Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.0.1 and Avaya Aura® Application Enablement Services R6.1 to interoperate with Speech Technology Centre Smart Logger II v7.6 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for the Speech Technology Centre Smart Logger II solution with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Speech Technology Centre Smart Logger II system is a voice recording solution which can be used to record voice streams for Avaya telephony.

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

1. Introduction

The purpose of this document is to describe the compliance testing carried out using the Multiple Device Registration recording method on Speech Technology Centre Smart Logger II with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. It includes a description of the configuration of both the Avaya and the Speech Technology Centre solutions, a description of the tests that were performed and a summary of the results of those tests.

Speech Technology Centre Smart Logger II is a voice recording system which can be used to record the voice stream of Avaya telephony endpoints. In this compliance test, it uses Avaya Aura® Communication Manager's Multiple Device Registration feature via the Avaya Aura® Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface to capture the audio and call details for call recording. Speech Technology Centre Smart Logger II uses the Avaya Aura® Application Enablement Services DMCC service to register extensions on Avaya Aura® Communication Manager that are to be recorded. When the extension registered by Speech Technology Centre Smart Logger II receives an event pertaining to the start of a call, Speech Technology Centre Smart Logger II receives the extensions RTP media stream.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of Smart Logger II to carry out call recording in a variety of scenarios using DMCC with AES and Communication Manager. The test approach was to verify that the calls placed and recorded using the Smart Logger II with Avaya solution functioned correctly with good audio quality received. Functionality testing included basic telephony operations such as answer, hold/retrieve, transfer, conference, bridged appearance and calls to/from the PSTN. Tests also included ACD Agent recording. All tests were successful.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios to ensure good quality audio recordings were received. Intra-switch calls were made on the Communication Manager and external calls were made to, and received from the PSTN. The serviceability testing focused on verifying the ability of Smart Logger II to recover from disconnection and reconnection of the Avaya solution.

2.2. Test Results

All functionality and serviceability test cases were completed successfully. The following observations were made:

- The serviceability tests were performed by disconnecting the Smart Logger II server from the network/power and ensuring successful recording of calls and good audio quality on re-connection. It was noticed that there was an inconsistent delay in reconnection of Smart Logger II to the configured digital phone when power was restored.

- Due to disk write caching on the SmartLogger II server OS, calls in progress for a short time when the power to the recorder was disconnected, are lost. This can be addressed with a freeware disk caching utility used to amend the rate at which data is committed to the hard drive.
- Upon reconnection of AES, Smart Logger II displays endpoints on a call during disconnection, as still on a call, regardless of if the call has ended or not. This is remedied once a call is placed or received on the relevant endpoint.

2.3. Support

Technical support can be obtained for the Speech Technology Centre Smart Logger II solution as follows:

- Email: support@speechpro.com
- Website: www.speechpro.com
- Phone: +7-812-331-0665

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of an Avaya S8800 Server running Communication Manager with Avaya G650 Media Gateway as the PBX. An Avaya S8800 Server hosts the Application Enablement Services software. Avaya 9600 series, 1600 series IP telephones and 2400 series Digital telephones are connected to the PBX and used in the testing. The Smart Logger II server running on a VMWare platform was used during the testing.

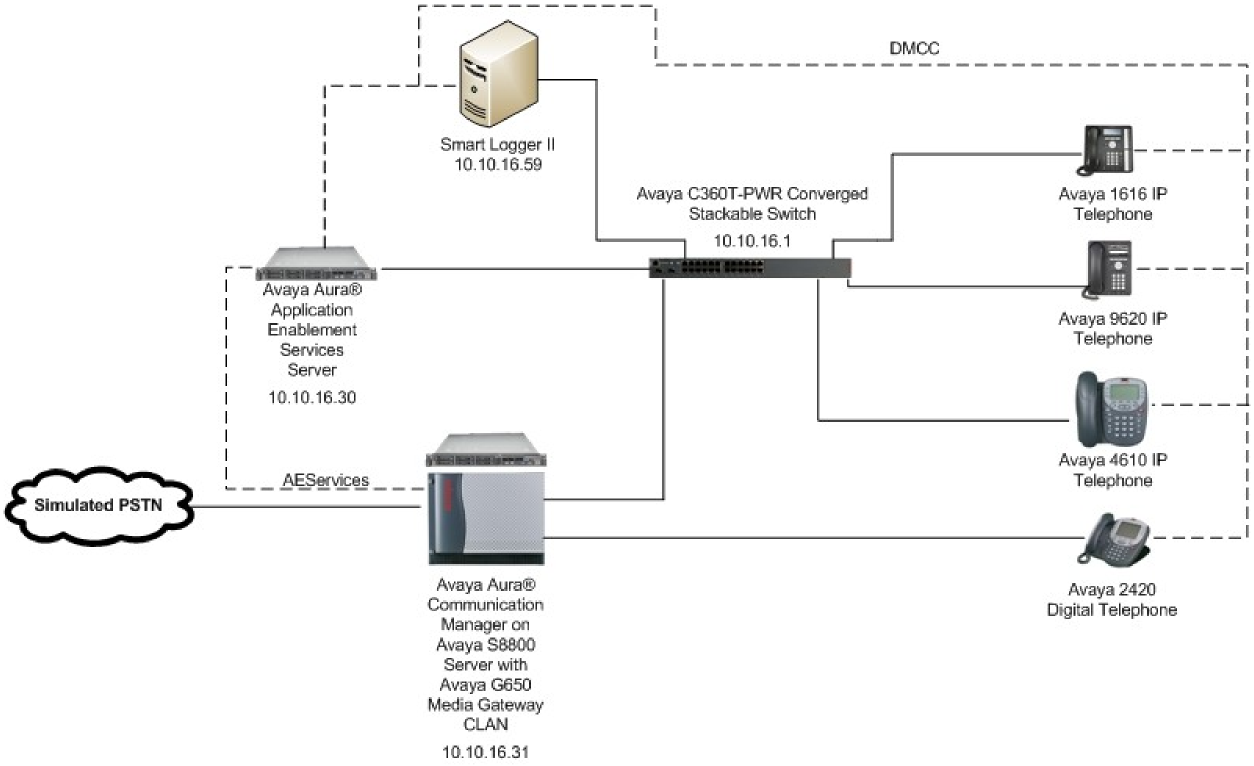


Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Application Enablement Services Server and Speech Technology Centre Smart Logger II Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration as shown in **Figure 1.**

Equipment	Software
Avaya Aura® S8800 Server	Avaya Aura® Communication Manager R6.0.1 R16.00.1.510.1-19100
Avaya G650- Media Gateway Avaya TN799DP C-LAN Circuit Pack Avaya TN2602AP Media Processor Circuit Pack	 HW1 FW40 HW8 FW58
Avaya Aura® S8800 Server	Avaya Aura® Application Enablement Services R6.1
Avaya 9620C IP Telephone	3.110b
Avaya 1616 IP Telephone	1_3000
Avaya 4610 IP Telephone	2.3
Avaya 2420 Digital Telephone	REL 4.00 HWV 1 FWV 4
Generic VMWare Server	Speech Technology Centre Smart Logger II 7.6.15.2555

5. Configure Avaya Aura® Communication Manager

The configuration and verification steps illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 10**. The configuration steps described in this section can be summarized as follows:

- Verify System Parameters Customer Options
- Verify System Parameters Features
- Configure Service Observe
- Configure Target Stations to be Recorded
- Configure Station Button Assignments
- Configure Hunt Group
- Configure Agent
- Configure Interface to Avaya Aura® Application Enablement Services

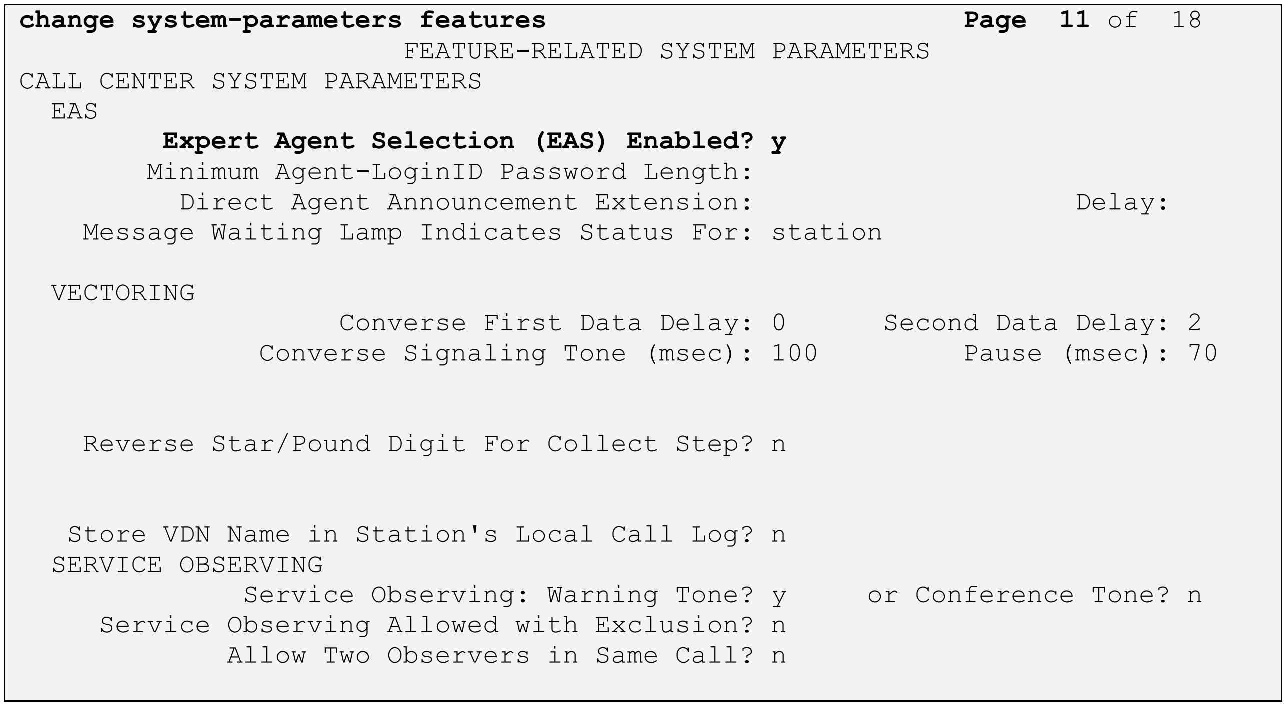
5.1. Verify System Parameters Customer Options

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

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

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



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

5.2. Verify System Parameters Features

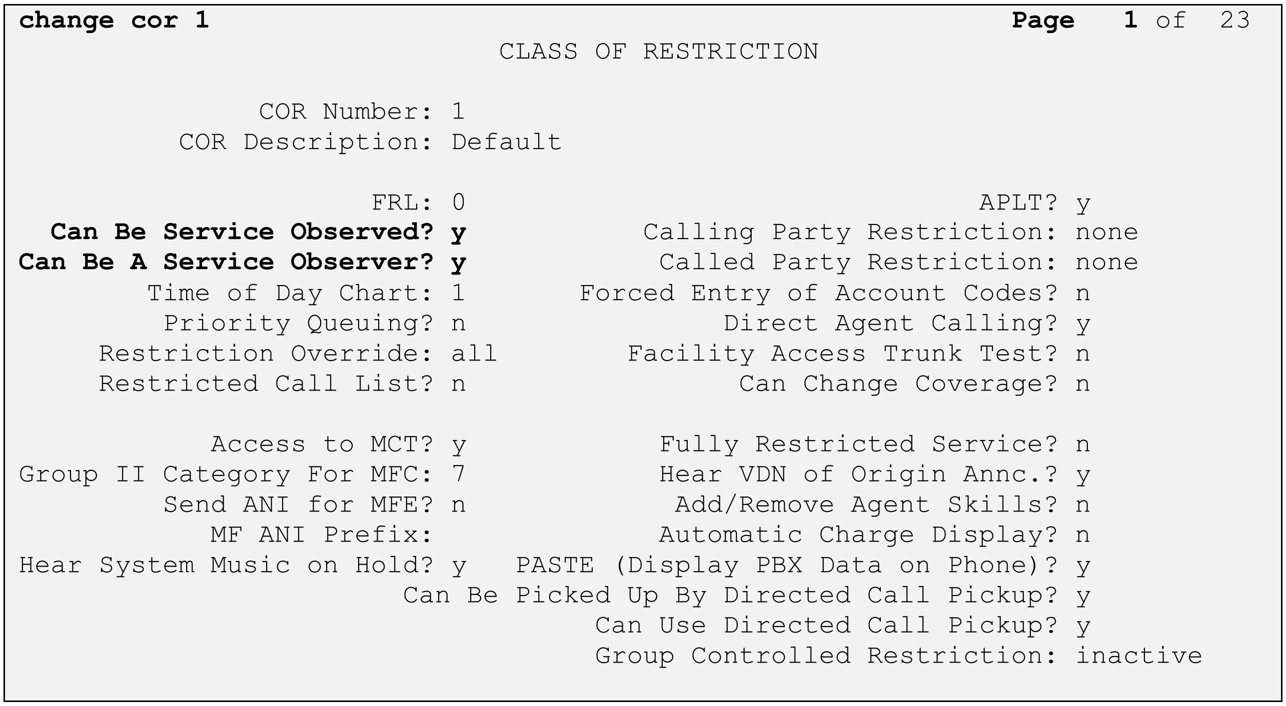
Expert Agent Selection is used for the configuration and routing of calls to ACD Agents. Use **change system-parameters features command** and on **Page 11** of the system-parameters features form, set **Expert Agent Selection (EAS) Enabled?** to **y.**



```
change system-parameters features                          Page  11 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length:
          Direct Agent Announcement Extension:                    Delay:
    Message Waiting Lamp Indicates Status For: station

  VECTORING
                    Converse First Data Delay: 0      Second Data Delay: 2
               Converse Signaling Tone (msec): 100         Pause (msec): 70


    Reverse Star/Pound Digit For Collect Step? n


   Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
              Service Observing: Warning Tone? y     or Conference Tone? n
     Service Observing Allowed with Exclusion? n
             Allow Two Observers in Same Call? n
```

