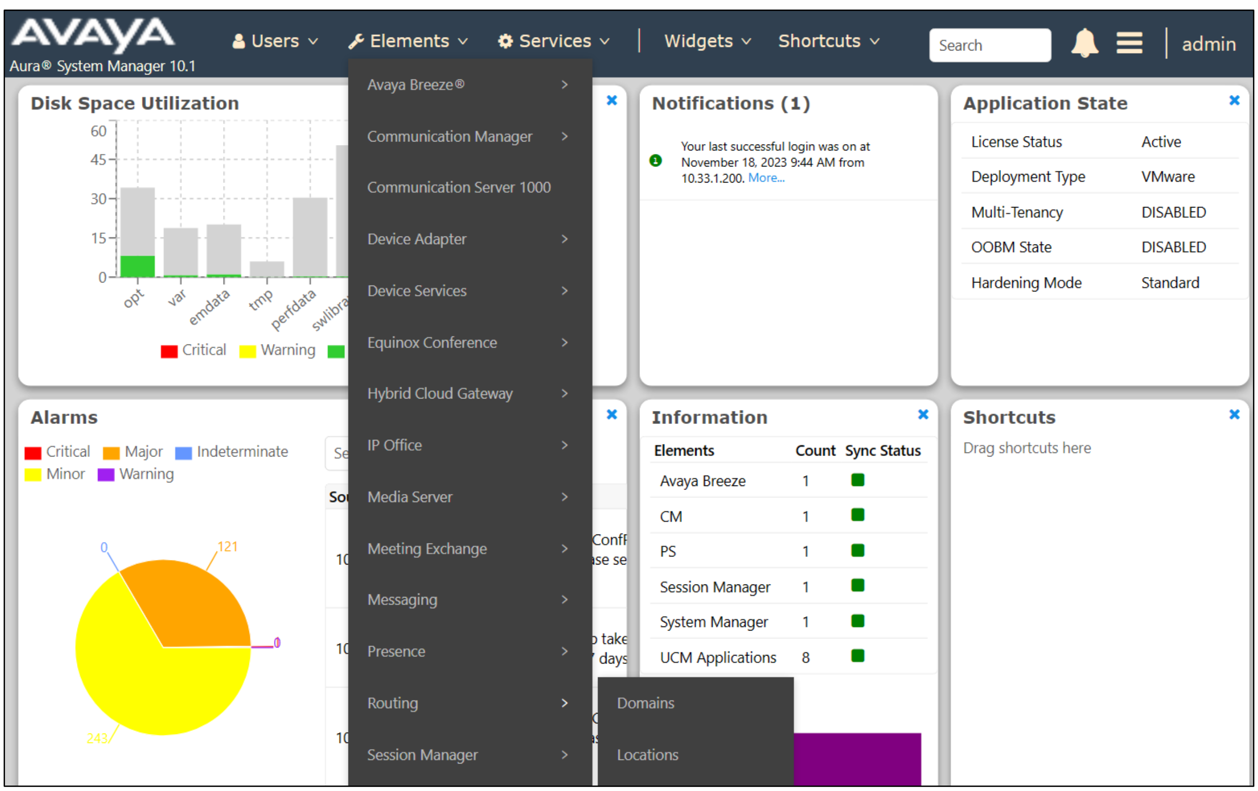
This section provides the procedures for configuring Session Manager. The procedures include the following areas:

- Launch System Manager.
- Administer Domain.
- Administer Locations.
- Administer SIP Entities.
- Administer Routing Policies.
- Administer 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.

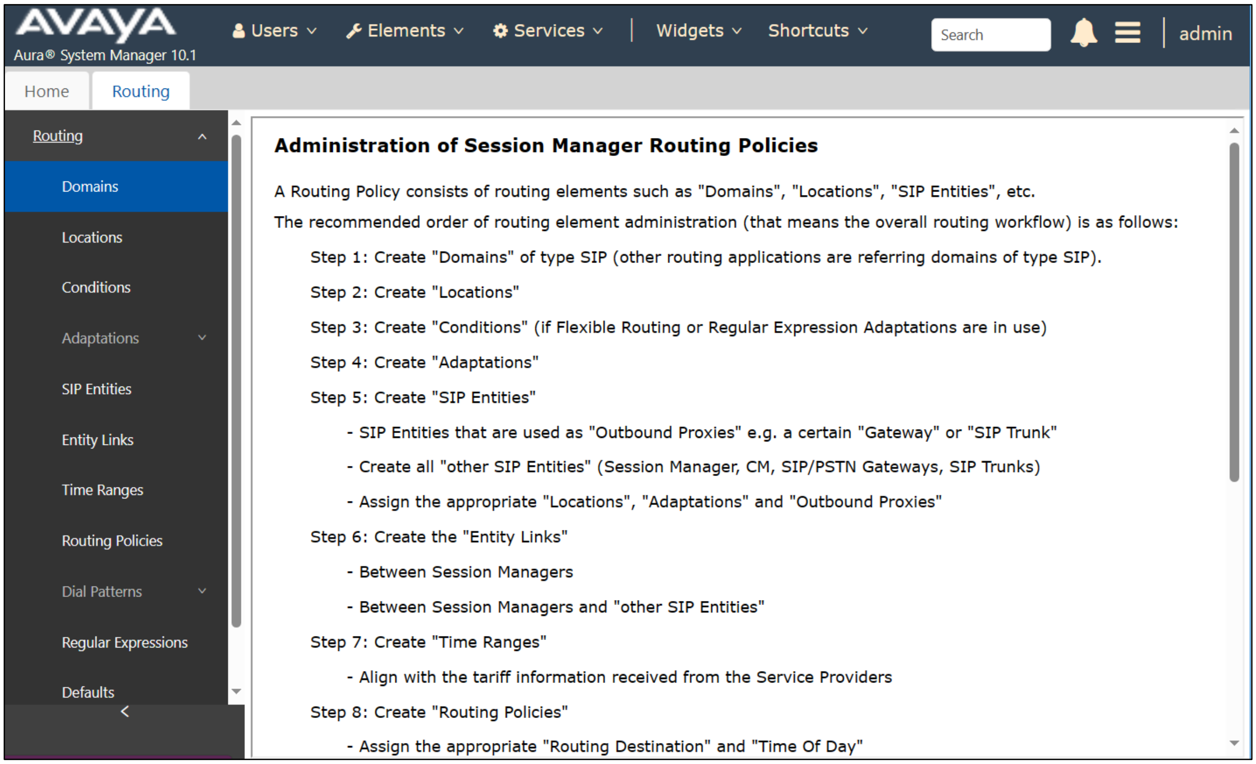
6.1. Launch System Manager

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**.

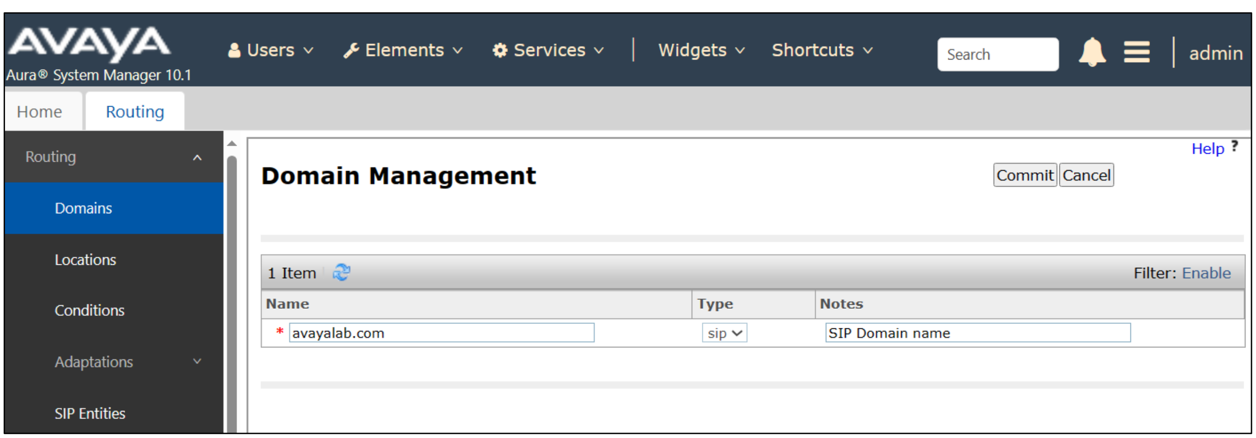


6.2. Administer Domain

In the subsequent screen (not shown), select **Elements → Routing** to display the **Administration of Session Manager Routing Policies** screen below. Select **Routing → Domains** from the left pane and click **New** in the subsequent screen (not shown) to add a new domain.



The **Domain Management** screen is displayed. In the **Name** field enter the domain name, select “sip” from the **Type** drop down menu and provide any optional **Notes**.



6.3. Administer Locations

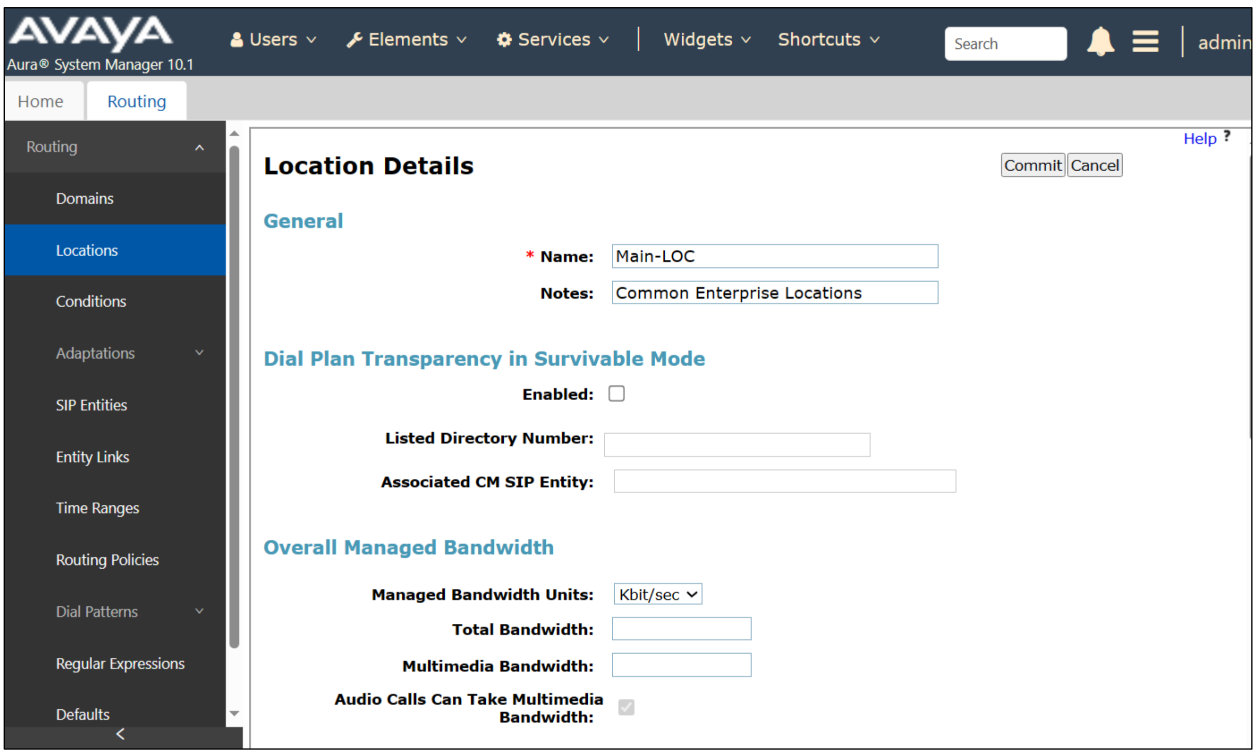
Locations identify logical and/or physical locations where SIP Entities reside, used for routing purposes. In the reference configuration, three locations are specified:

- **Main-LOC** – The enterprise site containing System Manager, Session Manager and other local servers and SIP endpoints.
- **CM-LOC** – Communication Manager, designated for Fonolo VCB.
- **SBC-LOC** – Avaya SBC.

6.3.1. Main Location

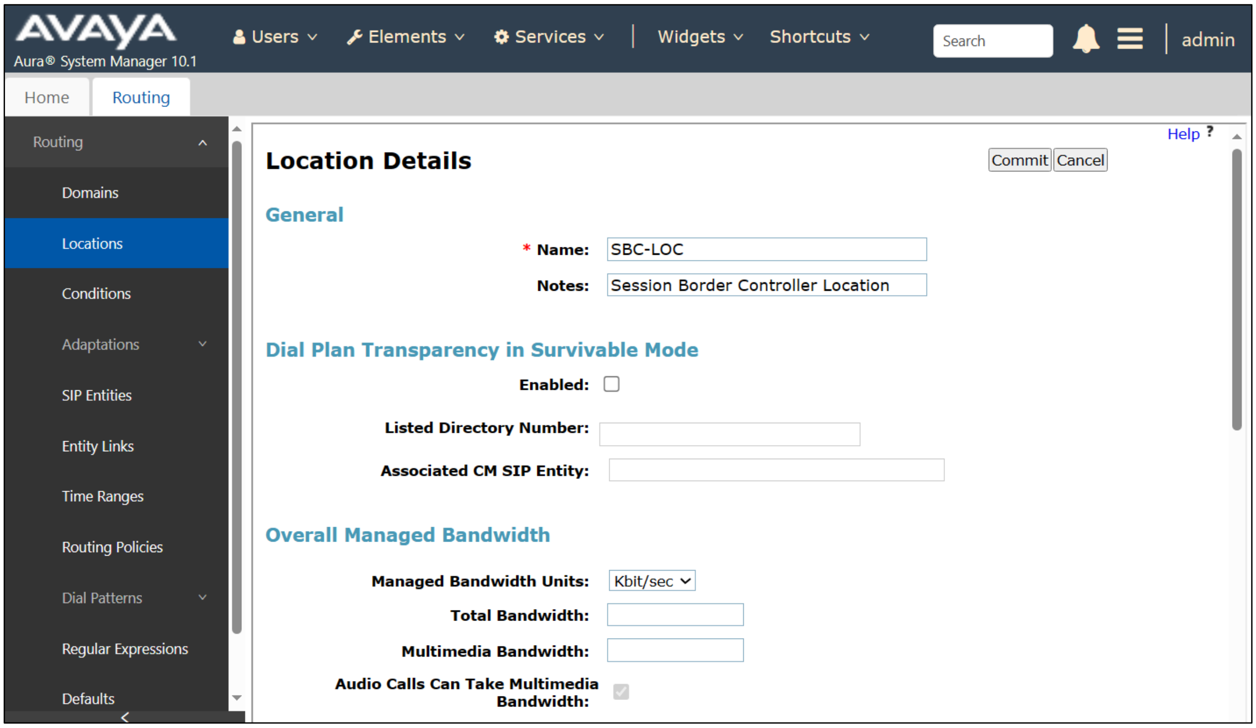
Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

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

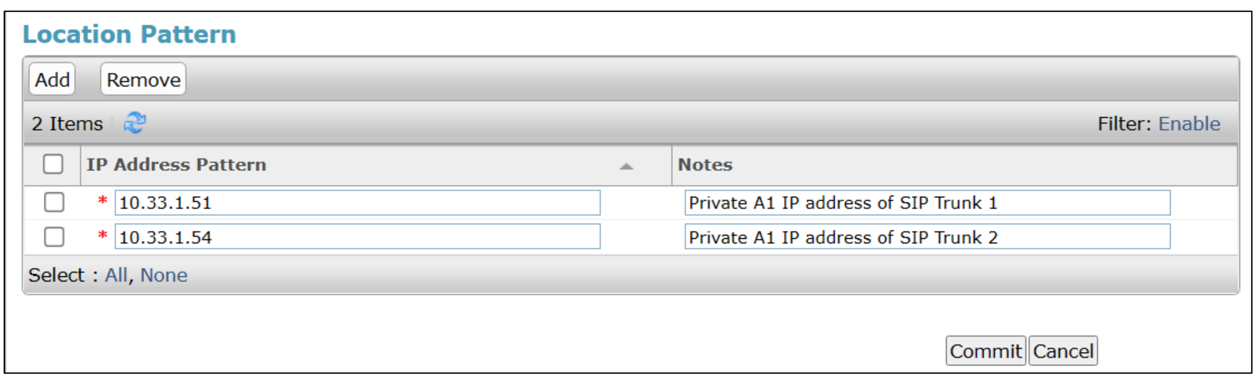


6.3.2. Avaya SBC Location

To configure Avaya SBC Location, repeat the steps in **Section 6.3.1** with the following changes:

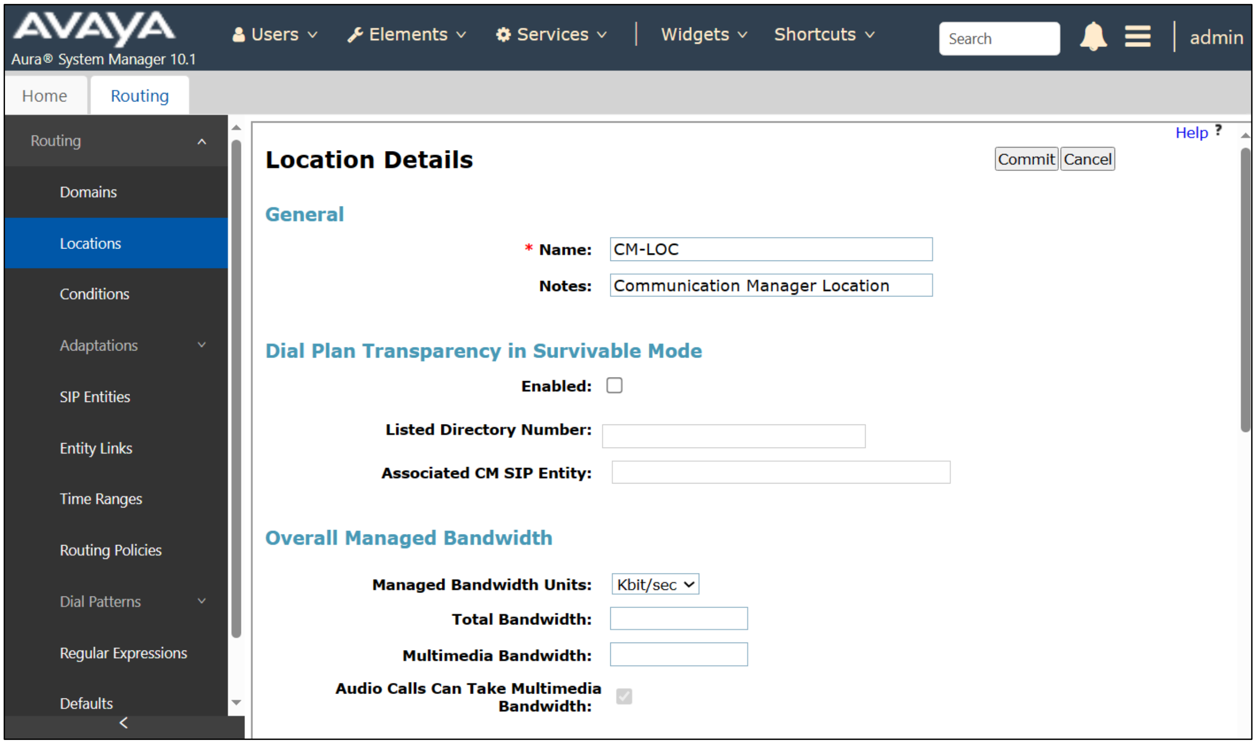


Scroll down to the **Location Pattern** sub-section, click **Add** and enter the private IP addresses of the SBC involved in the compliance testing in **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.

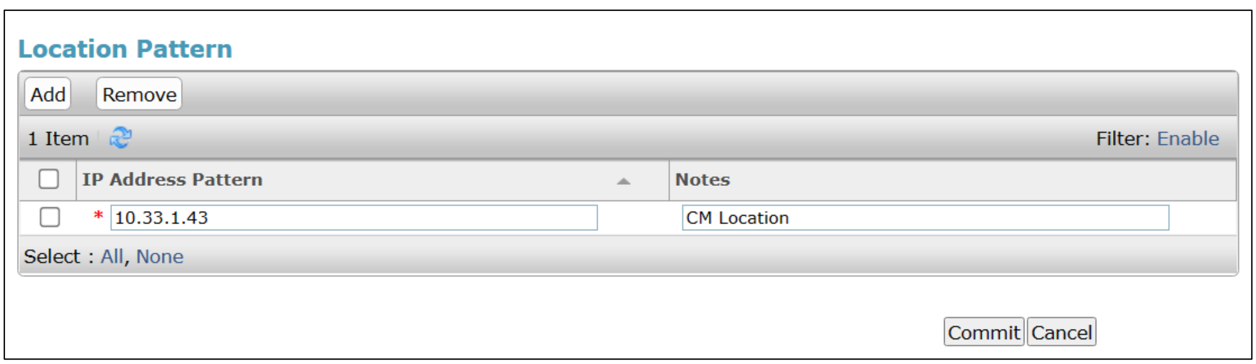


6.3.3. CM Location

To configure the Communication Manager location, repeat the steps in **Section 6.3.1** with the following changes:



Scroll down to the **Location Pattern** sub-section, click **Add** and enter the processor IP addresses of Communication Manager in **IP Address Pattern**, as shown below.

