Avaya Solution & Interoperability Test Lab

Application Notes for Fonolo Voice Call-Backs Version 3.3 with Avaya Aura® Communication Manager Release 8.1 and Avaya Aura® Session Manager Release 8.1 using SIP Trunks and TLS – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs application to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks and TLS.

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 Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks and TLS. Fonolo VCB provides functionality to replace hold time with a call back. During this compliance testing, Fonolo VCB was hosted in the cloud by Fonolo. The solution communicates via SIP/SRTP. The Fonolo VCB functionality was compliance tested utilizing SIP trunks to Session Manager. The configuration allowed Communication Manager to use SIP trunking for calls to and from the VCB application. The Fonolo VCB is a call center solution where instead of a caller staying in the queue when agents are all busy, caller 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 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 a Session Manager SIP trunk 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 a SIP trunk with Session Manager 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 prompts 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 a SIP trunk to Communication Manager and connects the caller with the available 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 call flows between Communication Manager, Session Manager 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 asks 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 utilizes TLS, use of secure media SRTP, and secure encrypted SRTCP 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 Fonolo VCB application is hosted in a cloud environment by Fonolo and the VCB application was installed and synchronized with the Fonolo on-premise appliances residing in customer’s side. SIP trunks were used to connect the VCB application with Communication Manager via Session Manager. The following features and functionality were covered during compliance testing:

- Establishment of SIP trunk connectivity between Fonolo VCB and Session Manager including session refresh.
- Testing of G.711MU codec.
- Incoming calls to a VDN of Communication Manager call center can be redirected to the VCB application via the SIP trunk based on vector scripting. Outgoing calls from the VCB appliance to the VDN via Session Manager 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 who had selected the call back option and merge the call between the caller and available agent. The outbound call is made from Communication Manager via Session Manager, Session Border Controller for Enterprise, and uses 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 trunk going down (using ‘busyout’ command) and reboot of Session Manager.

2.2. Test Results

All test cases were executed and passed with the following exceptions/observations:

- Fonolo VCB only supports G.711u codec.
- Fonolo VCB only supports encrypted SRTCP therefore only Avaya SIP IP telephones were used as agent telephones since Avaya H.323 telephones do not support encrypted SRTCP.

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 were used during compliance testing. As shown in **Figure 1**, SIP trunks were used to connect Fonolo VCB on-premise appliance with Communication Manager via Session Manager. The configuration of Fonolo VCB was done from their cloud and was synched with the Fonolo on-premise appliances via https. Avaya Session Border Controller for Enterprise was used to provide SIP connection to SIP Service Provider for external call to PSTN. A skill set queue is configured on Communication Manager with two agents belonging to this queue. The configuration allowed the enterprise site to use SIP trunking for calls to and from Fonolo VCB via the Session Manager.

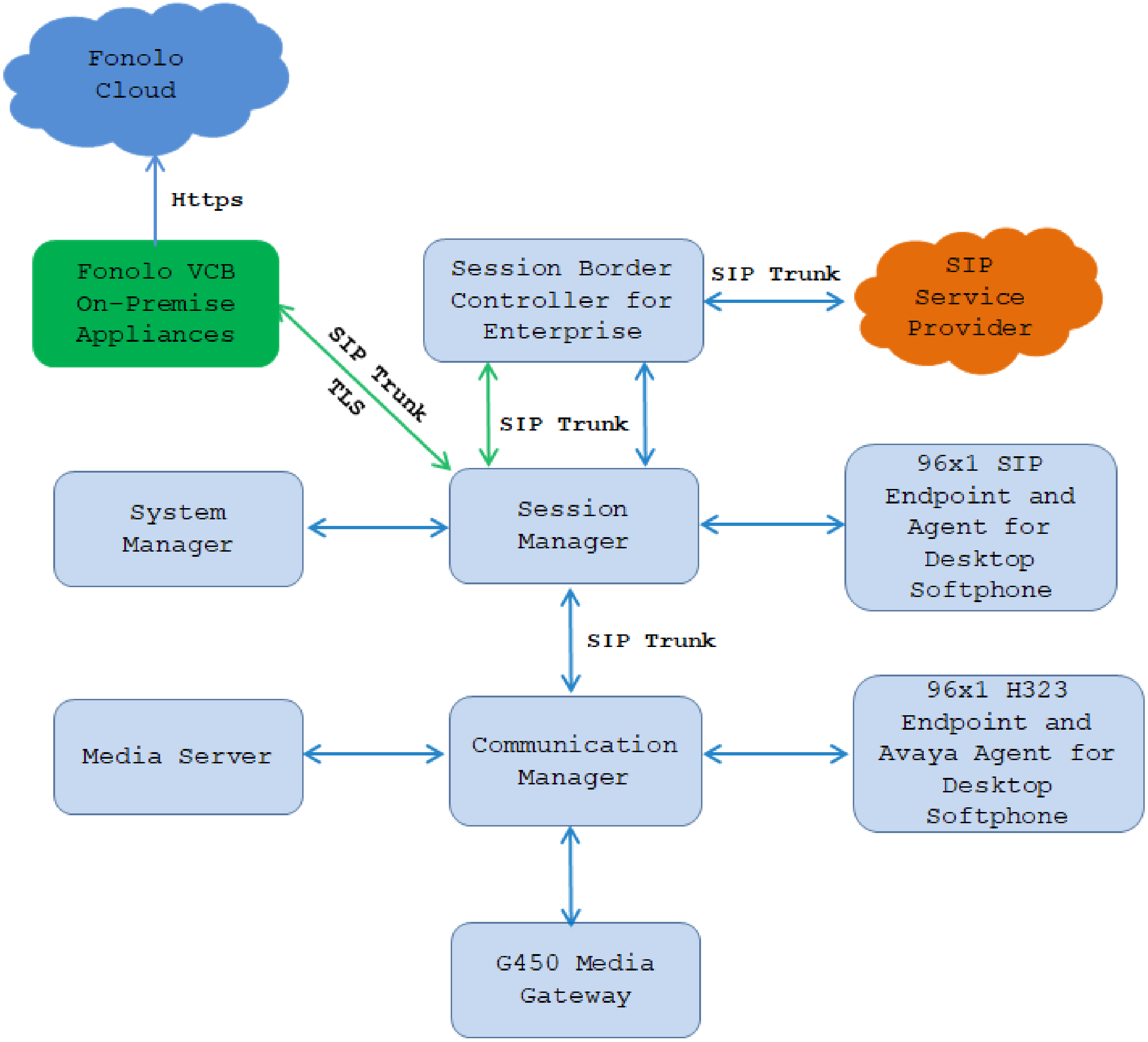

Fonolo Cloud
Https
Fonolo VCB On-Premise Appliances
SIP Trunk TLS
Session Border Controller for Enterprise
SIP Trunk
SIP Service Provider
SIP Trunk
System Manager
Session Manager
96x1 SIP Endpoint and Agent for Desktop Softphone
SIP Trunk
Media Server
Communication Manager
96x1 H323 Endpoint and Avaya Agent for Desktop Softphone
G450 Media Gateway

Figure 1: Test Diagram 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 Aura® Media Server running on Virtual Environment	8.0 8.0.2.163
Avaya 9641GS SIP Deskphone	7.1.9.0.8
Avaya 179J SIP Deskphone	4.0.10.3.2
Avaya Agent for Desktop (AAfD) Softphone	2.0.6.18
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 into 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. Administer IP Node Names

Use the “change node-names ip” command 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
```

5.3. 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. As per the observation noted in **Section** Error! Reference source not found. only configure **G.711MU** and **Encrypted SRTP** is set to “**best-effort**” that means the CM can communicate with other end either unencrypted SRTP or encrypted SRTCP. The codec shown below was used in the compliance testing.

```
change ip-codec-set 2                                              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: best-effort
 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 the codec set number 2 for integration with Fonolo VCB as configured in **Section 5.3**.

```
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: 2               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 “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 network region number 2.

- **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: 2

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
```

5.6. 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** “tie”.
- **Signaling Group:** Enter the signaling group that has been created in **Section 5.5**.
- **Number of Members**: Enter a number of SIP trunk member, in this case 10 was used.

```
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 3                                           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 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? 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
```

5.7. 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
```

5.8. 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
```

5.9. 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
```

5.10. 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.
- **Numbering Format**: Set to “lev0-pvt” which is private numbering plan.

```
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
```

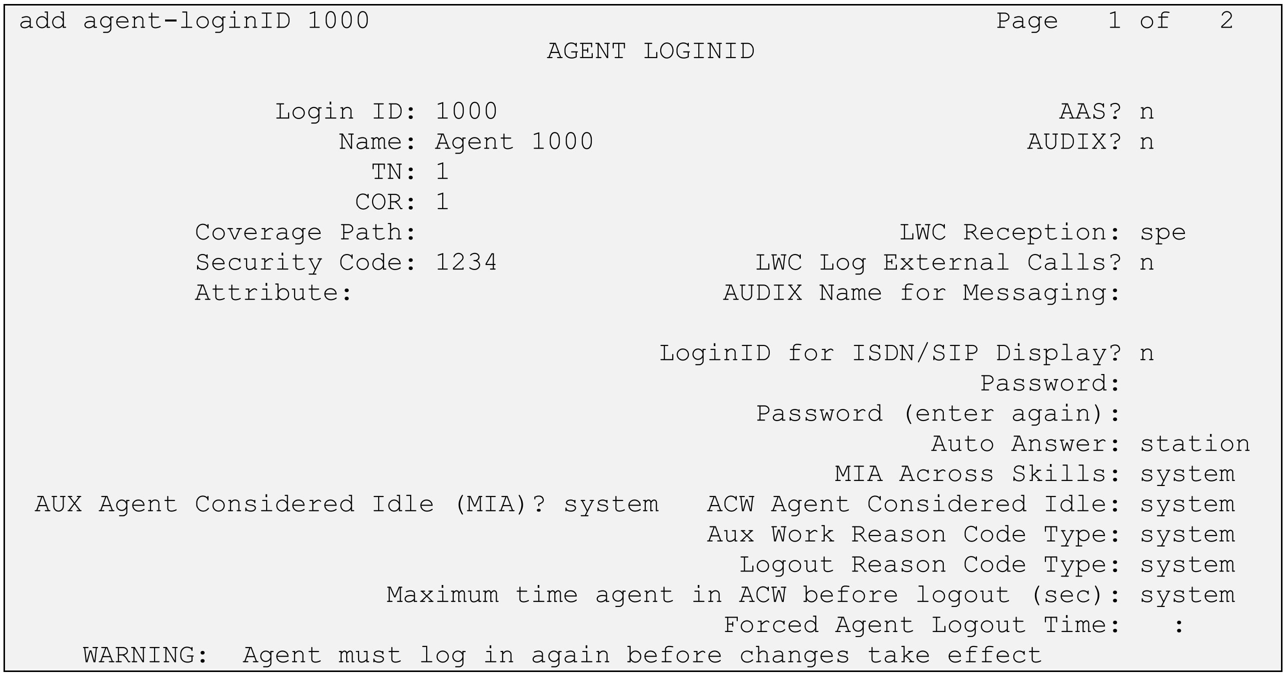
5.11. Administer AAR Analysis

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
```

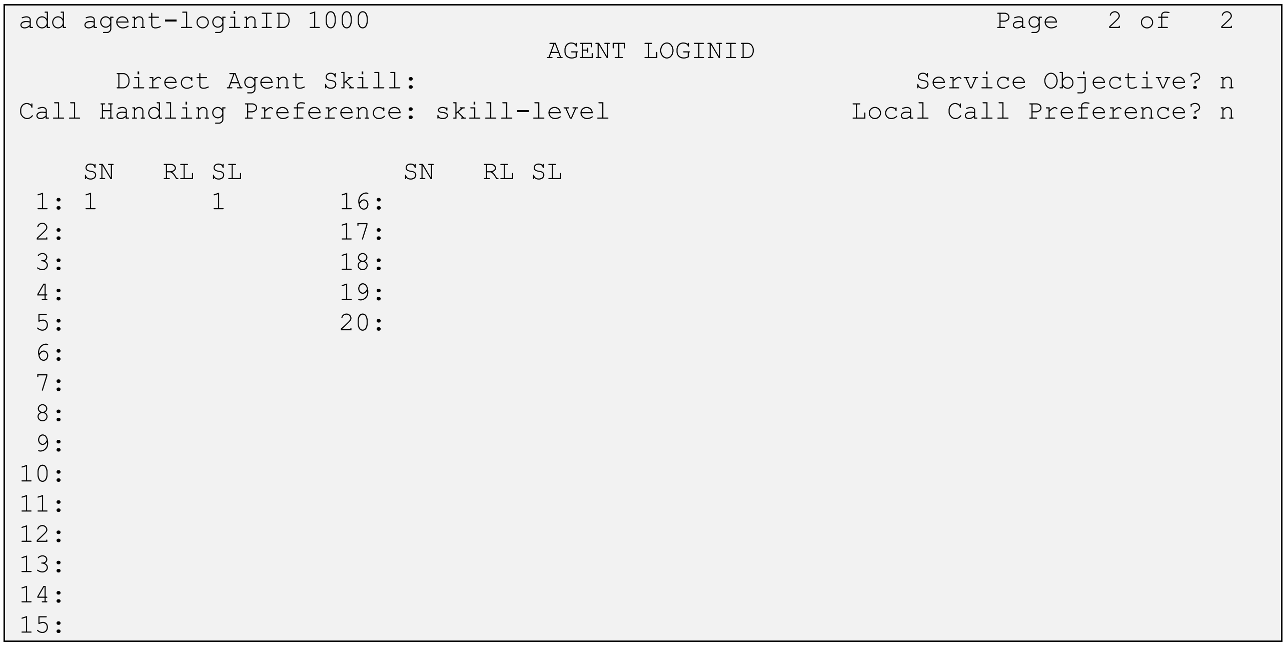
5.12. Administer Agent Login ID

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 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
```

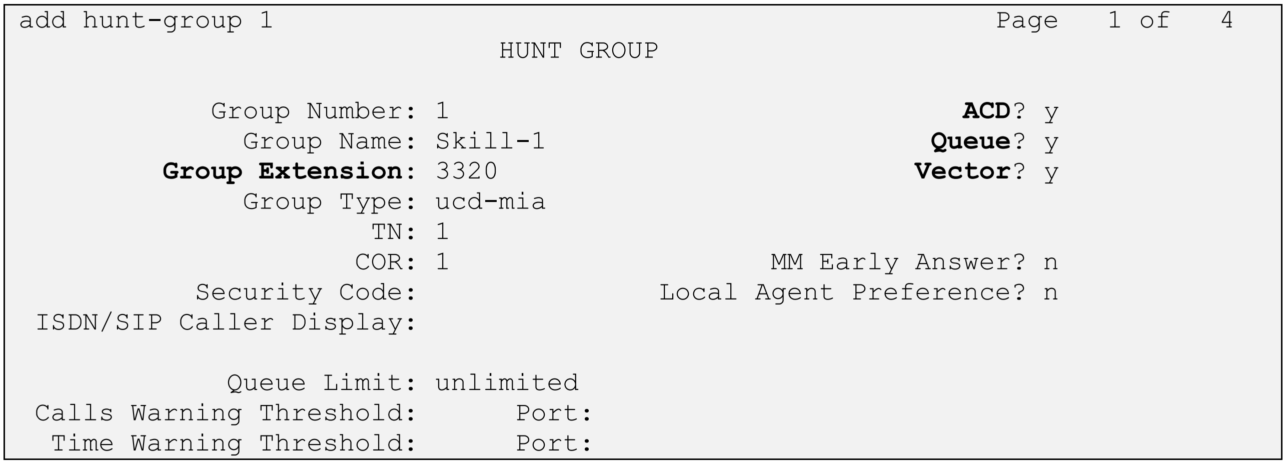
On **Page 2** of the **Agent LoginID** form, set the skill number (**SN**) to hunt group 1, which is the hunt group (skill) that the agents will log into.



