Avaya Solution & Interoperability Test Lab

Application Notes for Seoul Commtech adva MRS with Avaya Communication Manager and Avaya Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the Seoul Commtech adva MRS Version 2006.7.1.1 to monitor and record calls placed to and from Avaya IP and Digital telephones, Avaya IP Softphones, and agents on Avaya Communication Manager Release 3.1.2. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a compliance-tested configuration comprised of Avaya Communication Manager, Avaya Application Enablement Services (AES) and Seoul Commtech adva MRS.

The adva MRS is an IP-based recording system which records, plays, evaluates, manages and captures screen images and voice conversations. It provides corporations as well as customer service centers with optimized functions to collect the history of communications with customers.

The four types of users utilizing the system are:

- Agents – from which communication contents are recorded through their interactions with customers
- Supervisors – who manage agents
- Evaluators – who listen and evaluate agents' communication contents
- Administrators – who monitor and manage the system

The main features are as follows:

- Customized service
    - Integration with Customer Relationship Management (CRM) systems
    - Web interface for easy access and usage
    - Customizable statistics
    - Agent free-sitting supported
    - On-demand recording supported
- Intelligent system
    - Integrated with customer information through the Computer Telephony Interface (CTI) link
    - Agent Coaching functionality
- Modularized System Design
    - Easy administration
    - Scalable to handle large call recording volume
- Real time monitoring using the Web interface
    - Agents' PC screen and voice contents
    - System status

Figure 1 illustrates a sample configuration consisting of an Avaya S8500B Media Server, an Avaya G650 Media Gateway, an Avaya AES Server, Avaya IP and Digital telephones, an agent PC running Avaya IP Softphone, two agent PCs without Avaya IP Softphone, and two Windows 2003 servers running Seoul Commtech adva MRS Server software. The agent PCs were also installed with the Seoul Commtech adva MRS Screen Recording Client for screen recording. The

adva MRS VRC Server registers IP station endpoints with Avaya Communication Manager via Avaya Application Enablement Services using the Device and Media Control (formerly known as Communication Manager API or CMAPI) Service for voice recording. Each IP station recording endpoint is configured to Service-Observe an agent extension that is required to be recorded. The adva MRS CLC Server monitors the agent extension using the TSAPI Service to retrieve call related information. Both the Device and Media Control and TSAPI services are provided by the Avaya AES Server.

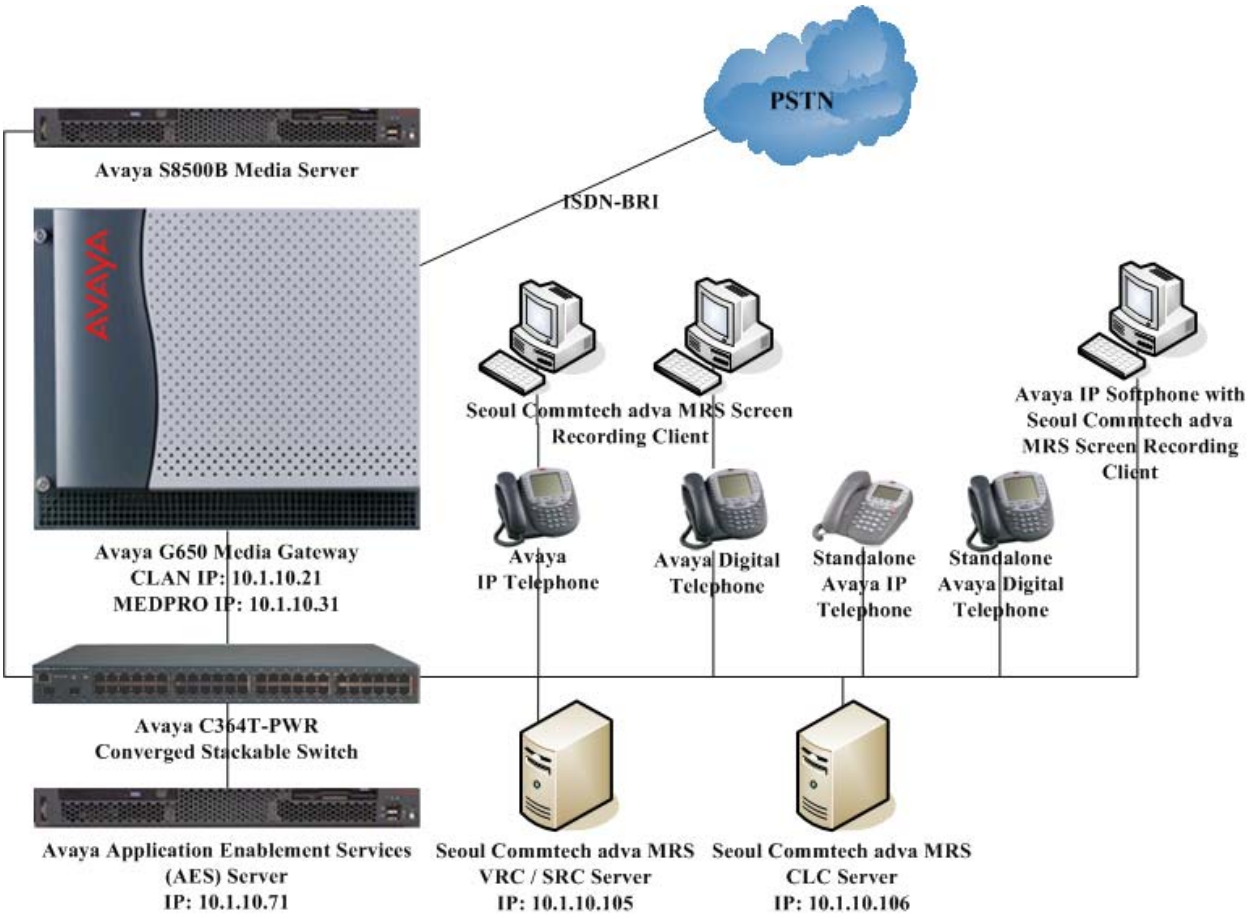


Figure 1: Sample Configuration

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8500B Media Server	3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway • TN2312BP IP Server Interface • TN799DP C-LAN Interface • TN2302AP IP Media Processor	- HW07, FW031 HW01, FW017 HW20, FW111
Avaya Application Enablement Services	3.0.1 (r3-0-0-build-50-1-0)
Avaya 4600 Series IP Telephones	2.4 (4610SW) 2.4 (4621SW) 2.5 (4625SW)
Avaya 2400 Series Digital Telephone	-
Avaya IP Softphone	5.2 Service Pack 1
Avaya C364T-PWR Converged Stackable Switch	4.3.12
Seoul Commtech adva MRS (model number SEP-MRS100AP/AV)	Version 2006.7.1.1
Apache Tomcat	5.5.17
Microsoft SQL Server	2000 with Service Pack 4

3. Configure Avaya Communication Manager

This section describes the steps for configuring Computer Telephony Integration (CTI) links, Hunt/Skill Groups, Vectors, Vector Directory Numbers (VDNs), Agents, Feature Access Codes, IP station recording endpoints and voice codecs on Avaya Communication Manager. The steps are performed through the System Access Terminal (SAT) interface.

3.1. AES Link between Avaya Communication Manager and Avaya Application Enablement Services Server

The Avaya Application Enablement Services (AES) server forwards CTI requests, responses, and events between the Seoul Commtech adva MRS CLC Server and Avaya Communication Manager. The AES server communicates with Avaya Communication Manager over an AES link. Within the AES link, a CTI link is configured to provide TSAPI service to the adva MRS CLC Server. The following steps demonstrate the configuration of the Avaya Communication Manager side of the AES and CTI link. See Section 4 for the details of configuring the AES side of the AES and CTI link.

Step	Description
1.	Enter the **display system-parameters customer-options** command. On Page 3, verify that **Computer Telephony Adjunct Links** is set to ***y***. If not, contact an authorized Avaya account representative to obtain the license.

```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? n           Audible Message Waiting? n
        Access Security Gateway (ASG)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? n Backup Cluster Automatic Takeover? n
 A/D Grp/Sys List Dialing Start at 01? n                         CAS Branch? n
Answer Supervision by Call Classifier? n                           CAS Main? n
                                  ARS? y                  Change COR by FAC? n
                  ARS/AAR Partitioning? y  Computer Telephony Adjunct Links? y
           ARS/AAR Dialing without FAC? n   Cvg Of Calls Redirected Off-net? n
           ASAI Link Core Capabilities? n                       DCS (Basic)? n
           ASAI Link Plus Capabilities? n                  DCS Call Coverage? n
       Async. Transfer Mode (ATM) PNC? n                 DCS with Rerouting? n
  Async. Transfer Mode (ATM) Trunking? n
              ATM WAN Spare Processor? n    Digital Loss Plan Modification? n
                                  ATMS? n                            DS1 MSP? n
                   Attendant Vectoring? n             DS1 Echo Cancellation? n
```

2.	Enter the **add cti-link m** command, where m is a number between 1 and 16, inclusive. Enter an **Extension** valid under the provisioned dial plan in Avaya Communication Manager, set **Type** to ***ADJ-IP*** and assign a descriptive **Name** to the CTI link.

```
add cti-link 1                                                  Page   1 of   2
                                     CTI LINK
 CTI Link: 1
Extension: 19001
     Type: ADJ-IP
                                                                      COR: 1
     Name: AES TSAPI Svc
```

3.	Enter the **display node-names ip** command. Note the node name and IP address of the CLAN board. In the compliance-tested configuration, one C-LAN board (**s8500-clan1**) was used for H.323 endpoint (Avaya IP Telephones and IP Softphone, and AES Device and Media Control API stations) registration. The same C-LAN board was also enabled with Application Enablement Services to serve the AES link (see **Step 4**).

Step	Description

	`display node-names ip`
	`IP NODE NAMES`
	`Name  IP Address`
	`aes1  10 .1  .10 .71`
	`default  0  .0  .0  .0`
	`procr  10 .1  .10 .10`
	`s8500  10 .1  .10 .10`
	`s8500-clan1  10 .1  .10 .21`
	`s8500-medpro1  10 .1  .10 .31`

4.	Enter the **change ip-services** command. On Page 1, configure the C-LAN board for Application Enablement Services as follows: • **Service Type** – set to ***AESVCS*** • **Enabled** – set to ***y*** • **Local Node** – set to the node name ***s8500-clan1*** (See **Step 3**) • **Local Port** – set to ***8765***

	`change ip-services  Page 1 of 3`
	`IP SERVICES`
	`Service Type  Enabled  Local Node  Local Port  Remote Node  Remote Port`
	`AESVCS  y  s8500-clan1  8765`

	On Page 3 of the **ip-services** form, enter the hostname of the AES server for **AE Services Server** and an alphanumeric password for **Password**, and set **Enabled** to ***y***. The same password will be configured on the AES server in **Section 4.4 Step 2**.

	`change ip-services  Page 3 of 3`
	`AE Services Administration`
	`Server ID  AE Services Server  Password  Enabled  Status`
	`1:  aes1  abcdef123456  y``  idle`
	`2:`

3.2. Agent Hunt/Skill Groups, Agent Logins, and Call Vectoring

The following steps describe the configuration of hunt/skill groups, agent logins, and call vectoring in Avaya Communication Manager.

Step	Description
1.	Enter the **display system-parameters customer-options** command. On Page 6, verify that **ACD** and **Vectoring (Basic)** are set to ***y***. If not, contact an authorized Avaya account representative to obtain these licenses. **Expert Agent Selection** was enabled for the testing, but the feature is not mandatory.

