Avaya Solution & Interoperability Test Lab

Application Notes for Presence Technology OpenGate 8.1 with Avaya Aura® Communication Manager and Avaya Aura ® Session Manager – 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 OpenGate provides ACD and CTI capabilities to companies that do not have any existing CTI or ACD capabilities on their PBX. Presence 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 can successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. 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. The focus of the interoperability test is the ACD functionality offered by Presence Technology OpenGate. For the sample configuration discussed in this document the PSTN connection is to the Avaya Aura® Communication Manager, all calls are received from the PSTN by Avaya Aura® Communication Manager and routed via a SIP Trunk to Avaya Aura® Session Manager, Avaya Aura® Session Manager is then responsible for routing the call to Presence Technology OpenGate to receive ACD treatment. Presence Technology OpenGate can route calls to Presence agents served by Avaya endpoints, Presence agent served via the PSTN or Presence agent served directly from Presence Technology OpenGate. Presence Technology OpenGate is part of the Presence Suite group of products, these Application Notes assumes that the installation and configuration relating to Presence Suite has already been completed and is not discussed. Presence Technology OpenGate specifies where to route each call and hence how to handle the calls, based on agent status information that the system tracks from the Presence Agent software, as well as the SIP trunk messaging for the calls it has routed.

In the sample configuration described by these Application Notes, calls will be accepted from the PSTN and routed to Presence Technology OpenGate on digits 8501, Presence Technology OpenGate will then map these digits to an internal number of 1801 which represents the ACD service queue within Presence Technology OpenGate. Presence Technology OpenGate then routes the call to an available agent by dialing that agent's extension number. The calling number will appear as the Presence Technology OpenGate service number, i.e. 1801.

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 centre functions including, inbound voice call 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. All the test cases passed successfully.

2.1 Interoperability Compliance Testing

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

2.2 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 Avaya Aura® Communication Manager and an Avaya G650 Media Gateway were used as the hosting PBX. SIP trunks are configured between Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Presence OpenGate to carry calls between them. Presence Suite, including Presence Agent PC's, were connected to the LAN to provide Agent desktop application connectivity.

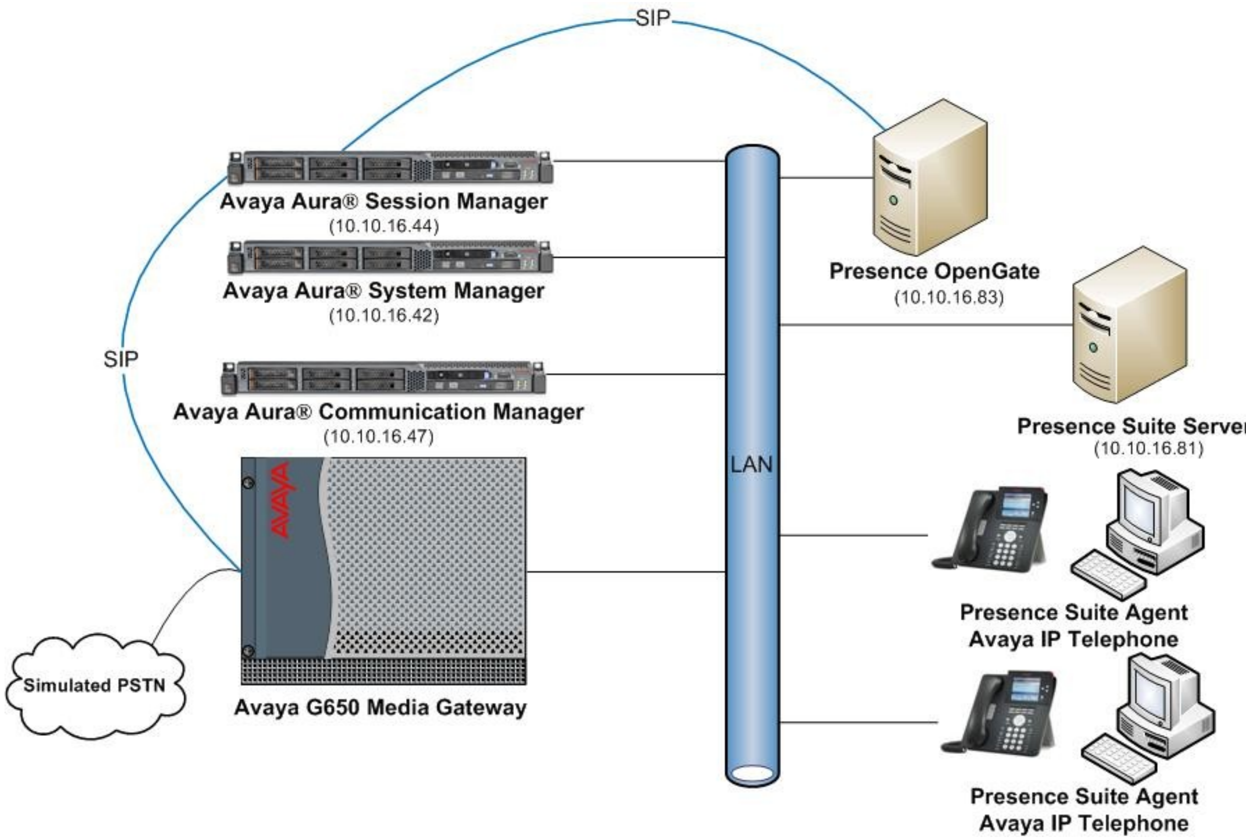


Figure 1: Network Topology Used to Test Presence Technology OpenGate

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server running Avaya Aura® Communication Manager	Avaya Aura® Communication Manager 6.0 Service Pack 01
Avaya G650 Media Gateway CLAN -TN799DP MEDPRO- TN2302AP	 HW 01 FW 024 HW 08 FW 055
Avaya S8800 Server running Avaya Aura® Session Manager	Avaya Aura® Session Manager 6.0 (Build - 6.0.1.0.601009)
Avaya S8800 Server running Avaya Aura® System Manager	Avaya Aura® System Manager 6.0 (Template – 6.0.7.0)
Avaya 96xx Telephones (H.323)	3.1.1
Presence Suite Server	8.1
Operating System for Presence Agent PC's	Windows XP Professional SP3 Windows Vista Business

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 Avaya Aura® Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Avaya Aura® 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
- Configure SIP Trunk
- Administer Route Selection for OpenGate calls
- Administer Incoming Digit Translation

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** 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 enabled.

```
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 enabled.

```
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 **Reference [1]** for further details.

```
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.

```
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: *24
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 5
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *25    Deactivation: #25
```

5.3 Administer Dial Plan

For the testing, two number ranges were used on Communication Manager. The first range is used for agent stations configured on Communication Manager and are defined in the dial plan as **ext,** these begin with **16** and are four digits in length. The second range is used to deliver and identify calls to OpenGate, this range begins with digits **85**, are four digits long, and are defined as **udp** within the dial plan.

```
display 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
   16          4   ext
   5           1   fac
   600         4   ext
   7           3   dac
   85          4   udp
   9           1   fac
   *           3   fac
   #           3   fac
```

5.4 Configure SIP Trunk

In the **Node Names IP** form, assign an IP address and host name for the C-LAN board in the Avaya G650 Media Gateway and for the SIP Signaling interface on the Session Manager. The host names will be used throughout the other configuration screens of Communication Manager.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
AES522              10.10.16.25
CLAN                10.10.16.31
CM521               10.10.16.23
Gateway             10.10.16.1
MedPro              10.10.16.32
SM1                 10.10.16.43
default             0.0.0.0
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**. 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: avaya.com
    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 transparency tcp was used during this compliance test but the recommended method is 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 C-LAN board in the G650 Media Gateway 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 the node name for the C-LAN board in the G650 Media Gateway (node name **CLAN**). This value is taken from the **IP Node Names** form shown in **Section 5.4**
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM1**), also shown in **Section 5.4**.
- Ensure that the recommended TCP port value of **5060** 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 in **Section 5.4.** 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 5                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 5             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n                                               SIP Enabled LSP? n
     IP Video? n                                     Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: CLAN                   Far-end Node Name: Presence
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         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? n                    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 5                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 5                    Group Type: sip           CDR Reports: y
  Group Name: to Presence                 COR: 1        TN: 1        TAC: 705
   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: 5
                                                     Number of Members: 30
```

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 5                                            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
```

5.5 Administer Route Selection for OpenGate Calls

As digits 85xx 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 **85** that are **4** 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
  85              4   0                   aar  n
                                               n
```

Use the **change aar analysis** command to further configure the routing of the dialed digits. Calls to OpenGate begin with **85** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 5**, 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
    85                     4    4     5         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 5** is used to route calls to trunk group **(Grp No) 5**.

```
change route-pattern 5                                          Page   1 of   3
                    Pattern Number: 5   Pattern Name: to presence
                             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: 5    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            rest                                        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
```

5.6 Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DID calls from the PSTN network to the extension(s) that will be used to access OpenGate. In these application notes trunk group 1 serves as the PSTN connection, use the command **change inc-call-handling-trmt trunk-group 1**. The entry displayed below translates incoming DID numbers in the range 0207222-85xx to the corresponding 4 digit extension 85xx by deleting the leading 7 digits.

```
change inc-call-handling-trmt trunk-group 1                     Page   1 of   3
                        INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    11  020722285       7
 public-ntwrk
```

6. Configuring Avaya Aura® Session Manager

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

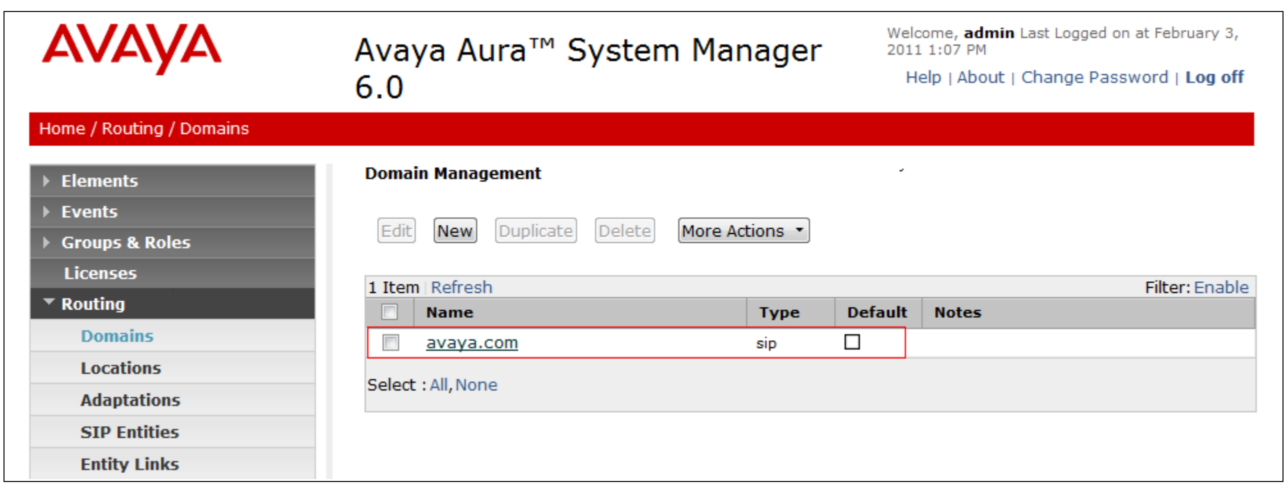
- Log in to Avaya Aura® Session Manager
- Administer SIP Domain
- Administer Location
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Avaya Aura® Communication Manager as Managed Element
- Administer Application for Avaya Aura® Communication Manager
- Administer Application Sequence for Avaya Aura® Communication Manager

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. Log in using appropriate credentials (not shown).

