AVAYA

Application Notes for configuring Fonolo In-Call Rescue with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 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 R6.3 and Avaya Aura® Session Manager R6.3 using SIP trunks.

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.

RS; Reviewed:
SPOC 06/04/14

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

1 of 37
Fonolo_SM_CM

1. Introduction

These Application Notes describe the configuration steps required for Fonolo In-Call Rescue (ICR) to interoperate with Avaya Aura® Communication Manager R6.3 (Communication Manager) and Avaya Aura® Session Manager R6.3 (Session Manager) using SIP trunks. ICR provides functionality to replace hold-time with a call-back. The solution combines hosted services with optional hardware (to keep voice data on-premise). The solution communicates via SIP/RTP. The ICR functionality was compliance tested utilizing SIP trunks to Avaya Aura® Session Manager. The configuration allowed Communication Manager to use SIP trunking for calls to and from the ICR application.

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.

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.

2.1. Interoperability Compliance Testing

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

- Establishment of SIP trunks between Fonolo and Session Manager.
- Incoming calls to a skill set queue on Communication Manager can be directed to the ICR application via the SIP trunks.
- The ICR application can call into an agent in a skill set queue and also make an outbound call and connect them together when an agent is available.
- DTMF transmission.

Serviceability testing focused on verifying the ability of ICR to recover from adverse conditions, such as the SIP trunks going down and reboot of the application.

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.
- 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.

2.3. Support

Technical support on Fonolo ICR can be obtained through the following:
- **Phone:** 1-855-366-2500 (Toll-free)
- **Web:** http://fonolo.com/contact/

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 three 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.

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 contact 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.
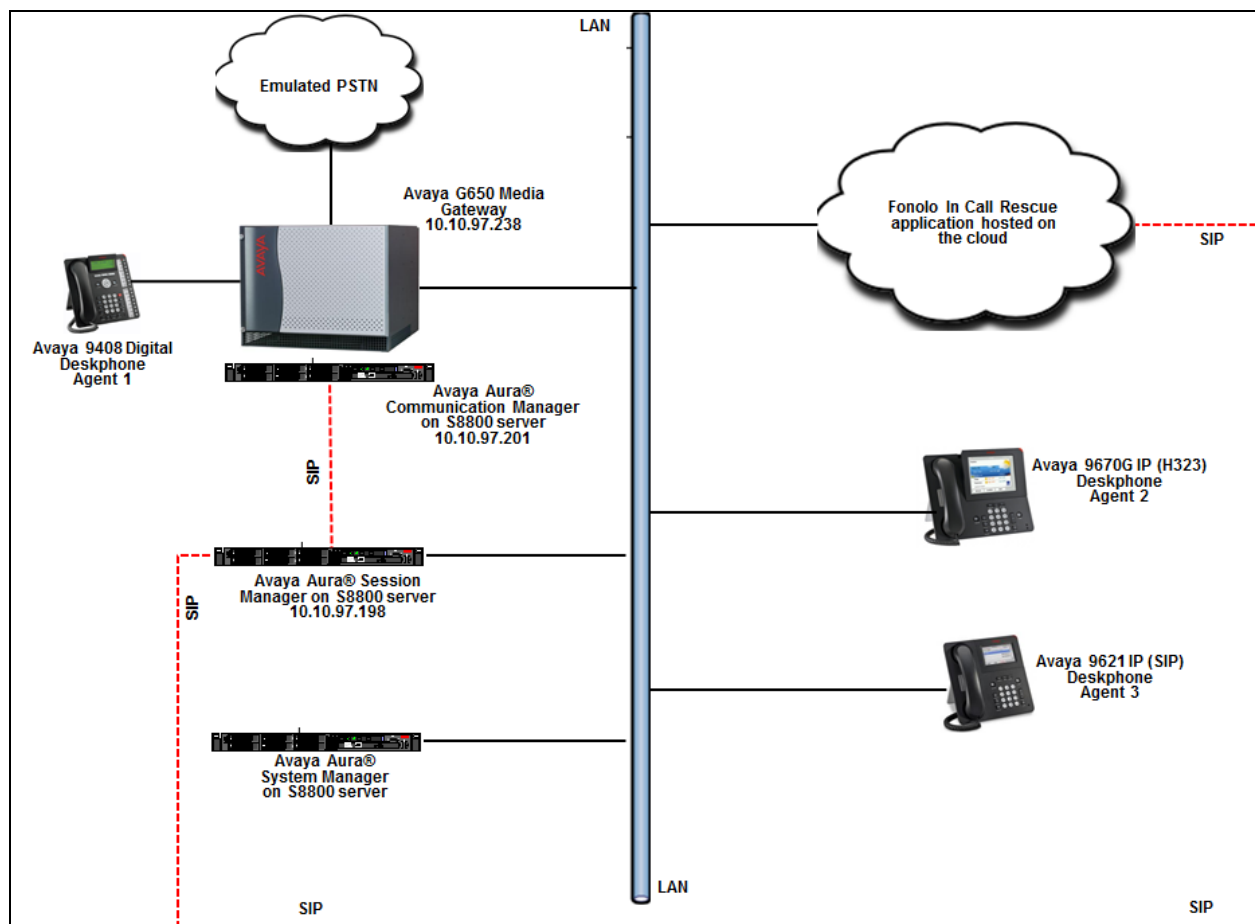
Figure 1: Fonolo In-Call Rescue with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunks

