Avaya Solution & Interoperability Test Lab

Application Notes for the Mercom Audiolog Call Recording Server with Avaya Communication Manager and Avaya Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the Mercom Audiolog 3.3 Call Recording Server to monitor and record calls placed to and from stations, softphones, and agents on Avaya Communication Manager 3.0. In the configuration described in these Application Notes, Audiolog uses the Call Control Services and Device and Media Control Services of Avaya Application Enablement Services to perform recording. During compliance testing, the Audiolog Call Recording Server successfully recorded calls placed to and from Avaya IP and Digital Telephones, analog telephones, Avaya IP Softphones, and agents, as well as calls placed to a Vector Directory Number (VDN) and then queued to an agent hunt/skill group. 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 the Mercom Audiolog Call Recording Server. Audiolog monitors, records, stores, and plays back phone calls for verification and quality assurance.

Audiolog interacts with an Avaya AES server, which in turn interacts with Avaya Communication Manager. Audiolog uses the Call Control Services, specifically the Telephony Services Application Programming Interface (TSAPI), of Avaya AES to receive event reports and call information concerning particular stations, agents, and agent hunt/skill groups, and can use those event reports as recording triggers. Audiolog also uses the Device and Media Control Services (formerly known as Communication Manager Application Programming Interface, or CMAPI) of Avaya AES to register AES Device and Media Control API "virtual" stations with Avaya Communication Manager. The AES Device and Media Control API stations essentially appear as IP softphones to Avaya Communication Manager. For full time and scheduled recording, Audiolog records a call by issuing a Single Step Conference (SSC) request via TSAPI to bridge an AES Device and Media Control API station onto an active call. For on-demand recording, Audiolog records a call by dynamically programming an AES Device and Media Control API station to service observe the station to be recorded. In both cases, since the IP address of the AES Device and Media Control API station is that of the Audiolog server, the audio portion of the call is directed to the Audiolog server and can thus be recorded.

Figure 1 illustrates a sample configuration consisting of a pair of redundant Avaya S8710 Media Servers, an Avaya G650 Media Gateway, an Avaya AES server, Avaya IP and Digital Telephones, analog telephones, Avaya IP Softphones, and a Mercom Audiolog Call Recording Server. Avaya Communication Manager runs on the active S8710 Media Server. The solution described herein is also extensible to other Avaya Media Servers and Media Gateways.
The Mercom Audiolog Call Recording Server contains two network interfaces, one of which is for communicating with the Avaya Application Enablement Services and the other is for receiving RTP traffic from the Media Processor (MedPro) boards. Note that the latter network interface, hereafter referred to as the Audiolog RTP network interface, resides on the same subnet (192.45.103.0/24) as the MedPro boards in the Avaya G650 Media Gateway. However, the Audiolog RTP network interface is not required to reside on the same subnet as the MedPro boards as long as the Audiolog RTP network interface is reachable from the MedPro boards.

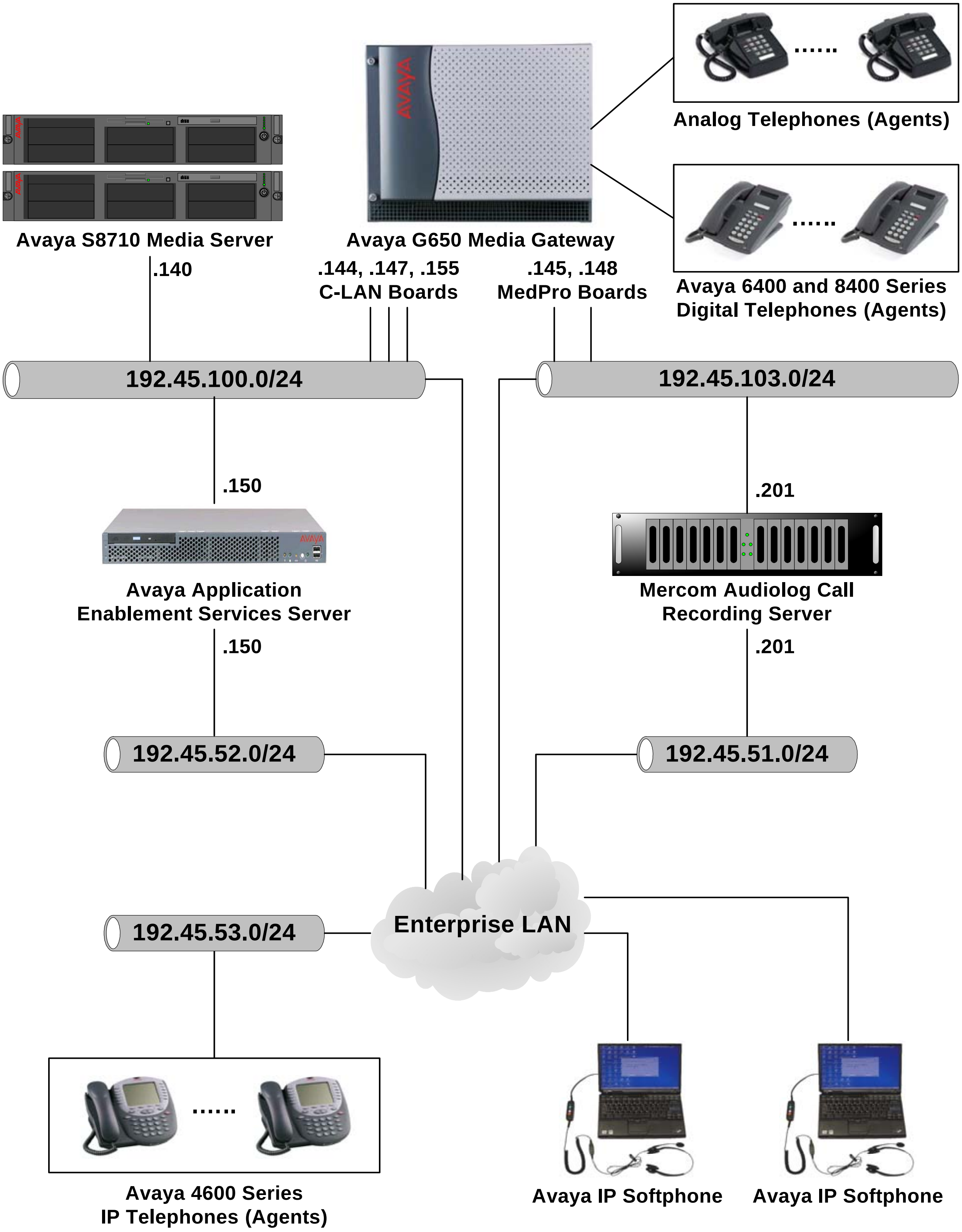


Figure 1: Sample Configuration.

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8710 Media Server	Avaya Communication Manager 3.0.1 (R013x.00.1.346.0)
Avaya G650 Media Gateway	-
TN2312BP IP Server Interface	22
TN799DP C-LAN Interface	15
TN2302AP IP Media Processor	107
TN2602AP IP Media Resource 320	7
Avaya 4600 Series IP Telephones	1.8.3 (4606) 1.8.3 (4612) 1.8.3 (4624) 2.3 (4602SW) 2.3 (4610SW) 2.3 (4620SW) 2.5 (4625SW)
Avaya IP Softphone	5.2 Service Pack 1
Avaya 6400 Series Digital Telephones	-
Avaya 8400 Series Digital Telephones	-
Analog Telephones	-
Avaya Application Enablement Services Server	3.0.1
Mercom Audiolog Call Recording Server	3.3
CTILink.exe	3.30.0.422
SwitchSrv.exe	3.20.0.6
RAPISrv.exe	3.30.0.305
Recorder.exe	3.30.0.57
Rodni.exe	3.20.0.47
AlChannel.dll	3.30.0.303
aes.cmapi.dll	1.0.5.0

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, agent login/logoff codes, recording ports, and 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 Mercom Audiolog Call Recording Server and Avaya Communication Manager. The AES server communicates with Avaya Communication Manager over an "AES" link. Within the AES link, CTI links may be configured to provide CTI services to CTI applications such as Audiolog. The following steps demonstrate the configuration of the Avaya Communication Manager side of the AES and CTI links. See Section 4 for the details of configuring the AES side of the AES and CTI links.

Step	Description
1.	Enter the **display system-parameters customer-options** command. On Page 3 of the system-parameters customer-options form, verify that **ASAI Link Core Capabilities** is set to "**y**". If not, contact an authorized Avaya account representative to obtain the license.

```
display system-parameters customer-options                    Page   3 of  10
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? n           Audible Message Waiting? n
        Access Security Gateway (ASG)? n               Authorization Codes? n
        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? n  Computer Telephony Adjunct Links? n
          ARS/AAR Dialing without FAC? y   Cvg Of Calls Redirected Off-net? n
          ASAI Link Core Capabilities? y                      DCS (Basic)? y
          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



        (NOTE: You must logoff & login to effect the permission changes.)
```

Step **Description**

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 2                                                Page   1 of   2
                                   CTI LINK
 CTI Link: 2
Extension: 2002
     Type: ADJ-IP
                                                                     COR: 1
     Name: AES-DevCon1 TSAPI/JTAPI
```

3. Enter the **display node-names ip** command. Note the node names and IP addresses of the C-LAN boards. In the compliance-tested configuration, two C-LAN boards (**CLAN-1A02** and **C-LAN-1B02**) were dedicated for H.323 endpoint (Avaya IP Telephones and IP Softphones, and AES Device and Media Control API stations) registration, and one C-LAN board (**C-LAN-1A06**) was enabled with Application Enablement Services to serve the AES link (see Step 4).

Notes:

1. Additional C-LAN boards may be enabled with Application Enablement Services so that the AES link may be spread across multiple C-LAN boards.
2. Although two C-LAN boards were dedicated for H.323 endpoint registration during compliance testing, actual configurations may dedicate more or fewer C-LAN boards for this purpose according to the number of expected H.323 endpoint registrations.

```
display node-names ip                                         Page   1 of   1
                                 IP NODE NAMES
    Name              IP Address
CLAN-1A02           192.45 .100.144
CLAN-1A06           192.45 .100.147
CLAN-1B02           192.45 .100.155
MEDPRO-1A03         192.45 .103.145
MEDPRO-1A13         192.45 .103.148
default             0   .0   .0   .0
procr                  .    .    .
```

Step	Description
4.	Enter the **change ip-services** command. On Page 1 of the **ip-services** form, configure entries for C-LAN boards that are not dedicated for H.323 endpoint registration as follows: • **Service Type –** set to "**AESVCS**". • **Enabled –** set to "**y**". • **Local Node –** set to the node name of the C-LAN. • **Local Port –** set to "**8765**".

```
change ip-services                                              Page   1 of   3

                                     IP SERVICES
 Service     Enabled     Local         Local        Remote       Remote
  Type                   Node          Port         Node         Port
AESVCS         y       CLAN-1A06       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 4.2 Step 3.

```
change ip-services                                              Page   3 of   3
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      AES-DevCon1      aespassword1          y        idle
      2:
      3:
      4:
      5:
      6:
      7:
      8:
      9:
     10:
     11:
     12:
     13:
     14:
     15:
     16:
```

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 of the **system-parameters customer-options** form, 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 required.

```
display system-parameters customer-options                    Page   6 of  10
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 3.0

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

Step	Description
2.	Enter the **add hunt-group n** command, where n is an unused hunt group number. On Page 1 of the **hunt group** form, 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 served by a queue. When **Vector** is enabled, the hunt group will be vector controlled.

```
add hunt-group 1                                              Page   1 of  61
                                  HUNT GROUP

            Group Number: 1                                ACD? y
              Group Name: Agent pool                     Queue? y
         Group Extension: 73000                         Vector? y
              Group Type: ucd-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.

```
add hunt-group 1                                              Page   2 of   3
                                  HUNT GROUP

                    Skill? y
                      AAS? n
                 Measured: internal
     Supervisor Extension:


      Controlling Adjunct: none






                                      Redirect on No Answer (rings): 3
                                                    Redirect to VDN:
                   Forced Entry of Stroke Counts or Call Work Codes? n
```

Step	Description
3.	Enter the **add agent-loginID p** command, where p is an extension valid under the provisioned dial plan. On Page 1 of the **agent-loginID** form, enter a descriptive **Name** and **Password**.

