Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the ESNA Officelinx iLink Pro 9.1 with Avaya Aura® Agile Communication Environment VE 6.2.1 FP2, Avaya Aura® Messaging 6.2 and Avaya Aura® Communication Manager 6.3 - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the ESNA Officelinx iLink Pro 9.1 SP1, Avaya Agile Communication Environment 6.2 FP2, Avaya Aura® Communication Manager 6.3 and Avaya Aura® Messaging 6.2. iLink Pro is an application that allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). iLink Pro controls a physical telephone using Third Party Call Control (v2 and v2.4), Call Notification web service of Avaya Agile Communication Environment 6.2.1 FP2.

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.

Contents

1. Introduction

These Application Notes describe the procedure for configuring ESNA Telephony Officelinx to successfully interoperate with Avaya Aura® Agile Communication Environment (ACE), Avaya Aura® Communication Manager and Avaya Aura® Messaging solutions.

iLink Pro is Google Application made by ESNA that allows a user to operate a physical telephone and view call and telephone display information through Chrome browser. iLink Pro controls a physical telephone using third-party call control, specifically the third party call (v2 and v2.4), call notification web service of Avaya Aura® Agile Communication Environment. Also, there is a flashing on message tab on iLink Pro to indicate there is a message waiting on Avaya Aura® Messaging.

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 ESNA Officelinx with Avaya H323 and SIP desk phones. Phone operations such as off-hook, on-hook, dialing, answering, etc., was performed using both the physical phones and iLink Pro. In addition, phone displays and call states on the physical phones and iLink Pro was verified for consistency. The following testing was covered successfully:

1. Click and call on iLink Pro and the voice path is established on 2 physical phones.
2. Put a call on hold and retrieve call.
3. Transfer a call.
4. Retrieve the voice message in Google Mail (SMTP replay).
5. Verify Message Waiting Indication (MWI).
6. G.711MU and G.711A codec.
7. Send and receive fax through email.

2.2. Test Results

All test cases had been executed and completed with the observations as list below:

1. Prior to configuration of the Esna Officelinx Cloudlink Edition server, the Officelinx Cloudlink Edition menu provides feature button labels for actions on incoming calls. The "Take Message" feature was tested but the redirected call did not properly integrate with the correct voicemail box. It is recommended that this feature option be disabled by the ESNA Officelinx Cloudlink Edition Administrator.

2. When a user receives a message, iLink Pro receives and indicates that there is a new message, and the message waiting indicator (MWI) is turned on. When a user retrieves a message using iLink Pro, MWI is turned off on iLink Pro and the physical phone, but when Messaging maintenance subsequently runs, MWI is turned on again and Messaging indicates there is a new message. This is a known limitation and is due to the fact that Esna Officelinx Cloudlink Edition does not currently use the ACE Messaging API to “synchronize” the information to Messaging. This capability is planned for implementation in a future release of ESNA Officelinx Cloudlink Edition.

3. Call extension of parties after a call is transferred does not update. This is a known limitation in the current version of Esna Officelinx Cloudlink Edition. A fix is planned for a future release of ESNA Officelinx Cloudlink Edition.

4. Call forward is not supported on ASAI Service Provider. If you make a call to an unavailable iLink Pro user, the call can be forwarded to Messaging, but the caller gets the general greeting, instead of the greeting for the user that was called. To avoid this issue the call can be forced to ring at the called party’s phone by not entering the Messaging hunt group number in the Officelinx configuration.

5. A physical phone A is not monitored by ESNA Officelinx, make a call to iLink Pro user B (physical phone B is monitored) then phone A performs a consultative transfer to iLink Pro user C (physical phone C is monitored). iLink Pro user C later tries to put the call on Hold using iLink Pro - Hold option, the call is not put on hold and the user C loses call control UI on iLink Pro. A work around is to put the call on hold using the physical phone. This is a known limitation of Esna Officelinx Cloudlink Edition. To avoid this issue all internal phones must be monitored by Officelinx.

6. When Device A (DA) makes a call to iLink Pro user B and iLink Pro user B transfers the call to iLink Pro user C, iLink Pro user C sometimes receives 2 popup messages: “Call Disconnected from DA” and “Incoming call from DA”. After 3 second the extraneous “Call Disconnected” popup message is closed. iLink Pro user C can click answer on the “Incoming call” popup window to connect the call. The two popup windows do not impact the call operation, however having 2 popup windows displayed at the same time can confuse the user. User should ignore the extraneous “Call Disconnected” message when it occurs. A fix is planned for a future release of ESNA Officelinx Cloudlink Edition.

7. If the phones of iLink Pro user A, and iLink Pro user B are off-hook (e.g. A and B are on a call), the status of iLink Pro user A and B are displayed to iLink Pro user C as “On the Phone”. If iLink Pro user C makes a call to iLink Pro user A, and iLink Pro user C then disconnects the call (hangs up) before iLink Pro user A answers, the display of iLink Pro user A’s status on iLink Pro user C is changed to indicate that iLink Pro user A is not on the phone, even though the call between iLink Pro user A and iLink Pro user B is still connected. A fix is planned for a future release of ESNA Officelinx Cloudlink Edition.

8. iLink Pro user A is on a call with iLink Pro user B. iLink Pro user C attempts to call iLink Pro user A, iLink Pro user A receives an alert message for the incoming call. If iLink Pro user A clicks "Answer", ACE generates an exception, "Exception 10001 Service Error occurred", for the second call and the first call remains connected. This is due to the fact that ACE expects the first call to be put on hold before the second call is answered. If iLink Pro user A puts the first call on hold before clicking answer on the second call the problem does not occur. Also, the problem does not occur if iLink Pro user A answers the second call by pressing the answer button on the device, as Communication Manager will automatically put the first call on hold before answering the second.

9. When a user double clicks on the Answer option, multiple requests for Answer call are sent to ACE which is causing ACE to return an exception.

2.3. Support

Technical support for the ESNA Telephony Officelinx solution can be obtained by contacting ESNA:

- Website: www.esna.com.
- Email: techsupport@esna.com.
- Phone: +1(905) 707-1234.

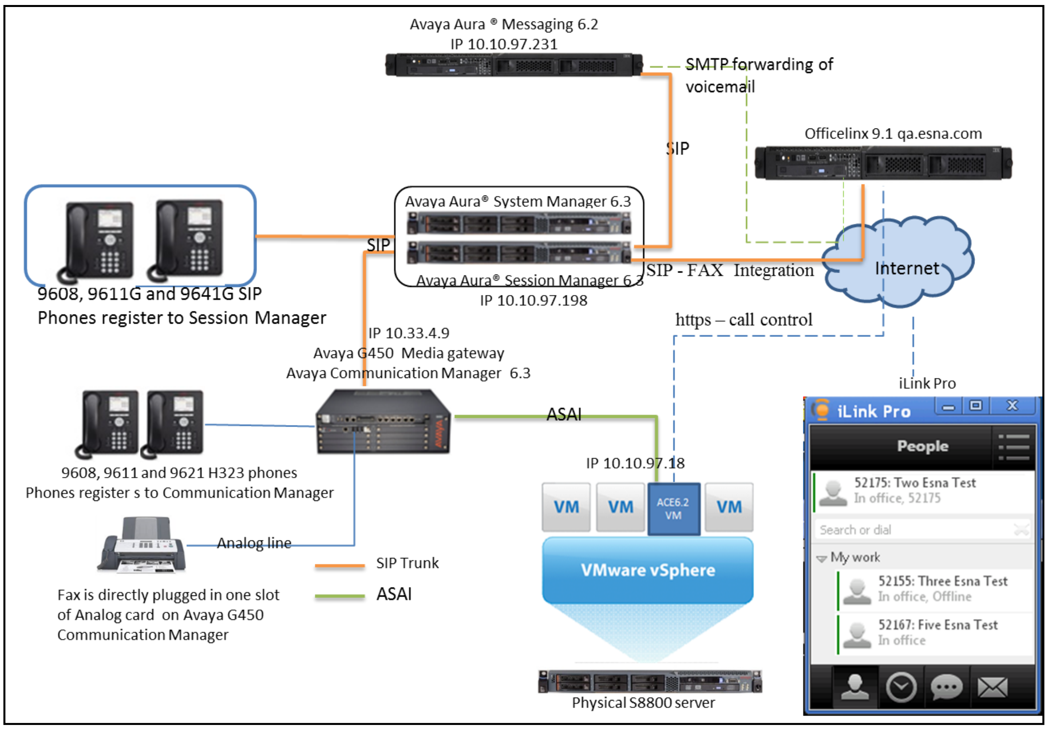
3. Reference Configuration

Figure below illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with a Session Manager and Communication Manager on S8300D Server with an Avaya G450 Media Gateway. Endpoints include Avaya 9600 Series SIP and H.323 IP Telephones.

ESNA Telephony Officelinx is configured as a trusted SIP entity with the Session Manager.

Users are able to click and call on the iLink Pro as well as received notify message from Messaging on their ESNA Gmail account.

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



Test Configuration of Avaya ACE and Avaya Aura® systems provide services to ESNA Telephony Officelinx

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on an Avaya S8300D Media Server	R016x.03.0.124 Patch 03.0.124.20850
Avaya G450 Media Gateway	33.13.0 (B)
Avaya Aura® System Manager running on an Avaya S8800 Server	6.3.0 FP2 SU 6.3.2.4.1399
Avaya Aura® Session Manager running on an Avaya S8800 Server	6.3.2.0. 632023
Avaya Aura® Messaging running on an Avaya S8800 Server	R016x.02.0.823
Avaya S8800 Server with VMWare 5.1 running Avaya Agile Communication Environment VE	6.2.1FP2
Avaya 9611G, 9608 H323 Phone	6.2
Avaya 9611G, 9608 SIP Phone	6.2
Avaya 9630 H323 Phone	3.1.05
ESNA Officelinx	9.1 SP1
iLink Pro	9.1.14.1227

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager. A SIP trunk, with Fax pass through enabled is created between Communication Manager and Session Manager. It is assumed the general installation of Communication Manager on Avaya G450 Media Gateway and Session Manager has been previously installed correctly.

In configuring Communication Manager, various components such as IP-network-regions, signaling groups, trunk groups, etc., need to be selected or created for use with the SIP connection to Session Manager. Unless specifically stated otherwise, any unused IP-network-region, signaling group, trunk group, etc. can be used for this purpose.

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

5.1. Configure SIP Trunk

The following sections show the necessary steps required to configure Communication Manager to interoperate correctly with Session 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 **Maximum Administered 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 IP Codec Set

This section describes the steps for 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. Use the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used for configuring IP network region to specify which codec sets may be used within and between network regions. Below is example of **G.711MU** and **G.711A** code used in compliance test.

```
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.711A           n          2        20
```

As ESNA Officelinx only support fax pass-through mode, in ip-codec-set on **page 2**, **FAX** is configured using **pass-through**.

```
                                                      Page   2 of   2
                          IP Codec Set
                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:  4096:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:  4096:Kbits
                    Mode                    Redundancy
    FAX             pass-through              0
    Modem           off                       0
    TDD/TTY         US                        3
    Clear-channel   n                         0
```

5.1.3. Configure IP Network Region

This section describes the steps for 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. This name appears in the "From" header of SIP messages originating from this IP region.
- **Codec Set** – Set the configured codec set number. In this example, **Codec Set 1** is used.

```
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

Use the **display node-names ip** command to verify that node names have been previously defined for the IP addresses of the Avaya S8300D Server running Communication Manager **(procr 10.33.4.9**) and for Session Manager (**DevASM 10.10.97.198**). These node names will be needed for defining signaling group.

```
display node-names ip                                        Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
DevASM              10.10.97.198
procr               10.33.4.9
procr6              ::
default             0.0.0.0
```

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**.
- **Far-end Node Name** – Set to the Session Manager name configured in node-names ip.
- **Far-end Network Region** – Set to the configured region.
- **Far-end Domain** – Set to **bvwdev.com**. This should match the SIP Domain value in **Session Manager**.
- **Direct IP-IP Audio Connections** – Set to **y**, since the 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: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1
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 associate trunk group for created signaling 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 configured signaling group.
- **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.
- Default values were used for all other fields.

```
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.** This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign when passed in the SIP From, Contact and P-Asserted Identity headers.

```
display 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 and **Numbering Format** is **lev0-pvt**. The default values for the other fields may be used.

```
change 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, Private Numbering and AAR to route calls over a SIP trunk to Session Manager and ultimately to Messaging, ESNA without the need to dial a Feature Access Code (FAC).

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

- **399**95 – Avaya Aura Messaging Auto Attendant extension.
- **399**90 – Avaya Aura Messaging Pilot extension.
- **521** – Endpoint extension in Communication Manager.
- **782** – Extension to route a call to ESNA Officelinx server. This setup is used to route the fax call to ESNA Officelinx.

```
change dialplan analysis                                          Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 3
    Dialed    Total  Call      Dialed    Total  Call      Dialed    Total  Call
    String    Length Type      String    Length Type      String    Length Type
   1            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 extensions to pilot number of Messaging. As shown below, any number dialed to **399**xx totaling **5**-digits will be routed to the AAR.

```
change 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
 782              5    0                  aar  n
```

Use the command **display private-numbering 0** to view the extensions of all calls traversing SIP trunks in the appropriate private numbering table on the Numbering-Private Format screen.

```
display private-numbering 0                                    Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk         Private          Total
Len Code             Grp(s)      Prefix           Len
 5  782              5                            5     Total Administered: 12
 5  54               5                            5        Maximum Entries: 540
 5  521              5                            5
 5  782              5                            5
 5  3999             5                            5
```

For the AAR Analysis Table, create the dial strings that will route calls to Messaging, Telephony Officelinx 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). The dialed string created in the AAR Digit Analysis table should contain a map to the Messaging pilot number and Officelinx extension. During the configuration of the AAR table, the Call Type field was set to **unku** for **399xx** and to **aar** for **521xx and 782xx**.

```
change 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
    782                   5    5     5        aar           n
```

5.1.9. 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, example: **Messaging.**
- **Group Extension** – Enter an extension valid in the provisioned dial plan, example **39991**.

```
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 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
```

5.1.10. 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. The default values for the other fields may be used.

```
add 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:
```

5.1.11. 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** 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.

```
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 7.7** for step on how to create SIP user on Session Manager. On the station form in Communication Manager, on the last page is a Third Party Call Control setting. Set value for **Type of 3PCC Enabled: Avaya.** This setup makes sure that ACE Notification service can send out the notification for SIP Phone.

```
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 show user step to configure Outbound Proxy set in the locations form. Enter "**change locations**" set the value for **Proxy Rte** to route pattern that will go to Session Manager. During compliance test, route **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 Adjunct/Switch Applications Interface Link

This section provides the procedures for configuring an ASAI link between Communication Manager and ACE. The procedures include the following areas:

- Verify license permission.
- Configuring AE Services and 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 **Computer Telephony Adjunct Links** customer option is set to "**y**" on **Page 3**.

```
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? n               DCS Call Coverage? y
          ASAI Link Plus Capabilities? n              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, you must enter a Local Port number. These values must match the Port value you will enter when creating ASAI service provider on ACE. Enter **change ip-services.** 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 ACE server name and password must be entered. These values must match the ACE Server Name and Password values you will enter when adding ASAI service provider on ACE.

5.2.3. Add a CTI link

A CTI Link number is added and this value must match the CTI Link number entered when adding ASAI service provider on ACE.

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 procedure includes the following:

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

See references **Section 12** for standard installation and configuration information. General knowledge of the configuration tools and interfaces is assumed.

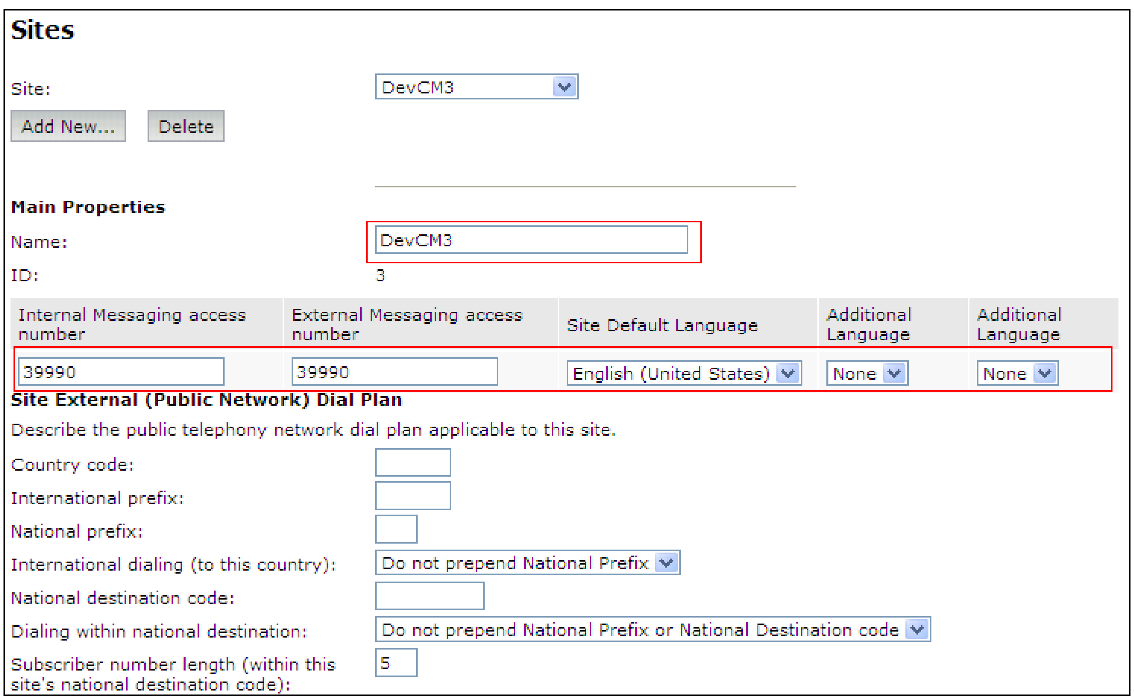
6.1. Administer Sites

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** (not shown). In the left panel, under **Messaging System (Storage)** select **Sites** (not shown)**,** click **Add New**. In the right panel fill in the following:

Under **Main Properties**:

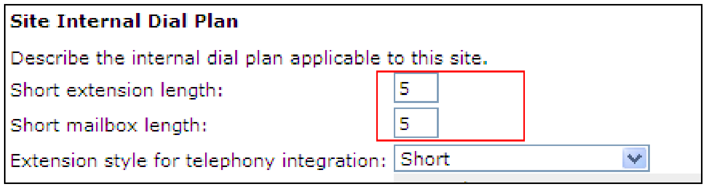
- **Name** Enter site name.
- **Messaging access number (internal)** Enter a Messaging Pilot number.

Sites detail screen show Messaging access number.



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

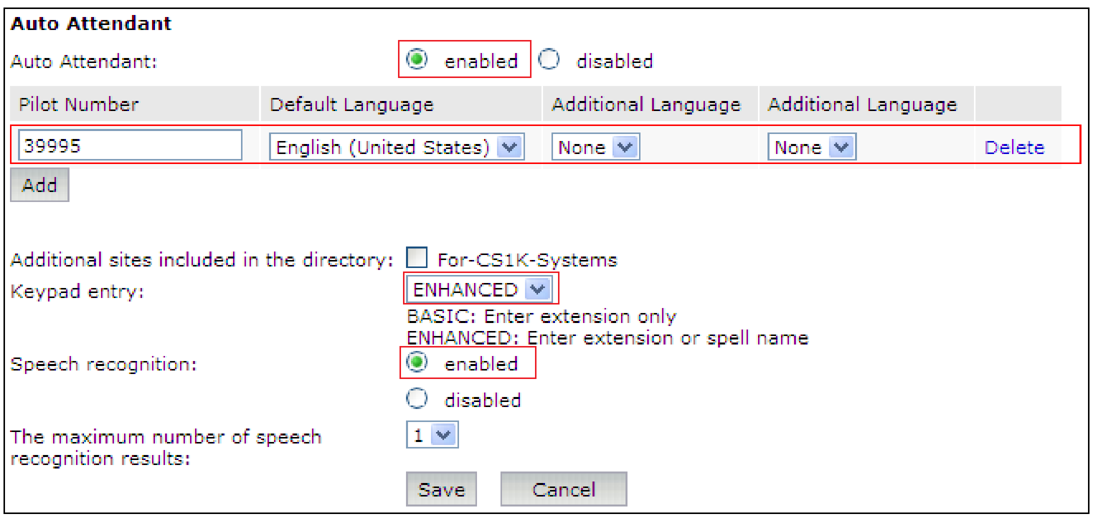
- **Short Extension Length** Enter the number of digits in extensions.
- **Short Mailbox Length** Enter the number of digits in mailbox numbers.



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 **ENHANCED.**
- **Speech recognition** Select **Enabled.**

Click **Save** to save changes.



