Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Dialogic® ControlSwitch™ System with Avaya Aura® Session Manager R6.3, Avaya Aura® Experience Portal 7.0 and Avaya Proactive Outreach Manager 3.0 using SIP Trunking - Issue 1.0

Abstract

These Application Notes describe the procedure to configure Dialogic® ControlSwitch™ System to interoperate with Avaya Aura® Session Manager, Avaya Aura® Experience Portal 7.0 and Avaya Proactive Outreach Manager 3.0 using SIP trunking.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 procedure to configure Dialogic® ControlSwitch™ System to interoperate with Avaya Aura® Session Manager, Avaya Aura® Experience Portal 7.0 and Avaya Proactive Outreach Manager 3.0 using SIP trunking for Proactive outbound calls.

The Dialogic® ControlSwitch™ System is an IP softswitch that provides a smooth migration path from existing TDM voice networks to the Next Generation Network/IP Multimedia Subsystem (NGN/IMS) by enabling the interconnection of a mix of traditional and IP-based voice networks. The complete system will hereafter be referred to as ControlSwitch.

This compliance testing primary focus is on the ControlSwitch and its SIP-ISUP gateway functions.

2. General Test Approach and Test Results

The interoperability compliance test included outbound calls and serviceability. During the test, various outbound call scenarios were exercised including complete and incomplete call attempts to verify call interoperability of Dialogic® ControlSwitch™ with Dialogic® I-Gate® 4000 Edge Media Gateway and Avaya products. Network and server outage conditions were used to verify serviceability of the joint solution.

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 primary focus of the testing was to verify proactive outbound calls through SIP trunk and verifying the interoperability between an Avaya SIP-based network and Dialogic® ControlSwitch™ System. Test cases were selected to verify the following areas.

Basic Interoperability:

- Basic outbound calls with playback announcement
- Multiple codecs support, e.g. G.711MU and G.729A
- Codec Negotiation
- DTMF Support using inband and out of band
- Call display of far end user
- Incomplete call attempts for various scenarios like far end busy, no answer, number unallocated, no route to destination, no circuit or call rejected by network

At the same time, Proactive Outreach Manager Outbound Call Details report were checked for all call scenarios.

The serviceability testing focused on verifying the ability of the solution to recover from adverse conditions, such as network failures and ControlSwitch System reboot.

2.2. Test Results

All test cases were executed and verified. The following were not tested:

- Out of band DTMF as the test setup doesn't support to NAT the public IP in the contact header of the INFO message.
- G.729 codec was tested but not other variance though it was indicated that Dialogic Media Gateway can support them.

2.3. Support

Technical Support on Dialogic® ControlSwitch™ System can be obtained through the following phone contacts:

- Phone: +1 866 535 0946
- E-mail: GlobalSupport@dialogic.com

3. Reference Configuration

The reference configuration consists of Communication Manager, Session Manager, System Manager, Experience Portal, Proactive Outreach Manager and ControlSwitch. Proactive Outreach Manager (POM) is installed with Avaya Aura® Experience Portal Manager on the same server with Avaya Aura® Media Processing Platform (MPP) on a separate server. Dialogic® I-Gate® 4000 Edge Media Gateway is used as a SIP/ISUP gateway for PSTN access for Dialogic® ControlSwitch™. Session Manager functions as a SIP proxy for Communication Manager with a G430 Media Gateway. Session Manager, managed through System Manager, routes calls between different entities using SIP Trunks. SIP Trunking between Session Manager and (MPP) is done over private network within the Local Area Network (LAN). SIP Trunking between Session Manager and ControlSwitch is done over public internet because of the impossibility to co-locate the equipment. The test configuration shows an enterprise site connected to Dialogic® ControlSwitch™ through the public IP network. For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out throughout the document. A complete discussion of the configuration for connectivity over public network is beyond the scope of these Application Notes. However, it should be noted that SIP and RTP traffic between the Dialogic ControlSwitch and Avaya network must be allowed to pass through the public internet.

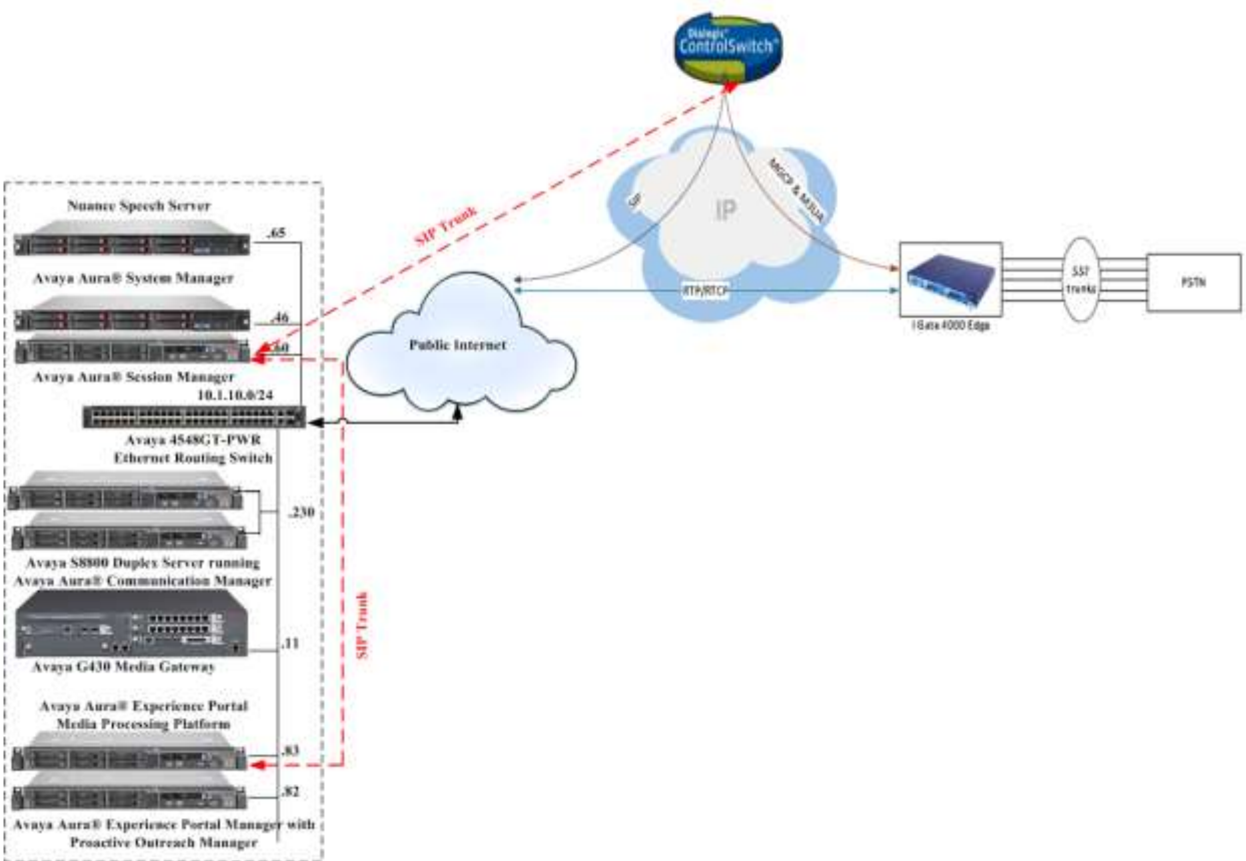


Figure 1 – Sample configuration

4. Equipment and Software Validated

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

Equipment/Software	Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	6.3.11 (Build R016x.03.0.124.0-22361)
Avaya G430 Media Gateway	FW 36.14.0
Avaya Aura® Session Manager running on VMware 5.5	6.3.14.11.3595
Avaya Aura® System Manager running on VMware 5.5	6.3.14.0.631402
Avaya Aura® Experience Portal running on VMware 5.1	EPM - 7.0.1.0.1601 MPP - 7.0.1.0.1605
Proactive Outreach Manager	3.00.01.00.150
Nuance Speech Server on Microsoft Windows Server 2003	5.0
RealSpeak Text-to-Speech (TTS) on Microsoft Windows Server 2003	4.5.0.0
Dialogic® ControlSwitch™ System	5.9.2.62-03
Dialogic® Media Gateway I Gate® 4000 Edge	C2.8.2.47

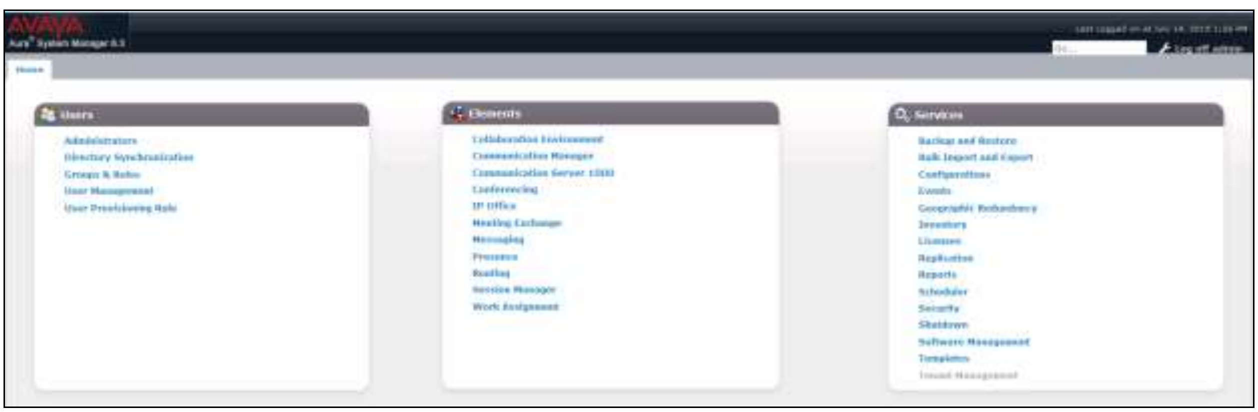
5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, assuming the basic configuration has been installed and licensed including SIP Trunks setup with Communication Manager. For information on these installation tasks refer to **[1]** & **[2]** in the Additional References **Section 11**. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to System Manager
- Identify the SIP Domain
- Identify the Locations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns

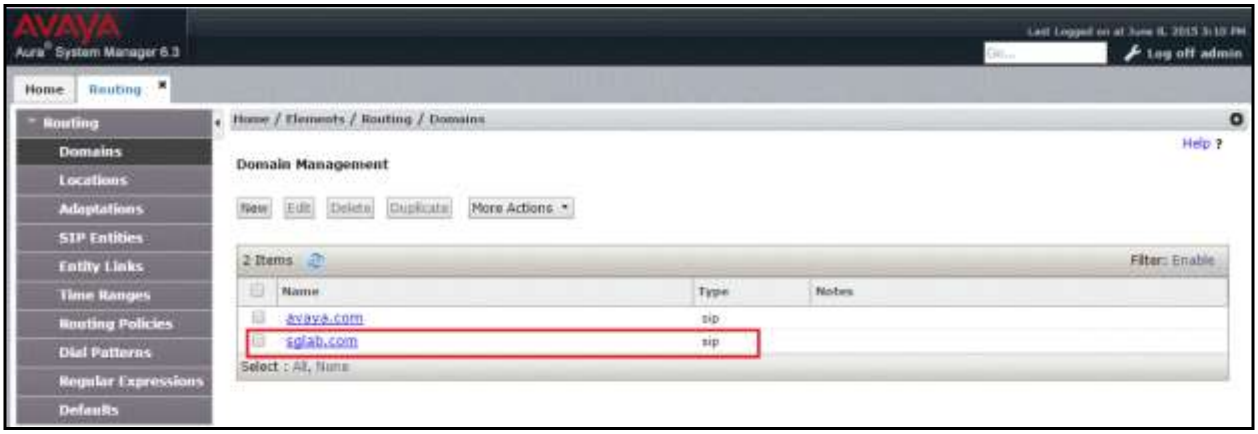
5.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering **http://<FQDN** or **IP Address>/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown). The menu shown below is displayed. Click on **Elements → Routing**.



5.2. Identify the SIP Domain

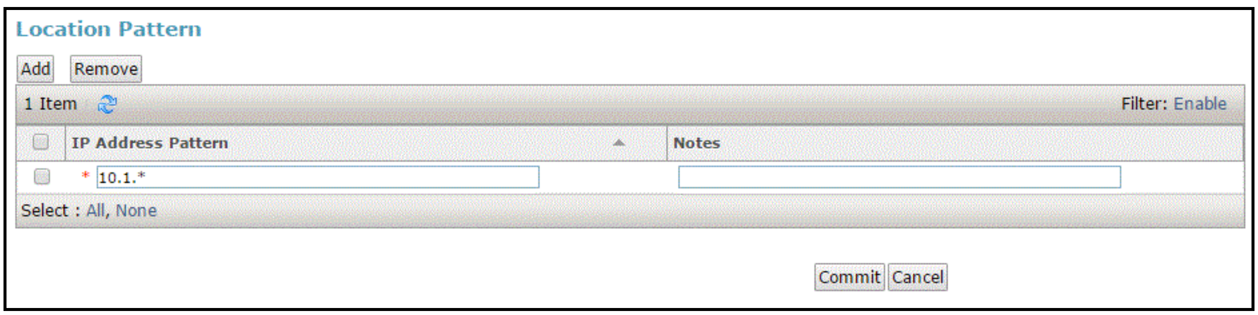
SIP domains are created as part of Session Manager basic configuration. There will be at least one for which System Manager is the authoritative SIP controller. Navigating from the Home screen, under the **Elements** section click **Routing → Domains**. In this compliance testing, note the SIP domain **sglab.com** is used in later part of the configuration.



5.3. Identify the Locations

Session Manager uses the origination location to determine which dial patterns to look at when routing a call. In this example, one Location has already been created during basic installation which will reference both the Session Manager, Experience Portal and ControlSwitch location. Navigate to **Home → Elements → Routing → Locations** and note the location name.

Select **Location1** and at the bottom of the same page the **Location Pattern** is defined. Note the Location pattern already defined as part of basic installation. In this case the **IP Address Pattern** is **10.1.*** as shown below.



5.4. Administer SIP Entities

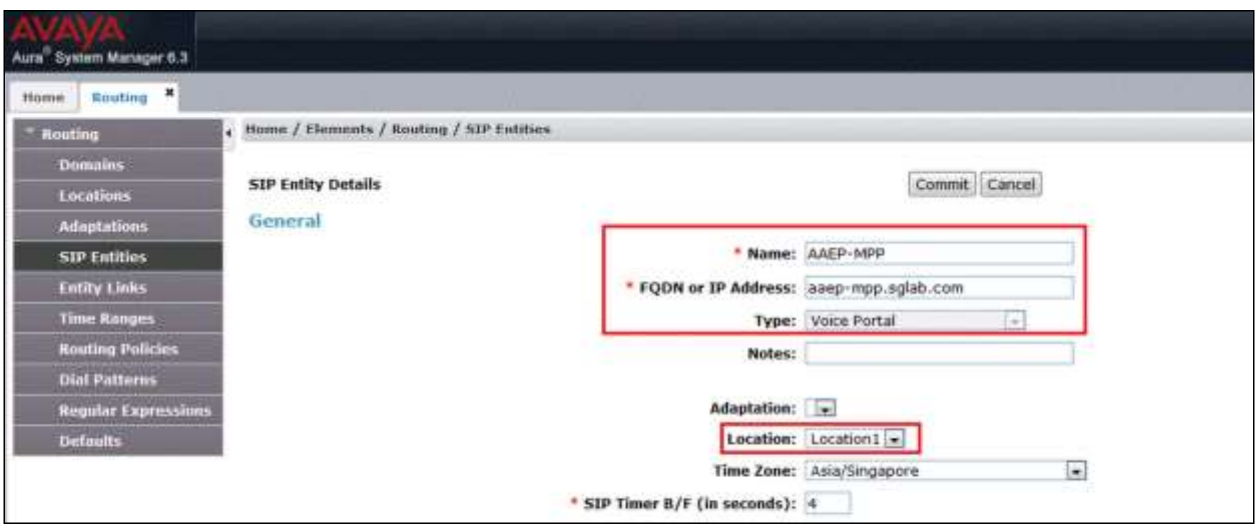
Each SIP device (other than Avaya SIP Phones) that communicates with Session Manager requires a SIP Entity configuration. This section details the steps to create SIP Entities for MPP and ControlSwitch respectively.

5.4.1. Session Manager SIP Signaling Interface Entity

Click **Home → Elements → Routing → SIP Entities** and note the existing Session Manager **sm1** already defined during basic installation.

