Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3 to interoperate with Speech Technology Centre Smart Logger II v8.4 using Multiple Device Registration – 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 is a voice recording solution which can be used to record voice streams for Avaya telephony.

Readers should pay attention to section 2, in particular the scope of testing as outlined in Section 2.1 as well as the observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

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/records the RTP media stream to and from the extension.

2. General Test Approach and Test results

The interoperability compliance test 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.

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

2.1. Interoperability Compliance Testing

The 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. The serviceability testing focused on verifying the ability of Smart Logger II to recover from disconnection and reconnection of the Avaya solution. Other areas of focus included the recording of calls in following scenarios:

- Basic calls to/from Extensions
- Basic calls to/from Agents
- Basic calls to Hunt Groups (Skills)
- Calls to/from the PSTN
- Hold/Retrieve
- Blind and Supervised Transfers
- Conference Calls

Note: Bridged appearances or EC500 was not tested during compliance testing. At the request of Speech Technology Centre SIP endpoints were not monitored.

2.2. Test Results

Tests were performed to ensure full interoperability of Speech Technology Centre Smart Logger II with Communication Manager and AES (using Multiple Registrations). The tests were all functional in nature and performance testing was not included. All the test cases passed successfully with the following observation:

- Due to disk write caching on the Smart Logger II server OS, calls in progress for a short time are lost when the power to the recorder was disconnected. This can be addressed with a freeware disk caching utility used to amend the rate at which data is committed to the hard drive.

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 configuration used during compliance testing. The Avaya solution consists of Communication Manager, System Manager, Session Manager, AES and an Avaya G430 Gateway. The Communication Manager is configured to communicate to the Smart Logger II server via the Application Enablement Services. Smart Logger II records voice conversations from telephones registered to the Communication Manager (Communication Manager extensions). The TSAPI and DMCC services provided by AES are used to monitor call activity and capture voice streams associated with the Communication Manager extensions.

When a call is recorded, the Smart Logger II system uses the Communication Manager Multiple Registrations feature to initiate monitoring for calls which it wishes to record. The voice stream for such calls is received via the LAN interface to the Communication Manager. A Smart Logger II Client is configured to allow users to replay the recorded calls which are stored on the Smart Logger II Server.

Note: The Smart Logger II Client was configured on the Smart Logger II Server during compliance testing, but may also be installed on a separate PC.

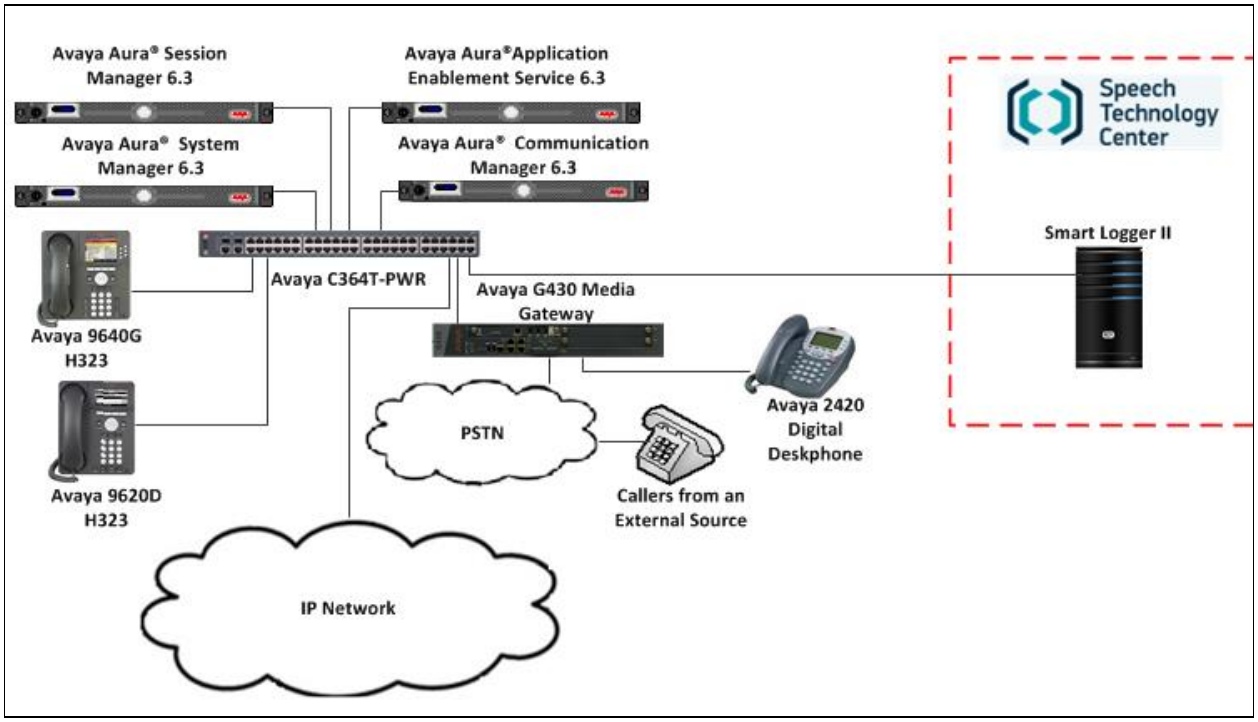

Avaya Aura® Session Manager 6.3
Avaya Aura®Application Enablement Service 6.3
Avaya Aura® System Manager 6.3
Avaya Aura® Communication Manager 6.3
Speech Technology Center
Smart Logger II
Avaya C364T-PWR
Avaya G430 Media Gateway
Avaya 9640G H323
Avaya 9620D H323
Avaya 2420 Digital Deskphone
PSTN
Callers from an External Source
IP Network

Figure 1: Avaya and Speech Technology Centre Reference Configuration

4. Equipment and Software Validated

The hardware and associated software used for the compliance test is listed below.

Avaya Equipment	**Software Version**
Avaya Aura® Communication Manager	R6.3 Build R016x.03.0.124.0
Avaya Aura® Session Manager	R6.3.7 Software Update 6.3.7.0.637008
Avaya Aura® System Manager	R6.3.7 Build 6.3.0.8.5682-6.3.8.-3204 Update 6.3.7.7.2275
Avaya Aura® Application Enablement Services	R6.3 Build 6.3.0.0.212-0
Avaya G430 Media Gateway Module MM710 (DSP MP20)	Version 36.7.0/1 Version HW04 FW021
Avaya Media Gateway DSP module	MP20 FW 132
Avaya 96xx IP phones 9640G 9620D Avaya 2420 Digital phone	 3.1.05S 3.1.01S Rel 6.0, FWV 6
Speech Technology Centre Equipment	**Software Version**
Windows 2008 Server R2 Enterprise SP1 (64 bit)	STC Smart Logger II Avaya DMCC Recorder package 8.4.2050 STC Smart Logger II CTI Analyzer package 8.4.2042 Smart Logger II client 8.4.2183.2612 Microsoft SQL Express 2008 Microsoft .Net Framework 4.0

Table 1: Hardware and Software Version Numbers

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on the Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of the Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

It is implied a working system is already in place. The configuration operations described in this section can be summarized as follows: (Note: during compliance testing all inputs not highlighted in bold were left as default).

- Verify System Parameters Customer Options
- Verify System Parameters Features
- Configure Service Observe
- Configure Target Stations to be Recorded
- Configure Hunt Group
- Configure Agents
- Create Node Name for Avaya Aura® Application Enablement Services
- Create CTI Link to Avaya Aura® Application Enablement Services
- Configure IP 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. Those items shown in **bold** indicate required values or minimum capacity requirements. If these are not met in the configuration, please contact an Avaya representative for further assistance.

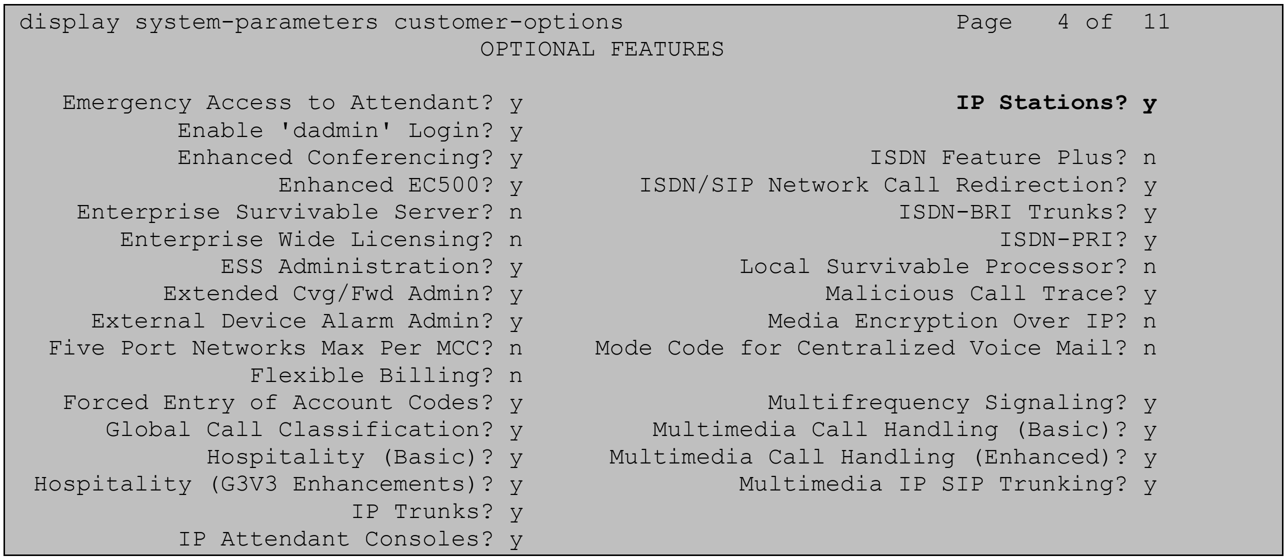
On **Page 2** the **Maximum Concurrently Registered IP Stations** must be sufficient to support the total number of IP stations.

```
   display system-parameters customer-options                       Page   2 of  11
                                   OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 14
           Maximum Concurrently Registered IP Stations: 18000 5
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 1
                   Maximum Video Capable IP Softphones: 18000 4
                       Maximum Administered SIP Trunks: 24000 120
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

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? y
             Access Security Gateway (ASG)? n                Authorization Codes? y
             Analog Trunk Incoming Call ID? y                         CAS Branch? n
      A/D Grp/Sys List Dialing Start at 01? y                           CAS Main? n
     Answer Supervision by Call Classifier? y                 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? n                        DCS (Basic)? y
              ASAI Link Core Capabilities? n                  DCS Call Coverage? y
              ASAI Link Plus Capabilities? n                 DCS with Rerouting? y
                              Async. Transfer Mode (ATM) PNC? n
       Async. Transfer Mode (ATM) Trunking? n     Digital Loss Plan Modification? y
                  ATM WAN Spare Processor? n                            DS1 MSP? y
                                     ATMS? y              DS1 Echo Cancellation? y
                                         Attendant Vectoring? y
```

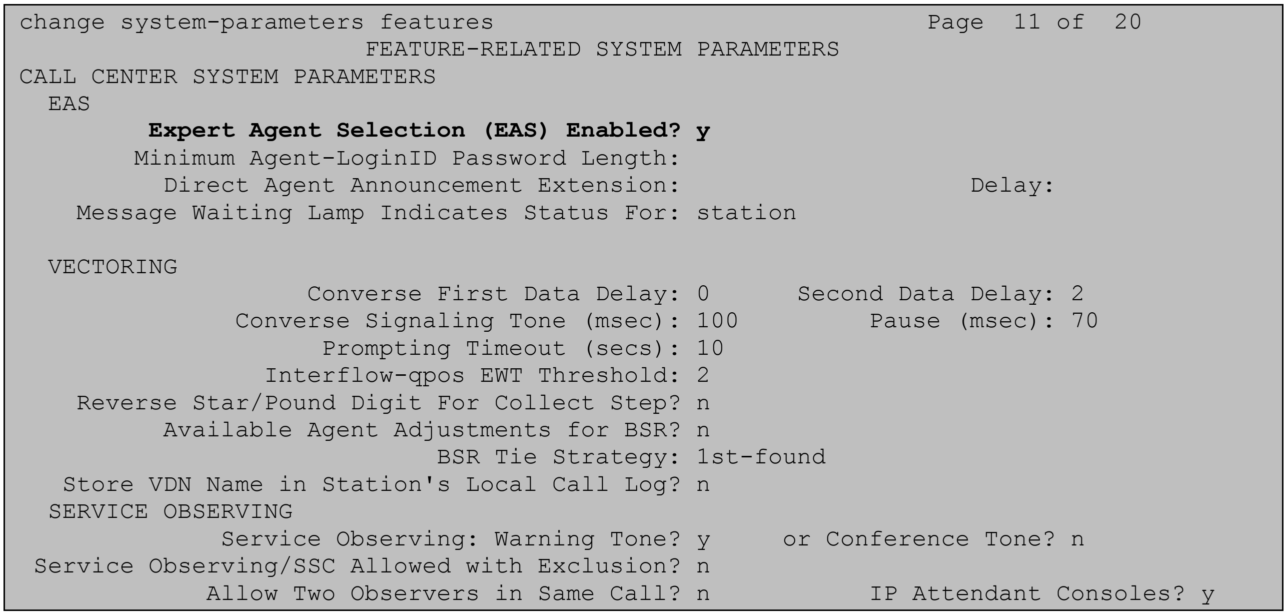
On **Page 4, IP Stations** must be set to **y**.



```
display system-parameters customer-options                       Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                        ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? y               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? y                 Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                 Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y               Multimedia IP SIP Trunking? y
                       IP Trunks? y
           IP Attendant Consoles? y
```

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  20
                        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
                     Prompting Timeout (secs): 10
                 Interflow-qpos EWT Threshold: 2
    Reverse Star/Pound Digit For Collect Step? n
          Available Agent Adjustments for BSR? n
                             BSR Tie Strategy: 1st-found
   Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
              Service Observing: Warning Tone? y     or Conference Tone? n
 Service Observing/SSC Allowed with Exclusion? n
             Allow Two Observers in Same Call? n          IP Attendant Consoles? y
```

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. Use the **change cor 1** command and enter the following:

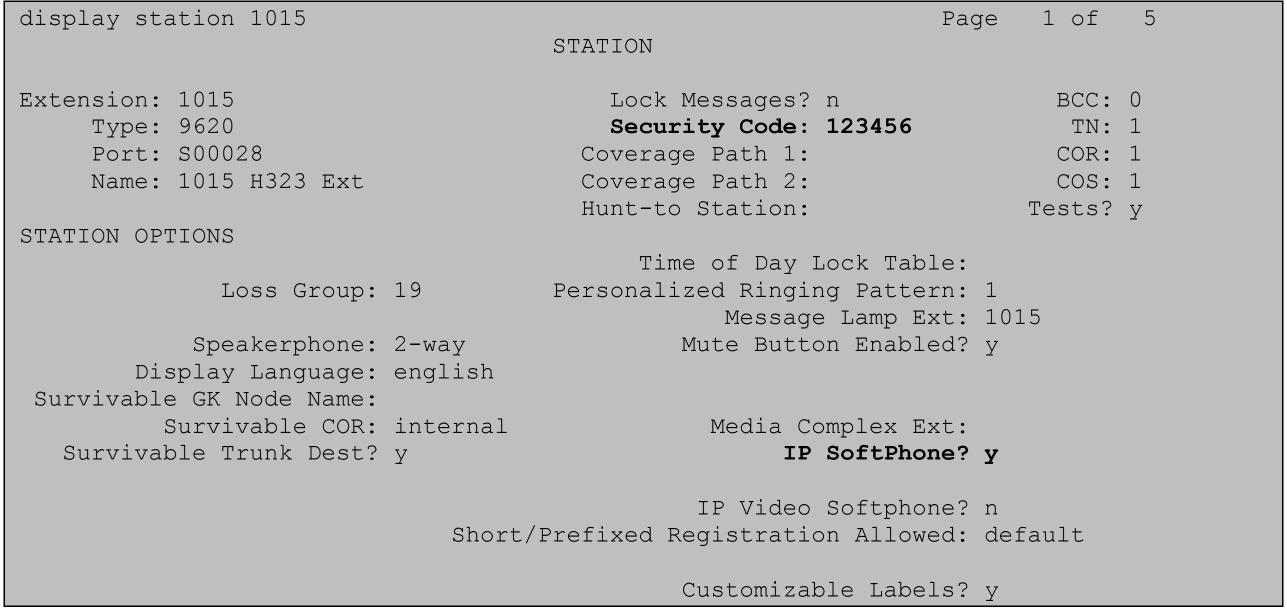
- **Can Be Service Observed?** Enter **y**
- **Can Be A Service Observer?** Enter **y**

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

               COR Number: 1
          COR Description: COR1

                      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? y
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: none       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.? n
         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)? n
                        Can Be Picked Up By Directed Call Pickup? n
                                    Can Use Directed Call Pickup? n
                                    Group Controlled Restriction: inactive
```

