



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 6.0 - 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.

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. Configure Hunt Group for Avaya Aura Messaging | 15 |
| 5.1.10. Configure Coverage Path to Avaya Aura Messaging | 16 |
| 5.1.11. Administer a Station for Coverage to Avaya Aura Messaging | 17 |
| 5.1.12. Configure Hunt Group for ESNA Office-LinX | 18 |
| 5.1.13. Configure Coverage Path to ESNA Office-LinX | 19 |
| 5.1.14. Configure SIP Endpoint | 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. Administer a network region | 22 |
| 5.2.6. Administer media gateway | 22 |
| 5.2.7. Verify a media processor circuit pack | 23 |
| 6. CONFIGURE AE SERVER | 23 |
| 6.1. Verify Device and Media Call Control API Station licenses | 23 |
| 6.2. Configure Switch Connection: Add switch, edit IP, H323 Gatekeeper | 25 |

| | | |
|-----------|---|-----------|
| 6.3. | Enable TR8/7 Port | 27 |
| 6.4. | Enable TR/87 service setting | 28 |
| 6.5. | Configure dialing plan | 28 |
| 6.6. | Add TSAPI link | 29 |
| 6.7. | Checking the status of a switch connection from Communication Manager to the AE Server | 30 |
| 6.8. | Checking the status of a switch connection -- from the AE Server to Communication Manager | 30 |
| 7. | CONFIGURE AVAYA AURA® MESSAGING | 31 |
| 7.1. | Administer Sites | 31 |
| 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 | 46 |
| 8.8. | Configure Managed Elements | 47 |
| 8.9. | Configure Applications | 49 |
| 8.10. | Define Application Sequence | 50 |

| | | |
|--------------|---|-----------|
| 8.11. | Configure SIP Users | 52 |
| 8.12. | Synchronization Changes with Avaya Aura® Communication Manager | 56 |
| 9. | CONFIGURE AVAYA ACE 3.0 | 56 |
| 9.1. | Administer certificate | 57 |
| 9.1.1. | Creating a directory for the OpenSSL CA files | 57 |
| 9.1.2. | Creating an OpenSSL configuration file | 58 |
| 9.1.3. | Generating a CA certificate | 58 |
| 9.1.4. | Create a server certificate request for AE Services | 59 |
| 9.1.5. | Creating the ACE certificate request | 60 |
| 9.1.6. | Signing an AES certificate request | 61 |
| 9.1.7. | Signing an ACE certificate request | 61 |
| 9.1.8. | Importing the server certificate into AE Services | 62 |
| 9.1.9. | Add Trusted Host | 64 |
| 9.2. | Certificate management using the IBM Integrated Solutions Console for ACE on Linux | 65 |
| 9.2.1. | Creating a key store using the IBM Integrated Solutions Console | 66 |
| 9.2.2. | Export ACE server cert | 68 |
| 9.2.3. | Administer Keystore | 68 |
| 9.2.4. | Restart Avaya ACE and AE server | 71 |
| 9.3. | Add Service Provider | 72 |
| 9.3.1. | Add AE server provider using TR87 service | 72 |
| 9.3.2. | Add Session Manager as a service provider in Avaya ACE | 74 |
| 9.4. | Add user | 75 |
| 9.5. | Add Translation rule to Service Provider | 77 |
| 10. | CONFIGURE THE ESNA TELEPHONY OFFICE-LINX | 77 |
| 10.1. | Configure SIP Configuration Tool | 77 |
| 10.2. | Configure UC ACE Wizard | 81 |
| 10.3. | Configure user mailbox in Office-LinX Admin | 82 |
| 10.4. | Install and Configure UC Client Manager Application | 83 |
| 11. | VERIFICATION STEPS | 84 |
| 11.1. | Verify Avaya Aura® Communication Manager | 84 |
| 11.2. | Verify Avaya Aura® Session Manager | 85 |
| 11.2.1. | Verify Avaya Aura® Session Manager is Operational | 85 |
| 11.2.2. | Verify SIP Entity Link Status | 85 |
| 11.3. | Verify AE Server | 86 |
| 11.3.1. | Verify Services are running. | 86 |

| | | |
|--------------|---|-----------|
| 11.3.2. | Verify DMCC Service Summary – Session Summary | 86 |
| 11.3.3. | Verify AE Server and Avaya ACE are Communicating | 87 |
| 11.3.4. | Verify AE Server and Switch are talking | 88 |
| 11.4. | Verify Avaya ACE | 89 |
| 11.4.1. | Verify Service Provider status in Avaya ACE | 89 |
| 11.4.2. | Verify Avaya ACE Server status | 89 |
| 11.5. | Verify Avaya Aura Messaging | 89 |
| 11.5.1. | Verify Avaya Aura Messaging can make a call to phones | 89 |
| 11.5.2. | Verify user can receive and retrieve Avaya Aura Messaging voice message on ESNA Web Client: | 90 |
| 11.6. | Verify ESNA Office-LinX server and UC Client Manager. | 91 |
| 11.6.1. | Verify the log file UCServer of ESNA Office-LinX. | 91 |
| 11.6.2. | Verify UC Client Manager – Desktop | 91 |
| 12. | CONCLUSION | 92 |
| 13. | ADDITIONAL REFERENCES | 93 |

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.

Esna Office-LinX 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 relay).
- Redirect call.
- 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. This is intermittent and being investigated by Avaya ACE team.
- 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

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 SIP IP Telephones, H.323 IP Telephones, and an Avaya Digital Telephone.

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.

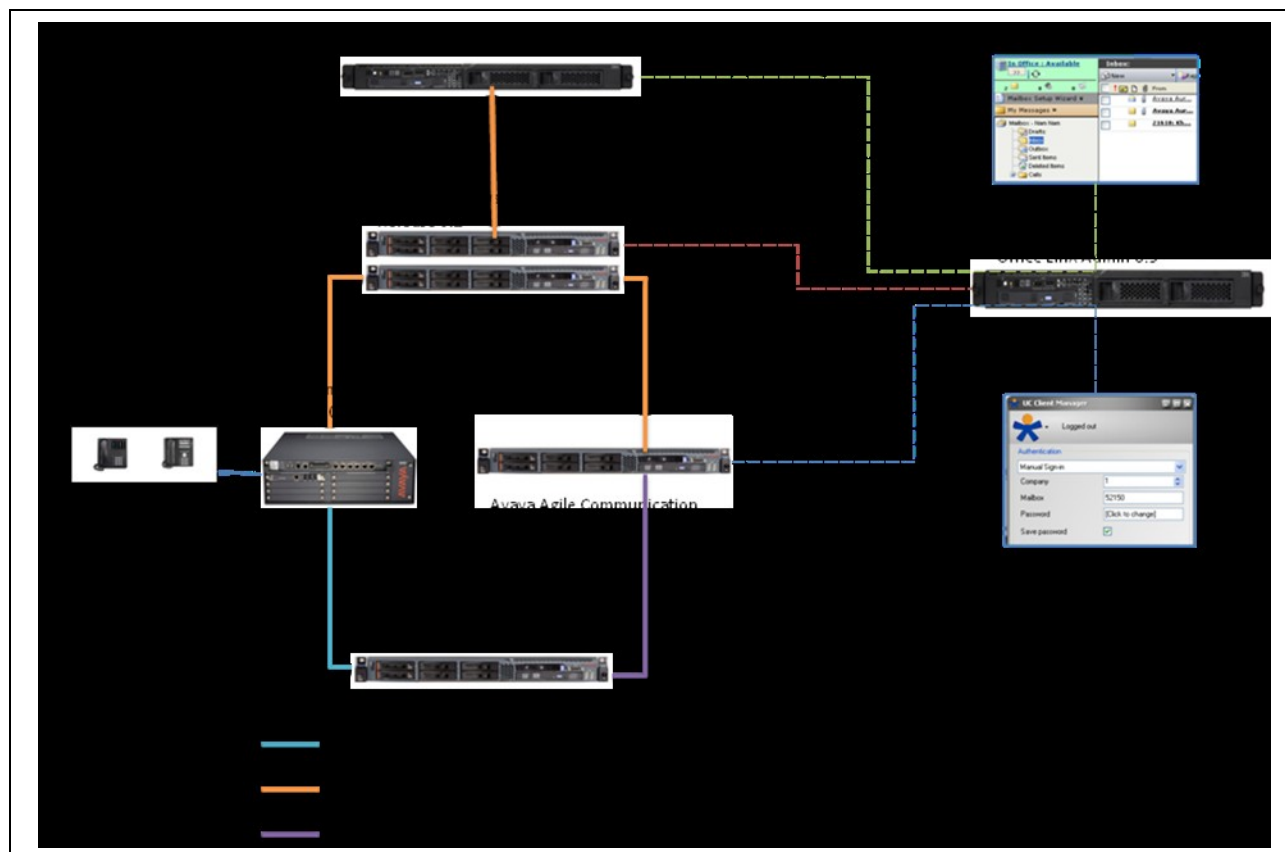


Figure 1: Test Configuration

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 6.0 (R016x.00.0.345.0) with Patch 00.0345.0-18246 |
| 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™ | Avaya ACE 3.0.2 |
| Avaya 9621G SIP Phone | 6.0 |
| Avaya 9611G H323 Phone | 6.0 |
| Avaya 1416 Digital Telephone | - |
| 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.

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

number between **1** and **7**, inclusive. IP codec sets are used in **Section 5.1.3** for configuring IP network region to specify which codec sets may be used within and between network regions.

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

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

IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size(ms)
1: G.711MU      n           2          20
2: G.711A      n           2          20
3:
4:
5:
6:
7:
```

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
H.323 IP ENDPOINTS                                     AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y                           RSVP Enabled? n
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

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

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 Night Service:
Dial Access? n 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
```

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 | | |
| | | | | | | | | | | | | | | | 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.
- 521 – 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 | String | Length | Type | |
| 1 | 3 | dac | 8 | 1 | fac | | | | | | |
| 5300 | 5 | ext | 9 | 1 | fac | | | | | | |
| 399 | 5 | ext | * | 4 | dac | | | | | | |
| 521 | 5 | ext | | | | | | | | | |

Use the command **change uniform dial-plan 1** to create an entry in the UDP table which covers extensions to 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 Pattern | Len | Del | Insert Digits | Net | Conv | Node Num |
| 399 | 5 | 0 | | aar | n | |
| 5300 | 5 | 0 | | aar | n | |
| 52 | 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 String | Total Min | Total Max | Route Pattern | Call Type | Node Num | ANI Regd |
| 399 | 5 | 5 | 5 | unku | | n |
| 5300 | 5 | 5 | 5 | unku | | n |
| 52 | 5 | 5 | 5 | aar | | n |

5.1.9. Configure Hunt Group for Avaya Aura Messaging

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

- **Group Name** – Enter a descriptive name
- **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 | |

5.1.10. 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 |
| All? | n | | n |
| DND/SAC/Goto Cover? | y | | y |
| Holiday Coverage? | n | | n |
| Number of Rings: 2 | | | |
| COVERAGE POINTS | | | |
| Terminate to Coverage Pts. with Bridged Appearances? n | | | |
| Point1: h2 | Rng: 2 | Point2: | |
| Point3: | | Point4: | |

5.1.11.Administer a Station for Coverage to Avaya Aura Messaging

Configure any and all phones that have a mailbox on the messaging server for call coverage. Use the command **change station xyz** and on **Page1 for Coverage Path 1** use the coverage path defined in **Section 5.1.10** in the example below station 52150 was configured to cover to messaging using cover path 2.

| | | |
|---------------------------|--|--------|
| change station 52151 | Page 1 of 5 | |
| STATION | | |
| Extension: 52151 | Lock Messages? n | BCC: 0 |
| Type: 9650 | 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 | | |
| Loss Group: 19 | Time of Day Lock Table: | |
| | Personalized Ringing Pattern: 1 | |
| | Message Lamp Ext: 52151 | |
| Speakerphone: 2-way | Mute Button Enabled? y | |
| Display Language: english | Button Modules: 0 | |
| Survivable GK Node Name: | | |
| Survivable COR: internal | Media Complex Ext: | |
| Survivable Trunk Dest? y | IP SoftPhone? y | |
| | IP Video Softphone? n | |
| | Short/Prefixed Registration Allowed: default | |
| | Customizable Labels? y | |

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

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

5.1.12. Configure 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.

| 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 |

5.1.13. 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 |
| All? | n | | n |
| DND/SAC/Goto Cover? | y | | y |
| Holiday Coverage? | n | | n |
| Number of Rings: 2 | | | |
| COVERAGE POINTS | | | |
| Terminate to Coverage Pts. with Bridged Appearances? n | | | |
| Point1: h1 | Rng: 2 | Point2: | |
| Point3: | | Point4: | |

5.1.14. Configure SIP Endpoint

SIP endpoints and off-pbx-telephone stations will be automatically created in Communication manager when users (SIP endpoints) were created in Session Manager. Go to **Section 8.11** for step on how to create SIP user on Session Manager. On the station form in CM, on the last page is a Third Party Call Control setting. Set value for **Type of 3PCC Enabled: Avaya**. This setup makes sure that ACE Notification service can send out the notification for SIP Phone.

| | | | |
|-----------------------------|--|-------------|--|
| change station 52152 | | Page 6 of 6 | |
| STATION | | | |
| SIP FEATURE OPTIONS | | | |
| Type of 3PCC Enabled: Avaya | | | |
| SIP Trunk: aar | | | |

5.2. 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

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          Digital Loss Plan Modification? y
Async. Transfer Mode (ATM) Trunking? n     DS1 MSP? y
ATM WAN Spare Processor? n                 DS1 Echo Cancellation? y
ATMS? 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
Private Networking? y                     Uniform Dialing Plan? y
Processor and System MSP? y               Usage Allocation Enhancements? y
Processor Ethernet? y                     Wideband Switching? y
Remote Office? y                           Wireless? n
Restrict Call Forward Off Net? y
Secondary Data Module? y

