Avaya Solution & Interoperability Test Lab

Application Notes for Aura Alliance Client SIP Softphone with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Session Manager 6.3 - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the Aura Alliance Client IBM® Notes® and IBM® Sametime® plugin to interoperate with Avaya Aura® Communication Manager 6.3, Avaya Aura® Messaging 6.2 and Avaya Aura® Session Manager 6.3.

The Aura Alliance Client is an IBM® Sametime® plug-in which works as a SIP endpoint. It provides telephony features to users of IBM Lotus Notes and offers SIP calling features.

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

Aura Alliance Client is a plug-in of IBM® Sametime® Connect. It provides two functionalities:

1. A SIP soft phone client which works together with IBM Lotus Sametime Connect, providing telephony features to users of IBM Lotus Notes and offers SIP calling features.

2. A CTI client to allow a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). Aura Alliance Client controls a physical telephone using Third Party Call (v3, v2/v2.4) and Call Notification web service of Avaya ACE 6.2.1VE.

This Application Note only describes the procedure for configuring Aura Alliance Client as a **SIP client** to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

A separate Application Note will describe how to configure Aura Alliance Client as a **CTI soft phone clien**t.

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 objective of the compliance testing performed on the AAC was to verify that it is compatible with Communication Manager and Session Manager. This includes verifying that the essential AAC features function properly when used with Communication Manager, and that Communication Manager Features are not hindered by the interaction with AAC.

2.2. Test Results

The following testing was covered successfully:

- Incoming call
- Outgoing call
- Call hold
- Call hold with consultation
- Unattended transfer
- Attended transfer
- Call forward unconditional
- Call forward busy and no answer

- 3-way conference
- Call waiting
- DTMF transmission
- Priority call
- Transfer to voice mail
- Last number dialed
- Send all calls

The following items were observed during testing:

- It is recommended that the user must not check "music on hold" or the call will be put on mute every time the user resumes the call from the hold status.
- In order to make a transfer call, the user must make sure the "Unattended transfer not supported" checkbox is checked.
- Direct Call Pickup feature is not supported with this solution.
- Aura Alliance Client SIP Softphone does not support update extension (CallerID) after a call had been transferred.

2.3. Support

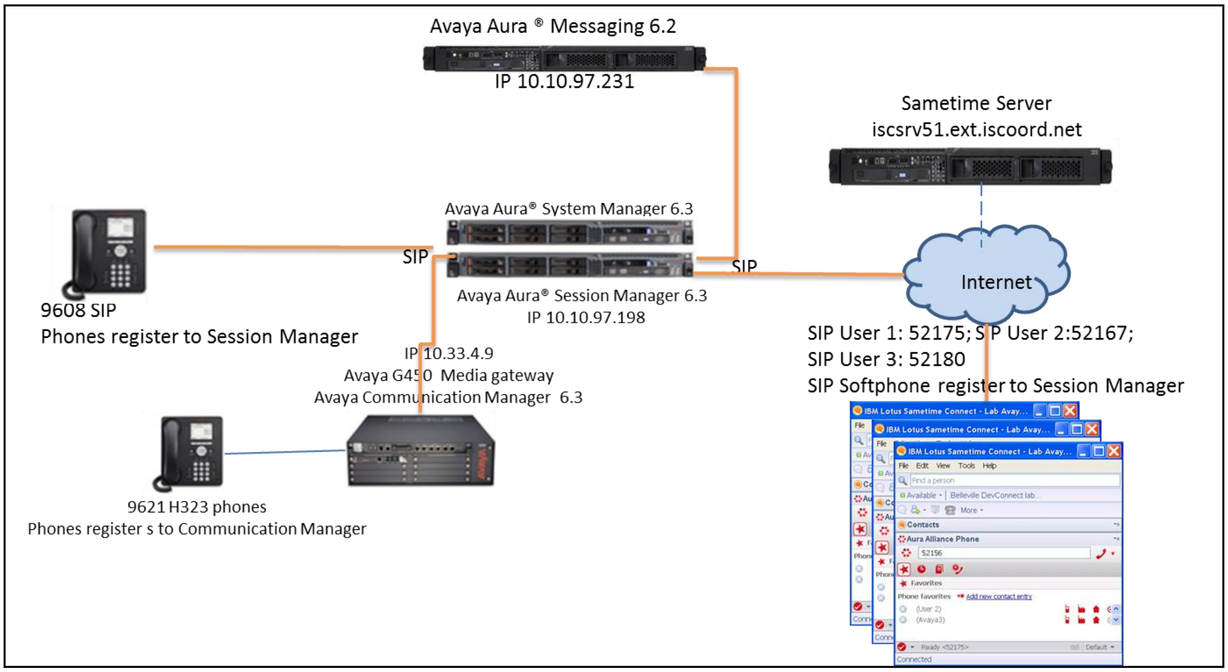
Technical support for Aura Alliance Client for IBM® Notes® and IBM® Sametime® can be obtained by contacting Aura Alliance:

- 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 deployment which includes a Session Manager and Communication Manager on S8300D Server with an Avaya G450 Media Gateway. Aura Alliance Client SIP Softphone registers to Session Manager as SIP end point.

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



Test Configuration of Aura Alliance Client SIP Softphone with Avaya Aura® systems

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 SP3
Avaya Aura® System Manager running on S8800 Server	Avaya Aura® System Manager 6.3.4
Avaya Aura® Session Manager running on S8800 Server	Avaya Aura® Session Manager 6.3SP4
Avaya Aura® Messaging running on S8800 Server	Avaya Aura® Messaging 6.2
Avaya 9621G H323 IP Desk phone	6.2.3
Avaya 9608 SIP Phone	6.2.2
Avaya 1416 Digital IP Desk phone	N/A
Aura Alliance Client SIP Softphone	1.0.9

5. Configure Avaya Aura® Communication Manager

It is assumed the general installation of Communication Manager on the Avaya G450 Media Gateway and the installation of Session Manager have been previously completed. It is also assumed that the SIP trunk connection between Communication Manager to Session Manager is already in place and operational. This section only describes the procedure for configuring feature access codes used for Aura Alliance Client SIP Softphone.

Communication Manager Configuration was performed using the Communication Manager System Access Terminal (SAT) interface. Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

Please note that in the sample screenshots listed below the “display” command was used instead of the “change” or “add” commands, this is because all necessary changes were already in place when the screenshots were taken.

5.1. Verify system-parameters customer-options

5.1.1. SIP Trunk capacity verification

Enter the **display system-parameters customer-options** command. Navigate to **page 2** and 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. Configure system-parameter features

Use the **change system-parameters features** command to configure the features required to support the Aura Alliance SIP Softphone. If the **Directed Call Pickup** feature is to be used by the SIP-phone, this feature must be set to "y".

```
display system-parameters features                              Page  19 of  20
                              FEATURE-RELATED SYSTEM PARAMETERS
IP PARAMETERS
                        Direct IP-IP Audio Connections? y
                                   IP Audio Hairpinning? n
                                Synchronization over IP? n

                         SIP Endpoint Managed Transfer? n

   Expand ISDN Numbers to International for 1XCES? n
CALL PICKUP
  Maximum Number of Digits for Directed Group Call Pickup: 4
                        Call Pickup on Intercom Calls? y     Call Pickup Alerting? n
      Temporary Bridged Appearance on Call Pickup? y       Directed Call Pickup? y
                           Extended Group Call Pickup: none
                        Enhanced Call Pickup Alerting? n


                              Display Information With Bridged Call? n
  Keep Bridged Information on Multiline Displays During Calls? y
                       PIN Checking for Private Calls? n
```

5.1.3. Configure Dial Plan

Use the command **change dialplan analysis 1** to create an entry in the dialplan analysis table. The following dialplan was used during compliance test.

- 399 – Messaging Pilot extension
- 521 – Endpoint extension in Communication Manager.
- *7 – Use for Feature access code.

```
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
   *7           4    fac      9            1    fac
   399          5    ext      *            4    dac
   521          5    ext
```

5.1.4. Configure Class of Restriction

Use the **change cor** command to configure Class of Restriction (COR) 1 with parameters required to use the call pickup feature of the AAC SIP Softphone.

