Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the ESNA Office-LinX™ Cloudlink™ Edition UC Client Manager Google Gadget with Avaya Agile Communication Environment™, Avaya Aura® Messaging and Avaya Communication Server 1000E Release 7.5 - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the ESNA Office-LinX™ Cloudlink™ Edition UC Client Manager to interoperate with Avaya Agile Communication Environment™, Avaya Aura® Messaging and Avaya Communication Server 1000 Release 7.5.

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

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

Table of Contents

1. Introduction

These Application Notes describe the procedure for configuring ESNA Telephony Office-LinX, Avaya Agile Communication Environment™, Avaya Aura® Communication Server 1000E Release 7.5 and Avaya Aura® Messaging solutions.

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

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

2. General Test Approach and Test Result

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

2.1. Interoperability Compliance Testing

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

2.2. Test Results

The following testing was covered successfully:

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

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

The following was observed during testing:

- ESNA UC Client lost call control at times when it receives an unexpected OnDisconnect. When a user attempts a transfer the call is put on hold but the transfer does not complete. These issues are being investigated by the ACE team.
- The following is only happening on CS1K: On the screen of the transferred UC Client, user receives 2 incoming call displays; 1 incoming call from transferring extension and 1 incoming call from originator extension. This is the design intent of Avaya ACE for CS1K.
- The following issues are under investigation by ESNA:
  - UC Client loses call control while a call is put on Hold in the following scenario: A calls B, A places the call on hold, B transfers the call to C; both A and C lose call control and A still has the call on hold. A can resume the call by using the physical phone.
  - ESNA UC Server fails to start Call Notification if a phone that is unavailable or unreachable exists in the UC ACE Wizard list. A workaround is to go into UC ACE wizard, remove the phone that is unavailable, and restart the service. Then the server is able to start Call Notification for each of the phones in the list.
  - The caller ID does not update on a transferred UC Client, it still shows the originator extension. A calls B, caller ID of A shows B and vice versa, A transfers call to C. C answers and is talking to B, but the caller ID on B still shows A instead of C, while C correctly shows B's caller ID.
- Cancel Call and Call Forward are not available in this version of Office-LinX.

2.3. Support

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

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

3. Reference Configuration

Figure 1 illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with a Session Manager and an Avaya Communication Server 1000E Release 7.5. Endpoints include Avaya 1110, 1165 Series IP Telephones.

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

A user is able to click and call through the UC Client Manager app as well as receive notify messages from Avaya Aura® Messaging on their ESNA Google mailbox.

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

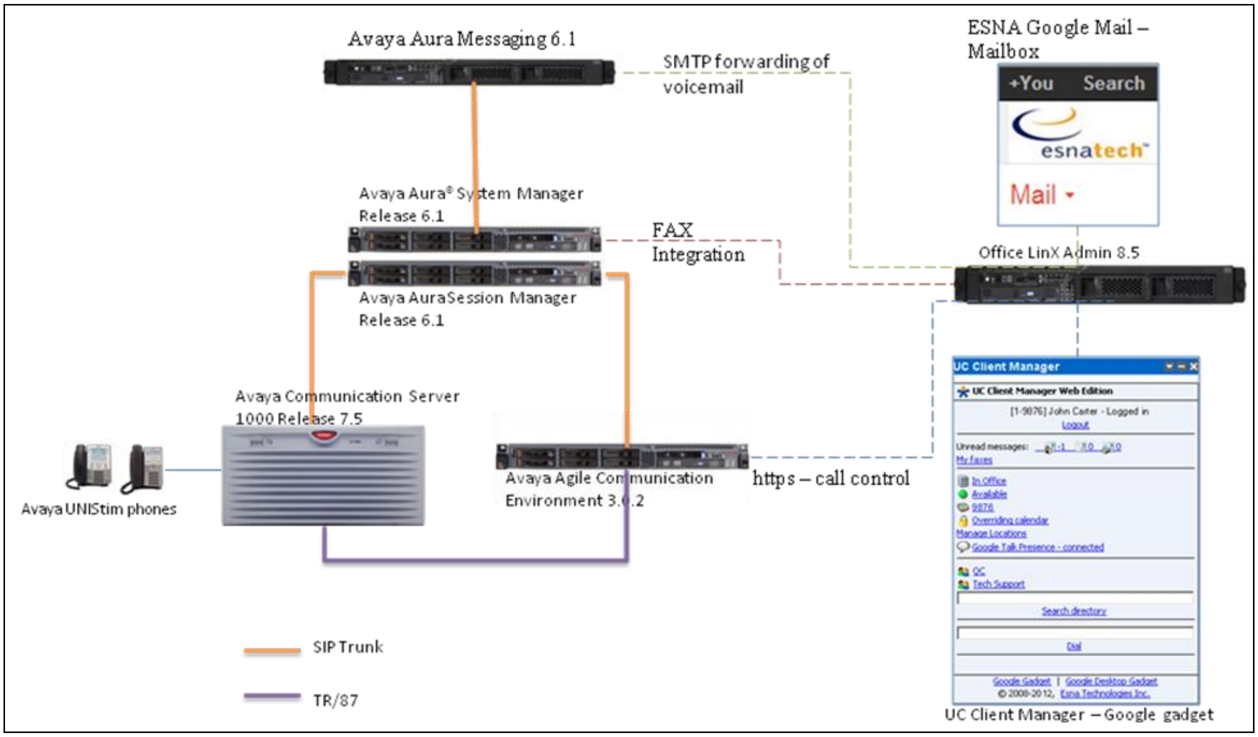

Avaya Aura Messaging 6.1
SMTP forwarding of voicemail
ESNA Google Mail – Mailbox
+You Search
esnatech™
Mail ▾
Avaya Aura® System Manager Release 6.1
FAX Integration
Office LinX Admin 8.5
Avaya AuraSession Manager Release 6.1
Avaya Communication Server 1000 Release 7.5
Avaya UNIStim phones
Avaya Agile Communication Environment 3.0.2
https – call control
UC Client Manager
UC Client Manager Web Edition
[1-9876] John Carter - Logged in
Logout
Unread messages: 1 0 0
My faxes
In Office
Available
9876
Overriding calendar
Manage Locations
Google Talk Presence - connected
QC
Tech Support
Search directory
Dial
Google Gadget | Google Desktop Gadget
© 2008-2012, Esna Technologies Inc.
UC Client Manager – Google gadget
SIP Trunk
TR/87

Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya Communication Server 1000E	Call Server (CPPM Linux): 7.50Q+ DepList 1: Core Issue: 01 2012-07-16 Signaling Server (CPPM): 7.50.17.00
Avaya Aura® System Manager	Release 6.1
Avaya Aura® Session Manager	Release 6.1
Avaya Aura® Messaging	Release 6.1
Avaya Agile Communication Environment	Avaya Agile Communication Environment 3.0.2
Avaya UNIStim Telephones: 1165 1110	0623C8J
ESNA Telephony Office-LinX	8.5 SP2
UC Client Manager	8.5 SP2

5. Configure Avaya Communication Server 1000E R7.5

This section describes the procedure for setting up Communication Server 1000E. The steps include setting up and verifying the system capabilities:

- Verify the Communication Server 1000E Packages
- Verify that sufficient license parameters and system limits
- Verify that there are sufficient virtual trunks (SIP Access Ports)
- SIP Solutions
- Verify the number of configured SIP access ports
- Add Avaya ACE server as SIP Entity on Session Manager
- Add a CS 1000 service provider on Avaya ACE
- 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)
- Provision a CS 100 TR/87 service provider on Avaya ACE
- Enable ELAN
- 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 1000E configurations are performed through Unified Communications Manager (UCM), Element Manager (EM) and Command Line Interface (CLI) via a telnet session to the Call Server.

5.1. Verify the Communication Server 1000E Packages

Verify that the appropriate packages have been installed.

- Package 406 (SIP)
- Package 408 (Multimedia Systems Convergence)

Obtain feature package information using Element Manager.

1. Log in to the UCM.
2. Click the **CS1000 Element Manager**.
3. Navigate to **Tools → Logs and reports → Equipped feature packages**
4. Verify that the following patches have been added.

5.2. Verify that sufficient license parameters and system limits

When deploying an Avaya ACE solution, ensure that the Communication Server 1000E Release 7.5 system has sufficient license parameters to support not only the Communication Server 1000E Release 7.5 system and Communication Server 1000E Release 7.5 system users but also any ACE applications to be deployed within the existing customer network.
• Associated Set (AST) licenses are required for any terminal number (TN) that sends Application Module Link (AML) events to a client application, for example:
- Meridian Link CTI applications such as Call Recording or Screen Pop/Desktop Computer Telephony Integration (CTI).
- Some aspects of the Contact Center 6.0 suite of applications.
- Converged Office.
- ACE services that require CTI/TR/87 operations, for example, send remote call control (RCC) messages and the ability to monitor a directory number (DN) for Presence and call states.
• Virtual Trunks (SIP or H.323 IP Peer access ports) are required for any calls between CS 1000 peer systems.
- SIP IP Peer access ports are required for SIP virtual trunking.
- H.323 IP Peer access is used for H.323 virtual trunking.

1. Log in to the UCM.
2. Click **CS1000 Element Manager**.
3. Navigate to **Tools → Logs and reports → System License Parameters**
4. 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.

5.3. Verify that there are sufficient virtual trunks (SIP Access Ports)

1. Log in to the UCM.

2. Click **Element Manager**.
3. Click **Routes and Trunks**.
4. On the Routes and Trunks page, expand the required **customer number**.
5. From the resulting drop down list, expand the required **route number**.
6. Ensure that the system has sufficient number of trunks configured.

Note:
To configure virtual trunks, see *SIP Line Fundamentals Avaya Communication Server 1000E* (NN43001-508).

5.4. SIP Solutions

5.4.1. Verify the number of configured SIP access ports

Ensure there are sufficient SIP Access ports beyond the existing customer requirements.

1. Log in to the UCM.
2. Click **Element Manager**.
3. Click **Routes and Trunks**.
4. On the Routes and Trunks page, expand the required **customer number**.
5. From the resulting drop down list, expand the required **route number**.
6. Ensure that the system has sufficient number of trunks configured.

5.4.2. Add Avaya ACE server as SIP Entity on Session Manager

See **Section 7.3** for detail steps how to add a SIP entity on Session Manager.

5.4.3. Add a Communication Server 1000E service provider on Avaya ACE

See **Section 8.1.1** for detail step how to add Communication Server 1000E on Avaya ACE.

5.5. TR/87 solutions

5.5.1. Adding an AML

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

About this task
The Ethernet AML is the main interface that supports call control requests from SIP CTI Clients and the Communication Server 1000E Release 7.5 system. Use this procedure to check if the Communication Server 1000E system is already set up for CTI services.

Procedure

1. Log in to the UCM.
2. Click **CS1000 Element Manager**.
3. On the left hand tree view, click **Interfaces → Application Module Link**.
4. 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 Communication Server 1000E system, the link number should be between 32 through 47 (inclusive) and for a large Communication Server 1000E system, the link number should be between 32 through 127 (inclusive).

5. If there is no port number assigned to CTI, click **Add**.
6. In the **Port number** field, enter a number 32 or higher. E.g. 36 is used during testing
7. In the **Description** field, enter a suitable description for the AML, for example, CTI.
8. Select the **Link control system parameters** check box to enable the Maximum octets list.
9. From the **Maximum octets** list, select the maximum number of octets for each High level Data Link Control (HDLC) frame. (The default is 512).
10. Click **Save**.

5.5.2. Adding VAS

One Value Added Server (VAS) must be defined for each configured AML.

About this task

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

5.5.3. Node IP (SIP Gateway) Configuration

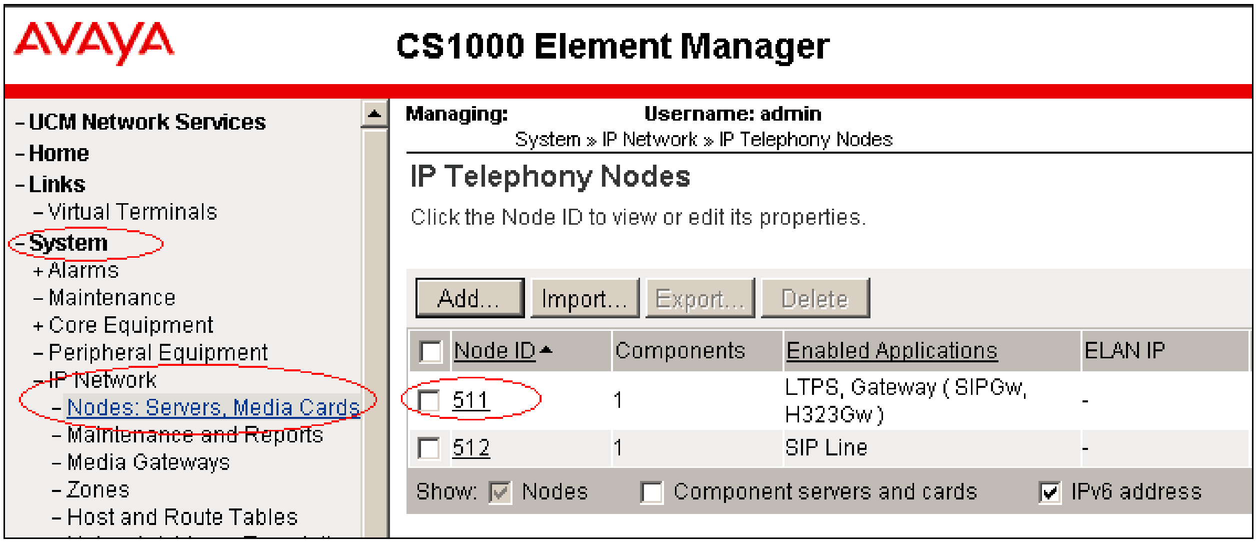
This section only describes the configuration of the SIP Gateway application running on the Communication Server 1000E signaling server. In the solution test, Node ID **511** is configured, that has the SIP Gateway application enabled on it. For additional information on Nodes configuration refer to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

Ensure that user able to:

- Access to UCM.

- CS 1000 element manager configured.
- SIP CTI services enabled and configured.

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.

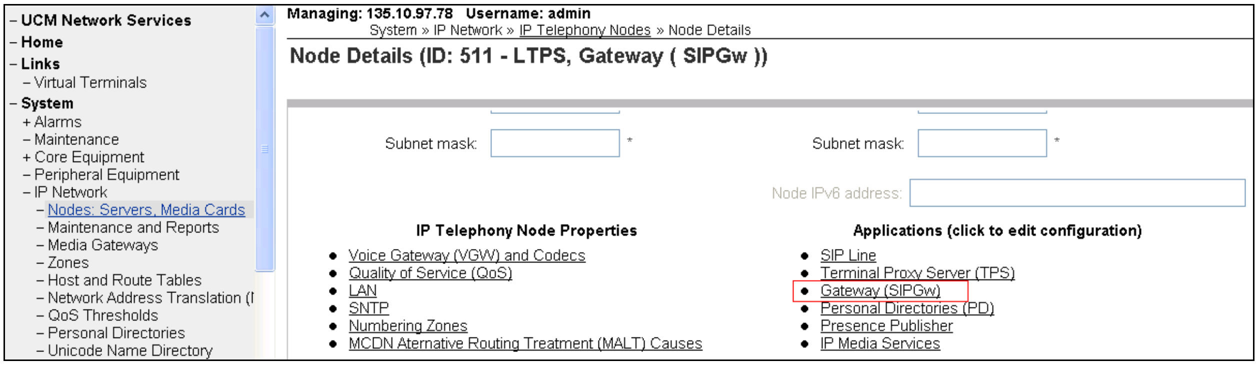


IP Telephony Nodes

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	-

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



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

IP Telephony Node Properties

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

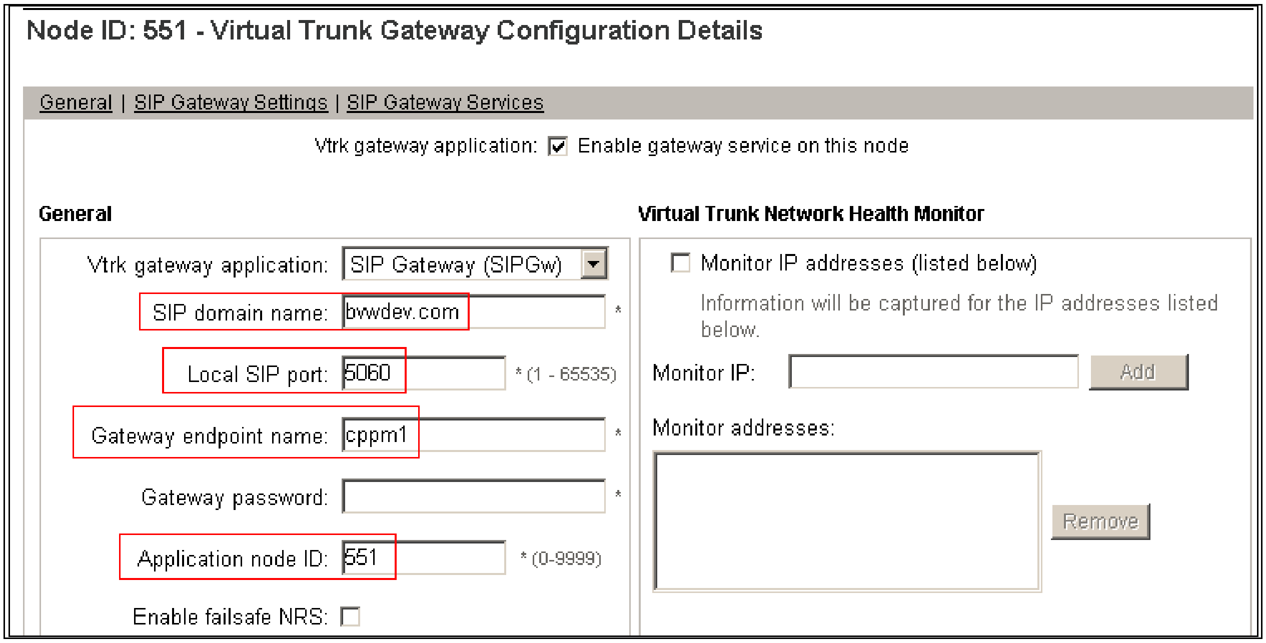
Applications (click to edit configuration)

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

5.5.3.1 Configure General section

In General section, enter the following information:

1. **SIP domain name:** domain name that is configured in Session Manager e.g. **bvwdev.com** as configured in **Section 7.1**
2. **Local SIP port** as **5060.**
3. **Gateway endpoint name:** enter SIP entity name of Communication Server 1000E configured on Session Manager e.g. **cppm1**
4. **Application node ID:** enter the Node ID of the current node as mentioned in **Section 5.5.3**.



Node ID: 551 - Virtual Trunk Gateway Configuration Details

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: cppm1 *

Gateway password: *

Application node ID: 551 * (0-9999)

Enable failsafe NRS: □

Virtual Trunk Network Health Monitor

□ Monitor IP addresses (listed below)

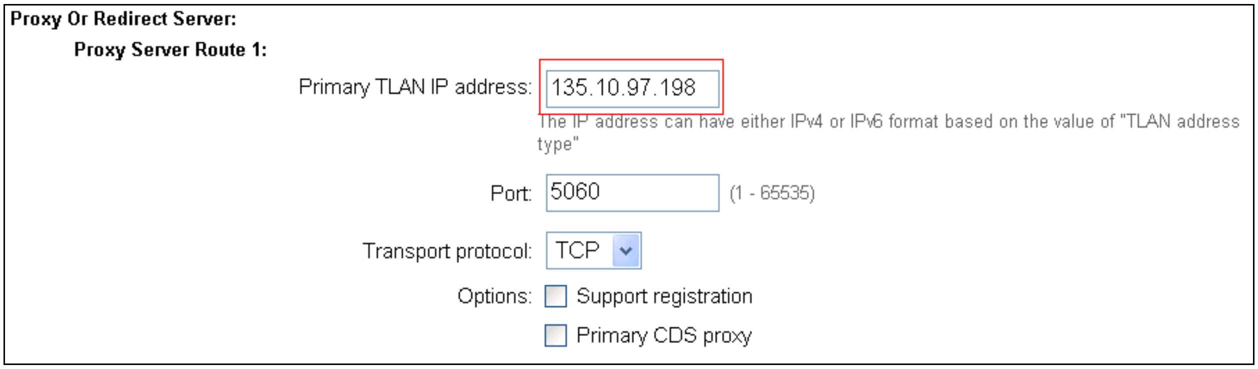
Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

5.5.3.2 Configure SIP Gateway Settings – Proxy Or Redirect Server:

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



Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 135.10.97.198

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

Port: 5060 (1 - 65535)

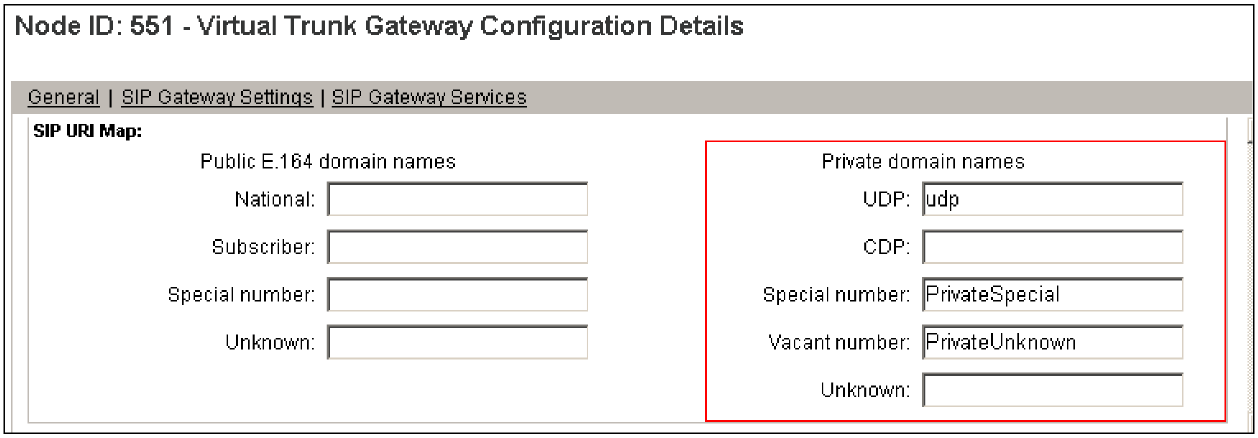
Transport protocol: TCP

Options: □ Support registration

□ Primary CDS proxy

5.5.3.3 Configure SIP URI Map for Private domain names:

The **UDP** field is configured as **udp.** The rest of the fields are left as default.



Node ID: 551 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

SIP URI Map:

Public E.164 domain names

National:

Subscriber:

Special number:

Unknown:

Private domain names

UDP: udp

CDP:

Special number: PrivateSpecial

Vacant number: PrivateUnknown

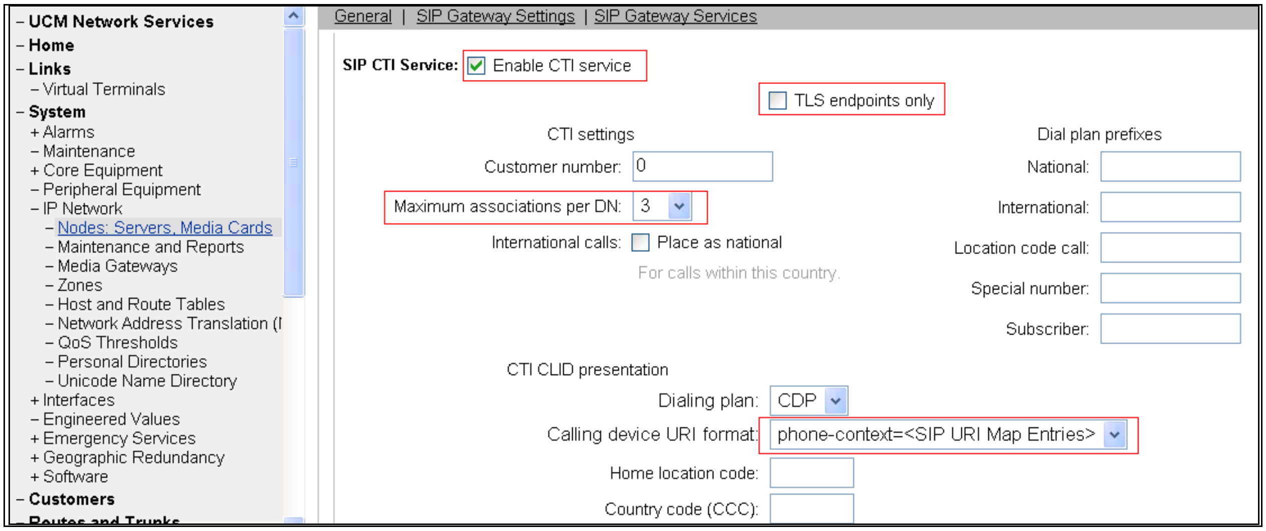
Unknown:

5.5.3.4 Enable CTI service

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.

