Avaya Solution & Interoperability Test Lab

Application Notes for configuring Enghouse Presence OpenGate R12.1 to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Enghouse Presence OpenGate to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Enghouse Presence OpenGate provides ACD and CTI capabilities to companies without the requirement of existing CTI or ACD capabilities on their PBX. Enghouse Presence OpenGate integrates with the Avaya solution using SIP trunks and digit manipulation.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect Compliance Testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration used to verify Enghouse Presence OpenGate R12.1 can successfully interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1. Presence OpenGate can be used as an external Automatic Call Distribution (ACD) routing engine and IVR as well as a trunk gateway between the PSTN and an existing PBX, such as Avaya Aura® Communication Manager.

Presence OpenGate replaces the requirement for a CTI connection using Avaya Aura® Application Enablement Services specifically for Enghouse Presence Suite, by utilizing a SIP connection to Avaya Aura® Session Manager used to route calls to the Avaya Aura® Communication Manager endpoints in order to connect incoming "contact center" type calls. Presence Suite makes use of Presence OpenGate and the connection to Avaya Aura® Session Manager to deliver calls to Avaya endpoints that are associated with Presence Agent. The Presence Suite includes the Presence Server, Presence Mail Interactions Server, Presence Web Interactions Server, Presence Unified Manager and Presence Agent. Please note that these Application Notes only describe the setup required to add Enghouse Presence OpenGate. All the routing and intelligence takes place on Presence OpenGate. The only configuration required on the Avaya setup is a SIP trunk to allow the OpenGate call to Avaya phone/endpoints to facilitate agents speaking to the incoming calls. The setup of Enghouse Presence Suite is outside the scope of these Application Notes, please contact Enghouse for any information on the setup of Presence Suite.

2. General Test Approach and Test Results

Testing was performed manually by dialing numbers that were configured to route to Presence OpenGate and receive ACD treatment provided by Presence OpenGate. 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. OpenGate is capable or other services such as Web Chat and Email but does not utilize the Avaya phones for such functions and so was not tested. Functionality testing included basic telephony operations such as answer, hold/retrieve, transfer, and conference. The serviceability test cases were performed manually by busying out and releasing the SIP trunk and by disconnecting and reconnecting the LAN cables. Link Failure\Recovery was tested to ensure successful reconnection on link failure.

For the sample configuration discussed in this document, all calls received from the PSTN by Communication Manager were routed via a SIP Trunk to Session Manager. Session Manager is then responsible for routing the call to Presence OpenGate to receive ACD treatment. Presence OpenGate can route calls to Presence agents served by Avaya endpoints. Note that two Presence Agents were used for compliance testing one associated with an Avaya H.323 IP Phone and another associated with an Avaya SIP phone. This allowed the testing of transfer, conference as well as testing both Avaya IP phones.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by

DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

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

2.1 Interoperability Compliance Testing

In the sample configuration described by these Application Notes, calls will be accepted from the PSTN and routed to Presence OpenGate. Presence OpenGate will then map these digits to an internal number which represents the ACD service queue within Presence OpenGate. Presence OpenGate then routes the call to an available Avaya endpoint by dialing that station extension number. There is no configuration required on Communication Manger other than the setup of a SIP trunk to allow calls from OpenGate to the Avaya endpoints. When incoming calls are made to a service these calls are routed to OpenGate where they are processed and OpenGate then calls to an Avaya endpoint and merges the calls.

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 Avaya endpoints. The serviceability testing focused on verifying the ability of Presence OpenGate to recover from adverse conditions, such as disconnecting the Ethernet cable from the server.

2.2 Test Results

All test cases passed successfully, with the following observation.

When doing a transfer to either an Avaya endpoint or another PSTN the transfer-to party display is not updated after the transfer is completed. This is only the case for the Supervised Transfer as Blind Transfer works as expected and the PSTN callers ID is passed onto the transfer-to correctly. Enghouse are investigating the issue.

2.3 Support

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

- Email: *Presence.Support@enghouse.com*
- Website: *https://www.enghouseinteractive.es/en*
- Phone: +34 93 10 10 300

3. Reference Configuration

Figure 1 shows the network topology in place during compliance testing. Communication Manager and an Avaya G430 Media Gateway were used as the hosting PBX. SIP trunks are configured between Communication Manager, Session Manager and Presence OpenGate to transport calls between them.

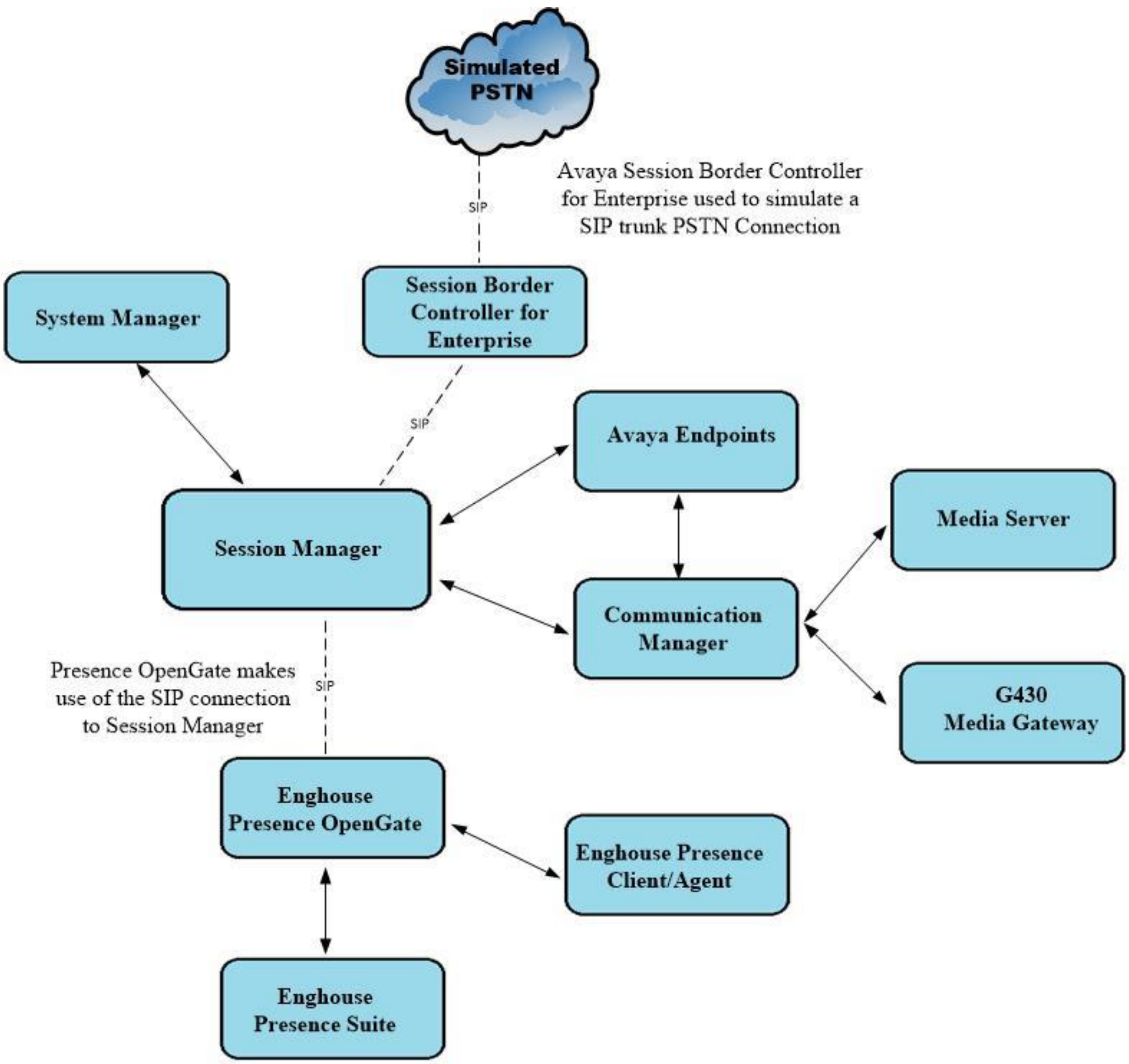


Figure 1: Network Topology used to test Enghouse Presence OpenGate R12.1 with Avaya Aura® Session Manager R8.1 and Avaya Aura® Communication Manager R8.1

4. Equipment and Software Validated

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

Avaya Equipment	**Software / Firmware Version**
Avaya Aura® System Manager running on a virtual server	8.1.3.2 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.2.1012646 Service Pack 2
Avaya Aura® Session Manager running on a virtual server	8.1.3.2 Build No. – 8.1.3.2.813207
Avaya Aura® Communication Manager running on a virtual server	8.1.3.2 – FP3SP2 R018x.01.0.890.0 Update ID 01.0.890.0-26989
Avaya Aura® Media Server	8.0.2.184
Avaya G430 Media Gateway	41.16.0/1
Avaya J179 H.323 Deskphone	6.8502
Avaya J189 SIP Deskphone	4.0.10.1.2
Avaya 9408 Digital Deskphone	V2.0
Enghouse Equipment	**Software / Firmware Version**
Enghouse Presence Suite running on Windows Server 2019 Server	R12.1
Enghouse Presence OpenGate running on Windows Server 2019 Server	R12.1
Enghouse Presence Client running on Windows 10	R12.1

Table 1: Hardware and Software Version Numbers

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. Please note outlined are the steps to add Presence OpenGate only, the setup of Presence Suite is outside the scope of these Application Notes but can be found in the Application Notes titled *Application Notes for Configuring Enghouse Presence Suite R12.1 with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1.*

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

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

Note: The configuration of the simulated PSTN is outside the scope of these Application Notes.

5.1 Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that the **Maximum Administered SIP Trunks** have sufficient capacity. Each call that receives ACD treatment from Presence 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 two 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 4**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

```
display system-parameters customer-options                      Page   4 of  12
                                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 6**, ensure that **Uniform Dialing Plan** is set to **y**.

```
display system-parameters customer-options                      Page   6 of  12
                                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 to 6300 were to be sent across the SIP trunk to Session Manager and therefore to Presence OpenGate. To achieve this routing, automatic alternate routing (aar) will be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this routing.

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

```
change dialplan analysis                                           Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 3

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

5.4 Administer Route Selection for Presence OpenGate Calls

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

```
change uniform-dialplan 6                                       Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                    Insert              Node
  Pattern       Len  Del      Digits      Net  Conv  Num
 6300            4    0                   aar   n
 65              4    0                   aar   n
                                                n
                                                n
                                                n
                                                n
                                                n
                                                n
```

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

```
change aar analysis 6                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 3
    Dialed                    Total     Route     Call   Node  ANI
    String                   Min  Max  Pattern    Type   Num   Reqd
    6                         7    7     254       aar          n
    6300                      4    4     1         lev0         n
    65                        4    4     1         aar          n
    7                         7    7     254       aar          n
    8                         7    7     254       aar          n
    9                         7    7     254       aar          n
                                                                n
                                                                n
                                                                n
                                                                n
                                                                n
```

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

```
change route-pattern 1                                            Page   1 of   3
                    Pattern Number: 1      Pattern Name: SIP TRUNK
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 1    0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            unre                               lev0-pvt  none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

5.5 Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of the **procr** and Session Manager (**SM80vmpg**). 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
                                  IP NODE NAMES
    Name              IP Address
AMS80vmpg           10.10.40.61
G450                10.10.40.14
IPOffice            10.10.40.25
NRS                 10.10.40.101
PGDECT              10.10.40.50
SM80vmpg            10.10.40.58
SM_Oceana           10.10.41.26
aes80vmpg           10.10.40.56
default             0.0.0.0
procr               10.10.40.59

( 16 of 18   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.1**. 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 codecs supported for calls routed over the SIP trunk to Presence OpenGate. The form is accessed via the **display ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), **G.711MU** (mu-law) and **G729A** which are supported by Presence OpenGate.

Media Encryption is used on the Avaya sets where possible these use **srtp-aescm128-hmac80** media encryption. **None** is also present to facilitate any extension not capable of handling encryption.

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

                          IP MEDIA PARAMETERS
    Codec Set: 1

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

     Media Encryption                 Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
```

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, **tls** (Transport Layer Security) should be used for DevConnect testing.
- The **Peer Detection Enabled** field should be set to **y** allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM80vmpg**), also shown above.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above**.** This field logically establishes the **far-end** for calls using this signaling group as network region **1**.
- The **Far-end Domain** field can be set to the domain name specified in the IP Network Region.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The default values for the other fields may be used.

Note: These were the settings for compliance testing, however, this trunk may be setup differently on each customer site depending on the customer's requirements for SIP routing.

```
change signaling-group 1                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n          Transport Method: tls
        Q-SIP? n
     IP Video? n                                    Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                  Far-end Node Name: SM80vmpg
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: devconnect.local
                                             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 Presence OpenGate. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```
change trunk-group 1                                            Page   1 of  21
                                TRUNK GROUP

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

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

```
change trunk-group 1                                            Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                           Redirect On OPTIM Failure: 5000

            SCCAN? n                              Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n




 Caller ID for Service Link Call to H.323 1xC: station-extension
```

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

```
change trunk-group 1                                            Page   4 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                      Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: shared

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

Settings on **Page 5** are as follows.

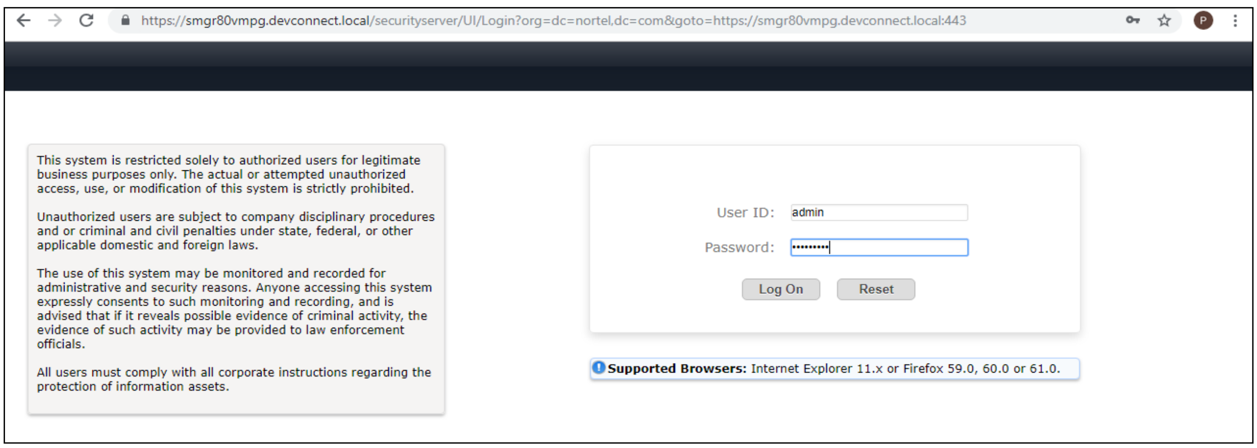
```
change trunk-group 1                                            Page   5 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? 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? n
                                              Enable Q-SIP? n

