Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 to interoperate with Presence Technology OpenGate R10.0 – 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.

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 R10.0 can successfully interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3. 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.

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.

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 focus of the interoperability test is the ACD functionality offered by OpenGate. OpenGate replaces the Avaya Aura® Application Enablement Services requirement for a CTI connection to Communication Manager by utilizing a SIP connection to Session Manager routing calls to the Communication Manager handsets. For the sample configuration discussed in this document, all calls are received from the PSTN by Communication Manager and 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.

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. The setup of Presence Suite is outside the scope of these Application Notes; please refer to **Section 10** in order to find information for the configuration of Presence Server.

In the sample configuration described by these Application Notes, calls will be accepted from the PSTN and routed to OpenGate on digits 43xxxx, 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. An Avaya S8800 Server running 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.

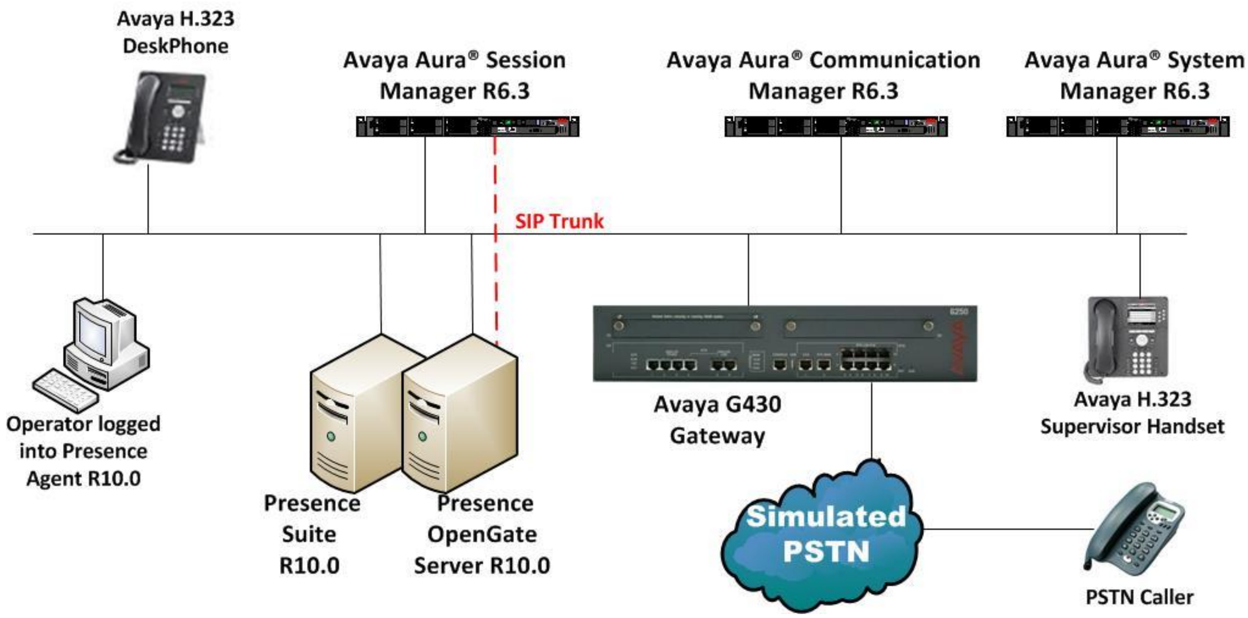


Figure 1: Network Topology used to test Presence Technology Presence OpenGate R10 with Avaya Aura® Session Manager R6.3

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 Avaya S8800 Server	System Manager 6.3.0 - FP2 Build No. - 6.3.0.8.5682-6.3.8.1814 Software Update Revision No: 6.3.3.5.1719
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.3 SP1 R016x.03.0.124.0
Avaya Aura® Session Manager running on Avaya S8800 Server	Session Manager R6.3 (SP3) SM 6.3.3.0.633004
Avaya G430 Gateway	R6.3
Avaya 96xx Series Deskphone	96xx H.323 Release 3.1 SP2
Presence Suite running on Windows Server 2008 SP2	R10.0
Presence OpenGate Server running on Windows Server 2008 SP2	R10.0

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**. 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 **Maximum Administered SIP Trunks** has 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
                                                       Uniform Dialing Plan? y
                     Private Networking? 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 Attd-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 beginning with 43 with a total length of 6 digits were to be sent across the SIP trunk to Session Manager and therefore to OpenGate. In order to achieve this automatic alternate routing (aar) would be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this.

Type **change dialplan analysis** in order to make changes to the dial plan. Ensure that **43** is added with a **Total Length** of **6** and a **Call Type** of **udp**.

```
change dialplan analysis                                       Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 2

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   2           4   ext
   3           4   ext
   43          6   udp
   5           4   ext
   6           4   ext
   7           3   dac
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   fac
```

5.4 Administer Route Selection for OpenGate Calls

As digits **43**xxxx were defined in the dial plan as udp (**Section 5.3**) use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **43** that are **6** digits in length will be matched. No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

```
change uniform-dialplan 8                                        Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                               Percent Full: 0

  Matching                    Insert              Node
  Pattern       Len Del       Digits      Net Conv Num
  43             6   0                    aar  n
                                               n
```

Use the **change aar analysis** command to further configure the routing of the dialed digits. Calls to OpenGate begin with **43** 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 85                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

    Dialed                  Total      Route    Call   Node  ANI
    String                 Min  Max   Pattern   Type   Num   Reqd
    43                     6    6      1        unku         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**.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: SIPTRK
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 1    0                                                               n   user
 2:                                                                      n   user
 3:                                                                      n   user
 4:                                                                      n   user
 5:                                                                      n   user
 6:                                                                      n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                  Dgts Format
                                                          Subaddress
 1: y y y y y n  n            unre                                           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
 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 the Session Manager (**SM63vmpg**). 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
AES63VMPG           10.10.40.30
PGDECT              10.10.40.50
SM63vmpg            10.10.40.34
default             0.0.0.0
procr               10.10.40.31
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                                       Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: devconnect.local
    Name: Default region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

In the **IP Codec Set** form, select the audio codec's 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.729**, **G.711MU** (mu-law) and **G.711A** (a-law), which are supported by OpenGate.

```
change ip-codec-set 1                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 1

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

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) Note, for compliance testing this was set to tls.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above.
- 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 **SM63vmpg**), as per **Section 5.5**.
- 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.
- Leave the **Far-end Domain** field blank to allow Communication Manager to accept any domain.
- 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? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                  Far-end Node Name: SM63vmpg
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain:
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

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: SIP TRK                   COR: 1        TN: 1        TAC: *11
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                 Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 1
                                                    Number of Members: 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. Session refresh is used throughout the duration of the call, to check the other side has not gone away, 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
```

Settings on **Page 3** can be left as default.

```
change trunk-group 1                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


                                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? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  Network Call Redirection? n

                                     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? y
                                              Enable Q-SIP? n
```

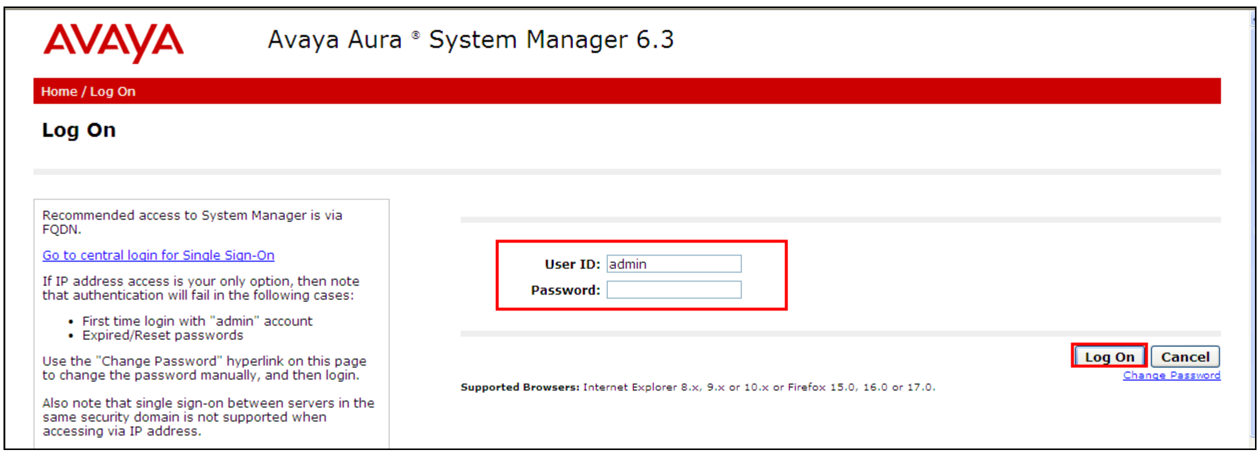
6. Configuring Avaya Aura® Session Manager

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.

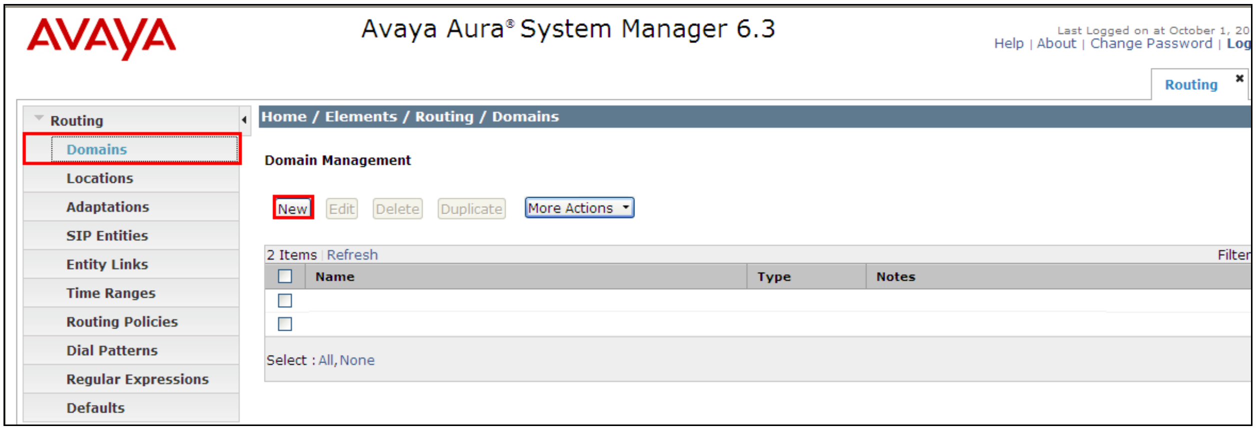
6.1 Log in to Avaya Aura® System Manager

Access the 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 Adddress >/SMGR**. Log in using appropriate credentials.