In Sip Gateway Service section, browse to SIP CTI Service enter then following information:

1. **SIP CTI Service**: Select the Enable CTI service check box
2. **TLS Service Enabled**: Disable. After a system reboot, review this setting again. User may have to disable this again.
3. **Customer Number:** Enter the number used for the customer, for example, 0.
4. Maximum Associations per DN: Select a number between 1 and 10.
5. **Place International Calls Within This Country As National Calls**: Enable if applicable.
6. **National Prefix, International Prefix, Location Code Call Prefix, Special Number Prefix, Subscriber Prefix:** Enter number according to dialing plan, as appropriate.
7. **Dialing Plan**: Select the dialing plan for user's engineered system, for example, CDP.
8. **Calling Device URI format**: Select **phone-context=<SIP URI Map Entries>**.



General | SIP Gateway Settings | SIP Gateway Services

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

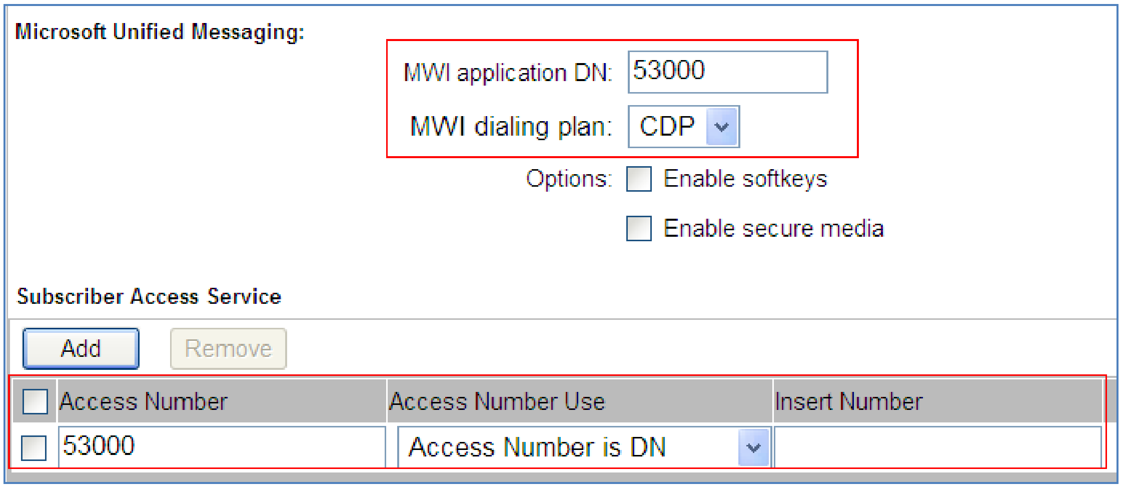
Calling device URI format: phone-context=<SIP URI Map Entries>

Home location code:

Country code (CCC):

5.5.3.5 Configure Microsoft Unified Messaging

In **Microsoft Unified Messaging, MWI application DN** is configured as **53000**. This is the pilot DN being used to reach the Office-LinX during the solution testing. **CDP** is the selected **MWI dialing plan**.



Microsoft Unified Messaging:

MWI application DN: 53000

MWI dialing plan: CDP

Options: □ Enable softkeys

□ Enable secure media

Subscriber Access Service

□ Access Number	Access Number Use	Insert Number
□ 53000	Access Number is DN	

Note: Above configurations is important. If these fields are not configured, the Office-LinX receives the SIP Message Header with Content-Type: multipart/mixed which Office-LinX does not currently support. This will therefore cause the solution to fail to accept calls with multipart/mixed message bodies. Office-LinX requires Content-Type: application/sdp.

5.5.4. Save changes and restart signaling Server

5.5.5. 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), Associated Set (AST), and KEY prompts.

CLS Determines the calling options and features available to the telephone.
• Make sure that Remote Call Control is allowed (T87A). By default, this feature is denied ((T87D).
• Make sure that Converged Desktop Multimedia feature is Restricted (CLS = CDMR). CMDR is the default.

AST: Defines key number to be used as the monitor key.
• Make sure that a Single Call Ringing (SCR) key number is assigned, for example, 00 for Key 0. Note: User cannot choose just any key. Some keys are pre-assigned or reserved for other features.
• Each terminal number requires one AST.

KEY Defines telephone function key assignments

- Make sure that the mnemonic MARP appears by Key 0, the primary directory number (DN) for the phone.
- The “Multiple Appearance DN Redirection Prime” (MARP) tells the system which TN (phone) configuration to use for call redirection purposes, for example, where to route a call in a busy situation.

```
    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 FBD WTA LPR MTD FND HTD TDD HFA CRPD
         MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
         POD SLKD CCSD SWA LND CNDA
         CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
         ICDD CDMD LLCN MCTD CLBD AUTU
         GPUD DPUD DNDA CFXD 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 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
```

5.5.6. Provision a Communication Server 1000 TR/87 service provider on Avaya ACE

See Section **8.2.1** for detail step on how to add Communication Server 1000E on Avaya ACE.

5.5.7. 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**.

5.5.8. Verify SIP route configuration.

Virtual routes let user assign common characteristics to trunks belonging to the same route; for example, zone to use for bandwidth management, associated node ID for data networking purposes, and access code. A route can contain one trunk or many trunks. Route can be build or review using the command line interface (LD 16/Print LD 21).

Use the command line interface (LD 16) or Element Manager to verify that the Network Calling Name Allowed (NCNA) and Network Call Redirection (NCRD) are allowed.

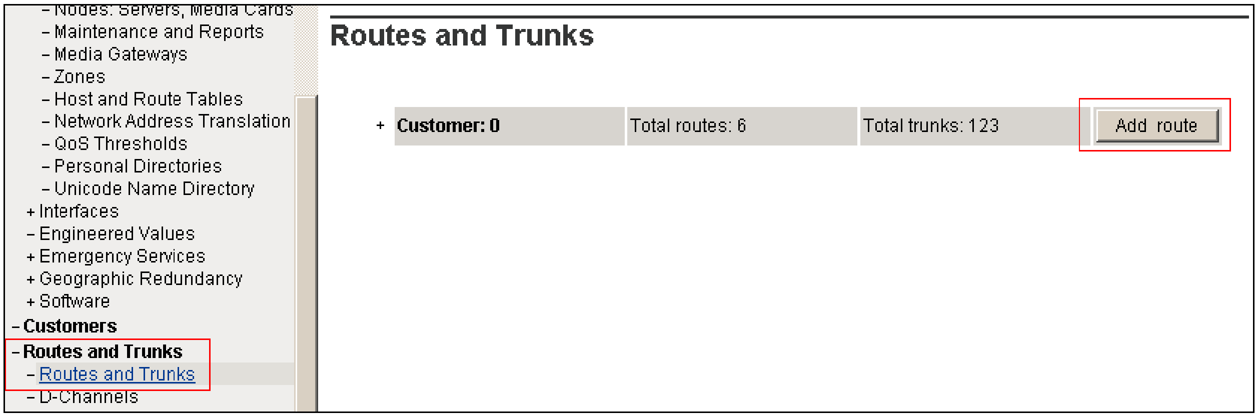
LD 21: RDB

The LD 21 printout shows the Route Data Block (RDB) for **Customer 0**, **Route 20**. Note: it is a **SIP** route and that the **NCNA** and **NCRD** prompts are set to YES.

```
REQ: prt
TYPE: rdb
CUST 0
ROUT 10
TYPE RDB
CUST 00
DMOD
ROUT 66
DES SIP ROUTE
TKTP TIE
NPID_TBL_NUM 0
SAT NO
RCLS EXT
VTRK YES
ZONE 100
PCID SIP
CRID NO
IFC SL1
PNI 00001
NCNA YES
NCRD YES
FALT NO
CTYP CDP
INAC YES
ISAR NO
DAPC NO
```

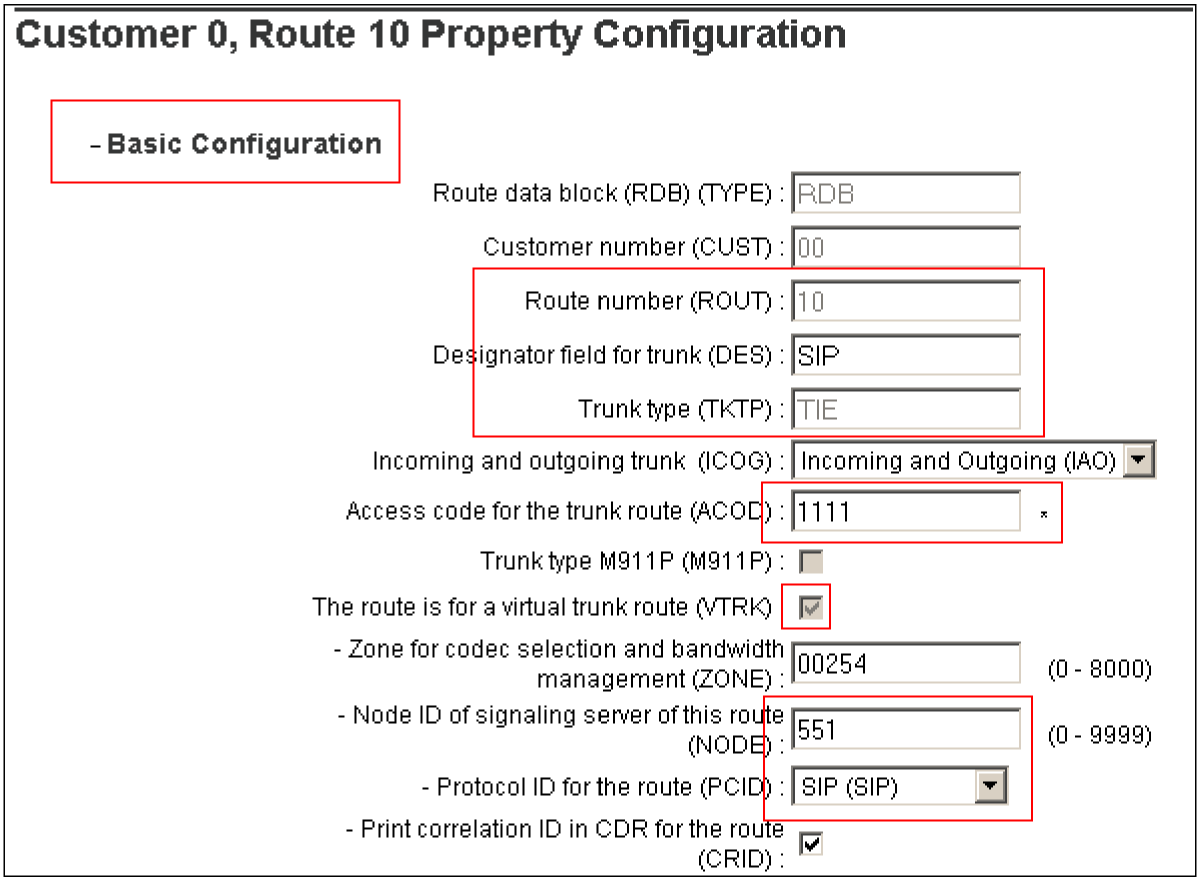
5.6. Route, RLB and DSC Configuration

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



+ **Customer: 0** | Total routes: 6 | Total trunks: 123

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



Customer 0, Route 10 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE) : RDB

Customer number (CUST) : 00

Route number (ROUT) : 10

Designator field for trunk (DES) : SIP

Trunk type (TKTP) : TIE

Incoming and outgoing trunk (ICOG) : Incoming and Outgoing (IAO)

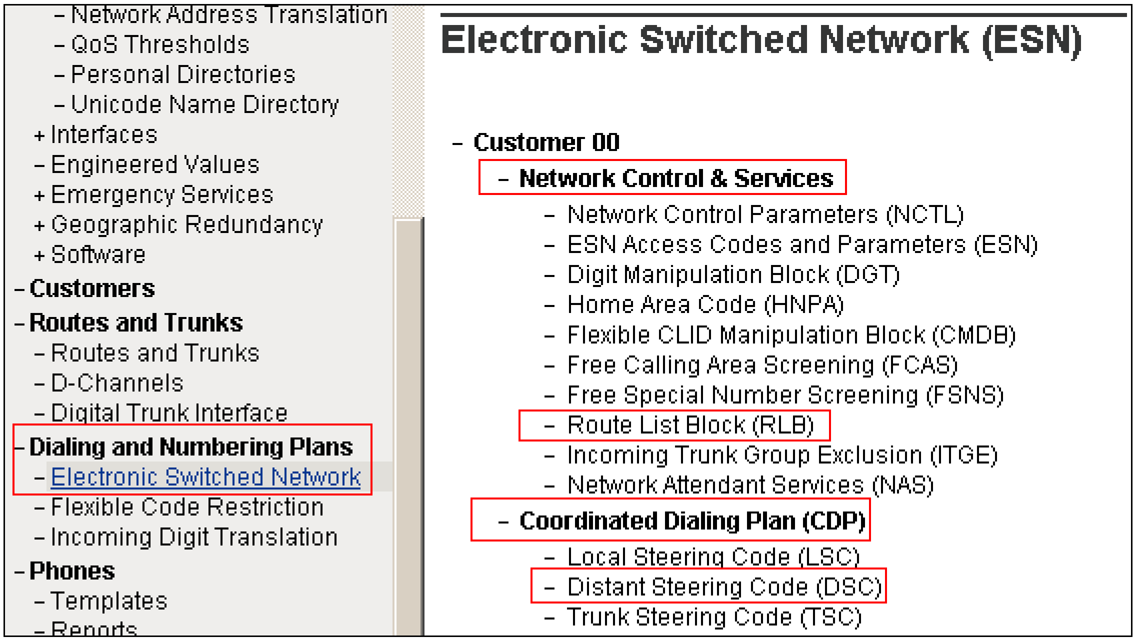
Access code for the trunk route (ACOD) : 1111 *

Trunk type M911P (M911P) : ☐

The route is for a virtual trunk route (VTRK) : ☑

- Zone for codec selection and bandwidth management (ZONE) : 00254 (0 - 8000)
- Node ID of signaling server of this route (NODE) : 551 (0 - 9999)
- Protocol ID for the route (PCID) : SIP (SIP)
- Print correlation ID in CDR for the route (CRID) : ☑

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

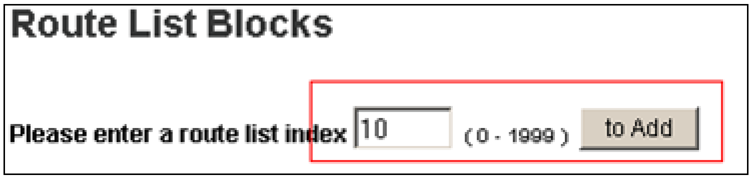
Electronic Switched Network (ESN)

- 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)

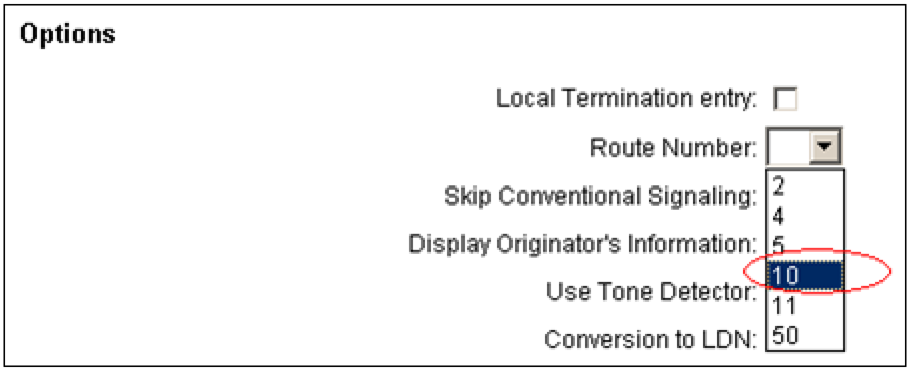
Enter the value of the route list index and click on **to Add** button to continue the configuration as shown below. During the solution testing the value of **10** was added.



Route List Blocks

Please enter a route list index 10 (0 - 1999) to Add

The **Route Number 10** being selected to the RLB created. Route **10** is selected since it was the route number assigned while adding a route as shown in **Figure** above.



Options

Local Termination entry: □

Route Number:

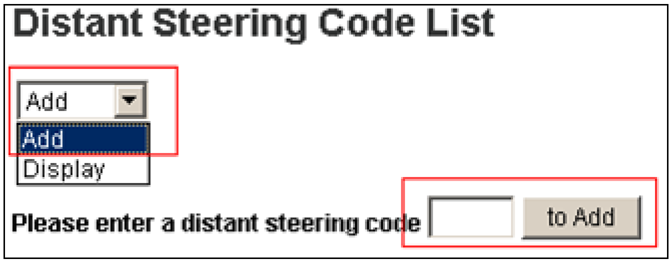
Skip Conventional Signaling:

Display Originator's Information:

Use Tone Detector:

Conversion to LDN:

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 in **Figure 14**.



Distant Steering Code List

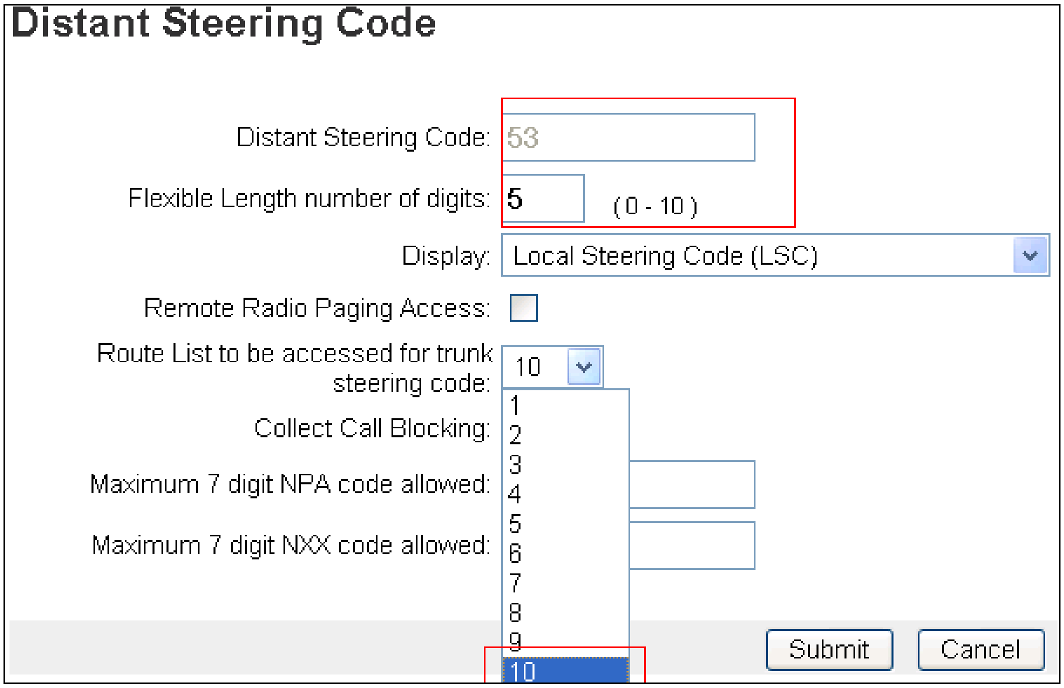
Add

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 53 was added during the solution testing. The value **53** was configured since the pilot DN of the Office-LinX system was **53000**.

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

Route List to be accessed for trunk steering code is selected as **10** from the drop down list. This value is selected based on the RLB created in above step.



Distant Steering Code

Distant Steering Code: 53

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: 10

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** of these Application Notes.

5.7. 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 1000E from overlay LD 11/20. Refer to **Section 12** for further information regarding add/configuration of endpoints/telephones.

In **Figure**, values that are shown in red are to be configured by the user. The **FDN** and **HUNT** value of **39000** was used during the solution testing as the access number to Avaya Aura® Messaging.

```
    Ld 11
    REQ: prt
    TYPE: 1165
    TN    096 0 00 17
    FDN   39000
    …
    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 39000
    …
    KEY   00 SCR 54312 0     MARP
             CPND
               CPND_LANG ROMAN
                 NAME DN 54312
                 XPLN 13
              DISPLAY_FMT FIRST,LAST
```

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.

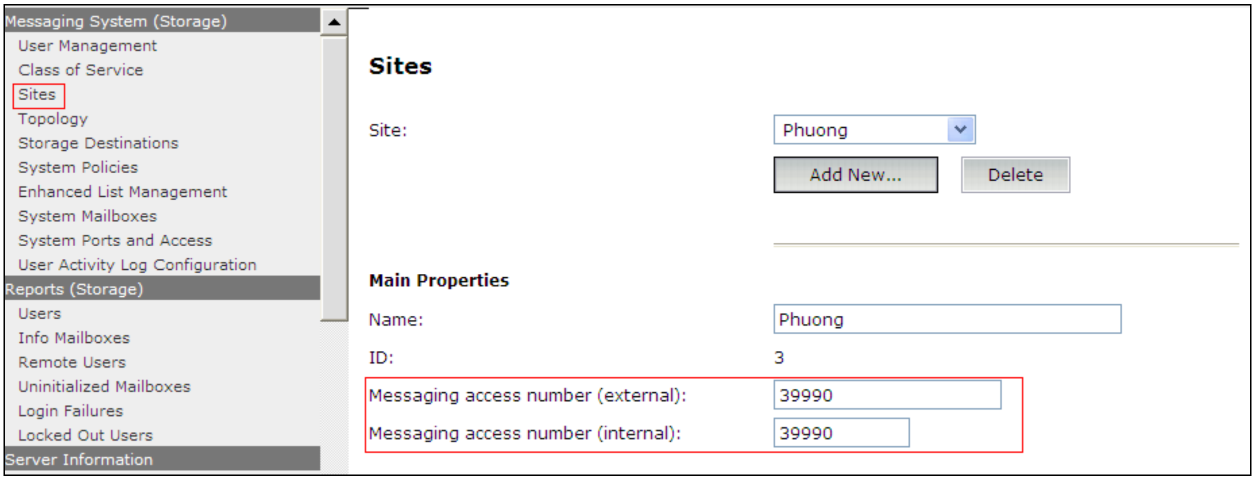
6.1. Administer Sites

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
- **Messaging access number (internal)** Enter a Messaging Pilot number

Sites detail screen on AAM shows Messaging access number.



Sites

Site: Phuong

Main Properties

Name: Phuong

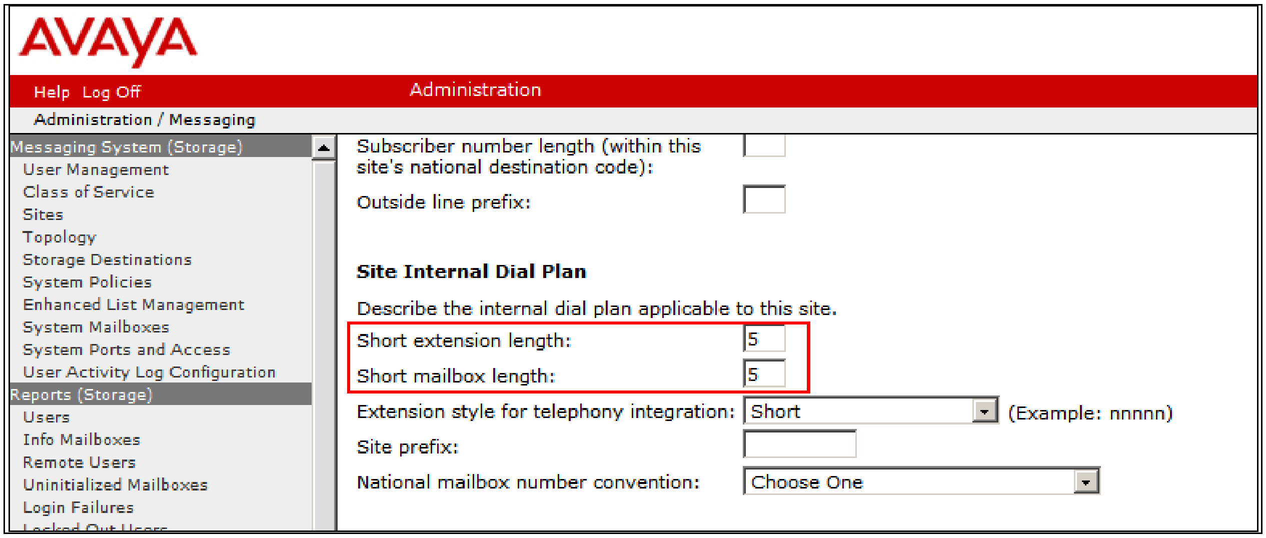
ID: 3

Messaging access number (external): 39990

Messaging access number (internal): 39990

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



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

Outside line prefix:

Site Internal Dial Plan

Describe the internal dial plan applicable to this site.