5.3. Configure Service Observe

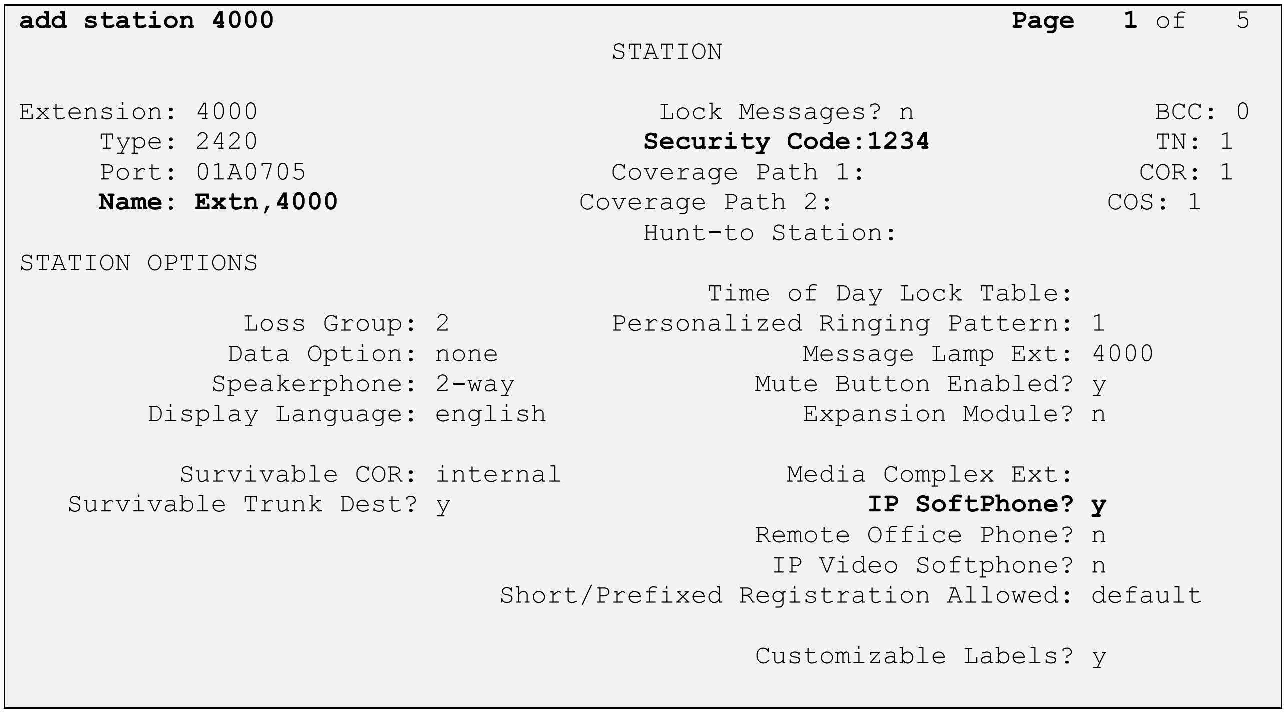
For the purposes of Multiple Device Registration, Service Observe must be enabled for the Class of Restriction to which the Target Stations will be assigned. Using the command **change cor 1** set both **Can Be Service Observed?** and **Can Be A Service Observer?** to **y**.



```
change cor 1                                                  Page   1 of  23
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description: Default

                      FRL: 0                                APLT? y
  Can Be Service Observed? y           Calling Party Restriction: none
Can Be A Service Observer? y            Called Party Restriction: none
        Time of Day Chart: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? y
     Restriction Override: all        Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

            Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7            Hear VDN of Origin Annc.? y
         Send ANI for MFE? n             Add/Remove Agent Skills? n
            MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? y
                        Can Be Picked Up By Directed Call Pickup? y
                                    Can Use Directed Call Pickup? y
                                    Group Controlled Restriction: inactive
```

5.4. Configure Target Stations to be Recorded

For the purpose of the compliance test, extensions 4000-4003 were configured. Use the **add station** command to configure a station for each of the target stations to be recorded. Enter in a descriptive **Name** and **Security Code** for each one. Set the **IP Softphone?** to **y**.



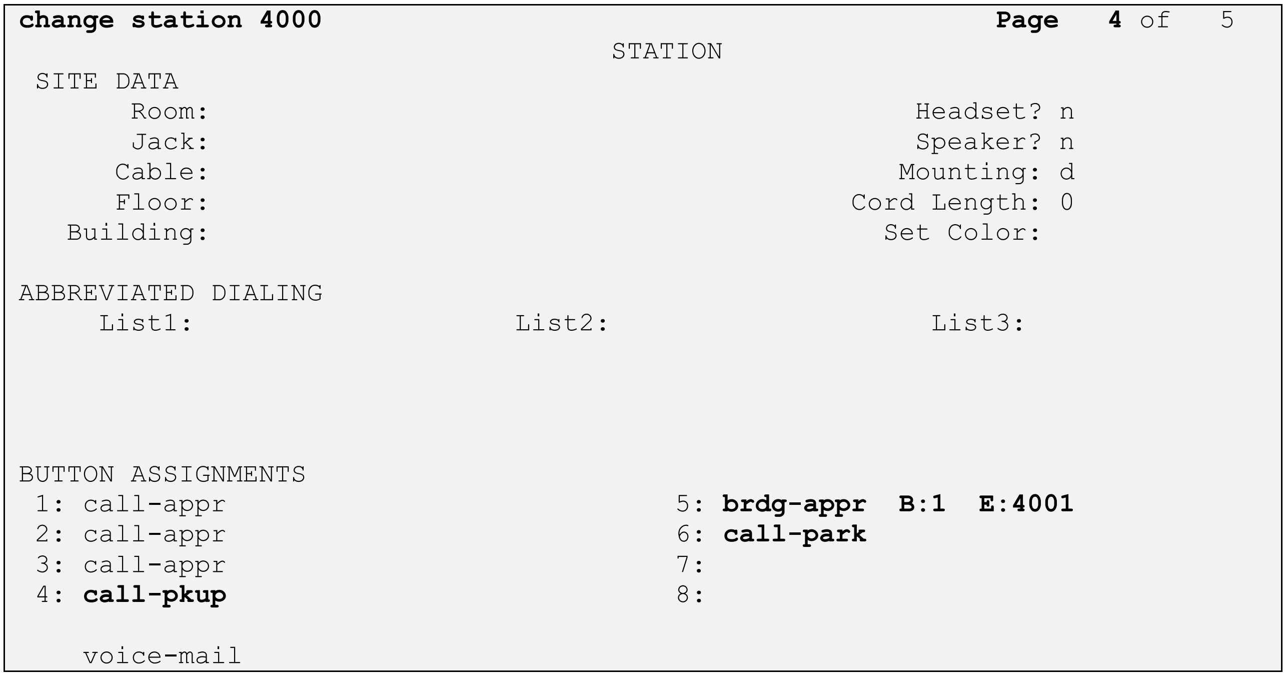
```
add station 4000                                              Page   1 of   5
                                     STATION

Extension: 4000                         Lock Messages? n               BCC: 0
     Type: 2420                        Security Code:1234              TN: 1
     Port: 01A0705                   Coverage Path 1:                 COR: 1
     Name: Extn,4000               Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 2          Personalized Ringing Pattern: 1
             Data Option: none                   Message Lamp Ext: 4000
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                Expansion Module? n

          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y
                                              Remote Office Phone? n
                                               IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default

                                              Customizable Labels? y
```

On **Page 2**, ensure that the **Multimedia Mode** is set to **enhanced**.

```
add station 4000                                                Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe            Auto Select Any Idle Appearance? n
          LWC Activation? y                       Coverage Msg Retrieval? y
  LWC Log External Calls? n                                  Auto Answer:
none
             CDR Privacy? n                             Data Restriction? n
   Redirect Notification? y                  Idle Appearance Preference? n
 Per Button Ring Control? n                Bridged Idle Line Preference? n
   Bridged Call Alerting? n                    Restrict Last Appearance? y
  Active Station Ringing: single
                                                           EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                      EC500 State: enabled
         Multimedia Mode: enhanced                  Audible Message Waiting? n
    MWI Served User Type:                        Display Client Redirection? n
              AUDIX Name:                       Select Last Used Appearance? n
                                                  Coverage After Forwarding? s
                                                    Multimedia Early Answer? n
 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio
Connections? y
  Emergency Location Ext: 4000          Always Use? n IP Audio Hairpinning? n
```

5.5. Configure Station Button Assignments

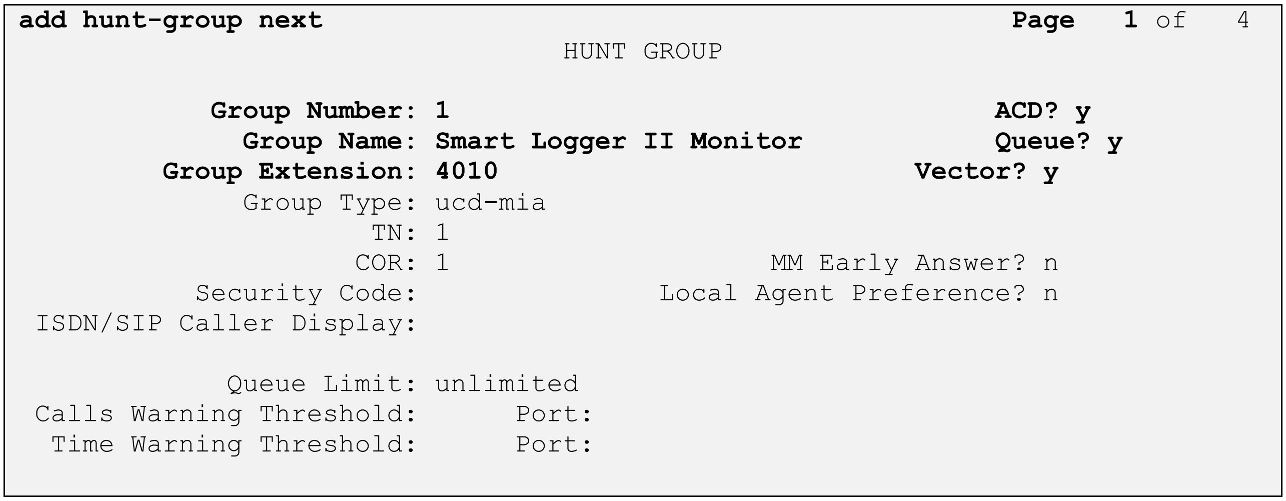
Use the **change station** command to configure the button assignments of the stations to be recorded, as required. Add the appropriate button assignments as shown on **Page 4** below. In this case there are three call appearance buttons **call-appr**. There are also buttons assigned for the call functions call-pickup, bridged appearance and call park: **call-pkup**, **brdg-appr**, **call-park**.



```
change station 4000                                          Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                                Headset? n
       Jack:                                                Speaker? n
      Cable:                                               Mounting: d
      Floor:                                            Cord Length: 0
   Building:                                              Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                            5: brdg-appr  B:1  E:4001
 2: call-appr                            6: call-park
 3: call-appr                            7:
 4: call-pkup                            8:

    voice-mail
```

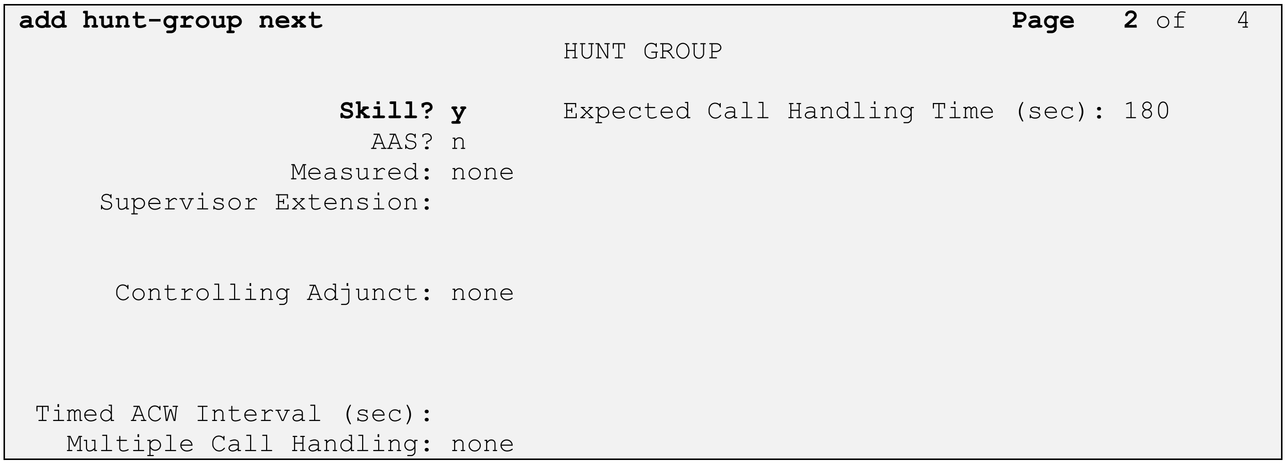
5.6. Configure Hunt Group

For the purposes of recording agents, a skilled hunt group must be added. Agents who log in to this skill will be recorded. Using the command **add hunt-group next**, assign the hunt group with a **Group Extension** valid in the dialplan, **Group Name** for identification purposes, and set **ACD, Queue** and **Vector** to **y (yes)**. Note the **Group Number 1**.



```
add hunt-group next                                           Page   1 of   4
                                  HUNT GROUP

            Group Number: 1                                  ACD? y
              Group Name: Smart Logger II Monitor            Queue? y
         Group Extension: 4010                          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:
```

Navigate to **Page 2,** set **Skill** to **y.**



```
add hunt-group next                                           Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n
                 Measured: none
     Supervisor Extension:


      Controlling Adjunct: none



 Timed ACW Interval (sec):
   Multiple Call Handling: none
```

5.7. Configure Agents

Agents to be recorded should be assigned the Smart Logger Monitor Skill configured in the previous step.

```
add agent-loginID 4011                                        Page   1 of   3
                                 AGENT LOGINID

                Login ID: 4011                                    AAS? n
                    Name: Agent1                                AUDIX? n
                      TN: 1                            LWC Reception: spe
                     COR: 1                   LWC Log External Calls? n
           Coverage Path:                   AUDIX Name for Messaging:
           Security Code:123456
                                        LoginID for ISDN/SIP Display? n
                                                          Password:123456
                                              Password (enter again):123456
                                                         Auto Answer: station
                                                   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
                                            Forced Agent Logout Time:   :

     WARNING:  Agent must log in again before changes take effect
```

Navigate to **Page 2**, set **1** in the Skill Number (**SN**).

```
add agent-loginID 4202                                        Page   2 of   3
                                 AGENT LOGINID
      Direct Agent Skill:                                Service Objective? n
Call Handling Preference: skill-level                Local Call Preference? n

    SN   RL SL           SN   RL SL           SN   RL SL           SN   RL 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:
```

5.8. Configure Interface to Avaya Aura® Application Enablement Services

Enter the node **Name** and **IP Address** for the AES, in this case **devconaes61** and **10.10.16.30** respectively. Take a note of the **CLAN** node **Name** and **IP Address** as it is used later in this section

```
change node-names ip                                           Page   1 of   2
                                     IP NODE NAMES
    Name                  IP Address
CLAN                    10.10.16.31
CM521                   10.10.16.23
Gateway                 10.10.16.1
IPbuffer                10.10.16.184
Intuition               10.10.16.51
MedPro                  10.10.16.32
Presence                10.10.16.83
RDTT                    10.10.16.185
SESMNGR                 10.10.16.44
SM1                     10.10.16.43
SM61                    10.10.16.201
default                 0.0.0.0
devconaes61             10.10.16.30
```

In order for Communication Manager to establish a connection to AES, administer the CTI Link as shown below. Specify an available **Extension** number as per the dialplan, set the **Type** as **ADJ-IP**, which denotes that this is a link to an IP connected adjunct, and name the link for easy identification, in this instance, the node-name is used.

```
add cti-link 1                                                Page   1 of   3
                                       CTI LINK
 CTI Link: 1
Extension: 1111
     Type: ADJ-IP
                                                                          COR:
1
     Name: devconaes61
```

Configure IP-Services for the **AESVCS** service using **change ip-services** command and using the C-LAN node name as noted above i.e. **CLAN.**

```
change ip-services                                          Page   1 of   4

                                   IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port

CDR1                       CLAN             0        IPbuffer         9000
CDR2                       CLAN             0        RDTT             9001
AESVCS         y           CLAN          8765
```

Navigate to **Page 4,** set the **AE Services Server** node-name and the **Password** the AES Server will use to authenticate with Communication Manager, set **Enabled** to **y**.

```
change ip-services                                         Page   4 of   4
                            AE Services Administration

   Server ID    AE Services        Password          Enabled    Status
                 Server
      1:       devconaes61       Avayapassword1         y         in use
```