RS; Reviewed:
SPOC 06/04/14
Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.
4 of 37
Fonolo_SM_CM

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager running on S8800 Server with an Avaya G650 Media Gateway	6.3 (R016x.03.0.124.0)
Avaya Aura® System Manager running on S8800 Server	6.3.0-FP2
Avaya Aura® Session Manager running on S8800 Server	6.3.2.0.632023
Avaya IP Deskphones • 9670 (H.323) • 9621G (SIP)	S3.1 6.3.0.73
Avaya Digital Deskphone (9408)	Rel 12.0
Fonolo In-Call Rescue	Version 2.0

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

5.1. Verify Communication Manager License

Log in to the System Access Terminal (SAT) 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. The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options                      Page   2 of  11
                              OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                    Maximum Administered H.323 Trunks: 12000 0
          Maximum Concurrently Registered IP Stations: 18000 7
            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 2
                  Maximum Video Capable IP Softphones: 18000 2
                    Maximum Administered SIP Trunks: 24000 140
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                            Maximum TN2501 VAL Boards: 128   1
                   Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   1
  Maximum Number of Expanded Meet-me Conference Ports: 300   0


        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer IP Codec Set

Use the **change ip-codec-set n** command (not shown), where **n** is an existing codec set number that will be used for integration with ICR configuration. Enter the audio codec type *G.711MU* in the **Audio Codec** fields. Note only G.711u codec was used since ICR only supports this. Screen below displays the ip-codec-set after it has been configured.

```
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
```

5.3. Administer IP Network Region

Use the **change ip-network-region n** command (not shown), where **n** is an existing network region that will be used for integration with the ICR configuration. Enter an **Authoritative Domain** (e.g. *bvwdev.com*). For the **Codec Set** field, enter the codec set number from **Section 5.2**. Retain default values for the remaining field. Ensure that both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** are set to **yes**. Screen below displays the ip-network-region after it has been configured.

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

5.4. Administer IP Node Names

Use the **change node-names ip** command (not shown), and add an entry for Session Manager. In this case, **SM61** and **10.10.97.198** are entered as **Name** and **IP Address**. Note the **procr** / **10.10.97.201** entry, which is the node **Name** / **IP address** for the processor board. It will be used later to configure the SIP trunk to Session Manager. Screen below displays the node-names ip after it has been configured.

```
display node-names ip
                              IP NODE NAMES
    Name              IP Address
SM61              10.10.97.198
procr             10.10.97.201
```

5.5. Administer SIP Signaling Group

Administer a SIP signaling group for a new trunk that will be created for the connection between Communication Manager and Session Manager. Use the **add signaling-group n** command (not shown), where **n** is an available signaling group number. Enter the following values for the specified fields and retain the default values for the remaining fields as displayed in the screen below.