Short extension length: 5

Short mailbox length: 5

Extension style for telephony integration: Short (Example: nnnnn)

Site prefix:

National mailbox number convention: Choose One

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:

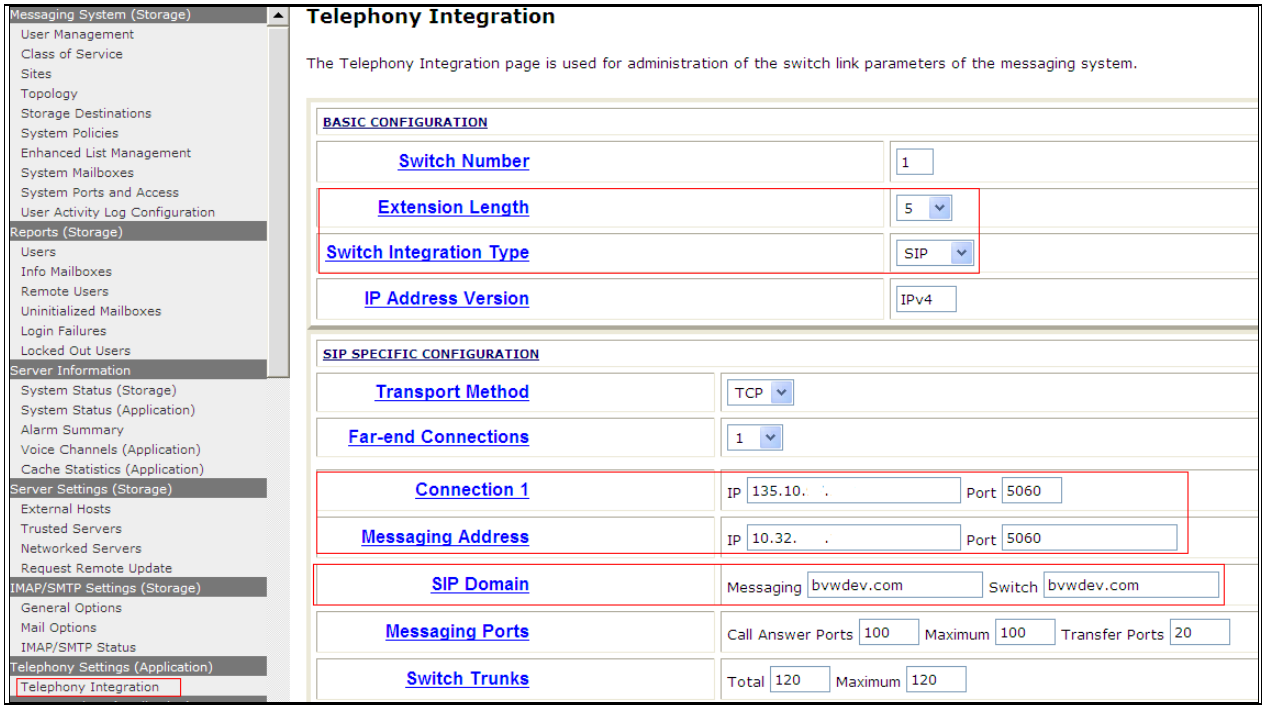
Under **Basic Configuration:**

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

Under **SIP Specific Configuration:**

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

Click **Save** to save changes.



Telephony Integration

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

BASIC CONFIGURATION

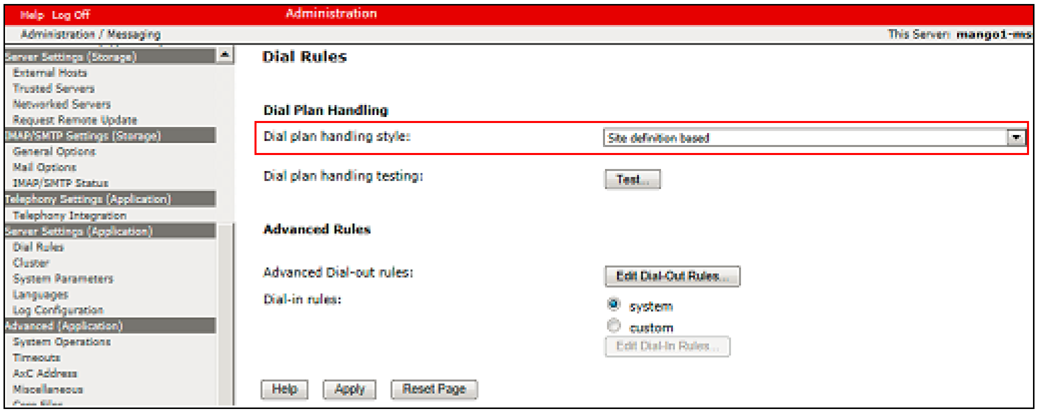
Switch Number	1
Extension Length	5
Switch Integration Type	SIP
IP Address Version	IPv4

SIP SPECIFIC CONFIGURATION

Transport Method	TCP
Far-end Connections	1
Connection 1	IP 135.10. . Port 5060
Messaging Address	IP 10.32. . Port 5060
SIP Domain	Messaging 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

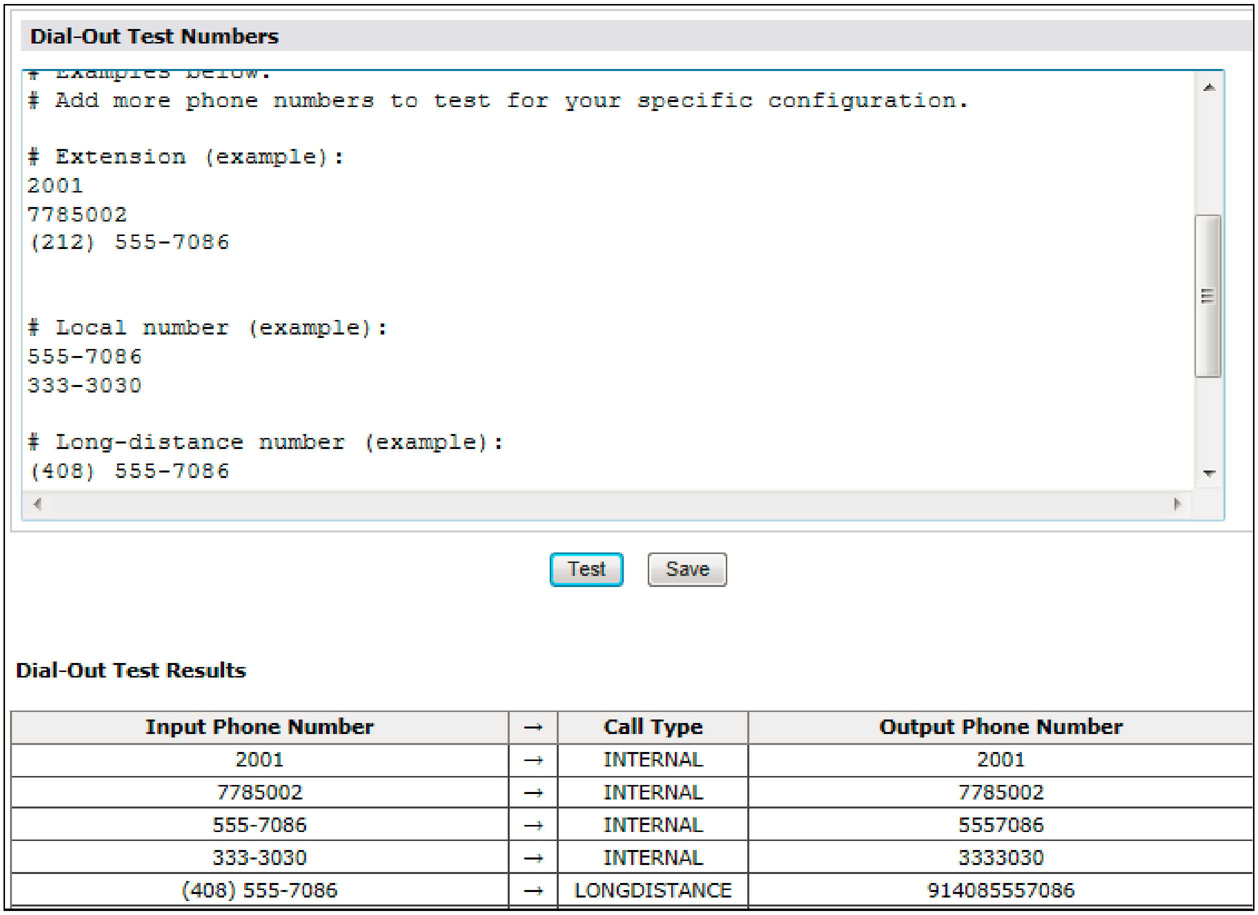
Dial plan handling testing:

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 Manager, whether the call is destined for another extension or ultimately expected to be routed to the PSTN.