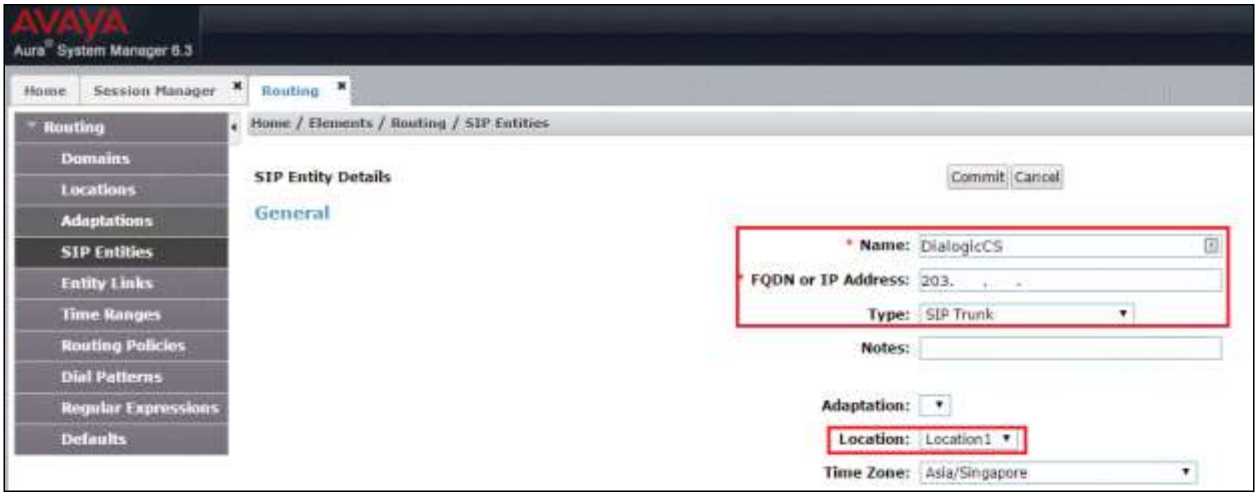
5.4.2. Configure Avaya Aura® Media Processing Platform SIP Entity

Click **Home → Elements → Routing → SIP Entities → New** assign an identifying **Name**, the **FQDN or IP Address** for the MPP, set the **Type** to **Voice Portal** and the **Location** as **Location1**; leave all other settings default and click **Commit**.



5.4.3. Configure Dialogic® ControlSwitch™ SIP Entity

Click **Home → Elements → Routing → SIP Entities → New** assign an identifying **Name**, the **FQDN or IP Address** for the ControlSwitch, set the **Type** to **SIP Trunk**, select **Location** as **Location1;** and leave all other settings default and click **Commit**.



5.5. Administer SIP Entity Link

A SIP Trunk between a Session Manager and a telephony system is described by an Entity Link. An entity link needs to be created between Session Manager with both MPP and ControlSwitch.

5.5.1. Administer SIP Entity Link from Avaya Aura® Session Manager to Avaya Aura® Media Processing Platform (MPP)

Click on **Home → Elements → Routing → Entity Links → New** assign an identifying **Name**. Choose the entity assigned to the Session Manager SIP Signaling Interface as **SIP Entity 1**, set the **Protocol** as **TCP**, enter **5060** for the **Port**, choose the MPP entity as **SIP Entity 2** and set the **Port** to **5060**, select **Trusted** from the **Connection Policy** drop-down list. Click **Commit** when done. This establishes the Session Manager end of the SIP Trunk to MPP.

5.5.2. Administer SIP Entity Link from Avaya Aura® Session Manager to Dialogic® ControlSwitch™

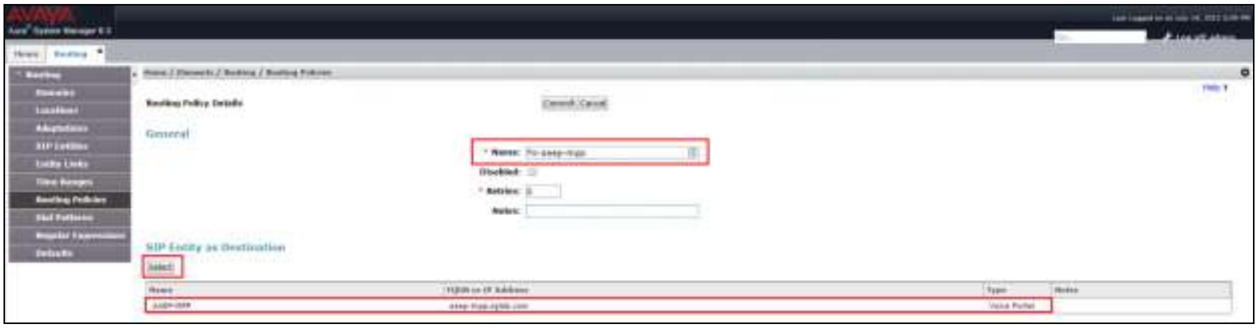
Click on **Home** → **Elements** → **Routing** → **Entity Links** → **New** assign an identifying **Name** choose the entity assigned to the Session Manager SIP Signaling Interface as **SIP Entity 1**, set the **Protocol** as **UDP**, enter **5060** for the **Port**, choose the ControlSwitch entity as **SIP Entity 2** and set the **Port** to **5060**, select **Trusted** from the **Connection Policy** drop-down list. Click **Commit** when done. This establishes the Session Manager end of the SIP Trunk to ControlSwitch.

5.6. Administer Routing Policies

To complete the routing configuration, a Routing Policy is created. Routing policies direct how calls will be routed to an attached system. Two routing policies must be created, one for ControlSwitch and the other for MPP. These will be associated with the Dial Patterns created in **Section 5.7**.

5.6.1. Create Routing Policy to Avaya Aura® Media Processing Platform

Click **Home → Elements → Routing → Routing Polices →New** assign an identifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select** and choose the MPP SIP Entity and click **Select**. Click **Commit** when done.



5.6.2. Create Routing Policy to Dialogic® ControlSwitch™

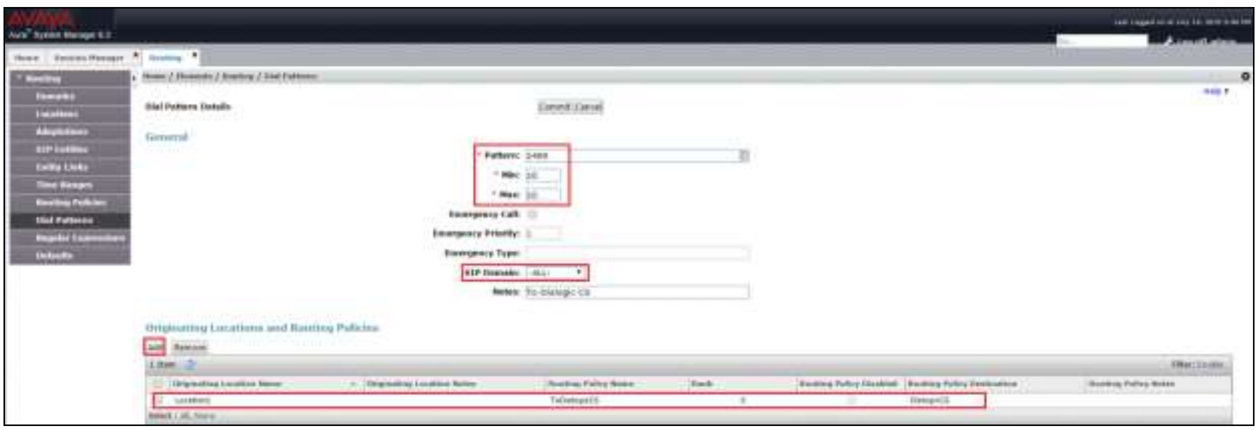
Click **Home → Elements → Routing → Routing Polices →New** assign an identifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select** and choose the ControlSwitch SIP Entity and click **Select**. Click **Commit** when done.

5.7. Administer Dial Patterns

As one of its main functions, Session Manager routes SIP traffic between connected devices. Dial Patterns are created as part of the configuration to manage SIP traffic routing, which will direct calls based on the number dialed to the appropriate system.

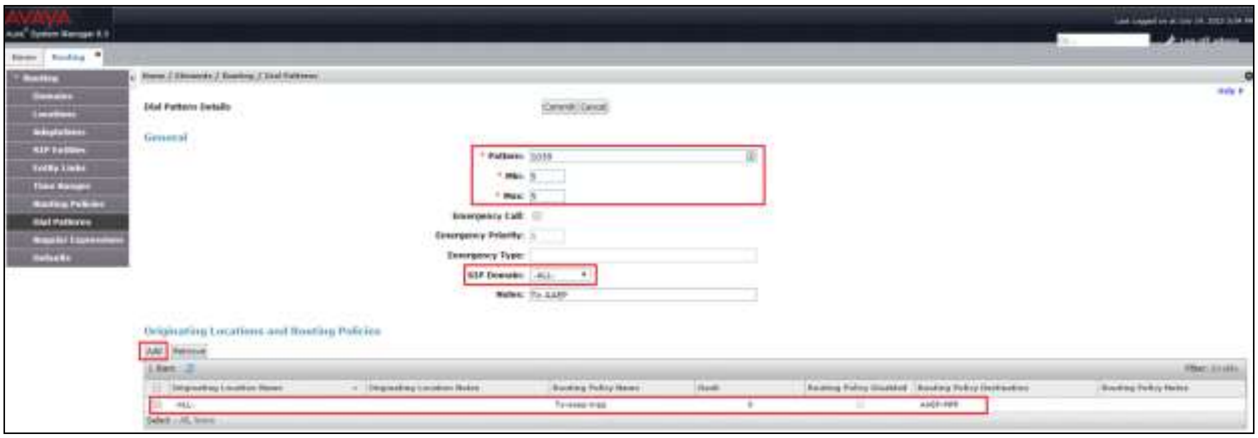
5.7.1. Create Dial Pattern to Dialogic® ControlSwitch™

Click **Home → Elements → Routing → Dial Patterns →New.** Under **Pattern** enter the numbers destined for ControlSwitch, in the **Pattern** box. Set **Min** and **Max** digit string length, and set **SIP Domain** to **ALL**. In the **Originating Locations and Routing Policies** section of the web page, click **Add.** In the **Origination Location** section (not shown) click the location specified in **Section 5.3**, in the **Routing Policies** section (not shown) click the routing policy created for ControlSwitch. Click **Select** when done. Click **Commit** when complete.



5.7.2. Create Dial Pattern to Avaya Aura® Media Processing Platform (MPP)

An additional Dial Pattern must be created on Session Manager to route incoming calls to MPP such as calls from Communication Manager. Click **Home → Elements → Routing → Dial Patterns →New.** Under **Pattern** enter the numbers presented to Session Manager by Communication Manager destined to MPP in the **Patterns** box. Set **Min** and **Max** digit string length, and set **SIP Domain** to **ALL**. In the **Originating Locations and Routing Policies** section of the web page, click **Add.** In the **Origination Location** section (not shown)**,** click **ALL**, in the **Routing Policies** section (not shown) click the routing policy created for MPP. Click **Select** when done. Click **Commit** once finished.



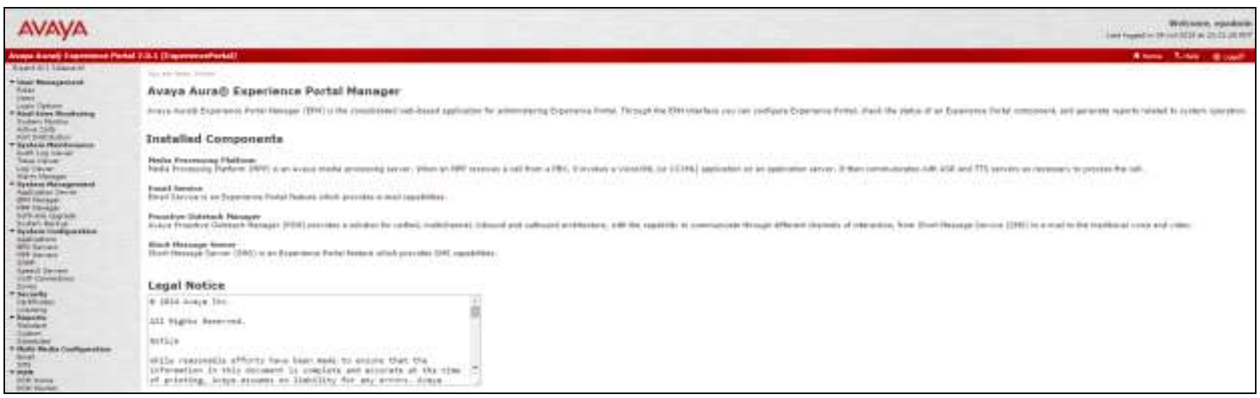
6. Configure Avaya Aura® Experience Portal

This section provides the procedures for configuring Experience Portal, assuming the basic configuration has been installed and licensed including the MPP. For information on these installation tasks refer to **[4]** & **[5]** in the Additional References **Section 11**. The procedures include the following areas:

- Log in to Experience Portal Manager (EPM)
- Administer Text-To-Speech (TTS) Speech Server
- Administer VoIP connections to Session Manager
- Administer MPP VoIP settings

6.1. Log in to Avaya Aura® Experience Portal Manager

Access the EPM using a Web Browser by entering **http://<FQDN or IP Address >/VoicePortal**, where **<FQDN>** is the fully qualified domain name of EPM. Log in using appropriate credentials (not shown). The menu shown below is displayed.

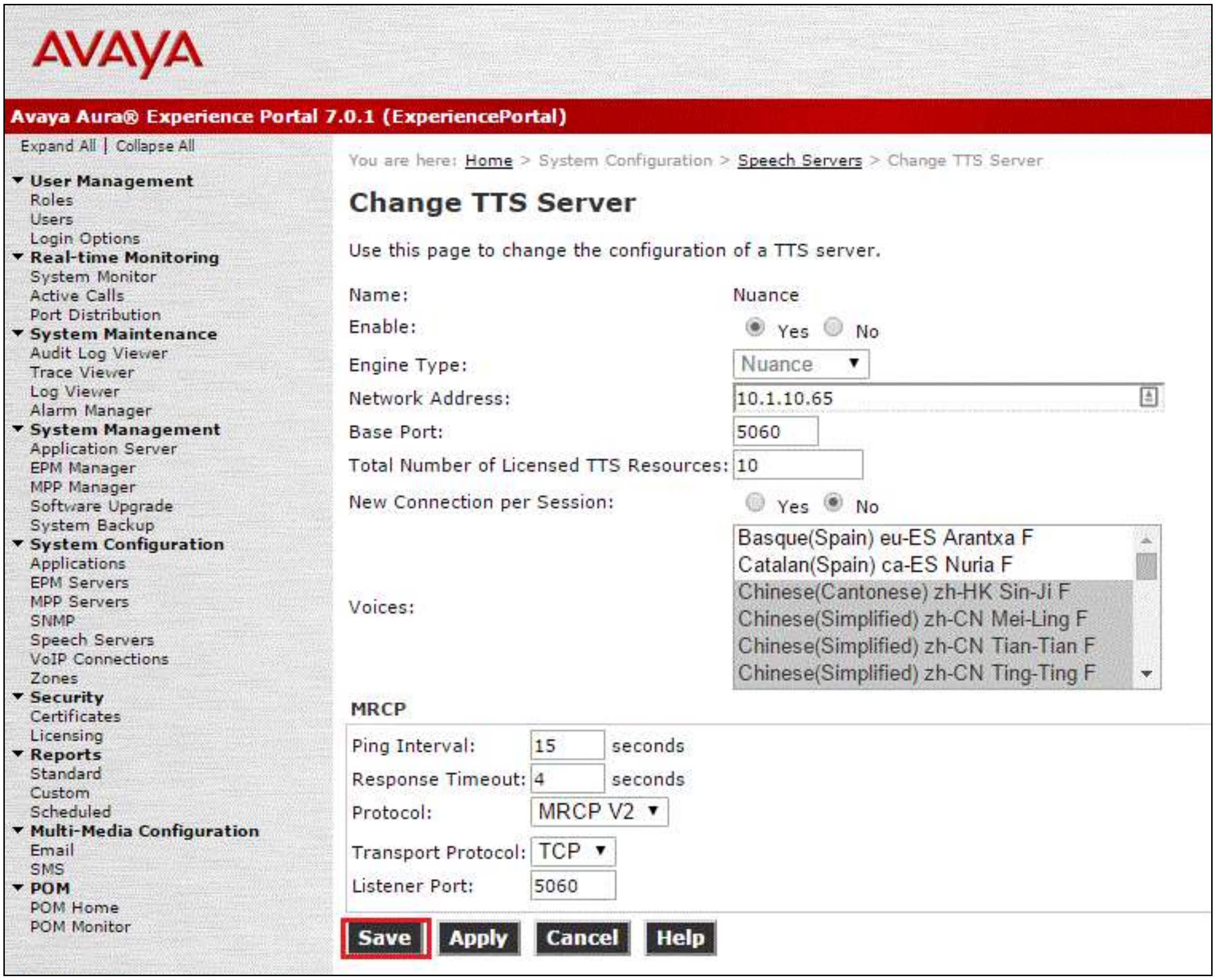


6.2. Administer Text-To-Speech (TTS) Speech Server

In this compliance test, Nuance is used to provide the TTS resources. This section provides the procedures for configuring using Nuance as TTS Server. Nuance is use in PomDriverApp applications as TTS resource in **Section 7.1**.