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                Request URI Contents: may-have-extra-digits
```

6. Configuring Avaya Aura® Session Manager

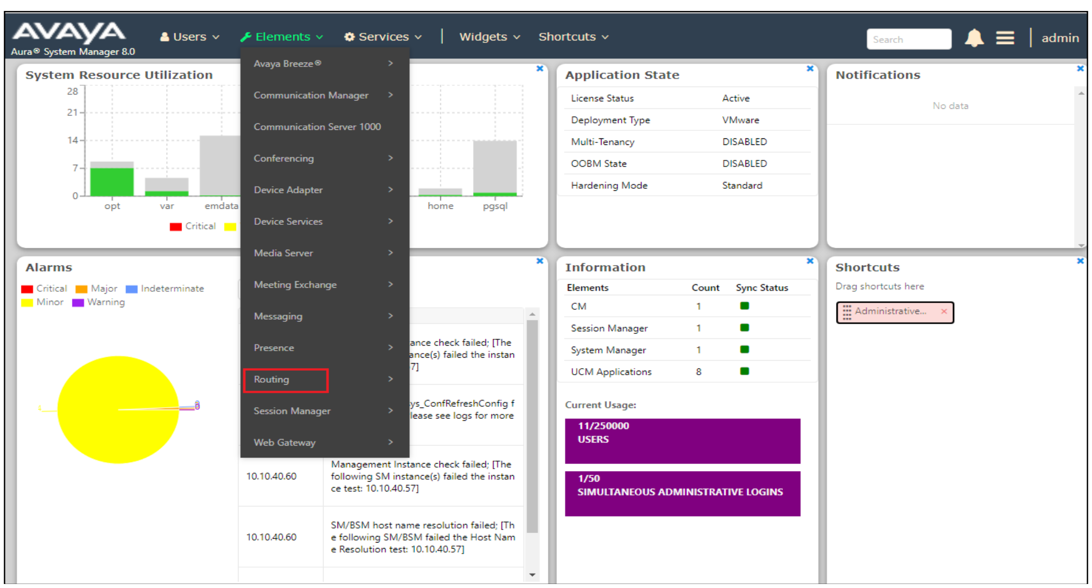
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Configure SIP Entity
- Configure Entity Link
- Configure Routing Policy
- Configure Dial Pattern

To make changes on Session Manager a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to **https://<System Manager FQDN>/SMGR**. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On**.



Once logged in navigate to **Elements** and click on **Routing** highlighted below.

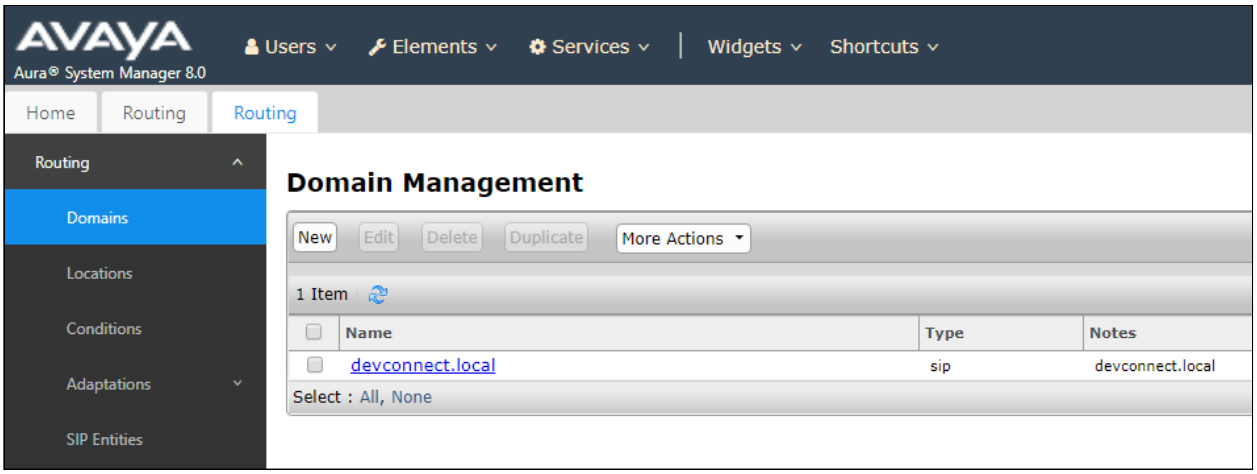


6.1 Domains and Locations

Note: It is assumed that a domain and a location have already been configured, therefore a quick overview of the domain and location that was used in compliance testing is provided here.

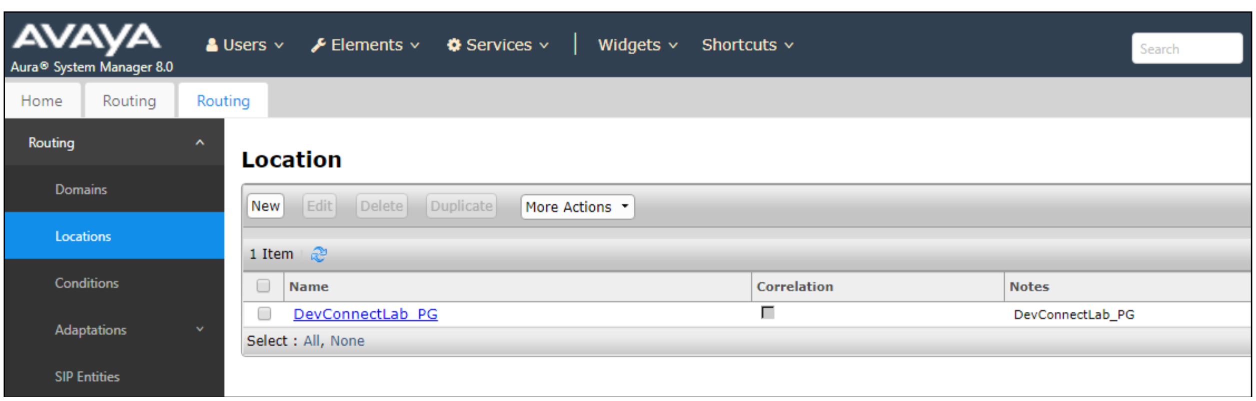
6.1.1 Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **devconnect.local** as shown below. If a domain is not already in place, click on **New**. This will open a new window (not shown) where the domain can be added.



6.1.2 Display the Location

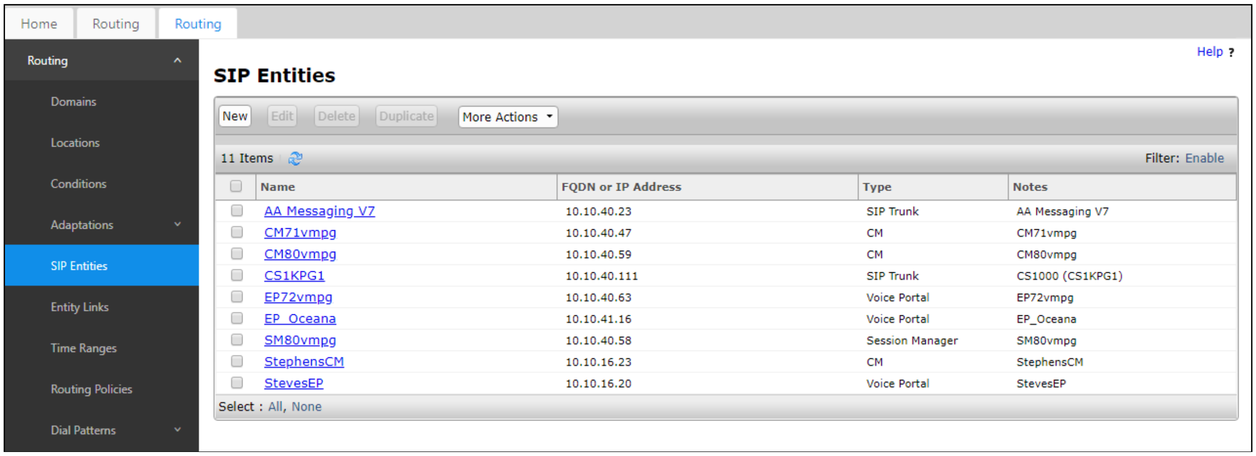
Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectLab_PG** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.



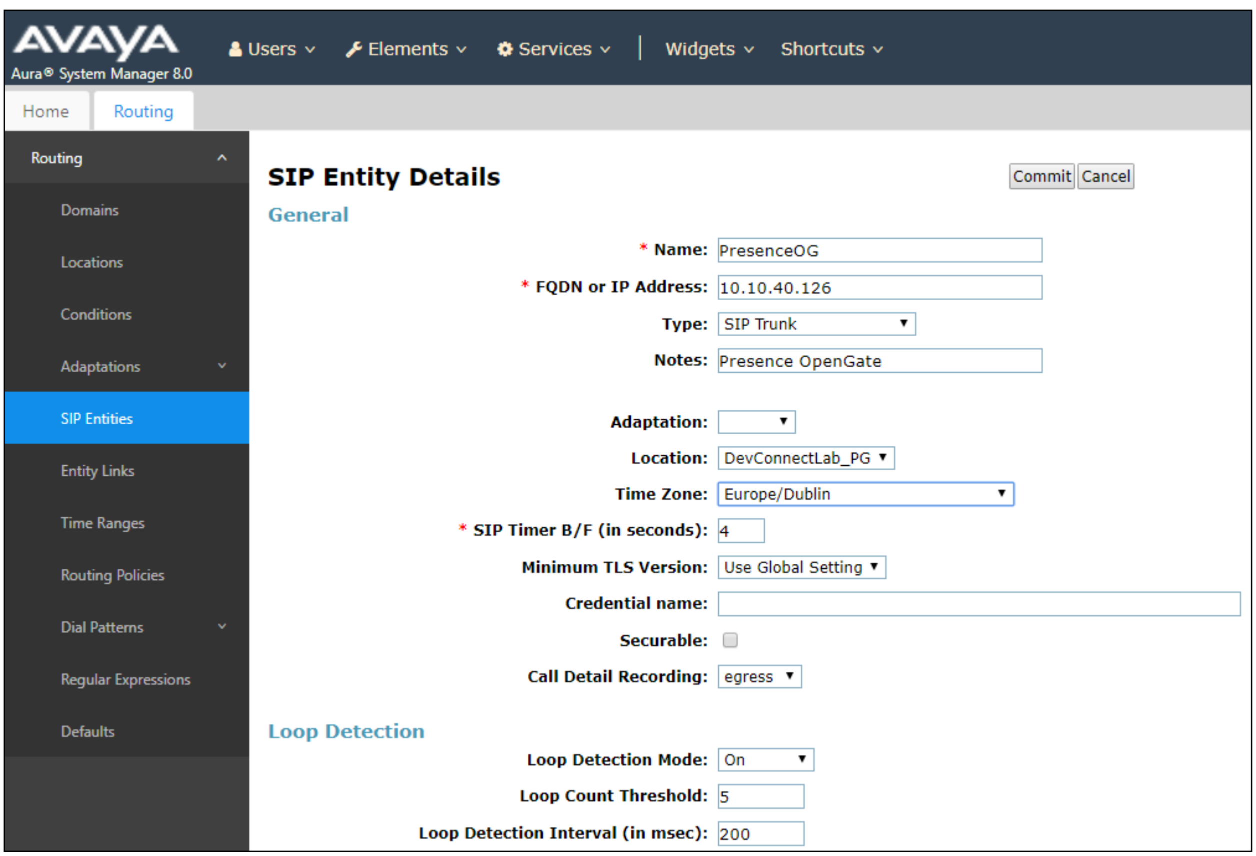
6.2 Configure Presence OpenGate SIP Entity

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

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



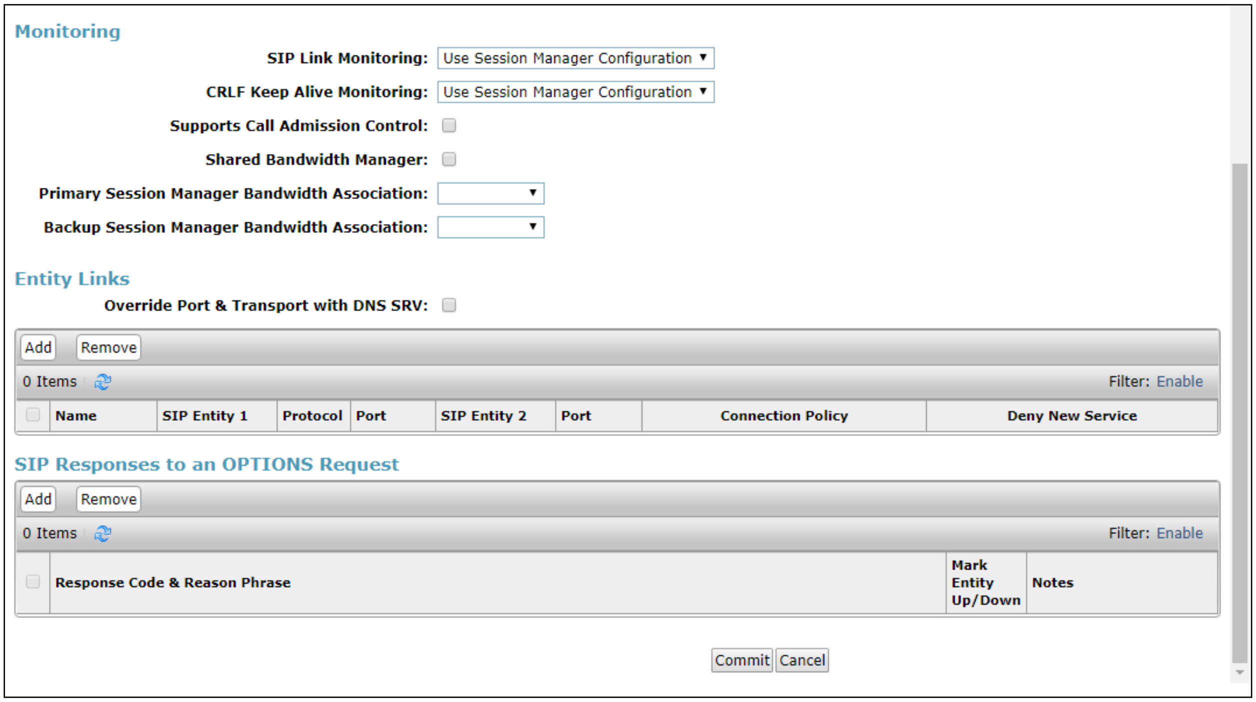
Enter a suitable **Name** for the new SIP Entity and the **IP Address** of the Presence OpenGate server. Set **Type** to **SIP Trunk**. Enter the correct **Time Zone** and **Location** and scroll down to SIP Entity Links.



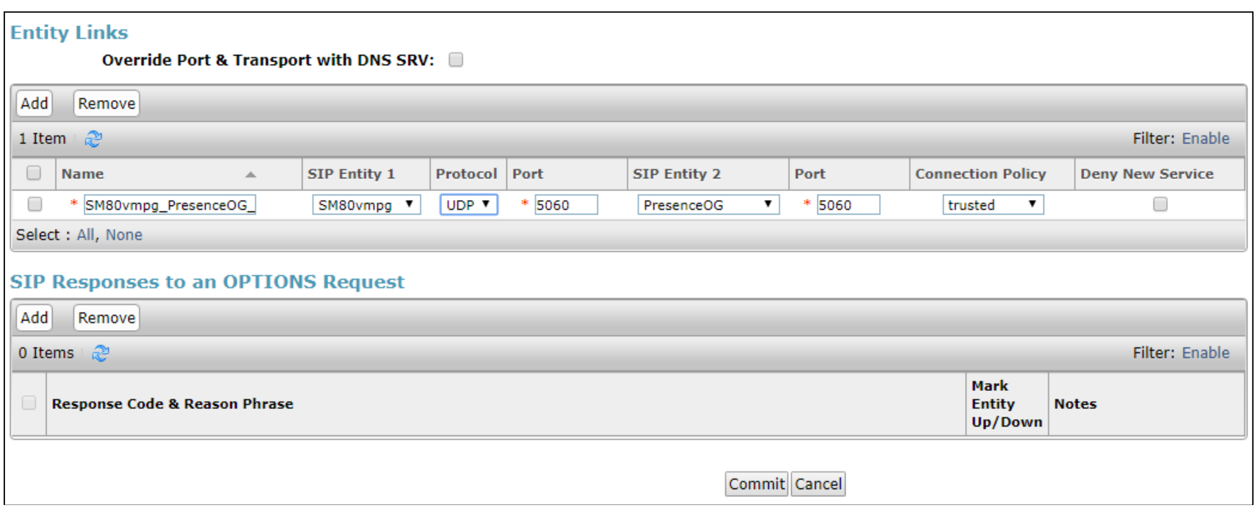
6.3 Configure Presence OpenGate SIP Entity Link

An Entity link can be added from the SIP Entities page. Using the page from the previous page scroll down to Entity Links.

Upon scrolling down to **Entity Links** click on **Add**.

