Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the ESNA Office-LinX™ Cloudlink™ Edition UC Client Manager with Avaya Agile Communication Environment™, Avaya Aura® Messaging and Avaya Aura® Communication Manager 5.2.1 - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the ESNA Office-LinX™ Cloudlink™ Edition UC Client Manager to interoperate with Avaya Agile Communication Environment™, Avaya Aura® Messaging and Avaya Aura® Communication Manager.

The Telephony Office-LinX™ Cloudlink™ Edition UC Client Manager is a SIP-based voice processing system that functions with an organization's existing telephone system to enhance its overall telecommunications environment.

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.

©2011 Avaya Inc. All Rights Reserved.

Table of Contents

1. INTRODUCTION 6

2. GENERAL TEST APPROACH AND TEST RESULT 6

2.1. Interoperability Compliance Testing 6

2.2. Test Results 6

2.3. Support 7

3. REFERENCE CONFIGURATION 8

4. EQUIPMENT AND SOFTWARE VALIDATED 9

5. CONFIGURE AVAYA AURA® COMMUNICATION MANAGER 9

5.1. Configure SIP trunk between Avaya Communication Manager and Session Manager 9
5.1.1. Capacity Verification 10
5.1.2. IP Codec Set 10
5.1.3. Configure IP Network Region 11
5.1.4. Configure IP Node Name 12
5.1.5. Configure SIP Signaling 12
5.1.6. Configure Trunk Group 13
5.1.7. Configure Route Pattern 14
5.1.8. Administer Dialplan 14
5.1.9. Administering an extension number for the station that an Office-LinX application monitors 15
5.1.10. Configure Hunt Group for Avaya Aura Messaging 16
5.1.11. Configure Coverage Path to Avaya Aura Messaging 17
5.1.12. Administer a Station for Coverage to Avaya Aura Messaging 17
5.1.13. Configure Hunt Group for ESNA Office-LinX 18
5.1.14. Configure Coverage Path to ESNA Office-LinX 19

5.2. Configure CTI link between Communication Manager and AE Server 19
5.2.1. Verify license 20
5.2.2. Enable Processor Ethernet 20
5.2.3. Enable AE Services change ip-services. 21
5.2.4. Add a CTI link 22
5.2.5. Method for adding DMCC Softphone to the network region 22
5.2.6. Administer media gateway 23
5.2.7. Verify a media processor circuit pack 23

6. CONFIGURE AE SERVER 24

6.1. Verify Device and Media Call Control API Station licenses 24

6.2. Configure Switch Connection: Add switch, edit IP, H323 Gatekeeper 25

©2011 Avaya Inc. All Rights Reserved.

6.3. Enable TR8/7 Port 27
6.4. Enable TR/87 service setting 28
6.5. Configure dialing plan 29
6.6. Add TSAPI link 29
6.7. Checking the status of a switch connection from Communication Manager to the AE Server 31
6.8. Checking the status of a switch connection -- from the AE Server to Communication Manager 31
7. CONFIGURE AVAYA AURA® MESSAGING 31
7.1. Administer Sites 32
7.2. Administer Telephony Integration 33
7.3. Configure Dial Rules 34
7.4. Configure Class of Service 35
7.5. Administer Subscribers 36
7.6. Administer Topology 38
7.7. Administer External Host 39
7.8. Configure Notify Me 40
8. CONFIGURE AVAYA AURA® SESSION MANAGER 40
8.1. Configure SIP Domain 40
8.2. Configure Locations 41
8.3. Configure SIP Entities 42
8.4. Configure Entity Links 43
8.5. Time Ranges 44
8.6. Configure Routing Policy 45
8.7. Dial Patterns 45
8.8. Synchronization Changes with Avaya Aura® Communication Manager 46
9. CONFIGURE AVAYA ACE 3.0 47
9.1. Administer certificate 48
9.1.1. Creating a directory for the OpenSSL CA files 48

©2011 Avaya Inc. All Rights Reserved.

9.1.2. Creating an OpenSSL configuration file 49
9.1.3. Generating a CA certificate 49
9.1.4. Create a server certificate request for AE Services 50
9.1.5. Creating the ACE certificate request 52
9.1.6. Signing an AES certificate request 52
9.1.7. Signing an ACE certificate request 53
9.1.8. Importing the server certificate into AE Services 53
9.1.9. Add Trusted Host 56

9.2. Certificate management using the IBM Integrated Solutions Console for ACE on Linux 56
9.2.1. Creating a key store using the IBM Integrated Solutions Console 57
9.2.2. Export ACE server cert 60
9.2.3. Administer Keystore 60
9.2.4. Restart Avaya ACE and AE server 63

9.3. Add Service Provider 64
9.3.1. Add AE server provider using TR87 service 64
9.3.2. Add Session Manager as a service provider in Avaya ACE 66

9.4. Add user 67

9.5. Add Translation rule to Service Provider 68

10. CONFIGURE THE ESNA TELEPHONY OFFICE-LINX 69

10.1. Configure SIP Configuration Tool 69

10.2. Configure UC ACE Wizard 72

10.3. Configure user mailbox in Office-LinX Admin 74

10.4. Install and Configure UC Client Manager Application 74

11. VERIFICATION STEPS 75

11.1. Verify Avaya Aura® Communication Manager 75

11.2. Verify Avaya Aura® Session Manager 76
11.2.1. Verify Avaya Aura® Session Manager is Operational 76
11.2.2. Verify SIP Entity Link Status 76

11.3. Verify AE Server 77
11.3.1. Verify Services are running. 77
11.3.2. Verify DMCC Service Summary – Session Summary 77
11.3.3. Verify AE Server and Avaya ACE are Communicating 78
11.3.4. Verify AE Server and Switch are talking 79

11.4. Verify Avaya ACE 80
11.4.1. Verify Service Provider status in Avaya ACE 80
11.4.2. Verify Avaya ACE Server status 80

11.5. Verify Avaya Aura Messaging 80

©2011 Avaya Inc. All Rights Reserved.

11.5.1. Verify Avaya Aura Messaging can make a call to phones 80
11.5.2. Verify user can receive and retrieve Avaya Aura Messaging voice message on ESNA Web Client: 81

11.6. Verify ESNA Office-LinX server and UC Client Manager. 82
11.6.1. Verify the log file UCServer of ESNA Office-LinX. 82
11.6.2. Verify UC Client Manager – Desktop 82

12. CONCLUSION 83

13. ADDITIONAL REFERENCES 84

©2011 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedure for configuring ESNA Office-LinX, Avaya Agile Communication Environment™, Avaya Aura® Communication Manager and Avaya Aura® Messaging solutions.

The Telephony Office-LinX™ Cloudlink™ Edition UC Client Manager is a software application that allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). Esna Office-LinX controls a physical telephone using third-party call control, specifically the Third Party Call (v2), Call Notification web service of Avaya ACE.

Additionally, ESNA Telephony Office-LinX provides unified messaging and integration services between the ESNA Telephony Office-LinX system and other messaging systems. Using a combination of IMAP4, MAPI and Web Services based protocols, the unified messaging system provides an easily manageable and highly scalable system that supports message, calendar and contact synchronization on a broad range of messaging platforms including Microsoft Exchange, Google G-mail, Lotus Domino, Novell Groupwise and others.

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 will be to verify the integration of the Esna Office-LinX with Avaya IP and digital phones. Phone operations such as off-hook, on-hook, dialing, answering, etc. will be performed from the physical phones and from the Office-LinX application. In addition, phone displays and call states on the physical phones and Esna Office-LinX application will be verified for consistency.

2.2. Test Results

The following testing was covered successfully:

- Click and call on UC Client Manager and the voice path is established on 2 physical phones.
- Off-hook and on-hook a device, phone states are consistent with its associated physical phone states.
- Put a call on hold and retrieve call.
- Transfer a call.
- Retrieve the Avaya Aura Messaging voice message from web client (SMTP replay).
- Redirect call

©2011 Avaya Inc. All Rights Reserved.

- Leave messages for subscribers and retrieve the message through the web client.
- Message Waiting Indication (MWI).
- DTMF using the voicemail.
- G.711MU and G.711A codec's.

The following was observed during testing:

- Cannot perform transfer using UC Client Manager Call control, ESNA UC Client user lost their Call Control due to receive unexpected OnDisconnect. This issue is intermittent and targetted to be fixed in the next ACE release.
- Lost call control while using the Hold button, Fail to start Call Notification when there is an unavailable device in the UCACEWizard list; cannot perform transfer using UC Client Manager and the current call is put on hold. These issues are being investigated by ESNA.
- Cancel Call and Call Forward are not available in this version of Office-LinX.

2.3. Support

Technical support for the ESNA Telephony Office-LinX solution can be obtained by contacting ESNA:

- URL – techsupport@esna.com
- Phone – (905) 707-1234

©2011 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with a Session Manager and an Avaya S8300D Server with an Avaya G450 Media Gateway. Endpoints include Avaya 9600 Series H.323 Telephones

.

ESNA Telephony Office-LinX does not register with the Session Manager as an endpoint but instead is configured as a trusted SIP entity.

A user is able to click and call through the UC Client Manager app as well as received and check voice message from Avaya Aura Messaging from the web client.

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

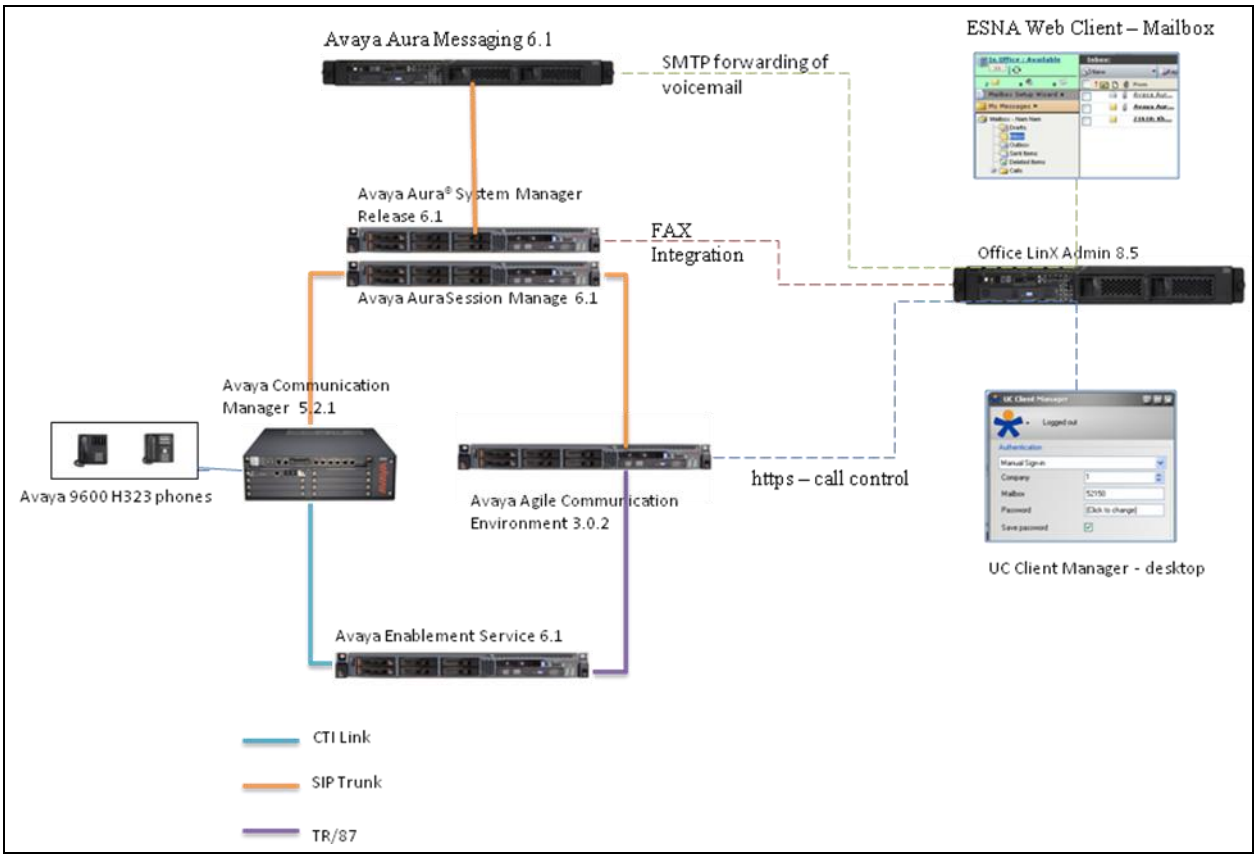


Figure 1: Test Configuration

©2011 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Media Server with Avaya G450 Media Gateway	Avaya Aura® Communication Manager 5.2.1 with latest Service Pack
Avaya Aura® System Manager S8800 Server	Avaya Aura® System Manager 6.1
Avaya Aura® Session Manager S8800 Server	Avaya Aura® Session Manager 6.1
Avaya Aura® Messaging S8800 Server	Avaya Aura® Messaging 6.1
Avaya Aura® Application Enablement Services S8800 Server	Avaya Aura® Application Enablement Services 6.1
Avaya Agile Communication Environment™	3.0.2
Avaya 9600 H323 Phone	6.2
ESNA Telephony Office-LinX	8.5 SP2
UC Client Manager	8.5 SP2

5. Configure Avaya Aura® Communication Manager

5.1. Configure SIP trunk between Avaya Communication Manager and Session Manager

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

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

©2011 Avaya Inc. All Rights Reserved.

5.1.1. Capacity Verification

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

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

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

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

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

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

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

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

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

5.1.2. IP Codec Set

This section describes 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. Enter the **change ip-codec-set <c>** command, where **c** is a

©2011 Avaya Inc. All Rights Reserved.

number between **1** and **7**, inclusive. IP codec sets are used in the IP network region to specify which codec sets may be used within and between network regions.

***Note**: ESNA Telephony Office-LinX supports G.711MU and G.711A. Thus, these two codecs were tested during the compliance test.*

1. Ensure that G.711A, G.711MU are the only codes administered.
2. Verify that the **Silence Suppression** field is set to **n**.

```
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
 3:
    Media Encryption
 1: none
```

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, in **Section 8.1**.
- **Codec Set** – Set the codec set number as provisioned in **Section 5.1.2**.

```
change ip-network-region 1                                     Page   1 of  20
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: bvwdev.com
    Name:Phuong system SIP
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```


©2011 Avaya Inc. All Rights Reserved.

5.1.4. Configure IP Node Name

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

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
DevASM                  135.10.87.xxx
default                 0.0.0.0
procr                   10.64.41.21
procr6                  ::
```

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 **tcp**.
- **Near-end Node Name** – Set to **procr** as displayed in **Section 5.1.4**.
- **Far-end Node Name** – Set to the Session Manager name configured in **Section 5.1.4**.
- **Far-end Network Region** – Set to the region configured in **Section 5.1.3**.
- **Far-end Domain** – Set to **bvwdev.com**. This should match the SIP Domain value in **Section 8.1**.
- **Direct IP-IP Audio Connections** – Set to **y**, since the shuffling is enabled during the compliance test

```
add signaling-group 5
                                SIGNALING GROUP

 Group Number: 5                Group Type: sip
  IMS Enabled? n          Transport Method: tcp
        Q-SIP? n                                          SIP Enabled LSP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM


   Near-end Node Name: procr                 Far-end Node Name: DevASM
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                         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? n
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 6
```


©2011 Avaya Inc. All Rights Reserved.

5.1.6. Configure Trunk Group

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

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

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

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

On **Page 3**, set the Numbering Format field to **unk-pvt.**

```
add trunk-group 5                                                Page   3 of  21
                                 TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                         Maintenance Tests? y

                     Numbering Format: unk-pvt
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: no
 Show ANSWERED BY on Display? y
```


©2011 Avaya Inc. All Rights Reserved.

5.1.7. Configure Route Pattern

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

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

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                   Dgts Format
                                                            Subaddress
 1: y y y y y n  n           rest                                lev0-pvt    none
 2: y y y y y n  n           rest                                            none
 3: y y y y y n  n           rest                                            none
 4: y y y y y n  n           rest                                            none
 5: y y y y y n  n           rest                                            none
 6: y y y y y n  n           rest                                            none
```

5.1.8. Administer Dialplan

Configure dialplan analysis, Uniform Dialing and AAR to route calls over a SIP trunk to Session Manager and ultimately to Avaya Aura® Messaging, 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

- 53000 – ESNA Office-LinX extension.
- 39995 – Avaya Aura® Messaging Auto Attendant pilot number.
- 39990 – Avaya Aura® Messaging access number.
- 216 – Endpoint extension in Communication Manager

```
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
   5300        5   ext       9          1    fac
   399         5   ext       *          4    dac
   216         5   ext
```


©2011 Avaya Inc. All Rights Reserved.

Use the command **change uniform dial-plan 1** to create an entry in the UDP table which covers extensions to Messaging access number and ESNA Office-LinX extensions.

As shown below, any number dialed to 399xx or 5300x totaling 5-digits will be routed to the AAR

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

  Matching                    Insert              Node
  Pattern        Len Del      Digits     Net Conv Num
 399              5   0                  aar  n
 5300             5   0                  aar  n
 216              5   0                  aar  n
```

For the AAR Analysis Table, create the dial strings that will route calls to Avaya Aura Messaging and Office-LinX 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 access number and Office-LinX extension. During the configuration of the aar table, the Call Type field was set to **unku**.

```
display aar analysis 0                                          Page   1 of   2
                            AAR DIGIT ANALYSIS TABLE
                                  Location: all            Percent Full: 3

        Dialed           Total     Route     Call   Node  ANI
        String          Min  Max  Pattern    Type   Num   Reqd
    399                   5    5     5        unku         n
    5300                  5    5     5        unku         n
    216                   5    5     5        aar          n
```

5.1.9. Administering an extension number for the station that an Office-LinX application monitors

Follow these steps from a Communication Manager SAT to administer an extension number for the physical station the application is monitoring.

1. Type change station *nnnnn* (where *nnnn* is the extension number of the physical station the application is monitoring or controlling).
2. Check the settings on the STATION form. If the STATION form is not already administered this way, follow these steps:
   a. In the **IP Softphone** field, type y.
   b. In the **Security Code** field, type a <*numeric security code*>. This is used when user log in the physical phone.

©2011 Avaya Inc. All Rights Reserved.

```
change station 21613                                          Page   1 of   5
                                    STATION
Extension: 21613                      Lock Messages? n                BCC: 0
     Type: 9630                       Security Code: 1234              TN: 1
     Port: S00028                   Coverage Path 1: 5                COR: 1
     Name: Mot Ba                   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: 21613
           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
                                        Customizable Labels? y
```

5.1.10. 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.

```
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 ESNA Telephony Office-LinX.
- **Routing Digit (e.g. AAR/ARS Access Code)** – Enter the AAR Access Code as defined in the Feature Access Code form.

```
add hunt-group 2                                              Page   2 of  60
                                    HUNT GROUP
                        Message Center: sip-adjunct
     Voice Mail Number        Voice Mail Handle          Routing Digits
                                                  (e.g., AAR/ARS Access Code)
     39990                    39990                      9
```


©2011 Avaya Inc. All Rights Reserved.

5.1.11.Configure Coverage Path to Avaya Aura Messaging

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

```
add coverage path 2                                                Page   1 of   1
                                  COVERAGE PATH
                    Coverage Path Number: 2
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                        Next Path Number:          Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside     Outside Call
             Active?             n              n
               Busy?             y              y
       Don't Answer?             y              y         Number of Rings: 2
                All?             n              n
 DND/SAC/Goto Cover?             y              y
   Holiday Coverage?             n              n
COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h2            Rng:2    Point2:
  Point3:                        Point4:
```

5.1.12.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 **Page1** for **Coverage Path 1** use the coverage path defined in **Section 5.1.11** in the example below station 21613 was configured to cover to messaging using cover path 2.

```
change station 21613                                               Page   1 of   5
                                     STATION

Extension: 21613                         Lock Messages? n                BCC: 0
     Type: 9630                          Security Code: *                 TN: 1
     Port: S00024                       Coverage Path 1: 2               COR: 1
     Name: Nam Mot                      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
```


©2011 Avaya Inc. All Rights Reserved.

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

```
change station 21613                                          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: 21613         Always Use? n IP Audio Hairpinning? n
```

5.1.13. Configure Hunt Group for ESNA Office-LinX

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.

```
Add hunt-group 1                                          Page   1 of  60
                                    HUNT GROUP
            Group Number: 1                                   ACD? n
              Group Name: ESNA                              Queue? n
         Group Extension: 53001                             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 ESNA Office-LinX.
- **Voice Mail Handle –**Enter the Voice Mail Handle which is the extension of ESNA Telephony Office-LinX.
- **Routing Digit (e.g. AAR/ARS Access Code)** – Enter the AAR Access Code as defined in the Feature Access Code form.

©2011 Avaya Inc. All Rights Reserved.

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

                      Message Center: sip-adjunct

     Voice Mail Number        Voice Mail Handle         Routing Digits
                                                  (e.g., AAR/ARS Access Code)
     53000                    53000                     9
```

5.1.14.Configure Coverage Path to ESNA Office-LinX

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 **h1** is used to represent the hunt group number 1. The default values for the other fields may be used.

```
add coverage path 1                                              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: h1            Rng:2    Point2:
  Point3:                        Point4:
```

5.2. Configure CTI link between Communication Manager and AE Server

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

- Verify license
- Enable Processor Ethernet
- Enable AE Services change ip-services.
- Add a CTI link
- Administer a network region
- Add DMCC soft phones to the network region
- Add a media gateway to the network
- Verify a media processor

©2011 Avaya Inc. All Rights Reserved.

5.2.1. Verify license

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**. If this option is not set to "y", then contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                    Page   3 of  11
                              OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                ARS? y   Computer Telephony Adjunct Links? y
                ARS/AAR Partitioning? y  Cvg Of Calls Redirected Off-net? y
         ARS/AAR Dialing without FAC? n                          DCS (Basic)? y
         ASAI Link Core Capabilities? 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. Enable Processor Ethernet

On the S8300 Communication Manager Media servers, Processor Ethernet support is enabled by default. If not, then set to y.

1. Type **display system-parameters customer-options**.

```
display system-parameters customer-options                    Page   5 of  11
                              OPTIONAL FEATURES

                Multinational Locations? n                Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n          Station as Virtual Extension? y
                     Multiple Locations? n
                                                 System Management Data Transfer? n
          Personal Station Access (PSA)? y                  Tenant Partitioning? y
                       PNC Duplication? n           Terminal Trans. Init. (TTI)? y
                  Port Network Support? n                  Time of Day Routing? y
                       Posted Messages? y           TN2501 VAL Maximum Capacity? y
                                                          Uniform Dialing Plan? y
                    Private Networking? y         Usage Allocation Enhancements? y
               Processor and System MSP? y
                     Processor Ethernet? y                  Wideband Switching? y
                                                                    Wireless? n
                         Remote Office? y
          Restrict Call Forward Off Net? y
                   Secondary Data Module? y
        (NOTE: You must logoff & login to effect the permission changes.)
```


©2011 Avaya Inc. All Rights Reserved.

2. Verify that Processor Ethernet is enabled, see above figure. You must perform this verification step before proceeding with the next step.
3. Type "**add ip-interface procr** or "**display ip-interface procr**" if it is existed.

```
add ip-interface procr                                          Page   1 of   2
                                  IP INTERFACES
                  Type: PROCR
                                                        Target socket load: 4800

      Enable Interface? y                             Allow H.323 Endpoints? y
                                                       Allow H.248 Gateways? y
        Network Region: 1                               Gatekeeper Priority: 5
                                 IPV4 PARAMETERS
             Node Name: procr
           Subnet Mask: /26
```

5.2.3. Enable AE Services change ip-services.

Enabling AE Services refers to administering the transport link between Communication Manager and AE Services. You need to enable AE Services for the following applications. Device, Media, and Call Control (DMCC) applications that use Call Information Services, DMCC applications that use Call Control Services

Complete Page 1 of the IP SERVICES form as follows:
a. In the **Service Type** field, type AESVCS.
b. In the **Local Node** field, type the appropriate entry based on whether you are using a Processor Ethernet interface or a CLAN interface:

For Communication Manager S8300 systems that use a processor Ethernet interface, 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 AE Server, for example: DevAES.

```
change ip-services                                          Page   3 of   3
                            AE Services Administration
   Server ID    AE Services       Password          Enabled    Status
                   Server
        1:      DevAES            aespassword         y        in use
```

Note:
a. On the AE Server you can obtain this name by typing uname -n at the command prompt. The name you use on Communication Manager must match the AE Server name exactly.
b. In the **Password** field, create a password that consists of 12 to 16 alphanumeric characters, for example aespassword1.

©2011 Avaya Inc. All Rights Reserved.

Important: This is the password that the AE Services administrator must set on the AE Server (**Communication Manager Interface → Switch Connections → Edit Connection → Switch Password**). The passwords must exactly match on both Communication Manager and the AE Server.
c. Set the **Enabled** field to y.

5.2.4. Add a CTI link

Add a CTI link using the "add cti-link n" command, where "n" is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter "ADJ-IP" in the **Type** field, and a AES server name 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: 21613
     Type: ADJ-IP
                                                                COR: 1
Name: DevEAS
```

5.2.5. Method for adding DMCC Softphone to the network region

Use the **change ip-network-map** command. On the IP ADDRESS MAPPING form, specify the IP address of the AE Server and assign a network region created in **Section 5.1.3.**

```
change ip-network-map                                          Page   1 of  63
                              IP ADDRESS MAPPING
                                              Subnet Network     Emergency
 IP Address                                   Bits   Region VLAN Location Ext
 ------------------------------------------- ------ ------ ---- -------------
 FROM: 135.10.97.x                           /        1      n
   TO: 135.10.97.x
```


©2011 Avaya Inc. All Rights Reserved.

5.2.6. Administer media gateway

Type display media-gateway 1; verify network region is assigned to network region created in **Section 5.1.3.**

```
display media-gateway 1
                              MEDIA GATEWAY
         Number: 1                              Registered?  y
           Type: g450                FW Version/HW Vintage: 28 .22 .0  /1
           Name: Media Gateway 1            MGP IP Address: 135.10 .97 .247
      Serial No: 08IS38199691        Controller IP Address: 135.10 .97 .219
   Encrypt Link? y                              MAC Address: 00:1b:4f:03:51:08
 Network Region: 1    Location: 1                Enable CF? n
                                                 Site Data:
  Recovery Rule: none

Slot   Module Type            Name                     DSP Type  FW/HW version
 V1:   S8300                  ICC MM                   MP80      15   2
 V2:
 V3:   MM712                  DCP MM
 V4:   MM710                  DS1 MM
 V5:
 V6:   MM711                  ANA MM
 V7:
 V8:                                                 Max Survivable IP Ext: 8
 V9:   gateway-announcements  ANN VMM
```

Note:
If the media gateway used and the configuration needs media encryption, "**Encrypt Link?"** must be set to "**y**". If you do not enable this setting, your application will not get a talk path.

5.2.7. Verify a media processor circuit pack

Type change **node-names ip** and add a node name for Avaya AES along with its IP address, e.g: DevAES.

```
change node-names ip                                    Page   1 of   2
                                    IP NODE NAMES
   Name                IP Address
   DevAES               135.10.97.xx
   DevASM               135.10.97.1xx
   procr                135.10.xx.x
   procr6               ::
```

Use the **list ip-interface all** command to view the IP interfaces used in this configuration.

```
list ip-interface all

                                IP INTERFACES

                                                                        Net
ON Type    Slot  Code/Sfx      Node Name/       Mask  Gateway Node      Rgn  VLAN
                               IP-Address
-- ------ ----- --------      ---------------  ----  ---------------   ---  ----
 y PROCR                      135.10.97.xxx    /26   135.10.97.xxx     1
```


©2011 Avaya Inc. All Rights Reserved.

6. Configure AE Server

The Application Enablement Services server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager. This section assumes that installation and basic administration of the Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user and a DMCC port.

This section provides the procedures for configuring AE Server. The procedures include the following areas:

- Verify license
- Configure Switch Connection: Add switch, edit IP, H323 Gatekeeper
- Configure TR8/7 Port
- Configure service setting TR/87
- Configure dialing plan
- Add switch Connection on OAM.
- Add dial plan on OAM for switch.
- Add TSAPI link.

6.1. Verify Device and Media Call Control API Station licenses

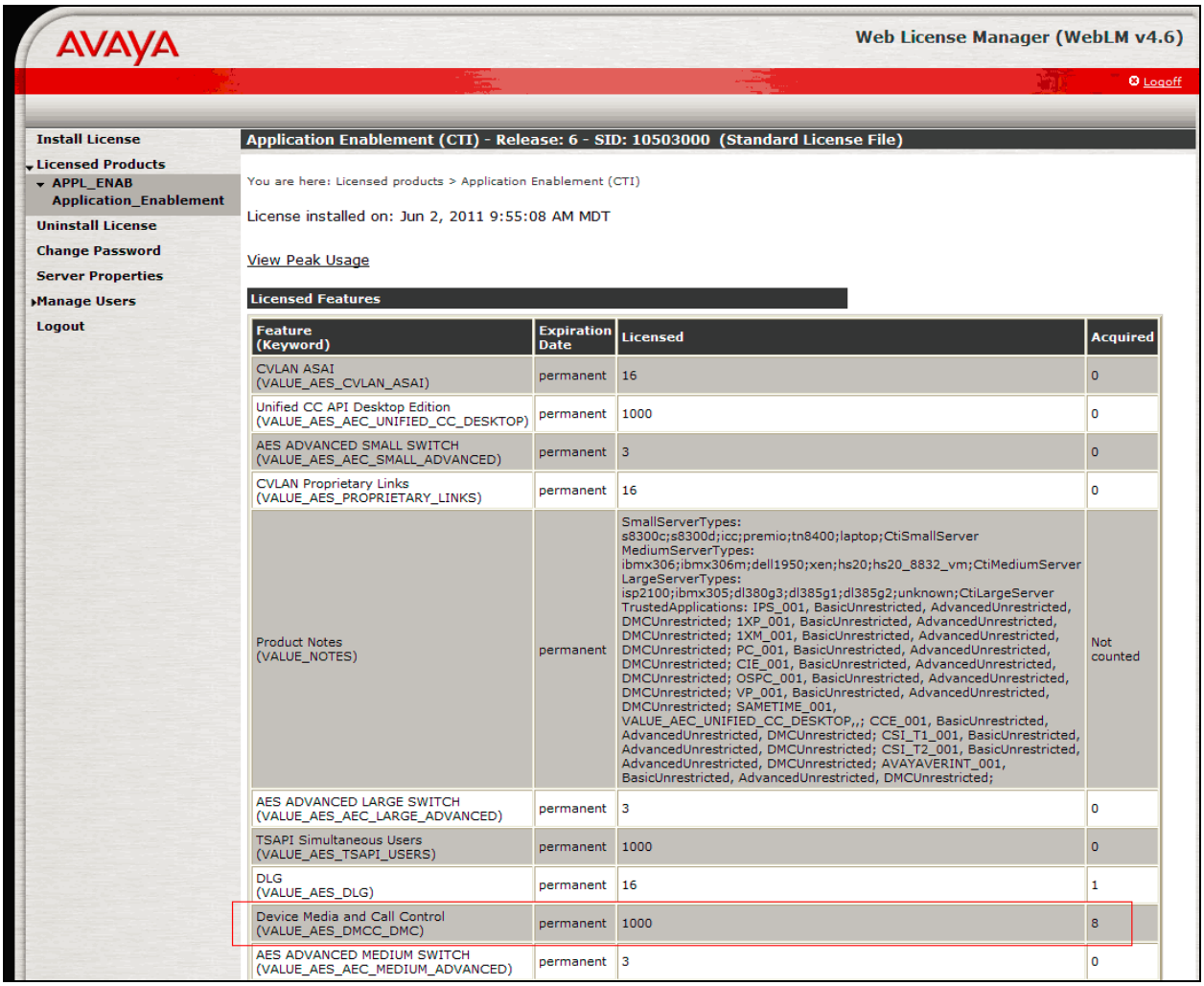
To check and verify that there are sufficient DMCC licenses, log in to https://<IP address of the Application Enablement Services server>/index.jsp, and enter appropriate login credentials to access the Application Enablement Services Management Console page. Select the **Licensing →WebLM Server Access** link from the left pane of the window.

