



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

**Abstract**

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Result .....	4
2.1.	Interoperability Compliance Testing .....	5
2.2.	Test Results .....	6
2.3.	Support.....	7
3.	Reference Configuration .....	8
4.	Equipment and Software Validated .....	9
5.	Configure Avaya Aura® Communication Manager .....	10
5.1.	Configure SIP Trunk.....	10
5.1.1.	Capacity Verification .....	10
5.1.2.	Configure IP Codec Set .....	11
5.1.3.	Configure IP Network Region .....	12
5.1.4.	Configure IP Node Name.....	12
5.1.5.	Configure SIP Signaling .....	13
5.1.6.	Configure Trunk Group .....	14
5.1.7.	Configure Route Pattern .....	15
5.1.8.	Administer Dialplan.....	15
5.1.9.	Configure Hunt Group for Avaya Aura® Messaging.....	17
5.1.10.	Configure Coverage Path to Avaya Aura® Messaging .....	18
5.1.11.	Administer a Station for Coverage to Avaya Aura® Messaging.....	19
5.1.12.	Configure SIP Endpoint.....	20
5.1.13.	Configure Location .....	20
5.2.	Configure ASAI Link .....	21
5.2.1.	Verify License Permission.....	21
5.2.2.	Configuring AE Services and Avaya Agile Communication Environment™ as an AE Service Server .....	21
5.2.3.	Add a CTI link .....	22
6.	Configure Avaya Aura® Messaging.....	23
6.1.	Administer Sites.....	24
6.2.	Administer Telephony Integration .....	25
6.3.	Configure Dial Rules .....	26
6.4.	Configure Class of Service .....	27
6.5.	Administer Subscribers .....	28
6.6.	Administer Topology .....	30
6.7.	Administer External Host .....	30
6.8.	Recording Format .....	31
6.9.	Configure Notify Me for Avaya Aura® Messaging mailboxes.....	32
7.	Configure Avaya Aura® Session Manager .....	33

7.1.	Configure SIP Domain.....	34
7.2.	Configure Locations.....	35
7.3.	Configure SIP Entities .....	36
7.4.	Configure Entity Links .....	39
7.5.	Configure Routing Policies.....	40
7.6.	Configure Dial Patterns.....	42
7.7.	Configure SIP Users .....	44
8.	Configure Avaya Agile Communication Environment™ 6.2 .....	48
8.1.	Configuring the Communication Manager's SSL certificate Signing Authority as Trusted on Avaya ACE.....	48
8.2.	Add ASAI Service Provider.....	49
8.3.	Add User .....	53
8.4.	Add Role .....	54
9.	Configure the Esna Telephony Officelinx .....	56
9.1.	Configure SIP Configuration Tool.....	56
9.2.	Configure UC ACE Wizard .....	59
9.3.	Administer Company Profiles.....	60
9.4.	Configure User Mailbox in Officelinx Admin.....	61
9.5.	Configure Fax .....	64
9.6.	Install and Configure iLink Pro on Salesforce.com.....	65
9.6.1.	Install open CTI Integration.....	65
9.6.2.	Call Center Definition.....	67
9.6.3.	Login iLink Pro on Salesforce.com .....	68
10.	Verification Steps.....	69
10.1.	Verify Avaya Aura® Communication Manager.....	69
10.2.	Verify Avaya Aura® Session Manager .....	70
10.2.1.	Verify Avaya Aura® Session Manager is Operational.....	70
10.2.2.	Verify SIP Entity Link Status .....	70
10.3.	Verify Avaya Agile Communication Environment™ .....	71
10.3.1.	Verify Avaya Agile Communication Environment™ Server Status .....	72
10.4.	Verify Avaya Aura® Messaging .....	73
10.4.1.	Verify Avaya Aura® Messaging can Make Calls to Phones.....	73
10.5.	Verify user can Receive and Retrieve Avaya Aura® Messaging Voice Message using Google Mail .....	74
10.6.	Verify user can send a fax through Google email.....	74
10.7.	Verify user able to make a call using iLink Pro on Salesforce.com .....	75
11.	Conclusion .....	76
12.	Additional References.....	76

# 1. Introduction

The Avaya Agile Communication Environment™ (ACE) interacts with the Avaya Aura® service provider to provide web services and enable communications between Avaya ACE client applications and an Avaya Aura® communications solution. Avaya Aura® can provide services to Avaya ACE in a number of different configurations. Each configuration provides certain services that define which Avaya ACE services are available. In this solution, the configuration used is Avaya Aura Adjunct Switch Application Interface (ASAI) service provider for services where Avaya ACE needs to control a Computer Telephony Integration (CTI)-capable terminal on the Avaya Aura® Communication Manager (Communication Manager).

These Application Notes describe the procedure for configuring Esna Officelinx to successfully interoperate with Avaya ACE, Communication Manager. And configure Esna Officelinx to receive voice message on Avaya Aura® Messaging (Messaging) via SMTP.

iLink Pro is installed as a plug in to Salesforce.com (SFDC). This provides users with contact, presence and call management function directly with in SFDC. iLink Pro controls a physical telephone by using Third-Party Call control, specifically the Third Party Call (v2 and v2.4) and Call Notification web service which provided by Avaya ACE.

## 2. General Test Approach and Test Result

The feature test cases were performed manually and automatic. During configuration of the Officelinx server and UCACE Wizard a list of devices is setup for monitoring. The applications automatically requested monitoring of these devices.

For the manual part of the testing, manually place a call using iLink Pro on SFDC to verify call features such as make call, answer call, transfer or put call on hold. When the call is placed, Officelinx will send the web service request to ACE to control the monitored device which is configured on the Esna UCACE Wizard. In Google mail, verify that the fax feature such as send and receive fax via email, also verify that a copy of the Messaging voice messaging is send to Google mail and it can be opened and played on the web.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to Esna Officelinx.

The verification of tests included human checking of proper states of the iLink Pro plugin at the user desktops and telephones, and reviewing the UCACEServeryyyymmdd log on Officelinx.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

## 2.1. Interoperability Compliance Testing

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

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

## 2.2. Test Results

Interoperability testing of ACE, Messaging, and Communication Manager with Officelinx 9 SP1 – iLink Pro was completed and passed with observations as list below:

1. Prior to configuration of the Esna Officelinx Cloudlink Edition server, the Officelinx Cloudlink Edition menu provides feature button labels for actions on incoming calls. The “Take Message” feature was tested but the redirected call did not properly integrate with the correct voicemail box. It is recommended that this feature option be disabled by the Esna Officelinx Cloudlink Edition Administrator.
2. When a user receives a message, iLink Pro receives and indicates that there is a new message, and the message waiting indicator (MWI) is turned on. When a user retrieves a message using iLink Pro, MWI is turned off on iLink Pro and the physical phone. But when Messaging maintenance subsequently runs, MWI is turned on again and Messaging indicates there is a new message. This is a known limitation and is due to the fact that Esna Officelinx Cloudlink Edition does not currently use the ACE Messaging API to “synchronize” the information to Messaging. This capability is planned for implementation in a future release of Esna Officelinx Cloudlink Edition.
3. Call extension of parties after a call is transferred does not update. This is a known limitation in the current version of Esna Officelinx Cloudlink Edition. A fix is planned for a future release of Esna Officelinx Cloudlink Edition.
4. Call forward is not supported on ASAI Service Provider. If you make a call to an unavailable iLink Pro user, the call can be forwarded to Messaging, but the caller gets the general greeting, instead of the greeting for the user that was called. To avoid this issue the call can be forced to ring at the called party’s phone by not entering the Messaging hunt group number in the Officelinx configuration.
5. A physical phone A is not monitored by Esna Officelinx, make a call to iLink Pro user B (physical phone B is monitored) then phone A perform consult transfer to iLink Pro user C (physical phone C is monitored). iLink Pro C later tries to put the call on Hold using iLink Pro - Hold option, the call is not put on hold and the user C loses call control UI on iLink Pro. Work around is to put the call on hold using physical phone. This is a known limitation of Esna Officelinx Cloudlink Edition. To avoid this issue all internal phones must be monitored by Officelinx.
6. When Device A (DA) makes a call to iLink Pro user B and iLink Pro user B transfers the call to iLink Pro user C, iLink Pro user C sometimes receives 2 popup messages: “Call Disconnected from DA” and “Incoming call from DA”. After 3 second the extraneous “Call Disconnected” popup message is closed. iLink Pro user C can click answer on the “Incoming call” popup window to connect the call. The two popup windows do not impact the call operation; however having 2 popup windows displayed at the same time can confuse the user. User should ignore the extraneous “Call Disconnected” message when it occurs. A fix is planned for a future release of Esna Officelinx Cloudlink Edition.

7. If the phones of iLink Pro user A, and iLink Pro user B are off-hook (e.g. A and B are on a call), the status of iLink Pro user A and B are displayed to iLink Pro user C as “On the Phone”. If iLink Pro user C makes a call to iLink Pro user A, and iLink Pro user C then disconnects the call (hangs up) before iLink Pro user A answers, the display of iLink Pro user A’s status on iLink Pro user C is changed to indicate that iLink Pro user A is not on the phone, even though the call between iLink Pro user A and iLink Pro user B is still connected. A fix is planned for a future release of Esna Officelinx Cloudlink Edition.
8. iLink Pro user A is on a call with iLink Pro user B. iLink Pro user C attempts to call iLink Pro user A, iLink Pro user A receives an alert message for the incoming call. If iLink Pro user A clicks “Answer”, ACE generates an exception, “Exception 10001 Service Error occurred”, for the second call and the first call remains connected. This is due to the fact that ACE expects the first call to be put on hold before the second call is answered. If iLink Pro user A puts the first call on hold before clicking answer on the second call the problem does not occur. Also, the problem does not occur if iLink Pro user A answers the second call by pressing the answer button on the device, as Avaya Aura Communication Manager will automatically put the first call on hold before answering the second.
9. When a user double clicks on the Answer option, multiple requests for Answer call are sent to ACE which is causing ACE to return an exception.

## 2.3. Support

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

- URL: [www.esna.com](http://www.esna.com)
- Email: [techsupport@esna.com](mailto:techsupport@esna.com)
- Phone: +1(905) 707-1234

There are three main parts in this setup:

- Endpoints include Avaya 9600 Series SIP and H.323 IP Telephones. For security purposes public IP addresses have been masked out or altered in this document.





## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on an Avaya S8300D Media Server	R016x.03.0.124 Patch 03.0.124.20850
Avaya G450 Media Gateway	33.13.0 (B)
Avaya Aura® System Manager running on an Avaya S8800 Server	6.3.0 FP2 SU 6.3.2.4.1399
Avaya Aura® Session Manager running on an Avaya S8800 Server	6.3 SP4
Avaya Aura® Messaging running on an Avaya S8800 Server	R016x.02.0.823
Avaya S8800 Server with VMWare 5.1 running Avaya Agile Communication Environment VE	6.2.1FP2
Avaya 9611G, 9608 H323 Phone	6.2
Avaya 9611G, 9608 SIP Phone	6.2
Avaya 9630 H323 Phone	3.1.05
Esna Officelinx	9.1 SP1
iLink Pro	9.1.14.1227
Salesforce.com (SFDC)	14

## 5. Configure Avaya Aura® Communication Manager

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

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

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

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

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

### 5.1. Configure SIP Trunk

The following sections show the necessary steps required to configure Communication Manager to interoperate correctly with Session Manager.

#### 5.1.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient **Maximum Off-PBX Telephones – OPS licenses**. If not, contact an authorized Avaya account representative to obtain additional licenses

display system-parameters customer-options		Page	1 of 11
OPTIONAL FEATURES			
G3 Version: V16	Software Package: Standard		
Location: 2	System ID (SID): 1		
Platform: 28	Module ID (MID): 1		
			USED
Platform Maximum Ports: 6400			185
Maximum Stations: 500			19
Maximum XMOBILE Stations: 2400			0
Maximum Off-PBX Telephones - EC500: 10			0
<b>Maximum Off-PBX Telephones - OPS: 500</b>			<b>9</b>
Maximum Off-PBX Telephones - PBFMC: 10			0
Maximum Off-PBX Telephones - PVFMC: 10			0
Maximum Off-PBX Telephones - SCCAN: 0			0
Maximum Survivable Processors: 0			0

On **Page 2** of the form, verify that the number of **Maximum Administered SIP Trunks** supported by the system is sufficient for the number of SIP trunks needed. If not, contact an authorized Avaya account representative to obtain additional licenses.

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES			USED	
Maximum Administered H.323 Trunks:			4000	20
Maximum Concurrently Registered IP Stations:			2400	3
Maximum Administered Remote Office Trunks:			4000	0
Maximum Concurrently Registered Remote Office Stations:			2400	0
Maximum Concurrently Registered IP eCons:			68	0
Max Concur Registered Unauthenticated H.323 Stations:			100	0
Maximum Video Capable Stations:			2400	0
Maximum Video Capable IP Softphones:			10	0
<b>Maximum Administered SIP Trunks:</b>			<b>4000</b>	<b>110</b>
Maximum Administered Ad-hoc Video Conferencing Ports:			4000	0
Maximum Number of DS1 Boards with Echo Cancellation:			80	0
Maximum TN2501 VAL Boards:			10	0
Maximum Media Gateway VAL Sources:			50	0
Maximum TN2602 Boards with 80 VoIP Channels:			128	0
Maximum TN2602 Boards with 320 VoIP Channels:			128	0
Maximum Number of Expanded Meet-me Conference Ports:			8	0

### 5.1.2. Configure IP Codec Set

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

change ip-codec-set 1		Page	1 of	2
IP Codec Set				
Codec Set: 1				
Codec	Audio	Silence	Frames	Packet
	Suppression	Per Pkt	Size (ms)	
1: G.711MU	n	2	20	
2: G.711A	n	2	20	

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

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

### 5.1.3. Configure IP Network Region

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

- **Authoritative Domain** – Enter the appropriate name for the Authoritative Domain. During the compliance test, the authoritative domain is set to **bvwdev.com**. This should match the SIP Domain value on Session Manager. This name appears in the “From” header of SIP messages originating from this IP region.
- **Codec Set** – Set the configured codec set number. In this example, **Codec Set 1** is used.