- **Group Type:** **sip**
- **IMS Enabled?** **n**
- **Transport Method:** **tcp**
- **Peer Detection Enabled?** **y**
- **Peer Server:** **SM** (this field will be automatically populated)
- **Near-end Node Name:** Processor node name from **Section 5.4,** i.e. **procr**
- **Near-end Listen Port:** **5060**
- **Far-end Node Name:** Session Manager node name from **Section 5.4**, i.e. **SM61**
- **Far-end Listen Port:** **5060**
- **Far-end Network Region:** The IP network region number from **Section 5.3**, i.e. **1**
- **Direct IP-IP Audio Connections:** *y*

```
display signaling-group 1                                      Page   1 of   2
                            SIGNALING GROUP


 Group Number: 1                   Group Type: sip
  IMS Enabled? n           Transport Method: tcp
        Q-SIP? n
    IP Video? y          Priority 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


   Near-end Node Name: procr                 Far-end Node Name: SM61
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region: 1


Far-end Domain: bvwdev.com
                                         Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate              RFC 3389 Comfort Noise? n
        DTMF over IP: rtp-payload       Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3               IP Audio Hairpinning? n
       Enable Layer 3 Test? y             Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n        Alternate Route Timer(sec): 30
```

5.6. Administer SIP Trunk Group

Administer a SIP trunk group to interface with the Session Manager. Use the **add trunk-group n** command (not shown), where **n** is an available trunk group number. Set the **Group Type** to **sip**, and **Service Type** to **tie**. Enter a descriptive **Group Name**, and an available trunk access code for the **TAC** field. Set **Member Assignment Method** to **auto**, **Signaling Group** to the signaling group number from **Section 5.5**, and enter a desired value for number of trunk group members for **Number of Members** as displayed in the screen below.

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

Group Number: 1                       Group Type: sip          CDR Reports: y
  Group Name: Private trunk                 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: 15

                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                      Number of Members: 50
```

Navigate to **Page 3**, and enter **private** for the **Numbering Format** field as shown below.

```
display 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


                          Modify Tandem Calling Number: no
             Send UCID? y



 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.

```
display 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
```

5.7. Administer Route Pattern

Create a route pattern to use for the newly created SIP trunk group. Use the **change route-pattern n** command (not shown), where **n** is an available route pattern. Enter a descriptive **Pattern Name**, i.e. **To- SM61**. In the **Grp No** field, enter the trunk group number from **Section 5.6**. In the **FRL** field, enter a level that allows access to this trunk. Set the corresponding **Number Format** for entry **1:** to **lev0-pvt** as displayed in the screen below. Retain default values for other fields.

```
display route-pattern 1                                        Page   1 of   3
                    Pattern Number: 1        Pattern Name: To-SM61
                               SCCAN? n     Secure SIP? 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  No. Numbering LAR
     0 1 2 M 4 W    Request                                  Dgts Format
                                                             Subaddress
 1: y y y y y n  n            rest                                lev0-pvt  none
 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
```

5.8. Administer Private Numbering

Use the **change private-numbering 0** command (not shown), to define the calling party number to send to Session Manager. Add an entry for the trunk group defined in **Section 5.6**. In the screen displayed below, all calls originating from a 5-digit extension beginning with 3 or 5 and routed over trunk group 1, will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

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

Ext Ext          Trk        Private          Total
Len Code         Grp(s)     Prefix           Len
 5   3           1                            5      Total Administered: 5
 5   5           1                            5        Maximum Entries: 540
```

5.9. Administer AAR Analysis

This section provides a sample AAR routing used for routing calls to Session Manager. Note that other methods of routing may be used. Use the **change aar analysis n** command (not shown), where **n** is an available dial pattern and add an entry to specify to route calls to Session Manager. In the screen displayed below, calls with digits **37xxx** will be routed as an AAR call using route pattern **1** from **Section 5.7**. These calls will be routed to Session Manager and then to ICR.

