Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.2 and Avaya Aura® Application Enablement Services R6.2 with Voxtronic Communication Server using Single Step Conference – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Voxtronic Communication Server to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services. Voxtronic Communication Server is a call recording solution. In the compliance testing, Voxtronic Communication Server used the Avaya Aura® Application Enablement Services Device, Media, and Call Control (DMCC) interface to register a number of configured Single Step Conference Stations configured on Avaya Aura® Communication Manager. A number of stations configured on Avaya Aura® Communication Manager were monitored for which calls were to be recorded using the Telephony Services Application Programming Interface (TSAPI) of Avaya Aura® Application Enablement Services via DMCC.

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

These Application Notes describe the configuration used to enable the Voxtronic Communication Server call recorder to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. The Voxtronic Communication Server call recorder offers various methods of voice recording. For the purpose of the tests described by these Application Notes, the Avaya Aura® Communication Manager Single Step Conference feature was used.

Voxtronic Communication Server can be configured to monitor specific local endpoints and record calls made to or from those endpoints. Calls between or among local endpoints which are each monitored produce multiple voice files: one for each monitored endpoint.

2. General Test Approach and Test Results

The general test approach was to validate correct recording of calls in a variety of call handling scenarios and recovery from network interruption. Parties involved in calls, clarity of recording and accurate call times and durations were verified. The resumption of call recording following outages of various components of the solution was also checked.

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

Interoperability compliance testing consisted of the successful, clear and accurate recording and playback via the Voxtronic Communication Server web interface of both monitored and unmonitored extensions, as well as recovery from failure in the following scenarios:

- Internal calls – called/calling party ends call
- Calls between networked PBX's - inbound/outbound called party/calling party ends call
- PSTN Calls – inbound/outbound called party/calling party ends call
- Hold/Retrieve
- Supervised/Unsupervised Transfer
- Conference
- Call Forwarding
- Hunt Group Calls
- Bridged Appearance – answered/placed by bridged appearance
- Calls gone to cover
- PBX restart recovery
- Voxtronic Communication Server network recovery
- Voxtronic Communication Server power outage recovery

2.2. Test Results

All test cases passed successfully with the following observations:

- Where an inbound trunk call is made to a monitored station the call appears on the Voxtronic Communication Server call recording web interface as A-PSTN with the "Other Party" field filled with the actual DDI dialed by the PSTN.
- Where a station is forwarded, the record is presented as the calling and answering party and does not include the forwarded party. Similarly this is the case where a coverage path is used.
- Where A is a monitored station and e is not monitored and e is configured with a bridged appearance for A; if a call from an unmonitored station to A is answered by its bridged appearance on e, the call is not recorded.
- Where A is a monitored station and e is not monitored and e is configured with a bridged appearance for A; if a call is placed to an unmonitored station from the bridged appearance of A on e, the call is not recorded.
- Where the LAN cable to the Voxtronic Communication Server is disconnected during a monitored call, the call is recorded up to the point of the disconnection and appears on the web interface after reconnection of the LAN. If the call is ended after the reconnection of the LAN an additional call record without the remaining audio recording is presented on the web interface.

2.3. Support

Support for Voxtronic Communication Server is available as follows:

- General technical support from Voxtronic Communication Server can be obtained by sending mail to: support@voxtronic.com.
- A support enquiry can also be presented through the form available at the Voxtronic web site: http://www.voxtronic.com/en/Request-Support

3. Reference Configuration

Figure 1 shows an Avaya S8800 Server running Avaya Aura® Communication Manager R6.2 serving H.323 endpoints with an Avaya G450 Media Gateway was configured along with Avaya Aura® Session Manager R6.2 hosted on an Avaya S8800 Server providing SIP endpoints. Voxtronic Communication Server was configured on the same IP network for connection to Avaya Aura® Application Enablement Services over DMCC.

Note: Only a DMCC connection was created between Application Enablement Services and Voxtronic Communication Server. Required TSAPI features such as monitoring of stations was triggered via the DMCC connection.

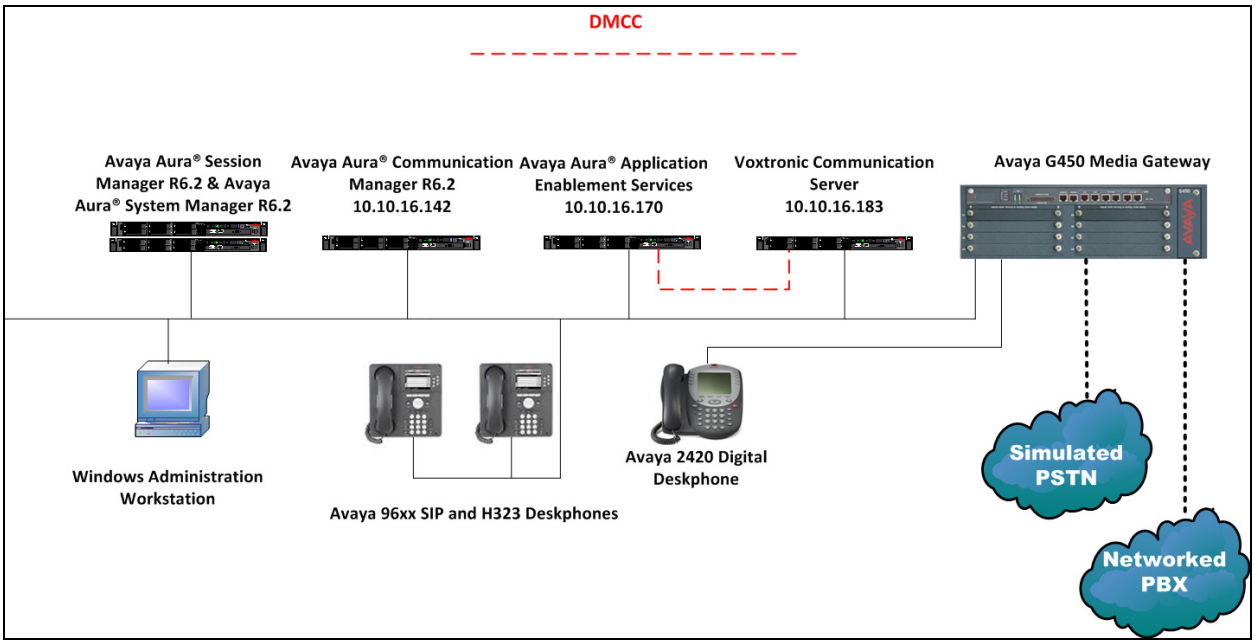


Figure 1: Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services with Voxtronic Communication Server

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.2 SP5 build R016x.02.0.823.0-20396
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.2 SP4
Avaya Aura® Application Enablement Services	R6.2 patch 1
Avaya G450 Media Gateway • MM710 • MM712	32.24.0 • HW5 FW22 • HW7 FW14
Avaya 9630 IP Deskphone	• H.323 3.2 • SIP 2.6 SP8
Avaya 2420 Digital Deskphone	2420 Rel 6.00 HWT=51H HWV=1 FWV=6
Voxtronic Communication Server running on virtualized Microsoft Windows 7 Professional	• Voxtronic Communication Server 4.1.3.D • VoxAvayarps Call Control Module - 0.1.0.2 • Avaya Aura® Application Enablement Services DMCC Java SDK 6.2.0.69

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using the Communication Manager System Access Terminal (SAT). It is assumed that the relevant dialplan, hunt groups, stations, trunks and call routing have been configured. The connection from Communication Manager to Session Manager is not specific to the test environment and is therefore not detailed below.

The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as installation and configuration, please refer to the product documentation in **Section 10**.

5.1. Configure AE Services

An AE Services link must be established between Communication Manager and Application Enablement Services. Enter the command **change node-names ip** and enter the node **Name** and **IP Address** for Application Enablement Services in this case **10.10.16.170**. Take a note of the **procr** node **Name** and **IP Address**, in this case **10.10.16.142.**

```
change node-names ip                                            Page   1 of   2
                                   IP NODE NAMES
    Name               IP Address
procr               10.10.16.142
default             0.0.0.0
aes62vm             10.10.16.170
```

In order for Communication Manager to establish a connection to Application Enablement Services, administer the CTI Link as shown below. Using the **add cti-link next** command specify an available **Extension** number, 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 next                                               Page   1 of   3
                                     CTI LINK
 CTI Link: 1
Extension: 5899
     Type: ADJ-IP
                                                                      COR: 1
     Name: aes62vm
```

Using the command **change ip-services,** configure IP Services using **AESVCS** as the **Service Type** enter the **procr** node name as noted above as the **Local Node**.

