Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.0.1 and Avaya Aura® Session Manager R6.1 to interoperate with Netcall SEMAP+ – Issue 1.1

Abstract

The Application Notes describe the configuration steps for the Netcall SEMAP+ solution to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Netcall SEMAP+ system can host multiple applications such as IVR and Voicemail via connection to Avaya Aura® Session Manager over a SIP Trunk.

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

The purpose of this document is to describe the compliance tested configuration between Avaya Aura® Session Manager and the Netcall SEMAP+ platform with Avaya Aura® Communication Manager providing telephony features configured as an Evolution Server. This document includes a description of the configuration of both the Avaya and the Netcall solutions, a description of the tests that were performed and a summary of the results of those tests.

Netcall SEMAP+ is a Speech Enabled Multi Application Platform which integrates with the Avaya solution using a SIP trunk. SEMAP+ enables the hosting of multiple solutions concurrently on the same platform.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of Netcall SEMAP+ to carry out call handling and routing using in a variety of scenarios using the ContactPortal (ASR) and Messaging+ applications. For the purposes of the compliance test the Speech Recognition and Messaging applications were used to test the call handling functions of the SEMAP+ platform. These applications were used to give a broad overview of the call handing abilities of the Netcall SEMAP+ platform and are indicative of the way calls to other SEMAP+ applications are handled.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing calls in different call scenarios, to ensure successful routing of the call depending on the application used. Call handling and routing functions are common across SEMAP+ these tests are indicative of the way SEMAP+ handles calls. However for the purpose of the compliance testing for SEMAP+, the ContactPortal® ASR and Messenger+ voicemail modular applications were used, and the tests carried out included:

- Successful Speech recognition
- Barge-in
- Correct call routing
- Transfer to busy/engaged/dnd/restricted user
- SIP REFER usage
- Hold/Retrieve
- Call Transfer
- Intra switch call

- Inbound trunk call
- Outbound trunk call
- Out of band Signaling (DTMF)
- Logging

In the case of the Messaging+ application:

- Coverage to correct mailbox
- Message retrieval
- User recognition from CPN
- MWI
- Greeting recording
- Intra switch call
- Inbound trunk call

The serviceability testing focused on verifying the ability of Netcall SEMAP+ to recover from disconnection and reconnection to the Avaya solution and power failure.

2.2. Test Results

All functionality and serviceability test cases were completed successfully with the following observation:

- In the case where an extension is called which has an unconditional divert set to another extension, and the extension being forwarded to has a divert set to the SEMAP+ Messaging+ application, the voicemail will answer on the mailbox of the person originally called e.g. 4001 calls 4002, 4002 is on unconditional divert to 4003, 4003 has divert set to the SEMAP+ Messaging+ application, call from 4001 covers to the voicemail box of 4002. This is by design.

2.3. Support

Technical support can be obtained for the Netcall SEMAP+ solution as follows:

- Email: technical.support@netcall.com
- Website: http://www.netcall.com
- Phone: + 44 330 333 6100

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of an Avaya S8800 Server running Communication Manager with Avaya G650 Media Gateway. An Avaya S8800 Server hosts Session Manager. Another Avaya S8800 Server hosts System Manager. A variety of Avaya H.323, Digital and SIP endpoints (not shown) were used in the testing. SEMAP+ was hosted on a Microsoft Windows 2003 server provided by Netcall.

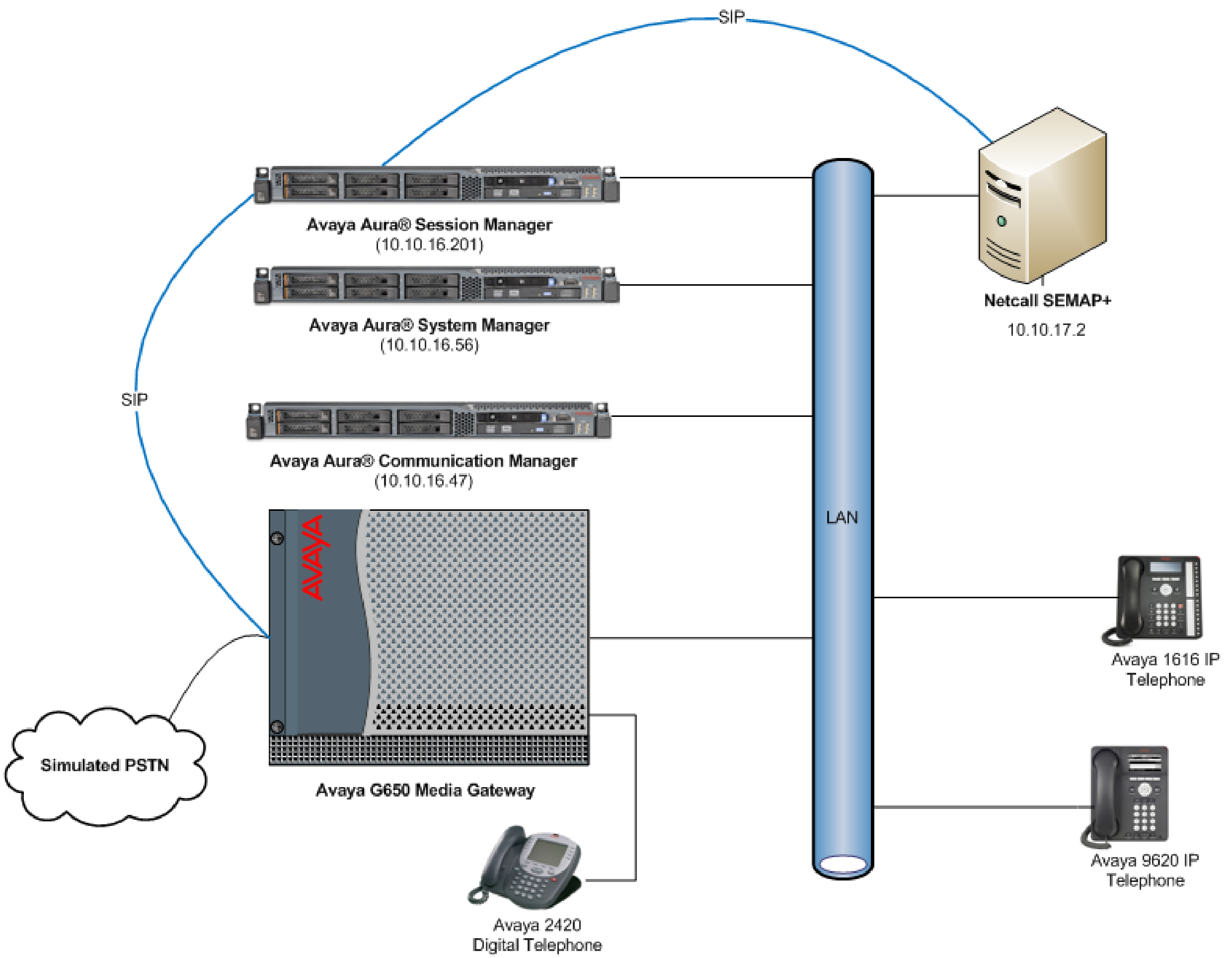


Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Session Manager and Avaya Aura® System Manager and Netcall SEMAP+ Solution.

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.0.1 SP6 R16.00.1.510.1-19350
Avaya G650 Media	• TN2602AP HW8 FW61 • TN799DP HW01 FW040 • TN 2464CP HW02 FW024
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.1 SP6 6.1.6.0.616008
Avaya Aura® System Manager running on Avaya S8800 Server	R6.1 SP6 Build Number 6.1.0.0.7345-6.1.5.606 Software Update Revision Number 6.1.10.1.1774
Avaya H323 IP Telephones	• 1616 FW 1.301S • 9620 FW 3.102S
Avaya Digital Telephone	• 2420 REL 4.00 HWV 1 FWV 4
Netcall Server	Netcall SEMAP+ 18.16 Messaging+ / Contactportal

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 as referenced in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Configure node-name
- Configure SIP Signaling Group
- Configure SIP Trunk
- Configure Route Pattern
- Configure AAR
- Configure Coverage Paths
- Configure Station

5.1. Configure Node Names

The Application Note assumes a C-LAN interface or equivalent is administered on Communication Manager. These Application Notes also assume that the Session Manager SIP Signaling Interface has been configured on Session Manager. In order to create the SIP Trunk between Communication Manager and Session Manager a node-name needs to be specified for the Session Manager SIP Signaling Interface, this will be used in **Section 5.2**. Enter the command **change node-names ip** and enter an identifying **Name** for the Session Manager SIP Signaling Interface and its **IP address**, in this case **sesmgr-sm100** and **10.10.16.201** respectively. Take a note here of the C-LAN node name, **clancm601**.

```
change node-names ip                                              Page   1 of
2
                                  IP NODE NAMES
    Name                  IP Address
clancm601               10.10.16.31
default                 0.0.0.0
devconaes61             10.10.16.30
ipo7.0                  10.10.16.105
medprocm601             10.10.16.32
procr                   10.10.16.47
procr6                  ::
sesmgr-sm100            10.10.16.201















( 8  of 8    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
```

5.2. Configure SIP Signaling Group

A signaling group must be used to specify the signaling type and node-names to be used for the SIP Trunk configured in **Section 5.3**. Enter the command **add signaling-group next**, take a note of the **Group Number**, set the **Group Type** to **sip**, **Transport Method** to **tcp**, set the **Near-end Node Name** to the node name of the C-LAN, in this case **clancm601**, and the **Far-end Node Name** to that configured in **Section 5.1**, in this case **sesmgr-sm100**. Leave all other settings as default.

```
add signaling-group next                                      Page   1 of   1
                                SIGNALING GROUP

 Group Number: 2              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: clancm601             Far-end Node Name: sesmgr-sm100
 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? y                     Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

5.3. Configure SIP Trunk

To route calls between Communication Manager and Session Manager the SIP trunk must use the signaling group setup in **Section 5.2**. Enter the command **add trunk-group next**, on **Page 1** take a note of the **Group Number**, this will be used when configuring route patterns. Set the **Group Type** to **sip** and assign the trunk an identifying **Group Name.** Set the **TAC** according to the dialplan. Set the **Service Type** as **public-ntwrk** and assign the **Signaling Group** as added in **Section 5.2**, set **Number of Members** according to requirements.

```
add trunk-group 2                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 2                   Group Type: sip            CDR Reports: y
  Group Name: SIP TRUNK TO SES-MGR        COR: 1        TN: 1        TAC: 702
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 2
                                                    Number of Members: 30
```

On **Page 3** set the **Numbering Format** as **Private**.

```
add trunk-group 2                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                       Maintenance Tests? y



                     Numbering Format: private
                                               UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

On **Page 4** set the **Send Diversion Header** to **y** and the **Identity for Calling Party Display** to **From**.

```
add trunk-group 2                                                    Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? y
                  Support Request History? n
             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: From
                             Enable Q-SIP? n
```

5.4. Configure Route Pattern

In order to place calls from via Communication Manager to Session Manager and on to SEMAP+ a route pattern must be created from Communication Manager to Session Manager. The route pattern will use the trunk created in **Section 5.3**. Enter the command **change route-pattern x** where **x** is an unused route pattern, configure an identifying **Pattern Name**, the **Grp No** setup in the previous Section, and an **FRL** accordingly.

```
change route-pattern 2                                                Page   1 of   3
                    Pattern Number: 2   Pattern Name: to ses-mgr
                             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: 2    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
```

5.5. Configure Dialplan

Enter the command **change dialplan analysis** to configure the digit string to be routed to Session Manager and onto SEMAP+. In the example below, **Dialed String** beginning with **85** and a **Total Length** of **4** is set to the **call type udp**, this will route the dialed string to the uniform dialplan for further classification.

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

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   13          4   ext       #           3   fac
   15          4   ext
   16          4   ext
   18          4   ext
   2           3   ext
   30          4   ext
   4           4   ext
   5           1   fac
   70          3   dac
   71          3   dac
   77          3   ext
   85          4   udp
   9           1   fac
   *           3   fac
```

5.6. Configure Uniform Dialplan

Enter the command **change uniform-dialplan 85**, set the **Matching Pattern** to **85**, the **Len** to **4** and the **Net** to **aar**, this will route the 4 digit number beginning with **85** to the **aar** table where a route pattern is defined.

```
change uniform-dialplan 85                                      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
```

5.7. Configure AAR

The AAR table must be configured in order that calls to SEMAP+ are routed using the pattern configured in **Section 5.4**. Enter the command **change aar analysis 0**, in this example when a **4** digit number beginning with digits **85** is dialed, it will be placed using route pattern **2**. Configure the **Dialed String 85**, **Min 4** and **Max 4**, **Route Pattern 2** and **Call Type aar** as shown below.

```
change aar analysis 0                                            Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 0

          Dialed             Total      Route     Call   Node  ANI
          String            Min  Max   Pattern    Type   Num   Reqd
    85                      4    4      2         aar          n
    201                     3    3      4         aar          n
    2456                    4    4      2         aar          n
    400                     3    3      5         aar          n
    5                       7    7      999       aar          n
    6                       7    7      999       aar          n
    7                       7    7      999       aar          n
    8                       5    5      3         aar          n
    9                       7    7      999       aar          n
                                                               n
```

5.8. Configure Coverage Paths

Cover paths must be administered in order to route calls to the SEMAP+ Messaging+ application. For the purposes of the compliance test, both a cover path and a remote cover path were added. Enter the command **change coverage remote 1**, enter the extension assigned in **Section 7.3** for voicemail deposit, in this case **8502** in an available field, in this example **02**. This is referred to as r2.

```
change coverage remote 1                                           Page   1 of  23

                       REMOTE CALL COVERAGE TABLE
                       ENTRIES FROM 1    TO 1000

01: 90857412987           16:                        31:
02: 8502                  17:                        32:
03:                       18:                        33:
04:                       19:                        34:
05:                       20:                        35:
06:                       21:                        36:
07:                       22:                        37:
08:                       23:                        38:
09:                       24:                        39:
10:                       25:                        40:
11:                       26:                        41:
12:                       27:                        42:
13:                       28:                        43:
14:                       29:                        44:
15:                       30:                        45:
```

Enter the command **add coverage path next**, take a note of the **Coverage Path Number**, in this case **5**, and enter **r2** in **Point 1**.

```
add coverage path next                                          Page   1 of   1
                                 COVERAGE PATH

                   Coverage Path Number: 5
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?            n               n
               Busy?            y               y
       Don't Answer?            y               y        Number of Rings: 2
                All?            n               n
 DND/SAC/Goto Cover?            y               y
   Holiday Coverage?            n               n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: r2             Rng:    Point2:
  Point3:                        Point4:
  Point5:                        Point6:
```

5.9. Configure Station

A station must be administered with the coverage path configured in the previous section for use with the SEMAP+ Messaging+ application. Enter the command **add station x** in this case station **4001** is used. Configure according to requirements and set the **Coverage Path** to **5**.

```
add station 4001                                             Page   1 of   5
                                     STATION

Extension: 4001                           Lock Messages? n             BCC: 0
     Type: 9620                           Security Code: 1234           TN: 1
     Port: S00018                       Coverage Path 1: 5             COR: 1
     Name: Richard Pope                 Coverage Path 2:               COS: 1
                                        Hunt-to Station:
STATION OPTIONS
                                            Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                  Message Lamp Ext: 4001
            Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal               Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? y

                                               IP Video Softphone? n
                               Short/Prefixed Registration Allowed: default

