Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the ESNA Officelinx iLink Pro 9.1 with Avaya Aura® Agile Communication Environment VE 6.2 FP2, Avaya Aura® Messaging 6.2 and Avaya Communication Server 1000 Release 7.6 - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the ESNA Officelinx iLink Pro 9.1 SP1, Avaya Agile Communication Environment 6.2 FP2, Avaya Communication Server 1000 Release 7.6 and Avaya Aura® Messaging 6.2. iLink Pro is a application that allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). iLink Pro controls a physical telephone using Third Party Call (v2, v2.4), Call Notification 4.0 web service of 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

These Application Notes describe the procedure for configuring ESNA Telephony Officelinx, Avaya Aura® Agile Communication Environment (ACE), Avaya Communication Server 1000 and Avaya Aura® Messaging (Messaging) solutions.

iLink Pro is Google Application client of ESNA Officelinx that allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). iLink Pro controls a physical telephone using Third Party Call (v2 and v2.4), Call Notification 4.0 web service of Avaya Aura® Agile Communication Environment.

2. General Test Approach and Test Result

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

2.1. Interoperability Compliance Testing

The general test approach will be to verify the integration of the Esna Officelinx with Avaya IP UNIStim phones only. Phone operations such as off-hook, on-hook, dialing, answering, etc. will be performed from the physical phones and from the iLink Pro application. In addition, phone displays and call states on the physical phones and iLink Pro application will be verified for consistency.

2.2. Test Results

The following testing was covered successfully:

1. Click and call on iLink Pro and the voice path is established on 2 physical phones.
2. Off-hook and on-hook a device, phone states are consistent with its associated physical phone states.
3. Put a call on hold and retrieve call.
4. Transfer a call.
5. Leave an Avaya Aura Messaging voice message and retrieve it on Google mail (Gmail) web. (SMTP replay).
6. Redirect call to Avaya Aura Messaging.
7. Message Waiting Indication (MWI).
8. Send and receive a fax through Gmail.

The following was observed during testing:

1. User A makes a call to user B. If user B selects the "Take Message" option on the incoming call, the call is re-redirected to AAM and A is able to leave the voice message for B. If user A hangs up a call (after leaving a message or not leaving a message) by hanging up the physical device or by selecting the Hang Up option in iLink Pro, then as

observed in the UCACEServer log file, there is no remove CallID event and disconnected event for the completed call. Officelinx needs to have a proper procedure to clean up the callID for a completed call. This “Take Message” option **MUST** 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 AAM maintenance subsequently runs, MWI is turned on again and AAM 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 of the ACE Messaging API to “synchronize” the information to Avaya Aura Messaging. This capability is planned for implementation in a future release of ESNA Officelinx Cloudlink Edition.

3. Call extension of parties after a transfer call do 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. Make a call to unavailable iLink Pro user, the call will be forwarded to AAM. If the user hangs up the call (after leave a message or does not leave a message) by hanging up the physical device or by selecting the Hang Up option in iLink Pro, then as observed in the UCACEServer log file, there is no remove CallID event and disconnected event for the completed call. Officelinx needs to have a proper procedure to clean up the callID for a completed call. The Administrator **MUST NOT** configure the “HuntGroup” setting on Officelinx to prevent the call being left in an orphan state after the call is completed.

5. A physical phone A is not monitored by ESNA Officelinx. Make a call to iLink Pro user B (physical phone B is monitored) and then phone A performs a 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. Users 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. 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
- Email – techsupport@esna.com
- Phone – (905) 707-1234

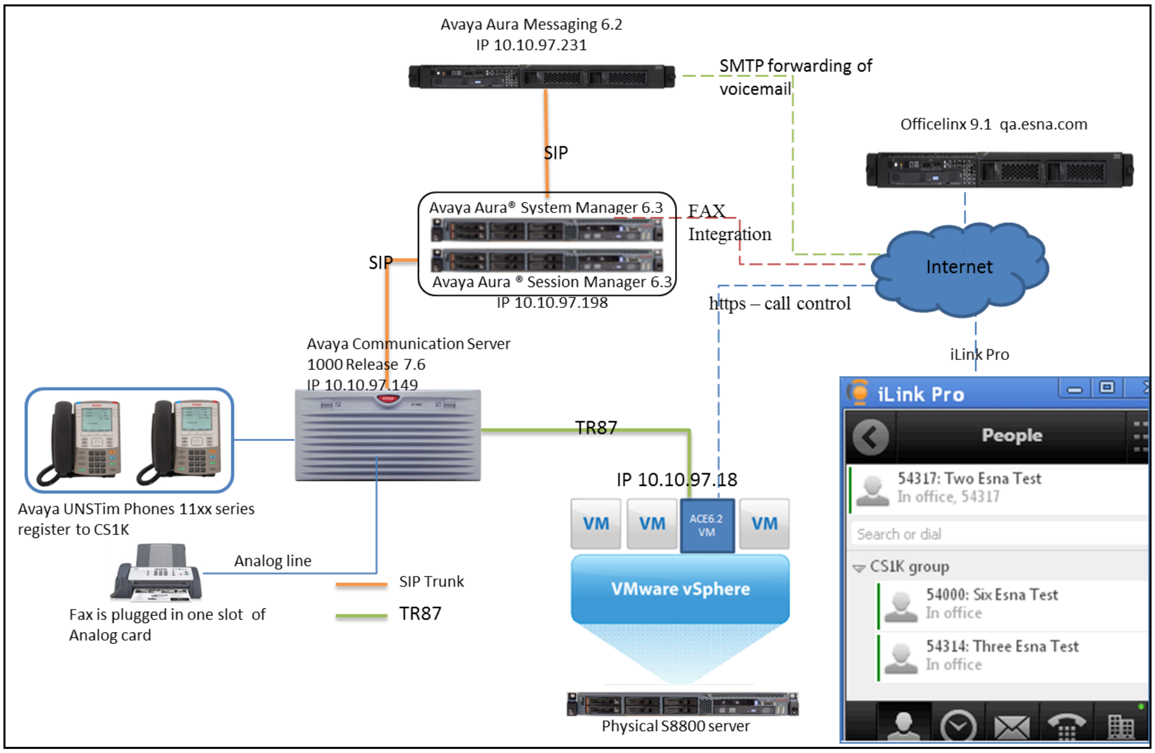
3. Reference Configuration

The figure below illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with a Session Manager and an Avaya Communication Server 1000 Release 7.6. Endpoints include Avaya 1110, 1140 and 2004p1 Series IP Telephones (UNSTim).

ESNA Telephony Officelinx is configured as SIP entity on the Avaya Aura®Session Manager.

A user is able to click and call through the iLink Pro as well as received notify messages from Avaya Aura® Messaging in their Google email.

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



Test Configuration of Avaya ACE and Avaya Aura® system provides services to ESNA Telephony Officelinx

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya Communication Server 1000	Avaya Communication Server Release 7.65 P Deplist 1 (created: 2013-09-24) and Service Update 3 (Created: Sept 24, 2013)
Avaya Aura® System Manager S8800 Server	Avaya Aura® System Manager 6.3.4
Avaya Aura® Session Manager S8800 Server	Avaya Aura® Session Manager 6.3SP4
Avaya Aura® Messaging S8800 Server	Avaya Aura® Messaging 6.2
Avaya S8800 Server with VMWare 5.1	Avaya Agile Communication Environment VE 6.2.1 FP2
Avaya UNIStim Telephones: 2004p1, 1110 and 1140	0623C8J
ESNA Telephony Officelinx Cloudlink Edition	9.1
iLink Pro	9.1.14.1227

5. Configure Avaya Communication Server 1000 R7.6

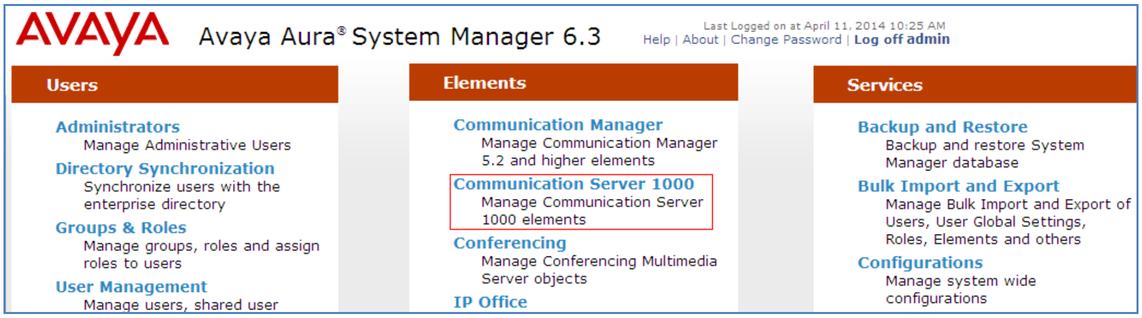
This section describes the procedure for setting up Communication Server 1000. A CTI TR/87 link is created between Avaya Communication Server 1000 and Avaya ACE. The steps include setting up and verifying the system availabilities:

- Verify the Communication Server 1000 Packages and license information
- Verify the number of configured SIP access ports
- Configure TR/87 solutions
- Adding an AML
- Adding VAS
- Node IP (SIP Gateway) Configuration
- Save changes and restart signaling Server
- IP Phone configuration for SIP CTI (TR/87)
- Verify SIP route configuration.
- Route, RLB and DSC Configuration
- Endpoint/Telephone Configuration

The values used in this guide may be unique to the example shown. User will have to use values unique to their site, where this solution is being deployed e.g. site's IP address, extension numbers, etc. Communication Server 1000 configurations are performed through Unified Communications Manager (UCM), Element Manager (EM) and Command Line Interface (CLI) via a telnet session to the Call Server. Review Avaya ACE Service Provider for details of adding TR87 Service Provider on ACE list in **Section 12**.

5.1. Login Unified Communication Manager

To login UCM, login System Manager, then select **Communication Server 1000**.



AVAYA Avaya Aura® System Manager 6.3

Last Logged on at April 11, 2014 10:25 AM
Help | About | Change Password | **Log off admin**

Users

- **Administrators** Manage Administrative Users
- **Directory Synchronization** Synchronize users with the enterprise directory
- **Groups & Roles** Manage groups, roles and assign roles to users
- **User Management** Manage users, shared user

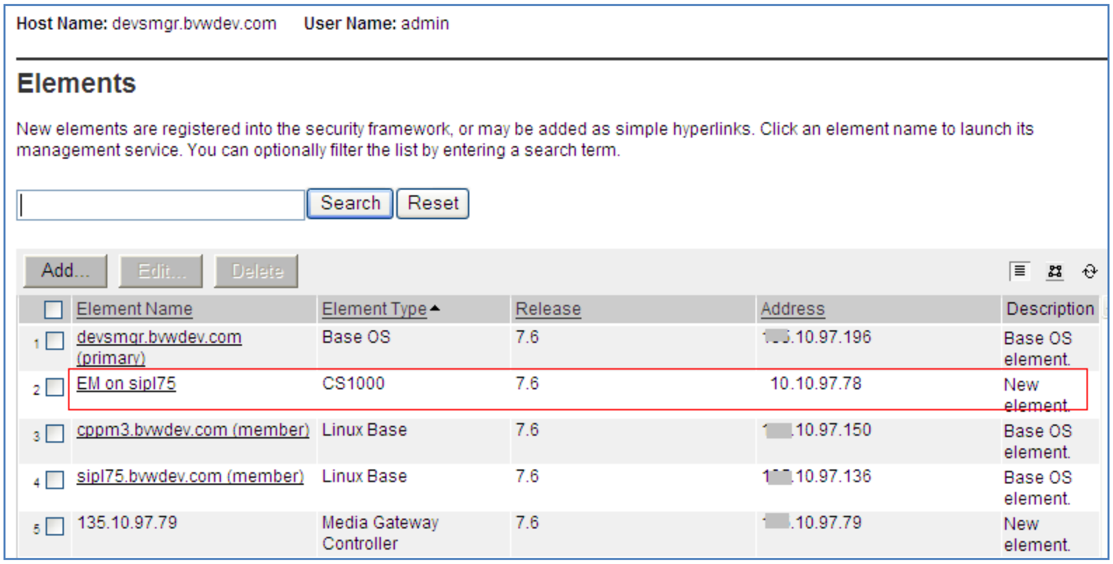
Elements

- **Communication Manager** Manage Communication Manager 5.2 and higher elements
- **Communication Server 1000** Manage Communication Server 1000 elements
- **Conferencing** Manage Conferencing Multimedia Server objects
- **IP Office**

Services

- **Backup and Restore** Backup and restore System Manager database
- **Bulk Import and Export** Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
- **Configurations** Manage system wide configurations

In the UCM, click on **EM** to open Element manager.



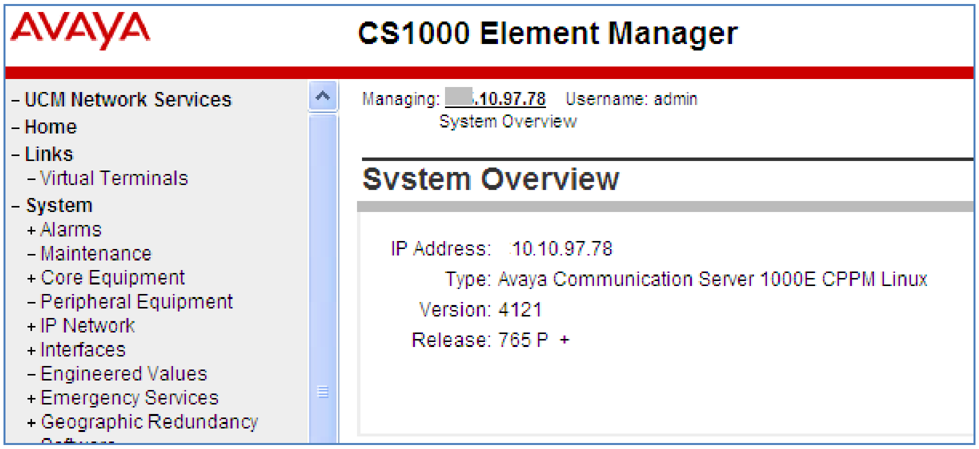
Host Name: devsmgr.bvwdev.com **User Name:** admin

Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

	□	Element Name	Element Type ▲	Release	Address	Description
1	□	devsmgr.bvwdev.com (primary)	Base OS	7.6	[redacted].10.97.196	Base OS element.
2	□	EM on sipl75	CS1000	7.6	10.10.97.78	New element.
3	□	cppm3.bvwdev.com (member)	Linux Base	7.6	[redacted].10.97.150	Base OS element.
4	□	sipl75.bvwdev.com (member)	Linux Base	7.6	[redacted].10.97.136	Base OS element.
5	□	135.10.97.79	Media Gateway Controller	7.6	[redacted].10.97.79	New element.

Communication Server 1000 Element Manager launched.



AVAYA **CS1000 Element Manager**

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - + IP Network
  - + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Geographic Redundancy

Managing: [redacted].10.97.78 Username: admin
System Overview

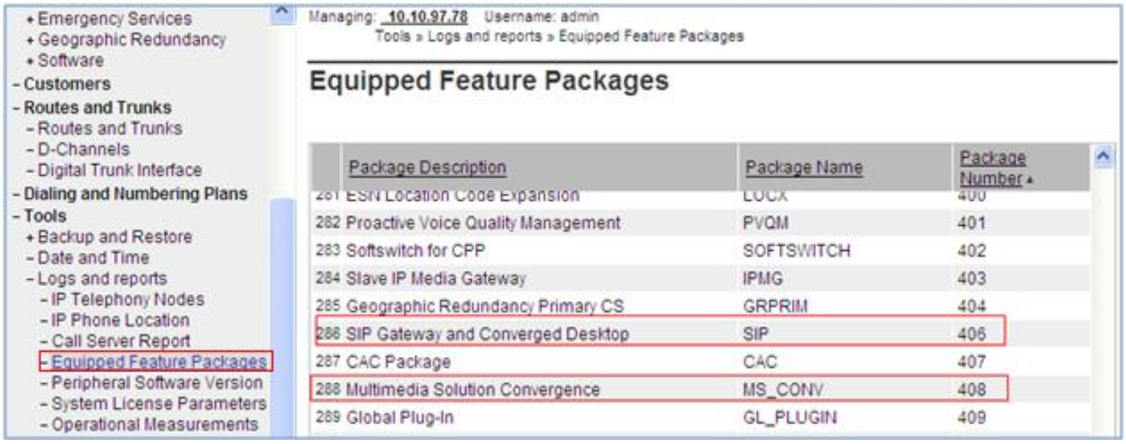
Svstem Overview

IP Address: 10.10.97.78
Type: Avaya Communication Server 1000E CPPM Linux
Version: 4121
Release: 765 P +

5.2. Verify the Communication Server 1000 Packages

Obtain feature package information using Element Manager.

1. In the **CS1000 Element Manager**.
2. Navigate to **Tools → Logs and reports → Equipped feature packages**
3. Verify that Package 406 (SIP), Package 408 (Multimedia Systems Convergence) have been added.



Managing: 10.10.97.78 Username: admin
Tools » Logs and reports » Equipped Feature Packages

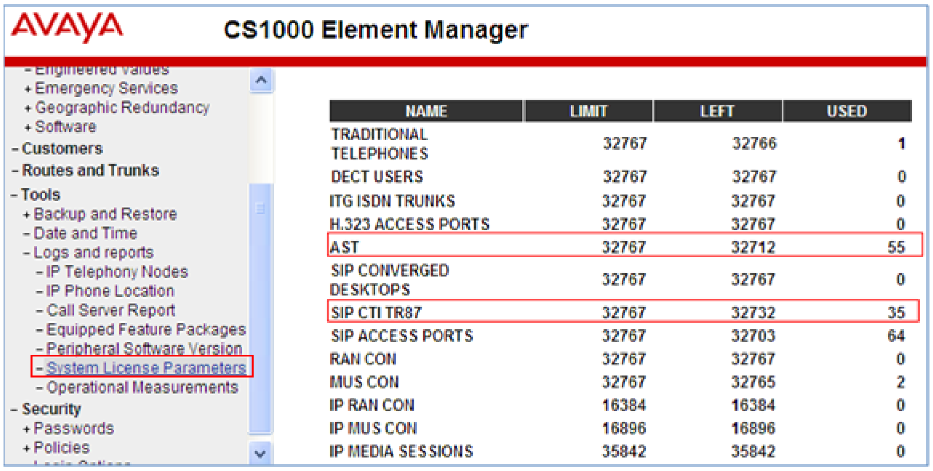
Equipped Feature Packages

	Package Description	Package Name	Package Number ▲
281	ESN Location Code Expansion	LOCX	400
282	Proactive Voice Quality Management	PVQM	401
283	Softswitch for CPP	SOFTSWITCH	402
284	Slave IP Media Gateway	IPMG	403
285	Geographic Redundancy Primary CS	GRPRIM	404
286	SIP Gateway and Converged Desktop	SIP	406
287	CAC Package	CAC	407
288	Multimedia Solution Convergence	MS_CONV	408
289	Global Plug-In	GL_PLUGIN	409

5.3. Verify that sufficient license parameters and system limits

When deploying an ACE solution, ensure that the CS 1000 system has sufficient license parameters to support not only the CS 1000 system and CS 1000 system users, but also any ACE applications to be deployed within the existing customer network.

1. In the **CS1000 Element Manager**. Navigate to **Tools → Logs and reports → System License Parameters**
2. Verify that the following licenses have been added:
   - SIP CTI: Configured based on the number of devices that need to be controlled using TR/87.
   - Associates Set (AST): Configured based on the number of monitor keys required for Presence and Call states.



CS1000 Element Manager

NAME	LIMIT	LEFT	USED
TRADITIONAL TELEPHONES	32767	32766	1
DECT USERS	32767	32767	0
ITG ISDN TRUNKS	32767	32767	0
H.323 ACCESS PORTS	32767	32767	0
AST	32767	32712	55
SIP CONVERGED DESKTOPS	32767	32767	0
SIP CTI TR87	32767	32732	35
SIP ACCESS PORTS	32767	32703	64
RAN CON	32767	32767	0
MUS CON	32767	32765	2
IP RAN CON	16384	16384	0
IP MUS CON	16896	16896	0
IP MEDIA SESSIONS	35842	35842	0

5.4. TR/87 solutions

Using the Avaya Communication Server 1000 (CS 1000) TR/87 service provider, you can enable Avaya ACE to control a Computer Telephony Integration (CTI) capable terminal on the CS 1000 system. This solution supports telephony and other services such as click-to-dial, call notification, presence, remote call control (RCC), and selected services within Avaya.

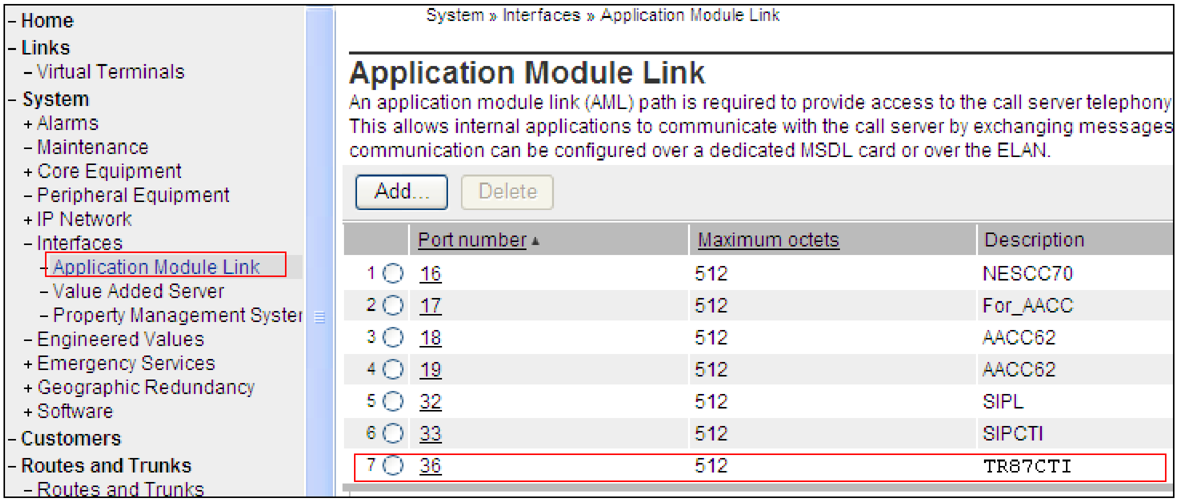
5.4.1. Adding an AML

An application module link (AML) path is required to provide access to the call server telephony functions. The Ethernet AML is the main interface that supports call control requests from SIP CTI Clients and the CS 1000 system. Use this procedure to check if the CS1000 system is already set up for CTI services.

Procedure

1. In the **CS1000 Element Manager**. On the left hand tree view, click **Interfaces → Application Module Link**.
2. Check the port number associated with CTI. Ensure that the port number is 32 or higher. Ports 0–31 are reserved for other functions. Therefore, assign an available virtual port, 32 or higher. For a small CS1000 system, the link number should be between 32 through 47 (inclusive) and for a large CS1000 system, the link number should be between 32 through 127 (inclusive).
3. If there is no port number assigned to CTI, click **Add**.
4. In the **Port number** field, enter a number 32 or higher. E.g. **36** is used during testing
5. In the **Description** field, enter a suitable description for the AML, for example, CTI.
6. Select the **Link control system parameters** check box to enable the Maximum octets list.
7. From the **Maximum octets** list, select the maximum number of octets for each High level Data Link Control (HDLC) frame. (The default is 512).
8. Click **Save**.

Below show **AML 36** is configure in Communication Server 1000:



Application Module Link

An application module link (AML) path is required to provide access to the call server telephony
This allows internal applications to communicate with the call server by exchanging messages
communication can be configured over a dedicated MSDL card or over the ELAN.

	Port number ▴	Maximum octets	Description
1 ○	16	512	NESCC70
2 ○	17	512	For_AACC
3 ○	18	512	AACC62
4 ○	19	512	AACC62
5 ○	32	512	SIPL
6 ○	33	512	SIPCTI
7 ○	36	512	TR87CTI

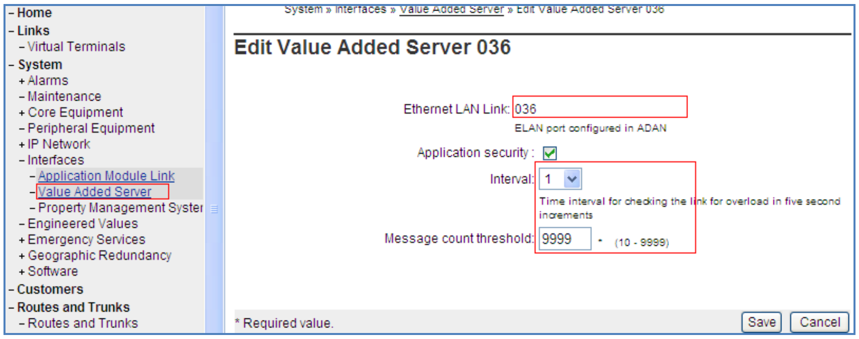
5.4.2. Adding VAS

One Value Added Server (VAS) must be defined for each configured AML. Because Ports 0-31 are reserved for other functions, assign an available virtual port numbered 32 or above. The port assignment for the AML and the VAS may match, but the matching is not a requirement. However, the responses to ELAN and VSID prompts must match. Use the following procedure to associate a Value Added Server (VAS) with AML over ELAN.

Procedure

1. In the **CS1000 Element Manager**. On the left hand tree view, click **Interfaces → Value Added Server.**
2. Click **Add → Ethernet LAN Link**
3. In the **Value Added Server ID** field, enter a number 32 or higher. E.g. **36** is used during testing
4. In the **Ethernet LAN Link** field, enter a number greater than or equal to 32.
1. The ELAN port configured in ADAN must be greater than or equal to 32.
5. Ensure the **Application Security** check box is cleared.
6. Ensure that the **Interval** field is set to 1.
7. Ensure that the **Message Count Threshold** field is 9999. The range is 10 through 9999 and the default value is 9999.
8. Click **Save**.

Below is detail of **VAS 36** configured on Communication Server 1000:



System » Interfaces » Value Added Server » Edit Value Added Server 036

Edit Value Added Server 036

Ethernet LAN Link: 036

ELAN port configured in ADAN

Application security : ☑

Interval: 1

Time interval for checking the link for overload in five second increments

Message count threshold: 9999 * (10 - 9999)

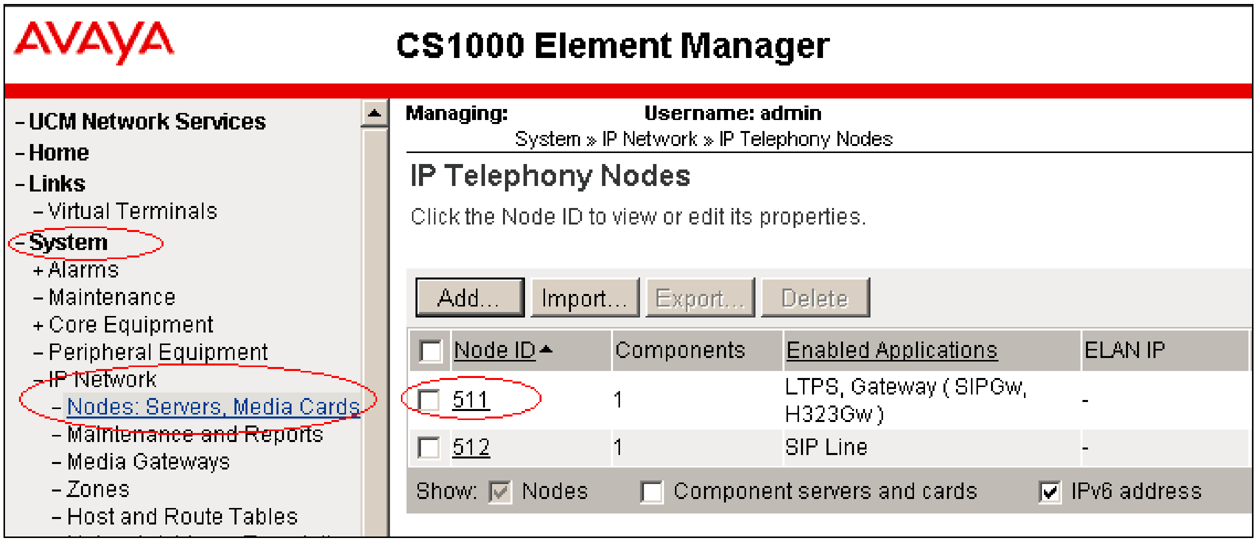
* Required value.

5.4.3. Node IP (SIP Gateway) Configuration

This section only describes the configuration of the SIP Gateway application running on the Communication Server 1000 signaling server. In the solution test, Node ID **511** is configured, that has the SIP Gateway application enabled on it. For additional information on Nodes configuration, refer to **Section 12**.

