



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

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.



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

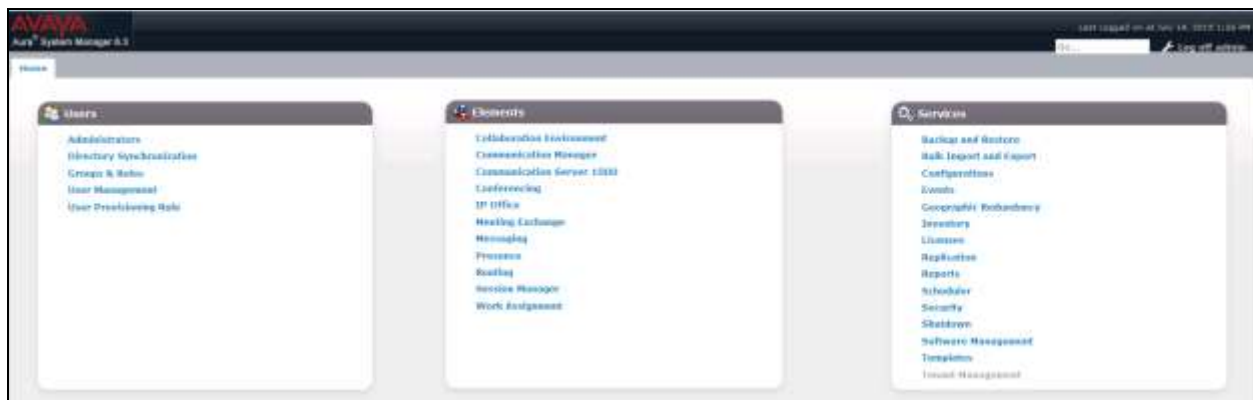
5. Configure Avaya Aura® Session Manager

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

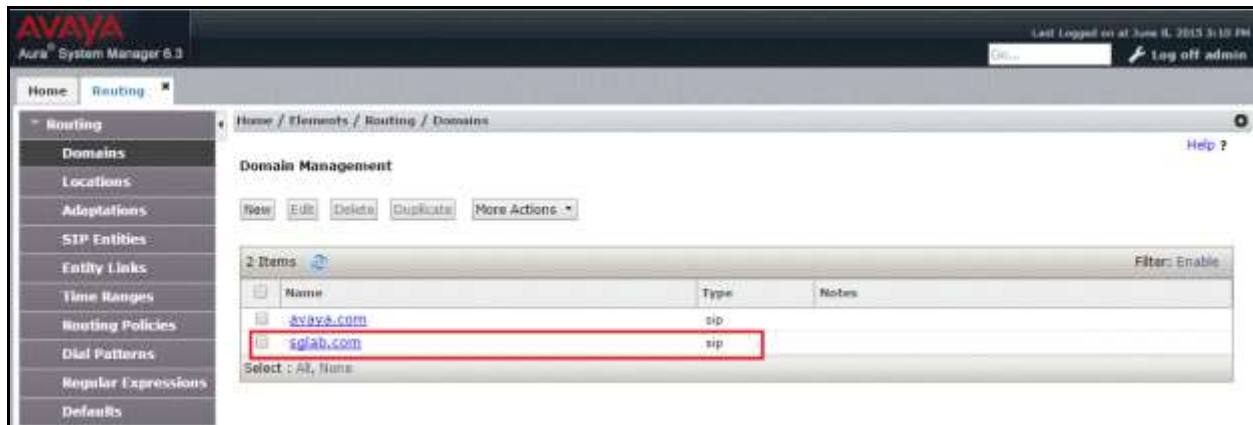
5.1. Log in to Avaya Aura® System Manager

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.

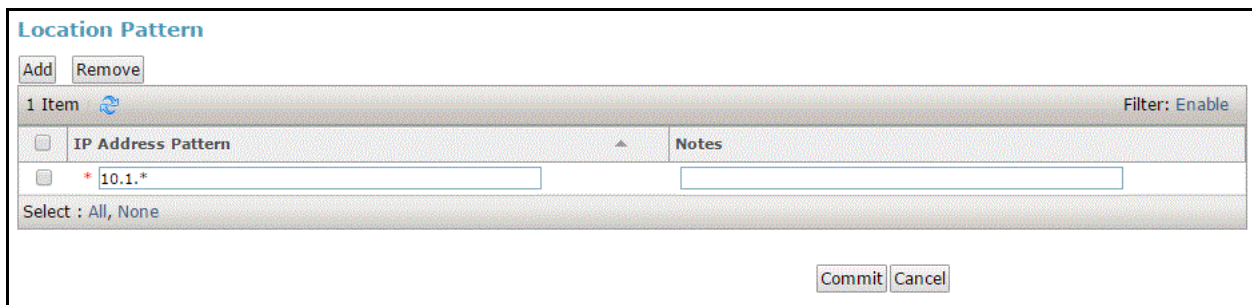


5.3. Identify the Locations

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.

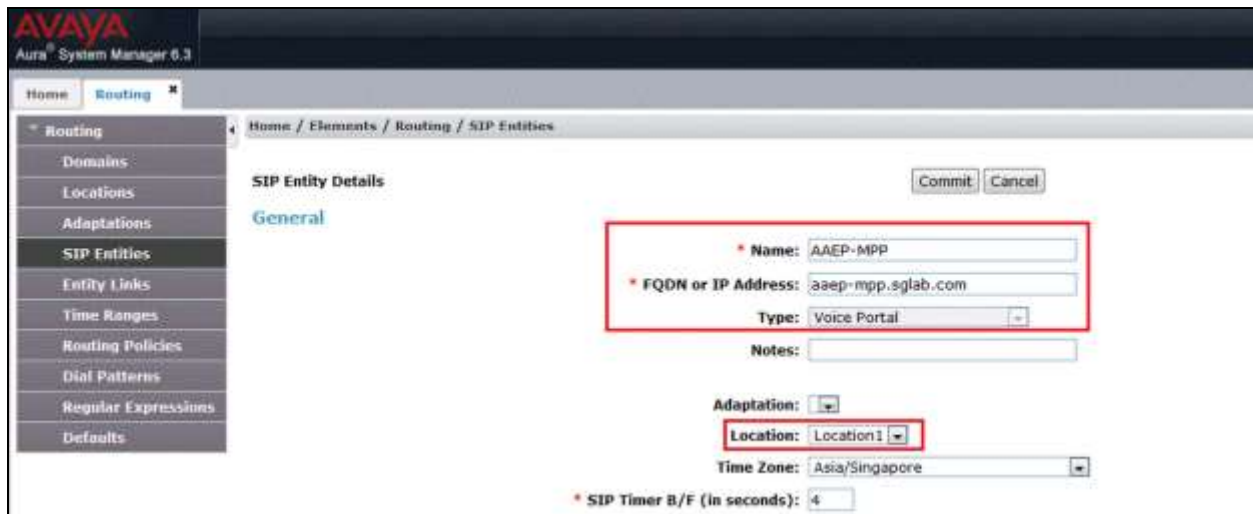
5.4.1. Session Manager SIP Signaling Interface Entity

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**.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area shows the 'SIP Entity Details' page for a new entity. The breadcrumb trail at the top reads 'Home / Elements / Routing / SIP Entities'. The 'General' tab is selected. The form includes the following fields: 'Name' (set to 'DialogicCS'), 'FQDN or IP Address' (set to '203.'), 'Type' (set to 'SIP Trunk'), 'Notes' (empty), 'Adaptation' (dropdown), 'Location' (set to 'Location1'), and 'Time Zone' (set to 'Asia/Singapore'). 'Commit' and 'Cancel' buttons are located at the top right of the form area.

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.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	SIP Description	Port	Connection Policy	Drop New Service	Notes
SIP_SIP_MPP	SIP	TCP	5060	SIP-MPP		5060	Trusted	<input type="checkbox"/>	

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**.