```
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:
```

5.13. Administer Hunt Group

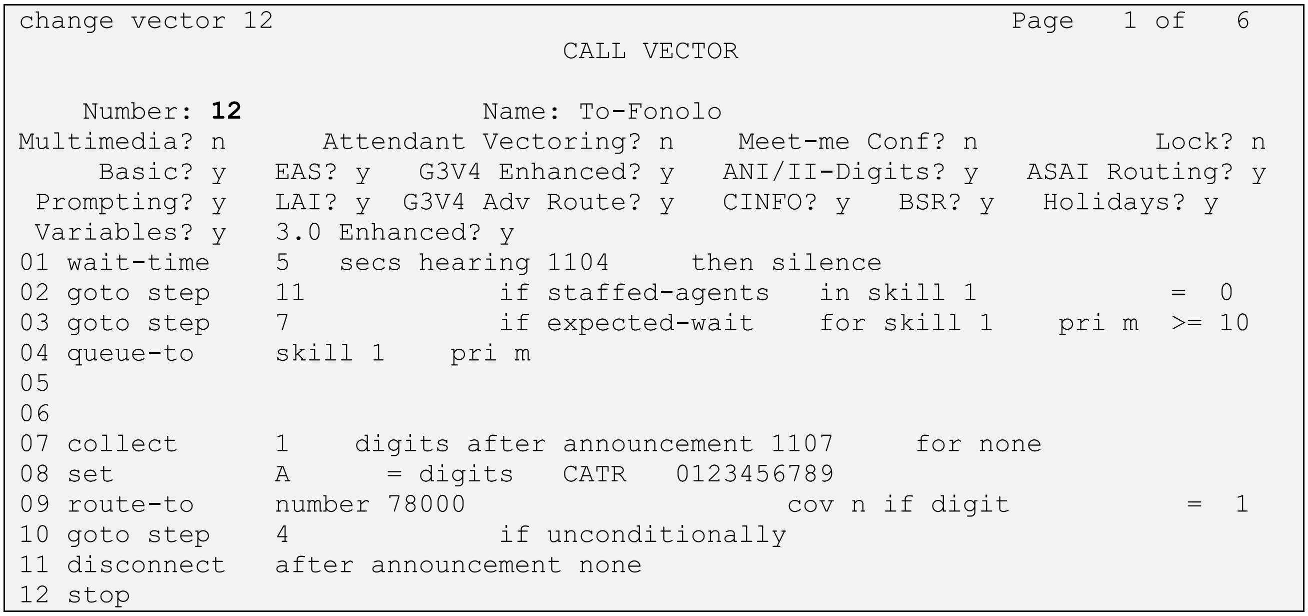
This section provides the Hunt Group configuration for the call center agents. Agents will log into Hunt Group 1 configured below. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.12**.



```
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:
```

5.14. Administer Vector

Use the command "change vector n" where "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 dial out 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
```

5.15. 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 Media Server and Avaya SIP Telephone

6.1. Configure 46xxsettings File to Enable SRTCP

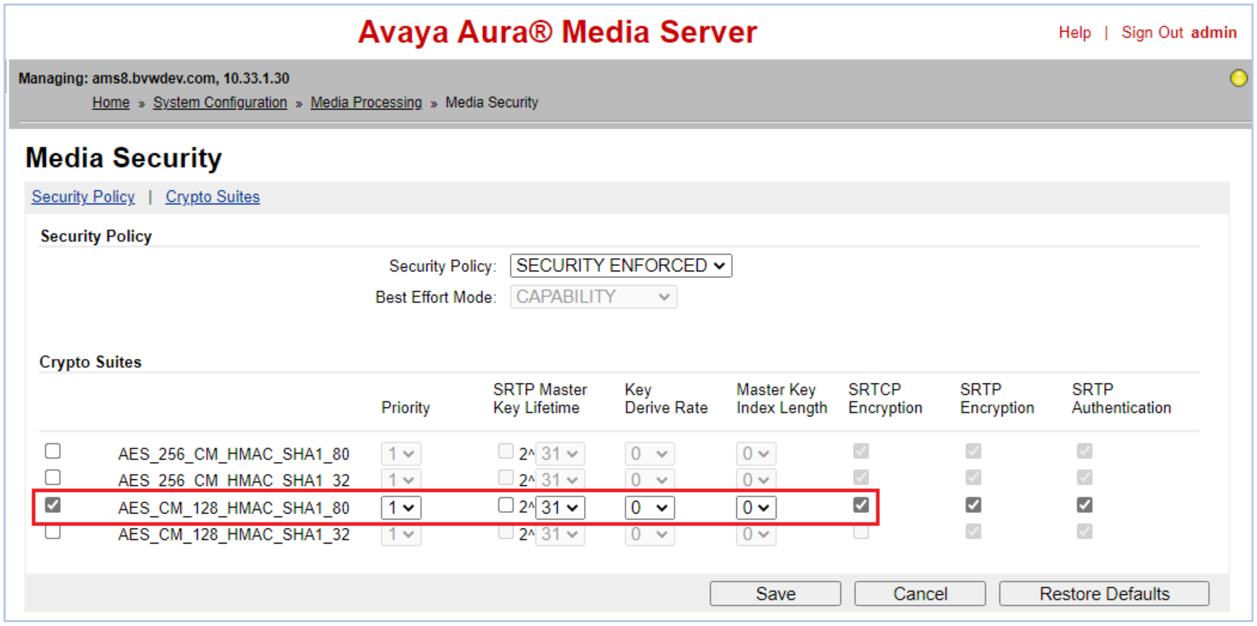
Use an editor application to modify the 46xxsettings to enable secure media SRTP and encrypted SRTCP for Avaya SIP IP telephones as shown in the highlighted text below. Make sure the SIP IP telephone is able to get the 46xxsettings file from HTTP server. The setup of HTTP server is out of scope this document.

```
#############################################################################
#########
##
##     AVAYA IP TELEPHONE CONFIGURATION FILE TEMPLATE
##             *** 21 Dec 2021  ***
##
## This file is intended to be used as a template for configuring Avaya IP 
telephones.
## Parameters supported by software releases up through the following are 
included:
##
##      J100 SIP R4.0.10.1 (J129, J139, J159, J169, J179, J189)
##      96x1 SIP R7.1.14.0
##      Avaya Vantage Devices SIP R3.1.1.0 (K155/K175)
##      Avaya Vantage builtin Unified Communication Experience R3.1.1.0 
(Known also as Avaya Vantage Connect)
##      J159/J169/J179/J189 H.323 R6.8.5.1
##      96x1 H.323 R6.8.5.1
##      B189 H.323 R6.8.5.1
##      Avaya Vantage Devices SIP R2.2.0.6 (K155/K165/K175)
##      Avaya Vantage Connect Application SIP R2.2.0.6
##      Avaya IX Workplace 3.8 (running on Avaya Vantage Devices)(f.k.a Avaya
Equinox)
##      96x0 H.323 R3.2.4
##      96x0  SIP  R2.6.14.5
##      H1xx  SIP  R1.0.2
##      16xx H.323 R1.3.3
##
## Note: At the end of the file there is HISTORY TABLE to track changes in
this file.
## MEDIAENCRYPTION specifies which media encryption (SRTP) options will be
supported.
##  Up to 2 or 3 options may be specified in a comma-separated list.
##  2 options are supported by:
##    1. Prior releases to 96x1 SIP 7.0.0
##    2. H1xx SIP R1.0 and later
##    3. 96x0 SIP R1.0 to R2.6.14.1
##  3 options are supported by 96x1 SIP R7.0.0 and later, J129  SIP  R1.0.0.0
(or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later, J139 SIP
R3.0.0.0 and later, J159 SIP R4.0.3.0 and later, J189 SIP R4.0.6.1 and later
and H1xx SIP R1.0.1 and later.
##  For 96x0 SIP R2.6.14.5 and later, up to 3 options may be specified, but
only the first two supported options are used.
##  Options should match those specified in CM IP-codec-set form.
##     1 = aescm128-hmac80
##     2 = aescm128-hmac32
##     3 = aescm128-hmac80-unauth
##     4 = aescm128-hmac32-unauth
##     5 = aescm128-hmac80-unenc
##     6 = aescm128-hmac32-unenc
##     7 = aescm128-hmac80-unenc-unauth
##     8 = aescm128-hmac32-unenc-unauth
##     9 = none (default)
##    10 = aescm256-hmac80
##    11 = aescm256-hmac32
##  Options 10 and 11 are supported by 96x1 SIP R7.0.0 and later, H1xx SIP
R1.0.1 and later and J129 SIP  R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0,
J100 SIP R2.0.0.0 and later, J139 SIP R3.0.0.0 and later,
##   J159 SIP R4.0.3.0 and later, J189 SIP R4.0.6.1 and later.
##  Note: The list of media encryption (SRTP) options is ordered from high
(left) to the low (right) options. The phone will publish this list in the
SDP-OFFER
##  or choose from SDP-OFFER list according to the list order defined in
MEDIAENCRYPTION. Please note that  Avaya Communication Manager has the
capability
##  to change the list order in the SDP-OFFER (for audio only) when the SDP-
OFFER pass through CM.
##  This parameter is supported by:
##       J129  SIP  R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP
R2.0.0.0 and later, J159 SIP R4.0.3.0 and later, J189 SIP R4.0.6.1 and later
##       Avaya IX Workplace 3.1.2 and later; supported values: 1,2,9,10 and
11. The default value is 1,2,9.
##       Avaya Vantage Connect Application SIP R1.0.0.0 and later; supported
```

```
values: 1,2,9,10 and 11. The default value is 1,2,9.
##        96x1 SIP R6.0 and later
##        H1xx SIP R1.0 and later
##        96x0 SIP R1.0 and later
SET MEDIAENCRYPTION 1
## SET MEDIAENCRYPTION 10,1,9
## ENCRYPT_SRTCP specifies whether RTCP packets are encrypted or not. SRTCP
is only used if SRTP is enabled using
## MEDIAENCRYPTION (values other than 9 (none) are configured).
## This parameter controls RTCP encryption for RTCP packets exchanged between
peers.
## RTCP packets sent to Voice Monitoring Tools are always sent unencrypted.
##  Value  Operation
##   0         SRTCP is disabled (default).
##   1     SRTCP is enabled.
##  This parameter is supported by:
##     J129  SIP  R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP
R2.0.0.0 and later, J139 SIP R3.0.0.0 and later, J159 SIP R4.0.3.0 and later,
J189 SIP R4.0.6.1 and later
##        Avaya IX Workplace 3.1.2 and later
##        96x1 SIP R7.1.0.0 and later
##        Avaya Vantage Connect Application SIP R1.0.0.0 and later
SET ENCRYPT_SRTCP 1
```

6.2. Configure Avaya Media Server

By default, SRTCP encryption in Media Server is disabled, to enable the SRTCP encryption. From the home page of Media Server (not shown), navigate to **System Configuration →Media Processing → Media Security**, check the box in the crypto suite in the SRTCP Encryption column as highlighted in the screenshot below.



Managing: ams8.bvwdev.com, 10.33.1.30

Home » System Configuration » Media Processing » Media Security

Media Security

Security Policy | Crypto Suites

Security Policy

Security Policy: SECURITY ENFORCED

Best Effort Mode: CAPABILITY

Crypto Suites

		Priority	SRTP Master Key Lifetime	Key Derive Rate	Master Key Index Length	SRTCP Encryption	SRTP Encryption	SRTP Authentication
☐	AES_256_CM_HMAC_SHA1_80	1	☐ 2^ 31	0	0	☑	☑	☑
☐	AES_256_CM_HMAC_SHA1_32	1	☐ 2^ 31	0	0	☑	☑	☑
☑	AES_CM_128_HMAC_SHA1_80	1	☐ 2^ 31	0	0	☑	☑	☑
☐	AES_CM_128_HMAC_SHA1_32	1	☐ 2^ 31	0	0	☐	☑	☑

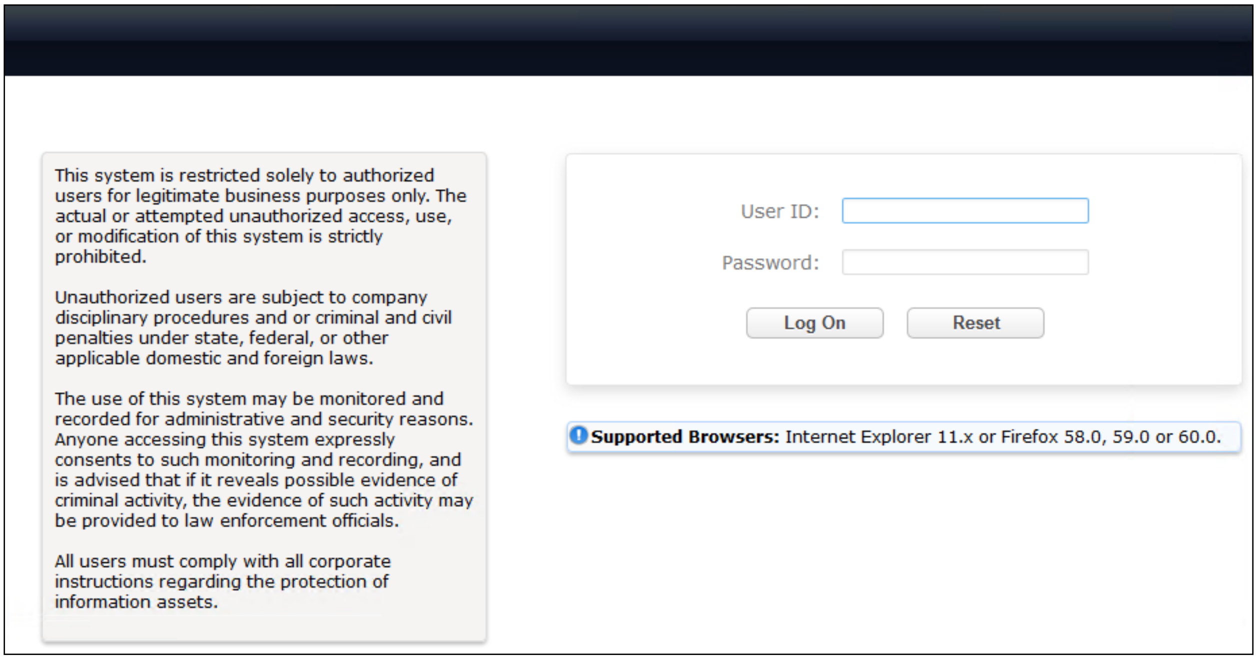
7. Configure Avaya Aura® Session Manager

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
- Administer Certificate for VCB Appliance

7.1. 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.



This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

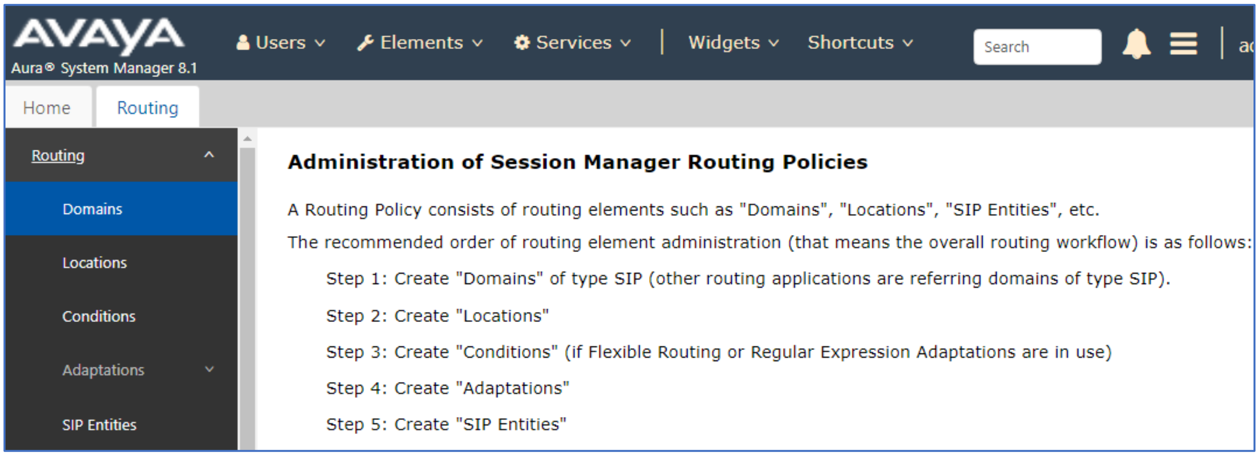
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

Supported Browsers: Internet Explorer 11.x or Firefox 58.0, 59.0 or 60.0.

7.2. 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



Administration of Session Manager Routing Policies

A Routing Policy consists of routing elements such as "Domains", "Locations", "SIP Entities", etc.

