



## Avaya Solution & Interoperability Test Lab

---

# **Application Notes for Configuring the ESNA Office-LinX™ Cloudlink™ Edition UC Client Manager Google Gadget with Avaya Agile Communication Environment™, Avaya Aura Messaging® and Avaya Aura® Communication Manager 5.2 - 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 Google Gadget 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

<b>1. INTRODUCTION</b>	<b>6</b>
<b>2. GENERAL TEST APPROACH AND TEST RESULT</b>	<b>6</b>
2.1. Interoperability Compliance Testing	6
2.2. Test Results	6
2.3. Support	7
<b>3. REFERENCE CONFIGURATION</b>	<b>8</b>
<b>4. EQUIPMENT AND SOFTWARE VALIDATED</b>	<b>9</b>
<b>5. CONFIGURE AVAYA AURA® COMMUNICATION MANAGER</b>	<b>9</b>
5.1. Configure SIP trunk between Avaya Communication Manager and Session Manager	9
5.1.1. Capacity Verification	10
5.1.2. IP Codec Set	10
5.1.3. Configure IP Network Region	11
5.1.4. Configure IP Node Name	12
5.1.5. Configure SIP Signaling	12
5.1.6. Configure Trunk Group	13
5.1.7. Configure Route Pattern	14
5.1.8. Administer Dialplan	14
5.1.9. Administering an extension number for the station that an Office LinX application monitors	15
5.1.10. Configure Hunt Group for Avaya Aura Messaging	16
5.1.11. Configure Coverage Path to Avaya Aura Messaging	17
5.1.12. Administer a Station for Coverage to Avaya Aura Messaging	17
5.1.13. Configure Hunt Group for ESNA Office-LinX	18
5.1.14. Configure Coverage Path to ESNA Office-LinX	19
5.2. Configure CTI link between Communication Manager and AE Server	19
5.2.1. Verify license	20
5.2.2. Enable Processor Ethernet	20
5.2.3. Enable AE Services change ip-services.	21
5.2.4. Add a CTI link	22
5.2.5. Method for adding DMCC Softphone to the network region	22
5.2.6. Administer media gateway	23
5.2.7. Verify a media processor circuit pack	23
<b>6. CONFIGURE AE SERVER</b>	<b>24</b>
6.1. Verify Device and Media Call Control API Station licenses	24
6.2. Configure Switch Connection: Add switch, edit IP, H323 Gatekeeper	26

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	31
<b>7.</b>	<b>CONFIGURE AVAYA AURA® MESSAGING</b>	<b>31</b>
7.1.	Administer Sites	32
7.2.	Administer Telephony Integration	33
7.3.	Configure Dial Rules	34
7.4.	Configure Class of Service	35
7.5.	Administer Subscribers	36
7.6.	Administer Topology	38
7.7.	Administer External Host	39
7.8.	Configure Notify Me	40
<b>8.</b>	<b>CONFIGURE AVAYA AURA® SESSION MANAGER</b>	<b>40</b>
8.1.	Configure SIP Domain	40
8.2.	Configure Locations	41
8.3.	Configure SIP Entities	42
8.4.	Configure Entity Links	43
8.5.	Time Ranges	44
8.6.	Configure Routing Policy	45
8.7.	Dial Patterns	45
8.8.	Configure Managed Elements	Error! Bookmark not defined.
8.9.	Configure Applications	Error! Bookmark not defined.
8.10.	Define Application Sequence	Error! Bookmark not defined.

<b>8.11.</b>	<b>Synchronization Changes with Avaya Aura® Communication Manager</b>	<b>46</b>
<b>9.</b>	<b>CONFIGURE AVAYA ACE 3.0</b>	<b>47</b>
<b>9.1.</b>	<b>Administer certificate</b>	<b>48</b>
9.1.1.	Creating a directory for the OpenSSL CA files	48
9.1.2.	Creating an OpenSSL configuration file	49
9.1.3.	Generating a CA certificate	49
9.1.4.	Create a server certificate request for AE Services	50
9.1.5.	Creating the ACE certificate request	52
9.1.6.	Signing an AES certificate request	52
9.1.7.	Signing an ACE certificate request	53
9.1.8.	Importing the server certificate into AE Services	53
9.1.9.	Add Trusted Host	56
<b>9.2.</b>	<b>Certificate management using the IBM Integrated Solutions Console for ACE on Linux</b>	<b>56</b>
9.2.1.	Creating a key store using the IBM Integrated Solutions Console	57
9.2.2.	Export ACE server cert	60
9.2.3.	Administer Keystore	60
9.2.4.	Restart Avaya ACE and AE server	63
<b>9.3.</b>	<b>Add Service Provider</b>	<b>64</b>
9.3.1.	Add AE server provider using TR87 service	64
9.3.2.	Add Session Manager as a service provider in Avaya ACE	66
<b>9.4.</b>	<b>Add user</b>	<b>67</b>
<b>9.5.</b>	<b>Add Translation rule to Service Provider</b>	<b>68</b>
<b>10.</b>	<b>CONFIGURE THE ESNA TELEPHONY OFFICE-LINX</b>	<b>69</b>
<b>10.1.</b>	<b>Configure SIP Configuration Tool</b>	<b>69</b>
<b>10.2.</b>	<b>Configure UC ACE Wizard</b>	<b>73</b>
<b>10.3.</b>	<b>Message Synchronization</b>	<b>75</b>
10.3.1.	TSE IMAP Configuration	75
<b>10.4.</b>	<b>Configure user mailbox in Office-LinX Admin</b>	<b>76</b>
<b>10.5.</b>	<b>Configure mailbox to be synchronized with a Google App IMAP account</b>	<b>77</b>
<b>10.6.</b>	<b>Feature Group</b>	<b>78</b>
<b>10.7.</b>	<b>Synchronization through OAuth (superuser)</b>	<b>79</b>
10.7.1.	Configuring OAuth	79
<b>10.8.</b>	<b>Install and Configure UC Client Google Gadget on Gmail</b>	<b>81</b>
<b>11.</b>	<b>VERIFICATION STEPS</b>	<b>83</b>

<b>11.1.</b>	<b>Verify Avaya Aura® Communication Manager</b>	<b>83</b>
<b>11.2.</b>	<b>Verify Avaya Aura® Session Manager</b>	<b>84</b>
11.2.1.	Verify Avaya Aura® Session Manager is Operational	84
11.2.2.	Verify SIP Entity Link Status	84
<b>11.3.</b>	<b>Verify Avaya Aura® Application Enablement Server</b>	<b>85</b>
11.3.1.	Verify Services are running.	85
11.3.2.	Verify DMCC Service Summary – Session Summary	85
11.3.3.	Verify AE Server and Avaya ACE are Communicating	86
11.3.4.	Verify AE Server and Switch are talking	87
<b>11.4.</b>	<b>Verify Avaya Aura® Avaya ACE</b>	<b>88</b>
11.4.1.	Verify Service Provider status in Avaya ACE	88
11.4.2.	Verify Avaya ACE Server status	88
<b>11.5.</b>	<b>Verify Avaya Aura Messaging</b>	<b>88</b>
11.5.1.	Verify Avaya Aura Messaging can make a call to phones	88
11.5.2.	Verify user can receive and retrieve Avaya Aura Messaging voice message on ESNA Web Client or Google Mail account	89
<b>11.6.</b>	<b>Verify ESNA Office-LinX server and UC Client Google gadget.</b>	<b>90</b>
11.6.1.	Verify the log file UCServer of ESNA Office-LinX.	90
11.6.2.	Verify User can make a call using UC Client Google Gadget in the Gmail	90
<b>12.</b>	<b>CONCLUSION</b>	<b>91</b>
<b>13.</b>	<b>ADDITIONAL REFERENCES</b>	<b>91</b>

# 1. Introduction

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

The Telephony Office-LinX™ Cloudlink™ Edition UC Client Manager Google Gadget 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 Google gadget and the voice path is established on 2 physical phones.
- Put a call on hold and retrieve call.
- Transfer a call.
- Retrieve the voice message from AAM in Gmail account (SMTP replay).
- Leave messages for subscribers and retrieve the message through the web client.
- Message Waiting Indication (MWI).
- DTMF using the voicemail.

- G.711MU and G.711A codec's.

The following was observed during testing:

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

### 2.3. Support

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

- URL – [techsupport@esna.com](mailto:techsupport@esna.com)
- Phone – (905) 707-1234

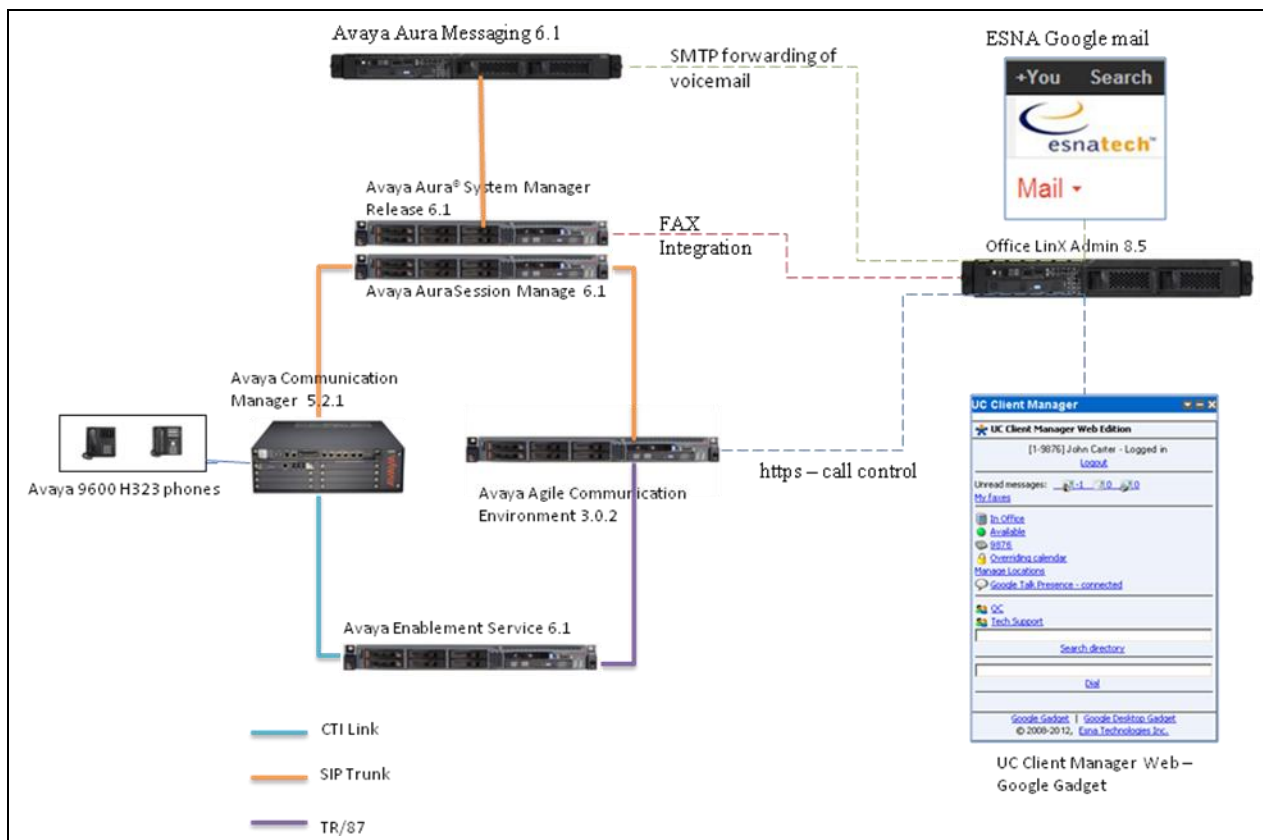
### 3. Reference Configuration

**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 H.323 Telephones.

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

A user is able to click and call through the UC Client Manager Google gadget as well as received notify message from Avaya Aura Messaging on their ESNA Gmail account.

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 5.2.1 with latest Service Pack
Avaya Aura® System Manager S8800 Server	Avaya Aura® System Manager 6.1
Avaya Aura® Session Manager S8800 Server	Avaya Aura® Session Manager 6.1
Avaya Aura® Messaging S8800 Server	Avaya Aura® Messaging 6.1
Avaya Aura® Application Enablement Services S8800 Server	Avaya Aura® Application Enablement Services 6.1
Avaya Agile Communication Environment™	3.0.2
Avaya 9600 H323 Phone	6.2
ESNA Telephony Office-LinX	8.5 SP2
UC Client Manager Google Gadget	8.5 SP2
ESNA Gmail Account	test2@esnasolutions.com

## 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 the IP network region to specify which codec sets may be used within and between network regions.

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

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

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

                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.711MU      n           2          20
2: G.711A      n           2          20
3:
Media Encryption
1: none
```

### 5.1.3. Configure IP Network Region

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

- **Authoritative Domain** – Enter the appropriate name for the Authoritative Domain. During the compliance test, the authoritative domain is set to **bvwdev.com**. This should match the SIP Domain value on Session Manager, in **Section 8.1**.
- **Codec Set** – Set the codec set number as provisioned in **Section 5.1.2**.

```
change ip-network-region 1                               Page 1 of 20

                                IP NETWORK REGION

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

#### 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 **bvwdev.com**. This should match the SIP Domain value in **Section 8.1**.
- **Direct IP-IP Audio Connections** – Set to **y**, since the shuffling is enabled during the compliance test

add signaling-group 5		SIGNALING GROUP
Group Number: 5	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		SIP Enabled LSP? n
IP Video? n		Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: DevASM	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain: bvwdev.com		
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
Dial Access? n Night Service:
Queue Length: 0
Service Type: tie Auth Code? n
Member Assignment Method: auto
Signaling Group: 5
Number of Members: 20
```

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

```
add trunk-group 5                                     Page 3 of 21
                                     TRUNK FEATURES
ACA Assignment? n Measured: none
Maintenance Tests? y
Numbering Format: unk-pvt
UUI Treatment: service-provider
Replace Restricted Numbers? n
Replace Unavailable Numbers? n
Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y
```

### 5.1.7. Configure Route Pattern

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

add route-pattern 5															Page 1 of 3						
Pattern Number: 5															Pattern Name: IMS SIP trunk						
SCCAN? n															Secure SIP? n						
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted								DCS/	IXC					
No			Mrk	Lmt	List	Del	Digits								QSIG						
Dgts															Intw						
1: 5 0															n	user					
2:															n	user					
3:															n	user					
4:															n	user					
5:															n	user					
6:															n	user					
BCC VALUE															TSC	CA-TSC	ITC BCIE Service/Feature PARM			No. Numbering	LAR
0 1 2 M 4 W															Request					Dgts Format	
																		Subaddress			
1: y y y y y n n															rest			lev0-pvt	none		
2: y y y y y n n															rest				none		
3: y y y y y n n															rest				none		
4: y y y y y n n															rest				none		
5: y y y y y n n															rest				none		
6: y y y y y n n															rest				none		

### 5.1.8. Administer Dialplan

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

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

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

display dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 3		
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call
String	Length	Type	String	Length	Type	String	Length	Type
1	3	dac	8	1	fac			
5300	5	ext	9	1	fac			
399	5	ext	*	4	dac			
216	5	ext						

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
```

UNIFORM DIAL PLAN TABLE						
			Page 1 of 2		Percent Full: 0	
Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node Num
399	5	0		aar	n	
5300	5	0		aar	n	
216	5	0		aar	n	

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

display aar analysis 0

Page 1 of 2

AAR DIGIT ANALYSIS TABLE

Location: all

Percent Full: 3

Dialed 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
216	5	5	5	aar		n

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

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

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

change station 21613		Page 1 of 5
STATION		
Extension: 21613	Lock Messages? n	BCC: 0
Type: 9630	Security Code: 1234	TN: 1
Port: S00028	Coverage Path 1: 5	COR: 1
Name: Mot Ba	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 21613	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Button Modules: 0	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Customizable Labels? y	