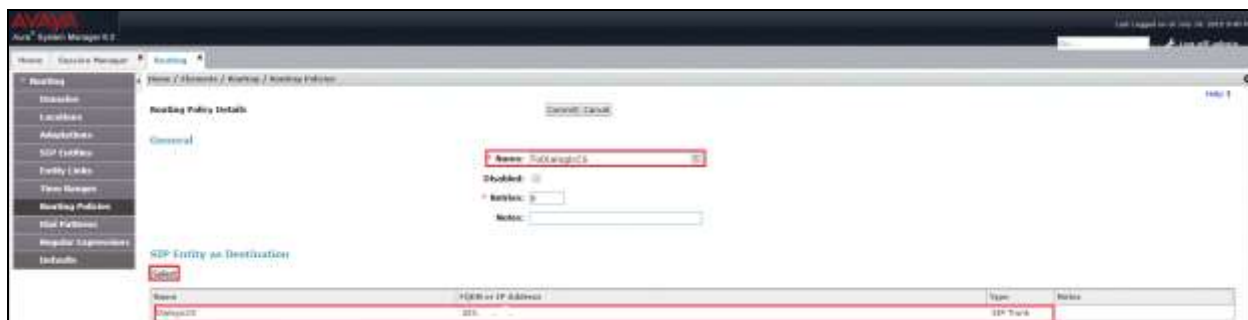
5.6.1. Create Routing Policy to Avaya Aura® Media Processing Platform

Click **Home** → **Elements** → **Routing** → **Routing Policies** → **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 Policies** → **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.

The screenshot displays the Avaya System Manager 6.2 web interface for configuring Dial Patterns. The left sidebar shows the navigation menu with 'Dial Patterns' selected. The main content area is titled 'Dial Patterns Details' and includes a 'General' tab. The 'Pattern' field is set to '2-4444', with 'Min' set to '2' and 'Max' set to '4'. The 'SIP Domain' is set to 'ALL'. The 'Originating Locations and Routing Policies' section shows a table with one entry: 'Locations' (Origination Location Name), 'TollManager' (Routing Policy Name), '0' (Cost), and 'DialogicCS' (Routing Policy Destination). The 'Add' button is highlighted in the 'Originating Locations and Routing Policies' section.

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.

The screenshot displays the Avaya Aura System Manager interface for creating a new dial pattern. The left sidebar shows the navigation menu with 'Dial Patterns' selected. The main content area is titled 'New Dial Pattern' and includes the following fields:

- Pattern:** 0010
- Min:** 3
- Max:** 3
- Emergency Call:** ☐
- Emergency Priority:** 0
- Emergency Type:**
- SIP Domain:** ALL
- Notes:** To-MPP-MPP

Below these fields is the 'Originating Locations and Routing Policies' section. It contains an 'Add' button and a table with the following data:

Origination Location Name	Origination Location Notes	Routing Policy Name	Route	Routing Policy Disabled	Routing Policy Description	Routing Policy Notes
ALL		To-MPP-MPP	0			

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.

AVAYA

Avaya Aura® Experience Portal 7.0.1 (ExperiencePortal)

Expand All | Collapse All

You are here: [Home](#) > [System Configuration](#) > [Speech Servers](#) > [Change TTS Server](#)

Change TTS Server

Use this page to change the configuration of a TTS server.

Name: Nuance

Enable: ☒ Yes ☐ No

Engine Type: Nuance

Network Address: 10.1.10.65

Base Port: 5060

Total Number of Licensed TTS Resources: 10

New Connection per Session: ☐ Yes ☒ No

Voices:

- Basque(Spain) eu-ES Arantxa F
- Catalan(Spain) ca-ES Nuria F
- Chinese(Cantonese) zh-HK Sin-Ji F
- Chinese(Simplified) zh-CN Mei-Ling F
- Chinese(Simplified) zh-CN Tian-Tian F
- Chinese(Simplified) zh-CN Ting-Ting F

MRCP

Ping Interval: 15 seconds

Response Timeout: 4 seconds

Protocol: MRCP V2

Transport Protocol: TCP

Listener Port: 5060

Save **Apply** **Cancel** **Help**

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**.

AVAYA
Avaya Aura® Experience Portal 7.0.1 (ExperiencePortal)

Expand All | Collapse All

You are here: [Home](#) > [System Configuration](#) > [VoIP Connections](#) > [Change SIP Connection](#)

Change SIP Connection

Use this page to change the configuration of a SIP connection.

- The information that you entered has been saved.

Name: SM1

Enable: ☒ Yes ☐ No

Proxy Transport: TCP ▼

☒ Proxy Servers ☐ DNS SRV Domain

Address	Port	Priority	Weight	
10.1.10.60	5060	0	0	Remove

[Additional Proxy Server](#)

Listener Port: 5060

SIP Domain: sglab.com

P-Asserted-Identity:

Maximum Redirection Attempts: 0

Consultative Transfer: ☒ INVITE with REPLACES ☐ REFER

SIP Reject Response Code: ☒ ASM (503) ☐ SES (480) ☐ Custom 503

SIP Timers

T1: 250 milliseconds

T2: 2000 milliseconds

B and F: 4000 milliseconds

Call Capacity

Maximum Simultaneous Calls: 7

☒ All Calls can be either inbound or outbound

☐ Configure number of inbound and outbound calls allowed

Save **Apply** **Cancel** **Help**

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**.

AVAYA

Avaya Aura® Experience Portal 7.0.1 (ExperiencePortal)

Expand All | Collapse All

User Management
Roles
Users
Login Options

Real-time Monitoring
System Monitor
Active Calls
Port Distribution

System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

System Management
Application Server
EPM Manager
MPP Manager
Software Upgrade
System Backup

System Configuration
Applications
EPM Servers
MPP Servers
SNMP
Speech Servers
VoIP Connections
Zones

Security
Certificates
Licensing

Reports
Standard
Custom
Scheduled

Multi-Media Configuration
Email
SMS

POM
POM Home
POM Monitor

You are here: [Home](#) > [System Configuration](#) > [MPP Servers](#) > [VoIP Settings](#)

VoIP Settings

Voice over Internet Protocol (VoIP) is the process of sending voice data through a network. If you make any changes to this page, you must restart all MPPs.

Port Ranges

	Low	High
UDP:	30000	30999
TCP:	31000	33499
MRCP:	34000	36499
H.323 Station:	37000	39499

RTCP Monitor Settings

Host Address:

Port:

VoIP Audio Formats

MPP Native Format: **audio/basic**

Audio Codecs

Packet Time: **20** milliseconds

G729: ☐ Yes ☒ No

Reduced Complexity Encoder: ☒ Yes ☐ No

Discontinuous Transmission: ☒ Yes ☐ No

First Offered: **G729**

QoS Parameters

Out of Service Threshold (% of VoIP Resources)

Call Progress

Miscellaneous

Inband DTMF Detection Enabled: ☒ Yes ☐ No

Pre-Energy Record Time: **0** milliseconds

H323 Force Registration: **Never**

Save **Apply** **Cancel** **Help**

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.

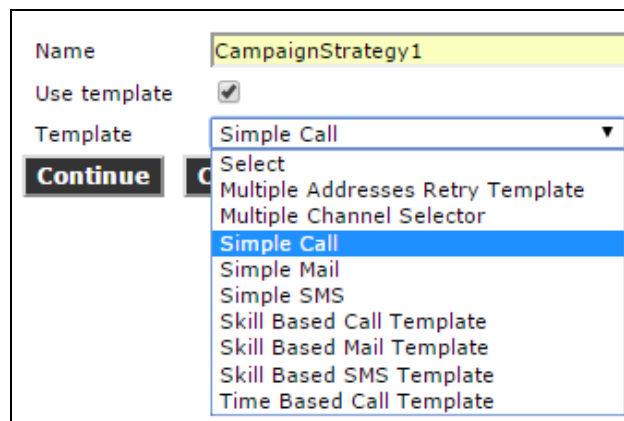
[illegible]

7.2. Create Campaigns

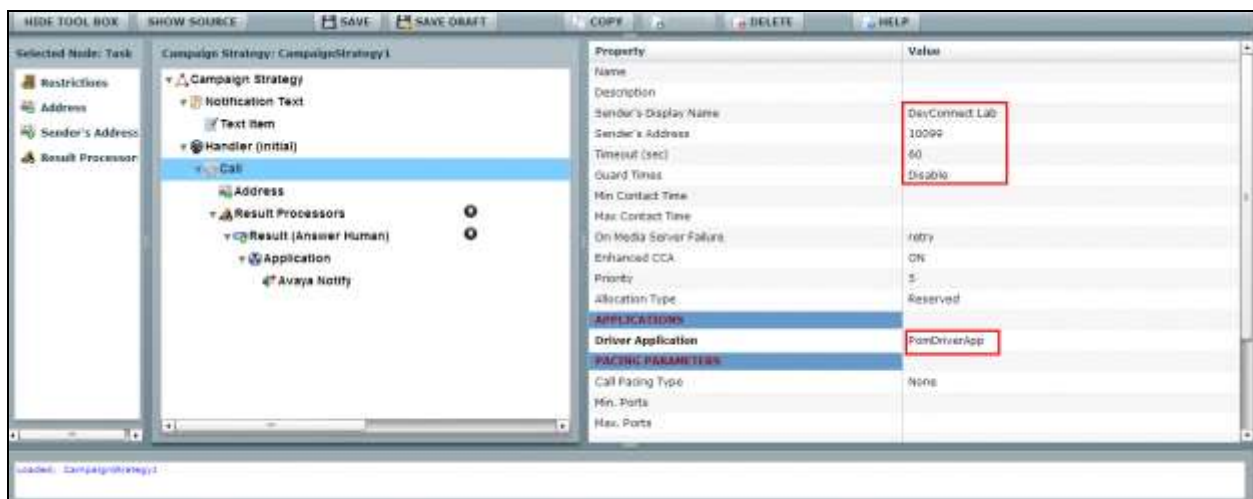
Campaign was created and run manually for testing outbound voice calls. To do that, campaign strategies using a simple call template and contact list were created.