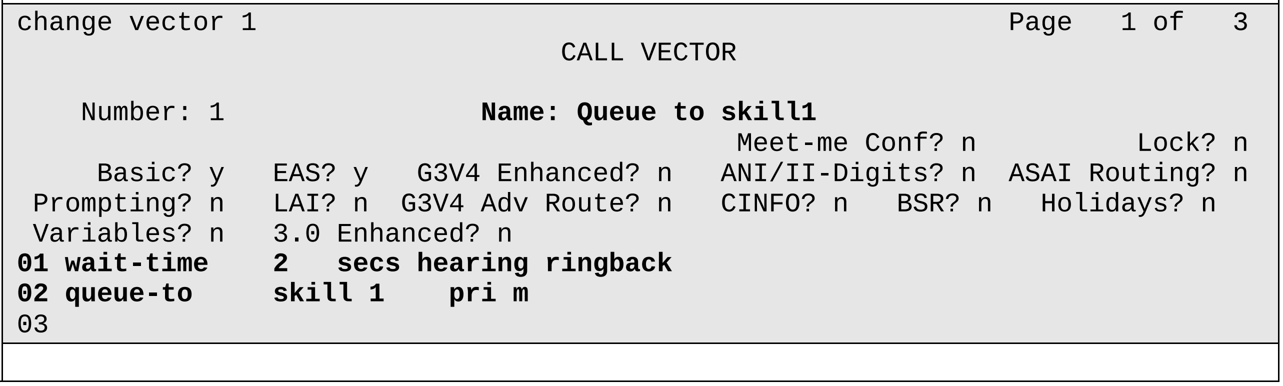
```
add agent-loginID 75001                                       Page   1 of   2
                                 AGENT LOGINID

                Login ID: 75001                                      AAS? n
                    Name: Agent-75001                              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: 12345
                                                  Password (enter again): 12345
                                                             Auto Answer: all
                                                       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 extensions.

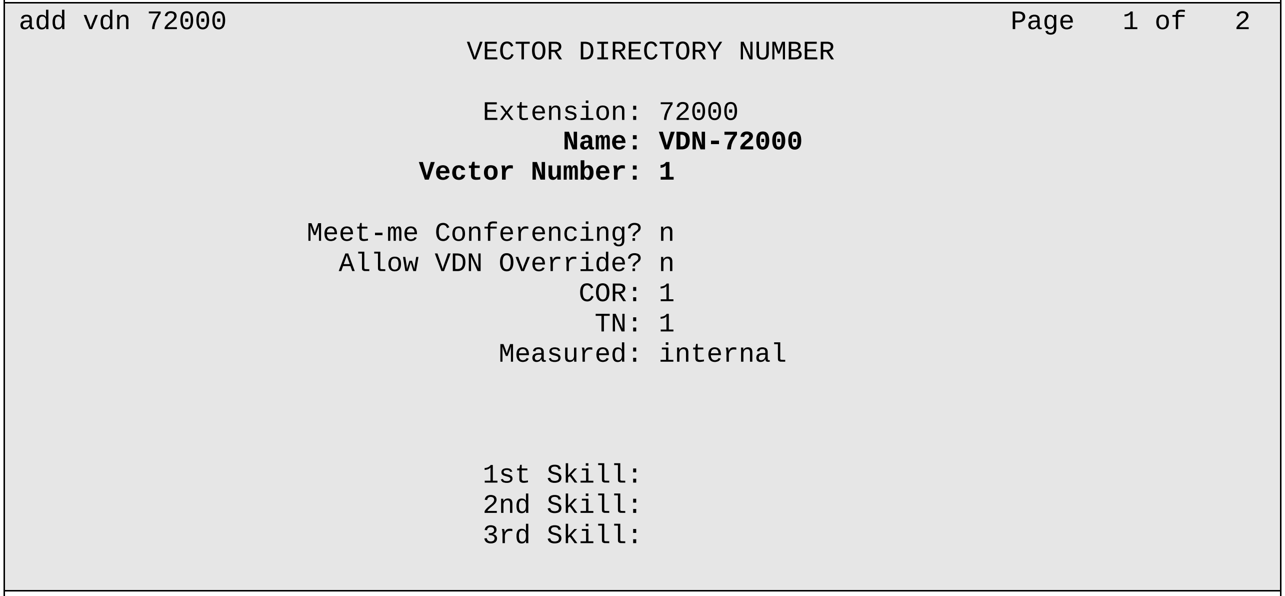
```
add agent-loginID 75001                                       Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:
Call Handling Preference: skill-level               Local Call Preference? n

    SN      SL          SN      SL          SN      SL          SN      SL
 1: 1       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:
```

Step	Description
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.



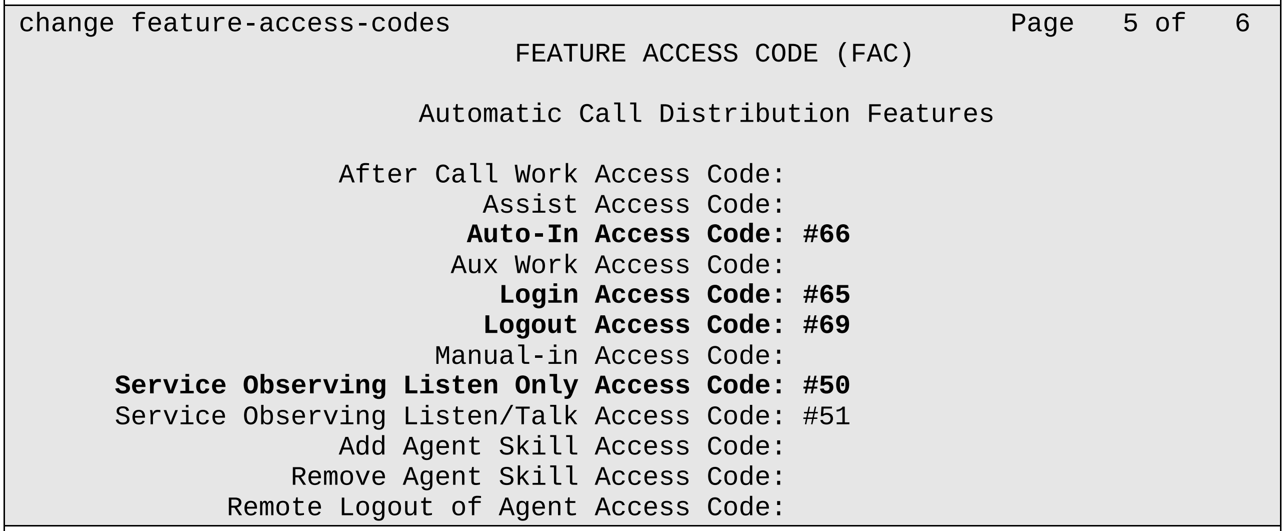
```
change vector 1                                               Page   1 of   3
                                  CALL VECTOR

    Number: 1                Name: Queue to skill1
                                             Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? n   ANI/II-Digits? n  ASAI Routing? n
 Prompting? n   LAI? n  G3V4 Adv Route? n   CINFO? n   BSR? n   Holidays? n
 Variables? n   3.0 Enhanced? n
01 wait-time    2   secs hearing ringback
02 queue-to     skill 1    pri m
03
```

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 the example below, incoming calls to the extension 72000 will be routed to VDN 72000, which in turn will invoke the actions specified in vector 1.



```
add vdn 72000                                                  Page   1 of   2
                           VECTOR DIRECTORY NUMBER

                            Extension: 72000
                                 Name: VDN-72000
                        Vector Number: 1

                 Meet-me Conferencing? n
                   Allow VDN Override? n
                                  COR: 1
                                   TN: 1
                             Measured: internal



                            1st Skill:
                            2nd Skill:
                            3rd Skill:
```

Step	Description
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**[1].

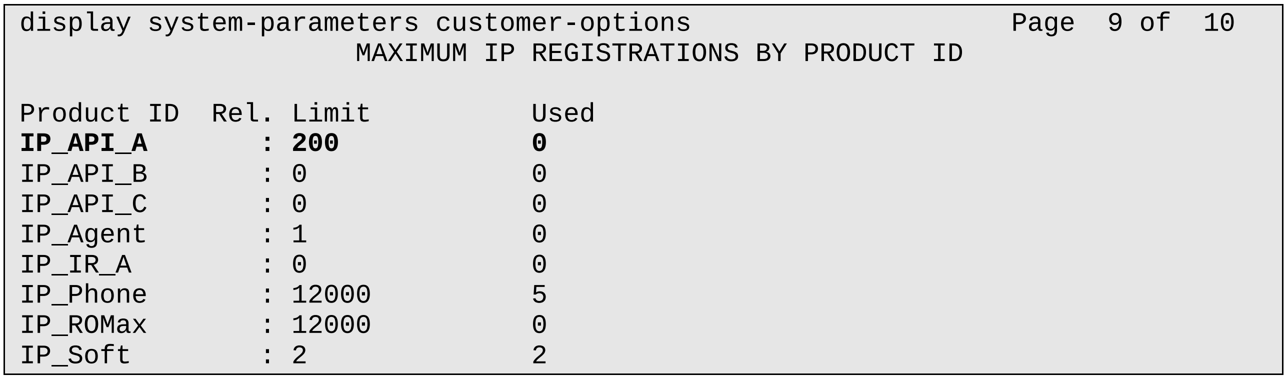


```
change feature-access-codes                                    Page   5 of   6
                              FEATURE ACCESS CODE (FAC)

                        Automatic Call Distribution Features

                   After Call Work Access Code:
                            Assist Access Code:
                           Auto-In Access Code: #66
                          Aux Work Access Code:
                             Login Access Code: #65
                            Logout Access Code: #69
                         Manual-in Access Code:
      Service Observing Listen Only Access Code: #50
      Service Observing Listen/Talk Access Code: #51
                   Add Agent Skill Access Code:
                Remove Agent Skill Access Code:
             Remote Logout of Agent Access Code:
```

[1] Audiolog on-demand recording uses the Service Observing Listen Only Access Code (see Section 5 Step 4).

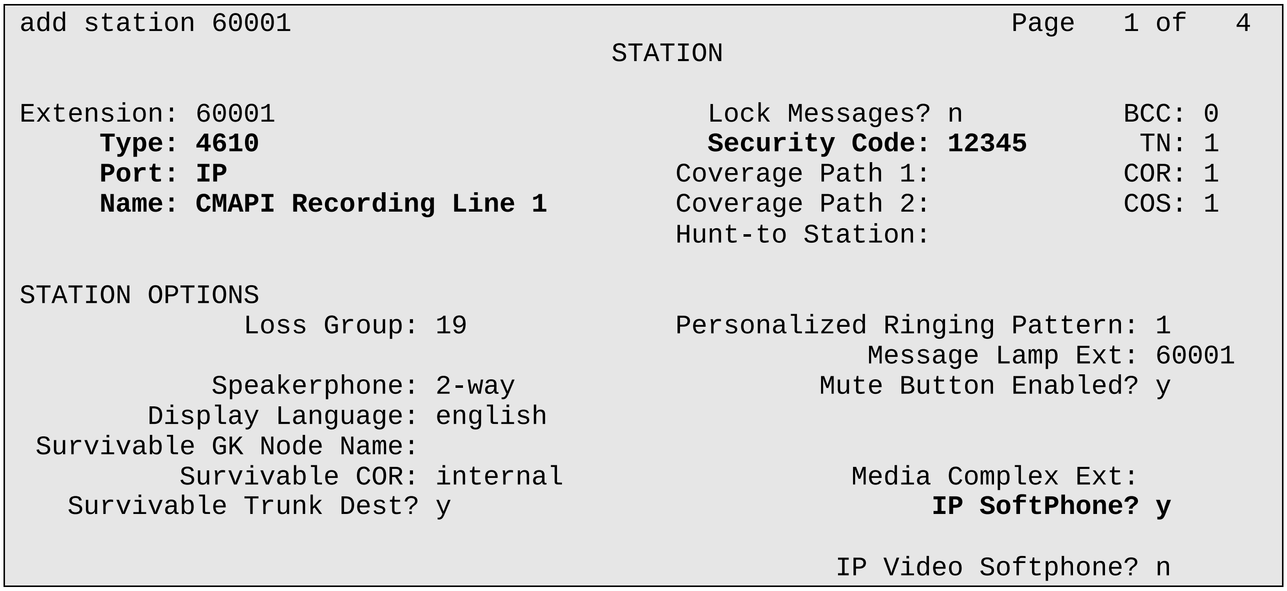
3.3. Recording Ports

The recording ports in this configuration are AES Device and Media Control API stations that essentially appear as IP softphones 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. 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  9 of  10
                     MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit          Used
IP_API_A       : 200            0
IP_API_B       : 0              0
IP_API_C       : 0              0
IP_Agent       : 1              0
IP_IR_A        : 0              0
IP_Phone       : 12000          5
IP_ROMax       : 12000          0
IP_Soft        : 2              2
```

Enter the **add station s** command, where s is an extension valid under the provisioned dial plan. On Page 1 of the **station** form, set **Type** to an IP or Digital telephone set type, set **Port** to **IP**, enter a descriptive **Name**, specify the **Security Code**, and set **IP SoftPhone** to “**y.**” Repeat this as necessary, with the same **Security Code**[2], to configure additional AES Device and Media Control API stations.



```
add station 60001                                              Page   1 of   4
                                     STATION

Extension: 60001                          Lock Messages? n         BCC: 0
     Type: 4610                           Security Code: 12345      TN: 1
     Port: IP                           Coverage Path 1:           COR: 1
     Name: CMAPI Recording Line 1       Coverage Path 2:           COS: 1
                                        Hunt-to Station:

STATION OPTIONS
              Loss Group: 19            Personalized Ringing Pattern: 1
                                                    Message Lamp Ext: 60001
            Speakerphone: 2-way                  Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal                 Media Complex Ext:
   Survivable Trunk Dest? y                             IP SoftPhone? y

                                                  IP Video Softphone? n
```

[2] Not a strict requirement, but would simplify recording channel configuration in Audiolog. See Section 5 Step 7.

3.4. Recorded Stations

The stations that were recorded during the compliance testing include analog, digital, and IP telephones and Avaya IP Softphones in both Road Warrior mode and Telecommuter mode. The extensions used were in the ranges 50001 – 50016, 50101 – 50228, and 51001 – 51002.

3.5. Codec Configuration

Enter the **change ip-codec-set t** command, where t is a number between 1 and 7, inclusive. In the first row, enter a codec for **Audio Codec**. "**G711MU**" was used during compliance testing; the Mercom Audiolog server also supports G.711A, G.729A, and G.723 and is able to automatically detect the codec in the RTP stream.

