Avaya Solution & Interoperability Test Lab

Application Notes for Fonolo Voice Call-Backs Version 3.3 with Avaya Session Border Controller for Enterprise 8.1 using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs application to interoperate with Avaya Session Border Controller for Enterprise using SIP trunks.

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

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

1. Introduction

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs (Fonolo VCB) to interoperate with Avaya Session Border Controller for Enterprise (Avaya SBCE) using SIP trunks. Fonolo VCB provides functionality to replace hold-time with a call-back and during this compliance testing Fonolo servers/appliances was deployed in the DevConnect lab and its configuration and information was synchronized with Fonolo cloud over Internet. The solution communicates via SIP/RTP. Fonolo VCB functionality was compliance tested utilizing SIP trunks to Avaya SBCE. The configuration allowed Communication Manager to use SIP trunking for calls to and from the VCB application. Fonolo VCB integrates with call center to provide call-back solution where instead of a caller staying in the queue when agents are all busy, can request to get a call back when an agent becomes available.

When a caller encounters a scenario where no agents are available in a call center environment and Communication Manager is part of that environment, the caller is presented with options to either continue waiting in the queue or receive a call back. If the caller chose the latter, then Communication Manager directs the caller to the Fonolo VCB via Avaya SBCE 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 with Session Manager to call back into Communication Manager and wait in the queue until an agent becomes available. When an agent becomes available and connects with Fonolo VCB, 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 then calls the caller via SIP trunks to Communication Manager and connects the caller with the agent. When Fonolo VCB makes an outbound call to the caller and agent via Session Manager, it makes two SIP INVITE requests, one to the available agent and one to the caller, and then mixes the audio within the Fonolo VCB server.

For security purposes public and lab IP addresses have been altered in this document.

2. General Test Approach and Test Results

The interoperability compliance testing focused on verifying inbound and outbound calls flows between Communication Manager, Session Manager, Avaya SBCE and Fonolo VCB. The feature test cases were performed manually. Calls were placed manually from users on the PSTN to a call center Vector Directory Number (VDN). During compliance testing Call Center Elite within Communication Manager was used. An assumption was made during compliance testing in the vector script to direct callers to Fonolo VCB when no agents are available. When a caller is connected with Fonolo VCB, Fonolo VCB reads the call back number of the caller or asked the caller to input a new call back number. Fonolo VCB recognized the Dual Tone Multi Frequency (DTMF) input provided by the caller confirming the call back number. For compliance testing purposes, agents were made available after the above call between the caller and Fonolo VCB is completed. Fonolo VCB then called into the call center VDN and connected with an available agent. Fonolo VCB provided a recording, informing the agent of a call in waiting, and checked if the agent wanted to get connected to the PSTN caller. The agent can accept the call by using DTMF input. Fonolo VCB then made the second outbound call to the PSTN caller via Communication Manager and if the PSTN caller answered the call they then get connected with the agent.

The serviceability test cases were performed manually by disconnecting and reconnecting the SIP trunk connection to Fonolo VCB.

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 these Application Notes, the interface between Avaya systems and Fonolo did not include use of any specific encryption features as requested by Fonolo.

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 following features and functionality were covered during compliance testing:

- Establishment of SIP trunks connectivity between Fonolo VCB and Avaya SBCE including session refresh.
- Testing of G.711MU codec.
- Incoming calls to a VDN of Communication Manager can be redirected to the VCB appliance via the SIP trunks based on vector scripting. Outgoing calls from the VCB appliance to the VDN via Session Manager and Avaya SBCE when callers decide on Call back. During this compliance testing Call Center of Communication Manager was used and is not the scope of these Application Notes.
- The VCB application can make an outbound call to the PSTN caller via Communication Manager and Session Manager who had selected the call back option and merge the call between the caller and available agents. The outbound call is made from Communication Manager via Session Manager and using SIP INVITE.
- DTMF transmission to ensure that options selected by the caller and agent is accepted correctly by Fonolo VCB.
- User-to-User Information (UUI) is sent from Communication Manager to the VCB application and that the same information is sent back to the agent from the VCB application.

Serviceability testing focused on verifying the ability of Fonolo VCB to recover from adverse conditions, such as the SIP trunks going down (using 'busyout' command) and reboot of restarting Avaya SBCE.

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 on-premise appliance with Avaya Session Border Controller for Enterprise. Avaya Session Border Controller for Enterprise also had another 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. The configuration allowed the enterprise site to use SIP trunking for calls to and from Fonolo VCB via Avaya SBCE.

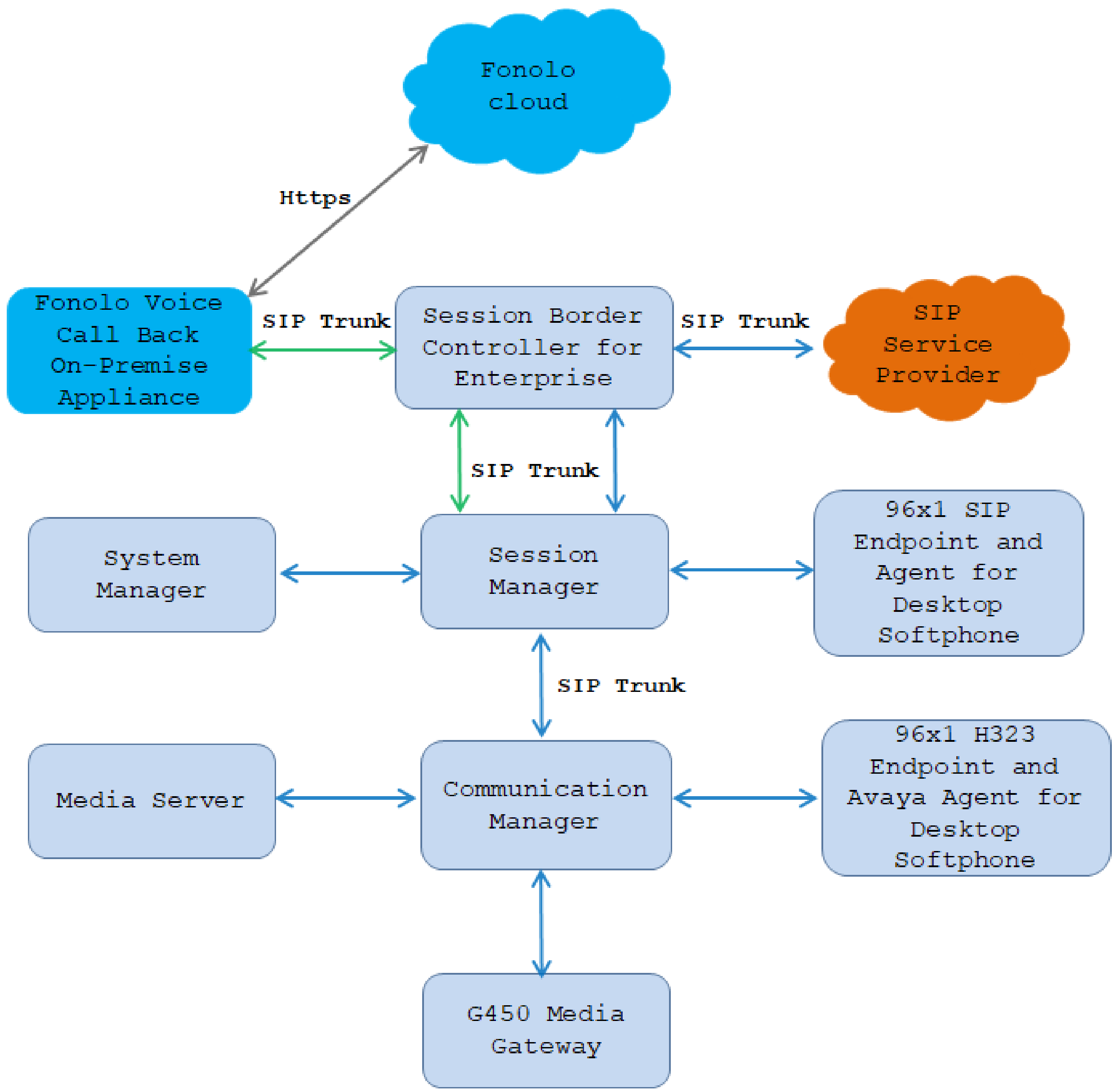


Figure 1: Reference Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtual Environment	8.1.3 8.1.3.2.0.890.26989
Avaya Aura® Media Server running on Virtual Environment	8.0.2
Avaya G450 Media Gateway	41.34.0
Avaya Aura® System Manager running on Virtual Environment	8.1.3 8.1.3.0.1011784
Avaya Aura® Session Manager running on Virtual Environment	8.1.3 8.1.3.0.813014
Avaya Session Border Controller for Enterprise running on Virtual Environment	8.1.3 8.1.3.0-31-21052
Avaya 9641GS IP Deskphone	7.1.9.0.8 6.8511 (H.323)
Avaya J179 SIP Deskphone	4.0.10.3.2
Avaya Agent for Desktop (AAfD) Softphone	2.0.6.18 (SIP and H.323)
Fonolo Voice Call-Backs On-premise Appliance	Version 3.3

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.

The administration of the routing and basic connectivity between Communication Manager and Session Manager or the setting up of skill set, hunt group, vectors for a call center type environment on the Communication Manager are not the focus of these Application Notes; however, some details are provided only for informational purposes and completeness.

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     20
       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     1
               Maximum Video Capable IP Softphones:  18000    12
                   Maximum Administered SIP Trunks: 40000     64
  Max Administered Ad-hoc Video Conferencing Ports: 24000      0
   Max Number of DS1 Boards with Echo Cancellation: 999    0
```

5.2. System Feature

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming calls from the PSTN to be transferred to Fonolo VCB. If for security reasons incoming calls should not be allowed to transfer back to the PSTN, then leave the field set to **none**.

```
change system-parameters features                               Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                  AAR/ARS Dial Tone Required? y
                              Music/Tone on Hold: music Type: ext   1103
              Music (or Silence) on Transferred Trunk Calls? no
              DID/Tie/ISDN/SIP Intercept Treatment: attendant
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n




             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

5.3. Administer IP Node Names

Use the "change node-names ip" command (not shown) and add an entry for Session Manager. In this case, **interopASM** and **10.33.1.12** are entered as **Name** and **IP Address**. Note the **procr** and **10.33.1.6** 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
interopASM            10.33.1.12
lsp                   10.33.1.7
procr                 10.33.1.6
```

5.4. 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. As per the observation noted in **Section** Error! Reference source not found. only configure **G.711MU**. The codec shown below was used in the compliance testing. Note that Fonolo only supports codec G.711 during the compliance test.

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

                          IP MEDIA PARAMETERS
    Codec Set: 1

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

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

5.5. 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 1                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: bvwdev.com
    Name: Loc-1                 Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.6. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling 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 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 1                                        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: 5061                  Far-end Listen Port: 5061
                                          Far-end Network Region: 1

Far-end Domain: bvwdev.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
```

5.7. 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** "tie".
- **Signaling Group:** Enter the signaling group that has been created in **Section 5.5**.

```
add trunk-group 1                                           Page   1 of   5
                                TRUNK GROUP

Group Number: 1                    Group Type: sip          CDR Reports: y
  Group Name: Private Trunk               COR: 1        TN: 1        TAC: #01
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

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

```
add trunk-group 1                                          Page   3 of   4
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                         Maintenance Tests? y

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

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no



 Show ANSWERED BY on Display? y
```

Navigate to **Page 5** and enter “y” for the **Convert 180 to 183 for Early Media** field as shown below.

```
add trunk-group 1                                            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? n
                              Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? y
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                Request URI Contents: may-have-extra-digits
```

5.8. Administer Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to Fonolo VCB. Add an entry for the trunk group defined in **Section 5.6**. In the example shown below, all calls originating from a 4-digit extension beginning with **33** and **34** and routed to trunk group **1** will result in a 4-digit calling number. The calling party number will be in the SIP “From” header.

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

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 4  33               1                           4  Total Administered: 15
 4  34               1                           4     Maximum Entries: 540
```

5.9. 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
```

5.10. 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
```

5.11. 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 "1". 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 1                                        Page   1 of   4
                    Pattern Number: 1      Pattern Name: SIP-TLS-To-SM
    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: 1    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
```

5.12. 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 010**.

```
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     1        aar          n
```

5.13. Administer Agent Login ID

To add an agent login ID, use the command “add agent-loginID <agent ID>” for each agent. In the compliance test, three agent login IDs 1000 and 1001 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 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:
```

5.14. 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 login IDs configured in **Section 5.12**.

```
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:
```

5.15. 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" or stay in the queue if all agents are busy. If caller presses "1", then the call is routed to "78000", which is the number to VCB. Also, 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
```

5.16. Administer VDN

Use the "add vdn n" command to add a VDN number. In the **Destination** field, enter **Vector Number** 1 as configured in **Section 5.14** 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*:
```

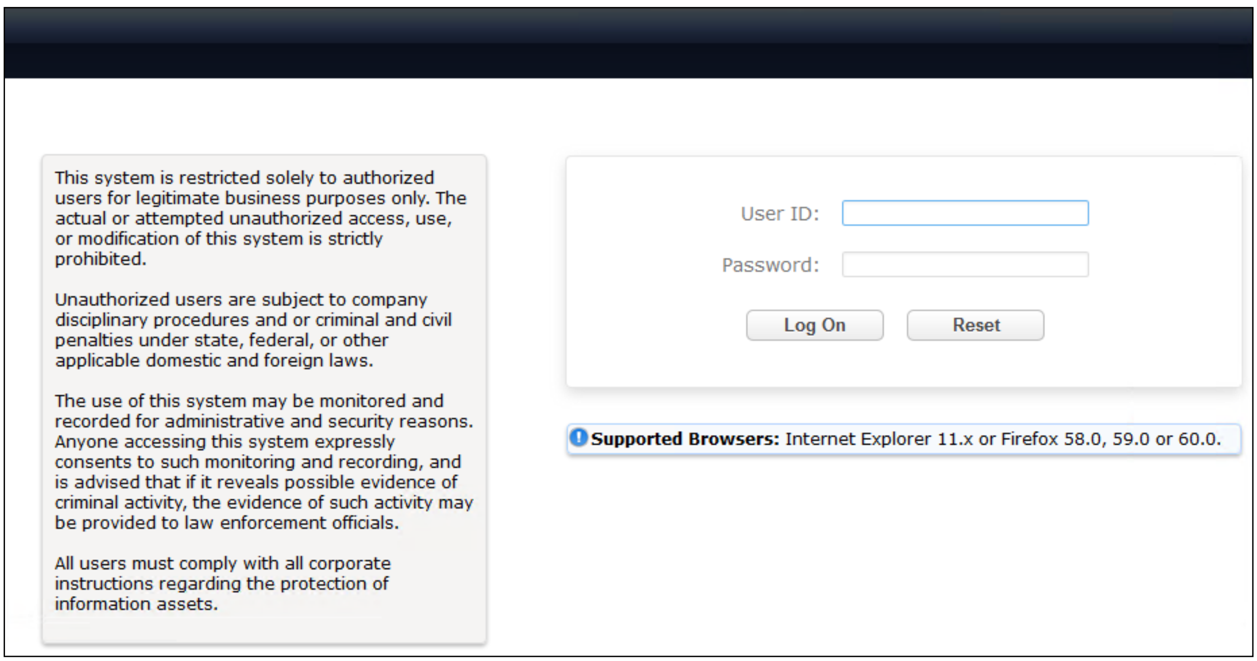
6. Configure Avaya Aura® Session Manager

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

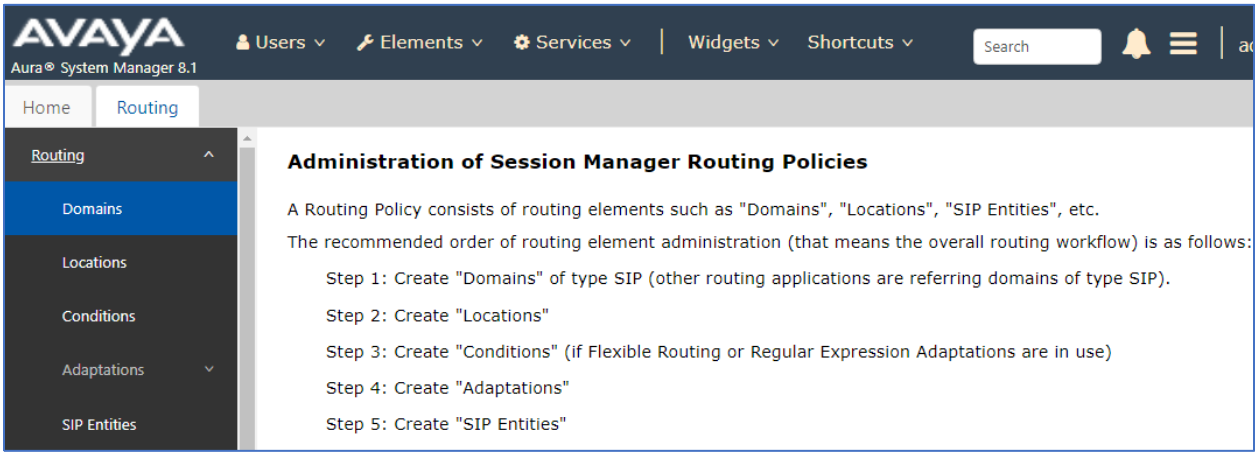
6.1. Launch System Manager

Access the System Manager web interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of System Manager. Log in using the appropriate credentials.

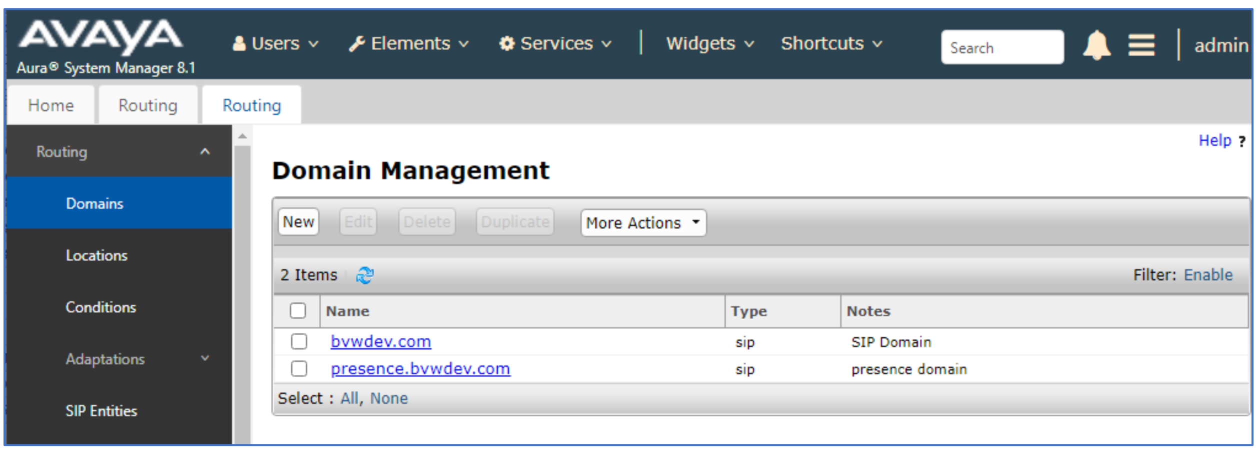


6.2. Administer Domain

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



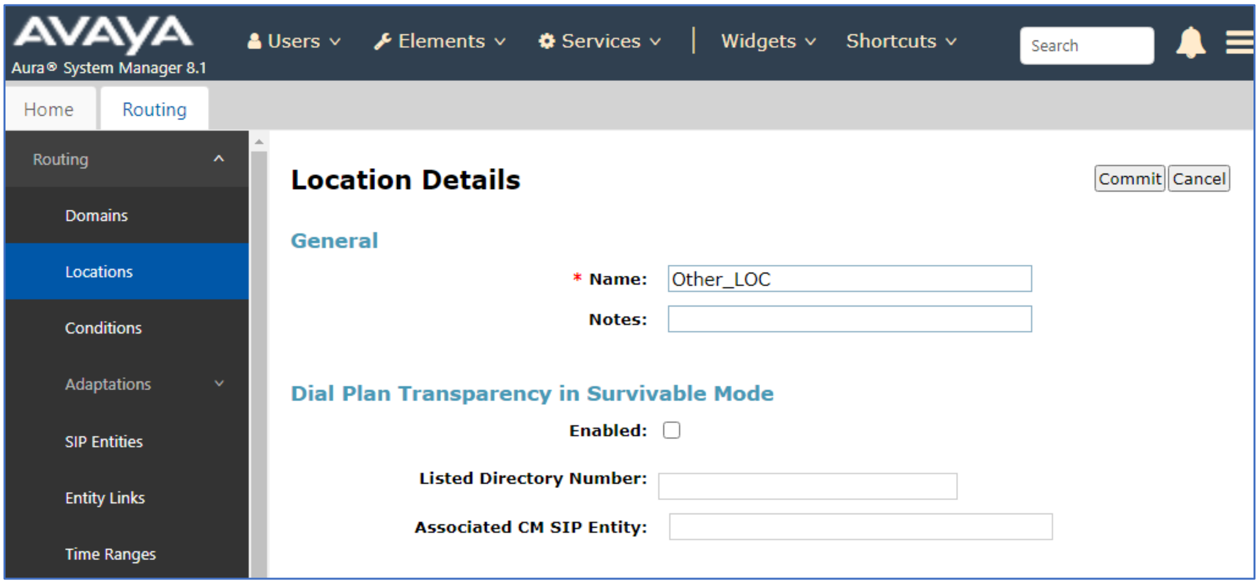
The **Domain Management** screen is displayed. In the **Name** field enter the domain name, select "sip" from the **Type** drop down menu and provide any optional **Notes**.



6.3. Administer Locations

Select **Routing → Locations** from the left pane and click **New** in the subsequent screen (not shown) to add a new location for VCB.

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. Retain the default values in the remaining fields.

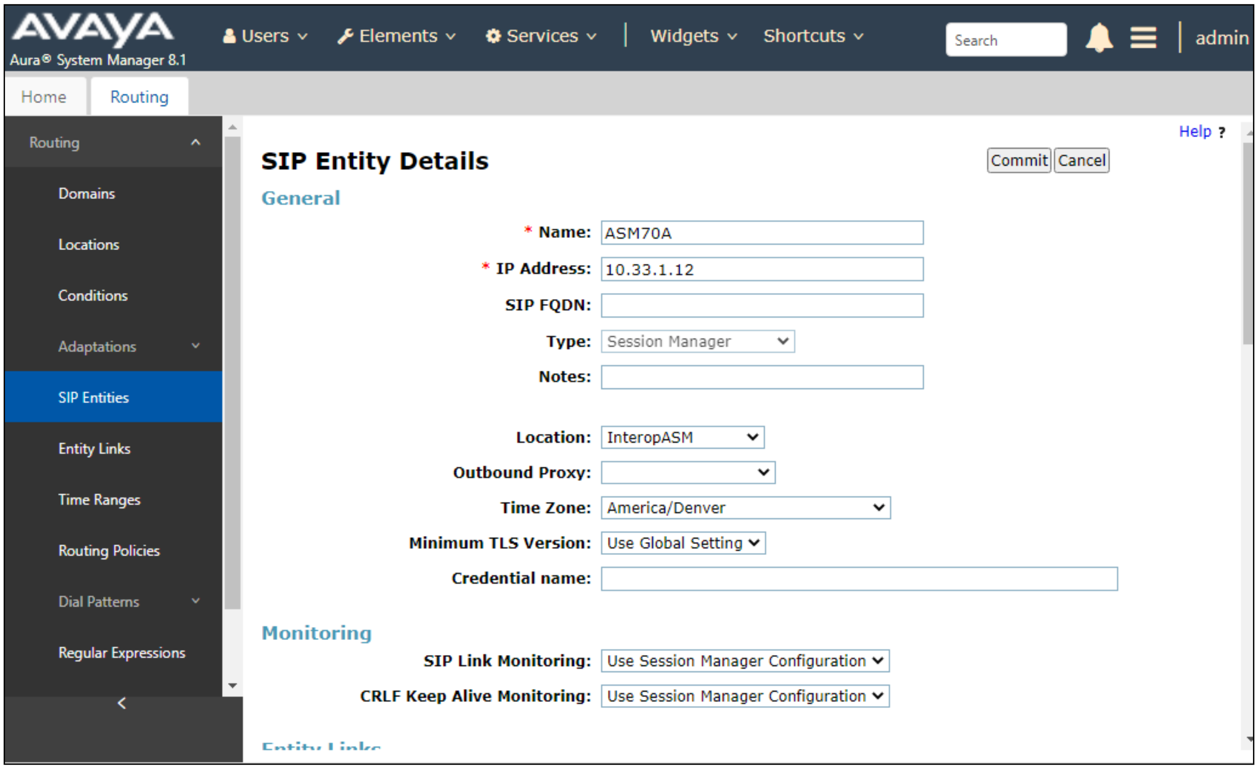


6.4. Administer SIP Entities

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 SBCE.

6.4.1. Configure Session Manager SIP Entity

The following screen shows the previously configured Session Manager SIP Entity named **ASM70A**. The IP address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.1.12**.

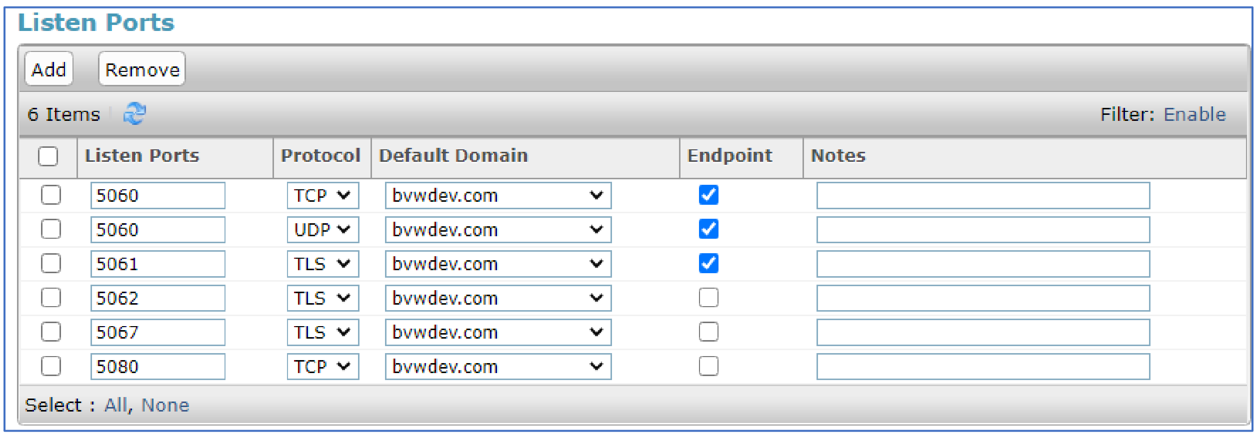

AVAYA
Aura® System Manager 8.1
Users
Elements
Services
Widgets
Shortcuts
Search
admin
Home
Routing
Routing
Domains
Locations
Conditions
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Help ?
SIP Entity Details
Commit
Cancel
General
* Name: ASM70A
* IP Address: 10.33.1.12
SIP FQDN:
Type: Session Manager
Notes:
Location: InteropASM
Outbound Proxy:
Time Zone: America/Denver
Minimum TLS Version: Use Global Setting
Credential name:
Monitoring
SIP Link Monitoring: Use Session Manager Configuration
CRLF Keep Alive Monitoring: Use Session Manager Configuration

The ports need to be defined in Session Manager for other endpoints to connect, scroll down to the **Listen Ports** section of the **SIP Entity Details** screen. Note that this section is only present for the **Session Manager** SIP Entity.