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.



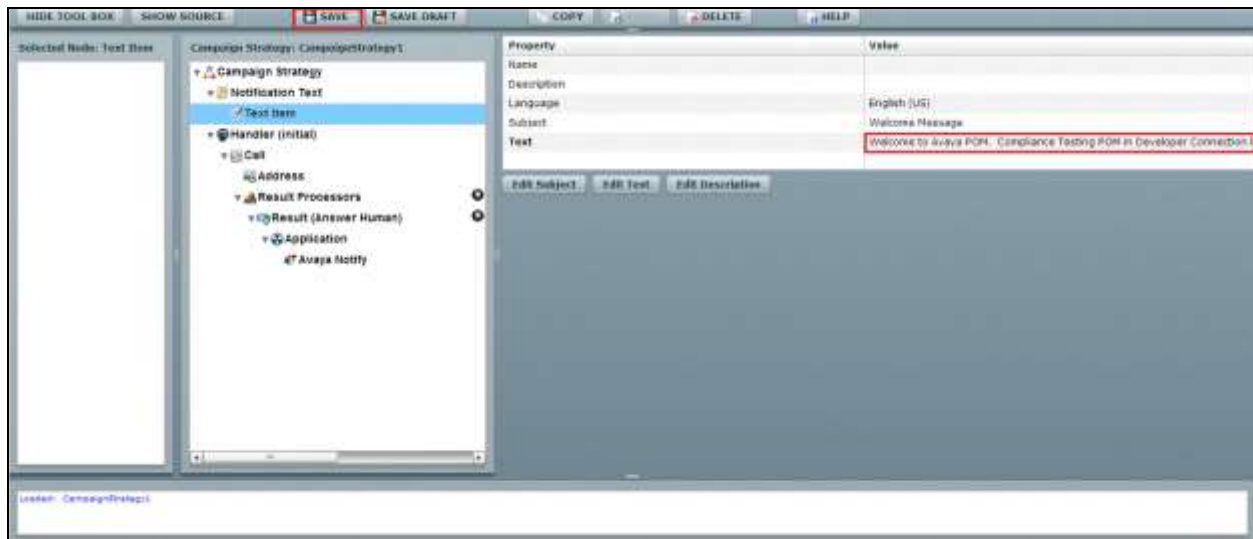
Property	Value
Name	CampaignStrategy1
Description	
Sender's Display Name	DevConnect Lab
Sender's Address	10099
Timeout (sec)	60
Guard Times	Disable
Min Contact Time	
Max Contact Time	
On Media Server Failure	retry
Enhanced CCA	ON
Priority	5
Allocation Type	Reserved
APPLICATIONS	
Driver Application	PomDriverApp
POC/HC PARAMETERS	
Call Fading Type	None
Min. Ports	
Max. Ports	

```

Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:1409322070@sglab.com;user=phone SIP/2.0
Message Header
From: "DevConnect Lab" <sip:10099@sglab.com;user=phone>;tag=da19ab8c6e24e51f713001a53a
To: <sip:1409322070@sglab.com;user=phone>
Call-ID: f819ab8c6e24e51f813001a53a
CSeq: 1 INVITE
Max-Forwards: 70

```

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 announcement. Click **Notification Text** → **Text** on the **Property** column on far right panel and enter the desired TTS announcement 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**.

Add New Contact List

This page allows you to add new Contact List.

Name

Description

Save **Cancel** **Help**

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.

AVAYA

Avaya Aura® Experience Portal 7.0.1 (ExperiencePortal)

Expand All | Collapse All

- User Management
 - Roles
 - Users
 - Login Options
- Real-time Monitoring
 - System Monitor
 - Active Calls
 - Port Distribution
- System Maintenance
 - Audit Log Viewer
 - Trace Viewer
 - Log Viewer
 - Alarm Manager
- System Management
 - Application Server
 - SRM Manager
 - MPP Manager
 - Software Upgrade
 - System Backup
- System Configuration
 - Applications
 - SRM Servers
 - MPP Servers
 - SRMP
 - Speech Servers
 - VoIP Connections
 - Zones

Proactive Outreach Manager 3.0

POM Home Campaigns

Contact Browser

This page shows Contacts present in Contact List DialogicCS.

Contact search and sort criteria:

Search Contact where Attribute

Sort Contact using Attribute in order **Apply Criteria**

Records Per Page: Page Number: 1
Total Pages: 1

System Contact ID	ID	First Name	Last Name	Phone 1	Phone 1 Country Code	Time Zone	E-Mail	Language	Action
11	5	Dialogic	CSCM	1409322070	65	Singapore	user1@sglab.net	en-us	

Back **Add** **Help**

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.







The screenshot shows the 'LGW Details' configuration window. The fields are as follows:

- ID: 5005
- Admin State: UNLOCKED
- OP State: ENABLED
- Name: AVAYA-LGW
- Protocol: SIP
- Type: Direct
- ICE Name: ICE
- Primary ICE:
 - Primary IP Address: 203.111.111.111
 - OR Manually Enter IP Address: (empty)
 - Secondary IP Address: (empty)
 - OR Manually Enter IP Address: (empty)
- Secondary ICE:
 - Primary IP Address: (empty)
 - OR Manually Enter IP Address: (empty)
 - Secondary IP Address: (empty)
 - OR Manually Enter IP Address: (empty)
- Signaling Port: 5060
- System Cause Location: User




Buttons: OK, Cancel

Below is the Local Gateways Summary screenshot.

Local Gateways Summary

Name	ID	Protocol	Type	ICE Platform	ICE Name	IP Address	OP State	Admin State	Actions
AWAY-LGW	5003 SIP	Direct	CSP1	ICE	203	10.108.60.117	ENABLED	UNLOCKED	
LGW-2	5002 SIP	Direct	CSP1	ICE	10.108.60.117	ENABLED	UNLOCKED		
LGW-3	5003 SIP	Direct	CSP1	ICE	10.108.60.117	ENABLED	UNLOCKED		
LGW117	5001 SIP	Direct	CSP1	ICE	10.108.60.117	ENABLED	UNLOCKED	  	

Associated Timers

Timer	Description	Unit	Value	Actions
intCTMF	Internal CTMF timer in digit collection timeout scenario	SEC	4	
intT1	Internal release request timer from SIP gateway	SEC	80	
intT7	Internal setup timer for incoming SIP call	SEC	1500	

Status

REFRESH SUMMARY TABLE action completed.

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 groupThe 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.

The screenshot shows the 'Detail' page for a SIP Trunk Group named 'AVAYA' with ID 7 and Admin State 'UNLOCKED'. The 'IP Configuration Parameters' section is active, showing the 'Trunk Group Type' set to 'Direct' (selected) and 'SIP-ISUP Direct' (unselected). The 'Security Profile' is set to a default value. The 'Remote Gateway Primary Address' is set to '11E...'. The 'Remote Gateway Port' is set to '5060'. The 'Remote Gateway Secondary Address' and 'Remote Gateway Alternate Primary Address' fields are empty. The 'Remote Gateway Alternate Secondary Address' field is also empty. At the bottom, there are tabs for 'Additional Parameters' (Common, General, Digit Rules, Egress, Ingress, Routing, Services) and a row of buttons for 'Codecs', 'Local Gateways', 'PSTN Handoff', 'SIP Parameters', and 'Digit Rules Maintenance'.