The recommended order of routing element administration (that means the overall routing workflow) is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

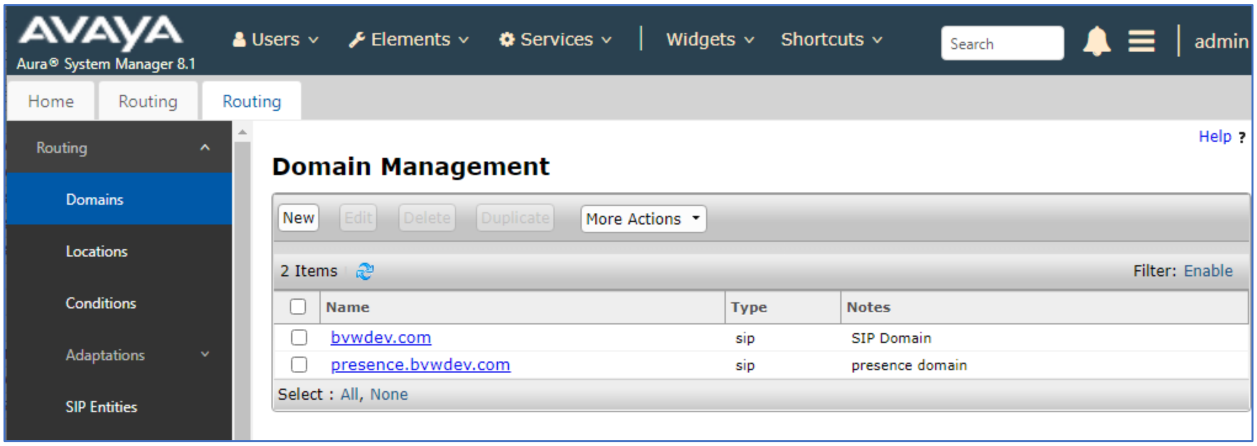
Step 2: Create "Locations"

Step 3: Create "Conditions" (if Flexible Routing or Regular Expression Adaptations are in use)

Step 4: Create "Adaptations"

Step 5: Create "SIP Entities"

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**.



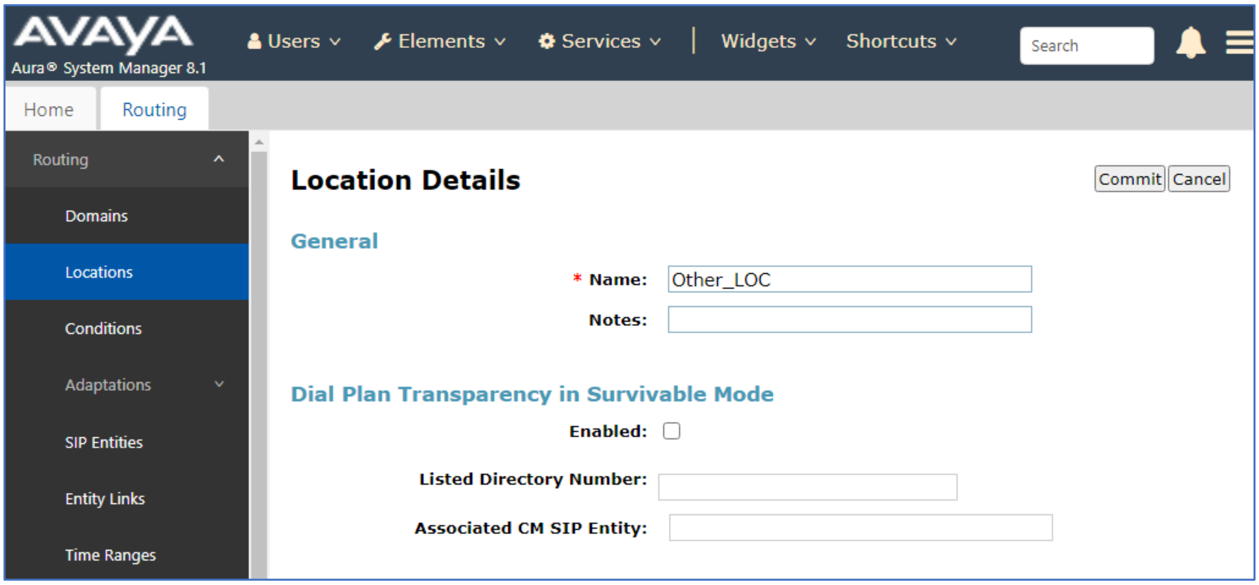
Domain Management

□	Name	Type	Notes
□	bvwdev.com	sip	SIP Domain
□	presence.bvwdev.com	sip	presence domain

7.3. 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.



Location Details

General

* Name: Other_LOC

Notes:

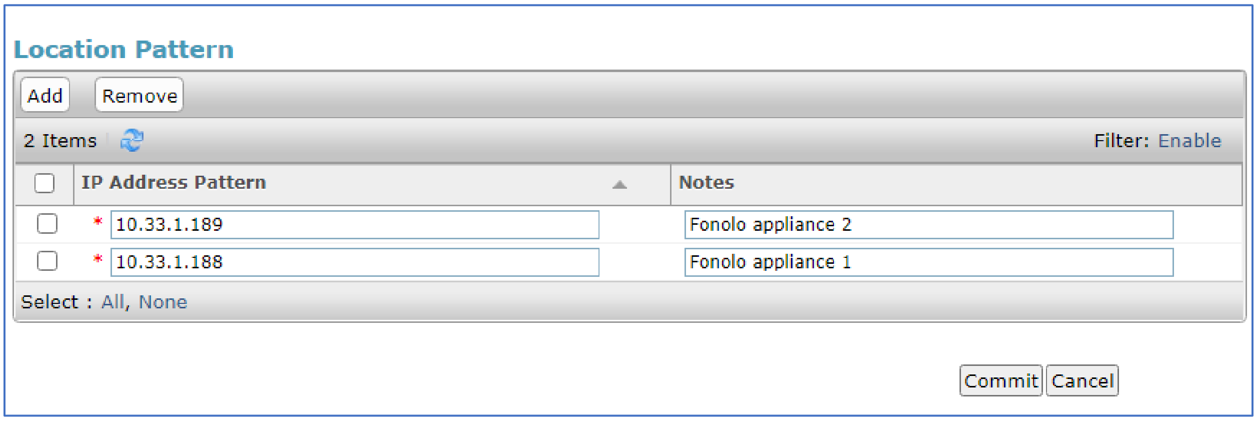
Dial Plan Transparency in Survivable Mode

Enabled: □

Listed Directory Number:

Associated CM SIP Entity:

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



Location Pattern

2 Items

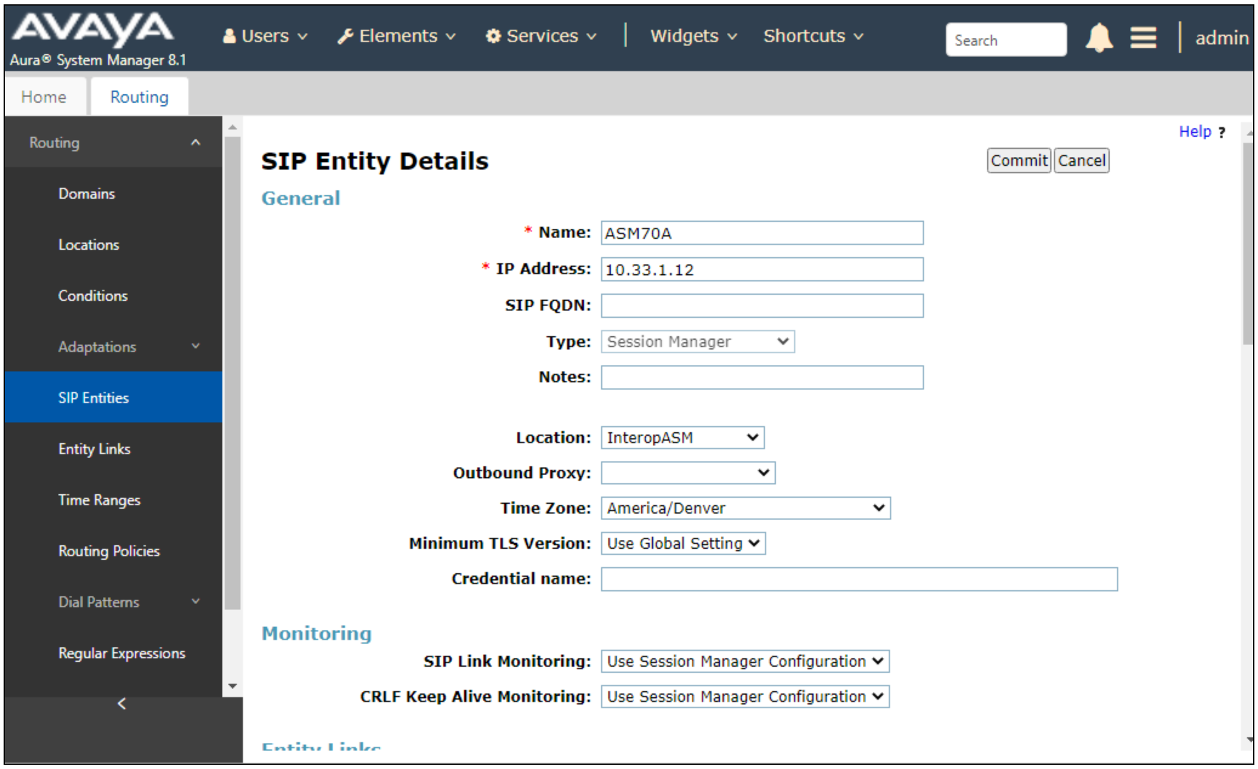
□	IP Address Pattern	Notes
□	* 10.33.1.189	Fonolo appliance 2
□	* 10.33.1.188	Fonolo appliance 1

7.4. 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 Fonolo appliances.

7.4.1. 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**.



SIP Entity Details

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

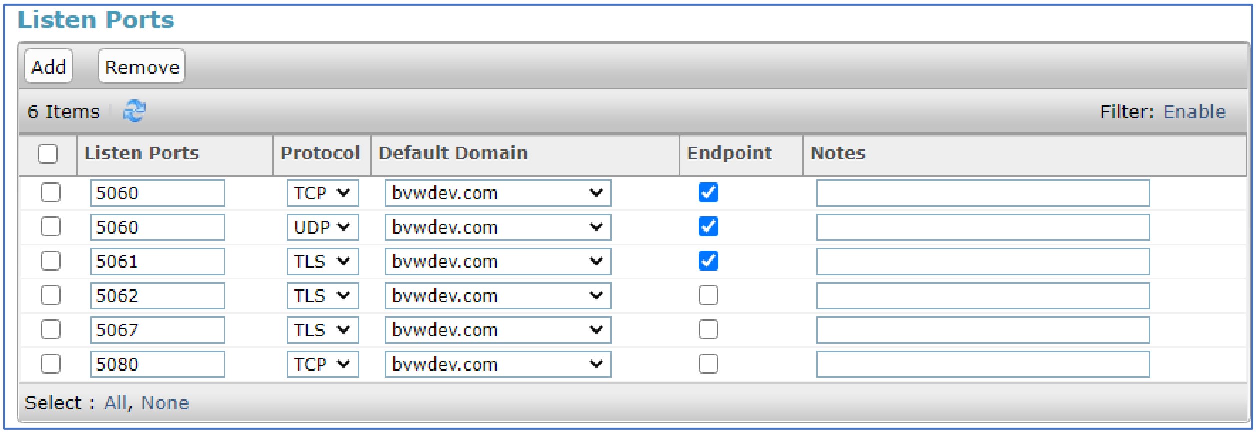
SIP Link Monitoring:	Use Session Manager Configuration
CRLF Keep Alive Monitoring:	Use Session Manager Configuration

Entity Links

The ports need to be defined in Session Manager for other endpoints to connect to, 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.



Listen Ports

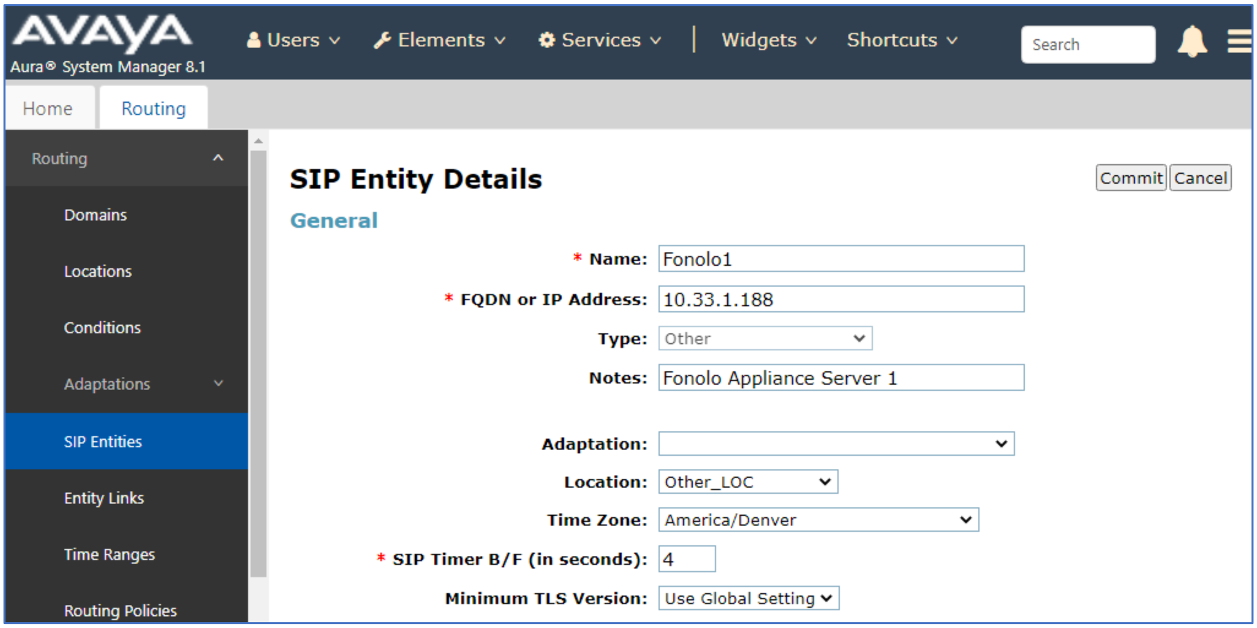
□	Listen Ports	Protocol	Default Domain	Endpoint	Notes
□	5060	TCP	bvwdev.com	☑	
□	5060	UDP	bvwdev.com	☑	
□	5061	TLS	bvwdev.com	☑	
□	5062	TLS	bvwdev.com	□	
□	5067	TLS	bvwdev.com	□	
□	5080	TCP	bvwdev.com	□	

7.4.2. SIP Entity for Fonolo Voice Call-Backs

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

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 Fonolo VCB appliance
- **Type:** Set is as"Other".
- **Notes:** Enter desired notes.
- **Location:** Select appropriate location name from **Section 7.3**.
- **Time Zone:** Select the applicable time zone.
- **SIP Link Monitoring:** Select "Link Monitoring Enabled" (not shown).



SIP Entity Details

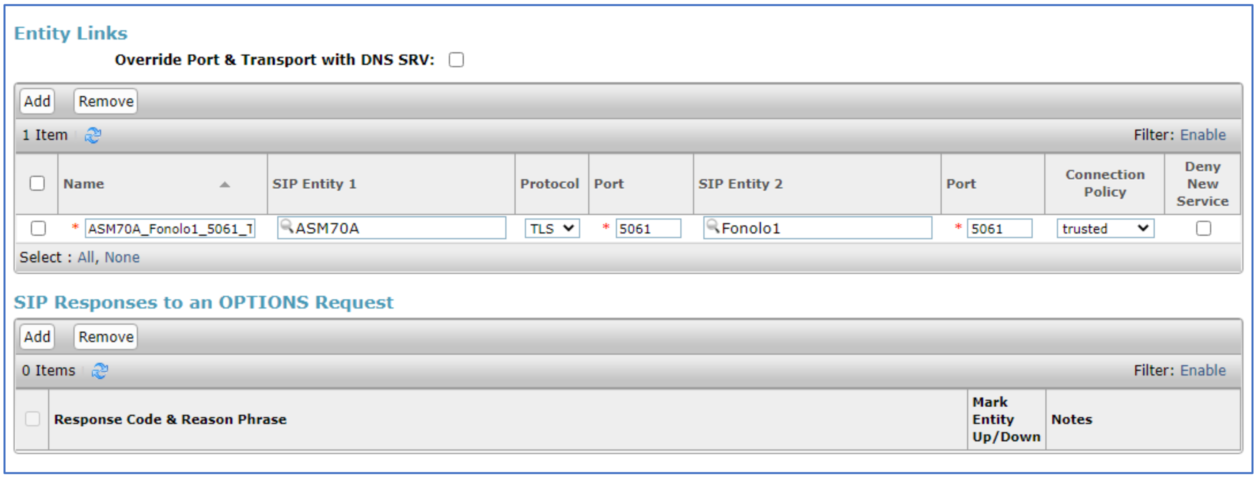
General

* Name:	Fonolo1
* FQDN or IP Address:	10.33.1.188
Type:	Other
Notes:	Fonolo Appliance Server 1
Adaptation:	
Location:	Other_LOC
Time Zone:	America/Denver
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting

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:** The VCB entity name from this section.
- **Port:** Set it as "5061".
- **Connection Policy:** **Select** "trusted".

