



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 7.0 and Avaya Aura® Session Manager 7.0 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 7.0 (Communication Manager) and Avaya Aura® Session Manager 7.0 (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.

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.

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.
- User-to-User Information (UUI).
- 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:** <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 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.

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.

The following values were configured during compliance testing,

VDN: 56004

Vector: 2

SkillSet: 1

Agent Login ID: 1000, 1001 and 1002

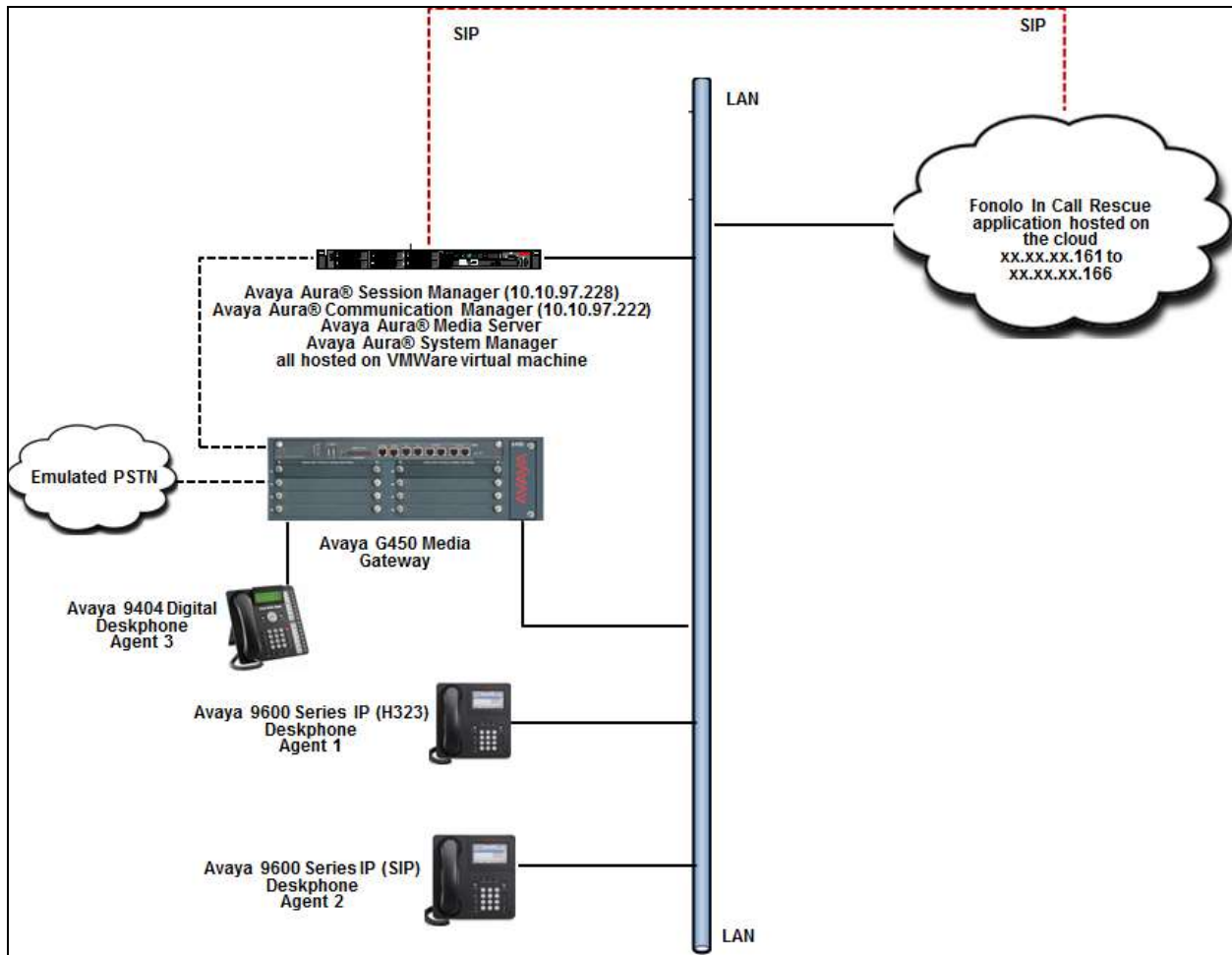


Figure 1: Reference Configuration

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager	7.0.0.1.0-SP1 (R017x.00.0.441.0)
Avaya Aura® Session Manager	7.0.0.0.700007
Avaya Aura® System Manager	7.0.0.0
Avaya Aura® Media Server	7.7.0.226
Avaya G450 Media Gateway	37 .19 .0 /1
Avaya IP Deskphones <ul style="list-style-type: none">• 9641 (H.323)• 9621 (SIP)	6.6115 7.0.0.39
Avaya Digital Deskphone (9404)	R 0.15 V21
Fonolo In-Call Rescue	Version 2.6

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

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.