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

                          IP Codec Set

    Codec Set: 1

    Audio      Silence      Frames   Packet
    Codec      Suppression  Per Pkt  Size(ms)
 1: G.711MU         n         2        20
 2:
 3:
 4:
 5:
 6:
 7:
```

3.6. IP Network Regions

During compliance testing, the two C-LAN boards dedicated for H.323 endpoint registration were assigned to IP network region 3. The Avaya IP telephones and IP Softphones, as well as the AES Device and Media Control API stations used by Audiolog, registered with those C-LAN boards and were thus also assigned to IP network region 3. Furthermore, two MedPro boards were also assigned to IP network region 3. One consequence of assigning the aforementioned IP telephones, IP Softphones, AES Device and Media Control API stations, and MedPro boards to a common IP network region[3] is that the RTP traffic between them is governed by the same codec set. Other configurations where multiple IP network regions are utilized are possible, as long as careful consideration is given to the assignment of codec sets between IP network regions.

[3] The assignment of IP network regions on C-LAN and MedPro boards is configured using the **change ip-interface** SAT command.

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

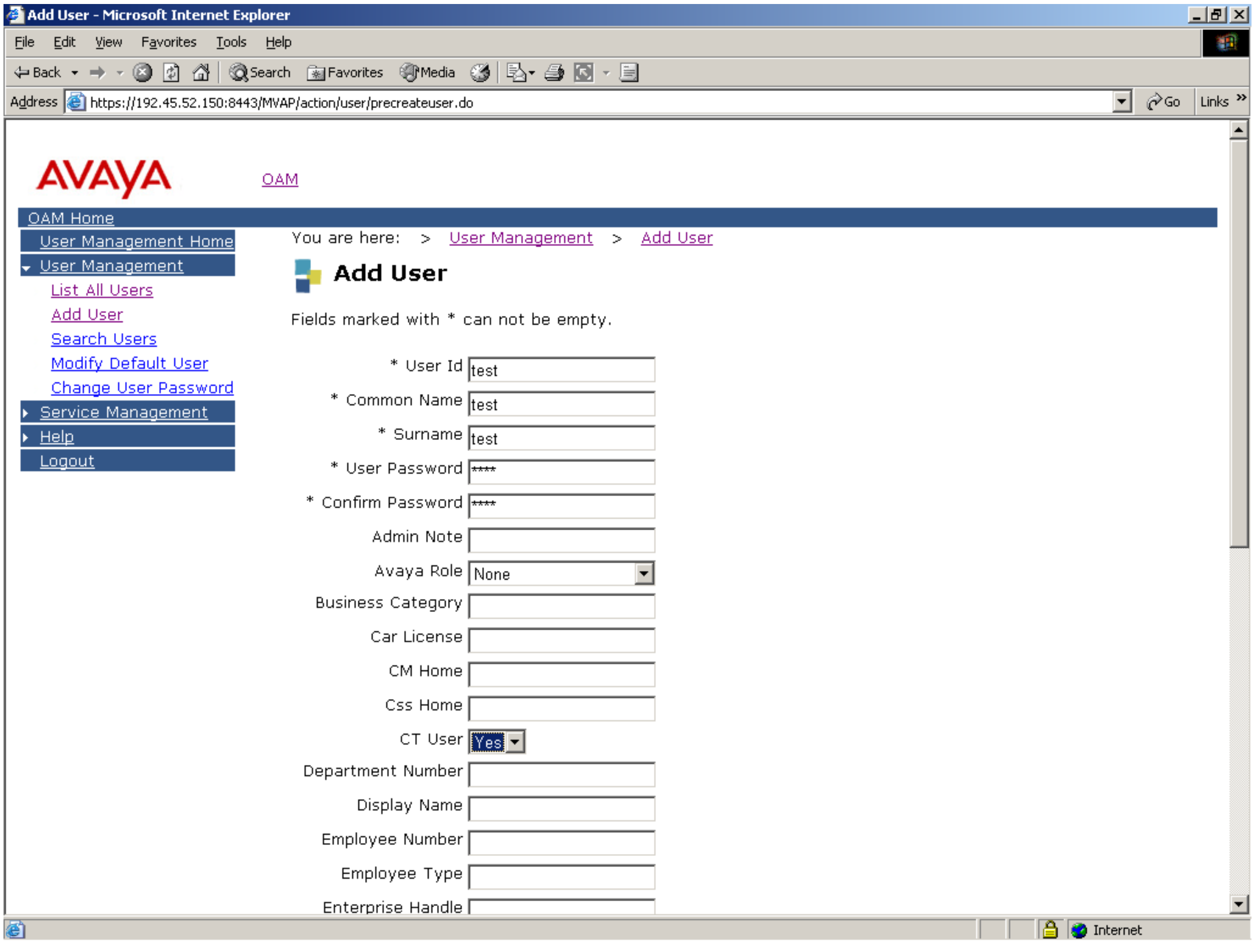
```
change ip-network-region 3                                  Page   1 of  19
                               IP NETWORK REGION
  Region: 3
Location:         Authoritative Domain:
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 3028
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? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

4. Configure Avaya Application Enablement Services

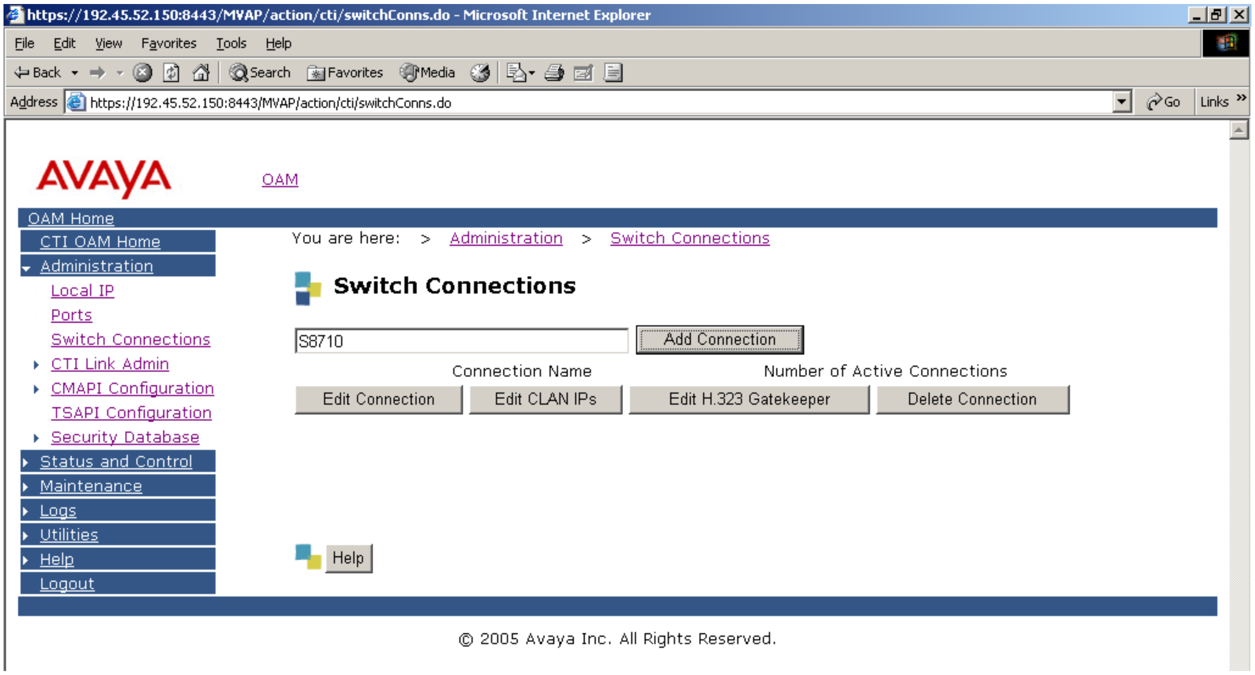
This section assumes that installation and basic administration of an Avaya Application Enablement Services server has been performed. Consult [1] for further guidance. The steps in this section describe the configuration of a TSAPI CTI user for Mercom Audiolog, a "Switch Connection" to Avaya Communication Manager, and a TSAPI CTI link.

4.1. User Management

Step	Description
1.	Launch a web browser, enter https://<IP address of AES server>:8443/MVAP in the URL, and log in with the appropriate credentials for accessing the AES User Management pages.

Step	Description
2.	Click on **User Management**, then **User Management → Add User** in the left pane. Configure the asterisked fields and set **CT User** to "**Yes**". Audiolog will use this **User Id** and **Password** to access the AES server. Scroll down to the bottom of the page and click on "**Apply**".  Add User - Microsoft Internet Explorer Address https://192.45.52.150:8443/MVAP/action/user/precreateuser.do OAM OAM Home User Management Home User Management List All Users Add User Search Users Modify Default User Change User Password Service Management Help Logout You are here: > User Management > Add User Add User Fields marked with * can not be empty. * User Id: test * Common Name: test * Surname: test * User Password: **** * Confirm Password: **** Admin Note: Avaya Role: None Business Category: Car License: CM Home: Css Home: CT User: Yes Department Number: Display Name: Employee Number: Employee Type: Enterprise Handle: Internet

4.2. CTI OAM Admin

Step	Description
1.	Launch a web browser, enter https://<IP address of AES server>:8443/MVAP in the URL, and log in with the appropriate credentials for accessing the AES CTI OAM pages.
2.	Click on **CTI OAM Home → Administration → Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the AES server and Avaya Communication Manager. Enter a descriptive name for the Switch Connection and click on "**Add Connection**". 

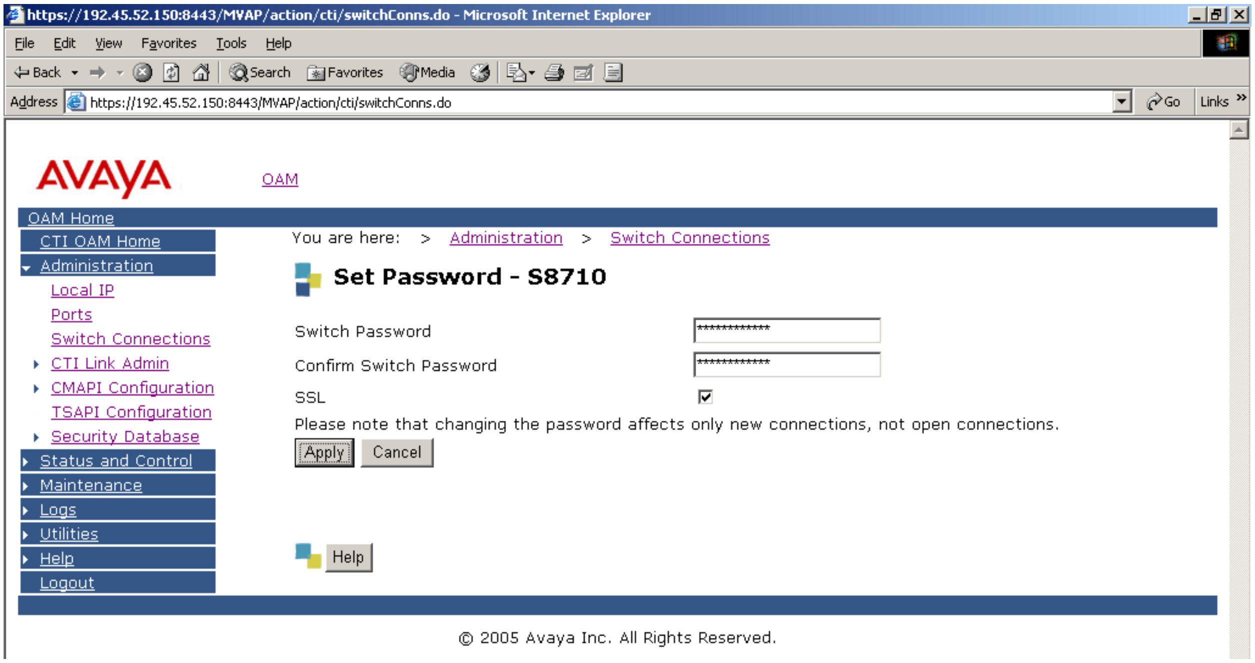
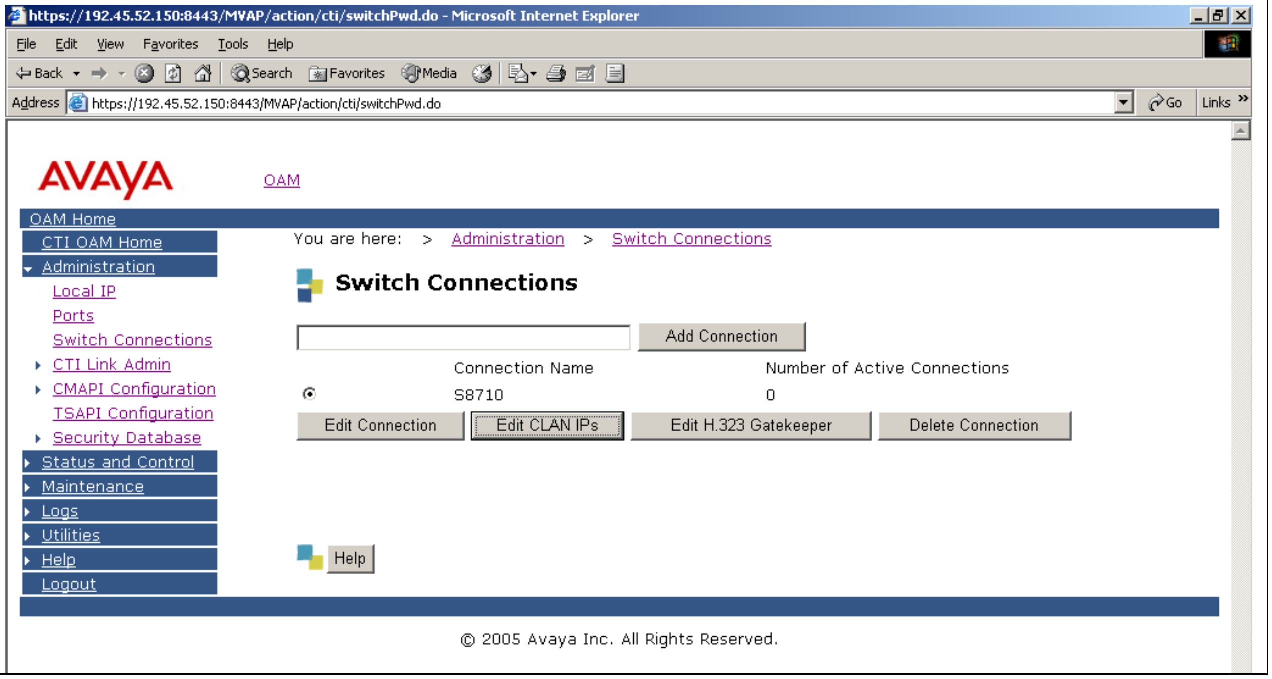
https://192.45.52.150:8443/MVAP/action/cti/switchConns.do - Microsoft Internet Explorer