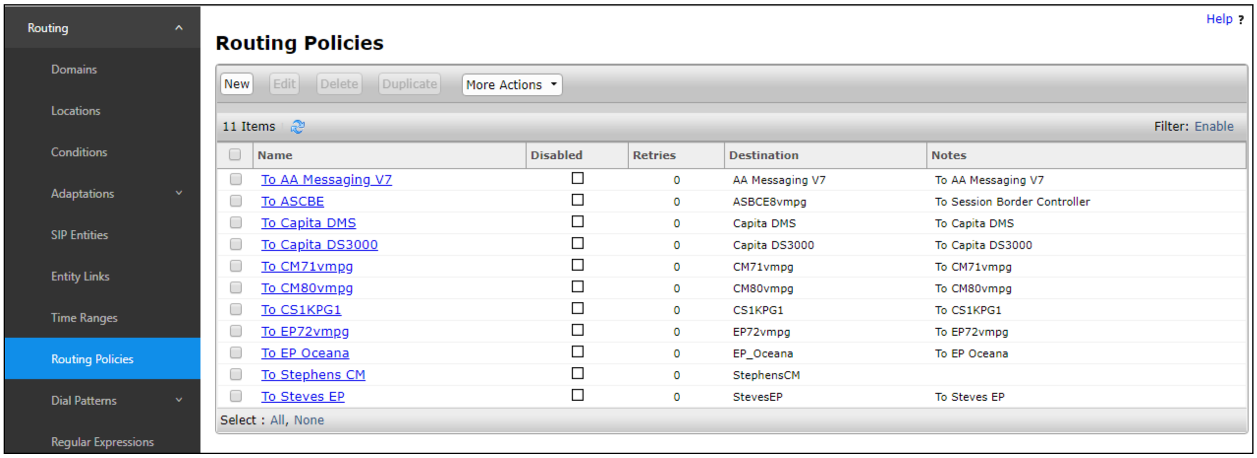


Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created Presence OpenGate SIP Entity for **SIP Entity 2**. Ensure that **UDP** is selected for the **Protocol** and that **Port 5060** is used. Click on **Commit** once finished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

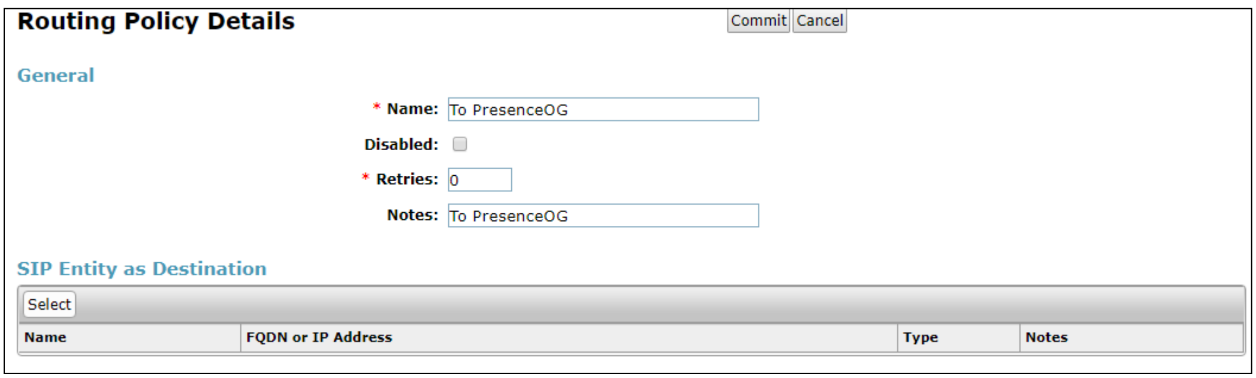


6.4 Configure Routing Policy for Presence OpenGate

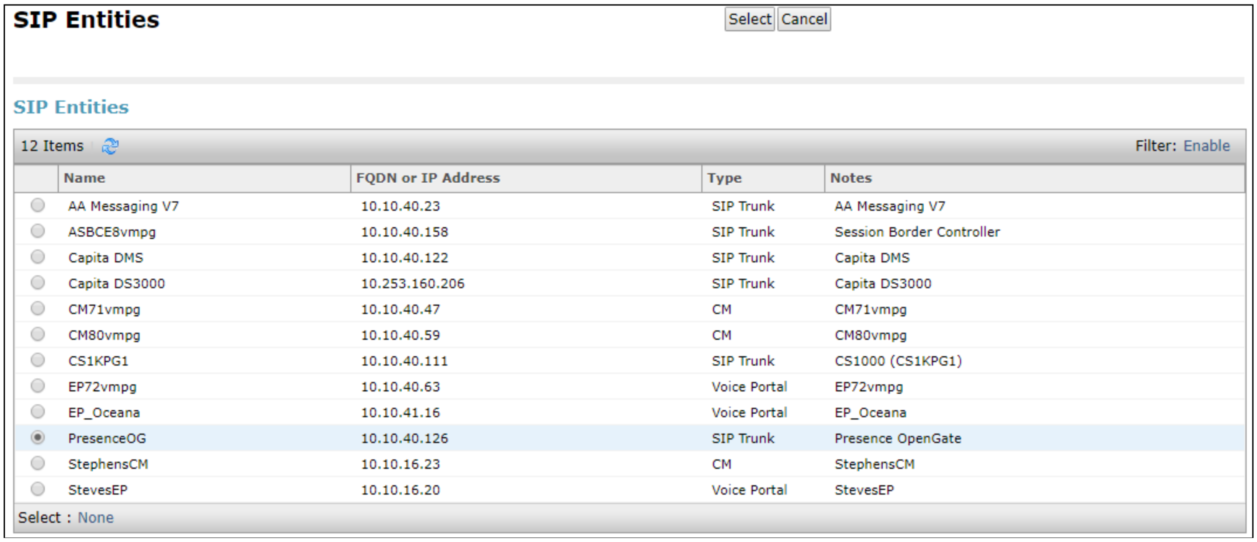
Click on **Routing Policies** in the left window and select **New** in the main window.



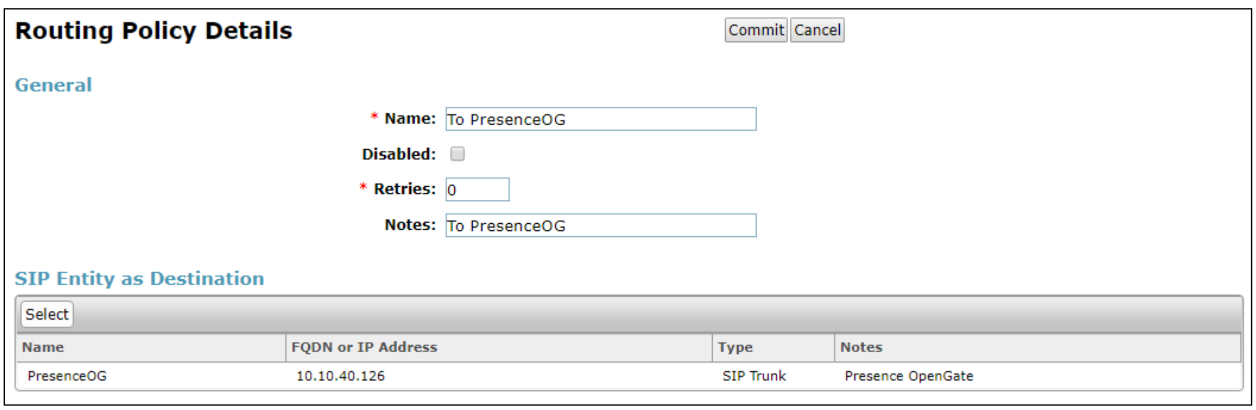
Enter a suitable **Name** for the Routing Policy and click on **Select** under **SIP Entity as Destination**, highlighted below.



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

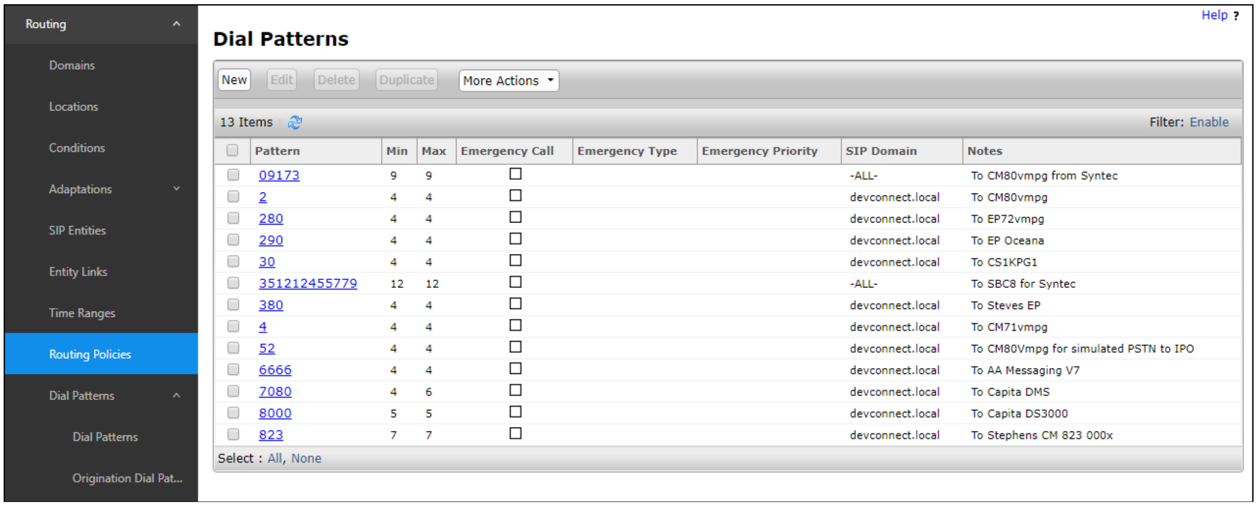


The selected destination is now shown, click on **Commit** to save this.

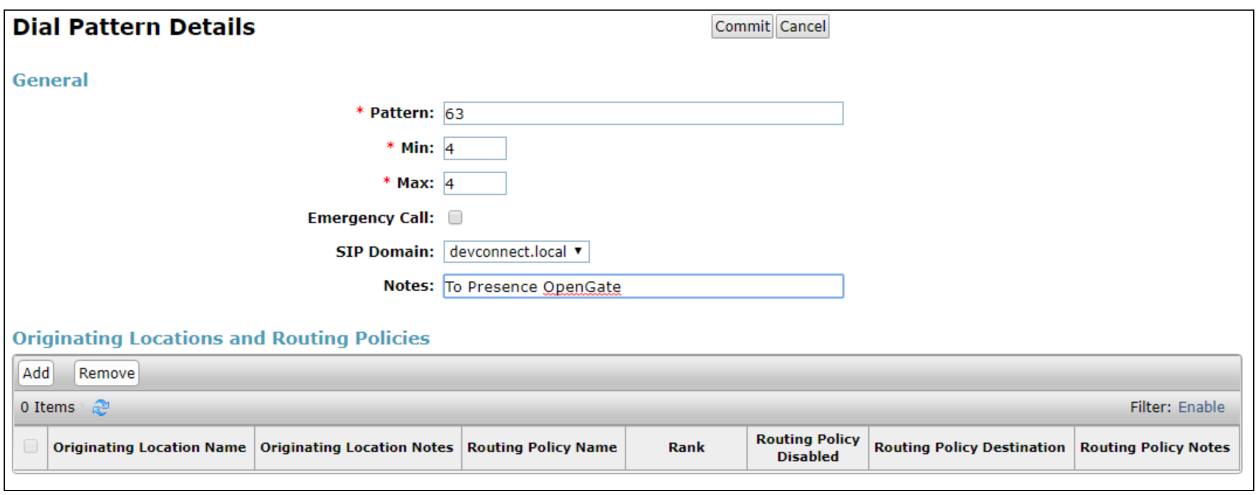


6.5 Configure Presence OpenGate Dial Patterns

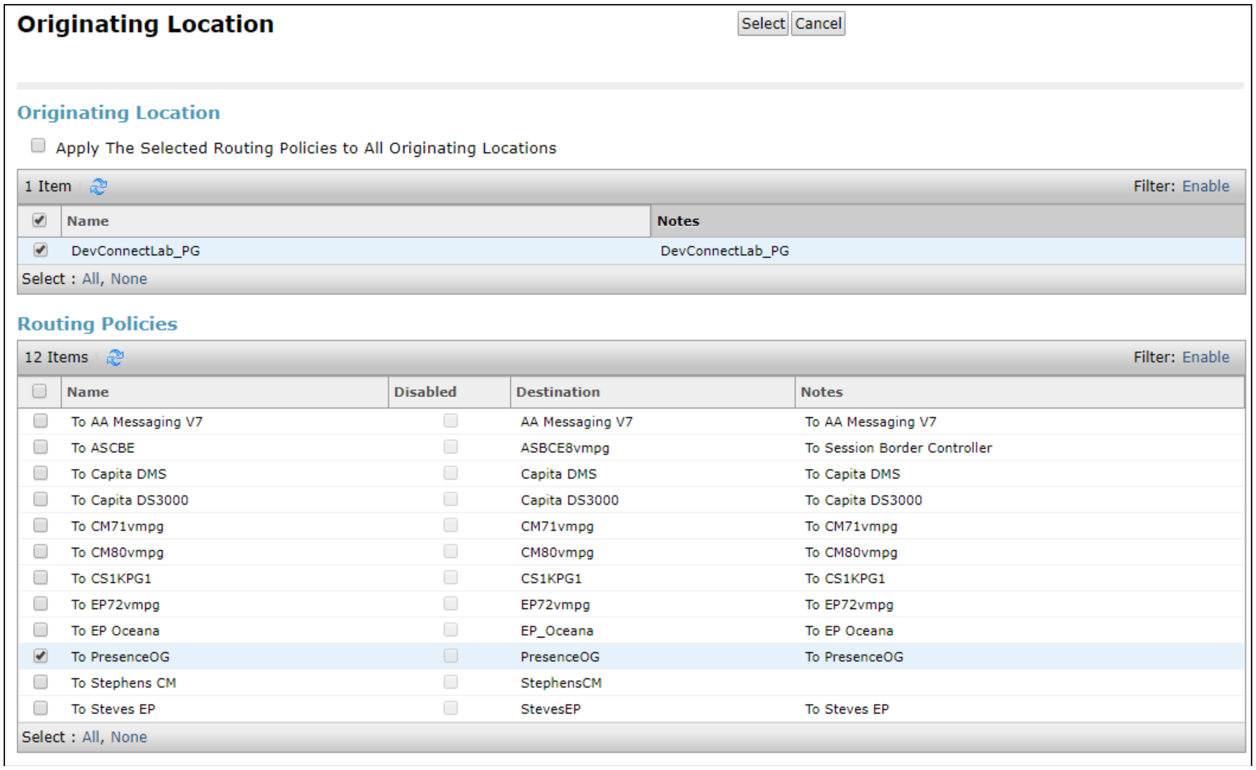
Select **Dial Patterns** in the left window and select **New** in the main window.



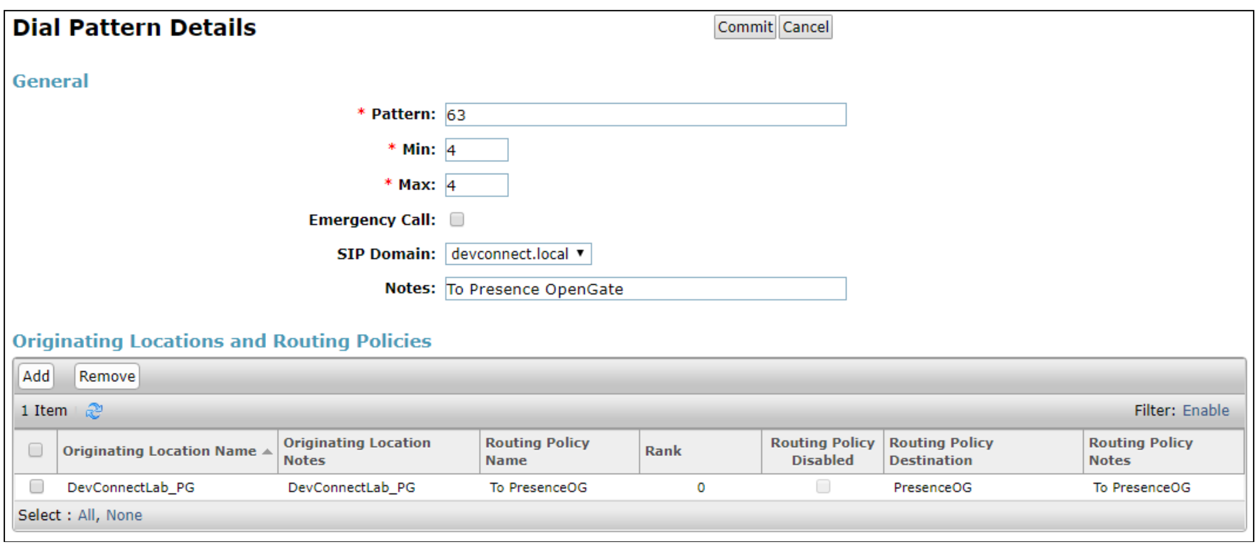
Enter the required digits for the Routing Pattern, in the example below **63** is used. This ensures that when 63xx is dialled it will route to the Presence OpenGate. Enter the appropriate domain for **SIP Domain** in this example the domain created in **Section 6.2** is added. Click on **Add** under **Originating Locations and Routing Policies** to select this Routing Policy.



Select the **Originating Location**, this will be the location added in **Section 6.1.2** select the newly created Routing Policy for Presence OpenGate.



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



7. Configure Enghouse Presence OpenGate

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

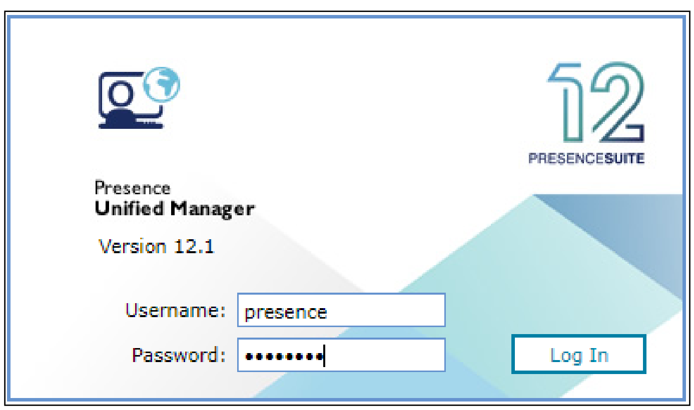
This section will cover the following areas:

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

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.

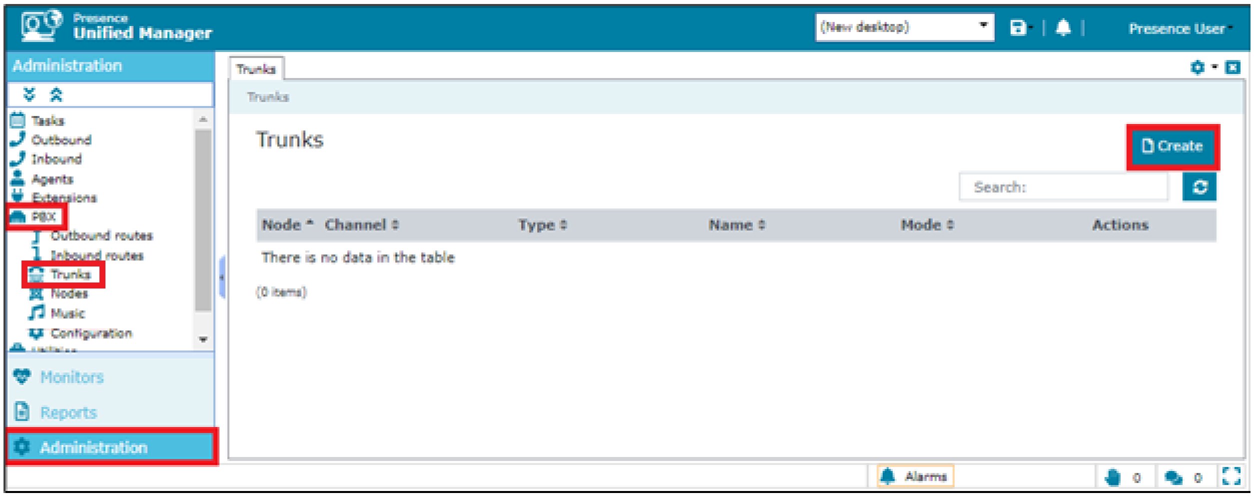