In the **Listen Ports** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port**: Port number on which Session Manager listens for SIP requests.
- **Protocol**: Transport protocol to be used with this port.
- **Default Domain**: The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain.

The compliance test used port **5060** for **UDP** and **5061** for **TLS** for connecting to the Avaya SBCE and Communication Manager.


Listen Ports

Add Remove

6 Items Filter: Enable

Listen Ports	Protocol	Default Domain	Endpoint	Notes
5060	TCP	bvwdev.com	✓	
5060	UDP	bvwdev.com	✓	
5061	TLS	bvwdev.com	✓	
5062	TLS	bvwdev.com		
5067	TLS	bvwdev.com		
5080	TCP	bvwdev.com		

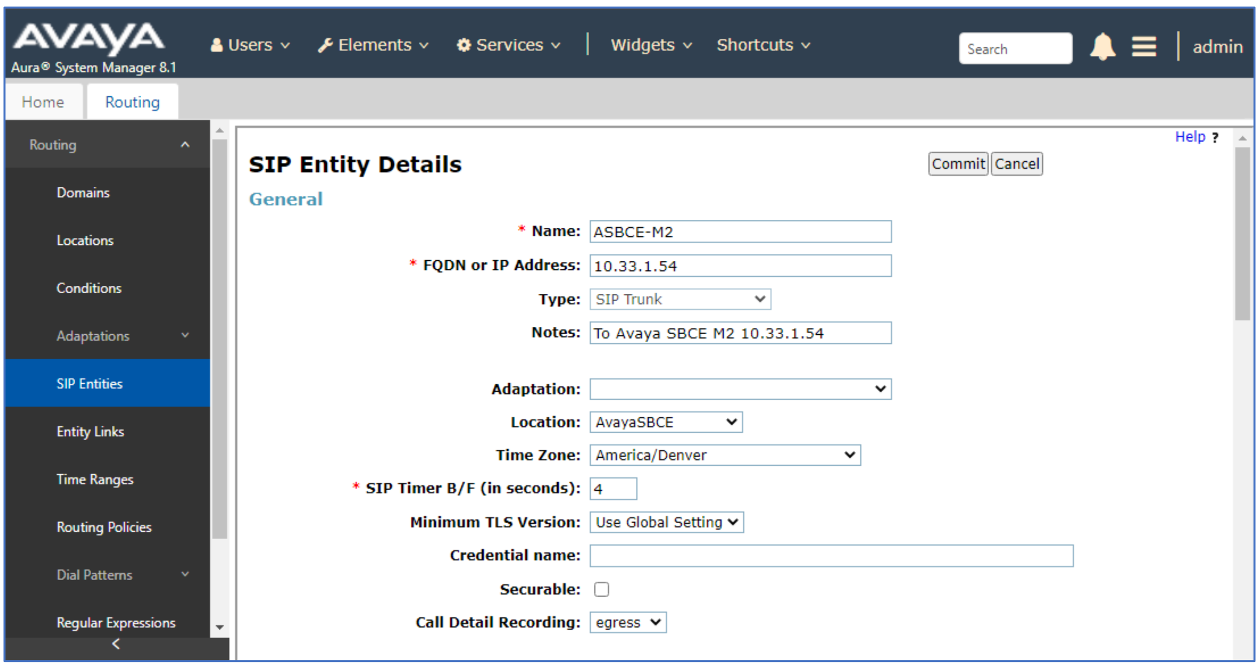
Select : All, None

6.4.2. SIP Entity for Avaya SBCE

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 SBCE.

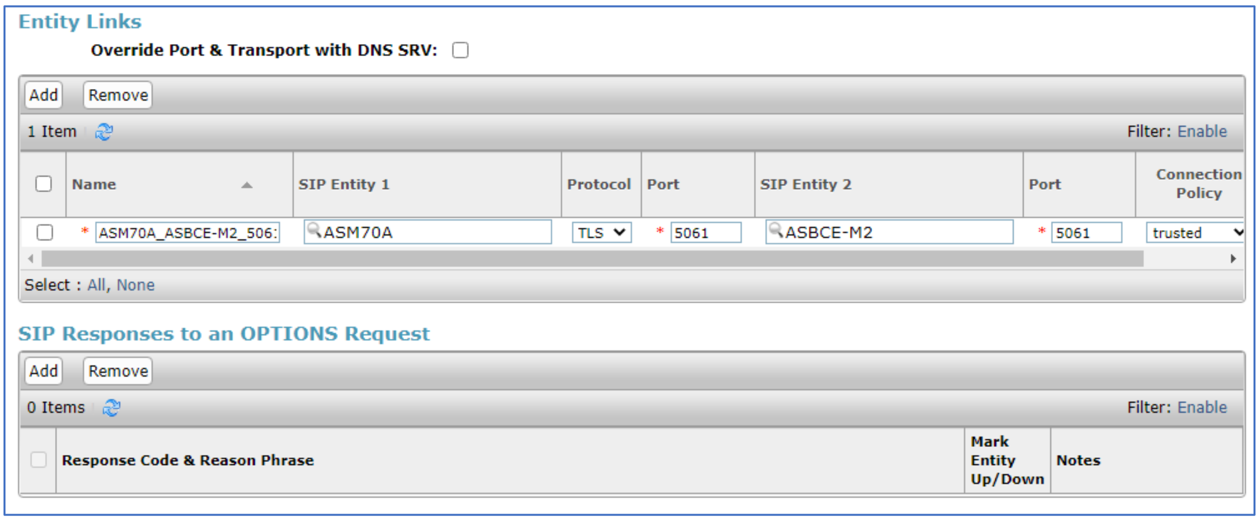
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** The IP address of internal interface of Avaya SBCE.
- **Type:** Set is as "SIP Trunk".
- **Notes:** Enter desired notes.
- **Location:** Select the desired location name from the list.
- **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 “ASM70A”.
- **Protocol:** Set it as “TLS”.
- **Port:** Set it as “5061”.
- **SIP Entity 2:** Avaya SBCE entity name from this section.
- **Port:** Set it as “5061”.
- **Connection Policy:** Select “trusted”.

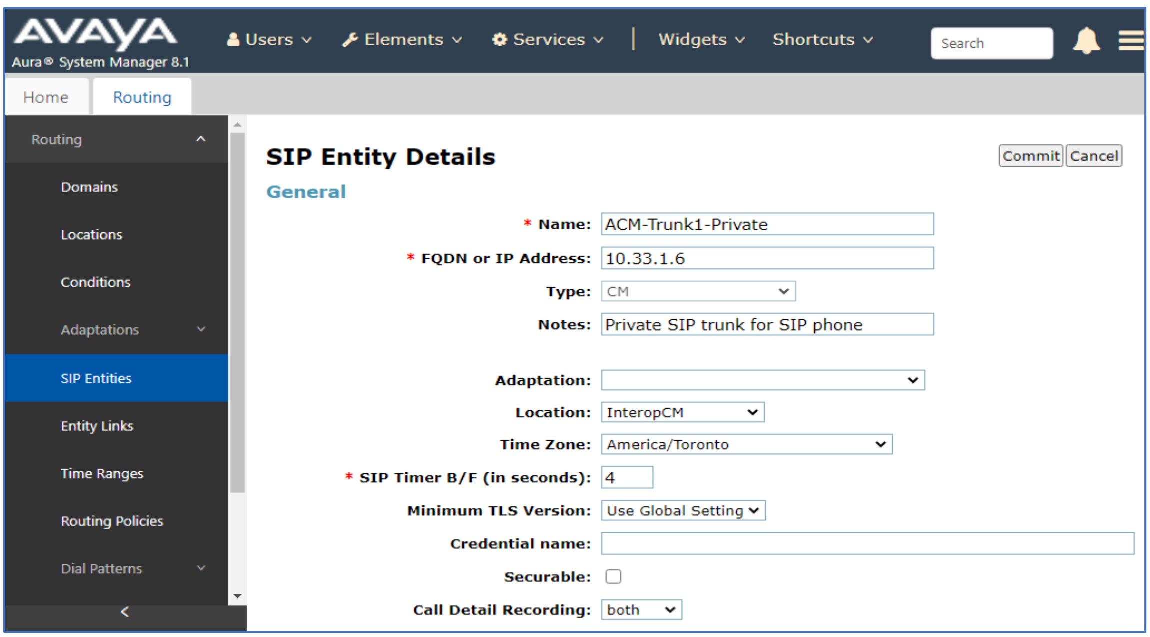


6.4.3. SIP Entity for Communication Manager

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.

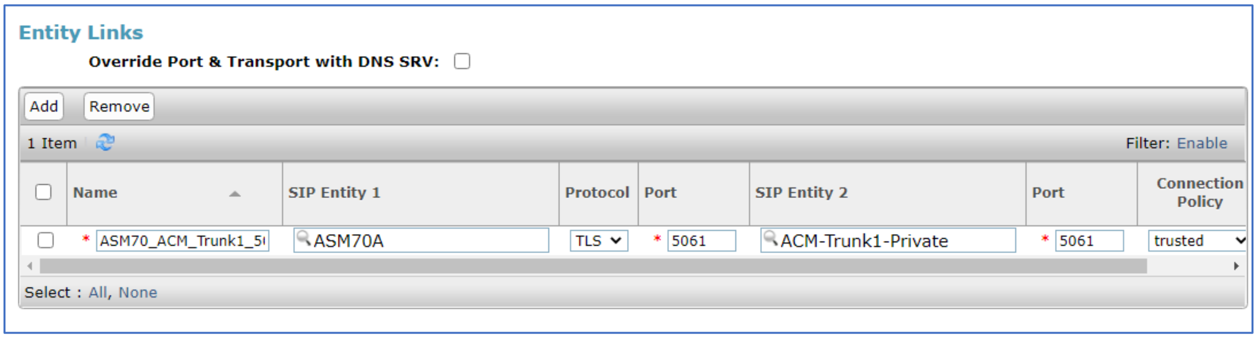
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **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 the applicable location for Communication Manager.
- **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 "ASM70A".
- **Protocol:** The signaling group transport TLS method.
- **Port:** The signaling group listen port 5061.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group listen port 5061 number.
- **Connection Policy:** Select "trusted".



6.5. Administer Routing Policies

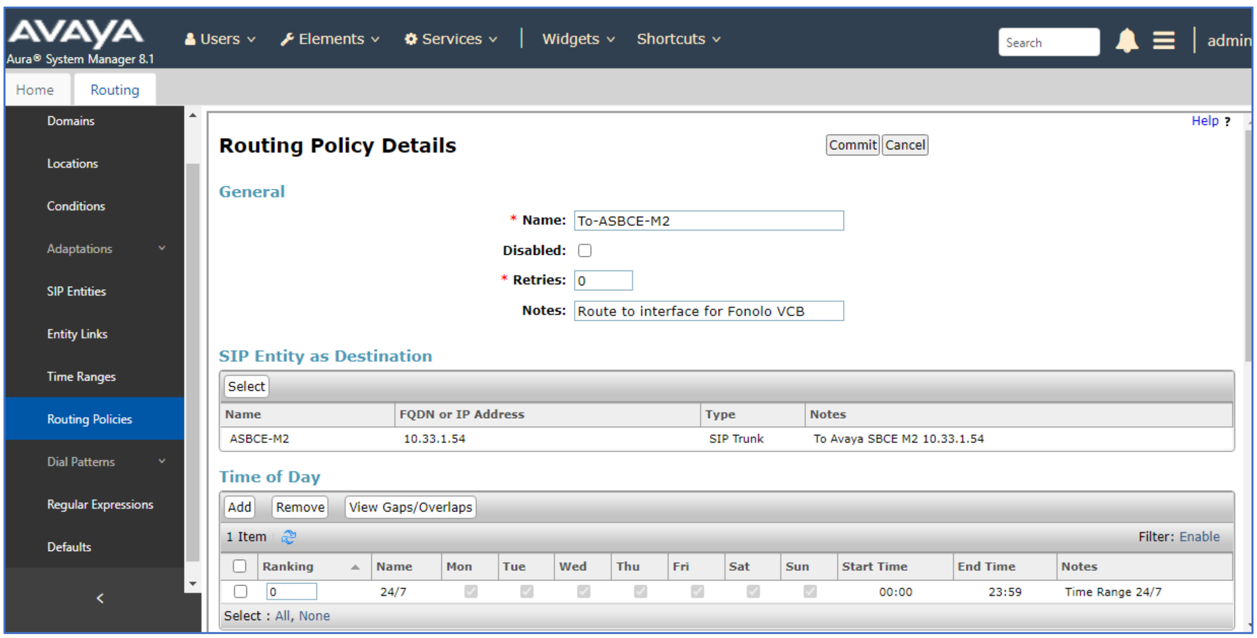
Add two new routing policies, one for Avaya SBCE and one for the SIP trunks with Communication Manager.

6.5.1. Routing Policy for Avaya SBCE

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 SBCE.

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 Avaya SBCE SIP entity name from **Section 6.4.2**. In the **Time of Day** sub-section, leave the default setting.

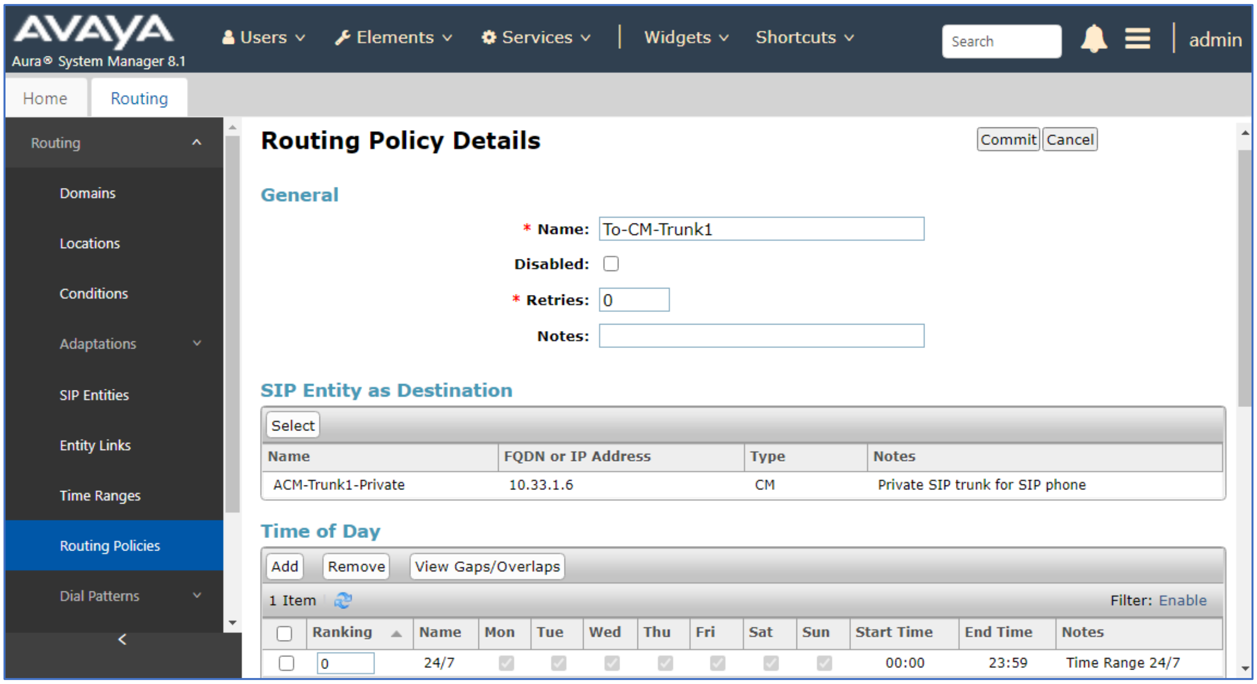


6.5.2. Routing Policy for Communication Manager

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 entity name from **Section 6.4.33**. The screen below shows the result of the selection.



6.6. Administer Dial Patterns

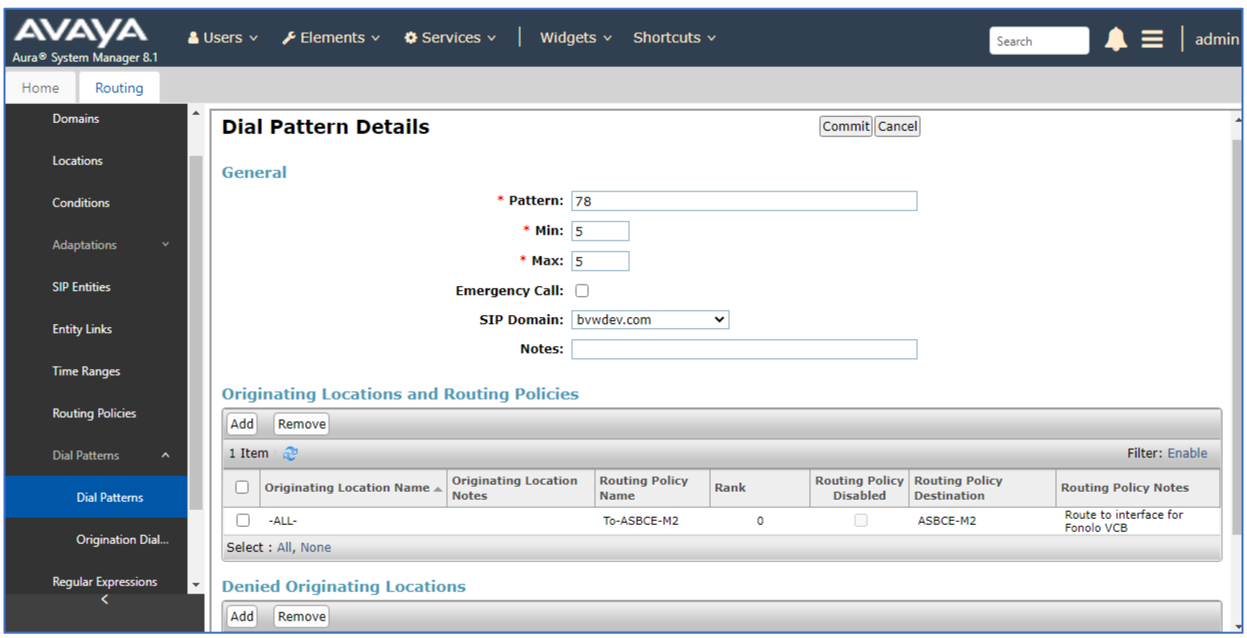
Add a new dial pattern for Avaya SBCE and Communication Manager.

6.6.1. Dial Pattern for Avaya SBCE

Select **Routing → Dial Patterns** from the left pane and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach the Fonolo appliance through Avaya SBCE. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case "78".
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain**: The signaling group domain name from **Section 6.2**.

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

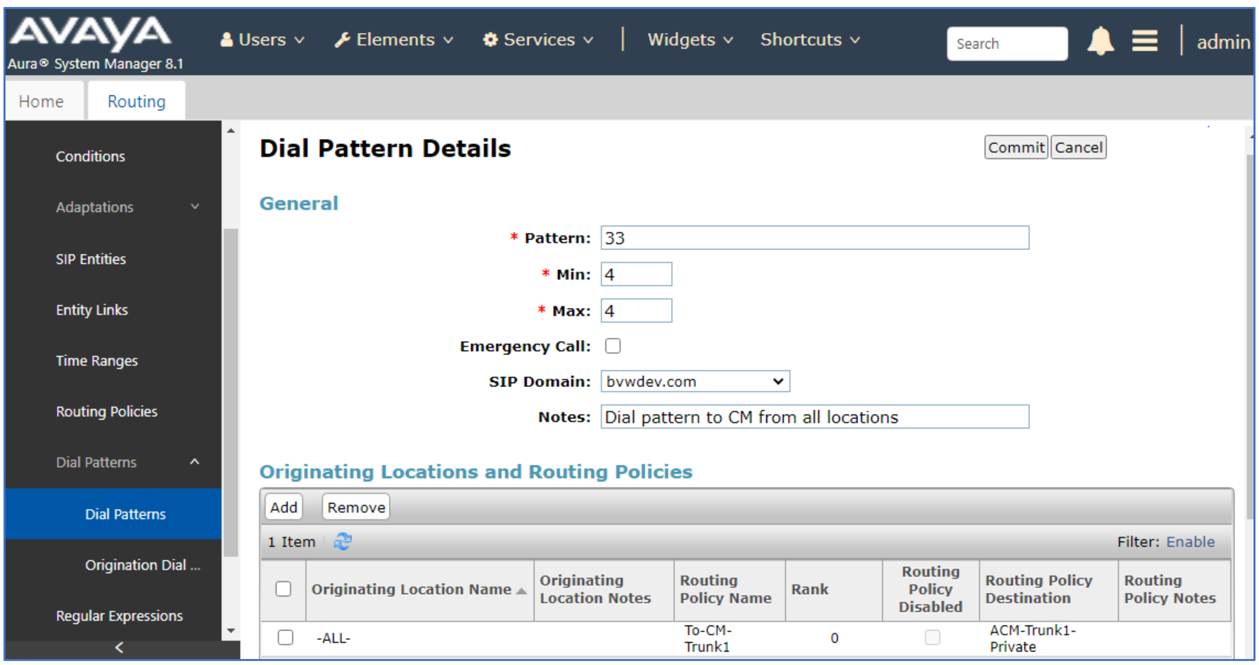


6.6.2. Dial Pattern for Communication Manager

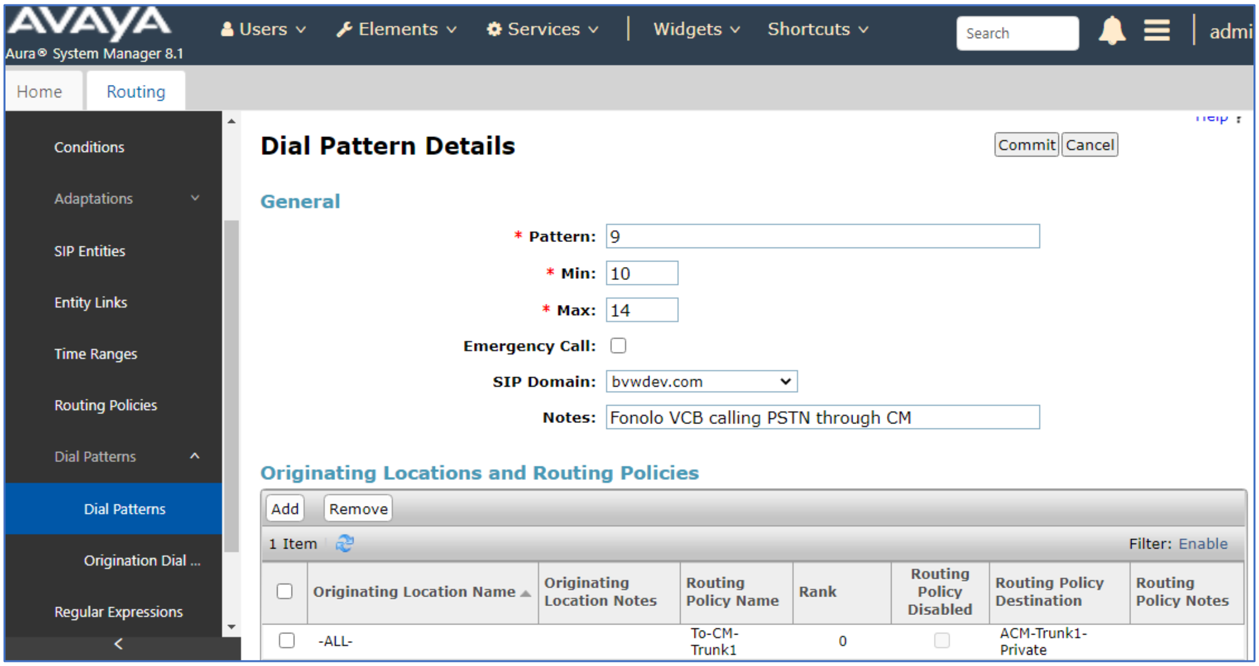
Select **Routing → Dial Patterns** from the left pane and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach Communication Manager. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, two dial patterns “33” and “9” were added.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain**: The signaling group domain name from **Section 6.2**.

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 in locations. The Communication Manager routing policy from **Section 6.5.2** was selected as shown below.



Below is the dial pattern with the leading digit "9" for the outbound call from Fonolo VCB to PSTN through Avaya SBCE, Session Manager and Communication Manager. The digit '9" is the access code in Communication Manager.



7. Configure Avaya Session Border Controller for Enterprise

This section describes the required configuration of the Avaya SBCE to connect to Fonolo VCB appliances.