Note that only **TLS** protocol was tested.



Entity Links

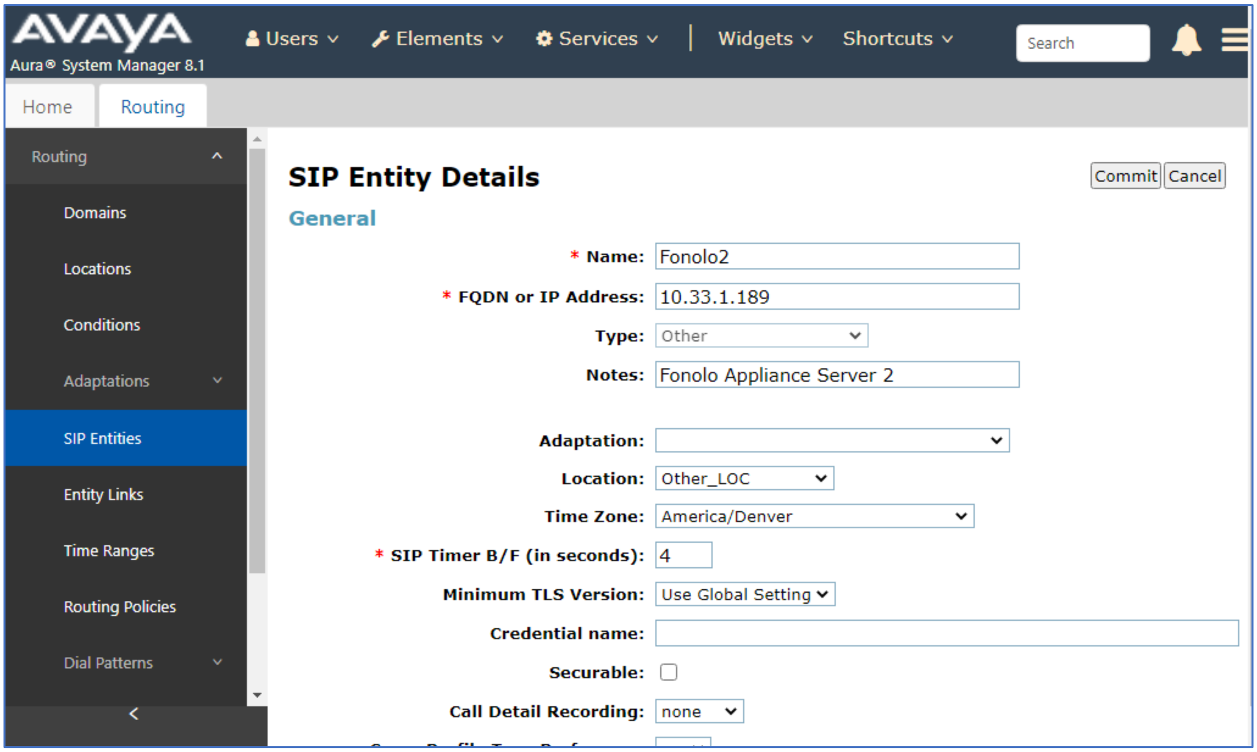
Override Port & Transport with DNS SRV: □

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	* ASM70A_Fonolo1_5061_T	ASM70A	TLS	* 5061	Fonolo1	* 5061	trusted	□

SIP Responses to an OPTIONS Request

□	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

Repeat the procedure above to add another SIP entity for VCB, during the compliance testing two Fonolo appliances were used for outgoing and incoming calls between Communication Manager and Fonolo appliances.

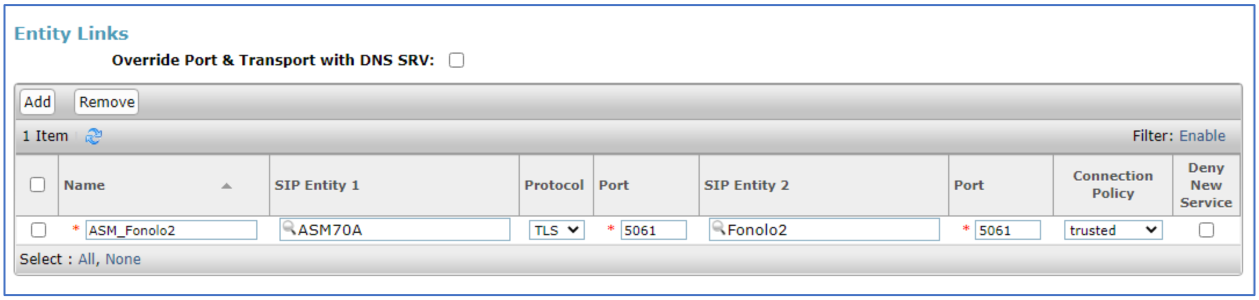


SIP Entity Details

General

* Name:	Fonolo2
* FQDN or IP Address:	10.33.1.189
Type:	Other
Notes:	Fonolo Appliance Server 2
Adaptation:	
Location:	Other_LOC
Time Zone:	America/Denver
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	none

The screen below shows the entity link for the Fonolo VCB appliance server 2.



Entity Links

Override Port & Transport with DNS SRV: □

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	* ASM_Fonolo2	ASM70A	TLS	* 5061	Fonolo2	* 5061	trusted	□

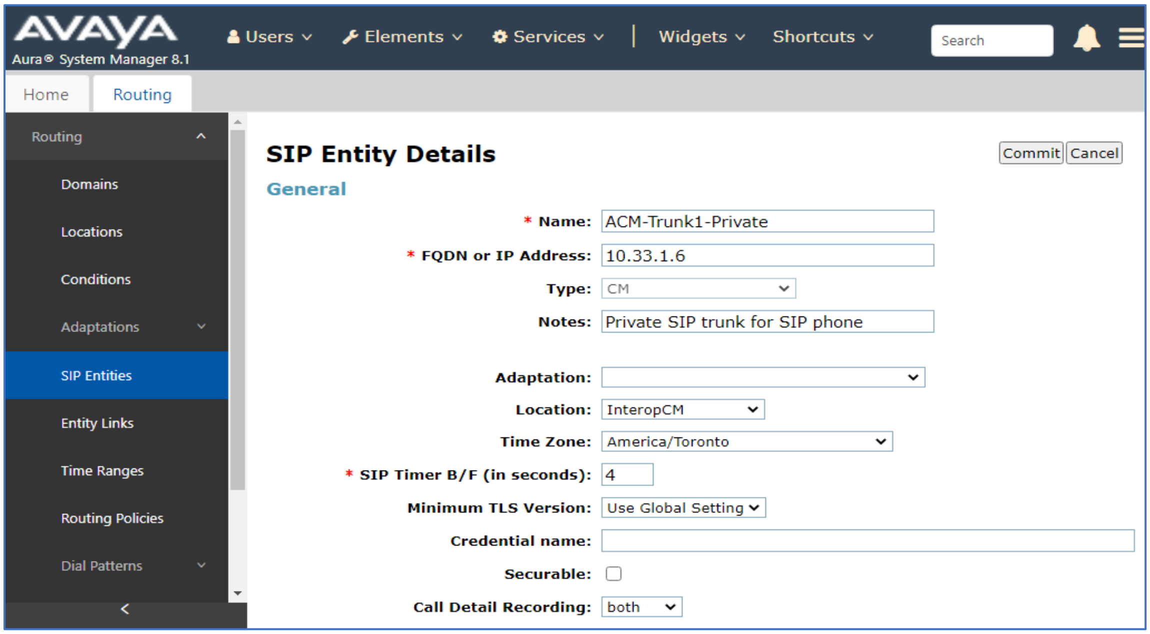
Select : All, None

7.4.3. 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.



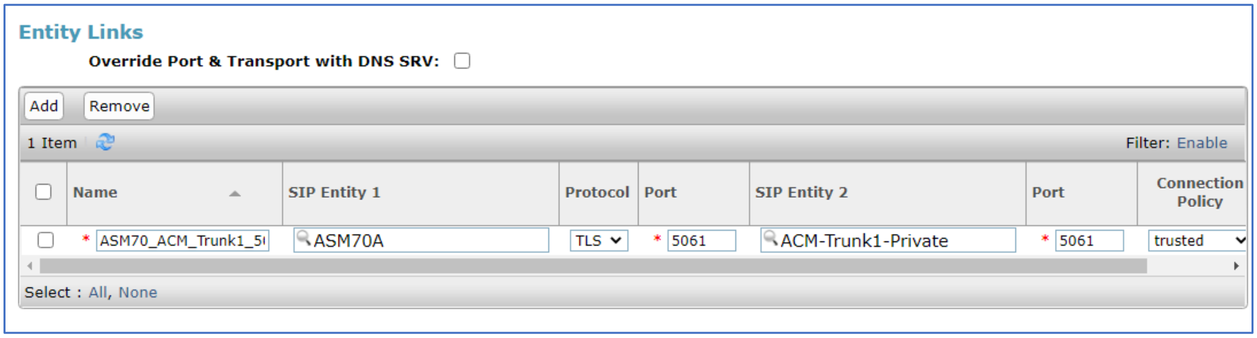
SIP Entity Details

General

* Name:	ACM-Trunk1-Private
* FQDN or IP Address:	10.33.1.6
Type:	CM
Notes:	Private SIP trunk for SIP phone
Adaptation:	
Location:	InteropCM
Time Zone:	America/Toronto
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	both

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".



Entity Links

Override Port & Transport with DNS SRV: □

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
□	* ASM70_ACM_Trunk1_5(	ASM70A	TLS	* 5061	ACM-Trunk1-Private	* 5061	trusted

7.5. Administer Routing Policies

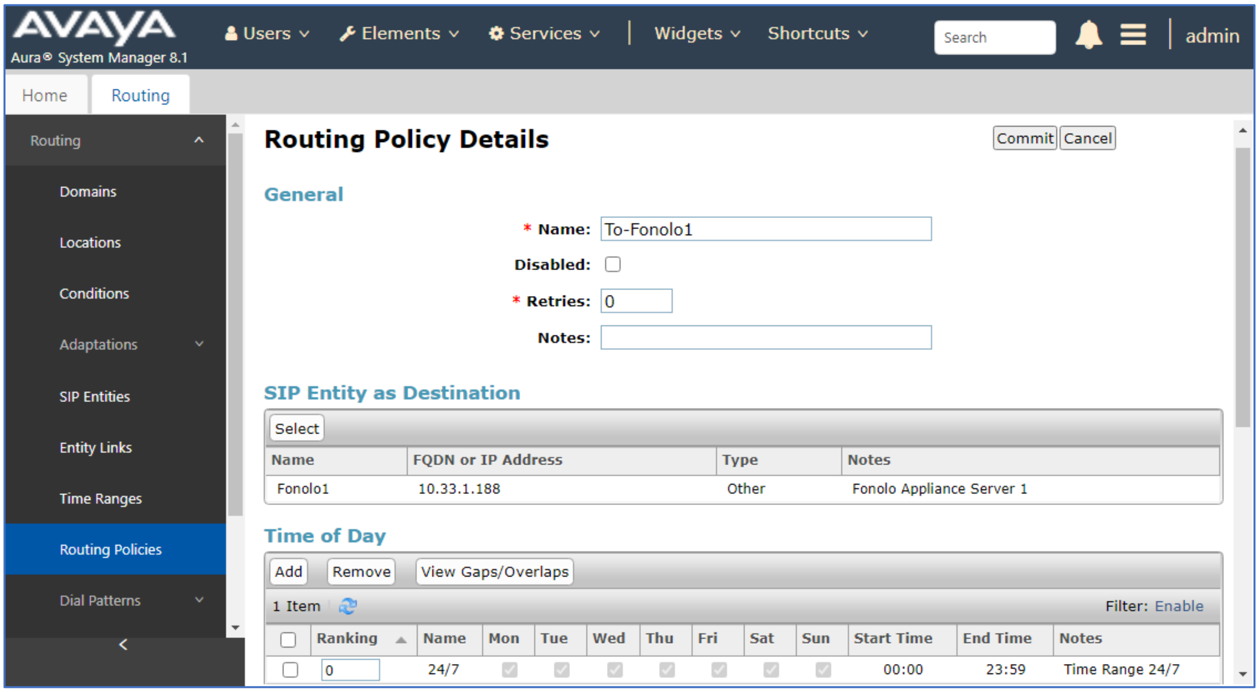
Add two new routing policies, one for VCB and one for the new SIP trunks with Communication Manager.

7.5.1. Routing Policy for Fonolo VCB

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

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 Fonolo SIP entity name from **Section 7.4.2**. In the **Time of Day** sub-section, enter "0" for **Ranking**. Ranking option is only configured for the two outgoing routing policies of VCB so that calls can be load balanced. The screen below shows the result of the selection.



Routing Policy Details

General

* Name: To-Fonolo1

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Fonolo1	10.33.1.188	Other	Fonolo Appliance Server 1

Time of Day

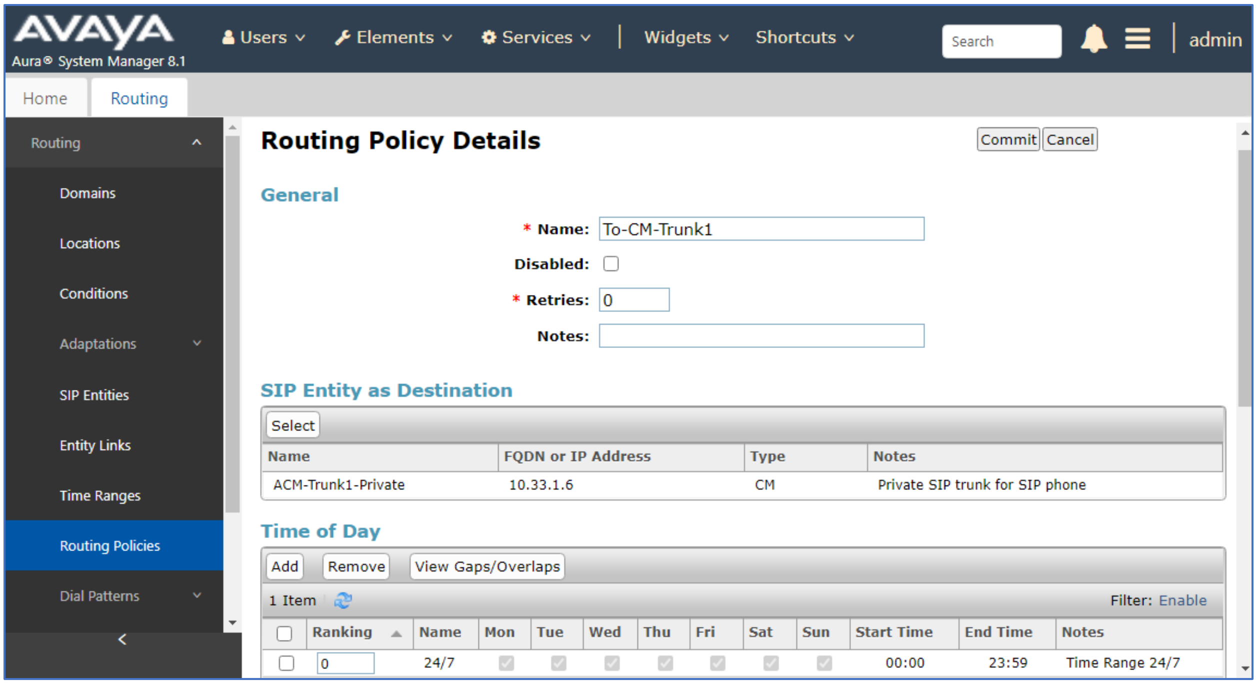
□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

7.5.2. 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 7.4.3**. The screen below shows the result of the selection.