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

The screenshot shows the 'Detail' page for a trunk group named 'AVAYA-SIP' with ID '95' and Admin State 'UNLOCKED'. Under the 'General Parameters' section, the 'Trunk Group Name' is 'AVAYA-SIP', 'Trunk Group Type' is 'SIP', 'Country' is 'India', and 'Trunk Group Number' is empty. At the bottom, a row of tabs includes 'Common', 'Digit Rules' (highlighted with a red box), 'Egress', 'IP Configuration', 'Ingress', 'Routing', and 'Services'.

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.

The screenshot shows the 'Detail' page for the same trunk group, now with the 'Digit Rules' tab selected. The 'Digit Rules Parameters' section contains three rows: 'Incoming DA Rule', 'Outgoing DA Rule', and 'Digit Collection Rule'. Each row has a text input field and a 'CONFIGURE' button (the first 'CONFIGURE' button is highlighted with a red box).

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.

The screenshot displays the 'Detail' configuration page for a device named 'AVAYA' (ID: 7, Admin State: UNLOCKED). The 'Routing Parameters' section is active, showing various settings for call routing. The 'Custom Routing Plan' is set to 'AVAYA'. Other settings include 'Forced DN Routing' (Off), 'National Destination Code' (empty), 'Call Direction' (Bidirectional), 'Append QoR Capability' (No), 'Terminating Trunk Group' (No), 'Maximum Satellite Hops' (empty), 'Use Single Local Gateway In Egress' (No), 'Forced CPN Routing' (Off), 'Is PSTN Handoff Trunk Group' (No), 'Time Zone' (empty), 'Class Of Service Usage' (Ignore), 'Veraz Call Block' (No), 'Satellite Trunk Group' (No), and 'Class Of Service Profile' (empty). At the bottom, there are tabs for 'Additional Parameters': Common, General, Digit Rules, Egress, IP Configuration, Ingress, and Services.

Routing Parameters	
Custom Routing Plan:	AVAYA
* Forced DN Routing:	Off
National Destination Code:	
* Call Direction:	Bidirectional
* Append QoR Capability:	No
* Terminating Trunk Group:	No
Maximum Satellite Hops:	
* Use Single Local Gateway In Egress:	No
* Forced CPN Routing:	Off
* Is PSTN Handoff Trunk Group:	No
Time Zone:	
Class Of Service Usage:	<input type="radio"/> Exclude <input type="radio"/> Include <input checked="" type="radio"/> Ignore
* Veraz Call Block:	No
* Satellite Trunk Group:	No
Class Of Service Profile:	

Additional Parameters: Common General Digit Rules Egress IP Configuration Ingress Services

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.

Detail

Name: **AVAYA** ID: 7 Admin State: **UNLOCKED**

Common Parameters

* Speech :	Yes ▾	* 3.1 KHz Audio :	Yes ▾
* UDI :	Yes ▾	* Echo Cancellation :	Yes ▾
* Silence Suppression :	No ▾	* Is International :	No ▾
Route Type :	▾	* Minimum Packetization Period :	10
* Maximum Packetization Period :	20	CODEC Priority Order :	Don't Care ▾
* Negotiate CODEC With Gateway :	Yes ▾	* Max-Forwards to Hop Counter Factor :	0
* Hop Counter to Max-Forwards Factor :	0	* Enable Propagation delay Counter :	No ▾
Propagation Delay :			

Additional Parameters

General Digit Rules Egress IP Configuration Ingress Routing Services

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.

The screenshot shows a 'Detail' window for a configuration item named 'AVAYA' with ID 7 and Admin State 'UNLOCKED'. The 'Ingress Parameters' section is active. It contains the following fields:

- CPN Presentation Indicator: Pass As Is (dropdown)
- Connected Number Presentation Indicator: Pass As Is (dropdown)
- CPN Required: No (dropdown)
- Charge Number: (text field)
- Charge Number Handling: Pass As Is (dropdown)
- Nature Of Address: (text field)
- OU: (text field)

At the bottom, there are tabs for 'Additional Parameters': Common, General, Digit Rules, Egress, IP Configuration, Routing, and Services.

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.

The screenshot shows the same 'Detail' window, but the 'Egress Parameters' section is active. It contains the following fields:

- Calling Party Presentation Indicator: Pass As Is (dropdown)
- Connected Number Presentation Indicator: Pass As Is (dropdown)
- HOP Counter Activation: No (dropdown)
- HOP Counter: 20 (text field)
- Send CPN: Yes (dropdown)

At the bottom, the 'Egress' tab is selected under 'Additional Parameters'.

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.

Detail

Name: AWAYA ID: 7 Admin State: UNLOCKED

Services Parameters:

Service Resolution (SRS): Off Service: Tandem

Service Execution Element: SEE Subscription Flag: No

Service Trigger Plan Group: Custom QoS Plan Group:

Additional Parameters Common General Digit Rules Egress IP Configuration Ingress Routing

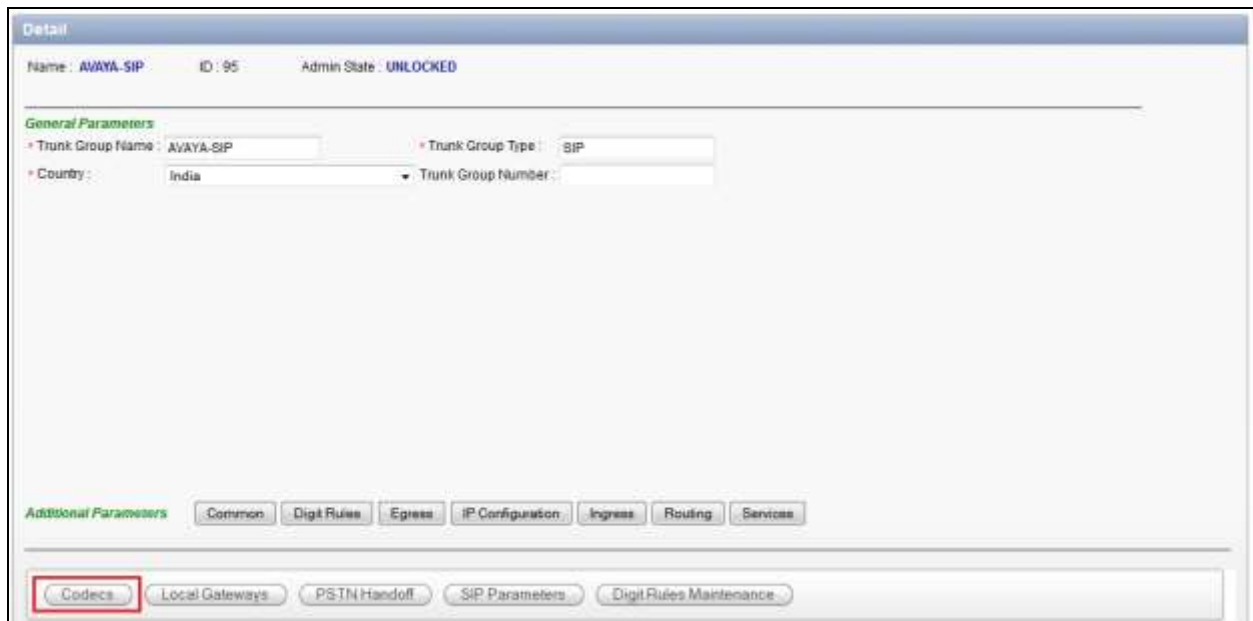
10. Click the **Save** icon to create the Trunk Group (TG) in the EMS database.

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.