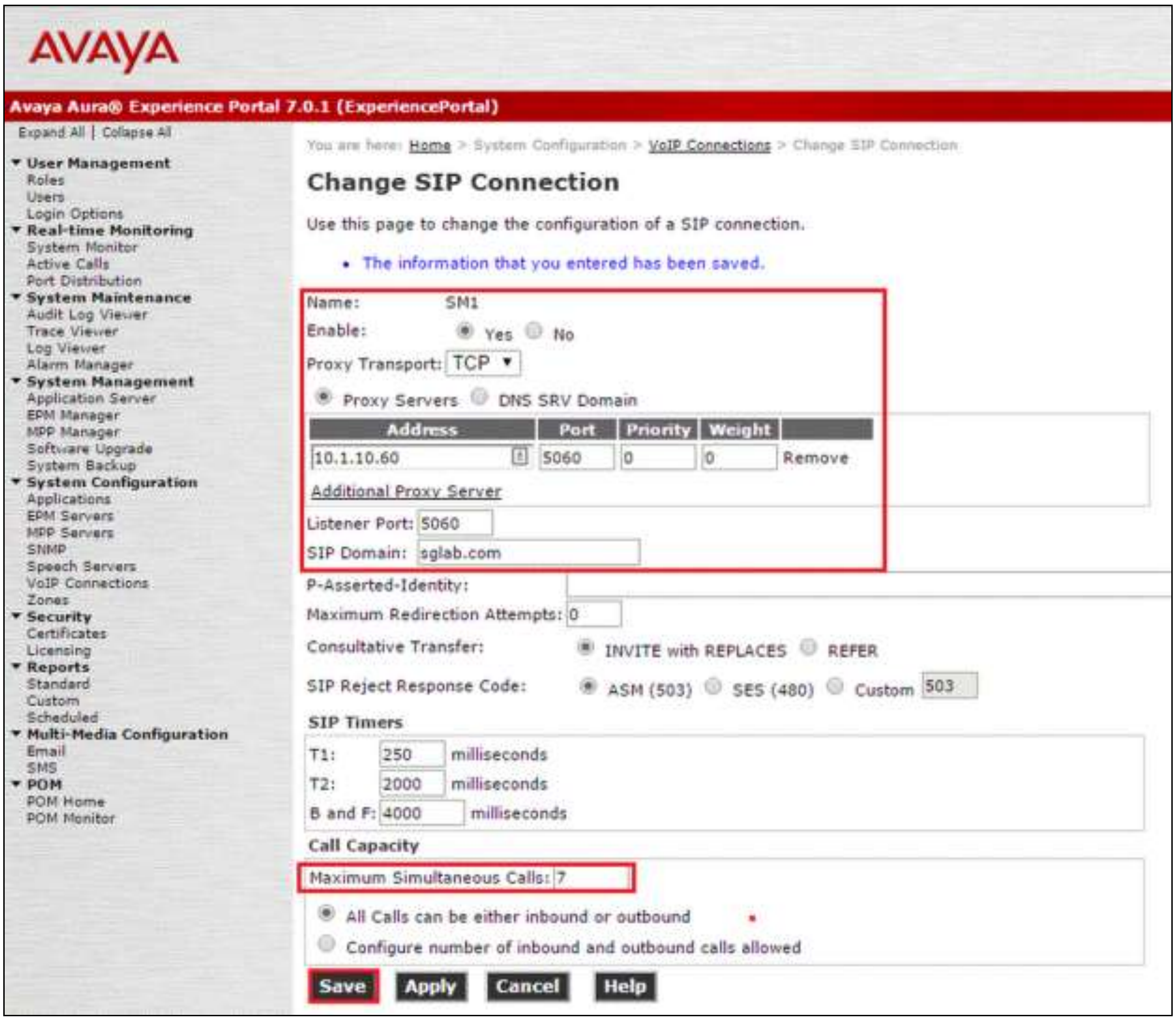
6.2.1. Adding TTS Server

Under **System Configurations** on the left panel, click **Speech Servers → TTS tab → Add** (not shown). In the form presented, enter appropriate **Name** and **Enable** the server. Select **Engine Type** as **Nuance**. Enter **Network Address** of the Nuance Server, the **Base Port** as **5060** and the **Total Number of Licensed TTS Resources** available depending on the license on the Nuance and EPM. Configure the **Protocol** supported by Nuance as appropriate. Leave all other settings default and click **Save** to complete. Below are the configured Nuance TTS Server used during the compliance testing.



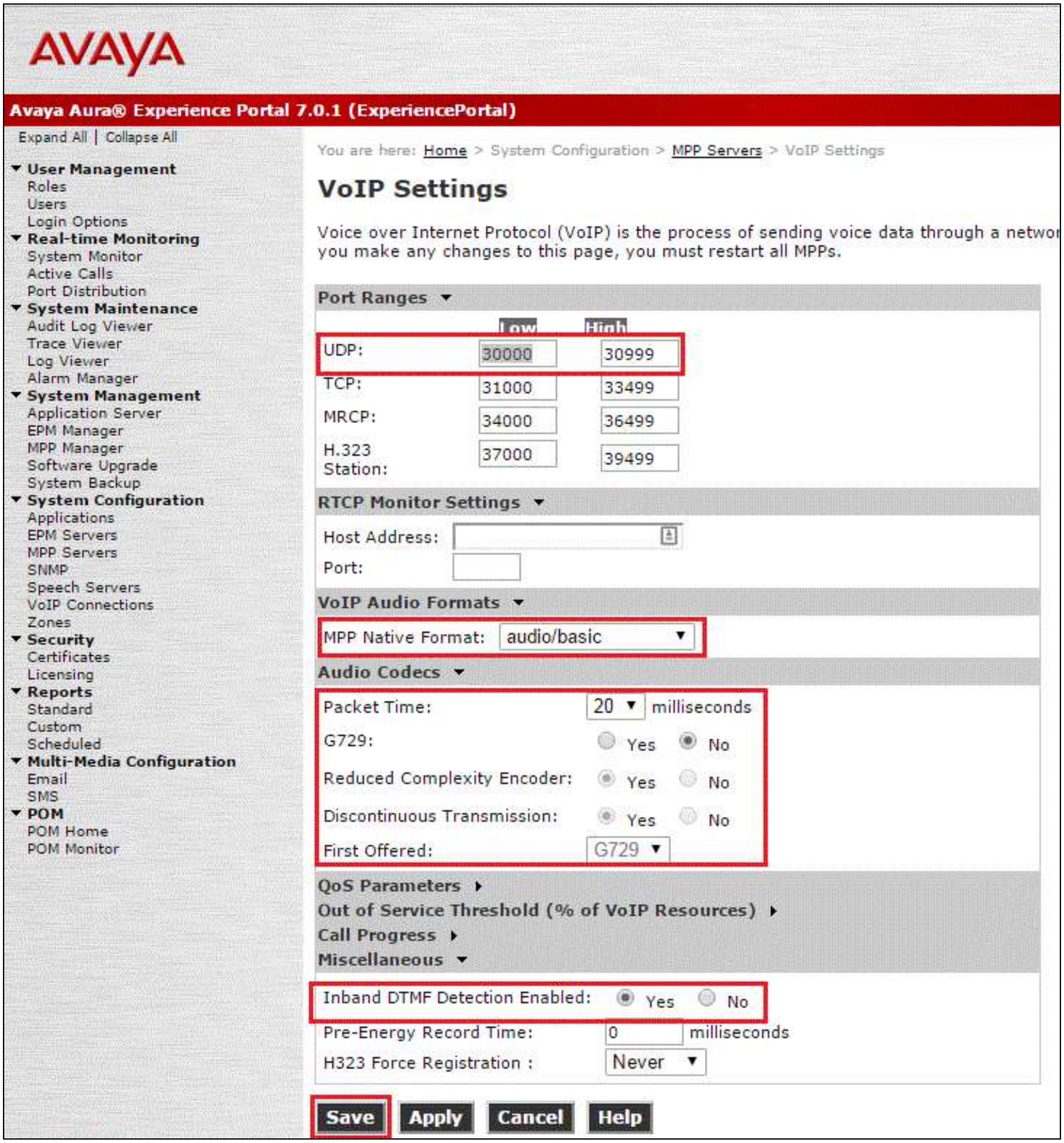
6.3. Administer SIP Connections to Session Manager

In this compliance testing, SIP trunk will be used for both inbound and outbound calls to/from the MPP. Under **System Configurations** on the left panel, click **VoIP Connections → SIP tab → Add**. In the form presented, enter appropriate **Name** and **Enable** the VoIP connections. Click **TCP** from the drop down list in the **Proxy Transport** corresponding to the transport administered in the SIP Entity Link in **Section 5.5.1**. Enter the IP address of the Session Manager in **Address** and **Port 5060**. Enter the **Listener Port** as **5060** and the **SIP Domain** as **sglab.com** defined in **Section 5.2** for Session Manager; leave all other settings default and click **Save**.



6.4. Administer MPP VoIP Settings

Under **System Configurations** on the left panel, click **MPP Servers → VoIP Settings** (not shown). Set the **UDP Port Ranges** between **Low** and **High** mark as desired for the RTP traffic. Under **VoIP Audio Formats**, select **audio/basic** from drop down list of **MPP Native Format** for mu-Law encoding format. In Audio Codecs, click **G729** as **No** if audio data compression for SIP connections if G711 is desired. Set **the Inband DTMF Detection Enabled** as **Yes** under **Miscellaneous** to support Inband DTMF. Leave all other settings default and click **Save**.



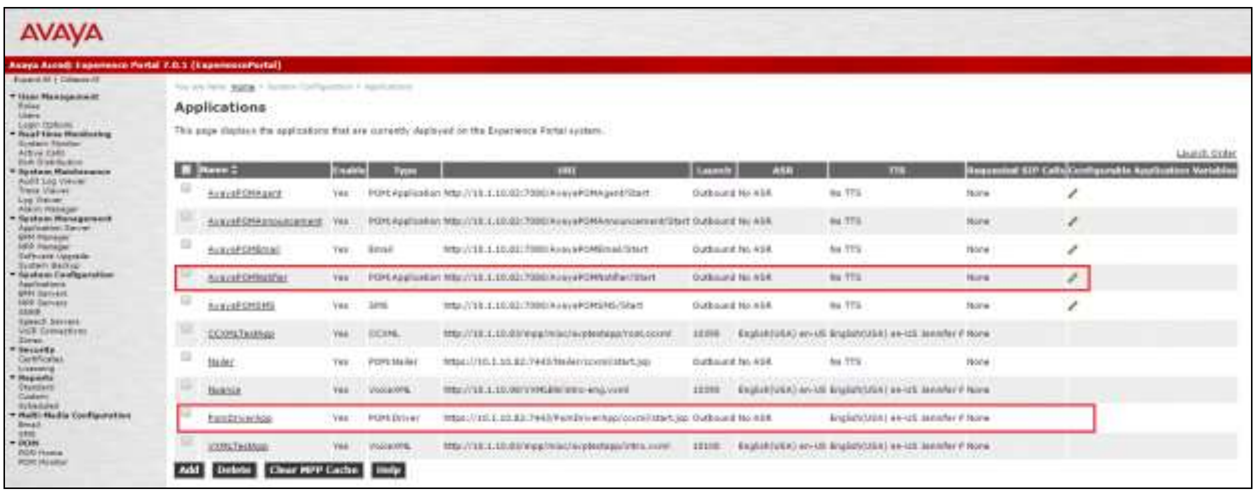
7. Configure Avaya Outreach Manager (POM)

This section provides the procedures for configuring POM, assuming the basic configuration has been installed and licensed. For information on these installation tasks refer to **[6]** in the Additional References **Section 11**. POM administration is done through the EPM (installed with plugin) and login procedures is as detailed in **Section 6.1**. The procedures include the following areas:

- Configure Applications
- Create Campaigns

7.1. Create Applications

The basic configuration of POM stock applications include **PomDriverApp** and **AvayaPOMNotifier** which setup will not be detailed here as this is part of the basic installation. For more information on these tasks refer to **[6]** in the Additional References **Section 11**. The**PomDriverApp** application manages the execution of outbound calls and **AvayaPOMNotifier** plays a recorded welcome message followed by a simple Text-To-Speech (TTS) text; will be used for running the campaign to make outbound calls. Note that the **PomDriverApp** uses the TTS from Nuance Speech Server.

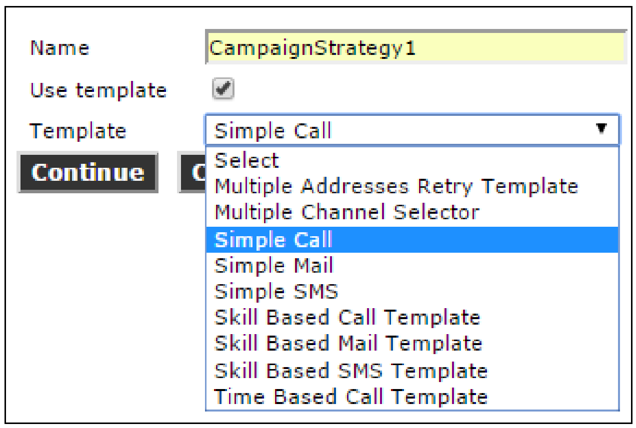


7.2. Create Campaigns

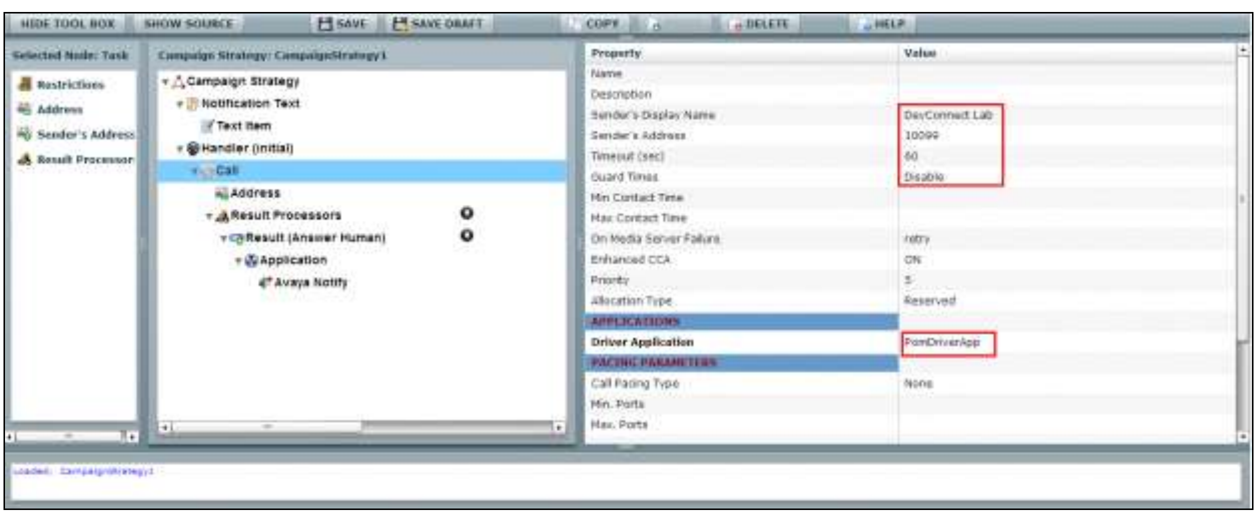
Campaign was created and run manually for testing outbound voice calls. To do that, campaign strategies using a simple call template and contact list were created.

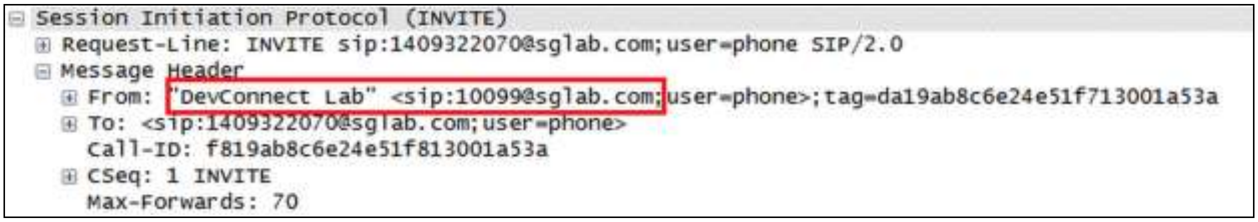
7.2.1. Campaign Strategies

Under **POM→ POM Home** (not shown) on the left panel, click from the drop down menu of **Campaign → Campaign Strategies → Add** (not shown) and provide an appropriate **Name** for the campaign strategy. Check **Use template** and select **Simple Call** from the drop down list as below.

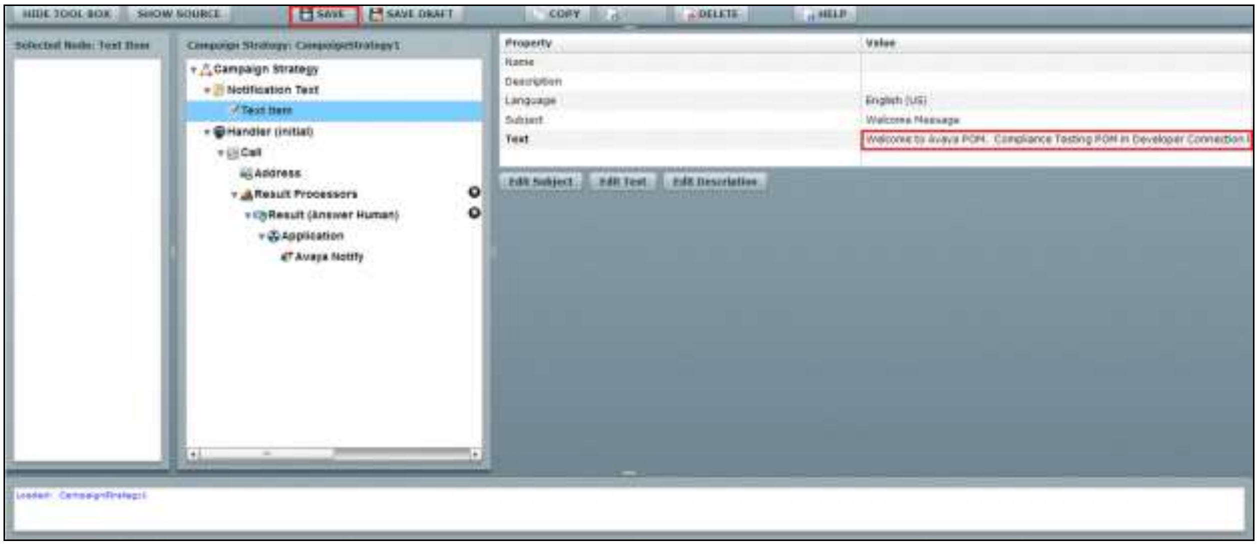


Click **Continue** and the following form pops out. Click on **Call** and under **APPLICATIONS - Driver Application** on the far right panel, select from the drop down menu **PomDriverApp** to handle outbound calls. Enter the desired **Sender's Display Name** and **Sender's Address** which will reflect in the **From**: message header in *SIP INVITE* shown in the bottom screenshot of trace taken. The **Guard Times** is set to "**Disable**" during this test to disable any time restriction for outbound calls. **Timeout (sec)** is set at **60** seconds to allow called party sufficient time to answer.