Step	Description

	`display system-parameters customer-options  Page  6 of  11`
	`CALL CENTER OPTIONAL FEATURES`
	
	`Call Center Release: 3.0`
	
	`ACD? y` `Reason Codes? y`
	`BCMS (Basic)? y  Service Level Maximizer? n`
	`BCMS/VuStats Service Level? n  Service Observing (Basic)? y`
	`BSR Local Treatment for IP & ISDN? n  Service Observing (Remote/By FAC)? y`
	`Business Advocate? n  Service Observing (VDNs)? y`
	`Call Work Codes? y  Timed ACW? y`
	`DTMF Feedback Signals For VRU? n` **`Vectoring (Basic)? y`**
	`Dynamic Advocate? n  Vectoring (Prompting)? y`
	`Expert Agent Selection (EAS)? y` `Vectoring (G3V4 Enhanced)? y`
	`EAS-PHD? y  Vectoring (3.0 Enhanced)? y`
	`Forced ACD Calls? n  Vectoring (ANI/II-Digits Routing)? y`
	`Least Occupied Agent? y  Vectoring (G3V4 Advanced Routing)? y`
	`Lookahead Interflow (LAI)? y  Vectoring (CINFO)? y`
	`Multiple Call Handling (On Request)? n  Vectoring (Best Service Routing)? y`
	`Multiple Call Handling (Forced)? n  Vectoring (Holidays)? y`
	`PASTE (Display PBX Data on Phone)? y  Vectoring (Variables)? y`
	`(NOTE: You must logoff & login to effect the permission changes.)`

2.	Enter the **add hunt-group n** command, where n is an unused hunt group number. On Page 1, assign a descriptive **Group Name** and **Group Extension** valid under the provisioned dial plan and set **ACD**, **Queue**, and **Vector** to ***y***. When **ACD** is enabled, hunt group members serve as ACD agents and must log in to receive ACD split/skill calls. When **Queue** is enabled, calls to the hunt group will be queued when no agents are available. When **Vector** is enabled, the hunt group will be vector controlled.

	`add hunt-group 101  Page  1 of  3`
	`HUNT GROUP`
	
	`Group Number: 101` **`ACD? y`**
	`Group Name: Agents` **`Queue? y`**
	`Group Extension: 13001` **`Vector? y`**
	`Group Type: ead-mia`
	`TN: 1`
	`COR: 1` `MM Early Answer? n`
	`Security Code:` `Local Agent Preference? n`
	`ISDN/SIP Caller Display:`
	
	`Queue Limit: unlimited`
	`Calls Warning Threshold:  Port:`
	`Time Warning Threshold:  Port:`

	On Page 2, set **Skill** to ***y***, which means that agent membership in the hunt group is based on skills, rather than pre-programmed assignment to the hunt group.

Step	Description
	add hunt-group 101 Page 2 of 3 HUNT GROUP **Skill? y** Expected Call Handling Time (sec): 180 AAS? n Service Level Target (% in sec): 80 in 20 Measured: both Supervisor Extension: Controlling Adjunct: none Timed ACW Interval (sec): Redirect on No Answer (rings): Redirect to VDN: Forced Entry of Stroke Counts or Call Work Codes? n
3.	Enter the **add agent-loginID p** command, where p is an extension valid under the provisioned dial plan. On Page 1, enter a descriptive **Name** and **Password**.
	add agent-loginID 11001 Page 1 of 2 AGENT LOGINID Login ID: 11001 AAS? n **Name: Alice** AUDIX? n TN: 1 LWC Reception: spe COR: 1 LWC Log External Calls? n Coverage Path: AUDIX Name for Messaging: Security Code: LoginID for ISDN Display? n **Password: 11001** **Password (enter again): 11001** Auto Answer: none MIA Across Skills: system ACW Agent Considered Idle: system Aux Work Reason Code Type: system Logout Reason Code Type: system Maximum time agent in ACW before logout (sec): system WARNING: Agent must log in again before changes take effect

On Page 2, set the Skill Number (**SN**) to the hunt group number assigned in Step 2. The Skill Level (**SL**) may be set according to customer requirements. Repeat this step as necessary to configure additional agent login IDs.

```
add agent-loginID 11001                                          Page   2 of   2
                                   AGENT LOGINID
      Direct Agent Skill: 101
Call Handling Preference: skill-level               Local Call Preference? n

    SN      SL          SN      SL          SN      SL          SN      SL
 1: 101     1       16:                 31:                 46:
 2:                 17:                 32:                 47:
 3:                 18:                 33:                 48:
 4:                 19:                 34:                 49:
 5:                 20:                 35:                 50:
 6:                 21:                 36:                 51:
 7:                 22:                 37:                 52:
 8:                 23:                 38:                 53:
 9:                 24:                 39:                 54:
10:                 25:                 40:                 55:
11:                 26:                 41:                 56:
12:                 27:                 42:                 57:
13:                 28:                 43:                 58:
14:                 29:                 44:                 59:
15:                 30:                 45:                 60:
```

4. Enter the **change vector q** command, where q is an unused vector number. Enter a descriptive **Name**, and program the vector to deliver calls to the hunt/skill group number defined in **Step 2**. Agents that are logged into the hunt/skill group will be able to answer calls queued to the hunt/skill group.

```
change vector 101                                                Page   1 of   3
                                   CALL VECTOR

    Number: 101              Name: Queue to Agents
                                          Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    0   secs hearing ringback
02 queue-to     skill 101  pri m
03 wait-time    120 secs hearing music
04 disconnect   after announcement none
05
```

Step	Description
5.	Enter the **add vdn r** command, where r is an extension valid under the provisioned dial plan. Specify a descriptive **Name** for the VDN and the **Vector Number** configured in **Step 4**. In this sample configuration, incoming calls from the PSTN will be routed to VDN 14001, which in turn will invoke the actions specified in vector 101.

```
add vdn 14001                                                   Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 14001
                                 Name*: Queue to Agents
                         Vector Number: 101

                   Meet-me Conferencing? n
                     Allow VDN Override? n
                                    COR: 1
                                    TN*: 1
                              Measured: none


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:



* Follows VDN Override Rules
```

6.	Enter the **change feature-access-codes** command. Define the **Auto-In Access Code**, **Login Access Code**, **Logout Access Code**, and **Service Observing Listen Only Access Code**. The adva MRS uses the Service Observing Listen Only Access Code (see **Section 5.2.2 Step 10**) for call recording.

```
change feature-access-codes                                     Page   5 of   7
                               FEATURE ACCESS CODE (FAC)

                         Automatic Call Distribution Features

                    After Call Work Access Code: *61
                             Assist Access Code: *62
                           Auto-In Access Code: *63
                          Aux Work Access Code: *64
                             Login Access Code: *65
                            Logout Access Code: *66
                         Manual-in Access Code: *67
      Service Observing Listen Only Access Code: *68
      Service Observing Listen/Talk Access Code: *69
          Service Observing No Talk Access Code: *70
                    Add Agent Skill Access Code: *71
                 Remove Agent Skill Access Code: *72
              Remote Logout of Agent Access Code: *73
```

3.3. IP Station Recording Endpoints

The IP station recording endpoints in this configuration are AES Device and Media Control API stations that essentially appear as IP softphone endpoints to Avaya Communication Manager. Each AES Device and Media Control API station requires an ***IP_API_A*** license. Note that this is separate and independent of Avaya IP Softphone licenses, which are required for Avaya IP Softphones but not required for AES Device and Media Control API stations.

Step	Description
1.	Enter the **display system-parameters customer-options** command and verify that there are sufficient **IP_API_A** licenses. If not, contact an authorized Avaya account representative to obtain these licenses.

```
display system-parameters customer-options                      Page  10 of  11
                     MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit          Used
IP_API_A       : 500            0
IP_API_B       : 0              0
IP_API_C       : 0              0
IP_Agent       : 100            0
IP_IR_A        : 100            0
IP_Phone       : 2400           4
IP_ROMax       : 2400           0
IP_Soft        : 100            0
```

2.	Enter the **add station t** command, where **t** is an extension valid under the provisioned dial plan. On Page 1, set **Type** to an IP telephone set type, enter a descriptive **Name**, specify the **Security Code**, and set **IP SoftPhone** to ***y***. Repeat this as necessary to configure additional AES Device and Media Control API stations.

```
add station 19901                                               Page   1 of   4
                                     STATION

Extension: 19901                          Lock Messages? n          BCC: 0
     Type: 4621                           Security Code: 00000       TN: 1
     Port: IP                           Coverage Path 1:            COR: 1
     Name: adva MRS #1                  Coverage Path 2:            COS: 1
                                        Hunt-to Station:

STATION OPTIONS
              Loss Group: 19            Personalized Ringing Pattern: 1
                                                   Message Lamp Ext: 19901
            Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english                 Expansion Module? n
 Survivable GK Node Name:
          Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                            IP SoftPhone? y

                                                 IP Video Softphone? n


                                                Customizable Labels? y
```

3.4. Recorded Stations

The stations that were recorded during the compliance testing include Avaya Digital and IP telephones and Avaya IP Softphones in Road Warrior mode. The extensions used were in the range 10001 to 10006.

3.5. Codec Configuration

Enter the **change ip-codec-set u** command, where **u** is a number between 1 and 7, inclusive. Enter ***G.711MU*** for **Audio Codec**. The adva MRS currently supports the G.711MU codec only.

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

                           IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
```

3.6. IP Network Regions

During compliance testing, the C-LAN board was assigned to IP network region 1 for H.323 endpoint registration. One MedPro board was also assigned to IP network region 1 to support the RTP voice traffic between all IP telephones, IP Softphones and IP station recording endpoints. As such, all the RTP traffic between them is governed by the same codec set as configured in **Section 3.5**.

Enter the **change ip-network-region v** command, where ***v*** is the number of the IP network region discussed above. Set **Codec Set** to the ip-codec-set number configured in **Section 3.5**.

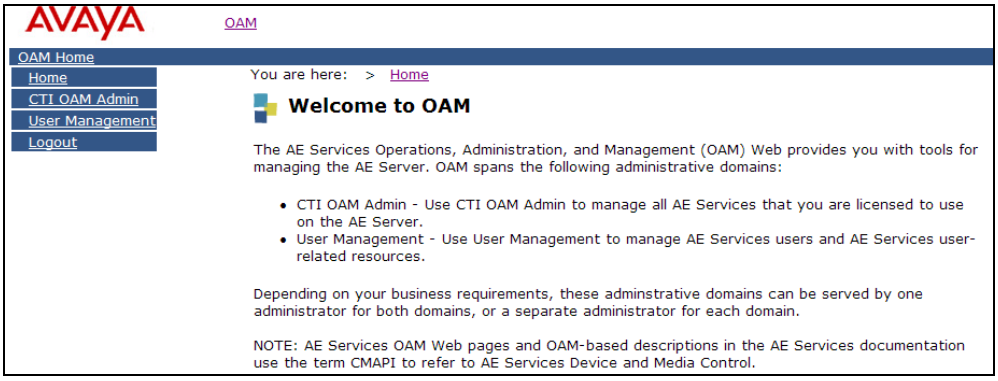
```
change ip-network-region 1                                     Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain:
    Name: Site A - Main
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 7999
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? n
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

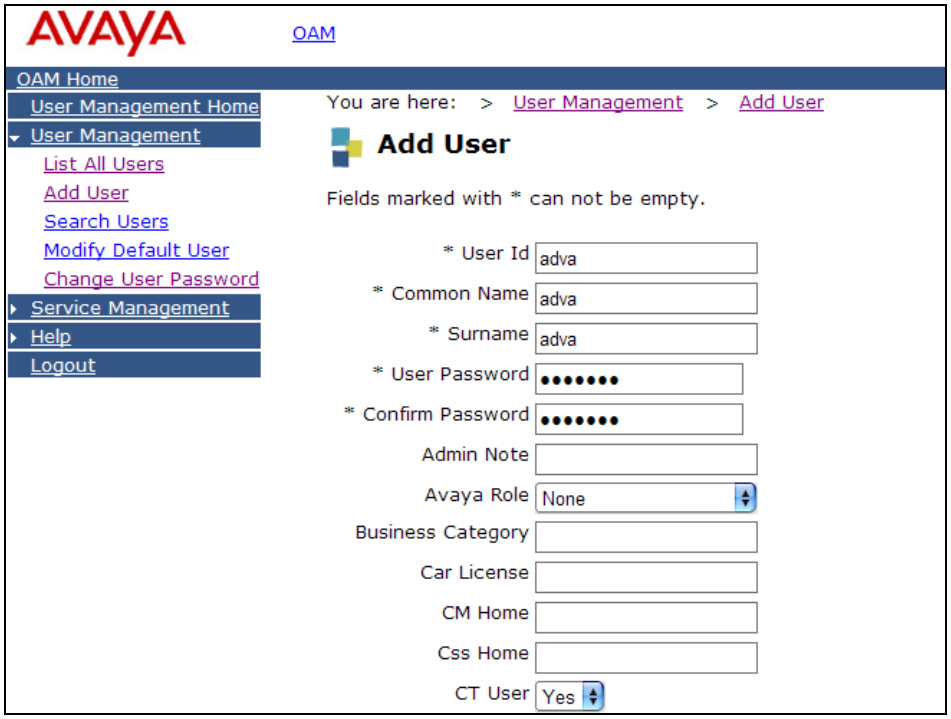
4. Configure Avaya Application Enablement Services