Dial-Out Test Numbers

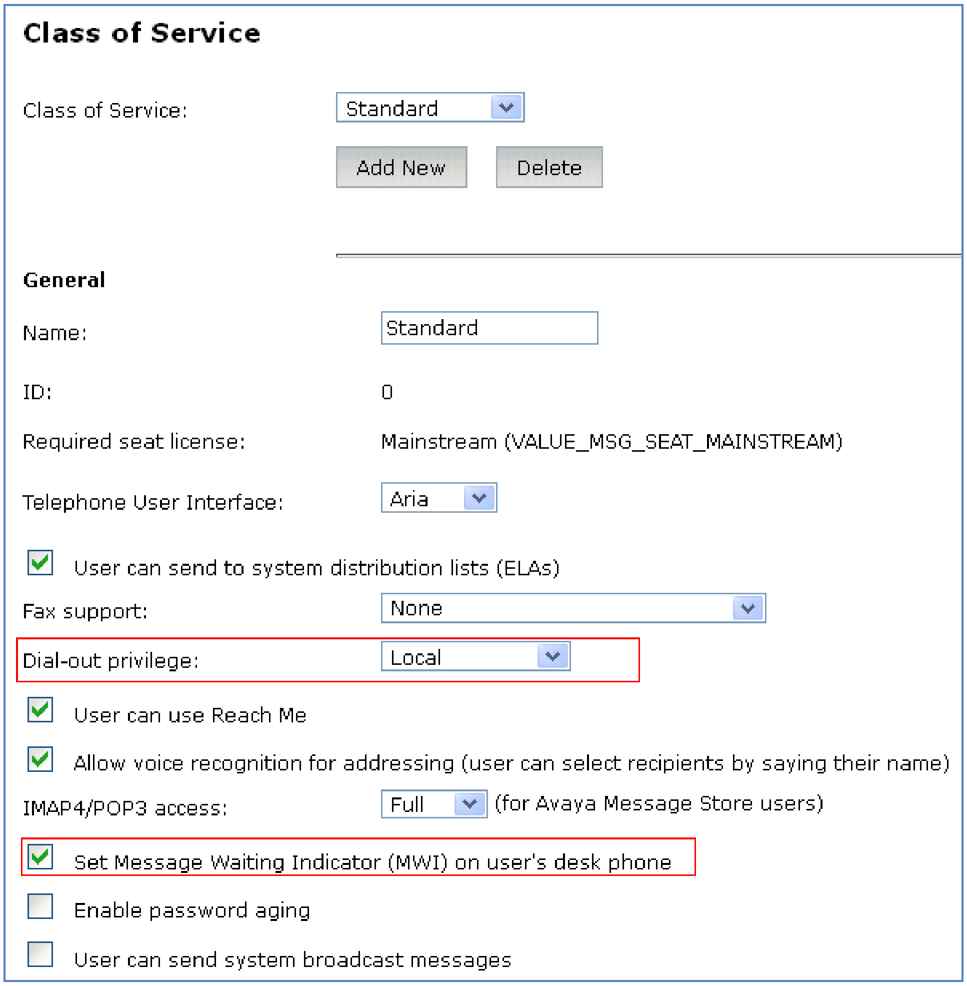
```
# Examples below.
# Add more phone numbers to test for your specific configuration.

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


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

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

Dial-Out Test Results

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

6.4. Configure Class of Service

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



Class of Service

Class of Service: Standard

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

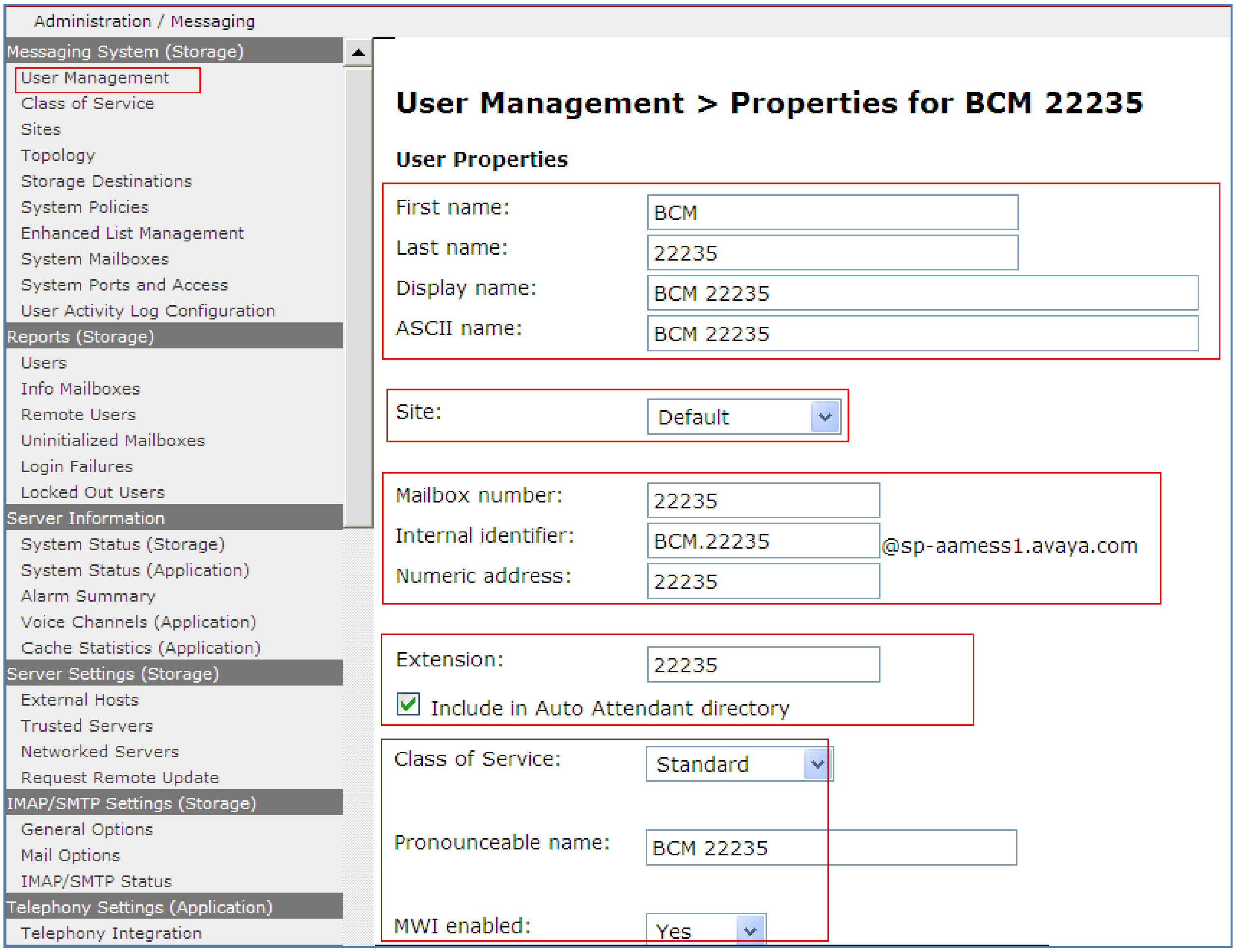
□ User can send system broadcast messages

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 i.e. **22235**
• **Internal identifier**	Enter the name for internal use
• **Numeric address**	Enter the mailbox number
• **Extension**	Enter desired extension number i.e. **22235**



User Management > Properties for BCM 22235

User Properties

First name: BCM
Last name: 22235
Display name: BCM 22235
ASCII name: BCM 22235

Site: Default

Mailbox number: 22235
Internal identifier: BCM.22235 @sp-aamess1.avaya.com
Numeric address: 22235

Extension: 22235
☑ Include in Auto Attendant directory

Class of Service: Standard

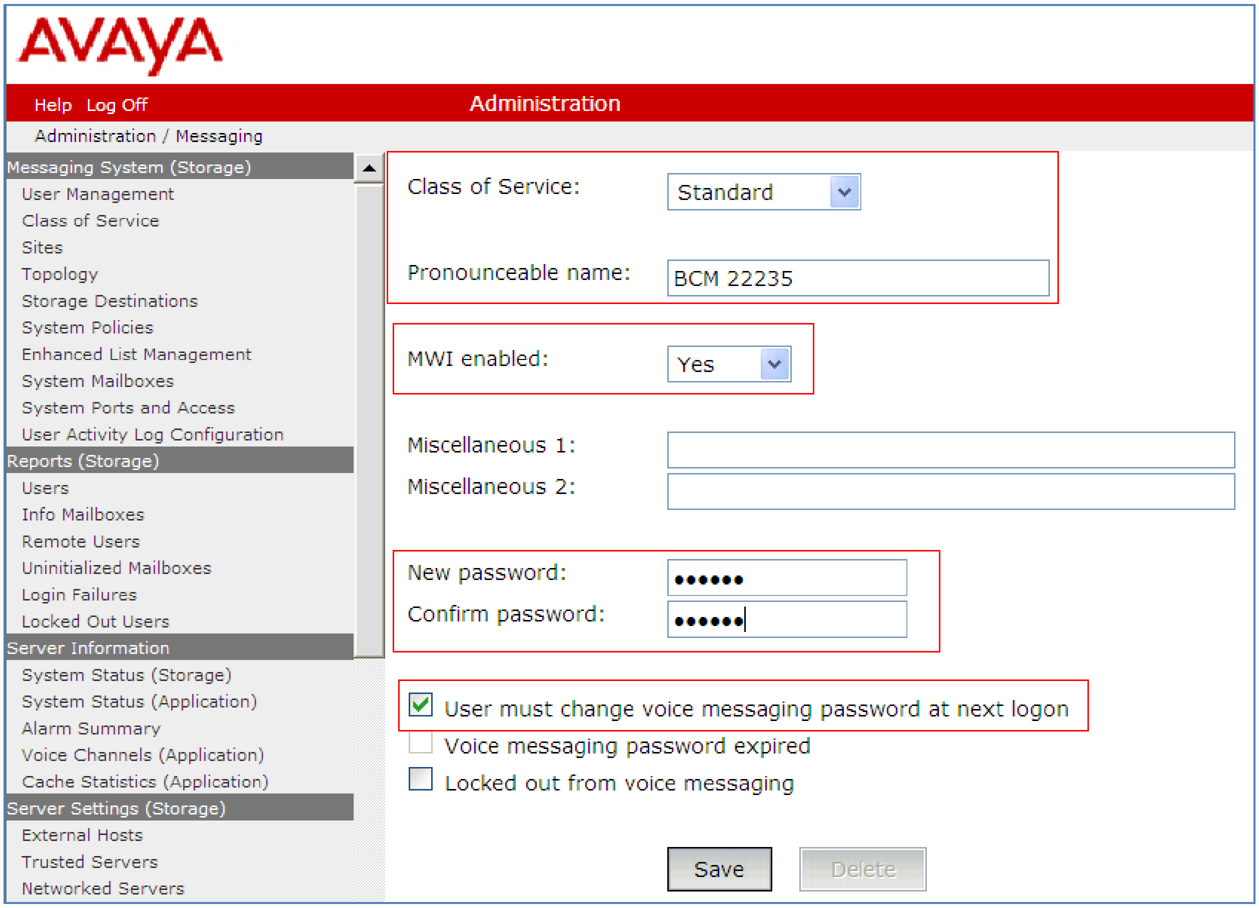
Pronounceable name: BCM 22235

MWI enabled: Yes

Scroll down on the page to Class of Service.

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

Click **Save** to save changes.



Class of Service: Standard

Pronounceable name: BCM 22235

MWI enabled: Yes

Miscellaneous 1:

Miscellaneous 2:

New password: ••••••

Confirm password: ••••••

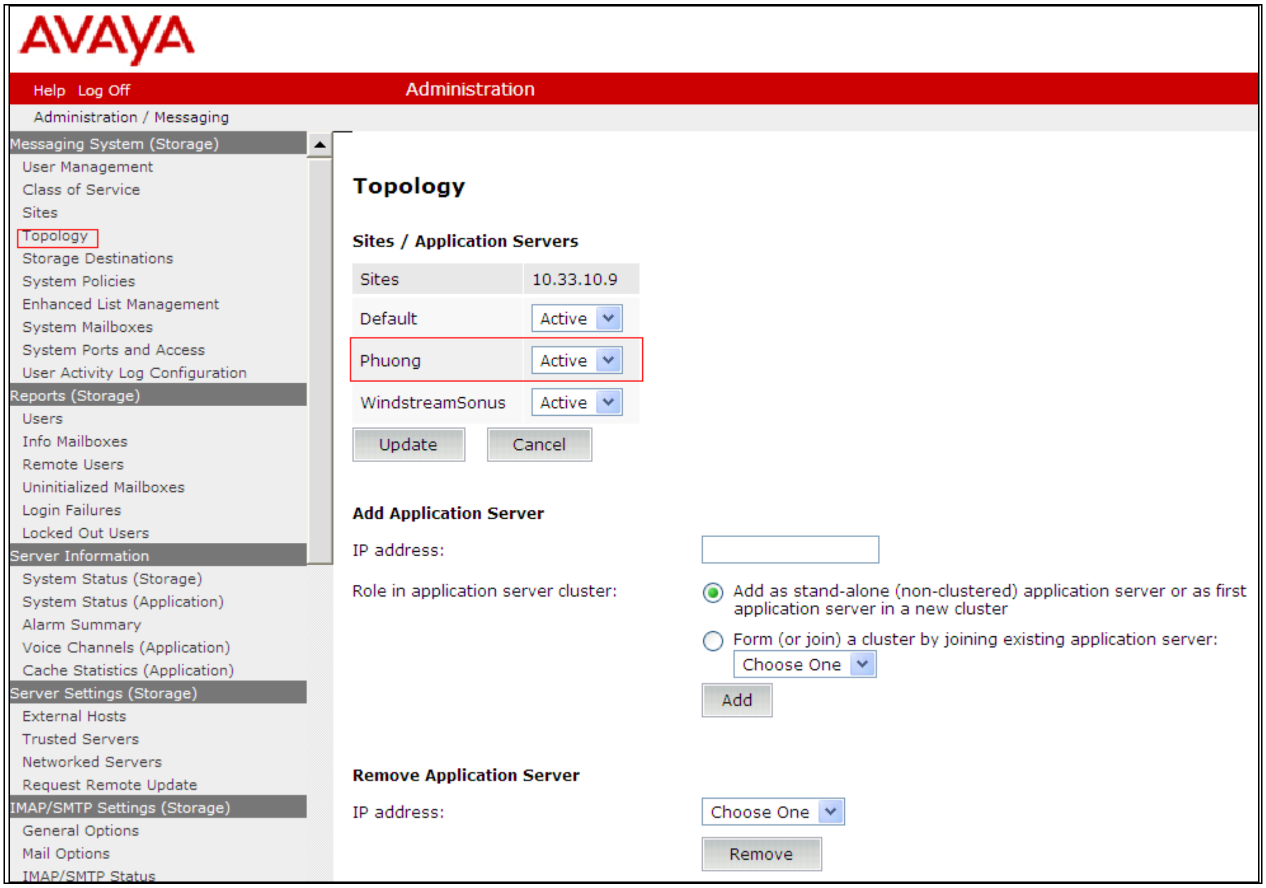
☑ User must change voice messaging password at next logon

□ Voice messaging password expired

□ Locked out from voice messaging

6.6. Administer Topology

Select Topology under Messaging System (Storage).
Verify the site that was defined in **Section6.1** is Active



Topology

Sites / Application Servers

Sites	10.33.10.9
Default	Active
Phuong	Active
WindstreamSonus	Active

Add Application Server

IP address:

Role in application server cluster:

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

○ Form (or join) a cluster by joining existing application server: Choose One

Remove Application Server

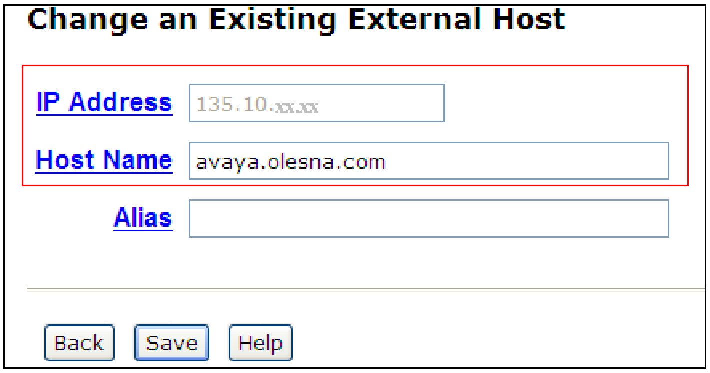
IP address: Choose One

6.7. Administer External Host

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

Select Server\Settings (Storage) → External Hosts, click Add
In Add a New External Host page:
IP Address: Enter IP address of the External SMTP Server, in this compliance test it is IP address of ESNA server.
Host Name: Enter host Name of the External SMTP Server.

Below is detail on how the ESNA Server was configured in this compliance test:


Change an Existing External Host

IP Address: 135.10.xx.xx

Host Name: avaya.olesna.com

Alias:

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
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- Manage Element
- Applications
- Application Sequence
- User Management
- Synchronization

7.1. Configure SIP Domain

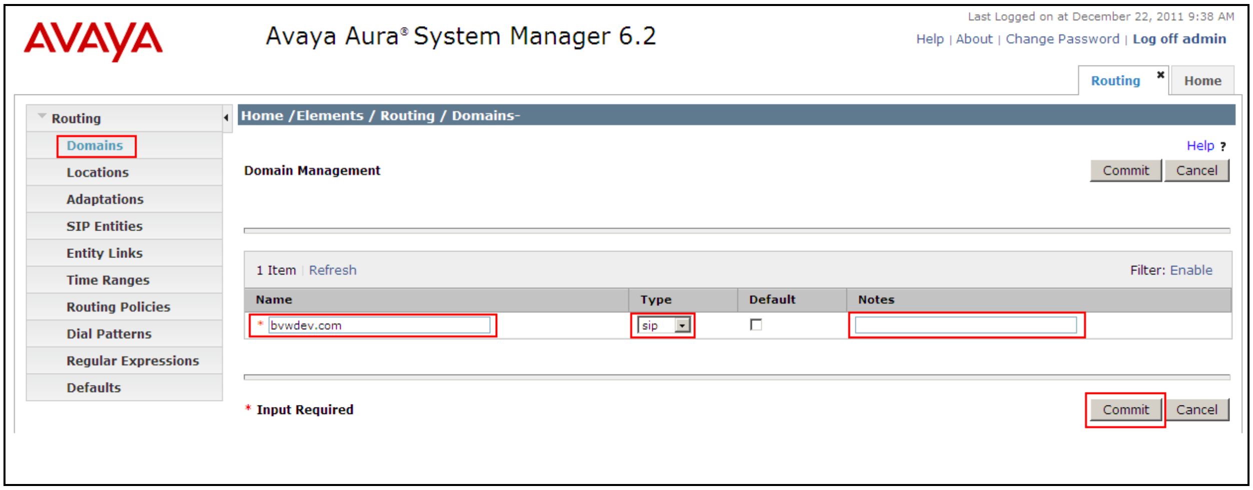
Launch a web browser, enter **http://<IP address of System Manager>/SMGR** in the URL, and log in with the appropriate credentials.

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

- **Name** – Enter the Authoritative Domain Name in this solution setup, **bvwdev.com** domain is used.

- **Type** – Select **SIP**

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



Domain Management

Name	Type	Default	Notes
* bvwdev.com	sip	□	

* Input Required

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.

General section

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

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

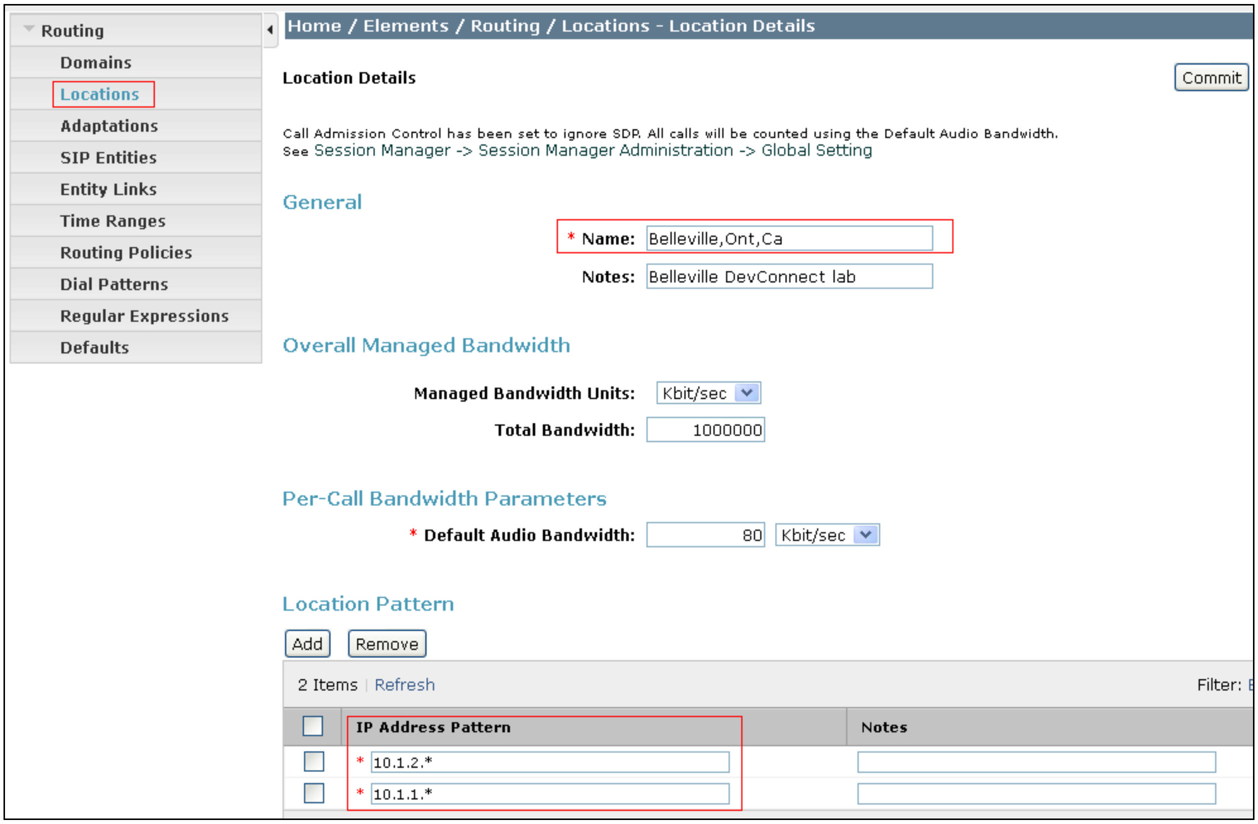
Location Pattern section

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

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

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

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



Location Details

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

General

* Name: Belleville,Ont,Ca

Notes: Belleville DevConnect lab

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth: 1000000

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

2 Items | Refresh

□	IP Address Pattern	Notes
□	* 10.1.2.*	
□	* 10.1.1.*	

7.3. Configure SIP Entities

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

- Session Manager itself.
- Communication Server 1000E 7.5
- Avaya Aura® Messaging
- Avaya ACE
- ESNA server

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

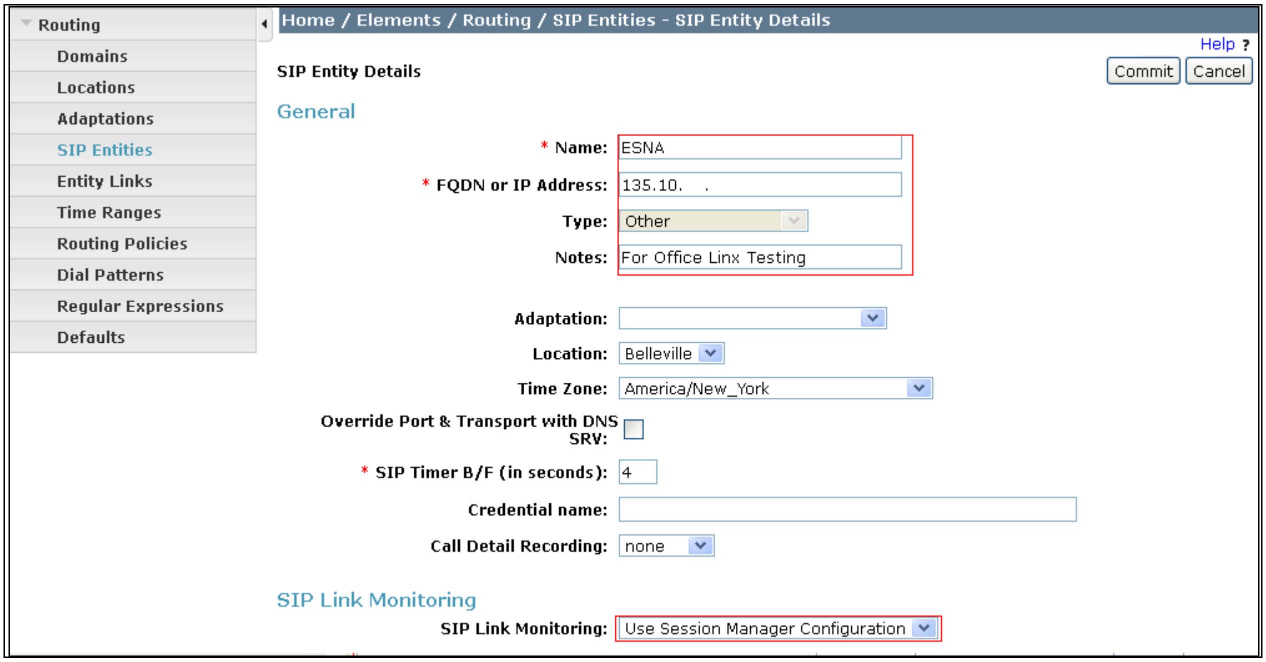
General section

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

- Enter a descriptive Location name in the Name field.
- Enter IP address for signaling interface on each Communication Server 1000E 7.5, virtual SM-100 interface on Session Manager, Avaya Aura® Messaging, Avaya ACE and ESNA.
- From the **Type** drop down menu select a type that best matches the SIP Entity.
    - For Communication Server 1000E 7.5, select SIP Trunk

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

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



SIP Entity Details

General

* Name: ESNA

* FQDN or IP Address: 135.10. .

Type: Other

Notes: For Office Linx Testing

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

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Repeat all the steps for each new entity

7.4. Configure Entity Links

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

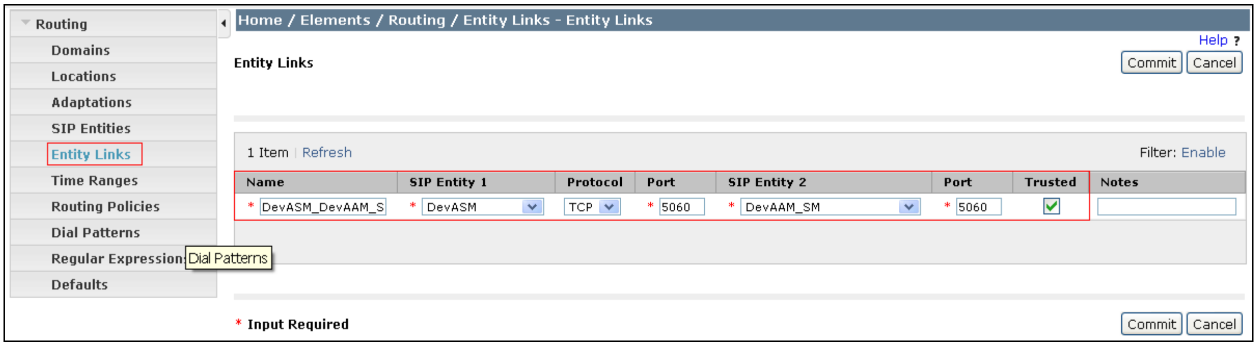
- Session Manager ⇔ Communication Server 1000E Release 7.5
- Session Manager ⇔ ESNA
- Session Manager ⇔ Avaya Aura® Messaging
- Session Manager ⇔ Avaya ACE

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

- Enter a descriptive name in the **Name** field.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section 7.3**.
- In the **Protocol** drop down menu, select the protocol to be used.

- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
  - UDP or TCP – 5060
- In the **SIP Entity 2** drop down menu, select an entity created in **Section 7.3**.
- In the **Port** field, enter the port to be used (e.g. **5060**).
- Check the **Trusted** box.
- Enter a description in the **Notes** field if desired.

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



Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* DevASM_DevAAM_S	* DevASM	TCP	* 5060	* DevAAM_SM	* 5060	☑	

* Input Required

Repeat the steps to define Entity Links between Session Manager, Communication Server 1000E 7.5, ESNA (TCP/UDP-5060) and Avaya ACE (UDP-5060).

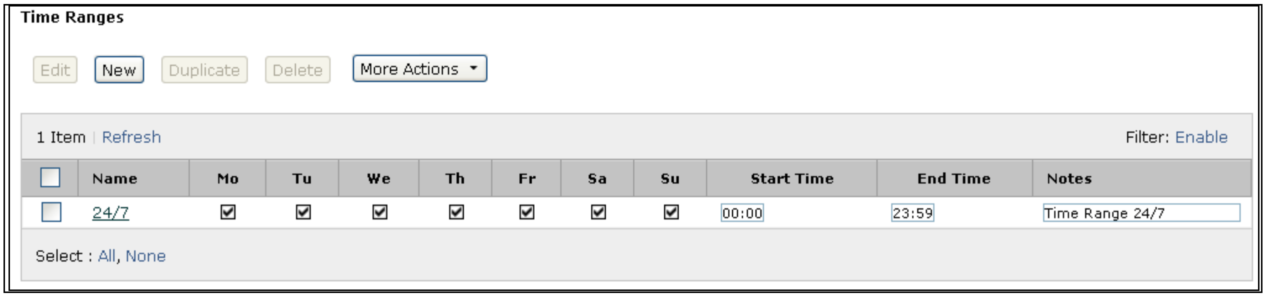
7.5. Time Ranges

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

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

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

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



□	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
□	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

7.6. Configure Routing Policy

Routing Policies associate destination SIP Entities with Time of Day admission control parameters and Dial Patterns. In the reference configuration, Routing Policies are defined for: Communication Server 1000E Release 7.5.

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