### 5.1.10. Configure Hunt Group for Avaya Aura Messaging

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

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

Add hunt-group 2		Page 1 of 60
HUNT GROUP		
Group Number: 1	ACD? n	
Group Name: Messaging	Queue? n	
Group Extension: 39991	Vector? n	
Group Type: ucd-mia	Coverage Path:	
TN: 1	Night Service Destination:	
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		

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

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

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



### 5.1.11. Configure Coverage Path to Avaya Aura Messaging

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

```
add coverage path 2                                     Page 1 of 1

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

COVERAGE CRITERIA
  Station/Group Status   Inside   Outside Call
    Active?              n         n
    Busy?                y         y
    Don't Answer?        y         y      Number of Rings: 2
    All?                 n         n
  DND/SAC/Goto Cover?    y         y
  Holiday Coverage?      n         n

COVERAGE POINTS
  Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h2           Rng: 2   Point2:
  Point3:              Point4:
```

### 5.1.12. Administer a Station for Coverage to Avaya Aura Messaging

Configure any and all phones that have a mailbox on the messaging server for call coverage. Use the command **change station xyz** and on **Page1** for **Coverage Path 1** use the coverage path defined in **Section 5.1.11** in the example below station 21613 was configured to cover to messaging using cover path 2.

```
change station 21613                                     Page 1 of 5

                                STATION
                                Extension: 21613
                                Type: 9630
                                Port: S00024
                                Name: Nam Mot
                                Lock Messages? n
                                Security Code: 1234
                                Coverage Path 1: 2
                                Coverage Path 2:
                                Hunt-to Station:
                                BCC: 0
                                TN: 1
                                COR: 1
                                COS: 1

STATION OPTIONS
  Loss Group: 19
  Speakerphone: 2-way
  Display Language: english
  Survivable GK Node Name:
  Survivable COR: internal
  Survivable Trunk Dest? y
  Time of Day Lock Table:
  Personalized Ringing Pattern: 1
  Message Lamp Ext: 52151
  Mute Button Enabled? y
  Button Modules: 0
  Media Complex Ext:
  IP SoftPhone? y
  IP Video Softphone? n
  Customizable Labels? y
```

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

change station 21613		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced	Audible Message Waiting? n	
<b>MWI Served User Type: sip-adjunct</b>	Display Client Redirection? n	
	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? n	
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 21613	Always Use? n IP Audio Hairpinning? n	

### 5.1.13. Configure Hunt Group for ESNA Office-LinX

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

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

Add hunt-group 1		Page 1 of 60
HUNT GROUP		
Group Number: 1	ACD? n	
<b>Group Name: ESNA</b>	Queue? n	
<b>Group Extension: 53001</b>	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

#### 5.1.14. Configure Coverage Path to ESNA Office-LinX

This section describes the steps for administering coverage path in Communication Manager. Enter the **add coverage path <s>** command, where **s** is a valid coverage path number. The Point1 value of **h1** is used to represent the hunt group number 1. The default values for the other fields may be used.

add coverage path 1		Page 1 of 1
COVERAGE PATH		
Coverage Path Number: 1		
Cvg Enabled for VDN Route-To Party? n	Hunt after Coverage? n	
Next Path Number:	Linkage	
COVERAGE CRITERIA		
Station/Group Status	Inside	Outside Call
Active?	n	n
Busy?	y	y
Don't Answer?	y	y
All?	n	n
DND/SAC/Goto Cover?	y	y
Holiday Coverage?	n	n
COVERAGE POINTS		
Terminate to Coverage Pts. with Bridged Appearances? n		
Point1: h1	Rng: 2	Point2:
Point3:		Point4:

#### 5.2. Configure CTI link between Communication Manager and AE Server

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

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

### 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** or “**display ip-interface procr**” if it is existed.

add ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: PROCR	Target socket load: 4800	
Enable Interface? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr		
Subnet Mask: /26		

### 5.2.3. Enable AE Services change ip-services.

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

Complete Page 1 of the IP SERVICES form as follows:

- 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	Local Port	Remote Node	Remote Port	
AESVCS	y	procr	8765			

Complete Page 3 of the IP SERVICES form as follows

In the **AE Services Server** field, type the name of the AE Server, for example: DevAES.

change ip-services					Page 3 of 3
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	DevAES	aespassword	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.
- 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	CTI LINK	Page 1 of 3
CTI Link: 5		
Extension: 21613		
Type: ADJ-IP		
Name: DevEAS		COR: 1

#### 5.2.5. Method for adding DMCC Softphone to the network region

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

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

### 5.2.6. Administer media gateway

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

```
display media-gateway 1

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

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

Max Survivable IP Ext: 8
```

#### Note:

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

### 5.2.7. Verify a media processor circuit pack

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

```
change node-names ip

IP NODE NAMES
Name      IP Address
DevAES    135.10.97.xx
DevASM    135.10.97.1xx
procr     135.10.xx.x
procr6    ::

Page 1 of 2
```

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

```
list ip-interface all

IP INTERFACES

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

## 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.
- Add TSAPI link.

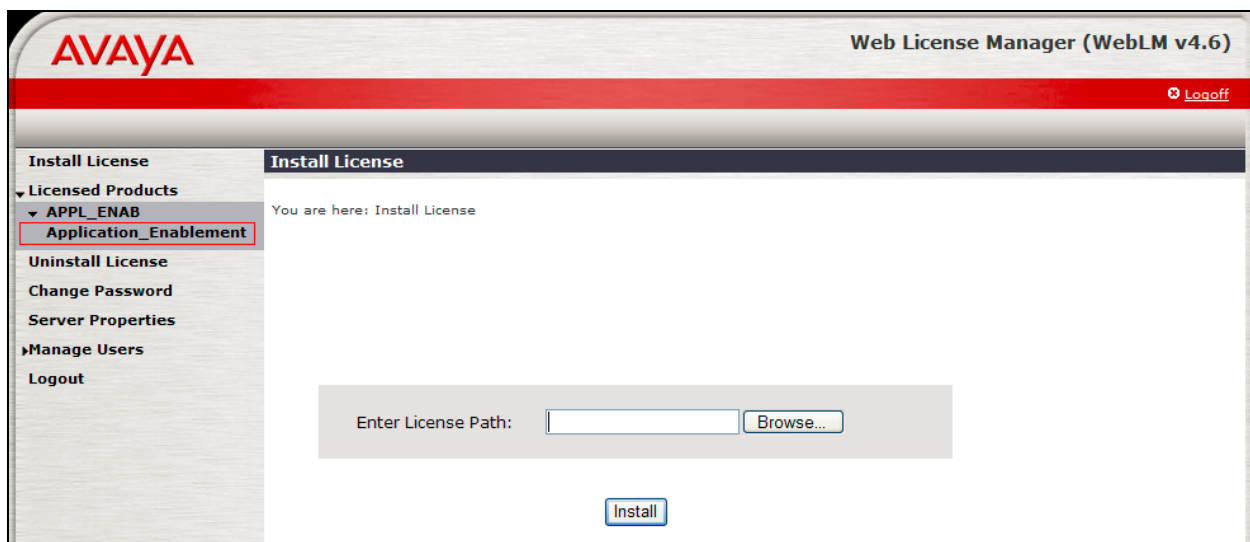
### 6.1. Verify Device and Media Call Control API Station licenses

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;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;d1380g3;d1385g1;d1385g2;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 shows 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". On the left is a sidebar menu with options like "AE Services", "Communication Manager Interface", "Switch Connections", "Dial Plan", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "Switch Connections" and features a text input field with "S8300D" and an "Add Connection" button. Below this is a table with columns: "Connection Name", "Processor Ethernet", "Msg Period", and "Number of Active Connections". The table contains one entry: "G650" with "No" for Processor Ethernet, "30" for Msg Period, and "0" for Number of Active Connections. Below the table are buttons for "Edit Connection", "Edit PE/CLAN IPs", "Edit H.323 Gatekeeper", "Delete Connection", and "Survivability Hierarchy".

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

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**.

The screenshot shows the "Connection Details - S8300D" window. It has a sidebar menu on the left with "Switch Connections" selected. The main area contains fields for "Switch Password" and "Confirm Switch Password", both masked with dots. Below these are fields for "Msg Period" (set to 30) and "SSL" (checked). There are also checkboxes for "Processor Ethernet" and "H.323 Gatekeeper", both of which are checked. At the bottom are "Apply" and "Cancel" buttons.

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

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

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.

<b>▼ Networking</b> AE Service IP (Local IP) Network Configure <b>Ports</b> TCP Settings <b>► Security</b> <b>► Status</b> <b>► User Management</b> <b>► Utilities</b> <b>► Help</b>		<table border="1"> <tr> <td>Encrypted TCP Port</td> <td>9998</td> <td><input checked="" type="radio"/> <input type="radio"/></td> </tr> <tr> <td>DLG Port</td> <td>TCP Port</td> <td>5678</td> </tr> <tr> <td colspan="3">TSAPI Ports</td> </tr> <tr> <td>TSAPI Service Port</td> <td>450</td> <td><input checked="" type="radio"/> <input type="radio"/></td> </tr> <tr> <td colspan="3">Local TLINK Ports</td> </tr> <tr> <td>TCP Port Min</td> <td>1024</td> <td></td> </tr> <tr> <td>TCP Port Max</td> <td>1039</td> <td></td> </tr> <tr> <td colspan="3">Unencrypted TLINK Ports</td> </tr> <tr> <td>TCP Port Min</td> <td>1050</td> <td></td> </tr> <tr> <td>TCP Port Max</td> <td>1065</td> <td></td> </tr> <tr> <td colspan="3">Encrypted TLINK Ports</td> </tr> <tr> <td>TCP Port Min</td> <td>1066</td> <td></td> </tr> <tr> <td>TCP Port Max</td> <td>1081</td> <td></td> </tr> <tr> <td colspan="3">DMCC Server Ports</td> </tr> <tr> <td>Unencrypted Port</td> <td>4721</td> <td><input checked="" type="radio"/> <input type="radio"/></td> </tr> <tr> <td>Encrypted Port</td> <td>4722</td> <td><input checked="" type="radio"/> <input type="radio"/></td> </tr> <tr> <td>TR/87 Port</td> <td>4723</td> <td><input checked="" type="radio"/> <input type="radio"/></td> </tr> </table>	Encrypted TCP Port	9998	<input checked="" type="radio"/> <input type="radio"/>	DLG Port	TCP Port	5678	TSAPI Ports			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	1050		TCP Port Max	1065		Encrypted TLINK Ports			TCP Port Min	1066		TCP Port Max	1081		DMCC Server Ports			Unencrypted Port	4721	<input checked="" type="radio"/> <input type="radio"/>	Encrypted Port	4722	<input checked="" type="radio"/> <input type="radio"/>	TR/87 Port	4723	<input checked="" type="radio"/> <input type="radio"/>
Encrypted TCP Port	9998	<input checked="" type="radio"/> <input type="radio"/>																																																			
DLG Port	TCP Port	5678																																																			
TSAPI Ports																																																					
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	1050																																																				
TCP Port Max	1065																																																				
Encrypted TLINK Ports																																																					
TCP Port Min	1066																																																				
TCP Port Max	1081																																																				
DMCC Server Ports																																																					
Unencrypted Port	4721	<input checked="" type="radio"/> <input type="radio"/>																																																			
Encrypted Port	4722	<input checked="" type="radio"/> <input type="radio"/>																																																			
TR/87 Port	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.

<b>► AE Services</b> Communication Manager Interface Licensing Maintenance Networking <b>▼ Security</b> Account Management Audit Certificate Management Enterprise Directory <b>▼ Host AA</b> Trusted Hosts <b>Service Settings</b>	<h3>Service Settings</h3> <table border="1"> <tr> <th>Services</th> <th>Authenticate Client Cert with Trusted Certs</th> <th>Require Trusted Host Entry</th> </tr> <tr> <td>TR/87</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>DMCC</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </table> <p> <input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/> </p>	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"/>
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

**From TelURI**

Pattern Type Pattern ▼

Minimum Length 5

Maximum Length 5

Matching Pattern tel: + 216

Delete Length 0

Replacement String

Apply Changes Cancel Changes

Detail configuration of To TelURI using during compliance test

**To TelURI**

Pattern Type Pattern ▼

Minimum Length 5

Maximum Length 5

Matching Pattern 216

Delete Length 0

Replacement String tel: +

Apply Changes Cancel Changes

## 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 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](#)

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

Once you have added a switch connection on the AE Server, you validate the switch connection by checking its status on both the AE Server and on Communication Manager.

To check the status of a switch connection on Communication Manager, type `status aesvcs link`.

```
status aesvcs link
```

AE SERVICES LINK STATUS						
Srvr/	AE Services	Remote IP	Remote	Local Node	Msgs	Msgs
Link	Server		Port		Sent	Rcvd
01/01	DevAES	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**.

Switch Connections Summary

☐ Enable page refresh every 60 seconds

	Switch Conn	Conn State	Processor Ethernet	Since	Online/Offline	Active/Standby/Admin'd AEP Conns	Num of TCI Conns	SSL	Msgs To Switch	Msgs From Switch	Msg Period
<input checked="" type="radio"/>	CM450Rls5	Talking	Yes	Fri Jun 8 11:52:02 2012	Online	1 / 0 / 1	1	Enabled	615	630	30
<input type="radio"/>	DevCM3link	Talking	Yes	Thu Jun 7 10:50:12 2012	Online	1 / 0 / 1	2	Enabled	616	628	30

## 7. Configure Avaya Aura® Messaging

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

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

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

## 7.1. Administer Sites

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

Under **Main Properties**:

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

Sites detail screen on AAM show Messaging access number

**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: 39995

Additional sites included in the directory: ☐ Default ☐ WindstreamSonus

Keypad entry: BASIC

Speech recognition: ☒ enabled ☐ disabled

Save Cancel

## 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**

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
Default	Active
<b>Phuong</b>	<b>Active</b>
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](mailto: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
- 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.



Routing \* Home

Home / Elements / Routing / Domains-

Domain Management

1 Item Refresh Filter: Enable

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

\* Input Required

Commit Cancel

## 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

At the top right of the form, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

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.

Entity Links

1 Item | Refresh

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* DevASM_DevAAM_S	* DevASM	TCP	* 5060	* DevAAM_SM	* 5060	<input checked="" type="checkbox"/>	

\* Input Required

Commit Cancel

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.

Time Ranges

Edit New Duplicate Delete More Actions

1 Item | Refresh

	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	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

## 8.6. Configure Routing Policy

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

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

### General section

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

### SIP Entity as Destination section

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

### Time of Day section

- Leave default values.

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

**Routing Policy Details** [Commit] [Cancel]

**General**

\* Name:

Disabled: ☐

Notes:

**SIP Entity as Destination**

Name	FQDN or IP Address	Type	Notes
ESNA	135.10. .	Other	For Office Linx Testing

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.

- 216x – Communication Manager 5.2 extension
- 53000 – ESNA pilot number

- 39990 – Avaya Aura Messaging Pilot Number.

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

#### General section

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

#### Originating Locations and Routing Policies section

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

Click the **Commit** button to save the new definition. The following screen shows the dial pattern used for Communication Manager 5.2 during the compliance test.

**Dial Pattern Details**

**General**

\* Pattern: 216

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: bwvdev.com

Notes: Dialing Plan for CM5.2.1 to ACE

**Originating Locations and Routing Policies**

Add Remove


1 Item Refresh

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	Belleville	Belleville DevConnect lab	ACE_to_CM5.2.1	0	<input type="checkbox"/>	CM_G450

## 8.8. Synchronization Changes with Avaya Aura® Communication Manager

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

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"/>	<a href="#">CM2 Rel-6_G450</a>	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"/>	<a href="#">CM_G450_Instance</a>	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"/>	<a href="#">DevCM</a>	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"/>	<a href="#">DevCM3</a>	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"/>	<a href="#">Select row 4   e-devmes-cm</a>	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

## 9. Configure Avaya ACE 3.0

This section provides information on how to manage certificates for Avaya 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 ACEc
a.crt -config openssl.conf
Generating a 1024 bit RSA private key
..+++++
.....+++++
writing new private key to 'ACEca.private.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

#### 9.1.4. Create a server certificate request for AE Services

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

**AVAYA** Application Enablement Services Management Console

Welcome: User admin  
Last login: Thu Sep 28 13:24:13 2011 from 133.20.117.222  
HostName/IP: scalab136.aceott.avaya.com 133.20.245.136  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-0-20-0

**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 comma 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:**

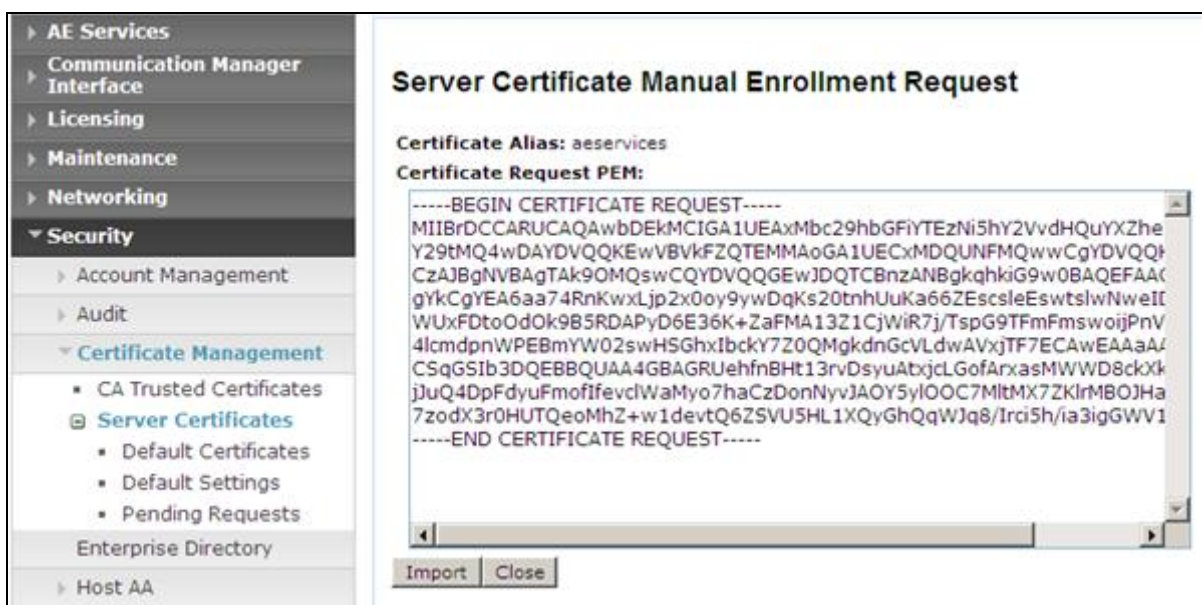
☐ SSL/TLS Web Server Authentication  
☐ SSL/TLS Web Client Authentication  
☐ Code signing  
☐ Email Protection (S/MIME)

**SCEP Parameters:**

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

The hostname is often the FQDN but check

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