(NOTE: You must logoff & login to effect the permission changes.)
```

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**. IP Address is Avaya Communication Manager IP Address.

| add ip-interface procr | | Page 1 of 2 |
|------------------------|--------------------------|-------------|
| IP INTERFACES | | |
| Type: PROCR | Target socket load: 4800 | |
| Enable Interface? y | Allow H.323 Endpoints? y | |
| Network Region: 1 | Allow H.248 Gateways? y | |
| | Gatekeeper Priority: 5 | |
| IPV4 PARAMETERS | | |
| Node Name: procr | IP Address: 10.33.4.x | |
| Subnet Mask: /24 | | |

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:

- In the **Service Type** field, type AESVCS.
- 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 Type | Enabled | Local Node |
| 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 Server | Enabled |
| 1: | DevAES | y |
| | | in use |

Note:

- 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.

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: 52100 | | | |
| Type: ADJ-IP | | | |
| Name: DevEAS | | COR: | |

5.2.5. Administer a network region

See **Section 5.1.3**. The same network region will be used.

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 | | Page 1 of 2 | |
| MEDIA GATEWAY 1 | | | |
| Type: g450 | | | |
| Name: DevCM3G450 | | | |
| Serial No: 12N503843299 | | | |
| Encrypt Link? y | | | |
| Network Region: 1 | | Location: 1 | |
| | | Site Data: | |
| Recovery Rule: none | | | |
| Registered? y | | | |
| FW Version/HW Vintage: 31 .22 .0 /1 | | | |
| MGP IPV4 Address: 10.33.4.y | | | |
| MGP IPV6 Address: | | | |
| Controller IP Address: 10.33.4.x | | | |
| MAC Address: cc:f9:54:27:95:d0 | | | |

Note:

If you are using a media gateway, and your application needs media encryption, you must set **Encrypt Link?** to y. If you do not enable this setting, your application will not get a talkpath.

5.2.7. Verify a media processor circuit pack

If you are using a media server that uses a media processor (MEDPRO) circuit pack, you must add the media processor circuit pack to the Communication Manager network.

| 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 | 10.33.4.x | |
| procr6 | :: | |

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:

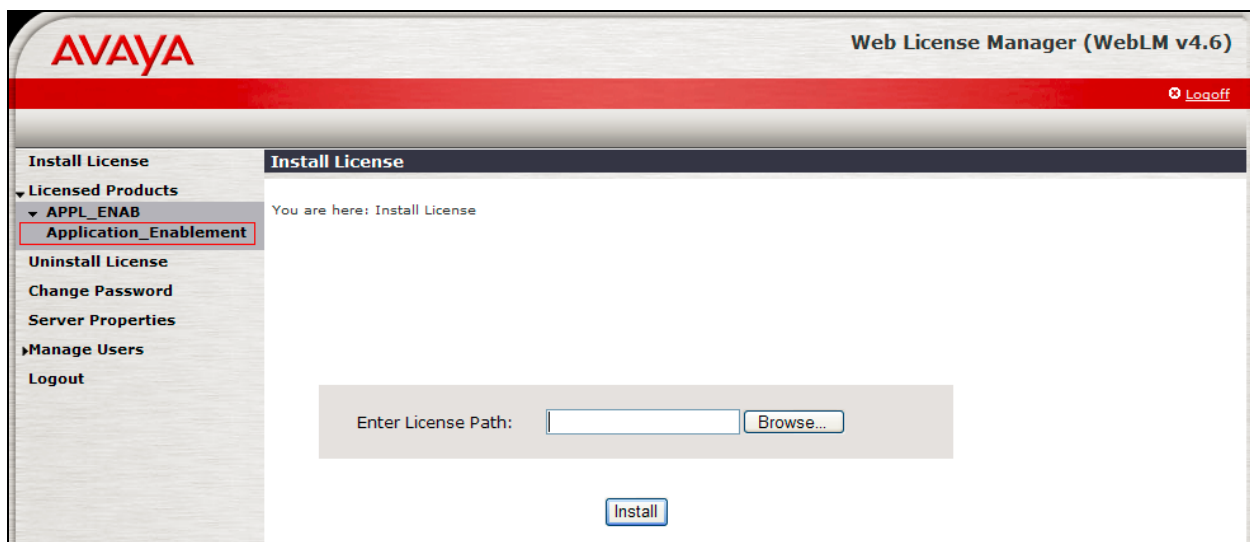
- Verify license
- Configure Switch Connection: Add switch, edit IP, H323 Gatekeeper
- Configure TR8/7 Port
- Configure service setting TR/87
- Configure dialing plan
- Add switch Connection on OAM.
- Configure CM following chapter 2 of Services Administration and Maintenance documentation.
- Add dial plan on OAM for switch added in step 1.
- 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

| Feature (Keyword) | Expiration Date | Licensed | Acquired |
|---|-----------------|--|-------------|
| CVLAN ASAI (VALUE_AES_CVLAN_ASAI) | permanent | 16 | 0 |
| Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP) | permanent | 1000 | 0 |
| AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED) | permanent | 3 | 0 |
| CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS) | permanent | 16 | 0 |
| Product Notes (VALUE_NOTES) | permanent | SmallServerTypes: s8300c;s8300d;jcc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;del1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_AEC_UNIFIED_CC_DESKTOP;; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; | Not counted |
| AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED) | permanent | 3 | 0 |
| TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS) | permanent | 1000 | 0 |
| DLG (VALUE_AES_DLG) | permanent | 16 | 1 |
| Device Media and Call Control (VALUE_AES_DMCC_DMC) | permanent | 1000 | 8 |
| AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED) | permanent | 3 | 0 |

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**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" with login details. A red navigation bar contains "Communication Manager Interface | Switch Connections" and links for "Home | Help | Logout". A left sidebar lists navigation options: AE Services, Communication Manager Interface (selected), Switch Connections (highlighted), Dial Plan, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area, titled "Switch Connections", features a text input field containing "S8300D" and an "Add Connection" button. Below this is a table with the following data:

| Connection Name | Processor Ethernet | Msg Period | Number of Active Connections |
|-----------------|--------------------|------------|------------------------------|
| G650 | No | 30 | 0 |

At the bottom of the table are five buttons: "Edit Connection", "Edit PE/CLAN IPs", "Edit H.323 Gatekeeper", "Delete Connection", and "Survivability Hierarchy".

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**.

Application Enablement Services
Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Communication Manager Interface | Switch Connections
Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Connection Details - S8300D

Switch Password
Confirm Switch Password

Msg Period
30
Minutes (1 - 72)

SSL
☒

Processor Ethernet
☒

Apply
Cancel

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.

Application Enablement Services
Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Communication Manager Interface | Switch Connections
Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Switch Connections


Add Connection

| Connection Name | Processor Ethernet | Msg Period | Number of Active Connections |
|---|--------------------|------------|------------------------------|
| <input type="radio"/> G650 | No | 30 | 0 |
| <input checked="" type="radio"/> S8300D | Yes | 30 | 1 |

Edit Connection
Edit PE/CLAN IPs
Edit H.323 Gatekeeper
Delete Connection
Survivability Hierarchy

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.



Application Enablement Services
Management Console

Welcome: User craft
 Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10
 HostName/IP: aes.avaya.com/10.64.43.40
 Server Offer Type: VIRTUAL_APPLIANCE
 SW Version: r6-1-1-30-0

Communication Manager Interface | Switch Connections
 Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 Licensing
 Maintenance
 Networking
 Security
 Status
 User Management
 Utilities
 Help

Edit H.323 Gatekeeper - S8300D
 Name or IP Address

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.

Networking
 AE Service IP (Local IP)
 Network Configure
 Ports
 TCP Settings
 Security
 Status
 User Management
 Utilities
 Help

| | | |
|-------------------------|-----------------------------------|--|
| Encrypted TCP Port | <input type="text" value="9998"/> | <input checked="" type="radio"/> <input type="radio"/> |
| DLG Port | TCP Port | 5678 |
| TSAPI Ports | | Enabled Disabled |
| TSAPI Service Port | 450 | <input checked="" type="radio"/> <input type="radio"/> |
| Local TLINK Ports | | |
| TCP Port Min | 1024 | |
| TCP Port Max | 1039 | |
| Unencrypted TLINK Ports | | |
| TCP Port Min | <input type="text" value="1050"/> | |
| TCP Port Max | <input type="text" value="1065"/> | |
| Encrypted TLINK Ports | | |
| TCP Port Min | <input type="text" value="1066"/> | |
| TCP Port Max | <input type="text" value="1081"/> | |
| DMCC Server Ports | | Enabled Disabled |
| Unencrypted Port | <input type="text" value="4721"/> | <input checked="" type="radio"/> <input type="radio"/> |
| Encrypted Port | <input type="text" value="4722"/> | <input checked="" type="radio"/> <input type="radio"/> |
| TR/87 Port | <input type="text" value="4723"/> | <input checked="" type="radio"/> <input type="radio"/> |

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.

The screenshot shows the 'Service Settings' configuration page. On the left is a navigation menu with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security (expanded), and Host AA. Under Security, 'Service Settings' is selected. The main content area is titled 'Service Settings' and contains a table with two columns: 'Services' and 'Require Trusted Host Entry'. The 'Authenticate Client Cert with Trusted Certs' row is highlighted with a red box, showing 'TR/87' in the 'Services' column and a checked checkbox in the 'Require Trusted Host Entry' column. Below the table are 'Apply Changes' and 'Cancel Changes' buttons.

| Services | Authenticate Client Cert with Trusted Certs | Require Trusted Host Entry |
|----------|---|-------------------------------------|
| TR/87 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| DMCC | <input type="checkbox"/> | <input type="checkbox"/> |

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

The screenshot shows the 'Edit Dial Plan Settings DevCM3link' page. The left navigation menu is expanded to 'Dial Plan', with 'Switch Administration' selected. The main content area is titled 'From TelURI' and contains the following fields: 'Pattern Type' (dropdown menu set to 'Pattern'), 'Minimum Length' (text box with '4'), 'Maximum Length' (text box with '4'), 'Matching Pattern' (text box with 'tel:+ 52'), 'Delete Length' (text box with '0'), and 'Replacement String' (empty text box). A note on the right says 'Note: omit "+" from Delete Length'. At the bottom are 'Apply Changes' and 'Cancel Changes' buttons.

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.
 - 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**.

Service Controller

| Service | Controller Status |
|---|-------------------|
| <input type="checkbox"/> ASAI Link Manager | Running |
| <input type="checkbox"/> DMCC Service | Running |
| <input type="checkbox"/> CVLAN Service | Running |
| <input type="checkbox"/> DLG Service | Running |
| <input type="checkbox"/> Transport Layer Service | Running |
| <input checked="" type="checkbox"/> TSAPI Service | Running |

For status on actual services, please use [Status and Control](#)

Buttons: Start Stop Restart Service **Restart AE Server** Restart Linux Restart Web Server

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/ Link | AE Services Server | Remote IP | Remote Port | Local Node | Msgs Sent | Msgs Rcvd |
| 01/01 | DevAES | 135.10.97.62 | 34298 | procr | 664 | 655 |

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**.

Messaging System (Storage)

- User Management
- Class of Service
- Sites**
- Topology
- Storage Destinations
- System Policies
- Enhanced List Management
- System Mailboxes
- System Ports and Access
- User Activity Log Configuration

Reports (Storage)

- Users
- Info Mailboxes
- Remote Users
- Uninitialized Mailboxes
- Login Failures
- Locked Out Users

Server Information

Sites

Site:

Main Properties

Name:

ID:

Messaging access number (external):

Messaging access number (internal):

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

AVAYA

Help Log Off Administration

Administration / Messaging

Messaging System (Storage)

- User Management
- Class of Service
- Sites**
- Topology
- Storage Destinations
- System Policies
- Enhanced List Management
- System Mailboxes
- System Ports and Access
- User Activity Log Configuration

Reports (Storage)

- Users
- Info Mailboxes
- Remote Users
- Uninitialized Mailboxes
- Login Failures
- Locked Out Users

Subscriber number length (within this site's national destination code):

Outside line prefix:

Site Internal Dial Plan

Describe the internal dial plan applicable to this site.

Short extension length:

Short mailbox length:

Extension style for telephony integration: (Example: nnnnn)

Site prefix:

National mailbox number convention:

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.

Auto Attendant

Auto Attendant: ☒ enabled ☐ disabled

Auto Attendant pilot number:

Additional sites included in the directory: ☐ Default ☐ WindstreamSonus

Keypad entry:

BASIC: Enter extension only
ENHANCED: Enter extension or spell name

Speech recognition: ☒ enabled ☐ disabled

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:

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.

Telephony Integration

The Telephony Integration page is used for administration of the switch link parameters of the messaging system.

BASIC CONFIGURATION

Switch Number 1

Extension Length 5

Switch Integration Type SIP

IP Address Version IPv4

SIP SPECIFIC CONFIGURATION

Transport Method TCP

Far-end Connections 1

Connection 1 IP 135.10. . Port 5060

Messaging Address IP 10.32. . Port 5060

SIP Domain Messaging bvwddev.com Switch bvwddev.com

Messaging Ports Call Answer Ports 100 Maximum 100 Transfer Ports 20

Switch Trunks Total 120 Maximum 120

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.

Administration

Help Log Off

Administration / Messaging This Server: mango1-ms

Dial Rules

Dial Plan Handling

Dial plan handling style: Site definition based

Dial plan handling testing: Test...

Advanced Rules

Advanced Dial-out rules: Edit Dial-Out Rules...

Dial-in rules: system custom Edit Dial-In Rules...

Help Apply Reset Page

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.

Dial-Out Test Numbers