General section

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

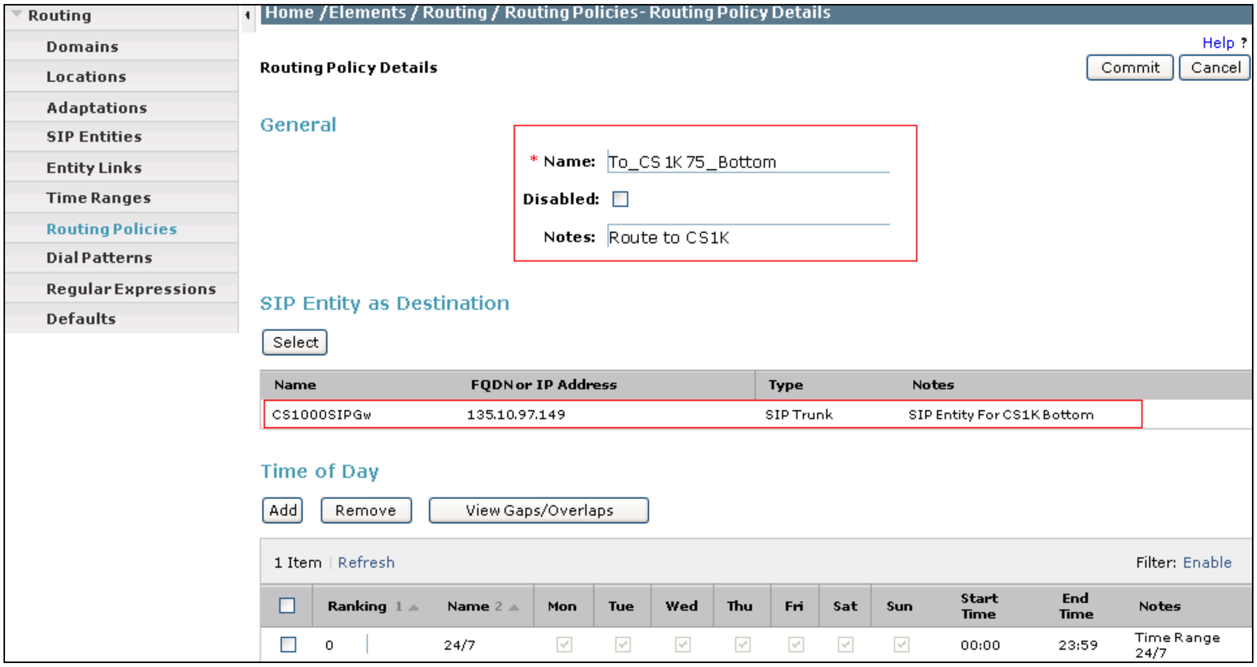
SIP Entity as Destination section

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

Time of Day section

- Leave default values.

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



Routing Policy Details

General

* Name: To_CS 1K 75_Bottom

Disabled: □

Notes: Route to CS1K

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CS1000SIPGw	135.10.97.149	SIP Trunk	SIP Entity For CS1K Bottom

Time of Day

□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Repeat the steps to define routing policies to others Entities.

7.7. Dial Patterns

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

- 54xxx – SIP endpoints in Avaya Communication Server 1000E Release 7.5
- 53000 – ESNA pilot number
- 39990 – Avaya Aura® Messaging Pilot Number.

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

General section

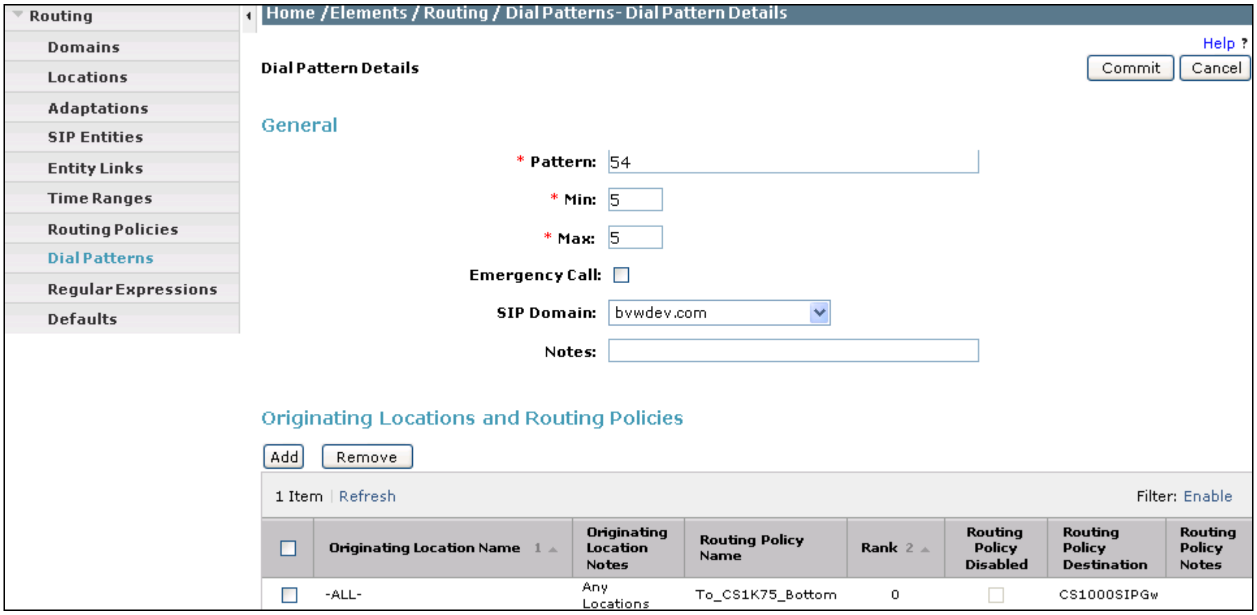
- Enter a unique pattern in the **Pattern** field (e.g. **54**).
- In the **Min** field enter the minimum number of digits (e.g. **5**).
- In the **Max** field enter the maximum number of digits (e.g. **5**).
- In the **SIP Domain** field drop down menu select the domain that will be contained in the Request URI *received* by Session Manager from Communication Manager.
- Enter a description in the **Notes** field if desired.

Originating Locations and Routing Policies section

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

- Routing Policies **To_CS1K75_Bottom**.
- Click on the **Select** button and return to the Dial Pattern window.

Click the **Commit** button to save the new definition. The following screen shows the dial pattern used for Communication Server 1000E 7.5 during the compliance test.



Dial Pattern Details

General

* Pattern: 54

* Min: 5

* Max: 5

Emergency Call: □

SIP Domain: bvwdev.com

Notes:

Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	To_CS1K75_Bottom	0	□	CS1000SIPGw	

8. Configure Avaya ACE 3.0

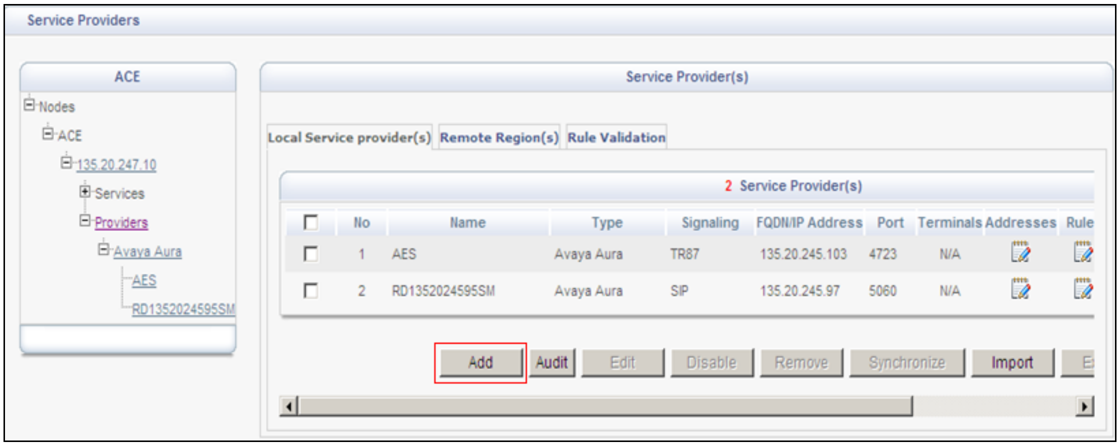
8.1. Add Communication Server 1000E SIP Service Provider

8.1.1. Add CS1K server provider using SIP service.

Add an Avaya CS 1000 SIP network element as a service provider on Avaya ACE to enable communication between two systems using the SIP protocol.

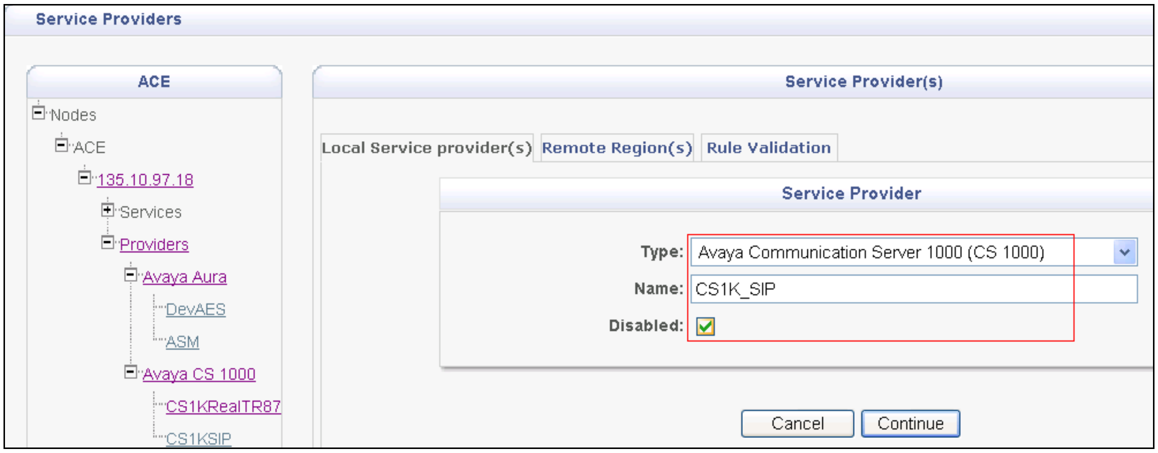
Procedure

1. Login https://<ACEipaddress>:9443/oamp.
2. On the menu bar, choose **Configuration** and then **Service Providers**. The Service Providers window appears.
3. Click **Add**. The Service Provider dialog box appears.



☐	No	Name	Type	Signaling	FQDN/IP Address	Port	Terminals	Addresses	Rule
☐	1	AES	Avaya Aura	TR87	135.20.245.103	4723	N/A		
☐	2	RD1352024595SM	Avaya Aura	SIP	135.20.245.97	5060	N/A		

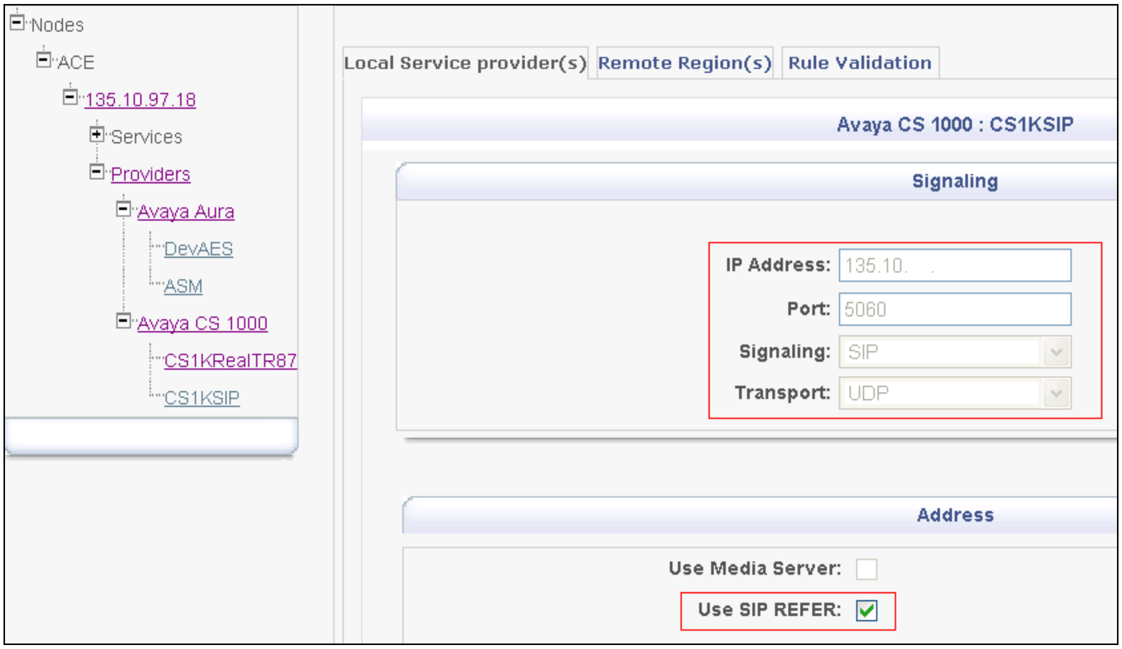
4. From the **Type** list, select **Avaya Communication Server 1000 (CS 1000)**.
5. In the **Name** field, enter a name for the Communication Server 1000 service provider.
6. Select the **Disable** check box to add the service provider in a disabled state.



Type: Avaya Communication Server 1000 (CS 1000)
Name: CS1K_SIP
Disabled: ☑

Note:
User can continue to update service provider configuration (including rules configuration) after it is added in the disabled state. Disabling the provider only makes it unavailable to handle Web service requests for the duration for which it is disabled. However, all configuration information is preserved. User can enable the provider at a later time.

7. Clicks continue**.** The Service Providers window for COMMUNICATION SERVER 1000 appears.
8. In the **Signaling** dialog box, enter the IP address of the Session Manager in the **IP Address** field. In the **Port** field, enter the port used for signaling. Accept the default 5060 if applicable.
9. In the **Signaling** list, select **SIP**.
10. To support Third Party Call Control (V2), select the **Use SIP REFER** check box to generate a ring back tone from the called party to be heard by the calling party, when a call is initiated. See example in the figure:



Avaya CS 1000 : CS1KSIP

Signaling

IP Address: 135.10. .

Port: 5060

Signaling: SIP

Transport: UDP

Address

Use Media Server: □

Use SIP REFER: ☑

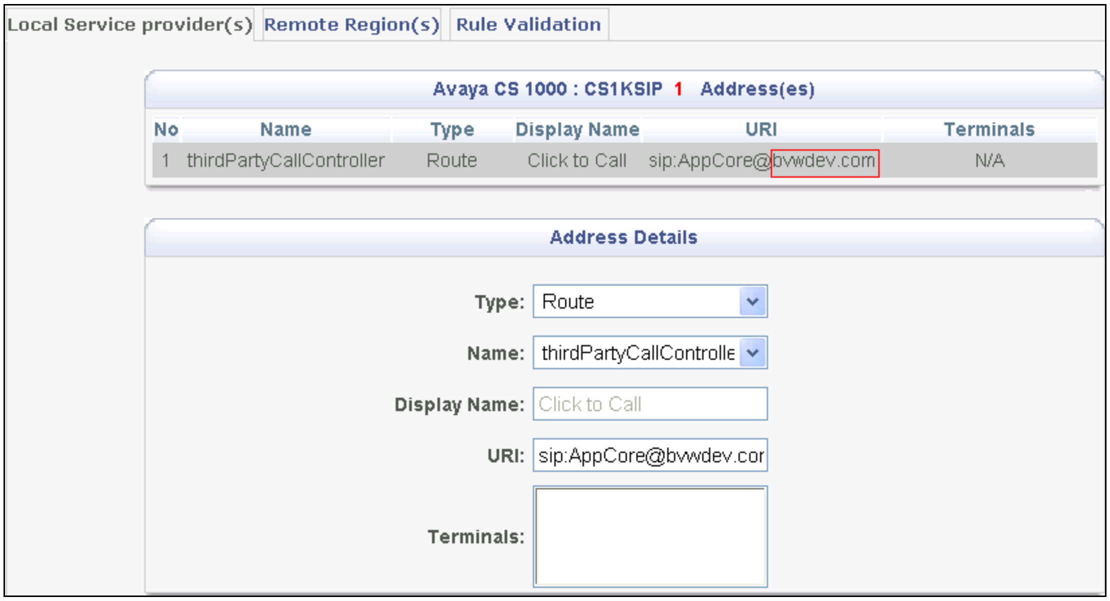
11. Click **Next**. The ACE GUI takes to the next task in the service provider configuration.

8.1.2. Configuring the route address

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 add a service provider that supports third party call control, the system automatically adds a default route address (sip:AppCore@Avaya.com).

Procedure

1. Make sure that the **Service Providers - Addresses** window is open.
2. In the **Addresses** dialog box, select the route entry. The details of the route address appear in the **Address Details** dialog box.
3. In the **Display Name** field, enter a name for the route address.
4. In the **URI** field, enter a valid URI to identify the route address. E.g. **bvwdev.com**
5. Click **Modify** to configure the route address. The route address is updated in the **Addresses** dialog box as shown in the figure:



Avaya CS 1000 : CS1KSIP 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: thirdPartyCallControlle

Display Name: Click to Call

URI: sip:AppCore@bvwdev.cor

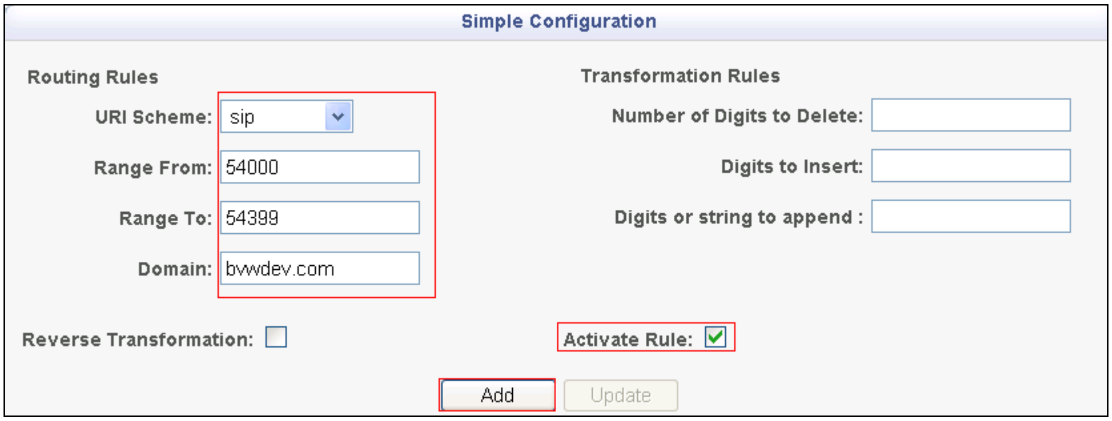
Terminals:

6. Click **Next**. The Avaya ACE GUI takes to the next task in the service provider configuration.

8.1.3. Configuring simple translation rules

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.

1. Ensure that the Translation Rule for Service Provider - <service provider type: service provider name> window is open. The **Calling Party Translation Rule** window opens with the Simple Configuration dialog box.
2. To add a simple rule, enter information in the appropriate fields for routing rules and/or transformation rules.
    a. **URI Scheme** :sip
    b. **Range From/To**: 54000-54399
    c. **Domain**: bvwdev.com
3. To activate the rule, select the **Activate Rule** check box.
   Important:
   To ensure the correctness of each rule that is configured, validate the rule using the Avaya ACE rule validation tool, before activate it.
4. Click **Add**. Below figure is an example of Calling Party Translation Rules during testing this solution:



Simple Configuration

Routing Rules

URI Scheme: sip

Range From: 54000

Range To: 54399

Domain: bvwdev.com

Transformation Rules

Number of Digits to Delete:

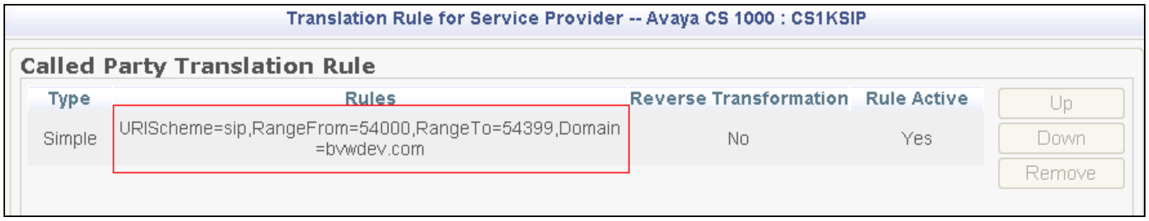
Digits to Insert:

Digits or string to append :

Reverse Transformation: □

Activate Rule: ☑

5. Click **Next** to configure called party translation rules.
6. Click **Submit** to save the rule configuration. Below is an example of simple Called Party Translation rule:

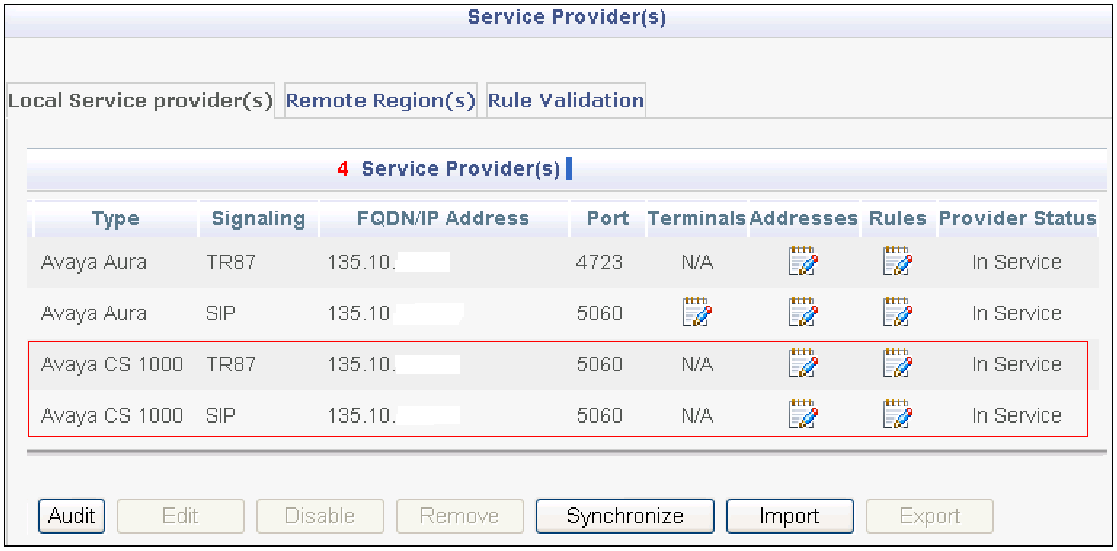


Translation Rule for Service Provider -- Avaya CS 1000 : CS1KSIP

Called Party Translation Rule

Type	Rules	Reverse Transformation	Rule Active
Simple	URIScheme=sip,RangeFrom=54000,RangeTo=54399,Domain=bvwdev.com	No	Yes

The Service Providers window appears. Selected the Activate check box, ACE applies the rules to web service traffic that it processes. Verify the status of service providers is “In Service”:



Service Provider(s)

4 Service Provider(s)

Type	Signaling	FQDN/IP Address	Port	Terminals	Addresses	Rules	Provider Status
Avaya Aura	TR87	135.10.[redacted]	4723	N/A	✎	✎	In Service