Provide appropriate login credentials to access the Web License Manager page (not shown).

On the Install License page, select **License Products →Application Enablement** link from the left pane of the window.

On the Licensed Features page, verify that there are sufficient DMCC licenses

©2011 Avaya Inc. All Rights Reserved.

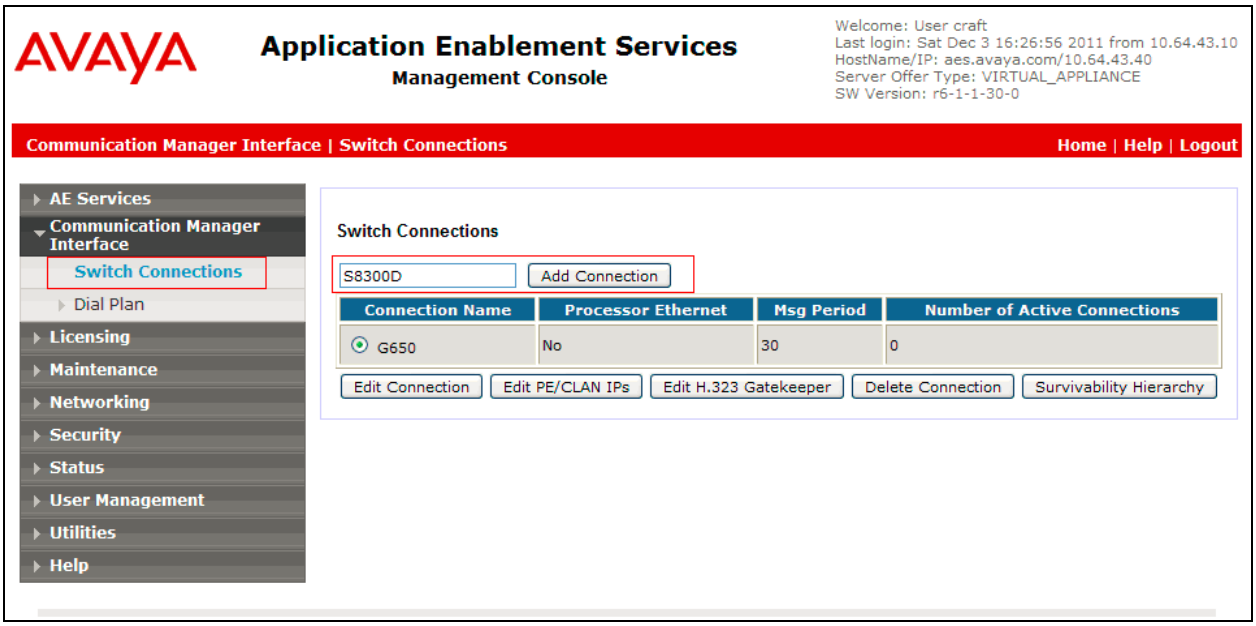


6.2. Configure Switch Connection: Add switch, edit IP, H323 Gatekeeper

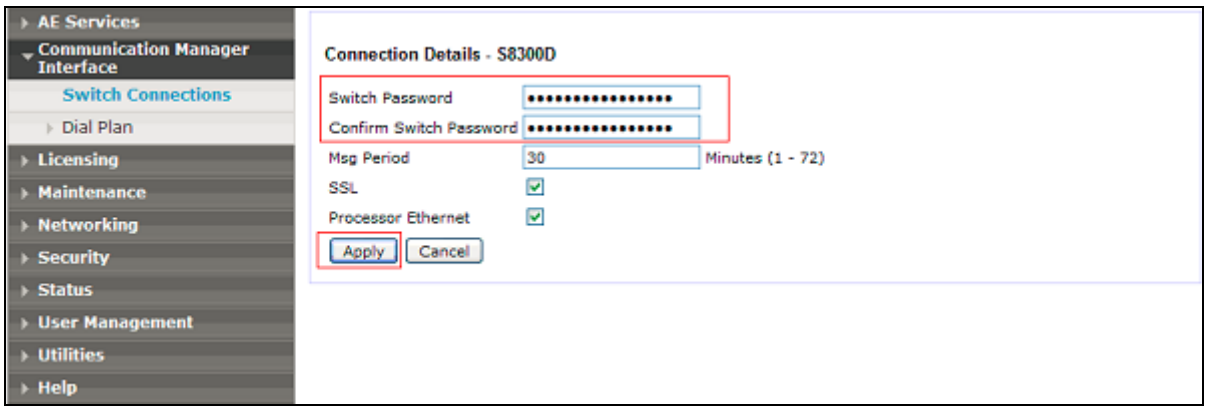
Launch a web browser, enter https://<IP address of the Application Enablement Services server> in the address field, and log in with the appropriate credentials for accessing the Application Enablement Services Management Console pages (not shown).

A Switch Connection defines a connection between the Application Enablement Services server and Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection.**

©2011 Avaya Inc. All Rights Reserved.

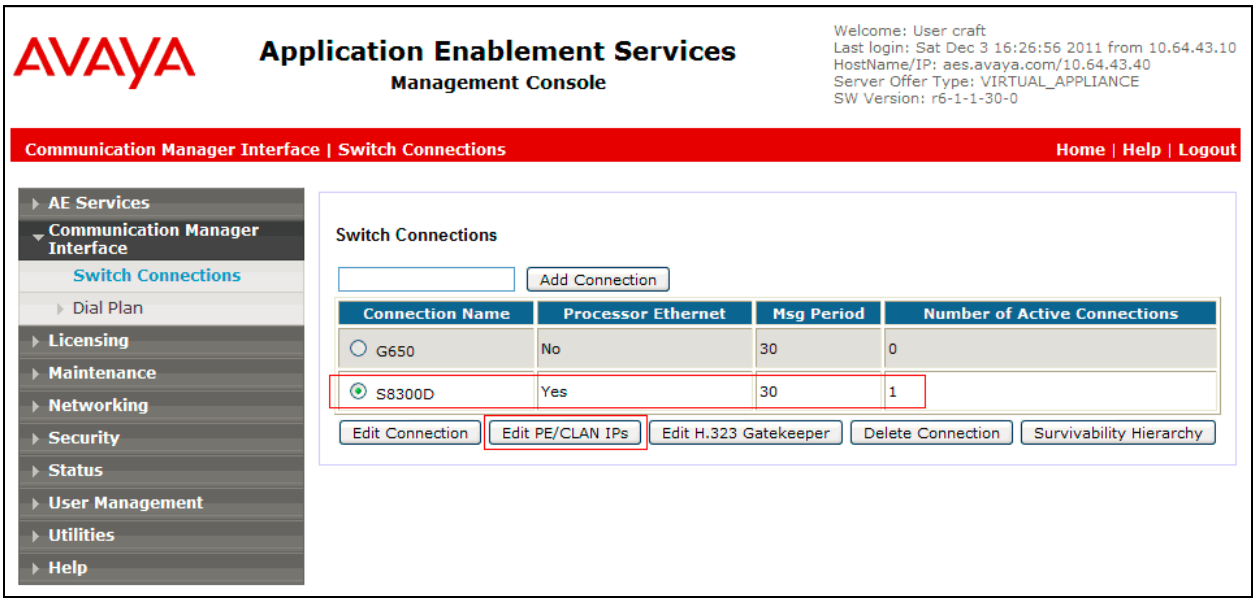


The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Communication Manager in **Section 5.2.3**. Click on **Apply**.



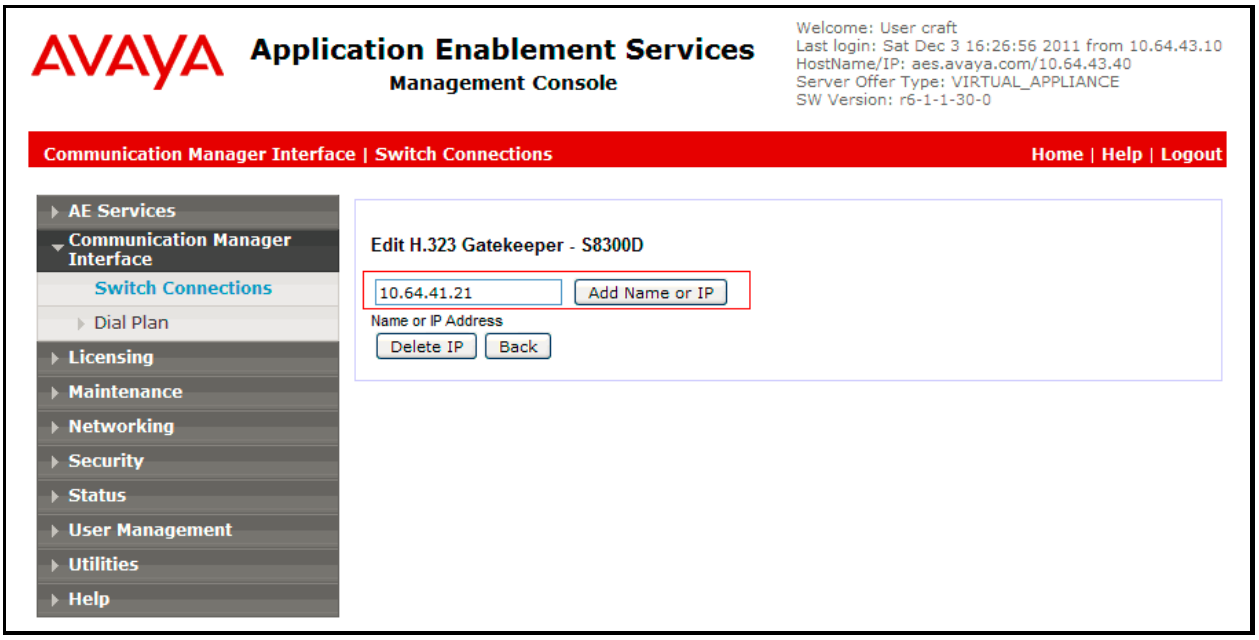
After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on the **Edit PE/CLAN IPs** button.

©2011 Avaya Inc. All Rights Reserved.



On the **Edit PE/CLAN IPs – S8300D** page, enter the procr IP address which will be used for the DMCC service. Click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services (not shown).

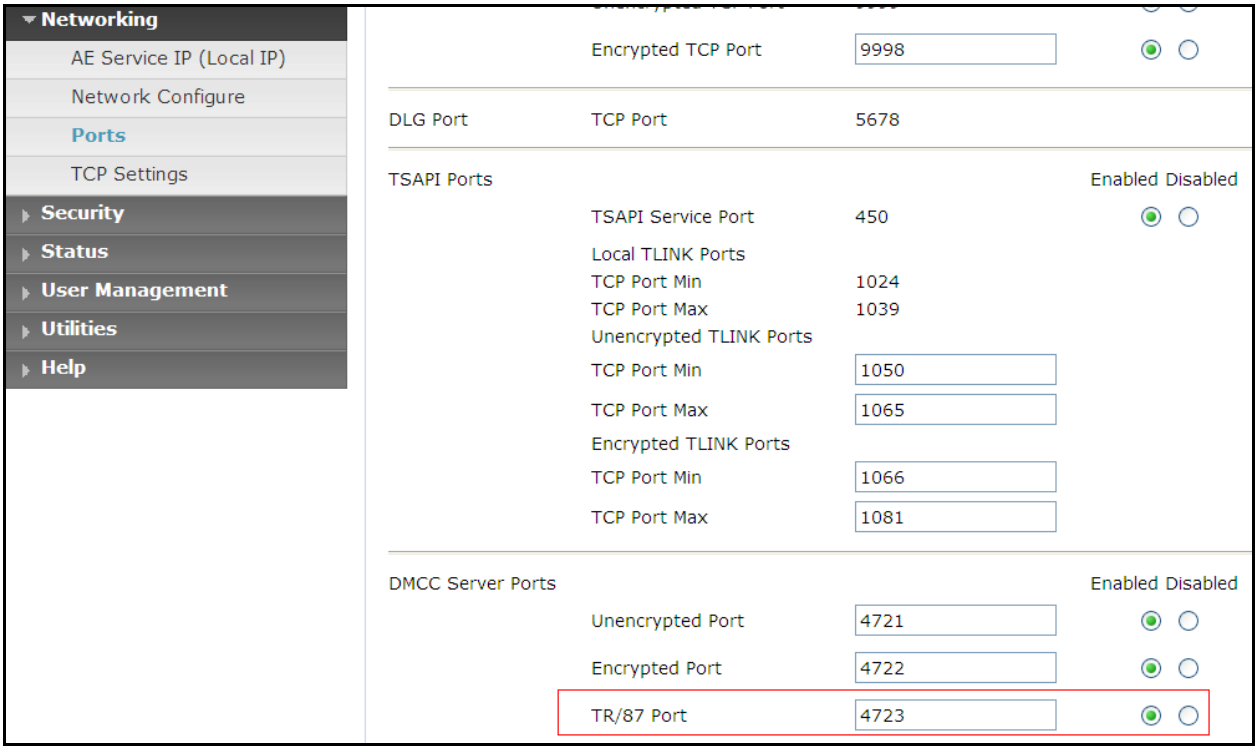
On the **Edit H.323 Gatekeeper – S8300D** page, enter the procr IP address which will be used for the DMCC service. Click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.



6.3. Enable TR8/7 Port

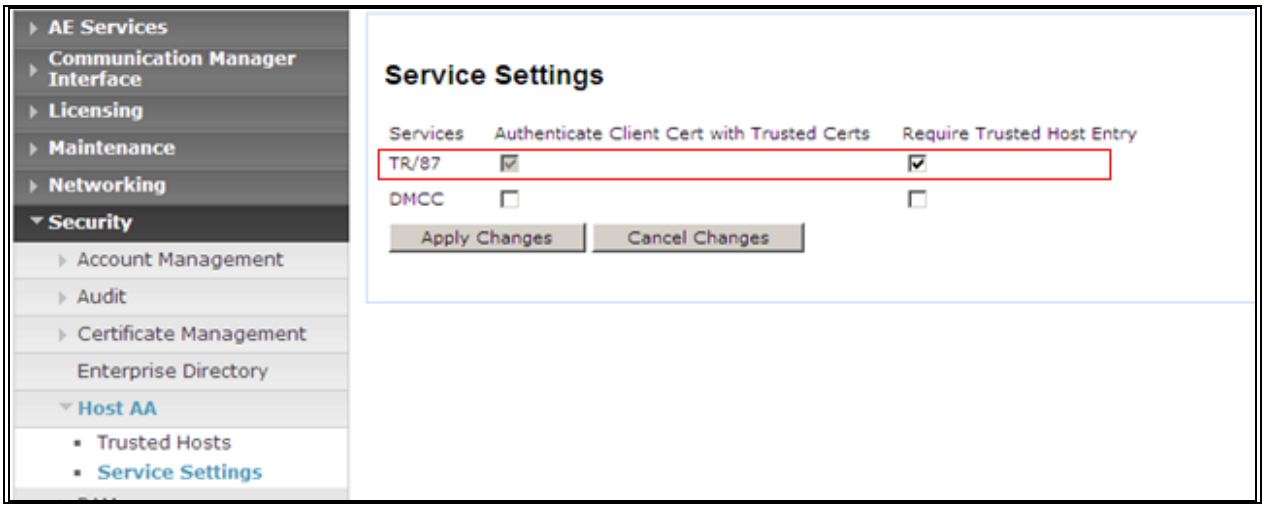
Select Networking – Ports, make sure DMCC Server Ports TR/87 Port is Enable. If it is not, enable it and click Apply changes.

©2011 Avaya Inc. All Rights Reserved.



6.4. Enable TR/87 service setting

Select Security – Service Settings, make sure TR/87 Authenticate Client Cert with Trusted Certs and Require Trusted Host Entry are checked. If they are not, enable them and click Apply changes.

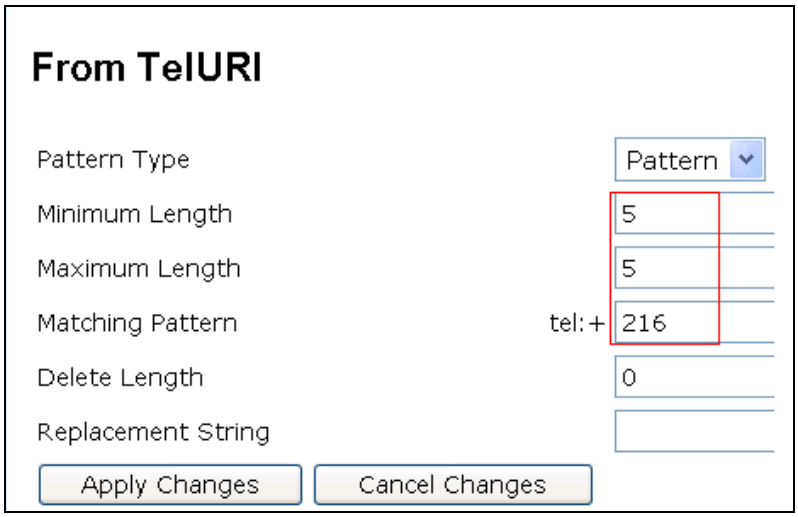


©2011 Avaya Inc. All Rights Reserved.

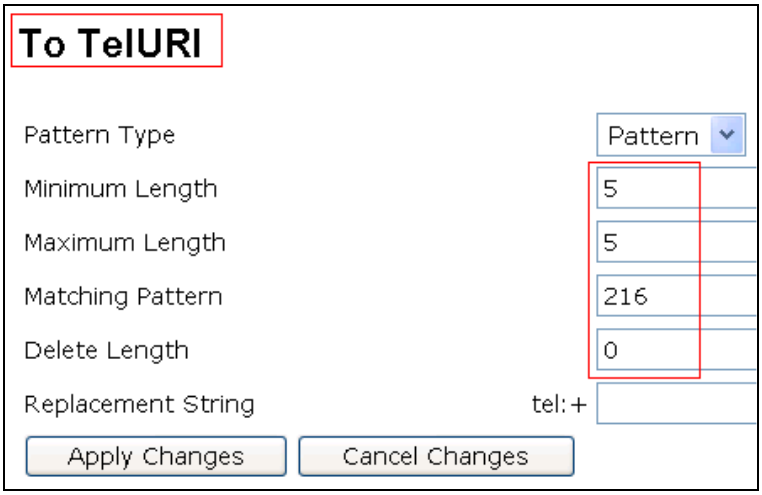
6.5. Configure dialing plan

To make sure AE Services works with DMCC applications working in TelURI mode, user need to setup Dial Plan for switch connection, make sure this dial plan is configured according to ACE rules, and CM dial plan.

Detail configuration of From TelURI using during compliance test



Detail configuration of To TelURI using during compliance test

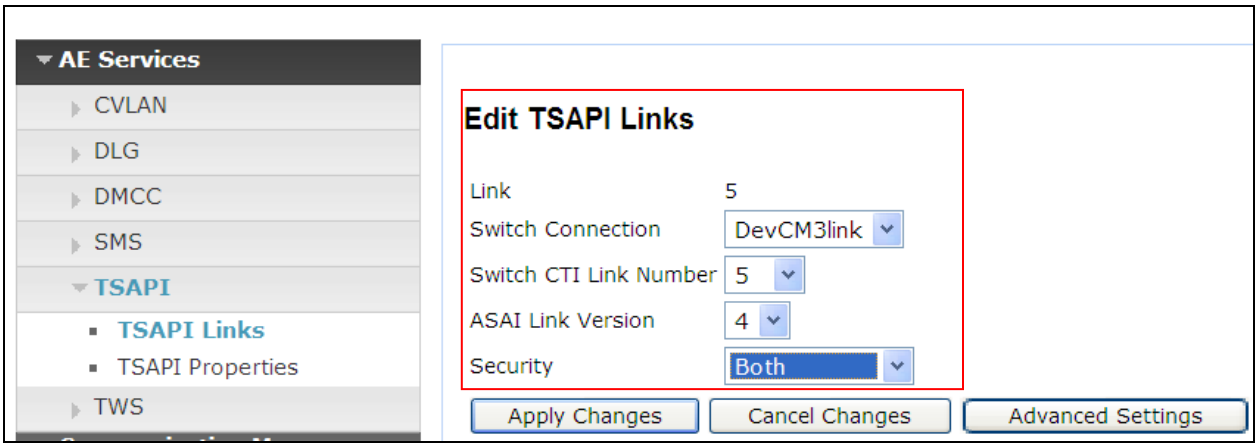


6.6. Add TSAPI link

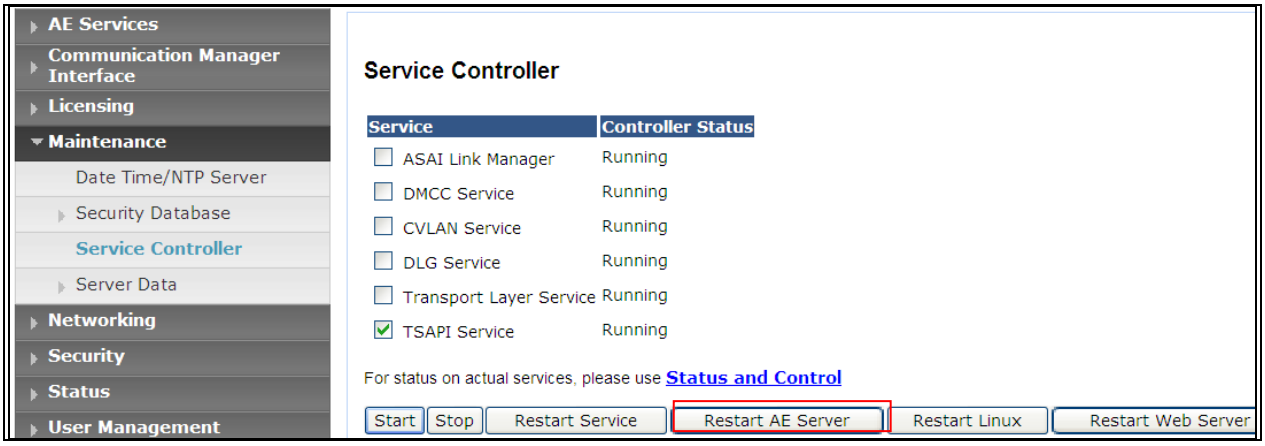
1. From the AE Services Management Console main menu, select **AE Services →TSAPI → TSAPI Links**.
2. From the **TSAPI Links** page, click **Add Link**.
3. On the **Add TSAPI Links** page do the following:
a. In the **Link** field, select the link number.

©2011 Avaya Inc. All Rights Reserved.

b. In the **Switch Connection** field, select the switch connection that you want to use.
c. In the **Switch CTI Link Number** field, select the switch CTI link number administered on Communication Manager for this TSAPI link.
d. In the **ASAI Link Version** field, select either **4** or **5**.
Below is detail of TSAPI Links.



Click **Apply Changes**.
4. On the **Apply Changes to a Link** page, click **Apply Changes**.
5. Restart the TSAPI service as follows:
a. Select **Maintenance > Service Controller**.
b. From the **Service Controller** page, click **Restart AE Server**.



©2011 Avaya Inc. All Rights Reserved.

6.7. Checking the status of a switch connection from Communication Manager to the AE Server

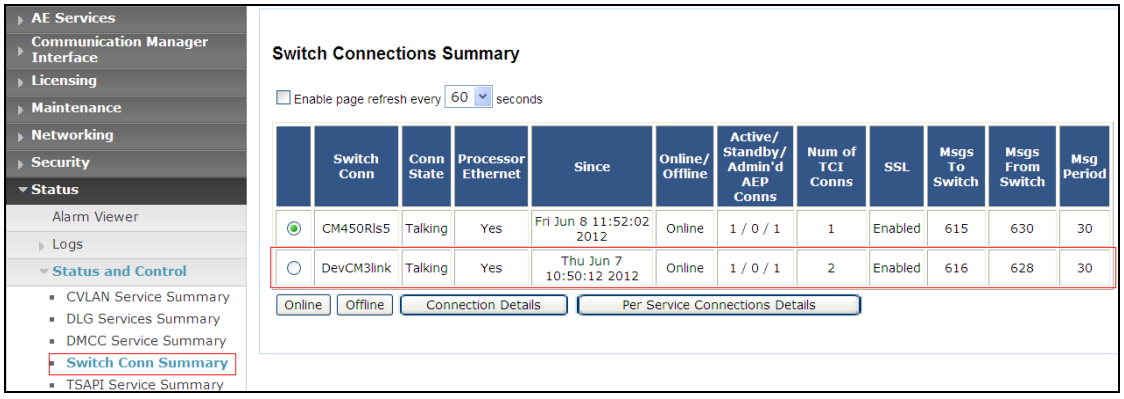
Once you have added a switch connection on the AE Server, you validate the switch connection by checking its status on both the AE Server and on Communication Manager.
To check the status of a switch connection on Communication Manager, type status aesvcs link.

```
status aesvcs link

                          AE SERVICES LINK STATUS
Srvr/   AE Services     Remote IP        Remote  Local Node       Msgs     Msgs
Link    Server                           Port                     Sent     Rcvd
01/01   DevAES                           34298   procr            664      655
                        135.10.97.62
```

6.8. Checking the status of a switch connection -- from the AE Server to Communication Manager

1. From the AE Services Management Console main menu, select **Status → Status and Control → Switch Conn Summary**.
2. From the **Switch Connections Summary** page, select the switch connection you just added.
3. Click **Connection Details**.
4. Review the information on the **Connection Details** page. Verify that the connection state is **Talking** and the Online/Offline status is **Online**.



7. Configure Avaya Aura® Messaging

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

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

©2011 Avaya Inc. All Rights Reserved.