```
change ip-services                                              Page   1 of   4

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

AESVCS         y           procr           8765
```

On **Page 4**, set the **AE Services Server** hostname and the **Password** that Application Enablement Services will use to authenticate with Communication Manager.

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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:       aes62vm           Avayapassword1        y        in use
```

5.2. Configure Single Step Conference Stations

Voxtronic Communication Server uses a pool of stations as recording extensions, these are used to conference into stations which are configured to have their calls monitored. Enter the command **add station next** and configure a relevant **Extension**, set the **Security Code** which must be common for all of the configured recording extensions, set the **Type** as **4624**, the **Port** as **IP** and assign an identifying **Name**. Ensure that **IP SoftPhone** is set to **y**. Repeat this according to the number extensions required by Voxtronic Communication Server. During the compliance test 8 stations were configured for this purpose, 6500 – 6507.

```
add station next                                                Page   1 of   6
                                        STATION
Extension: 6500                             Lock Messages? n              BCC: 0
     Type: 4624                             Security Code: 1234            TN: 1
     Port: IP                           Coverage Path 1:                COR: 1
     Name: Recorder,6500                    Coverage Path 2:                COS: 1
                                            Hunt-to Station:
STATION OPTIONS
                                                Time of Day Lock Table:
              Loss Group: 19            Personalized Ringing Pattern: 1
                                                  Message Lamp Ext: 6500
            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
```

5.3. Configure SIP Stations for CTI Control

SIP stations must be configured so they can be monitored by Voxtronic Communication Server, enter the command **change station xxxx** where **xxxx** is a SIP extension and configure **Type of 3PCC Enabled** to **Avaya** in this instance on **Page 6**. For the purposes of the compliance test SIP stations 6002 and 6003 were configured.

```
change station 6002                                             Page   6 of   6
                                        STATION
SIP FEATURE OPTIONS
         Type of 3PCC Enabled: Avaya
                    SIP Trunk: aar
```