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 12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 4000 10
    Maximum Concurrently Registered IP Stations: 2400 2
      Maximum Administered Remote Office Trunks: 4000 0
Maximum Concurrently Registered Remote Office Stations: 2400 0
      Maximum Concurrently Registered IP eCons: 68 0
    Max Concur Registered Unauthenticated H.323 Stations: 100 0
      Maximum Video Capable Stations: 2400 1
      Maximum Video Capable IP Softphones: 2400 3
      Maximum Administered SIP Trunks: 4000 24
    Maximum Administered Ad-hoc Video Conferencing Ports: 4000 0
    Maximum Number of DS1 Boards with Echo Cancellation: 80 0
```

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 codec. 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**. Ensure that both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** are set to **yes**. Retain default values for the remaining field. 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: 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
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, **SM-VM** and **10.10.97.228** are entered as **Name** and **IP Address**. Note the **procr / 10.10.97.222** 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	
SM-VM	10.10.97.228	
procr	10.10.97.222	

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
- **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. **SM-VM**
- **Far-end Listen Port:** 5060
- **Far-end Network Region:** The IP network region number from **Section 5.3**, i.e. **1**
- **Far-end Domain:** **bvwdev.com** as configured in **Section 5.3**
- **Direct IP-IP Audio Connections:** y

```
display signaling-group 1                               Page 1 of 3
                SIGNALING GROUP

Group Number: 1                      Group Type: sip
  IMS Enabled? n                      Transport Method: tcp
    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: 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? n
H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
```

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: 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 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
                                  Hold/Unhold Notifications? y
  Send UCID? y                Modify Tandem Calling Number: no
  Show ANSWERED BY on Display? y
  DSN Term? n                  SIP ANAT Supported? n
```

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

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

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 SM on VM**. 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 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          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
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 **56** 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 Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	56	1		5	Total Administered: 4 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 **30xxx** 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 0
```

Page 1 of 2

AAR DIGIT ANALYSIS TABLE
Location: all Percent Full: 2

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
30	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 **30** was added since 30xxx 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 Pattern	Len	Del	Insert Digits	Net Conv	Node Num
30	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 **30** was added since 30xxx 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: 2
```

Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
30	5	ext						

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 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 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.

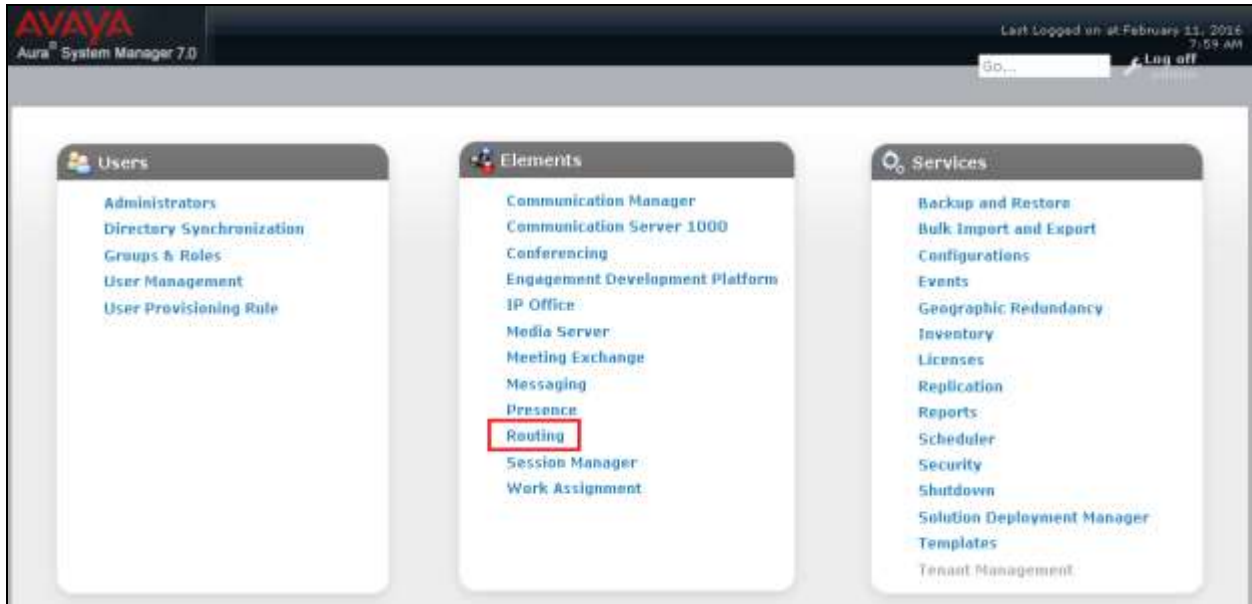
The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

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 (not shown). The main page for the administrative interface is shown below.