```

# Examples below.
# Add more phone numbers to test for your specific configuration.

# Extension (example):
2001
7785002
(212) 555-7086

# Local number (example):
555-7086
333-3030

# Long-distance number (example):
(408) 555-7086

```

Test

Save

Dial-Out Test Results

| 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.

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.

Class of Service

Class of Service: Standard

Add New Delete

General

Name: Standard

ID: 0

Required seat license: Mainstream (VALUE_MSG_SEAT_MAINSTREAM)

Telephone User Interface: Aria

☒ User can send to system distribution lists (ELAs)

Fax support: None

Dial-out privilege: Local

☒ User can use Reach Me

☒ Allow voice recognition for addressing (user can select recipients by saying their name)

IMAP4/POP3 access: Full (for Avaya Message Store users)

☒ Set Message Waiting Indicator (MWI) on user's desk phone

☐ Enable password aging

☐ User can send system broadcast messages

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
- **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**

Administration / Messaging

Messaging System (Storage)

User Management

Class of Service

Sites

Topology

Storage Destinations

System Policies

Enhanced List Management

System Mailboxes

System Ports and Access

User Activity Log Configuration

Reports (Storage)

Users

Info Mailboxes

Remote Users

Uninitialized Mailboxes

Login Failures

Locked Out Users

Server Information

System Status (Storage)

System Status (Application)

Alarm Summary

Voice Channels (Application)

Cache Statistics (Application)

Server Settings (Storage)

External Hosts

Trusted Servers

Networked Servers

Request Remote Update

IMAP/SMTP Settings (Storage)

General Options

Mail Options

IMAP/SMTP Status

Telephony Settings (Application)

Telephony Integration

User Management > Properties for BCM 22235

User Properties

First name: BCM

Last name: 22235

Display name: BCM 22235

ASCII name: BCM 22235

Site: Default

Mailbox number: 22235

Internal identifier: BCM.22235 @sp-aamess1.avaya.com

Numeric address: 22235

Extension: 22235

☒ Include in Auto Attendant directory

Class of Service: Standard

Pronounceable name: BCM 22235

MWI enabled: Yes

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.

AVAYA

[Help](#)
[Log Off](#)

Administration

Administration / Messaging

Messaging System (Storage)

User Management

Class of Service

Sites

Topology

Storage Destinations

System Policies

Enhanced List Management

System Mailboxes

System Ports and Access

User Activity Log Configuration

Reports (Storage)

Users

Info Mailboxes

Remote Users

Uninitialized Mailboxes

Login Failures

Locked Out Users

Server Information

System Status (Storage)

System Status (Application)

Alarm Summary

Voice Channels (Application)

Cache Statistics (Application)

Server Settings (Storage)

External Hosts

Trusted Servers

Networked Servers

Class of Service:

Standard

Pronounceable name:

BCM 22235

MWI enabled:

Yes

Miscellaneous 1:

Miscellaneous 2:

New password:

••••••

Confirm password:

••••••

☒ User must change voice messaging password at next logon

☐ Voice messaging password expired

☐ Locked out from voice messaging

Save

Delete

7.6. Administer Topology

Select Topology under Messaging System (Storage).

Verify the site that defined in **Section 7.1** is Active

AVAYA

Help Log Off Administration

Administration / Messaging

Messaging System (Storage)

User Management

Class of Service

Sites

Topology

Storage Destinations

System Policies

Enhanced List Management

System Mailboxes

System Ports and Access

User Activity Log Configuration

Reports (Storage)

Users

Info Mailboxes

Remote Users

Uninitialized Mailboxes

Login Failures

Locked Out Users

Server Information

System Status (Storage)

System Status (Application)

Alarm Summary

Voice Channels (Application)

Cache Statistics (Application)

Server Settings (Storage)

External Hosts

Trusted Servers

Networked Servers

Request Remote Update

IMAP/SMTP Settings (Storage)

General Options

Mail Options

IMAP/SMTP Status

Topology

Sites / Application Servers

| Sites | Status |
|-----------------|--------|
| 10.33.10.9 | Active |
| Phuong | Active |
| WindstreamSonus | Active |

Update Cancel

Add Application Server

IP address:

Role in application server cluster:

☒ Add as stand-alone (non-clustered) application server or as first application server in a new cluster

☐ Form (or join) a cluster by joining existing application server:

Choose One

Add

Remove Application Server

IP address: Choose One

Remove

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:

Change an Existing External Host

IP Address

Host Name

Alias

Back Save Help

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. 52150) 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: 52150@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
- Manage Element
- Applications
- Application Sequence
- User Management
- 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.

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.

The screenshot shows the 'Domain Management' page. On the left is a sidebar with 'Routing' expanded and 'Domains' selected. The main area has a breadcrumb 'Home / Elements / Routing / Domains-' and a 'Domain Management' title. Below the title is a table with one item. The table has columns: Name, Type, Default, and Notes. The row contains 'sipdev.com', 'sip', an unchecked checkbox, and an empty field. At the bottom right are 'Commit' and 'Cancel' buttons. A red box highlights the 'Commit' button.

| Name | Type | Default | Notes |
|------------|------|--------------------------|-------|
| sipdev.com | sip | <input type="checkbox"/> | |

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.

Home / Elements / Routing / Locations - Location Details

Location Details Commit

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth:

Location Pattern

Add Remove

2 Items | Refresh Filter: t

| <input type="checkbox"/> | IP Address Pattern | Notes |
|--------------------------|--------------------|----------------------|
| <input type="checkbox"/> | * 10.1.2.* | <input type="text"/> |
| <input type="checkbox"/> | * 10.1.1.* | <input type="text"/> |

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

- 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.

The screenshot displays the 'SIP Entity Details' configuration page. The left sidebar shows a navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields and values:

- Name:** ESNA
- FQDN or IP Address:** 135.10.
- Type:** Other
- Notes:** For Office Linx Testing
- Adaptation:** (empty dropdown)
- Location:** Belleville
- Time Zone:** America/New_York
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration

Buttons for 'Commit' and 'Cancel' are located in the top right corner.

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**).

- 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.

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 for this call (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.

Routing Policy Details

CommitCancel

General

* Name: RoutetoDevCM3

Disabled: ☐

Notes: Route to DevCM3

SIP Entity as Destination

Select

| Name | FQDN or IP Address | Type | Notes |
|--------|--------------------|------|-----------------|
| DevCM3 | 10.33. . | CM | G450CM Rls6.0.3 |

Time of Day

AddRemoveView Gaps/Overlaps

1 Item RefreshFilter: Enable

| <input type="checkbox"/> | Ranking 1 ▲ | Name 2 ▲ | Mon | Tue | Wed | Thu | Fri | Sat | Sun | Start Time | End Time | Notes |
|--------------------------|-------------|----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|------------|----------|-----------------|
| <input type="checkbox"/> | 0 | 24/7 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 00:00 | 23:59 | Time Range 24/7 |

Select : All, None

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.

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

Originating Locations and Routing Policies section

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

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

Dial Pattern Details
Commit
Cancel

General

* Pattern: 521
* Min: 5
* Max: 5
Emergency Call: ☐
SIP Domain: bvwdev.com
Notes: Dialing Plan for DevCM3 system

Originating Locations and Routing Policies

Add Remove

1 Item Refresh
Filter: Enable

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|---------------------|------|--------------------------|----------------------------|----------------------|
| <input type="checkbox"/> | -ALL- | Any Locations | RoutetoDevCM3 | 0 | <input type="checkbox"/> | DevCM3 | Route to DevCM3 |

Select : All, None

8.8. Configure Managed Elements

To define a new Managed Element, navigate to **Elements → Inventory → Manage Elements**. Click on the **New** button to open the **New Entities Instance** page.

In the **New Entities Instance** Page

- In the **Type** field, select **CM** using the drop-down menu and the **New CM Instance** page opens (not shown).

In the **New CM Instance** Page, provide the following information:

- Application section
 - Name** – Enter name for Communication Manager Evolution Server.
 - Description** - Enter description if desired.
 - Node** – Enter IP address of the administration interface. During the compliance test, the procr IP address, example: 10.33.4.9 was utilized.

The screenshot shows a window titled "Edit CM: DevCM3" with two tabs: "Application" and "Attributes". The "Attributes" tab is active. It contains the following fields:

- Name:** DevCM3
- Type:** CM (dropdown menu)
- Description:** G+50 CM
- Node:** 10.33.4.9

A red rectangular box highlights the "Name", "Type", "Description", and "Node" fields. In the top right corner, there are "Commit" and "Cancel" buttons.

- Leave the fields in the Port and Access Point sections blank. In the SNMP Attributes section, verify the default value of **None** is selected for the Version field.

Attributes section.

System Manager uses the information entered in this section to log into Communication Manager using its administration interface. Enter the following values and use default values for remaining fields.

- **Login** – Enter login used for administration access
- **Password** – Enter password used for administration access
- **Confirm Password** – Repeat value entered in above field.
- **Is SSH Connection** – Check the check box.
- **Port** – Verify **5022** has been entered as default value

Edit CM: DevCM3 [Commit] [Cancel]

Application * **Attributes ***

SNMP Attributes ▾

* Version ☒ None ☐ V1 ☐ V3

Attributes ▾

* Login

Password

Confirm Password

Is SSH Connection ☒

* Port

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Is ASG Enabled ☐

Click **Commit** to save the element. The element created, DevCM3, during the compliance test.

8.9. Configure Applications

To define a new Application, navigate to **Elements → Session Manager → Application Configuration → Applications**. Click **New** (not shown) to open the Applications Editor page, and provide the following information:

- Application Editor section
 - **Name** – Enter name for the application.
 - **SIP Entity** - Select SIP Entity for Communication Manager.
 - **CM System for SIP Entity** – Select name of Managed Element defined for Communication Manager.
 - **Description** – Enter description if desired.

Application Editor

Application

*Name

*SIP Entity

*CM System for SIP Entity [View/Add CM Systems](#)

Description

- Leave fields in the Application Attributes (optional) section blank.

Click the **Commit** button (not shown) to save the Application. The screen below shows the Application, DevCM3-G450, defined for Communication Manager.

| Applications | | |
|--|-----------------------------|---------------|
| This page allows you to add, edit, or remove applications for available SIP Entities. | | |
| Application Entries | | |
| <input type="button" value="New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> | | |
| 11 Items Refresh | | |
| <input type="checkbox"/> | Application Name | SIP Entity |
| <input checked="" type="checkbox"/> | DevCM3-G450 | DevCM3 |
| | | Phuong system |

8.10. Define Application Sequence

Navigate to **Elements → Session Manager → Application Configuration → Application Sequences**. Click **New** (not shown) and provide the following information:


- Sequence Name section
 - **Name** – Enter name for the application
 - **Description** – Enter description, if desired.

Application Sequence Editor

Application Sequence

***Name**

Description

- Available Applications section
 - Click  icon associated with the Application for Communication Manager defined in **Section 8.9** to select this application.
 - Verify a new entry is added to the Applications in this Sequence table as shown below.

Click the **Commit** button (not shown) to save the new Application Sequence.

Applications in this Sequence

1 Item

| <input type="checkbox"/> | Sequence Order (first to last) | Name | SIP Entity | Mandatory | Description |
|--------------------------|-----------------------------------|-----------------------------|------------|-------------------------------------|---------------|
| <input type="checkbox"/> | | DevCM3-G450 | DevCM3 | <input checked="" type="checkbox"/> | Phuong system |

Select: All, None

Available Applications

11 Items | Refresh

| | Name | SIP Entity | Description |
|--|-----------------------------|------------|---------------|
| | DevCM3-G450 | DevCM3 | Phuong system |

The screen below shows the Application Sequence, DevCM3_G450_Seq, defined during the compliance test.

Application Sequences
This page allows you to add, edit, or remove sequences of applications.

Application Sequences

New

Edit

Delete

11 Items | Refresh

| <input type="checkbox"/> | Name | Description |
|-------------------------------------|---------------------------------|--------------------------|
| <input type="checkbox"/> | dev-cm-seq1 | CM Sequence |
| <input checked="" type="checkbox"/> | DevCM3_G450_Seq | Sequen for CMG450 system |

Repeat steps if multiple applications are needed as part of the Application Sequence.

8.11. Configure SIP Users

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

- General section
 - **Last Name** – Enter last name of user.
 - **First Name** – Enter first name of user.

User Profile Edit: 52153@bvwddev.com

Identity * Communication Profile * Membership Contacts

Identity ▼

* Last Name: Nam

* First Name: Ba

Middle Name:

Description:

Status: Offline

Update Time : June 15, 2012 4:40:56

* Login Name: 52153@bvwddev.com

* Authentication Type: Basic ▼

[Change Password](#)

Source: local

Localized Display Name: Nam, Ba

Endpoint Display Name: Nam, Ba

Honorific:

Language Preference: English ▼

Time Zone: (-4:0)Eastern Time (US & Canada)

- Identity section (not shown)
 - **Login Name** – Enter extension number@sip domain. The sip domain is defined in **Section 8.1**.
 - **Authentication Type** – Verify **Basic** is selected.
 - **SMGR Login Password** – Enter password to be used to log into System Manager.
 - **Confirm Password** – Repeat value entered above.
 - **Shared Communication Profile Password** – Enter a numeric value used to logon to SIP telephone.
 - **Confirm Password** – Repeat numeric password
- Communication Profile section (not shown)

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

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

- Communication Address sub-section

Select **New** to define a **Communication Address** for the new SIP user, and provide the following information.

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

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

- Session Manager Profile section

- **Primary Session Manager** – Select one of the Session Managers.
- **Secondary Session Manager** – Select **(None)** from drop-down menu.
- **Origination Application Sequence** – Select Application Sequence defined in **Section 8.10** for Communication Manager.
- **Termination Application Sequence** – Select Application Sequence defined in **Section 8.10** for Communication Manager.
- **Survivability Server** – Select **(None)** from drop-down menu.
- **Home Location** – Select Location defined in **Section 8.2**.

The screenshot displays the configuration interface for a SIP user. The top section, titled "Communication Address", includes "New", "Edit", and "Delete" buttons. Below these is a table with columns for checkboxes, Type, Handle, and Domain. A single entry is shown: "Avaya SIP" with Handle "52153" and Domain "bvwddev.com". Below the table is a "Select : All, None" option. The bottom section, titled "Session Manager Profile", is checked. It contains two rows for Session Manager selection. The first row, "Primary Session Manager", has a dropdown set to "DevASM" and a table with values: Primary 40, Secondary 0, Maximum 40. The second row, "Secondary Session Manager", has a dropdown set to "(None)" and an empty table. Below these are four dropdown menus: "Origination Application Sequence" (DevCM3_G450_Seq), "Termination Application Sequence" (DevCM3_G450_Seq), "Survivability Server" (None), and "* Home Location" (Belleville). A red box highlights the last three dropdowns.

| | Type | Handle | Domain |
|--------------------------|-----------|--------|-------------|
| <input type="checkbox"/> | Avaya SIP | 52153 | bvwddev.com |

Select : All, None

☒ Session Manager Profile

* Primary Session Manager: DevASM

| Primary | Secondary | Maximum |
|---------|-----------|---------|
| 40 | 0 | 40 |

Secondary Session Manager: (None)

| Primary | Secondary | Maximum |
|---------|-----------|---------|
| | | |

Origination Application Sequence: DevCM3_G450_Seq

Termination Application Sequence: DevCM3_G450_Seq

Survivability Server: (None)

* Home Location: Belleville

- Endpoint Profile section

- **System** – Select Managed Element defined in **Section 8.8** for Communication Manager Feature Server.

- **Use Existing Endpoints** - Leave unchecked to automatically create new endpoint when new user is created. Or else, check the box if endpoint is already defined in Communication Manager.
- **Extension** - Enter same extension number used in this section.
- **Template** – Select template for type of SIP phone
- **Security Code** – Enter numeric value used to logon to SIP telephone. (**Note:** this field must match the value entered for the Shared Communication Profile Password field.
- **Port** – Select **IP** from drop down menu
- **Voice Mail Number** – Enter **Pilot Number** for Avaya Modular Messaging if installed. Or else, leave field blank.
- **Delete Station on Unassign of Endpoint** – Check the box to automatically delete station when Endpoint Profile is un-assigned from user.

☒ **Endpoint Profile**

* **System** DevCM3

* **Profile Type** Endpoint

Use Existing Endpoints ☐

* **Extension** 52153 [Endpoint Editor](#)

Template Select/Reset

Set Type 9640SIP

Security Code

* **Port** S00026

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User or on Delete User. ☐


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

| User Management | | | | | |
|---|--------|---------------|-------------------|-------------|------------|
| Users | | | | | |
| View Edit New Duplicate Delete More Actions | | | | | |
| 41 Items Refresh Show 20 Advanced Search | | | | | |
| Filter: Enable | | | | | |
| <input type="checkbox"/> | Status | Name | Login Name | E164 Handle | Last Login |
| <input type="checkbox"/> | | Lyrix 75016 | 75016@bvwdev7.com | 75016 | |
| <input type="checkbox"/> | | Lyrix, SIP | 76000@bvwdev7.com | 76000 | |
| <input type="checkbox"/> | | MTS SIP x3573 | 7763573@avaya.com | 7763573 | |
| <input checked="" type="checkbox"/> | | Nam, Ba | 52153@bvwdev7.com | 52153 | |

8.12. Synchronization Changes with Avaya Aura® Communication Manager

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

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

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

Synchronize CM Data and Configure Options

Synchronize CM Data/Launch Element Cut Through | Configuration Options |
Expand All | Collapse All

Synchronize CM Data/Launch Element Cut Through ▾

5 Items Refresh Show ALL ▾

| <input type="checkbox"/> | Element Name | FQDN/IP Address | Last Sync Time | Last Translation Time | Sync Type | Sync Status | Location |
|-------------------------------------|--|-----------------|---------------------------------------|------------------------------|-------------|-------------|-----------------------|
| <input type="checkbox"/> | CM2_Rel-6_G450 | 135.10.97.246 | July 9, 2012 11:00:09 PM -04:00 | 10:00 pm MON JUL 9, 2012 | Incremental | Completed | Belleville |
| <input type="checkbox"/> | CM_G450_Instance | 135.10.97.219 | July 9, 2012 11:00:11 PM -04:00 | 10:00 pm MON JUL 9, 2012 | Incremental | Completed | |
| <input type="checkbox"/> | DevCM | 135.10.97.201 | July 9, 2012 11:00:12 PM -04:00 | 10:00 pm MON JUL 9, 2012 | Incremental | Completed | |
| <input checked="" type="checkbox"/> | DevCM3 | 10.33.4.9 | July 9, 2012 11:00:09 PM -04:00 | 10:00 pm TUE JUL 10, 2012 | Incremental | Completed | |
| <input type="checkbox"/> | Select row 4 e-devmes-cm | 135.10.97.23 | July 9, 2012 11:00:09 PM -04:00 | 10:01 pm MON JUL 9, 2012 | Incremental | Completed | CM in the Cage Lab |

Select : All, None

☐ Initialize data for selected devices
☒ Incremental Sync data for selected devices
☐ Save Translations for selected devices

Now Schedule Cancel Launch Element Cut Through

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
- 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
```

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:

```
[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 ACEca.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

The hostname is often the FQDN but check

Welcome: User admin
Last login: Thu Sep 20 13:24:13 2011 from 135.20.117.222
HostName/IP: scalab136.aceott.avaya.com 135.20.245.136
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-0-20-0

AVAYA Application Enablement Services Management Console

Security | Certificate Management | Server Certificate Home | Help | Logout

Add Server Certificate

Certificate Alias: **aeservices** ← Pick aeservices from pull-down

☐ Create Self-Signed Certificate

Enrollment Method: **Manual**

Certificate Key Parameters:

Encryption Algorithm: **3DES**

Password: ********* ← Put in the password from the certs

Re-enter Password: *********

Key Size: **1024**

Certificate Request Parameters:

Certificate Validity: **1825**

Distinguished Name (DN): **O=AVAYA,OU=ACE,CN=scalab136.aceott.avaya.com** ← Make sure to put the FQDN of the AES in here

(In DN use comma ',' as attributes separator. To include colons, use backslash, e.g. \.)

Challenge Password: *********

Re-enter Challenge Password: *********

Key Usage:

☐ Digital Signature
☐ Non-repudiation
☐ Key encipherment
☐ Data encipherment
☐ Key agreement
☐ Key certificate sign
☐ CRL sign
☐ Encipher only
☐ Decipher only

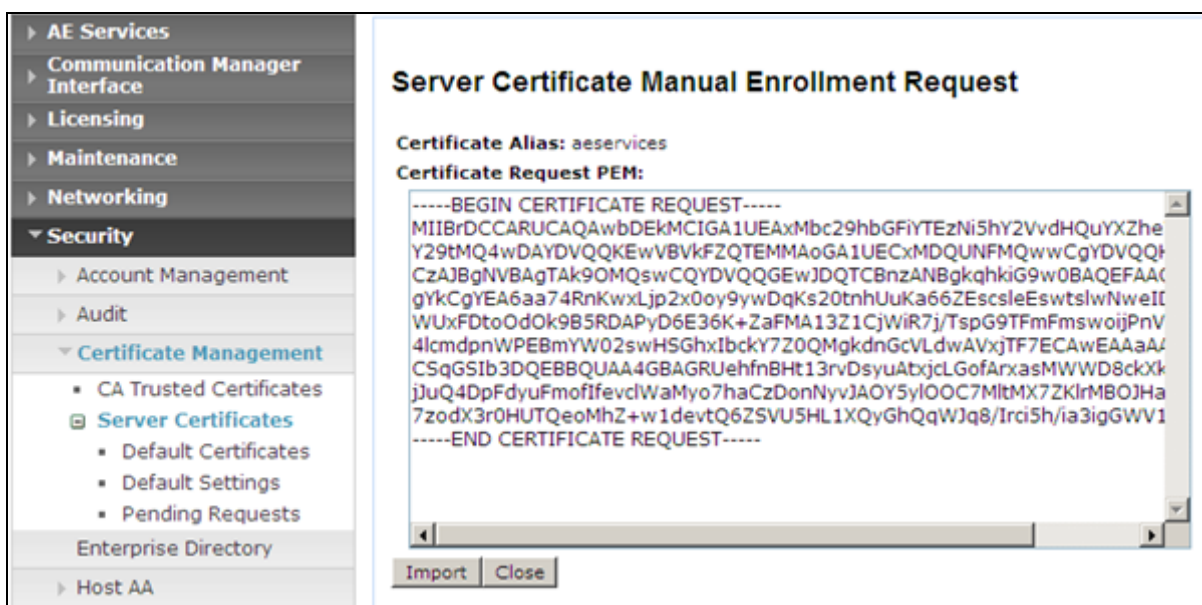
Extended Key Usage:

☐ SSL/TLS Web Server Authentication
☐ SSL/TLS Web Client Authentication
☐ Code Signing
☐ Email Protection (S/MIME)

SCEP Parameters:

SCEP Server URL: *********

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



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 :wq!
9. Save file as aes.req in CA folder. See below figure.

