Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Aura Alliance Phone with Avaya Aura® Agile Communication Environment VE 6.2.1, Avaya Aura Messaging® 6.1 and Avaya Aura® Communication Manager 6.3 - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the IBM Sametime Aura Alliance Phone plugin to interoperate with Avaya Aura® Agile Communication Environment VE 6.2.1, Avaya Aura® Messaging 6.1 and Avaya Aura® Communication Manager 6.3.

The Aura Alliance Phone is an IBM Sametime plug-in and enables CTI features. It provides control of the existing hard phone such as making & holding call, call transfer & conference and more out of one single user interface. Aura Alliance Phone controls a physical telephone using Third Party Call (v3, v2/v2.4) and Call Notification web service of Avaya ACE 6.2.1 VE.

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.

Table of Contents

1. Introduction

These Application Notes describe the procedure for configuring IBM Sametime plugin Aura Alliance Phone (AAP) with Avaya Aura® Agile Communication Environment (ACE), Avaya Aura® Communication Manager (CM) and Avaya Aura® Messaging (AAM) solutions.

Aura Alliance Phone is an add-on of IBM Lotus Sametime Connect. Aura Alliance Phone plug-in allows a user to operate a physical telephone and view call & telephone display information through a graphical user interface (GUI). Aura Alliance Phone controls a physical telephone using Third Party Call (v3, v2/v2.4) and Call Notification web service of Avaya ACE 6.2.1VE.

2. General Test Approach and Test Result

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 general test approach was to verify the integration of the Aura Alliance Phone plug-in with Avaya SIP phones. Phone operations such as off-hook, on-hook, dialing, answering, conferencing , etc. was performed from the physical phones and from the Aura Alliance Phone application. In addition, phone displays and call states on the physical phones and Aura Alliance Phone was verified for consistency.

2.2. Test Results

The following testing was covered successfully:

- Click and call on Aura Alliance Phone for establishing call and voice path between 2 physical phones.
- Hold and retrieve call.
- Single Step Transfer a call.
- Consult Transfer a call.
- Retrieve voice message from AAM.
- G.711MU and G.711A codec's.
- Create a conference call.
- Add and drop parties for conference.

The following issues were observed during testing:

- An AAP conference host cannot place a conference call on hold using the AAP host's hold button. The host can use the physical phone to put the call on hold. This issue occurs in a configuration with Communication Manager and ACE using ASAI. If Application Enablement Services (AES) is used to interface between ACE and Communication Manger, the issue is not seen. Avaya is investigating this issue.

- An issue was observed with transferring calls. A Communication Manager patch was installed that fixed the issue. This fix will be included in Communication Manager 6.3 SP 1.

- An issue with AAP send incorrect Notification respone to ACE server which causing subscription expire after period of 24 hour.This issue is fixed in AAP version 1.0.9

2.3. Support

Technical support for Aura Alliance Phone can be obtained by contacting Aura Alliance:

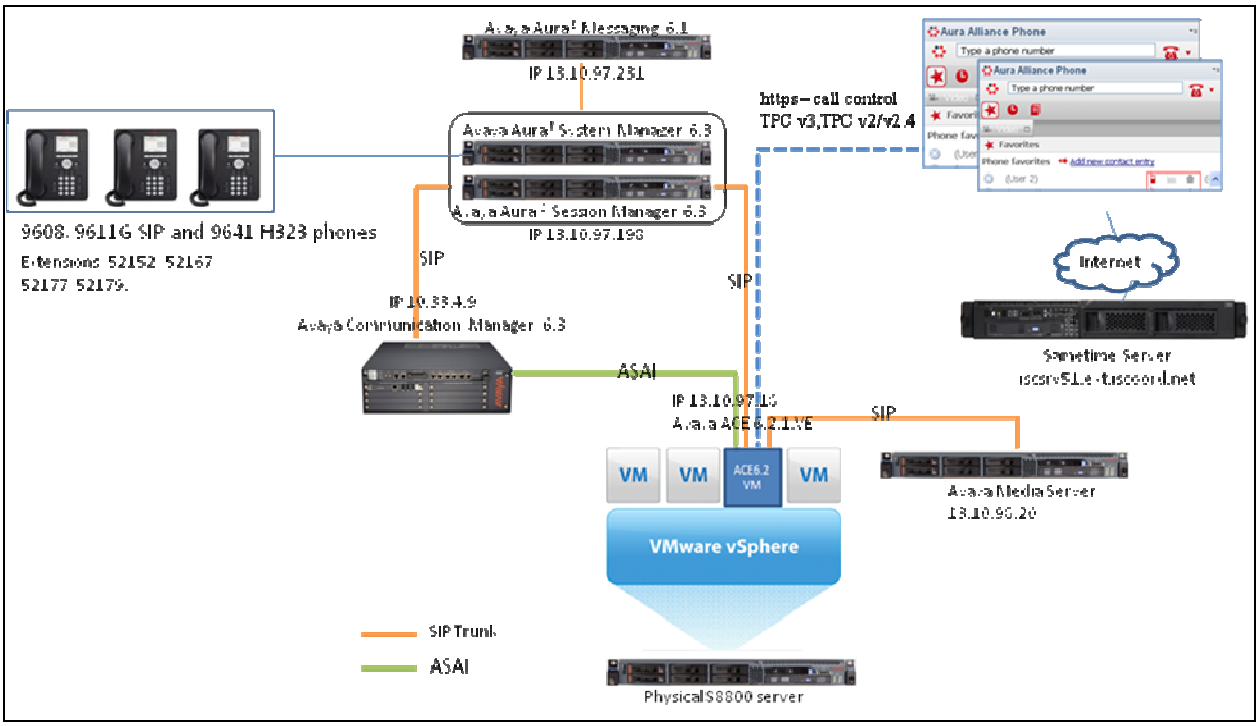
- URL: http://auraalliance.com/support
- Phone: +44 (0) 20 3128 7761.

3. Reference Configuration

The **Figure** below illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with a Session Manager with System Manager, and Communication Manager running on S8300D Server inside an Avaya G450 Media Gateway. Endpoints are Avaya 9600 Series SIP and H.323 phones.

Aura Alliance Phone logins using username and password were created on Avaya ACE.

For Security purposes public IP addresses have been masked or altered in this document.



Test Configuration of Avaya ACE and Avaya Aura Messaging providing services to Aura Alliance Phone

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300D Media Server with Avaya G450 Media Gateway	Avaya Aura® Communication Manager 6.3 SP1*
Avaya Aura® System Manager S8800 Server	Avaya Aura® System Manager 6.3
Avaya Aura® Session Manager S8800 Server	Avaya Aura® Session Manager 6.3
Avaya Aura® Messaging S8800 Server	Avaya Aura® Messaging 6.1
Avaya S8800 Server with VMWare 5.1	Avaya Agile Communication Environment VE 6.2.1
Avaya 9641G H323 Phone	6.2
Avaya 9611G, 9608 SIP Phones	6.2
Aura Alliance Phone	V1.0.7

***A patch was included in the testing, which will be part of SP 1.**

5. Configure Avaya Aura® Communication Manager

5.1. Configure SIP trunk between Communication Server and Session Manager

This section describes the procedure for setting up a SIP trunk between Communication Manager and Session Manager. The steps include setting up an IP codec set, an IP network region, IP node name, a signaling group, a trunk group, and a SIP station. Before a trunk can be configured, it is necessary to verify if there is enough capacity to setup an additional trunk. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Communication Manager System Access Terminal (SAT) interface. All SIP telephones are configured as off-PBX telephones in Communication Manager.

5.1.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient Maximum Off-PBX Telephones – OPS licenses.

If not, contact an authorized Avaya account representative to obtain additional licenses

```
display system-parameters customer-options                    Page   1 of  11
                              OPTIONAL FEATURES

    G3 Version: V16                              Software Package: Standard
      Location: 2                                 System ID (SID): 1
      Platform: 28                                Module ID (MID): 1

                                                          USED
                              Platform Maximum Ports: 6400  185
                                   Maximum Stations: 500   19
                            Maximum XMOBILE Stations: 2400  0
                    Maximum Off-PBX Telephones - EC500: 10    0
                    Maximum Off-PBX Telephones -   OPS: 500   9
                    Maximum Off-PBX Telephones - PBFMC: 10    0
                    Maximum Off-PBX Telephones - PVFMC: 10    0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                         Maximum Survivable Processors: 0     0
```

On **Page 2** of the form, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed.

If not, contact an authorized Avaya account representative to obtain additional licenses.

```
display system-parameters customer-options                    Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  20
          Maximum Concurrently Registered IP Stations: 2400  3
            Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 10    0
                       Maximum Administered SIP Trunks: 4000  110
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 8     0
```

5.1.2. IP Codec Set

This section describes administering a codec set in Communication Manager. This codec set is used in the IP network region for communications between Communication Manager and Session Manager. Enter the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 5.1.3** for configuring IP network region to specify which codec sets may be used within and between network regions.

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

                         IP Codec Set

    Codec Set: 1

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

5.1.3. Configure IP Network Region

This section describes administering an IP network region in Communication Manager. Enter the **change ip-network-region <n>** command, where **n** is a number between **1** and **250** inclusive, and configure the following:

- **Authoritative Domain** – Enter the appropriate name for the Authoritative Domain. During the compliance test, the authoritative domain is set to **bvwdev.com**. This should match the SIP Domain value on Session Manager, in **Section 7.1**.
- **Codec Set** – Set the codec set number as provisioned in **Section 5.1.2**.

```
change ip-network-region 1                                    Page   1 of  20
                            IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: bvwdev.com
    Name:Phuong system SIP
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
```

5.1.4. Configure IP Node Name

This section describes setting IP node name for Session Manager in Communication Manager. Enter the **change node-names ip** command, and add a node name for Session Manager along with its IP address. Perform same step for Avaya ACE.

```
change node-names ip                          Page   1 of   2
                            IP NODE NAMES
    Name                  IP Address
DevASM                  13.10.97.xxx
default                 0.0.0.0
procr                   10.33.4.9
procr6                  ::
DevACE                  13.10.98.19
```

5.1.5. Configure SIP Signaling

Enter the **add signaling-group <s>** command, where **s** is an available signaling group and configure the following:

- **Group Type** – Set to **sip**.
- **IMS Enabled** – Verify that the field is set to **n**. Setting this filed to **y** will cause Communication Manager to behave as a Feature Server.
- **Transport Method** – Set to **tls**
- **Near-end Node Name** – Set to **procr** as displayed in **Section 5.1.4**.
- **Far-end Node Name** – Set to the Session Manager name configured in **Section 5.1.4**.
- **Far-end Network Region** – Set to the region configured in **Section 5.1.3**.
- **Far-end Domain** – Set to **bvwdev.com**. This should match the Authoritative Domain value in **Section 5.1.3**.
- **Direct IP-IP Audio Connections** – Set to **y**, since media shuffling is enabled during the compliance test
- **Initial IP-IP Direct Media** – Set to **y.**

```
add signaling-group 5
                                SIGNALING GROUP

 Group Number: 5                Group Type: sip
   IMS Enabled? n          Transport Method: tls          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: procr                  Far-end Node Name: DevASM
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                          Far-end Network Region: 1
                                  Far-end Secondary Node Name:

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

5.1.6. Configure Trunk Group

To configure the associated trunk group, enter the **add trunk-group <t>** command, where **t** is an available trunk group and configure the following:

- **Group Type** – Set the Group Type field to **sip**.
- **Group Name** – Enter a descriptive name.
- **TAC** (Trunk Access Code) – Set to any available trunk access code.
- **Service Type** – Set the Service Type field to **tie**.
- **Signaling Group** – Set to the Group Number field value for the signalling group configured in **Section 5.1.5**
- **Number of Members –** Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

```
add trunk-group 5                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 92                    Group Type: sip           CDR Reports: y
        Group Name: NO IMS SIP trk  COR: 1        TN: 1        TAC: 115
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                                Member Assignment Method: auto
                                                          Signaling Group: 5
                                                        Number of Members: 20
```

On **Page 3**, set the Numbering Format field to **private.**

```
add trunk-group 5                                          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
```

5.1.7. Configure Route Pattern

For the trunk group, define the route pattern by entering the **change route-pattern <r>** command, where **r** is an unused route pattern number. The route pattern consists of a list of trunk groups that can be used to route a call. The following screen shows route-pattern 5 will utilize the trunk group 5 to route calls. The default values for the other fields may be used.

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

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                           Subaddress
1: y y y y y n  n            rest                               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
```

5.1.8. Administer Dialplan

Configure dialplan analysis, Uniform Dialing and AAR to route calls over a SIP trunk to Session Manager and ultimately to Avaya Aura® Messaging without the need to dial a Feature Access Code (FAC).

Use the command **change dialplan analysis 1** to create an entry in the Dial Plan Analysis Table

- 399 – Starting digits for Avaya Aura Messaging Pilot extension
- 521 – Starting ditits for endpoint extensions in Communication Manager 6.3

```
display 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           3   dac      8          1   fac
  782         5   ext      9          1   fac
  399         5   ext      *          4   dac
  521         5   ext
```

Use the command **change uniform dial-plan 1** to create an entry in the UDP table which covers dial patterns the pilot number of Avaya Aura® Messaging and for endpoint extensions.

As shown below, any number dialed to 399xx or 521xx totaling 5-digits will be routed to AAR.

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

  Matching                    Insert              Node
  Pattern        Len Del      Digits     Net Conv Num
 399              5   0                  aar  n
 521              5   0                  aar  n
```

For the AAR Analysis Table, create the dial strings that will route calls to Avaya Aura® Messaging and endpoint extensions via the route pattern created in above section. Enter the **change aar analysis <x>** command, where **x** is a starting partial digit (or full digit) string. The dialed string created in the AAR Digit Analysis Table contains a dialed digit map to the Messaging pilot number or endpoint extensions. During the configuration of the AAR table, the Call Type field was set to **unku** for **399xx** and **aar** for **521xx**.

```
display aar analysis 0                                      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
 399                    5    5     5         unku          n
 52                     5    5     5         aar           n
```

5.1.9. Configure Hunt Group for Avaya Aura® Messaging

This section describes administering a hunt group in Communication Manager. Enter the **add hunt-group <h>** command, where **h** is an available hunt group number. The following fields were configured for the compliance test.

- **Group Name** – Enter a descriptive name
- **Group Extension** – Enter an extension valid in the provisioned dial plan.

```
Add hunt-group 2                                            Page   1 of  60
                                  HUNT GROUP

            Group Number: 1                               ACD? n
              Group Name: Messaging                      Queue? n
       Group Extension: 39991                            Vector? n
              Group Type: ucd-mia                Coverage Path:
                      TN: 1           Night Service Destination:
                     COR: 1                    MM Early Answer? n
           Security Code:                 Local Agent Preference? n
 ISDN/SIP Caller Display:
```

On **Page 2**, provide the following information:

- **Message Center** – Enter **sip-adjunct**, indicating the type of messaging adjunct used for this hunt group. This value will also be used in the Station form.
- **Voice Mail Number** – Enter the Voice Mail Number, which is the extension of AAM.
- **Voice Mail Handle –**Enter the Voice Mail Handle which is the extension of AAM.
- **Routing Digit (e.g. AAR/ARS Access Code)** – Enter the AAR Access Code as defined in the Feature Access Code form.

```
add hunt-group 2                                              Page   2 of  60
                                HUNT GROUP
                        Message Center: sip-adjunct

     Voice Mail Number         Voice Mail Handle          Routing Digits
                                                      (e.g., AAR/ARS Access Code)
     39990                     39990                      9
```

5.1.10. Configure Coverage Path to Avaya Aura® Messaging

This section describes administering coverage path in Communication Manager. Enter the **add coverage path <s>** command, where **s** is a valid coverage path number. The Point1 value of **h2** is used to represent the hunt group number 2. The default values for the other fields may be used.

```
add coverage path 2                                           Page   1 of   1
                                COVERAGE PATH

                  Coverage Path Number: 2
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside     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: h2            Rng:2    Point2:
   Point3:                        Point4:
```

5.1.11. Administer a Station for Coverage to Avaya Aura® Messaging

Configure any and all phones that have a mailbox on the messaging server for call coverage. Use the command **change station <xyz>** to open the Station form for extension **xyz**. On **Page1**, for **Coverage Path 1** enter the coverage path defined in **Section 5.1.10.** **I**n the example below station 52155 was configured to cover to messaging using cover path 2.

```
change station 52155                                          Page   1 of   5
                                    STATION

Extension: 52155                        Lock Messages? n              BCC: 0
     Type: 96                         Security Code: *              TN: 1
     Port: S00024                     Coverage Path 1: 2            COR: 1
     Name: Nam Nam                    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: 52151
           Speakerphone: 2-way                Mute Button Enabled? y
         Display Language: english                 Button Modules: 0
 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
```

Navigate to page 2 and set the **MWI Served User Type** to **sip-adjunct**.

```
change station 52151                                          Page   2 of   5
                                    STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                          Coverage Msg Retrieval? y
  LWC Log External Calls? n                                Auto Answer: none
            CDR Privacy? n                           Data Restriction? n
   Redirect Notification? y                   Idle Appearance Preference? n
 Per Button Ring Control? n                  Bridged Idle Line Preference? n
   Bridged Call Alerting? n                      Restrict Last Appearance? y
  Active Station Ringing: single
                                                      EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
      Service Link Mode: as-needed                    EC500 State: enabled
       Multimedia Mode: enhanced                Audible Message Waiting? n
   MWI Served User Type: sip-adjunct          Display Client Redirection? n
                                             Select Last Used Appearance? n
                                               Coverage After Forwarding? s
                                                 Multimedia Early Answer? n
 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 52151         Always Use? n IP Audio Hairpinning? n
```

5.1.12.Configure SIP Endpoint

SIP endpoints and off-pbx-telephone stations will be automatically created in Communication manager when users (SIP endpoints) were created in Session Manager. Go to section Section 7.8 for steps to create SIP user on Session Manager. On the Station form in CM, on the last page is a Third Party Call Control setting. Enter **Avaya** for **Type of 3PCC Enabled.** This setup ensures that ACE Notification service can send out notifications for SIP Phones.

```
change  station 52152                                          Page   6 of   6
                                    STATION

SIP FEATURE OPTIONS
       Type of 3PCC Enabled: Avaya
                     SIP Trunk: aar
```

5.1.13.Configure Location

This section configures outbound Proxy Route in the Locations form. Use the command **change locations** to set the value for **Proxy Rte** to the route pattern for routing calls to Session Manager. During compliance testing, route pattern 5 is used.

```
change locations                                               Page   1 of  16
                                  LOCATIONS
                ARS Prefix 1 Required For 10-Digit NANP Calls? y
Loc Name           Timezone DST     City/ ARS Atd Loc  Disp   Prefix   Proxy Sel
No                 Offset           Area  FAC FAC Parm Parm             Rte Pat
1: Main            + 00:00  0                      1    1                5
```

5.2. Configure ASAI link between Communication Manager and Avaya ACE

This section provides the procedures for configuring ASAI link on Communication Manager. The procedures include the following areas:

- Verify license permission.
- Configuring AE Services and Avaya ACE as an AE Services server
- Configuring a CTI link

5.2.1. Verify license permission

Log in to the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that the **ASAI Link Core Capabilities, ASAI Link Plus Capabilities** and **Computer Telephony Adjunct Links** customer options are set to "y" on **Page 3**. If any of these options is not set to "y", contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                    Page   3 of  11
                              OPTIONAL FEATURES
    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                      CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                        CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                ARS? y  Computer Telephony Adjunct Links? y
                ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
         ARS/AAR Dialing without FAC? n                       DCS (Basic)? y
         ASAI Link Core Capabilities? y                DCS Call Coverage? y
         ASAI Link Plus Capabilities? y               DCS with Rerouting? y
      Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
             ATM WAN Spare Processor? n                            DS1 MSP? y
                               ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2.2. Configuring AE Services and Avaya ACE as an AE Service server

Enabling AE Services refers to administering the transport link between Communication Manager and AE Services. In this procedure, a Local Port number is entered that must match the Port value entered when performing the procedure in **Section 8.2**.

Enter the **change ip-services** command. Complete Page 1 of the IP SERVICES form as follows:

- In the **Service Type** field, type **AESVCS**.
- In the **Enabled**, enter **y**.
- In the **Local Node** field, type **procr**.
- In the **Local Port** field, accept the default (**8765**).

```
change ip-services                                            Page   1 of   3
                                  IP SERVICES
 Service      Enabled      Local        Local       Remote       Remote
  Type                     Node         Port        Node         Port
AESVCS          y       procr           8765
```

Complete Page 3 of the IP Services form as follows:

- In the **AE Services Server** field, type the name of the ACE Server, for example: **DevACE**.
- Enter **Password**, see note below.
- Set the **Enabled** field to **y**.

```
change ip-services                                          Page   3 of   3
                          AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
        1:      DevACE            DevConnect123       y        in use
```

Note:
In this procedure, the Avaya ACE server name and password must be entered. These values must match the ACE Server Name and Password values entered when performing the procedure in **Section 8.2**.

5.2.3. Add a CTI link

In this procedure, you must enter a CTI Link number. This value must match the CTI Link No value entered when performing the procedure in **Section 8.2**.

Add a CTI link using the **add cti-link <n>** command; where **n** is an available CTI link number. Complete the **CTI LINK** form as follows:

- Enter an available extension number in the **Extension** field.
- Enter **ADJ-IP** in the **Type** field
- Enter description for this link, example: DevACE in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 5                                  Page   1 of   3
                                CTI LINK
 CTI Link: 5
Extension: 52100
     Type: ADJ-IP

                                                        COR: 1
     Name: DevACE
```

6. Configure Avaya Aura® Messaging

Messaging was configured for SIP communication with Session Manager. The procedures include the following areas:

- Administer Sites
- Administer Telephony Integration
- Administer Dial Rules
- Administer Class of Service to enable Message Waiting
- Administer Subscribers
- Administer Topology

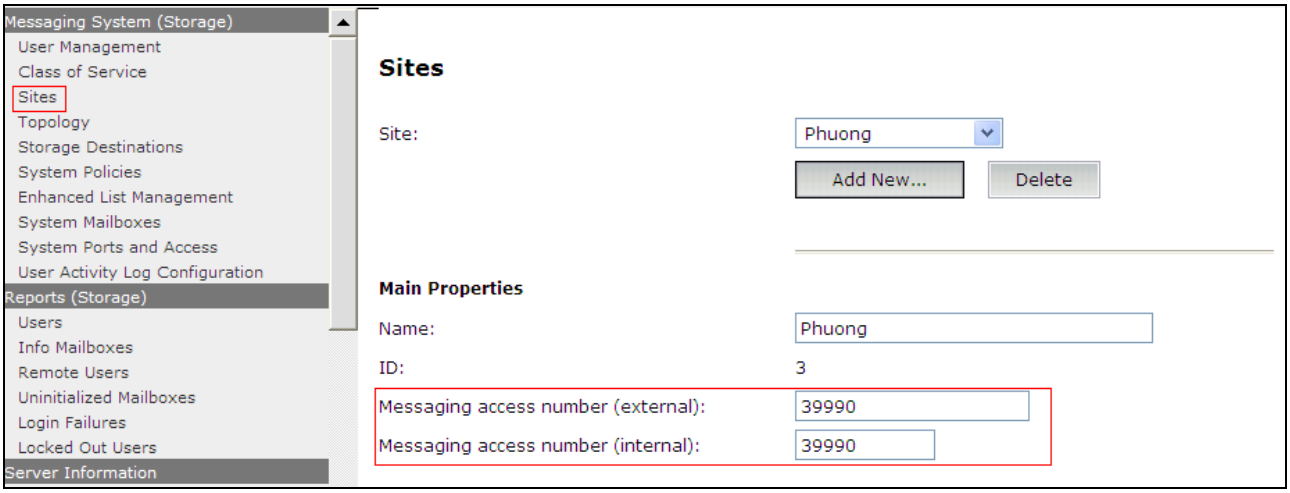
See references **Section 13** for standard installation and configuration information. General knowledge of the configuration tools and interfaces is assumed.