```
display aar analysis 3                                    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
        37                 5    5     1        aar         n
```

5.10. Administer Uniform Dial Plan

This section provides a sample of adding an extension to the uniform dial plan. Use the **change uniform-dialform n** command (not shown), where **n** is an available dial plan pattern and add an entry. During compliance testing 37 was added since 37xxx will be the number used to dial and reach the ICR.

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

  Matching                   Insert            Node
  Pattern      Len Del       Digits    Net Conv Num
  37            5   0                   aar  n
```

5.11. Administer Dialplan

This section provides a sample of adding an extension to the dialplan. Use the **change dialplan analysis** command (not shown), and add an entry. During compliance testing **37** was added since 37xxx will be the number used to dial and reach ICR.

```
display 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

    37          5   udp
```

5.12. 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 caller presses "1", then the call is routed to "37000", which is the number to dial out to ICR.

```
display vector 4                                                Page   1 of   6
                               CALL VECTOR

    Number: 4                    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    10              if staffed-agents   in skill 7        =  0
03 goto step    7               if expected-wait    for skill 7    pri m  >= 10
04 queue-to     skill 7    pri m
05
06
07 collect      1    digits after announcement 1008      for none
08 route-to     number 37000             with cov n if digit         =  1
09 goto step    4               if unconditionally
10 disconnect   after announcement none
11 stop
12
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as shown in the reference configuration. All provisioning for Session Manager is performed via the System Manager web interface. System Manager delivers a set of shared, secure management services and a common console across multiple products in the Avaya Aura® network, including the central administration of routing policies, and a common format for logs and alarms.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

The procedures described in this section include configurations for the following:

- **SIP Domains** – SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Network Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined default SIP proxy or one discovered through DNS).
- **Locations** – Locations define the physical and/or logical locations in which SIP Entities reside. Call Admission Control (CAC) / bandwidth management may be administered for each location to limit the number of calls to and from a particular Location.
- **SIP Entities** – SIP Entities represent SIP network elements such as Session Manager instances, Communication Manager systems, Session Border Controllers, SIP gateways, SIP trunks, and other SIP network devices.
- **Entity Links** – Entity Links define the SIP trunk/link parameters, e.g., ports, protocol (UDP/TCP/TLS), and trust relationship, between Session Manager instances and other SIP Entities.
- **Routing Policies** – Routing Policies are used in conjunction with a Dial Pattern to specify a SIP Entity that a call should be routed to.