```

root@ace1:~/CA2
-----BEGIN CERTIFICATE REQUEST-----
MIIBrDCCARUCAQAwbDEkMCIGA1UEAxMbc29hbGFiYTEzNi5hY2VvdHQuYXZheWEu
Y29tMQ4wDAYDVQQKEwVBVkfZQTEMMaGA1UECxMDQUNFMQwwCgYDVQQHEwNPVFQx
CzAJBgNVBAGTAk9OMQswCQYDVQQGEwJDQTCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEA6aa74RnKwxLjp2x0oy9ywDqKs20tnhUuKa66ZEscsleEswtswNweIDj
WUxFTdoOdOk9B5RDAPyD6E36K+ZaFMA13Z1CjWiR7j/TspG9TFmFmswoijPnV
4lcmdpnWPEBmYW02swHSghxIbckY7Z0QMgkdnGcVLdwAVxjTF7ECAwEAAaAAMAOG
CSqGSIb3DQEBBQUAA4GBAGRUehfnBHt13rvDsyuAtxjclGofArxasMWWd8ckXk1m
jJuQ4DpFdyuFmofIfevclWaMyo7haCzDonNyyJAoy5yloOC7MltMX7ZKlrMBOJHa
7zodX3rOHUTQeoMhZ+w1devtQ6ZSVU5HL1XQyGhQqWJq8/Irci5h/ia3igGWV18M
-----END CERTIFICATE REQUEST-----
~
~
:wq!

```

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=ace1.gmiott.avaya.com" -newkey rsa:1024 -sha1 -nodes -keyout ace.private.key -out ace.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 -CAcreateserial
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

9.1.7. Signing an ACE certificate request

Sign the certificate request. Enter:

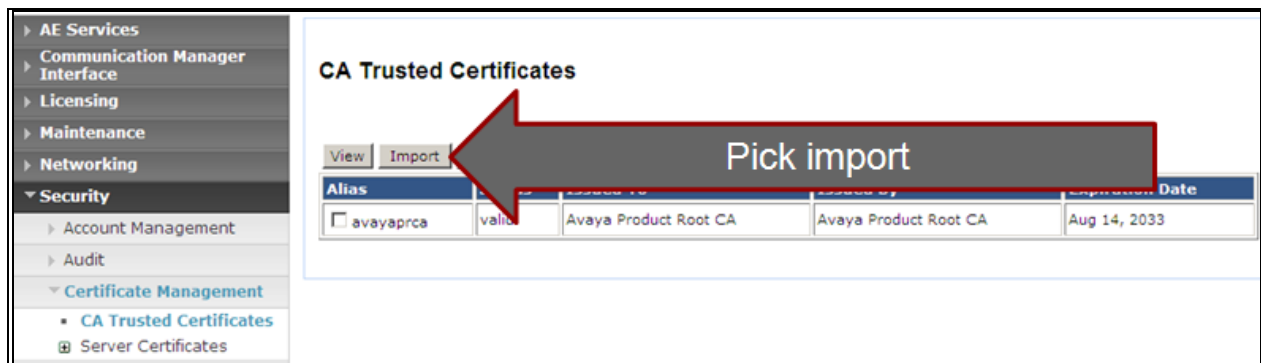
openssl x509 -req -in **ace.req** -out **ace.crt** -CA **ACEca.crt** -CAkey **ACEca.private.key** -days **500** -extfile openssl.conf -extensions usr_cert -CAcreateserial

```
[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]#
```

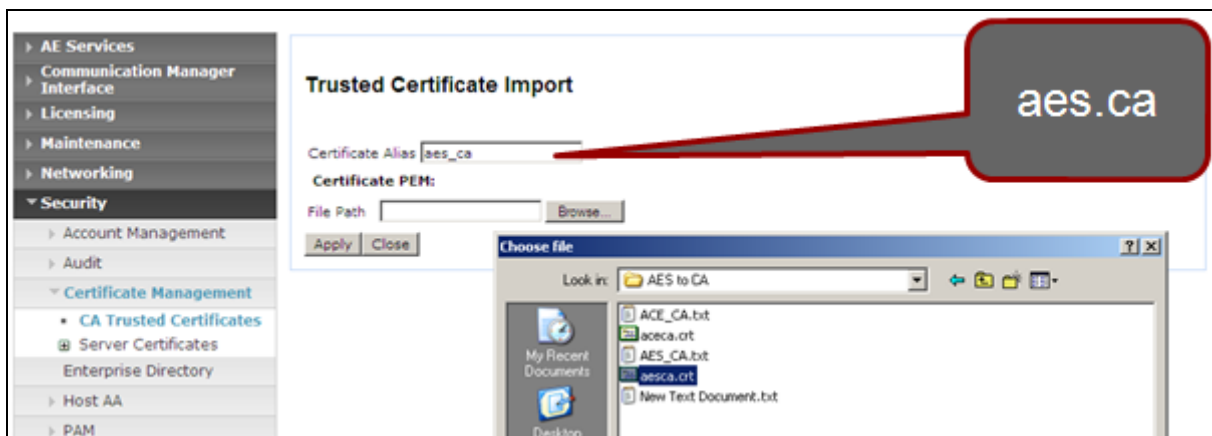
Download the certificate to your AE Services administrative workstation, and save it with a unique name, for example C:\CA\ACEca.crt

9.1.8. Importing the server certificate into AE Services

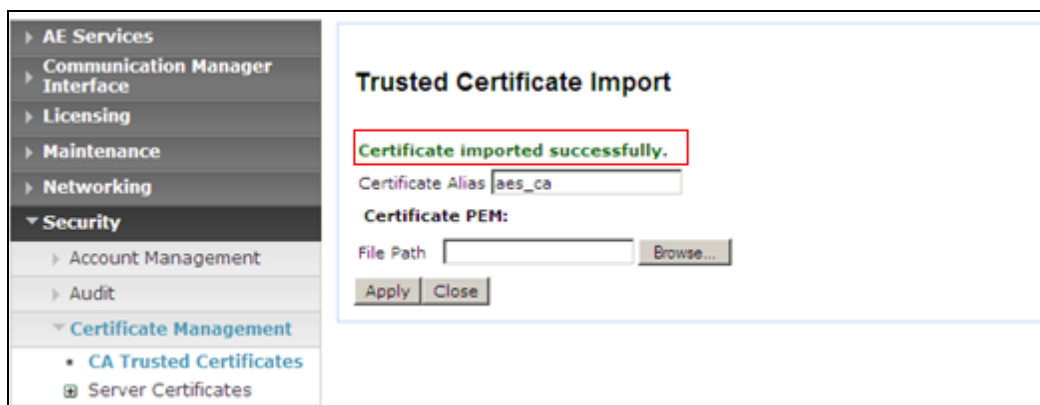
On AES select **Security** → **Certificate Management** → **CA Trusted Certificates**, click **Import**



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

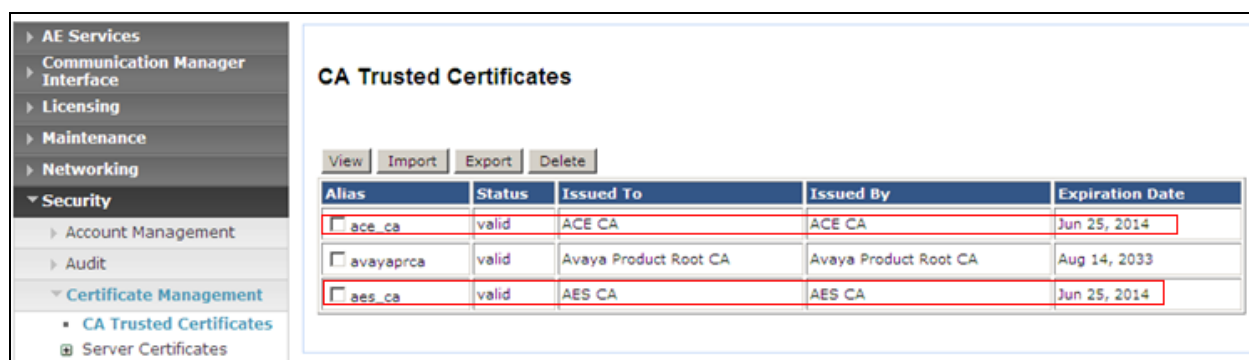


Ensure the cert is imported successfully.

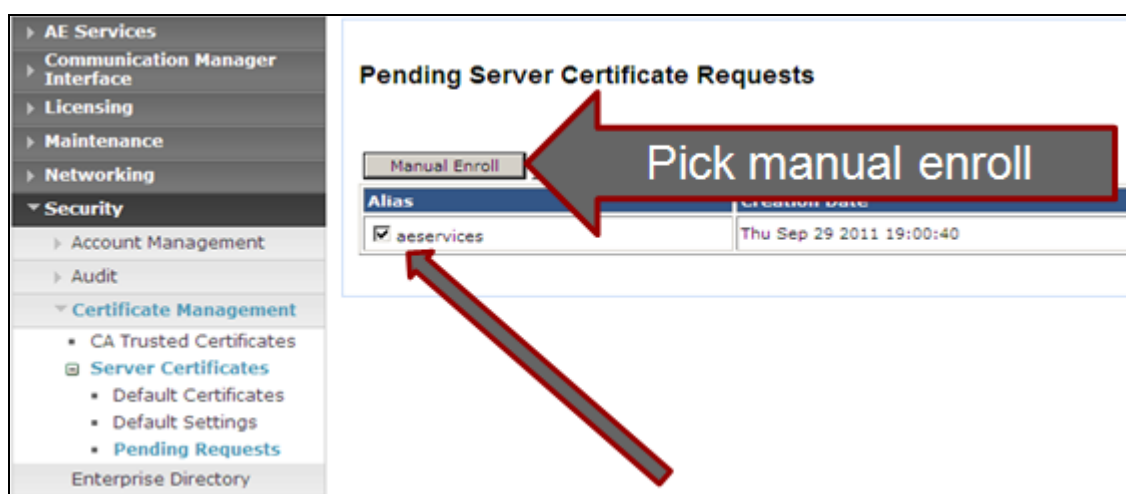


Repeat the same step for ACEca.crt.

Go to **Security → Certificate Management → CA Trusted Certificates**: verify CA trusted certificates now in place and their status are Valid.



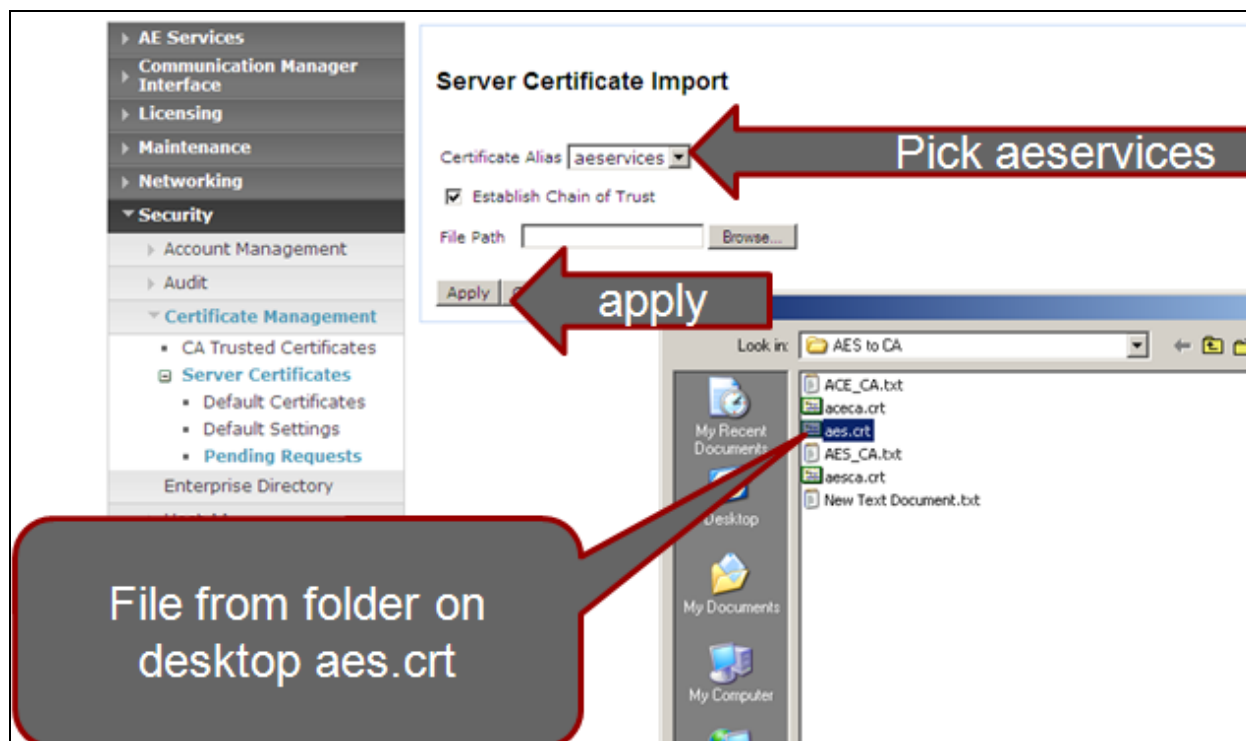
Select **Security → Certificate Management → Server Certificates → Pending Request**



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

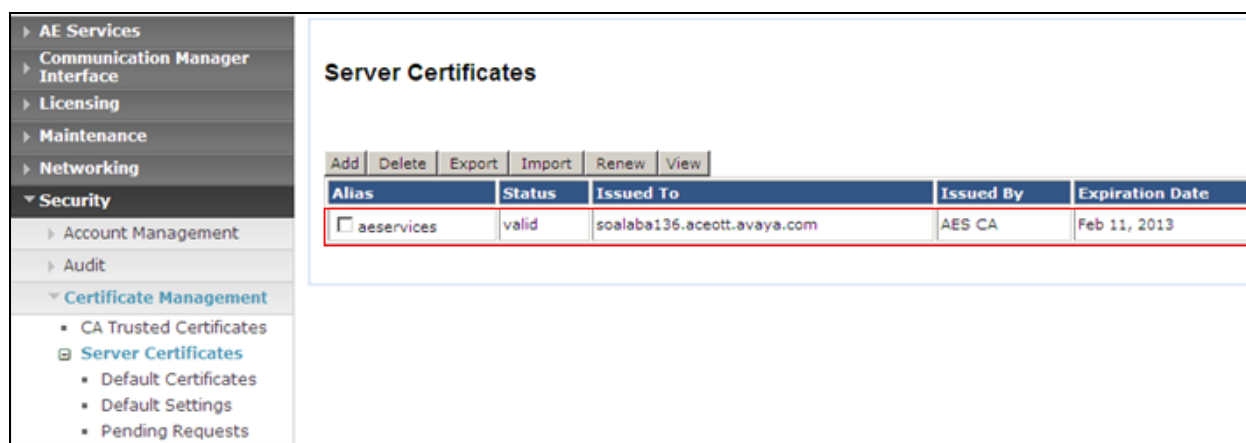
Download the certificate to your AE Services administrative workstation, and save it with a unique name, for example C:\CA\aes.crt

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



Make sure import is successful.

Verify the server certificate in place and its status is valid.



9.1.9. Add Trusted Host

Select **Security** → **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 C42]# hostname
ace1.gmiott.avaya.com
[root@ace1 C42]#
```

Add Trusted Host

Certificate CN or SubAltName:

Service Type*:

User Authentication Policy*:

User Authorization Policy*:

The "All" Service Type can be used to specify a user authorization policy for both the DMCC and TR/87 services. The TR/87 service cannot perform user authentication. Therefore, if a user authentication policy of "User Authentication Required" is selected with a Service Type of "All" that will only enable user authentication on the DMCC service.

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.

Trusted Hosts*

| Certificate CN or SubAltName | Service Type | User Authentication Policy | User Authorization Policy |
|------------------------------|--------------|-----------------------------|---------------------------|
| ace1.gmiott.avaya.com | ALL | AUTHENTICATION_NOT_REQUIRED | UNRESTRICTED_ACCESS |

* Note: This page is only enforced to be configured if the "Require Trusted Host Entry" checkbox is checked on the "Service Settings" page.