A node is defined as a collection of signaling servers and voice gateway media cards. Each node in the network has a unique Node ID.

To configure the SIP Gateway from EM, navigate to **System →IP Network →Nodes: Servers, Media Cards** and click on the **Node ID 511** as shown in figure below.



Managing: Username: admin

System » IP Network » IP Telephony Nodes

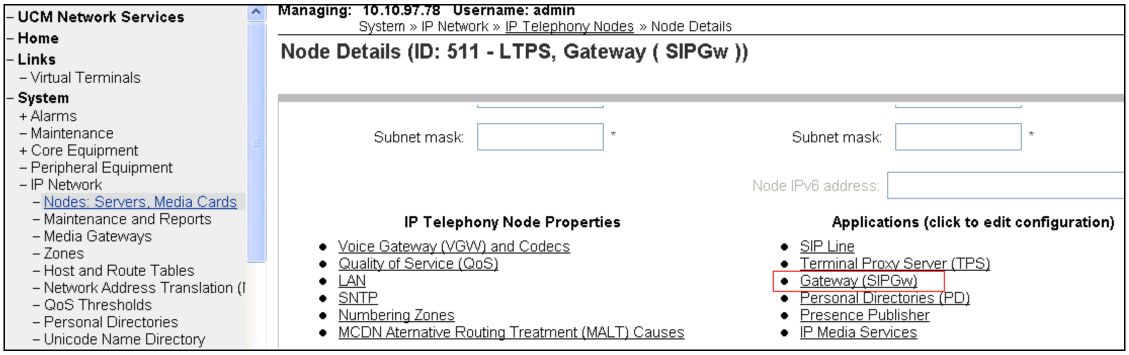
IP Telephony Nodes

Click the Node ID to view or edit its properties.

□	Node ID ▲	Components	Enabled Applications	ELAN IP
□	511	1	LTPS, Gateway (SIPGw, H323Gw)	-
□	512	1	SIP Line	-

Show: ☑ Nodes □ Component servers and cards ☑ IPv6 address

Click on the link **Gateway (SIPGw)** link as shown in figure below.



Managing: 10.10.97.78 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 511 - LTPS, Gateway (SIPGw))

Subnet mask: *

Subnet mask: *

Node IPv6 address:

IP Telephony Node Properties

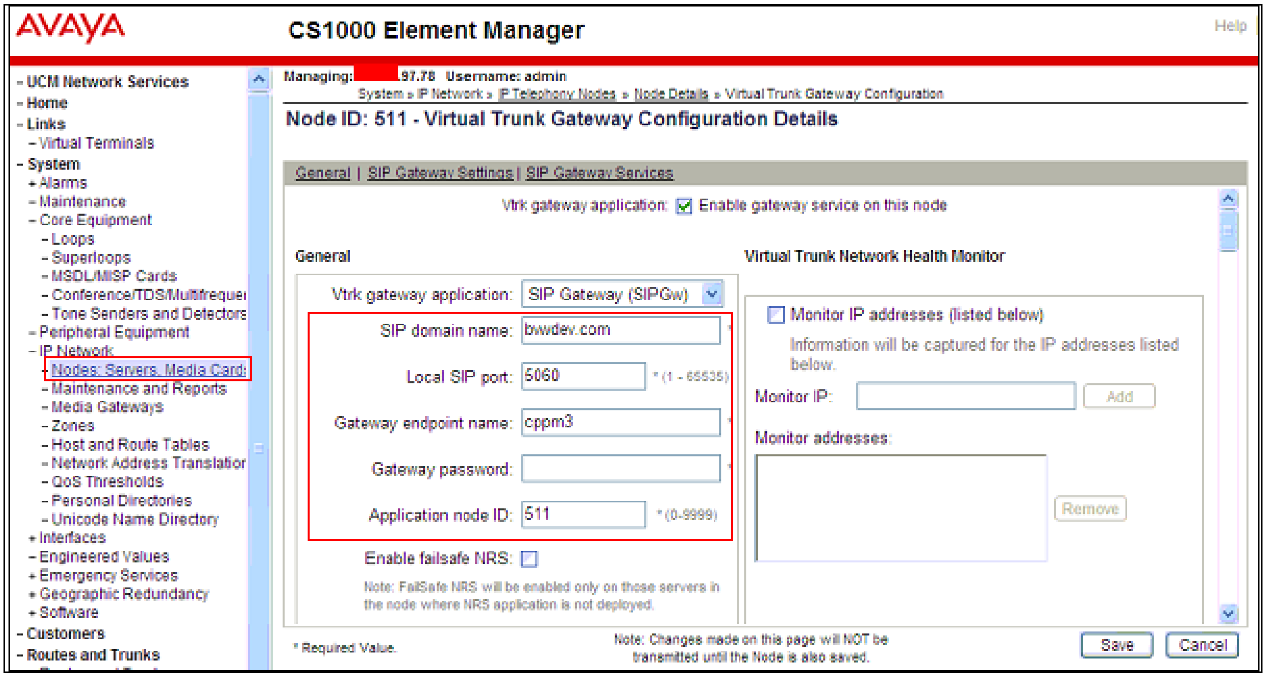
- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

In General section, enter the following information:

1. **SIP domain name:** domain name that is configured in Session Manager e.g. **bvwdev.com.**
2. **Local SIP port** as **5060.**
3. **Gateway endpoint name:** enter SIP entity name of Communication Server 1000 configured on Session Manager e.g. **cppm3**
4. **Application node ID:** enter the Node ID **511** of the current node.



Managing: [redacted].97.78 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 511 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☑ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw)

SIP domain name: bvwdev.com

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: cppm3

Gateway password:

Application node ID: 511 * (0-9999)

Enable failsafe NRS: □

Note: FailSafe NRS will be enabled only on those servers in the node where NRS application is not deployed.

Virtual Trunk Network Health Monitor

□ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP: Add

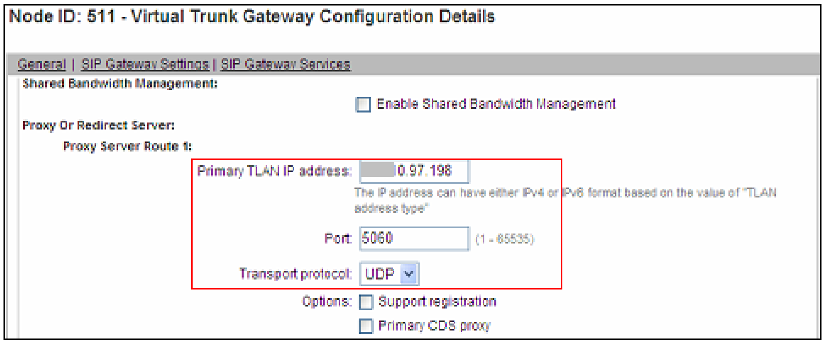
Monitor addresses: Remove

* Required Value.

Note: Changes made on this page will NOT be transmitted until the Node is also saved.

Save Cancel

In the **Proxy Server Route 1**, **Primary TLAN IP address,** enter the **IP address of the Session Manager**. The rest of the fields are left at default.



Node ID: 511 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Shared Bandwidth Management:

□ Enable Shared Bandwidth Management

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: [redacted]0.97.198

The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

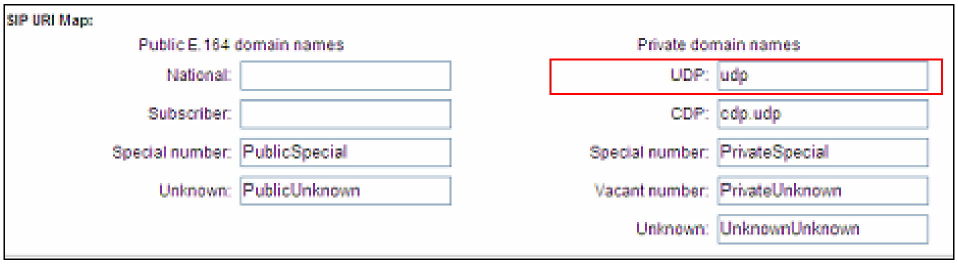
Port: 5060 (1 - 65535)

Transport protocol: UDP

Options: □ Support registration

□ Primary CDS proxy

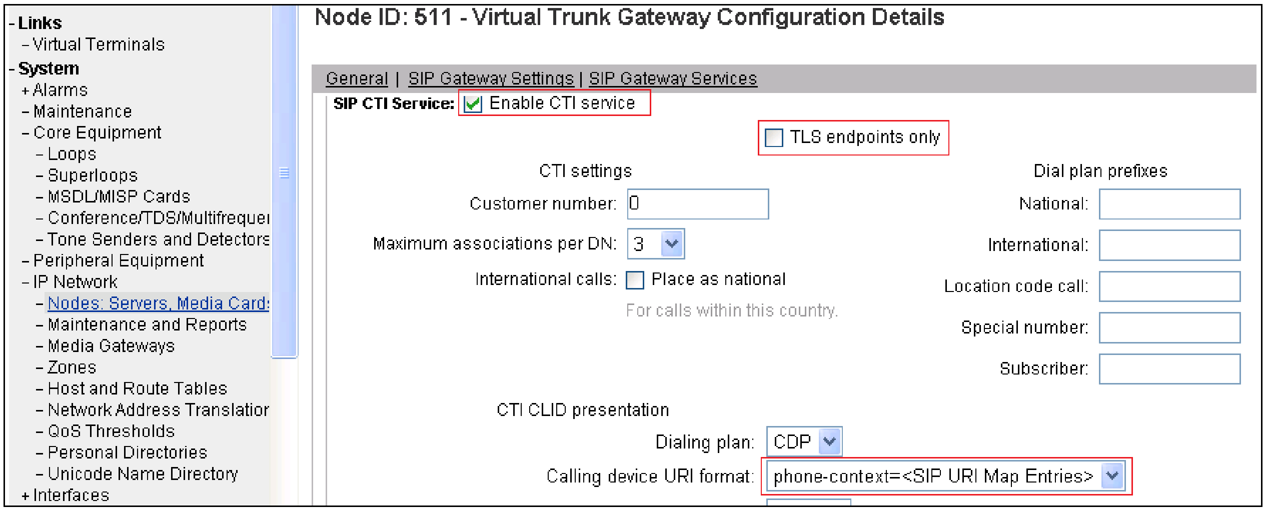
In the **SIP URI Map** for Private domain names, verify the **UDP** field is configured as **udp.** The rest of the fields are left as default.



SIP URI Map:

Public E.164 domain names		Private domain names	
National:		UDP:	udp
Subscriber:		CDP:	cdp.udp
Special number:	PublicSpecial	Special number:	PrivateSpecial
Unknown:	PublicUnknown	Vacant number:	PrivateUnknown
		Unknown:	UnknownUnknown

In **SIP CTI Server** section, make sure the **Enable CTI service** checkbox is checked. Using SIP CTI (TR/87) services on the CS 1000 Telephony nodes, applications can send control messages to CS 1000 terminal devices, such as IP phones, to obtain presence information or invoke a make call operation. Enter the rest of information as following: **TLS endpoints only**: Unchecked. After a system reboot, review this setting again. User may have to uncheck this again. **Calling Device URI format**: Select **phone-context=<SIP URI Map Entries>**. Leave other fields as default. Save changes and restart Signaling Server.



Node ID: 511 - Virtual Trunk Gateway Configuration Details

SIP CTI Service: ☑ Enable CTI service

□ TLS endpoints only

CTI settings

Customer number: 0

Maximum associations per DN: 3

International calls: □ Place as national

For calls within this country.

Dial plan prefixes

National:

International:

Location code call:

Special number:

Subscriber:

CTI CLID presentation

Dialing plan: CDP

Calling device URI format: phone-context=<SIP URI Map Entries>

5.4.4. IP Phone configuration for SIP CTI (TR/87)

Phones are programmed and printed on an individual basis in linked LDs 10/11/20 or using a supported system management application such as Telephony Manager.
When configuring a phone to support SIP CTI operations, pay special attention to the Class of Service (CLS): **TR87A, CMDR**; Associated Set (**AST**) is assigned to **00** - SCR Key 0, and KEY prompts. Make sure that the mnemonic **MARP** appears by **Key 0**, the primary directory number (DN) for the phone.

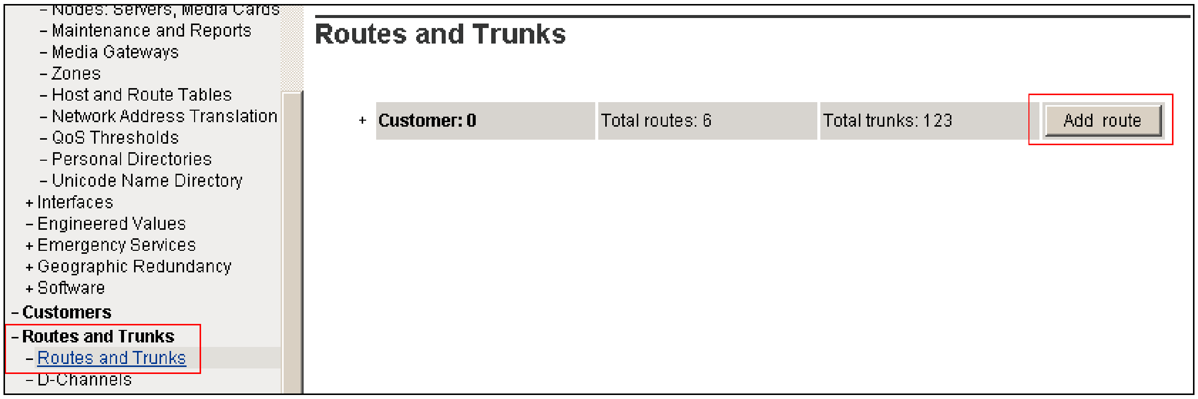
```
TYPE: 1150
TN   96 0 1 3

DES  1150
TN   096 0 01 03  VIRTUAL
TYPE 1150
CDEN 8D
CTYP XDLC
CUST 0
CUR_ZONE 00001
MRT
ERL
CLS  CTD … USMD USRD ULAD CCBD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87A SBMD
     KEM3 MSNV FRA  PKCH MUTA MWTD DVLD CROD ELCD
CPND_LANG ENG
AST  00
IAPG 0
AACS YES
ACQ  AS: AST-DN
ASID 36
SFNB  1  2  3  5  6  7  8  9  10  11  12  13  15  16  17  18  19  20  21  22  23
24  25  32  33  34  35  36  37  38  39
SFRB  32  33  34  35  36  37  38  39
USFB  1  2  3  4  5  6  7  8  9  10  11  12  13  14  15
CALB  0  1  2  3  4  5  6  7  8  9  10  11
FCTB
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY  00 SCR 54314 0      MARP
        CPND
          CPND_LANG ROMAN
            NAME 1150E
            XPLN 13
            DISPLAY_FMT FIRST,LAST
     01
     02 CWT
     03
  04
```

5.4.5. Enable ELAN

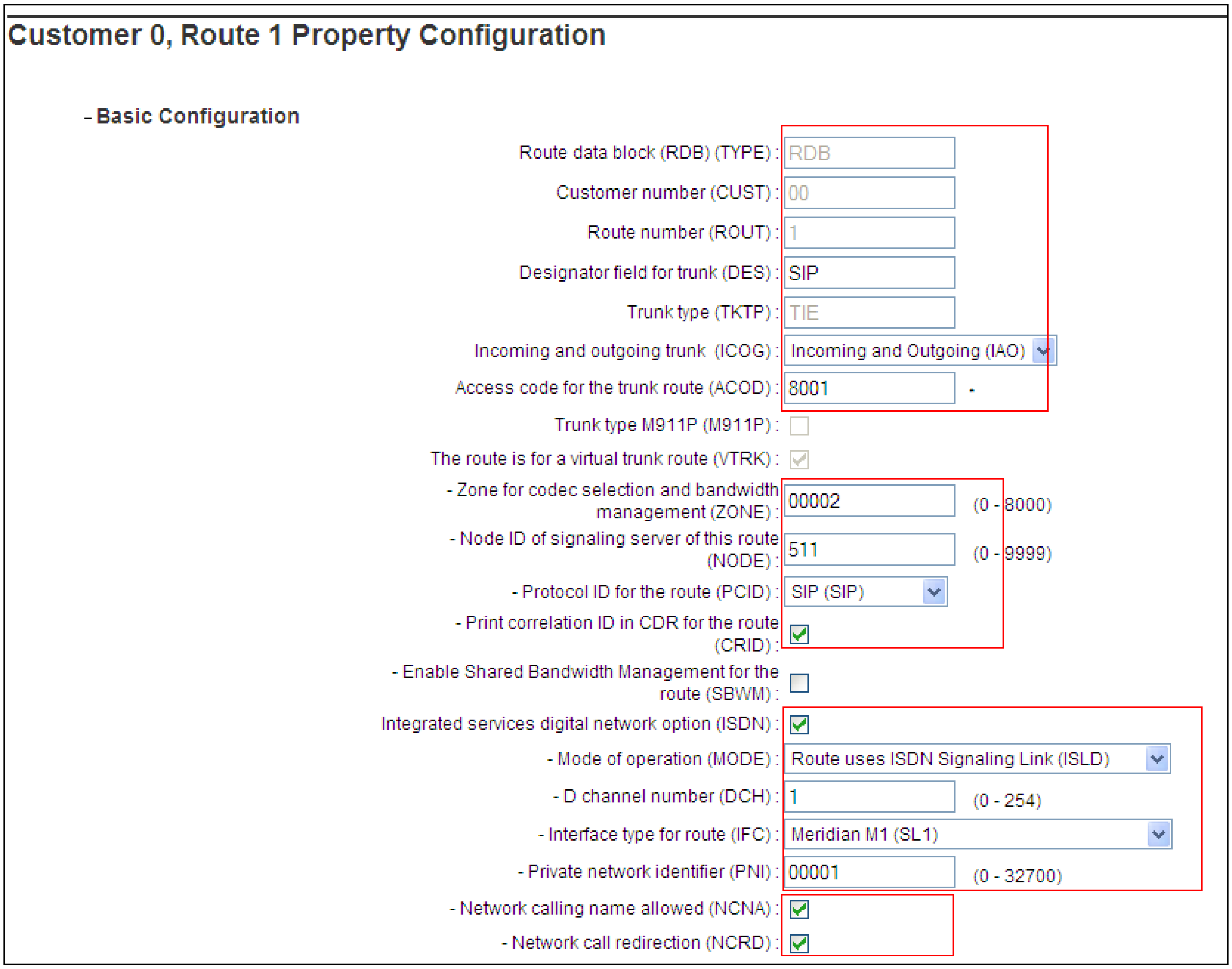
1. In the left pane directory tree of the Element Manager, navigate to **System** → **Maintenance**.
2. Select **"Select by Overlay"**.
3. Select LD 48
4. The system displays the Select Group window.
5. Select **AML diagnostics**.
6. Select the **ENL ELAN** command and click **Submit**.

5.5. Route, RLB and DSC Configuration

This section explains the steps to configure a routing from the Communication Server 1000 using the RLB and DSC values. After logging into the UCM, click on the EM link of the respective Communication Server 1000 (Not Shown). In the EM navigate to **Routes and Trunks → Routes and Trunks.** Click on **Add route.**



The figure below shows the configuration of the route being added. The values that are boxed in red are to be configured by the user. The values shown are examples used during the solution testing.

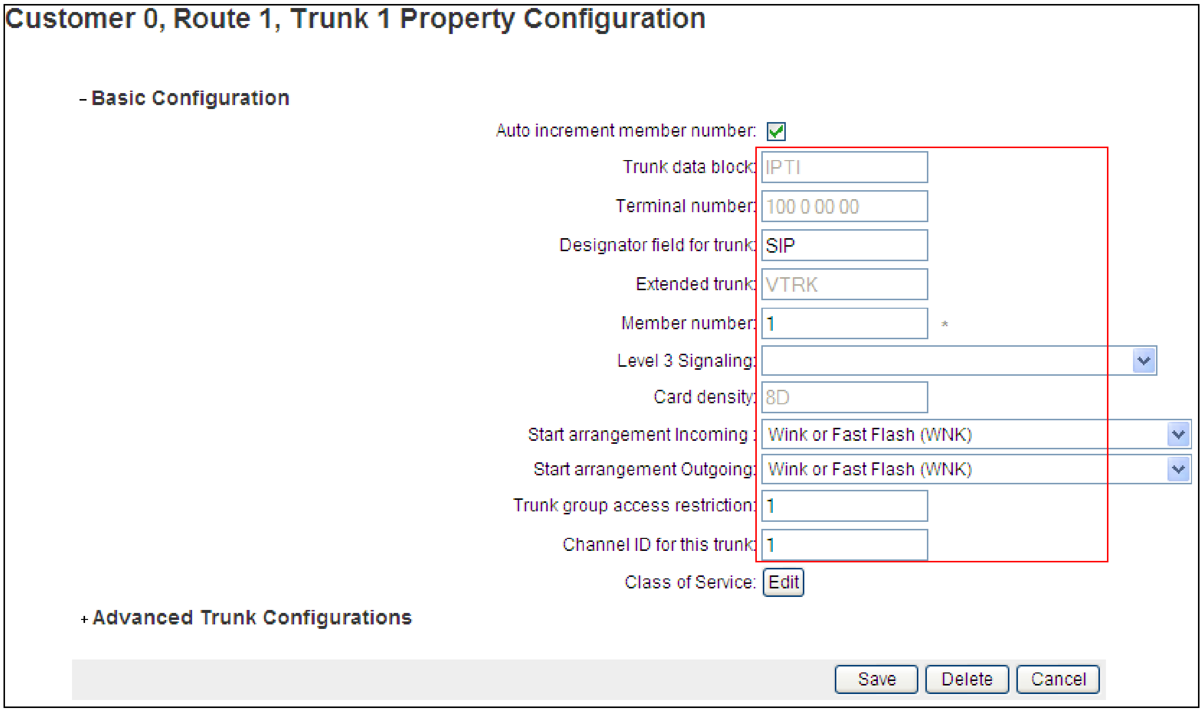


Customer 0, Route 1 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE) :	RDB	
Customer number (CUST) :	00	
Route number (ROUT) :	1	
Designator field for trunk (DES) :	SIP	
Trunk type (TKTP) :	TIE	
Incoming and outgoing trunk (ICOG) :	Incoming and Outgoing (IAO)	
Access code for the trunk route (ACOD) :	8001	-
Trunk type M911P (M911P) :	□	
The route is for a virtual trunk route (VTRK) :	☑	
- Zone for codec selection and bandwidth management (ZONE) :	00002	(0 - 8000)
- Node ID of signaling server of this route (NODE) :	511	(0 - 9999)
- Protocol ID for the route (PCID) :	SIP (SIP)	
- Print correlation ID in CDR for the route (CRID) :	☑	
- Enable Shared Bandwidth Management for the route (SBWM) :	□	
Integrated services digital network option (ISDN) :	☑	
- Mode of operation (MODE) :	Route uses ISDN Signaling Link (ISLD)	
- D channel number (DCH) :	1	(0 - 254)
- Interface type for route (IFC) :	Meridian M1 (SL1)	
- Private network identifier (PNI) :	00001	(0 - 32700)
- Network calling name allowed (NCNA) :	☑	
- Network call redirection (NCRD) :	☑	

Example of trunk configured during compliance test:



Customer 0, Route 1, Trunk 1 Property Configuration

- Basic Configuration

Auto increment member number: ☑

Trunk data block: IPTI

Terminal number: 100 0 00 00

Designator field for trunk: SIP

Extended trunk: VTRK

Member number: 1 *

Level 3 Signaling:

Card density: 8D

Start arrangement Incoming : Wink or Fast Flash (WNK)

Start arrangement Outgoing: Wink or Fast Flash (WNK)

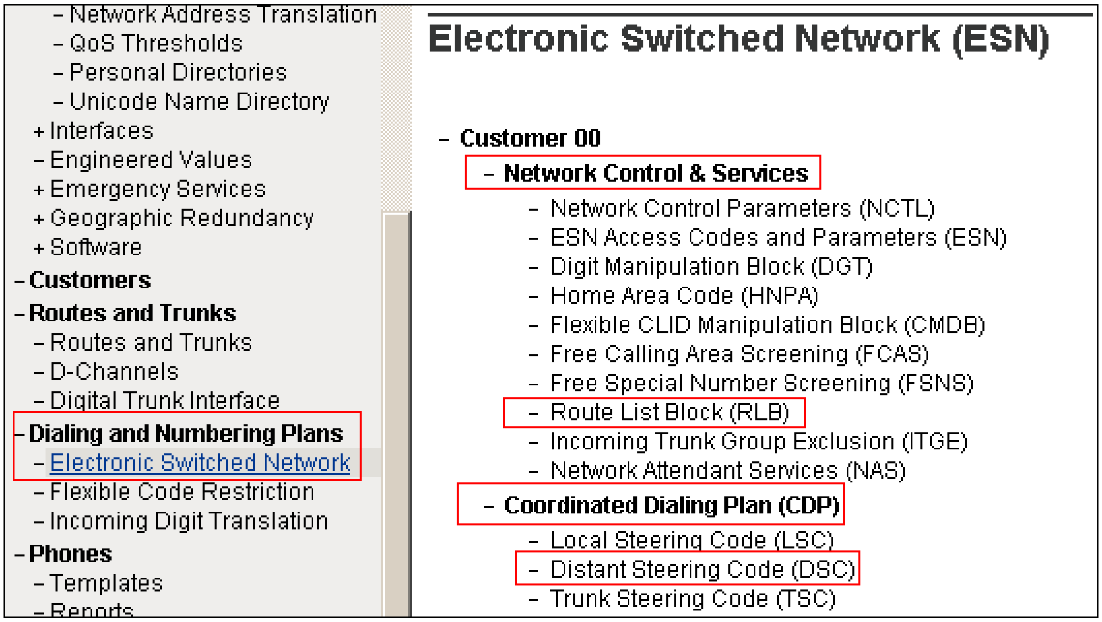
Trunk group access restriction: 1

Channel ID for this trunk: 1

Class of Service: Edit

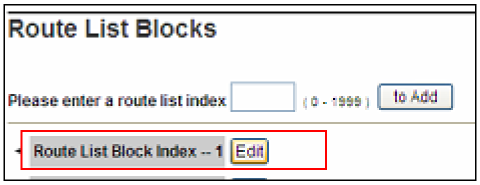
+ Advanced Trunk Configurations

To configure the RLB using EM navigate to **Dialing and Numbering Plans →Electronic Switched Network →Network Control & Services →Route List Block (RLB)**.



- Network Address Translation
- QoS Thresholds
- Personal Directories
- Unicode Name Directory
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
- Phones
- Templates
- Reports
Electronic Switched Network (ESN)
- Customer 00
- Network Control & Services
- Network Control Parameters (NCTL)
- ESN Access Codes and Parameters (ESN)
- Digit Manipulation Block (DGT)
- Home Area Code (HNPA)
- Flexible CLID Manipulation Block (CMDB)
- Free Calling Area Screening (FCAS)
- Free Special Number Screening (FSNS)
- Route List Block (RLB)
- Incoming Trunk Group Exclusion (ITGE)
- Network Attendant Services (NAS)
- Coordinated Dialing Plan (CDP)
- Local Steering Code (LSC)
- Distant Steering Code (DSC)
- Trunk Steering Code (TSC)

Enter the value of the route list index and click on **to Add** button to continue the configuration as shown below. During the solution testing the value of **1** was added.