Routing Policy Details

General

* Name: To-CM-Trunk1

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
ACM-Trunk1-Private	10.33.1.6	CM	Private SIP trunk for SIP phone

Time of Day

1 Item

☐	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

7.6. Administer Dial Patterns

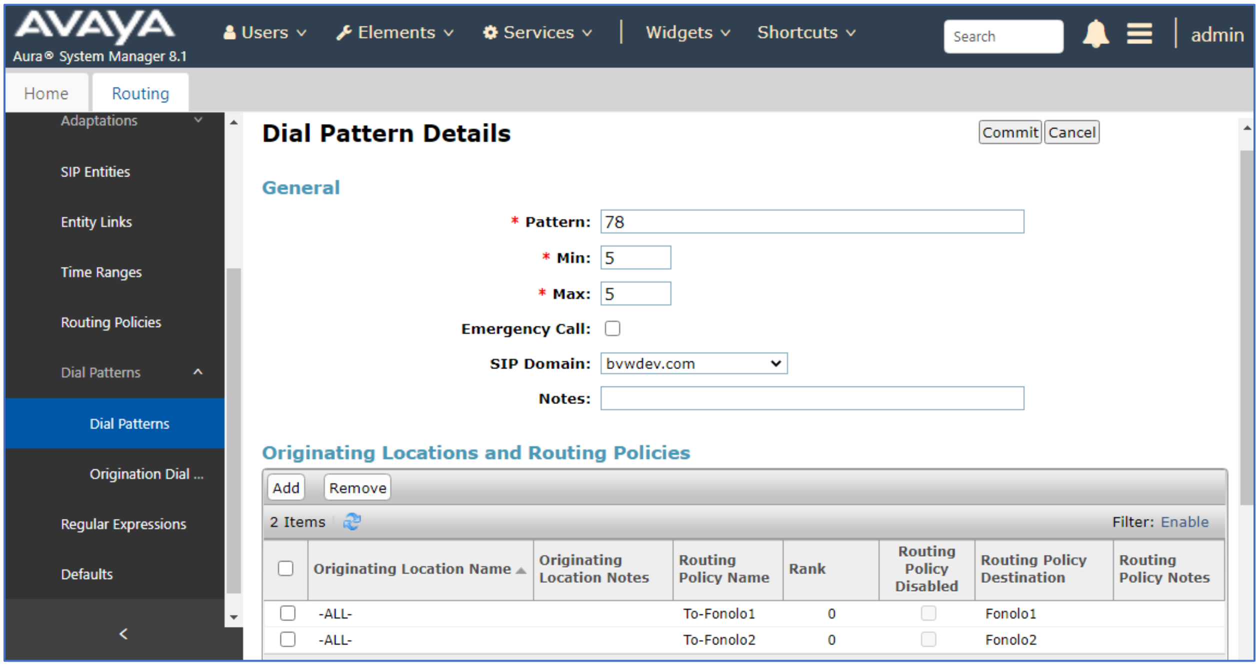
Add a new dial pattern for Fonolo VCB and Communication Manager.

7.6.1. Dial Pattern for Fonolo VCB

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. 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 7.2**

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching the Fonolo VCB. In the compliance testing, the entry allowed for call originations from all Communication Manager endpoints in locations "All". The VCB routing policy from **Section 7.5.1** was selected as shown below. Note that two routing policies are selected since during this compliance testing, two outgoing routing policies were configured for calls made from Communication Manager to VCB.



Dial Pattern Details

General

* Pattern: 78

* Min: 5

* Max: 5

Emergency Call: □

SIP Domain: bvwdev.com

Notes:

Originating Locations and Routing Policies

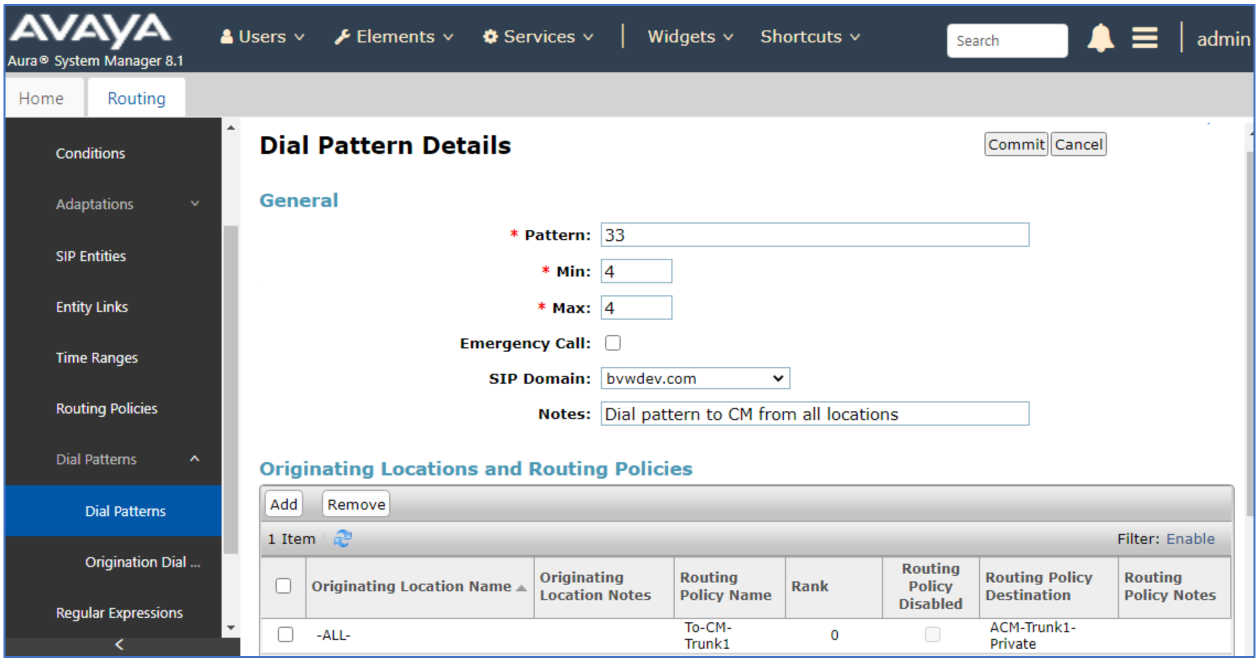
□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		To-Fonolo1	0	□	Fonolo1	
□	-ALL-		To-Fonolo2	0	□	Fonolo2	

7.6.2. 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, in this case "33" and "9"
- **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 7.2**

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 VCB endpoints in all locations . The Communication Manager routing policy from **Section 7.5.2** was selected as shown below.



Dial Pattern Details

General

* Pattern: 33

* Min: 4

* Max: 4

Emergency Call: □

SIP Domain: bvwdev.com

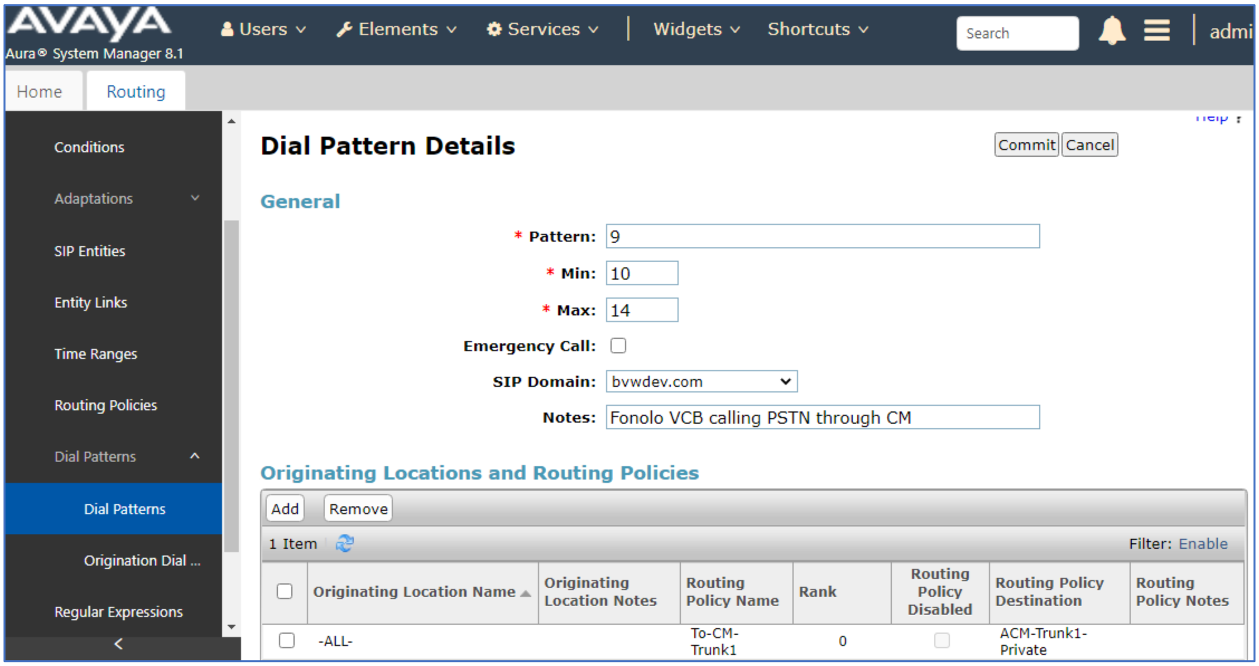
Notes: Dial pattern to CM from all locations

Originating Locations and Routing Policies

1 Item Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		To-CM-Trunk1	0	□	ACM-Trunk1-Private	

Below is the dial pattern with the leading digit “9” for the outbound call from Fonolo VCB to PSTN through Communication Manager. The digit ‘9” is the ARS access code in Communication Manager.



Dial Pattern Details

General

* Pattern:	9
* Min:	10
* Max:	14
Emergency Call:	□
SIP Domain:	bvwdev.com
Notes:	Fonolo VCB calling PSTN through CM

Originating Locations and Routing Policies

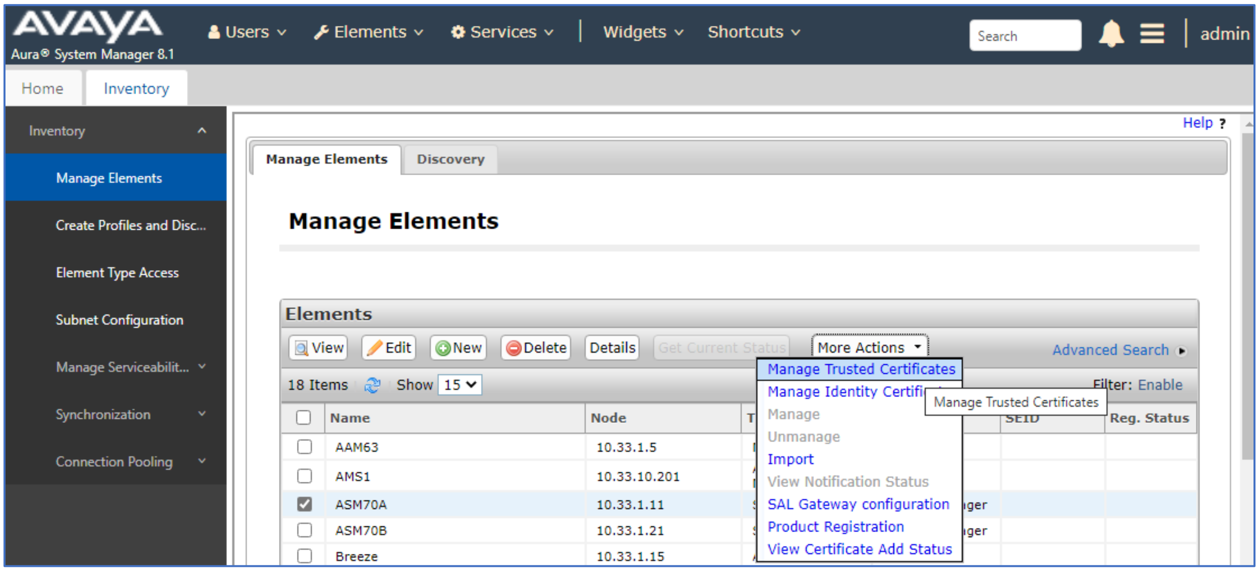
1 Item Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		To-CM-Trunk1	0	□	ACM-Trunk1-Private	

7.7. Administer Fonolo VCB Certificate

During the testing, Mutual TLS authentication between Fonolo VCB appliances and Session Manager was used. Certificate Authority (CA) certificate of each side was installed on the server/appliance of the other side.

To add Fonolo trust certificate in Session Manager, in the home page of System Manager, navigate to **Services → Inventory → Manage Elements**. The **Manage Elements** page displays, in the **Elements** section, click on Session Manager **ASM70A** and then select **More Actions → Manage Trusted Certificates** as shown in the screenshot below.



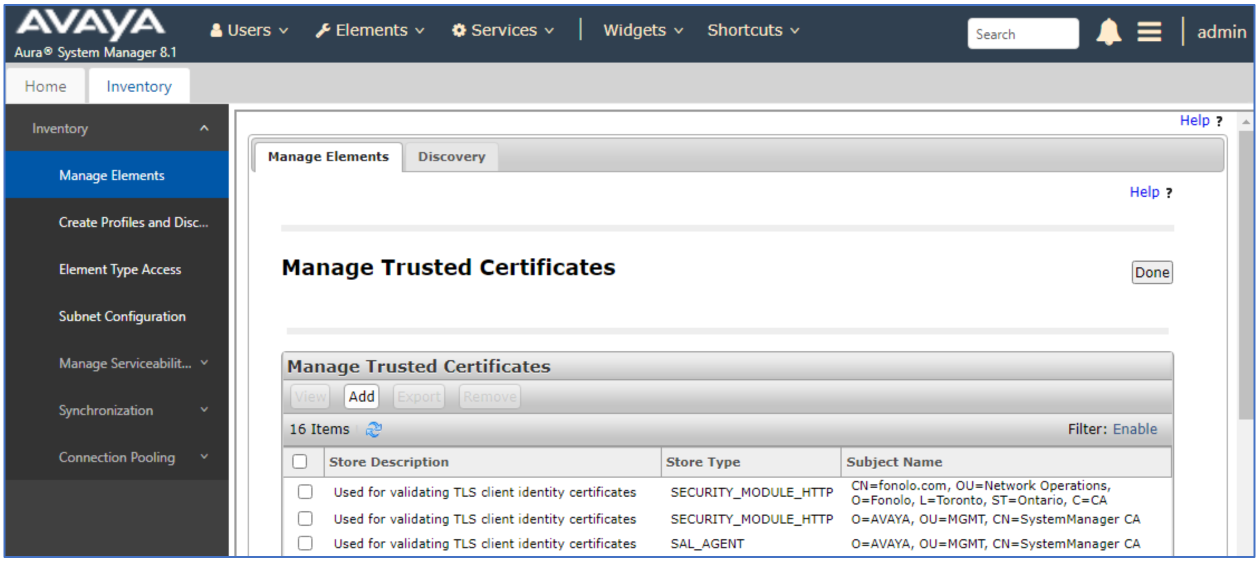
Manage Elements

Elements

18 Items Show 15

☐	Name	Node	T	SEID	Reg. Status
☐	AAM63	10.33.1.5			
☐	AMS1	10.33.10.201			
☑	ASM70A	10.33.1.11			
☐	ASM70B	10.33.1.21			
☐	Breeze	10.33.1.15			

The **Manage Trusted Certificates** page displays, select **Add**.