6.2. Administer Telephony Integration

A SIP trunk needs to be configured from Messaging to Session Manager. Log into the Messaging System Management Interface (SMI) and go to **Administration → Messaging** (not shown). In the left panel, under **Telephony Settings (Application)** select **Telephony Integration**. In the right panel fill in the following:

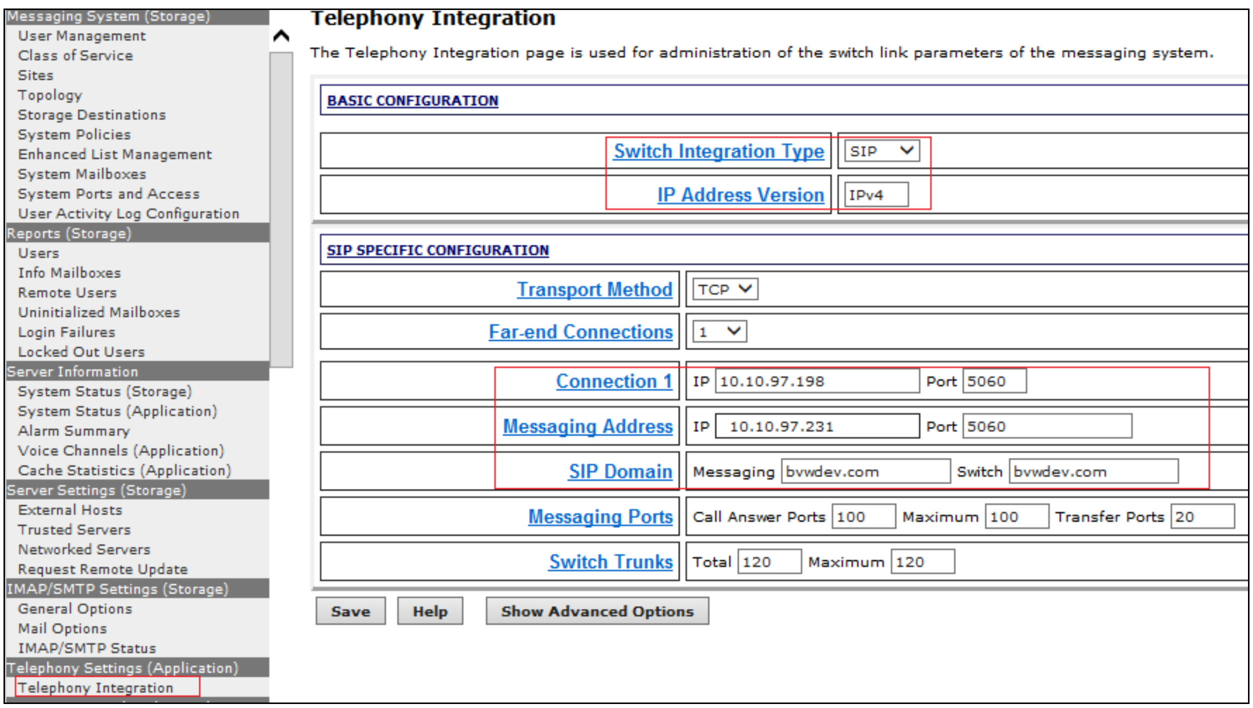
Under **Basic Configuration:**

- **Switch Integration Type:** **SIP**.
- **IP Address Version**: **IPv4**.

Under **SIP Specific Configuration:**

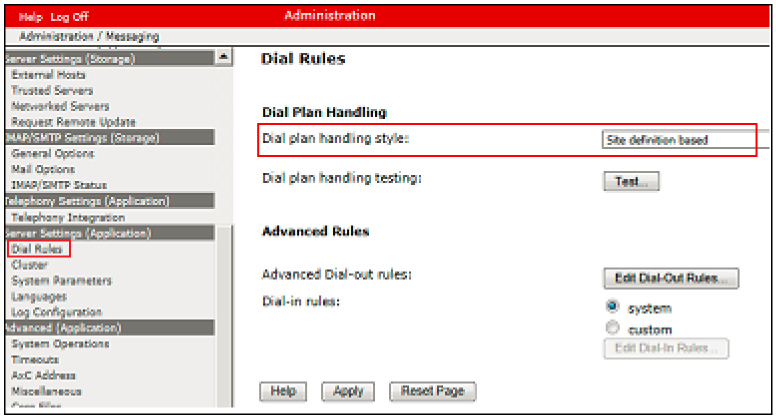
- **Transport Method: TCP**.
- **Connection 1:**Enter the Session Manager signaling IP address and TCP port number.
- **Messaging Address:** Enter the Messaging IP address and TCP port number.
- **SIP Domain:** Enter the Messaging and Session Manager domain names.

Click **Save** to save changes.

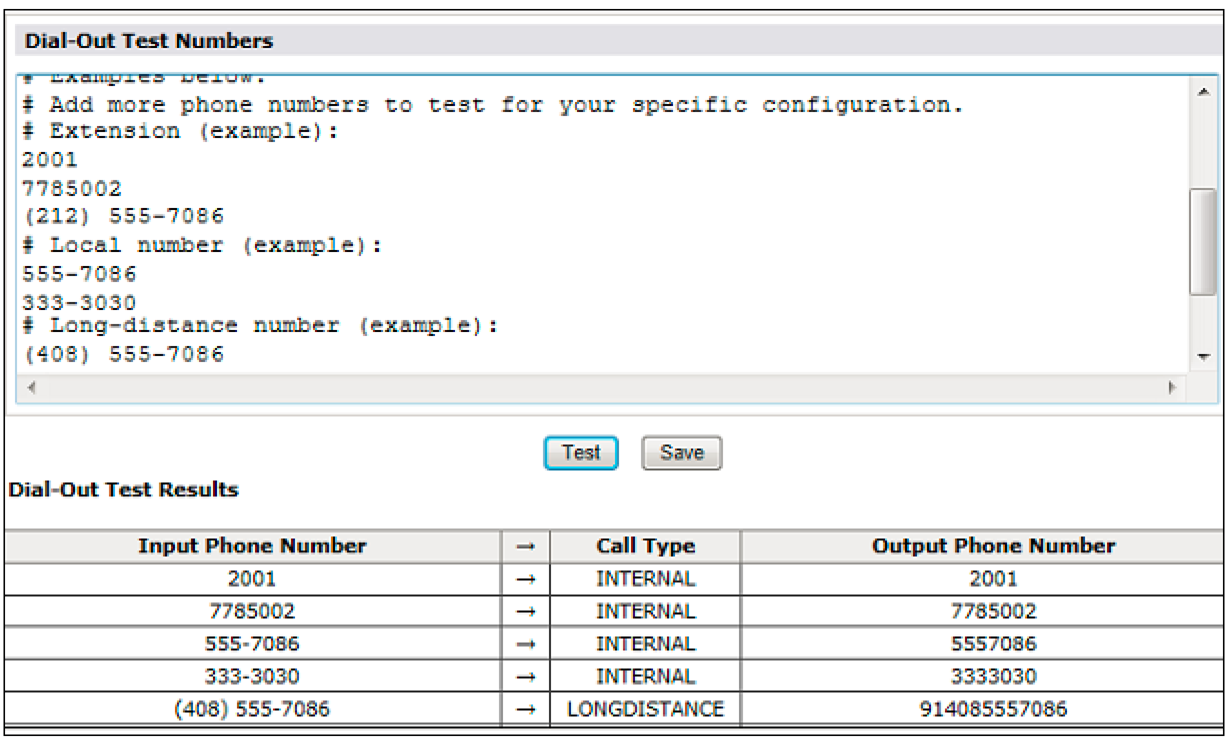


6.3. Configure Dial Rules

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 (shown above) to verify the appropriate parameters for outbound dialing from Messaging were set. These dial rules help 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.



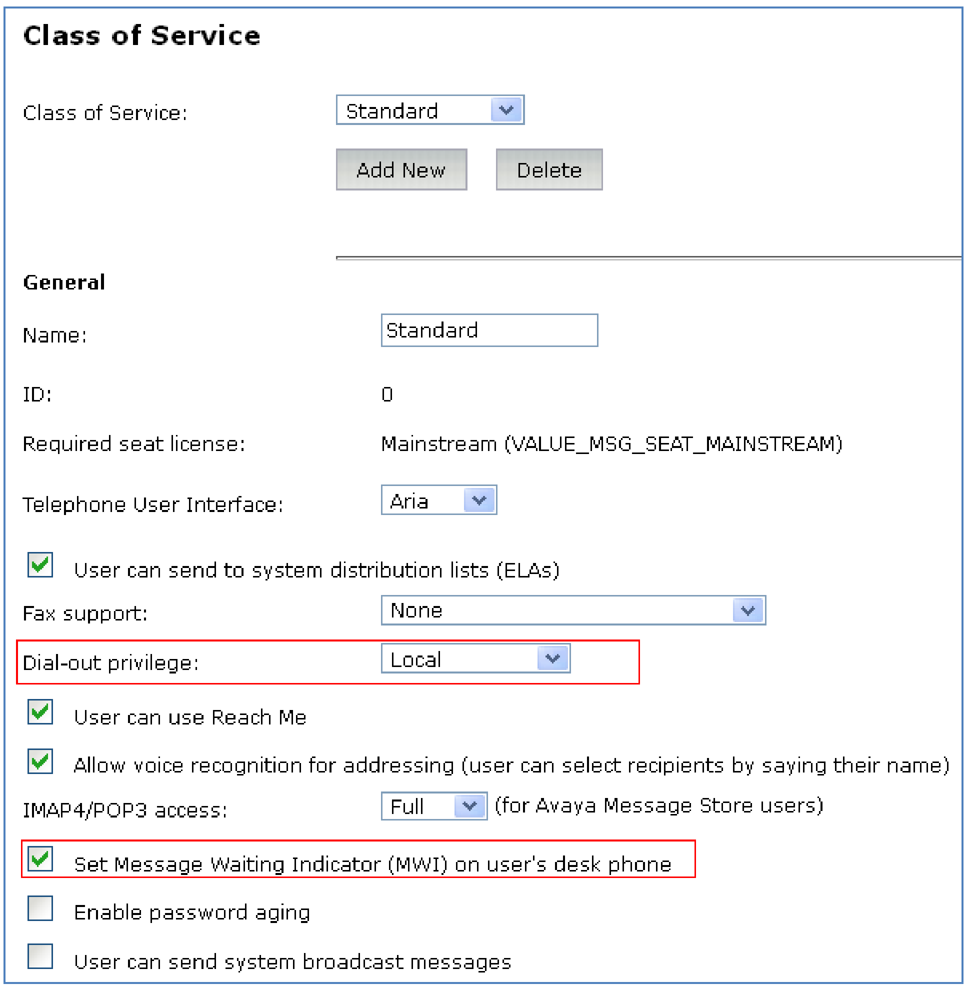
Input Phone Number	→	Call Type	Output Phone Number
2001	→	INTERNAL	2001
7785002	→	INTERNAL	7785002
555-7086	→	INTERNAL	5557086
333-3030	→	INTERNAL	3333030
(408) 555-7086	→	LONGDISTANCE	914085557086

6.4. Configure Class of Service

Verify Messaging Waiting is enabled for all subscribers. Use **Administration → Messaging** menu and select **Class of Service** under **Messaging System (Storage)** (not shown)**.** Select **"Standard"** from the **Class of Service** drop-down menu. Under **General** section, enter the following value and use default values for remaining fields.

- Select **Dial-out privilege** to **Local**.
- Check **Set Message Waiting Indicator (MWI) on user's desk phone.**

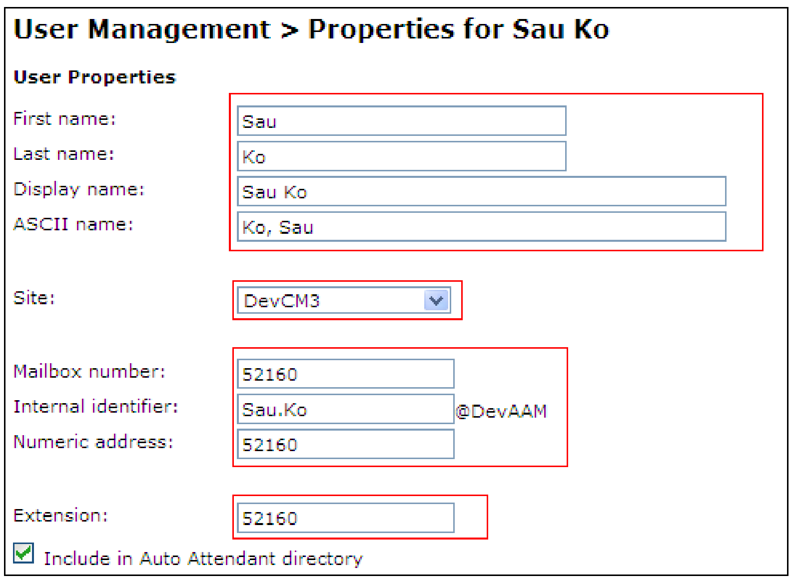
Click **Save** to save changes (not shown). The following screen shows the settings defined for the "**Standard**" Class of Service in the sample configuration.



6.5. Administer Subscribers

In the left panel, under **Messaging System (Storage)** select **User Management** (not shown). In the right panel fill in the following under **User Properties:**

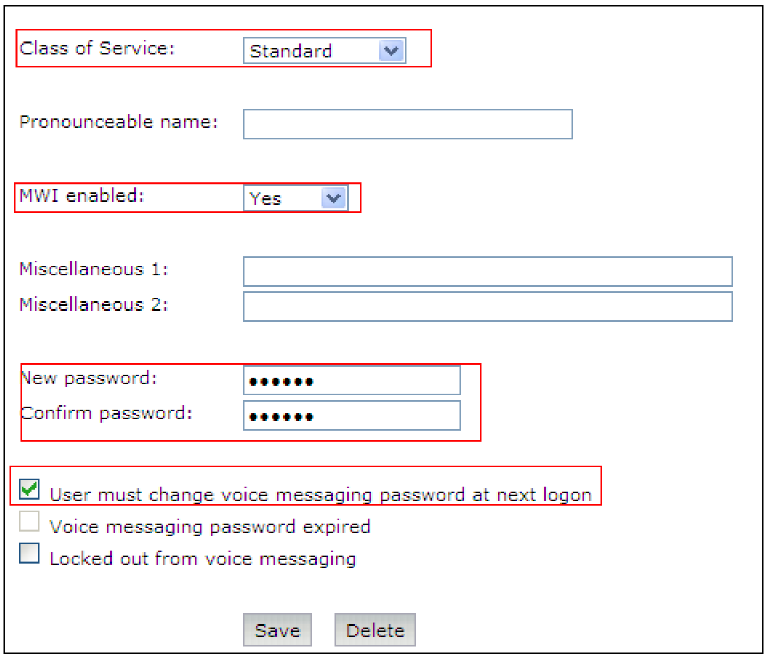
- **First Name** Enter first name.
- **Last Name** Enter last name.
- **Display Name** Enter display name.
- **ASCII name** Enter the ASCII name.
- **Site** Enter site defined in **Section 6.1**.
- **Mailbox Number** Enter desired mailbox number.
- **Internal identifier** Enter the name for internal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



Scroll down on the page to Class of Service.

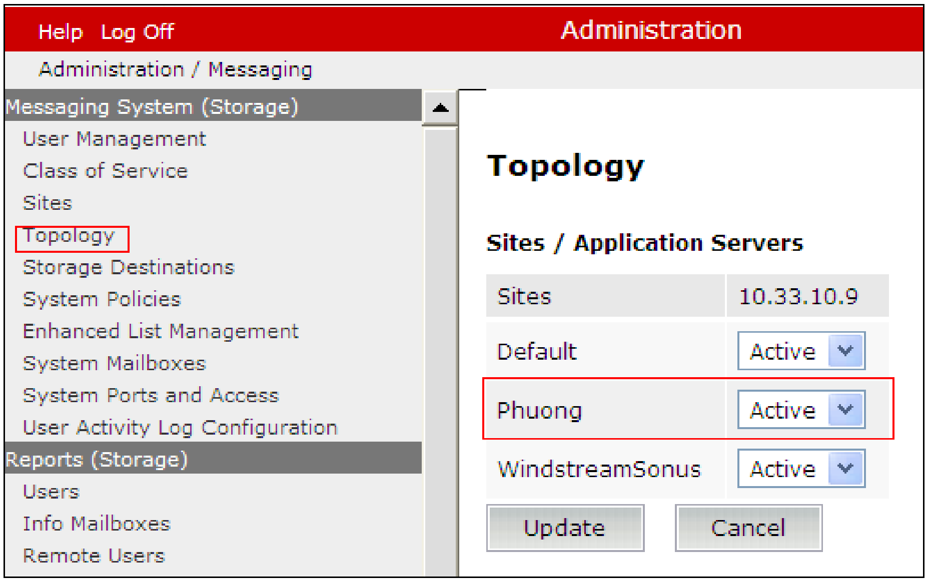
- **Class of Service** Select a Class of Service.
- **Pronounceable Name** Enter a pronounceable name to be used when dialing the extension using voice commands.
- **MWI Enabled** Select **Yes** to enable the MWI light on phones.
- **New Password/Confirm Password** Enter desired extension password.
- **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 created in above section is **Active**.

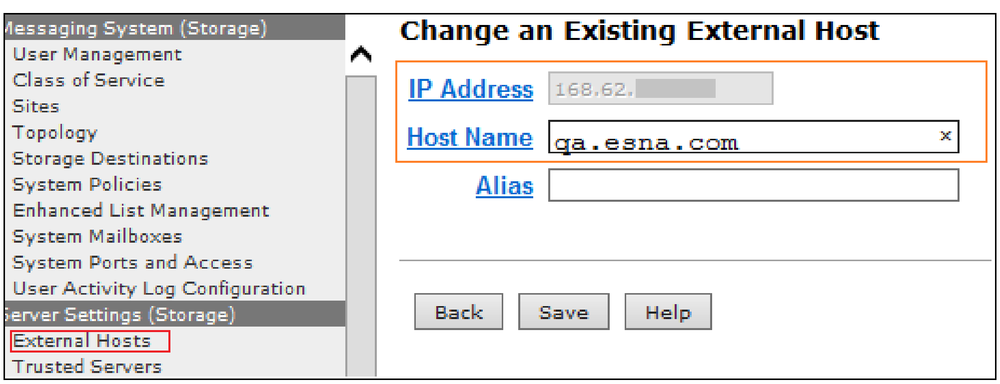


6.7. Administer External Host

Messaging uses an external SMTP relay host to forward text notifications and outbound voice Messages, enable this function by configuring the mail gateway on the External Hosts Web page. Select **Server\Settings (Storage) → External Hosts**, click Add (not shown). In Add a New External Host page:

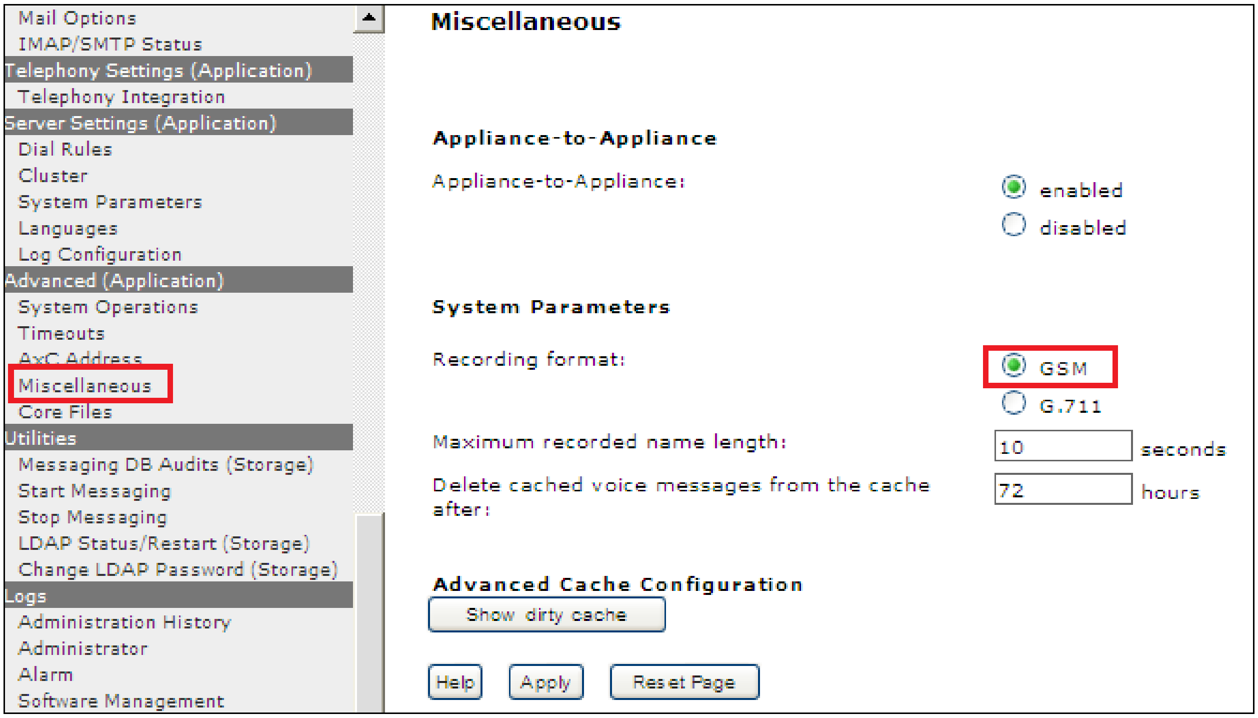
- **IP Address**: Enter IP address of the External SMTP Server, in this compliance test it is IP address of ESNA server.
- **Host Name**: Enter host Name of the External SMTP Server. This case is ESNA host name.