6.1. Administer Sites

A Messaging access number and a Messaging Auto Attendant number needs to be defined. Log into the Messaging System Management Interface (SMI) and go to **Administration → Messaging**. In the left panel, under **Messaging System (Storage)** select **Sites,** click Add New. In the right panel fill in the following:

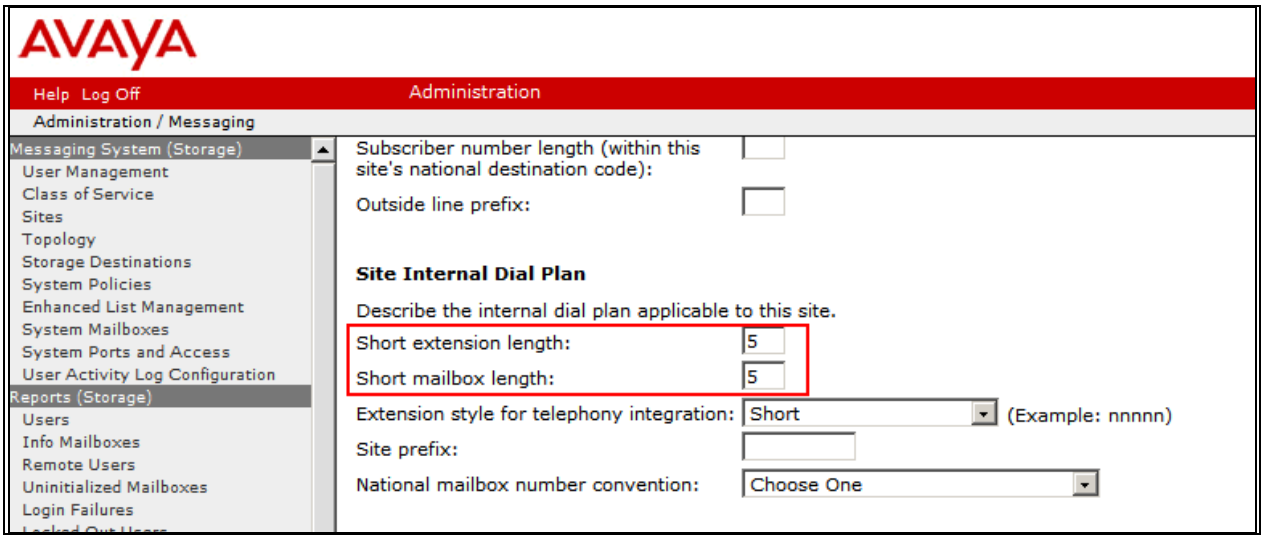
Under **Main Properties:**

- **Name**: Enter site name
- **Messaging access number (internal)** Enter a Messaging Pilot number



Scroll down to the **Site Internal Dial Plan** section.
Under **Site Internal Dial Plan:**

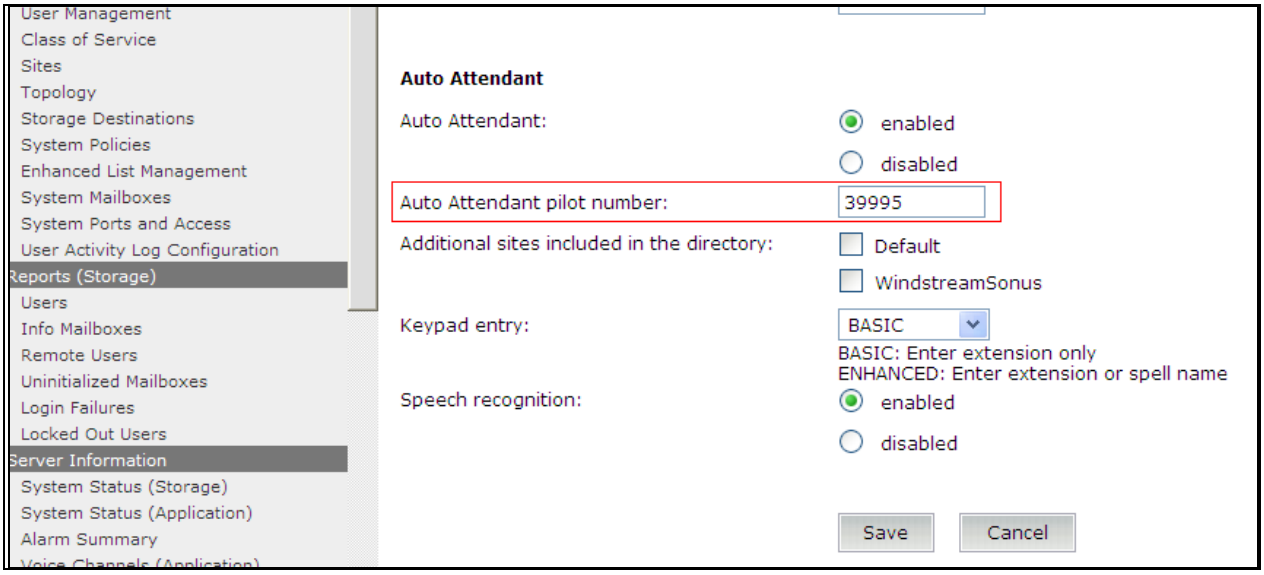
- **Short Extension Length** Enter the number of digits in extensions
- **Short Mailbox Length** Enter the number of digits in mailbox numbers



Scroll down to the **Auto Attendant** section.
Under **Auto Attendant:**

- **Auto Attendant** Select **Enabled**
- **Auto Attendant pilot number** Enter an Auto Attendant number
- **Keypad entry** Select **BASIC**
- **Speech recognition** Select **Enabled**

Click **Save** to save changes.



6.2. Administer Telephony Integration

A SIP trunk needs to be configured from AAM to Session Manager. Log into the Messaging System Management Interface (SMI) and go to **Administration → Messaging**. In the left panel, under **Telephony Settings (Application)** select **Telephony Integration**. In the right panel fill in the following:

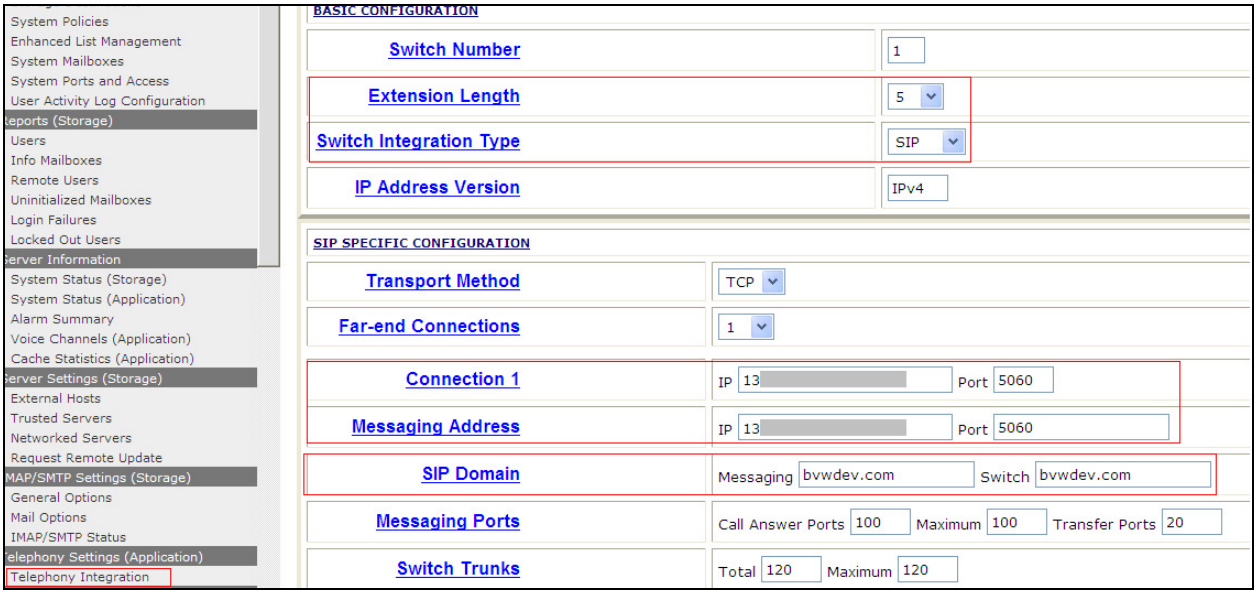
Under **Basic Configuration:**

- **Extension Length:** Enter the length of extensions
- **Switch Integration Type:** **SIP**

Under **SIP Specific Configuration:**

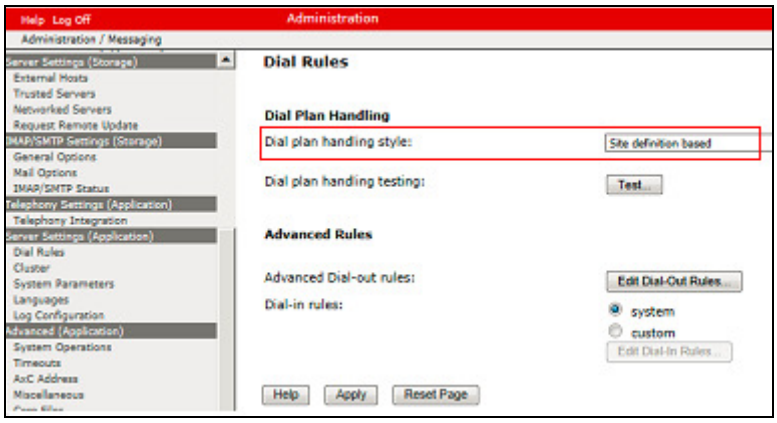
- **Transport Method:** **TCP**
- **Connection 1** Enter the Session Manager signaling IP address and TCP port number
- **Messaging Address** Enter the AAM IP address and TCP port number
- **SIP Domain** Enter the Messaging and Session Manager domain names

Click **Save** (not shown) to save changes.

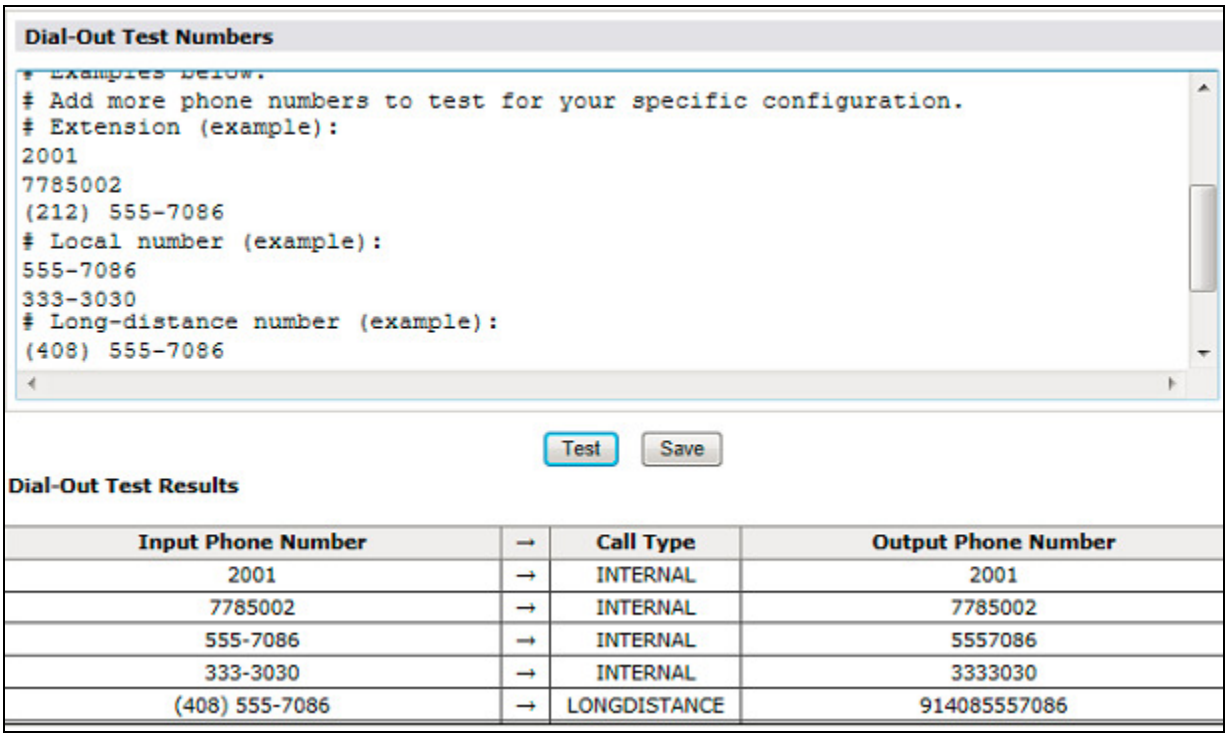


6.3. Configure Dial Rules

Navigate to **Administration→Messaging→Server Settings (Application) → Dial Rules** to configure the dial rules. Set the **Dial plan handling style** field to **Site definition based** as shown below.



Next select the **Edit Dial-Out Rules** button to verify the appropriate rules specification for outbound dialing from Avaya Aura® Messaging. These dial rules help Avaya Aura® Messaging send the correct number and combination of digits when originating a call to Communication Manager, whether the call is destined for another extension or ultimately expected to be routed to the PSTN.



Input Phone Number	→	Call Type	Output Phone Number
2001	→	INTERNAL	2001
7785002	→	INTERNAL	7785002
555-7086	→	INTERNAL	5557086
333-3030	→	INTERNAL	3333030
(408) 555-7086	→	LONGDISTANCE	914085557086

6.4. Configure Class of Service

Use **Administration→Messaging** menu, and in the left navigation panel select **Class of Service** under **Messaging System (Storage).**

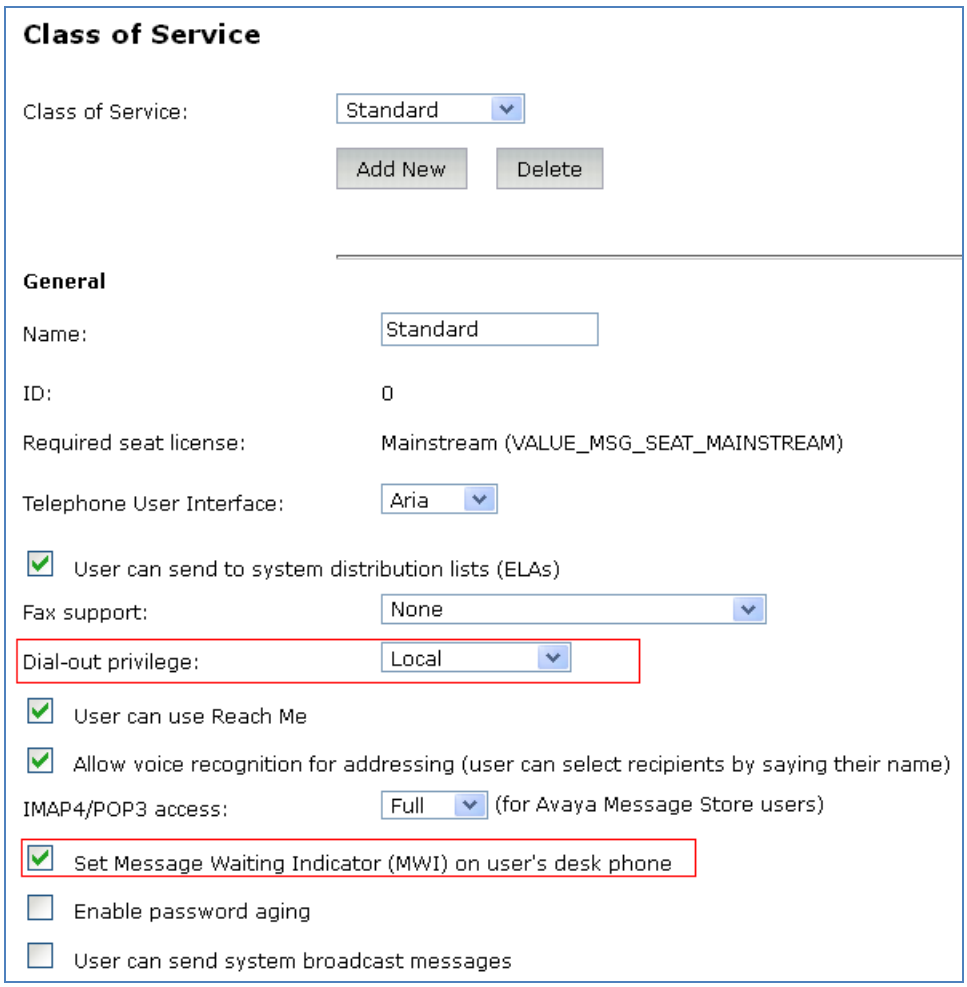
Select **"Standard"** from the **Class of Service** drop-down menu.

Under **General**, enter values, or make selections as shown below and use default values for remaining fields.

Under **Greetings**, select **Two Greetings (different greetings for busy and no answer)** to allow subscribers to record different personal greetings for busy and no-answer scenarios (not shown).

Click **Save** (not shown) to save changes.

The following screen shows the settings defined for the "**Standard**" Class of Service in the sample configuration.

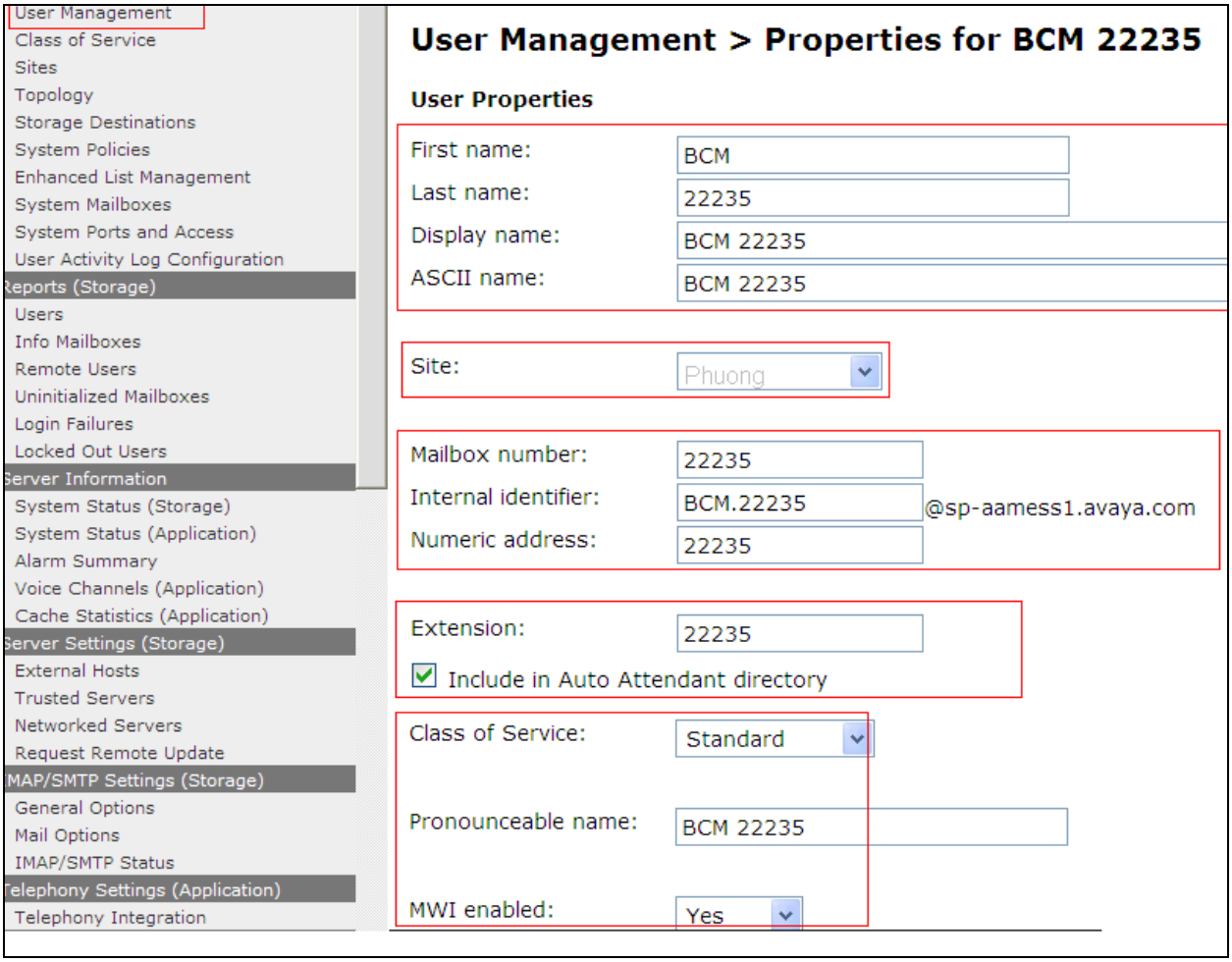


6.5. Administer Subscribers

Log into the Messaging System Management Interface (SMI) and go to **Administration → Messaging**. In the left panel, under **Messaging System (Storage)** select **User Management**. In the right panel fill in the following:

Under **User Properties:**

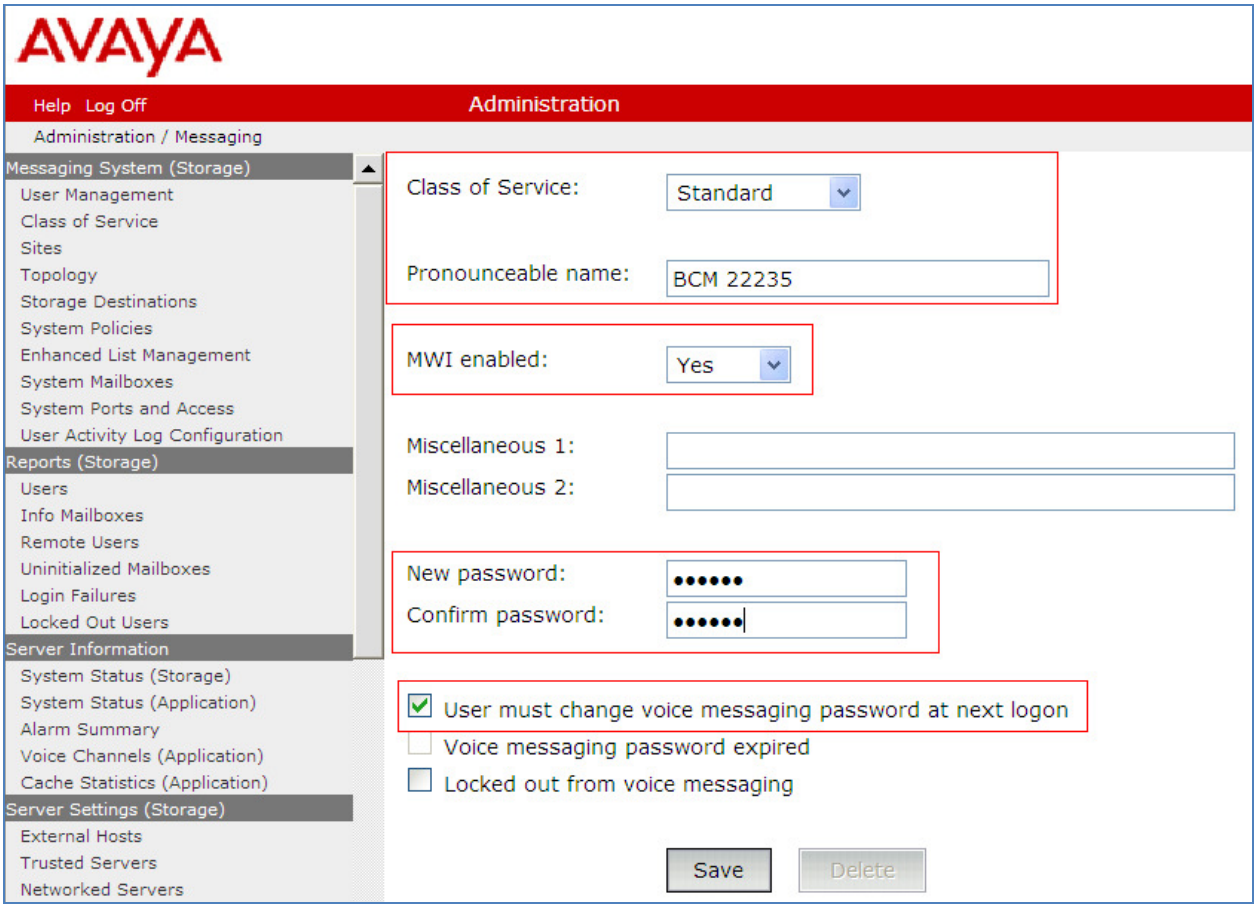
- **First Name** Enter first name
- **Last Name** Enter last name
- **Display Name** Enter display name
- **ASCII name** Enter the ASCII name
- **Site** Enter site defined in **Section 6.1**
- **Mailbox Number** Enter desired mailbox number, e.g., **22235**
- **Internal identifier** Enter the name for internal use
- **Numeric address** Enter the mailbox number
- **Extension** Enter desired extension number, e.g., **22235**



Scroll down on the page to Class of Service.

- **Class of Service** Select a Class of Service
- **Pronounceable name** Enter a pronounceable name to be used when dialing the extension using voice commands
- **MWI Enabled** Select **Yes** to enable the MWI light on the phone
- **New Password/Confirm Password** Enter desired extension password
- **Next logon password change** Select the checkbox

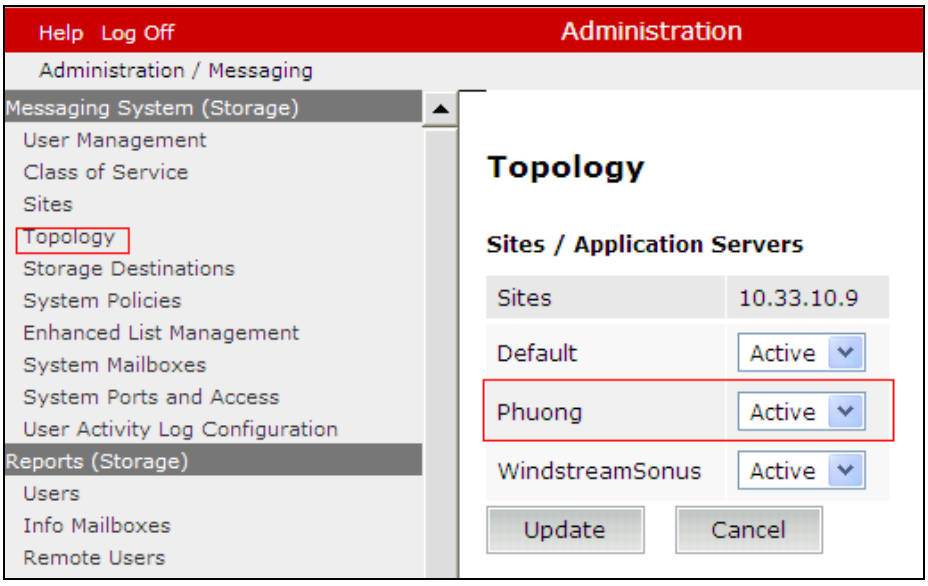
Click **Save** to save changes.



6.6. Administer Topology

Select **Topology** under **Messaging System (Storage)**.

Verify the site defined in **Section6.1** is **Active**



7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager Web interface and is then downloaded into Session Manager.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

In this section, the following topics are discussed:

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- Manage Element
- Applications
- Application Sequence
- User Management
- Synchronization

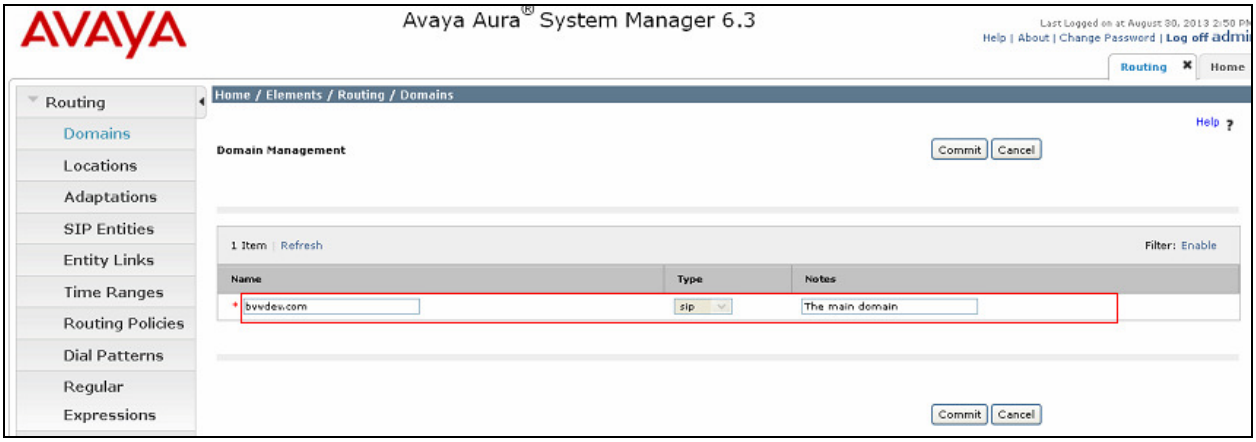
7.1. Configure SIP Domain

Launch a web browser, enter **http://<IP address of System Manager>/SMGR** in the URL, and log in with the appropriate credentials.

Navigate to **Routing → Domains**, and click on the **New** button (not shown) to create a new SIP Domain. Enter the following values and use default values for remaining fields:

- **Name –** Enter the Authoritative Domain Name specified in **Section 4.3**, which is **bvwdev.com**.
- **Type** – Select **sip**

Click **Commit** to save. The following screen shows the Domains page used during the compliance test.



7.2. Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.

Navigate to **Routing → Locations**, and click on the **New** button (not shown) to create a new SIP endpoint location.

General section

Enter the following values and use default values for remaining fields.

- Enter a descriptive Location name in the Name field.
- Enter a description in the **Notes** field if desired.

Location Pattern section

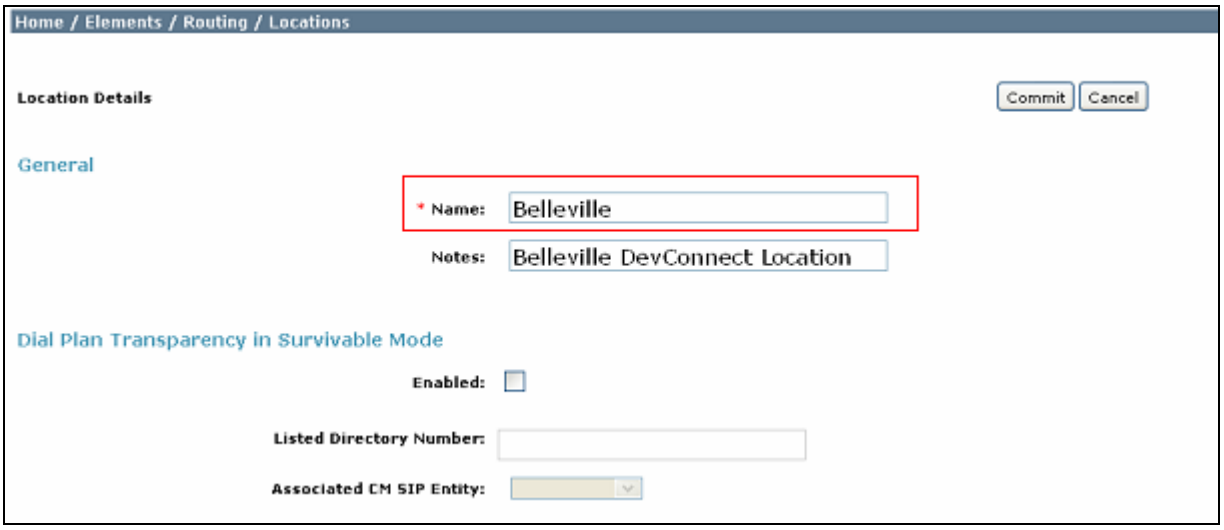
Click **Add** and enter the following values:

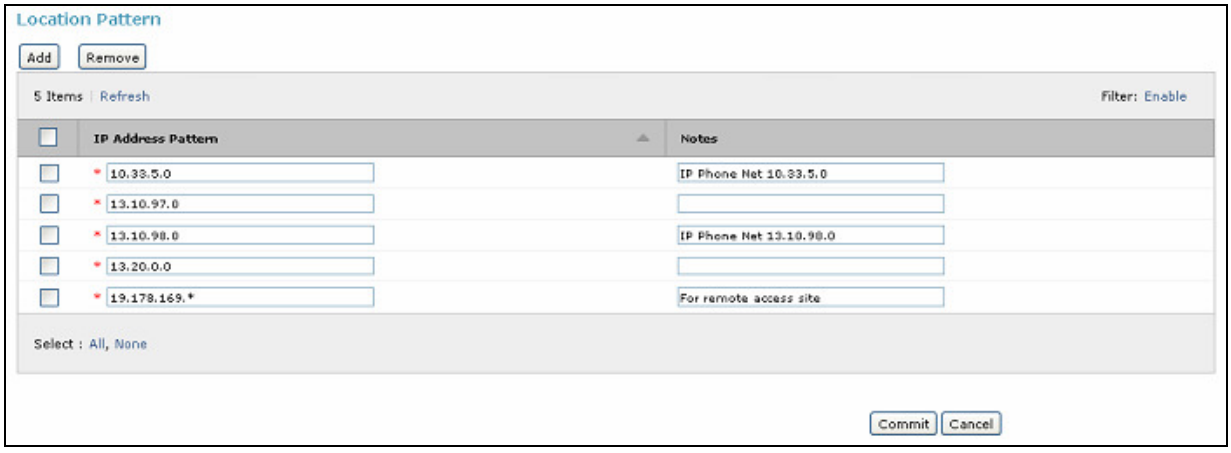
- Enter the IP address information for the IP address Pattern (e.g. **13.10.97.***)
- Enter a description in the **Notes** field if desired.

Repeat steps in the Location Pattern section if the Location has multiple IP segments.

Modify the remaining values on the form, if necessary; otherwise, retain the default values. Click on the **Commit** button.

Repeat all the steps for each new Location. The following screen shows the Locations page used during the compliance test.





7.3. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk provisioned to Session Manager. During the compliance test, the following SIP Entities were configured: Session Manager itself, Communication Manager, Avaya Aura® Messaging, and Avaya ACE

Navigate to **Routing → SIP Entities**, and click on the **New** button (not shown) to create a new SIP Entity. Provide the following information:

General section

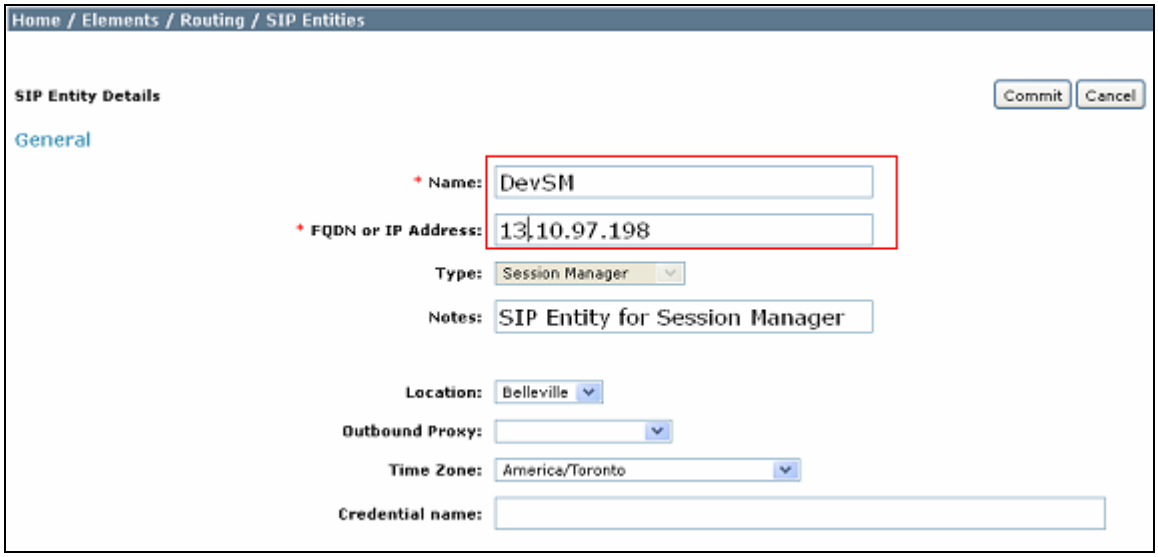
Enter the following values and use default values for remaining fields.

- Enter a descriptive name in the **Name** field.
- Enter IP address for signaling interface on Communication Manager, Session Manager, Avaya Aura® Messaging and Avaya ACE.
- From the **Type** drop down menu select a type that best matches the SIP Entity. For Communication Manager, select CM. For Session Manager, select Session Manager. For Messaging, select Modular Messaging. For Avaya ACE, select Others.
- Enter a description in the **Notes** field if desired.
- Select the appropriate time zone.
- Accept the other default values.

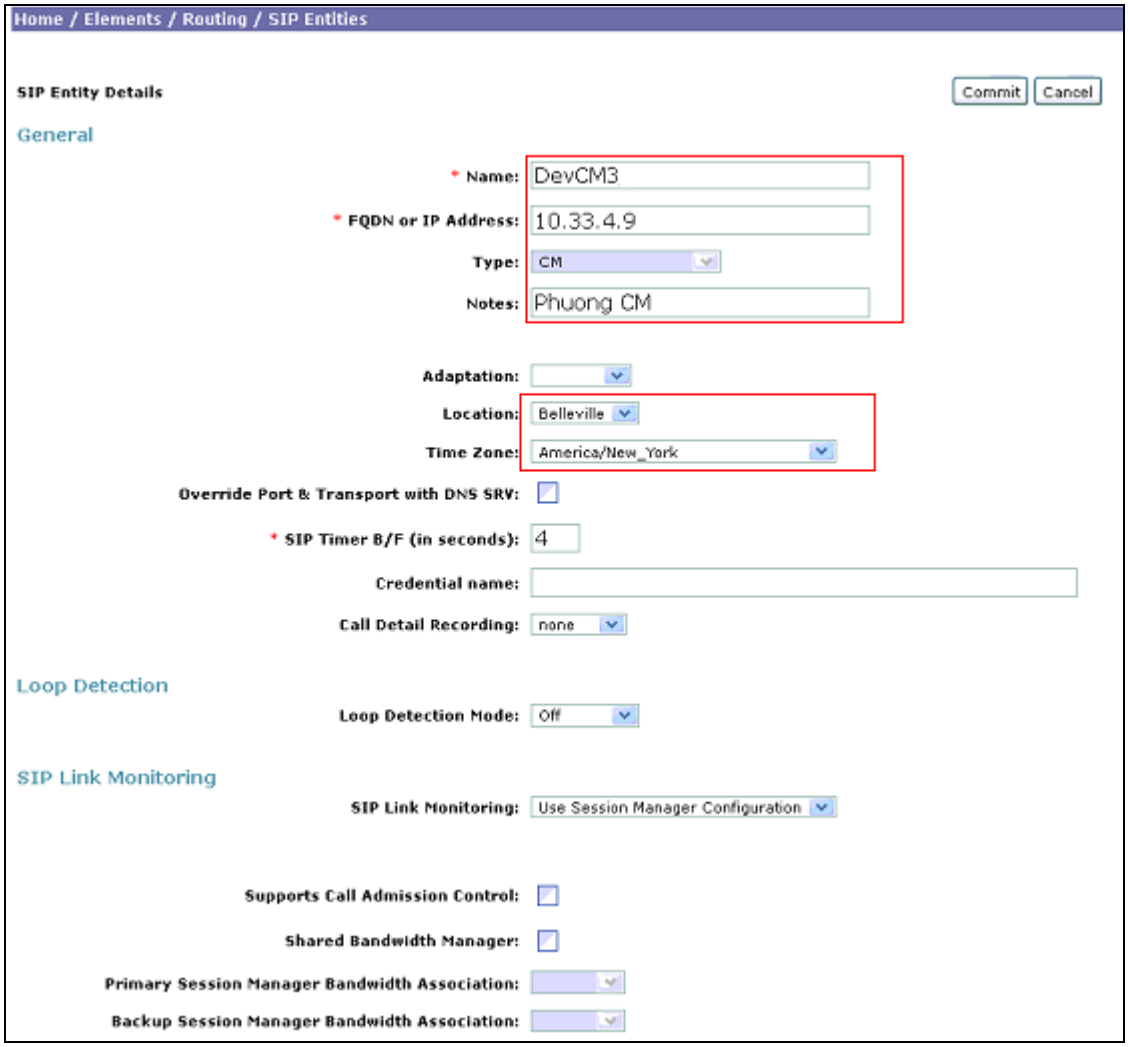
Click on the **Commit** button to save configuration for each SIP Entity.

The following screens show the SIP Entities page used during the compliance test.