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

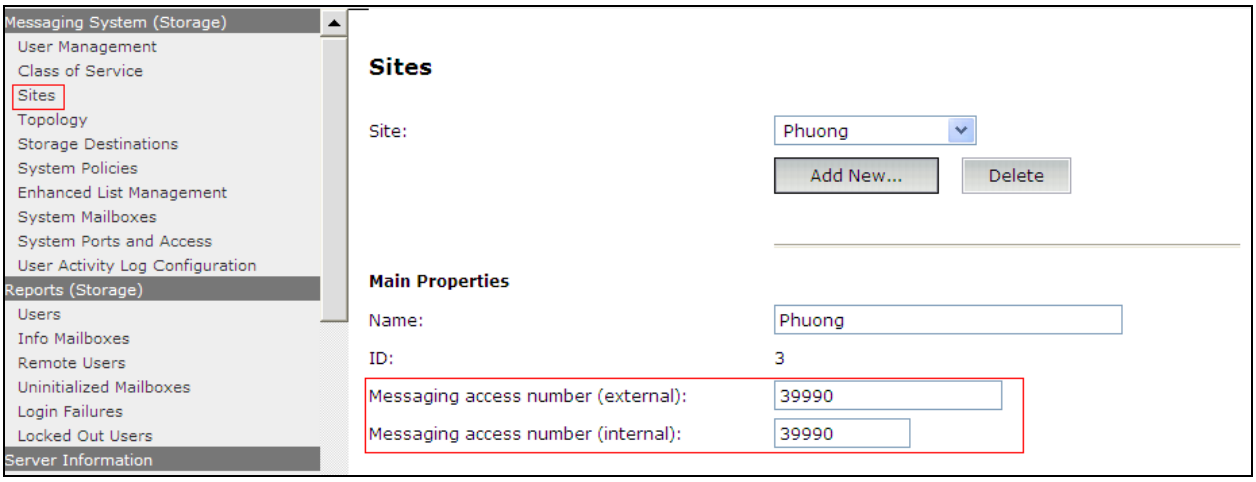
7.1. Administer Sites

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

Under **Main Properties:**

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

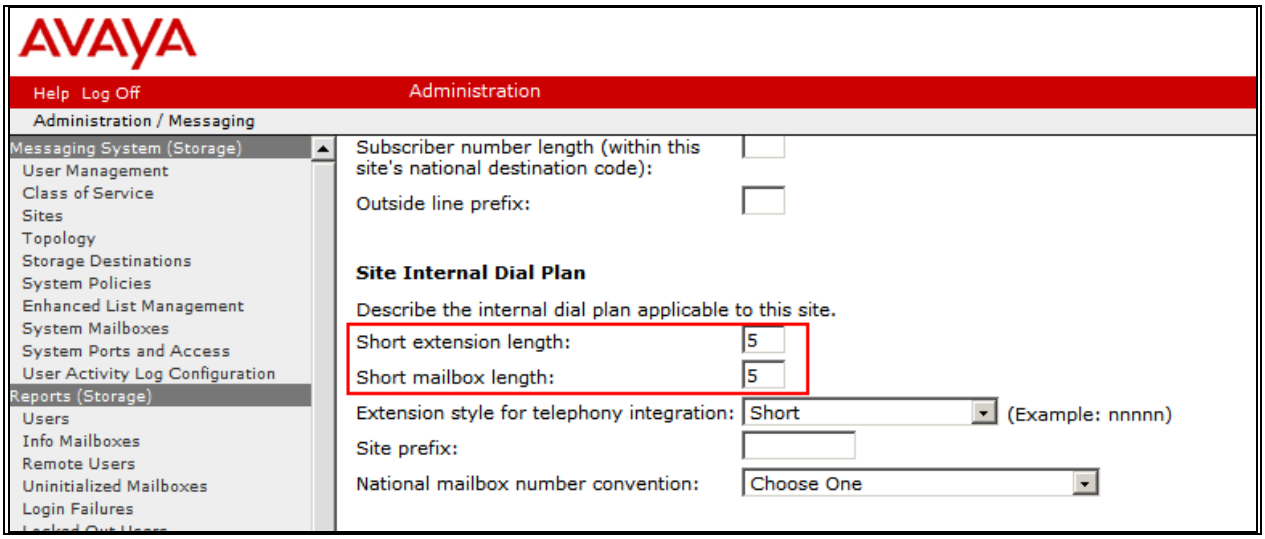
Sites detail screen on AAM show Messaging access number



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

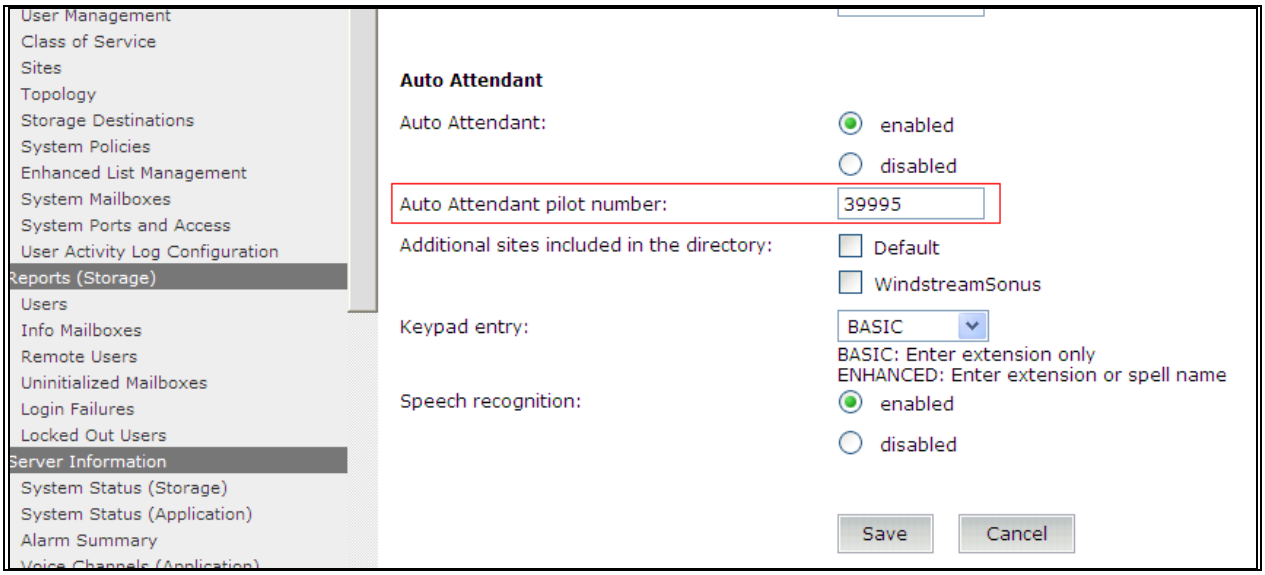
©2011 Avaya Inc. All Rights Reserved.



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.



7.2. 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**. In the left panel, under **Telephony Settings (Application)** select **Telephony Integration**. In the right panel fill in the following:

©2011 Avaya Inc. All Rights Reserved.

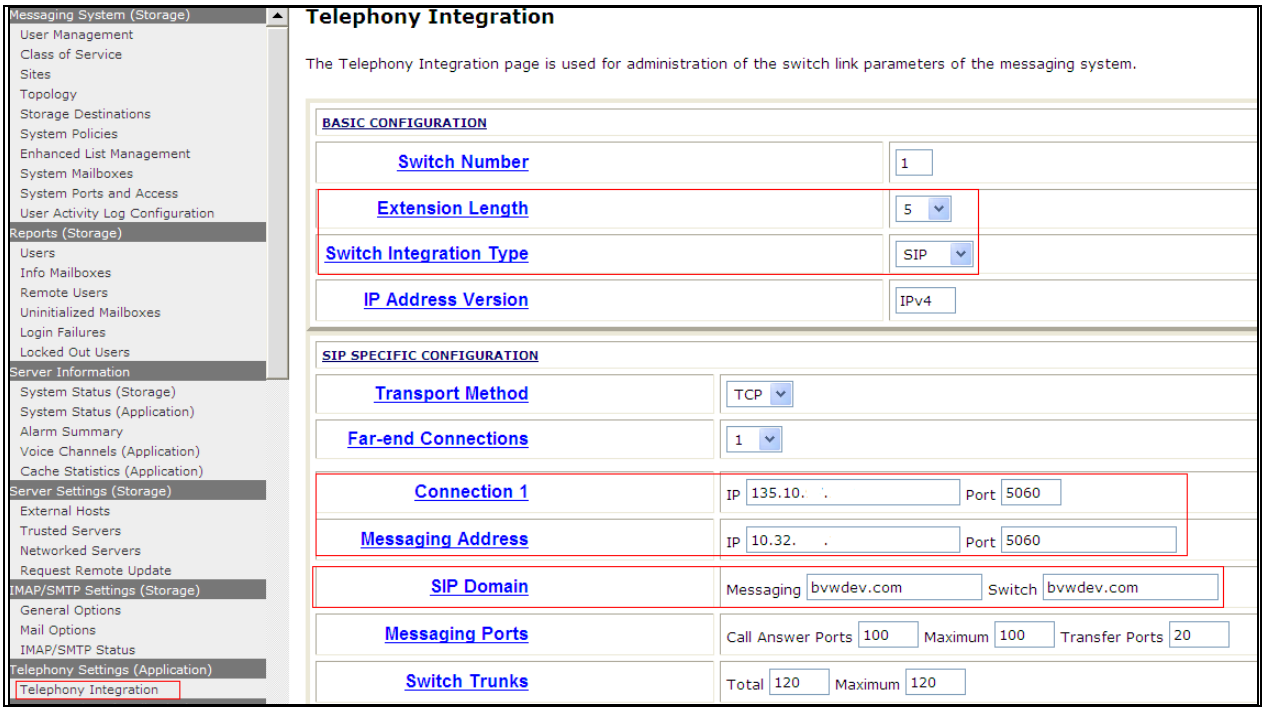
Under **Basic Configuration:**

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

Under **SIP Specific Configuration:**

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

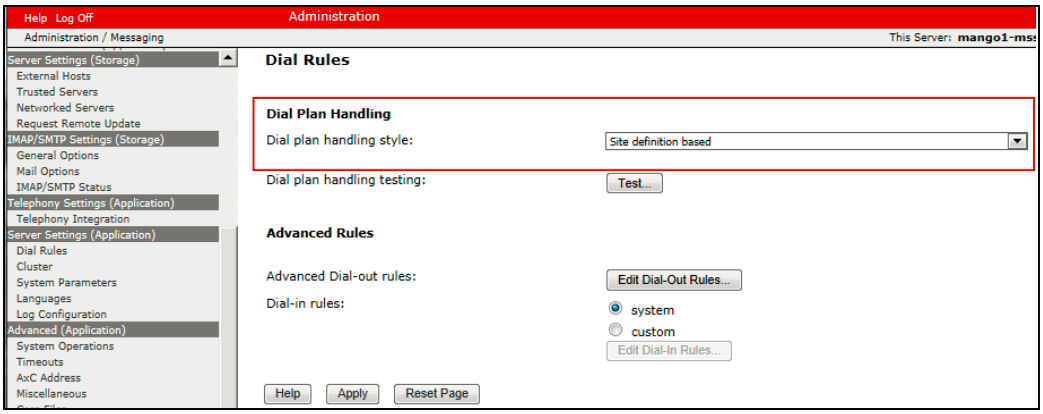
Click **Save** to save changes.



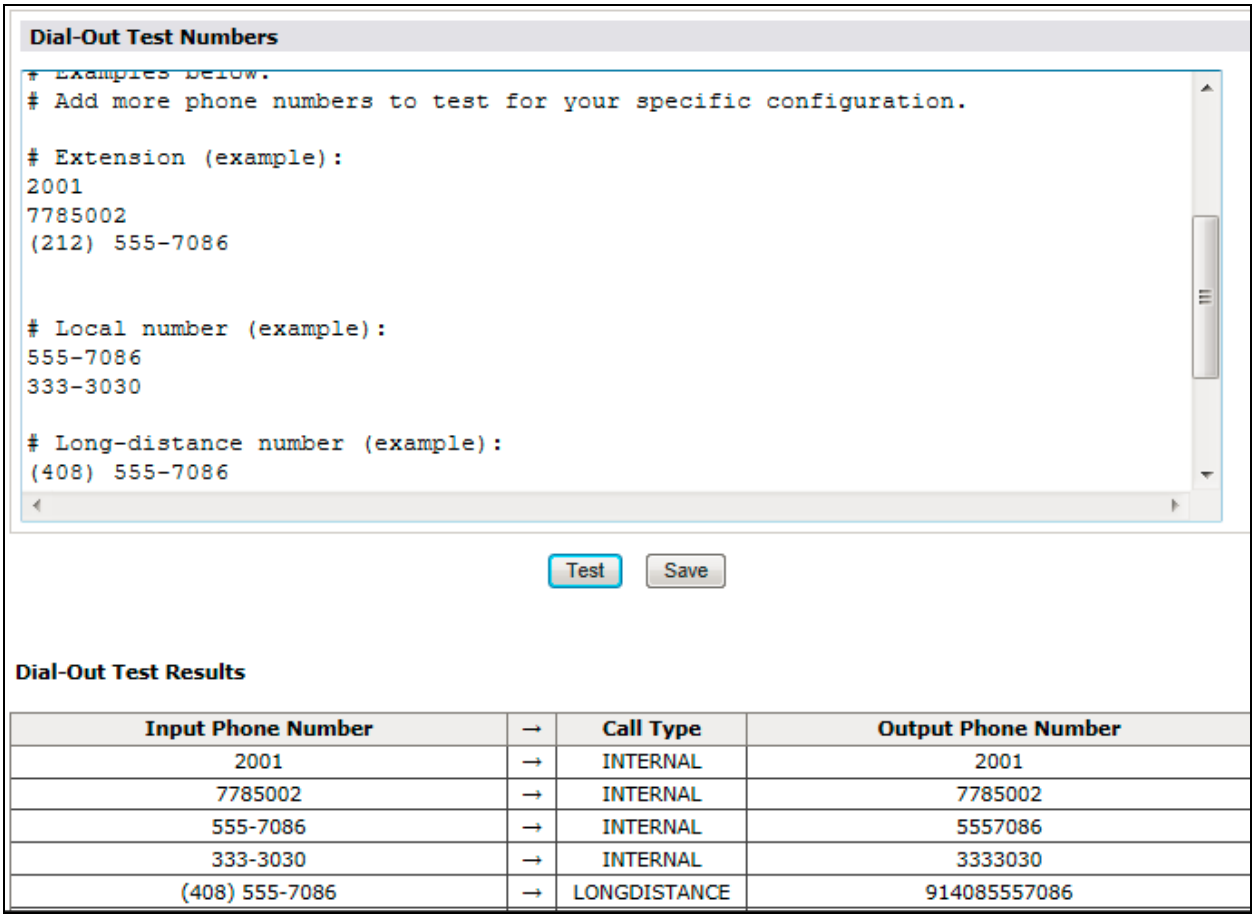
7.3. Configure Dial Rules

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.

©2011 Avaya Inc. All Rights Reserved.



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



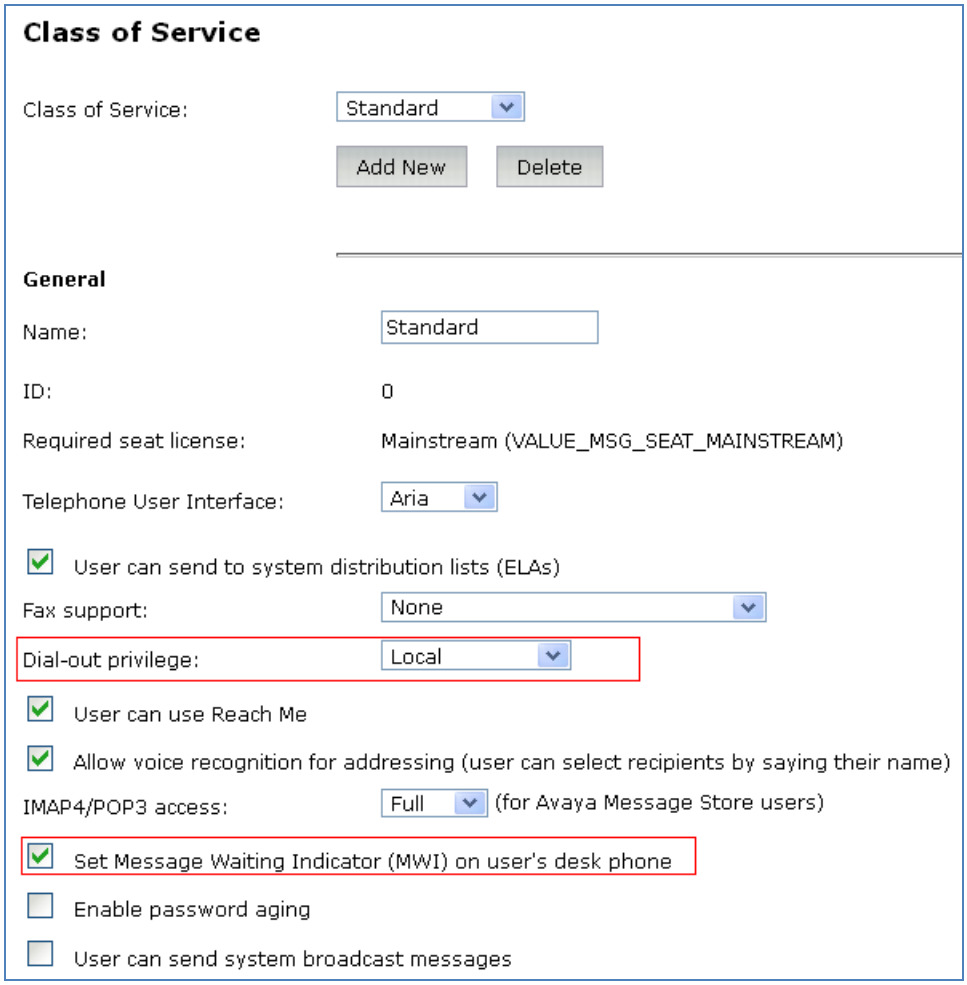
Input Phone Number	→	Call Type	Output Phone Number
2001	→	INTERNAL	2001
7785002	→	INTERNAL	7785002
555-7086	→	INTERNAL	5557086
333-3030	→	INTERNAL	3333030
(408) 555-7086	→	LONGDISTANCE	914085557086

7.4. Configure Class of Service

Verify Messaging Waiting is enabled for all subscribers.

©2011 Avaya Inc. All Rights Reserved.

Use **Administration → Messaging** menu and select **Class of Service** under **Messaging System (Storage).** Select **"Standard"** from the **Class of Service** drop-down menu.
Under **General** section, enter the following value and use default values for remaining fields.
Set **Message Waiting Indicator (MWI):** Enter Under **Greetings** section, enter for **Two Greetings (different greetings for busy and no answer)** field to allow subscribers to record different personal greetings for busy and no-answer scenarios.
Click **Save** (not shown) to save changes.
The following screen shows the settings defined for the "**Standard**" Class of Service in the sample configuration.



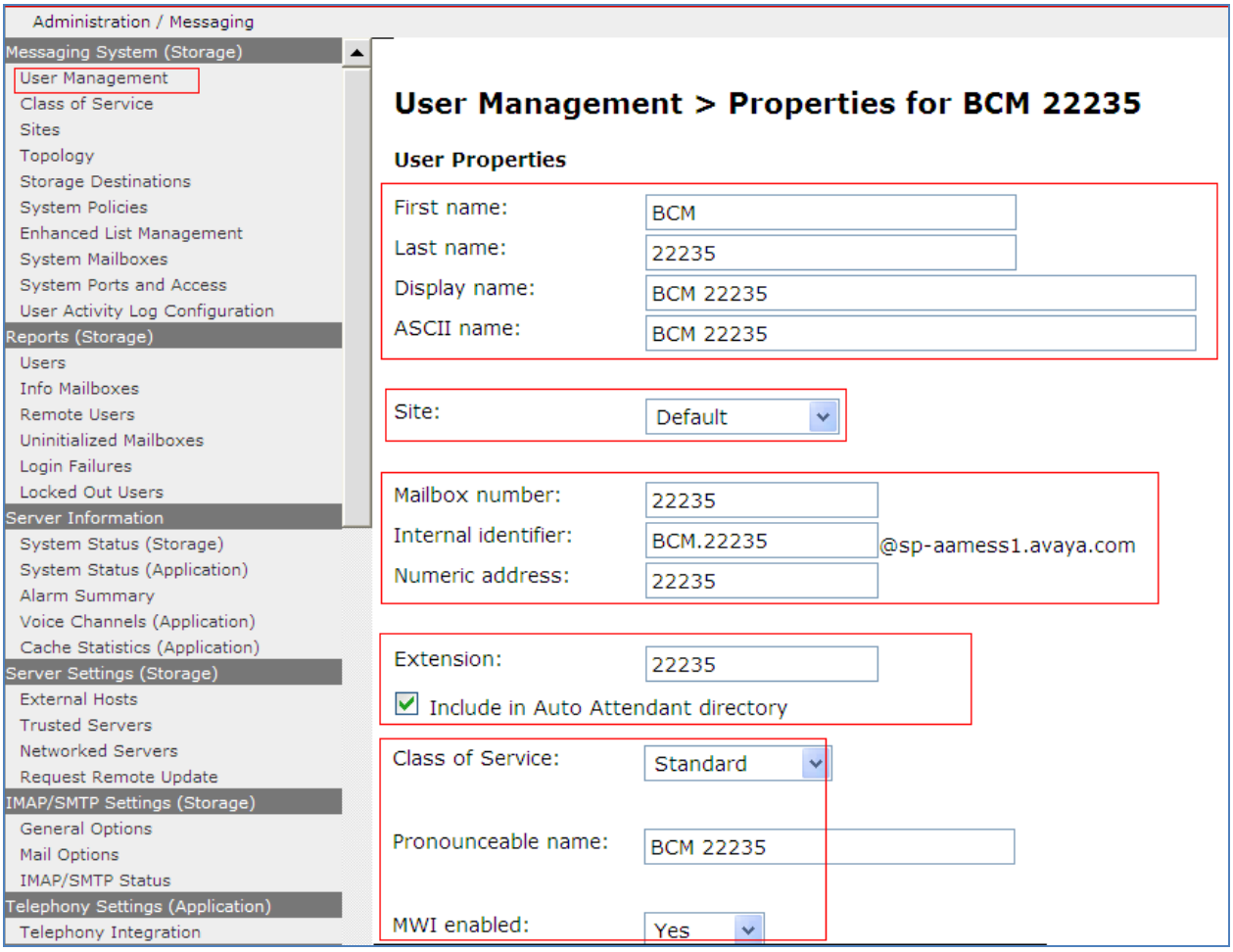
7.5. Administer Subscribers

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

- **First Name** Enter first name
- **Last Name** Enter last name
- **Display Name** Enter display name

©2011 Avaya Inc. All Rights Reserved.

- **ASCII name** Enter the ASCII name
- **Site** Enter site defined in **Section 7.1**
- **Mailbox Number** Enter desired mailbox number i.e. **22235**
- **Internal identifier** Enter the name for internal use
- **Numeric address** Enter the mailbox number
- **Extension** Enter desired extension number i.e. **22235**

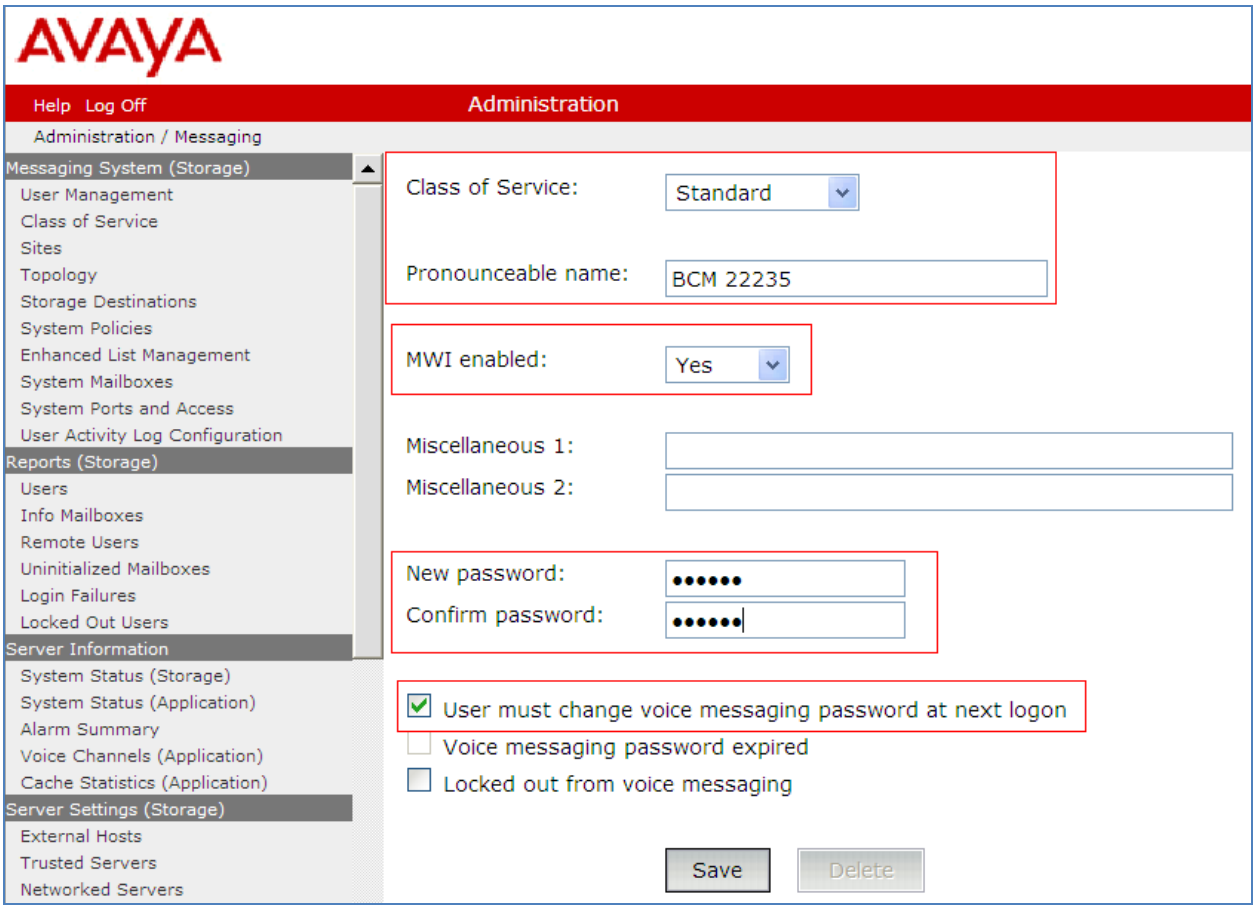


Scroll down on the page to Class of Service.

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

Click **Save** to save changes.

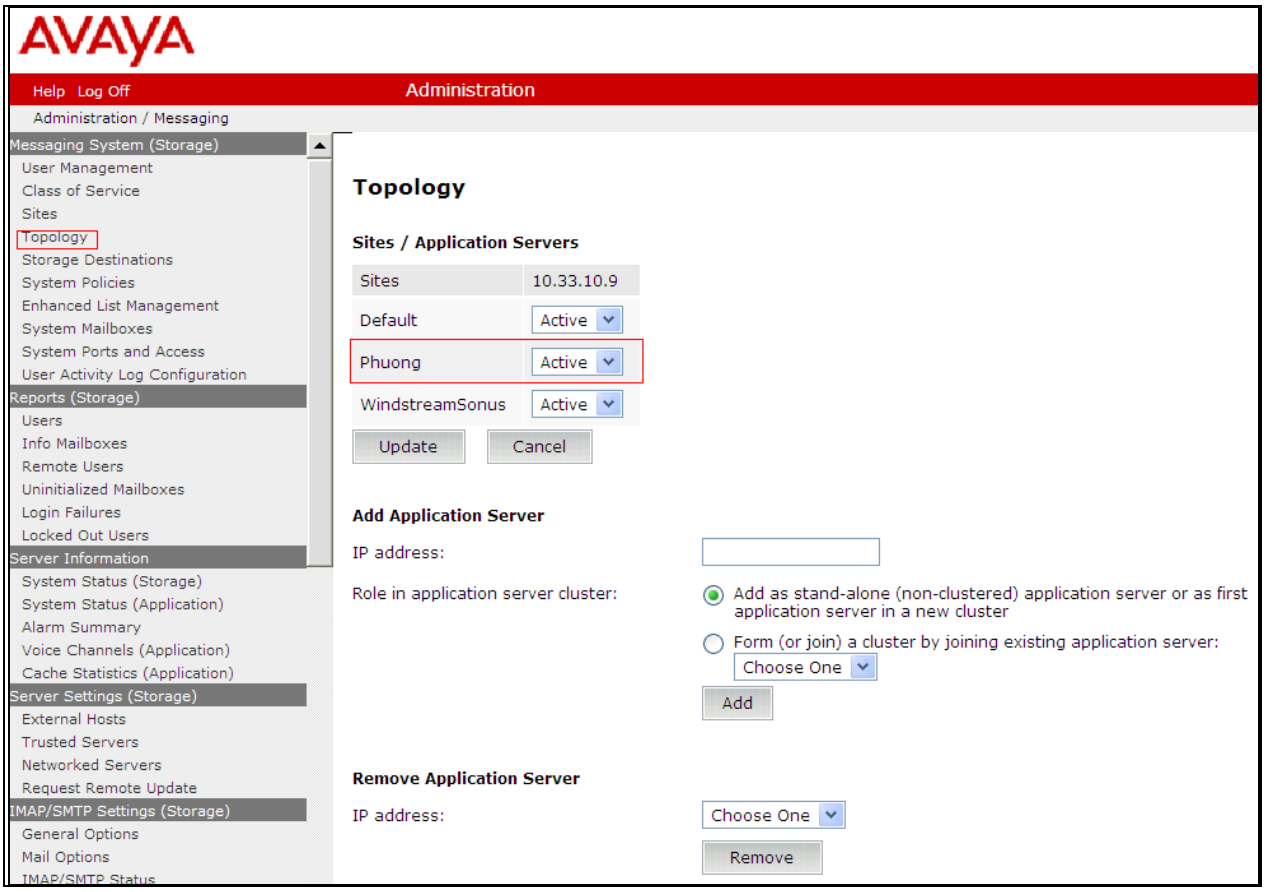
©2011 Avaya Inc. All Rights Reserved.



7.6. Administer Topology

Select Topology under Messaging System (Storage).
Verify the site that defined in **Section7.1** is Active

©2011 Avaya Inc. All Rights Reserved.



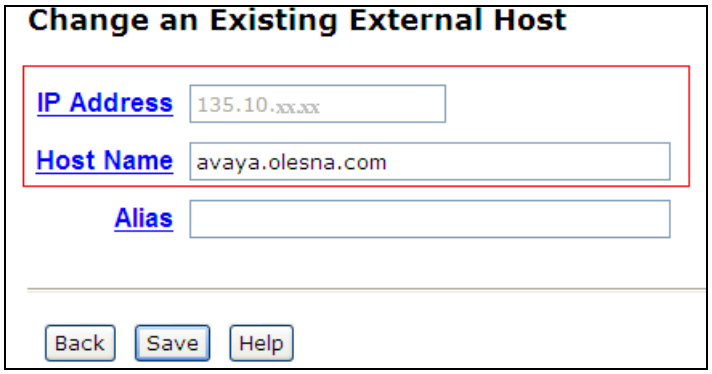
7.7. Administer External Host

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
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.

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

©2011 Avaya Inc. All Rights Reserved.



7.8. Configure Notify Me

Log into the Messaging System Management Interface (SMI) and go to **Administration → Messaging**. In the left panel, under **Messaging System (Storage)** select **User Management**. In the right panel enter mailbox number (e.g. 21613) and Click Edit. Scroll right down to **User Preferences** and select **Open User Preference for** Mailbox number user name:

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 email address: 21613@avaya.olesna.com with the option **Include the recording**. Click Save.

8. Configure Avaya Aura® Session Manager

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

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

In this section, the following topics are discussed:

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- Synchronization

8.1. Configure SIP Domain

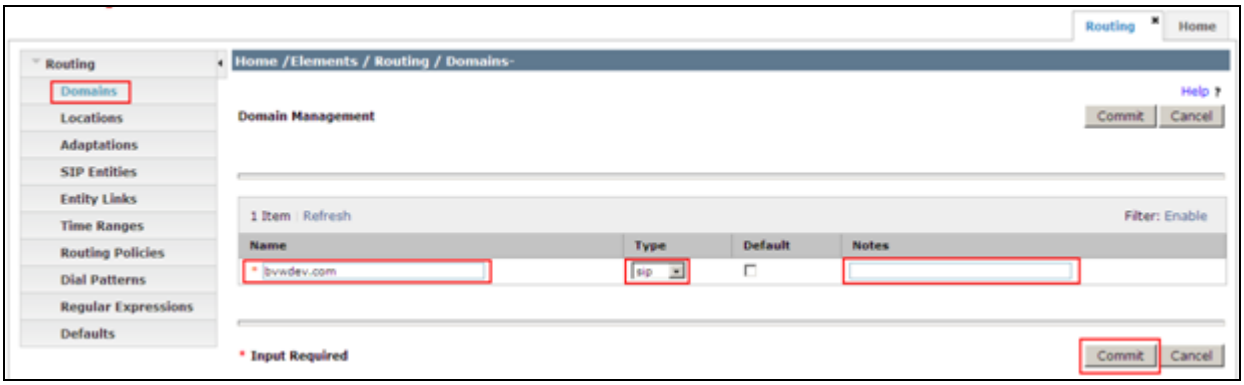
Launch a web browser, enter **http://<IP address of System Manager>/SMGR** in the URL, and log in with the appropriate credentials.