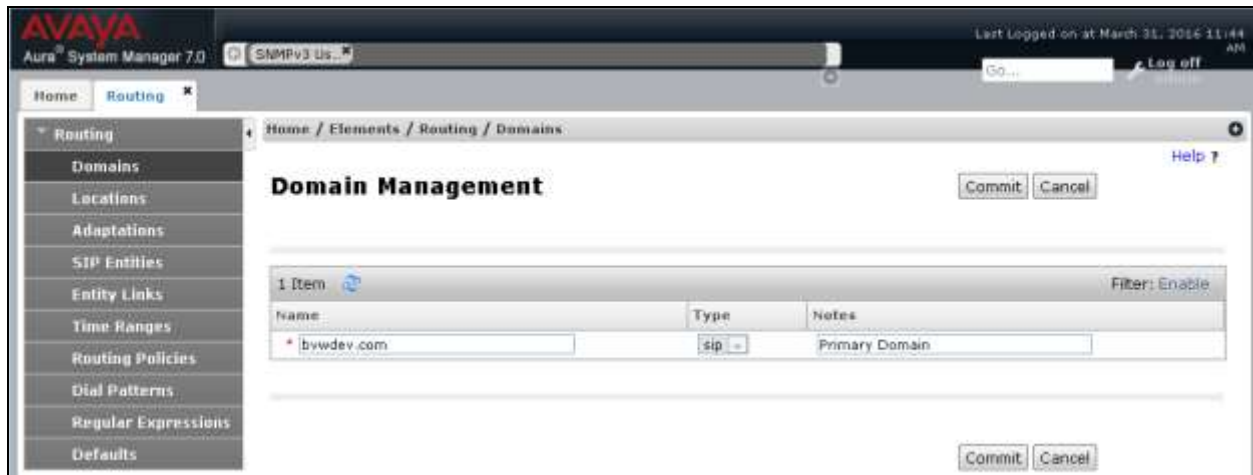


6.1. Specify SIP Domain

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 (not shown) to add the Location. Enter the following information:

Under **General**:

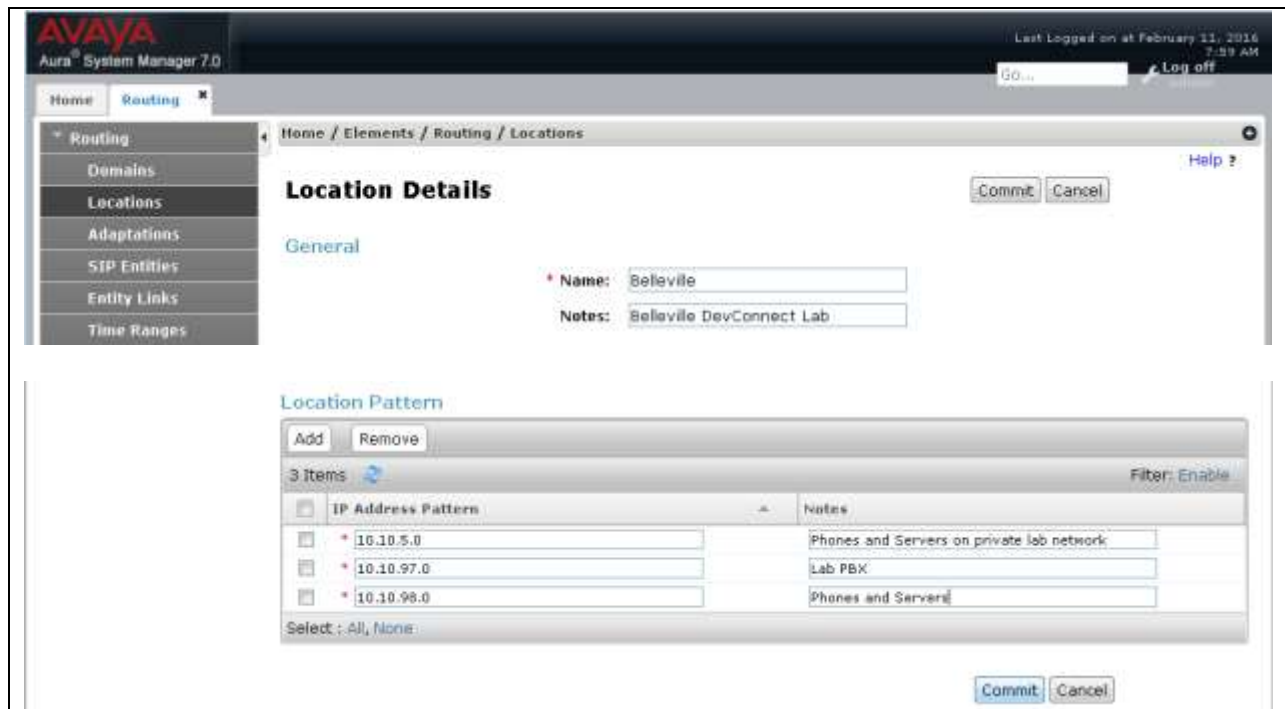
- **Name:** a descriptive name
- **Notes:** optional descriptive text

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 :

- **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 ports are configured (i.e. **Port 5060 / Protocol TCP**, **Port 5060 / Protocol UDP** and **Port 5061 / Protocol TLS**). If necessary, click the **Add** button to add a listening port and then click **Commit** to save the changes (not shown).

Listen Ports	Protocol	Default Domain	Notes
5060	TCP	bvwdev.com	
5060	UDP	bvwdev.com	
5061	TLS	bvwdev.com	

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**:

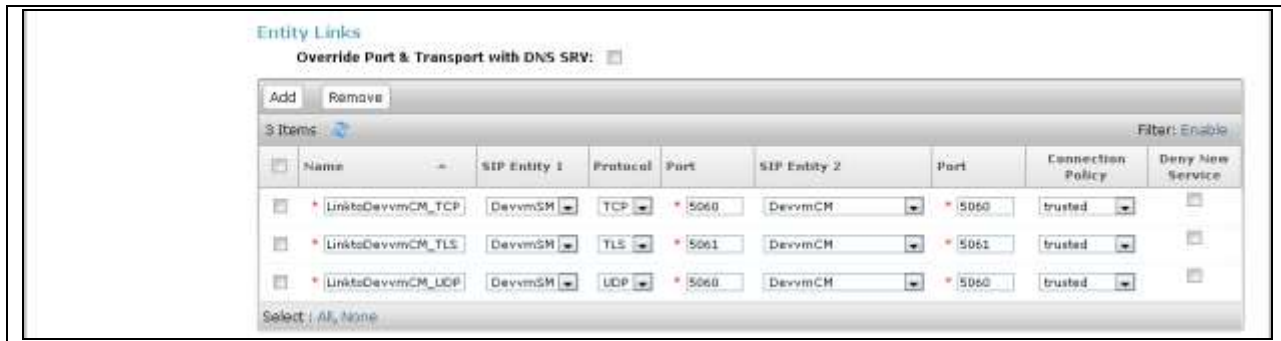
- **Name:** a descriptive name
- **FQDN or IP Address:** 10.10.97.222 is the IP address of the procr used during compliance testing.
- **Type:** select **CM**
- **Location:** select the location configured in **Section 6.2**
- **SIP Link Monitoring:** Retain the default value, **Use Session Manager Configuration** 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.