Manage Trusted Certificates

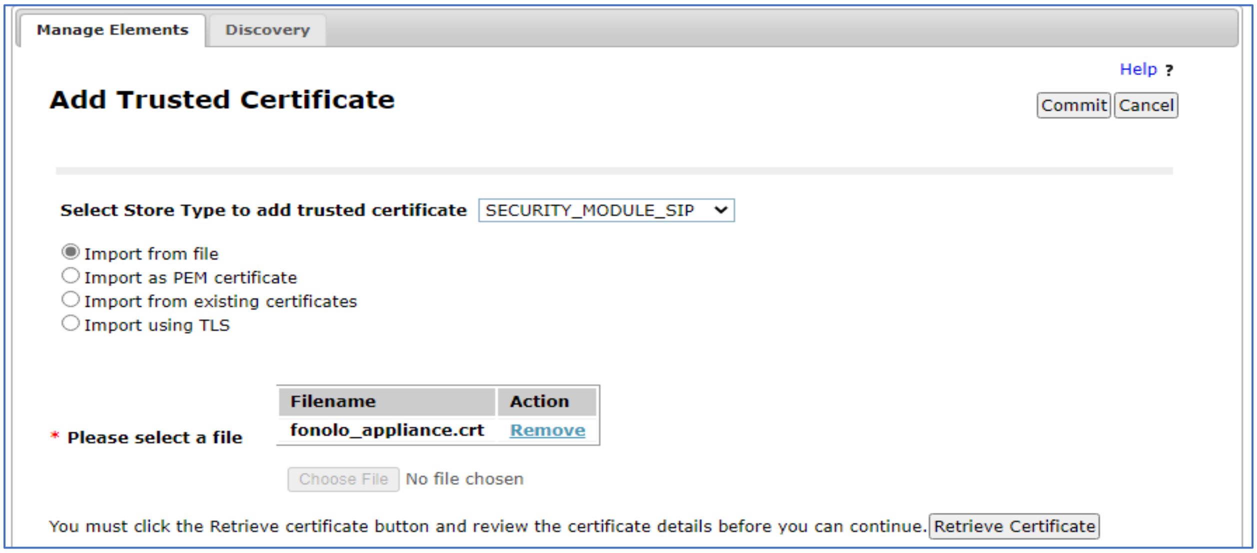
Manage Trusted Certificates

16 Items

☐	Store Description	Store Type	Subject Name
☐	Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	CN=fonolo.com, OU=Network Operations, O=Fonolo, L=Toronto, ST=Ontario, C=CA
☐	Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	O=AVAYA, OU=MGMT, CN=SystemManager CA
☐	Used for validating TLS client identity certificates	SAL_AGENT	O=AVAYA, OU=MGMT, CN=SystemManager CA

In the **Add Trusted Certificate** page, do the following:

- **Select Store Type to add trusted certificate**: Select **SECURITY_MODULE_SIP** from the drop-down menu
- **Import from file**: Select this option
- **Choose File**: Browse to Fonolo certificate file
- **Retrieve Certificate**: Select this button to retrieve the certificate



Add Trusted Certificate

Select Store Type to add trusted certificate: SECURITY_MODULE_SIP

● Import from file
○ Import as PEM certificate
○ Import from existing certificates
○ Import using TLS

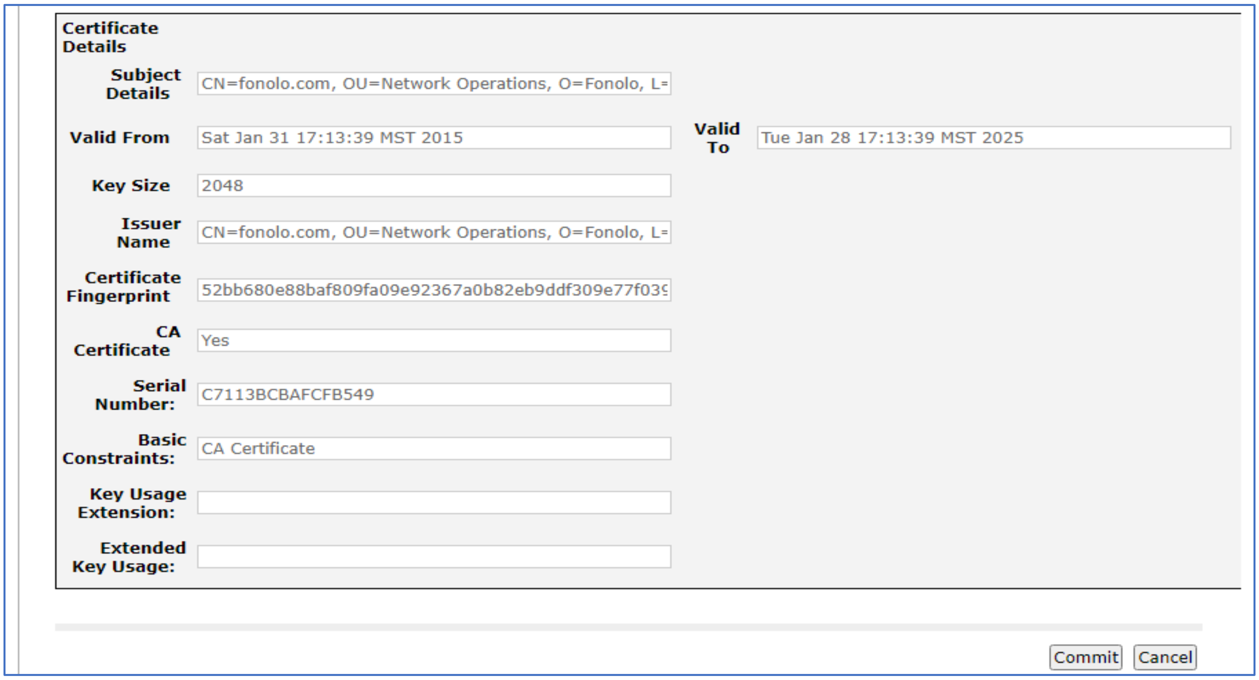
* Please select a file

Filename	Action
fonolo_appliance.crt	Remove

No file chosen

You must click the Retrieve certificate button and review the certificate details before you can continue.

After retrieving the certificate successfully, select **Commit** button to confirm the addition of the certificate.



Certificate Details

Subject Details	CN=fonolo.com, OU=Network Operations, O=Fonolo, L=		
Valid From	Sat Jan 31 17:13:39 MST 2015	Valid To	Tue Jan 28 17:13:39 MST 2025
Key Size	2048		
Issuer Name	CN=fonolo.com, OU=Network Operations, O=Fonolo, L=		
Certificate Fingerprint	52bb680e88baf809fa09e92367a0b82eb9ddf309e77f03\9		
CA Certificate	Yes		
Serial Number:	C7113BCBAFCFB549		
Basic Constraints:	CA Certificate		
Key Usage Extension:			
Extended Key Usage:			

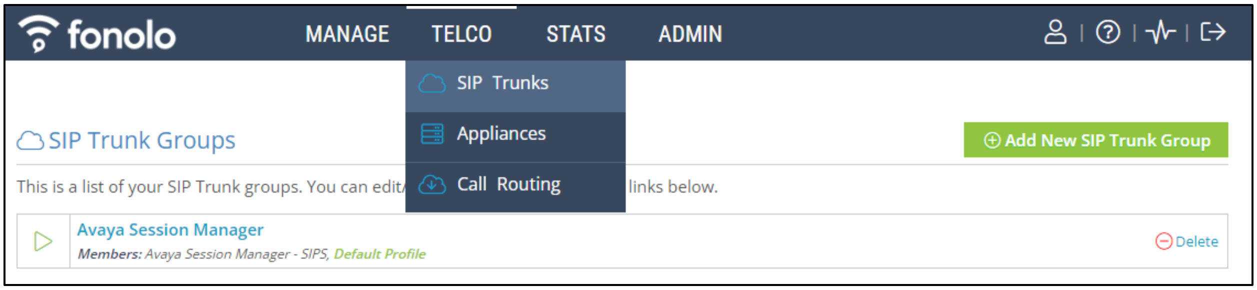
8. Configure Fonolo Voice Call-Backs

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 for reference only. 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 Session Manager** was used as the label. Then select **Add New SIP Trunk** (not shown).



This is a list of your SIP Trunk groups. You can edit links below.

Avaya Session Manager
Members: Avaya Session Manager - SIPS, Default Profile

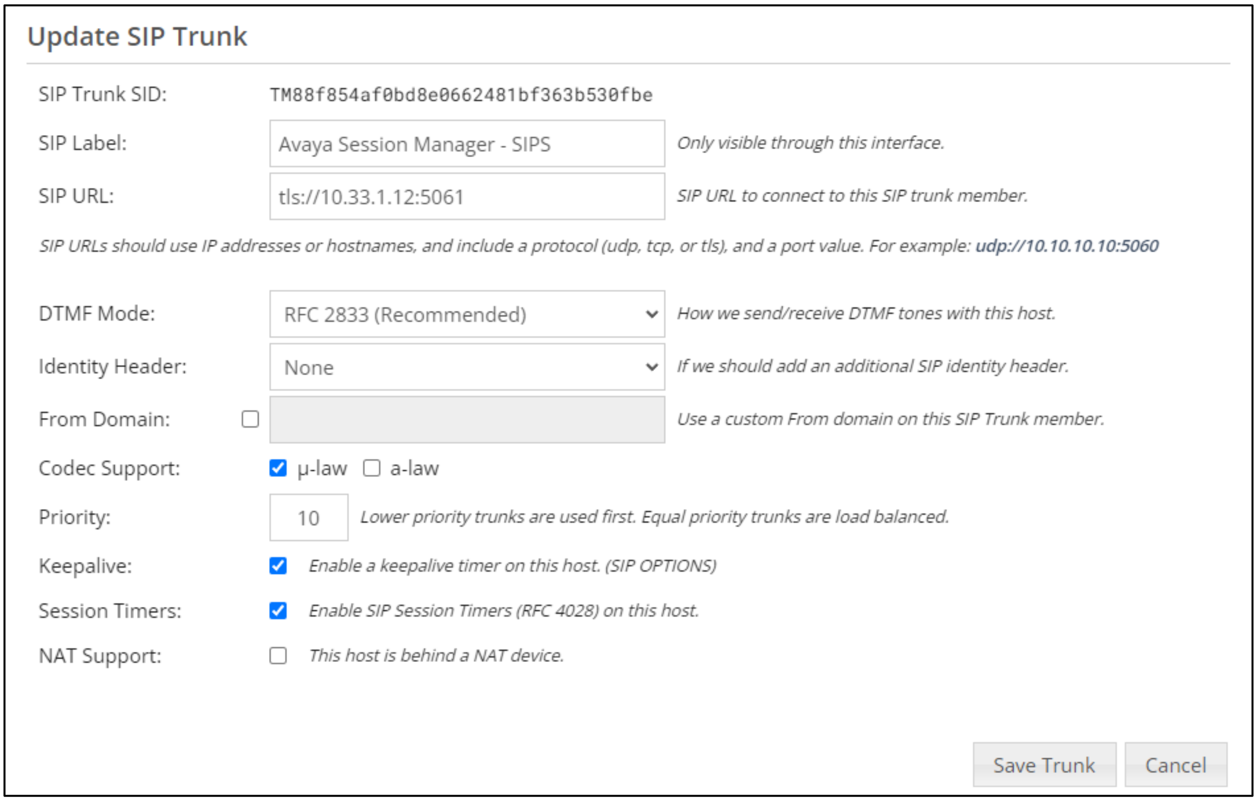
Under the **Members** tab in this new SIP trunk group, click the **Add New Member** button (not shown), and the **Add New SIP Trunk** dialog will appear as shown below.

Under **Add New SIP Trunk**:

- **SIP URL**: The IP address of Session Manager formatted as a fully qualified URL, defining the protocol and SIP port.
- **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 an 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 IP address of Session Manager, formatted as a fully qualified URL, defining the protocol and SIP port, then click the **Save Trunk** button. During compliance testing, the protocol **TLS** and port **5061** is used for the SIP service with Session Manager, and the default values for the remaining SIP trunk group member settings.



Update SIP Trunk

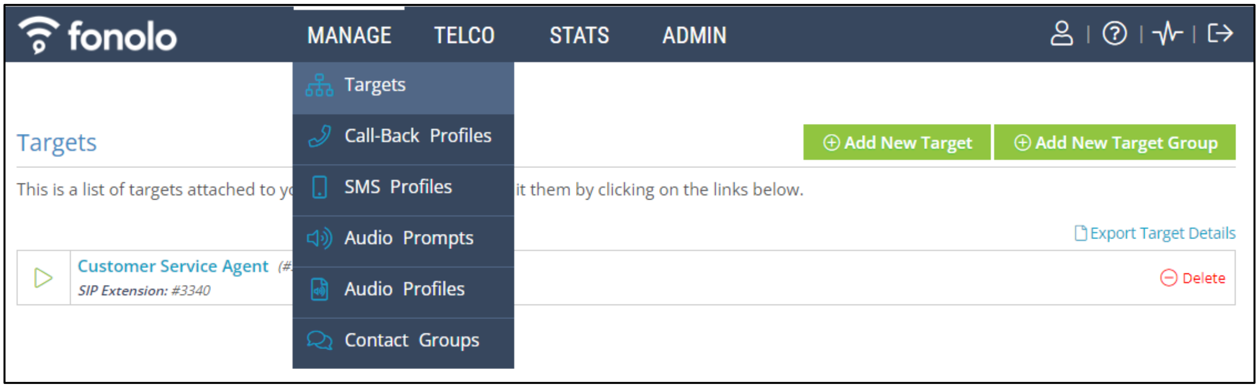
SIP Trunk SID:	TM88f854af0bd8e0662481bf363b530fbe	
SIP Label:	Avaya Session Manager - SIPS	*Only visible through this interface.*
SIP URL:	tls://10.33.1.12:5061	*SIP URL to connect to this SIP trunk member.*

SIP URLs should use IP addresses or hostnames, and include a protocol (udp, tcp, or tls), and a port value. For example: ***udp://10.10.10.10:5060***

DTMF Mode:	RFC 2833 (Recommended)	*How we send/receive DTMF tones with this host.*
Identity Header:	None	*If we should add an additional SIP identity header.*
From Domain:	□	*Use a custom From domain on this SIP Trunk member.*
Codec Support:	☑ µ-law □ a-law	
Priority:	10	*Lower priority trunks are used first. Equal priority trunks are load balanced.*
Keepalive:	☑	*Enable a keepalive timer on this host. (SIP OPTIONS)*
Session Timers:	☑	*Enable SIP Session Timers (RFC 4028) on this host.*
NAT Support:	□	*This host is behind a NAT device.*

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 (shown below) for **Dial Method** and enter the VDN to reach the pertinent skillset via Session Manager in the **Extension** field.

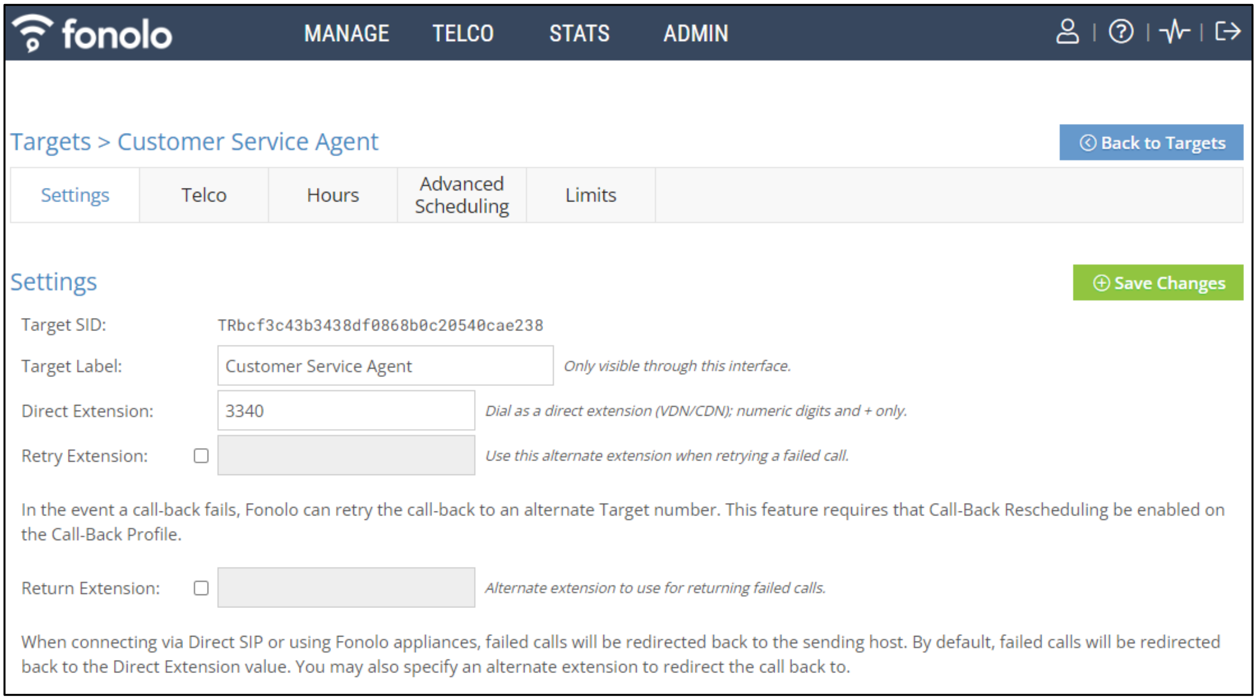


Targets

This is a list of targets attached to y… …it them by clicking on the links below.

