Avaya Solution & Interoperability Test Lab

Application Notes for configuring Fonolo In-Call Rescue with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Fonolo In-Call Rescue application to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager 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 In-Call Rescue (ICR) to interoperate with Avaya Aura® Communication Manager (Communication Manager) via Avaya Aura® Session Manager (Session Manager) using SIP trunks. ICR provides functionality to replace hold-time with a call-back and during this compliance tesing was hosted on the cloud by Fonolo. The solution communicates via SIP/RTP. The ICR 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 ICR application. The ICR is a call center 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 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 ICR via Session Manager SIP trunks where ICR then provides a message to the caller to leave a call back number, so that ICR can call back the caller when an agent becomes available. Once ICR receives the confirmed call back number from the caller, ICR uses 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, ICR 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, ICR then calls the caller via SIP trunks to Communication Manager and connects the caller with the available agent. When ICR 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 ICR 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 and ICR. 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 the Call Center within Communication Manager was used. The assumption was made during compliance testing in the vector script to direct callers to ICR when no agents are available. When a caller connected with ICR, ICR read the call back number of the caller or asked caller to input a new call back number. ICR 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 caller and ICR is completed. ICR then called into the call center VDN and connected with an available agent. ICR provided a recording informing the agent of a call in waiting and if the agent wants to get connected to the PSTN caller. The agent accepted the call by using DTMF input. ICR then made the second outbound call to the PSTN caller via Communicaton 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 ICR.

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 ICR application is hosted in a cloud environment by Fonolo. SIP trunks were used to connect the ICR application with Communication Manager via Session Manager. The following features and functionality were covered during compliance testing:

- Establishment of SIP trunks connectivity between ICR 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 ICR application via the SIP trunks based on vector scripting. Outgoing calls from ICR to the VDN via Session Manager when callers decide on Call back. During this compliance testing the Call Center of Communication Manager was used and is not the scope of these Application Notes.
- The ICR application can make outbound call to the caller via Communication Manager who had selected the call back option and merge the call between the caller and 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 ICR.
- User-to-User Information (UUI) is sent from Communication Manager to ICR and that the same information is sent back to the agent from ICR.

Serviceability testing focused on verifying the ability of ICR to recover from adverse conditions, such as the SIP trunks 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:

- ICR only supports G.711u codec.
- ICR only supports RFC2833 for DTMF transmission.
- During this compliance testing, for testing of Direct IP-IP Media (shuffling), it was ensured that Avaya Deskphones were configured such that the ICR application in the cloud can contact them for RTP stream.
- ICR needs to receive 183 early media so that it can provide a ringback tone to the agent before they are connected to the PSTN, else agents will hear silence when the call is being connected to PSTN. This condition was not experienced during compliance testing however Fonolo suggested this as a best practice.

2.3. Support

Technical support on Fonolo ICR 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 ICR with Communication Manager via Session Manager. Communication Manager is connected to an emulated PSTN using T1/PRI. 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 ICR via the Session Manager.

During compliance testing inbound calls to Fonolo were sent to two of Fonolo's specific servers and outbound calls from Fonolo came from four of Fonolo's other servers. This architecture was implemented by Fonolo due to some PBX vendors being unable to support inbound and outbound calls on the same SIP trunk. Due to this design intent of Fonolo, inbound and outbound calls to and from Fonolo were handled by different servers. All these servers were hosted on the cloud by Fonolo.

The following values were configured during compliance testing:

- VDN: 56004
- Vector: 2
- SkillSet: 1
- Agent Login ID: 1000, 1001

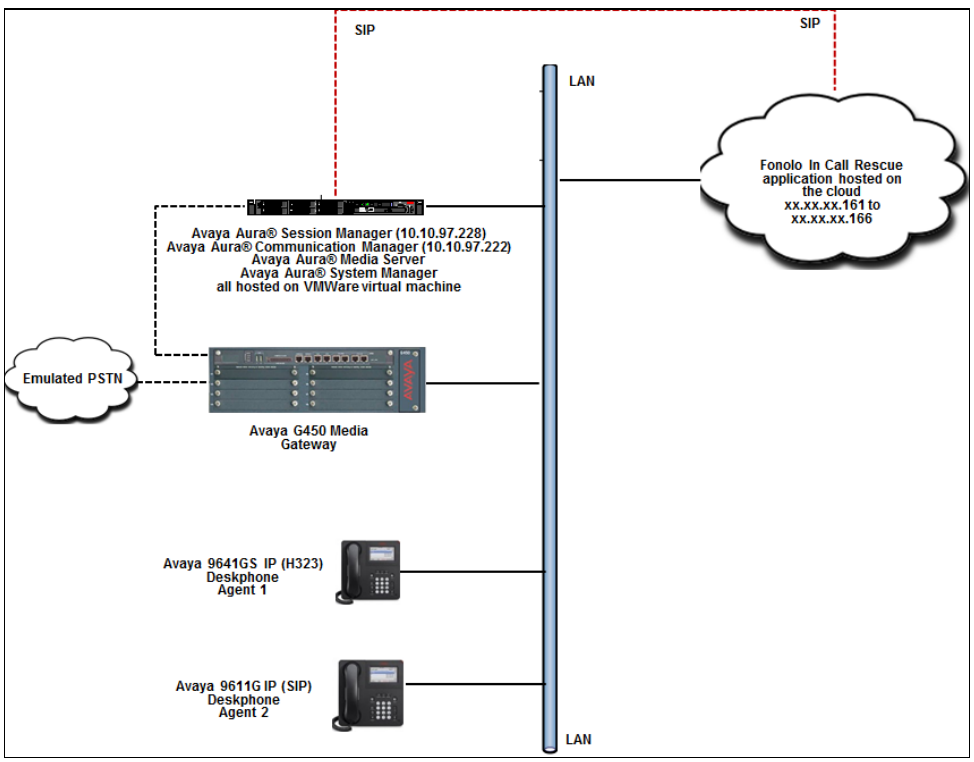


Figure 1: Reference Configuration

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 server	08.0.0.0.822
Avaya Aura® Media Server running on virtual server	8.0.0.117
Avaya G450 Media Gateway	40.10.0/1
Avaya Aura® System Manager running on virtual server	8.0.0.0.931077
Avaya Aura® Session Manager running on virtual server	8.0.0.0.800035
Avaya IP Deskphones - 9641GS (H.323) - 9611G (SIP)	 6.6604 7.1.3.0.8
Fonolo In-Call Rescue hosted on a cloud	Version 3.2

5. Configure Avaya Aura® Communication Manager

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

- Verify Communication Manager License
- Administer SIP Trunk Group
- Administer IP Node Names
- Administer SIP Signaling Group
- Administer SIP Trunk Group Members
- Administer IP Network Region
- Administer IP Codec Set
- Administer Route Pattern
- Administer Private Numbering
- Administer Dial Plan
- Administer Uniform Dial Plan
- Administer AAR Analysis
- Sample Vector

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 Avaya Aura® Communication Manager License

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

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

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 10
           Maximum Concurrently Registered IP Stations: 18000 5
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 0
                   Maximum Video Capable IP Softphones: 18000 1
                       Maximum Administered SIP Trunks: 30000 34
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 688   0
```

5.2. 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:** “sip”.
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”.

```
add trunk-group 1                                           Page   1 of  22
                                TRUNK GROUP

Group Number: 1                 Group Type: sip             CDR Reports: y
  Group Name: Trunk to SM on VM        COR: 1        TN: 1          TAC: #001
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: tie                      Auth Code? n
                                           Member Assignment Method: auto
                                                    Signaling Group: 1
                                                  Number of Members: 24
```

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

```
add trunk-group 1                                             Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y


                     Numbering Format: private
                                              UUI Treatment: shared
                                            Maximum Size of UUI Contents: 128
                                               Replace Restricted Numbers? n
                                              Replace Unavailable Numbers? n

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

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   5 of  22
                              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? n
                                   Support Request History? y
                              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
```

5.3. Administer IP Node Names

Use the “change node-names ip” command (not shown) and add an entry for Session Manager. In this case, **SM-VM** and **10.10.97.228** are entered as **Name** and **IP Address**. Note the **procr** and **10.10.97.222** entry, which is the node **Name** and **IP address** for the processor board. These values will be used later to configure the SIP trunk to Session Manager in **Section 5.4**.

```
change node-names ip
                                  IP NODE NAMES
    Name                  IP Address
SM-VM                   10.10.97.228
procr                   10.10.97.222
```

5.4. 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:** "sip".
- **Transport Method:** "tls".
- **Near-end Node Name:** An existing C-LAN node name or "procr" from **Section 5.3**.
- **Far-end Node Name:** The existing node name for Session Manager from **Section 5.3**.
- **Near-end Listen Port:** An available port for integration with Session Manager.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** An existing network region to use with Session Manager.
- **Far-end Domain:** The applicable domain name for the network.
- **Direct IP-IP Audio Connections?:** "y".
- **Initial IP-IP Direct Media?:** "y".

```
display 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? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                    Far-end Node Name: SM-VM
 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? y
         Enable Layer 3 Test? y                      Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n               Alternate Route Timer(sec): 6
```

5.5. Administer SIP Trunk Group Members

Use the "change trunk-group n" command, where "n" is the trunk group number from **Section 5.2**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Signaling Group:** The signaling group number from **Section 5.44**.
- **Number of Members:** The desired number of members, in this case "24".

```
change trunk-group 1                                            Page   1 of  22
                                TRUNK GROUP

Group Number: 1                    Group Type: sip          CDR Reports: y
  Group Name: Trunk to SM on VM           COR: 1        TN: 1        TAC: #001
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                            Member Assignment Method: auto
                                                     Signaling Group: 1
                                                   Number of Members: 24
```

5.6. 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 5.44**.

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 ICR.