This section provides the procedures for configuring Avaya Application Enablement Services. The procedures fall into the following areas:

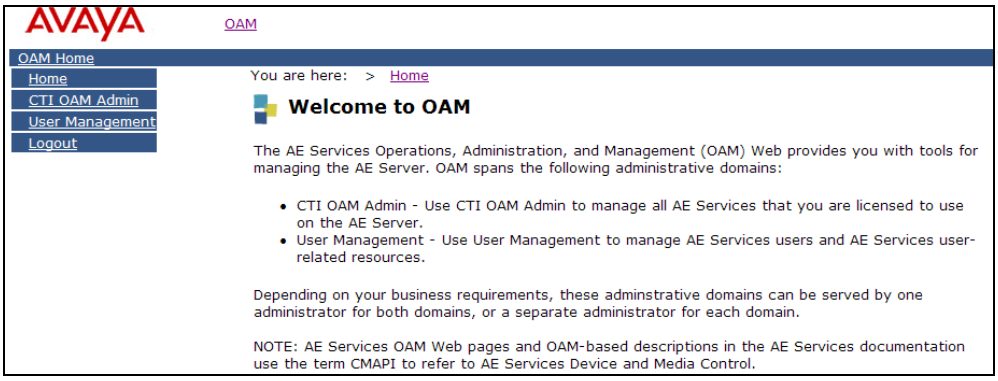
- Administer adva MRS CTI user
- Verify Avaya Application Enablement Services license
- Administer local IP
- Administer switch connection
- Administer TSAPI link
- Administer CTI user permission

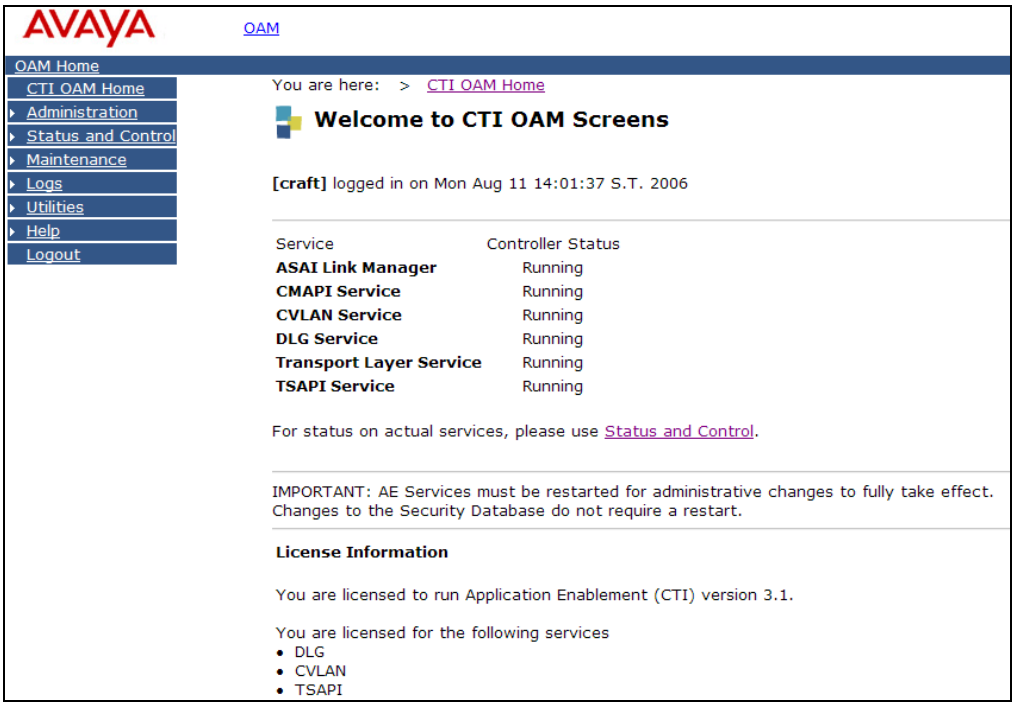
4.1. Administer adva MRS CTI User

Step	Description
1.	Launch a web browser and enter **https://<IP address of AES server>:8443/MVAP** to access the AES OAM web based interface. The AES OAM includes two separate administrative accounts, one to manage CTI OAM Admin and a separate one for User Management. Log in to AES OAM using the User Management Admin user and password, and the Welcome to OAM screen will be displayed. 

Step	Description
2.	Click **User Management**, then **User Management > Add User** in the left pane. Specify values for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. Set **CT User** to ***Yes***. The adva MRS uses this **User Id** and **Password** to access the AES server. Scroll down to the bottom of the page and click **Apply**. 

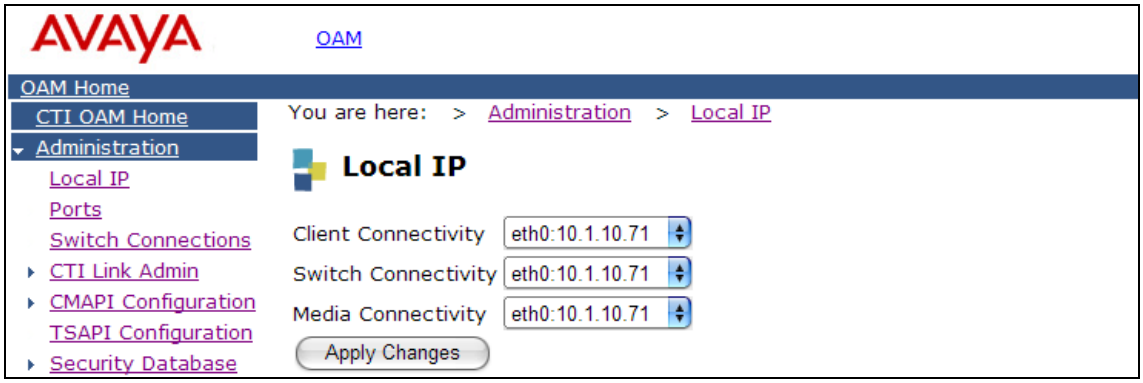
4.2. Verify Avaya Application Enablement Services License

Step	Description
1.	Launch a web browser and enter **https://<IP address of AES server>:8443/MVAP** to access the AES OAM web based interface. Log in to AES OAM using the CTI OAM Admin user and password, and the Welcome to OAM screen will be displayed. 

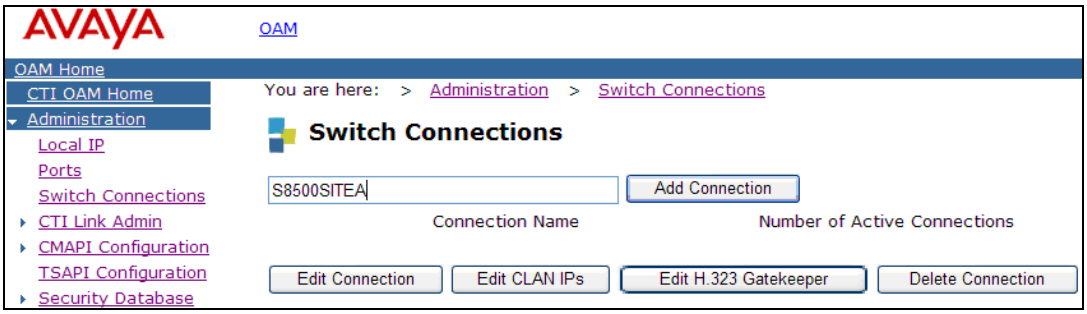
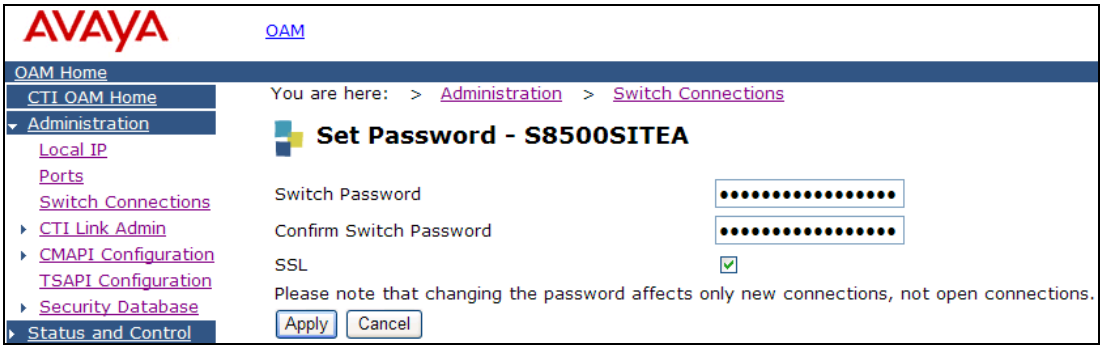
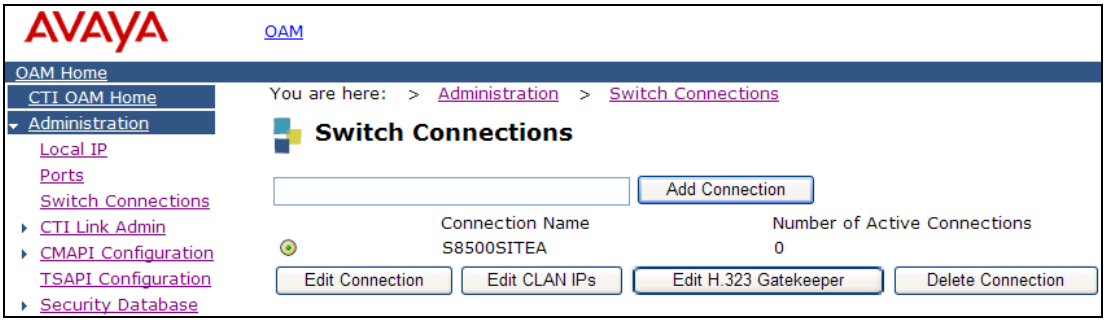
Step	Description
2.	Select **OAM Home > CTI OAM Home**. From the Welcome to CTI OAM screen, verify that the Avaya Application Enablement Services license has proper permissions for the features illustrated in these Application Notes by ensuring that the TSAPI service is licensed. If the TSAPI service is not licensed, then contact an authorized Avaya sales team or business partner for a proper license file. 

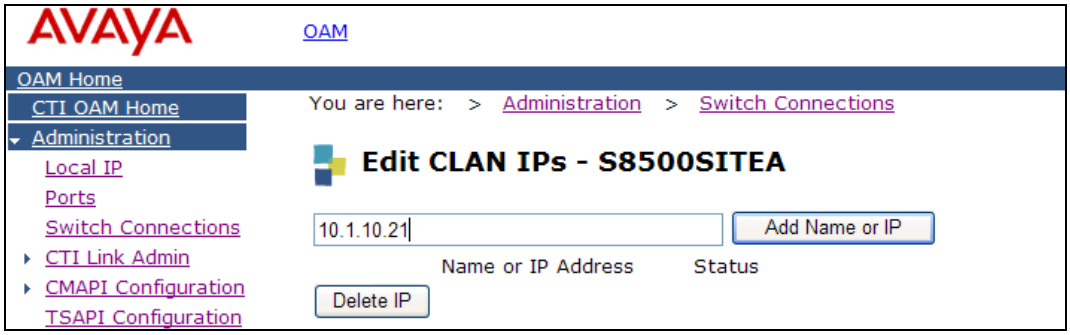
4.3. Administer Local IP

From the CTI OAM Home menu, select **Administration > Local IP**. In the **Client Connectivity** and **Media Connectivity** fields, select the AES server IP address that will be used to connect to the adva MRS. In the **Switch Connectivity** field, select the AES server IP address that will be used to connect to Avaya Communication Manager. In this configuration, the same IP address is used for all connections. Click **Apply Changes**.