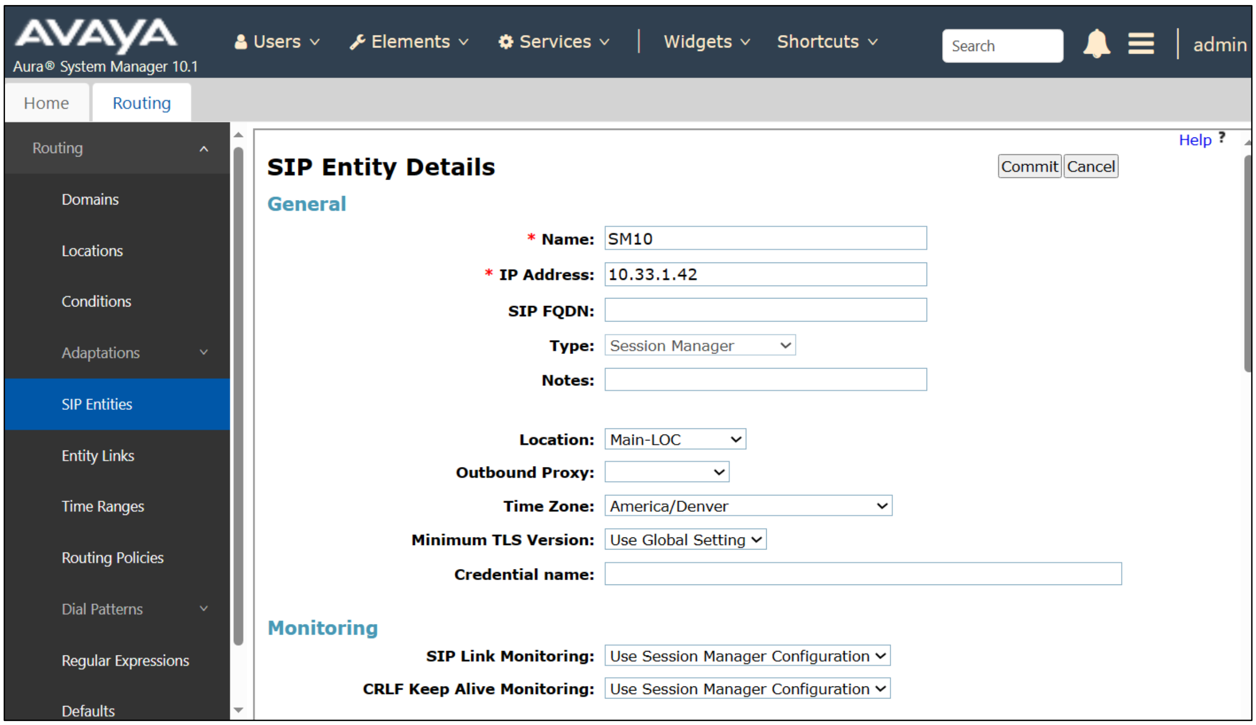


6.4. Administer SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager, which includes Communication Manager and Avaya SBC.

6.4.1. Configure Session Manager SIP Entity

The following screen shows the previously configured Session Manager SIP Entity named **SM10**. The IP address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.1.42** and select the location **Main-LOC** as defined in **Section 6.3.1** in the **Location** field.

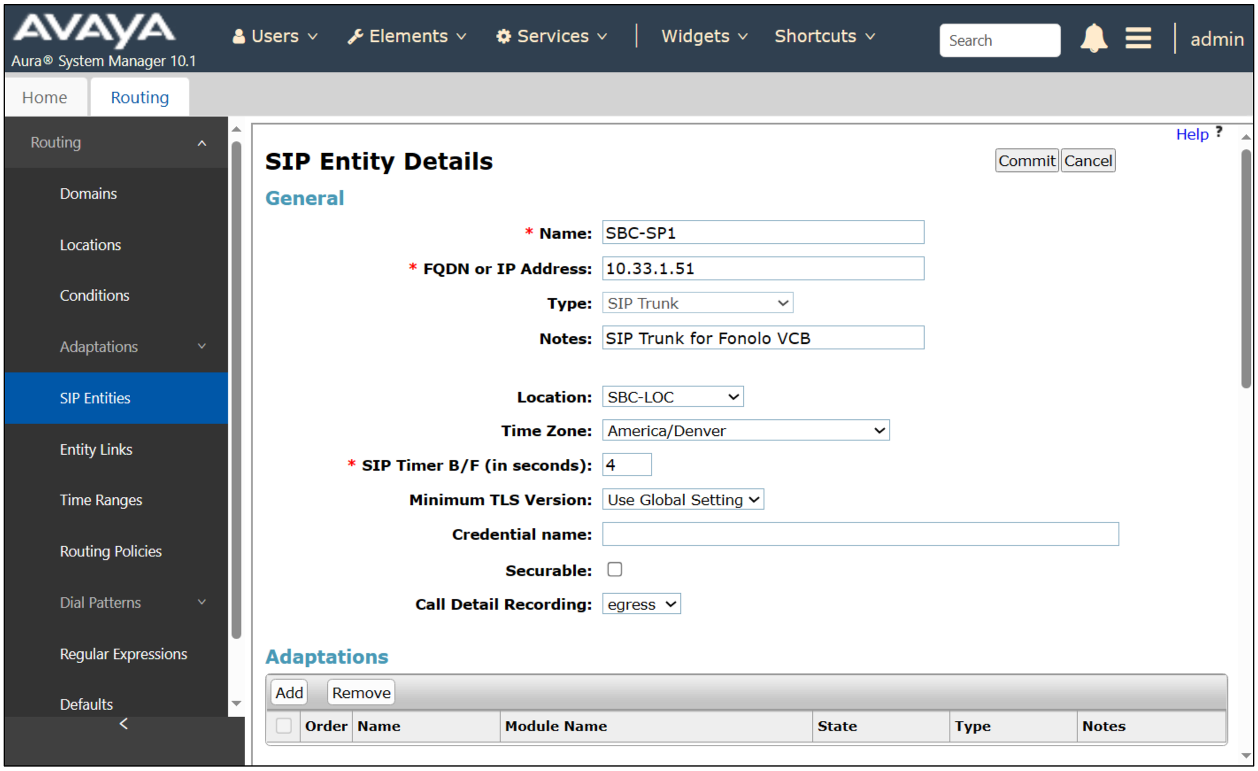


6.4.2. SIP Entity for Avaya SBC

Select **Routing → SIP Entities** from the left pane and click **New** in the subsequent screen (not shown) to add a new SIP entity for Avaya SBC.

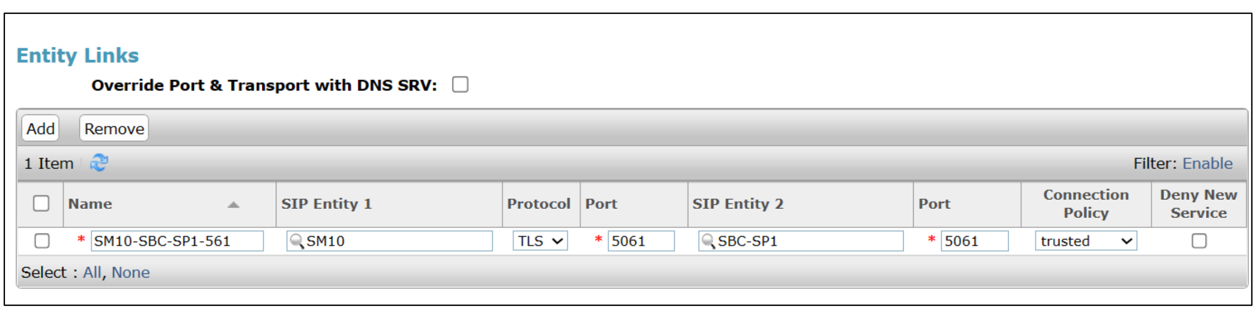
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** The IP address of private A1 interface of Avaya SBC.
- **Type:** Set is as"SIP Trunk".
- **Notes:** Enter desired notes.
- **Location:** Select the **SBC-LOC** location as defined in **Section 6.3.2**.
- **Time Zone:** Select the applicable time zone.
- **SIP Link Monitoring:** Select "Link Monitoring Enabled" (not shown).



Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case "SM10".
- **Protocol:** Set it as "TLS".
- **Port:** Set it as "5061".
- **SIP Entity 2:** Avaya SBC entity name from this section.
- **Port:** Set it as "5061".
- **Connection Policy:** **Select** "trusted".

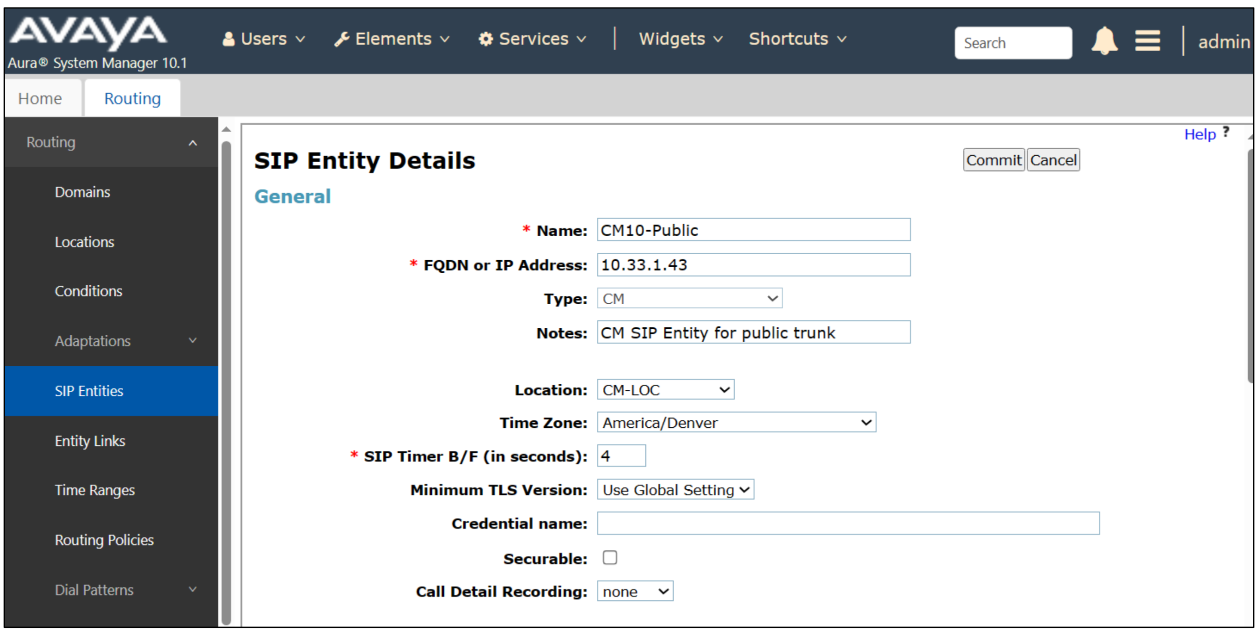


6.4.3. SIP Entity for Communication Manager

Select **Routing → SIP Entities** from the left pane and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager. Note that the screen below shows the previous configured SIP Entity of Communication Manager it is shown here for reference and display purpose.

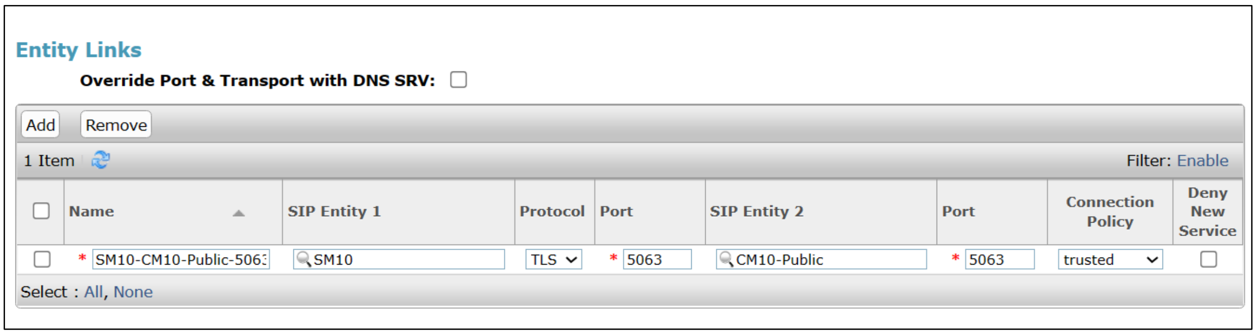
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** The IP address of the processor interface.
- **Type:** Select "CM".
- **Notes:** Any desired notes.
- **Location:** Select "CM-LOC" location as defined in **Section 6.3.3**.
- **Time Zone:** Select the applicable time zone.



Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case "SM10".
- **Protocol:** The signaling group transport TLS method.
- **Port:** The signaling group listen port 5063.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group listen port 5063 number.
- **Connection Policy:** Select "trusted".



6.5. Administer Routing Policies

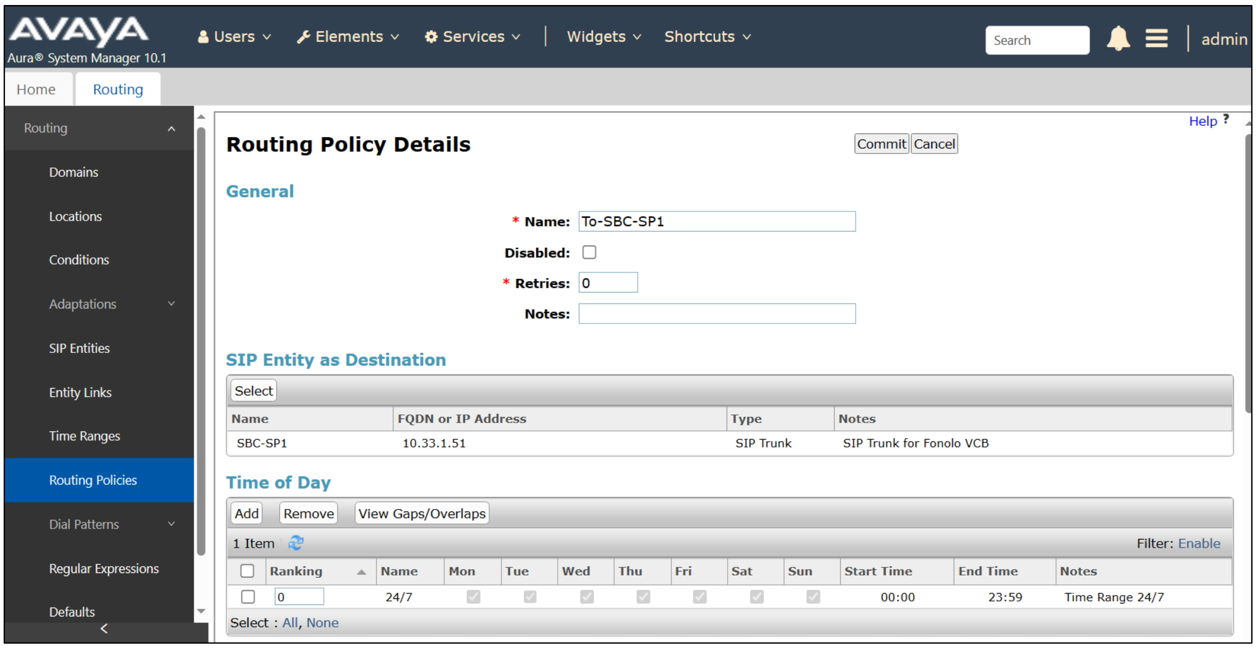
There were two routing policies used for the testing, one for Avaya SBC to reach to Fonolo VCB and one for Communication Manager.

6.5.1. Routing Policy for Avaya SBC

Select **Routing → Routing Policies** from the left pane and click **New** in the subsequent screen (not shown) to add a new routing policy for Avaya SBC.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the SBC SIP entity name as created from **Section 6.4.2** in the **SIP Entities** window (not shown), leave the **Time of Day** sub-section as default. Click **Commit** to save.

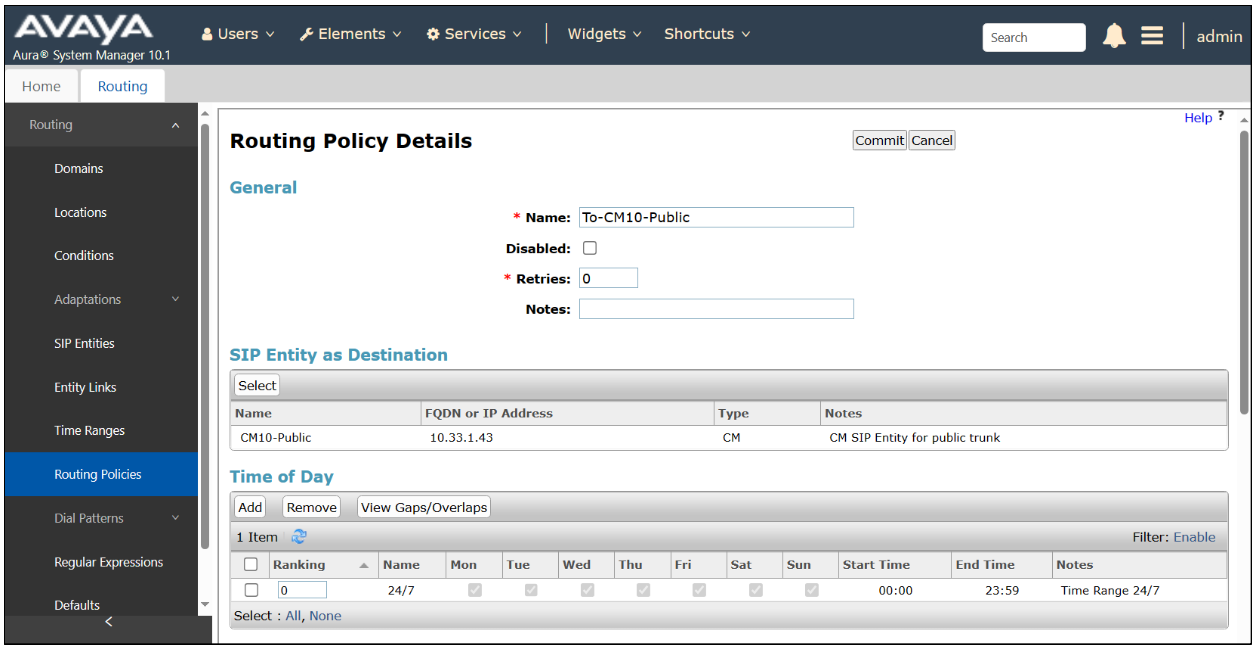


6.5.2. Routing Policy for Communication Manager

Select **Routing → Routing Policies** from the left pane and click **New** in the subsequent screen (not shown) to add a new routing policy for Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager SIP entity in the **SIP Entities** window (not shown) and leave the **Time of Day** field as default. Click **Commit** to save.



6.6. Administer Dial Patterns

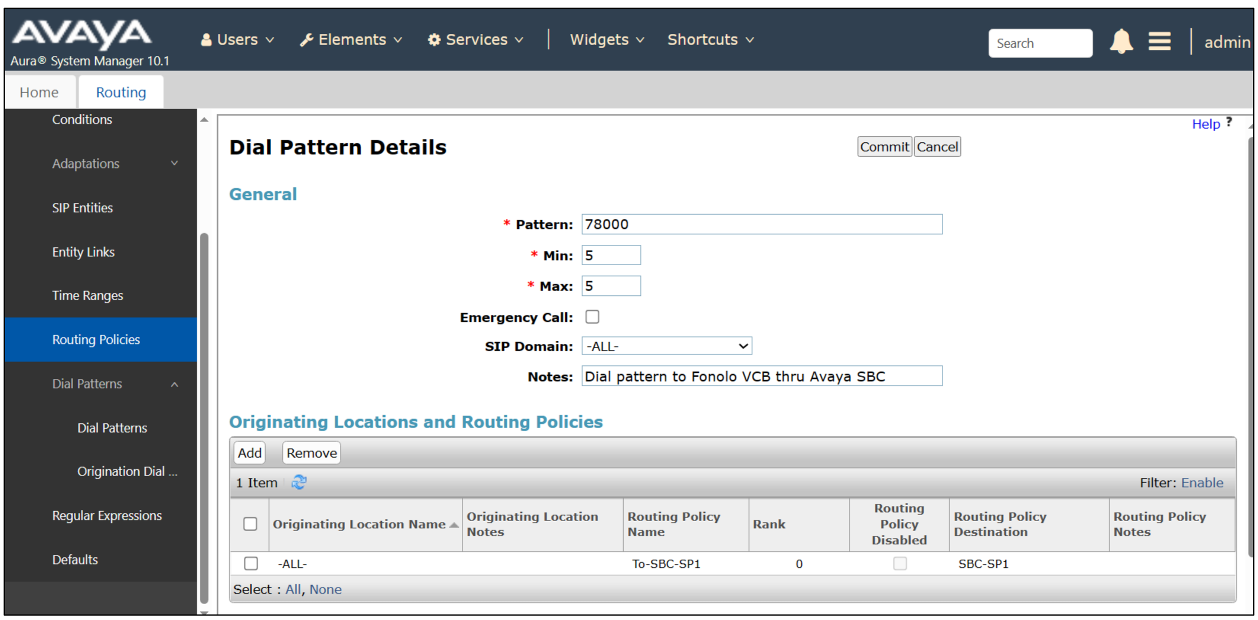
Dial patterns are defined to direct calls to the appropriate SIP Entity. In the sample configuration, dial pattern 78000 was routed to the Fonolo VCB, through Avaya SBC and the dial pattern 3340 was routed to Communication Manager.

6.6.1. Dial Pattern for 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., **78000**).
- **Min** and **Max** – Minimum and maximum length of dialed number (e.g., **5)**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Avaya SBC. In the compliance testing, the entry allowed for call originations from all Communication Manager endpoints in locations "All". The SBC routing policy from **Section 6.5.1** was selected as shown below.

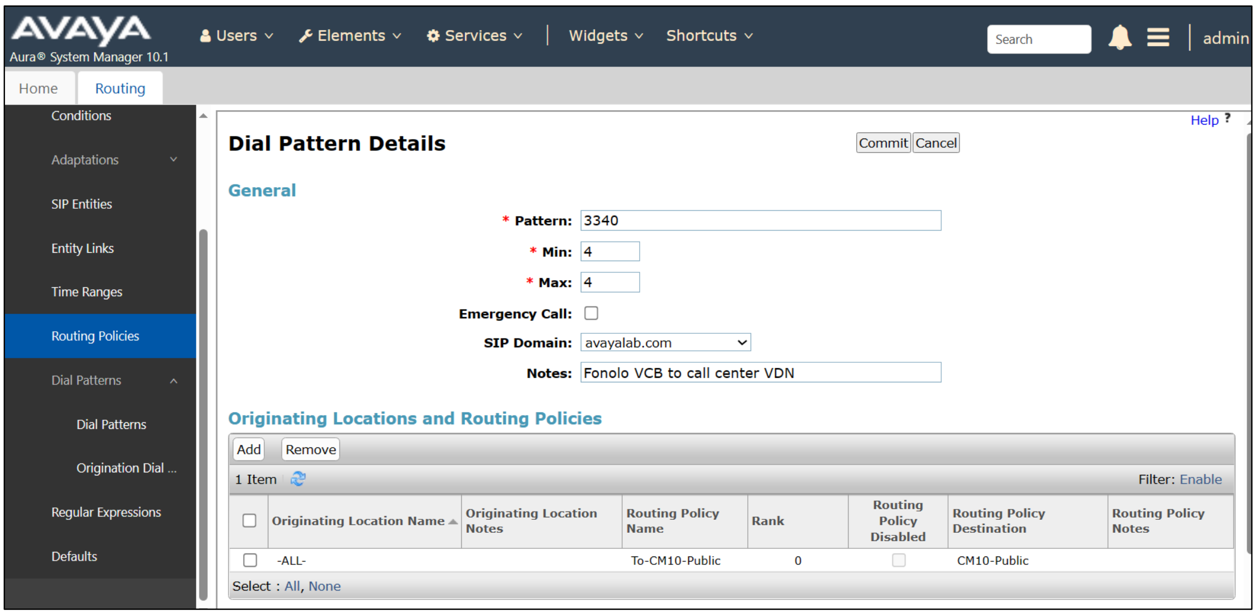


6.6.2. Dial Pattern for Communication Manager

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., **3340**).
- **Min** and **Max** – Minimum and maximum length of dialed number (e.g., **4)**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Communication Manager. In the compliance testing, the entry allowed for call originations from all locations "All". The CM routing policy from **Section 6.5.2** was selected as shown below.