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

### 5.1.4. Configure IP Node Name

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

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

### 5.1.5. Configure SIP Signaling

Enter the **add signaling-group <n>** command, where **n** 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 **tls**
- **Near-end Node Name:** Set to **procr**.
- **Far-end Node Name:** Set to the Session Manager name configured in node-names ip, example: **DevASM**.
- **Far-end Network Region:** Set to the configured region, example: **1**.
- **Far-end Domain:** Set to **bvwdev.com**. This should match the SIP Domain value in Session Manager.
- **Direct IP-IP Audio Connections:** Set to **y**, since the shuffling is enabled during the compliance test
- **Initial IP-IP Direct Media:** Set to **y**.

```
add signaling-group 5
                                SIGNALING GROUP

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

Near-end Node Name: procr      Far-end Node Name: DevASM
Near-end Listen Port: 5061     Far-end Listen Port: 5061
Far-end Network Region: 1
Far-end Domain: bvwdev.com

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? y
                                           Alternate Route Timer(sec): 6
```

### 5.1.6. Configure Trunk Group

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

- **Group Type:** Set the Group Type field to **sip**.
- **Group Name:** Enter a descriptive name.
- **TAC (Trunk Access Code):** Set to any available trunk access code.
- **Service Type:** Set the Service Type field to **tie**.
- **Signaling Group:** Set to the Group Number field value for the configured signaling group, example: **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, example: **20**.
- Default values were used for all other fields.

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

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

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign when passed in the SIP From, Contact and P-Asserted Identity headers.

```
display trunk-group 5                               Page 3 of 21
TRUNK FEATURES
    ACA Assignment? n                Measured: none
                                Maintenance Tests? y
                                Numbering Format: private
                                UI 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 <n>** command, where **n** 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 **trunk group 5** to route calls and **Numbering Format** is **lev0-pvt**. The default values for the other fields may be used.

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

### 5.1.8. Administer Dialplan

Configure dialplan analysis, Uniform Dialing, Private Numbering and AAR to route calls over a SIP trunk to Session Manager and ultimately to Messaging and 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. Below is the example of dialing plan used during compliance test.

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

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				
		782	5	ext	9	1	fac		
399	5	ext	*	4	dac				
521	5	ext							

Use the command **change uniform dial-plan 1** to create an entry in the UDP table which covers extensions to pilot number of Messaging. As shown below, any number dialed to **399xx** totaling 5-digits will be routed to the AAR

display uniform-dialplan 1					Page 1 of 2	
UNIFORM DIAL PLAN TABLE						
Percent Full: 0						
Matching		Insert		Node		
Pattern	Len	Del	Digits	Net	Conv	Num
399	5	0		aar	n	
521	5	0		aar	n	
782	5	0		aar	n	

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

change private-numbering 0					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext		Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len		
5	782	5		5	Total Administered: 12	
5	54	5		5	Maximum Entries: 540	
5	521	5		5		
5	782	5		5		
5	3999	5		5		

For the AAR Analysis Table, create the dial strings that will route calls to Avaya Aura Messaging, Telephony Officelinx extensions via the route pattern created in above section. Enter the **change aar analysis <n>** command, where **n** is a starting partial digit (or full digit). The dialed string created in the AAR Digit Analysis table should contain a map to the Messaging pilot number and Officelinx extension. During the configuration of the AAR table, the Call Type field was set to **unku** for **399xx** and to **aar** for **521xx** and **782xx**.

change aar analysis 0						Page 1 of 2		
AAR DIGIT ANALYSIS TABLE								
Location: all						Percent Full: 3		
Dialed		Total		Route	Call	Node	ANI	
String	Min	Max	Pattern	Type	Num	Reqd		
399	5	5	5	unku		n		
52	5	5	5	aar		n		
782	5	5	5	aar		n		



### 5.1.9. Configure Hunt Group for Avaya Aura® Messaging

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

- **Group Name:** Enter a descriptive name, example: **Messaging**.
- **Group Extension:** Enter an extension valid in the provisioned dial plan, example **39991**.

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

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

- **Message Center:** Enter **sip-adjunct**, indicating the type of messaging adjunct used for this hunt group. This value will also be used in the Station form.
- **Voice Mail Number:** Enter the Voice Mail Number, which is the extension of Messaging.
- **Voice Mail Handle:** Enter the Voice Mail Handle which is the extension of Messaging.

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

### 5.1.10. Configure Coverage Path to Avaya Aura® Messaging

This section describes the steps for administering coverage path in Communication Manager. Enter the **add coverage path <n>** command; where **n** 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.