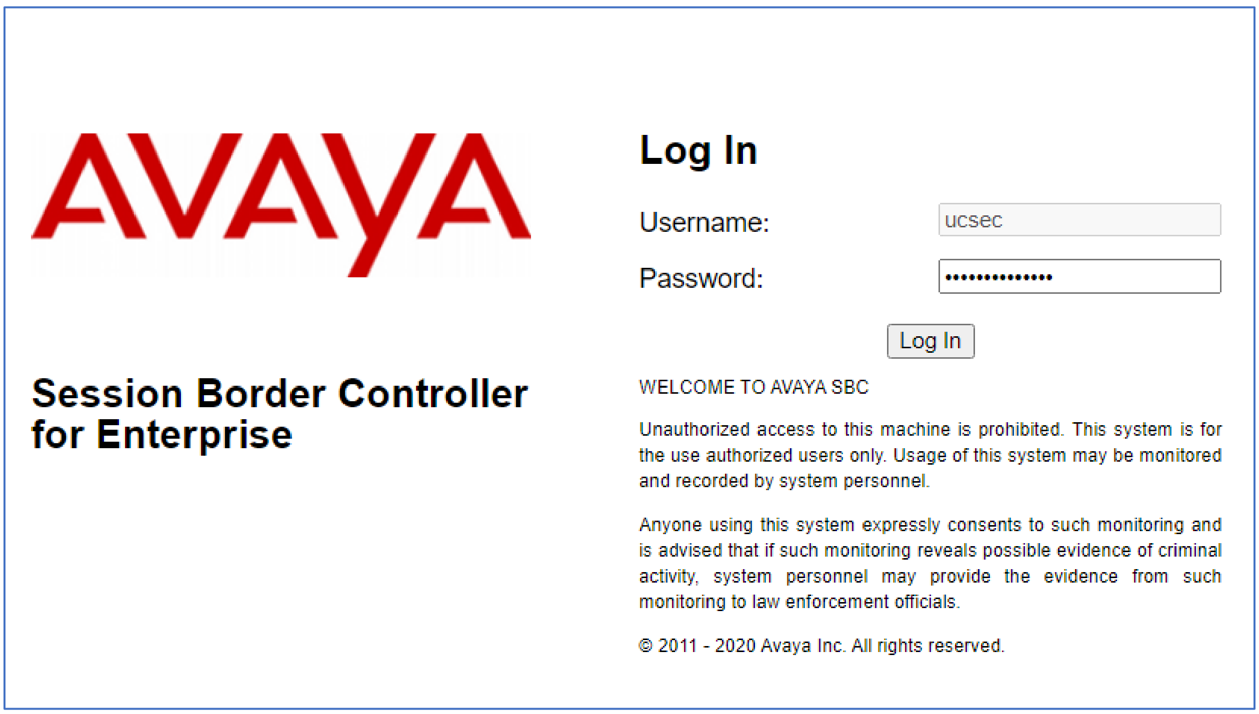
It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

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.

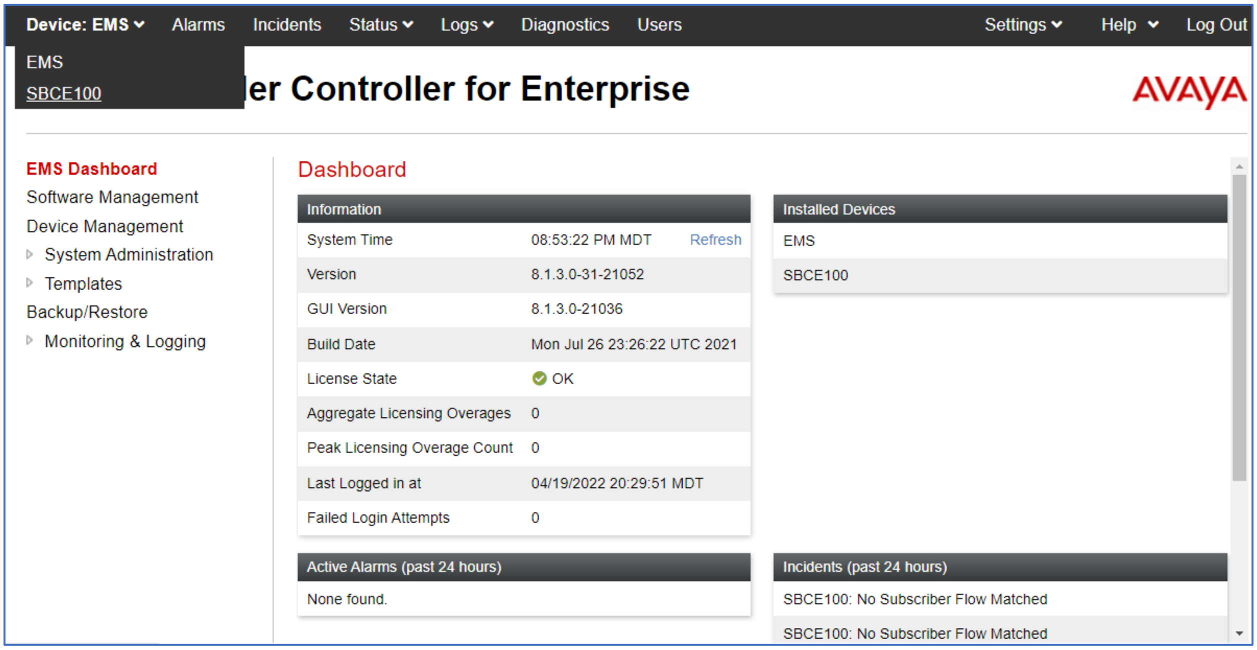
7.1. Log in Avaya SBCE

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

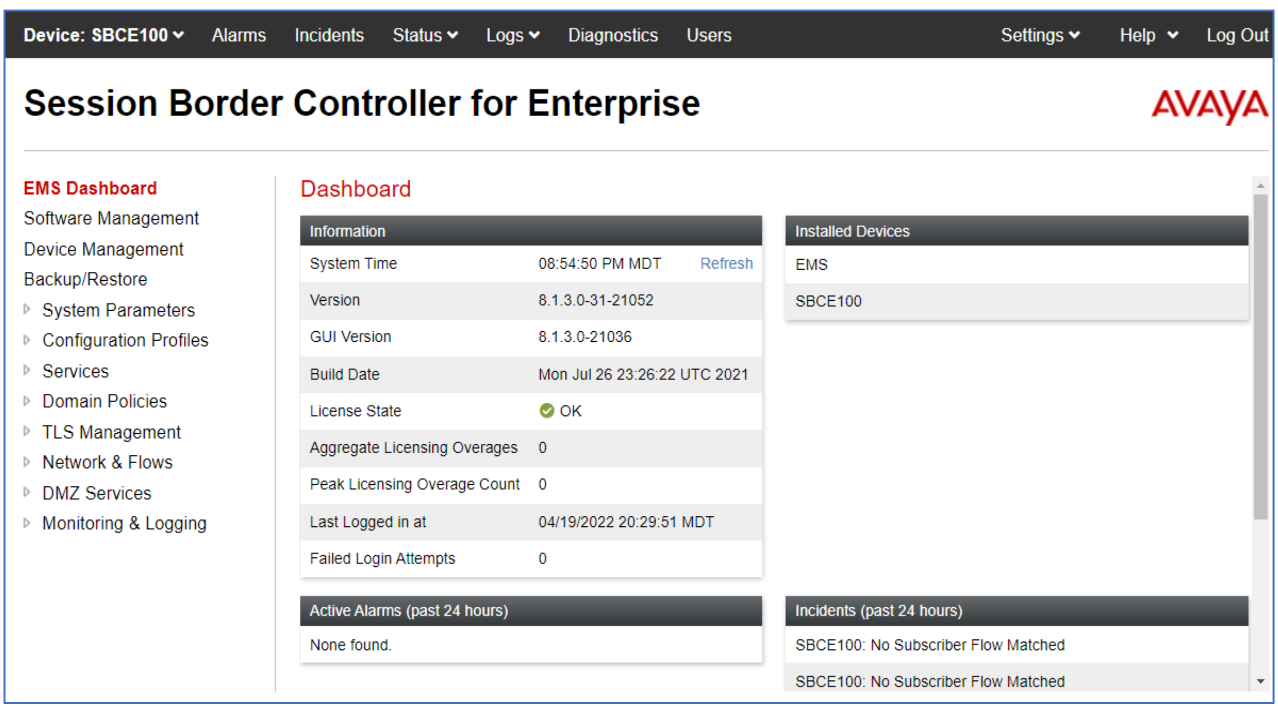
Enter the appropriate credentials and click **Log In**.



Once logged in, on the top left of the screen, under **Device:** select the device being managed, **SBCE100** in the sample configuration.

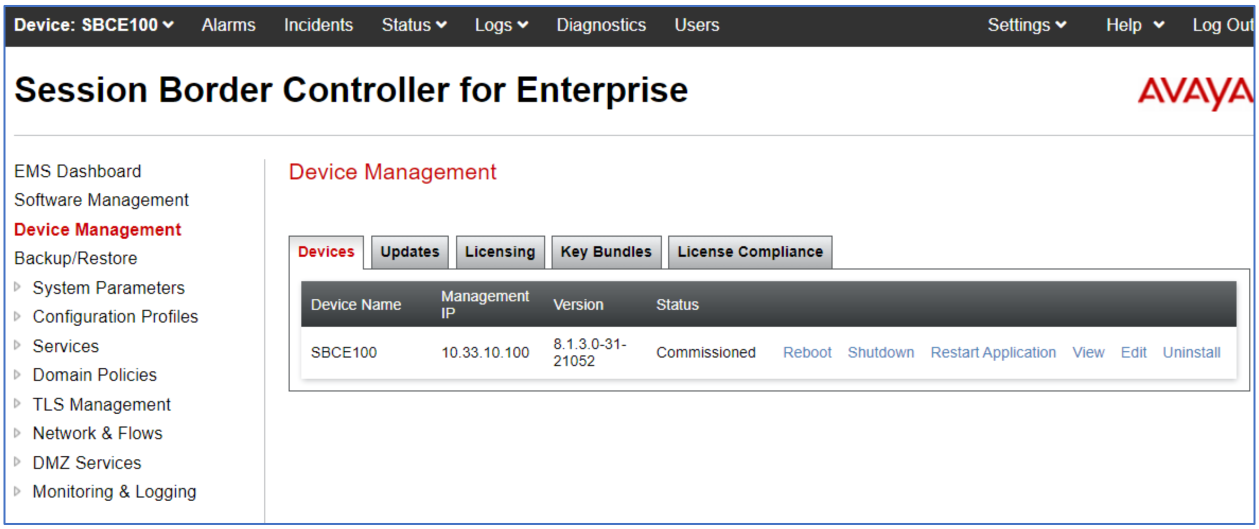


The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.



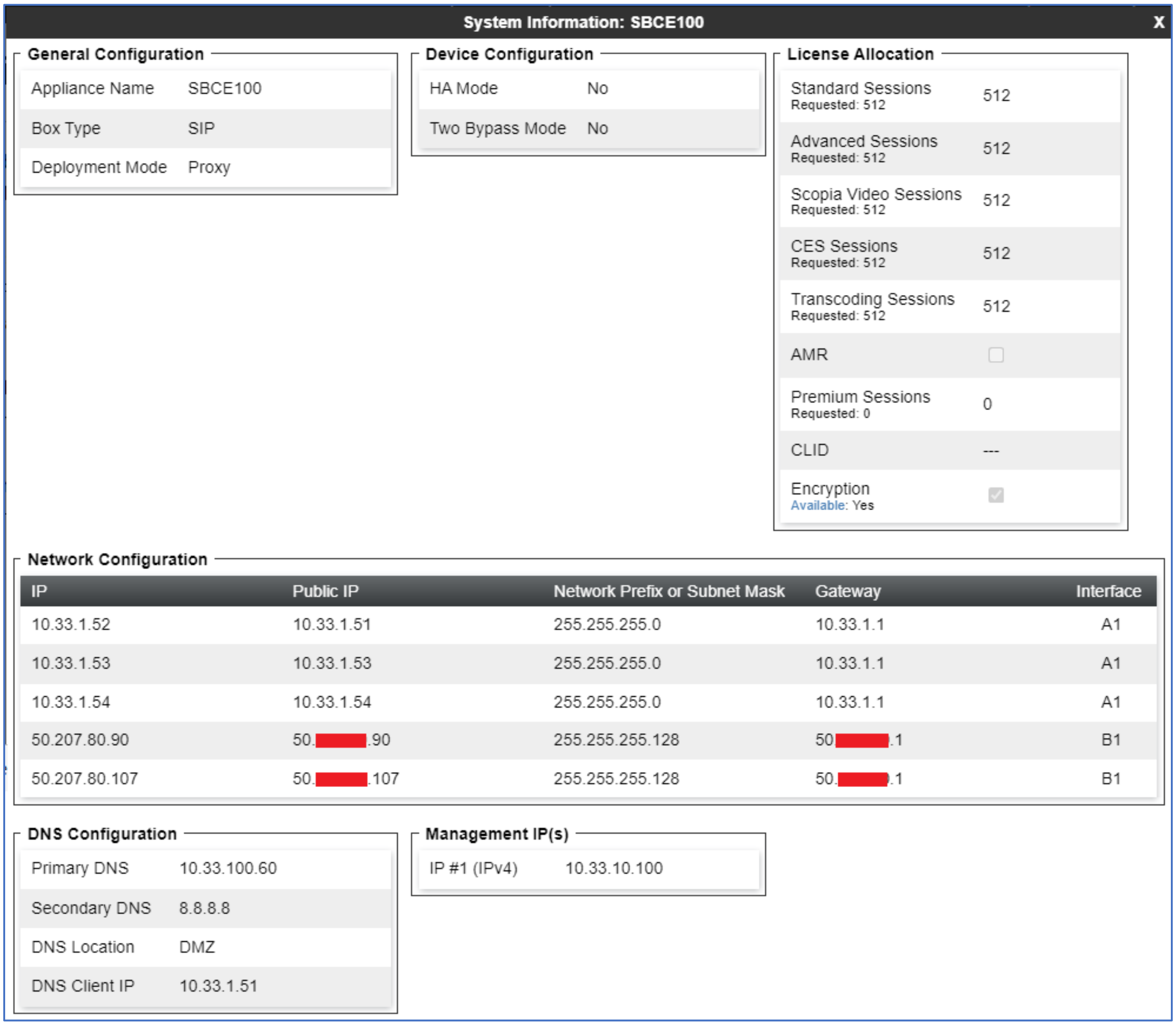
7.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named **SBCE100** is shown.. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, 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 Avaya SBCE, 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. 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 appliance and are the ones relevant to these Application Notes. Other IP addresses assigned to the Avaya SBCE **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 Avaya SBCE (10.33.1.54) was used to connect to the enterprise network, while its public interface (50.xxx.xxx.90) was used to connect to the Fonolo VCB appliance. See **Figure 1**.

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

7.3. Configuration Profiles

The **Configuration Profiles** (not shown) option, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

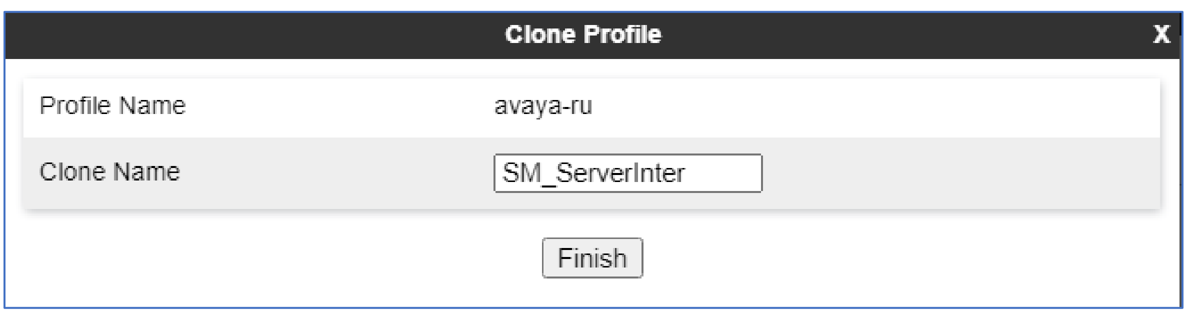
7.3.1. Server Interworking – Session Manager

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or "cloned". Since directly modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or "cloned". If needed, the profile can then be modified to meet specific requirements for the enterprise SIP-enabled solution.

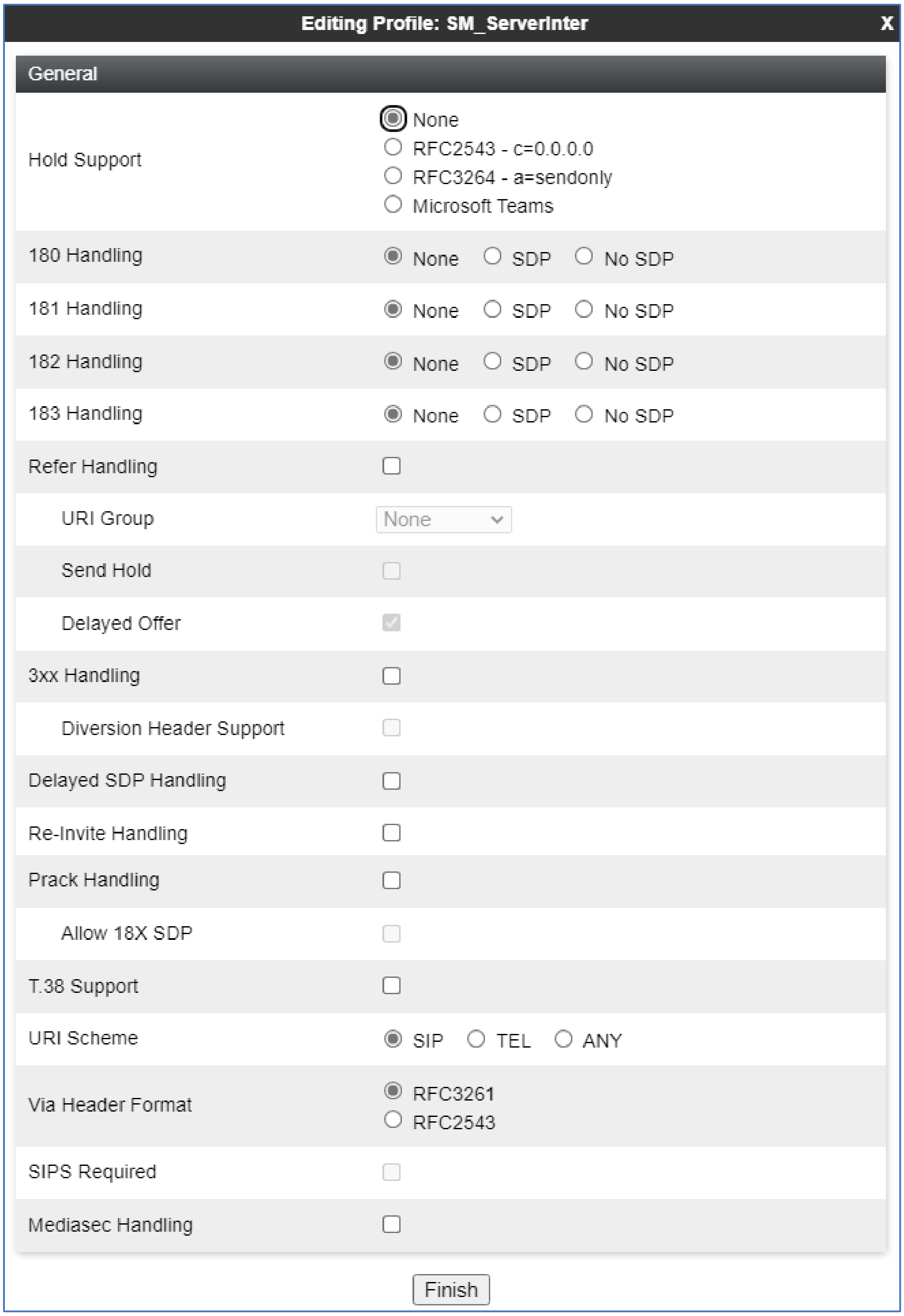
On the left navigation pane, select **Configuration Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **avaya-ru.** Click **Clone** on top right of the screen (not shown).

Enter the new profile name in the **Clone Name** field, the name of **SM_ServerInter** was chosen in this example. Click **Finish**.

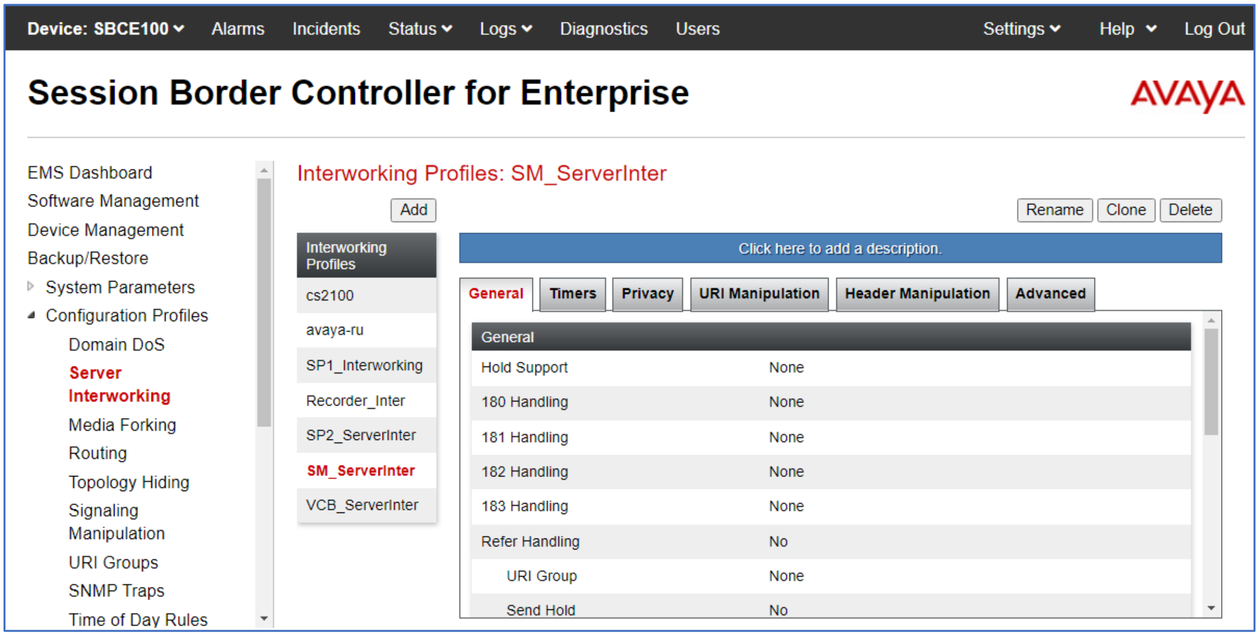


Click **Edit** on the newly cloned **SM_ServerInter** interworking profile:

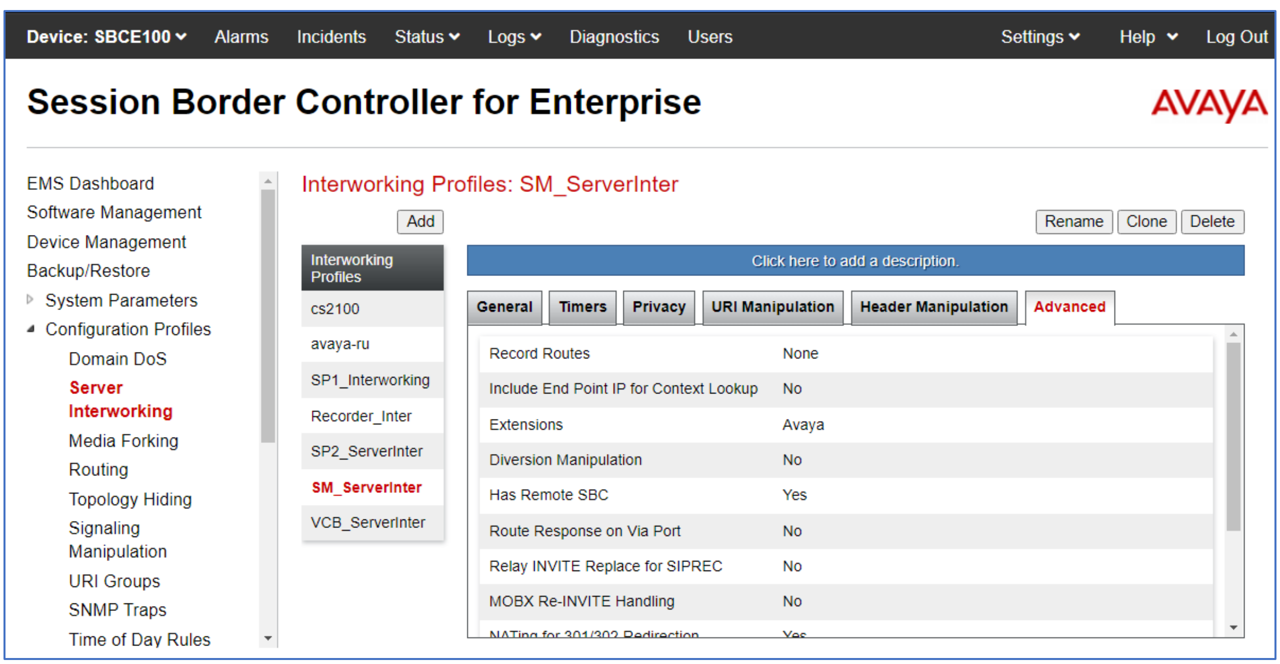
- Leave remaining fields with default values.
- Click **Finish**.



The following screen capture shows the **General** tab of the newly created **SM_ServerInter** Server Interworking Profile.



The following screen capture shows the **Advanced** tab of the newly created **SM_ServerInter** Server Interworking Profile.

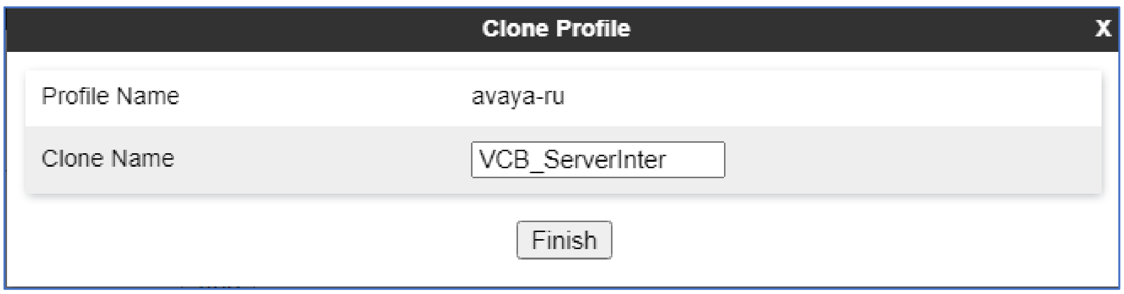


7.3.2. Server Interworking – Fonolo VCB

A new Server Interworking profile named **VCB_ServerInter** was created for the Fonolo VCB appliance.