                                                Customizable Labels? y
```

6. Configure Avaya Aura® Session Manager

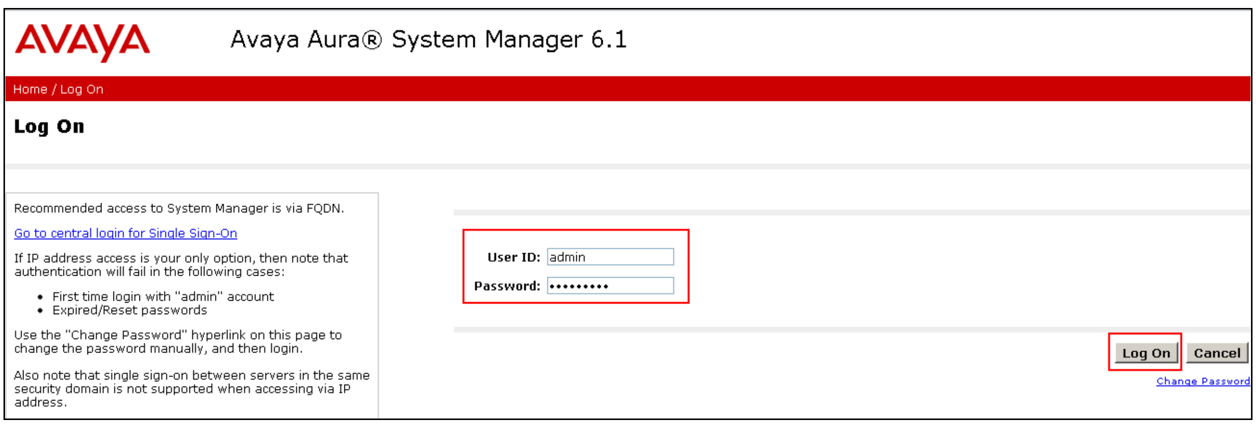
System Manager is used to configure Session Manager SIP Entities and manages the connections between related SIP trunks and endpoints. It is also used to configure dial patterns and route calls according to defined rules. The configuration and verification operations illustrated in this section were all performed using the System Manager Web Interface.

This section provides the procedure for configuring Session Manager. For further reference documents, refer to **Section 10** of this document. The procedures include the following areas:

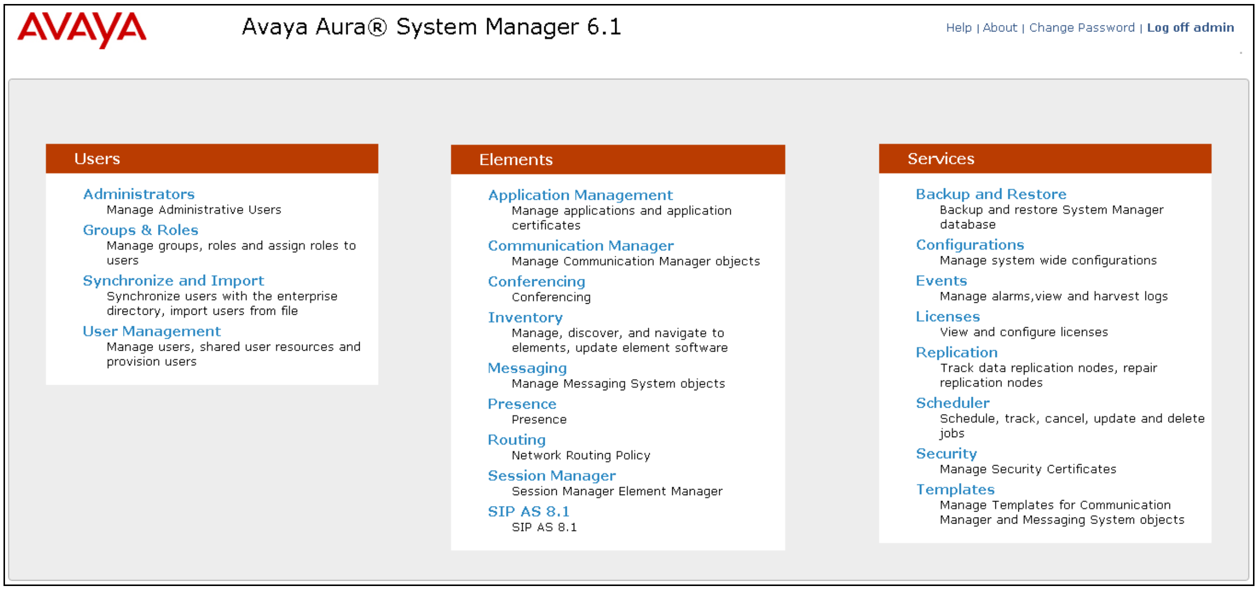
- Log in to Avaya Aura® System Manager
- Administer Adaptation
- Administer SIP Entity
- Administer Entity Link
- Administer Routing Policies
- Administer Dial Patterns

6.1. Log in to Avaya Aura® System Manager

Log into the System Manager web interface using the System Manager IP address, in this case https://10.10.16.56/index.jsp enter the appropriate credentials and click **Log On**.

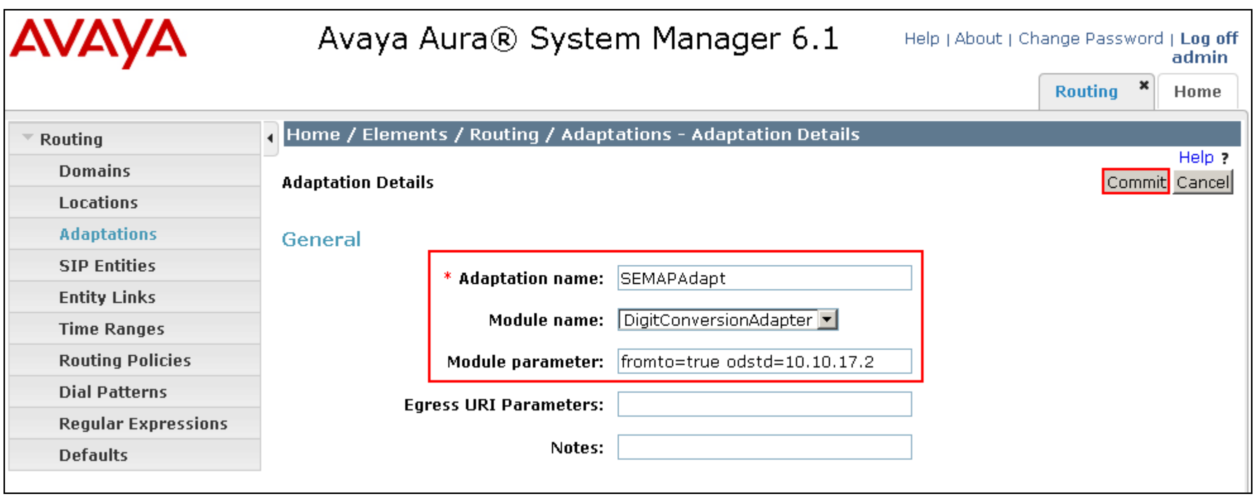


The home screen is divided into three sections with hyperlinked categories below.



6.2. Administer Adaptation

In order for successful interoperation of SEMAP+ with Session Manager over a SIP trunk, an Adaptation must be configured to replace the outbound domain destination with the IP address of the SEMAP+ server. Click **Home → Elements → Routing →Adaptations→New** assign and identifying **Adaptation name**, select **Click to add module** from the drop down box next to **Module Name** and set the **New Module Name** to **DigitConversionAdapter,** set the **Module Parameter** to **fromto=true odstd=10.10.17.2** and click on **Commit**.

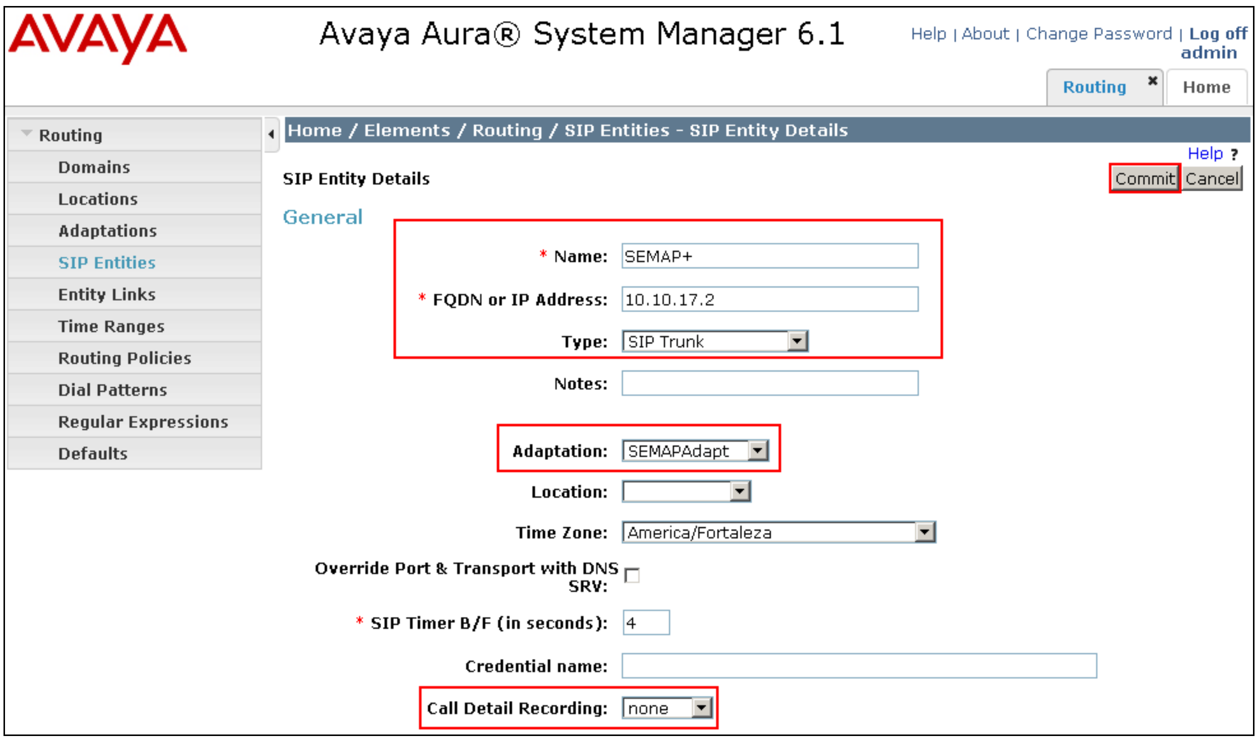


6.3. Administer SIP Entity

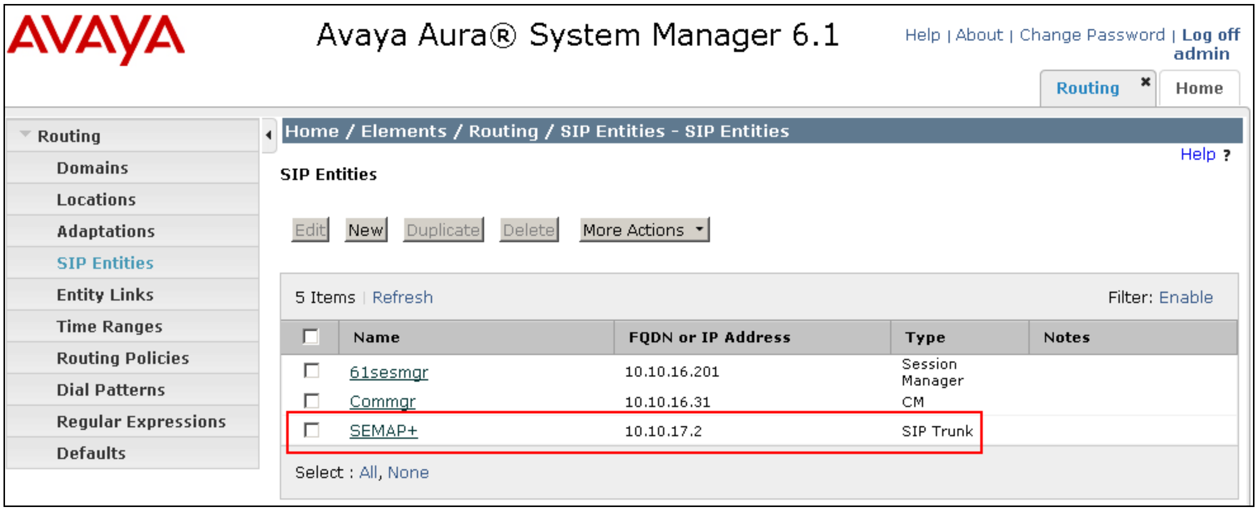
Each SIP device (other than Avaya SIP Phones) that communicates with the Session Manager requires a SIP Entity configuration. This section details the steps to create SIP Entity for the SEMAP+ Solution.

6.3.1. Configure Netcall SEMAP+ Entity

Click **Home → Elements → Routing → SIP Entities → New** assign an identifying **Name**, the **FQDN or IP Address** for the SEMAP+ server, set the **Type** to **SIP Trunk**, choose the **Adaptation** configured in **Section 6.4** from the drop down box and set **Call Detail Recording** to **none**, leave all other settings default and click **Commit**.



The screen below will now be displayed confirming the entry.

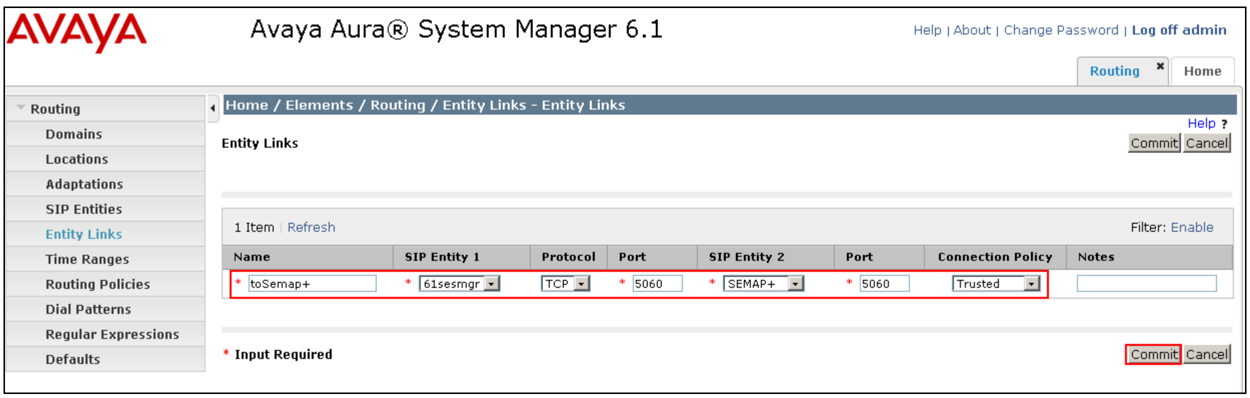


6.4. Administer SIP Entity Link

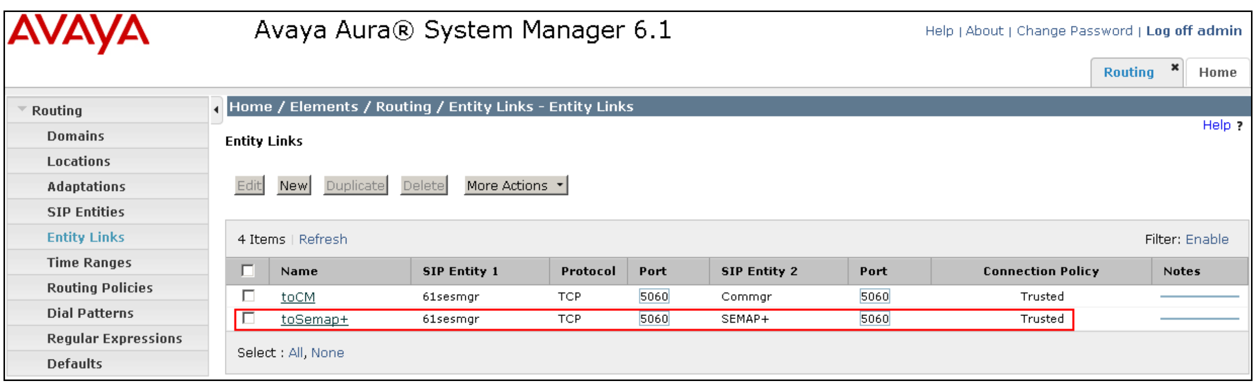
A SIP Trunk between a Session Manager and a telephony system is described by an Entity Link. An Entity Link needs to be created between Session Manager and SEMAP+.

6.4.1. Administer SIP Entity Link from Avaya Aura® Session Manager to Netcall SEMAP+

Click on **Home → Elements → Routing → Entity Links → New** assign an identifying **Name** choose the entity assigned to the Session Manager SIP Signaling Interface as **SIP Entity 1**, set the **Protocol** as **TCP**, enter **5060** for the **Port**, choose the SEMAP+ entity as **SIP Entity 2** and set the **Port** to **5060**, select **Trusted** from the **Connection Policy** drop down box. Click **Commit** when done. This establishes the Session Manager end of the SIP Trunk to SEMAP+.