Address: https://192.45.52.150:8443/MVAP/action/cti/switchConns.do

You are here: > Administration > Switch Connections

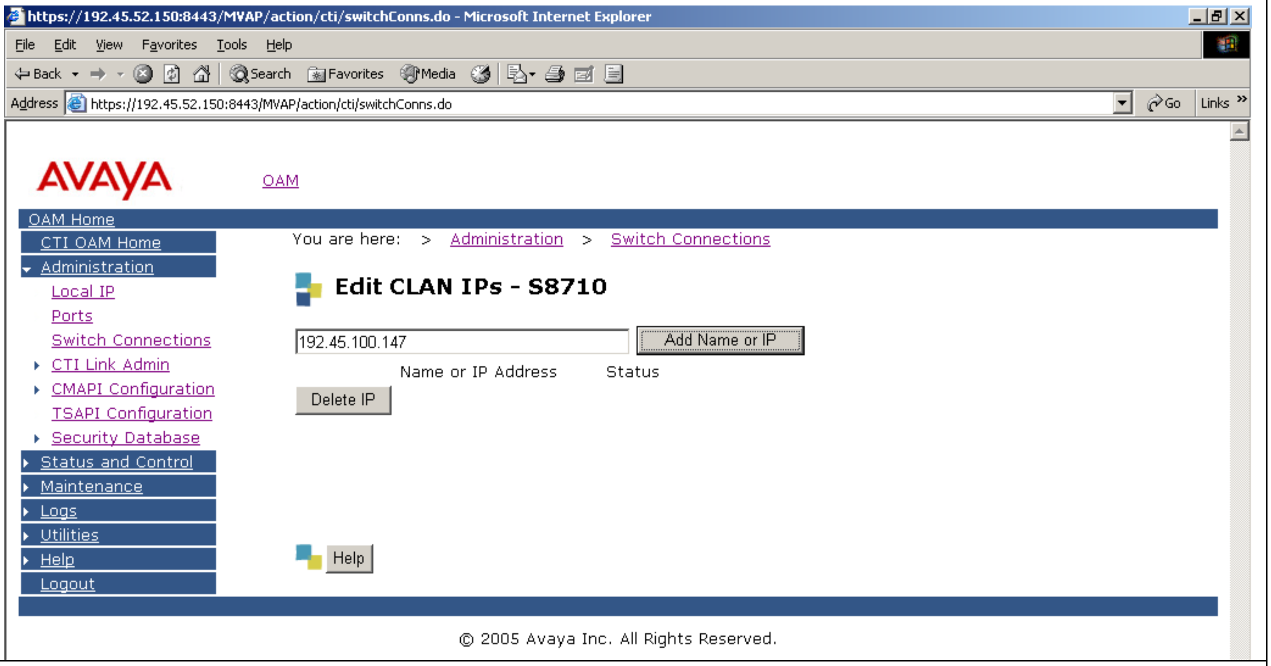
Switch Connections

S8710 — Add Connection

Step	Description
3.	The next window that appears prompts for the Switch Connection password. Enter the same password that was administered on Avaya Communication Manager in Section 3.1 Step 4. Click on "**Apply**".  https://192.45.52.150:8443/MVAP/action/cti/switchConns.do - Microsoft Internet Explorer Address https://192.45.52.150:8443/MVAP/action/cti/switchConns.do You are here: > Administration > Switch Connections Set Password - S8710 Switch Password ************ Confirm Switch Password ************ SSL ☑ Please note that changing the password affects only new connections, not open connections. Apply Cancel © 2005 Avaya Inc. All Rights Reserved. OAM Home CTI OAM Home Administration Local IP Ports Switch Connections CTI Link Admin CMAPI Configuration TSAPI Configuration Security Database Status and Control Maintenance Logs Utilities Help Logout
4.	After returning to the Switch Connections page, select the radio button corresponding to the switch connection added in Steps 2 – 3, and click on "**Edit CLAN IPs**".  https://192.45.52.150:8443/MVAP/action/cti/switchPwd.do - Microsoft Internet Explorer Address https://192.45.52.150:8443/MVAP/action/cti/switchPwd.do You are here: > Administration > Switch Connections Switch Connections Add Connection Connection Name: S8710 ● Number of Active Connections: 0 Edit Connection Edit CLAN IPs Edit H.323 Gatekeeper Delete Connection © 2005 Avaya Inc. All Rights Reserved. OAM Home CTI OAM Home Administration Local IP Ports Switch Connections CTI Link Admin CMAPI Configuration TSAPI Configuration Security Database Status and Control Maintenance Logs Utilities Help Logout

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td><b>5.</b></td><td>

Enter the IP address of a C-LAN board enabled with Application Enablement Services (see Section 3.1 Step 4) and click on “**Add Name or IP**”. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.



https://192.45.52.150:8443/MVAP/action/cti/switchConns.do - Microsoft Internet Explorer

Address https://192.45.52.150:8443/MVAP/action/cti/switchConns.do

You are here: > Administration > Switch Connections

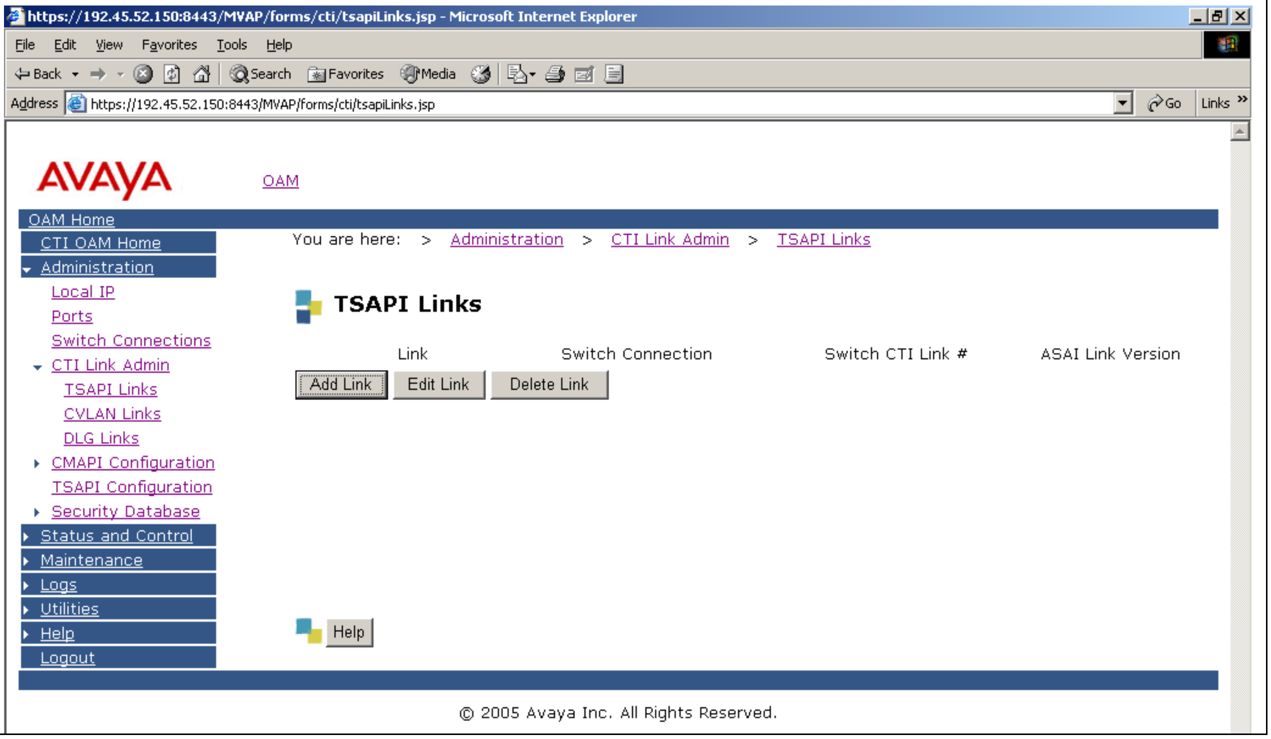
Edit CLAN IPs - S8710

192.45.100.147

© 2005 Avaya Inc. All Rights Reserved.

</td></tr>
<tr><td><b>6.</b></td><td>

Under **Administration** in the left pane, click on **CTI Link Admin → TSAPI Links**. Click on “**Add Link**”.



https://192.45.52.150:8443/MVAP/forms/cti/tsapiLinks.jsp - Microsoft Internet Explorer

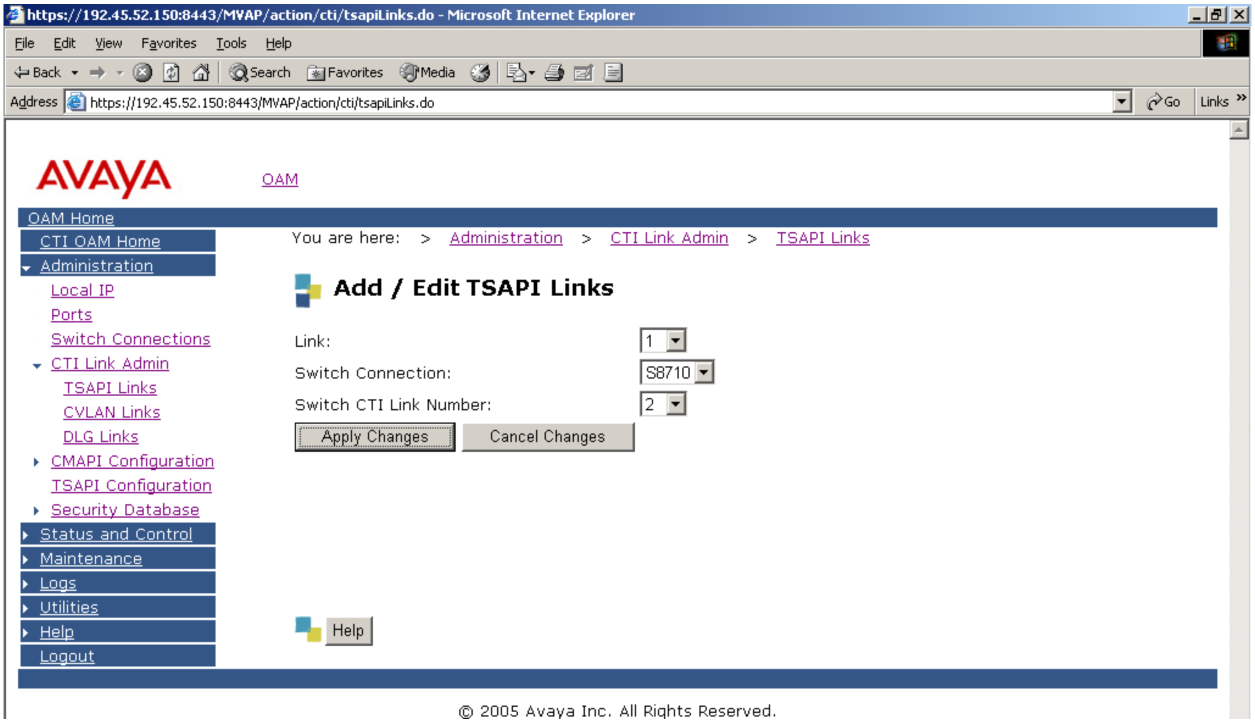
Address https://192.45.52.150:8443/MVAP/forms/cti/tsapiLinks.jsp

You are here: > Administration > CTI Link Admin > TSAPI Links

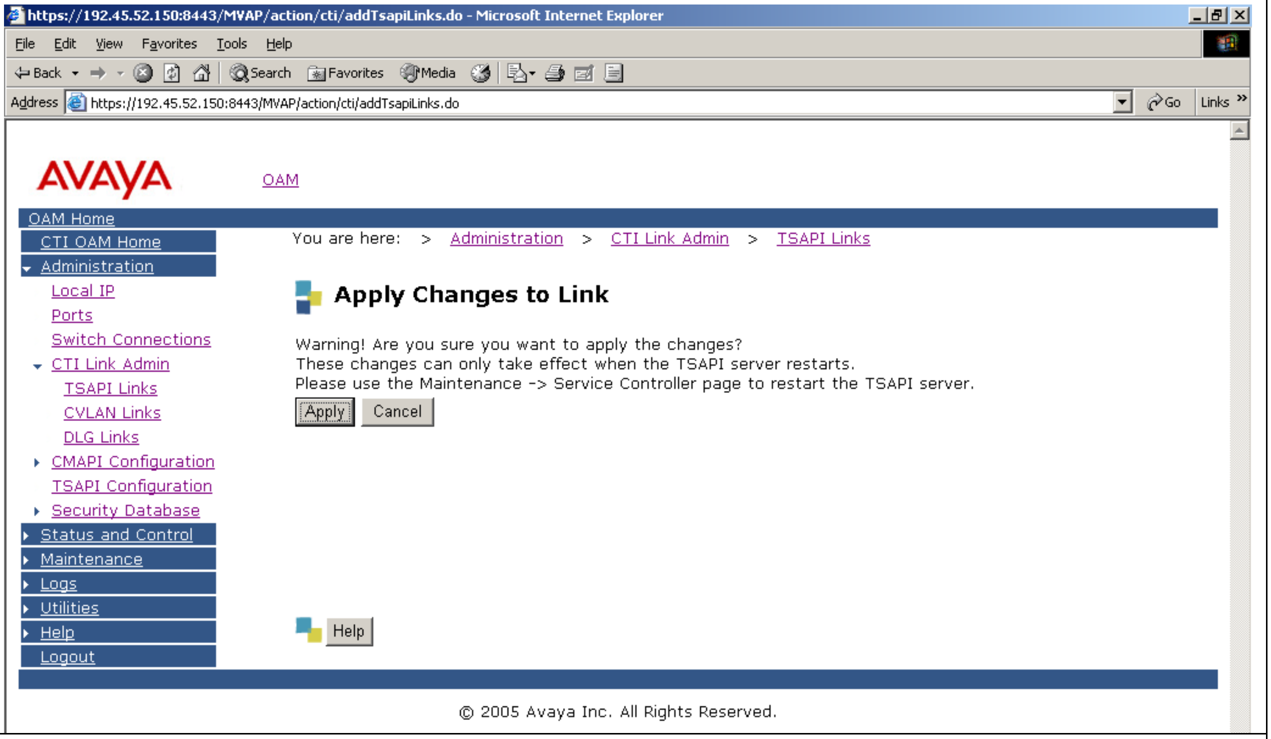
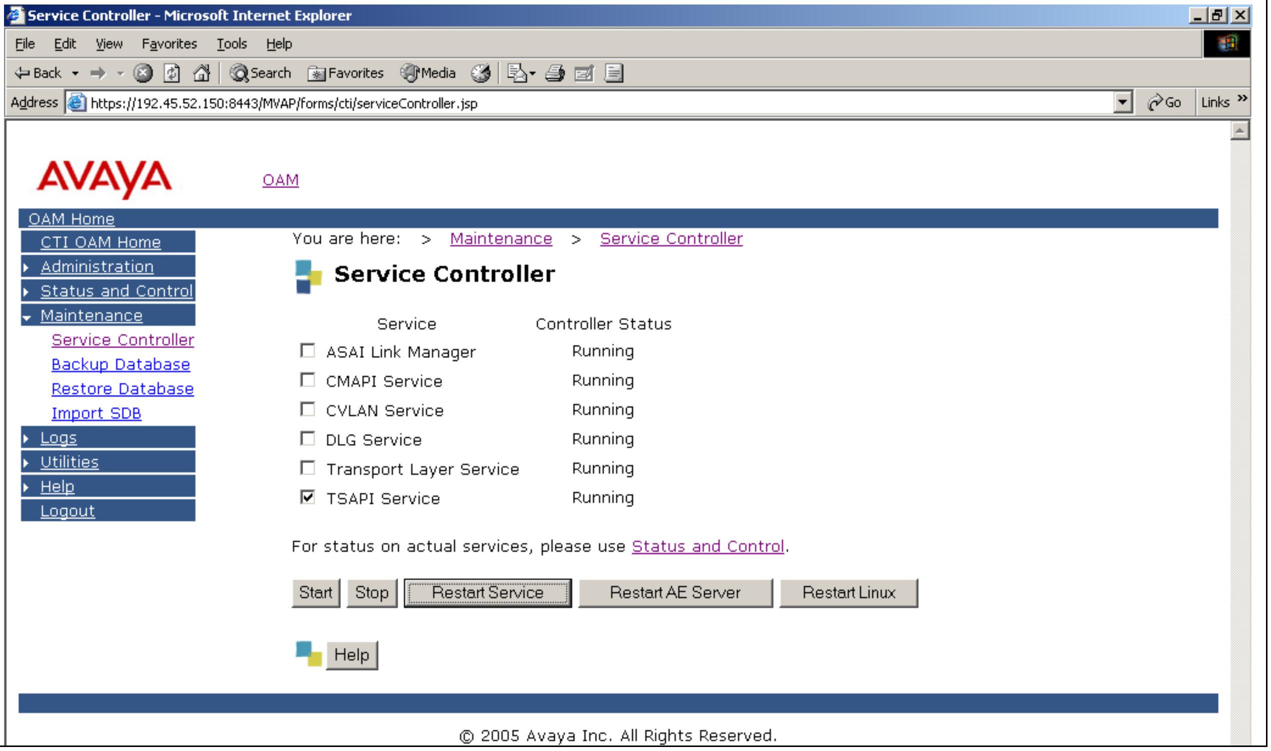
TSAPI Links