5.4. Configure SIP Signaling Group

It is assumed that the necessary configuration has been previously administered to service SIP endpoints. Enter the command **change signaling group x** where **x** is the relevant SIP trunk. **Ensure that Initial IP-IP Direct Media** is set to **n** in order to successfully record calls between SIP endpoints.

```
change signaling-group 1                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? y      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM

   Near-end Node Name: procr                 Far-end Node Name: sm62sigint
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain:
                                           Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload          Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                   IP Audio Hairpinning? n
         Enable Layer 3 Test? y                 Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

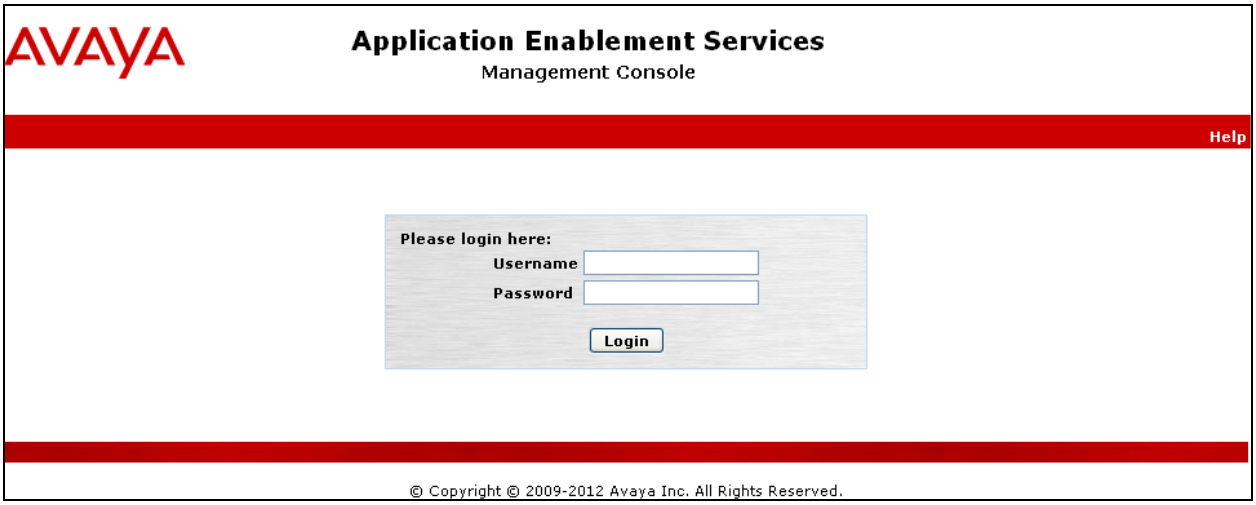
6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

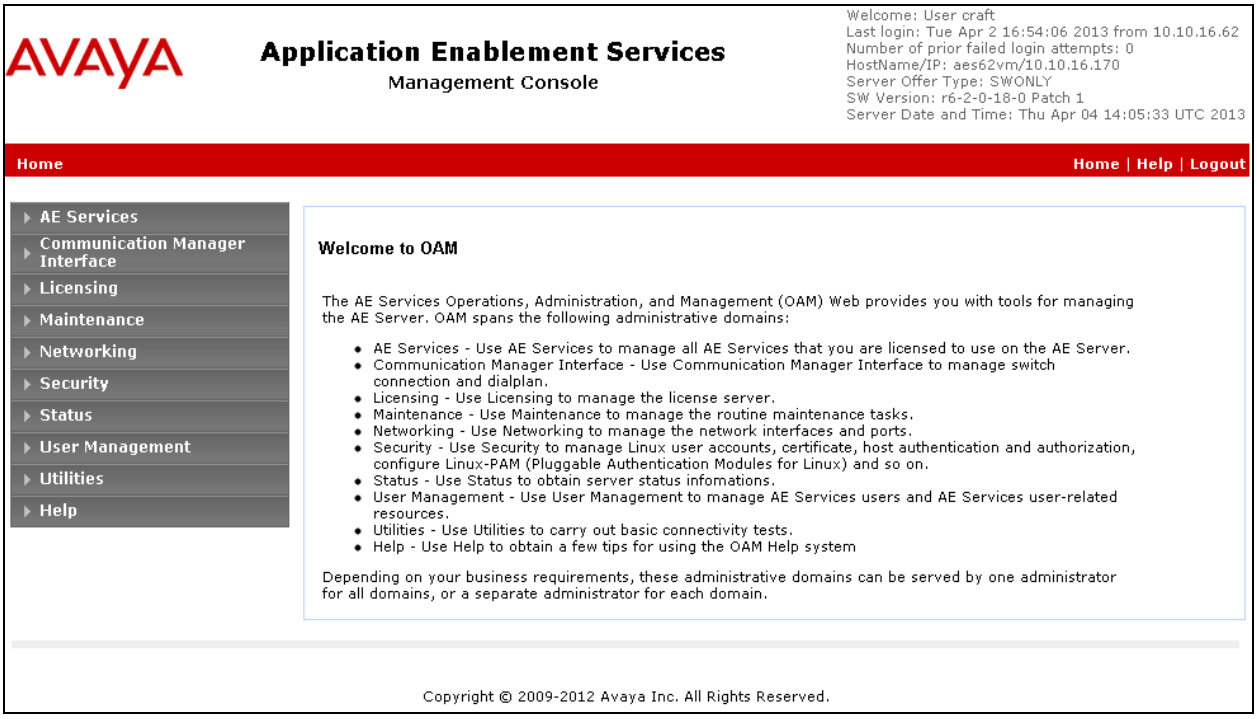
- Launch OAM interface
- Administer the Switch Connection
- Administer TSAPI Link
- Restart TSAPI Service
- Obtain Tlink name
- Administer Avaya CTI User

6.1. Launch OAM Interface

Access the OAM web-based interface of Application Enablement Services, in this instance using the URL https://10.10.16.170 . The Management Console is displayed. Log in using the appropriate credentials.

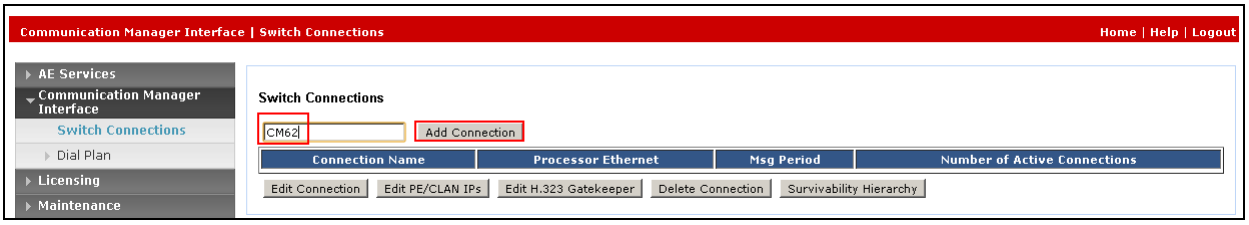


The **Welcome to OAM** screen is displayed next.

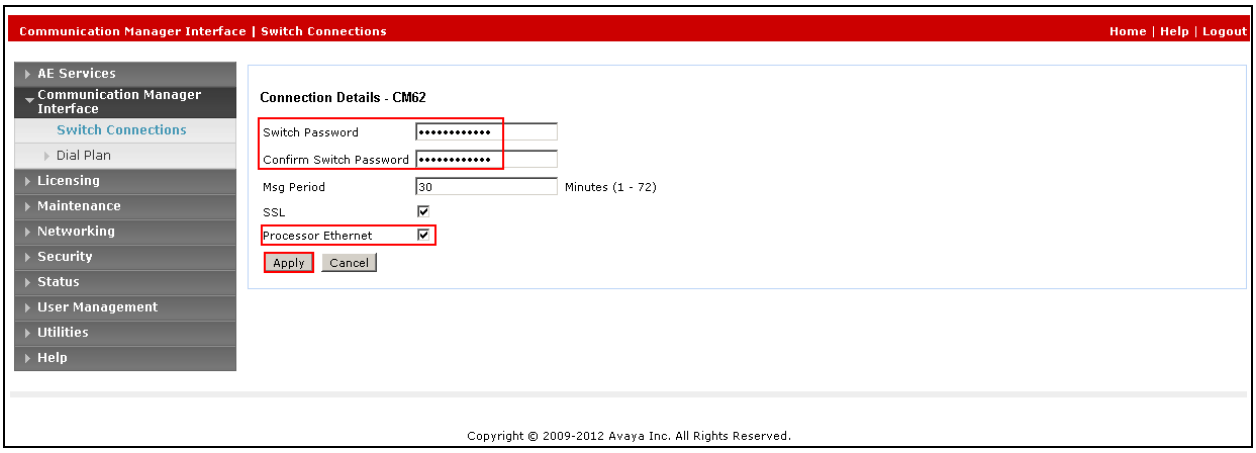


6.2. Administer the Switch Connection

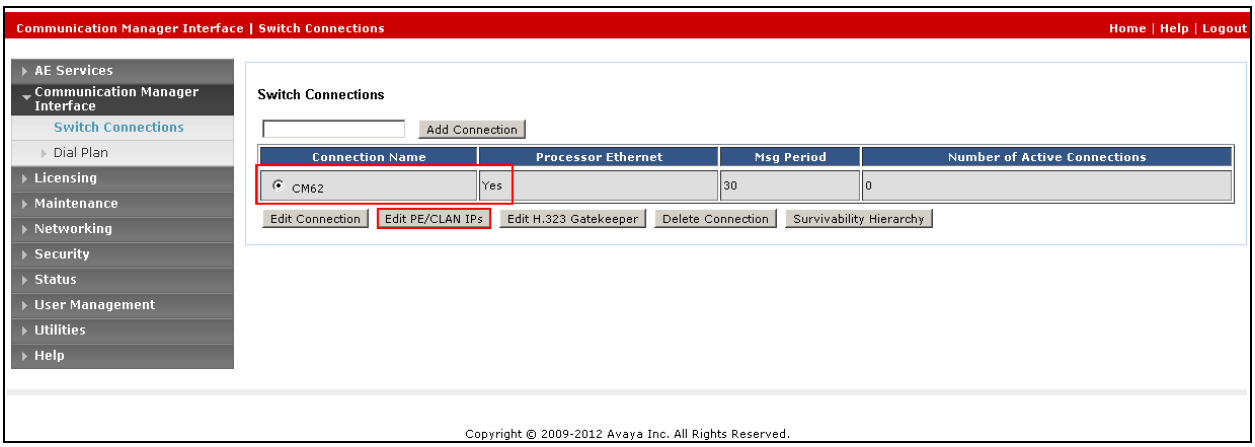
To establish the connection between Communication Manager and Application Enablement Services, click **Communication Manager Interface → Switch Connections**. In the field next to **Add Connection** enter an appropriate Switch Connection name, in this case **CM62** and click on **Add Connection**.



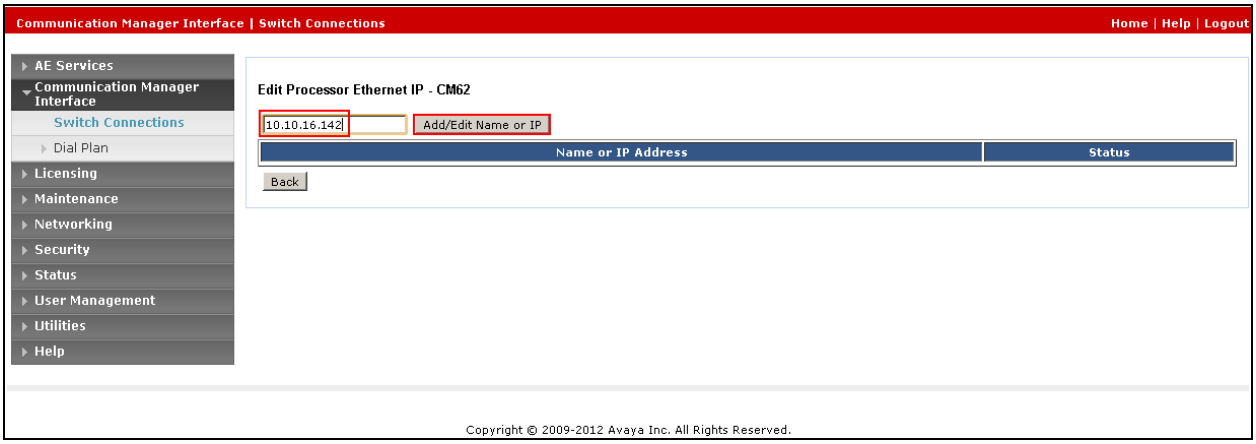
The following screen is displayed. Complete the configuration as shown and enter the password specified in **Section 5.1** when configuring AESVCS in ip-services. Place a check in the **Processor Ethernet** box as in this case a C-LAN is not being used in the configuration and the Switch Connection is made to the Communication Manager procr IP address. Click on **Apply** when done.



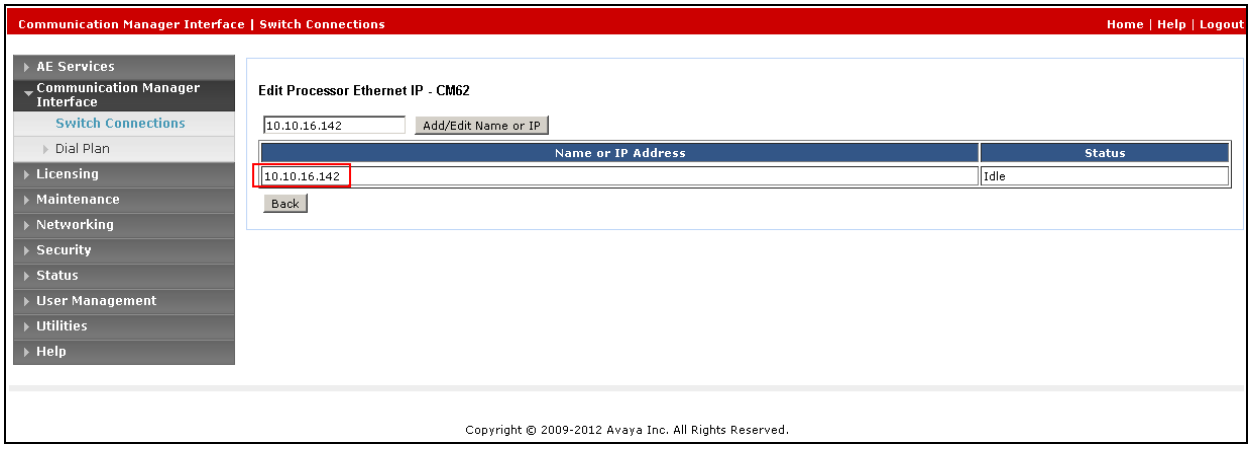
The following screen will be shown displaying the newly added switch connection, click on **Edit PE/CLAN IPs** in order to specify the IP address of the procr, as noted in **Section 5.1**.



Next to **Add Name or IP,** enter the IP address of the procr as shown below.

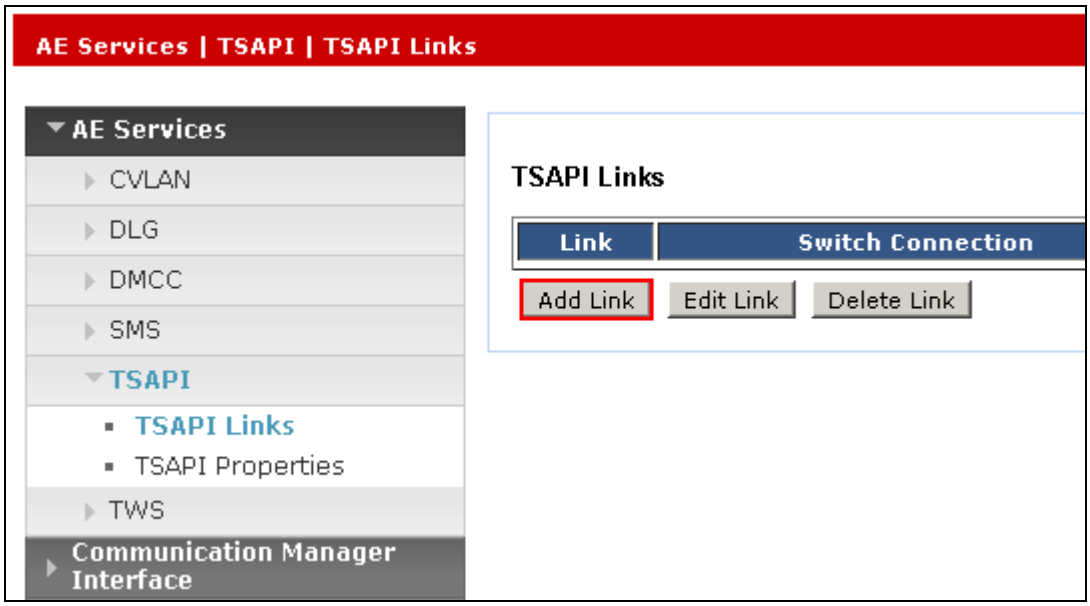


The following screen will now appear displaying the newly added IP address.



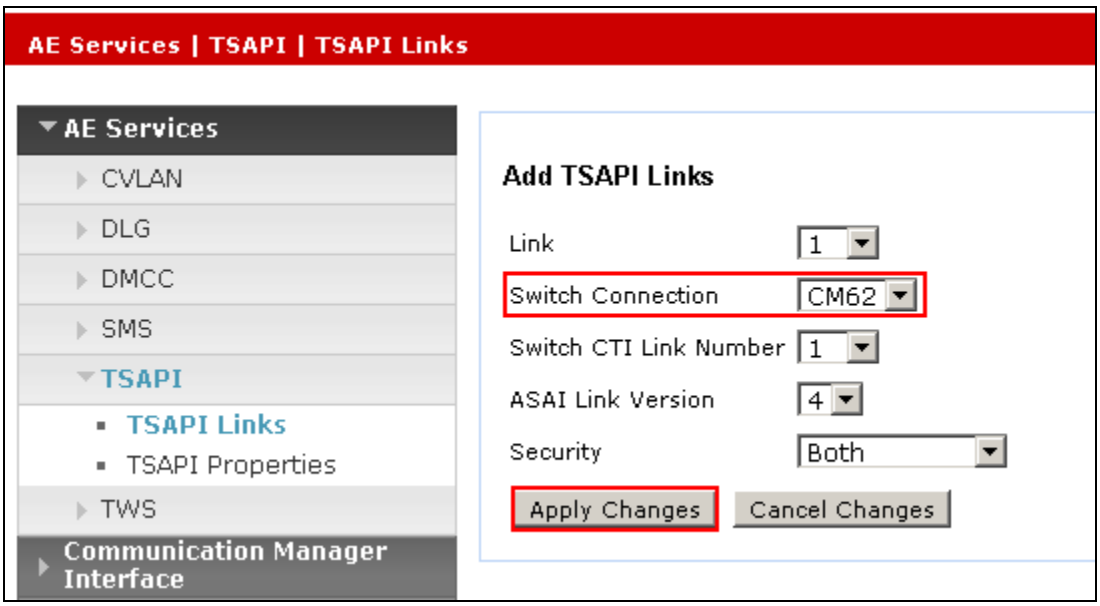
