



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Presence Technology OpenGate R11.0 to interoperate with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Session Manager R7.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Presence Technology OpenGate to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Presence Technology OpenGate provides ACD and CTI capabilities to companies that do not have any existing CTI or ACD capabilities on their PBX. Presence Technology OpenGate integrates with the Avaya solution using SIP trunks and digit manipulation.

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 configuration used to verify Presence Technology OpenGate R11.0 can successfully interoperate with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Session Manager R7.1. Presence Technology OpenGate can be used as an external Automatic Call Distribution (ACD) routing engine and IVR as well as a trunk gateway between the PSTN and an existing PBX, such as Avaya Aura® Communication Manager.

Presence Technology OpenGate replaces the Avaya Aura® Application Enablement Services requirement for a CTI connection to Communication Manager by utilizing a SIP connection to Session Manager for routing calls to the Communication Manager handsets. Presence Suite is required to test the connection of Presence OpenGate to Session Manager. The Presence Suite includes the Presence Server, Presence Mail Interactions Server, Presence Web Interactions Server, Presence Administrator, Presence Supervisor, and Presence Agent. Please note that these Application Notes only describe the setup required to add Presence Technology OpenGate. The setup of Presence Technology Presence Suite is outside the scope of these Application Notes but can be found in the Application Notes titled *Application Notes for Configuring Presence Technology Presence Suite R11.0 with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1*.

2. General Test Approach and Test Results

Testing was performed manually by dialing numbers that were configured to route to OpenGate and receive ACD treatment. Testing included validation of correct operation of typical contact center functions including, inbound voice calls being delivered on an agent skill level basis and call queuing. Functionality testing included basic telephony operations such as answer, hold/retrieve, transfer, and conference. The serviceability test cases were performed manually by busying out and releasing the SIP trunk and by disconnecting and reconnecting the LAN cables. Link Failure\Recovery was tested to ensure successful reconnection on link failure.

For the sample configuration discussed in this document, all calls received from the PSTN by Communication Manager were routed via a SIP Trunk to Session Manager. Session Manager is then responsible for routing the call to OpenGate to receive ACD treatment. OpenGate can route calls to Presence agents served by Avaya endpoints.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya

products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and OpenGate did not include use of any specific encryption features as requested by Presence Technology.

2.1 Interoperability Compliance Testing

In the sample configuration described by these Application Notes, calls will be accepted from the PSTN and routed to OpenGate. OpenGate will then map these digits to an internal number which represents the ACD service queue within OpenGate. OpenGate then routes the call to an available Avaya extension by dialing that extension number.

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on verifying OpenGate was capable of receiving calls from Communication Manager and providing ACD treatment to route those calls to available extensions. The serviceability testing focused on verifying the ability of OpenGate to recover from adverse conditions, such as disconnecting the Ethernet cable from the server.

2.2 Test Results

All test cases passed successfully.

2.3 Support

Technical support can be obtained for Presence Technology OpenGate as follows:

- Email: support@presenceco.com
- Website: www.presenceco.com
- Phone: +34 93 10 10 300

3. Reference Configuration

Figure 1 shows the network topology in place during compliance testing. Communication Manager and an Avaya G430 Media Gateway were used as the hosting PBX. SIP trunks are configured between Communication Manager, Session Manager and OpenGate to transport calls between them. Presence Suite, including Presence Agent PC's, were connected to the LAN to provide Agent desktop application connectivity.

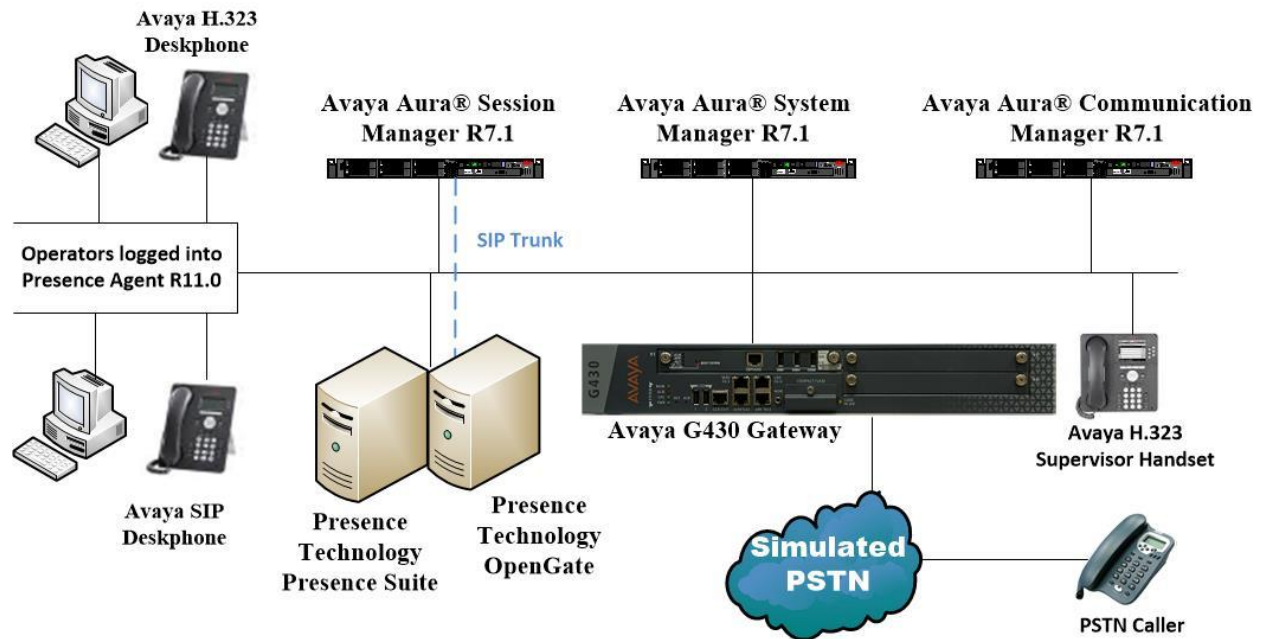


Figure 1: Network Topology used to test Presence Technology OpenGate R11.0 with Avaya Aura® Session Manager R7.1 and Avaya Aura® Communication Manager R7.1

4. Equipment and Software Validated

All the hardware and associated software used in the compliance testing is listed below.

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.1.1.0 Build No. - 7.1.0.0.1125193 Software Update Revision No: 7.1.1.0.046931 Feature Pack 1 Service Pack 1
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.1 SP1 Build No. – 7.1.1.0.711008
Avaya Aura® Communication Manager running on Virtual Server	R017x.01.0.532.0 R7.1.1.0.0 - FP1 Update ID 01.0.532.0-23985
Avaya Aura® Media Server running on Virtual Server	R7.8
Avaya G430 Gateway	37.42.0 /1
Avaya 96x1 H323 Deskphone	96x1 H323 Release 6.6401
Avaya 96x1 SIP Deskphone	96x1 SIP Release 7.1.0.1.1
Presence Technology Presence Suite running on Windows Server 2016 Server	R11.0
Presence Technology OpenGate running on Windows Server 2016 Server	R11.0
Presence Technology Presence Client running on Windows 7 SP1	R11.0

Table 1: Hardware and Software Version Numbers

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. Please note that this is the setup required to add OpenGate only the setup of the other possible Presence Suite is outside the scope of these Application Notes but can be found in the Application Notes titled *Application Notes for Configuring Presence Technology Presence Suite R11.0 with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1*.

The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options
- System Features and Access Codes
- Administer Dial Plan
- Administer Route Selection for OpenGate calls
- Configure SIP Trunk

Note: The configuration of the PRI interface to the PSTN is outside the scope of these Application Notes.

5.1 Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that the **Maximum Administered SIP Trunks** have sufficient capacity. Each call that receives ACD treatment from OpenGate uses a minimum of one SIP trunk. Calls that are routed back to stations commissioned on Communication Manager, or calls that are routed back to Communication Manager to access the PSTN, use 2 SIP trunks.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES	USED		
Maximum Administered H.323 Trunks:	12000	250	
Maximum Concurrently Registered IP Stations:	18000	2	
Maximum Administered Remote Office Trunks:	12000	0	
Maximum Concurrently Registered Remote Office Stations:	18000	0	
Maximum Concurrently Registered IP eCons:	414	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	18000	0	
Maximum Video Capable IP Softphones:	18000	0	
Maximum Administered SIP Trunks:	24000	319	
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0	

On **Page 3**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

display system-parameters customer-options	Page 3 of 11
OPTIONAL FEATURES	
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y
Access Security Gateway (ASG)? n	Authorization Codes? y
Analog Trunk Incoming Call ID? y	CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n
Answer Supervision by Call Classifier? y	Change COR by FAC? n
ARS? y	Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? y	DCS (Basic)? y

On **Page 5**, ensure that **Uniform Dialing Plan** is set to **y**.

display system-parameters customer-options	Page 5 of 11
OPTIONAL FEATURES	
Multinational Locations? n	Station and Trunk MSP? y
Multiple Level Precedence & Preemption? n	Station as Virtual Extension? y
Multiple Locations? n	System Management Data Transfer? n
Personal Station Access (PSA)? y	Tenant Partitioning? y
PNC Duplication? n	Terminal Trans. Init. (TTI)? y
Port Network Support? y	Time of Day Routing? y
Posted Messages? y	TN2501 VAL Maximum Capacity? y
Private Networking? y	Uniform Dialing Plan? y
	Usage Allocation Enhancements? y

5.2 System Features and Access Codes

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 10** for supporting documentation.

display system-parameters features	Page 1 of 19
FEATURE-RELATED SYSTEM PARAMETERS	
Self Station Display Enabled? n	
Trunk-to-Trunk Transfer: all	
Automatic Callback with Called Party Queuing? n	
Automatic Callback - No Answer Timeout Interval (rings): 3	
Call Park Timeout Interval (minutes): 10	
Off-Premises Tone Detect Timeout Interval (seconds): 20	
AAR/ARS Dial Tone Required? y	
Music (or Silence) on Transferred Trunk Calls? no	
DID/Tie/ISDN/SIP Intercept Treatment: attd	
Internal Auto-Answer of Attnd-Extended/Transferred Calls: transferred	
Automatic Circuit Assurance (ACA) Enabled? n	
Abbreviated Dial Programming by Assigned Lists? n	
Auto Abbreviated/Delayed Transition Interval (rings): 2	
Protocol for Caller ID Analog Terminals: Bellcore	
Display Calling Number for Room to Room Caller ID Calls? n	

Use the **display feature-access-codes** command to verify that a FAC (feature access code) has been defined for both AAR and ARS. Note that **8** is used for AAR and **9** for ARS routing.

display feature-access-codes	Page 1 of 10
FEATURE ACCESS CODE (FAC)	
Abbreviated Dialing List1 Access Code:	
Abbreviated Dialing List2 Access Code:	
Abbreviated Dialing List3 Access Code:	
Abbreviated Dial - Prgm Group List Access Code:	
Announcement Access Code:	
Answer Back Access Code:	
Attendant Access Code:	
Auto Alternate Routing (AAR) Access Code: 8	
Auto Route Selection (ARS) - Access Code 1: 9	Access Code 2:
Automatic Callback Activation: *25	Deactivation: #25

5.3 Administer Dial Plan

It was decided for compliance testing that all calls to 6300 were to be sent across the SIP trunk to Session Manager and therefore to OpenGate. In order to achieve this routing, automatic alternate routing (aar) will be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this routing.