```
root@ace1:~/CA2
-----BEGIN CERTIFICATE REQUEST-----
MIIBrDCCARUCAQAwbDEkMCIGA1UEAxMbc29hbGFiYTEzNi5hY2VvdHQuYXZheWEu
Y29tMQ4wDAYDVQQKEwVBVkfZQTEMMaGA1UECxMDQUNFMQwwCgYDVQQHEwNPVFQx
CzAJBgNVBAGTAk9OMQswCQYDVQQGEwJDQTCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYKCGYEA6aa74RnKwLjp2x0oy9ywDqKs20tnhUuKa66ZEscsleEswtswNweIDj
WUxFDtoOdOk9B5RDAPyD6E36K+ZaFMA13Z1CjWiR7j/TspG9TFmFmswoijPnVpKR
4lcmdpnWPEBmYW02swHSGhxIbckY7Z0QMgkdnGcVLdwAVxjTF7ECAwEAAaAAMAOG
CSqGSIb3DQEBBQUAA4GBAGRUehfnBHt13rvDsyuAtxjclGofArxasMWWd8ckXk1m
jJuQ4DpFdyuFmofIfevclWaMyo7haCzDonNyyJA0Y5y1OOC7MltMX7ZKlrMBOJHa
7zodX3r0HUTQeoMhZ+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 a  
ce.req -config openssl.conf  
Generating a 1024 bit RSA private key  
.....+++++  
.....+++++  
writing new private key to 'ace.private.key'  
-----  
[root@ace1 CA2]#
```

### 9.1.6. Signing an AES certificate request

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

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

```
[root@ace1 CA2]# openssl x509 -req -in aes.req -out aes.crt -CA AESca.crt -CAkey  
AESca.private.key -days 500 -extfile openssl.conf -extensions usr_cert -CAcreat  
eserial  
Signature ok  
subject=/CN=soalabal36.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:

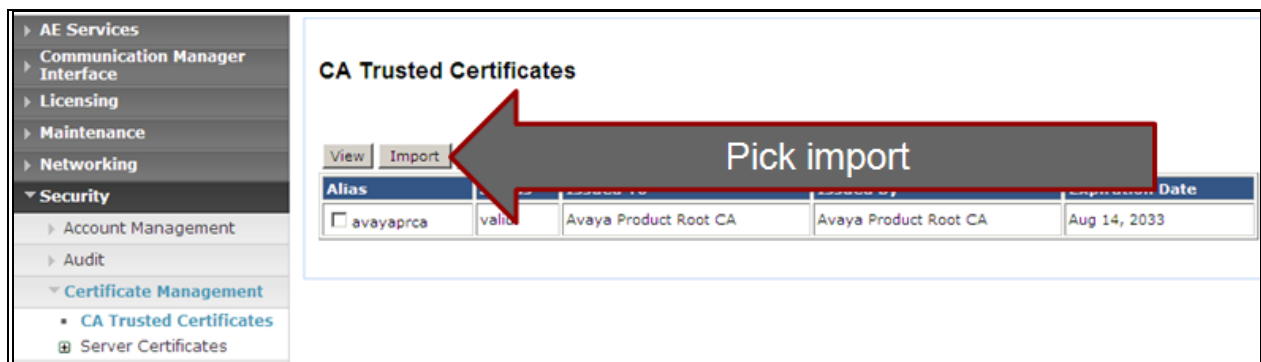
```
openssl x509 -req -in ace.req -out ace.crt -CA ACEca.crt -CAkey ACEca.private.key -days 500 -extfile openssl.conf -extensions usr_cert -CAcreateserial
```

```
[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]#
```

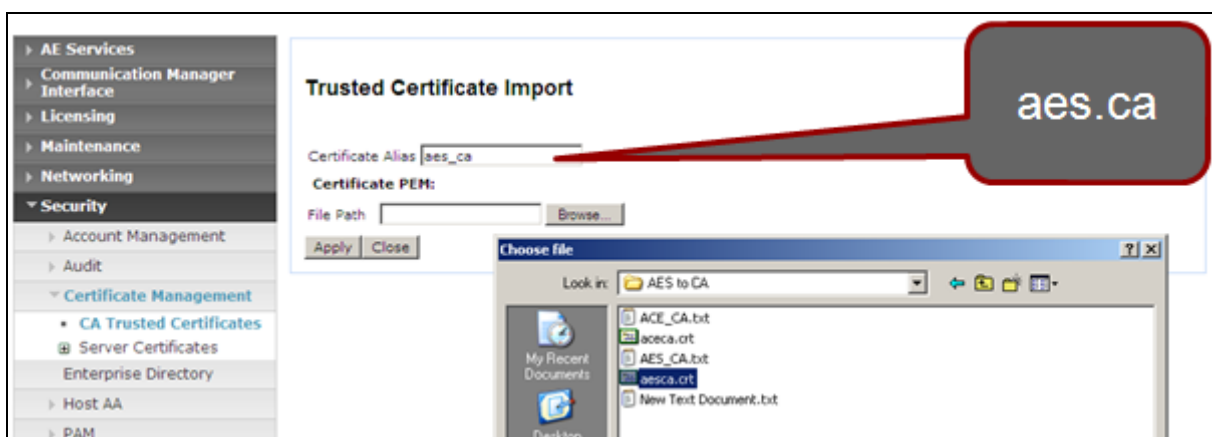
Download the certificate to your AE Services administrative workstation, and save it with a unique name, for example C:\CA\ACEca.crt

### 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 aesca.crt



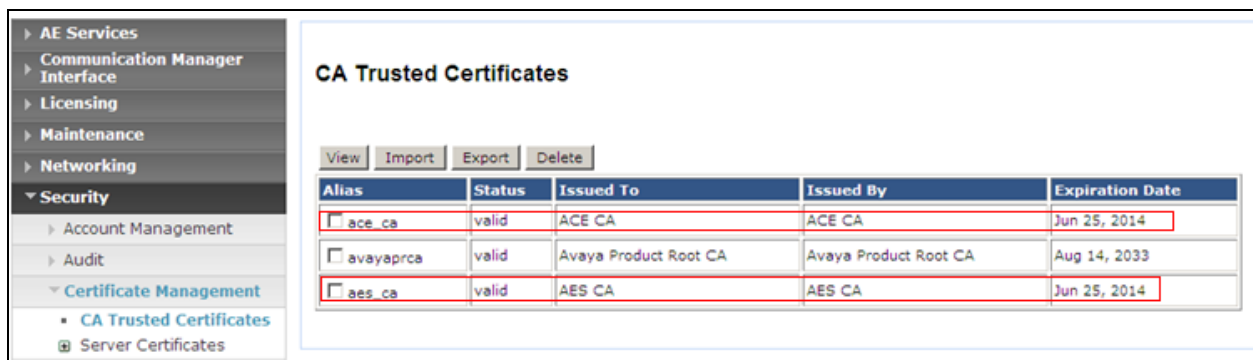
Ensure the cert is imported successfully.



The image shows a web interface for 'Trusted Certificate Import'. On the left is a navigation menu with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, and Enterprise Directory. Under Security, there are sub-items: Account Management, Audit, Certificate Management, CA Trusted Certificates, and Server Certificates. The main panel is titled 'Trusted Certificate Import' and contains a green message box that says 'Certificate imported successfully.'. Below this, there is a 'Certificate Alias' field with the value 'aes\_ca', a 'Certificate PEM' section with a 'File Path' field and a 'Browse...' button, and 'Apply' and 'Close' buttons at the bottom.

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.



The image shows the 'CA Trusted Certificates' page. It has a navigation menu on the left similar to the previous screenshot. The main panel is titled 'CA Trusted Certificates' and has buttons for 'View', 'Import', 'Export', and 'Delete'. Below these buttons is a table with the following data:

Alias	Status	Issued To	Issued By	Expiration Date
<input type="checkbox"/> ace_ca	valid	ACE CA	ACE CA	Jun 25, 2014
<input type="checkbox"/> avayaprca	valid	Avaya Product Root CA	Avaya Product Root CA	Aug 14, 2033
<input type="checkbox"/> aes_ca	valid	AES CA	AES CA	Jun 25, 2014

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



The image shows the 'Pending Server Certificate Requests' page. The navigation menu on the left is expanded to show 'Server Certificates' and 'Pending Requests'. The main panel is titled 'Pending Server Certificate Requests' and has a 'Manual Enroll' button. Below the button is a table with the following data:

Alias	Request Date
<input checked="" type="checkbox"/> aceservices	Thu Sep 29 2011 19:00:40

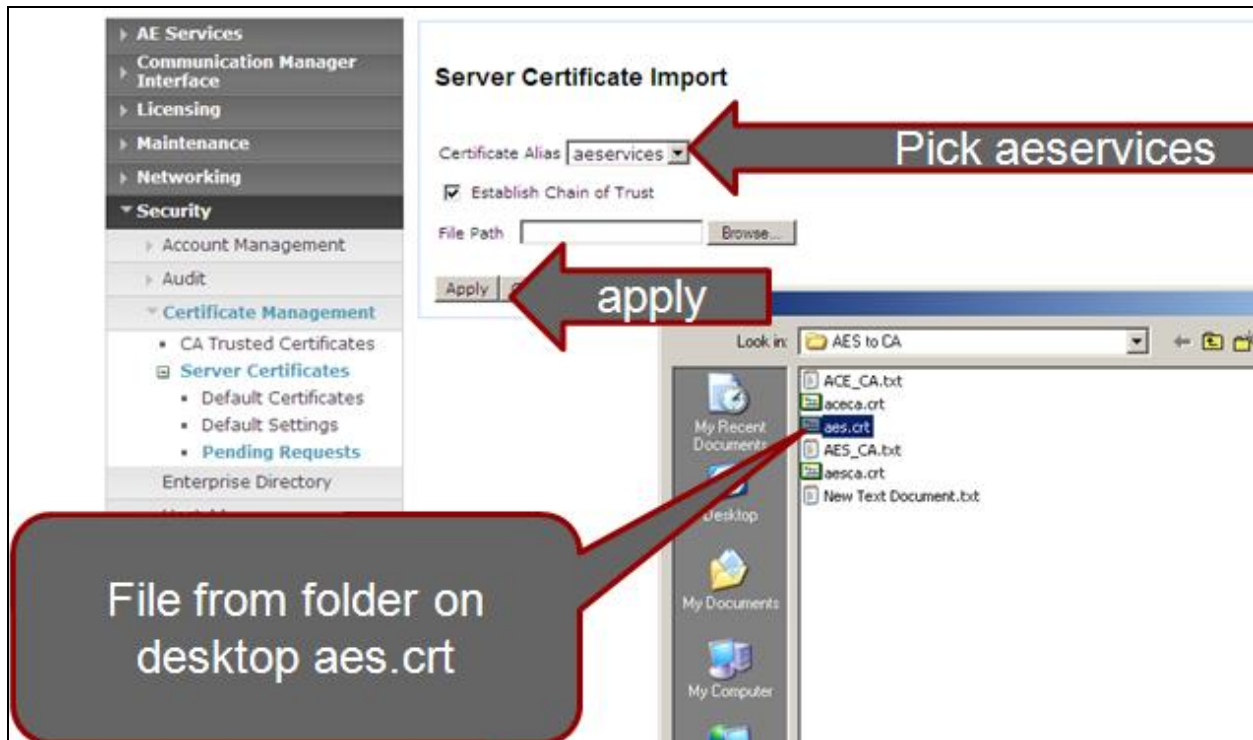
Two red arrows are overlaid on the image. One arrow points from the text 'Pick manual enroll' to the 'Manual Enroll' button. The other arrow points from the same text to the 'aceservices' entry in the table.



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

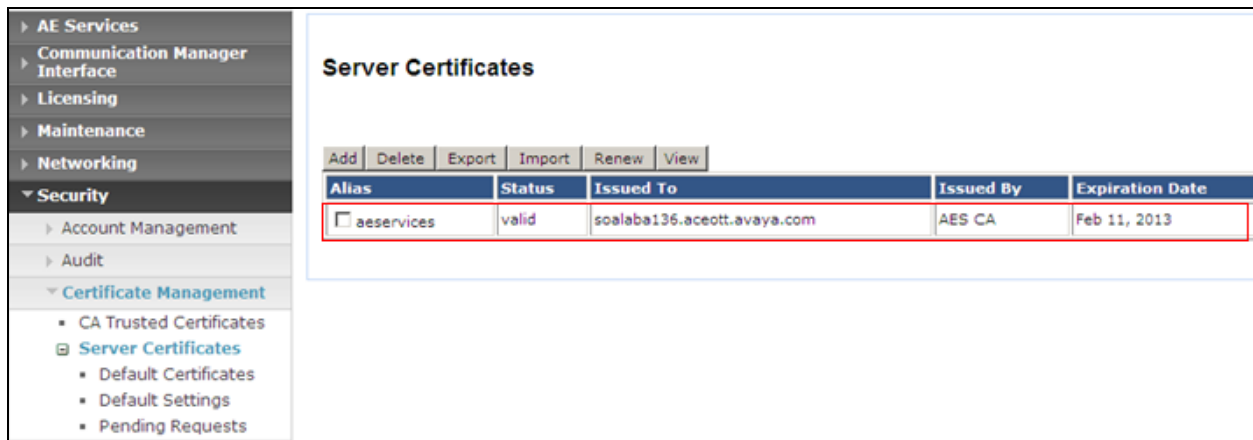
Download the certificate to your AE Services administrative workstation, and save it with a unique name, for example C:\CA\aes.crt

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 SubAltName.