```
change ip-network-region 1                                      Page   1 of  20
                              IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: bvwdev.com
    Name: Region1               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
```

Navigate to **Page 4**, and specify this codec set to be used for calls with network regions used by Avaya endpoints and by the trunk to the PSTN. In the compliance testing, network region "1" was used by the Avaya endpoints and by the trunk to the PSTN.

```
change ip-network-region 1                                      Page   4 of  20

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

5.7. Administer IP Codec Set

Use the "change ip-codec-set n" command, where "n" is the codec set number from **Section 5.66**. Update the audio codec types in the **Audio Codec** fields as necessary. As per the observation noted in **Section 2.2** only configure G.711MU. The codec shown below was used in the compliance testing.

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

                          IP CODEC SET
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2:
Media Encryption                   Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3: none
```

5.8. Administer Route Pattern

Use the "change route-pattern n" command, where "n" is an existing route pattern number to be used to reach ICR, in this case "1". Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.2**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1      Pattern Name: To SM on VM
    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                    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  none
```

5.9. Administer Private Numbering

Use the "change private-numbering 0" command, to define the calling party number to send to ICR. Add an entry for the trunk group defined in **Section 5.2**. In the example shown below, all calls originating from a 5-digit extension beginning with 56 and routed to trunk group 1 will result in a 5-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
 5  56               1                           5     Total Administered: 4
                                                        Maximum Entries: 540
```

5.10. Administer Dial Plan

This section provides a sample dial plan used for routing calls with dialed digits 30xxx to ICR. Use the “change dialplan analysis 0” command and add an entry to specify the use of digits pattern 30, as shown below.

```
display dialplan analysis                                          Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all            Percent Full: 2

    Dialed    Total  Call      Dialed    Total  Call      Dialed    Total  Call
    String    Length Type      String    Length Type      String    Length Type
   1            4    ext
   30           5    udp
```

5.11. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 30xxx to ICR. 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 30xxx, 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
 30              5   0                    aar   n
```

5.12. Administer AAR Analysis

Use the “change aar analysis 0” command and add an entry to specify how to route calls to 30xxx. In the example shown below, calls with digits 30xxx will be routed as an AAR call using route pattern “1” from **Section 5.88**.

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

          Dialed           Total     Route     Call    Node   ANI
          String          Min  Max   Pattern   Type    Num    Reqd
        30                 5    5      1          aar            n
```

5.13. Sample Vector

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 “30000”, which is the number to dial out to ICR. Also, in “Step 8” a line was added to send UUI information to Fonolo ICR for testing purposes.

```
display vector 2                                                  Page   1 of   6
                                  CALL VECTOR