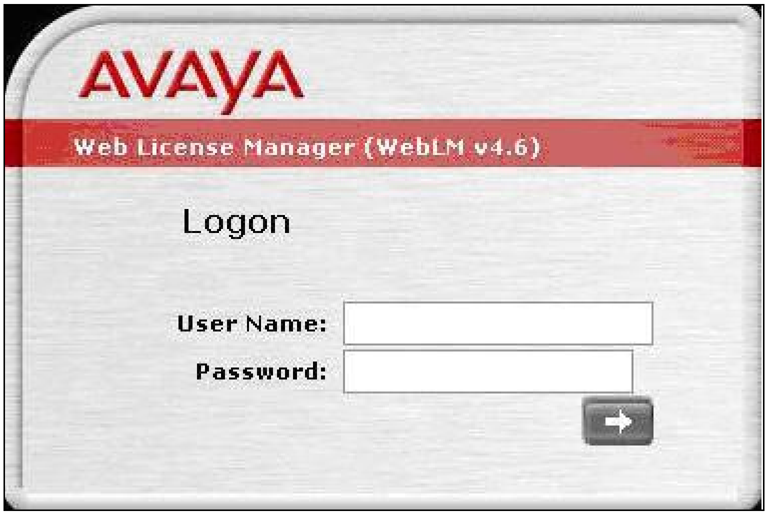
6. Configuration of Avaya Aura® Application Enablement Services

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

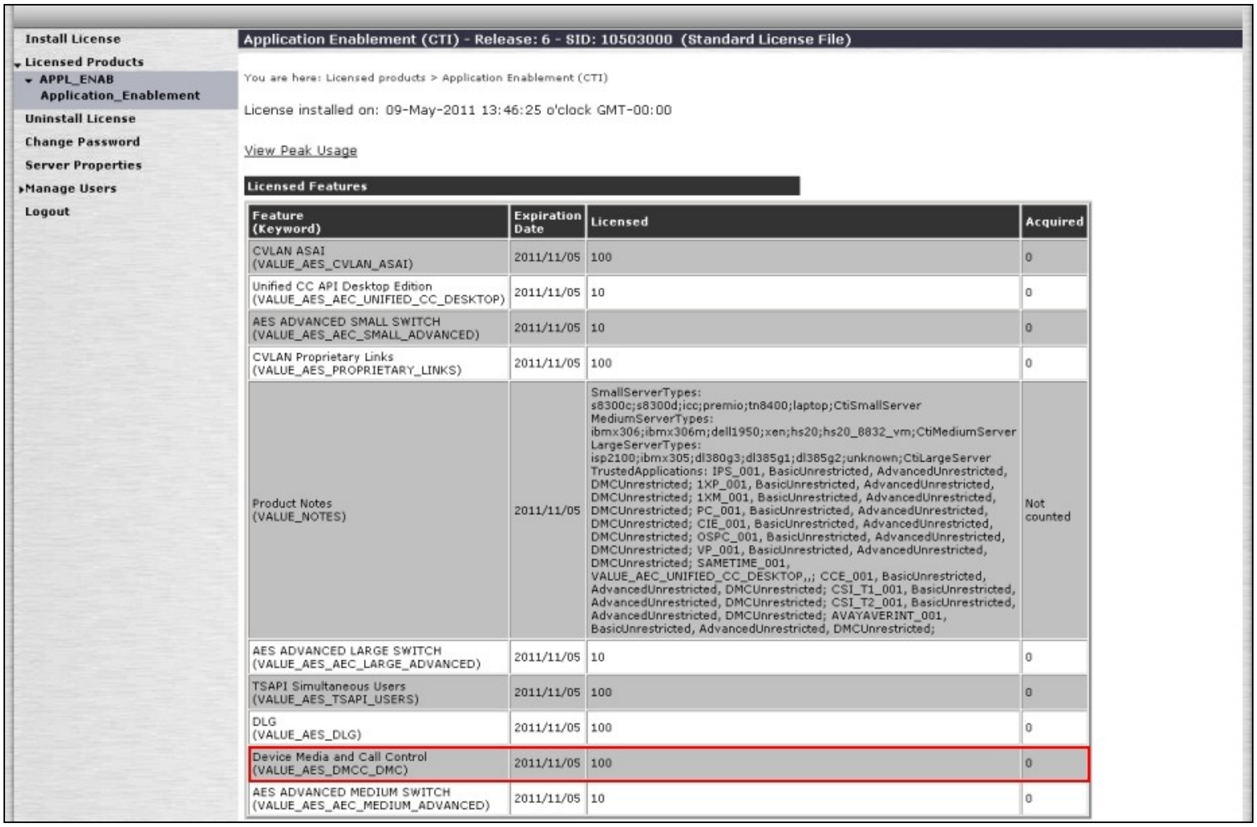
- Verify Licensing
- Create Switch Connection
- Create CTI User
- Enable CTI User
- Configure DMCC Port
- Enable Security Database

6.1. Verify Licensing

Access the Web License Manager of the Application Enablement Services Server, in this instance using the URL https://10.10.16.30/WebLM/index.jsp. The Web License Manager Screen is displayed, and login using the appropriate credentials.



The **Web License Manager** screen below is displayed. Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane. Verify that there are sufficient licenses for **Device Media and Call Control**, as shown below. If not, consult with an Avaya Account Manager or Business Partner to acquire the proper licenses.



Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License File)

You are here: Licensed products > Application Enablement (CTI)

License installed on: 09-May-2011 13:46:25 o'clock GMT-00:00

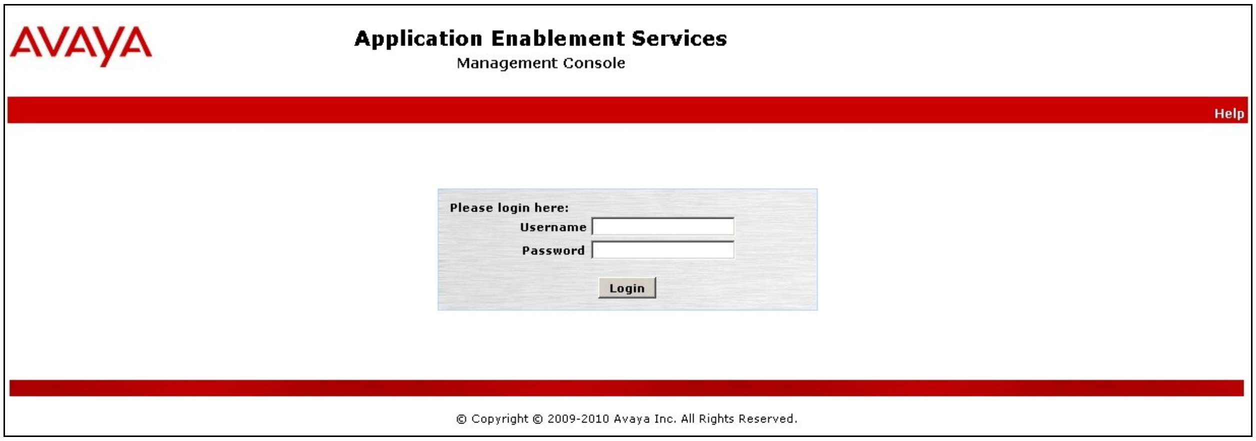
View Peak Usage

Licensed Features

Feature (Keyword)	Expiration Date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	2011/11/05	100	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	2011/11/05	10	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	2011/11/05	10	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	2011/11/05	100	0
Product Notes (VALUE_NOTES)	2011/11/05	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	2011/11/05	10	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	2011/11/05	100	0
DLG (VALUE_AES_DLG)	2011/11/05	100	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	2011/11/05	100	0
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	2011/11/05	10	0

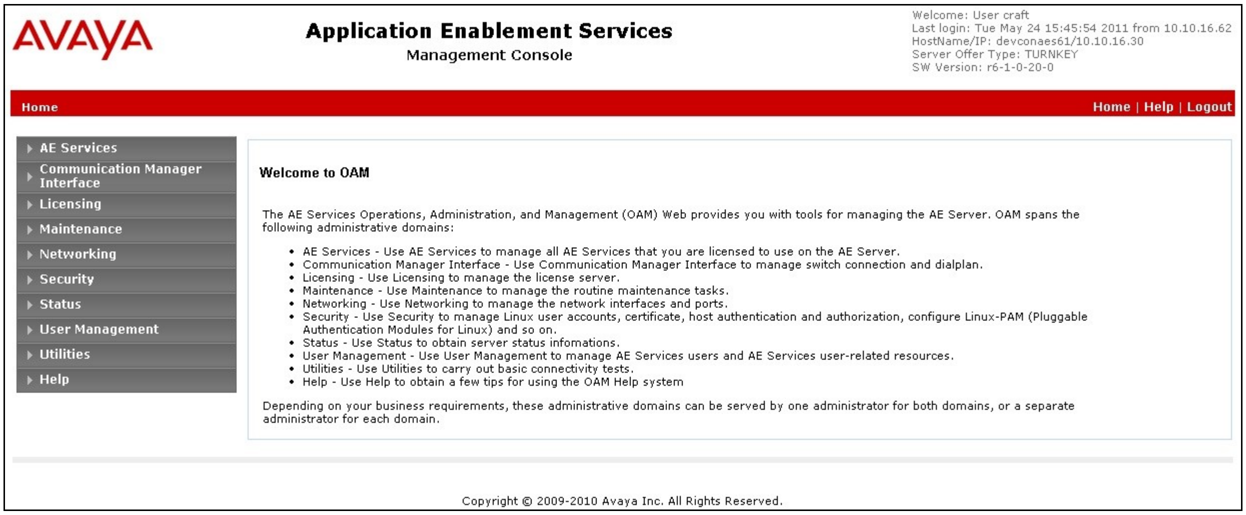
6.2. Create Switch Connection

Access the OAM web-based interface of the Application Enablement Services Server, in this instance using the URL https://10.10.16.30. The Management console is displayed, and login using the appropriate credentials.



© Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

The **Welcome to OAM** screen is displayed next.



Welcome: User craft
Last login: Tue May 24 15:45:54 2011 from 10.10.16.62
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURNKEY
SW Version: r6-1-0-20-0

Welcome to OAM

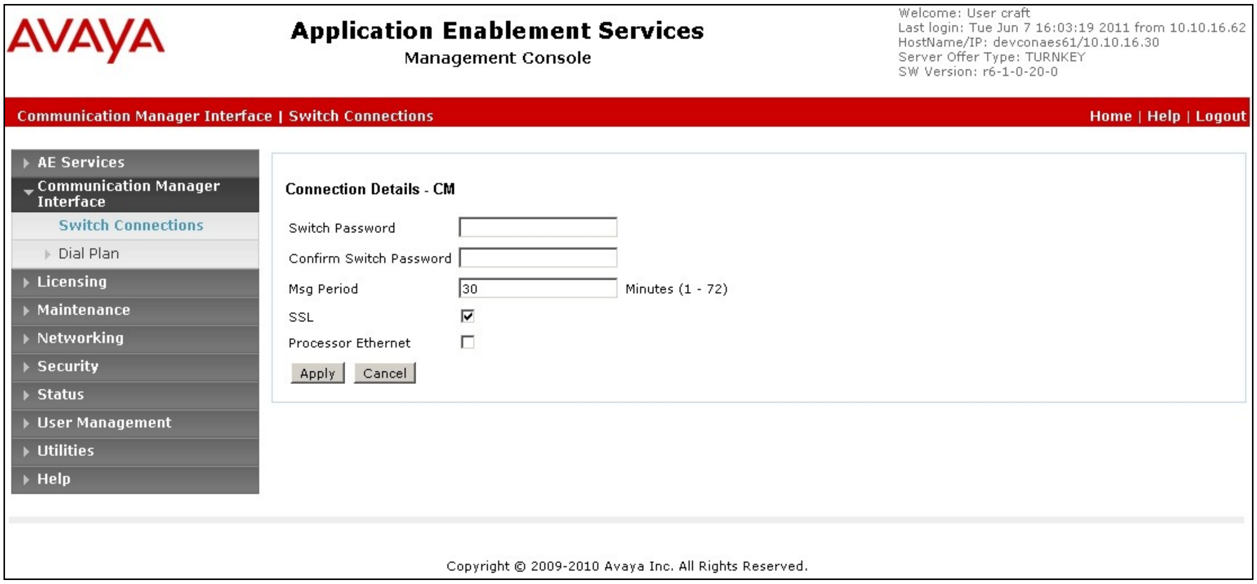
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status infomations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain.

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

To establish the connection between Communication Manager and the Application Enablement Services Server, click **Communication Manager Interface → Switch Connections**. In the field next to next to **Add Connection**, enter **CM** and click on **Add Connection**, the following screen will be displayed. Complete the configuration as required and enter the password specified in **Section 5.8** when configuring AESVCS in ip-services. In this instance the password is **Avayapassword1**. Click on **Apply**.



Welcome: User craft
Last login: Tue Jun 7 16:03:19 2011 from 10.10.16.62
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURNKEY
SW Version: r6-1-0-20-0

Connection Details - CM

Switch Password

Confirm Switch Password

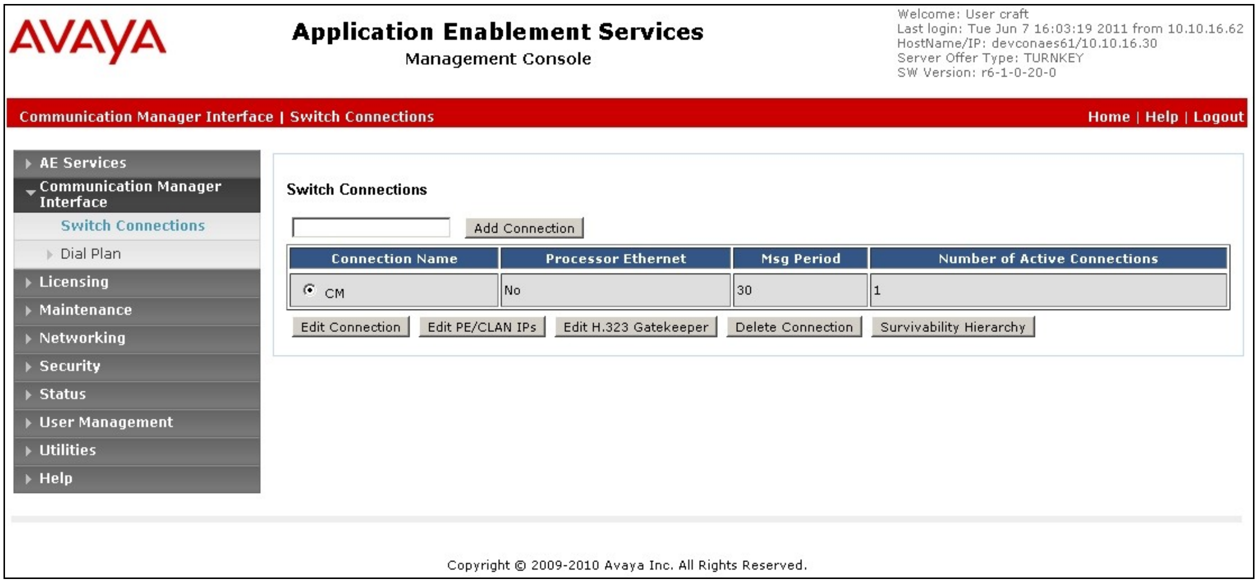
Msg Period 30 Minutes (1 - 72)

SSL ☑

Processor Ethernet □

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

The screen below is displayed. Click on **Edit PE/CLAN IPs** in order to specify the IP address of the C-CLAN, as noted in **Section 5.8**.