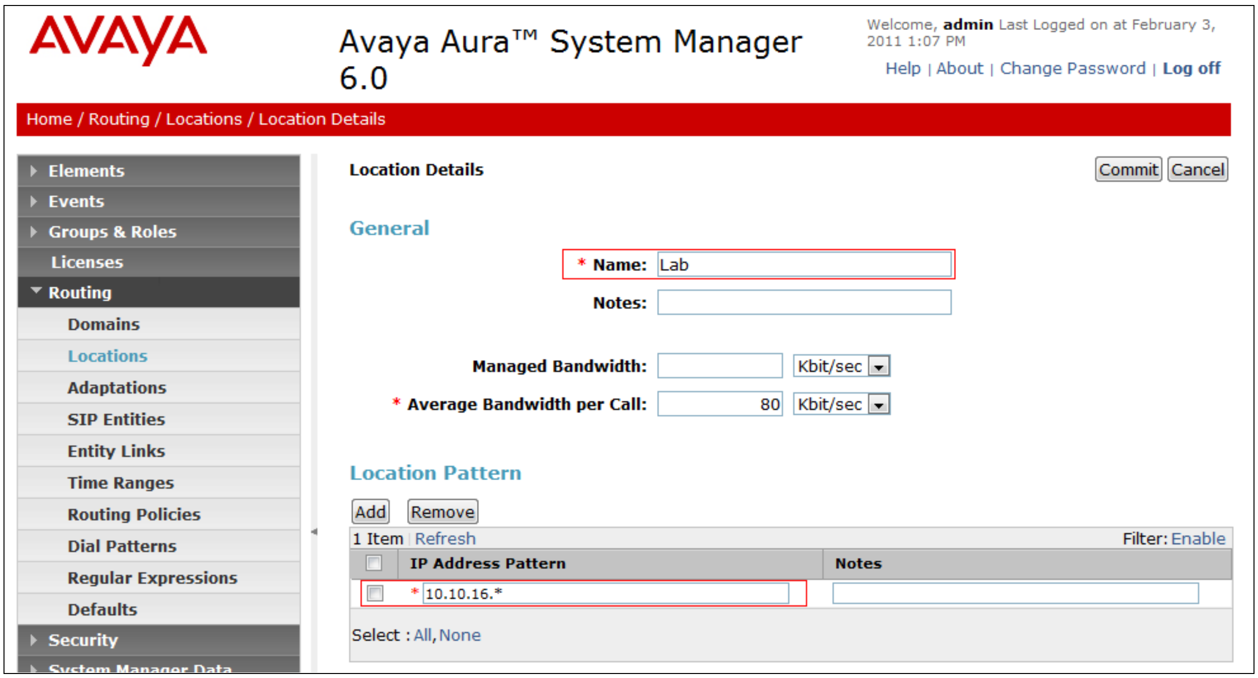
6.2 Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing → SIP Domains** from left hand menu. Click the **New** button (not shown) to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **avaya.com**) and optionally a description for the domain in the **Notes** field. Click **Commit** to save changes.



6.3 Administer Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management. A single location is added to the configuration for all of the SIP entities used during the test. Select **Routing → Locations** from the left hand menu and click new (not shown). Under **General,** in the **Name** field enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern** click **Add,** then enter an **IP Address Pattern** in the resulting new row. ‘*’ is used to specify any number of allowed characters at the end of the string.



6.4 Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity. Under **General:**

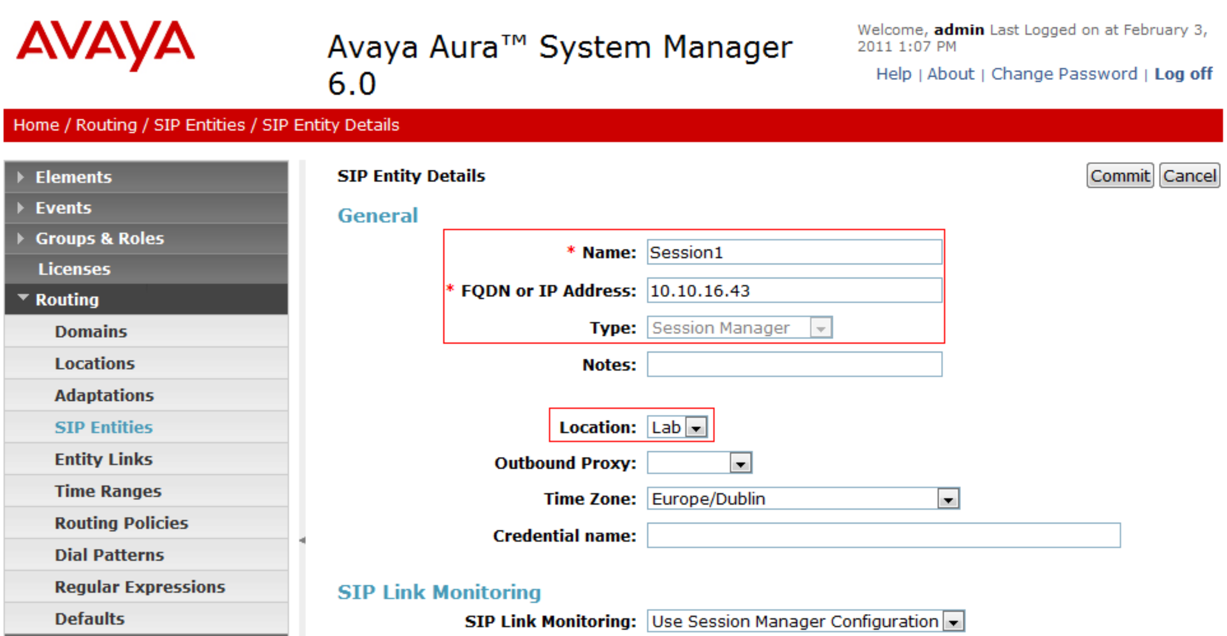
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **SIP Trunk** for the OpenGate SIP entity.
- In the **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field enter the time zone for the SIP Entity

In this configuration there are three SIP Entities.

- Session Manager SIP Entity
- Communication Manager SIP Entity
- OpenGate SIP Entity

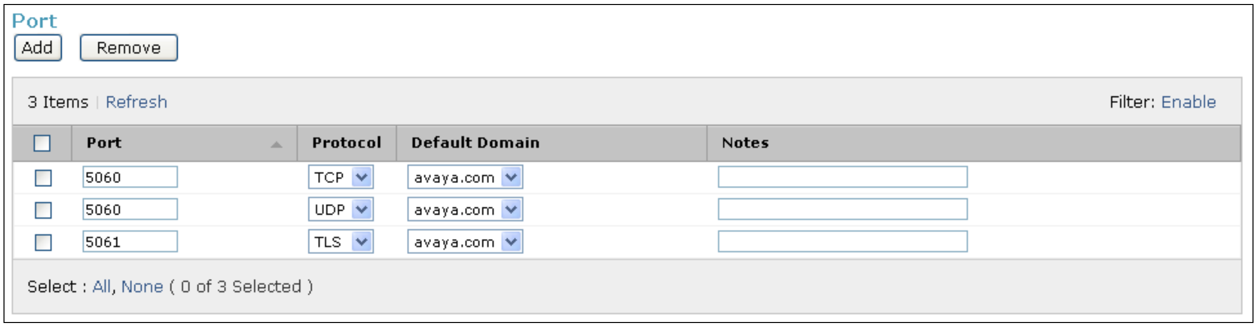
6.4.1 Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signaling interface.



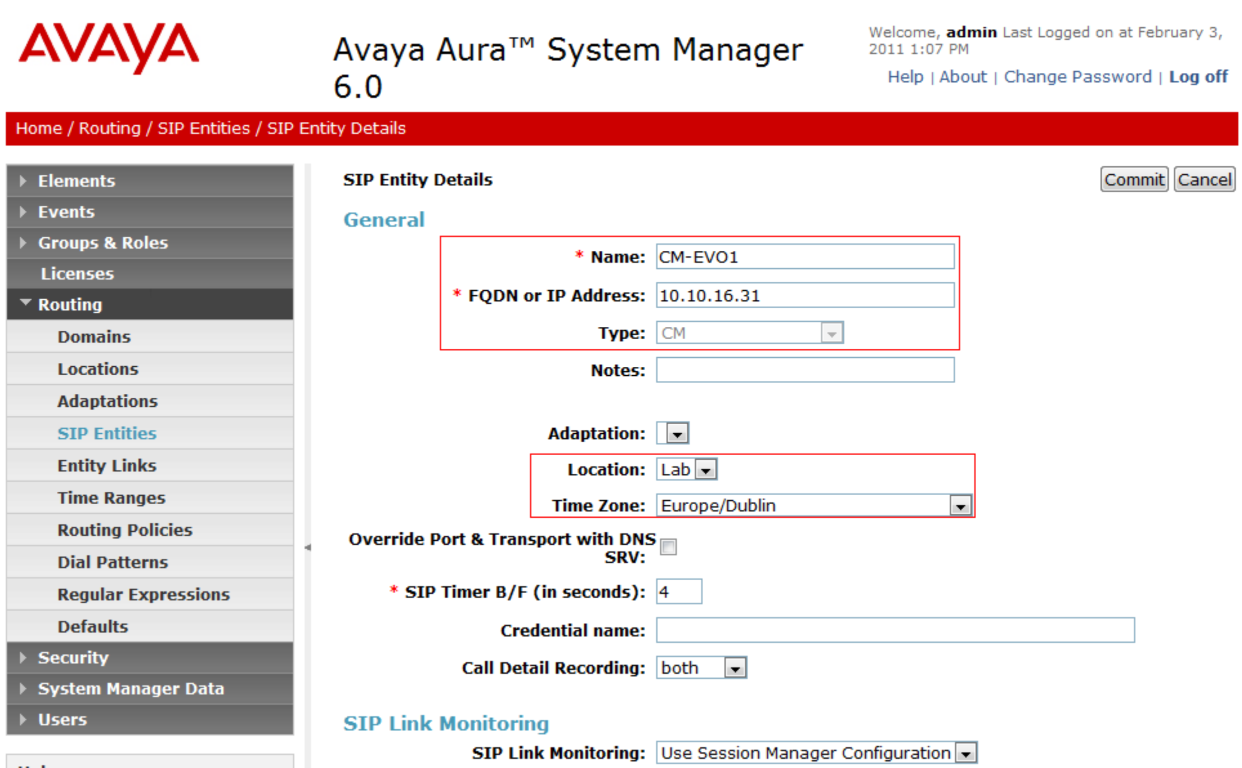
The Session Manager must be configured with the port numbers for the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port** click **Add,** then edit the fields in the resulting new row

- In the **Port** field enter the port number on which the system listens for SIP requests
- In the **Protocol** field enter the transport protocol to be used for SIP requests
- In the **Default Domain** field select the appropriate domain from the drop down menu. In the test, the domain of **avaya.com** was used as the default domain.



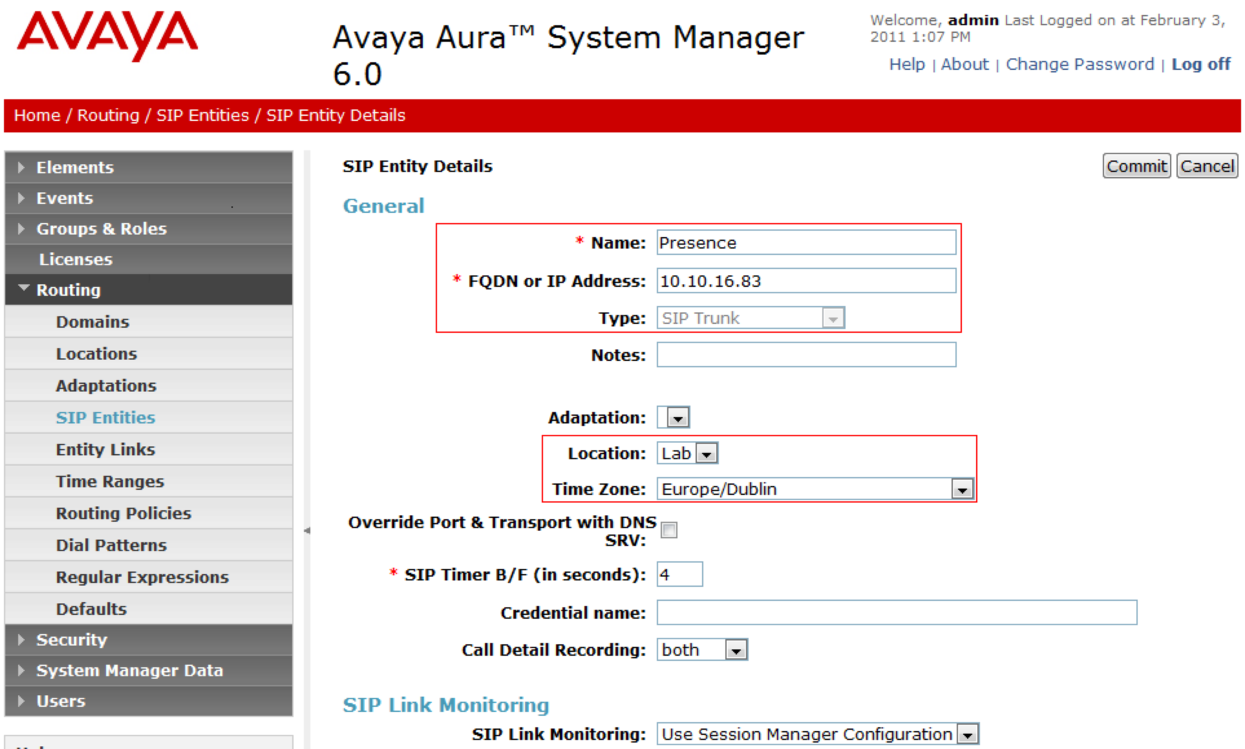
6.4.2 Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an evolution server. The **FQDN or IP Address** field is set to the IP address of the C-LAN board in the Avaya G650 Media Gateway.



6.4.3 OpenGate SIP Entity

The following screen shows the SIP Entity for OpenGate. The **FQDN or IP Address** field is set to the IP address of the OpenGate telephony server (see **Figure 1**).