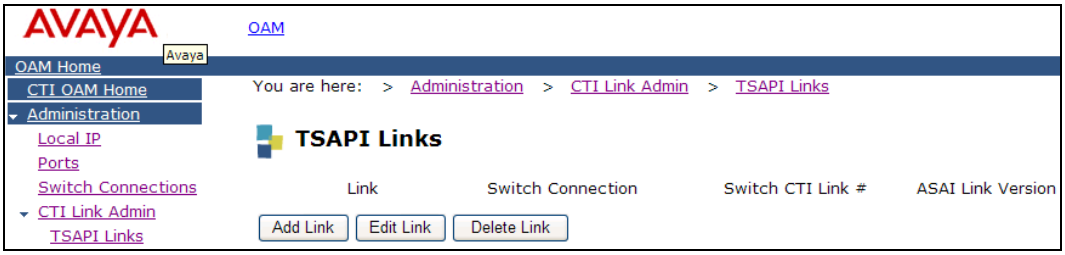


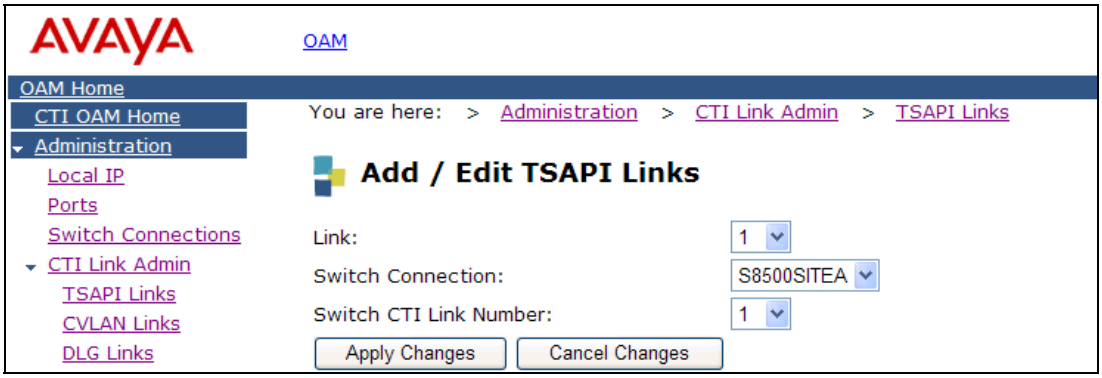
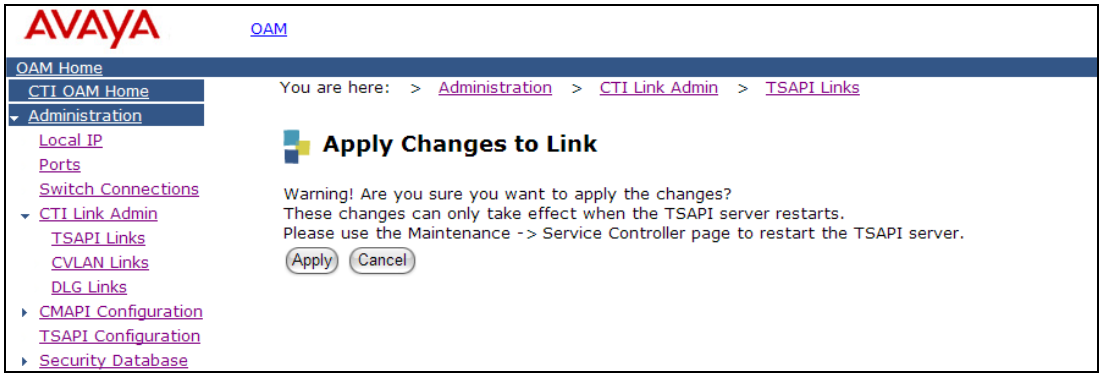
4.4. Administer Switch Connection

Step	Description
1.	From the CTI OAM Home menu, select **Administration > Switch Connections**. Enter a descriptive name for the switch connection and click **Add Connection**. In this case, ***S8500SITEA*** is used. 
2.	The Set Password screen is displayed. For the **Switch Password** and **Confirm Switch Password** fields, enter the password that was administered in Avaya Communication Manager using the ip-services form in **Section 3.1 Step 4**. The **SSL** field needs to be checked for the S8500 Media Server. Click on **Apply**. 
3.	The Switch Connections screen is displayed. Select the newly added switch connection name and click **Edit CLAN IPs**. 

Step	Description
4.	In the Edit CLAN IPs screen, enter the host name or IP address of the C-LAN used for AES connectivity. In this case, ***10.1.10.21*** is used, which corresponds to the IP address of the C-LAN administered on Avaya Communication Manager in **Section 3.1 Step 4**. Click **Add Name or IP**. 

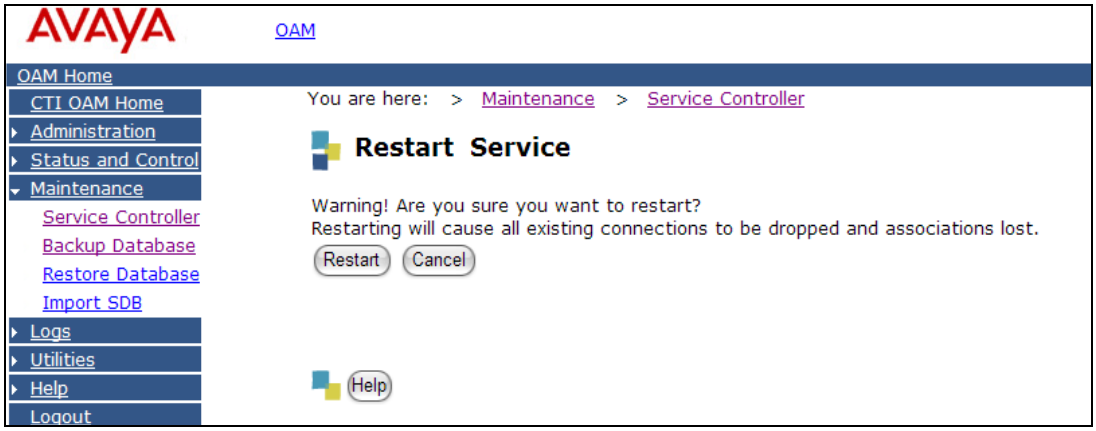
4.5. Administer TSAPI Link

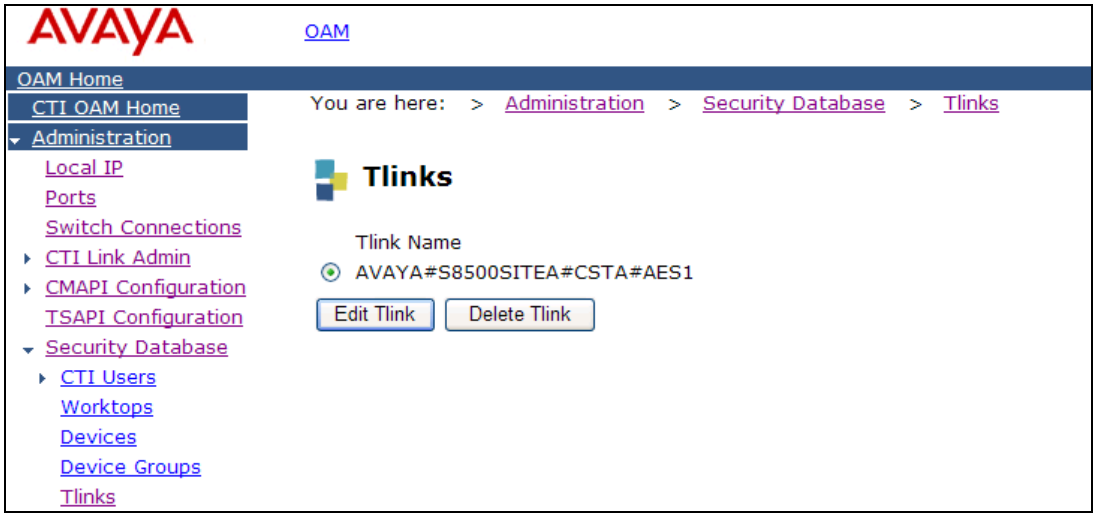
Step	Description
1.	To administer a TSAPI link on AES, select **Administration > CTI Link Admin > TSAPI Links** from the CTI OAM Home menu. Click **Add Link**. 

Step	Description
2.	In the Add/Edit TSAPI Links screen, select the following values: • **Link:** Select an available Link number from 1 to 16. • **Switch Connection:** Administered switch connection in **Section 4.4 Step 1**. • **Switch CTI Link Number:** Corresponding CTI link number in **Section 3.1 Step 2**. Click **Apply Changes**.  In the Apply Changes to Link screen, click **Apply** to confirm the changes. 

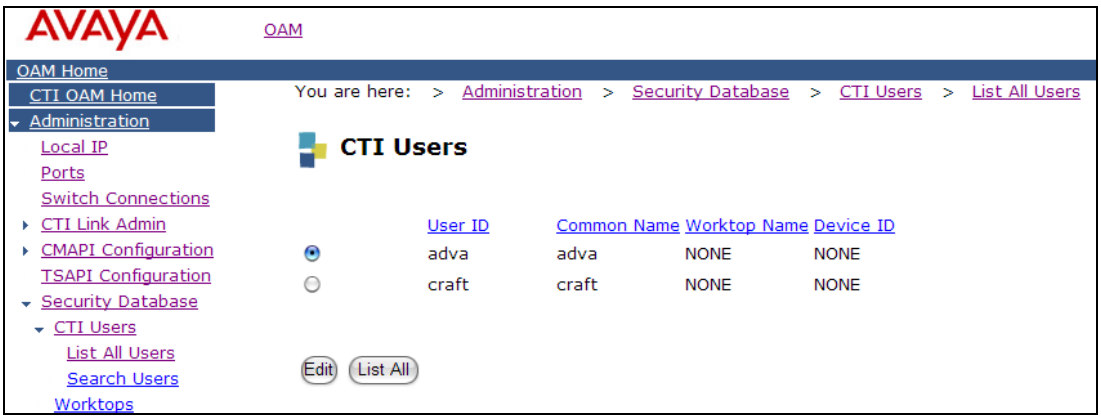
Step	Description
3.	To restart the TSAPI Service, select **Maintenance > Service Controller** from the CTI OAM Home menu. Check the **TSAPI Service** checkbox and click **Restart Service**.

In the Restart Service screen, click **Restart** to confirm the restart.