Type **change dialplan analysis** in order to make changes to the dial plan. Note that **6** is of call type **udp** which means any numbers beginning with 6 are a part of the uniform dial plan.

change dialplan analysis

Page 1 of 12

DIAL PLAN ANALYSIS TABLE

Location: all

Percent Full: 3

Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	4	udp	#	3	fac			
2	4	udp						
3	4	udp						
4	4	ext						
5	4	udp						
58	5	ext						
5999	4	ext						
6	4	udp						
6666	4	ext						
7	4	udp						
781	5	ext						
8	1	fac						
9	1	fac						
*	3	fac						
*8	4	dac						

5.4 Administer Route Selection for OpenGate Calls

Use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to 6300 will use Automatic Alternate Routing (aar). No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

change uniform-dialplan 6						Page	1 of	2
UNIFORM DIAL PLAN TABLE						Percent Full: 0		
Matching			Insert			Node		
Pattern	Len	Del	Digits	Net	Conv	Num		
6300	4	0		aar	n			
65	4	0		aar	n			
					n			
					n			
					n			
					n			
					n			
					n			

Use the **change aar analysis** command to further configure the routing of the dialed digits. Calls to OpenGate are achieved by dialing 6300 and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

change aar analysis 6						Page	1 of	2
AAR DIGIT ANALYSIS TABLE						Percent Full: 3		
Location: all								
Dialed	Total		Route	Call	Node	ANI		
String	Min	Max	Pattern	Type	Num	Reqd		
6	7	7	254	aar		n		
6300	4	4	1	aar		n		
65	4	4	1	aar		n		
7	7	7	254	aar		n		
8	7	7	254	aar		n		
9	7	7	254	aar		n		
						n		
						n		
						n		
						n		
						n		

Use the **change route-pattern *n*** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, Route Pattern Number **1** is used to route calls to trunk group (Grp No) **1**, this is the SIP Trunk configured in **Section 5.5**. The **Numbering Format** was set to **lev0-pvt**.

change route-pattern 1										Page 1 of 3	
Pattern Number: 1										Pattern Name: SIP TRUNK	
SCCAN? n		Secure SIP? n		Used for SIP stations? n							
Grp		FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC		
No				Mrk	Lmt	List	Del	Digits	QSIG		
								Dgts	Intw		
1:	1	0							n	user	
2:									n	user	
3:									n	user	
4:									n	user	
5:									n	user	
6:									n	user	
		BCC VALUE		TSC	CA-TSC		ITC BCIE Service/Feature		PARM	Sub	Numbering LAR
		0	1	2	M	4	W	Request		Dgts	Format
1:	y	y	y	y	y	n	n		unre		lev0-pvt none
2:	y	y	y	y	y	n	n		rest		none
3:	y	y	y	y	y	n	n		rest		none
4:	y	y	y	y	y	n	n		rest		none
5:	y	y	y	y	y	n	n		rest		none
6:	y	y	y	y	y	n	n		rest		none

5.5 Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of the **procr** and Session Manager (**SM71vmpg**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

display node-names ip		Page	1 of	2
		IP NODE NAMES		
Name	IP Address			
AES71vmpg	10.10.40.43			
AMS71vmpg	10.10.40.49			
GW71vmpg	10.10.40.15			
SM70vmpg	10.10.40.12			
SM71vmpg	10.10.40.52			
default	0.0.0.0			
procr	10.10.40.47			
procr6	::			

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.2**. In this configuration, the domain name is **devconnect.local**. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

```

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

```

In the **IP Codec Set** form, select the audio codecs supported for calls routed over the SIP trunk to OpenGate. The form is accessed via the **change ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), **G.711MU** (mu-law) and **G729A** which are supported by OpenGate.

```

change ip-codec-set 1
IP MEDIA PARAMETERS
Codec Set: 1

```

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1: G.711A	n	2	20
2: G.711MU	n	2	20
3: G.729A	n	2	20
4:			
5:			
6:			
7:			

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the desired transport method; **tcp** (transport control protocol) or **tls** (Transport Layer Security).
- The **Peer Detection Enabled** field should be set to **y** allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM71vmpg**), also shown above.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above. This field logically establishes the **far-end** for calls using this signaling group as network region **1**.
- The **Far-end Domain** field can be set to the domain name specified in the IP Network Region.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The default values for the other fields may be used.

change signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y Peer Server: SM		
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: SM71vmpg	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
Far-end Network Region: 1		
Far-end Domain: devconnect.local		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from OpenGate. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

change trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: SIPTRUNK	COR: 1	TN: 1	TAC: *801
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 1		
	Number of Members: 10		

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Presence to prevent unnecessary SIP messages during call setup. For the compliance test a value of **600** was used.

change trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n	Digital Loss Group: 18		
	Preferred Minimum Session Refresh Interval(sec): 600		
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto		Delay Call Setup When Accessed Via IGAR? n	
Caller ID for Service Link Call to H.323 1xC: station-extension			

Settings on **Page 4** are as follows. These are the values used during compliance testing.

change trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: private
	UUI Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

Settings on **Page 4** are as follows.

change trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
	Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? y	
Send Diversion Header? n	
Support Request History? y	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

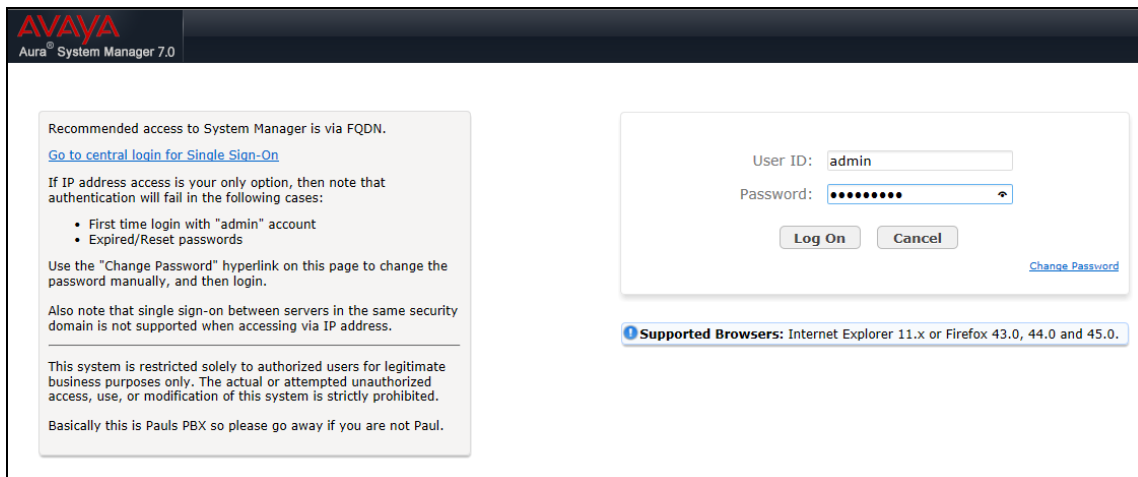
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® Session Manager
- Administer SIP Domain
- Administer Location
- Administer SIP Entities
- Administer Routing Policies
- Administer Dial Patterns

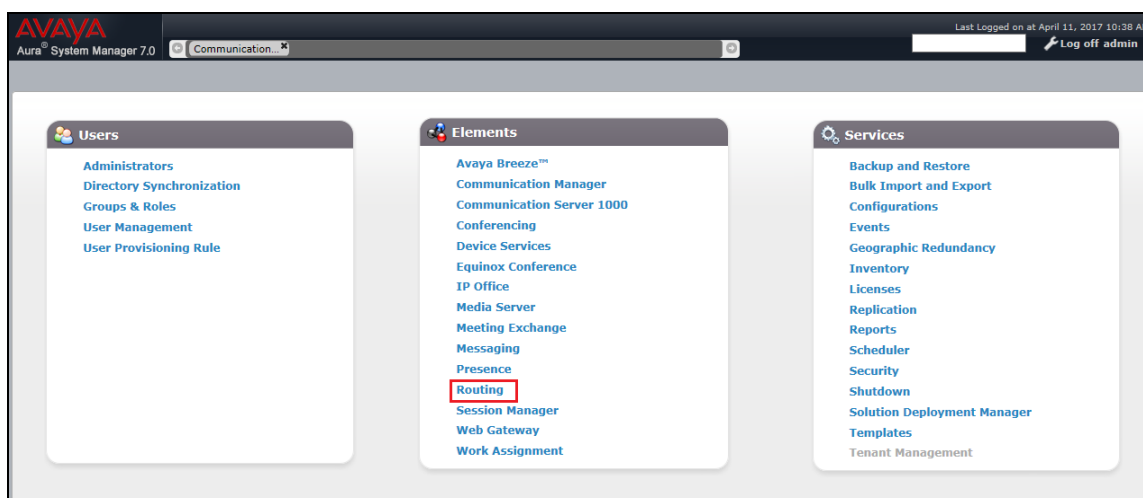
6.1 Log in to Avaya Aura® System Manager

Access System Manager using a Web Browser by entering **http://<FQDN>/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager or **http://<IP Address>/SMGR**. Log in using appropriate credentials.