Below is detail of ESNA Server configured in this compliance test:



6.8. Recording Format

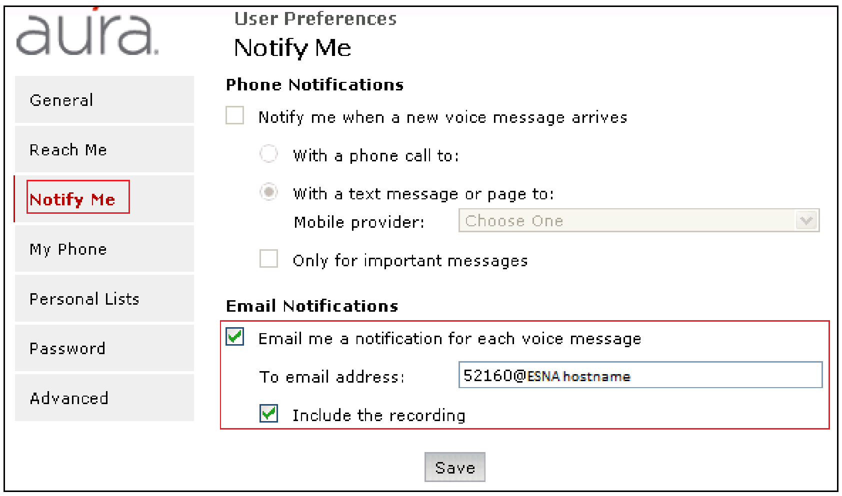
This setup is needed as ESNA only able to recognize the record in GSM format only. In the left window, under **Advanced (applications),** select **Miscellaneous**. In the main window ensure that **Recording format** is set to **GSM**.



6.9. Configure Avaya Aura® Messaging Mailboxes for Notify Me

This is a setting to notify the user on iLink Pro that they have a voice message from Messaging. In the left panel, under **Messaging System (Storage)** select **User Management** (not shown). In the right panel enter mailbox number (e.g. 52160) and click **Edit** (not shown). Scroll right down to **User Preferences** and select **Open User Preference for** Mailbox number user name, (not shown).

In the **User Preferences** detail screen, select **Notify Me**. In the Notify Me detail page, enable checkbox Email me a notification for each voice message to iLink Pro user's email address: example during compliance test the following email is used for iLink Pro user that has extension 52160: 52160@ESNA host name with the option **Include the recording**. Click **Save**.



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 to or synchronized with Session Manager.

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

In this section, the following topics are discussed:

- SIP Domains.
- Locations, Logical/physical location that can be occupied by SIP Entities.
- SIP Entities corresponding to Communication Manager, Session Manager, Messaging and ESNA Officelinx server.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policy, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.

It may not be necessary to create all the items above since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities and Session Manager itself. However, each item should be reviewed to verify the configuration.

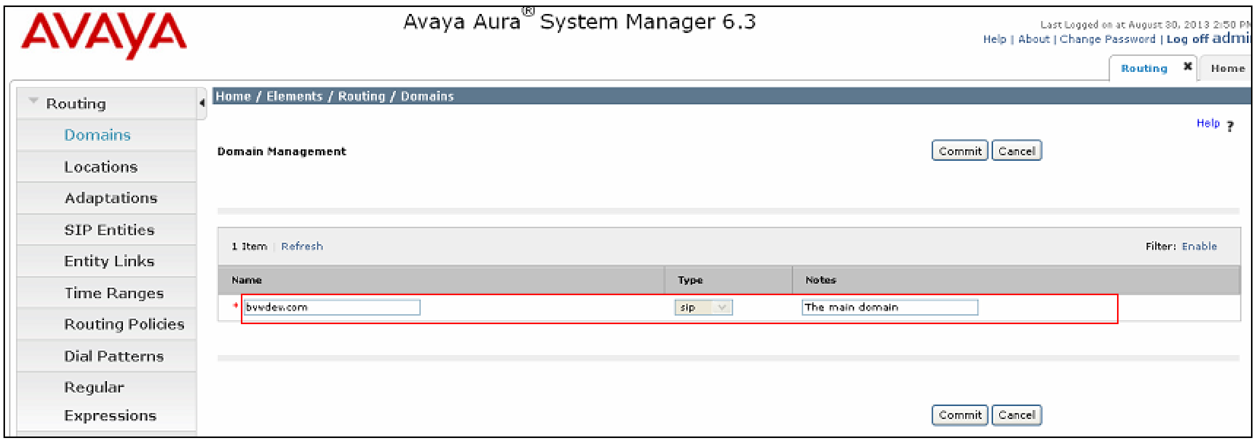
7.1. Configure SIP Domain

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

Create a SIP domain for each domain for which Session Manager will need to be aware of in order to route calls. For the compliance test, this includes the enterprise domain, **bvwdev.com**. To add a domain, navigate to **Routing → Domains**, and click on the **New** button (not shown). Enter the following values and use default values for remaining fields:

- **Name –** Enter the Authoritative Domain Name, 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.

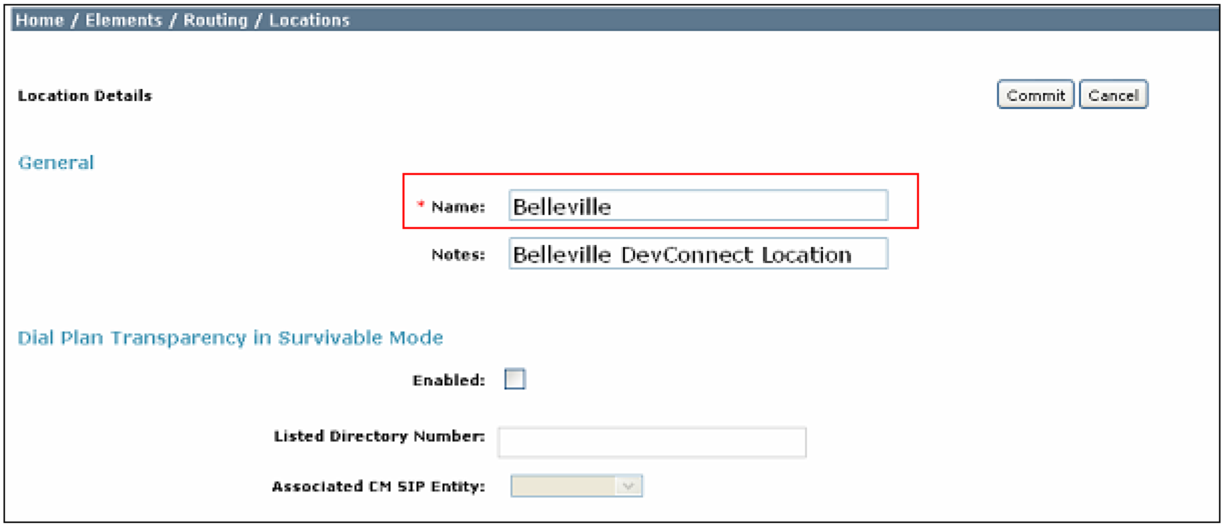
In **General** section, enter the following values and use default values for remaining fields.

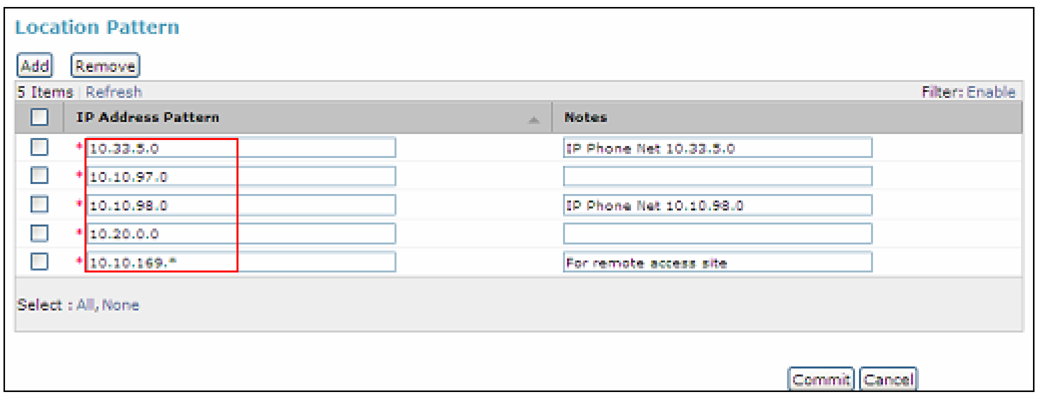
- Enter a descriptive Location name in the **Name** field.
- Enter a description in the **Notes** field if desired.

In **Location Pattern** section, click **Add** and enter the following values:

- **IP address Pattern**: Enter the IP Pattern to identify the location.
- **Notes**: Enter a description in the **Notes** field if desired.

The following screen shows the **Locations** page used during the compliance test. Once the correct information has been filled in, click on the **Commit** button.





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:

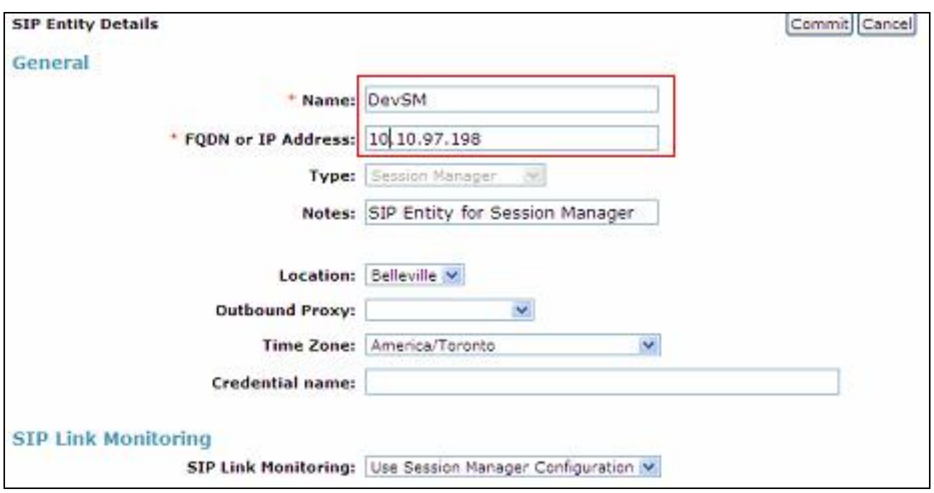
- Session Manager.
- Communication Manager.
- Messaging.
- ESNA Officelinx.

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

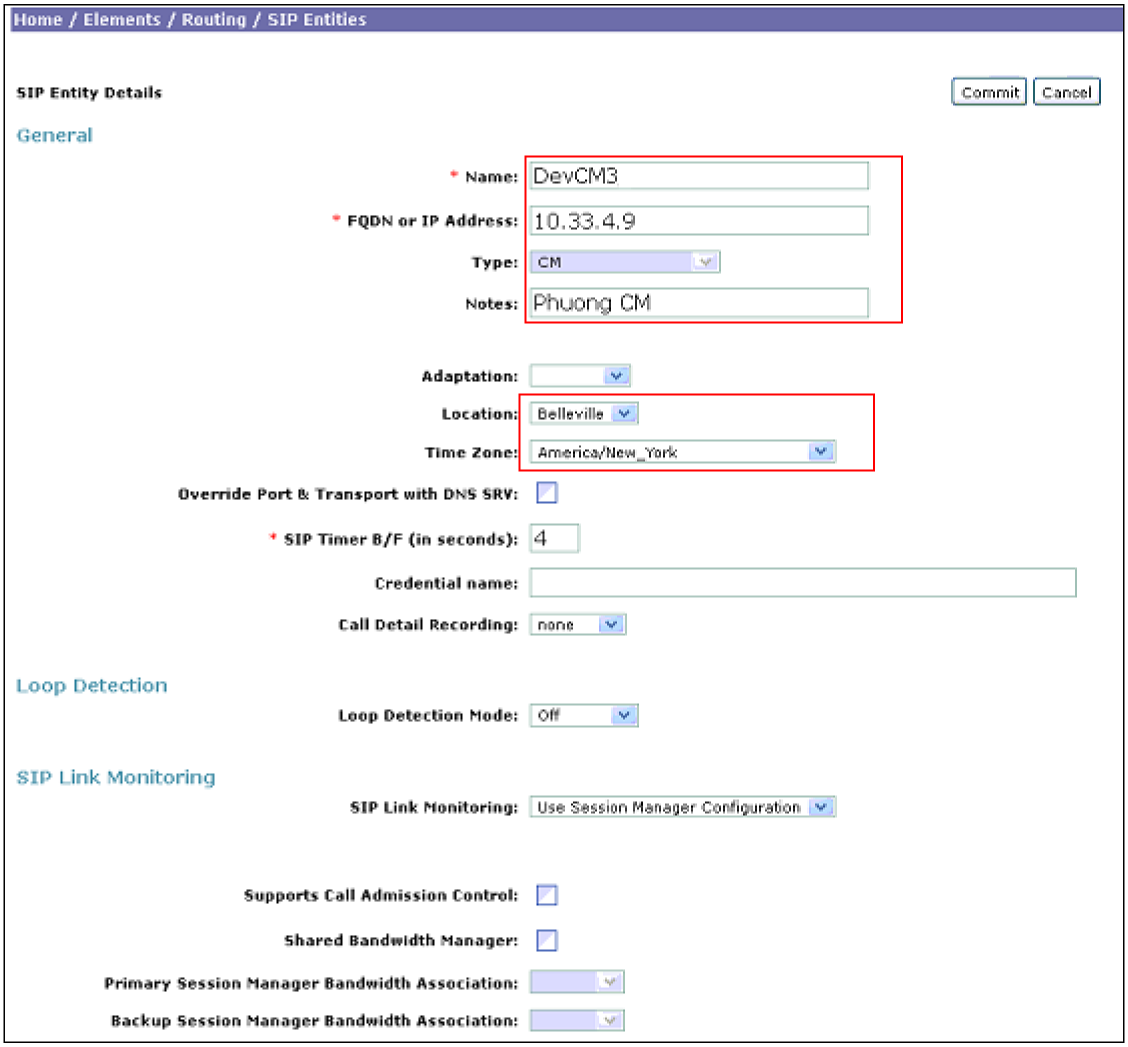
- Enter a descriptive name in the **Name** field.
- Enter IP address of SIP Entity that used for SIP signaling. Enter IP address of Communication Manager, Session Manager, Messaging and ESNA Officelinx.
- From the **Type** drop down menu select a type that best matches the SIP Entity. For Communication Manager, select CM. For Session Manager, select Session Manager. For Messaging, select Modular Messaging.
- Enter a description in the **Notes** field if desired.
- Select appropriate Location.
- 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.

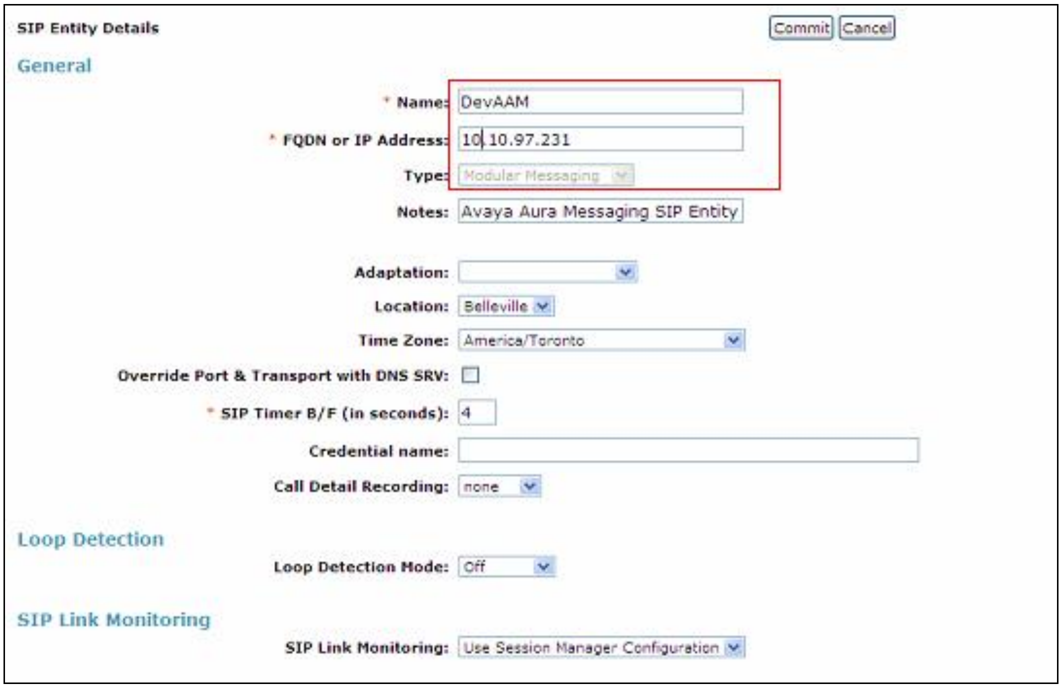
Session Manager SIP Entity.



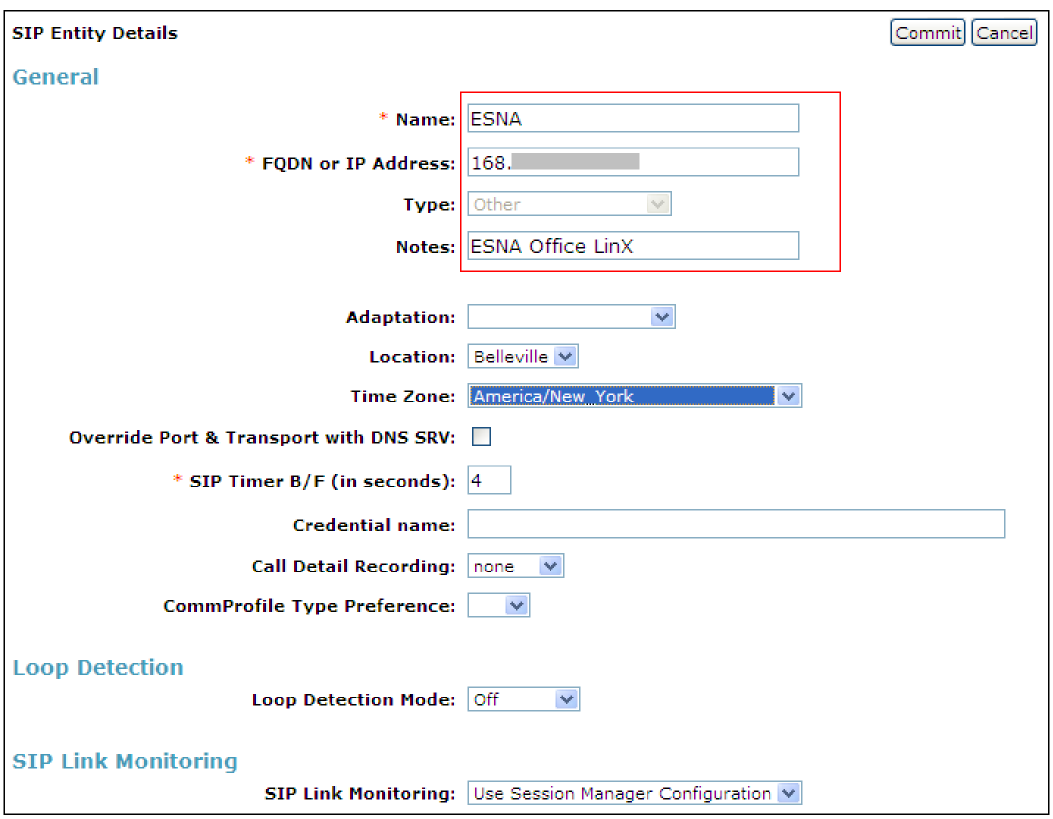
Communication Manager SIP Entity.



Messaging SIP Entity.



ESNA Officelinx SIP Entity.