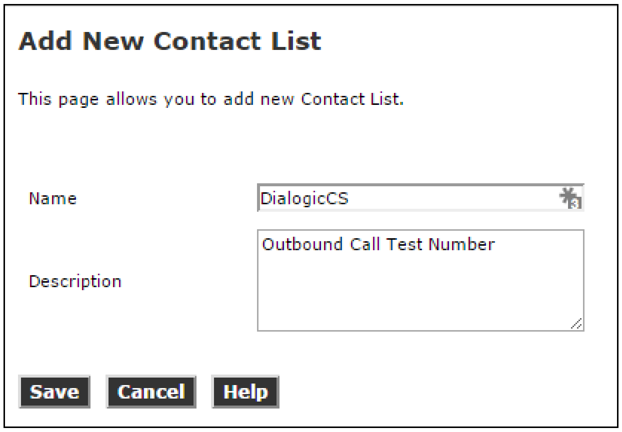


A text is also created for the Text-To-Speech (TTS) engine to be used for the outbound call where far end will hear the annoucement. Click **Notification Text → Text** on the **Property** column on far right panel and enter the desired TTS annoucement for called party to hear. Click **Save** once finished.

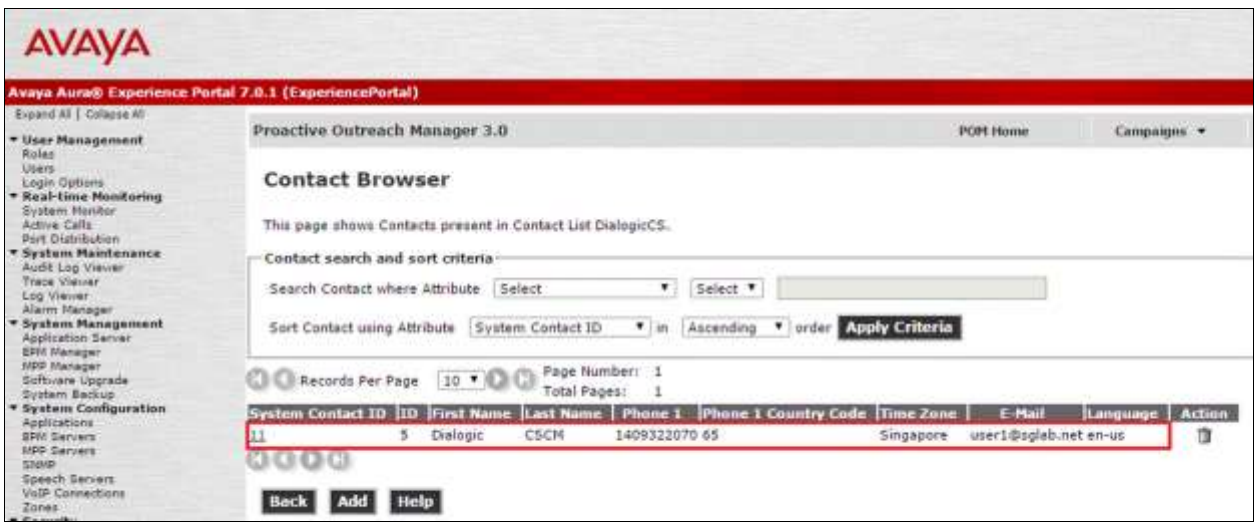


7.2.2. Contact List

Under **POM → POM Home** on the left panel, click from the drop down menu of **Contacts → Contact Lists → Add** (not shown) and provide an appropriate **Name** for the Contact List with **Description** as sample below. Upon completion, click **Save**.



Subsequently, select the upload of the Contact List (not shown) prepared in proper text format. Below is the Contact List created for the outbound call to ControlSwitch.



8. Configure Dialogic® ControlSwitch™ System

For the compliance test, two trunking interfaces were configured on Dialogic® ControlSwitch™. A SIP trunk interface was used to connect to Session Manager and an ISUP SS7 interface was used to connect to PSTN through Dialogic® I-Gate™ 4000 Edge Media Gateway. This section focuses on the configuration at the SIP side which enabled ControlSwitch to interoperate with Session Manager and Experience Portal.

It is assumed that basic administration such as IP addresses, default gateways and loaded with the software along with the other elements have been configured during installation. It is also assumed that the PSTN trunk has been properly configured, which includes the ISUP SS7 trunk group associated I-Gate 4000 Edge and the underlining E1 interface.

This section provides the procedures for configuring ControlSwitch, assuming it has been installed and licensed. The procedures include the following items:

- Launch EMS Management Interface
- Configure Local Gateway
- Configure SIP Trunk Group
- Configure Routing Configuration

8.1. Launch Management Interface

ControlSwitch is administered using an EMS web based management user interface. To access the interface, enter **http://<ip-addr>** as the URL in a web browser where <ip-addr> is the IP Address of the Dialogic ControlSwitch EMS. Enter the appropriate credentials to log in. The following screenshot is displayed.

8.2. Configure Local Gateway

Prerequisite

• Interactive Connectivity Establishment (ICE) need to be provisioned.

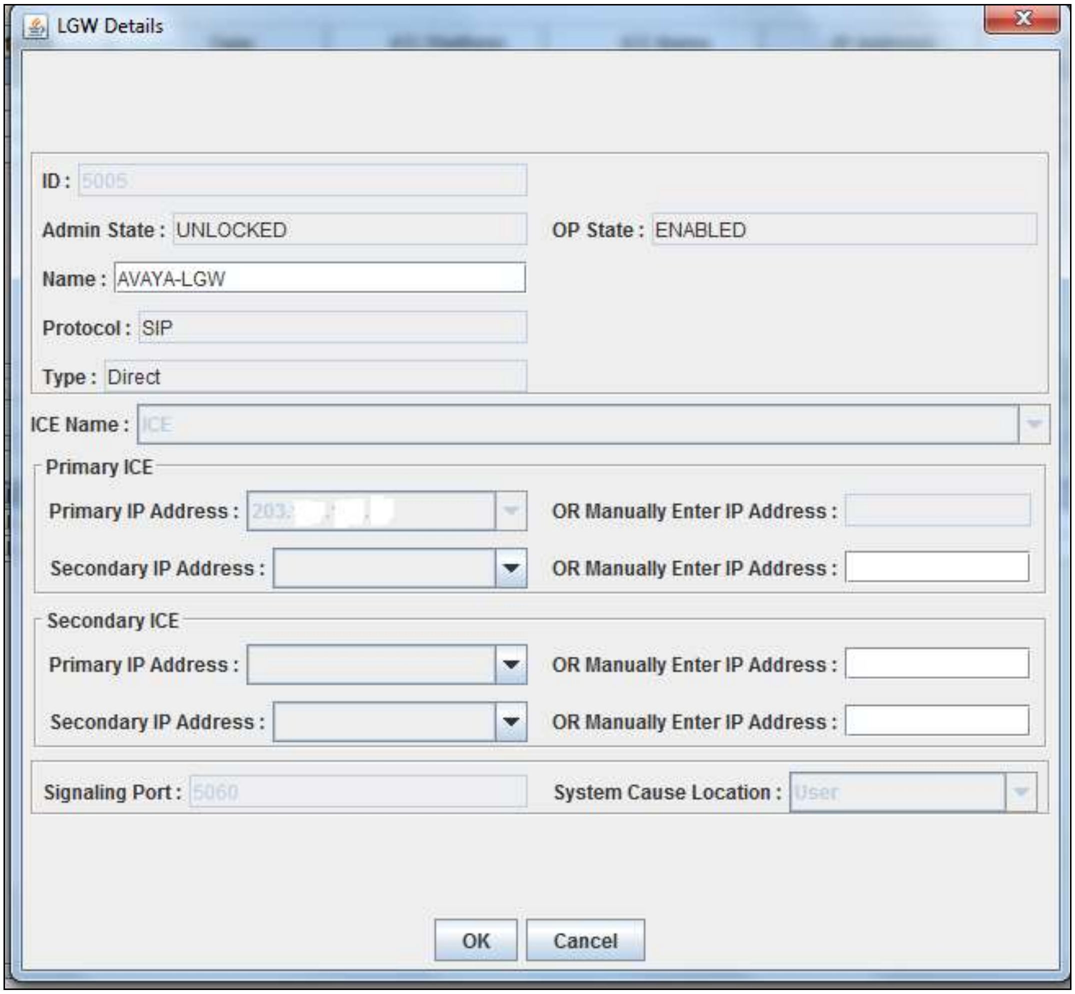
To create an SIP (Direct type) Local Gateway:

1. Select **Network Elements → Local Gateway → Create Icon**(not shown).
2. Use the following fields on the **Local Gateway Maintenance** to enter the entries and selections to create the local gateway:
    - **Name –** Provide appropriate name
    - **Protocol** - select **SIP**
    - **Type** - select **Direct**
    - **ICE Name –** Provide appropriate name
    - **IP Address** of local gateway
    - **Signaling Port**
        - For SIP, the valid signaling port value is **5060** or a number within the range of 2000 through 3000.
    - **System Cause Location** — select **User**

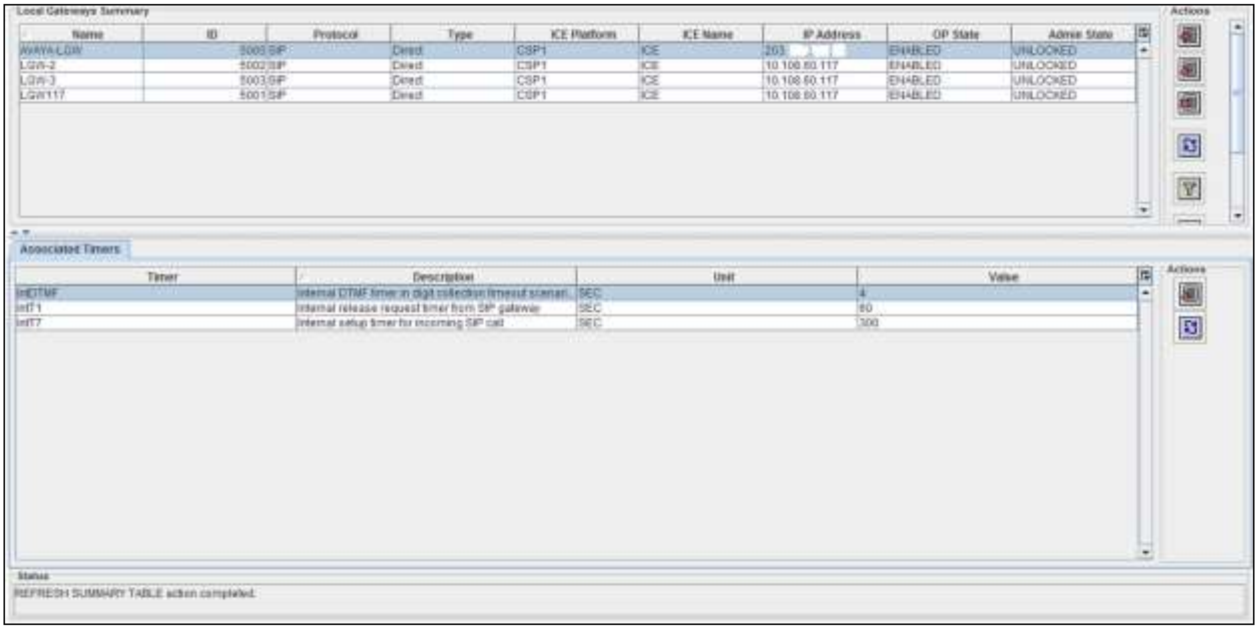
Leave all other settings as default. Click **OK** to complete.

Note: For the compliance test there is only one IP address defined on the Local Gateway. But it is a recommended practice to set the secondary IP address if there is any network level redundancy.

Below is the Avaya Local Gateway screenshot.



Below is the Local Gateways Summary screenshot.

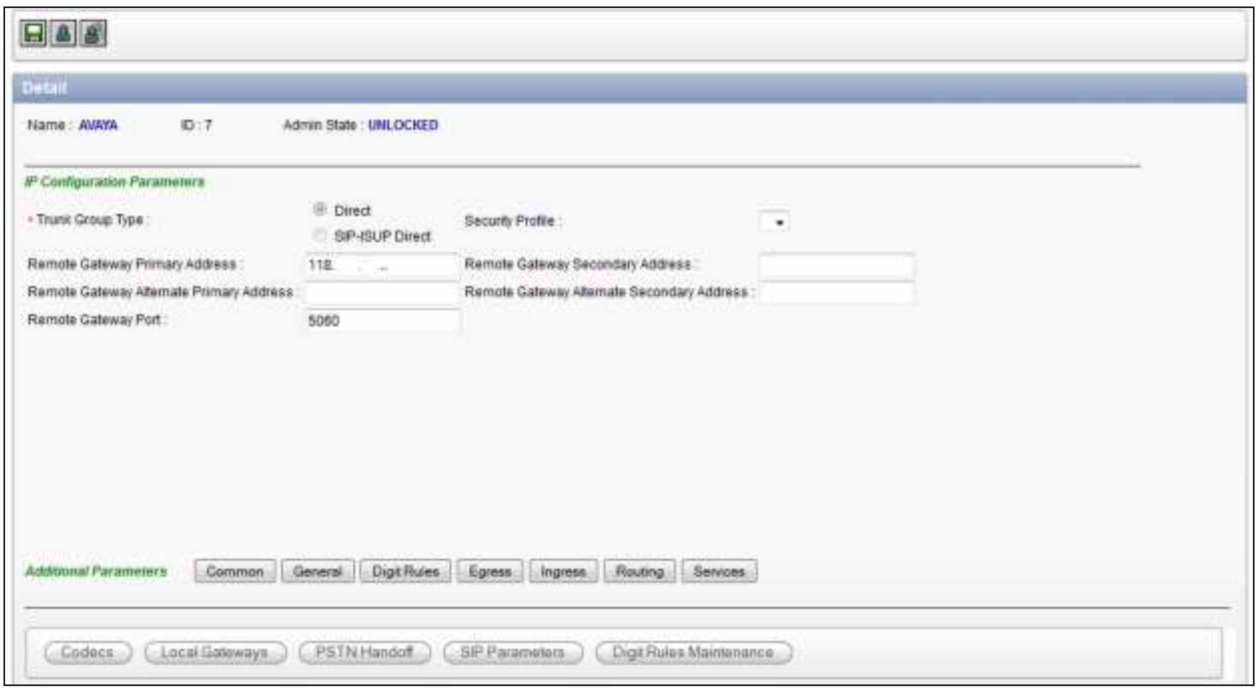


8.3. Configure SIP Trunk Group

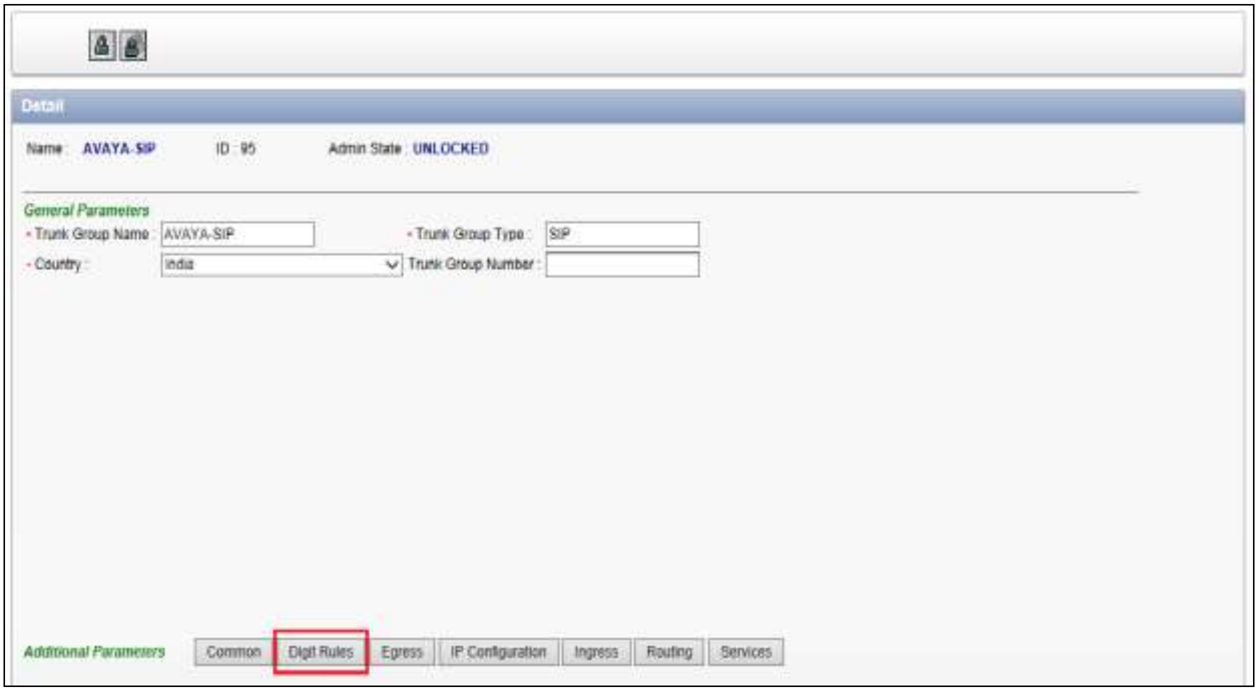
1. Click **Network Elements → Trunk Groups →New Trunk Group** icon.
2. In the **Trunk Group Detail** (not shown), complete the following fields:
   - **Trunk Group Type** -Select **SIP**
   - **Country** - location of the trunk group