6.3. Administer TSAPI Link

Select **AE Services → TSAPI → TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, click **Add Link**.

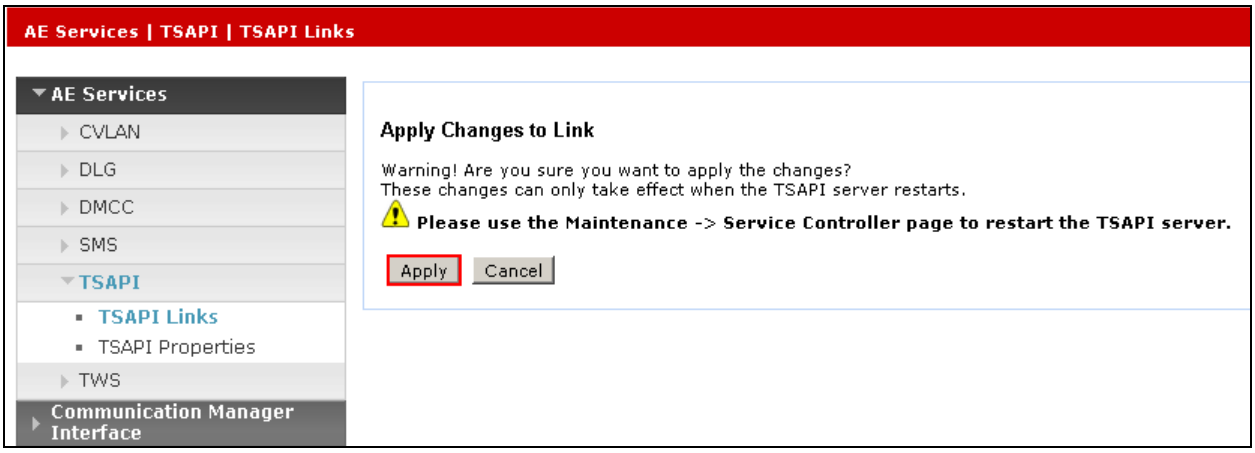


Configure the TSAPI Link using the newly configured **Switch Connection** as follows and click **Apply Changes**.

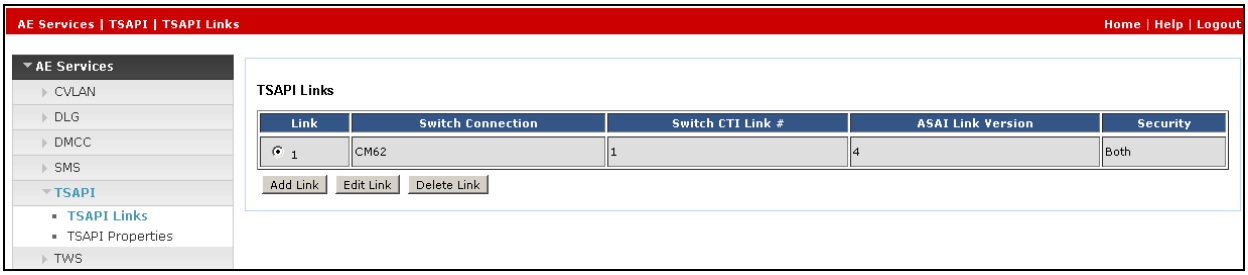
- **Link** – select the next available link number
- **Switch Connection** – select the newly configured Switch Connection
- **Switch CTI Link Number** - enter the CTI Link number configured in **Section 5.1**
- **Security** – set to **Both** to enable both Encrypted and Unencrypted TSAPI connections. Voxtronic Communication Server uses an unsecure connection



The screen below will be displayed with instructions to restart the TSAPI Server. Click **Apply** taking note of the instructions given.

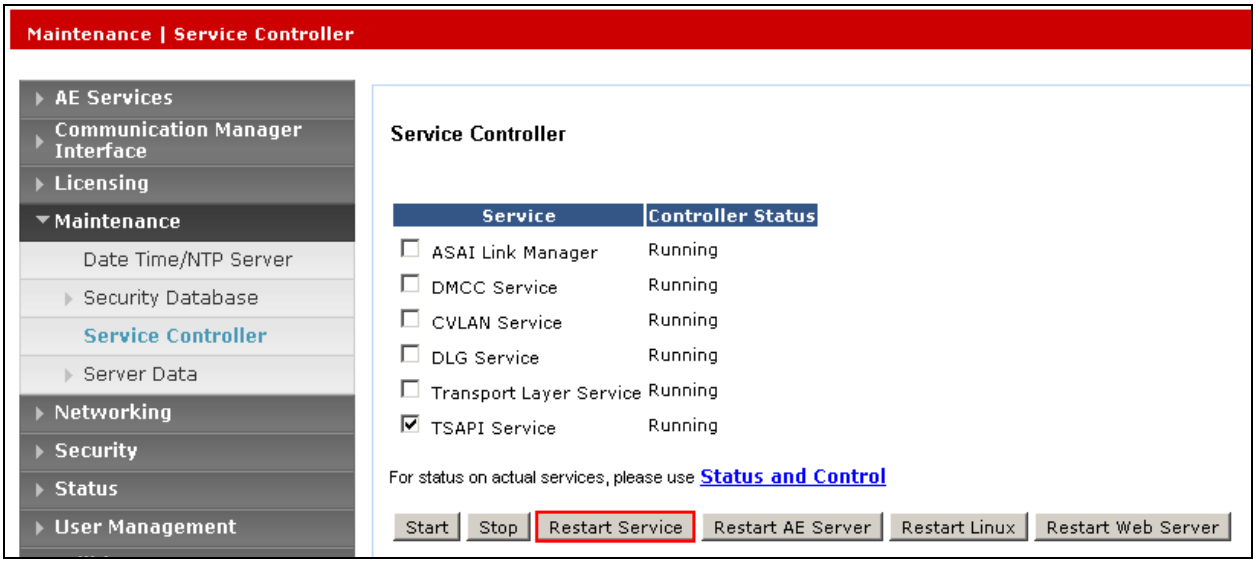


The following screen will be displayed showing the TSAPI Link.



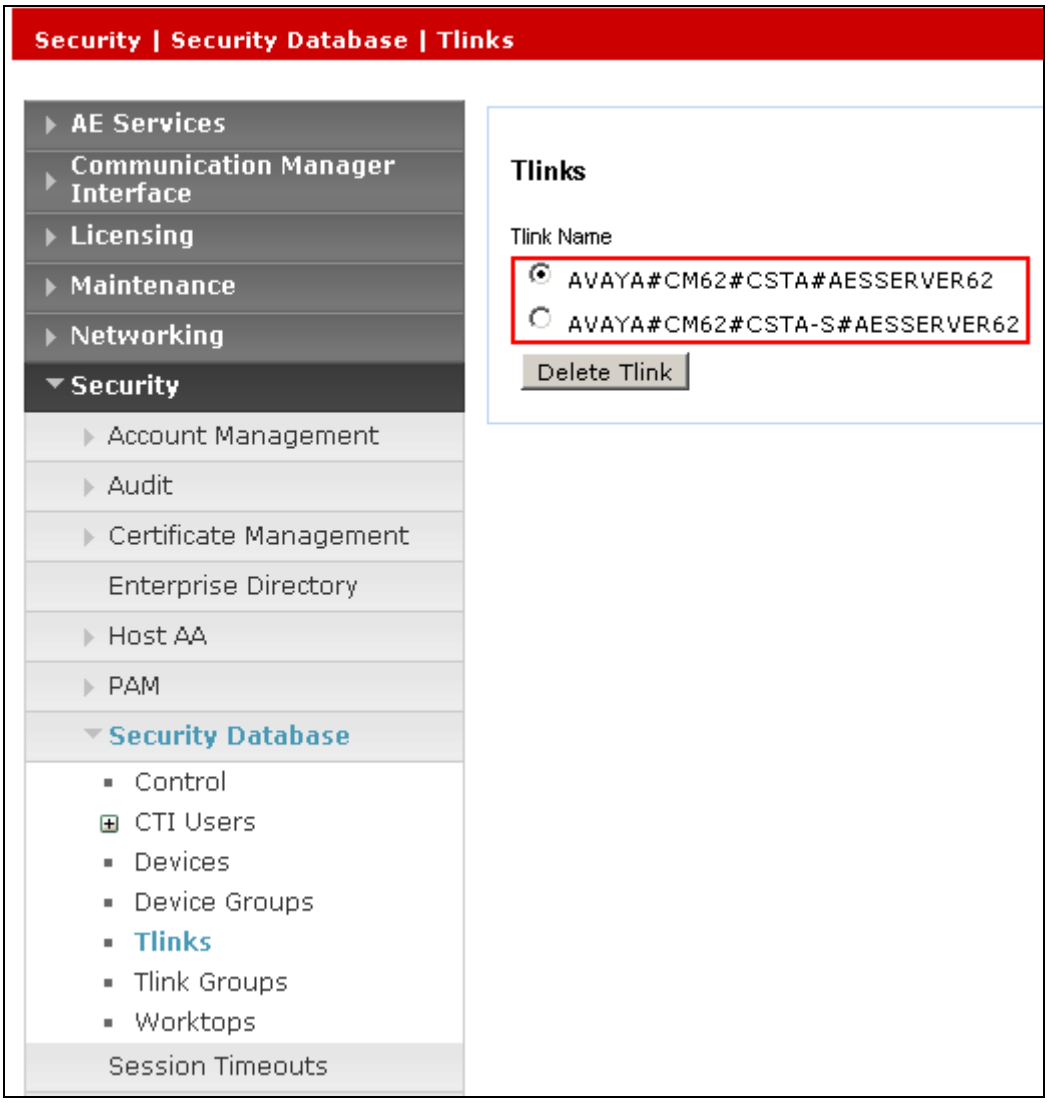
6.4. Restart TSAPI Service

Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check the **TSAPI Service**, and click **Restart Service.**



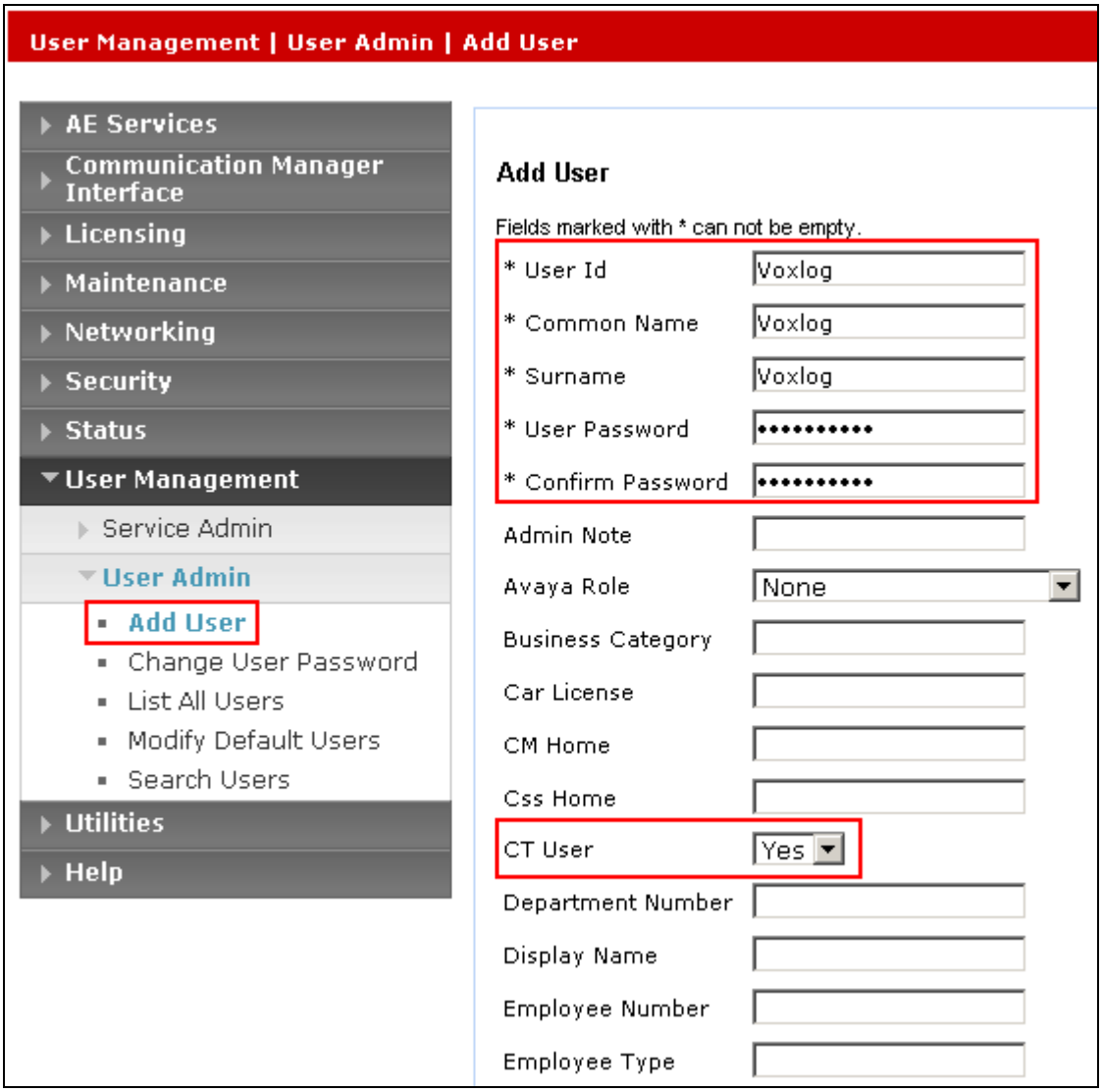
6.5. Obtain Tlink Name

Select **Security → Security Database → Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name.

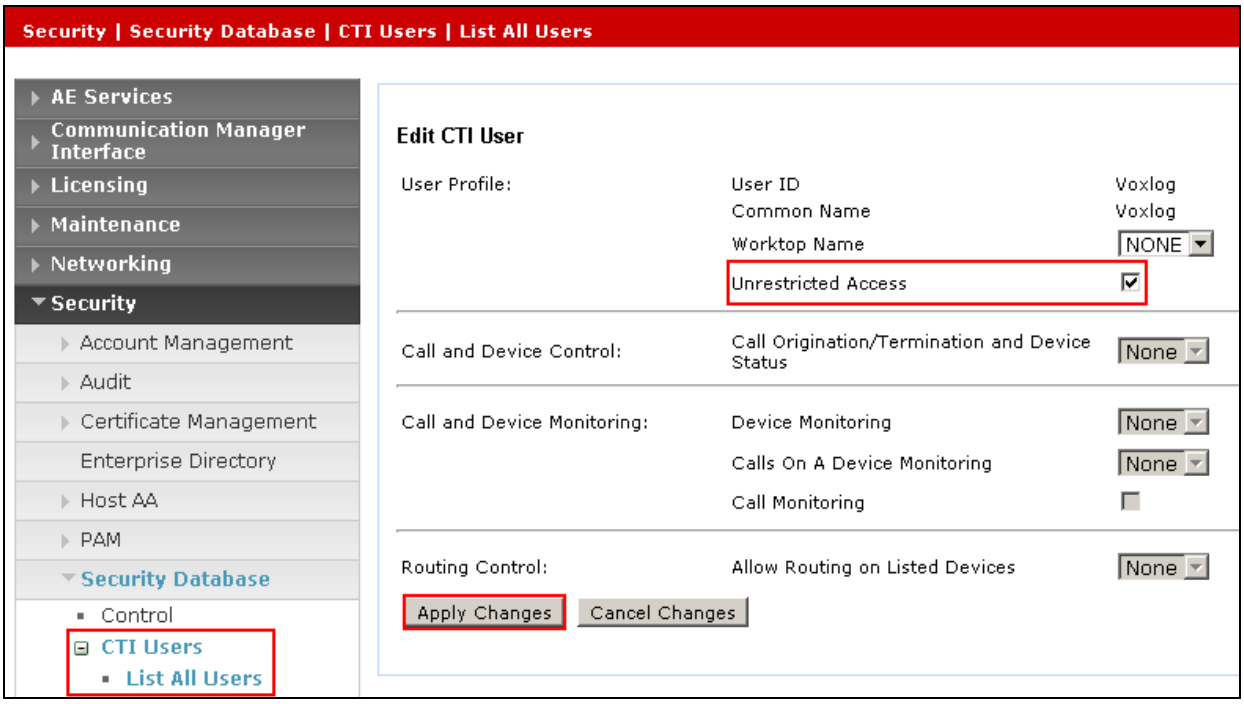


6.6. Administer CTI User

In this section a CTI user is configured for Voxtronic Communication Server to communicate with 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 **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).

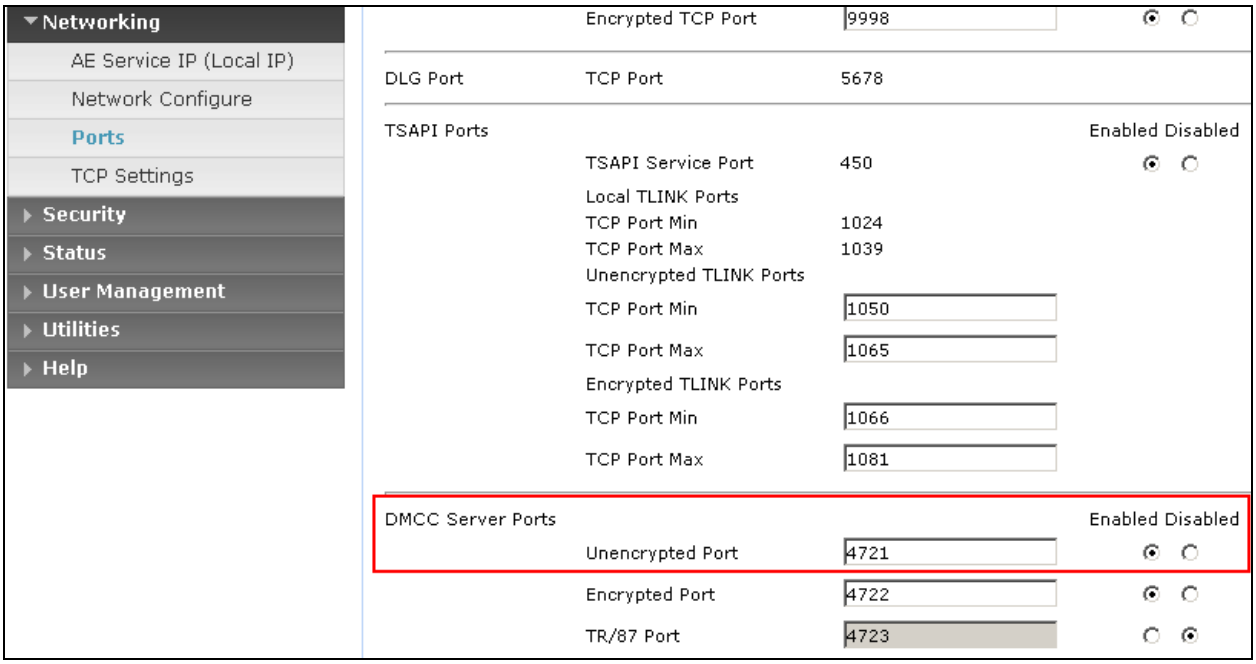


This user should be configured as an unrestricted user. Select **Security→ Security Database → CTI Users → List All Users** from the left pane, click on the radio button beside the user created above, in this case, **Voxlog** and click **Edit.** Place a tick in the box next to **Unrestricted Access**, as shown in the image below. Click **Apply Changes** when done.



6.7. Configure Port for Unencrypted DMCC Connection

Click **Networking → Ports**, in the **DMCC Server Ports** section ensure that **Unencrypted Port** is **Enabled** and set to **4721**. Click Apply Changes (not shown) when done.



7. Configure Voxtronic Communication Server

The configuration values for the external interfaces used by Voxtronic Communication Server are read from the **config.xml** configuration file located in the **C:\voxtronic\config\VoxAvayaRps** directory This XML property file contains a series of keys and associated values for various interface settings. For the purposes of the compliance test the following configuration file was used where the following values pertinent to the connection the Avaya solution are highlighted:

- <entry key="voxlogMode">CALL_BASED</entry> - the recording mode is defined
- <entry key="recordingMethod">SINGLE_STEP_CONFERENCING</entry> - the recording method is defined