7.1 Login to Presence Unified Manager

Enter **https://<ip-addr>/websupervisor** as the URL in an Internet browser. This is the IP address of the Presence Unified Administrator, which happens to be installed on the same server as the other modules of Presence Suite. The username and password that appear in the **User** and **Password** fields are created during the Presence Server installation.



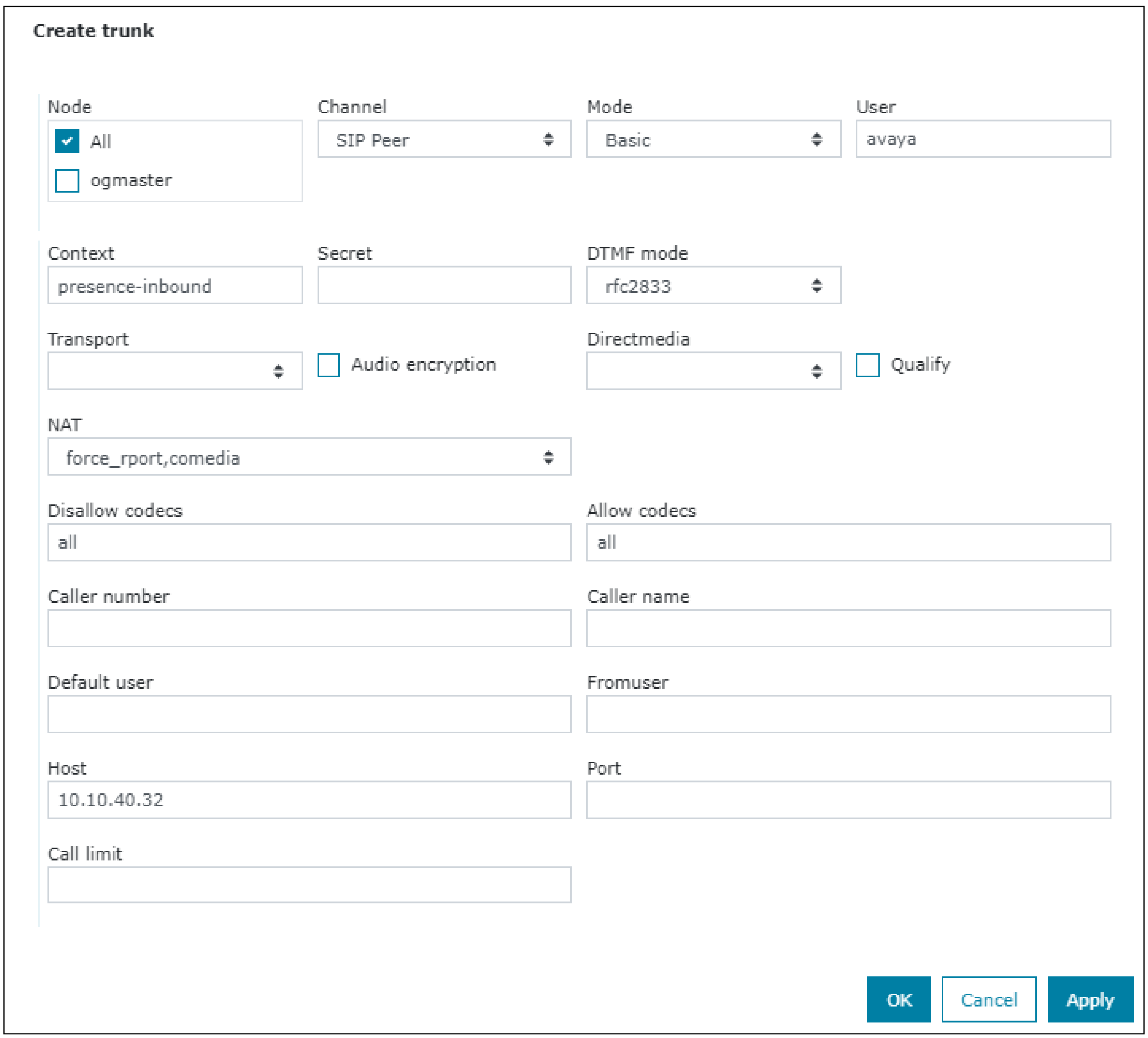
7.2 Administer SIP Trunk to Avaya Aura® Session Manager

Go to **Administration → PBX → Trunks** from the main menu on the left-hand side. Double click in **Trunks** to open a new tab and click on **Create** to create a new trunk.



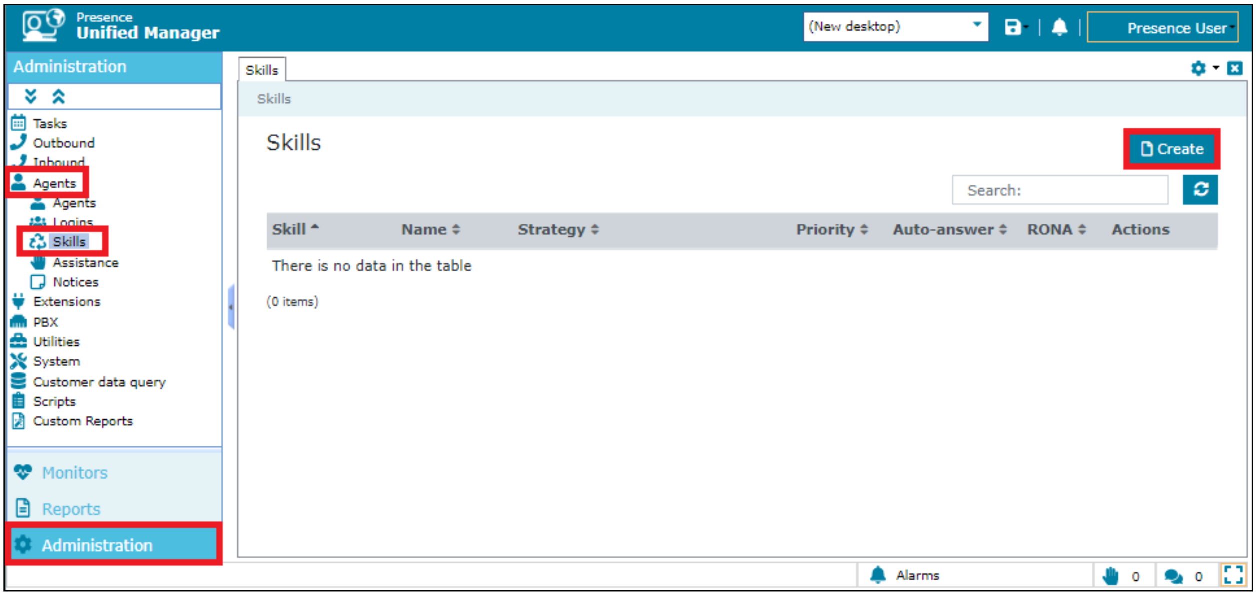
Fill in the information as shown below. Please note that the **Node ogmaster** has already been established during the install of Presence Presence OpenGate. Select **SIP Peer** as the **Channel** and **Basic** as the **Mode**. Enter a suitable name for the **User**. Note the following in the main window.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

- **Node** = all
- **Channel** = SIP Peer
- **Context** = presence-inbound
- **DTMF mode** = rfc2833
- **NAT** = force_rport,comedia
- **Disallow codecs** = all
- **Allow codecs** = all
- **Host =** IP address of Session Manager

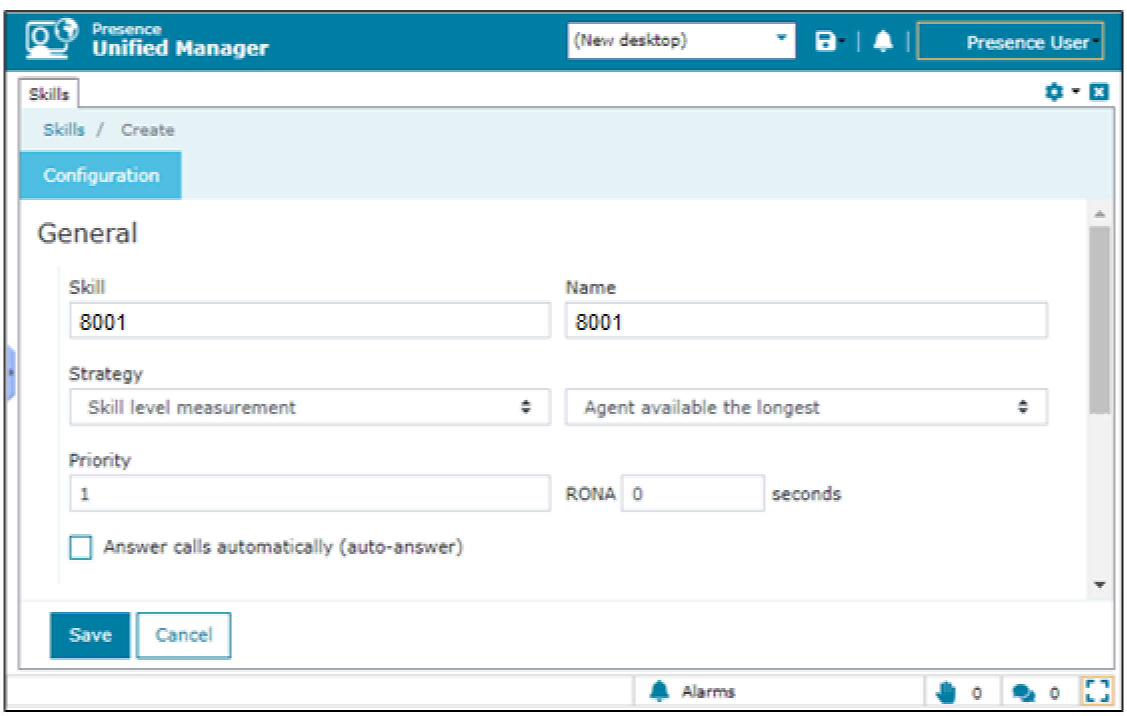


7.3 Presence OpenGate Skill Configuration

Go to **Administration → Agents → Skills** from the main menu on the left-hand side. Double click in **Skills** to open a new tab and click on **Create** to create a new skill.

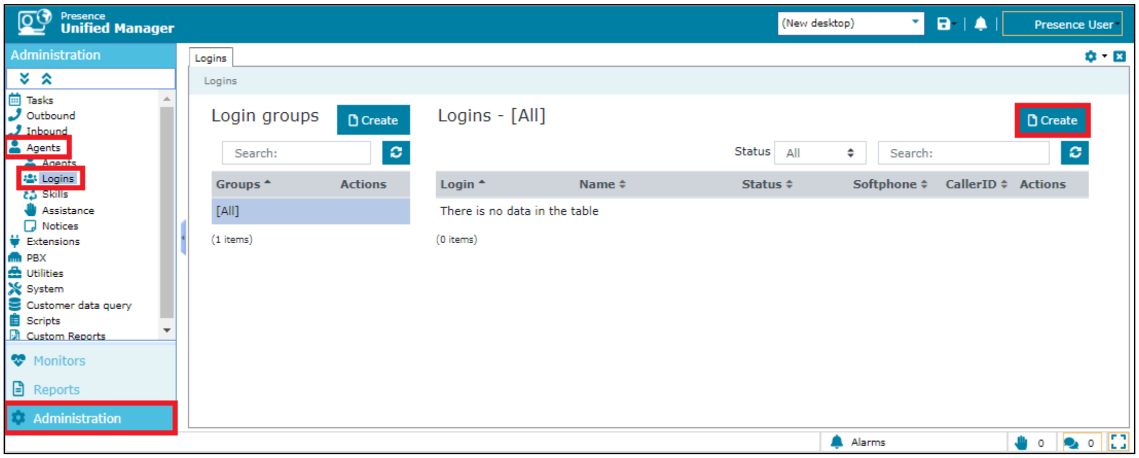


In the resulting screen, define a **Skill** number and enter a **Name** to identify the skill. In the **Strategy** field, use the two drop down menus to define the selection strategy that will be used by the skill. Set a **Priority** for the skill. All remaining fields can be left with default values. Click **Save** to save the configuration. Note that two Skills were configured for testing but only one (inbound 8001) was used.

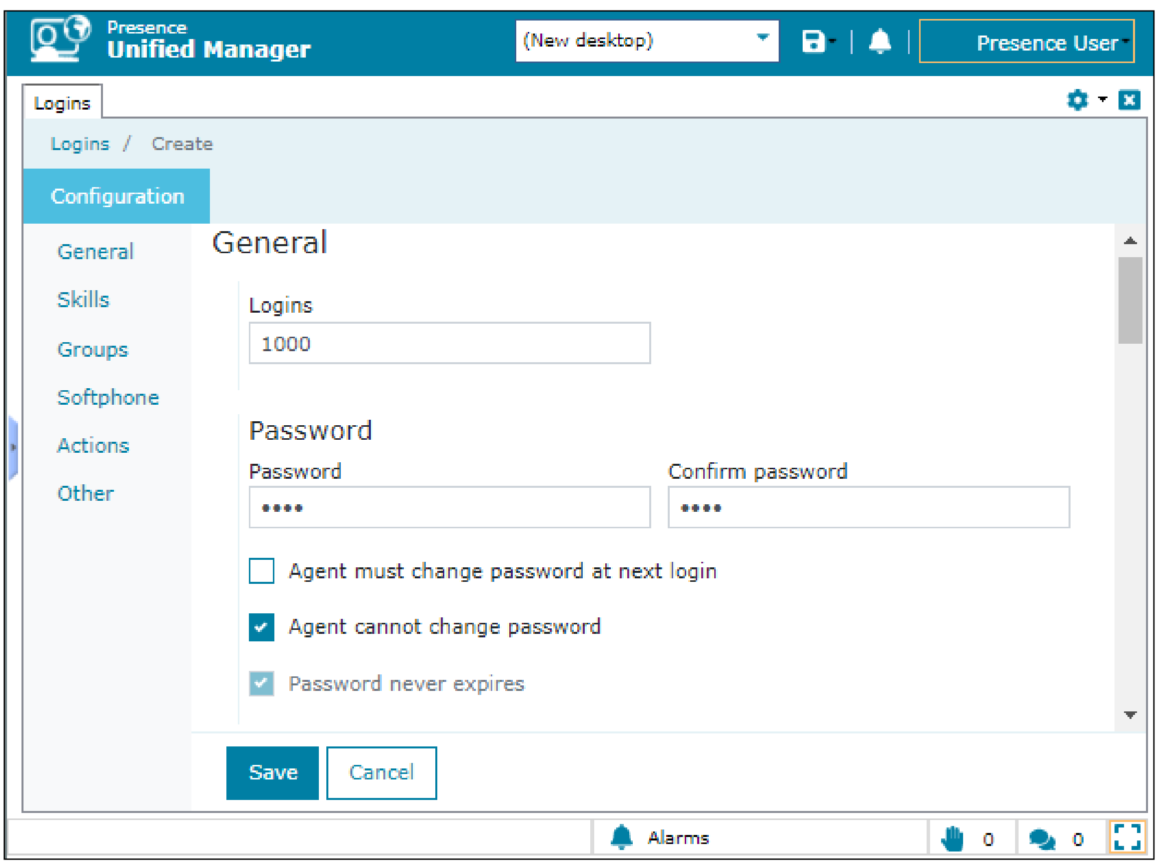