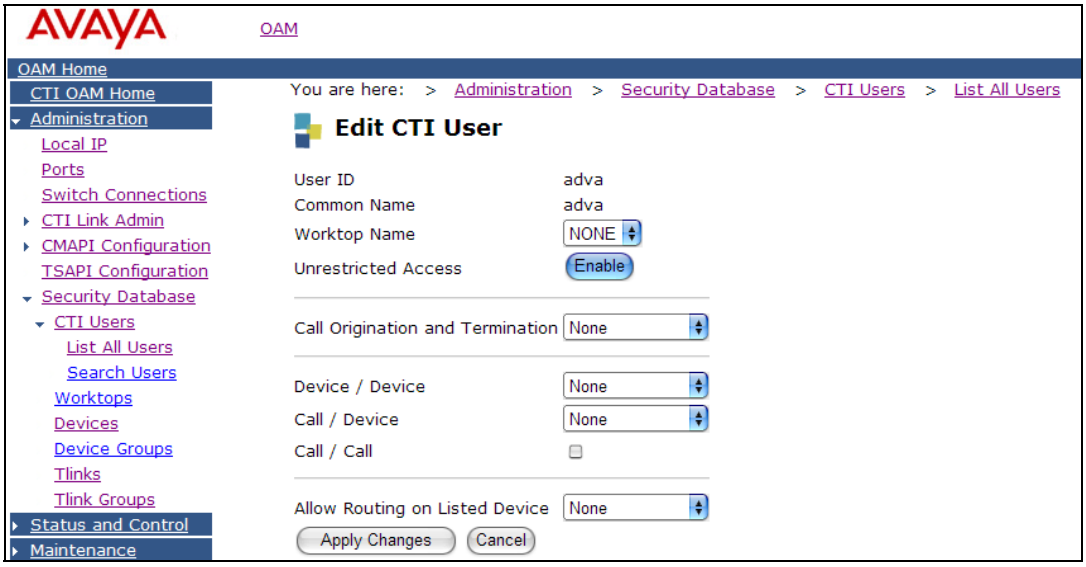


Step	Description
4.	Navigate to the Tlinks screen by selecting **Administration > Security Database > Tlinks** from the CTI OAM Home menu. Note the value of the **Tlink Name**, as this will be needed to configure the adva MRS CLC Server in **Section 5.2.2 Step 4**. In this configuration, the **Tlink Name** is ***AVAYA#S8500SITEA#CSTA#AES1***, which is automatically assigned by the AES server. 

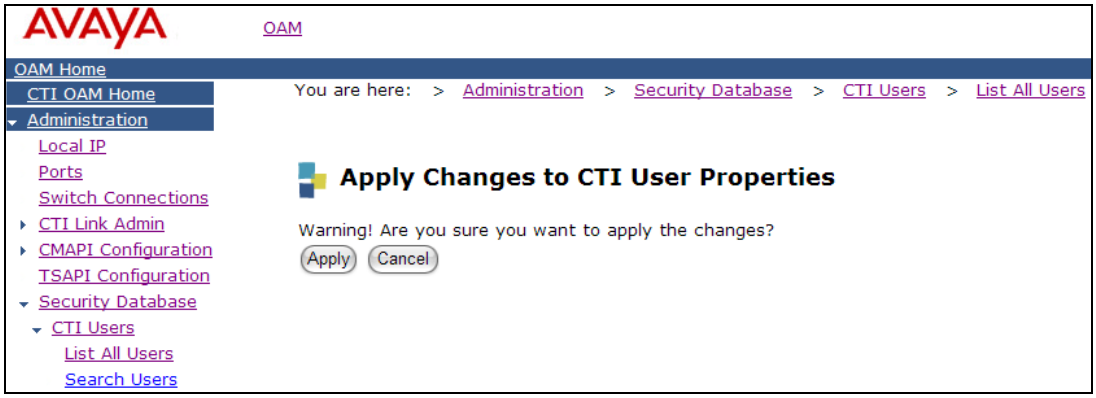
4.6. Administer CTI User Permission

Step	Description
1.	Under **Administration** in the left pane, click on **Security Database > CTI Users > List All Users**. Select the **User ID *adva*** created in **Section 4.1 Step 2** and click **Edit**. 

Step	Description
2.	Assign access rights and call/device privileges according to customer requirements. For simplicity in configuration, **Unrestricted Access** was enabled during compliance testing. If **Unrestricted Access** is not desired, then consult [1] for guidance on configuring the call/device privileges as well as devices and device groups. Click **Enable**.



In the Apply Changes to CTI User Properties screen, click **Apply** to apply the changes.



5. Configure Seoul Commtech adva MRS

This section provides the procedures for configuring the Seoul Commtech adva MRS. The adva MRS solution was installed on two generic Intel Pentium 4 2.8 GHz servers with 1 GB of memory each running Microsoft Windows Server 2003 with Service Pack 1. The adva MRS VRC and SRC server components were installed on the first server. On the second server, the adva MRS CLC server component was installed, together with the Apache Tomcat 5.5 for web administration and Microsoft SQL Server 2000 with Service Pack 4 for the storing of system configuration and voice recording call details.

5.1. Configure Avaya CT TS Win32 Client Software

The adva MRS CLC server component uses the Avaya CT TS Win32 Client software to communication with the TSAPI Service on the AES server. During the installation of the adva MRS CLC server component, the installer is prompted to install the Avaya CT TS Win32 client. The installation runs through the following steps:

a. A welcome window will be displayed. Click **Next** to continue.

b. Leave the **Administration** utilities unchecked, accept the **Destination Folder** and click **Next**. The **Administration** utilities are not applicable for the AES.

c. In the **Host Name or IP Address** field, enter the IP Address of the AES server and click **Add to List**. In this configuration, enter **10.1.10.71**. Click **Next**.

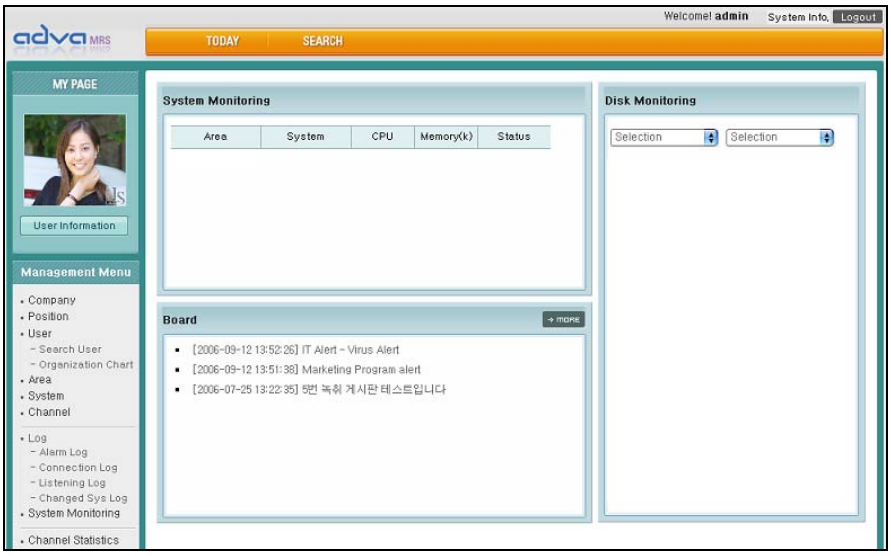
d. At the end of installation process, click **Finish**.

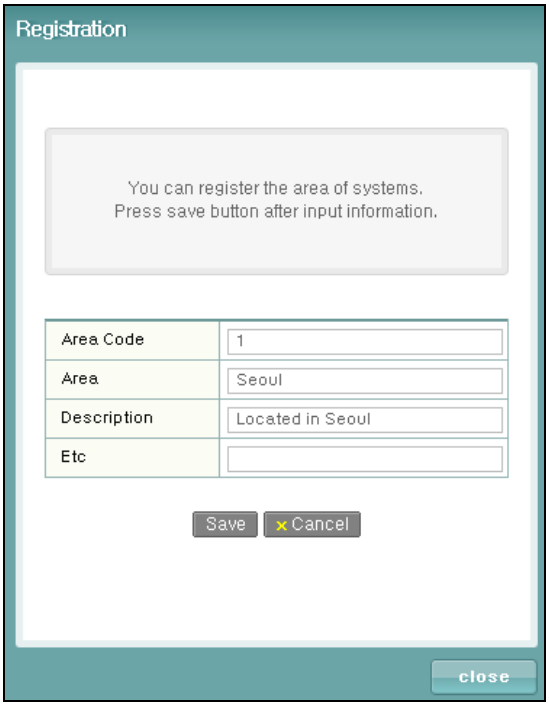
5.2. Configure Seoul Commtech adva MRS

The configuration of the adva MRS falls in the following areas:

- Configure adva MRS System Parameters
- Configure adva MRS Servers

5.2.1. Configure adva MRS System Parameters

Step	Description
	Configure Area
1.	Launch Microsoft Internet Explorer and enter **http://<IP address of adva MRS CLC server>/mrs** to access the adva MRS web based interface. Log in using a user with Administrator privileges to display the Today page as shown below. 

Step	Description
2.	From the **Management Menu**, click **Area** to display the Area page. Click **Registration** to add a new **Area**. An adva MRS system can be distributed over different **Area** locations. 
3.	In the Registration pop up page, specify a number for **Area Code** and enter a descriptive name for **Area** and **Description**. Click **Save**. Click **close** to close the page. 

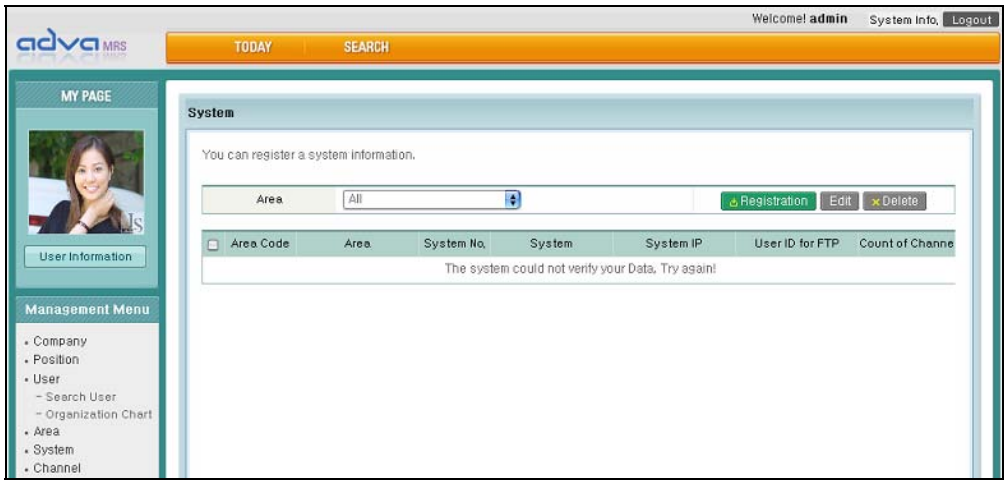
Step	Description
	Configure Systems

4. An adva MRS system consists of one **DB**, one **CLC** and up to 4 **VRC** and **SRC** systems. In this configuration, the systems are defined as follows:

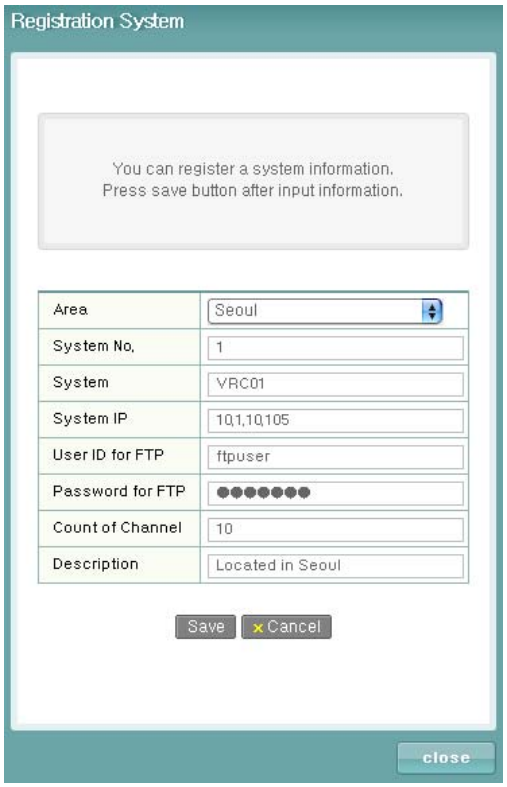
Area	System No.	System	System IP	User ID for FTP	Password for FTP	Count of Channel
Seoul	1	VRC01	10.1.10.105	ftpuser	ftpuser	10
Seoul	2	SRC01	10.1.10.105	ftpuser	ftpuser	10
Seoul	3	DB01	10.1.10.106	ftpuser	ftpuser	10
Seoul	4	CLC01	10.1.10.106	ftpuser	ftpuser	10

The **User ID for FTP** and **Password for FTP** fields are used internally by the system to access the files stored on different servers.