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

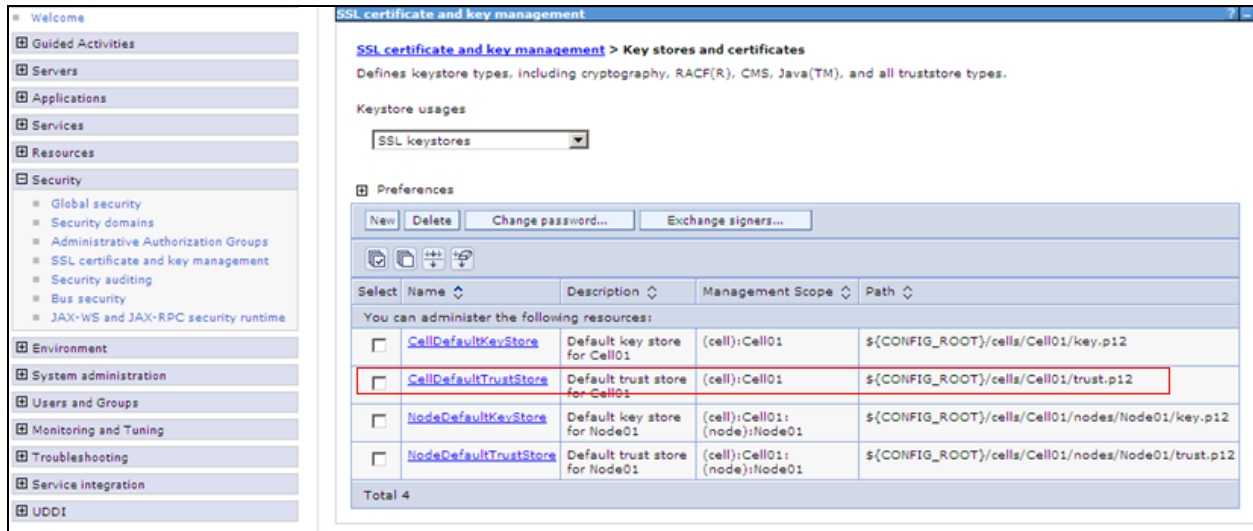
For Avaya Agile Communication Environment™ (ACE) on Linux installations, you can manage certificates on using the IBM Integrated Solutions Console. Procedures documented in this section are based on IBM WebSphere documentation. IBM WebSphere product documentation is available online at the following location:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?S_TACT=105AGX10&S_CMP=LP.

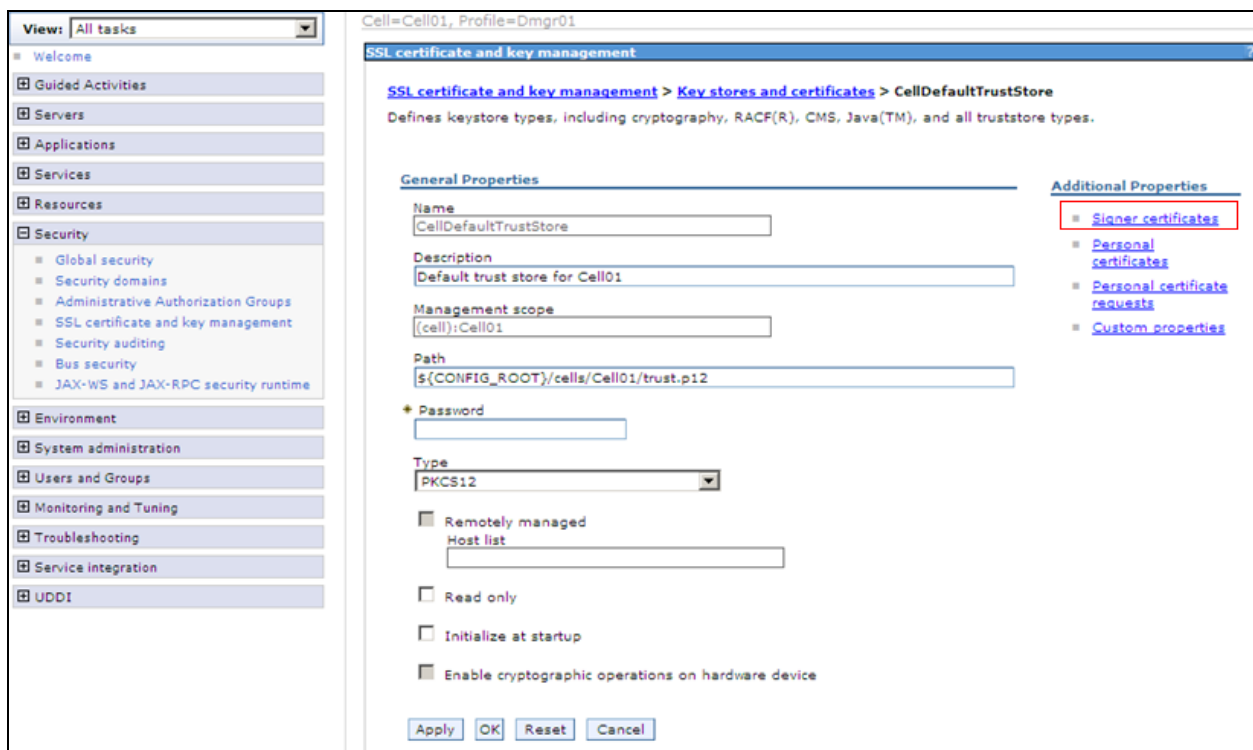
Open web browser and go to ACE WAS admin page <https://<ACEipaddress>:9043/admin>

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:

SSL certificate and key management

[SSL certificate and key management](#) > [Key stores and certificates](#) > [CellDefaultTrustStore](#) > [Signer certificates](#) > [Add signer certificate](#)

Adds a signer certificate to a key store.

General Properties

* Alias

* File name

Data type

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

Cell=Cell01, Profile=Dmgr01

SSL certificate and key management

Messages

- Changes
 - Save
 - Review

An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).

The server may need to be restarted for these changes to take effect.

SSL certificate and key management > [Key stores and certificates](#) > [CellDefaultTrustStore](#) > [Signer certificates](#) > [Add signer certificate](#) > aes_ca

Manages signer certificates in key stores.

General Properties

Alias

Version

Key size

Serial number

Validity period

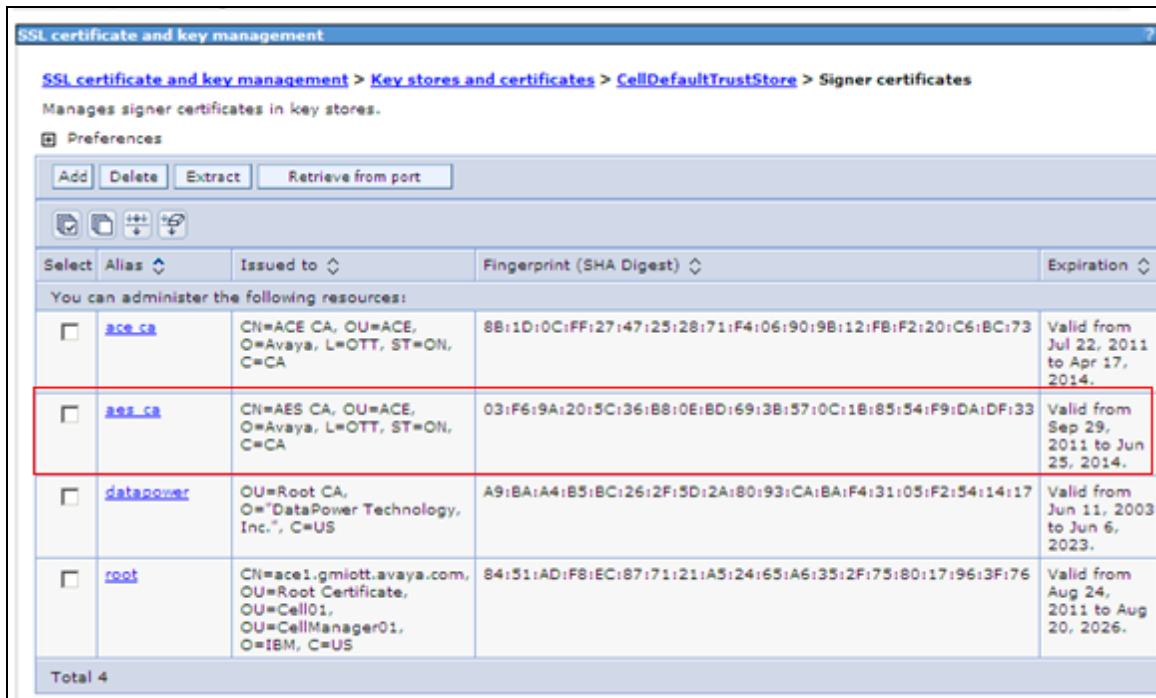
Issued to

Issued by

Fingerprint (SHA digest)