7.4 Presence OpenGate Agent Login Configuration

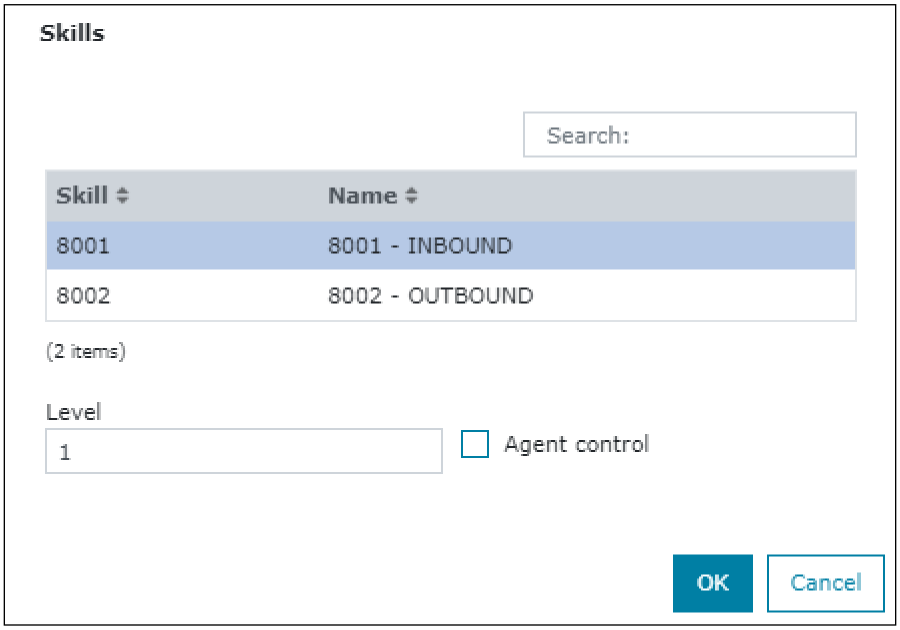
The login configured here will be used by the agent to login to Presence OpenGate. The Agents will connect to Presence OpenGate via the Presence Agent application. To configure an ACD agent login, from the left-hand side select **Administration → Agents → Logins** from the Presence Unified Manager main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



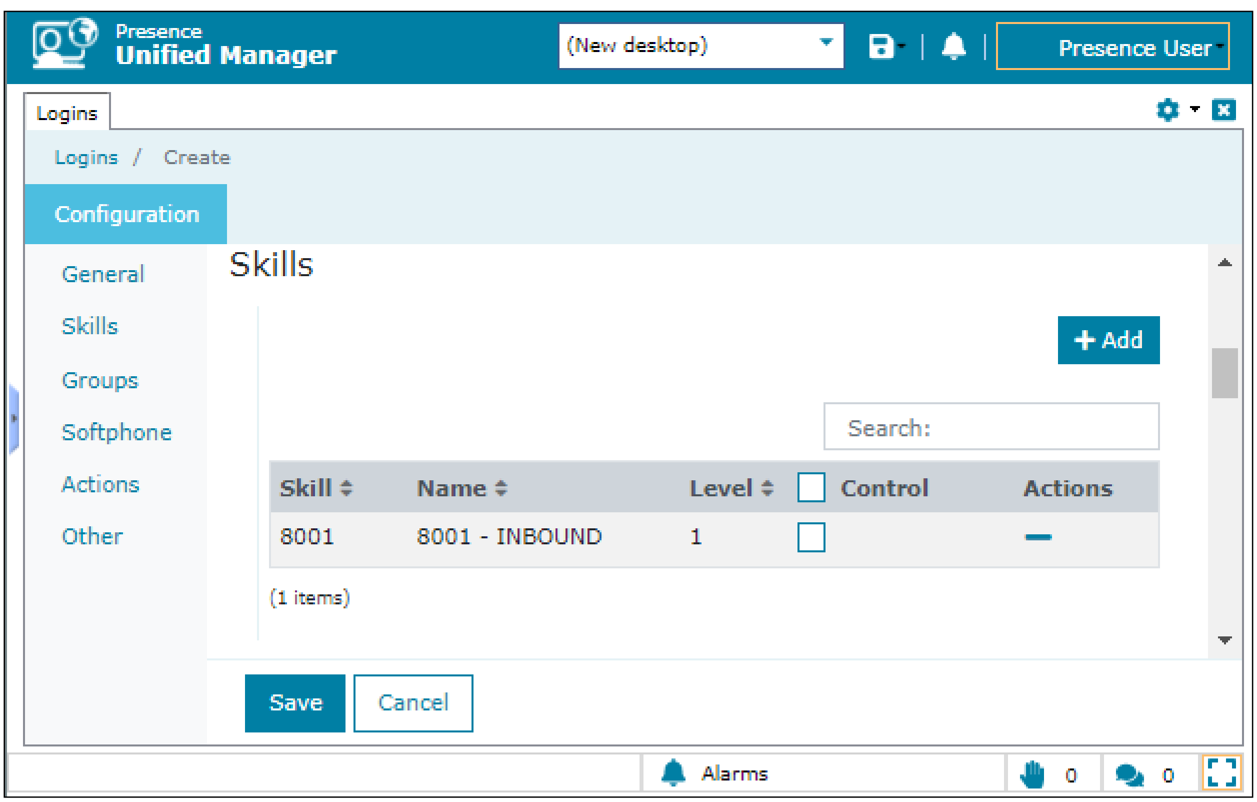
Go to **General** section and enter a numerical ID in the **Logins** field. Define a **Password** for the agent login and repeat in the **Confirm Password** field.



Go to **Skills** section, click to **Add** button to select the **Skill** configured in **Section 7.3** and specify a **Level** for the skill to be applied against this agent login.

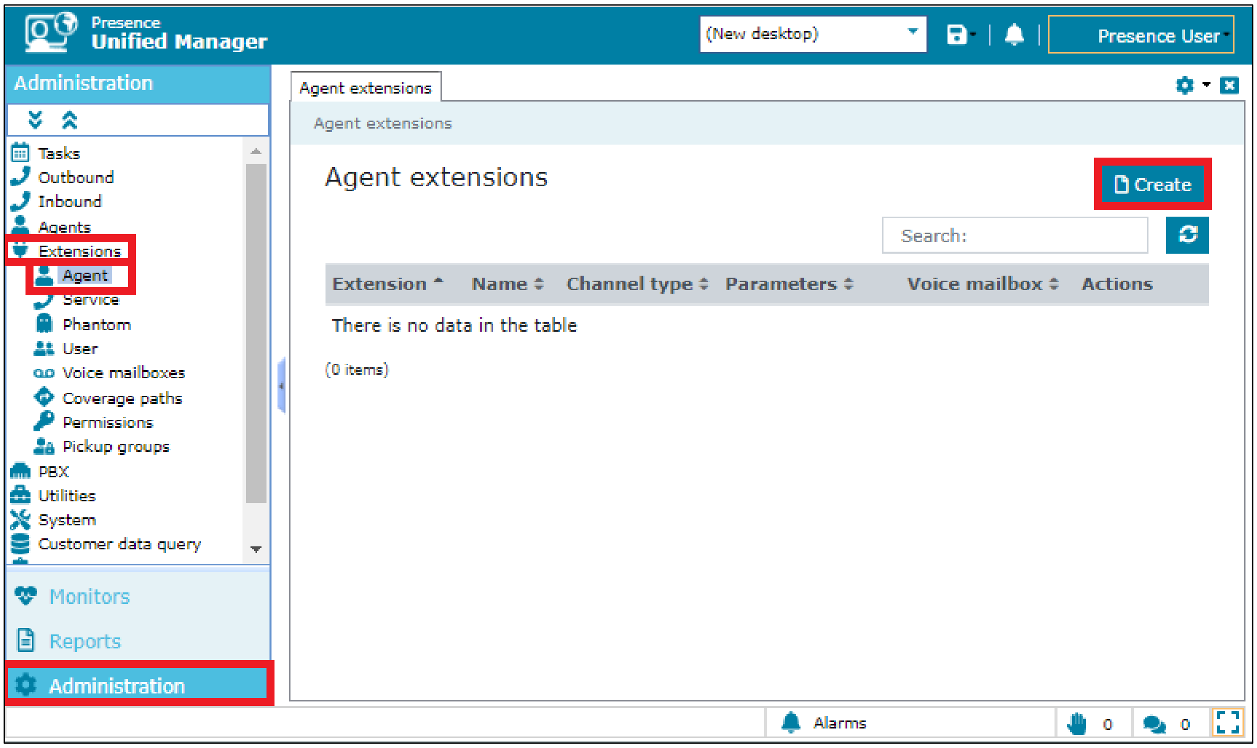


Click the **OK** button and the skill should appear under assigned **skills**. Click **Save** to save the login configuration.



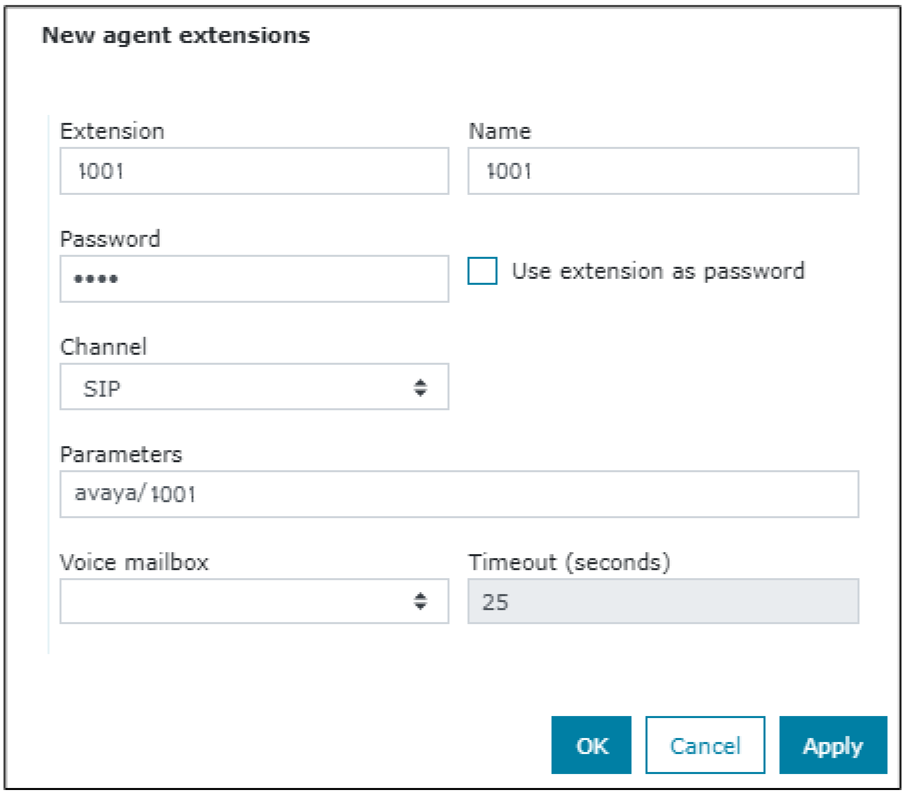
7.5 Presence OpenGate Station Configuration

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



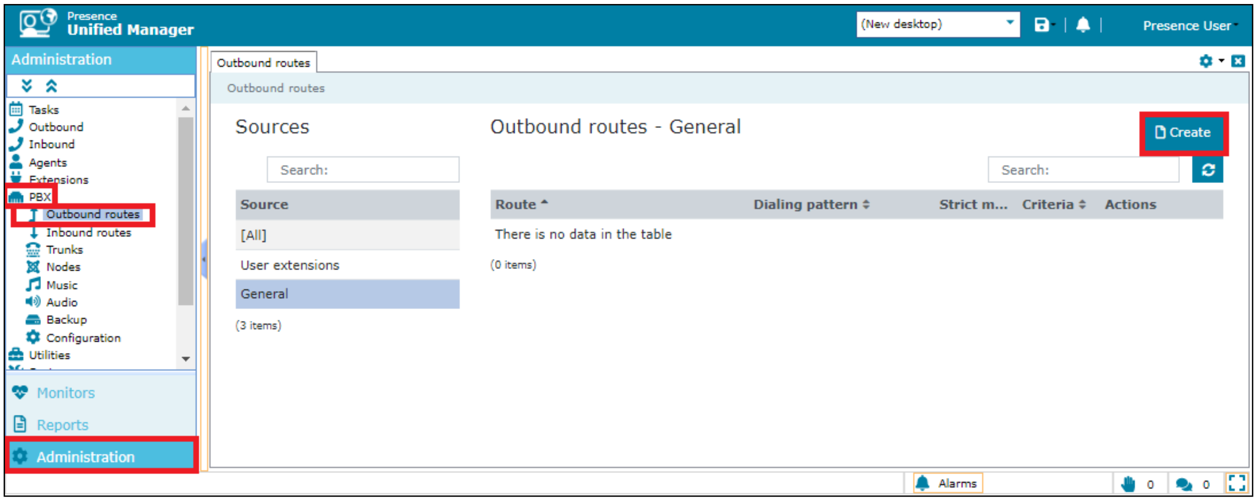
In the resulting screen specify, an **Extension** number that will be used by the Presence Agent application. Note that this number is an existing extension number on Communication Manager. Set a **Name** that the Agent extension will be known as. The password is not required in this case. In the **Channel** field, use the drop-down arrow to select **SIP**. In the following field, define the number that will be dialled, and the route used to reach the station. For this test, **avaya/1001** is configured, this will use trunk "avaya" to route the call. Note **avaya** is the SIP Trunk user configured in **Section 7.2**.

Note: For compliance testing extension 1001 is a H.323 extension on Communication Manager, a second association from another agent was made to extension 1101, which is a SIP extension on Communication Manager, that association is not shown below.