Note: to verify ACE FQDN, in ACE putty type host name

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

**Add Trusted Host**

Certificate CN or SubAltName: ace1.gmiott.avaya.com

Service Type\*: All

User Authentication Policy\*: Not Required

User Authorization Policy\*: Unrestricted Host

Apply Changes Cancel Changes

The "All" Service Type can be used to specify a user authorization policy for both the DMCC and TR/S7 services. The TR/S7 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

Add Edit Delete

\* 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:

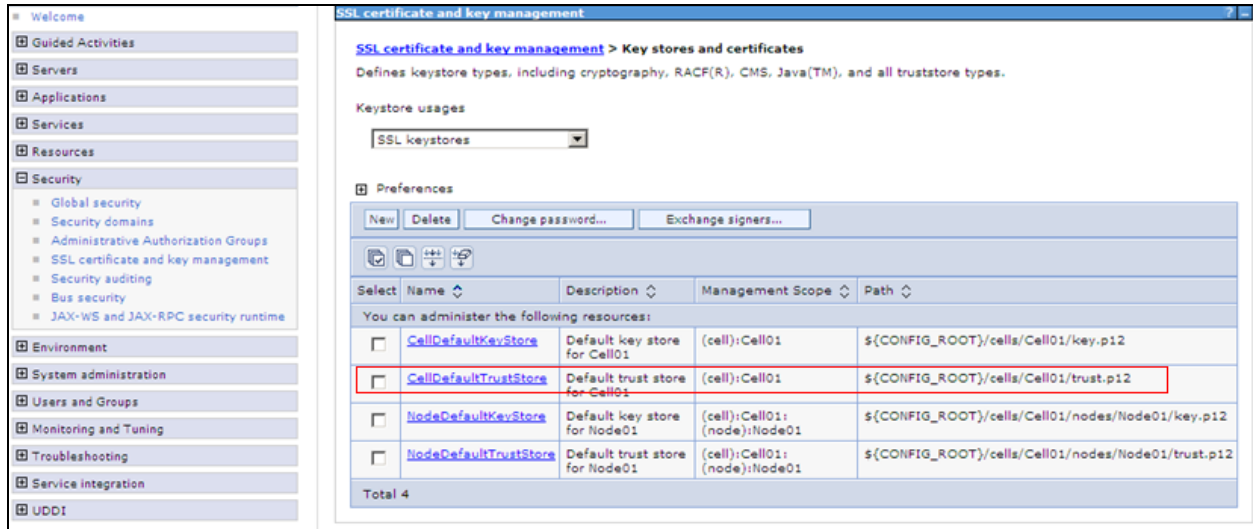
[http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?S\\_TACT=105AGX10&S\\_CMP=LP](http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?S_TACT=105AGX10&S_CMP=LP).



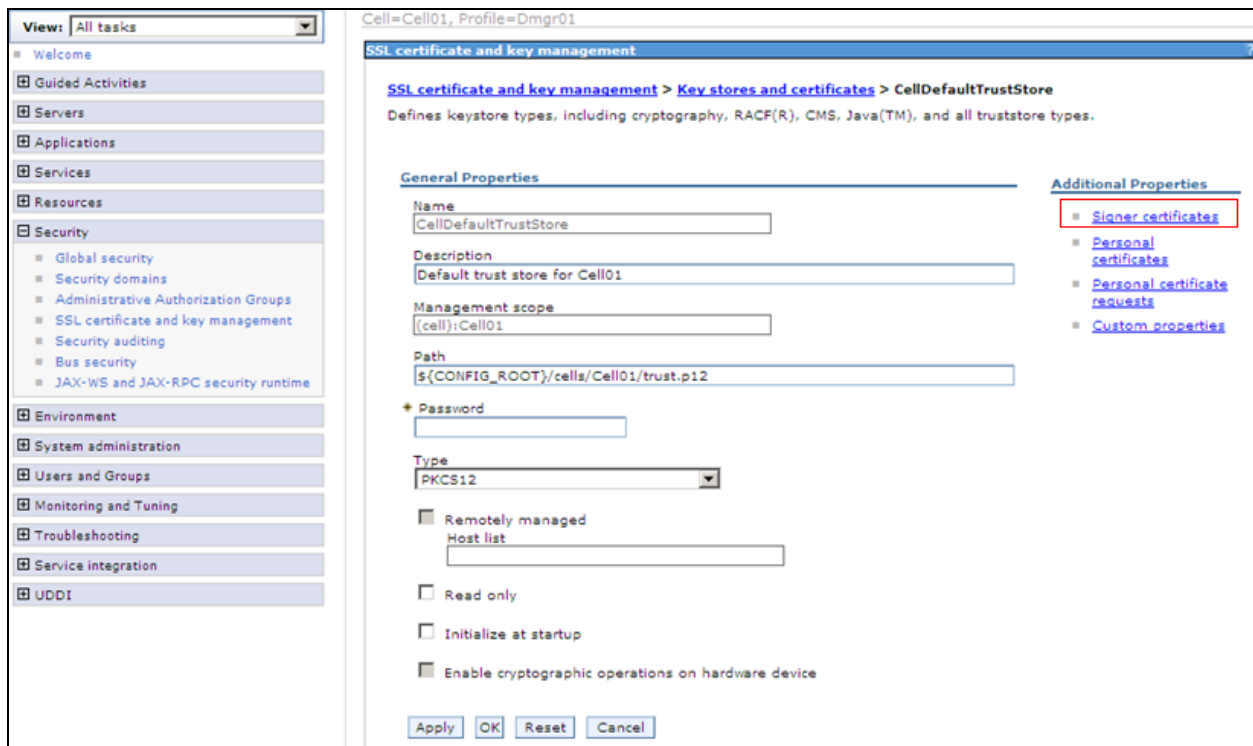
Open web browser and go to ACE WAS admin page <https://<ACEipaddress>:9043/admin>

### 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  
aes\_ca

\* File name  
/root/CA2/AESca.crt

Data type  
Base64-encoded ASCII data ▼

Apply OK Reset Cancel

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.

Make sure to Save

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

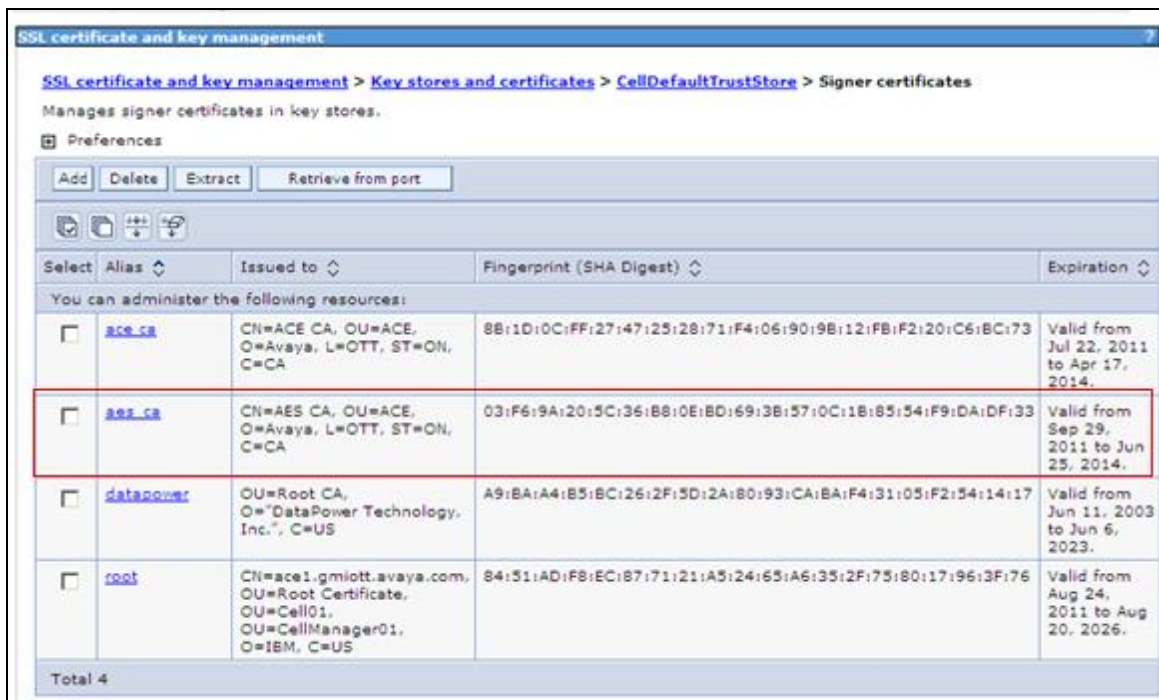
Manages signer certificates in key stores.

#### General Properties

Alias	aes_ca
Version	3
Key size	1024
Serial number	16928843064874124727
Validity period	Valid from Sep 29, 2011 to Jun 25, 2014.
Issued to	CN=AES CA, OU=ACE, O=Avaya, L=OTT, ST=ON, C=CA
Issued by	CN=AES CA, OU=ACE, O=Avaya, L=OTT, ST=ON, C=CA
Fingerprint (SHA digest)	03:F6:9A:20:5C:36:B8:0E:BD:69:3B:57:0C:1B:85:54:F9:DA:DF:33
Signature algorithm	SHA1withRSA(1.2.840.113549.1.1.5)

Back

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) Get key store aliases

Key store password

☒ Key store file

\* Key file name

Type

\* Key file password  
 Get Key File Aliases

Certificate alias to import

Imported certificate alias

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"/>	<a href="#">ACESpecific</a>	(cell):Cell01
<input type="checkbox"/>	<a href="#">CellDefaultSSLSettings</a>	(cell):Cell01
<input type="checkbox"/>	<a href="#">NodeDefaultSSLSettings</a>	(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](#)

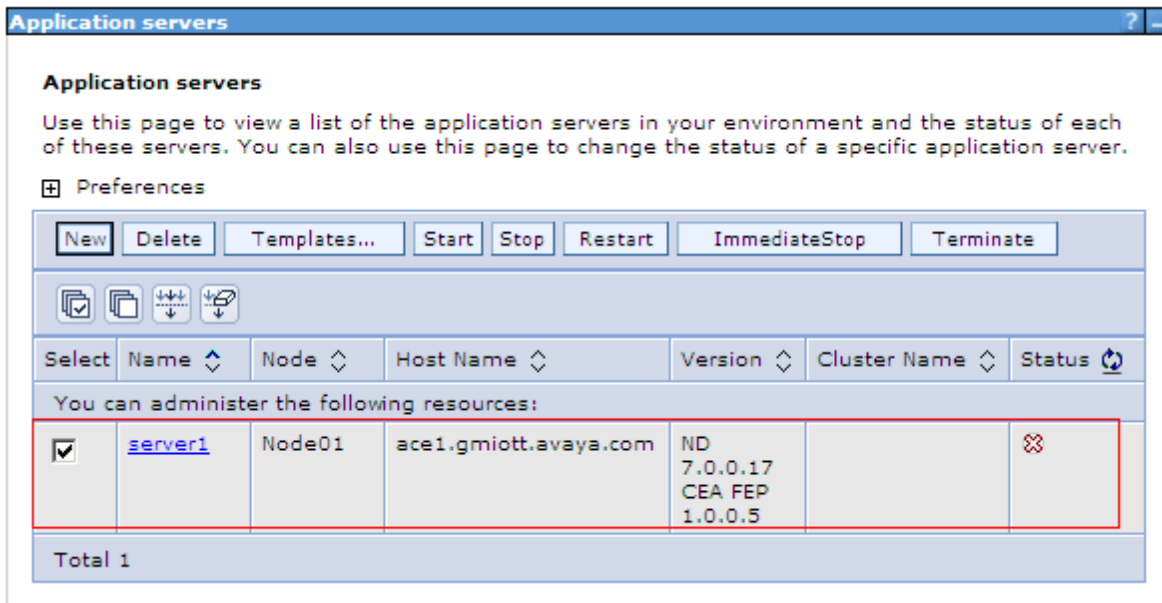
**Related Items**

- [Key stores and certificates](#)

Make sure to click **Save**.

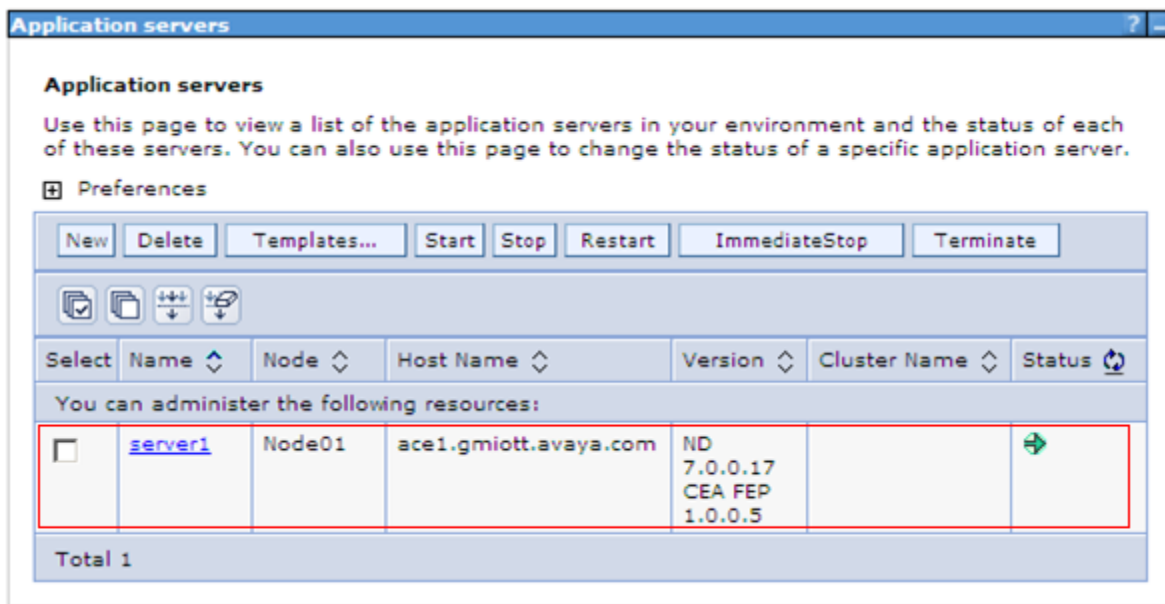
#### 9.2.4. Restart Avaya ACE and AE server

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).

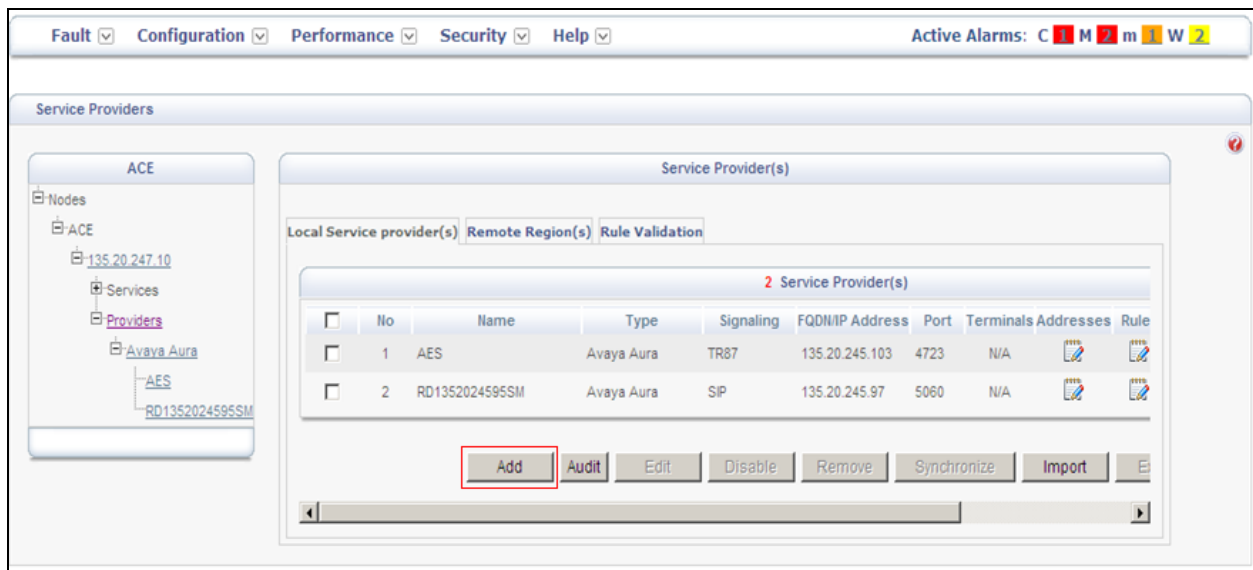
Go to ACE IBM Integrated Solution Console and start ACE by select **Servers** → **WebSphere Application Server** and select **Start**. Verify the server status is back and indicated with a green arrow.