Signature algorithm

New alias is added



9.2.2. Export ACE server cert

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

```
[root@ace1 CA2]#  
[root@ace1 CA2]# openssl pkcs12 -export -in ace.crt -inkey ace.private.key -name  
"ACE Certificate" -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

SSL certificate and key management

Messages

Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

An option to synchronize the configuration across multiple nodes after saving can be enabled in Preferences.

The server may need to be restarted for these changes to take effect.

SSL certificate and key management > Key stores and certificates > CellDefaultKeyStore > Personal certificates > Import certificates from a key file or key store

Imports a certificate, including the private key, from a key store file or from an existing key store.

General Properties

☐ Managed key store

Key store

CellDefaultKeyStore ((cell):Cell01)

Key store password

Get key store aliases

☒ Key store file

* Key file name

/root/CA2/ace.p12

Type

PKCS12

* Key file password

Get Key File Aliases

Certificate alias to import

ace certificate

Imported certificate alias

ACEcert

Apply OK Reset Cancel

Click Apply and click Save.

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

SSL certificate and key management

[SSL certificate and key management](#) > **SSL configurations**

Defines a list of Secure Sockets Layer (SSL) configurations.

⊞ Preferences

New Delete

⊞ ⊞ ⊞ ⊞

| Select | Name | Management Scope |
|---|--|-----------------------------|
| You can administer the following resources: | | |
| <input type="checkbox"/> | ACESpecific | (cell):Cell01 |
| <input type="checkbox"/> | CellDefaultSSLSettings | (cell):Cell01 |
| <input type="checkbox"/> | NodeDefaultSSLSettings | (cell):Cell01:(node):Node01 |
| Total 3 | | |

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

SSL certificate and key management

[SSL certificate and key management](#) > [SSL configurations](#) > **ACESpecific**

Defines a list of Secure Sockets Layer (SSL) configurations.

General Properties

* Name
ACESpecific

Trust store name
CellDefaultTrustStore ((cell):Cell01)

Keystore name
CellDefaultKeyStore ((cell):Cell01) [Get certificate aliases](#)

Default server certificate alias
acecert

Default client certificate alias
acecert

Management scope
(cell):Cell01

[Apply](#) [OK](#) [Reset](#) [Cancel](#)

Additional Properties

- [Quality of protection \(QoP\) settings](#)
- [Trust and key managers](#)
- [Custom properties](#)

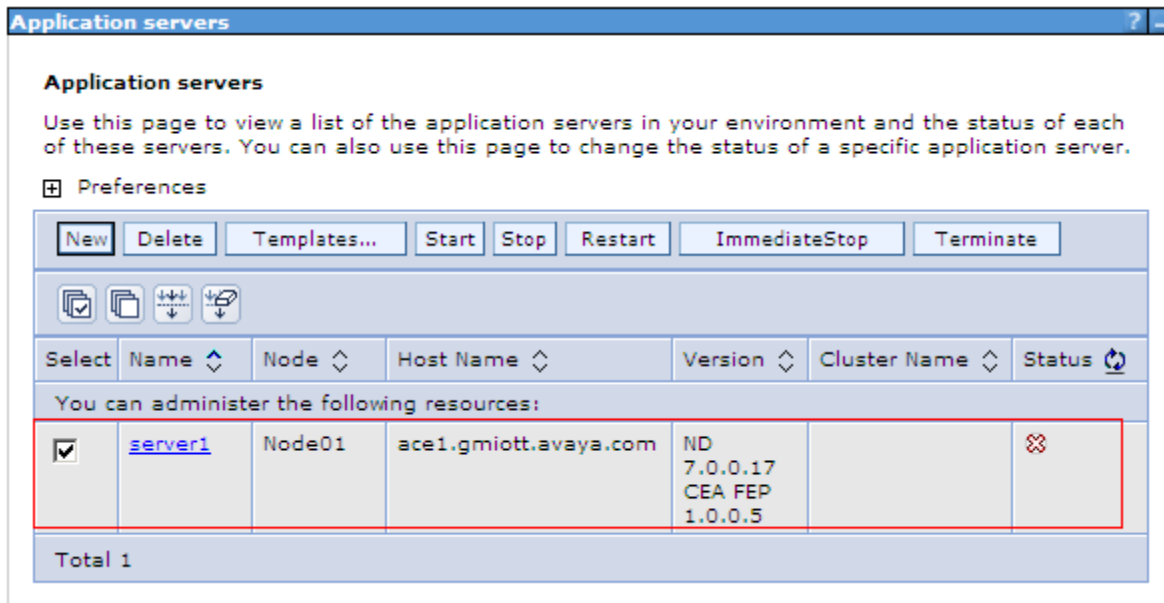
Related Items

- [Key stores and certificates](#)

Make sure to click Save.

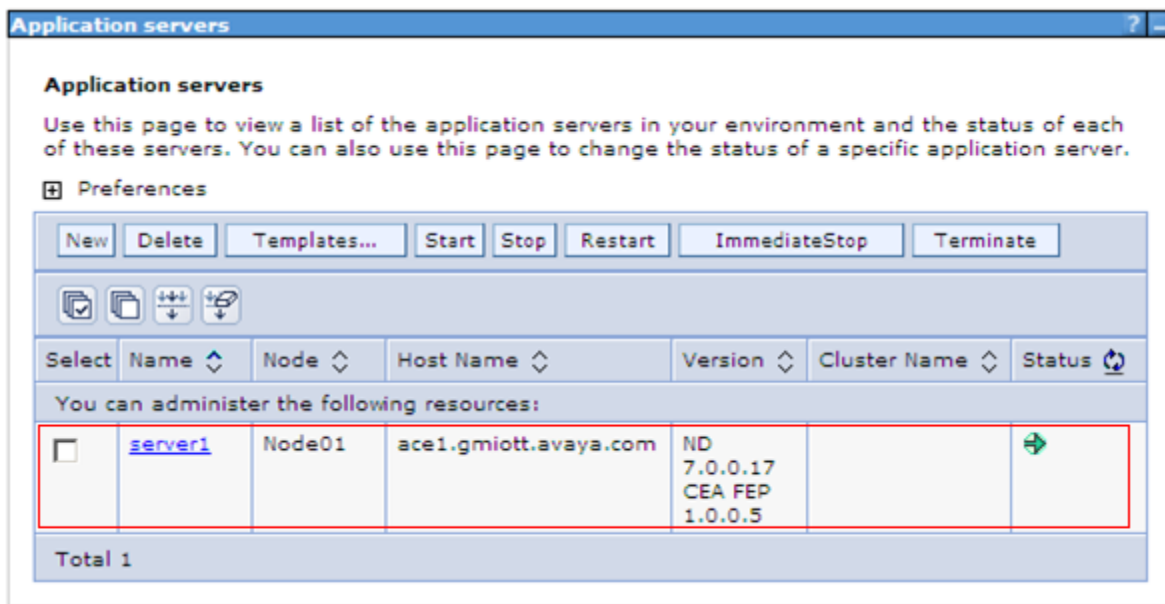
9.2.4. Restart Avaya ACE and AE server

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).

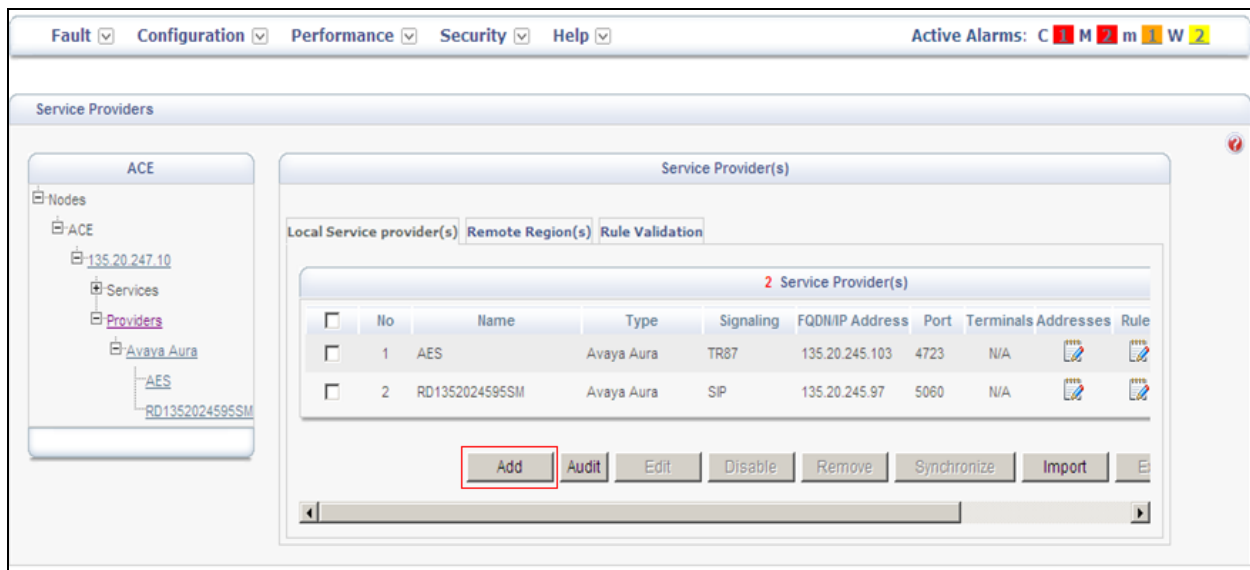
Go to ACE IBM Integrated Solution Console and start ACE by select **Servers** → **WebSphere Application Server** and select **Start**. Verify the server status is back and indicated with a green arrow.



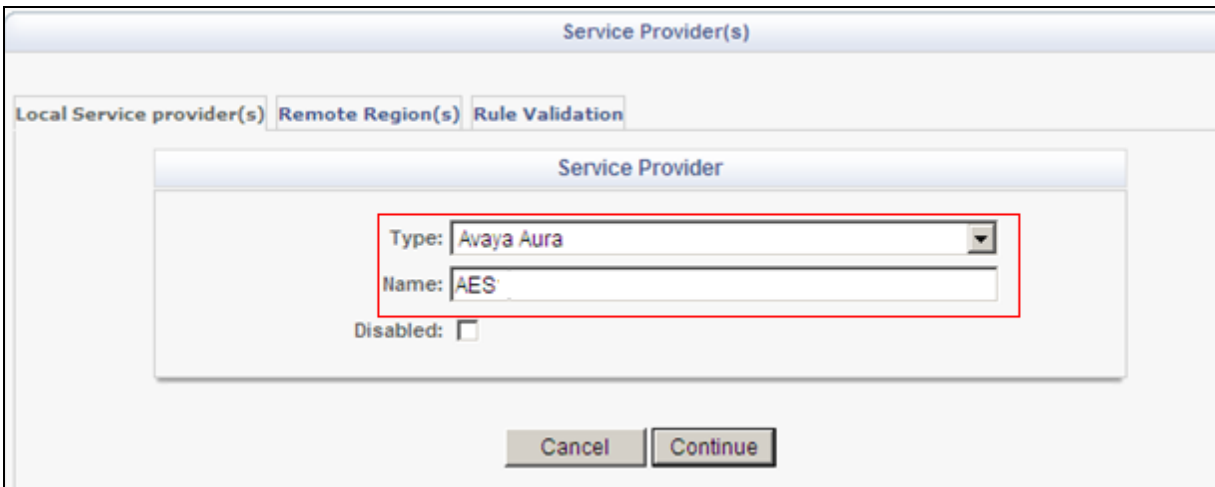
9.3. Add Service Provider

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



Type: Avaya Aura
Name: AES



The image shows a 'Service Provider(s)' configuration window. It has three tabs: 'Local Service provider(s)', 'Remote Region(s)', and 'Rule Validation'. The 'Local Service provider(s)' tab is selected. Inside this tab, there is a 'Service Provider' sub-window. In this sub-window, the 'Type' dropdown is set to 'Avaya Aura' and the 'Name' text field contains 'AES'. A red rectangle highlights these two fields. Below the text fields is a 'Disabled' checkbox, which is unchecked. At the bottom of the window are 'Cancel' and 'Continue' buttons.

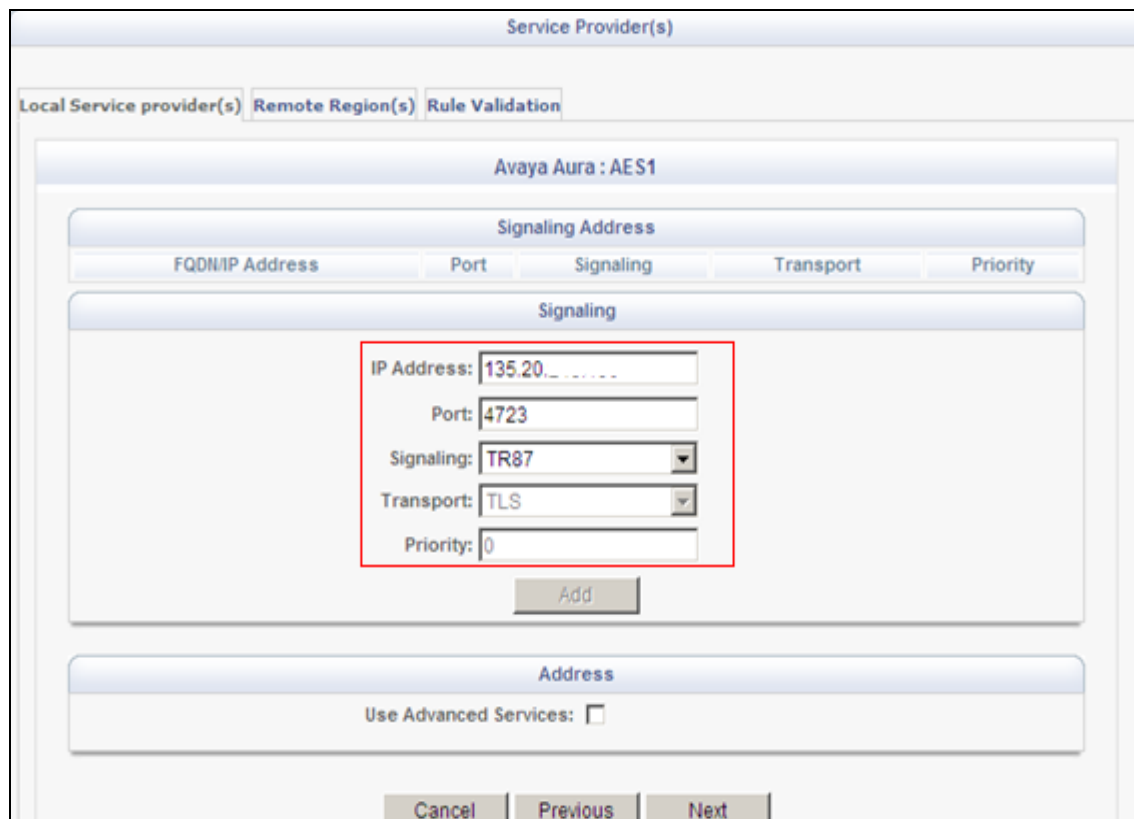
Click **Continue**

IP Address: Enter IP address of AES server, can be provisioned via FQDN

Port: 4723

Signalling: TR/87. There is a warning when user picks TR/87 as signalling. Click OK

Transport: TLS



The image shows the 'Avaya Aura : AES1' configuration window. It has three tabs: 'Local Service provider(s)', 'Remote Region(s)', and 'Rule Validation'. The 'Local Service provider(s)' tab is selected. Inside this tab, there is a 'Signaling Address' sub-window. This sub-window has a table with columns: 'FQDN/IP Address', 'Port', 'Signaling', 'Transport', and 'Priority'. Below the table is a 'Signaling' sub-window. In this sub-window, the 'IP Address' text field contains '135.20.', the 'Port' text field contains '4723', the 'Signaling' dropdown is set to 'TR87', the 'Transport' dropdown is set to 'TLS', and the 'Priority' text field contains '0'. A red rectangle highlights these five fields. Below the text fields is an 'Add' button. At the bottom of the window are 'Cancel', 'Previous', and 'Next' buttons.

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:

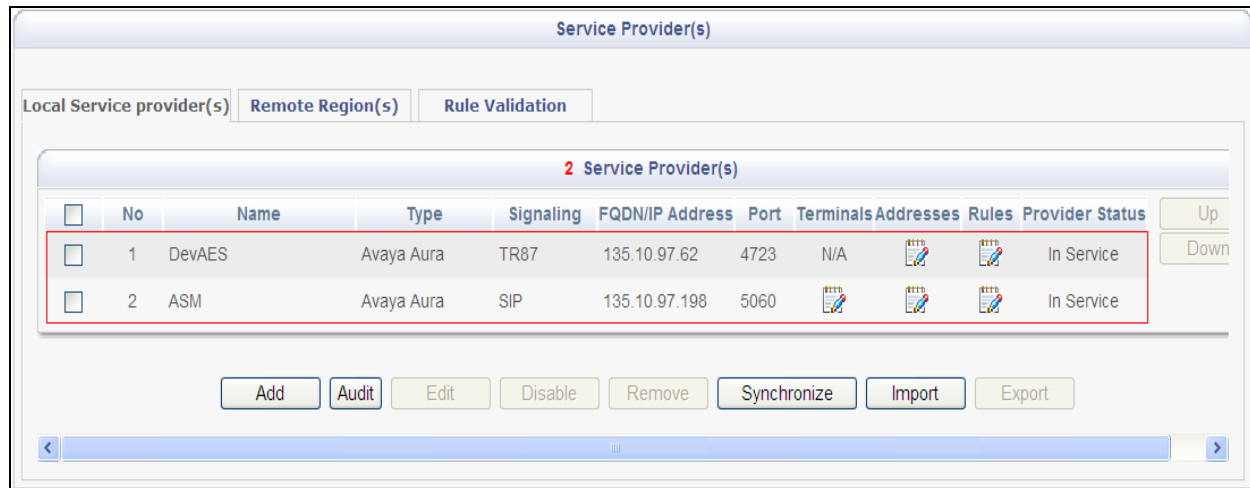
The screenshot shows the 'Service Provider(s)' configuration window. It has three tabs: 'Local Service provider(s)', 'Remote Region(s)', and 'Rule Validation'. The 'Local Service provider(s)' tab is active, showing a table titled 'Avaya Aura : DevAES 1 Address(es)'. The table has columns: No, Name, Type, Display Name, URI, and Terminals. There is one row with No. 1, Name 'thirdPartyCallController', Type 'Route', Display Name (empty), URI 'sip:AppCore@bvwdev.com', and Terminals 'N/A'. Below the table is an 'Address Details' section with the following fields: Type (dropdown set to 'Route'), Name (dropdown set to 'thirdPartyCallControle'), Display Name (text field), URI (text field with 'sip:AppCore@bvwdev.cor'), and Terminals (text area). At the bottom are buttons: Done, Add, Modify, Remove, and Reset.

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)

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.

Create User

User Information

User | **Personal Data** | Organization Data | Preferences | User Group Membership | Account Policy

User ID: esna-admin1

Account State: Enabled

User Password:

Confirm User Password: Passwords Match

☐ User must change password at next logon

Submit Reset

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.

User ID: esna_admin1

User | Personal Data | Organization Data | Preferences | **User Group Membership** | Account Policy

Available User Groups

ESNA User
FederationGroup
SystemMonitorGroup

View User Group

>>

<<

Member User Groups

ESNA Admin
SystemAdminGroup

View User Group

Submit Reset Back

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 screenshot displays the 'Service Provider(s)' configuration page. The 'Remote Region(s)' tab is selected, showing the 'Translation Rule for Service Provider -- Avaya Aura : DevAES'. A red box highlights the 'Calling Party Translation Rule' section. Below it is a table with three rules, all of which are active and have 'Reverse Transformation' set to 'No'. The middle rule, which matches the range 52150-52169, is highlighted with a red border.

| Type | Rules | Reverse Transformation | Rule Active |
|--------|---|------------------------|-------------|
| Simple | URIScheme=tel,RangeFrom=21600,RangeTo=21666,Insert Digit=+, | No | Yes |
| Simple | URIScheme=tel,RangeFrom=52150,RangeTo=52169,Insert Digit=+, | No | Yes |
| Simple | URIScheme=tel,RangeFrom=1129,RangeTo=1132,InsertDigit=+, | No | Yes |

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

This screenshot is similar to the one above, showing the 'Called Party Translation Rule' section for the same service provider. The table contains the same three rules, with the middle rule (range 52150-52169) highlighted by a red border.

| Type | Rules | Reverse Transformation | Rule Active |
|--------|---|------------------------|-------------|
| Simple | URIScheme=tel,RangeFrom=21600,RangeTo=21666,Insert Digit=+, | No | Yes |
| Simple | URIScheme=tel,RangeFrom=52150,RangeTo=52169,Insert Digit=+, | No | Yes |
| Simple | URIScheme=tel,RangeFrom=1129,RangeTo=1132,InsertDigit=+, | No | Yes |

10. Configure the ESNA Telephony Office-LinX

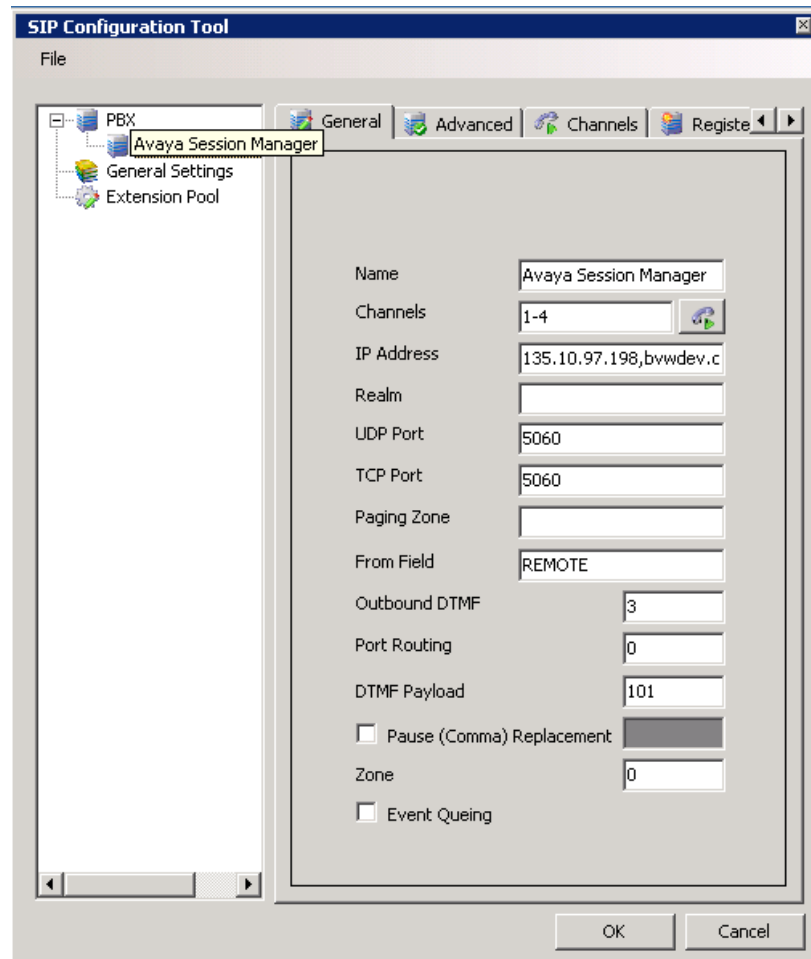
ESNA installs, configures, and customizes the Telephony Office-LinX application for their customers. Thus, this section only describes the interface configuration, so that the Telephony Office-LinX can talk to Avaya Session Manager, Avaya ACE and Avaya Aura Messaging.

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:

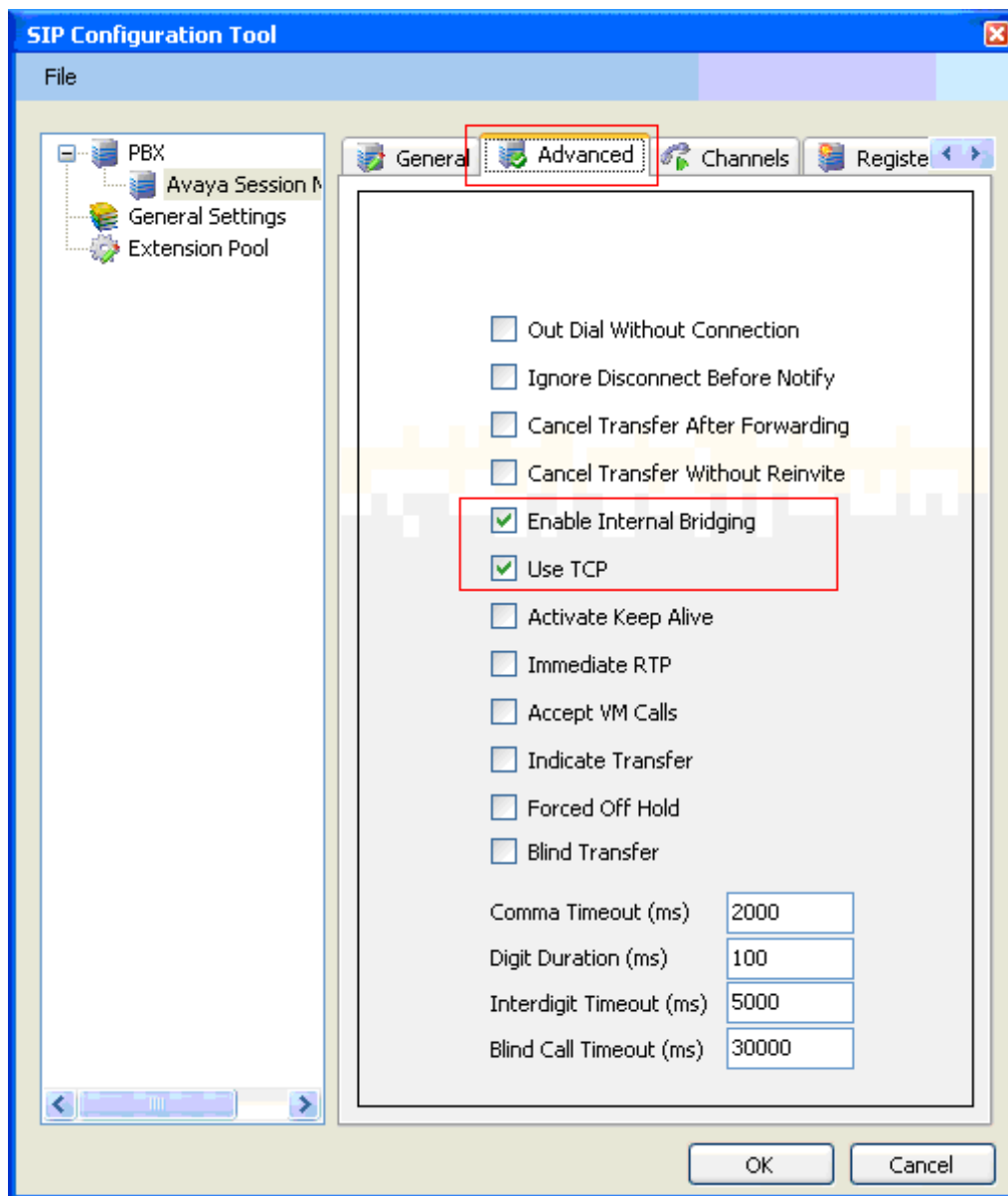
- **IP Address** – Enter **IP address** and **Domain** in the field