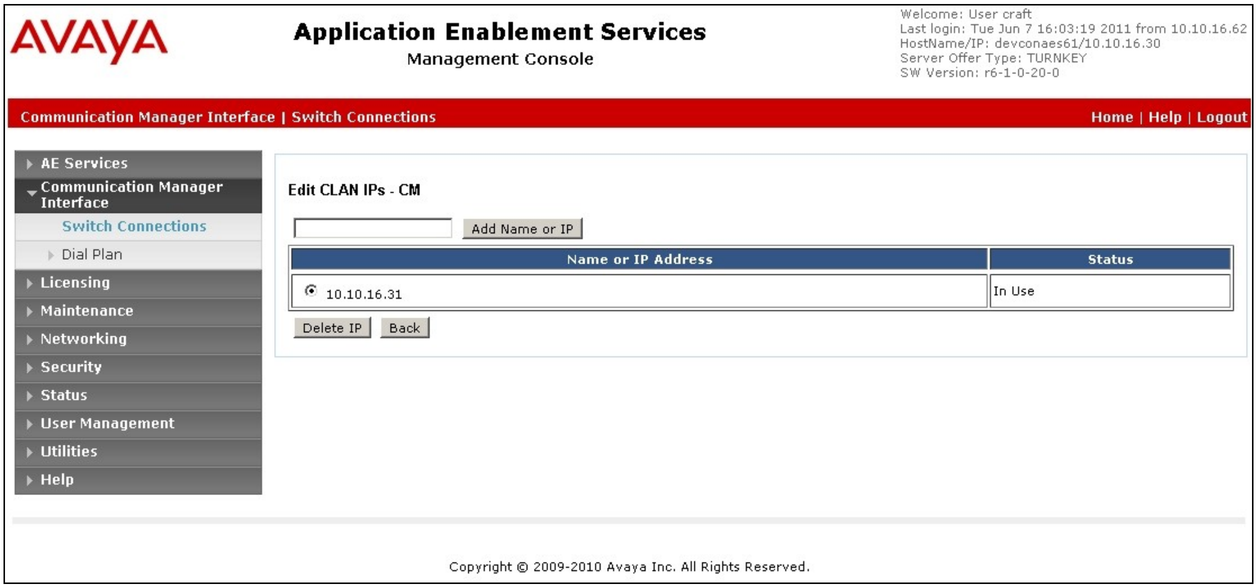
Welcome: User craft
Last login: Tue Jun 7 16:03:19 2011 from 10.10.16.62
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURNKEY
SW Version: r6-1-0-20-0

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● CM	No	30	1

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

Next to **Add Name or IP,** enter the IP address of the C-LAN and click on **Add Name or IP**.



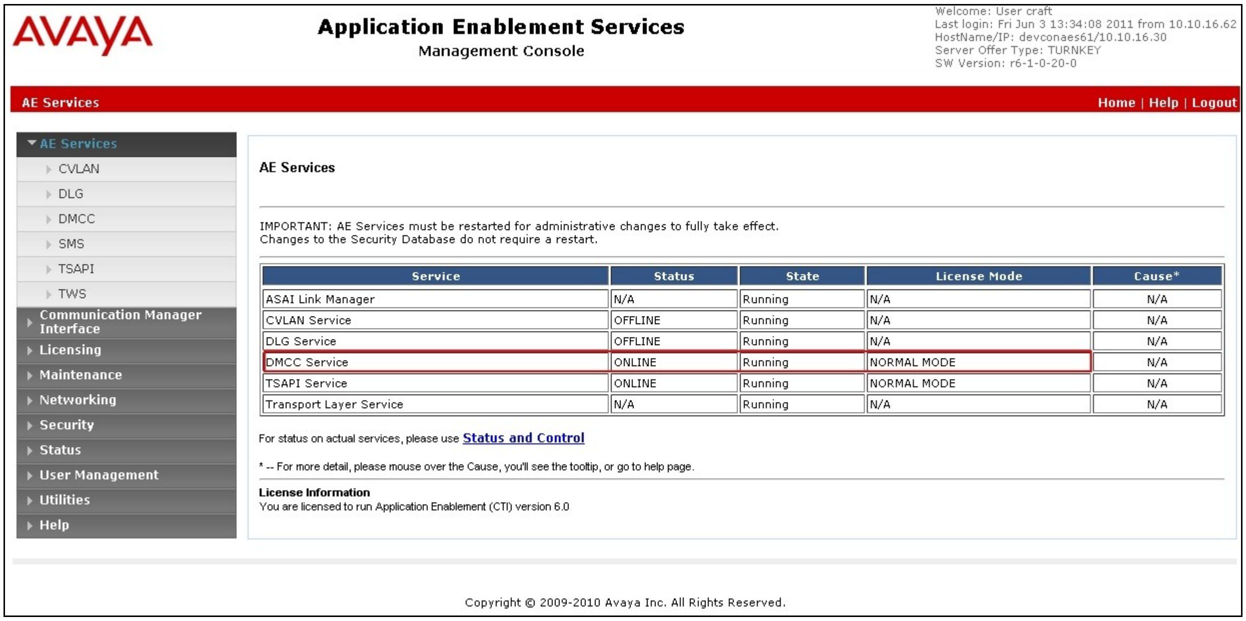
Welcome: User craft
Last login: Tue Jun 7 16:03:19 2011 from 10.10.16.62
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURNKEY
SW Version: r6-1-0-20-0

Edit CLAN IPs - CM

Name or IP Address	Status
● 10.10.16.31	In Use

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

Select **AE Services** on the left frame and verify that the **DMCC Service** is licensed by ensuring that **DMCC Service** is in the list of services and that the **License Mode** is showing **NORMAL MODE**. If not, consult with your Avaya Account Manager or Business Partner to acquire the proper license.



Welcome: User craft
Last login: Fri Jun 3 13:34:08 2011 from 10.10.16.62
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURNKEY
SW Version: r6-1-0-20-0

AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

For status on actual services, please use Status and Control

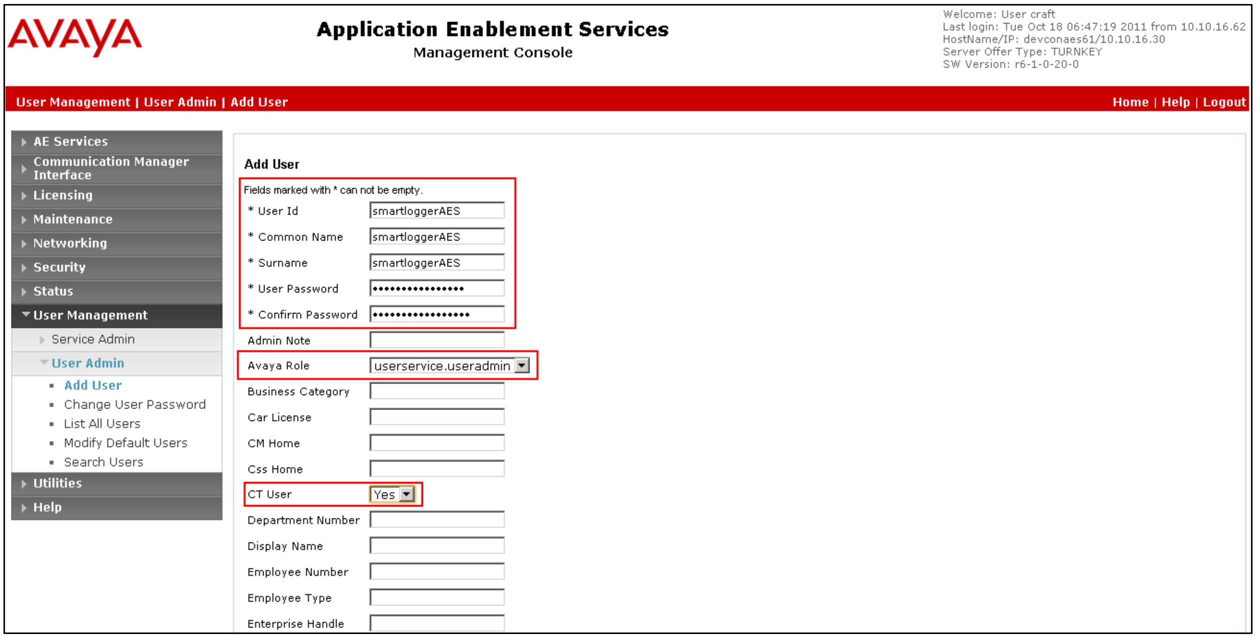
* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information
You are licensed to run Application Enablement (CTI) version 6.0

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

6.3. Create CTI User

A user ID and password needs to be configured for Smart Logger II to communicate as a DMCC Client with the Application Enablement Services. Select **User Management → User Admin → Add User** from the left pane, to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. For **Avaya Role**, select **userservice.useradmin** from the drop down list. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).



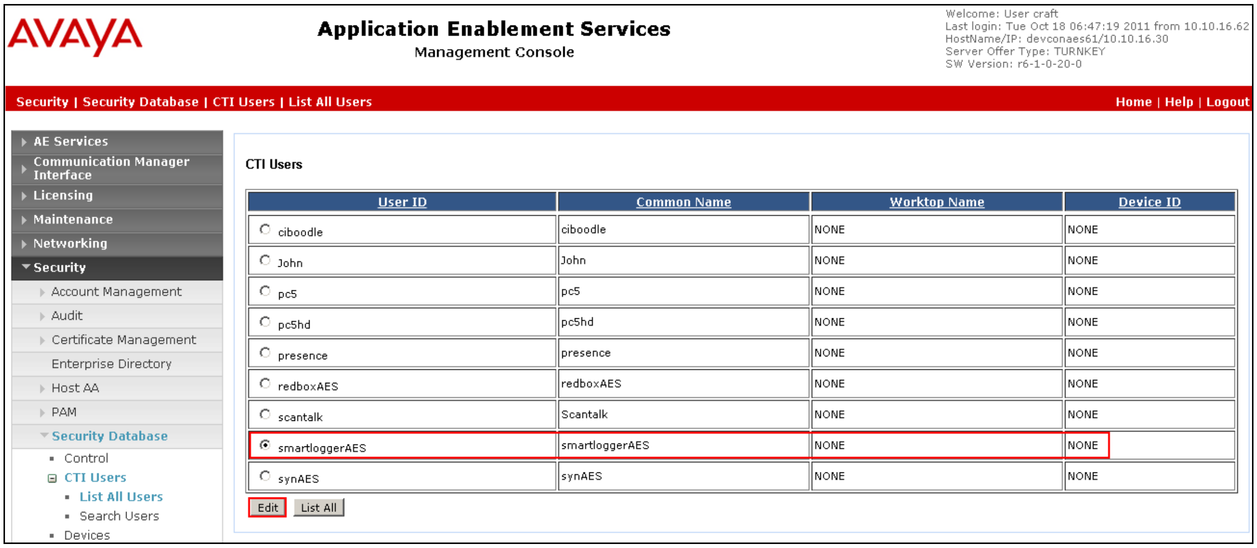
Add User

Fields marked with * can not be empty.

* User Id	smartloggerAES
* Common Name	smartloggerAES
* Surname	smartloggerAES
* User Password	••••••••••••••••
* Confirm Password	•••••••••••••••••
Admin Note	
Avaya Role	userservice.useradmin
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	

6.4. Enable CTI User

Navigate to the users screen by selecting **Security → Security Database → CTI Users → List All Users.** In the **CTI Users** window, select the user that was set up in **Section 6.3** and select the **Edit** option.

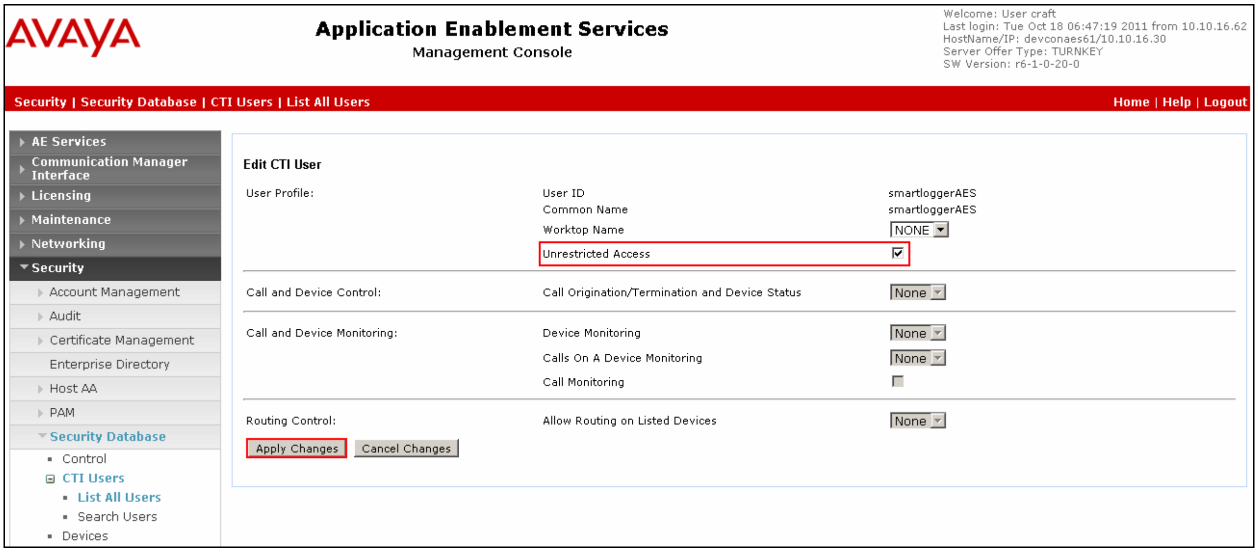


Welcome: User craft
Last login: Tue Oct 18 06:47:19 2011 from 10.10.16.62
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURNKEY
SW Version: r6-1-0-20-0

CTI Users

User ID	Common Name	Worktop Name	Device ID
○ ciboodle	ciboodle	NONE	NONE
○ John	John	NONE	NONE
○ pc5	pc5	NONE	NONE
○ pc5hd	pc5hd	NONE	NONE
○ presence	presence	NONE	NONE
○ redboxAES	redboxAES	NONE	NONE
○ scantalk	Scantalk	NONE	NONE
● smartloggerAES	smartloggerAES	NONE	NONE
○ synAES	synAES	NONE	NONE

The **Edit CTI User** screen appears. Tick the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Tue Oct 18 06:47:19 2011 from 10.10.16.62
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURNKEY
SW Version: r6-1-0-20-0