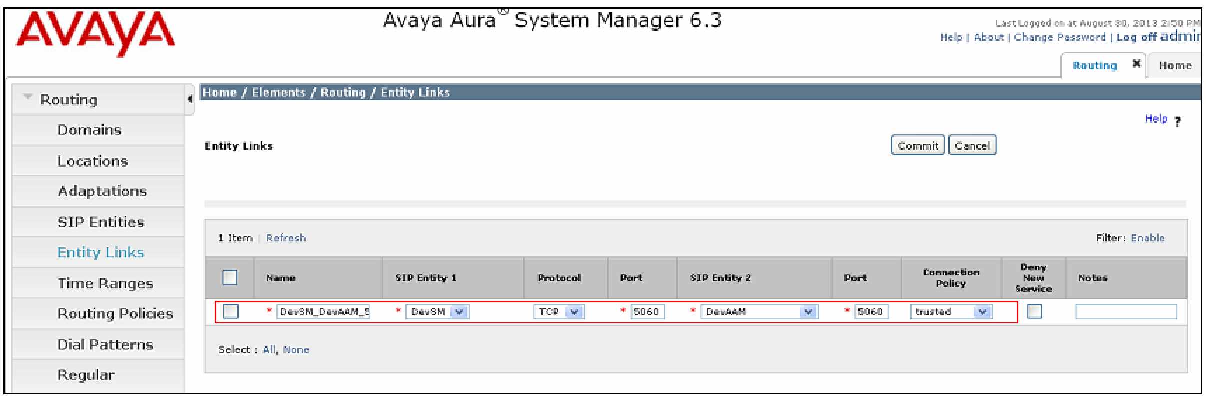


7.4. Configure Entity Links

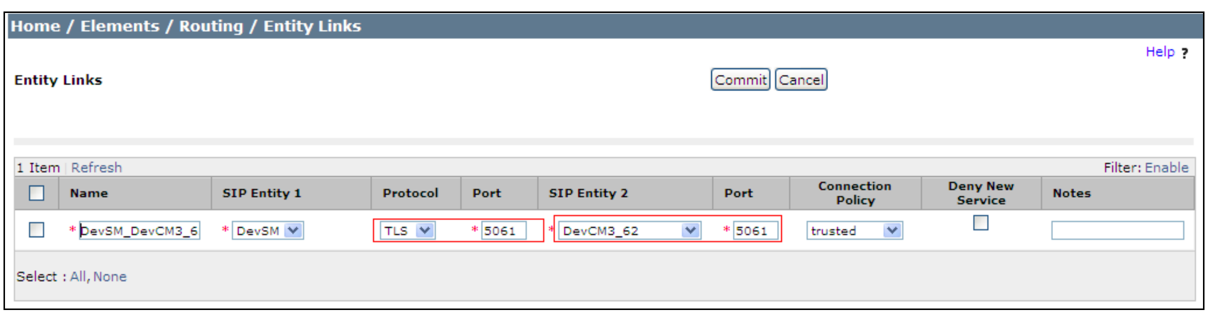
Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the three entities links are defined: one to Communication Manager (Avaya G450 with S8300D Server), one to Messaging and one for Esna Officelinx. To add an entity link, navigate to **Routing → Entity Links**, and click on the **New** button (not shown). 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.
- In the **Protocol** drop down menu, select the protocol to be used.
- In the **Port** field, enter the port to be used, UDP or TCP – 5060.
- In the **SIP Entity 2** drop down menu, select an entity for desired entity.
- In the **Port** field, enter the port to be used (e.g. **5060**).
- Select the **Trusted** option for **Connection Policy**.
- Enter a description in the **Notes** field if desired.

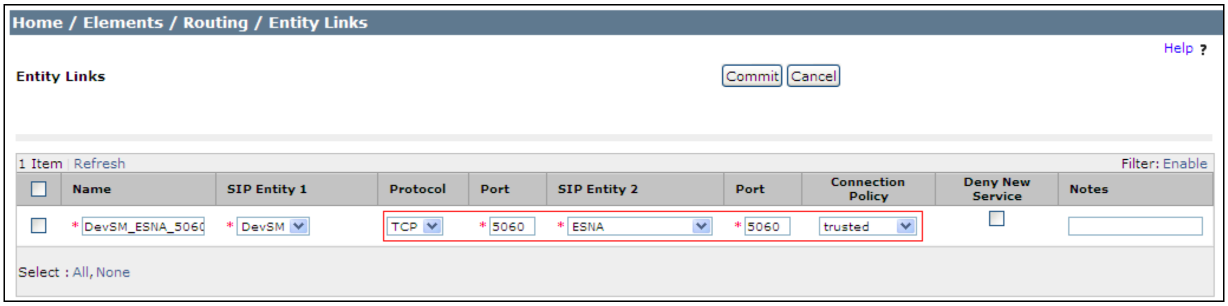
Click on the **Commit** button to save each Entity Link definition. The following screen shows an Entity Links page (between Session Manager and Messaging) used during the compliance test.



Entity Link page (between Session Manager and Communication Manager): **DevSM_DevCM3_62_5061_TLS**.



Entity Link page (between Session Manager and Esna Officelinx): **DevSM_ESNA_5060_TCP**.



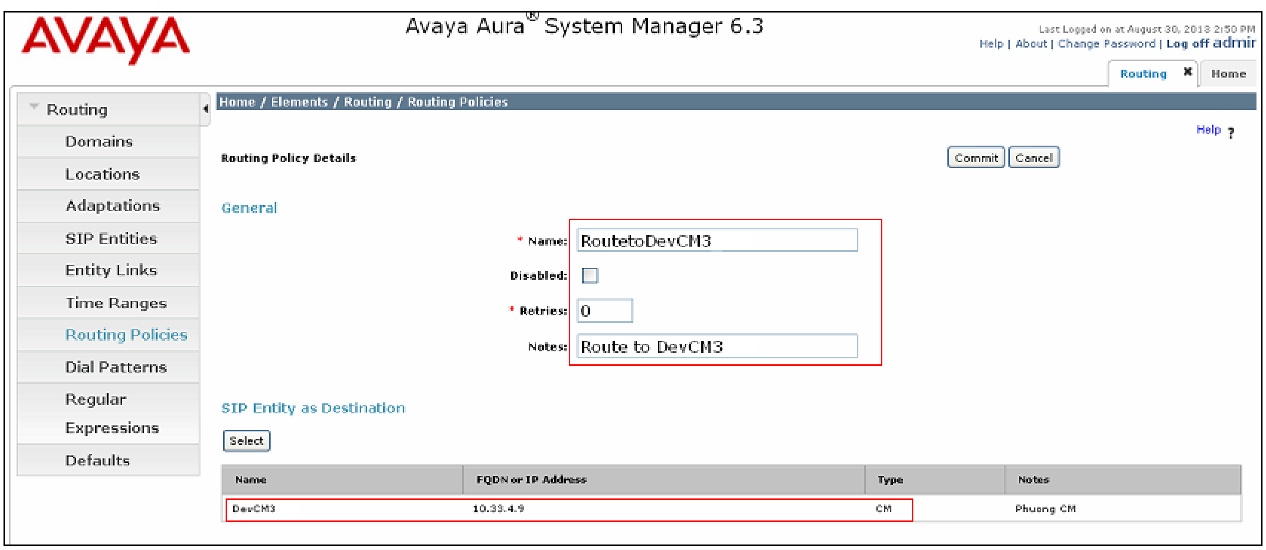
7.5. Configure Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities. Three routing policies must be added, one for Communication Manager, one for Messaging and one for Esna Officelinx. To add a routing policy, navigate to **Routing→Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following: In the **General** section, enter the following values. Use default values for all remaining fields:

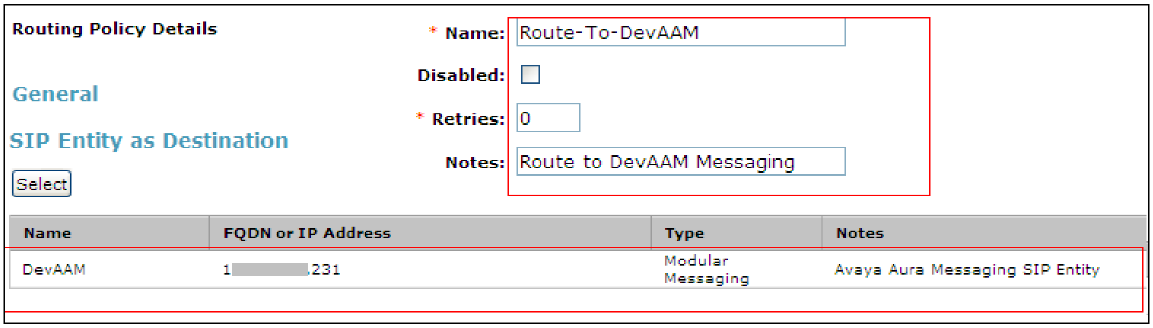
- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP entity displays on the **Routing Policy Details** page as shown below. Use default values for the remaining fields. Click **Commit** to save. The following screens show the routing policy for Communication Manager.

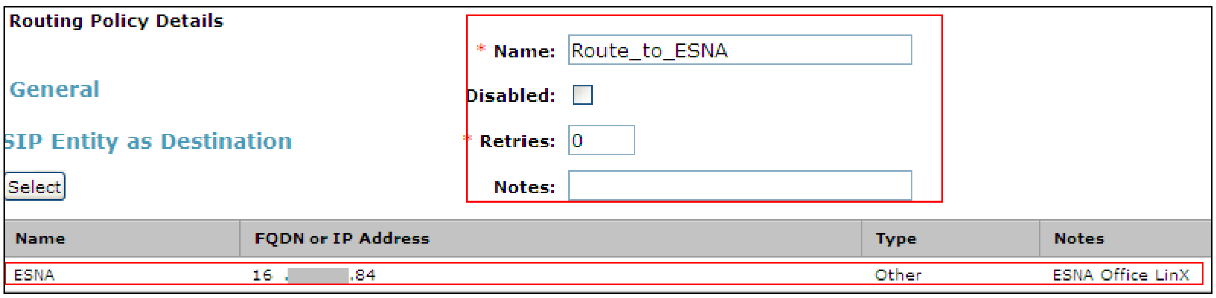
The following screen shows the Routing Policy used for Communication Manager.



Routing policy used for Messaging: **Route-To-DevAAM**.



Routing policy used for ESNA Officelinx: **Route_to_ESNA**.



7.6. Configure 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 from Session Manager.

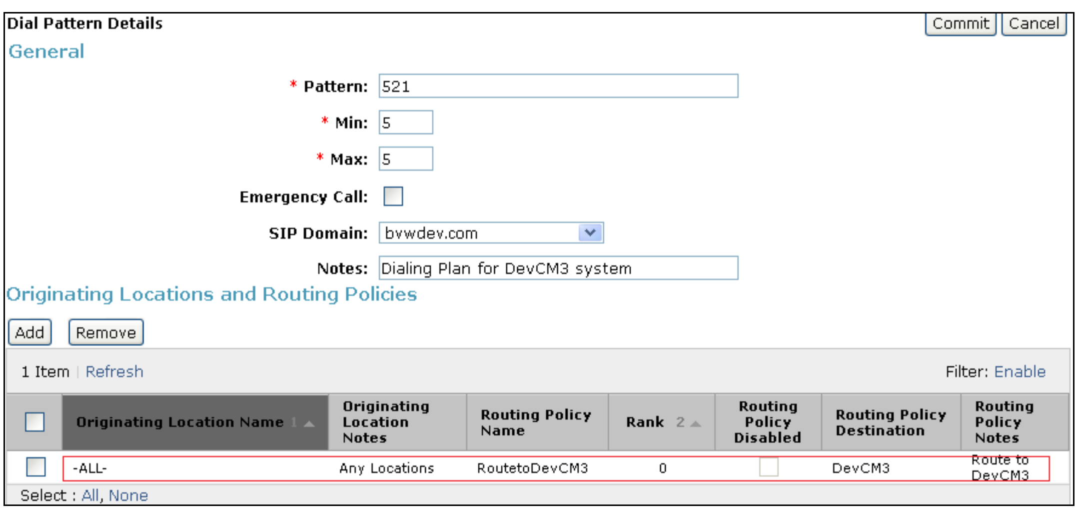
- 5215x – SIP endpoints in Avaya S8300D Server.
- 39990 – Messaging Pilot Number.
- 782xx – ESNA Officelinx pilot number.

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:

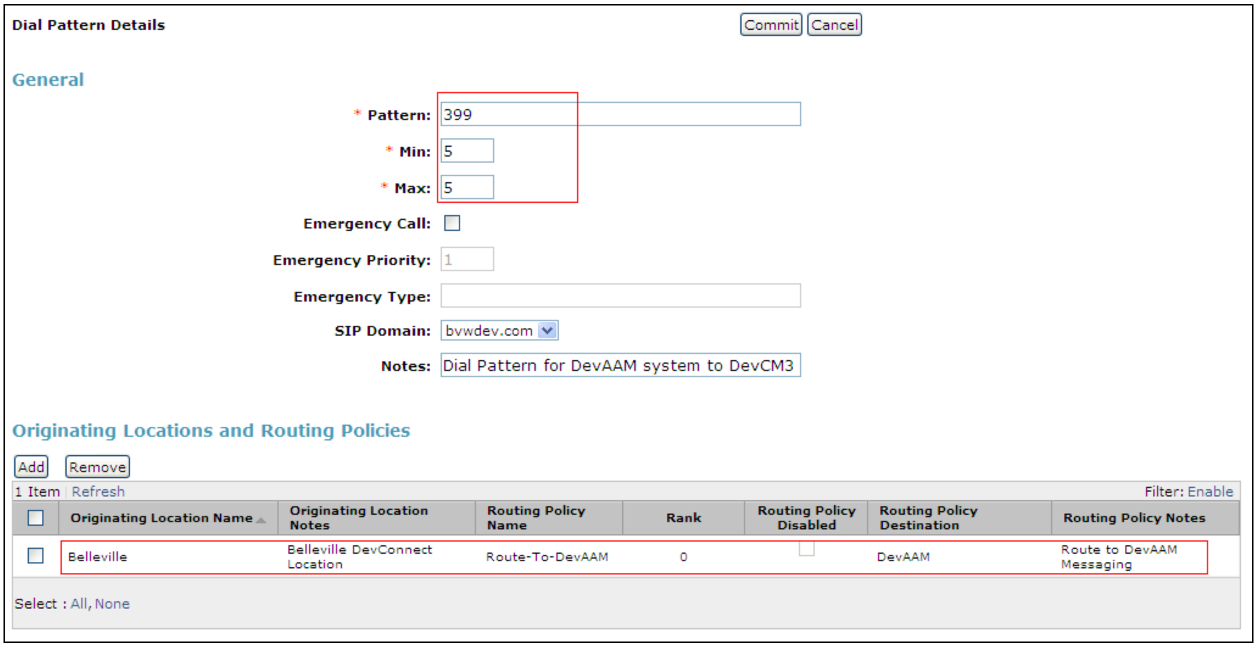
In the **General** section, enter the following values. Use default values for all remaining fields:

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

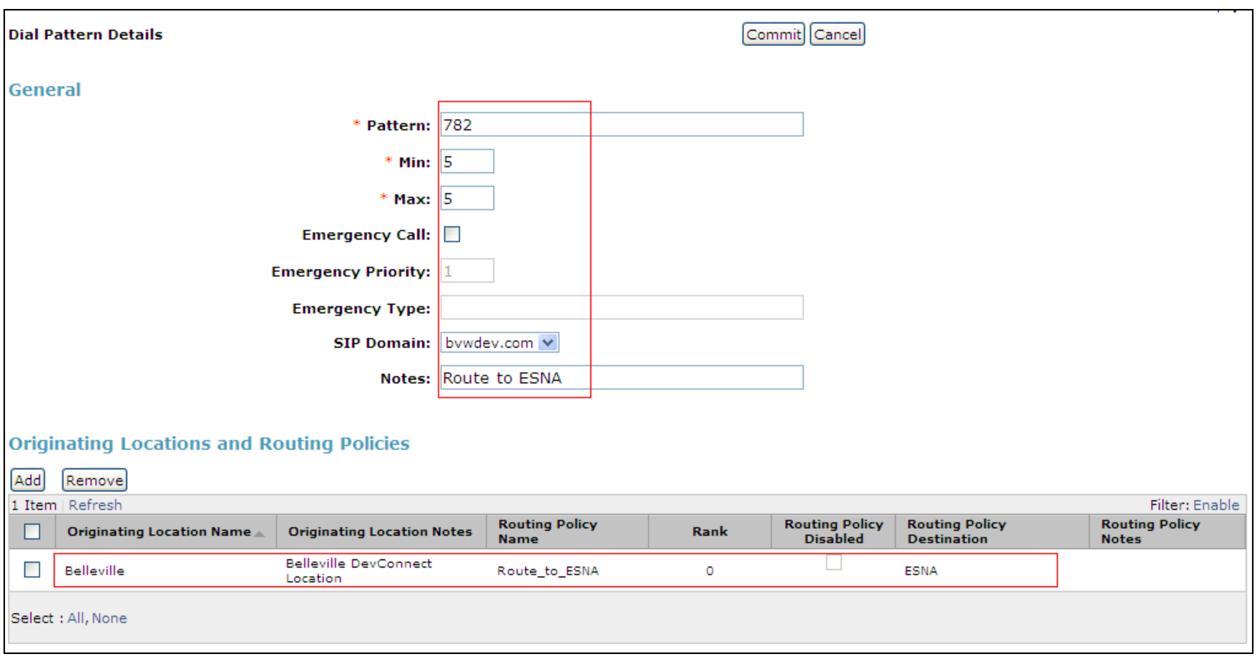
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route calls that match the specified criteria. Click **Select**. Default values can be used for the remaining fields. Click the **Commit** button to save the new definition. The following screen shows the dial pattern used for DevCM3 during the compliance test.



Dial Pattern for Messaging: **399**.



Dial Pattern for ESNA Officelinx: **782**.

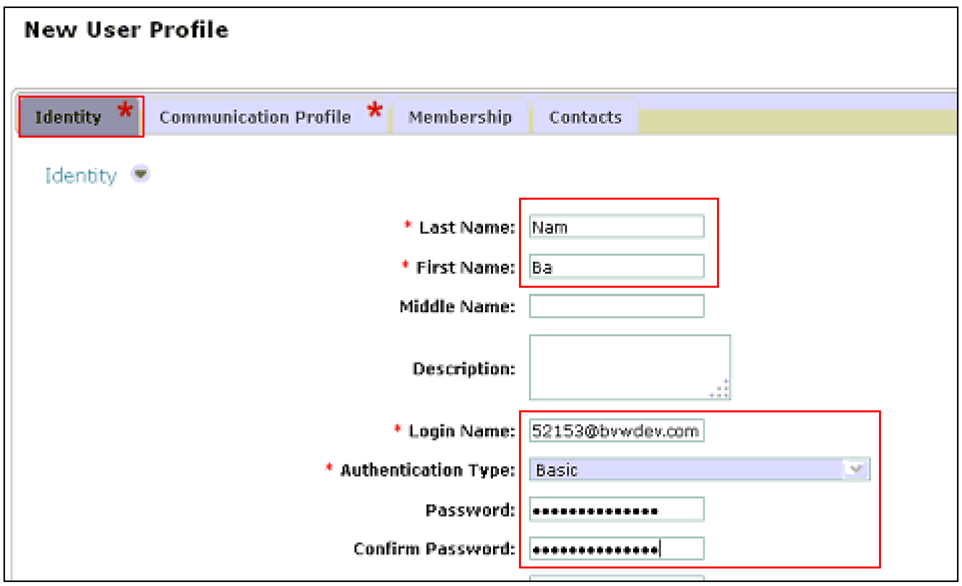


7.7. Configure SIP Users

This section describes the steps required to create SIP user for the Avaya SIP IP Deskphones. To add new SIP users, Navigate to **Users → Manage Users**. Click **New** (not shown) and provide the following information:

In **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**.



In the Communication Profile tab, under Communication Profile section: (not shown).

- **Communication Profile Password –** 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: (not shown).