    Number: 2                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    2   secs hearing ringback
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 56005    for none
08 set          A      = none   CATR   0123456789
09 route-to     number 30000           with cov n if digit           =  1
10 goto step    4             if unconditionally
11 disconnect   after announcement none
12 stop
```

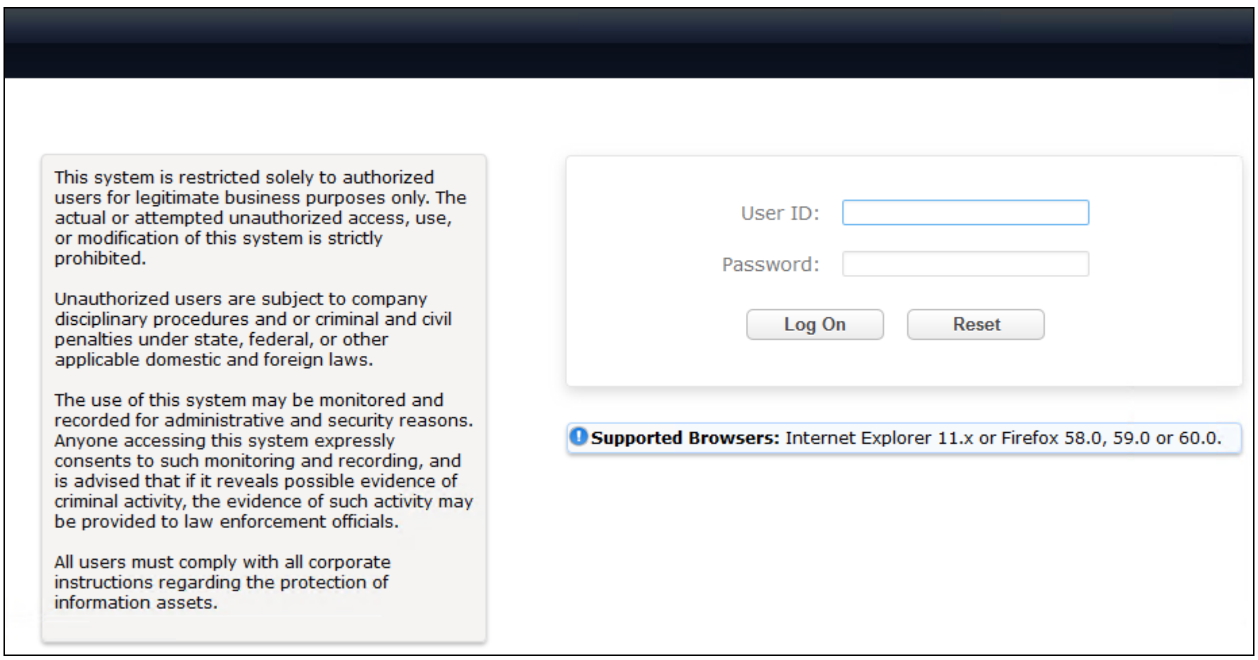
6. Configure Avaya Aura® Session Manager

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

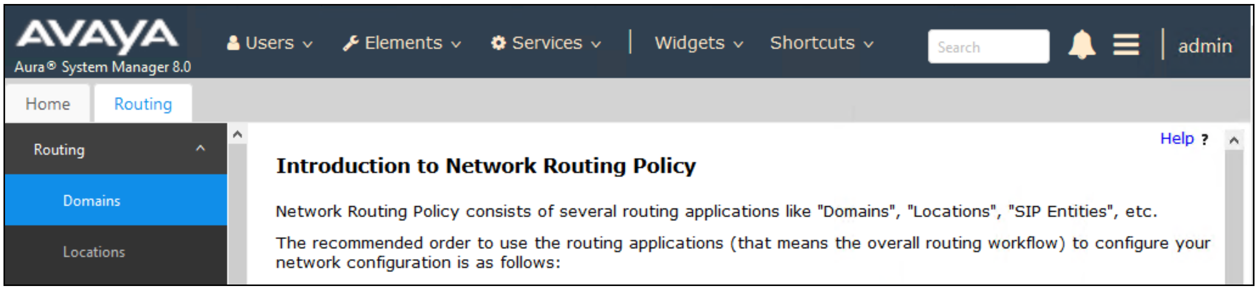
6.1. Launch System Manager

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.

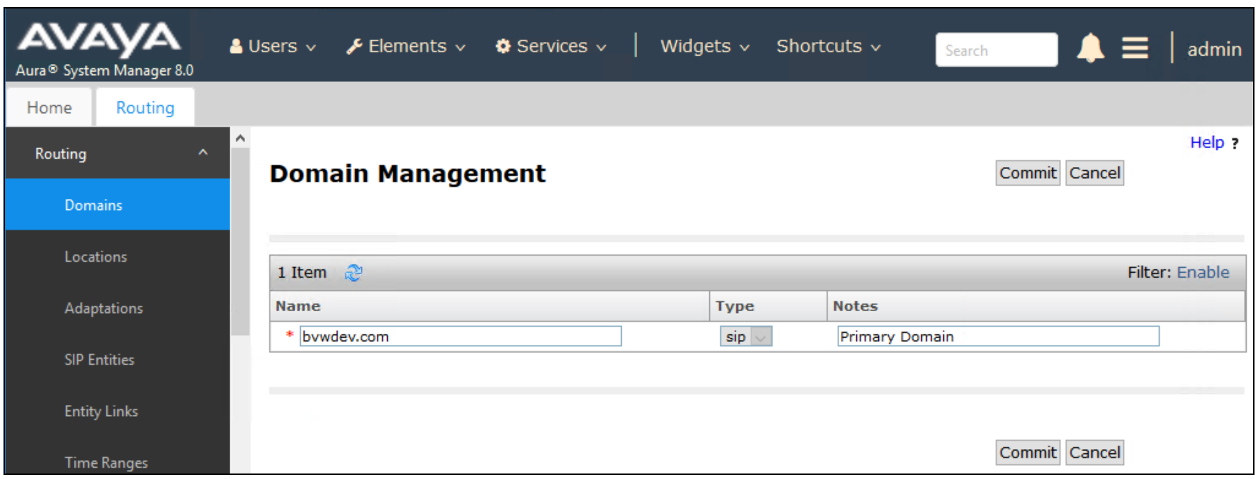


6.2. Administer Domain

In the subsequent screen (not shown), select **Elements → Routing** to display the **Introduction to Network Routing Policy** 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**.

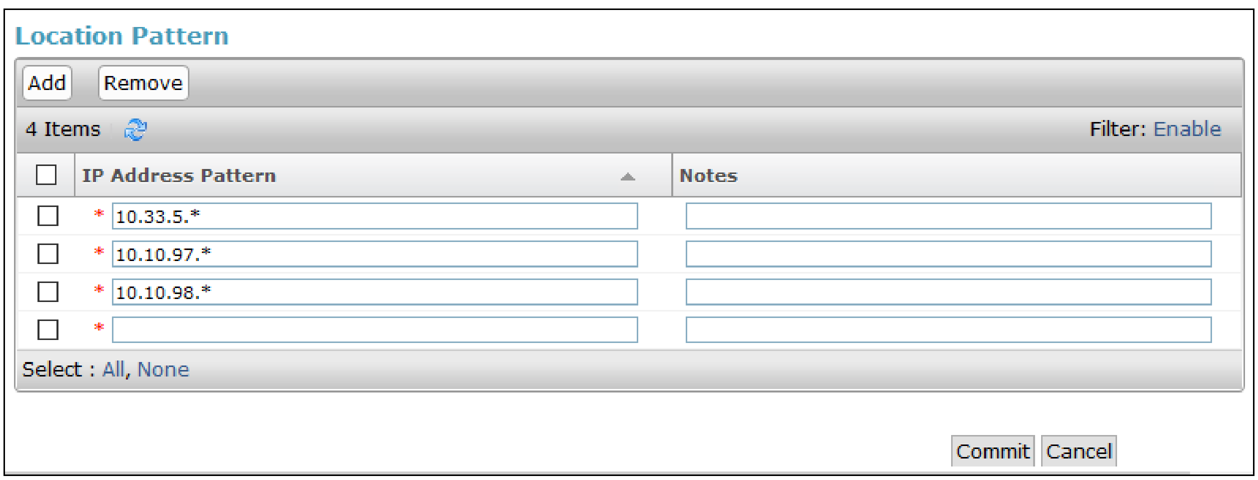


6.3. Administer Locations

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

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.

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.



6.4. Administer SIP Entities

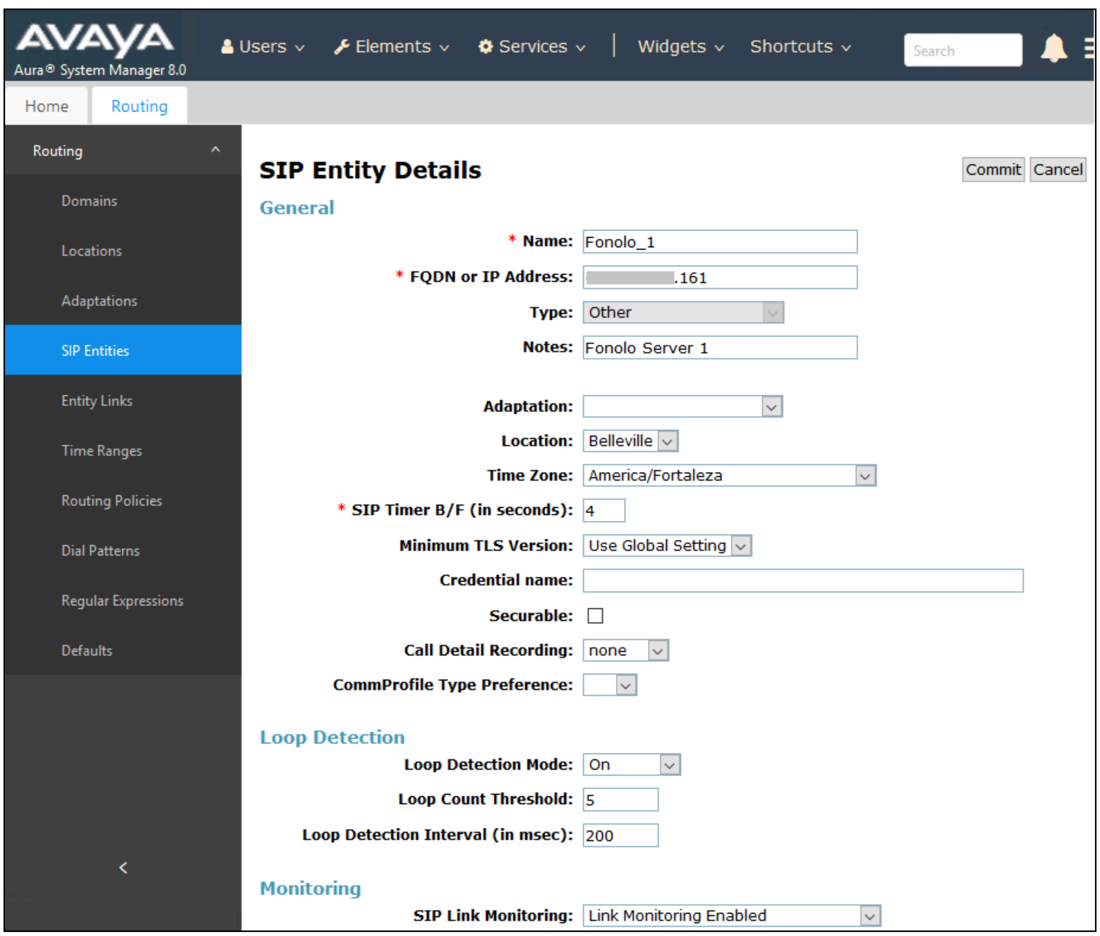
Add seven new SIP entities, six for ICR and one for the new SIP trunks with Communication Manager.

6.4.1. SIP Entity for Fonolo ICR

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

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

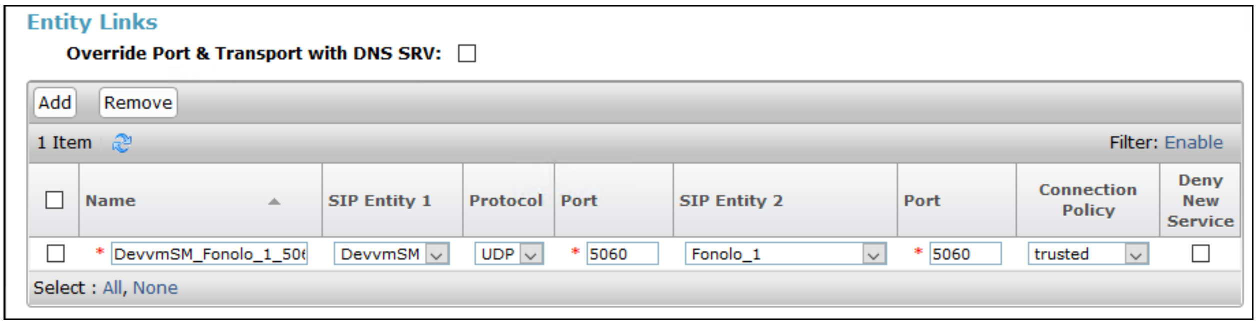
- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of ICR SIP Server.
- **Type:** "Other"
- **Notes:** Any desired notes.
- **Location:** Select the ICR location name from **Section 6.3**.
- **Time Zone:** Select the applicable time zone.
- **SIP Link Monitoring:** Select "Link Monitoring Enabled".



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 “DevvmSM”.