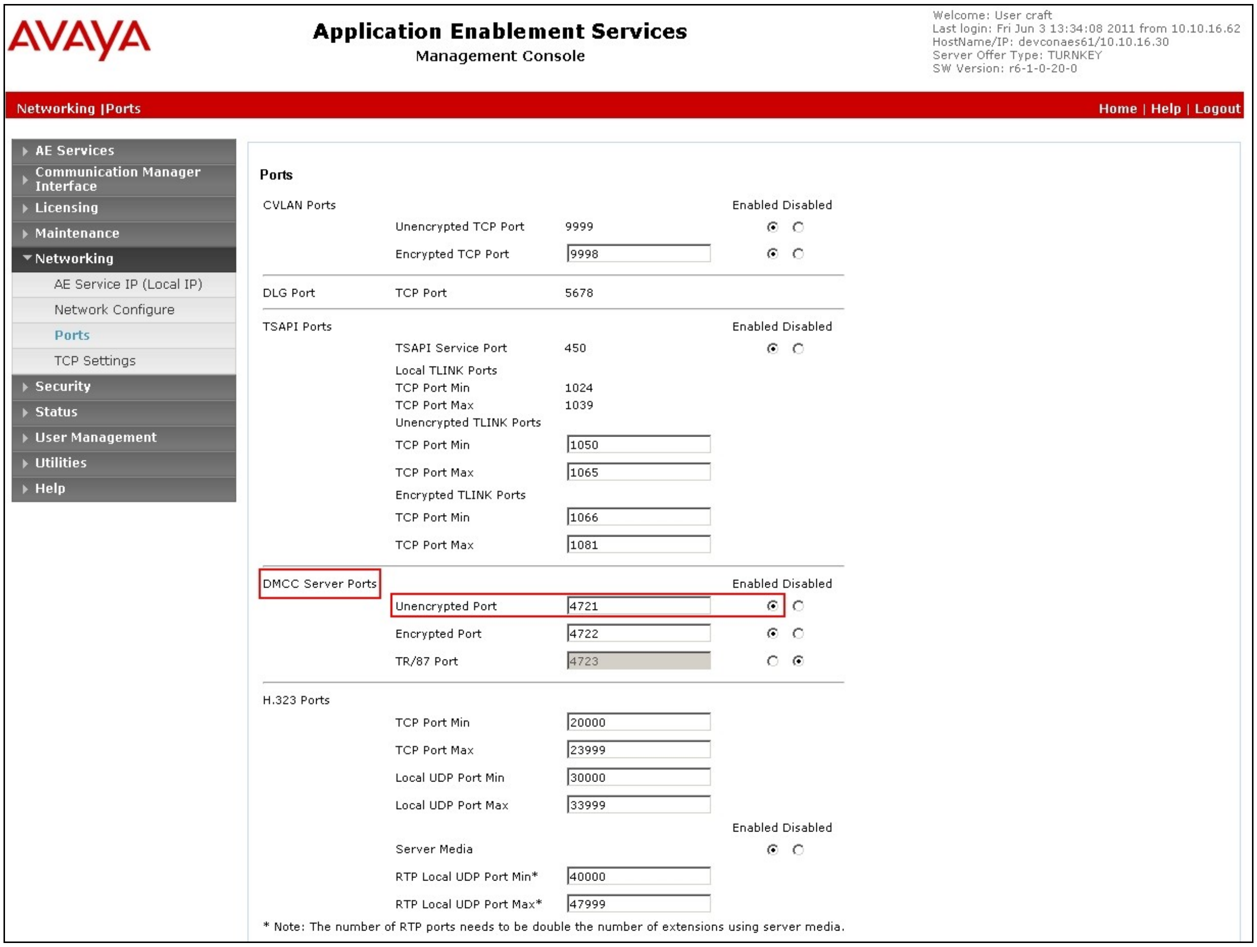
Edit CTI User

User Profile:	User ID	smartloggerAES
	Common Name	smartloggerAES
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	□
Routing Control:	Allow Routing on Listed Devices	None

Apply Changes | Cancel Changes

6.5. Configure DMCC Port

On the AES Management Console navigate to **Networking → Ports** to set the DMCC server port. During the compliance test, the **Unencrypted Port** set to **4721** was **Enabled** as shown in the screen below. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.



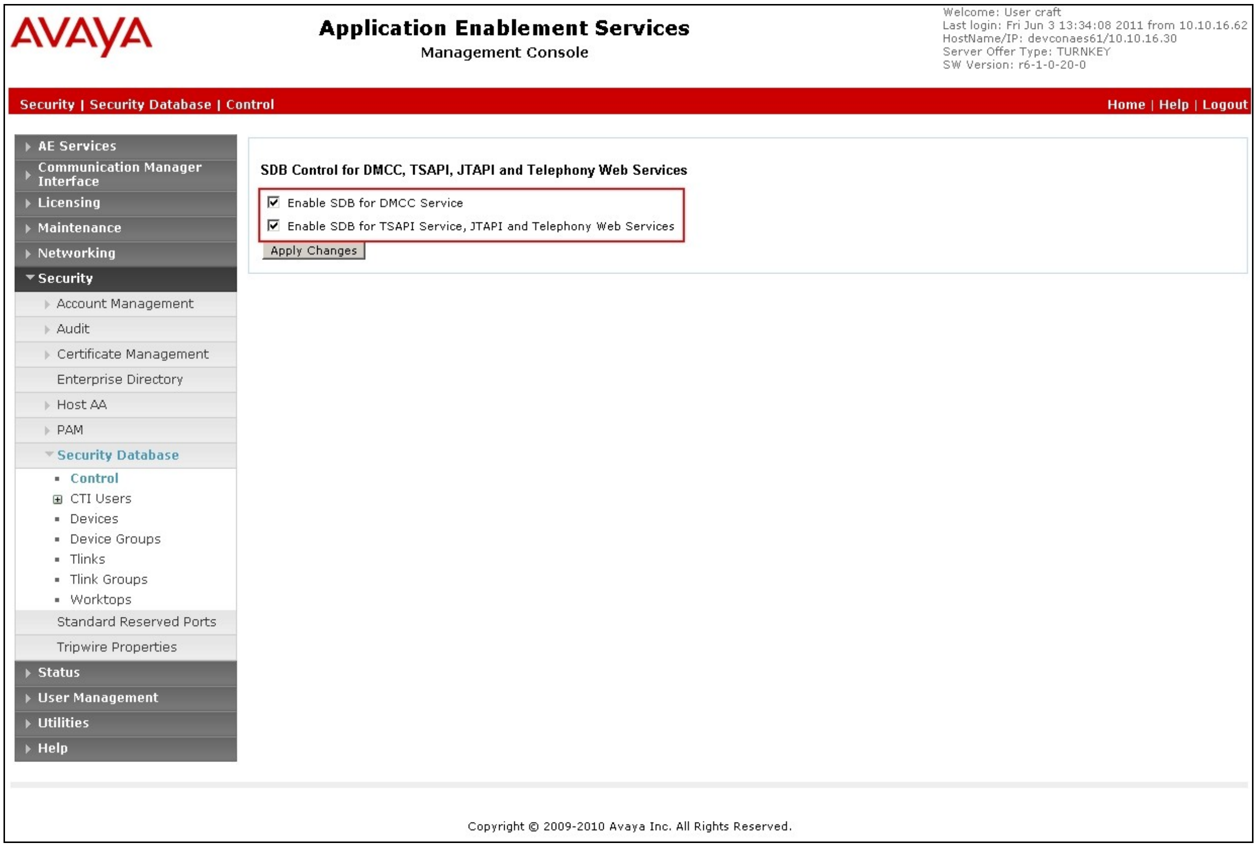
Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports				
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports				
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	○	●
H.323 Ports				
	TCP Port Min	20000		
	TCP Port Max	23999		
	Local UDP Port Min	30000		
	Local UDP Port Max	33999		
	Server Media		●	○
	RTP Local UDP Port Min*	40000		
	RTP Local UDP Port Max*	47999		

* Note: The number of RTP ports needs to be double the number of extensions using server media.

6.6. Enable Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC and TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Check **Enable SDB for DMCC Service** and **Enable SDB TSAPI Service, JTAPI and Telephony Web Services**, and click **Apply Changes.**



SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☑ Enable SDB for DMCC Service

☑ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

7. Configuration of Speech Technology Centre Smart Logger II

The Smart Logger II application is provided and installed by Speech Technology Centre. Smart Logger II runs on Windows XP and configured to obtain a reserved IP address using DHCP. The configuration of this is outside of the scope of this Application Note. The installation process of Smart Logger II is comprised of 4 Microsoft Installation packages (MSI) for each component of the application, installed in the following order:

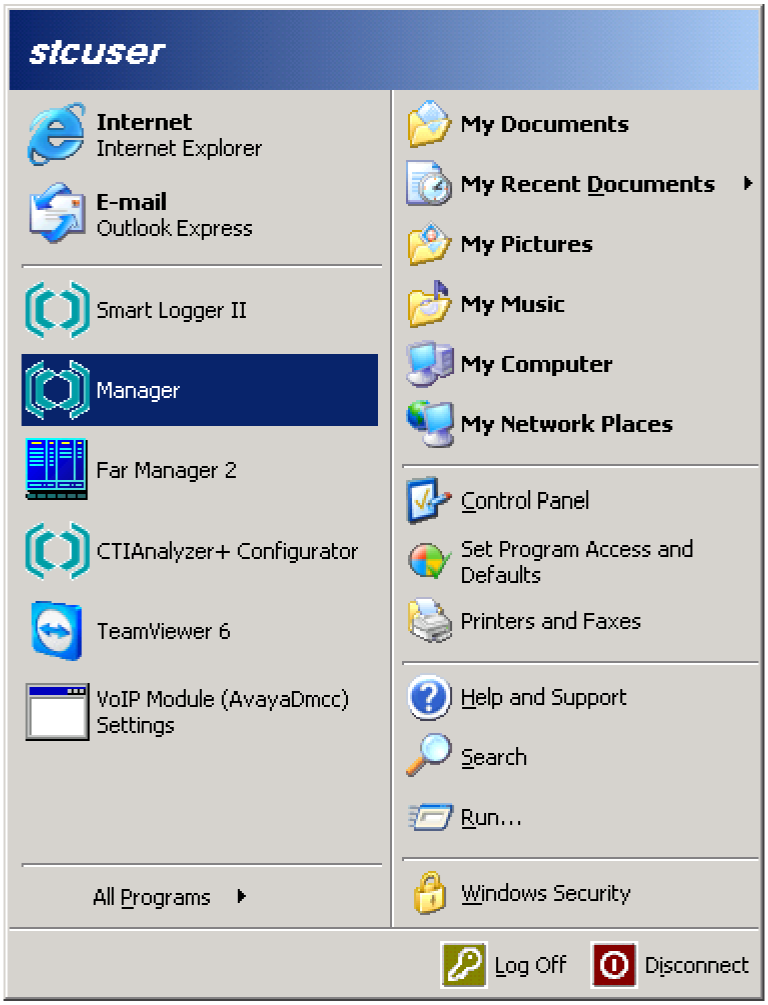
- SmartLoggerII_7.6.15 – the Smart Logger II Application
- SLII_AvayaDmccSource2_7.6.15 – for DMCC connectivity to AES
- SLII_CTIAnalyzerPlus_7.6.15 – for DMCC connection management.
- SLII_Operator_7.6.15 – GUI for Smart Logger II

As a prerequisite, Microsoft SQL, was supplied and installed by Speech Technology Centre to provide the database for calls. Full installation of each component is performed by Speech Technology Centre, only the elements relevant to the configuration for interoperability are detailed here. These can be summarized as:

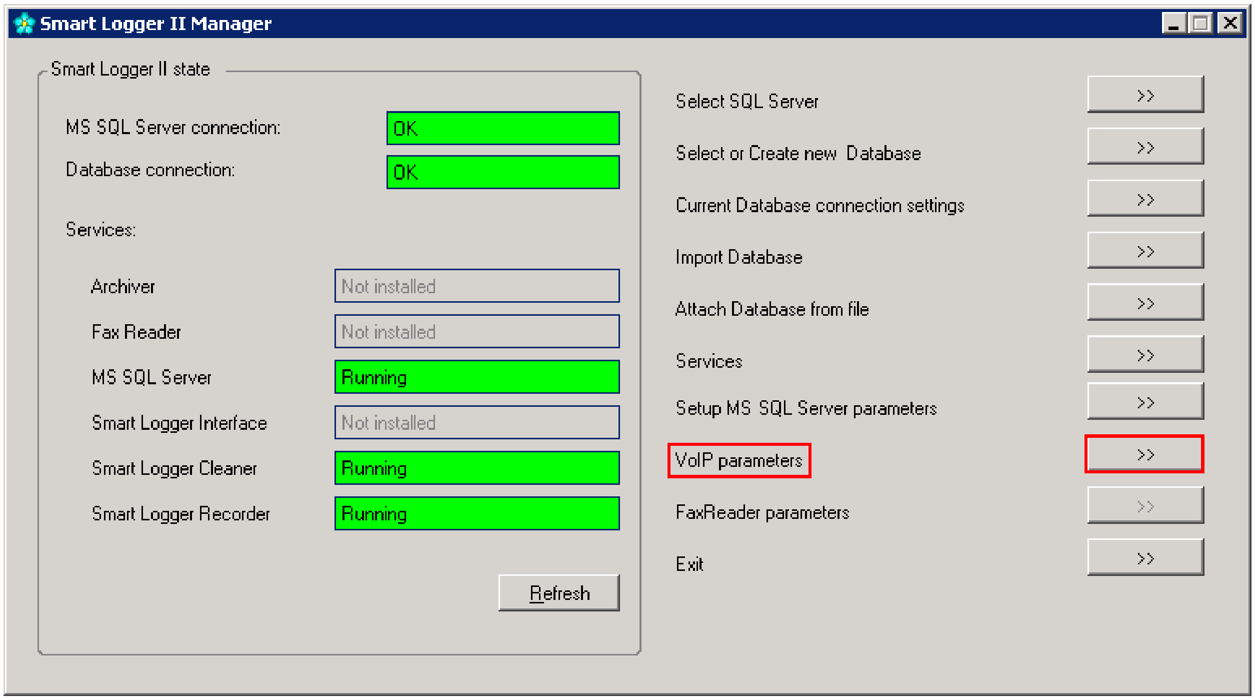
- Register extensions to Smart Logger II
- Configure Smart Logger II connection to AES

7.1. Register extensions to Smart Logger II

On the PC hosting Smart Logger II, click the **Start** menu and click **Manager.**



The screen shown below will be presented, click >> next to **VoIP Parameters**.



Smart Logger II Manager

Smart Logger II state

MS SQL Server connection: OK

Database connection: OK

Services:

Archiver: Not installed

Fax Reader: Not installed

MS SQL Server: Running

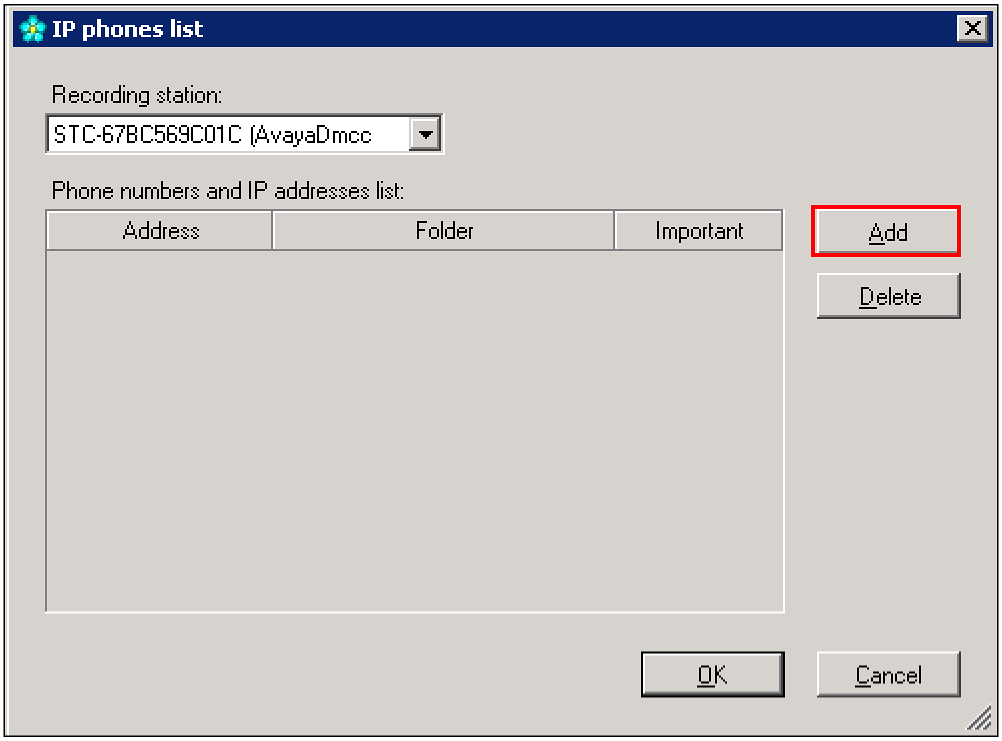
Smart Logger Interface: Not installed

Smart Logger Cleaner: Running

Smart Logger Recorder: Running

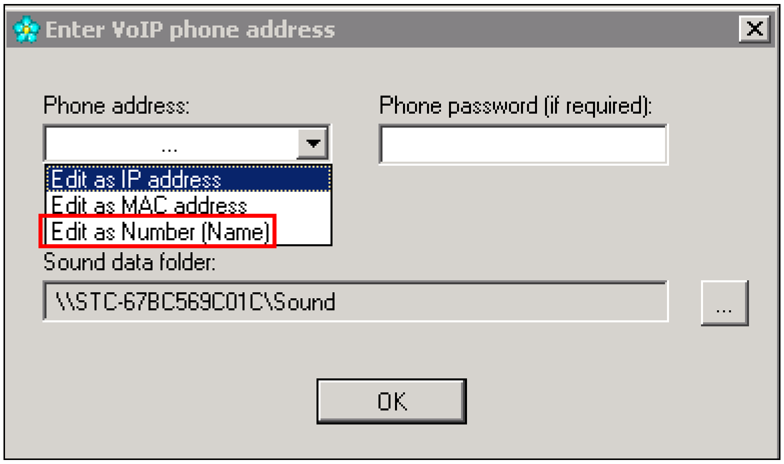
Refresh
Select SQL Server >>
Select or Create new Database >>
Current Database connection settings >>
Import Database >>
Attach Database from file >>
Services >>
Setup MS SQL Server parameters >>
VoIP parameters >>
FaxReader parameters >>
Exit >>