### 9.3. Add Service Provider

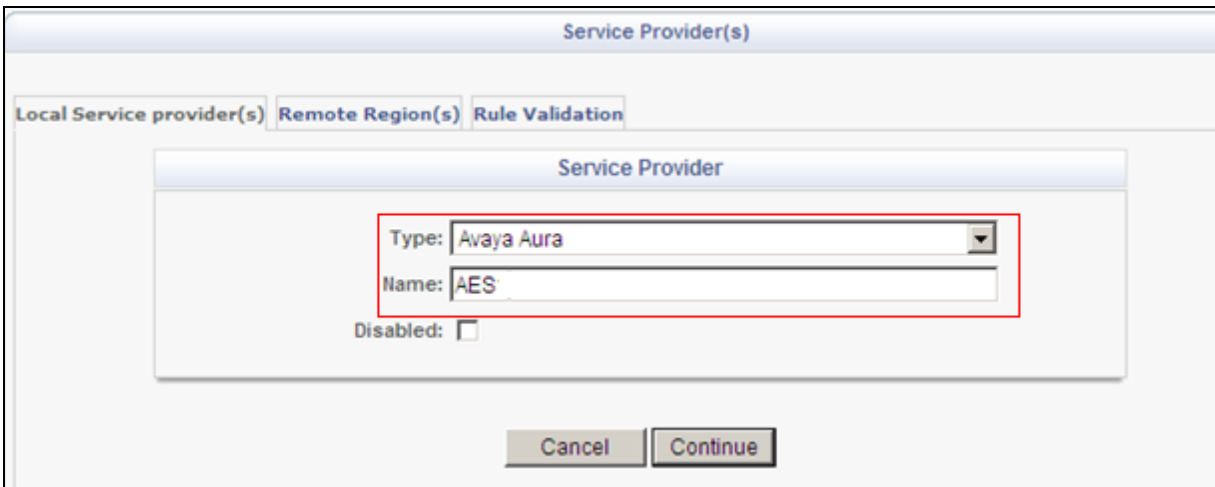
#### 9.3.1. Add AE server provider using TR87 service

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 field is a 'Disabled' checkbox, which is unchecked. At the bottom of the window are 'Cancel' and 'Continue' buttons.

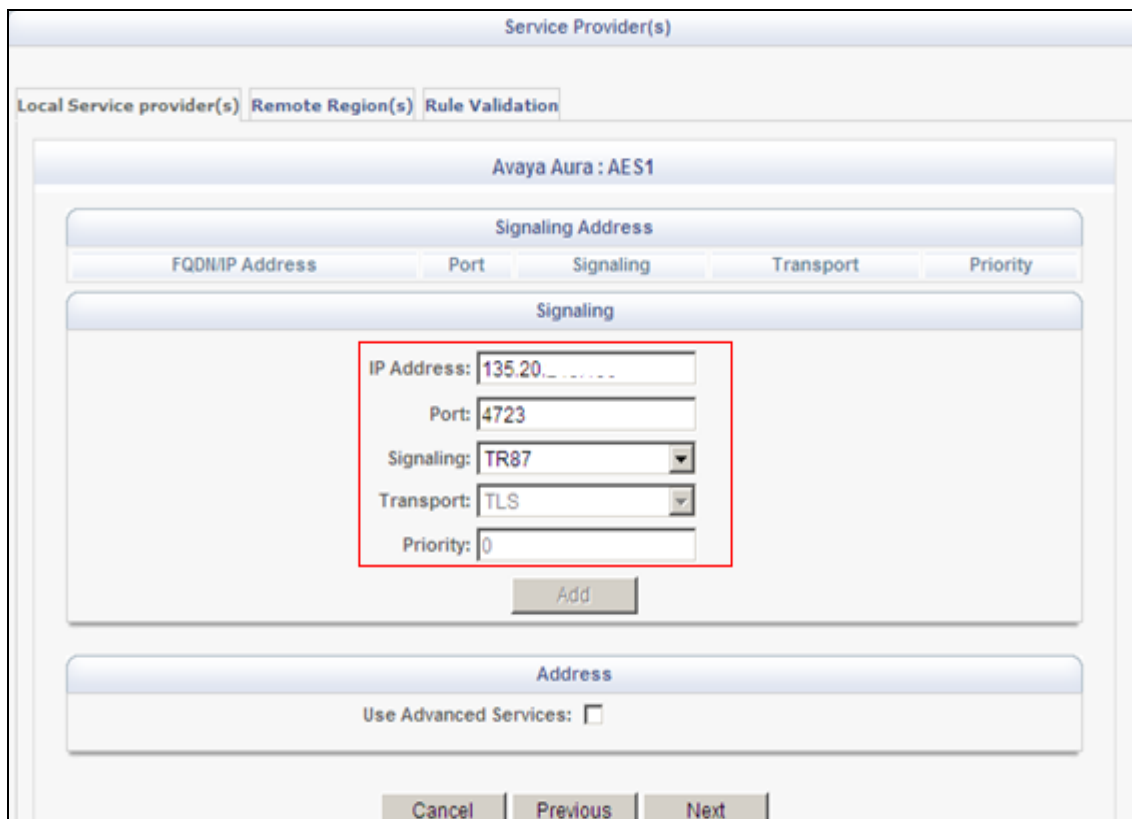
Click **Continue**

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

**Port:** 4723

**Signalling:** select 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 the 'IP Address', 'Port', 'Signaling', and 'Transport' fields. Below the 'Signaling' sub-window 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 of addresses for 'Avaya Aura : DevAES 1'. The table has columns: No, Name, Type, Display Name, URI, and Terminals. One entry is shown with No '1', Name 'thirdPartyCallController', Type 'Route', Display Name empty, URI 'sip:AppCore@bvwdev.com', and Terminals 'N/A'. Below the table is the 'Address Details' form. It contains: 'Type' dropdown set to 'Route', 'Name' dropdown set to 'thirdPartyCallController', 'Display Name' text box empty, 'URI' text box containing 'sip:AppCore@bvwdev.com', and 'Terminals' text box empty. At the bottom are buttons: 'Done', 'Add', 'Modify', 'Remove', and 'Reset'.

No	Name	Type	Display Name	URI	Terminals
1	thirdPartyCallController	Route		sip:AppCore@bvwdev.com	N/A

**Address Details**

Type: Route

Name: thirdPartyCallController

Display Name:

URI: sip:AppCore@bvwdev.com

Terminals:

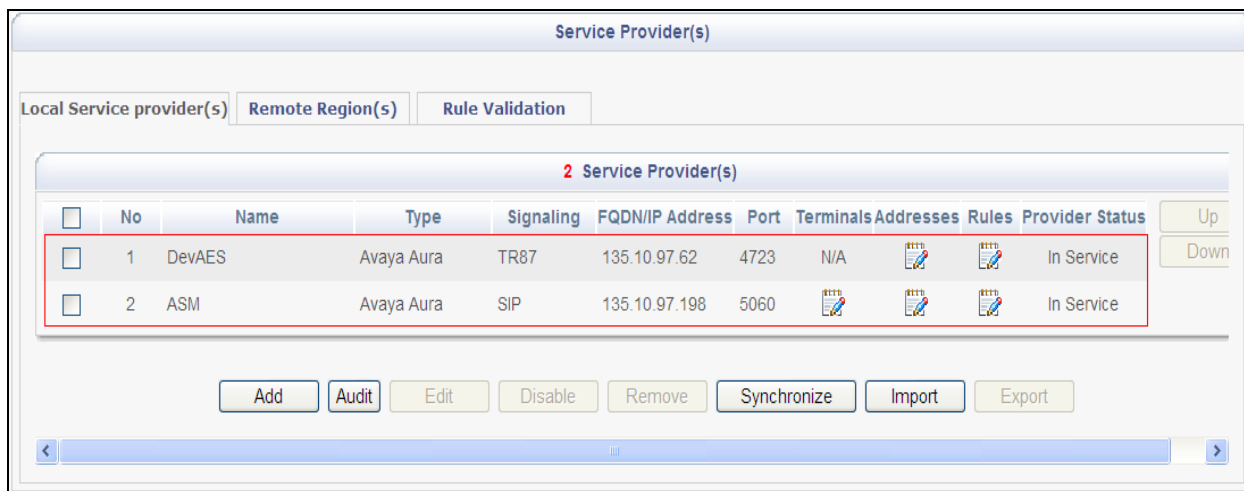
Done Add Modify Remove Reset

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:



No	Name	Type	Signaling	FQDN/IP Address	Port	Terminals	Addresses	Rules	Provider Status
1	DevAES	Avaya Aura	TR87	135.10.97.62	4723	N/A			In Service
2	ASM	Avaya Aura	SIP	135.10.97.198	5060				In Service

#### 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.

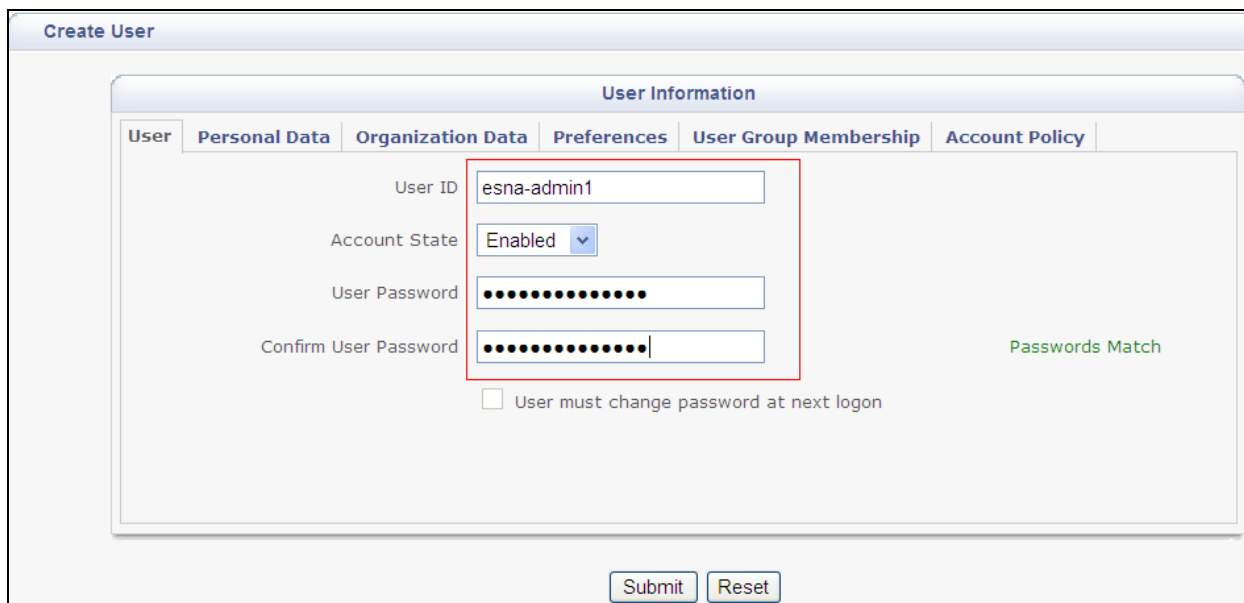
This section will setup a user belong to System Admin Group used by ESNA Office-LinX – Avaya ACE Wizard.

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 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

Available User Groups

- ESNA User
- FederationGroup
- SystemMonitorGroup

Member User Groups

- ESNA Admin
- SystemAdminGroup

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.

Service Provider(s)

Local Service provider(s) Remote Region(s) Rule Validation

Translation Rule for Service Provider -- Avaya Aura : DevAES

Calling Party Translation Rule

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

Up Down Remove

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

**Service Provider(s)**

Local Service provider(s) Remote Region(s) Rule Validation

**Translation Rule for Service Provider -- Avaya Aura : DevAES**

**Called Party Translation Rule**

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,InsertDi git=+,	No	Yes

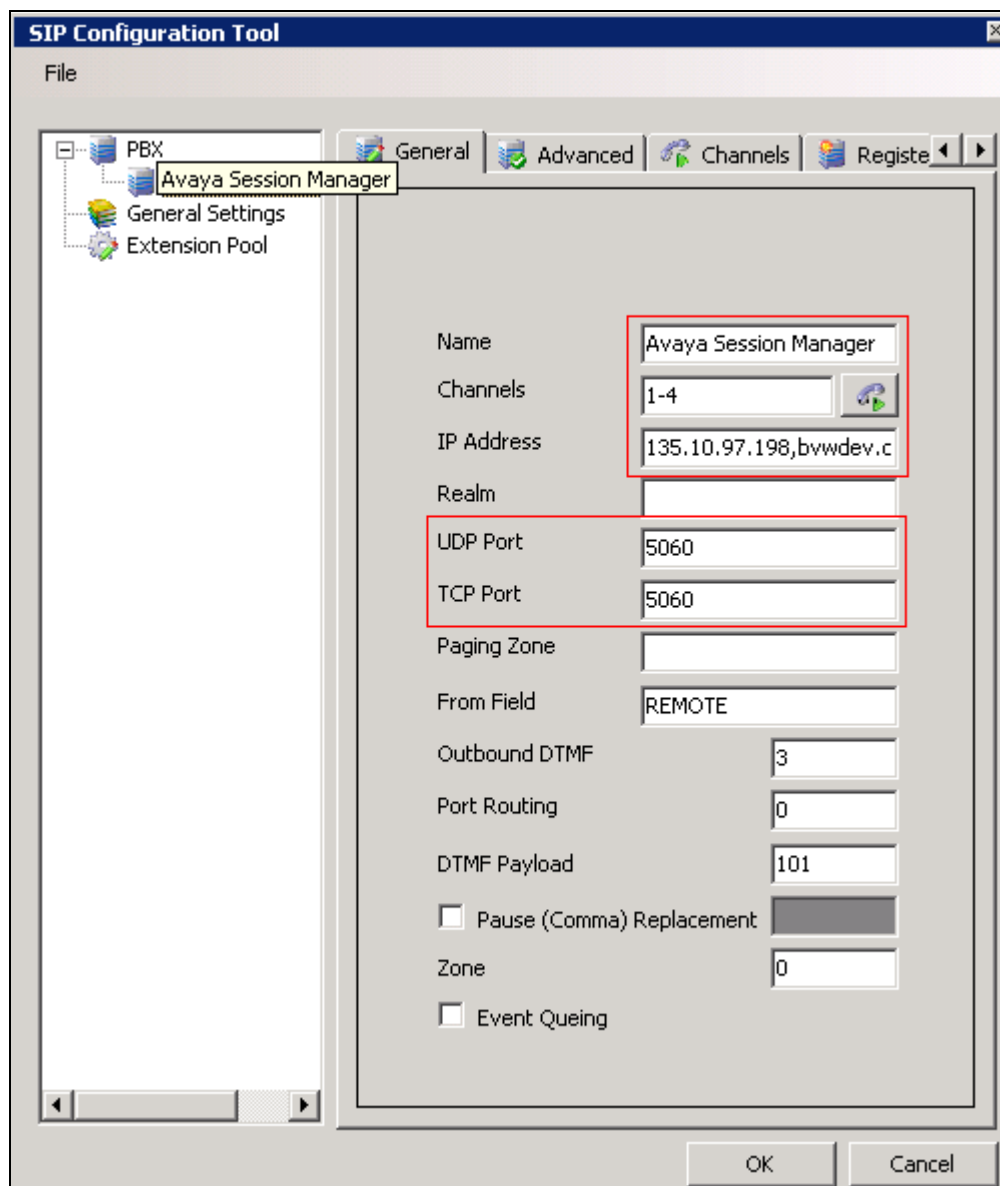
## 10. Configure the ESNA Telephony Office-LinX