7. Configure Avaya Session Border Controller

This section describes the required configuration of Avaya SBC to connect to Fonolo VCB using Cloud SIP Connect.

It is assumed that Avaya SBC was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBC web interface.

Note: In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

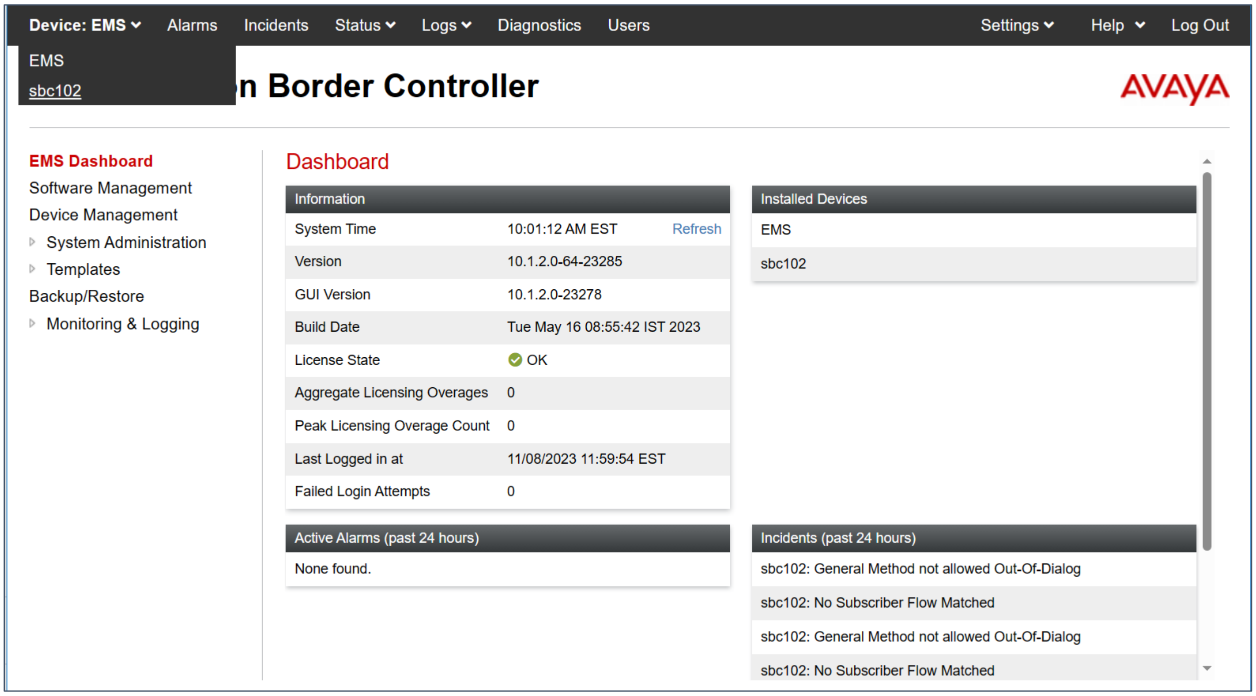
7.1. Log in Avaya Session Border Controller

Use a Web browser to access the Avaya SBC Web interface. Enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the Avaya SBC management IP address.

Enter the appropriate credentials and click **Log In**.

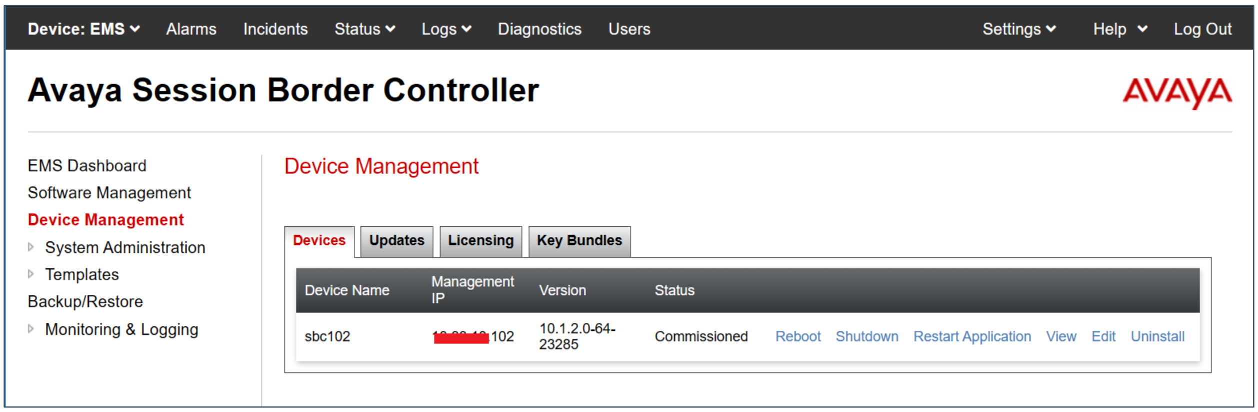
Once logged in, on the top left of the screen, under **Device:** select the device being managed, **sbc102** in the sample configuration.

The left navigation pane contains the different available menu items used for the configuration of Avaya SBC. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.



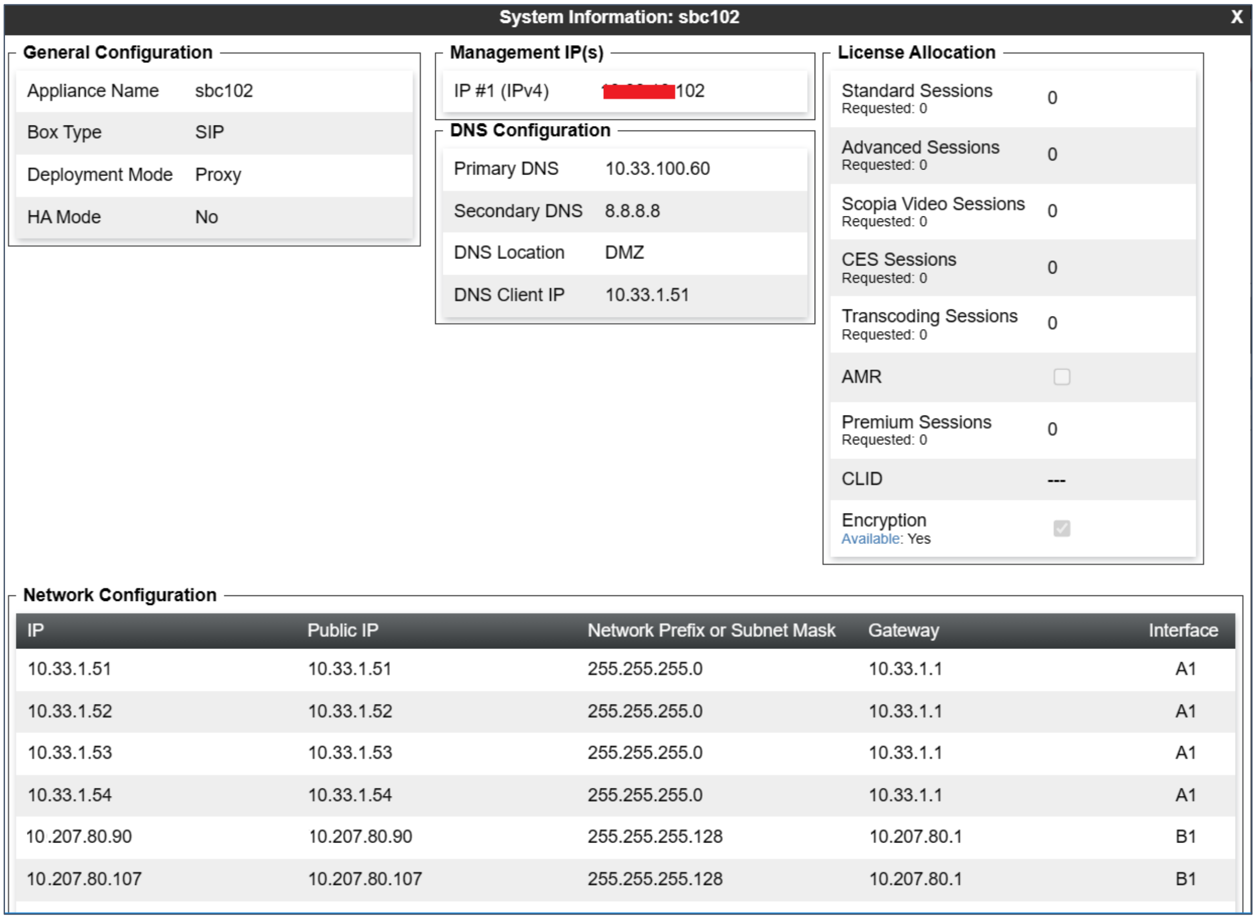
7.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named **sbc102** is shown. The management IP address that was configured during installation is masked out for security reasons; the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of Avaya SBC, segmented from all VoIP traffic. Verify that the **Status** is **Commissioned**, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.



To view the network configuration assigned to the SBC, click **View** on the screen above. The **System Information** window is displayed, containing the current device configuration and network settings.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.



The IP addresses in the **System Information** screen shown above are the ones used for the SIP trunk to the Fonolo VCB and are the ones relevant to these Application Notes. Other IP addresses assigned to the SBC **A1** and **B1** interfaces are used to support remote workers and other SIP trunks, and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked out in this document.

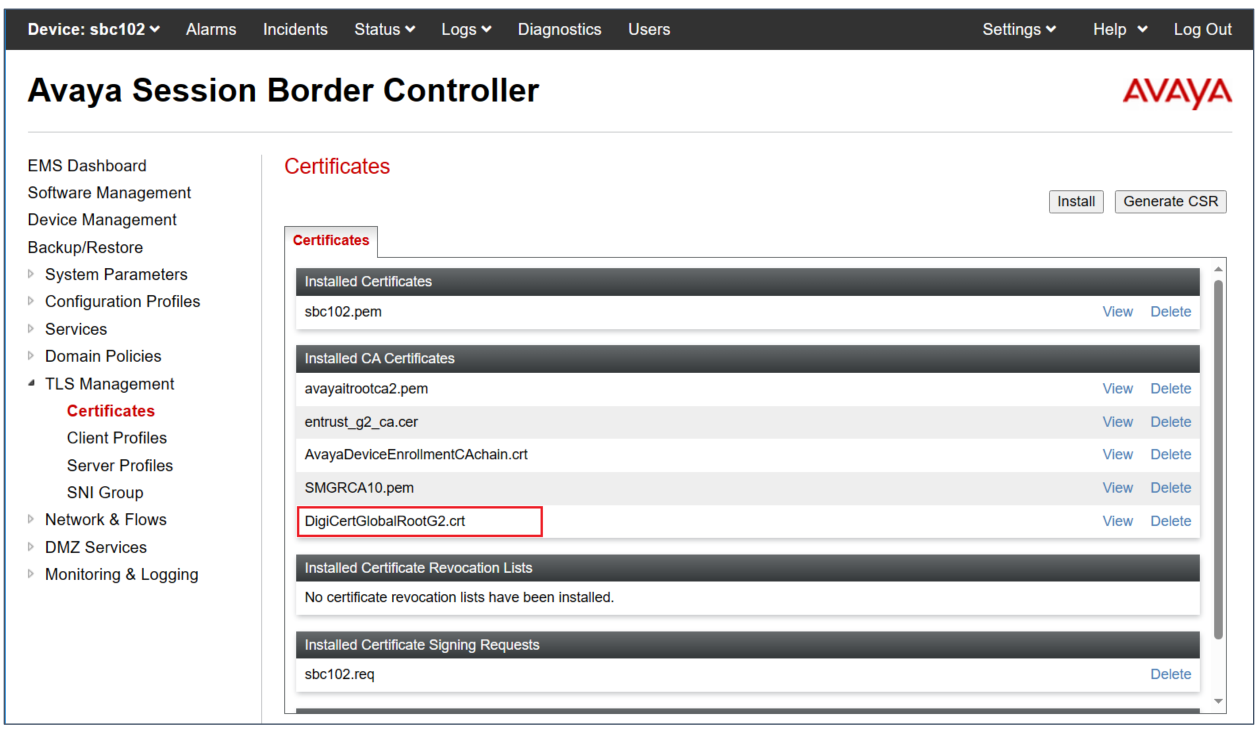
In the reference configuration, the private interface of the SBC (10.33.1.51) was used to connect to the enterprise network, while its public interface (10.207.80.107) was used to connect to the Fonolo VCB. See **Figure 1**.

7.3. TLS Management

Note –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.

The TLS connection from Avaya SBC to Fonolo Cloud SIP Connect 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 Fonolo Cloud SIP Connect, so the DigiCert Global Root G2 certificate needed to be downloaded and imported into Avaya SBC trust store.

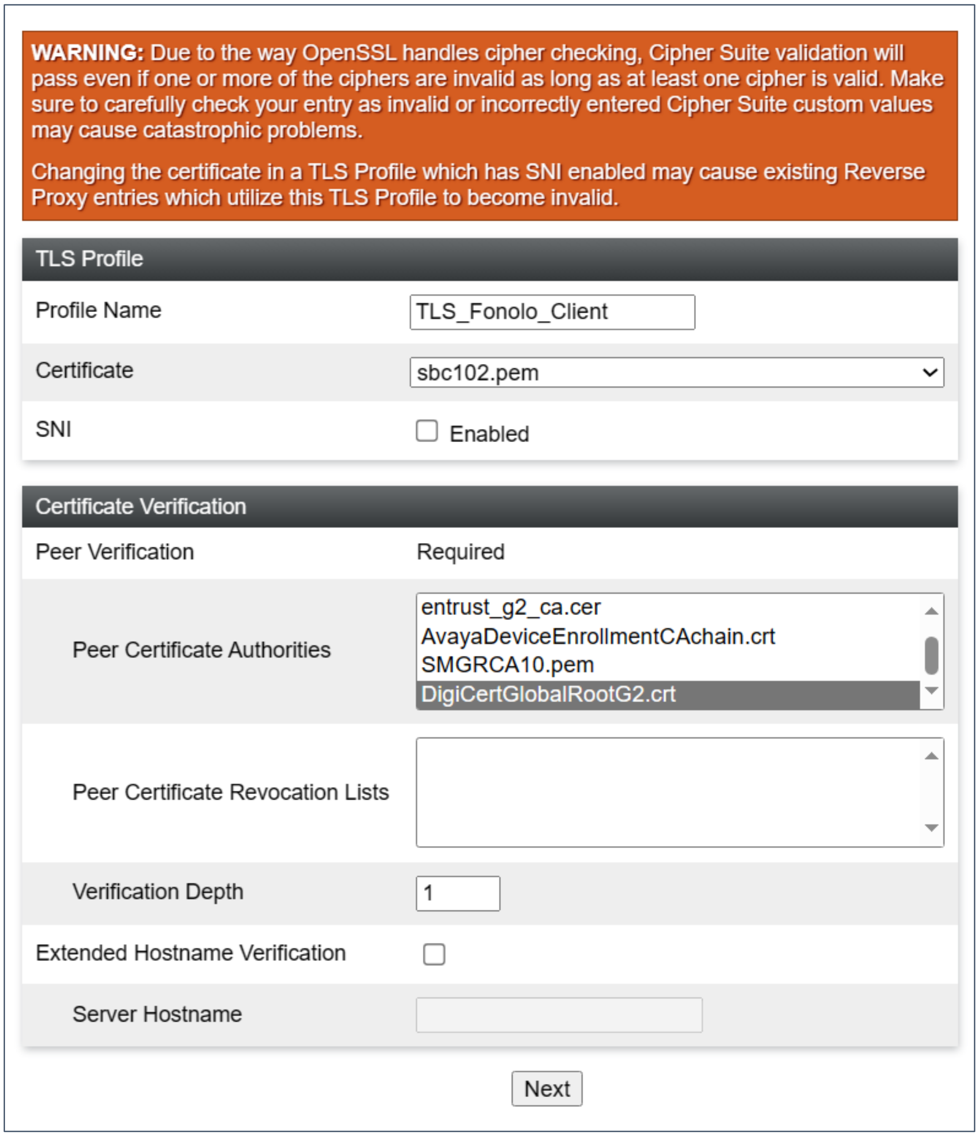
In the reference configuration, TLS transport is used for the communication between Avaya SBC and Fonolo Cloud SIP Connect. This section covers the installation of the root certificate and the configuration of the TLS client profile, used in the connection to Fonolo Cloud SIP Connect. By default, the DigiCert Global Root G2 certificate is already installed in the trusted CA of Avaya SBC as shown below.



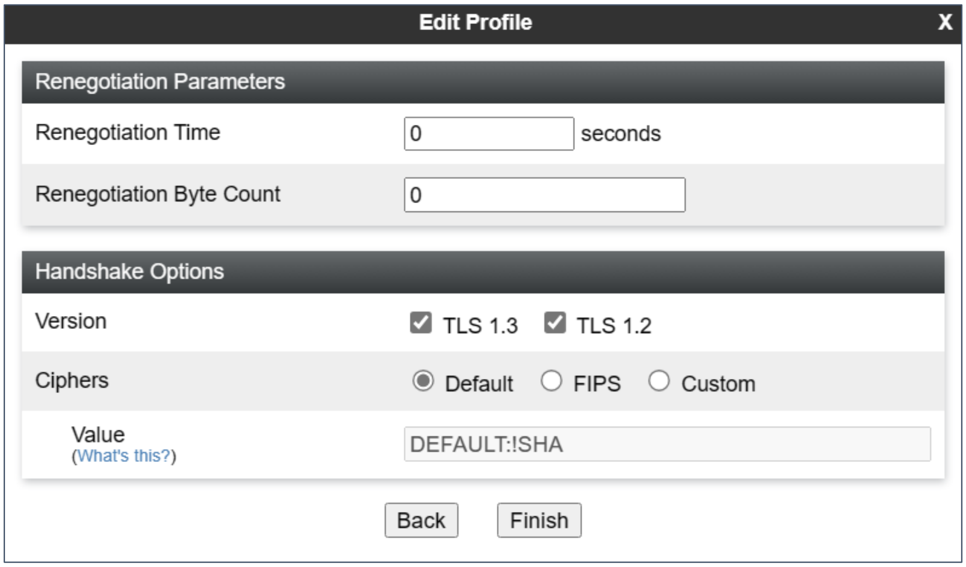
7.3.1. TLS Client Profile for Fonolo Cloud SIP Connect

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

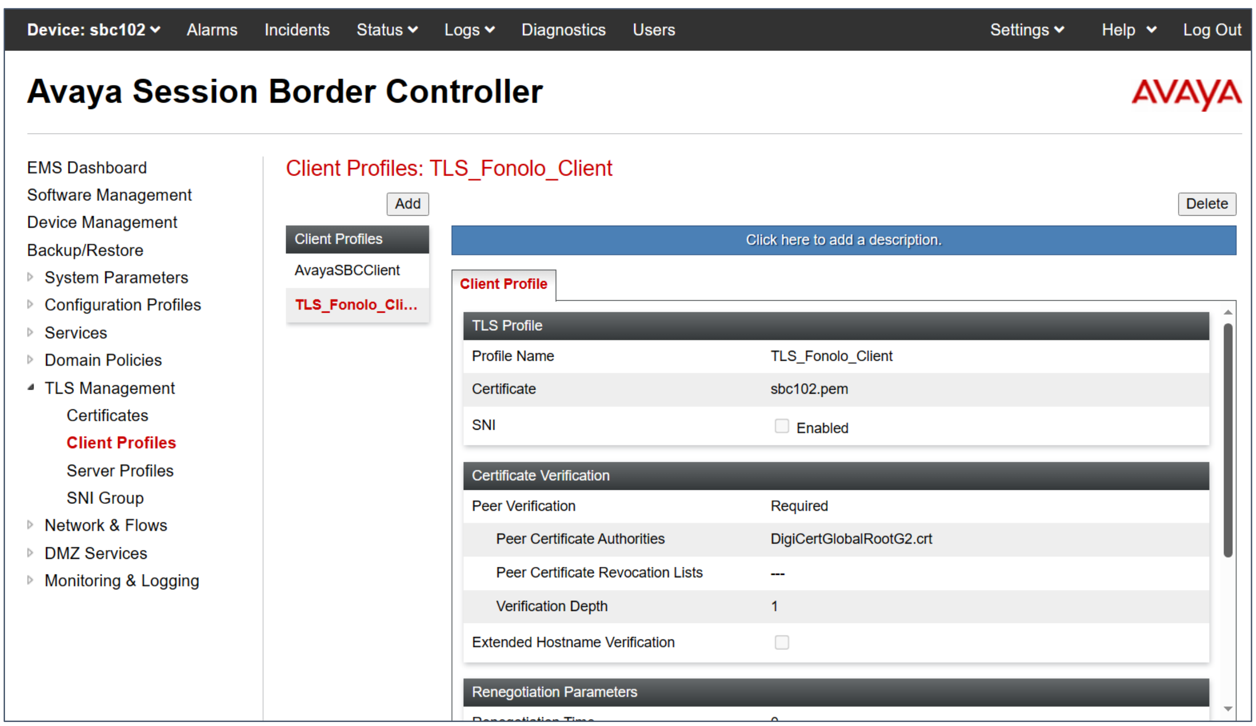
- **Profile Name:** enter descriptive name.
- **Certificate:** select the existing SBC identity certificate from the pull-down menu.
- **Peer Verification** = **Required**.
- **Peer Certificate Authorities:** Select the **DigiCertGlobalRootG2.pem** certificate.
- **Verification Depth:** enter **1**.
- Click **Next**.