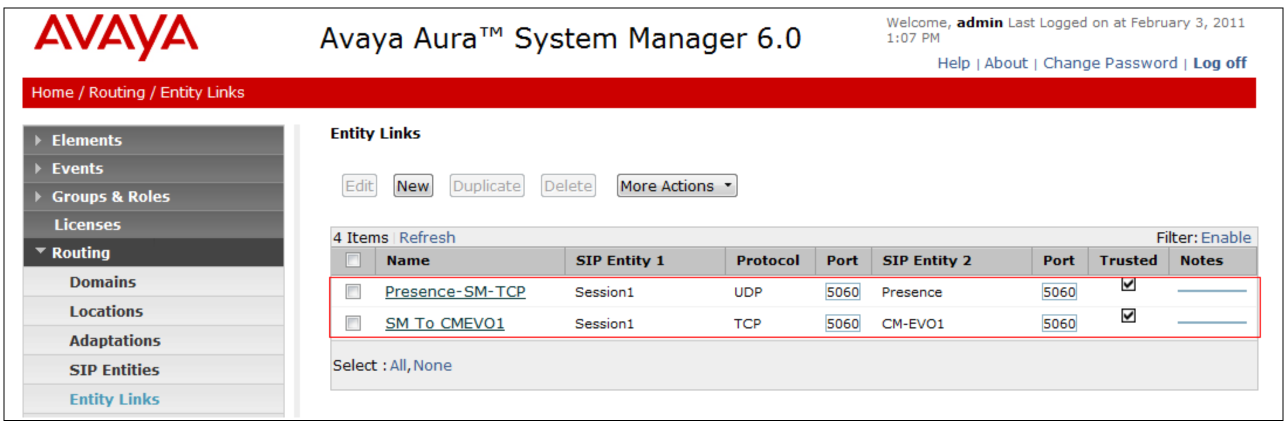


6.5 Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Routing →Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select the Session Manager, in this case **Session1**
- In the **Port** field enter the port number to which the other system sends its SIP requests
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.4**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- Select the **Trusted** tick box to make the other system trusted
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in this configuration.

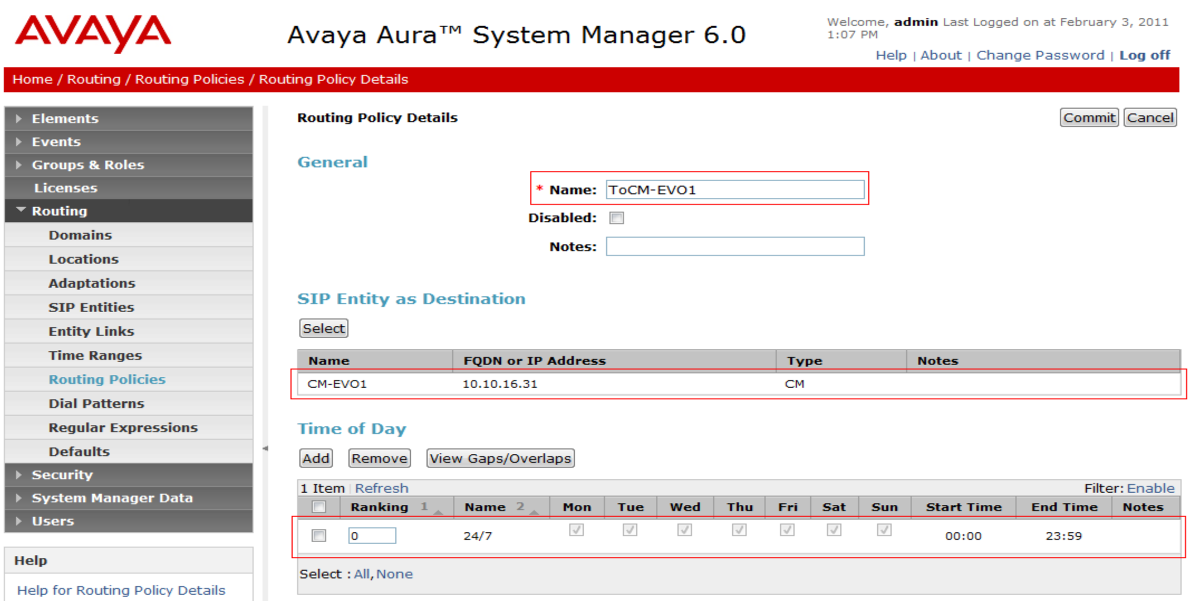


6.6 Administer Routing Policies

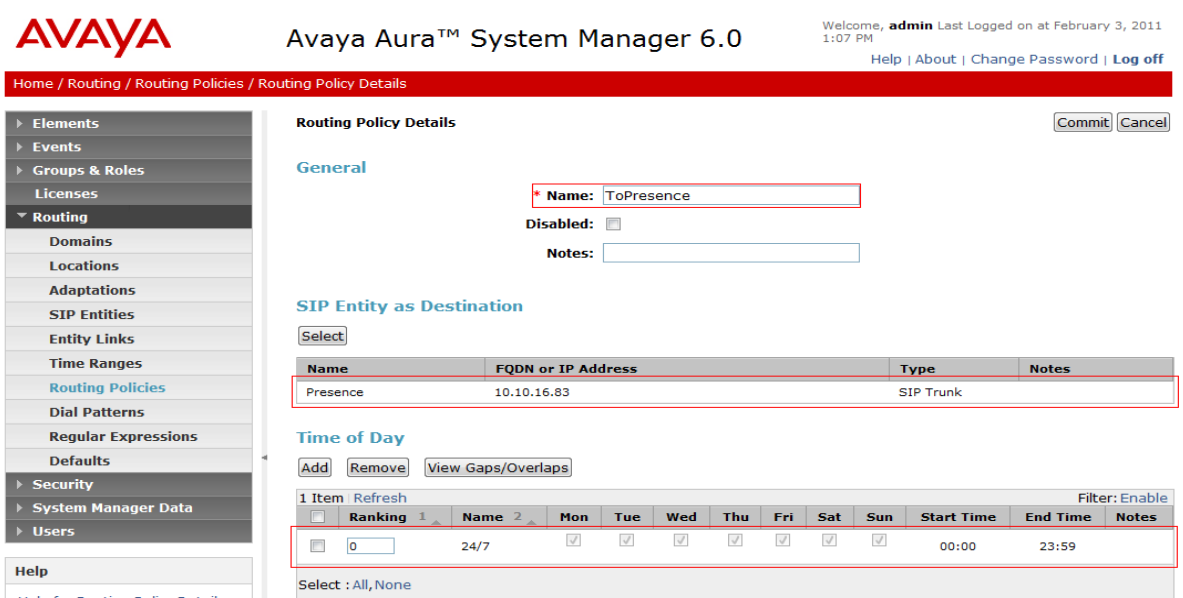
Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing → Routing Policies** on the left panel menu and then click on the **New** button (not shown).

- Under **General** enter an informative name in the **Name** field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies
- Under **Time of Day**, click **Add**, and then select the time range

The following screen shows the routing policy for Communication Manager



The following screen shows the routing policy for OpenGate.



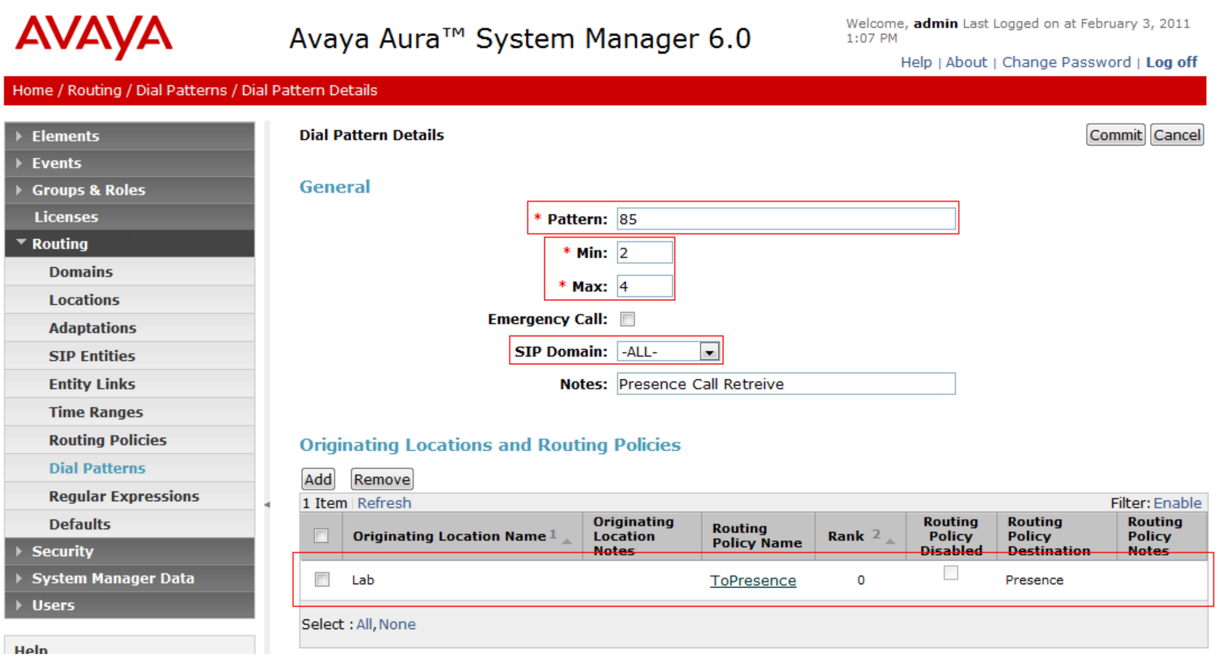
6.7 Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Routing → Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

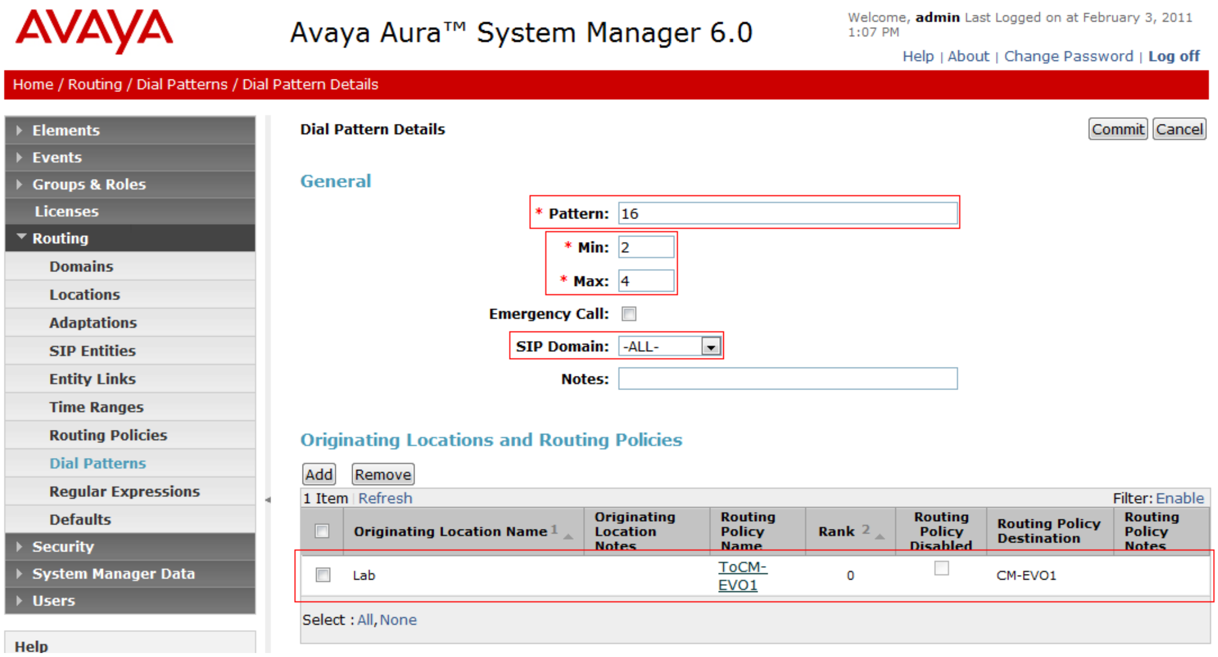
Under **General:**

- In the **Pattern** field enter a dialed number or prefix to be matched
- In the **Min** field enter the minimum possible length of the dialed number
- In the **Max** field enter the maximum possible length of the dialed number
- In the **SIP Domain** field select **ALL**

Under **Originating Locations and Routing Policies** Click **Add**, in the resulting screen (not shown) Under **Originating Location** select **Lab** and under **Routing Policies** select one of the routing policies defined in **Section 6.6.** Click the **Commit** button to save. The following screen shows an example dial pattern configured for OpenGate.