```
display coverage path 2                                     Page 1 of 1
                                COVERAGE PATH
                                Coverage Path Number: 1
                                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           y
  Don't Answer?             y           y           y   Number of Rings: 2
  All?                      n           n
  DND/SAC/Goto Cover?       y           y
  Holiday Coverage?         n           n
COVERAGE POINTS
  Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h2                Rng:2       Point2:
  Point3:                   Point4:
```

### 5.1.11. Administer a Station for Coverage to Avaya Aura® Messaging

Configure any and all phones that have a mailbox on the messaging server for call coverage. Use the command **change station <n>** where **n** is an extension and on **Page 1** for **Coverage Path 1** use the configured coverage path. In the example below station 52155 was configured to cover to messaging using cover path 2.

display station 52155	Page 1 of 5	
STATION		
Extension: 52155	Lock Messages? n	BCC: 0
Type: 96	Security Code: *	TN: 1
Port: S00024	<b>Coverage Path 1: 2</b>	COR: 1
Name: Nam Nam	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 52151	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

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

change station 52151		Page 2 of 5	
		STATION	
FEATURE OPTIONS			
LWC Reception: spe		Auto Select Any Idle Appearance? n	
LWC Activation? y		Coverage Msg Retrieval? y	
LWC Log External Calls? n		Auto Answer: none	
CDR Privacy? n		Data Restriction? n	
Redirect Notification? y		Idle Appearance Preference? n	
Per Button Ring Control? n		Bridged Idle Line Preference? n	
Bridged Call Alerting? n		Restrict Last Appearance? y	
Active Station Ringing: single			
		EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?		
Service Link Mode: as-needed		EC500 State: enabled	
Multimedia Mode: enhanced		Audible Message Waiting? n	
<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: 52151	Always Use? n IP Audio Hairpinning? n		

### 5.1.12. Configure SIP Endpoint

SIP endpoints and off-pbx-telephone stations will be automatically created in Communication manager when users (SIP endpoints) are created in Session Manager. Go to **Section 7.7** for steps on how to create SIP users on Session Manager. On the station form in Communication Manager, on the page 6 is a Third Party Call Control setting. Set value for **Type of 3PCC Enabled: Avaya**. This setup makes sure that ACE Notification service can send out the notification for SIP Phone.

change station 52152	Page 6 of 6
STATION	
SIP FEATURE OPTIONS	
<b>Type of 3PCC Enabled: Avaya</b>	
SIP Trunk: aar	

### 5.1.13. Configure Location

This section shows the steps to configure Outbound Proxy in the locations form. Use the command **change locations** to set the value for **Proxy Rte** to the route pattern that will go to Session Manager. During compliance test, route **5** is used.

change locations										Page 1 of 16
LOCATIONS										
ARS Prefix 1 Required For 10-Digit NANP Calls? y										
Loc Name	Timezone	DST	City/	ARS	Atd	Loc	Disp	Prefix	<b>Proxy</b>	Sel
No	Offset		Area	FAC	FAC	Parm	Parm		<b>Rte</b>	Pat
1: Main	+ 00:00	0				1	1		<b>5</b>	

## 5.2. Configure ASAI Link

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

- Verify License Permission.
- Configuring AE Services and ACE as an AE Services server.
- Configuring a CTI link.

### 5.2.1. Verify License Permission

To verify that the Communication Manager license has proper permissions for the features illustrated in these Application Notes, use the command **display system-parameters customer-options** to verify that the **Computer Telephony Adjunct Links** customer option is set to **y** on Page 3.

display system-parameters customer-options		Page 3 of 11
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	<b>Computer Telephony Adjunct Links? y</b>	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? n	DCS Call Coverage? y	
ASAI Link Plus Capabilities? n	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n		
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification? y	
ATM WAN Spare Processor? n	DS1 MSP? y	
ATMS? y	DS1 Echo Cancellation? y	
Attendant Vectoring? y		
(NOTE: You must logoff & login to effect the permission changes.)		

### 5.2.2. Configuring AE Services and Avaya Agile Communication Environment™ as an AE Service Server

Enabling AE Services refers to administering the transport link between Communication Manager and AE Services. In this procedure, you must enter a Local Port number. These values must match the Port value you will enter when creating ASAI service provider on ACE. Enter the **change ip-services** command. Complete Page 1 of the IP SERVICES form as follows:

- **Service Type:** Enter AESVCS.
- **Enabled:** Enter y.
- **Local Node:** Enter procr.
- **Local Port:** Accept the default (8765).

change ip-services		Page 1 of 3
IP SERVICES		
Service Type	Enabled	Local Node
AESVCS	y	procr
		Local Port
		8765
		Remote Node
		Remote Port

Complete Page 3 of the **ip-services** form as follows:

- In the **AE Services Server** field, type the name of the ACE Server, for example: DevACE.
- Enter **Password**, see note below.
- Set the **Enabled** field to y.

change ip-services		AE Services Administration			Page 3 of 3
Server ID	AE Services Server	Password	Enabled	Status	
1:	DevACE	DevConnect123	y	in use	

**Note:** In this procedure, the ACE server name and password must be entered. These values must match the ACE Server Name and Password values you will enter when adding the ASAI service provider on ACE.

### 5.2.3. Add a CTI link

In this procedure, you must enter a CTI Link number. This value must match the CTI Link No value you will enter when adding the ASAI service provider on ACE.

Add a CTI link using the **add cti-link n** command; where **n** is an available CTI link number. Complete the **CTI LINK** form as follows:

- Enter an available extension number in the **Extension** field.
- Enter **ADJ-IP** in the **Type** field.
- Enter a description for this link, example: **DevACE** in the **Name** field. Default values may be used in the remaining fields.

add cti-link 5	Page 1 of 3
CTI LINK	
CTI Link: 5	
Extension: 52100	
Type: ADJ-IP	
Name: DevACE	COR: 1

## 6. Configure Avaya Aura® Messaging

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

- Administer Sites
- Administer Telephony Integration
- Configure Dial Rules
- Configure Class of Service
- Administer Subscribers
- Administer Topology
- Administer External Host
- Recording Format
- Configure Notify Me for Avaya Aura® Messaging mailboxes.

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

## 6.1. Administer Sites

A Messaging access number and a Messaging Auto Attendant number needs to be defined. Log into the Messaging System Management Interface (SMI) and navigate to **Administration** → **Messaging** (not shown). In the left panel, under **Messaging System (Storage)** select **Sites**, click **Add New** (not shown). In the right panel fill in the following:

Under **Main Properties** enter the following:

- **Name:** Enter site name, example: **DevCM3**.
- **Internal Messaging access number:** Enter a Messaging Pilot number, during compliance test **39990** is used. Leave other fields as default value.

Below is detail of **Sites DevCM3** configured on Messaging.

**Sites**

Site: DevCM3 ▼

Add New... Delete

---

**Main Properties**

Name: DevCM3

ID: 3

Internal Messaging access number	External Messaging access number	Site Default Language	Additional Language	Additional Language
<span>39990</span>	<span>39990</span>	<span>English (United States)</span> <span>▼</span>	<span>None</span> <span>▼</span>	<span>None</span> <span>▼</span>

**Site External (Public Network) Dial Plan**

Describe the public telephony network dial plan applicable to this site.

Country code:

International prefix:

National prefix:

International dialing (to this country): Do not prepend National Prefix ▼

National destination code:

Dialing within national destination: Do not prepend National Prefix or National Destination code ▼

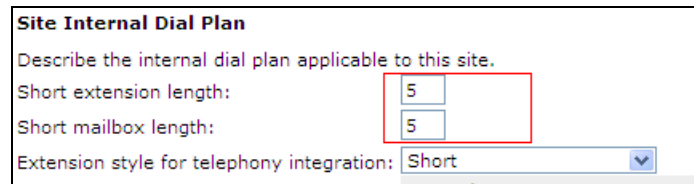
Subscriber number length (within this site's national destination code): 5



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

Under **Site Internal Dial Plan** enter the following:

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



Default values may be used in the remaining fields. Click **Save** (not shown) to save changes.

## 6.2. Administer Telephony Integration

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