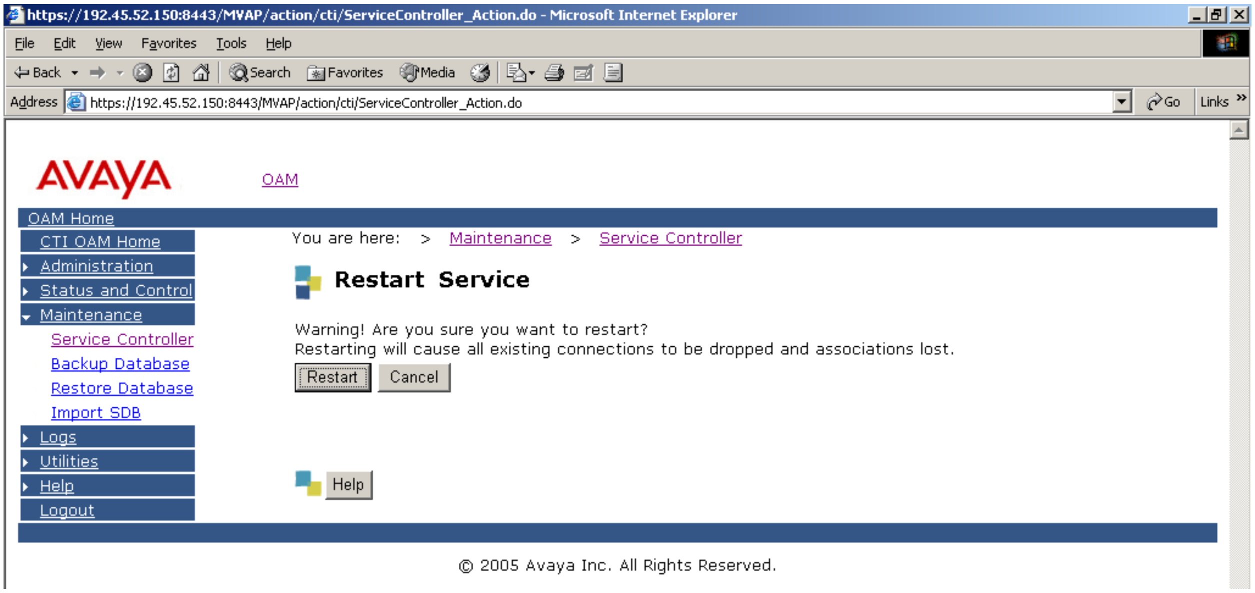
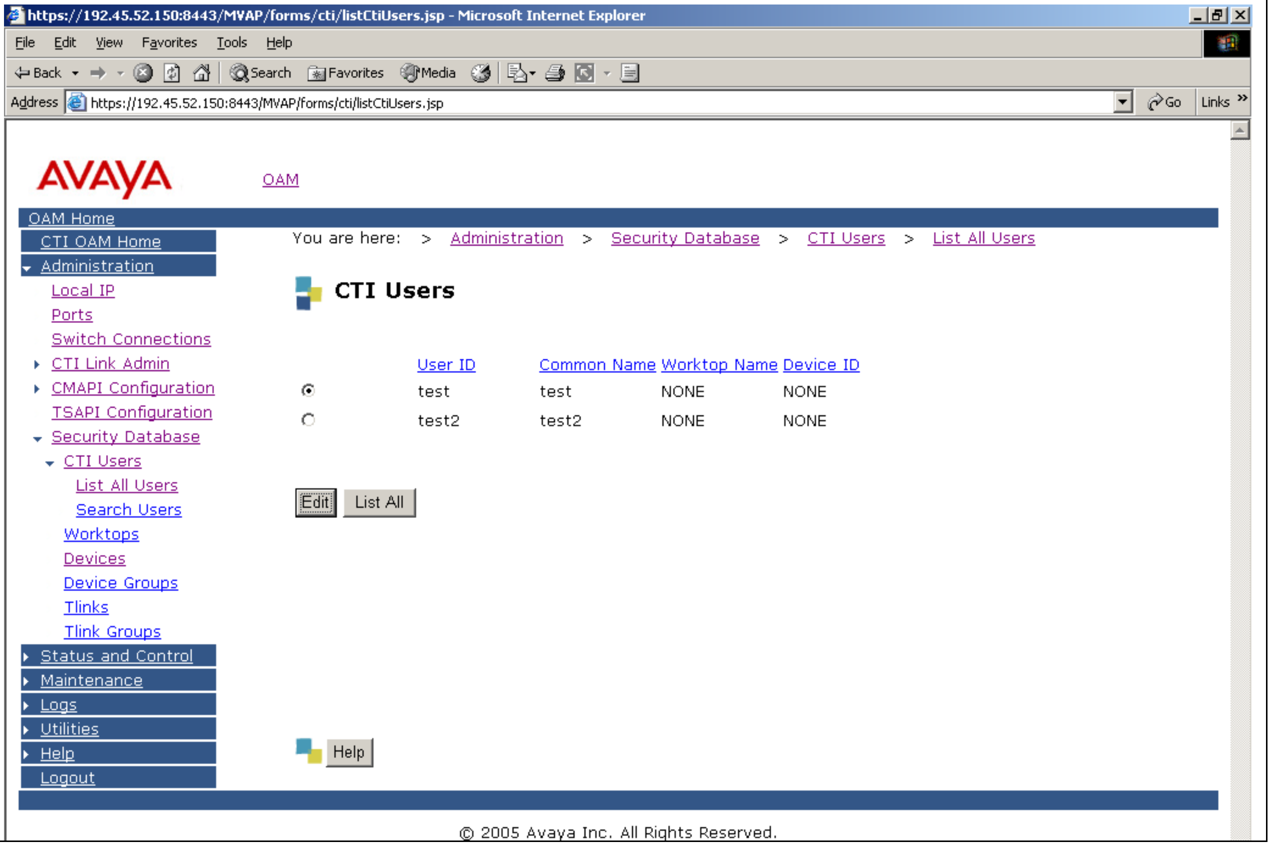
© 2005 Avaya Inc. All Rights Reserved.

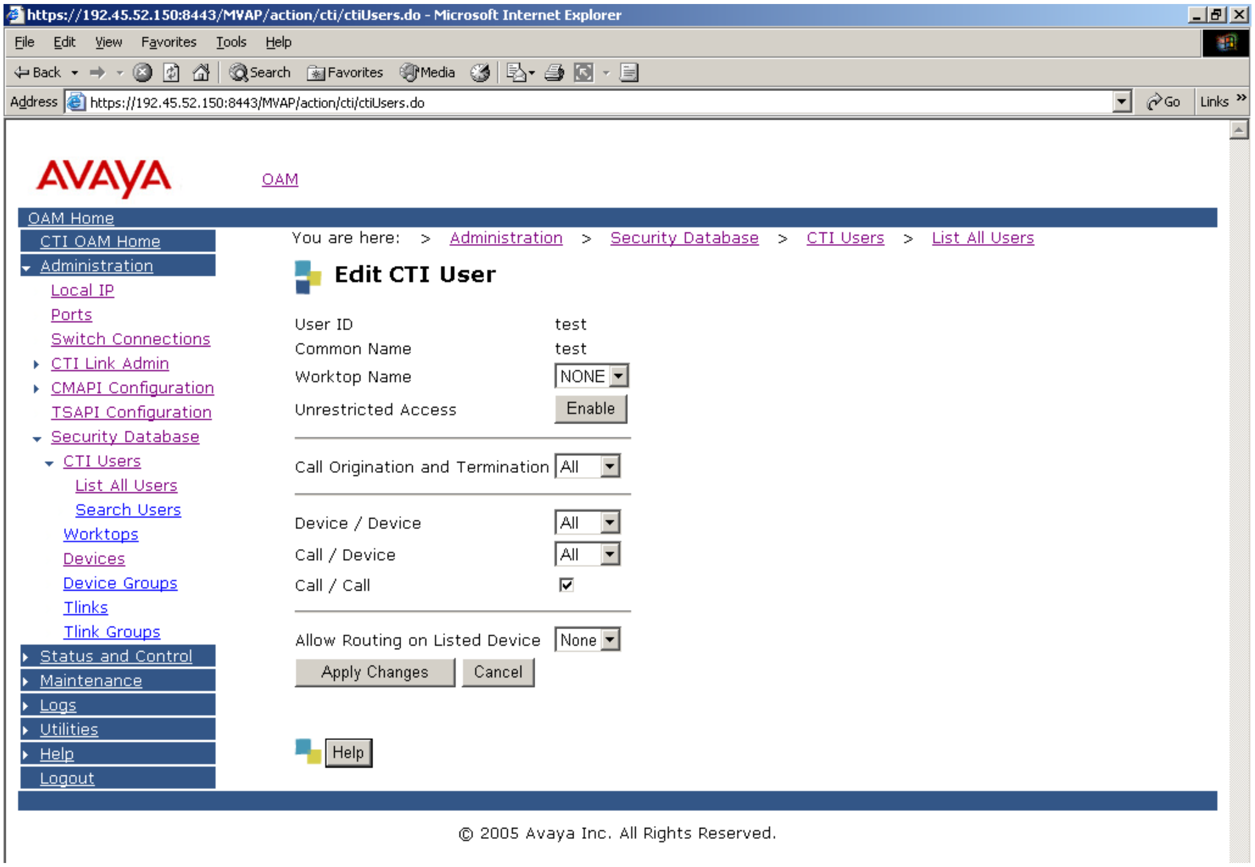
</td></tr>
</table>

Step	Description
7.	Set **Switch Connection** to the switch connection added in Steps 2 – 3 and **Switch CTI Link Number** to the CTI link number configured on Avaya Communication Manager in Section 3.1 Step 2. The TSAPI **Link** field is locally significant to this AES server only and may be set to any unused value. Click on "**Apply Changes**".  Add / Edit TSAPI Links Link: 1 Switch Connection: S8710 Switch CTI Link Number: 2

https://192.45.52.150:8443/MVAP/action/cti/tsapiLinks.do - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://192.45.52.150:8443/MVAP/action/cti/tsapiLinks.do
Go Links
OAM
OAM Home
CTI OAM Home
Administration
Local IP
Ports
Switch Connections
CTI Link Admin
TSAPI Links
CVLAN Links
DLG Links
CMAPI Configuration
TSAPI Configuration
Security Database
Status and Control
Maintenance
Logs
Utilities
Help
Logout
You are here: > Administration > CTI Link Admin > TSAPI Links
Apply Changes
Cancel Changes
Help
© 2005 Avaya Inc. All Rights Reserved.

Step	Description
8.	Click on **Apply** to confirm the changes.  https://192.45.52.150:8443/MVAP/action/cti/addTsapiLinks.do - Microsoft Internet Explorer Address https://192.45.52.150:8443/MVAP/action/cti/addTsapiLinks.do You are here: > Administration > CTI Link Admin > TSAPI Links **Apply Changes to Link** Warning! Are you sure you want to apply the changes? These changes can only take effect when the TSAPI server restarts. Please use the Maintenance -> Service Controller page to restart the TSAPI server. © 2005 Avaya Inc. All Rights Reserved. File Edit View Favorites Tools Help Back Search Favorites Media Go Links AVAYA OAM OAM Home CTI OAM Home Administration Local IP Ports Switch Connections CTI Link Admin TSAPI Links CVLAN Links DLG Links CMAPI Configuration TSAPI Configuration Security Database Status and Control Maintenance Logs Utilities Help Logout Apply Cancel Help
9.	Under **Maintenance** in the left pane, click on **Service Controller**. Check the "**TSAPI Service**" checkbox and click on "**Restart Service**".  Service Controller - Microsoft Internet Explorer Address https://192.45.52.150:8443/MVAP/forms/cti/serviceController.jsp You are here: > Maintenance > Service Controller **Service Controller** Service Controller Status □ ASAI Link Manager Running □ CMAPI Service Running □ CVLAN Service Running □ DLG Service Running □ Transport Layer Service Running ☑ TSAPI Service Running For status on actual services, please use Status and Control. © 2005 Avaya Inc. All Rights Reserved. File Edit View Favorites Tools Help Back Search Favorites Media Go Links AVAYA OAM OAM Home CTI OAM Home Administration Status and Control Maintenance Service Controller Backup Database Restore Database Import SDB Logs Utilities Help Logout Start Stop Restart Service Restart AE Server Restart Linux Help