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

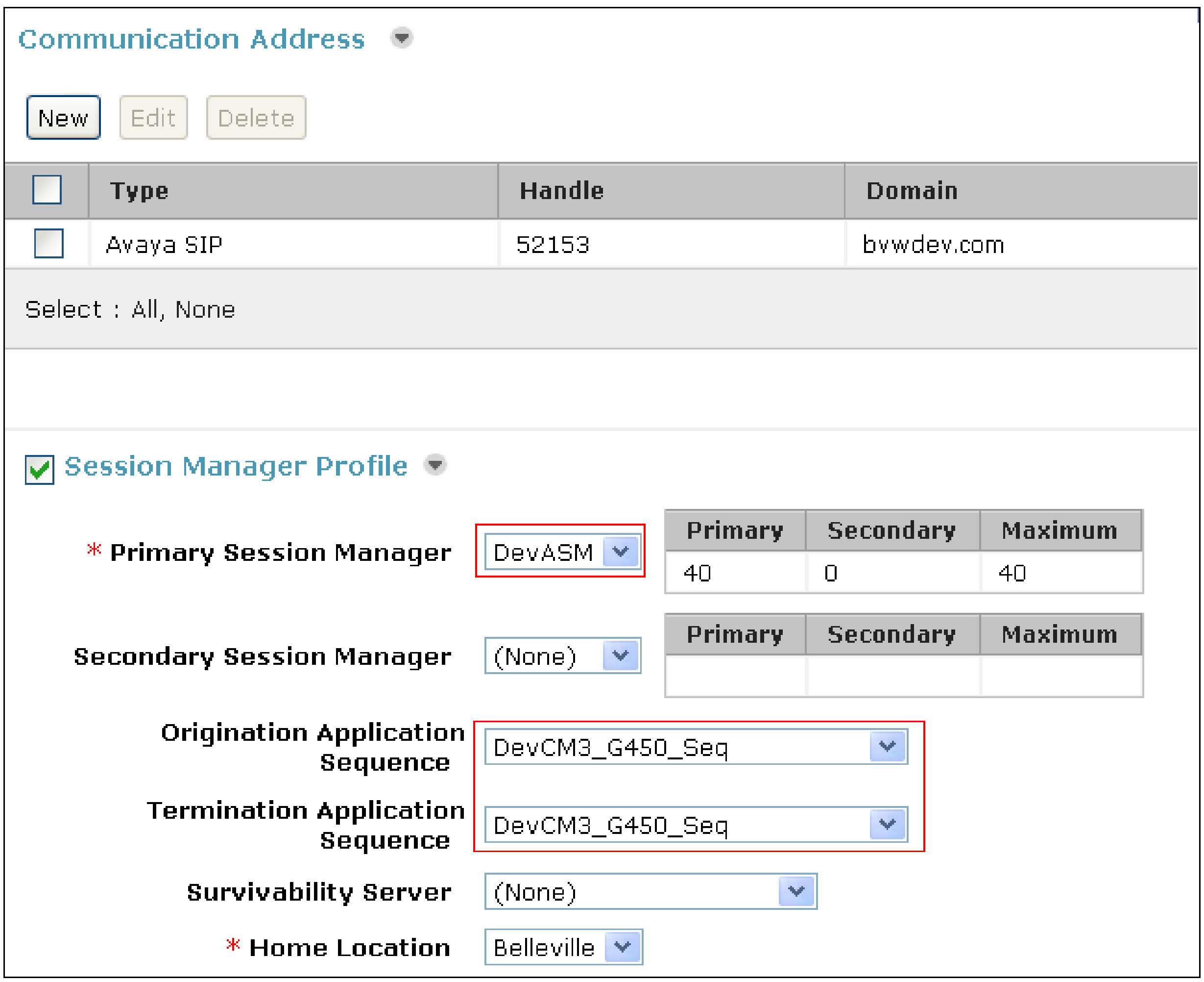
In Communication Address sub-section, select **New** to define a **Communication Address** for the new SIP user, and provide the following information.

- **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.

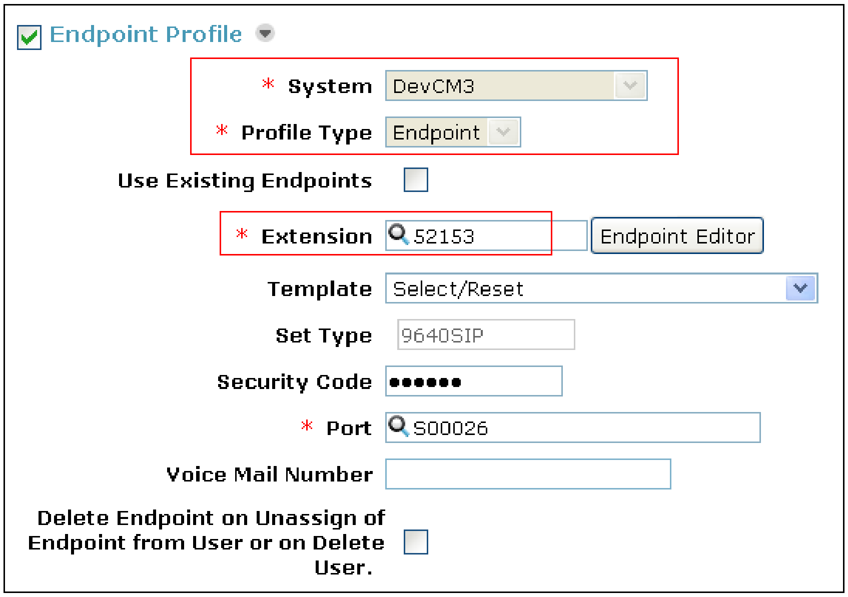
In Session Manager Profile sub-section, enter the following:

- **Primary Session Manager** – Select the 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 above.

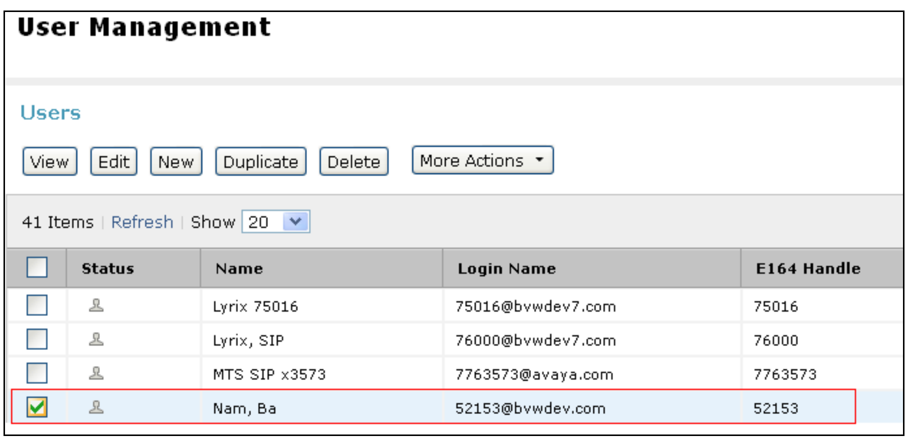


In **Endpoint Profile** sub-section, enter the following information:

- **System** – Communication Manager of interest.
- **Profile Type** – Verify **Endpoint** is selected.
- **Extension** - Enter same extension number used in this section.
- **Template** – Select appropriate template for type of SIP phone. And leave other fields as default.



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



8. Configure Avaya Aura® Agile Communication Environment VE 6.2

This section describes the steps on how to setup ASAI Service provider, create account and role for ESNA Officelinx on ACE.

8.1. Configuring the Avaya Aura® Communication Manager SSL certificate Signing Authority as Trusted on Avaya Aura® Agile Communication Environment

In order for ACE and Communication Manager to establish SSL connectivity, the signing authority of Communication Manager's Server certificate must be configured as trusted on ACE. Refer **Section 12** for the list of relevant documents.

When ACE is initially installed, some signing authorities are automatically configured as trusted on ACE. For example, by default, ACE trusts any certificate signed by SIP Product Certificate Authority or Avaya Product Root CA. In Communication Manager SAT type this command **tlscertmanage –l** to verify current certificate on Communication Manager.

If Communication Manager is configured with a server certificate signed by such an authority, then no further configuration is needed on 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 ACE. Please see "Configuring the Communication Manager's SSL certificate signing authority as trusted on ACE" in **Reference Section 12**.

8.2. Add Adjunct/Switch Applications Interface Service Provider

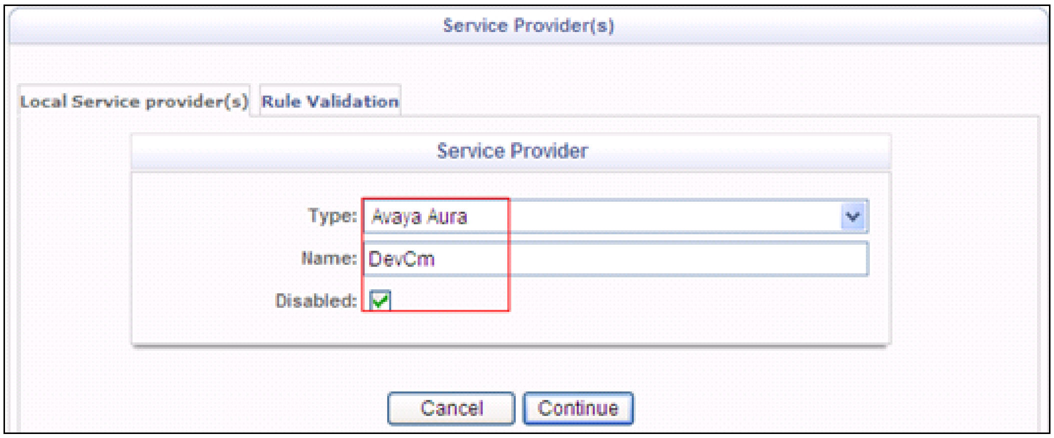
This section creates ASAI Service Provide which provides web services Third Party Call Control v2 and v2.4 such as “make call”, “Single Step Transfer” or “hang up call”.

Open a web browser and enter the following URL to view the ACE administrative console:
https://<hostname>:9449/oamp/

On the menu bar, choose **Configuration → Service Providers**. In the Service Providers window, click **Add** and enter the following information:

- **Type**: select **Avaya Aura** from the **Type** list.
- **Name**: enter a name for the Avaya Aura service provider.
- **Disable**: Select the **Disable** check box to add the service provider in a disabled state.

Click **Continue**.



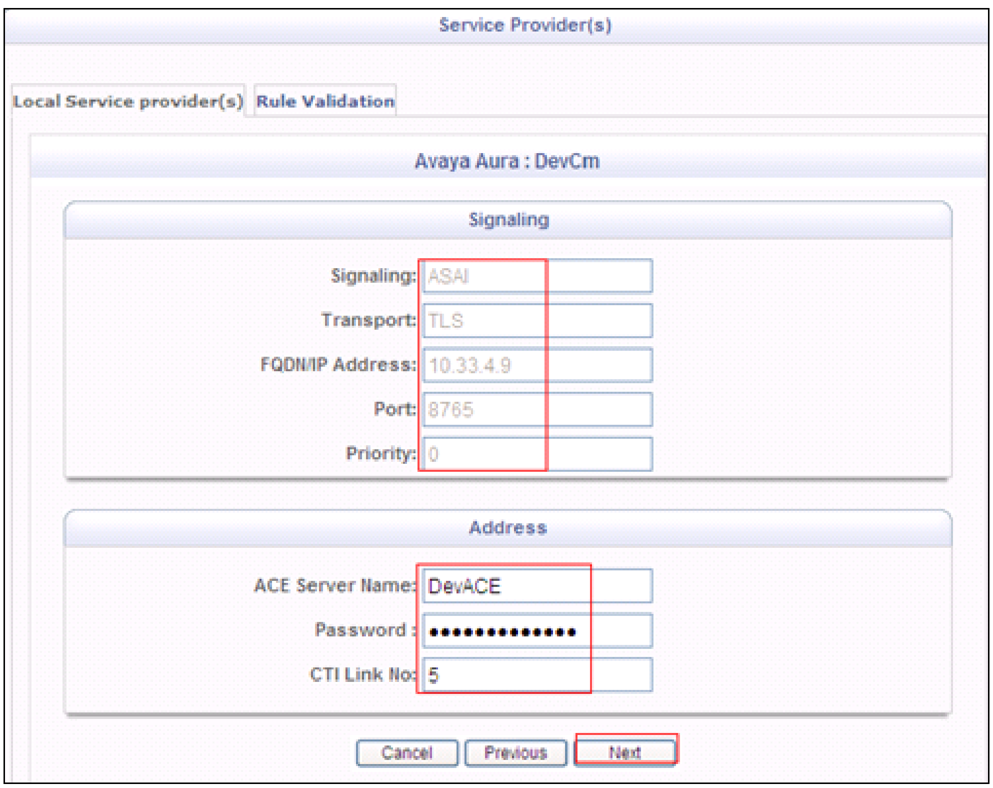
In the Service Providers window enter the following information for Signaling:

- **Signaling:** select **ASAI**.
- **Transport**: when ASAI selected, Transport is set to TLS.
- **FQDN/IP Address:** enter the IP address of the Communication Manager server. Using the fully qualified domain name (FQDN) is not supported for the Avaya Aura ASAI service provider.
- **Port**: when ASAI selected, the **Port** is set to **8765** and the **Priority** is set to **0**. 9. If you want to set the **Port** value to a non-default value, enter the number in the **Port** field.

In Address section, enter ACE server and CTI information created on Communication Manager in **Section 5.2**:

- **ACE Server Name:** enter ACE Server name. In compliance test name is DevACE.
- **Password:** enter password that created in **Section 5.2**.
- **CTI Link No:** enter CTI number created in **Section 5.2**.

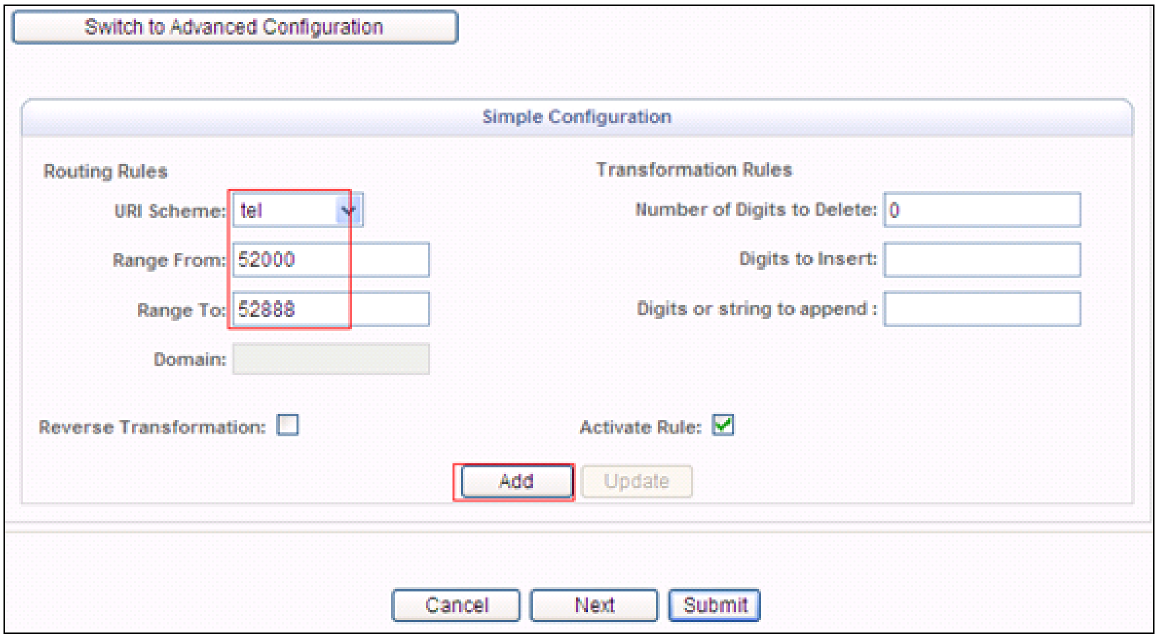
Click **Next** to add **Rules** for ASAI service provider.



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

- **URI Scheme**: **tel.**
- **Range from**: Enter a dialling plan of Communication Manager; example: **52000.**
- **Range to**: Enter a dialling plan of Communication Manager; example: **52888.**
- **Activate Rule**: checked.

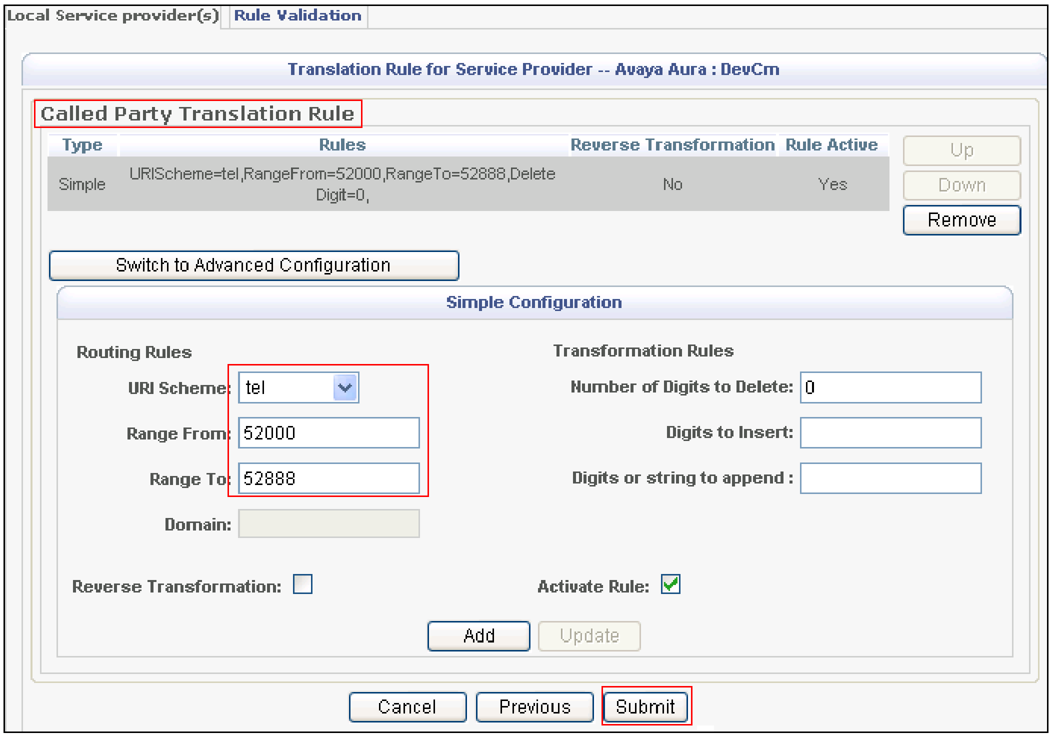
Click **Add** to add the new rule.



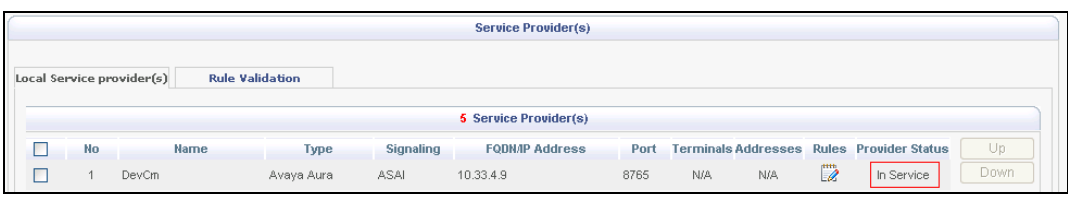
Click **Next** to add rule for Called Party. Enter information for **Called Party Translation Rule - Simple Configuration** rule as show below:

- **URI Scheme**: **tel**.
- **Range from**: Enter a dialling plan of Communication Manager; example: **52000**.
- **Range to**: Enter a dialling plan of Communication Manager; example: **52888**.
- **Activate Rule**: checked.

Click **Add** to add the new rule. Then click Submit to Submit new **Service Provider**.



Verify the status of service providers is “**In Service**”, as per the screen shot below.



8.3. Add User

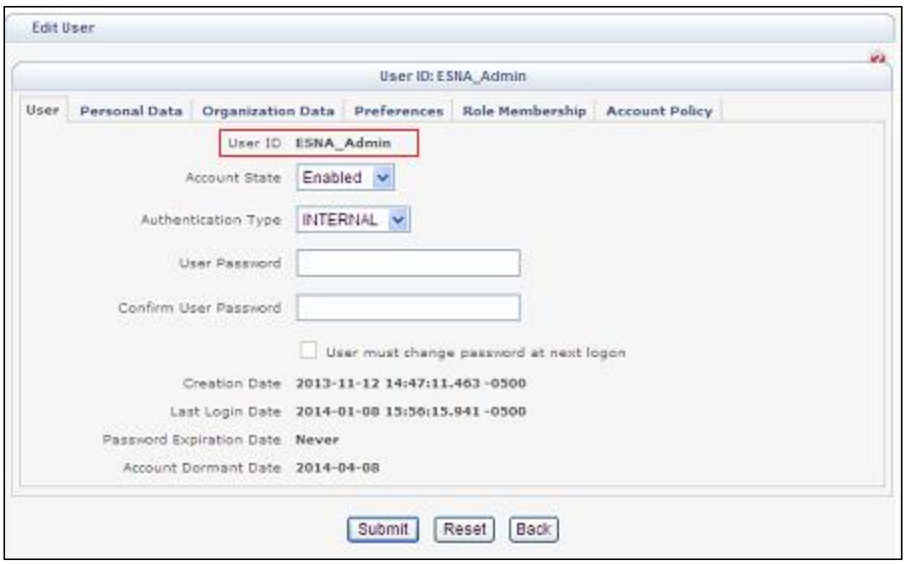
The web service client ESNA Officelinx – ACE Wizard is a configured user on ACE.

The web service client belongs to a role on ACE with a role type of **user** or higher, and with the appropriate access control rules configured for the Third Party Call Control (v2) service. See next section for steps on how to create new role for user.

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

- Enter **User ID**: User used to login ACE web service of the web client (application) (e.g ESNA_Admin).
- **Account State**: Enable.
- **Password**: password (e.g DevConnect@123).

Select **Submit** to create user. Below is the screen shot of ACE user detail used during compliance test.