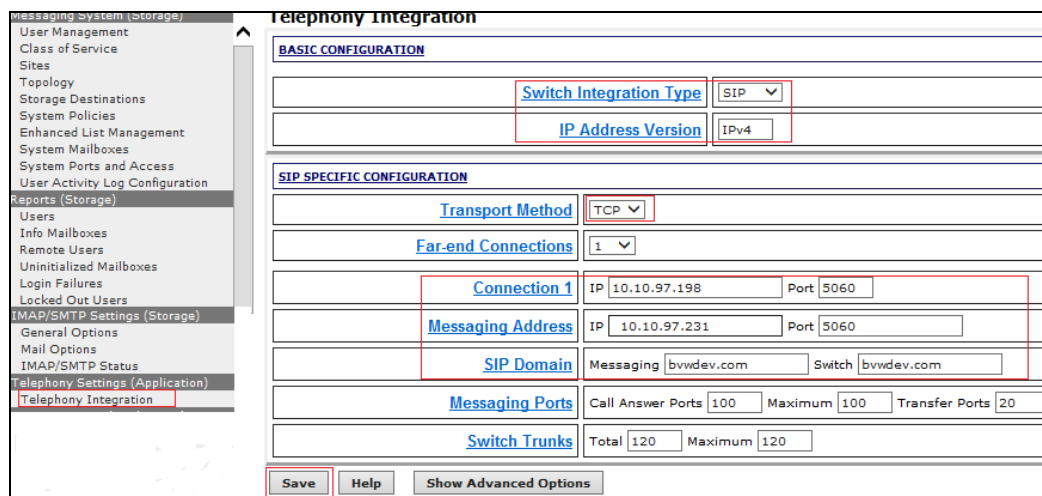
Under **Basic Configuration** enter the following:

- **Switch Integration Type:** Select **SIP**.
- **IP Address Version:** Accept default value **IPv4**.

Under **SIP Specific Configuration:**

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

Click **Save** to save changes.



### 6.3. Configure Dial Rules

Navigate to **Administration Messaging**→**Server Settings (Application)** → **Dial Rules** to configure the dial rules. Set the **Dial plan handling style** field to **Site definition based** as shown below.



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

**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

**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

## 6.4. Configure Class of Service

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

- **Dial-out privilege:** Select **Local**.
- **Set Message Waiting Indicator (MWI) on user’s desk phone** is checked.

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

## 6.5. Administer Subscribers

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

Under **User Properties**:

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

**User Management > Properties for Sau Ko**

**User Properties**

First name: Sau

Last name: Ko

Display name: Sau Ko

ASCII name: Ko, Sau

Site: DevCM3

Mailbox number: 52160

Internal identifier: Sau.Ko @DevAAM

Numeric address: 52160

Extension: 52160

☒ Include in Auto Attendant directory

Scroll down on the page to Class of Service.

- **Class of Service:** Select a Class of Service
- **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.

Class of Service:	Standard
Pronounceable name:	
MWI enabled:	Yes
Miscellaneous 1:	
Miscellaneous 2:	
New password:	•••••
Confirm password:	•••••
<input checked="" type="checkbox"/> User must change voice messaging password at next logon	
<input type="checkbox"/> Voice messaging password expired	
<input type="checkbox"/> Locked out from voice messaging	
Save	Delete

## 6.6. Administer Topology

Select **Topology** under **Messaging System (Storage)**. Verify the site **DevCM3** is **Active**.

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	

### Topology

#### Sites / Application Servers

Sites	Status
Default	Active
DevCM3	Active
WindstreamSonus	Active

Update Cancel

## 6.7. Administer External Host

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

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

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

### Change an Existing External Host

IP Address	168.62.
Host Name	interc.
Alias	

Back Save Help

## 6.8. Recording Format

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

The screenshot displays the Esna configuration web interface. On the left, a sidebar menu lists various configuration sections. The 'Miscellaneous' option under the 'Advanced (Application)' category is selected and highlighted with a red box. The main content area is titled 'Miscellaneous' and contains several configuration sections:

- Appliance-to-Appliance**: The 'Appliance-to-Appliance' setting is shown as 'enabled' with a selected radio button.
- System Parameters**: The 'Recording format' is set to 'GSM' (selected radio button, highlighted with a red box). Other options include 'G.711'. Below this, 'Maximum recorded name length' is set to '10' seconds, and 'Delete cached voice messages from the cache after' is set to '72' hours.
- Advanced Cache Configuration**: Includes a 'Show dirty cache' button.

At the bottom of the main panel, there are three buttons: 'Help', 'Apply', and 'Reset Page'.

## 6.9. Configure Notify Me for Avaya Aura® Messaging mailboxes

If there is a voice message left for Communication Manager Extension, this setting will allow Messaging to send a voice message as an email to appropriate iLink Pro user on Officelinx. Select **Administration** → **Messaging**. In the left panel, under **Messaging System (Storage)** select **User Management**. In the right panel enter mailbox number (e.g. 52160) and click **Edit** (not shown). Scroll right down to **User Preferences** at the bottom of the screen and select link **Open User Preference for Mailbox User name** (not shown).

In the **User Preferences** detail screen, select **Notify Me**. In the Notify Me detail page, enable checkbox **Email me a notification for each voice message** to iLink Pro user's email address configured on Officelinx; example during compliance test the following email is used [52160@Esna host name](mailto:52160@Esna host name) with the option **Include the recording**. Click Save. Below is an example set up for extension 52160.

aura.

User Preferences  
Notify Me

**Phone Notifications**

☐ Notify me when a new voice message arrives

☐ With a phone call to:

☒ With a text message or page to:

Mobile provider: Choose One

☐ Only for important messages

**Email Notifications**

☒ Email me a notification for each voice message

To email address: 52160@ESNA hostname

☒ Include the recording

Save



## 7. Configure Avaya Aura® Session Manager

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

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

In this section, the following topics are discussed:

- Configure SIP Domain
- Configure Locations
- Configure SIP Entities
- Configure Entity Links
- Configure Routing Policies
- Configure Dial Patterns
- Configure SIP Users

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

## 7.1. Configure SIP Domain

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

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

- **Name:** Enter the Authoritative Domain Name, **bvwdev.com** as configured in **Section 5.1.5**.
- **Type:** Select **SIP**.

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

Avaya Aura<sup>®</sup> System Manager 6.3

Last Logged on at August 30, 2013 2:50 PM  
Help | About | Change Password | Log off admin

Routing Domains Home

Home / Elements / Routing / Domains

Domain Management

Commit Cancel

1 Item Refresh Filter: Enable

Name	Type	Notes
bvwdev.com	sip	The main domain

Commit Cancel

## 7.2. Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing. Navigate to **Routing** → **Locations**, and click on the **New** button (not shown) to create a new SIP endpoint location.

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

- **Name:** Enter a descriptive Location name.
- **Note:** Enter a description if desired.

Home / Elements / Routing / Locations

Location Details

Commit Cancel

General

\* Name: Belleville

Notes: Belleville DevConnect Location

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

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

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

The following screen shows the Locations page used during the compliance test. Click on the **Commit** button.

Location Pattern

Add Remove

5 Items Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.33.5.0	IP Phone Net 10.33.5.0
<input type="checkbox"/>	* 10.10.97.0	
<input type="checkbox"/>	* 10.10.98.0	IP Phone Net 10.10.98.0
<input type="checkbox"/>	* 10.20.0.0	
<input type="checkbox"/>	* 10.10.169.*	For remote access site

Select : All, None

Commit Cancel

### 7.3. Configure SIP Entities

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

- Session Manager.
- Communication Manager.
- Messaging.
- Esna Officelinx.

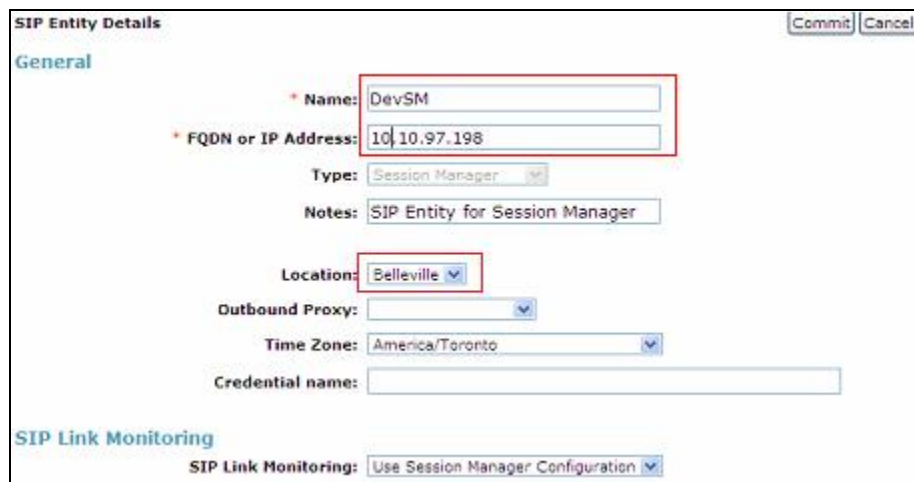
Navigate to **Routing → SIP Entities**, and click on the **New** button (not shown) to create a new SIP entity. Enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name in the **Name** field.
- **FQDN or IP Address:** Enter IP address of SIP Entity that used for SIP signaling. Enter IP address of Communication Manager, Session Manager, Messaging and Esna Officelinx.
- **Type:** 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.
- **Note:** Enter a description if desired.
- **Location:** Select the appropriate location.

Accept the other default values or modify them if needed.

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

#### Session Manager SIP Entity:



The screenshot shows the 'SIP Entity Details' form with the 'General' tab selected. The form contains the following fields and values:

- Name:** DevSM
- FQDN or IP Address:** 10.10.97.198
- Type:** Session Manager (dropdown menu)
- Notes:** SIP Entity for Session Manager
- Location:** Belleville (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** America/Toronto (dropdown menu)
- Credential name:** (empty text field)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)

The 'Commit' and 'Cancel' buttons are located in the top right corner of the form.

## Communication Manager SIP Entity:

**SIP Entity Details** Commit Cancel

**General**

\* Name: DevCM3