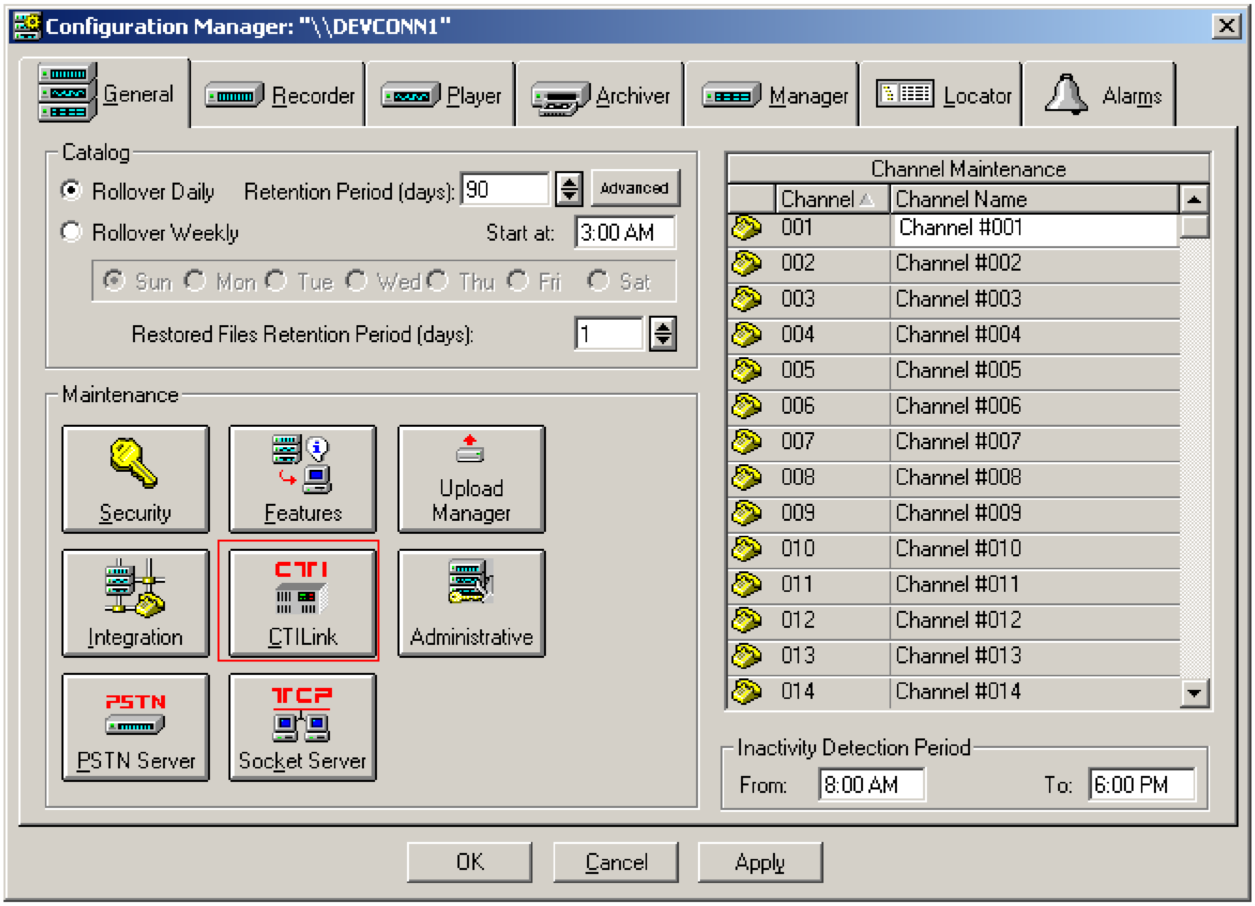
Step	Description
10.	Click on “**Restart**” to confirm the restart.  https://192.45.52.150:8443/MVAP/action/cti/ServiceController_Action.do - Microsoft Internet Explorer Address https://192.45.52.150:8443/MVAP/action/cti/ServiceController_Action.do You are here: > Maintenance > Service Controller Restart Service Warning! Are you sure you want to restart? Restarting will cause all existing connections to be dropped and associations lost. Restart Cancel Help © 2005 Avaya Inc. All Rights Reserved. File Edit View Favorites Tools Help Back Search Favorites Media Go Links AVAYA OAM OAM Home CTI OAM Home Administration Status and Control Maintenance Service Controller Backup Database Restore Database Import SDB Logs Utilities Help Logout
11.	Under **Administration** in the left pane, click on **Security Database → CTI Users → List All Users**. Select the **User ID** created in Section 4.1 Step 2 and click on “**Edit**”.  https://192.45.52.150:8443/MVAP/forms/cti/listCtiUsers.jsp - Microsoft Internet Explorer Address https://192.45.52.150:8443/MVAP/forms/cti/listCtiUsers.jsp You are here: > Administration > Security Database > CTI Users > List All Users CTI Users User ID Common Name Worktop Name Device ID ● test test NONE NONE ○ test2 test2 NONE NONE Edit List All Help © 2005 Avaya Inc. All Rights Reserved. File Edit View Favorites Tools Help Back Search Favorites Media Go Links AVAYA OAM OAM Home CTI OAM Home Administration Local IP Ports Switch Connections CTI Link Admin CMAPI Configuration TSAPI Configuration Security Database CTI Users List All Users Search Users Worktops Devices Device Groups Tlinks Tlink Groups Status and Control Maintenance Logs Utilities Help Logout

Step	Description
12.	Assign access rights and call/device privileges according to customer requirements. For convenience, **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 on **Apply Changes**.  https://192.45.52.150:8443/MVAP/action/cti/ctiUsers.do - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Media Address https://192.45.52.150:8443/MVAP/action/cti/ctiUsers.do Go Links AVAYA OAM OAM Home CTI OAM Home Administration Local IP Ports Switch Connections CTI Link Admin CMAPI Configuration TSAPI Configuration Security Database CTI Users List All Users Search Users Worktops Devices Device Groups Tlinks Tlink Groups Status and Control Maintenance Logs Utilities Help Logout © 2005 Avaya Inc. All Rights Reserved. You are here: > Administration > Security Database > CTI Users > List All Users **Edit CTI User** User ID: test Common Name: test Worktop Name: NONE Unrestricted Access: [Enable] Call Origination and Termination: All Device / Device: All Call / Device: All Call / Call: ☑ Allow Routing on Listed Device: None [Apply Changes] [Cancel] [Help]

5. Configure Mercom Audiolog

The steps in this section describe the configuration of CTI settings, stations/agents to be recorded full time, and recording stations on Mercom Audiolog. Consult Mercom documentation for instruction on administering and using scheduled and on-demand recording.

Step	Description
1.	On the Mercom Audiolog Call Recording Server, launch the Configuration Manager.

Step	Description
2.	In the **General** tab, click on the “**CTILink**” icon. 

Configuration Manager: "\\DEVCONN1"

Catalog

● Rollover Daily Retention Period (days): 90 Advanced

○ Rollover Weekly Start at: 3:00 AM

● Sun ○ Mon ○ Tue ○ Wed ○ Thu ○ Fri ○ Sat

Restored Files Retention Period (days): 1

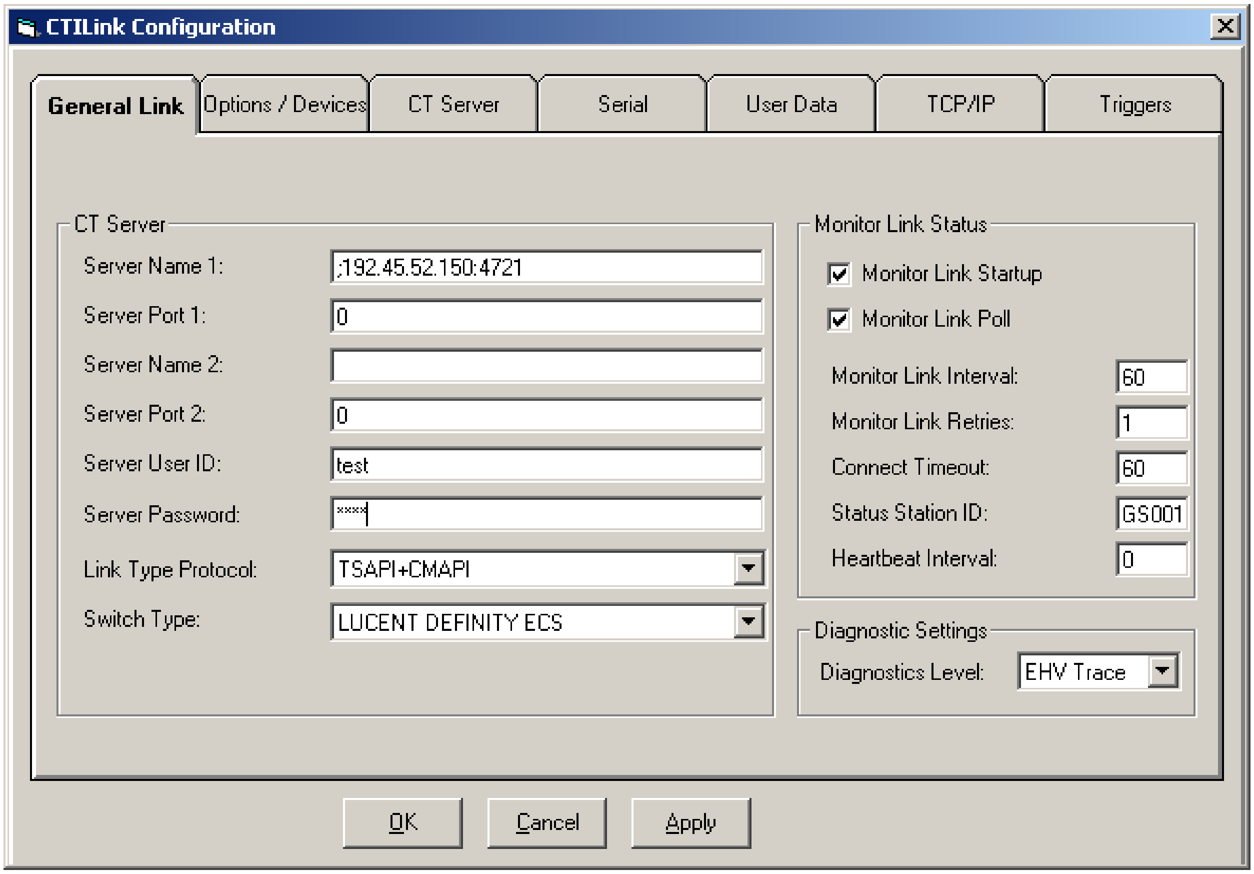
Maintenance

Channel Maintenance

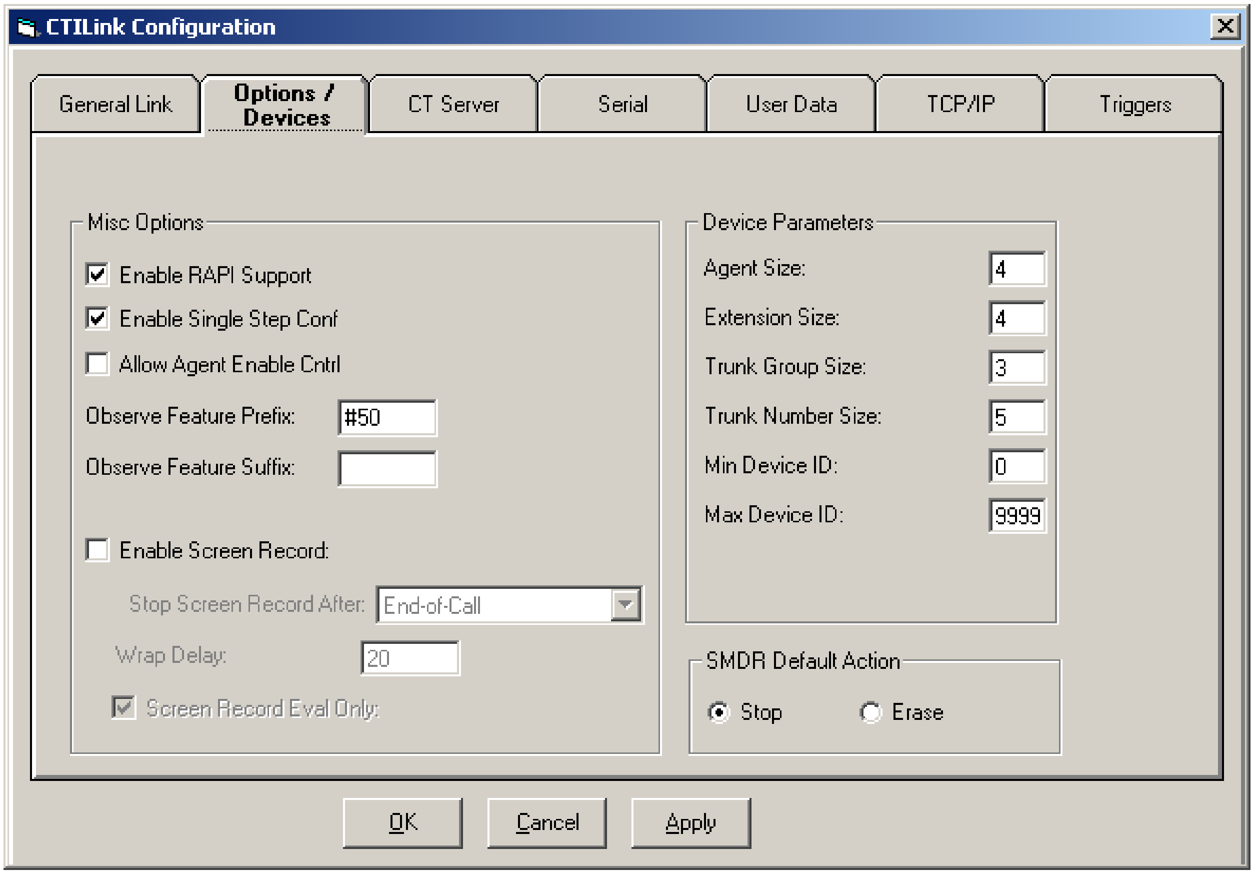
Channel	Channel Name
001	Channel #001
002	Channel #002
003	Channel #003
004	Channel #004
005	Channel #005
006	Channel #006
007	Channel #007
008	Channel #008
009	Channel #009
010	Channel #010
011	Channel #011
012	Channel #012
013	Channel #013
014	Channel #014