   The following field is optional:
   - Trunk Group Number
3. **The IP Configuration tab** is the first tab that comes up. Enter the entries or selections for the following fields:
   - **Type -** This field is used to select the type of local gateway used by the trunk group. Select the **Direct** radio button for this field
   - **Remote Gateway Primary Address -** Use this field to enter the IP address of the primary destination for the SIP trunk group
   - **Remote Gateway Port -** Use this field to enter the Remote Gateway's port **5060**

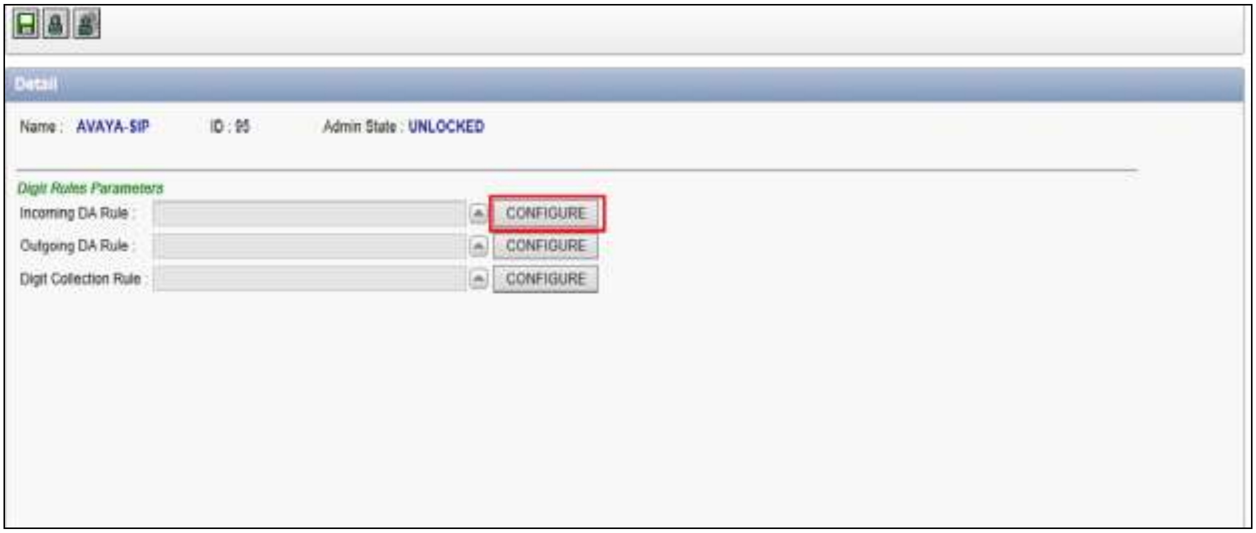
   Leave all other settings as default.



4. Select the **Digit Rules** tab under trunk group details.

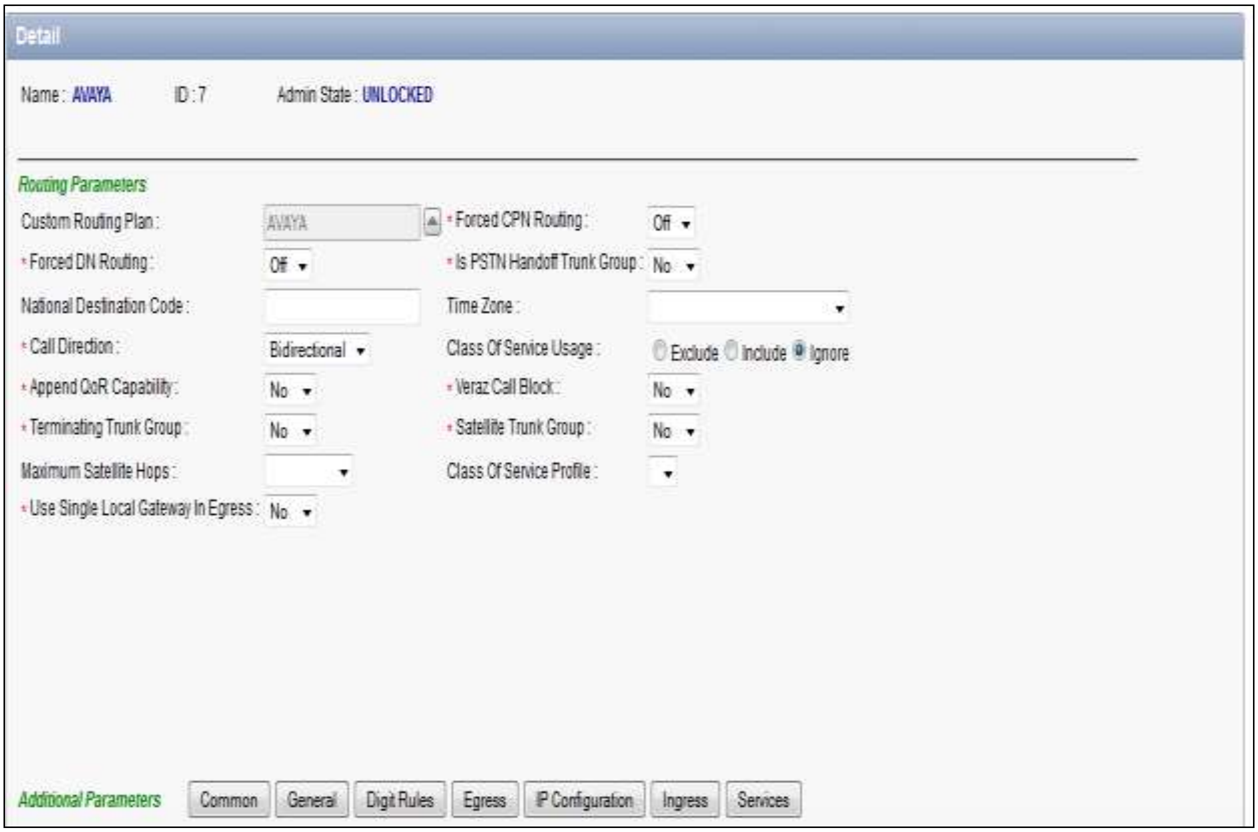


After navigating to the **Digit Rules** tab, click on the **configure** button to select the **incoming DA rule** or **outgoing DA rule** whichever is applicable. DA rules are not mandatory and can be left blank which was done here.



5. Select the **Routing** tab and complete the following fields:
   - **Custom Routing Plan –** Provide appropriate name
   - **Call Direction –** Select **Bidirectional**
   - **Class of Service Usage –** Check **Ignore** as this is not use here for testing
   - **Append QoR Capability –** Select **No**
   - **Veraz call Block –** Select **No**
   - **Terminating Trunk Group** - Select **No**
   - **Satellite Trunk Group –** Select **No**
   - **Use Single Local Gateway In Egress –** Select **No**

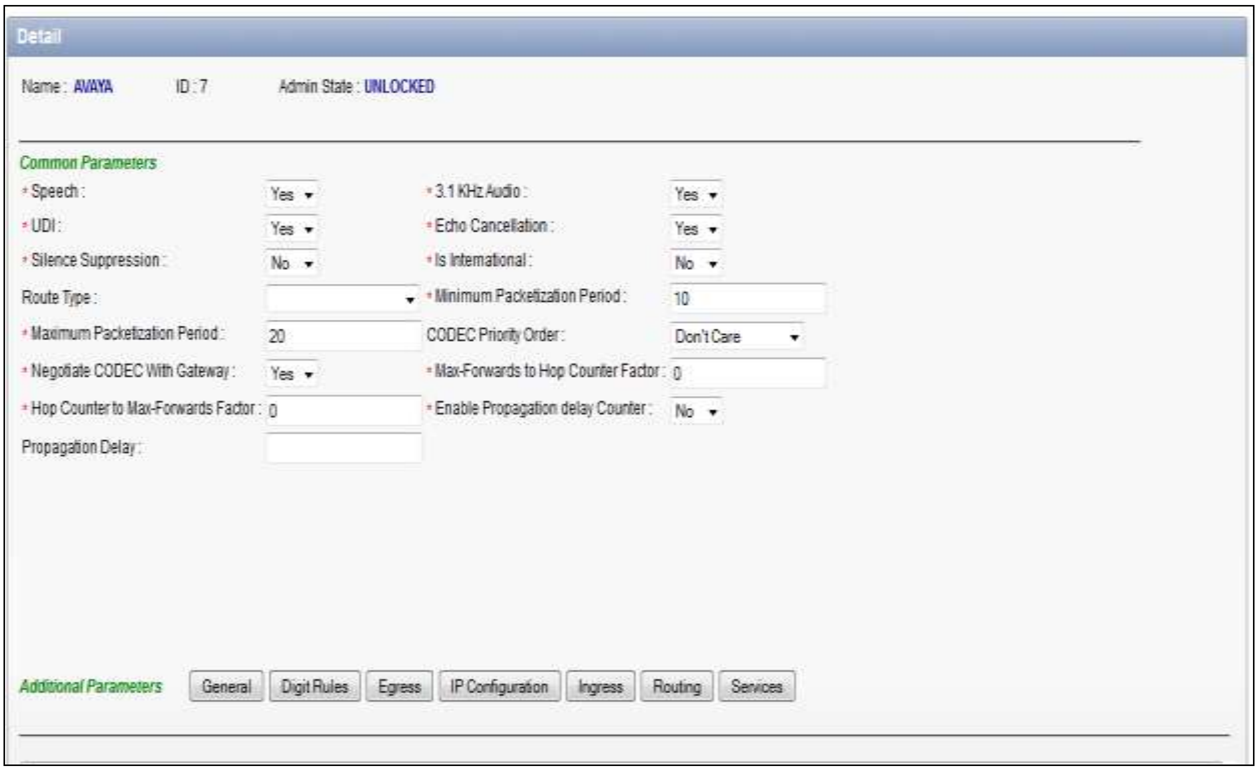
   Leave all other settings as default.



6. Select the **Common** tab and complete the following fields:

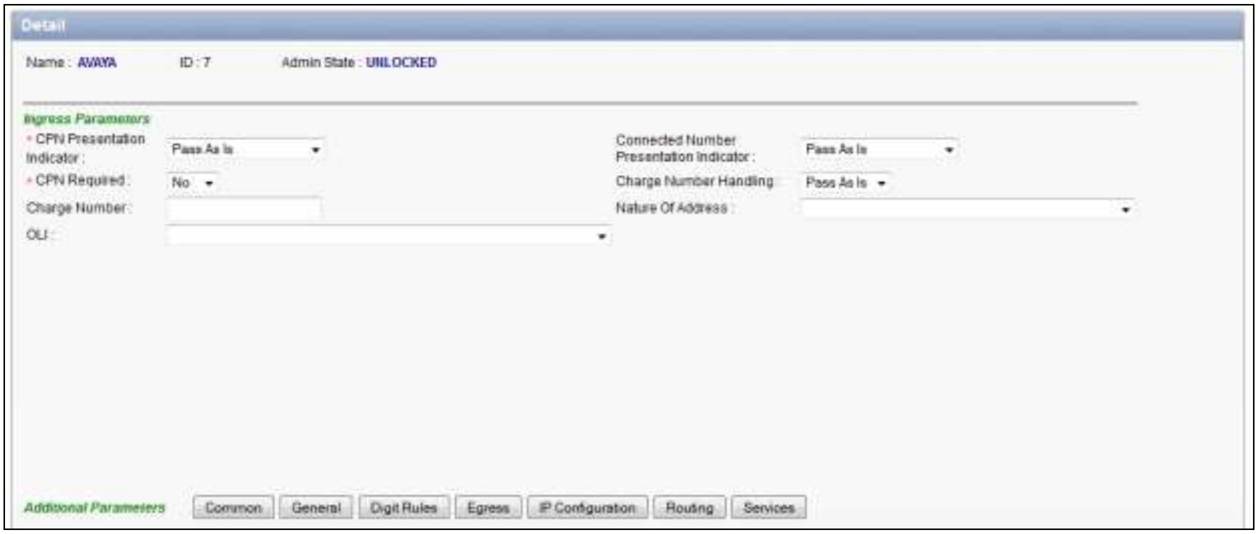
- **Speech** - This field is not applicable for SIP trunk group
- **3.1 KHz Audio** - This field is not applicable for SIP trunk group
- **UDI** – This field is not applicable for SIP trunk group
- **Echo Cancellation** - This field is not applicable for SIP trunk group
- **Silence Suppression** - This field is not applicable for SIP trunk group
- **Is International** – Select **No**
- **Minimum Packetization Period** - This field is not applicable for SIP trunk group
- **Maximum Packetization Period -** This field is not applicable for SIP trunk group
- **CODEC Priority Order** - This is the order of the Codecs between the Ingress and Egress trunk Groups
- **Negotiate CODEC with Gateway -** check this box if a list of CODECs to be sent to the Gateway involved in the call. The Gateway then selects the CODEC(s)

Leave all other settings as default.



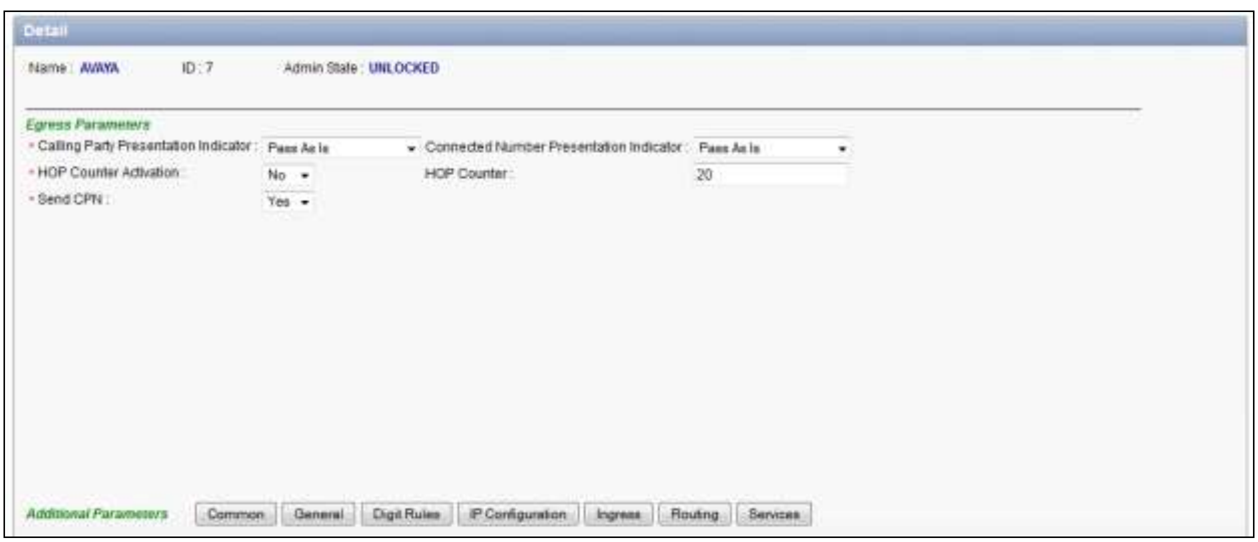
7. Select the **Ingress** tab and complete the following fields:
- **CPN Presentation Indicator –** Select **Pass As Is**
- **Connected Number Presentation Indicator –** Select **Pass As Is**
- **CPN Required –** Select **No**

Leave all other settings as default.



8. Select the **Egress** tab and complete the following fields:
- **Calling Party Presentation Indicator -** Select **Pass As Is**
- **Connected Number Presentation Indicator –** Select **Pass As Is**
- **Send CPN** - Select **Yes**. If 'Send CPN' is set to 'No' then the calling party number is not sent. This means that the CPN Presentation Indicator will also not be sent and thus becomes meaningless.

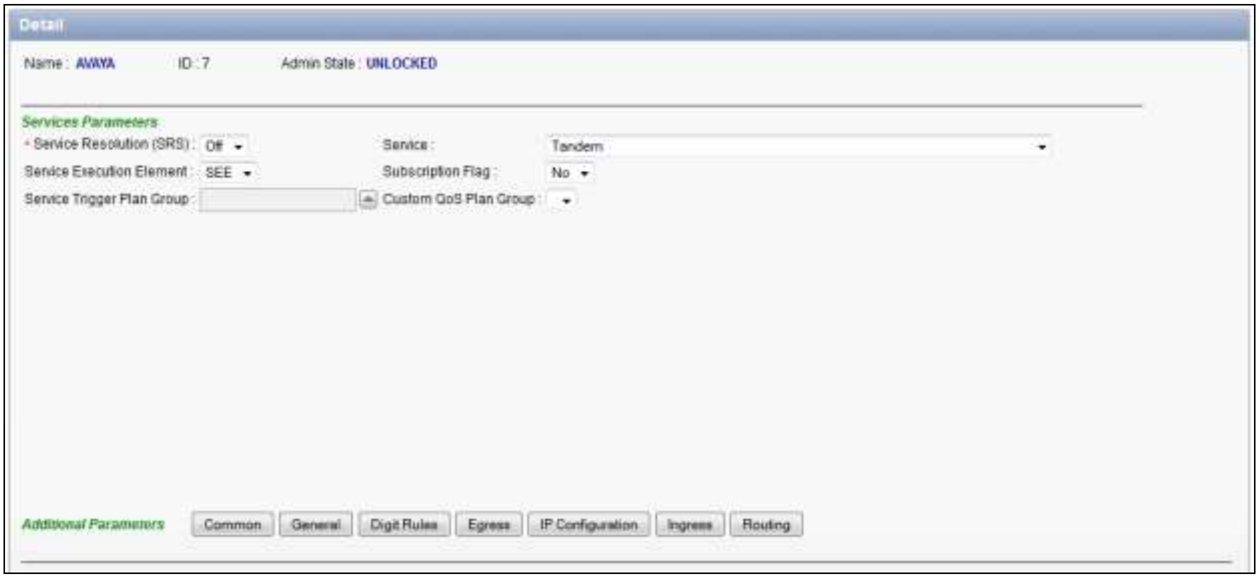
Leave all other settings as default.