Make sure the **TLS 1.2** is selected and click **Finish** on the next window to save configuration.



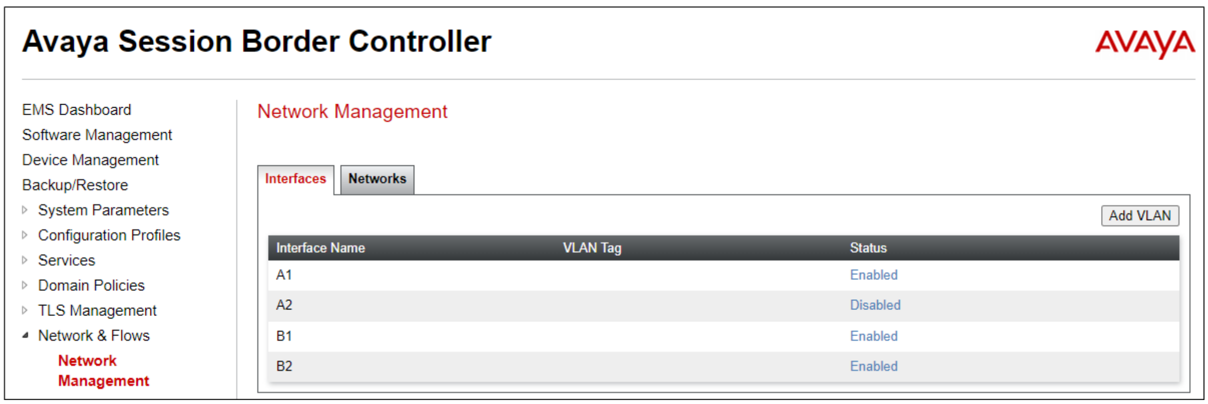
The following screen shows the completed TLS **Client Profile** form:



7.4. 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.

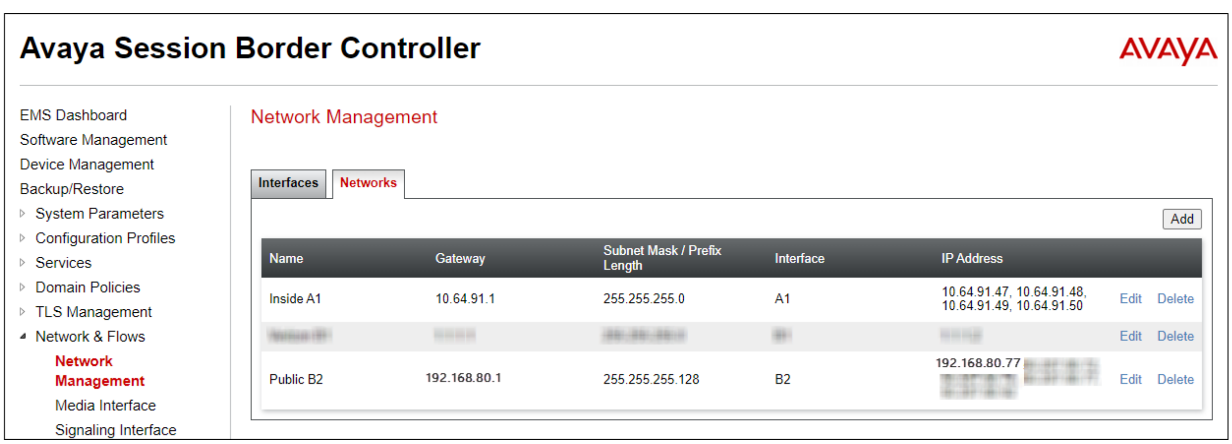
Select **Networks & Flows → Network Management** from the menu on the left-hand side. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 and B2 are used.



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 Fonolo VCB traffic:

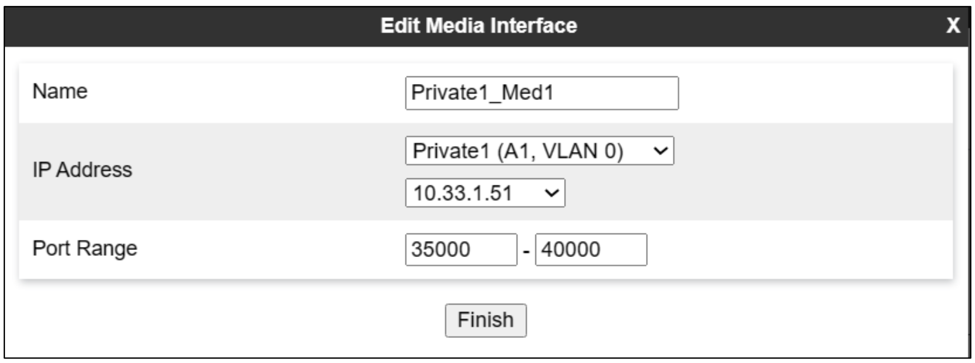
- **A1**: **10.33.1.51** – "Inside" IP address, toward Session Manager.
- **B1: 10.207.80.107** – "Outside" IP address toward the SIP trunk to Fonolo Cloud SIP Connect.



7.5. Media Interfaces

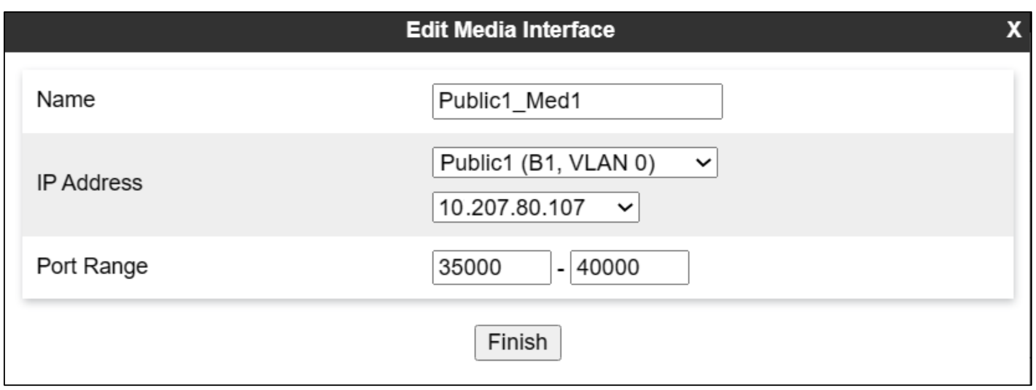
To add to the internal media interface toward the enterprise select **Network & Flows → Media Interface** from the menu on the left-hand side. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name**: Enter an appropriate name (e.g., **Private1_Med1**).
- **IP Address**: Select **PrivateA1 (A1,VLAN0)** and the IP address used for traffic towards Communication Manager (e.g., **10.33.1.51**) from the drop-down menus.
- **Port Range**: **35000 – 40000**.
- Click **Finish**.



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

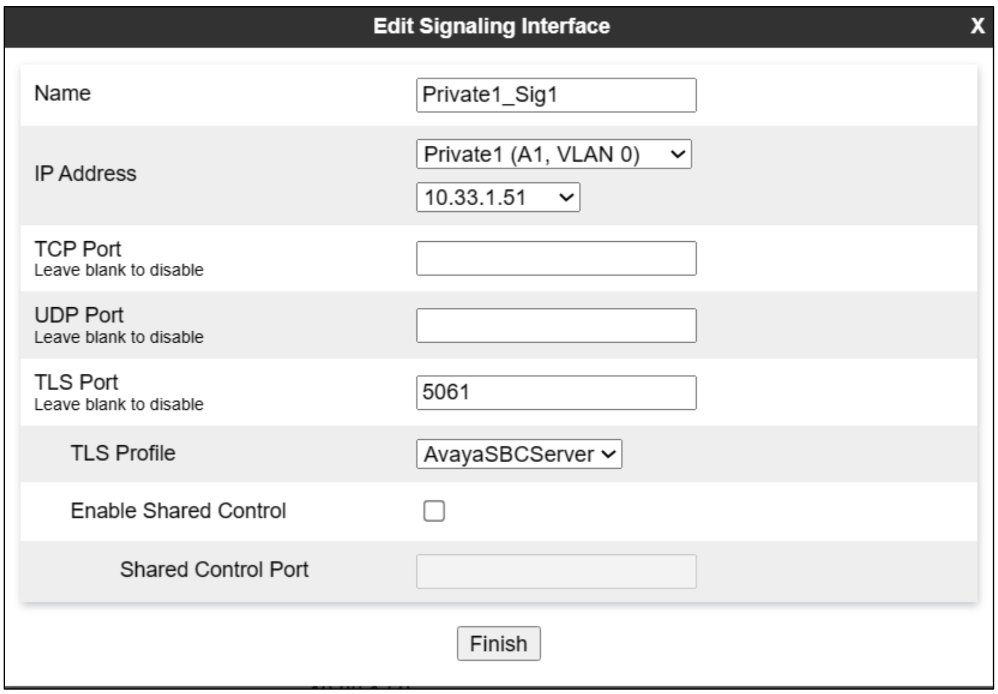
- **Name**: Enter an appropriate name (e.g., **Public1_Med1**).
- **IP Address**: Select **Public1 (B1, VLAN0)** and the IP address used for the SIP trunk to Fonolo VCB (e.g., **10.207.80.107**) from the drop-down menus.
- **Port Range**: **35000 – 40000**.
- Click **Finish**.



7.6. Signaling Interfaces

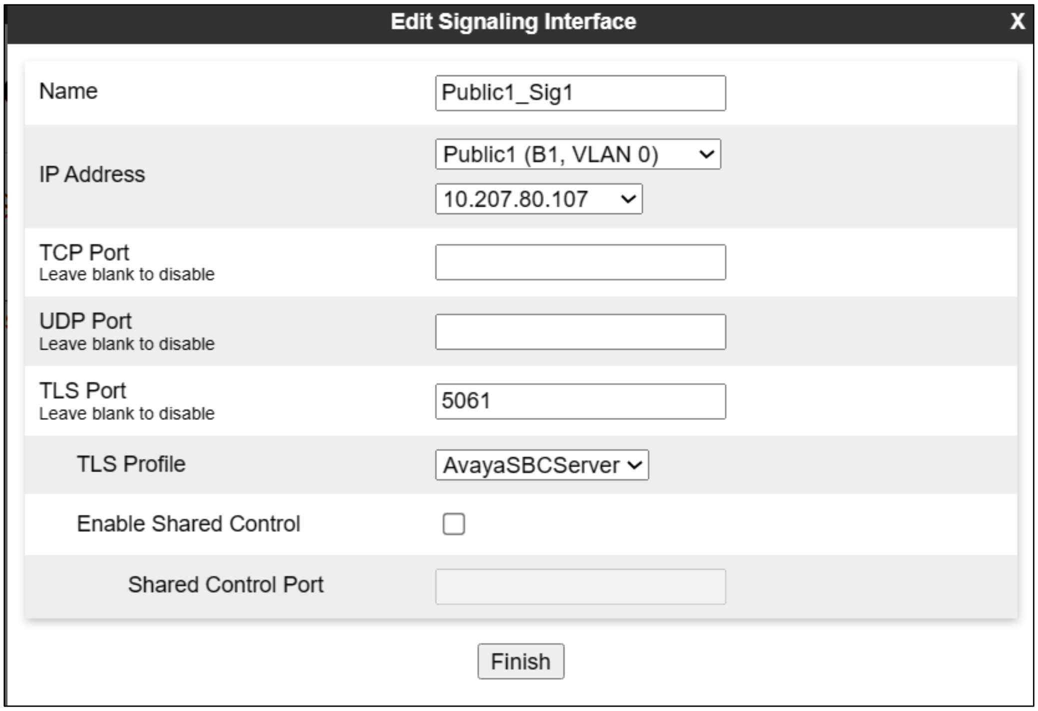
Select **Network & Flows → Signaling Interface** from the menu on the left-hand side.
Select **Add** (not shown) to add to the internal signaling interface toward the enterprise. Enter the following:

- **Name**: Enter an appropriate name (e.g., **Private1_Sig1**).
- **IP Address**: Select **Private1 (A1, VLAN0)** and **10.33.1.51**.
- **TLS Port**: **5061**.
- **TLS Profile**: Select the existing TLS server profile on the enterprise (e.g., **AvayaSBCServer**). See **Note** on **Section 7.3.**
- Click **Finish**.



Select **Add** (not shown), to add to the external signaling interface toward the Fonolo VCB

- **Name**: Enter an appropriate name (e.g., **Public1_Sig1**).
- **IP Address**: Select **Public1 (B1, VLAN0)** and **10.207.80.107.**
- **TLS Port**: **5061.**
- **TLS Profile**: Select the existing TLS server profile on the enterprise (e.g., **AvayaSBCServer**). See **Note** on **Section 7.3**.



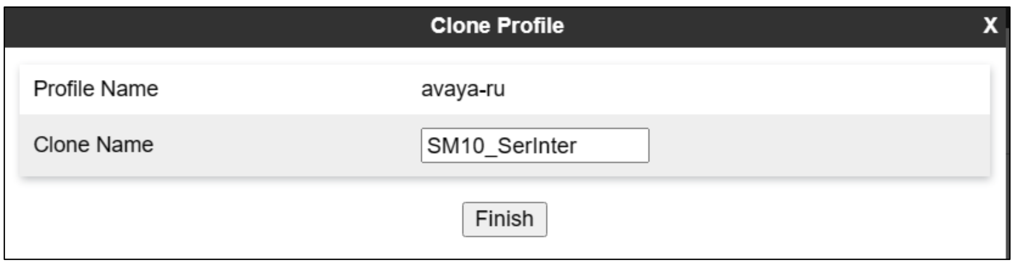
7.7. Server Interworking Profiles

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

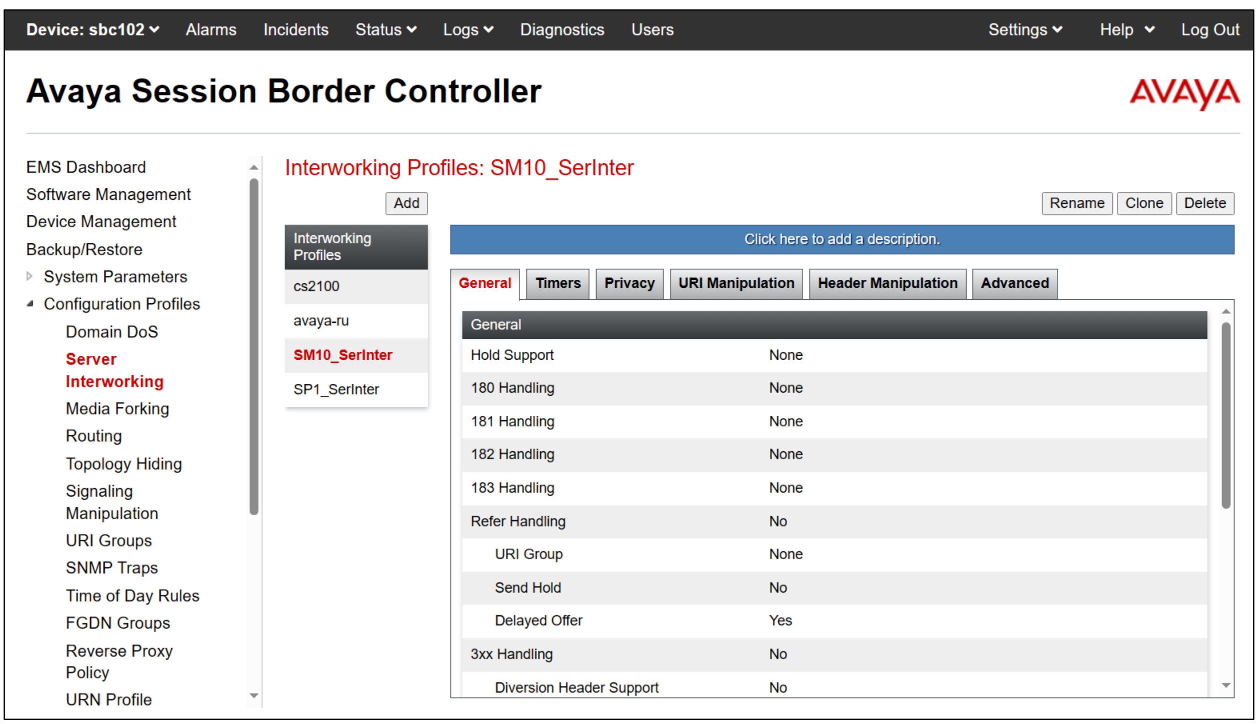
7.7.1. Server Interworking Profile for Session Manager

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.

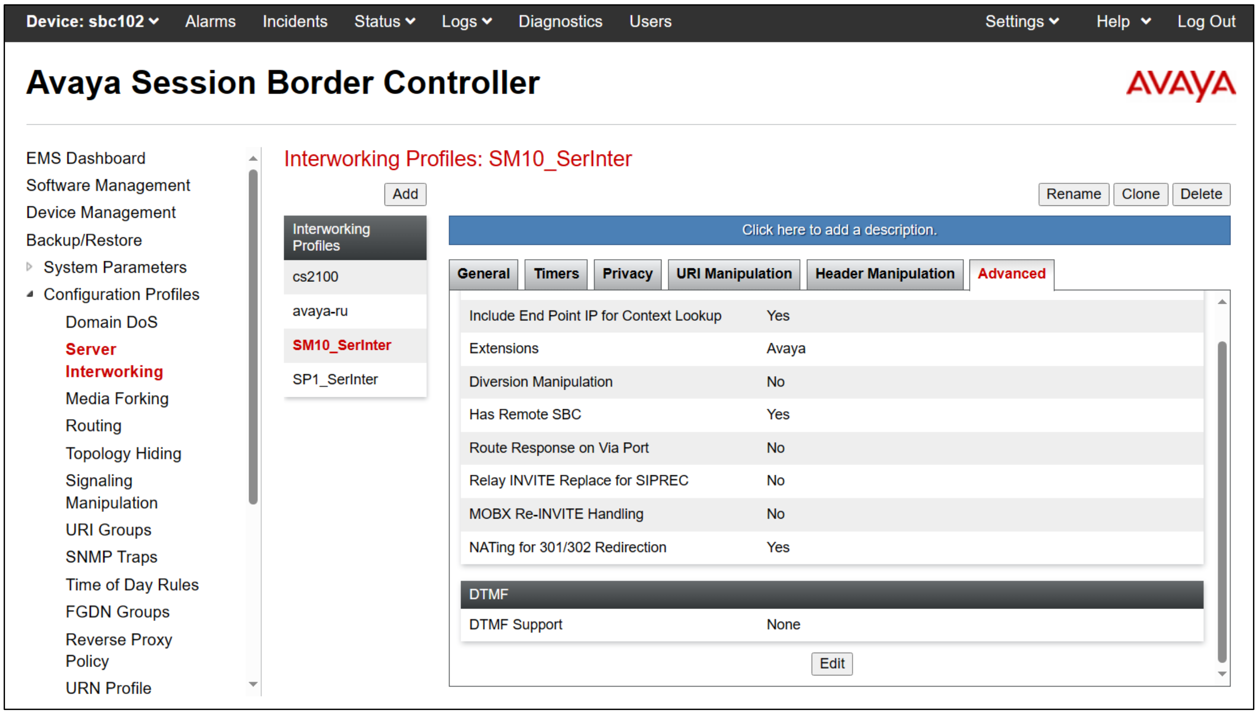
- Select the pre-defined **avaya-ru** profile and click the **Clone** button.
- Enter profile name: (e.g., **SM10_SerInter** and click **Finish** to continue.



The **General** tab below shows the default settings used.



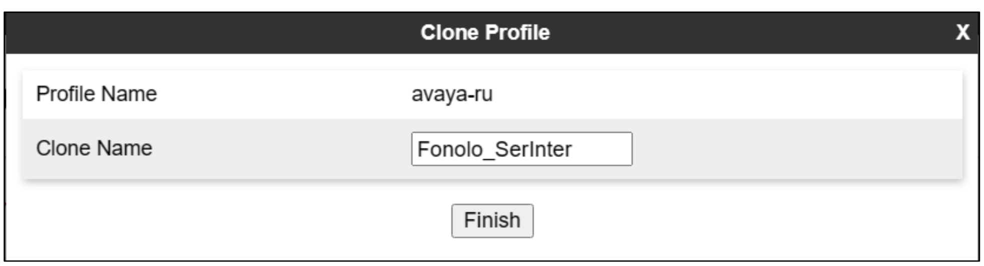
The Advanced tab below shows the default settings used.



7.7.2. Server Interworking Profile for Fonolo VCB

The server interworking profile used in the connection to the Fonolo VCB 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., **Fonolo_SerInter**), and click **Finish**.



7.8. SIP Server Profiles

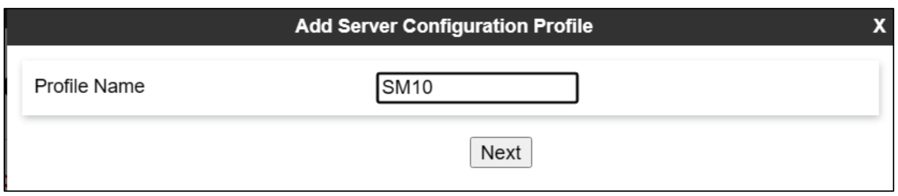
SIP Server Profiles are required for each server connected to Avaya SBC. A new server profile was created for Fonolo VCB. The SIP Server Profile for Session Manager was already in place and reused in the configuration.

Note: Avaya SBC in the test configuration used identity 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.