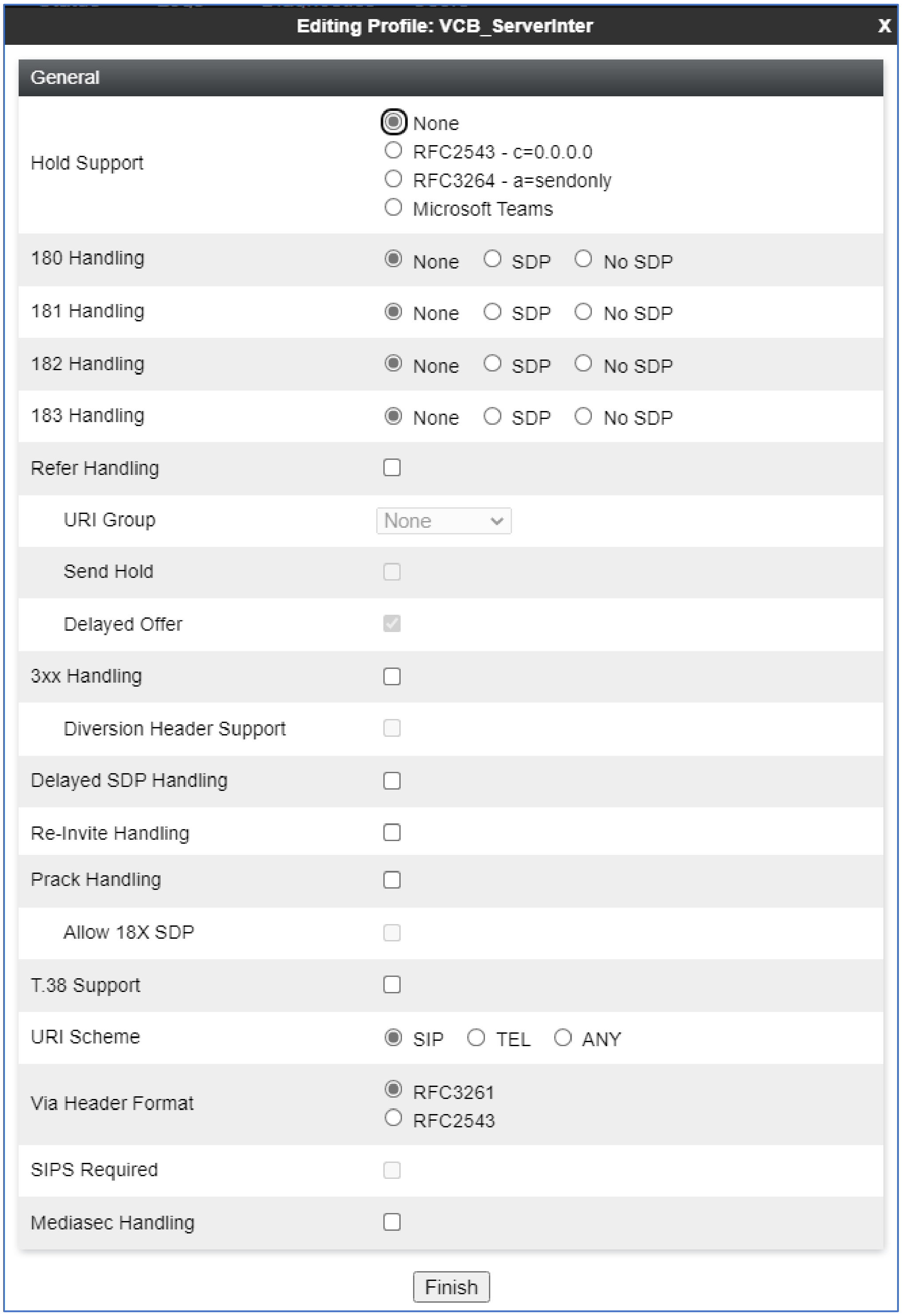
On the left navigation pane, select **Configuration Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **avaya-ru.** Click **Clone** on top right of the screen (not shown).

Enter the new profile name in the **Clone Name** field, the name of **VCB_ServerInter** was chosen in this example. Click **Finish**.

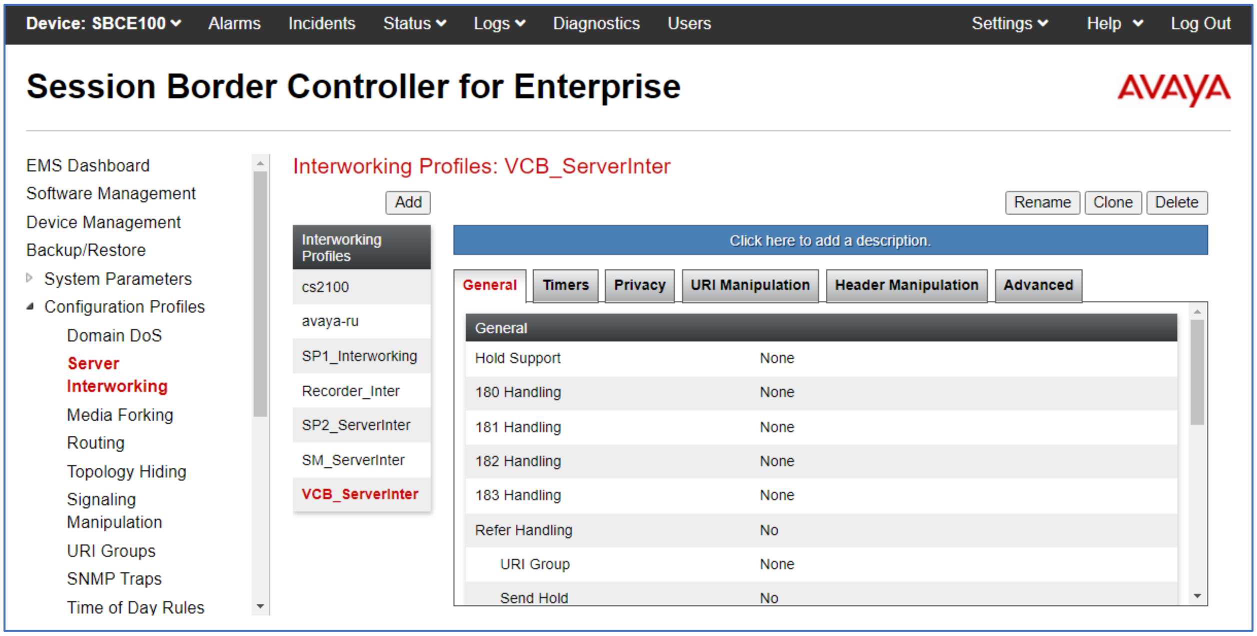


Click **Edit** on the newly cloned **VCB_ServerInter** interworking profile:

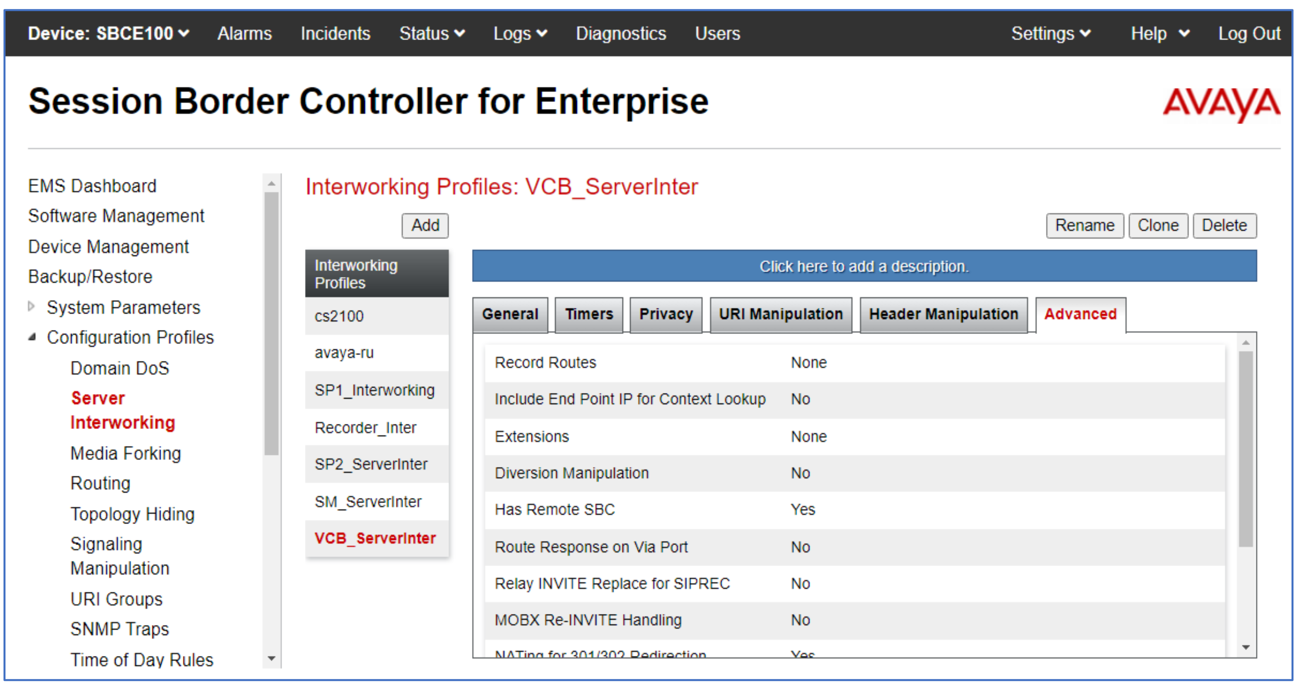
- Leave remaining fields with default values.
- Click **Finish**.



The following screen capture shows the **General** tab of the newly created **VCB_ServerInter** Server Interworking Profile.



The following screen capture shows the **Advanced** tab of the newly created **VCB_ServerInter** Server Interworking Profile.

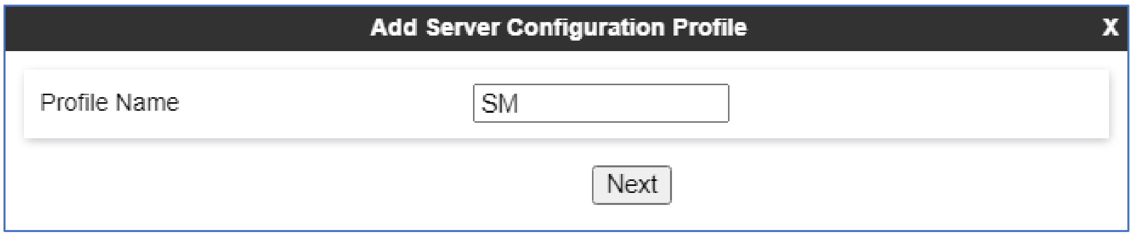


7.3.3. SIP Server Configuration

SIP Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (Session Manager) and the Trunk Server or SIP Proxy at the service provider's network, during the testing Fonolo VCB acted like the SIP service provider.

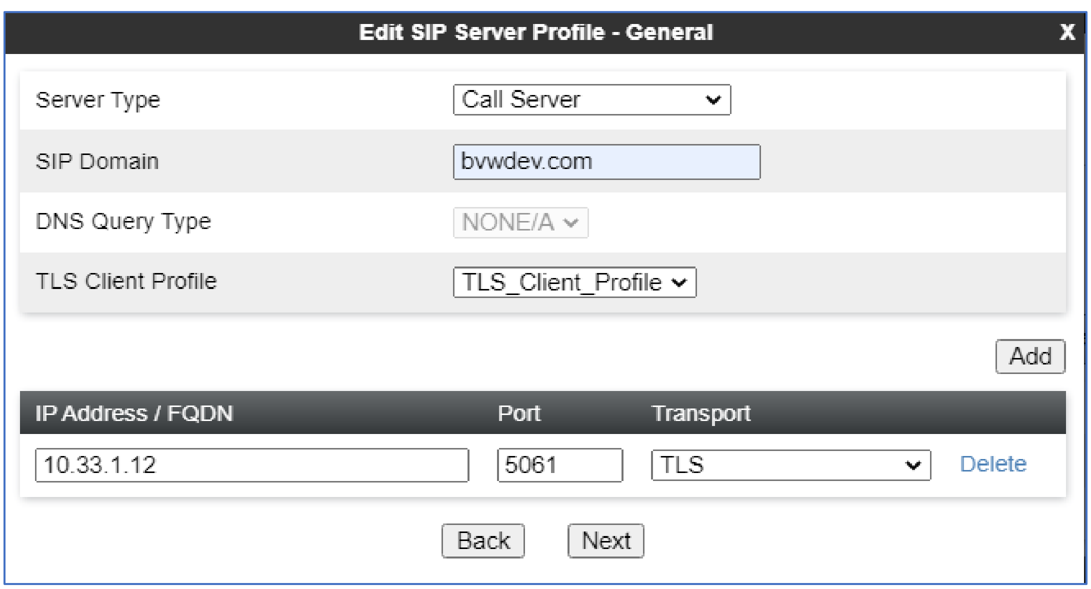
To add the SIP Server profile for the Call Server, from the **Services** menu on the left-hand navigation pane, select **SIP Servers** (not shown). Click **Add** (not shown) and enter the profile name: **SM**.

- Click **Next**.

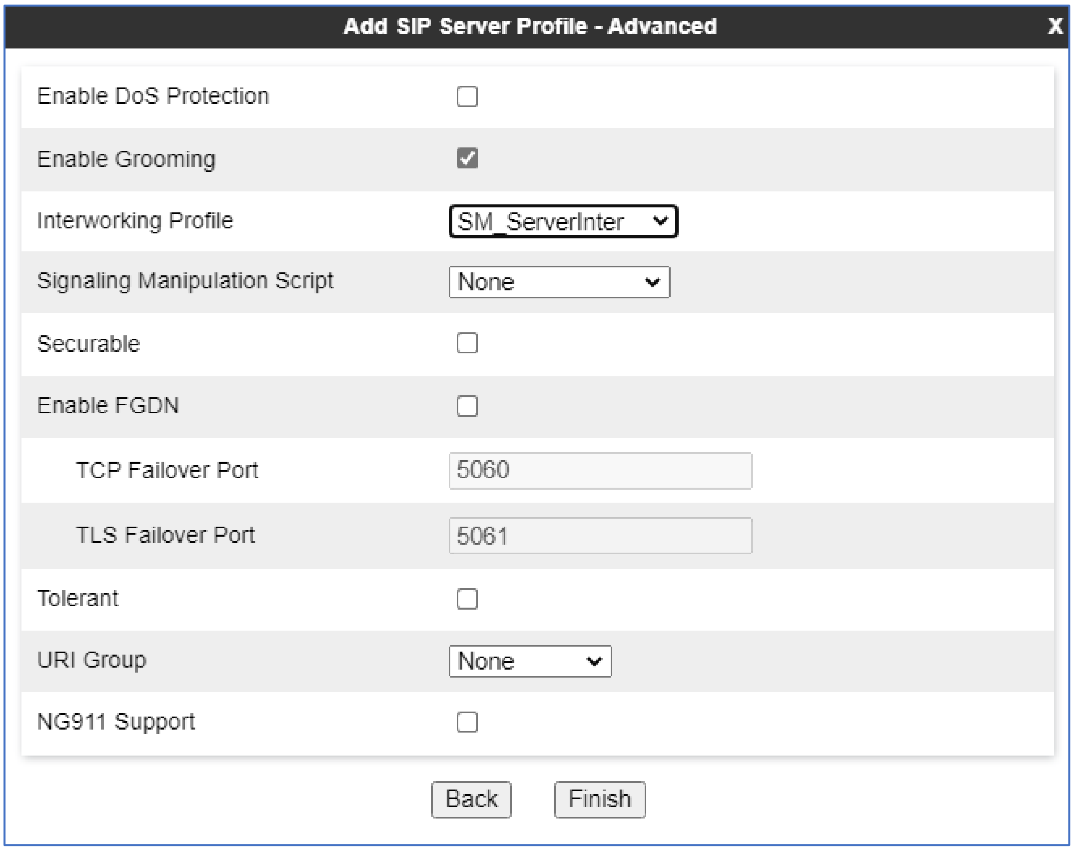


On the **Edit SIP Server Profile – General** window:

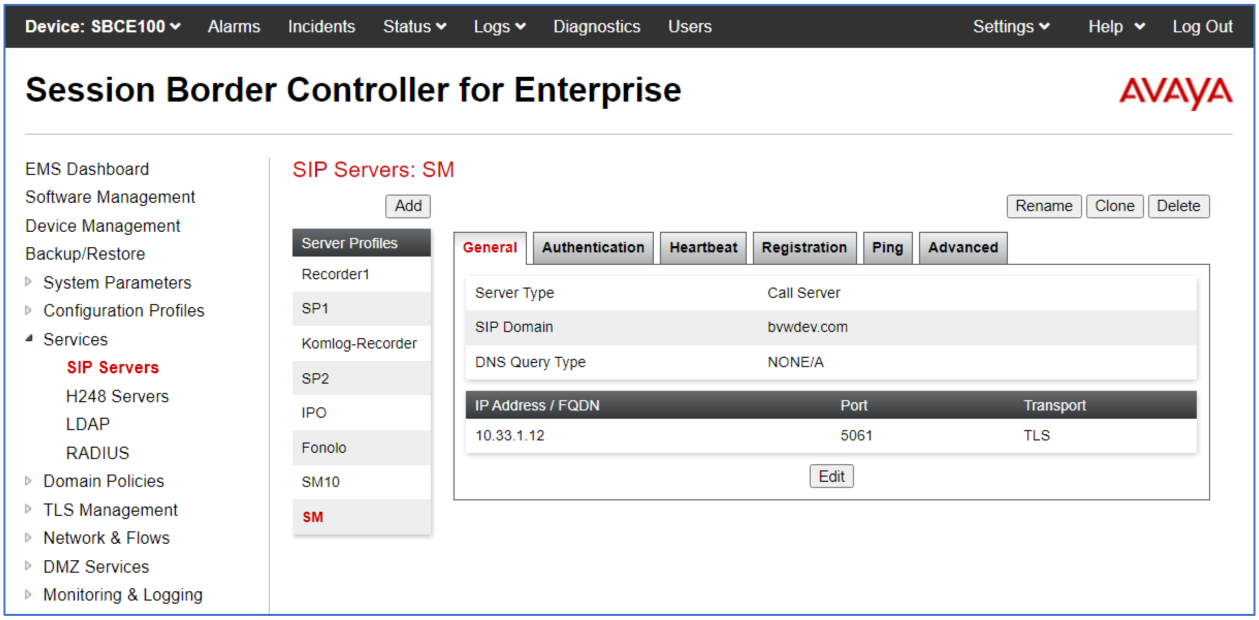
- **Server Type**: Select **Call Server**.
- **SIP Domain**: Enter the enterprise SIP domain as defined in **Section 6.2**.
- **IP Address / FQDN**: **10.33.1.12** (IP Address of Session Manager).
- **Port**: **5061**
- **Transport**: Select **TLS**.
- Select a **TLS Client Profile**. Note that the TLS client profile was previously configured.
- Click **Next**.



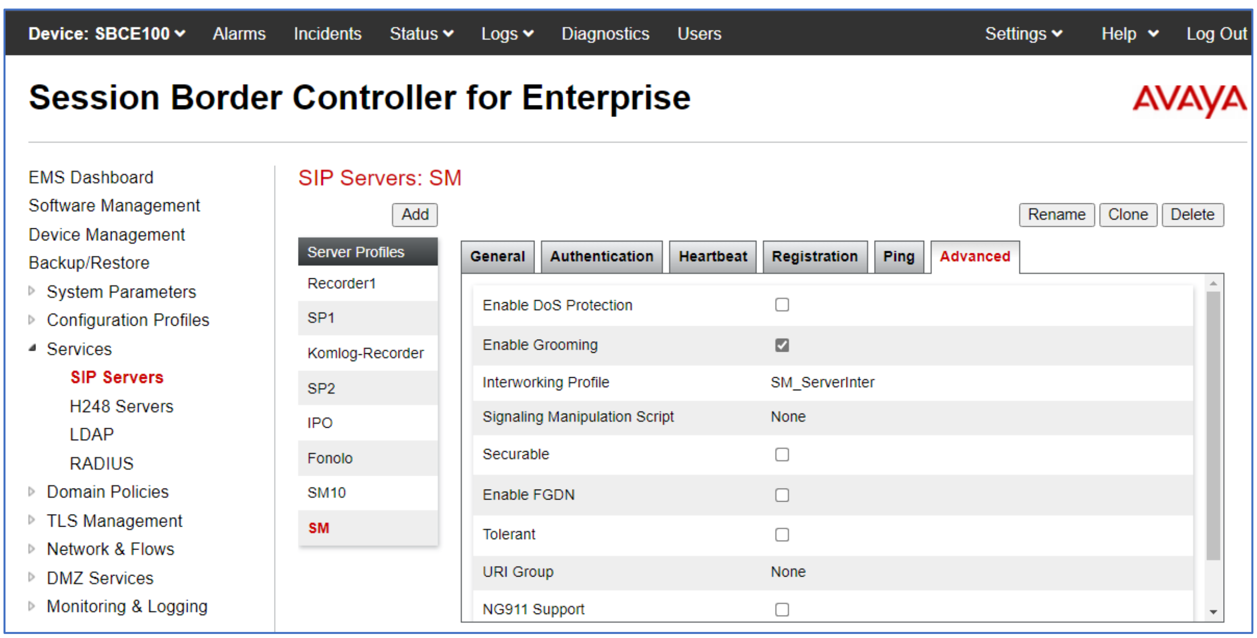
- Click **Next** until the **Add SIP Server Profile - Advanced** tab is reached (not shown).
- On the **Add SIP Server Profile - Advanced** tab:
- Verify that **Enable Grooming** is checked.
- Select **SM_ServerInter** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.



The following screen capture shows the **General** tab of the newly created **SM** SIP Server Configuration Profile.

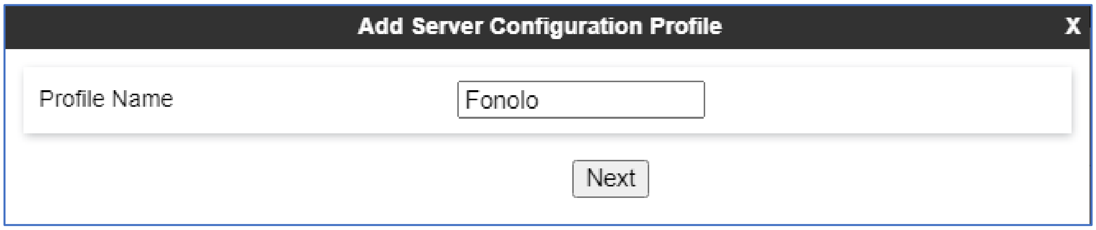


The following screen capture shows the **Advanced** tab of the newly created **SM** SIP Server Configuration Profile.



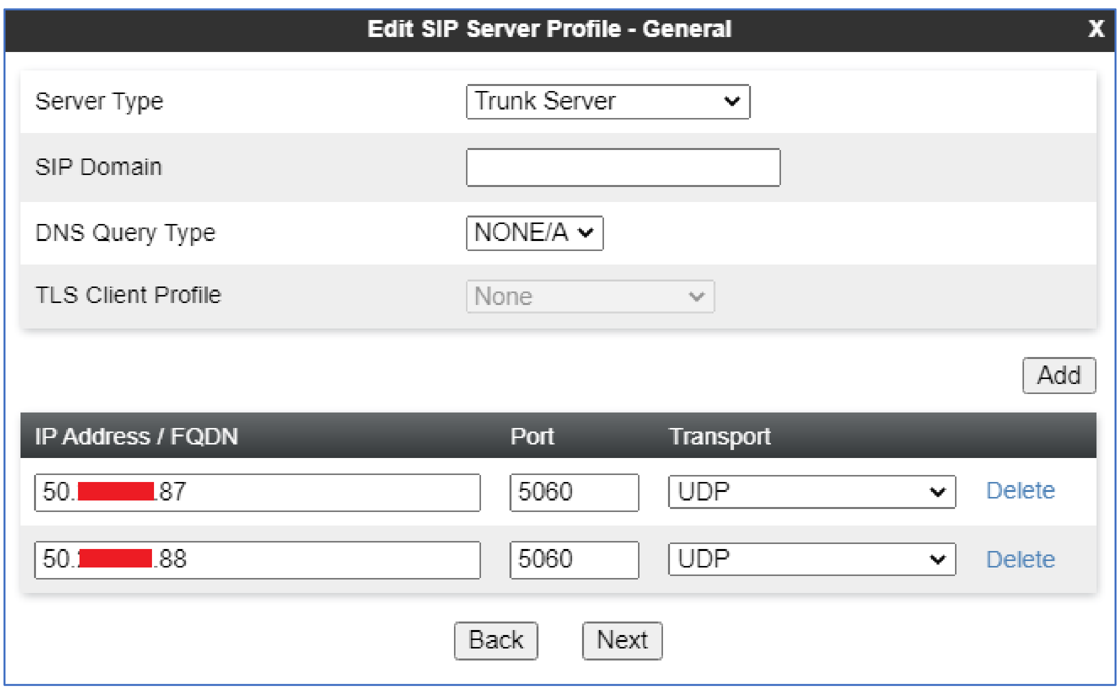
To add the SIP Server profile for the Fonolo Trunk Server, from the **Services** menu on the left-hand navigation pane, select **SIP Servers** (not shown). Click **Add** (not shown) and enter the profile name: **Fonolo**.

- Click **Next**.