- **Dial Patterns** – A Dial Pattern specifies a set of criteria and a set of Network Routing Policies for routing calls that match the criteria. The criteria include the called party number and SIP domain in the Request-URI, and the Location from which the call originated. For example, if a call arrives at Session Manager and matches a certain Dial Pattern, then Session Manager selects one of the Network Routing Policies specified in the Dial Pattern. The selected Network Routing Policy in turn specifies the SIP Entity to which the call is to be routed.

Access the System Manager administration web interface by entering https://<ip-address>/SMGR as the URL in an Internet browser, where *<ip-addr>* is the IP address of the System Manager server.

Log in using appropriate credentials. The main page for the administrative interface is shown below.

RS; Reviewed:
SPOC 06/04/14
Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.
16 of 37
Fonolo_SM_CM
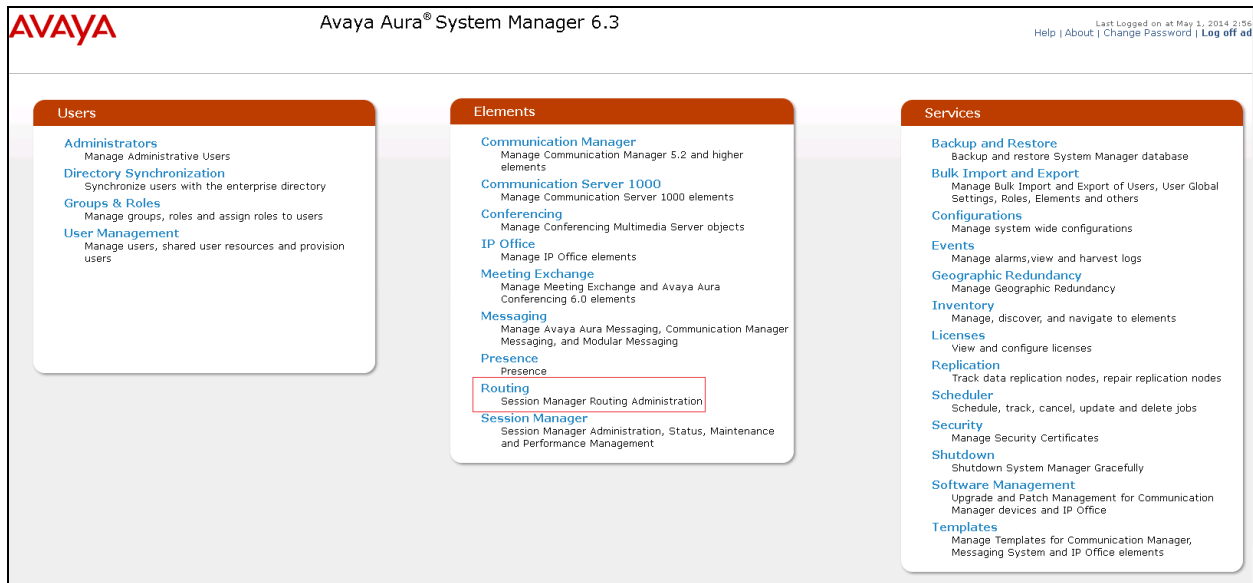
6.1.   Specify SIP Domain

Navigate to **Elements →Routing→Domains**, and click the **New** button to add the SIP domain with the following:

- **Name**: *bvwdev.com* (as set in **Section 5.3**)
- **Type**: *sip*
- **Notes**: optional descriptive text

Click **Commit** to save the configuration.

6.2.   Add Location

Locations identify logical and/or physical locations where SIP entities reside. Only one Location was configured for compliance testing.

Navigate to **Elements**➔**Routing**➔**Locations** and click the **New** button to add the Location. Enter the following information:

Under **General** (not shown):
- **Name**: a descriptive name
- **Notes**: optional descriptive text

The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity.

Under **Location Pattern**, click the **Add** button to add a new line (not shown):
- **IP Address Pattern**: Enter the logical pattern used to identify the location. During compliance testing ***10.10.98.0 and 10.10.97.0*** was used.
- **Notes**: optional descriptive text

Click **Commit** to save the configuration.

6.3.   Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration a SIP Entity is added for the Session Manager, Communication Manager, and ICR.

Note, the Session Manager SIP Entity is assumed to have already been configured. Navigate to **Elements → Routing→SIP Entities**, check the checkbox for the Session Manager SIP Entity, and click the **Edit** button (not shown). Under the **Port** section, verify the required Session Manager listening port is configured (i.e. **Port** *5060* / **Protocol** *TCP,* **Port** *5060* / **Protocol** *UDP* and **Port** *5061* / **Protocol** *TLS*). If necessary, click the **Add** button to add the listening port and then click **Commit** to save the changes.

Port		Protocol	Default Domain	Notes
TCP Failover port:				
TLS Failover port:				
Add Remove				
3 Items │ Refresh				Filter: Enable
☐	Port ▲	Protocol	Default Domain	Notes
☐	5060	TCP ▾	bvwdev.com ▾	
☐	5060	UDP ▾	bvwdev.com ▾	
☐	5061	TLS ▾	bvwdev.com ▾	
Select : All, None				

To add a SIP Entity, navigate to **Elements → Routing→SIP Entities** and click the **New** button (not shown).

The configuration details for the SIP Entity defined for Communication Manager are below:

Under **General**:
- **Name**: a descriptive name
- **FQDN or IP Address**: *10.10.97.201* is the IP address of the procr used during compliance testing.
- **Type**: select *CM*
- **Location**: select the location configured in **Section 6.2**
- **SIP Link Monitoring:** Select *Use Session Manager Configuration* from the drop down menu**.**
- **Entity Links:** This was added in a subsequent edit to the Entity record using the **Add** button but is described here for brevity purposes**.** See **Section 6.4** for how the Entity Link was created.

Default settings can be used for the remaining fields. Click **Commit** to save the SIP Entity definition.

The following screen shows addition of the ICR SIP Entity. Note the selection of **Other** for **Type**.