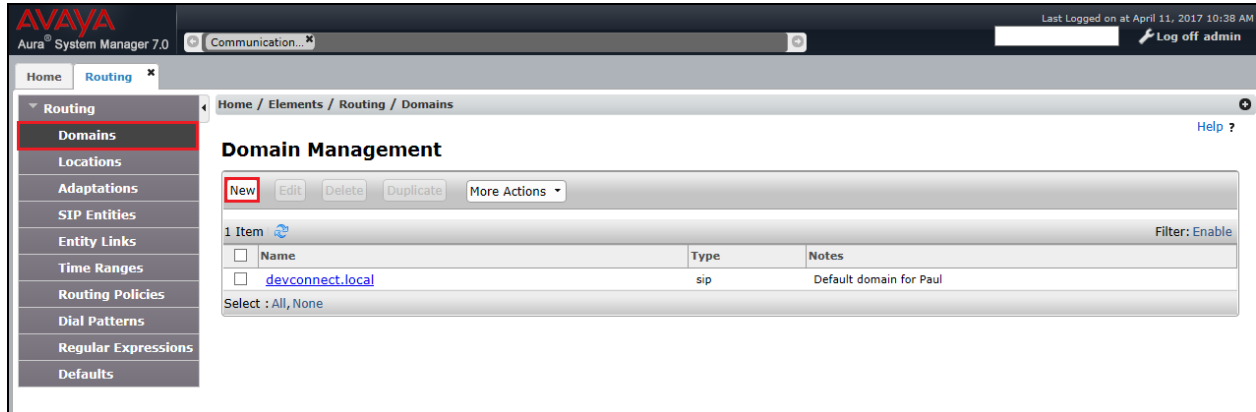
The screenshot shows the Avaya Aura System Manager 7.0 login page. On the left, there is a text box with instructions: "Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases: First time login with 'admin' account, Expired/Reset passwords. Use the 'Change Password' hyperlink on this page to change the password manually, and then login. Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address. This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited. Basically this is Pauls PBX so please go away if you are not Paul." On the right, there is a login form with fields for "User ID" (containing "admin") and "Password" (masked with dots). Below the fields are "Log On" and "Cancel" buttons, and a "Change Password" link. At the bottom, a blue banner states "Supported Browsers: Internet Explorer 11.x or Firefox 43.0, 44.0 and 45.0."

Once logged in click on **Routing** highlighted below.

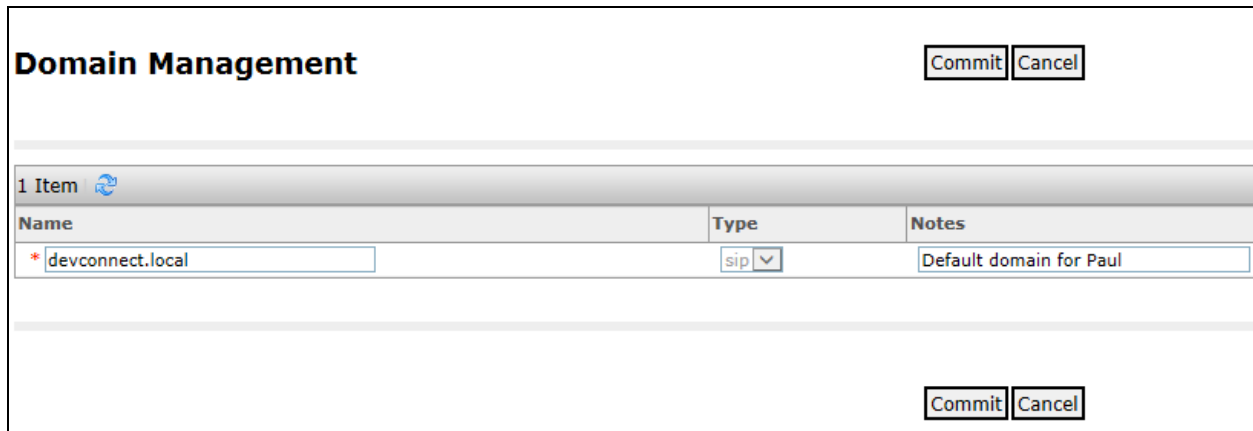


6.2 Administer SIP Domain

Click on **Domains** in the left window. If there is not a domain already configured click on **New** highlighted below.



Note the domain **Name** used in the compliance testing was **devconnect.local**. Note this domain is also referenced in **Section 5.5**. Once the domain name is entered, click on **Commit** to save this configuration.



6.3 Administer Location

If a location is not already in place then one must be added to include the IP address range of the Avaya solution. Click on **New** as is highlighted below to add a new location.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 7.0', and a 'Communication' tab. The left sidebar contains a menu with 'Routing' expanded, showing sub-items like 'Domains', 'Locations' (highlighted with a red box), 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area displays the 'Location' page with a breadcrumb trail 'Home / Elements / Routing / Locations'. Below the breadcrumb, there is a 'Location' title and a 'New' button (highlighted with a red box) along with 'Edit', 'Delete', 'Duplicate', and 'More Actions' buttons. A table below shows one item with columns 'Name', 'Correlation', and 'Notes'. The item is 'PGLAB' with a correlation of 'Pauls Lab'. A 'Filter: Enable' link is also present. At the bottom, it says 'Select : All, None'.

Name	Correlation	Notes
<input type="checkbox"/> PGLAB	<input type="checkbox"/>	Pauls Lab

Enter a suitable **Name** and add the IP address ranges at the bottom of the screen under **Location Pattern** and click on **Commit** once this is done.

Location Details

CommitCancel

General

*

Name:

PGLAB

Notes:

Pauls Lab

Dial Plan Transparency in Survivable Mode

Enabled:

☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

2000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

2000

Kbit/Sec

*

Minimum Multimedia Bandwidth:

64

Kbit/Sec

*

Default Audio Bandwidth:

80

Kbit/sec

Alarm Threshold

Overall Alarm Threshold:

80

%

Multimedia Alarm Threshold:

80

%

*

Latency before Overall Alarm Trigger:

5

Minutes

*

Latency before Multimedia Alarm Trigger:

5

Minutes

Location Pattern

AddRemove

2 Items

☐

IP Address Pattern

Notes

☐

*

10.10.40.*

Pauls subnet

Select : All, None

PG; Reviewed:
SPOC 2/7/2018

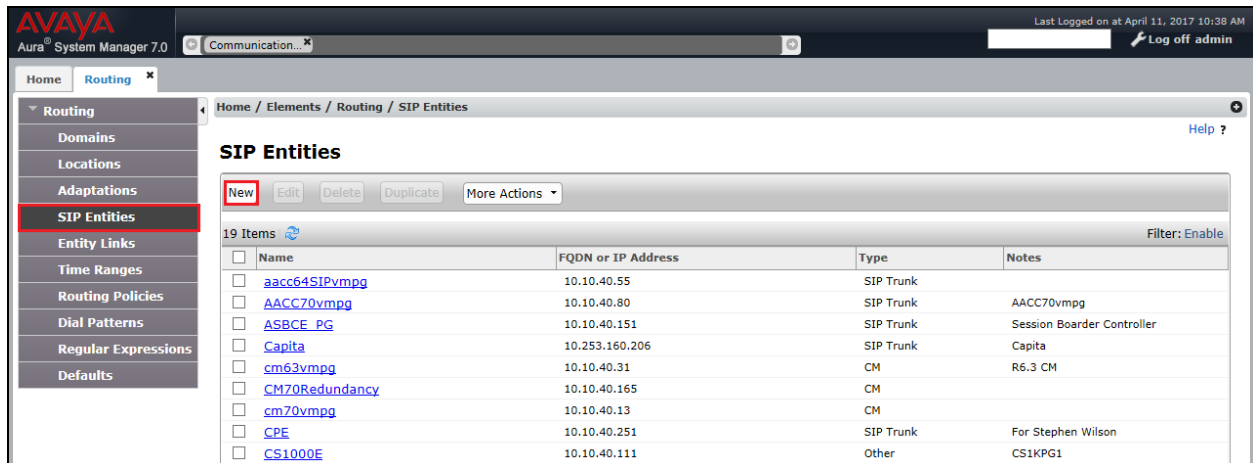
Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

18 of 43
PrOG11SM71CM71

6.4 Configure OpenGate SIP Entity

Each SIP device (other than Avaya SIP Phones) that communicates with Session Manager requires a SIP Entity and Entity Link configuration.

Click on **SIP Entities** in the left column and select **New** in the right window.



AVAYA
Aura® System Manager 7.0

Home / Elements / Routing / SIP Entities

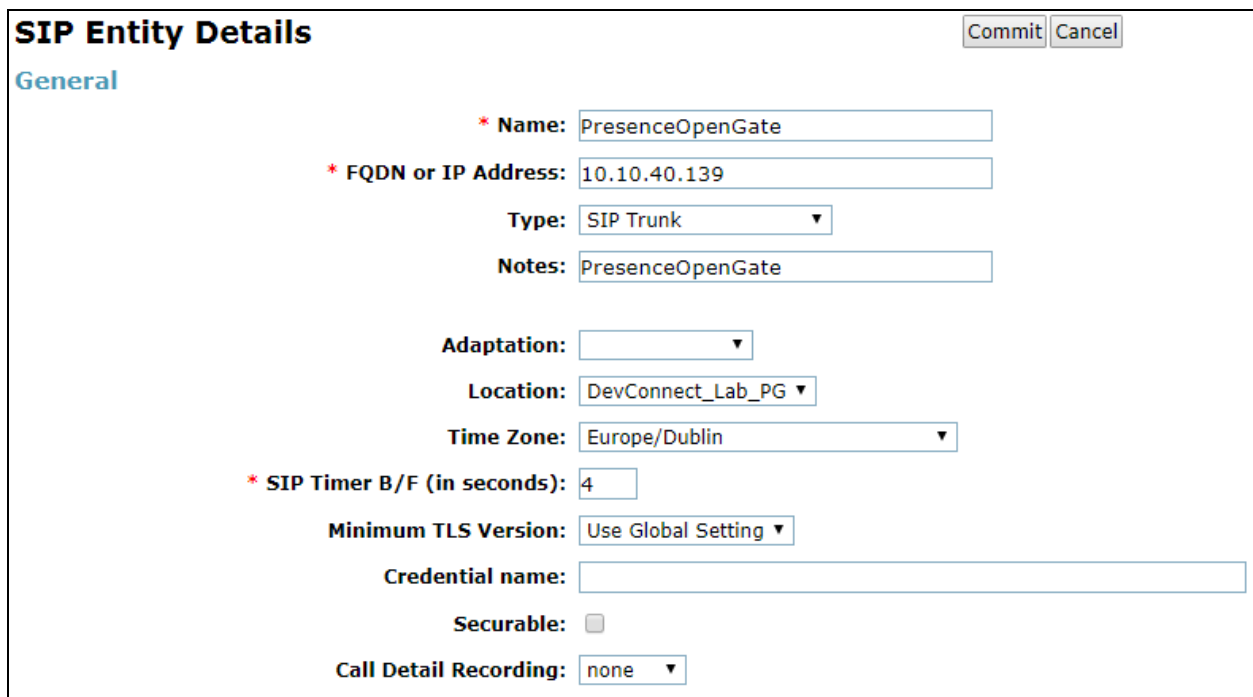
SIP Entities

New Edit Delete Duplicate More Actions

19 Items Filter: Enable

Name	FQDN or IP Address	Type	Notes
aacc64SIPvmg	10.10.40.55	SIP Trunk	
AACC70vmg	10.10.40.80	SIP Trunk	AACC70vmg
ASBCE_PG	10.10.40.151	SIP Trunk	Session Boarder Controller
Capita	10.253.160.206	SIP Trunk	Capita
cm63vmg	10.10.40.31	CM	R6.3 CM
CM70Redundancy	10.10.40.165	CM	
cm70vmg	10.10.40.13	CM	
CPE	10.10.40.251	SIP Trunk	For Stephen Wilson
CS1000E	10.10.40.111	Other	CS1KPG1