The screen below will be shown confirming the entry.

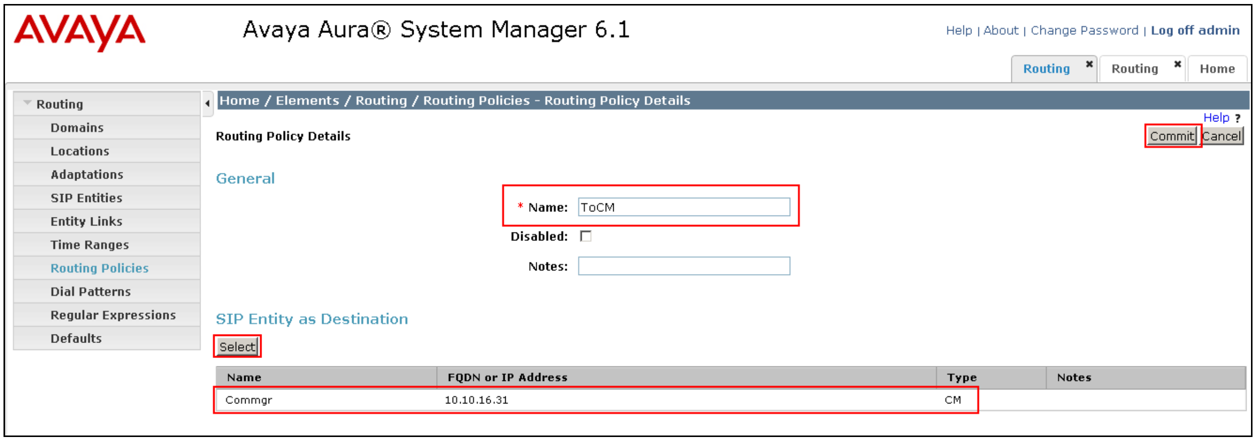


6.5. Administer Routing Policies

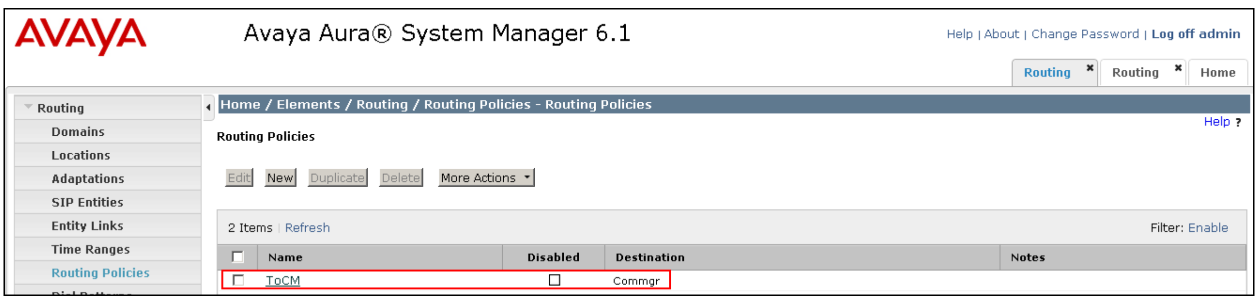
To complete the routing configuration, a Routing Policy is created. Routing policies direct how calls will be routed to an attached system. Two routing policies must be created, one for the Communications Manager and the second for SEMAP+. These will be associated with the Dial Patterns created in **Section 6.10**.

6.5.1. Create Routing Policy to Avaya Aura® Communication Manager

Click **Home → Elements → Routing → Routing Polices →New** assign an indentifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select** and choose the CM SIP Entity and click **Select**. Click **Commit** when done.

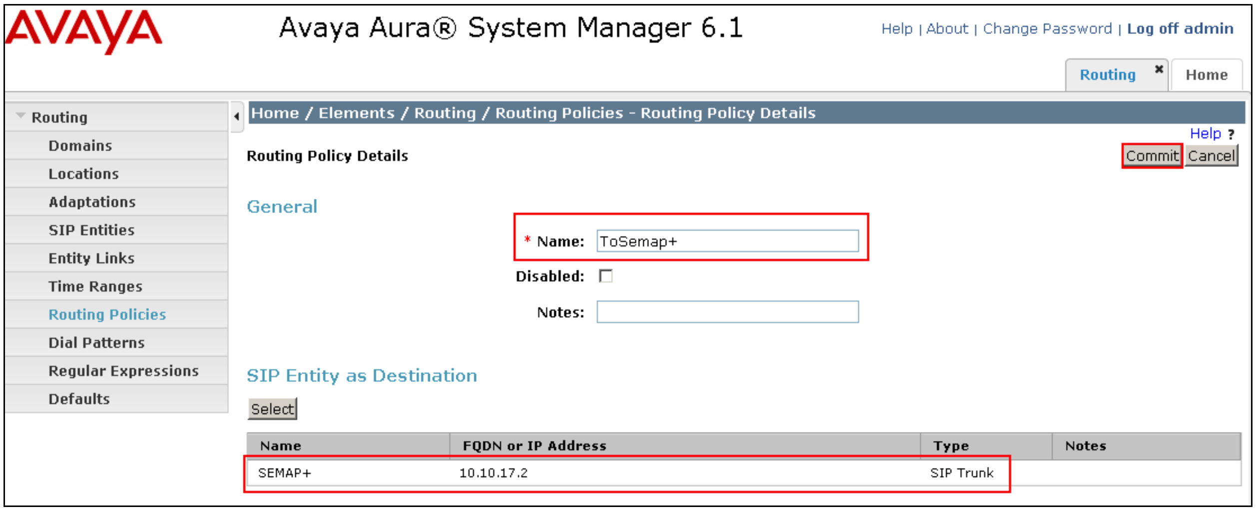


The screen below will be shown confirming the entry.

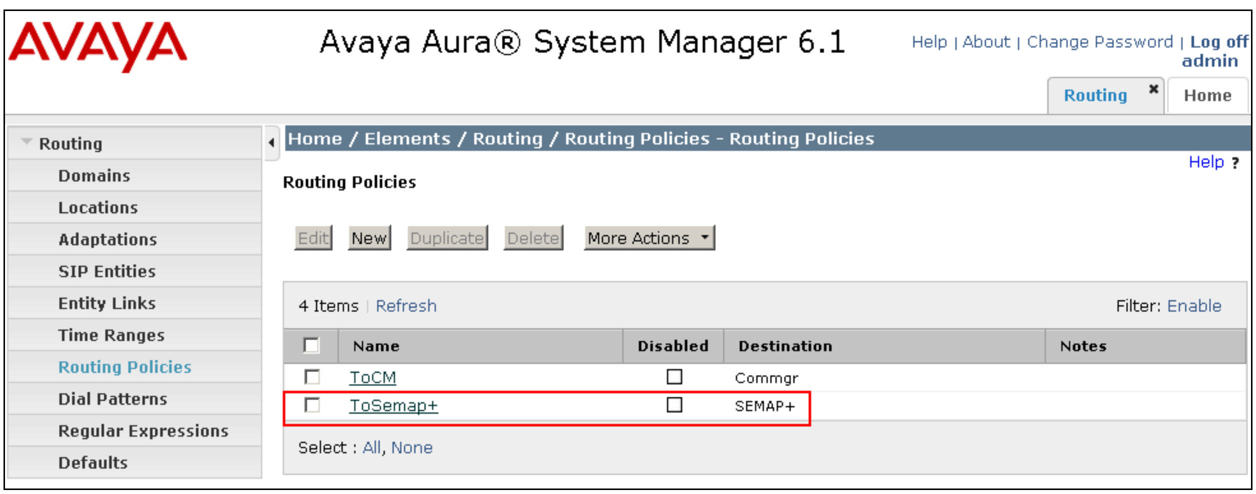


6.5.2. Create Routing Policy to Netcall SEMAP+

Click **Home → Elements → Routing → Routing Polices →New** assign an indentifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select** and choose the **SEMAP+** SIP Entity and click **Select**. Click **Commit** when done.



The screen below will be shown confirming the entry.

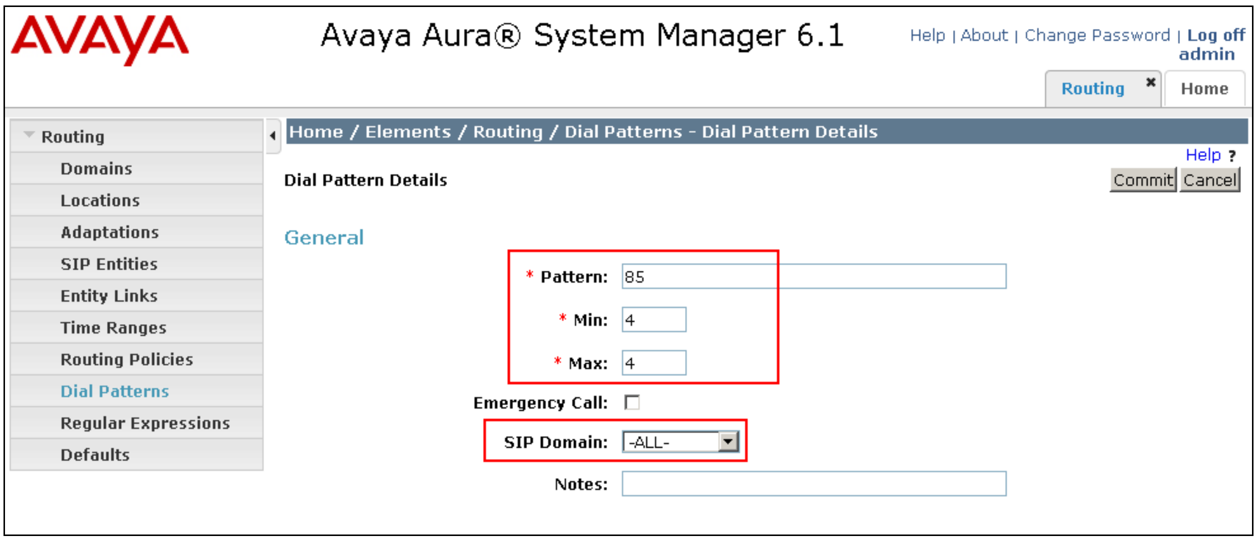


6.6. Administer Dial Patterns

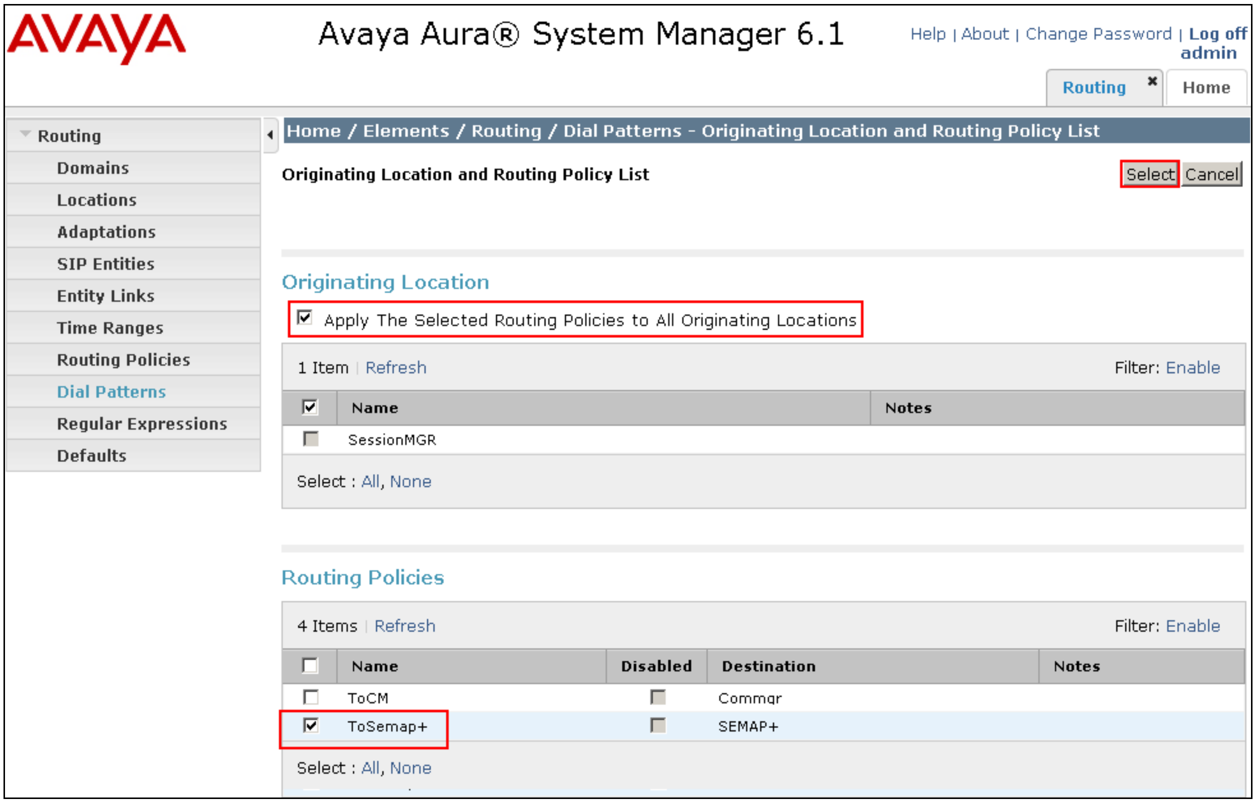
As one of its main functions, Session Manager routes SIP traffic between connected devices. Dial Patterns are created as part of the configuration to manage SIP traffic routing, which will direct calls based on the number dialed to the appropriate system.

6.6.1. Create Dial Pattern for calls to Netcall SEMAP+

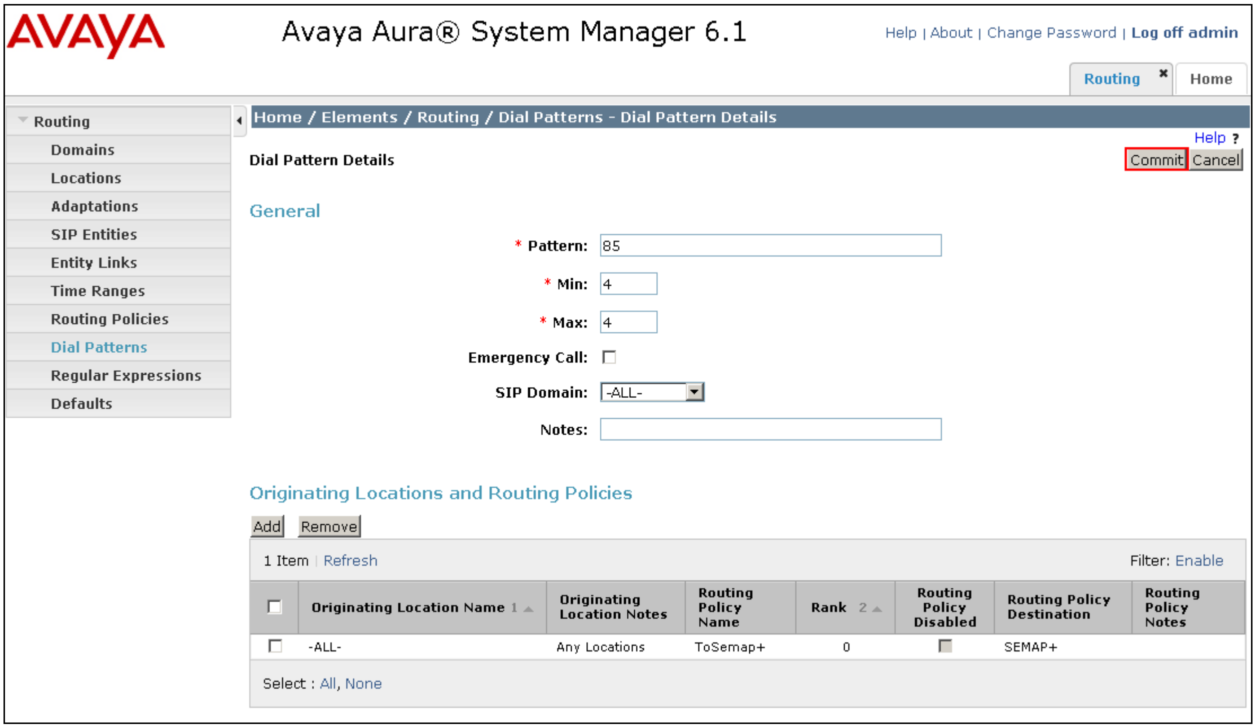
In **Section 5.7** Communication Manager is configured to route **4** digit strings beginning with **85** to Session Manager. To create a Dial Pattern to route these digits from Session Manager to SEMAP+ click **Home → Elements → Routing → Dial Patterns →New.** Under **Pattern** enter the numbers presented to Session Manager by Communication Manager in the **Patterns** box. Set **Min** and **Max** digit string length, and set **SIP Domain** to **ALL**.



In the **Originating Locations and Routing Policies** section of the web page, click **Add.** In the **Origination Location** section place a tick in the box next to **Apply The Selected Routing Policies to All Originating Locations**, in the **Routing Policies** section click the routing policy created for SEMAP+. Click **Select** when done.



Click **Commit** when complete.



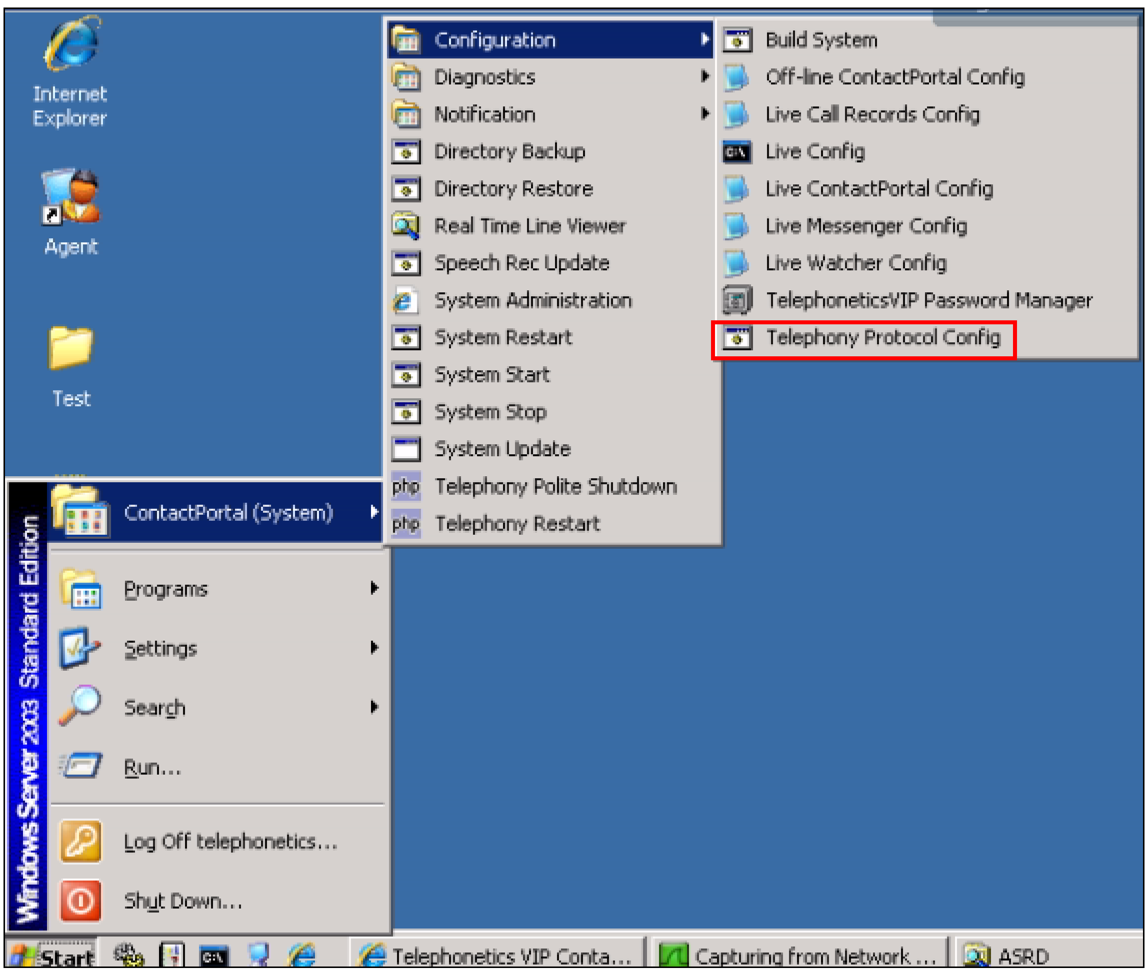
7. Configure Netcall SEMAP+

These Application Notes assume that a SIP build of SEMAP+ v18.16 with a G5 SEMAP+ processor or above is provided and installed by Netcall. Administration of the interface between SEMAP+ and the Avaya solution is summarized as follows:

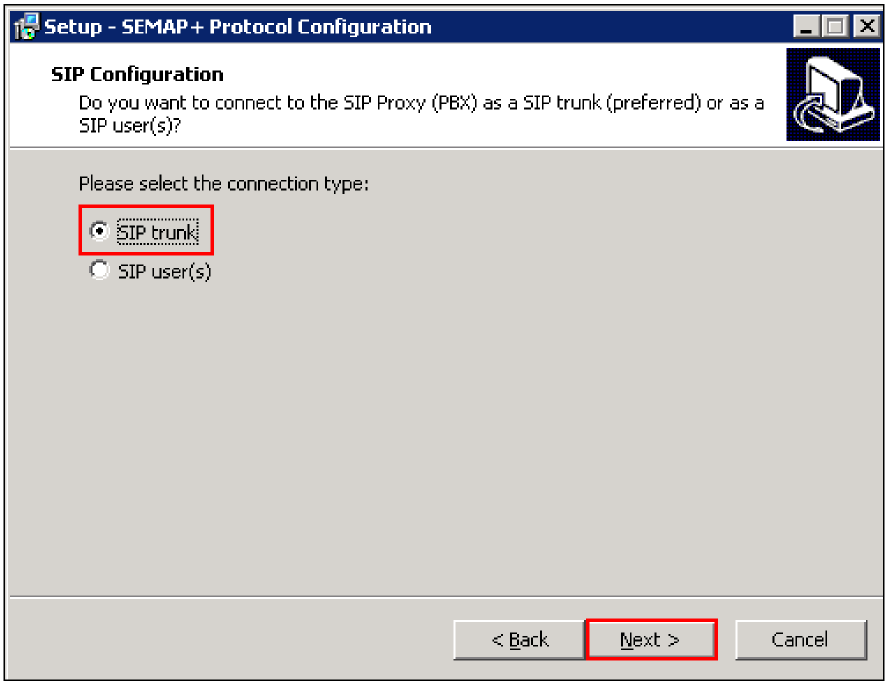
- Netcall SEMAP+ Protocol Configuration Wizard Setup
- Configure Netcall SEMAP+ Avaya MWI Special Settings
- Configure Netcall SEMAP+ Routing Rules
- Configure Netcall SEMAP+ Number Range Details
- Configure Netcall SEMAP+ Test User and Mailbox

7.1. Netcall SEMAP+ Protocol Configuration Wizard Setup

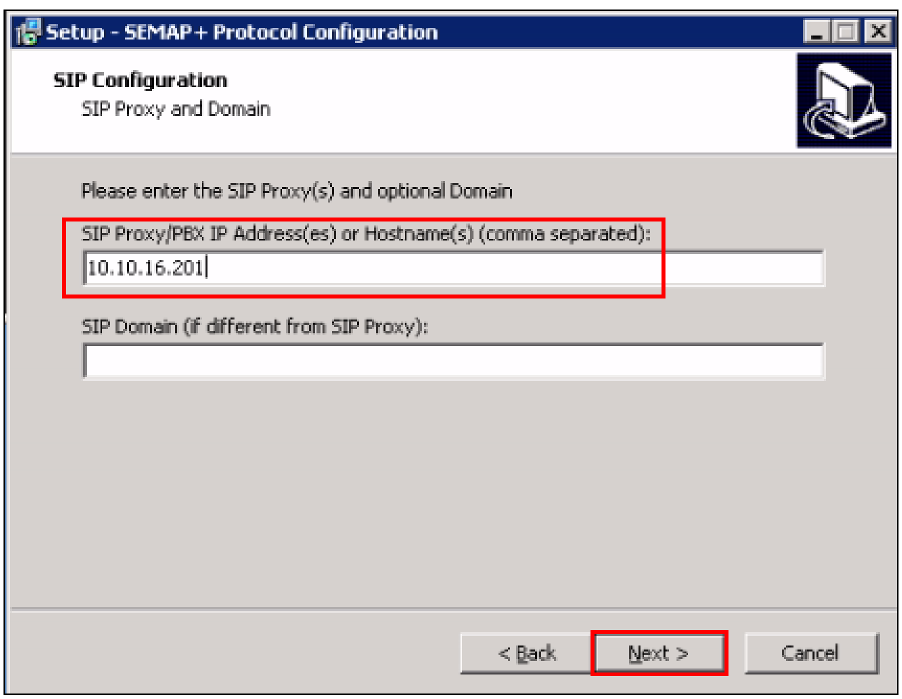
On the SEMAP+ server log in to the Windows OS and click **Start → ContactPortal → Configuration → Telphony Protocol Config**.



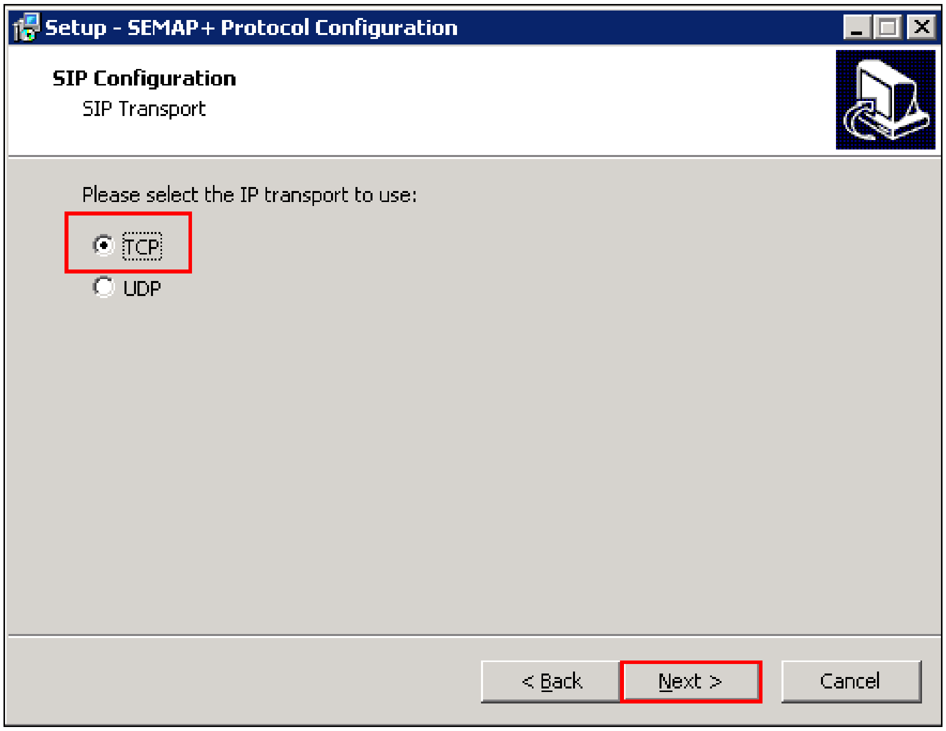