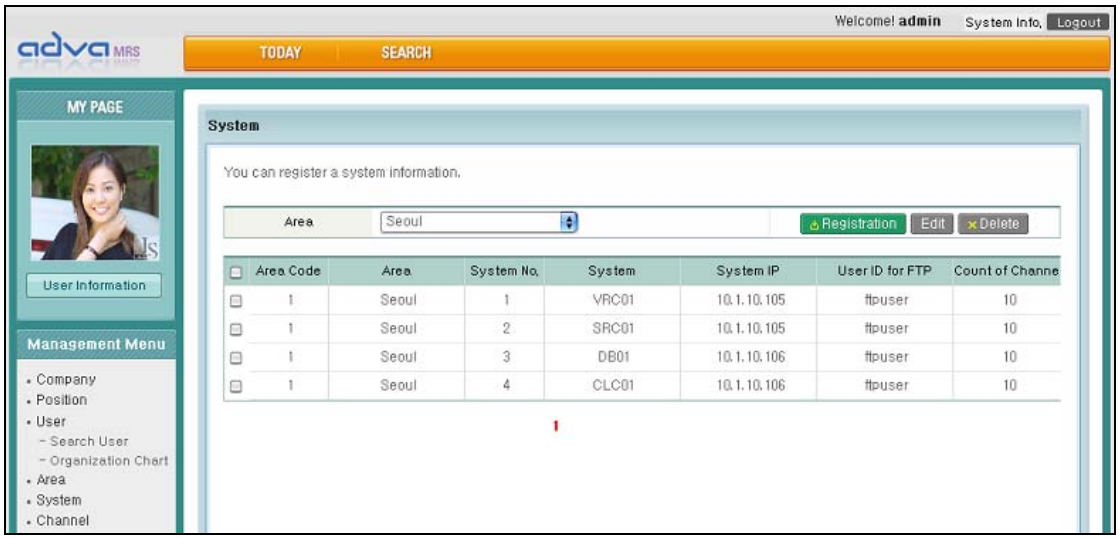
From the **Management Menu**, click **System** to display the System page.

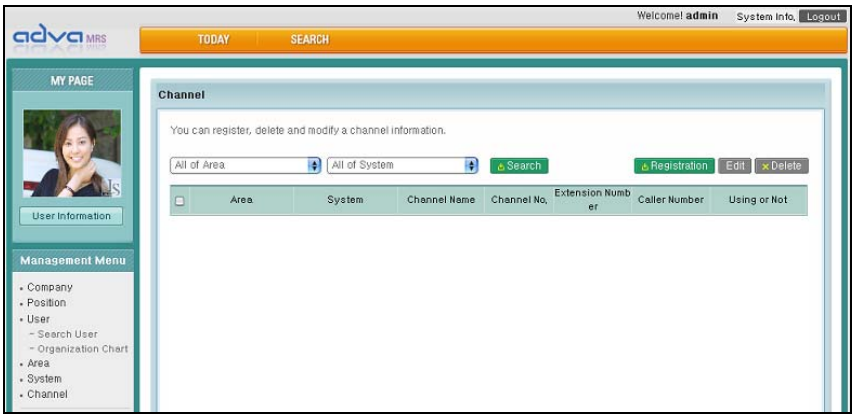
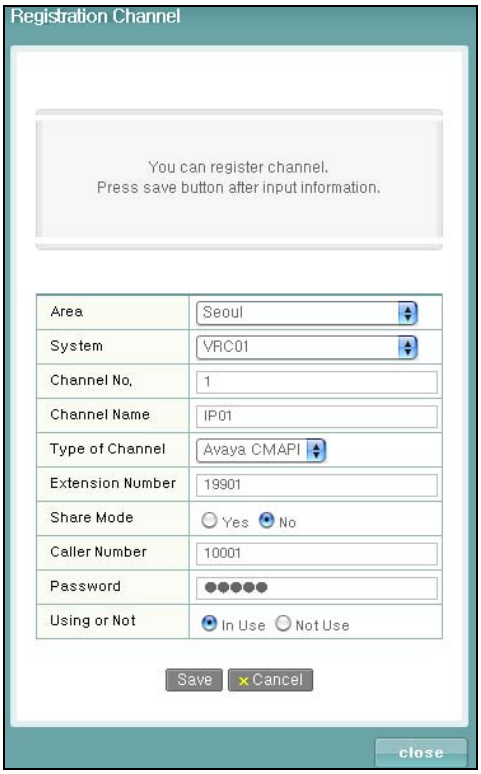


5. Click **Registration** to add a new **System**. In the Registration System pop up page, specify the values for the **VRC01** system as shown in the table in **Step 4**. Click **Save**. Click **close** to close the page.

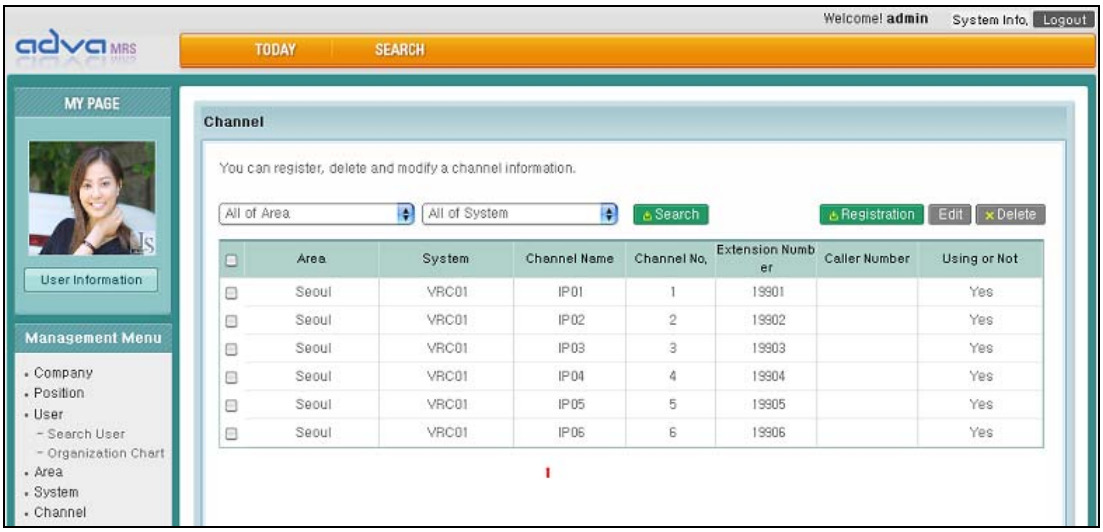


6. Repeat **Step 5** to add the remaining 3 systems. The System page below shows the administered systems when completed.



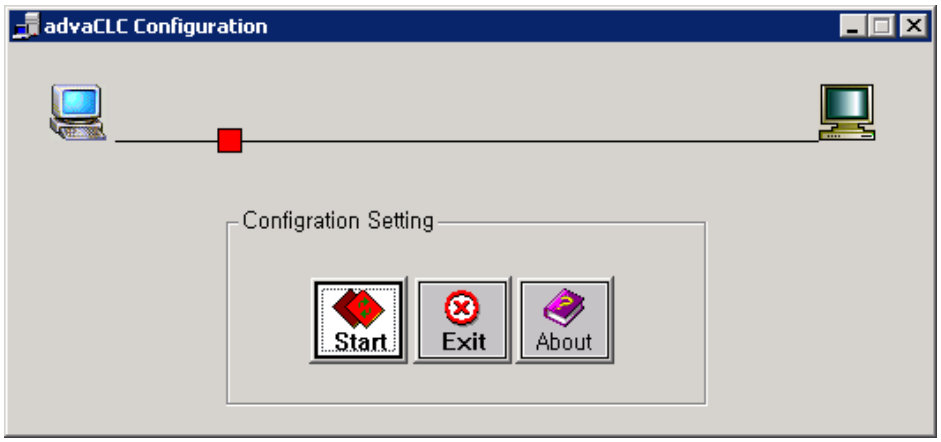
Step	Description
	Configure Channels
7.	From the **Management Menu**, click **Channel** to display the Channel page. 
8.	Click **Registration** to add a new **Channel**. In the Registration Channel pop up page, select the Area created in **Step 3** for **Area** and ***VRC01*** for **System**. Specify the **Channel No.**, **Channel Name** and select ***Avaya CMAPI*** for **Type of Channel**, ***No*** for **Share Mode** and ***In Use*** for **Using or Not**. Enter an extension for **Extension Number** and the **Security Code** for **Password** as created in **Section 3.3 Step 2**. For **Caller Number**, enter an extension to be recorded by this channel. Click **Save**. Click **close** to close the page. 

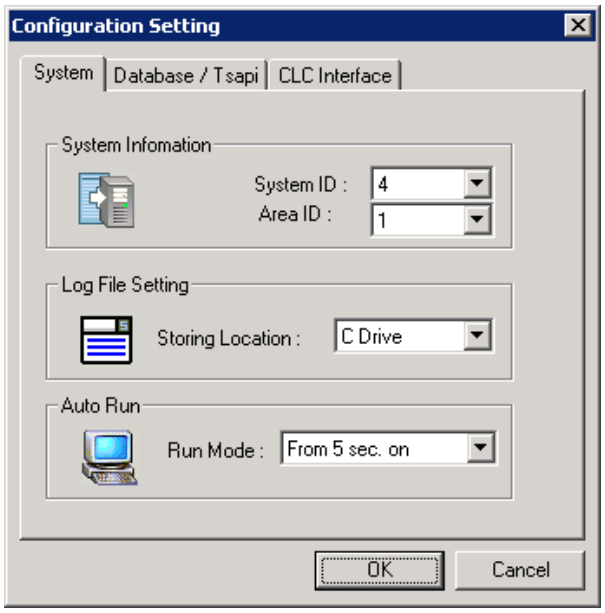
9.	Repeat **Step 8** to configure more channels to record other extensions. In this configuration, 6 channels were created for voice recording. The Channel page below shows the administered channels when completed.

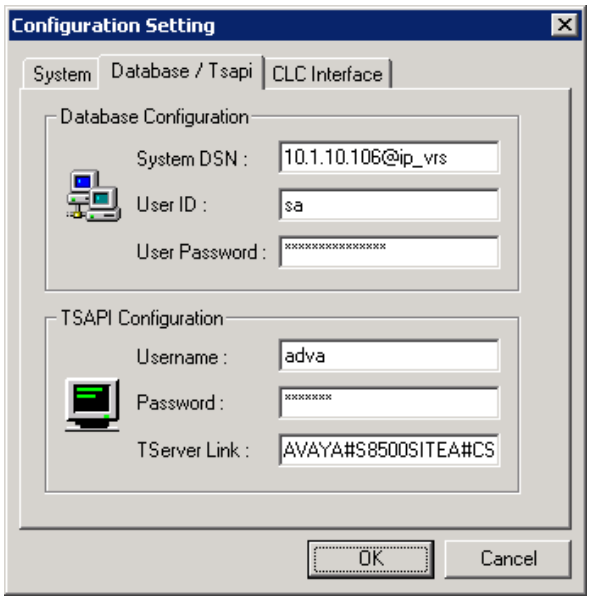
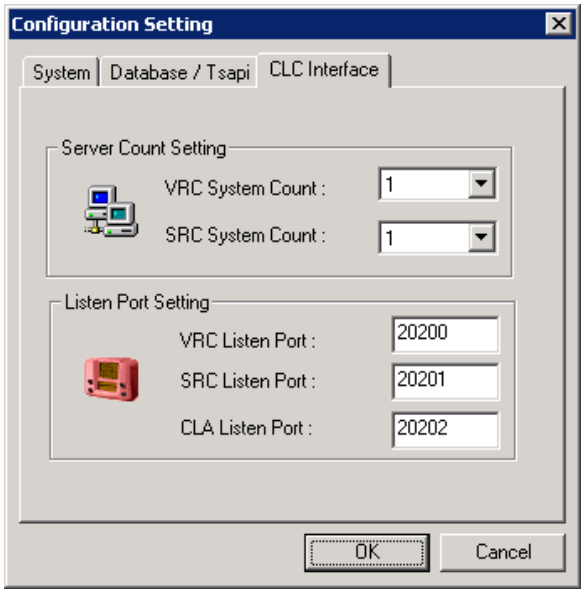