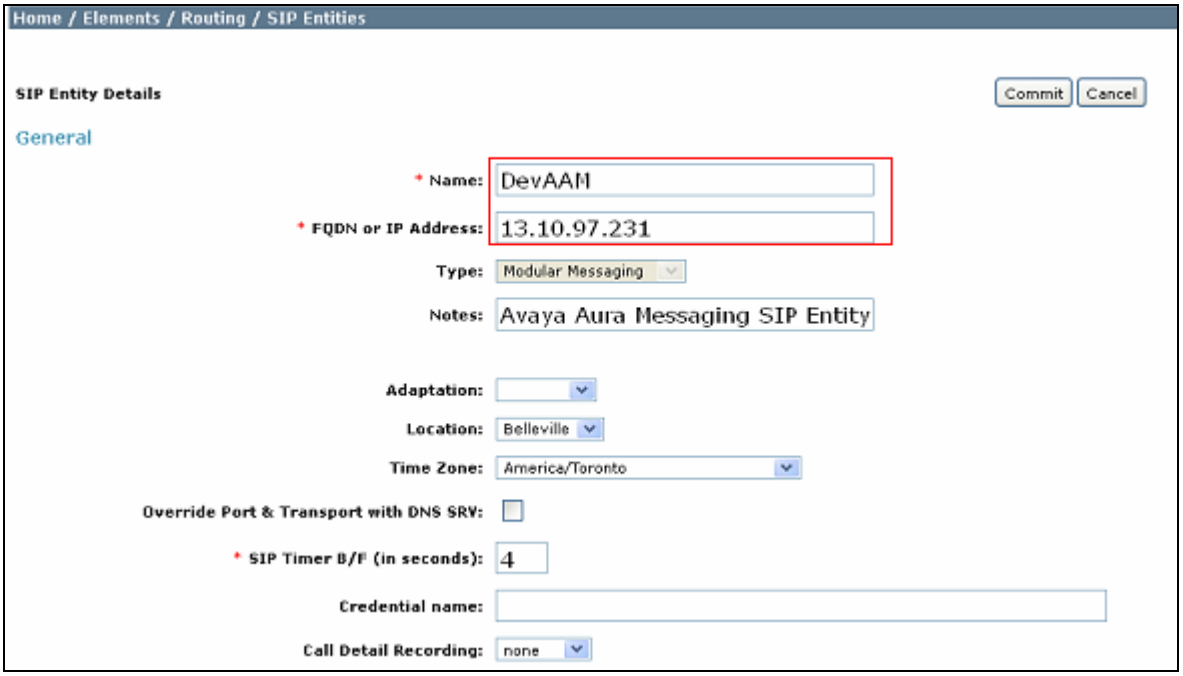
Session Manager SIP Entity:



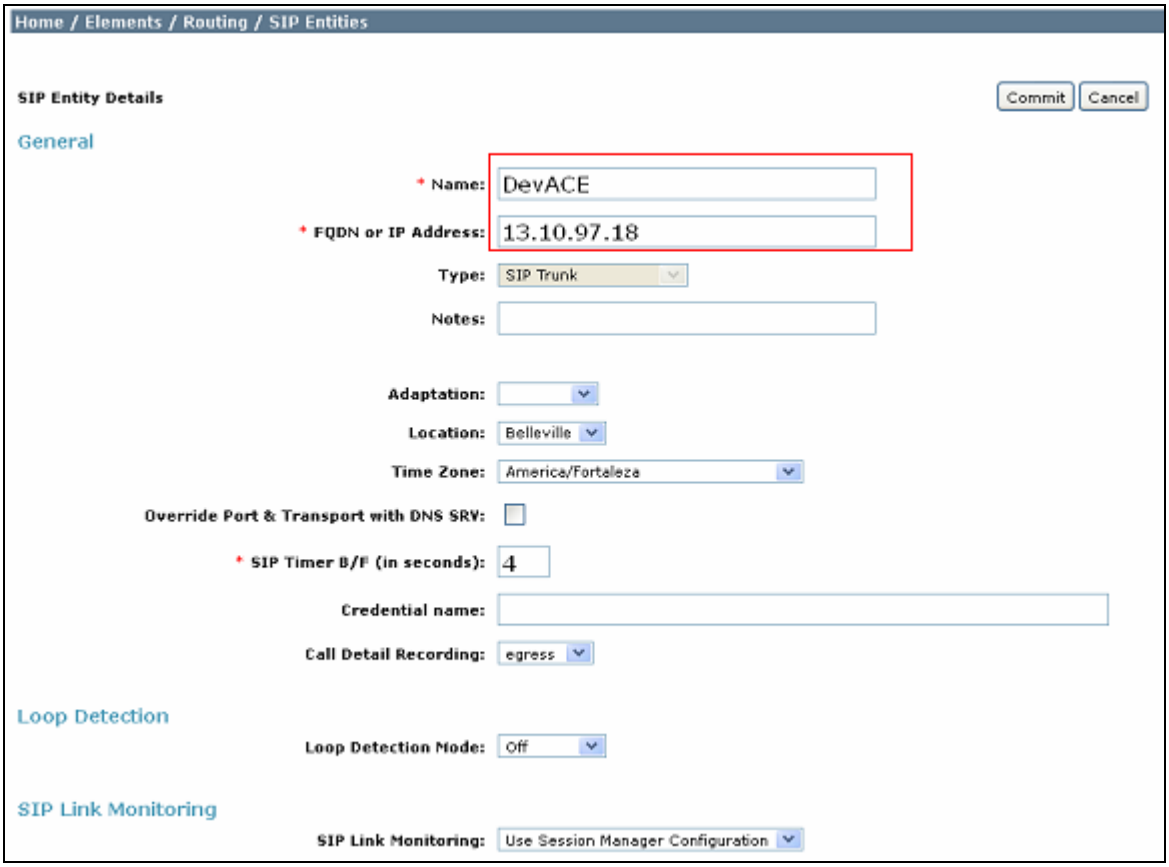
Communication Manager SIP Entity:



AAM SIP Entity:



Avaya ACE SIP Entity:



7.4. Configure Entity Links

Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following Entity Links are defined.

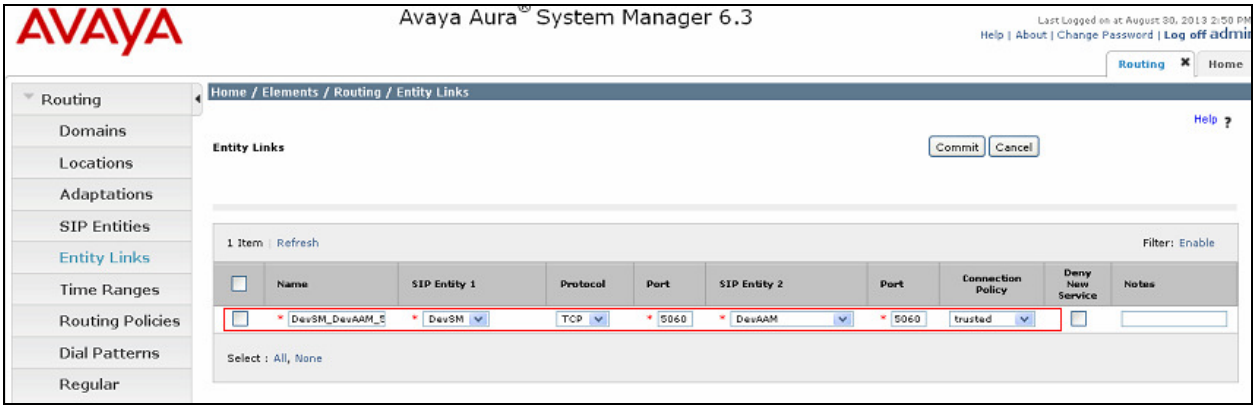
- Session Manager ⇔ Communication Manager
- Session Manager ⇔ Avaya Aura® Messaging
- Session Manager ⇔ Avaya ACE

Navigate to **Routing → Entity Links**, and click on the **New** button (not shown) to create a new Entity Link. Provide the following information:

- Enter a descriptive name in the **Name** field.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section 7.3**.
- In the **Protocol** drop down menu, select the transport protocol to be used on this link.
- In the **Port** field, enter the port on Session Manager to receive SIP messages from the SIP Entity on the other end of the link (e.g., **5060** or **5061**).
- In the **SIP Entity 2** drop down menu, select an entity created in **Section 7.3**.
- In the **Port** field, enter the port on the remote SIP Entity to receive SIP messages (e.g., **5060** or **5061**).
- Check the **Trusted** box.
- Enter a description in the **Notes** field if desired.

Click on the **Commit** button to save each Entity Link definition.

The following screen shows an Entity Links page (between Session Manager and AAM) used during the compliance test.



Repeat the steps to define Entity Links between Session Manager and Communication Manager and between Session Manager and Avaya ACE.

7.5. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section 7.3**) with Time of Day admission control parameters (**Section 7.5**) and Dial Patterns (**Section 7.7**). In the reference configuration, Routing Policies are defined for Communication Manager.

To add a Routing Policy, navigate to **Routing → Routing Policy**, and click on the **New** button (not shown) on the right. Provide the following information:

General section

- Enter a descriptive name in the **Name** field.
- Enter a description in the **Notes** field if desired.

SIP Entity as Destination section

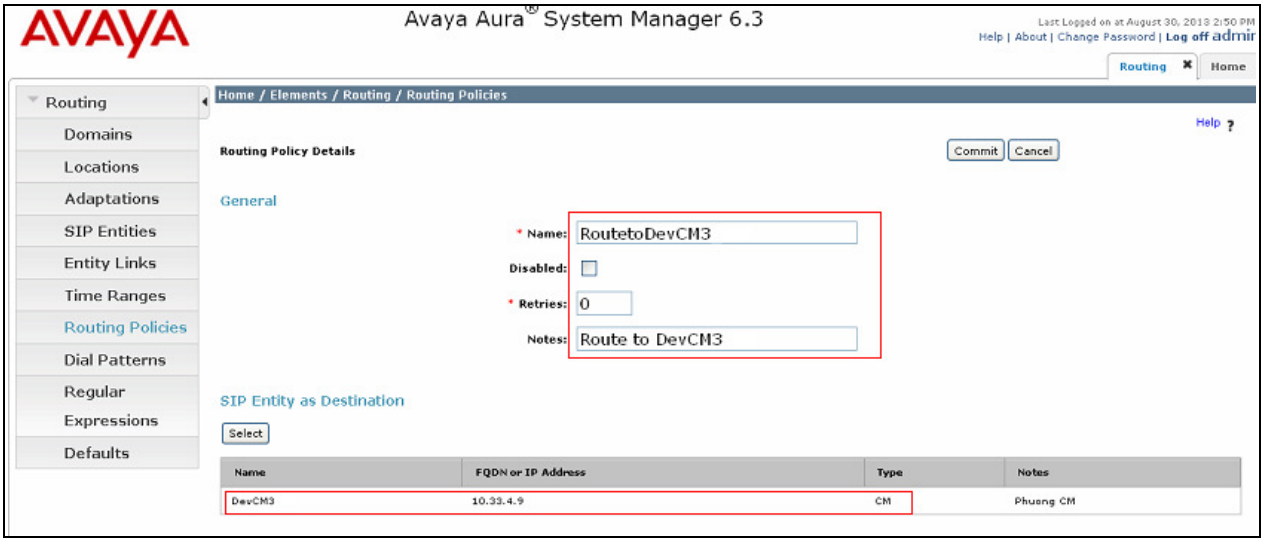
- Click the **Select** button.
- Select the SIP Entity that will be the route destination (not shown).
- Click the **Select** button and return to the Routing Policy Details form.

Time of Day section

- Leave default values.

Click **Commit** to save the Routing Policy definition.

The following screen shows the Routing Policy used for the compliance test.



Repeat the steps to define routing policies to others Entities.

7.6. Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In addition, the domain in the request URI is also examined. In the compliance test, the following Dial Patterns are defined.

- 5215x – SIP endpoints

- 39990 – Avaya Aura® Messaging Pilot Number.

To add a Dial Pattern, select **Routing → Dial Patterns,** and click on the **New** button (not shown) on the right. During the compliance test, 5-digit dial plan was utilized. Provide the following information:

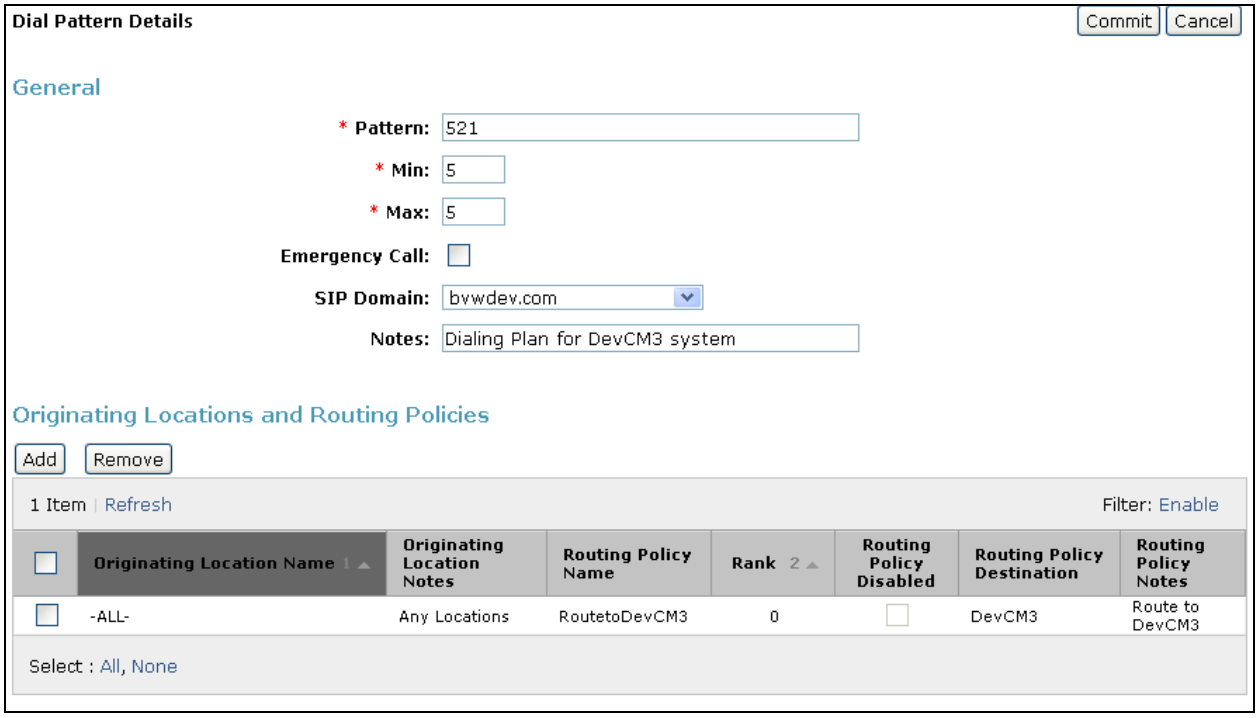
General section

- Enter a unique pattern in the **Pattern** field (e.g., **521**).
- In the **Min** field enter the minimum number of digits (e.g., **5**).
- In the **Max** field enter the maximum number of digits (e.g., **5**).
- In the **SIP Domain** field drop down menu select the domain that will be contained in the Request URI *received* by Session Manager from Communication Manager.
- Enter a description in the **Notes** field if desired.

Originating Locations and Routing Policies section

- Click on the **Add** button and a window will open (not shown).
- Click on the boxes for the appropriate Originating Locations (see **Section 7.2**), and Routing Policies (see **Section 7.6**) that pertain to this Dial Pattern.
  - Location: **–All-**.
  - Routing Policies: **RoutetoDevCM3**.
  - Click on the **Select** button and return to the Dial Pattern window.

Click the **Commit** button to save the new definition. The following screen shows the Dial Pattern used for routing calls to DevCM3 during the compliance test. The Dial Pattern for routing calls to AAM was similarly configured.

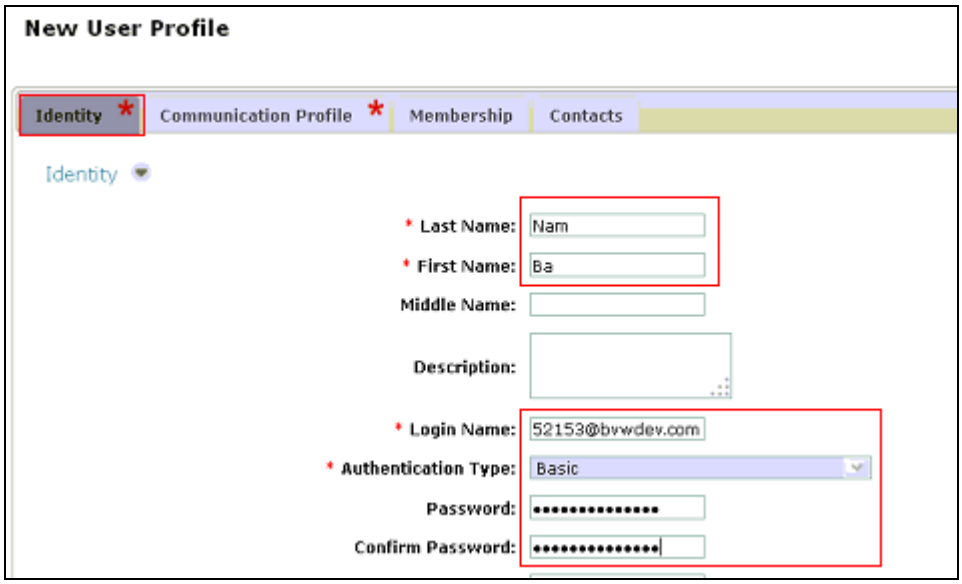


7.7. Configure SIP Users

To add new SIP users, Navigate to **Users → Manage Users**. Click **New** (not shown) and provide the following information:

Identity tab:

- **Last Name –** Enter last name of user.
- **First Name –** Enter first name of user.
- **Login Name** – Enter extension and domain name used in the system.
- **Authentication Type** – Default is **Basic**. Use this default value.
- **Password** – Enter password, it is used to log into System Manager. Repeat the same for **Confirm Password**.



Communication Profile tab:

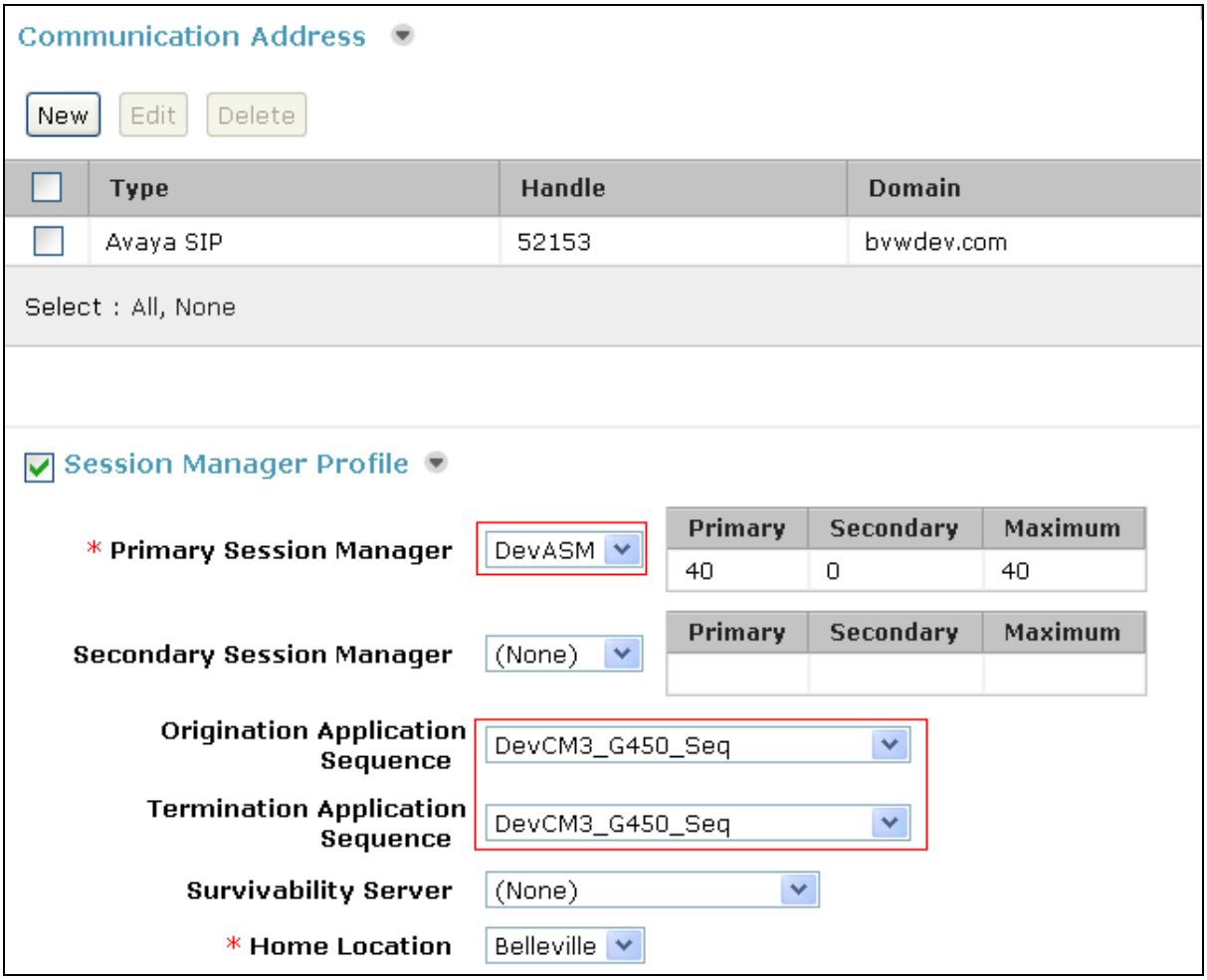
- Communication Profile section
  - **Communication Profile Passowrd –** enter numeric password which is used to log into device.

  Verify there is a default entry identified as the **Primary** profile for the new SIP user. If an entry does not exist, select **New** and enter values for the following required attributes:
  - **Name** – Enter **Primary**.
  - **Default** – Enter ☑

- Communication Address sub-section
  Select **New** to define a **Communication Address** for the new SIP user, and provide the following information.
  - **Type** – Select **Avaya SIP** from drop-down menu.
  - **Fully Qualified Address** – Enter same extension number and domain used for Login Name, created previously.

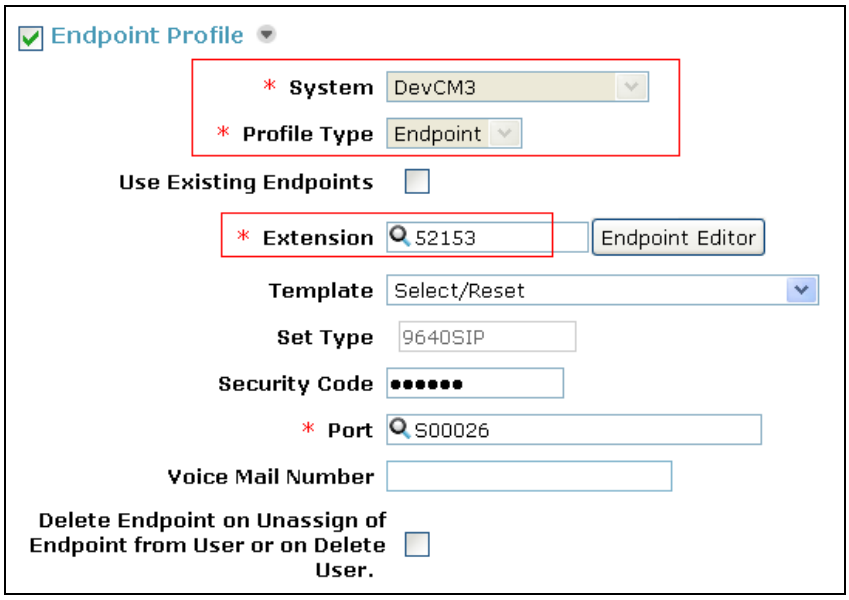
  Click the **Add** button to save the Communication Address for the new SIP user.

- Session Manager Profile sub-section
  - **Primary Session Manager** – Select the Session Managers of interest.
  - **Secondary Session Manager** – Select **(None)** from drop-down menu.
  - **Origination Application Sequence –** Select Application Sequence for Communication Manager.
  - **Termination Application Sequence** – Select Application Sequence for Communication Manager.
  - **Survivability Server** – Select **(None)** from drop-down menu.
  - **Home Location** – Select Location created in **Section 7.2**.