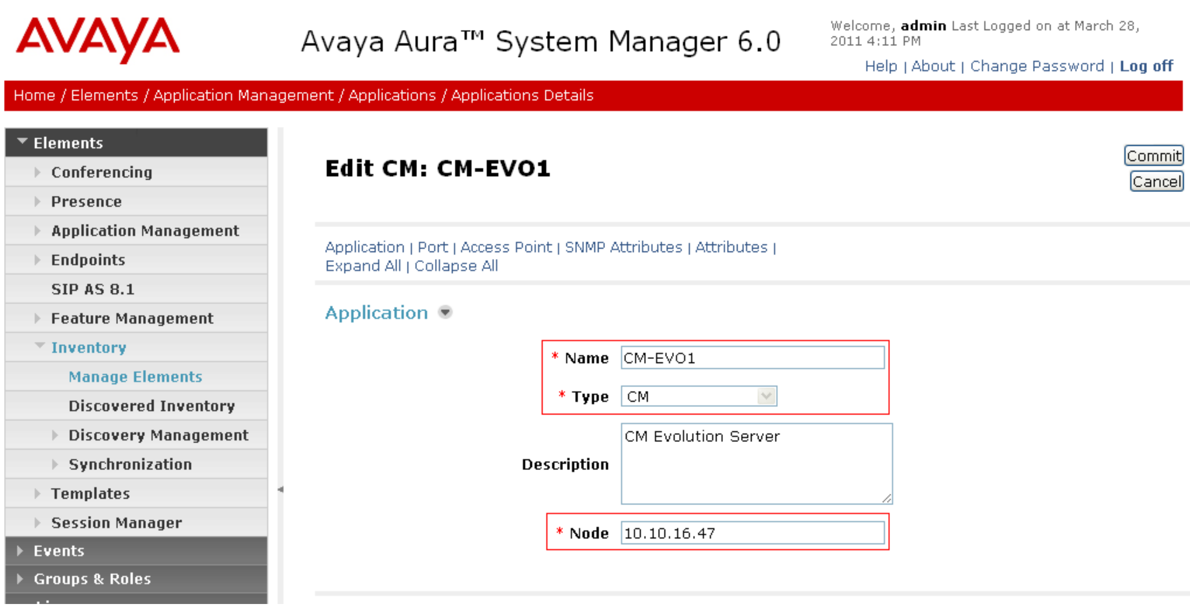
The following screen shows an example dial pattern configured for the Communication Manager.



6.8 Administer Avaya Aura® Communication Manager as a Managed Element

From the left panel menu select **Elements → Inventory → Manage Elements** and click **New** (not shown)**.** Under the **Application** heading, enter values in the following fields:

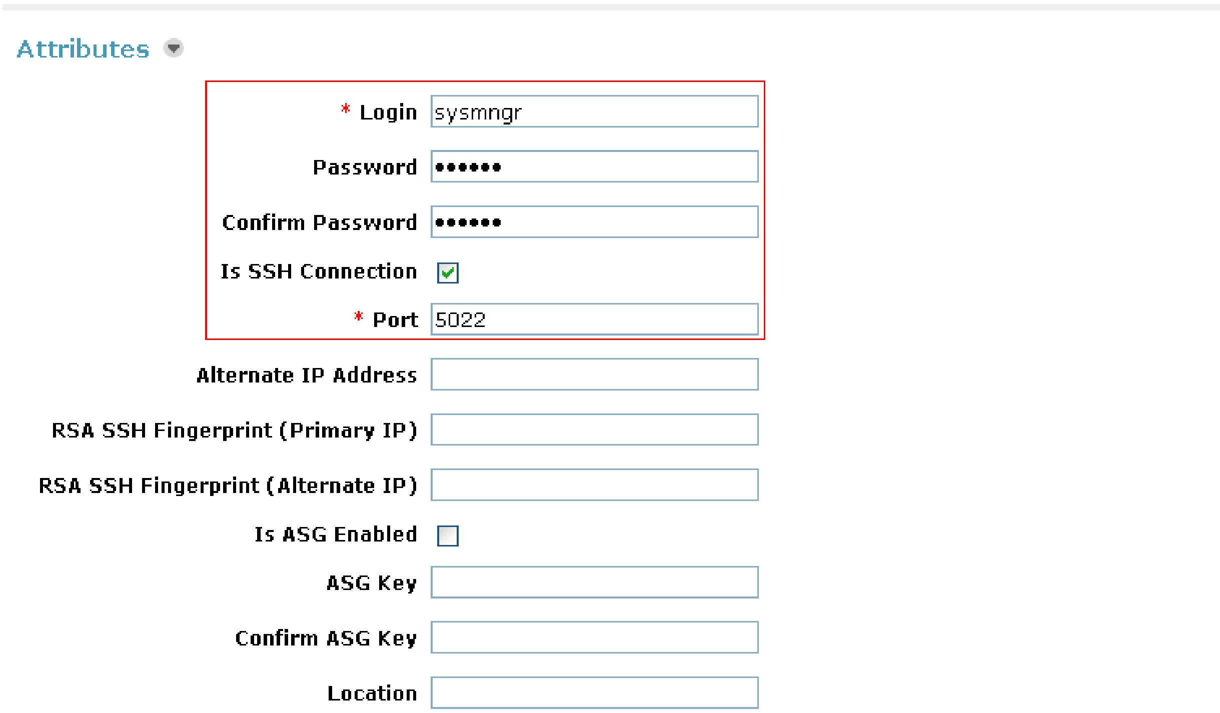
- In the **Name** field enter a descriptive name
- In the **Type** field select CM from the drop-down menu
- In the **Node** enter the IP address of the Communication Manager SAT interface



Scroll down the page and under the **Attributes** heading, enter values in the following fields. Use defaults for the remaining fields:

- In the **Login** field enter a login name for Communication Manager (SAT SSH login)
- In the **Password** and **Confirm Password** fields enter the Password for Communication Manager (SAT SSH password)
- Select the **Is SSH Connection** check box if SSH is to be used
- In the **Port** field enter the port number to use for SAT access

Select **Commit** (not shown). This causes System Manager to synchronize with the Communication Manager in the background.

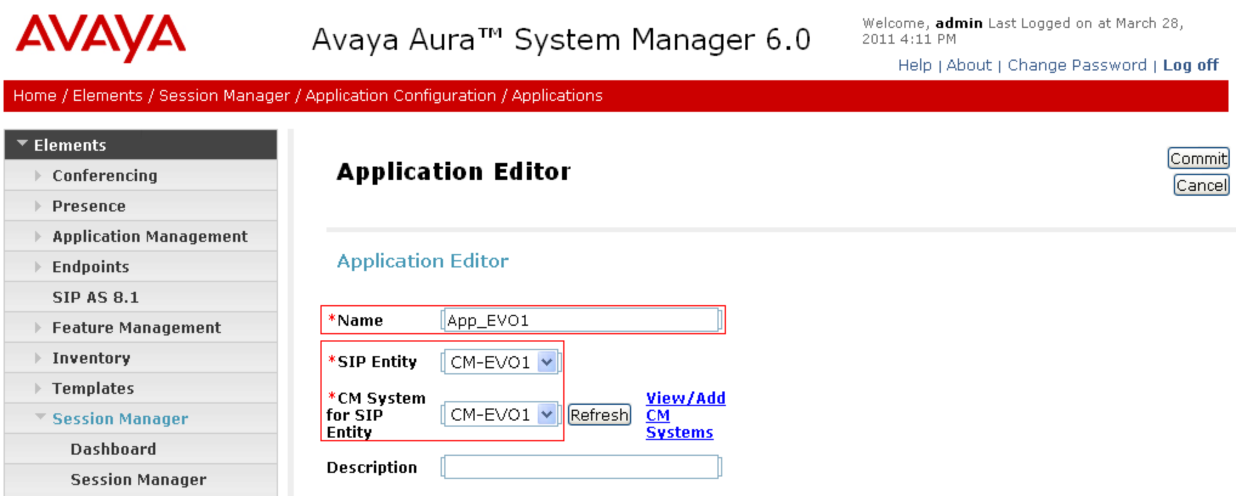


6.9 Administer Application for Avaya Aura® Communication Manager

From the left panel menu select **Elements → Session Manager → Application Configuration → Applications** and click **New** (not shown).

- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for the Communication Manager.
- In the **CM System for SIP Entity** field select the SIP entity for the Communication Manager.

Select **Commit** to save the configuration.

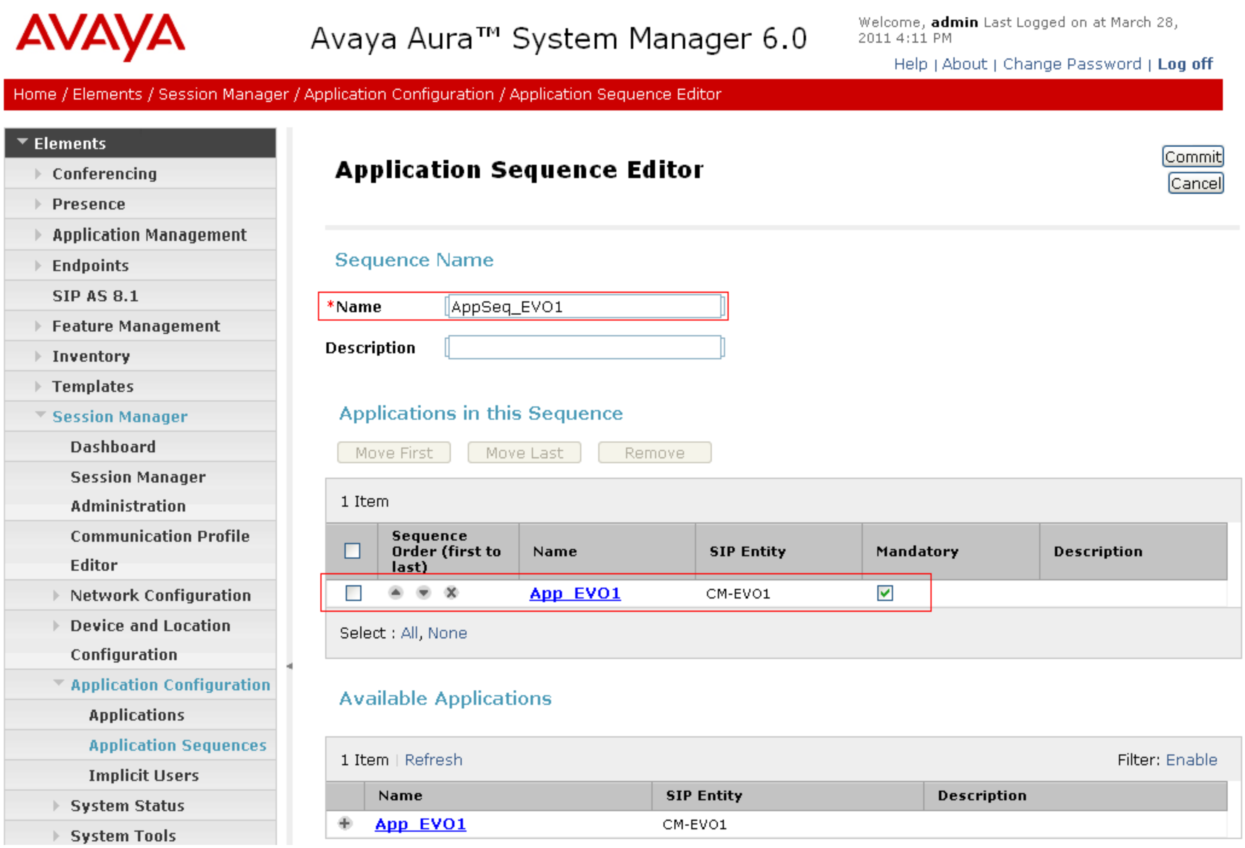


6.10 Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Elements** → **Session Manager** → **Application Configuration** → **Application Sequences** and click on **New** (not shown).

- In the **Name** field enter a descriptive name
- Under **Available Applications**, click the + sign in front of the appropriate application instance. When the screen refreshes the application should be displayed under the **Applications in this Sequence** heading.