9. Select the **Services** tab and complete the following fields:

- **Service Resolution (SRS) -** is always set to Off (the default) for SIP Trunk Group.
- **Service –** Select **Tandem**.
- **Service Execution Element** – Select **SEE**
- **Subscription Flag -** for this release set the flag to "**No**"

Leave all other settings as default.



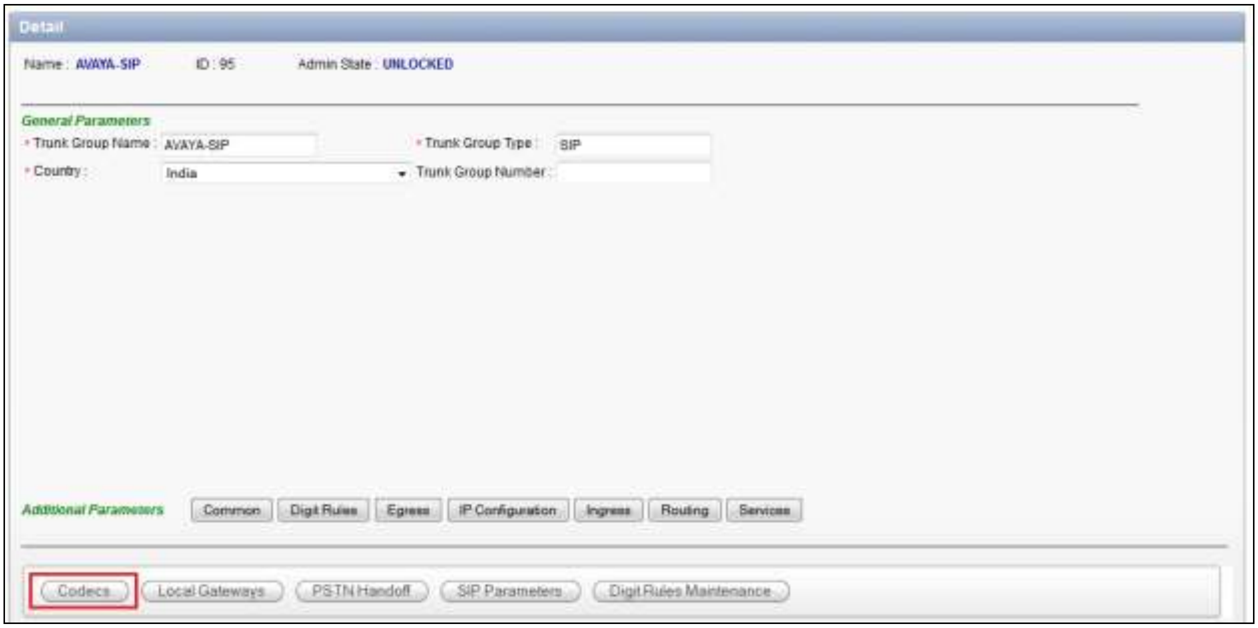
10. Click the **Save** icon to create the Trunk Group (TG) in the EMS database.

The profiles below need to be configured under TG,

- Codecs
- Local Gateways

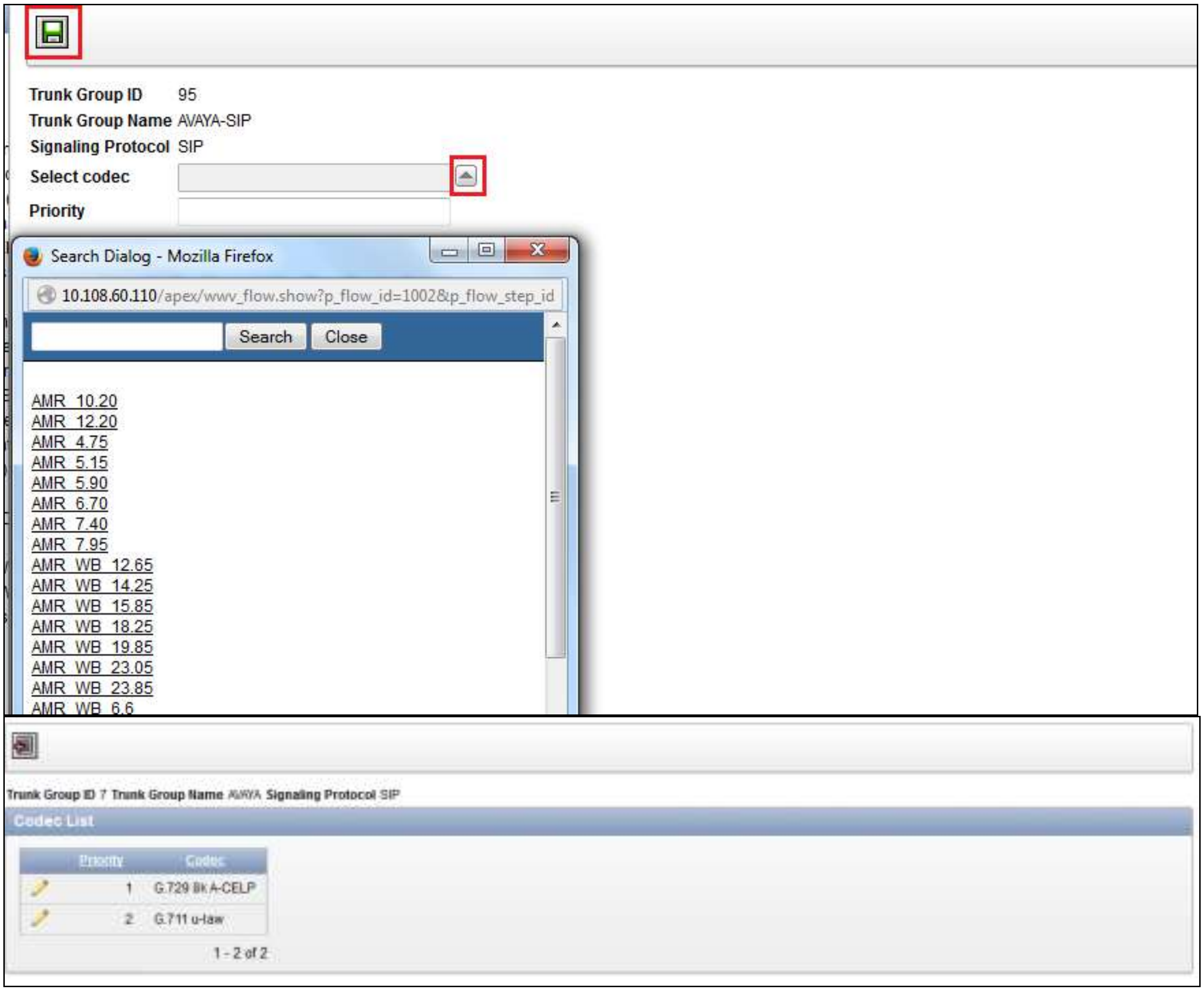
Codecs Profiles

Navigate to the **Network Elements→Trunk Groups (TG)** (not shown). Click on the **AVAYA-SIP** Trunk Group name and then click on the **Codecs** tab.



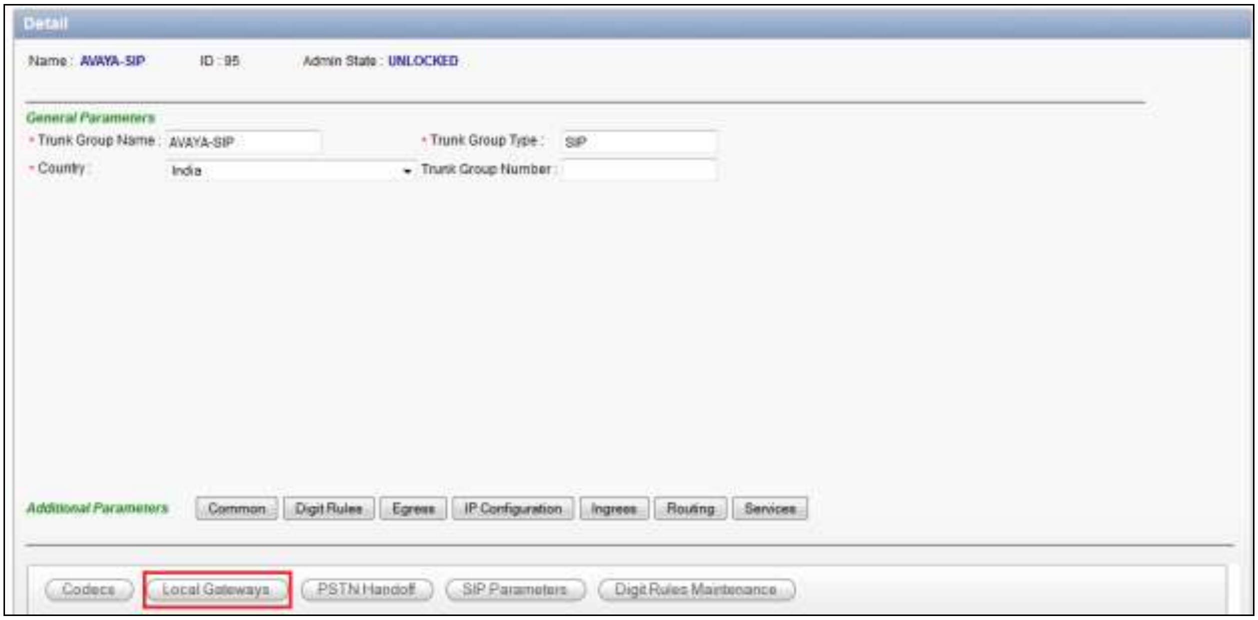
After navigating to the **Codecs** Tab, click on the **add** button.

Select the desired codec from the drop down menu, enter with priority and then save it (not shown). In this Compliance test, **G.729 8k A-CELP** and **G.711 u-law** were tested.



Local Gateways Profile

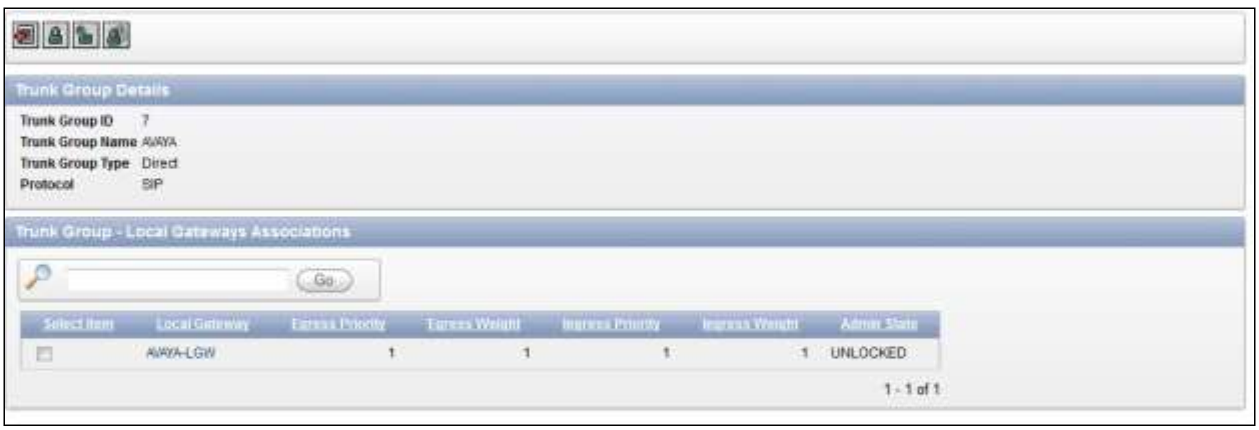
Navigate to the **Network Elements→Trunk Groups (TG)** (not shown). Click on the **AVAYA-SIP** Trunk Group name and then click on the **Local Gateways** tab.



After navigating to the **Local Gateways** tab, click on the **add** button to select the Local Gateway.

Select the desired local gateway from the drop down menu and then click on the **save** button (not shown). Leave the rest as default.

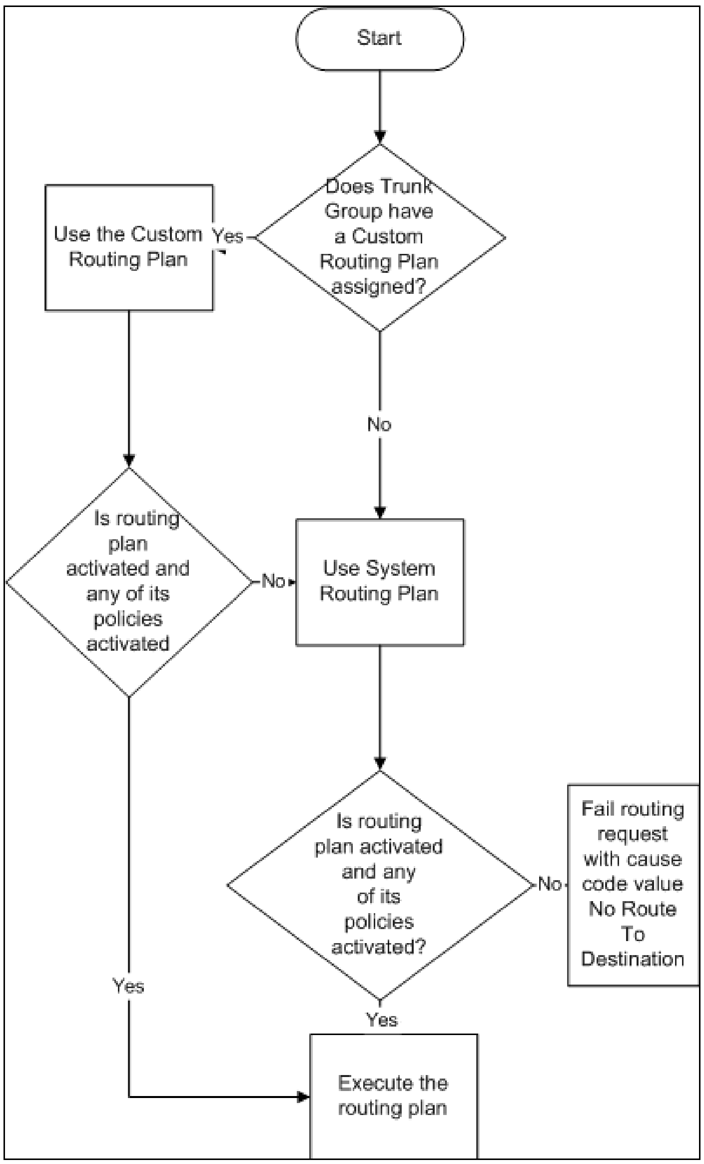
The AVAYA SIP Trunk Group details is shown below.



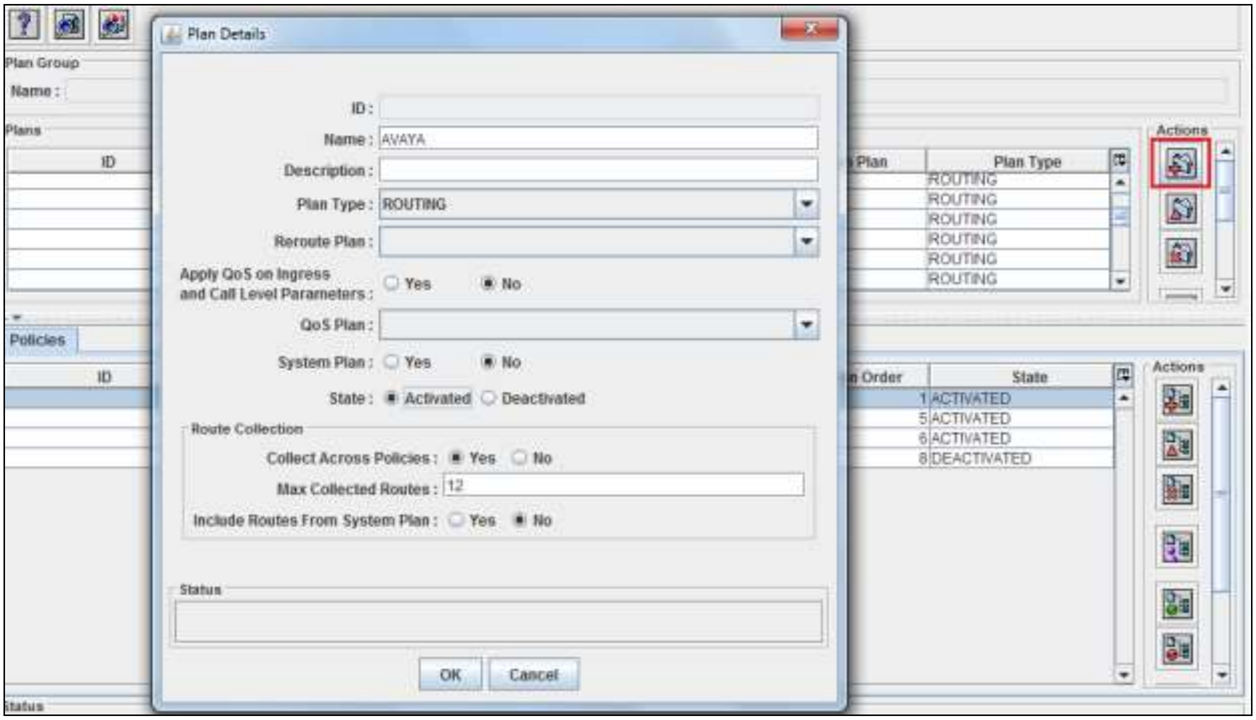
8.4. Configure Routing Configuration

A routing plan is a collection of routing policies ordered by a priority for an environment. Select for these policies, a rule or rules that are applied to calls. For each rule or set of rules, configure a treatment that describes how to treat the call that meets the conditions found in the rule(s), such as “Route” the call.