5.4. Configure Target Stations to be Recorded

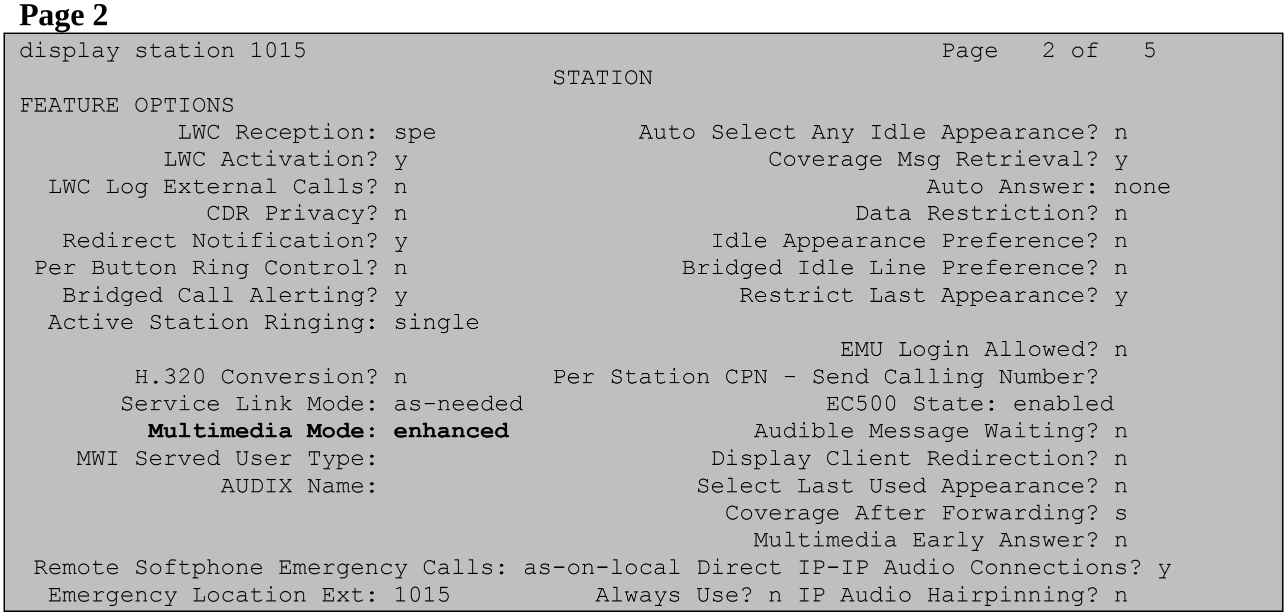
Each Station to be monitored must have **IP Softphone** set to **y** on **page 1** and **Multimedia Mode** set to **enhanced** on **page 2**. The example below shows the configuration of an IP station 1015 (note, TDM stations are configured in the same way). Note the **Security Code** as this will be required by Smart Logger II system in **Section 7.1.2**

Page 1



```
display station 1015                                            Page   1 of   5
                                     STATION

Extension: 1015                          Lock Messages? n               BCC: 0
     Type: 9620                          Security Code: 123456           TN: 1
     Port: S00028                      Coverage Path 1:                 COR: 1
     Name: 1015 H323 Ext               Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 1015
            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
                              Short/Prefixed Registration Allowed: default

                                              Customizable Labels? y
```

Page 2



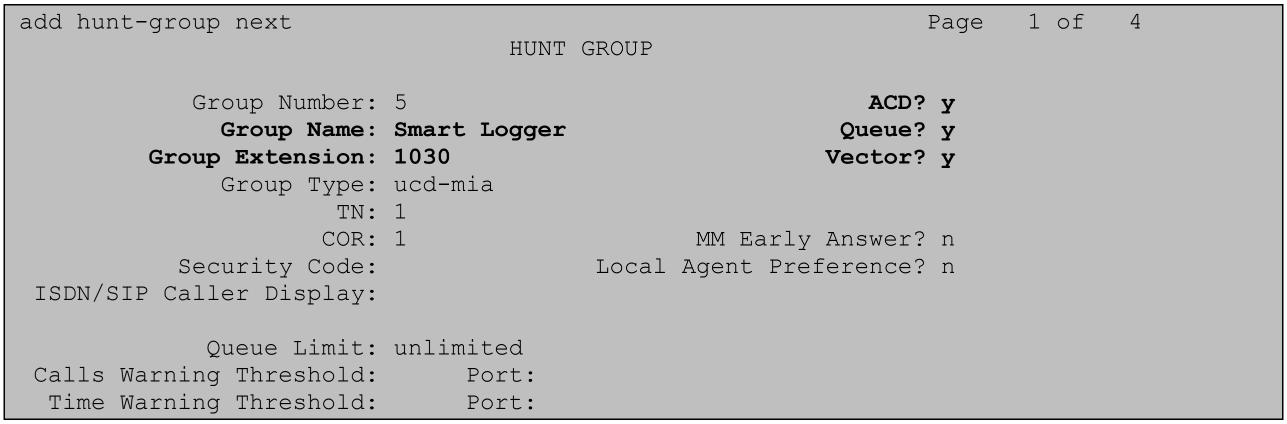
```
display station 1015                                            Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe             Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  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? y                      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: 1015          Always Use? n IP Audio Hairpinning? n
```

5.5. 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 **add hunt-group next** command and enter the following:

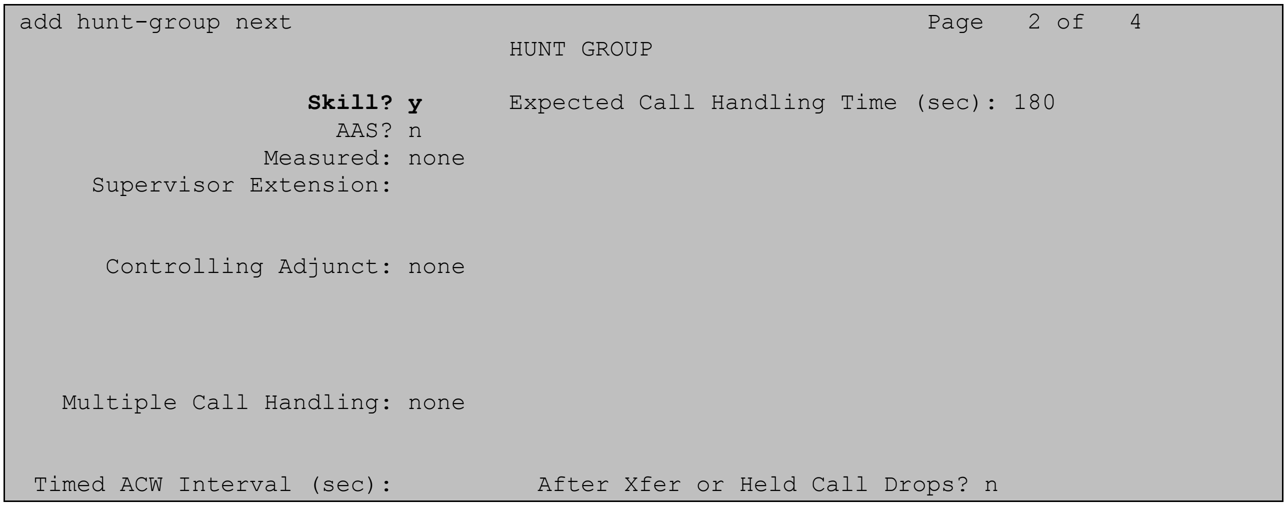
- **Group Name** Enter a group name for identification purposes (**Smart Logger**)
- **Group Extension** Enter an extension number that is valid in the dialplan (**1030**)
- **ACD?** Enter **y**
- **Queue?** Enter **y**
- **Vector?** Enter **y**

Note the **Group Number**. As it is required in **Section 5.6**.



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

            Group Number: 5                                ACD? y
              Group Name: Smart Logger                   Queue? y
         Group Extension: 1030                          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:
```

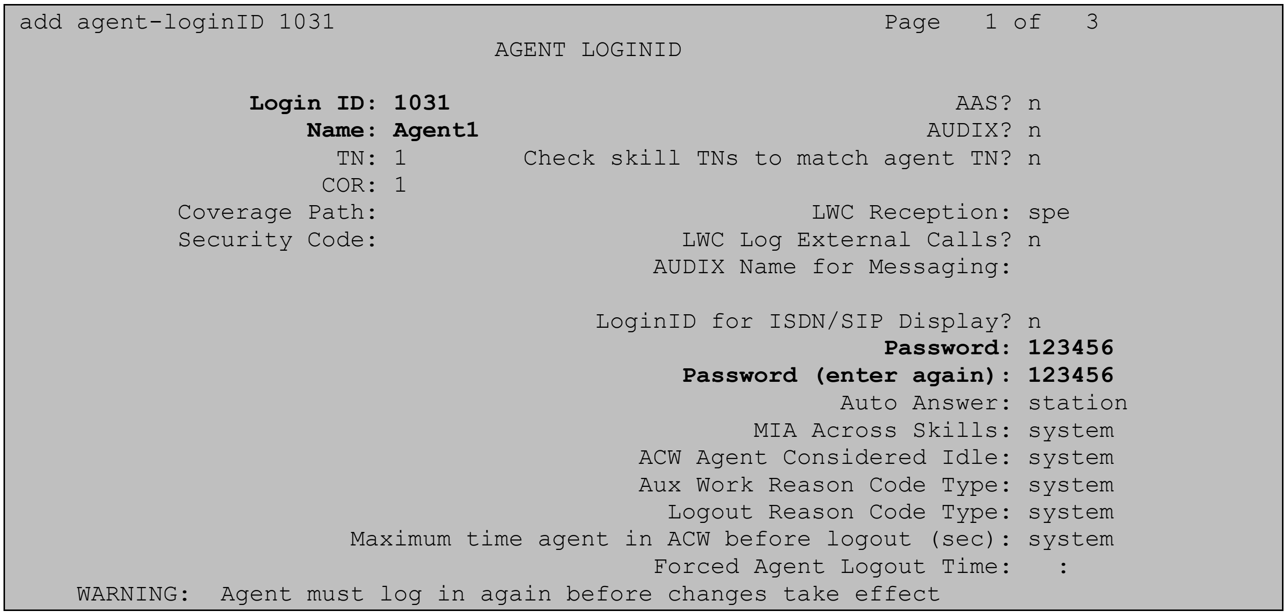
Navigate to **Page 2,** set **Skill** to **y.**



```
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




   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```

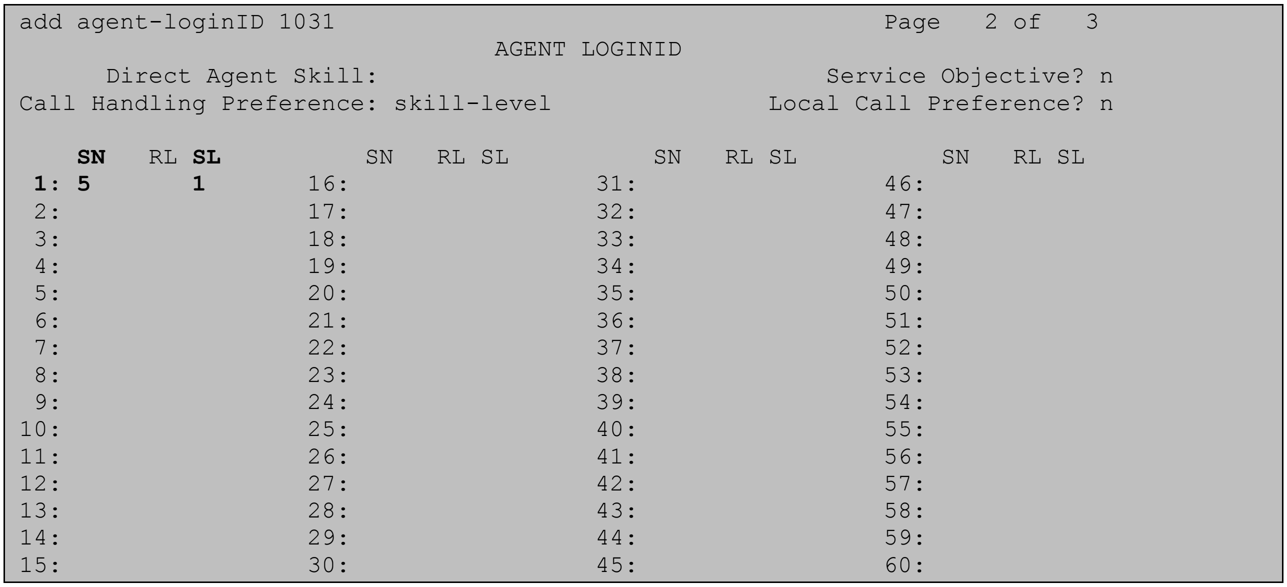
5.6. Configure Agents

Each Agent requires a **Login ID**, **Name** and **Password**. Shown below is the configuration of Agent1.



```
add agent-loginID 1031                                      Page   1 of   3
                                 AGENT LOGINID

                Login ID: 1031                                   AAS? n
                    Name: Agent1                               AUDIX? n
                      TN: 1        Check skill TNs to match agent TN? n
                     COR: 1
           Coverage Path:                              LWC Reception: spe
           Security Code:                     LWC Log External Calls? n
                                            AUDIX Name for Messaging:

                                        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 **5** for the Skill Number (**SN**), and the appropriate Skill Level (**SL)** (i.e. **1**) During compliance testing the Skill Number (Hunt Group) number was 5, as configured in **Section 5.5**.

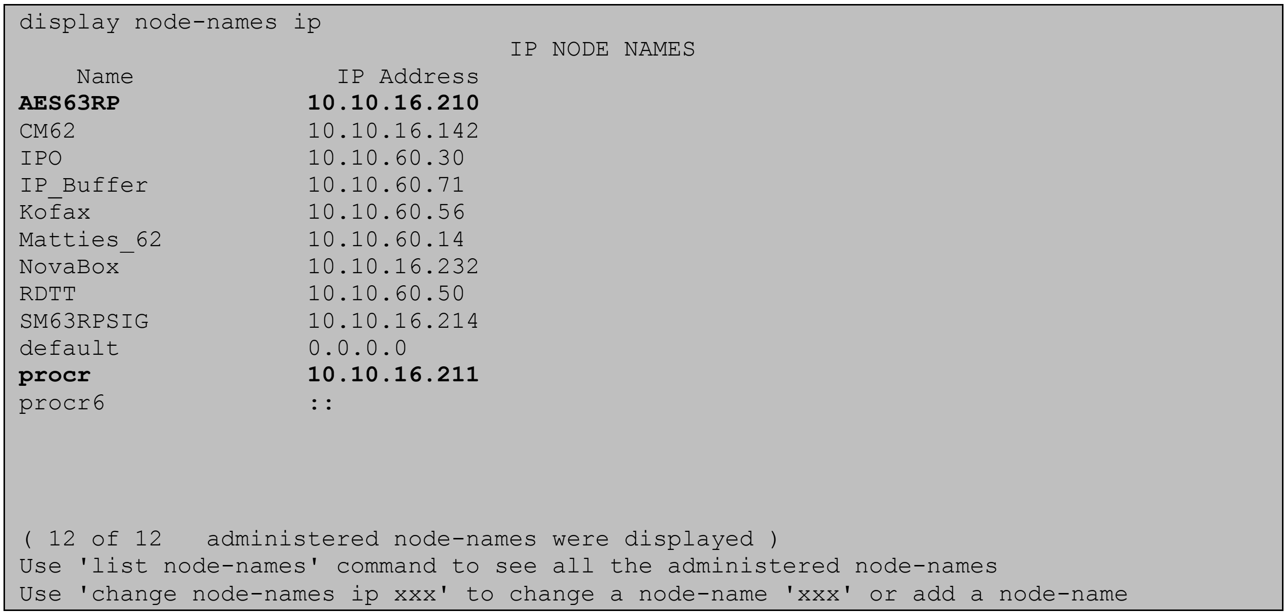


```
add agent-loginID 1031                                      Page   2 of   3
                                 AGENT LOGINID
      Direct Agent Skill:                               Service Objective? n
Call Handling Preference: skill-level               Local Call Preference? n

    SN   RL SL          SN   RL SL          SN   RL SL          SN   RL SL
 1: 5       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:
```

5.7. Create Node Name for Avaya Aura® Application Enablement Services

A Node Name needs to be created to associate Communication Manager with AES. Use the **change node-names ip** command and enter an informative name (**AES63RP**) and the IP address of the **AES** (**10.10.16.210**).

Note the **procr** IP address as it is required in **Section 7.1.1**.



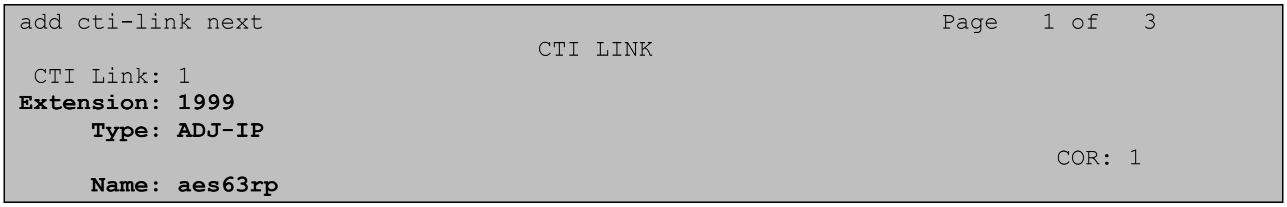
```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
AES63RP             10.10.16.210
CM62                10.10.16.142
IPO                 10.10.60.30
IP_Buffer           10.10.60.71
Kofax               10.10.60.56
Matties_62          10.10.60.14
NovaBox             10.10.16.232
RDTT                10.10.60.50
SM63RPSIG           10.10.16.214
default             0.0.0.0
procr               10.10.16.211
procr6              ::




( 12 of 12   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.8. Create CTI Link to the Aura® Application Enablement Services

A CTI Link needs to be created to enable Communication Manager to interoperate with AES. Use the **add cti-link next** command and enter the following:

- **Extension** Enter any unused **Extension** (**1999**)
- **Type** Enter **ADJ-IP**
- **Name** Enter the AES node name (**AES63RP** as created in **Section 5.7**)

Note: during compliance testing cti link 1 was added.