- **Can Be Picked Up By Directed Call Pickup?**: Enter “y” to allow calls to stations assigned to this COR to be answered via directed call pickup.
- **Use Directed Call Pickup?:** Enter “y” to allow the stations assigned to this COR to answer other telephones via directed call pickup.

```
display cor 1                                               Page   1 of  23
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description:

                      FRL: 0                                APLT? y
  Can Be Service Observed? n           Calling Party Restriction: none
Can Be A Service Observer? n            Called Party Restriction: none
        Time of Day Chart: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

            Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7            Hear VDN of Origin Annc.? n
         Send ANI for MFE? n             Add/Remove Agent Skills? n
            MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? n   PASTE (Display PBX Data on Phone)? n
                        Can Be Picked Up By Directed Call Pickup? y
                                    Can Use Directed Call Pickup? y
                                    Group Controlled Restriction: inactive
```

5.1.5. Configure Access to Extended Features

Use the **change feature-access-codes** command to assign unused feature codes to those features used by the AAC SIP Softphone, as shown in the following screens. Note the "*7" entry for the dial plan shown is used by these entries.

Call Forward Activation access codes:

```
display feature-access-codes                                    Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
             Automatic Callback Activation:            Deactivation:
Call Forwarding Activation Busy/DA: *712   All: *713   Deactivation: *714
   Call Forwarding Enhanced Status: *715   Act: *716   Deactivation: *717
                         Call Park Access Code: *718
                       Call Pickup Access Code: *719
CAS Remote Hold/Answer Hold-Unhold Access Code: *720
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code: *723
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code: *724     Close Code: *725
```

Direct Call Pickup, Last Number Dialed access code:

```
display feature-access-codes                                    Page   2 of  10
                               FEATURE ACCESS CODE (FAC)
                   Contact Closure  Pulse Code: *726

                  Data Origination Access Code: *727
                      Data Privacy Access Code: *728
              Directed Call Pickup Access Code: *729
       Directed Group Call Pickup  Access Code: *730
     Emergency Access to Attendant Access Code: *731
        EC500 Self-Administration Access Codes: *732
                     Enhanced EC500 Activation: *733   Deactivation: *734
           Enterprise Mobility User Activation: *735   Deactivation: *736
 Extended Call Fwd Activate Busy D/A *737 All: *738   Deactivation: *739
        Extended Group Call Pickup Access Code:
               Facility Test Calls Access Code: *741
                             Flash Access Code: *742
             Group Control Restrict Activation: *743   Deactivation: *744
                    Hunt Group Busy Activation: *745   Deactivation: *746
                              ISDN Access Code:
               Last Number Dialed Access Code: *748
     Leave Word Calling Message Retrieval Lock: *749
   Leave Word Calling Message Retrieval Unlock: *750
```

Priority Calling access code, **Send All Calls Activation**:

```
display feature-access-codes                                    Page   3 of  10
                               FEATURE ACCESS CODE (FAC)
                 Leave Word Calling Send A Message: *751
               Leave Word Calling Cancel A Message: *752
       Limit Number of Concurrent Calls Activation: *753   Deactivation: *754
                   Malicious Call Trace Activation:        Deactivation:
             Meet-me Conference Access Code Change: *757
              Message Sequence Trace (MST) Disable:

     PASTE (Display PBX data on Phone) Access Code: *758
      Personal Station Access (PSA) Associate Code:        Dissociate Code:
            Per Call CPN Blocking Code Access Code: *761
          Per Call CPN Unblocking Code Access Code: *762
                      Posted Messages Activation:          Deactivation:
                    Priority Calling Access Code: *763
                             Program Access Code: *764

           Refresh Terminal Parameters Access Code: *765
                  Remote Send All Calls Activation: *766   Deactivation: *767
                   Self Station Display Activation:
                        Send All Calls Activation: *769    Deactivation: *770
            Station Firmware Download Access Code: *771
```

Transfer to Voice Mail access code:

```
display feature-access-codes                                    Page   4 of  10
                               FEATURE ACCESS CODE (FAC)
                             Station Lock Activation: *772 Deactivation: *773
            Station Security Code Change Access Code: *774
                    Station User Admin of FBI Assign:      Remove:
        Station User Button Ring Control Access Code:
                   Terminal Dial-Up Test Access Code: *778
      Terminal Translation Initialization Merge Code:      Separation Code:
                  Transfer to Voice Mail Access Code: *781
                Trunk Answer Any Station Access Code: *782
                    User Control Restrict Activation: *783 Deactivation: *784
        Voice Coverage Message Retrieval Access Code: *785
       Voice Principal Message Retrieval Access Code: *786
                 Whisper Page Activation Access Code: *787
           3PCC H323 Override SIP Station Activation:      Deactivation:

          PIN Checking for Private Calls Access Code:
PIN Checking for Private Calls Using ARS Access Code:
PIN Checking for Private Calls Using AAR Access Code:
```

Use the **change off-pbx-telephone feature-name-extensions** command to assign extensions to features required by SIP telephones. Note that the extensions used here are assigned to speed dial entries for AAC SIP Softphone and the extensions will vary depending on the enterprise dialing plan. Below is example used during compliance test.

```
display off-pbx-telephone feature-name-extensions set 1       Page   1 of   2
     EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME
                     Set Name:

        Active Appearance Select:
             Automatic Call Back:
       Automatic Call-Back Cancel:
                Call Forward All: 52181
      Call Forward Busy/No Answer: 52182
             Call Forward Cancel: 52183
                        Call Park:
            Call Park Answer Back:
                     Call Pick-Up:
             Calling Number Block:
           Calling Number Unblock:
   Conditional Call Extend Enable:
  Conditional Call Extend Disable:
             Conference Complete:
            Conference on Answer:
            Directed Call Pick-Up: 52184
            Drop Last Added Party:
```

Page 2

```
display off-pbx-telephone feature-name-extensions set 1       Page   2 of   2
     EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME

       Exclusion (Toggle On/Off):
      Extended Group Call Pickup:
          Held Appearance Select:
          Idle Appearance Select:
              Last Number Dialed: 52185
            Malicious Call Trace:
     Malicious Call Trace Cancel:
             Off-Pbx Call Enable:
            Off-Pbx Call Disable:
                   Priority Call: 52186
                          Recall:
                  Send All Calls: 52187
           Send All Calls Cancel: 52188
               Transfer Complete:
              Transfer On Hang-Up:
          Transfer to Voice Mail: 52189
         Whisper Page Activation:
```

5.1.6. Configure Hunt Group for Avaya Aura® Messaging

This section describes the steps for 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.

```
display 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 Messaging.
- **Voice Mail Handle –**Enter the Voice Mail Handle which is the extension of Messaging.
- **Routing Digit (e.g. AAR/ARS Access Code)** – Enter the AAR Access Code as defined in the Feature Access Code form.

```
display 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
```

5.1.7. Configure Coverage Path to Avaya Aura® Messaging

This section describes the steps for 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**, which is created in the previous section. The default values for the other fields may be used.

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

                   Coverage Path Number: 1
     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:
```

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

Configure a phone that has a mailbox on the messaging server for call coverage. Use the command **change station xyz** and on **Page 1** for **Coverage Path 1** use the configured coverage path. In the example below station 52155 was configured to cover to messaging using cover path 2.

```
display station 52175                                             Page   1 of   5
                                     STATION

Extension: 52175                       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: 52155
            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 52175                                            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: 52175         Always Use? n IP Audio Hairpinning? n
```