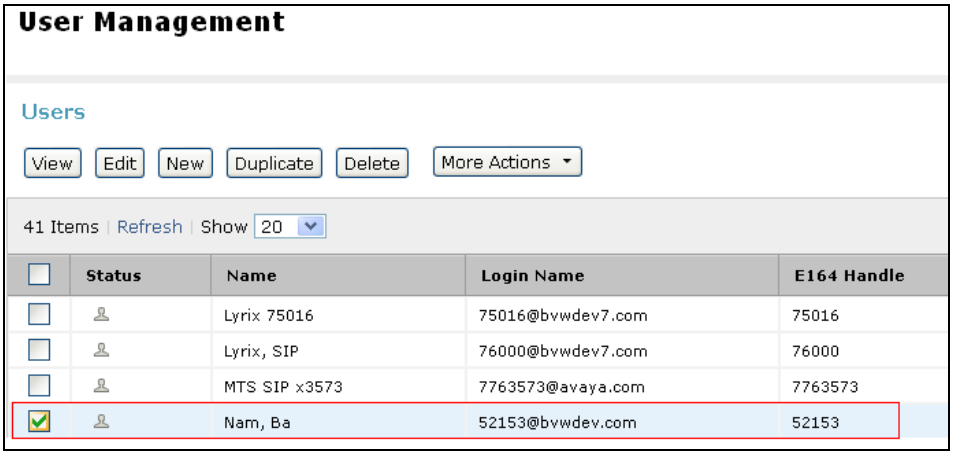


- CM Endpoint Profile sub-section
  - **System** – Communication Manager of interest.
  - **Profile Type** – Verify **Endpoint** is selected.
  - **Use Existing Endpoints -** Leave unchecked to automatically create new endpoint when new user is created. Otherwise, check the box if endpoint is already defined in Communication Manager.
  - **Extension** - Enter same extension number used in this section.
  - **Template** – Select template for type of SIP phone

- **Port** – Select **IP** from drop down menu
- **Voice Mail Number –** Enter **Pilot Number** for **AAM,** or else, leave field blank.
- **Delete Station on Unassign of Endpoint** – Check the box to automatically delete station when Endpoint Profile is un-assigned from user.



Click **Commit** to save definition of the new user. The following screen shows the created users during the compliance test.

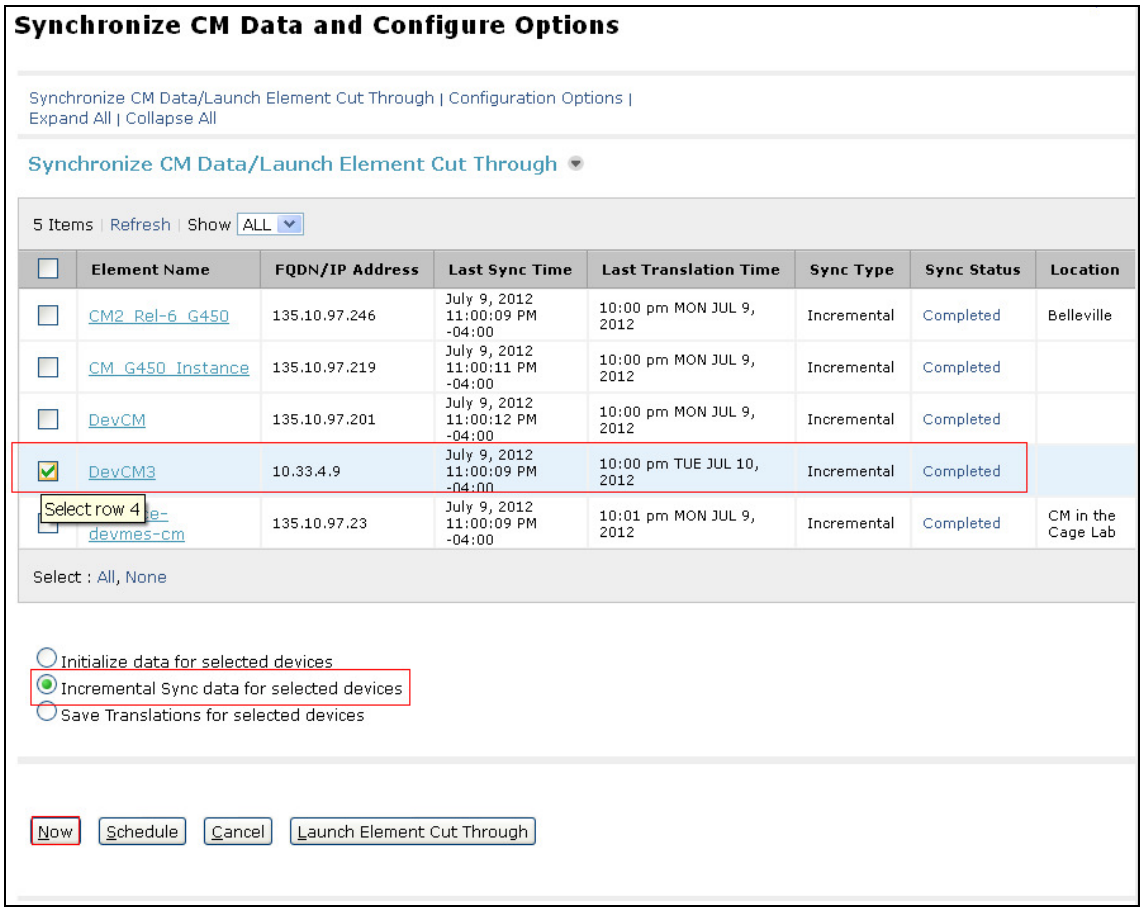


7.8. Synchronization Changes with Avaya Aura® Communication Manager

After completing these changes in System Manager, perform an on demand synchronization. Navigate to **Services → Inventory → Synchronization → Communication System.**

On the Synchronize CM Data and Configure Options page, the Synchronize CM Data/Launch Element Cut Through table is displayed. Select the Communication Manager for synchronization.

- Click ◉ to select **Incremental Sync data for selected devices** option. Click **Now** to start the synchronization.
- Use the **Refresh** button in the table header to verify status of the synchronization.
- Verify synchronization was successfully completed by verifying the status in the Sync. Status column shows **Completed**.



8. Configure Avaya Agile Communication Environment™

8.1. SSL Certificate Signing Authority

In order for Avaya Agile Communication Environment™ (ACE) and Communication Manager to establish SSL connectivity, the signing authority of Communication Manager's Server certificate must be configured as trusted on Avaya ACE. Refer **Section 13** for the list of relevant documents.

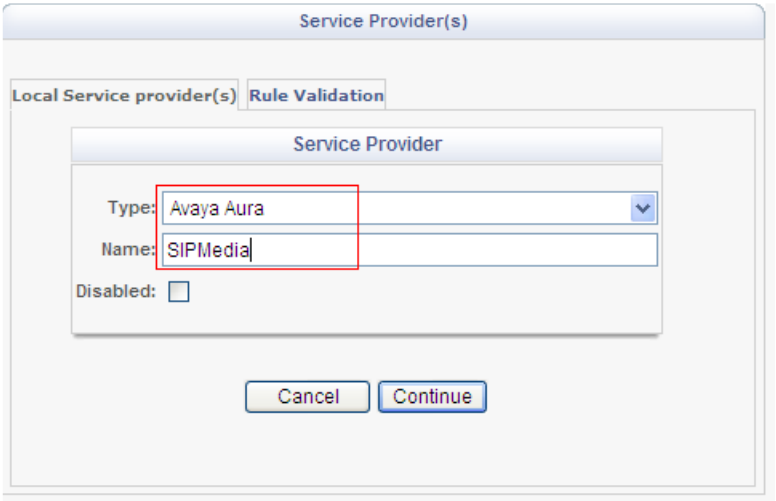
When Avaya ACE is initially installed, some signing authorities are automatically configured as trusted on Avaya ACE. For example, by default, Avaya ACE trusts any certificate signed by SIP Product Certificate Authority or Avaya Product Root CA. If Communication Manager is configured with a server certificate signed by such an authority, then no further configuration is needed on Avaya ACE. Skip this section and move to **Section 8.2**. If Communication Manager is not configured with a server certificate that is signed by such an authority, then further configuration may be needed on Avaya ACE. Please see section "Configuring the Communication Manager's SSL certificate signing authority as trusted on Avaya ACE" in [4].

8.2. Add SIP Service Provider

This step configures SIP Service Provider with Avaya Media Server which will provide web services Third Party Call v3 such as creating Conference call.

Open a web browser and enter the following URL to view the Avaya ACE administrative console: **https://<hostname>:9449/oamp/,** select **Configuration → Service Providers**.
In the Service Providers window, click **Add** (not shown).

- **Type -** select **Avaya Aura**.
- **Name -** enter a name for the Avaya Aura Service Provider. Example: SIPMedia.

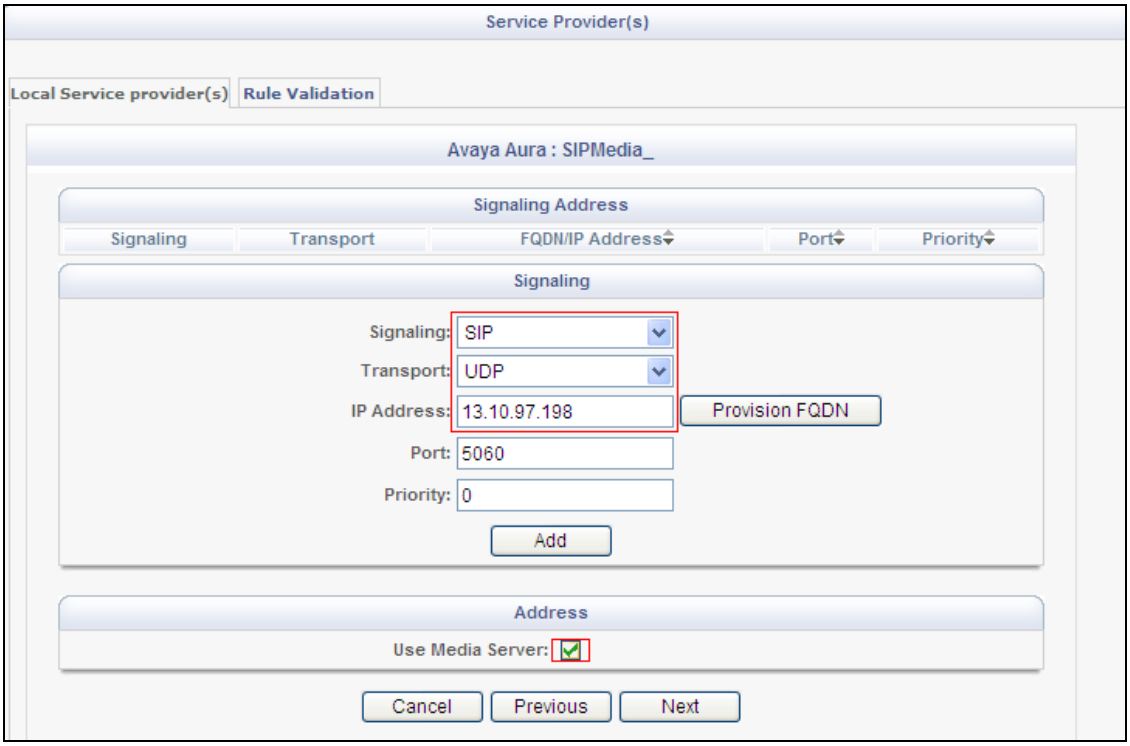


Click **Continue**.

In **Signaling** and **Address** sections:

- **Signaling** - select **SIP**.
- **Transport** - select **UDP**.
- **IP Address** - enter Session Manager's IP address.
- **Port** – verify **5060** is specified for UDP transport.
- **Priority** – leave as default.
- **Use Media Server** –checked

Click **Add**.

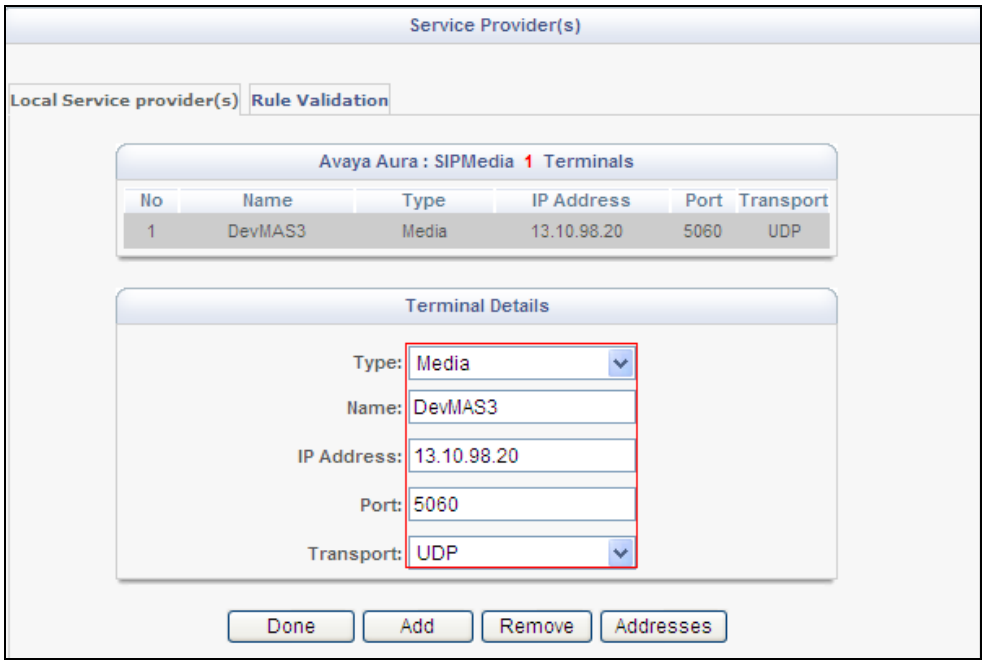


Click **Next** to enter detail for Media Server.

In Terminal Details section:

- Select **Media** from the **Type** list.
- Type in a descriptive name in **Name** field. Example: DevMAS3.
- In **IP Address** field, enter Avaya Media Server's IP address.
- In **Port** field, enter **5060**.
- Select **UDP** in the **Transport** list.

Click **Add** to add Media Server into Service Provider.

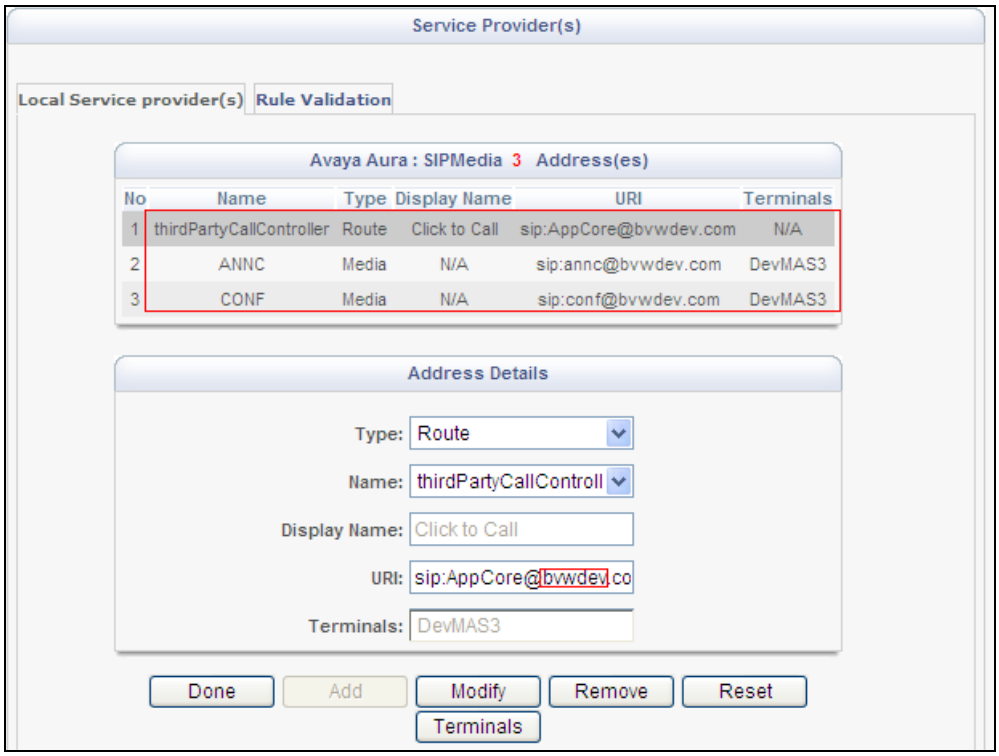


Click **Next** to addresses.

In the **Address(es)** section, default routes are displayed. To modify a route, select the route item from the table to edit in the **Address Details** section:

- **Name** - leave default value as **thirdPartyCallController**.
- **Display Name** - leave default values as **Click to Call**.
- **URI** field - leave default or modify the domain name if need. During the compliance test, domain name was modified to **bvwdev.com**.

Click **Modify** to save changes.



Next steps is to add **ANNC**. In the Address Details section:

- **Type** - select **Media**.
- **Name** - select **ANNC**.
- **URI** - enter sip:annc@<domain> where <domain> is the domain name of the media server. During compliance test **bvwdev.com** was used.
- **Terminals** - this field is read-only showing the name of the media server terminal created in the previous step.

Click **Add**.

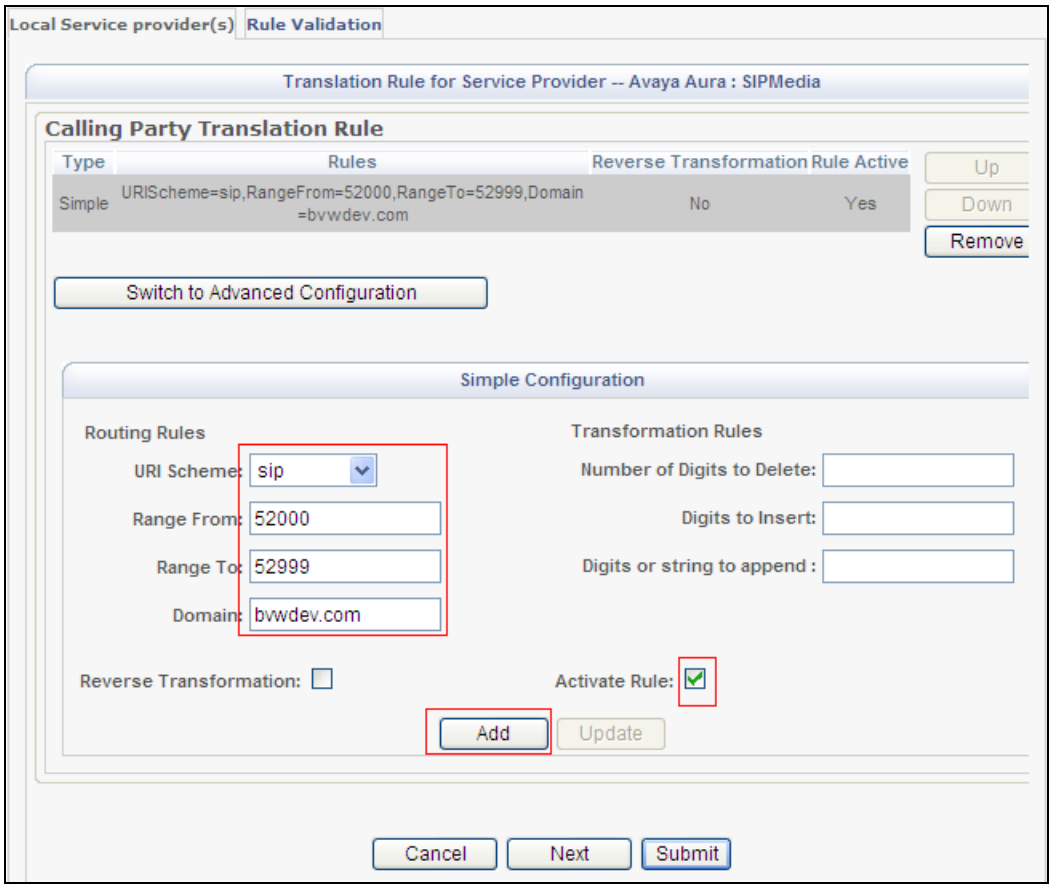
Repeat the same steps for **CONF**.

Click **Next** to enter Translation rule for this Service Provider.

In the **Calling Party Translation Rule**'s **Simple Configuration** section:

- **URI Scheme -** select **sip**.
- **Range From -** type in range from extesion, example: 52000 is a value used during compliance test.
- **Range To** - type in range to extesion. Example: 52999 is a value used during compliance test.
- **Domain** - enter the domain used in the system.
- **Active Rule** - checked.

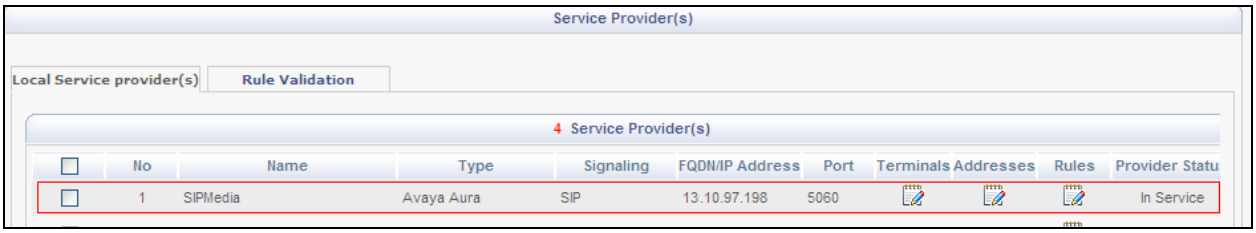
Click **Add** to add rule.



Click **Next** to move to Called Translation Rule detail. Repeat the same step as above to enter **Called Translation Rule**. Click **Add** to add rule.

Click Submit to submit SIP Service Provider.

Verify the status of newly created SIP Service Provider is "**In Service**"



8.3. Add ASAI Service Provider

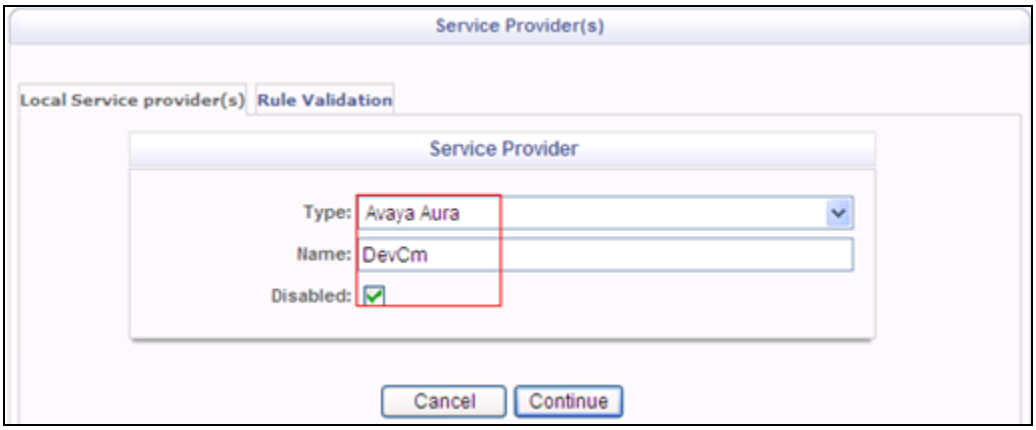
This section creates ASAI Service Provide which provides web services Third Party Call Control v2 and v2.4 such as make call, Single Step Transfer, Consult Transfer Hold call, cancel or hang up call.