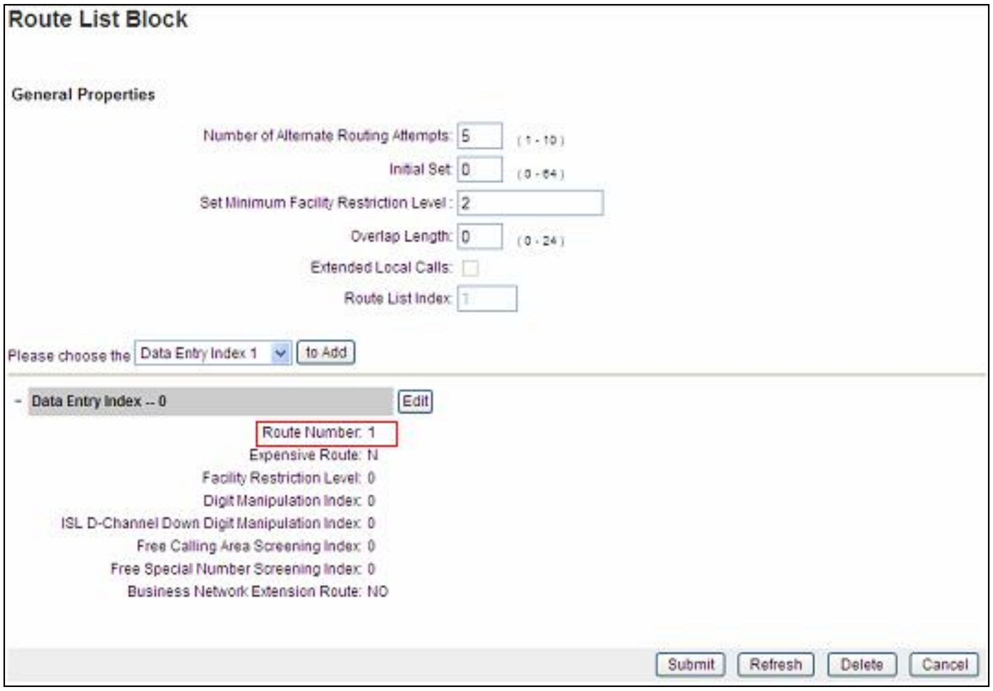


Route List Blocks

Please enter a route list index (0 - 1999) to Add

Route List Block Index -- 1 Edit

The **Route Number 1** being selected to the RLB created. Route **1** is selected since it was the route number assigned while adding a route. Below is detail of RLB 1



Route List Block

General Properties

Number of Alternate Routing Attempts: 5 (1 - 10)
Initial Set: 0 (0 - 64)
Set Minimum Facility Restriction Level : 2
Overlap Length: 0 (0 - 24)
Extended Local Calls: □
Route List Index: 1

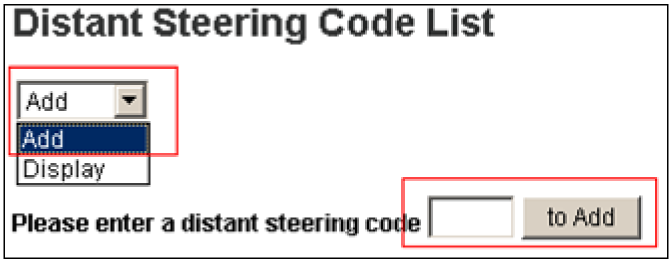
Please choose the Data Entry Index 1 to Add

- Data Entry Index -- 0 Edit

Route Number: 1
Expensive Route: N
Facility Restriction Level: 0
Digit Manipulation Index: 0
ISL D-Channel Down Digit Manipulation Index: 0
Free Calling Area Screening Index: 0
Free Special Number Screening Index: 0
Business Network Extension Route: NO

Submit Refresh Delete Cancel

To configure the DSC using EM navigate to **Dialing and Numbering Plans → Electronic Switched Network → Coordinated Dialing Plan (CDP) → Distant Steering Code (DSC)**. In the Distant Steering Code List page, select **Add** from the drop down list as shown below.



Distant Steering Code List

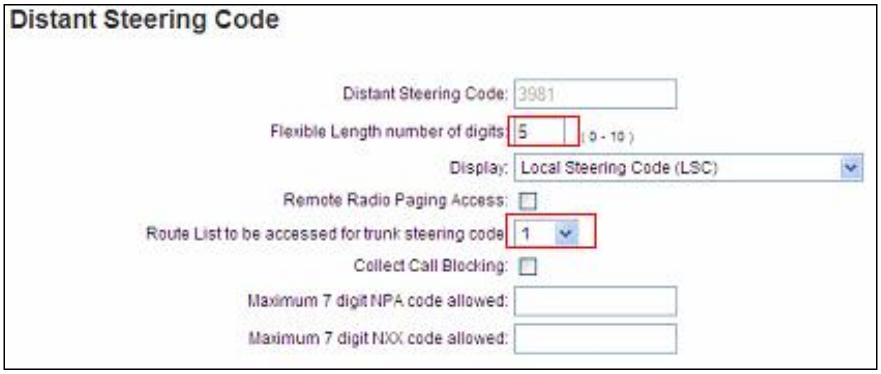
Add
Add
Display

Please enter a distant steering code to Add

Enter the value of the DSC and click on the **to Add** button (Not Shown). As shown below 39 was added during the solution testing. The value 39 was configured since the pilot DN of the AAM was **39900**.

Flexible Length number of digits indentifies length of the directory number (DN). During solution testing, a value of **5** was configured.

Route List to be accessed for trunk steering code is selected as **1** from the drop down list. This value is selected based on the RLB created in above step.



Distant Steering Code

Distant Steering Code: 3981

Flexible Length number of digits: 5 (0 - 10)

Display: Local Steering Code (LSC)

Remote Radio Paging Access: □

Route List to be accessed for trunk steering code 1

Collect Call Blocking: □

Maximum 7 digit NPA code allowed:

Maximum 7 digit NXX code allowed:

For additional information on Route, RLB and DSC configuration, refer to **Section 12.**

5.6. Endpoint/Telephone Configuration

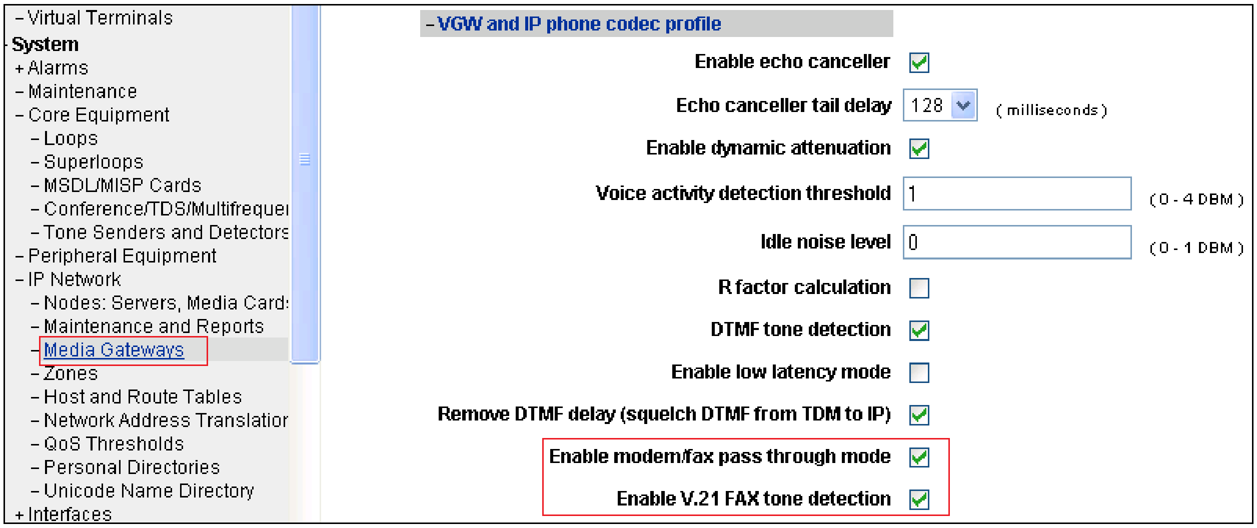
This section explains the provisioning of an endpoint/telephone that was configured for the solution testing. Endpoint/Telephone can be configured using the CLI of the Communication Server 1000 from overlay LD 11/20. Refer to **Section 12** for further information regarding the addition/configuration of endpoints/telephones.

In figure below, values that are shown in red are to be configured by the user. The **FDN** and **HUNT** value of **39900** was used during the solution testing as the pilot DN of the Avaya Aura Messaging.

```
Ld 11
REQ: prt
TYPE: 1165
TN   096 0 00 17
FDN  39900
…
CLS  UNR FBA WTA LPR MTD FNA HTA TDD HFA CRPD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LNA CNDA
     CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXA ARHD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
     UDI RCC HBTD AHD IPND  DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87A SBMD
     KEM3 MSSD[MSBT] FRA  PKCH MUTA MWTD DVLD CROD ELCD
CPND_LANG ENG
RCO  0
HUNT 39900
…
KEY  00 SCR 54312 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME DN 54312
            XPLN 13
         DISPLAY_FMT FIRST,LAST
```

5.7. Fax setting

In the EM navigate to navigate to Media Gateways, verify **Enable modem/fax pass through mode** and **EnableV.21 FAX tone detection** are checked.



- VGW and IP phone codec profile

Enable echo canceller ☑

Echo canceller tail delay 128 (milliseconds)

Enable dynamic attenuation ☑

Voice activity detection threshold 1 (0 - 4 DBM)

Idle noise level 0 (0 - 1 DBM)

R factor calculation ☐

DTMF tone detection ☑

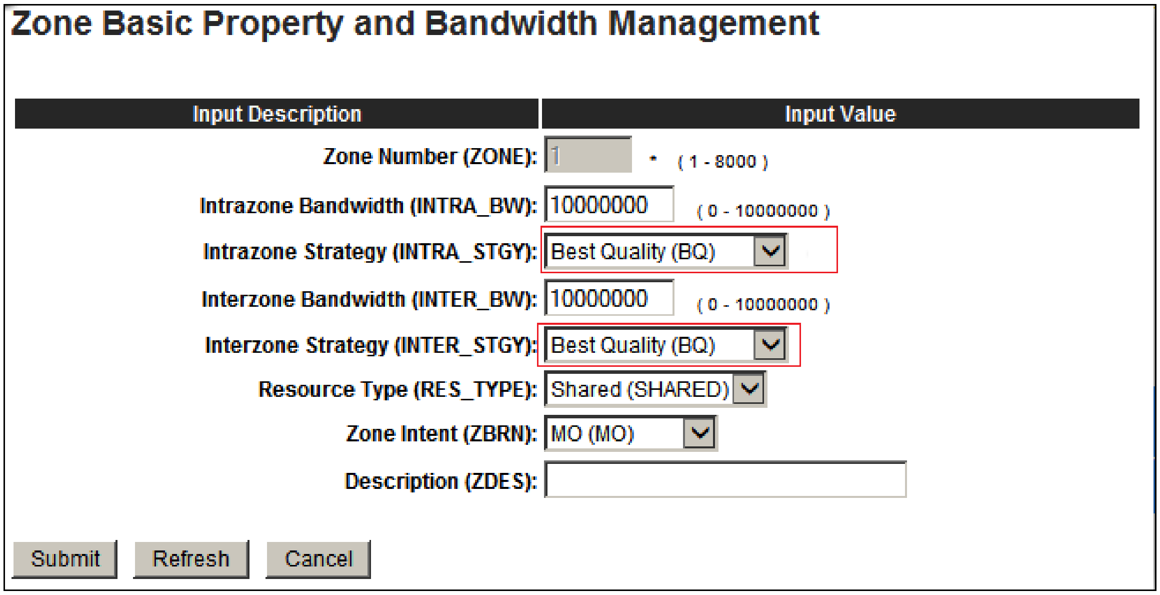
Enable low latency mode ☐

Remove DTMF delay (squelch DTMF from TDM to IP) ☑

Enable modem/fax pass through mode ☑

Enable V.21 FAX tone detection ☑

Verify MGC's (and VGW trunks) should be in a Zone with **Best Quality (BQ)**



Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	1 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	10000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	10000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	

Verifythe following Class Of Service is enabled for fax TNB: **FAXA** (Fax allowed) and **MPTD**. This setting will allow lower speed faxes (up to 14.4) to use T.38, and higher speed faxes to use G711 clear channel (no echo cancelation, no nonlinear DSP features).

```
DES  FROX
TN   004 0 05 00  VIRTUAL
TYPE 500
CDEN 4D
CUST 0
MRT
ERL  00000
WRLS NO
DN   54040 0     MARP
     CPND
       CPND_LANG ROMAN
         NAME Frox analog
         XPLN 23
         DISPLAY_FMT FIRST,LAST
AST  NO
IAPG 0
HUNT
TGAR 1
LDN  NO
NCOS 0
SGRP 0
RNPG 0
XLST
SCI  0
SCPW
SFLT NO
CAC_MFC 0
CLS  CTD DTN …
     MBXD CPFA CPTA UDI RCC HBTD IRGD  DDGA NAMA MIND
     NRWD NRCD NROD SPKD CRD PRSD MCRD
     EXR0 SHL SMSD ABDD CFHD DNDY DNO3
     CWND USMD USRD CCBD BNRD OCBD RTDD RBDD RBHD FAXA CNUD CNAD PGND FTTC
     FDSD NOVD CDMR PRED MCDD T87D SBMD PKCH MPTD ELCD
PLEV 02
PUID
UPWD
AACS NO
MLWU_LANG 0
DATE  4 JUL 2011
```

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

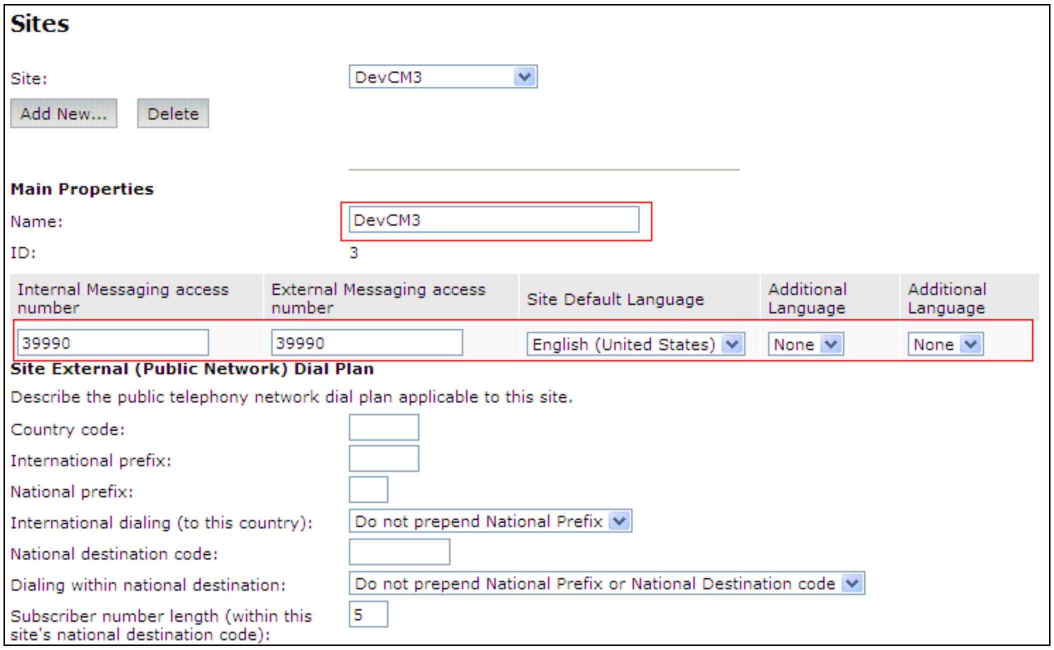
See references **Section 12** for standard installation and configuration information. General knowledge of the configuration tools and interfaces is assumed.

6.1. Administer Sites

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

Under **Main Properties:**

- **Name**: Enter site name
- **Internal Messaging access number:** Enter a Messaging Pilot number



Sites

Site: DevCM3

Main Properties

Name: DevCM3

ID: 3

Internal Messaging access number	External Messaging access number	Site Default Language	Additional Language	Additional Language
39990	39990	English (United States)	None	None

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

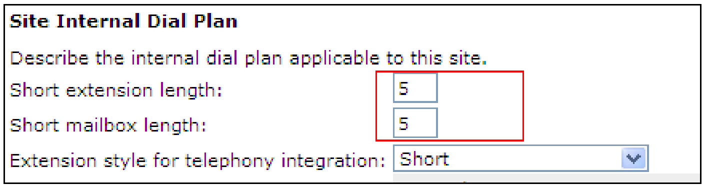
National destination code:

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:**

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



Site Internal Dial Plan

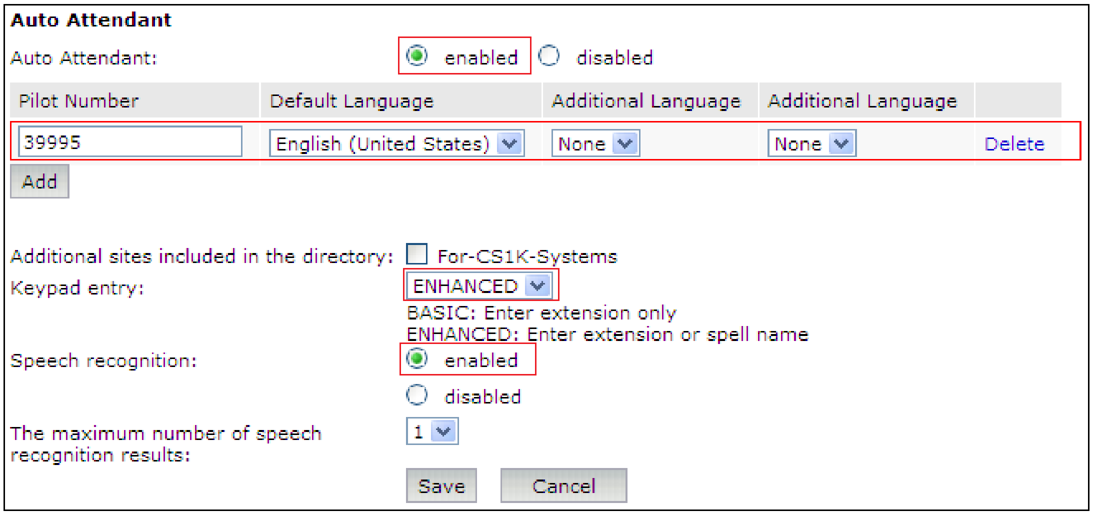
Describe the internal dial plan applicable to this site.

Short extension length: 5
Short mailbox length: 5
Extension style for telephony integration: Short

Scroll down to the **Auto Attendant** section.
Under **Auto Attendant:**

- **Auto Attendant** Select **Enabled**
- **Auto Attendant pilot number** Enter an Auto Attendant number
- **Keypad entry** Select **ENHANCED**
- **Speech recognition** Select **Enabled**

Click **Save** to save changes.



Auto Attendant

Auto Attendant: ● enabled ○ disabled

Pilot Number	Default Language	Additional Language	Additional Language	
39995	English (United States)	None	None	Delete

Additional sites included in the directory: □ For-CS1K-Systems
Keypad entry: ENHANCED
BASIC: Enter extension only
ENHANCED: Enter extension or spell name
Speech recognition: ● enabled
○ disabled
The maximum number of speech recognition results: 1

6.2. Administer Telephony Integration

A SIP trunk needs to be configured from Messaging to Session Manager. Log into the Messaging System Management Interface (SMI) and go to **Administration → Messaging**. In the left panel, under **Telephony Settings (Application)** select **Telephony Integration**. In the right panel fill in the following:

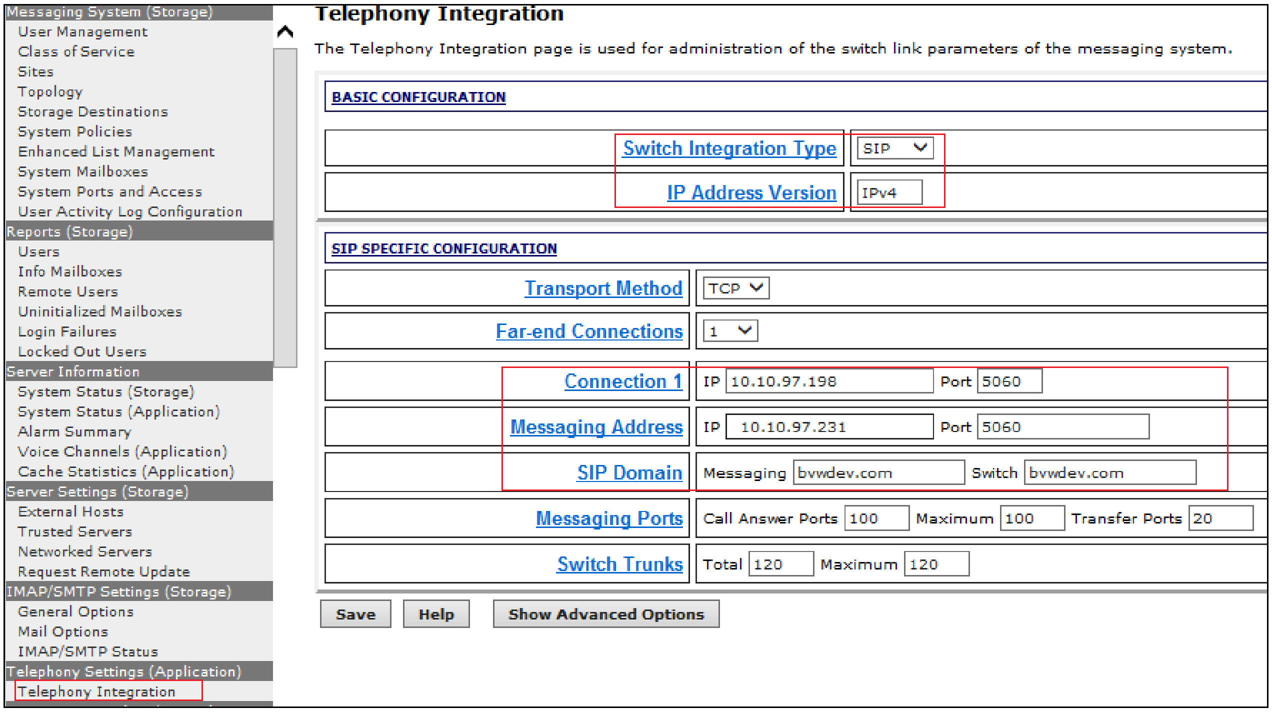
Under **Basic Configuration:**

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

Under **SIP Specific Configuration:**

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

Click **Save** to save changes.



Telephony Integration

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

BASIC CONFIGURATION

Switch Integration Type: SIP

IP Address Version: IPv4

SIP SPECIFIC CONFIGURATION

Transport Method: TCP

Far-end Connections: 1

Connection 1: IP 10.10.97.198 Port 5060

Messaging Address: IP 10.10.97.231 Port 5060

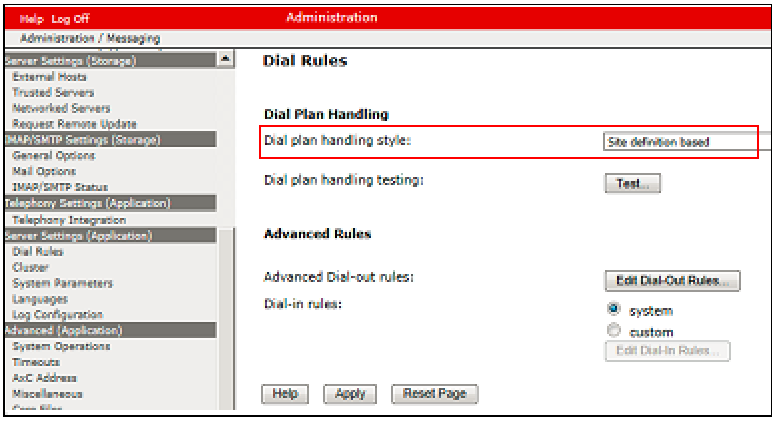
SIP Domain: Messaging bvwdev.com Switch bvwdev.com

Messaging Ports: Call Answer Ports 100 Maximum 100 Transfer Ports 20

Switch Trunks: Total 120 Maximum 120

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.



Dial Rules

Dial Plan Handling

Dial plan handling style: Site definition based

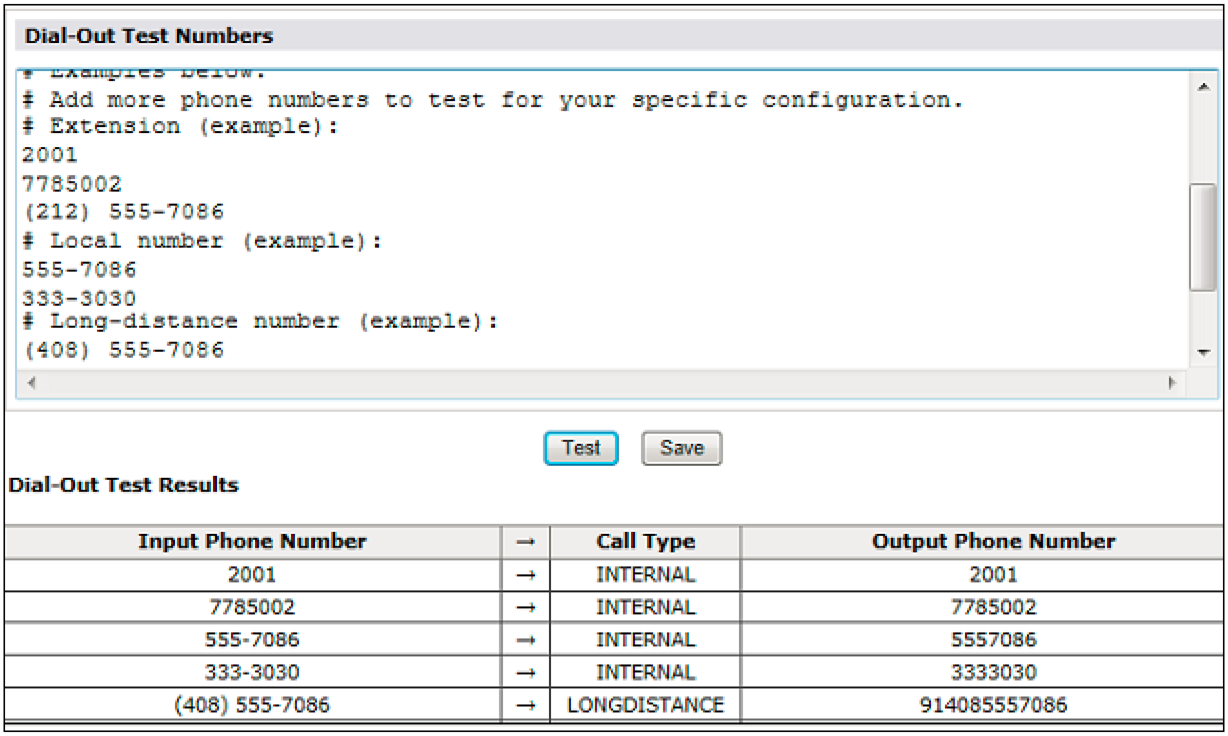
Dial plan handling testing:

Advanced Rules

Advanced Dial-out rules:

Dial-in rules: ● system ○ custom

Next select the **Edit Dial-Out Rules** button to verify the appropriate parameters for outbound dialing from Avaya Aura® Messaging were set above. These dial rules help Avaya Aura® Messaging send the correct number and combination of digits when originating a call to Communication Server, 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

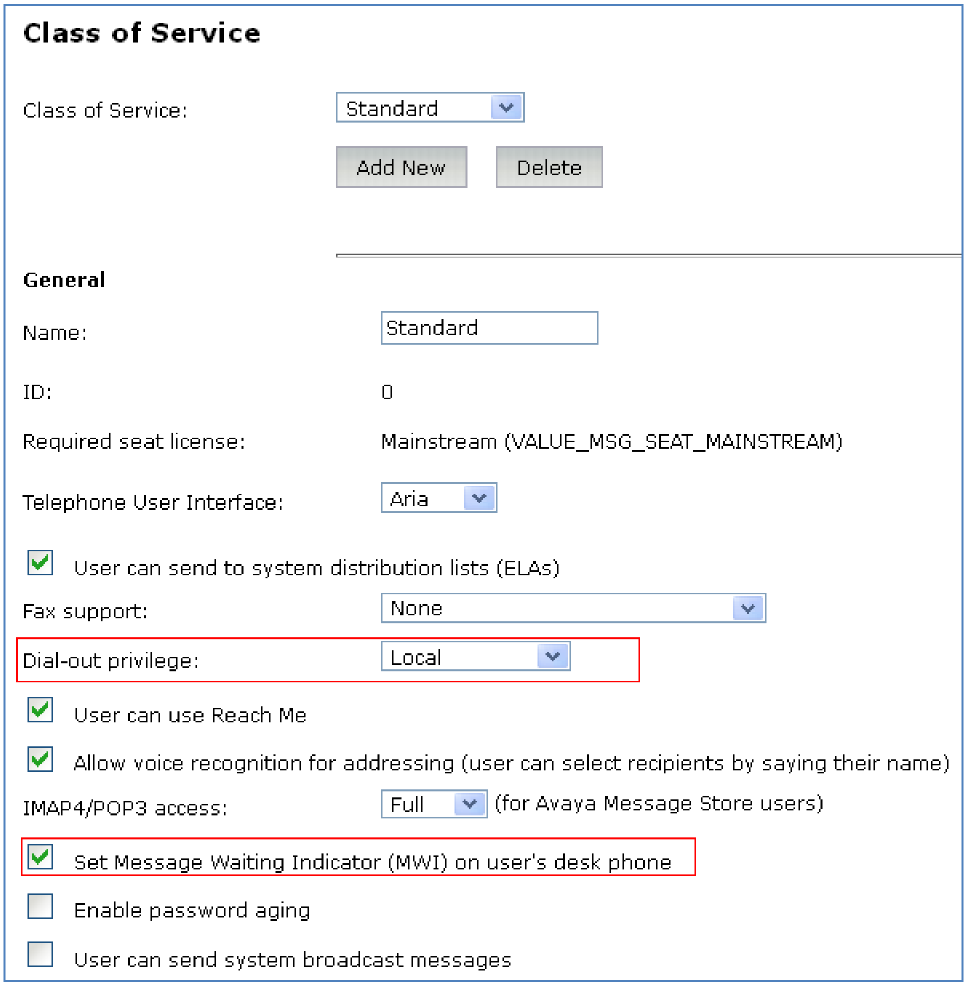
6.4. Configure Class of Service

Verify Messaging Waiting is enabled for all subscribers.
Use **Administration → Messaging** menu and select **Class of Service** under **Messaging System (Storage).** Select **"Standard"** from the **Class of Service** drop-down menu.
Under **General** section, enter the following value and use default values for remaining fields.