\* FQDN or IP Address: 10.33.4.9

Type: CM

Notes: Phuong CM

Adaptation:

Location: Belleville

Time Zone: America/New\_York

Override Port & Transport with DNS SRV: ☐

\* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

**Loop Detection**

Loop Detection Mode: Off

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

## Avaya Aura® Messaging SIP Entity:

**SIP Entity Details** Commit Cancel

**General**

\* Name: DevAAM

\* FQDN or IP Address: 10.10.97.231

Type: Modular Messaging

Notes: Avaya Aura Messaging SIP Entity

Adaptation:

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

\* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

**Loop Detection**

Loop Detection Mode: Off

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

## Esna Officelinx SIP Entity:

**SIP Entity Details** Commit Cancel

**General**

\* Name: ESNA

\* FQDN or IP Address: 16

Type: Other

Notes: ESNA Office LinX

Adaptation:

Location: Belleville

Time Zone: America/New\_York

Override Port & Transport with DNS SRV: ☐

\* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

**Loop Detection**

Loop Detection Mode: Off

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

## 7.4. Configure Entity Links

Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test 2 entities links are defined: one to Communication Manager (Avaya G450 with S8300D Server) and one to Messaging. To add an entity link, navigate to **Routing → Entity Links**, and click on the **New** button (not shown) to create a new entity link. Enter the following information:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select first SIP entity from drop down menu, Session Manager's SIP entity is selected.
- **Protocol:** Select the protocol to be used from the drop down menu.
- **Port:** By default the value will be set to **5060** for **TCP**.
- **SIP Entity 2:** Select appropriated entity.
- **Port:** By default the value will be set to **5060** for **TCP**.
- **Connection Policy:** Select **Trusted** option.

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

Avaya Aura System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
* DevSM_DevAAM_5	* DevSM	TCP	* 5060	* DevAAM	* 5060	trusted	<input type="checkbox"/>	

Select : All, None

Entity Link page (between Session Manager - Communication Manager):  
**DevSM\_DevCM3\_62\_5061\_TLS.**

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
* DevSM_DevCM3_6	* DevSM	TLS	* 5061	* DevCM3_62	* 5061	trusted	<input type="checkbox"/>	

Select : All, None

Entity Link page (between Session Manager – Esna Officelinx): **DevSM\_Esna\_5060\_TCP**.

## 7.5. Configure Routing Policies

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

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

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



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

Routing Policy Details

Commit

Cancel

General

\* Name:

Route-To-DevAAM

Disabled:

☐

\* Retries:

0

Notes:

Route to DevAAM Messaging

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
DevAAM	10.10.10.231	Modular Messaging	Avaya Aura Messaging SIP Entity

Routing policy used for Esna Officelinx: **Route\_to\_Esna**.

Routing Policy Details

Commit

Cancel

General

\* Name:

Route\_to\_ESNA

Disabled:

☐

\* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ESNA	168.159.1.84	Other	ESNA Office LinX

## 7.6. Configure Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In addition, the domain in the request URI is also examined. In the compliance test, the following dial patterns are defined from Session Manager.

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

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

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

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

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

**Dial Pattern Details** [Commit] [Cancel]

**General**

\* Pattern: 521

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: bwvdev.com

Notes: Dialing Plan for DevCM3 system

**Originating Locations and Routing Policies**

[Add] [Remove]

1 Item | Refresh Filter: Enable

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

## Dial Pattern for Messaging: 399.

Dial Pattern Details

CommitCancel

General

\* Pattern: 399

\* Min: 5

\* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwddev.com

Notes: Dial Pattern for DevAAM system to DevCM3

Originating Locations and Routing Policies

AddRemove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	Belleville DevConnect Location	Route-To-DevAAM	0	<input type="checkbox"/>	DevAAM	Route to DevAAM Messaging

Filter: Enable

## Dial Pattern for Esna Officelinx: 782.

Dial Pattern Details

CommitCancel

General

\* Pattern: 782

\* Min: 5

\* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwddev.com

Notes: Route to ESNA

Originating Locations and Routing Policies

AddRemove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	Belleville DevConnect Location	Route_to_ESNA	0	<input type="checkbox"/>	ESNA	

Filter: Enable

Select : All, None

## 7.7. Configure SIP Users

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

### Identity tab:

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

The screenshot shows the 'New User Profile' form with the 'Identity' tab selected. The form contains the following fields:

- Last Name:** Text input field with the value 'Nam'.
- First Name:** Text input field with the value 'Ba'.
- Middle Name:** Text input field (empty).
- Description:** Text area (empty).
- Login Name:** Text input field with the value '52153@bvwdev.com'.
- Authentication Type:** Dropdown menu with 'Basic' selected.
- Password:** Password input field (masked with dots).
- Confirm Password:** Password input field (masked with dots).

Red boxes highlight the 'Last Name', 'First Name', 'Login Name', 'Authentication Type', 'Password', and 'Confirm Password' fields.

In the Communication Profile tab, under Communication Profile section enter the **Communication Profile Password**, enter numeric password which is used to log into the device.

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

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

The screenshot shows a web-based configuration interface with four tabs: Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' tab is active and marked with a red asterisk. Below the tabs, there is a section titled 'Communication Profile' with a dropdown arrow. Under this section, there are two password fields: 'Communication Profile Password:' and 'Confirm Password:', both containing six dots. Below the password fields are four buttons: 'New', 'Delete', 'Done', and 'Cancel'. A table below the buttons has a header 'Name' and one row with a green circle icon and the text 'Primary'. Below the table is a 'Select : None' option. At the bottom, there is a red asterisk followed by 'Name:' and a text box containing 'Primary'. Below that is 'Default : ☒'. The entire form area is outlined with an orange border.

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

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

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

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

- **Primary Session Manager:** Select the Session Managers of interest.
- **Origination Application Sequence:** Select Application Sequence for Communication Manager.
- **Termination Application Sequence:** Select Application Sequence for Communication Manager.
- **Home Location:** Select Location created above.

**Communication Address**

New Edit Delete

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

Select : All, None

☒ **Session Manager Profile**

\* Primary Session Manager
DevASM

Primary
Secondary
Maximum

40
0
40

Secondary Session Manager
( None )

Primary
Secondary
Maximum

Origination Application Sequence
DevCM3\_G450\_Seq

Termination Application Sequence
DevCM3\_G450\_Seq

Survivability Server
( None )

\* Home Location
Belleville

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

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

☒ **Endpoint Profile**

\* **System** DevCM3

\* **Profile Type** Endpoint

Use Existing Endpoints ☐

\* **Extension** 52153 Endpoint Editor

**Template** Select/Reset

**Set Type** 9640SIP

**Security Code** .....

\* **Port** 500026

**Voice Mail Number**

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

Click **Commit** (not shown) to save the definition of the new user. The following screen shows the created users during the compliance test.

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