7.8.1. SIP Server Profile – Session Manager

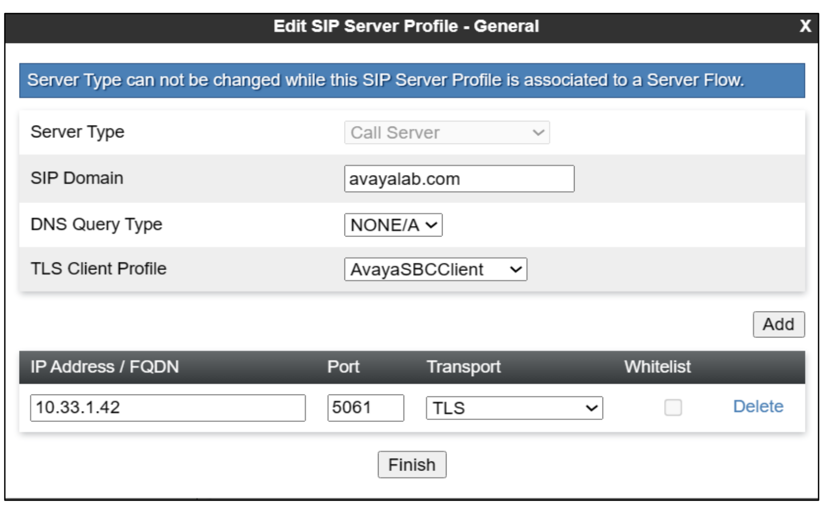
This section defines the SIP Server Profile for Avaya SBC connection to Session Manager.

- Select **Services → SIP Servers** from the left-hand menu.
- Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **SM10**) and click **Next**.



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

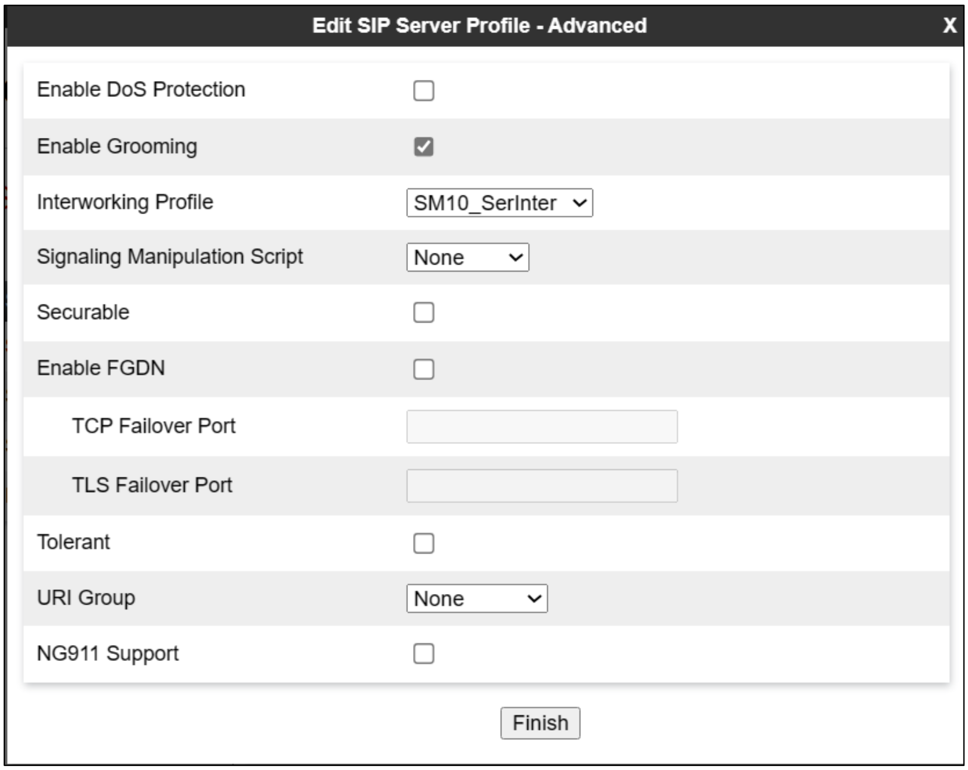
- **Server Type**: **Call Server**.
- **TLS Client Profile**: Select the existing TLS client profile on the enterprise (e.g., **AvayaSBCClient**).
- **IP Address**: **10.33.1.42** (Session Manager Security Module IP address).
- Select **Port**: **5061**, **Transport**: **TLS**.
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



Default values can be used on the **Authentication** tab.

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

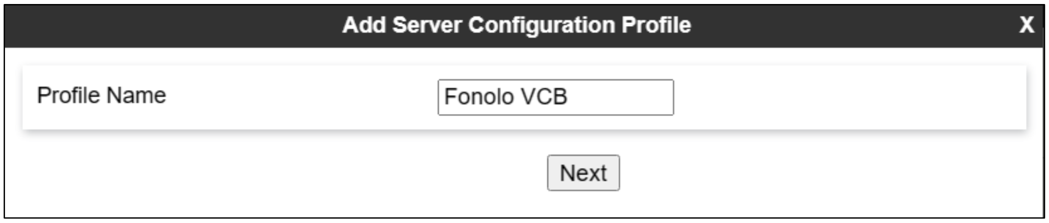
- Select the **SM10_SerInter** (**Section 7.7.1**), for **Interworking Profile**.
- Since TLS transport is specified, then the **Enable Grooming** option should be enabled.
- In the **Signaling Manipulation Script** field select **none**.
- Select **Finish**.



7.8.2. SIP Server Profile – Fonolo VCB

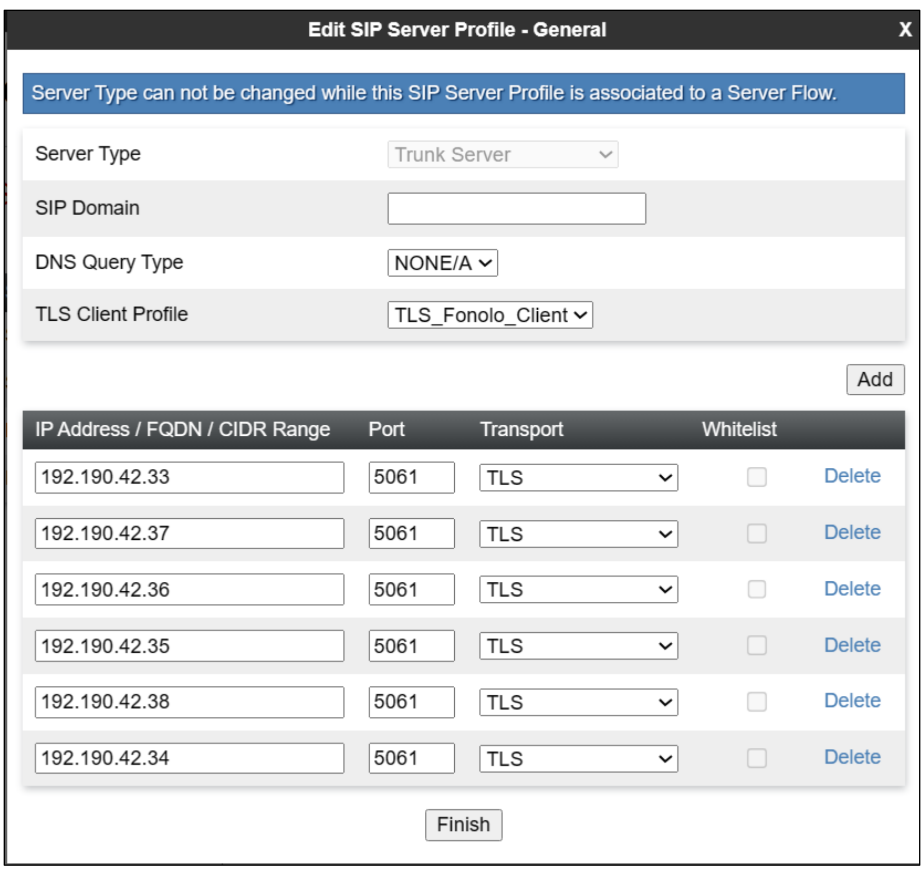
Repeat the steps in **Section 7.8.1**, with the following changes, to create a SIP Server Profile for Avaya SBC connection to Fonolo VCB.

Select **Add** and enter a Profile Name (e.g., **Fonolo VCB**) and select **Next**.

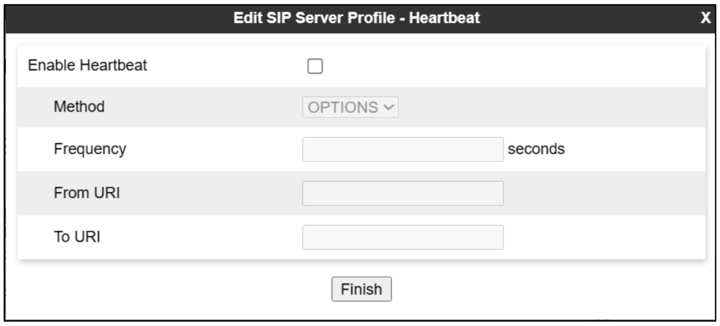


On the **General** window, enter the following:

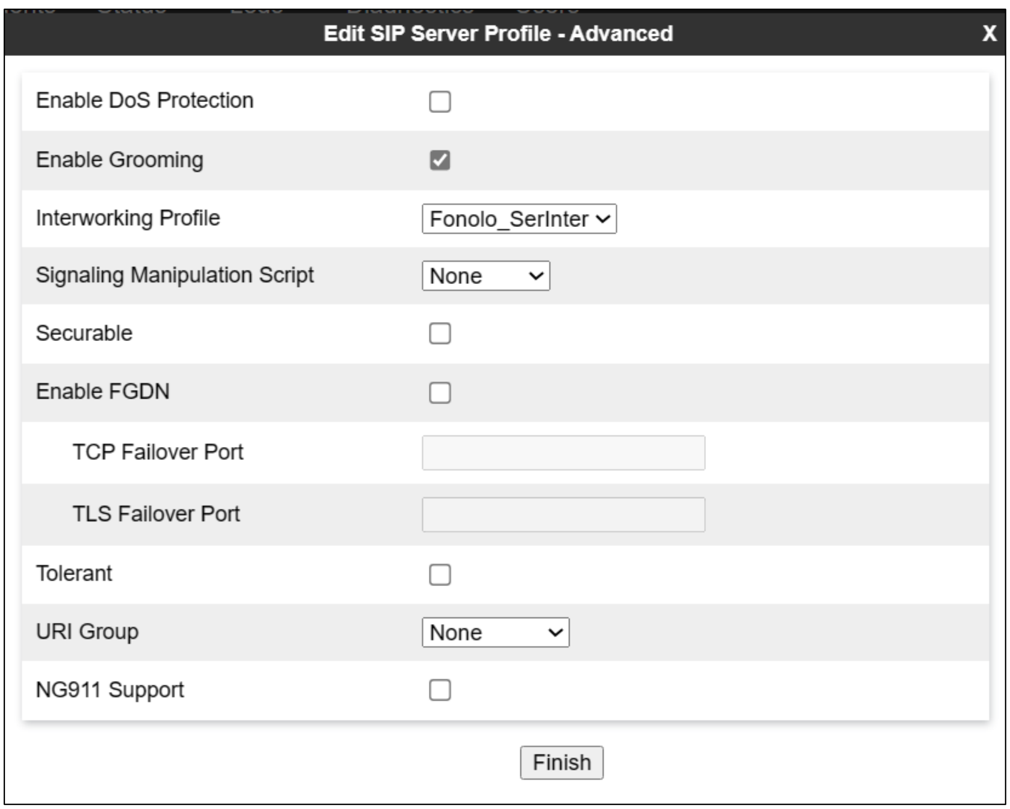
- **Server Type: Trunk Server**.
- **TLS Client Profile**: Select the client profile created in **Section 7.3.1**.
- Select **Add** and enter the IP addresses for the SIP connections to Fonolo VCB, provided by Fonolo. The service used in the reference configuration consists of 6 IP addresses.
- Select **Port**: **5061**, **Transport**: **TLS**.
- If adding the profile, click **Next** (not shown) to proceed to next tab.



Default values are used on the **Authentication** tab. On the **Heartbeat** tab, keep it as default (uncheck the **Enable Heartbeat)** to have Avaya SBC forward OPTIONS message from Session Manager to the Fonolo Cloud SIP servers. 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 **Fonolo_SerInter** (**Section 7.7.2**), for **Interworking Profile**. All other parameters retain their default values.



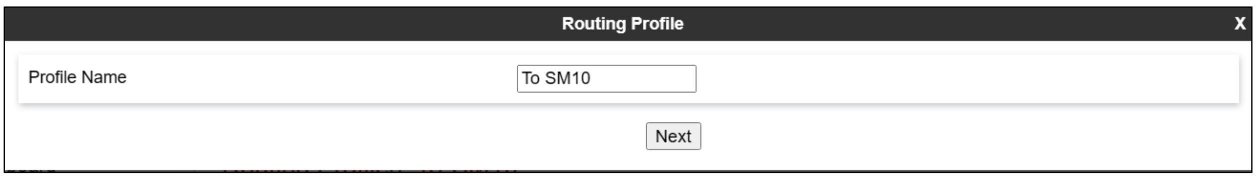
7.9. Routing Profiles

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 7.13**. The IP addresses and ports defined here will be used as destination addresses for signaling.

7.9.1. Routing Profile – Session Manager

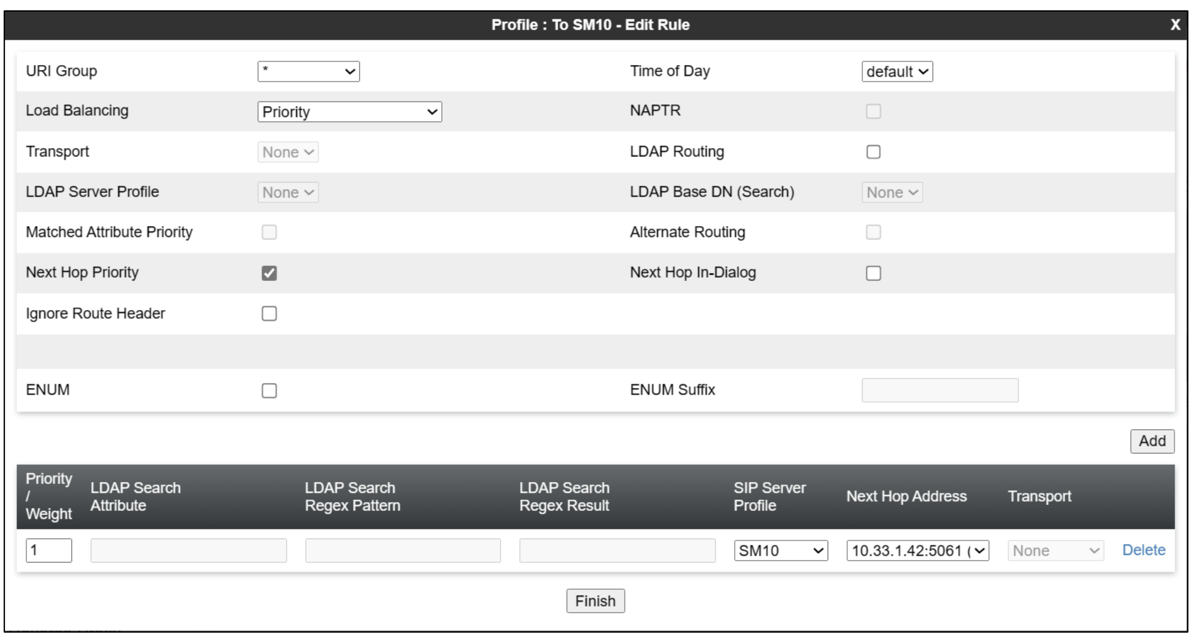
A routing profile for inbound calls to Session Manager was already in place, and it was reused in the configuration for Fonolo VCB. Follow the steps below to create a routing profile to the Session Manager if one doesn't already exist.

Navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** (e.g., **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:

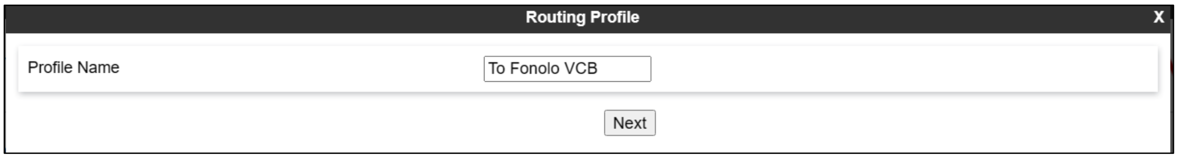
- **Priority/Weight**: **1**
- **SIP Server Profile**: **SM10** (from **Section 7.8.1**).
- **Next Hop Address:** Verify that the **10.33.1.42:5061 (TLS)** entry from the drop-down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out. Click **Finish**.



7.9.2. Routing Profile – Fonolo VCB

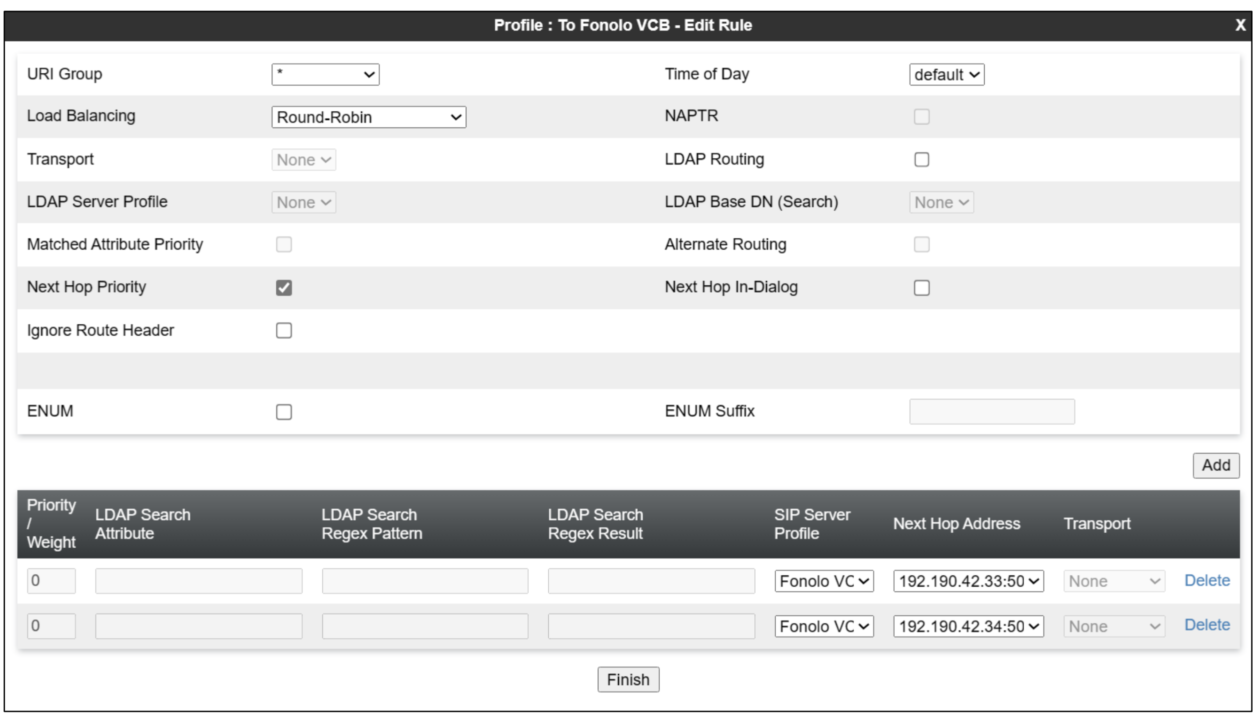
A routing profile for Fonolo VCB was already created during the testing, and it was shown in the configuration for reference purpose.

Navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** (e.g., **To Fonolo VCB**) 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, leave **URI Group** at default and select **Round-Robin** in the **Load Balancing** field. Click the **Add** button. The **Next-Hop Address** section will open at the bottom of the profile. Populate the following fields:

- **SIP Server Profile**: Select **Fonolo VCB** server profile (from **Section 7.8.2**).
- **Next Hop Address:** Select two IP addresses **192.190.42.33** and **192.190.42.34** (from **Section 7.8.2**). Note that Fonolo Cloud SIP Connect receives voice call-backs on these two dedicated IP addresses, other 4 IP addresses are used to place outbound calls. Click **Finish**.

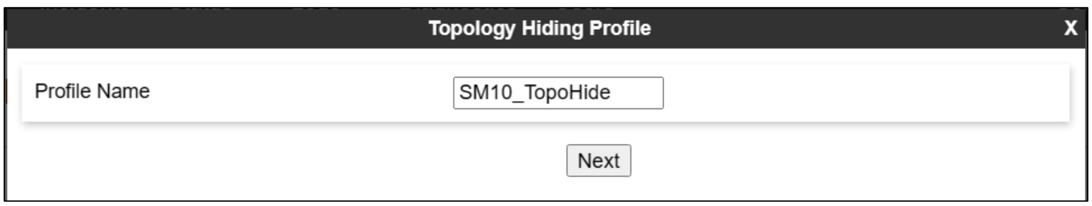


7.10. Topology Hiding Profile

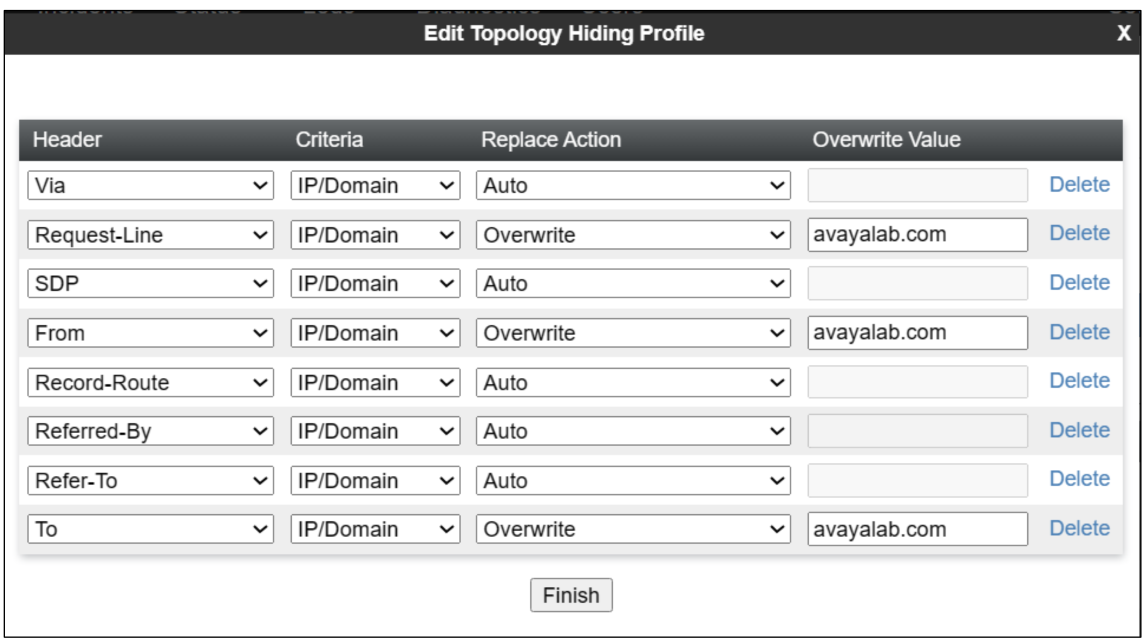
The **Topology Hiding** profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the security of the network. It hides the topology of the enterprise network from external networks.