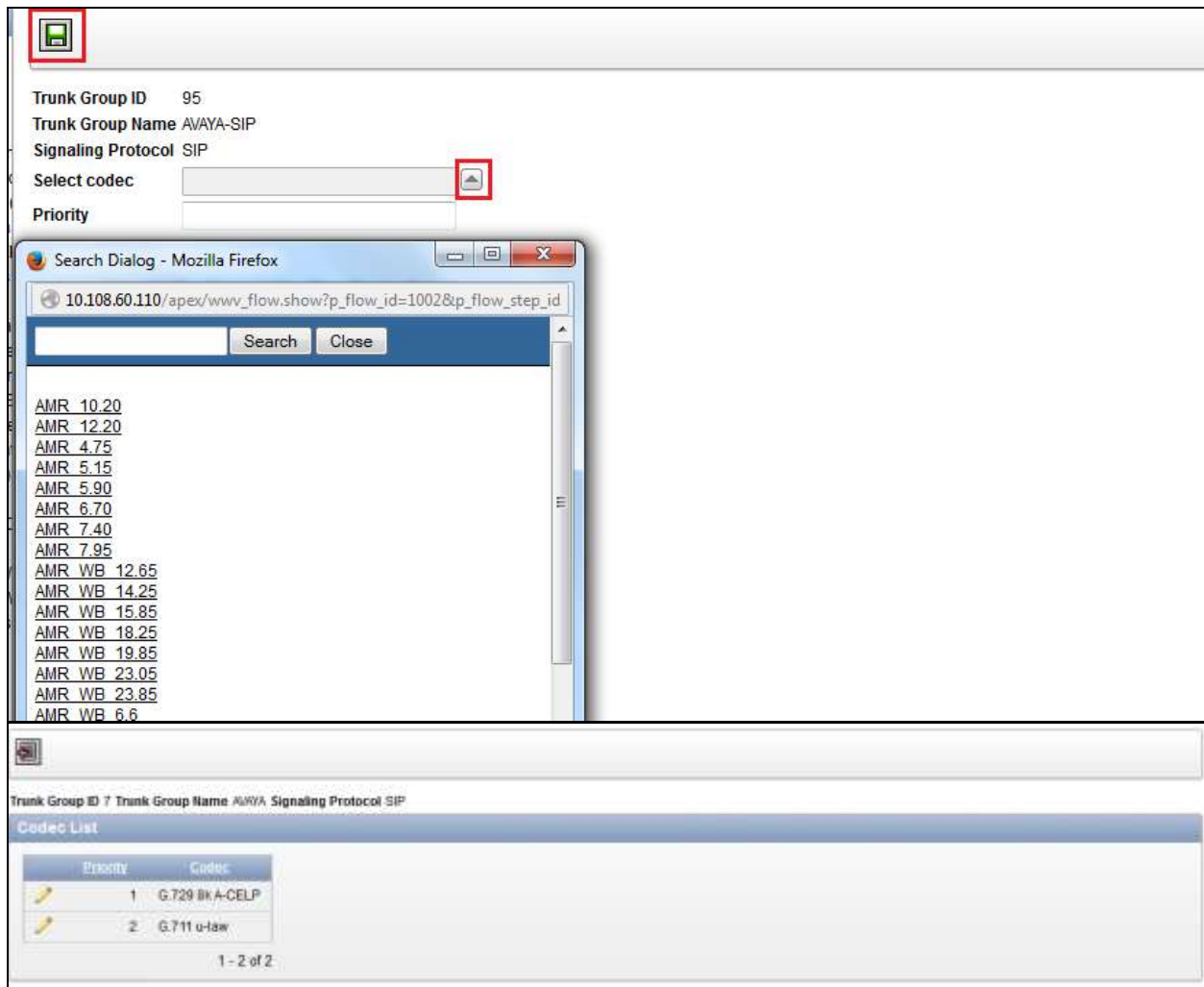
The screenshot shows the configuration page for a Trunk Group named 'AVAYA-SIP' with ID 95 and Admin State 'UNLOCKED'. The 'General Parameters' section includes fields for 'Trunk Group Name' (AVAYA-SIP), 'Trunk Group Type' (SIP), 'Country' (India), and 'Trunk Group Number'. Below this is the 'Additional Parameters' section with tabs for 'Common', 'Digit Rules', 'Egress', 'IP Configuration', 'Ingress', 'Routing', and 'Services'. At the bottom, a row of tabs includes 'Codecs' (highlighted with a red box), 'Local Gateways', 'PSTN Handoff', 'SIP Parameters', and 'Digit Rules Maintenance'.

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



The screenshot shows the 'Codecs List' section for Trunk Group ID 95, Trunk Group Name AVAYA-SIP, and Signaling Protocol SIP. A message states: 'No codecs are assigned to this trunk group. Click on insert [=] to assign codecs.' The 'add' button (represented by a small icon) is highlighted with a red box.

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.

The screenshot shows the 'Detail' page for the 'AVAYA-SIP' Trunk Group. The page has a header with 'Name: AVAYA-SIP', 'ID: 95', and 'Admin State: UNLOCKED'. Below this is the 'General Parameters' section with fields for 'Trunk Group Name' (AVAYA-SIP), 'Trunk Group Type' (SIP), 'Country' (India), and 'Trunk Group Number'. At the bottom, there are several tabs: 'Common', 'Digit Rules', 'Egress', 'IP Configuration', 'Ingress', 'Routing', 'Services', 'Codecs', 'Local Gateways' (highlighted with a red box), 'PSTN Handoff', 'SIP Parameters', and 'Digit Rules Maintenance'.

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

The screenshot shows the 'Trunk Group - Local Gateways Associations' page. At the top, there are three icons: a red 'add' button (highlighted with a red box), a green 'refresh' button, and a green 'delete' button. Below this is the 'Trunk Group Details' section with fields for 'Trunk Group ID' (95), 'Trunk Group Name' (AVAYA-SIP), 'Trunk Group Type' (Direct), and 'Protocol' (SIP). The main section is titled 'Trunk Group - Local Gateways Associations' and contains a search bar with a 'Go' button. Below the search bar, it states 'No local gateways are associated with this trunk group.'

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

Add Trunk Group - Local Gateway Associations

Trunk Group ID: 95
Trunk Group Name: AVAYA-SIP
Trunk Group Protocol: SIP

*Local Gateway Name: -- Select LGW Name --
*Egress Priority: -- Select LGW Name --
*Ingress Priority: -- Select LGW Name --

AVAYA-LGW
LGW4
LGW5
LGW58
LGW98
TEST
TESTbc1-63.218.79.231.2061

Egress Weight: 1
Ingress Weight: 1

Priority And Weight: 0
No data found.

th This Trunk Group

The AVAYA SIP Trunk Group details is shown below.

Trunk Group Details

Trunk Group ID: 7
Trunk Group Name: AVAYA
Trunk Group Type: Direct
Protocol: SIP

Trunk Group - Local Gateways Associations

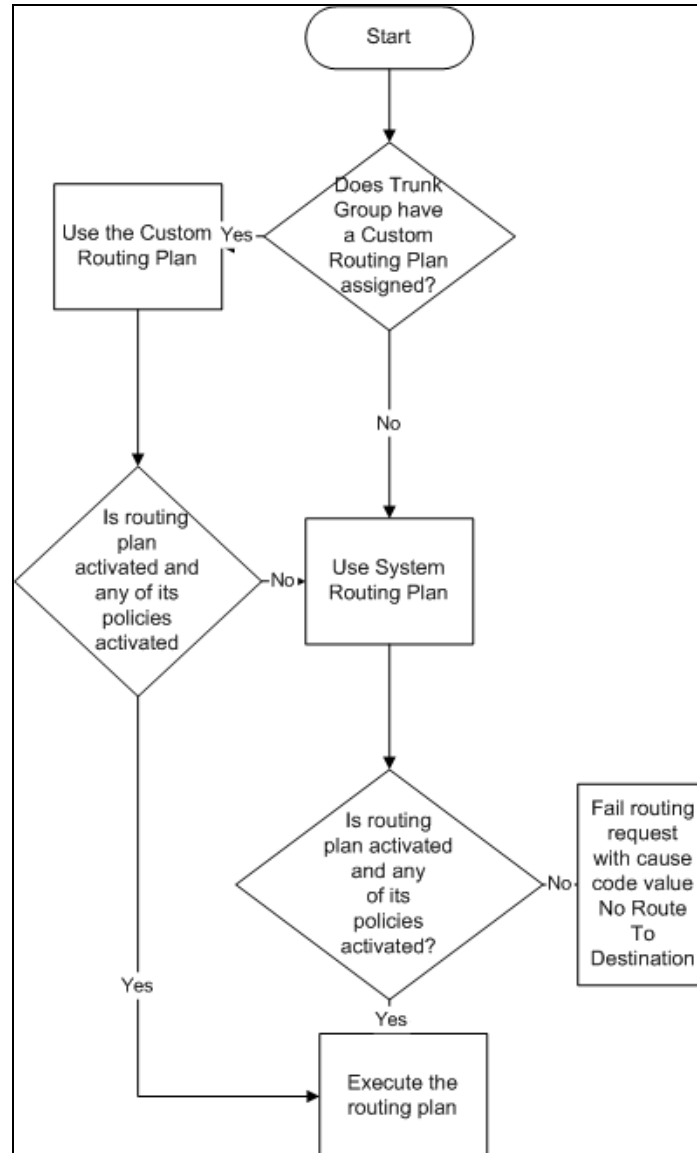
Select Item	Local Gateway	Egress Priority	Egress Weight	Ingress Priority	Ingress Weight	Admin State
	AVAYA-LGW	1	1	1	1	UNLOCKED

1 - 1 of 1

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.