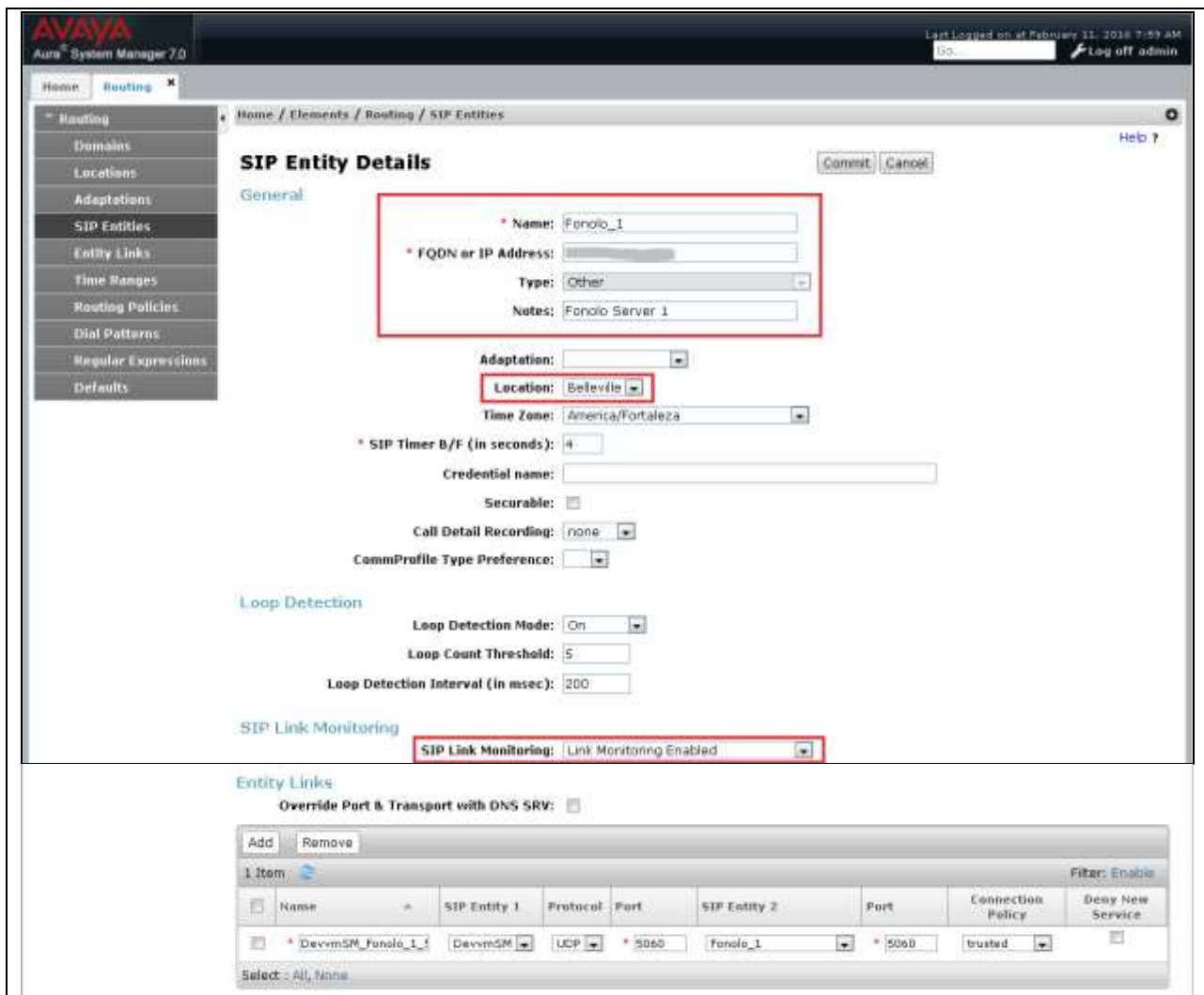
The screenshot shows the Avaya Aura System Manager 7.0 interface. The breadcrumb navigation is Home / Elements / Routing / SIP Entities. The page title is 'SIP Entity Details'. The 'General' tab is active. The configuration fields are as follows:

- Name: DevvmCM
- FQDN or IP Address: 10.10.97.222
- Type: CM
- Notes: CM 7.0 on VM
- Adaptation: (empty)
- Location: Belleville
- Time Zone: America/Fortaleza
- SIP Timer B/F (in seconds): 4
- Credential name: (empty)
- Securable:
- Call Detail Recording: none
- Loop Detection Mode: On
- Loop Count Threshold: 5
- Loop Detection Interval (in msec): 200
- SIP Link Monitoring: Use Session Manager Configuration

Buttons for 'Commit' and 'Cancel' are located at the top right of the configuration area.