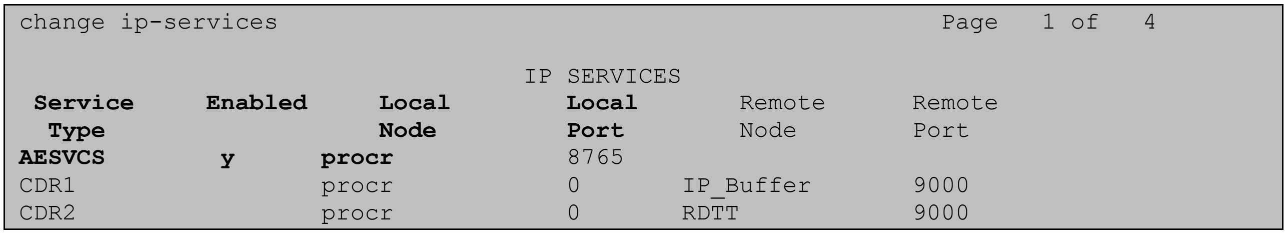
```
add cti-link next                                              Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 1999
     Type: ADJ-IP
                                                                       COR: 1
     Name: aes63rp
```

5.9. Configure IP Services

To configure the AES link use the **change ip-services** command and enter the following:

On Page 1

- **Service Type** Enter **AESVCS**
- **Enabled** Enter **y**
- **Local Node** Enter **procr**
- **Local Port** Enter **8765**

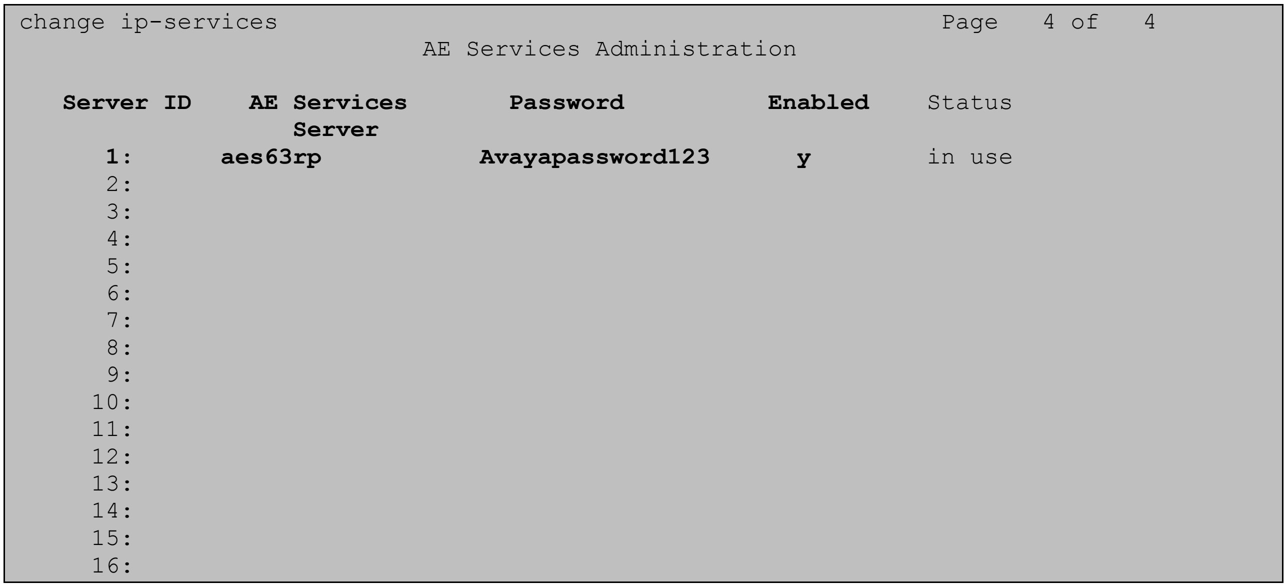


```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y      procr            8765
CDR1                 procr            0       IP_Buffer       9000
CDR2                 procr            0       RDTT            9000
```

Navigate to **Page 4** and enter the following:

- **Server ID** Enter **1**
- **AE Services Server** Enter **AES63RP** (The node created in **section 5.7**)
- **Password** Enter a password. This password will be used in **Section 6.3** to enable AES to communicate with Communication Manager.
- **Enabled** Enter **y**

Press **f3** button to save the new settings.