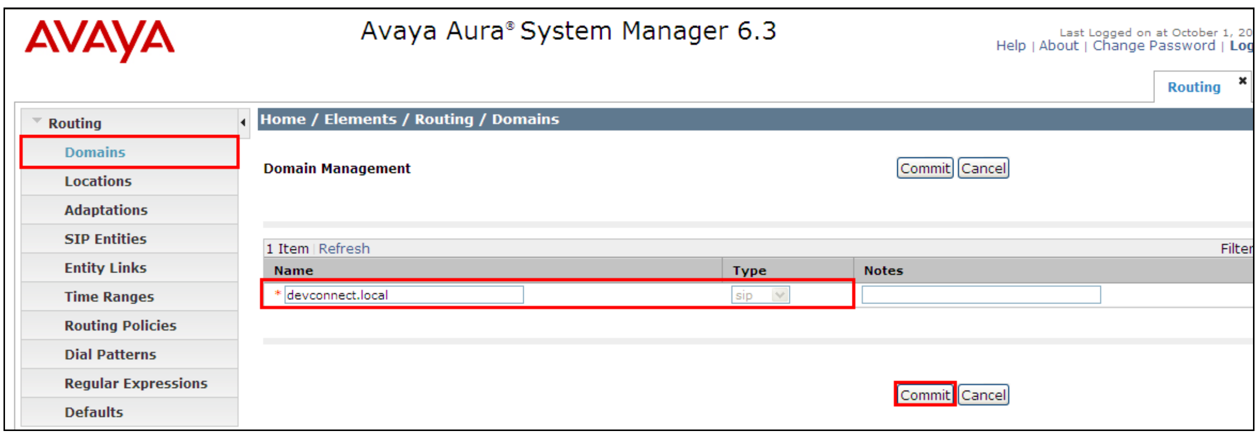


6.2 Administer SIP Domain

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

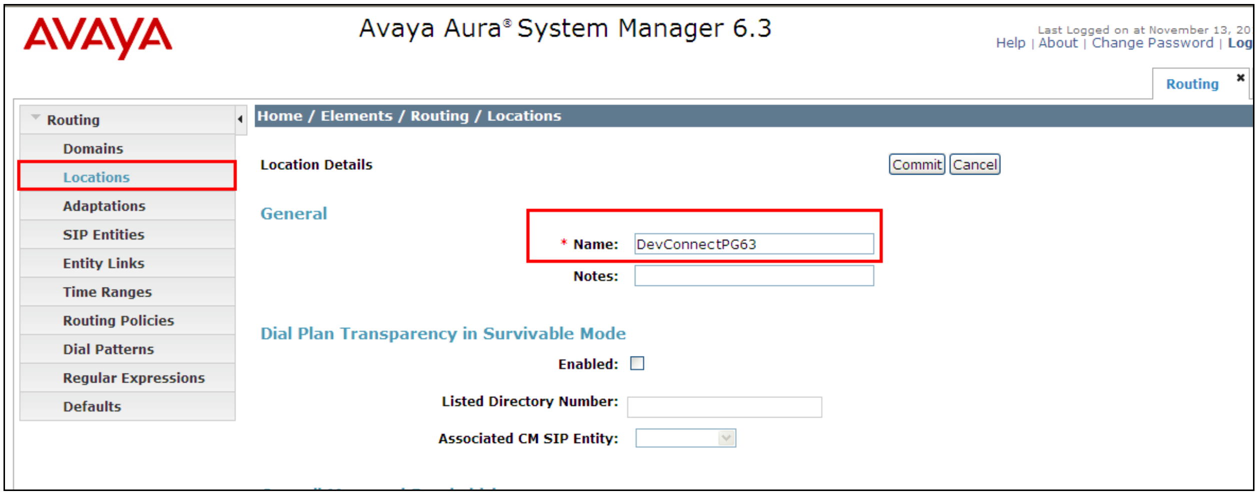


Note the domain **Name** used in the compliance testing was **devconnect.local**. Note this domain is also referenced in **Section 5.5**. Once the domain name is entered click on **Commit** to save this.

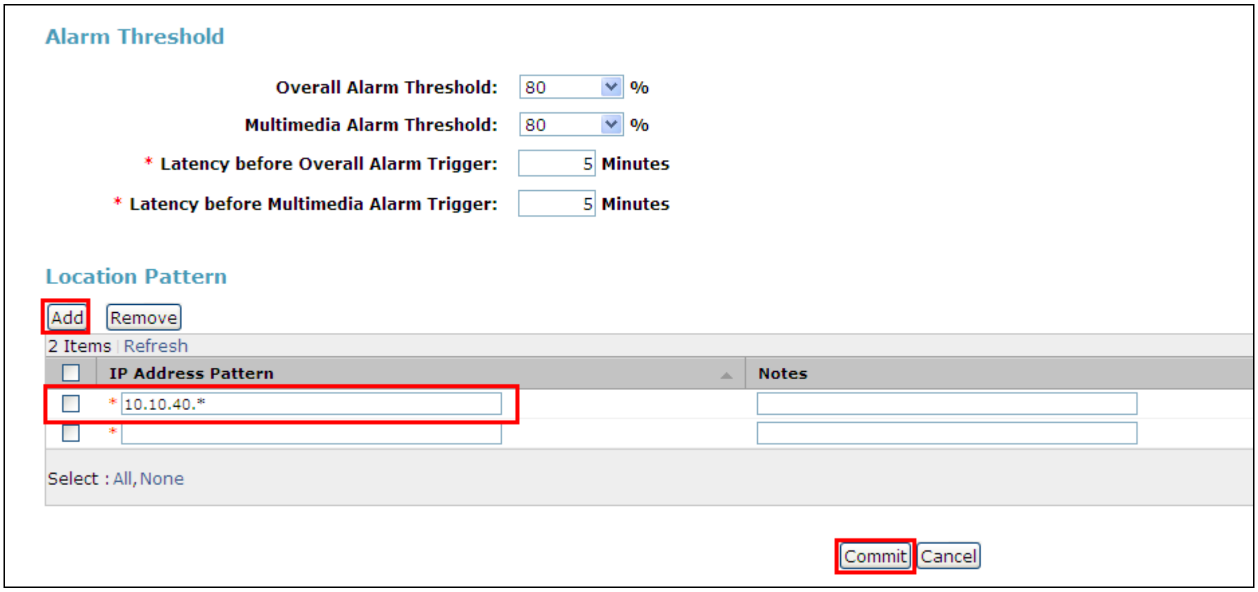


6.3 Administer Location

Session Manager uses the origination location to determine which dial patterns to look at when routing a call. In this example, one Location has been created which will reference both the Session Manager location and the OpenGate location. Navigate to **Home → Elements → Routing → Locations → New** enter an identifying **Name**, as shown below.



At the bottom of the same page the **Location Pattern** is defined. Click **Add** and enter the IP address range used to logically identify the location. In this case the **IP Address Pattern** is **10.10.40.*** as shown below. Click **Commit** when done.

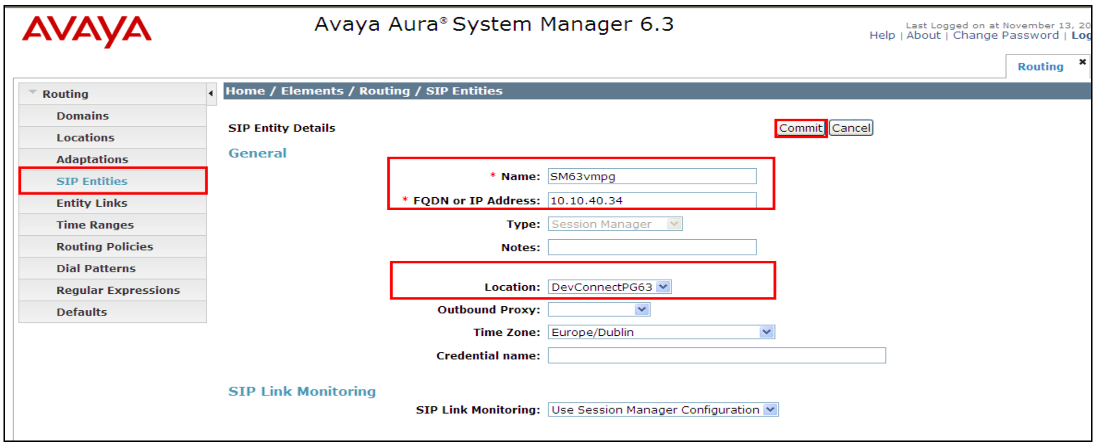


6.4 Administer SIP Entities

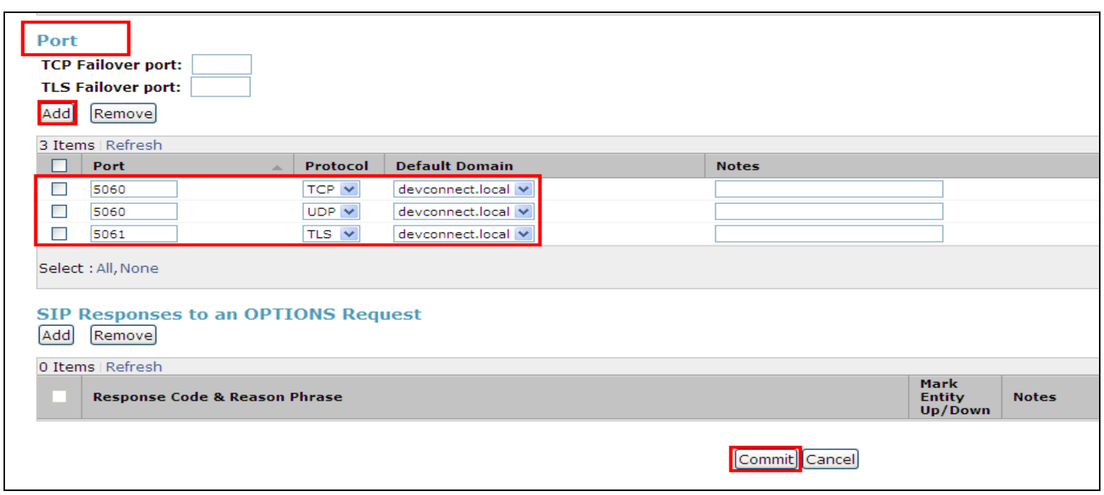
Each SIP device (other than Avaya SIP Phones) that communicates with Session Manager requires a SIP Entity configuration. This section details the steps to create SIP Entities for Session Manager SIP Signaling Interface, Communication Manager and OpenGate Solution respectively.

6.4.1 Configure Session Manager SIP Signaling Interface Entity

Click **Home** → **Elements** → **Routing** → **SIP Entities** → **New** assign an identifying **Name**, the **FQDN or IP Address** for Session Manager SIP Signaling Interface, set the **Type** to **Session Manager** and the **Location** to the Location configured in **Section 6.3** and click on **Commit**.