Open a web browser and enter the following URL to view the Avaya ACE administrative console: **https://<hostname>:9449/oamp/,** select **Configuration → Service Providers**. In the Service Providers window, click **Add** (not shown).

In the Service Provider section:

- **Type -** select **Avaya Aura**.
- **Name -** enter a name for the Avaya Aura Service Provider.
- **Disable –** checked to add the service provider in a disabled state.

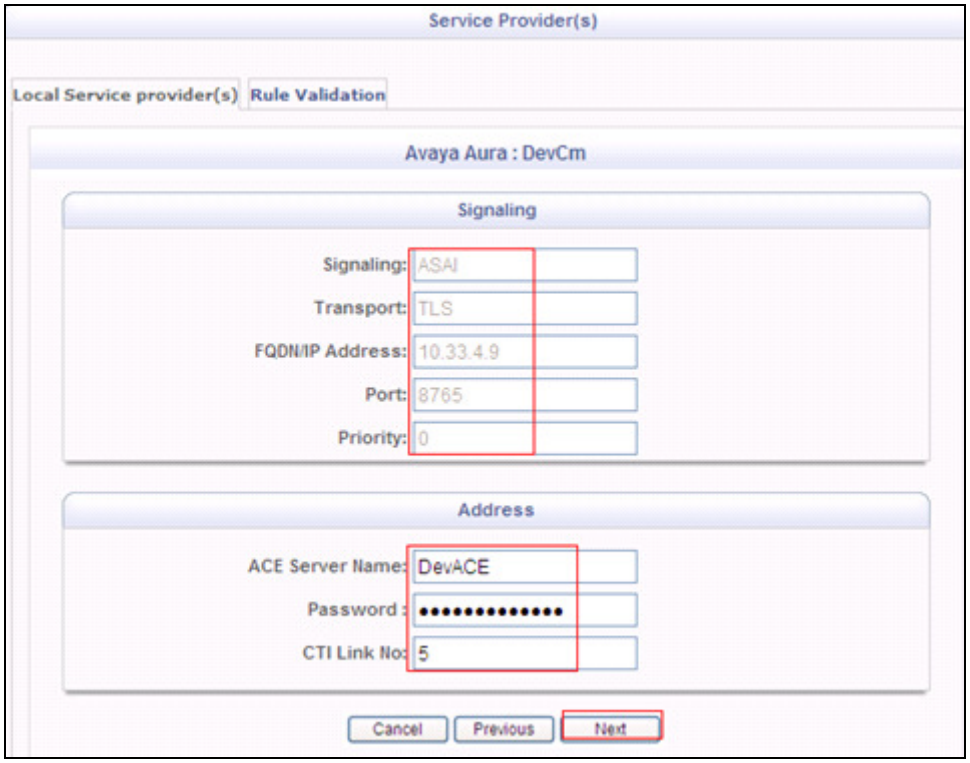
Click **Continue**.



The Service Providers window for Avaya Aura® appears. Enter the signaling information:

- **Signaling -** select **ASAI**.
- **FQDN/IP Address -** enter the IP address of the Communication Manager server. Using the fully qualified domain name (FQDN) is not supported for the ASAI Service Provider.
- When ASAI signaling, the **Port** is set to **8765**, the **Transport** protocol is set to **TLS**, and the **Priority** is set to **0**. The **Port** can be changed to a non-default value by entering the desired port number in the **Port** field.
- Enter the **ACE Server Name** and **Password** created in **Section 5.2.2.**
- Enter the **CTI Link No** created in **Section 5.2.3**.

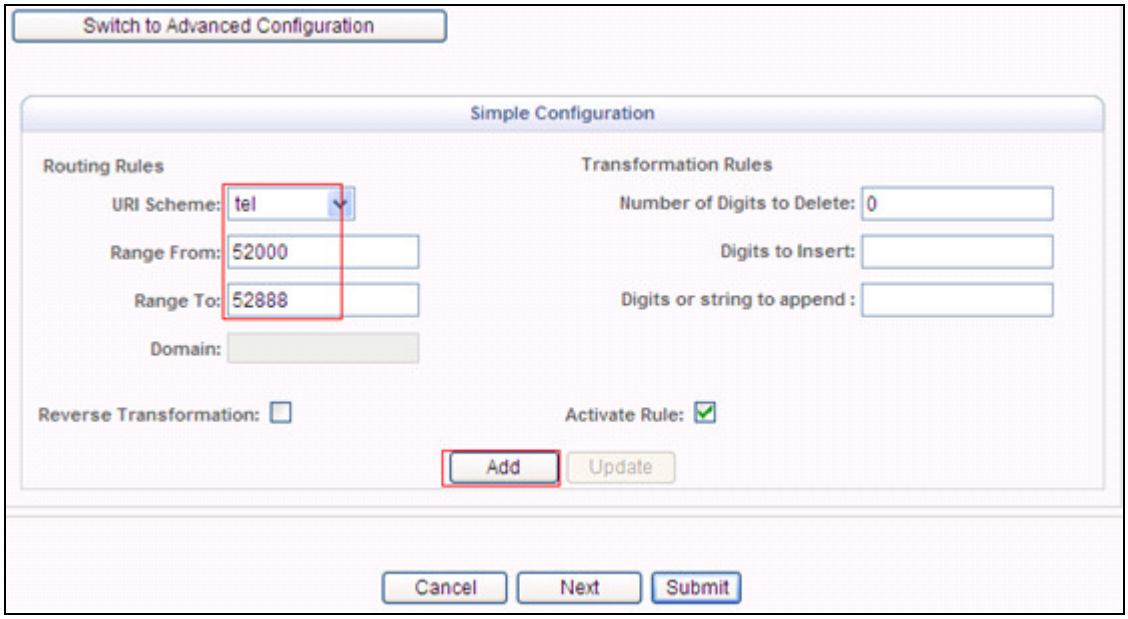
Click **Next** to add rules.



Enter information for **Calling Party Translation Rule - Simple Configuration** rule as shown below:

- **URI Scheme**: select **tel**.
- **Range from** - type in range from extesion, example: 52000 is a value used during compliance test.
- **Range to** - type in range to extesion. Example: 52999 is a value used during compliance test.
- **Activate Rule** - checked

Click **Add** to add the new rule.



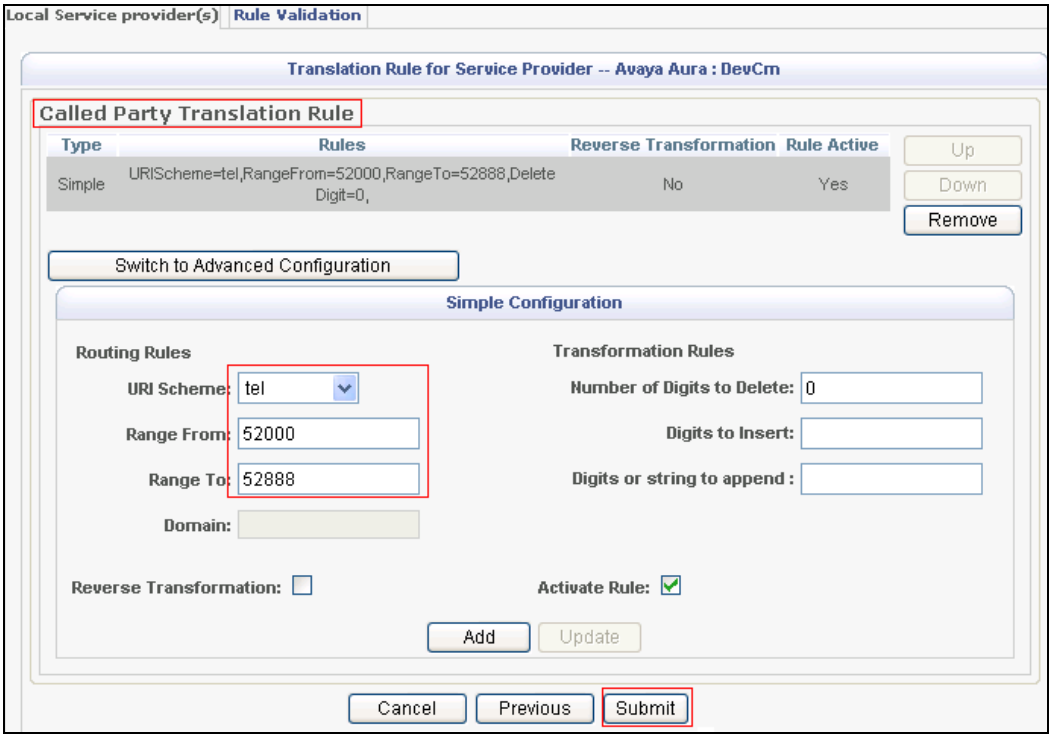
Click **Next** to add rule for Called Party.

Enter information for **Called Party Translation Rule - Simple Configuration** rule as show below:

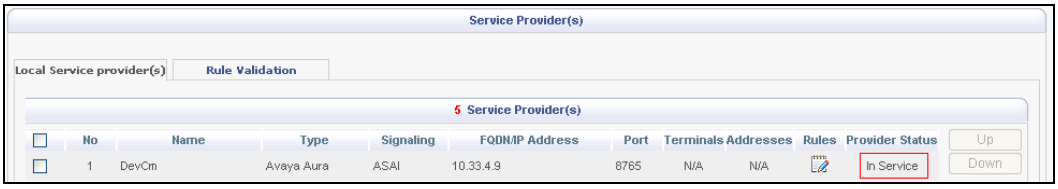
- **URI Scheme** - select **tel**.
- **Range from** - type in range from extesion, example: 52000 is a value used during compliance test.
- **Range to** - type in range from extesion, example: 52888 is a value used during compliance test.
- **Activate Rule** - checked

Click **Add** to add the new rule.

Click Submit to Submit new **Service Provider**.



Verify the status of the created Service Provider is “In Service” as shown below:,



8.4. Activate System Manager Certificate

Use this procedure to configure the Avaya ACE certificate on System Manager for secure TLS communication between Avaya ACE and System Manager.

Before you begin
You must know the System Manager Enrollment password.
The System Manager Enrollment password is configured in the System Manager web console under **Home → Services → Security → Certificates → Enrollment Password**.

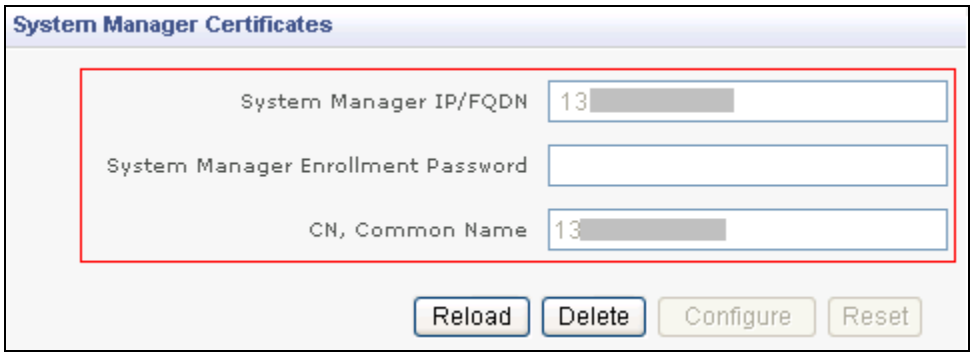
Follow steps below to add System Manager certificate on Avaya ACE

- Login Avaya ACE, select **Security → Certificate Management → System Manager Certificates**.
- Enter the System Manager IP address or fully qualified domain name (FQDN) in the **System Manager IP/FQDN** field. For example, 13.10.97.198
- Enter the **System Manager Enrollment Password** in the **System Manager Enrollment Password** field.
- Enter the FQDN of the Avaya ACE server (or IP) that will receive the certificate in the **CN, Common Name** field. For example, 13.10.97.18

Click **Configure**.

Secure TLS certificates are exchanged between Avaya ACE and System Manager. This may take a minute or so to complete. During this time you may be prompted to log out and log back in to the Avaya ACE GUI.

- Verify that the certificate configuration is successful. On the Avaya ACE GUI menu bar, choose **Security > Certificate Management > System Manager Certificates**. The System Manager IP should now be grayed out and the **Configure** button disabled as figure below show:



8.5. Certificate Expiry Date

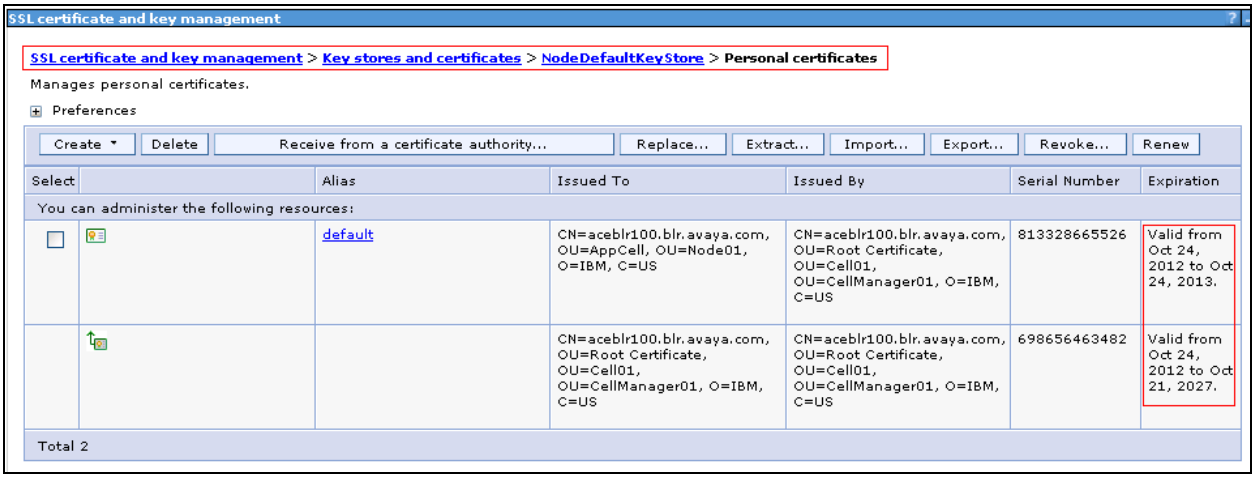
You must be aware of the security certificate expiry date. Allow a certificate to expire results in loss of service.

- Open a web browser and enter the following URL to view the WebSphere administrative console: https://<hostname>:9043/admin.
- The administrative console loads and a window opens for user ID and password (not shown). Log in using appropriate login credentials.
- In the navigation pane on the left, select **Security > SSL certificate and key management**.
- In the center pane, under **Related Items**, select **Key stores and certificates**.

- Click **CellDefaultKeyStore**.
- Under **Additional Properties**, select **Personal certificates**.
- View the date range in the **Expiration** column.

If the certificate has expired or is about to expire, click **Renew**.

The screen below shows the Personal Certificates used during compliance testing:



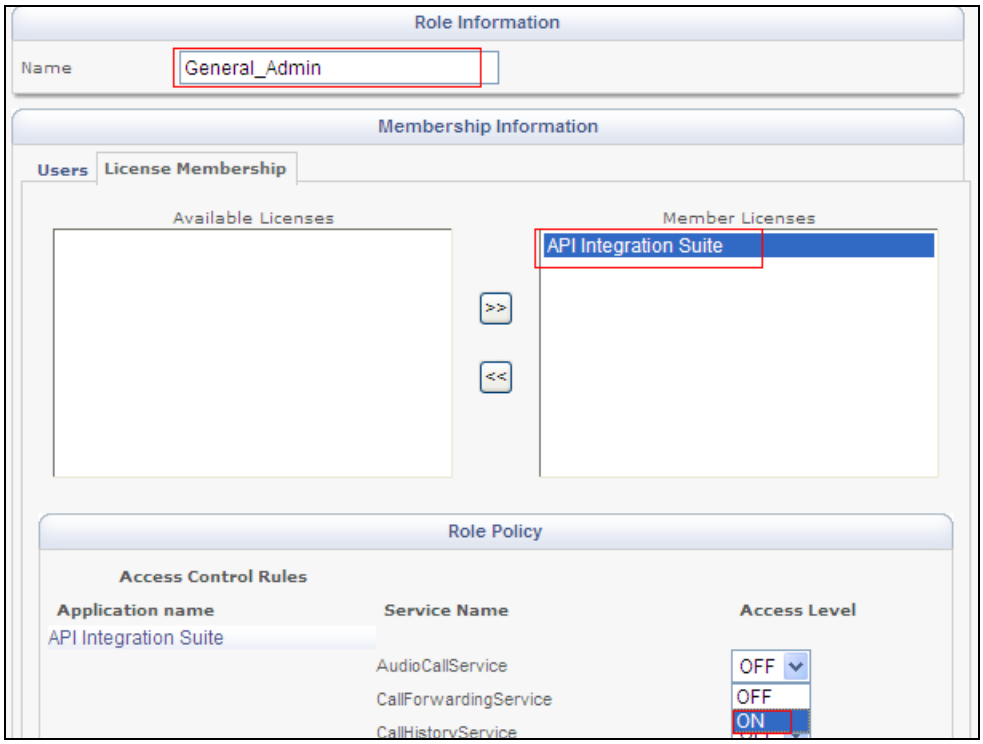
8.6. Add Role

This section describes how to create Role for user created in **Section 8.7**.

In Avaya ACE administrative console, select **Security → Role Management → Create Role.** Enter the following for a new Role

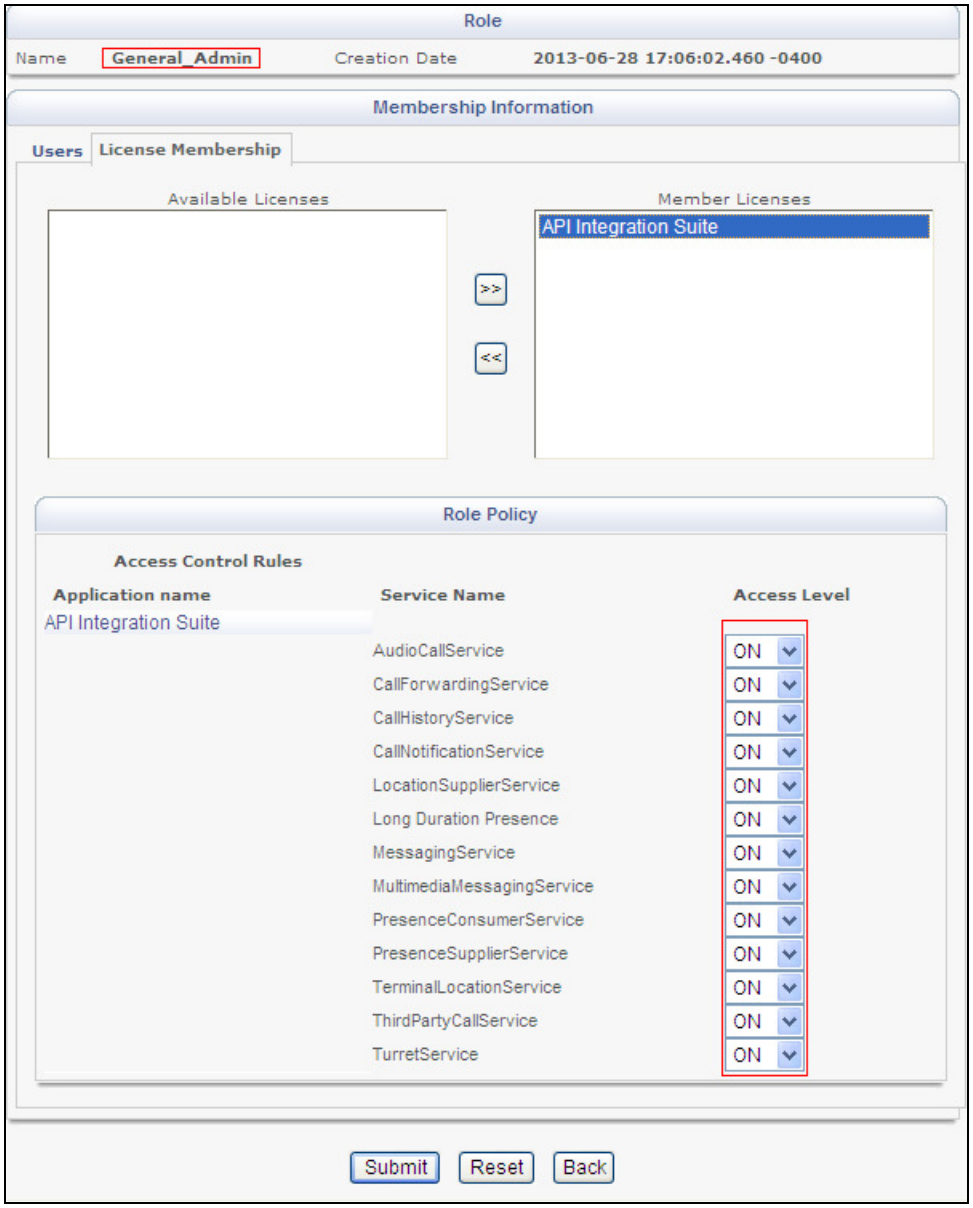
- **Name:** Enter any name for the new Role.
- **Role Member:** select user in the left panel and move it into the Role member.

Select the **License Membership** tab, assign **API Intergration Suite** to **Memember Lincense**. Make sure to turn on **Access Level** of all services.



- Click **Submit** to save changes.