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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      aes63rp           Avayapassword123      y        in use
      2:
      3:
      4:
      5:
      6:
      7:
      8:
      9:
     10:
     11:
     12:
     13:
     14:
     15:
     16:
```

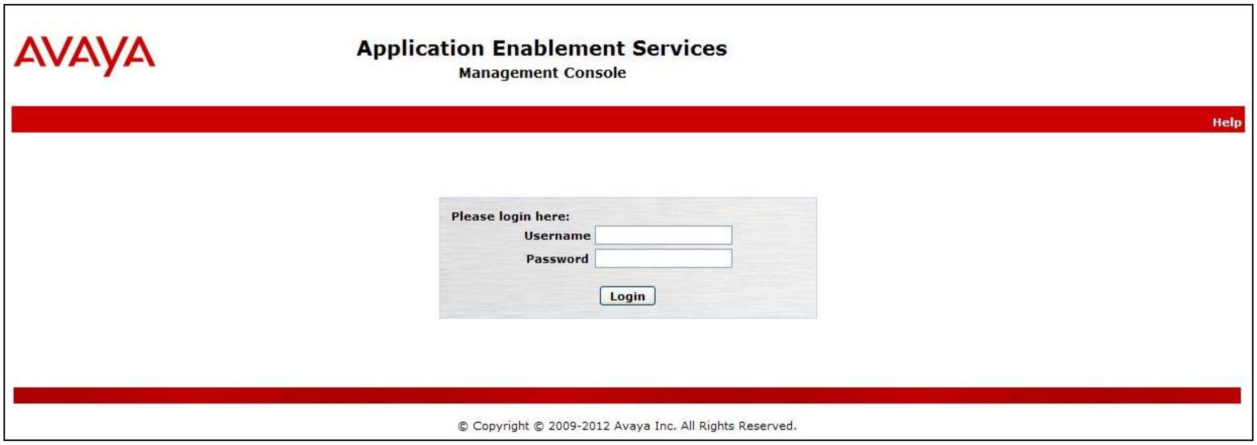
6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring AES. It is implied a working AES is already in place and the Security Database (SDB) is configured. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Logging into Avaya Aura® Application Enablement Services
- Verify Avaya Aura® Application Enablement Services License
- Create Avaya Aura® Communication Manager Switch Connection
- Create CTI User
- Enable CTI User
- Configure DMCC Port
- Restart DMCC Service

6.1. Logging into Avaya Aura® Application Enablement Services

To access the OAM web-based interface of the AES Server use the URL **http://x.x.x.x**, where **x. x. x. x** is the IP address of the AES Server. The **Management console** is displayed. Log in using the appropriate credentials.

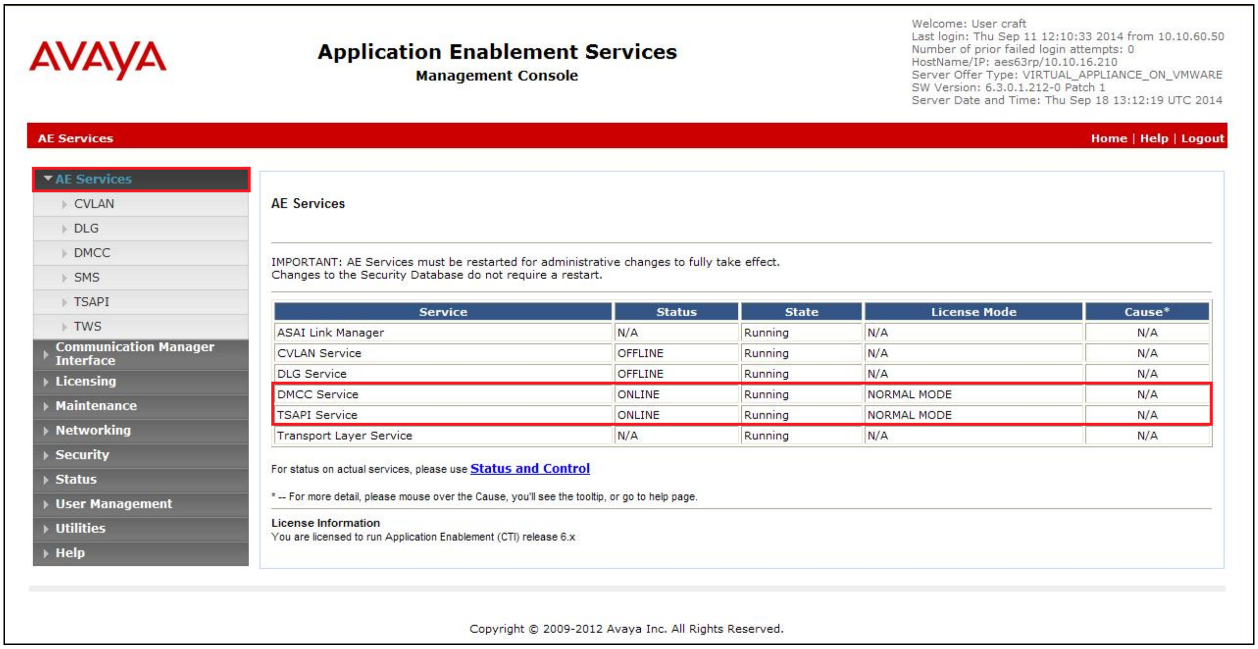

Application Enablement Services
Management Console

Please login here:
Username
Password

© Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

6.2. Verify Avaya Aura® Application Enablement Services License

Select **AE Services** on the left pane and verify that the **DMCC** and **TSAPI Services** are licensed by ensuring that **DMCC Service** and **TSAPI Service** are in the list of services and that the **License Mode** is showing **NORMAL MODE** for both services. If this is not the case, please contact an Avaya representative regarding licensing.


Application Enablement Services
Management Console

Welcome: User craft
Last login: Thu Sep 11 12:10:33 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Thu Sep 18 13:12:19 UTC 2014

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.

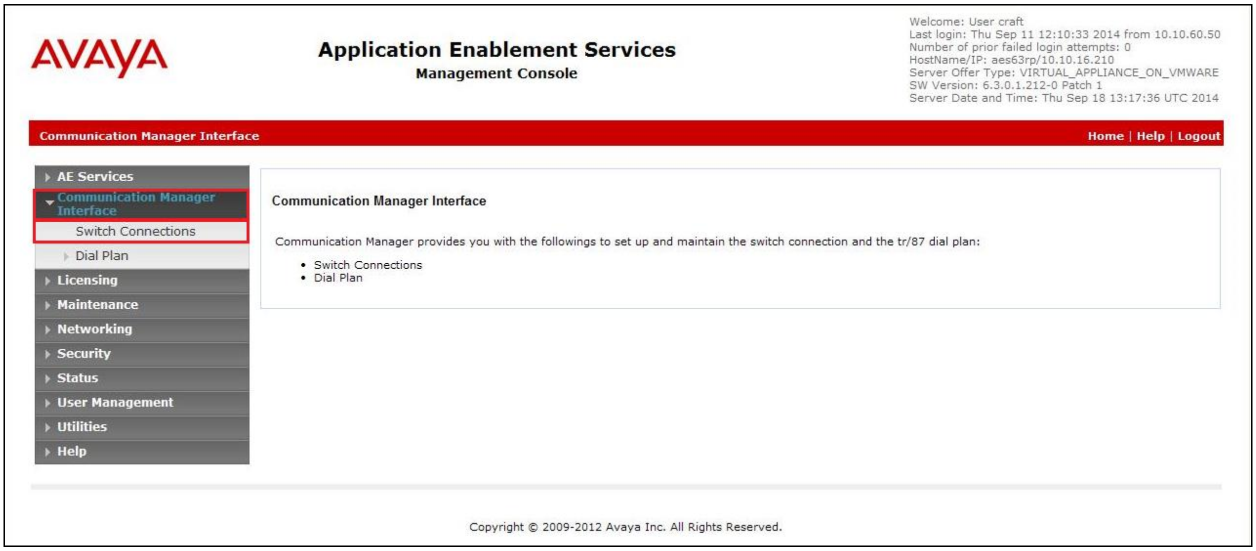
License Information
You are licensed to run Application Enablement (CTI) release 6.x

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

6.3. Create Avaya Aura® Communication Manager Switch Connection

A Communication Manager Switch Connection needs to be created to enable AES to communicate with Communication Manager. Navigate to **Communication Manager Interface**

→ **Switch Connections**.



Welcome: User craft
Last login: Thu Sep 11 12:10:33 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Thu Sep 18 13:17:36 UTC 2014

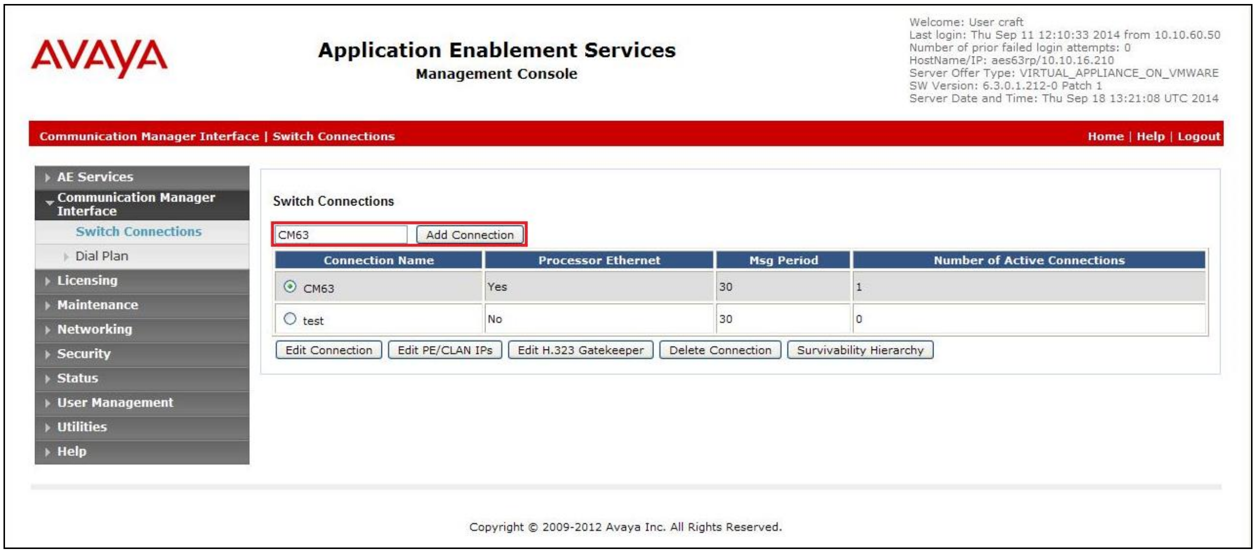
Communication Manager Interface

Communication Manager provides you with the followings to set up and maintain the switch connection and the tr/87 dial plan:

- Switch Connections
- Dial Plan

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

When the **Switch Connections** page opens, enter an informative name for Communication Manager (**CM63**). Click on the **Add Connection** button.



Welcome: User craft
Last login: Thu Sep 11 12:10:33 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Thu Sep 18 13:21:08 UTC 2014

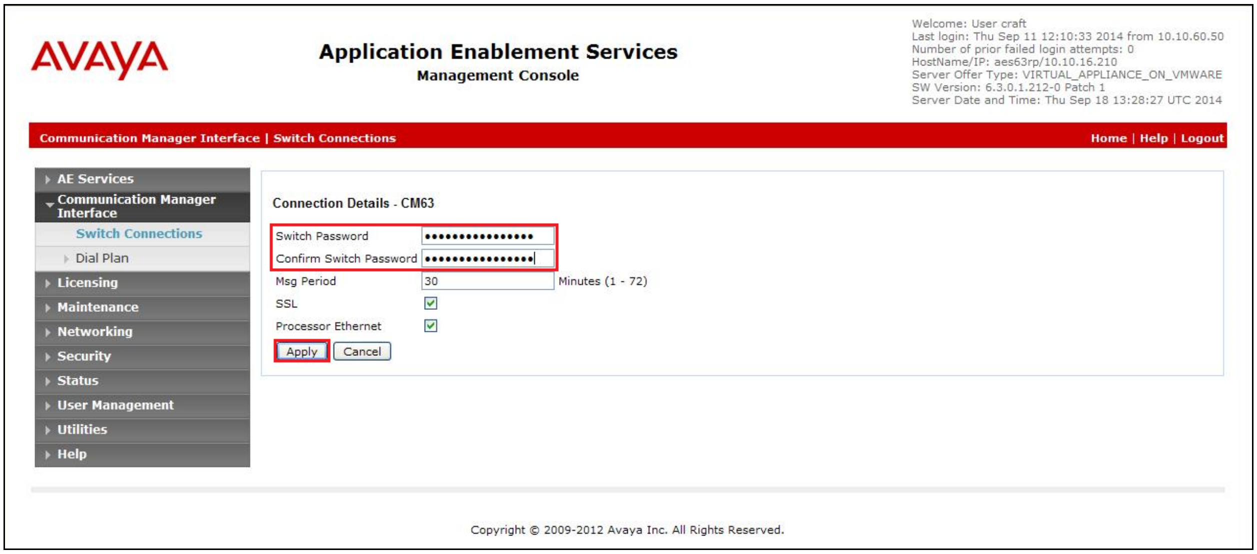
Switch Connections

CM63

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● CM63	Yes	30	1
○ test	No	30	0

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

Once the **Connection Details** window opens enter the **Switch Password** as was configured in **Section 5.9** then **Confirm Switch Password**. Click on the **Apply** button.



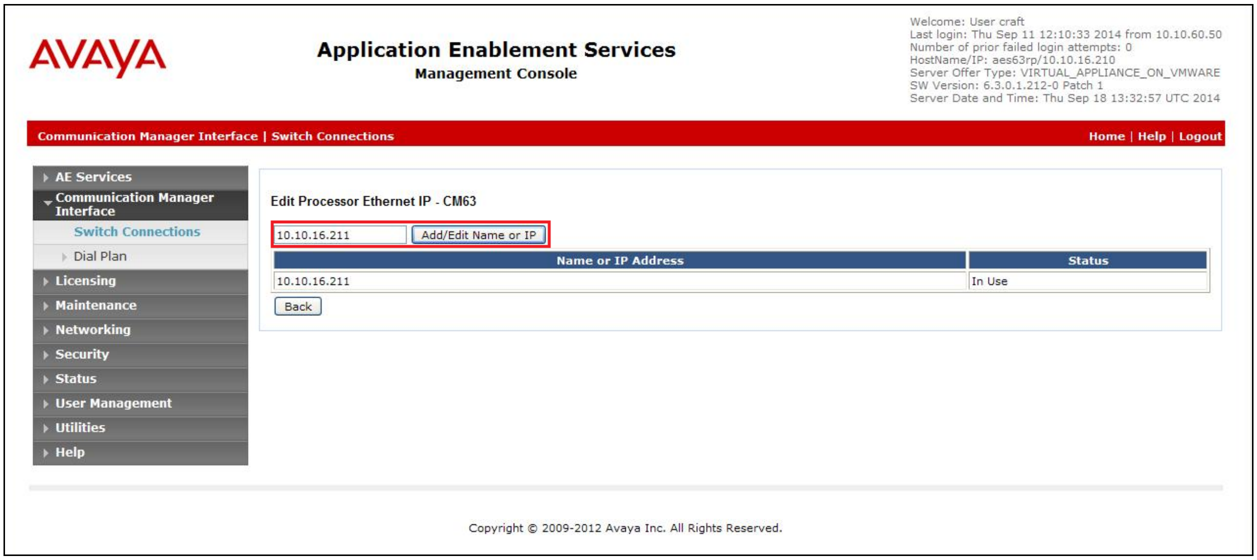
Welcome: User craft
Last login: Thu Sep 11 12:10:33 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Thu Sep 18 13:28:27 UTC 2014

Connection Details - CM63

Switch Password	••••••••••••••••
Confirm Switch Password	••••••••••••••••
Msg Period	30 Minutes (1 - 72)
SSL	☑
Processor Ethernet	☑

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

Click the **Edit PE/CLAN IPs** button (see screen at the bottome of page 17). Enter the IP address of the Processor Ethernet interface (procr IP address, see **Section 5.7**) that AES will use for communication with Communication Manager, and click the **Add/Edit Name or IP** button.



Welcome: User craft
Last login: Thu Sep 11 12:10:33 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Thu Sep 18 13:32:57 UTC 2014

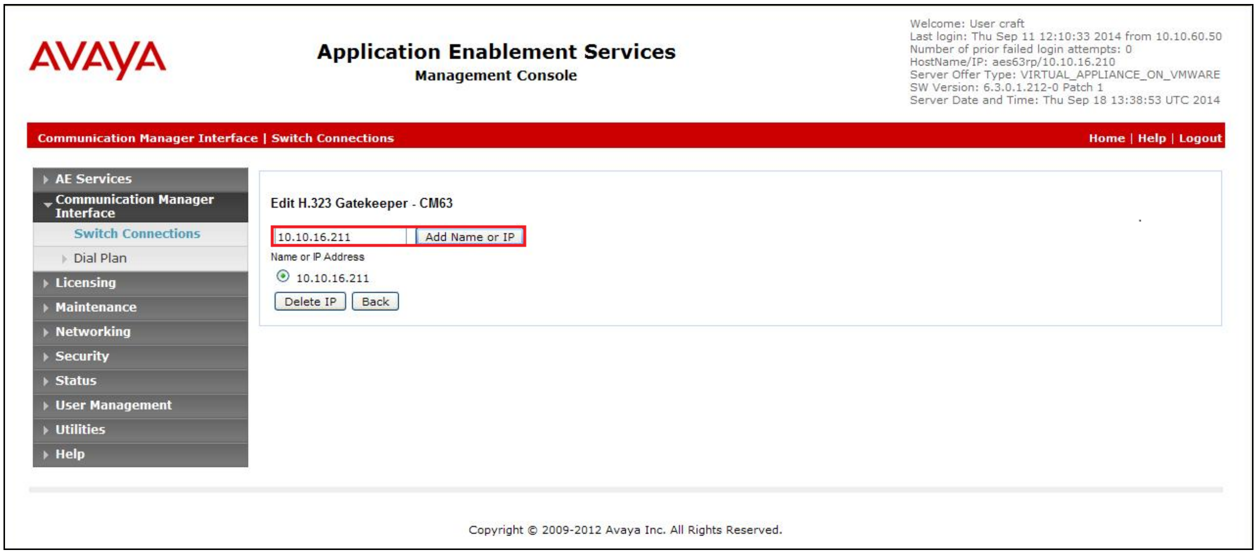
Edit Processor Ethernet IP - CM63

10.10.16.211

Name or IP Address	Status
10.10.16.211	In Use

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