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

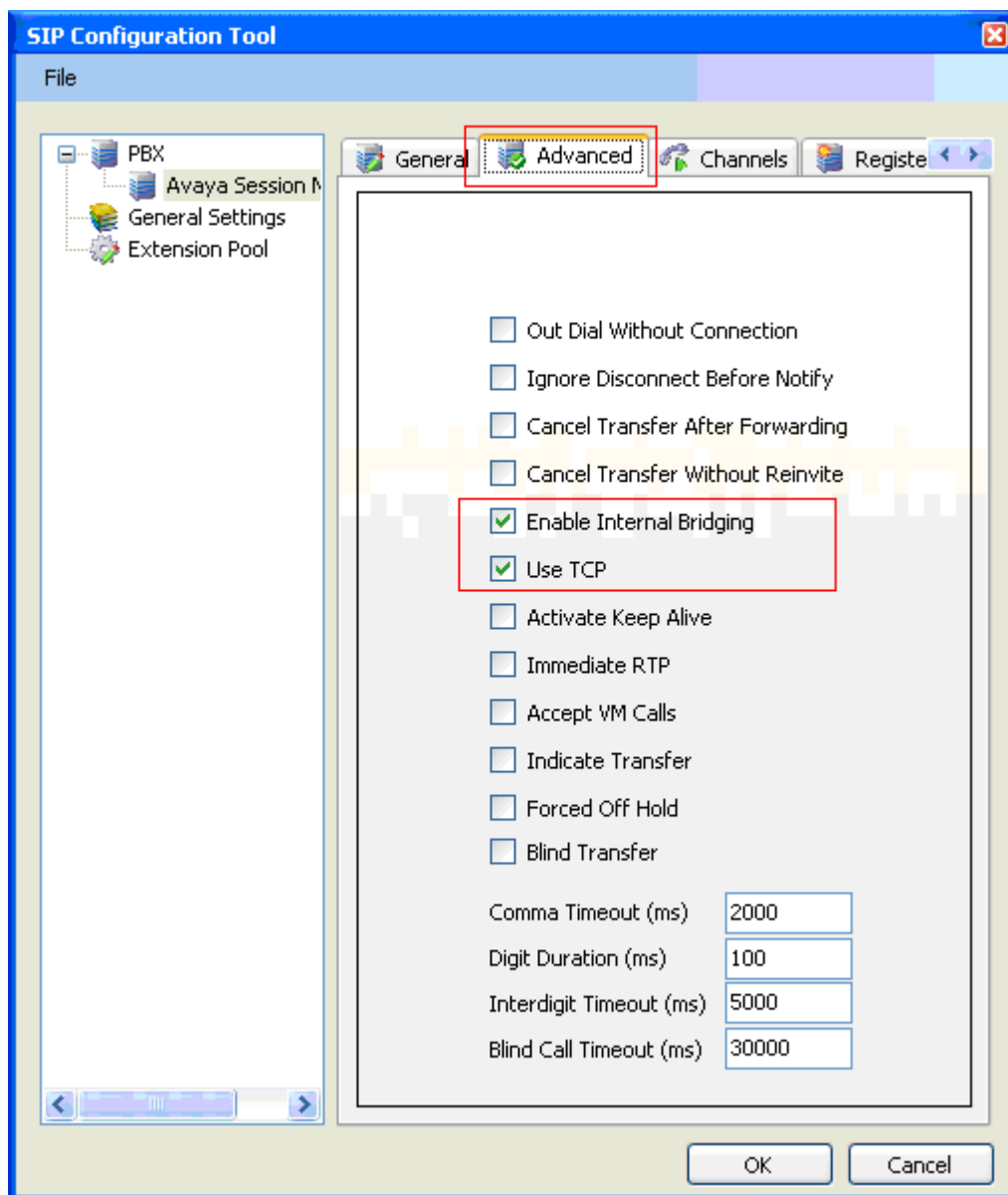
To configure ESNA Telephony Office-LinX, navigate to **Start → All Program → Telephony Office-LinX Enterprise Edition → SIP Configuration Tool**. Select **Avaya Session Manager** under PBX in the left pane. Provide the following information:

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

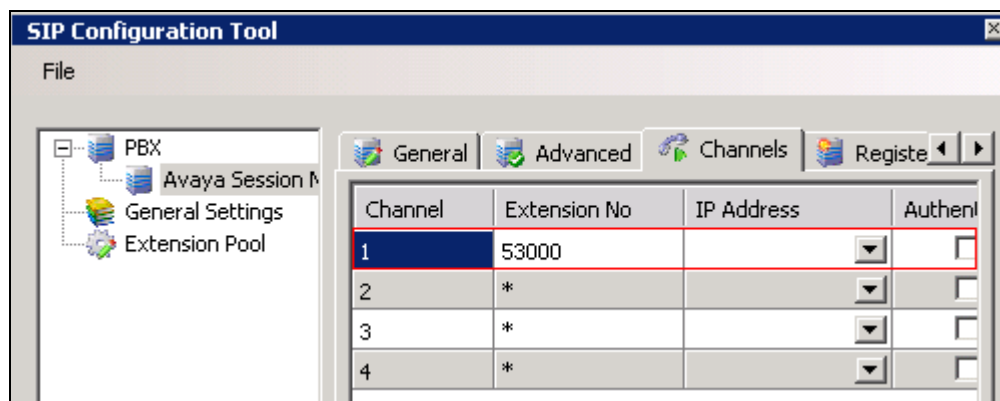


Click the **Advanced** tab in the right pane, and check the following check boxes:

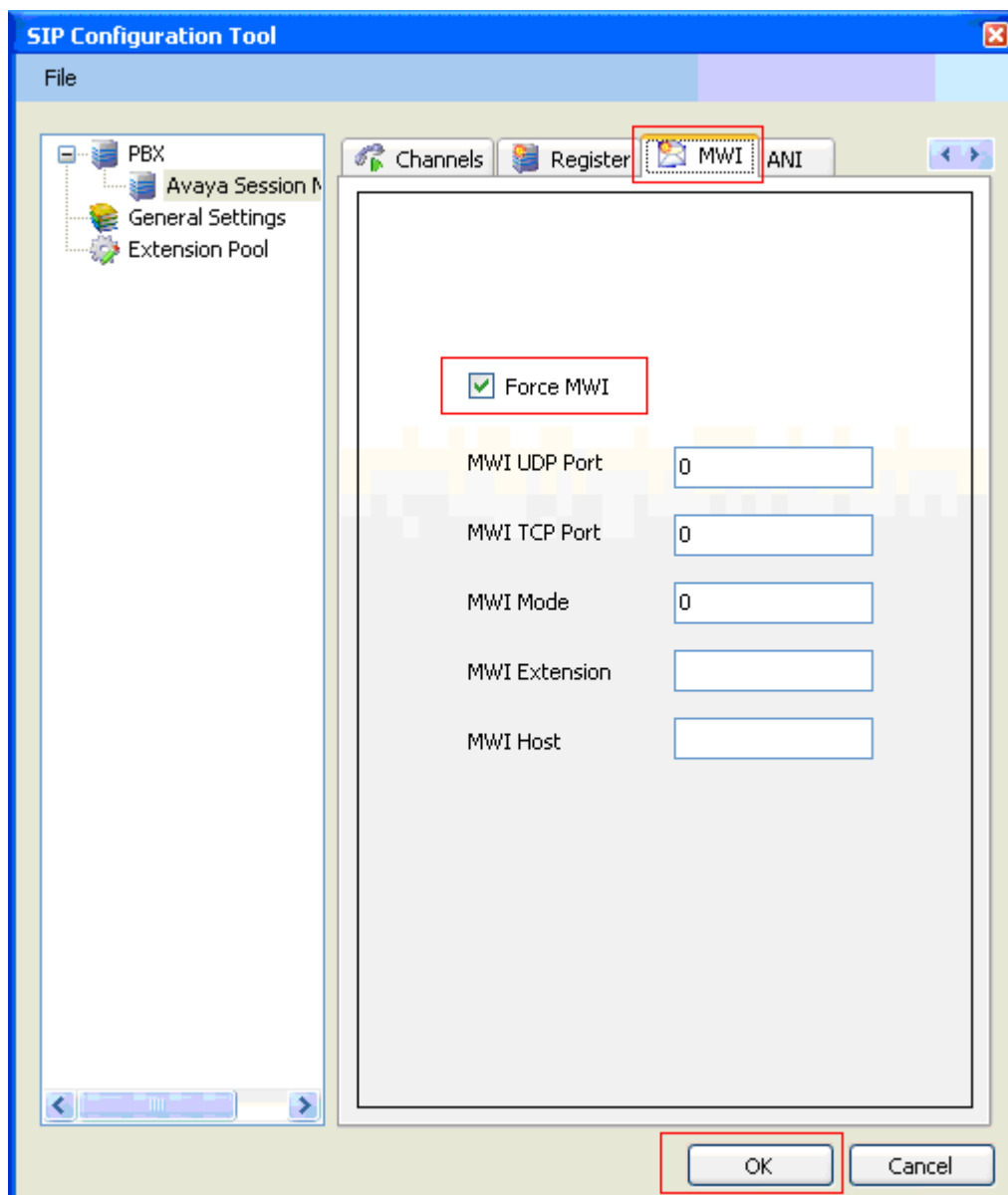
- Enable Internal Bridging
- Use TCP



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.



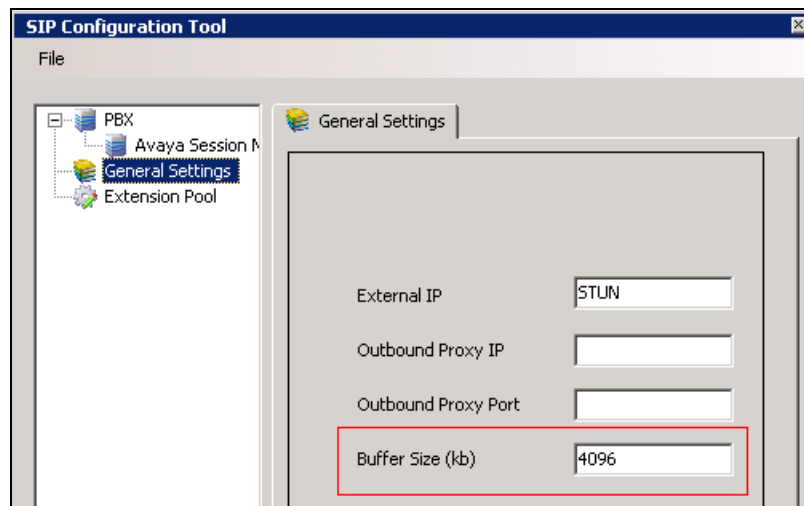


The following line must be added to the SIP Configuration file (ETSIPService.ini, found under C:\Windows\) manually under the [PBX#] heading:

### 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:

**User Name:** Enter user that created on Avaya ACE in **Section** Error! Reference source not found.

**Password:** the password that entered in **Section** Error! Reference source not found.

**IP Address:** Avaya ACE IP address.

**Avaya ACE Wizard**

**ACE Server Settings**

User Name:

Password:

IP Address:

Secure Socket ☐

**UC Server Settings**

Host IP Address:

TCP Port:

**ACE Notification Settings**

Callback IP Address:

Callback Port:

Log Path:

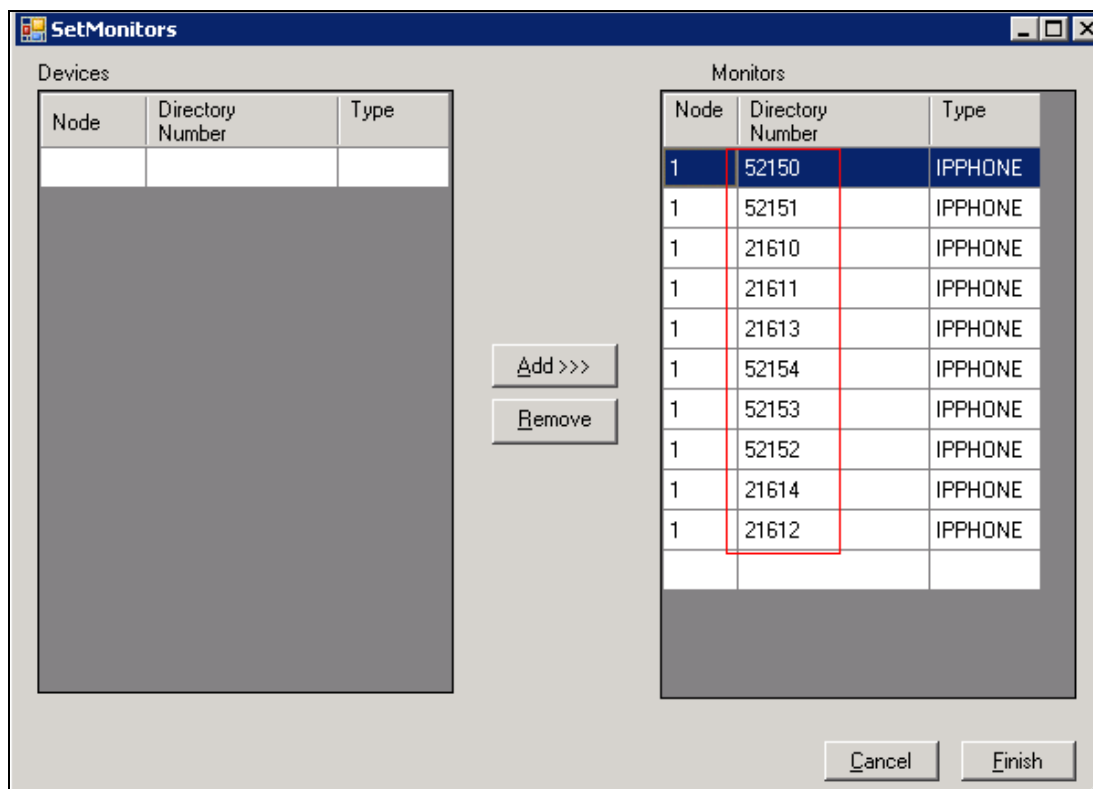
Pause Time (ms):

Click on Nodes to open the next window where user can enter device extension to get its notification. Click on Next button. Below is the list of extensions used during the testing:

**NodesFrm**

	NodeID	Starting DeviceID	Ending DeviceID	Type
▶	1	52150	52150	IPPHONE ▼
	1	52151	52151	IPPHONE ▼
	1	52153	52153	IPPHONE ▼
	1	21610	21614	IPPHONE ▼
	1	52154	52154	IPPHONE ▼
	1	52152	52152	IPPHONE ▼
*				▼

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



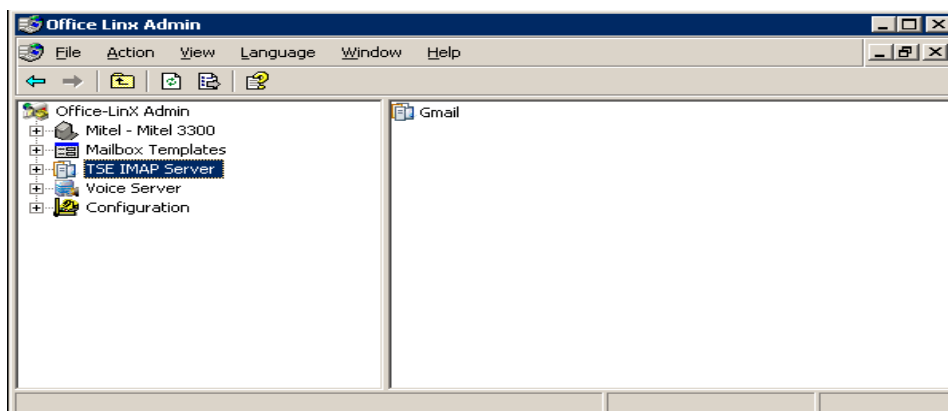
### 10.3. Message Synchronization

In order to achieve IMAP synchronization between Google Apps and Office-LinX, set the Google Apps mail mode to IMAP. All other configuration takes place in OL Admin where individual mailboxes hold the credentials for the corresponding Google Apps email account.