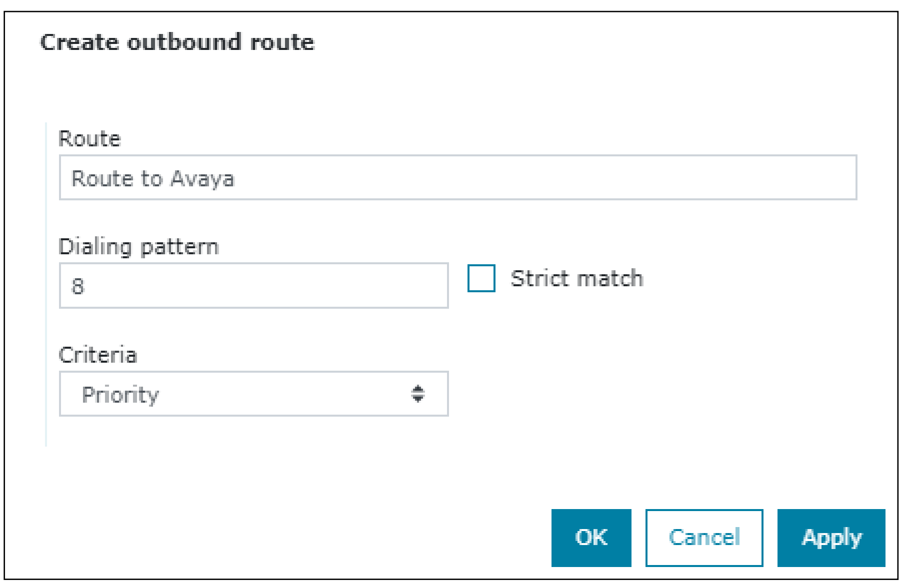


7.6 Outbound Routes

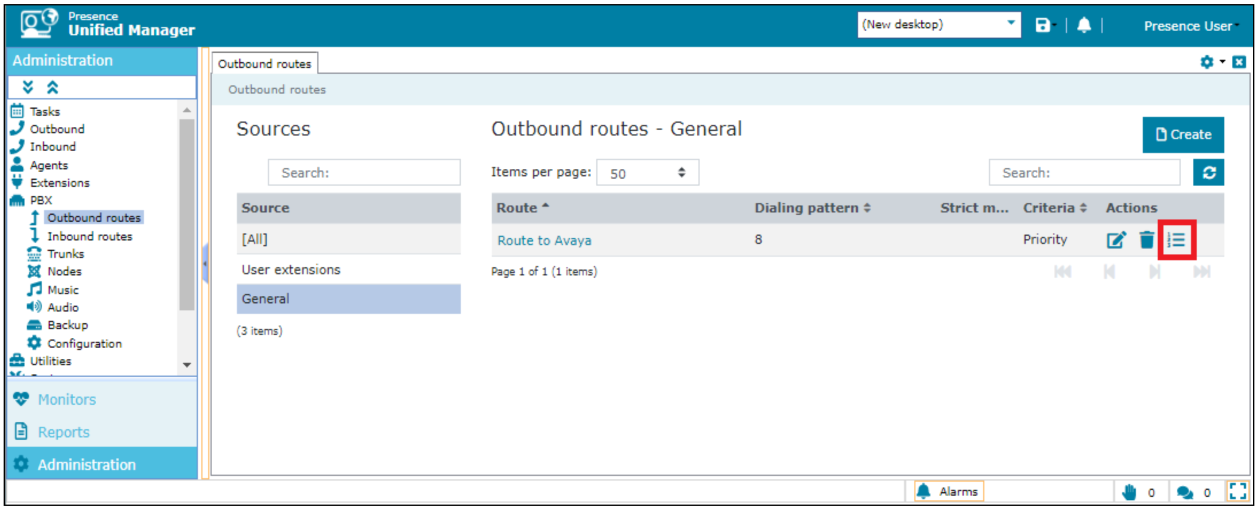
To define an outbound route, from the left-hand side navigate to **Administration → PBX → Outbound Routes** and click the **Create** button.



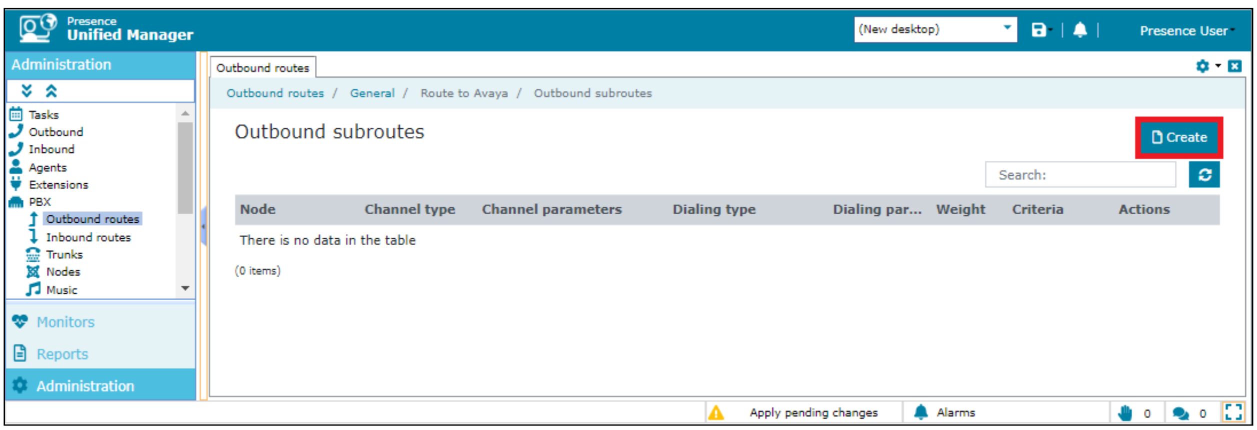
In the resulting screen, enter a descriptive name in the **Route** field and in the **Dialing pattern** field define any prefix required by outbound calls. This setup is only used for internal working of Presence OpenGate and is not related to routing calls on Communication Manager. For **Criteria**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



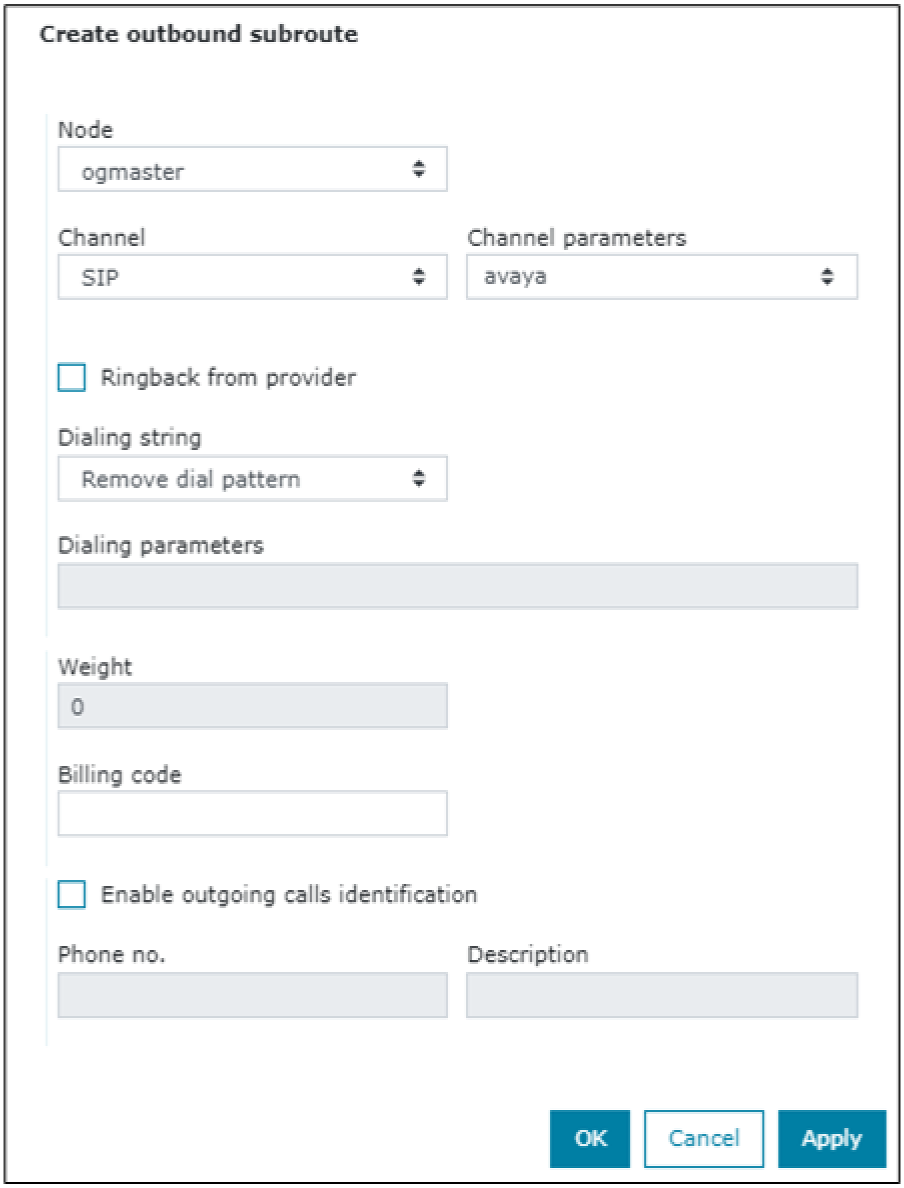
To add an outbound subroute, from the outbound routes main page shown above, click on the last action button to navigate to the outbound subroutes page.



The **Outbound subroutes** window is then displayed as shown below, Click **Create**.

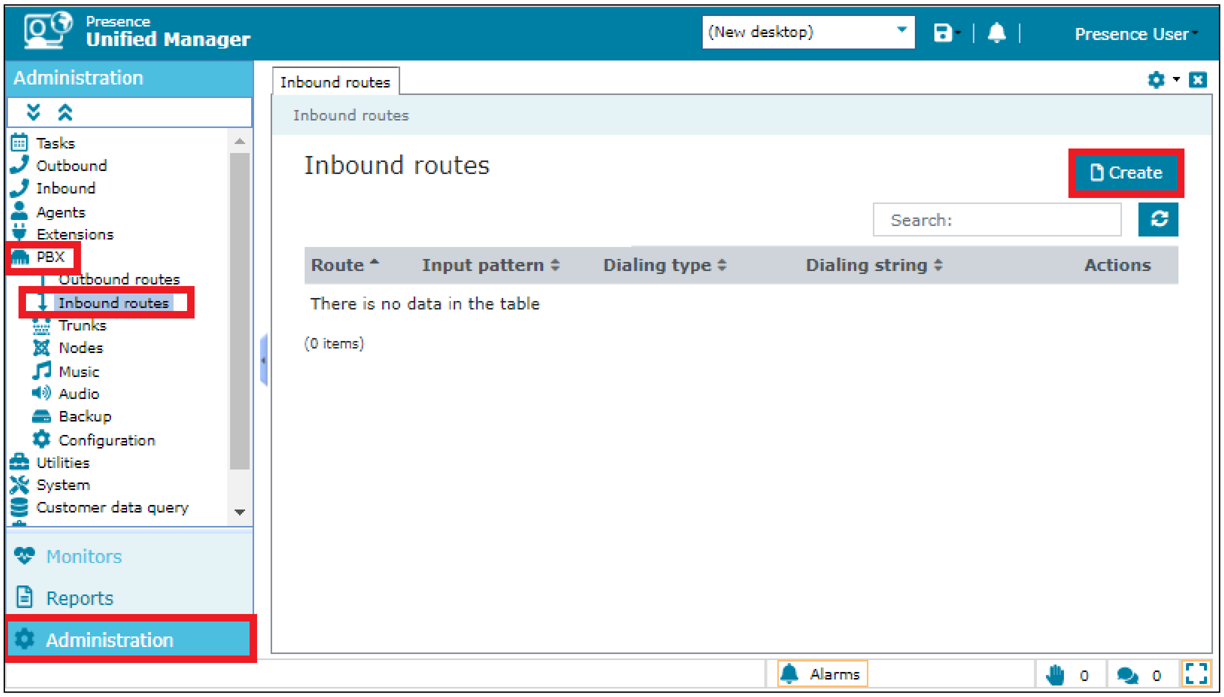


In the resulting window, select the relevant **Node** (**ogmaster**, created during the Presence OpenGate install), and under **Channel** select **SIP**. For **Dialing string** use the drop-down menu to select **Remove dial pattern** leaving the secondary field blank. This informs Presence OpenGate to remove the "8" used to define the pattern (also created during the Presence OpenGate install) before routing the call via the **avaya** trunk.

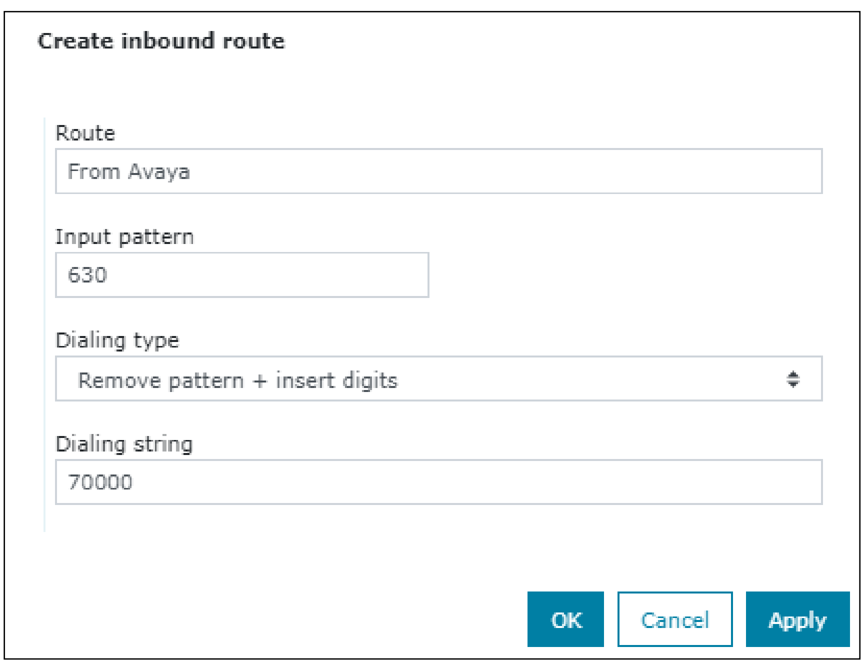


7.7 Inbound Routes

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

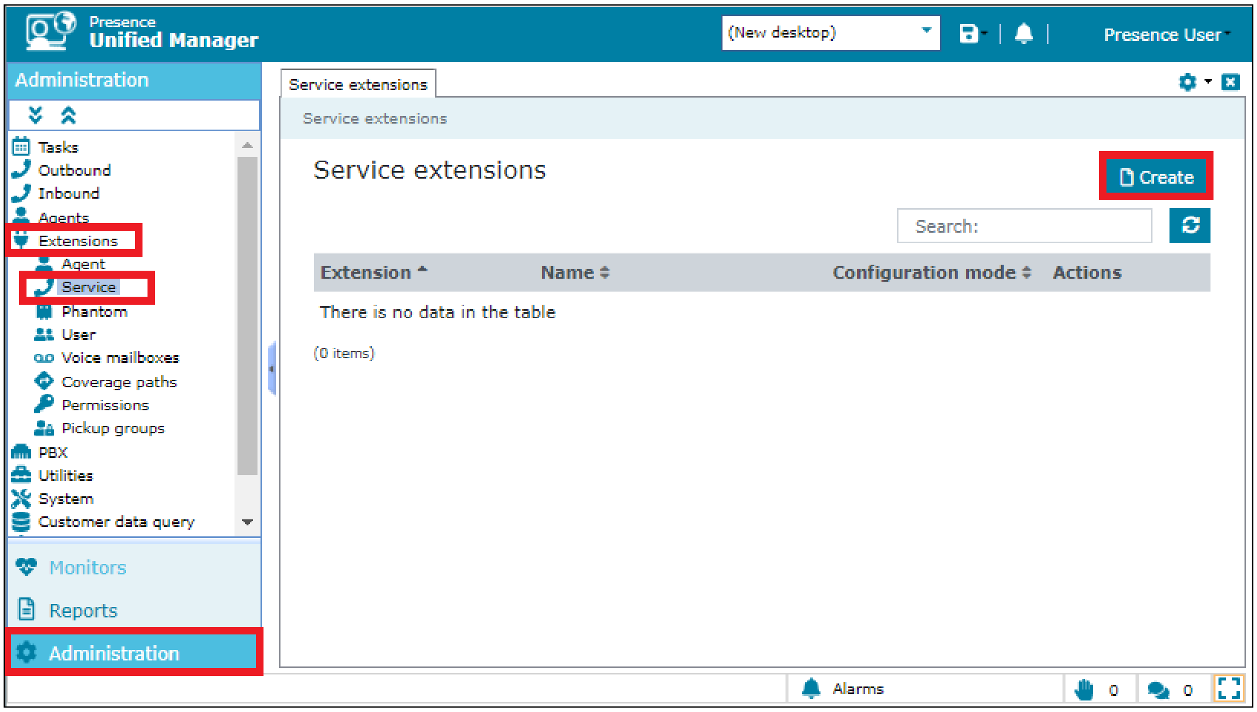


In the resulting window enter a descriptive name for **Route**. In this example any calls beginning with 630x will route to **70000** (this is simply internal routing for Presence OpenGate).

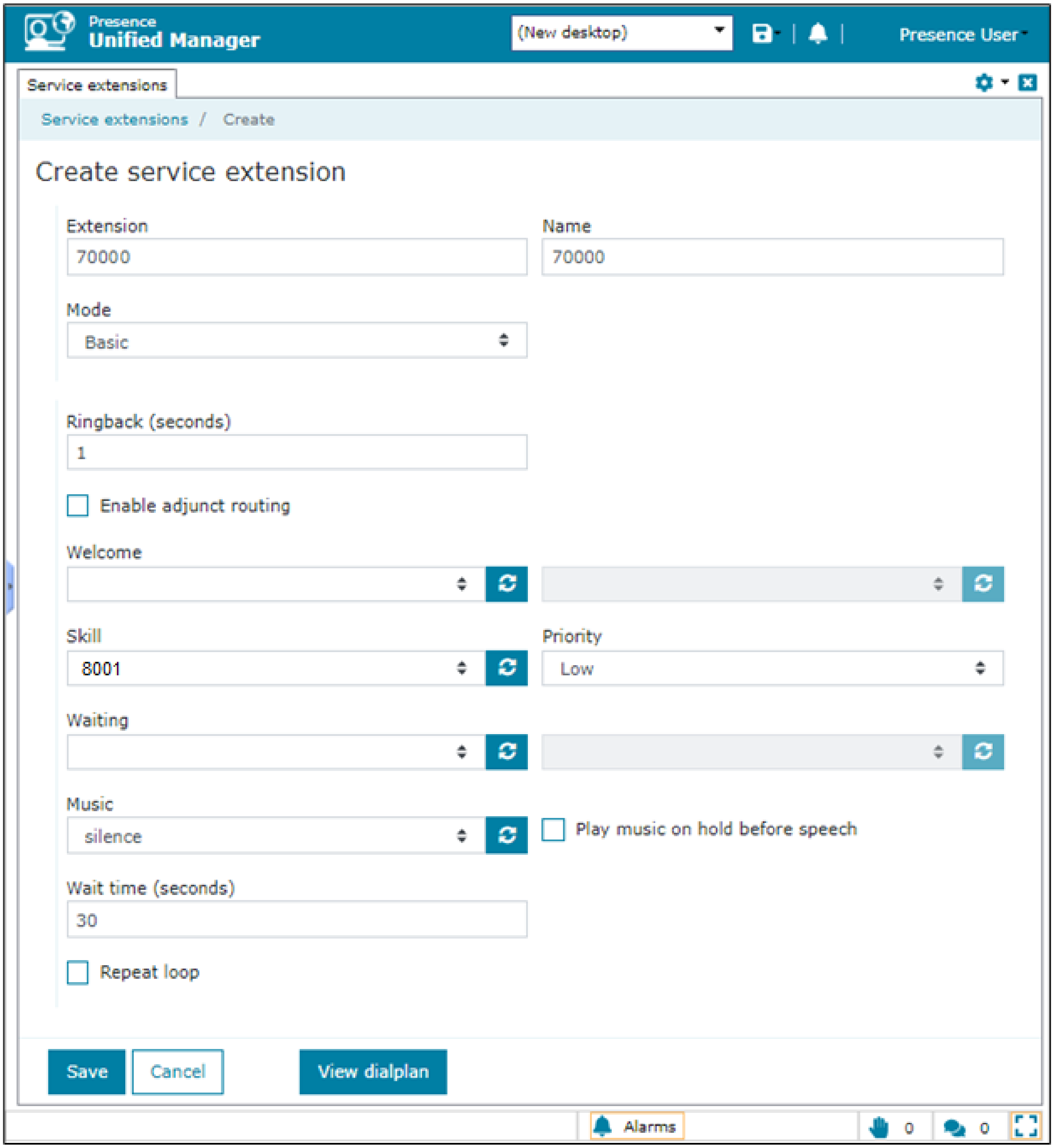


7.8 Service Extension

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



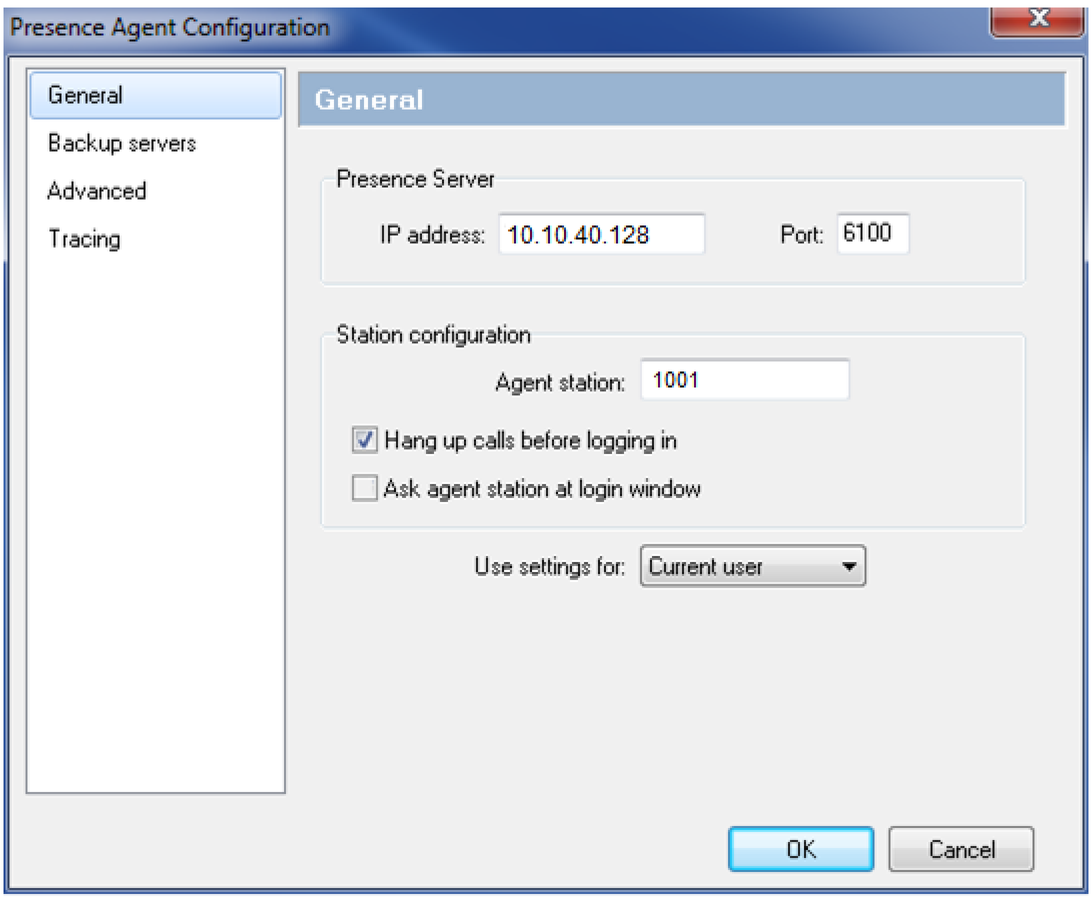
In the resulting windows enter the extension number in the **Extension** field and give it a descriptive name in the **Name** filed. Select the **Basic** mode under **Mode** and select **Skill** create in **Section 7.4**.