- **Protocol:** “UDP”.
- **Port:** “5060”.
- **SIP Entity 2:** The ICR entity name from this section.
- **Port:** “5060”.
- **Connection Policy:** “trusted”.

Note that only UDP protocol was tested.



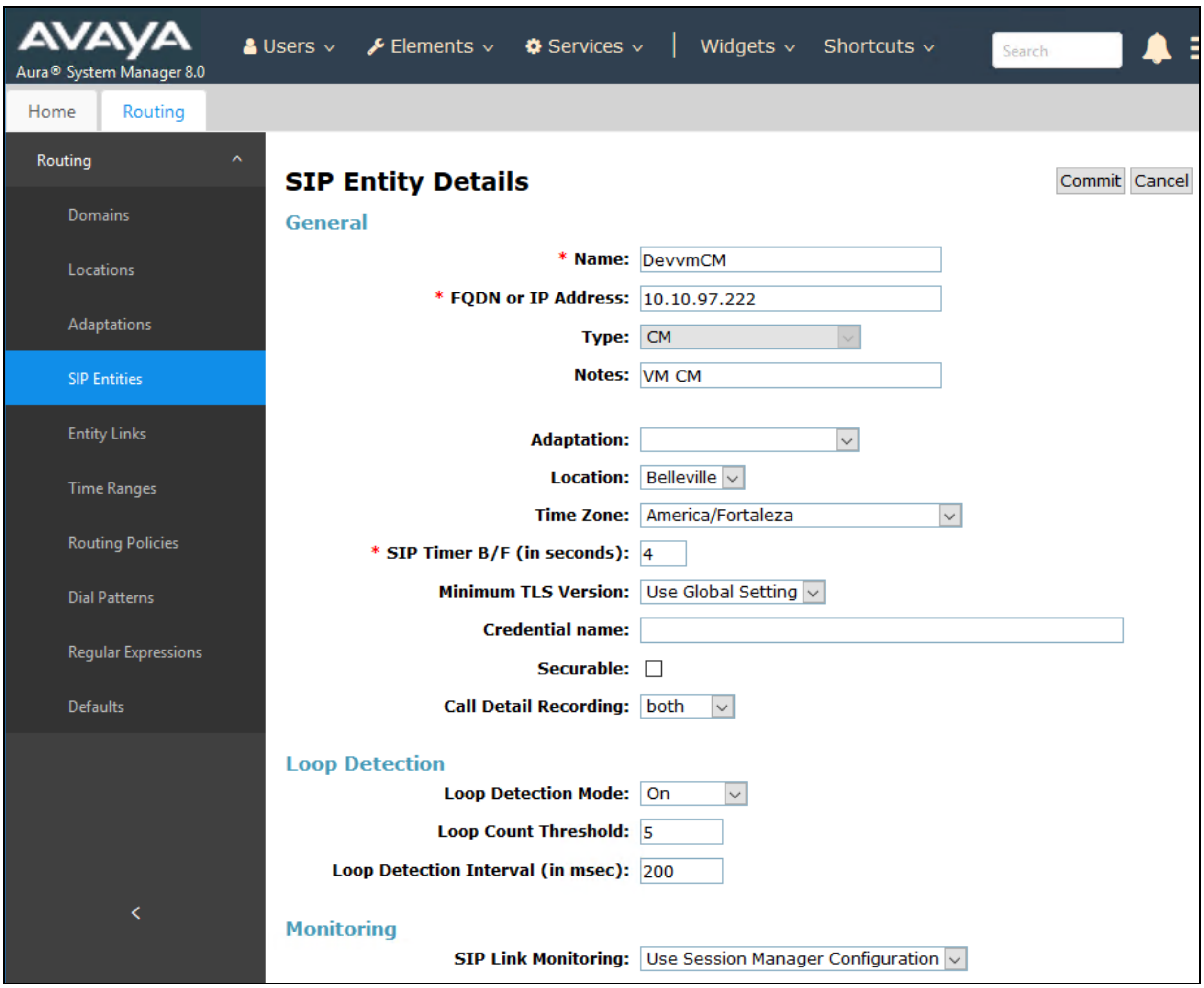
Repeat the above to configure a total of six SIP entities for ICR, since during the compliance testing two were used for outgoing calls from Communication Manager to ICR and four were used for incoming calls from ICR to Communication Manager.

6.4.2. SIP Entity for Avaya Aura® 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 this SIP entity is used for integration with ICR.

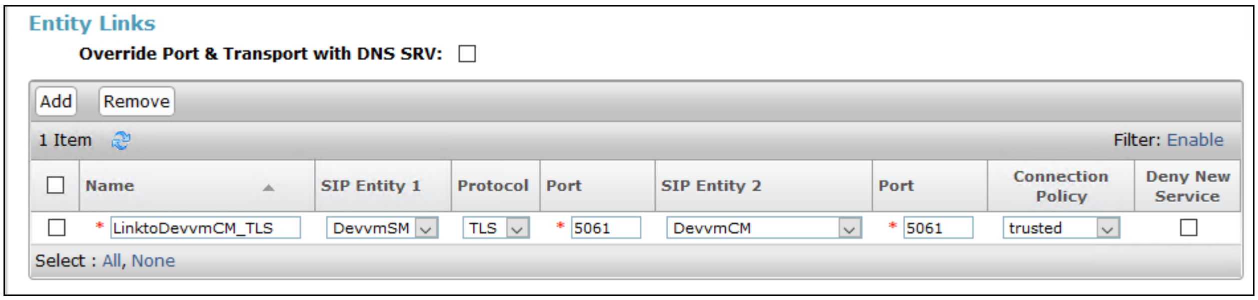
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of an existing CLAN or the processor interface.
- **Type:** "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 “DevvmSM”.
- **Protocol:** The signaling group transport (TLS) method from **Section 5.44**.
- **Port:** The signaling group listen port (5061) number from **Section 5.44**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group listen port (5061) number from **Section 5.44**.
- **Connection Policy:** “trusted”



6.5. Administer Routing Policies

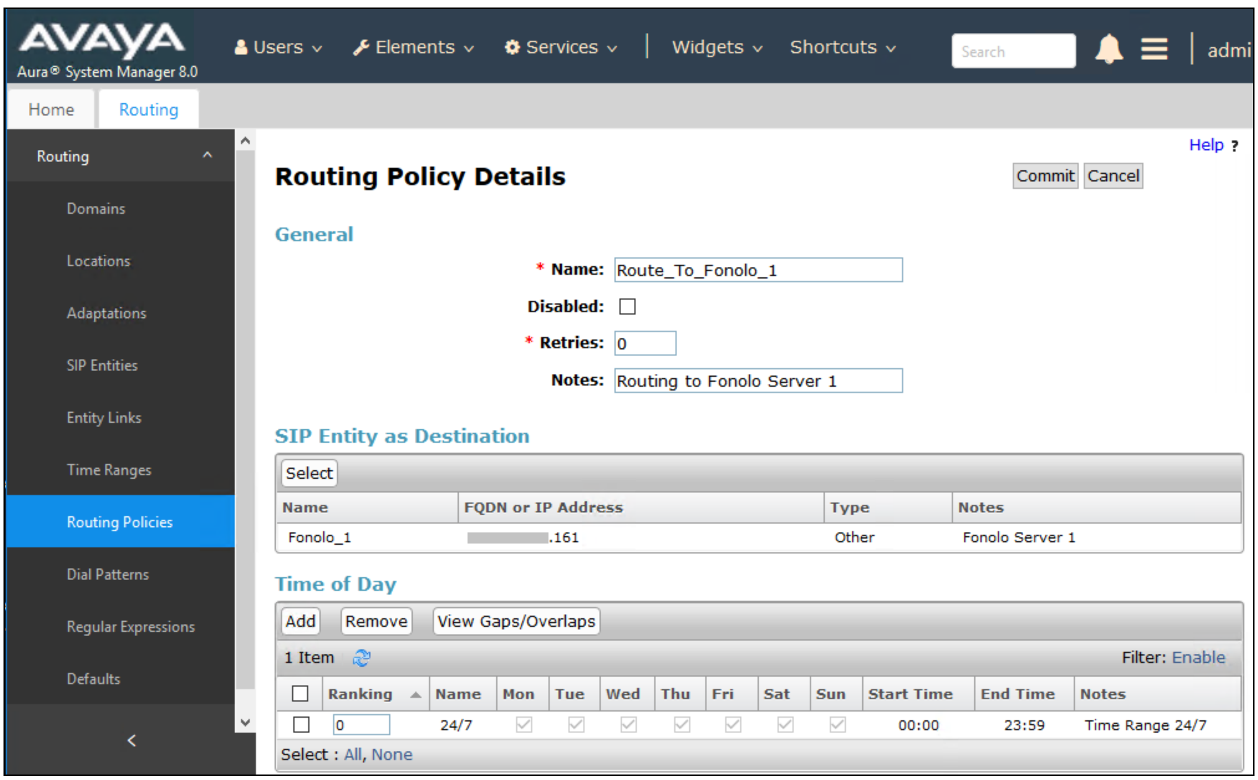
Add two new routing policies, one for ICR and one for the new SIP trunks with Communication Manager.

6.5.1. Routing Policy for Fonolo ICR

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

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 ICR entity name from **Section 6.4.1**. In the **Time of Day** sub-section, enter "0" for **Ranking**. Ranking option is only configured for the two outgoing routing policies of ICR so that calls can be load balanced. The screen below shows the result of the selection.

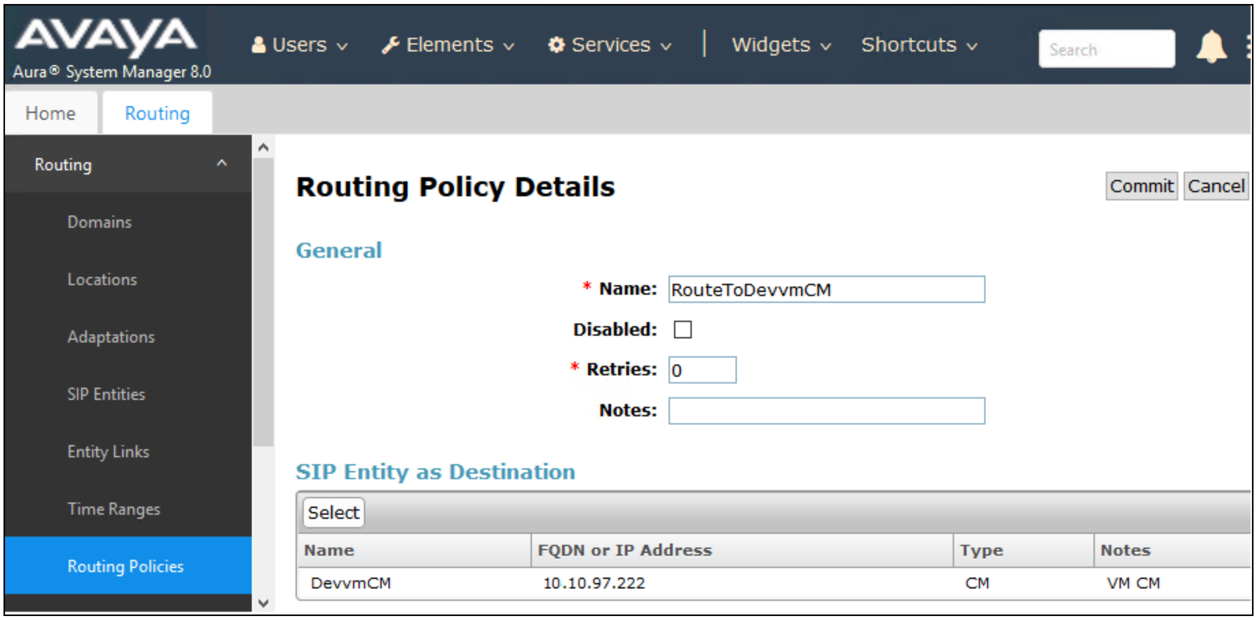


6.5.2. Routing Policy for Avaya Aura® Communication Manager