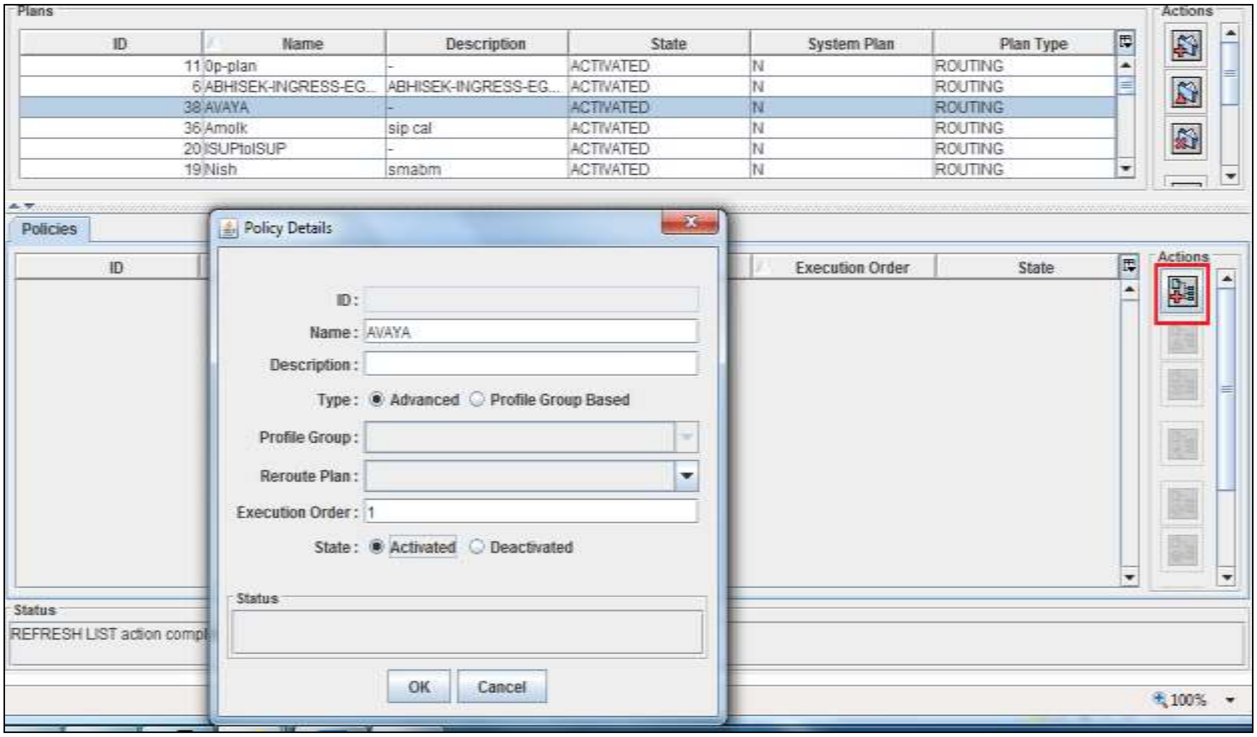
Below is the Routing Plan Call flow.



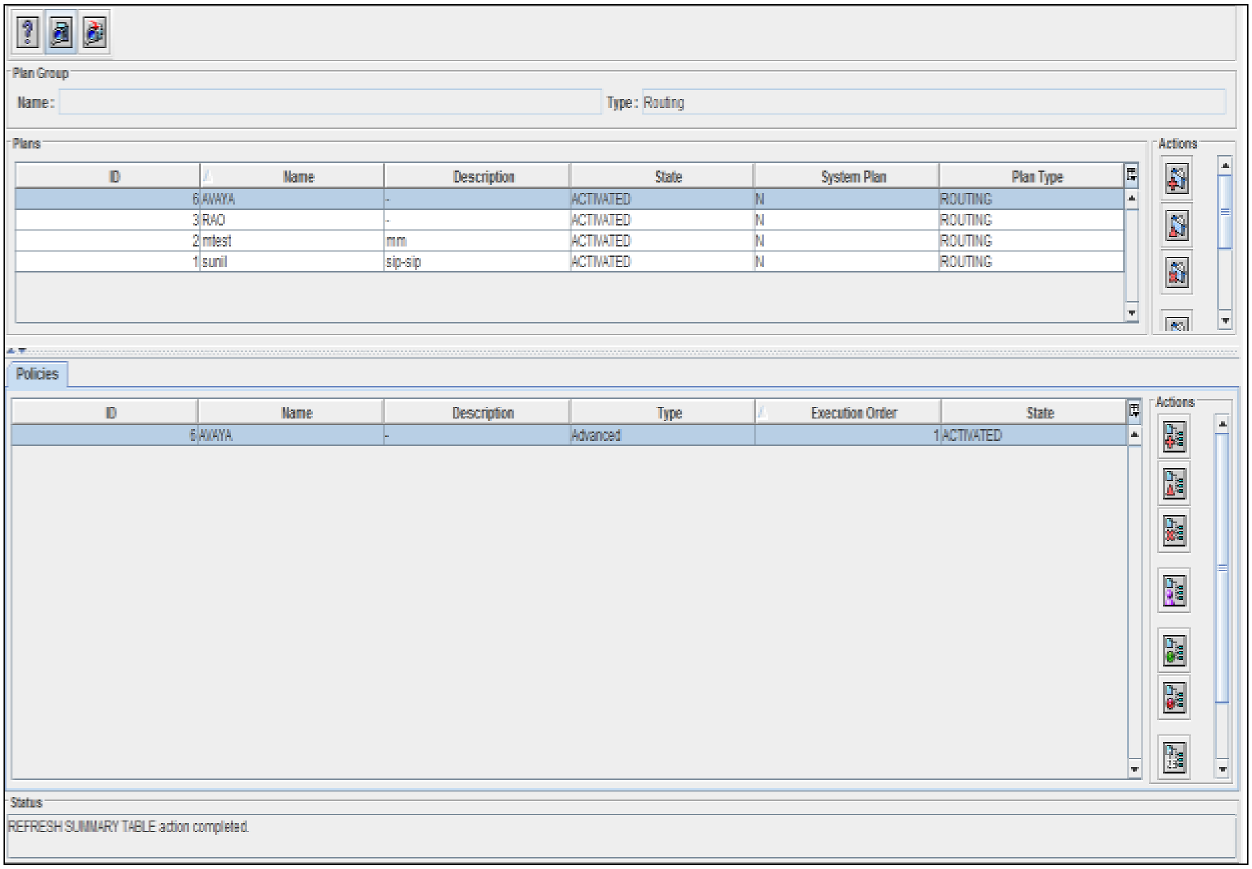
Navigate to the **Policies → Plan and Policies → Routing** (not shown). After navigating to the **Routing** screen**,** click on **Add** button on right side actions plane. Complete the Routing plan as below and activate it.



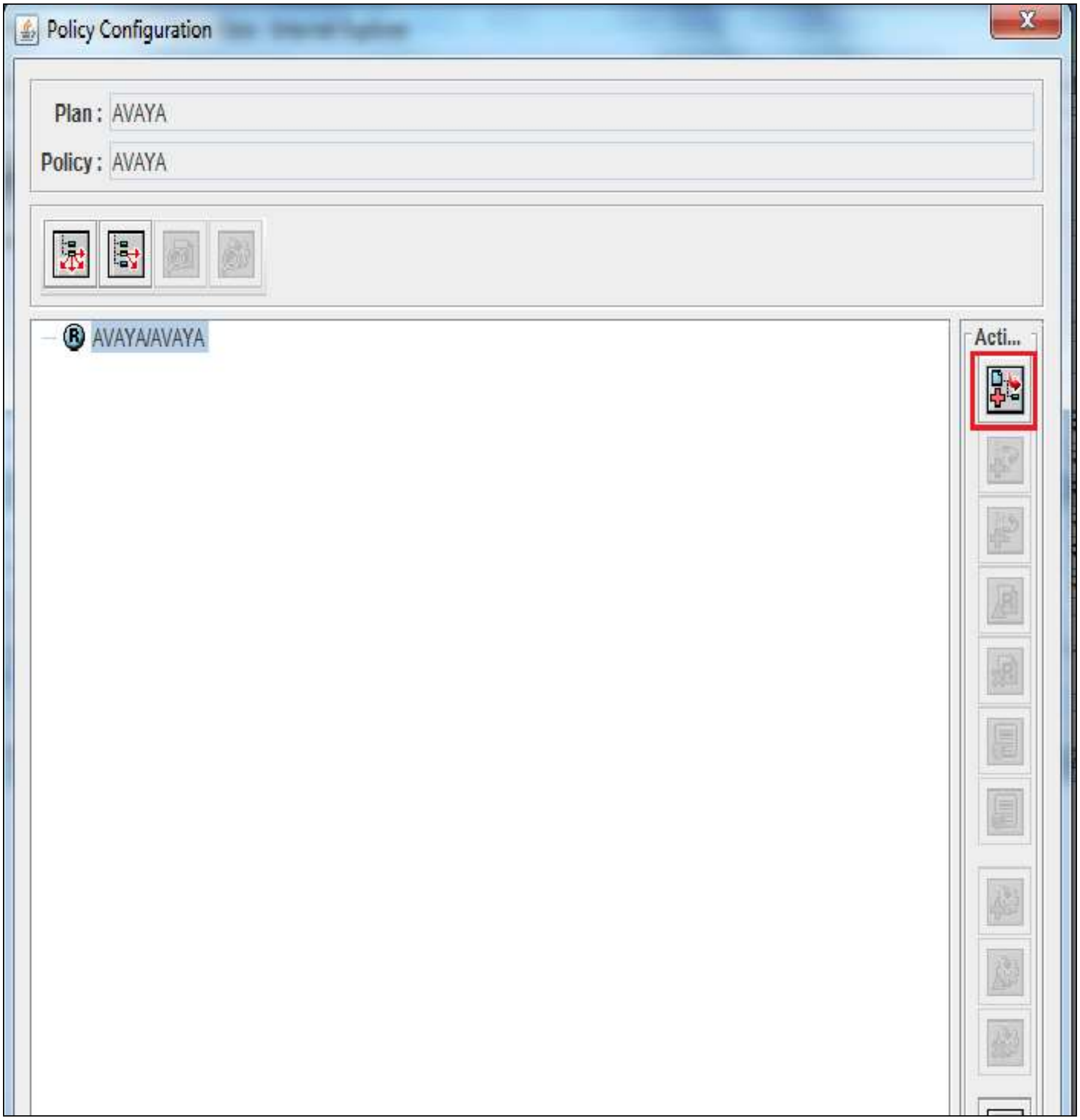
After completion of routing plan, create the policy under the plan by clicking the **Add** button under Policies **Actions plane** to create the policy. Complete the **Policy Details** as below and activate it.



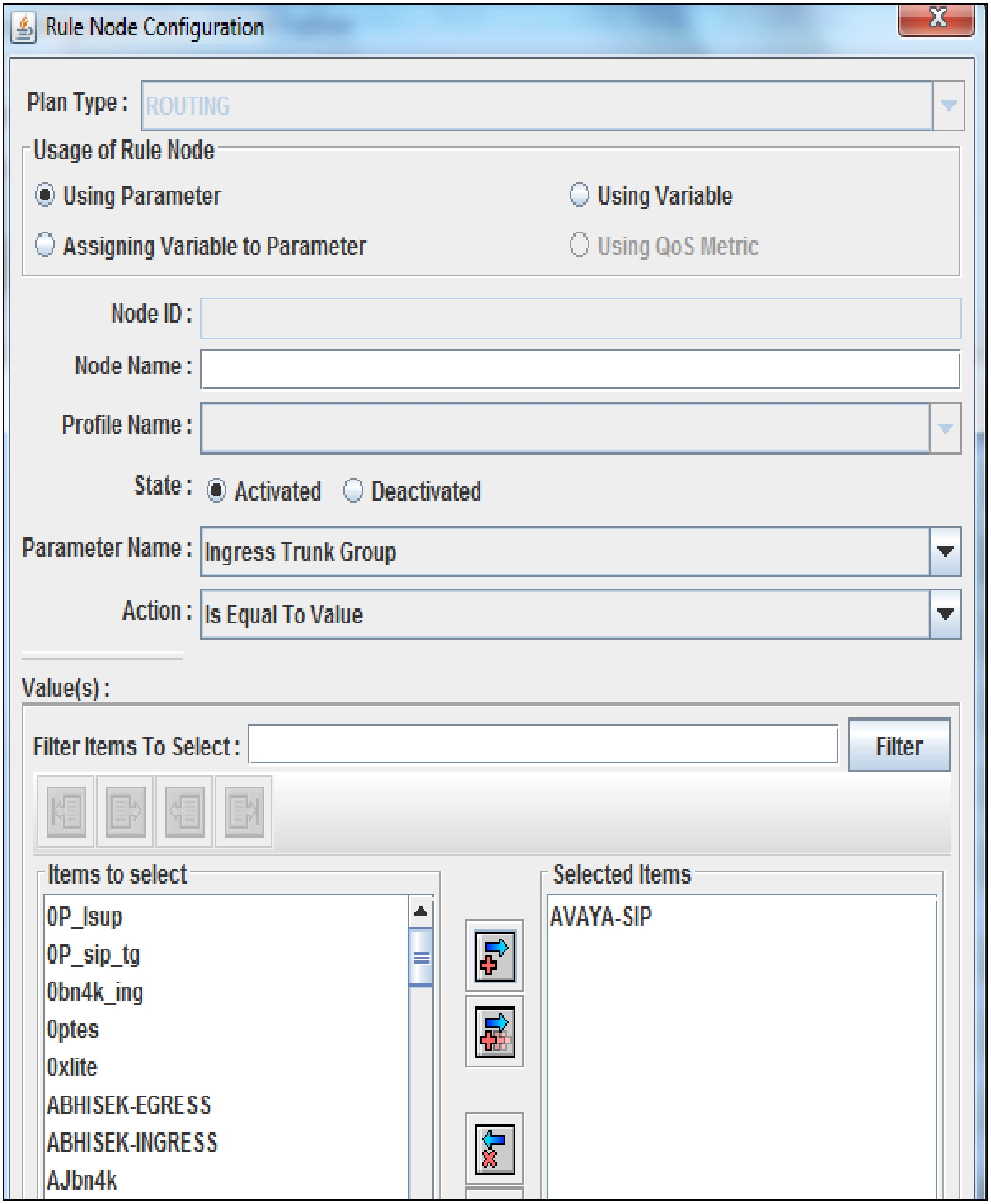
Below is the activated Routing Plan with policy screenshot.



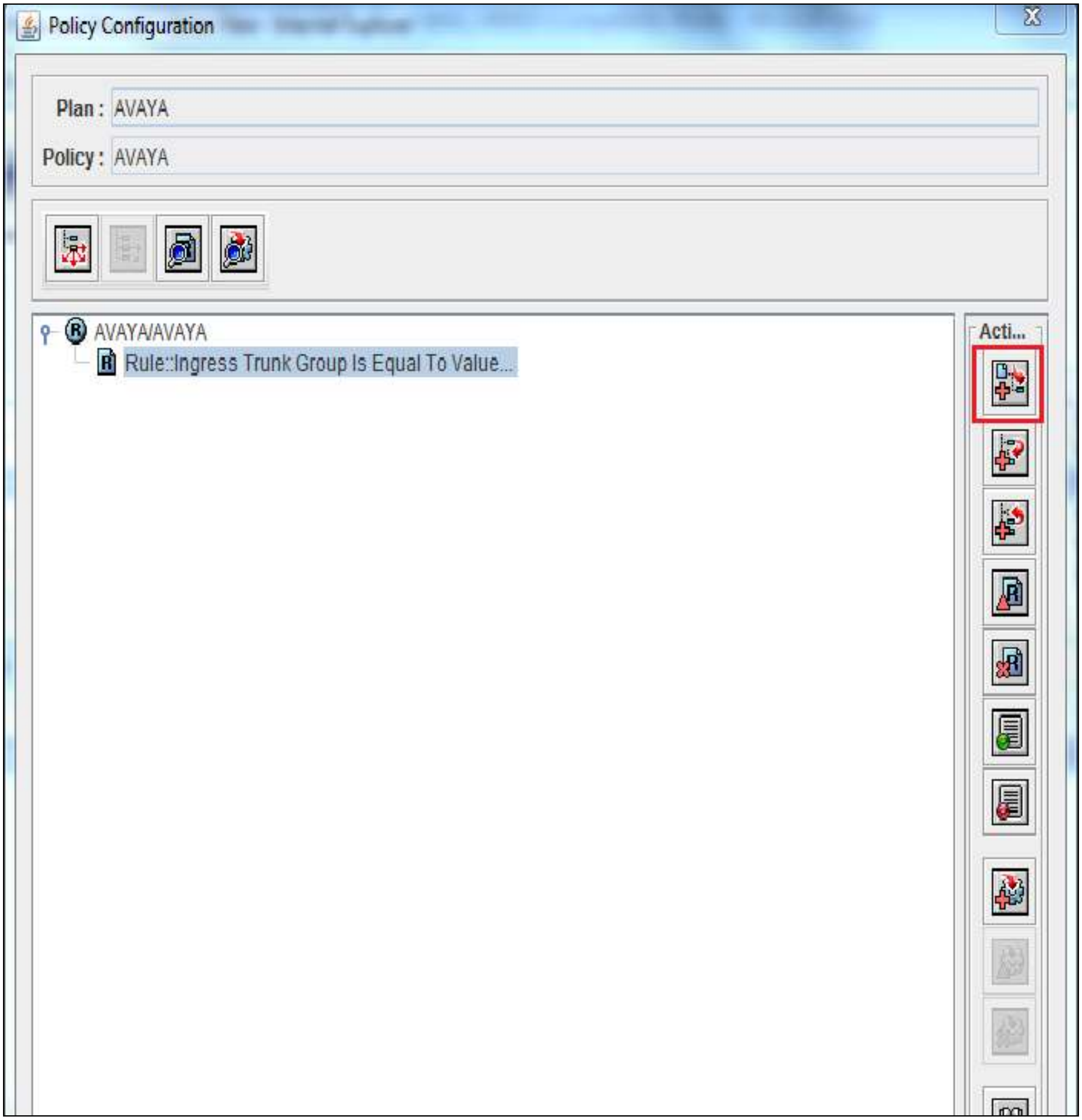
Double click on the policy, a new window will be opened where a new rule needs to be created. Click on the **Add** button on the Actions plane to create the new rule.