6. Configure Avaya Aura® Session Manager

6.1. Add a SIP User

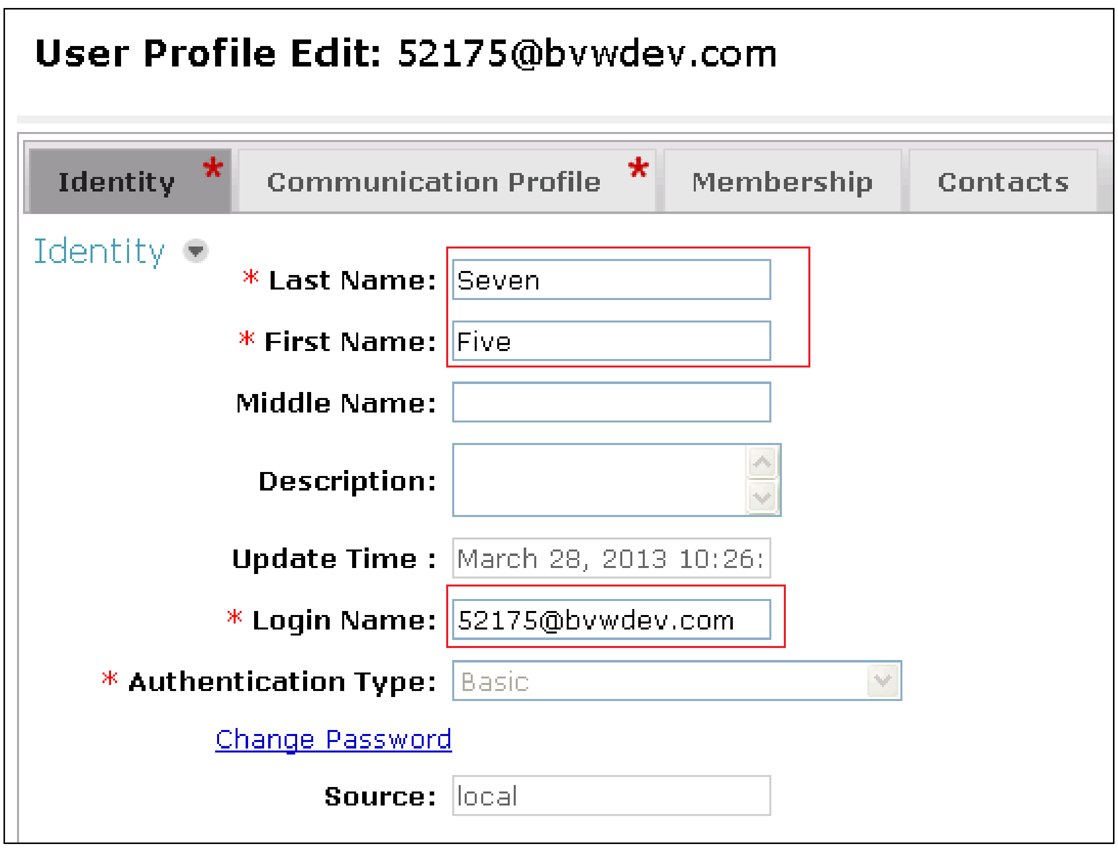
The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms. It also assumes that all SIP configurations have already been defined as part of the initial Session Manager installation. This includes items such as SIP domains, locations, SIP entities, Routing, Dial Pattern and Session Manager itself.

This section will describe the steps on how to create a SIP user for the Aura Alliance SIP Softphone. Please note that the sample screenshots may differ slightly from the text as the user was already created and in place when the screenshots were taken.

Login System Manager, to add new SIP users, navigate to **Users → Manage Users**. Click **New** (not shown)**,** in the **Identity** tab, provide the following information:

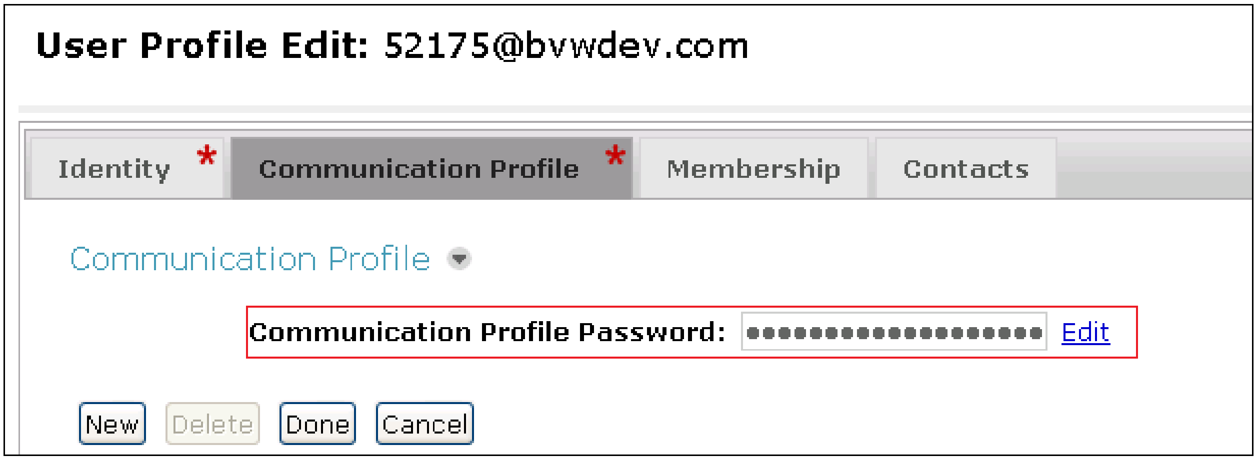
- **Last Name –** Enter last name of user.
- **First Name –** Enter first name of user.
- **Login Name** – Enter extension and domain name used in the system.
- **Authentication Type** – Default is **Basic**. Use this default value.
- **Password** – Enter password, this is used to log into System Manager.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

Below is the display detail of a SIP User Identity created during compliance test.



In the **Communication Profile** tab, under Communication Profile section:

- **Communication Profile Password** – enter a numeric password which is used to log into the device.



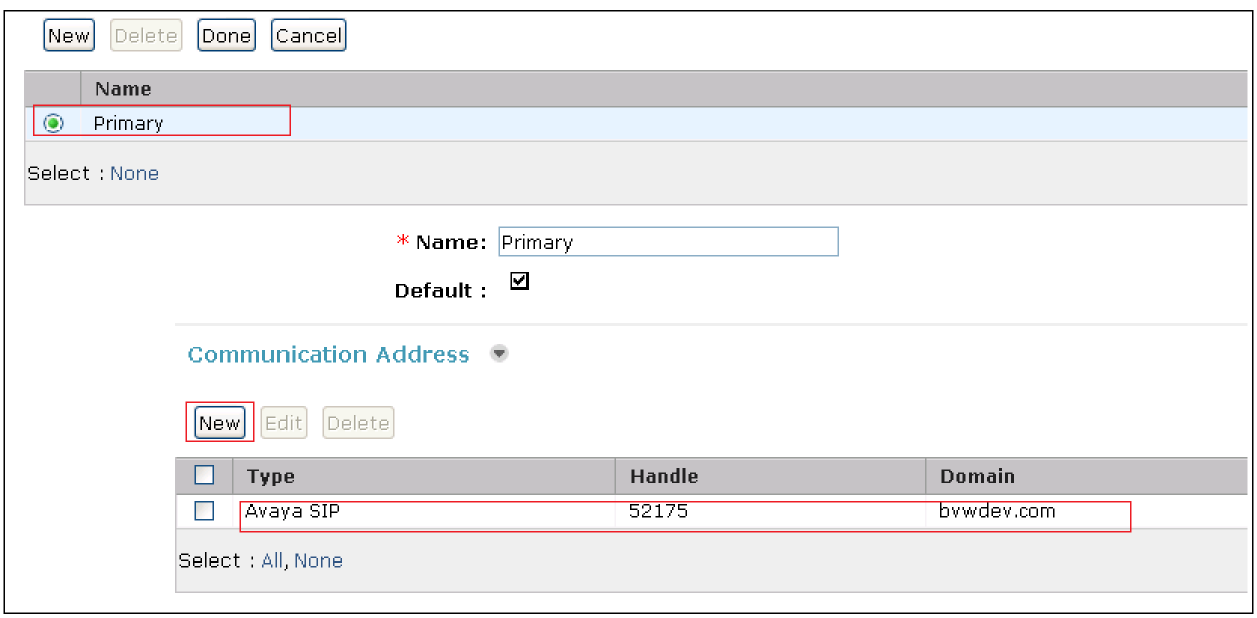
Verify there is a default entry identified as the **Primary** profile for the new SIP user. If an entry does not exist, select **New** and enter values for the following required attributes:

- **Name** – Enter **Primary**.
- **Default** – Enter ☑

In the **Communication Address** sub-section, select **New** to define a **Communication Address** for the new SIP user, and provide the following information.