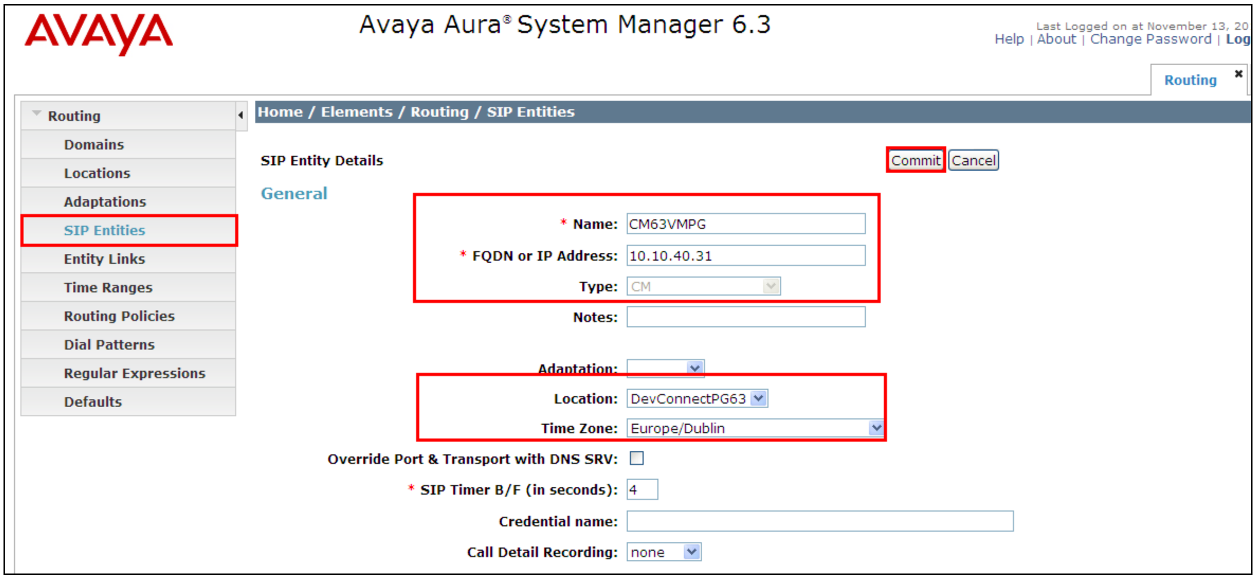


A signaling configuration is created for Session Manager allowing third party devices to connect using permitted protocols. Tick the box next to the entity that was just created and click **Edit** (not shown**)**. Scroll down the page until the **Port** section is displayed, click **Add** and configure the **Port** as **5060** the **Protocol TCP** and the **Default Domain** as the domain configured in **Section 6.2** this corresponds with the signaling group configured in **Section 5.3.** Repeat this for the **UDP** connection which will be established to the OpenGate server, as shown below **TLS** is shown below but was not used in the connection to the OpenGate server. Click **Commit** when done.



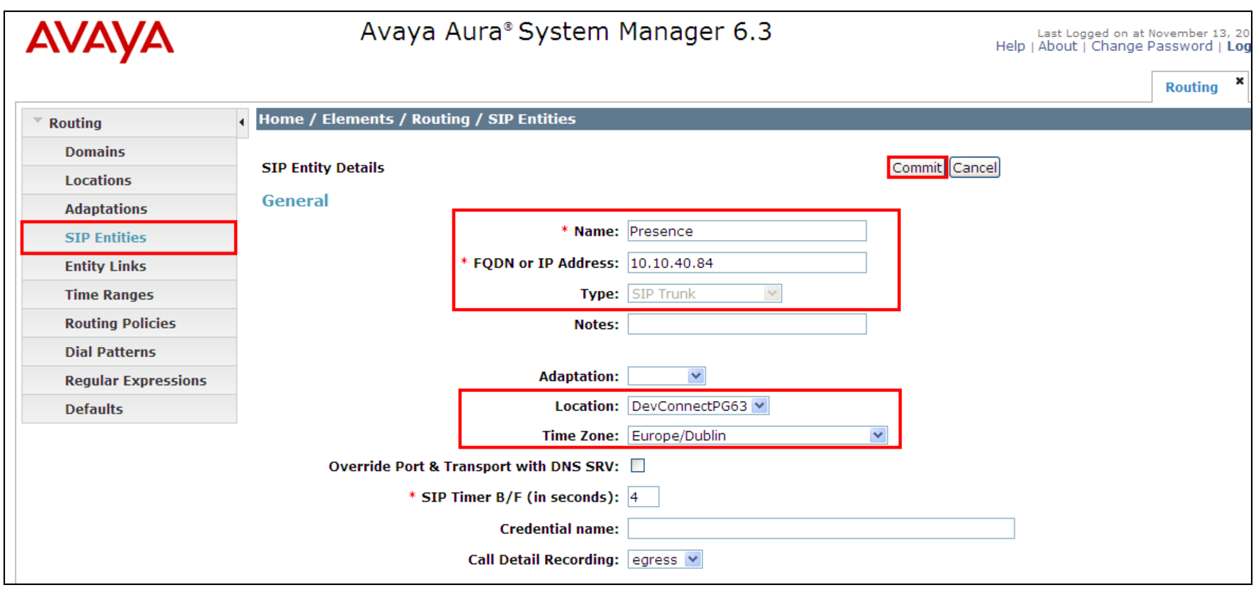
6.4.2 Configure Avaya Aura® Communication Manager Entity

Click **Home → Elements → Routing → SIP Entities → New** assign an identifying **Name**, the **FQDN or IP Address** for the procr, set the **Type** to **CM** and the **Location** to the Location configured in **Section 6.3** and click on **Commit**.



6.4.3 Configure Presence Technology OpenGate Entity

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

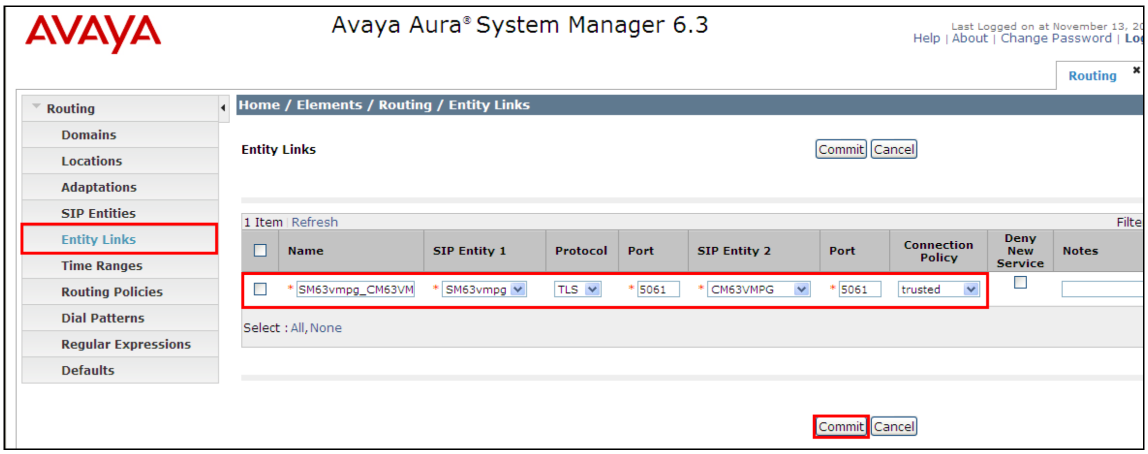


6.5 Administer SIP Entity Link

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 and both Communication Manager and OpenGate.

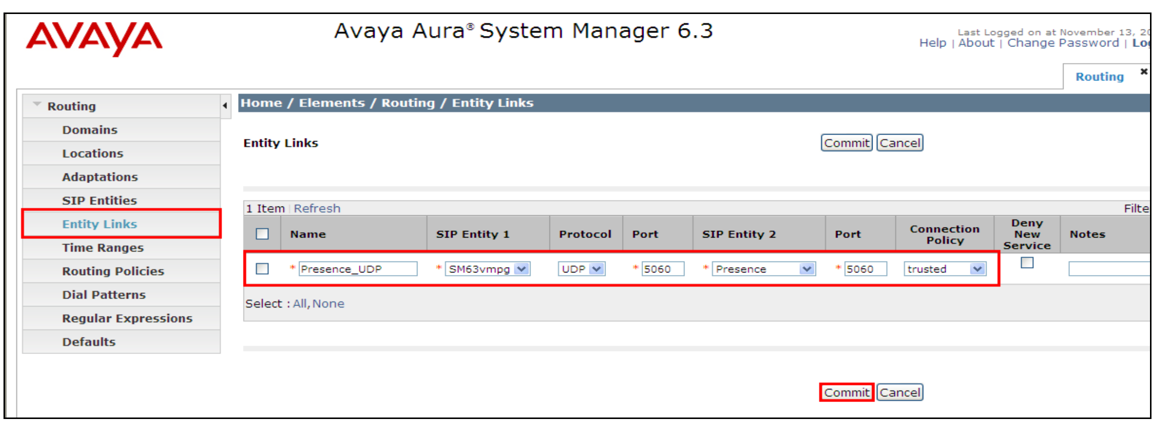
6.5.1 Administer SIP Entity Link from Avaya Aura® Session Manager to Avaya Aura® Communication Manager

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 **TLS**, enter **5061** for the **Port**, choose the Communication Manager entity as **SIP Entity 2** and set the **Port** to **5061**, place an arrow in the **Trusted** box. Click **Commit** when done.



6.5.2 Administer SIP Entity Link from Avaya Aura® Session Manager to OpenGate

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 OpenGate 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 OpenGate.

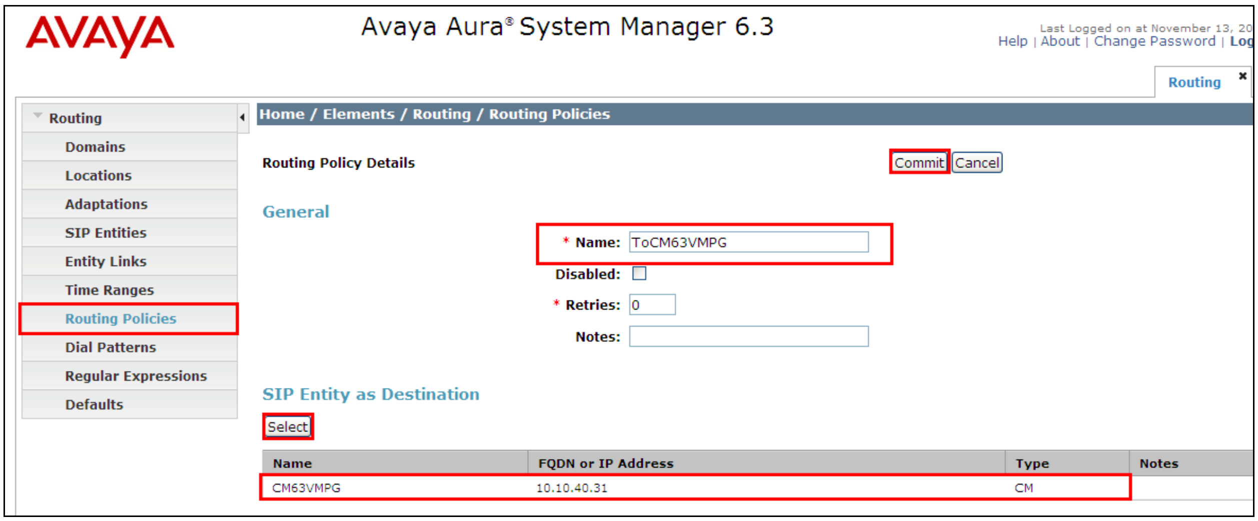


6.6 Administer Routing Policies

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 the Communications Manager and the second for OpenGate. These will be associated with the Dial Patterns created in **Section 6.7**.