RS; Reviewed:
SPOC 06/04/14

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

22 of 37
Fonolo_SM_CM

6.4. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. Two Entity Links were created:

- Session Manager ←→ Communication Manger
- Session Manager ←→ Fonolo ICR

Navigate to **Elements → Routing→Entity Links**, and click the **New** button (not shown) to add a new Entity Link. The screen below shows the configuration details for the Entity Link connecting Session Manager with Communication Manager.

- **Name**: a descriptive name
- **SIP Entity 1**: select the Session Manager SIP Entity.
- **Protocol**: select *TCP* as the transport protocol
- **Port**: *5060*. This is the port number to which the other system sends SIP requests
- **SIP Entity 2**: select the Communication Manager SIP Entity
- **Port**: *5060*. This is the port number on which the other system receives SIP requests
- **Connection Policy**: select *Trusted*
- **Notes**: optional descriptive text

  Click **Commit** to save the configuration.

The Entity Link for connecting Session Manager with ICR was similarly defined as shown in the screen below. Note the use of protocol **UDP** and port **5060**.

RS; Reviewed:
SPOC 06/04/14

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

24 of 37
Fonolo_SM_CM

6.5. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities connected to the Session Manager. One routing policy must be added for routing calls to Communication Manager and one for routing calls to the ICR.

Navigate to **Elements → Routing→Routing Policies**, and click the **New** button (not shown) to add a new Routing Policy. Enter the following information:

Under **General**:
- **Name**: a descriptive name
- **Notes**: optional descriptive text

Under **SIP Entity as Destination**
Click **Select** to select the appropriate SIP Entity to which the routing policy applies (not shown).

Default settings can be used for the remaining fields. Click **Commit** to save the configuration.

Note that the **Dial Patterns** shown below was added when the **Dial Pattern** was defined in **Section 6.6** but is shown here for brevity.

The following screen shows the Routing Policy for routing calls to Communication Manager.

RS; Reviewed:
SPOC 06/04/14

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

25 of 37
Fonolo_SM_CM

The following screen shows the Routing Policy for routing calls to ICR.

RS; Reviewed:
SPOC 06/04/14

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

26 of 37
Fonolo_SM_CM

6.6. Add Dial Patterns

Define dial patterns to direct calls to the appropriate SIP Entity.

Navigate to **Elements → Routing→Dial Patterns**, and click the **New** button (not shown) to add a new Dial Pattern.   Enter the following information to route calls that match the pattern *53* to Communication Manager. Similarly add *9* so that calls will be directed to the Communication Manager first and then to the PSTN.

Under **General**:
- **Pattern**: dialed number or prefix
- **Min**: minimum length of dialed number
- **Max**: maximum length of dialed number
- **SIP Domain**: select the SIP Domain created in **Section 6.1**
- **Notes**: optional descriptive text

Under **Originating Locations and Routing Policies**
Click **Add** to select the appropriate originating Location and Routing Policy from the list (not shown).

Default settings can be used for the remaining fields. Click **Commit** to save the configuration.

Enter the following information to route calls that match the pattern **37** to ICR. The Session Manager will then route these calls to the ICR.

RS; Reviewed:
SPOC 06/04/14

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

28 of 37
Fonolo_SM_CM