- **UDP Port** – Enter **5060**

- **TCP Port** – Enter **5060**

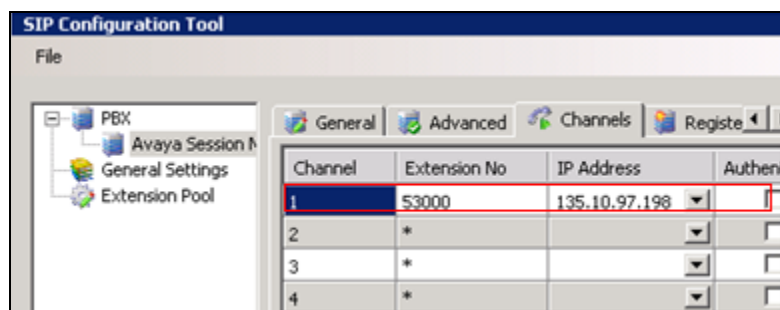


Click the **Advanced** tab in the right pane, and check the following check boxes:

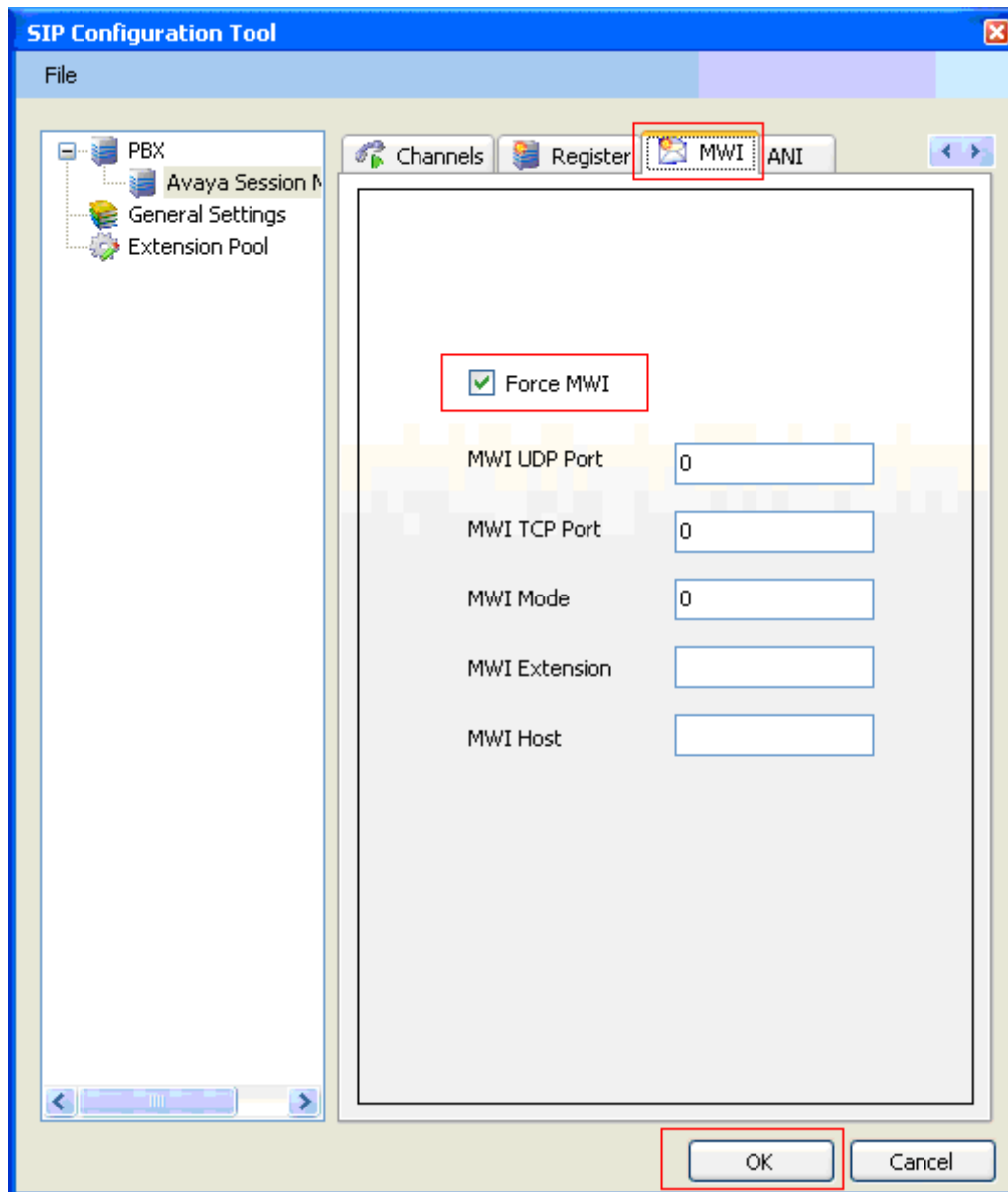
- Enable Internal Bridging
- Use TCP



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.



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

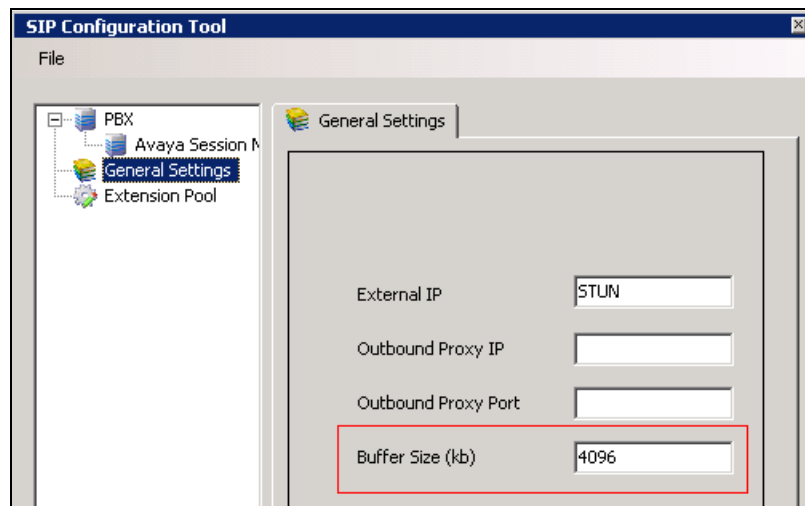


The following line must be added to the SIP Configuration file (ETSIPService.ini, found under C:\Windows\) manually under the [PBX#] heading:

Subscription State for MWI = 0

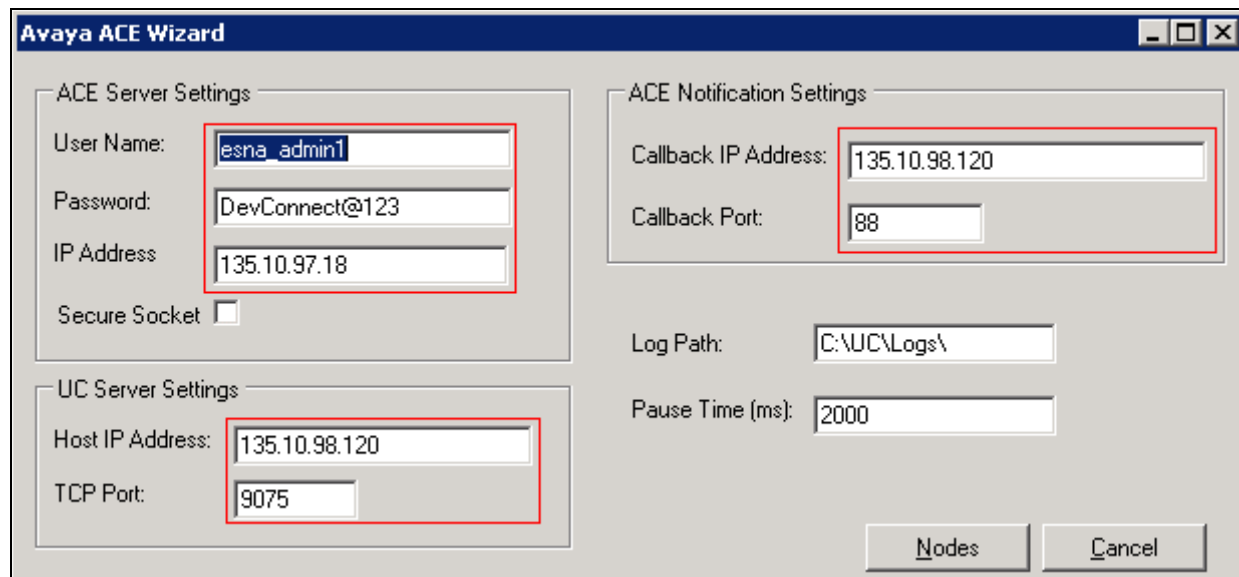
This provides a subscription state line in the message body indicating a subscription state is active, this is required even for unsolicited Notify messages for MWI with Session Manager.

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

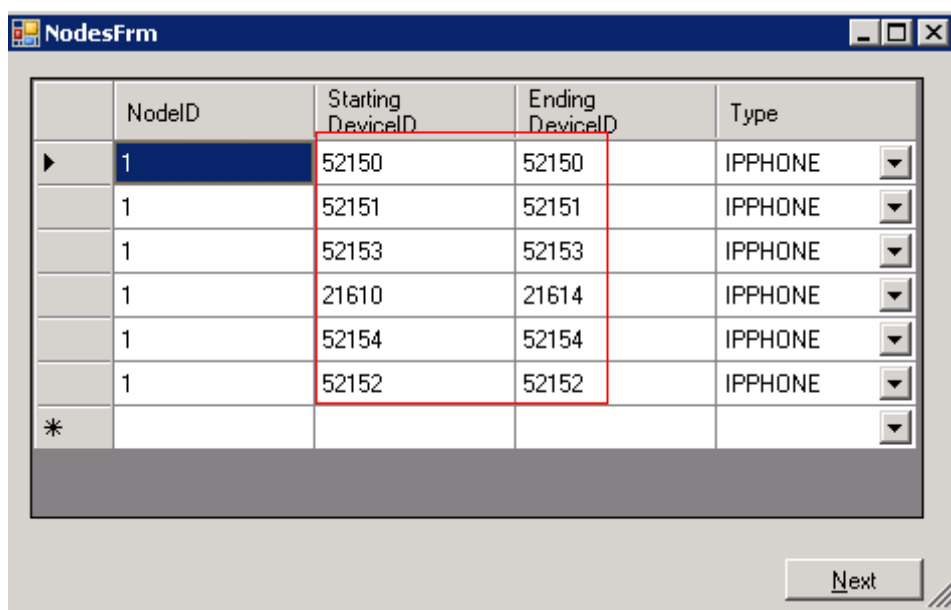


10.2. Configure UC ACE Wizard

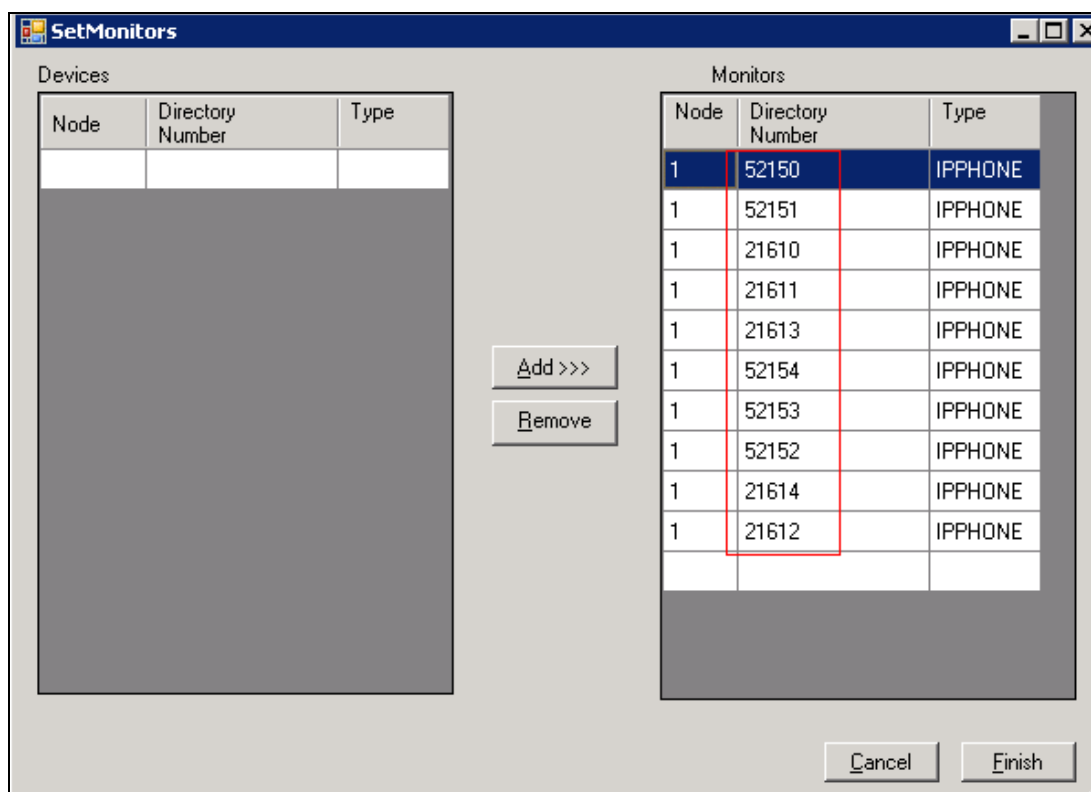
Double click on UC ACE Wizard shortcut to launch the setup window for Avaya ACE Wizard. Enter information as below:



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.



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 – S8300D Communication Manager Release 6** and highlight the **Mailbox Structure**. In the right panel right click on the window, select new to add new mailbox.

| Office-LinX Admin | Name | Number | Feature Group | Personal Operator | Tu... | Current Location | Location Availi... | Capability | Storage Mode | Read Msg | Unread ... | Web Client ... |
|----------------------------------|------------|--------|-----------------|-------------------|-------|------------------|--------------------|--------------|--------------|----------|------------|----------------|
| Avaya - S8300 Communication Mana | Muoi Khong | 21610 | 1:Default Users | | On | In Office | Available | Unified C... | Database | 0 | 6 | Yes |
| Release 6 | Muoi Mot | 21611 | 1:Default Users | | On | In Office | Available | Unified C... | Database | 0 | 1 | Yes |
| Mailbox Structure | Muoi Hai | 21612 | 1:Default Users | | On | In Office | Available | Unified C... | Database | 0 | 1 | Yes |
| Feature Group | Muoi Ba | 21613 | 1:Default Users | | On | In Office | Available | Unified C... | Database | 3 | 1 | Yes |
| Remote Site | Mot Bon | 21614 | 1:Default Users | | On | In Office | Available | Unified C... | Database | 0 | 1 | Yes |
| Routing Table | Nam Khong | 52150 | 1:Default Users | | On | Away on Business | Unavailable | Unified C... | IMAP | 18 | 3 | Yes |
| Voice Menu | Nam Mot | 52151 | 1:Default Users | 52150: Khong ... | On | At Lunch | Available | Unified C... | Database | 0 | 0 | Yes |
| Customize TUI | Nam Hai | 52152 | 1:Default Users | 52150: Khong ... | On | In Office | Available | Unified C... | Database | 5 | 1 | Yes |
| Print Server | Nam Ba | 52153 | 1:Default Users | | On | In Office | Available | Unified C... | Database | 0 | 1 | Yes |
| Fax Jobs | Nam Bon | 52154 | 1:Default Users | | On | In Office | Available | Unified C... | Database | 0 | 1 | Yes |
| Storage | | | | | | | | | | | | |

The screenshot shows the Office-LinX Admin interface. On the left, the tree structure is expanded to 'Avaya - S8300 Communication Manager Release 6' > 'Mailbox Structure'. The right pane displays a list of mailboxes. A 'Mailbox' configuration window is open, showing the configuration for mailbox 52155. The window has tabs for 'General', 'Advanced', 'Mailbox Options', 'Transfer Options', 'Message Options', and 'Notification'. The 'General' tab is active, showing fields for Mailbox Number (52155), Last Name, First Name, Gender, Feature Group (1: Default Users), Organizational Unit, Account Code, Current Default Phone Address (Not defined), Numeric Password, and POP3 / IMAP4 settings (User Name, Password, Confirm Password).

| Name | Number | Feature Group | Personal Operator | Tu... | Current Location |
|------------|--------|-----------------|-------------------|-------|------------------|
| Muoi Khong | 21610 | 1:Default Users | | On | In Office |
| Muoi Mot | 21611 | 1:Default Users | | On | In Office |
| Muoi Hai | 21612 | 1:Default Users | | On | In Office |
| Muoi Ba | 21613 | 1:Default Users | | On | In Office |
| Mot Bon | 21614 | 1:Default Users | | On | In Office |

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

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 Link | Version | Mnt Busy | AE Services Server | Service State | Msgs Sent | Msgs Rcvd |
| 5 | 4 | no | DevAES | established | 15 | 15 |
| 8 | | no | | down | 0 | 0 |




See **Section 6.7** Checking the status of a switch connection from Communication Manager to the 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:** 
- **Service State:** 

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

| <input type="checkbox"/> | Session Manager | Type | Alarms | Tests Pass | Security Module | Service State | Entity Monitoring | Active Call Count | Registrations | Version |
|--------------------------|------------------------|------|-----------------|--|--|--|-------------------|-------------------|---------------|----------------|
| <input type="checkbox"/> | DevASM | Core | 25552/2196/3060 |  |  |  | 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 |  | 200 OK | up |
| » Show | DevASM | 135.10.97.18 | 5060 | TCP |  | 200 OK | up |

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.

| ▼ AE Services | |
|-----------------------------------|--|
| ▶ CVLAN | |
| ▶ DLG | |
| ▶ DMCC | |
| ▶ SMS | |
| ▶ TSAPI | |
| ▶ TWS | |
| ▶ Communication Manager Interface | |
| ▶ Licensing | |
| ▶ Maintenance | |
| ▶ Networking | |
| ▶ Security | |
| ▶ Status | |

AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

| Service | Status | State | License Mode | Cause* |
|-------------------------|---------|---------|--------------|--------|
| ASAI Link Manager | N/A | Running | N/A | N/A |
| CVLAN Service | OFFLINE | Running | N/A | N/A |
| DLG Service | OFFLINE | Running | N/A | N/A |
| DMCC Service | ONLINE | Running | NORMAL MODE | N/A |
| TSAPI Service | ONLINE | Running | NORMAL MODE | N/A |
| Transport Layer Service | N/A | Running | N/A | N/A |

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.

AE Services

Communication Manager Interface

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

Utilities

Help

DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 seconds

Session Summary

Device Summary

Generated on Wed Aug 01 14:18:46 EDT 2012

Service Uptime: 19 days, 20 hours 40 minutes

Number of Active Sessions: 13

Number of Sessions Created Since Service Boot: 192

Number of Existing Devices: 0

Number of Devices Created Since Service Boot: 0

| | Session ID | User | Application | Far-end Identifier | Connection Type | # of Associated Devices |
|--------------------------|--|-----------------------------|-------------|---|--------------------|-------------------------|
| <input type="checkbox"/> | 6EBE0C7045E6F26E6 67CC240AC27A673-2 | sip:+21610@ 135.10.97.62 | ace | TR-87 Encrypted:135.10.97.18:135.10.97.18:016322481807081846 | TR-87 Encrypted | 1 |
| <input type="checkbox"/> | 58B60FBA73E88AD76 257845CFA009E04-3 | sip:+21611@ 135.10.97.62 | ace | TR-87 Encrypted:135.10.97.18:135.10.97.18:7855809904535266 | TR-87 Encrypted | 1 |
| <input type="checkbox"/> | 455314B4831E37CEE F64969AC9ADA97A-9 | sip:+21612@ 135.10.97.62 | ace | TR-87 Encrypted:135.10.97.18:135.10.97.18:9597535979353745 | TR-87 Encrypted | 1 |
| <input type="checkbox"/> | 3D71329E9827BB446 FC57883112B91B8-4 | sip:+21613@ 135.10.97.62 | ace | TR-87 Encrypted:135.10.97.18:135.10.97.18:5717104755239546 | TR-87 Encrypted | 1 |
| <input type="checkbox"/> | 6B141FA6E5D431B83 B37182D2A86B96D-8 | sip:+21614@ 135.10.97.62 | ace | TR-87 Encrypted:135.10.97.18:135.10.97.18:2646755702983494 | TR-87 Encrypted | 1 |
| <input type="checkbox"/> | 1F1B7E1EEE1A2281D 4295A549E3B848F-156 | sip:+52150@ 135.10.97.62 | ace | TR-87 Encrypted:135.10.97.18:135.10.97.18:8021101136221318 | TR-87 Encrypted | 1 |
| <input type="checkbox"/> | 9F70297819D650154 A389120E4D0647D-189 | sip:+52151@ 135.10.97.62 | ace | TR-87 Encrypted:135.10.97.18:135.10.97.18:7021515096377063 | TR-87 Encrypted | 1 |
| <input type="checkbox"/> | 29EEC2C49451E8FEF 915E288E3EF3EDF-118 | sip:+52152@ 135.10.97.62 | ace | TR-87 Encrypted:135.10.97.18:135.10.97.18:11209357261479524 | TR-87 Encrypted | 1 |

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`