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

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

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

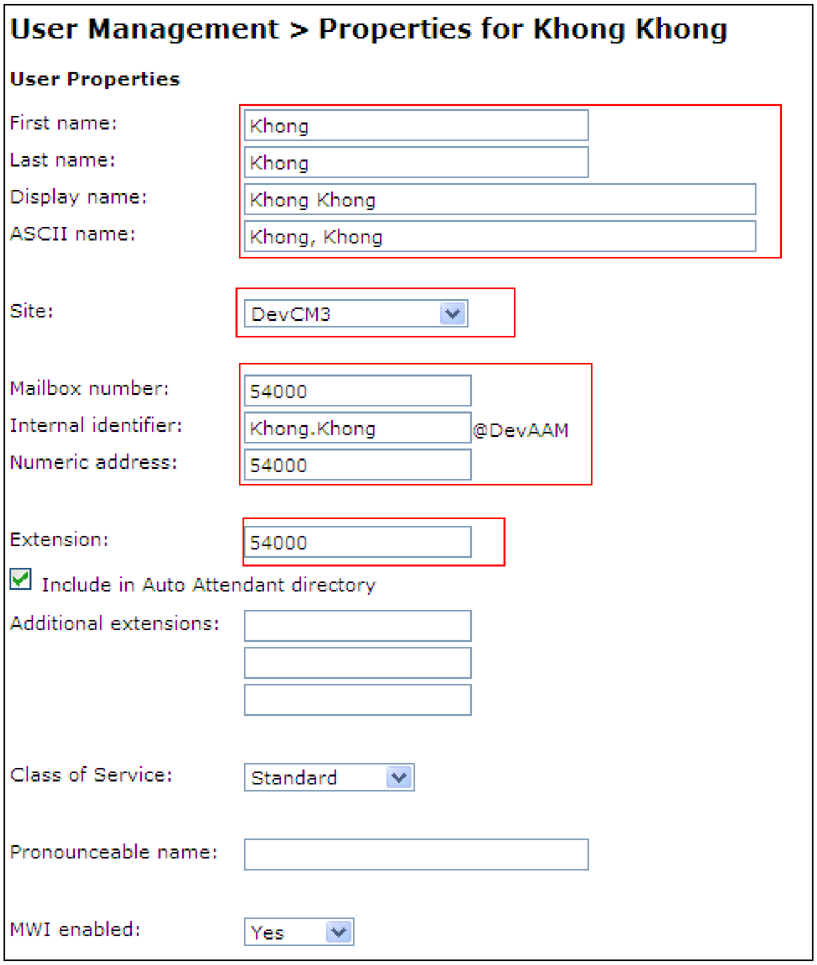
☐ User can send system broadcast messages

6.5. Administer Subscribers

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

Under **User Properties:**

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



User Management > Properties for Khong Khong

User Properties

First name: Khong

Last name: Khong

Display name: Khong Khong

ASCII name: Khong, Khong

Site: DevCM3

Mailbox number: 54000

Internal identifier: Khong.Khong @DevAAM

Numeric address: 54000

Extension: 54000

☑ Include in Auto Attendant directory

Additional extensions:

Class of Service: Standard

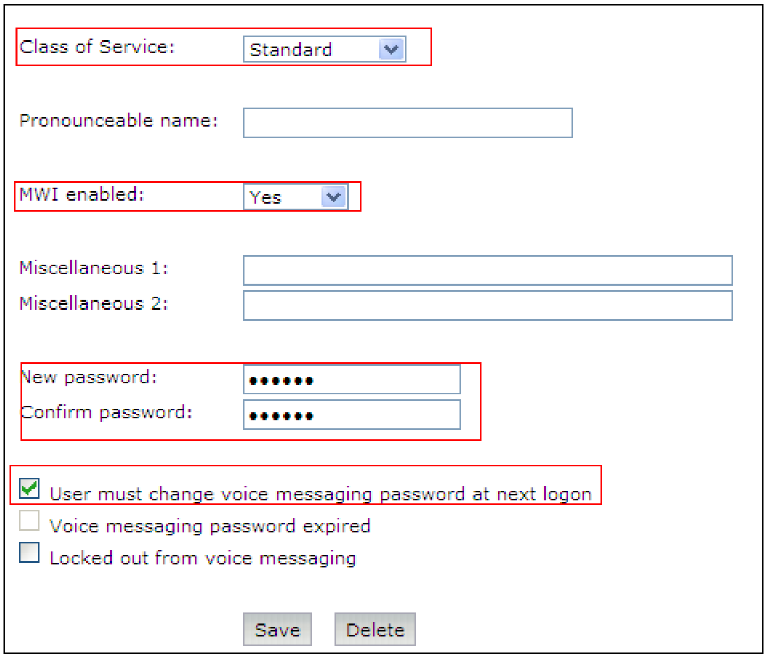
Pronounceable name:

MWI enabled: Yes

Scroll down on the page to Class of Service.

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

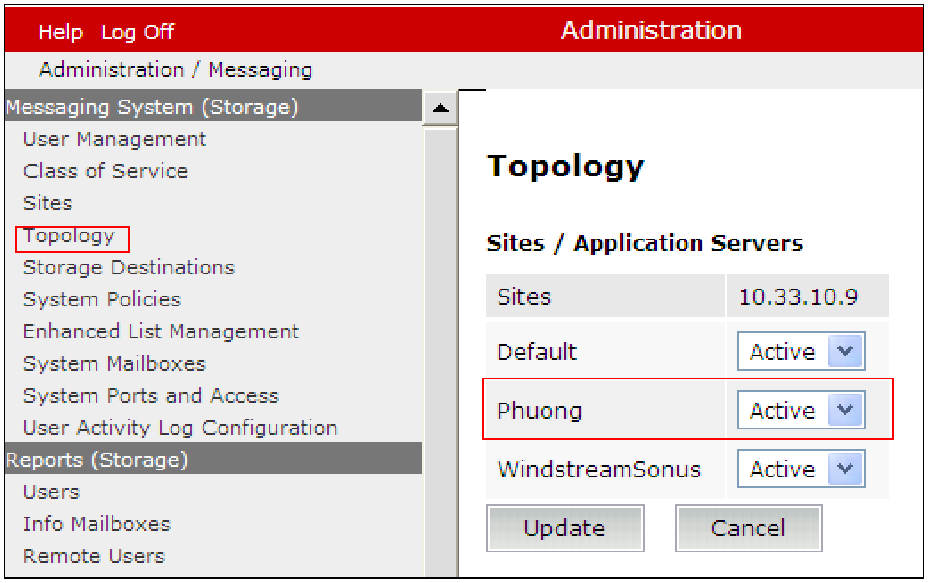
☑ User must change voice messaging password at next logon

□ Voice messaging password expired

□ Locked out from voice messaging

6.6. Administer Topology

Select **Topology** under **Messaging System (Storage)**.
Verify the site created in above section is **Active**.



Topology

Sites / Application Servers

Sites	10.33.10.9
Default	Active
Phuong	Active
WindstreamSonus	Active

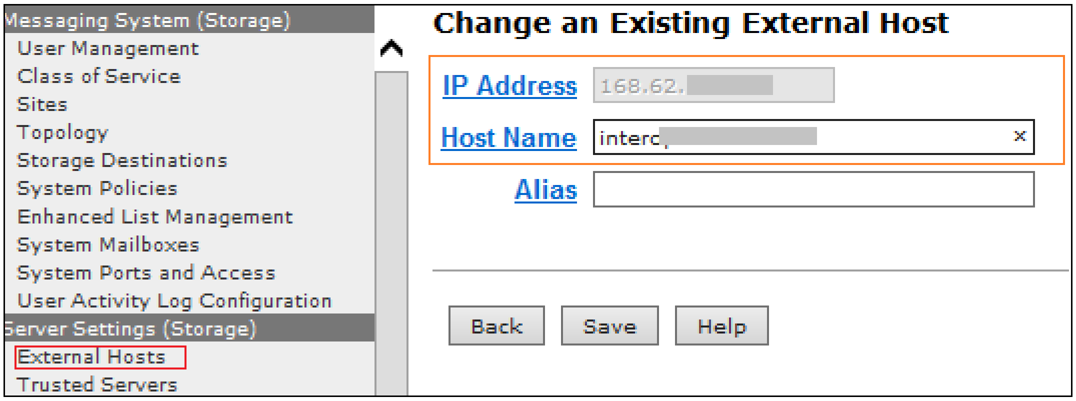
6.7. Administer External Host

Messaging uses an external SMTP relay host to forward text notifications and outbound voice. Messages enable this function by configuring the mail gateway on the External Hosts Web page.

Select **Server\Settings (Storage)** → **External Hosts**, and click **Add**.
In **Add a New External Host** page:

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

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



Change an Existing External Host

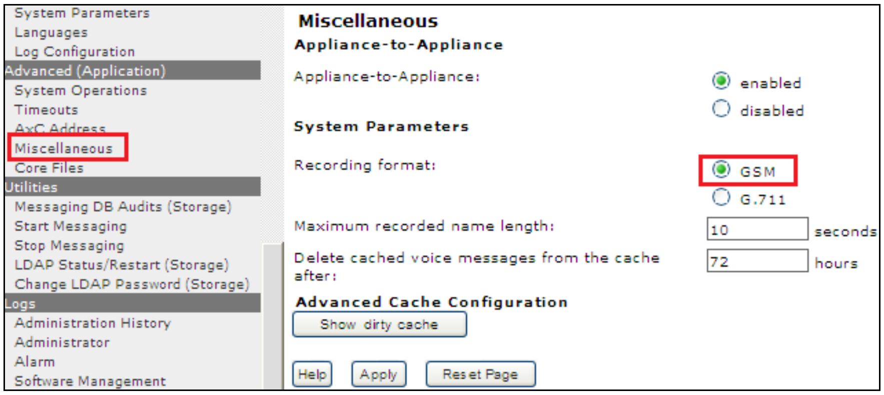
IP Address: 168.62.[redacted]

Host Name: interc[redacted]

Alias:

6.8. Recording Format

This setup is needed as ESNA is only able to recognize the record in GSM format only.



Miscellaneous

Appliance-to-Appliance

Appliance-to-Appliance: ● enabled ○ disabled

System Parameters

Recording format: ● GSM ○ G.711

Maximum recorded name length: 10 seconds

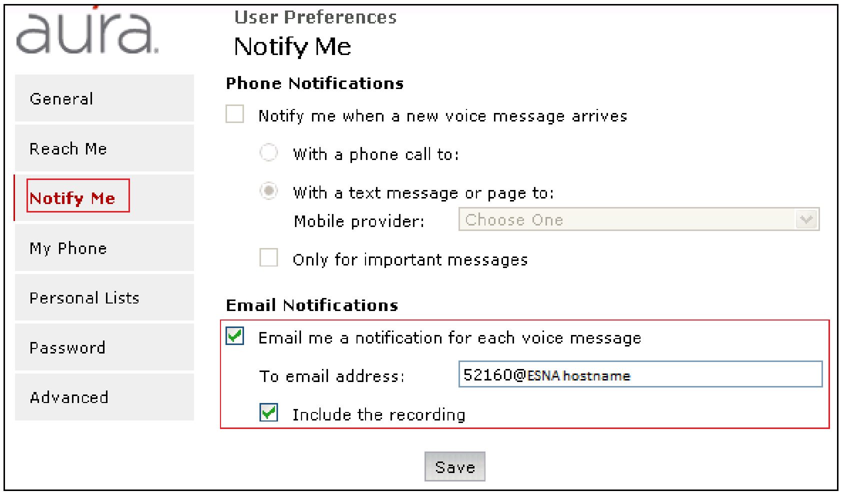
Delete cached voice messages from the cache after: 72 hours

Advanced Cache Configuration

6.9. Configure Notify Me

The Notify Me setting is used to allow a user to be notified on iLink Pro when they have the voice message from Avaya Aura Messaging. In the left panel, under **Messaging System (Storage)**, select **User Management**. In the right panel enter mailbox number (e.g. 54000) and click **Edit**. Scroll right down to **User Preferences** and select **Open User Preference for Mailbox number user name**:

In the **User Preferences** detail screen, select **Notify Me**. In the **Notify Me** detail page, enable checkbox for **Email me a notification for each voice message** to iLink Pro user's email address. For example, during compliance testing, the following email was used for the iLink Pro user that has extension 54000: 54000@ESNAhostname , with the option **Include the recording**. Click **Save**.



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

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 into Session Manager.

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

In this section, the following topics are discussed:

- SIP Domains
- Locations: Logical/physical location that can be occupied by SIP Entities.
- SIP Entities corresponding to Communication Server 1000 , Avaya Aura® Session Manager Messaging and Officelinx.
- Entity Links, which define the SIP trunk parameters used by Avaya Aura® Session Manager when routing calls to/from SIP Entities.
- Routing Policy, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.

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

7.1. Configure SIP Domain

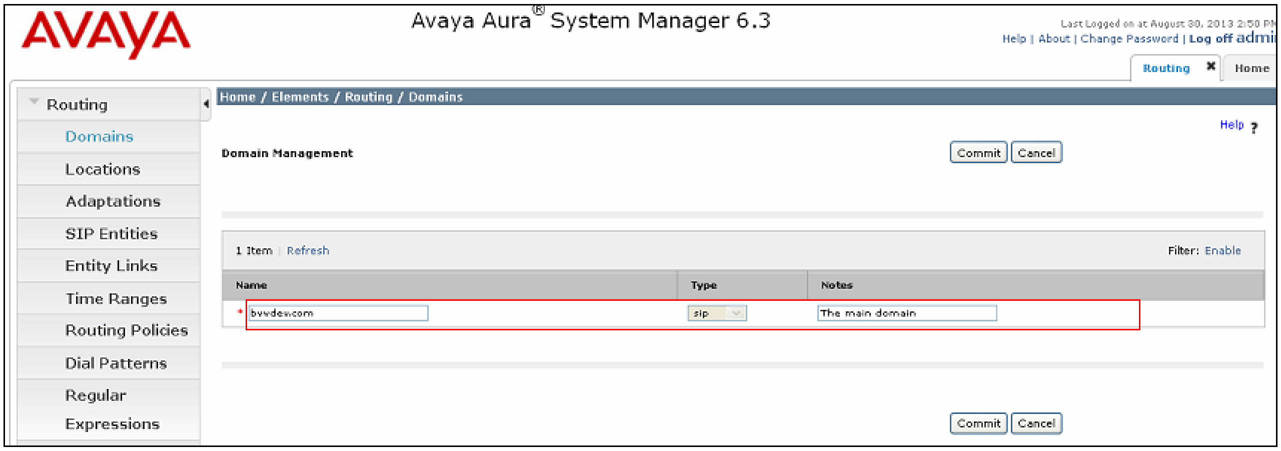
Launch a web browser, enter "**https://<IP address of System Manager>/SMGR**" in the URL, and log in with the appropriate credentials.

Create a SIP domain for each domain for which Avaya Aura® Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain: **bvwdev.com**.

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 remaining fields:

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

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



Domain Management

Name	Type	Notes
* bvwdev.com	sip	The main domain

7.2. Configure Locations

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

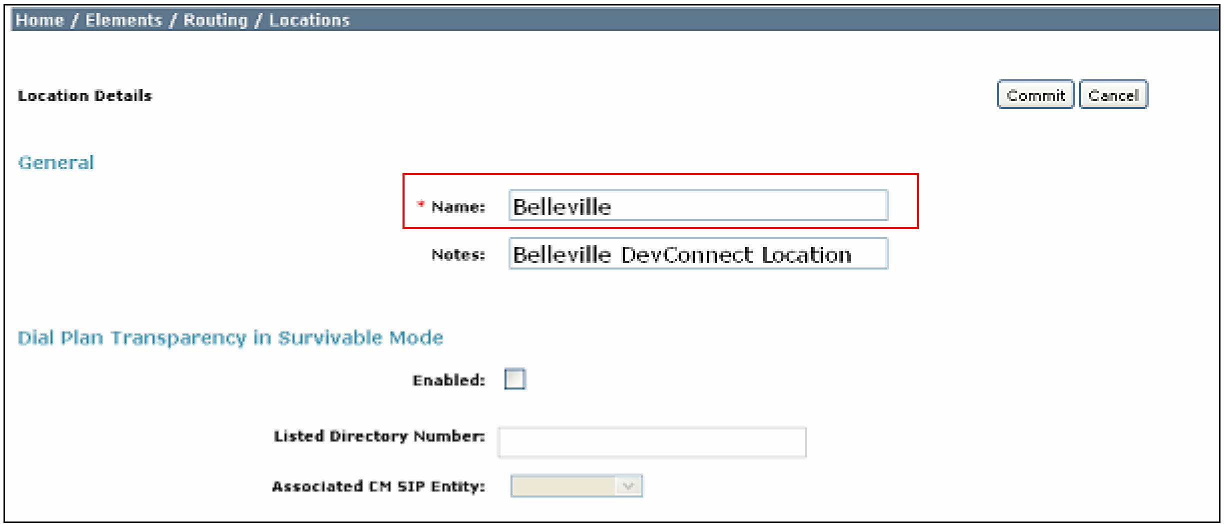
In **General** section, enter the following values and use default values for remaining fields.

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

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

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

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



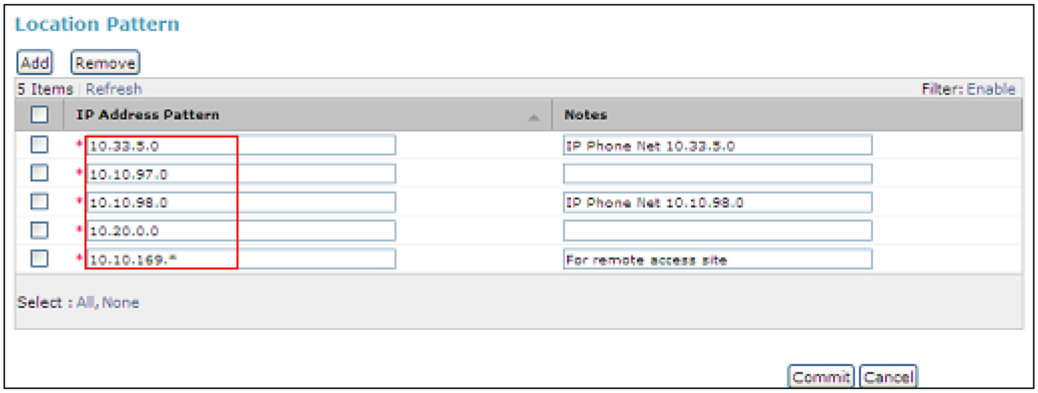
Location Details

General

* Name:	Belleville
Notes:	Belleville DevConnect Location

Dial Plan Transparency in Survivable Mode

Enabled:	□
Listed Directory Number:	
Associated CM SIP Entity:	



Location Pattern

□	IP Address Pattern	Notes
□	* 10.33.5.0	IP Phone Net 10.33.5.0
□	* 10.10.97.0	
□	* 10.10.98.0	IP Phone Net 10.10.98.0
□	* 10.20.0.0	
□	* 10.10.169.*	For remote access site

7.3. Configure SIP Entities

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

- Session Manager itself.
- Communication Server 1000
- Messaging
- ESNA Officelinx

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

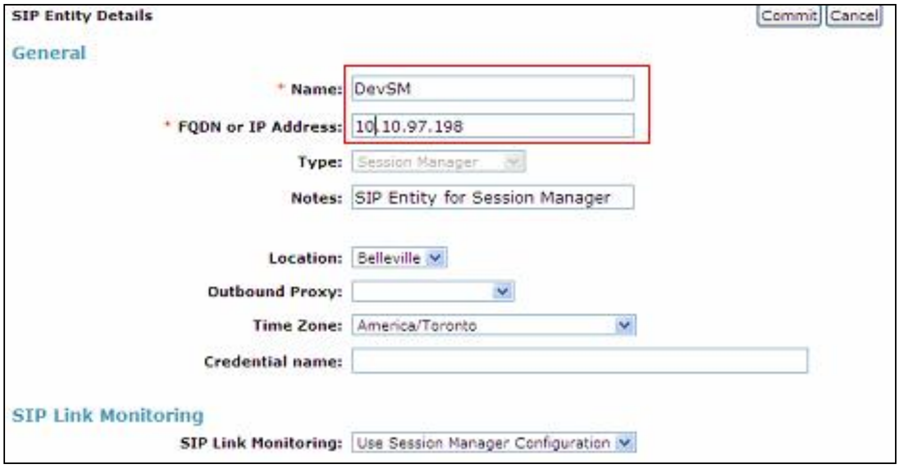
Enter the following values and use default values for remaining fields.

- Enter a descriptive name in the **Name** field.

- Enter **IP address** of SIP Entity that used for SIP signaling. Enter IP address of Communication Server 1000, Session Manager, Messaging and Officelinx.
- From the **Type** drop down menu select a type that best matches the SIP Entity. For Communication Server 1000, select **Other** For Session Manager, select **Session Manager**. For Messaging, select **Modular Messaging**. For **Officelinx**, select **Other**
- Enter a description in the **Notes** field if desired.
- Select the appropriate location.
- Select the appropriate time zone.
- Accept the other default values.

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

Session Manager SIP Entity:



SIP Entity Details

General

* Name: DevSM

* FQDN or IP Address: 10.10.97.198

Type: Session Manager

Notes: SIP Entity for Session Manager

Location: Belleville

Outbound Proxy:

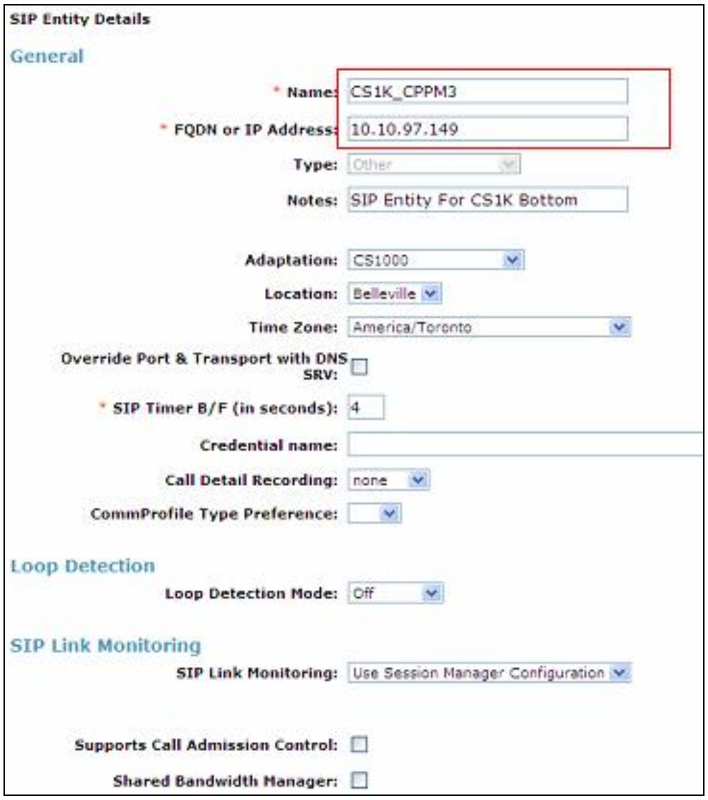
Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Communication Server 1000 SIP Entity:



SIP Entity Details

General

* Name: CS1K_CPPM3

* FQDN or IP Address: 10.10.97.149

Type: Other

Notes: SIP Entity For CS1K Bottom

Adaptation: CS1000

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

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

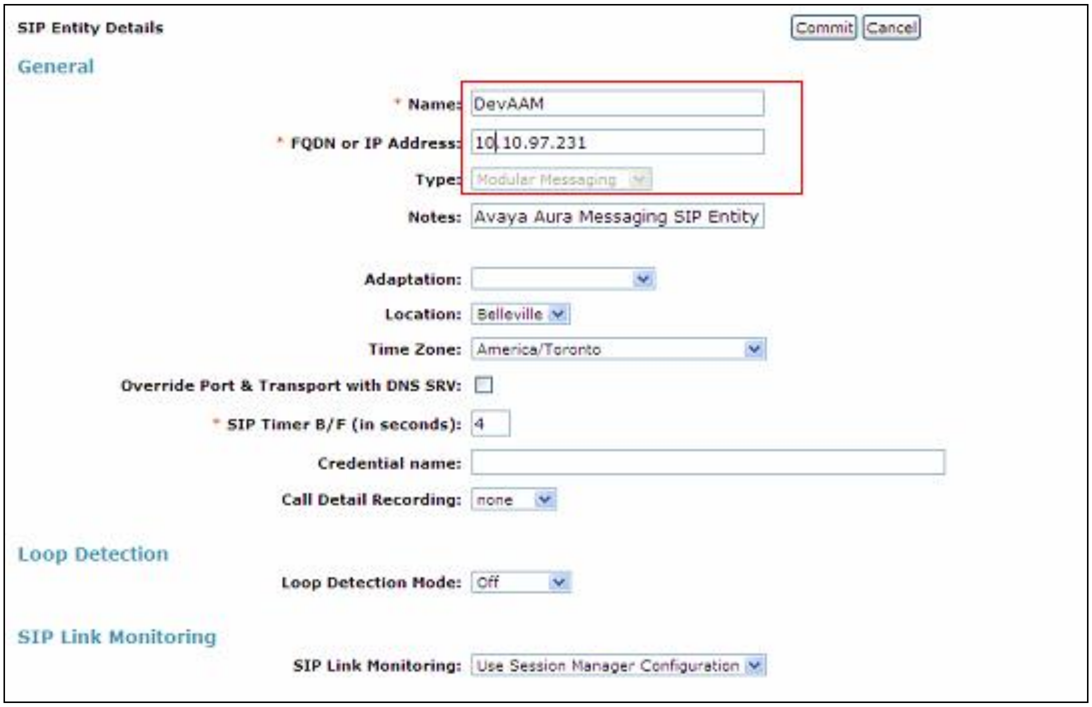
SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

AAM SIP Entity:



SIP Entity Details

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

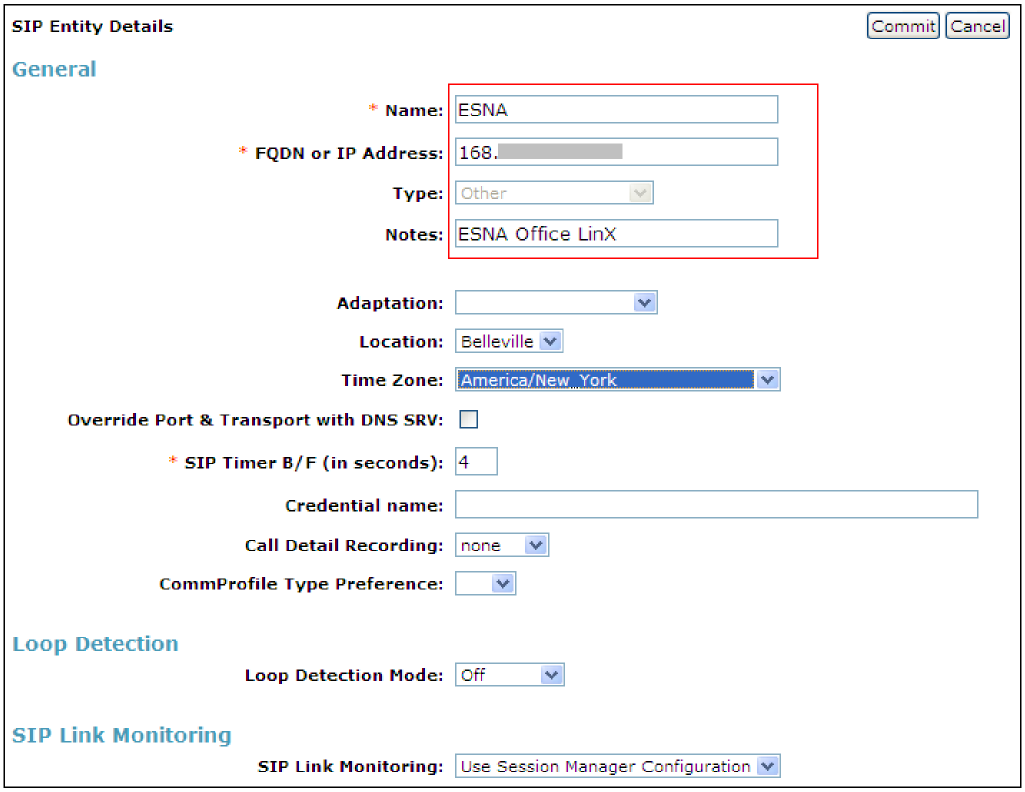
Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

ESNA Officelinx Entity:



General

* Name: ESNA

* FQDN or IP Address: 168.[redacted]

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

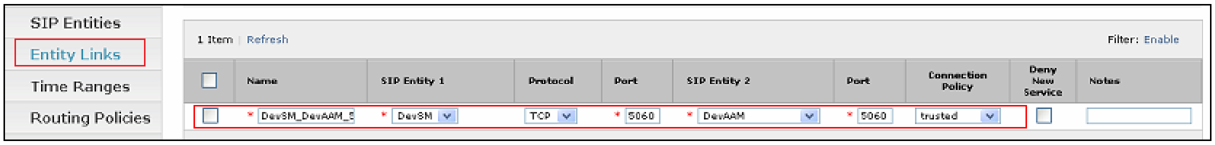
SIP Link Monitoring: Use Session Manager Configuration

7.4. Configure Entity Links

Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the 3 entities links are defined: one to Communication Server 1000, one to Messaging and one to Officelinx. Add an entity link, navigate to **Routing → Entity Links**, and click on the **New** button (not shown) to create a new entity link. Provide the following information:

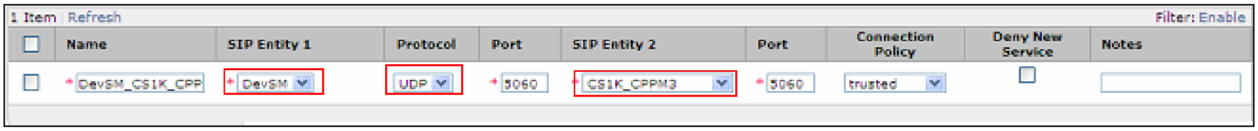
- Enter a descriptive name in the **Name** field.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity.
- In the **Protocol** drop down menu, select the protocol to be used.
- In the **Port** field, enter the port to be used, UDP or TCP – 5060
- In the **SIP Entity 2** drop down menu, select an entity for desired entity.
- In the **Port** field, enter the port to be used (e.g. **5060**).
- Select the **Trusted** option.
- Enter a description in the **Notes** field if desired.