On the screen that appears shown below, click **Add.**



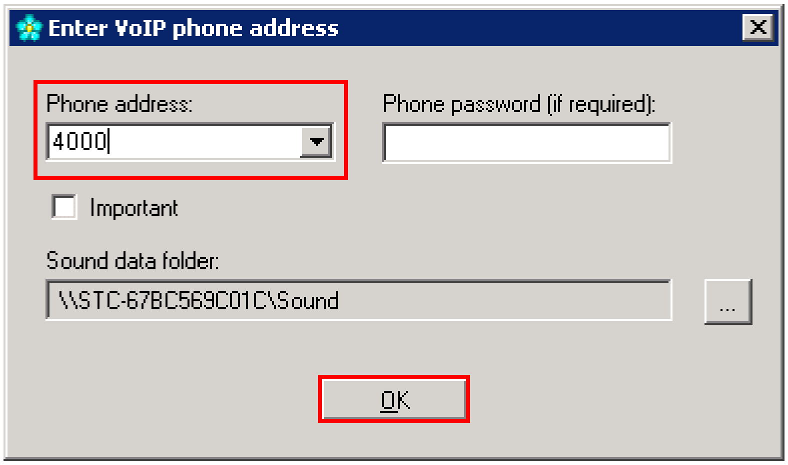
Recording station: STC-67BC569C01C (AvayaDmcc

Choose **Edit as Number (Name)** from the drop down list.



Sound data folder: \\STC-67BC569C01C\Sound

Enter the extension number of an extension to be recorded in the **Phone Address** field and click **OK**. A **Phone password** is not required, as the CTI user is configured on AES with Unrestricted Access.

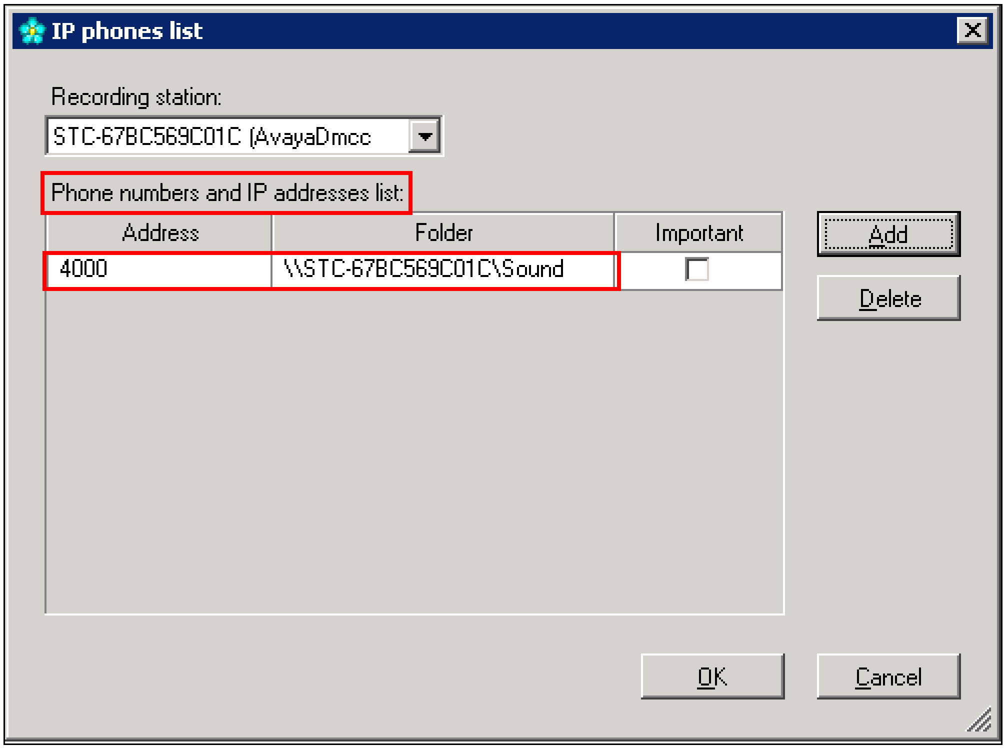


Phone address: 4000

□ Important

Sound data folder: \\STC-67BC569C01C\Sound

The screen below will appear, showing the extension specified above, added to **Phone numbers and IP addresses list**.

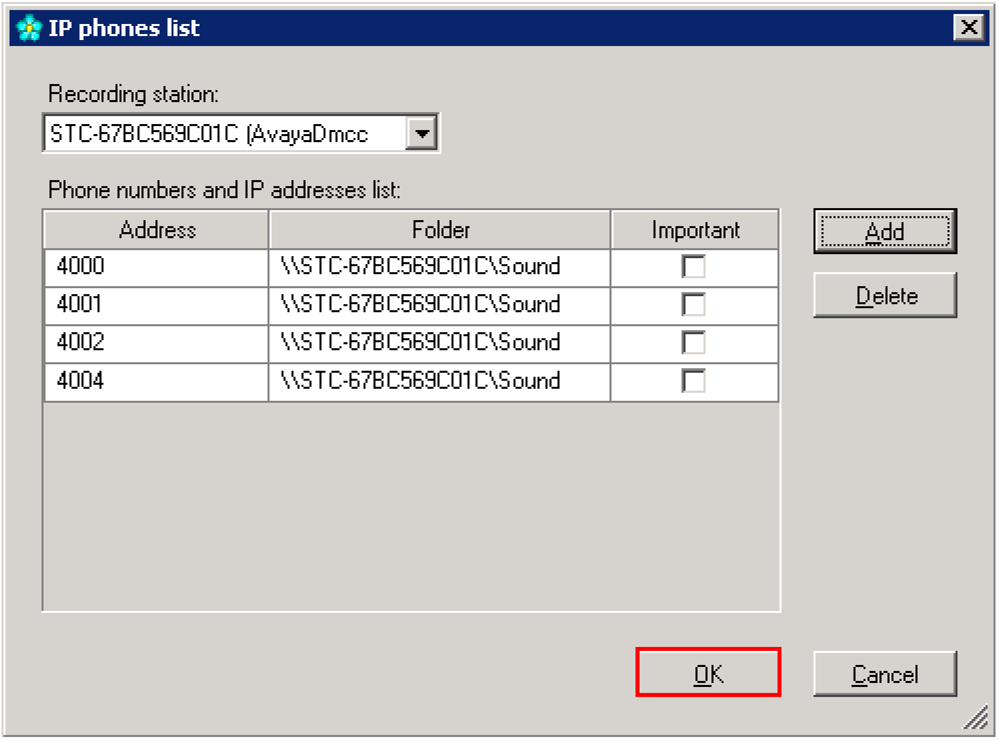


Recording station: STC-67BC569C01C (AvayaDmcc

Phone numbers and IP addresses list:

Address	Folder	Important
4000	\\STC-67BC569C01C\Sound	□

Repeat these steps for each extension to be recorded, click **OK** when complete.



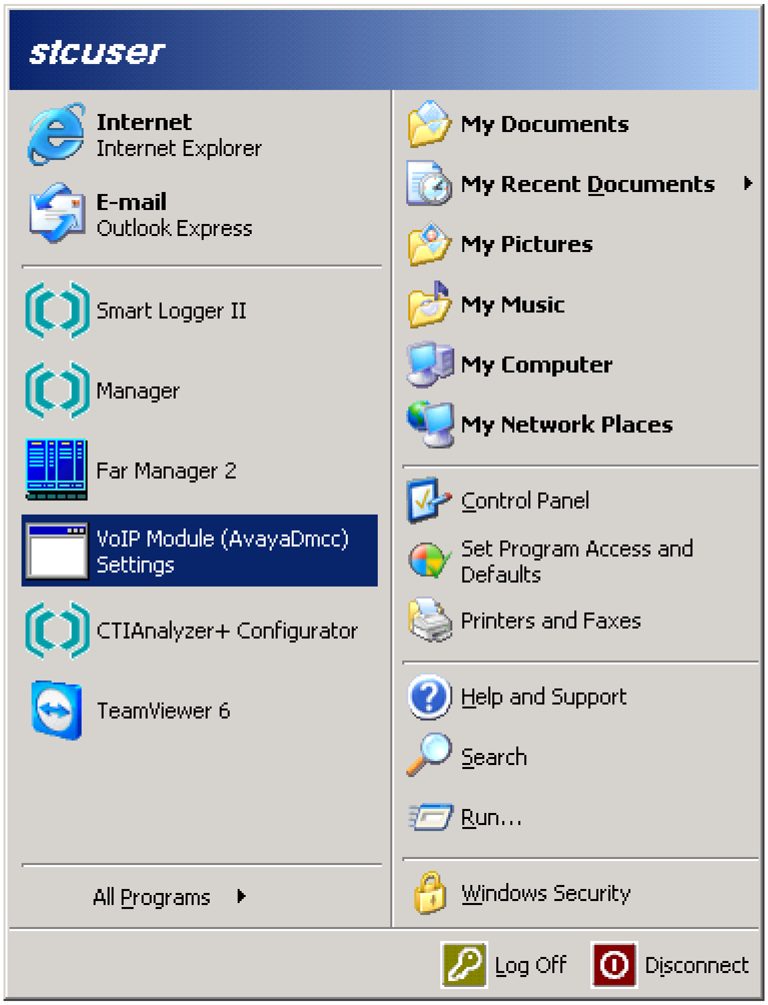
Recording station: STC-67BC569C01C (AvayaDmcc

Phone numbers and IP addresses list:

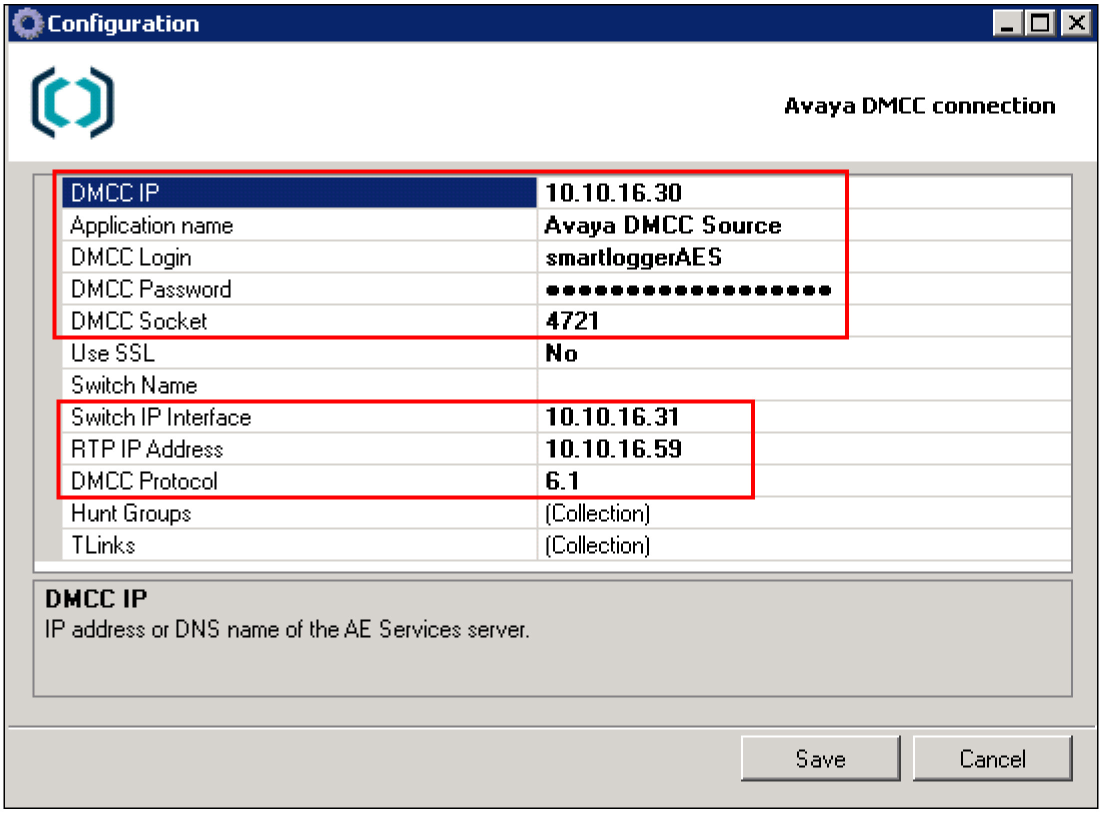
Address	Folder	Important
4000	\\STC-67BC569C01C\Sound	□
4001	\\STC-67BC569C01C\Sound	□
4002	\\STC-67BC569C01C\Sound	□
4004	\\STC-67BC569C01C\Sound	□

7.2. Configure Smart Logger II connection to Avaya Aura® Application Enablement Services

In order for Smart Logger II to connect to AES, the relevant settings must be configured. On the PC hosting Smart Logger II, click the **Start** menu and click **VoIP Module (AvayaDmcc) Settings**.