- Verify all the access level is "**ON**"

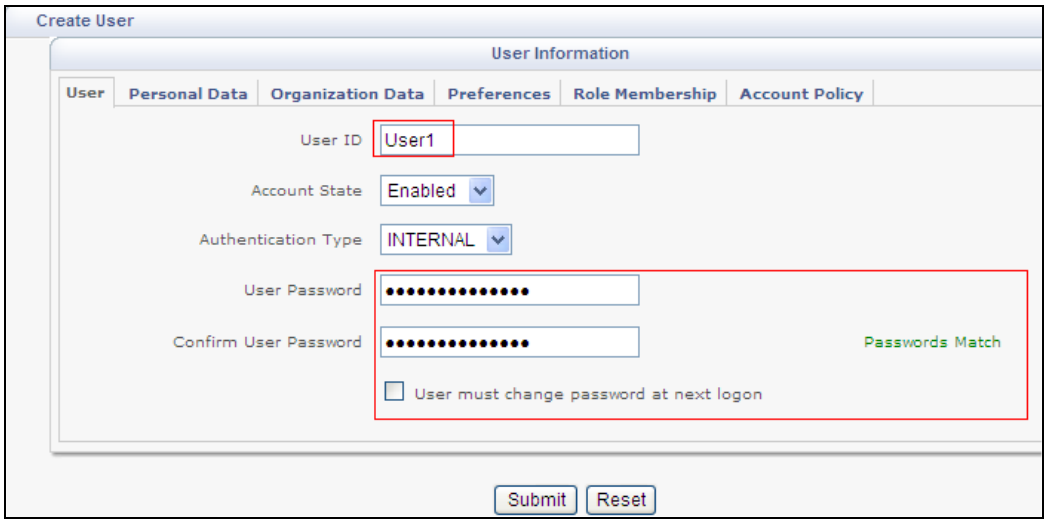


8.7. Add user

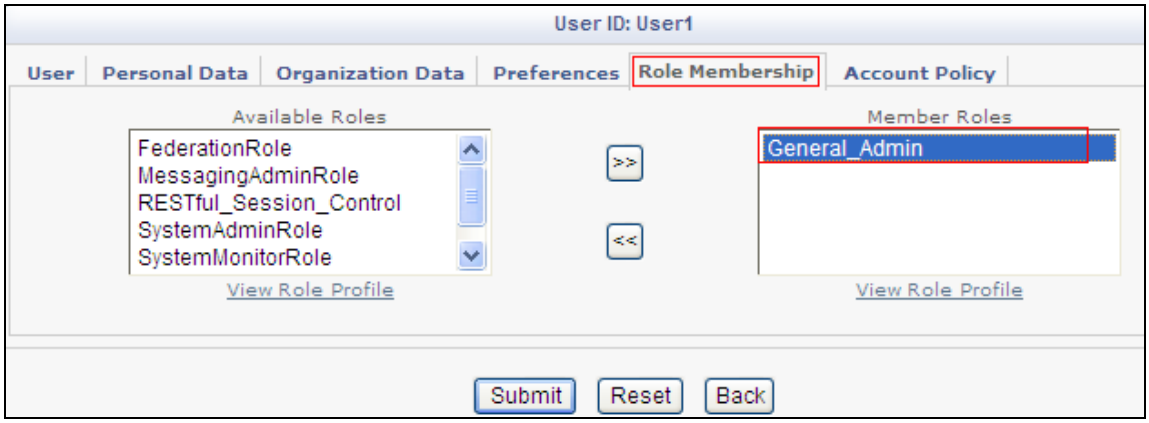
The web service client iLink is using a configured user on Avaya ACE.
The web service client belongs to a user group on Avaya ACE with a group type of **user** or higher, and with the appropriate access control rules configured for the Third Party Call Control service. See **Section 8.6** for step how to create new role for user.

Select **Security → User Management → Create User**

- Enter **User ID**: User to log into ACE web service of the web client (application) (e.g **User1**).
- **Account State**: select **Enabled**.
- **Password**: password (e.g DevConnect@123)



Select **Role Membeship** tab, assign Role created in previous section. Example: General_Admin.



Select **Submit** to create the user.

Repeat the same step to create User2 and User3. These users will be used to log in Aura® Alliance Phone in **Section 10.2.**

9. Configure Media Server

It is assumed that Avaya Media Server with required applications have been installed, fully licensed and in operaional state.

Perform the following procedures using Element Manager (EM) to configure items and tasks required to activate
Avaya Media Server. To interact with Avaya ACE, the Avaya Media Server network element must meet the following configuration requirements:

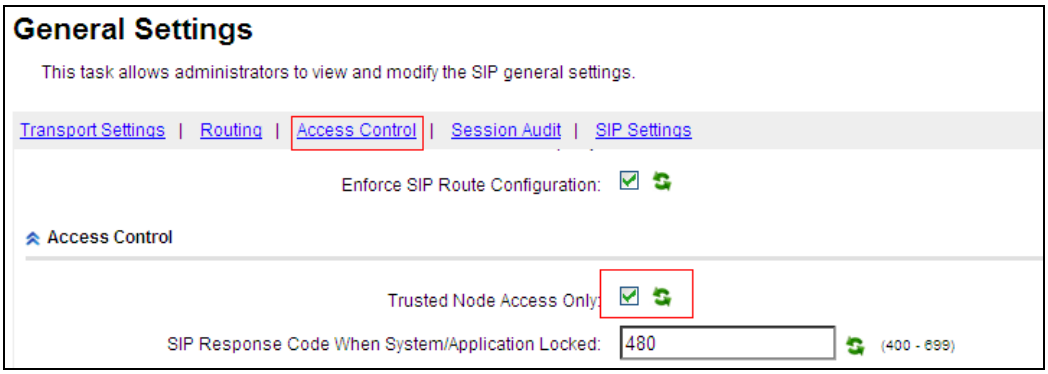
- Enable Trusted node access for SIP.
- Enable SIP signaling over UDP.
- Add ACE host as a SIP trusted node.

9.1. Enabling Trusted Node Access for SIP

To gain access to EM, use a Web browser with this URL: http://<serverIP>:8080/em, where serverIP is the address of your server. For example, http://135.60.86.209:8080/em.

Log in using the server admin or root user and password. Then navigate to **EM → System Configuration → Signaling Protocols → SIP →General Settings → Access Control**.

- Check **Trusted Node Access Only** checkbox.
- Click **Save**.



9.2. Enable SIP Signaling Over UDP

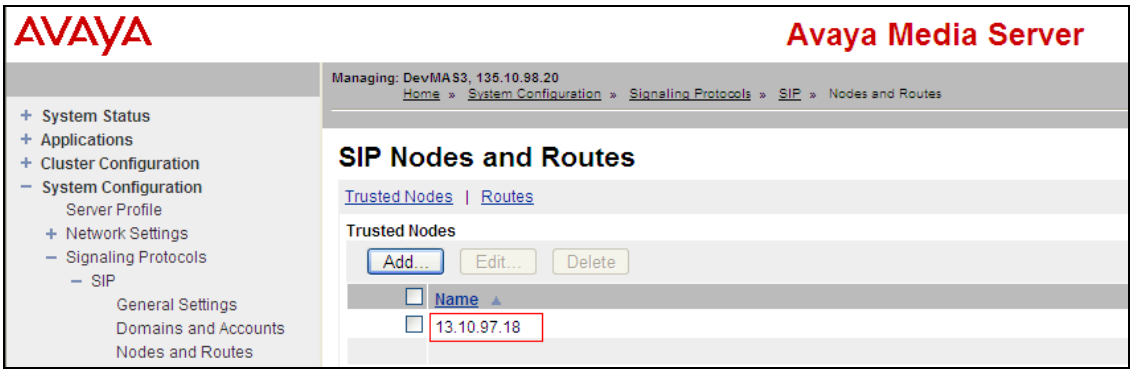
Navigate to **EM → System Configuration → Signaling Protocols → SIP → General Settings**.

- Make sure **SIP UDP Transport** option is enabled.
- Click **Save** if needed.

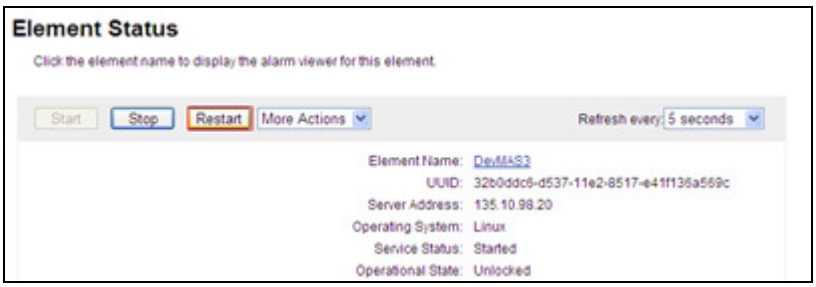
9.3. Add ACE Host as SIP Trusted Node

Add Avaya ACE as a trusted host on Media Server by navigate to **EM System Configuration → Signaling Protocols → SIP → Nodes and Routes → Trusted Nodes**.

- Click **Add…**
- Enter the IP of the SIP node from where you will get the test call. During the compliance test, IP of Avaya ACE is added.
- Click **Save**.



Navigate to **System Status →Element Status**, click **Restart** to restart Media Server.



10. Configure IBM Sametime

It is assumed that IBM Sametime Server and Client are installed and in operational. This section only describes how to install and login Aura® Alliance Phone plug-in on IBM Lotus Sametime client.

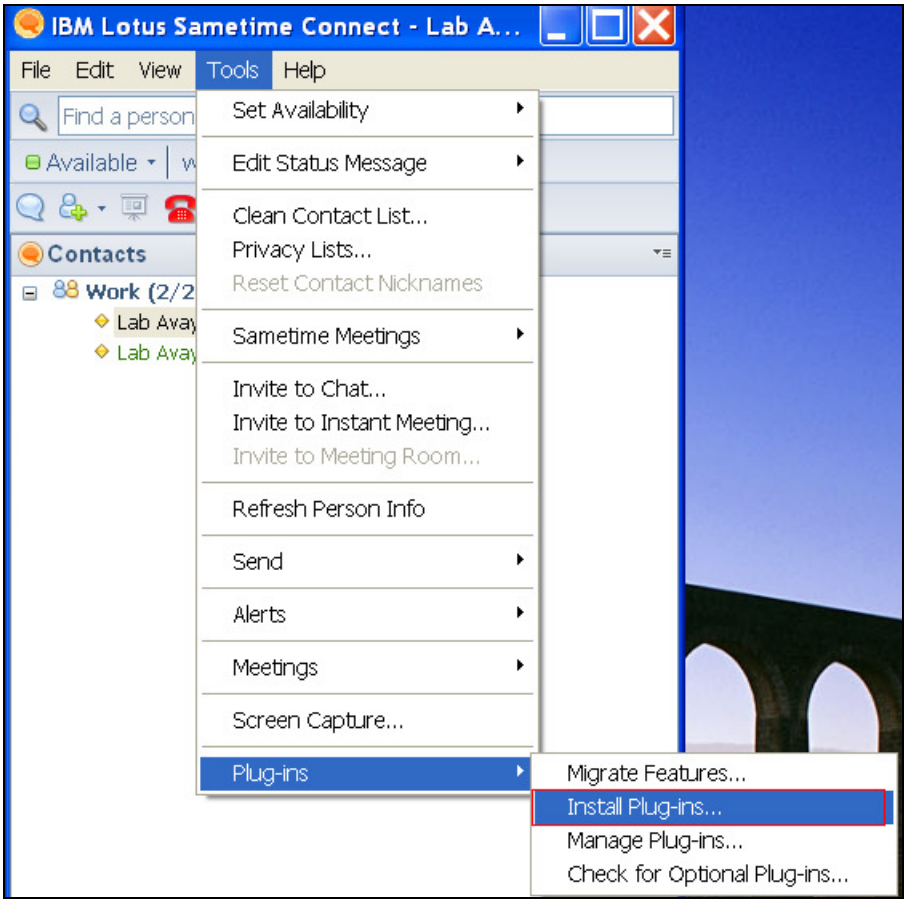
- Install Aura® Alliance Phone plug-in.
- Login Aura® Alliance Phone

10.1. Install Aura@ Alliance Phone Plug-in

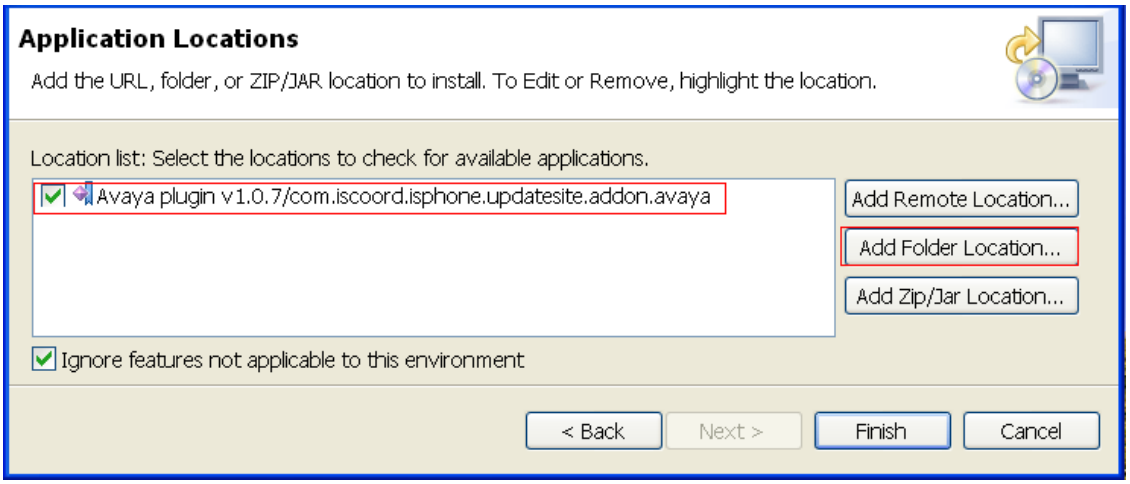
Before starting this section, make sure to download the Aura® Alliance Phone plug-in file onto the local PC. For the compliance test Avaya plugin v1.0.7 was downloaded and used. IBM Lotus Sametime users were created on the Sametime server.

Lanch and log into IBM Sametime using appropriate login credentials. During compliance testing 3 users were created: Lab Avaya1, Lab Avaya2 and Lab Avaya3.

In IBM Lotus Sametime Connect client. Select **Tool → Plug-ins → Install Plug-ins**



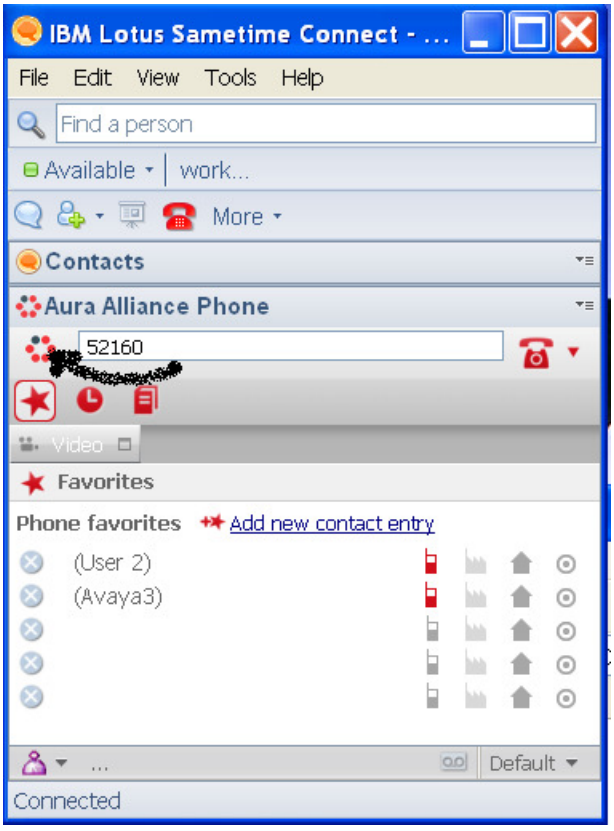
Click **Add Folder Location** button and select the patch file to *com.iscoord.isphone.updatesite.notes*. Click **Finish**.



Select the desired features and click **Finish** to install them. Follow the screen instruction to complete the installation. Restart IBM Lotus Sametime Connect. (not shown).

10.2. Log Into Aura® Alliance Phone.

Once the features are installed and IBM Lotus Notes has been restarted, Aura® Alliance Phone appears in the client. Click on the "" red icon on the leftside of the dialbar to log into Avaya ACE.

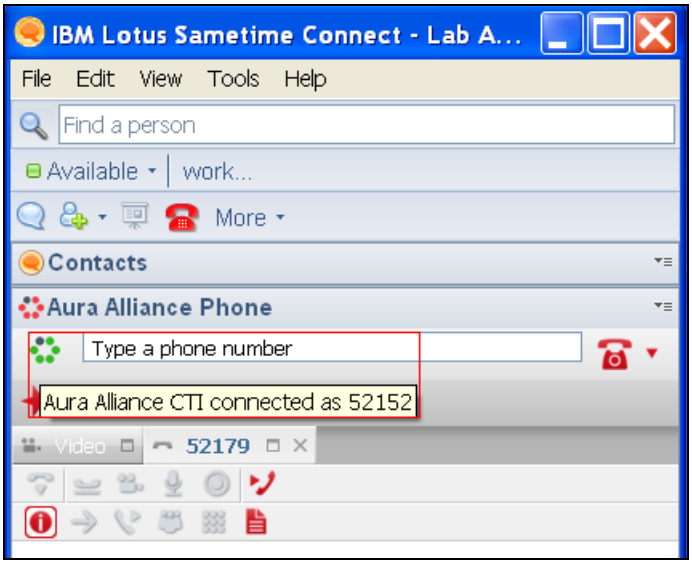


For first-time login, in the login window, enter the following information:

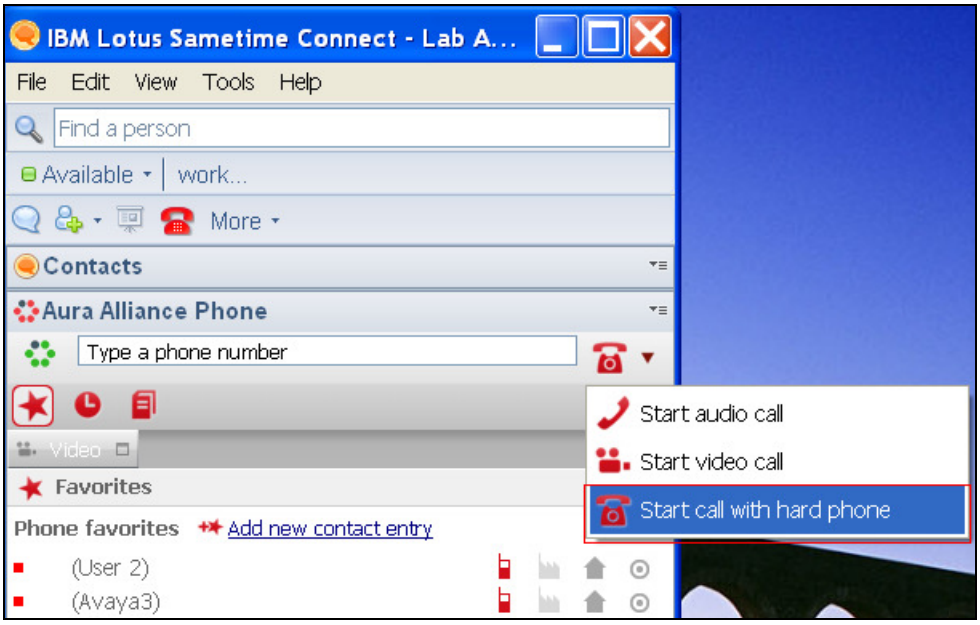
- **ACE Server address**: enter IP address of the ACE server.
- **User name**: enter user name created in Avaya ACE in **Section 8.7**.
- **Password:** enter password of user created in Avaya ACE in **Section 8.7**.
- **Extension:** enter extension used for Aura® Alliance Phone.
- **Domain:** enter domain (e.g., bvwdev.com, used during compliance testing).
- Click **Connect!** to log in Aura® Alliance Phone.

Note: The login information can be modified in **File →Auara Alliance Phone Setting →Aura Alliance CTI settings**.

If the login succeeds, the login icon turns to green"". Roll the mouse over the green login icon, the information of current extesion will be displayed.

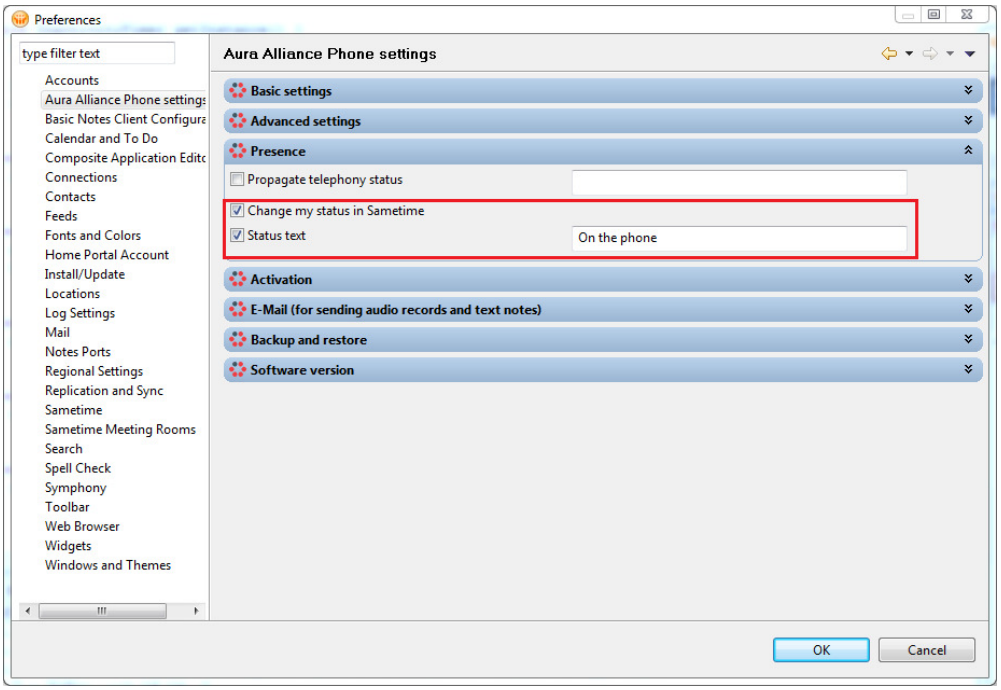


In order to make CTI calls, make sure to switch the call method from "**Start Audio Call**" to "**Start call with hard phone**" icon from the dropdown box right of the dial bar.



Now Aura® Alliance Phone is ready to make and received calls. See **Section 11.6** on how to make a call using Aura® Alliance Phone

Sametime presence change during a phone call can be configured in the Aura Alliance Phone settings under the Presence section.



11. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Avaya Aura® Application Enablement Services, Avaya ACE, Avaya Aura® Messaging and Aura® Alliance Phone application.

11.1. Verify Avaya Aura® Communication Manager

The following steps may be used to verify the configuration:

- From the Communication Manager SAT, use the **status signaling-group** xxx command (where xxx is a signaling group number) to verify that the SIP signaling group is **in-service**.
- From the Communication Manager SAT, use the **status trunk-group** xxx command (where xxx is a trunk group number) to verify that the SIP trunk group is **in-service**.
- Verify with the **list trace tac** xxx command (where xxx is the trunk access code for the sip trunk group) that calls are routed over the correct trunk group.