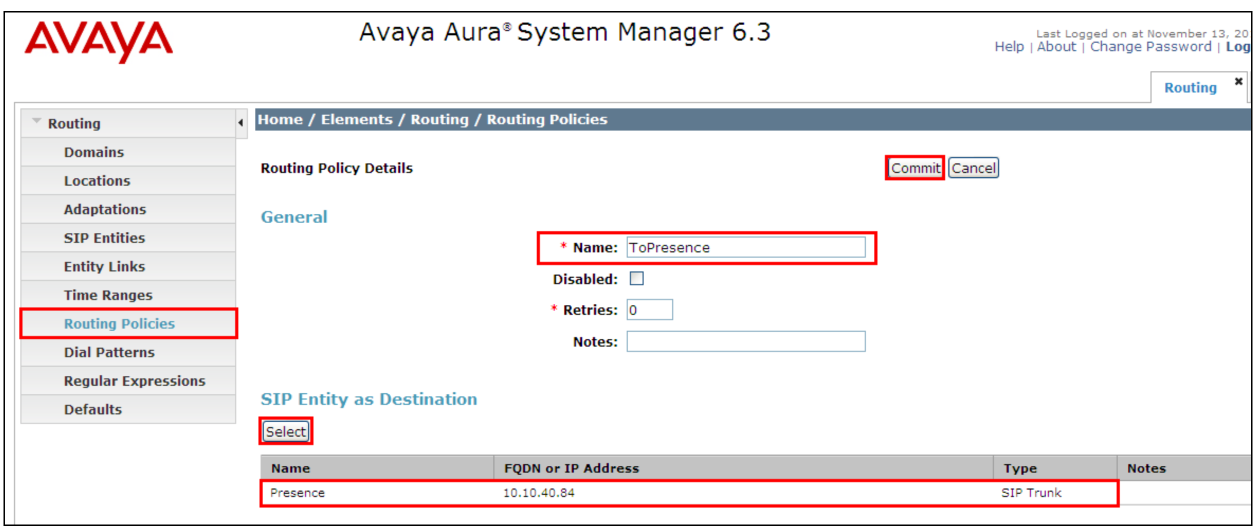
6.6.1 Create Routing Policy to Avaya Aura® Communication Manager

Click **Home → Elements → Routing → Routing Polices →New** assign an identifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select** and choose the Communication Manager SIP Entity and click **Select** (not shown). Click **Commit** when done.



6.6.2 Create Routing Policy to Presence Technology OpenGate

Click **Home → Elements → Routing → Routing Polices →New** assign an identifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select** and choose the OpenGate SIP Entity and click **Select** (not shown). Click **Commit** when done.

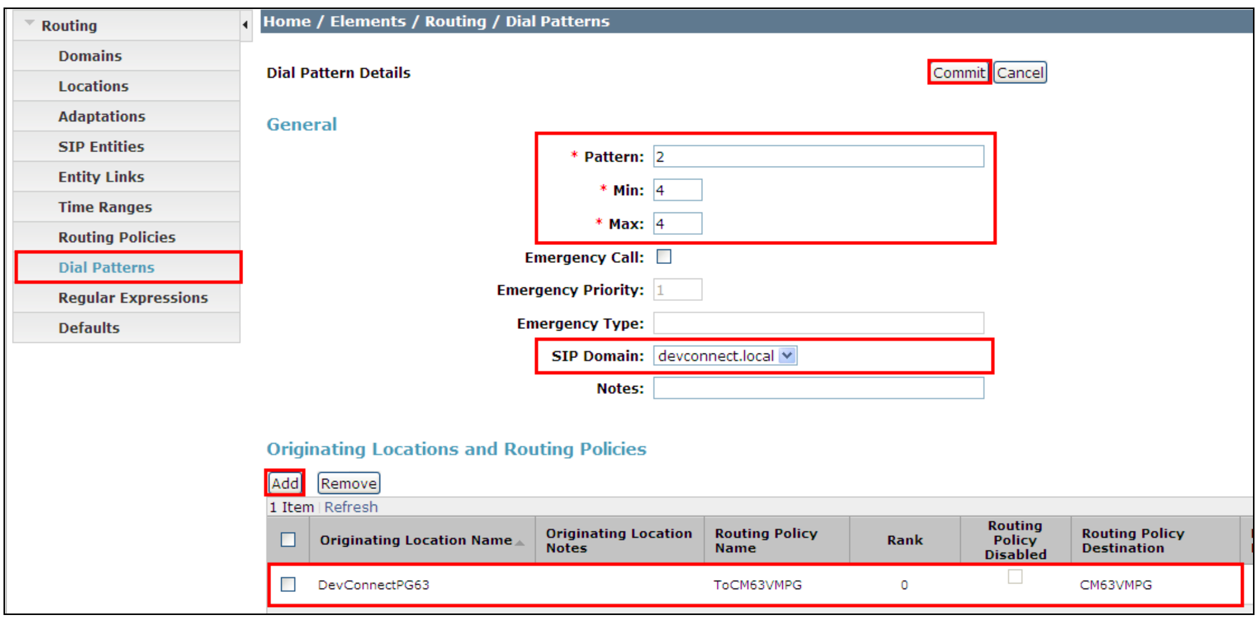


6.7 Administer Dial Patterns

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.

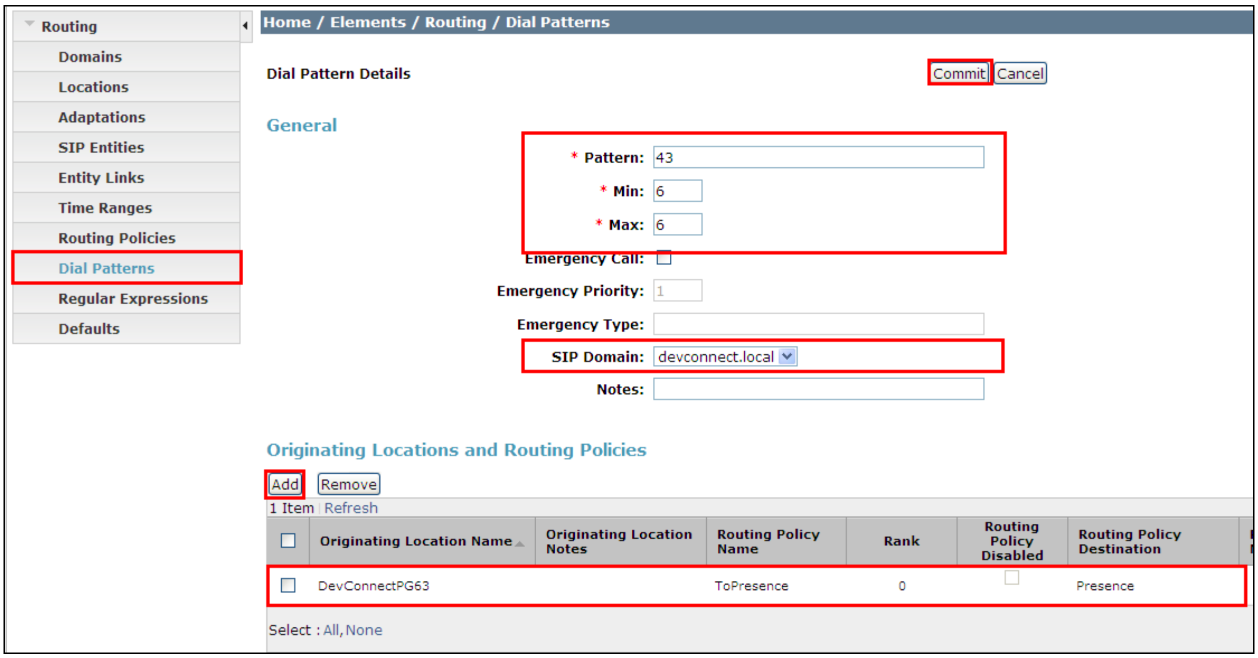
6.7.1 Create Dial Pattern to Avaya Aura® Communication Manager

An additional Dial Pattern must be created on Session Manager to route incoming calls from OpenGate to Communication Manager stations. For compliance testing Communication Manager phones were in the range 2000- 2999 so a dial pattern of 2 with a min and max of 4 was added to route calls 2xxx to Communication Manager. Click **Home → Elements → Routing → Dial Patterns →New.** Under **Pattern** enter the numbers presented to Session Manager by OpenGate destined for Communication Manager, in the **Patterns** box. Set **Min** and **Max** digit string length, and set **SIP Domain** to that which was created in **Section 6.2**. In the **Originating Locations and Routing Policies** section of the web page, click **Add.** In the **Origination Section,** click **All**, in the **Routing Policies** section click the routing policy created for Communication Manager. Click **Select** when done (not shown). Click **Commit** once finished.



6.7.2 Create Dial Pattern to OpenGate

In **Section 5.5** Communication Manager is configured to route the dialed numbers beginning **43**xxxx to Session Manager. To create a Dial Pattern to route **43**xxxx from Session Manager to OpenGate click **Home → Elements → Routing → Dial Patterns →New.** Under **Pattern** enter the numbers presented to Session Manager by Communication Manager destined for OpenGate, in the **Patterns** box. Set **Min** and **Max** digit string length, and set **SIP Domain** to that created in **Section 6.2**. In the **Originating Locations and Routing Policies** section of the web page, click **Add.** In the **Origination Location** section click **All**, in the **Routing Policies** section click the routing policy created for OpenGate. Click **Select** when done (not shown). Click **Commit** when complete.



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.

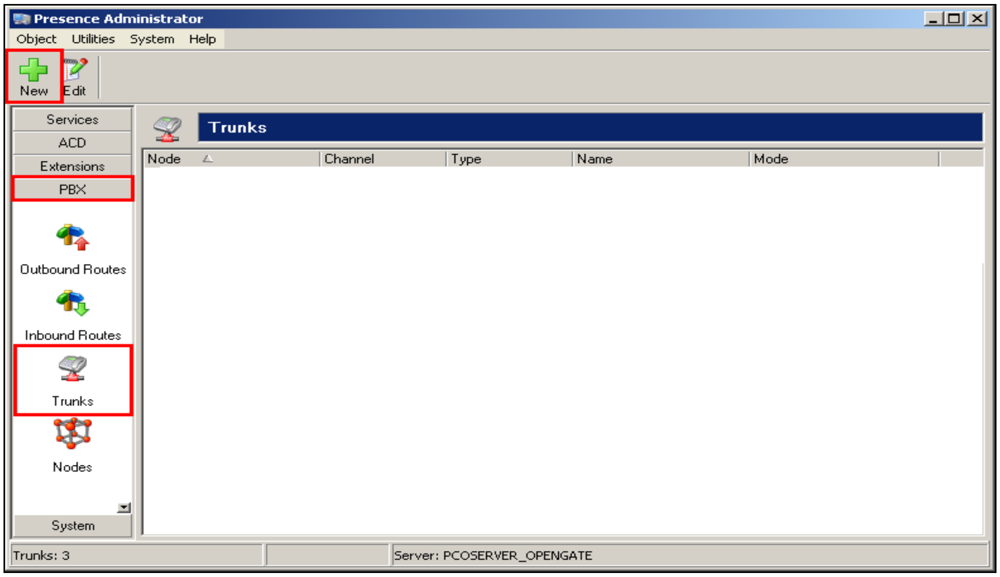
Note: The following configuration details for Agent Login and Skillsets are all a part of the Presence OpenGate internal Call Centre and are not referenced anywhere else in these Application Notes.