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. They represent only an example of the configuration GUI of ICR, available through the Fonolo Web Portal at https://portal.fonolo.com/. Other configurations are possible. Contact Fonolo for details on how to configure ICR.

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 CM 6.3** was used as the label. Then select **Save Changes** (not shown).

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

Add the IP address of the 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 to the Session Manager.

7.2. Adding the Agent Call-Back Endpoint

Navigate to **Manage → Phone Trees** and click the **Add New Phone Tree** button (not shown). Define a new label to identify this new Phone Tree. During compliance testing **Customer Service Agents** was used as the label. Select the **Direct Extension** option (shown below), and enter the VDN to reach the skill set queue on the Communcation Manager.

During compliance testing, VDN 53053 was configured on the Communication Manager. Then click on **Add New Phone Tree** button to save this Phone Tree.

From the Telco Settings section of the newly added Phone Tree, select the SIP Trunk to use for this Phone Tree, from the **Direct SIP** drop down menu shown below. Select the **Avaya CM 6.3** SIP Trunk, added in **Section 7.1**, then click on **Save Changes** button.

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

7.3. Adding New Channel Profile

Navigate to **Manage → Channel Profiles** and click on the **Add New Profile** button, and configure the new profile:

- **Profile Label:** a label to identify this new profile.
- **Channel:** select *In-Call Rescue*.
- **Language:** select the appropriate language for this skill set queue.
- **Customer CID Number:** the Caller-ID number the customer will see.
- **Customer 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 **Add New Channel Profile** button to add this new profile.

From the **Call Options** section of the new Channel Profile, select the Phone Tree added in
Section 7.2 and drag-and-drop the VDN value to the Channel Profile section on the right, as
shown below, then click **Save Changes** button.

This associates the skill set queue VDN with this new Channel Profile. Multiple Call Options can
be associated with a single Channel Profile, one for each Skillset queue call-backs are being
offered on.

From the **Telco Settings** section of the new Channel Profile, select the **Avaya CM 6.3** SIP Trunk group created in **Section 7.1** 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 **Save Changes** button.
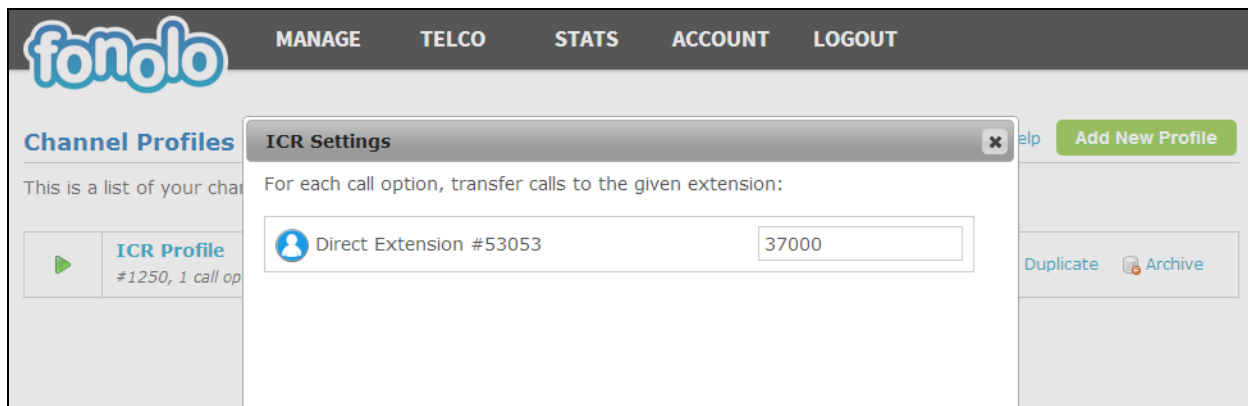
Navigate to **Manage → Channel Profiles** and click on the **In-Call Rescue** link on the newly created Channel Profile (not shown). The In-Call Rescue extensions dialog will appear (shown below), and include the inbound extensions to use for each configured skill set VDN. These are the extensions to transfer calls to, on the Fonolo cloud. During compliance testing, the extension 37000 is configured on the Fonolo system.

RS; Reviewed:
SPOC 06/04/14
Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.
34 of 37
Fonolo_SM_CM

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 5.5**. 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

0001/001 T00001    in-service/idle       no
0001/002 T00002    in-service/idle       no
0001/003 T00003    in-service/idle       no
0001/004 T00004    in-service/idle       no
0001/005 T00005    in-service/idle       no
0001/006 T00006    in-service/idle       no
0001/007 T00007    in-service/idle       no
0001/008 T00008    in-service/idle       no
0001/009 T00009    in-service/idle       no
0001/010 T00010    in-service/idle       no
```