©2011 Avaya Inc. All Rights Reserved.

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

- **Name –** Enter the Authoritative Domain Name specified in **Section 5.1.3**, which is **bvwdev.com**.
- **Type** – Select **SIP**

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



8.2. Configure Locations

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

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

General section

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

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

Location Pattern section

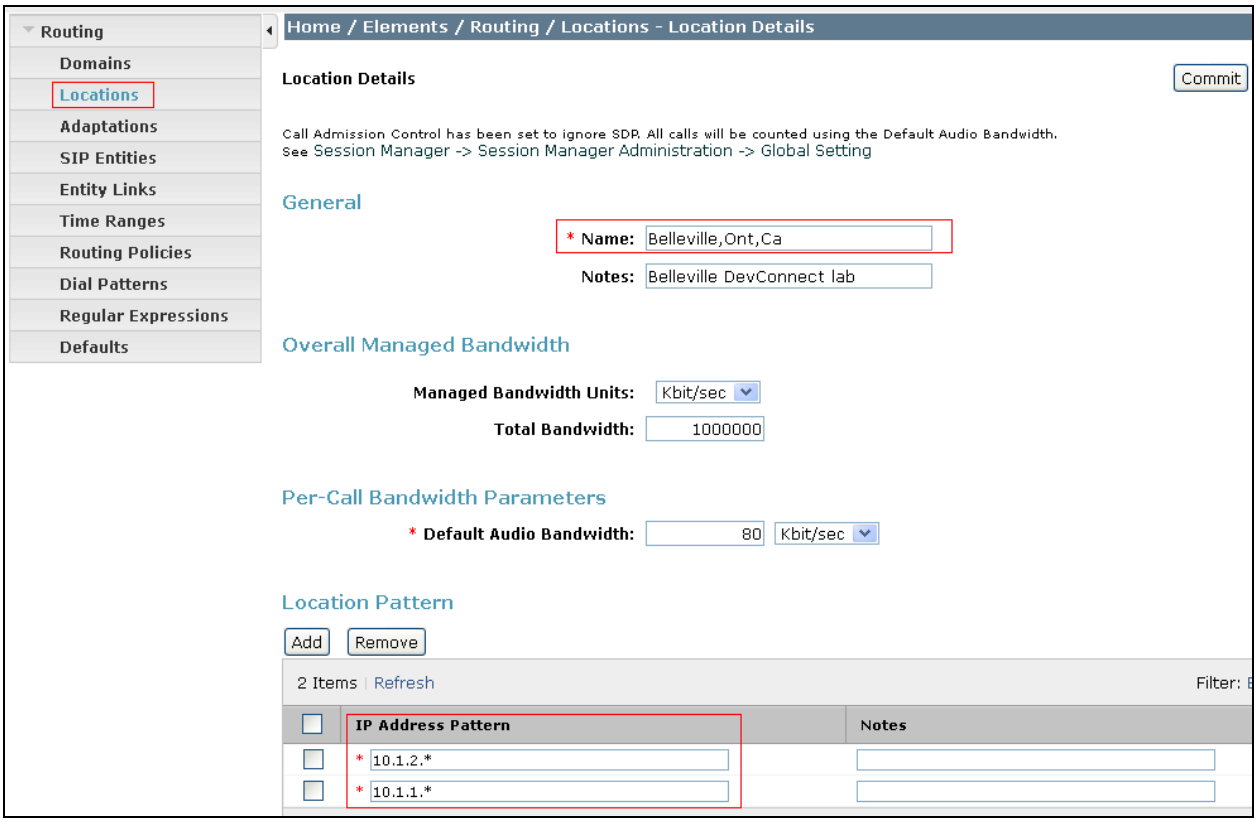
Click **Add** and enter the following values:

- Enter the IP address information for the IP address Pattern (e.g. **10.64.41.***)
- Enter a description in the **Notes** field if desired.

Repeat steps in the Location Pattern section if the Location has multiple IP segments.
Modify the remaining values on the form, if necessary; otherwise, retain the default values.
Click on the **Commit** button.

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

©2011 Avaya Inc. All Rights Reserved.



8.3. Configure SIP Entities

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

- Session Manager itself.
- Communication Manager
- Avaya Aura Messaging
- ESNA server
- Avaya ACE

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

General section

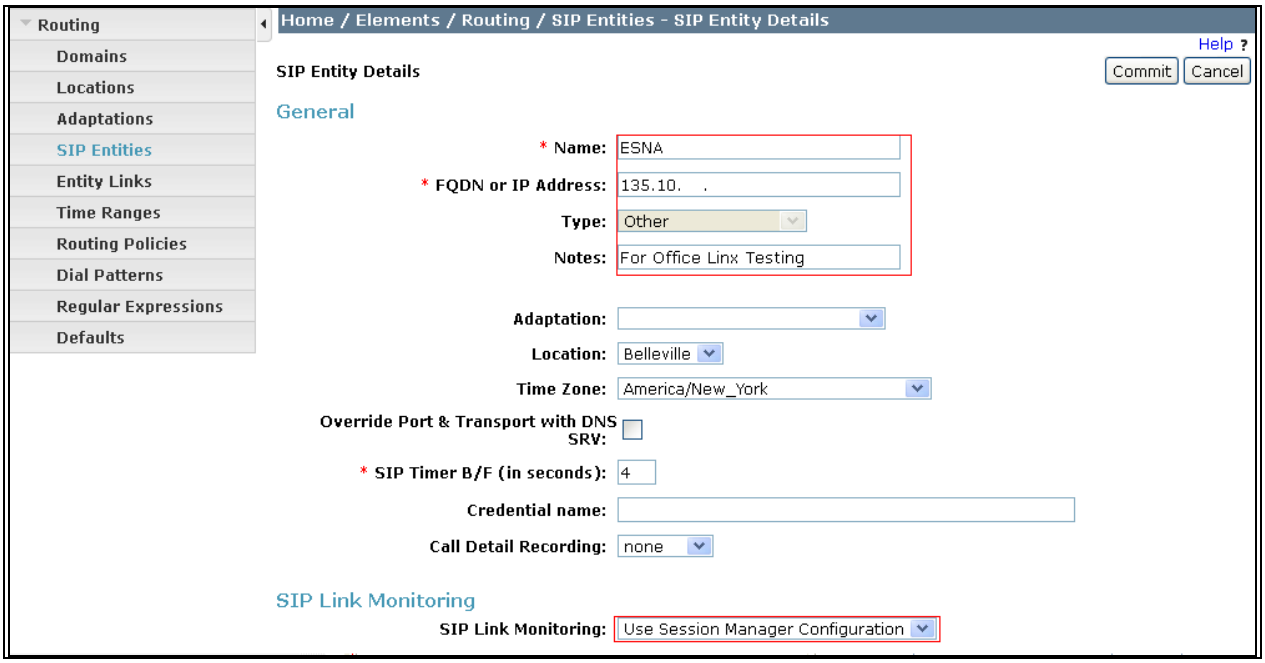
Enter the following values and use default values for remaining fields.

- Enter a descriptive Location name in the Name field.
- Enter IP address for signaling interface on each Communication Manager, virtual SM-100 interface on Session Manager, Avaya Aura Messaging, and ESNA.
- 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

©2011 Avaya Inc. All Rights Reserved.

    - For Messaging, select Modular Messaging
    - For ESNA and Avaya ACE, select Others
- Enter a description in the **Notes** field if desired.
- Select the appropriate time zone.
- Accept the other default values.

Click on the **Commit** button to save each SIP entity. The following screens show the SIP Entities page used during the compliance test.



Repeat all the steps for each new entity

8.4. Configure Entity Links

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

- Session Manager ⇔ Communication Manager (Avaya G450 with S8300D Server)
- Session Manager ⇔ ESNA
- Session Manager ⇔ Avaya Aura Messaging
- Session Manager ⇔ Avaya ACE

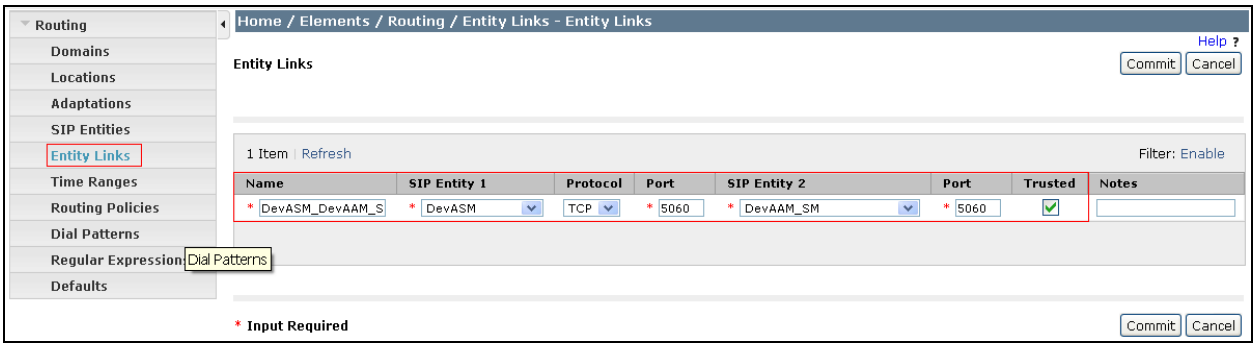
Navigate to **Routing → Entity Links**, and click on the **New** button (not shown) to create a new entity link. Provide the following information:

- Enter a descriptive name in the **Name** field.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section 8.3**.
- In the **Protocol** drop down menu, select the protocol to be used.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).

©2011 Avaya Inc. All Rights Reserved.

- UDP or TCP – 5060
- In the **SIP Entity 2** drop down menu, select an entity created in **Section 8.3**.
- In the **Port** field, enter the port to be used (e.g. **5060**).
- Check the **Trusted** box.
- Enter a description in the **Notes** field if desired.

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



Repeat the steps to define Entity Links between Session Manager, Communication Manager, ESNA (TCP/UDP-5060) and Avaya ACE (UDP-5060).

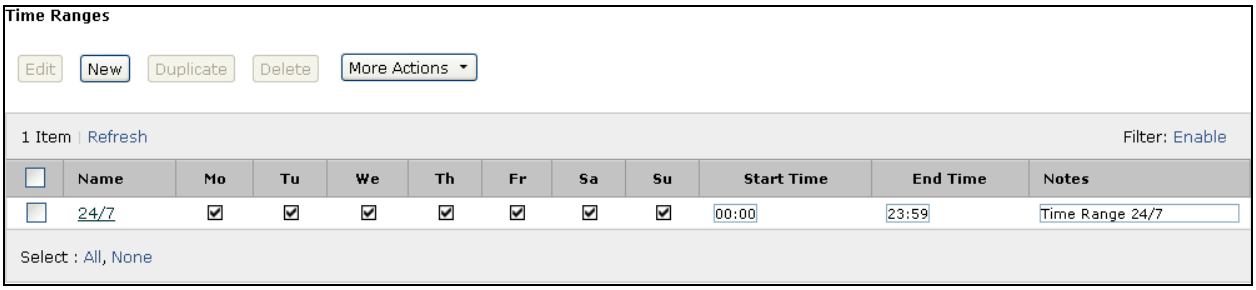
8.5. Time Ranges

The Time Ranges allows admission control criteria to be specified for Routing Policies. In the reference configuration, no restrictions were used.

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

- Enter a descriptive Location name in the **Name** field (e.g. **24/7**).
- Check each day of the week.
- In the **Start Time** field, enter **00:00**.
- In the **End Time** field, enter **23:59**.
- Enter a description in the **Notes** field if desired.

Click the **Commit** button. The following screen shows the Time Range page used during the compliance test.



©2011 Avaya Inc. All Rights Reserved.

8.6. Configure Routing Policy

Routing Policies associates destination SIP Entities with Time of Day admission control parameters and Dial Patterns. In the reference configuration, Routing Policies are defined for: Communication Manager.

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

General section

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

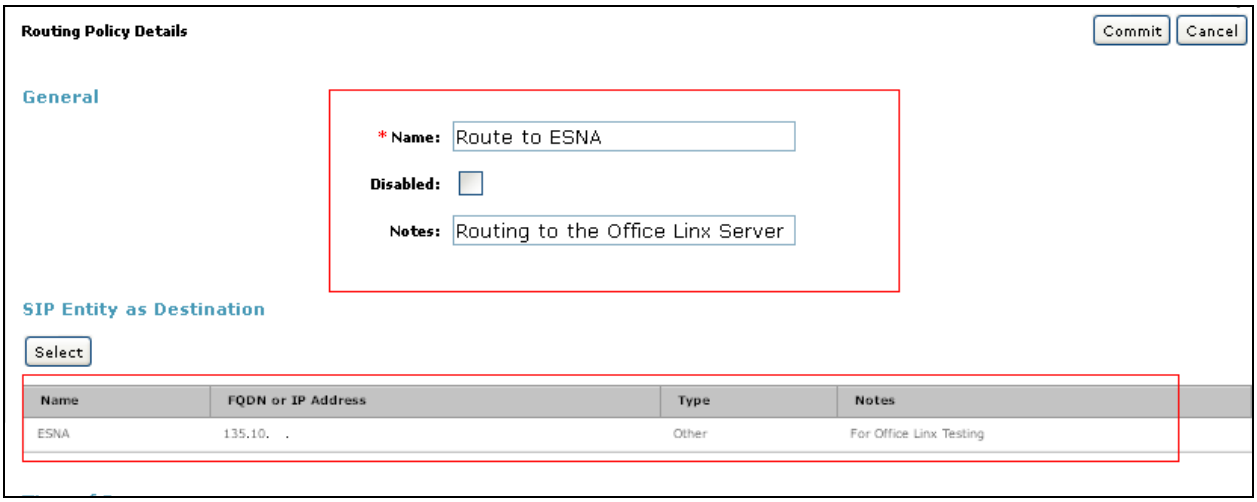
SIP Entity as Destination section

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

Time of Day section

- Leave default values.

Click **Commit** to save Routing Policy definition. The following screen shows the Routing Policy used for the compliance test.



Repeat the steps to define routing policies to others Entities.

8.7. 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.

- 216xx –Communication Manager 5.2 extensions.

©2011 Avaya Inc. All Rights Reserved.

- 53000 – ESNA pilot number
- 39990 – Avaya Aura Messaging access number.

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

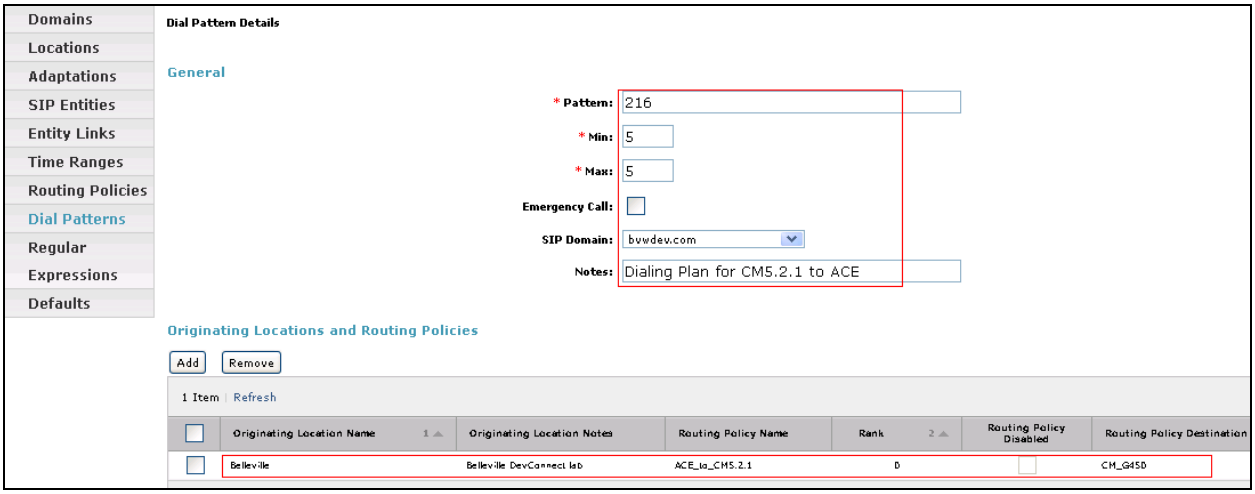
General section

- Enter a unique pattern in the **Pattern** field (e.g. **216**).
- In the **Min** field enter the minimum number of digits (e.g. **5**).
- In the **Max** field enter the maximum number of digits (e.g. **5**).
- In the **SIP Domain** field drop down menu select the domain that will be contained in the Request URI *received* by Session Manager from Communication Manager.
- Enter a description in the **Notes** field if desired.

Originating Locations and Routing Policies section

- Click on the **Add** button and a window will open (not shown).
- Click on the boxes for the appropriate Originating Locations, and Routing Policies that pertain to this Dial Pattern.
    - Location All.
    - Routing Policies **ACEtoCM5.2**.
    - Click on the **Select** button and return to the Dial Pattern window.

Click the **Commit** button to save the new definition. The following screen shows the dial pattern used for DevCM3 during the compliance test.



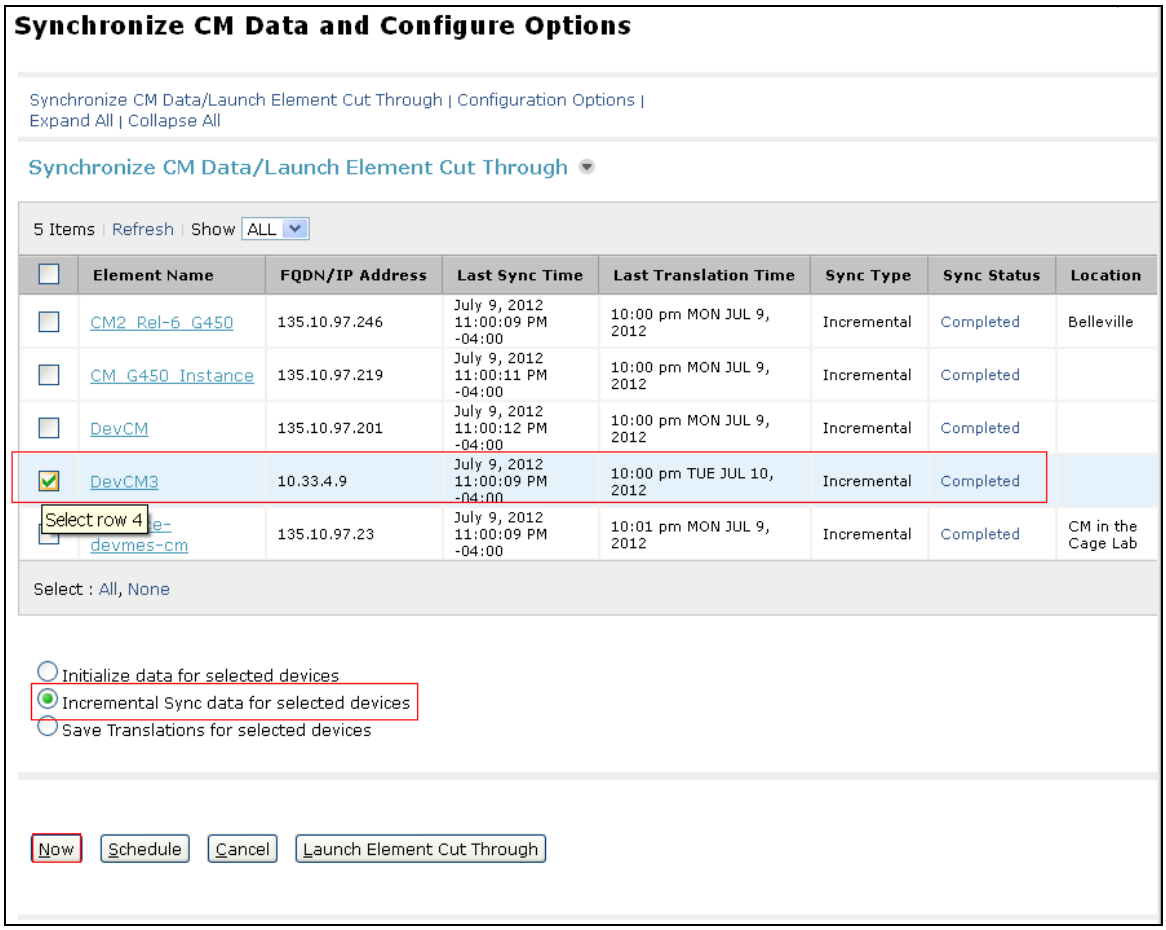
8.8. Synchronization Changes with Avaya Aura® Communication Manager

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

©2011 Avaya Inc. All Rights Reserved.

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**.



9. Configure Avaya ACE 3.0

This section provides information on how to manage certificates for Avaya Agile Communication Environment™ (ACE) on Linux installations using the OpenSSL version installed with Avaya ACE.
And the manual process on Avaya AES to manually carry out steps for obtaining and installing certificates such as submit a request to a CA, handle the receipt of the certificates, and then install the certificates.

- Creating a directory for the OpenSSL CA files
- Creating an OpenSSL configuration file

©2011 Avaya Inc. All Rights Reserved.

- Generating a CA certificate
- Create a server certificate request for AE Services
- Creating the ACE certificate request
- Signing an AES certificate request
- Signing an ACE certificate request
- Importing the server certificate into AE Services
- Add Trusted Host

9.1. Administer certificate

9.1.1. Creating a directory for the OpenSSL CA files

Using Putty to SSH into ACE and cd to root dir then create a dir called CA

```
[root@ace1 ~]#
[root@ace1 ~]#
[root@ace1 ~]# cd /root
[root@ace1 ~]# mkdir CA
```

Go to the directory you created for storing the OpenSSL CA files:
cd CA

```
[root@ace1 CA2]#
[root@ace1 CA2]# cd CA
```


©2011 Avaya Inc. All Rights Reserved.

9.1.2. Creating an OpenSSL configuration file

Create a file called openssl.conf that defines the OpenSSL configuration settings.
You do not need to modify the parameters as they will be set in a subsequent procedure. The file can exist as shown below.

```
HOME = .
RANDFILE = $HOME/.rnd
[ req ]
x509_extensions = v3_ca
distinguished_name = req_distinguished_name
string_mask = nombstr
[ req_distinguished_name ]
countryName = CA
countryName_default = CA
countryName_min = 2
countryName_max = 2
stateOrProvinceName = ON
stateOrProvinceName_default = Some-State
localityName = OTT
organizationName = Avaya
organizationName_default = Avaya
organizationalUnitName = ACE
commonName = ACE CA
commonName_max = 64
[ v3_ca ]
basicConstraints = CA:TRUE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
keyUsage = digitalSignature,cRLSign,keyCertSign
[ usr_cert ]
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = digitalSignature,keyEncipherment
extendedKeyUsage = clientAuth,serverAuth,msSGC,nsSGC
nsCertType = client,server
```

9.1.3. Generating a CA certificate

1. Log in to the ACE server as root.
2. Go to the directory you created for storing the OpenSSL CA files:
   cd CA
3. Generate the CA certificate. Enter:
   openssl req -new -x509 -subj "/C=CA/ST=ON/L=OTT/O=Avaya/OU=ACE/CN=ACE CA" -days 1000 -newkey rsa:1024 -sha1 -keyout ACEca.private.key -out ACEca.crt -config openssl.conf
4. At the prompt for a password, enter a password for the CA certificate private.
5. Verify ACEca.crt is created in CA folder.

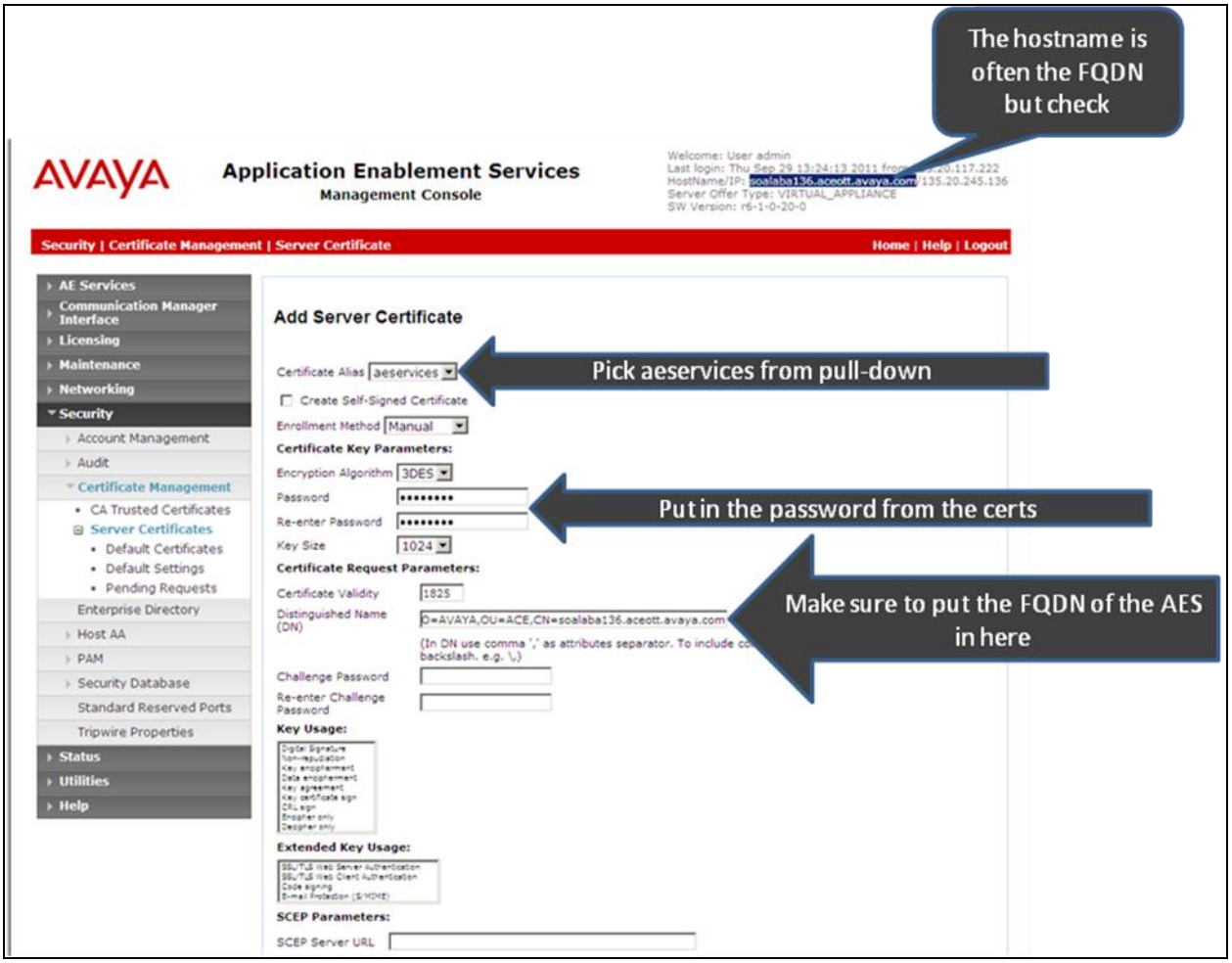
See screenshot below for detail of step 3 and 4:

©2011 Avaya Inc. All Rights Reserved.

```
[root@ace1 CA2]# openssl req -new -x509 -subj "/C=CA/ST=ON/L=OTT/O=Avaya/OU=ACE/
CN=ACE CA" -days 1000 -newkey rsa:1024 -sha1 -keyout ACEca.private.key -out ACEc
a.crt -config openssl.conf
Generating a 1024 bit RSA private key
..++++++
.........................++++++
writing new private key to 'ACEca.private.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

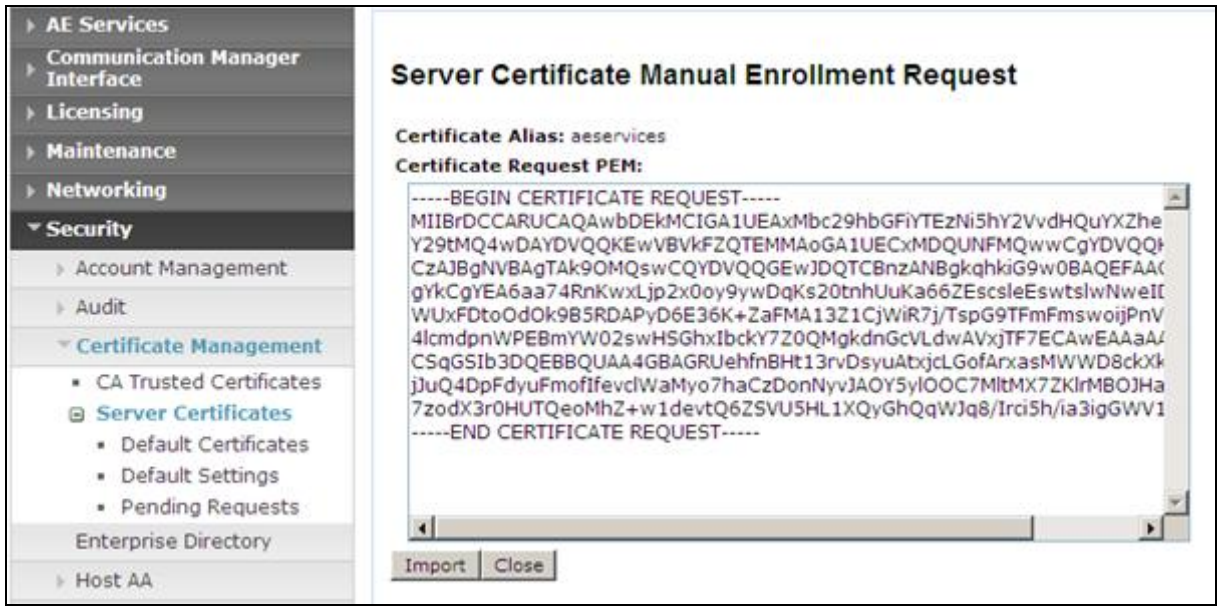
9.1.4. Create a server certificate request for AE Services

1. Login Avaya AES
2. Go to **Security → Certificate Management → Server Certificate,** click **Add.**
3. Enter information as figure below; example of what needs to be put into place: C=CA,ST=ON,L=OTT,O=Avaya,OU=ACE,CN=aesserver.avaya.com

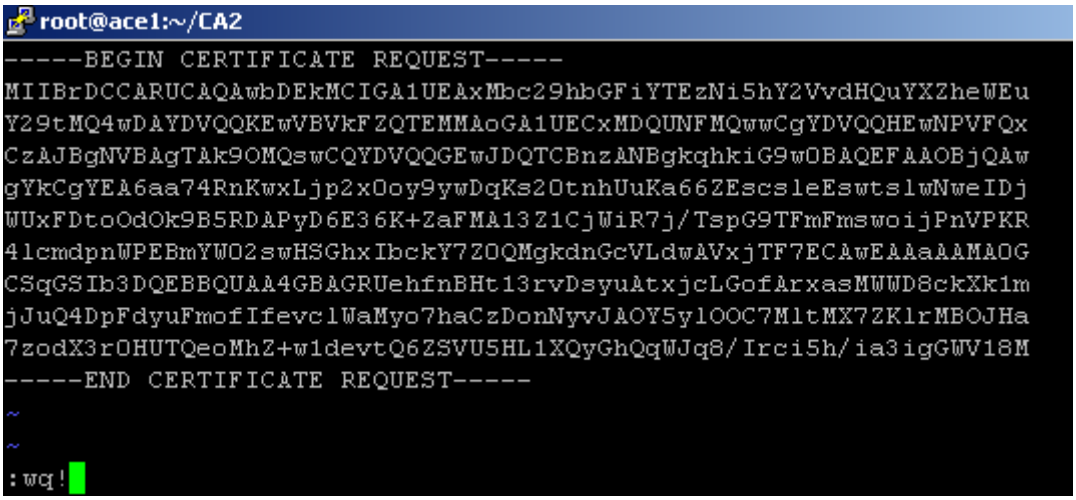


4. Click Apply to add.
5. The Server certificate Manual Enrollment Request display as figure below:

©2011 Avaya Inc. All Rights Reserved.



6. Copy content of this Certificate Request PEM.
7. On SSH screen of ACE server, type vi
8. Paste content copied in step 6 then hit Esc and type: wq!
9. Save file as aes.req in CA folder. See below figure.



©2011 Avaya Inc. All Rights Reserved.

9.1.5. Creating the ACE certificate request

1. Go to the directory you created for storing the OpenSSL CA files:
   cd CA
2. Create a certificate request. Enter:

openssl req -new -subj "<subject>" -newkey rsa:1024 -sha1 -nodes -keyout ace.private.key -out ace.req –config openssl.conf

Parameter	Description
Subject	Make appropriate for your site. In particular, set the CN to the FDQN of the ACE for which this certificate is destined. For example, "/C=CA/ST=ON/L=OTT/ O=Avaya/OU=ACE/CN=ace1.avaya.com"
ace.private.key	This file contains the unencrypted private key associated with the certificate that will be created based on this certificate request.
ace.req	This file contains the certificate request.

Output is:

```
[root@ace1 CA2]# openssl req -new -subj "/C=CA/ST=ON/L=OTT/O=Avaya/OU=ACE/CN=ace
1.gmiott.avaya.com" -newkey rsa:1024 -sha1 -nodes -keyout ace.private.key -out a
ce.req -config openssl.conf
Generating a 1024 bit RSA private key
.....................................++++++
.............++++++
writing new private key to 'ace.private.key'
-----
[root@ace1 CA2]#
```

9.1.6. Signing an AES certificate request

Input the following command to AES request. Note: phase is re-used again in next section (best practice to keep them all the same)

openssl x509 -req -in **aes.req** -out **aes.crt** -CA **ca.crt** -CAkey **ca.private.key** -days **500** -extfile openssl.conf -extensions usr_cert –CAcreateserial

```
[root@ace1 CA2]# openssl x509 -req -in aes.req -out aes.crt -CA AESca.crt -CAkey
 AESca.private.key -days 500 -extfile openssl.conf -extensions usr_cert -CAcreat
eserial
Signature ok
subject=/CN=soalaba136.aceott.avaya.com/O=AVAYA/OU=ACE/L=OTT/ST=ON/C=CA
Getting CA Private Key
Enter pass phrase for AESca.private.key:
[root@ace1 CA2]#
```

Download the certificate to your AE Services administrative workstation, and save it with a unique name, for example C:\CA\AESca.crt

©2011 Avaya Inc. All Rights Reserved.

9.1.7. Signing an ACE certificate request

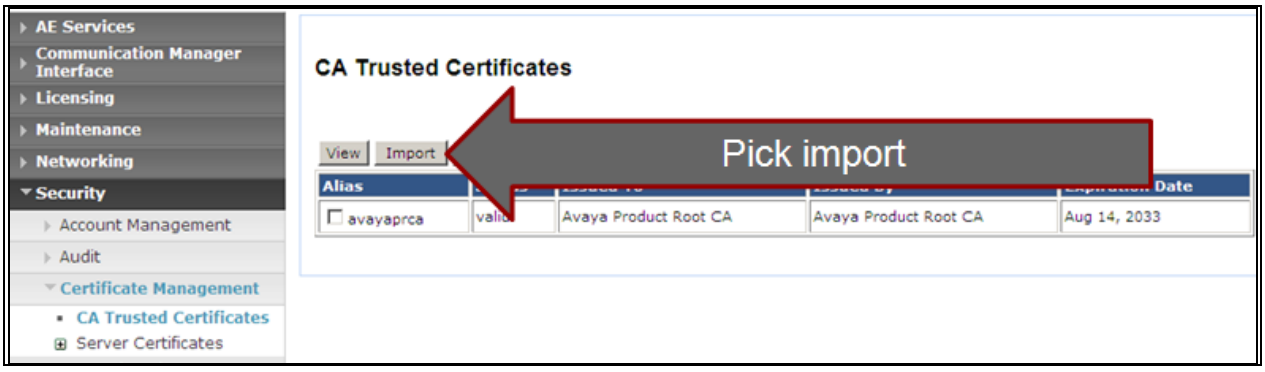
Sign the certificate request. Enter:
openssl x509 -req -in **ace.req** -out **ace.crt** -CA **ACEca.crt** -CAkey **ACEca.private.key** -days 500 -extfile openssl.conf -extensions usr_cert -CAcreateserial

```
[root@ace1 CA2]#
[root@ace1 CA2]# openssl x509 -req -in ace.req -out ace.crt -CA ACEca.crt -CAkey
 ACEca.private.key -days 500 -extfile openssl.conf -extensions usr_cert -CAcreat
eserial
Signature ok
subject=/C=CA/ST=ON/L=OTT/O=Avaya/OU=ACE/CN=ace1.gmiott.avaya.com
Getting CA Private Key
Enter pass phrase for ACEca.private.key:
[root@ace1 CA2]#
```

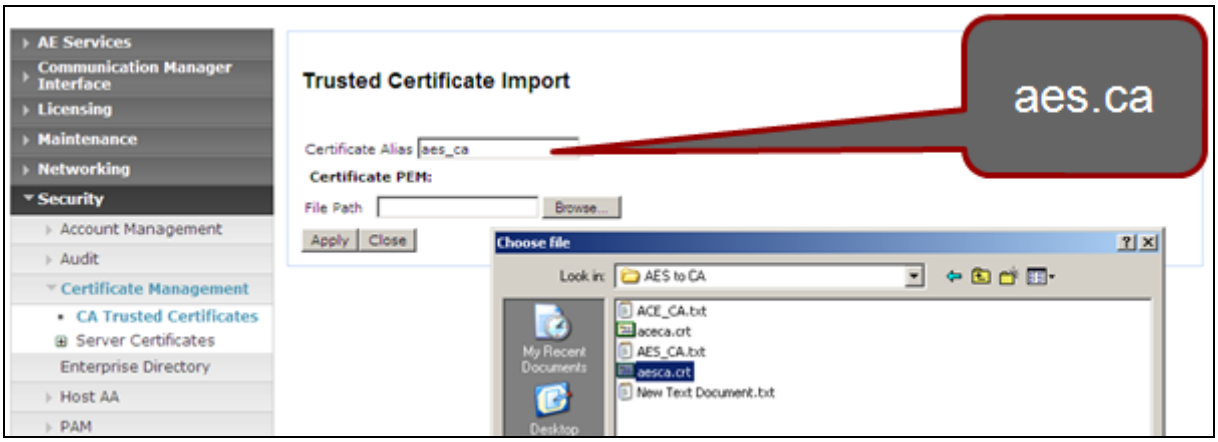
Download the certificate to your AE Services administrative workstation, and save it with a unique name, for example C:\CA\ACEca.crt

9.1.8. Importing the server certificate into AE Services

On AES select **Security → Certificate Management → CA Trusted Certificates,** click **Import**



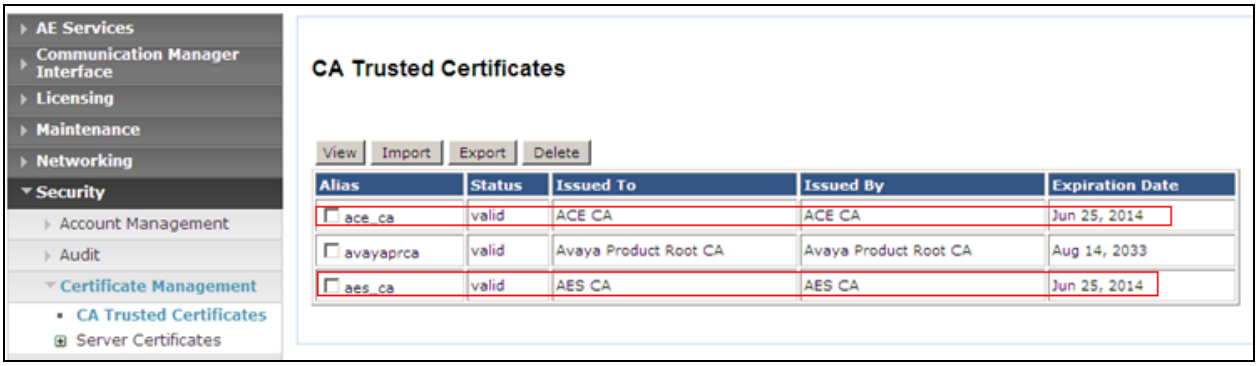
Browse to the folder on PC desktop pick the aesca.crt



©2011 Avaya Inc. All Rights Reserved.

Ensure the cert is imported successfully.

Repeat the same step for ACEca.crt.
Go to **Security → Certificate Management → CA Trusted Certificates**: verify CA trusted certificates now in place and their status are Valid.



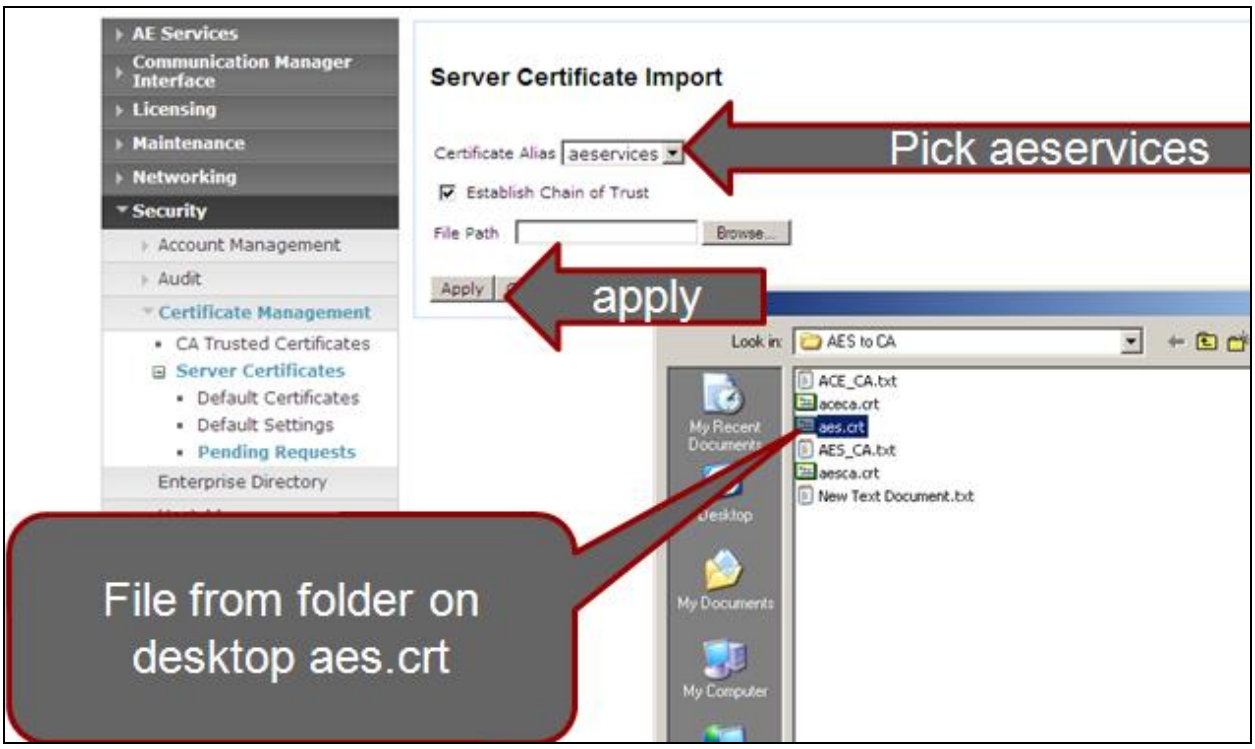
Select **Security → Certificate Management → Server Certificates → Pending Request**

©2011 Avaya Inc. All Rights Reserved.

In Server Certificate Manual Enrollment Request click on Import button (not shown)

Download the certificate to your AE Services administrative workstation, and save it with a unique name, for example C:\CA\aes.crt

Select **Security → Certificate Management → Server Certificates → Pending Request**



Make sure import is successful.
Verify the server certificate in place and its status is valid.

©2011 Avaya Inc. All Rights Reserved.

9.1.9. Add Trusted Host

Select S**ecurity → Host AA → Trusted hosts,** click **Add.**
Enter ACE FQDN for Certificate CN or SubAttName.
Note: to verify ACE FQDN, in ACE putty type host name