The following screen shows addition of the ICR SIP Entity. Note the selection of **Other** for **Type**. During compliance testing six SIP entities were configured for ICR, two for incoming calls to ICR and four for outgoing calls from ICR.



6.4. Add Entity Links

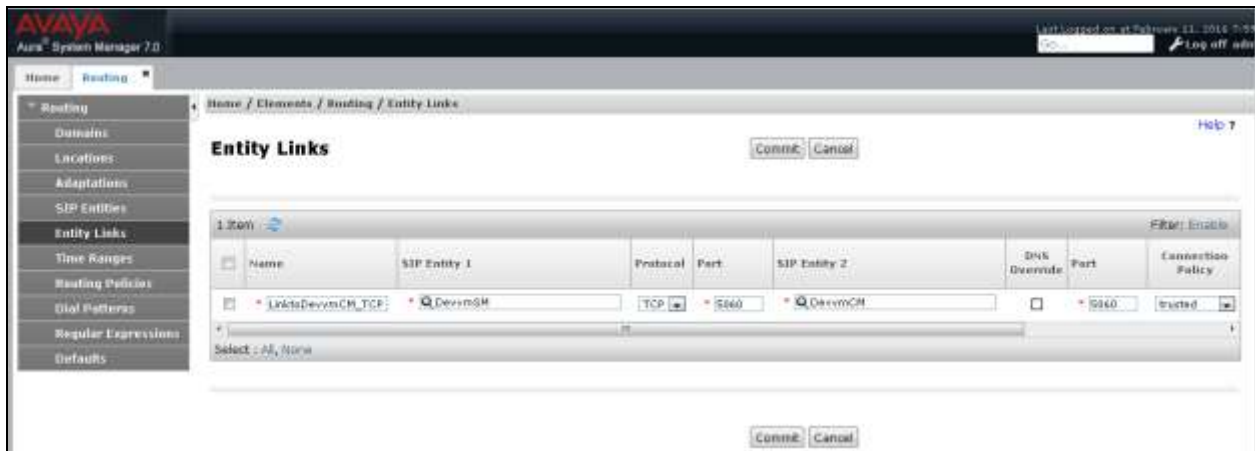
A SIP trunk between Session Manager and a telephony system is described by an Entity link. Two Entity Links were created:

- 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**. As explained in **Section 6.3**, six entity links were configured for the six Fonolo ICR servers.



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.

AVAYA
Aura System Manager 7.0

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel Help ?

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
DevvmCH	10.10.97.222	CH	

Dial Patterns

Add Remove

3 Items Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	15149626	8	36	<input type="checkbox"/>	bvwdev.com	Belleville	This is the number coming from Fonolo
<input type="checkbox"/>	5149626	7	36	<input type="checkbox"/>	bvwdev.com	Belleville	Tandem call route from CM 6.3 to IPO via CM 7.0
<input type="checkbox"/>	56	5	5	<input type="checkbox"/>	bvwdev.com	Belleville	Dial Pattern to VM CM

Select : All, None

The following screen shows the Routing Policy for routing calls to ICR. Six routing policies were configured for ICR. For the two incoming routing policies the **Ranking** under **Time of Day** was set to **0**, so that calls could be load balanced between the two incoming routing policies.

AVAYA
Aura System Manager 7.0

Last Logged on at February 21, 2016 1:59 AM
GO... Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details Commit Cancel

General

* Name: Route_To_Fonolo_1
 Disabled:
 * Retries: 0
 Notes: Routing to Fonolo Server 1

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Fonolo_1		Other	Fonolo Server 1

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	30	5	5	<input type="checkbox"/>	bvwdev.com	Belleville	Dial pattern to reach Fonolo servers

Select : All, None

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 **56** to Communication Manager. Similarly other patterns can be added 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.

The screenshot displays the Avaya Aura System Manager 7.0 interface for configuring a Dial Pattern. The breadcrumb path is Home / Elements / Routing / Dial Patterns. The 'Dial Pattern Details' page is shown with the 'General' tab selected. The 'Pattern' field is set to '56', 'Min' is '5', and 'Max' is '5'. The 'Emergency Call' checkbox is unchecked, 'Emergency Priority' is '1', and 'Emergency Type' is empty. The 'SIP Domain' is set to 'bvwdev.com' and the 'Notes' field contains 'Dial Pattern to VM CM'. Below this, the 'Originating Locations and Routing Policies' section features an 'Add' button and a table with one entry:

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	<input type="checkbox"/>	DevvmCM	

Enter the following information to route calls that match the pattern **30** to ICR. The Session Manager will then route these calls to the ICR.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The main content area is titled "Dial Pattern Details" and contains the following configuration fields:

- Pattern:** 30
- Min:** 5
- Max:** 5
- Emergency Call:**
- Emergency Priority:** 1
- Emergency Type:** (empty)
- SIP Domain:** bnxdev.com
- Notes:** Dial pattern to reach Fonolo servers

Below the configuration fields is a section titled "Originating Locations and Routing Policies" which contains a table with 4 items:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Belleville	DevConnect Lab	Route_To_Fonolo_1	0	<input type="checkbox"/>	Fonolo_1	Routing to Fonolo Server 1
Belleville	DevConnect Lab	Route_To_Fonolo_2	0	<input type="checkbox"/>	Fonolo_2	Routing to Fonolo Server 2

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 7.0** 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 **Add New SIP Trunk** dialog will appear as shown below.