7.1 Login to Presence Administrator

Having logged into the Windows Server, 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.

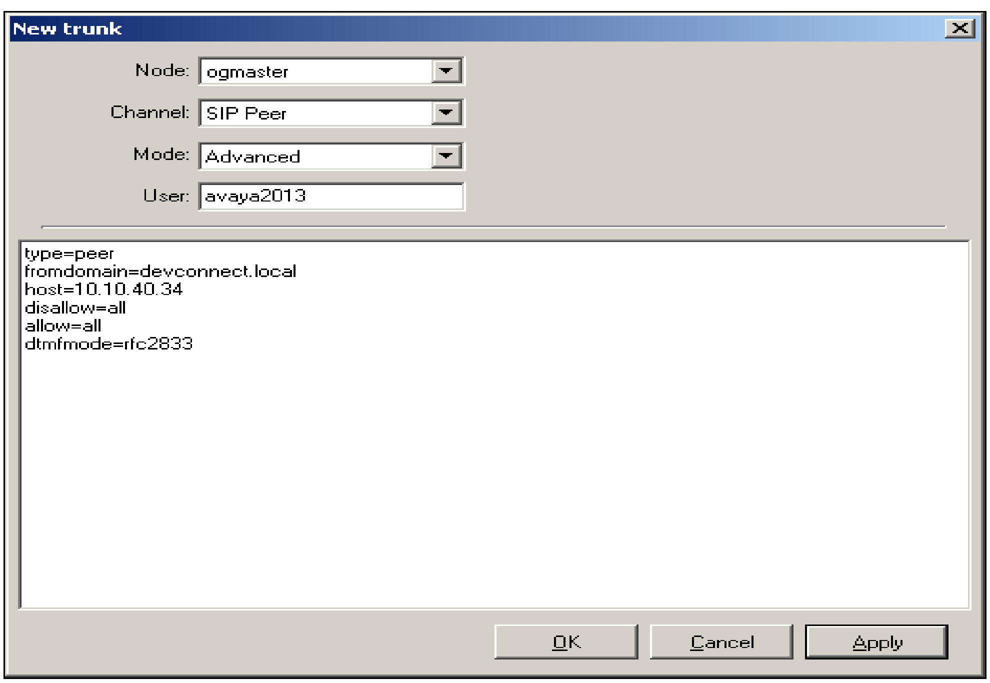
7.2 Administer SIP Trunk to Avaya Aura® Session Manager

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



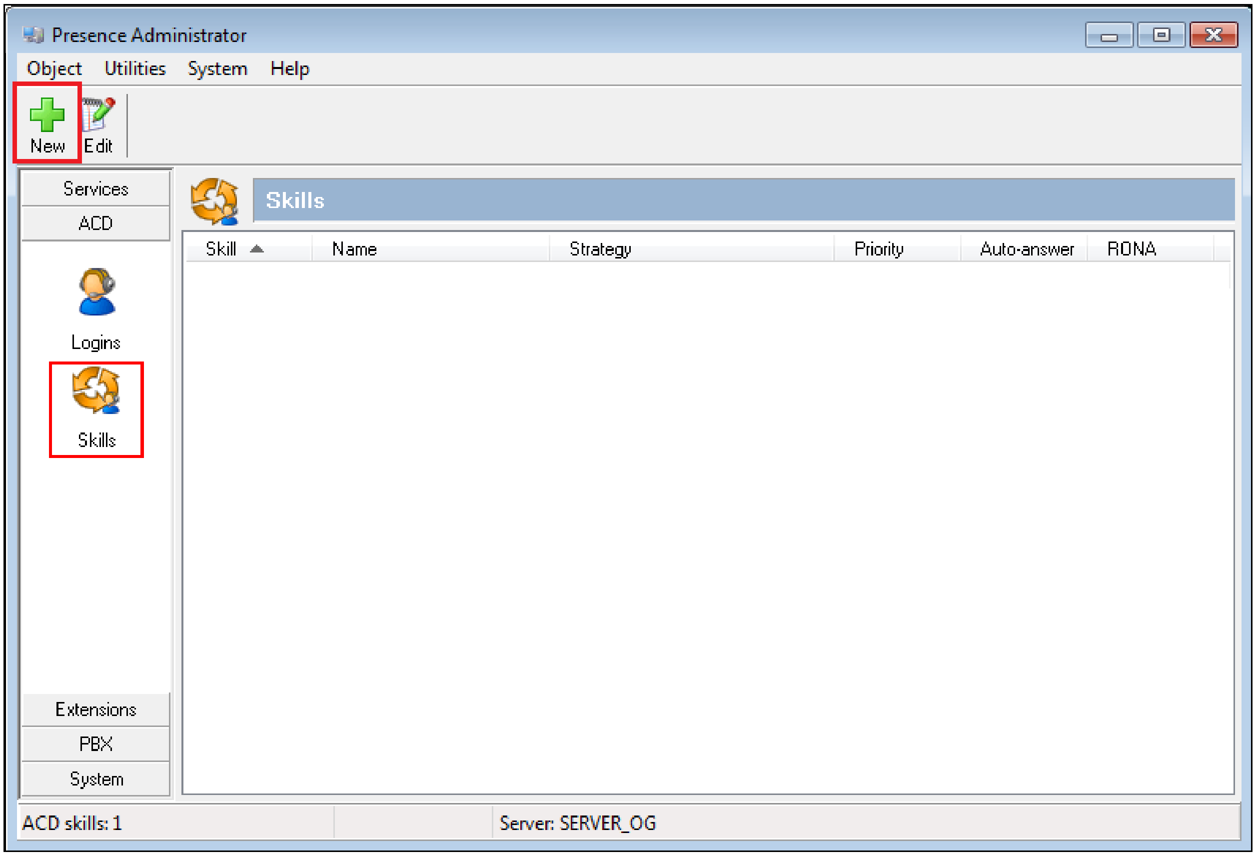
Fill in the information as shown below. Please note that the **Node ogmaster** has already been established during the install of Presence OpenGate. Select **SIP Peer** as the **Channel** and **Advanced** as the **Mode**. Enter a suitable name for the **User**. Note the following in the main window.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

- **Fromdomain** = the domain that is referenced in **Sections 6.2** and **5.5**.
- **Host** = IP address of Session Manager.

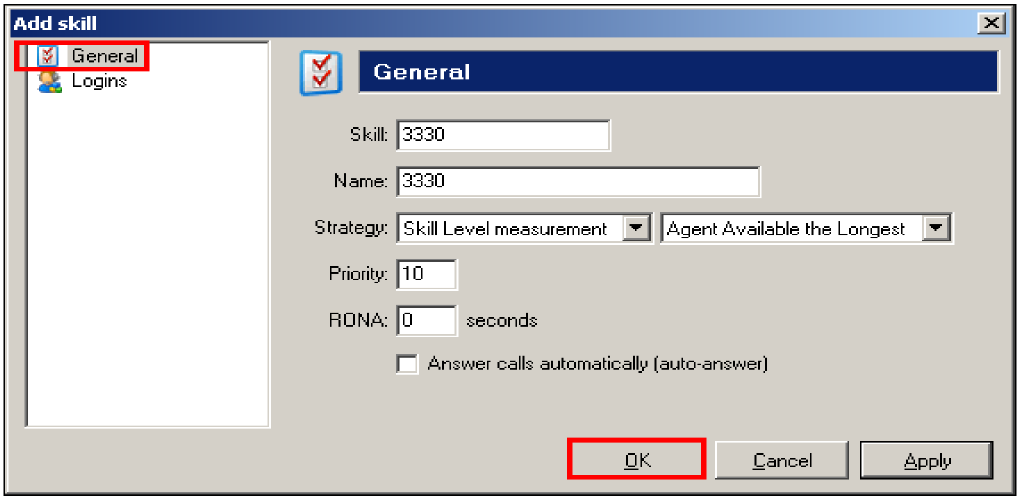


7.3 OpenGate Skill Configuration

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

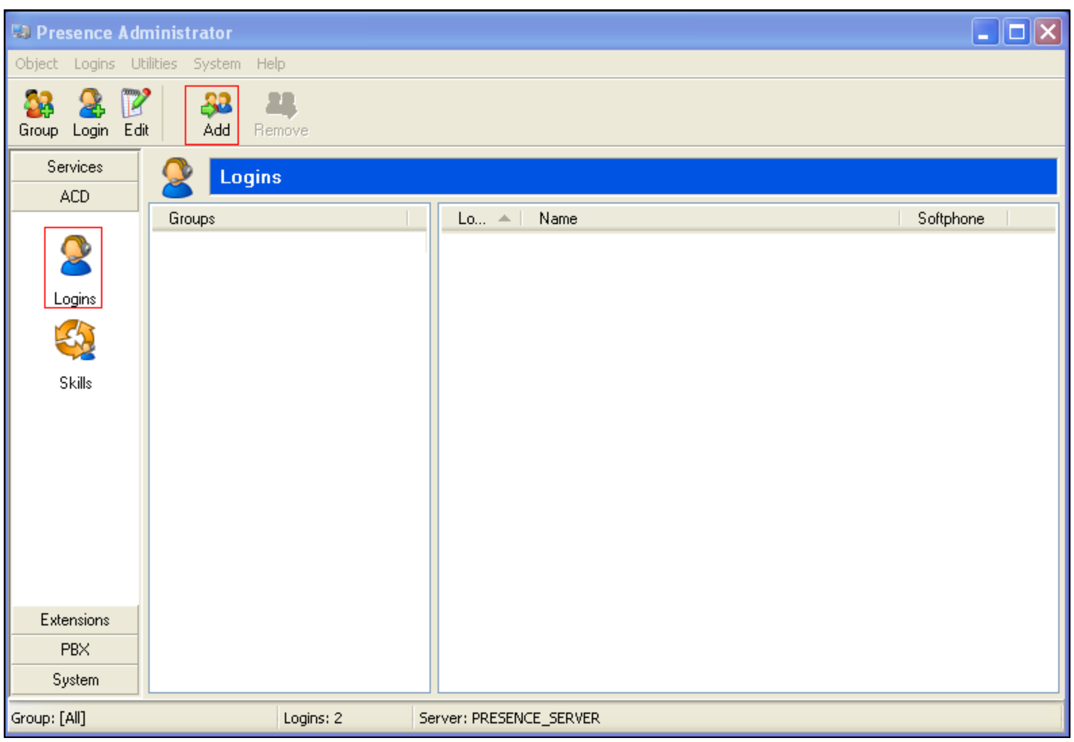


In the resulting screen define a **Skill** number and enter a **Name** to identify the skill. In the **Strategy** field use the two drop down menus to define the selection strategy that will be used by the skill. Set a **Priority** for the skill. All remaining fields can be left with default values.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