```
[root@ace1 CA2]# hostname
ace1.gmiott.avaya.com
[root@ace1 CA2]#
```

Click Apply Changes button. Then click Apply in Add Trusted Host screen. (Not shown)
Verify there is a record for ACE as a trusted host.

9.2. Certificate management using the IBM Integrated Solutions Console for ACE on Linux

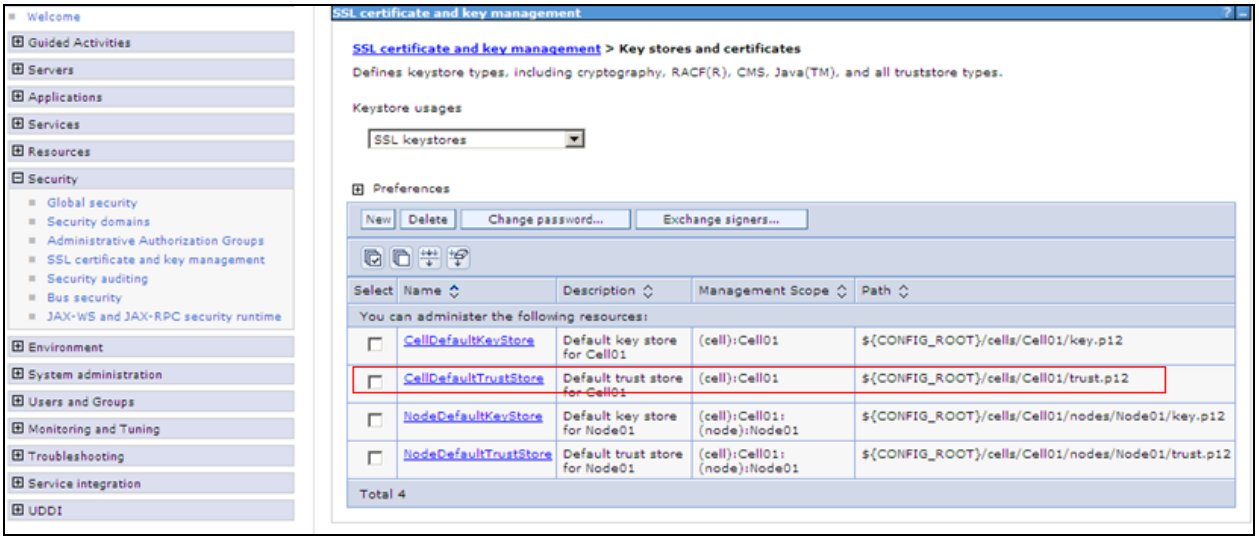
For Avaya Agile Communication Environment™ (ACE) on Linux installations, you can manage certificates on using the IBM Integrated Solutions Console. Procedures documented in this section are based on IBM WebSphere documentation. IBM WebSphere product documentation is available online at the following location:
http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?S_TACT=105AGX10&S_CMP=LP.

©2011 Avaya Inc. All Rights Reserved.

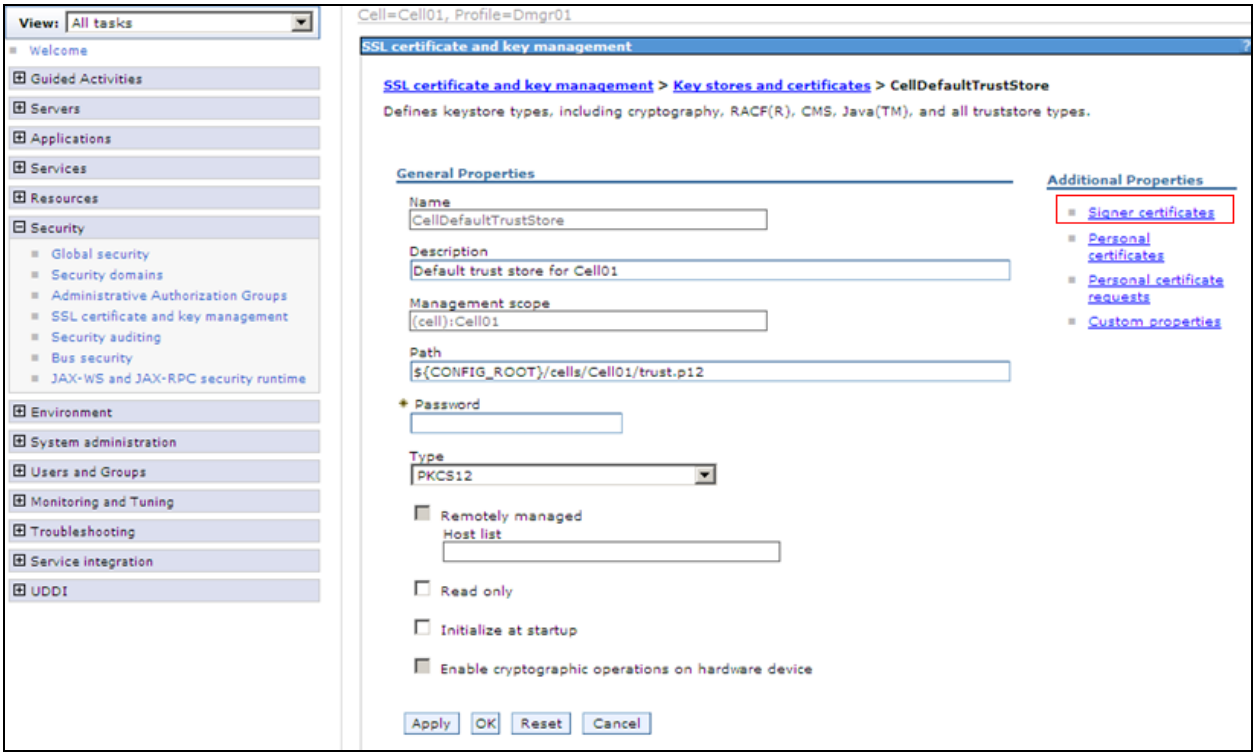
Open web browser and go to ACE WAS admin page https://<ACEipaddress>:9043/admin

9.2.1. Creating a key store using the IBM Integrated Solutions Console

Go to **Security → SSL Certificate and Key Management** then under **Related Items** pick **Key stores and certificates**

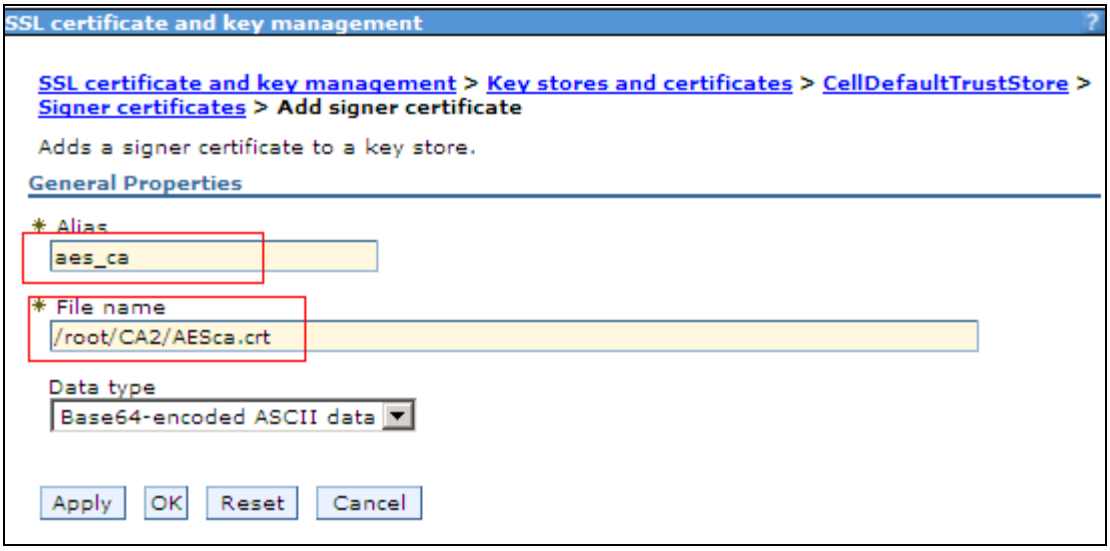


Select **celldefaulttruststore → Signer Certificates**



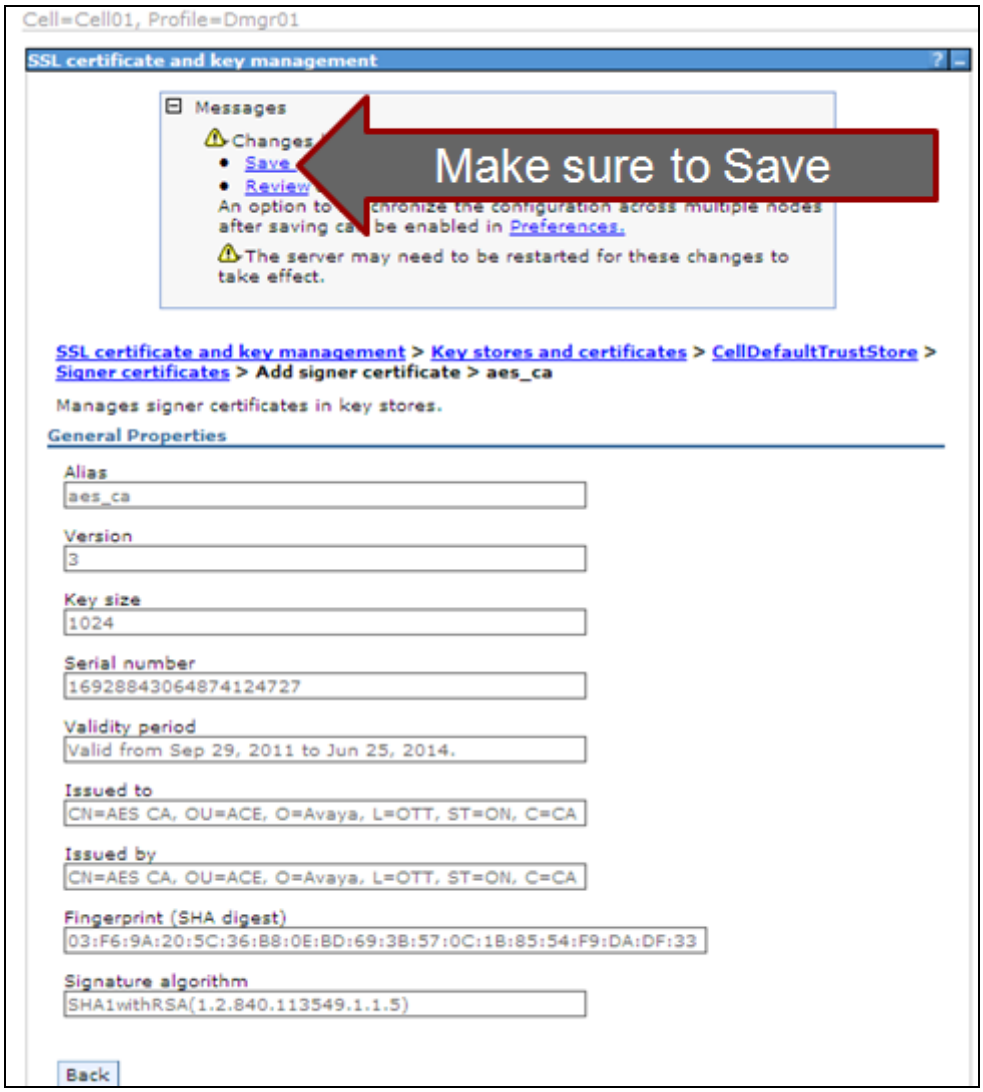
Once at the signer certs menu pick **Add**
Enter information as below figure:

©2011 Avaya Inc. All Rights Reserved.



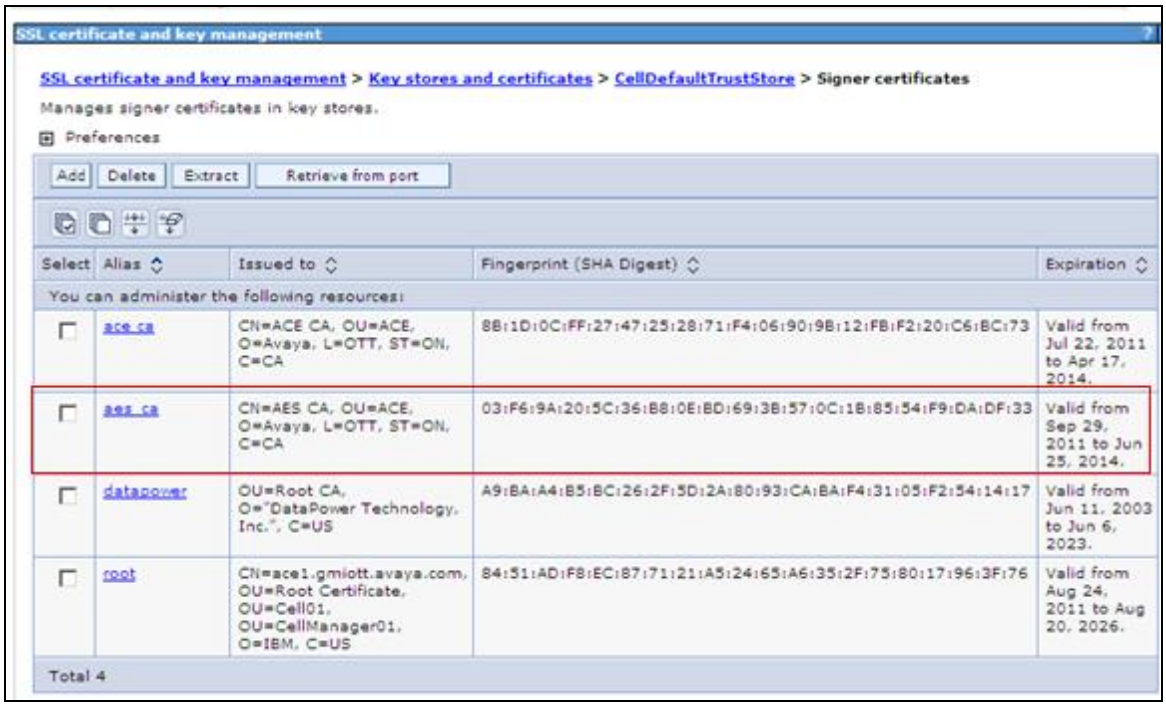
Make sure click save on the next screen. See figure below:

©2011 Avaya Inc. All Rights Reserved.



New alias is added

©2011 Avaya Inc. All Rights Reserved.



9.2.2. Export ACE server cert

openssl pkcs12 -export -in **ace.crt** -inkey **ace.private.key** -name "**ACE Certficate**" -out **ace.p12**

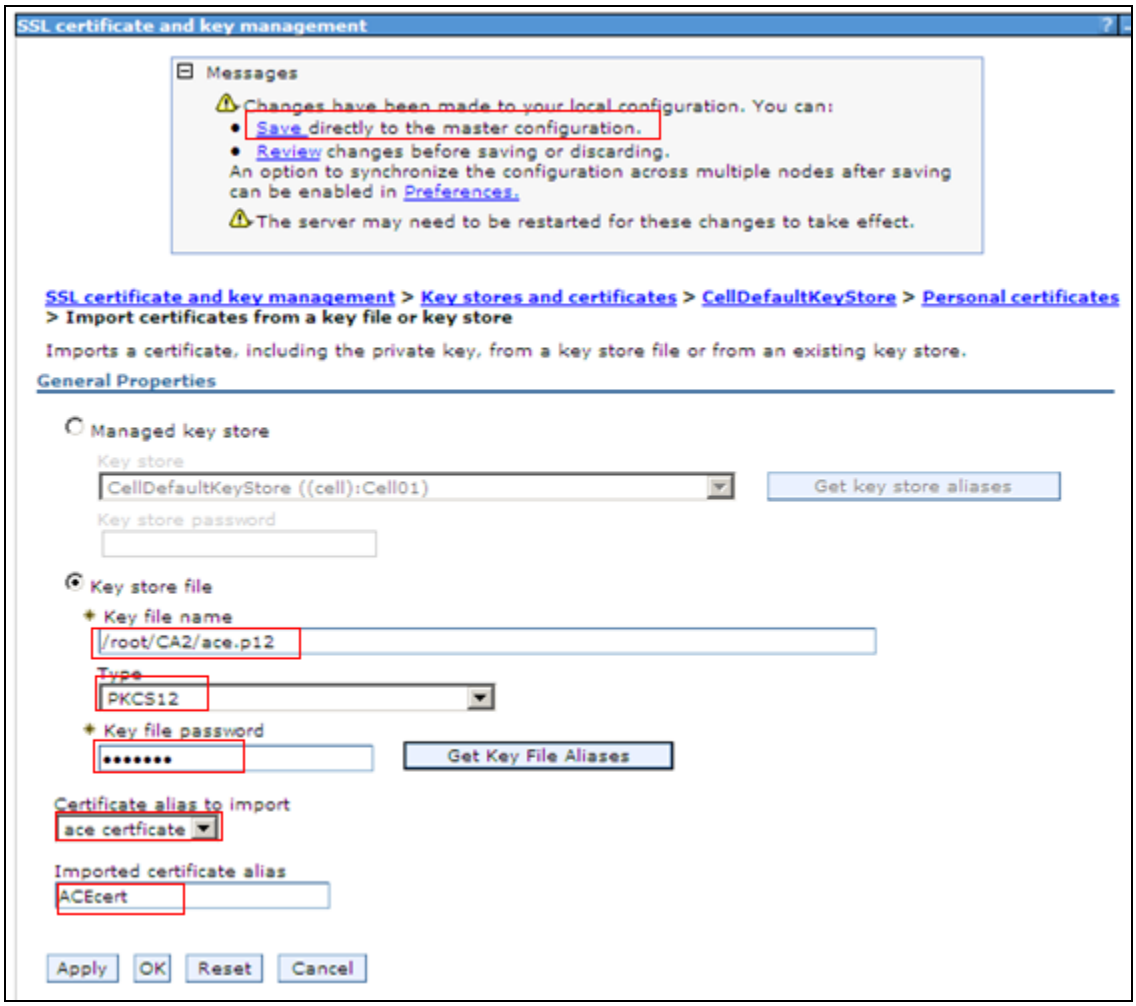
```
[root@ace1 CA2]#
[root@ace1 CA2]# openssl pkcs12 -export -in ace.crt -inkey ace.private.key -name
 "ACE Certficate" -out ace.p12
Enter Export Password:
Verifying - Enter Export Password:
[root@ace1 CA2]#
```

9.2.3. Administer Keystore

Select **Security → SSL Certificate and Key Management** then under **Related Items** pick **Key stores and certificates**

Select **celldefaultkeystore → Personal Certificates**
Select **Import**
In the next screen enter the following information:
Key File Name: File created in **Section 9.2.2**
Type: PKCS12
Key file password: key file password.
Certificate alias to Import: ace certificate
Imported certificate alias: ACEcert

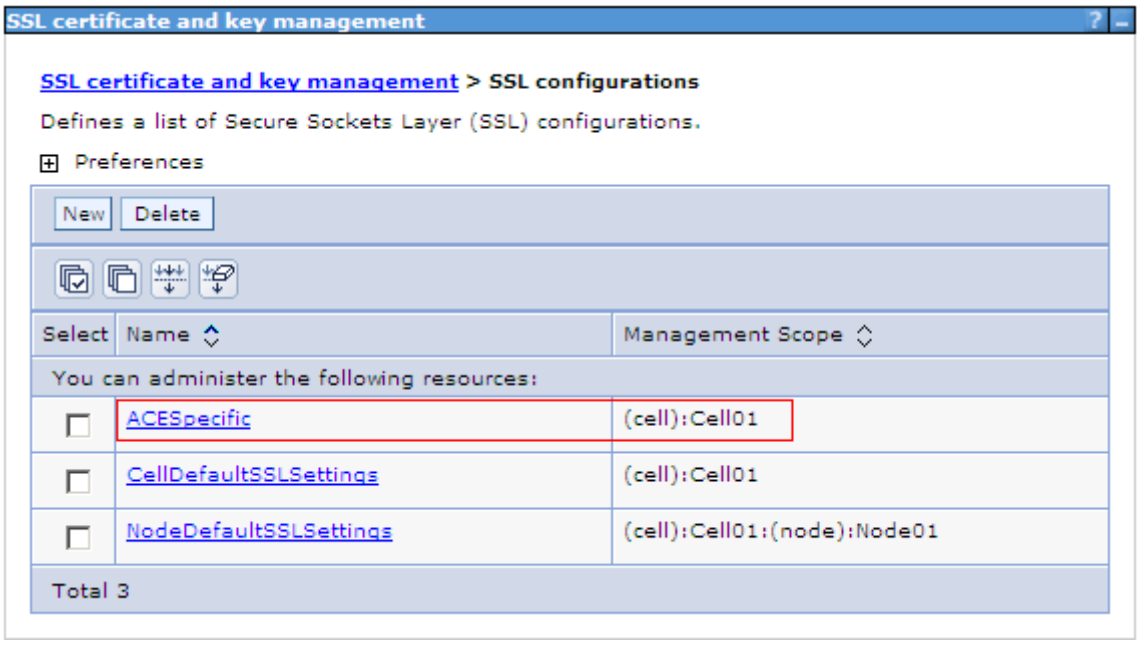
©2011 Avaya Inc. All Rights Reserved.



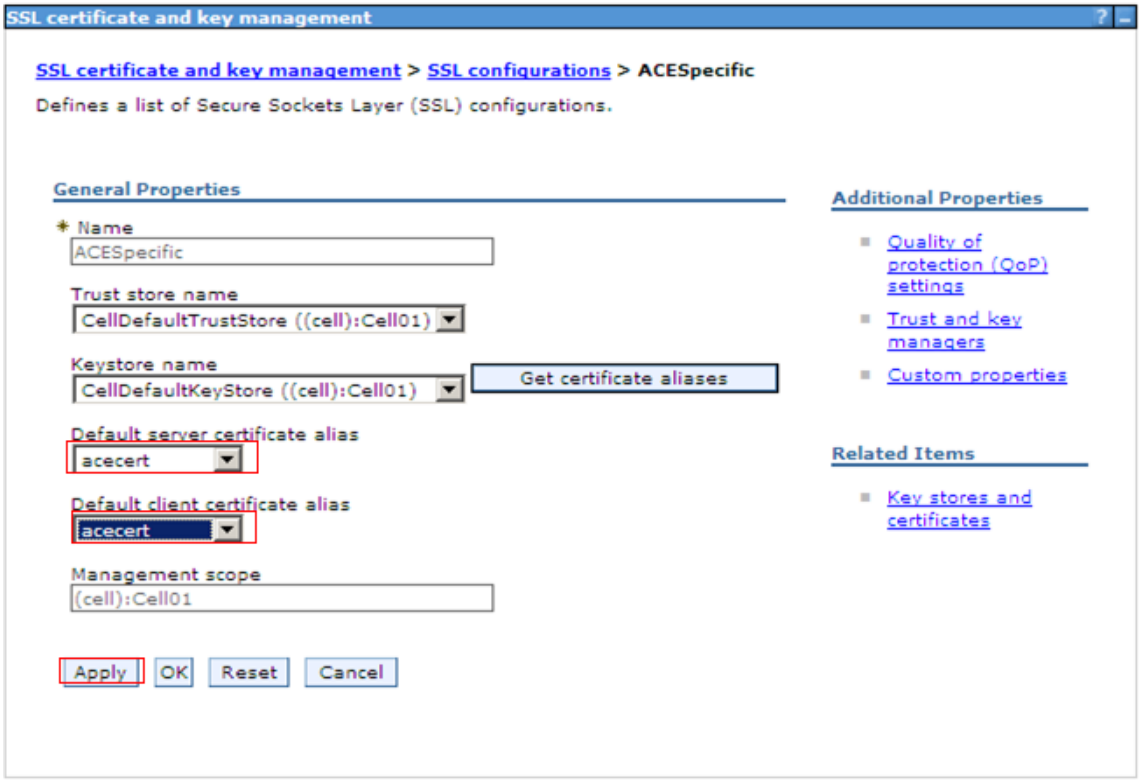
Click Apply and click Save.

Select **Security → SSL Certificate and Key Management**
Select **SSL Configuration → ACESpecific**

©2011 Avaya Inc. All Rights Reserved.



From the pull down options for default server and client pick acecert

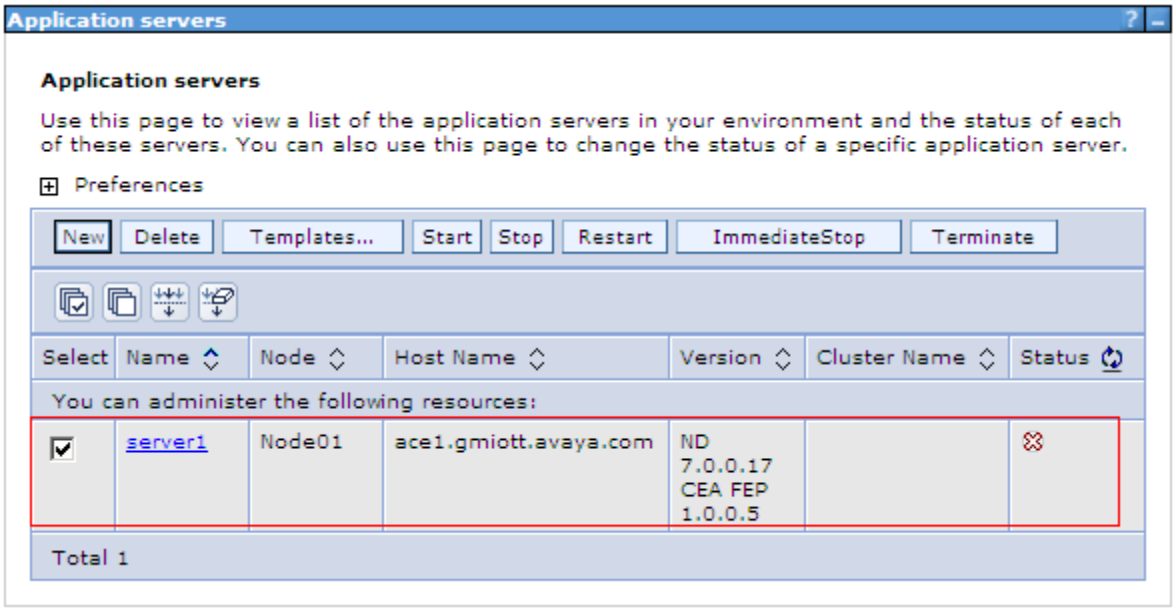


Make sure to click Save.

©2011 Avaya Inc. All Rights Reserved.

9.2.4. Restart Avaya ACE and AE server

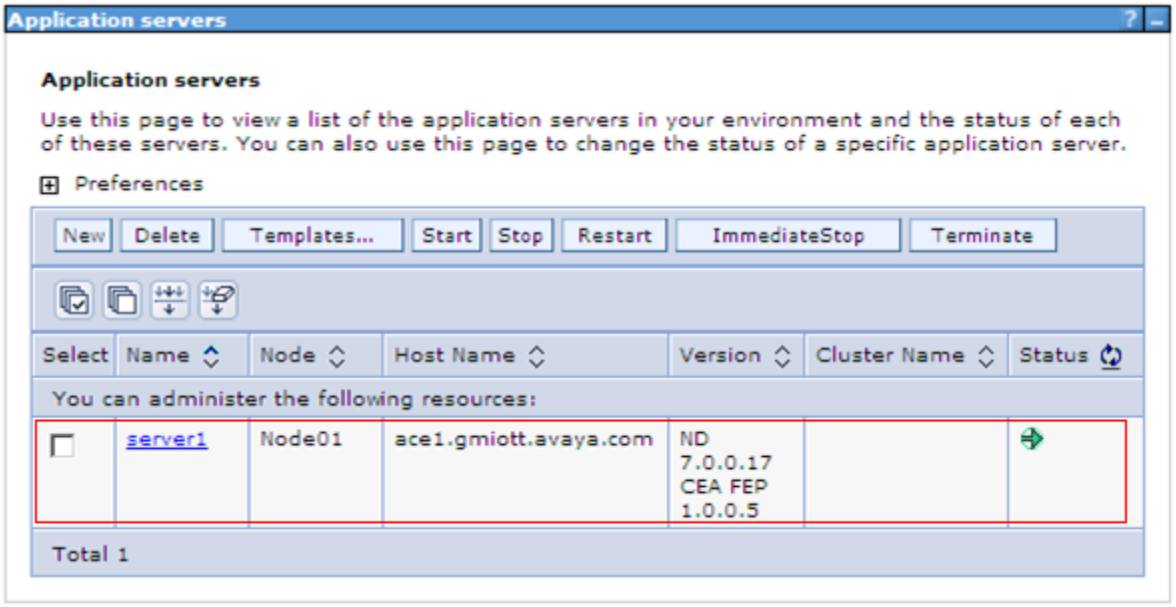
Restart Avaya ACE application server to have installed certificated get affect by go to **Servers → Server Types → WebSphere Application Servers** and click on **Stop** to stop the server. Click Ok to confirm. Below figure show the server status is Stop (shown by an X).



Restart AE server by login AE Server, select **Maintenance → Service Controller** and click on **Restart AE Server.** Then click on Restart button in the next screen to confirm restart (Not shown).

Go to ACE IBM Integrated Solution Console and start ACE by select **Servers → WebSphere Application Server** and select **Start.** Verify the server status is back and indicated with a green arrow.

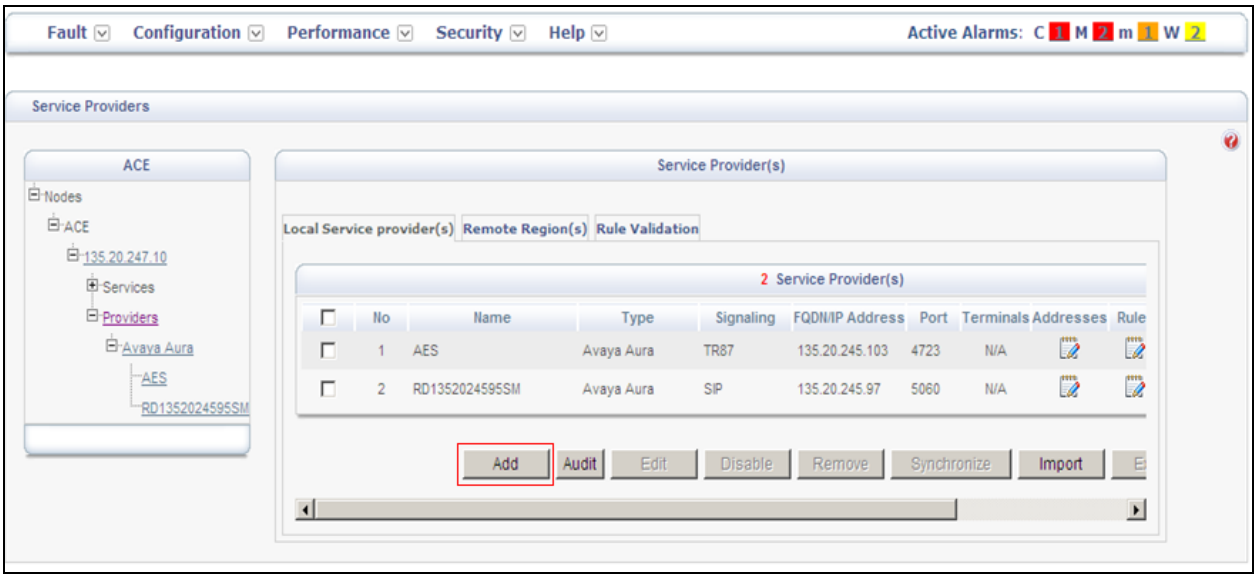
©2011 Avaya Inc. All Rights Reserved.



9.3. Add Service Provider

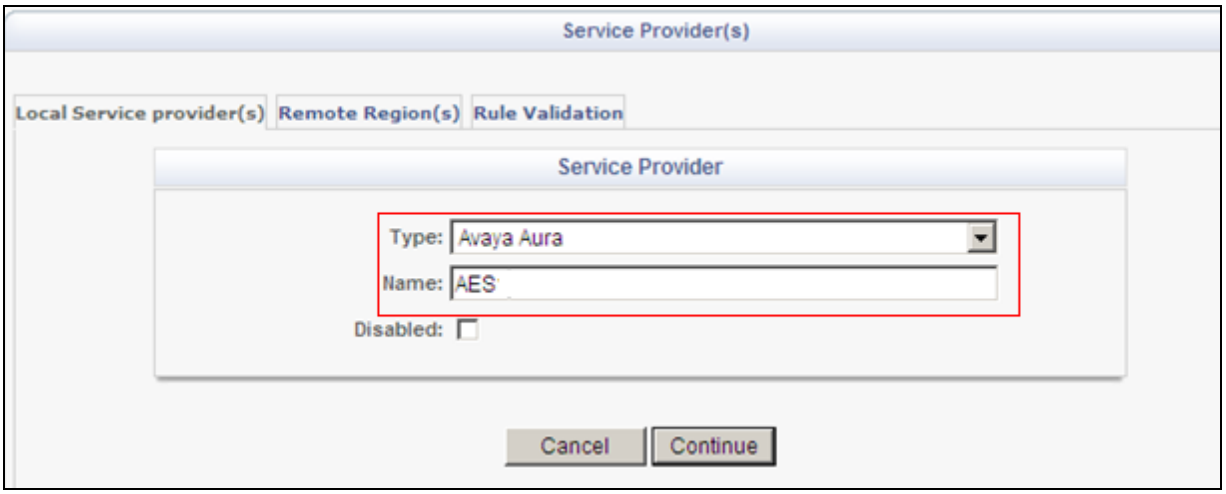
9.3.1. Add AE server provider using TR87 service

Log into ACE https://<ACEipaddress>:9443/oamp and go to service providers to add a new service provider

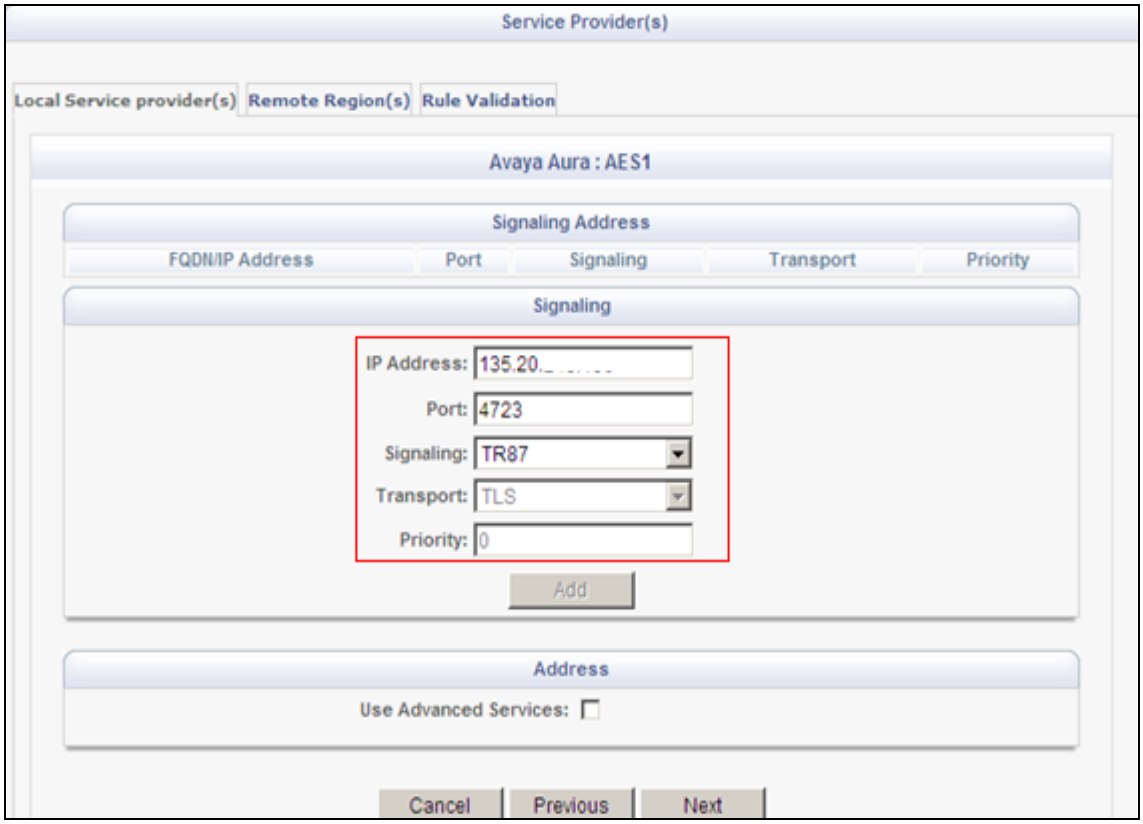


©2011 Avaya Inc. All Rights Reserved.

Type: Avaya Aura
Name: AES

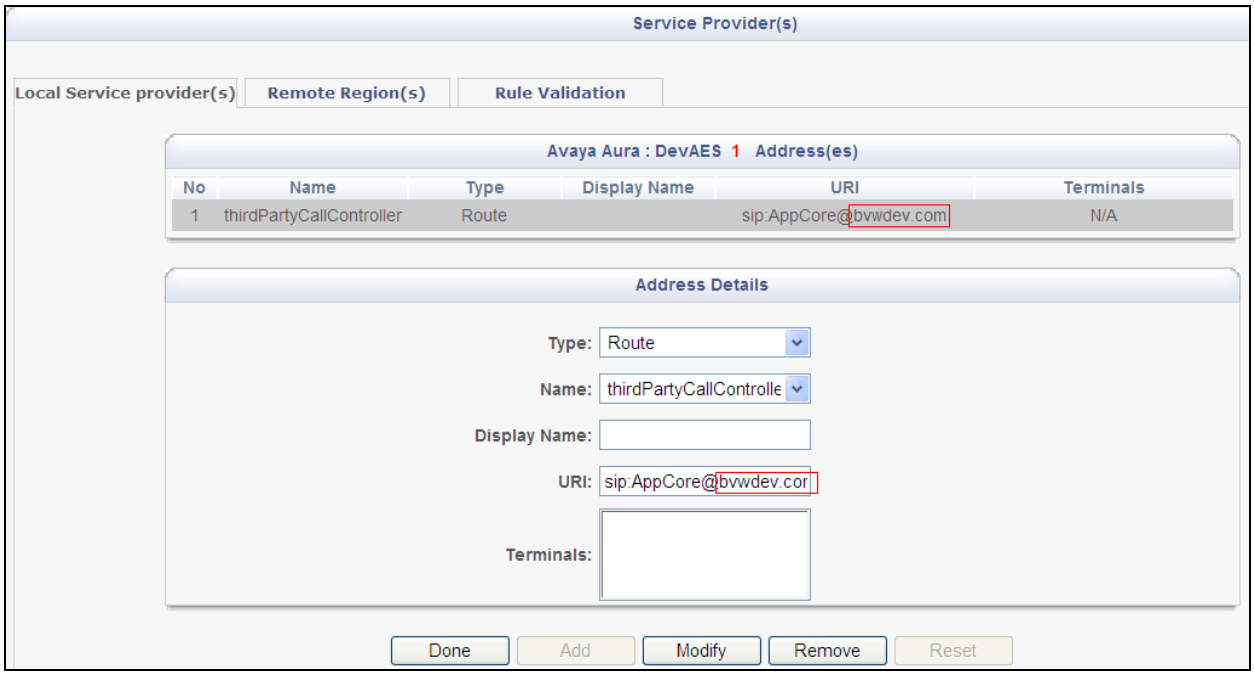


Click **Continue**
IP Address: Enter IP address of AES server, can be provisioned via FQDN
Port: 4723
Signalling: select TR/87. There is a warning when user picks TR/87 as signalling. Click OK
Transport: TLS



©2011 Avaya Inc. All Rights Reserved.

Click **Next** to edit **Address**(es) for Service Provider. By default, the domain for AppCore is avaya.com change it to current domain that is used in the system, see below example:



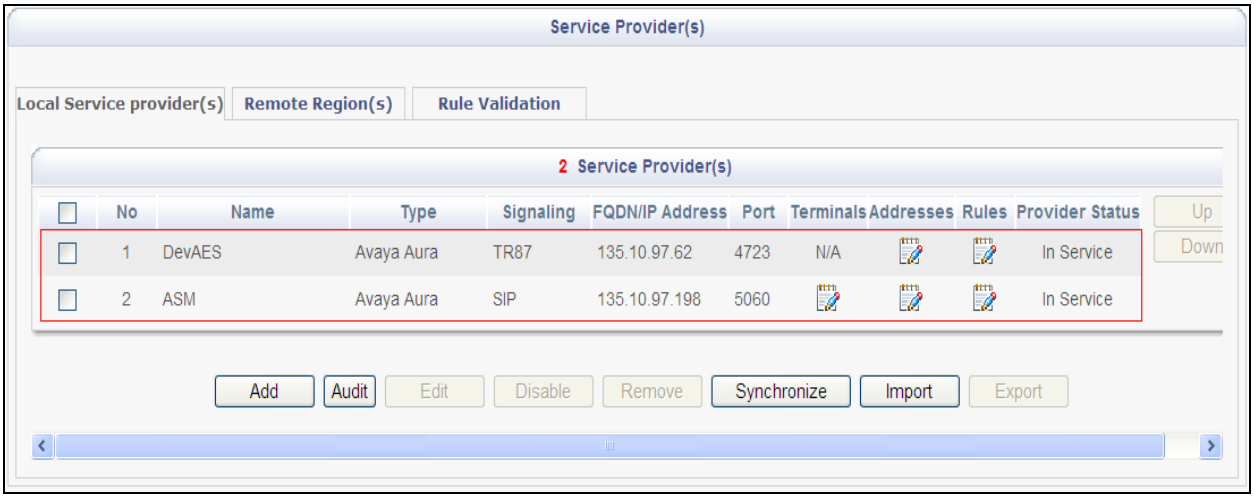
Click **Next** and **Submit** even though there is no rule yet.

9.3.2. Add Session Manager as a service provider in Avaya ACE

- In the **Port field, enter the port used for signaling.**
- In the **Signaling list, select SIP.**
- When you select SIP, the **Transport protocol is set to UDP.**
- If multiple Session Managers are deployed in a geo-redundant configuration, set a **Priority value.**
- If multiple Session Managers are deployed in a geo-redundant configuration, click **Add and then specify the IP address, Port, Signaling and Priority values for each** Session Manager. When all Session Managers have been added, continue to the next step.
- To support Third Party Call Control (v2), select the **Use SIP REFER check box** to generate a ring back tone from the called party to be heard by the calling party when a call is initiated. (Not shown)

©2011 Avaya Inc. All Rights Reserved.