The screenshot shows the Fonolo web portal interface. At the top, there is a navigation bar with 'MANAGE', 'TELCO', 'STATS', and 'ADMIN' tabs. The user is logged in as 'Administrator' with 'Account Settings | Logout' options. The main content area is titled 'SIP Trunks > Avaya CM 7.0'. Below this, there are tabs for 'SETTINGS', 'MEMBERS', and 'ACLS'. The 'MEMBERS' tab is active, and a 'Save Changes' button is visible. A modal dialog titled 'Add New SIP Trunk' is open, displaying the following configuration options:

- SIP URL:
- SIP URLs should use IP addresses, and include a protocol (udp, tcp, or tls), and a port value. For example: `udp://10.10.10.10:5060`
- DTMF Mode:
- Identity Header:
- Codec Support: μ -law a-law
- Priority:
- Keepalive: Enable a keepalive timer on this host, 60 to 999 secs
- Session Timers: Enable SIP Session Timers (RFC 4028) on this host, Expires MinSE Refresher
- NAT Support: This host is behind a NAT device.

At the bottom of the dialog, there are 'Save Trunk' and 'Cancel' buttons.

Under Add New SIP Trunk:

- **SIP URL:** The IP address of the 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:** If we should 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 a 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 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, 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 label. Select the **Extension** option (shown below), and enter the VDN to reach the skill set queue on the Communication Manager.

During compliance testing, VDN 56004 was configured on the Communication Manager. Then click on the **Add New Target** button to save this Target.

fonolo MANAGE TELCO STATS ADMIN Administrator Account Settings | Logout

Targets > Add New Target [? Help](#) [Cancel](#) [Add New Target](#)

Settings

Target Label: *Only visible through this interface.*

Phone Number: *Dial as a complete phone number; include the country code.*

Extension: *Dial as a direct extension (VDN/CDN); numeric digits only.*

When connecting using Fonolo Appliances, failed calls can be referred back to an alternate extension. When not set, failed calls are referred back to the Direct Extension.

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

By default, Fonolo assumes that this Phone Number/Extension connects directly to the skill/queue, without any IVR navigation. If this menu requires navigation to access the skill/queue, you must check this box to have Fonolo map out the IVR.

IVR Menu: *This number/extension has an IVR menu that Fonolo will need to navigate.*

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 CM 7.0** SIP trunk, added in **Section 7.1**, and then click the **Save Changes** button.

fonolo MANAGE TELCO STATS ADMIN Administrator Account Settings | Logout

Targets > Customer Service Agents [? Help](#) [Back to Targets](#)

SETTINGS TELCO SETTINGS HOURS ADVANCED SCHEDULES CALL-BACK LIMITS

Telco Settings [Save Changes](#)

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

Direct SIP: *Use this SIP Trunk.*

Fonolo Appliance: *No Appliance Groups defined. Visit the [Appliances Section](#) to add a new Appliance Group.*

7.3. Adding a New Call-Back Profile

Navigate to **Manage → Call-Back 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.

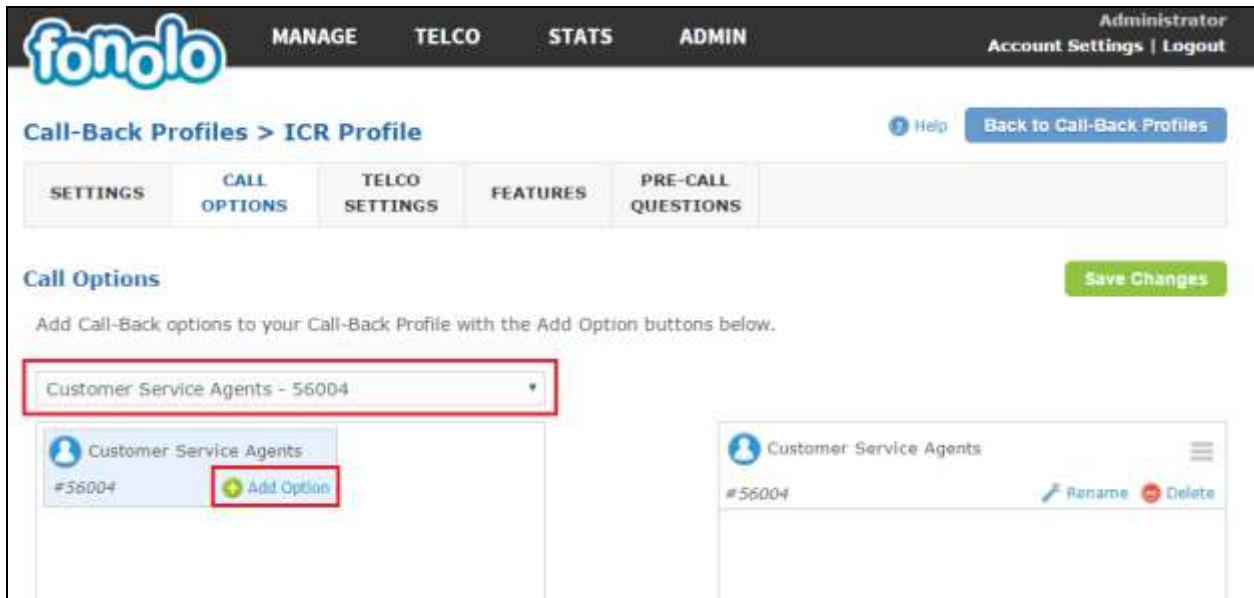
Click the **Add New Call-Back Profile** button to add this new profile.