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 6.4.2**. The screen below shows the result of the selection.



6.6. Administer Dial Patterns

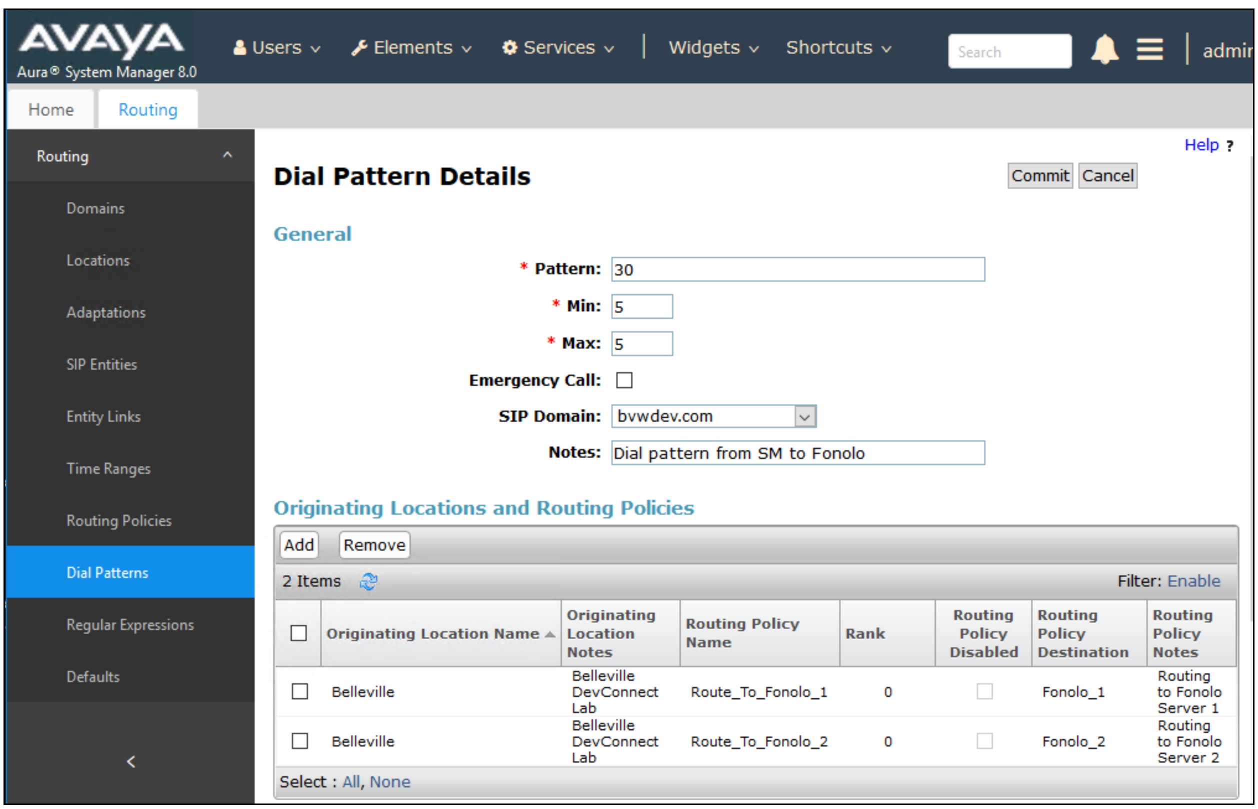
Add a new dial pattern for ICR and Communication Manager.

6.6.1. Dial Pattern for Fonolo ICR

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 ICR. 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 "30".
- **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 5.4**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching ICR. In the compliance testing, the entry allowed for call originations from all Communication Manager endpoints in locations "Belleville". The ICR routing policy from **Section 6.5.1** 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 ICR.

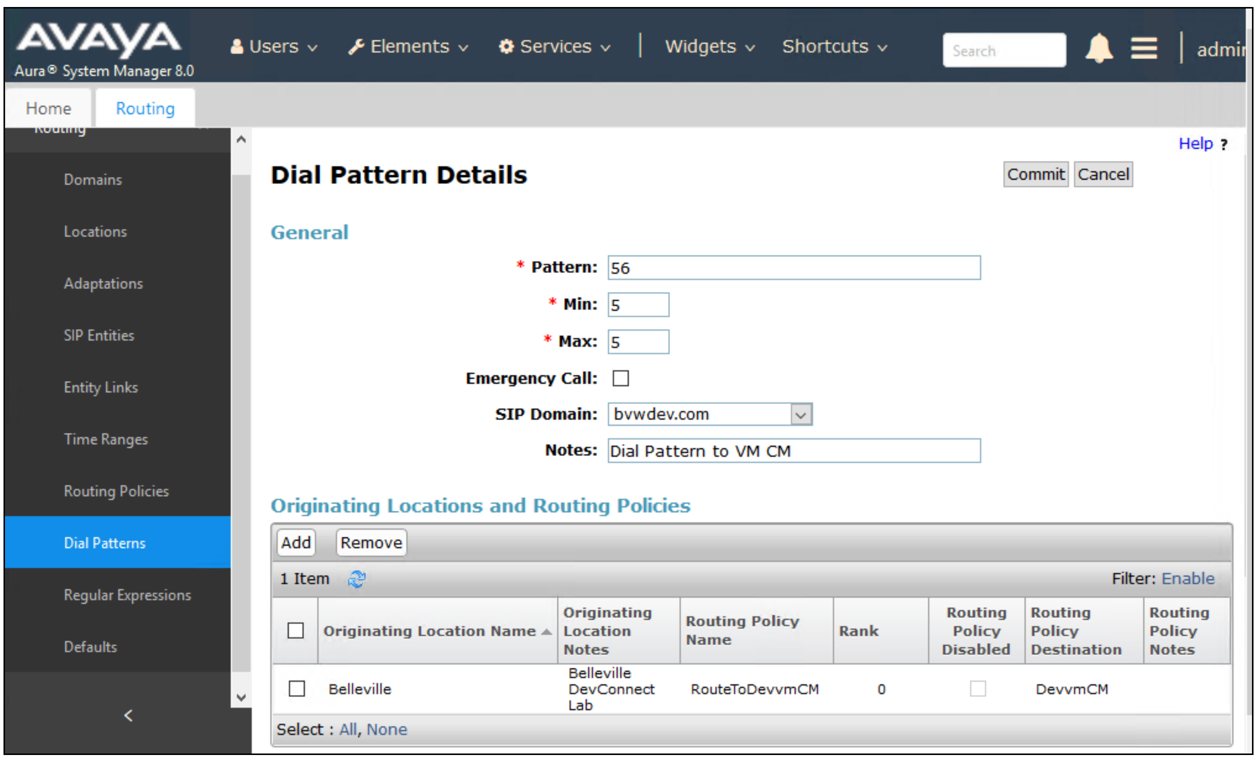


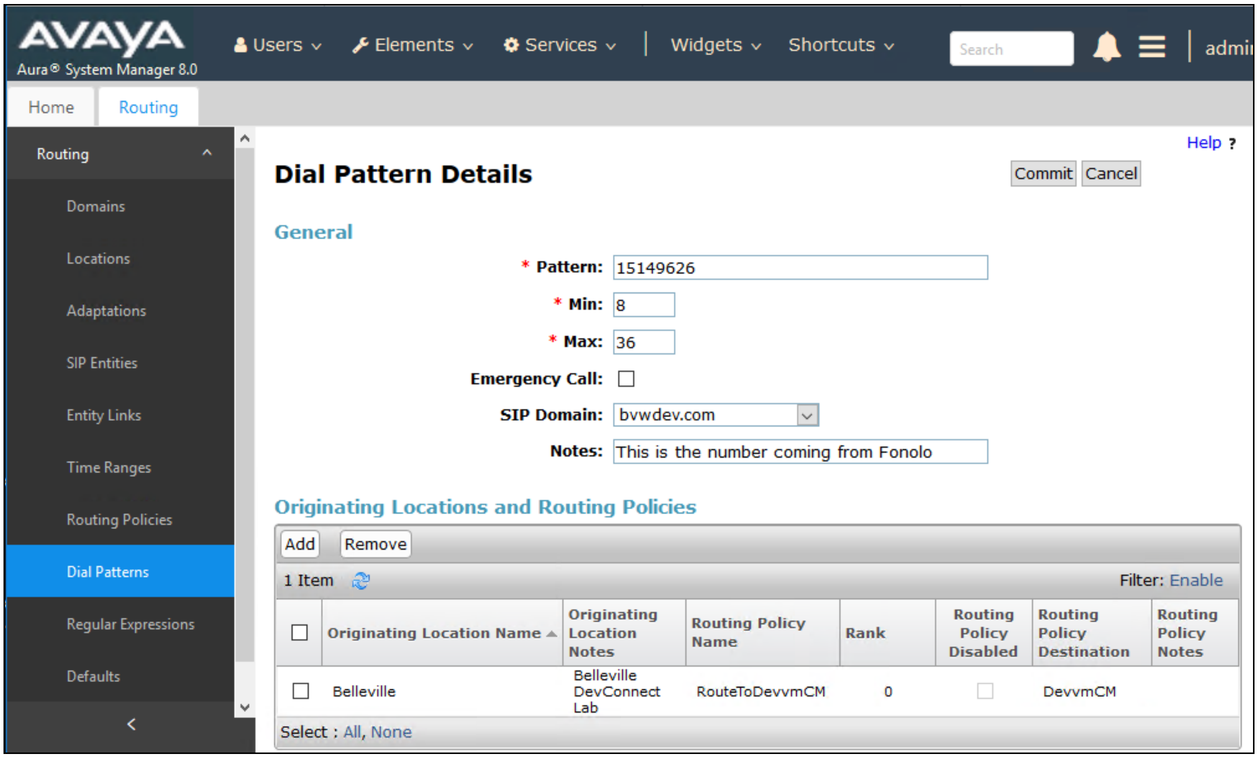
6.6.2. Dial Pattern for Communication Manager

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, in this case "56" and "15149626".
- **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 5.4**.

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




AVAYA
Aura® System Manager 8.0
Users
Elements
Services
Widgets
Shortcuts
Search
admi
Home
Routing
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Help ?
Dial Pattern Details
Commit
Cancel
General
* Pattern: 15149626
* Min: 8
* Max: 36
Emergency Call:
SIP Domain: bvwdev.com
Notes: This is the number coming from Fonolo
Originating Locations and Routing Policies
Add
Remove
1 Item
Filter: Enable
Originating Location Name
Originating Location Notes
Routing Policy Name
Rank
Routing Policy Disabled
Routing Policy Destination
Routing Policy Notes
Belleville
Belleville DevConnect Lab
RouteToDevvmCM
0
DevvmCM
Select : All, None

7. Configure Fonolo In-Call Rescue