Customer Service Agent (#…
SIP Extension: #3340

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



Targets > Customer Service Agent

Settings

Target SID: TRbcf3c43b3438df0868b0c20540cae238

Target Label: Customer Service Agent — *Only visible through this interface.*

Direct Extension: 3340 — *Dial as a direct extension (VDN/CDN); numeric digits and + only.*

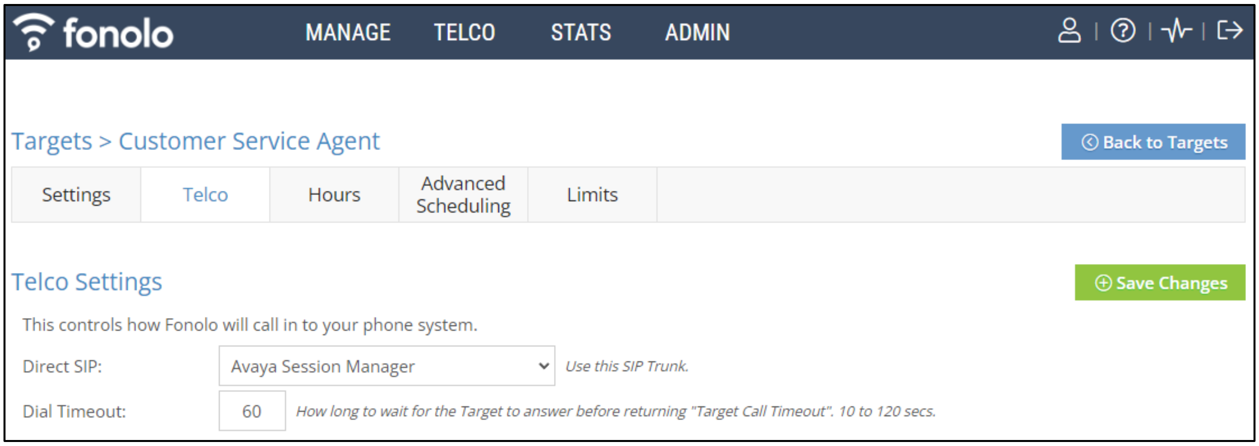
Retry Extension: ☐ — *Use this alternate extension when retrying a failed call.*

In the event a call-back fails, Fonolo can retry the call-back to an alternate Target number. This feature requires that Call-Back Rescheduling be enabled on the Call-Back Profile.

Return Extension: ☐ — *Alternate extension to use for returning failed calls.*

When connecting via Direct SIP or using Fonolo appliances, failed calls will be redirected back to the sending host. By default, failed calls will be redirected back to the Direct Extension value. You may also specify an alternate extension to redirect the call back to.

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 Session Manger** SIP trunk, added in **Section** Error! Reference source not found., and then click the **Save Changes** button.



Targets > Customer Service Agent

Telco Settings

This controls how Fonolo will call in to your phone system.

Direct SIP: Avaya Session Manager — *Use this SIP Trunk.*

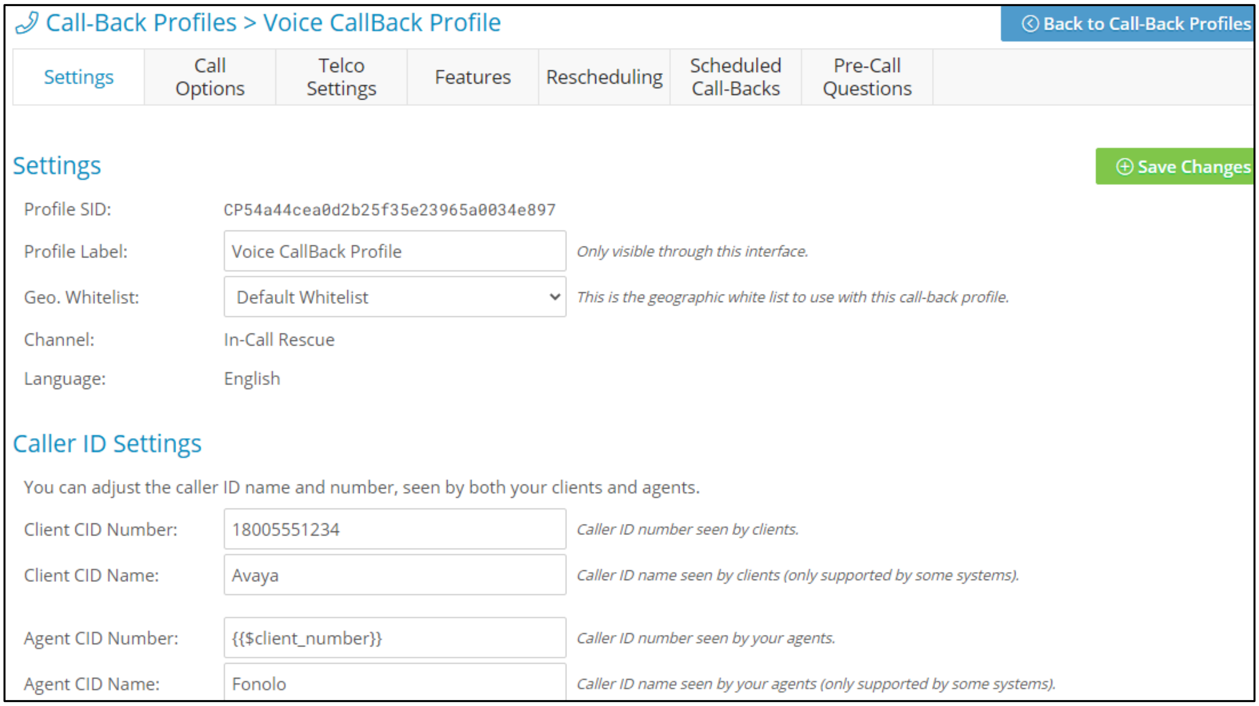
Dial Timeout: 60 — *How long to wait for the Target to answer before returning "Target Call Timeout". 10 to 120 secs.*

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.



Settings

Profile SID: CP54a44cea0d2b25f35e23965a0034e897

Profile Label: Voice CallBack Profile — *Only visible through this interface.*

Geo. Whitelist: Default Whitelist — *This is the geographic white list to use with this call-back profile.*

Channel: In-Call Rescue

Language: English

Caller ID Settings

You can adjust the caller ID name and number, seen by both your clients and agents.

Client CID Number: 18005551234 — *Caller ID number seen by clients.*

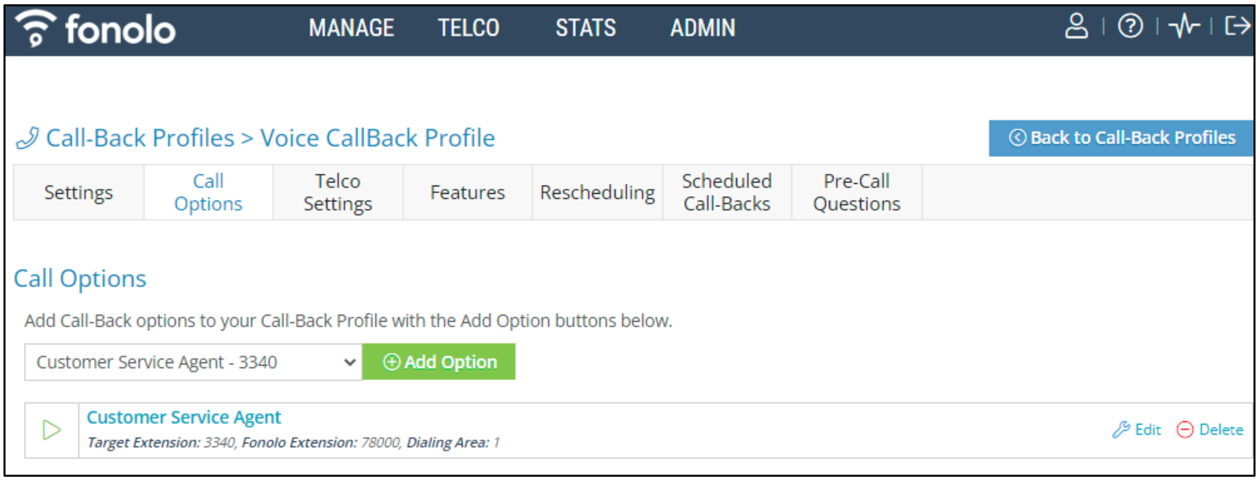
Client CID Name: Avaya — *Caller ID name seen by clients (only supported by some systems).*

Agent CID Number: {{$client_number}} — *Caller ID number seen by your agents.*

Agent CID Name: Fonolo — *Caller ID name seen by your agents (only supported by some systems).*

From the **Call Options** section of the new **Call-Back Profile**, select the Target added in **Section 8.2** (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.



Call Options

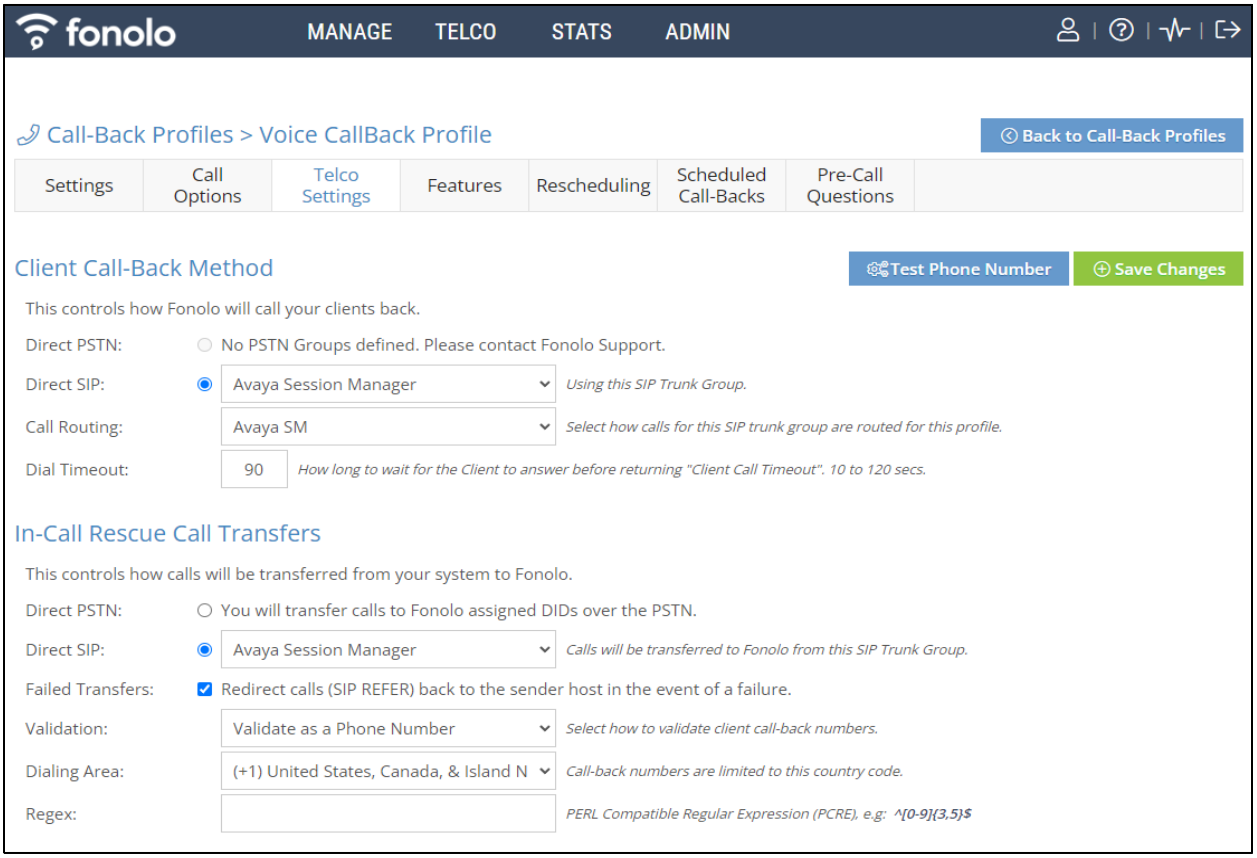
Add Call-Back options to your Call-Back Profile with the Add Option buttons below.

Customer Service Agent - 3340

Customer Service Agent

Target Extension: 3340, Fonolo Extension: 78000, Dialing Area: 1

From the **Telco Settings** section of the new **Call-Back Profile**, select the **Avaya Session Manager** 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.



Call-Back Profiles > Voice CallBack Profile

Back to Call-Back Profiles

Settings | Call Options | Telco Settings | Features | Rescheduling | Scheduled Call-Backs | Pre-Call Questions

Client Call-Back Method

Test Phone Number | Save Changes

This controls how Fonolo will call your clients back.

Direct PSTN: ○ No PSTN Groups defined. Please contact Fonolo Support.

Direct SIP: ● Avaya Session Manager — *Using this SIP Trunk Group.*

Call Routing: Avaya SM — *Select how calls for this SIP trunk group are routed for this profile.*

Dial Timeout: 90 — *How long to wait for the Client to answer before returning "Client Call Timeout". 10 to 120 secs.*

In-Call Rescue Call Transfers

This controls how calls will be transferred from your system to Fonolo.

Direct PSTN: ○ You will transfer calls to Fonolo assigned DIDs over the PSTN.

Direct SIP: ● Avaya Session Manager — *Calls will be transferred to Fonolo from this SIP Trunk Group.*

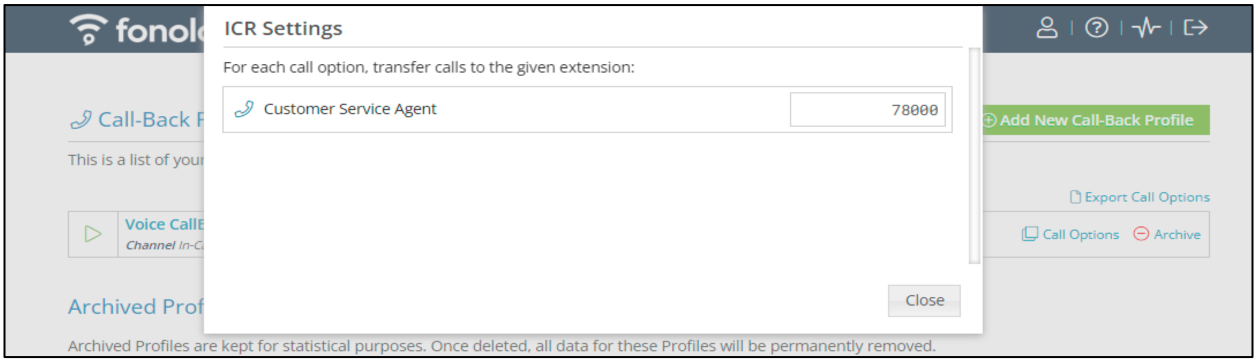
Failed Transfers: ☑ Redirect calls (SIP REFER) back to the sender host in the event of a failure.

Validation: Validate as a Phone Number — *Select how to validate client call-back numbers.*

Dialing Area: (+1) United States, Canada, & Island N — *Call-back numbers are limited to this country code.*

Regex: — *PERL Compatible Regular Expression (PCRE), e.g: **^[0-9]{3,5}$***

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** was configured on the Fonolo system.



ICR Settings

For each call option, transfer calls to the given extension:

Customer Service Agent — 78000

Close

Archived Profiles are kept for statistical purposes. Once deleted, all data for these Profiles will be permanently removed.