The screenshot shows the 'Add New Call-Back Profile' form in the Fonolo administrator interface. The form is organized into two main sections: 'Settings' and 'Caller ID Settings'. The 'Settings' section includes three fields: 'Profile Label' (text input with value 'ICR Profile'), 'Channel' (dropdown menu with value 'In-Call Rescue'), and 'Language' (dropdown menu with value 'English'). The 'Caller ID Settings' section includes four fields: 'Customer CID Number' (text input with value '18005551234'), 'Customer CID Name' (text input with value 'Acme Company'), 'Agent CID Number' (text input with value '{{client_number}}'), and 'Agent CID Name' (text input with value 'Fonolo'). Each field has a corresponding help text to its right. The form is located on a page with a dark header containing the 'fonolo' logo and navigation tabs for 'MANAGE', 'TELCO', 'STATS', and 'ADMIN'. The user is logged in as 'Administrator' and can see 'Account Settings' and 'Logout' options. The page title is 'Call-Back Profiles > Add New Call-Back Profile'.

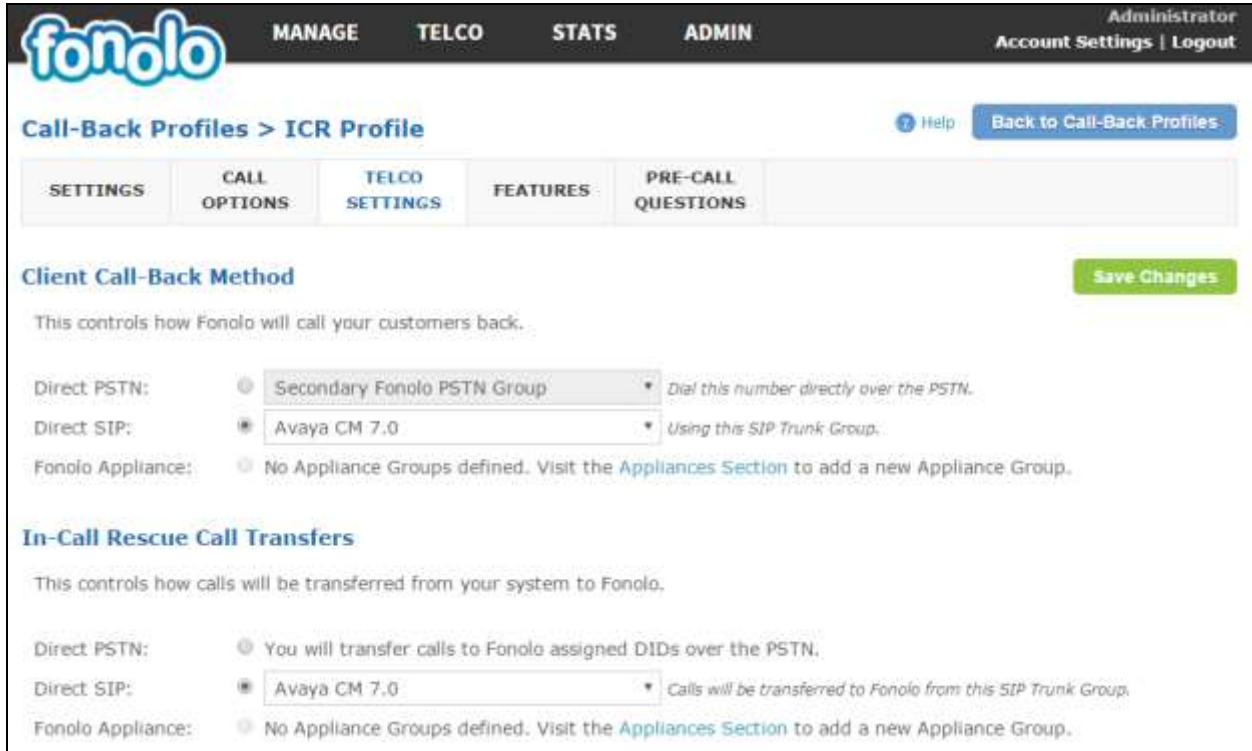
Field	Value	Help Text
Profile Label	ICR Profile	Only visible through this interface.
Channel	In-Call Rescue	This is the channel type: In-Call Rescue, Web, or Mobile.
Language	English	The language used for this channel.
Customer CID Number	18005551234	Caller ID number seen by customers.
Customer CID Name	Acme Company	Caller ID name seen by customer (only supported by some systems).
Agent CID Number	{{client_number}}	Caller ID number seen by your agents.
Agent CID Name	Fonolo	Caller ID name seen by your agents (only supported by some systems).

From the **Call Options** section of the new **Call-Back Profile**, select the Target added in **Section 7.2** (from the drop-down menu highlighted below), and click the **Add Option** link to add the VDN value to the section on the right, as shown below, then click the **Save Changes** button.