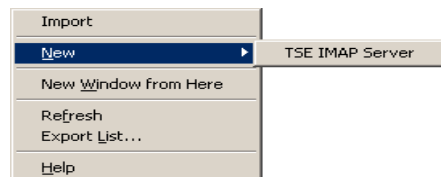
#### 10.3.1. TSE IMAP Configuration

Before you can synchronize your mailboxes with a Gmail account you must first configure your Office-LinX Admin so that it can access the Gmail IMAP server.

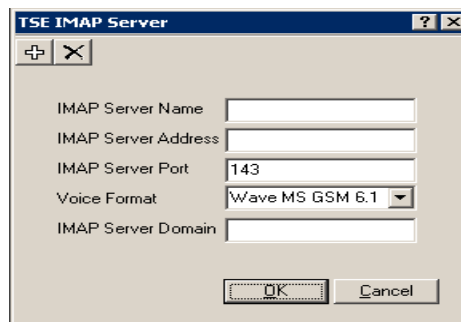
1. Locate and run **Office-LinX Admin** console.
2. From the left hand menu locate the **TSE IMAP Server**.



3. Right click on the **TSE IMAP Server** and the following menu appears. Select **New -> TSE IMAP Server**.



4. The **TSE IMAP Server** creation window opens. Fill out the boxes as follows:
- **IMAP Server Name:** Gmail (or Google Apps name for your company)
  - **IMAP Server Address:** imap.gmail.com
  - **IMAP Server Port:** 993
  - Click **OK**.



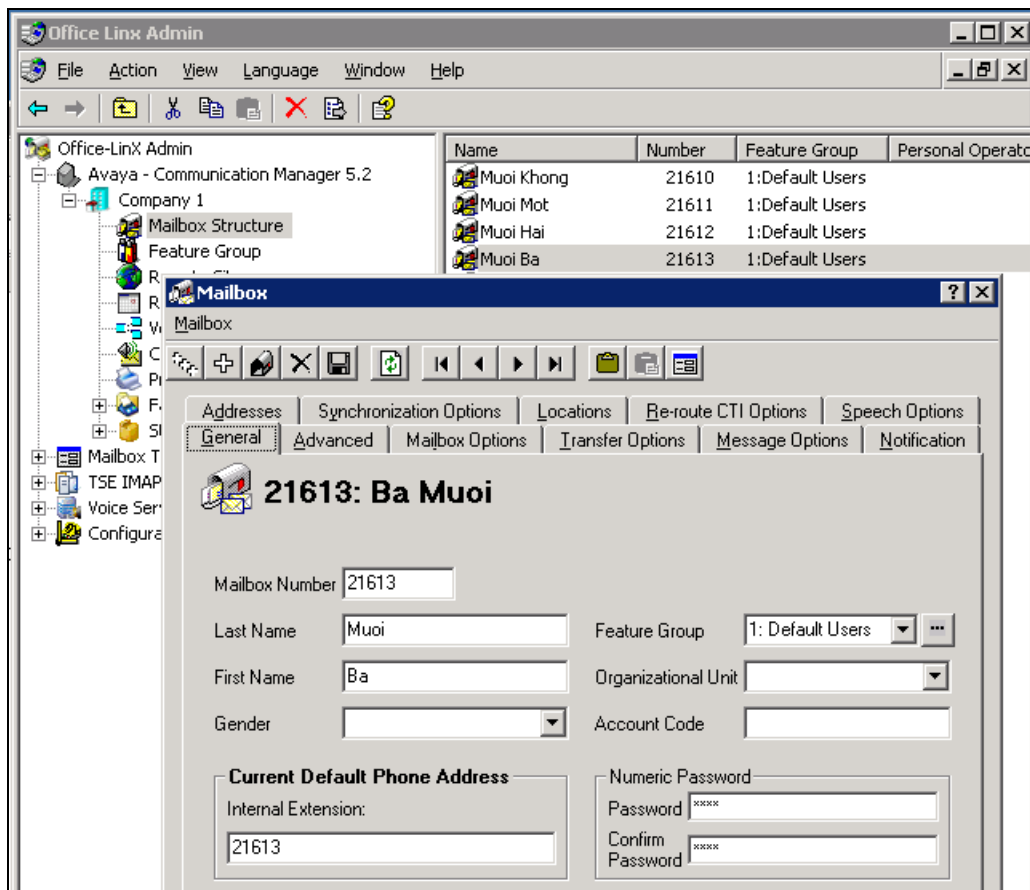
5. Restart the **TSE Cache Manager** Service from the Services panel. The Office-LinX UC platform is now ready to synchronize system mailboxes with Google Gmail IMAP accounts.

#### 10.4. Configure user mailbox in Office-LinX Admin

Double click on Office-LinX icon to launch the application window.

Expand the tree **Office-LinX Admin → Avaya – Communication Manager 5.2 → Company 1** and highlight the **Mailbox Structure**. In the right panel right click on the window, select new to add new mailbox (Not shown).

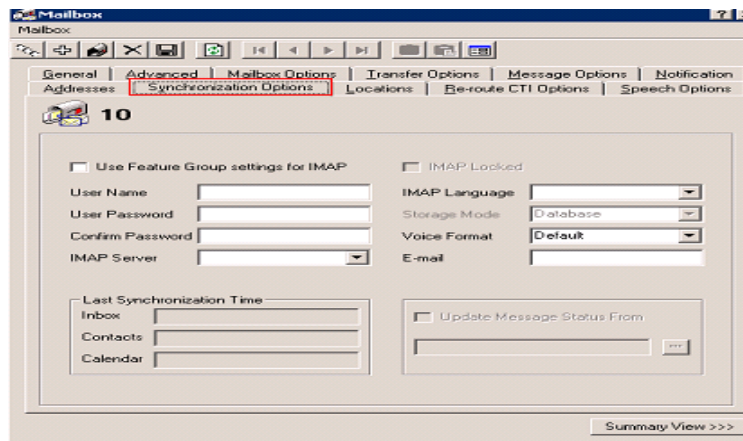
Leave all the value as default and modify it if need. Example below is mail box for extension **21613** and default password is 1111.



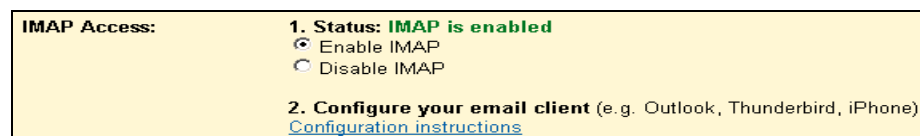
## 10.5. Configure mailbox to be synchronized with a Google App IMAP account

In order for your mailboxes to be synchronized with a Google Apps IMAP account you must individually setup each of the mailboxes accordingly. You must also ensure that the Google Apps/Gmail account that Office-LinX will be synchronizing with is configured for IMAP connection.

In **Office-LinX** → **Mailbox Structure**, double click on selected mailbox that used to sync with a Google Apps IMAP account. Select the **Synchronization Options** tab as shown below:



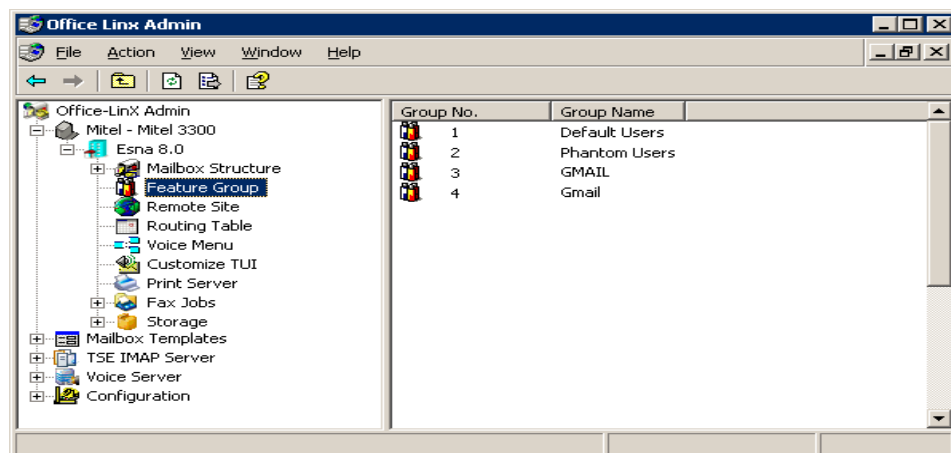
1. Fill out all the information as follows:
  - **User Name:** Type in the **email address** of the **Gmail** account that you have created for this mailbox.
  - **User Password:** Type in the password for the **Gmail** account.
  - **Confirm Password:** Type in the password for the **Gmail** account again to verify.
  - **IMAP Server:** From the dropdown menu select **Gmail**.
  - **IMAP Language:** From the dropdown menu select the language you will be using.
  - **Storage Mode:** From the dropdown menu select **IMAP**.
2. Close the configuration window and **save** your settings. Your messages to this mailbox will now be directly synchronized with the Gmail account that was configured.
3. From the Google Apps/Gmail account settings, open the Forwarding and POP/IMAP tab. Verify that IMAP Status is set to IMAP Enabled.



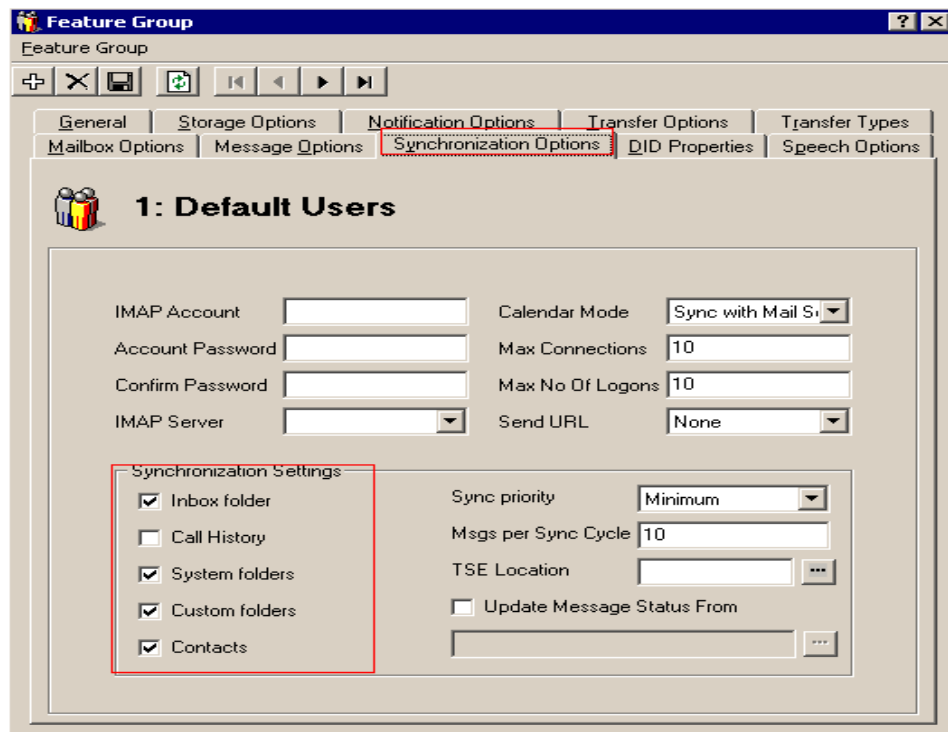
## 10.6. Feature Group

In order to ensure that there are no conflicts between Office-LinX and Gmail, please follow these steps to configure the Feature Group to synchronize the required information.

1. Locate and run **Office-LinX Admin** console.
2. From the left hand menu locate the **Feature Group**. Find the Feature Group that the mailboxes with Gmail synchronization are located in. Double click on the feature group to load the Feature Group configuration window.



3. From the Feature Group configuration window, open the **Synchronization Options** tab.
4. Under Synchronization Settings, enable all of the checkboxes that apply. These are the data types that will be synchronized between Office-LinX and Gmail.
5. Save and close the window after the changes are complete.



6. Your Office-LinX mailbox is now fully synchronized with the Gmail IMAP account.

**Note:** To make sure that your mailboxes are associated with the right Feature Group, check the Mailbox configuration window under the General tab.

## 10.7. Synchronization through OAuth (superuser)

Google Apps supports OAuth (superuser) authentication which makes the deployment of IMAP TSE synchronization easier. Rather than requiring the individual user's username and password in order to synchronize data between the Office-LinX and Google servers, you may use a single OAuth account which has the authority to oversee all of the Google accounts within an organization. This means that you no longer have to enter passwords for each individual user's mailbox settings. Simply define the OAuth settings in the Feature Group, then all mailboxes within that Feature Group can enter their user name only and skip the password on their mailbox settings. Another significant advantage of this authentication method is that users can change the password for their Google accounts without having changed any Office-LinX settings. Since the OAuth account oversees authentication, users are free to change their Google passwords without affecting the synchronization.

### 10.7.1. Configuring OAuth

**Note:** Your Google Apps must have its own domain name in order to utilize this feature.

The first step is to create an OAuth account from Google Apps.

1. Log into your Google Apps account as the administrator, then go to Manage Domain > Advanced tools > Manage OAuth Domain Key.
2. From here, select both Enable this consumer key and Allow access to all APIs.
3. Record the OAuth consumer key and the OAuth consumer secret.

4. The OAuth consumer key will act as the superuser account name while the OAuth consumer secret is the password for the account.
5. Once all the changes have been made, click on Save Changes.

Google apps Premier Edition

Search accounts Search Help Center

Dashboard Users and groups Domain settings Advanced tools Support Service settings

[Back to Advanced tools](#)

### Manage OAuth key and secret for this domain

OAuth consumer key: **OAuth** ☒ Enable this consumer key  
Allows this key and secret to be used to generate OAuth requests to Google Data APIs. [Learn more](#)

OAuth consumer secret: **WOWOWOWOWOWOWOWOY** [Regenerate OAuth consumer secret](#)

X.509 certificate: We do not have a certificate for your domain.

Upload a certificate: (Optional) [Browse...](#)  
File must be in PEM format. [Learn More](#)

Two-legged OAuth access control ☒ Allow access to all APIs  
The key and secret above are able to access any user's data for all Google Data APIs. [Learn more](#)

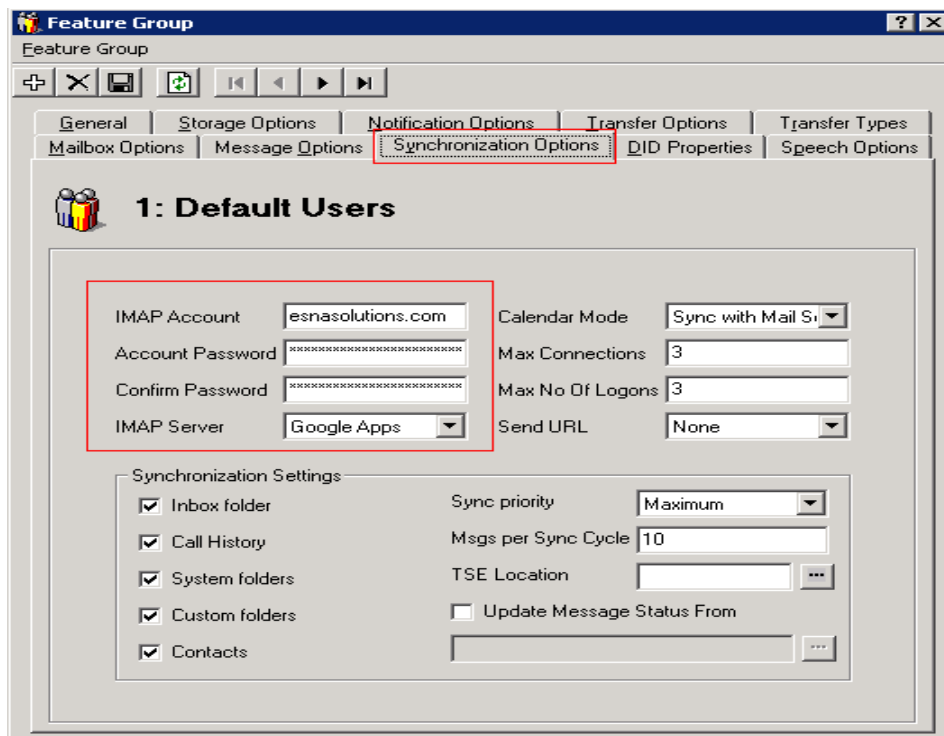
[Save changes](#) [Cancel](#)

The next step is to enter the OAuth information on the Feature Group.