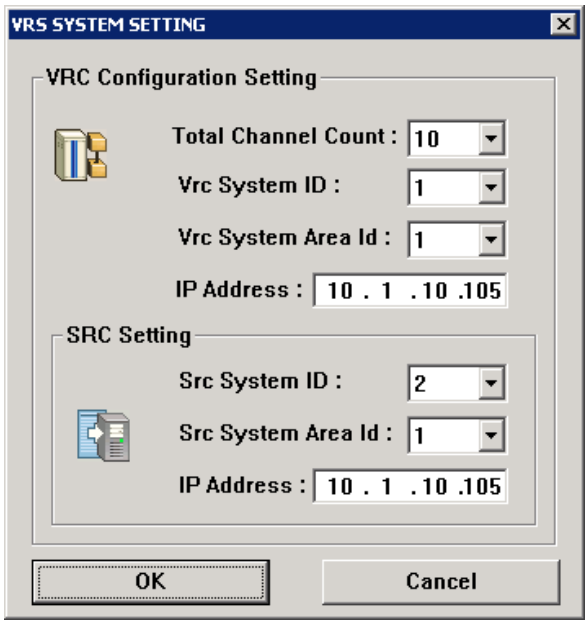
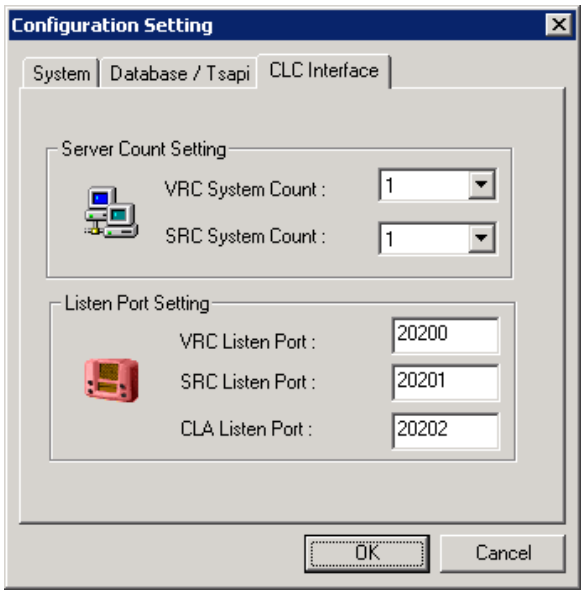
5.2.2. Configure adva MRS Servers

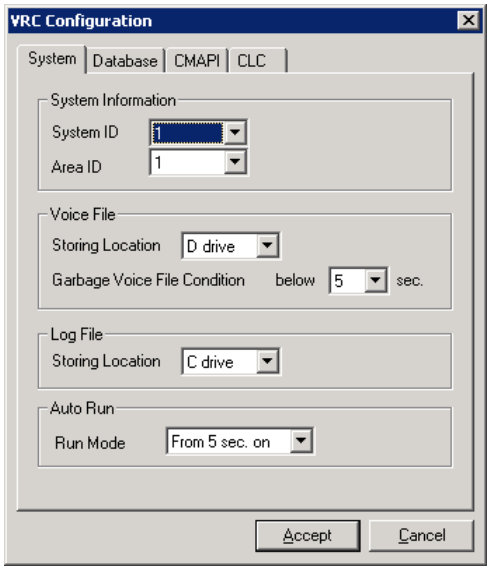
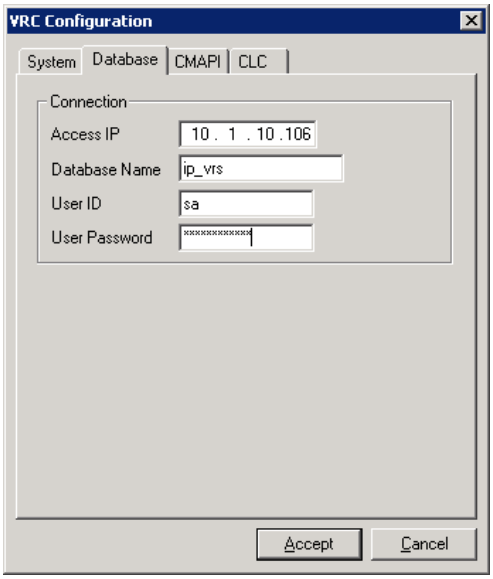
Step	Description
	adva MRS CLC Server Configuration
1.	To configure the adva MRS CLC server component, click **Start→All Programs→ advaCLC→advaCLC Config**. Click **Start**.

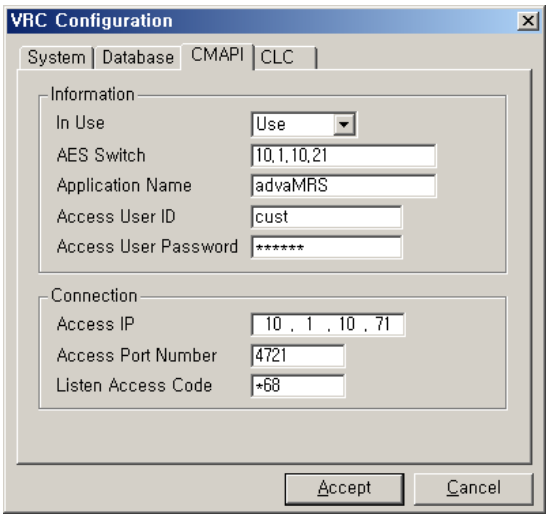
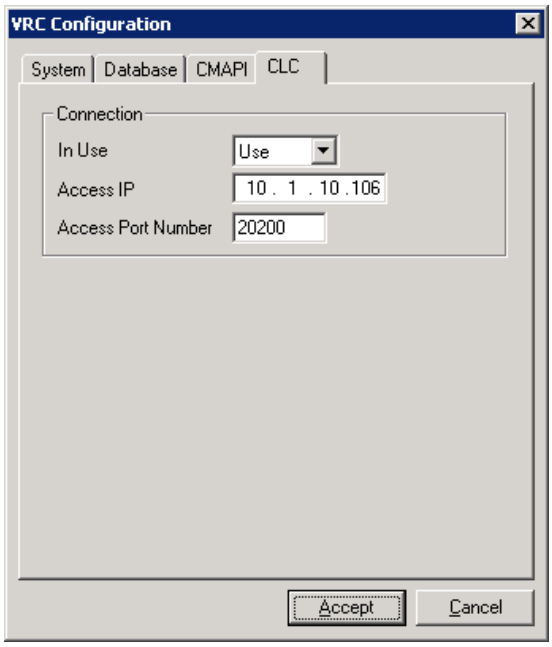


Step	Description
2.	Enter the administration login and password and click **Ok**. 
3.	In the **System** tab, select the **System ID** and **Area ID** for the CLC server as created in **Section 5.2.1 Step 3** and **4**. Select ***From 5 sec. on*** for **Run Mode** to configure the CLC server to start automatically when the machine powers on. 

Step	Description
4.	In the **Database / Tsapi** tab, enter ***10.1.10.106@ip_vrs*** for **System DSN**, where ***10.1.10.106*** is the IP address of the Microsoft SQL server and ***ip_vrs*** is the Database name. Enter a database user account with access rights to the ***ip_vrs*** database for **User ID** and **User Password**. For TSAPI Configuration, enter the CTI User created in **Section 4.1 Step 2** for **Username** and **Password** and the TLink Name as shown in **Section 4.5 Step 4** for **TServer Link**. 
5.	In the **CLC Interface** tab, select ***1*** for **VRC System Count**. 

Step	Description
6.	When selecting 1 for VRC System Count, the VRC System Setting window will pop up for the configuration of the VRC and SRC Servers. Referring to the table in **Section 5.2.1 Step 4** for the VRC system, enter the values for **Total Channel Count**, **Vrc System ID**, **Vrc System Area Id** and **IP Address**. Using the same table, enter the values for **Src System ID**, **Src System Area Id** and **IP Address** for the SRC setting. Click **OK** to return to the **CLC Interface** tab. 
7.	Select ***1*** for **SRC System Count**. Enter ***20200*** for **VRC Listen Port**, ***20201*** for **SRC Listen Port** and ***20202*** for **CLA Listen Port**. Click **OK**. 

Step	Description
	adva MRS VRC and SRC Server Configuration
8.	To configure the adva MRS VRC server component, click **Start→All Programs→ advaVRC→advaVRC Config**. The VRC Configuration window is displayed. In the **System** tab, select the **System ID** and **Area ID** for the VRC server as created in **Section 5.2.1 Step 3** and **4**. For the Voice File section, select a drive for Storing Location to store the voice files. Select ***From 5 sec. on*** for **Run Mode** to configure the VRC server to start automatically when the machine powers on. 
9.	In the **Database** tab, enter the IP address of the Microsoft SQL Server for **Access IP** and ***ip_vrs*** for **Database Name**. Enter a database user account with access rights to the ***ip_vrs*** database for **User ID** and **User Password**. 

Step	Description
10.	In the CMAPI tab, select ***Use*** for **In Use**. Enter the C-LAN IP address as shown in **Section 3.1 Step 3** for **AES Switch** and ***advaMRS*** for **Application Name**. Enter any value for **Access User ID** and **Access User Password**. The current version of AES does not perform user verification. In the Connection section, enter the IP address of the AES server for **Access IP**, ***4721*** for the **Access Port Number** and ****68*** for the **Listen Access Code**. 
11.	In the **CLC** tab, select ***Use*** for **In Use**. Set **Access IP** to the IP address of the CLC server and ***20200*** for **Access Port Number**. Click **Accept**. 

6. Interoperability Compliance Testing

The interoperability compliance test included feature, serviceability and performance testing.

The feature testing evaluated the ability of the Seoul Commtech adva MRS to monitor and record calls placed to and from Avaya IP and Digital telephones, IP Softphones and agents.

The serviceability testing introduced failure scenarios to see if adva MRS is able to resume recording after failure recovery.

The performance testing stressed the adva MRS by continuously placing calls to a VDN over an extended period of time.

6.1. General Test Approach

The general approach was to place various types of calls to and from telephones, IP Softphones and agents, monitor and record the calls using adva MRS, and verify the recordings. Some of the recorded calls included both the voice conversation and agent PC screen capture.

For feature testing, the types of calls included internal extension calls, internal ACD calls, inbound ACD trunk calls, inbound trunk calls, outbound trunk calls, transferred calls and conference calls.

For serviceability testing, reboots were applied to the adva MRS servers, the AES server and the Communication Manager Media Server to simulate system unavailability.

For performance testing, a call generator continuously placed calls to a VDN that queues the calls in a hunt/skill group, which in turn delivers the calls to agents logged into the hunt/skill group. The call generator played a recorded speech file continuously for the duration of each call.

6.2. Test Results

The adva MRS successfully monitored, recorded, stored and played back the various types of calls discussed in **Section 6.1**. For serviceability testing, The adva MRS was able to resume recording calls after the rebooting of the adva MRS servers, the AES server and the Avaya S8500B Media Server. For performance testing, the adva MRS successfully recorded 30 simultaneous calls for over 14 consecutive hours. In another test, the adva MRS also successfully recorded 120 simultaneous calls for over 3 consecutive hours.

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager, Avaya Application Enablement Services and Seoul Commtech adva MRS.