7.9 Presence Agent Configuration

The following steps are carried out on the Presence Suite agent PC. Prior to installing the Presence Client application, ensure that the DBExpress driver (dbexpoda40.dll) is located in the **C:\Windows\SysWOW64** directory. If not, contact Enghouse support outlined in **Section 2.3** of these Application Notes. The DBExpress driver allows the agent application to communicate with the Presence Suite/Presence 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 **10.10.40.128**. The **Presence Server port** can be left as the default value of **6100**. Enter the extension of the station that will be used with this workstation in the **Agent station** field. Check the **Hang up calls before logging in** check box is not selected. In the field **Use settings for** choose **Machine** from the drop-down menu. Click **OK**. This step is needed for each agent configured; only the agent station field will vary.



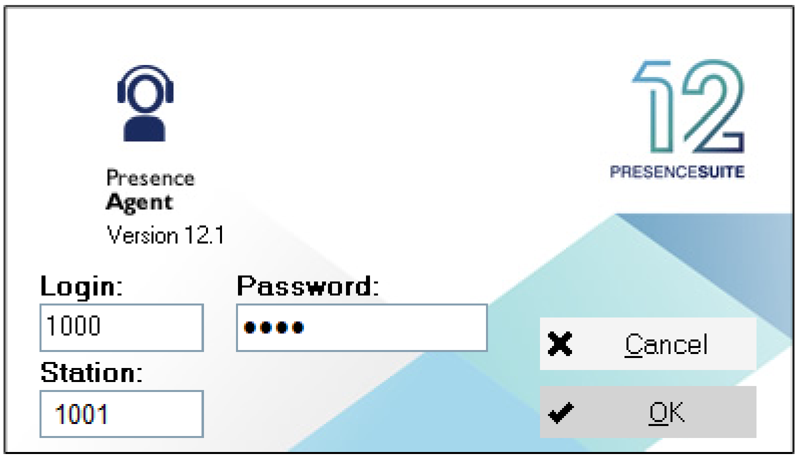
8. Verification Steps

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

8.1 Verify Enghouse Presence OpenGate

To receive calls from Presence OpenGate, users must log in to the system via the Presence Client application. This section describes the steps required to connect to Presence OpenGate as an agent to receive ACD calls.

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



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

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

8.2 Verify Avaya Aura® Communication Manager

The following steps can be taken if there are any issues with calls being made. This should help verify the links between the products. From the SAT interface, verify the status of the SIP trunk groups by using the **status trunk n** command, where "n" is the trunk group number administered in **Section 5.5**. Verify that all trunks are in the **in-service/idle** state as shown below.

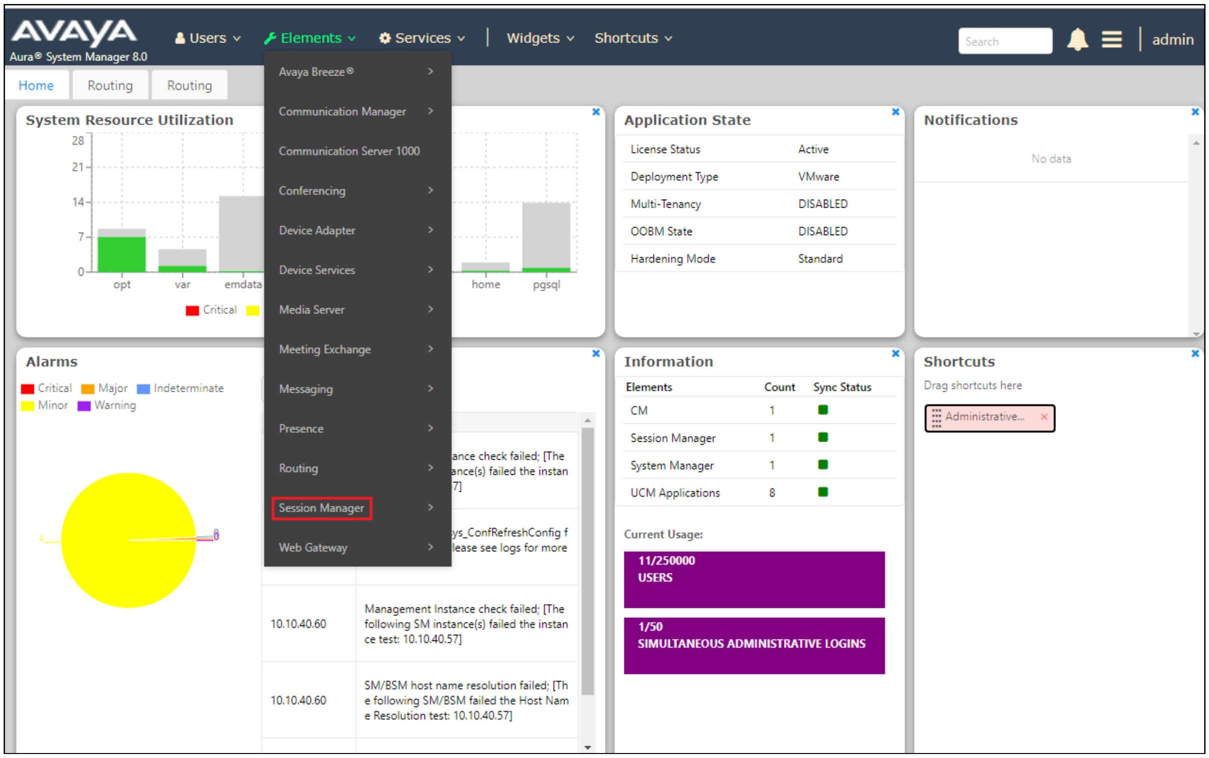
```
status trunk 1