Enter a suitable **Name** for the new SIP Entity and the **IP Address** of the OpenGate server. Enter the correct **Time Zone** and **Location** and click on **Commit**.



SIP Entity Details Commit Cancel

General

* Name: PresenceOpenGate

* FQDN or IP Address: 10.10.40.139

Type: SIP Trunk

Notes: PresenceOpenGate

Adaptation:

Location: DevConnect_Lab_PG

Time Zone: Europe/Dublin

* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: none

6.5 Configure OpenGate SIP Entity Link

An Entity Link was added for OpenGate. Click on **Entity Links** in the left column and select **New** in the main window.

Entity Links

New Edit Delete Duplicate More Actions

18 Items Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	aacc64SIPvmppg	sm70vmppg	TCP	5060	aacc64SIPvmppg	<input type="checkbox"/>	5060	trusted	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	AACC70vmppg	sm70vmppg	TCP	5060	AACC70vmppg	<input type="checkbox"/>	5060	trusted	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	ASBCE_TCP	sm70vmppg	TCP	5060	ASBCE_PG	<input type="checkbox"/>	5060	trusted	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	cm63vmppg_TLS	sm70vmppg	TLS	5061	cm63vmppg	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CPE	sm70vmppg	UDP	5060	CPE	<input type="checkbox"/>	5060	trusted	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	CS1000E	sm70vmppg	TCP	5060	CS1000E	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created OpenGate SIP Entity for **SIP Entity 2**. Ensure that **UDP** is selected for the **Protocol** and that **Port 5060** is used. Click on **Commit** once finished to save the new Entity Link.

Entity Links

Commit Cancel

1 Item Filter: Enable

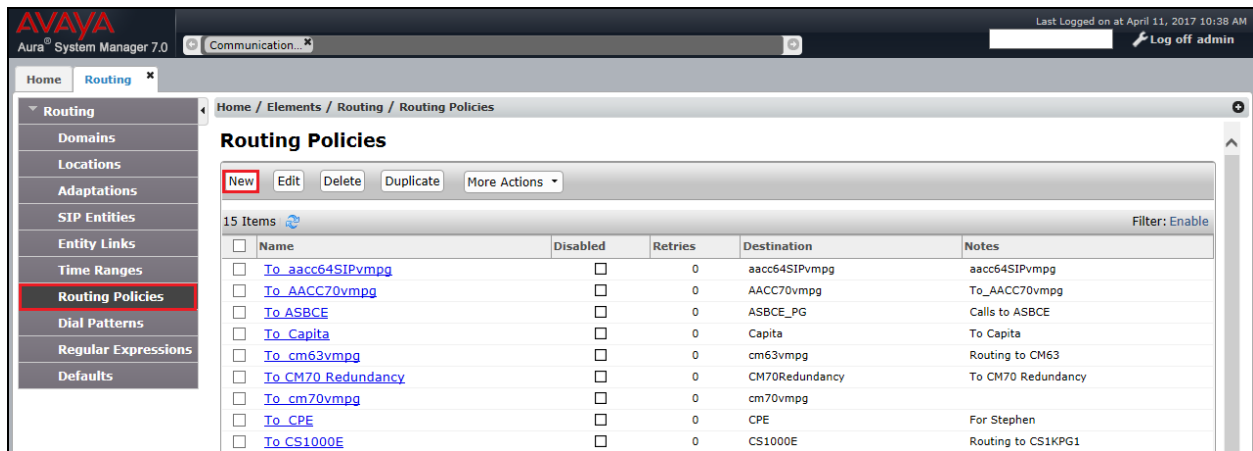
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	D	Ove
<input type="checkbox"/>	* SM_PresenceOG	* SM71vmppg	UDP	* 5060	* PresenceOpenGate	* 5060		

Select : All, None

Commit Cancel

6.6 Configure Routing Policy for OpenGate

Click on **Routing Policies** in the left window and select **New** in the main window.



Enter a suitable **Name** for the Routing Policy and click on **Select** under **SIP Entity as Destination**, highlighted below.

Routing Policy Details Commit Cancel

General

* **Name:**

Disabled: ☐

* **Retries:**

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes

Select the **OpenGate** SIP Entity as shown below and click on **Select**.

SIP Entities

SelectCancel

SIP Entities

9 Items

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	AACC71vmpg	10.10.40.80	SIP Trunk	AACC R7.1
<input type="radio"/>	AAMessagingR633	10.10.40.22	SIP Trunk	AAMessagingR633
<input type="radio"/>	AAMessagingR7	10.10.40.168	SIP Trunk	AAMessaging
<input type="radio"/>	cm70vmpg	10.10.40.13	CM	cm70vmpg
<input type="radio"/>	CM71vmpg	10.10.40.47	CM	CM71vmpg
<input type="radio"/>	CS1KPG1	10.10.40.111	SIP Trunk	CS1000 PG
<input type="radio"/>	MiCC	10.10.40.128	SIP Trunk	Mitel MiCC
<input checked="" type="radio"/>	PresenceOpenGate	10.10.40.139	SIP Trunk	PresenceOpenGate
<input type="radio"/>	SM71vmpg	10.10.40.52	Session Manager	SM71vmpg

Select : None

The selected destination is now shown, click on **Commit** to save this.

Routing Policy Details

CommitCancel

General

* Name:

To_PresenceOG

Disabled:

☐

* Retries:

0

Notes:

To_PresenceOG

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
PresenceOpenGate	10.10.40.139	SIP Trunk	PresenceOpenGate

6.7 Configure OpenGate Dial Patterns

Select **Dial Patterns** in the left window and select **New** in the main window.

Avaya Aura System Manager 7.0

Home / Elements / Routing / Dial Patterns

Dial Patterns

New Edit Delete Duplicate More Actions

17 Items Filter: Enable

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
10	4	4	<input type="checkbox"/>			devconnect.local	Ext 10xx on CM63vmpg
2016	4	4	<input type="checkbox"/>			devconnect.local	SIP Trunk to CM63
3	4	4	<input type="checkbox"/>			devconnect.local	To CS1000E
40	4	4	<input type="checkbox"/>			devconnect.local	Calls to SIP exts in CS1000
450	4	4	<input type="checkbox"/>			devconnect.local	To Capita
49	4	4	<input type="checkbox"/>			devconnect.local	To NovaLink 10.10.40.44
51	4	4	<input type="checkbox"/>			devconnect.local	To Etrali
52	4	4	<input type="checkbox"/>			devconnect.local	Was goign to IP Office 500 V2 Now CM70vmpg
5999	4	4	<input type="checkbox"/>			devconnect.local	Messaging (Voicemail)

Enter the required digits for the Routing Pattern, in the example below **6300** is used. This ensures that when 6300 is dialled it will route to the OpenGate. Enter the appropriate domain for **SIP Domain** in this example the domain created in **Section 6.2** is added. Click on **Add** under **Originating Locations and Routing Policies** in order to select this Routing Policy.

Dial Pattern Details Commit Cancel

General

* Pattern: 6300

* Min: 4

* Max: 4

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: devconnect.local

Notes: To PresenceOpenGate

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes

Select : All, None

Select the Originating Location, this will be the location added in **Section 6.3** select the newly created Routing Policy for OpenGate.

Originating Location
Select Cancel

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item

<input checked="" type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	DevConnect_Lab_PG	DevConnect_Lab_PG

Select : All, None

Routing Policies

8 Items

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To AACC71vmpg	<input type="checkbox"/>	AACC71vmpg	To AACC71vmpg
<input type="checkbox"/>	To_AAMessaging	<input type="checkbox"/>	AAMessagingR7	To_AAMessaging
<input type="checkbox"/>	To AA Messaging R633	<input type="checkbox"/>	AAMessagingR633	To AA Messaging R633
<input type="checkbox"/>	To_cm70vmpg	<input type="checkbox"/>	cm70vmpg	To_cm70vmpg
<input type="checkbox"/>	To_CM71vmpg	<input type="checkbox"/>	CM71vmpg	To_CM71vmpg
<input type="checkbox"/>	To_CS1KPG1	<input type="checkbox"/>	CS1KPG1	To_CS1KPG1
<input type="checkbox"/>	To_MiCC	<input type="checkbox"/>	MiCC	To Mitel MiCC
<input checked="" type="checkbox"/>	To_PresenceOG	<input type="checkbox"/>	PresenceOpenGate	To_PresenceOG

Select : All, None

With the Routing Policy selected click on **Commit** to finish adding the **Dial Pattern**.

Dial Pattern Details
Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	DevConnect_Lab_PG	DevConnect_Lab_PG	To_PresenceOG	0	<input type="checkbox"/>	PresenceOpenGate	To_PresenceOG

Select : All, None

7. Configure Presence Technology OpenGate

OpenGate is part of Presence Suite and is administered via Presence Administrator which resides on the Presence Server. A number of items are set up within Presence Administrator to configure the OpenGate ACD.