Plan Details

ID:

Name: AVAYA

Description:

Plan Type: ROUTING

Reroute Plan:

Apply QoS on Ingress and Call Level Parameters: ☐ Yes ☒ No

QoS Plan:

System Plan: ☐ Yes ☒ No

State: ☒ Activated ☐ Deactivated

Route Collection

Collect Across Policies: ☒ Yes ☐ No

Max Collected Routes: 12

Include Routes From System Plan: ☐ Yes ☒ No

Status:

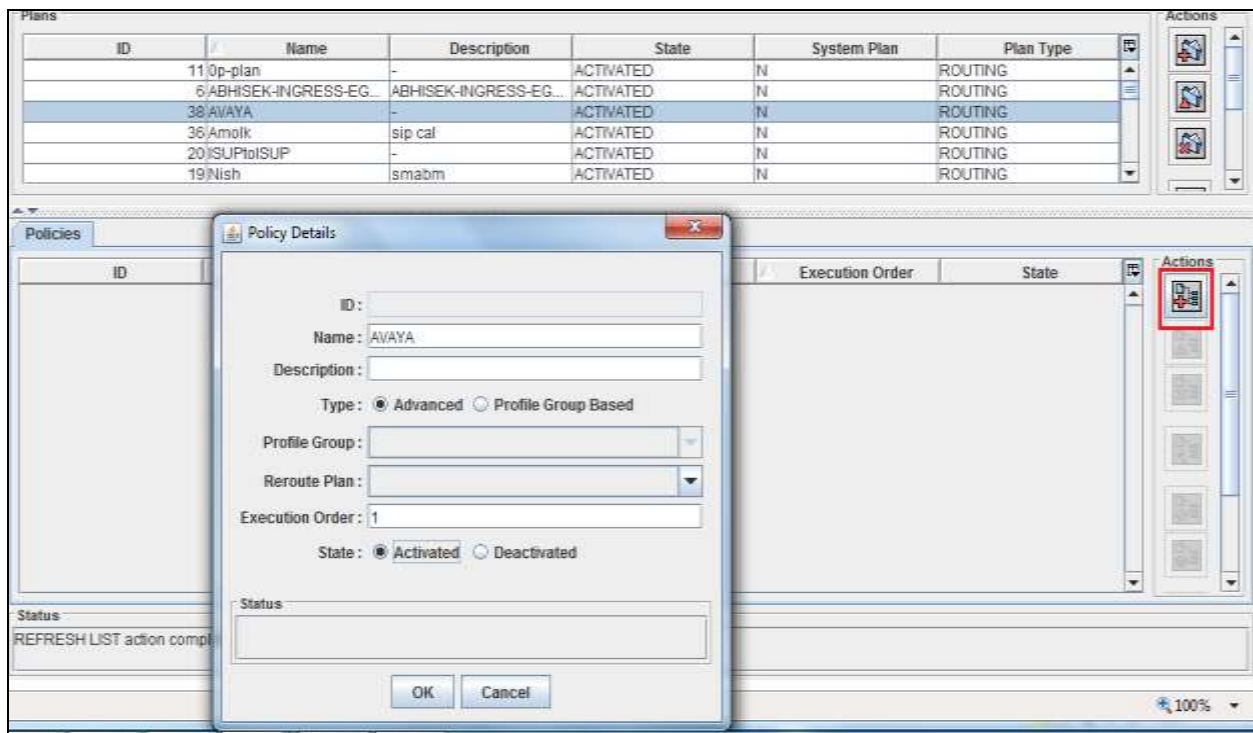
OK Cancel

Background Tables:

Plan	Plan Type
ROUTING	ROUTING
ROUTING	ROUTING
ROUTING	ROUTING
ROUTING	ROUTING
ROUTING	ROUTING

Order	State
1	ACTIVATED
5	ACTIVATED
6	ACTIVATED
8	DEACTIVATED

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.

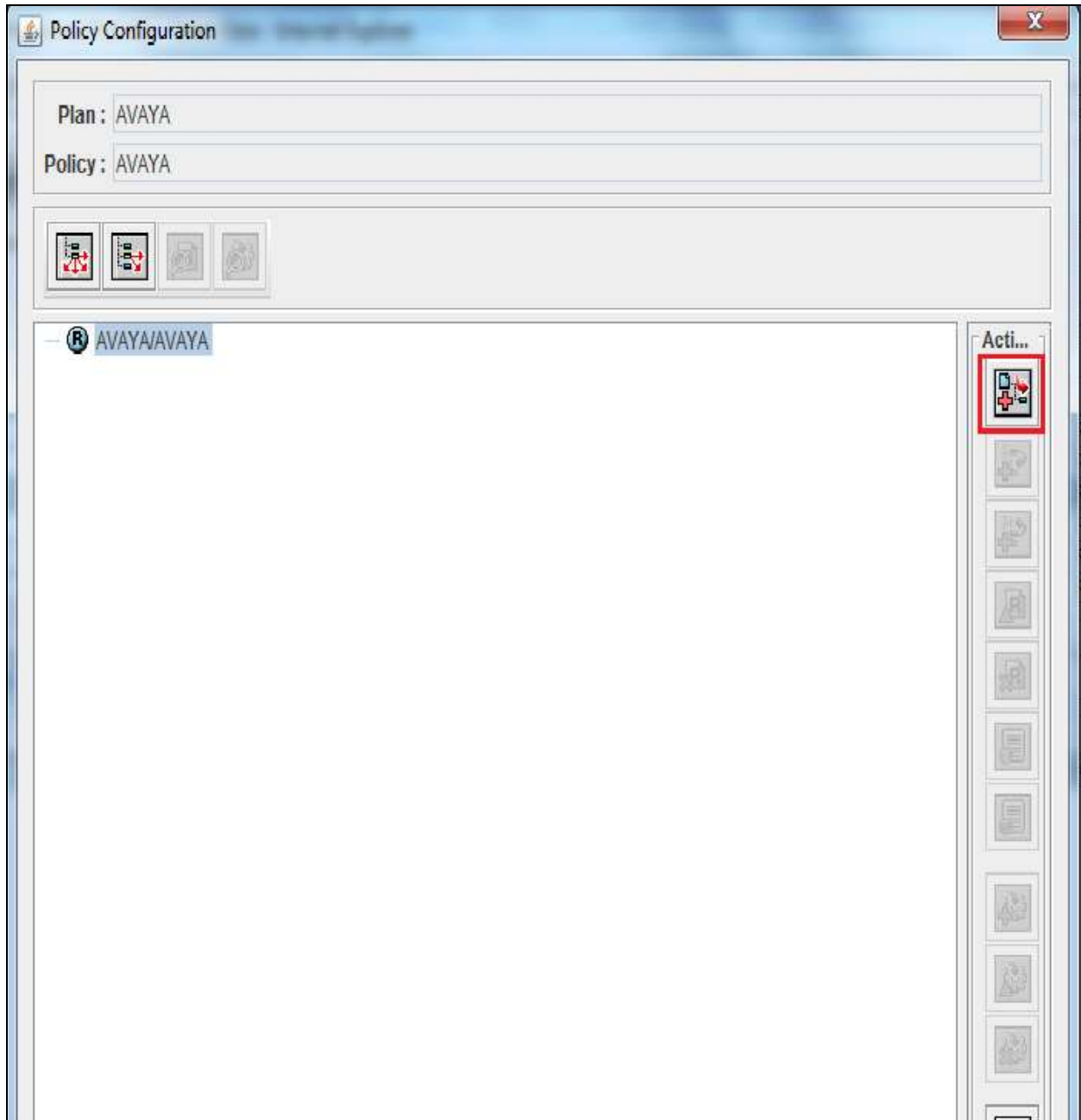
The screenshot displays a software interface for managing a Routing Plan. At the top, there is a 'Plan Group' section with a 'Name' field and a 'Type' dropdown set to 'Routing'. Below this is a 'Plans' table with columns: ID, Name, Description, State, System Plan, and Plan Type. The table contains four rows of data. To the right of the 'Plans' table is an 'Actions' column with icons for various operations. Below the 'Plans' table is a 'Policies' section with a table containing columns: ID, Name, Description, Type, Execution Order, and State. The 'Policies' table has one row of data. To the right of the 'Policies' table is another 'Actions' column with icons. At the bottom of the interface is a 'Status' bar showing the message 'REFRESH SUMMARY TABLE action completed.'