The following call flow were also verified,
- PSTN caller is provided an announcement from Communication Manager to select a call back option or wait in the queue when all agents are busy.
- PSTN caller is able to select the call back option and Communication Manager is able to direct this call to ICR.
- PSTN caller is able to hear the ICR menu and make the required choices.
- ICR is able to recognize the choices made by the PSTN user.
- ICR is able to call the queue and wait for an available agent.
- ICR is able to 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 (not shown). Verify the **Link Status** is *Up*. Repeat the procedure above selecting the ICR SIP Entity (not shown), 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**. Each SIP Trunk group will have a simple indicator icon, identifying the current Link Status of each SIP Trunk Member, as shown below. A green indicator identifies the Link as active. A red indicator indicates the link as down (not shown).
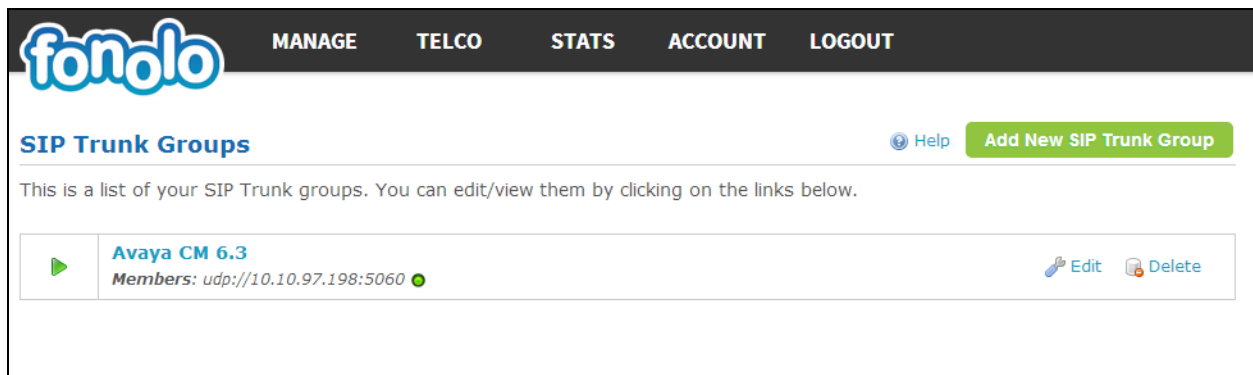
Additional information is available through the **Stats → Graphs** section of the web portal (not shown).

9. Conclusion

These Application Notes describe the configuration steps required for ICR to successfully interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3. 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. All Avaya documents are available at http://support.avaya.com.

1. *Administering Avaya Aura® Communication Manager*, October 2013, Release 6.3 Document 03-300509 Issue 9.
2. *Administering Avaya Aura® Session Manager,* October 2013, Release 6.3, Document 03-603324.
3. *Administering Avaya Aura® System Manager,* October 2013, Release 6.3.

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