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., **SM10_ToppHide**), and click **Finish** to continue.



- Edit the newly created **SM10_TopoHide** 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**.



Edit Topology Hiding Profile

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

Finish

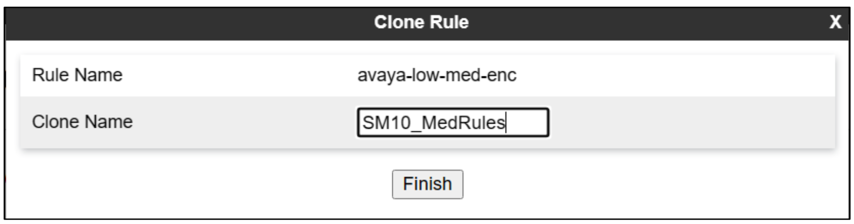
7.11. Media Rules

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 Fonolo VCB.

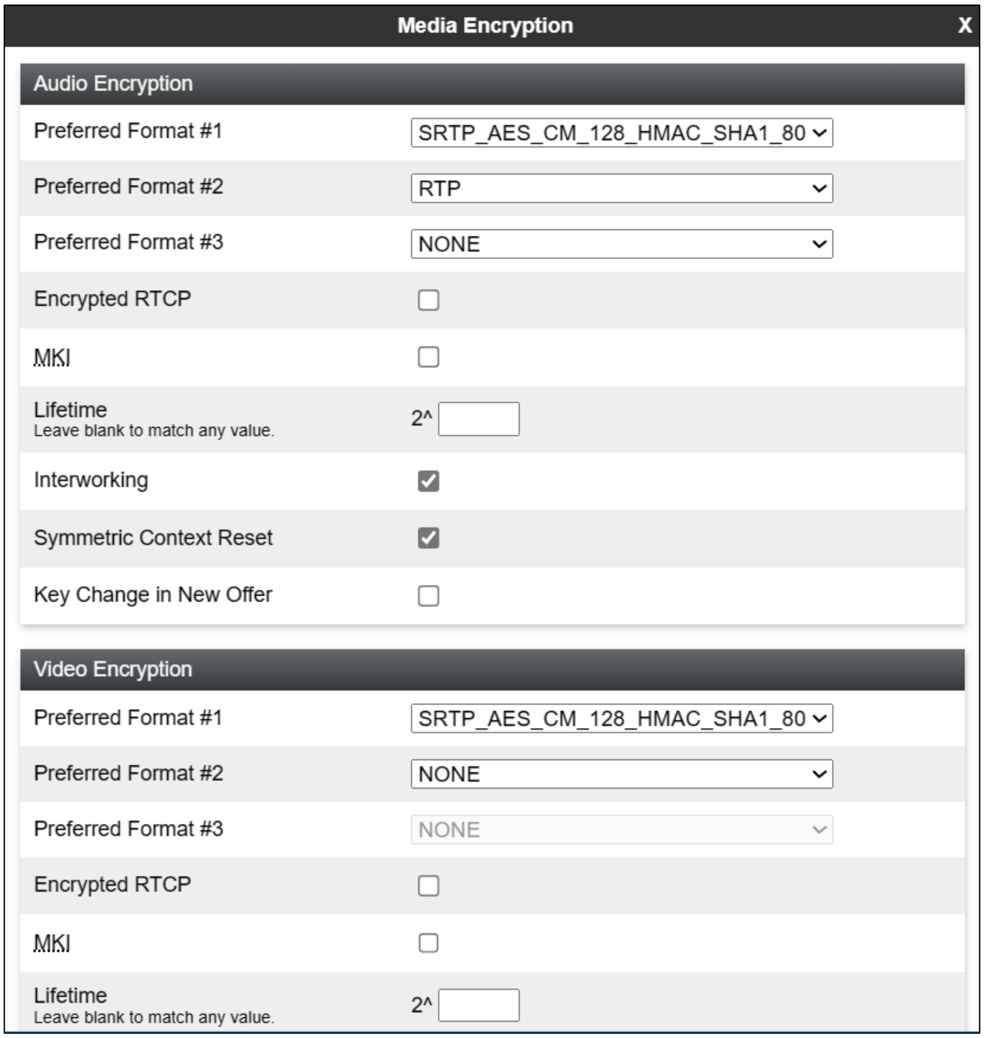
7.11.1. SM10– Media Rule

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., **SM10_MedRules**)
- Click **Finish.** The newly created rule will be displayed.



- On the **SM10_MedRules** 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 **NONE** for **Preferred Format #2**.
- In the **Miscellaneous** section, select **Capability Negotiation**.
- Click **Finish**.



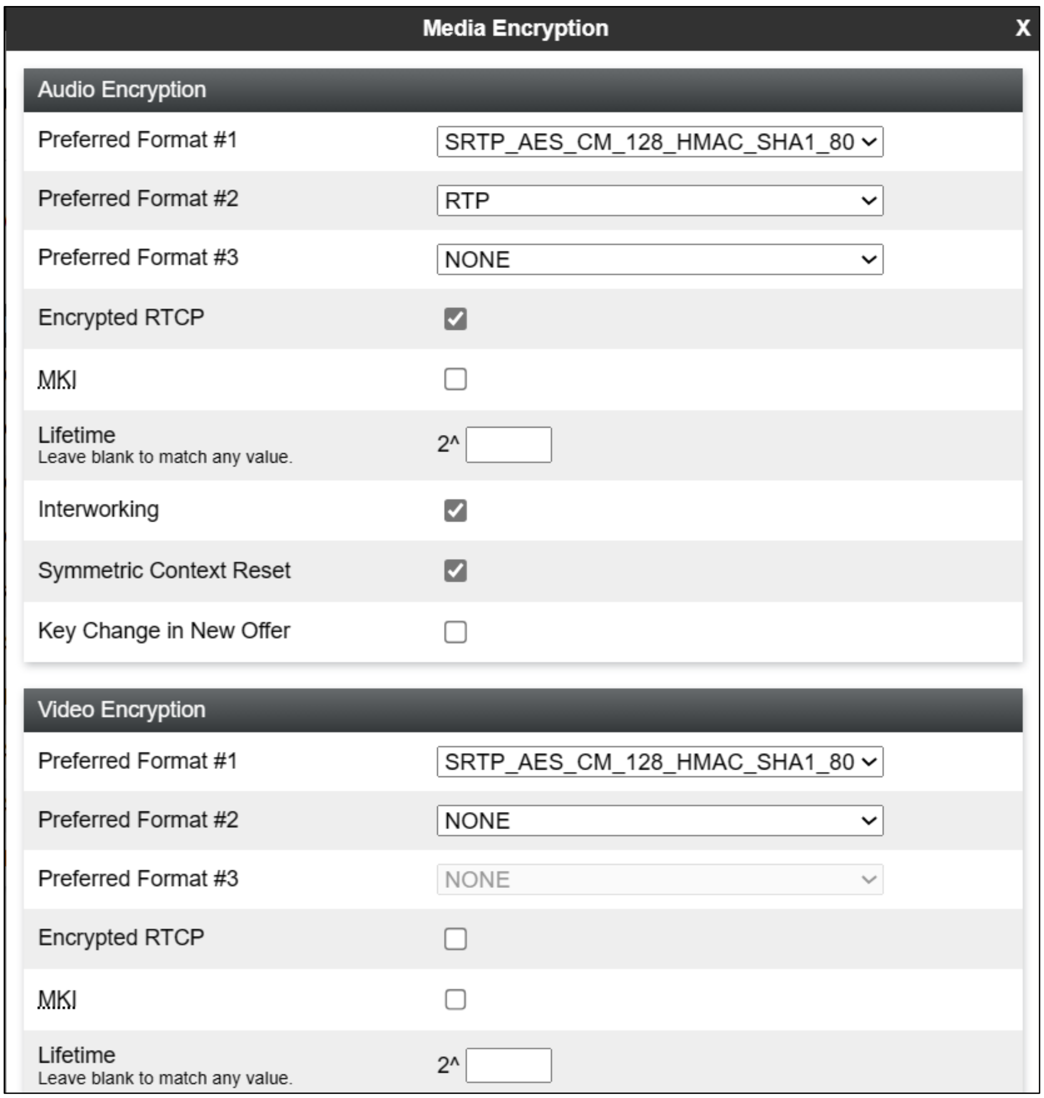
7.11.2. Fonolo VCB – Media Rule

Repeat the steps in **Section 7.11.1**, with the following changes, to create a Media Rule for Fonolo VCB

1. Clone the **avaya-low-med-enc** profile.
2. In the **Clone Name** field enter the new Media Rule name (e.g., **Fonolo_MedRules**).

The completed **Fonolo_MedRules** media rule is shown on the screen below.

Note: **Encrypted RTCP** for audio encryption must be selected otherwise the secure calls are rejected by Fonolo Cloud SIP servers.

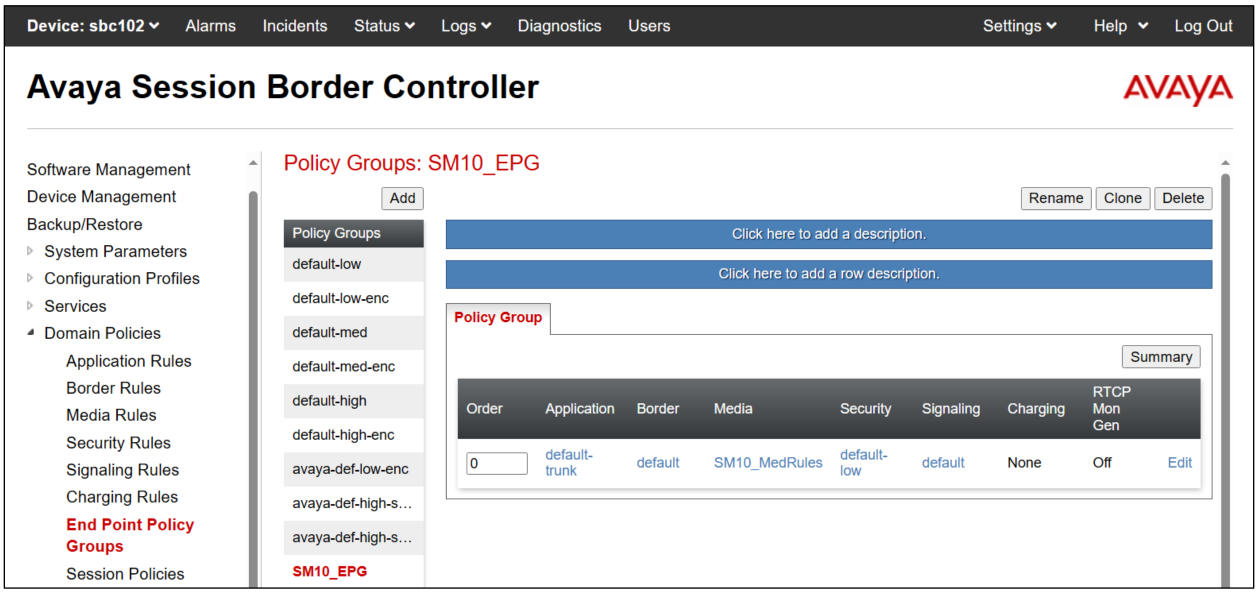


7.12. Endpoint Policy Groups

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 7.13**. A new Endpoint Policy Group was defined for Fonolo VCB, while a Policy Group for the enterprise (SM10) was already existing and re-used in this configuration.

7.12.1. Endpoint Policy Group – Session Manager

The following Policy Group named **SM10_EPG** was already defined in Avaya SBC for the enterprise, using the values shown on the screen below. The Media Rule is the **SM10_MedRules** shown on **Section 7.11.1**.

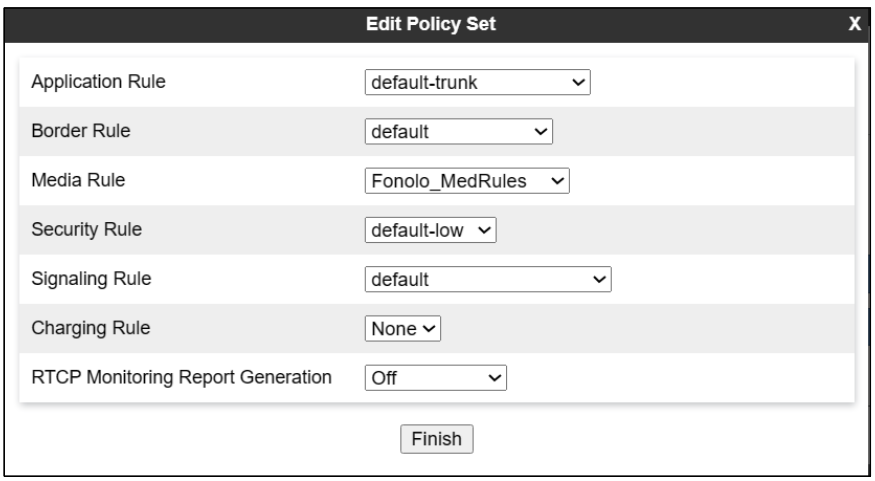


7.12.2. Endpoint Policy Group – Fonolo VCB

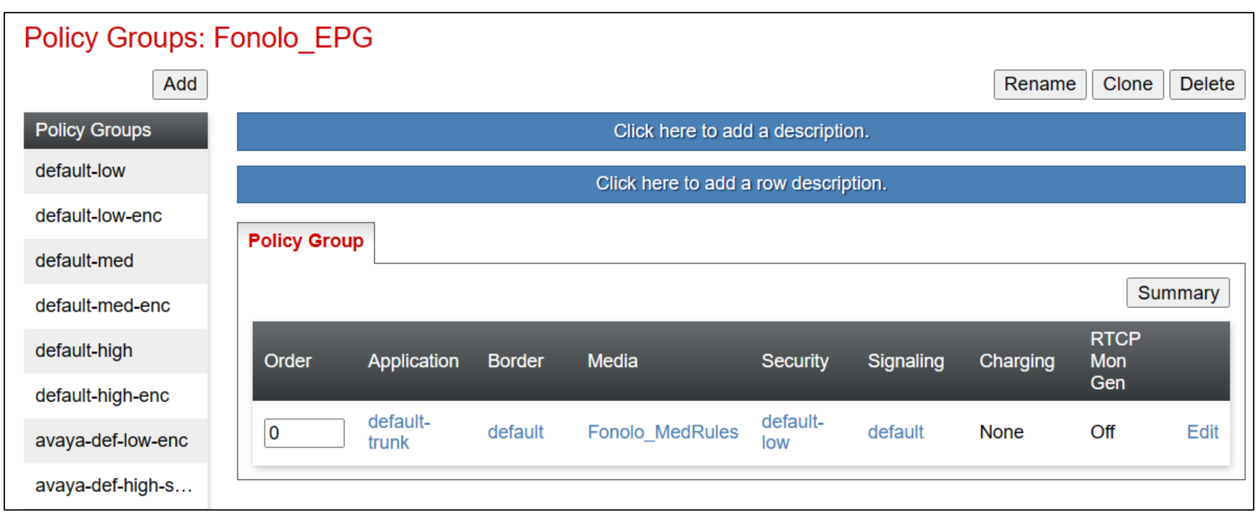
To create a new Endpoint Policy Group for Fonolo VCB, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the right pane, select **Add**. Enter a **Group Name** e.g., **Fonolo_EPG**, (not shown) and click **Next** to continue.

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**: **Fonolo_MedRules** as defined in **Section 7.11.2**.
- **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.



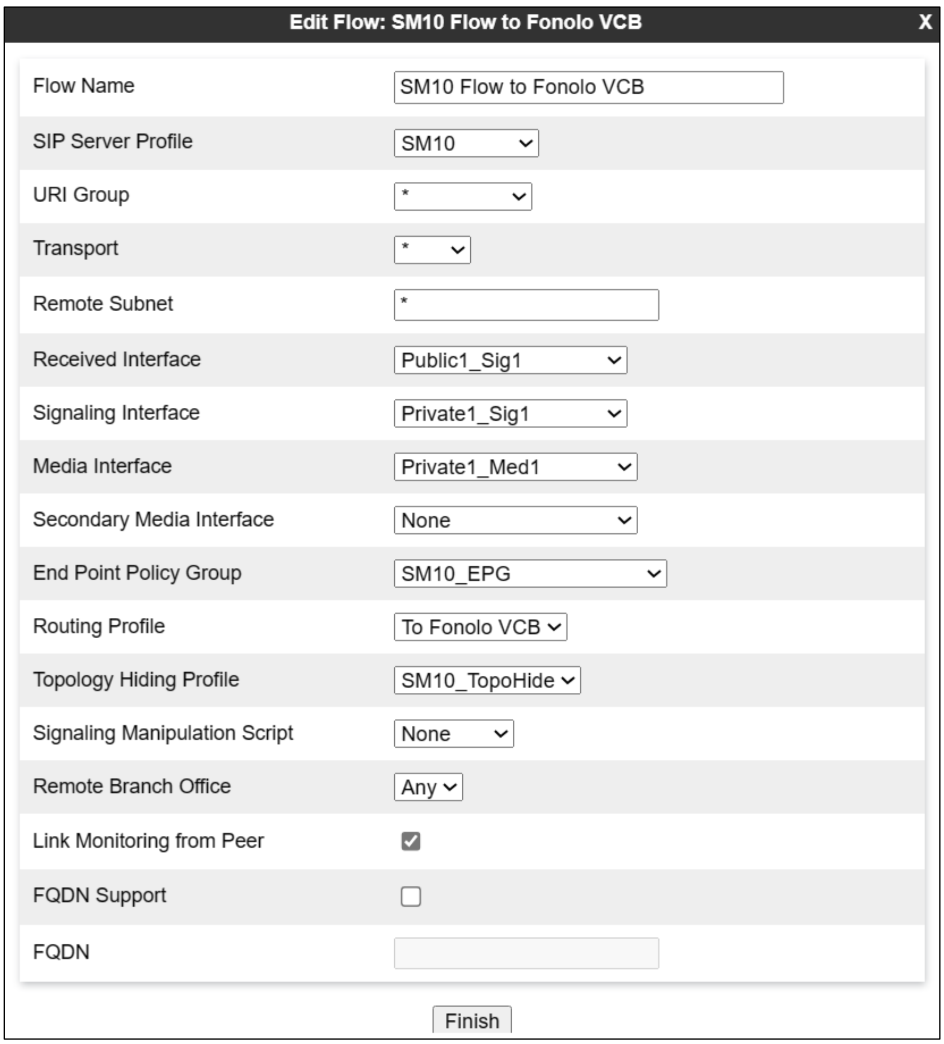
7.13. Endpoint Flows – Server Flows

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.

7.13.1. 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:

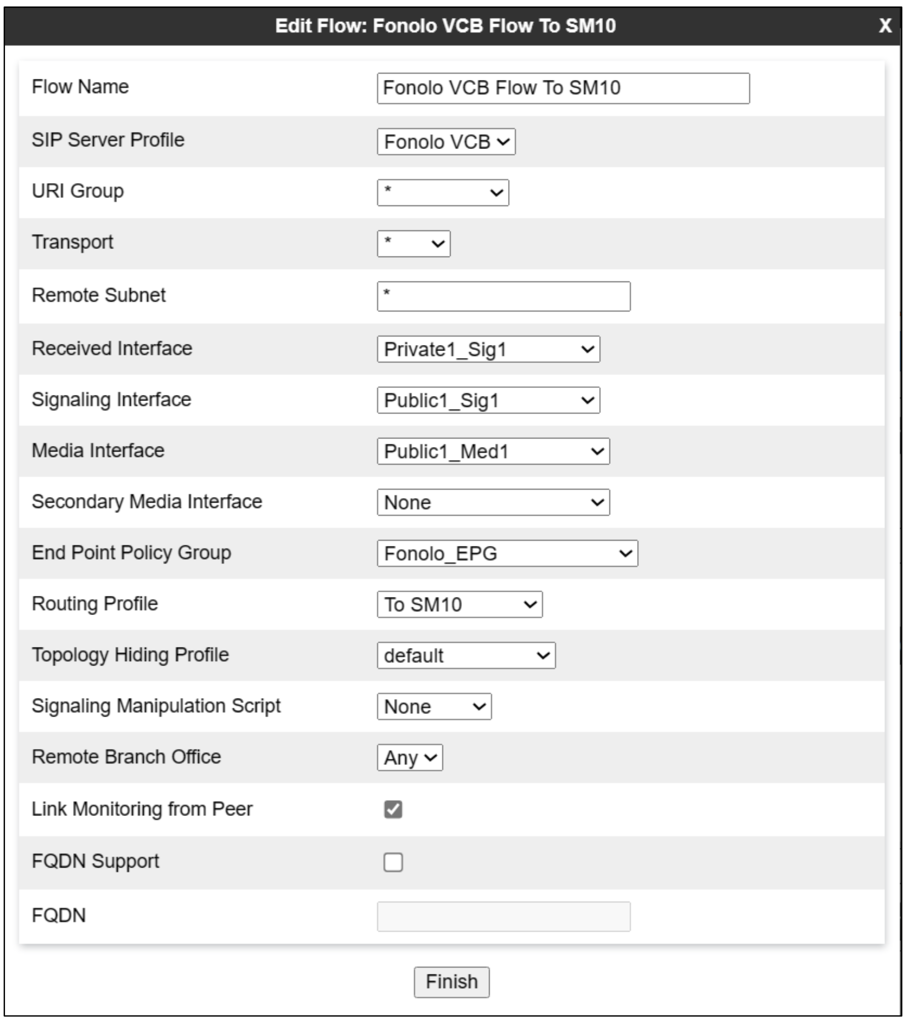
- **Flow Name**: Enter a descriptive name, e.g., **SM10 Flow to Fonolo VCB**.
- **SIP Server Profile**: Select **SM10** as defined in **Section 7.8.1**.
- **URI Group**, **Transport**, **Remote Subnet**: Leave it at default as *.
- **Received Interface**: Select **Public1_Sig1** as defined in **Section 7.6**.
- **Signaling Interface**: Select **Private1_Sig1** as defined in **Section 7.6**.
- **Media Interface**: Select **Private1_Med1** as defined in **Section 7.6.**
- **End Point Policy Group**: Select **SM10_EPG** as defined in **Section 7.12.1**.
- **Routing Profile**: Select **To Fonolo VCB** as defined in **Section 7.9.2**.
- **Topology Hiding Profile**: Select **SM10_TopoHide** as defined in **Section 7.10**.
- Check the **Link Monitoring from Peer** box.
- Let other fields at the default values. Click **Finish**.