Click the **Edit H.323 Gatekeeper** button, (not shown). Enter the IP address of the Processor Ethernet interface (procr. IP address, see **Section 5.7**). Click the **Add Name or IP** button.



Welcome: User craft
Last login: Thu Sep 11 12:10:33 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Thu Sep 18 13:38:53 UTC 2014

Edit H.323 Gatekeeper - CM63

10.10.16.211

Name or IP Address
● 10.10.16.211

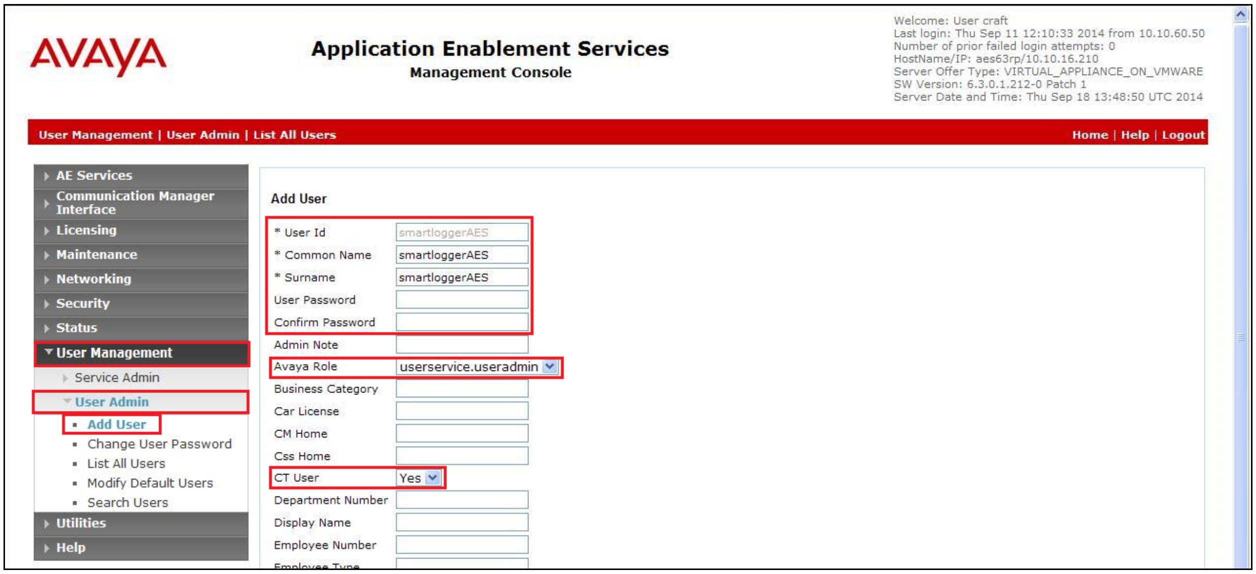
Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

6.4. Create CTI User

A user ID and password needs to be configured for Smart Logger II to communicate as a DMCC Client with AES. Navigate to **User Manager → User Admin**, and select **Add User**. On the **Add User** screen enter the following:

- **User Id**: Enter an informative name (**smartloggerAES**). This ID is required for the Smart logger II configuration in **Section 7.1**
- **Common Name**: Enter a Common Name (**smartloggerAES**)
- **Surname**: Enter a Surname (**smartloggerAES**)
- **User Password** Enter a password. This password is required for the Smart Logger II configuration in **Section 7.1**
- **Confirm Password** Confirm the password
- **Avaya Role** Select **userservice.useradmin** from the dropdown box
- **CT User** Select **Yes** from the dropdown box

Click the **Apply button** at the bottom of the page (not shown)



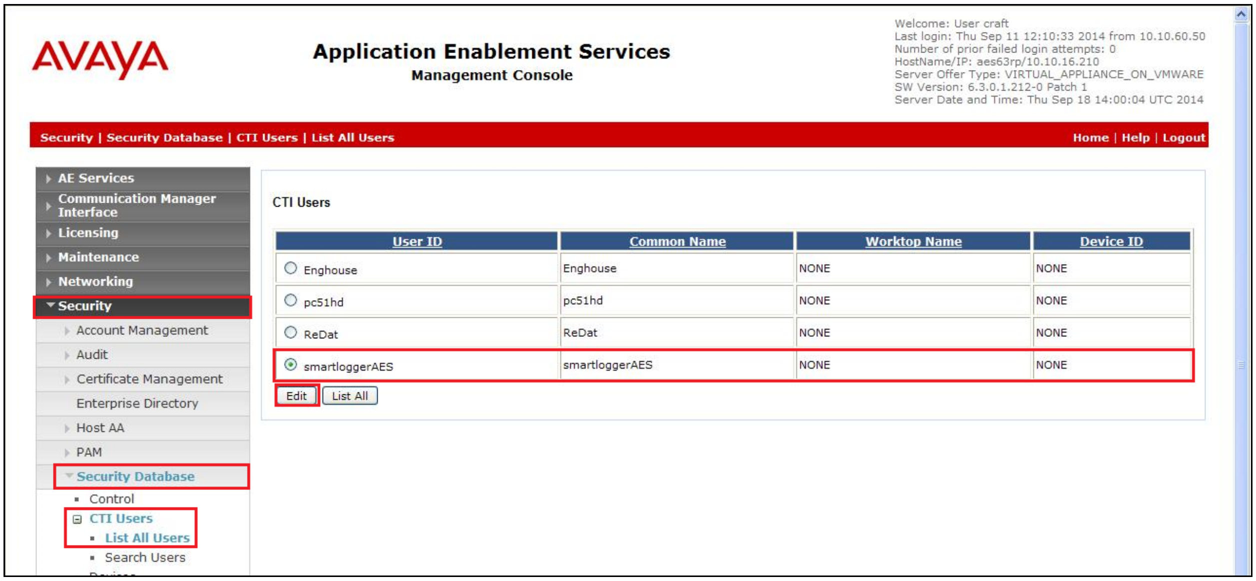
Welcome: User craft
Last login: Thu Sep 11 12:10:33 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Thu Sep 18 13:48:50 UTC 2014

Add User

* 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	

6.5. 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 Radio button relating to the CTI user created in **Section 6.4** (**smartloggerAES**) and click on the **Edit** button.



AVAYA

Application Enablement Services
Management Console

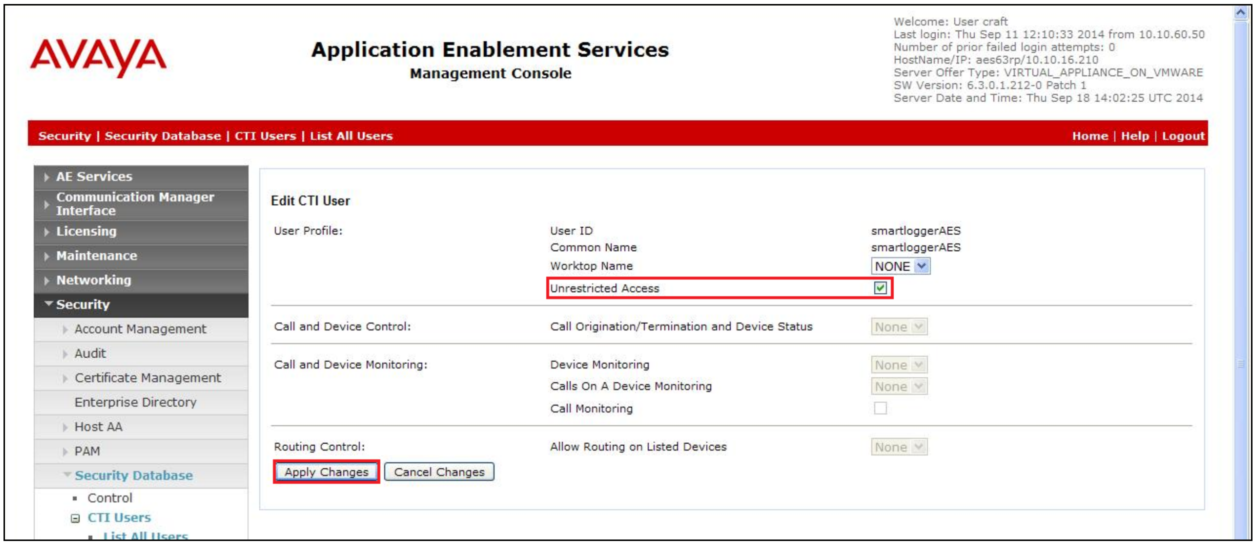
Welcome: User craft
Last login: Thu Sep 11 12:10:33 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Thu Sep 18 14:00:04 UTC 2014

Security | Security Database | CTI Users | List All Users — Home | Help | Logout

CTI Users

User ID	Common Name	Worktop Name	Device ID
○ Enghouse	Enghouse	NONE	NONE
○ pc51hd	pc51hd	NONE	NONE
○ ReDat	ReDat	NONE	NONE
● smartloggerAES	smartloggerAES	NONE	NONE

Once the **Edit CTI User** page appears, tick the **Unrestricted Access** check box and click the **Apply Changes button** at the bottom of the screen



AVAYA

Application Enablement Services
Management Console

Welcome: User craft
Last login: Thu Sep 11 12:10:33 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Thu Sep 18 14:02:25 UTC 2014

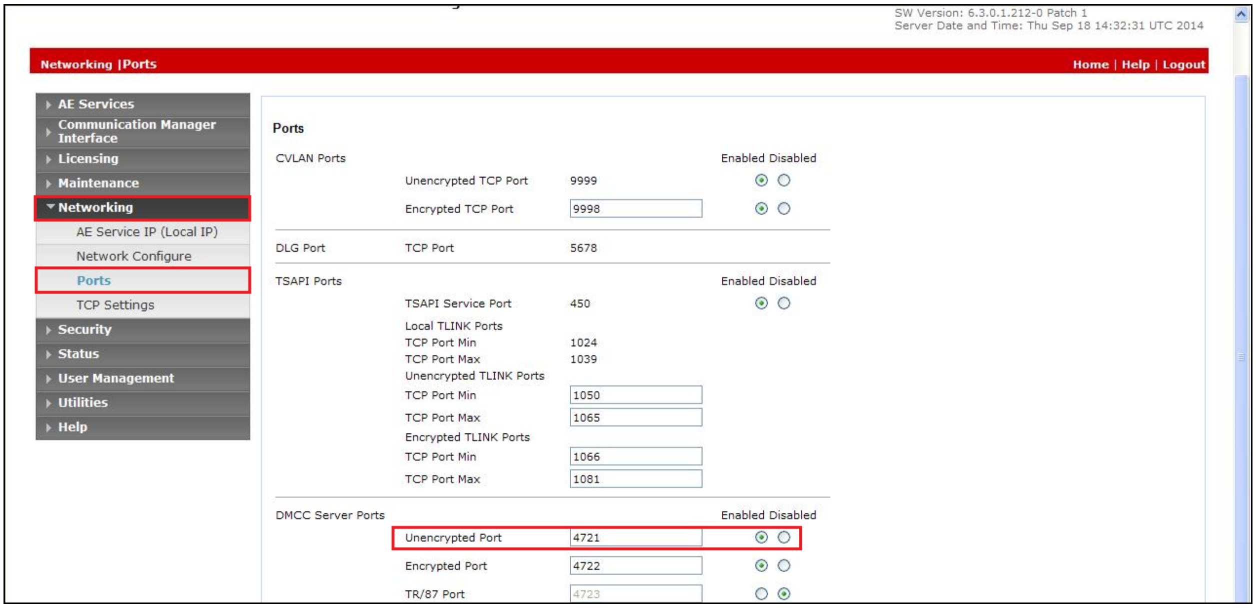
Security | Security Database | CTI Users | List All Users — Home | Help | Logout

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

6.6. Configure DMCC Port

Navigate to **Networking → Ports**. In the **DMCC Server Ports** area, enter **4721** in the **Unencrypted Port** box and click on the **Enabled** radio button. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.



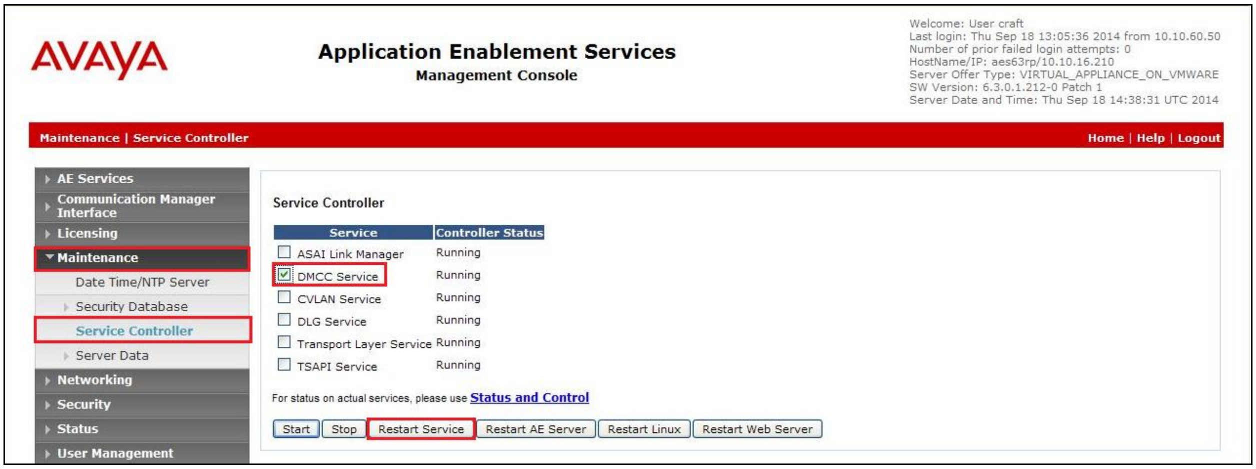
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Thu Sep 18 14:32:31 UTC 2014

Ports

			Enabled	Disabled
CVLAN Ports			Enabled	Disabled
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	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			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	○	●

6.7. Restart DMCC Service

After the AES configuration is completed the DMCC service needs to be restarted. To restart navigate to **Maintenance → Service Controller**. Tick the **DMCC Service** check box and click on the **Restart Service** button.



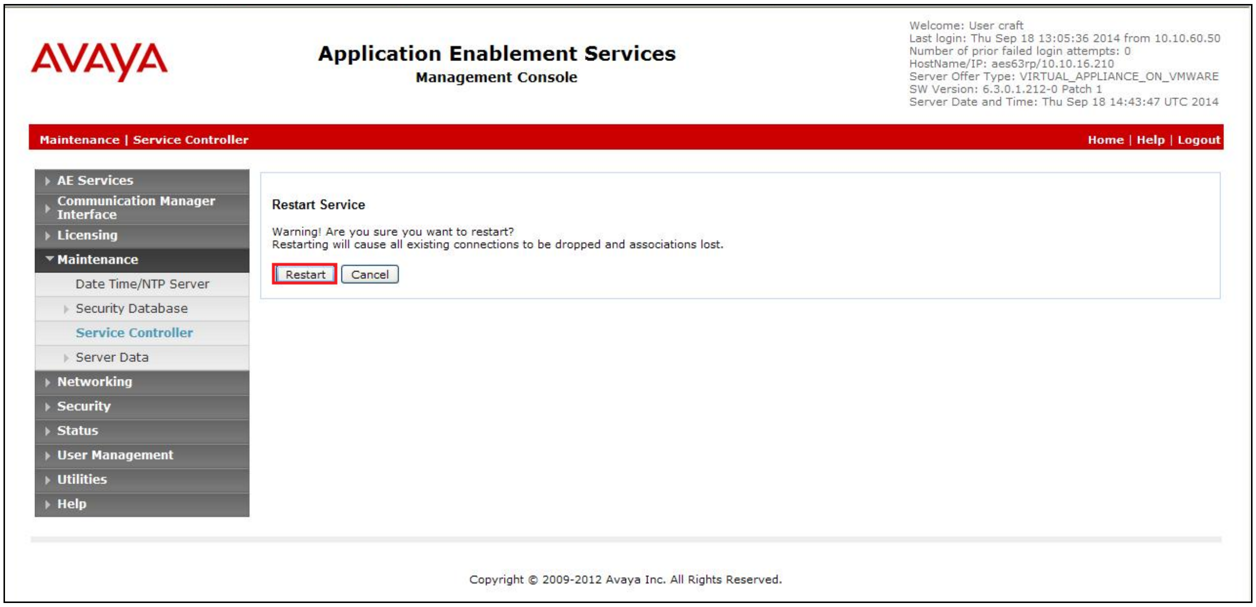
Welcome: User craft
Last login: Thu Sep 18 13:05:36 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Thu Sep 18 14:38:31 UTC 2014

Service Controller

Service	Controller Status
□ ASAI Link Manager	Running
☑ DMCC 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

When the Restart page opens click on the **Restart button**.



Welcome: User craft
Last login: Thu Sep 18 13:05:36 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Thu Sep 18 14:43:47 UTC 2014

Restart Service

Warning! Are you sure you want to restart?
Restarting will cause all existing connections to be dropped and associations lost.

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

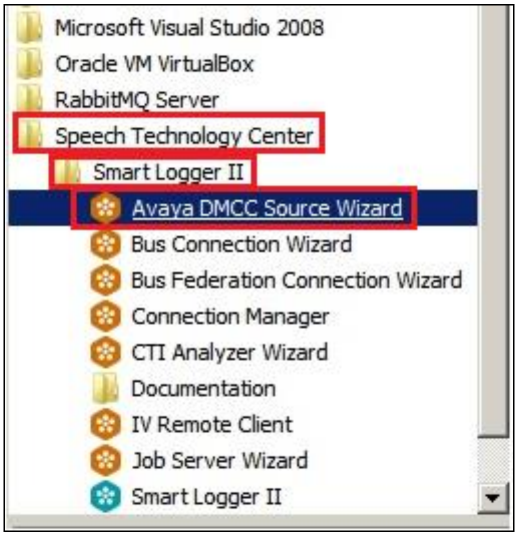
7. Configure Speech Technology Centre Smart Logger II