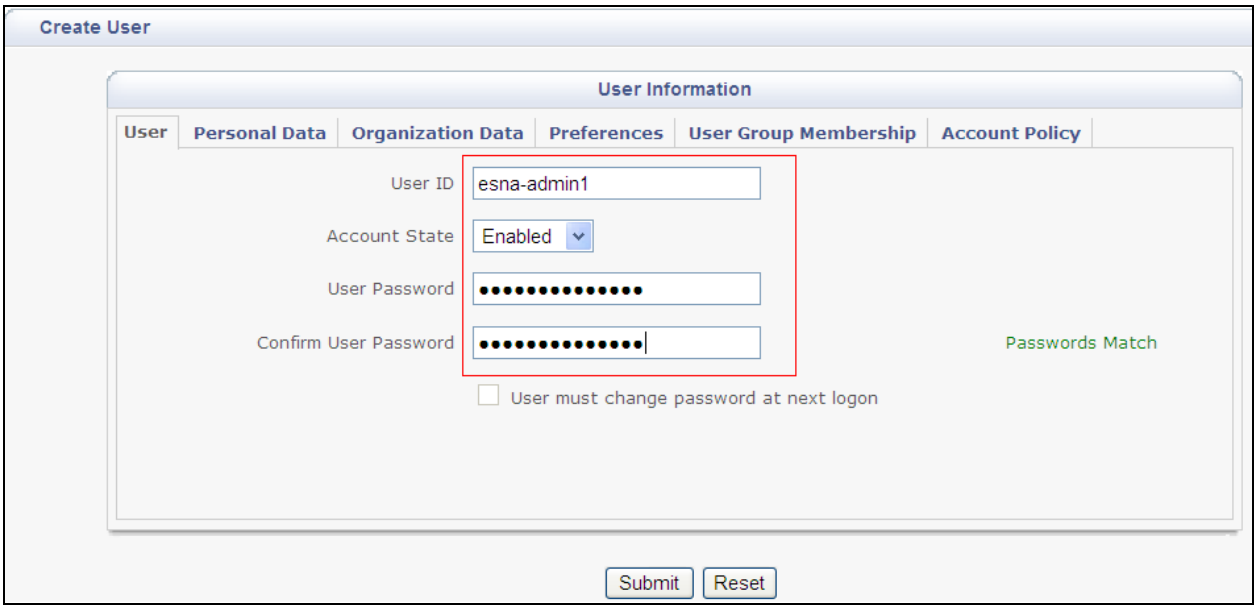
Verify the status of service providers is “In Service”, see below figure:



9.4. Add user

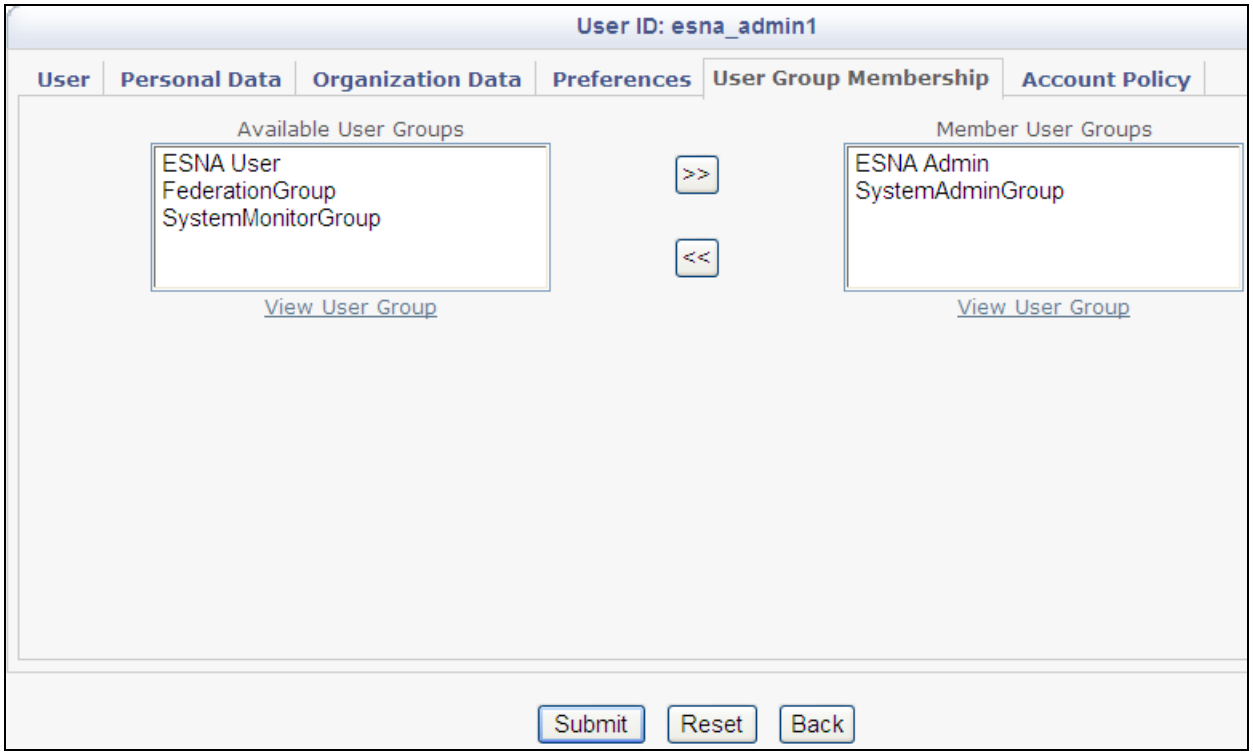
The web service client (application) ESNA Office-LinX – Avaya ACE Wizard is a configured user on Avaya ACE. The web service client (application) belongs to a user group on Avaya ACE with a group type of **user** or higher, and with the appropriate access control rules configured for the Third Party Call Control (v2) service.
This section will setup a user belong to System Admin Group used by ESNA Office-LinX – Avaya ACE Wizard.

Select Security → **User Management** → **Create User**
Enter **User ID**: User used to login ACE web service of the web client (application)
Password: password
Select **Submit** to create user.



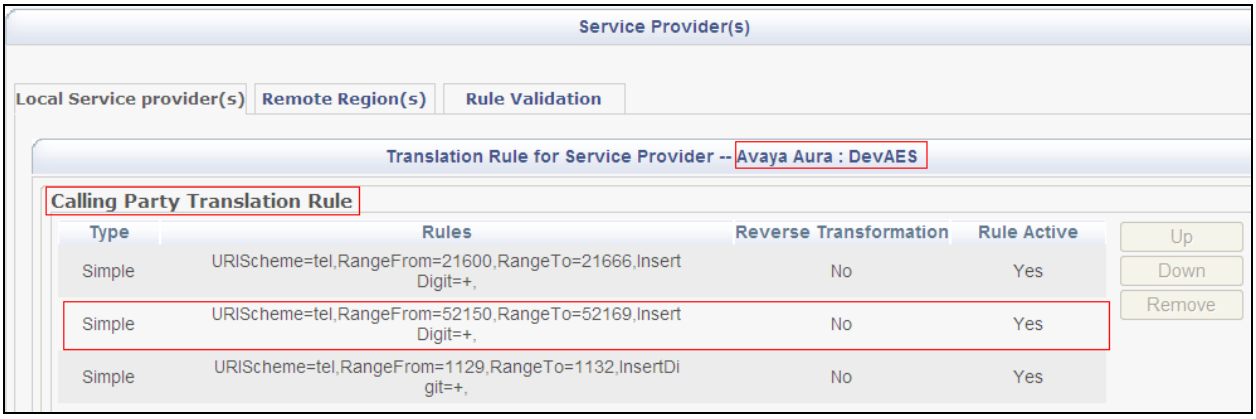
©2011 Avaya Inc. All Rights Reserved.

Assign user esna_admin1 to system Admin group by click on **User Group Membership** tab, select **SystemAdminGroup** in the Left window and click >> to add this group.



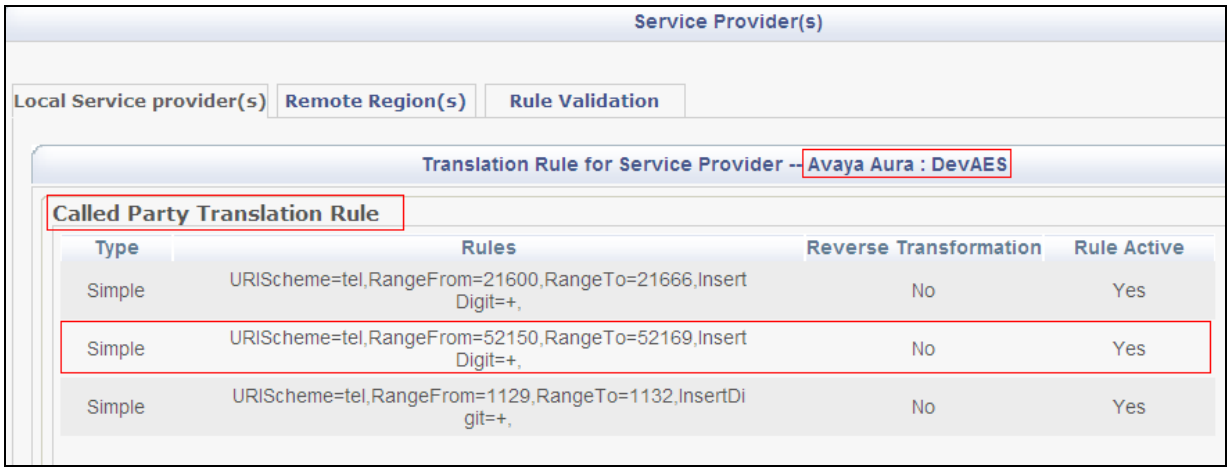
9.5. Add Translation rule to Service Provider

The calling and called translation rules are configured on Avaya ACE to associate the web service call participants with a service provider. The following screens show calling party translation rules of AES (TR/87) service provider.



The following screens show called party translation rules of AES (TR/87) service provider.

©2011 Avaya Inc. All Rights Reserved.



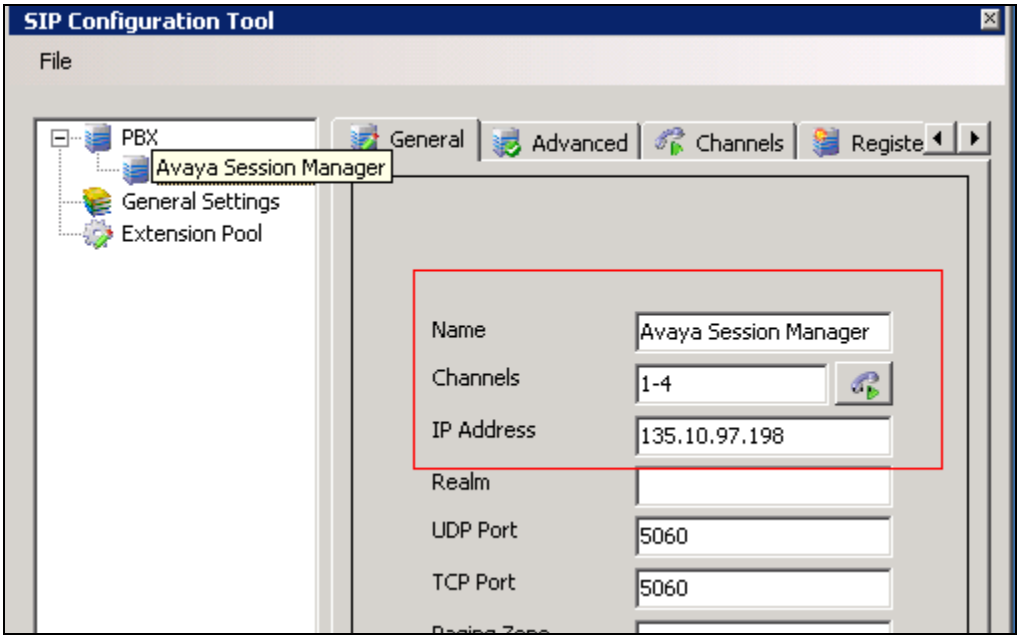
10. Configure the ESNA Telephony Office-LinX

ESNA installs, configures, and customizes the Telephony Office-LinX application for their customers. Thus, this section only describes the interface configuration, so that the Telephony Office-LinX can talk to Avaya Session Manager, Avaya ACE and Avaya Aura Messaging.

10.1. Configure SIP Configuration Tool

To configure ESNA Telephony Office-LinX, navigate to **Start → All Program → Telephony Office LinX Enterprise Edition → SIP Configuration Tool**. Select **Avaya Session Manager** under PBX in the left pane. Provide the following information:

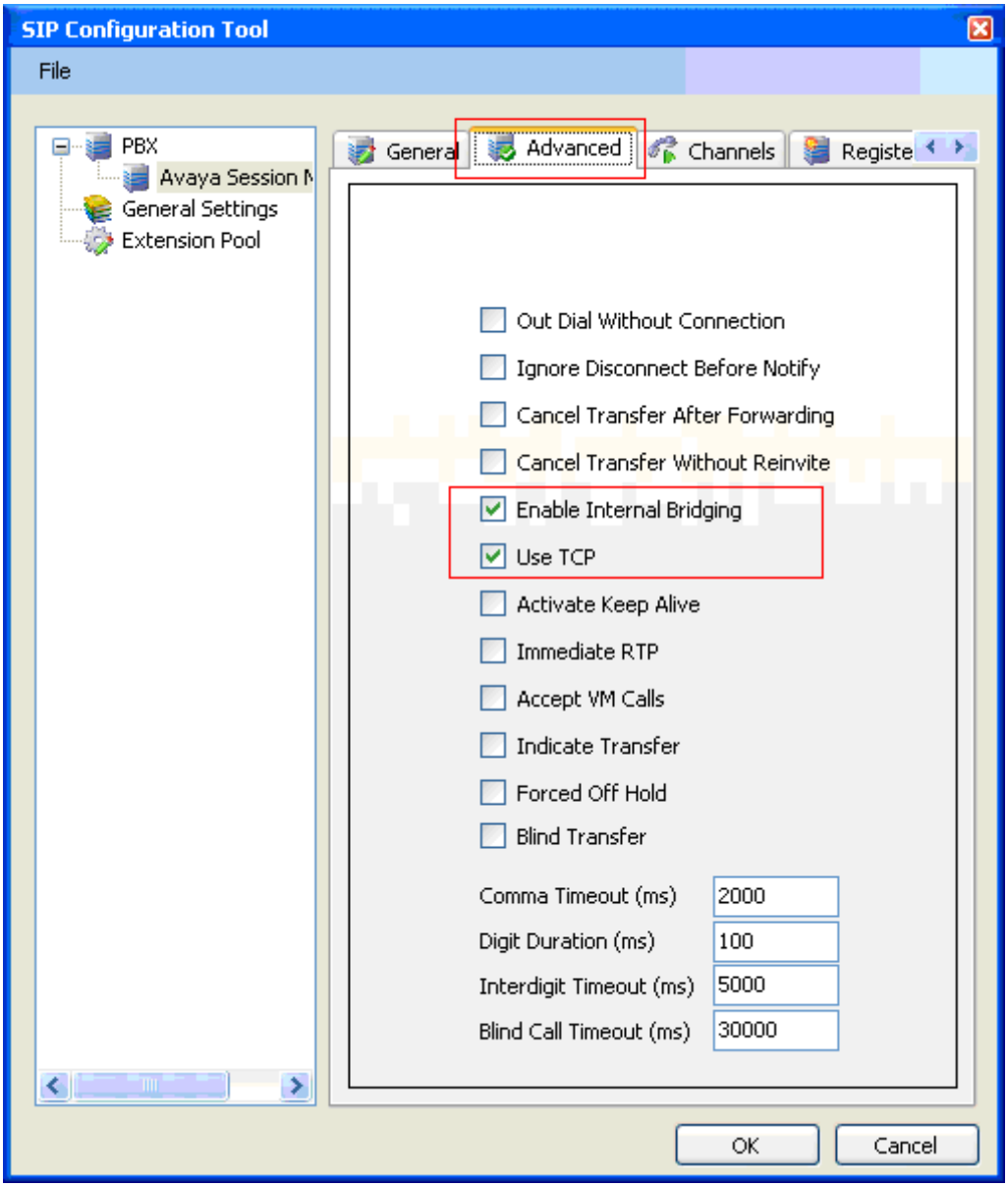
- **IP Address** – Enter **IP address** and **Domain** in the field
- **UDP Port** – Enter **5060**
- **TCP Port** – Enter **5060**



©2011 Avaya Inc. All Rights Reserved.

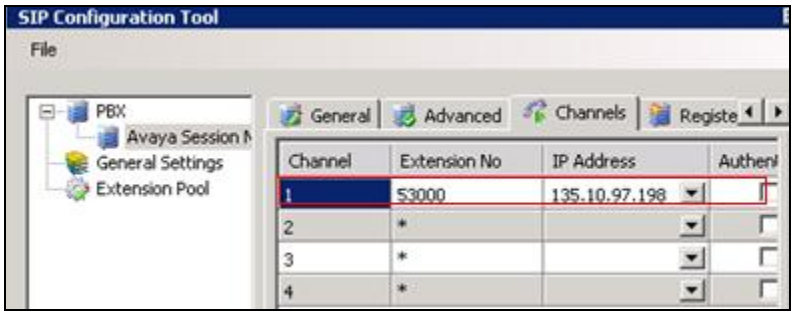
Click the **Advanced** tab in the right pane, and check the following check boxes:

- Enable Internal Bridging
- Use TCP

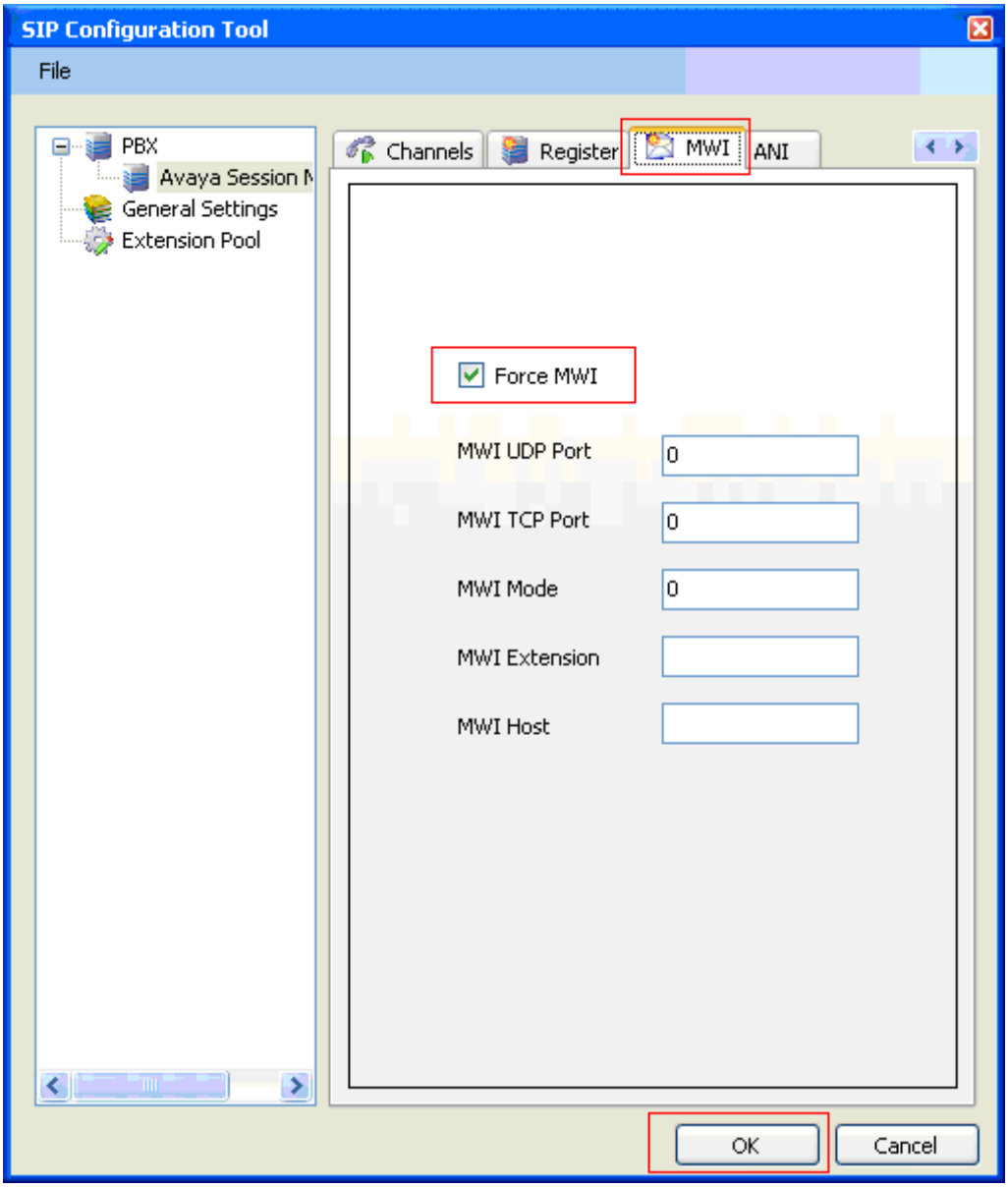


Click the **Channels** tab, and provide the Telephony Office-LinX extension. During the compliance test, extension 53000 was utilized for the Telephony Office-LinX extension.

©2011 Avaya Inc. All Rights Reserved.



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



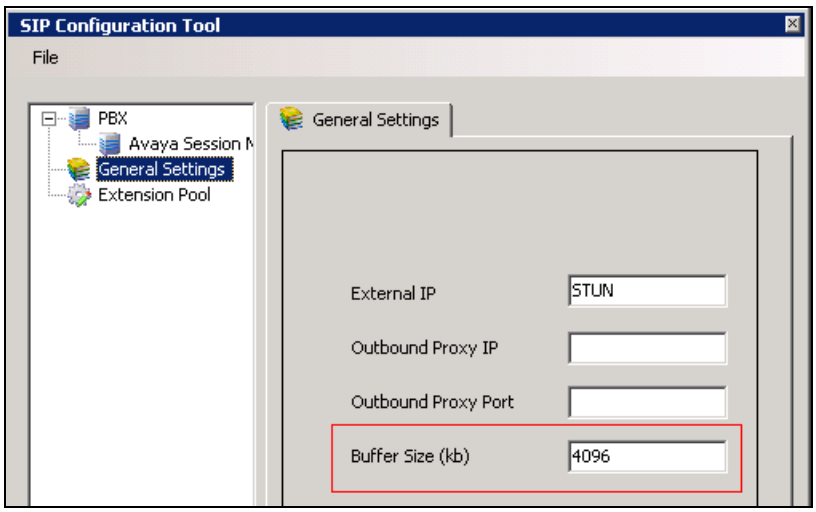
©2011 Avaya Inc. All Rights Reserved.

The following line must be added to the SIP Configuration file (ETSIPService.ini, found under C:\Windows\) manually under the [PBX#] heading:

Subscription State for MWI = 0

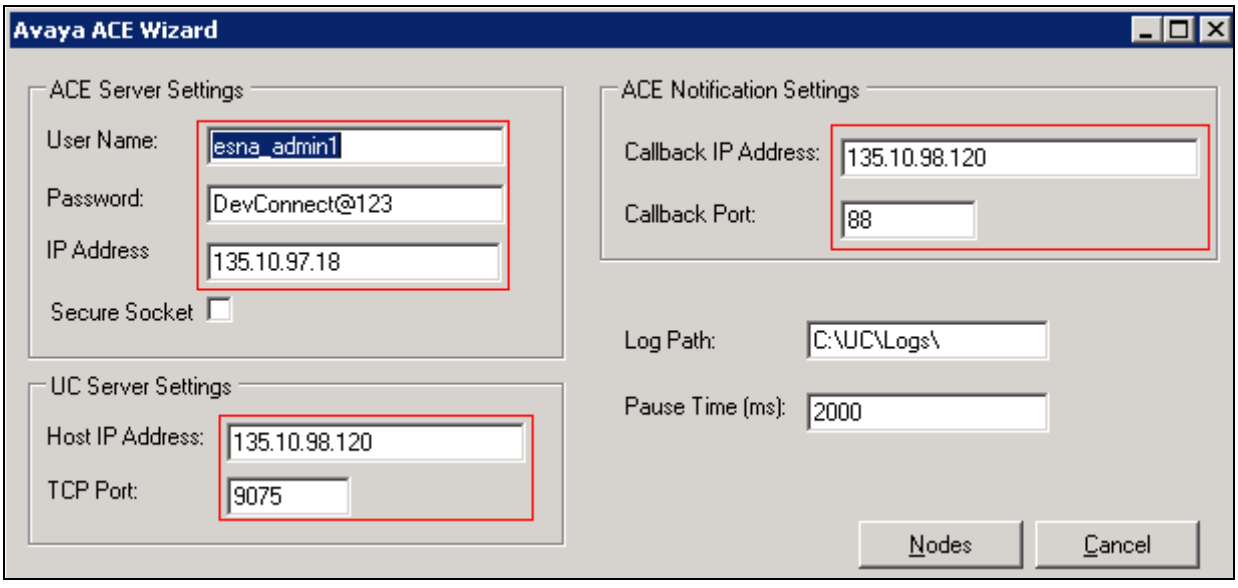
This provides a subscription state line in the message body indicating a subscription state is active; this is required even for unsolicited Notify messages for MWI with Session Manager.

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



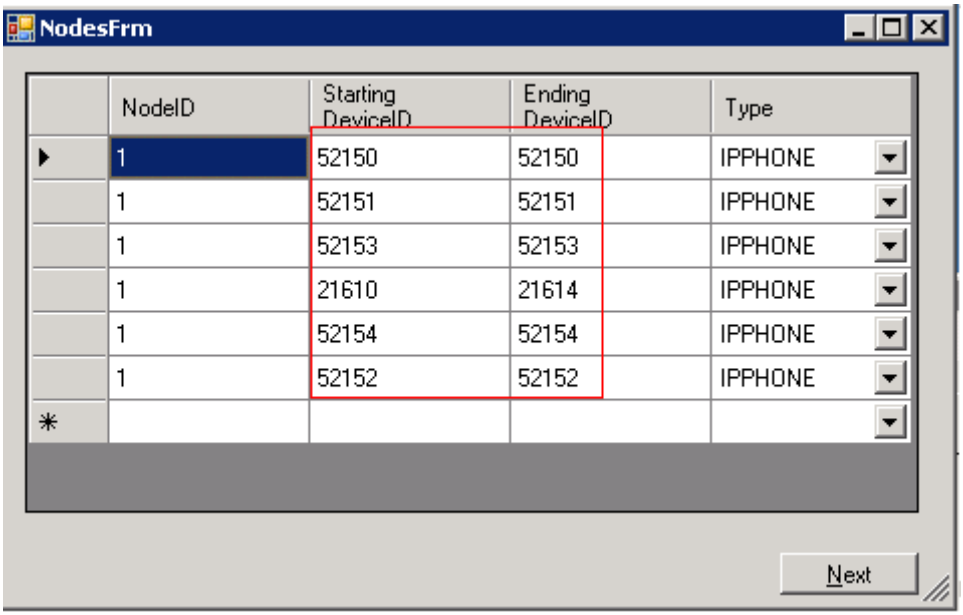
10.2. Configure UC ACE Wizard

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

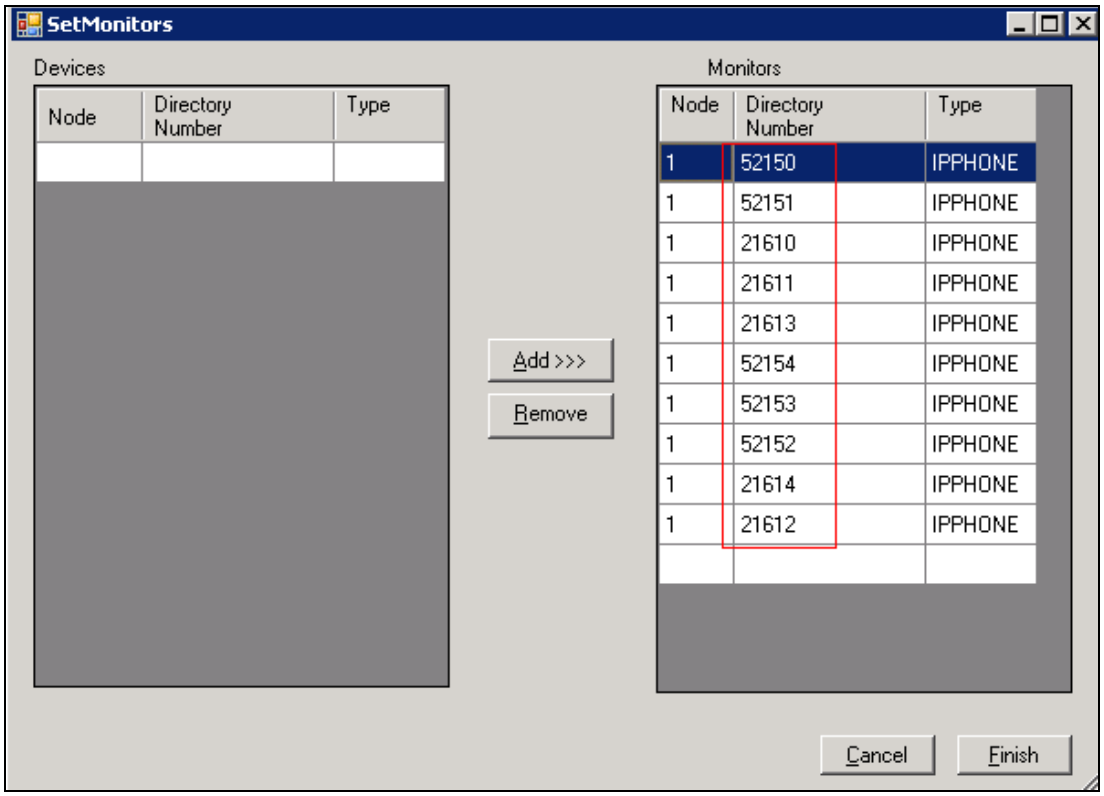


©2011 Avaya Inc. All Rights Reserved.

Click on Nodes to open the next window where user can enter device to get its notification. Click on Next button:



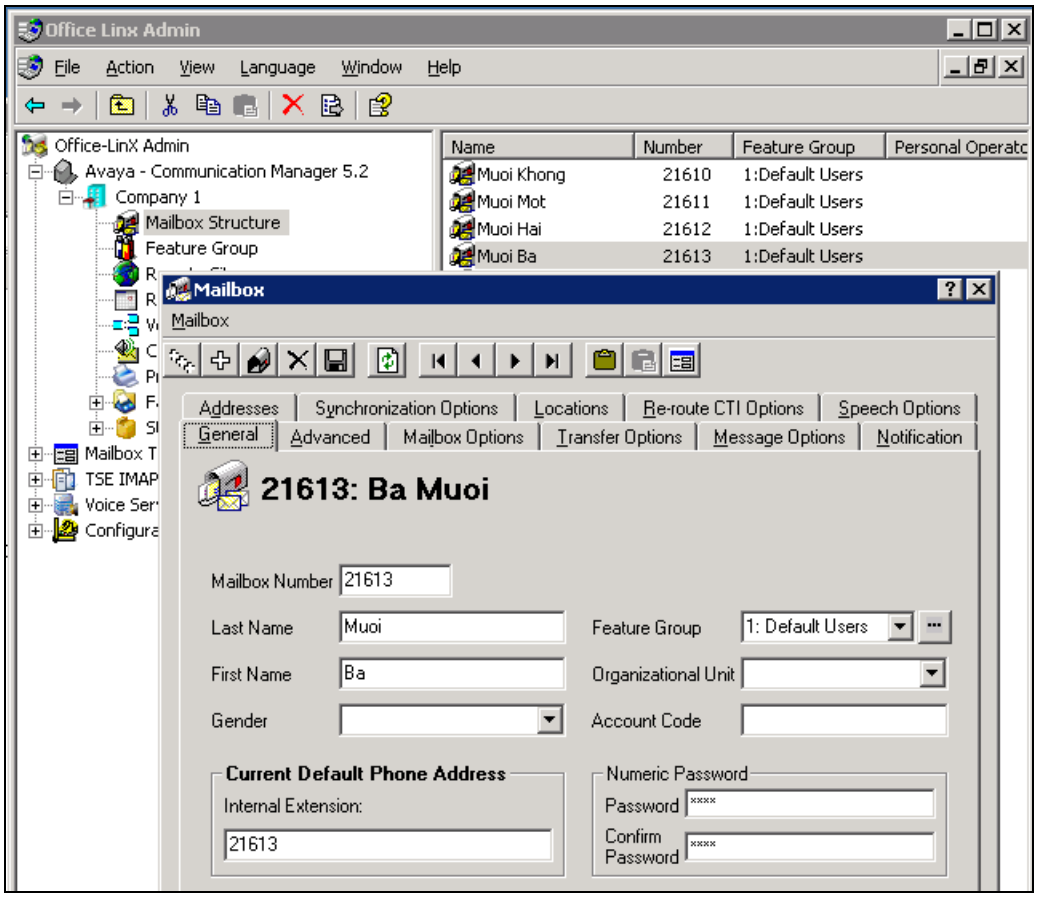
Select the list of device on the leftside and add it to the right window to start to monitor it. Or user can remove devide from monitor list by highlight select device and click remove.



©2011 Avaya Inc. All Rights Reserved.

10.3. Configure user mailbox in Office-LinX Admin

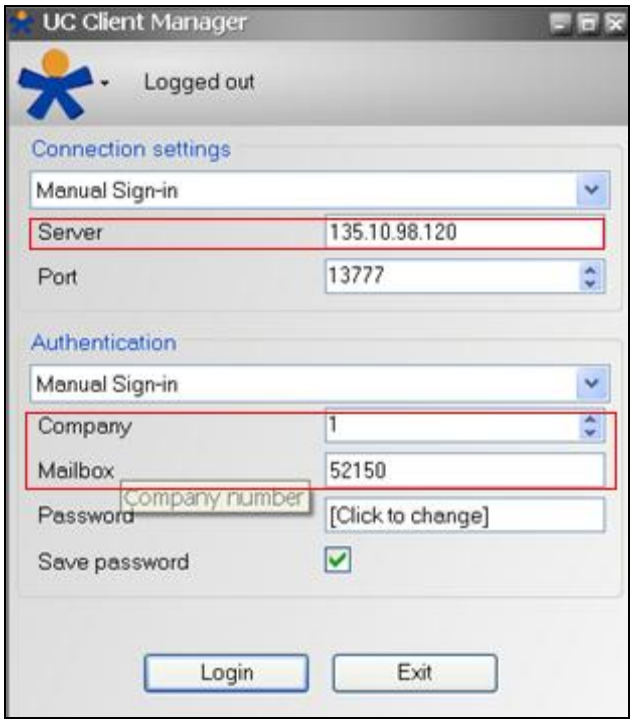
Double click on Office-LinX icon to launch the application window.
Expand the **tree Office-LinX Admin →Avaya – Communication Manager 5.2 → Company 1** and highlight the **Mailbox Structure**. In the right panel right click on the window, select new to add new mailbox (not shown).
Leave all the value as default and modify it if need. Example below is mail box for extension **21613** and default password is 1111.



10.4. Install and Configure UC Client Manager Application

On the client PC, open browser and browse to ESNA Office-LinX Server
Click on the link to download UC Client Application and following the instruction window to install.
Once finish, launch UC Client Manager and login using the mailbox and password created in **Section 10.3** Server is Office-LinX server IP address

©2011 Avaya Inc. All Rights Reserved.



11. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager, Session Manager, Avaya Application Enablement Services, Avaya ACE, Avaya Aura Messaging and ESNA Office-LinX – UC Client Manager application.

11.1. Verify Avaya Aura® Communication Manager

The following steps may be used to verify the configuration:

- From the Communication Manager SAT, use the **status signaling-group** xxx command 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     DevAES           established   15       15
8               no                      down          0        0
```