Select **Commit** to save the configuration



7. Configure the Presence OpenGate

Presence OpenGate is part of Presence Suite and is administered via Presence Administrator. A number of items are set up within Presence Administrator to configure the OpenGate ACD. This section will cover the following areas:

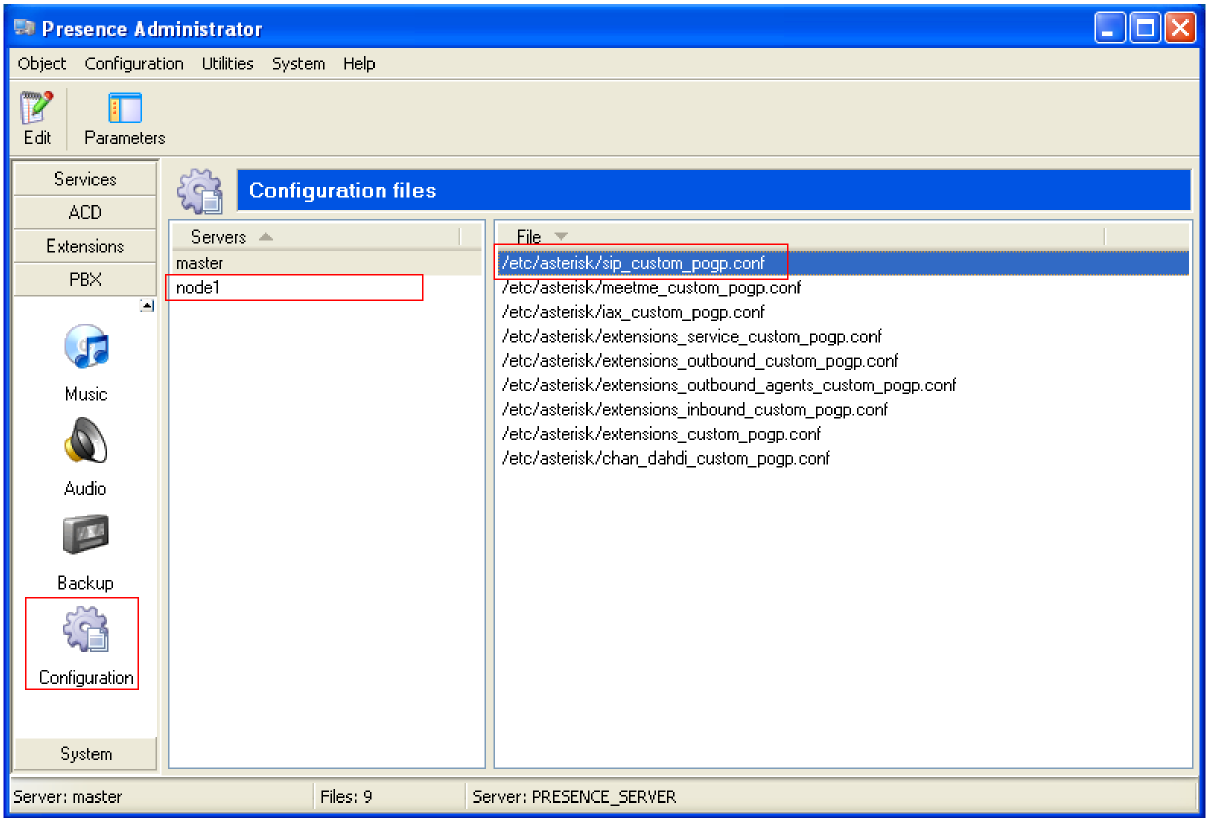
- Login to Presence Administrator
- Administer SIP trunk to Avaya Aura® Session Manager
- OpenGate Skill Configuration
- OpenGate Agent Login Configuration
- OpenGate Station Configuration
- OpenGate Service Configuration
- Outbound Routes
- Inbound Routes
- Logging in to OpenGate

7.1 Login to Presence Administrator

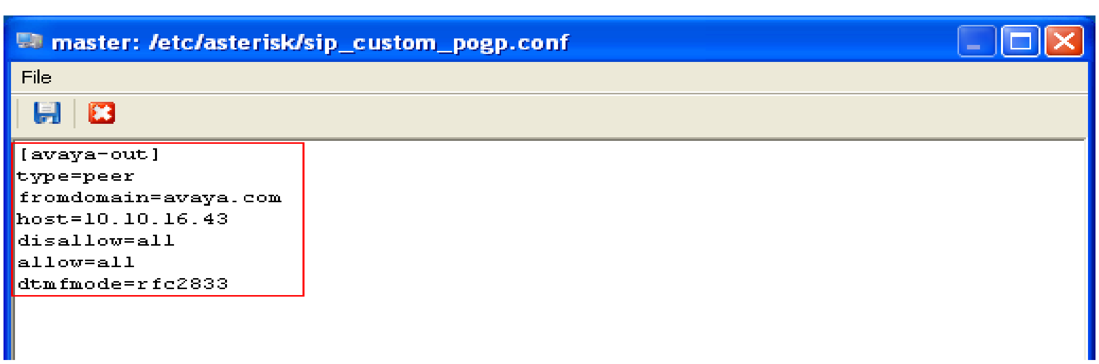
Launch the Presence Administrator application by double clicking the **pcoadmin.exe** located in the Presence folder. The username and password that appear in the **User** and **Password** fields are created during the Presence Server installation.

7.2 Administer SIP Trunk to Session Manager

From the left hand menu navigate to **PBX →Configuration** and in the right hand window select the presence server to configure (in this case it is called **node1**) and then open the file **/etc/asterisk/sip_custom_pogp.conf.**

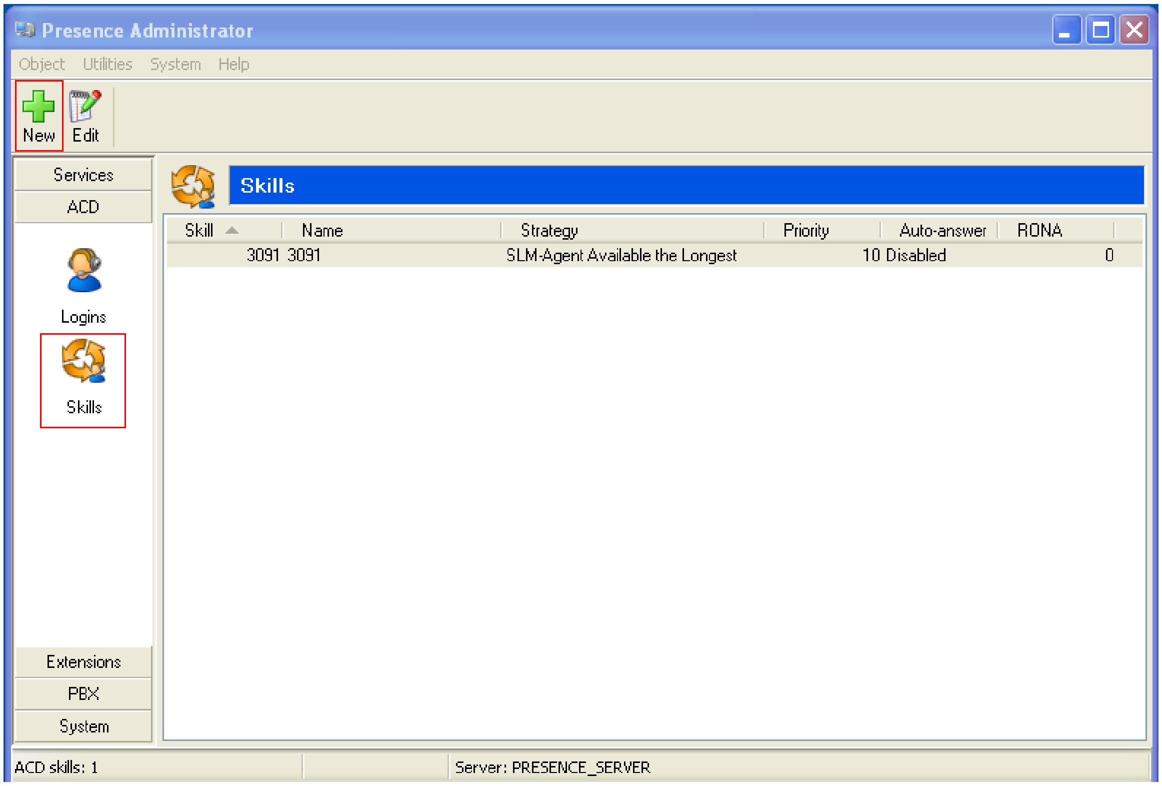


In the resulting window define the SIP trunk connection to Session Manager. At the top of the screen define a name for the connection within square brackets, in this example **[avaya-out]** is used by setting the **type** to **peer.** The **fromdomain** is set to the Session Manager domain defined in **Section 6.2.** The **host** field should be set to the IP address of the SIP interface on Session Manager. The **dtmfmode** field should be set to **rfc2833** to match the Communication Manager Signaling Group setting for DTMF transmission in **Section 5.4.** All remaining fields can be left with their default values. Click **OK** to save changes (not shown).

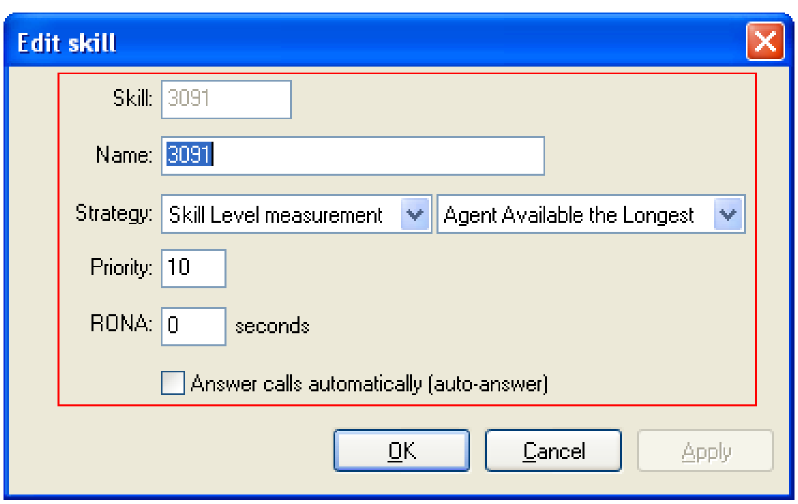


7.3 OpenGate Skill Configuration

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

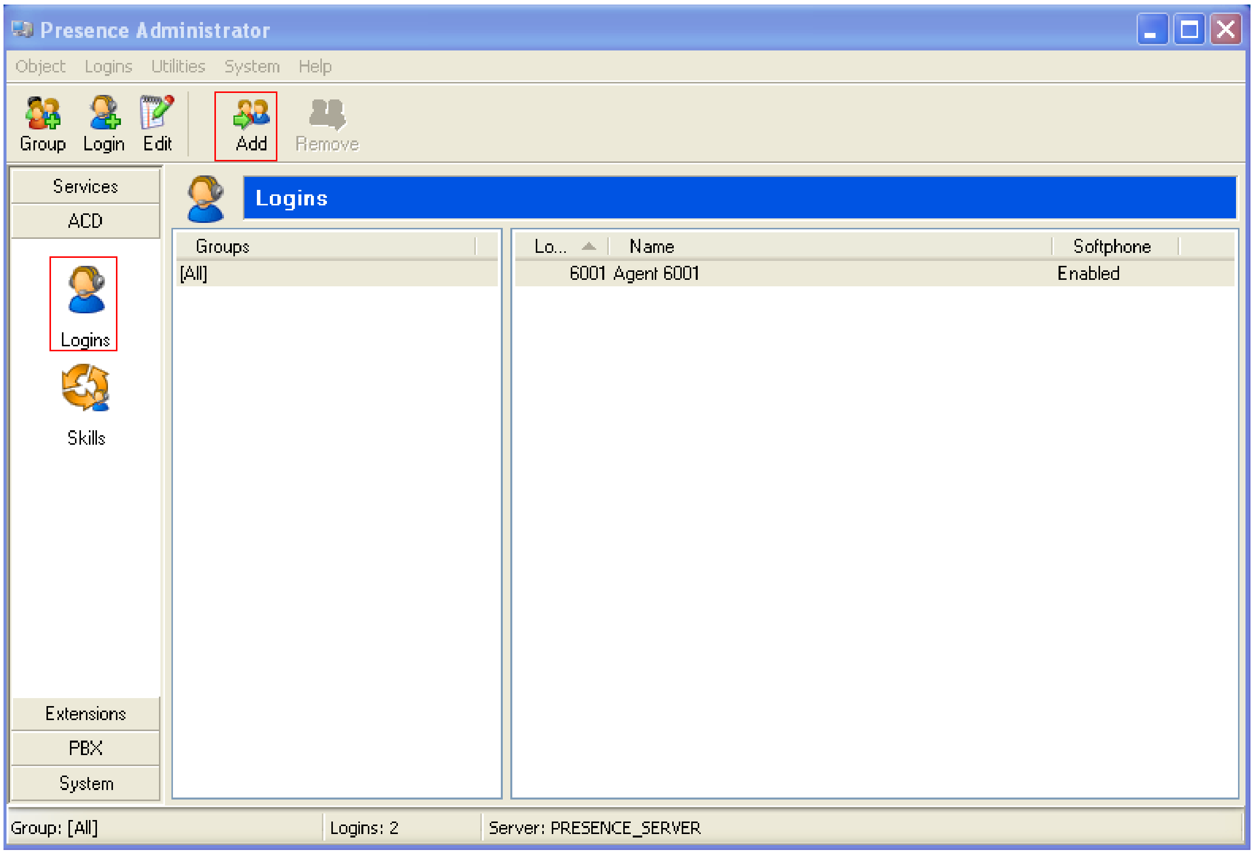


In the resulting screen define a **Skill** number and enter a **Name** to identify the skill. In the **Strategy** field use the two drop down menus to define the selection strategy that will be used by the skill. Set a **Priority** for the skill. All remaining fields can be left with default values.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