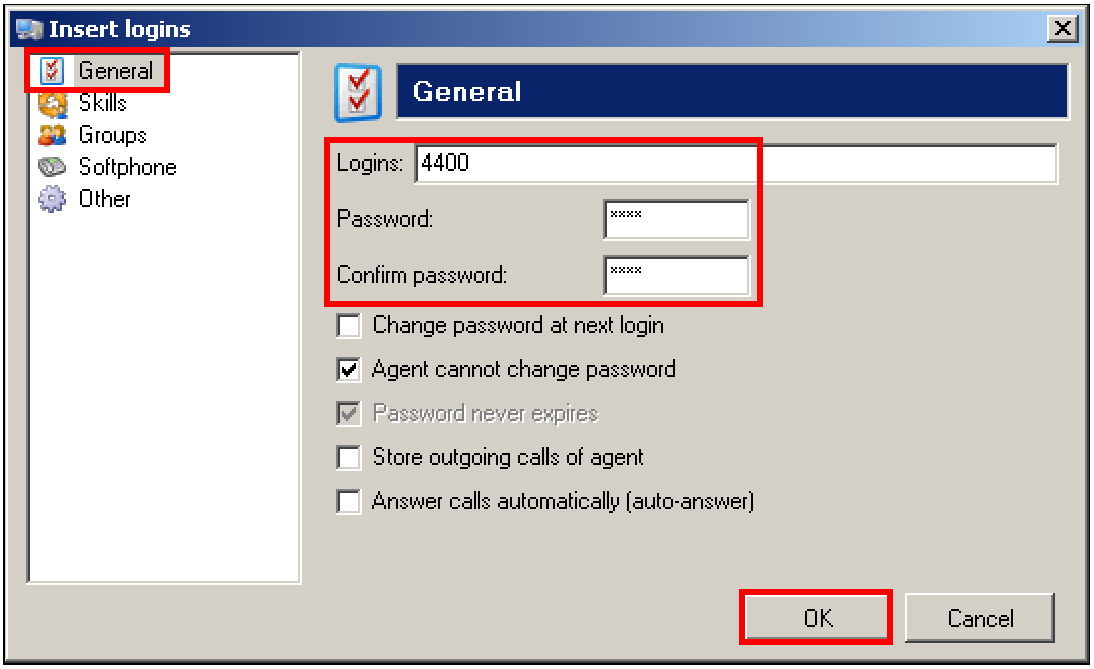


7.4 OpenGate Agent Login Configuration

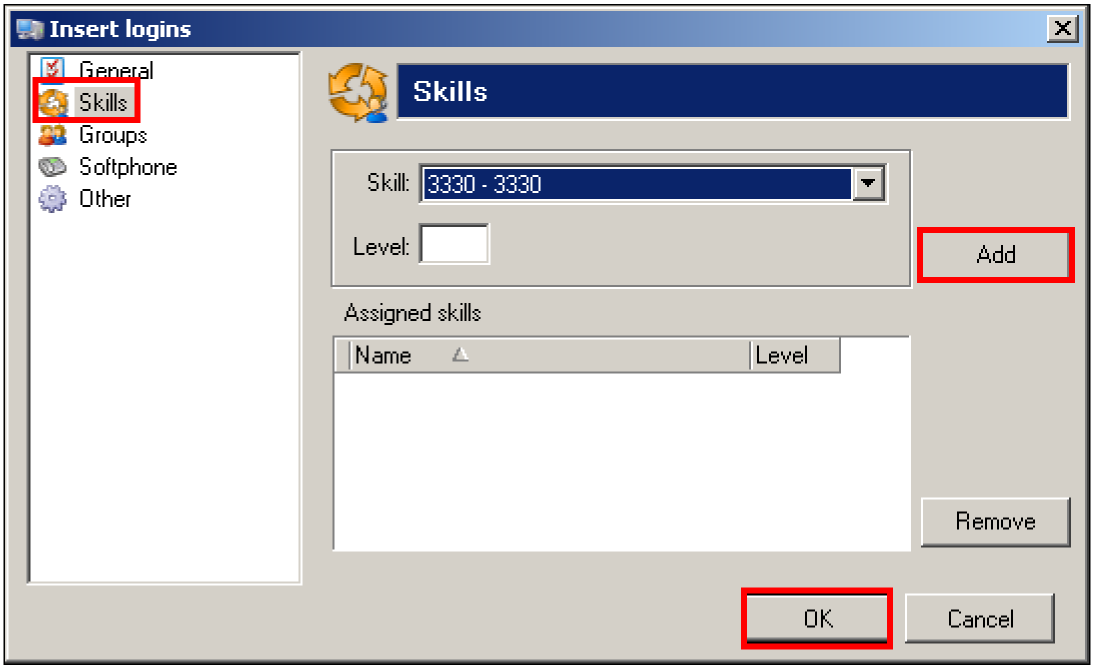
The login configured here will be used by the agent to login to OpenGate. The Agents will connect to OpenGate via the Presence Suite Agent application. To configure an ACD agent login, from the left hand side select **ACD → Logins** from the Presence Administrator main menu. Click the **Add** button.



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

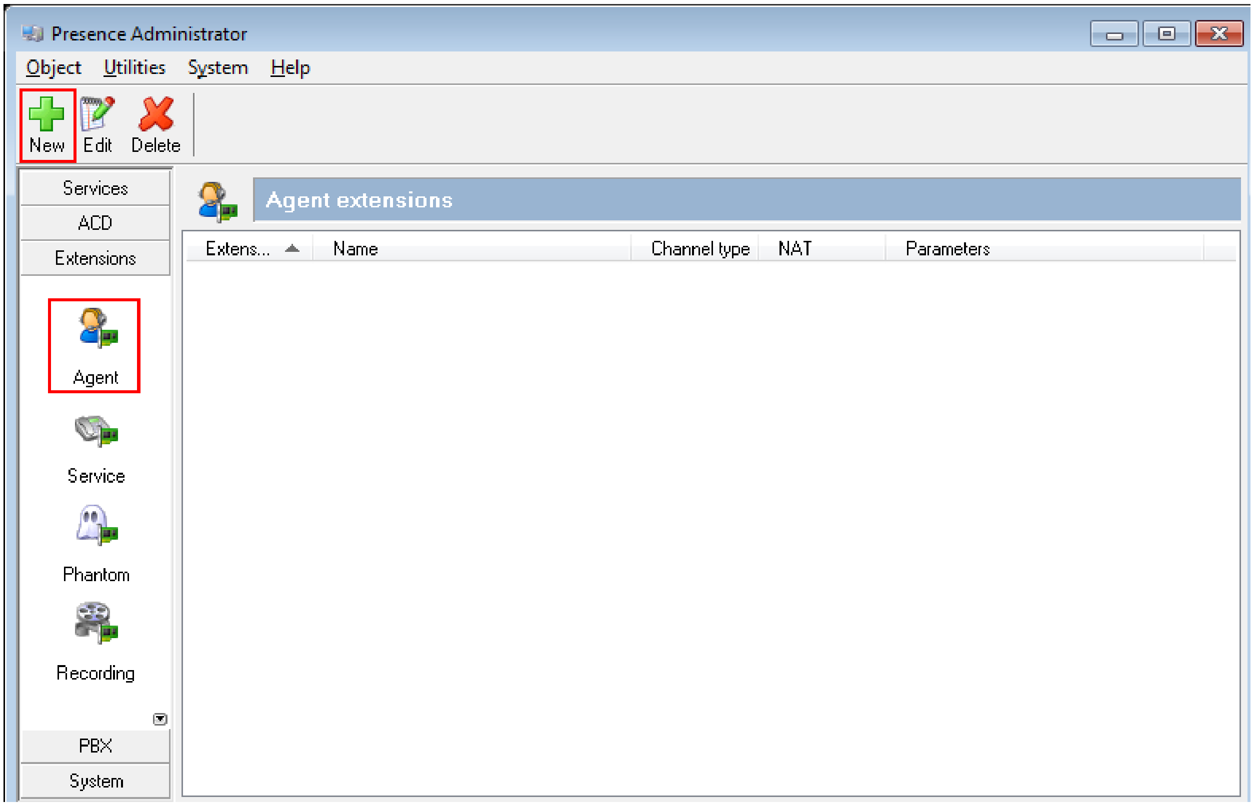


From the menu on the left side of the screen select **Skills,** use the drop down menu to select the **Skill** configured in **Section 7.3** and specify a **Level** for the skill to be applied against this agent login. Click the **Add** button and the skill should appear under **Assigned skills** (not shown here). Click **OK** to save the login configuration.

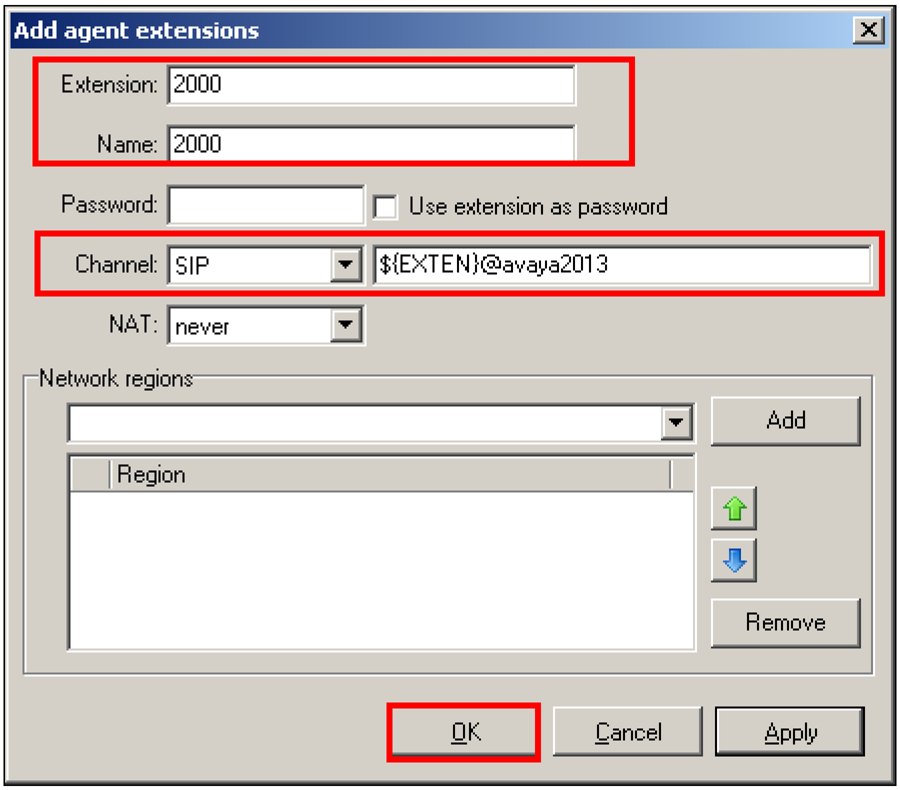


7.5 Presence Technology OpenGate Station Configuration

Each telephone/endpoint that OpenGate could 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.