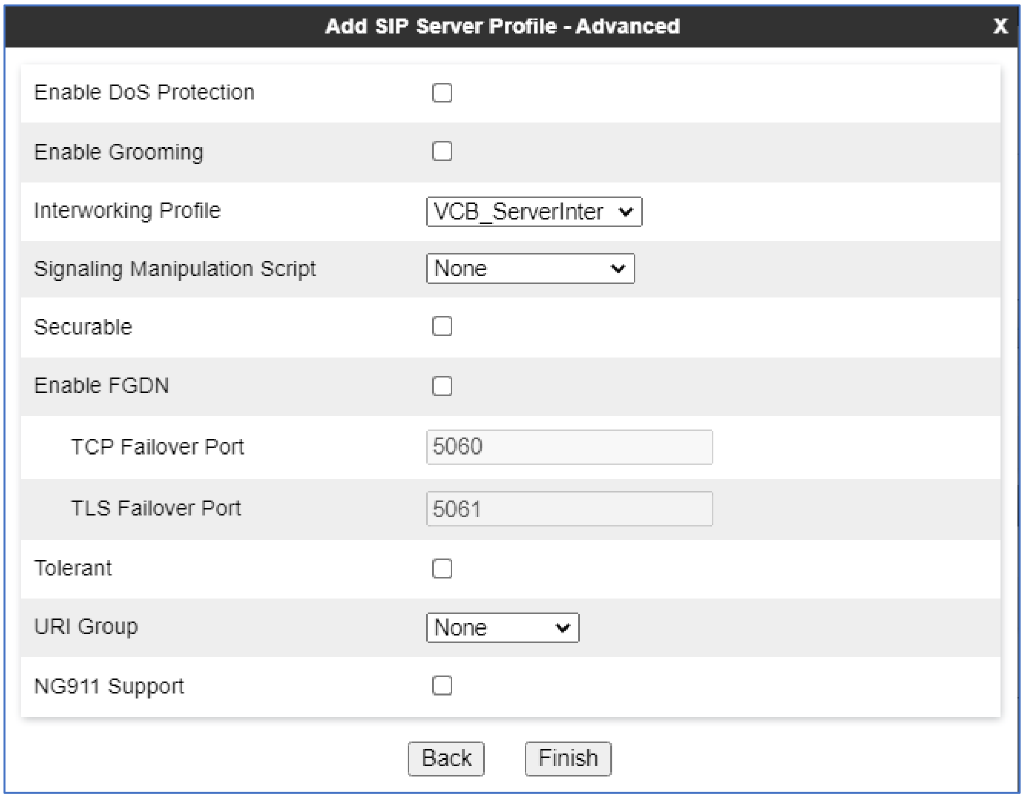


On the **Edit SIP Server Profile – General** window:

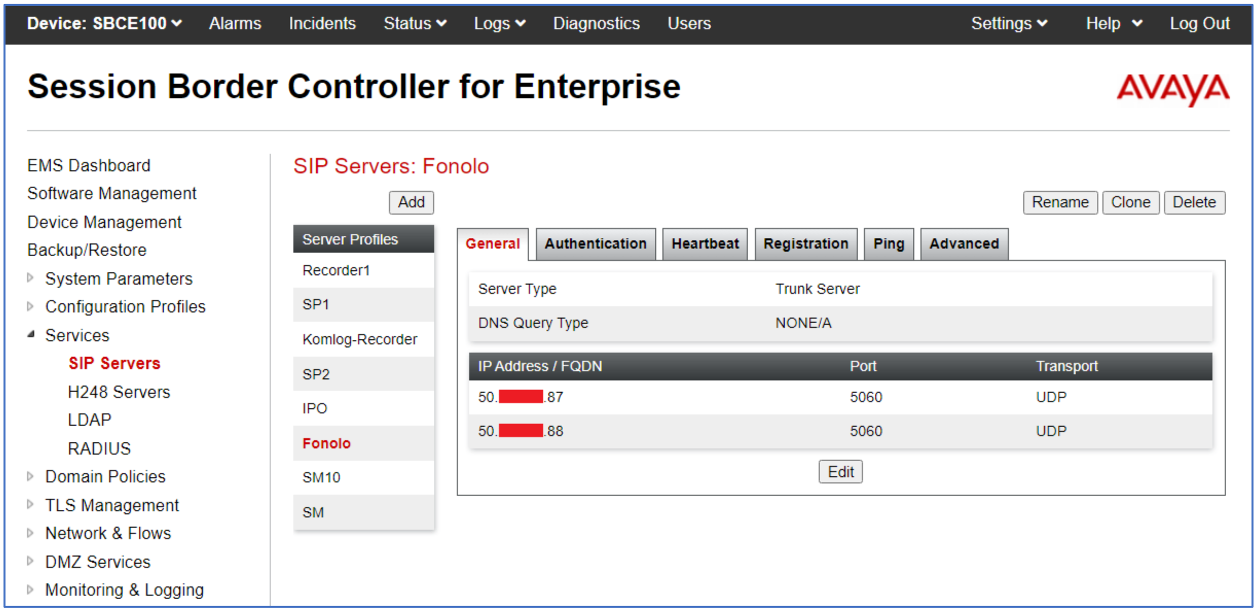
- **Server Type**: Select **Trunk Server**.
- Click on **Add** and under **IP Address / FQDN** enter: two server IP address of VCB appliance as shown below.
- **Port**: **5060**.
- **Transports**: Select **UDP**.
- Click **Next**.



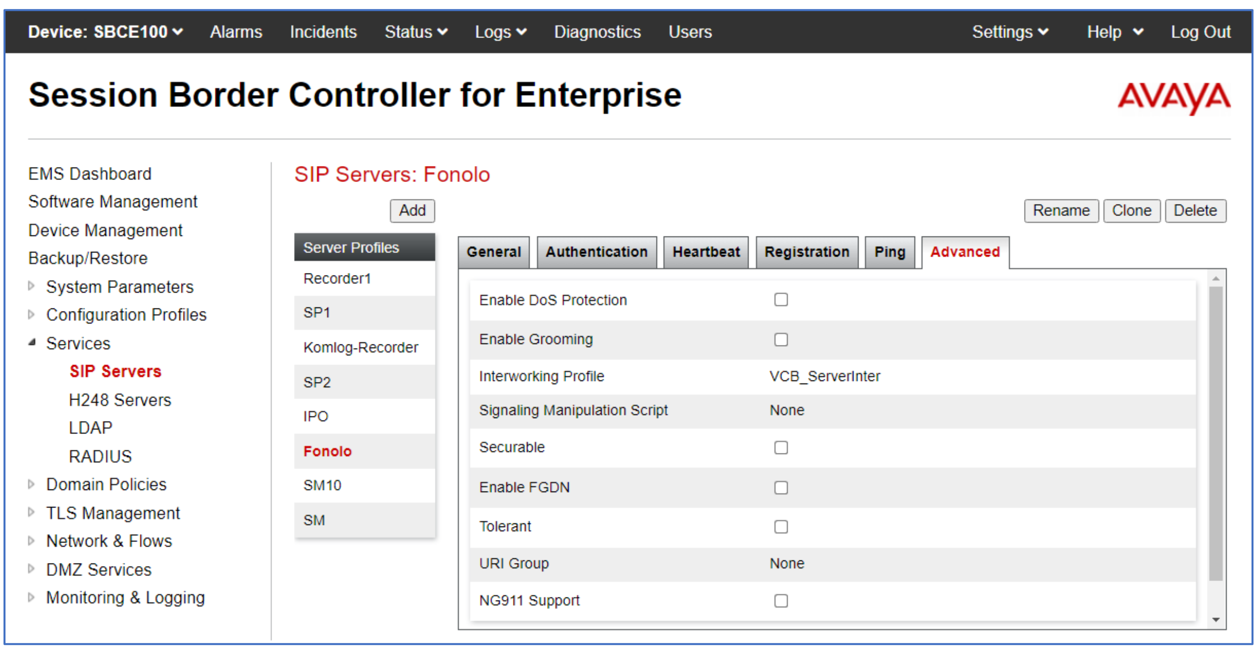
- Click **Next** until the **Add SIP Server Profile - Advanced** tab is reached (not shown).
- On the **Add SIP Server Profile - Advanced** tab:
- Verify that **Enable Grooming** is unchecked.
- Select **VCB_ServerInter** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.



The following screen capture shows the **General** tab of the newly created **Fonolo** SIP Server Configuration Profile.



The following screen capture shows the **Advanced** tab of the newly created **Fonolo** SIP Server Configuration Profile.



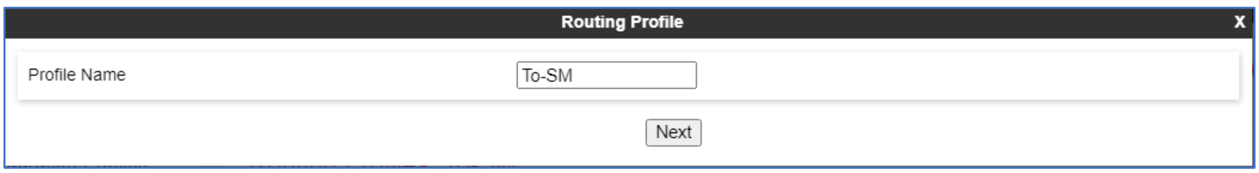
7.3.4. Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Two Routing profiles were created, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls to Fonolo VCB.

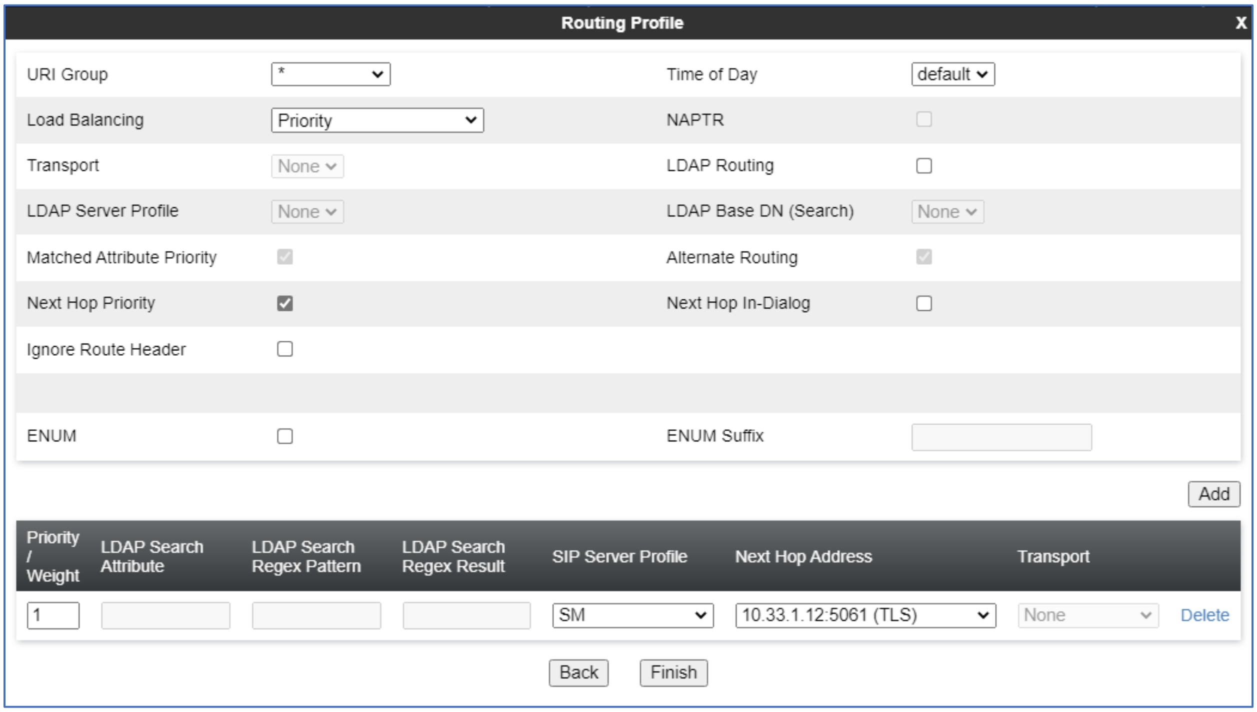
To create the inbound route, from the **Configuration Profiles** menu on the left-hand side (not shown):

- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **To-SM**.
- Click **Next**.

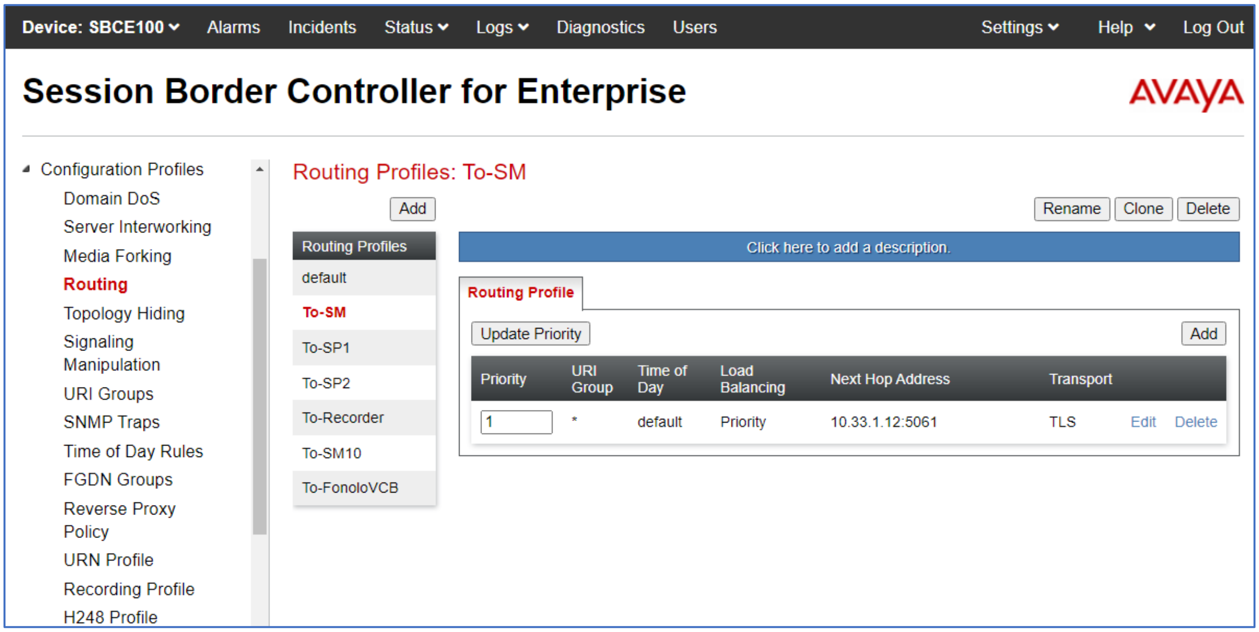


On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: **1**
- **SIP Server Profile**: Select **SM**.
- **Next Hop Address** is populated automatically with **10.33.1.12:5061 (TLS)** (Session Manager IP address, Port and Transport).
- Click **Finish**.

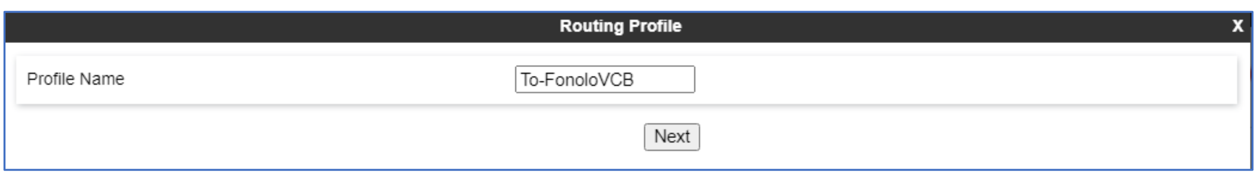


The following screen shows the newly created **To-SM** Routing Profile.



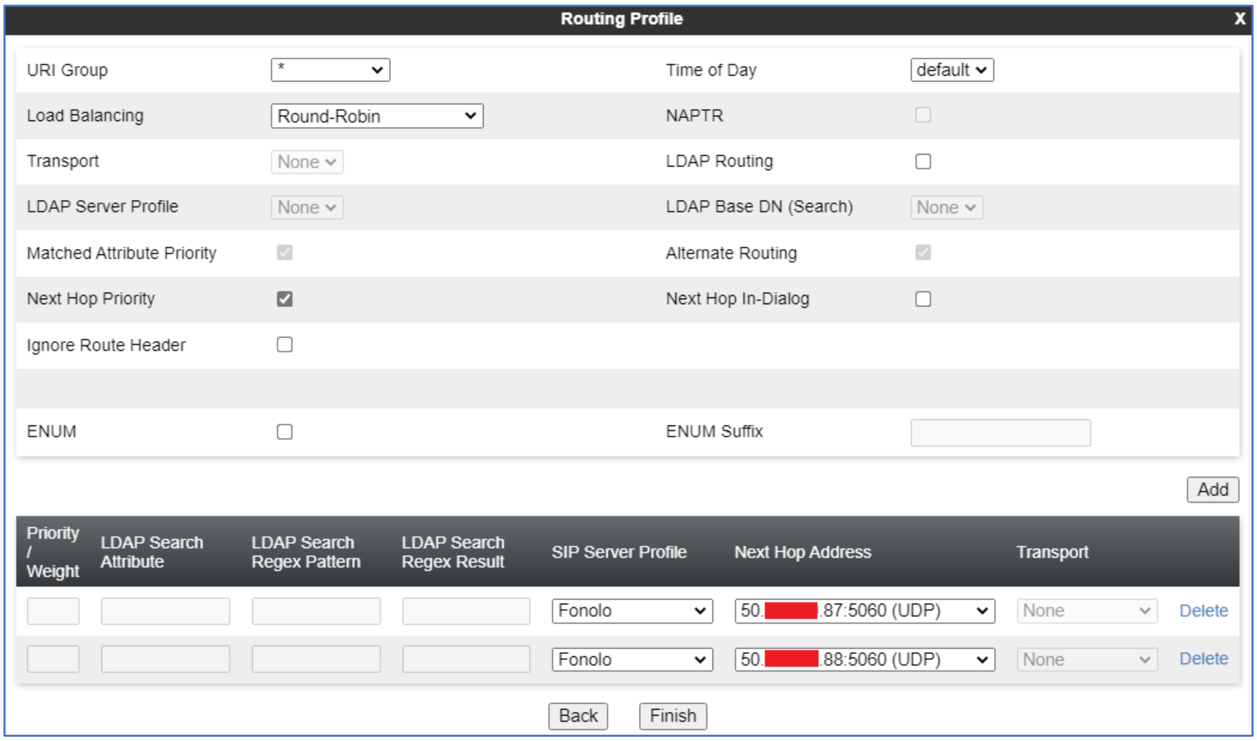
Similarly, for the outbound route to the Fonolo VCB appliance:

- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **To-FonoloVCB**.
- Click **Next**.

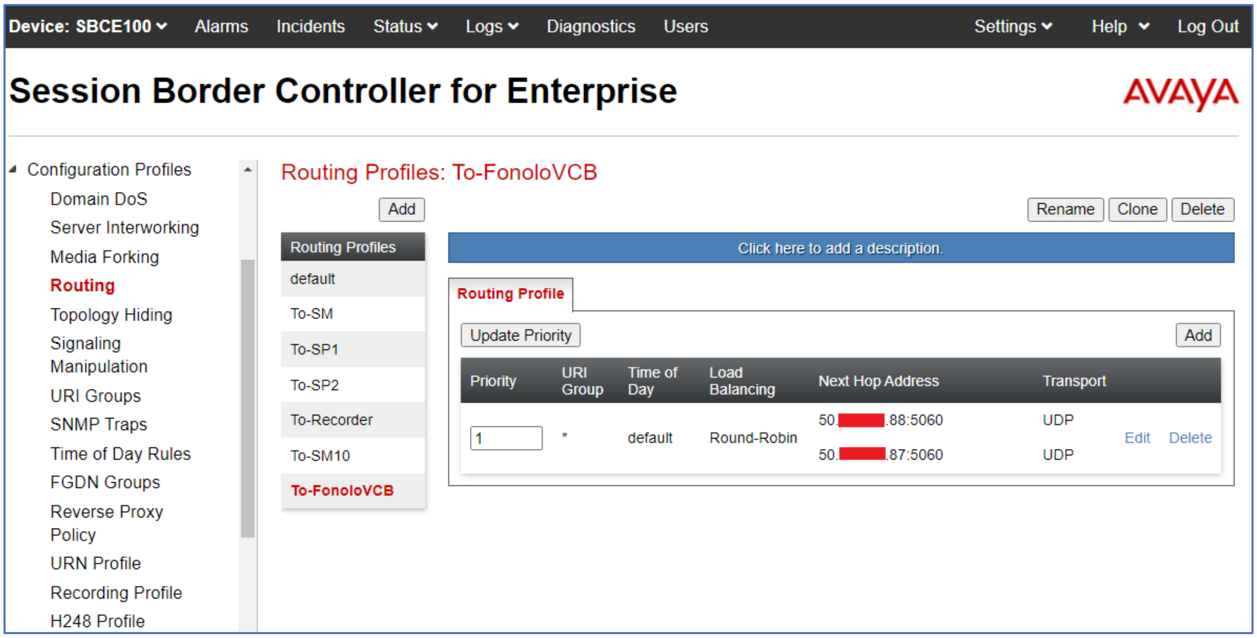


On the Routing Profile screen complete the following:

- **Load Balancing**: Select **Round-Robin**.
- Click on the **Add** button to add a **Next-Hop Address**.
- **SIP Server Profile**: Select two VCB appliances as shown below.
- The **Next Hop Address:** select the IP address of VCB appliances.
- Click **Finish**.



The following screen capture shows the newly created **To-FonoloVCB** Routing Profile.



7.3.5. Topology Hiding

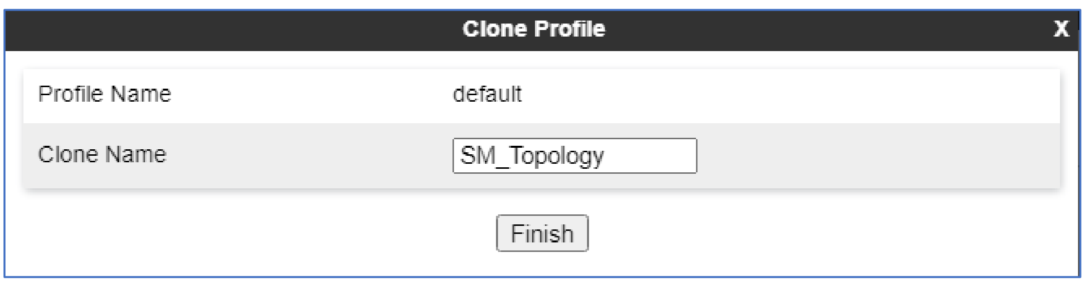
Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Session Manager and the SIP trunk service provider, allowing the call to be accepted in each case.

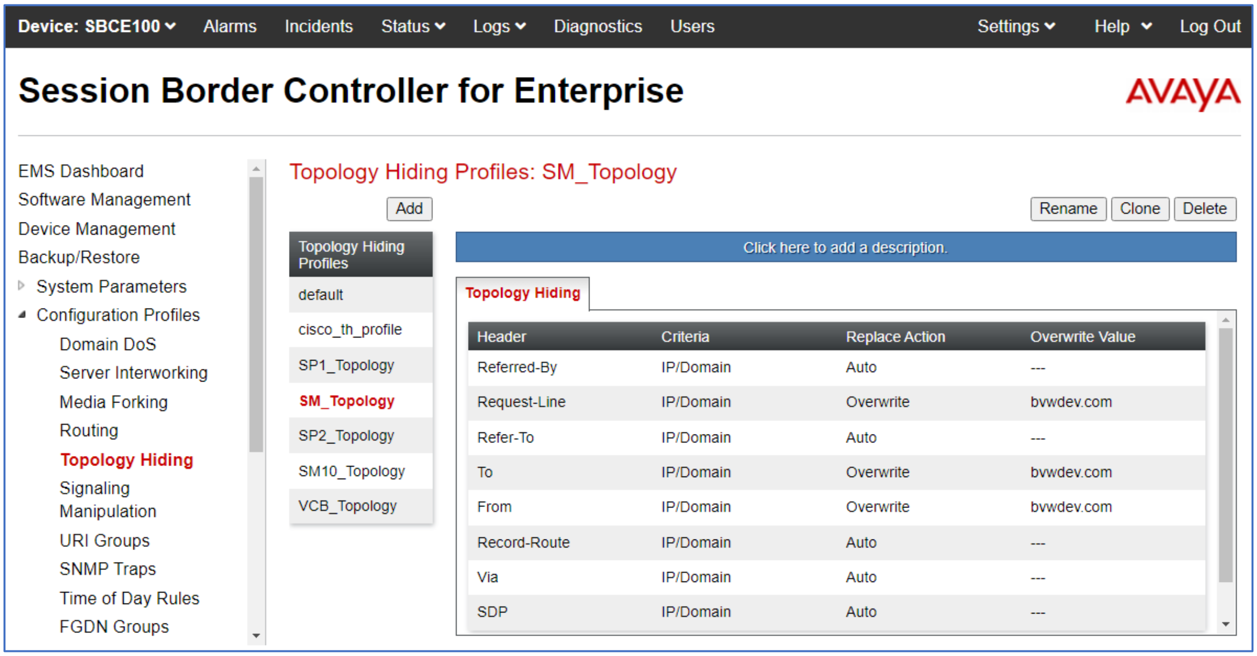
For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Configuration Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone Profile** (not shown).
- Enter the **Profile Name**: **SM_Topology**.
- Click **Finish**.

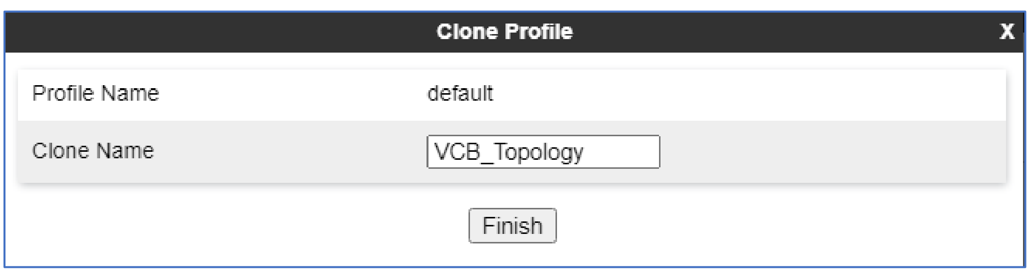


The following screen capture shows the newly added **SM_Topology** Topology Hiding Profile. Note that for Session Manager there are the **Request-Line**, **From**, and **To** headers overwritten with the sip domain "**bvwdev.com**" as defined in Session Manager.