©2011 Avaya Inc. All Rights Reserved.

See **Section 6.7** to verify the status of a switch connection from Communication Manager to AE Server

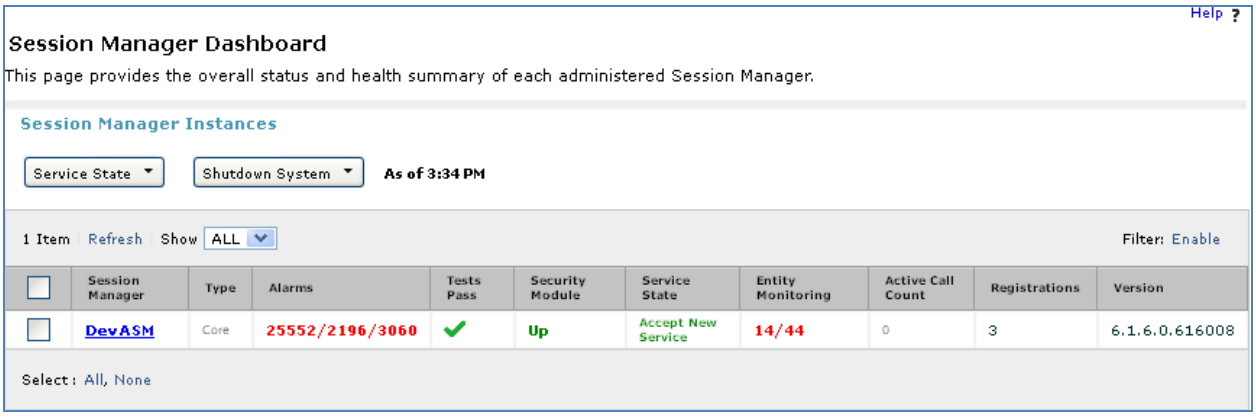
11.2. Verify Avaya Aura® Session Manager

11.2.1. 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


Help ?

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State | Shutdown System | As of 3:34 PM

1 Item | Refresh | Show ALL | Filter: Enable

Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
DevASM	Core	25552/2196/3060	✔	Up	Accept New Service	14/44	0	3	6.1.6.0.616008

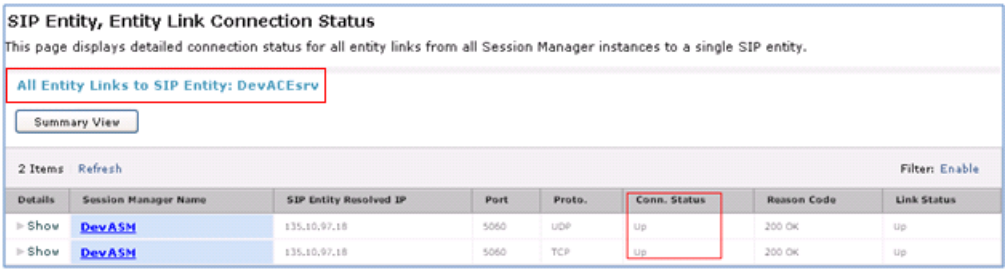
Select : All, None

11.2.2. Verify SIP Entity Link Status

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

Select the SIP Entity for 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.


SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: DevACEsrv

Summary View

2 Items | Refresh | Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	DevASM	135.10.97.18	5060	UDP	Up	200 OK	up
Show	DevASM	135.10.97.18	5060	TCP	Up	200 OK	up

©2011 Avaya Inc. All Rights Reserved.

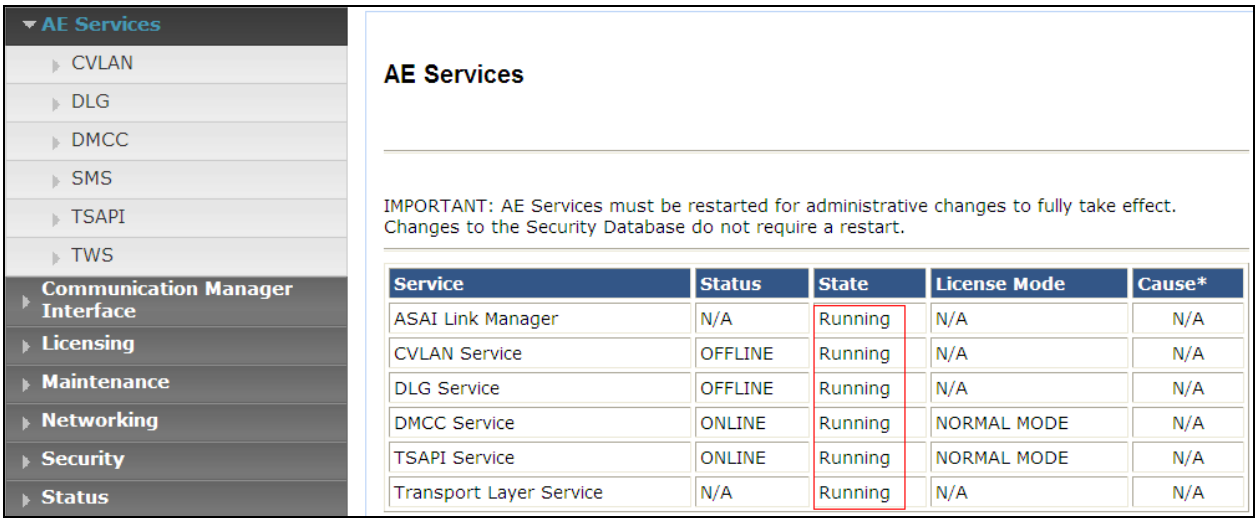
Repeat the same step to verify the status of Avaya Aura Messaging and Avaya Communication Manager are “Up”.

11.3. Verify AE Server

11.3.1. Verify Services are running.

Verify that the AE services are in running state. From the Application Enablement Services System Management console, go to **AE Services.**

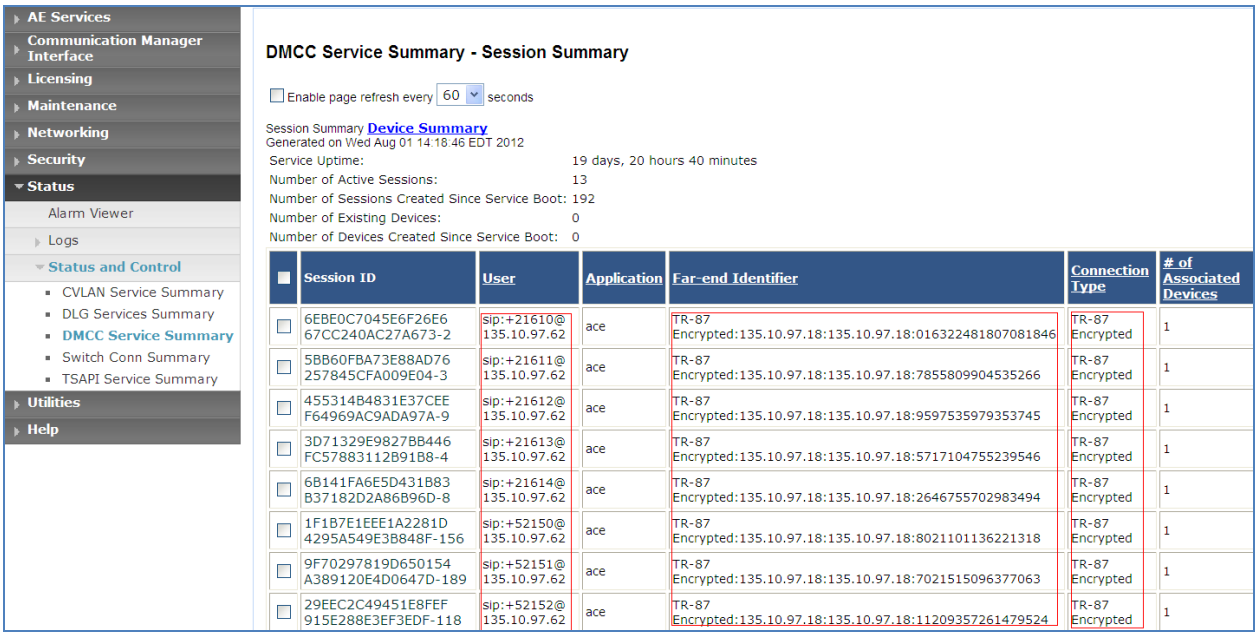
- Verify that the **DMCC Service** has an **ONLINE** status and a **Running** State.



11.3.2. Verify DMCC Service Summary – Session Summary

From the Application Enablement Services System management console, go to **Status → Status and Control → DMCC Service Summary** to view a summary of all active Device, Media, and Call Control (DMCC) sessions and TR/87 sessions.

©2011 Avaya Inc. All Rights Reserved.



11.3.3. Verify AE Server and Avaya ACE are Communicating

To verify that there is an established connection between the AES and ACE, log on to AES ssh console and run the following command: netstat –an|grep 4723

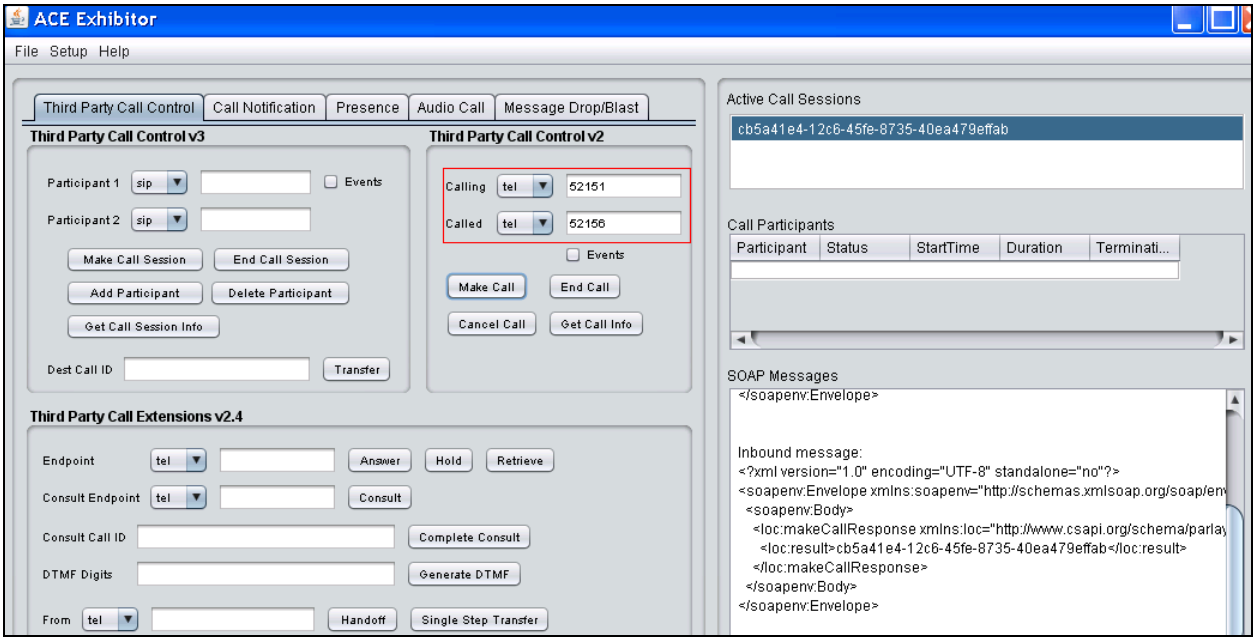
```
-bash-3.2$ netstat -an | grep 4723
tcp        0      0 ::ffff:127.0.0.1:4723       :::*                        LISTEN
tcp        0      0 ::ffff:135.10.97.62:4723    :::*                        LISTEN
tcp        0      0 ::ffff:135.10.xx.xx:4723    ::ffff:135.10.xx.xx:60328   ESTABLISHED
-bash-3.2$
```

The AES is listening on port 4723. There should be an ESTABLISHED link between the AE server and ACE Server.

Verify that the Avaya ACE and AE Server are up and running. To verify that the TLS connection between Avaya ACE and AE Server has been established, check the dmcc-trace.log.0 log file in opt/mvap/logs.

©2011 Avaya Inc. All Rights Reserved.

In AE Server ssh console type the following command: tail –f dmcc-trace.log.0. In a meantime perform call using ACE_EXHIBITOR or SOAP UI software, below is an example of using ACE Exhibitor: make a call from 52151 to 52156:



The AE Server log show call request make from Avaya ACE through TR87 connection:

```
-bash-3.2$ tail -f dmcc-trace.log.0
2012-08-03 00.09.19,264 com.avaya.common.nio.managed.tr87Impl.TR87Connector
processRequest
FINE: [0622204289036496 5@135.10.97.18] - request received on SIP connector: INFO
2012-08-03 00.09.19,265 com.avaya.mvcs.proxy.CstaRouterNode processPacket
FINE: invokeID= 6 Routing request=session[session 1C8FB6F5B6A25AE4EA581BD538E0A085-
204] ch.ecma.csta.binding.MakeCall@15aa8ce
2012-08-03 00.09.19,265 com.avaya.cs.callcontrol.CallControlSnapshotImpl
checkForListener
FINE: [tel:+52151]  has ccs listener in session state Active
2012-08-03 00.09.19,266 com.avaya.mvcs.proxy.CstaRouterNode processPacket
FINE: invokeID= 6 Received com.avaya.platform.broker.impl.AsyncResponse@d03e03 in
response to session[session 1C8FB6F5B6A25AE4EA581BD538E0A085-204]
ch.ecma.csta.binding.MakeCall@15aa8ce
```

11.3.4. Verify AE Server and Switch are talking

See **Section 6.8** Checking the status of a switch connection -- from the AE Server to Communication Manager

©2011 Avaya Inc. All Rights Reserved.

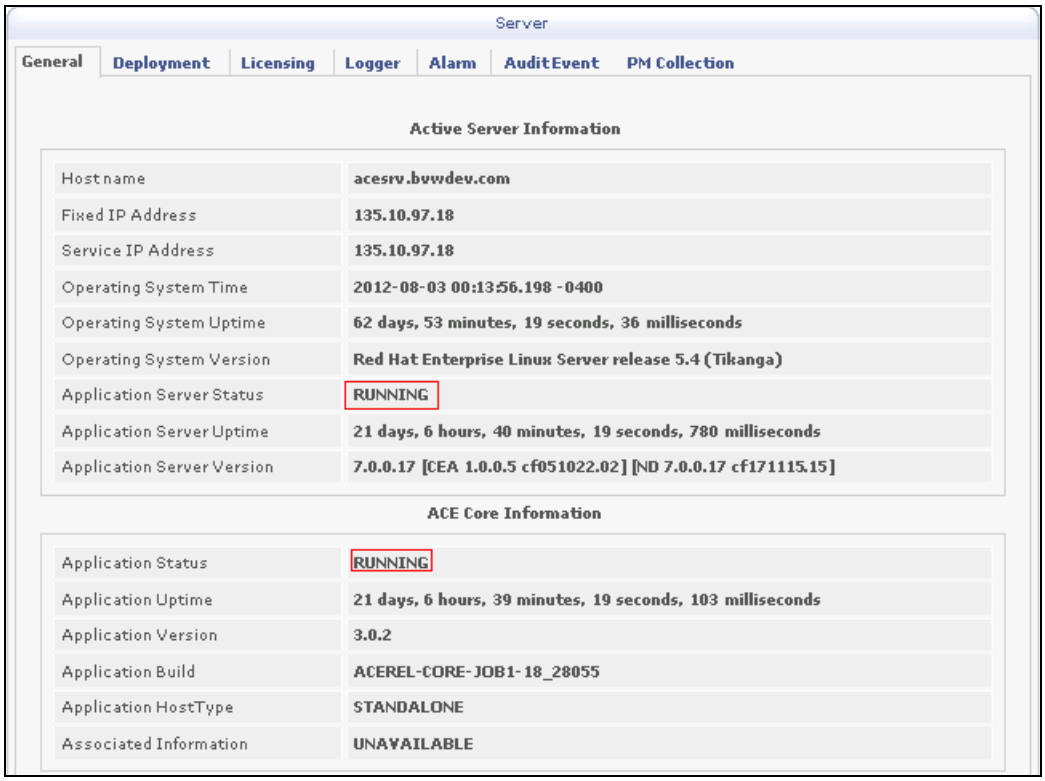
11.4. Verify Avaya ACE

11.4.1. Verify Service Provider status in Avaya ACE

See the end of **Section 9.3** Add service provider in Avaya ACE; to see the figure show that all service providers configured have status "In Service".

11.4.2. Verify Avaya ACE Server status

Select **Configuration → Server** to verify status of server:



11.5. Verify Avaya Aura Messaging

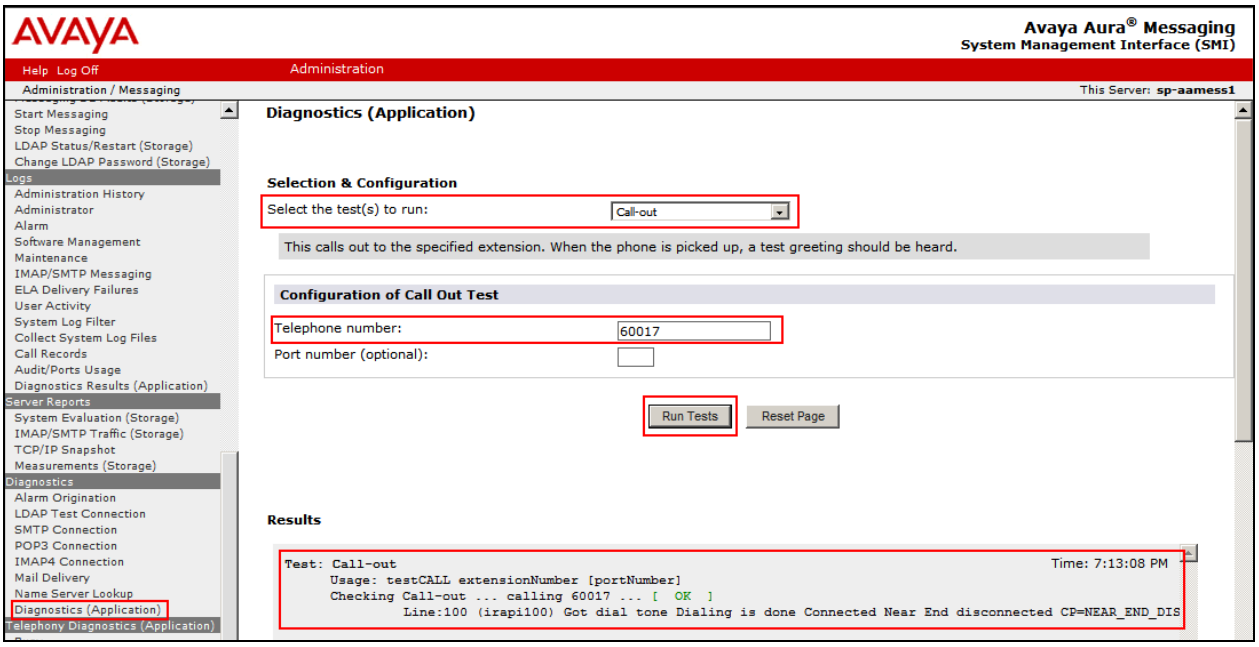
11.5.1. Verify Avaya Aura Messaging can make a call to phones

Test calls can be made from AAM 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.

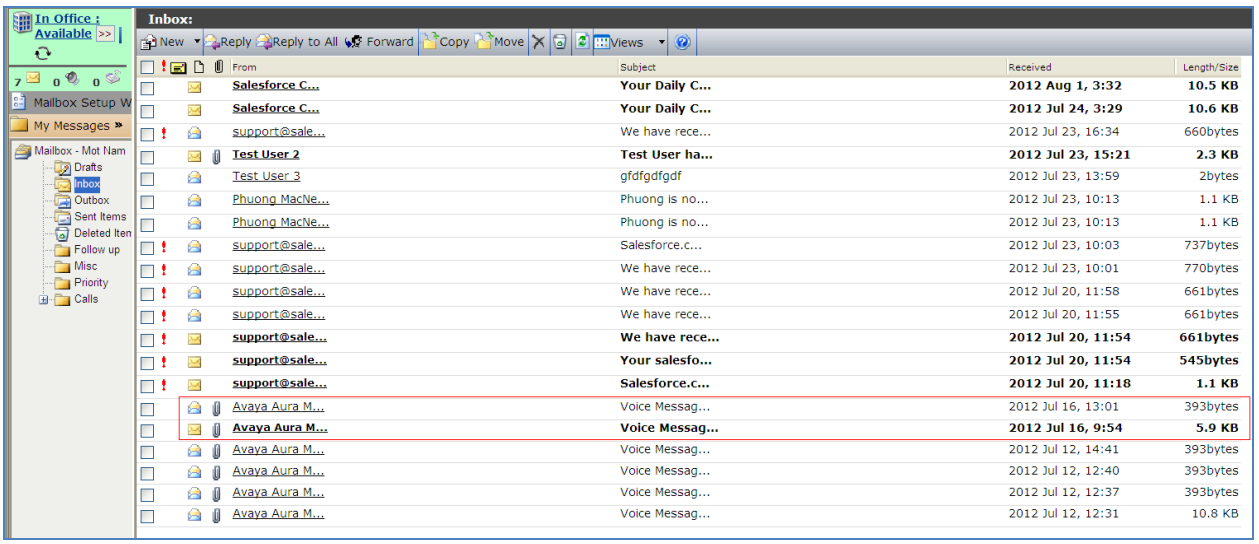
Click on **Run Tests** to start the test. The phone will ring and when answered a test message is played. The **Results** section of the page will update indicating that the call was ok as shown below.

©2011 Avaya Inc. All Rights Reserved.



11.5.2. Verify user can receive and retrieve Avaya Aura Messaging voice message on ESNA Web Client:

Make a call from a UC Client calls 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 Web client verify that user got the message from Avaya Aura Messaging and able to listen to the voice message. Verify that the MWI light turns off. (Notes: At this version of Office-LinX 8.5 SP2, when messages are read, Office-LinX should attempt to extinguish MWI via SIP if possible. This will not reflect actual message status on Avaya Aura Messaging). Example below show user has an incoming Avaya Aura voice message in the mailbox.



©2011 Avaya Inc. All Rights Reserved.

11.6. Verify ESNA Office-LinX server and UC Client Manager.

11.6.1. Verify the log file UCServer of ESNA Office-LinX.

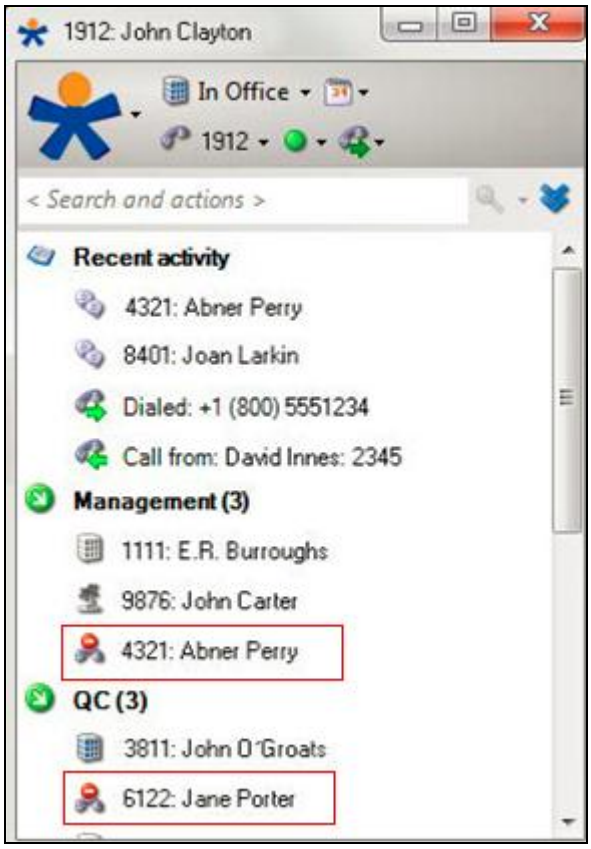
Log on to Office-LinX, open the log file UCServerYYYYMMDD.log in C:\UC\Logs\VServer. Below show detail log of ACE web services that Office-LinX is using such as Call Notification, Third Party Call.

```
11:41:07.390-[+][00000004][F:Init]client: 135.10.98.120Port : 88
11:41:07.671-[+][00000004][F:Init]VirtualAddr: http://135.10.98.120:88/
11:41:07.796-[+][0000000C][F:EventHandler]Start listening
11:41:07.859-[+][0000000C][F:EventHandler]assembly location
C:\WINDOWS\system32\UCACEServer.dll
11:41:07.890-[+][00000004][F:Initialize]Wait for HttpListener to start listening
11:41:08.437-[+][00000004][F:Initialize]Adding Devices to DeviceList
11:41:08.437-[+][00000008][F:Initialize]Exit NoOfDevices: 11
11:41:08.500-[+][00000004][F:Initialize]HttpListener is listening
11:41:10.125-[+][00000004][F:Initialize]Starting EventThread
11:41:10.437-[-][00000003][F:ESACEAgent:EventHandlerproc]Entry:
11:41:10.500-[+][00000004][F:Initialize]Strting Monitor
11:41:15.015-
[+][00000004][F:CallNotification:StartNotification]CallNotification(Called) is started
at http://135.10.98.120:88/ACENotificationServer
11:41:15.140-
[+][00000004][F:CallNotification:StartNotification]CallNotification(Calling)is started
at http://135.10.98.120:88/ACENotificationServer
11:41:15.140-[+][00000004][F:StartMonitor]After starting Call notification :
11:42:25.187-[-][0000000A][F:MakeCall]Entry Dest: 52156
11:42:25.187-[+][0000000A][F:MakeCall]DestBuffer: 52156
11:42:25.218-[+][0000000A][F:CallControl.MakeCall]Calling: tel:52150 Called: tel:52156
11:42:25.234-[+][00000010][F:CallProgressCallBack]Entry Dest:
11:42:25.437-[+][00000004][F:makeCallCompleted]Result: 3b21cc7a-4aee-4b74-b007-
ca5e35f75c2e
11:42:25.437-[+][00000004][F:UpdateCall] >>>>> Key: 521501_3b21cc7a-4aee-4b74-b007-
ca5e35f75c2ewas added
11:42:25.437-[+][00000004][F:PutEvent:makeCallCompleted]Event:
<CMDRESULT><InvokeID>1</InvokeID><Device
EvtDevice="True"><DeviceID>52150</DeviceID><NodeID>1</NodeID><Type>IPPHONE</Type></Dev
ice><Call><ID>3b21cc7a-4aee-4b74-b007-ca5e35f75c2e</ID></Call></CMDRESULT>
11:42:27.484-[+][00000003][F:EventHandlerProc]Recieved call Notification: Correlator:
Calling_ACEServer@135.10.98.120
Event: CalledNumber
Desc:
Calling: tel:52150 Calling Name:
Called: tel:52156 CallID: 3b21cc7a-4aee-4b74-b007-ca5e35f75c2e
```

11.6.2.Verify UC Client Manager – Desktop

Login UC Client Manager using mailbox created in **Section 10.3**. Perform the call to another UC client member. By select member and click on ( ) icon. The devices of calling and called are ringing. Called user picks up the phone and the voice path is established. And the status of member on UC Client change to busy ( ), see below figure:

©2011 Avaya Inc. All Rights Reserved.



12. Conclusion

Interoperability testing of Avaya Agile Communication Environment ™, Avaya Aura® Messaging, and Avaya Aura® Communication Manager 5.2 with Office-LinX 8.5 SP2 – UC Client Manager was successful. Observations are noted in **Section 2.2**.

©2011 Avaya Inc. All Rights Reserved.

13. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, May 2009, Release 5.2, Issue 5.0 Document Numbers 03-300509.
2. *Administering Avaya Aura® Session Manager,* August 2010, Release 6.0, Document Number 03-603324.
3. *Administering Avaya Aura® System Manager*, June 2010, Release 6.0.
4. Avaya Agile Communication Environment Avaya Aura Integration Release 3.0 NN10850 03.03 March 2012

The following document was provided by ESNA.

1. Office-LinX Unified Communication Server Configuration Guide Doc. Version: 8.5 (4) Jun 2012
2. Office-LinX Unified Communication Client Application Guide Doc. Version: 8.5 (5) Jun 2012
3. Google Integration.pdf - Office-LinX Feature Description Guide Chapter 5

©2011 Avaya Inc. All Rights Reserved.

©2012 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.