- <entry key="switchLinkName">CM62</entry> - enter the Switch Link Name configured in **Section 6.2**
- <entry key="CMServerIpAddr">10.10.16.142</entry> - enter the IP address of the procr
- <entry key="DMCCServerIpAddr">10.10.16.170</entry> - enter the IP address of Application Enablement Services
- <entry key="DMCCServerIpAddr">10.10.16.170</entry> - enter the IP address of Application Enablement Services
- <entry key="DMCCServerUserName">Voxlog</entry> - enter the CTI User configured in **Section 6.6**
- <entry key="DMCCServerPassword">Voxlog123!</entry> - enter the CTI User password configured in **Section 6.6**
- <entry key="voxGenericRpsIpAddr">10.10.16.183</entry> - enter the Voxtronic Communication Server IP address
- <entry key="voxMsFwIpAddr">10.10.16.183</entry> - enter the Voxtronic Communication Server IP address
- <entry key="dispatcherDevices">6000, 6001, 6002, 6003</entry> - enter the extension numbers to be monitored, in this instance SIP and H.323 extensions 6000-6003 were monitored
- <entry key="recordingDevices">6500, 6501, 6502, 6503, 6504, 6505, 6506, 6507</entry> - enter the Single Step Conference stations configured in **Section 5.2**
- <entry key="commonRDPassword">1234</entry> - enter the Security Code assigned to the Single Step Conference stations configured in **Section 5.2**
- <entry key="recorderCodecs">g711A, g711U</antry> - enter the codecs used

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?><properties>
      <comment>Config file of Avaya RPS for AVAYA client side IP
recording</comment>
      <entry key="ModuleEnabled">true</entry>

      <!-- 1.  Logger instance-id:
                  Logger-A: Logger-A
                  Logger-B: Logger-B
                  ================== -->
      <entry key="loggerId">Logger-A</entry>
```

```
<!-- 2.  Voxlog recording mode:
         DEVICE_BASED |
         CALL_BASED   |
         CALL_BASED_2 (BLKA) -->
<entry key="voxlogMode">CALL_BASED</entry>

<!-- 3.  Client-side Ip-call recording method:
         SINGLE_STEP_CONFERENCING |
      // SERVICE_OBSERVING |
      // MULTIPLE_REGISTRATIONS -->
<entry key="recordingMethod">SINGLE_STEP_CONFERENCING</entry>

<!-- 4.  Name of the communication link between AES and CM
             TKOPNOCM01
         S8500
         Evolution -->
<entry key="switchLinkName">CM62</entry>

<!-- 5.  CM-Server: IP-Address
             90.126.77.135
         10.64.120.12
         192.168.150.126 -->
<entry key="CMServerIpAddr">10.10.16.142</entry>

<!-- 6.  AES DMCC-Server: IP-Address (See: cmapi.server_ip)
             90.126.77.212
         10.64.120.15
         192.168.150.103 -->
<entry key="DMCCServerIpAddr">10.10.16.170</entry>

<!-- 7.  AES DMCC-Server: Port:      (See: cmapi.server_port)
         Unsecure connection: 4721,
      // Secure   connection: 4722 -->
<entry key="DMCCServerPort">4721</entry>

<!-- 8.  AES DMCC-Server: User name  (See: cmapi.username)