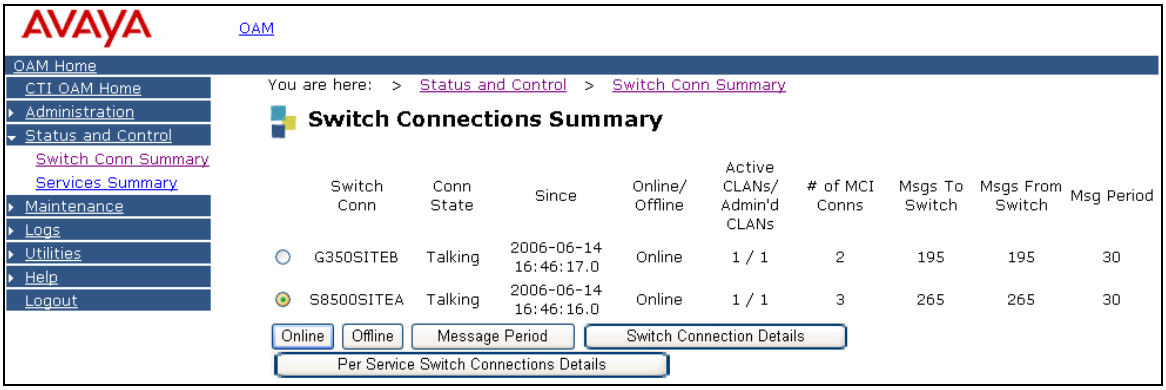
7.1. Verify Avaya Communication Manager

Verify the status of the administered CTI link by using the **status aesvcs cti-link** command. The **Service State** field should display ***established***.

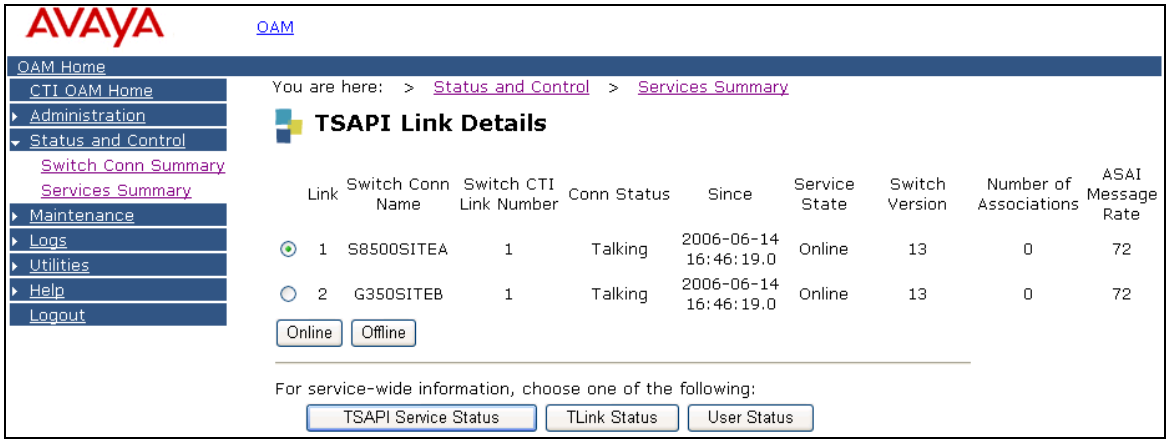
```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI    Version  Mnt    AE Services      Service       Msgs     Msgs
Link            Busy   Server           State         Sent     Rcvd

1      4        no     aes1             established   87       130
```

7.2. Verify Avaya Application Enablement Services

From the AES CTI OAM Home menu, select **Status and Control > Switch Conn Summary** and verify the status of the switch connection. The **Conn State** of the switch connection should display **Talking**.

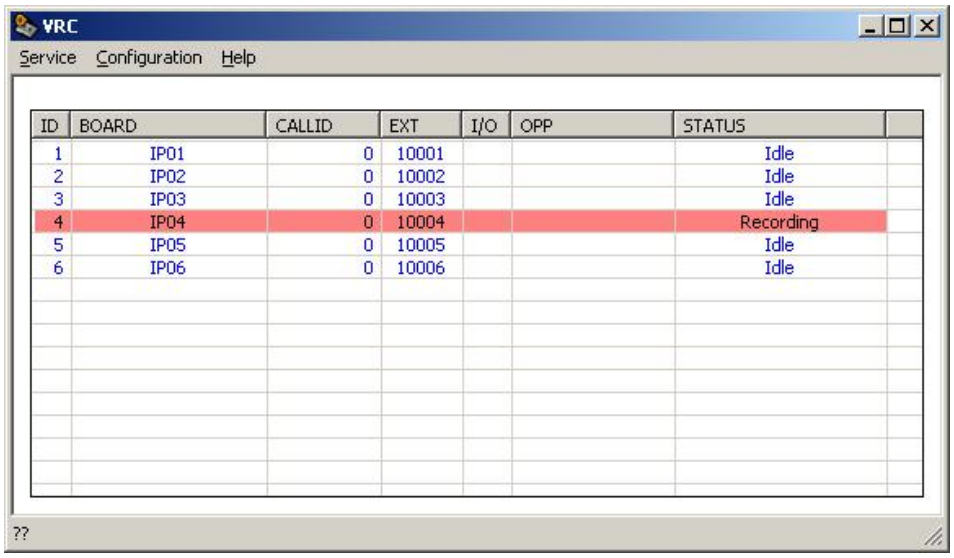


Verify the status of the TSAPI link by selecting **Status and Control > Services Summary** from the CTI OAM Home menu. Click on **TSAPI Service**, followed by **Details**. The TSAPI Link Details screen is displayed, as shown below. The **Conn Status** of the TSAPI Link should display **Talking** and **Service State** display **Online**.

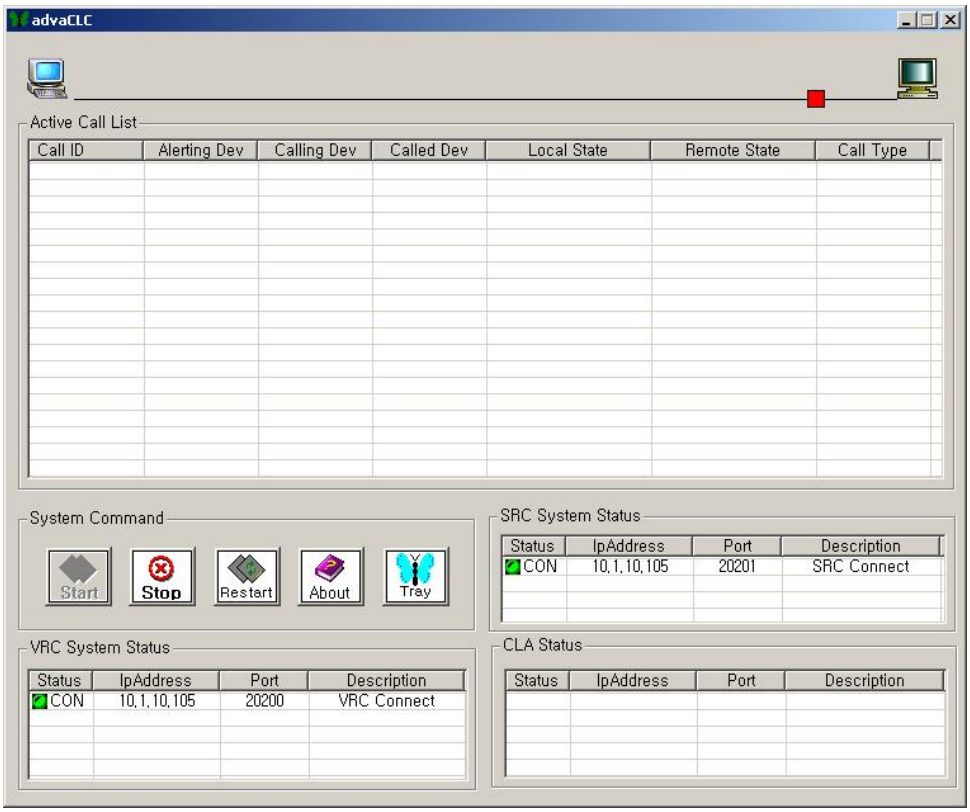


7.3. Verify Seoul Commtech adva MRS

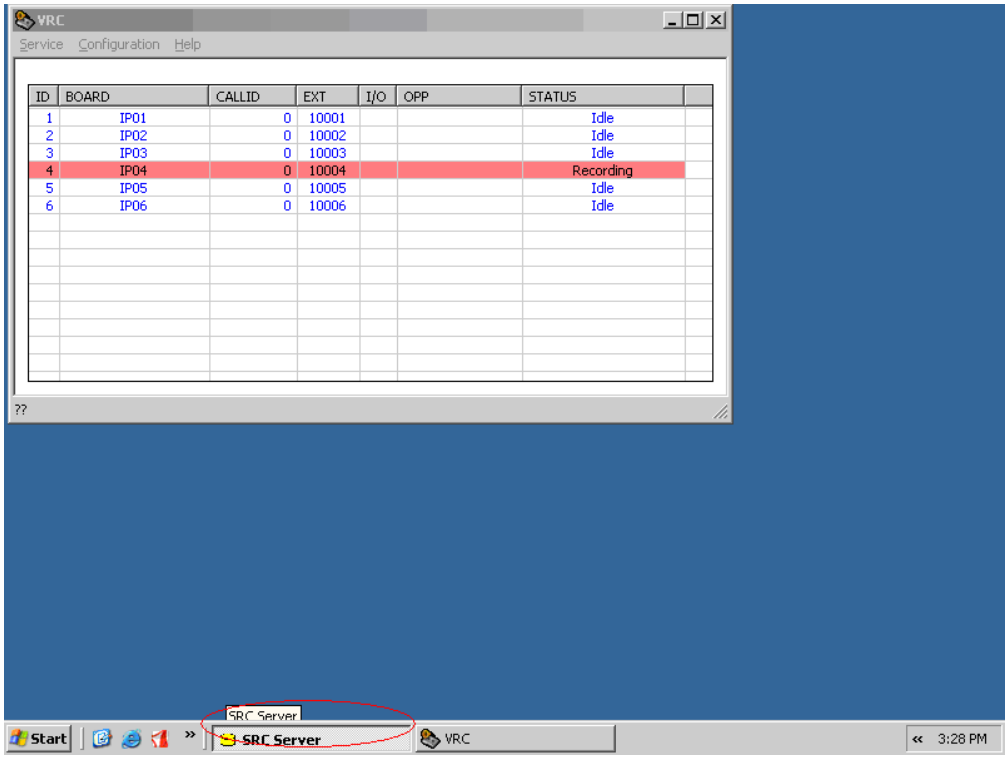
Verify the status of the adva MRS VRC Server from the VRC console. The **STATUS** of each channel should display ***Idle*** or ***Recording***.



Verify the status of the adva MRS CLC server from the CLC console. The **VRC System Status** and **SRC System Status** should display the connections from the VRC and SRC servers and the **Status** should display ***CON***.



The adva MRS SRC server does not have an interface. Verify that the SRC server is running by checking the Taskbar for the SRC Server.



8. Support

For technical support on Seoul Commtech adva MRS, contact Seoul Commtech at:

- Phone: +82-11-398-3896
- Email: sungwoo1974.kim@samsung.com

9. Conclusion

These Application Notes describe the procedures for configuring the Seoul Commtech adva MRS Version 2006.7.1.1 to monitor and record calls placed to and from Avaya IP and Digital telephones, Avaya IP Softphones, and agents on Avaya Communication Manager Release 3.1.2. In the configuration described in these Application Notes, the adva MRS uses the TSAPI Services and Device and Media Control Services of Avaya Application Enablement Services 3.0.1 to perform recording. During compliance testing, the adva MRS successfully monitored and recorded calls placed to and from Avaya IP and Digital Telephones, Avaya IP Softphones and agents, as well as calls placed to a VDN and then queued to an agent hunt/skill group. The adva MRS was also able to record calls under continuous call volumes over an extended period of time.

10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.

[1] *Avaya Application Enablement Services 3.0 Administration and Maintenance Guide*, Document ID 02-300357, Issue 1, June 2005.

Product information for Seoul Commtech adva MRS may be found at http://adva.scommtech.com/.

[2] *adva MRS Installation Manual*
[3] *adva MRS Maintenance Manual*
[4] *adva MRS Web User Manual*

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 Developer*Connection* Program at devconnect@avaya.com.