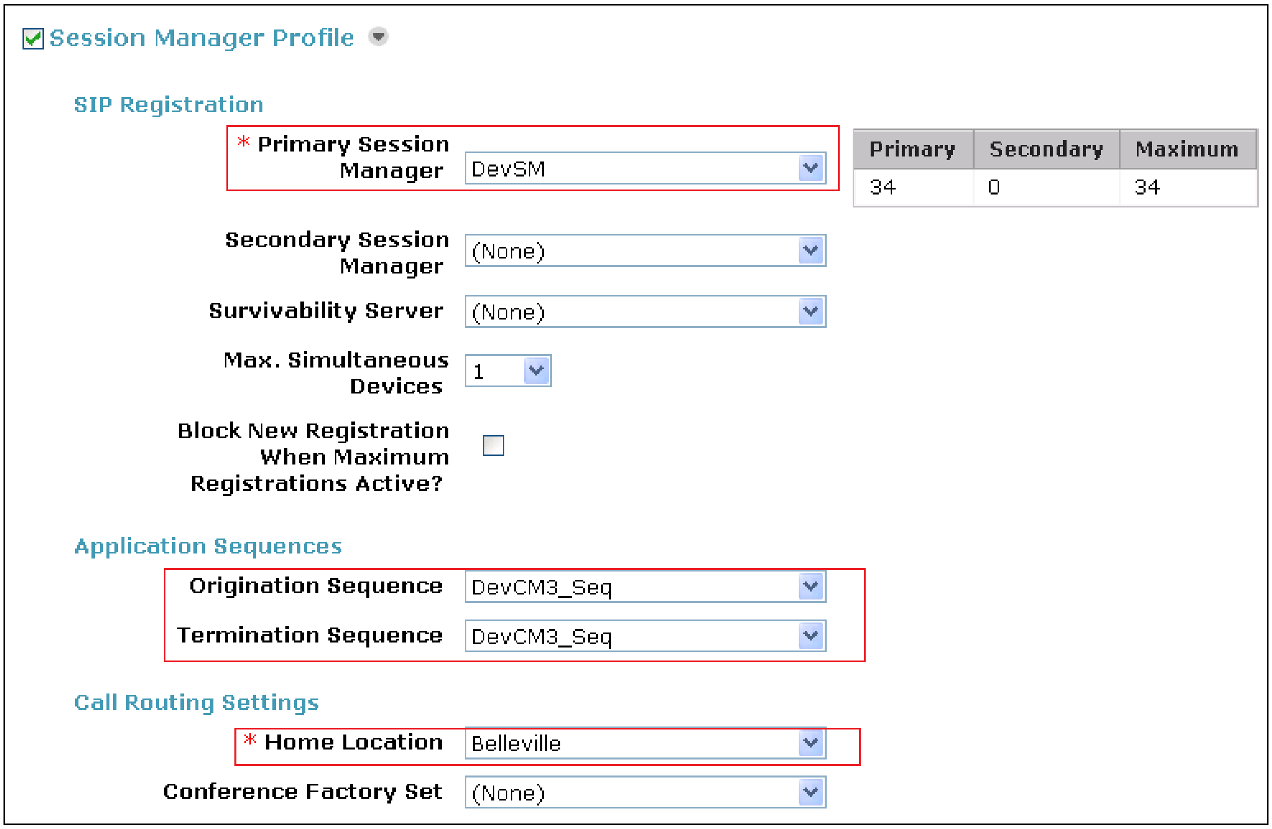
- **Type** – Select **Avaya SIP** from drop-down menu.
- **Fully Qualified Address** – Enter same extension number and domain used for Login Name, created previously.

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



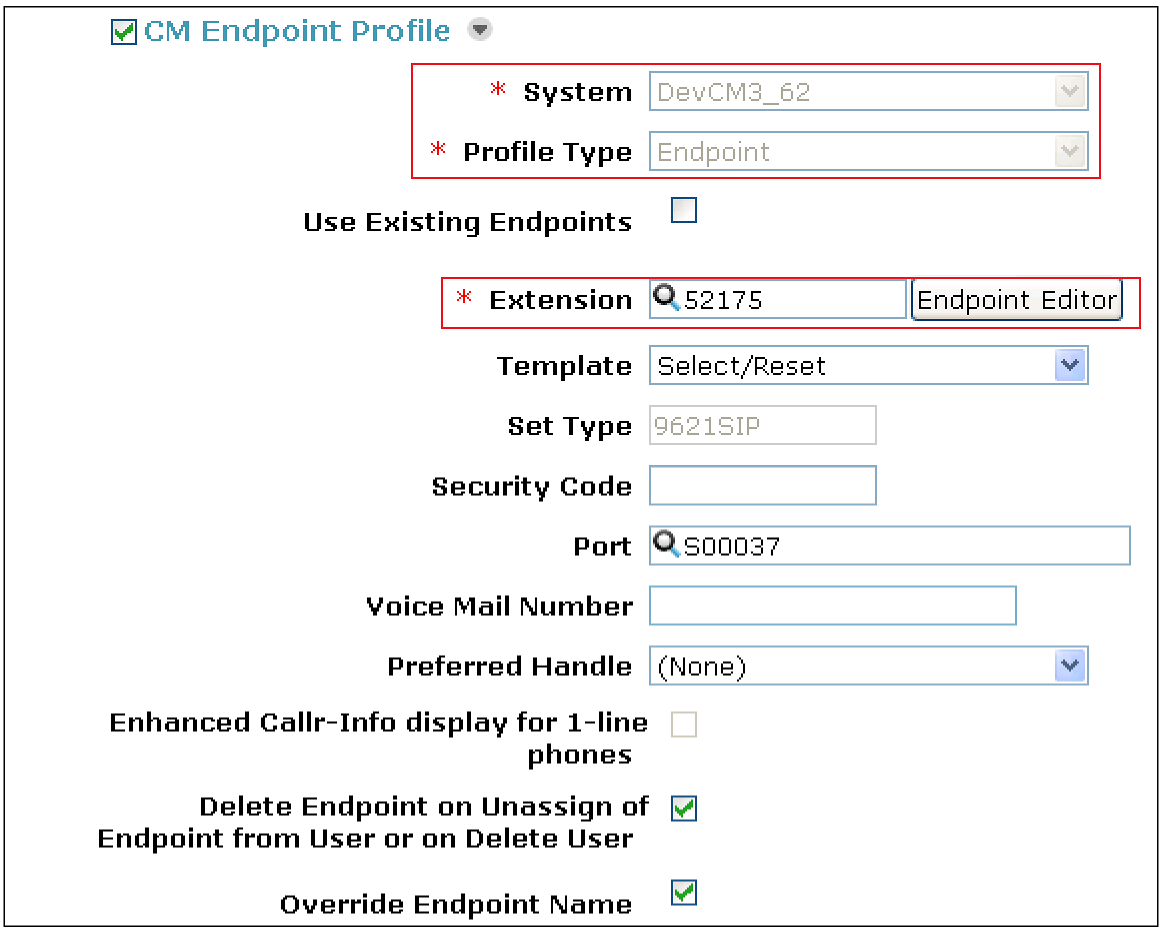
In Session Manager Profile sub-section, enter the following:

- **Primary Session Manager** – Select the required Session Manager.
- **Origination Application Sequence –** Select Application Sequence for Communication Manager.
- **Termination Application Sequence** – Select Application Sequence for Communication Manager.
- **Home Location** – Select the required Location.



In **CM Endpoint Profile** sub-section, enter the following information:

- **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.