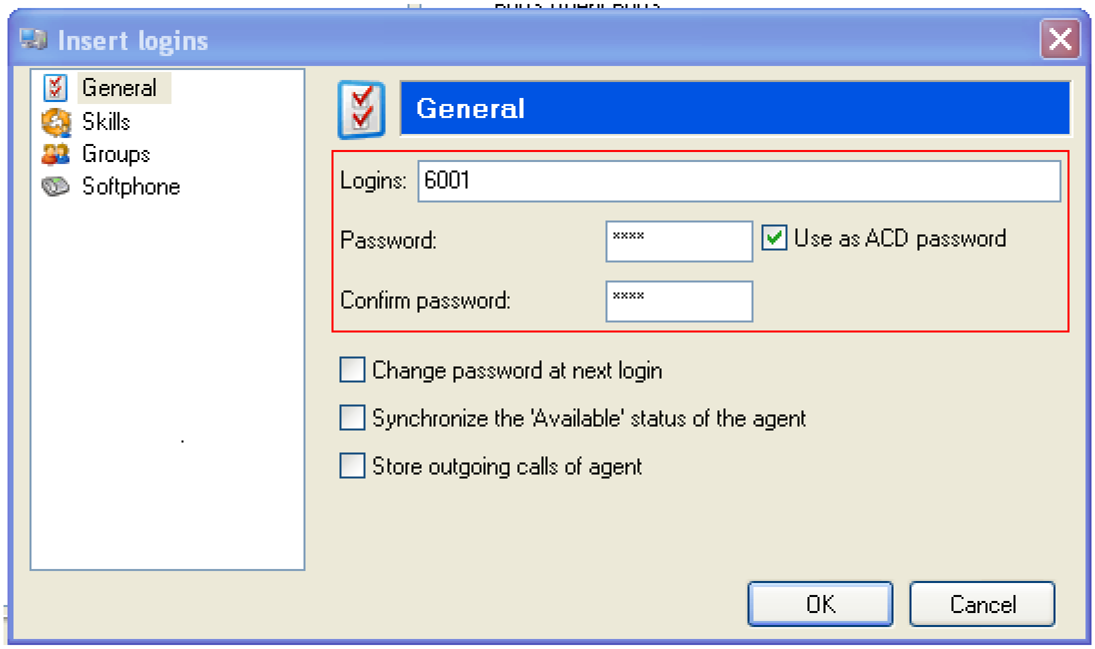


7.4 OpenGate Agent Login Configuration

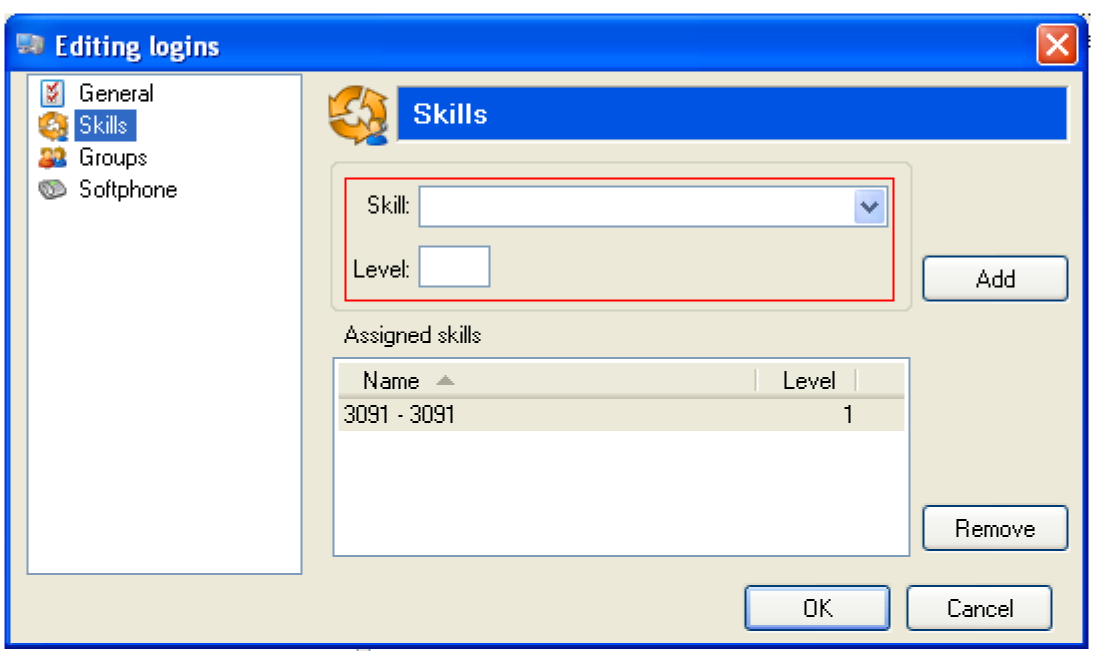
The login configured here will be used by the agent to login to OpenGate. The Agents will connect to OpenGate via the Presence Suite Agent application. To configure an ACD agent login, from the left hand side select **ACD → Logins** from the Presence Administrator main menu. Click the **Add** button.



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. Select the **Use as ACD password** check box.

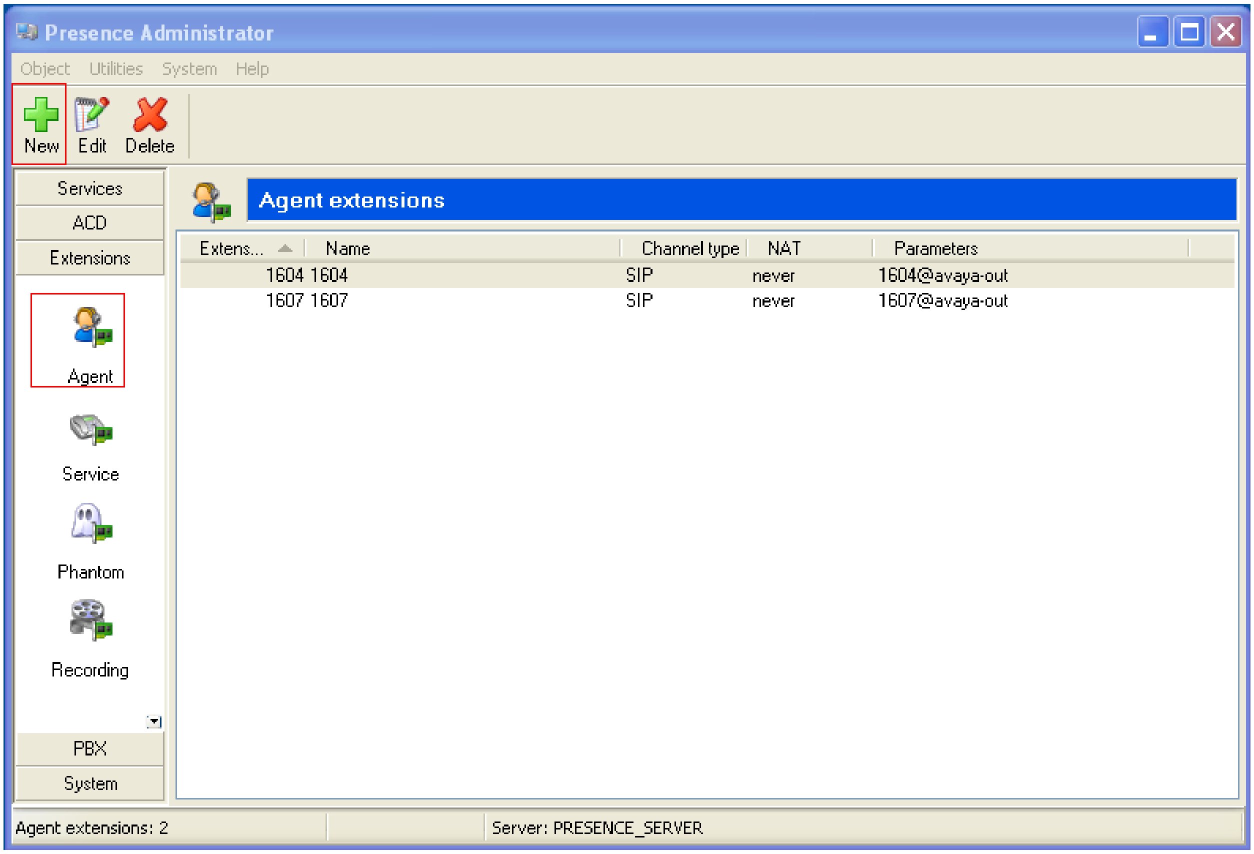


From the menu on the left side of the screen select **Skills,** use the drop down menu to select the **Skill** configured in **Section 7.3** and specify a **Level** for the skill to be applied against this agent login. Click the **Add** button and the skill should appear under **Assigned skills**. Click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

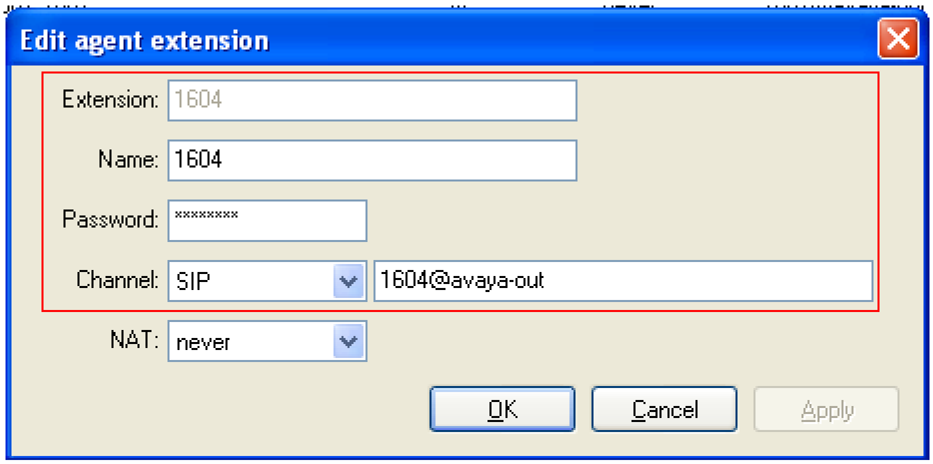


7.5 OpenGate Station Configuration

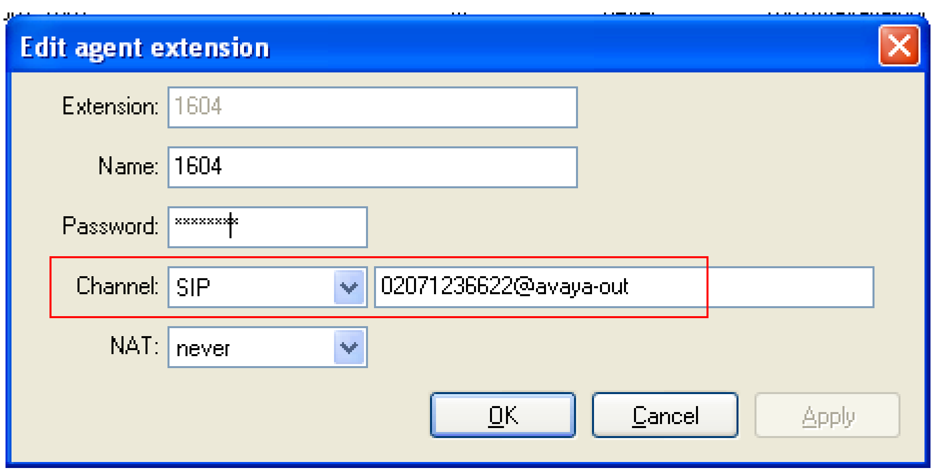
Each telephone/endpoint that OpenGate could route calls to must be defined within Presence Administrator as an Agent extension. To define an Agent extension from the left hand side navigate to **Extensions → Agents** and click the **New** button.



In the resulting screen specify an **Extension** number that will be used to configure the presence Suite Agent application **(Section 7.9.1)**. Set a **Name** that the Agent extension will be known as. It is recommended that the **Password** field is set, the password will only be required if an endpoint is to be registered directly with OpenGate. 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 1604 will be dialled using trunk avaya-out so the URI is formatted as **1604@avaya-out**.