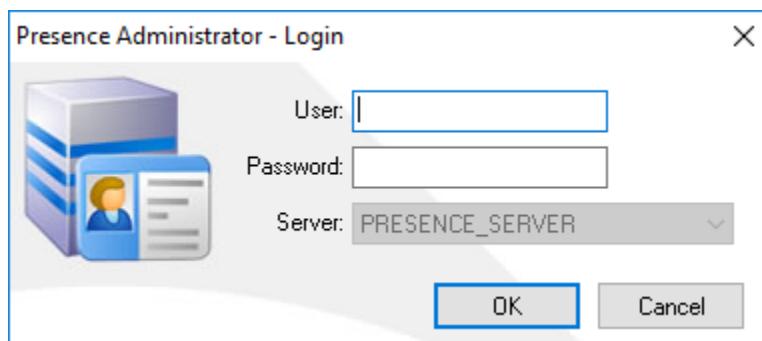
This section will cover the following areas:

- Login to Presence Administrator
- Administer SIP trunk to Avaya Aura® Session Manager
- OpenGate Skill Configuration
- OpenGate Agent Login Configuration
- OpenGate Station Configuration
- OpenGate Service Configuration
- Outbound Routes
- Inbound Routes
- Logging in to OpenGate

Note: The following configuration details for Agent Login and Skillsets are all a part of the Presence OpenGate internal Call Centre and are not referenced anywhere else in these Application Notes.

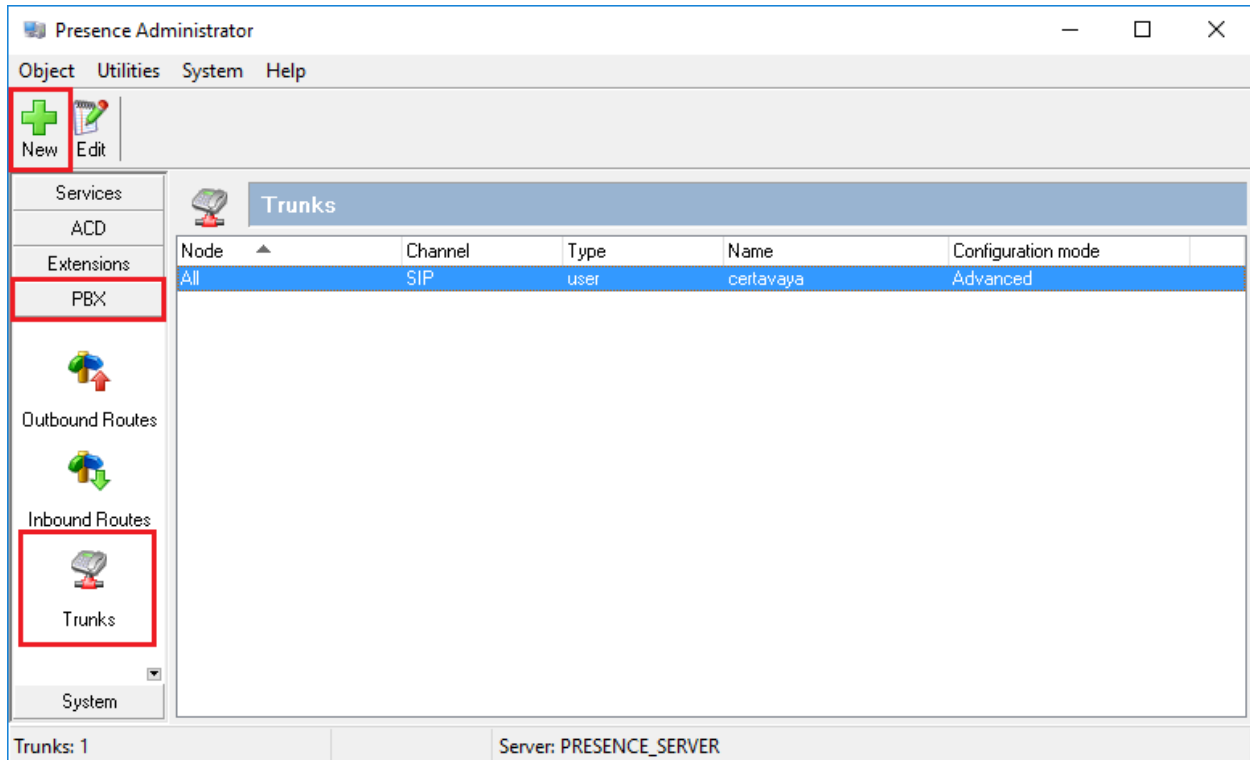
7.1 Login to Presence Administrator

Launch the Presence Administrator application by double clicking the **pcoadmin.exe** icon located in the Presence folder (not shown). The username and password that appear in the **User** and **Password** fields are created during the Presence Server installation.



7.2 Administer SIP Trunk to Avaya Aura® Session Manager

In the left window navigate to **PBX**→**Trunks**. Click on the **New** icon at the top left of the page.



Fill in the information as shown below. Please note that the **Node ogmaster11** has already been established during the install of Presence OpenGate. Select **SIP Peer** as the **Channel** and **Advanced** as the **Mode**. Enter a suitable name for the **User**. Note the following in the main window. Click on **OK** once finished.

- **type = peer**
- **host = IP address of Session Manager**
- **dtmfmode = rfc2833**
- **context = presence-inbound**
- **canreinvite = no**
- **allow = all**

New trunk

Node: ☒ All ☐ ogmaster11

Channel: SIP Peer

Mode: Advanced

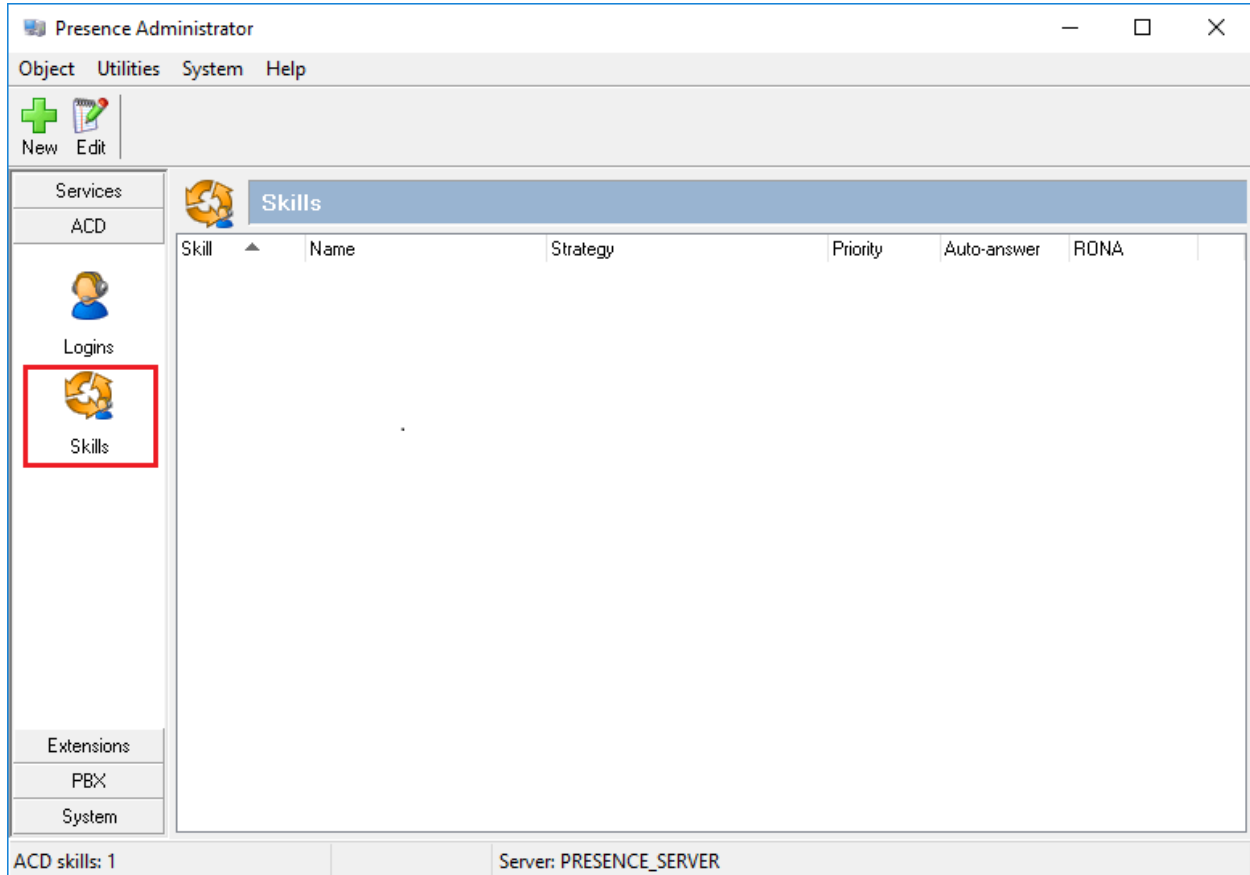
User: certavaya

type=peer
host=10.10.40.52
dtmfmode=rfc2833
context=presence-inbound
canreinvite=no
allow=all

OK Cancel **Apply**

7.3 OpenGate Skill Configuration

To configure a skill, from the left hand side select **ACD** → **Skills** from the Presence Administrator main menu. Click the **New** button.



In the resulting screen, define a **Skill** number and enter a **Name** to identify the skill. In the **Strategy** field, use the two drop down menus to define the selection strategy that will be used by the skill. Set a **Priority** for the skill. All remaining fields can be left with default values. Click **OK** to save the configuration.

Edit skill

☒ General
☐ Logins

Skill: 80000

Name: 80000

Strategy: Skill level measurement Agent available the longest

Priority: 1

RONA: 0 seconds

☐ Answer calls automatically (auto-answer)

OK Cancel Apply

7.4 OpenGate Agent Login Configuration

The login configured here will be used by the agent to login to OpenGate. The Agents will connect to OpenGate via the Presence Suite Agent application. To configure an ACD agent login, from the left hand side select **ACD** → **Logins** from the Presence Administrator main menu. Click the **Add** button.