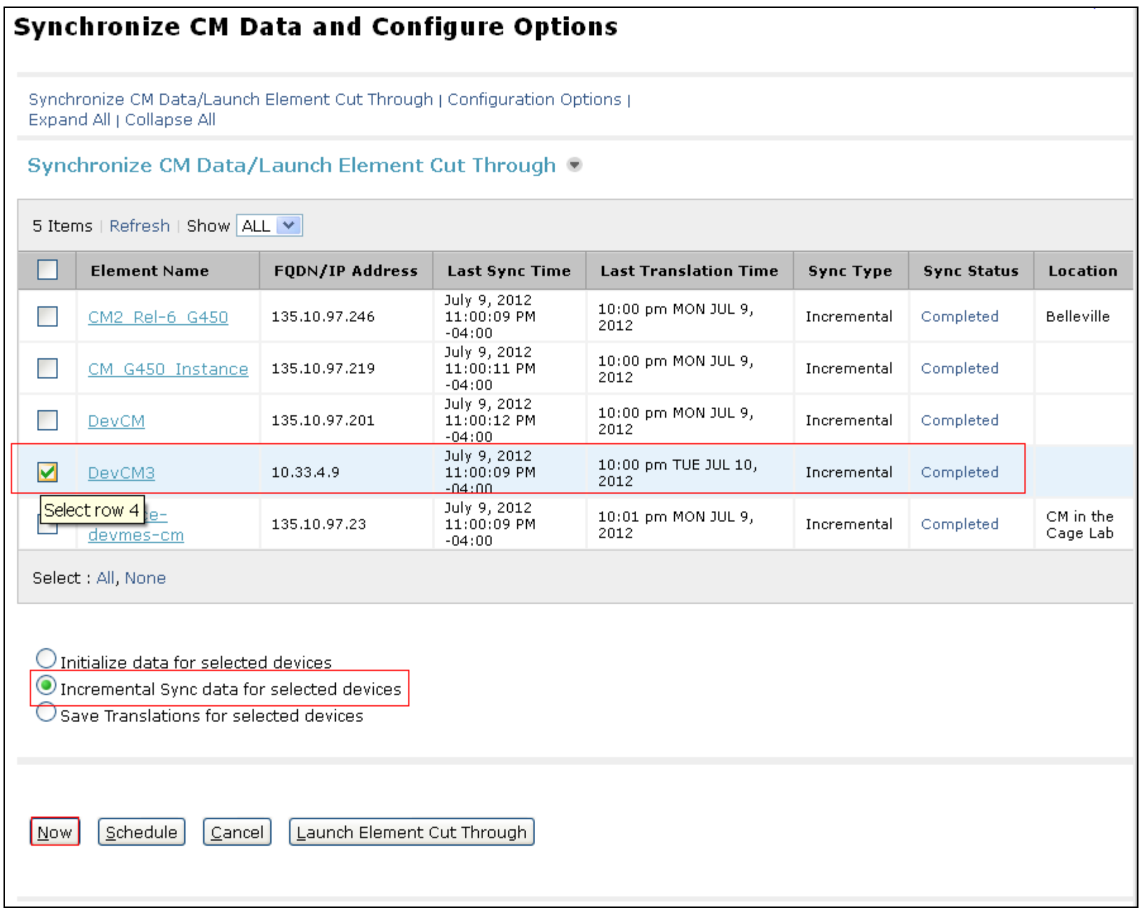
Click **Commit** to save definition of the new user.

6.2. Synchronization Changes with Avaya Aura® Communication Manager

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

On the **Synchronize CM Data and Configure Options** page, expand the Synchronize CM Data/Launch Element Cut Through table.

- 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 successfully completes by verifying the status in the **Sync. Status** column shows **Completed**.

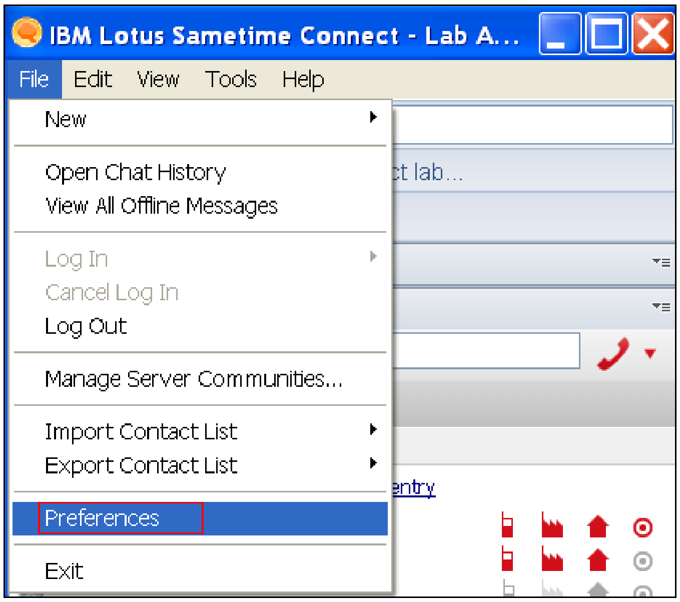


7. Configure Aura Alliance Client SIP Softphone

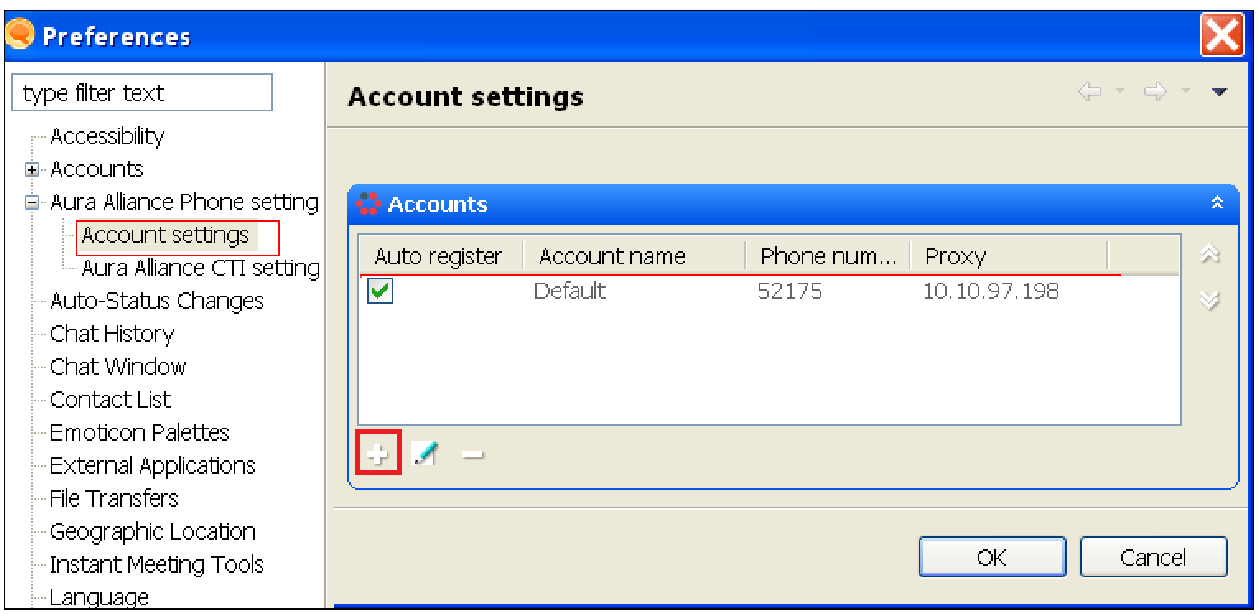
Aura Alliance installs, configures, and customizes the IBM Lotus Same Time Server for their customers. Thus, this section only describes the interface configuration, so that the Aura Alliance Client SIP Softphone can register to Session Manager and make call.

7.1. Add SIP user account

Select **File → Preferences** to open account setting for SIP user account.

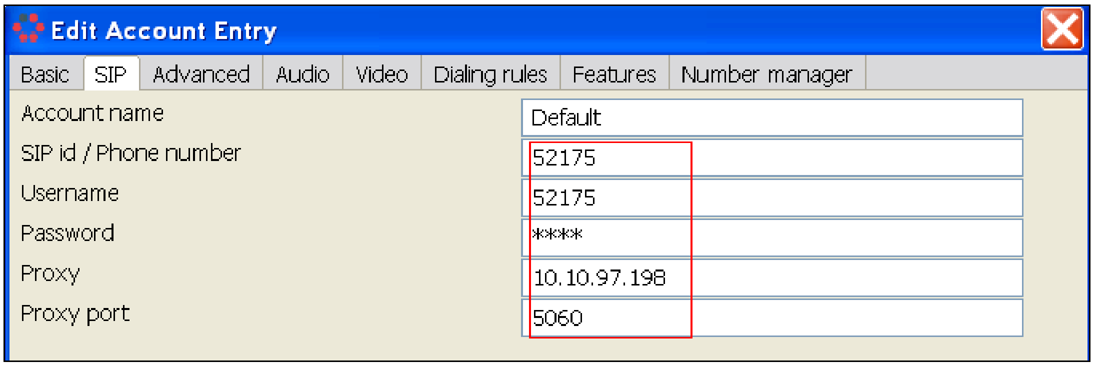


Select **Account settings**, click on "+" to add new account. During compliance test the **52175** account is added as shown.