             Logger-A: voxlog1
             Logger-B: voxlog2
             =================
         aessim
         avaya -->
<entry key="DMCCServerUserName">Voxlog</entry>

<!-- 9.  AES DMCC-Server: Password   (See: cmapi.password)
             Voxlog01!
         AESsim123#
         ou812 -->
<entry key="DMCCServerPassword">Voxlog123!</entry>

<!-- 10. Voxlog voxGenericRps: IP-Addresss
             Logger-A: 90.126.70.201
             Logger-B: 90.126.70.202
             =======================
         192.168.1.3
         192.168.150.13 -->
```

```
      <entry key="voxGenericRpsIpAddr">10.10.16.183</entry>

      <!-- 11. Voxlog voxGenericRps: Port
               Voxlog V4  6726
               Voxlog V3: 6814 -->
      <entry key="voxGenericRpsPort">6726</entry>

      <!-- 12. Voxlog voxMsFw: IP-Address
                   Logger-A: 90.126.70.201
                   Logger-B: 90.126.70.202
                   =======================
               90.126.70.202
               10.10.101.225
               192.168.150.13 -->
      <entry key="voxMsFwIpAddr">10.10.16.183</entry>

      <!-- 13. Voxlog voxMsFw: Start of the RTP port-range
               6000 -->
      <entry key="voxMsFwStartPort">6000</entry>

      <!-- 14. Comma-separated list of monitored Dispatcher-Device extensions
by CALL_MODE
               74001491, 74001492, 74001493, 74001494, 74001495, 74001496,
74001497, 74001498, 74001499, 74001500, 74001501, 74001502, 74001503,
74001504, 74001505, 74001506 -->
      <entry key="dispatcherDevices">6000, 6001, 6002, 6003</entry>

      <!-- 15. Comma-separated list of Recording-Device extensions (RD-Pool)
                 Must be provisioned with Avaya Communication Manager (ACM)
                 Logger-A: 798501, 798502, 798503, 798504, 798505, 798506,
798507, 798508, 798509, 798510, 798511, 798512, 798513, 798514, 798515,
798516
                 Logger-B: 798551, 798552, 798553, 798554, 798555, 798556,
798557, 798558, 798559, 798560, 798561, 798562, 798563, 798564, 798565,
798566

==============================================================================
============================================================ -->
      <entry key="recordingDevices">6500, 6501, 6502, 6503, 6504, 6505, 6506,
6507</entry>

      <!-- 16. Common password of all Recording-Devices
               1234 -->
      <entry key="commonRDPassword">1234</entry>

      <!-- 17. Comma-separated list of codecs (g711A,g711U, g723, g729,g729A)
               supported by the recorder: voxMsFw -->
      <entry key="recorderCodecs">g711A, g711U</entry>

      <!-- 18. Size of media packets in milliseconds requested for the
recorder: voxMsFw -->
      <entry key="recorderPacketSize">20</entry>

      <!-- 19. Feature Access Code (FAC) of
               'Service Observing No Talk'     ==> *882, *222
            // 'Service Observing Listen/Talk' ==> *881, *221
```