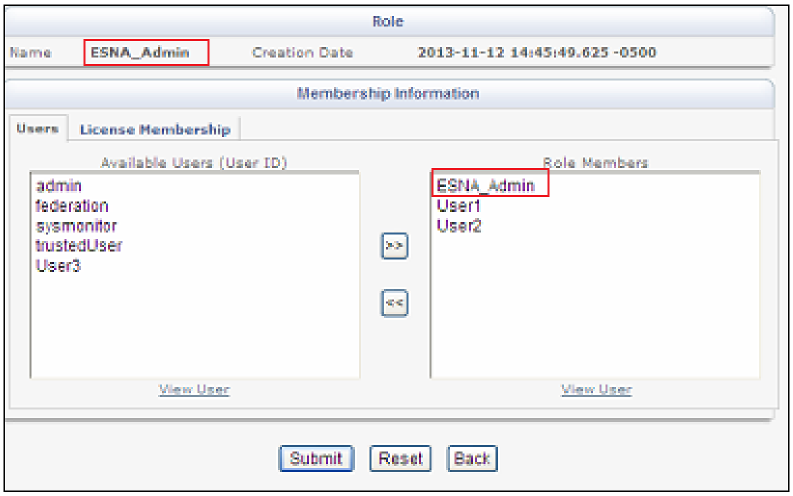


8.4. Add Role

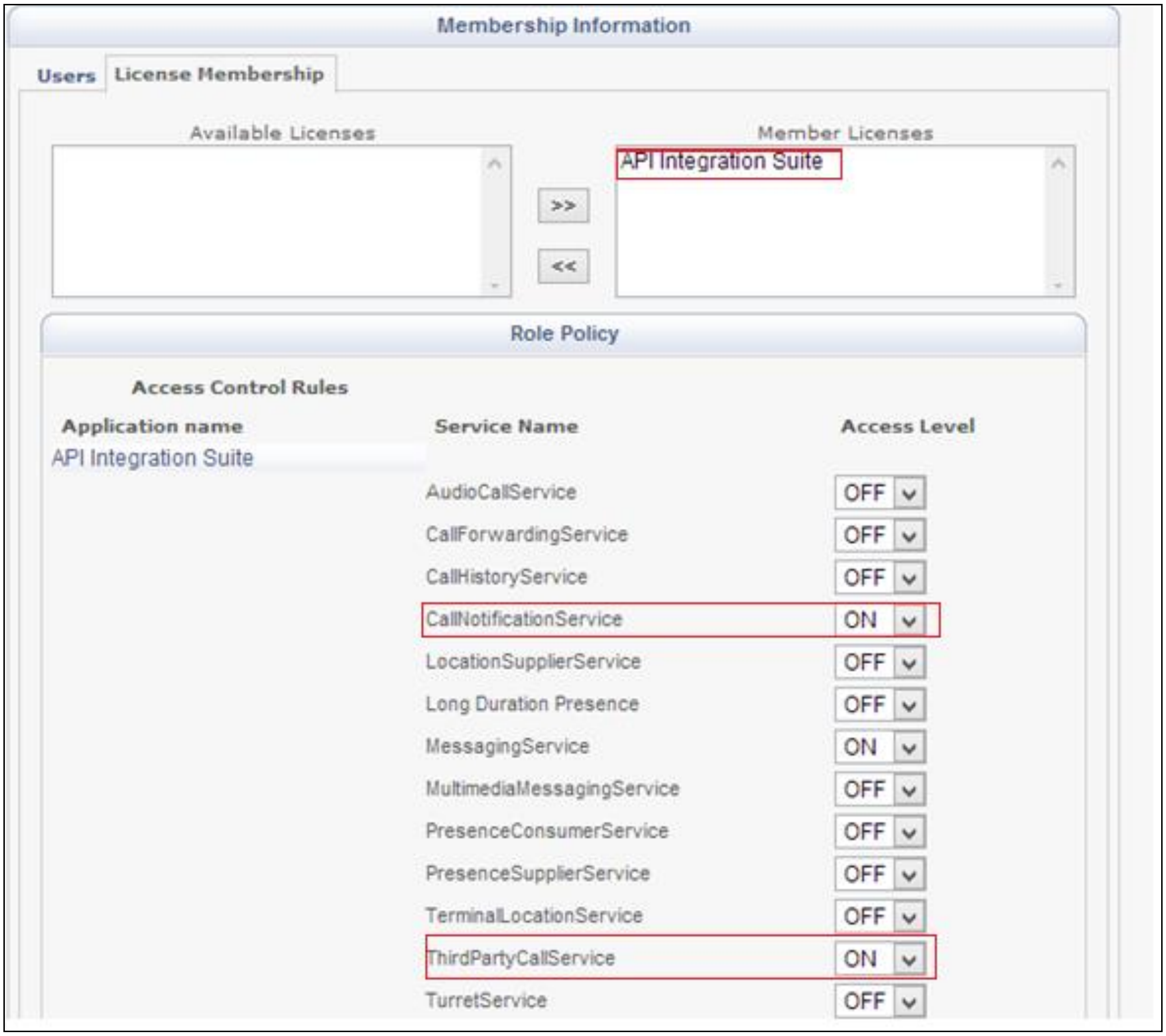
This section describes the step on how to create Role for user created in above section. Select **Security → Role Management → Create Role.** Enter the following for a new Role:

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

This is the screen shot of role that used during Compliance Test.



Click on **License Membership** tab, assign **API Integration Suite** license to **Member Licenses** (not shown). Turn **ON** the following services: **ThirdPartyCallService**, **CallNotification Service** of **API Integration Suite**. Click **Submit** to save changes.



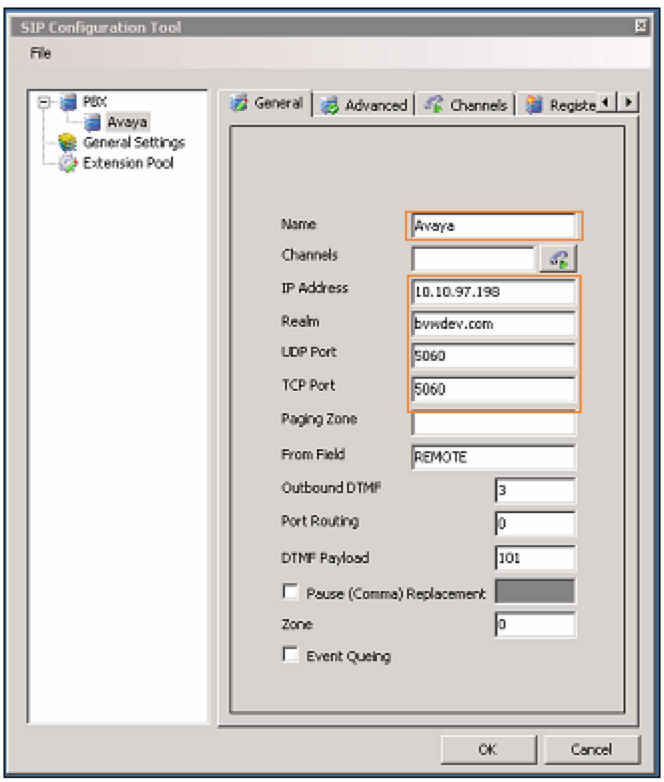
9. Configure the ESNA Telephony Officelinx

ESNA installs, configures, and customizes the Telephony Officelinx application for their customers. Thus, this section only describes the interface configuration, so that the Telephony Officelinx can talk to Session Manager, ACE and Messaging. See OL_CLIENT_APPS_GUIDE and OL_FEATURE_DESCRIPTION_GUIDE provide on ESNA website, see **Section 12** for the detail link.

9.1. Configure SIP Configuration Tool

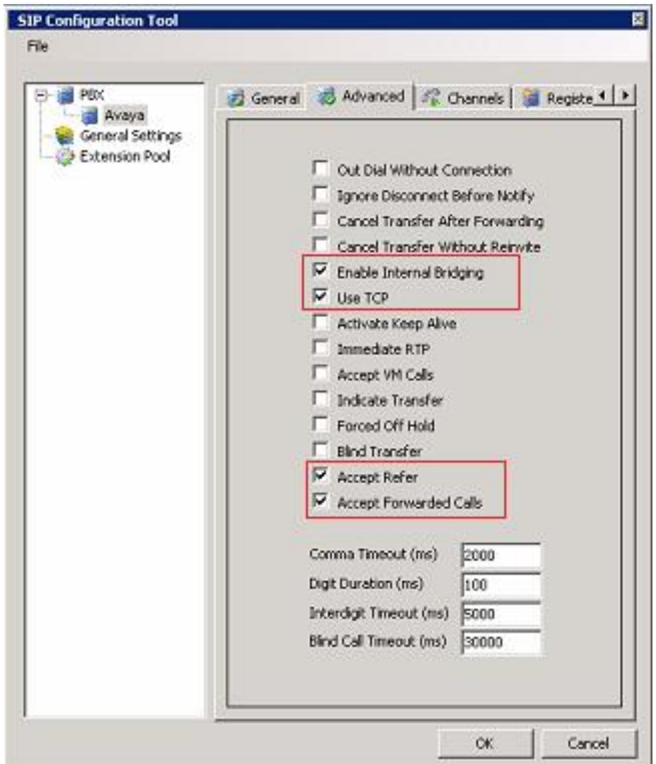
To configure ESNA Telephony Officelinx, navigate to **Start → All program → Telephony Officelinx Enterprise Edition → SIP Configuration Tool**. Select **Avaya** under PBX in the left pane. Provide the following information:

- **IP Address** – Enter **IP address** of **Session Manager**, example: **10.10.97.198**.
- **Realm** – Enter valid domain that configured in the system, example: **bvwdev.com**.
- **UDP Port** – Enter **5060**.
- **TCP Port** – Enter **5060**.

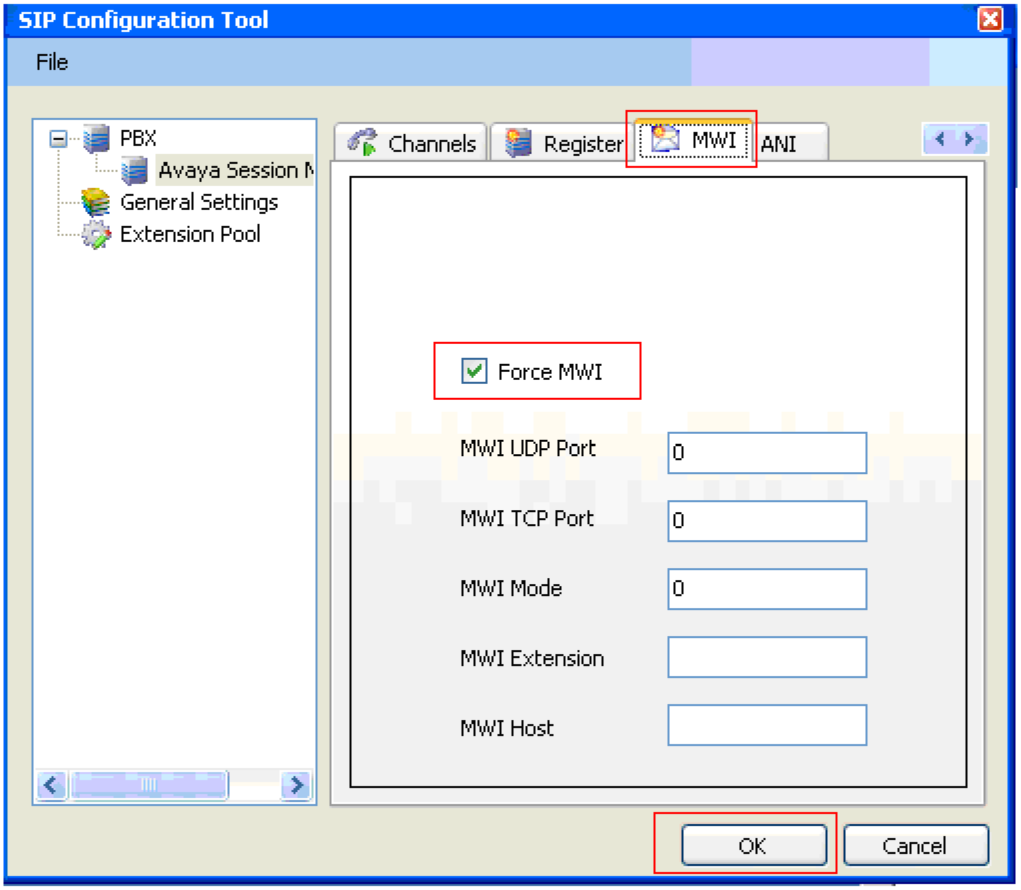


Click the **Advanced** tab in the right pane, and check the following check boxes:

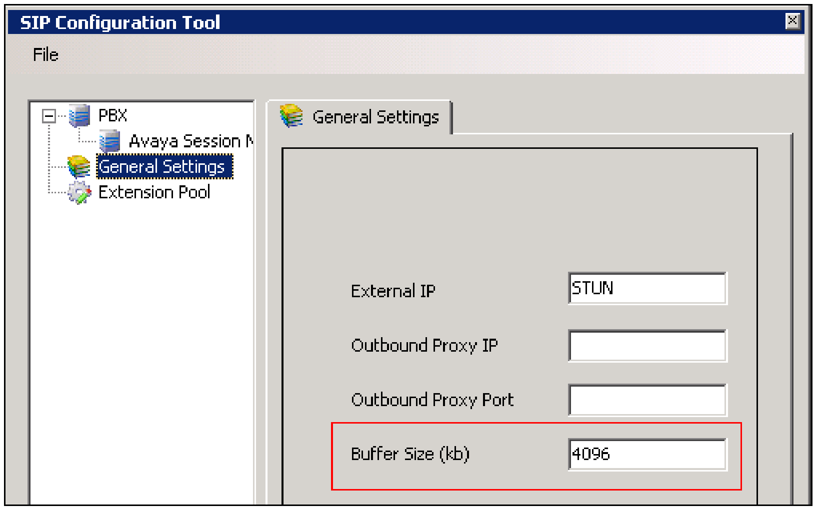
- **Enable Internal Bridging**.
- **Use TCP**.
- **Accept Refer**.
- **Accept Forward Calls**.



Click the **MWI** tab, and check the Force MWI check box. Click on the **OK** button.



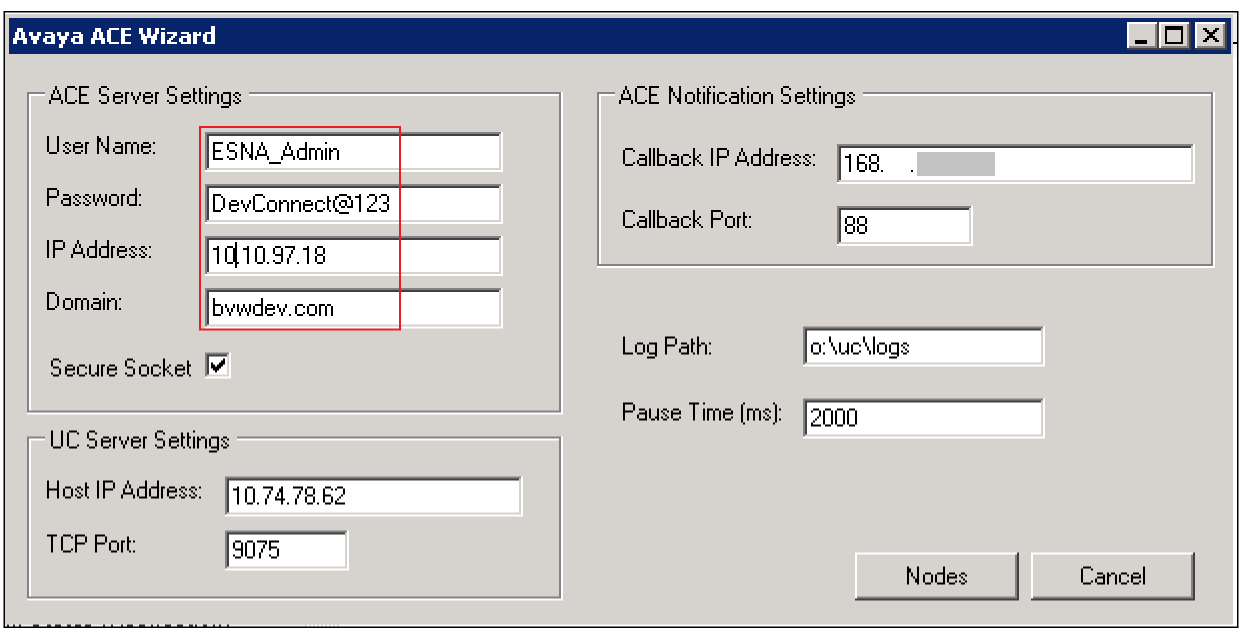
PBX – **General Settings**: **Buffer Size (kb)** =**4096**. This configuration allows Officelinx can handle SIP message sent from Session Manager.



9.2. Configure UC ACE Wizard

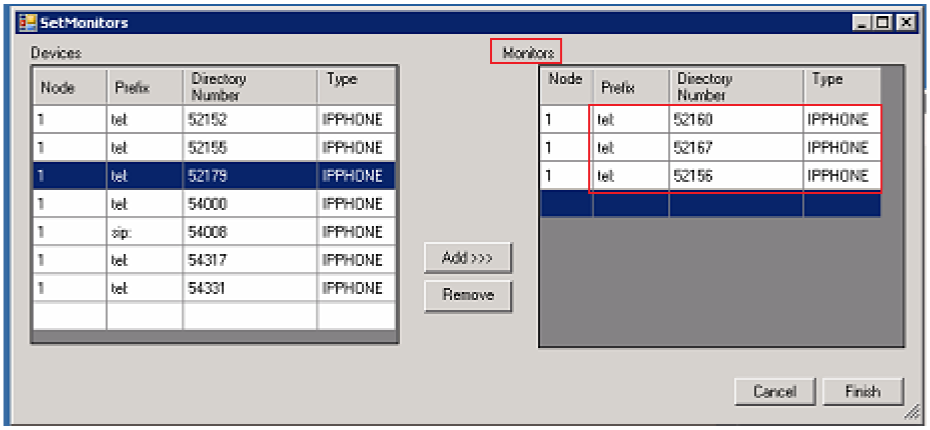
Double click on UC ACE Wizard shortcut to launch the setup window for Avaya ACE Wizard. Enter information as below:

- **User Name**: Enter user that created on ACE in **Section 8.3**.
- **Password:** the password for the ACE user created in **Section 8.3**.
- **IP Address:** ACE IP address.
- **Domain:** Enter domain name used in the system, during compliance test **bvwdev.com** used.



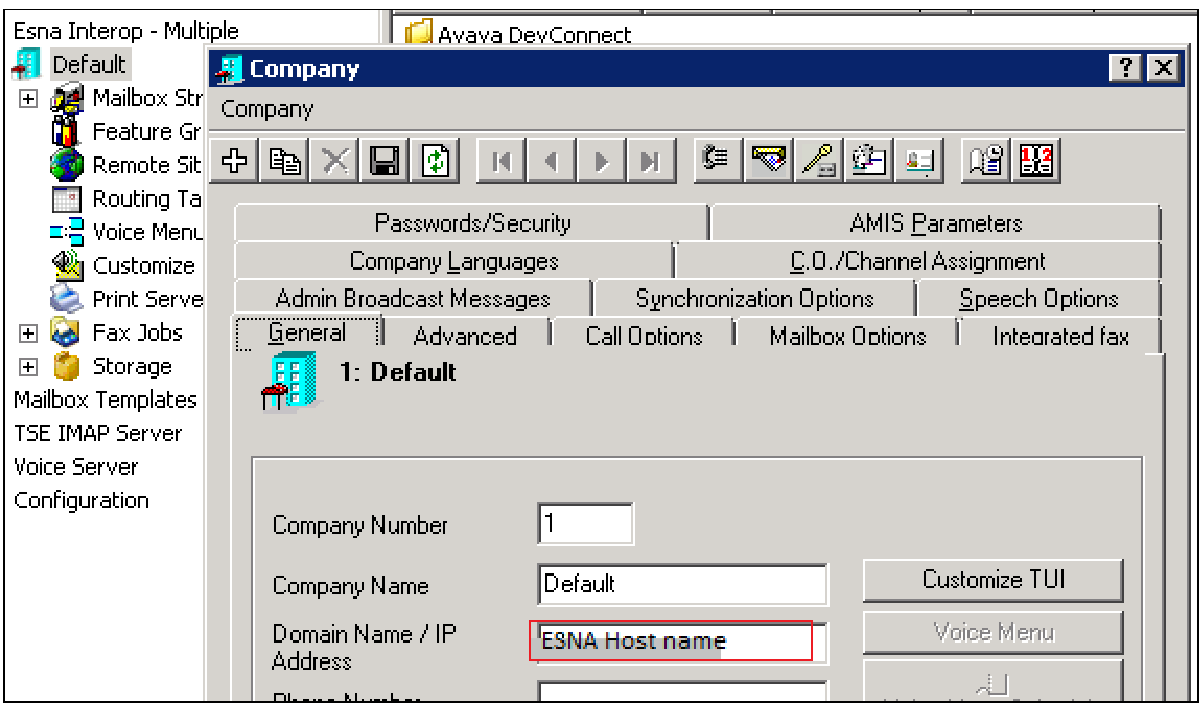
Click on Nodes (shown in previous screen shot) to open the next window where user manually enter device extension to get its notification. Click on Next button (not shown).