This section provides a "snapshot" of ICR configuration used during compliance testing. ICR 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 ICR, available through the Fonolo Customer Portal at https://portal.fonolo.com/. Other configurations are possible. Contact Fonolo for details on how to configure ICR. 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

7.1. Add a New SIP Trunk Group

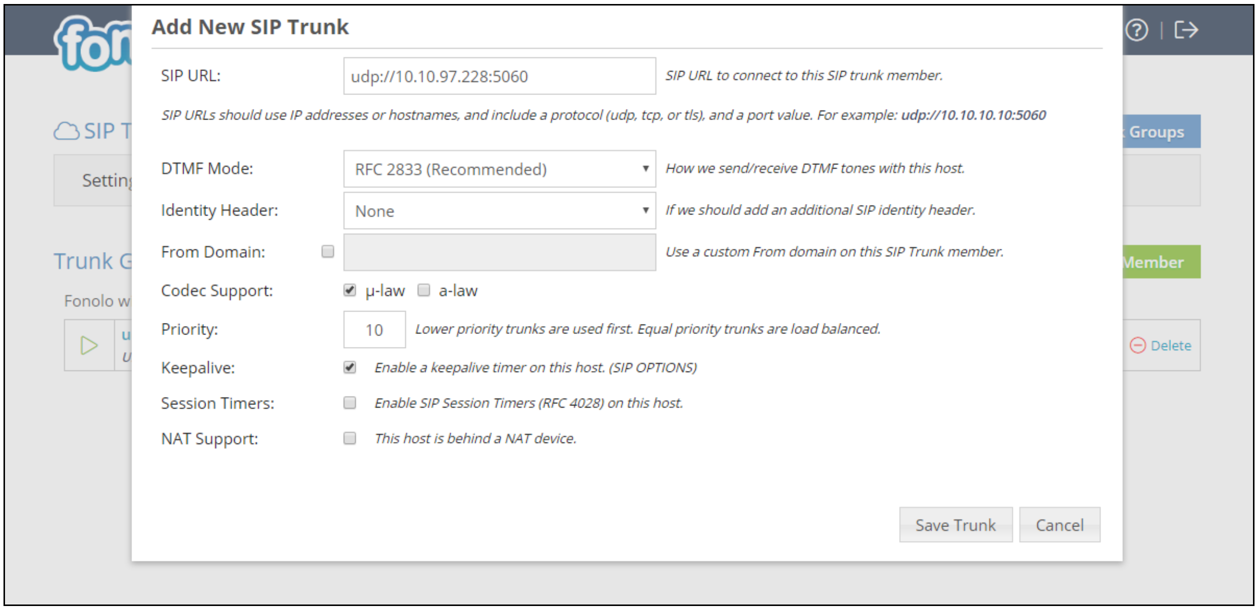
Navigate to **Telco → SIP Trunks** and click the **Add New SIP Trunk Group** button (not shown) at the top of the page. Define a new label to identify this SIP trunk group. During compliance testing **Avaya SM- Aura 8.0** was used as the label. Then select **Add New SIP Trunk** (not shown).

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 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.

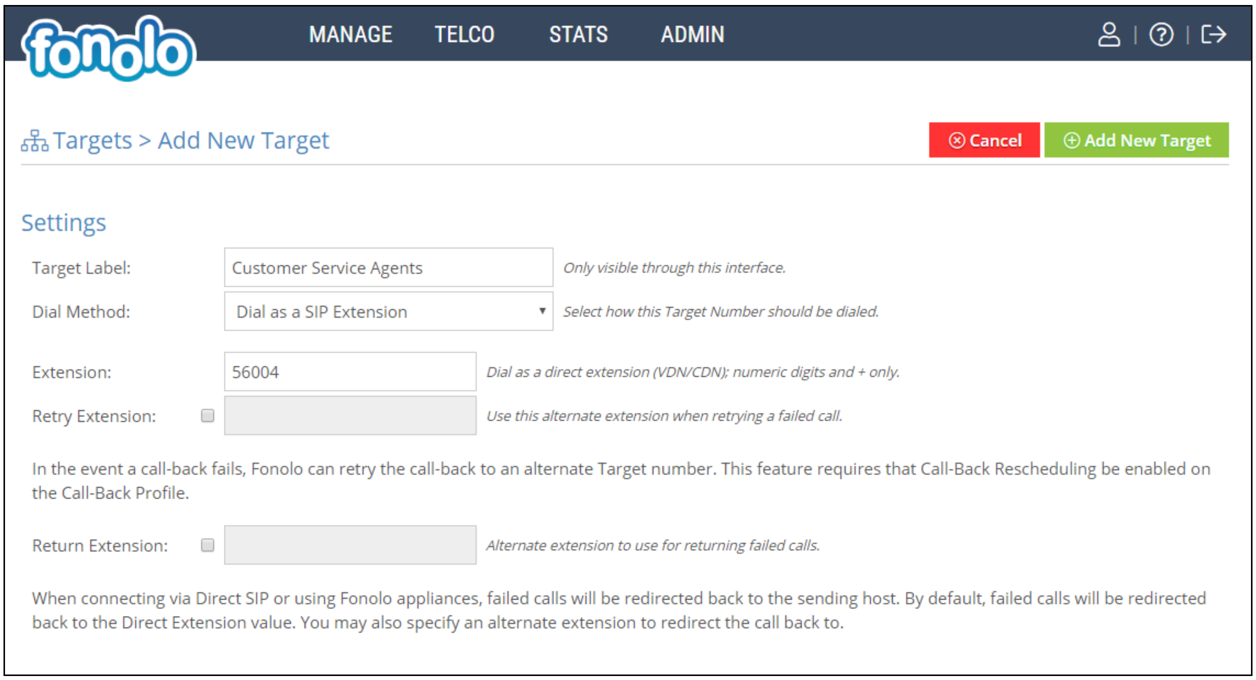
Add the IP address of Session Manager, formatted as a fully qualified URL, defining the protocol and SIP port, then click the **Save Trunk** button. During compliance testing, the protocol **UDP** and port **5060** is used for the SIP service with Session Manager, and the default values for the remaining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



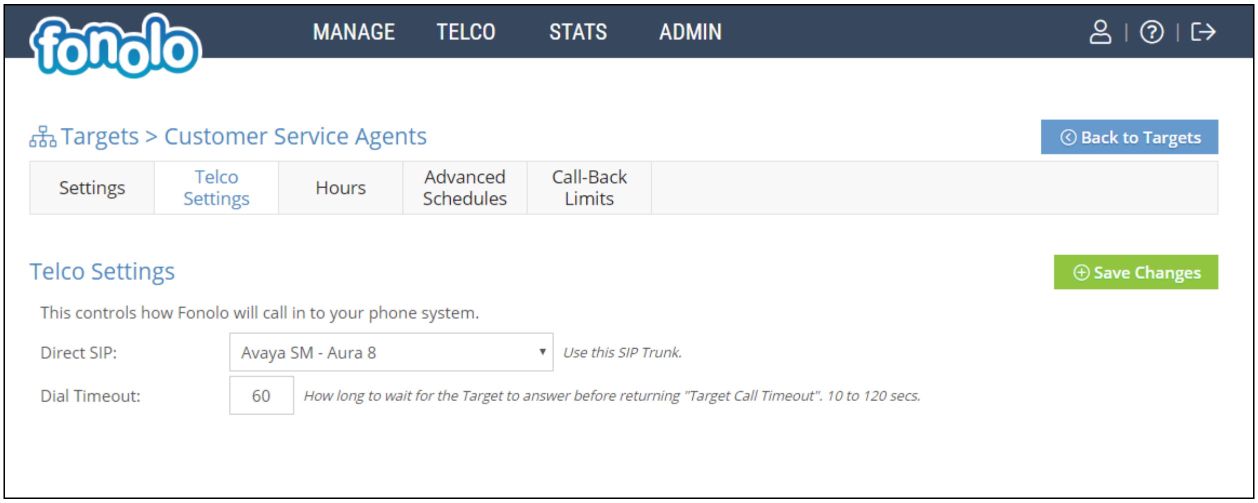
7.2. Adding the Agent Call-Back Endpoint

Navigate to **Manage → Targets** and click the **Add New Target** button (not shown). Define a new label to identify this new Target. During compliance testing **Customer Service Agents** 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.

During compliance testing, VDN 56004 was pre-configured on Communication Manager which was accessible via Session Manager. 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 SM - Aura 8.0** SIP trunk, added in **Section** Error! Reference source not found., and then click the **Save Changes** button.

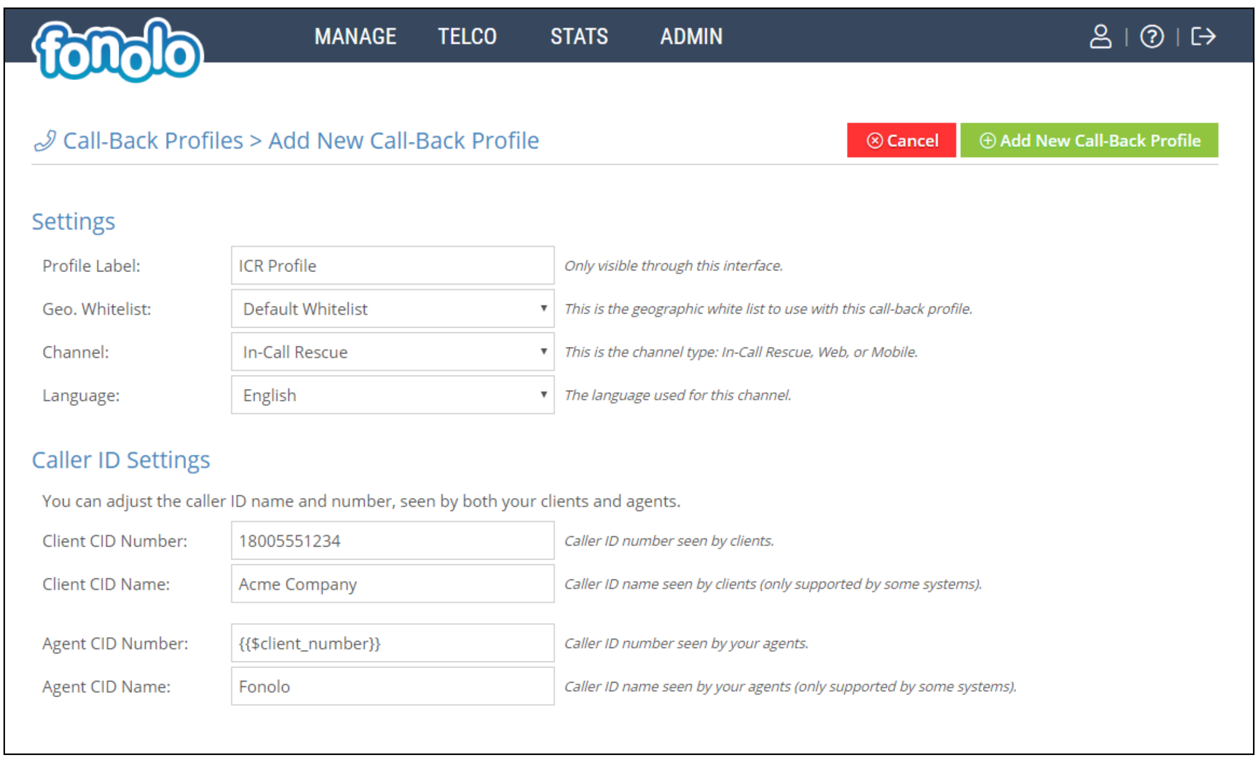