7.13.2. Server Flow – Fonolo VCB

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

- **Flow Name**: Enter a descriptive name, e.g., **Fonolo VCB Flow To SM10**.
- **SIP Server Profile**: Select **Fonolo VCB** as defined in **Section 7.8.2**.
- **URI Group**, **Transport**, **Remote Subnet**: Leave it at default as *****.
- **Received Interface**: Select **Private1_Sig1** as defined in **Section 7.6**.
- **Signaling Interface**: Select **Public1_Sig1** as defined in **Section 7.6**.
- **Media Interface**: Select **Public1_Med1** as defined in **Section 7.6.**
- **End Point Policy Group**: Select **Fonolo_EPG** as defined in **Section 7.12.2**.
- **Routing Profile**: Select **To SM10** as defined in **Section 7.9.1**.
- **Topology Hiding Profile**: Select **default**.
- Check the **Link Monitoring from Peer** box.
- Let other fields at the default values. Click **Finish**.



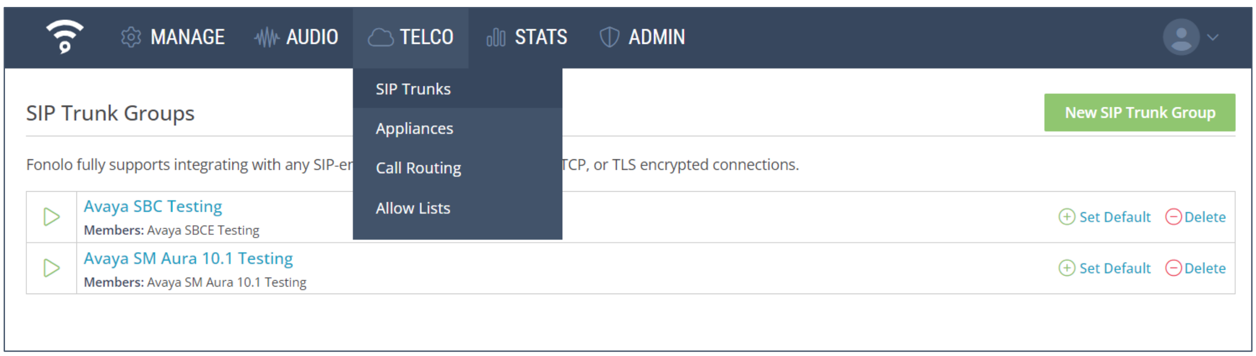
8. Configure Fonolo Voice Call-Backs

This section provides a "snapshot" of Fonolo VCB configuration used during compliance testing. Fonolo VCB is typically configured for customers by Fonolo. The screen shots and partial configuration shown below, supplied by Fonolo, are provided only for reference. These represent only an example of the configuration GUI of VCB, available through the Fonolo Customer Portal at https://portal.fonolo.com/. Other configurations are possible. Contact Fonolo for details on how to configure VCB. The configuration operations described in this section can be summarized as follows:

- Add a New SIP Trunk Group,
- Adding the Agent Call-Back Endpoint,
- Adding a New Call-Back Profile,

8.1. Add a New SIP Trunk Group

Navigate to **Telco → SIP Trunks** and click the **New SIP Trunk Group** at the top of the page. Define a new label to identify this SIP trunk group. During compliance testing a name **Avaya SBC** was used as the label. Then select **Add New SIP Trunk** (not shown).



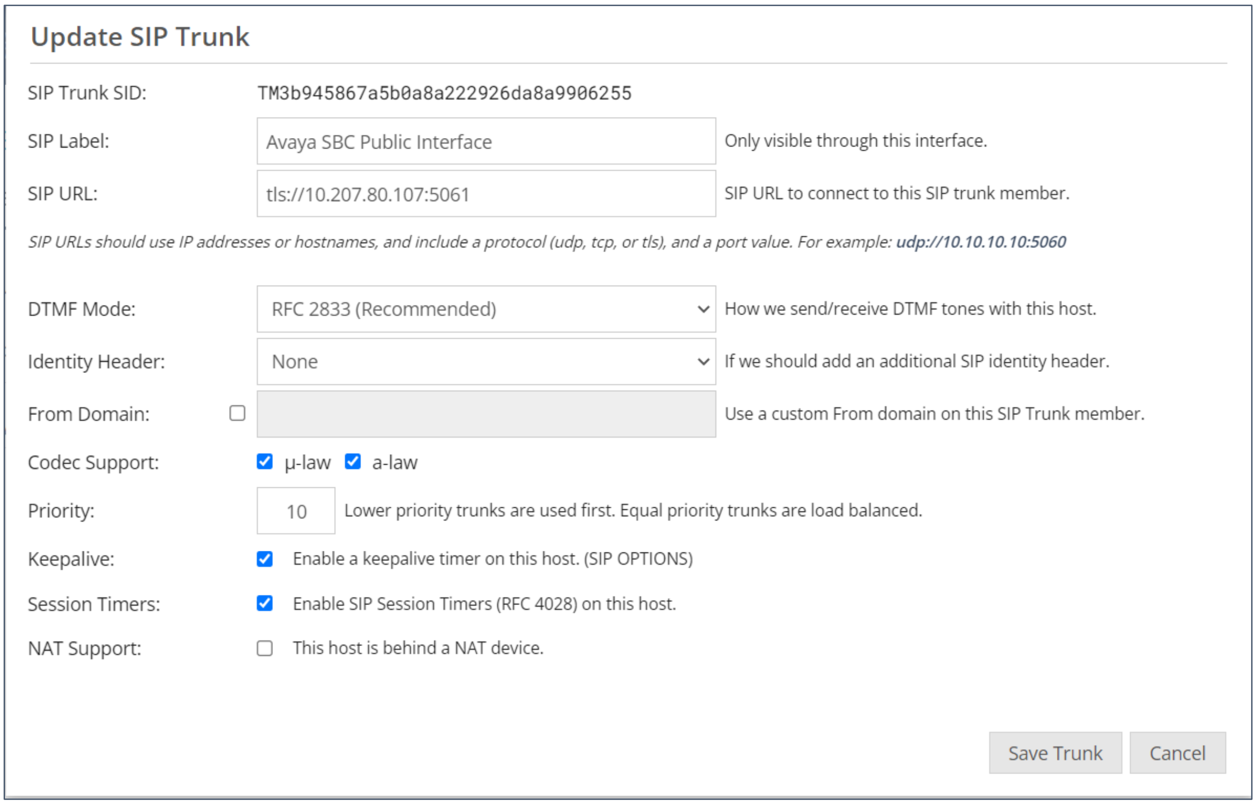
Under the **Members** tab in this new SIP trunk group, click the **Add New Member** button (not shown), and the **Add New SIP Trunk** dialog will appear as shown below.

Under **Add New SIP Trunk**:

- **SIP URL**: Ener the public IP address of Avaya SBC formatted as a fully qualified URL, defining the protocol and SIP port. During compliance testing, the protocol **TLS** and port **5061** was used for the SIP service with Avaya SBC.
- **DTMF Mode**: The mode to use for sending DTMF tones. Default is RFC 2833.
- **Identity Header**: Whether to include an identity header (either Remote-Party-ID or P-Asserted-Identity). Default is none.
- **Codec Support**: The list of audio codecs to use. Defaults are µ-law and a-law.
- **Priority**: A numeric value that can be used to determine failover or load balance groups when more than one SIP trunk group member is defined. Members with lower priority values are used first; members with equal priority values are load balanced.

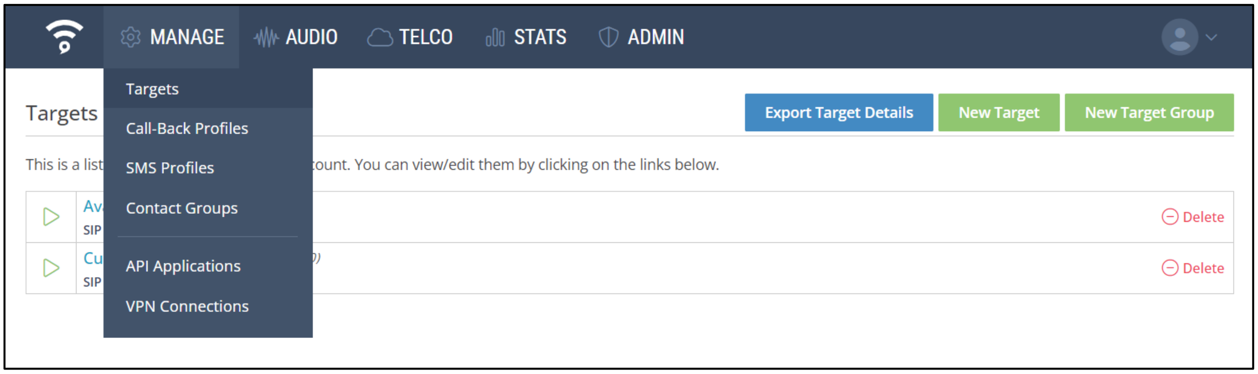
- **Keepalive**: This instructs the Fonolo VCB to perform regular keep-alive using SIP OPTIONS requests, based on the number of seconds defined.
- **Session Timers**: If Fonolo VCB should enable SIP Session Timers (RFC 4028).
- **NAT Support**: If the SIP trunk group member specified is located behind a NAT (Network Address Translation) device. Fonolo can compensate for the un-reachable RTP data specified in the SDP body of the INVITE request, using symmetric RTP.

Click **Save Trunk** button to save the changes.

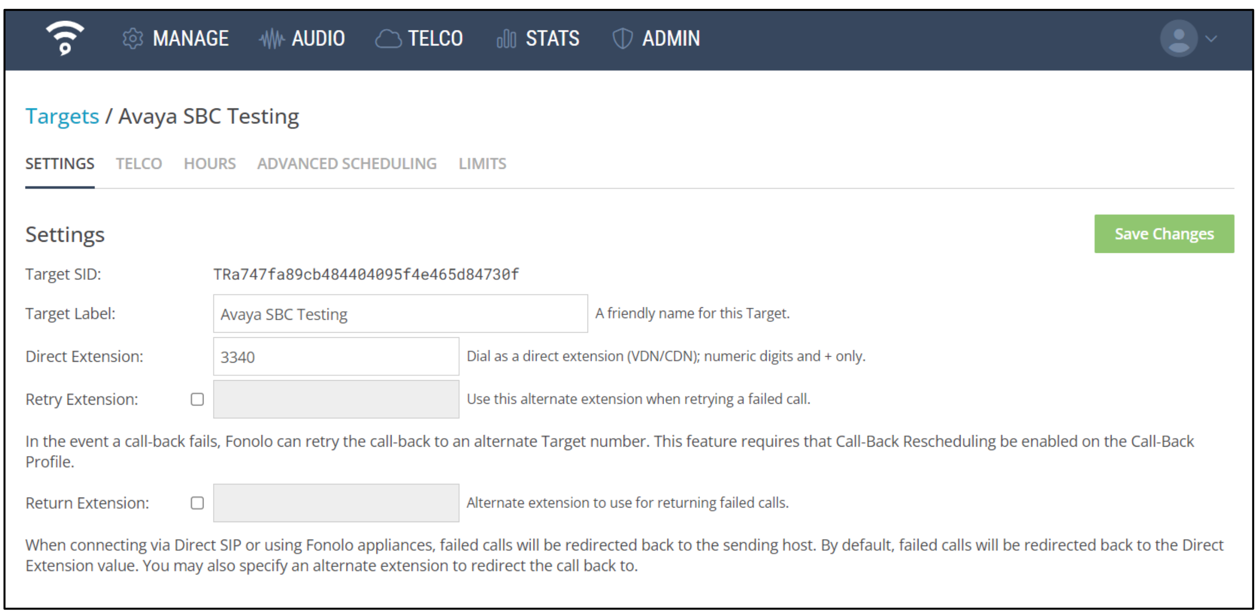


8.2. Adding the Voice Call-Back Endpoint

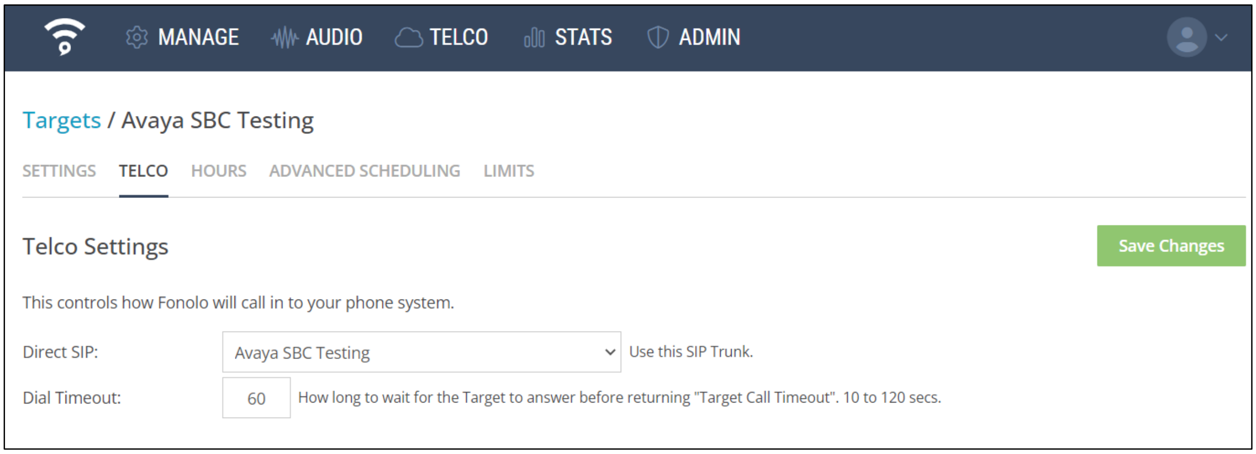
Navigate to **Manage → Targets** and click the **New Target** button. Define a new label to identify this new Target. During compliance testing **Avaya SBC Testing** was used as the **Target Label**. Select the **Dial as SIP Extension** option (shown below) for **Dial Method** and enter a call center VDN number to reach the pertinent skillset via Session Manager in the **Extension** field.



During compliance testing, VDN **3340** was pre-configured on Communication Manager which was accessible via Session Manager. Then click on the **Save Changes** button to save the changes.

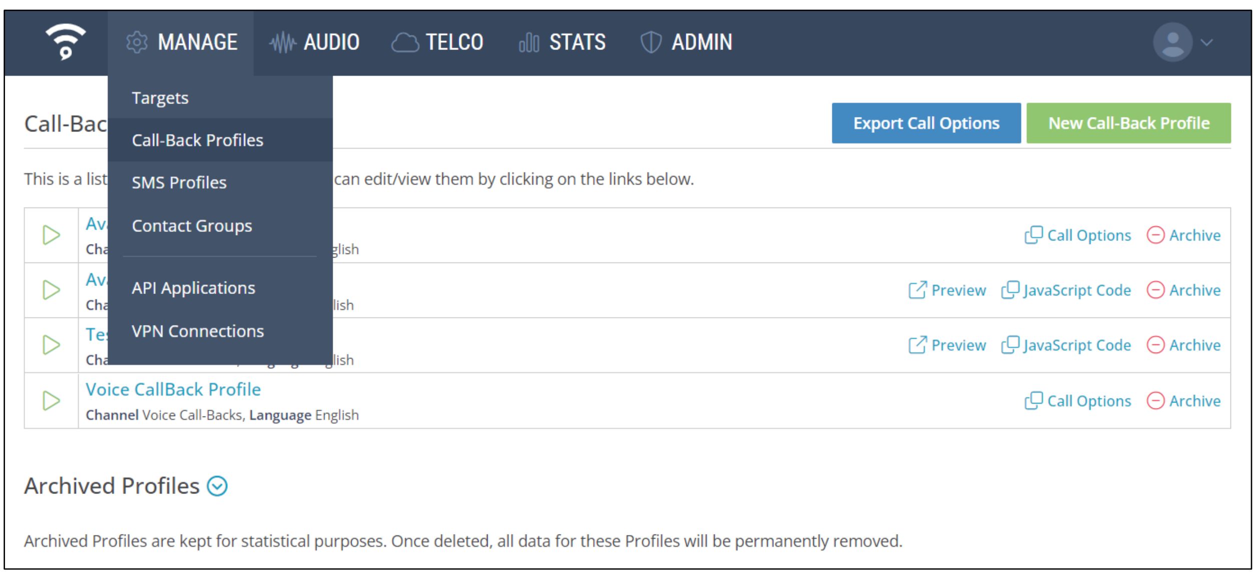


From the **Telco Settings** section of the newly added Target, select the SIP trunk to use for this Target, from the **Direct SIP** drop down menu shown below. Select the **Avaya SBC Testing** SIP trunk, added in **Section 8.1**, and then click the **Save Changes** button.



8.3. Adding a New Call-Back Profile

Navigate to **Manage → Call-Back Profiles** and click on the **New Call-Backs Profile** button as shown below.

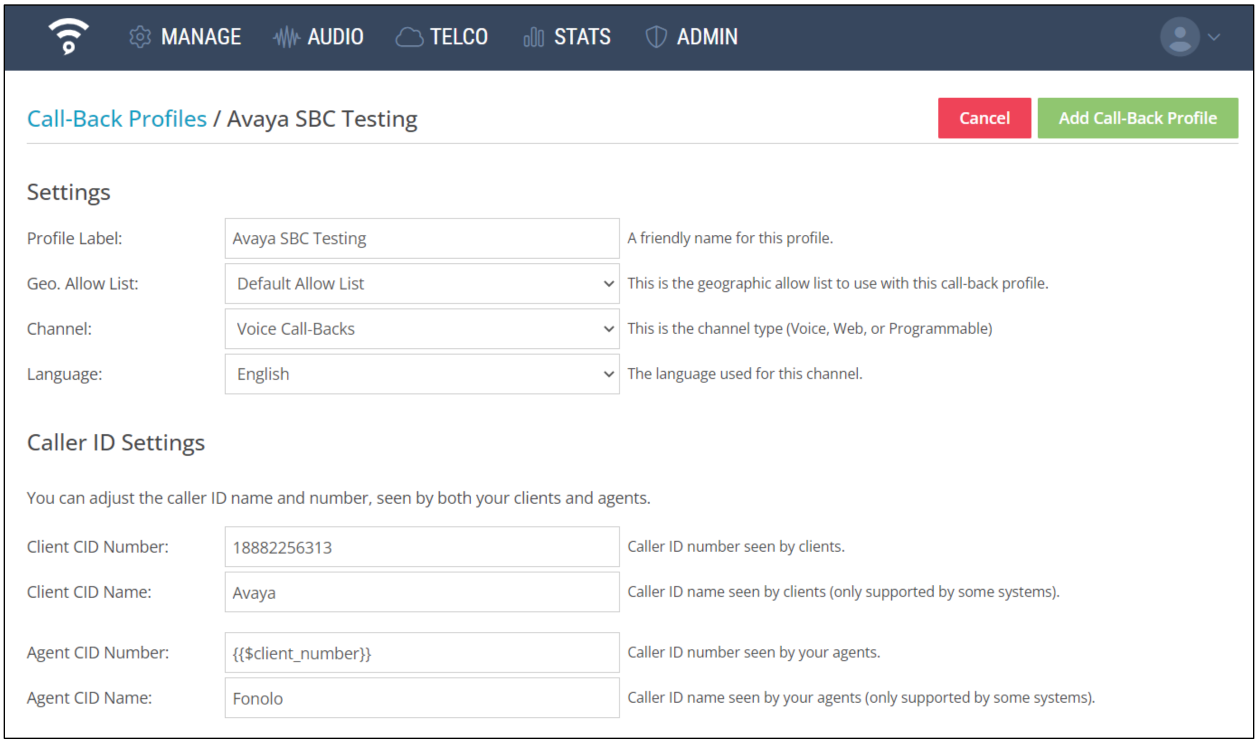


Enter values for the new profile:

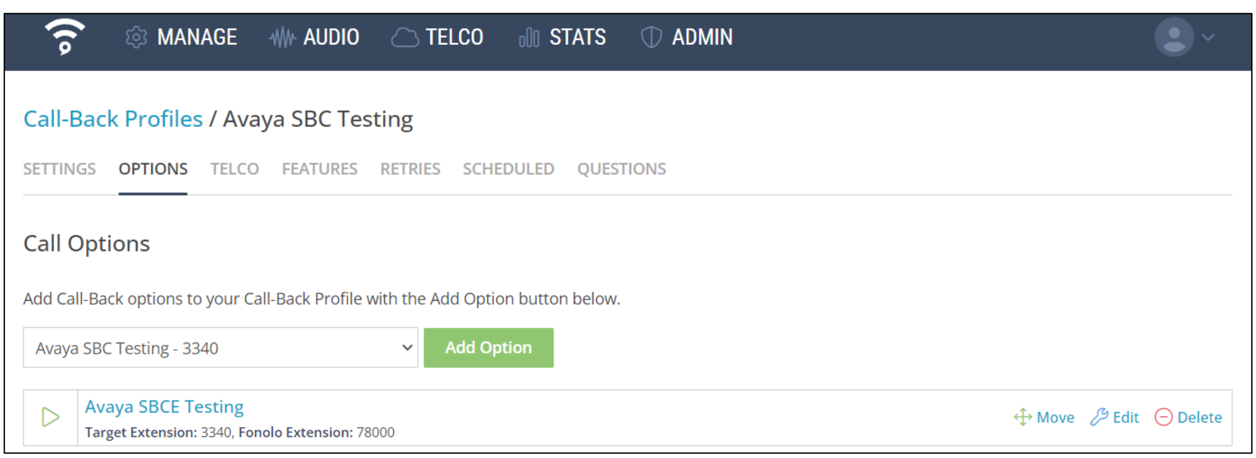
- **Profile Label:** Enter a profile name, e.g., Avaya SBC Testing.
- **Geo Allow List:** The Default Allow List is selected.
- **Channel:** Select Voice Call-Backs.
- **Language:** Select the appropriate language for this profile.
- **Client CID Number:** The Caller-ID number the customer will see.