In the **Edit Account Entry** account detail window, click on **SIP** tab to enter information for SIP account.

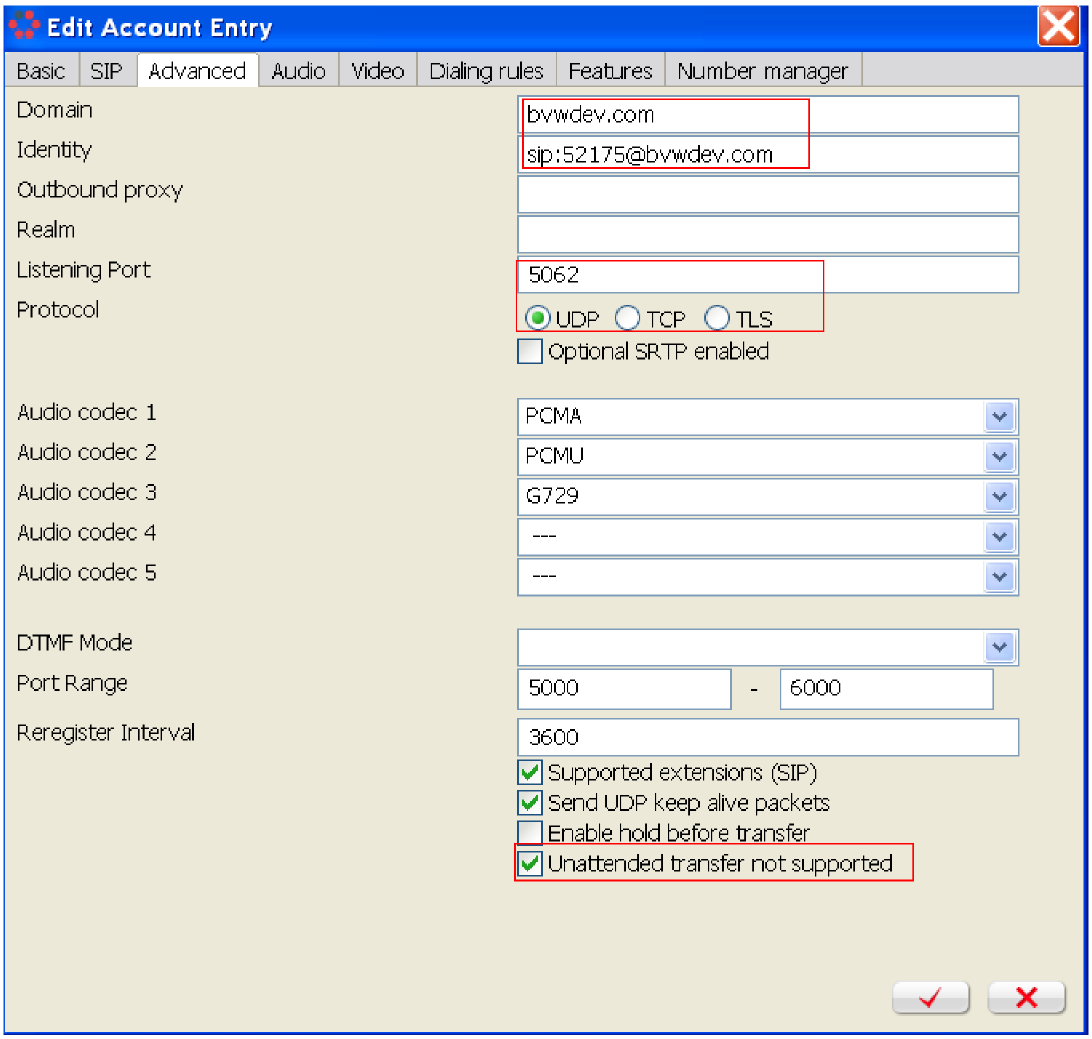
- **SIP id / Phone number**: enter SIP extension that was created in **Section 6.1**
- **Username**: enter a SIP user name.
- **Password**: enter a SIP user password.
- **Proxy**: enter the signalling IP address of Session Manager
- **Proxy port**: leave default port as **5060**.



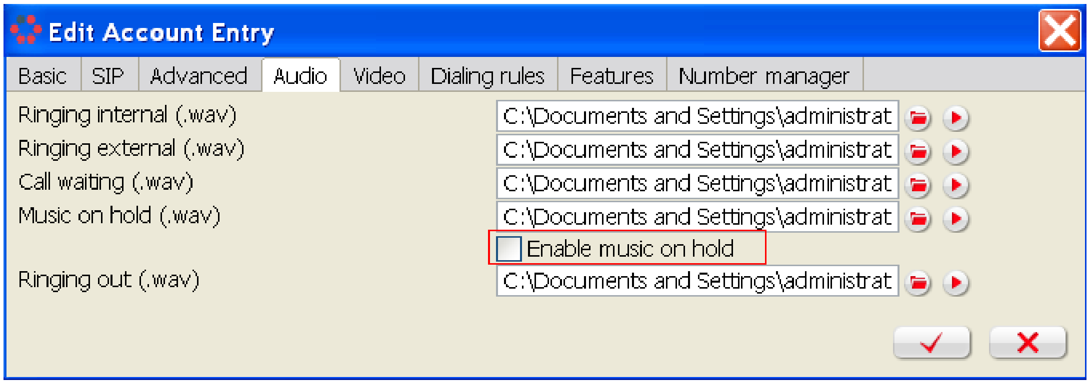
In the **Advanced** tab, enter the following info as shown below figure and leave other fields values as default:

- **Domain**: enter the domain name setup on System Manager.
- **Indentity**: enter SIP user identity.
- **Listening Port**: 5062.
- **Protocal**: select UDP.
- **Unattended transfer not supported**: make sure the checkbox is checked.

The figure below shows details of the SIP User used during compliance test:

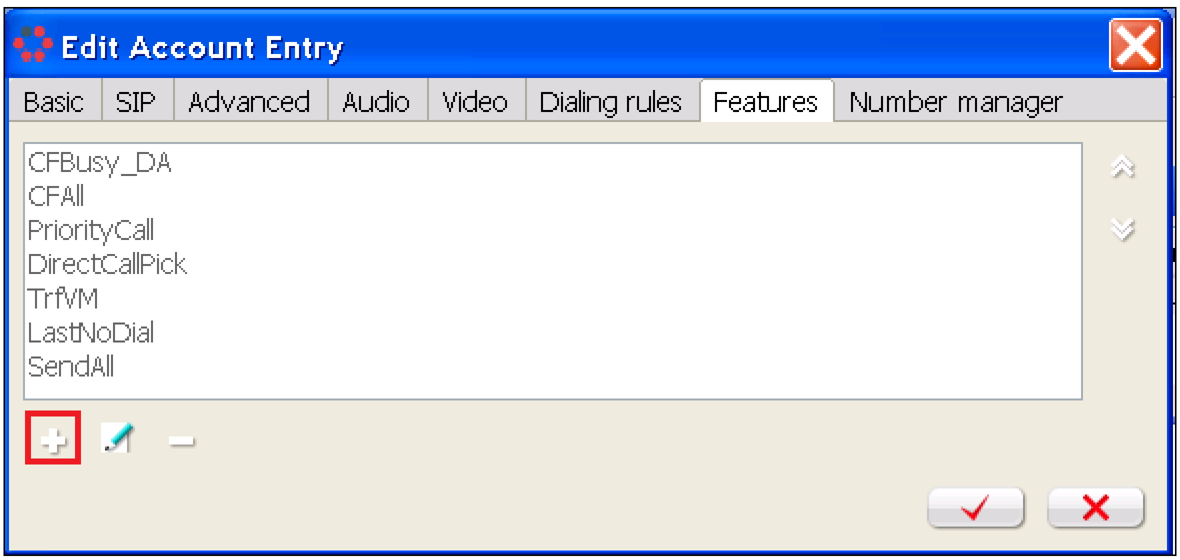


In the **Audio** tab, make sure uncheck the **Enable music on hold** checkbox. Click OK to save changes.