7.3. Adding a New Call-Back Profile

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

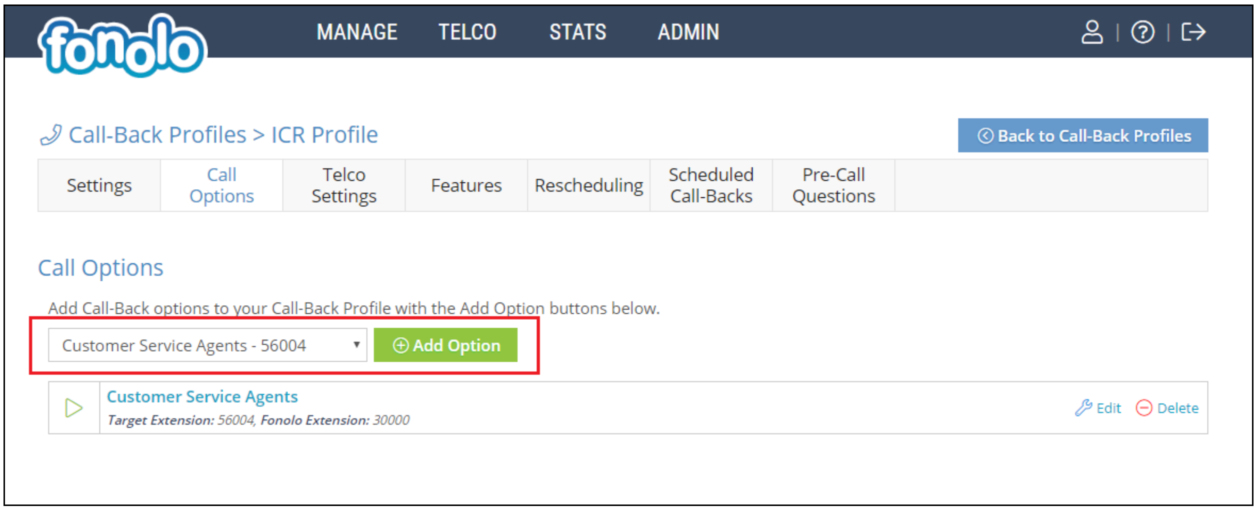
- **Profile Label:** A label to identify this new profile.
- **Geo Whitelist:** A geographic whitelist to use for this new profile.
- **Channel:** Select "In-Call Rescue".
- **Language:** Select the appropriate language for this skill set queue.
- **Client CID Number:** The Caller-ID number the customer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

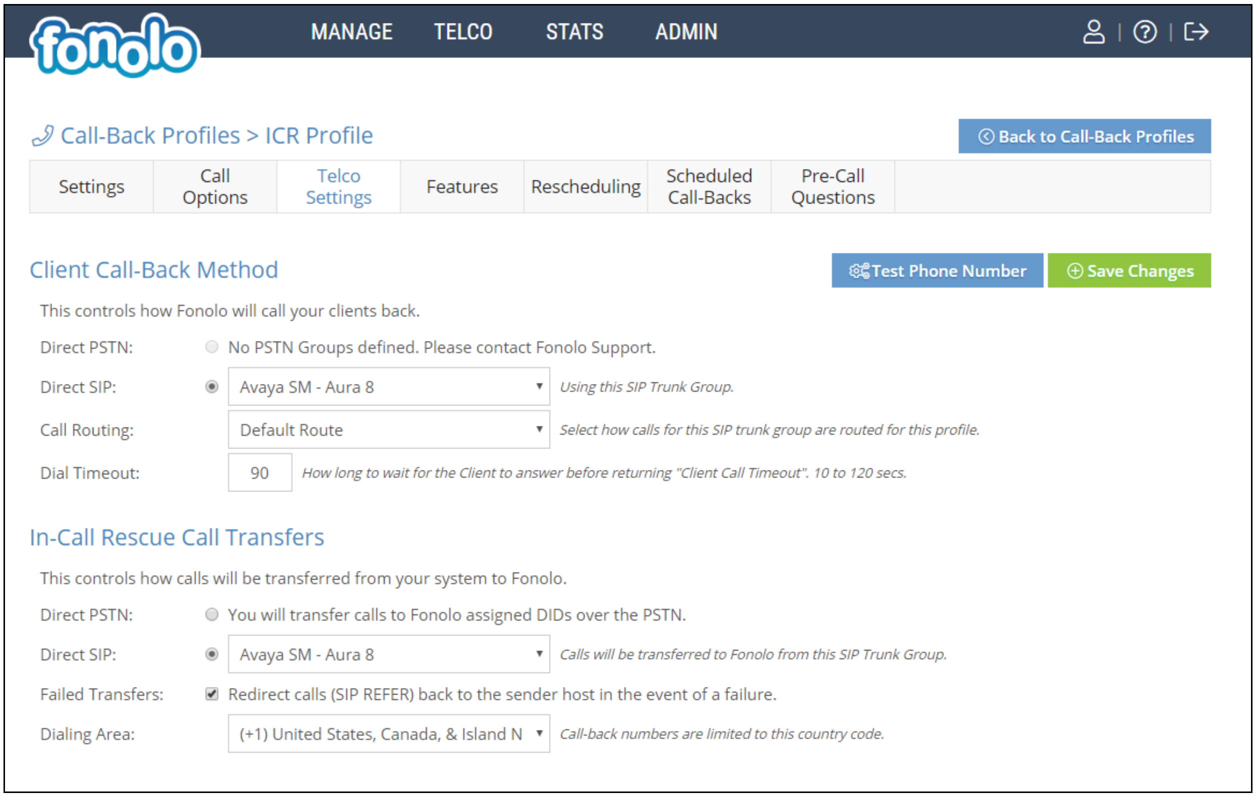


From the **Call Options** section of the new **Call-Back Profile**, select the Target added in **Section** Error! Reference source not found. (from the drop-down menu highlighted below), and click the **Add Option** link to add the VDN value to the section on the left, as shown below, then click the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

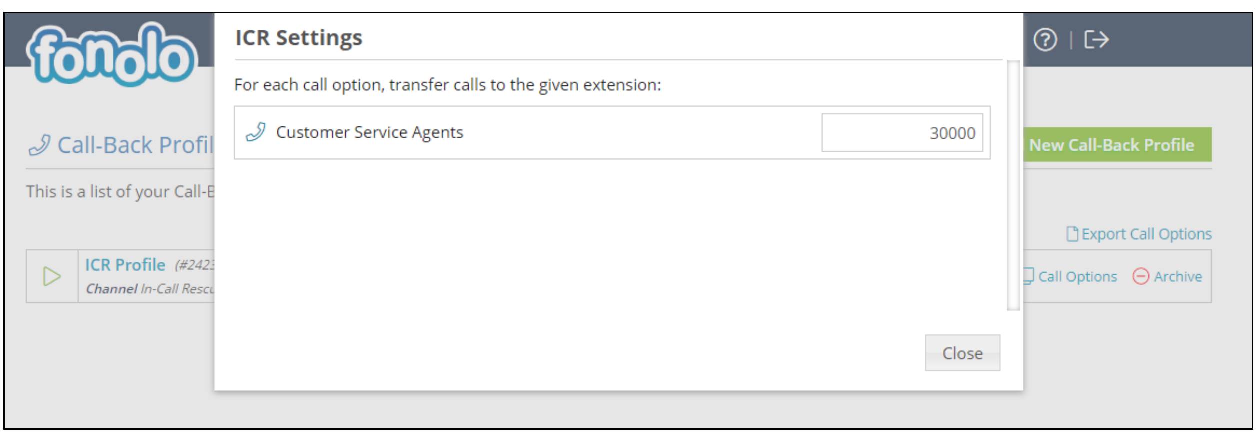
This associates the Target VDN with this new **Call-Back Profile**. Multiple call options can be associated with a single **Call-Back Profile**, one for each skill call-backs are being offered on.



From the **Telco Settings** section of the new **Call-Back Profile**, select the **Avaya SM - Aura 8.0** SIP trunk group created in **Section** Error! Reference source not found. 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 ICR system, when a call opts-in for a call-back. During compliance testing, the extension 30000 is configured on the Fonolo system.



8. Verification Steps

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

8.1. 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 5.44**. 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 5.2**. Verify that all trunks are in the **in-service/idle** state as shown below.

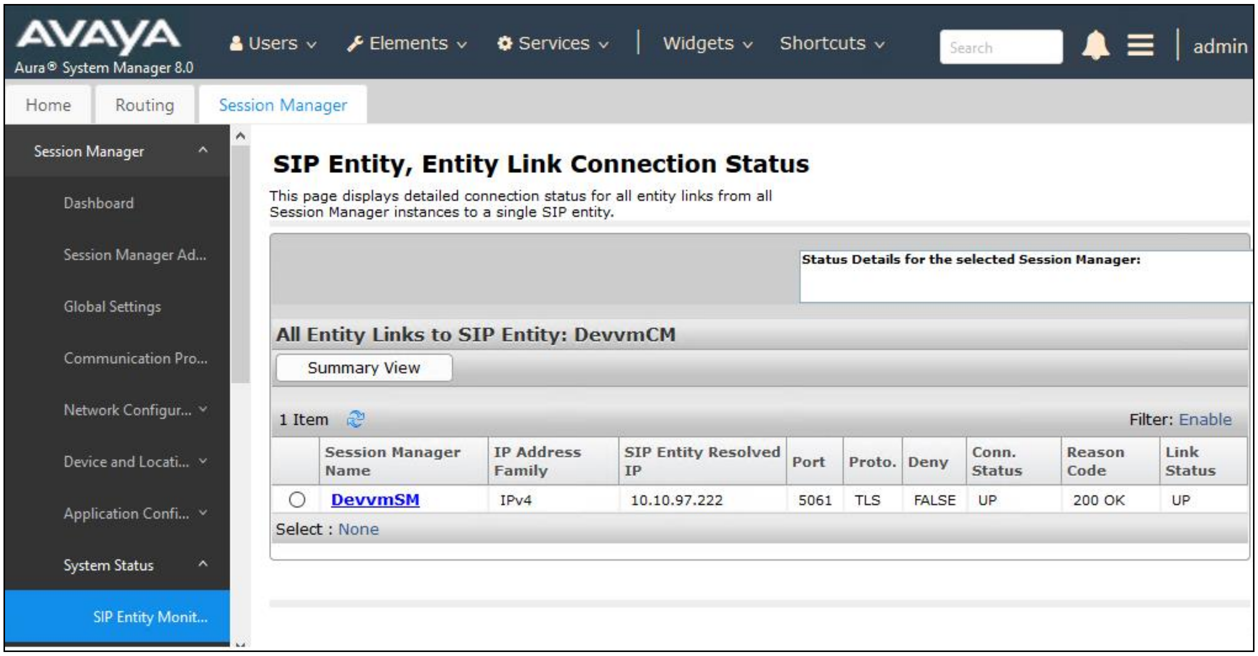
```
status trunk 1