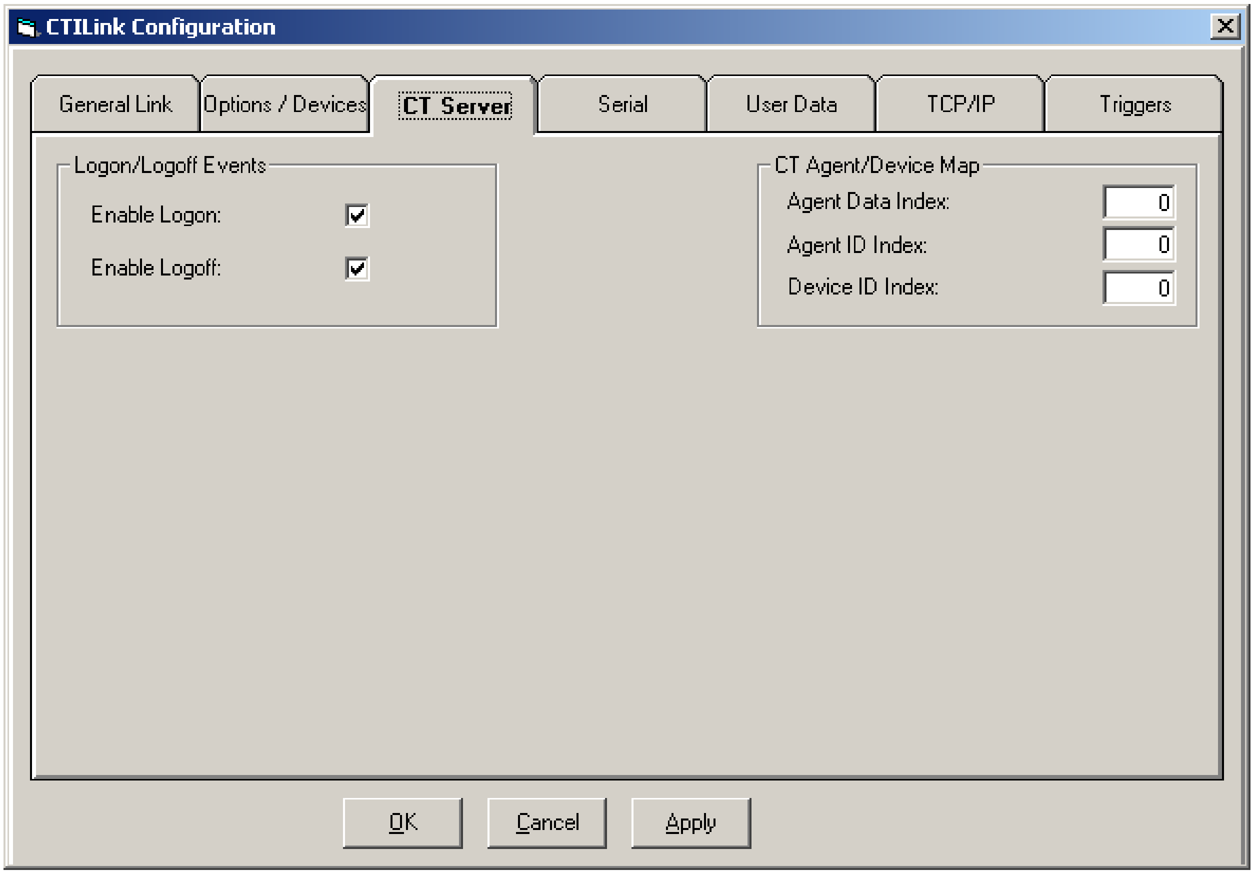
Inactivity Detection Period

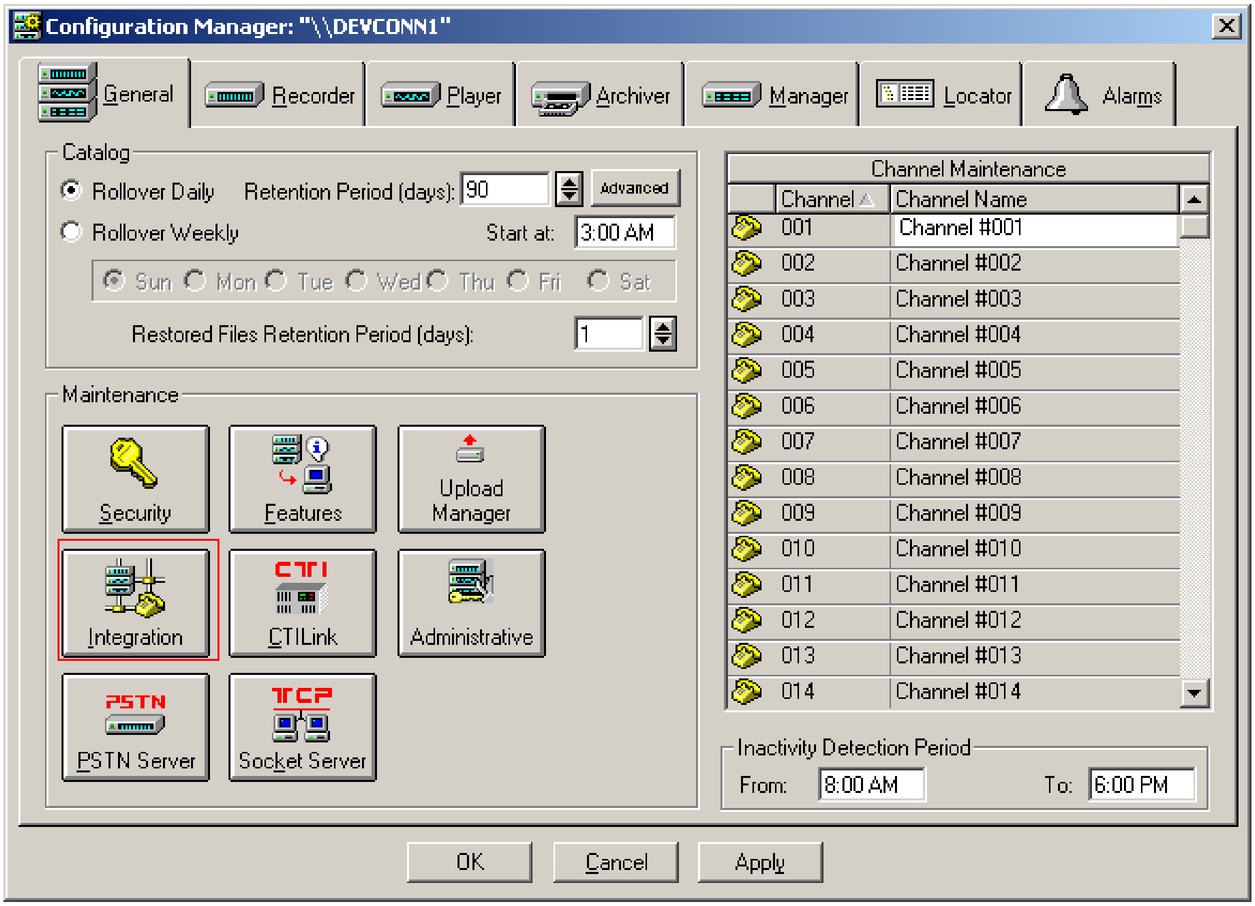
From: 8:00 AM To: 6:00 PM

Step	Description
3.	In the **General Link** tab, configure the following: • **Server Name 1** – set to the AES server client connectivity IP address[4] and port 4721. In the example below, the value "**;192.45.52.150:4721**" was entered. • **Server User ID** and **Server Password** – set to the user ID and password configured in Section 4.1**.** • **Link Type Protocol** – set to "**TSAPI+CMAPI**". • **Switch Type** - set to "**LUCENT DEFINITY ECS**".  CTILink Configuration General Link Options / Devices CT Server Serial User Data TCP/IP Triggers OK Cancel Apply CT Server Server Name 1: ;192.45.52.150:4721 Server Port 1: 0 Server Name 2: Server Port 2: 0 Server User ID: test Server Password: **** Link Type Protocol: TSAPI+CMAPI Switch Type: LUCENT DEFINITY ECS Monitor Link Status ☑ Monitor Link Startup ☑ Monitor Link Poll Monitor Link Interval: 60 Monitor Link Retries: 1 Connect Timeout: 60 Status Station ID: GS001 Heartbeat Interval: 0 Diagnostic Settings Diagnostics Level: EHV Trace

[4] The AES server client connectivity IP address may be obtained by clicking on **CTI OAM Admin -> Administration -> Local IP** in the AES CTI OAM page.

Step	Description
4.	Click on the **Options / Devices** tab. Check the checkboxes for "**Enable RAPI Support**" and "**Enable Single Step Conf**", and enter the Service Observing Listen Only Access Code from Section 3.2 Step 6 for **Observe Feature Prefix**.  CTILink Configuration General Link Options / Devices CT Server Serial User Data TCP/IP Triggers OK Cancel Apply Misc Options ☑ Enable RAPI Support ☑ Enable Single Step Conf □ Allow Agent Enable Cntrl Observe Feature Prefix: #50 Observe Feature Suffix: □ Enable Screen Record: Stop Screen Record After: End-of-Call Wrap Delay: 20 ☑ Screen Record Eval Only: Device Parameters Agent Size: 4 Extension Size: 4 Trunk Group Size: 3 Trunk Number Size: 5 Min Device ID: 0 Max Device ID: 9999 SMDR Default Action ● Stop ○ Erase

Step	Description
5.	Click on the **CT Server** tab. Check the checkboxes for “**Enable Logon**” and “**Enable Logoff**”. Click on “**OK**” to return to the Configuration Manager main window.  CTILink Configuration General Link Options / Devices CT Server Serial User Data TCP/IP Triggers Logon/Logoff Events CT Agent/Device Map OK Cancel Apply Enable Logon: ☑ Enable Logoff: ☑ Agent Data Index: 0 Agent ID Index: 0 Device ID Index: 0

Step	Description
6.	In the Configuration Manager **General** tab, click on the “**Integration**” icon. 

Configuration Manager: "\\DEVCONN1"

Catalog

● Rollover Daily   Retention Period (days): 90   Advanced

○ Rollover Weekly   Start at: 3:00 AM

● Sun ○ Mon ○ Tue ○ Wed ○ Thu ○ Fri ○ Sat

Restored Files Retention Period (days): 1

Maintenance

Channel Maintenance

Channel	Channel Name
001	Channel #001
002	Channel #002
003	Channel #003
004	Channel #004
005	Channel #005
006	Channel #006
007	Channel #007
008	Channel #008
009	Channel #009
010	Channel #010
011	Channel #011
012	Channel #012
013	Channel #013
014	Channel #014

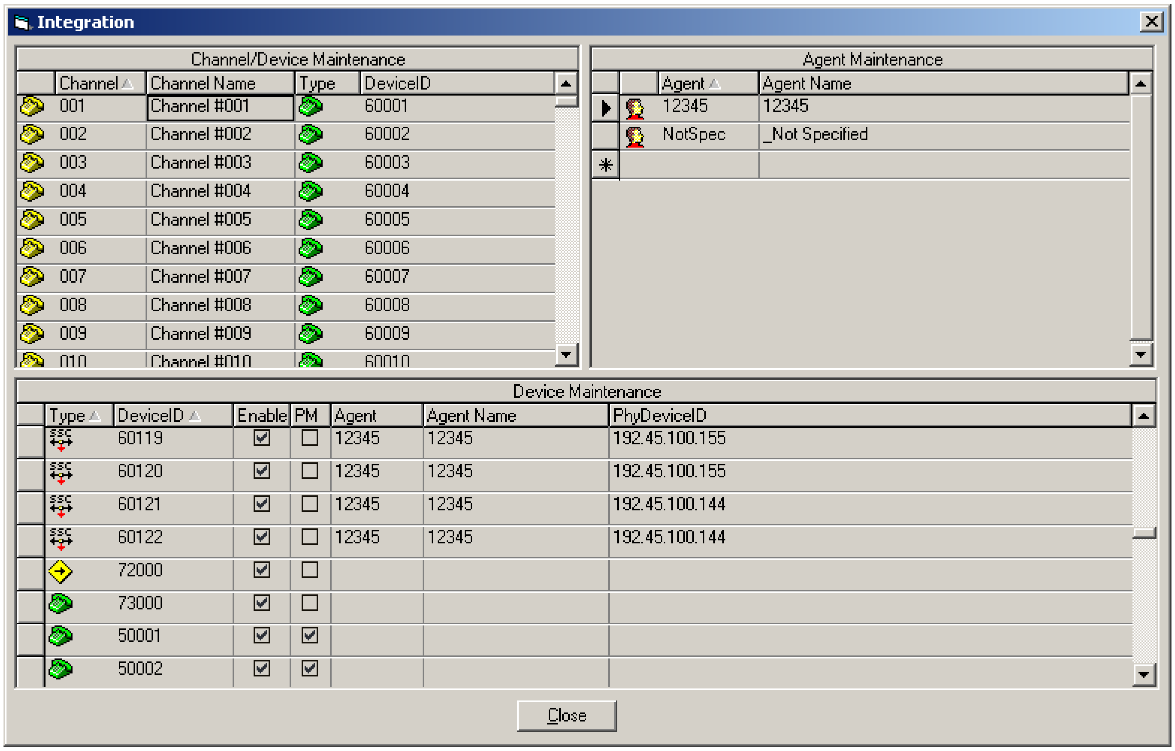
Inactivity Detection Period

From: 8:00 AM   To: 6:00 PM

Step	Description
7.	In the **Agent Maintenance** table, create an agent ID with the password (Security Code) common to all AES Device and Media Control API stations to be used for recording (see Section 3.3). This is not a real agent, it is used only as a password placeholder used in the Device Maintenance table. In the **Channel/Device Maintenance** table, for each channel, set **DeviceID** to an AES Device and Media Control API station extension and **Type** to a green telephone icon. In the **Device Maintenance** table, add entries as follows:

- Add an entry for each AES Device and Media Control API station extension. For each entry, set **Type** to the "**SSC**" icon, **Agent** to the placeholder agent created above, and **PhyDeviceID** to the IP address of a C-LAN board dedicated for H.323 endpoint registration, and check the **Enable** checkbox. In the example below, **DeviceIDs** 60119 through 60122 correspond to some of the AES Device and Media Control API stations configured in Section 3.3.
- Add an entry for each VDN to be monitored. For each entry, set **Type** to the yellow diamond icon, and check the **Enable** checkbox. In the example below, **DeviceID** 72000 corresponds to the VDN configured in Section 3.2 Step 5.
- Add an entry for each hunt/skill group to be monitored. For each entry, set **Type** to the green telephone icon, and check the **Enable** checkbox. In the example below, **DeviceID** 73000 corresponds to the hunt/skill group configured in Section 3.2 Step 2.
- Add an entry for each station to be recorded full time. For each entry, set **Type** to the green telephone icon, and check the **Enable** and **PM** checkboxes. In the example below, **DeviceIDs** 50001 and 50002 correspond to some of the stations to be recorded.