ID	Name	Description	State	System Plan	Plan Type
6	AWAYA	-	ACTIVATED	N	ROUTING
3	RAO	-	ACTIVATED	N	ROUTING
2	mtest	mm	ACTIVATED	N	ROUTING
1	sunil	sip-sip	ACTIVATED	N	ROUTING

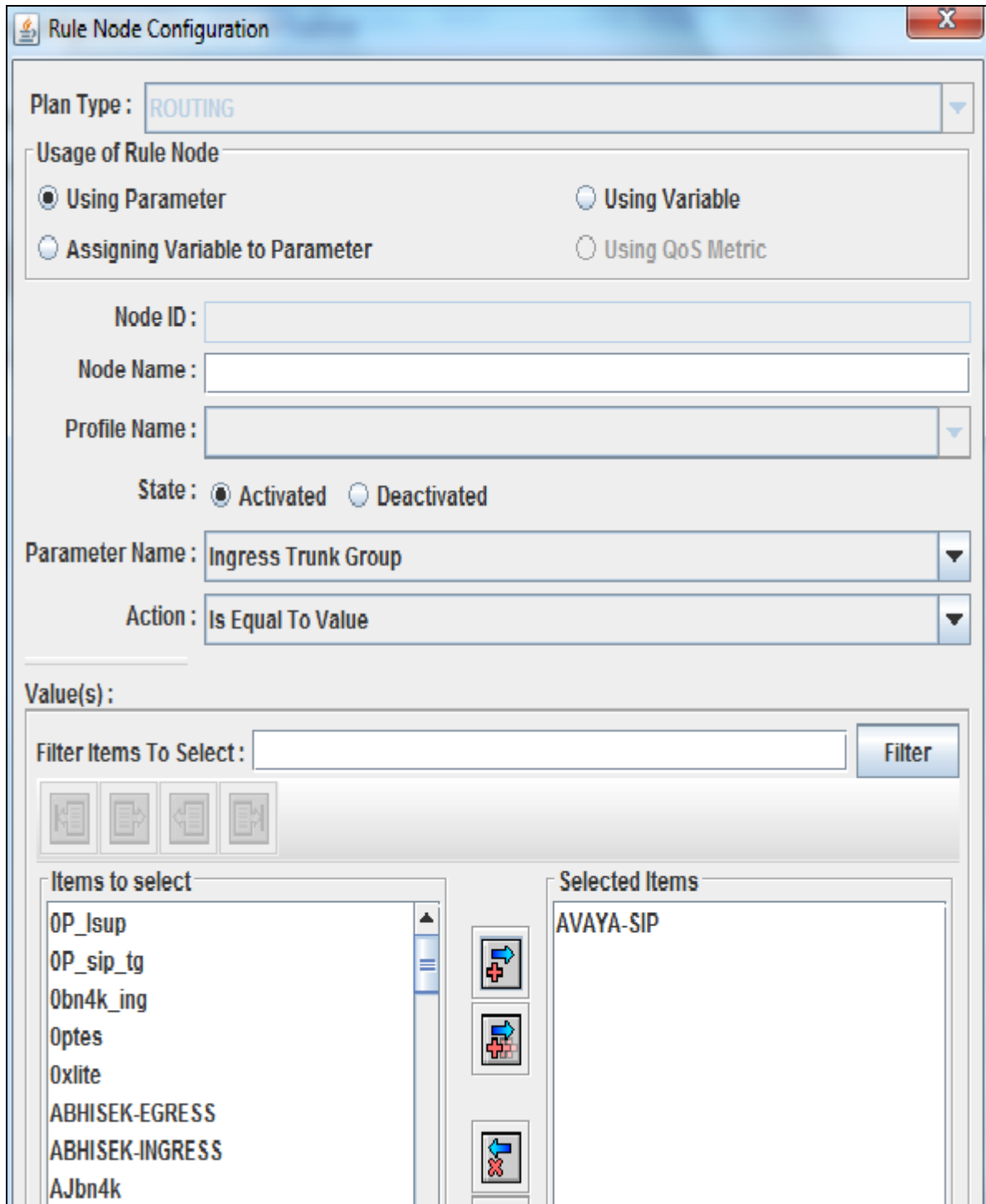
ID	Name	Description	Type	Execution Order	State
6	AWAYA	-	Advanced	1	ACTIVATED

Status
REFRESH SUMMARY TABLE action completed.

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.



The screenshot shows the 'Rule Node Configuration' dialog box. The 'Plan Type' is set to 'ROUTING'. Under 'Usage of Rule Node', 'Using Parameter' is selected. The 'Node ID' and 'Node Name' fields are empty. The 'Profile Name' is empty. The 'State' is set to 'Activated'. The 'Parameter Name' is 'Ingress Trunk Group' and the 'Action' is 'Is Equal To Value'. The 'Value(s)' section shows a list of items to select, with 'AVAYA-SIP' selected.

Rule Node Configuration

Plan Type : ROUTING

Usage of Rule Node

☒ Using Parameter ☐ Using Variable

☐ Assigning Variable to Parameter ☐ Using QoS Metric

Node ID :

Node Name :

Profile Name :

State : ☒ Activated ☐ Deactivated

Parameter Name : Ingress Trunk Group

Action : Is Equal To Value

Value(s) :