## 8. Configure Avaya Agile Communication Environment™ 6.2

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

### 8.1. Configuring the Communication Manager's SSL certificate Signing Authority as Trusted on Avaya ACE

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

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

If Communication Manager is configured with a server certificate signed by such an authority, then no further configuration is needed on ACE. Skip this section and move to **Section 8.2**. If Communication Manager is not configured with a server certificate that is signed by such an authority, then further configuration may be needed on ACE. Please see “Configuring the Communication Manager's SSL certificate signing authority as trusted on ACE” in **Reference Section 12**.



## 8.2. Add ASAI Service Provider

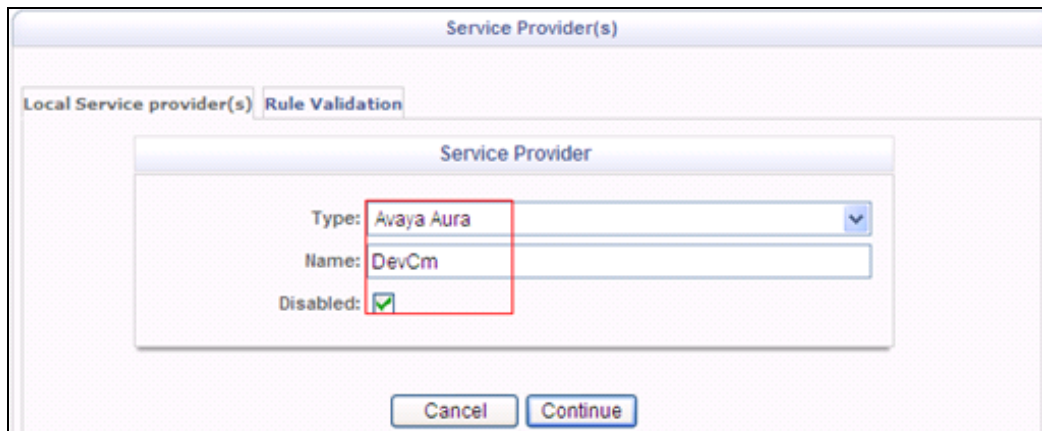
This section creates ASAI Service Provider which provides web services Third Party Call Control v2 and v2.4, such as make call, Single Step Transfer or hang up call.

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

On the menu bar, choose **Configuration → Service Providers**. In the Service Providers window, click **Add** (not shown) and enter the following information:

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

Click **Continue**.



The screenshot shows a web-based configuration interface. At the top, there is a tabbed window titled "Service Provider(s)". Inside, there are two tabs: "Local Service provider(s)" and "Rule Validation". The "Local Service provider(s)" tab is active. Within this tab, there is a "Service Provider" dialog box. This dialog box contains three fields: "Type" with a dropdown menu showing "Avaya Aura", "Name" with a text input field containing "DevCm", and "Disabled" with a checked checkbox. At the bottom of the dialog box, there are two buttons: "Cancel" and "Continue".

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

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

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

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

Click **Next** to add **Rules** for ASAI service provider. Below is example of ASAI Service Provider created and used in compliance test.

The screenshot shows the 'Service Provider(s)' configuration window for 'Avaya Aura : DevCm'. It has two tabs: 'Local Service provider(s)' and 'Rule Validation'. The 'Local Service provider(s)' tab is active, showing two sections: 'Signaling' and 'Address'.

**Signaling Section:**

- Signaling: ASAI
- Transport: TLS
- FQDN/IP Address: 10.33.4.9
- Port: 8765
- Priority: 0

**Address Section:**

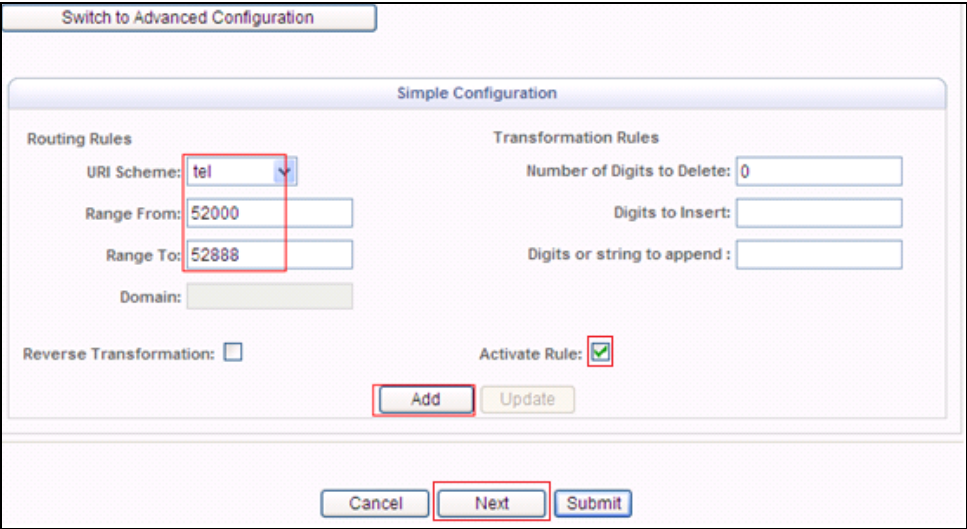
- ACE Server Name: DevACE
- Password: [Masked]
- CTI Link No: 5

At the bottom, there are three buttons: 'Cancel', 'Previous', and 'Next'. The 'Next' button is highlighted with a red border.

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

- **URI Scheme:** Select **tel** from the drop-down menu.
- **Range from:** Enter a dialling plan for Communication Manager; example: **52000**.
- **Range to:** Enter a dialling plan for Communication Manager; example: **52888**.
- **Activate Rule:** checked.

Click **Add** to add the new rule. Click **Next** to add rule for Called Party



The image shows a 'Simple Configuration' dialog box for a 'Calling Party Translation Rule'. At the top left is a button labeled 'Switch to Advanced Configuration'. The dialog is divided into two main sections: 'Routing Rules' on the left and 'Transformation Rules' on the right. Under 'Routing Rules', there is a 'URI Scheme' dropdown menu with 'tel' selected, a 'Range From' text box containing '52000', a 'Range To' text box containing '52888', and a 'Domain' text box. Under 'Transformation Rules', there is a 'Number of Digits to Delete' text box containing '0', a 'Digits to Insert' text box, and a 'Digits or string to append' text box. At the bottom left of the dialog is a 'Reverse Transformation' checkbox, which is unchecked. At the bottom right is an 'Activate Rule' checkbox, which is checked. Below these checkboxes are two buttons: 'Add' and 'Update'. At the very bottom of the dialog are three buttons: 'Cancel', 'Next', and 'Submit'. Red rectangular boxes highlight the 'URI Scheme' dropdown, the 'Range From' and 'Range To' text boxes, the 'Add' button, and the 'Next' button.

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

- **URI Scheme:** Select **tel** from the drop-down menu.
- **Range from:** Enter a dialling plan for Communication Manager; example: **52000**.
- **Range to:** Enter a dialling plan for Communication Manager; example: **52888**.
- **Activate Rule:** checked.

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

Local Service provider(s) Rule Validation

Translation Rule for Service Provider -- Avaya Aura : DevCm

**Called Party Translation Rule**

Type	Rules	Reverse Transformation	Rule Active
Simple	URIScheme=tel,RangeFrom=52000,RangeTo=52888,Delete Digit=0,	No	Yes

Up Down Remove

Switch to Advanced Configuration

**Simple Configuration**

Routing Rules

URI Scheme: tel

Range From: 52000

Range To: 52888

Domain:

Reverse Transformation: ☐

Transformation Rules

Number of Digits to Delete: 0

Digits to Insert:

Digits or string to append:

Activate Rule: ☒

Add Update

Cancel Previous Submit

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

Service Provider(s)

Local Service provider(s) Rule Validation

5 Service Provider(s)

No	Name	Type	Signaling	FQDN/IP Address	Port	Terminals Addresses	Rules	Provider Status
1	DevCm	Avaya Aura	ASAI	10.33.4.9	8765	N/A	N/A	In Service

Up Down

### 8.3. Add User

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

Select **Security → User Management → Create User** (not shown).

- **User ID:** Enter user name that is used to login ACE web service of the web client (application) (e.g **ESNA\_Admin**), this account is used by ESNA UCACEWizard application described in Section 9.2.
- **Account State:** Select Enable from the drop-down menu.
- **User Password:** Enter the password for user (e.g DevConnect@123).
- **Confirm User Password:** Re-enter above password to confirm.

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

The screenshot shows a web application window titled "Edit User". The window has a tabbed interface with tabs for "User", "Personal Data", "Organization Data", "Preferences", "Role Membership", and "Account Policy". The "User" tab is currently selected. The form displays the following information:

- User ID:** ESNA\_Admin
- Account State:** Enabled (dropdown menu)
- Authentication Type:** INTERNAL (dropdown menu)
- User Password:** [masked with dots]
- Confirm User Password:** [masked with dots]
- ☐ User must change password at next logon
- Creation Date:** 2013-11-12 14:47:11.463 -0500
- Last Login Date:** 2014-01-08 15:56:15.841 -0500
- Password Expiration Date:** Never
- Account Dormant Date:** 2014-04-08

At the bottom of the form are three buttons: "Submit", "Reset", and "Back".

## 8.4. Add Role

This section describes the steps on how to create Roles for users created in the above section. Select **Security → Role Management → Create Role** (not shown). Enter the following for a new Role:

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

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

The screenshot displays a web-based interface for managing roles. At the top, a header bar labeled 'Role' contains the role name 'ESNA\_Admin' and its creation date '2013-11-12 14:45:49.625 -0500'. Below this is a section titled 'Membership Information' with a tab labeled 'Users'. The interface is divided into two main panels: 'Available Users (User ID)' on the left and 'Role Members' on the right. The 'Available Users' panel lists 'admin', 'federation', 'sysmonitor', 'trustedUser', and 'User3'. The 'Role Members' panel lists 'ESNA\_Admin', 'User1', and 'User2'. Between the panels are two buttons: '>>' and '<<'. At the bottom of each panel is a 'View User' link. At the very bottom of the interface are three buttons: 'Submit', 'Reset', and 'Back'.

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

The screenshot shows the 'Membership Information' window with the 'License Membership' tab selected. The 'Available Licenses' list is empty, and the 'Member Licenses' list contains 'API Integration Suite'. Below this, the 'Role Policy' section is visible, showing 'Access Control Rules' for the 'API Integration Suite' application. A table lists various services and their access levels.

Application name	Service Name	Access Level
API Integration Suite	AudioCallService	OFF
	CallForwardingService	OFF
	CallHistoryService	OFF