A familiar setup Microsoft Software Installer will start, choose the relevant SEMAP+ program option (not shown) and click next. At the **SIP Configuration** page click the radio button next to **SIP trunk** and click **Next**.



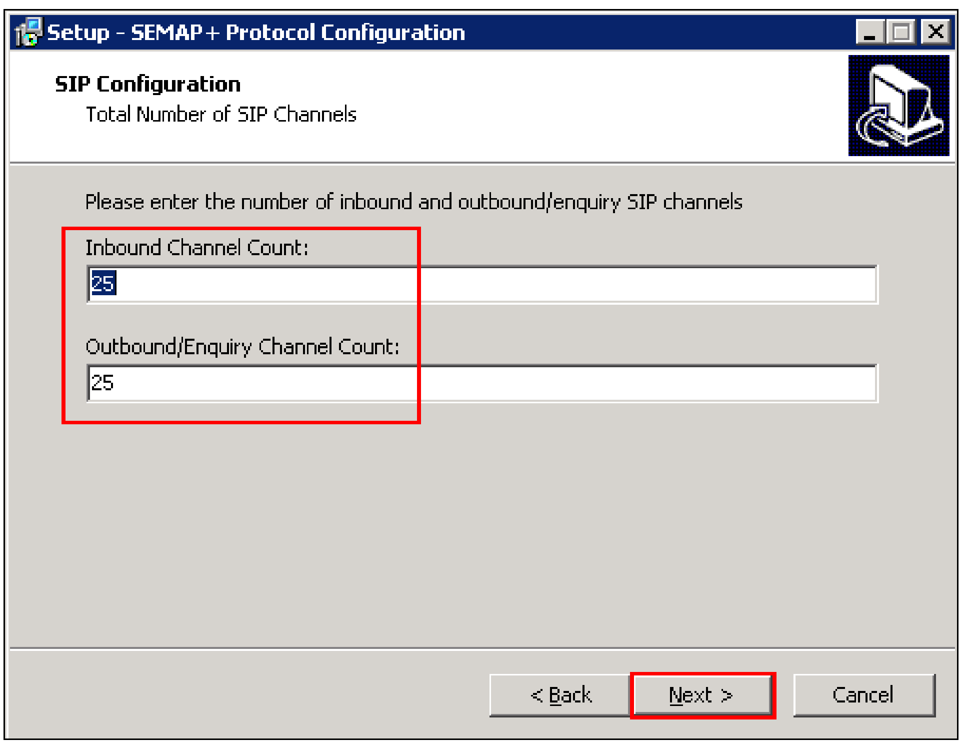
Enter the IP address of the Session Manager SIP Signalling interface in the **SIP Proxy/PBX IP Address(es) or Hostname(s) (comma separated):** box as shown below and click **Next**.



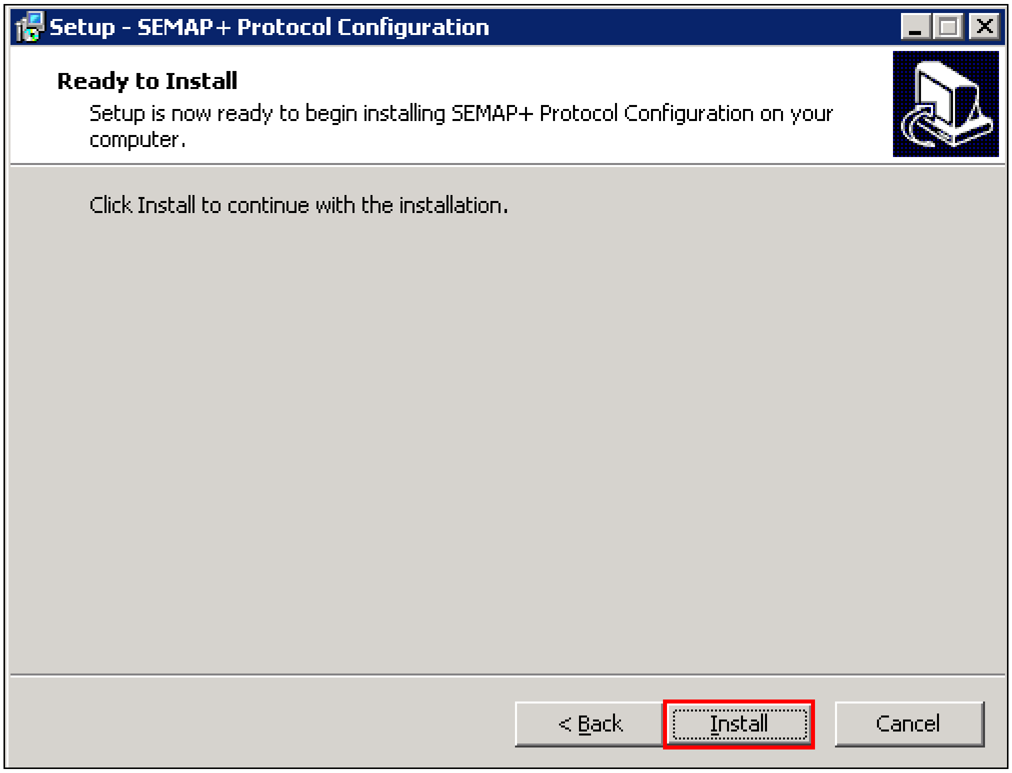
In the screen that appears, select **TCP** as the IP transport to use, and click **Next**.



Enter the **Inbound Channel Count** and **Outbound/Enquiry Channel Count**, according to requirements, as shown below and click **Next**.

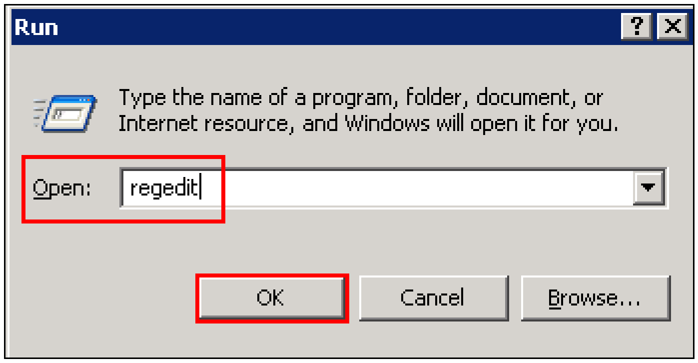


Click **Install** to complete the installation with the configuration specified.



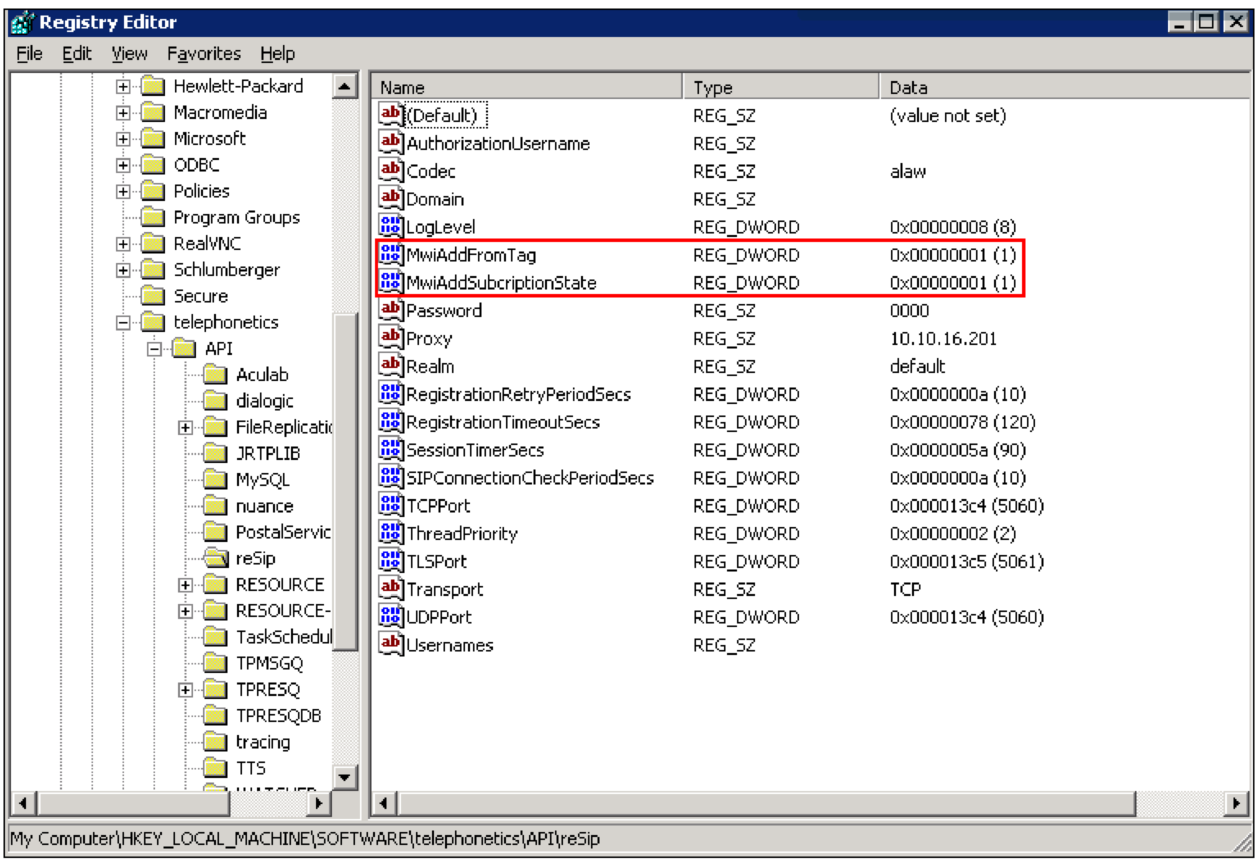
7.2. Configure Netcall SEMAP+ Avaya MWI Special Settings

On the SEMAP system two registry keys need to be added to ensure the MWI is sent to Session Manager in the correct format. From the SEMAP+ OS, click **Start → Run** type **regedit** in the Open box, and click **OK**.



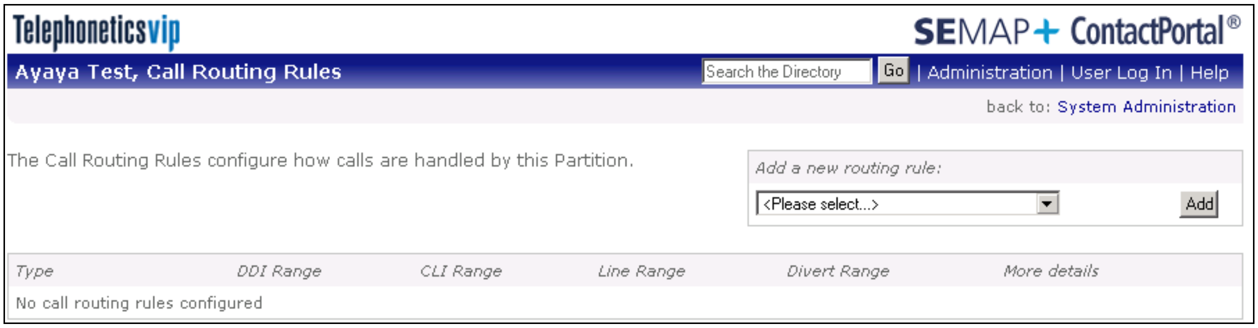
Navigate to **[HKEY_LOCAL_MACHINE\SOFTWARE\Telephonetics\API\reSip]** and add the following as shown below:

- **MwiAddSubcriptionState=dword:00000001**
- **MwiAddFromTag=dword:00000001**



7.3. Configure Netcall SEMAP+ Routing Rules

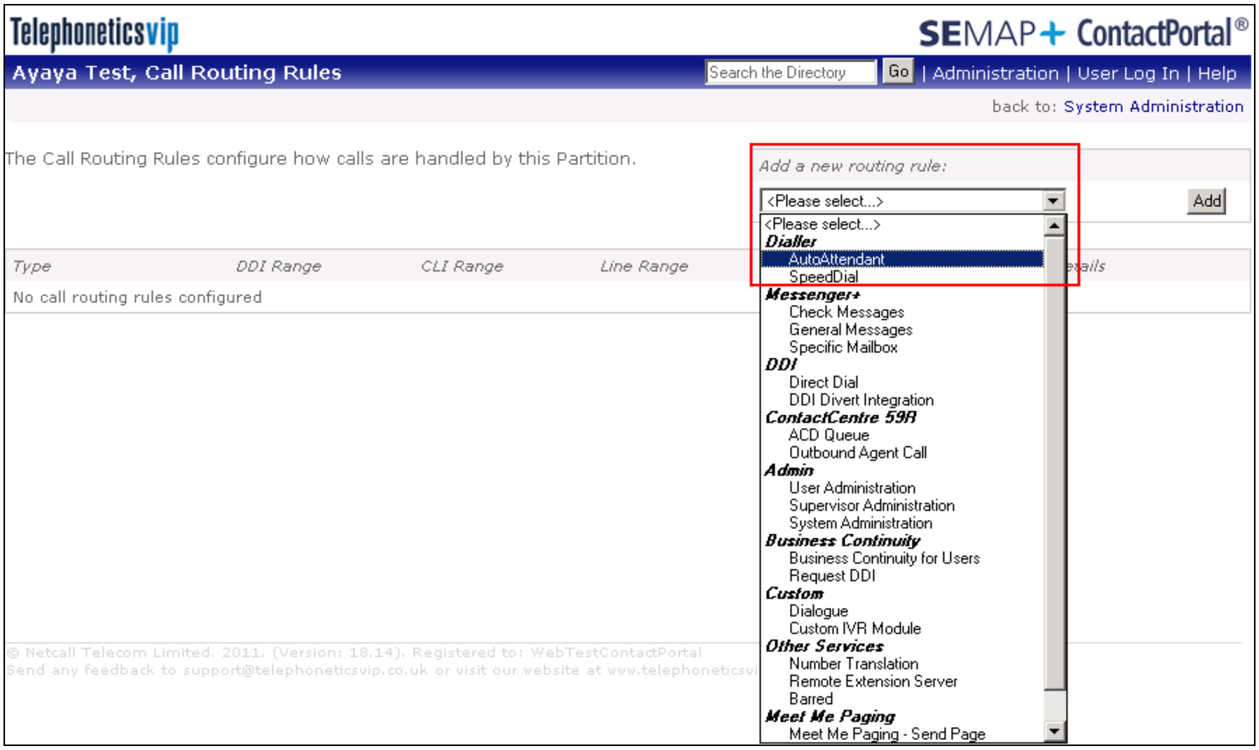
The SEMAP+ routing rules must be configured with the access number assigned in **Section 5.6**. Access the web interface of the SEMAP+ server using http://IP_OF_SEMAP+_SERVER/padmin and log in using the credentials provided by Netcall. Click **Partition Administration → Log In → System Settings → Call Routing** the screen shown below will appear.



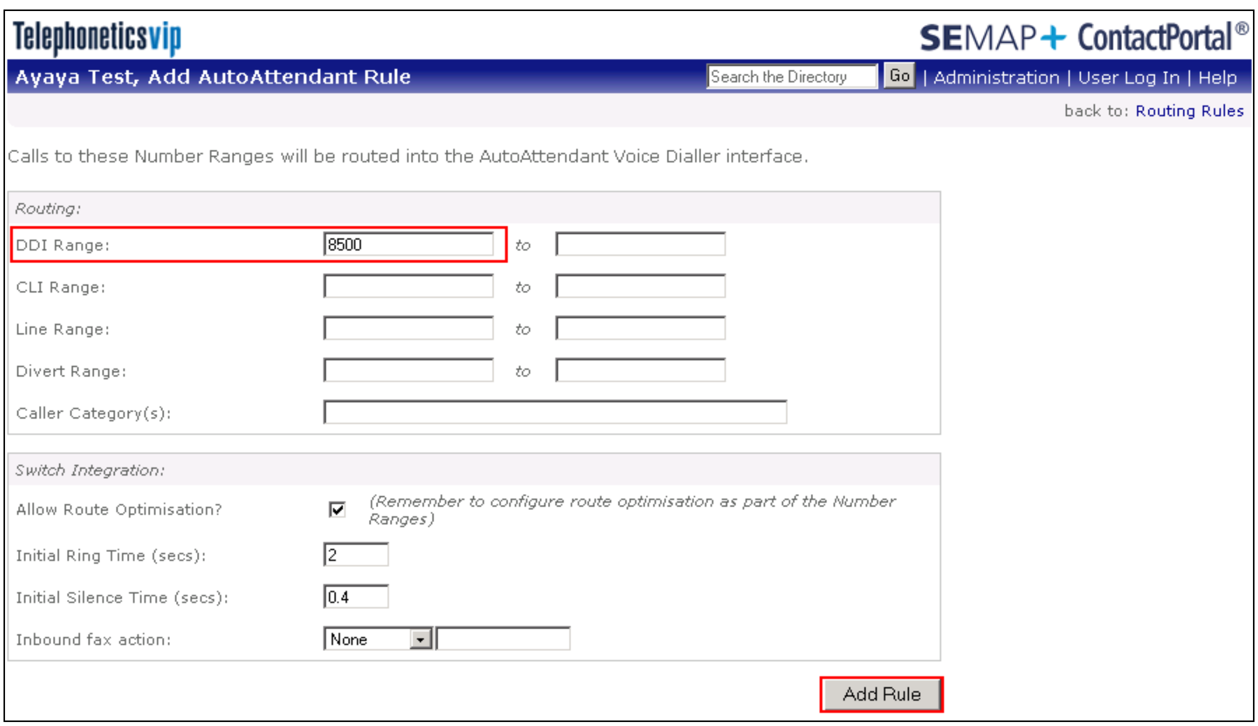
For the purposes of the compliance test, three call routing rules are created:

- 8500 – ContactPortal AutoAttendant
- 8502 – Voicemail Deposit
- 8503 - Voicemail Retrieval

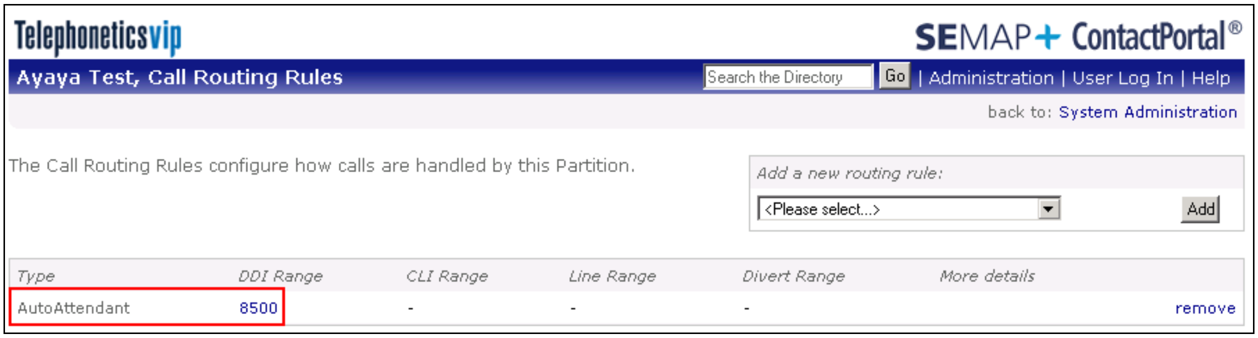
Select **AutoAttendant** under the **Dialler** section, from the **Add a new routing rule** drop down box.



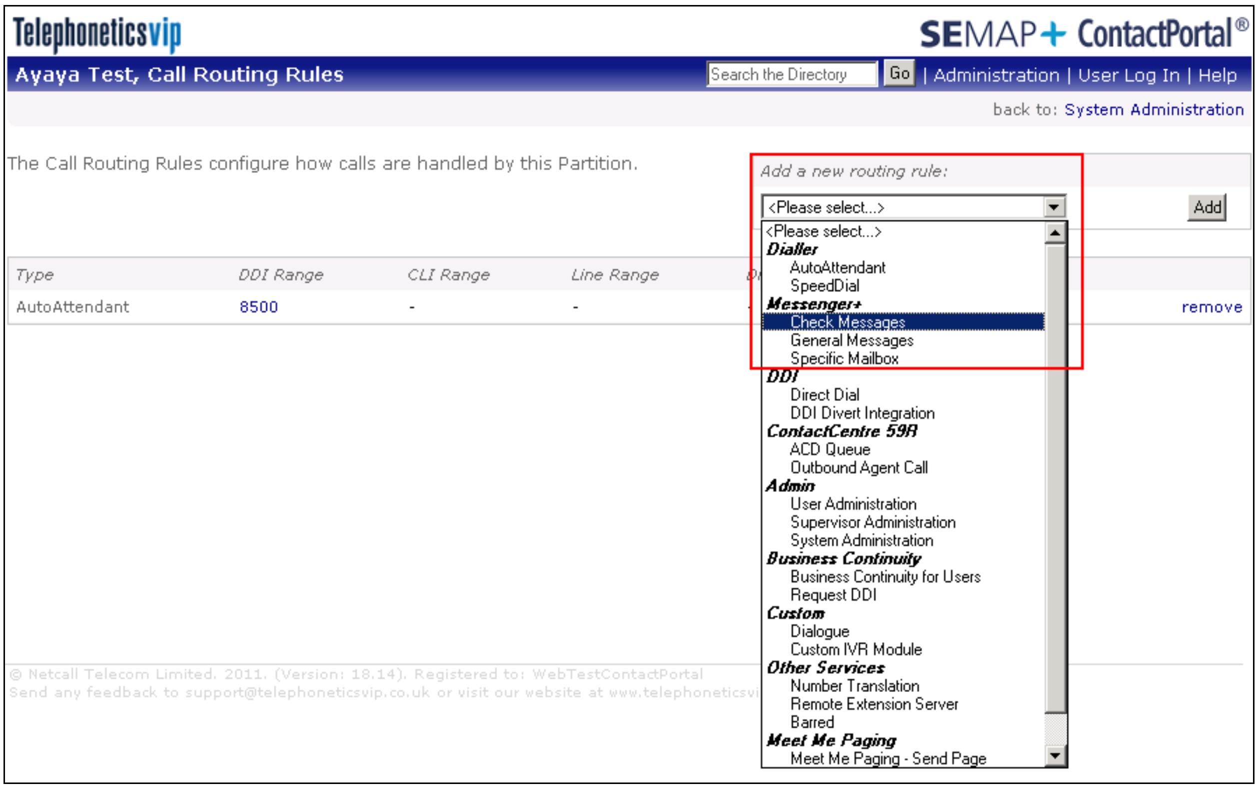
Enter **8500** in the **DDI Range** box, leave all other settings as default and click **Add Rule**.



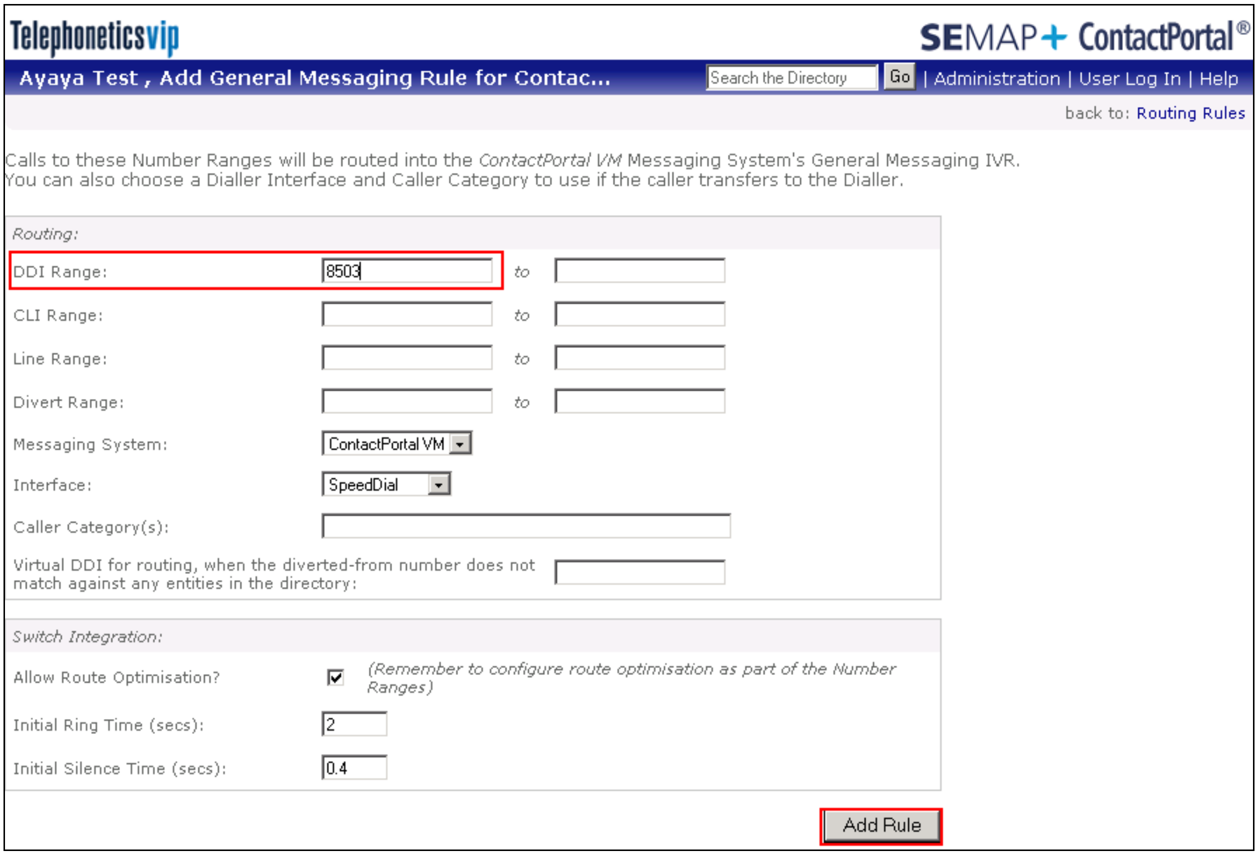
The screen below will appear showing the added **AutoAttendant** Rule.



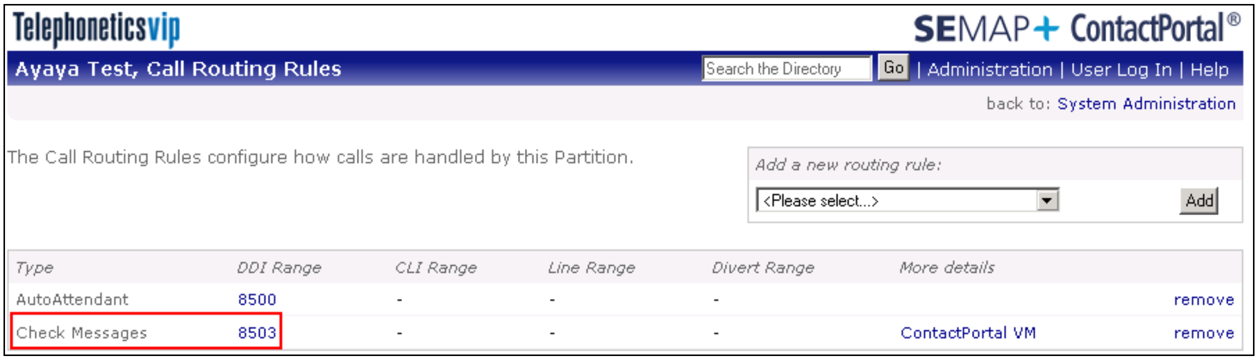
Select **Check Messages** under the **Messenger+** section, from the **Add a new routing rule** drop down box.



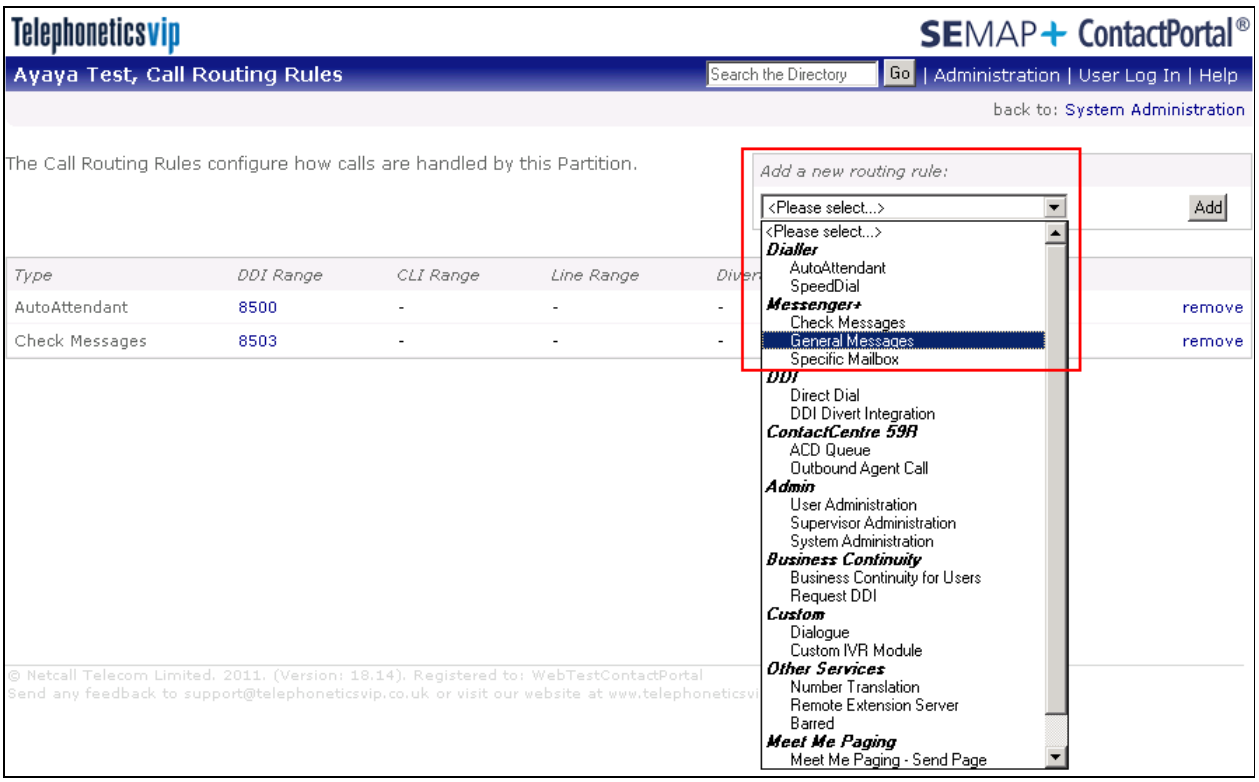
Enter **8503** in the **DDI** field, leave all others settings as default and click **Add Rule**.



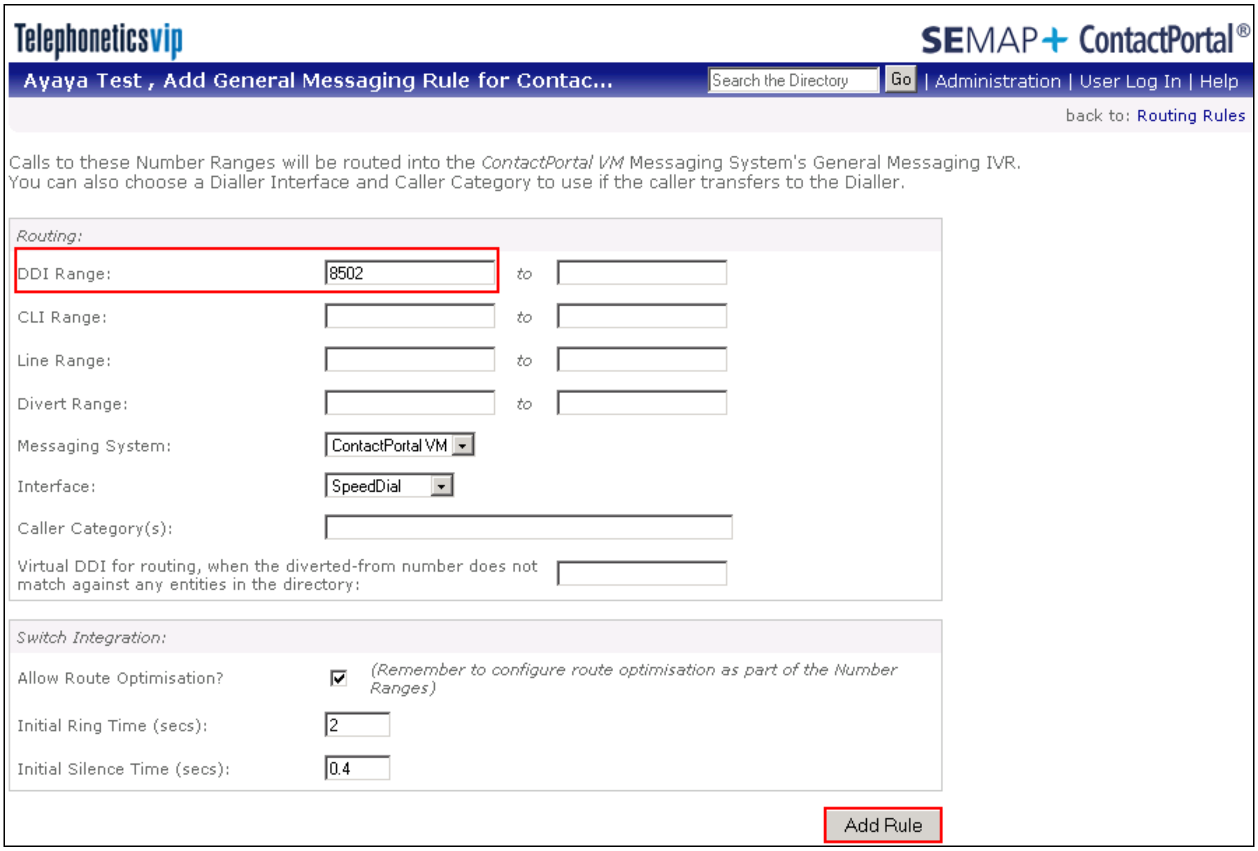
The screen below will appear showing the added **Check Messages** Rule.



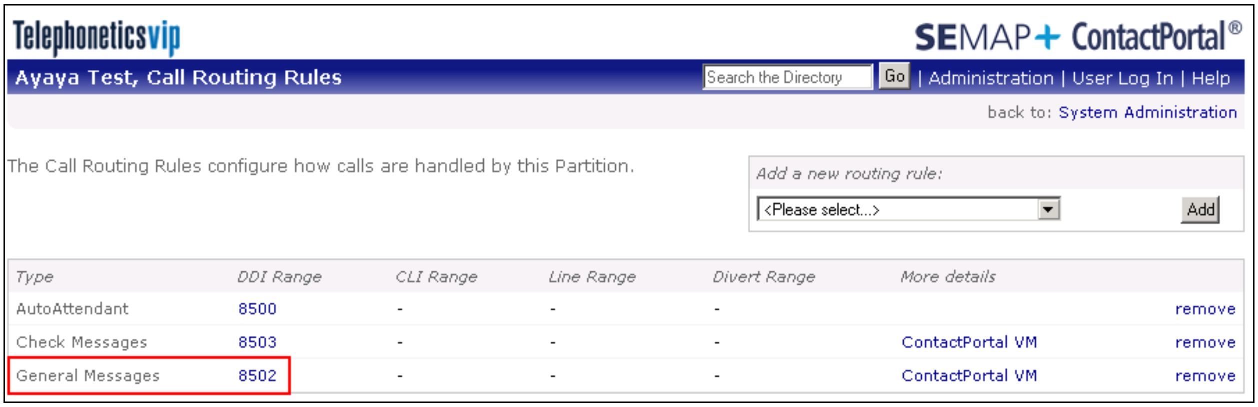
Select **General Messages** under the **Messenger+** section, from the **Add a new routing rule** drop down box.



Enter **8502** in the **DDI** field, leave all others settings as default and click **Add Rule**.

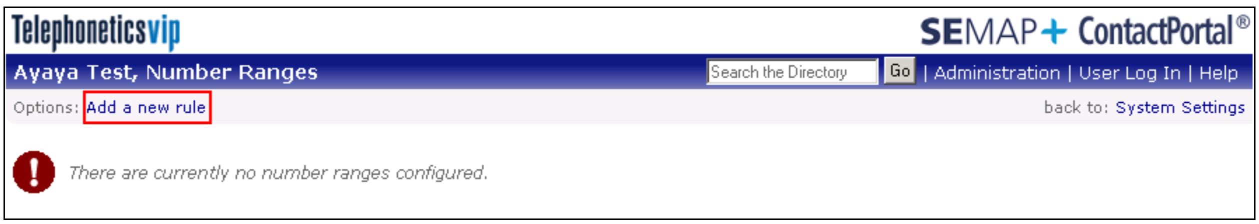


The screen below will appear showing the added **General Messages** Rule.



7.4. Configure Netcall SEMAP+ Number Range Details

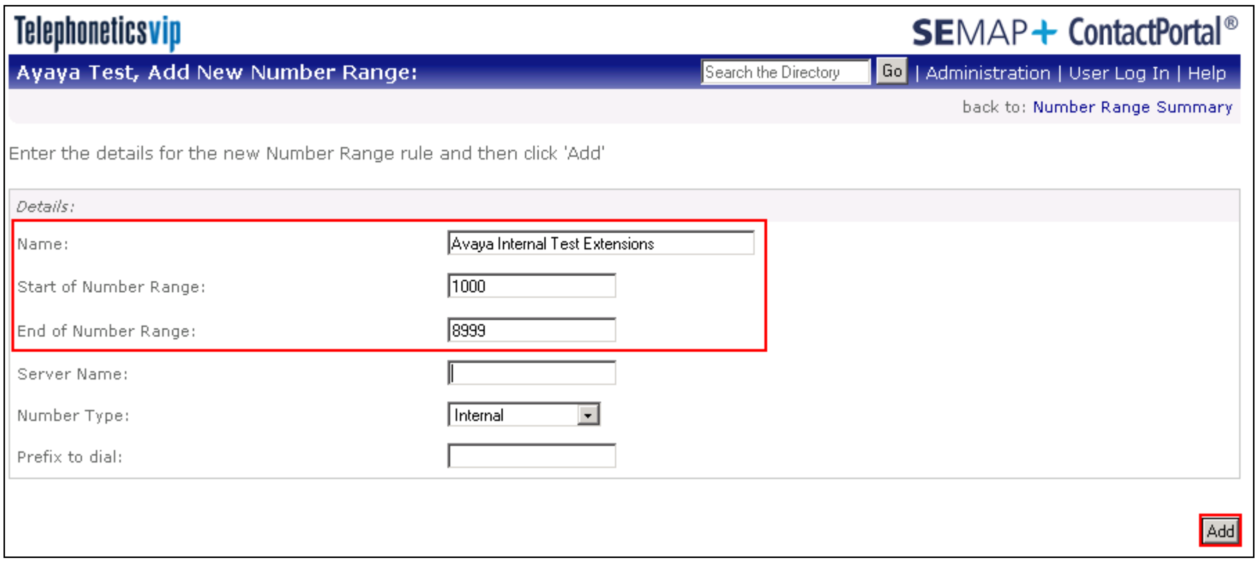
Routing rules must be configured to define internal, external and barred numbers. Click **System Administration → Number Range Details → Add a new rule**.



For the purposed of the compliance test, three new routing rules are added:

- Internal Numbers
- External Number
- Barred Number

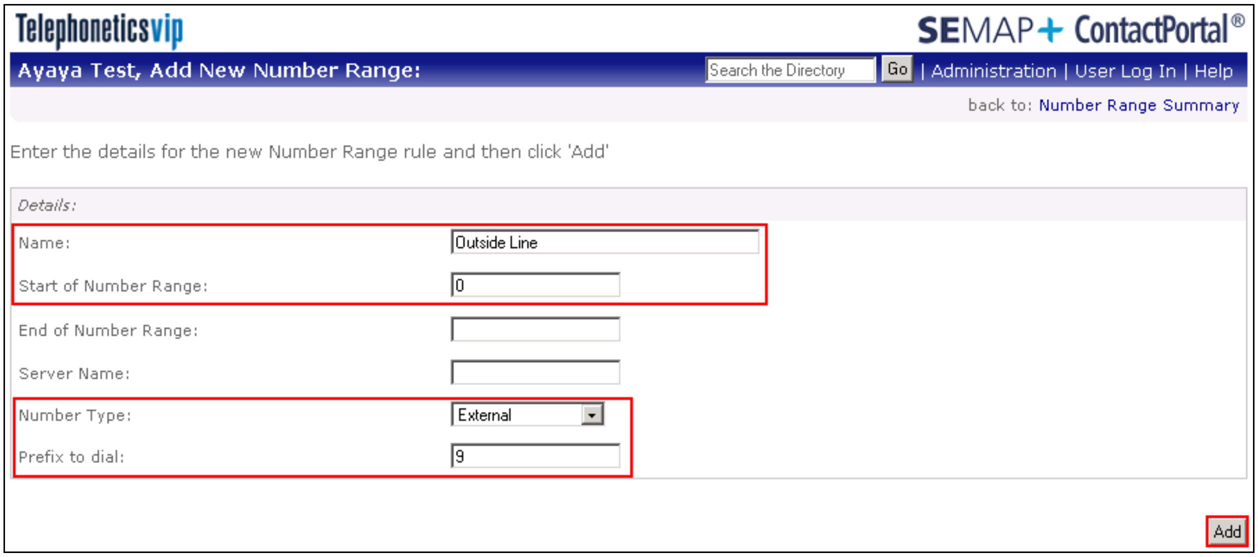
In the **Name** field enter an identifying name for the rule, in this case **Avaya Internal Test Extensions**, enter the **Start of Number Range** and **End of Number Range** accordingly, in this case **1000** and **8999** respectively, Leave all other fields as default and click **Add**.



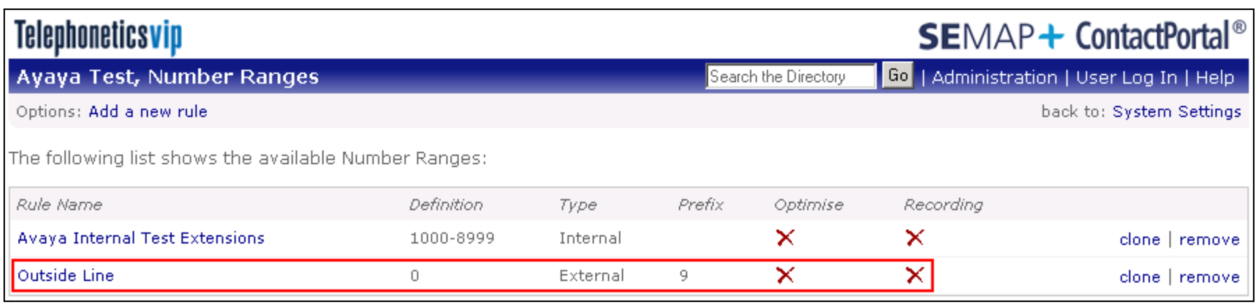
The following screen will appear displaying the new rule.

Note that Optimise is disabled, this rule can be edited to enable Optimise. This feature of SEMAP+ uses SIP REFER to free up SEMAP+ resources.

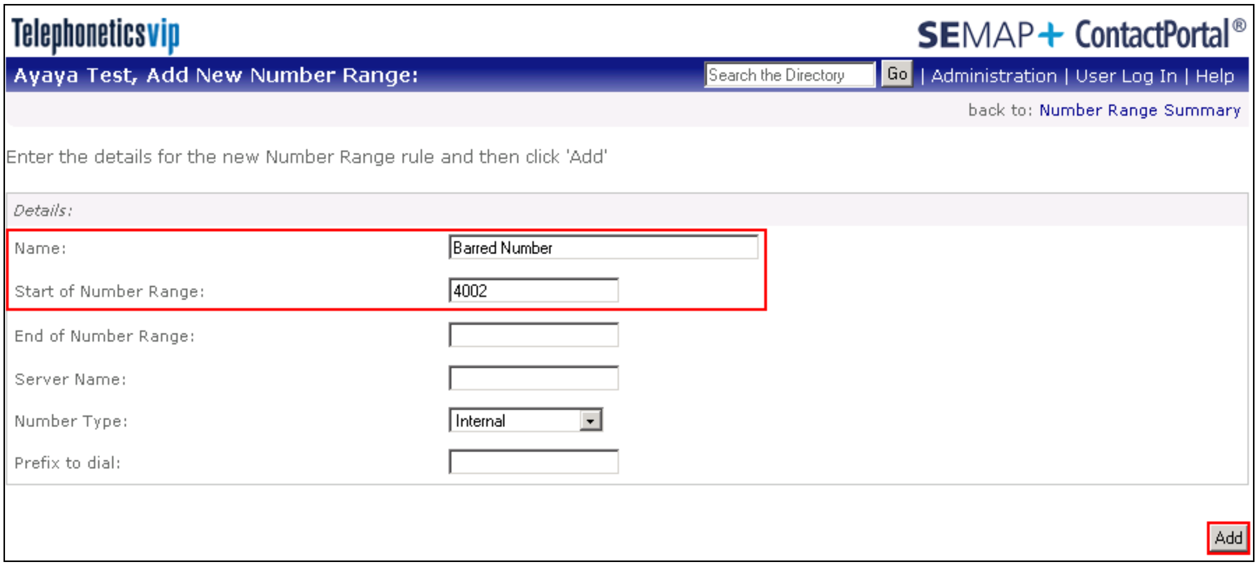
Click **Add a new rule,** in the **Name** field enter an identifying name for the rule, in this case **Outside Line**, set the **Start of Number Range** as **0**, this it the first digit for an external call, select **External** from the **Number Type** drop down box, and set **Prefix to dial** as **9** leave all other fields as default and click **Add**.



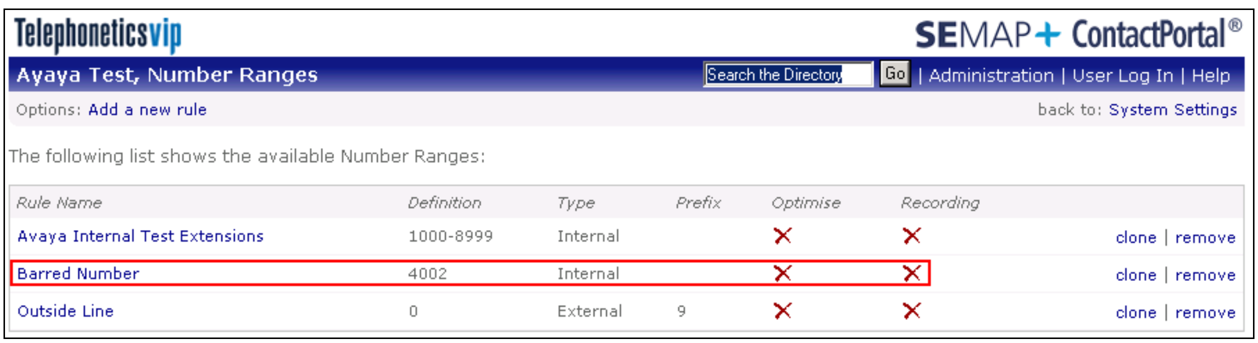
The following screen will appear displaying the new rule.



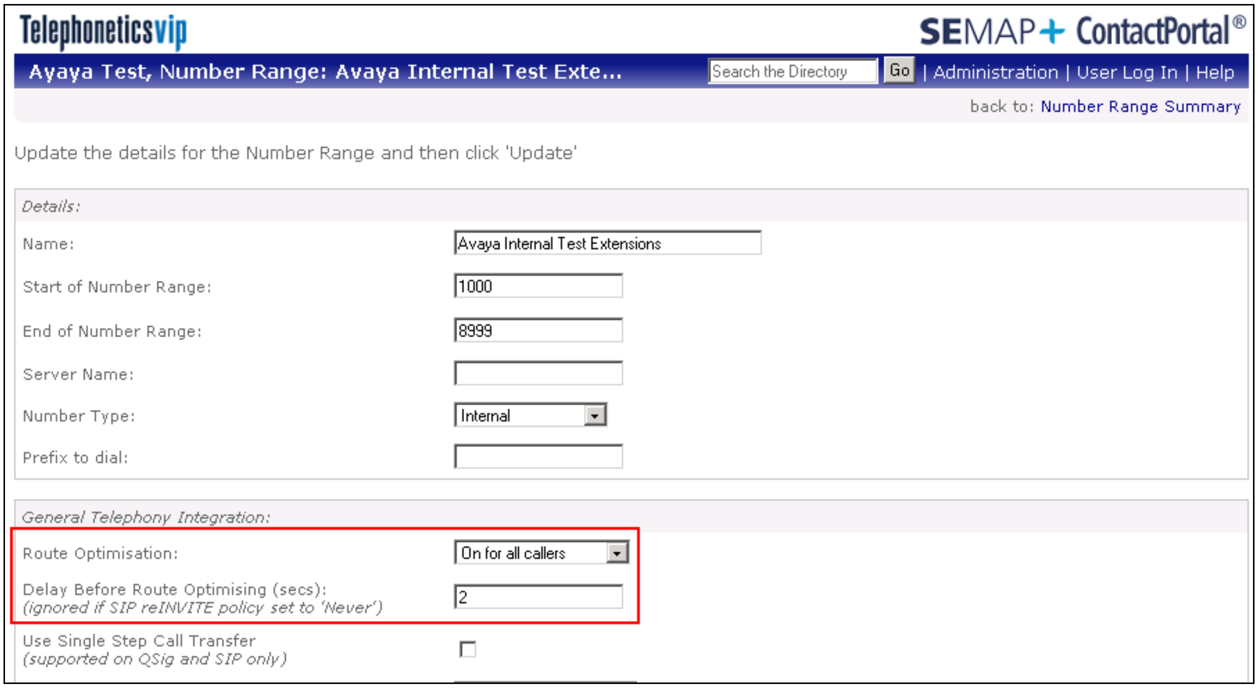
Click **Add a new rule,** in the **Name** field enter an identifying name for the rule, in this case **Barred Number**, set the **Start of Number Range** as **4002**, leave all other fields as default and click **Add**.



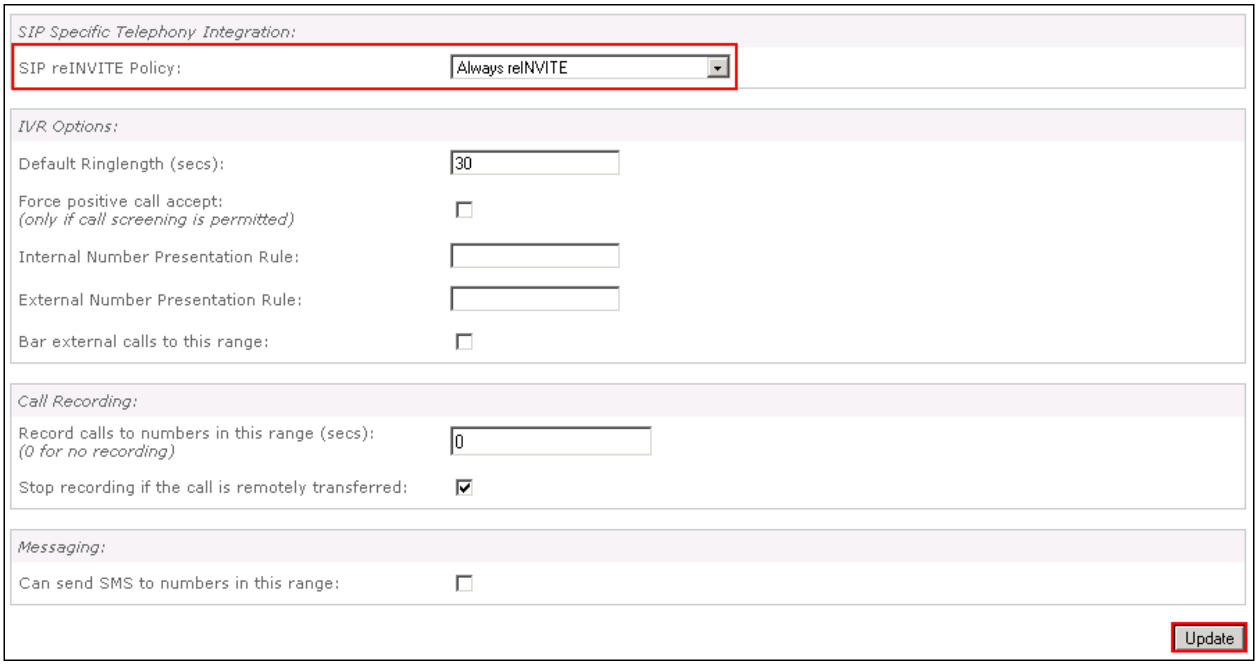
The following screen will appear displaying the new rule.



Once administered, the routing rules can be edited, click on the routing rule to edit, by default **Route Optimisation** is **Off** and **Delay** is set to **0,** change **Route Optimisation** to **On for all callers** and **Delay Before Route Optimising (secs)** to **2**. This will enable SIP REFER to take place 2 seconds until the established call.



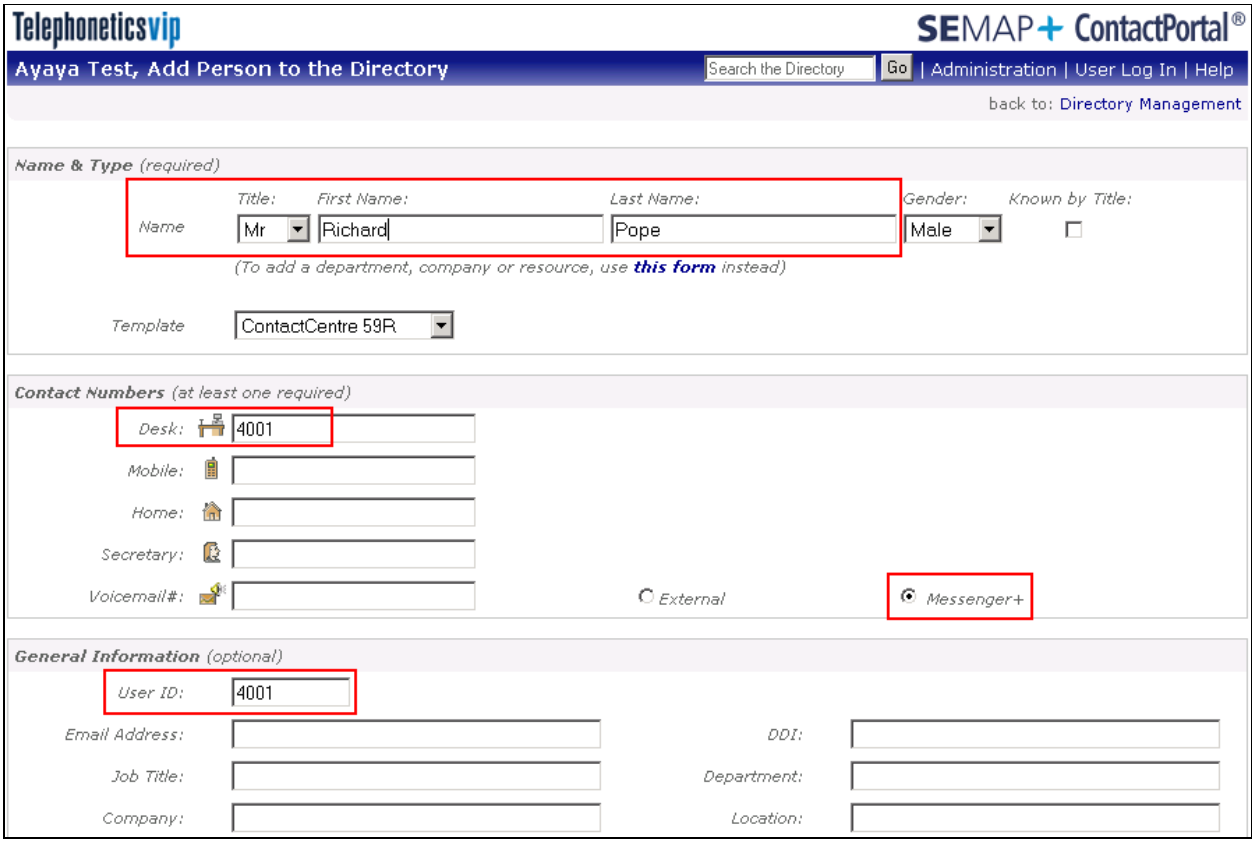
Scroll down the page and select **Always reINVITE** from the **SIP reINVITE Policy** drop down box, this will enable shuffling, it is not recommended that this is used where call recording is used in the solution. Click **Update** when done.



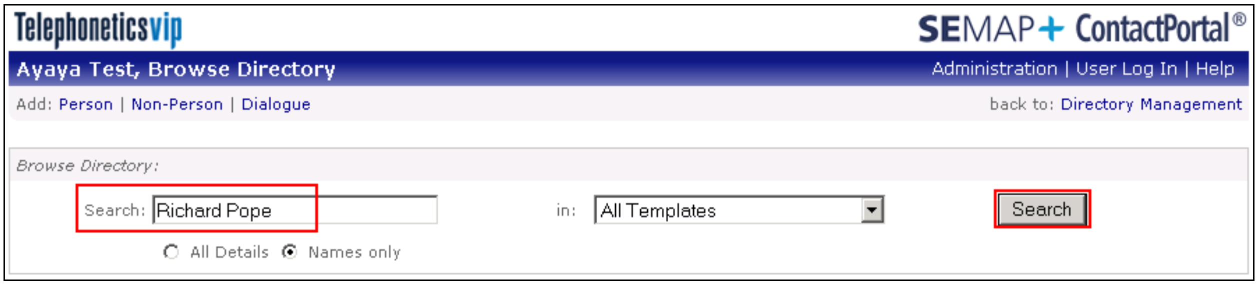
7.5. Configure Netcall SEMAP+ Test User and Mailbox

For the purposes of the compliance test, users are added manually. Continuing from the Number Range Details page click **System Settings → Administration Home → Directory Management** the screen below will appear, click on **Add a new Person**.

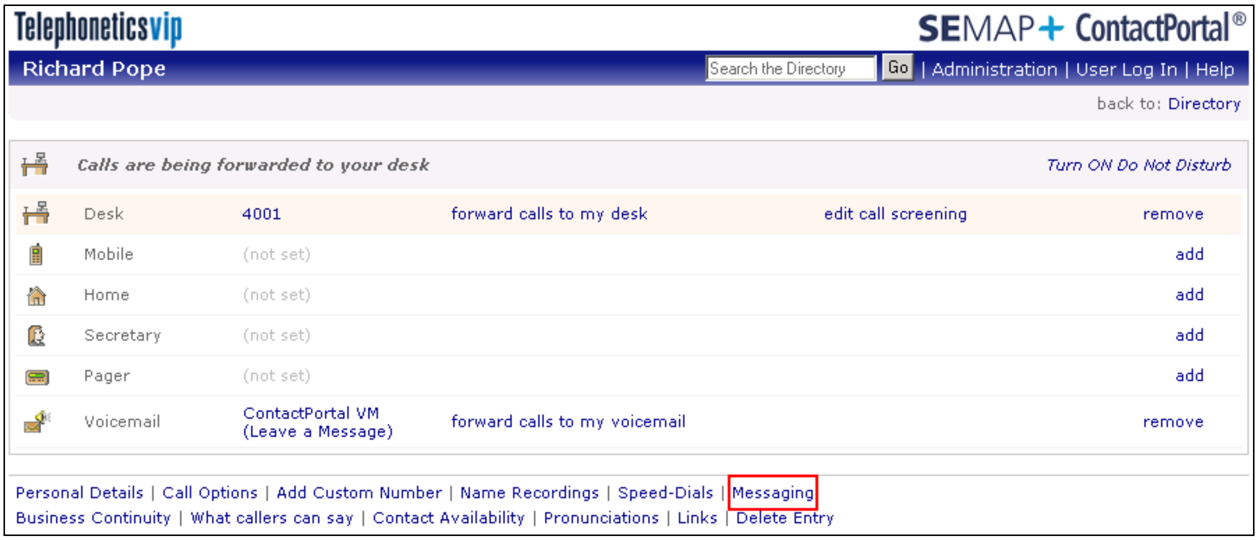
Enter the details and extension number as required, in this case the **Title, First Name** and **Last Name** are defined. Under the **Contact Numbers** section the **Desk** number is set to **4001** and a tick is placed next to **Messenger+** to define that this user has a voicemail box. In the **General Information** section the **User ID** is set to **4001**, click **Add Entry** (not shown) when done.



Click **Search Directory**, enter the name of the added user and click **Search**.

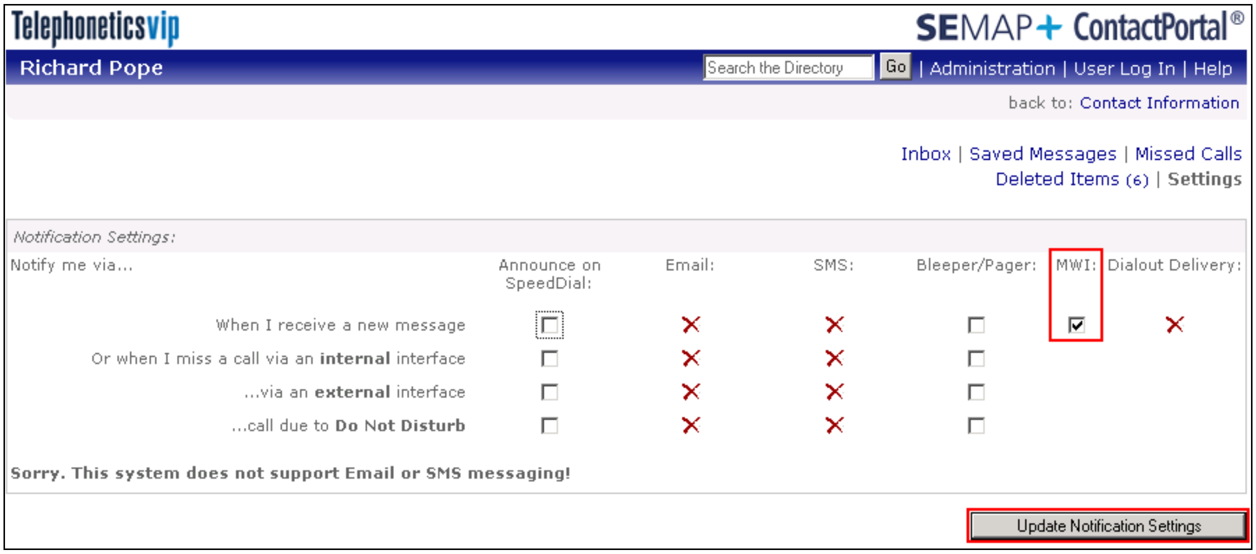


Click **Messaging**.



Click **Settings**.

Ensure a tick is placed next to **MWI** and click **Update Notification Settings**.



8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Avaya and SEMAP+.

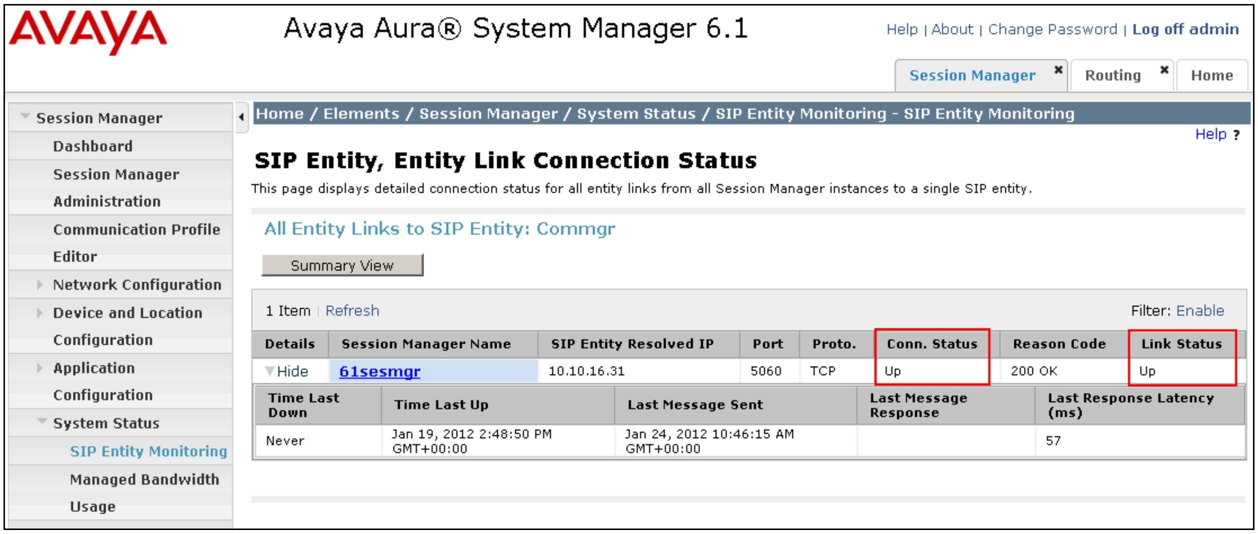
8.1. Verify Avaya Aura® Communication Manager SIP Trunk

Enter the command **status trunk x** where x is the trunk configured in **Section 5.3**. Confirm all channels are **in-service/idle**.