Select the list of device on the leftside and add it to the right window to start to monitor it. Or user can remove devide from monitor list by highlight select device and click remove.



9.3. Administer Company Profiles

In the **Company** window, modify the **Domain Name/IP Address** in FQDN format. This domain name is used in **Section 6.9** to configure Notify Me on Messaging.



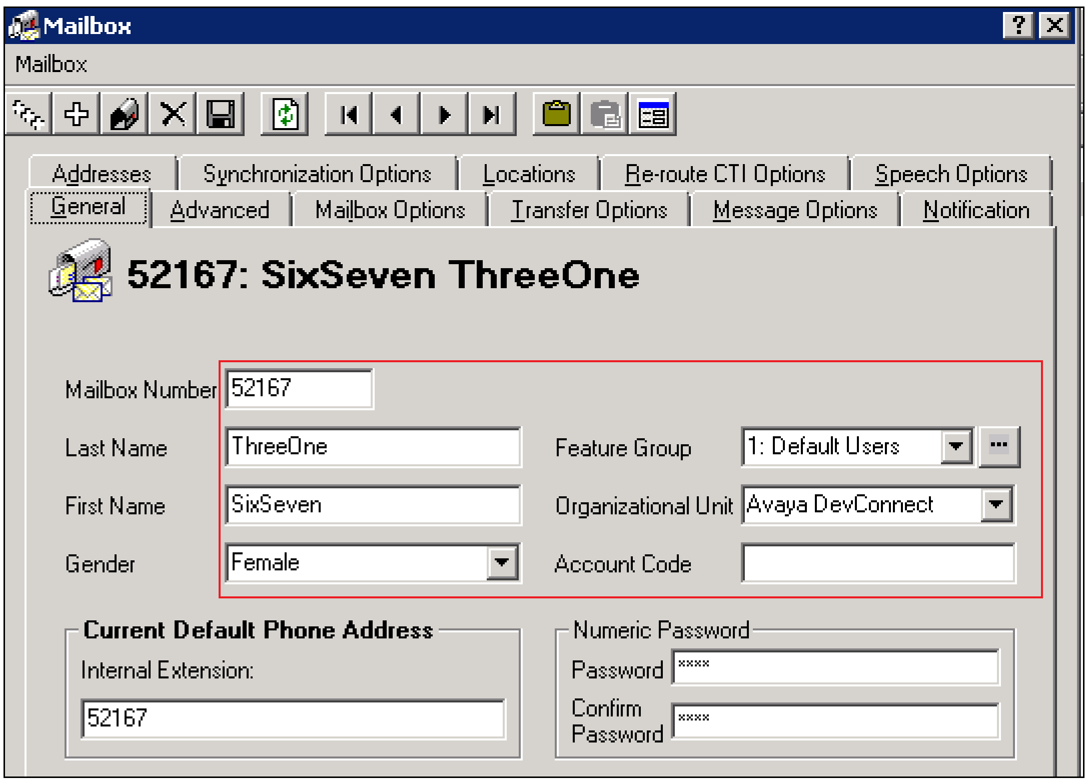
9.4. Configure User Mailbox in Officelinx Admin

Expand the **Officelinx → Esna Interop → Default → Mailbox Structure**. In the right panel right click on the window, select new to add new mailbox (not shown).

This section describes a sample configuration of mailbox 52167 for device 9608 H323 and this mailbox is linked to dev02@ESN Host name.

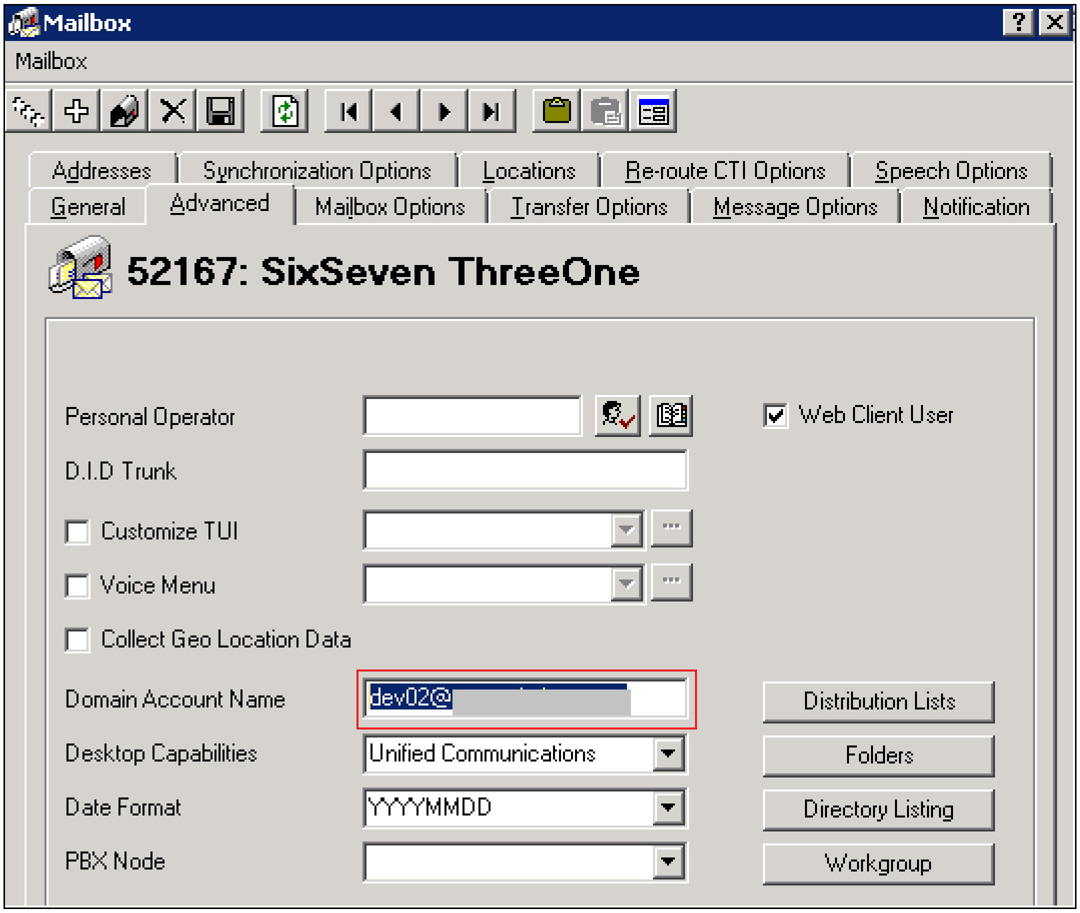
In **General** tab:

- **Mailbox Number**: enter the extension of physical device.
- **Feature Group**: select 1: Default Users; this is super group which setup to ensure that there are no conflicts between Officelinx and Gmail for more information please see document from ESNA in **Section 12**.
- **Last Name**: enter any name, example: **ThreeOne**.
- **First Name**: enter any name, example: **SixSeven**.



In **Advanced** tab:

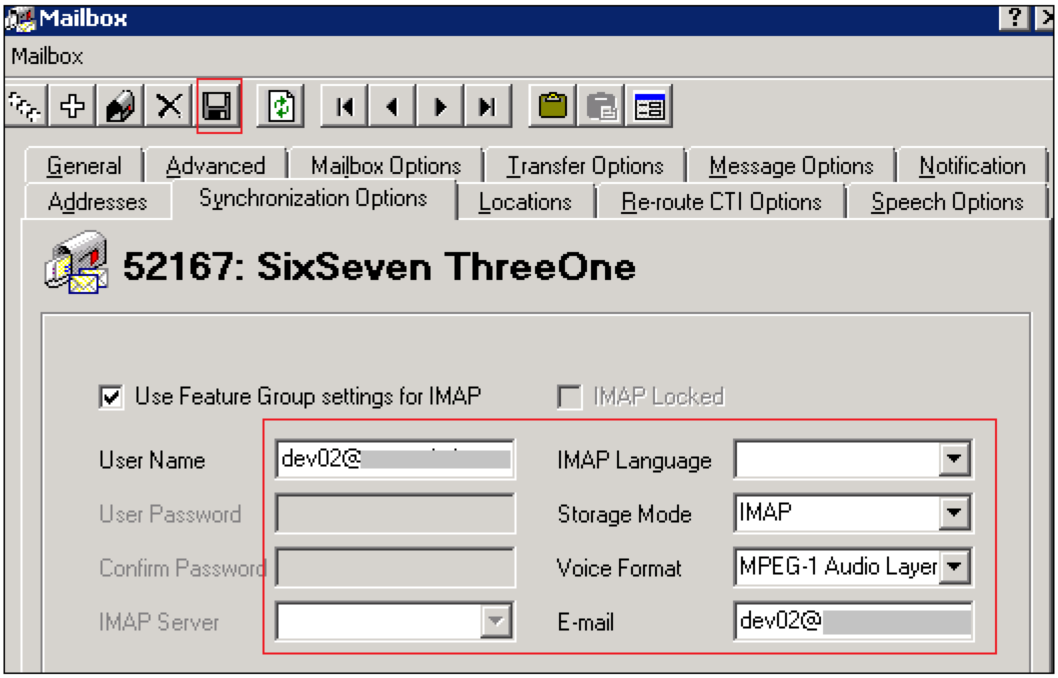
- **Domain Account Name**: enter **Gmail account** which connect to this mailbox dev02.
- **Desktop Capabilities**: select **Unified Communications**.



In **Synchronization Options** tab:

- **Use Feature Group setting for IMAP**: make sure this option is checked.
- **User Name**: enter google email account.
- **IMAP Language**: English.
- **Storage Mode**: IMAP.
- **Voice Format**: MPEG-1 Audio layer 3 (MP3).
- **E-mail**: enter google email account dev02.

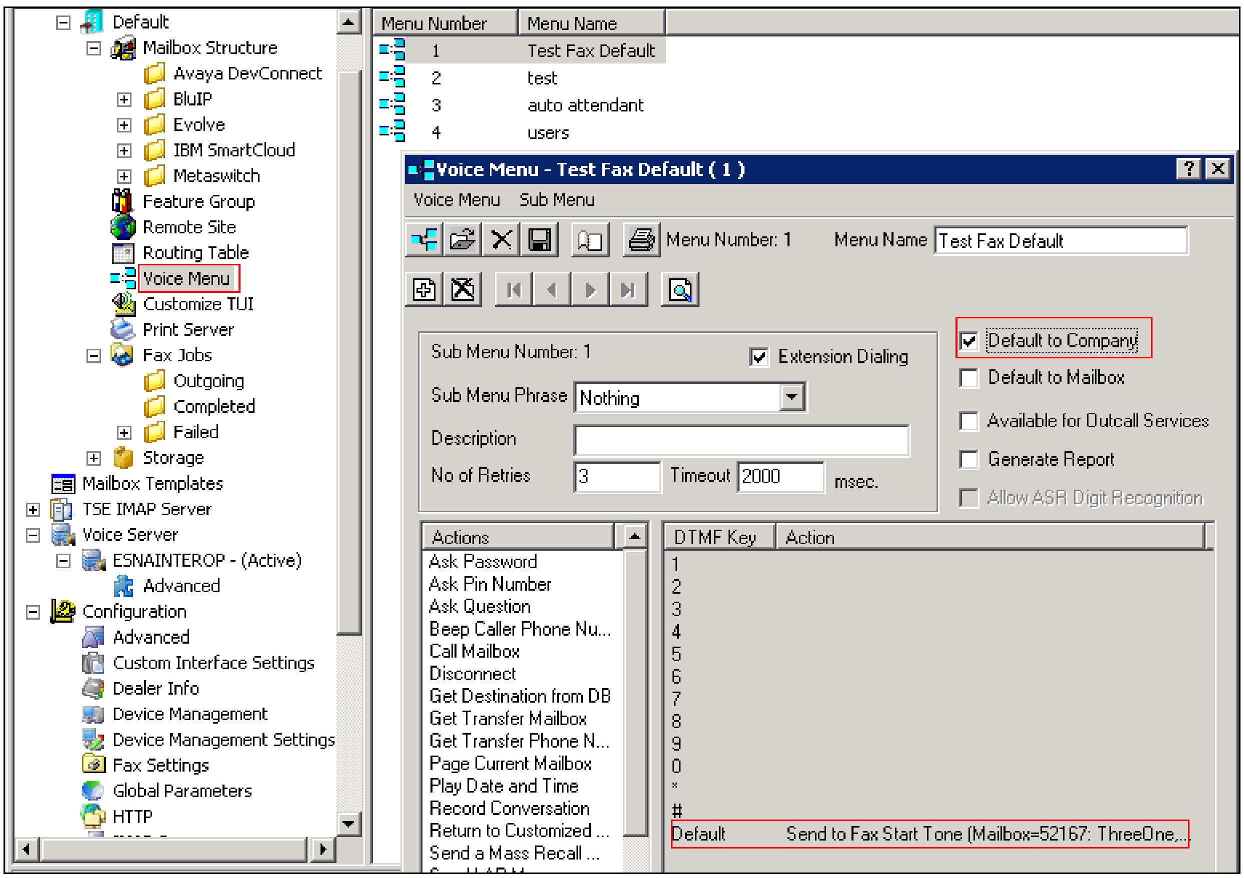
Click **Save** to save the changes.



9.5. Configure Fax

ESNA installs, configures, and customizes the Telephony Officelinx Fax Server for their customers. Please refer to ESNA Feature Description Guide, Chapters 18 and 19: Faxing and soft faxing. See Reference **Section 12** for detail. Thus, this section only describes the interface configuration used during compliance test, so that the user can send a fax-email from fax machine to iLink Pro user's mailbox. As there are more than one method of setting up fax, and ultimately it will depend on the nature of the enterprise fax requirements for setup and it is out of scope for this application note.

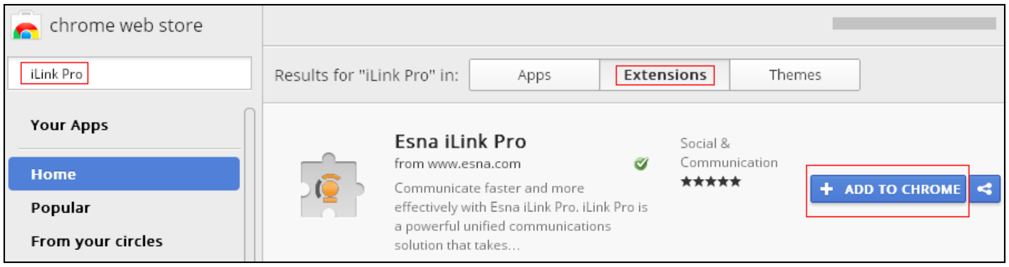
Expand the **Officelinx → Esna Interop → Default → Voice Menu.** Double click on Menu Number **1 – Test Fax Default.** Make sure **Default to Company** option is checked. Default: **Send to Fax Start Tone (Mailbox=52167…)** as shown in below figure:



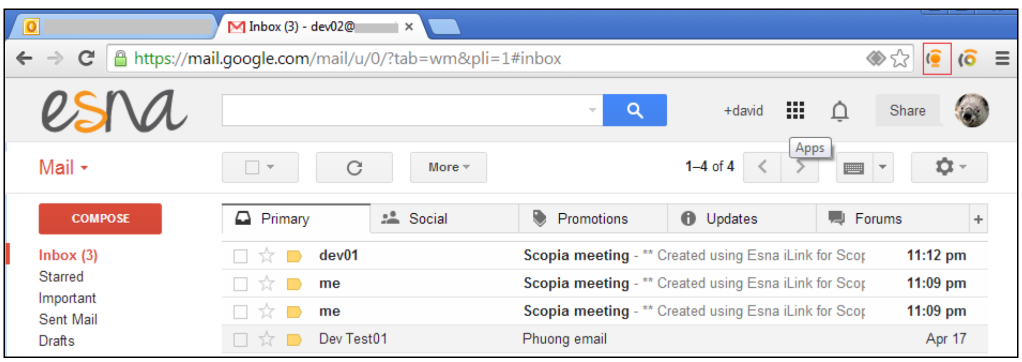
Note: This configuration was used because when the user sends a fax to Officelinx, there is no fax tone sent from the Officelinx Server and the fax on Communication Manager is waiting and as a result the fax get no answer, hence the "Default to Company" option with Default "Send to Fax start Tone" on Officelinx is checked in order for Officelinx send fax tone to fax machine.

9.6. Install and Configure iLink Pro

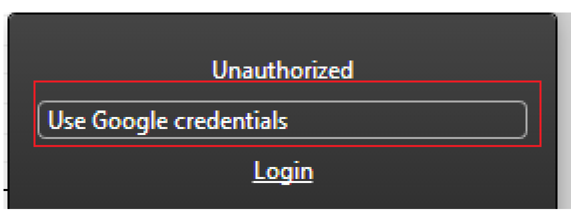
Note that iLink Pro is the google application made by ESNA this can be found in Google Store. Using Google Chrome browse to Chrome store. Perform the search for **iLink Pro**. Select **Extension** tab. Click on **Add to Chrome** to install **ESNA iLink Pro**. Follow the instruction to install **iLink Pro**.



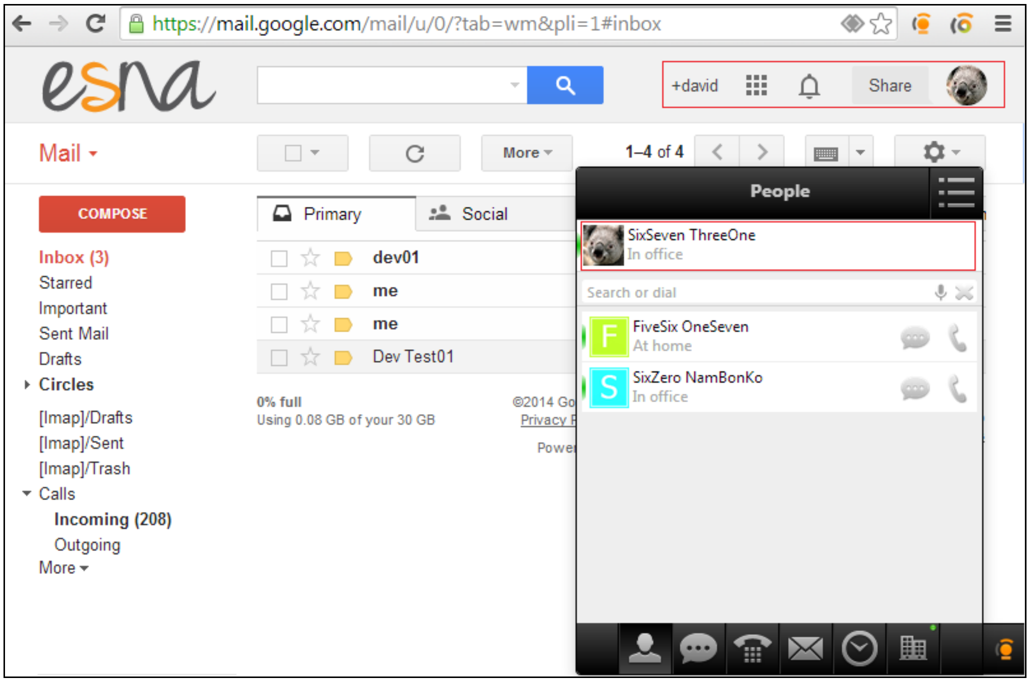
In Chrome browser, user login as **dev02@googleaccount.com**. Click **on iLink Pro** icon to launch iLink Pro.



On the log in credentials to login iLink Pro, select **Use Google credentials**. Click **Login**.



Following the instruction on the web grant access and login iLink Pro (not shown). Below is the screenshot of iLink Pro login successfully using dev02@googleaccount has Esna Officelinx mailbox name **SixSeven ThreeOne**, see account detail setup in Section **9.4** .



10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, ACE, Messaging and ESNA Officelinx and iLink Pro application.