1. Launch OL Admin and go to the Feature Group > Synchronization Options tab.
2. Enter the OAuth consumer key for the IMAP Account.
3. Enter the OAuth consumer secret for the Account Password and Confirm Password fields.

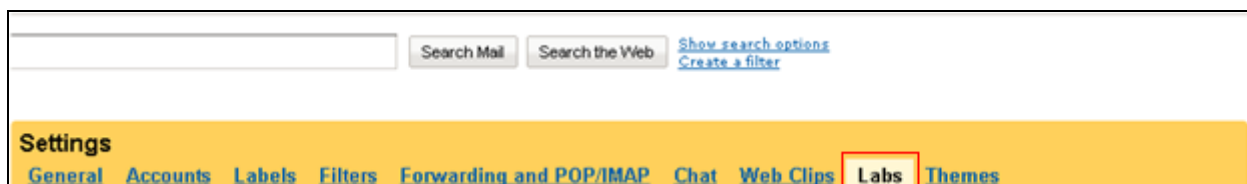
All mailboxes which belong to this Feature Group will now take advantage of the convenience of OAuth. Users will no longer have to define their Google account password on through Office-LinX.





## 10.8. Install and Configure UC Client Google Gadget on Gmail

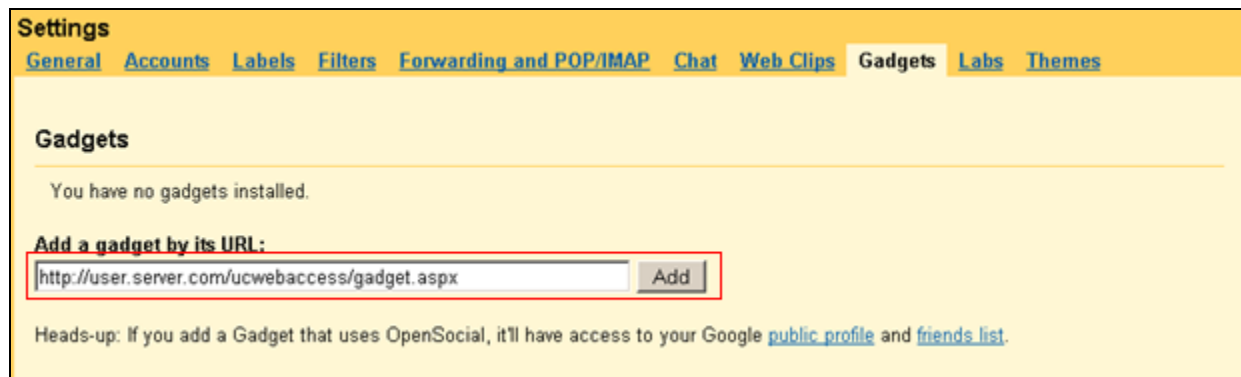
1. To add a UC Client Manager Web Gadget to the Gmail interface, log into your Gmail account and open the **Labs** tab under **Settings**.



2. Scroll down to the last entry “**Add any gadget by URL**”. Enable this option. Click **Save Changes**.

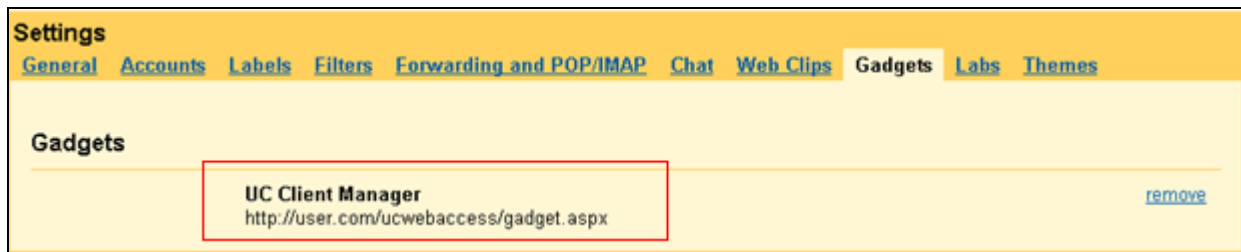


3. A new tab called **Gadgets** will appear under settings. In the address space, enter the URL: **http://USER.YOUR\_SERVER.COM/ucwebaccess/gadget.aspx**

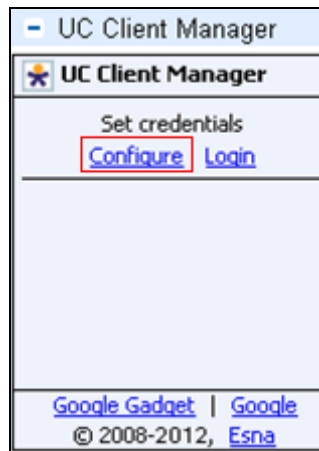


Replace USER.YOUR\_SERVER.COM with the address of your own UC server. When ready, click the **Add** button.


The UC Client Manager gadget is now listed on the **Gadgets** tab.



The UC Client Manager Gadget is now being available on the Gmail interface.

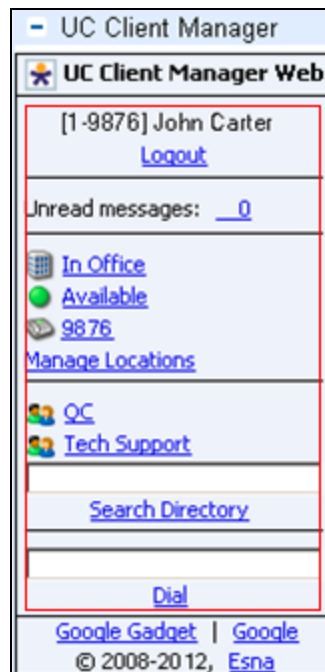


Click **Configure** to enter the necessary login information.



A dialog box titled "Set credentials" with three input fields: "Company" containing "1", "Mailbox" containing "9876", and "Password" containing seven dots. A red rectangle highlights the "Company" and "Mailbox" fields. At the bottom are "Save" and "Cancel" buttons.

Enter the company number (which is 1 in most cases), then enter mailbox number and password. Click **Save**. User is now login. See screen shot below.



A screenshot of the "UC Client Manager Web" interface. It shows a user profile for "[1-9876] John Carter" with a "Logout" link. Below this, it displays "Unread messages: 0". There are several status and action links: "In Office", "Available", "9876", "Manage Locations", "QC", "Tech Support", "Search Directory", and "Dial". At the bottom, it says "Google Gadget | Google" and "© 2008-2012, Esna". A red rectangle highlights the user profile and status links.

## 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 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:** 

Session Manager Dashboard <span>Help ?</span>										
This page provides the overall status and health summary of each administered Session Manager.										
Session Manager Instances										
<div>Service State ▾ Shutdown System ▾ As of 3:34 PM</div>										
<div>1 Item Refresh Show ALL ▾ Filter: Enable</div>										
<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		Up	Accept New Service	14/44	0	3	6.1.6.0.616008
Select: All, None										

### 11.2.2. Verify SIP Entity Link Status

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

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

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

**SIP Entity, Entity Link Connection Status**  
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

**All Entity Links to SIP Entity: DevACEsrv**

Summary View

2 Items Refresh Filter: Enable

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

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

## 11.3. Verify Avaya Aura® Application Enablement Server

### 11.3.1. Verify Services are running.

Verify that the AES 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	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"/>	5BB60FBA73E88AD76 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`

```

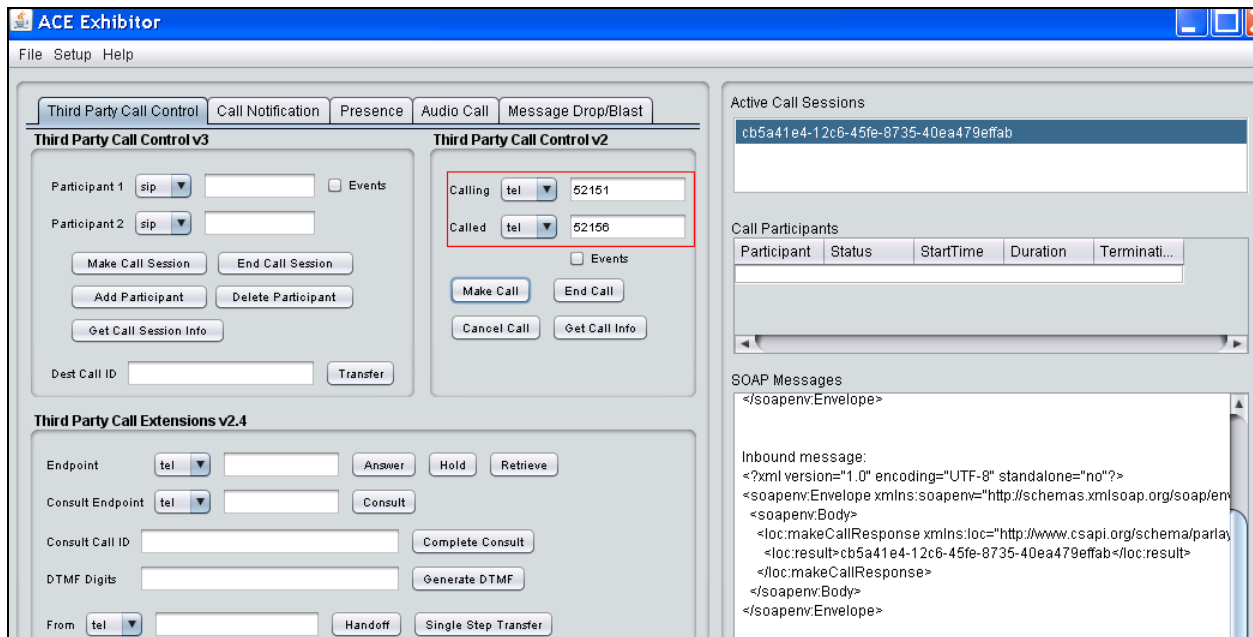
-bash-3.2$ netstat -an | grep 4723
tcp        0      0  :::ffff:127.0.0.1:4723  :::*           LISTEN
tcp        0      0  :::ffff:135.10.97.62:4723  :::*           LISTEN
tcp        0      0  :::ffff:135.10.xx.xx:4723  :::ffff:135.10.xx.xx:60328  ESTABLISHED
-bash-3.2$

```

The AES is listening on port 4723. There should be an ESTABLISHED link between the AES 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 AES 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 AES 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 Aura® 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	
Hostname	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	<b>RUNNING</b>
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	<b>RUNNING</b>
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

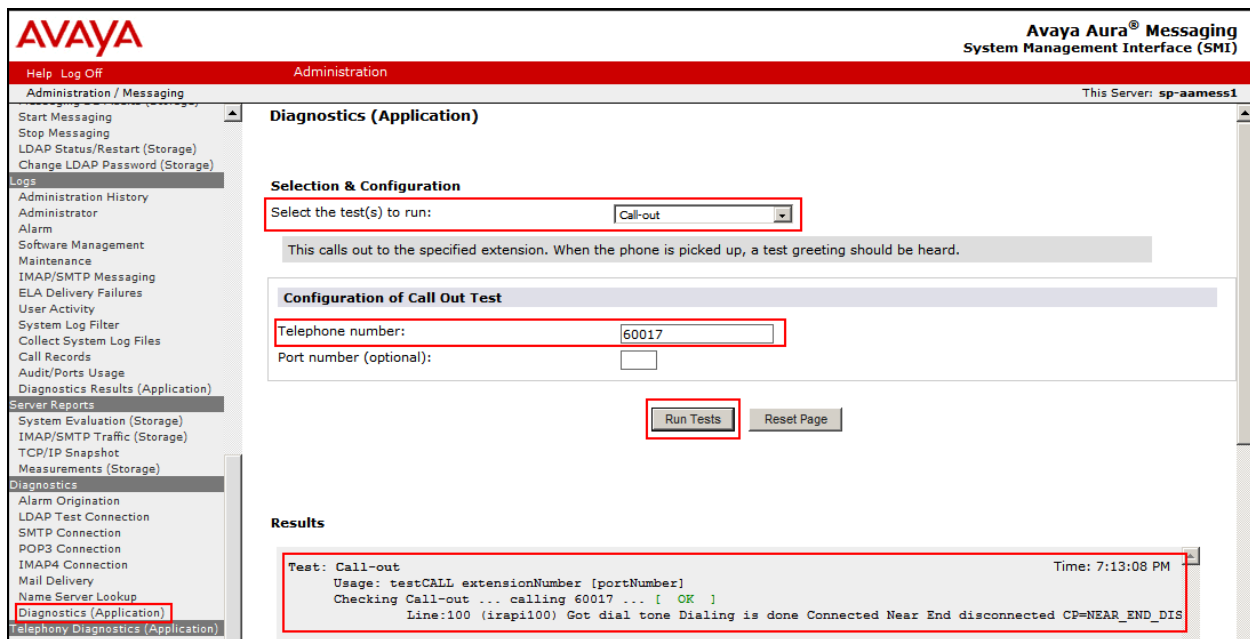
### 11.5.1. Verify Avaya Aura Messaging can make a call to phones

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 or Google Mail account

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/ Google mail account called user 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 Aura Messaging). Example below show user has incoming AAM voice message in the mailbox.

In Office 1 Available >>				
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	gfdgfdgfd	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 Google gadget.

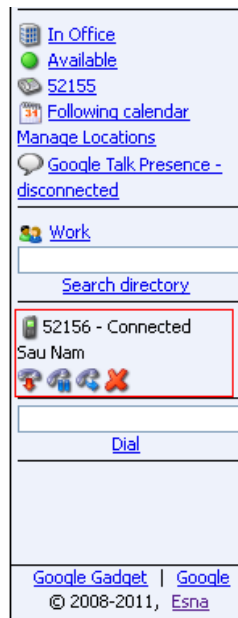
### 11.6.1. Verify the log file UCServer of ESNA Office-LinX.

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 User can make a call using UC Client Google Gadget in the Gmail

User login ESNA Gmail account as created in **Section 10.4**. User able to enter the number and click Dial. The devices are ringing. Called pick up the device. The 2 way voice path is established.



## 12. Conclusion

Interoperability testing of Avaya ACE, Avaya Aura® Messaging, and Avaya Aura® Communication Manager 5.2 with Office-LinX 8.5 SP2 – UC Client Google Gadget 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*, May 2009, Release 5.2, Issue 5.0 Document Numbers 03-300509.
2. *Administering Avaya Aura® Session Manager*, August 2010, Release 6.0, Document Number 03-603324.
3. *Administering Avaya Aura® System Manager*, June 2010, Release 6.0.
4. Avaya Agile Communication Environment Avaya Aura Integration Release 3.0 NN10850 03.03 March 2012

The following document was provided by ESNA.

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

---

**©2011 Avaya Inc. All Rights Reserved.**

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](mailto:devconnect@avaya.com).