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



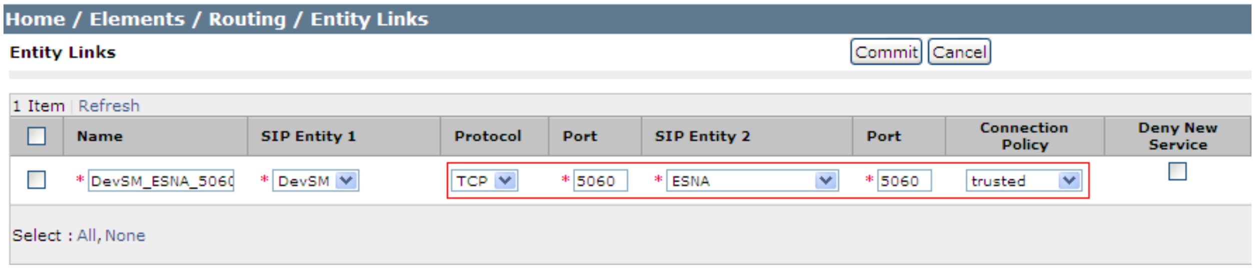
□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
□	* DevSM_DevAAM_5	* DevSM	TCP	* 5060	* DevAAM	* 5060	trusted	□	

Repeat the steps to define an Entity Link between Session Manager and Communication Server 1000 (UDP – 5060).



□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
□	* DevSM_CS1K_CPP	* DevSM	UDP	* 5060	* CS1K_CPPM3	* 5060	trusted	□	

Entity Link page (between Session Manager – ESNA Officelinx): **DevSM_ESNA_5060_TCP**



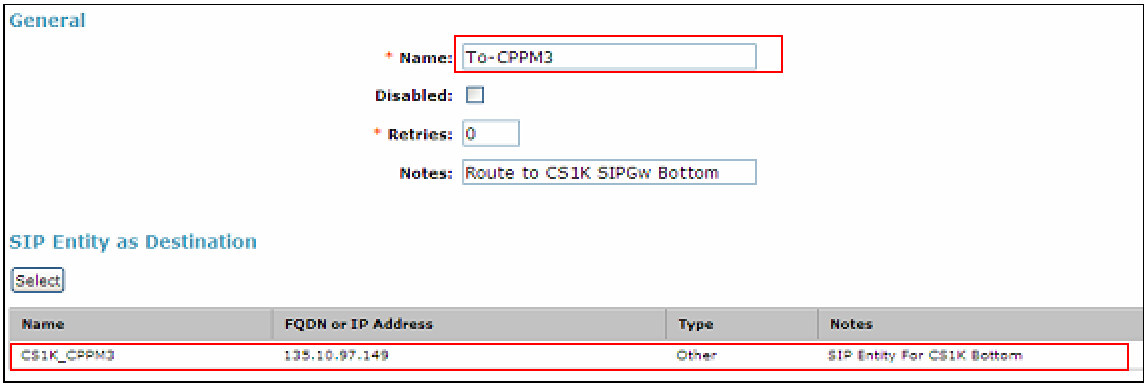
□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	* DevSM_ESNA_506(	* DevSM	TCP	* 5060	* ESNA	* 5060	trusted	□

7.5. Configure Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities. Three routing policies must be added: one for Communication Server 1000, one for Messaging and one to Officelinx. To add a routing policy, navigate to **Routing →Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following: In the **General** section, enter the following values. Use default values for all remaining fields:

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

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP entity displays on the **Routing Policy Details** page as shown below. Use default values for the remaining fields. Click **Commit** to save. The following screen shows the Routing Policy to Communication Server 1000.



General

* Name: To-CPPM3

Disabled: □

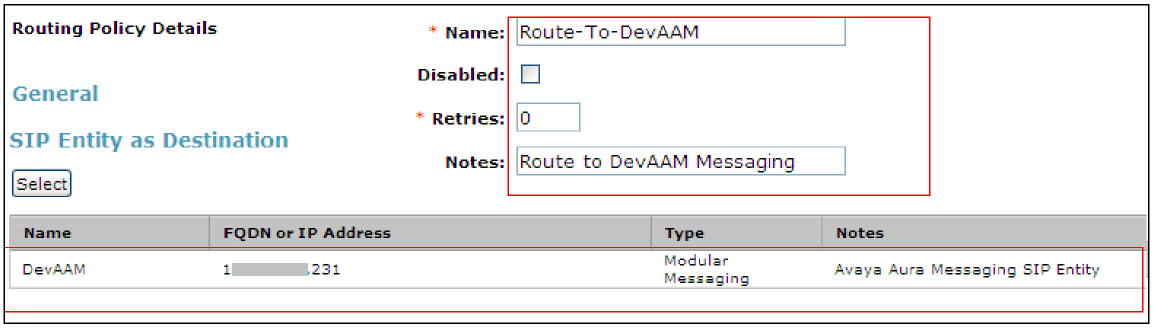
* Retries: 0

Notes: Route to CS1K SIPGw Bottom

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CS1K_CPPM3	135.10.97.149	Other	SIP Entity For CS1K Bottom

Repeat the steps to define routing policies to others Entities. Routing policy used for Messaging: **Route-To-DevAAM**.



Routing Policy Details

General

SIP Entity as Destination

* Name: Route-To-DevAAM

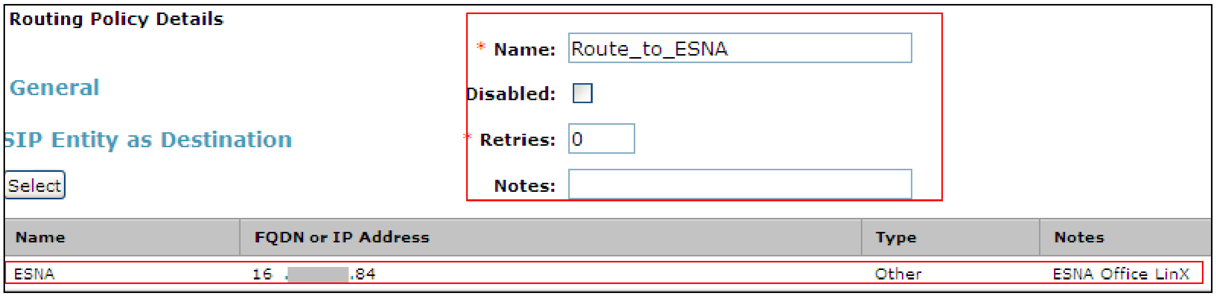
Disabled: □

* Retries: 0

Notes: Route to DevAAM Messaging

Name	FQDN or IP Address	Type	Notes
DevAAM	1[redacted].231	Modular Messaging	Avaya Aura Messaging SIP Entity

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



Routing Policy Details

General

SIP Entity as Destination

Select

* Name:	Route_to_ESNA
Disabled:	☐
* Retries:	0
Notes:	

Name	FQDN or IP Address	Type	Notes
ESNA	16 .[redacted].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.

- 54xxx – SIP endpoints
- 399xx – Pilot Number.
- 78xxx – Officelinx Number

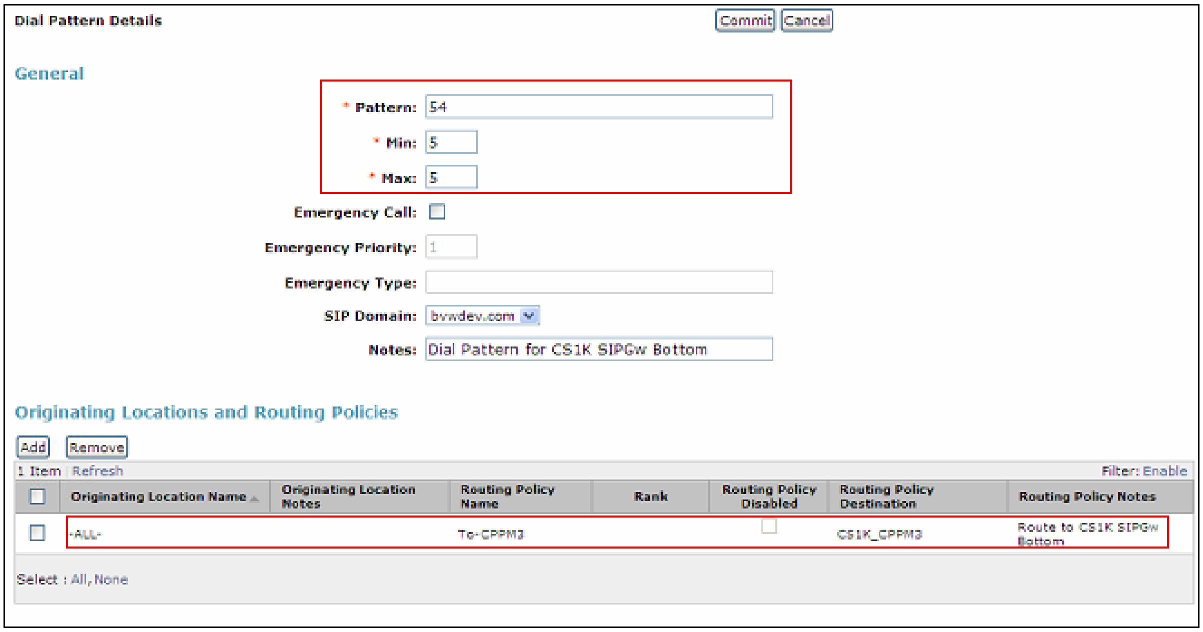
To add a Dial Pattern, select **Routing → Dial Patterns,** and click on the **New** button (not shown) on the right. During the compliance test, 5 digit dial plan was utilized. Provide the following information:
In the **General** section, enter the following values. Use default values for all remaining 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 **Commit** to save.

Click the **Commit** button to save the new definition. The following screen shows the dial pattern used for Communication Server 1000 during the compliance test.



Dial Pattern Details

General

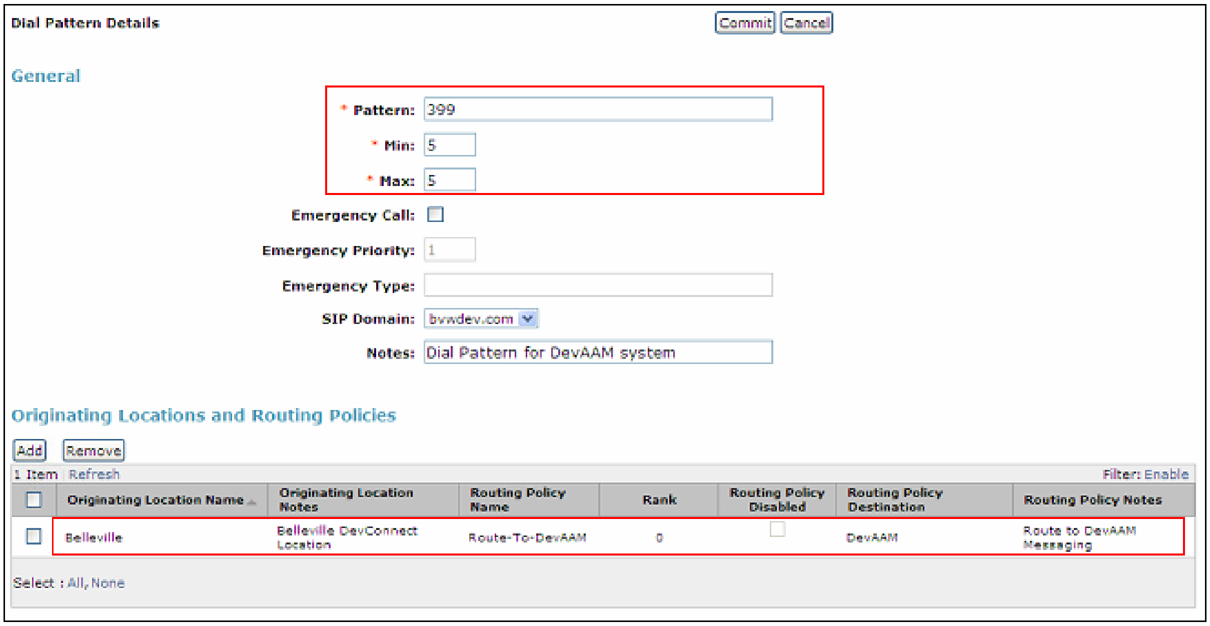
* Pattern:	54
* Min:	5
* Max:	5
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	bvwdev.com
Notes:	Dial Pattern for CS1K SIPGw Bottom

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		To-CPPM3		□	CS1K_CPPM3	Route to CS1K SIPGw Bottom

Select : All, None

Below is Dial Pattern for AAM:



Dial Pattern Details

General

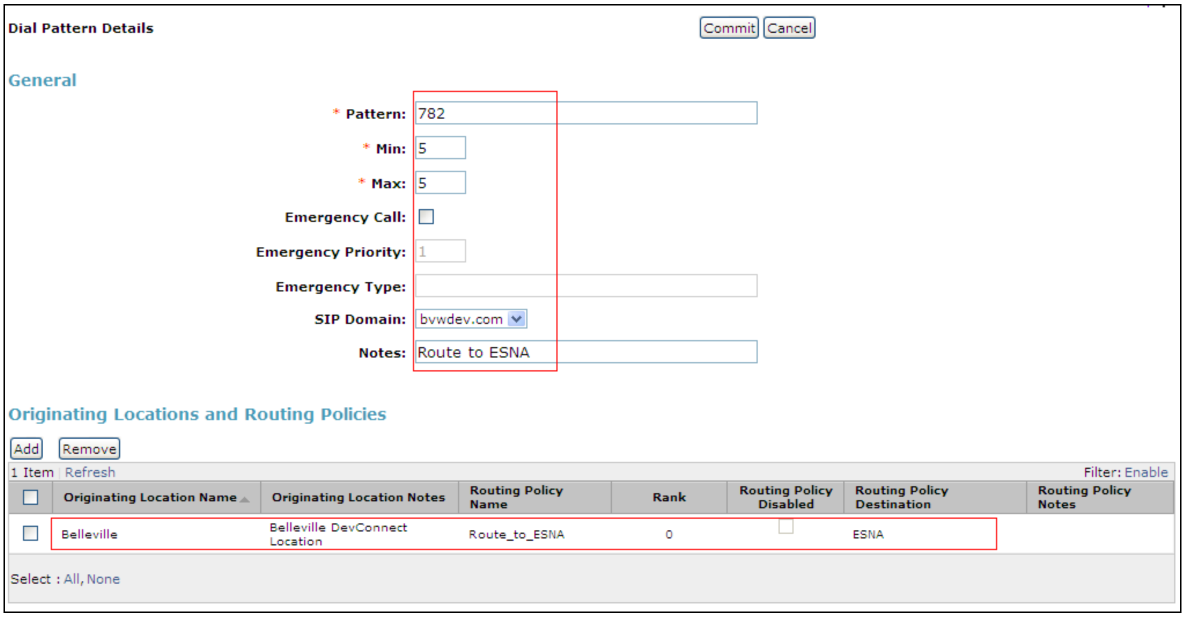
* Pattern:	399
* Min:	5
* Max:	5
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	bvwdev.com
Notes:	Dial Pattern for DevAAM system

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Belleville	Belleville DevConnect Location	Route-To-DevAAM	0	□	DevAAM	Route to DevAAM Messaging

Select : All, None

Dial Pattern for ESNA Officelinx: **78xxx**.



Dial Pattern Details

General

* Pattern:	782
* Min:	5
* Max:	5
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	bvwdev.com
Notes:	Route to ESNA

Originating Locations and Routing Policies

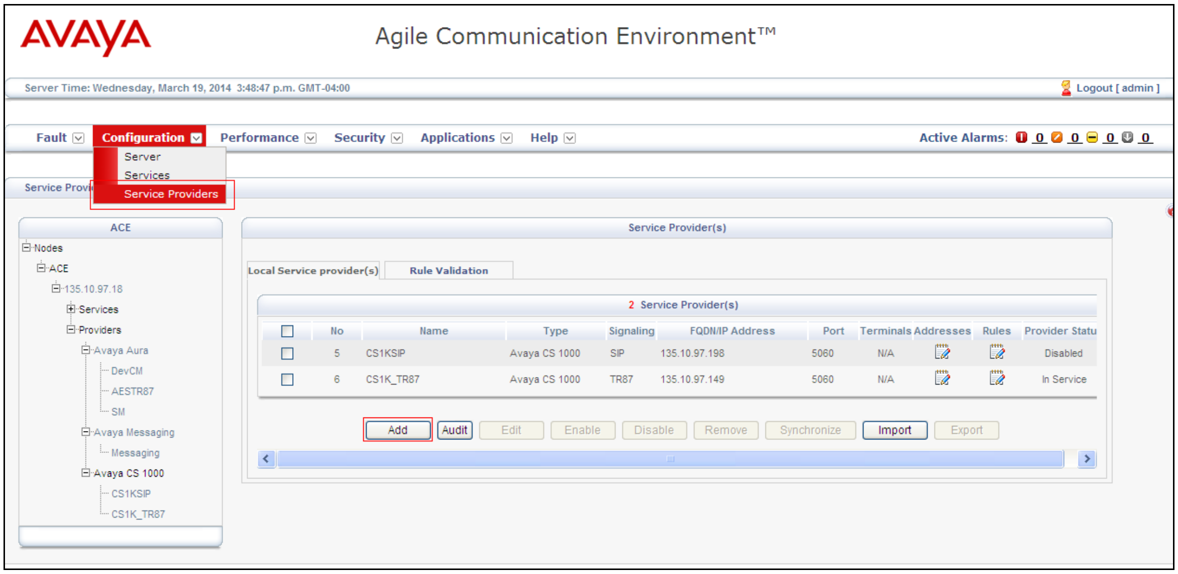
□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Belleville	Belleville DevConnect Location	Route_to_ESNA	0	□	ESNA	

Select : All, None

8. Configure Avaya ACE 6.2 FP2

8.1. Add Communication Server 1000 TR/78 Service Provider

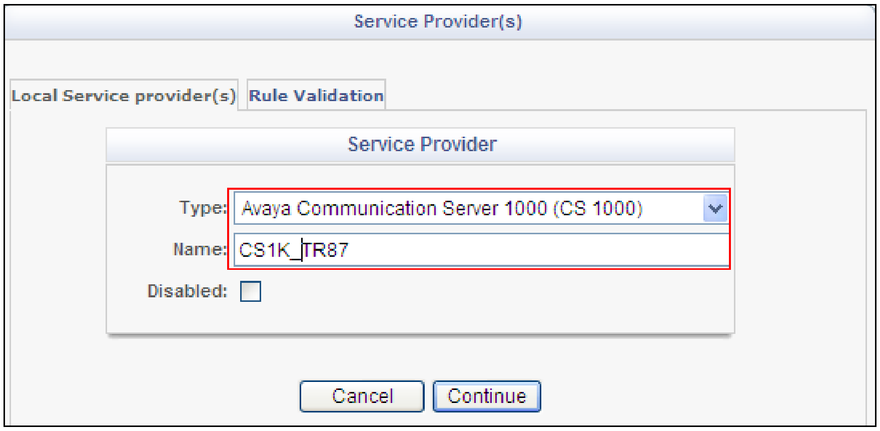
Add an Avaya CS 1000 TR/87 network element as a service provider on the Avaya ACE to enable communications between the Avaya CS 1000 element and the Avaya ACE using TR/87 protocol without advanced services support. On the menu bar, choose **Configuration → Service Providers**. In the Service Providers window, click **Add** as shown below:



☐	No	Name	Type	Signaling	FQDN/IP Address	Port	Terminals	Addresses	Rules	Provider Statu
☐	5	CS1KSIP	Avaya CS 1000	SIP	135.10.97.198	5060	N/A			Disabled
☐	6	CS1K_TR87	Avaya CS 1000	TR87	135.10.97.149	5060	N/A			In Service

Select Service Provider type and enter name as below:

- **Type**: select **Avaya Communication Server 1000(CS 1000)**.
- **Name**: enter a name for the CS10000 service provider.

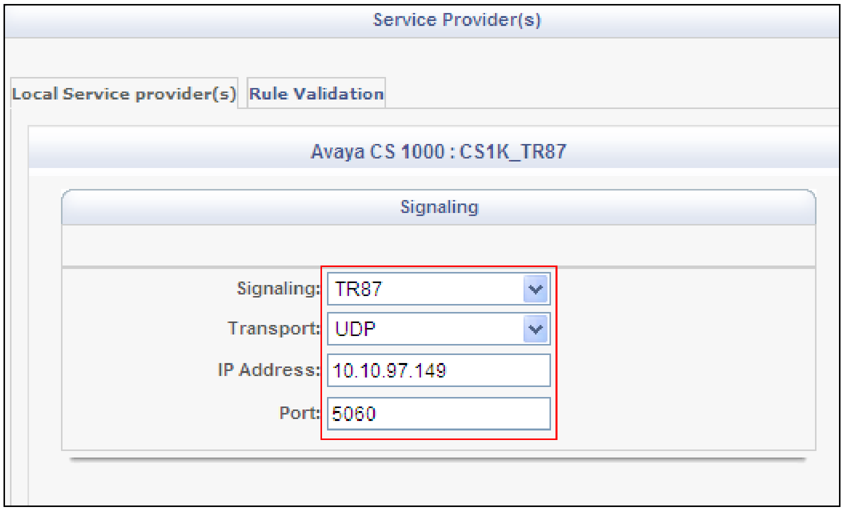


Type: Avaya Communication Server 1000 (CS 1000)
Name: CS1K_TR87
Disabled: ☐

Click **Continue**. Enter detail information for Service Provider:

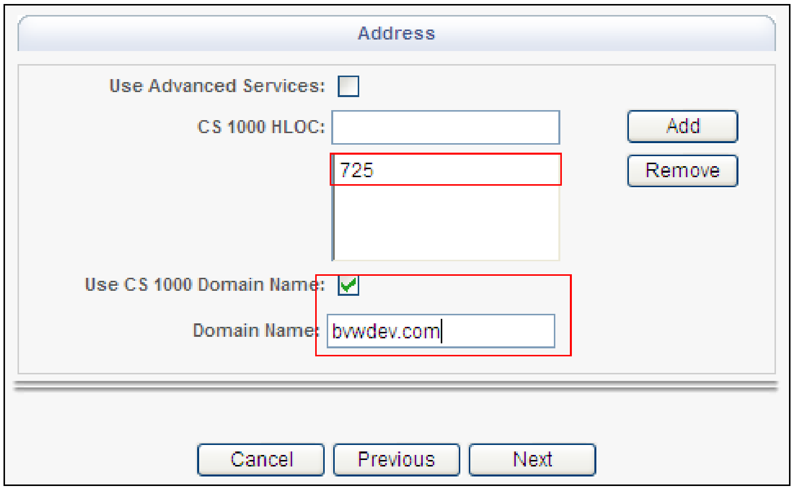
- **Signaling:** select **TR87**.
- **Transport**: select **UDP**.

- **IP Address**: enter the IP address of the **Communication Server 1000 Node**.
- **Port**: accept the default 5060 as the Transport is UDP.



Signaling: TR87
Transport: UDP
IP Address: 10.10.97.149
Port: 5060

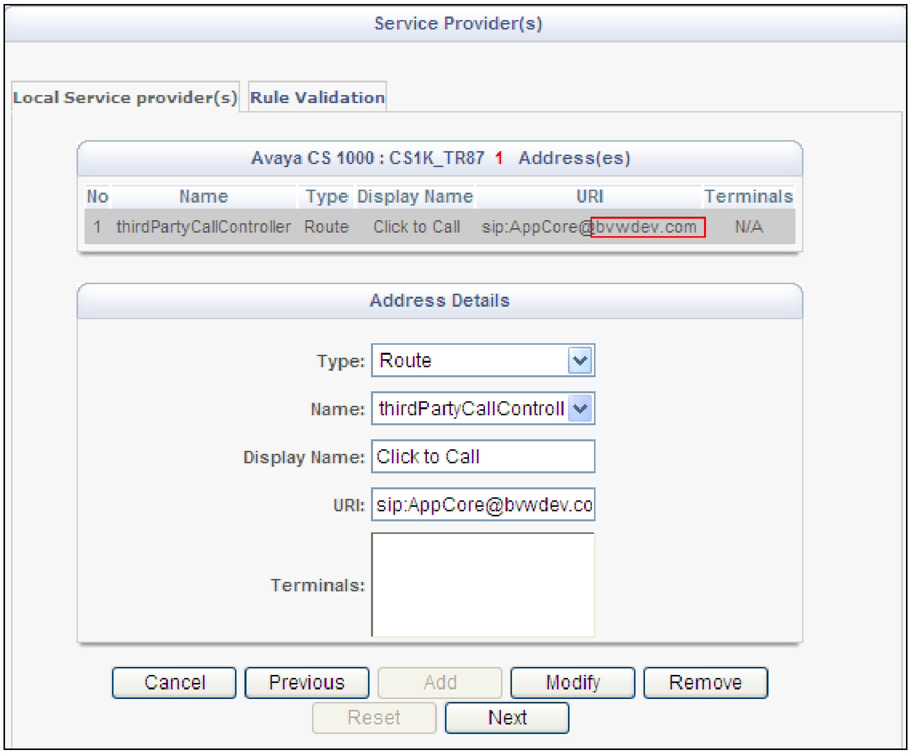
- **CS 1000 HLOC**: For networks with multiple systems (for example, an IP Peer Network), enter a one to seven-digit Home Location Code (HLOC) for the CS 1000, and click **Add**. *To find what is HLOC of CS1K, login to EM, select Dialing and Numbering Plans – Electronic Switch Network (ESN) and click on HLOC.*
- **Use CS 1000 Domain Name:** select checkbox. You must specify a CS 1000 domain name (which Avaya ACE appends to the outgoing TR/87 messages) so that messages can be routed to the appropriate node on the CS 1000.
- **Domain Name:** enter the CS 1000 domain name. In compliance test **bvwdev.com** is used.