Presence Administrator

Object Logins Utilities System Help

Group Login Edit Enable Disable Add Remove

Services

ACD

Logins

Skills

Extensions

PBX

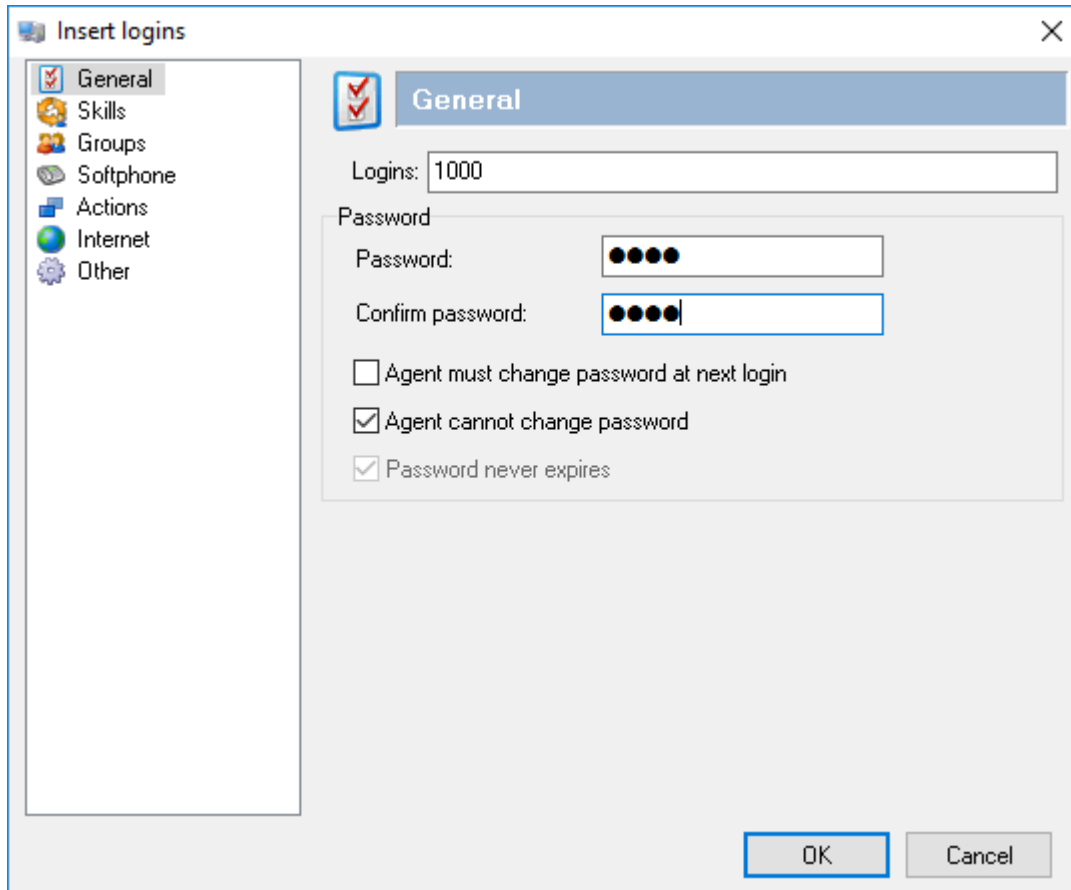
System

Logins

Login	Name	Softphone	CallerID
[All]			

Group: [All] Logins: 0 Server: PRESENCE_SERVER

From the menu on the left side of the screen, select **General**, and enter a numerical ID in the **Logins** field. Define a **Password** for the agent login and repeat in the **Confirm Password** field.



The screenshot shows a Windows-style dialog box titled "Insert logins". On the left is a tree view with icons and labels: General (checked), Skills, Groups, Softphone, Actions, Internet, and Other. The main area is titled "General" and contains the following fields and options:

- Logins:** A text box containing the value "1000".
- Password:** A text box containing four black dots.
- Confirm password:** A text box containing four black dots.
- ☐ Agent must change password at next login
- ☒ Agent cannot change password
- ☒ Password never expires

At the bottom right are "OK" and "Cancel" buttons.

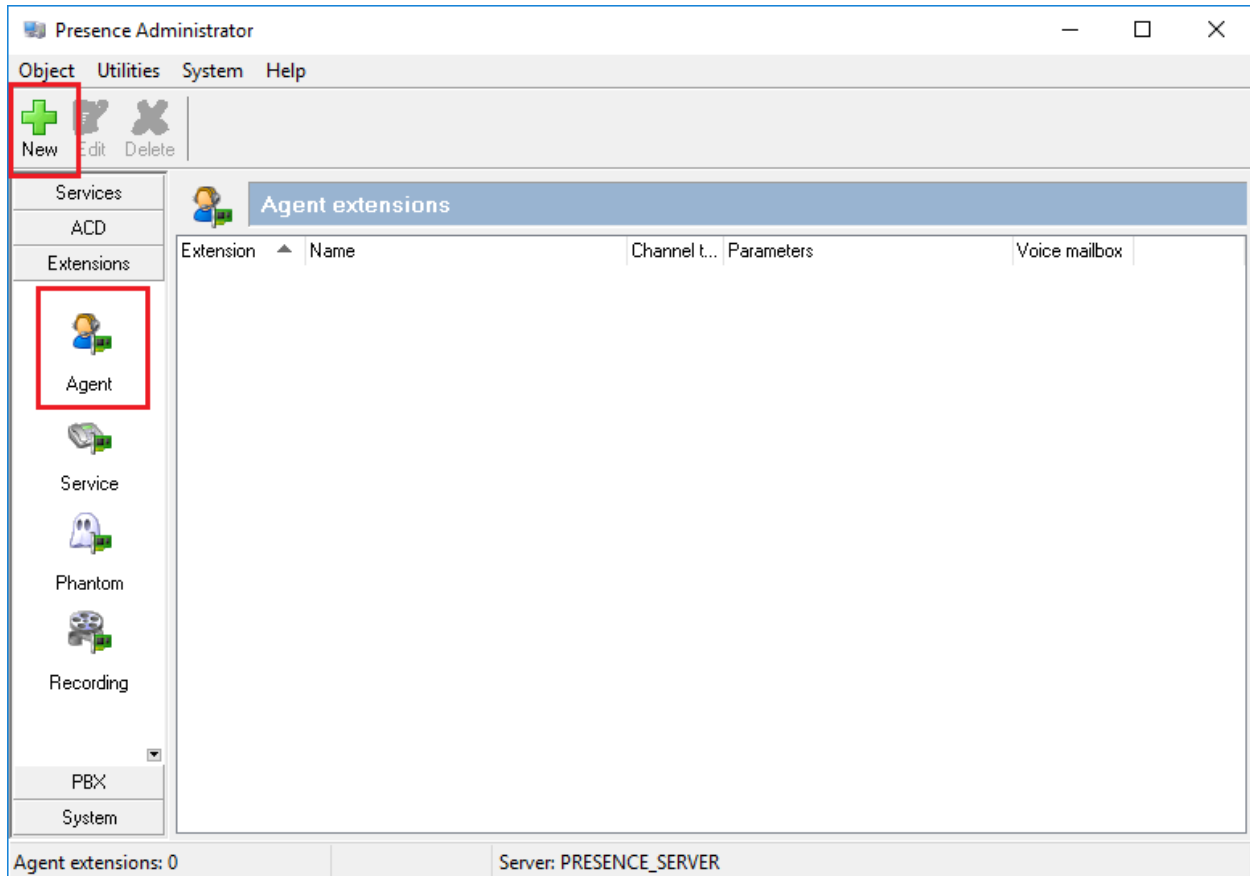
From the menu on the left side of the screen select **Skills**, use the drop down menu to select the **Skill** configured in **Section 7.3** and specify a **Level** for the skill to be applied against this agent login. Click the **Add** button and the skill should appear under **Assigned skills**. Click **OK** to save the login configuration.

The screenshot shows a software window titled "Insert logins" with a close button (X) in the top right corner. On the left is a vertical menu with icons and labels: "General" (checked), "Skills" (selected), "Groups", "Softphone", "Actions", "Internet", and "Other". The main area is titled "Skills" and contains a "Skill" dropdown menu showing "80000 - 80000", a "Level" text input field, and an "Add" button. Below this is a section labeled "Assigned skills" containing a table with two columns, "Name" and "Level". At the bottom right of the table area is a "Remove" button. At the very bottom of the dialog are "OK" and "Cancel" buttons.

Name	Level
------	-------

7.5 Presence Technology OpenGate Station Configuration

Each telephone/endpoint that OpenGate can route calls to must be defined within Presence Administrator as an Agent extension. To define an Agent extension, from the left hand side navigate to **Extensions** → **Agents** and click the **New** button.