The Smart Logger II application is provided and installed by Speech Technology Centre. Smart Logger II runs on Windows 2008 Server. The configuration of this is outside of the scope of these Application Notes. It is implied that all Speech Technology Centre and prerequisite software is installed including any appropriate licences.

Full installation of each component is performed by Speech Technology Centre, only the elements relevant to the configuration for the compliance test are detailed here.

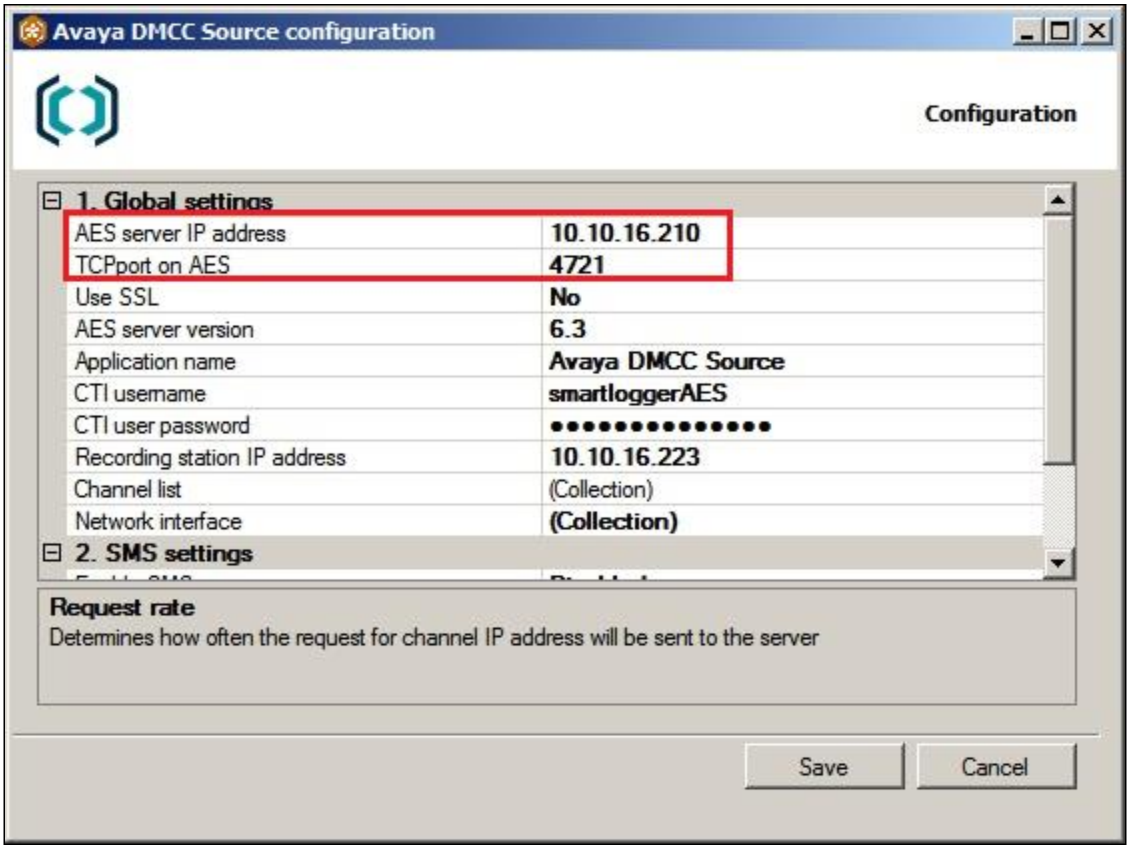
7.1. Avaya DMCC Source Wizard

In order for Smart Logger II to interoperate with AES and Communication Manager, the relevant settings must be configured. On the PC hosting Smart Logger II, click **Start → All Program** (not shown) then navigate to **Speech Technology Centre → Smart Logger II → Avaya DMCC Source Wizard**.



When the **Avaya DMCC Source Configuration** window opens, in the **Global settings** section configure the following:

- **AES Server IP address** Enter the IP address of the AES (**10.10.16.210**)
- **TCPport on AES** Enter the TCP port configured in **Section6.6** (**4721**)



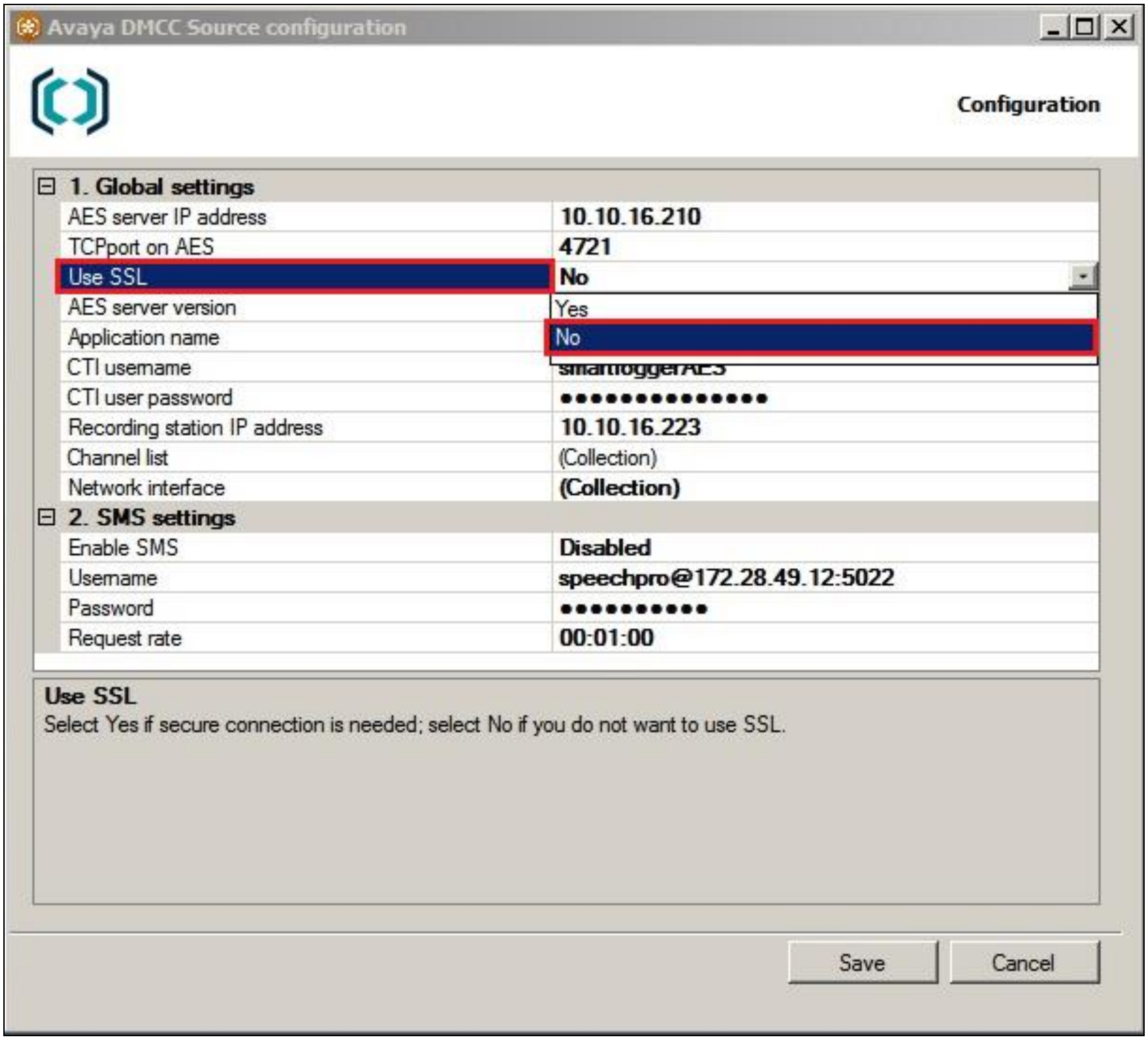
1. Global settings

AES server IP address	10.10.16.210
TCPport on AES	4721
Use SSL	No
AES server version	6.3
Application name	Avaya DMCC Source
CTI username	smartloggerAES
CTI user password	●●●●●●●●●●●●●●●
Recording station IP address	10.10.16.223
Channel list	(Collection)
Network interface	(Collection)

2. SMS settings

Request rate
Determines how often the request for channel IP address will be sent to the server

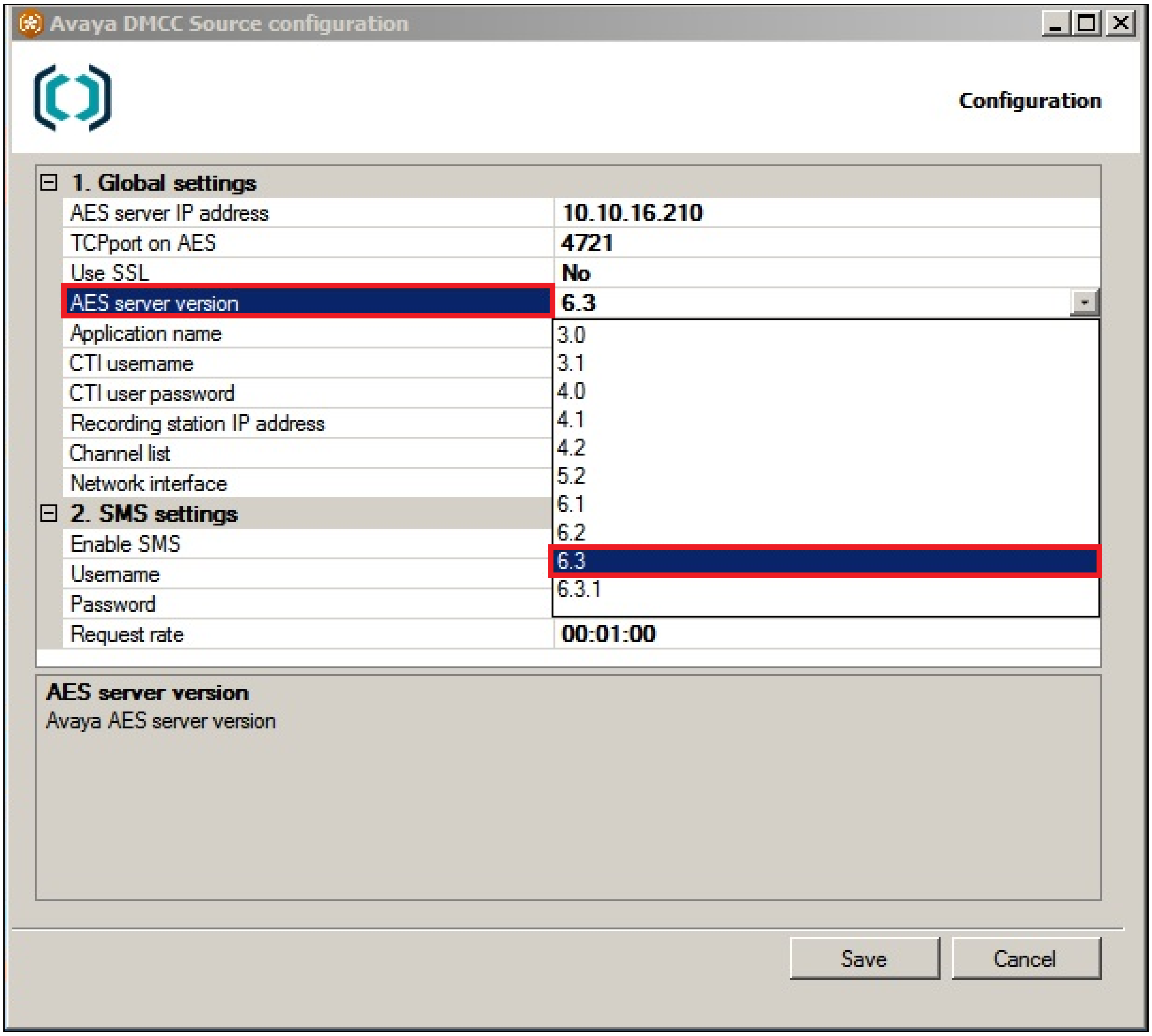
Click on the **Use SSL** field, and select **No** from the dropdown box.



1. Global settings	
AES server IP address	10.10.16.210
TCPport on AES	4721
Use SSL	No
AES server version	Yes
Application name	No
CTI usemame	smartloggerAES
CTI user password	●●●●●●●●●●●●●●
Recording station IP address	10.10.16.223
Channel list	(Collection)
Network interface	(Collection)
2. SMS settings	
Enable SMS	Disabled
Usemame	speechpro@172.28.49.12:5022
Password	●●●●●●●●●●
Request rate	00:01:00

Use SSL
Select Yes if secure connection is needed; select No if you do not want to use SSL.

Click on the **AES server version** field, and select **6.3** from the dropdown box.

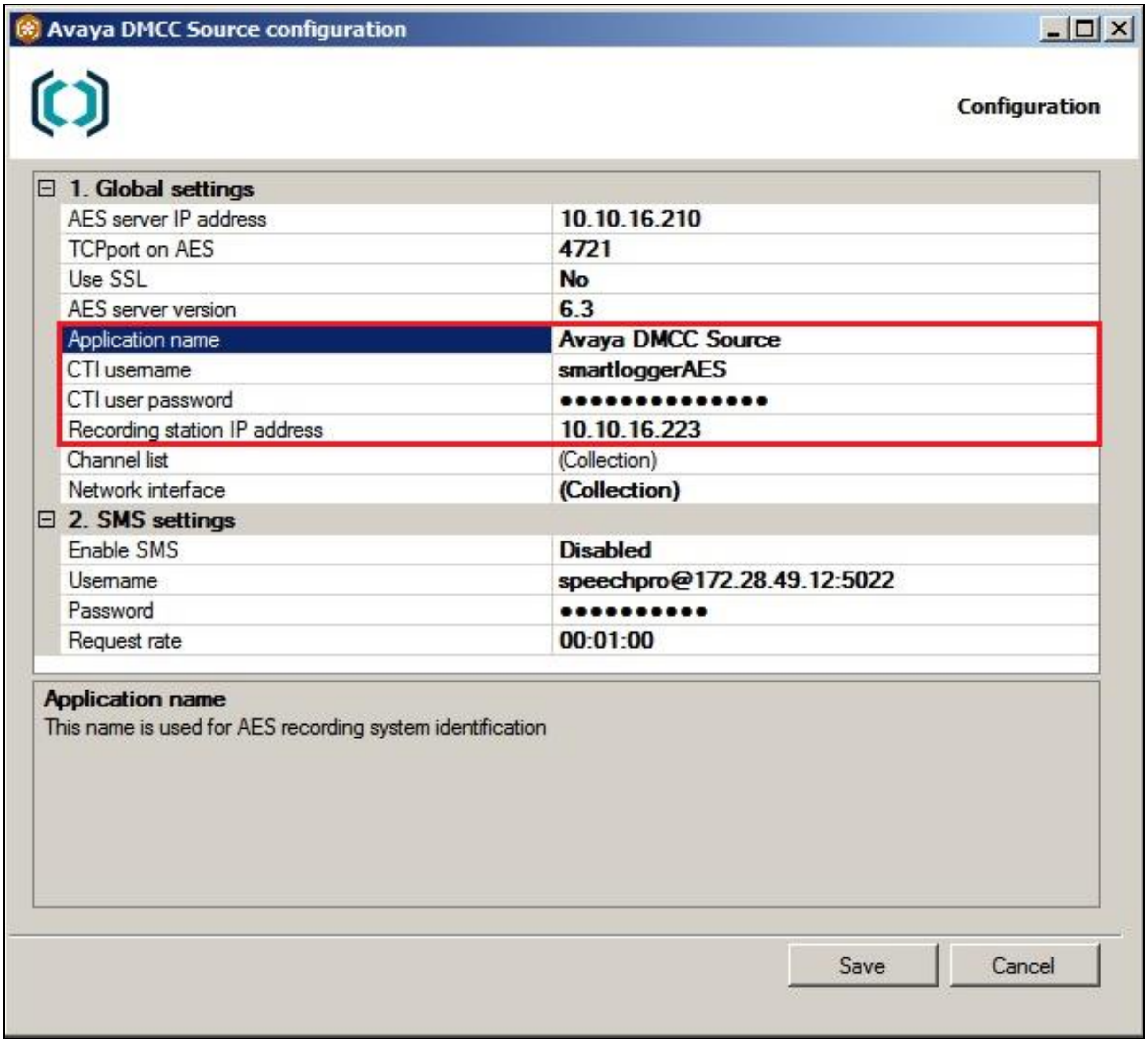


1. Global settings	
AES server IP address	10.10.16.210
TCPport on AES	4721
Use SSL	No
AES server version	6.3
Application name	
CTI username	
CTI user password	
Recording station IP address	
Channel list	
Network interface	
2. SMS settings	
Enable SMS	
Username	
Password	
Request rate	00:01:00

AES server version
Avaya AES server version

In the next fields enter the following:

- **Application name** Enter **Avaya DMCC Source**
- **CTI username** Enter the CTI username as configured in **Section6.4** (**smartloggerAES**)
- **CTI user password** Enter the CTI user password as configured in **Section6.4**
- **Recording station IP address** Enter the IP address of the server hosting Smart Logger II

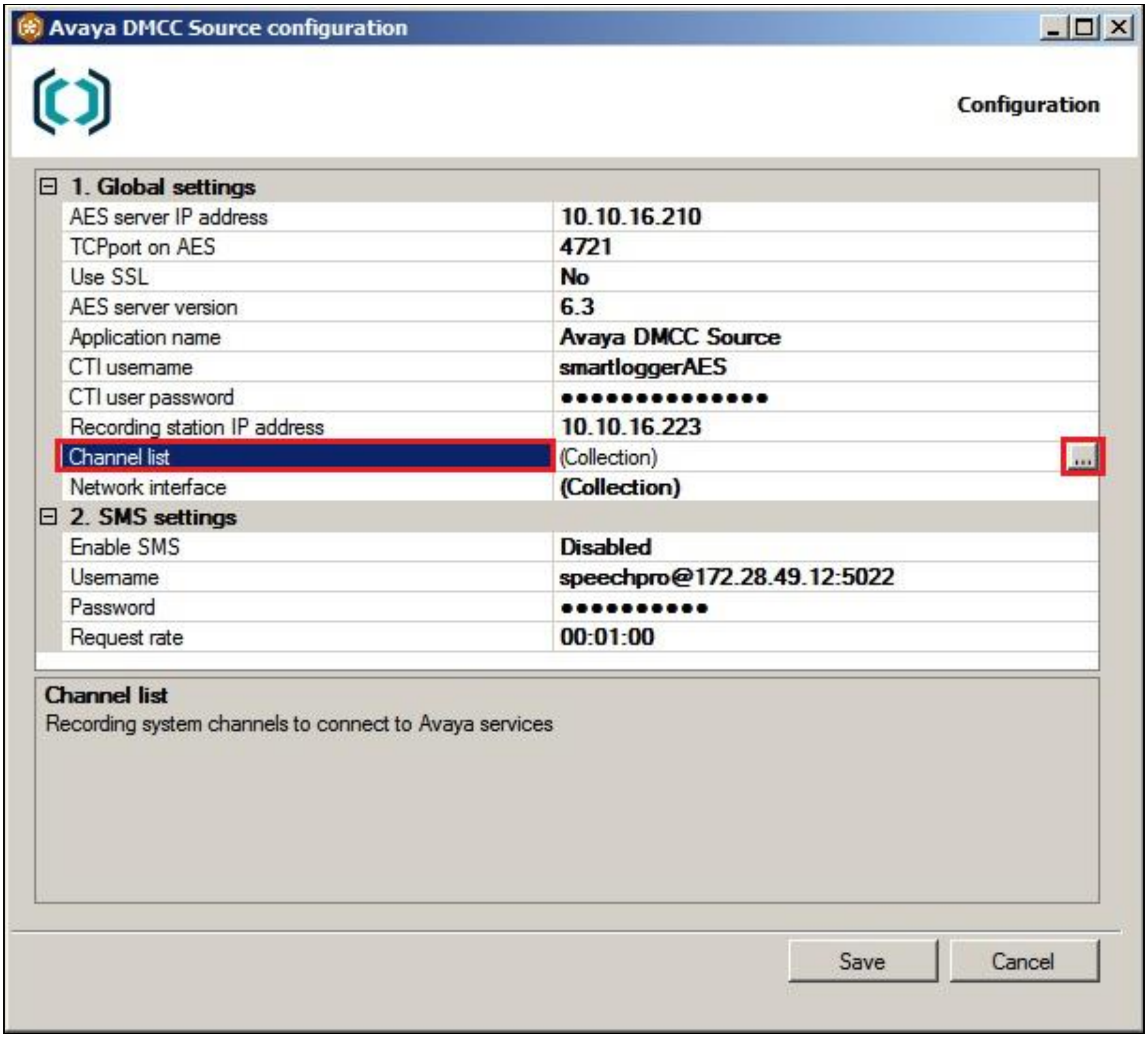


⊟ 1. Global settings	
AES server IP address	10.10.16.210
TCPport on AES	4721
Use SSL	No
AES server version	6.3
Application name	Avaya DMCC Source
CTI username	smartloggerAES
CTI user password	●●●●●●●●●●●●●●●
Recording station IP address	10.10.16.223
Channel list	(Collection)
Network interface	(Collection)
⊟ 2. SMS settings	
Enable SMS	Disabled
Username	speechpro@172.28.49.12:5022
Password	●●●●●●●●●●
Request rate	00:01:00

Application name
This name is used for AES recording system identification

7.1.1. Channel List

Click on the **Channel list** field, and then click on the new button as highlighted below.

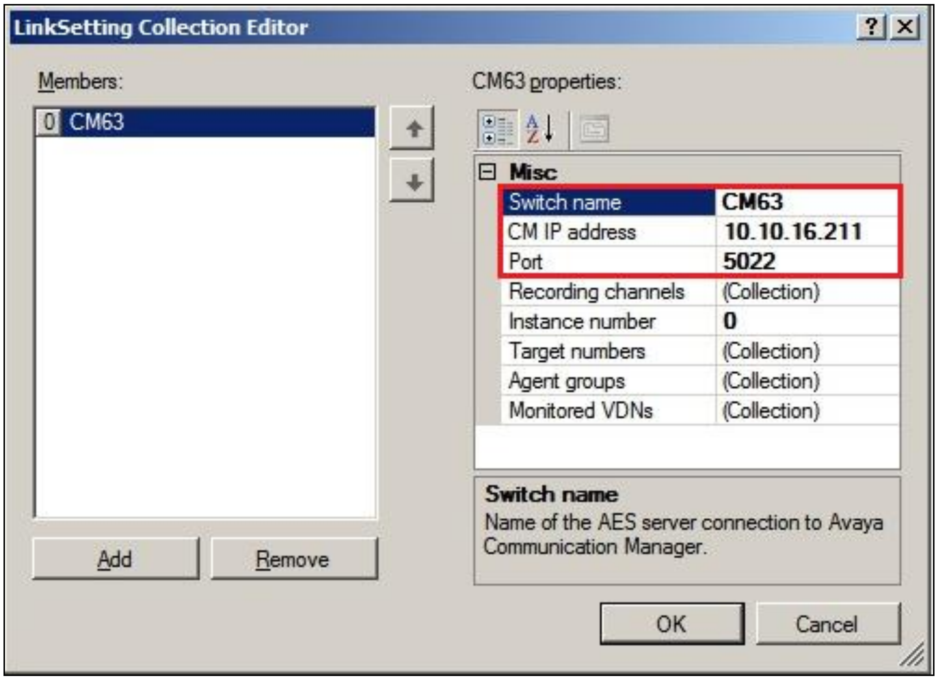


1. Global settings	
AES server IP address	10.10.16.210
TCPport on AES	4721
Use SSL	No
AES server version	6.3
Application name	Avaya DMCC Source
CTI username	smartloggerAES
CTI user password	●●●●●●●●●●●●●●
Recording station IP address	10.10.16.223
Channel list	(Collection)
Network interface	(Collection)
2. SMS settings	
Enable SMS	Disabled
Username	speechpro@172.28.49.12:5022
Password	●●●●●●●●●●
Request rate	00:01:00

Channel list
Recording system channels to connect to Avaya services

When the **LinkSetting Collection Editor** window opens, enter the following:

- **Switch name** Enter the Communication Manager name as configured in **Section 6.3**
- **CM IP address** Enter the IP address of the **procr** as shown in **Section 5.7**
- **Port** Enter **5022**

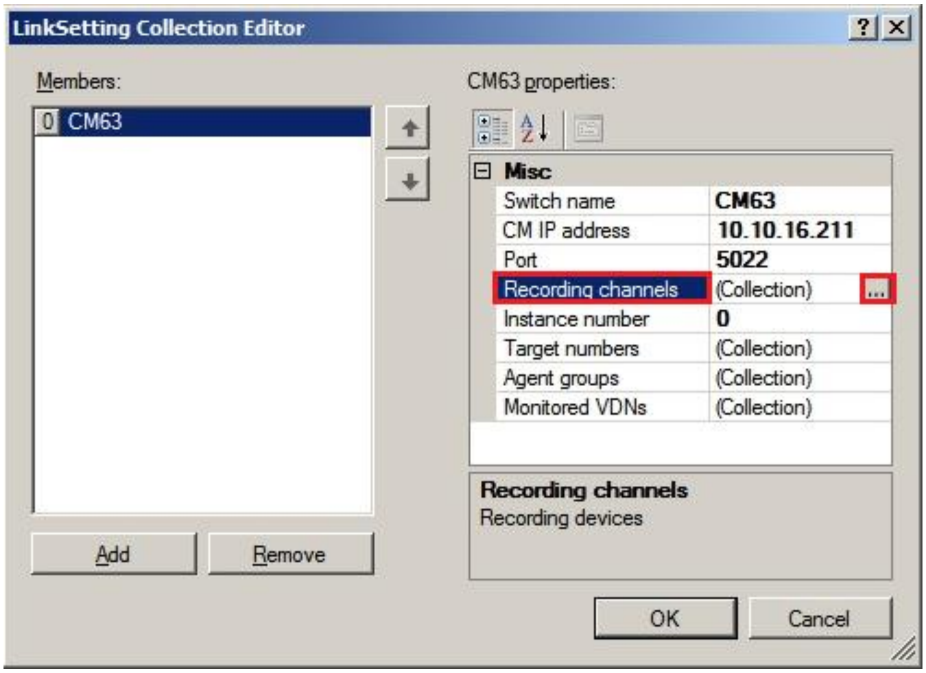


Misc	
Switch name	CM63
CM IP address	10.10.16.211
Port	5022
Recording channels	(Collection)
Instance number	0