- **Client CID Name:** The Caller-ID name the customer will see.
- **Agent CID Number:** The Caller-ID number the agent will see.
- **Agent CID Name:** The Caller-ID name the agent will see.

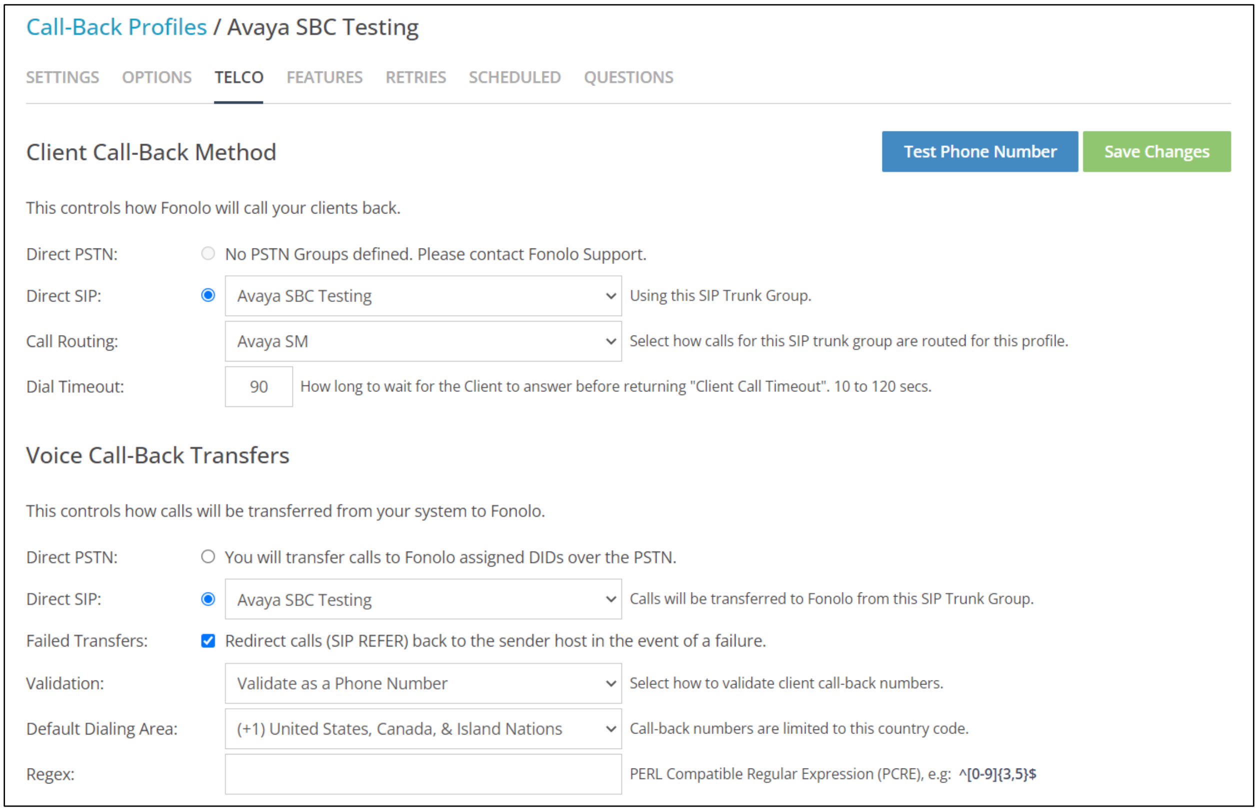
Click the **Add Call-Back Profile** button to save this new profile.



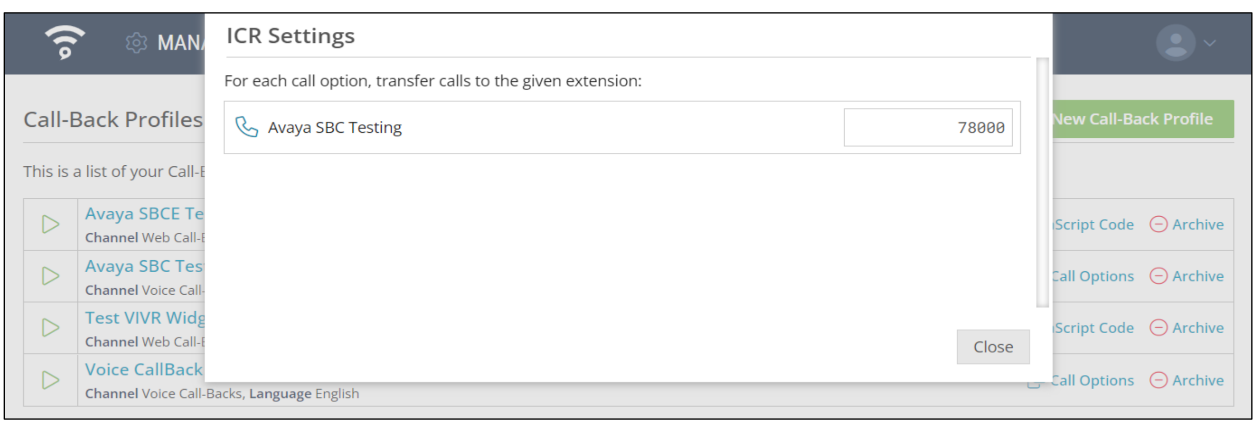
From the **Options** section of the new **Call-Back Profile**, select the Target added in **Section** Error! Reference source not found., and click the **Add Option** button to add the call options to this profile, as shown below, then click the **Save Changes** (not shown). This associates the Target VDN with this new **Call-Back Profile**. Multiple call options can be associated with a single **Call-Back Profile**, one for each skill call-backs are being offered on.



From the **Telco Settings** section of the new **Call-Back Profile**, select the **Avaya SBC** SIP trunk group created in **Section 8.1** as the **Direct SIP** value under both the **Client Call-Back Method** and the **Voice Call-Backs Transfers** section, as shown below, then click the **Save Changes** button.



Navigate to **Manage → Call-Back Profiles** and click on the **Call Options** link on the newly created **Call-Back Profile** (not shown). The **ICR Settings** dialog will appear (shown below) and include the inbound extensions to use for VDN. These are the extensions to transfer calls to, on the Fonolo VCB, when a call opts-in for a call-back. During compliance testing, the extension **78000** is configured for the Fonolo VCB.



9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, Avaya SBC and Fonolo VCB.

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the SIP signaling group by using the "status signaling-group n" command, where "n" is the signaling group number administered in **Section** Error! Reference source not found.**5**. Verify that the signaling group is **in-service** as indicated in the **Group State** field shown below.

```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

Verify the status of the local SIP trunk group by using the "status trunk n" command, where "n" is the trunk group number administered in **Section 5.6**. Verify that all trunks are in the **in-service/idle** state as shown below.

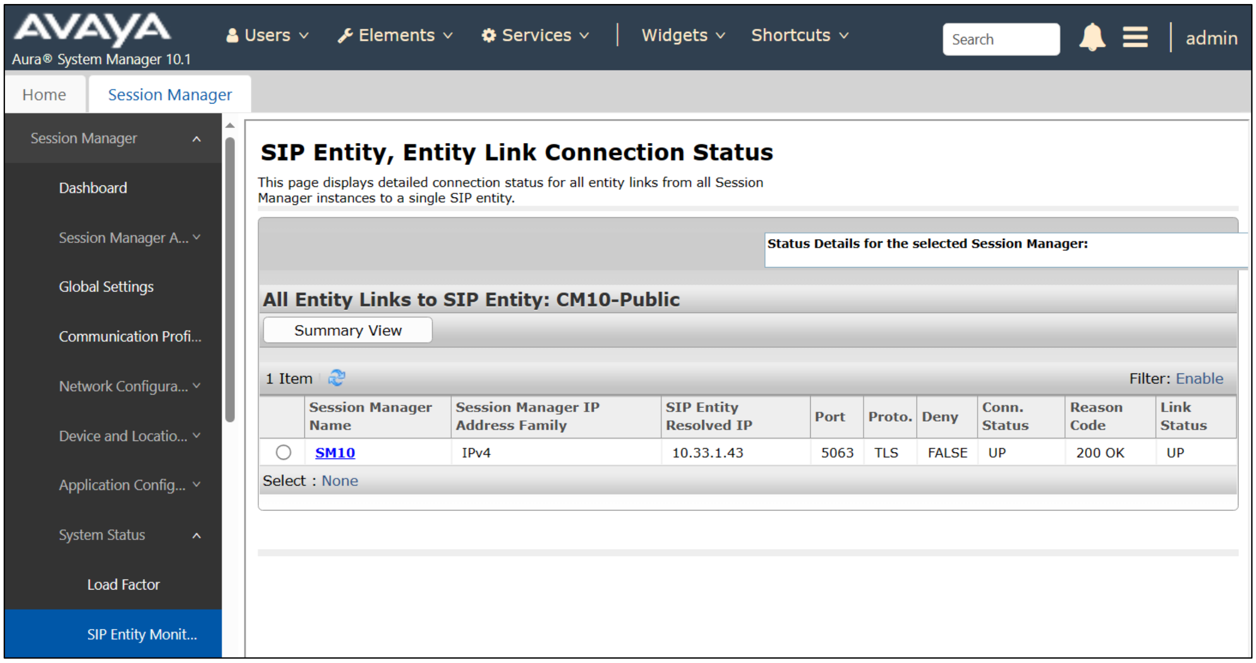
```
status trunk 1

                             TRUNK GROUP STATUS

Member    Port    Service State      Mtce Connected Ports
                                     Busy
0001/0001 T000001 in-service/idle    no
0001/0002 T000002 in-service/idle    no
0001/0003 T000003 in-service/idle    no
0001/0004 T000004 in-service/idle    no
0001/0005 T000005 in-service/idle    no
0001/0006 T000006 in-service/idle    no
```

The following tests were also performed to verify proper configuration of Fonolo VCB:

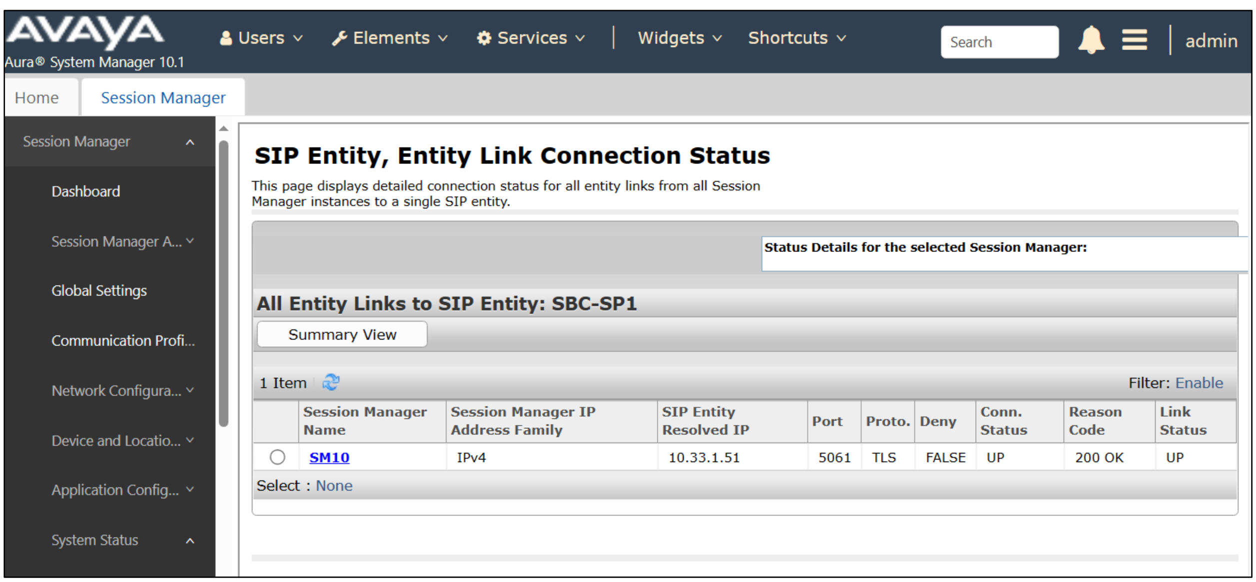
1. PSTN user places a call to ACD queue of call center in Communication Manager.
2. If there is no available agent, PSTN caller is given options whether continue staying in the queue or pressing number #1 to have a call-back.
3. PSTN user decides to have a call-back and press #1. The call is now routed to Fonolo VCB through Avaya SBC. The Fonolo VCB confirms a call-back number with PSTN user and schedule a voice call-back for PSTN user.
4. Fonolo VCB calls the ACD queue to connect to an available agent, as soon as the agent answers the ACD call, it asks the agent to press #1 to connect to the PSTN user.
5. If the agent is ready to connect to PSTN user, they press #1. Fonolo VCB is calling to PSTN user and connect the agent to PSTN user.

9.2. Verify Avaya Aura® Session Manager

Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** and select the Communication Manager SIP Entity. Verify the **Link Status** is **Up**.

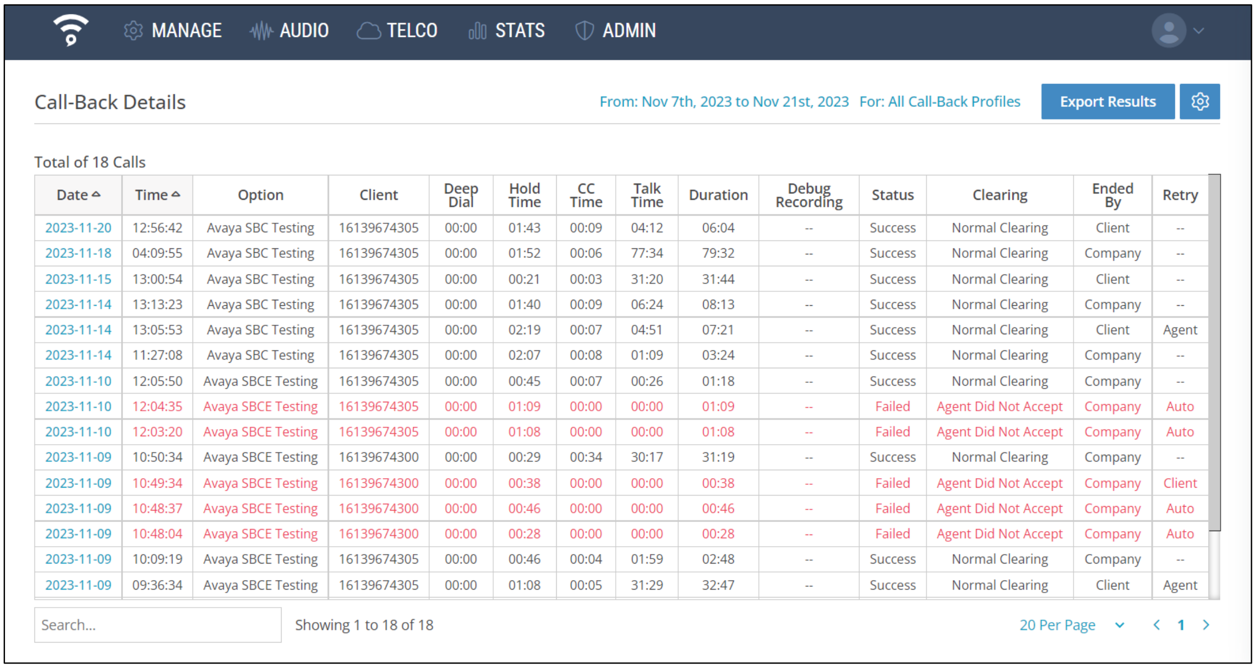


Repeat the same procedure selecting Avaya SBC SIP Entity and verify the **Link Status** is **Up**.



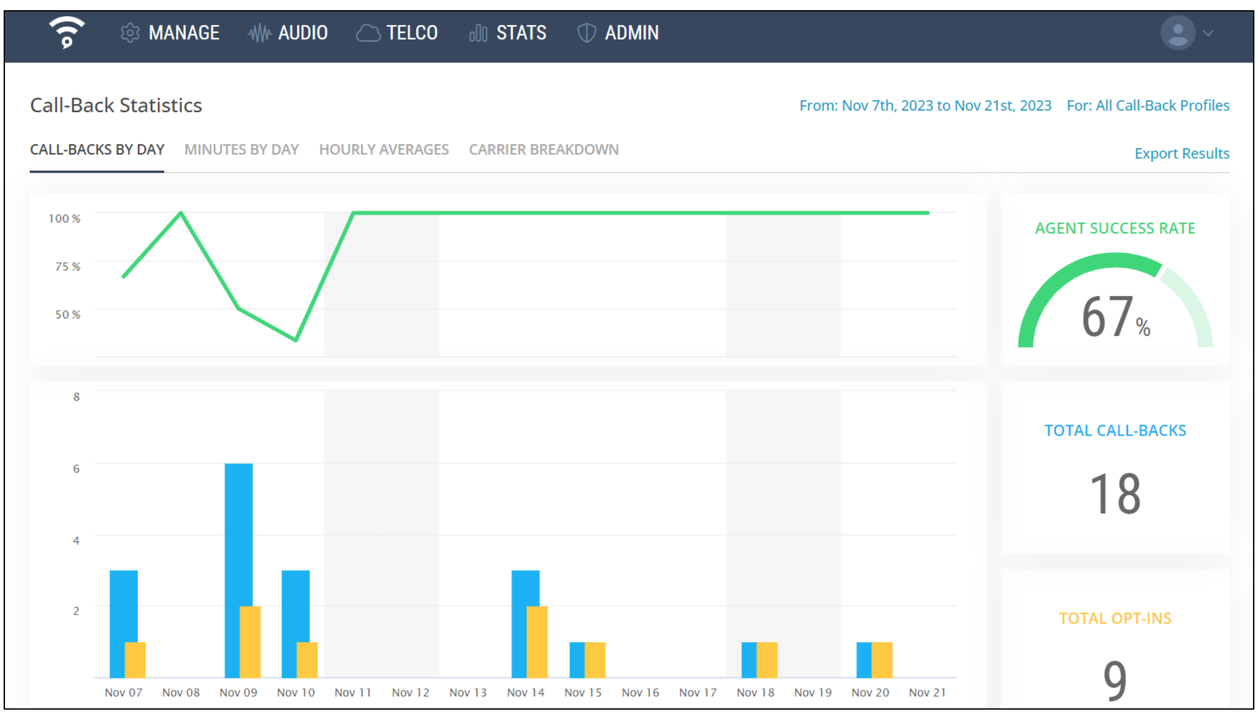
9.3. Verify Fonolo Voice Call Back

To verify the voice call-backs, log in to the Fonolo portal with appropriate credential and navigate to **STATS → Call Details**. The **Call-Back Details** window displays list of the call-back with detail information as shown below.



Date	Time	Option	Client	Deep Dial	Hold Time	CC Time	Talk Time	Duration	Debug Recording	Status	Clearing	Ended By	Retry
2023-11-20	12:56:42	Avaya SBC Testing	16139674305	00:00	01:43	00:09	04:12	06:04	--	Success	Normal Clearing	Client	--
2023-11-18	04:09:55	Avaya SBC Testing	16139674305	00:00	01:52	00:06	77:34	79:32	--	Success	Normal Clearing	Company	--
2023-11-15	13:00:54	Avaya SBC Testing	16139674305	00:00	00:21	00:03	31:20	31:44	--	Success	Normal Clearing	Client	--
2023-11-14	13:13:23	Avaya SBC Testing	16139674305	00:00	01:40	00:09	06:24	08:13	--	Success	Normal Clearing	Company	--
2023-11-14	13:05:53	Avaya SBC Testing	16139674305	00:00	02:19	00:07	04:51	07:21	--	Success	Normal Clearing	Client	Agent
2023-11-14	11:27:08	Avaya SBC Testing	16139674305	00:00	02:07	00:08	01:09	03:24	--	Success	Normal Clearing	Company	--
2023-11-10	12:05:50	Avaya SBCE Testing	16139674305	00:00	00:45	00:07	00:26	01:18	--	Success	Normal Clearing	Company	--
2023-11-10	12:04:35	Avaya SBCE Testing	16139674305	00:00	01:09	00:00	00:00	01:09	--	Failed	Agent Did Not Accept	Company	Auto
2023-11-10	12:03:20	Avaya SBCE Testing	16139674305	00:00	01:08	00:00	00:00	01:08	--	Failed	Agent Did Not Accept	Company	Auto
2023-11-09	10:50:34	Avaya SBCE Testing	16139674300	00:00	00:29	00:34	30:17	31:19	--	Success	Normal Clearing	Company	--
2023-11-09	10:49:34	Avaya SBCE Testing	16139674300	00:00	00:38	00:00	00:00	00:38	--	Failed	Agent Did Not Accept	Company	Client
2023-11-09	10:48:37	Avaya SBCE Testing	16139674300	00:00	00:46	00:00	00:00	00:46	--	Failed	Agent Did Not Accept	Company	Auto
2023-11-09	10:48:04	Avaya SBCE Testing	16139674300	00:00	00:28	00:00	00:00	00:28	--	Failed	Agent Did Not Accept	Company	Auto
2023-11-09	10:09:19	Avaya SBCE Testing	16139674305	00:00	00:46	00:04	01:59	02:48	--	Success	Normal Clearing	Company	--
2023-11-09	09:36:34	Avaya SBCE Testing	16139674305	00:00	01:08	00:05	31:29	32:47	--	Success	Normal Clearing	Client	Agent

The **Call-Back Statistics** is also provided in the **Graph** section of the **STATS** menu.



10. Conclusion

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs Version 3.9 using Fonolo Cloud SIP Connect to successfully interoperate with Avaya Session Border Controller Release 10.1 and Avaya Aura® Release 10.1. All feature and serviceability test cases were completed and passed.

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.

Fonolo provides their documentation upon delivery of their products/services.

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.