Use Advanced Services: □
CS 1000 HLOC:
725
Use CS 1000 Domain Name: ☑
Domain Name: bvwdev.com

Click **Next** to add Address for CS1K TR87 Service provider. Configure the route address to indicate from where a call is originating.
A route address represents the third party in a third party call control call. When adding a service provider that supports third party call control, the system automatically adds a default route

address (sip:AppCore@avaya.com), modify this URI if needed. During compliance test the **URI** was modified to **sip:AppCore@bvwdev.com**



Avaya CS 1000 : CS1K_TR87 1 Address(es)

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

Address Details

Type:	Route
Name:	thirdPartyCallControll
Display Name:	Click to Call
URI:	sip:AppCore@bvwdev.co
Terminals:	

Click **Next** to enter the rule for TR87 Service Provider. Configure simple translation rules to route a web service request to a particular service provider and if necessary, transform the parameters in the request, before presenting them to the service provider.

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

- **URI Scheme** :tel
- **Range From/To**: 54000-54399
- **Activate Rule:** checked box.

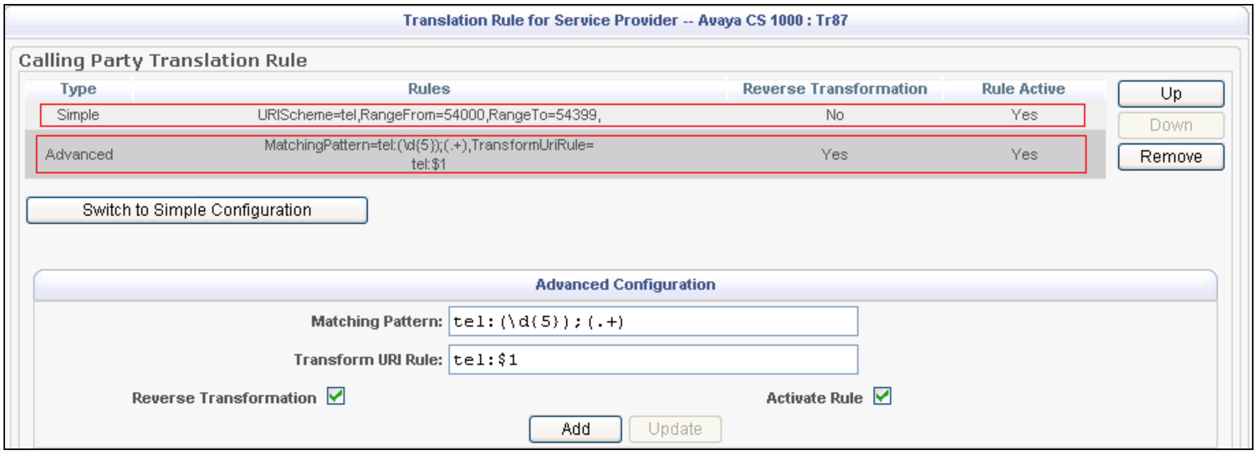
Click **Add** to add a new rule.

Click **Switch to Advanced Configuration** to add an Advanced **Reserve Transformation** rule. This configure is to remove phone-context in the Call event.

- **Matching Pattern** enter: tel:(\d{5});(.+).
- **Transform URI Rule** enter: tel:$1.

This is specific to the DevConnect lab configuration during compliance test in order to transfer **tel:54331;phone-context=cdp.udp** to **tel:54331**

Below figure is an example of Calling Party Translation Rules during testing this solution:



Translation Rule for Service Provider -- Avaya CS 1000 : Tr87

Calling Party Translation Rule

Type	Rules	Reverse Transformation	Rule Active
Simple	URIScheme=tel,RangeFrom=54000,RangeTo=54399,	No	Yes
Advanced	MatchingPattern=tel:(\d{5});(.+),TransformUriRule= tel:$1	Yes	Yes

Advanced Configuration

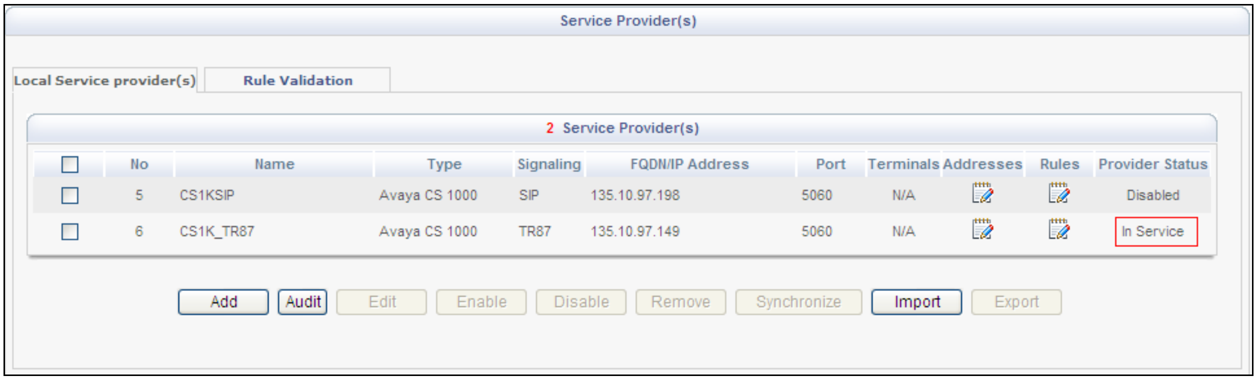
Matching Pattern: tel:(\d{5});(.+)

Transform URI Rule: tel:$1

Reverse Transformation ☑ Activate Rule ☑

Click **Next** to configure called party translation rules. Click **Submit** to save the rule configuration.

Verify the status of added service providers is “**In Service**”:



2 Service Provider(s)

☐	No	Name	Type	Signaling	FQDN/IP Address	Port	Terminals	Addresses	Rules	Provider Status
☐	5	CS1KSIP	Avaya CS 1000	SIP	135.10.97.198	5060	N/A	📝	📝	Disabled
☐	6	CS1K_TR87	Avaya CS 1000	TR87	135.10.97.149	5060	N/A	📝	📝	In Service

8.2. Add User

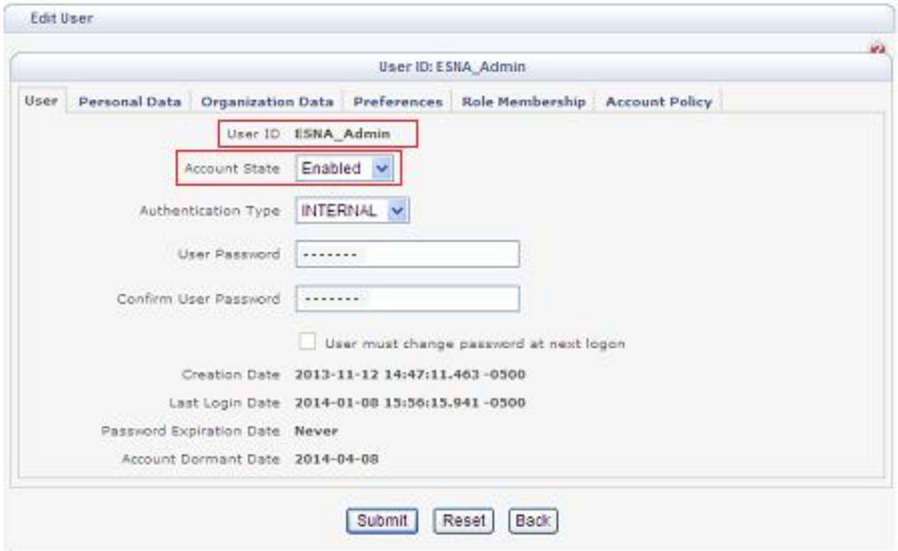
The web service client ESNA Officelinx – Avaya ACE Wizard is a configured user on Avaya ACE.

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

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

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

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



User ID: ESNA_Admin

User ID	ESNA_Admin
Account State	Enabled
Authentication Type	INTERNAL
User Password	-------
Confirm User Password	-------
	□ User must change password at next logon
Creation Date	2013-11-12 14:47:11.463 -0500
Last Login Date	2014-01-08 15:56:15.941 -0500
Password Expiration Date	Never
Account Dormant Date	2014-04-08

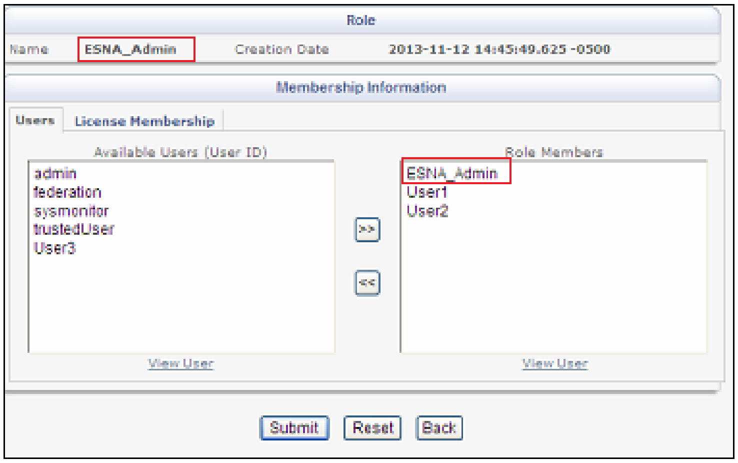
8.3. Add Role

This section describes the step on how to create Role for user created in above section.

Select **Security → Role Management → Create Role.** Enter the following for a new Role:

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

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



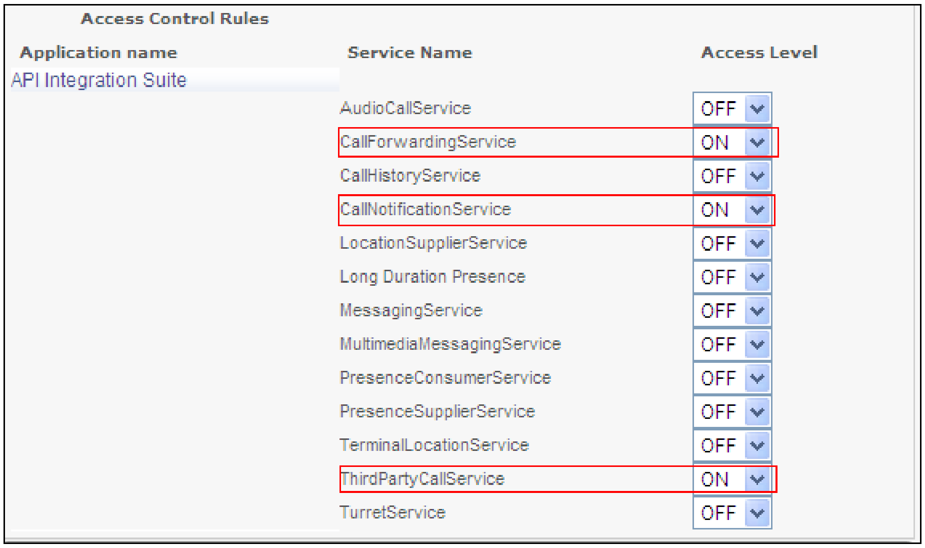
Role

Name: ESNA_Admin Creation Date: 2013-11-12 14:45:49.625 -0500

Membership Information

Available Users (User ID)	Role Members
admin	ESNA_Admin
federation	User1
sysmonitor	User2
trustedUser	
User3	

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



Access Control Rules

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

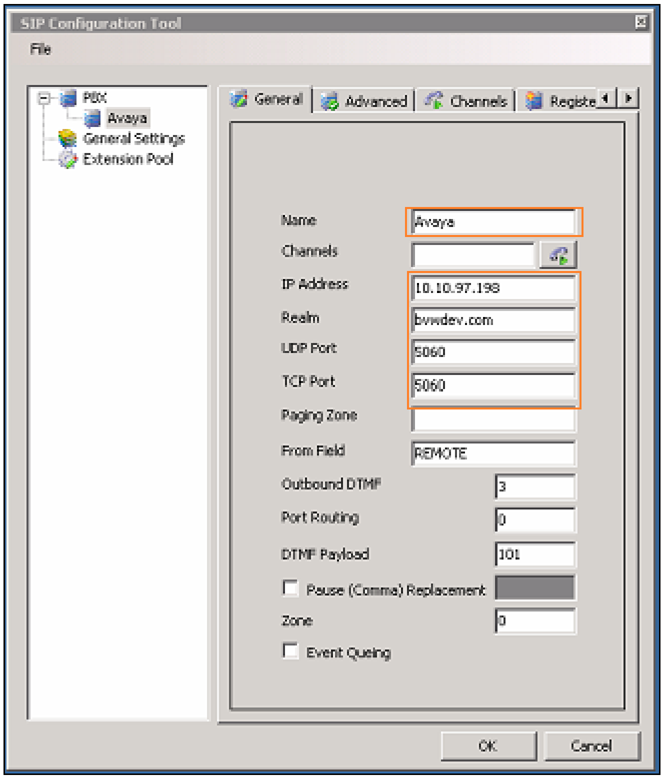
9. Configure the ESNA Telephony Officelinx

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 provided 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**. Select **Avaya** under **PBX** in the left pane. Provide the following information:

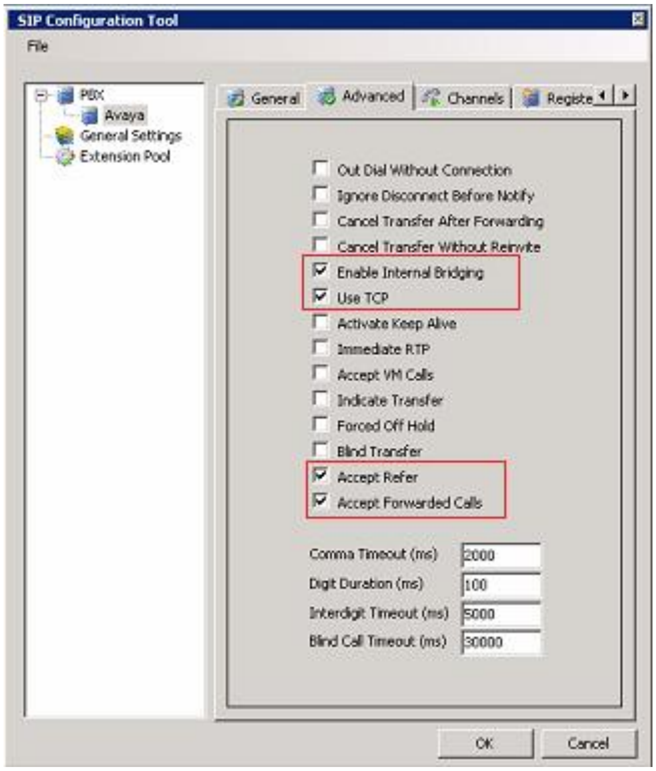
- **Name** – Type in any descriptive name.
- **IP Address** – Enter **IP address** of **Session Manager**, example: 10.10.97.198.
- **Realm** – Enter a valid domain that is configured in the system, example: bvwdev.com.
- **UDP Port** – Enter **5060**
- **TCP Port** – Enter **5060**



Name: Avaya
Channels:
IP Address: 10.10.97.198
Realm: bvwdev.com
UDP Port: 5060
TCP Port: 5060
Paging Zone:
From Field: REMOTE
Outbound DTMF: 3
Port Routing: 0
DTMF Payload: 101
☐ Pause (Comma) Replacement
Zone: 0
☐ Event Queing

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

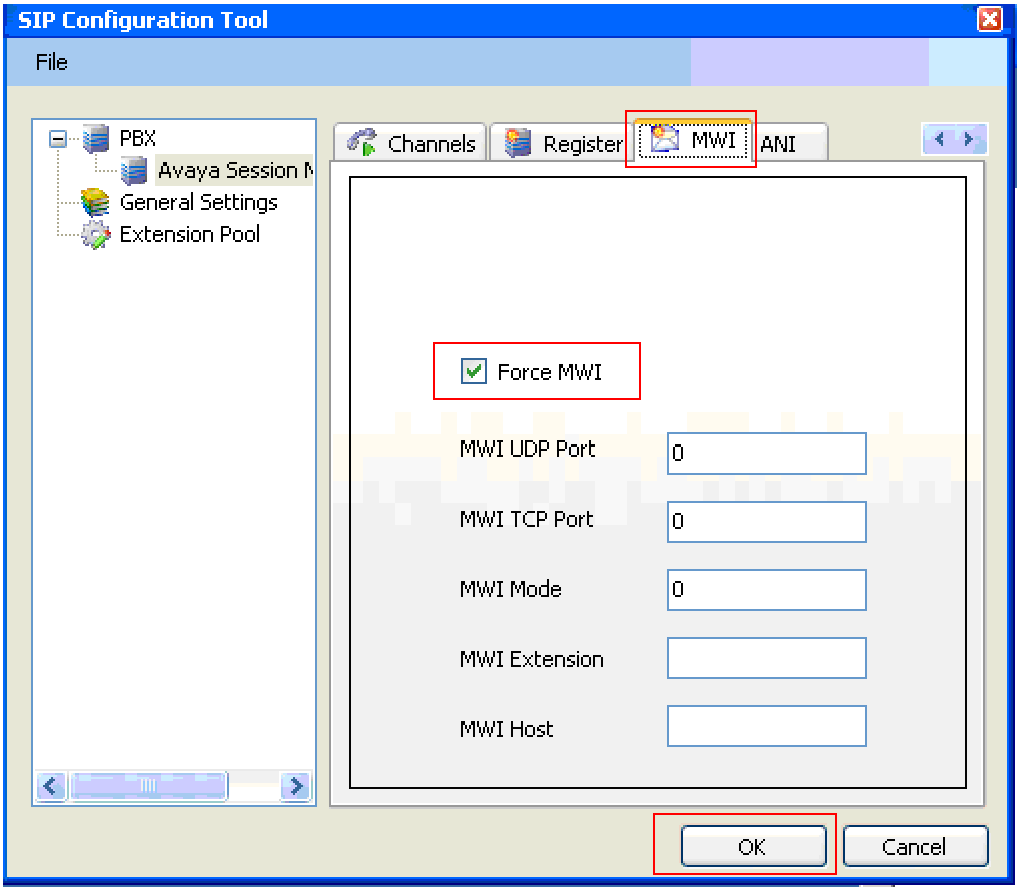
- **Enable Internal Bridging**
- **Use TCP**
- **Accept Refer**
- **Accept Forward Calls**



□ Out Dial Without Connection
□ Ignore Disconnect Before Notify
□ Cancel Transfer After Forwarding
□ Cancel Transfer Without Reinvite
☑ Enable Internal Bridging
☑ Use TCP
□ Activate Keep Alive
□ Immediate RTP
□ Accept VM Calls
□ Indicate Transfer
□ Forced Off Hold
□ Blind Transfer
☑ Accept Refer
☑ Accept Forwarded Calls

Comma Timeout (ms)	2000
Digit Duration (ms)	100
Interdigit Timeout (ms)	5000
Blind Call Timeout (ms)	30000

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



☑ Force MWI

MWI UDP Port: 0

MWI TCP Port: 0

MWI Mode: 0

MWI Extension:

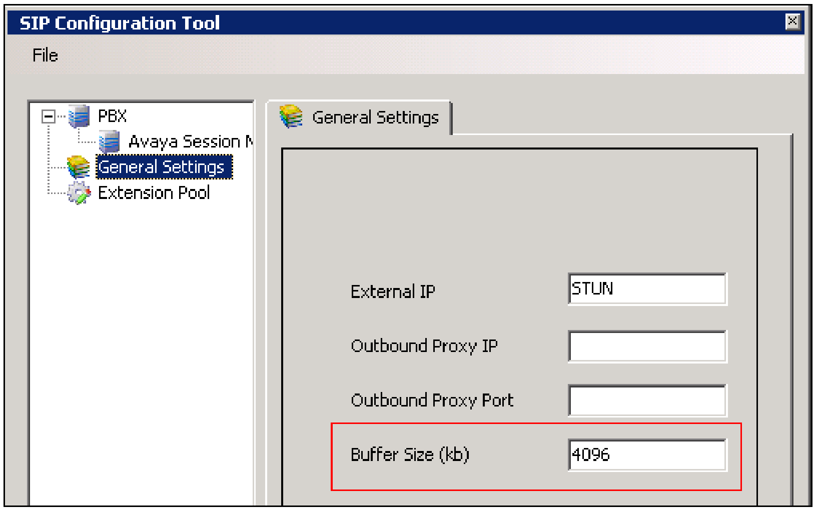
MWI Host:

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

Subscription State for MWI = 0

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

Click **PBX – General Settings**. Set **Buffer Size (kb)** to 4096. This configuration allows Officelinx to handle SIP messages sent from Session Manager.



External IP: STUN

Outbound Proxy IP:

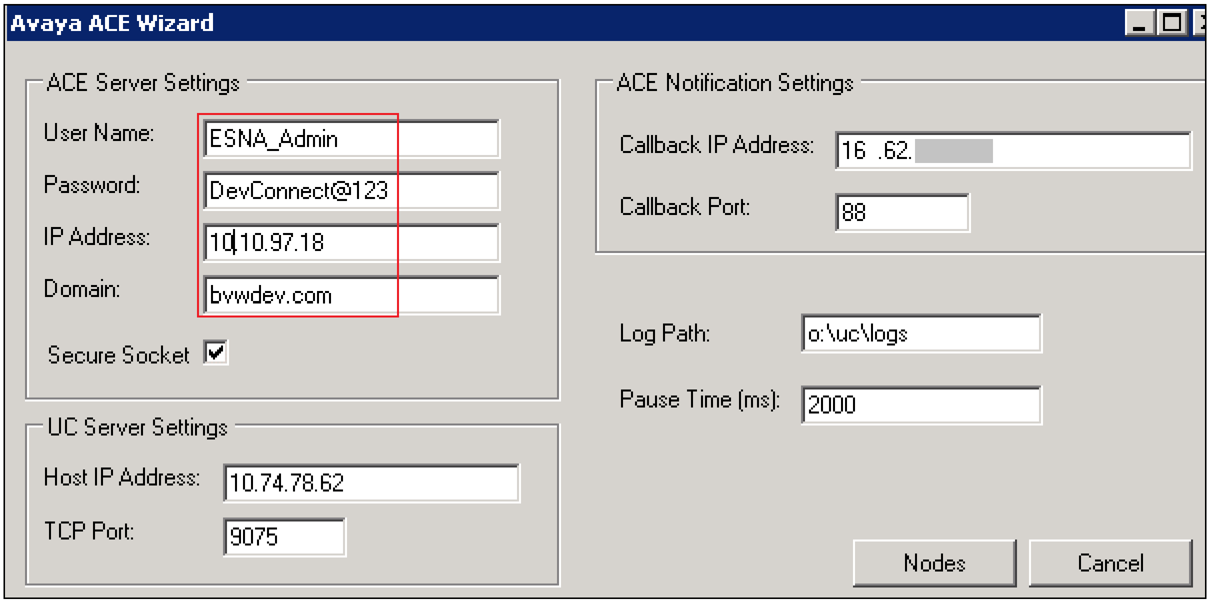
Outbound Proxy Port:

Buffer Size (kb): 4096

9.2. Configure UC ACE Wizard

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

- **User Name**: Enter user that created on Avaya ACE in **Section 8.2**
- **Password:** the password for the ACE user created in **Section 8.2**.
- **IP Address:** Avaya ACE IP address.
- **Domain:** Enter domain name used in the system, during compliance test bvwdev.com used.



User Name: ESNA_Admin

Password: DevConnect@123

IP Address: 1010.97.18

Domain: bvwdev.com

Secure Socket ☑

Host IP Address: 10.74.78.62

TCP Port: 9075

Callback IP Address: 16 .62.[redacted]

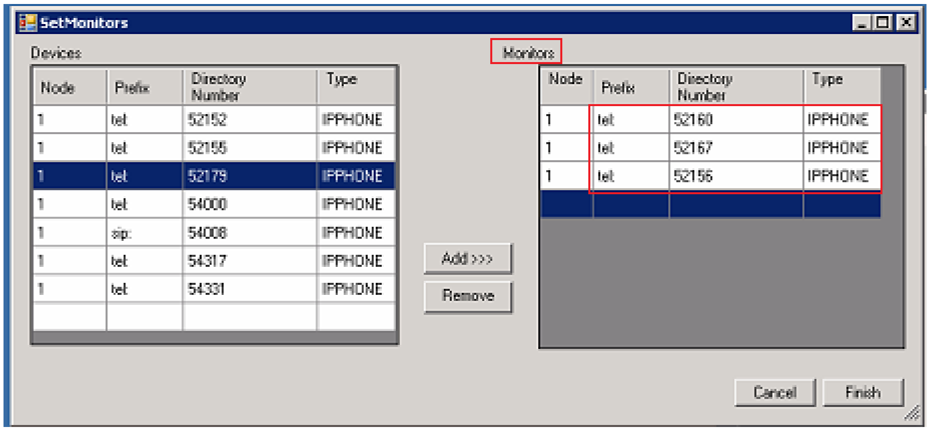
Callback Port: 88

Log Path: o:\uc\logs

Pause Time (ms): 2000

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

Select a device from the list of devices on the left side and add it to the right window to start to monitor it. Or a user can remove a device from the monitor list by selecting a device to highlight it and then clicking **Remove**.



Devices

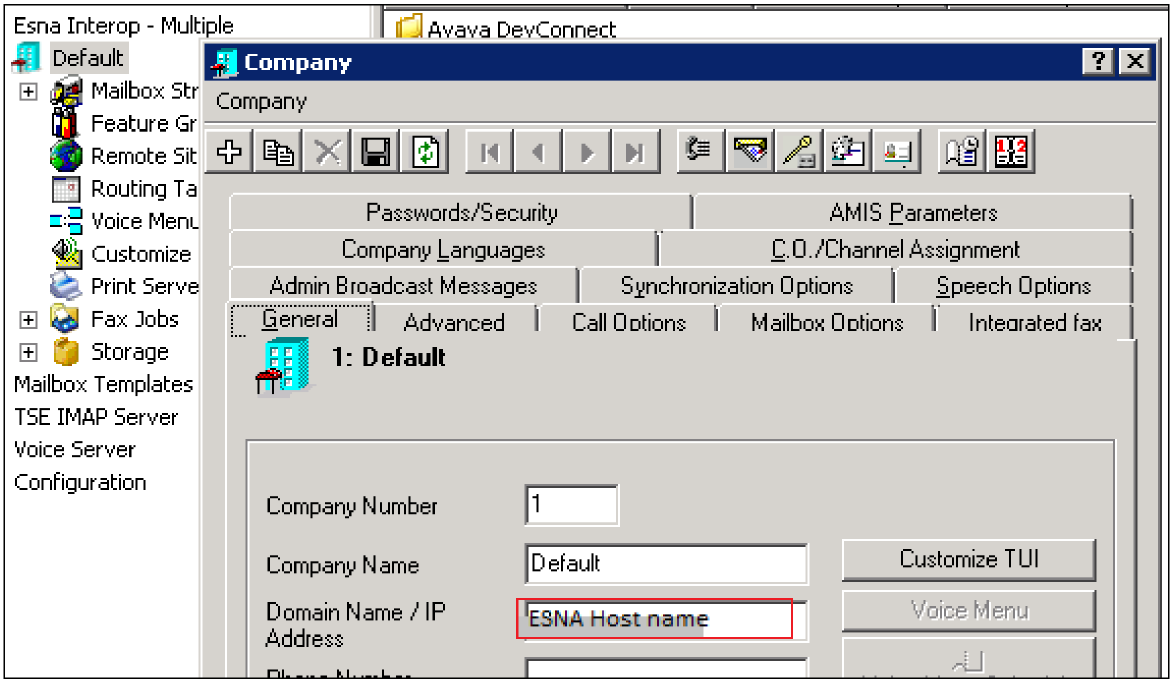
Node	Prefix	Directory Number	Type
1	tel:	52152	IPPHONE
1	tel:	52155	IPPHONE
1	tel:	52179	IPPHONE
1	tel:	54000	IPPHONE
1	sip:	54008	IPPHONE
1	tel:	54317	IPPHONE
1	tel:	54331	IPPHONE

Monitors

Node	Prefix	Directory Number	Type
1	tel:	52160	IPPHONE
1	tel:	52167	IPPHONE
1	tel:	52156	IPPHONE

9.3. Administer Company Profiles

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



Company Number: 1

Company Name: Default

Domain Name / IP Address: ESNA Host name

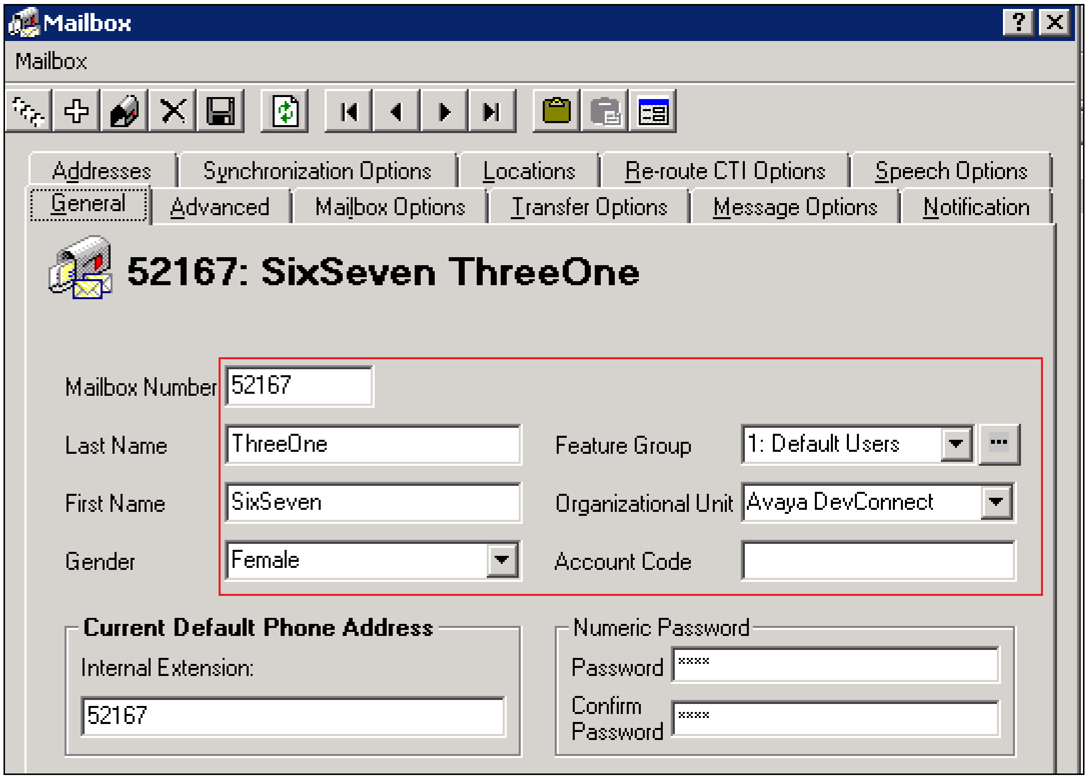
9.4. Configure User Mailbox in Officelinx Admin

Expand the **Officelinx → Esna Interop → Default → Mailbox Structure**. In the right panel, right click on the window, and select **new** to add new mailbox.