Avaya Aura	SIP	135.10[redacted]	5060	✎	✎	✎	In Service
Avaya CS 1000	TR87	135.10.[redacted]	5060	N/A	✎	✎	In Service
Avaya CS 1000	SIP	135.10.[redacted]	5060	N/A	✎	✎	In Service

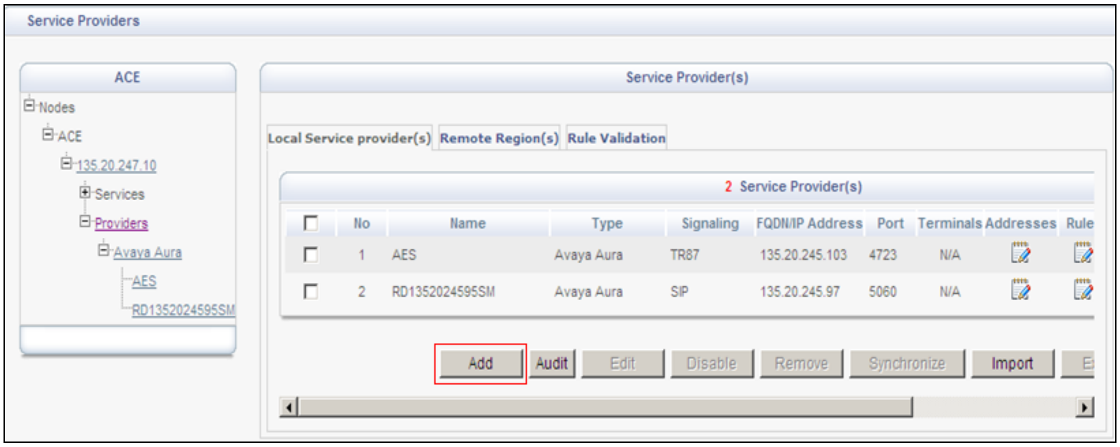
8.2. Add Communication Server 1000E TR/78 Service Provider

8.2.1. Add CS1K server provider using TR/87 service.

Add an Avaya Communication Server 1000 TR/87 network element as a service provider on the Avaya ACE to enable communications between the Communication Server 1000 element and the Avaya ACE uses TR/87 protocol without advanced services support.

Procedure

1. On the menu bar, choose **Configuration** and then **Service Providers**. The Service Providers window appears.
2. Click **Add**. The Service Provider dialog box appears.



Service Providers

ACE

- Nodes
  - ACE
    - 135.20.247.10
      - Services
      - Providers
        - Avaya Aura
          - AES
          - RD1352024595SM

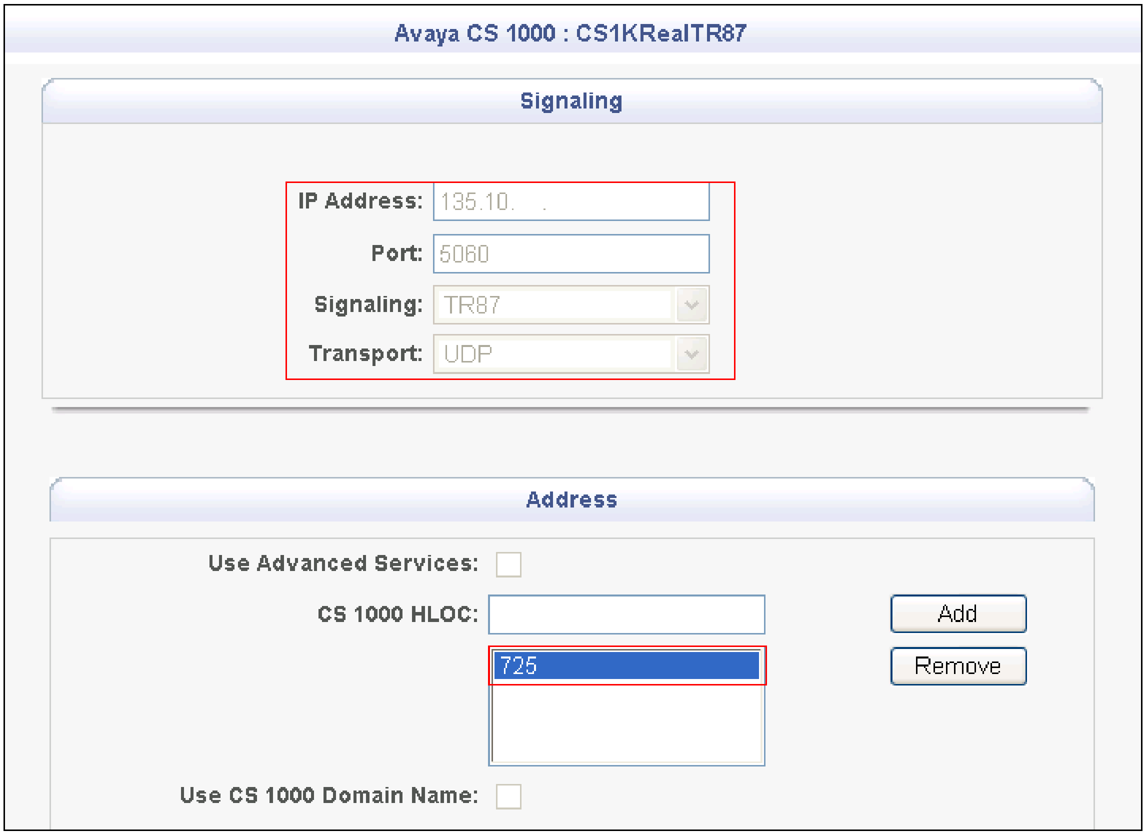
Service Provider(s)

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

2 Service Provider(s)

☐	No	Name	Type	Signaling	FQDN/IP Address	Port	Terminals	Addresses	Rule
☐	1	AES	Avaya Aura	TR87	135.20.245.103	4723	N/A	📝	📝
☐	2	RD1352024595SM	Avaya Aura	SIP	135.20.245.97	5060	N/A	📝	📝

3. From the **Type** list, select **Avaya Communication Server 1000 (CS 1000)**.
4. In the **Name** field, enter a name for the CS 1000 service provider.
5. Click Continue**.** The Service Providers window for CS 1000 appears.
6. In the **Signaling** dialog box, enter the IP address of the Communication Server 1000E Node IP in the **IP Address** field. In the **Port** field, enter the port used for signaling. Accept the default 5060 if applicable.
7. In the **Signaling** list, select **TR87**.
8. For networks with multiple systems (for example, an IP Peer Network), in the **CS 1000 HLOC** field, enter a one to seven-digit Home Location Code (HLOC) for the CS 1000, and click **Add**. See example in the figure:



Avaya CS 1000 : CS1KRealTR87

Signaling

IP Address: 135.10. .

Port: 5060

Signaling: TR87

Transport: UDP

Address

Use Advanced Services: □

CS 1000 HLOC:

725

Use CS 1000 Domain Name: □

9. Click **Next**. The ACE GUI takes to the next task in the service provider configuration.

8.2.2. Configuring the route address

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).

Procedure

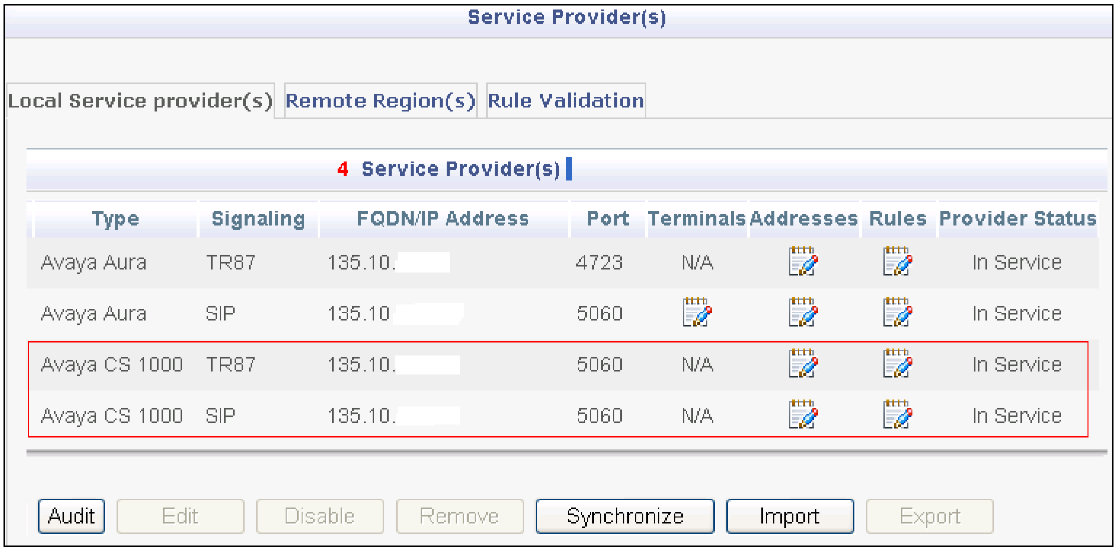
1. Make sure that the **Service Providers - Addresses** window is open.
2. In the **Addresses** dialog box, select the route entry. The details of the route address appear in the **Address Details** dialog box.
3. In the **Display Name** field, enter a name for the route address.
4. In the **URI** field, enter a valid URI to identify the route address. E.g. **bvwdev.com**
5. Click **Modify** to configure the route address. The route address is updated in the **Addresses** dialog box.
6. Click **Next**. The Avaya ACE GUI takes to the next task in the service provider configuration.

8.2.3. Configuring simple translation rules

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.

1. Ensure that the Translation Rule for Service Provider - <service provider type: service provider name> window is open. The **Calling Party Translation Rule** window opens with the Simple Configuration dialog box.
2. To add a simple rule, enter information in the appropriate fields for routing rules and/or transformation rules.
    a. **URI Scheme** :sip
    b. **Range From/To**: 54000-54399
    c. **Domain**: bvwdev.com
3. To activate the rule, select the **Activate Rule** check box.
   Important:
   To ensure the correctness of each rule that is configured, validate the rule using the Avaya ACE rule validation tool, and before activate it.
4. Click **Add**. Below figure is an example of Calling Party Translation Rules during testing this solution:
5. Click **Next** to configure called party translation rules.
6. Click **Submit** to save the rule configuration.

The Service Providers window appears. Select the Activate check box, ACE applies the rules to web service traffic that it processes. Verify the status of added service providers is "In Service":



4 Service Provider(s)

Type	Signaling	FQDN/IP Address	Port	Terminals	Addresses	Rules	Provider Status
Avaya Aura	TR87	135.10.[redacted]	4723	N/A	✎	✎	In Service
Avaya Aura	SIP	135.10[redacted]	5060	✎	✎	✎	In Service
Avaya CS 1000	TR87	135.10.[redacted]	5060	N/A	✎	✎	In Service
Avaya CS 1000	SIP	135.10.[redacted]	5060	N/A	✎	✎	In Service

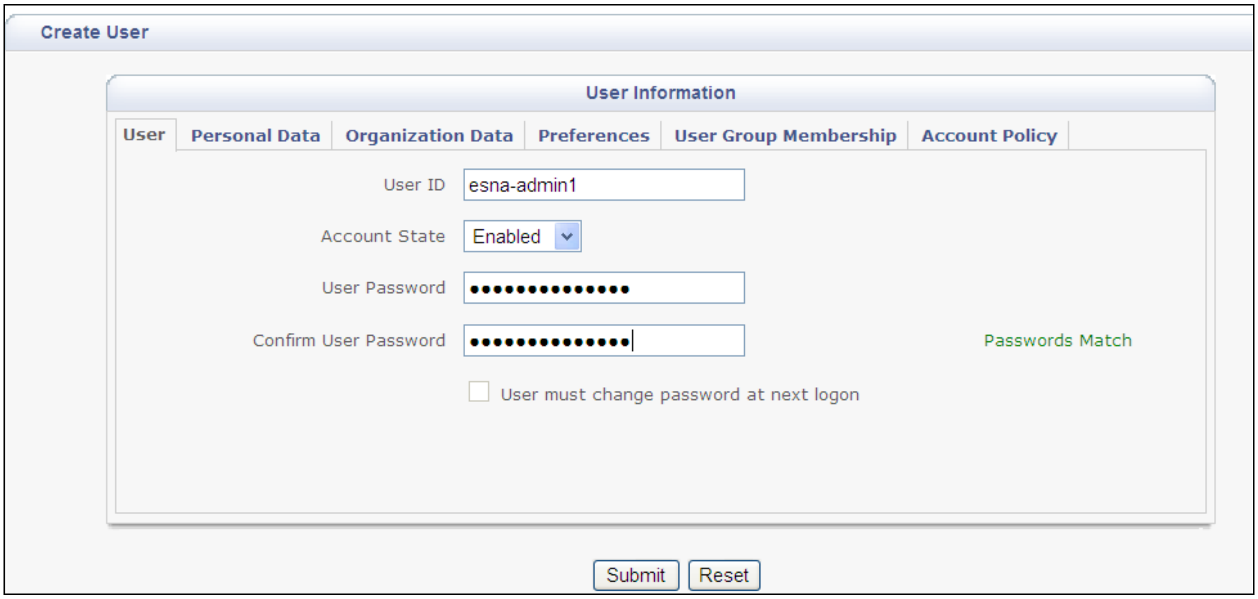
8.3. Add user

The web service client (application) ESNA Office-LinX – Avaya ACE Wizard is a configured user on Avaya ACE.

The web service client (application) belongs to a user group on Avaya ACE with a group type of **user** or higher, and with the appropriate access control rules configured for the Third Party Call Control (v2) service.

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

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


Create User

User Information

User ID esna-admin1

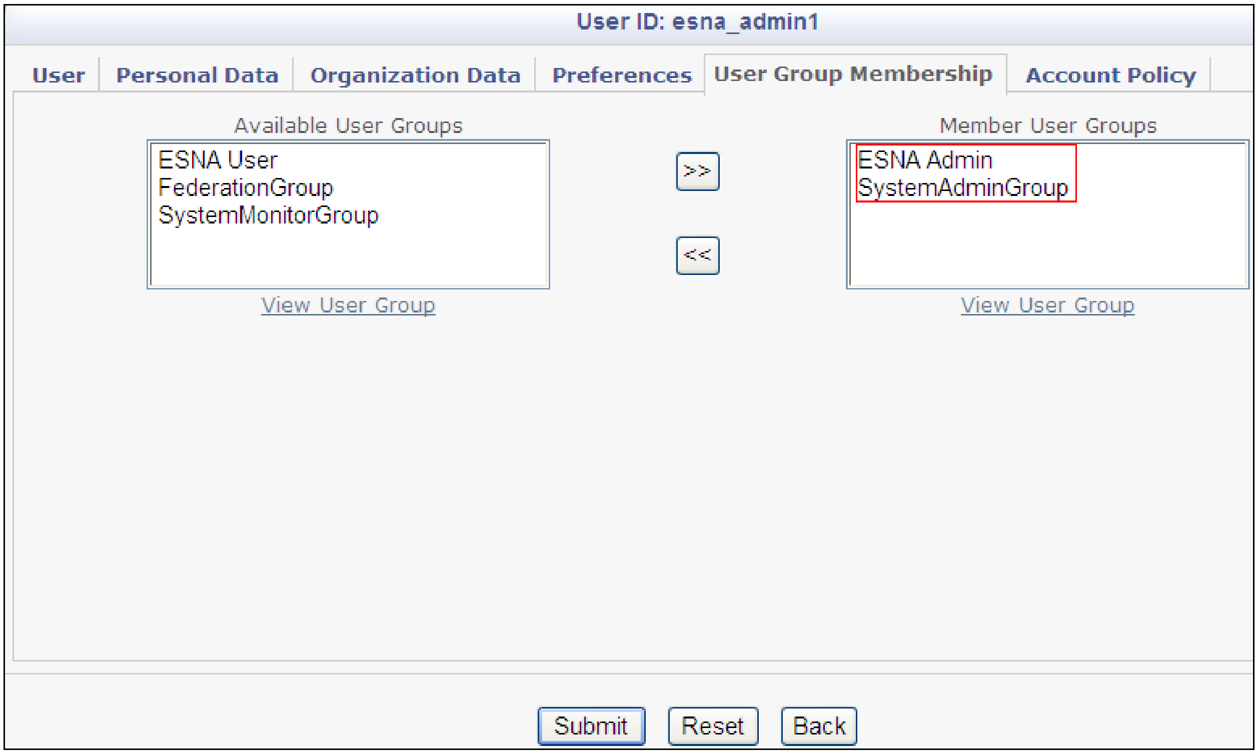
Account State Enabled

User Password ••••••••••••••

Confirm User Password •••••••••••••• Passwords Match

□ User must change password at next logon

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



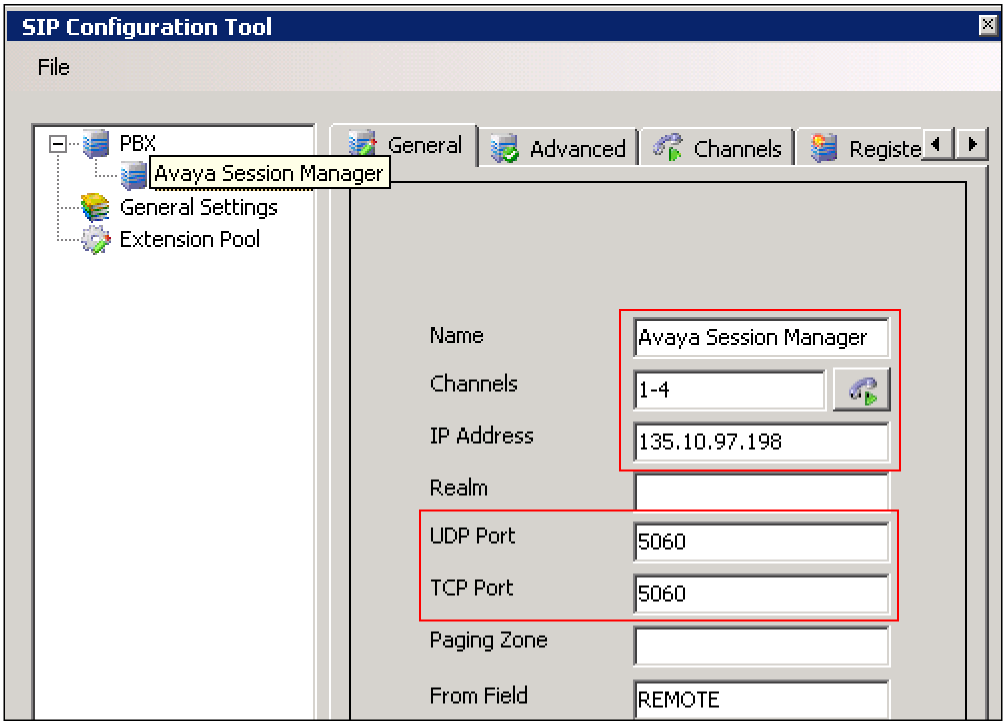
9. Configure the ESNA Telephony Office-LinX

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

9.1. Configure SIP Configuration Tool

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

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



Name: Avaya Session Manager

Channels: 1-4

IP Address: 135.10.97.198

Realm:

UDP Port: 5060

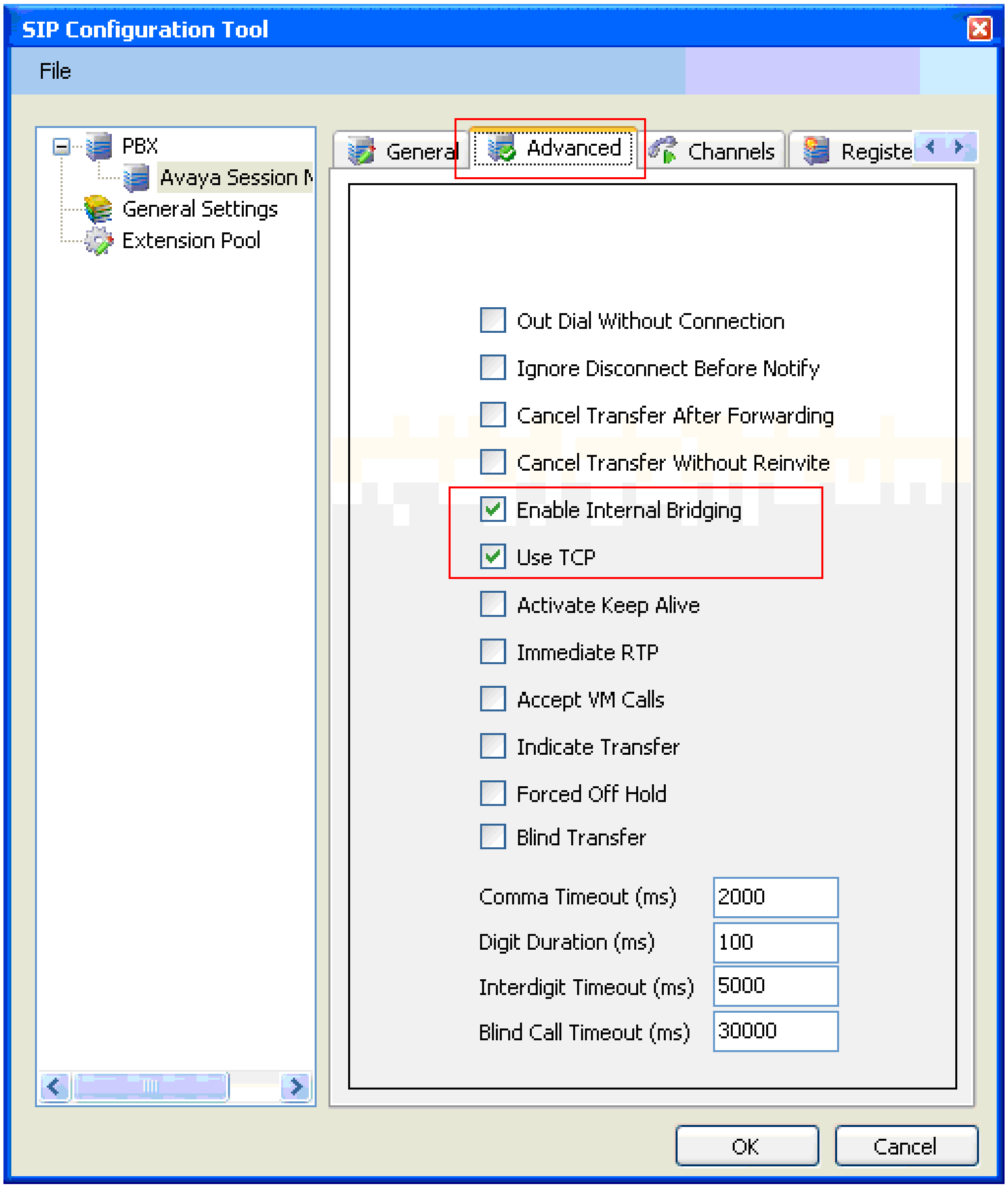
TCP Port: 5060

Paging Zone:

From Field: REMOTE

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

- Enable Internal Bridging
- Use TCP



☐ 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

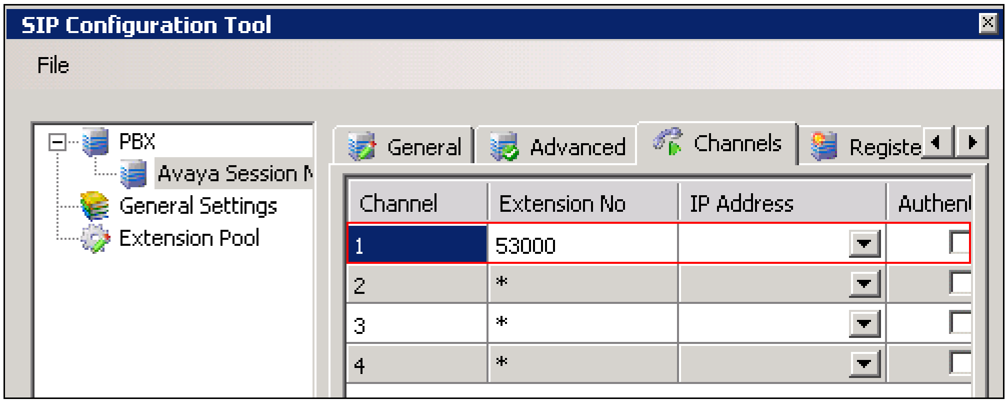
☐ Indicate Transfer

☐ Forced Off Hold

☐ Blind Transfer

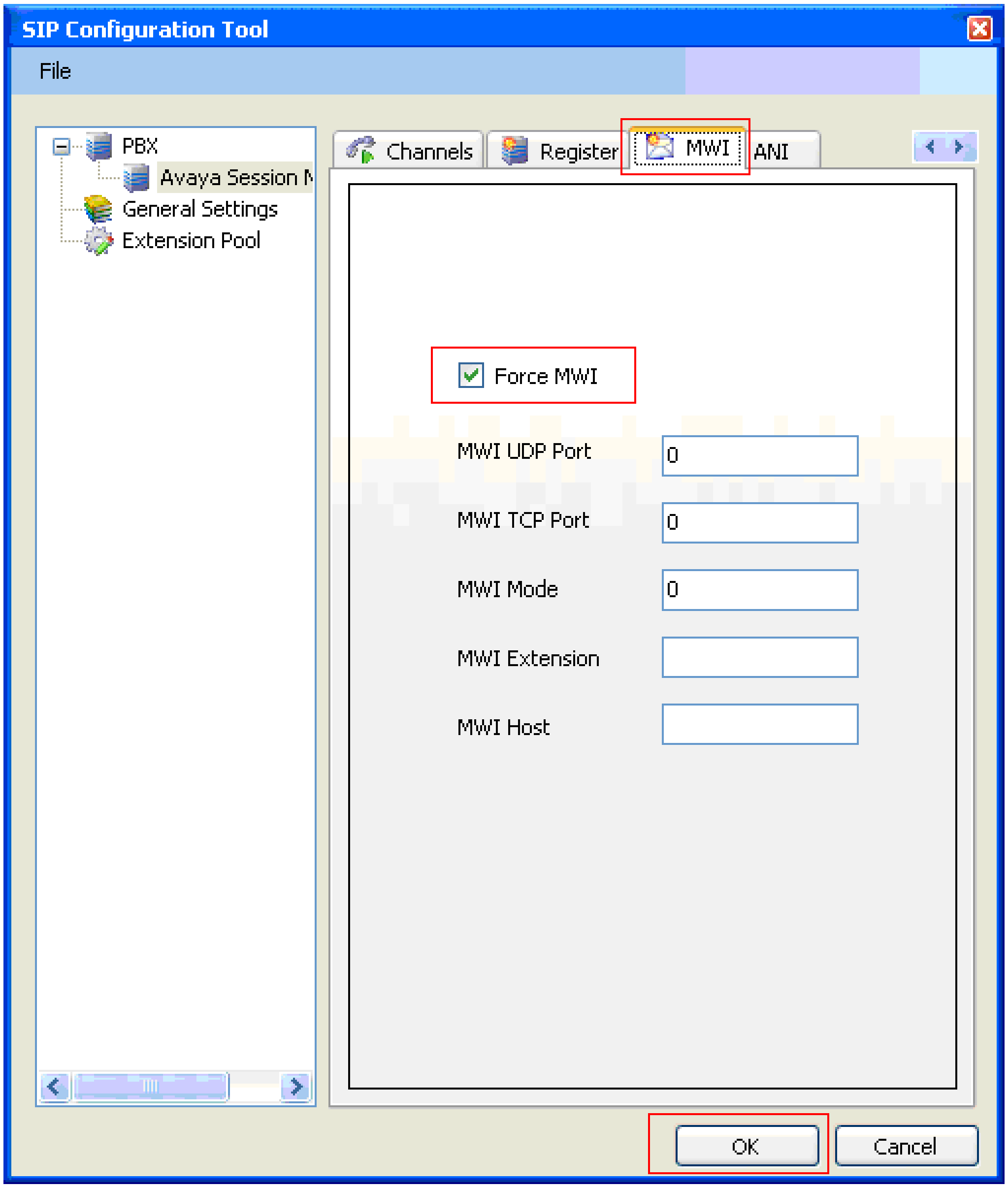
Comma Timeout (ms)	2000
Digit Duration (ms)	100
Interdigit Timeout (ms)	5000
Blind Call Timeout (ms)	30000

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



Channel	Extension No	IP Address	Authent
1	53000		☐
2	*		☐
3	*		☐
4	*		☐

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



☑ Force MWI

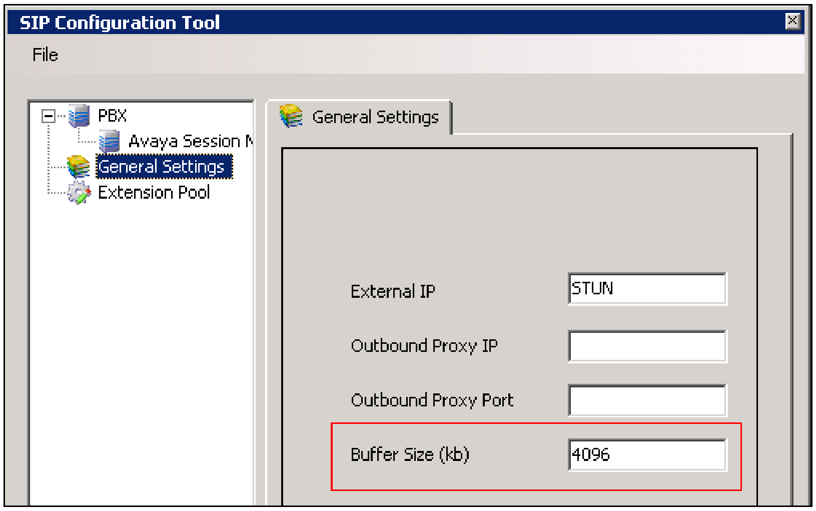
MWI UDP Port	0
MWI TCP Port	0
MWI Mode	0
MWI Extension	
MWI Host	

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.

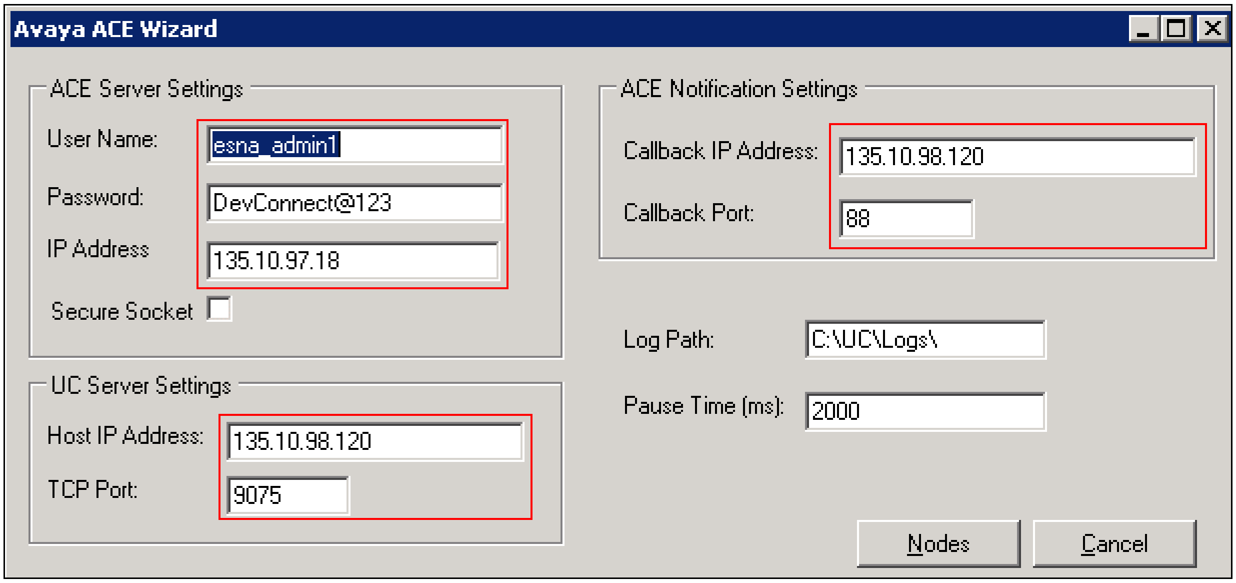
PBX – General Settings: Buffer Size (kb) =4096. This configuration allows Office-LinX can handle SIP message sent from Session Manager.



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 shown below:
User Name: Enter user that created on Avaya ACE in **Section** Error! Reference source not found.
Password: the password that entered in **Section** Error! Reference source not found.
IP Address: Avaya ACE IP address.



ACE Server Settings

User Name: esna_admin1

Password: DevConnect@123

IP Address 135.10.97.18

Secure Socket □

UC Server Settings

Host IP Address: 135.10.98.120

TCP Port: 9075

ACE Notification Settings

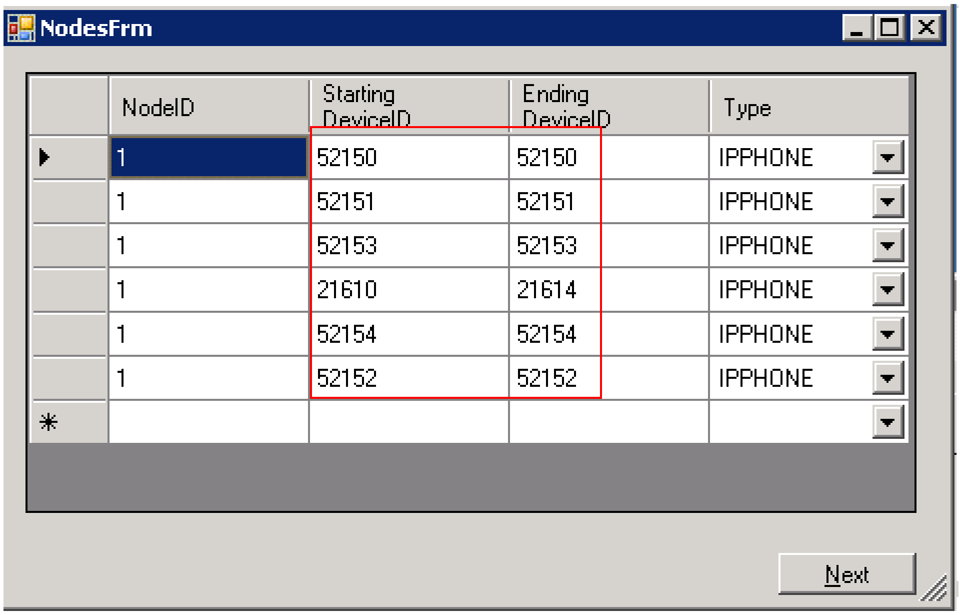
Callback IP Address: 135.10.98.120

Callback Port: 88

Log Path: C:\UC\Logs\

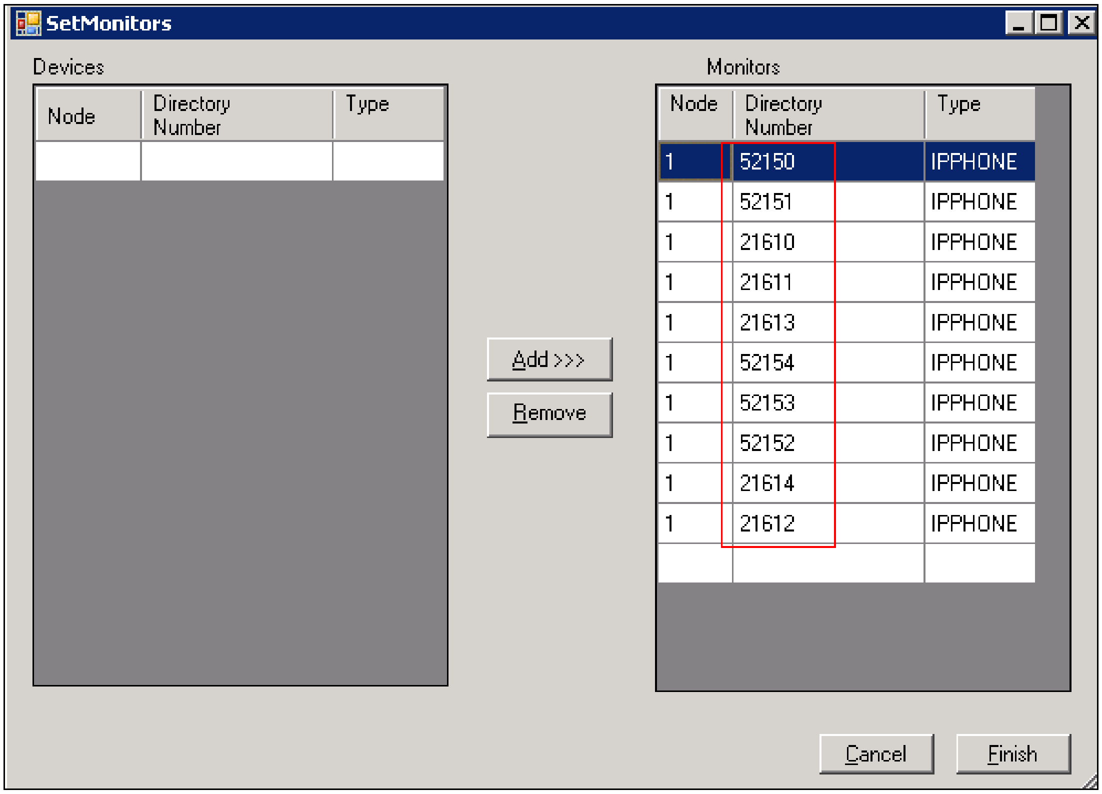
Pause Time (ms): 2000