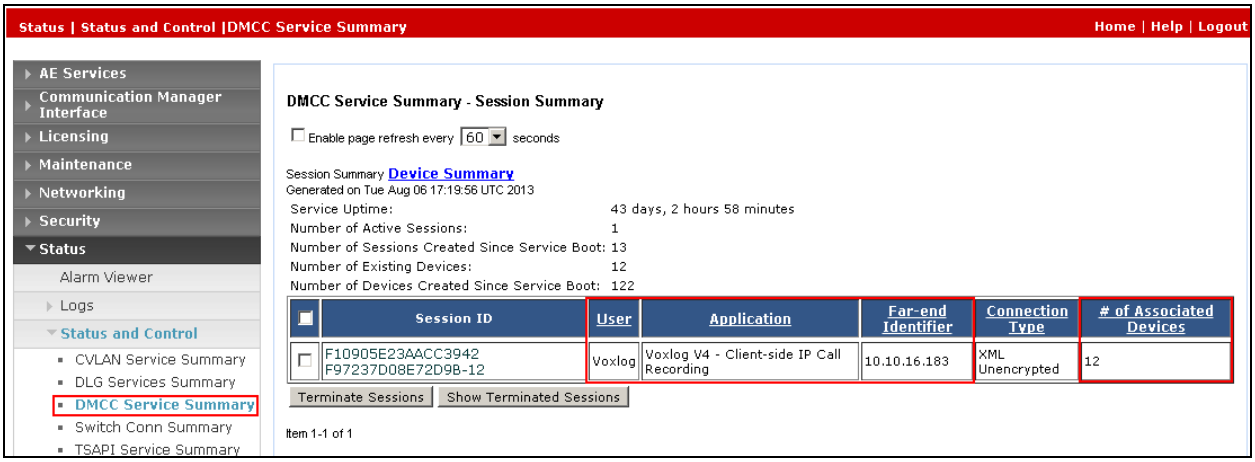
```
               // 'Service Observing Listen Only' ==> *880, *220 -->
      <entry key="serviceObservingFAC">*882</entry>

      <!-- 20. Session duration timer
               5..7200 seconds (heart beat). Default: 60 -->
      <entry key="sessionDurationTimer">60</entry>

      <!-- 21. Session cleanup delay
               0..7200 seconds.  Default: 300 -->
      <entry key="sessionCleanupDelay">300</entry>

      <!-- 22. Application Description -->
      <entry key="applicationDescription">Voxlog V4 - Client-side IP Call
Recording</entry>

      <!-- 23. PBX dialing number (Node Access Code)
                   0891895178
                   90739887 -->
      <entry key="pbxDialNum">0891895178</entry>
</properties>
```