This section describes a sample configuration of mailbox 52167 for device 9608 H323 and this mailbox is linked to Google mail account managed by ESNA dev02@solution.com.

In **General** tab:

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



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

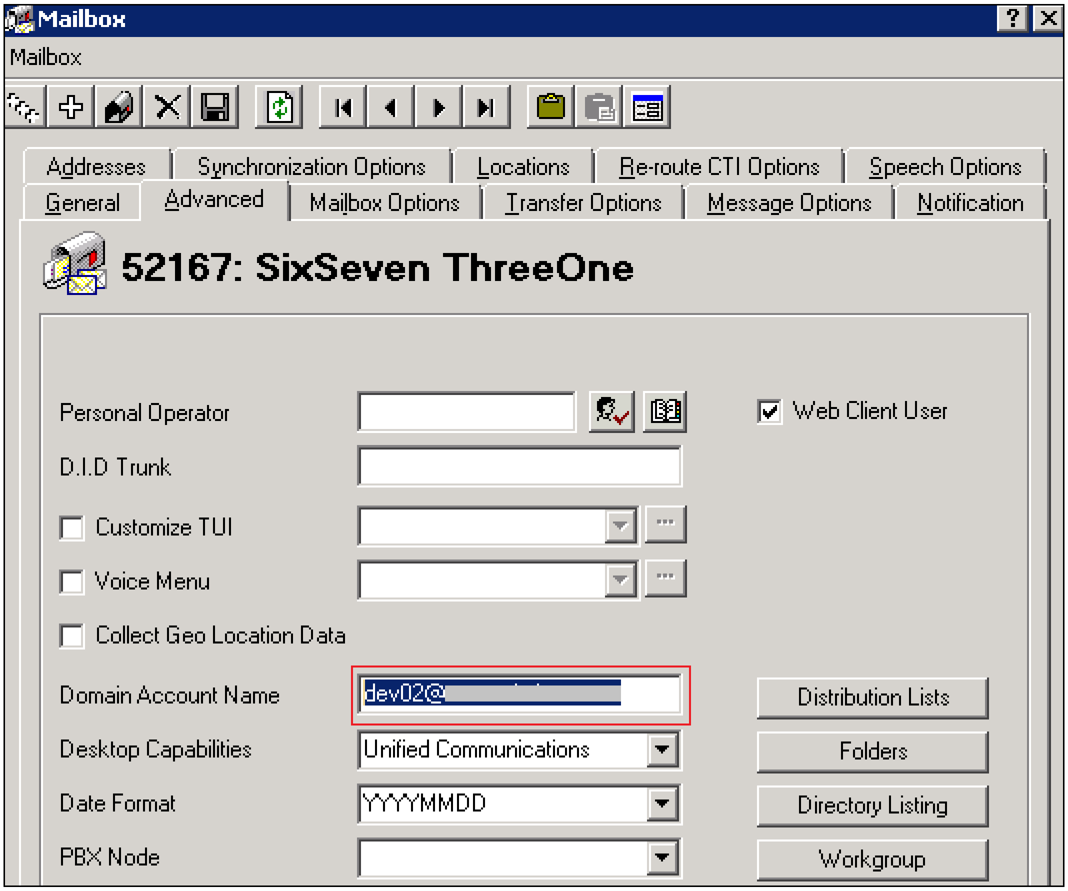
Numeric Password

Password: ****

Confirm Password: ****

In **Advanced** tab:

- **Domain Account Name**: enter the **Gmail account** which connects to this mailbox dev02@solution.com.
- **Desktop Capabilities**: select Unified Communications.



52167: SixSeven ThreeOne

Personal Operator

☑ Web Client User

D.I.D Trunk

☐ Customize TUI

☐ Voice Menu

☐ Collect Geo Location Data

Domain Account Name: dev02@[redacted]

Desktop Capabilities: Unified Communications

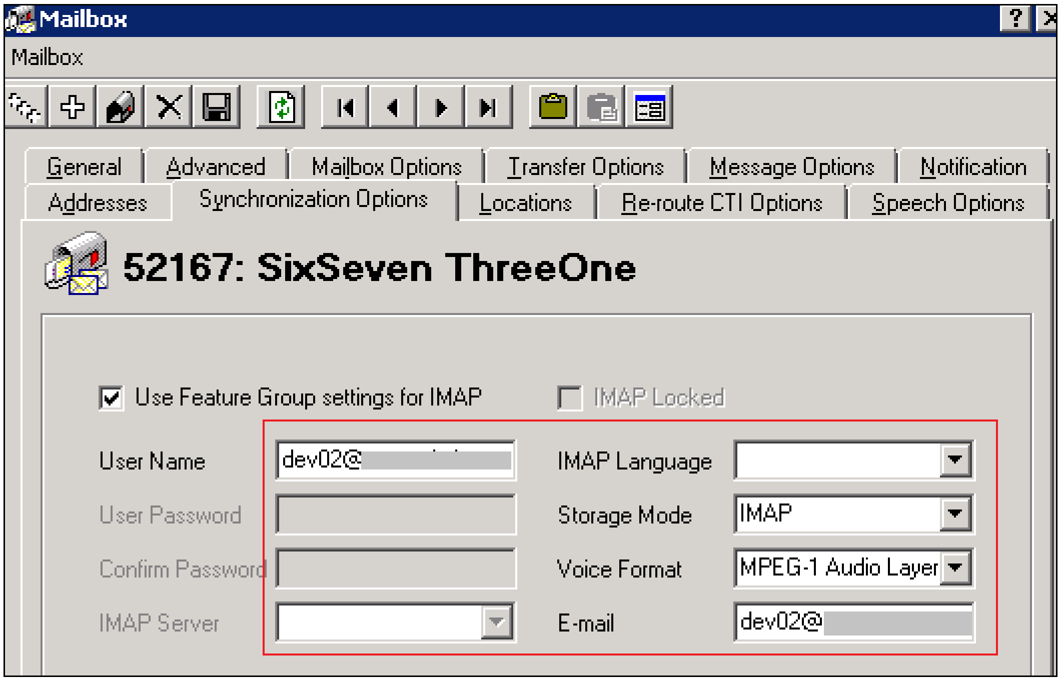
Date Format: YYYYMMDD

PBX Node

In **Synchronization Options** tab:

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

Click the **Save** icon to save the configuration.



52167: SixSeven ThreeOne

☑ Use Feature Group settings for IMAP

☐ IMAP Locked

User Name: dev02@[redacted]

User Password:

Confirm Password:

IMAP Server:

IMAP Language:

Storage Mode: IMAP

Voice Format: MPEG-1 Audio Layer

E-mail: dev02@[redacted]

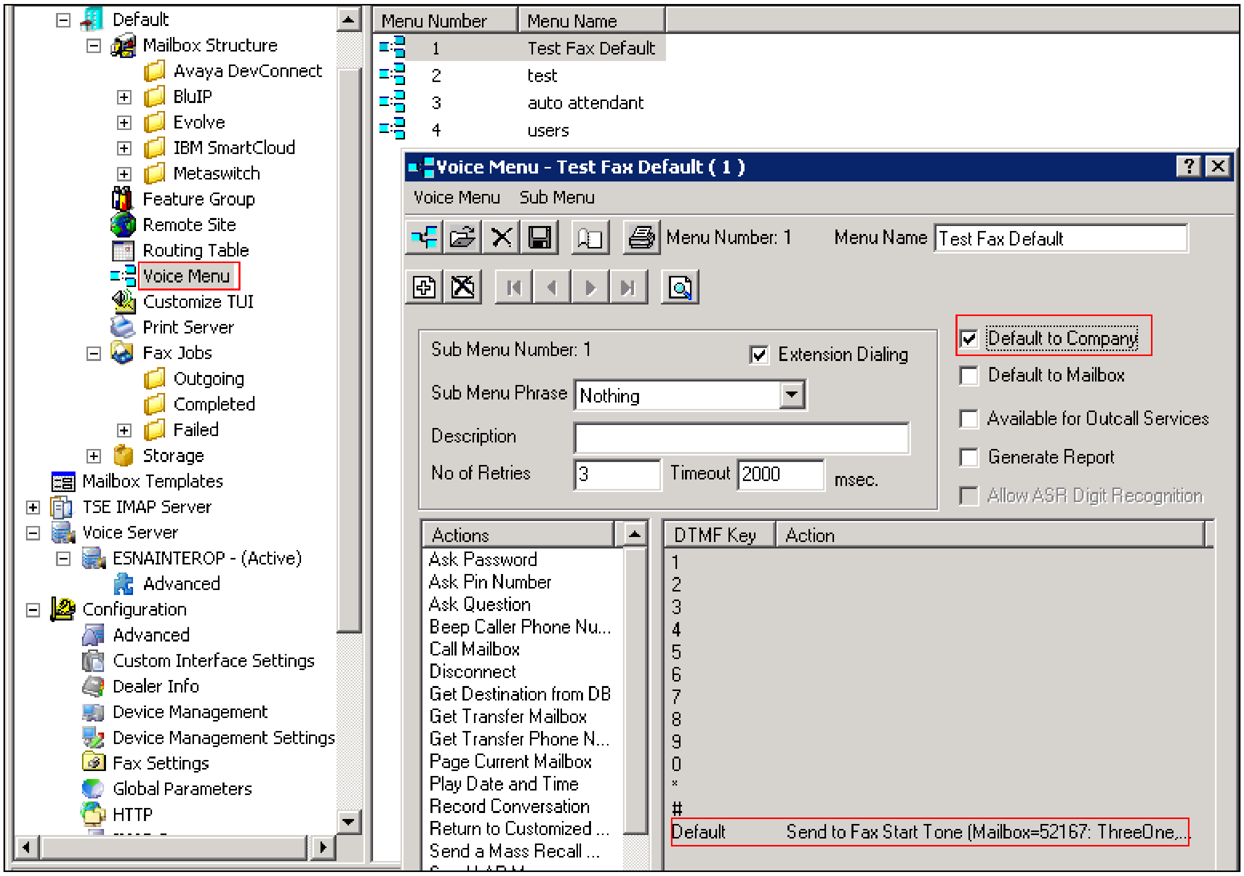
9.5. Configure Fax

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 References (**Section 12)** for details.

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 an iLink Pro user's mailbox.

As there are more than one method of setting up fax, and ultimately it will depend on the nature of the enterprise fax requirements for setup, fax setup 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 the **Default to Company** option is checked. Default: **Send to Fax Start Tone (Mailbox=52167…)** as shown in below figure:



Menu Number	Menu Name
1	Test Fax Default
2	test
3	auto attendant
4	users

Voice Menu - Test Fax Default (1)

Menu Number: 1 Menu Name: Test Fax Default

Sub Menu Number: 1 ☑ Extension Dialing

Sub Menu Phrase: Nothing

Description:

No of Retries: 3 Timeout: 2000 msec.

☑ Default to Company
☐ Default to Mailbox
☐ Available for Outcall Services
☐ Generate Report
☐ Allow ASR Digit Recognition

DTMF Key	Action
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
*	
#	
Default	Send to Fax Start Tone (Mailbox=52167: ThreeOne,...

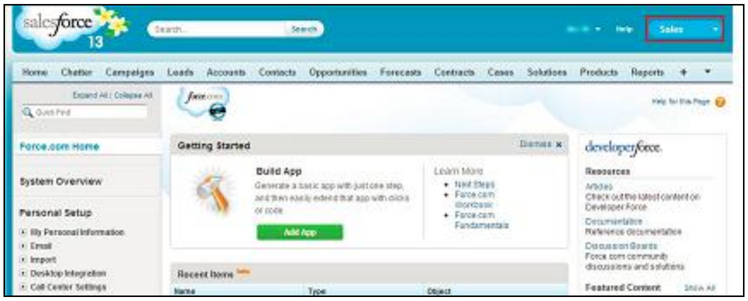
Note: This configuration was used because when a user sends the fax to Officelinx, there is no fax tone sent from Officelinx Server, and the fax on Communication Server 1000 is waiting. As a result, the fax gets no answer. It is necessary to check the "Default to Company" option with Default "Send to Fax start Tone" on Officelinx in order for Officelinx send fax tones to a fax machine.

9.6. Install and Configure iLink Pro on Salesforce

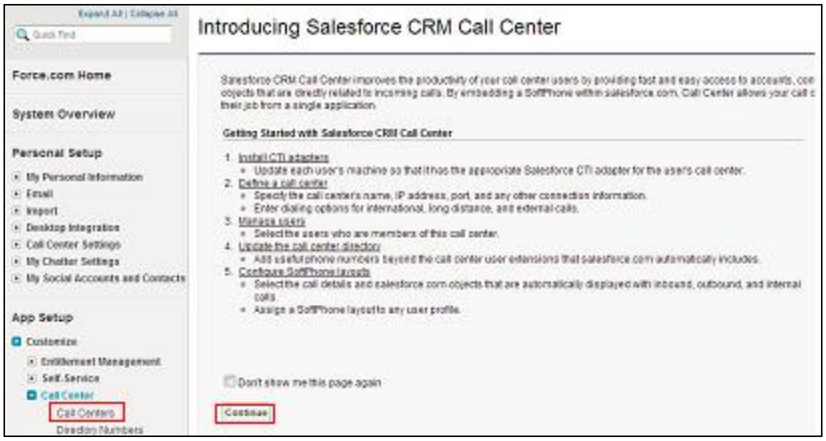
This section describe steps need to install and operate iLink Pro on Salesforce.

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 assume that all the proper and necessary configurations have been setup by ESNA technician. Login to Salesforce using an account with site administrator credentials. Go to the **Setup** page.



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



Introducing Salesforce CRM Call Center

Salesforce CRM Call Center improves the productivity of your call center users by providing fast and easy access to accounts, con objects that are directly related to incoming calls. By embedding a SoftPhone within salesforce.com, Call Center allows your call c their job from a single application.

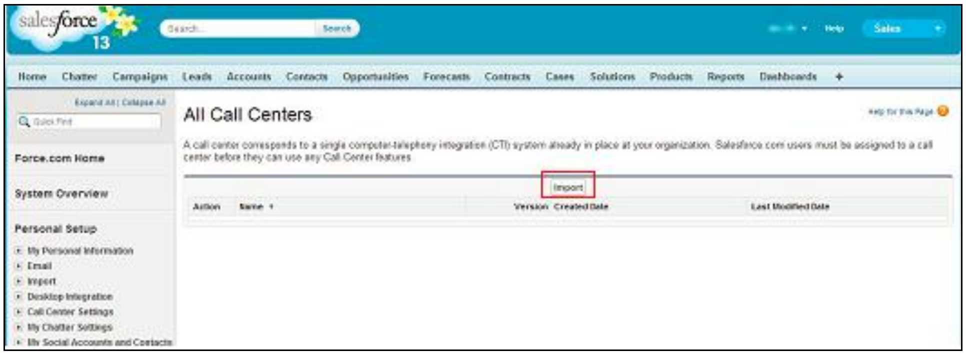
Getting Started with Salesforce CRM Call Center

1. Install CTI adapters
   - Update each user's machine so that it has the appropriate Salesforce CTI adapter for the user's call center.
2. Define a call center
   - Specify the call center's name, IP address, port, and any other connection information.
   - Enter dialing options for international, long distance, and external calls.
3. Manage users
   - Select the users who are members of this call center.
4. Update the call center directory
   - Add useful phone numbers beyond the call center user extensions that salesforce.com automatically includes.
5. Configure SoftPhone layouts
   - Select the call details and salesforce.com objects that are automatically displayed with inbound, outbound, and internal calls.
   - Assign a SoftPhone layout to any user profile.

□ Don't show me this page again

Continue

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



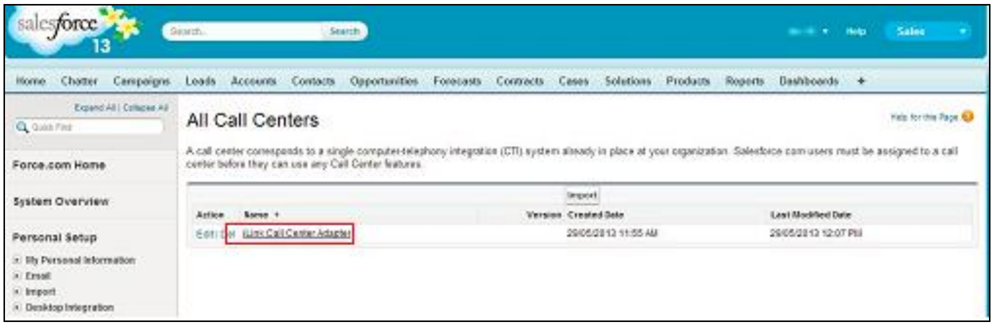
All Call Centers

A call center corresponds to a single computer-telephony integration (CTI) system already in place at your organization. Salesforce.com users must be assigned to a call center before they can use any Call Center features.

Import

Action	Name ↑	Version	Created Date	Last Modified Date

Click **Choose File**, and select the **Call Center Definition** file created in step 1. With that file selected, click **Import** (not shown). Returning to the **All Call Centers** window, choose the newly created **Call Center** and click **Edit**.

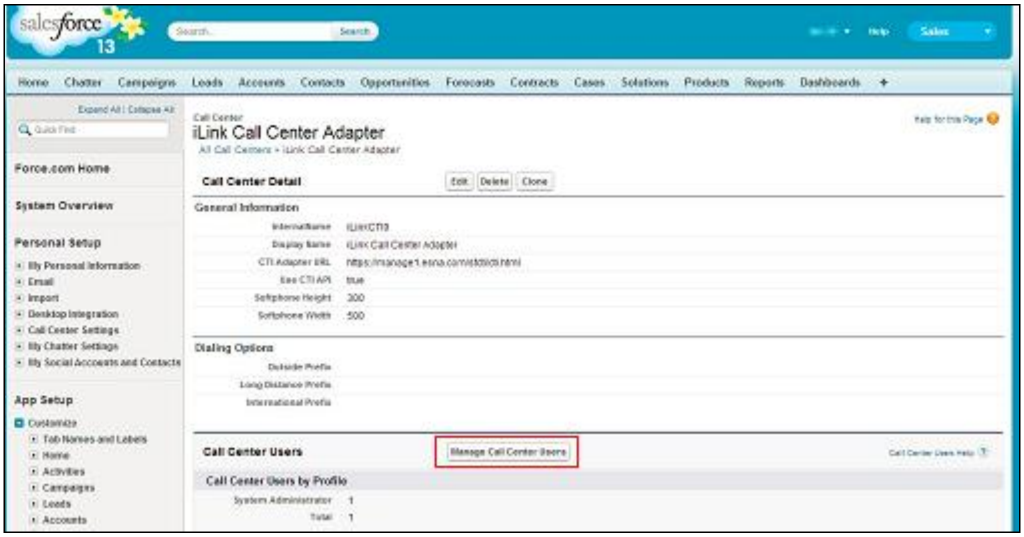


All Call Centers

A call center corresponds to a single computer-telephony integration (CTI) system already in place at your organization. Salesforce.com users must be assigned to a call center before they can use any Call Center features.

Action	Name ↑	Version	Created Date	Last Modified Date
Edit | Del	iLink Call Center Adapter		29/05/2013 11:55 AM	29/05/2013 12:07 PM

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



Call Center
iLink Call Center Adapter
All Call Centers » iLink Call Center Adapter

Call Center Detail

General Information

InternalName	iLinkCTI3
Display Name	iLink Call Center Adapter
CTI Adapter URL	https://manage1.esna.com/static/cti.html
Use CTI API	true
Softphone Height	300
Softphone Width	500

Dialing Options

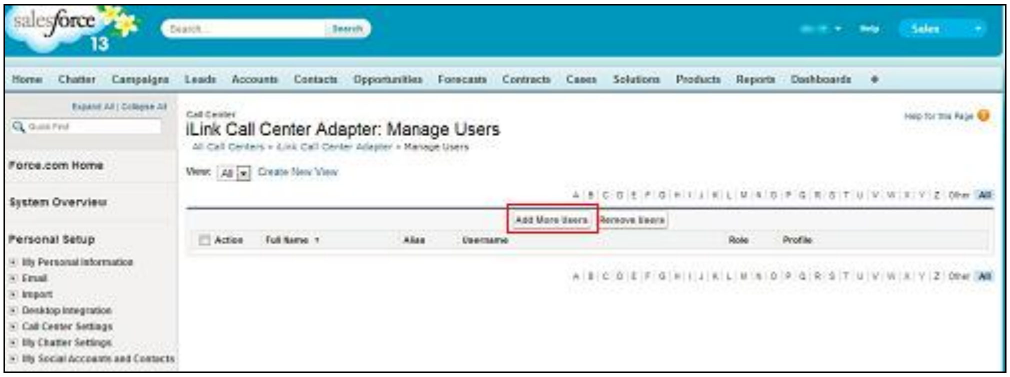
Outside Prefix	
Long Distance Prefix	
International Prefix	

Call Center Users

Call Center Users by Profile

System Administrator	1
Total	1

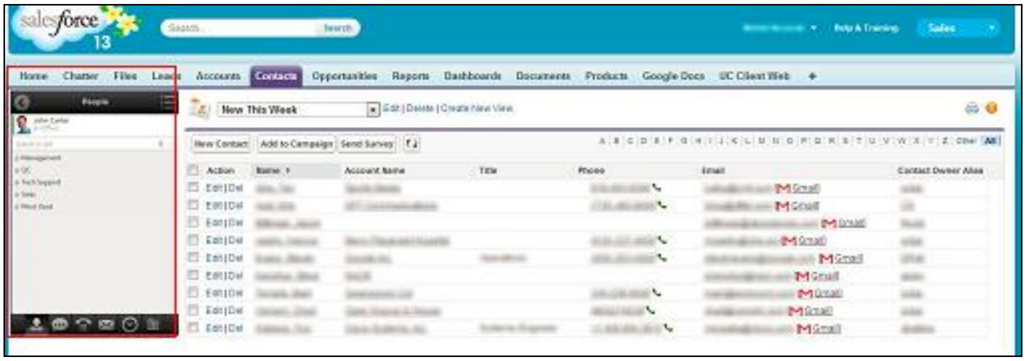
Click **Add More Users**. Add all of the required users to the list. Once all of the users have been added, click **Add to Call Center**.



Call Center
iLink Call Center Adapter: Manage Users
All Call Centers » iLink Call Center Adapter » Manage Users

□ Action	Full Name ↑	Alias	Username	Role	Profile

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.



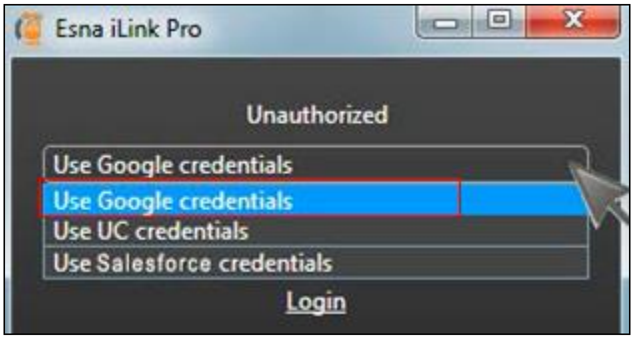
9.6.2. Call Center Definition

File The following file will be imported into Salesforce to setup the integration. 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:

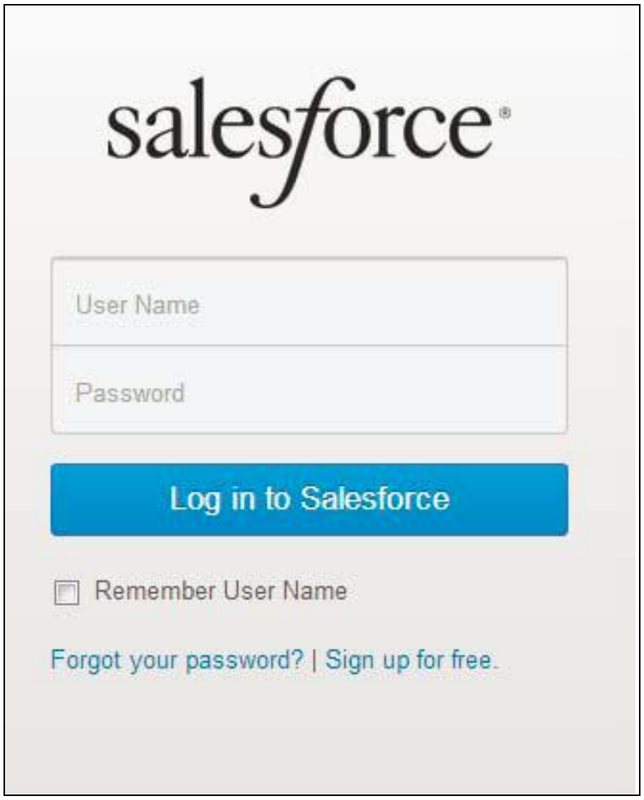
```
<callCenter> <section sortOrder="0" name="reqGeneralInfo" label="General Information">
<item sortOrder="0" name="reqInternalName" label="InternalName">iLinkCTI9</item> <item
sortOrder="1" name="reqDisplayName" label="Display Name">iLink Call Center
Adapter</item> <item sortOrder="2" name="reqAdapterUrl" 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 SFDC

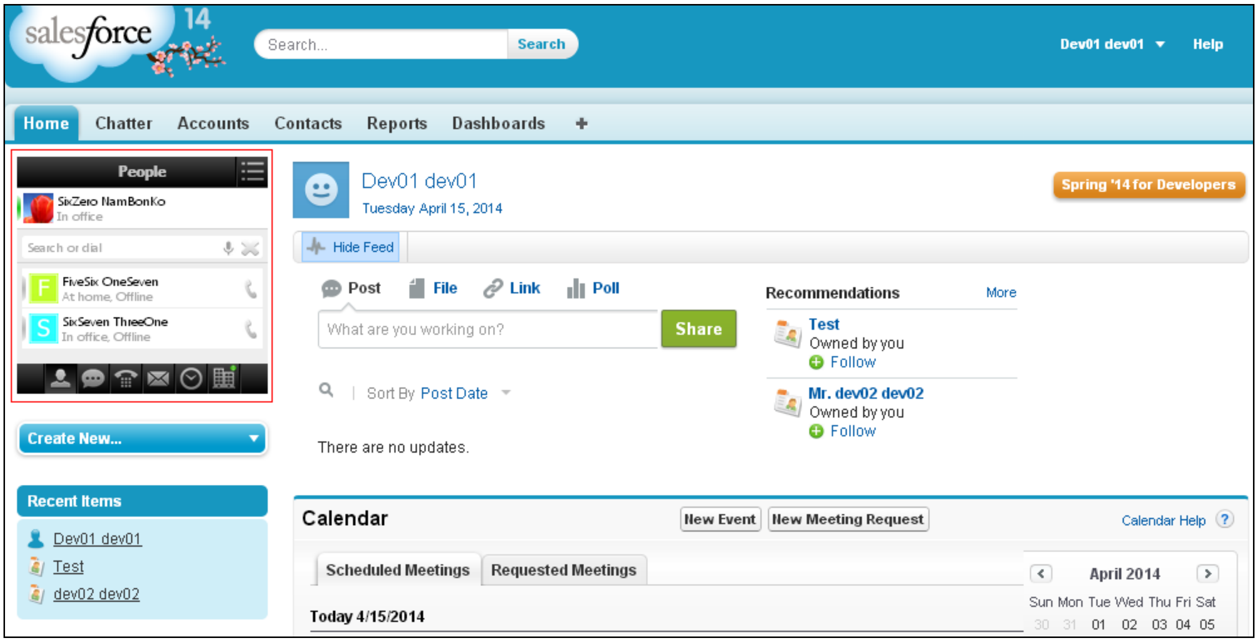
When launching iLink Pro from within Salesforce, the login screen provides a third option. The client can now select **Use Salesforce credentials** in addition to the Google and UC credentials.



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.



Below is the screenshot of user successfully login iLink Pro on Salesforce.



10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Server 1000, Session Manager, ACE, Messaging and ESNA Officelinx – iLink Pro application.

10.1. Verify Avaya Communication Server 1000 Release 7.6

After the telephone sets have been properly configured on Communication Server 1000, they should be in an "acquired" state which means that they are under control of the AML. This can be verified by using Overlay 20 on Communication Server 1000 to print the Terminal Number Block (TNB) for any phone as per the following example: Phone is in acquired state of the AML 36 setup in **Section 5.4.1**.