                             TRUNK GROUP STATUS

Member    Port    Service State      Mtce Connected Ports
                                     Busy

0001/0001 T000001 in-service/idle    no
0001/0002 T000002 in-service/idle    no
0001/0003 T000003 in-service/idle    no
0001/0004 T000004 in-service/idle    no
0001/0005 T000005 in-service/idle    no
0001/0006 T000006 in-service/idle    no
0001/0007 T000007 in-service/idle    no
0001/0008 T000008 in-service/idle    no
0001/0009 T000009 in-service/idle    no
0001/0010 T000010 in-service/idle    no
```

Verify the status of the SIP signaling groups by using the **status signaling-group n** command, where "n" is the signaling group number administered in **Section 5.5**. Verify that the signaling group is **in-service** as indicated in the **Group State** field shown below.

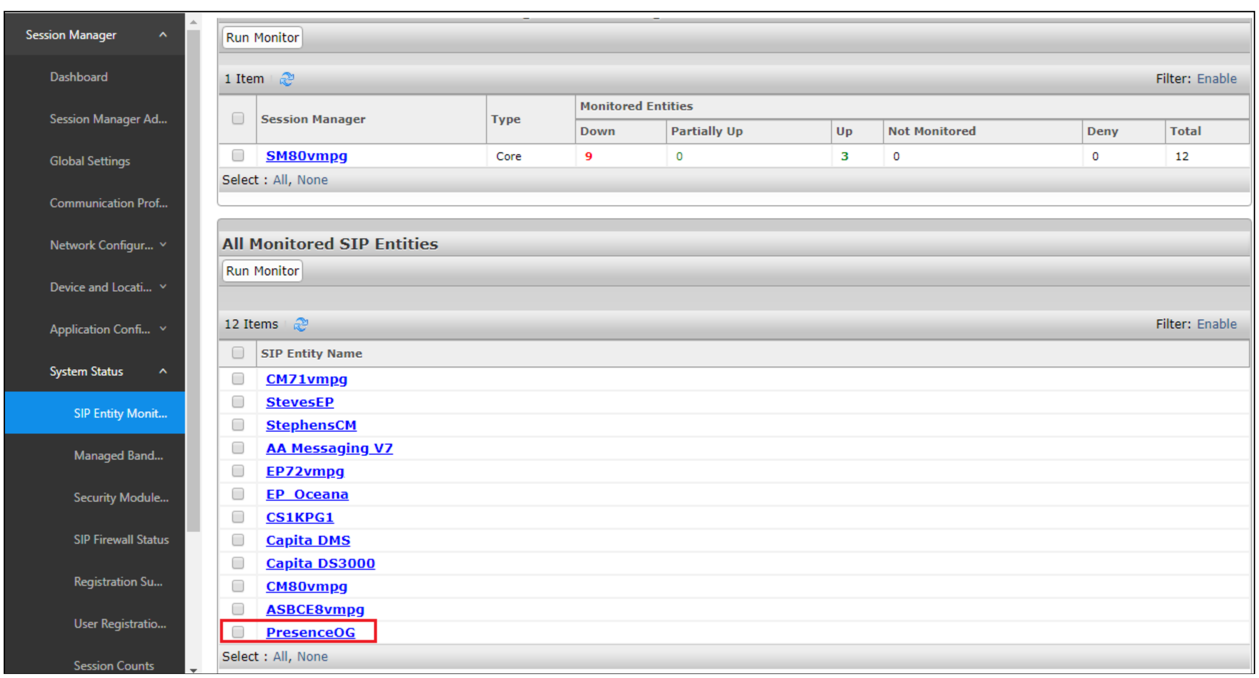
```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

8.3 Verify Presence OpenGate SIP Entity is up

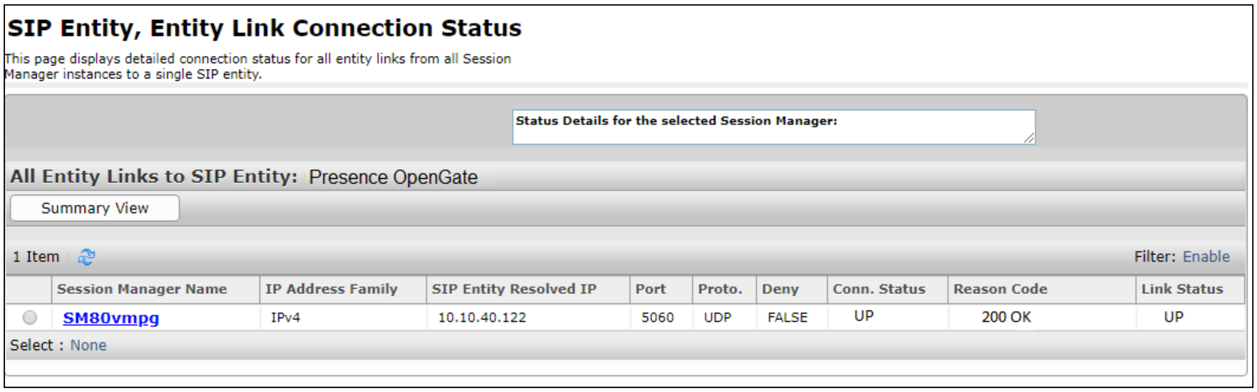
Log into System Manager as per **Section 6**. Navigate to **Elements** and click on **Session Manager**.



Select the Presence OpenGate SIP Entity.



The SIP Entity should show as **UP** as it is shown below.



9. Conclusion

These Application Notes describe the configuration steps required for Enghouse Presence OpenGate R12.1 to successfully interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1. All functionality and serviceability test cases were completed successfully.

10. Additional References

This section references the Avaya and Presence Suite product documentation that are relevant to these Application Notes.
Product documentation for Avaya products may be found at *http://support.avaya.com*.

[1] *Administering Avaya Aura® Communication Manager, Release 8.1.x, Issue 12, Jul 2021*
[2] *Administering Avaya Aura® Session Manager, Release 8.1.x, Issue 8, Feb 2021*
[3] *Avaya Aura® Communication Manager Screen Reference, Release 8.1.x Issue 12 September 2021*
[4] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 8.1.x Issue 17 August 2021*

The following documentation is available on request from Enghouse at www.enghouseinteractive.es/en

[1] *ACD Sys Presence Unified Manager Manual Presence Suite*, V12.1
[2] *Presence Installation Guides Presence Software*, V12.1
[3] *PBX/ACD Requirements Presence Software*, V12.1

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.