- Verify the status of the administered CTI links by using the **status aesvcs cti-link** command. Verify that the **Service State** is **established**.

```
status aesvcs cti-link
                    AE SERVICES CTI LINK STATUS
CTI    Version  Mnt   AE Services      Service        Msgs      Msgs
Link            Busy  Server           State          Sent      Rcvd

5      4        no    DevACE           established    15        15
8               no                     down           0         0
```

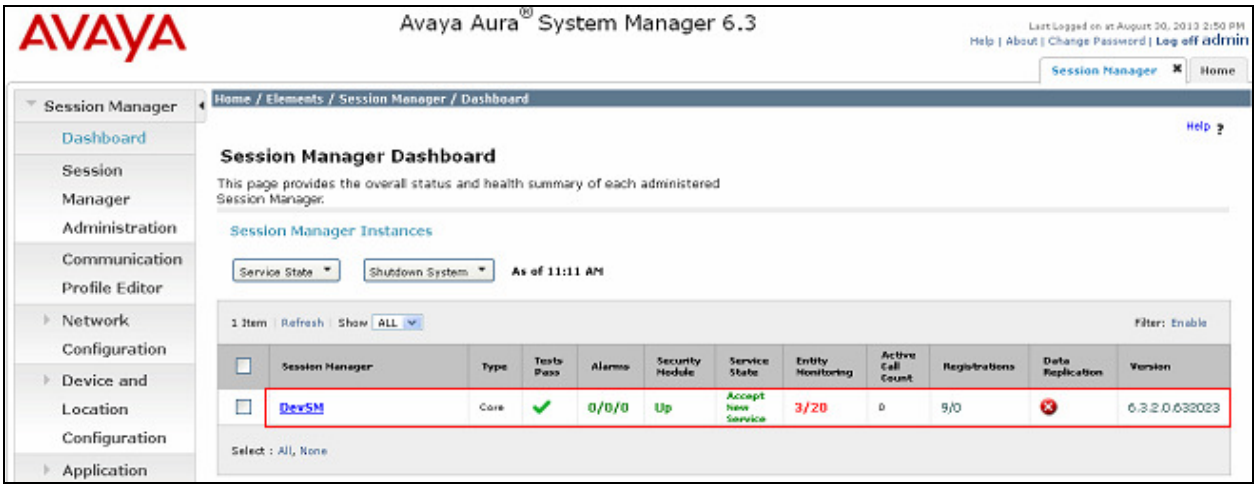
11.2. Verify Avaya Aura® Session Manager

11.2.1. Verify Avaya Aura® Session Manager is Operational

In System Manager's browser interface, navigate to **Elements → Session Manager → Dashboard** (not shown) to verify the overall system status for Session Manager.

Specifically, verify the status of the following fields as shown below:

- **Tests Pass:** ✔
- **Security Module:** Up
- **Service State:** Accept New Service

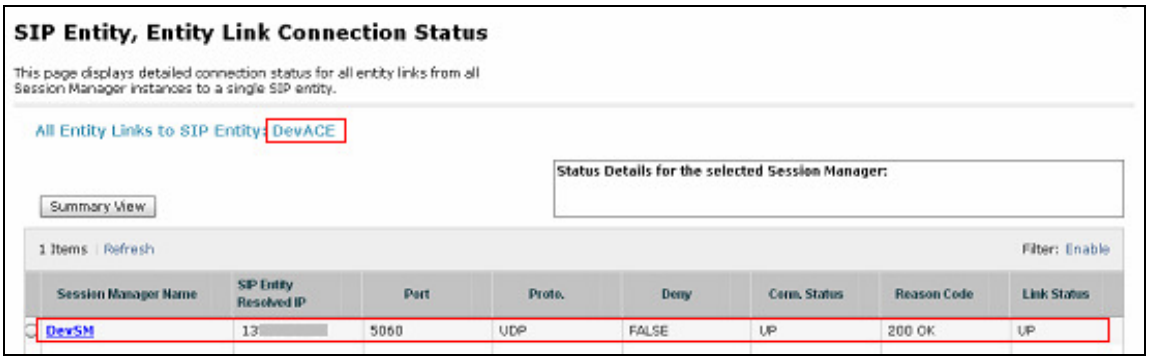


11.2.2. Verify SIP Entity Link Status

Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** (not shown) to view more detailed status information for one of the SIP Entity Links.

Select the SIP Entity for Avaya ACE from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

In the **All Entity Links to SIP Entity: DevACE** table, verify the **Conn. Status** for the link is "**Up**" as shown below.



Repeat the same step to verify the status of Enitity Links to Avaya Aura® Messaging and Avaya Aura® Communication Manager.

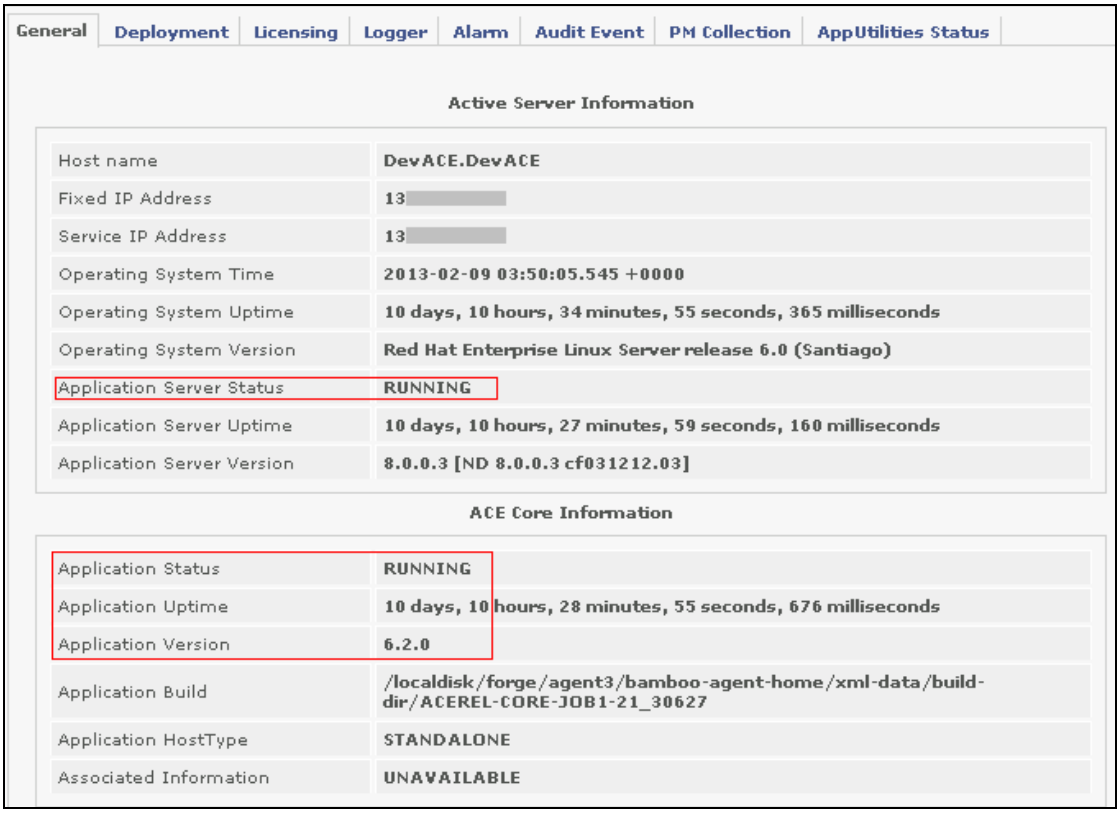
11.3. Verify Avaya ACE

11.3.1. Verify Service Provider Status

See the end of **Section 8.2** for verifying that all SIP Service Providers configured have the "In Service" status.

11.3.2. Verify Avaya ACE Server Status

In the Avaya ACE administrative web console, select **Configuration → Server** to verify Application Server Status and Application Status:



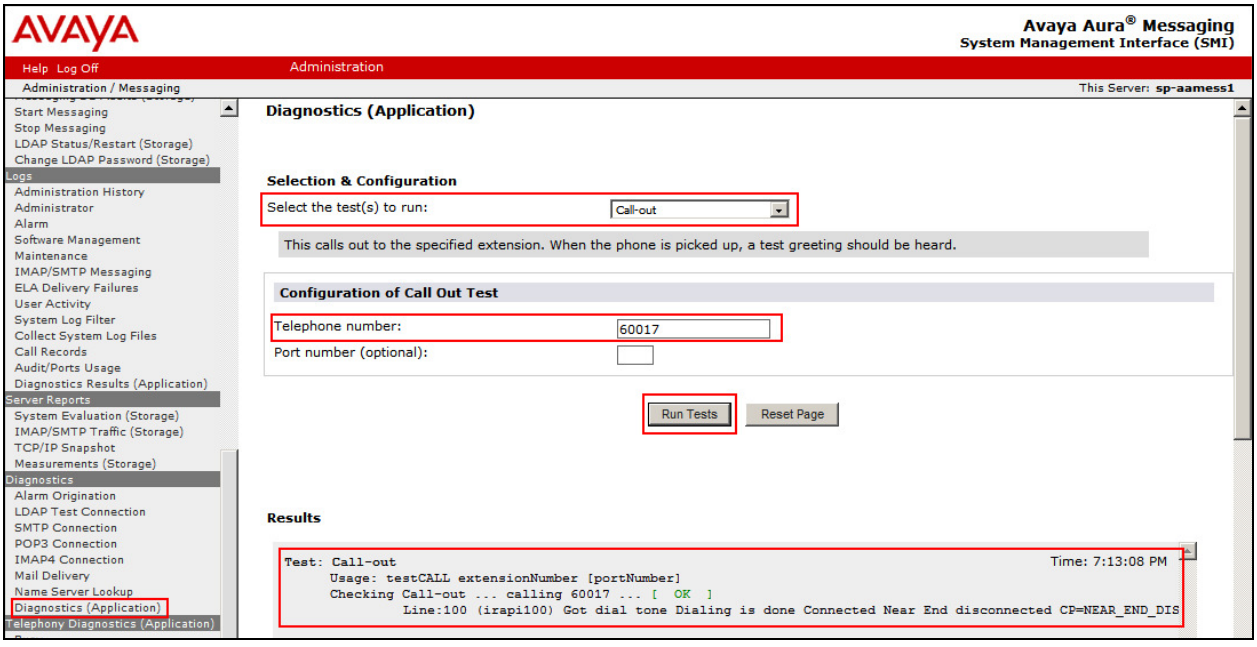
11.4. Verify Avaya Aura® Messaging

11.4.1.Verify Calls from Avaya Aura® Messaging

Test calls can be made from AAM to phones that are configured with mailboxes. To perform this test, select **Administration → Messaging** in the AAM administrative web console. In the left panel, under **Diagnostics** select **Diagnostics (Application)**. In the right panel fill in the following:

- **Select the test(s) to run:** Select **Call-out** from the drop down menu.
- **Telephone number:** Enter the number to call.

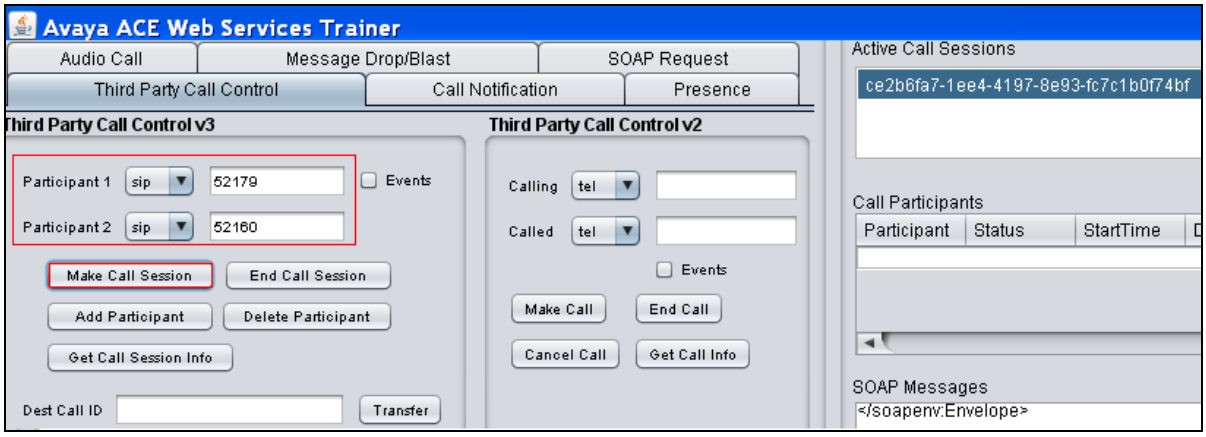
Click on **Run Tests** to start the test. The phone will ring and when answered a test message is played. The **Results** section of the page will update to indicate the call status as shown below.



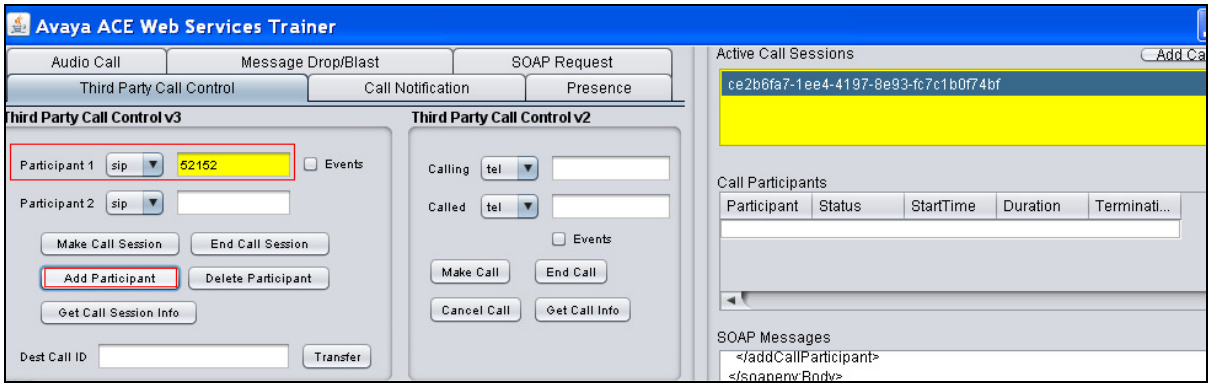
11.5. Verify Avaya Media Server

This section describes how to create conferece using Avaya ACE Web Service Trainer and to verify the session status on Media Server.

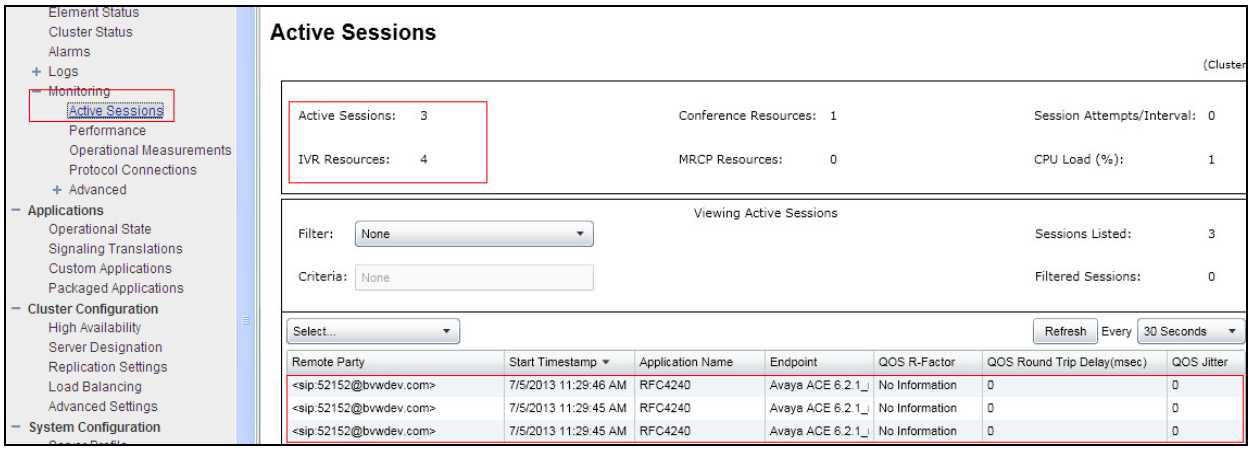
The screen below shows using Avaya ACE Web Service Trainer to start a conference session for. extensions 52179 and 52160.



The screen below shows using Avaya ACE Web Service Trainer to add extension 52152 to the conference.



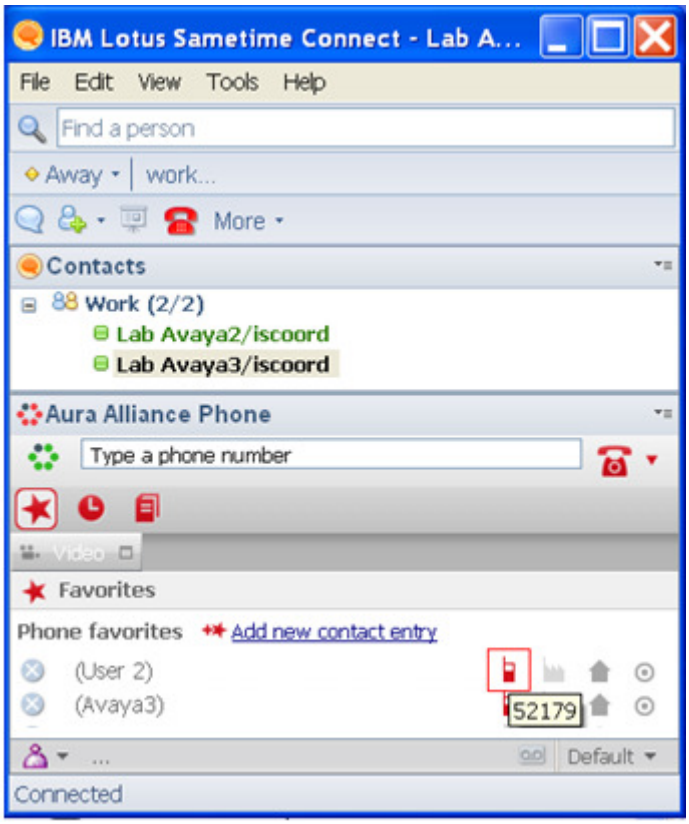
While the session is active, log into Avaya Media Server and navigate to **System Status → Monitoring → Active Session**. The details of active sessions are displayed.



11.6. Verify Aura® Alliance Phone.

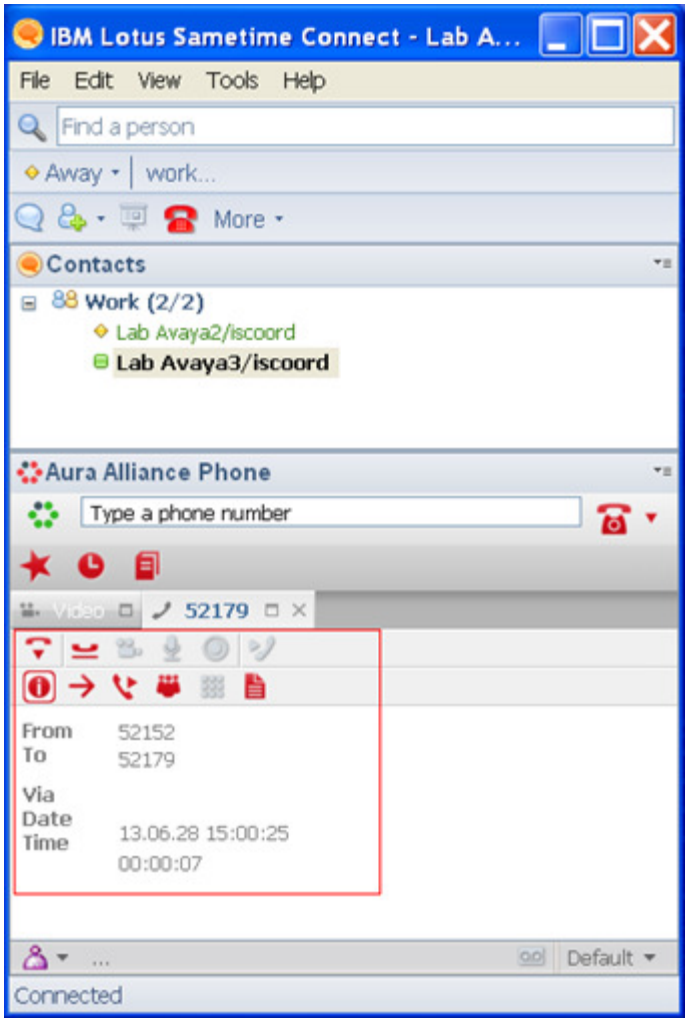
This section describes how to make an outgoing call using Aura® Alliance Phone.

Log into Aura® Alliance Phone as describe in **Section 10.2**. Aura® Alliance Phone can be used to call any valid extension in the system. The screen below shows clicking on the mobile icon of the User 2 to make a call to User 2.



If a user wants to call a Sametime contact (right mouseclick on a contact listed in the Sametime buddy list), then the phone number has to be defined in the user's contact profile in the Sametime settings – geographic location section

The calling and called devices ring for Users to pick up the device to answer the call. The 2 way voice path is established. A new tab of call information is added. The information tab provides information of the call, as well as others call fuctionalities such as Hang up, Hold, Unattended Transfer, Attended Transfer, Conference and add Note.



12. Conclusion

Interoperability testing of Avaya Aura® Agile Communication Environment VE 6.2.1, Avaya Aura® Messaging 6.1, Avaya Aura® Communication Manager 6.3 SP1 and Avaya Aura® Session Manager 6.3 with Aura® Alliance Phone v1.0.7 was successful. Obeservations are noted in **Section 2.2**.

13. Additional References

The following Avaya product documentation can be found at http://support.avaya.com

1. *Administering Avaya Aura® Communication Manager*, May 2013, Release 6.3, Document Number 03-300509.
2. *Administering Avaya Aura® Session Manager,* June 2013, Release 6.3
3. *Administering Avaya Aura® System Manager*, May 2013, Release 6.3.
4. *Avaya Agile Communication Environment™ Service Provider Administration* Release 6.2 NN10850-005, 10.01 November 2012
5. For information regarding security on Communication Manager, see *Avaya Aura Communication Manager Security Design* (03-601973).
6. For an alternate procedure to configure a signing authority as trusted on Avaya ACE, see *"Trusting a CA or self-signed certificate" in Avaya Agile Communication Environment™ User and Security Administration* (NN10850–010).

Following is a document provided by Aura® Alliance:

1. *Avaya plug-in documentation*

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.