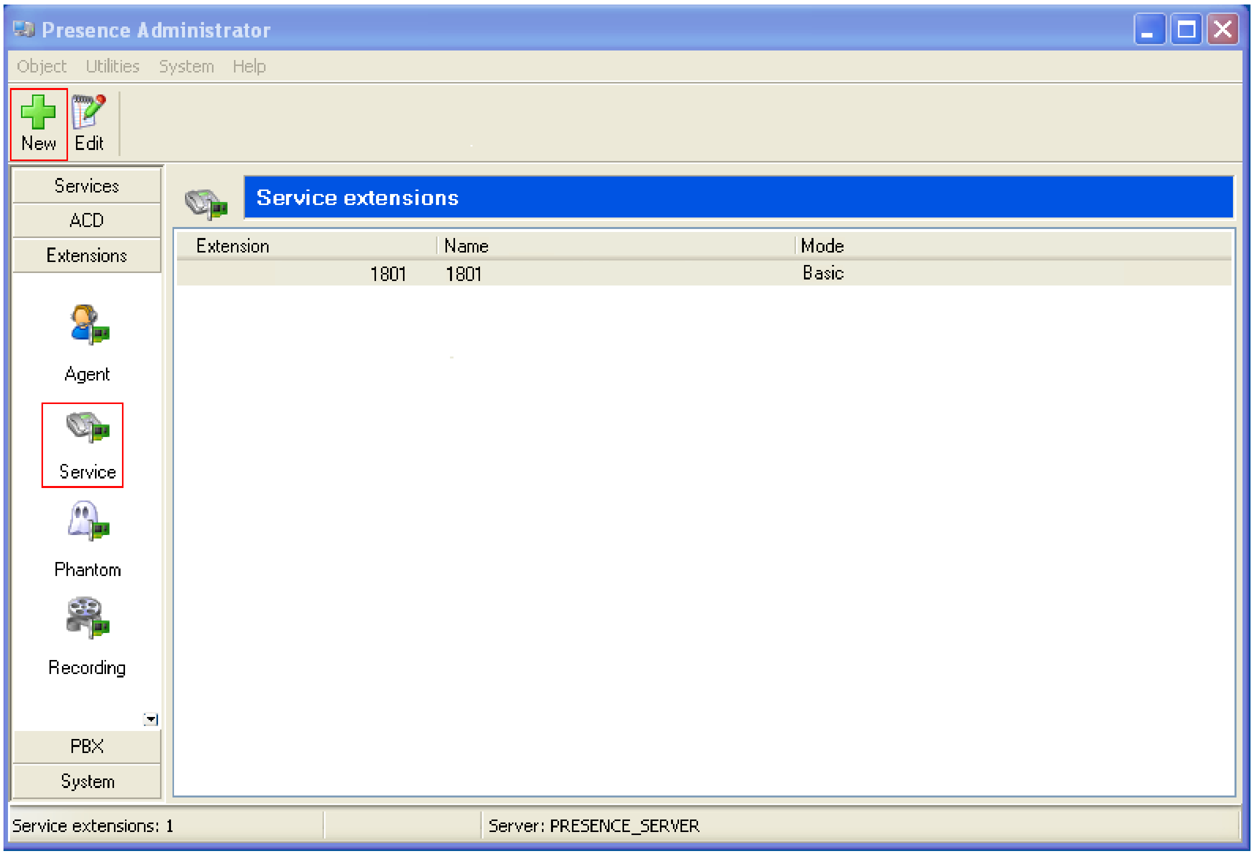


If the agent station can not be dialed locally by OpenGate (e.g. the agent is using a home phone on the PSTN) then the **Channel** can be configured to dial another number. To illustrate this, the screen below shows a DDI number configured to reach agent extension 1604. When OpenGate wants to deliver a call to agent extension 1604, it will dial 02071236622 using SIP trunk avaya-out, so the URI is formatted as **02071236622@avaya-out.**

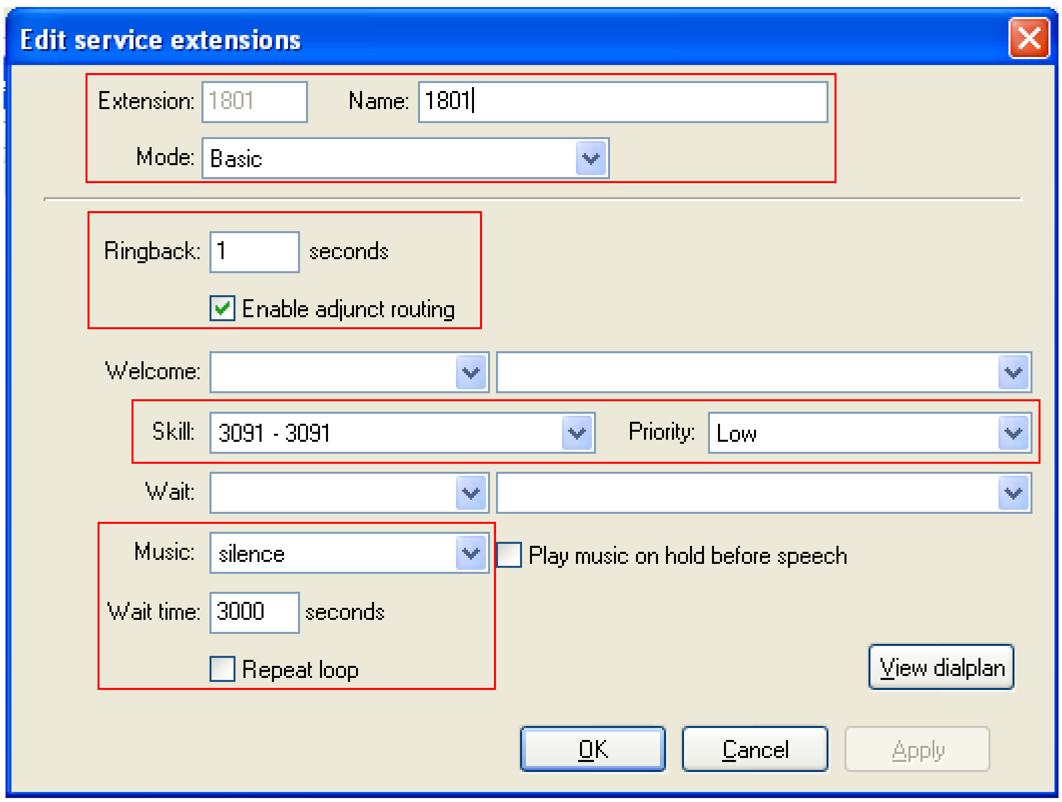


7.6 OpenGate Service Configuration

Service extensions are used to route calls to a skill and to provide call treatment such as welcome announcements to incoming calls. To define a Service extension, from the left hand side navigate to **Extensions → Service** and click the **New** button.



In the resulting window enter an **Extension** and **Name** for the service and using the drop down menu select **Basic** for the **Mode** field. The **Ringback** field defines in seconds the amount of time a caller will hear ringing before receiving any other treatment. Select the **Enable adjunct routing** check box, this allows calls in to this service to pass call control to other applications such as the call capturing feature provided by Presence Suite. See **Section 10** for details of this and other functions provided by presence suite. For **Skill** use the drop down menu to select the skill configured in **Section 7.3**. Select a Priority for the service to deliver the call to the skill, the default value for this field is **Medium**,. The example below uses a priority of **Low. The Music** field is used to define a category of music that can be played to callers while they are waiting for their call to be answered. In the example below no music is played so a value of **silence** is used. **Wait time** is set to the maximum amount of time a call will remain in queue without being answered, and if this threshold is reached before the call is answered then the call will be disconnected unless the **Repeat loop** check box is selected.



7.7 Outbound Routes

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

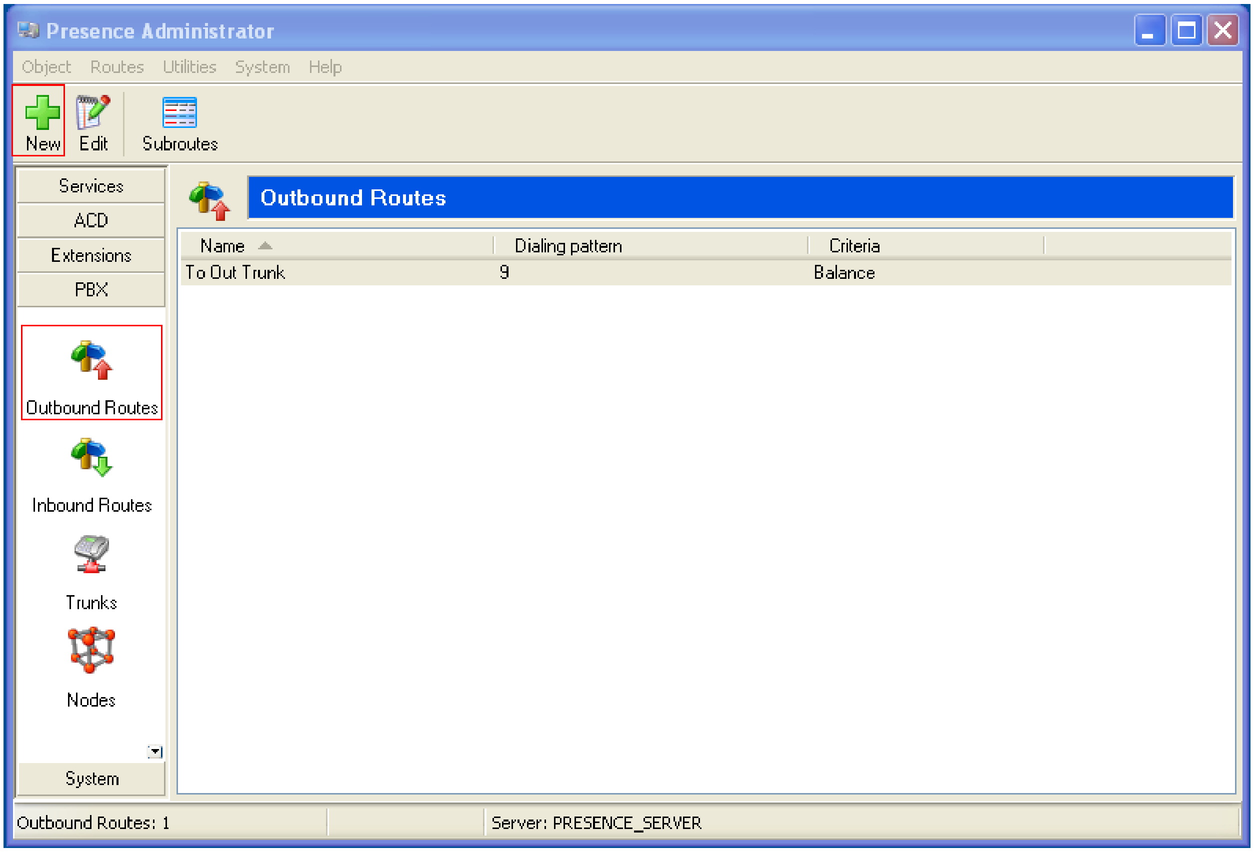
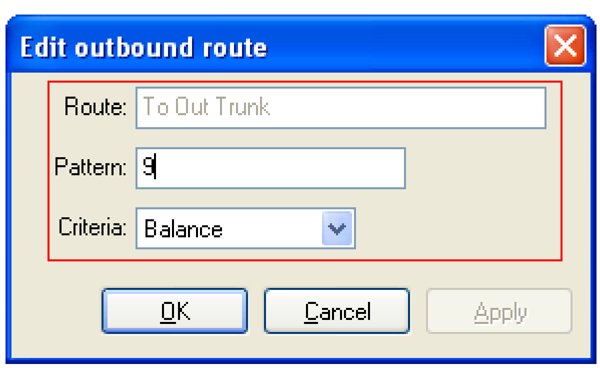
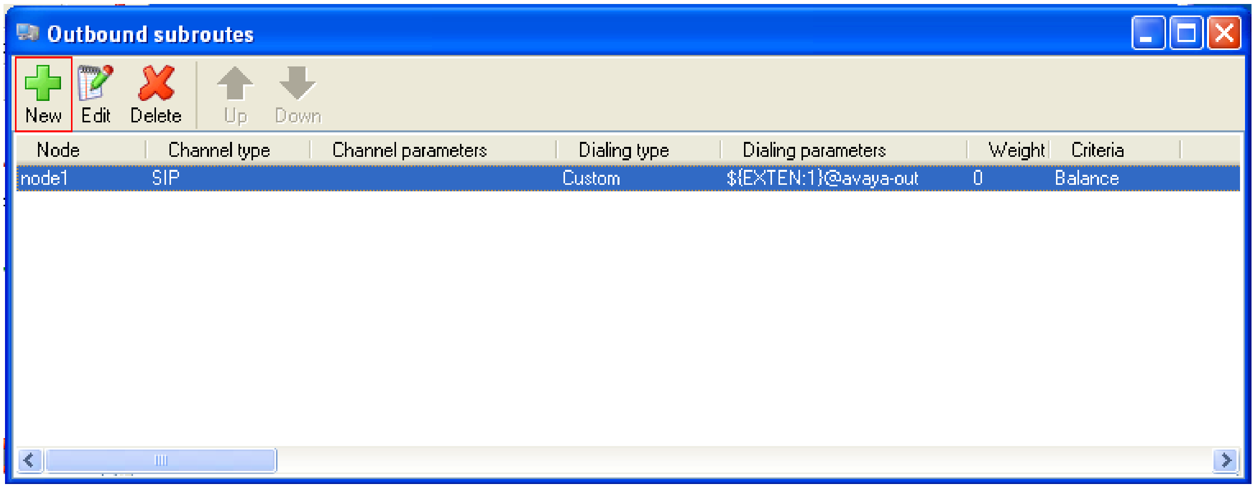


Figure 2: Outbound Routes Main Page

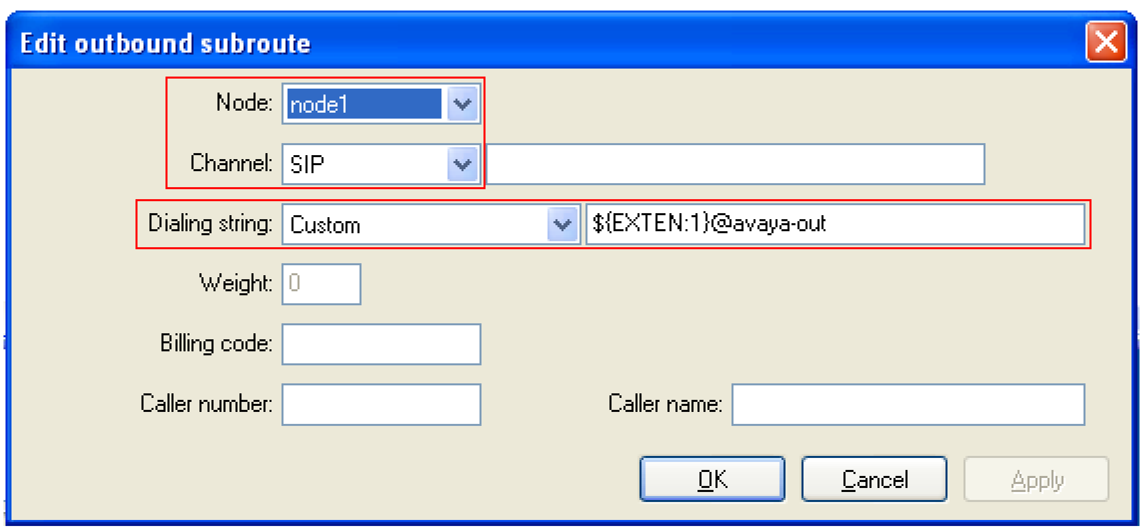
In the resulting screen enter a descriptive name in the **Route** field and in the **Pattern** field define any prefix required by outbound calls (e.g. **9** is the ARS code used on Communication Manager). For **Criteria** use the drop-down menu to select the method that will be used to distribute calls 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 in **Figure 2**) 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**.