	CallNotificationService	ON
	LocationSupplierService	OFF
	Long Duration Presence	OFF
	MessagingService	ON
	MultimediaMessagingService	OFF
	PresenceConsumerService	OFF
	PresenceSupplierService	OFF
	TerminalLocationService	OFF
	ThirdPartyCallService	ON
	TurretService	OFF

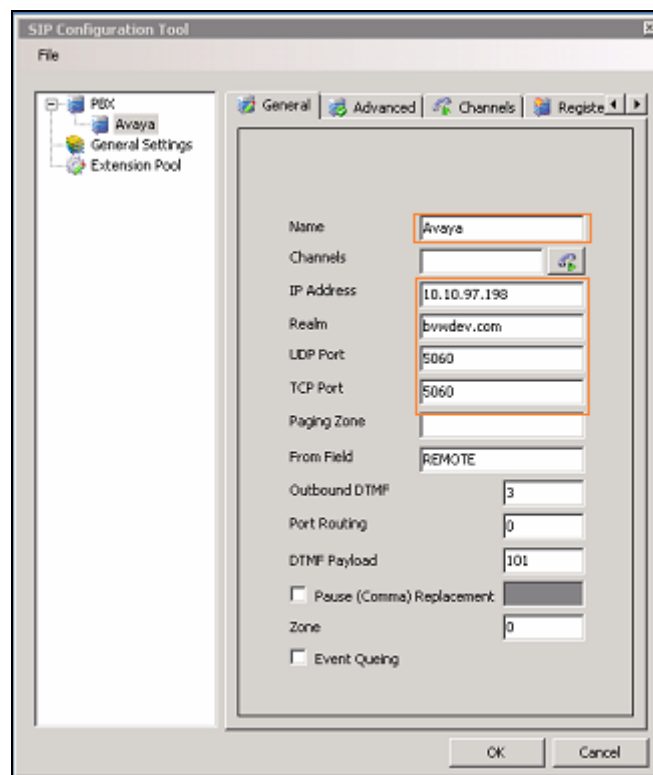
## 9. Configure the Esna Telephony Officelinx

Esna installs, configures, and customizes the Telephony Officelinx application for their customers. Thus, this section only describes the interface configuration, so that the Telephony Officelinx can talk to Session Manager, ACE and Messaging. See OL\_CLIENT\_APPS\_GUIDE and OL\_FEATURE\_DESCRIPTION\_GUIDE provide on the Esna website, see **Section 12** for the detailed link.

### 9.1. Configure SIP Configuration Tool

To configure Esna Telephony Officelinx, navigate to **Start → All program → Telephony Officelinx Enterprise Edition → SIP Configuration Tool** (not shown). Select **Avaya** under PBX in the left pane. Enter the following information:

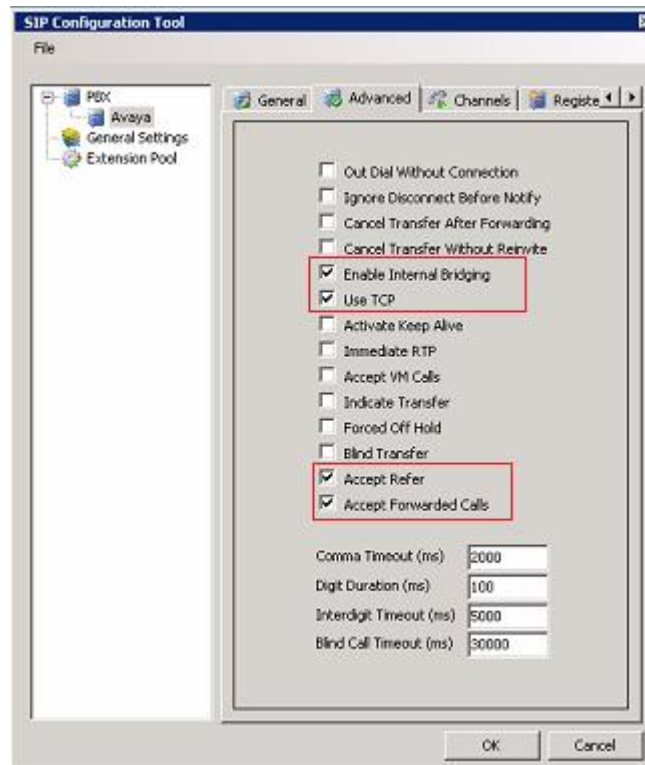
- **IP Address:** Enter the **IP address** of the **Session Manager**, example: 10.10.97.198.
- **Realm:** Enter a valid domain that is configured for the system, example: bvwdev.com.
- **UDP Port:** Enter **5060**.
- **TCP Port:** Enter **5060**.



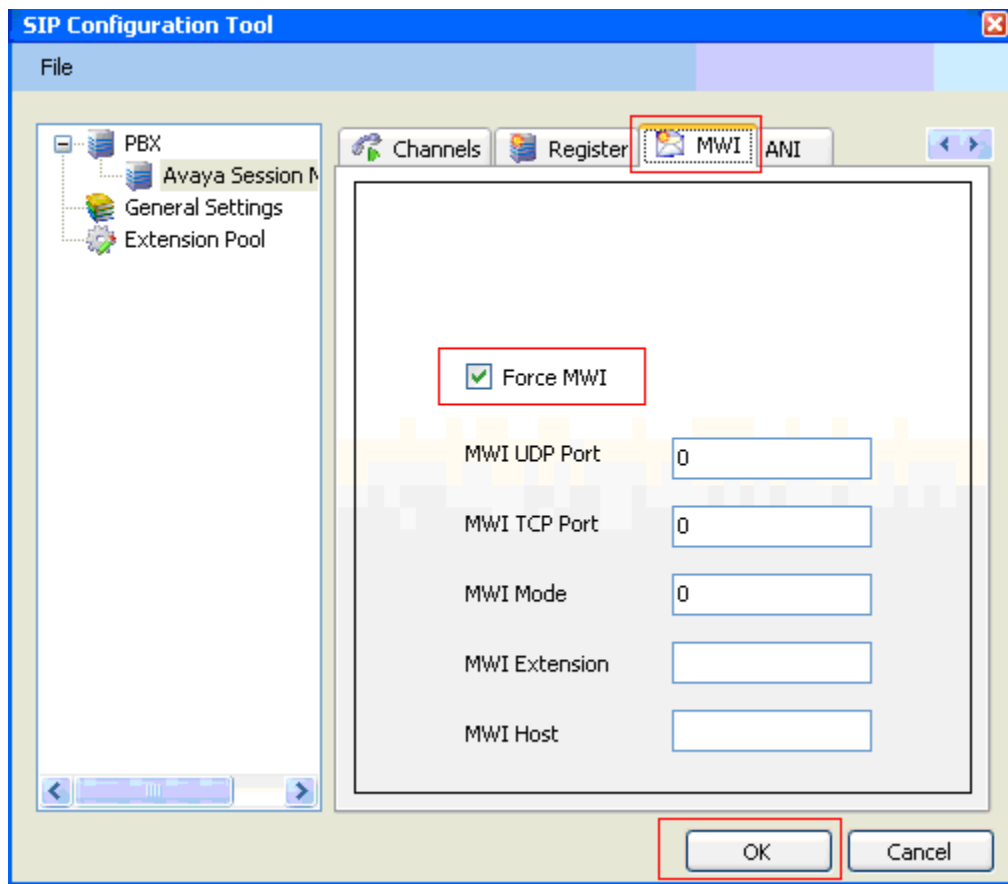


Click the **Advanced** tab in the right pane, and check the following check boxes:

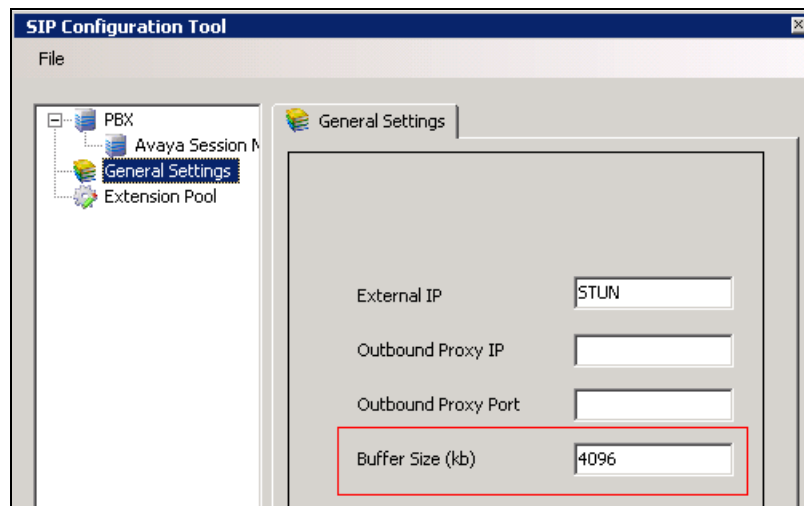
- Enable Internal Bridging.
- Use TCP.
- Accept Refer.
- Accept Forward Calls.



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



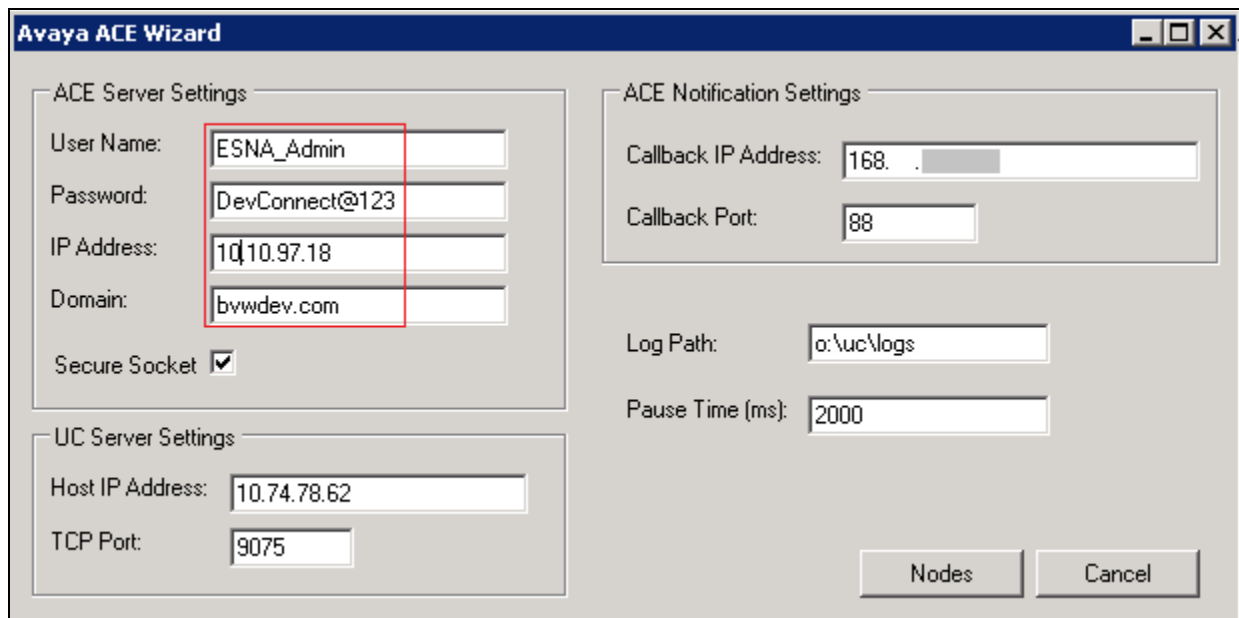
Navigate to **PBX → General Settings** and enter **Buffer Size (kb) =4096**. This configuration allows Officelinx to handle SIP messages sent from Session Manager.



## 9.2. Configure UC ACE Wizard

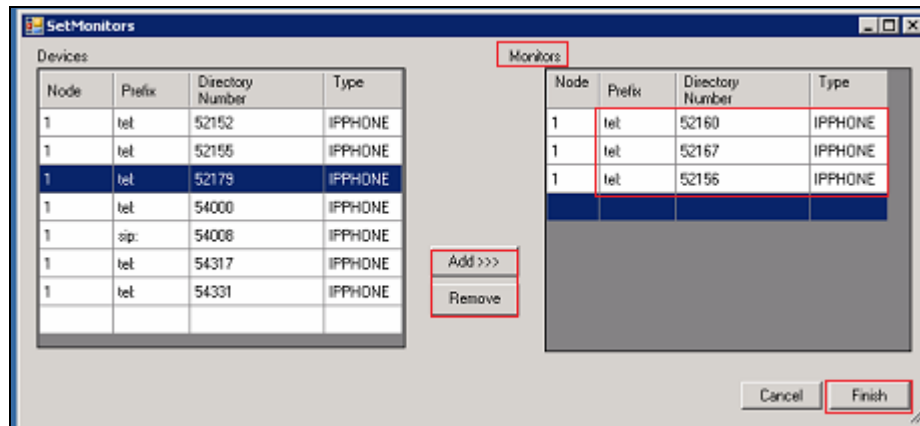
Double click on UC ACE Wizard shortcut to launch the setup window for Avaya ACE Wizard. Enter information as below:

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



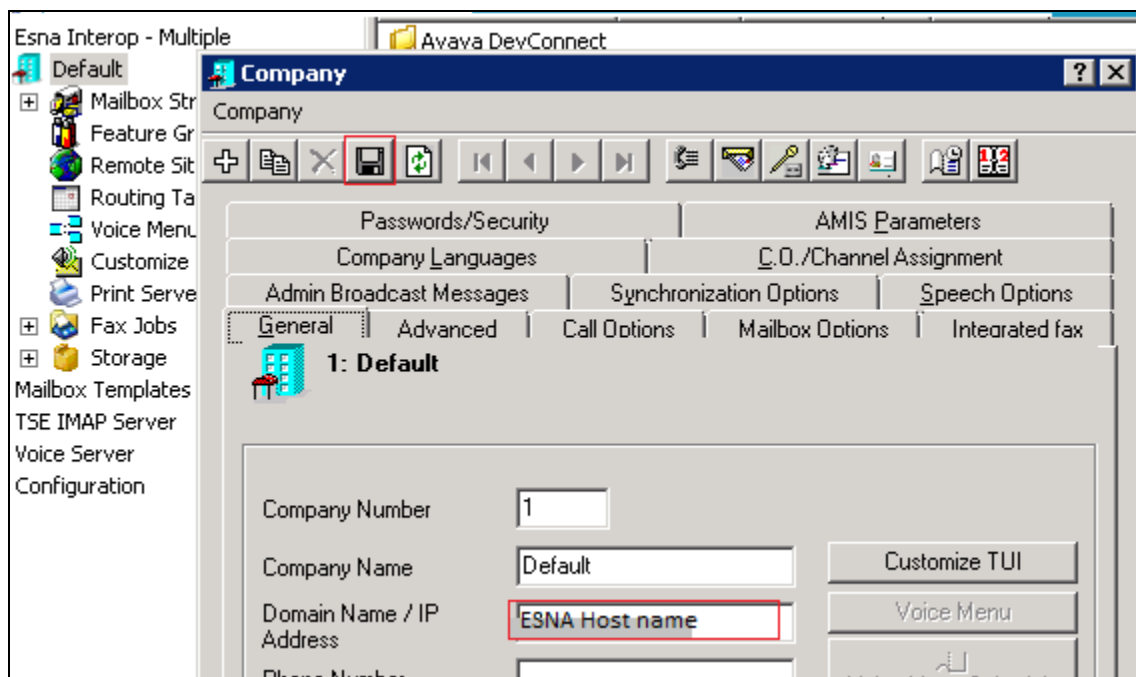
Click on **Nodes** (shown in previous screen shot) to open the next window, where the user manually enters the device extension to get its notification. Click on the **Next button** (not shown).

Select the list of device on the leftside and add it to the right window to start to monitor it. Or the user can remove the device from the monitor list by highlighting the device and click remove. Click **Finish** after complete to save changes.



### 9.3. Administer Company Profiles

In Officelinx, right click on **Default** node, select **Properties**. In the **Company** window, enter the **Domain Name/IP Address** in FQDN format. This domain name is used in **Section 6.9** to configure **Notify Me on Messaging**. Click **Save** to save all changes if needed.



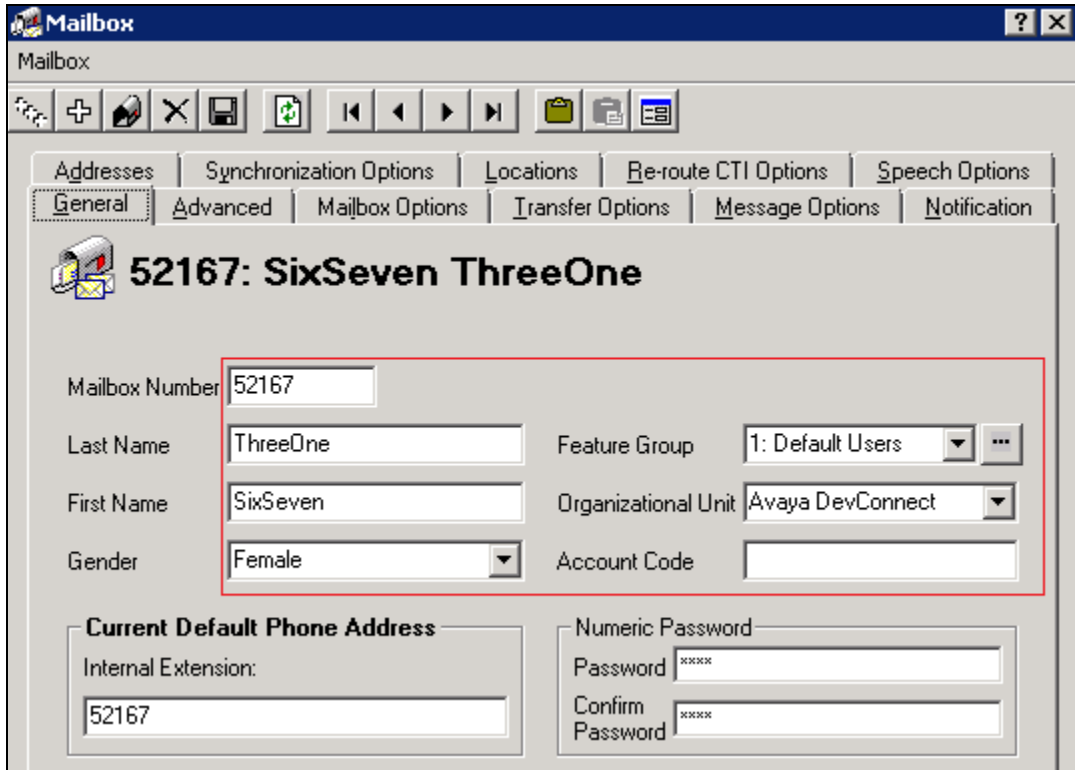
## 9.4. Configure User Mailbox in Officelinx Admin

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

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

In **General** tab enter the following:

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



**Mailbox**

Mailbox

Addresses | Synchronization Options | Locations | Re-route CTI Options | Speech Options

**General** | Advanced | Mailbox Options | Transfer Options | Message Options | Notification

**52167: SixSeven ThreeOne**

Mailbox Number: 52167

Last Name: ThreeOne

First Name: SixSeven

Gender: Female

Feature Group: 1: Default Users

Organizational Unit: Avaya DevConnect

Account Code:

**Current Default Phone Address**

Internal Extension: 52167

**Numeric Password**

Password:

Confirm Password:

In **Advanced** tab enter the following:

- **Domain Account Name:** Enter **Gmail account** which connects to this mailbox dev02.
- **Desktop Capabilities:** Select **Unified Communications**.

The screenshot shows the 'Mailbox' configuration window with the 'Advanced' tab selected. The window title is 'Mailbox'. Below the title bar is a toolbar with various icons. The tabs at the top are: Addresses, Synchronization Options, Locations, Re-route CTI Options, Speech Options, General, Advanced (selected), Mailbox Options, Transfer Options, Message Options, and Notification. The main content area is titled '52167: SixSeven ThreeOne'. It contains several configuration fields and checkboxes. The 'Domain Account Name' field is highlighted with a red box and contains the text 'dev02@'. The 'Desktop Capabilities' dropdown menu is also highlighted with a red box and shows 'Unified Communications' selected. Other fields include 'Personal Operator', 'D.I.D Trunk', 'Customize TUI', 'Voice Menu', 'Collect Geo Location Data', 'Date Format' (set to 'YYYYMMDD'), and 'PBX Node'. There are also buttons for 'Distribution Lists', 'Folders', 'Directory Listing', and 'Workgroup'.

Mailbox

Mailbox

Addresses | Synchronization Options | Locations | Re-route CTI Options | Speech Options

General | **Advanced** | Mailbox Options | Transfer Options | Message Options | Notification

**52167: SixSeven ThreeOne**

Personal Operator  ☒ Web Client User

D.I.D Trunk

☐ Customize TUI

☐ Voice Menu

☐ Collect Geo Location Data

Domain Account Name

Desktop Capabilities

Date Format

PBX Node

Distribution Lists

Folders

Directory Listing

Workgroup

In **Synchronization Options** tab enter the following:

- **Use Feature Group setting for IMAP:** make sure this option is checked.
- **User Name:** Enter google email account, example **dev02@googleaccount.com**.
- **Storage Mode:** Select **IMAP**.
- **Voice Format:** Select **MPEG-1 Audio layer 3 (MP3)**.
- **E-mail:** Enter the google email account.

Click Save icon to save the configuration.

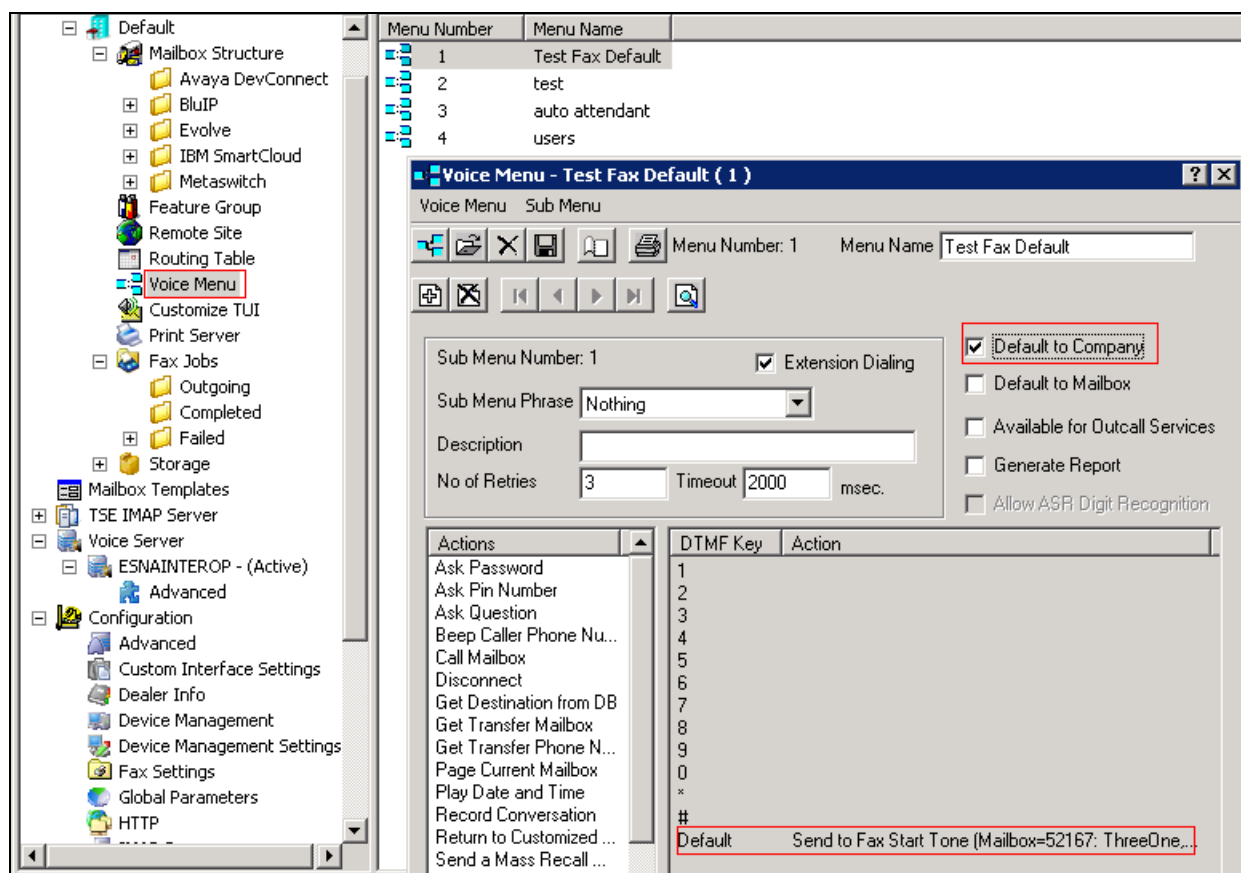
The screenshot shows the 'Mailbox' configuration window with the 'Synchronization Options' tab selected. The window title is 'Mailbox'. The tab bar includes: General, Advanced, Mailbox Options, Transfer Options, Message Options, Notification, Addresses, Synchronization Options (selected), Locations, Re-route CTI Options, and Speech Options. The main content area shows the configuration for mailbox '52167: SixSeven ThreeOne'. A red rectangle highlights the following fields:

<input checked="" type="checkbox"/> Use Feature Group settings for IMAP	<input type="checkbox"/> IMAP Locked
User Name: dev02@	IMAP Language: [dropdown]
User Password: [text box]	Storage Mode: IMAP [dropdown]
Confirm Password: [text box]	Voice Format: MPEG-1 Audio Layer [dropdown]
IMAP Server: [dropdown]	E-mail: dev02@

## 9.5. Configure Fax

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

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



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



## 9.6. Install and Configure iLink Pro on Salesforce.com

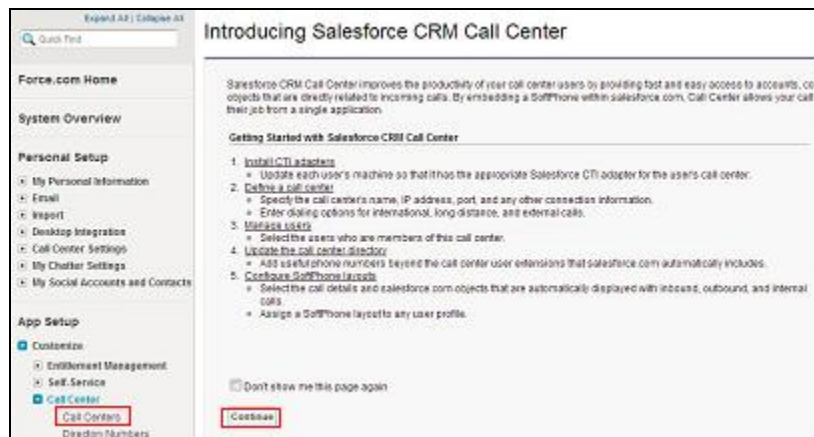
This section describes the steps needed to install and operate iLink Pro on Salesforce.

### 9.6.1. Install open CTI Integration

iLink Pro can be installed as a plugin to the Salesforce CRM program. This provides users with contact, presence, and call management functions directly within Salesforce. It is assumed that all the proper and necessary configurations have been setup by the Esna technician. Login to Salesforce using an account with site administrator credentials. Click on the **Setup** button.



Navigate to **App Setup**→**Customize**→**Call Center**→ **Call Centers** and click **Continue**.



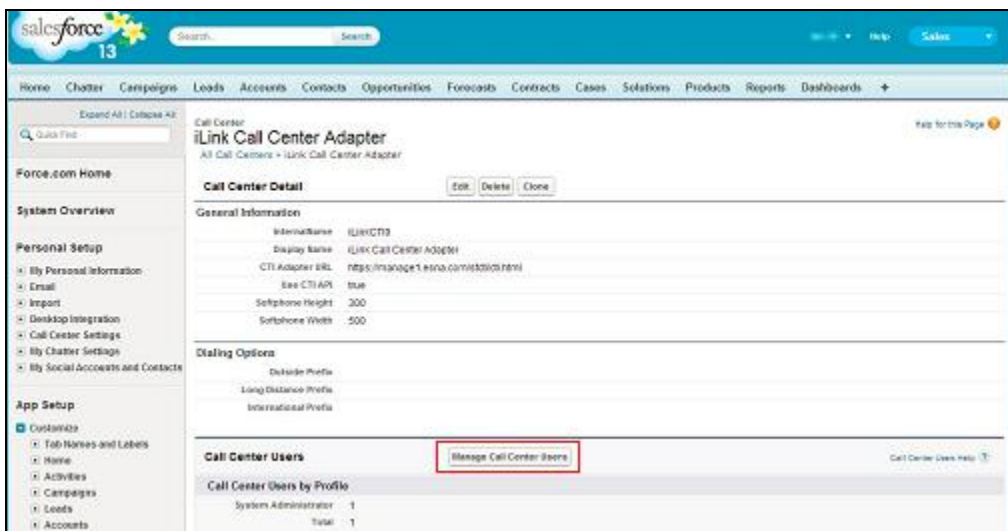
In the **All Call Centers** window, click **Import**.



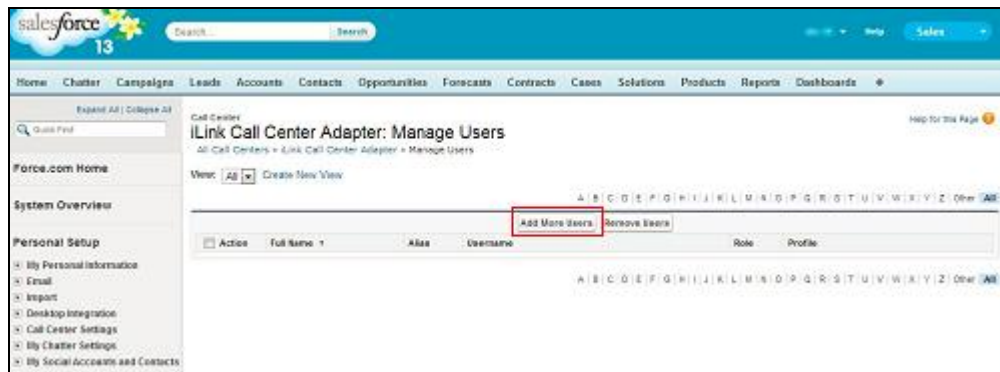
Click **Choose File**, and select the **Call Center Definition** file created in Section 9.6.2. With that file selected, click **Import** (not shown). Returning to the **All Call Centers** window, choose the newly created **Call Center** and click **Edit**.



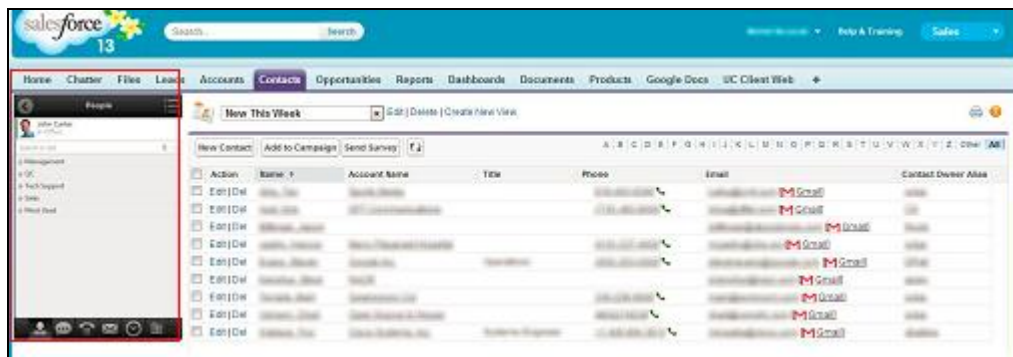
Click **Manage Call Center Users** to add clients to the new call center.



Click **Add More Users**. Add all of the required users to the list. Once all of the users have been added, click **Add to Call Center** (not shown).



Integration is now complete. Once it becomes available, clients will need to go to the Chrome web store (<https://chrome.google.com/webstore>) to download iLink Pro. Once that has been installed, you will have UC functionality available within Salesforce.



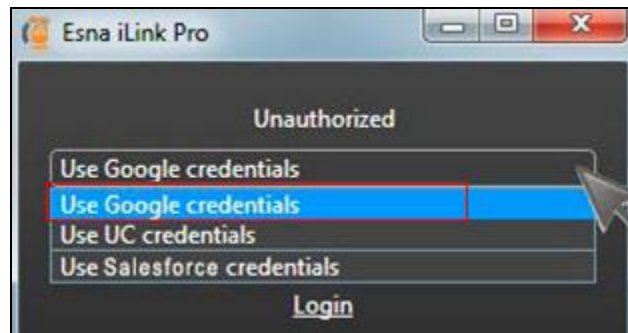
## 9.6.2. Call Center Definition

The following text will be imported into Salesforce to setup the integration in Section 9.6.1. Use any text editor (e.g. Notepad) to create the file and save it in the TXT format. Type the following into the appropriate file:

```
<callCenter> <section sortOrder="0" name="reqGeneralInfo" label="General Information">
<item sortOrder="0" name="reqInternalName" label="InternalName">iLinkCTI9</item> <item
sortOrder="1" name="reqDisplayName" label="Display Name">iLink Call Center
Adapter</item> <item sortOrder="2" name="reqAdapterUrl" label="CTI Adapter
URL">https://manage1.esna.com/sfcti/cti.bridge.html</item> <item sortOrder="3"
name="reqUseApi" label="Use CTI API">>true</item> <item sortOrder="4"
name="reqSoftphoneHeight" label="Softphone Height">300</item> <item sortOrder="5"
name="reqSoftphoneWidth" label="Softphone Width">500</item> </section> <section
sortOrder="1" name="reqDialingOptions" label="Dialing Options"> <item sortOrder="0"
name="reqOutsidePrefix" label="Outside Prefix"></item> <item sortOrder="1"
name="reqLongDistPrefix" label="Long Distance Prefix"></item> <item sortOrder="2"
name="reqInternationalPrefix" label="International Prefix"></item> </section> </callCenter>
```

### 9.6.3. Login iLink Pro on Salesforce.com

When launching iLink Pro from within Salesforce, the login screen provides a third option. The client can now select **Use Salesforce credentials** in addition to the Google and UC credentials.



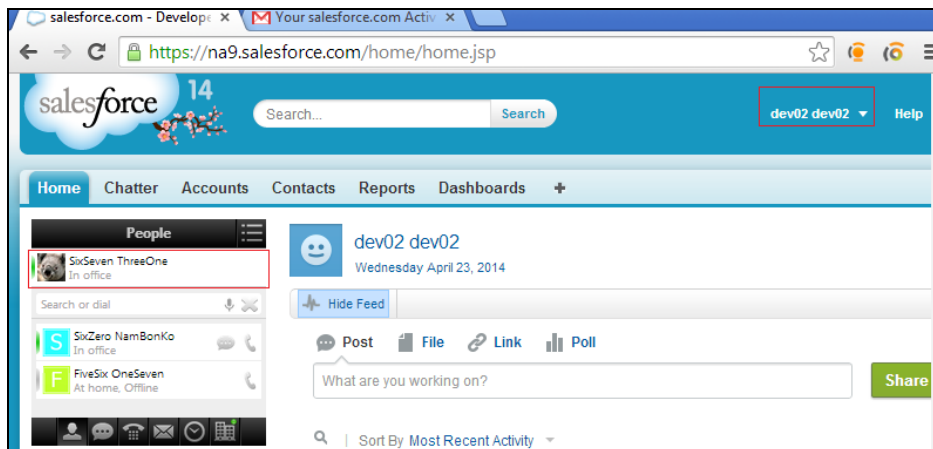
Google credentials are still preferred, but the Salesforce login is provided for sites where this is not an option.

Enter your Salesforce **User Name** and **Password** in the spaces provided.

Click **Log in to Salesforce** to launch the plugin.

A screenshot of the Salesforce login page. The page has a light gray background. At the top center is the 'salesforce' logo. Below the logo are two stacked input fields: the top one is labeled 'User Name' and the bottom one is labeled 'Password'. Below these fields is a prominent blue button with the text 'Log in to Salesforce'. At the bottom of the page, there is a checkbox labeled 'Remember User Name' and a link that reads 'Forgot your password? | Sign up for free.'

Below is the screenshot of a user **dev02**, created in Section 9.4, successfully logging into iLink Pro on Salesforce.



## 10. Verification Steps

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

### 10.1. Verify Avaya Aura® Communication Manager

The following steps may be used to verify the configuration:

- From the Communication Manager SAT, use the **status signaling-group xxx** command to verify that the SIP signaling group is **in-service** (not shown).
- From the Communication Manager SAT, use the **status trunk-group xxx** command to verify that the SIP trunk group is **in-service** (not shown).
- Verify with the **list trace tac xxx** command that calls are using the correct trunk, coverage (not shown).
- 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	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
5	4	no	DevACE	established	15	15
8		no		down	0	0

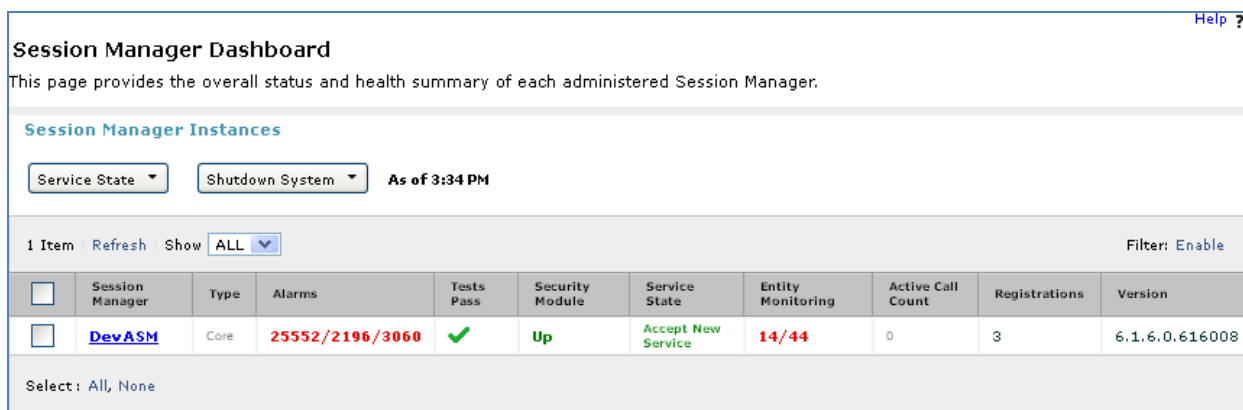
## 10.2. Verify Avaya Aura® Session Manager

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

### 10.2.1. Verify Avaya Aura® Session Manager is Operational

Log into the System Manager and navigate to **Elements → Session Manager → Dashboard** (not shown) to verify the overall system status for Session Manager. Specifically, verify the status of the following fields as shown below:

- **Tests Pass:** 
- **Security Module:** **Up**
- **Service State:** **Accept New Service**




**Session Manager Dashboard**

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

**Session Manager Instances**

Service State: [Dropdown] Shutdown System: [Dropdown] As of 3:34 PM

1 Item Refresh Show [ALL] Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
<input type="checkbox"/>	<a href="#">DevASM</a>	Core	25552/2196/3060		Up	Accept New Service	14/44	0	3	6.1.6.0.616008

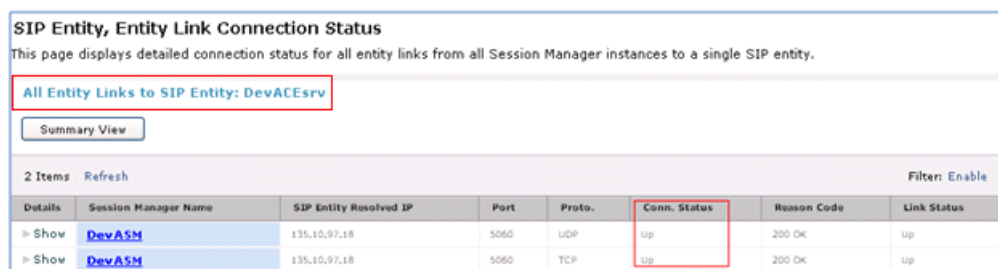
Select: All, None

### 10.2.2. Verify SIP Entity Link Status

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

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

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





**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	<a href="#">DevASM</a>	135.10.97.18	5060	UDP		200 OK	up
► Show	<a href="#">DevASM</a>	135.10.97.18	5060	TCP		200 OK	up

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

## 10.3. Verify Avaya Agile Communication Environment™

Perform a call using ACE\_EXHIBITOR or SOAP UI software. Below is an example of using ACE Exhibitor making a call from **52151** to **52156**.

The screenshot displays the ACE Exhibitor application window. The interface includes a menu bar (File, Setup, Help) and a tabbed control area with the following sections:

- Third Party Call Control v3:** Contains fields for Participant 1 and Participant 2 (both set to 'sip'), an 'Events' checkbox, and buttons for 'Make Call Session', 'End Call Session', 'Add Participant', 'Delete Participant', 'Get Call Session Info', and 'Transfer'.
- Third Party Call Control v2:** Contains 'Calling' and 'Called' fields (both set to 'tel' and '52151'/'52156' respectively), an 'Events' checkbox, and buttons for 'Make Call', 'End Call', 'Cancel Call', and 'Get Call Info'. This section is highlighted with a red rectangle.
- Third Party Call Extensions v2.4:** Contains fields for Endpoint, Consult Endpoint, Consult Call ID, and DTMF Digits, along with buttons for 'Answer', 'Hold', 'Retrieve', 'Consult', 'Complete Consult', 'Generate DTMF', 'Handoff', and 'Single Step Transfer'.

On the right side of the interface:

- Active Call Sessions:** Displays a session ID: 'cb5a41e4-12c6-45fe-8735-40ea479effab'.
- Call Participants:** A table with columns: Participant, Status, StartTime, Duration, and Termination.
- SOAP Messages:** A log showing an inbound message with XML content, including a 'makeCallResponse' element.



### 10.3.1. Verify Avaya Agile Communication Environment™ Server Status

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

General	Deployment	Licensing	Logger	Alarm	Audit Event	PM Collection	AppUtilities Status
Active Server Information							
Host name	DevACE.DevACE						
Fixed IP Address	13						
Service IP Address	13						
Operating System Time	2013-02-09 03:50:05.545 +0000						
Operating System Uptime	10 days, 10 hours, 34 minutes, 55 seconds, 365 milliseconds						
Operating System Version	Red Hat Enterprise Linux Server release 6.0 (Santiago)						
Application Server Status	RUNNING						
Application Server Uptime	10 days, 10 hours, 27 minutes, 59 seconds, 160 milliseconds						
Application Server Version	8.0.0.3 [ND 8.0.0.3 cf031212.03]						
ACE Core Information							
Application Status	RUNNING						
Application Uptime	10 days, 10 hours, 28 minutes, 55 seconds, 676 milliseconds						
Application Version	6.2.0						
Application Build	/localdisk/forge/agent3/bamboo-agent-home/xml-data/build-dir/ACEREL-CORE-JOB1-21_30627						
Application HostType	STANDALONE						
Associated Information	UNAVAILABLE						



## 10.4. Verify Avaya Aura® Messaging

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

### 10.4.1. Verify Avaya Aura® Messaging can Make Calls to Phones

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

**AVAYA** Avaya Aura® Messaging System Management Interface (SMI)

Help Log Off Administration This Server: sp-aamess1

Administration / Messaging

- Start Messaging
- Stop Messaging
- LDAP Status/Restart (Storage)
- Change LDAP Password (Storage)

**Diagnostics (Application)**

**Selection & Configuration**

Select the test(s) to run: Call-out

This calls out to the specified extension. When the phone is picked up, a test greeting should be heard.

**Configuration of Call Out Test**

Telephone number: 60017

Port number (optional):

**Run Tests** Reset Page

**Results**

Test: Call-out Time: 7:13:08 PM

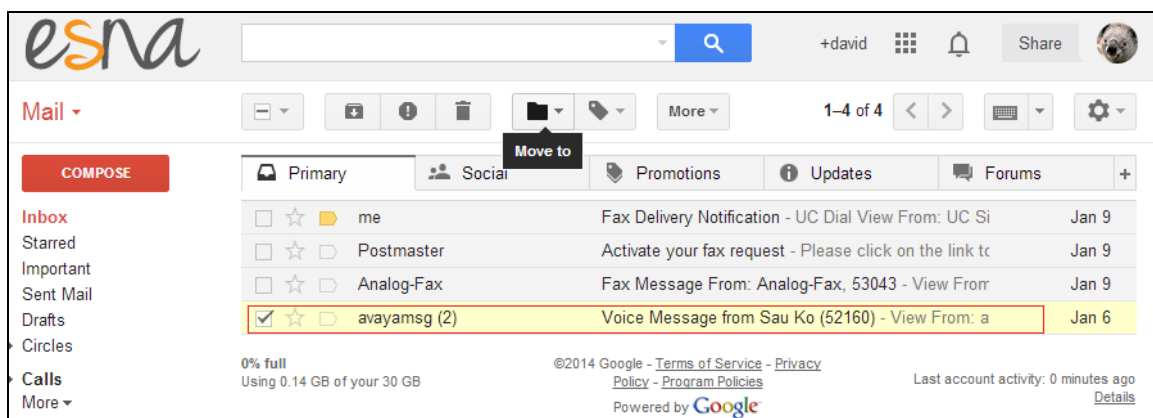
Usage: testCALL extensionNumber [portNumber]

Checking Call-out ... calling 60017 ... [ OK ]

Line:100 (irapi100) Got dial tone Dialing is done Connected Near End disconnected CP=NEAR\_END\_DIS

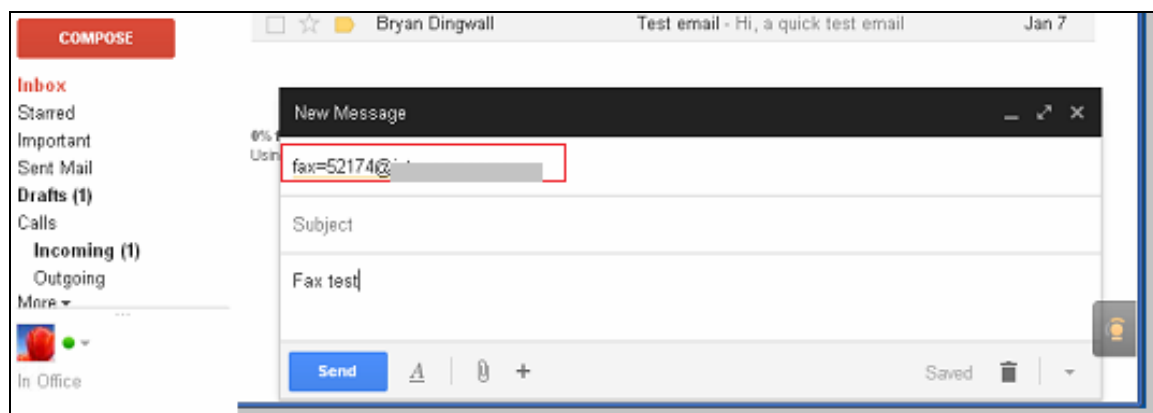
## 10.5. Verify user can Receive and Retrieve Avaya Aura® Messaging Voice Message using Google Mail

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

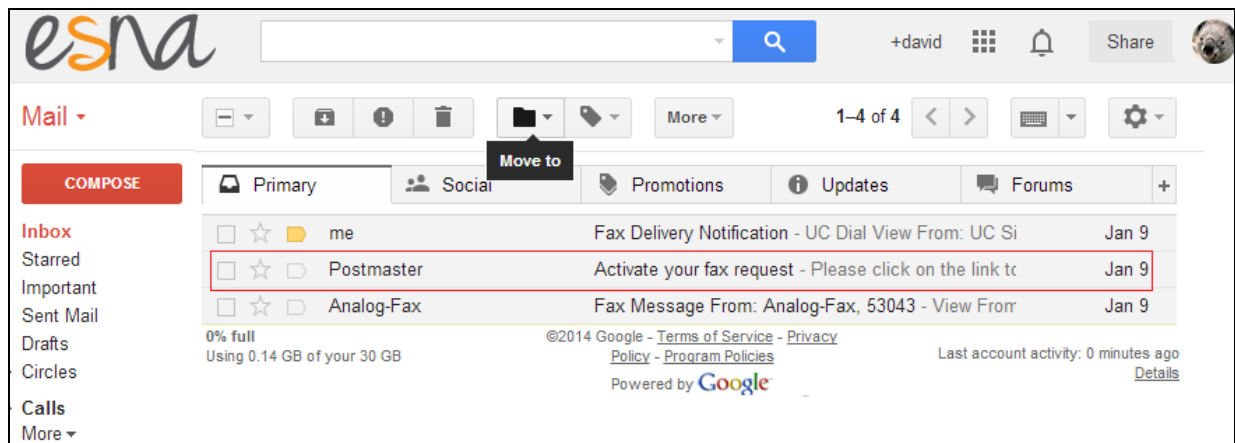


## 10.6. Verify user can send a fax through Google email

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



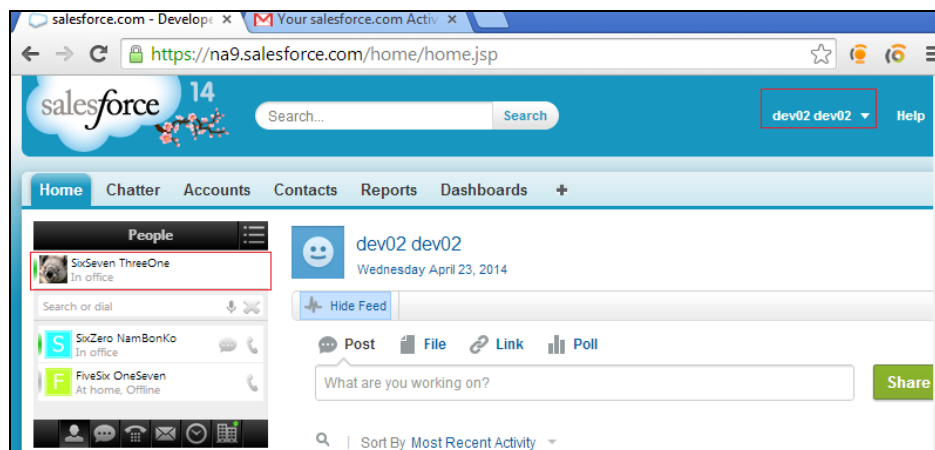
Verify that the user will received an email from **Postmaster** to ask the user to activate the fax request.



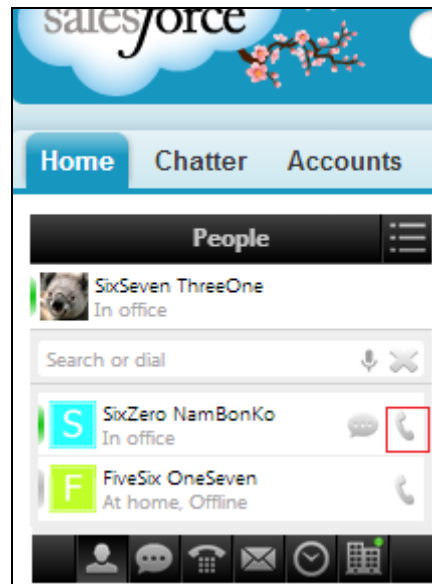
Click on the provided link in the Postmaster's email to confirm (not shown). Verify that the fax machine is able to receive and print out the fax content.

## 10.7. Verify user able to make a call using iLink Pro on Salesforce.com

Use appropriate credential to login SFDC (not shown). During compliance test account dev02 as configured in Section 9.4 is used. Below is detail of SFDC logged in as **dev02** with its Officelinx mailbox name is **SixSeven ThreeOne**.



To make a call, click on the phone icon beside selected user (shown below).



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

## 11. Conclusion

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

## 12. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, May 2013, Release 6.3, Document Number 03-300509.
2. *Administering Avaya Aura® Session Manager*, June 2013, Release 6.3
3. *Administering Avaya Aura® System Manager*, May 2013, Release 6.3.
4. *Avaya Agile Communication Environment™ Service Provider Administration* Release 6.2 NN10850-005, 10.01 November 2012
5. For information regarding security on Communication Manager, see *Avaya Aura Communication Manager Security Design* (03-601973).
6. For an alternate procedure to configure a signing authority as trusted on Avaya ACE, see *"Trusting a CA or self-signed certificate" in Avaya Agile Communication Environment™ User and Security Administration* (NN10850-010).

The following document was provided by Esna:

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

---

**©2014 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).