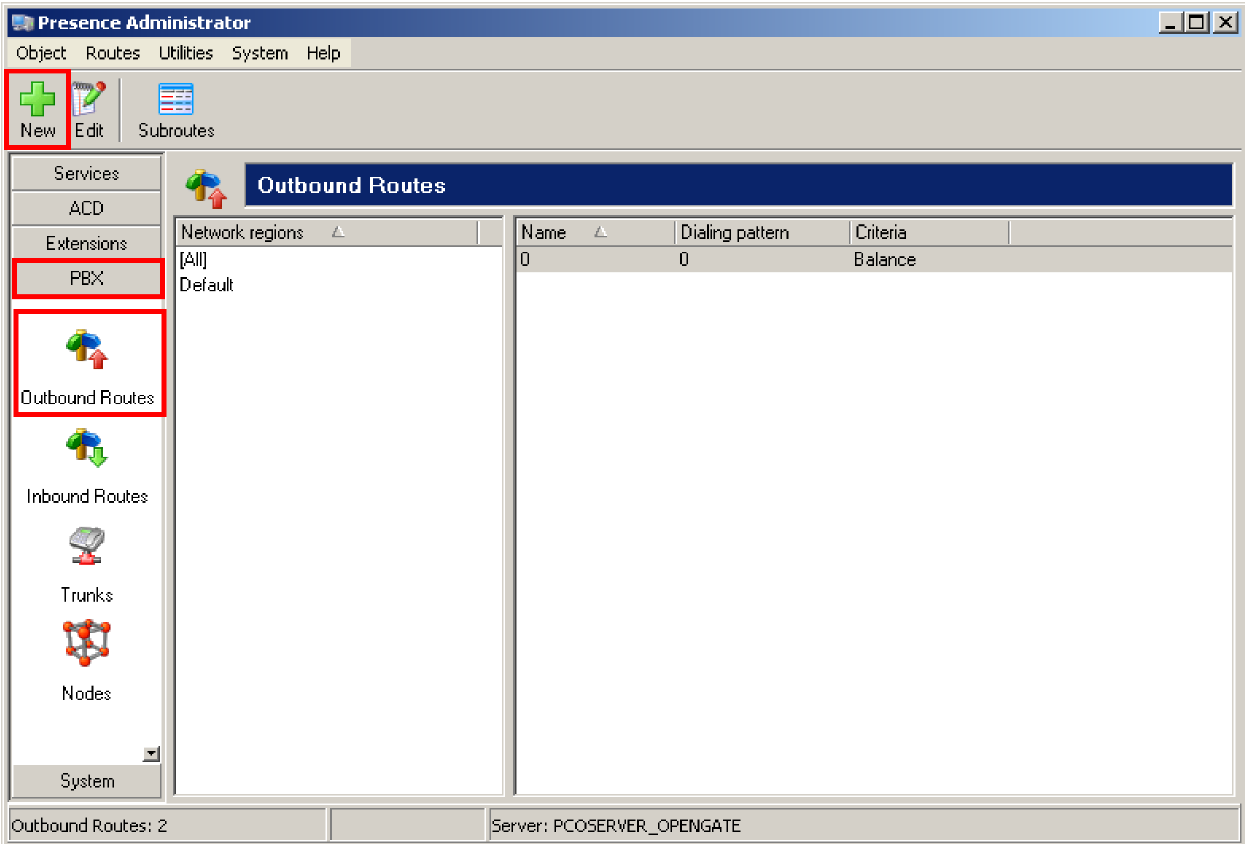


In the resulting screen specify an **Extension** number that will be used by the Presence Agent application **(Section 7.9.1)**. Note can be any existing extension number on Communication Manager. Set a **Name** that the Agent extension will be known as. The password is not required in this case. In the **Channel** field use the drop down arrow to select **SIP.** In the following field define the number that will be dialled and the route used to reach the station, which should be expressed in the form of a URI. The user part is set to the number to be dialled and the host part is set to the name of the sip trunk defined **Section 7.2**. In this example **${EXTEN}@avaya2013** is configured which means any number that is dialled will use trunk "avaya2013", note **avaya 2013** is the SIP Trunk configured in Section 7.2 above**,** so the URI is formatted as **${EXTEN}@avaya2013**.

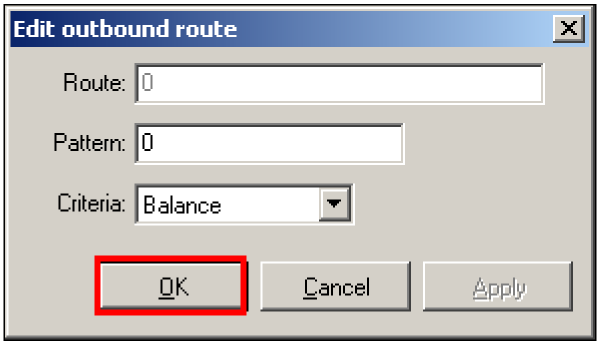


7.6 Outbound Routes

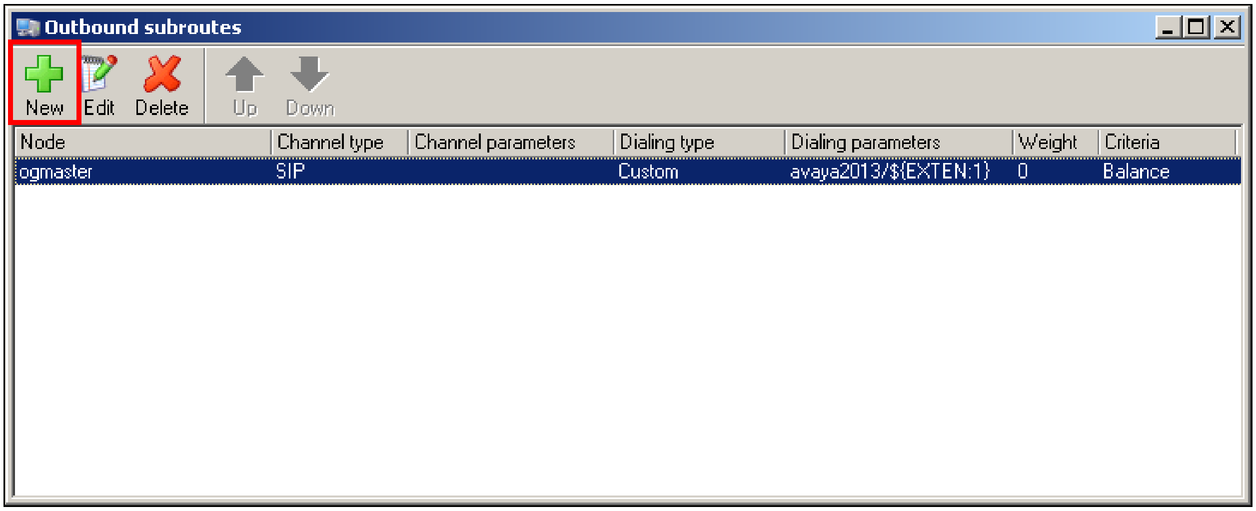
To define an outbound route, from the left hand side navigate to **PBX → Outbound Routes** and click the **New** button.



In the resulting screen enter a descriptive name in the **Route** field (note the same name as the patterns was used below) 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 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. **Balance** allows an even distribution of calls across the subroutes. Click **OK** to save the **outbound route**.



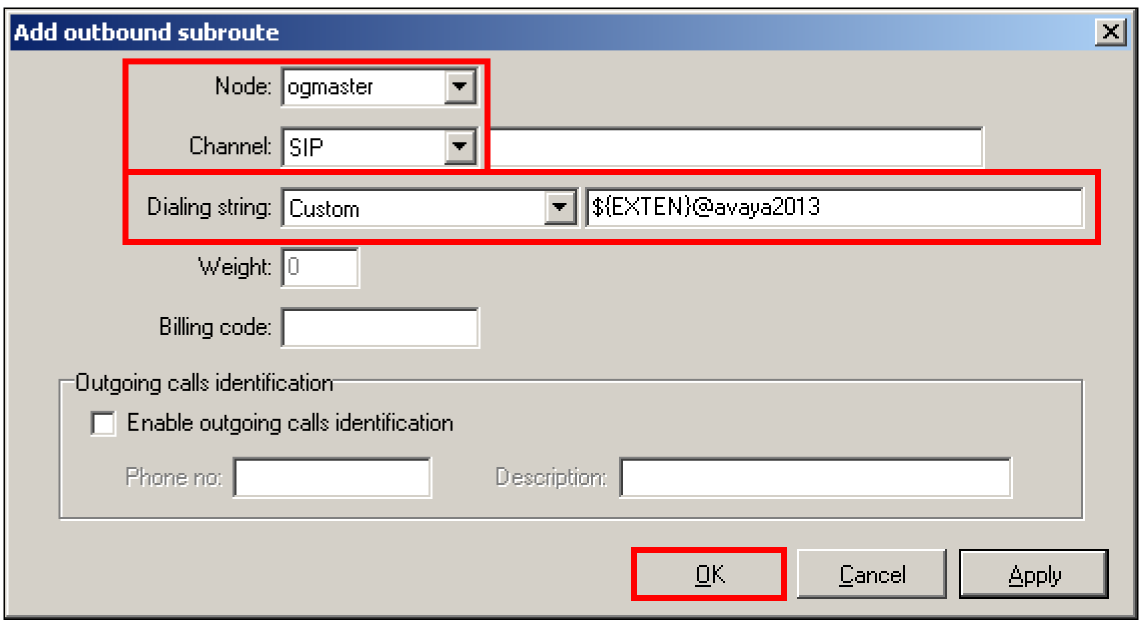
To add an outbound subroute, from the outbound routes main page shown above, highlight the outbound route that was added in the previous step and click the subroutes button at the top of the screen (not shown). The **Outbound subroutes** window is then displayed as shown below, Click **New**.