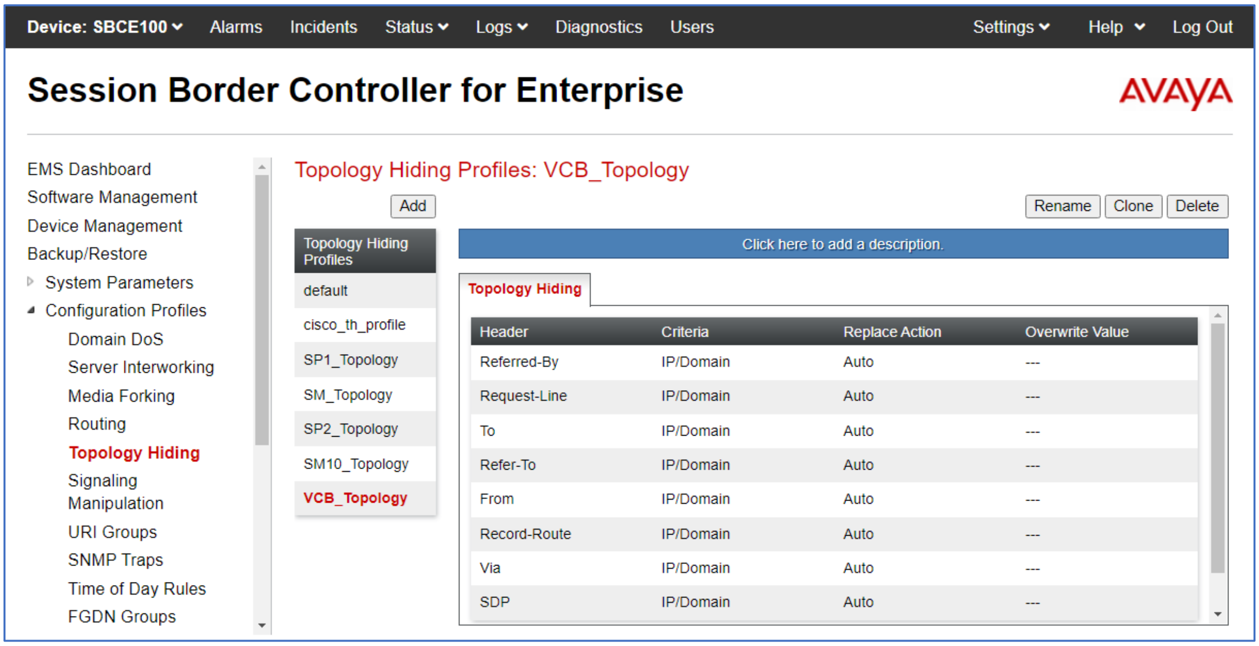
To add the Topology Hiding Profile in the Fonolo VCB direction, select **Topology Hiding** from the **Configuration Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone Profile** (not shown).
- Enter the **Profile Name**: **VCB_Topology**.
- Click **Finish**.



- Click **Edit** on the newly created **VCB_Topology** Topology Hiding profile and leave all the fields as default.
- Click **Finish**.

The following screen capture shows the newly added **VCB_Topology** Topology Hiding Profile.



7.4. Domain Policies

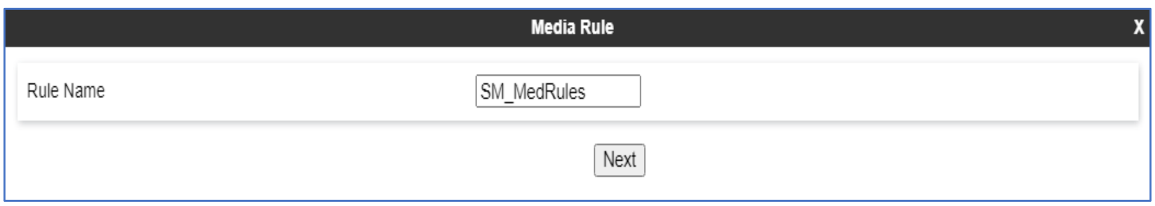
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.4.1. Media Rules

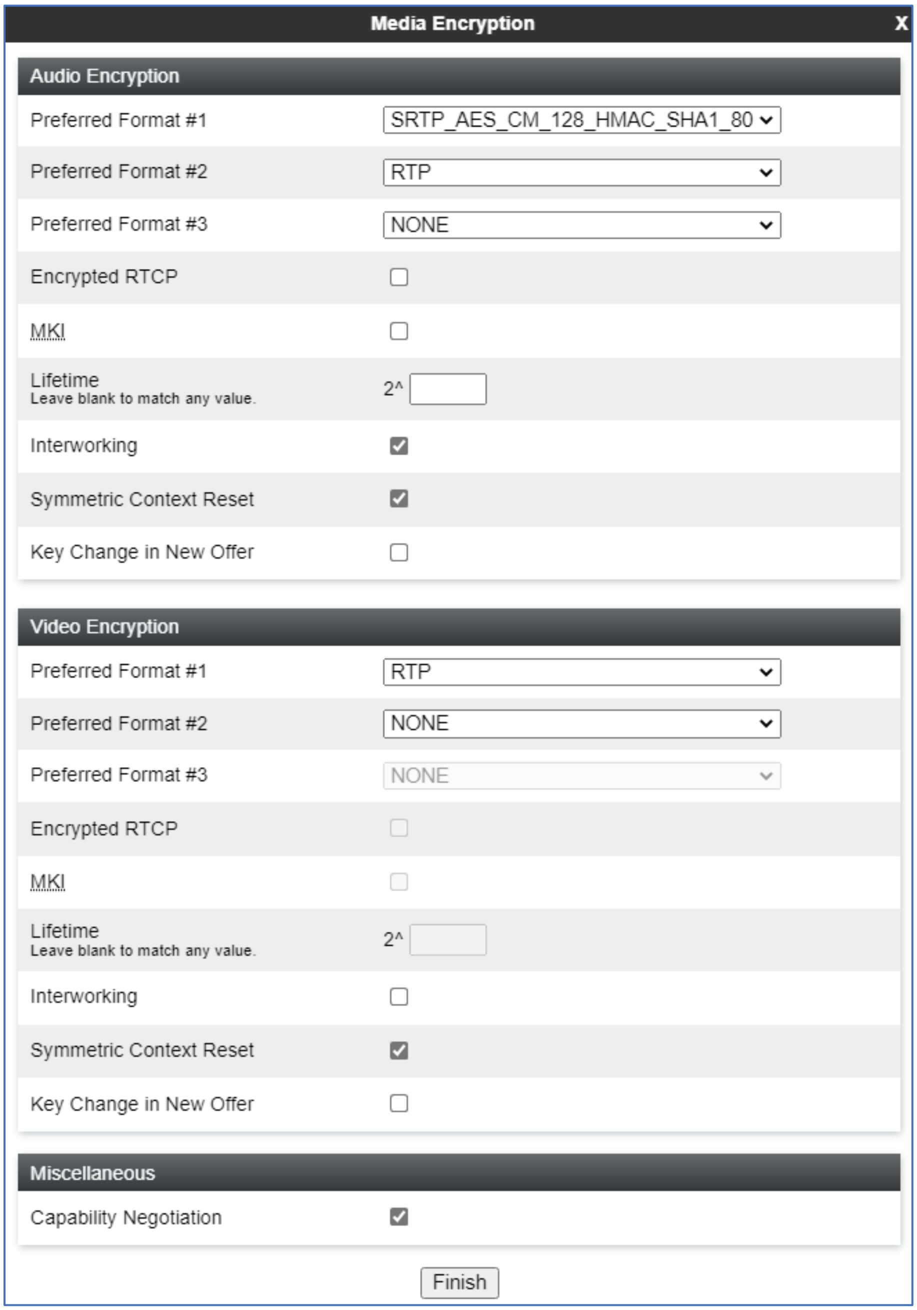
Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test one media rule was created toward Session Manager, the existing **default-low-med** media rule was used toward the Fonolo VCB.

To add a media rule in the Session Manager direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

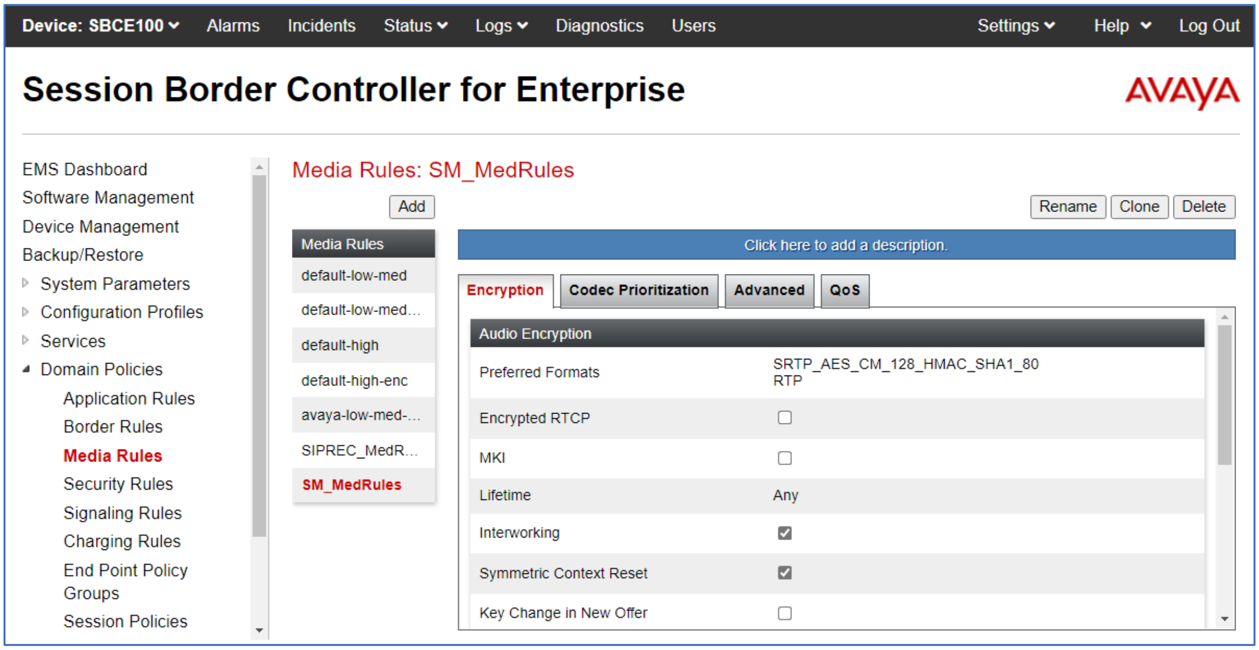
- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter **SM_MedRules**.
- Click **Next**.



- Under Audio Encryption, **Preferred Format #1**, select **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption**,** uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Under Miscellaneous check **Capability Negotiation**.
- Click **Next** (not shown).



- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown). The following screen capture shows the newly created **SM_MedRules** Media Rule.

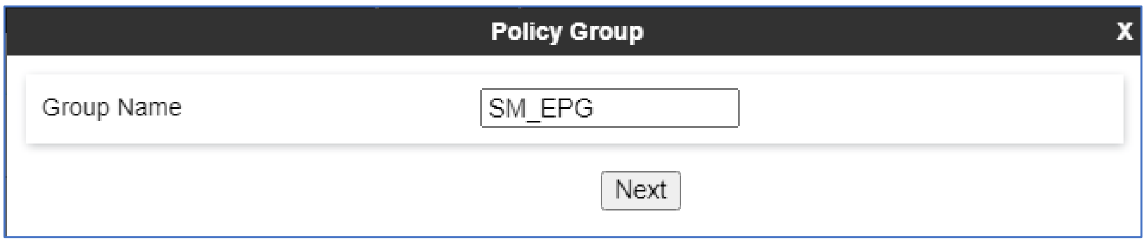


7.4.2. End Point Policy Groups

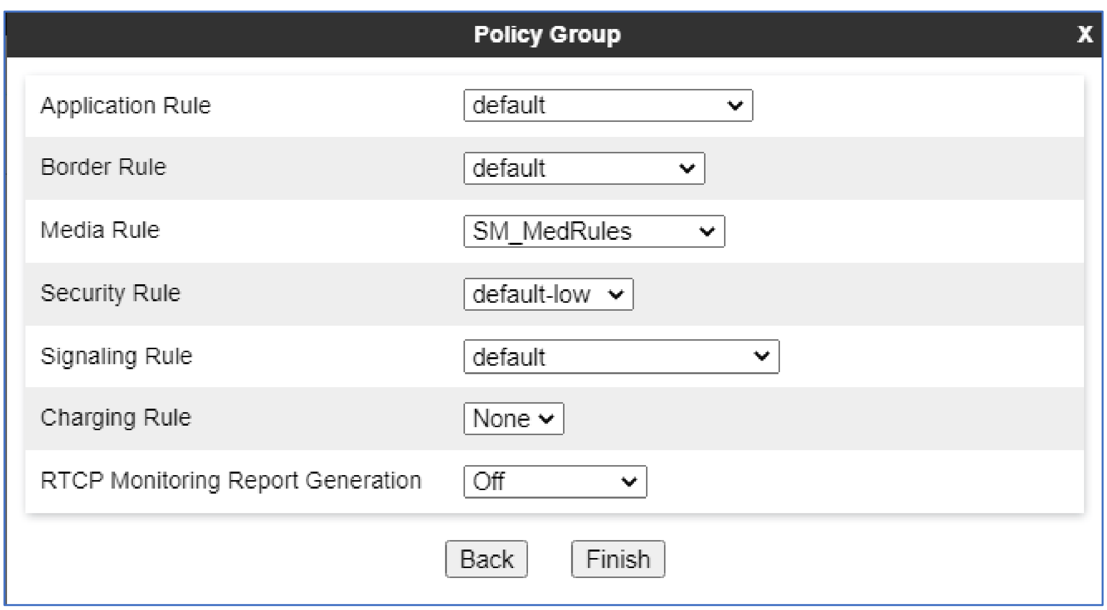
End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups** (not shown).

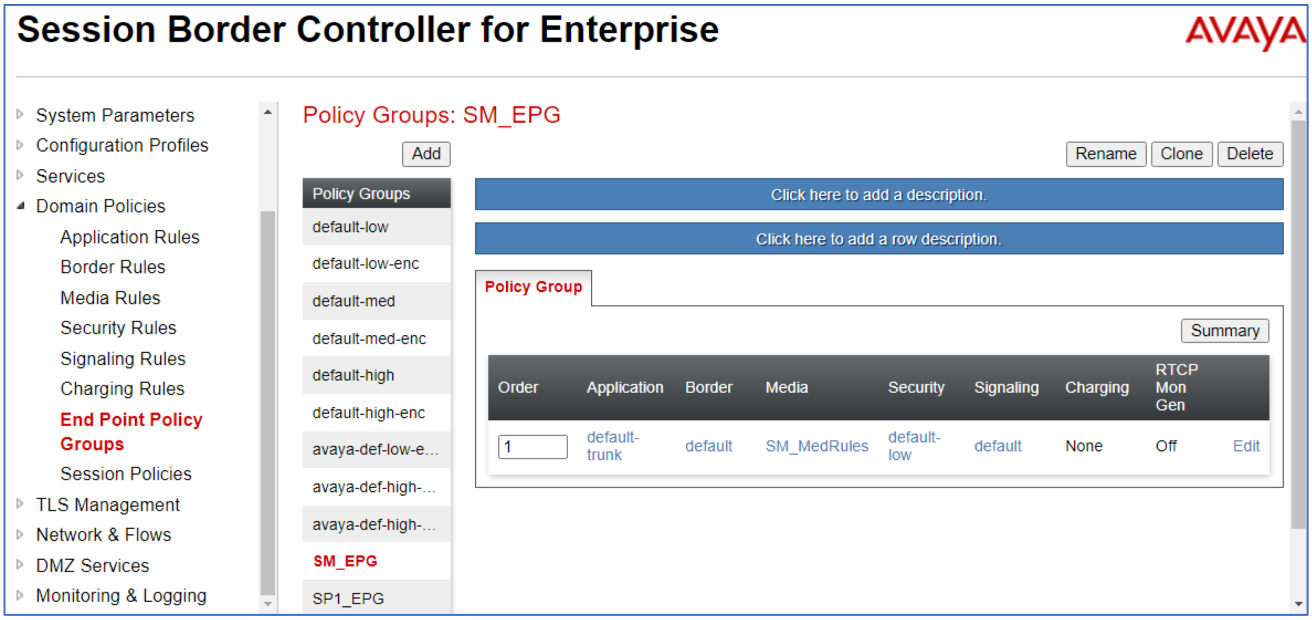
- Click on the **Add** button to add a new policy group (not shown).
- **Group Name**: **SM_EPG**.
- Click **Next**.



- **Application Rule**: select **default**.
- **Border Rule**: select **default**.
- **Media Rule**: select **SM_MedRules** (**Section 7.4.1**).
- **Security Rule**: select **default-low**.
- **Signaling Rule**: select **default**.
- Click **Finish**.



The following screen capture shows the newly created **SM_EPG** End Point Policy Group. In the compliance test, the default endpoint policy group was used for the Fonolo VCB.

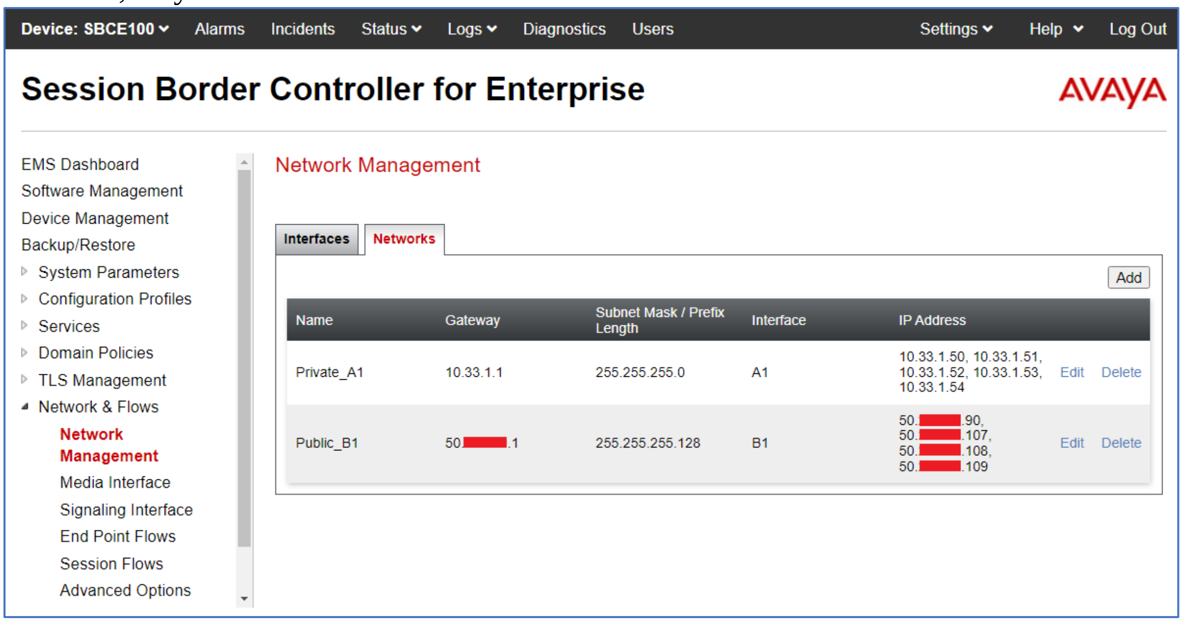


7.5. Network & Flows Settings

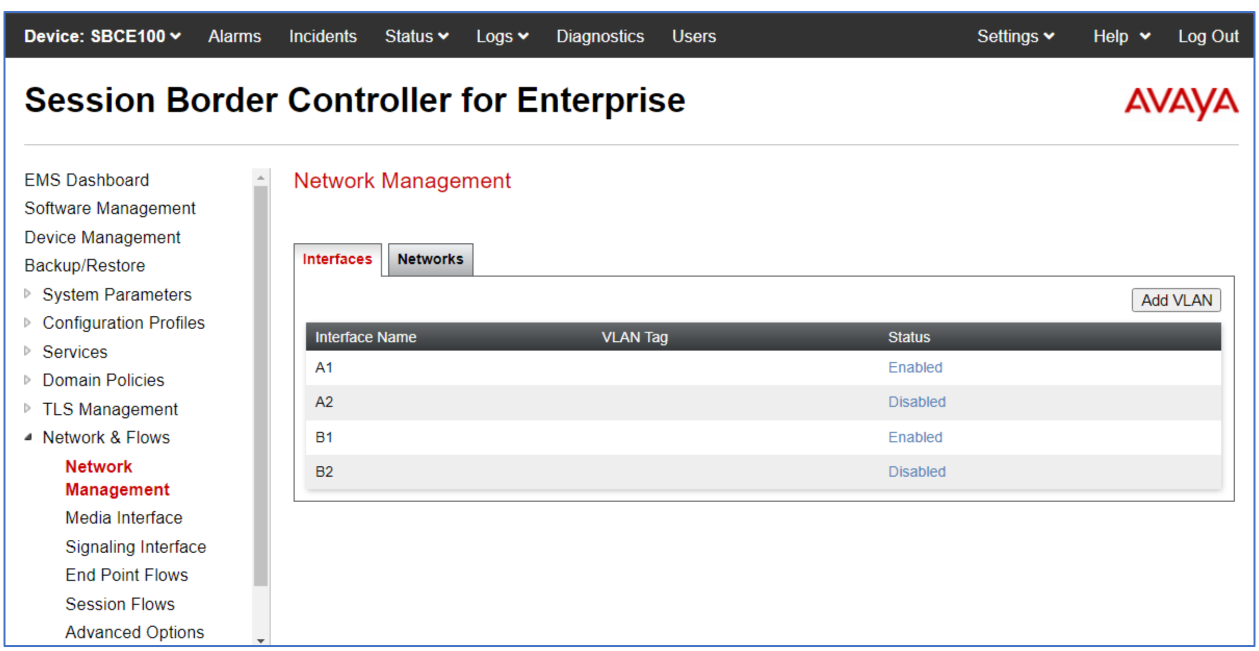
The **Network & Flows** settings allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

7.5.1. Network Management

The network information should have been previously completed. To verify the network configuration, from the **Network & Flows** on the left hand side, select **Network Management**. Select the **Networks** tab. In the event that changes need to be made to the network configuration information, they can be entered here.



On the **Interfaces** tab, click the **Status** control for interfaces **A1** and **B1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **Disabled**, so it is important to perform this step, or the Avaya SBCE will not be able to communicate on any of its interfaces.

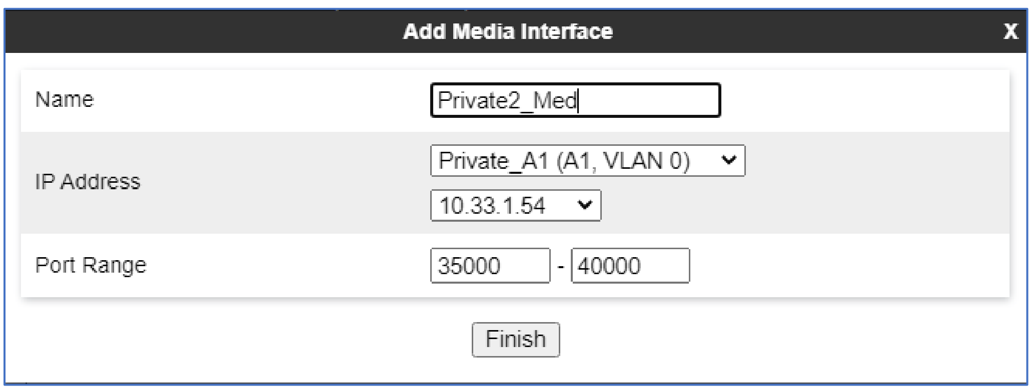


7.5.2. Media Interface

Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which the SBCE will accept media from the connected server. Create a SIP Media Interface for both the inside and outside IP interfaces. On the Private and Public interfaces of the Avaya SBCE, the port range 35000 to 40000 was used.

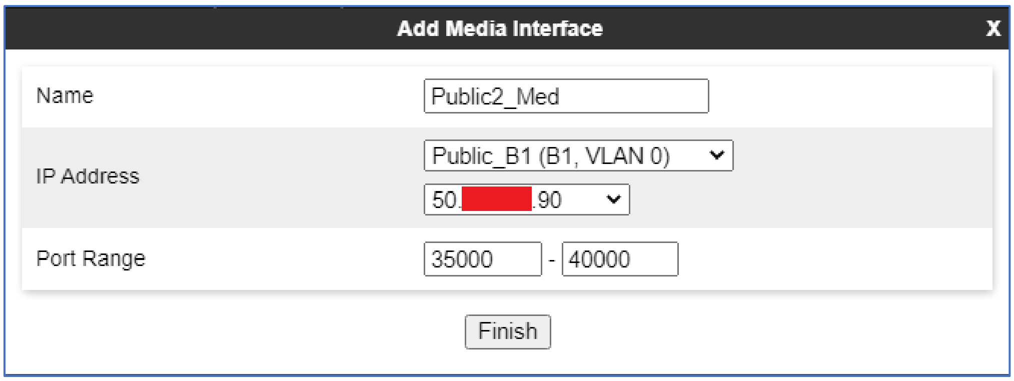
From the **Network & Flows** menu on the left-hand side, select **Media Interface** (not shown).

- Select **Add** in the **Media Interface** area (not shown).
- **Name**: **Private2_Med**.
- Under **IP Address** select: **Network_A1 (A1, VLAN 0)**
- Select **IP Address**: **10.33.1.54** (Inside IP Address of the Avaya SBCE, toward SM).
- **Port Range**: **35000-40000**.
- Click **Finish**.

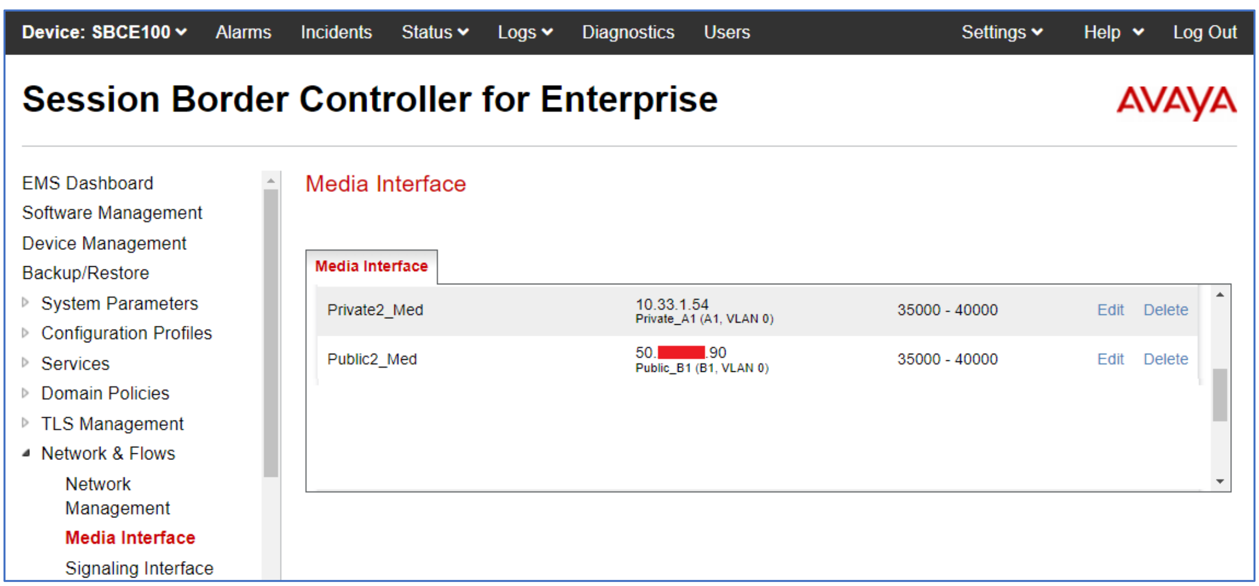


Select **Add** in the **Media Interface** area (not shown)**.**

- **Name**: **Public_med**.
- Under **IP Address** select: **Network_B1 (B1, VLAN 0)**
- Select **IP Address**: **50.207.80.90** (Outside IP Address of the Avaya SBCE, toward the VCB).
- **Port Range**: **35000-40000**.
- Click **Finish**.