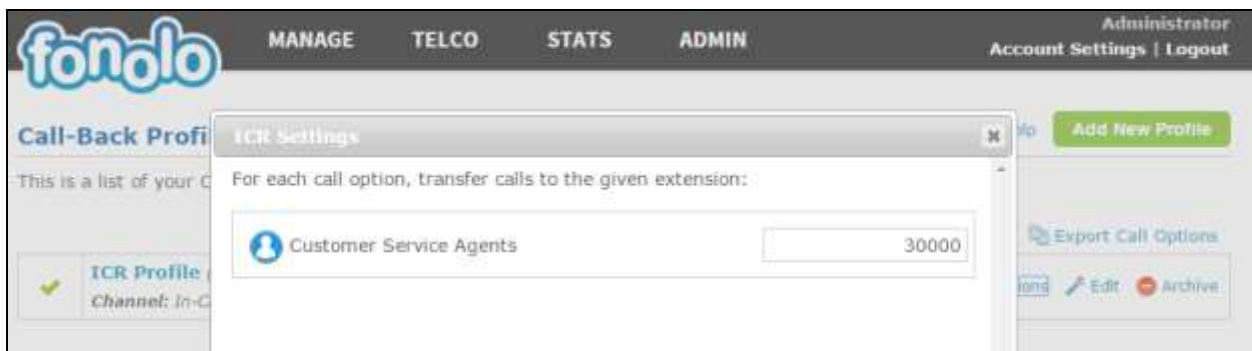
This associates the Target VDN with this new **Call-Back Profile**. Multiple call options can be associated with a single **Call-Back Profile**, one for each skill call-backs are being offered on.



From the **Telco Settings** section of the new **Call-Back Profile**, select the **Avaya CM 7.0** 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 the **Save Changes** button.



Navigate to **Manage → Call-Back Profiles** and click on the **In-Call Rescue** 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 each configured skill set VDN. These are the extensions to transfer calls to, on the Fonolo 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 5.5**. 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,

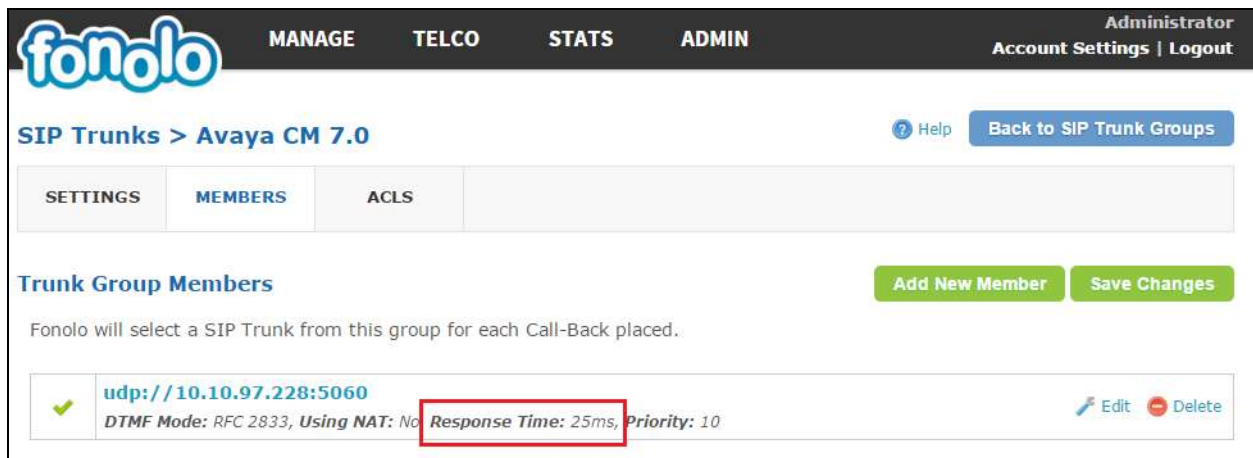
- PSTN caller is provided an announcement from Communication Manager to select a call back option or wait in the queue, when all agents are busy.
- PSTN caller is able to select the call back option and Communication Manager is able to direct this call to ICR.
- PSTN caller is able to hear the ICR menu 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 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.



The screenshot shows the Fonolo web portal interface. At the top, there is a navigation bar with the Fonolo logo and menu items: MANAGE, TELCO, STATS, ADMIN. On the right, it says 'Administrator Account Settings | Logout'. Below the navigation bar, the page title is 'SIP Trunks > Avaya CM 7.0'. There are tabs for 'SETTINGS', 'MEMBERS', and 'ACLS'. The 'MEMBERS' tab is active. Below the tabs, there are two green buttons: 'Add New Member' and 'Save Changes'. The main content area shows a list of SIP Trunk Group Members. The first member is 'udp://10.10.97.228:5060' with a green checkmark icon. Below the URL, it says 'DTMF Mode: RFC 2833, Using NAT: No' and 'Response Time: 25ms, Priority: 10'. The 'Response Time' value is highlighted with a red box. There are 'Edit' and 'Delete' icons to the right of the member entry.

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 ICR to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Session Manager 7.0. 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. *Implementing Avaya Aura® Session Manager* Document ID 03-603473.
2. *Administering Avaya Aura® Session Manager*, Doc ID 03-603324.
3. *Deploying Avaya Aura® System Manager*, Release 7.0.
4. *Administering Avaya Aura® System Manager for Release 7.0*, Release 7.0.
5. *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*.
6. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.7.
7. *Administering Avaya Aura® Communication Manager*, Release 7.0, 03-300509.
8. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, 555-245-205.

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

©2016 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.