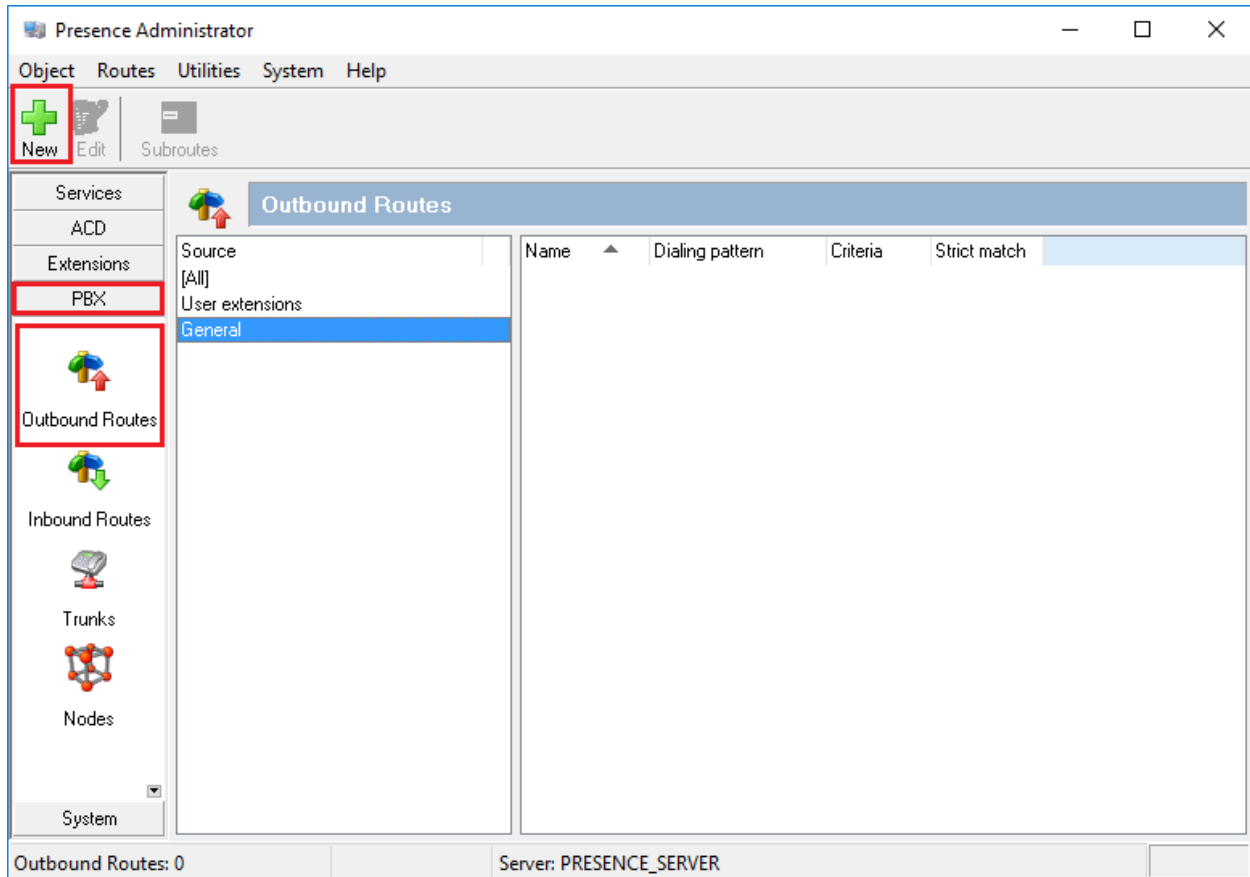
In the resulting screen specify, an **Extension** number that will be used by the Presence Agent application. Note that this number is an existing extension number on Communication Manager. Set a **Name** that the Agent extension will be known as. The password is not required in this case. In the **Channel** field, use the drop down arrow to select **SIP**. In the following field, define the number that will be dialed and the route used to reach the station. For this test, **certavaya/4000** is configured, this will use trunk “certavaya” to route the call. Note **certavaya** is the SIP Trunk configured in **Section 7.2** above.

The screenshot shows a dialog box titled "Add agent extensions" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

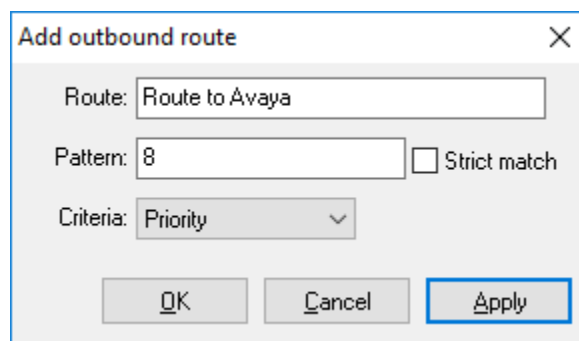
- Extension:** A text input field containing "4000".
- Name:** A text input field containing "4000".
- Password:** A text input field with four black dots, indicating a masked password. To its right is a checkbox labeled "Use extension as password", which is currently unchecked.
- Channel:** A dropdown menu showing "SIP". To its right is a text input field containing "certavaya/4000".
- Voice mailbox:** A dropdown menu with a downward arrow.
- Timeout:** A numeric input field showing "25" with up and down arrows, followed by the text "seconds".
- Buttons:** At the bottom right are three buttons: "OK", "Apply" (which is highlighted with a blue dashed border), and "Cancel".

7.6 Outbound Routes

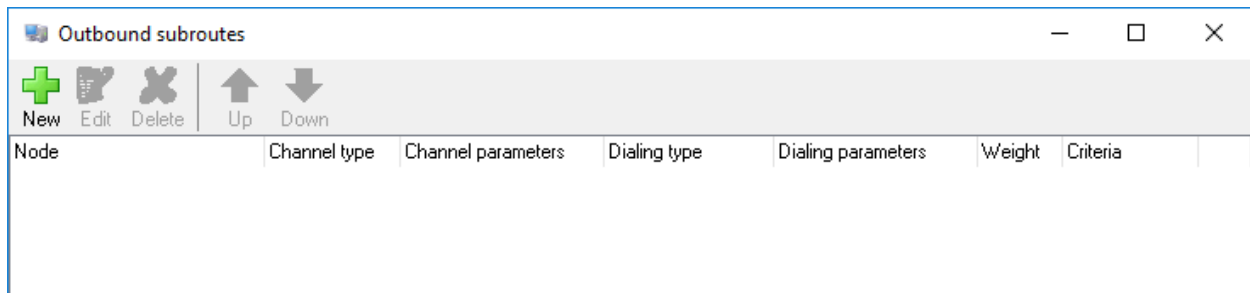
To define an outbound route, from the left hand side navigate to **PBX → Outbound Routes** and click the **New** button.



In the resulting screen, enter a descriptive name in the **Route** field and in the **Pattern** field define any prefix required by outbound calls. This setup is only used for internal working of OpenGate and is not related to routing calls on Communication Manager. For **Criteria** use the drop-down menu to select the method that will be used to distribute calls among the subroutes configured in the next step. **Priority** was chosen for compliance testing. Click **OK** to save the **outbound route**.



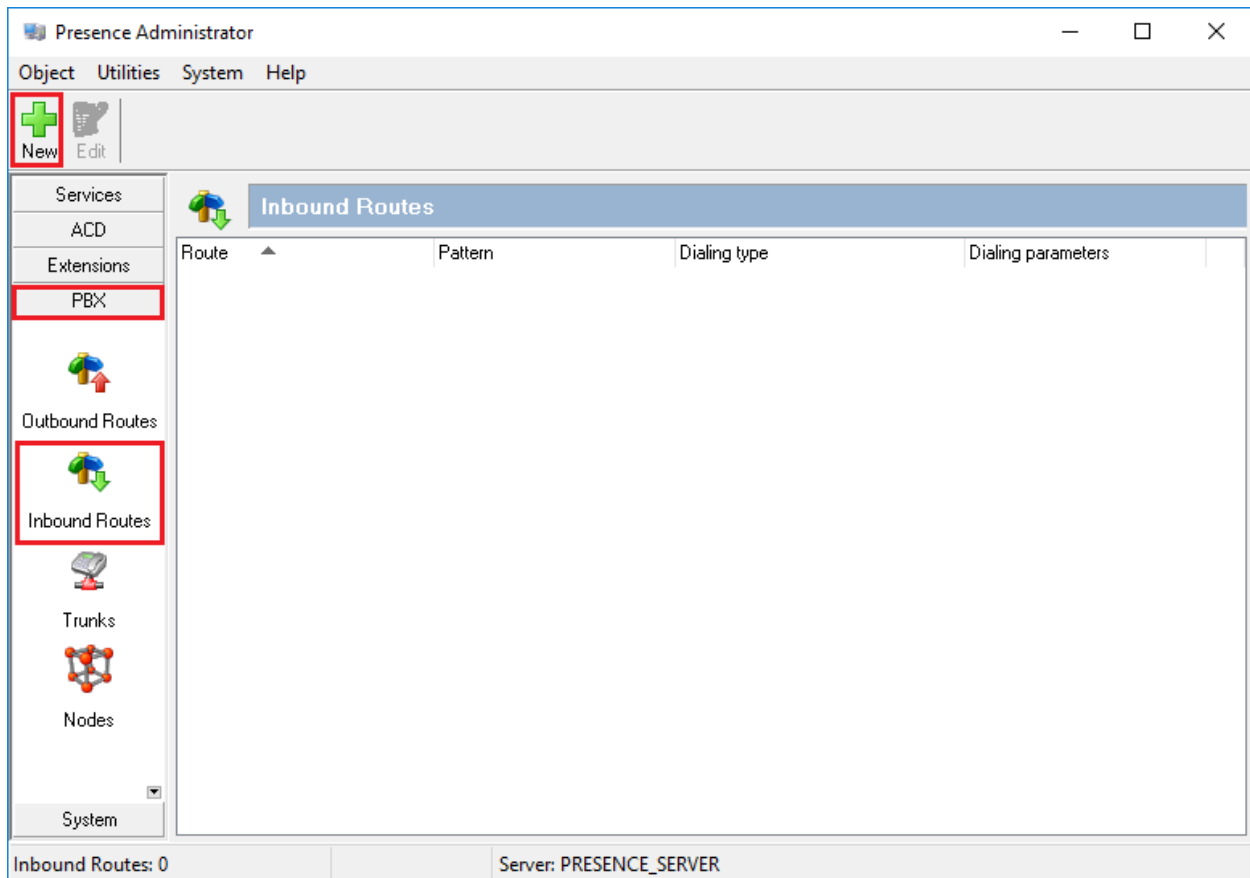
To add an outbound subroute, from the outbound routes main page shown above, highlight the outbound route that was added in the previous step and click the subroutes button at the top of the screen. The **Outbound subroutes** window is then displayed as shown below, Click **New**.



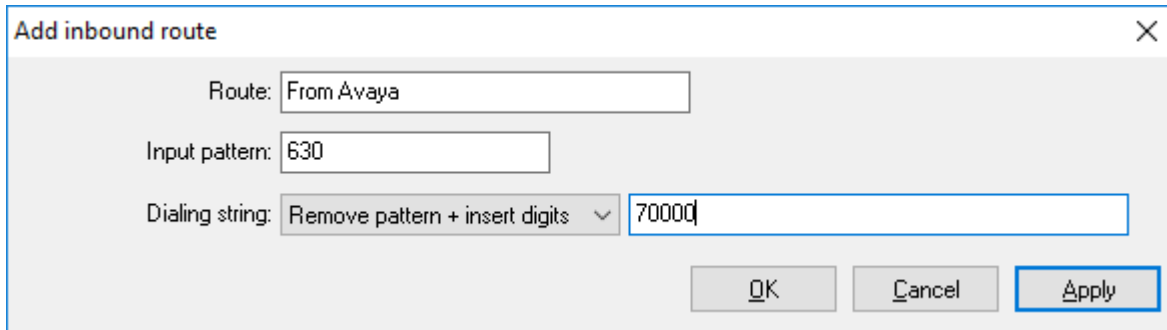
In the resulting window, select the relevant **Node** (**ogmaster11**, created during the OpenGate install), and under **Channel** select **SIP**. For **Dialing string** use the drop down menu to select **Remove Dial Pattern** leaving the secondary field blank. This informs OpenGate to remove the “8” used to define the pattern (also created during the OpenGate install) before routing the call via the **certavaya** trunk.