7.2. Configure Features

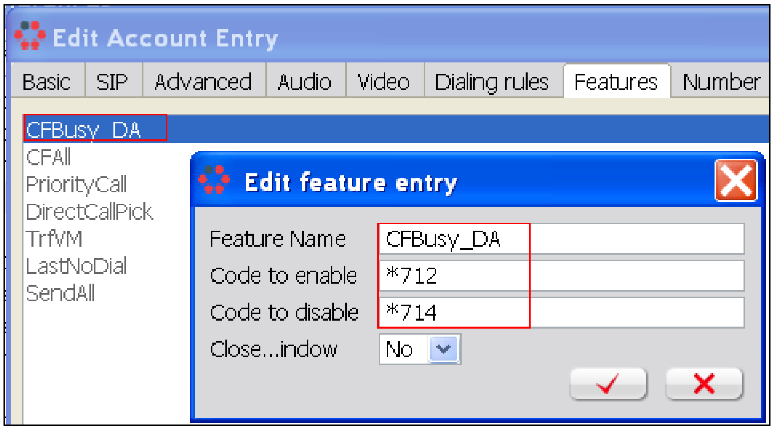
In **Edit Account Entry** window, select **Features** tab then click on "+" to add New Feature.



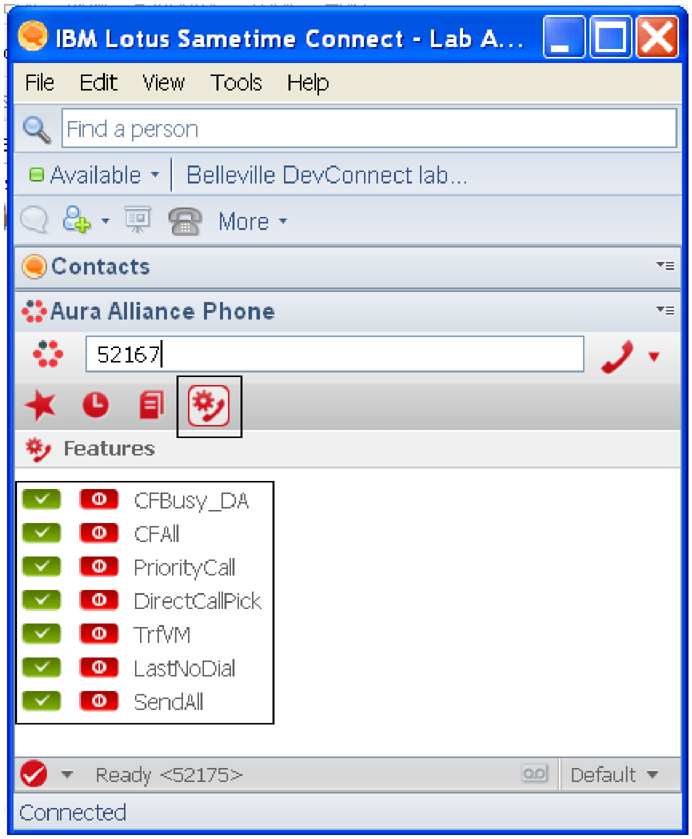
In the Edit feature entry, enter the following information:

- **Feature Name**: enter the name of the feature, example Call Forward Busy – Do not answer(CFBusy_DA)
- **Code to enable**: enter the extensions created in **Section 5.1.5**
- **Code to disable**: enter the extension created in **Section 5.1.5** to deactivate the feature. For those features for which there is no "OFF" condition to be defined, i.e. "Priority Call", this field can be left blank.

Click OK to save.



After this is done a green"ON" button icon and a red "OFF" button icon will appear in the call window which allows these features to be turned on or off. For those features for which there is no "OFF" state, i.e., "Priority Call", the "OFF" button can be ignored.

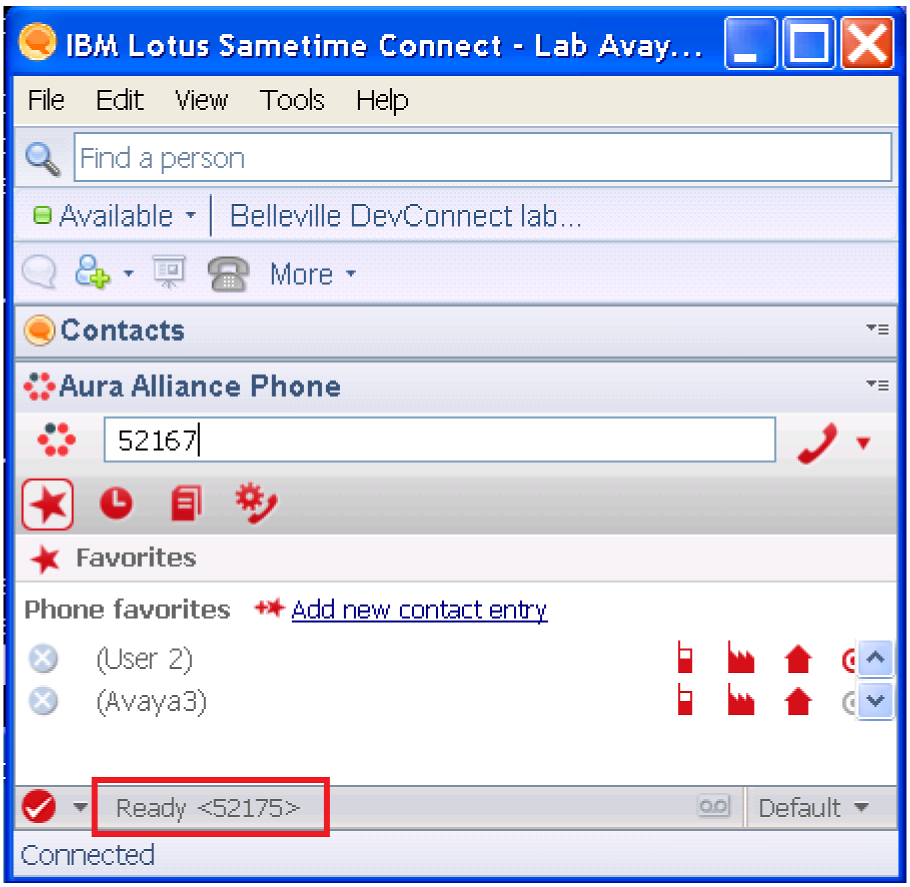


8. Verification Steps

This section provides details on tests that can be performed to verify proper configuration of Communication Manager, Session Manager and Aura Alliance Client SIP Softphone.