```
status trunk 2                                                       Page   1

                                TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0002/001 T00009   in-service/idle    no
0002/002 T00010   in-service/idle    no
0002/003 T00011   in-service/idle    no
0002/004 T00012   in-service/idle    no
0002/005 T00013   in-service/idle    no
0002/006 T00014   in-service/idle    no
0002/007 T00015   in-service/idle    no
0002/008 T00016   in-service/idle    no
0002/009 T00017   in-service/idle    no
0002/010 T00018   in-service/idle    no
0002/011 T00019   in-service/idle    no
0002/012 T00020   in-service/idle    no
0002/013 T00021   in-service/idle    no
0002/014 T00022   in-service/idle    no
```

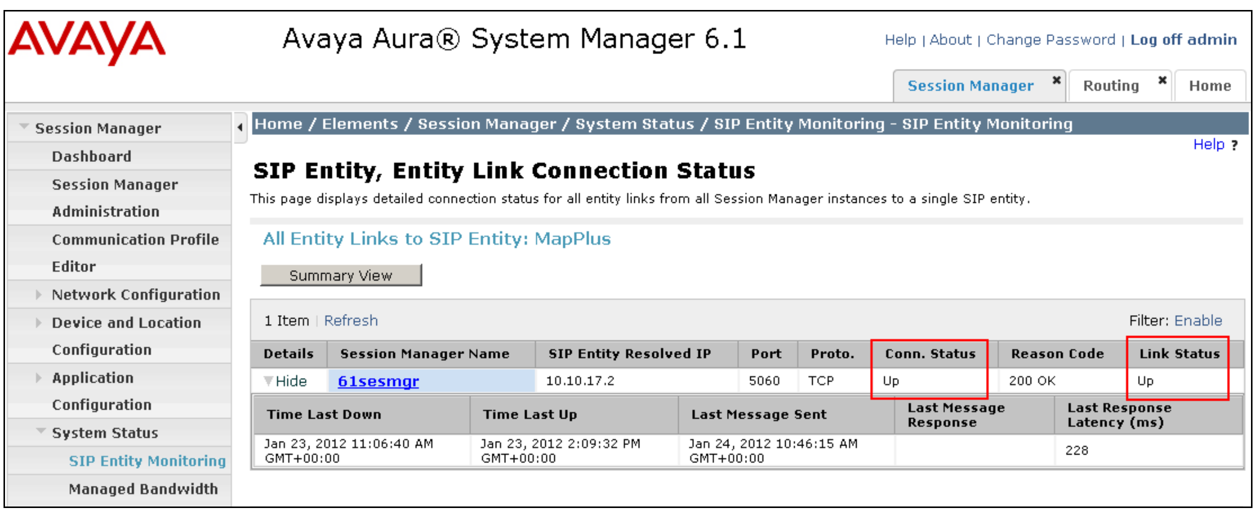
8.2. Verify Avaya Aura® Communication Manager Entity Link Status

From the System Manager web interface click **Home → Elements → Session Manager → System Status → SIP Entity Monitoring →Commgr → Show** verify **Conn. Status** and **Link Status** is **UP**.



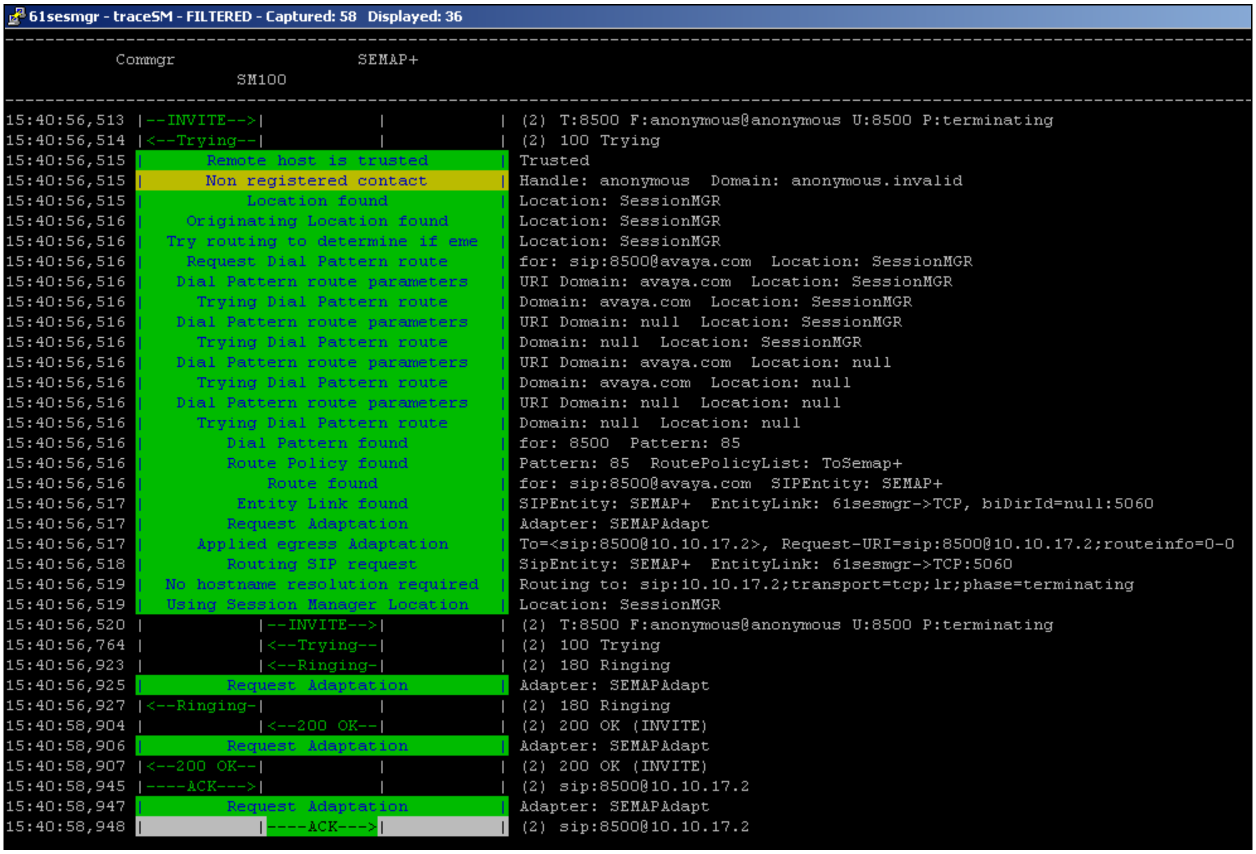
8.3. Verify Netcall SEMAP+ Entity Link Status

From the System Manager web interface click **Home → Elements → Session Manager → System Status → SIP Entity Monitoring →SEMAP+ → Show** verify **Conn. Status** and **Link Status** is **UP**.



8.4. Verify Avaya Aura® Session Manager SIP Call Routing

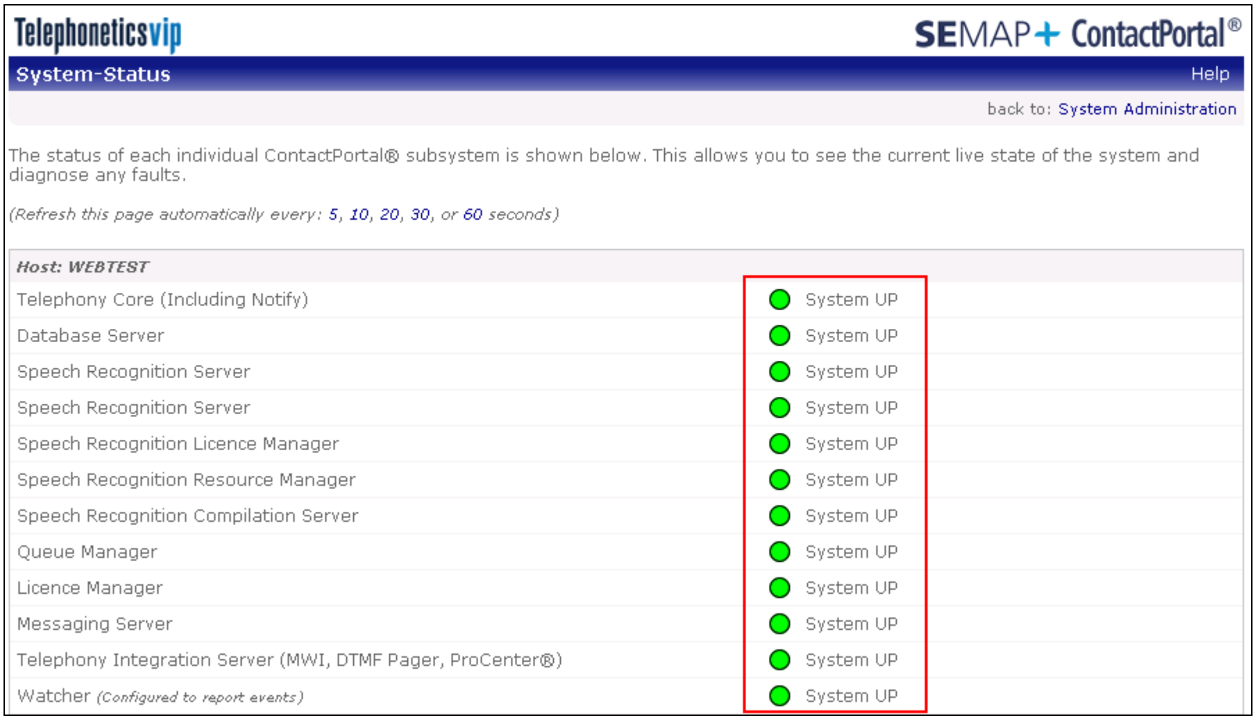
In order to verify the usage of the Session Manager entity link, adaptation and dial pattern configured, SSH into the Session Manager management interface, in this case, 10.10.16.54, and enter the command **traceSM**. Place a call to SEMAP+ and verify the use of the configured parameters as shown below.