7.7 Inbound Routes

Inbound routes are used to map dialed numbers received to internal extensions within OpenGate. To define an inbound route, from the left hand side navigate to **PBX → Inbound Routes** and click the **New** button.



In the resulting window enter a descriptive name for **Route**. In this example any calls beginning with 630x will route to **70000** (this is simply internal routing for OpenGate).

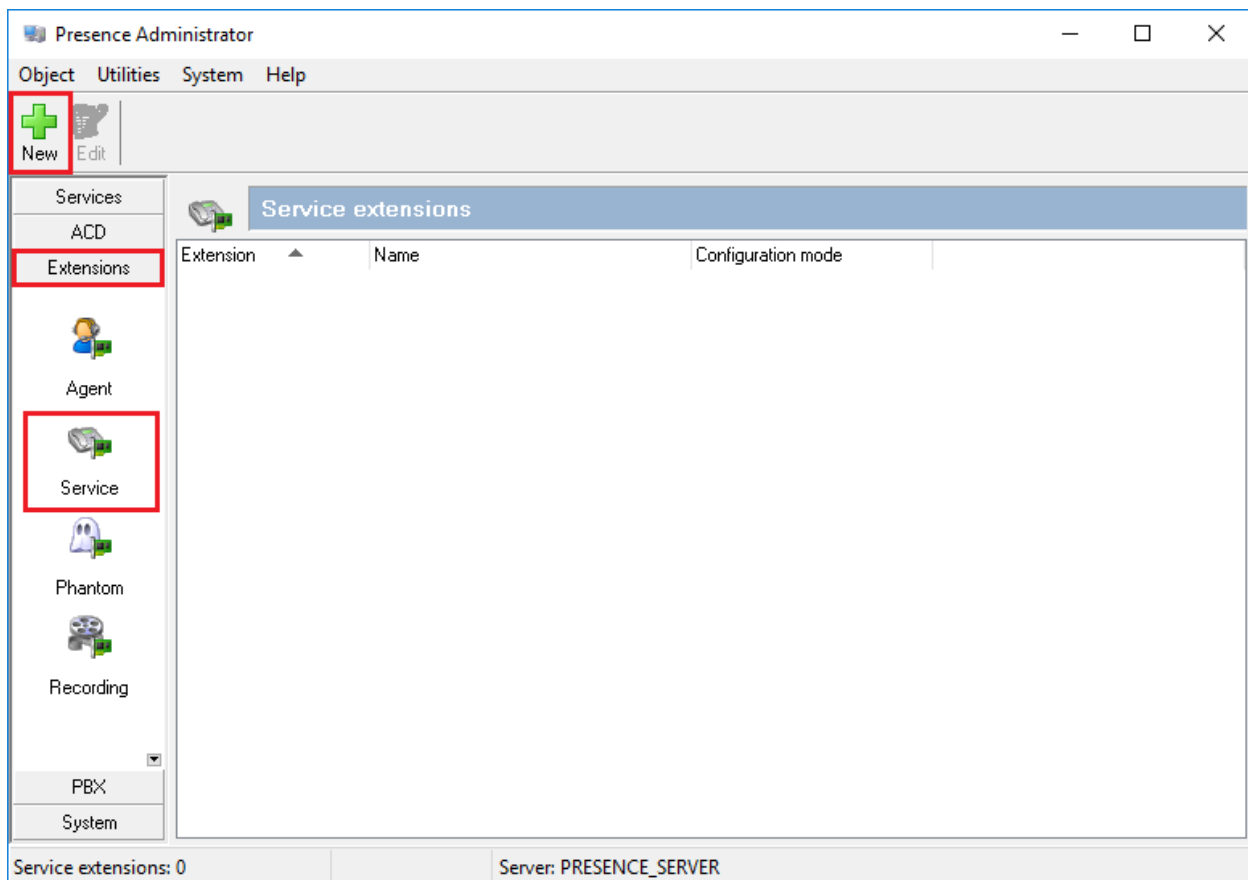


The 'Add inbound route' dialog box contains the following fields and controls:

- Route:** Text field containing 'From Avaya'.
- Input pattern:** Text field containing '630'.
- Dialing string:** A dropdown menu set to 'Remove pattern + insert digits' and a text field containing '70000'.
- Buttons:** 'OK', 'Cancel', and 'Apply' buttons at the bottom right.

7.8 Service Extension

Open Gate uses service extensions to direct calls to services. To define a service extension, from the left hand side navigate to **Extensions** → **Service** and click the **New** button.



In the resulting windows enter the extension number in the **Extension** field and give it a descriptive name in the **Name** field. Select the **Basic** mode under **Mode** and select **Skill** create in **Section 7.4**.

Add service extension [X]

Extension: Name:

Mode:

Ringback: seconds

☐ Enable adjunct routing

Welcome:

Skill: Priority:

Wait:

Music: ☐ Play music on hold before speech

Wait time: seconds

☐ Repeat loop

7.9 Presence Agent Configuration

The following steps are carried out on the Presence Agent PC. Prior to installing the Presence agent, ensure that the DBExpress driver (dpexpoda.dll) is located in the C:\Windows\System32 directory. If not, contact Presence Technology support outlined in **Section 2.3** of these Application Notes. The DBExpress driver allows the agent application to communicate with the Presence Suite/OpenGate database.

Launch the **Presence Agent Configuration** application by double clicking the **pcoagentcfg.exe** located in the C: \Presence folder (not shown). Enter the **Presence Server IP address** as **10.10.40.138**. The **Presence Server port** can be left as the default value of **6100**. Enter the extension of the station that will be used with this workstation in the **Agent station** field. Check the **Hang up calls before logging in** check box is not selected. In the field **Use settings for** choose **Machine** from the drop down menu. Click **OK**. This step is needed for each agent configured; only the agent station field will vary.

The screenshot shows the 'Presence Agent Configuration' dialog box with the 'General' tab selected. The 'General' tab is highlighted in the left sidebar and the top of the main content area. The 'Presence Server' section contains two text boxes: 'IP address' with the value '10.10.40.138' and 'Port' with the value '6100'. The 'Station configuration' section contains a text box for 'Agent station' with the value '4000'. Below this are two checkboxes: 'Hang up calls before logging in' (unchecked) and 'Ask agent station at login window' (checked). At the bottom of the configuration area is a dropdown menu labeled 'Use settings for:' with 'Current user' selected. The dialog box has 'OK' and 'Cancel' buttons at the bottom right.

Field	Value
Presence Server IP address	10.10.40.138
Presence Server Port	6100
Agent station	4000
Hang up calls before logging in	<input type="checkbox"/>
Ask agent station at login window	<input checked="" type="checkbox"/>
Use settings for	Current user

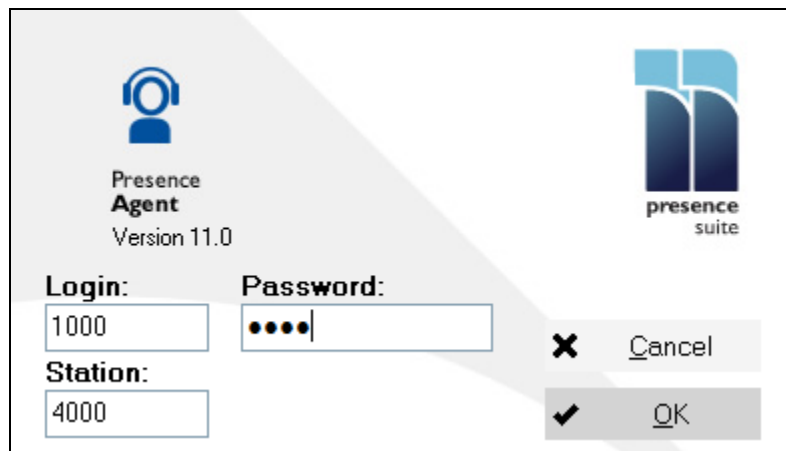
8. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

8.1 Logging into OpenGate

In order to receive calls from Open Gate, users must log in to the system via the Presence Agent application. This section describes the steps required to connect to OpenGate as an agent to receive ACD calls.

Launch the Presence agent configuration application by double clicking the **pcoagent.exe** located in the Presence folder. Enter the agent **Login** and **Password** configured in **Section 7.4** and click on **OK**.



A task bar is present at the top of the Agent PC. Click on the green arrow to put the agent into an available state.



The information status on the task bar goes to **Available** indicating the agent is ready to receive calls.



8.2 Verify SIP Entity is up

From System Manager Home Tab, click on Session Manager and navigate to **Session Manager** → **System Status** → **SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.

Note: The screen below serves as an example of what a successful connection should resemble.

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: SM1676

Summary View

Status Details for the selected Session Manager:

12 Items | Refresh

Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	CM1627	10.10.16.27	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	MSG1689	10.10.16.89	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	PresOG	10.10.16.130	5060	UDP	FALSE	UP	200 OK	UP
<input type="radio"/>	CS1kPG	10.10.40.111	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	AMS1616	10.10.16.16	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	CM1623	10.10.16.23	5060	TCP	FALSE	UP	200 OK	UP

From the Communication Manager SAT interface, run the command **status trunk *n*** where ***n*** is a previously configured SIP trunk. Observe if all channels on the trunk group display **in service/ idle**.

status trunk 1			
TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports
Busy			
0005/001	T00001	in-service/idle	no
0005/002	T00007	in-service/idle	no
0005/003	T00008	in-service/idle	no
0005/004	T00009	in-service/idle	no
0005/005	T00010	in-service/idle	no

9. Conclusion

These Application Notes describe the configuration steps required for Presence Technology OpenGate R11.0 to successfully interoperate with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Session Manager R7.1. All functionality and serviceability test cases were completed successfully.

10. Additional References

This section references the Avaya and Presence Suite product documentation that are relevant to these Application Notes.

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

[1] *Administering Avaya Aura® Communication Manager* – Release 7.1

[2] *Administering Avaya Aura® Session Manager* – Release 7.1

The following documentation is available on request from Presence: www.presenceco.com

[1] *ACD Sys Presence Administrator Manual Presence Suite*, V11.0

[2] *Presence Installation Guides Presence Software*, V11.0

[3] *PBX/ACD Requirements Presence Software*, V11.0

©2018 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.