                             TRUNK GROUP STATUS

Member   Port     Service State       Mtce Connected Ports
                                      Busy

0001/001 T00001   in-service/idle     no
0001/002 T00002   in-service/idle     no
```

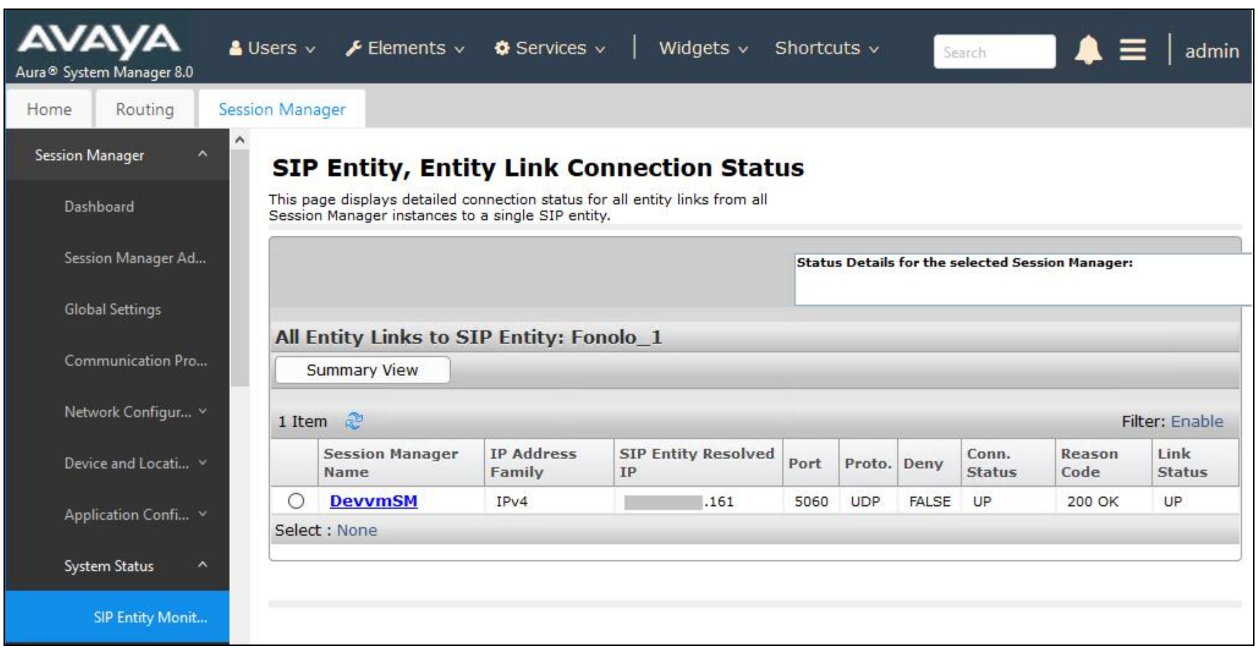
The following tests were also performed to verify proper configuration of ICR with Communication Manager.

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

8.2. Verify Avaya Aura® Session Manager

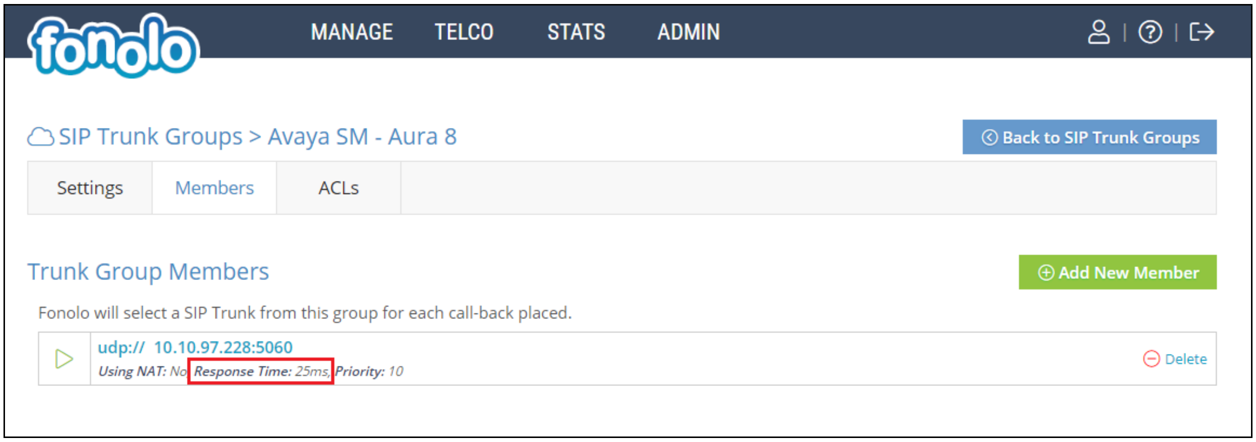
Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** and select the Communication Manager SIP Entity. Verify the **Link Status** is **Up**. Repeat the same procedure selecting the ICR SIP Entity and verify the **Link Status** is **Up**.





8.3. Verify Fonolo In-Call Rescue

In the Fonolo web portal, verify the link status of the SIP trunk group to the Session Manager, by navigating to **Telco → SIP Trunks** (not shown). Each SIP trunk group member will have a response time value, indicating the network latency (in milliseconds) between the Fonolo network, and the Session Manager. A positive **Response Time** value indicates a positive link status.



Additional information is available through the **Stats → Graphs** section of the Fonolo web portal (not shown).

9. Conclusion

These Application Notes describe the configuration steps required for Fonolo In-Call Rescue to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. All feature and serviceability test cases were completed and passed with the exceptions/observations noted in **Section 2.2**.

10. Additional References

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

Product documentation for Avaya products may be found at http://support.avaya.com.

1. *Deploying Avaya Aura® Communication Manager in Virtual Appliance*, Release 8.0, Issue 3 September 2018.
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.0, Issue 1 July 2018.
3. *Administering Avaya Aura® Communication Manager*, Release 8.0, Issue 1 July 2018.
4. *Avaya Aura® Communication Manager Screen Reference*, Release 8.0, Issue 2 August 2018.
5. *Deploying Avaya Aura® Session Manager in Virtual Appliance*, Release 8.0, Issue 2 September 2018.
6. *Administering Avaya Aura® Session Manager*, Release 8.0, Issue 2 August 2018.
7. *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.0, Issue 2 September 2018.
8. *Administering Avaya Aura® System Manager for Release 8.0,* Release 8.0, Issue 4 September 2018.
9. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0, Issue 2 July 2018.
10. *Implementing and Administering Avaya Aura® Media Server*, Release 8.0, Issue 2 July 2018.

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.