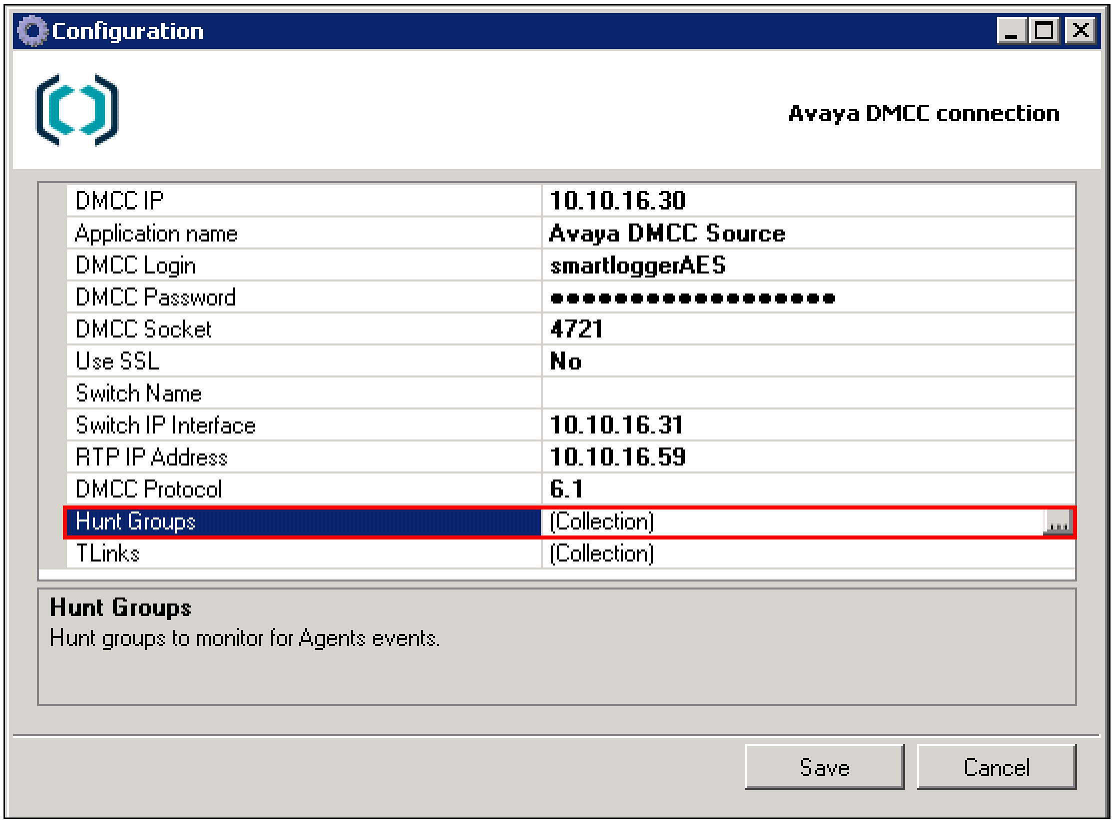
Complete the Avaya DMCC connection properties as shown below where, **DMCC IP** is the AES IP Address, **Application Name** is **Avaya DMCC Source, DMCC Login** is the user added on AES, **DMCC Password** is the password configured for the user added on AES, **DMCC Socket** is as specified in **Section 6.5**, **Switch IP Interface** is the address of the C-LAN and **RTP IP Address** is the IP address of the Smart Logger PC.



DMCC IP	10.10.16.30
Application name	Avaya DMCC Source
DMCC Login	smartloggerAES
DMCC Password	●●●●●●●●●●●●●●●●●●
DMCC Socket	4721
Use SSL	No
Switch Name	
Switch IP Interface	10.10.16.31
RTP IP Address	10.10.16.59
DMCC Protocol	6.1
Hunt Groups	(Collection)
TLinks	(Collection)

DMCC IP
IP address or DNS name of the AE Services server.

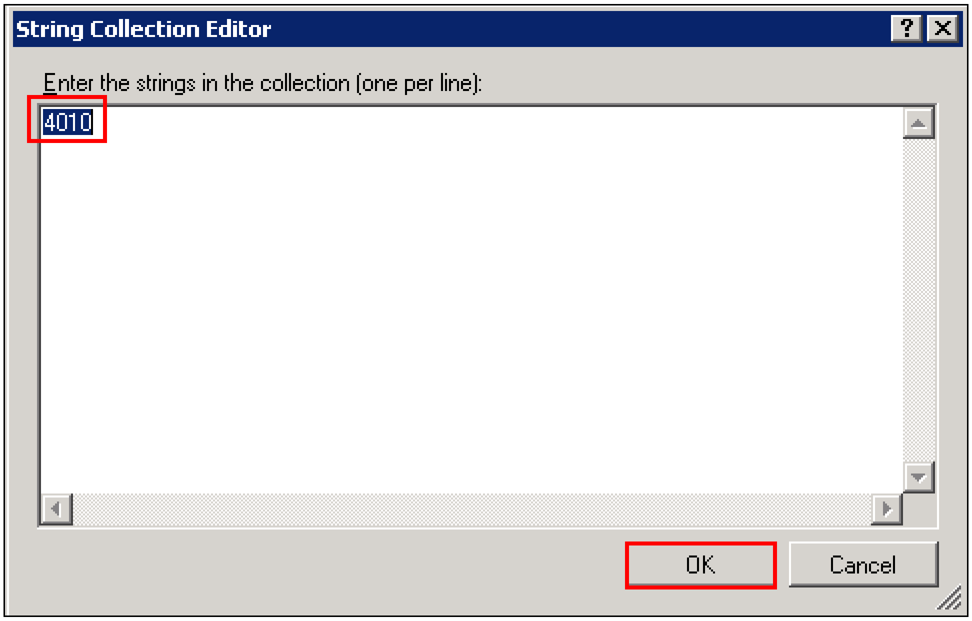
Select **Hunt Groups** and click **…**



DMCC IP	10.10.16.30
Application name	Avaya DMCC Source
DMCC Login	smartloggerAES
DMCC Password	●●●●●●●●●●●●●●●●●●
DMCC Socket	4721
Use SSL	No
Switch Name	
Switch IP Interface	10.10.16.31
RTP IP Address	10.10.16.59
DMCC Protocol	6.1
Hunt Groups	(Collection)
TLinks	(Collection)

Hunt Groups
Hunt groups to monitor for Agents events.

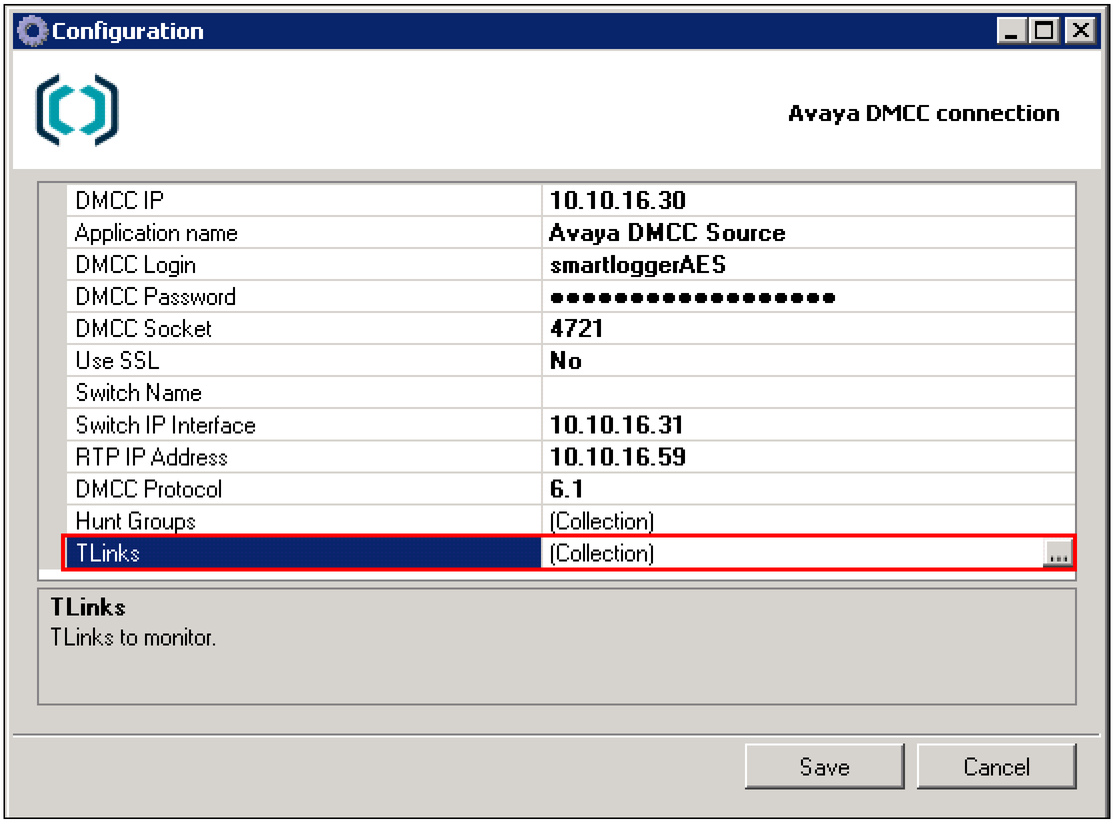
Enter the extension number of the Smart Logger II Monitor hunt group in the screen that appears and click **OK**, shown below.



Enter the strings in the collection (one per line):

4010

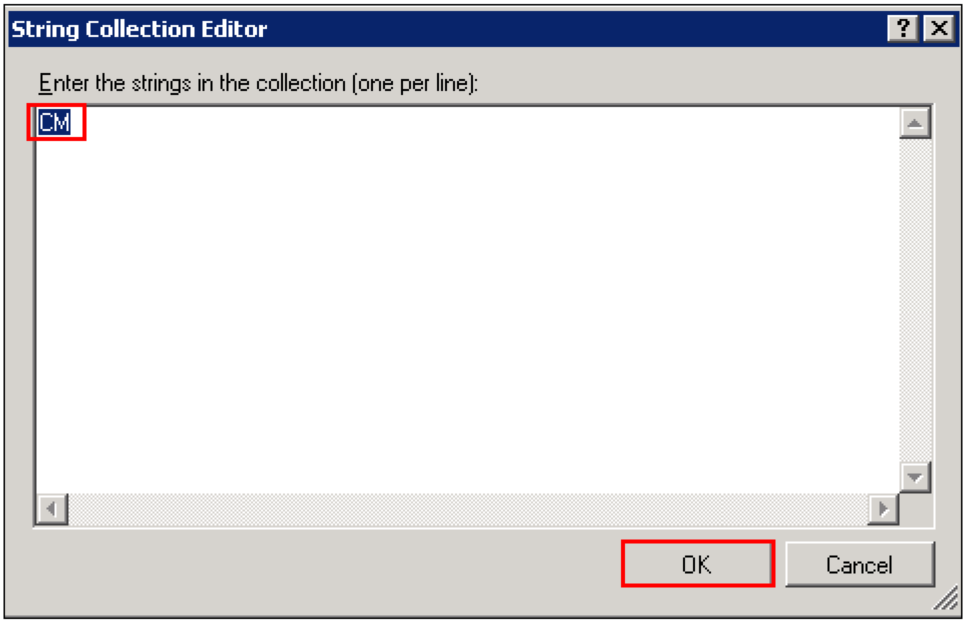
Select **TLinks** and click **…**



DMCC IP	10.10.16.30
Application name	Avaya DMCC Source
DMCC Login	smartloggerAES
DMCC Password	●●●●●●●●●●●●●●●●●●
DMCC Socket	4721
Use SSL	No
Switch Name	
Switch IP Interface	10.10.16.31
RTP IP Address	10.10.16.59
DMCC Protocol	6.1
Hunt Groups	(Collection)
TLinks	(Collection)

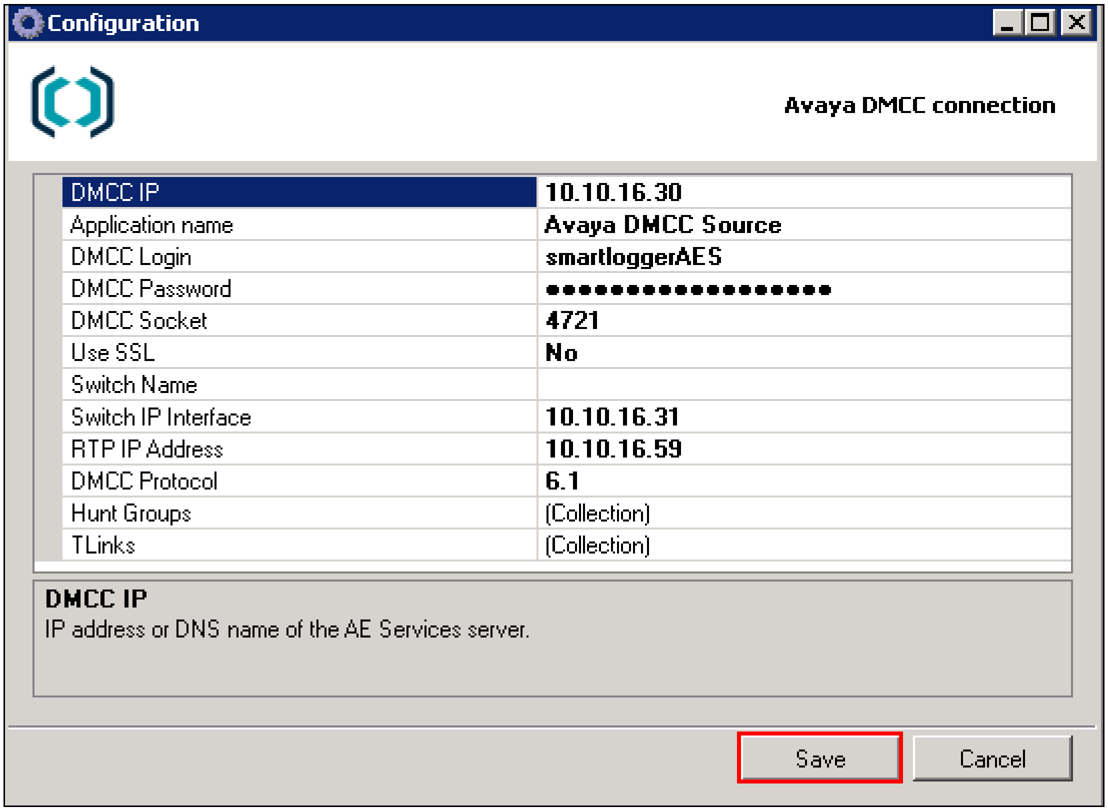
TLinks
TLinks to monitor.

Specify the name of the TLink, this must be identical to the name configured in the connection added in **Section 6.2** and click **OK.**



CM

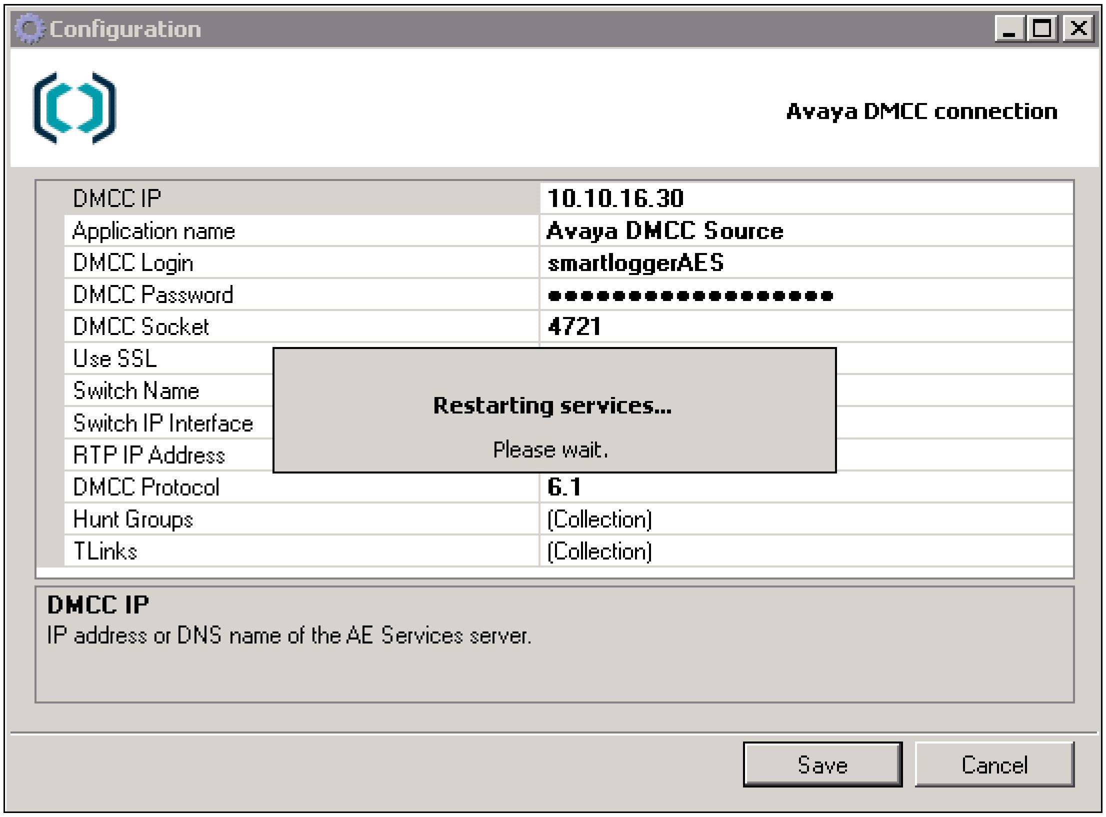
Click **Save** to commit the settings configured.