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



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

Select the list of device on the left side and add it to the right window to start to monitor it. A user can remove the device from monitor list by highlighting to select the device and clicking remove.



Node	Directory Number	Type
1	52150	IPPHONE
1	52151	IPPHONE
1	21610	IPPHONE
1	21611	IPPHONE
1	21613	IPPHONE
1	52154	IPPHONE
1	52153	IPPHONE
1	52152	IPPHONE
1	21614	IPPHONE
1	21612	IPPHONE

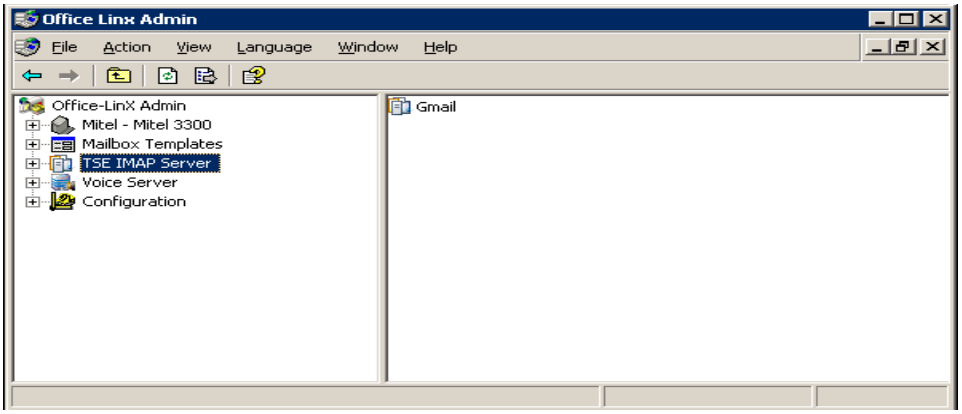
9.3. Message Synchronization

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

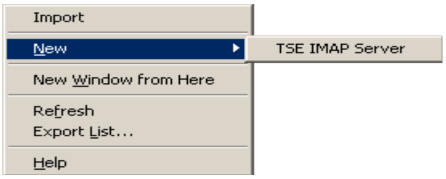
9.3.1. TSE IMAP Configuration

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

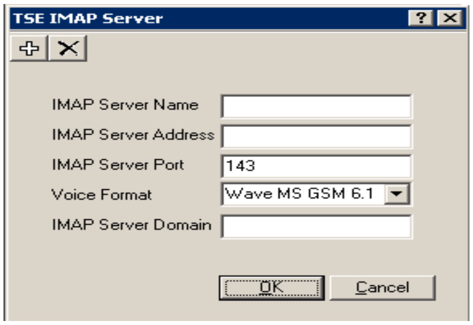
1. Locate and run **Office-LinX Admin** console.
2. From the left hand menu locate the **TSE IMAP Server**.



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



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



TSE IMAP Server

IMAP Server Name

IMAP Server Address

IMAP Server Port 143

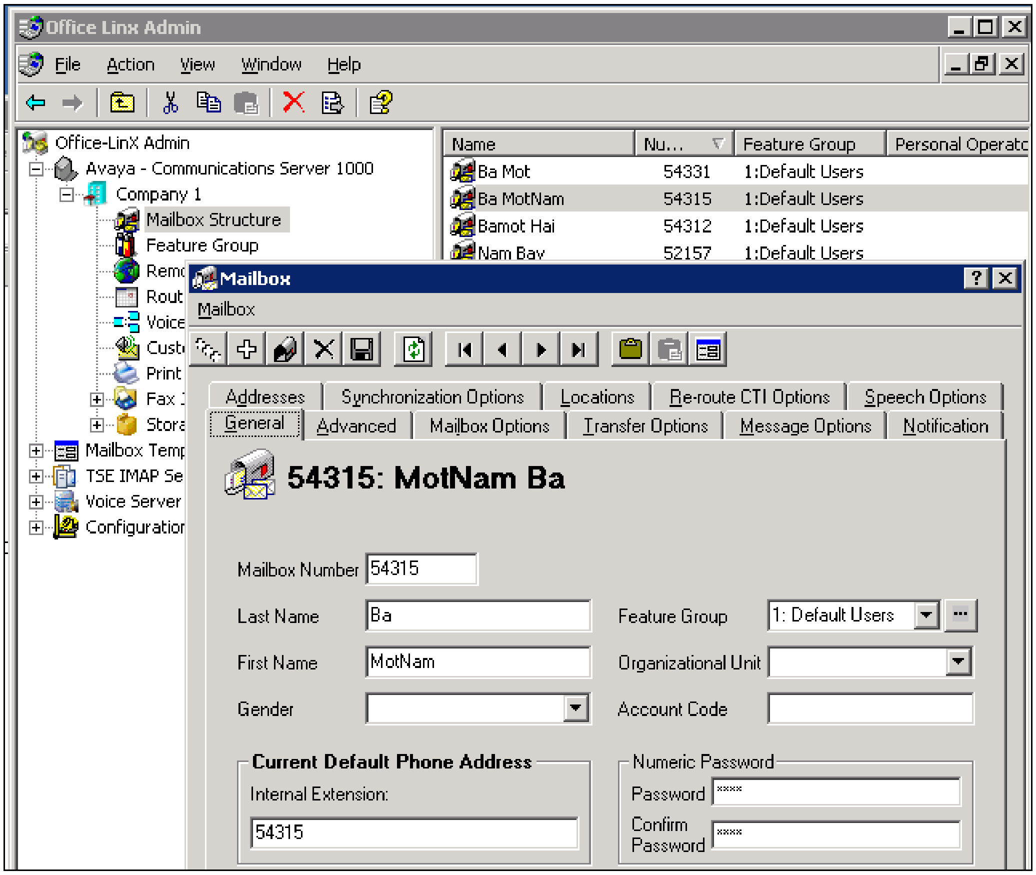
Voice Format Wave MS GSM 6.1

IMAP Server Domain

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

9.4. Configure user mailbox in Office-LinX Admin

Double click on Office-LinX icon to launch the application window.
Expand the **tree Office-LinX Admin → Avaya – Communication Server 1000 → Company 1** and highlight the **Mailbox Structure**. In the right panel right click on the window, select new to add new mailbox (Not shown).
Leave all the value as default and modify it if need. Example below is mail box for extension **54315**.



Name	Nu...	Feature Group	Personal Operatc
Ba Mot	54331	1:Default Users	
Ba MotNam	54315	1:Default Users	
Bamot Hai	54312	1:Default Users	
Nam Bay	52157	1:Default Users	

54315: MotNam Ba

Mailbox Number	54315		
Last Name	Ba	Feature Group	1: Default Users
First Name	MotNam	Organizational Unit	
Gender		Account Code	

Current Default Phone Address

Internal Extension: 54315

Numeric Password

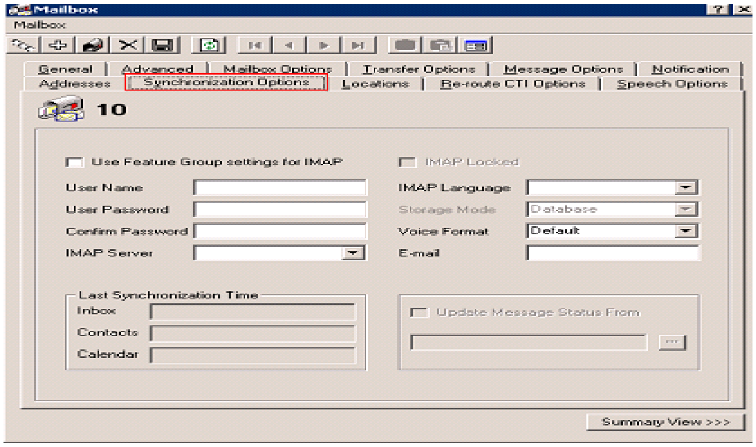
Password ****

Confirm Password ****

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

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

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



10

☐ Use Feature Group settings for IMAP

☐ IMAP Locked

User Name		IMAP Language	
User Password		Storage Mode	Database
Confirm Password		Voice Format	Default
IMAP Server		E-mail	

Last Synchronization Time

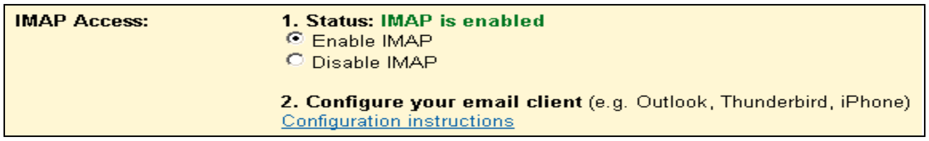
Inbox

Contacts

Calendar

☐ Update Message Status From

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



IMAP Access:

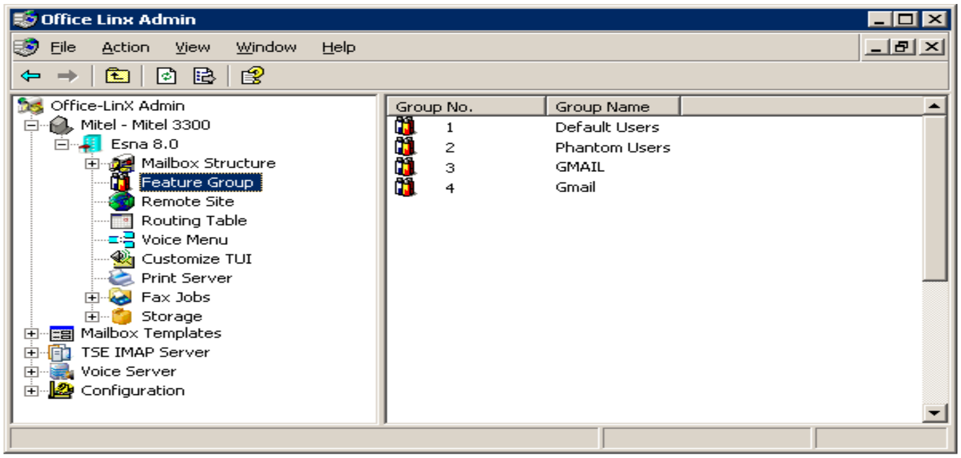
1. Status: IMAP is enabled
● Enable IMAP
○ Disable IMAP

2. Configure your email client (e.g. Outlook, Thunderbird, iPhone)
Configuration instructions

9.6. Feature Group

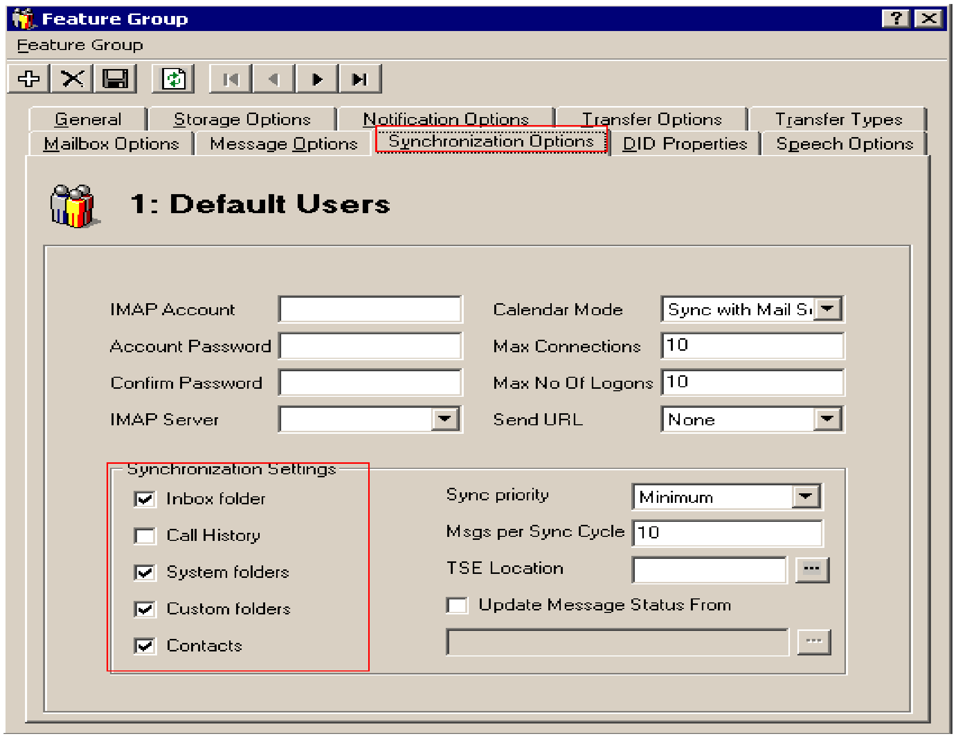
In order to ensure that there are no conflicts between Office-LinX and Gmail, please follow these steps to configure the Feature Group to synchronize the required information.

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



Group No.	Group Name
1	Default Users
2	Phantom Users
3	GMAIL
4	Gmail

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



1: Default Users

IMAP Account:
Account Password:
Confirm Password:
IMAP Server:
Calendar Mode: Sync with Mail S
Max Connections: 10
Max No Of Logons: 10
Send URL: None

Synchronization Settings

☑ Inbox folder
☐ Call History
☑ System folders
☑ Custom folders
☑ Contacts

Sync priority: Minimum
Msgs per Sync Cycle: 10
TSE Location:
☐ Update Message Status From

4. The Office-LinX mailbox is now fully synchronized with the Gmail IMAP account.

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

9.7. Synchronization through OAuth (superuser)

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

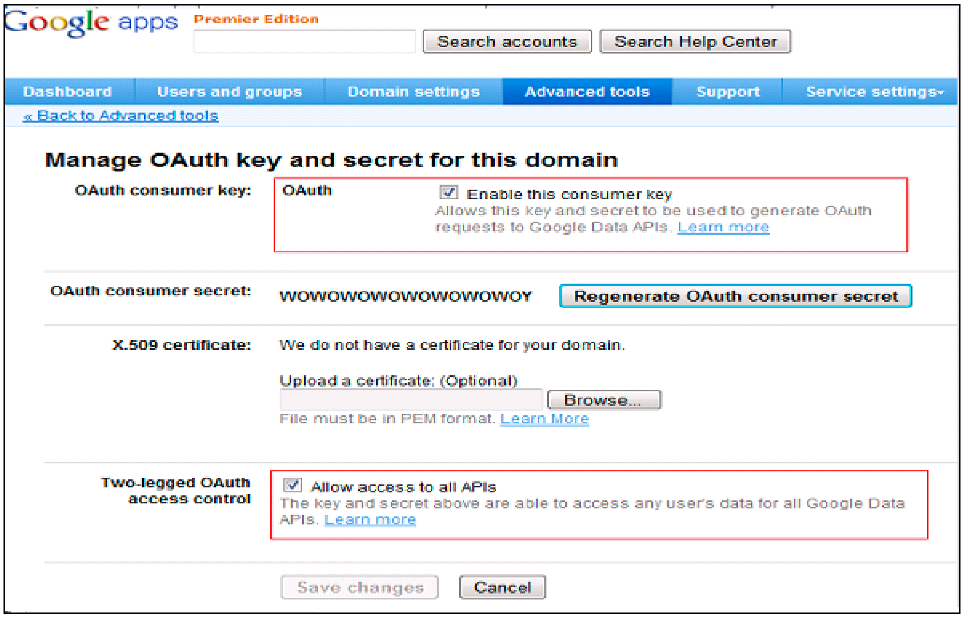
9.7.1. Configuring OAuth

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

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

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

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



Manage OAuth key and secret for this domain

OAuth consumer key: OAuth

☑ Enable this consumer key
Allows this key and secret to be used to generate OAuth requests to Google Data APIs. Learn more

OAuth consumer secret: WOWOWOWOWOWOWOWOWOY

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

Upload a certificate: (Optional)

File must be in PEM format. Learn More

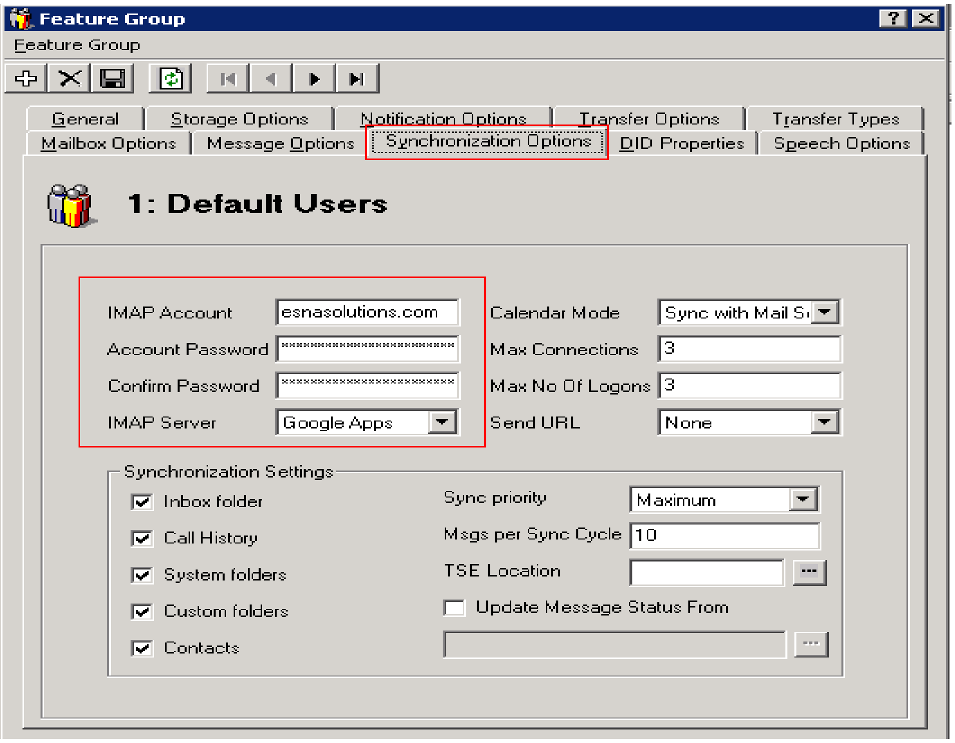
Two-legged OAuth access control

☑ Allow access to all APIs
The key and secret above are able to access any user's data for all Google Data APIs. Learn more

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

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

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



1: Default Users

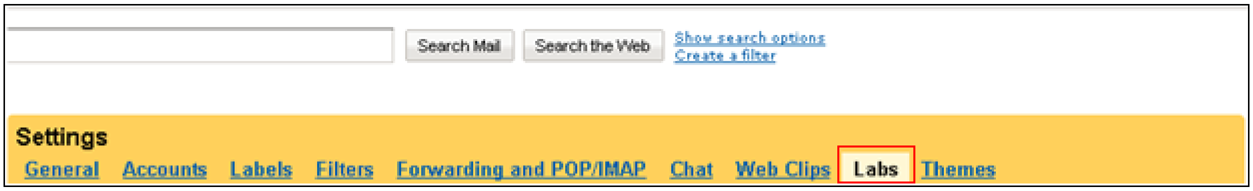
IMAP Account	esnasolutions.com	Calendar Mode	Sync with Mail S
Account Password	************************	Max Connections	3
Confirm Password	************************	Max No Of Logons	3
IMAP Server	Google Apps	Send URL	None

Synchronization Settings

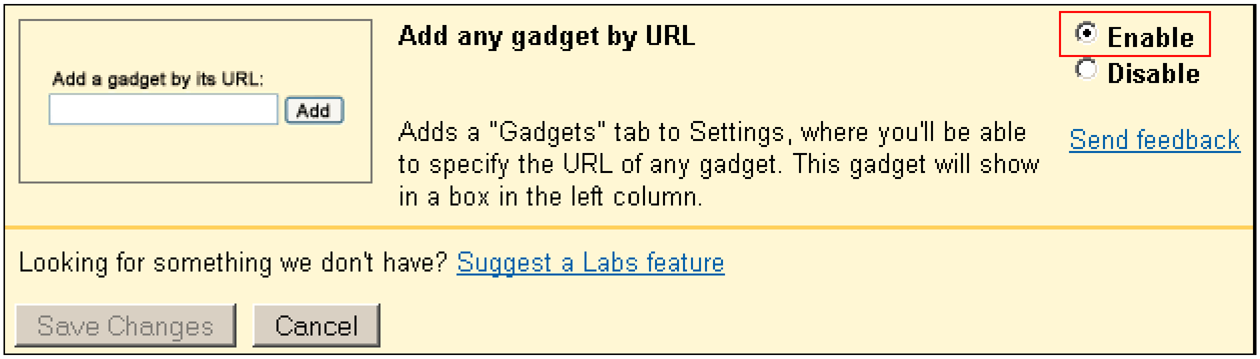
☑ Inbox folder	Sync priority	Maximum
☑ Call History	Msgs per Sync Cycle	10
☑ System folders	TSE Location	
☑ Custom folders	□ Update Message Status From	
☑ Contacts		

9.8. Install and Configure UC Client Google Gadget on Gmail

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



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



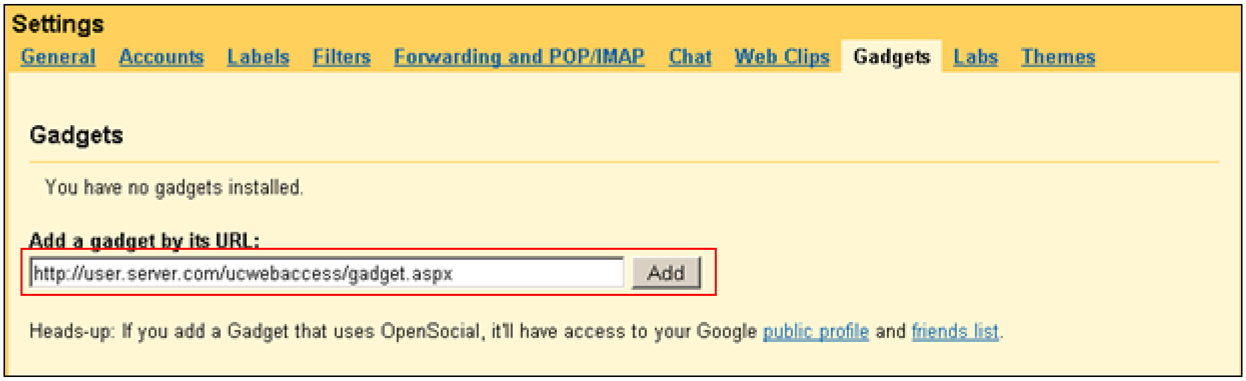
Add any gadget by URL

● Enable
○ Disable

Adds a "Gadgets" tab to Settings, where you'll be able to specify the URL of any gadget. This gadget will show in a box in the left column.

Looking for something we don't have? Suggest a Labs feature

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



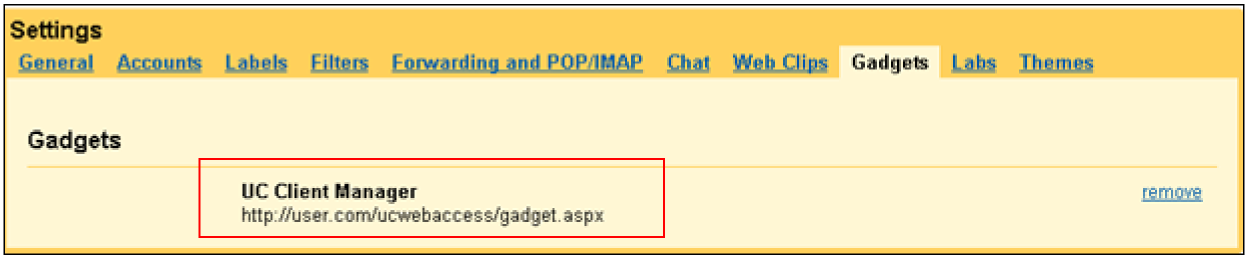
Gadgets

You have no gadgets installed.

Add a gadget by its URL: http://user.server.com/ucwebaccess/gadget.aspx

Heads-up: If you add a Gadget that uses OpenSocial, it'll have access to your Google public profile and friends list.

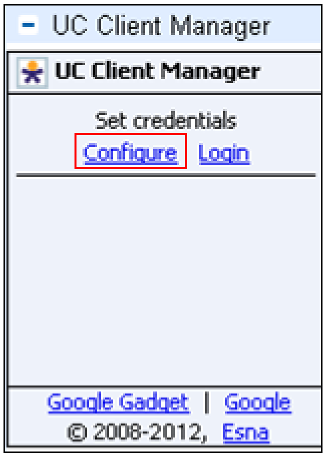
Replace USER.YOUR_SERVER.COM with the address of your own UC server. When ready, click the **Add** button.
The UC Client Manager gadget is now listed on the **Gadgets** tab.



Gadgets

UC Client Manager
http://user.com/ucwebaccess/gadget.aspx

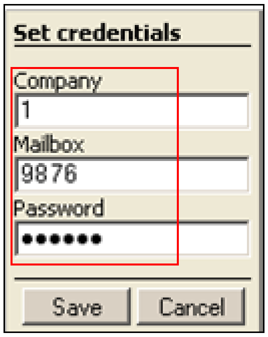
The UC Client Manager Gadget is now available on the Gmail interface.



Set credentials

© 2008-2012, Esna

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



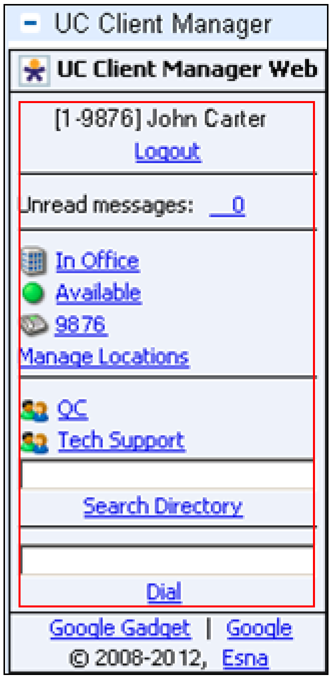
Set credentials

Company: 1

Mailbox: 9876

Password: ••••••

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



UC Client Manager

UC Client Manager Web

[1-9876] John Carter

Unread messages: 0

10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Server 1000E Release 7.5, Session Manager, Avaya ACE, Avaya Aura® Messaging and ESNA Office-LinX – UC Client Manager application.

10.1. Verify Avaya Communication Server 1000 Release 7.5

After the telephone sets have been properly configured on Communication Server 1000E, 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 1000E 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 **5.5.1**.