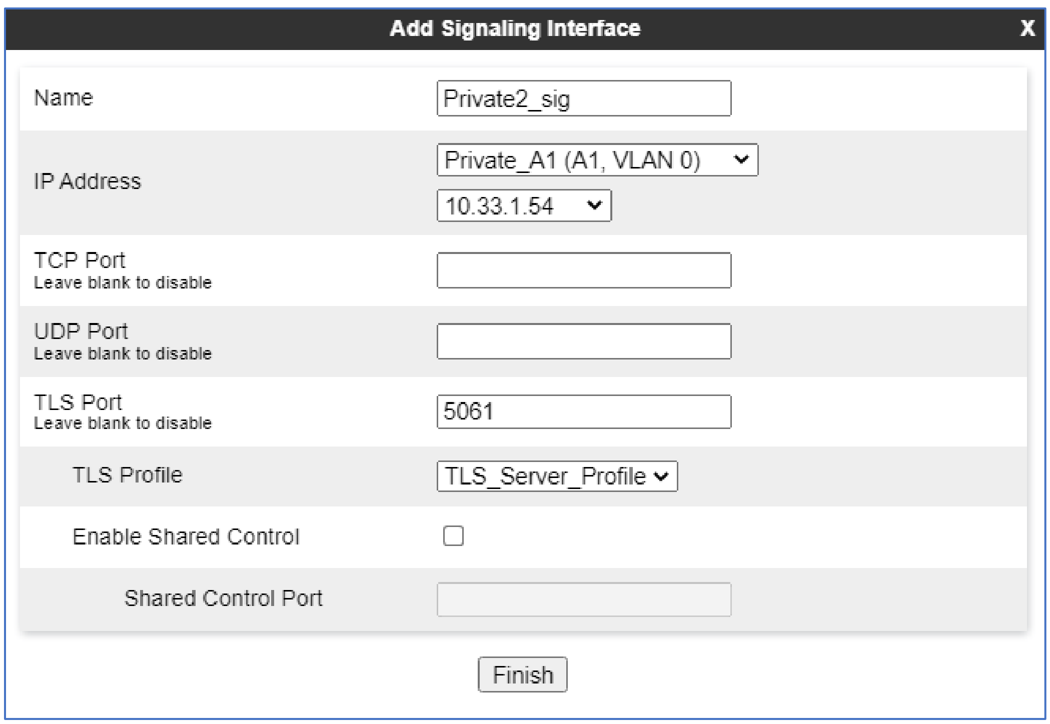
The following screen capture shows the newly created Media Interfaces.



7.5.3. Signaling Interface

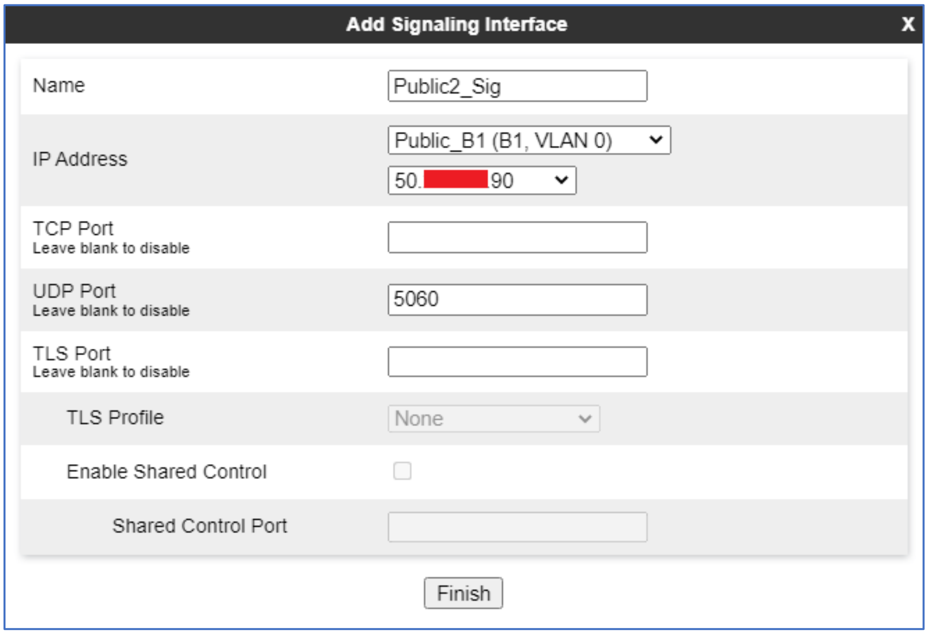
To create the Signaling Interface toward Session Manager, from the **Network & Flows** menu on the left hand side, select **Signaling Interface** (not shown).

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name**: **Private2_Sig**.
- Under **IP Address** select: **Network_A1 (A1, VLAN 0)**
- Select **IP Address**: **10.33.1.54** (Inside IP Address of the Avaya SBCE, toward Session Manager).
- **TLS Port**: **5061**.
- Select a **TLS Profile**. Note that the TLS profile was previously configured and not mentioned in this application notes.
- Click **Finish**.

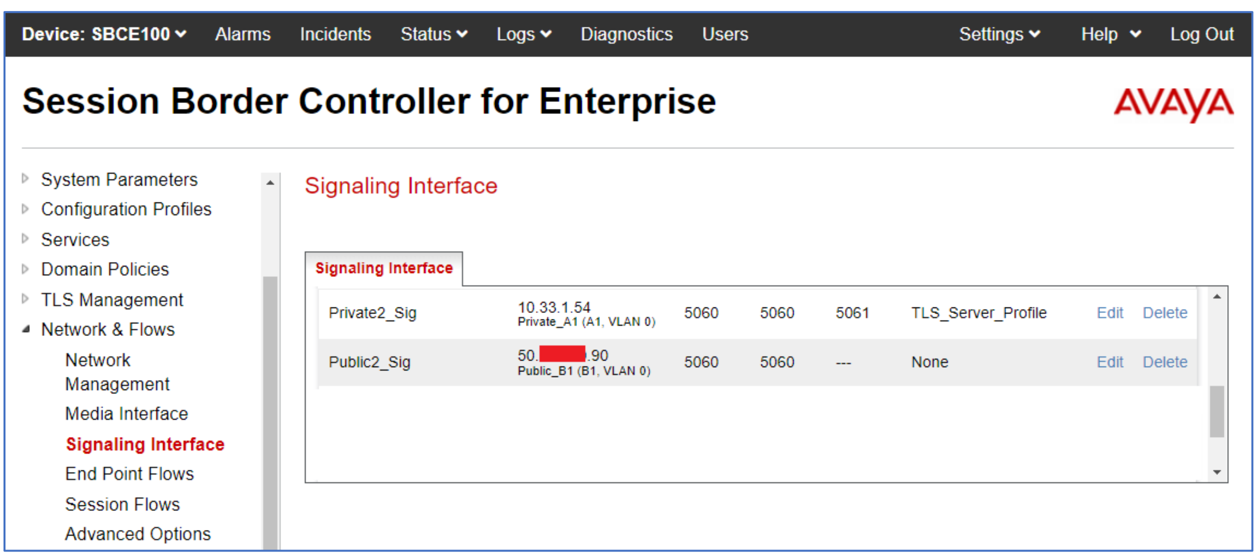


Repeat the same procedure above to add another signaling interface of Avaya SBCE toward the Fonolo VCB appliance.

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name**: **Public2_Sig**.
- Under **IP Address** select: **Network_B1 (B1, VLAN 0)**
- Select **IP Address**: **50.xxx.xxx.90** (outside or public IP Address of the Avaya SBCE, toward the VCB appliance).
- **UDP Port**: **5060**.
- Click **Finish**.

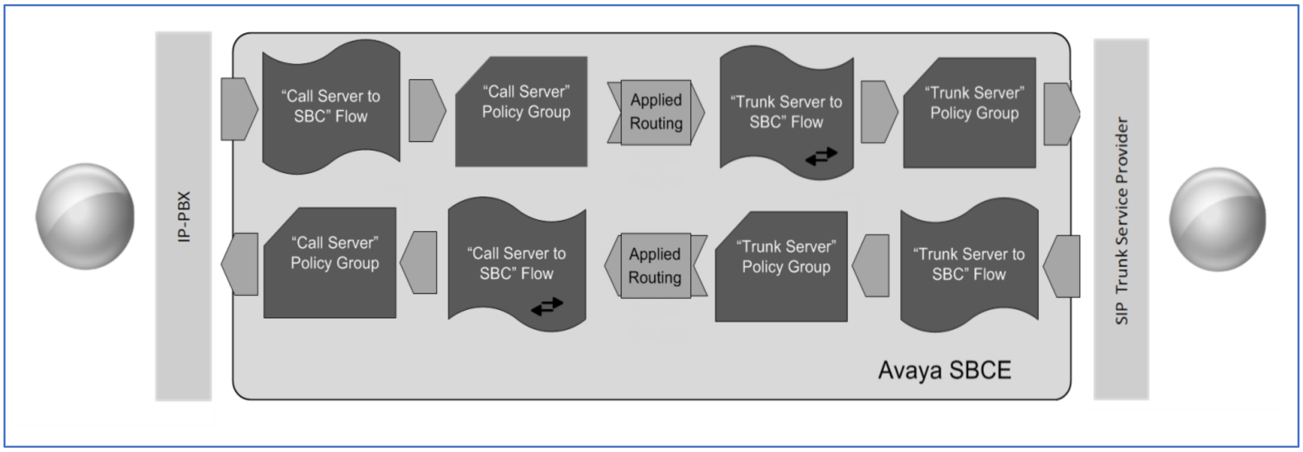


The following screen capture shows the newly created Signaling Interfaces.



7.5.4. End Point Flows

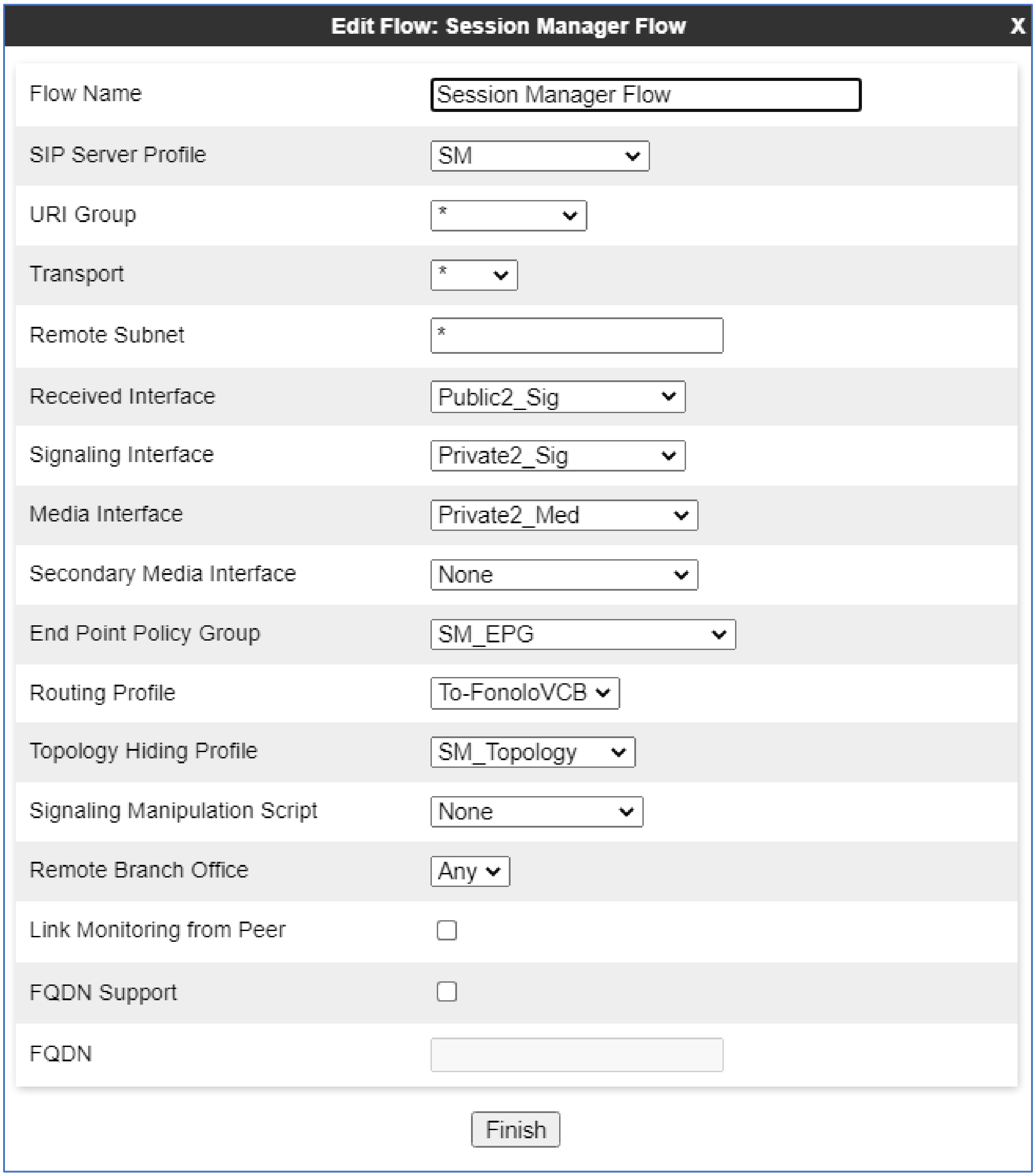
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing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



The **End-Point Flows** define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward Session Manager, from the **Network & Flows** menu, select **End Point Flows** (not shown**)**, then the **Server Flows** tab. Click **Add** (not shown).

- **Name**: **Session Manager Flow**.
- **Server Configuration: SM**.
- URI Group: *
- **Transport**: *
- **Remote Subnet**: *
- **Received Interface**: **Public2_Sig**.
- **Signaling Interface**: **Private2_Sig**.
- **Media Interface**: **Private2_Med**.
- **Secondary Media Interface**: **None**.
- **End Point Policy Group**: **SM_EPG**.
- **Routing Profile**: **To-FonoloVCB**.
- **Topology Hiding Profile**: **SM_Topology**.
- Click **Finish**.



Edit Flow: Session Manager Flow

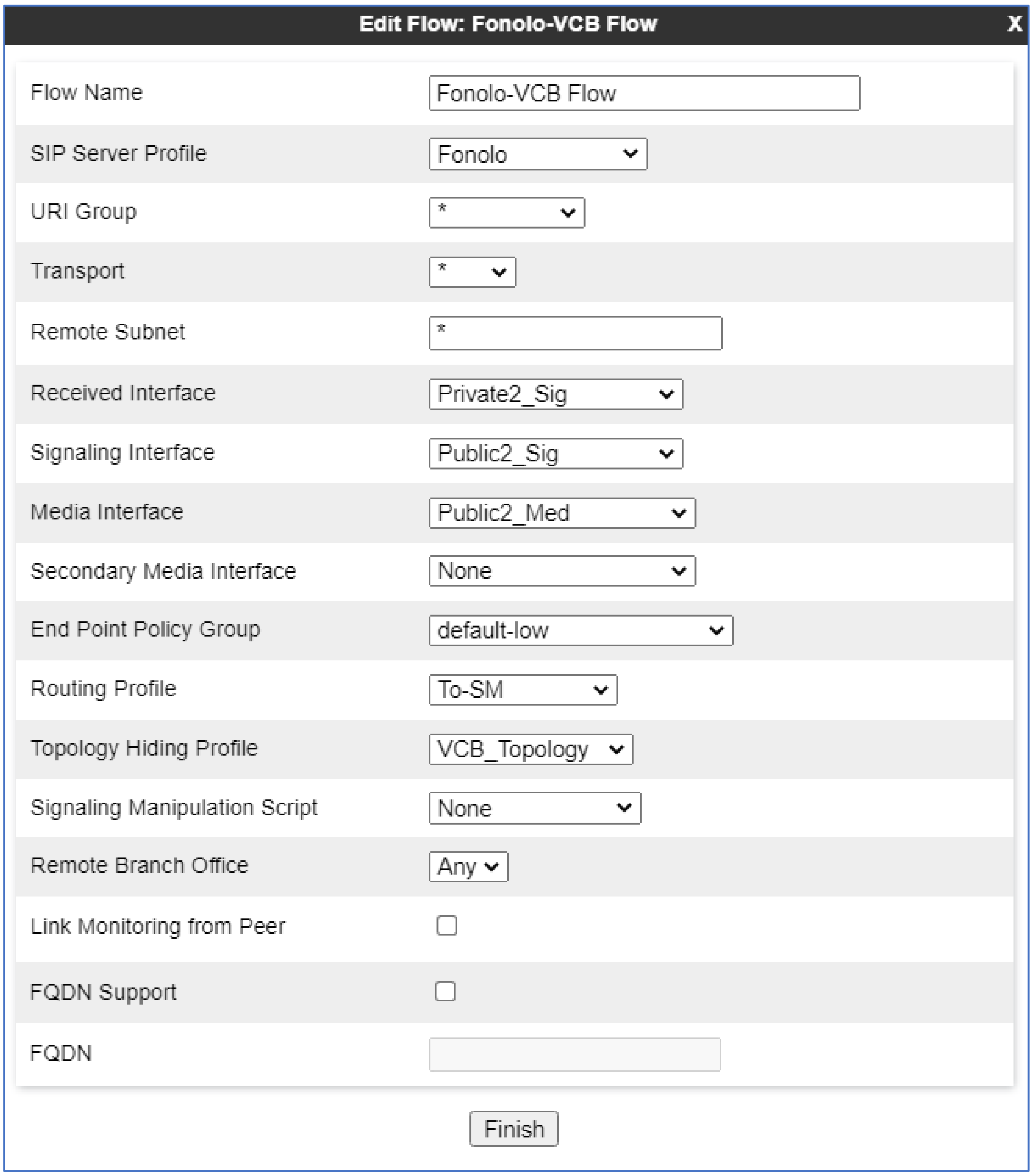
Flow Name	Session Manager Flow
SIP Server Profile	SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public2_Sig
Signaling Interface	Private2_Sig
Media Interface	Private2_Med
Secondary Media Interface	None
End Point Policy Group	SM_EPG
Routing Profile	To-FonoloVCB
Topology Hiding Profile	SM_Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☐
FQDN Support	☐
FQDN	

Finish

To create the call flow toward the Fonolo VCB, click **Add** (not shown).

- **Name**: **Fonolo VCB Flow**.
- **Server Configuration**: **Fonolo**.
- **URI Group**: *****
- **Transport**: *****
- **Remote Subnet: ***

- **Received Interface**: **Private2_Sig**.
- **Signaling Interface**: **Public2_Sig**.
- **Media Interface**: **Public2_Med**.
- **Secondary Media Interface**: **None**.
- **End Point Policy Group**: **default_low**.
- **Routing Profile**: **To-SM**.
- **Topology Hiding Profile**: **VCB_Topology**.
- Click **Finish**.



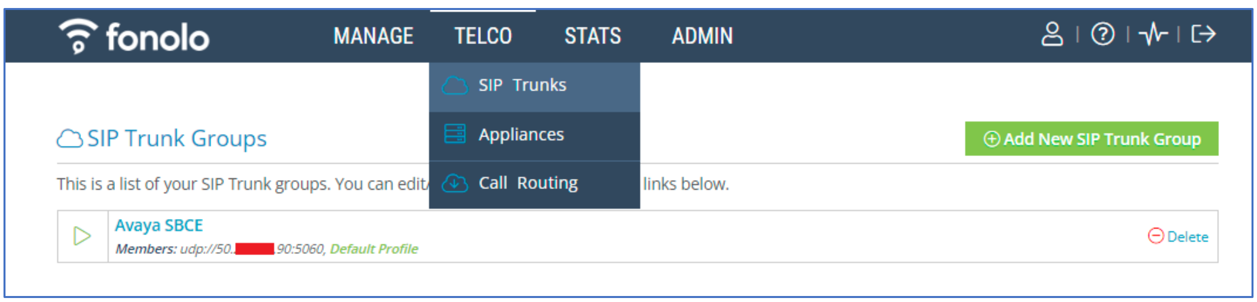
8. Configure Fonolo Voice Call-Backs

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 **Add New SIP Trunk Group** at the top of the page. Define a new label to identify this SIP trunk group. During compliance testing **Avaya SBCE** was used as the label. Then select **Add New SIP Trunk** (not shown).



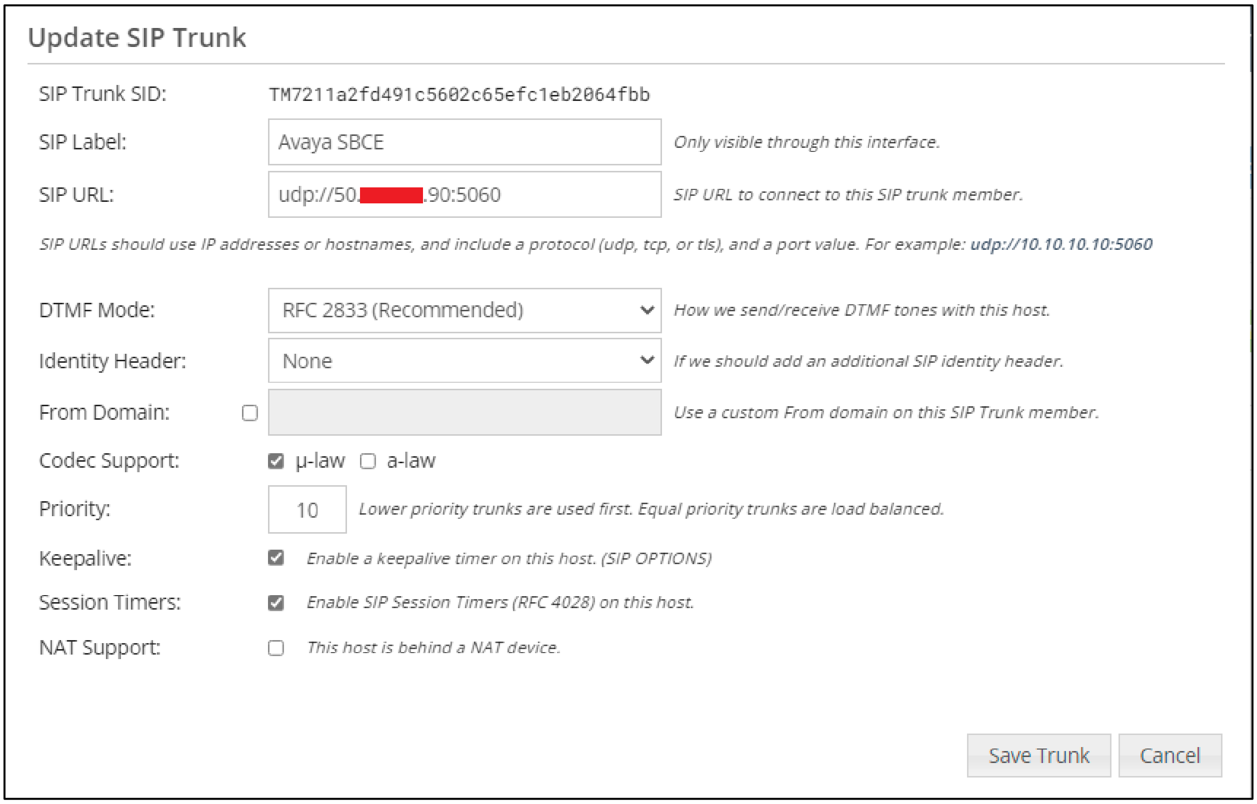
Under the **Members** tab in this new SIP trunk group, click the **Add New Member** button (not shown), and the **Add New SIP Trunk** dialog will appear as shown below.

Under **Add New SIP Trunk**:

- **SIP URL**: The IP address of Avaya SBCE formatted as a fully qualified URL, defining the protocol and SIP port 5060.
- **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. Default is μ-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 platform to perform regular keep-alive using SIP OPTIONS requests, based on the number of seconds defined. Default is disabled.

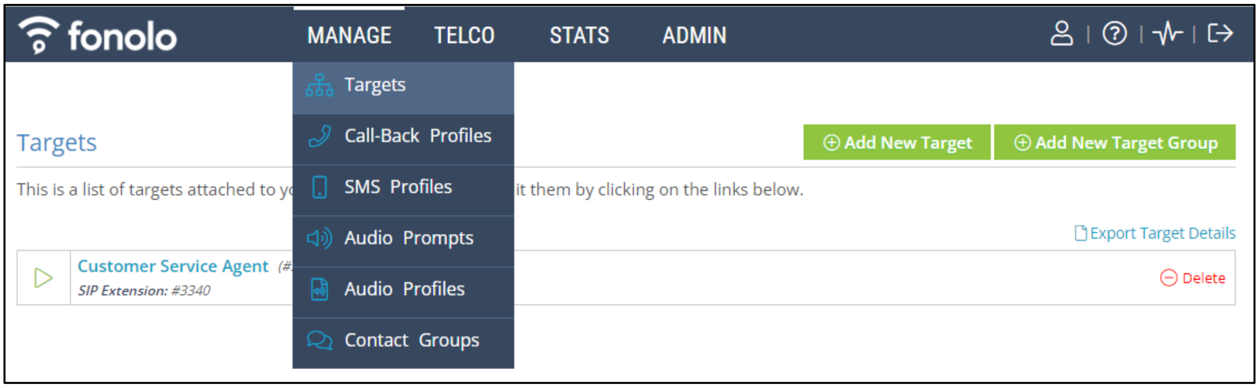
- **Session Timers**: If Fonolo should enable SIP Session Timers (RFC 4028). Default is disabled.
- **NAT Support**: If the SIP trunk group member specified is located behind a NAT (Network Address Translation) device. Fonolo can compensate for the un-reachable RTP data specified in the SDP body of the INVITE request, using symmetric RTP.