10.1. 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 to verify that the SIP signaling group is **in-service**.
- From the Communication Manager SAT, use the **status trunk-group** xxx command to verify that the SIP trunk group is **in-service**.
- Verify with the **list trace tac** xxx command that calls are using the correct trunk, coverage.
- 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
```

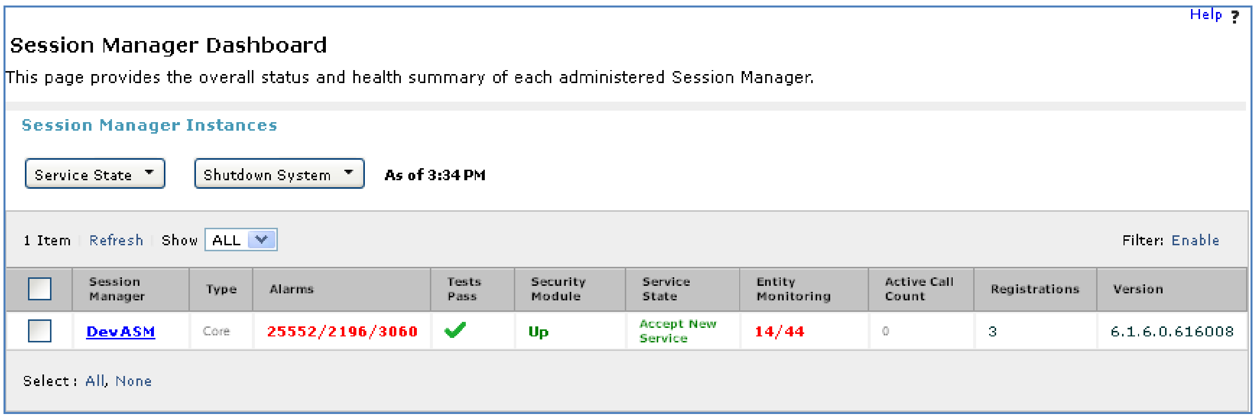
10.2. Verify Avaya Aura® Session Manager

This section describe the steps need to verify that Session Manager is operational.

10.2.1. Verify Avaya Aura® Session Manager is Operational

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 .

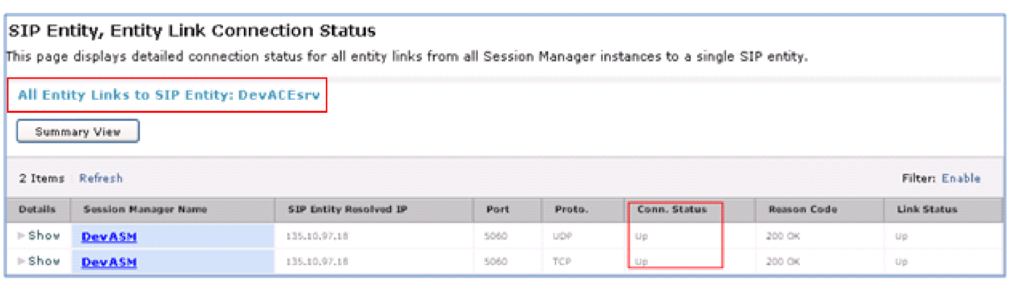


10.2.2. Verify SIP Entity Link Status

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

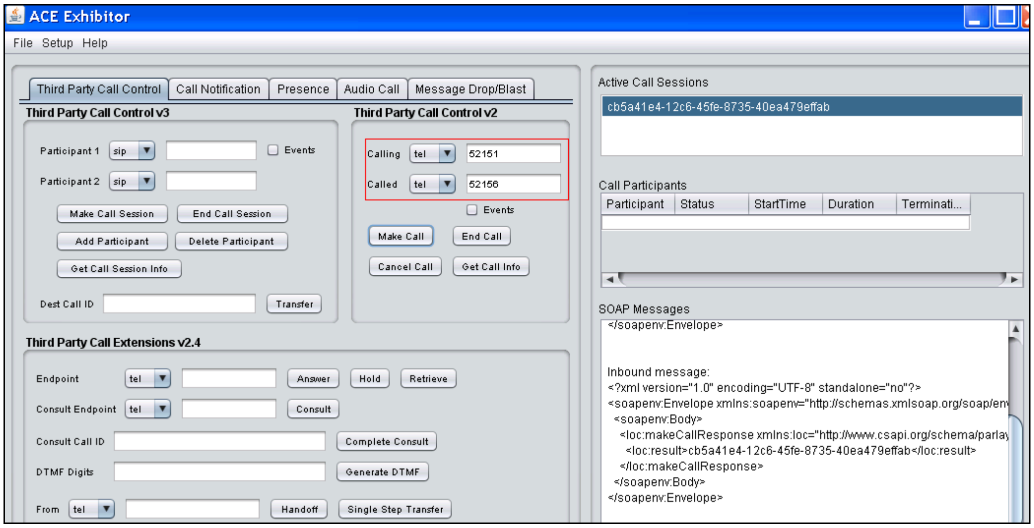
In the **All Entity Links to SIP Entity: DevACEsrv** table, verify the **Conn. Status** for the link is "**Up**" as shown below.



Repeat the same step to verify the status of Messaging and Communication Manager are "Up".

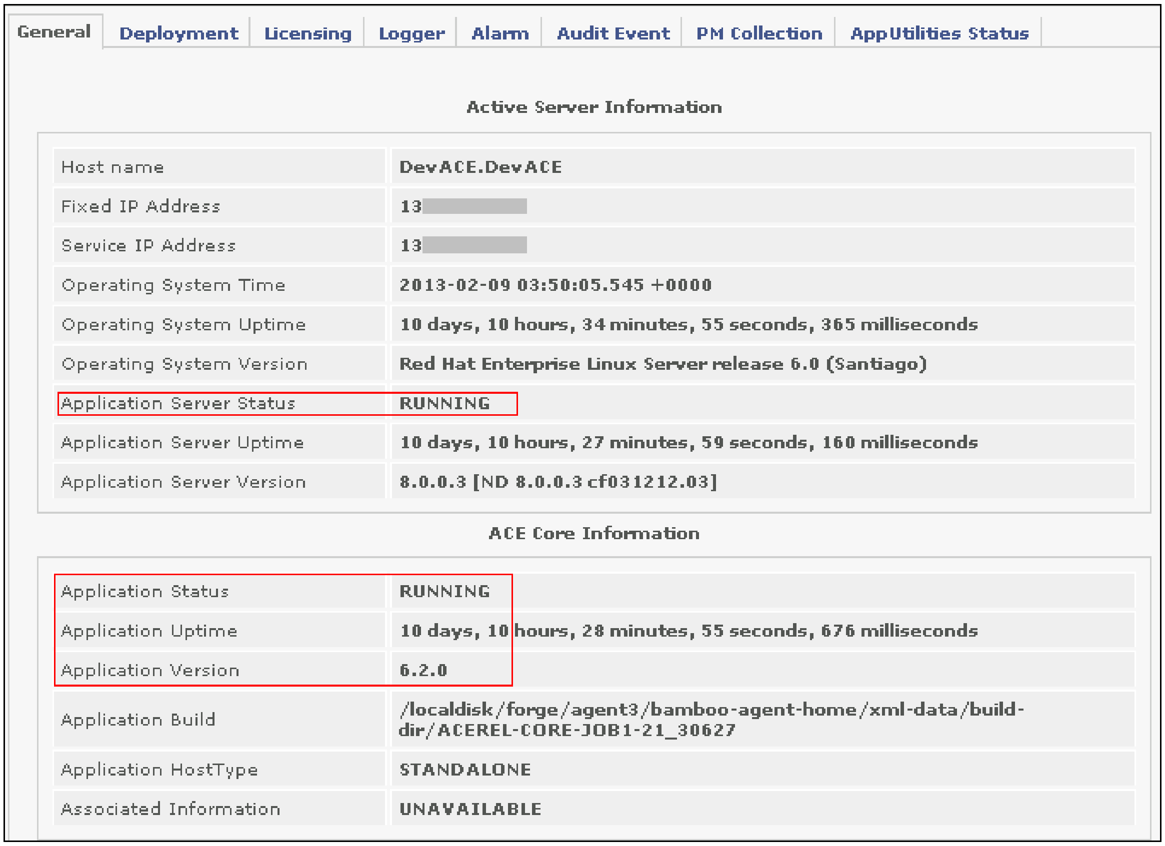
10.3. Verify Avaya ACE

Perform a call using ACE_EXHIBITOR or SOAP UI software, below is an example of using ACE Exhibitor: make a call from **52151** to **52156**:



10.3.1. Verify Avaya ACE Server Status

To verify the status of ACE server, select **Configuration → Server** to verify status of server.



10.4. Verify Avaya Aura® Messaging

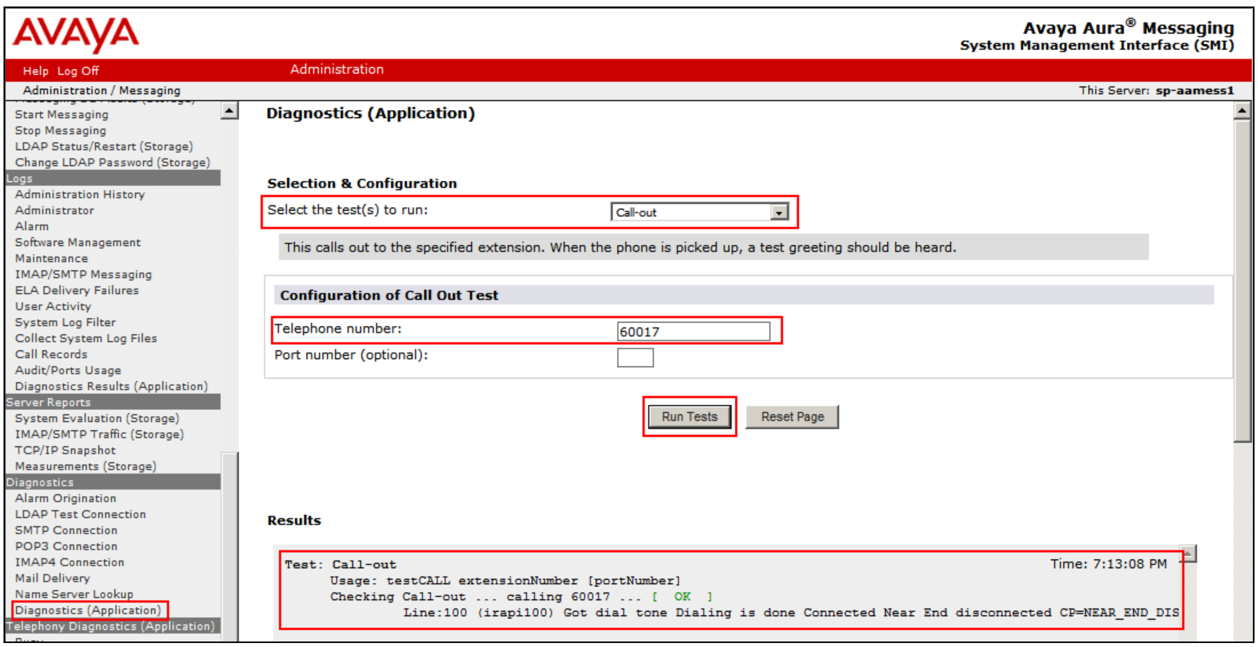
The following section will describe the steps required to verify the connection of messaging.

10.4.1. Verify Avaya Aura® Messaging Can Make Calls to Phones

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

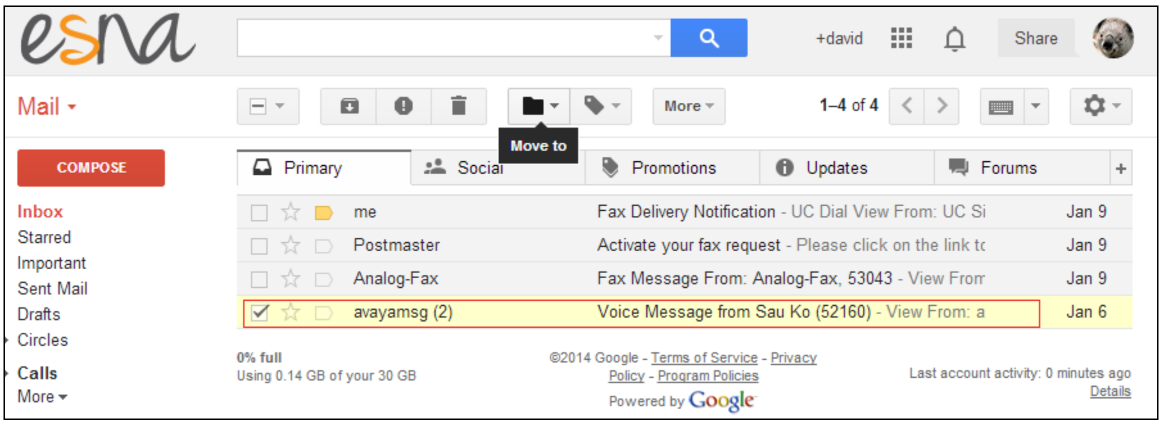
- **Select the test(s) to run:** Select **Call-out** from the drop down menu.
- **Telephone number:** Enter the number to call.

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 indicating that the call was ok as shown below.



10.4.2. Verify user can Receive and Retrieve Avaya Aura® Messaging Voice Message using Google Mail

Make a call from an iLink Pro to another device. Verify that the call covers to Messaging upon no answer. Leave a voice message. Verify that the MWI light of the called phone turns on. Log on ESNA Google mail account of called user verify that user got the message from Messaging and able to listen to the voice message. Verify that the MWI light turns off. (Notes: At this version of Officelinx 9, when messages are read, Officelinx should attempt to extinguish MWI via SIP if possible. This will not reflect actual message status on Messaging. The example below shows that the user has an incoming voice message in the mailbox.

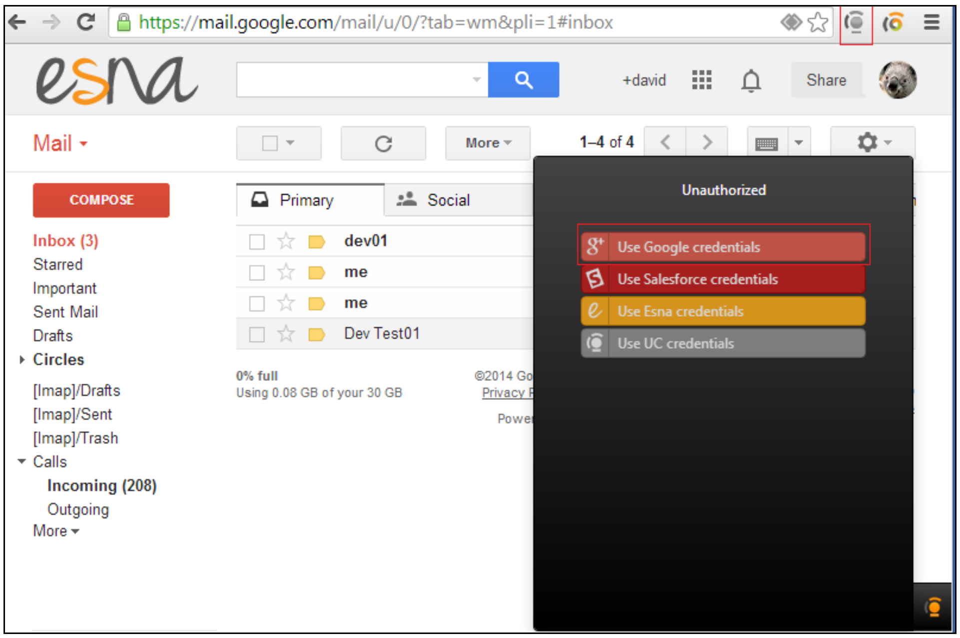


10.5. Verify ESNA Officelinx Server and iLink Pro

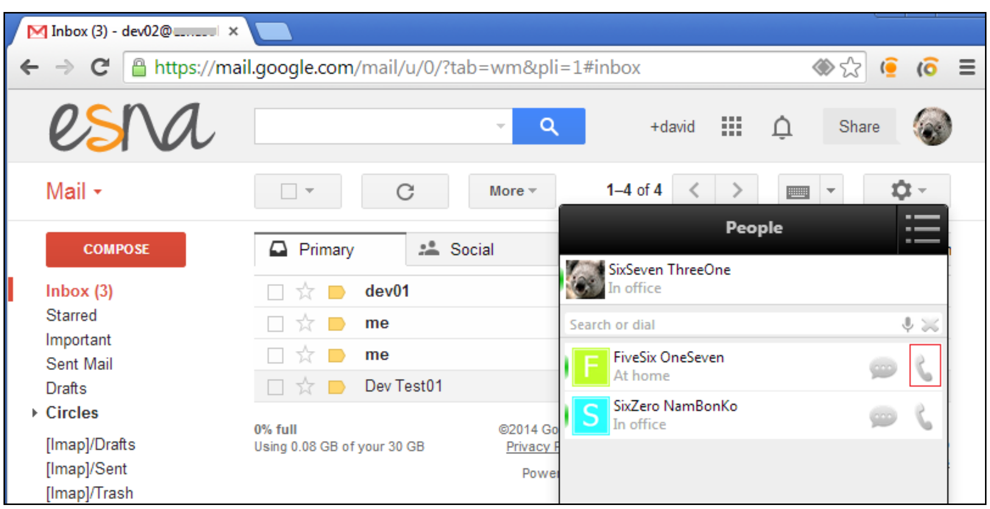
This section describes the steps to verify that user able to make a call using iLink Pro, send fax through Google email account.

10.5.1. Verify User can make a Call Using iLink Pro

Click on iLink Pro icon on Chrome browser to launch application. Select Use Google credential as shown below:



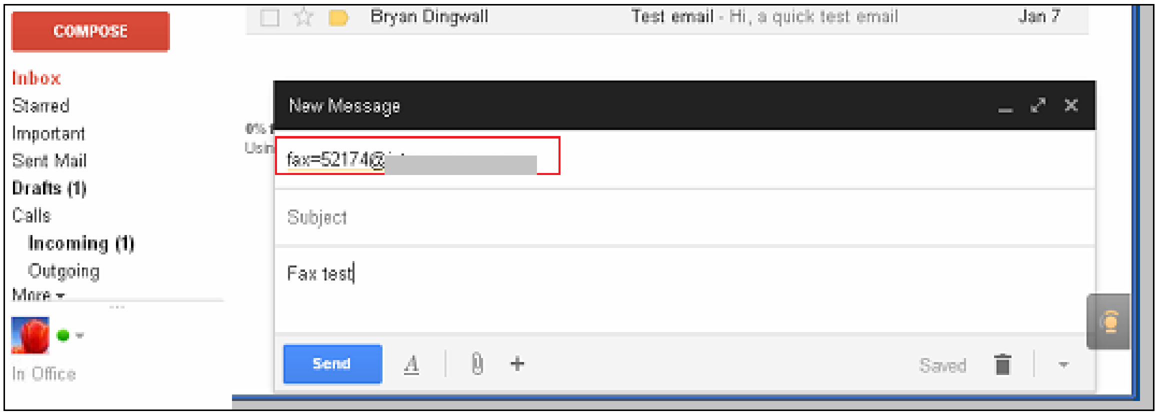
Follow the instruction on the web to select Google account to login, in this case dev02 account is selected and follow to screen to grant access right to the application (not shown). Verify that user successfully login iLink Pro with dev02@googleaccount. Make a call to another user by click on the phone icon beside user name (shown below).



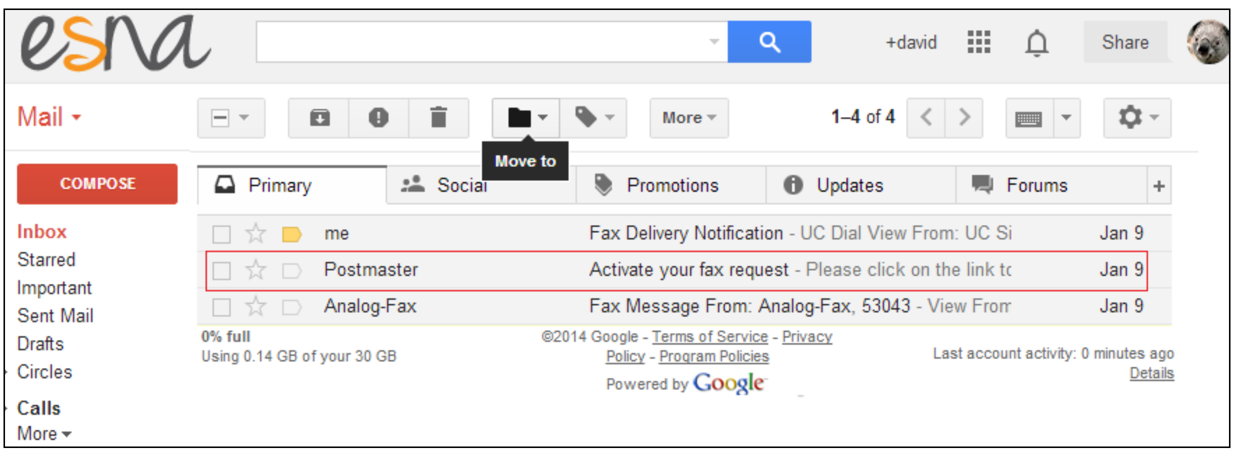
Verify that the devices of calling and called user are ringing. Verify that the called user answers the phone and that two-way voice path is established.

10.5.2. Verify user can send fax through email

In the Google mail, click **Compose** to start a new message. In the **To**: field, enter the fax a full fax address, example during the compliance test, fax=52174@ESNAHostname is used. Enter subject and fax content, click **Send**.



Verify that user will received an email from Officelinx to ask user activate the fax request. Click on the provided link to confirm.



Verify that the fax machine able to receive and print out the fax content.

11. Conclusion

Interoperability testing of Avaya Aura® Agile Communication Environment 6.2.2, Avaya Aura® Messaging 6.2, and Avaya Aura® Communication Manager 6.3 with Officelinx 9 SP1 – iLink Pro was completed and passed with the list of observations are noted in **Section 2.2**.

12. 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).

The following document was provided by ESNA:

1. http://documents.esna.com/home/officelinx-9-1/9-1-primary-documents

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.