Filter Items To Select: Filter

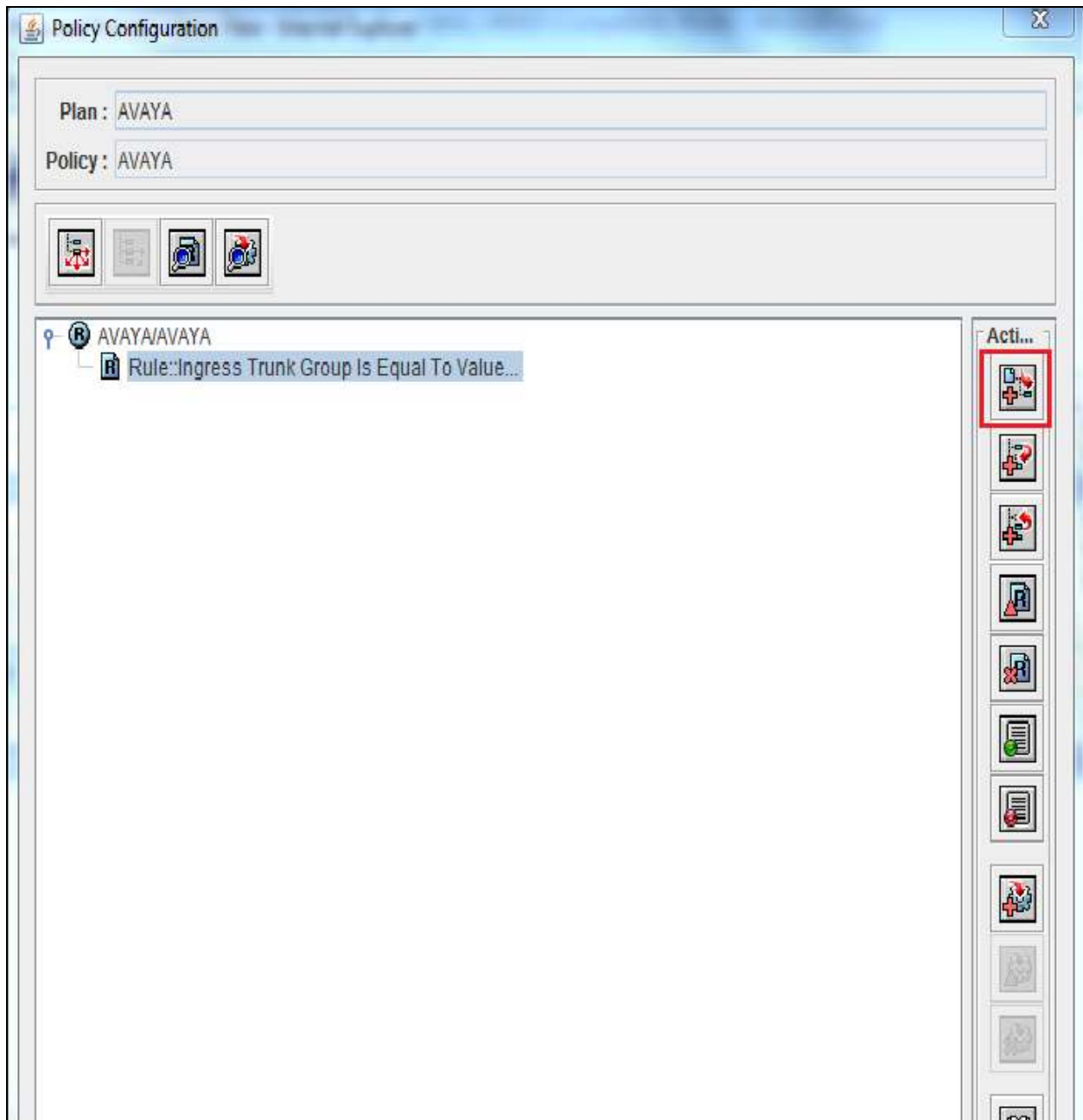
Items to select

- OP_Isup
- OP_sip_tg
- Obn4k_ing
- Optes
- Oxlite
- ABHISEK-EGRESS
- ABHISEK-INGRESS
- AJbn4k

Selected Items

- AVAYA-SIP

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.

Modify Treatment Node

Plan Type : **ROUTING**

Node ID : 110

Profile Name :

Treatment Type : **Route**

Treatment Parameters

Charge Band | **Reroute Plan** | Service Name | Satellite Hop Count | Qos Plan

Egress Points | Features | Call Type

Egress Types : **Trunk Group**

Items to select:

- AVAYA
- INET
- RAO-SIP
- Sunil-In
- Sunil-egr
- mtest
- murali

Selected Items:

- ISUP

Egress Properties

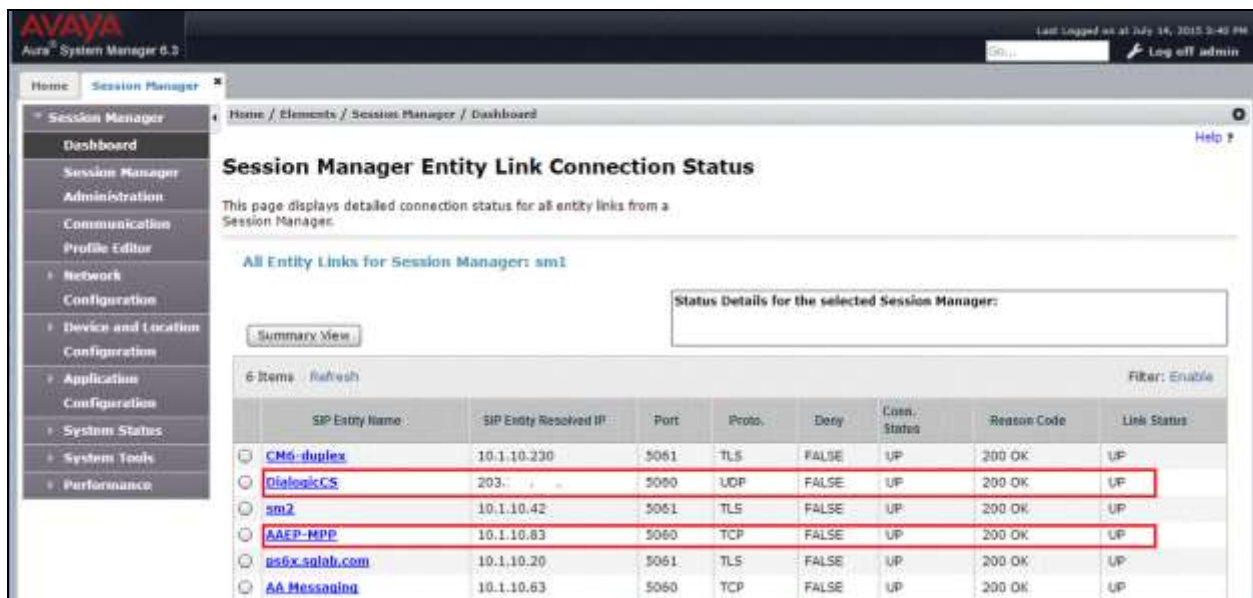
Type	Item	Priority	Weight	Charge Band	Reroute Plan	Digit Collection ...
Trunk Group	ISUP					

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**.



Avaya Aura® System Manager 6.3

Last Logged in at July 14, 2015 3:42 PM

Log off admin

Home / Elements / Session Manager / Dashboard

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: sm1

Status Details for the selected Session Manager:

Summary View

6 Items Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto	Deny	Conn. Status	Reason Code	Link Status
<input type="checkbox"/>	CM6-duplex	10.1.10.230	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	DialogicCS	203.113.113.113	5060	UDP	FALSE	UP	200 OK	UP
<input type="radio"/>	sm2	10.1.10.42	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	AAEP-MPP	10.1.10.83	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	ps6x.snlab.com	10.1.10.20	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	AA Messaging	10.1.10.63	5060	TCP	FALSE	UP	200 OK	UP

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**.

Avaya Aura® Experience Portal 7.0.1 (ExperiencePortal)

Welcome, eadmin
Last logged in today at 23:13:41 PDT

Expand All | Collapse All

- User Management
 - Roles
 - Users
 - Login Options
- Real-time Monitoring
 - System Monitor
 - Active Calls
 - Port Distribution
- System Maintenance
 - Audit Log Viewer
 - Trace Viewer
 - Log Viewer
 - Alarm Manager
- System Management
 - Application Server
 - EPH Manager
 - MPP Manager
 - Software Upgrade
 - System Backup
- System Configuration
 - Applications
 - EPH Servers
 - MPP Servers
 - SNMP
 - Speech Servers
 - VoIP Connections
 - Zones
- Security
 - Certificates
 - Licensing
- Reports
 - Standard
 - Custom
 - Scheduled
- Multi-Media Configuration
 - Email
 - SMS

You are here: Home > Real-Time Monitoring > Port Distribution > Port Distribution Report

Port Distribution Report (15-Jul-2015 01:00:30 PDT)

This page displays information about how the telephony resources have been distributed to the HPPs. You configure the telephony resources on the VoIP Connections page.

Servers: AAEP-MPP
Total Ports: 10
Last Poll: 15-Jul-2015 01:00:26 PDT

Port	Mode	State	Port Group	Protocol	Current Allocation	Base Allocation
10101	Inbound	In service	CH_Duplex	H323	AAEP-MPP	
10102	Inbound	In service	CH_Duplex	H323	AAEP-MPP	
10103	Inbound	In service	CH_Duplex	H323	AAEP-MPP	
2	Online	In service SM1	SIP_Trunk	AAEP-MPP		

Help

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.

Avaya Aura® Experience Portal 7.0.1 (ExperiencePortal)

Proactive Outreach Manager 3.0

POM Home

Campaign Manager

Last poll: 15/07/2015 02:04:21

This page displays Campaigns and actions associated with Campaigns depending on your user role.

Search: [] [X] Advanced

Show: 50 | Page: 1/1

Name	Type	Campaign Strategy	Contact Lists	Last Executed	Actions
TestCampaign	Finite	CampaignStrategy1	DialogicCS	15/07/2015 01:27:30	[] [] [] [] [] []

* In Progress means Campaign job can be in any one of the states - running, pausing, paused, callback, stopping.

Add Help

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



Campaign Name	Campaign Type	Job ID	Status	Contact List(s)	Organization	Start Time	Total Contacts	Processed Contacts
TestCampaign	Test	148	Running	DialogicCS		07/15/2015 5:11	1	0

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



Standard Reports

Use this page to generate standard reports. Click on the report name to view the report.

Report Name	View Report
Application Summary	
Application Detail	
Contact Summary	
Contact Detail	
Performance	
Session Summary	
Session Detail	
Data Export	
POM Campaign Detail	
POM Campaign Parameters History	
POM Campaign Summary	
POM Completion Code Summary	
POM Completion Code Trend	
POM Contact List Import Detail	
POM Contact List Import Summary	
POM DNC Import Details	
POM DNC Import Summary	
POM Individual Import Details	

Help

[illegible]

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**.

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

- Dialogic[®] products references are available on <http://www.dialogic.com/en/products.aspx>.

©2015 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.