9. Verification Steps

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

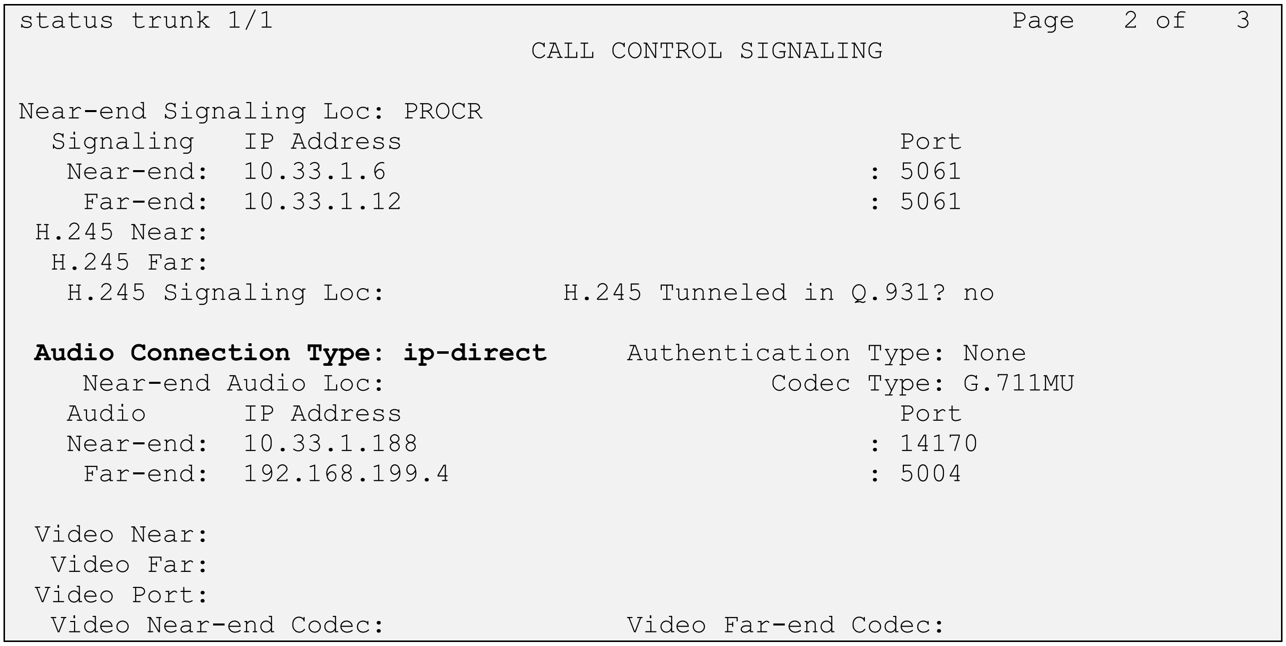
```
status trunk 1

                             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.

- PSTN caller can select the call back option and get redirected to VCB via Communication Manager/Session Manager.
- 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.

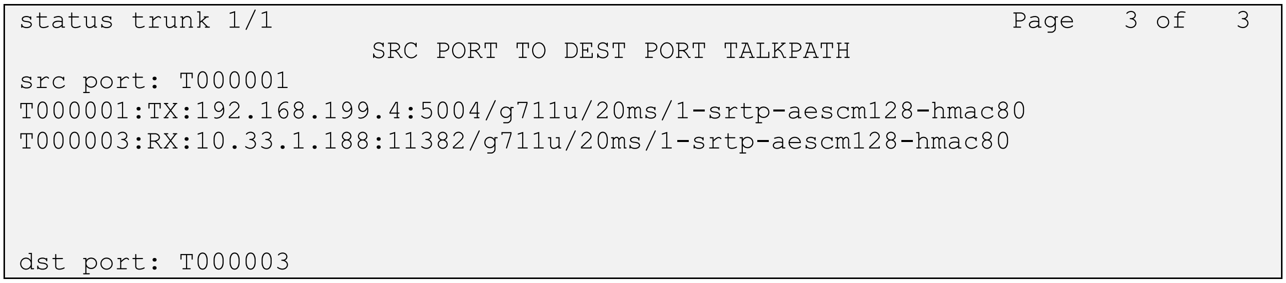
- As soon as VCB connects to an available agent, it calls out to the PSTN caller and connects them to the agent.

The Following screenshots show the connection type as “ip-direct” between SIP agent telephone and VCB appliance.



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

Near-end Signaling Loc: PROCR
  Signaling   IP Address                              Port
   Near-end:  10.33.1.6                             : 5061
    Far-end:  10.33.1.12                            : 5061
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.711MU
   Audio      IP Address                              Port
   Near-end:  10.33.1.188                           : 14170
    Far-end:  192.168.199.4                         : 5004

 Video Near:
  Video Far:
 Video Port:
  Video Near-end Codec:               Video Far-end Codec:
```

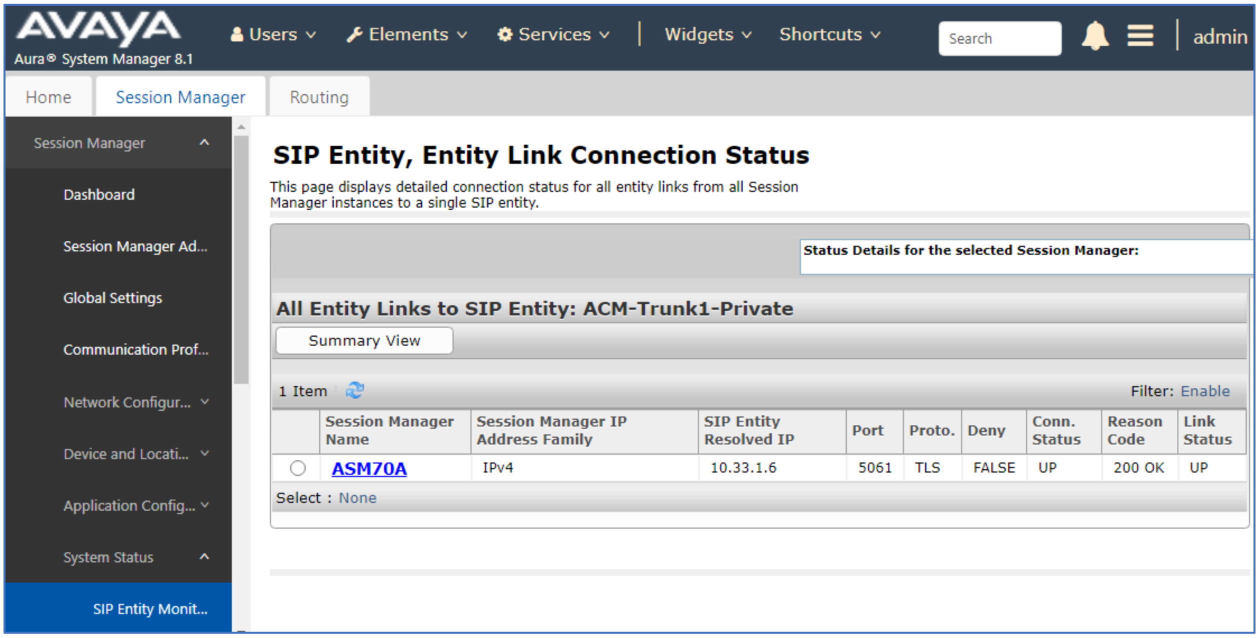
The following screen shows that SRTP was used for the call.



```
status trunk 1/1                                              Page   3 of   3
                      SRC PORT TO DEST PORT TALKPATH
src port: T000001
T000001:TX:192.168.199.4:5004/g711u/20ms/1-srtp-aescm128-hmac80
T000003:RX:10.33.1.188:11382/g711u/20ms/1-srtp-aescm128-hmac80




dst port: T000003
```

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**.



SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: ACM-Trunk1-Private

Summary View

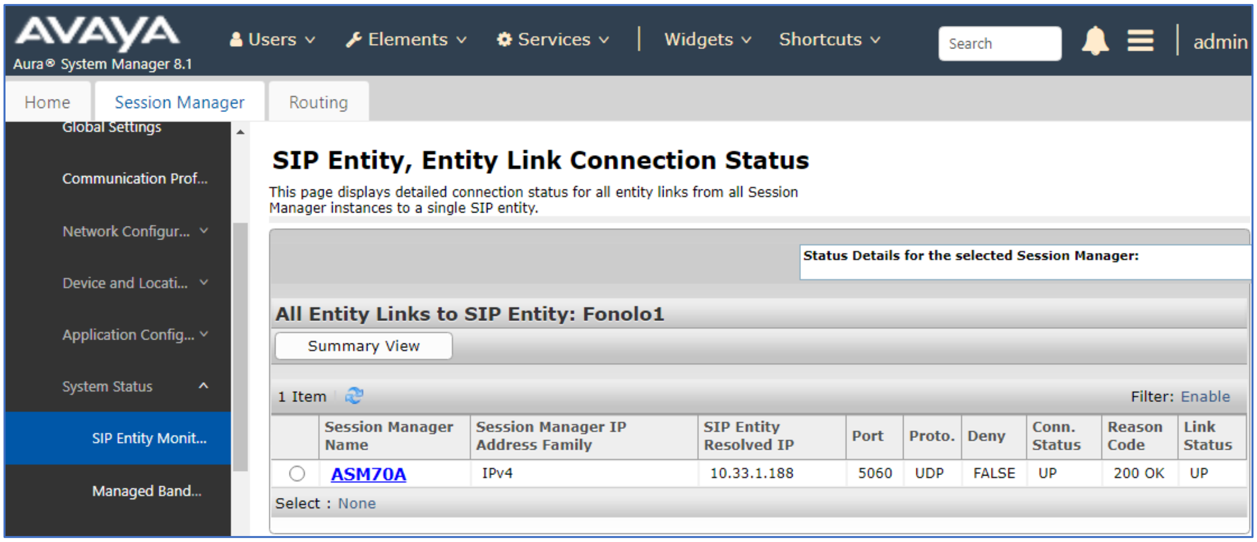
1 Item

Filter: Enable

	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	ASM70A	IPv4	10.33.1.6	5061	TLS	FALSE	UP	200 OK	UP

Select : None

Repeat the same procedure selecting each Fonolo VCB SIP Entity and verify the **Link Status** is **Up**.



SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: Fonolo1

Summary View

1 Item

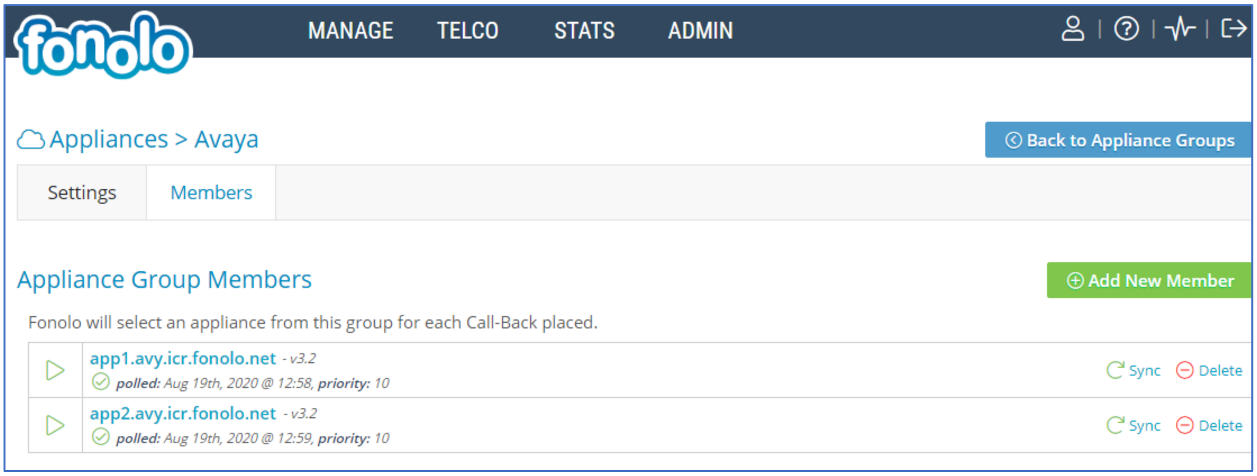
Filter: Enable

	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	ASM70A	IPv4	10.33.1.188	5060	UDP	FALSE	UP	200 OK	UP

Select : None

9.3. Verify Fonolo Voice Call-Back

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



Appliances > Avaya

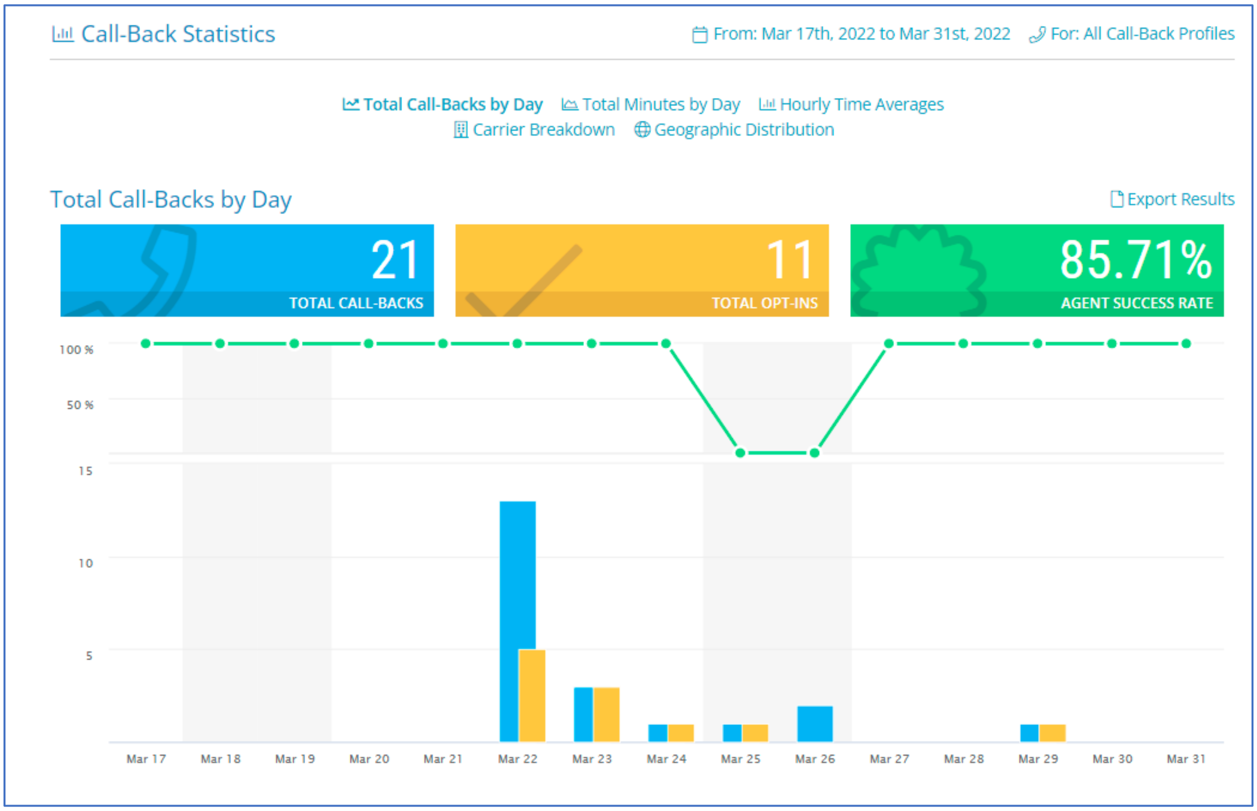
Appliance Group Members

Fonolo will select an appliance from this group for each Call-Back placed.

app1.avy.icr.fonolo.net - *v3.2*
polled: Aug 19th, 2020 @ 12:58, priority: 10

app2.avy.icr.fonolo.net - *v3.2*
polled: Aug 19th, 2020 @ 12:59, priority: 10

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



Call-Back Statistics

From: Mar 17th, 2022 to Mar 31st, 2022 For: All Call-Back Profiles

Total Call-Backs by Day

21 TOTAL CALL-BACKS

11 TOTAL OPT-INS

85.71% AGENT SUCCESS RATE

10. Conclusion

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP TLS. All feature and serviceability test cases were completed and passed with the exceptions/observations noted in **Section** Error! Reference source not found..

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, March 2021
2. *Administering Avaya Aura® Session Manager*, Release 8.1, Issue 3, March 2021
3. *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.1.x, Issue 4, March 2021
4. *Administering Avaya Aura® System Manager for Release 8.1*, Release 8.1.x, Issue 5, March 2021

Avaya Aura® Communication Manager

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

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.