```

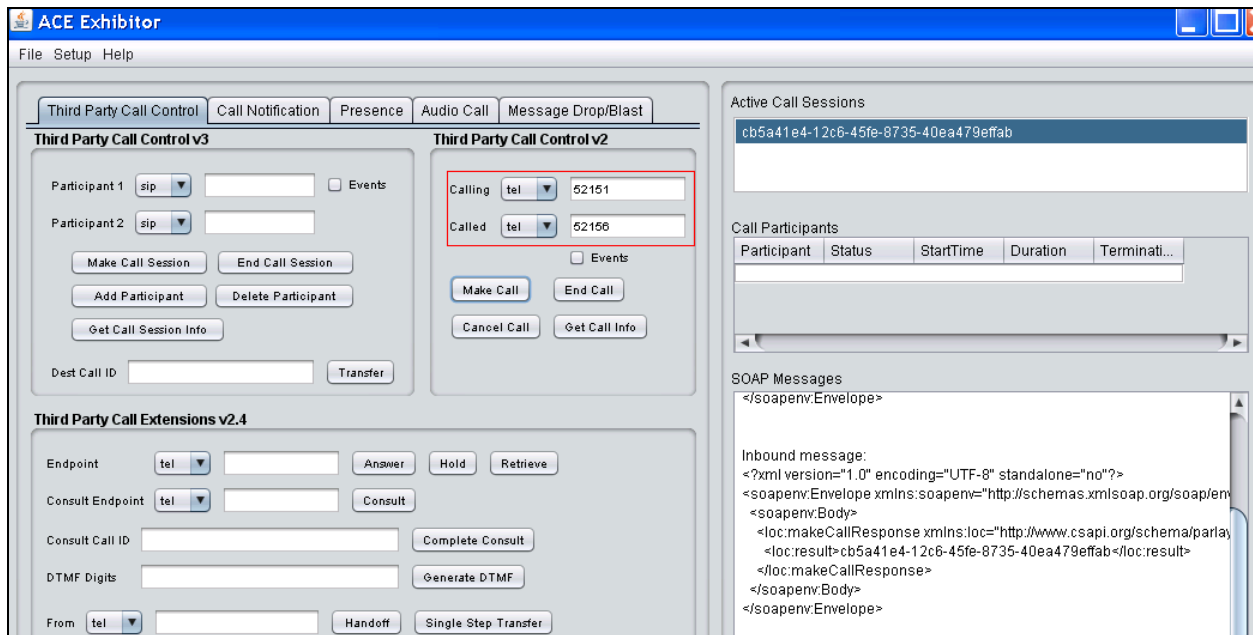
-bash-3.2$ netstat -an | grep 4723
tcp        0      0  ::ffff:127.0.0.1:4723  :::*           LISTEN
tcp        0      0  ::ffff:135.10.97.62:4723  :::*           LISTEN
tcp        0      0  ::ffff:135.10.xx.xx:4723  ::ffff:135.10.xx.xx:60328  ESTABLISHED
-bash-3.2$

```

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`.

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: [06222042890364965@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

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:

| Server | |
|----------------------------|--|
| General | Deployment Licensing Logger Alarm AuditEvent PM Collection |
| Active Server Information | |
| Host name | acesrv.bvwdev.com |
| Fixed IP Address | 135.10.97.18 |
| Service IP Address | 135.10.97.18 |
| Operating System Time | 2012-08-03 00:13:56.198 -0400 |
| Operating System Uptime | 62 days, 53 minutes, 19 seconds, 36 milliseconds |
| Operating System Version | Red Hat Enterprise Linux Server release 5.4 (Tikanga) |
| Application Server Status | RUNNING |
| Application Server Uptime | 21 days, 6 hours, 40 minutes, 19 seconds, 780 milliseconds |
| Application Server Version | 7.0.0.17 [CEA 1.0.0.5 cf051022.02] [ND 7.0.0.17 cf171115.15] |
| ACE Core Information | |
| Application Status | RUNNING |
| Application Uptime | 21 days, 6 hours, 39 minutes, 19 seconds, 103 milliseconds |
| Application Version | 3.0.2 |
| Application Build | ACEREL-CORE-JOB1-18_28055 |
| Application HostType | STANDALONE |
| Associated Information | UNAVAILABLE |

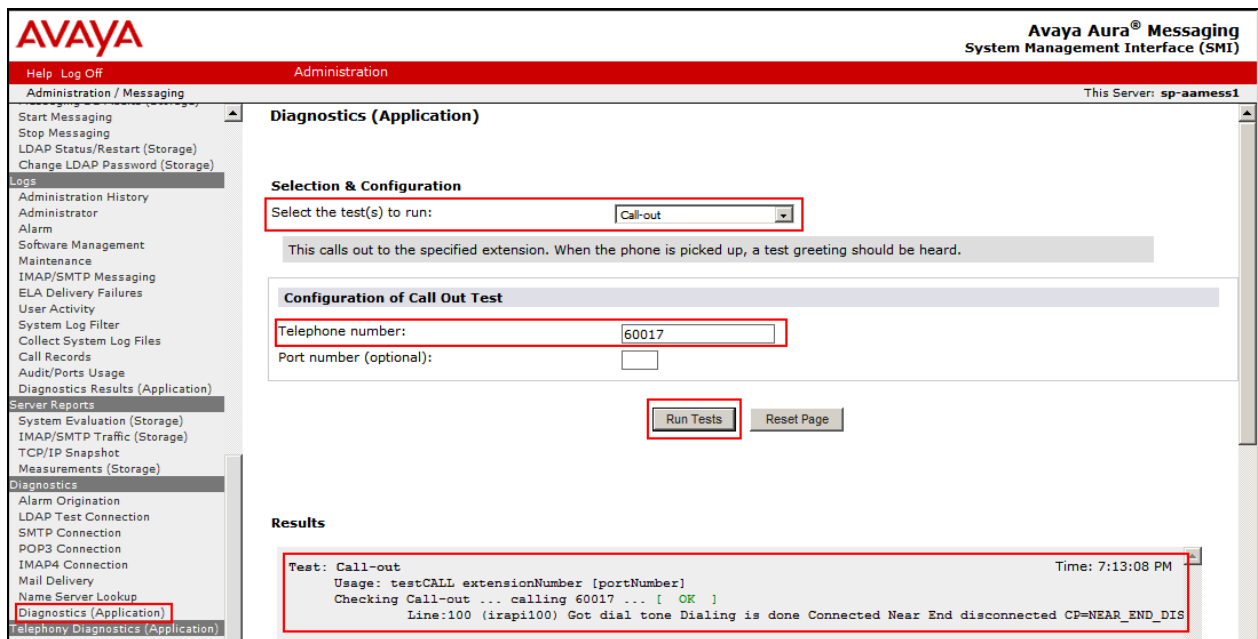
11.5. Verify Avaya Aura Messaging

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.



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.

| Inbox: | | | | |
|--------|-----------------|-----------------|--------------------|-------------|
| | From | Subject | Received | Length/Size |
| | Salesforce C... | Your Daily C... | 2012 Aug 1, 3:32 | 10.5 KB |
| | Salesforce C... | Your Daily C... | 2012 Jul 24, 3:29 | 10.6 KB |
| | support@sale... | We have rece... | 2012 Jul 23, 16:34 | 660bytes |
| | Test User 2 | Test User ha... | 2012 Jul 23, 15:21 | 2.3 KB |
| | Test User 3 | gfdgfdgdf | 2012 Jul 23, 13:59 | 2bytes |
| | Phuong MacNe... | Phuong is no... | 2012 Jul 23, 10:13 | 1.1 KB |
| | Phuong MacNe... | Phuong is no... | 2012 Jul 23, 10:13 | 1.1 KB |
| | support@sale... | Salesforce.c... | 2012 Jul 23, 10:03 | 737bytes |
| | support@sale... | We have rece... | 2012 Jul 23, 10:01 | 770bytes |
| | support@sale... | We have rece... | 2012 Jul 20, 11:58 | 661bytes |
| | support@sale... | We have rece... | 2012 Jul 20, 11:55 | 661bytes |
| | support@sale... | We have rece... | 2012 Jul 20, 11:54 | 661bytes |
| | support@sale... | Your salesfo... | 2012 Jul 20, 11:54 | 545bytes |
| | support@sale... | Salesforce.C... | 2012 Jul 20, 11:18 | 1.1 KB |
| | Avaya Aura M... | Voice Messag... | 2012 Jul 16, 13:01 | 393bytes |
| | Avaya Aura M... | Voice Messag... | 2012 Jul 16, 9:54 | 5.9 KB |
| | Avaya Aura M... | Voice Messag... | 2012 Jul 12, 14:41 | 393bytes |
| | Avaya Aura M... | Voice Messag... | 2012 Jul 12, 12:40 | 393bytes |
| | Avaya Aura M... | Voice Messag... | 2012 Jul 12, 12:37 | 393bytes |
| | Avaya Aura M... | Voice Messag... | 2012 Jul 12, 12:31 | 10.8 KB |



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

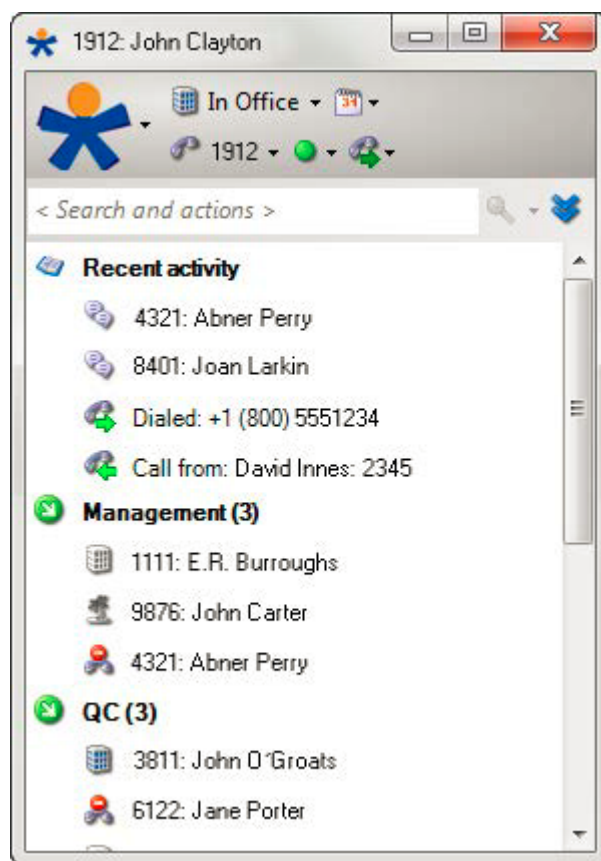
11.6.1. Verify the log file UCServer of ESNA Office-LinX.

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:



12. Conclusion

Interoperability testing of Avaya Agile Communication Environment™, Avaya Aura® Messaging, and Avaya Aura® Communication Manager 6.0 with Office-Linx 8.5 SP2 – UC Client Manager was successful. Observations are noted in **Section 2.2**.

13. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, June 2010, Release 6.0, Document Number 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 Intergration 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

©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.