Add the public IP address of Avaya SBCE, formatted as a fully qualified URL, defining the protocol and SIP port, then click the **Save Trunk** button. During compliance testing, the protocol **UDP** and port **5060** is used for the SIP service with Avaya SBCE, and the default values for the remaining SIP trunk group member settings.

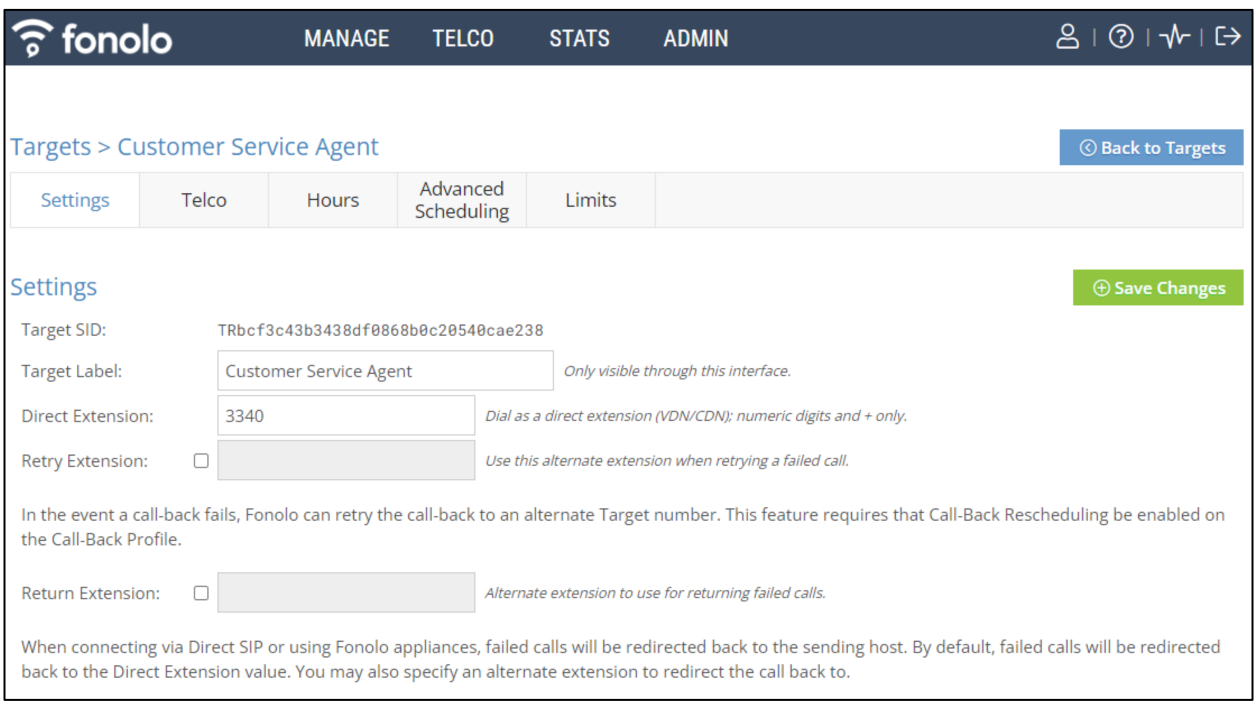


8.2. Adding the Voice Call-Back Endpoint

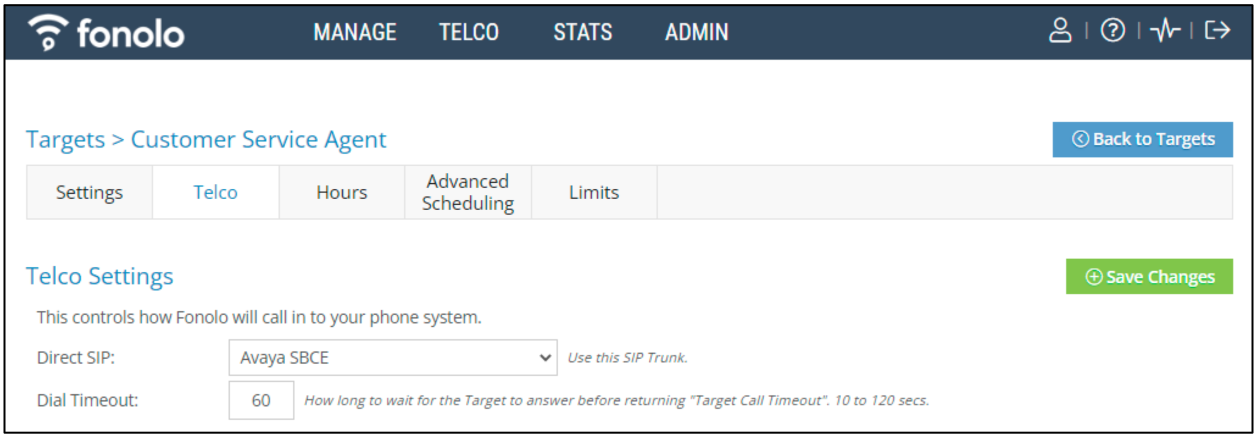
Navigate to **Manage → Targets** and click the **Add New Target** button. Define a new label to identify this new Target. During compliance testing **Customer Service Agent** was used as the **Target Label**. Select the **Dial as SIP Extension** option (not shown) for **Dial Method** and enter the VDN to reach the pertinent skillset via Avaya SBCE in the **Extension** field.



During compliance testing, VDN **3340** was pre-configured in Section 5.16 on Communication Manager which was accessible via Avaya SBCE. Then click on the **Add New Target** button to save this Target.



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 SBCE** SIP trunk, added in **Section 8.1**, and then click the **Save Changes** button.

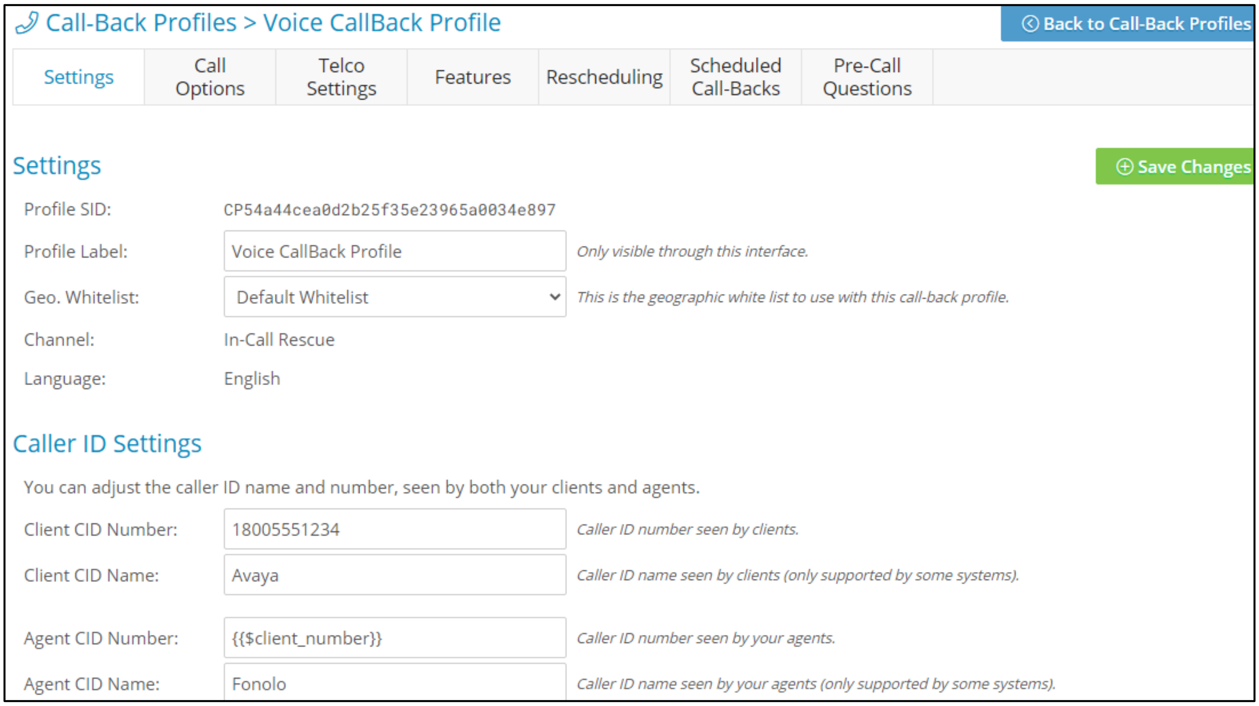


8.3. Adding a New Call-Back Profile

Navigate to **Manage → Call-Back Profiles** and click on the **Add New Profile** button (not shown), and configure the new profile:

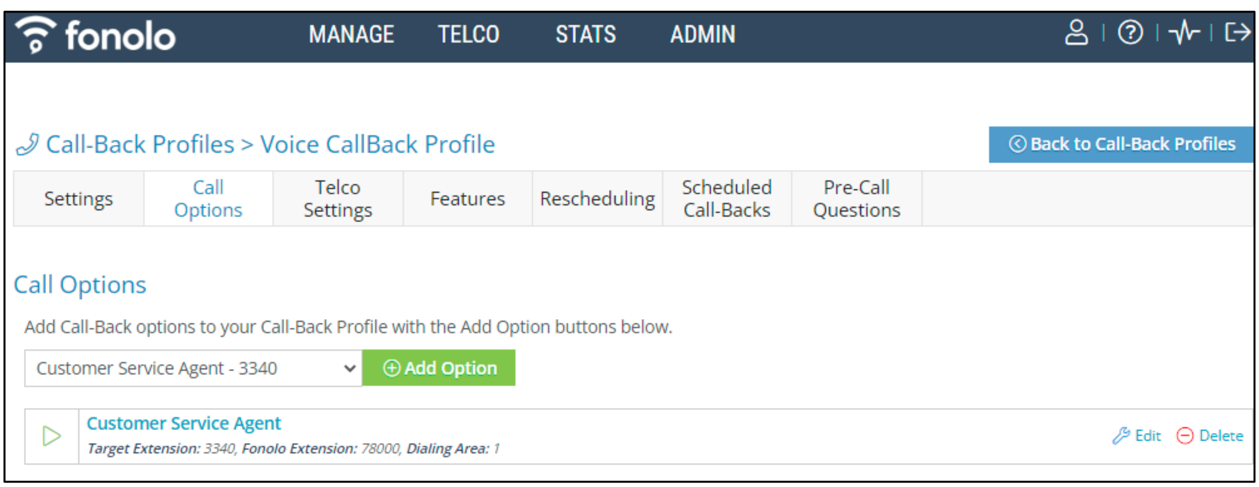
- **Profile Label:** A label to identify this new profile.
- **Geo Whitelist:** A geographic whitelist to use for this new profile.
- **Channel:** Select "In-Call Rescue".
- **Language:** Select the appropriate language for this skill set queue.
- **Client CID Number:** The Caller-ID number the customer 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 New Call-Back Profile** button to add this new profile.

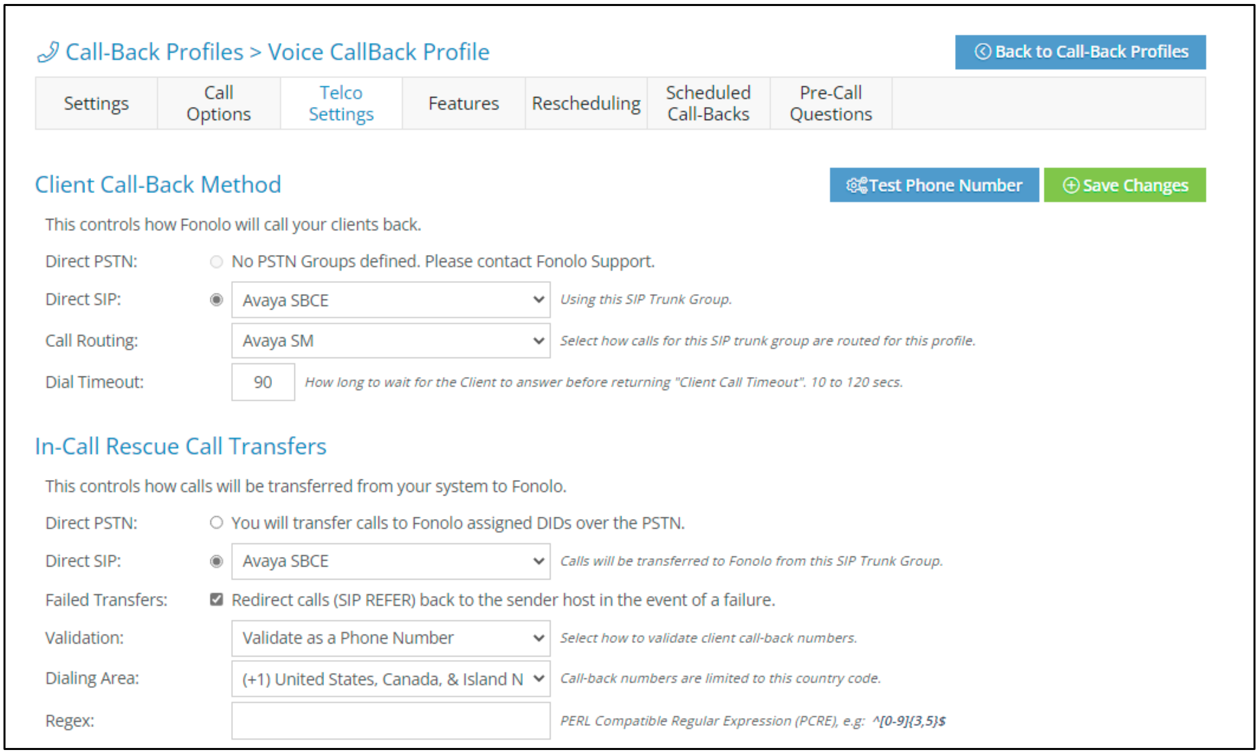


From the **Call Options** section of the new **Call-Back Profile**, select the Target added in **Section** Error! Reference source not found. (from the drop-down menu highlighted below), and click the **Add Option** link to add the VDN value to the section on the left, as shown below, then click the **Save Changes** (not shown) button.

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 SBCE** SIP trunk group created in **Section 8.1** as the **Direct SIP** value under both the **Client Call-Back Method** and the **In-Call Rescue Call 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 VCB system, when a call opts-in for a call-back. During compliance testing, the extension **78000** is configured on the Fonolo system.

9. Verification Steps

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

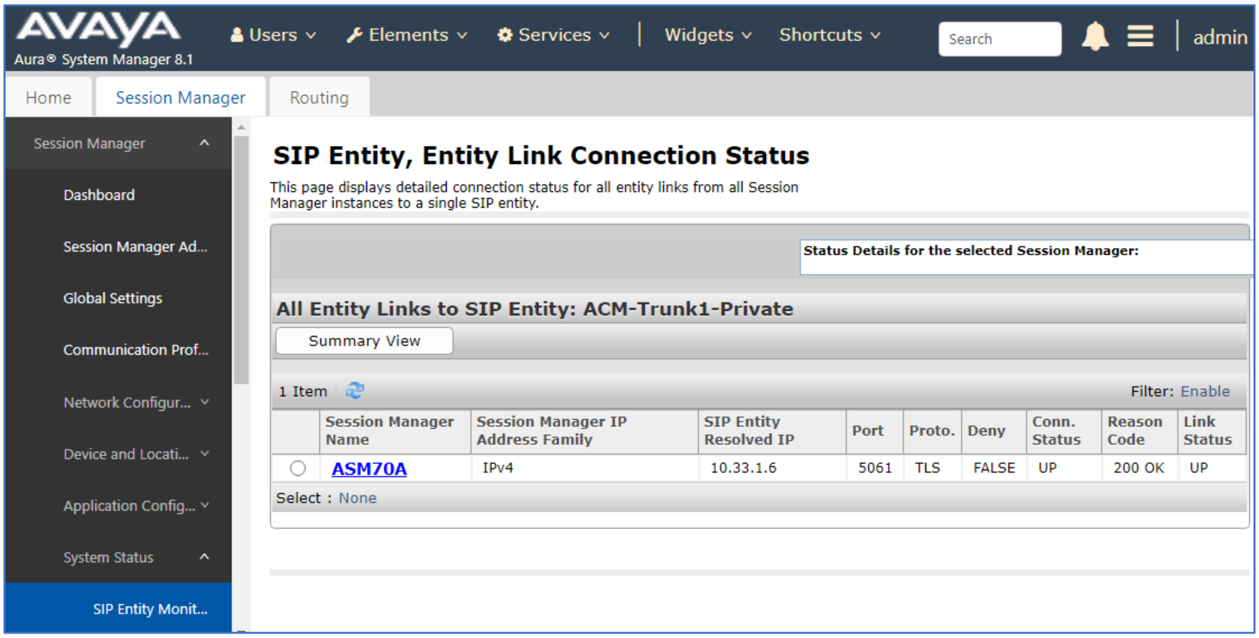
```
status trunk 1

                             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
0001/0007 T000007 in-service/idle    no
0001/0008 T000008 in-service/idle    no
```

The following tests were also performed to verify proper configuration of Fonolo VCB with Communication Manager and Avaya SBCE.

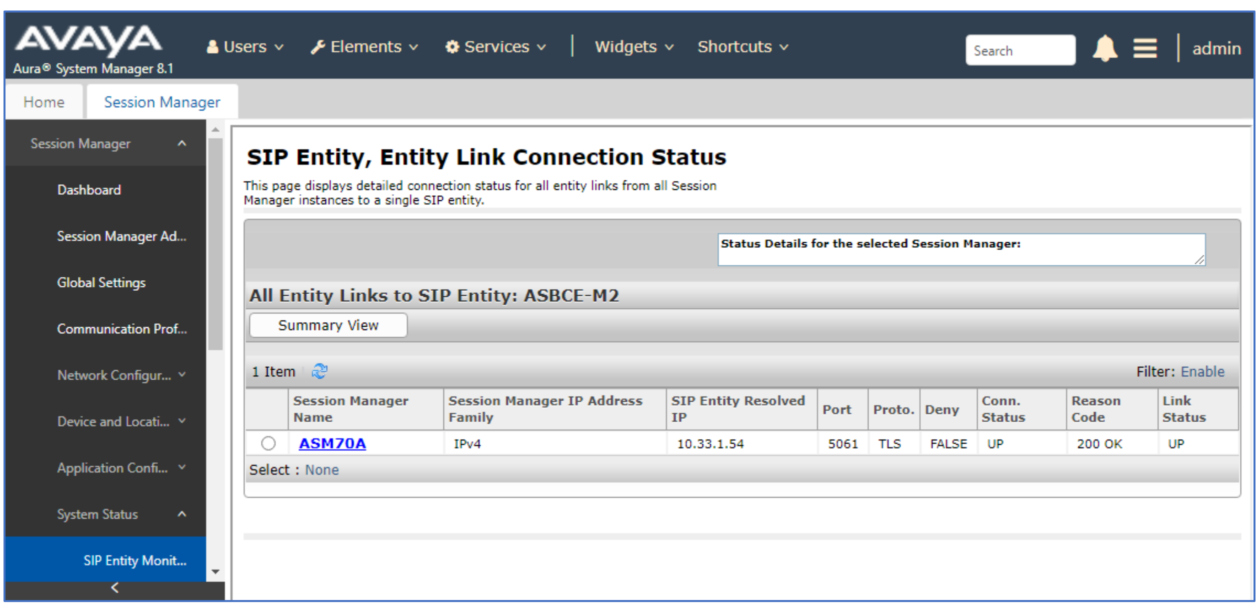
- PSTN caller can select the call back option and get redirected to VCB via Communication Manager, Session Manager and Avaya SBCE.
- PSTN caller can hear the VCB menu and make the required choices.
- VCB can recognize the choices made by the PSTN user.
- VCB can call the VDN and wait for an available agent.
- VCB can call out to the PSTN caller and connect them to an available agent.

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**.

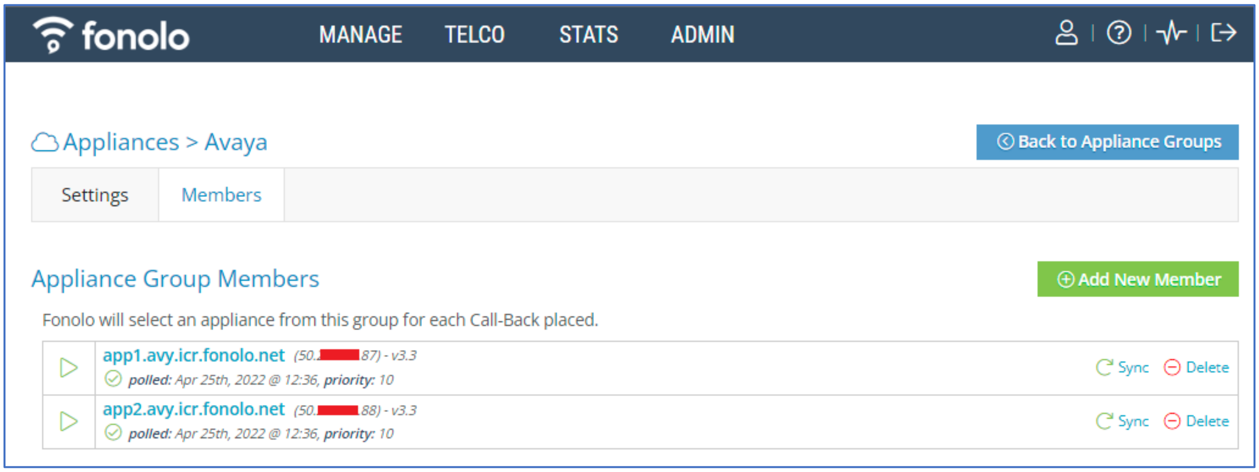


Repeat the same procedure selecting the Avaya SBCE SIP Entity and verify the **Link Status** is **UP**.

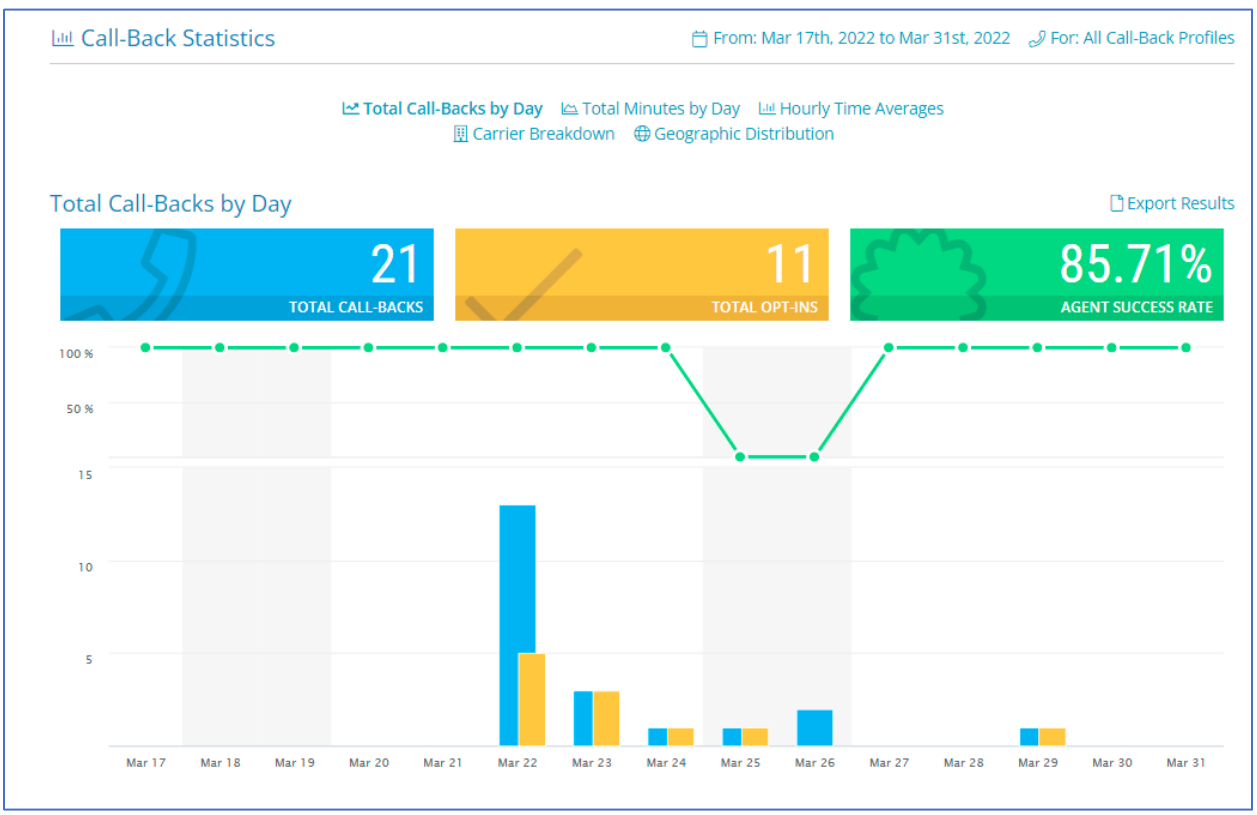


9.3. Verify Fonolo Voice Call Back

In the Fonolo customer portal, verify the link status of the SIP trunk group to Avaya SBCE, by navigating to **Telco → Appliances** and select the group of appliance (not shown) and then select the **Member** tab. All appliances should be synched successfully.



Additional information is available through the **Stats → Graphs** section of the Fonolo web portal.



10. Conclusion

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs to successfully interoperate with Avaya Session Border Controller for Enterprise. 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

Avaya Aura® Session Manager/System Manager

1. *Deploying Avaya Aura® Session Manager and Branch Session Manager in Virtualized Environment*, Release 8.1, Issue 3, August 2021
2. *Administering Avaya Aura® Session Manager*, Release 8.1, Issue 3, August 2021
3. *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.1.x, Issue 4, August 2021
4. *Administering Avaya Aura® System Manager for Release 8.1*, Release 8.1.x, Issue 5, August 2021
5. Administering Avaya Session Border Controller for Enterprise, Release 8.1, Issue 1, April 2021

Avaya Aura® Communication Manager

6. *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 8.1.x, Issue 4, August 2021
7. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, August 2021
8. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1.x, Issue 6, August 2021
9. *Administering Avaya G430 Branch Gateway*, Release 8.1.x, Issue 3, August 2021
10. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.2, Issue 9, December 2019

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.