Click on "**Close**" to return to the Configuration Manager main window.



Channel/Device Maintenance

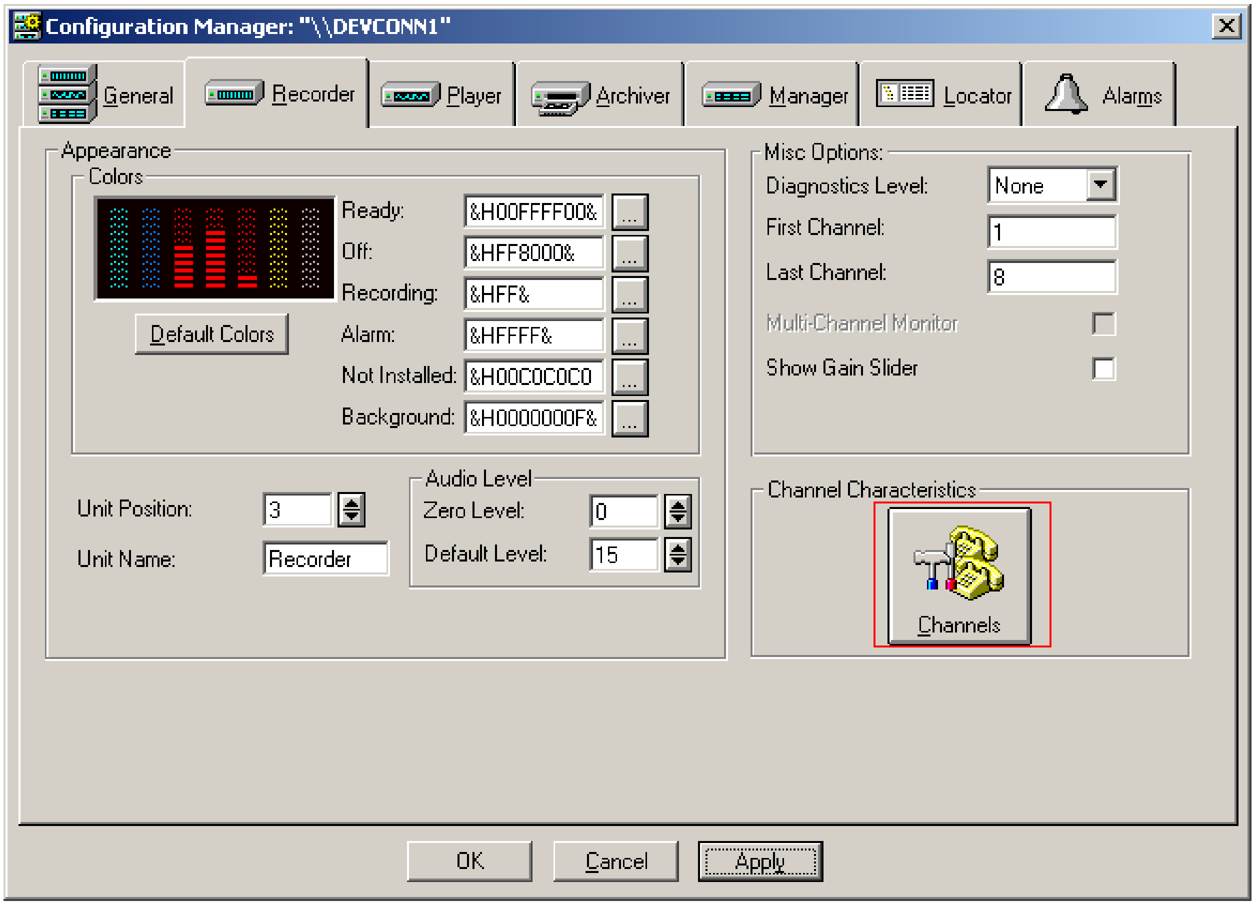
Channel	Channel Name	Type	DeviceID
001	Channel #001	☎	60001
002	Channel #002	☎	60002
003	Channel #003	☎	60003
004	Channel #004	☎	60004
005	Channel #005	☎	60005
006	Channel #006	☎	60006
007	Channel #007	☎	60007
008	Channel #008	☎	60008
009	Channel #009	☎	60009
010	Channel #010	☎	60010

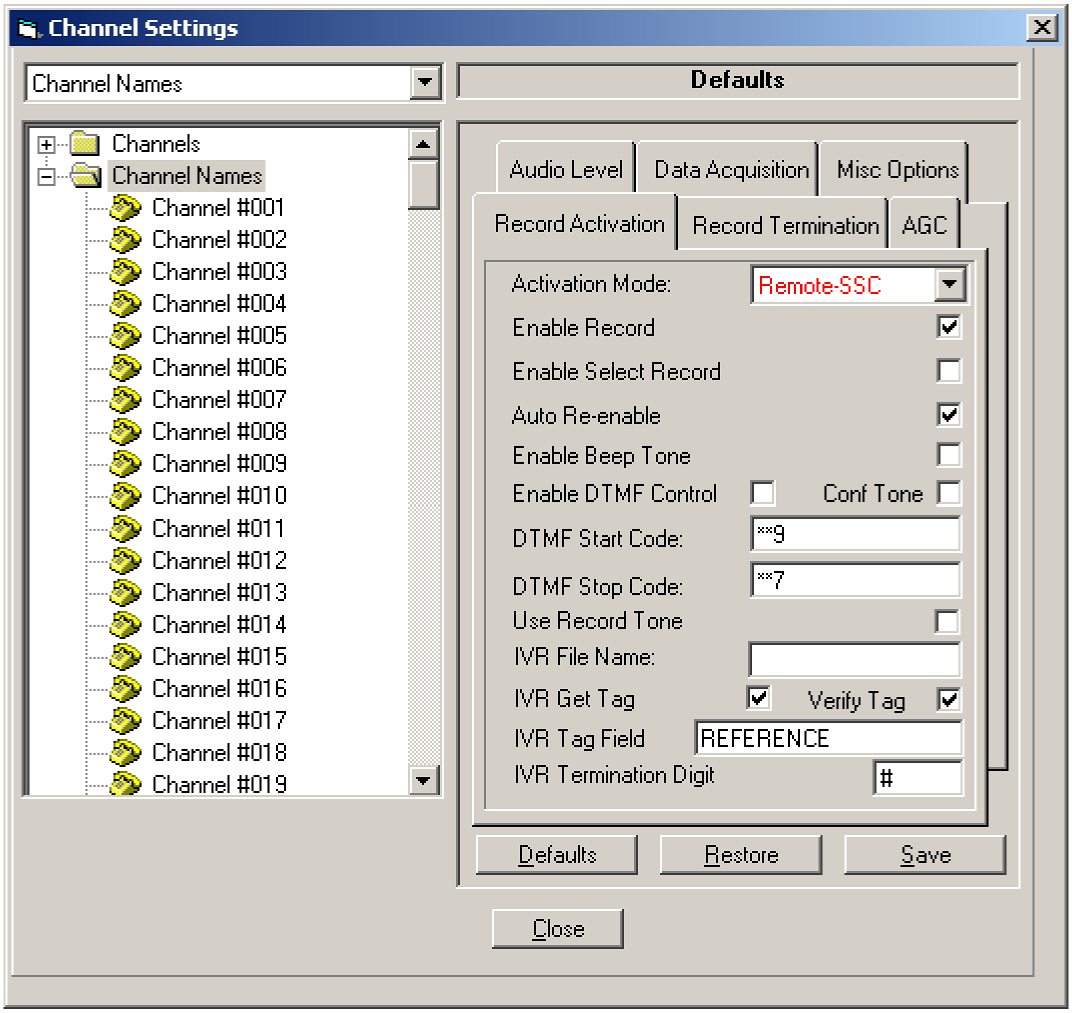
Agent Maintenance

Agent	Agent Name
12345	12345
NotSpec	_Not Specified

Device Maintenance

Type	DeviceID	Enable	PM	Agent	Agent Name	PhyDeviceID
SSC	60119	☑	□	12345	12345	192.45.100.155
SSC	60120	☑	□	12345	12345	192.45.100.155
SSC	60121	☑	□	12345	12345	192.45.100.144
SSC	60122	☑	□	12345	12345	192.45.100.144
◆	72000	☑	□			
☎	73000	☑	□			
☎	50001	☑	☑			
☎	50002	☑	☑			

Step	Description
8.	In the Configuration Manager main window, select the **Recorder** tab. Set **Last Channel** to the maximum number of recording channels. Click on the "**Channels**" icon.  Configuration Manager: "\\DEVCONN1" Appearance Colors Ready: &H00FFFF00& Off: &HFF8000& Recording: &HFF& Alarm: &HFFFFF& Not Installed: &H00C0C0C0 Background: &H0000000F& Unit Position: 3 Unit Name: Recorder Audio Level Zero Level: 0 Default Level: 15 Misc Options: Diagnostics Level: None First Channel: 1 Last Channel: 8 Multi-Channel Monitor □ Show Gain Slider □ Channel Characteristics General Recorder Player Archiver Manager Locator Alarms Default Colors Channels OK Cancel Apply

Step	Description
9.	In the **Record Activation** tab, set **Activation Mode** to “**Remote-SSC**”. Click on “**Close**” to return to the Configuration Manager main window.  Channel Settings Channel Names Defaults Channels Channel Names Channel #001 Channel #002 Channel #003 Channel #004 Channel #005 Channel #006 Channel #007 Channel #008 Channel #009 Channel #010 Channel #011 Channel #012 Channel #013 Channel #014 Channel #015 Channel #016 Channel #017 Channel #018 Channel #019 Audio Level Data Acquisition Misc Options Record Activation Record Termination AGC Defaults Restore Save Close Activation Mode: Remote-SSC Enable Record ☑ Enable Select Record ☐ Auto Re-enable ☑ Enable Beep Tone ☐ Enable DTMF Control ☐ Conf Tone ☐ DTMF Start Code: **9 DTMF Stop Code: **7 Use Record Tone ☐ IVR File Name: IVR Get Tag ☑ Verify Tag ☑ IVR Tag Field REFERENCE IVR Termination Digit #
10.	Click on “**OK**” in the Configuration Manager main window to save changes and exit.
11.	Open the TSLIB.INI file located in the C:\WINDOWS folder. Add the following line in the **[Telephony Servers**] section of the file: <AES Server Client Connectivity IP address>=450. For example, the following line was entered during compliance testing: 192.45.52.150=450

6. Interoperability Compliance Testing

The interoperability compliance testing included feature, serviceability, and performance testing. The feature testing evaluated the ability of the Mercom Audiolog Call Recording Server to monitor and record calls placed to and from stations, agents, and VDNs. The serviceability testing introduced failure scenarios to see if Audiolog is able to resume recording after failure recovery. The performance testing stressed the Audiolog server 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 stations, IP Softphones, agents, and VDNs, monitor and record the calls using Audiolog, and verify the recordings. For feature testing, the types of calls included internal calls, inbound trunk calls, outbound trunk calls, transferred calls, conference calls, Redirection On No Answer (RONA) calls, and Switch-Classified calls. 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. For serviceability testing, failures such as network disconnects/reconnects and device resets were applied.

6.2. Test Results

Audiolog successfully monitored, recorded, stored, and played back the various types of calls discussed in Section 6.1. For serviceability testing, Audiolog was able to resume recording calls after restoration of connectivity to the Avaya Application Enablement Services (AES) server, and after resets of the Audiolog server and AES server. For performance testing, Audiolog successfully recorded calls under a low to moderate call volume for over 21 consecutive hours.

The following are notes and observations were obtained from testing:

1. Audiolog does not record outbound calls placed from a bridged call appearance on a secondary station. Audiolog does record inbound calls to a bridged call appearance that are answered on the secondary station.
2. Audiolog recommends configuring two more recording channels than the number of recorded stations.
3. The AES server does not notify Audiolog of CTI link failures. As a result, Audiolog must be restarted after the CTI link recovers. Avaya expects to resolve this issue in a future release.

7. Verification Steps

The following steps may be used to verify the configuration:

- From the Mercom Audiolog Call Recording Server, ping the Avaya Application Enablement Services (AES) server and verify connectivity.
- From the Mercom Audiolog Call Recording Server, ping the Avaya G650 Media Gateway MedPro boards and verify connectivity.
- Verify that Application Enablement Services is enabled and listening on at least one C-LAN board (use the **status aesvcs interface** command on the SAT).
- Verify communication between Avaya Communication Manager and the Avaya AES server (use the **status aesvcs link** command on the SAT, or navigate to **Status and Control -> Switch Conn Summary** on the AES CTI OAM page and verify that the state of the Switch Connection is "**talking**").
- Verify that CTI link configured in Section 3.1 Step 2 is established (use the **status aesvcs cti-link** command on the SAT).
- Verify that the Mercom Audiolog recording ports are registered as "IP_API_A" stations in Avaya Communication Manager (use the **list registered-ip-stations** command on the SAT).
- Verify that calls may be successfully completed between the Avaya IP and Digital telephones, analog telephones, and Avaya IP Softphones. Verify that the call recordings are accurate and complete.
- Log agents into a hunt/skill group and verify that calls may be successfully completed to and from the agents. Verify that the call recordings are accurate and complete.

8. Support

For technical support on Mercom products, contact Mercom at:

- Phone: 201-507-8800
- Email: tech.support@mercom.com

9. Conclusion

These Application Notes describe the procedures for configuring the Mercom Audiolog 3.3 Call Recording Server to monitor and record calls placed to and from stations, softphones, and agents on Avaya Communication Manager 3.0. In the configuration described in these Application Notes, Audiolog uses the Call Control Services and Device and Media Control Services of Avaya Application Enablement Services to perform recording. During compliance testing, Audiolog successfully monitored and recorded calls placed to and from Avaya IP and Digital Telephones, analog telephones, Avaya IP Softphones, and agents, as well as calls placed to a VDN and then queued to an agent hunt/skill group. Audiolog 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 MultiVantage™ Application Enablement Services 3.0 Administration and Maintenance Guid*e, Issue 1, June 2005, Document Number 02-300357.

Product information for Mercom products may be found at http://mercom.com/products/.

[2] Mercom Call Center Suite Brochure
[3] Audiolog Brochure

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.