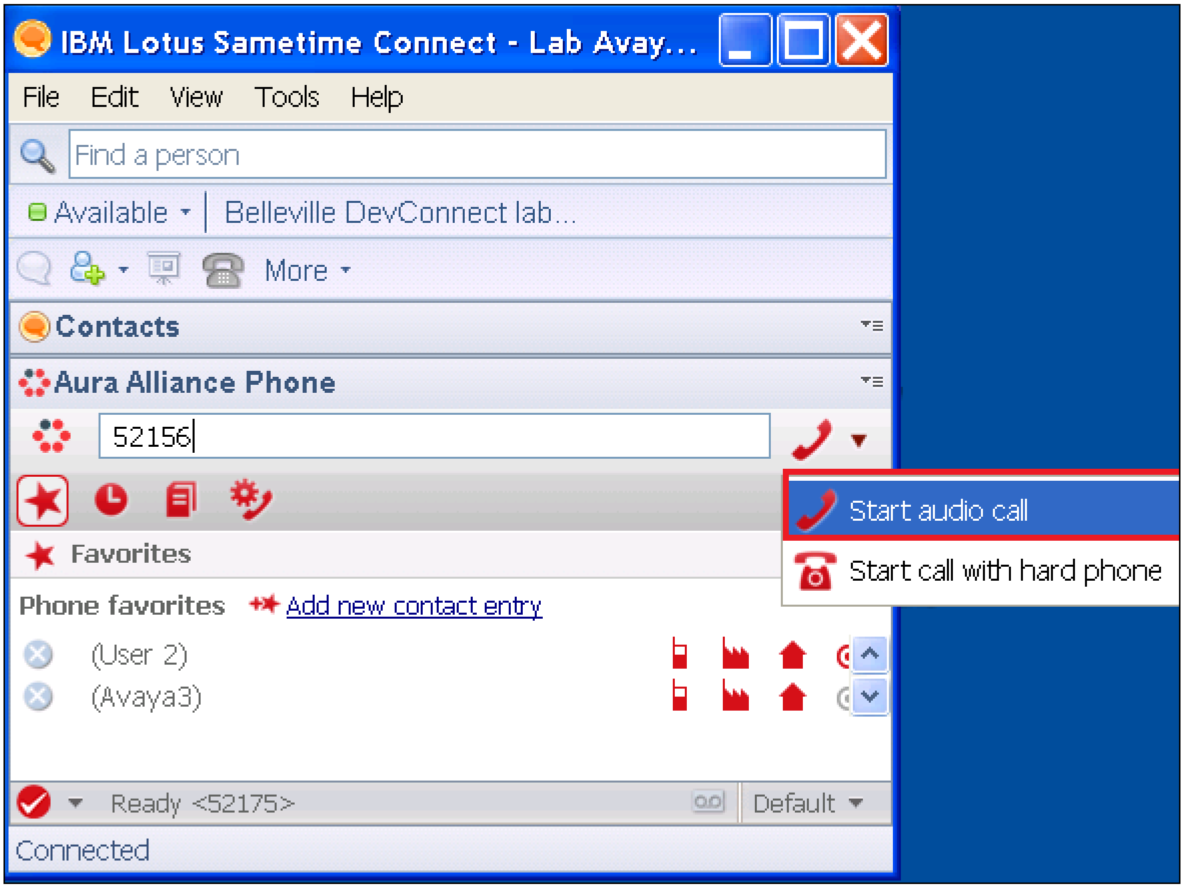
8.1. Verify user can register Aura Alliance Client SIP Softphone to Avaya Aura® Session Manager

Verify at the left bottom of the softphone window if the SIP user successfully logged in, the status should show **Ready** <extension> as shown below: SIP user 52175 is successfully logged in and registered to Session Manager.

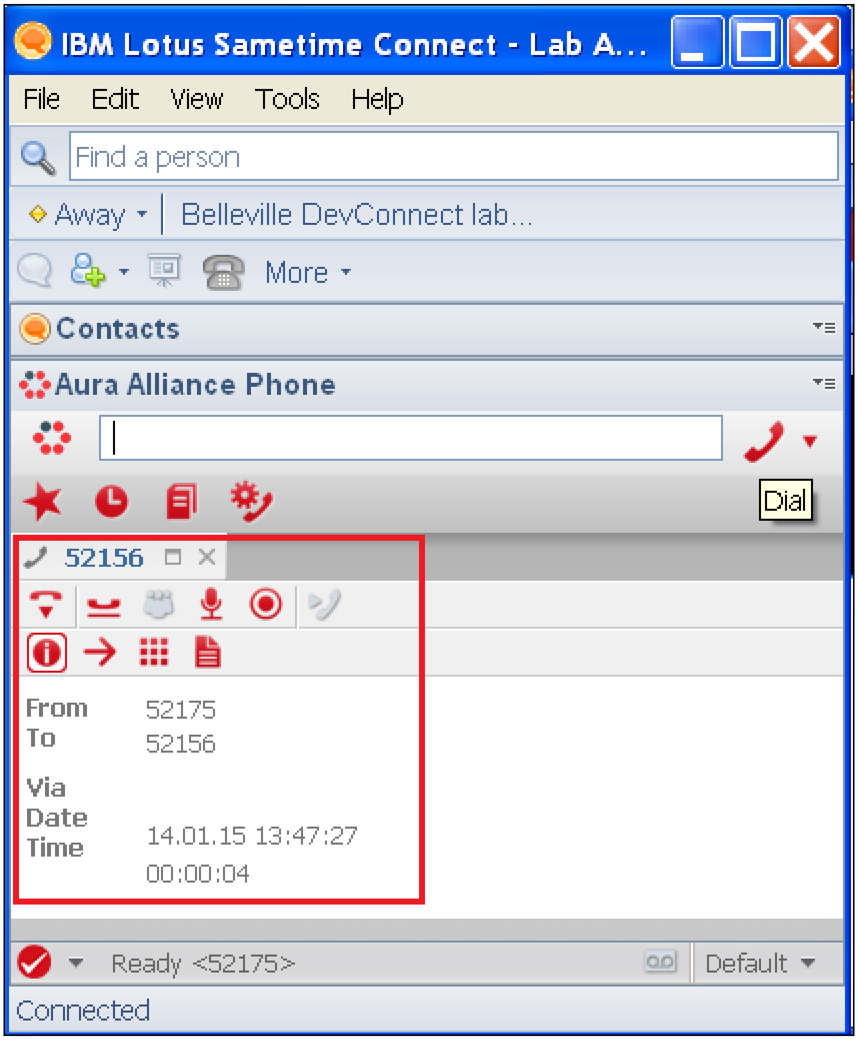


8.2. Verify user can make a call using Aura Alliance Client SIP Softphone

Once user is successfully logged in, a user will be able to enter the number and select **Start audio call** from softphone as shown below.

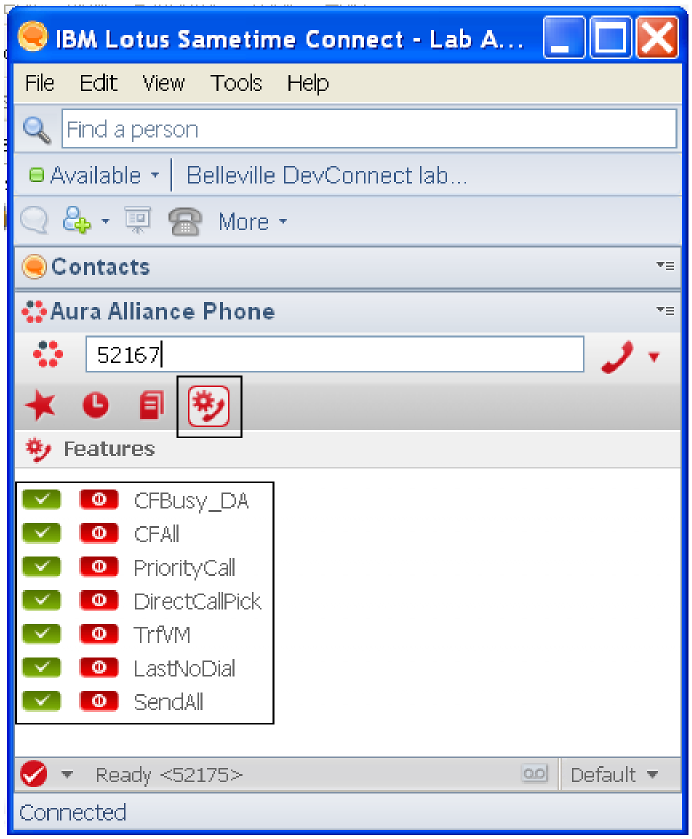


When the call is connected the call information is display as shown below:



8.2.1. Verify user can launch feature call

Click on the Features icon to launch list of available features. Turn on selected feature, for example Call Forward All (**CFAll**) by clicking on the green button, listen to the tone then enter the extension to forward the call to, once confirmed the call information window of this feature setup is closed. Make a call to this extension. Verify that the call is forwarded to the correct extension. Cancel the forward feature by clicking on the red button (**CFAll**). For those features for which there is no "OFF" state, i.e., "Priority Call", the "OFF" button can be ignored.



9. Conclusion

Interoperability testing of Avaya Aura® Communication Manager 6.3 and Avaya Aura® Session Manager with Aura Alliance Client SIP Softphone was completed and passed. Observations are noted in **Section 2.2**.

10. 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.

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.