DMCC IP	10.10.16.30
Application name	Avaya DMCC Source
DMCC Login	smartloggerAES
DMCC Password	●●●●●●●●●●●●●●●●●●
DMCC Socket	4721
Use SSL	No
Switch Name	
Switch IP Interface	10.10.16.31
RTP IP Address	10.10.16.59
DMCC Protocol	6.1
Hunt Groups	(Collection)
TLinks	(Collection)

DMCC IP
IP address or DNS name of the AE Services server.

The screen below will be shown, advising the restart of the Smart Logger II services with the new configuration.



DMCC IP	10.10.16.30
Application name	Avaya DMCC Source
DMCC Login	smartloggerAES
DMCC Password	●●●●●●●●●●●●●●●●●●
DMCC Socket	4721
Use SSL	
Switch Name	
Switch IP Interface	
RTP IP Address	
DMCC Protocol	6.1
Hunt Groups	(Collection)
TLinks	(Collection)

Restarting services...

Please wait.

DMCC IP
IP address or DNS name of the AE Services server.

8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Avaya and Speech Technology Centre solution.

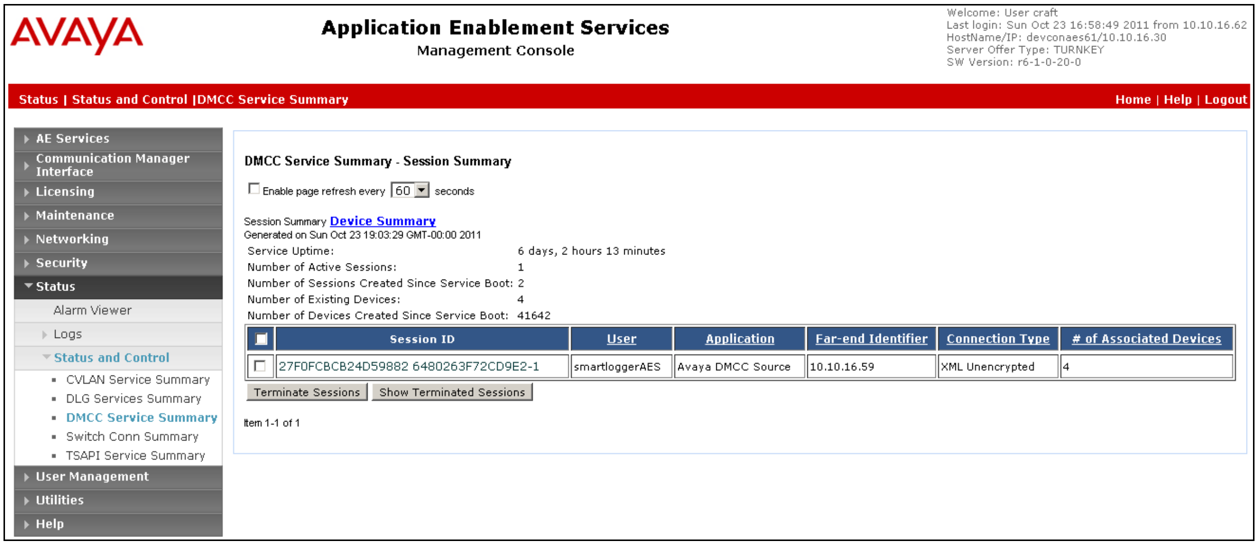
8.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Using SAT connect to Communication Manager and check the AESVCS link status with Application Enablement Services by using the command **status aesvcs cti-link**. The CTI Link is 1. Verify the **Service State** of the CTI link is **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      devconaes61    established   18       18
```

8.2. Verify Avaya Aura® Application Enablement Services DMCC Service

The following steps are carried out on the AES to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly. Verify the status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary.** The **DMCC Service Summary – Session Summary** screen is displayed as shown below. It shows a connection to the Smart Logger II PC, IP address **10.10.16.59**. The **Application** is set to **Avaya DMCC Source** and the **Far-end Identifier** is given as the IP address **10.10.16.59** as expected.



Welcome: User craft
Last login: Sun Oct 23 16:58:49 2011 from 10.10.16.62
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURNKEY
SW Version: r6-1-0-20-0

DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Sun Oct 23 19:03:29 GMT-00:00 2011

```
Service Uptime:                              6 days, 2 hours 13 minutes
Number of Active Sessions:                   1
Number of Sessions Created Since Service Boot: 2
Number of Existing Devices:                  4
Number of Devices Created Since Service Boot: 41642
```

☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	27F0FCBCB24D59882 6480263F72CD9E2-1	smartloggerAES	Avaya DMCC Source	10.10.16.59	XML Unencrypted	4

Item 1-1 of 1

8.3. Verify Smart Logger II Configuration

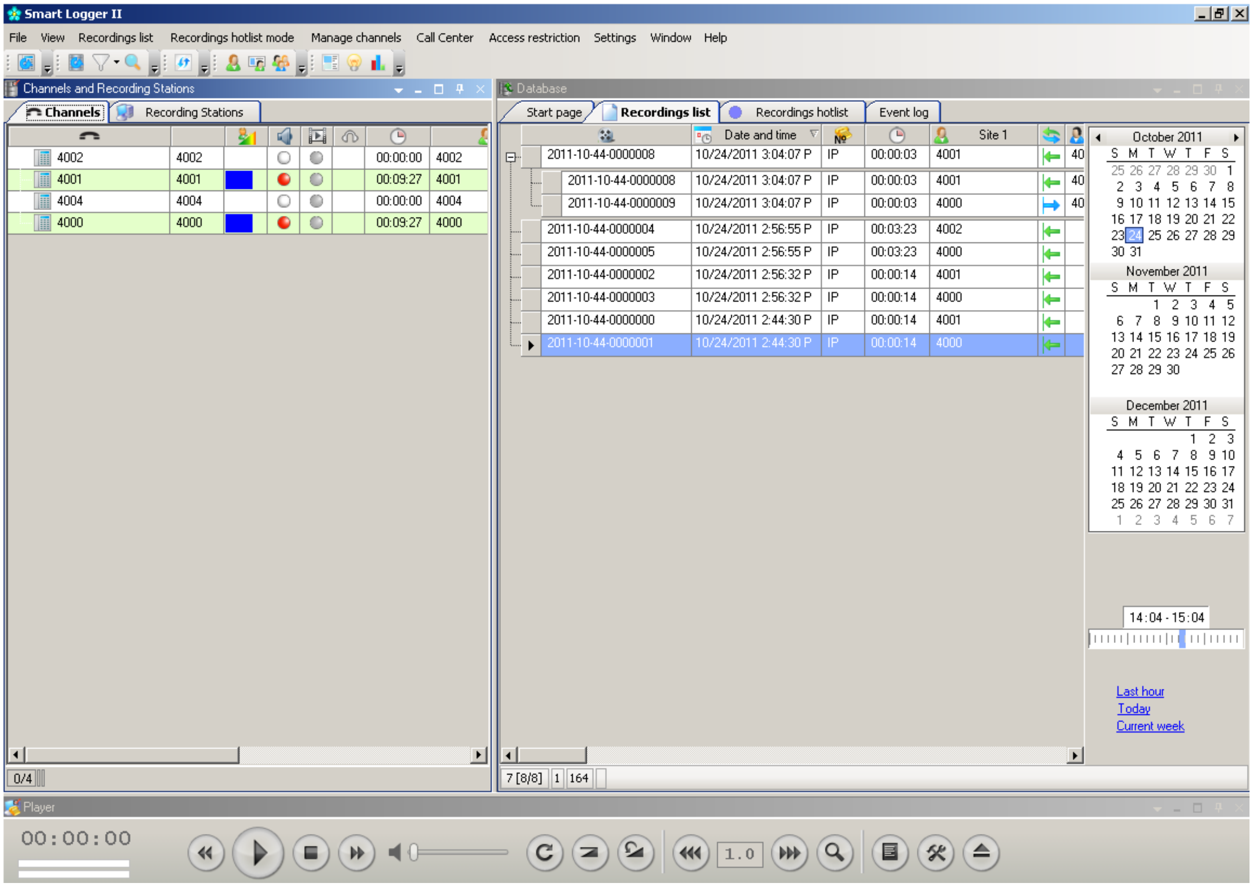
The following steps can be performed to verify the basic operation of the system components. To confirm DMCC connection to AES, in an appropriate text editor, on the Smart Logger II PC, open **AvayaDmccFull.log** contained in **c:\program files\Speech Technology Centre\CTIAnalyzerPlus\logs**. A successful connection can be verified by the following lines contained in the log:

```
2011-10-10 19:06:45,359 [Connection restore] DEBUG avaya_dmcc_source -
Conncting to AES with settings:
(SessionSettings)
ServerIp:                          10.10.16.30
ServerPort:                        4721
ApplicationName:                   Avaya DMCC Source
UserName:                          smartloggerAES
UserPassword:                      smartloggerAES123!
SessionCleanupDelay:               60
SessionDuration:                   180
ProtocolVersion:                   http://www.ecma-
international.org/standards/ecma-323/csta/ed3/priv5
Secure:                            False
UserState:
StartAutoKeepAlive:                True
AllowCertificateHostnameMismatch:  True

2011-10-10 19:06:45,906 [Connection restore] DEBUG avaya_dmcc_source -
ConnectionWatcher.ThreadFunc: Connected to AES
```

In the same file, the following lines verify successful registration of a recorded endpoint:

```
2011-10-17 19:18:27,085 [Device connect] INFO  avaya_dmcc_source -
(InteractCore.DmccDevice) InitializeDeviceId: DeviceId initialized
successfully for extension '4000'
2011-10-17 19:18:27,242 [Device connect] INFO  avaya_dmcc_source -
(InteractCore.DmccDevice) InitializeCallsMonitoring: Call monitirong
initialized successfully for extension '4000'
2011-10-17 19:18:27,242 [Device connect] INFO  avaya_dmcc_source -
(InteractCore.DmccDevice) StartMonitorMediaEvents: Media monitirong
initialized successfully for extension '4000'
2011-10-17 19:18:27,382 [Device connect] INFO  avaya_dmcc_source -
DmccDevice.RegisterAsTerminal: Terminal successfully registered for extension
'4000'
2011-10-17 19:18:27,398 [Device connect] INFO  avaya_dmcc_source -
DmccDevice.StartPhoneMonitor: Phone monitoring successfully started for
extension '4000'. MonitorId - '14240'
```

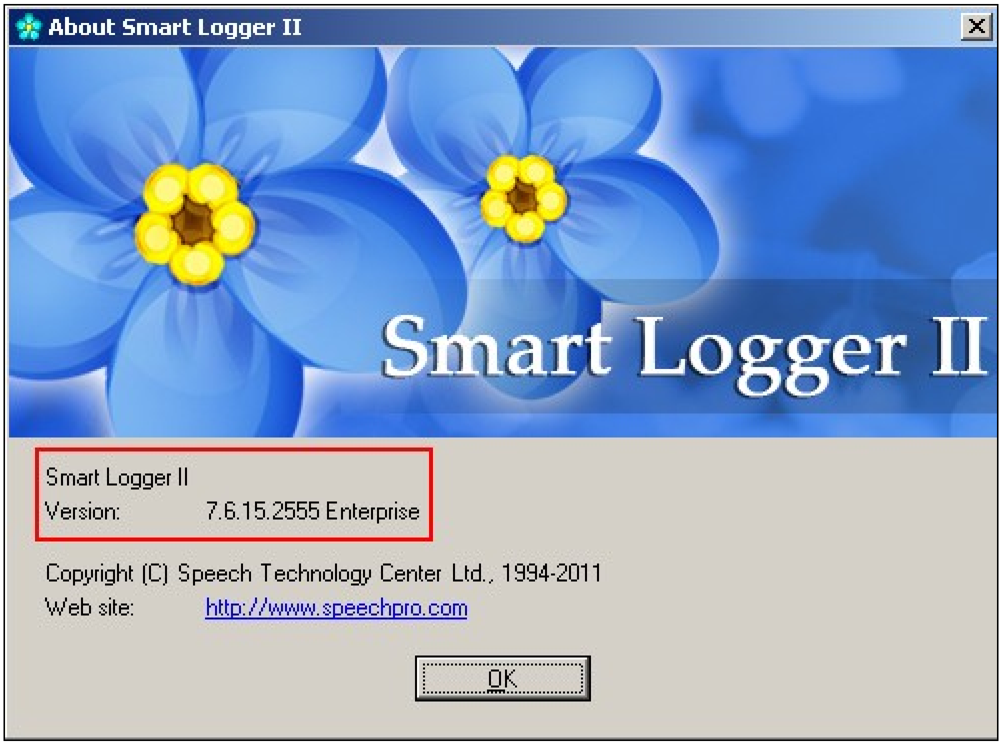
In the **Channels and Recording Stations** pane of the Smart Logger II application, verify that there are no alarms. If all is functioning as expected Smart Logger II application page should appear as in the screen below. Recorded calls are in the right hand pane, and calls in progress, denoted by a red dot next to them are in the left pane. The pane at the bottom of the screen allows playback control of a selected call.



4002	4002		○	●		00:00:00	4002
4001	4001	🟦	🔴	●		00:09:27	4001
4004	4004		○	●		00:00:00	4004
4000	4000	🟦	🔴	●		00:09:27	4000

	Date and time			Site 1		
2011-10-44-0000008	10/24/2011 3:04:07 P	IP	00:00:03	4001	←	40
2011-10-44-0000008	10/24/2011 3:04:07 P	IP	00:00:03	4001	←	40
2011-10-44-0000009	10/24/2011 3:04:07 P	IP	00:00:03	4000	→	40
2011-10-44-0000004	10/24/2011 2:56:55 P	IP	00:03:23	4002	←	
2011-10-44-0000005	10/24/2011 2:56:55 P	IP	00:03:23	4000	←	
2011-10-44-0000002	10/24/2011 2:56:32 P	IP	00:00:14	4001	←	
2011-10-44-0000003	10/24/2011 2:56:32 P	IP	00:00:14	4000	←	
2011-10-44-0000000	10/24/2011 2:44:30 P	IP	00:00:14	4001	←	
2011-10-44-0000001	10/24/2011 2:44:30 P	IP	00:00:14	4000	←	

Click on **Help → About** to check the version number of the recorder to ensure that the version is as expected.



About Smart Logger II

Smart Logger II
Version: 7.6.15.2555 Enterprise

Copyright (C) Speech Technology Center Ltd., 1994-2011
Web site: http://www.speechpro.com

9. Conclusion

These Application Notes describe the configuration steps required for the Speech Technology Centre Smart Logger II to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All functionality and serviceability test cases were completed successfully, and observations made during compliance testing are detailed in **Section 2.2**.

10. Additional References

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

[1] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide – Release 6.1, Issue 2, February 2011*

[2] *Administering Avaya Aura® Communication Manager – Release 6.0, Issue 6.0, June 2010*

Product documentation for Smart Logger II can be found at http://www.speechpro.com

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