Target numbers	(Collection)
Agent groups	(Collection)
Monitored VDNs	(Collection)

Switch name
Name of the AES server connection to Avaya Communication Manager.

7.1.2. Recording Channels

Click on the **Recording channels** field, and then click on the new button as highlighted below.

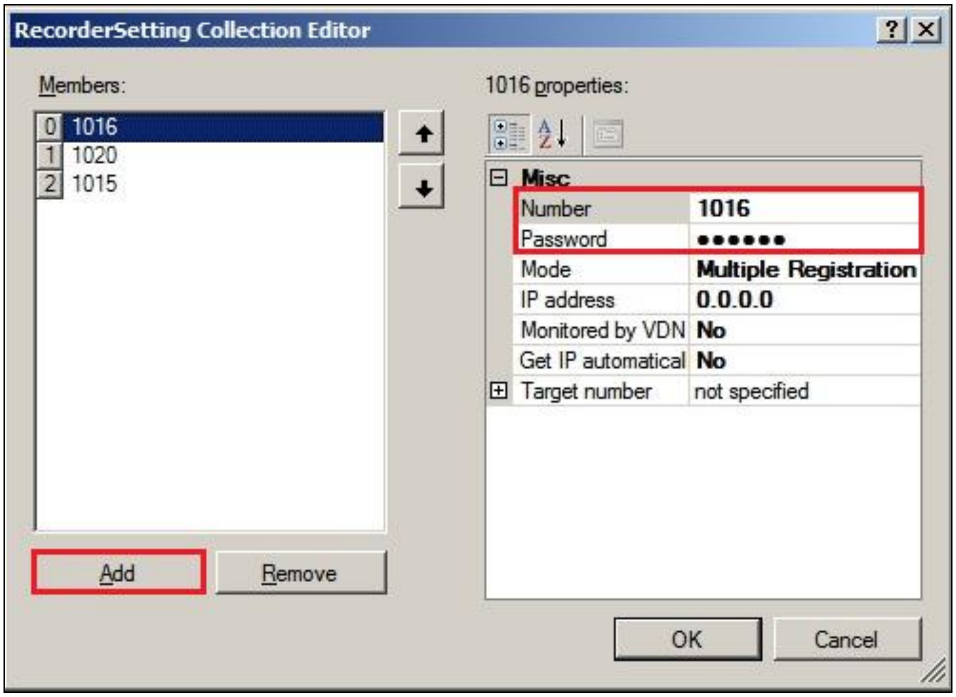


Misc	
Switch name	CM63
CM IP address	10.10.16.211
Port	5022
Recording channels	(Collection)
Instance number	0
Target numbers	(Collection)
Agent groups	(Collection)
Monitored VDNs	(Collection)

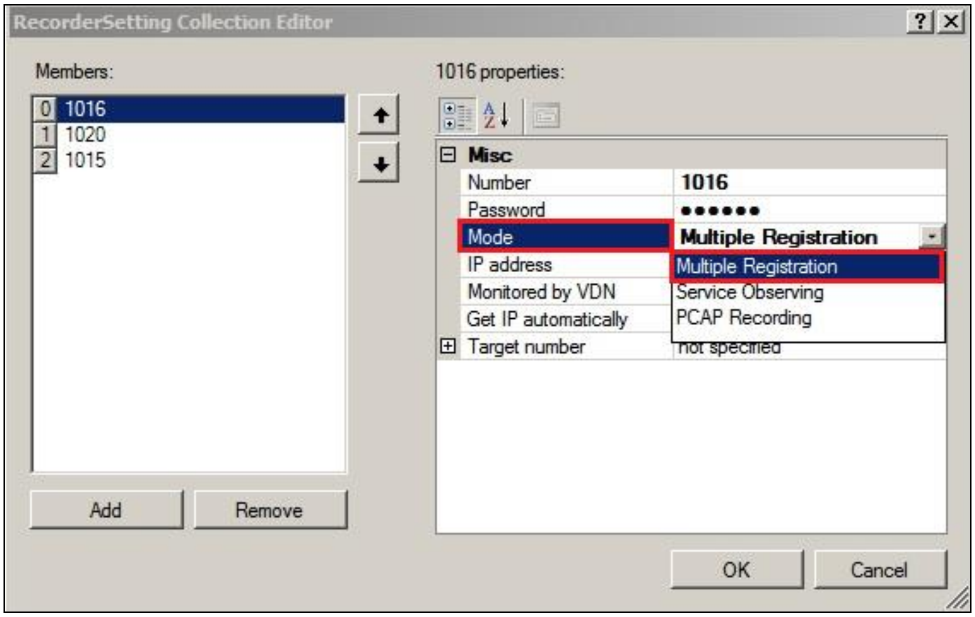
Recording channels
Recording devices

When the **RecorderSetting Collection Editor** window opens, click on the **Add** button and enter the following:

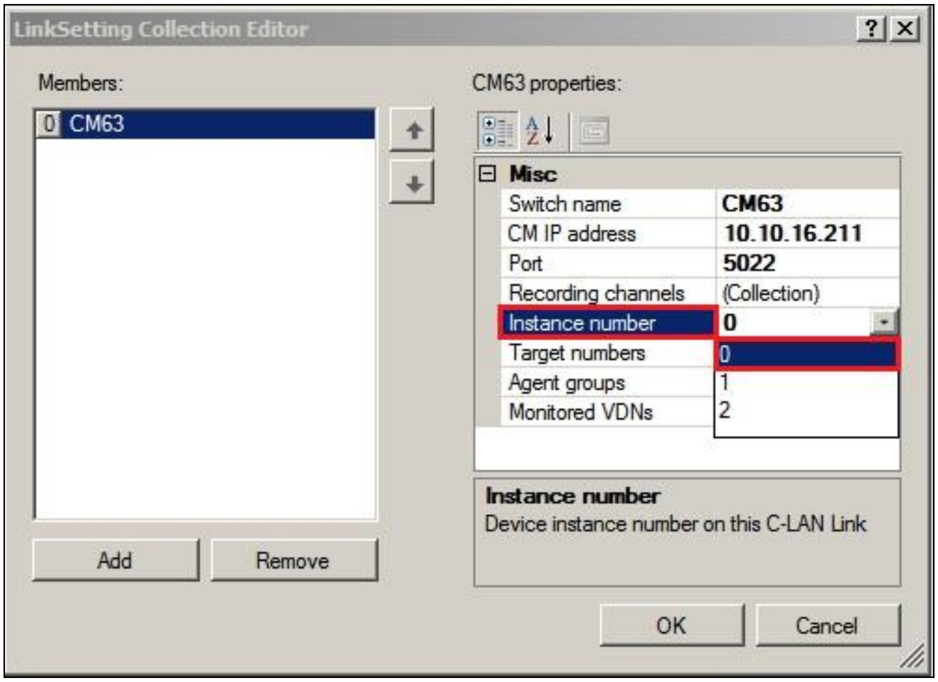
- **Number** Enter the extension to be monitored (extensions as configured in **Section 5.4**)
- **Password** Enter the extension password as configured in **Section 5.4**



Click on **Mode** field, and select **Multiple Registration** from the dropdown box. Leave the remaining fields as default. Click on the **OK** button to save. Repeat **Section 7.1.2** for each extension to be monitored.



After the Recording channels are configured, return to the **LinkSetting Collection Editor** window and click on the **Instance number** field. From the dropdown box select **0**.



LinkSetting Collection Editor

Members:

0 CM63

CM63 properties:

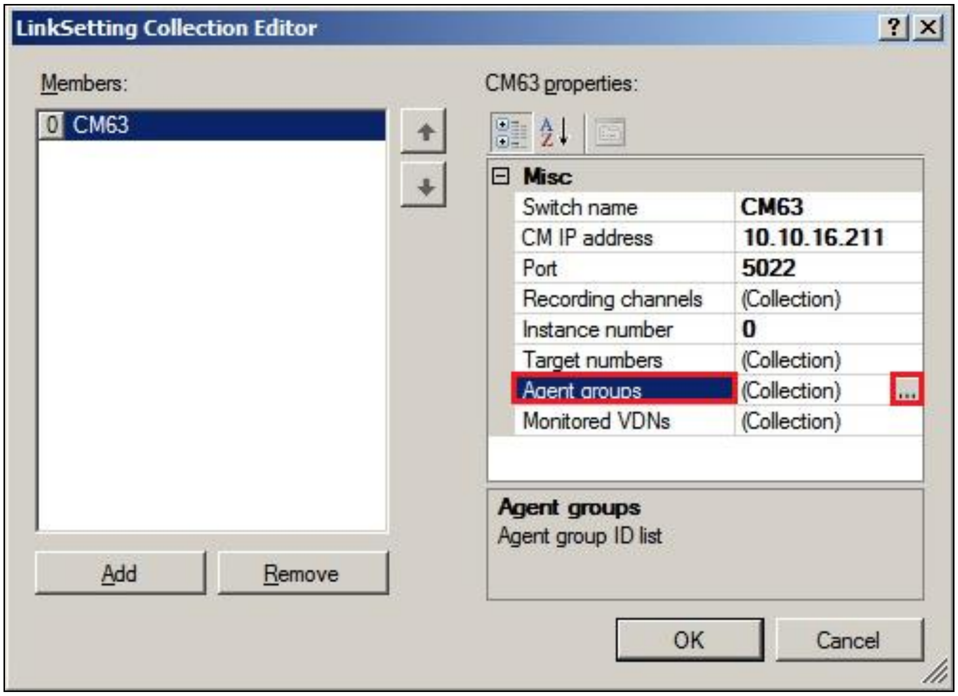
Misc

Switch name	CM63
CM IP address	10.10.16.211
Port	5022
Recording channels	(Collection)
Instance number	0
Target numbers	
Agent groups	
Monitored VDNs	

Instance number
Device instance number on this C-LAN Link

7.1.3. Agent Groups

For the purposes of recording agents, the **Agent groups** field is configured. Agents who log in to this skill will be recorded. Click on the **Agent groups** field, and then click on the new button as highlighted below.



LinkSetting Collection Editor

Members:

0 CM63

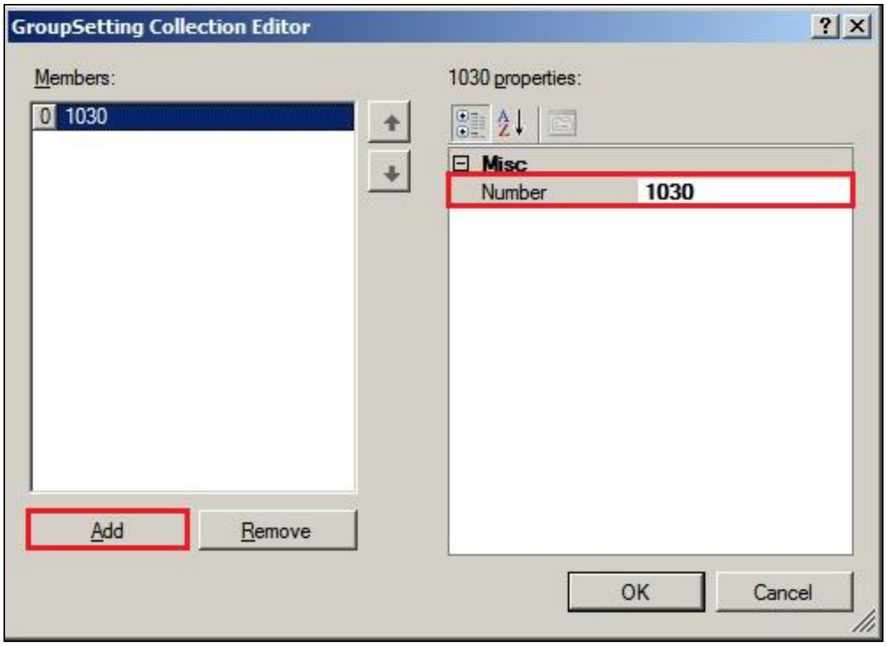
CM63 properties:

Misc

Switch name	CM63
CM IP address	10.10.16.211
Port	5022
Recording channels	(Collection)
Instance number	0
Target numbers	(Collection)
Agent groups	(Collection)
Monitored VDNs	(Collection)

Agent groups
Agent group ID list

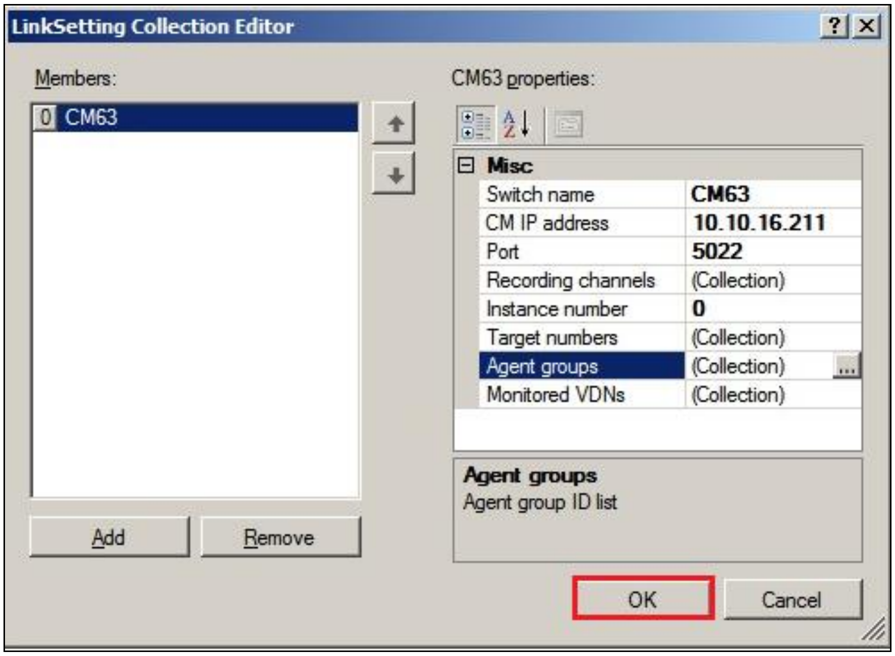
When the **GroupSetting Collection Editor** window opens, click on the **Add** button and enter the **group extension** (skilled hunt group) as configured in **Section 5.5**. Click on the **OK** button to save. Repeat **Section 7.1.3** for each skilled hunt group to be monitored.



Number 1030

After the Agent groups are configured, return to the **LinkSetting Collection Editor** window and click on the **OK** button to complete the configuration of the **Channel list** field.

Note: The **Target numbers** and **Monitored VDNs** fields were not configured during compliance testing. If configuration of these fields is required, use the procedure described in this section.

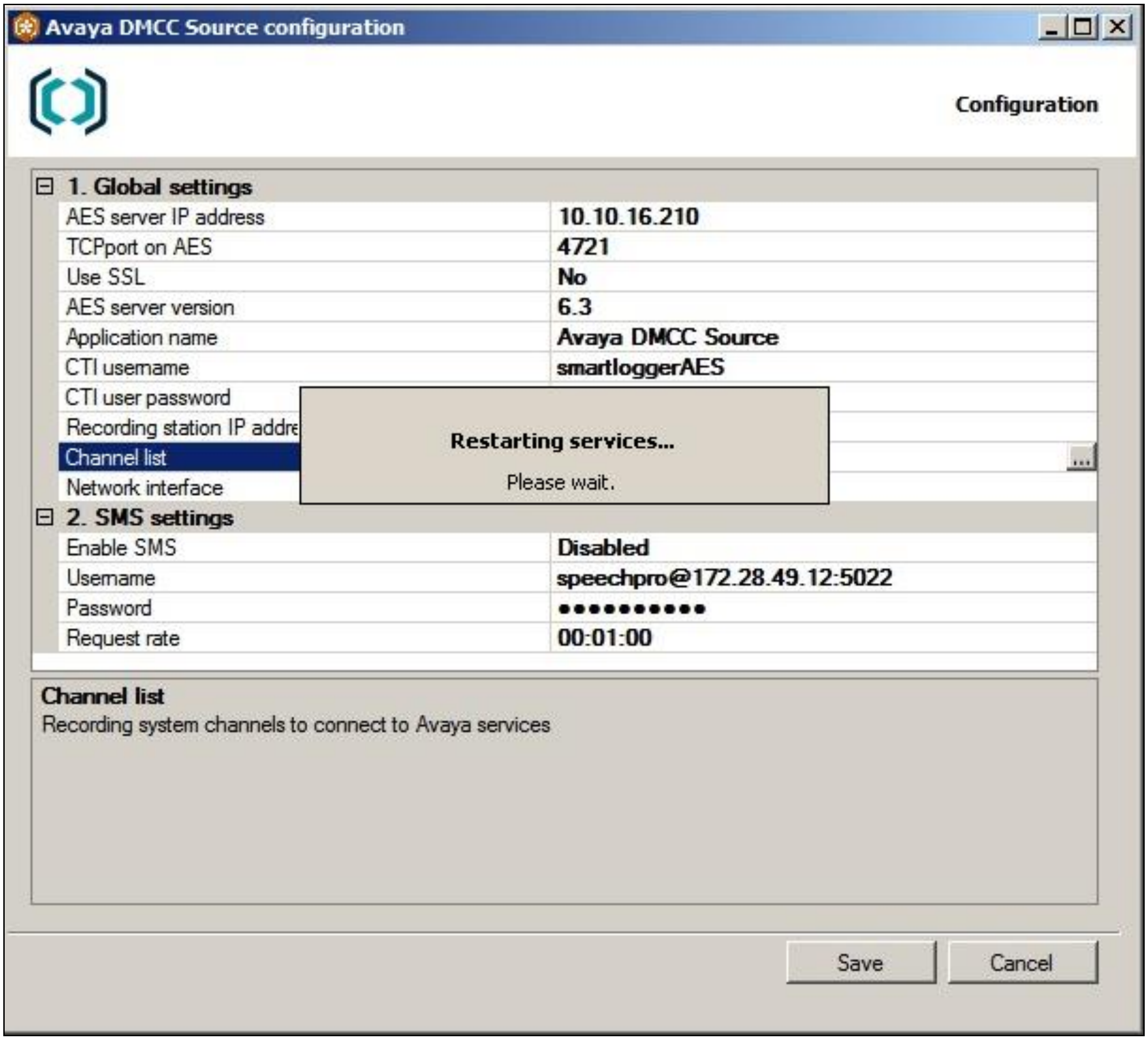


Switch name	CM63
CM IP address	10.10.16.211
Port	5022
Recording channels	(Collection)
Instance number	0
Target numbers	(Collection)
Agent groups	(Collection)
Monitored VDNs	(Collection)

Agent groups
Agent group ID list

On returning to the main configuration window, click on the **Save** button to complete the relevant settings. The screen below will be shown, advising the restart of the Smart Logger II services with the new configuration.

Note: The **Network interface** field or any field in **SMS settings** were not configured during compliance testing.



Avaya DMCC Source configuration

Configuration

1. Global settings	
AES server IP address	10.10.16.210
TCPport on AES	4721
Use SSL	No
AES server version	6.3
Application name	Avaya DMCC Source
CTI username	smartloggerAES
CTI user password	
Recording station IP addre	
Channel list	...
Network interface	
2. SMS settings	
Enable SMS	Disabled
Username	speechpro@172.28.49.12:5022
Password	●●●●●●●●●●
Request rate	00:01:00

Restarting services...

Please wait.

Channel list
Recording system channels to connect to Avaya services

8. Verification Steps

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

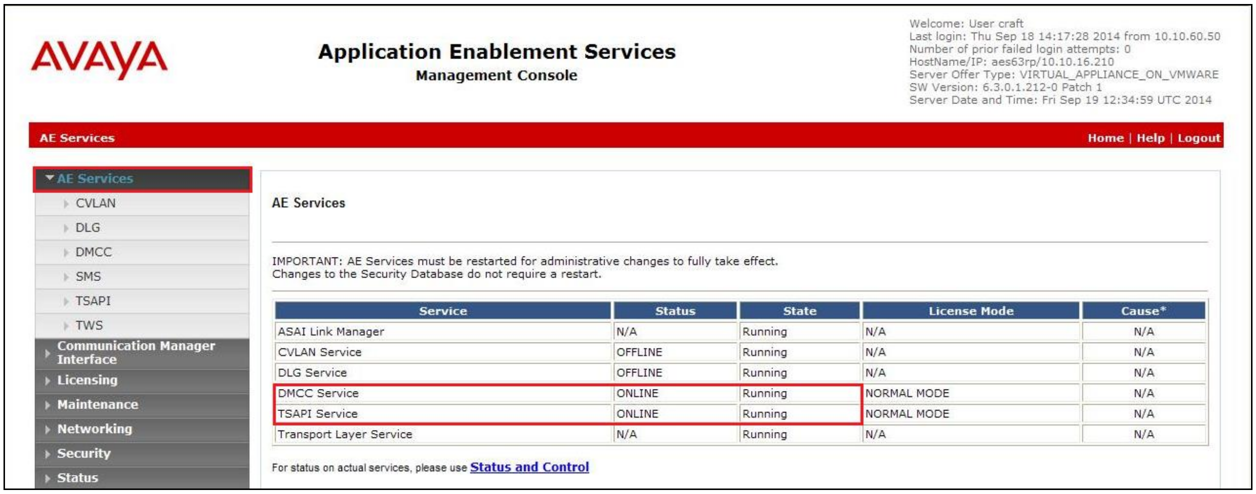
8.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can ensure that the communication between Communication Manager and AES is functioning correctly. Use SAT to connect to Communication Manager and check the AESVCS link status with AES 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    aes63rp          established   17       15
```