```
61sesmgr - traceSM - FILTERED - Captured: 58  Displayed: 36
          Commgr                   SEMAP+
                     SM100
15:40:56,513 |--INVITE-->|           |           | (2) T:8500 F:anonymous@anonymous U:8500 P:terminating
15:40:56,514 |<--Trying--|           |           | (2) 100 Trying
15:40:56,515 |      Remote host is trusted       | Trusted
15:40:56,515 |      Non registered contact       | Handle: anonymous  Domain: anonymous.invalid
15:40:56,515 |          Location found           | Location: SessionMGR
15:40:56,516 |    Originating Location found     | Location: SessionMGR
15:40:56,516 |  Try routing to determine if eme  | Location: SessionMGR
15:40:56,516 |    Request Dial Pattern route     | for: sip:8500@avaya.com  Location: SessionMGR
15:40:56,516 |   Dial Pattern route parameters   | URI Domain: avaya.com  Location: SessionMGR
15:40:56,516 |     Trying Dial Pattern route     | Domain: avaya.com  Location: SessionMGR
15:40:56,516 |   Dial Pattern route parameters   | URI Domain: null  Location: SessionMGR
15:40:56,516 |     Trying Dial Pattern route     | Domain: null  Location: SessionMGR
15:40:56,516 |   Dial Pattern route parameters   | URI Domain: avaya.com  Location: null
15:40:56,516 |     Trying Dial Pattern route     | Domain: avaya.com  Location: null
15:40:56,516 |   Dial Pattern route parameters   | URI Domain: null  Location: null
15:40:56,516 |     Trying Dial Pattern route     | Domain: null  Location: null
15:40:56,516 |        Dial Pattern found         | for: 8500  Pattern: 85
15:40:56,516 |        Route Policy found         | Pattern: 85  RoutePolicyList: ToSemap+
15:40:56,516 |           Route found             | for: sip:8500@avaya.com  SIPEntity: SEMAP+
15:40:56,517 |        Entity Link found          | SIPEntity: SEMAP+  EntityLink: 61sesmgr->TCP, biDirId=null:5060
15:40:56,517 |        Request Adaptation         | Adapter: SEMAPAdapt
15:40:56,517 |     Applied egress Adaptation     | To=<sip:8500@10.10.17.2>, Request-URI=sip:8500@10.10.17.2;routeinfo=0-0
15:40:56,518 |        Routing SIP request        | SipEntity: SEMAP+  EntityLink: 61sesmgr->TCP:5060
15:40:56,519 | No hostname resolution required   | Routing to: sip:10.10.17.2;transport=tcp;lr;phase=terminating
15:40:56,519 |  Using Session Manager Location   | Location: SessionMGR
15:40:56,520 |           |--INVITE-->|           | (2) T:8500 F:anonymous@anonymous U:8500 P:terminating
15:40:56,764 |           |<--Trying--|           | (2) 100 Trying
15:40:56,923 |           |<--Ringing-|           | (2) 180 Ringing
15:40:56,925 |        Request Adaptation         | Adapter: SEMAPAdapt
15:40:56,927 |<--Ringing-|           |           | (2) 180 Ringing
15:40:58,904 |           |<--200 OK--|           | (2) 200 OK (INVITE)
15:40:58,906 |        Request Adaptation         | Adapter: SEMAPAdapt
15:40:58,907 |<--200 OK--|           |           | (2) 200 OK (INVITE)
15:40:58,945 |----ACK--->|           |           | (2) sip:8500@10.10.17.2
15:40:58,947 |        Request Adaptation         | Adapter: SEMAPAdapt
15:40:58,948 |           |----ACK--->|           | (2) sip:8500@10.10.17.2
```

8.5. Verify SEMAP+ Subsystem Status

From the SEMAP+ web interface, click **System Staus**, verify all systems are **UP**.



8.6. Verify SEMAP+ Access

Manually place a call to the SEMAP+ and verify successful interpretation of ASR and appropriate response of the Messaging+ application.

8.7. Verify Netcall SEMAP+ Logging and SEMAP+ Version

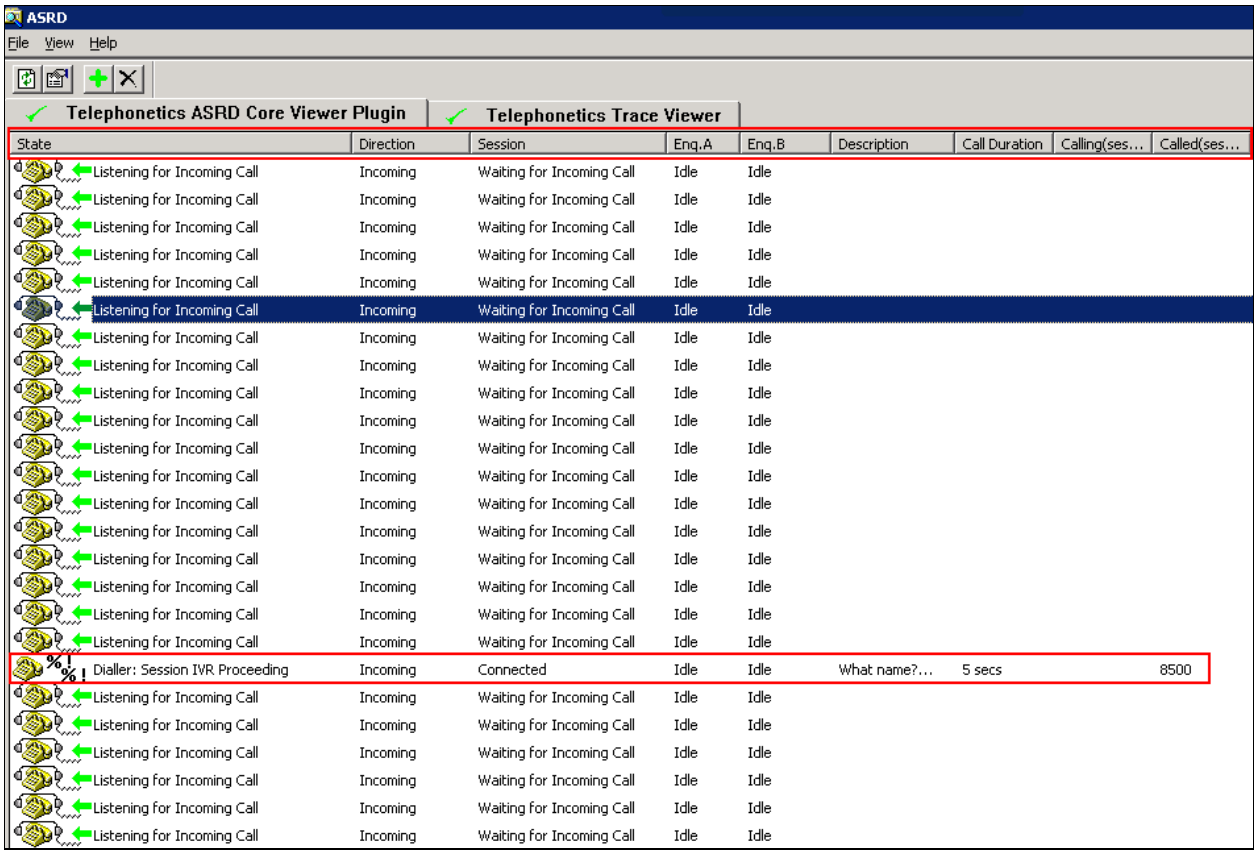
On the SEMAP+ server, browse to **E:\tptrace\<date>.log** and verify the file contains application logging information including SIP messaging. Confirm that the **User-Agent** is shown as **ContactPortal/18.16**.