```
Ld 20
REQ: prt
TYPE: tnb
TN   96 0 1 3

DES  1150
TN   096 0 01 03  VIRTUAL
TYPE 1150
CDEN 8D
CTYP XDLC
CUST 0
CUR_ZONE 00001
AST  00
IAPG 0
AACS YES
ACQ  AS: AST-DN
ASID 36
SFNB  1  2  3  5  6  7  8  9  10  11  12  13  15  16  17  18  19  20  21  22  23
24  25  32  33  34  35  36  37  38  39
SFRB  32  33  34  35  36  37  38  39
USFB  1  2  3  4  5  6  7  8  9  10  11  12  13  14  15
CALB  0  1  2  3  4  5  6  7  8  9  10  11
FCTB
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY  00 SCR 54314 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME 1150E
            XPLN 13
            DISPLAY_FMT FIRST,LAST
     01
     02 CWT
     03
```

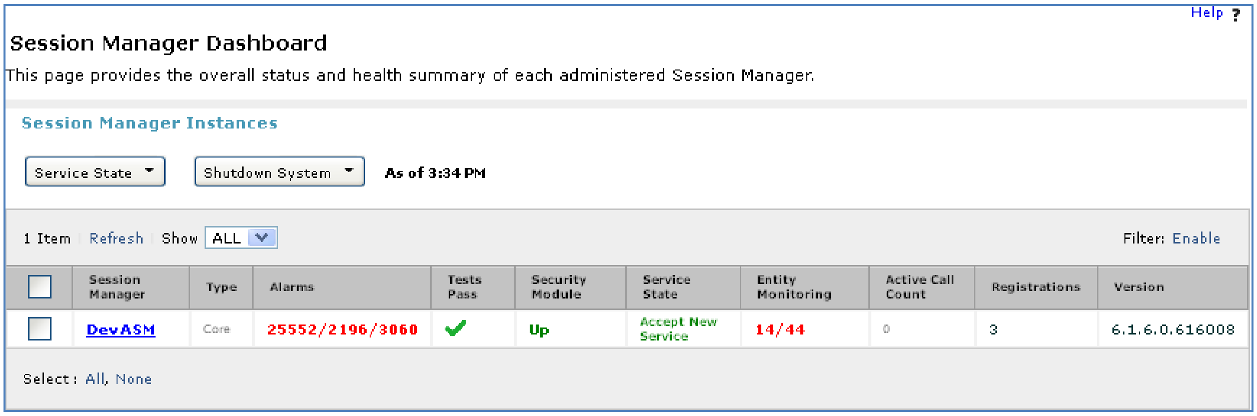
10.2. Verify Avaya Aura® Session Manager

10.2.1. Verify Avaya Aura® Session Manager is Operational

Navigate to **Elements → Session Manager → Dashboard** (not shown) to verify the overall system status for Session Manager.

Specifically, verify the status of the following fields as shown below:

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



Help ?

Session Manager Dashboard

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

Session Manager Instances

As of 3:34 PM

1 Item Refresh Show ALL ▾ Filter: Enable

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

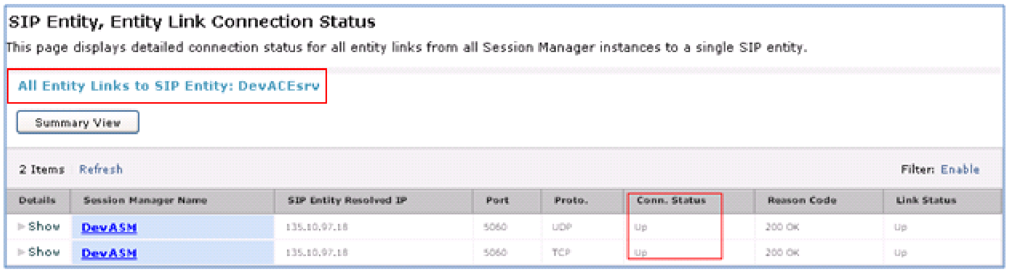
Select : All, None

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 ACE 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

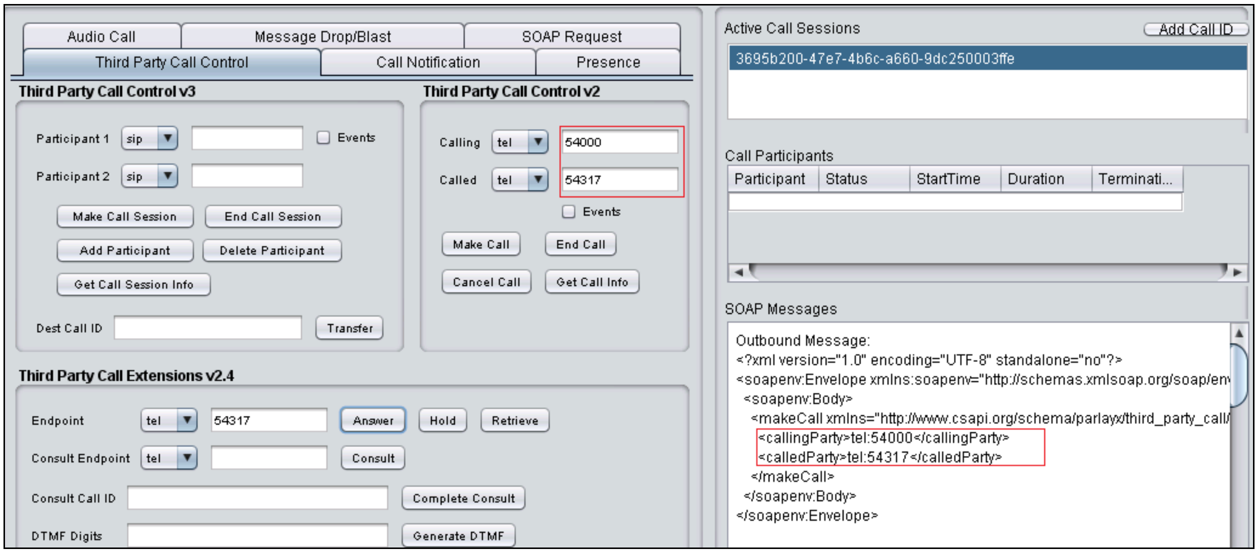
2 Items Refresh Filter: Enable

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

Repeat the same step to verify the status of Messaging, Communication Server and Officelinx are "Up".

10.3. Verify make call using ACE Web Service Trainer

Make a call using the ACE Web Service Trainer.Below is an example of using ACE Exhibitor: make a call from 54000 to 54317. Verify the call is made successfully.



Calling: tel 54000

Called: tel 54317

Endpoint: tel 54317

Active Call Sessions

3695b200-47e7-4b6c-a660-9dc250003ffe

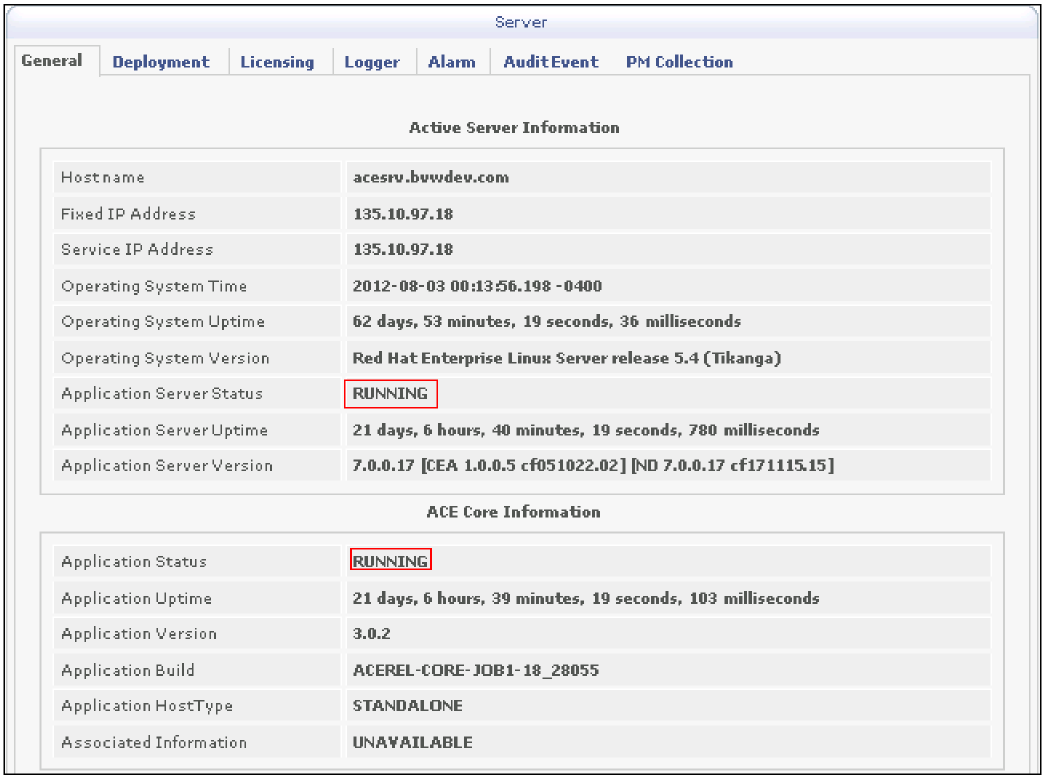
SOAP Messages

```
Outbound Message:
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/env
  <soapenv:Body>
    <makeCall xmlns="http://www.csapi.org/schema/parlayx/third_party_call/
      <callingParty>tel:54000</callingParty>
      <calledParty>tel:54317</calledParty>
    </makeCall>
  </soapenv:Body>
</soapenv:Envelope>
```

10.4. Verify Avaya Aura® Avaya ACE

10.4.1. Verify Avaya ACE Server status

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



Active Server Information

Hostname	acesrv.bvwdev.com
Fixed IP Address	135.10.97.18
Service IP Address	135.10.97.18
Operating System Time	2012-08-03 00:13:56.198 -0400
Operating System Uptime	62 days, 53 minutes, 19 seconds, 36 milliseconds
Operating System Version	Red Hat Enterprise Linux Server release 5.4 (Tikanga)
Application Server Status	RUNNING
Application Server Uptime	21 days, 6 hours, 40 minutes, 19 seconds, 780 milliseconds
Application Server Version	7.0.0.17 [CEA 1.0.0.5 cf051022.02] [ND 7.0.0.17 cf171115.15]

ACE Core Information

Application Status	RUNNING
Application Uptime	21 days, 6 hours, 39 minutes, 19 seconds, 103 milliseconds
Application Version	3.0.2
Application Build	ACEREL-CORE-JOB1-18_28055
Application HostType	STANDALONE
Associated Information	UNAVAILABLE

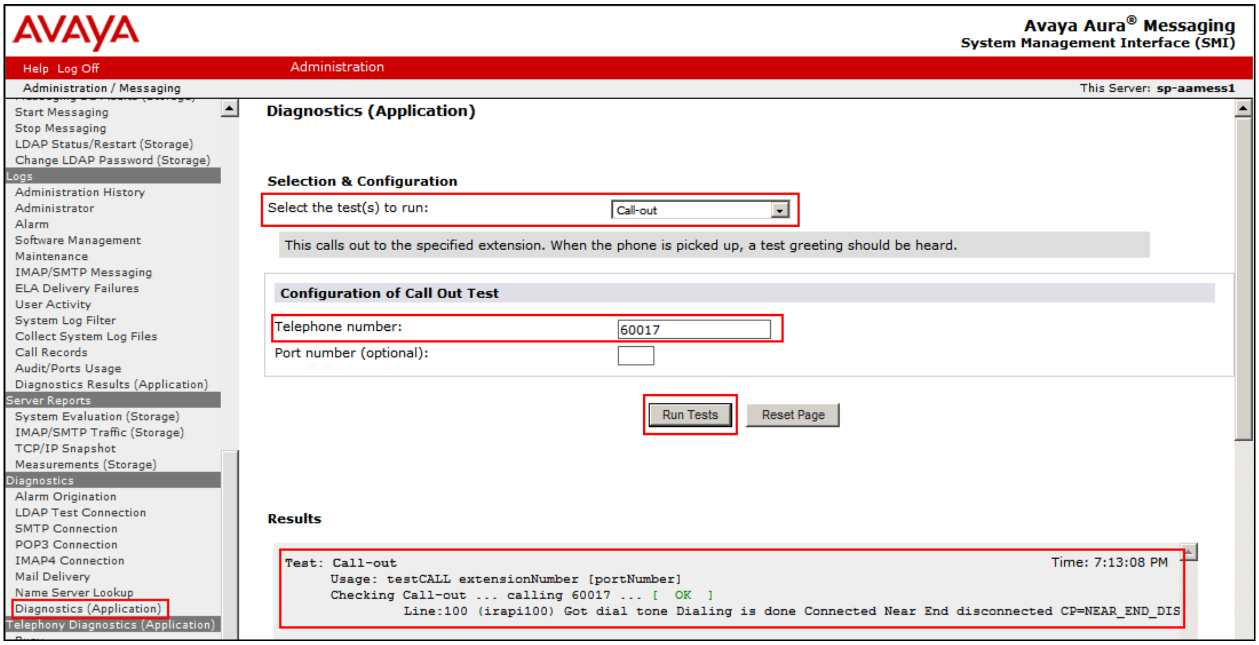
10.5. Verify Avaya Aura Messaging

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

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

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

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



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

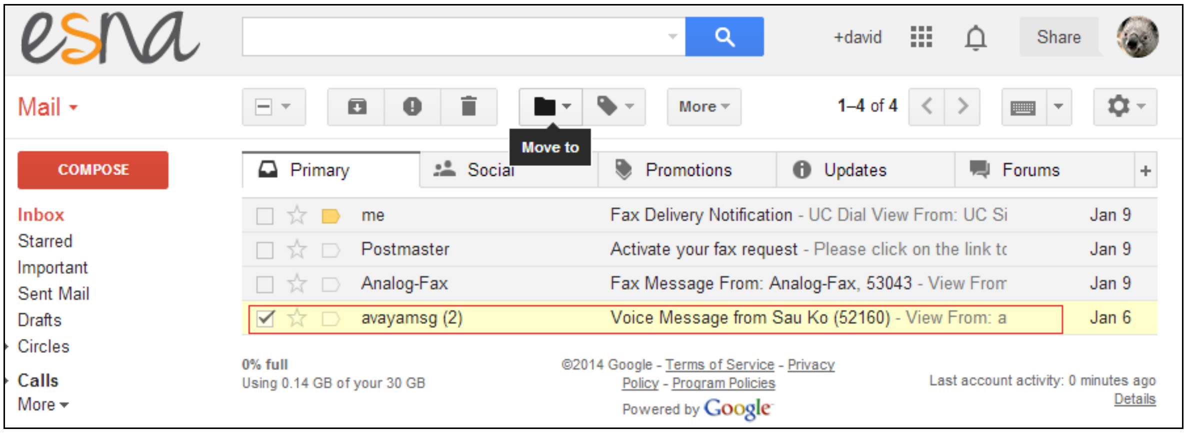
Port number (optional):

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
```

10.5.2. Verify user can receive and retrieve Avaya Aura Messaging voice message using Google Mail

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



□ ☆	me	Fax Delivery Notification - UC Dial View From: UC Si	Jan 9
□ ☆	Postmaster	Activate your fax request - Please click on the link tc	Jan 9
□ ☆	Analog-Fax	Fax Message From: Analog-Fax, 53043 - View Frorr	Jan 9
☑ ☆	avayamsg (2)	Voice Message from Sau Ko (52160) - View From: a	Jan 6

0% full
Using 0.14 GB of your 30 GB

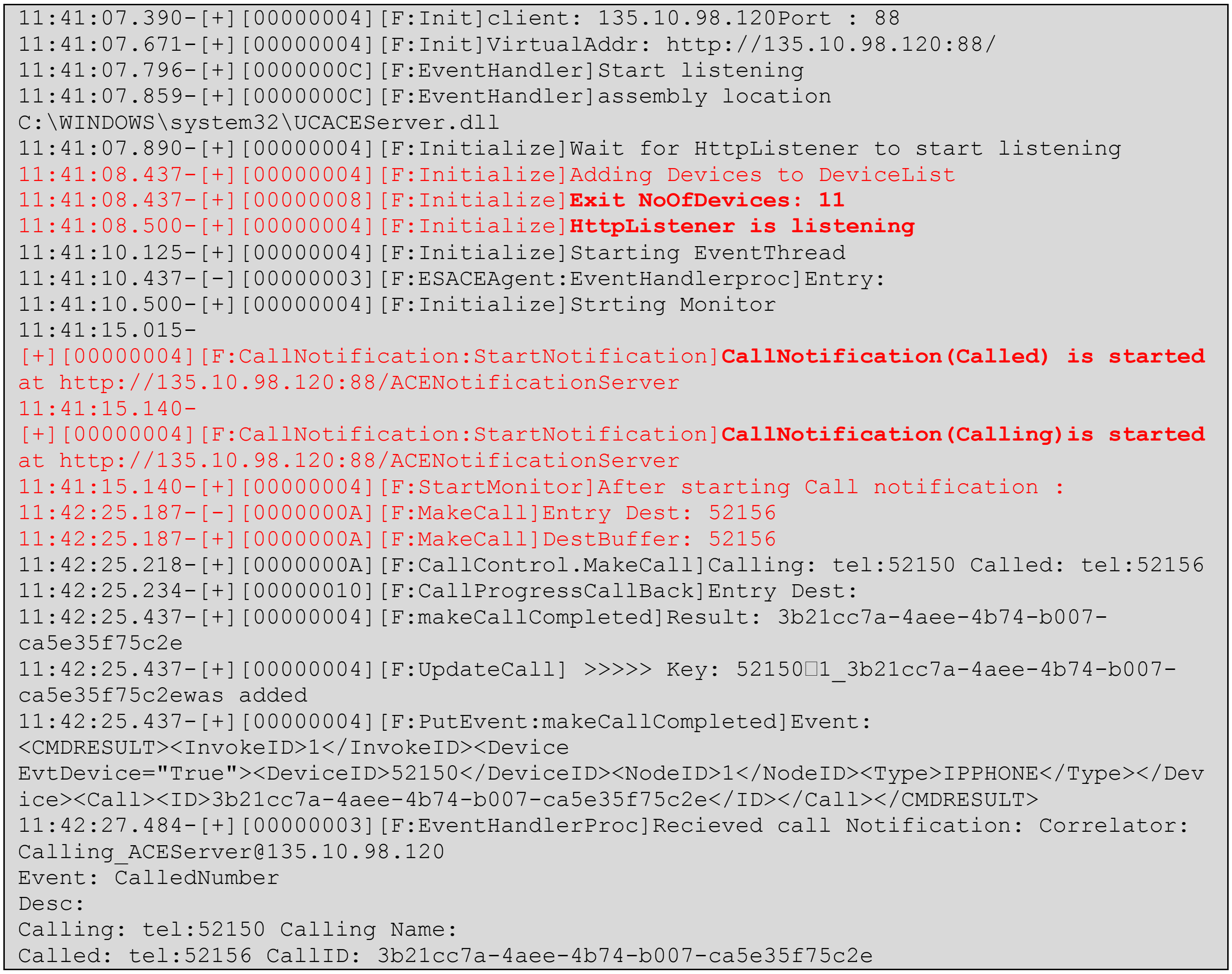
©2014 Google - Terms of Service - Privacy Policy - Program Policies
Powered by Google

Last account activity: 0 minutes ago
Details

10.6. Verify ESNA Officelinx server and iLink Pro

10.6.1. Verify the log file UCServer of ESNA Officelinx.

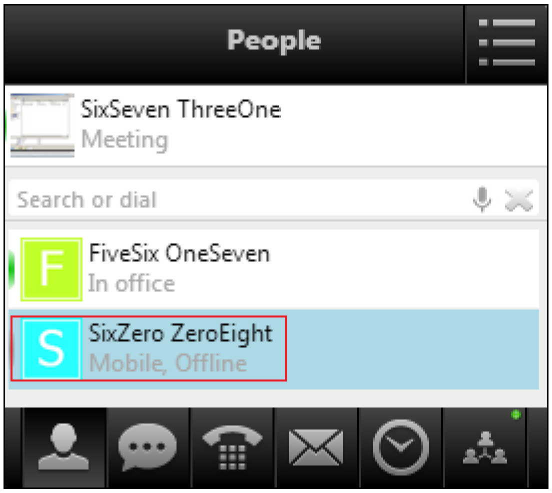
Log on to Officelinx, and open the log file UCServerYYYYMMDD.log in C:\UC\Logs\VServer. The log screenshot below shows that Officelinx successfully monitored devices on CS1K as well as call information.



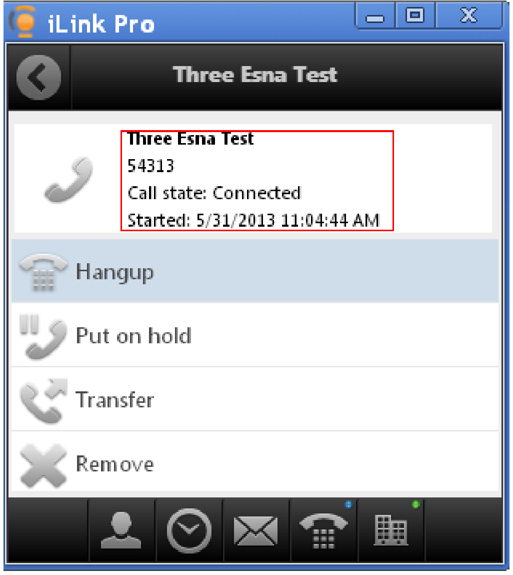
```
11:41:07.390-[+][00000004][F:Init]client: 135.10.98.120Port : 88
11:41:07.671-[+][00000004][F:Init]VirtualAddr: http://135.10.98.120:88/
11:41:07.796-[+][0000000C][F:EventHandler]Start listening
11:41:07.859-[+][0000000C][F:EventHandler]assembly location
C:\WINDOWS\system32\UCACEServer.dll
11:41:07.890-[+][00000004][F:Initialize]Wait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

10.6.2.Verify User can make a call using iLink Pro

Have a user log in to the ESNA Gmail account as created in **Section 9.3**. Verify the user is able to click and call another user on the list. Verify the called party is ringing,The called party can pick up the device, anda 2-way voice path is established.



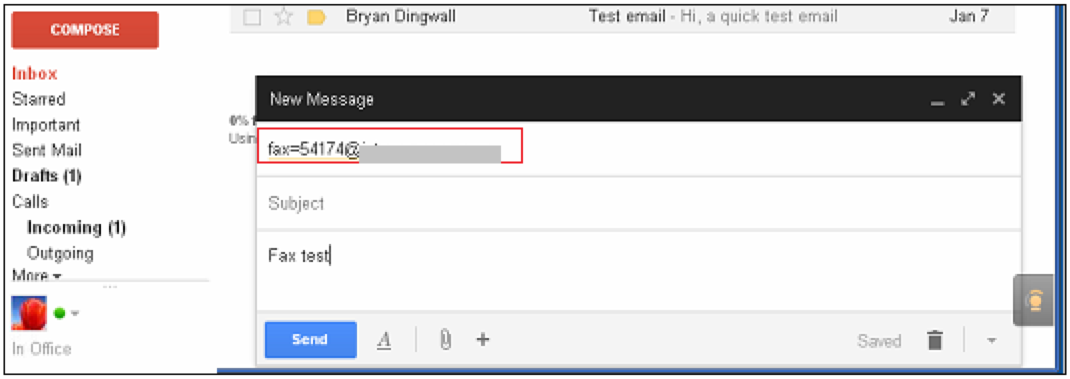
Below is screenshot of the active call along with call information.



Three Esna Test
54313
Call state: Connected
Started: 5/31/2013 11:04:44 AM

10.6.3. Verify user can send fax through email

In the Google mail, click **Compose** to start a new message. In the **To**: field, enter a full fax address. For example, during the compliance test, fax=54174@ESNHostname is used. Enter subject and fax content, and click **Send**.



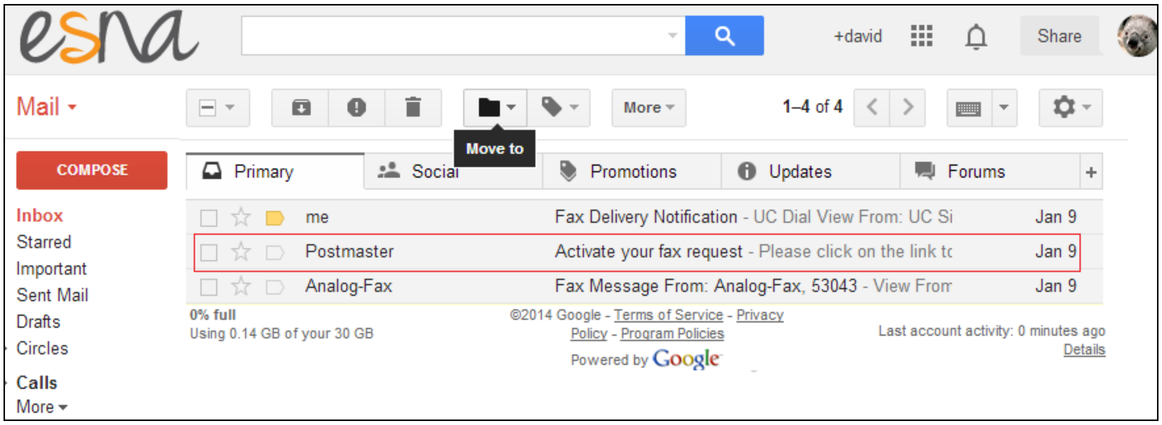
Bryan Dingwall	Test email - Hi, a quick test email	Jan 7

fax=54174@[redacted]

Subject

Fax test

Verify that the user will received an email from **Postmaster** to ask the user to activate their fax request (shown below). Click on the provided link to confirm (not shown). Verify that fax machine is able to receive and print out the fax content.



me	Fax Delivery Notification - UC Dial View From: UC Si	Jan 9
Postmaster	Activate your fax request - Please click on the link tc	Jan 9
Analog-Fax	Fax Message From: Analog-Fax, 53043 - View Frorr	Jan 9

0% full
Using 0.14 GB of your 30 GB

©2014 Google - Terms of Service - Privacy Policy - Program Policies
Powered by Google

Last account activity: 0 minutes ago
Details

11. Conclusion

Interoperability testing of Avaya Aura® Agile Communication Environment, Avaya Aura® Messaging, and Avaya Communication Server 1000 Release 7.6 with Officelinx 9.1 – 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. *SIP Line Fundamentals Avaya Communication Server 1000* (NN43001-508).
2. *Element Manager System Reference - Administration Avaya Communication Server 1000* November 2013 NN43001-632 Issue 06.03
3. *Administering Avaya Aura® Session Manager*, June 2013, Release 6.3
4. *Administering Avaya Aura® System Manager*, May 2013, Release 6.3.
5. *Avaya Agile Communication Environment™ Service Provider Administration* NN10850-005,
6. For an alternate procedure to configure a signing authority as trusted on Avaya ACE, see *"Trusting a CA or self-signed certificate" in Avaya Agile Communication Environment™ User and Security Administration* (NN10850–010).

The following document was provided by ESNA:

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.