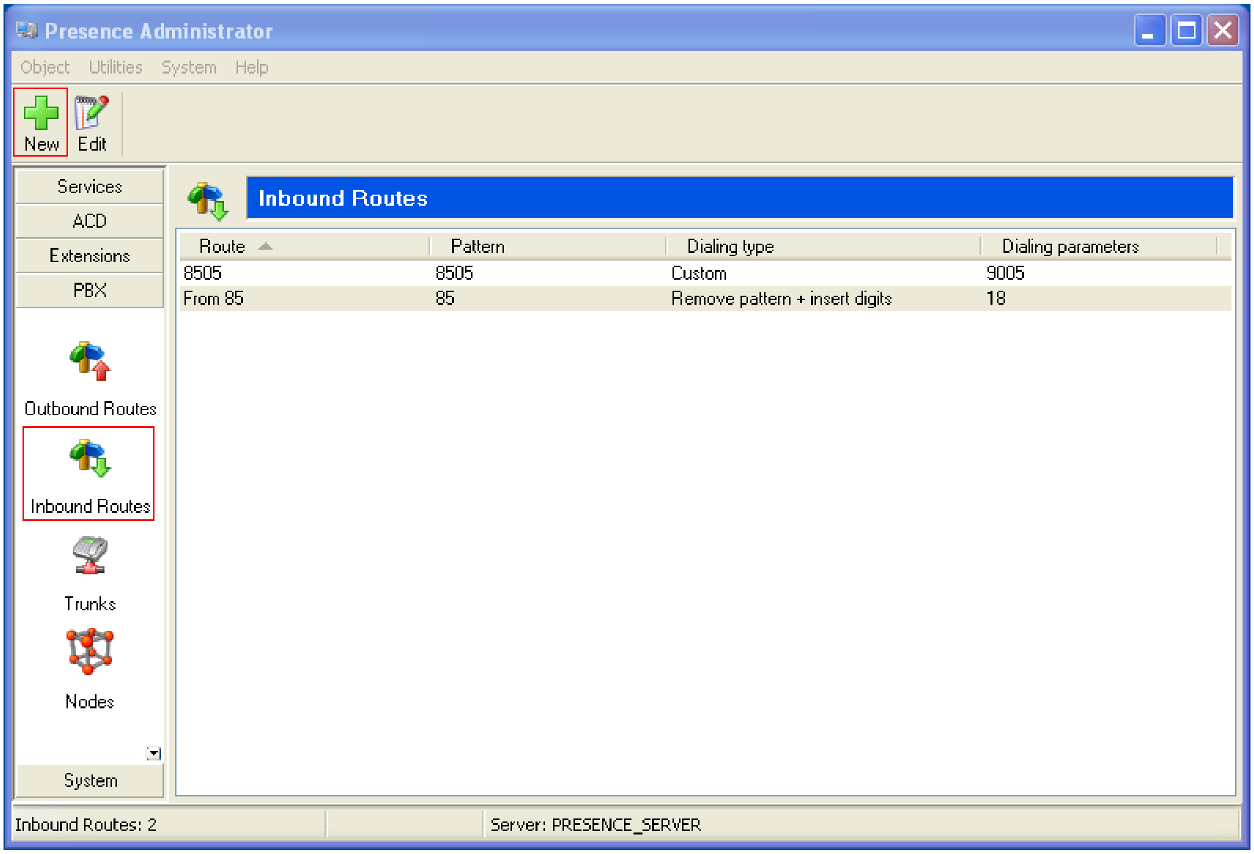


In the resulting window select the relevant Node, under channel select the appropriate connection type. For **Dialing string** use the drop down menu to select **Custom** and in the secondary field enter a matching pattern using a regular expression. In the example below the expression used is **${EXTEN:1}@avaya-out**. 'EXTEN' is an internal variable which represents the called number therefore this pattern will match any called number beginning with a 1 (e.g. 1801) and route it via the avaya-out trunk defined in **Section 6.2**.

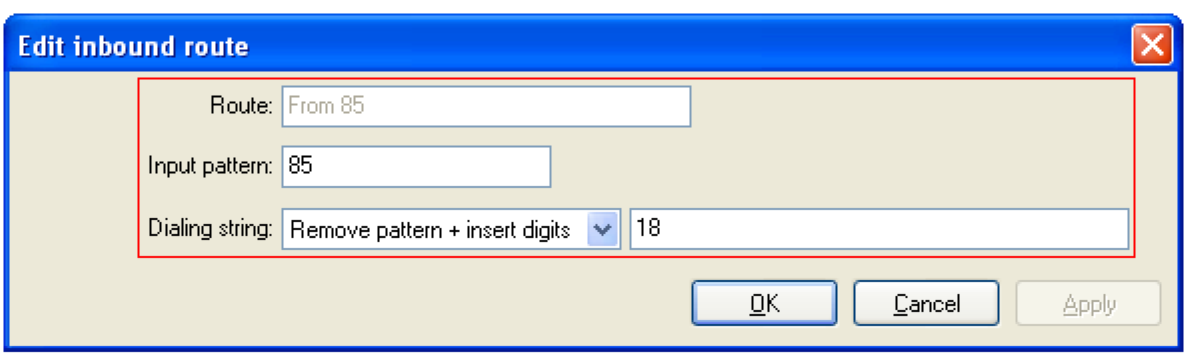


7.8 Inbound Routes

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 below example incoming digits 85 will be replaced with 18, this will match digits 8501 being received from Communication Manager and convert to 1801 which is the internal Service extension used within OpenGate.

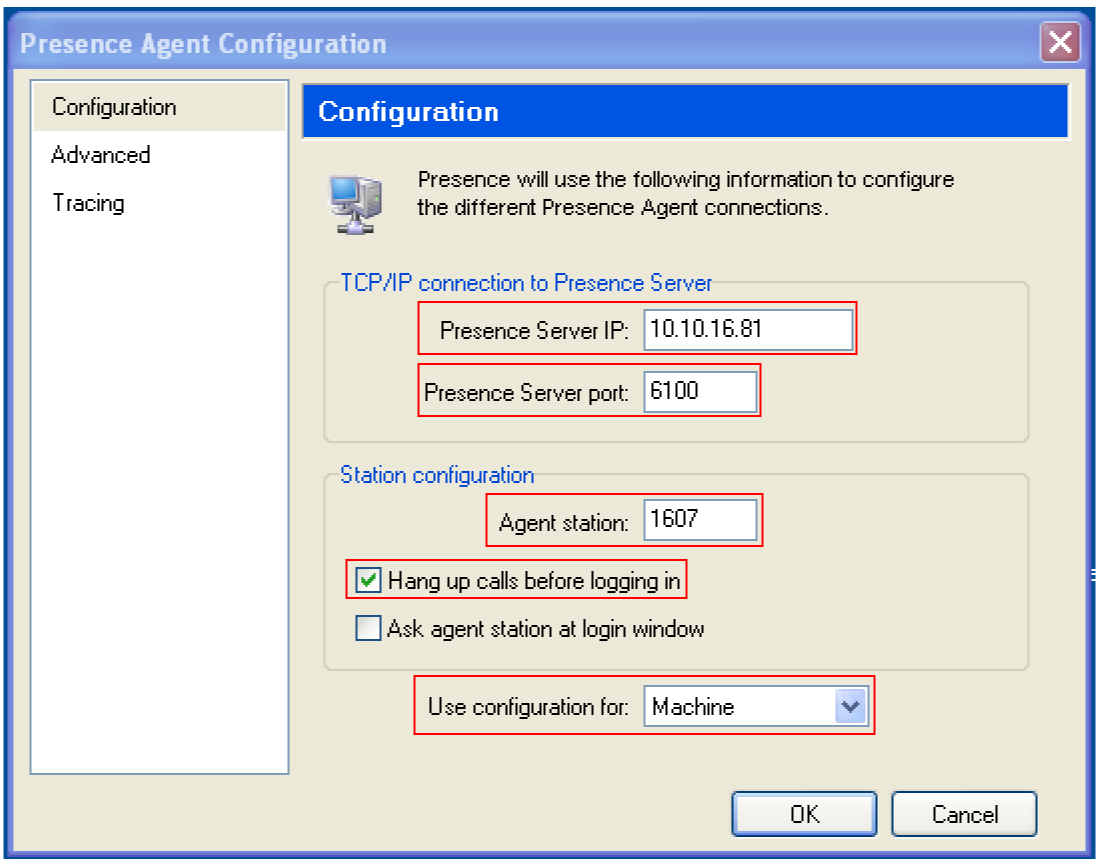


7.9 Logging into OpenGate

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.

7.9.1 Presence Agent Configuration

The following steps are carried out on the Presence Suite Agent PC. Prior to installing the Presence agent, ensure that the DBExpress driver (dpexpoda.dll) is located in the **C:\Windows\System32** directory. 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. Enter the **Presence Server IP** address as **10.10.16.81**. 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.

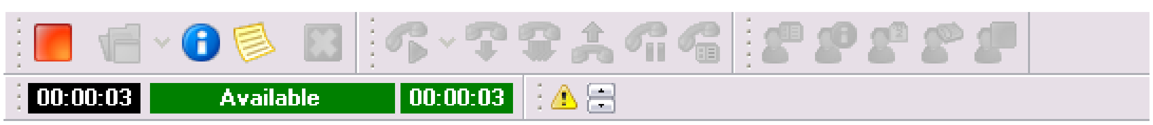


7.9.2 Logging in Presence Agent

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.

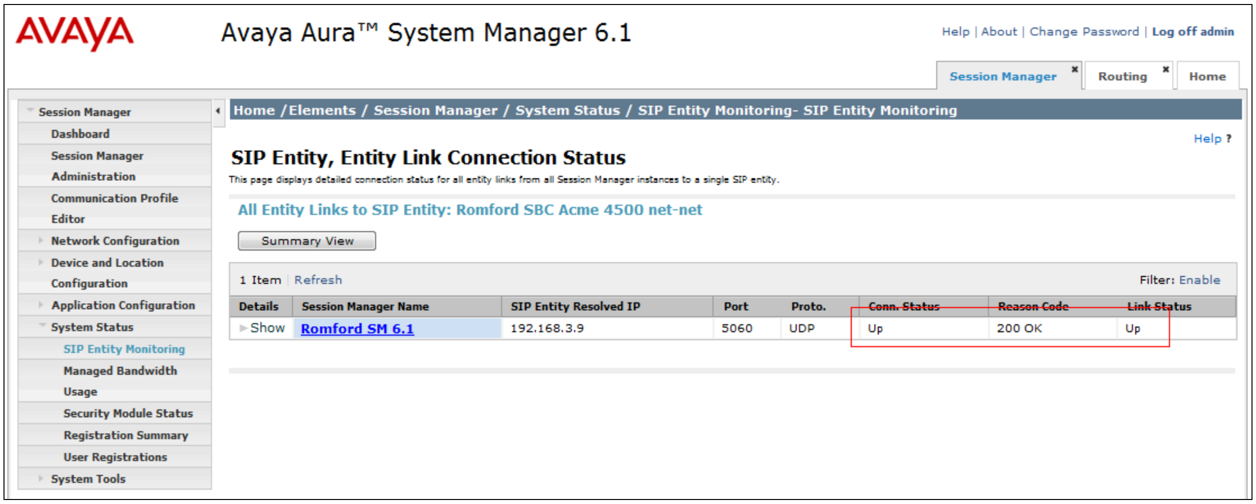
The information status on the task bar goes to available indicating the agent is ready to receive calls.



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 5

                             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. Verify that calls can be placed to OpenGate and routed to Agents.

9. Conclusion

These Application Notes describe the configuration steps required for Presence Technology OpenGate 8.1 to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. 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, Document No. 03-300509, May 2009
2. Administering Avaya Aura® Session Manager, Document No. 03-603324 ; February 2011

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

1. ACD Sys Presence Administrator Manual Presence Suite, V8.0
2. Presence Installation Guides Presence Software, V8.0
3. PBX/ACD Requirements Presence Software, V8.0

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.