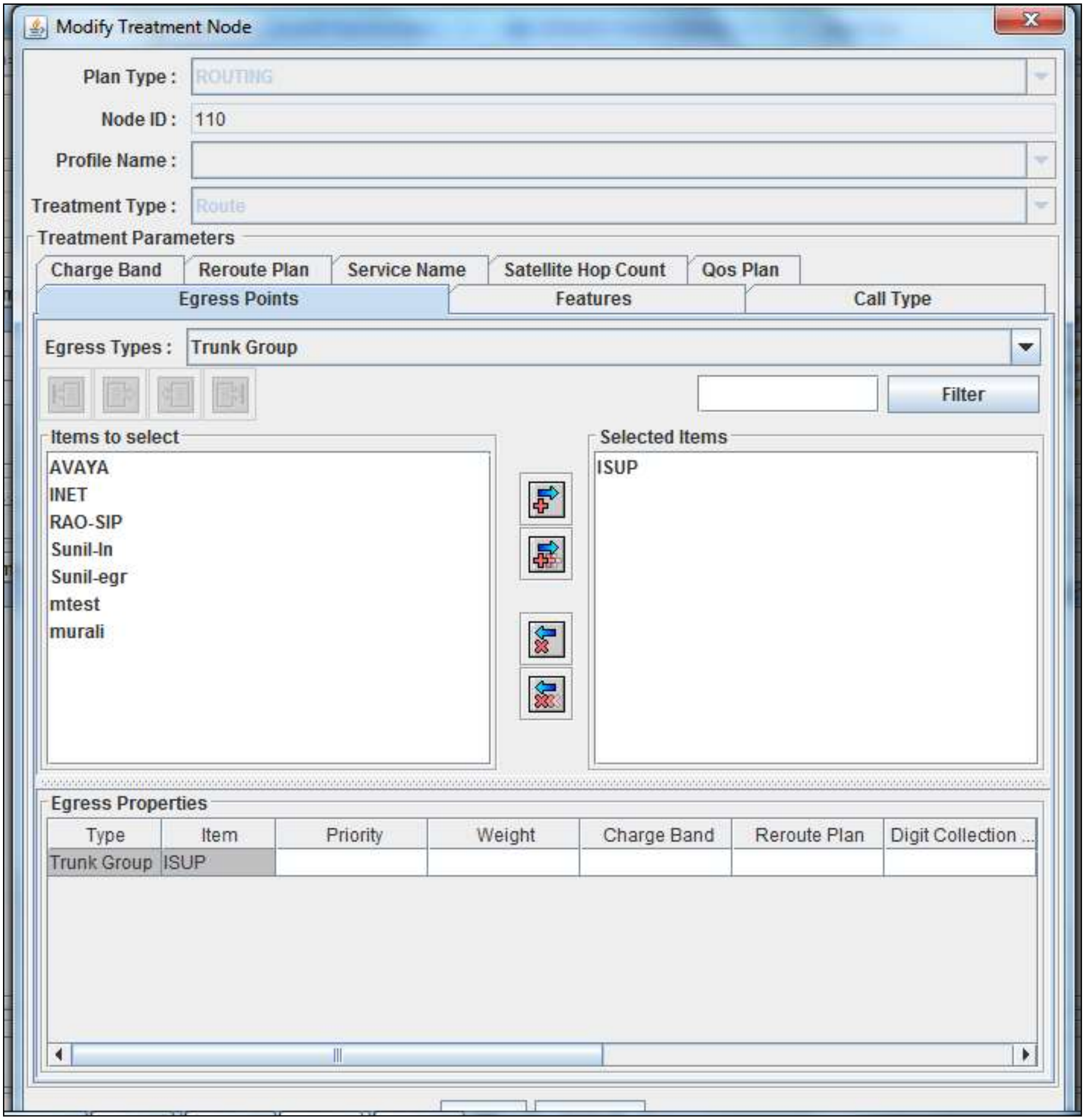
The completed rule is **Activated** as screenshot below **using parameter** for the rule.



To add treatment under the rule, click on the **Add** button on the **Actions plane** to create the treatment.



The treatment screenshot is shown below with the **Egress Types** selected as **Trunk Group ISUP**. The routing plan applied at TG level is shown in **Section 8.3** Step 5.

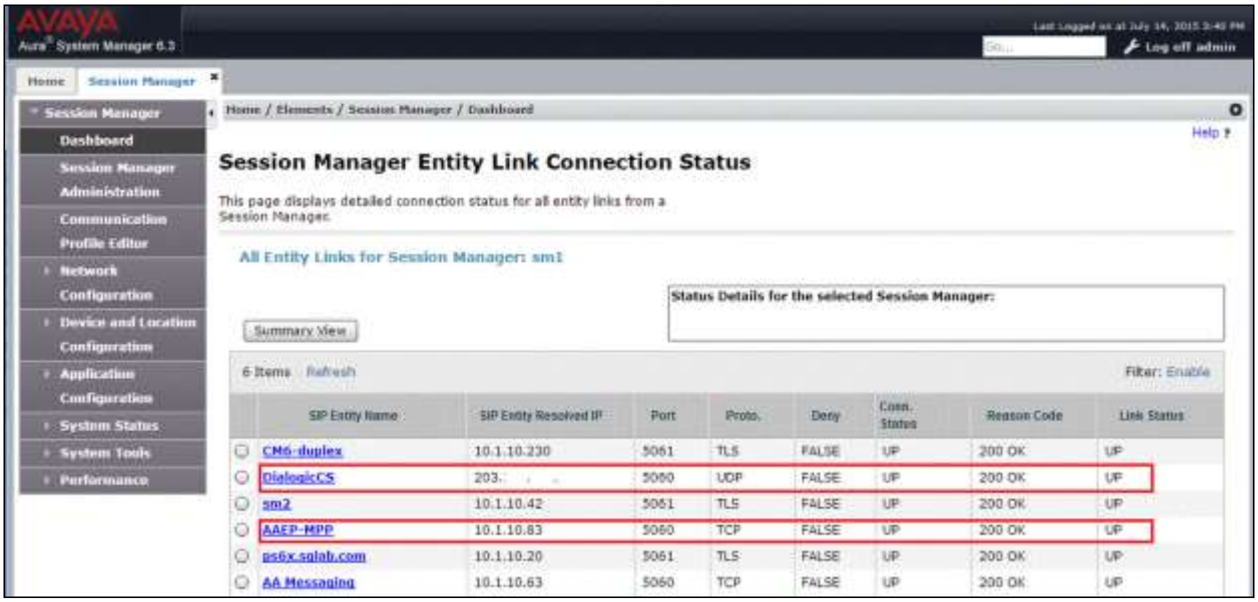


9. Verification Steps

This section provides the verification steps that may be performed to verify that Avaya Aura® enterprise network can establish outbound calls to ControlSwitch.

9.1. Verify Entity Link Status on Avaya Aura® Session Manager

To verify connectivity to ControlSwitch, click **Session Manager** on the Home page of System Manager web interface. Select **Dashboard** on the left panel and click the **Entity Monitoring** status of **sm1** (not shown) on the right panel. Below is the summary view in which both the **Conn. Status** and **Link Status** fields should display **UP** for both **SIP Entity Name, DialogicCS** and **AAEP-MPP**.

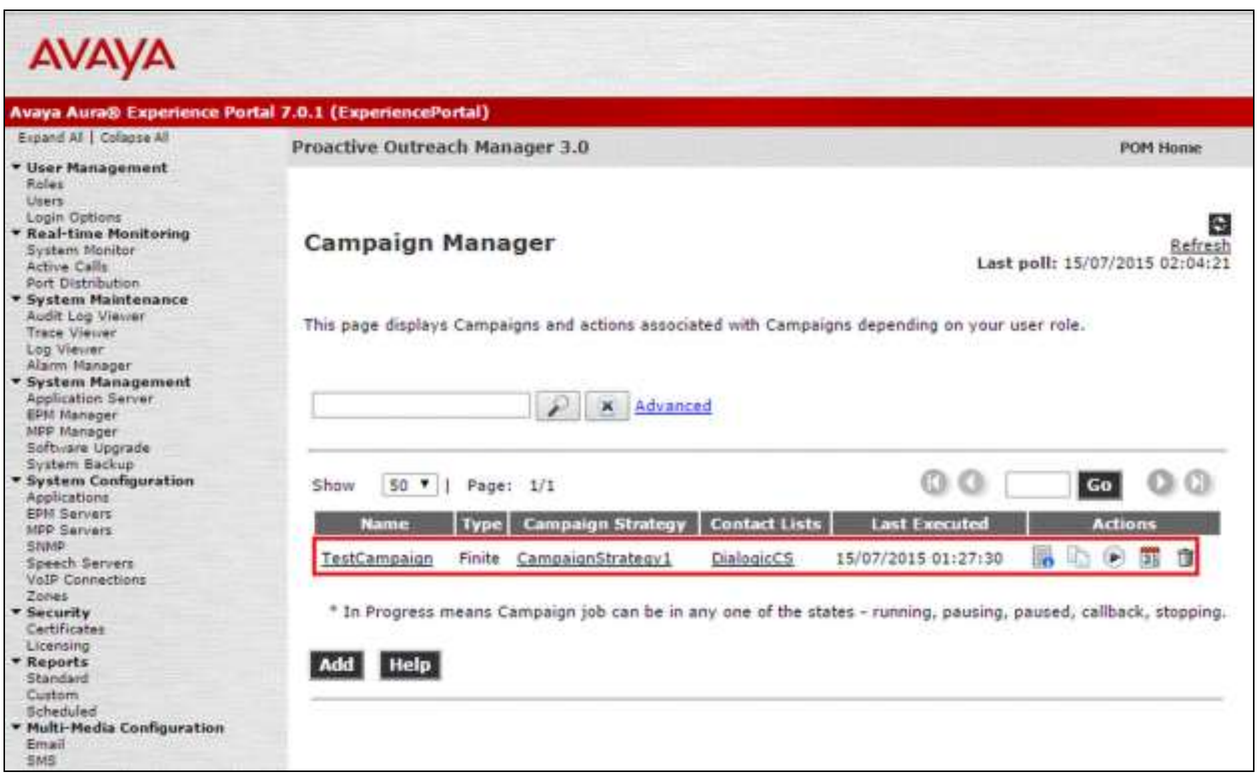


9.2. Verify Port Status on Avaya Aura® Media Processing Platform

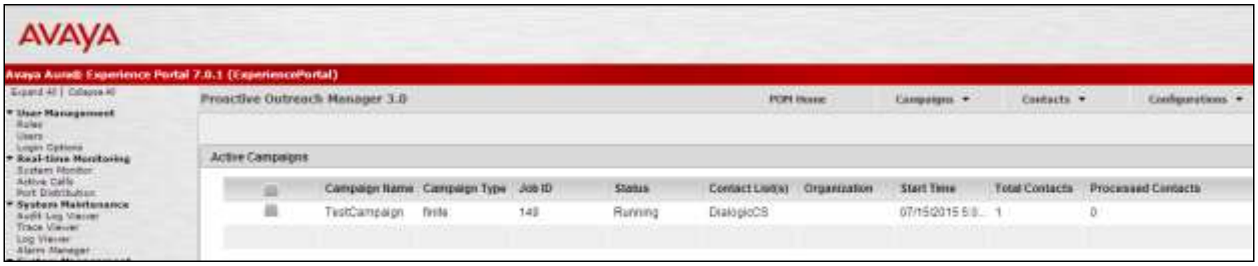
To verify the SIP Trunk status on the MPP; log in to EPM and navigate to **Real-time Monitoring → Port Distribution,** select **AAEP-MPP** (not shown). Click OK and observed under the **Mode** column for the SIP Trunk is **online**.

9.3. Outbound calls

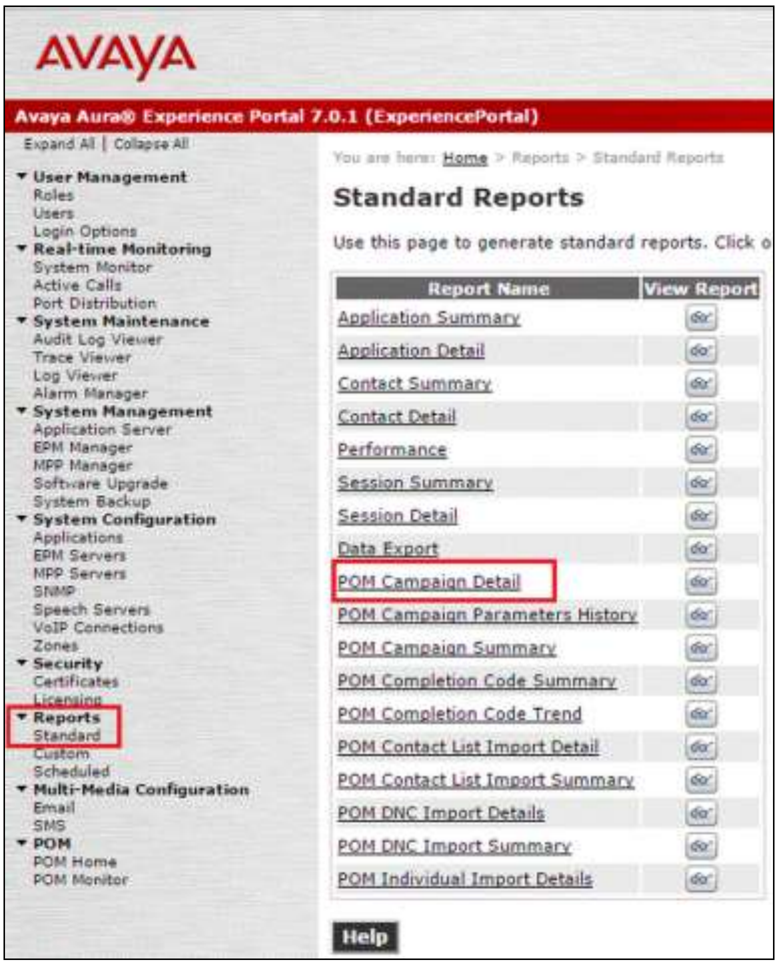
Log in to EPM portal and start a campaign by navigating **POM → POM Home → Campaigns → Campaign Manager**. Start the campaign by clicking the play button to make outbound voice to ControlSwitch. Observe that the far end is answered and announcement is heard.



Navigate to **POM → POM Monitor** to observer that the campaign is **Running** under **Status**.



Navigate to **Reports → Standard** and click **POM Campaign Detail**.



Select the appropriate **Date and Time** (not shown) to display the campaign already completed to check campaigns that are attempted and/or completed under the **Completion Code**. For the call below, it is answered and **Answer Human** is one the system completion codes. The list of completion codes can be found on the portal **Proactive Outreach Manager Help** manual.

10. Conclusion

These Application Notes describe the configuration steps required for configure Dialogic® ControlSwitch™ System to interoperate with Avaya Aura® Session Manager, Avaya Aura® Experience Portal 7.0 and Avaya Proactive Outreach Manager 3.0 using SIP trunking for Proactive Outbound calls. All feature and serviceability test cases were completed with observations noted in **Section 0**.

11. Additional References

Avaya references are available at http://support.avaya.com

[1] Administering Avaya Aura® Session Manager, Release 6.3, Issue 5, June 2014
[2] Deploying Avaya Aura® Session Manager using VMware® in the Virtualized Environment, Issue 6, Release 6.3, November 2014
[3] Administering Avaya Aura® Experience Portal, Release 7.0.1, April 2015
[4] Deploying Avaya Aura® Experience Portal in an Avaya Customer Experience Virtualized Environment, Release 7.0.1, November 2015
[5] Implementing Avaya Aura® Experience Portal on multiple servers, Release 7.0.1 Issue 1, November 2014
[6] Implementing Proactive Outreach Manager, Release 3.0.1, March 2014

Dialogic® products references are available on http://www.dialogic.com/en/products.aspx.

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.