8. Verification Steps

The following steps can be used to verify the correct operation of the Avaya and Voxtronic solution.

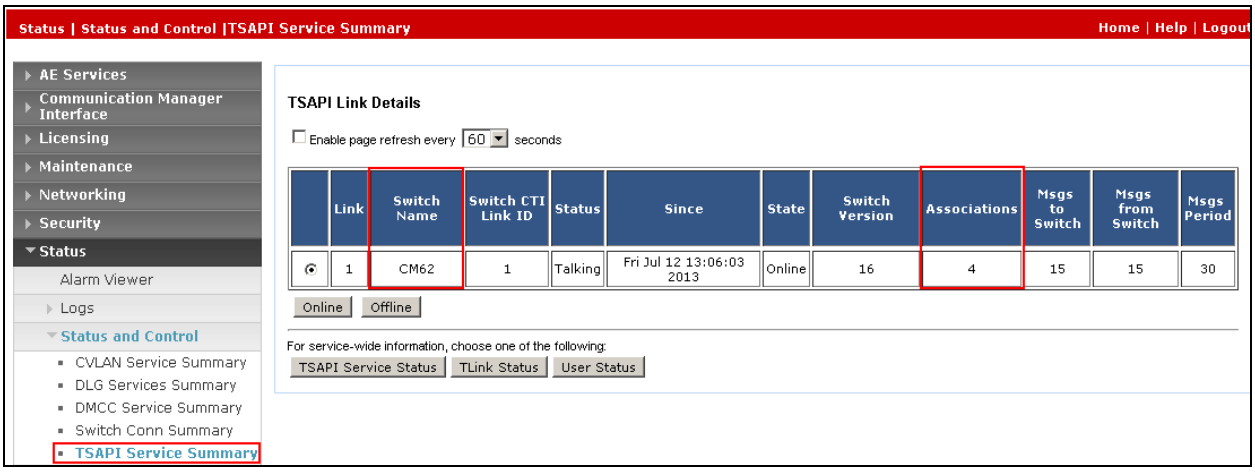
8.1. Verify Avaya Aura® Application Enablement Services DMCC Status

Using the Application Enablement Services web interface click **Status → Status and Control → DMCC Service Summary** confirm that there is an active **Session ID**, the **User** is that configured in **Section 6.6**, the **Application** is **Voxlog V4 – Client-side IP Call Recording** which represents the Voxtronic Communication Server , the **Far-end Identifier** is the IP address assigned to the Voxtronic Communication Server, and the **# of Associated Devices** relates to the number of Single Step Conference recorder stations and monitored stations configured, in this case **12**.



8.2. Verify Avaya Aura® Application Enablement Services TSAPI Status

Using the Application Enablement Services web interface click **Status → Status and Control → TSAPI Service Summary** confirm the number of **Associations** for the relevant **Switch Name** matches the number of monitored stations, in this case **4**.



8.3. Verify Avaya Aura® Communication Manager Single Step Conference Station Registrations

From the SAT enter the command **list registered-ip-stations** and confirm that the configured Single Step Conference Stations **6500-6507** are listed, the **Prod ID/Release** is **IP_API_A 3.2040** and the **Station IP Address** is that of Application Enablement Services and the **Gatekeeper IP Address** is that assigned to the **procr**.

```
list registered-ip-stations                                          Page   1

                              REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ----------------------------------
-----
6500          4624      IP_API_A    y  10.10.16.170
              1         3.2040         10.10.16.142
6501          4624      IP_API_A    y  10.10.16.170
              1         3.2040         10.10.16.142
6502          4624      IP_API_A    y  10.10.16.170
              1         3.2040         10.10.16.142
6503          4624      IP_API_A    y  10.10.16.170
              1         3.2040         10.10.16.142
6504          4624      IP_API_A    y  10.10.16.170
              1         3.2040         10.10.16.142
6505          4624      IP_API_A    y  10.10.16.170
              1         3.2040         10.10.16.142
6506          4624      IP_API_A    y  10.10.16.170
              1         3.2040         10.10.16.142
6507          4624      IP_API_A    y  10.10.16.170
              1         3.2040         10.10.16.142
```

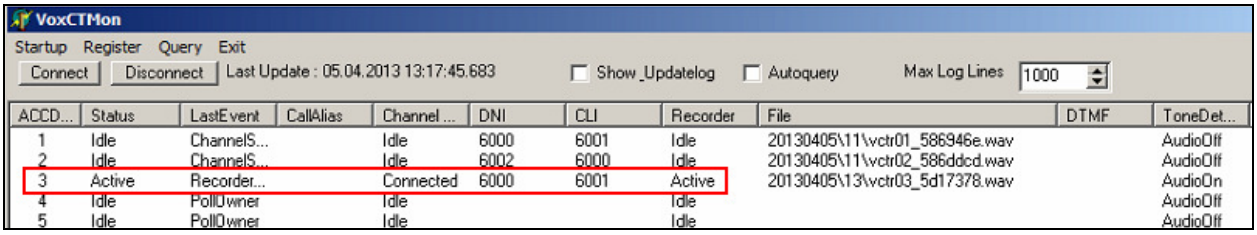
8.4. Verify Avaya Aura® Communication Manager Monitored Stations

From the SAT enter the command **list monitored-station** and confirm the stations which are to have their calls recorded are listed, in this case **6000-6003**

```
list monitored-station

                              MONITORED STATION

  Station    Association 1    Association 2    Association 3    Association 4
  Ext        CTI Link  CRV    CTI Link  CRV    CTI Link  CRV    CTI Link  CRV
  -------     -------------    -------------    -------------    ------------
_
6000           1          15
6001           1          16
6002           1          17
6003           1          18
```

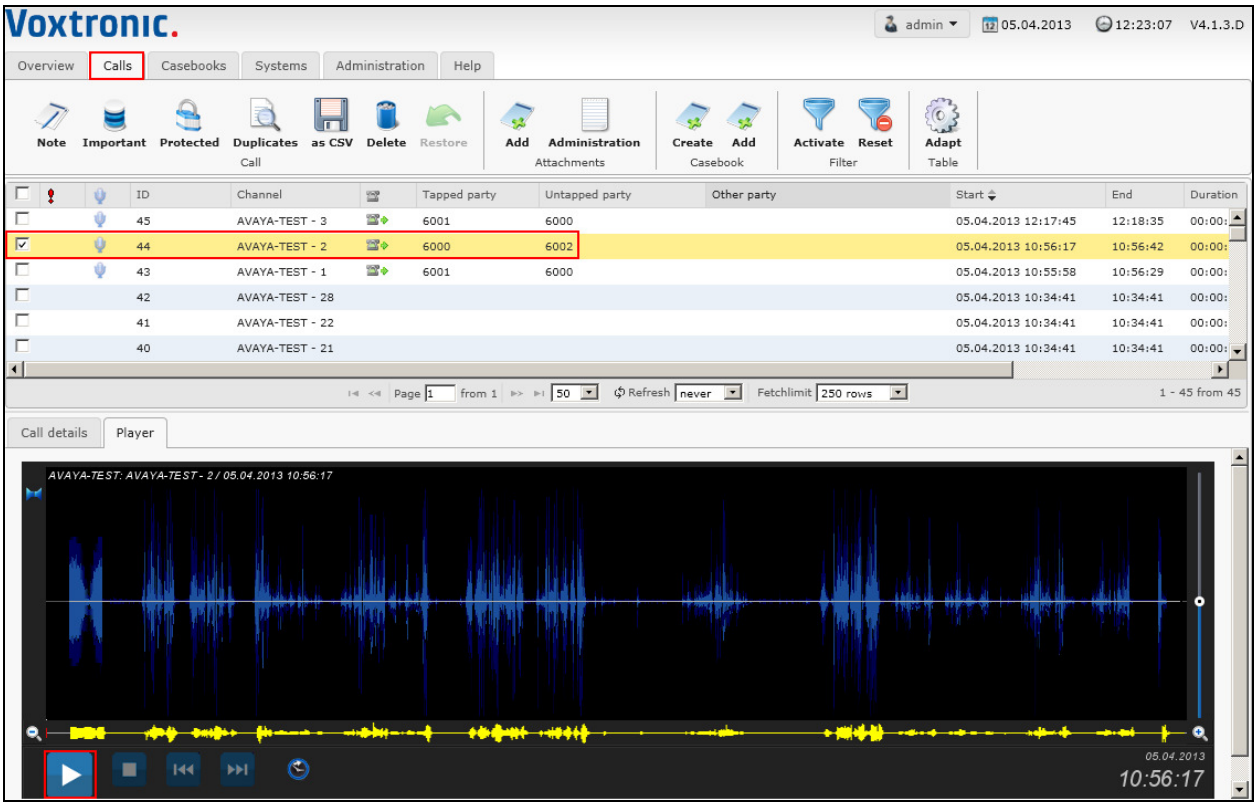
8.5. Verify Voxtronic Communication Server VoxCTMon

From the Voxtronic Server, run the VoxCTMon application from the shortcut on the desktop and ensure that the recorder activity on the is accurately displayed. In this case, extensions **6000** and **6001** are **Active** and being recorded.



8.6. Verify Voxtronic Communication Server Search Results and Playback

From the Voxtronic Communcation Server's web interface, click the **Calls** tab and verify that the recent call activity is accurately displayed. Click the appropriate call for playback and click the **Player** tab click the ▶ icon and verify the expected call audio playback is heard.



9. Conclusion

These Application Notes describe the required configuration steps for Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Voxtronic Communication Server to successfully record calls using the Single Step Conference Feature. All test cases completed successfully with the observations and exceptions noted in **Section 2.2**

10. Additional References

This section references the product documentations that are relevant to these Application Notes.

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

- *Administering Avaya Aura® Communication Manager, Release 6.2,* 03-300509, Issue 7.0 December 2012

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.