8.2. Verify Avaya Aura® Application Enablement Services Status

Login to AES, and navigate to the **AE Services** screen. Verify that the DMCC and TSAPI Services are **ONLINE**, and **Running**.



Welcome: User craft
Last login: Thu Sep 18 14:17:28 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Fri Sep 19 12:34:59 UTC 2014

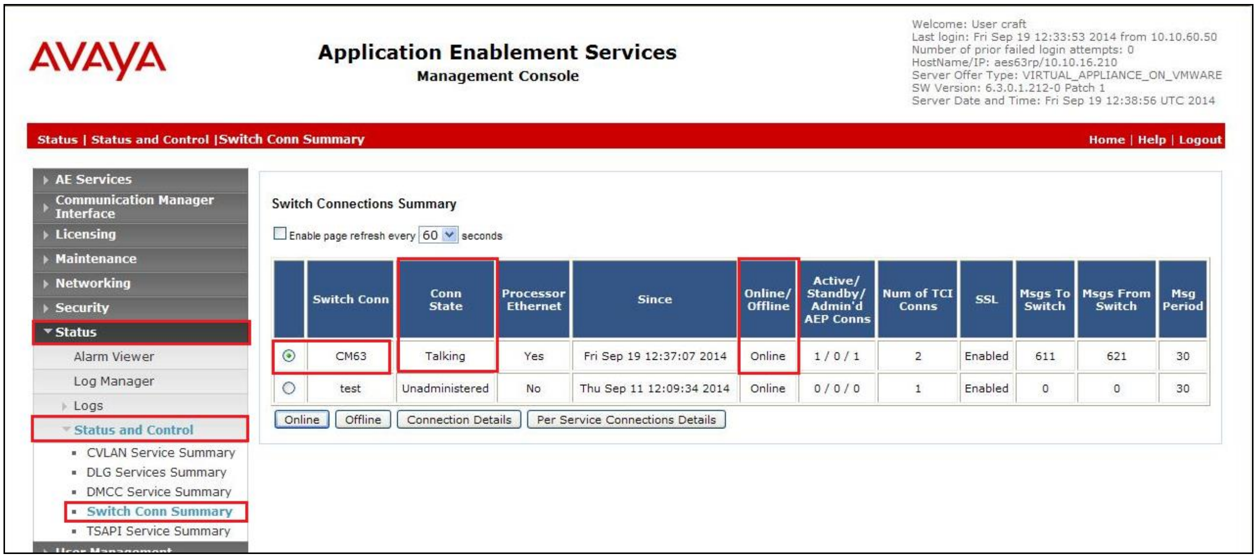
AE Services

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

Navigate to **Status → Status and Control -> Switch Conn Summary**. Verify that **Conn State** is **Talking** and **Online/Offline** is **Online** for the configured Communication Manager switch connection.



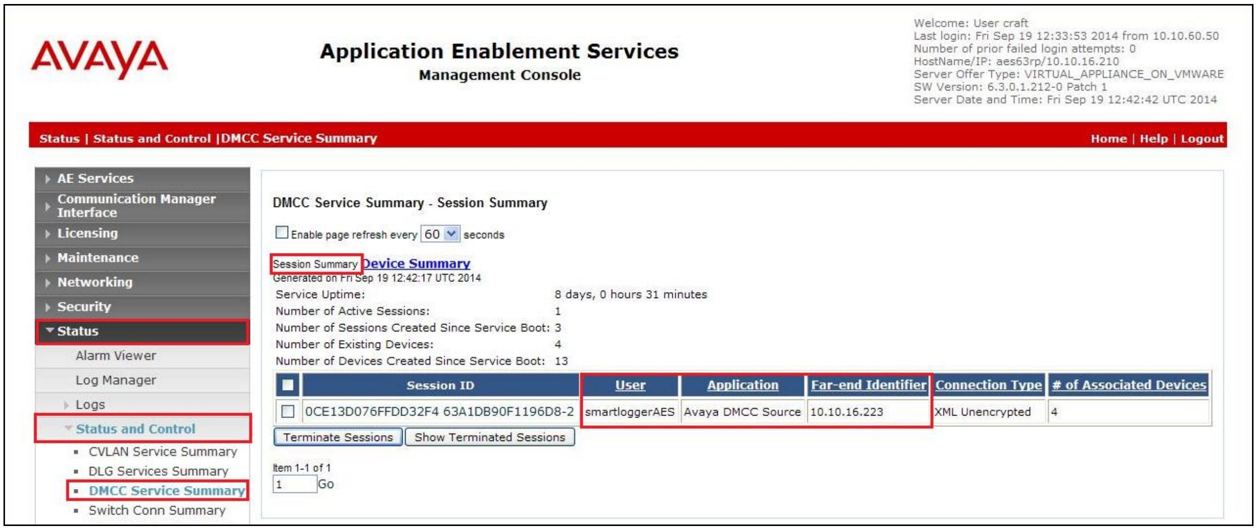
Welcome: User craft
Last login: Fri Sep 19 12:33:53 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Fri Sep 19 12:38:56 UTC 2014

Switch Connections Summary

□ Enable page refresh every 60 seconds

	Switch Conn	Conn State	Processor Ethernet	Since	Online/ Offline	Active/ Standby/ Admin'd AEP Conns	Num of TCI Conns	SSL	Msgs To Switch	Msgs From Switch	Msg Period
●	CM63	Talking	Yes	Fri Sep 19 12:37:07 2014	Online	1 / 0 / 1	2	Enabled	611	621	30
○	test	Unadministered	No	Thu Sep 11 12:09:34 2014	Online	0 / 0 / 0	1	Enabled	0	0	30

Navigate to **Status → Status and Control -> DMCC Service Summary** and click **Service Summary** on the right. Verify that the User (**samartloggerAES**) shows the **Application** is set to **Avaya DMCC Source** and the **Far-end Identifier** is set to the IP address of the Smart Logger II Server (**10.10.16.223**).



Welcome: User craft
Last login: Fri Sep 19 12:33:53 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.1.212-0 Patch 1
Server Date and Time: Fri Sep 19 12:42:42 UTC 2014

DMCC Service Summary - Session Summary

□ Enable page refresh every 60 seconds

Generated on Fri Sep 19 12:42:17 UTC 2014

Service Uptime:	8 days, 0 hours 31 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	3
Number of Existing Devices:	4
Number of Devices Created Since Service Boot:	13

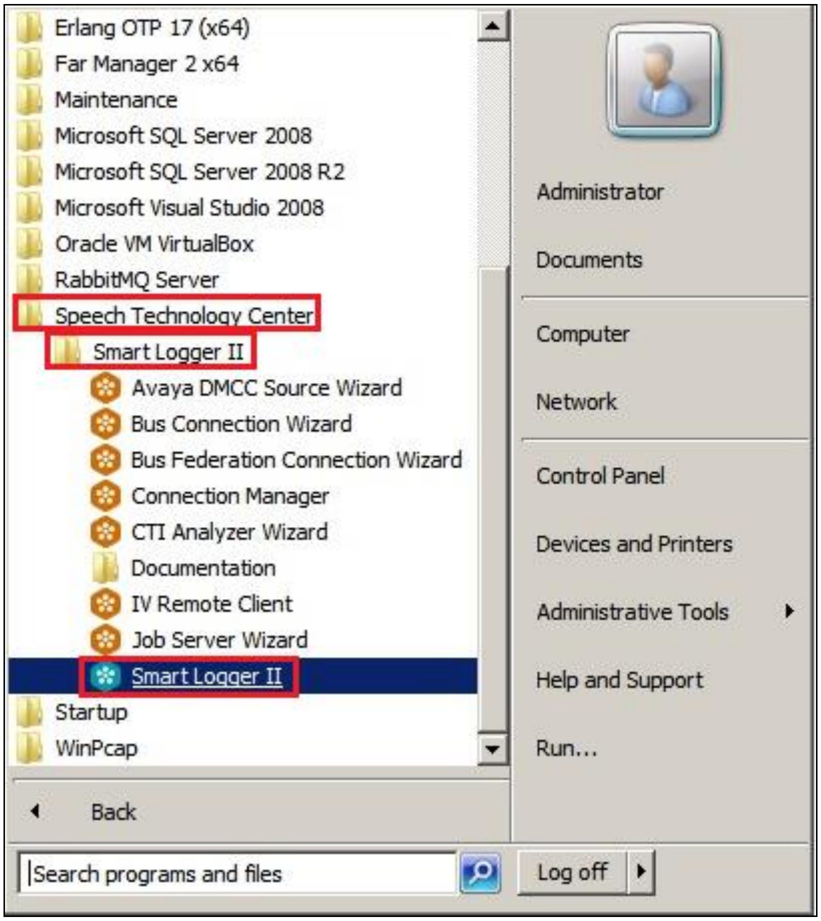
□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	0CE13D076FFDD32F4 63A1DB90F1196D8-2	smartloggerAES	Avaya DMCC Source	10.10.16.223	XML Unencrypted	4

Item 1-1 of 1

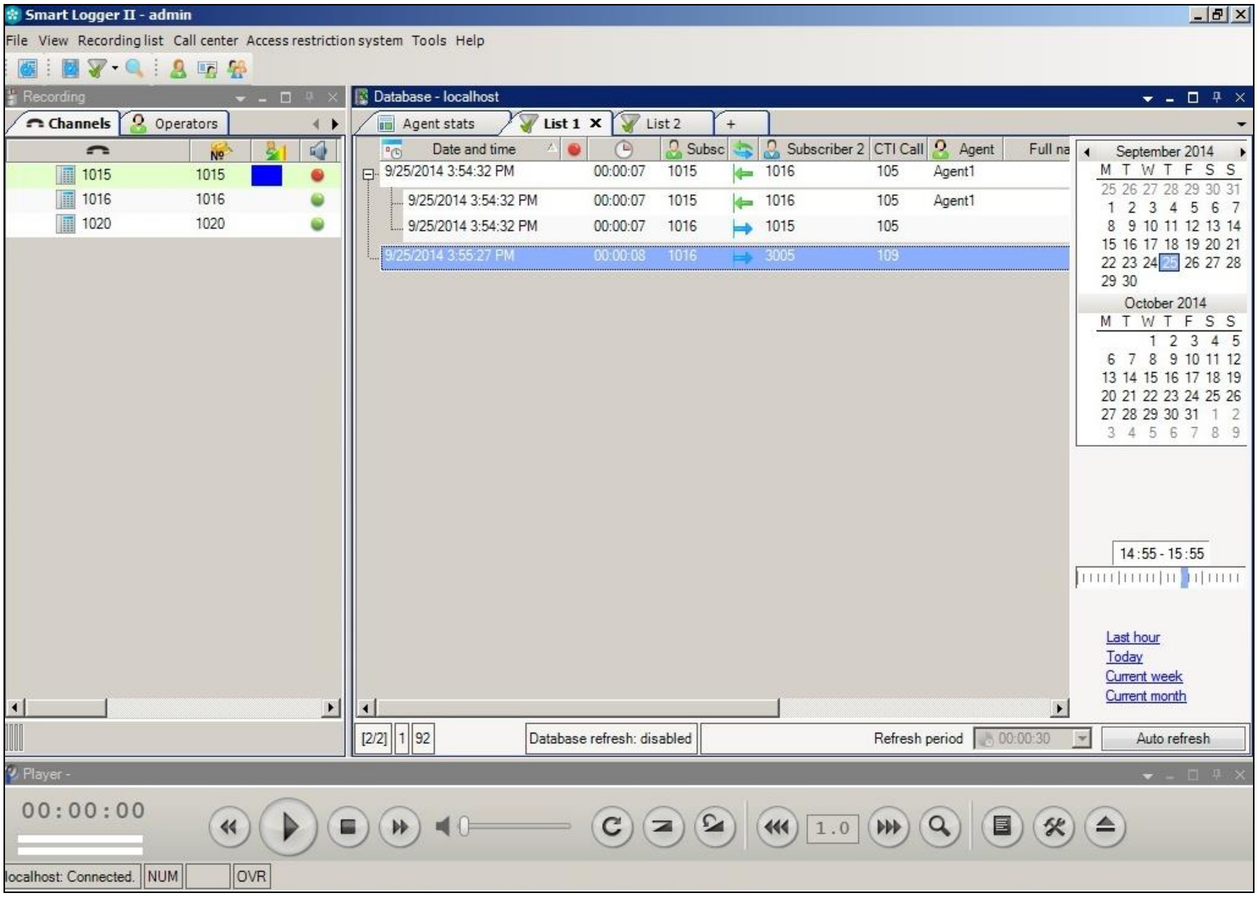
1

8.3. Verify Speech Technology Centre Smart Logger II

On the PC hosting Smart Logger II, click **Start** → **All Program** (not shown) then navigate to **Speech Technology Centre** →**Smart Logger II**→ **Smart Logger II**.



In the Smart Logger II application window, verify that the **localhost: Connected** status is shown in the window's status bar at the bottom. 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.



☎	№		
1015	1015	🟦	🔴
1016	1016		🟢
1020	1020		🟢

Date and time	●		Subsc		Subscriber 2	CTI Call	Agent	Full na
9/25/2014 3:54:32 PM		00:00:07	1015	←	1016	105	Agent1	
9/25/2014 3:54:32 PM		00:00:07	1015	←	1016	105	Agent1	
9/25/2014 3:54:32 PM		00:00:07	1016	→	1015	105		
9/25/2014 3:55:27 PM		00:00:08	1016	→	3005	109		

September 2014

M	T	W	T	F	S	S
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

October 2014

M	T	W	T	F	S	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

14:55 - 15:55

Last hour
Today
Current week
Current month

[2/2] 1 92 Database refresh: disabled Refresh period 00:00:30 Auto refresh

00:00:00

localhost: Connected. NUM OVR

9. Conclusion

A full and comprehensive set of feature functional test cases were performed during compliance testing. Speech Technology Centre Smart Logger II v8.4 is considered compliant with Avaya Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3. All test cases have passed and met the objectives outlined in **Section 2.2** with one observation.

10. Additional References

This section references the Avaya and Speech Technology Centre documentation that is relevant to these Application Notes. Avaya product documentations, including the following, are available at *http://support.avaya.com*.

[1] *Administering Avaya Aura® Communication Manager, Release 6.3, October 2013, Document Number 03-300509, Issue 9.0.*

[2] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 6.3, May 2013, Document Number 555-245-205, Issue 10.0.*

[3] *Administering Avaya Aura® Session Manager, Release 6.3, Issue 3 October 2013.*

[4] *Administering Avaya Aura® System Manager, Release 6.3, Issue 3, October, 2013.*

[5] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 6.3, Issue 2 October 2013.*

Product Documentation for Speech Technology Centre can be obtained at the website: http://*www.speechpro.com/support/download*

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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*.