In the resulting window select the relevant **Node** (this was created during the OpenGate install), and under **Channel** select **SIP**. For **Dialing string** use the drop down menu to select **Custom** and in the secondary field enter a matching pattern using a regular expression. In the example below the expression used is **${EXTEN:1}@avaya2013**. The expression performs the following:

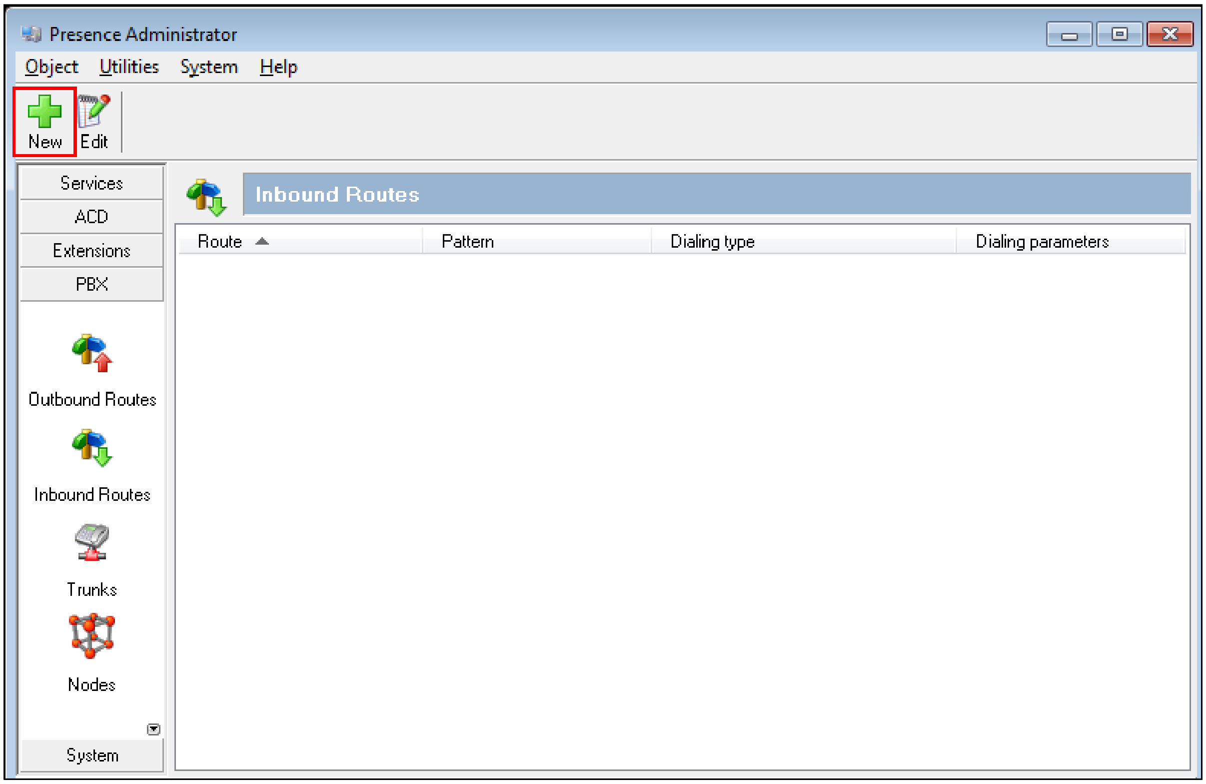
- **EXTEN** is an internal variable which represents the called number, therefore this pattern will match any called number beginning with a 0(2000).
- Remove the leading character (leaving 2000).
- Route it via the **avaya2013** trunk defined in **Section 7.2**.

This is done in order to use the same numbers that may be used on the Avaya PBX. Using 0 to make outgoing calls and then stripping the 0 before the call reaches the Session Manager and Communication Manager. For more information on the routing of call in OpenGate please refer to the following document referenced in Section 10 of these Application Notes. *ACD Sys Presence Administrator Manual Presence Suite*, V10.0

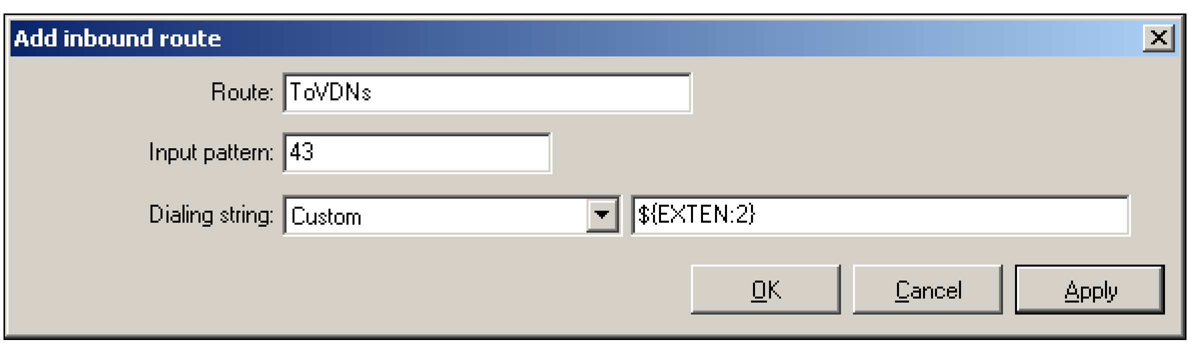


7.7 Inbound Routes

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 the **Input pattern** field enter a numerical pattern that the inbound route will use to match incoming digits. Use the drop down menu in the **Dialing string** field to specify the digit manipulation to be performed. In the example below, incoming digits **43** will be replaced with **${EXTEN:2)**. This will remove two digits from the incoming call i.e., the 43 from the incoming call leaving 3300, which is the internal Service Extension used within OpenGate. Note 3300 was configured in Section 7.4 as an OpenGate skill.



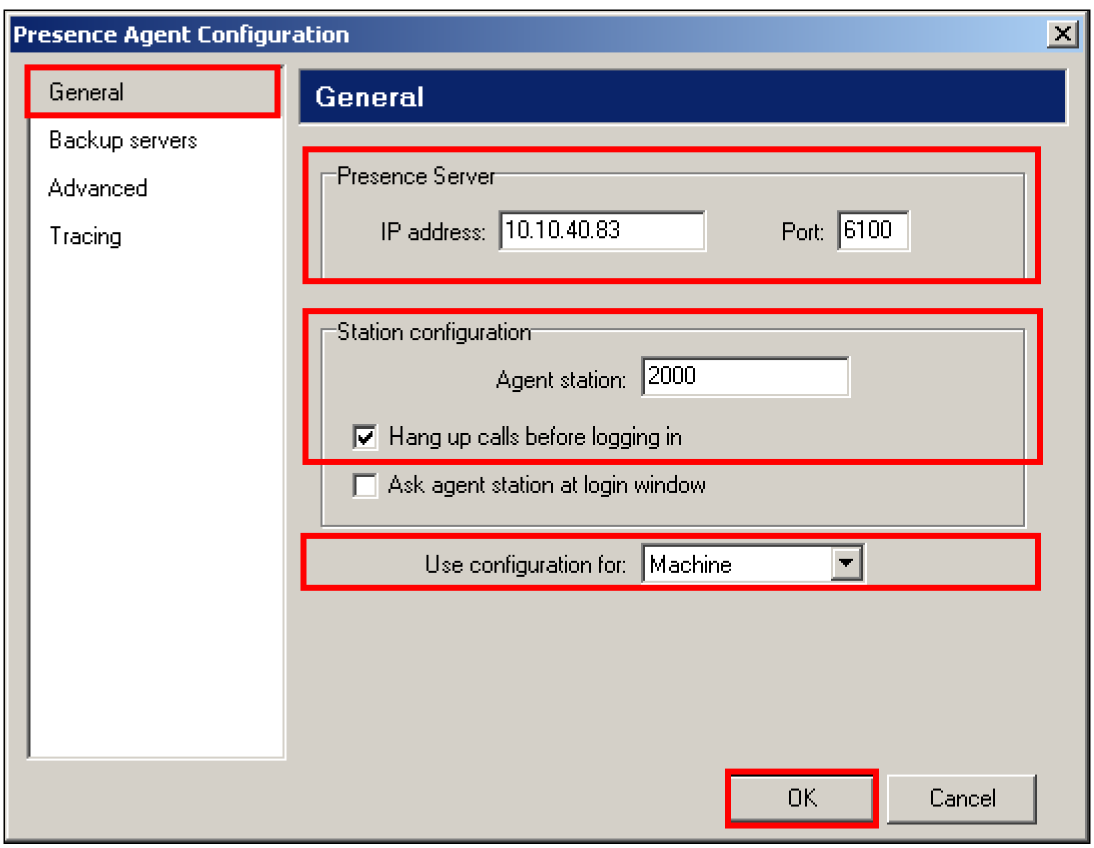
7.8 Logging into OpenGate

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.

7.8.1 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 Applciation 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 **10.10.40.83**. 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. In the field **Use configuration 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.



7.8.2 Logging in Presence Agent

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**.

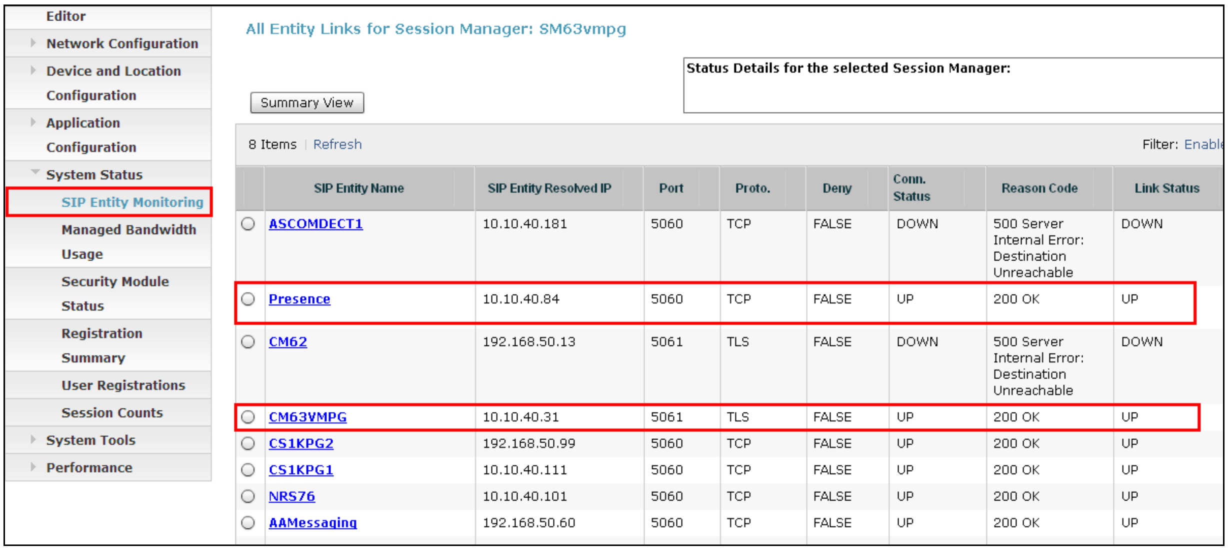
A task bar is present at the top of the Agent PC. Click on the green arrow to put the agent into an available state.

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

8. Verification Steps

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

1. 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**.



2. 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
```

3. Manually verify that calls can be placed to OpenGate and routed to Agents. Make a call from any Communication Manager phone to a number associated with an OpenGate skill. Note for compliance testing 433300 was used as an example. This call will then get routed to an Agent logged into a Communication Manager phoneset associated with this OpenGate skill.

9. Conclusion

These Application Notes describe the configuration steps required for Presence Technology OpenGate R10.0 to successfully interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3. 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 6.3.

[2] *Administering Avaya Aura® Session Manager* – Release 6.3.

The following documentation is available on request from Presenceat http://www.presenceco.com.

[1] *ACD Sys Presence Administrator Manual Presence Suite*, V10.0.

[2] *Presence Installation Guides Presence Software*, V10.0.

[3] *PBX/ACD Requirements Presence Software*, V10.0.

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.