```
OPTIONS sip:10.10.16.201:5060;transport=tcp SIP/2.0
Via: SIP/2.0/ ;branch=z9hG4bK-d8754z-9e3c2854a804f834-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:contactportal>
To: <sip:10.10.16.201:5060;transport=tcp>
From: <sip:contactportal@10.10.16.201>;tag=415d4964
Call-ID: YTYzOTA3OGM4MDQ2ZTVmZmFjNjQzMWUxMjA1MWUzY2E.
CSeq: 1 OPTIONS
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, INFO, NOTIFY
Supported: timer
Content-Length: 0
```

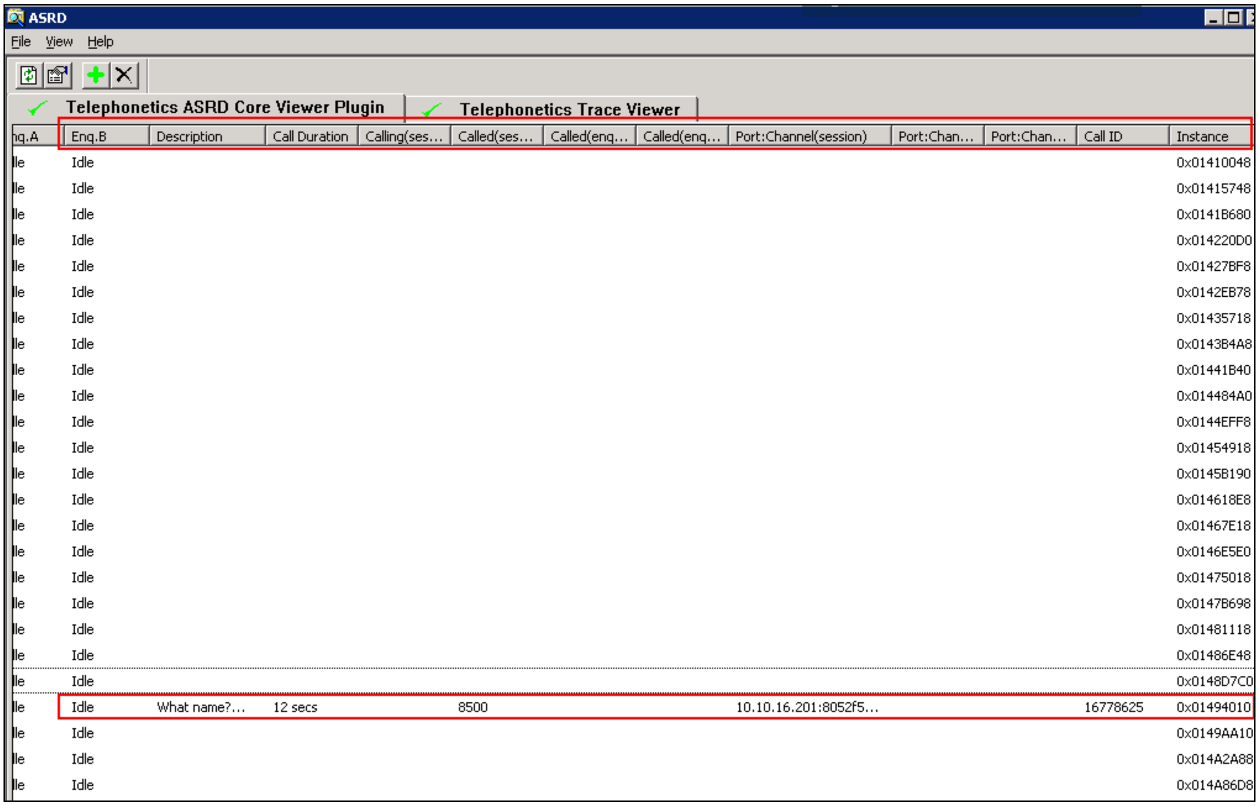
```
Contact: <sip:8500@10.10.17.2>
To: <sip:8500@10.10.17.2>;tag=bc77c625
From: "PSTN,4000"<sip:anonymous@anonymous.invalid>;tag=0d84ae9625de117f4f475d9000
Call-ID: 0d84ae9625de118f4f475d9000
CSeq: 1 INVITE
Session-Expires: 1200;refresher=uac
Min-SE: 1200
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, INFO, NOTIFY
Content-Type: application/sdp
Supported: timer
User-Agent: ContactPortal/18.16
Content-Length: 207
```

8.8. Verify Netcall SEMAP+ Real Time Line Viewer

Click **Start→ ContactPortal (System) → Real Time Line Viewer**, place call to SEMAP+ and verify the **State, Direction, Session, Description, Call Duration** and **Called** are accurately presented.



On the same screen, use the bar at the bottom of the screen to scroll to the right and verify the **Port:Channel(session)** column displays a connection to the IP address of the Session Manager SIP Signaling Interface.



9. Conclusion

These Application Notes describe the configuration steps required for Netcall SEMAP+ to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® System Manager and Avaya Aura® Session Manager. All functionality and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

10. Additional References

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

[1] *Administering Avaya Aura® Communication Manager – Release 6.0, Issue 6.0, June 2010*

[2] *Administering Avaya Aura® Session Manager – Release 6.1, Issue 1, November 2010*

Netcall SEMAP+ Documentation can be found at http://www.netcall.com

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.