```
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

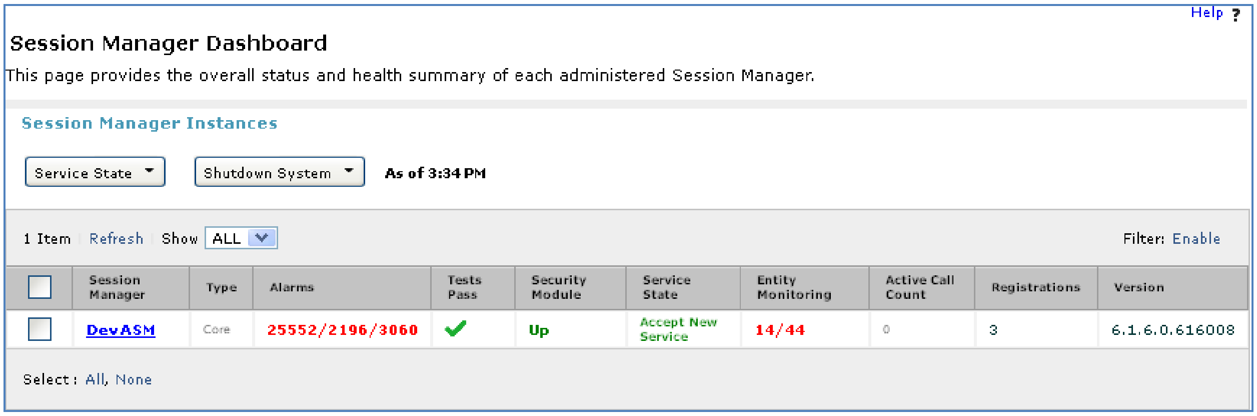
10.2.1. Verify Avaya Aura® Session Manager is Operational

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

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

1 Item Refresh Show ALL ▾ Filter: Enable

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

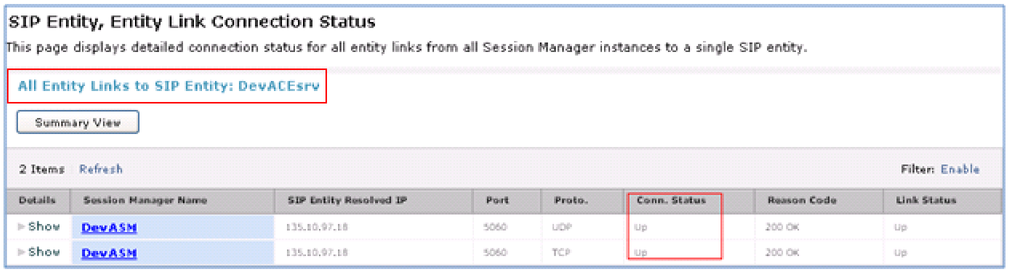
Select : All, None

10.2.2. Verify SIP Entity Link Status

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

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

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



SIP Entity, Entity Link Connection Status

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

All Entity Links to SIP Entity: DevACEsrv

Summary View

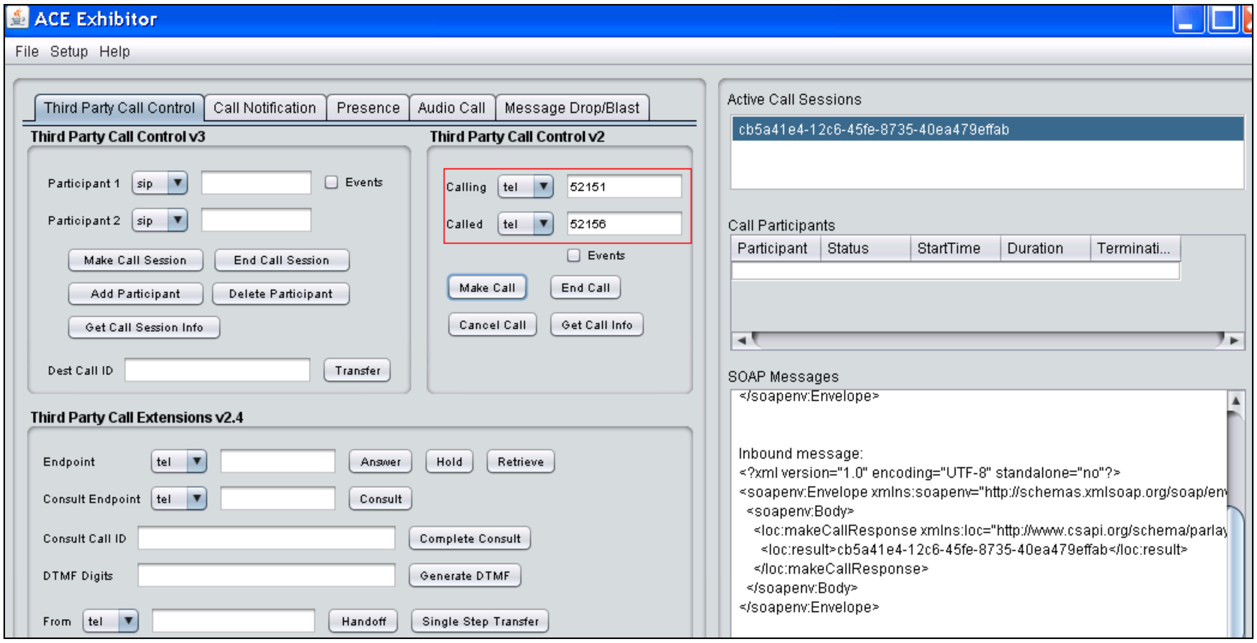
2 Items Refresh Filter: Enable

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

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

10.3. Verify make call using ACE_EXHIBITOR or SOAP UI software

Perform call using ACE_EXHIBITOR or SOAP UI software, below is an example of using ACE Exhibitor: make a call from 52151 to 52156. Call is made successfully.



Participant 1: sip
Participant 2: sip
Events: □

Calling: tel 52151
Called: tel 52156
Events: □

Endpoint: tel
Consult Endpoint: tel
From: tel

Active Call Sessions: cb5a41e4-12c6-45fe-8735-40ea479effab

Participant	Status	StartTime	Duration	Terminati...

SOAP Messages

```
</soapenv:Envelope>


Inbound message:
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/en
  <soapenv:Body>
    <loc:makeCallResponse xmlns:loc="http://www.csapi.org/schema/parlay
      <loc:result>cb5a41e4-12c6-45fe-8735-40ea479effab</loc:result>
    </loc:makeCallResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

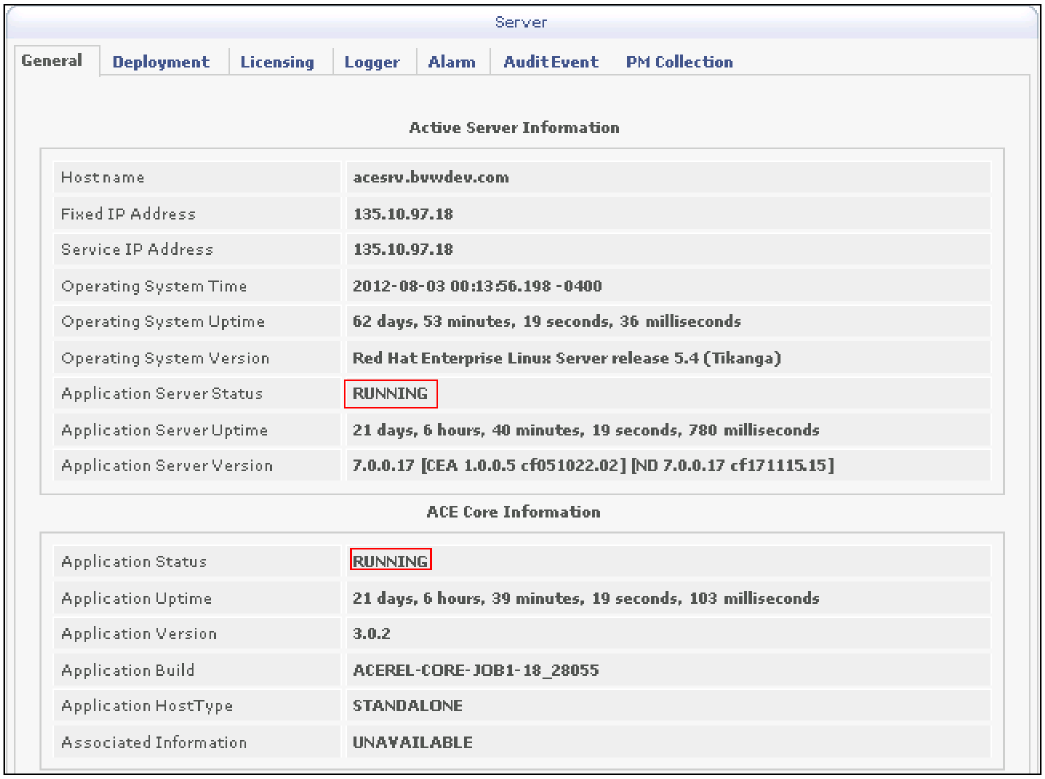
10.4. Verify Avaya ACE

10.4.1. Verify Service Provider status in Avaya ACE

See the end of **Section** 8.1 Add service provider in Avaya ACE; to see the figure showing that all service providers configured have status “In Service”.

10.4.2. Verify Avaya ACE Server status

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

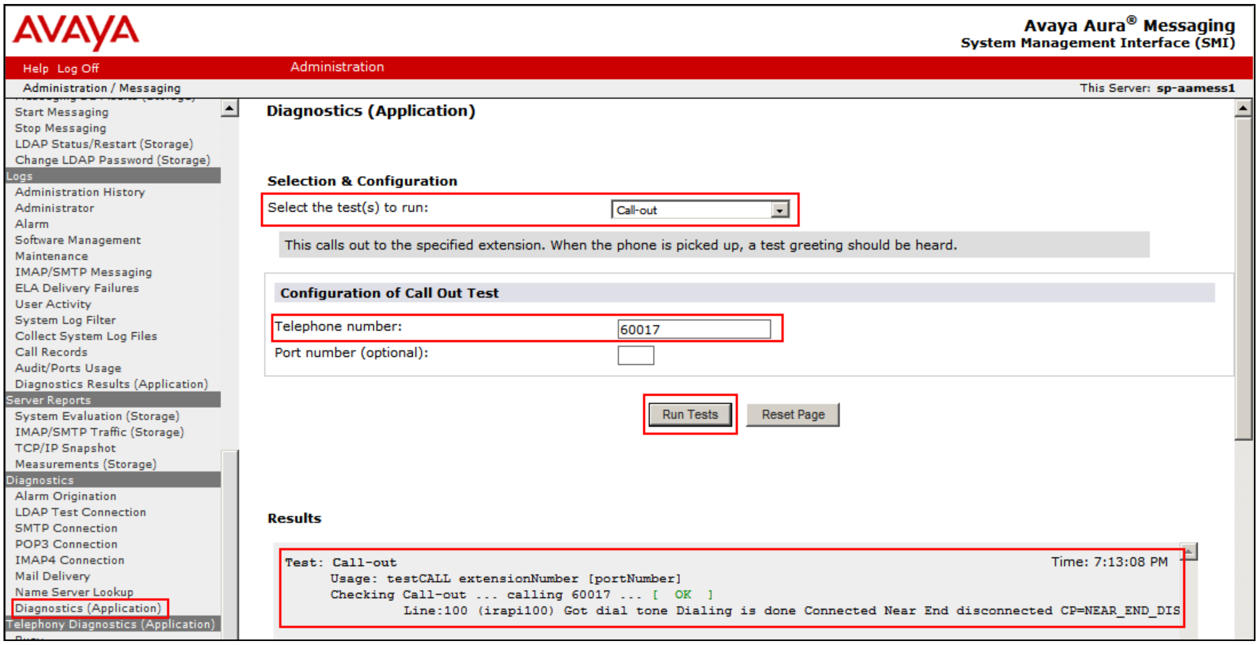
10.5. Verify Avaya Aura® Messaging

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

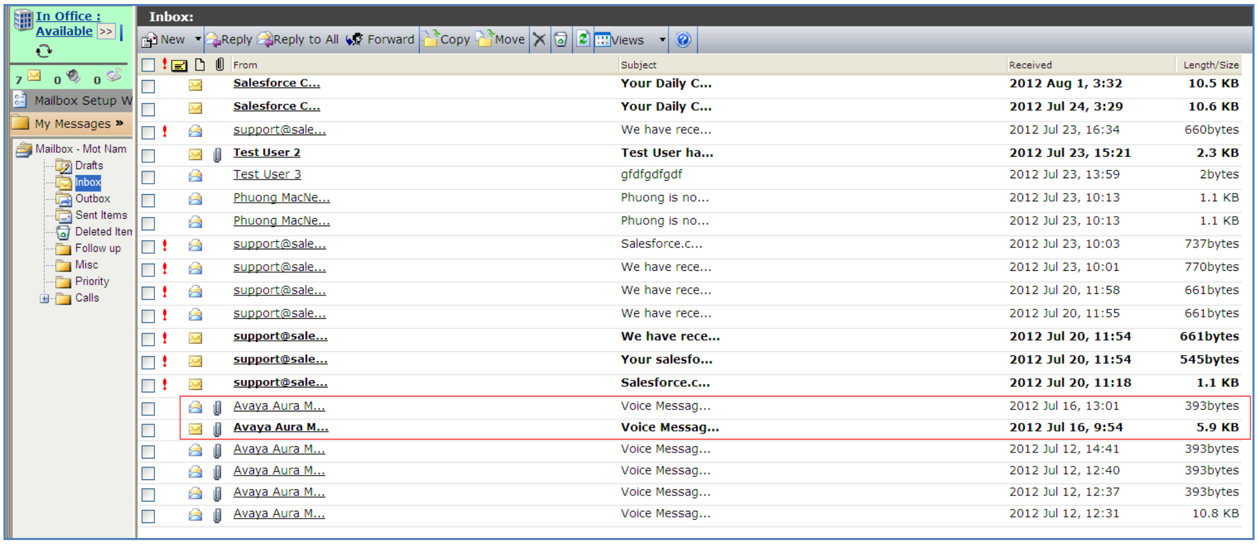
Port number (optional):

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 on ESNA Web Client or Google Mail account

Make a call from a UC Client calls another device verify that the call covers to Messaging upon no answer. Leave a voice message. Verify that the MWI light of the called phone turns on. Log on ESNA Web client/ Google mail account called user verify that user got the message from Avaya Aura® Messaging and able to listen to the voice message. Verify that the MWI light turns off. (Notes: At this version of Office-LinX 8.5 SP2, when messages are read, Office-LinX should attempt to extinguish MWI via SIP if possible. This will not reflect actual message status on Avaya Aura® Messaging). Example below show user has incoming AAM voice message in the mailbox.



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

10.6. Verify ESNA Office-LinX server and UC Client Google gadget.

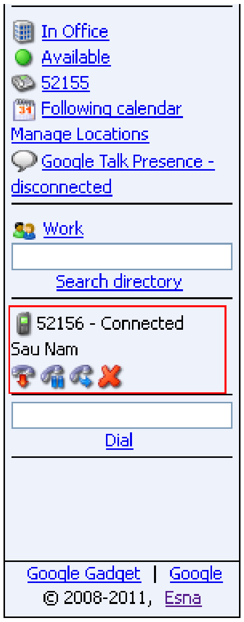
10.6.1. Verify the log file UCServer of ESNA Office-LinX.

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

```
11:41:07.390-[+][00000004][F:Init]client: 135.10.98.120Port : 88
11:41:07.671-[+][00000004][F:Init]VirtualAddr: http://135.10.98.120:88/
11:41:07.796-[+][0000000C][F:EventHandler]Start listening
11:41:07.859-[+][0000000C][F:EventHandler]assembly location
C:\WINDOWS\system32\UCACEServer.dll
11:41:07.890-[+][00000004][F:Initialize]Wait for HttpListener to start listening
11:41:08.437-[+][00000004][F:Initialize]Adding Devices to DeviceList
11:41:08.437-[+][00000008][F:Initialize]Exit NoOfDevices: 11
11:41:08.500-[+][00000004][F:Initialize]HttpListener is listening
11:41:10.125-[+][00000004][F:Initialize]Starting EventThread
11:41:10.437-[-][00000003][F:ESACEAgent:EventHandlerproc]Entry:
11:41:10.500-[+][00000004][F:Initialize]Strting Monitor
11:41:15.015-
[+][00000004][F:CallNotification:StartNotification]CallNotification(Called) is started
at http://135.10.98.120:88/ACENotificationServer
11:41:15.140-
[+][00000004][F:CallNotification:StartNotification]CallNotification(Calling)is started
at http://135.10.98.120:88/ACENotificationServer
11:41:15.140-[+][00000004][F:StartMonitor]After starting Call notification :
11:42:25.187-[-][0000000A][F:MakeCall]Entry Dest: 52156
11:42:25.187-[+][0000000A][F:MakeCall]DestBuffer: 52156
11:42:25.218-[+][0000000A][F:CallControl.MakeCall]Calling: tel:52150 Called: tel:52156
11:42:25.234-[+][00000010][F:CallProgressCallBack]Entry Dest:
11:42:25.437-[+][00000004][F:makeCallCompleted]Result: 3b21cc7a-4aee-4b74-b007-
ca5e35f75c2e
11:42:25.437-[+][00000004][F:UpdateCall] >>>>> Key: 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 UC Client Google Gadget in the Gmail

User login ESNA Gmail account as created in **section 9.4.** User able to enter the number and click Dial. The devices are ringing. Called pick up the device. The 2 way voice path is established.


In Office
Available
52155
Following calendar
Manage Locations
Google Talk Presence - disconnected
Work
Search directory
52156 - Connected
Sau Nam
Dial
Google Gadget | Google
© 2008-2011, Esna

11. Conclusion

Interoperability testing of Avaya ACE, Avaya Aura® Messaging, and Avaya Communication Server 1000 Release 7.5 with Office-LinX 8.5 SP2 – UC Client Google gadget was successful. Observations are noted in **Section 2.2**.

12. Additional References

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

1. *Administering Avaya Aura® Session Manager*, August 2010, Release 6.0, Document Number 03-603324.
2. *Administering Avaya Aura® System Manager*, June 2010, Release 6.0.
3. Avaya Agile Communication Environment Avaya Aura® Integration Release 3.0 NN10850 03.03 March 2012
4. *SIP Line Fundamentals Avaya Communication Server 1000* (NN43001-508).
5. Avaya Agile Communication Environment™ Communication Server 1000 Integration - Release 3.0.0 NN10850-023, 06.03 December 2011

The following documents were provided by ESNA.

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

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.